Administering Avaya Aura® Conferencing

Release 8.0.1
04-604453
Issue 1
October 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.

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

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

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

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

License types

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

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or

corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with 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.

Virtualization

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

Third Party Components

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

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

Note to Service Provider

The product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

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.

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.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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.

Contents

Chapter 1: Introduction 16
Administrator responsibilities 16
Documentation 17
Administration 17
Overview 18
Supporting 18
Implementation 19
Deploying online help 20
Supported hardware 21
Chapter 2: Management Tools 23
System Manager overview 23
Managing roles 25
Element Manager Console overview 39
Element Manager Console window 40
Tool bar 41
Logical and physical views of network elements 42
Recommended PC hardware and software requirements for running Element Manager Console 43
Logging on to Element Manager Console 44
Logging off from Element Manager Console 48
Provisioning Client overview 48
Recommended PC hardware and software requirements for running Provisioning Client 48
Logging on to Provisioning Client 49
Logging off from Provisioning Client 52
Chapter 3: Managing Users and Templates 53
Managing Users 53
Searching for a user 54
Adding a user from System Manager 55
Adding a user from Provisioning Client 63
Modifying a user 68
Modifying multiple users at one time 69
Modifying a user's conferencing settings 71
Deleting a user 73
Managing User Templates 74
Adding a user template 75
Modifying a user template 76
Deleting a user template 77
Viewing the list of operators 77
Operators page field descriptions 78

Chapter 4: Managing Loads and Patches 79
About loads and patches 79
Viewing the information for a load or patch 79
Installing a patch 79
Upgrading a network element instance 80
Viewing the version information for the Avaya Aura® Conferencing software installed on the server 80
Chapter 5: Customizing Collaboration Agent 81
Creating a custom theme for Collaboration Agent 87
Downloading the sample theme 88
Modifying the theme colors for Collaboration Agent 89
Modifying the logos for Collaboration Agent 91
Modifying the title and header for Collaboration Agent 92
Preparing the custom theme for upload 93
Modifying a custom theme for Collaboration Agent 94
Applying a custom theme for Collaboration Agent 94
Replacing the custom theme for Collaboration Agent 95
Removing the custom theme for Collaboration Agent 96
Downloading the custom theme for Collaboration Agent 97
Forcing an update to the custom theme for Collaboration Agent 98
Retaining/restoring logo customizations during an upgrade 99
Chapter 6: Managing the Avaya Aura® Conferencing Default Settings 102
Configuring the system operator 103
Modifying the conference class of service for the guest login 103
Modifying the maximum participant/moderator code entry attempts setting 104
Modifying the media cascading setting 104
Modifying the conferencing fast start setting 105
Modifying the conferencing continuation setting 105
Modifying the bandwidth management setting 106
Modifying the recording setting 107
Modifying the user password owned locally setting 107
Modifying the Collaboration Agent plug-in setting 108
Modifying the Presentation Mode setting 109
System Default Settings page field descriptions 109
Chapter 8: Managing Your Domains 112
Viewing user domains 112
User Domains page field descriptions 113
Viewing LDAP domains 113
Adding a user domain 113
Adding an LDAP domain 114
Deleting a domain 114
Chapter 9: Managing Locations 116
Adding a location 116

Location page field descriptions..... 117
Add Location page field descriptions..... 117
Modifying a location..... 117
Modify Location page field descriptions..... 118
Deleting a location..... 118
Modifying location settings..... 119
Modify Location Settings page field descriptions..... 119
Configuring IP address patterns..... 119
Location Address Patterns page field descriptions..... 120
Adding an IP address pattern..... 121
Copying an IP address pattern..... 121
Deleting an IP address pattern..... 122
Optimizing the bandwidth for a location..... 122
Bandwidth Optimization page field descriptions..... 123
Configuring media stream cascading for a location..... 124
Media Stream Cascading tab field descriptions..... 124
Configuring a hosting location..... 126
Hosting Locations tab field descriptions..... 126
Configuring a regional cascading location..... 127
Media Cascading Locations tab field descriptions..... 128
Configuring locations and media server clusters for recording..... 129
Chapter 10: Managing Conference Access Numbers..... 131
Managing Conference Access Numbers..... 131
Adding a conference access number..... 131
Modifying a conference access number..... 133
Deleting a conference access number..... 133
Managing Conference Access Numbers Displayed in Collaboration Agent..... 134
Adding a conference access number to be displayed in Collaboration Agent..... 134
Modifying a conference access number displayed in Collaboration Agent..... 135
Changing the order of conference access numbers displayed in Collaboration Agent..... 135
Deleting a conference access number displayed in Collaboration Agent..... 136
Chapter 11: Managing Video Class of Service..... 137
Adding a video class of service..... 137
Video Class of Service page field descriptions..... 137
Modifying a video class of service..... 138
Deleting a video class of service..... 139
Chapter 12: Managing Conference Class of Service..... 140
Adding a conference class of service..... 140
Conference Class of Service page field descriptions..... 140
Modifying a conference class of service..... 141
Viewing the users assigned to a conference class of service..... 142
List of Users page field descriptions..... 142
Deleting a conference class of service..... 143

Chapter 13: Managing IP Addresses 144
Adding an IP address 144
Modifying an IP address 144
Deleting an IP address 145
Chapter 14: Managing External Nodes 146
Adding an external node 146
Modifying an external node 146
Add/Edit External Node dialog box field descriptions 147
Deleting an external node 147
Chapter 15: Managing Avaya Aura System Manager Elements 148
Does this section apply? 148
Modifying the Avaya Aura® System Manager element 148
Refreshing the Avaya Aura® System Manager element 148
Chapter 16: Managing Avaya Aura Session Manager Elements 150
Does this section apply? 150
Adding an Avaya Aura® Session Manager element 150
Modifying an Avaya Aura® Session Manager element 150
Add/Edit Session Manager dialog box field descriptions 151
Deleting an Avaya Aura® Session Manager element 152
Refreshing an Avaya Aura® Session Manager element 152
Chapter 17: Managing OAM Profiles 153
Managing OSS Servers 153
Adding an OSS server 153
Modifying an OSS server 153
Deleting an OSS server 154
Refreshing an OSS server 154
Managing OSS Endpoints 154
Adding an OSS endpoint 154
Modifying an OSS endpoint 155
Deleting an OSS endpoint 155
Refreshing an OSS endpoint 155
Managing FTP Push Destinations 156
Adding an FTP push destination 156
Modifying an FTP push destination 156
Deleting an FTP push destination 156
Refreshing an FTP push destination 157
Managing Log Filters 157
Adding a log filter 157
Modifying a log filter 157
Deleting a log filter 158
Refreshing a log filter 158
Managing Log Browser Feeds 159
Modifying a log browser feed 159

Refreshing the log browser feed 159
Managing SNMP Managers 159
Adding an SNMP manager 159
Modifying an SNMP manager 160
Deleting an SNMP manager 160
Chapter 18: Security 161
Configuring Cipher Suites 161
Configuring OAMP channel cipher suites 161
Configuring external OAMP cipher suites 161
Configuring HTTPS cipher suites 162
Configuring signaling cipher suites 162
Managing Certificates 163
Creating a certificate for network elements 163
Managing Keystore Certificates 163
Managing Truststore Certificates 164
Managing Certificate Revocation Lists 165
Modifying the SRTP settings 166
SRTP Settings dialog box field descriptions 166
Chapter 19: Managing Servers 169
Adding a server 169
Modifying a server 169
Add/Edit Server dialog box field descriptions 170
Deleting a server 170
Configuring alarm thresholds for a server 171
Starting the monitor service for a server 171
Stopping the monitor service for a server 172
Generating an analysis of all servers 172
Chapter 20: Managing SNMP Profiles 173
Adding an SNMP profile 173
Modifying an SNMP profile 173
Add/Edit Server SNMP Profiles dialog box field descriptions 174
Deleting an SNMP profile 174
Associating an SNMP profile with a server 174
Chapter 21: Managing the Database 176
Adding a database instance 176
Deleting a database instance 176
Starting the monitor service for the database 176
Stopping the monitor service for the database 177
Chapter 22: Managing the Element Manager 178
Modifying the element manager 178
Add/Edit Element Manager dialog box field descriptions 178
Modifying the configuration parameters of the element manager 179
Element Manager Configuration Parameters window field descriptions 179

Managing element manager instances ... 181
Adding an element manager instance ... 181
Modifying an element manager instance ... 182
Deleting an element manager instance ... 182
Deploying an element manager instance ... 183
Undeploying an element manager instance ... 183
Starting an element manager instance ... 183
Stopping an element manager instance ... 183
Restarting an element manager instance ... 184
Killing an element manager instance ... 184
Viewing the details for an element manager instance ... 184
Managing SNMP Managers for the element manager ... 185
Adding an SNMP Manager for the element manager ... 185
Modifying an SNMP Manager for the element manager ... 185
Deleting an SNMP Manager for the element manager ... 186
Managing log processing rules for the element manager ... 186
Enabling a log rule for the element manager ... 186
Disabling a log rule for the element manager ... 186
Managing log storage rules for the element manager ... 187
Managing log north bound server feed rules for the element manager ... 189
Managing log UDP client feed rules ... 191
Managing log FTP push rules for the element manager ... 192
Chapter 23: Managing Accounting Managers ... 194
Adding an accounting manager ... 194
Modifying an accounting manager ... 194
Add/Edit Accounting Manager dialog box field descriptions ... 195
Deleting an accounting manager ... 195
Managing accounting manager instances ... 196
Adding an accounting manager instance ... 196
Modifying an accounting manager instance ... 196
Deleting an accounting manager instance ... 196
Starting an accounting manager instance ... 197
Stopping an accounting manager instance ... 197
Restarting an accounting manager instance ... 197
Deploying an accounting manager instance ... 198
Undeploying an accounting manager instance ... 198
Killing an accounting manager instance ... 198
Viewing the details for an accounting manager instance ... 199
Managing accounting rules for an accounting manager ... 199
Enabling an accounting rule for an accounting manager ... 199
Disabling an accounting rule for an accounting manager ... 199
Managing storage rules for an accounting manager ... 200
Managing north bound server feed rules for an accounting manager ... 202

Managing FTP push rules for an accounting manager 204
Chapter 24: Managing Provisioning Managers 208
Adding a provisioning manager 208
Modifying a provisioning manager 208
Add/Edit Provisioning Manager dialog box field descriptions 209
Deleting a provisioning manager 210
Modifying the configuration parameters of a provisioning manager 210
Provisioning Manager Configuration Parameters window field descriptions 211
Managing provisioning manager instances 215
Adding a provisioning manager instance 215
Modifying a provisioning manager instance 216
Deleting a provisioning manager instance 216
Deploying a provisioning manager instance 217
Undeploying a provisioning manager instance 217
Starting a provisioning manager instance 217
Stopping a provisioning manager instance 217
Restarting a provisioning manager instance 218
Killing a provisioning manager instance 218
Viewing the details for a provisioning manager instance 218
Chapter 25: Managing Collaboration Agent Managers 220
Adding a Collaboration Agent manager 220
Add/Edit Collaboration Agent Manager dialog box field descriptions 220
Modifying a Collaboration Agent manager 221
Deleting a Collaboration Agent manager 221
Modifying the configuration parameters of a Collaboration Agent manager 222
Managing Collaboration Agent Managers instances 222
Adding a Collaboration Agent manager instance 222
Modifying a Collaboration Agent manager instance 223
Deleting a Collaboration Agent manager instance 223
Deploying a Collaboration Agent manager instance 223
Undeploying a Collaboration Agent manager instance 224
Starting a Collaboration Agent manager instance 224
Stopping a Collaboration Agent manager instance 224
Restarting a Collaboration Agent manager instance 225
Killing a Collaboration Agent manager instance 225
Viewing the details for a Collaboration Agent manager instance 225
Chapter 26: Managing Application Servers 227
Adding an application server 227
Add/Edit Application Server dialog box field descriptions 227
Modifying an application server 228
Deleting an application server 228
Modifying the configuration parameters of an application server 229
Application Server Configuration Parameters field descriptions 229

Modifying the active speaker reporting interval..... 239
Specifying the Avaya Aura® Session Manager that manages bandwidth for an application server..... 239
Managing application server instances..... 240
Adding an application server instance..... 240
Modifying an application server instance..... 240
Deleting an application server instance..... 241
Deploying an application server instance..... 241
Undeploying an application server instance..... 241
Starting an application server instance..... 242
Stopping an application server instance..... 242
Restarting an application server instance..... 242
Killing an application server instance..... 243
Viewing the details for an application server instance..... 243
Chapter 27: Managing Media Servers..... 244
Adding a media server..... 244
Modifying a media server..... 244
Add/Edit Media Server dialog box field descriptions..... 245
Deleting a media server..... 245
Modifying the configuration parameters of a media server..... 246
Media Server Configuration Parameters window field descriptions..... 246
Configuring logs for a media server..... 249
Downloading logs for a media server..... 250
Accessing the session detail record browser for a media server..... 250
Managing Media Server Instances..... 250
Adding a media server instance..... 250
Modifying a media server instance..... 251
Deleting a media server instance..... 251
Deploying a media server instance..... 252
Undeploying a media server instance..... 252
Starting a media server instance..... 252
Stopping a media server instance..... 253
Restarting a media server instance..... 253
Killing a media server instance..... 253
Viewing the details for a media server instance..... 254
Locking the service maintenance of a media server..... 254
Administering a pending lock on the service maintenance of a media server..... 254
Unlocking the service maintenance of a media server..... 255
Managing Custom Prompts..... 255
About custom prompts..... 255
Uploading custom prompts to the media servers..... 263
Downloading custom prompts from the media servers..... 264
Downloading default prompts from the media servers..... 265

Deleting custom prompts from the media servers ... 265
Managing Custom Music on Wait ... 266
About custom music on wait files ... 266
Uploading custom music on wait files to the media servers ... 266
Downloading custom music on wait files from the media servers ... 267
Deleting custom music on wait files from the media servers ... 268
Managing Media Server Resources ... 269
Associating a media server cluster with a location ... 269
Assigning a media server cluster to a physical location (by location) ... 270
Assigning a media server cluster to a physical location (by media server cluster) ... 272
Configuring media stream cascading for a location ... 272
Configuring a hosting location ... 276
Configuring a regional cascading location ... 277
Configuring media server clusters for an Event conference ... 279
Chapter 28: Managing Media Server Clusters ... 281
Adding a media server cluster ... 281
Add/Edit Media Server Cluster dialog box field descriptions ... 281
Modifying a media server cluster ... 282
Deleting a media server cluster ... 282
Modifying the default media server cluster ... 283
Modifying the database replication settings for a media server cluster ... 283
Modifying the audio codec settings for a media server cluster ... 283
Media Server Cluster Audio Codec Settings dialog box field descriptions ... 284
Modifying the recording trunk codec settings ... 285
Recording Trunk Codec Settings dialog box field descriptions ... 285
Modifying the cascading trunk codec settings ... 285
Cascading Trunk Codec Settings dialog box field descriptions ... 286
Modifying the media port settings for a media server cluster ... 286
Modifying the DSCP settings for a media server cluster ... 286
Modifying the video settings for a media server cluster ... 287
Media Server Cluster Video Settings dialog box field descriptions ... 287
Modifying the trace file history settings for a media server cluster ... 288
Modifying the comfort noise setting for a media server cluster ... 288
Media Server Cluster Comfort Noise Settings dialog box field descriptions ... 289
Associating a media server cluster with a location ... 289
Media Server Serving Locations tab field descriptions ... 289
Assigning a media server cluster to a physical location (by media server cluster) ... 290
Media Server Cluster Physical Location tab field descriptions ... 291
Assigning a media server cluster to a physical location (by location) ... 292
Configuring media server clusters for an Event conference ... 293
Media Server Clusters for Event Conference field descriptions ... 293
Chapter 29: Managing Web Conferencing ... 295
A single document conversion server (DCS) or multiple DCSs? ... 295

Managing document conversion servers 295
Adding a web conferencing document conversion server 296
Modifying a web conferencing document conversion server 297
Modifying the configuration parameters of a document conversion server 297
Deleting a web conferencing document conversion server 300
Configuring the default document conversion server 300
Managing document conversion server instances 301
Deploying a document conversion server instance 301
Undeploying a document conversion server instance 301
Starting a document conversion server instance 302
Stopping a document conversion server instance 302
Restarting a document conversion server instance 302
Killing a document conversion server instance 303
Modifying a document conversion server instance 303
Assigning document conversion servers to locations 305
Managing Web Conferencing Management Servers 305
Adding a web conferencing management server 305
Modifying a web conferencing management server 306
Deleting a web conferencing management server 307
Modifying the configuration parameters of a web conferencing management server 307
Modifying the meeting event processor for a web conferencing management server 309
Managing Web Conferencing Management Server Instances 309
Managing Web Conferencing Servers 313
Adding a web conferencing server 313
Modifying a web conferencing server 314
Deleting a web conferencing server 314
Modifying the configuration parameters of a web conferencing server 315
Managing Web Conferencing Server Instances 317
Managing Web Conferencing Server Clusters 320
Web Conferencing Server (WCS) clusters 320
Updating the host table entries 329
Modifying the Collaboration Library settings 330
Collaboration Library dialog box field descriptions 331
Setting a web conferencing host name 331
Web Conferencing Host page field descriptions 331
Chapter 30: Managing Audio and Video SRTP 332
Administering the SRTP settings for Avaya Aura Conferencing 333
SRTP Settings dialog box field descriptions 334
Modifying Communication Manager settings for SRTP 336
Communication Manager field descriptions 338
Chapter 31: Managing the Recording feature 340
Configuring the system-wide Recording setting 340
Assign a Recording media server cluster to locations 340

Modifying a single user ... 341
Scheduling a backup and/or purge of the Recording server ... 341
Backup/Purge Settings dialog box field descriptions ... 342
Backing up and/or purging the Recording server now ... 343
Modifying the backup/purge settings for the Recording server ... 344
Modifying the purge threshold settings for the Recording server ... 344
Purge Thresholds dialog box field descriptions ... 345
Restoring a backup to the Recording server ... 345
Managing Recording server backup locations ... 346
Adding a backup location for the Recording server ... 346
Modifying a backup location for the Recording server ... 347
Deleting a backup location for the Recording server ... 347
Chapter 32: Managing LDAP directory integration ... 349
Managing the directory access servers ... 349
Modifying the connection credentials for directory access servers ... 349
Modifying the directory access servers for synchronization ... 350
Modifying the directory access servers for user authentication ... 351
Managing the synchronization service ... 352
Modifying the directory synchronization timeouts ... 352
Configuring directory synchronization filters ... 352
Configuring a directory synchronization schema ... 354
Performing a directory synchronization now ... 357
Scheduling a directory synchronization ... 358
Testing the directory synchronization connection and schema ... 358
Modifying the directory authentication timeouts ... 359
Configuring the directory access passcode ... 360
Modify Auth Passcode page field descriptions ... 360
Configuring enterprise domain authentication ... 361
Modify Auth Schema page field descriptions ... 361
Configuring LDAP directory-synchronized users on System Manager ... 362
Chapter 33: Element Manager Console Local Logon Administration Tasks ... 364
Changing the password for your local logon user ID for Element Manager Console ... 365
Changing the password for the other local logon user IDs for Element Manager Console ... 365
Configuring the password rules for the local logon user IDs for Element Manager Console ... 366
Password Rules dialog box field descriptions ... 366
Configuring the login rules for the local logon user IDs for Element Manager Console and Provisioning Client ... 368
Login Rules dialog box field descriptions ... 369
Forcing off a user logged into Element Manager Console ... 369
Viewing the users logged into Element Manager Console ... 370
Chapter 34: Importing and Exporting Data ... 371
Importing configuration data into Element Manager Console ... 371
Exporting configuration data from Element Manager Console ... 371

Chapter 35: Deploying the Avaya Aura® Conference Manager Add-in for Microsoft Outlook® 373
Implementing a ClickOnce deployment 374
Implementing a centralized software deployment 375

Chapter 1: Introduction

This document provides the procedures that you perform to administer an Avaya Aura® Conferencing 8.0 system that has been installed and initially configured. Using this document, you can:

- add and manage Avaya Aura® Conferencing user accounts and capabilities
- install software patches
- modify the Avaya Aura® Conferencing system settings
- add and manage conference access numbers
- add and manage Avaya Aura® Conferencing components (such as servers, media servers, media server clusters, and network elements)
- add and manage web conferencing components and capabilities

Related Links

Administrator responsibilities on page 16
Documentation on page 17
Deploying online help on page 20
Supported hardware on page 21

Administrator responsibilities

As the administrator for Avaya Aura® Conferencing 8.0, you are responsible for:

- managing Avaya Aura® Conferencing users
- managing software loads and patches
- managing Avaya Aura® Conferencing network elements (for example, media servers, media server clusters, and web conferencing resources)
- managing system security
- monitoring system alarms and logs
- monitoring system performance
- backing up the Avaya Aura® Conferencing system periodically
- restore the Avaya Aura® Conferencing system in the event of data loss

Related Links

Introduction on page 16

Documentation

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

The Avaya Support website also includes the latest information about product compatibility, ports and Avaya Aura® Conferencing releases.

Related Links

Introduction on page 16
Administration on page 17
Overview on page 18
Supporting on page 18
Implementation on page 19

Administration

Document number	Title	Use this document to:	Audience
04-604378	*Administering Avaya Aura® Conferencing*	Perform system-wide administration tasks	System administrators
04-604403	*Migrating Avaya Aura® Conferencing*	Perform system-wide security administration and backup/restore tasks	System administrators
04-604398	*Maintaining and Troubleshooting Avaya Aura® Conferencing*	Perform maintenance and troubleshooting tasks. Understand logs and fault tracking.	System administrators Partners, Services, and Support personnel

Related Links

Documentation on page 17

Overview

Document number	Title	Use this document to:	Audience
04-604343	*Avaya Aura® Conferencing Overview and Specification for Avaya Aura®*	Understand the high-level features and functionality of the product	Customers, Partners, Services, and Support personnel
04-604344	*Avaya Aura® Conferencing Overview and Specification for Turnkey*	Understand the high-level features and functionality of the product	Customers, Partners, Services, and Support personnel
04-604323	*Avaya Aura® Conferencing Solution Description for SME*	Understand the high-level features and functionality of the solution	Customers, Partners, Services, and Support personnel
04-604328	*Avaya Aura® Conferencing Solution Description for Medium Enterprises*	Understand the high-level features and functionality of the solution	Customers, Partners, Services, and Support personnel
04-604333	*Avaya Aura® Conferencing Solution Description for Large Enterprises*	Understand the high-level features and functionality of the solution	Customers, Partners, Services, and Support personnel

Related Links

Documentation on page 17

Supporting

Document number	Title	Use this document to:	Audience
04–604423	*Avaya Aura® Conferencing Accounting Records Reference*	Collect information about accounting records	System administrators Customers, Partners, Services, and Support personnel

Document number	Title	Use this document to:	Audience
04-604443	*Avaya Aura® Conferencing Alarms and Logs Reference*	Collect information about alarms and logs, including the alarms and logs families	System administrators Customers, Partners, Services, and Support personnel
04-604444	*Avaya Aura® Conferencing Operational Measurements Reference*	Collect information about operational measurements	System administrators Customers, Partners, Services, and Support personnel

Related Links

Documentation on page 17

Implementation

Document number	Title	Use this document to:	Audience
04-604418	*Deploying Avaya Aura® Conferencing: Basic Installation*	Perform installation and configuration tasks	Partners, Services, and Support personnel
04-604363	*Deploying Avaya Aura® Conferencing: Advanced Installation and Configuration*	Perform installation and configuration tasks	Partners, Services, and Support personnel
04-604353	*Upgrading Avaya Aura® Conferencing*	Perform upgrading and configuration tasks	Partners, Services, and Support personnel

Related Links

Documentation on page 17

Deploying online help

Avaya Aura® Conferencing contains a number of online help files and online manuals to guide you through the process of installing, configuring, and maintaining your conferencing system. These online help files include:

- Online help for Element Manager
- Online help for the Provisioning Client
- Online help for Reports
- Online help for users of Collaboration Agent

By default, each of these online help packages is fully integrated with the component which it describes. So, for example, if you view help on Element Manager, you can access the Element Manager online help. The Element Manager online help file describes each of the Element Manager fields and describes many of the common procedures that you can perform using the Element Manager interface.

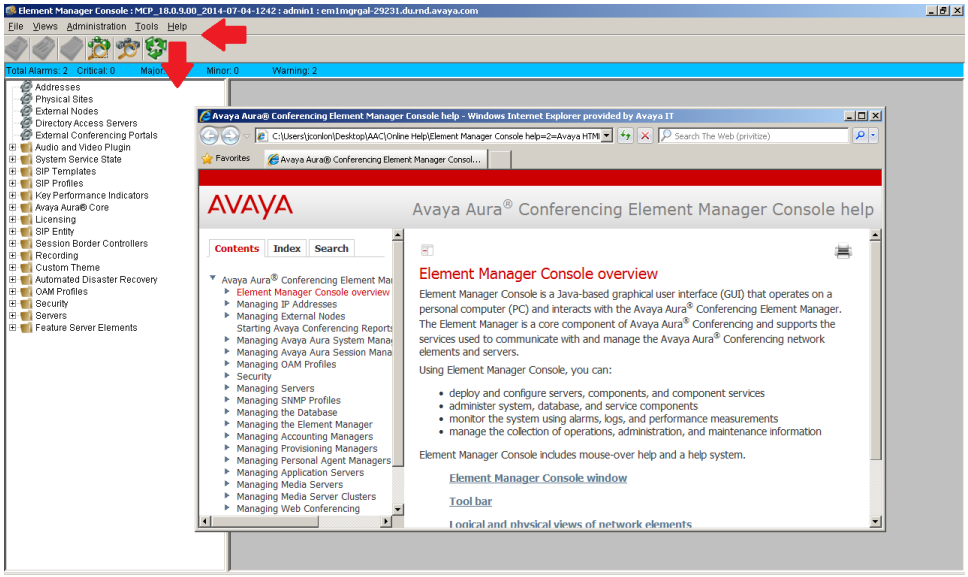


Figure 1: Online Help for Element Manager

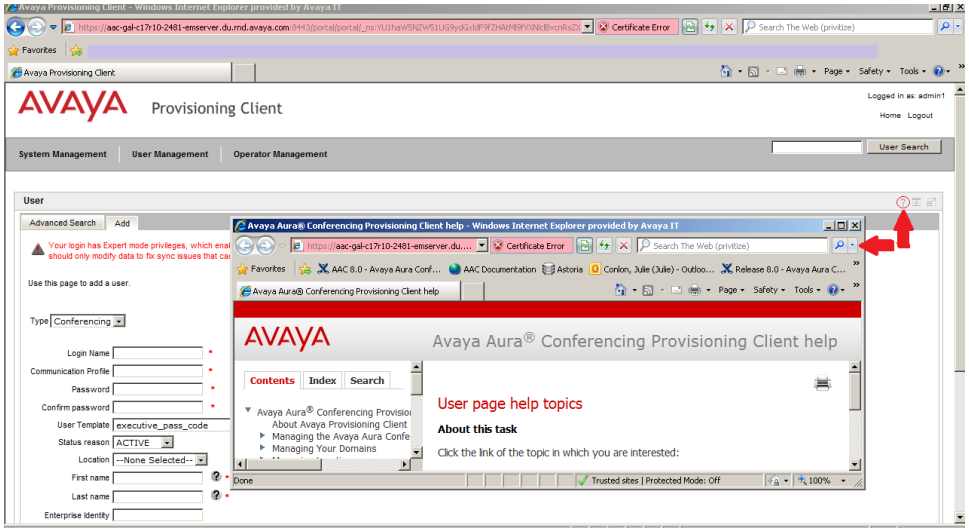


Figure 2: Online Help for the Provisioning Client

In the case of the online help for users of Collaboration Agent, Avaya has translated the online help into several languages. The list of available languages conforms with the i18n and L10n (internationalization and localization standards). When users install the Collaboration Agent application, it chooses which language to display based on the computer's locale.

The online help files are packaged within the Avaya Aura® Conferencing software application bundle.

Related Links

Introduction on page 16

Supported hardware

Avaya Aura® Conferencing 8.0 supports the HP ProLiant DL360p G8 for all deployment configurations. Alternatively, if you have an existing HP ProLiant DL360 G7, you can reuse it. If you have existing Dell 610 or IBM S8800 servers, you may be able to reuse them as cascading Avaya Media Server (MS)'s. However, you cannot reuse the Dell 610 or IBM S8800 servers as Avaya Aura® Conferencing 8.0 core servers.

The hardware requirements for Avaya Aura® Conferencing 8.0 are the same whether you are installing the product in an Avaya Aura® deployment or a Turnkey deployment. In both cases, it is the HP ProLiant DL360p G8 server.

Server type	Supported use
HP ProLiant DL360p G8	Used for new installations of Avaya Aura® Conferencing 8.0.
HP ProLiant DL360 G7	Can be reused when upgrading existing Avaya Aura® Conferencing 7.2 deployments to Avaya Aura® Conferencing 8.0.[1]

Server type	Supported use
Dell 610	Can only be used as cascading media servers within Avaya Aura® Conferencing 8.0 deployments.[2]
IBM S8800	Can only be used as cascading media servers within Avaya Aura® Conferencing 8.0 deployments.[2]

Related Links

Introduction on page 16

[1] For Large deployments (previously known as Standalone in the Avaya Aura® Conferencing 7.x releases) the server hosting the Element Manager and Database must have more than 12GB of RAM. If your server only has 12GB of RAM please contact Avaya for a memory expansion kit and apply this kit prior to the upgrade to Avaya Aura® Conferencing 8.x. For more information on installing and configuring the memory expansion kit, see *Deploying Avaya Aura® Conferencing 7.2.2*, which is available from https://support.avaya.com/.

[2] For more information on cascading media servers, see BROKEN LINK: Configuring cascading.

Chapter 2: Management Tools

To administer Avaya Aura® Conferencing 8.0, you will use the following applications:

- Element Manager Console
- Provisioning Client
- Avaya Aura® System Manager

  System Manager is only required for Avaya Aura® deployments. It is not required for Turnkey deployments.

  Note:

  Avaya Aura® Conferencing supports several releases of System Manager. In some instances, the field names and screen layouts differ slightly from release to release. The field names and screen layouts in this section refer to System Manager 6.2 Feature Pack 4. If you are using a alternative release of System Manager, you can still refer to the same task flow, but be aware that there may be subtle variances between the documented steps and your actual steps.

Related Links

[System Manager overview](#) on page 23
[Element Manager Console overview](#) on page 39
[Provisioning Client overview](#) on page 48

System Manager overview

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

System Manager includes the following shared management services:

Service	Description
Users	Provides features to administer users, shared address, public contact list, and system presence access control list information. You can: • Associate the user profiles with groups, roles, and communication profiles. • Create a contact list.

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

Service	Description
	• Downloading the new release from Avaya PLDS and using for upgrading the device software.

Related Links

Management Tools on page 23

Managing roles

Role Based Access Control

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

- Built-in
- Custom

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

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

Related Links

System Manager overview on page 23

Built-in roles

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

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

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

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

Related Links

System Manager overview on page 23

Custom roles

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

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

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

Related Links

System Manager overview on page 23

Checklist for creating an Avaya Aura® Conferencing custom role

If you want to access Element Manager Console and the Provisioning Client through Avaya Aura® System Manager, you must have an administrative account on Avaya Aura® System Manager that is configured for accessing Avaya Aura® Conferencing. The default administrator account is automatically configured for accessing Avaya Aura® Conferencing. So, you can use the default administrator account. In the Avaya Aura® System Manager interface, the default administrator account has the **User ID** of **admin** and has the **Name**: **Default Administrator** or **Default Security Administrator**. The exact wording depends on your version of Avaya Aura® System Manager. However, Avaya recommends creating a custom role for accessing Avaya Aura® Conferencing. The benefit of creating a custom role is that you can confine the Avaya Aura® Conferencing administrator role to a single element and you can limit the associated rights in accordance with your preferences.

Note:

Unless instructed by Avaya Support, you should always log on to Element Manager Console and the Provisioning Client using single sign-on access through Avaya Aura® System Manager.

No.	Task	Description	Notes	✔
1	Create a custom role on Avaya Aura® System Manager.	Adding a custom role on page 31		
2	Map the **Conferencing** element to this role.	Using templates for mapping permissions on page 33	You can choose from the following permissions for the **Conferencing** element. • **Read**: This is an administrative user that only has read access to Element Manager and Provisioning Manager. This user	

Comments? infodev@avaya.com

No.	Task	Description	Notes	✔
			cannot change any data or manage any network elements. • **Write**: This is an administrative user that has write access to Element Manager and Provisioning Manager. This user can change data but cannot manage network elements. • **Maintenance**: This is an administrative user that can manage (deploy, start, top, undeploy) network elements in the Element Manager Console. • **Expert Mode**: This is an administrative user with all rights available in Avaya Aura® Conferencing.	
3	Map the **Operation** resource type to this role.	Using templates for mapping permissions on page 33	Select the following permissions for the **Operation** resource type. • **Elements** • **Elements/Conferencing** • **Elements/Conferencing/ Dashboard** • **Elements/Conferencing/Sync** (since Avaya Aura® System Manager 6.3.7 Service Pack 7 + Patch and System Manager 6.3.9 Service Pack 9) • **RTS_Administration** (in System Manager 6.3 Feature Pack 1, Feature Pack 2 and Feature Pack 3 and their service packs)	
4	If you have System Manager 6.3 Feature Pack 4 or later, map the **Elements** resource type to this role.	Using templates for mapping permissions on page 33	You can choose from the following permissions for the **Elements** resource type. • **view**: This level allows the administrative user with the role to view items on **Elements** panel in System Manager • **edit**: This level allows the administrative user to edit items on **Elements** panel in System Manager.	

No.	Task	Description	Notes	✔
5	Create a new administrative user on System Manager and assign the role to them.	Assigning users to a role on page 33		

Note:

You do not require RTS_Administration permissions for System Manager 6.2 GA and the associated 6.2 service packs. However, if you migrated from System Manager 6.2 GA or the 6.2 associated service packs to System Manager 6.3 Feature Pack 1–3 or the associated 6.3 service packs, you must add RTS_Administration permissions for your custom role. If you do not add the RTS_Administration permissions, the custom role will not operate successfully.

Note:

You do no require the Elements resource type for System Manager 6.2 GA and the associated 6.2 service packs. However, if you migrated from System Manager 6.2 GA or the associated 6.2 service packs to System Manager 6.3 Feature Pack 4 or later, you must add the Elements resource type for your custom role. If you do not add the Elements resource type, the custom role will not operate successfully.

Tip:

For more information on System Manager, you can download the System Manager documentation set from https://support.avaya.com/.

Related Links

System Manager overview on page 23

Viewing user roles

Procedure

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

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

Related Links

System Manager overview on page 23

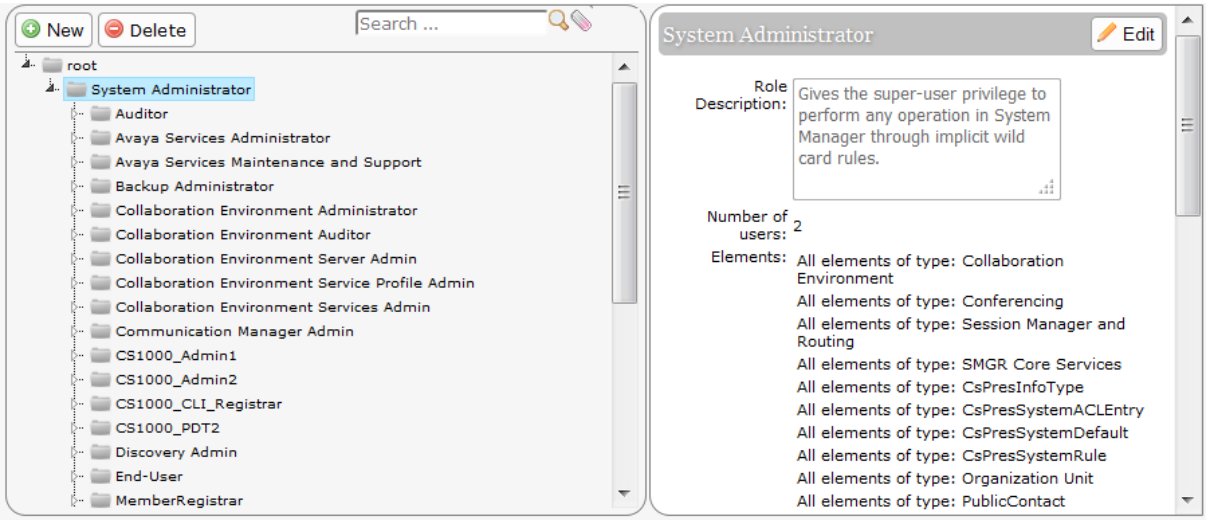
Adding a custom role

Procedure

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

3. On the Roles page, select a role, and perform one of the following:
   - Click **New**.
   - Right-click and select **New**.

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



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

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

   The system displays the Role Details page.

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

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

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

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

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

   The title of the Permission Mapping page displays the element type that you selected.

10. On the Permission Mapping page, change the permissions that are available for this role as appropriate.

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

11. Click **Commit**.

    The system displays the Role Details page and the selected permissions.

12. Click **Commit**.

Related Links

System Manager overview on page 23

Mapping permissions by using the template

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.
4. In the **Element/Service Permissions** tab, click **Add Mapping**.
5. In the **Element or Resource Type** field, select an element, for example, CS 1000.
6. Click **Next**.

   The system displays the permission mapping for the element that you selected.

7. Perform the following as appropriate to modify permissions:
   a. Select a different permission from the **Template for permission set** field.
   b. Select permissions.
   c. Clear permissions.
8. Click **Commit**.

Related Links

System Manager overview on page 23

Assigning users to a role

To assign a role to an end user, follow the instructions outlined in Assigning roles to a user. An end user is a user with no role or the End-User role.

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.
4. On the Role Details page, click the **Assigned Users** tab.
5. Click **Select Users** to assign a role to users or edit a role.

The system displays the Assigned Users page.

Note:

The system does not display end users in the **Assigned Users** list. You can assign a role to an end user from **User Management** > **Manage Users**. For more information, see Assigning roles to a user.

6. Select users to whom you want to assign the role.
7. Click **Commit**.

   The system displays the permissions for the role on the Role Details page.

Related Links

System Manager overview on page 23

Unassigning users from role

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.
4. On the Role Details page, click the **Assigned Users** tab.
5. Click **Selected Users**.
6. On the Assigned Users page, clear the check box of the user whom you want to unassign.
7. Click **Commit**.

Related Links

System Manager overview on page 23

Copying permission mapping for a role

Procedure

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

   The system displays the Permission Mapping page.
6. In the **Copy From Role** field, select a role.

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

Note:

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

7. Click **Copy**.

   The system displays the Role Details page

8. Click **Commit**.

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

Related Links

System Manager overview on page 23

Editing a custom role

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.
4. On the Role Details page, edit the **Role Name** and **Description** fields.
5. Click **Commit and Continue**.
6. On the **Element/Service Permissions** tab, click **Add mapping** and change the permissions for a role as appropriate.

   For more information, see Mapping permissions using the template.

7. Click **Commit**.

Related Links

System Manager overview on page 23

Deleting custom roles

Procedure

1. On the System Manager web console, click **Users** > **Groups & Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select one or more roles that you must delete and perform one of the following:
   - Click **Delete**.
   - Right-click and select **Delete**.
4. On the Delete Roles page, click **Delete** to continue with the deletion.

   When you delete a role, the system deletes all child roles of the role.

You cannot delete the implicit roles from the Roles page. However, the system deletes the implicit roles when the administrator deletes the tenant or site.

Related Links

System Manager overview on page 23

Roles field descriptions

The Roles page contains two panes. The left pane displays the tree structure of roles. The right pane displays the details of the role that you select on the left pane.

Field	Description
Role Description	A brief description of the role
No of users	The number of users associated with the role
Elements	The name of elements that are mapped to the role

Button	Description
New	Displays the Add New Role page where you can add a custom role.
Delete	Displays the Delete Roles page where you can confirm the deletion of the custom role.
Edit	Displays the Role Details page where you can change the custom role.

Icon	Description
	Searches for the role based on the search text.
	Clears the search text.

Related Links

System Manager overview on page 23

Add New Role field descriptions

Field	Description
Parent Role Name	The parent role that you selected on the Roles page to create the new role. **Parent Role Name** is a read-only field.
Role Name	The name of the custom role that you want to add. The name must be 1 to 256 characters long and can include characters: a-z, A-Z, 0-9, -, _, and space. You can add up to 1500 roles.
Role Description	A brief description of the role.

Button	Description
Commit and Continue	Saves the role name and description and takes you to the Roles Details page.
Cancel	Cancels the permission mapping and takes you back to the Roles page.

Related Links

System Manager overview on page 23

Role Details field descriptions

Field	Description
Parent Role Name	The parent role that you selected on the Roles page to create the new role. **Parent Role Name** is a read-only field.
Role Name	The name of the custom role that you want to add. The name must be 1 to 256 characters long and can include characters: a-z, A-Z, 0-9, -, _, and space.
Description	A brief description of the role that you add.

Button	Description
Commit	Saves the changes and returns to the Roles page.
Cancel	Discards the changes to the permission mapping and returns to the Roles page.
Add Mapping	Displays the permissions page where you can map permissions for the role.
Delete Mapping	Displays the Delete Mapping page where you can delete a permissions set.
Copy All From	Displays the Permission Mapping page where you can copy a permission set.

Related Links

System Manager overview on page 23

Add Mapping field descriptions

Field	Description
Group Name	The name of the group that you can select for the role. The options are: • When you select a group, the system disables the **Element or Resource Type** field. • When you do not select a group, the **Element or Resource Type** field is mandatory.

Field	Description
Element or Resource Type	The element types that are available. The system displays elements in **Element or Resource Instance** based on the element type that you select in this field.
Element or Resource Instance	The elements that are available or the resource instance. The field lists the available elements based on the element type that you selected in the **Element or Resource Type** field. When you select a group in **Group Name**, the system disables the **Element or Resource Type** field.

Button	Description
Next	Saves your changes in this page and takes you to the Permission Mapping page.
Cancel	Cancels your selection and takes you to the Roles Details page.

Related Links

System Manager overview on page 23

Assigned Users field descriptions

The system displays the Assigned Users page when you click **Select Users** on the **Assigned Users** tab of the Role Details page. You can select users to grant permissions that are associated with this role.

Field	Description
User Name	The name of the user that you assign to the role.
Full Name	The full name of the user that is assigned to the role.
Type	The type of user. The options are: • **local**: Indicates that users are stored in the directory server of System Manager. • **external**: Indicates that users are stored in the directory server of the customer.

Button	Description
Commit	Assigns the selected users to the role.
Cancel	Cancels the action and returns to the Role Details page.

Related Links

System Manager overview on page 23

Permission mapping field descriptions

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

Field	Description
Copy from Role	The role from where you can copy all permission mappings for the element or service

Button	Description
Copy	Copies the permission mapping for your custom role.
Cancel	Cancels the copy action and returns to the Role Details page.

Related Links

System Manager overview on page 23

Permission mapping field descriptions

The page displays the following fields when you click **Add Mapping** on the Role Details page.

Field	Description
Template for permission set	The permission to which you want to map the role.
Select/Unselect All	A toggle button to select or clear the functions that users with a role can perform on the element.

Button	Description
Commit	Maps the permissions to the custom role.
Cancel	Cancels the permission mapping action and returns to the Role Details page.

Related Links

System Manager overview on page 23

Element Manager Console overview

Element Manager Console is a Java-based graphical user interface (GUI) that operates on a personal computer (PC) and interacts with the Avaya Aura® Conferencing Element Manager. The Element Manager is a core component of Avaya Aura® Conferencing and supports the services used to communicate with and manage the Avaya Aura® Conferencing network elements and servers.

Using Element Manager Console, you can:

- deploy and configure servers, components, and component services
- administer system, database, and service components
- monitor the system using alarms, logs, and performance measurements
- manage the collection of operations, administration, and maintenance information

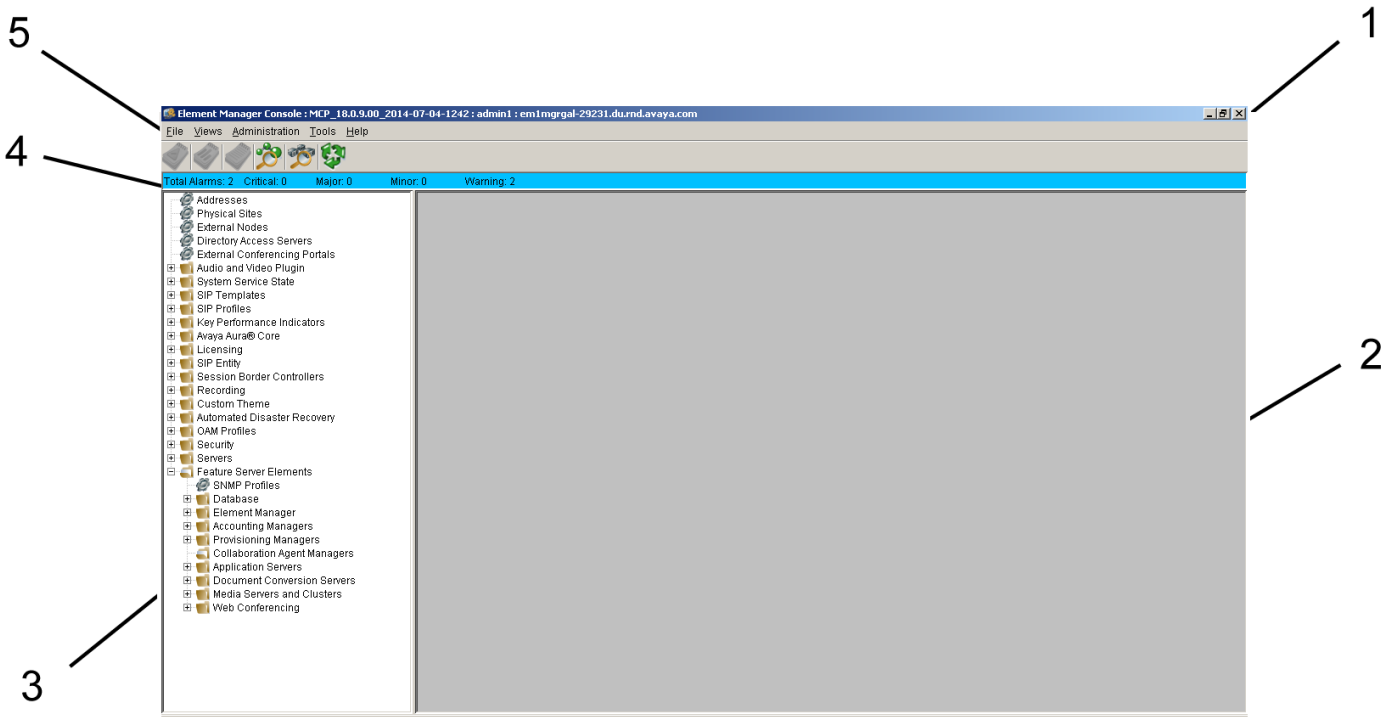
Element Manager Console includes mouse-over help and a help system.

Related Links

[Management Tools](#) on page 23
[Element Manager Console window](#) on page 40
[Tool bar](#) on page 41
[Logical and physical views of network elements](#) on page 42
[Recommended PC hardware and software requirements for running Element Manager Console](#) on page 43
[Logging on to Element Manager Console](#) on page 44
[Logging off from Element Manager Console](#) on page 48

Element Manager Console window

The following figure shows a sample Element Manager Console window.



No.	Name	Description
1	Title bar	Displays the following information: • name of the application • software version • user ID of the person logged in • IP address/name of the Avaya Aura® Conferencing Element Manager .
2	Work area	Displays the window or dialog box for the node selected in the navigation pane (3).
3	Navigation pane	Displays the nodes for the Avaya Aura® Conferencing Element Manager components.
4	Alarm Summary bar	Provides a concise, system-wide summary of alarms for managed and monitored network elements. The background color of the alarm bar indicates the most severe alarm for the system. The alarm color codes are: • Blue - warning • Green - no alarms • Yellow - minor • Orange - major • Red - critical The total number of alarms for the system, as well as the number of alarms of reach severity level appears on the alarm summary bar. The summary bar also includes a section called ACK Critical, which shows the number of previously acknowledged, but not yet cleared alarms.
5	Tool bar	Provides button shortcuts for commonly used menu commands.

Related Links

Element Manager Console overview on page 39

Tool bar

The icons on the tool bar are button shortcuts. Not all tool bar options are available for every component or server. Icons that appear disabled are unavailable for the element selected in the navigation pane.

The following figure shows the tool bar.



Button	Name
	Alarm Browser. This button displays the Alarm Browser window, which displays information about current alarms on the selected network element. The Alarm Browser button is disabled until you select a network element.
	OM Browser. This button displays the OM Browser window, which displays OM details about the selected network element. The OM Browser button is disabled until you select a network element.
	Log Browser. This button displays the Logs window, which displays the logs for the selected network element. The Log Browser button is disabled until you select a network element.
	Logical View button. This button opens the Logical View window. For more information, see Logical View window on page 42.
	Physical View button. This button opens the Physical View window. For more information, see Physical View window on page 43.
	Refresh button. This button refreshes the current view.

Related Links

Element Manager Console overview on page 39

Logical and physical views of network elements

Element Manager Console provides two graphical views to help you to quickly identify and diagnose alarm and fault conditions for all Avaya Aura® Conferencing network elements:

- the Logical View window, which organizes and displays network elements by element type.
- the Physical View window, which organizes and displays network elements by server.

You open these windows from the tool bar or the Views menu.

Related Links

Element Manager Console overview on page 39

Logical View window on page 42

Physical View window on page 43

Logical View window

The Logical View window provides a graphical view of network elements, servers, and logical databases. The network element instances are organized by type. In this view, you cannot determine which network elements are deployed on which servers.

Use this view to see the alarm conditions for all equipment for each network element type. The Alarm Browser button, Log Browser button, and OM Browser button are disabled until you select an network element instance, server, or Avaya media server.

Related Links

Logical and physical views of network elements on page 42

Physical View window

The Physical View window provides a graphical view of the system. The network elements are organized by server. Under each server, the network element applications deployed on the server are displayed.

Use this view to see alarm conditions for all monitored equipment. The Alarm Browser button, Log Browser button, and OM Browser button are disabled until you select an network element instance, server, or Avaya media server.

Related Links

Logical and physical views of network elements on page 42

Recommended PC hardware and software requirements for running Element Manager Console

Avaya recommends that the management PC (the PC that you use to run Avaya Aura® Conferencing Element Manager Console) meets the requirements described in the following table.

Category	Minimum requirement	Recommended requirement
Processor	600 MHz Pentium-class or equivalent processor	1.0 GHz (or higher) Pentium-class or equivalent processor
Available RAM	64 MB of RAM This requirement is in addition to the memory requirements of the operating system and other concurrent applications.	64 MB of RAM This requirement is in addition to the memory requirements of the operating system and other concurrent applications.
Available hard disk space	50 MB	50 MB
Mouse	Required	Required
Video graphics card	800 x 600 @16bpp [65,536 colors] VGA	1024x768 @16bpp [65,536 colors] VGA or better
Sound card	Not applicable	Not applicable
Operating system	Microsoft Windows 7, 8, or Microsoft Server 2003.	Microsoft Windows 7, 8, or Microsoft Server 2003
Network connectivity	56 Kbps modem	10Base-T or other fast network connection (such as DSL, Cable, or LAN)
Internet browser	Microsoft Internet Explorer 7.0, 8.0, 9.0, 10.0	Microsoft Internet Explorer 7.0, 8.0, 9.0, 10.0

Category	Minimum requirement	Recommended requirement
	Mozilla Firefox 10 Google Chrome 35	Mozilla Firefox 10 or later Google Chrome 35
Java	Latest Oracle JRE Version 1.7	Latest Oracle JRE Version 1.7
Cookies	Enabled	Enabled
Javascript	Enabled	Enabled

Important:

If you use a Proxy server in the Java network configuration, the Proxy server must allow access to the IP address and port. If there is no access to the IP address and port, use the Direct Connection option in the Java network configuration.

Related Links

Element Manager Console overview on page 39

Logging on to Element Manager Console

There are two ways to log on to Element Manager Console:

- single sign-on access through Avaya Aura® System Manager (This applies to Avaya Aura® deployments only.)
- locally (This applies to both Avaya Aura® and Turnkey deployments.)

Single sign-on access through Avaya Aura® System Manager

For single sign-on access through Avaya Aura® System Manager, you must use the Avaya Aura® System Manager default administrative account or an account that is configured for accessing Avaya Aura® Conferencing. For more information on creating an account that is configured for accessing Avaya Aura® Conferencing, see Checklist for creating an Avaya ®Aura Conferencing custom role on page 29. To log on to Element Manager Console using single sign-on access, you must log into the central login page for Single Sign-On for System Manager. Once you log into System Manager successfully, you can access Element Manager Console from the Conferencing Dashboard in System Manager.

When you log on to Element Manager Console using single sign-on access through Avaya Aura® System Manager, System Manager controls password administration, session time limits, and the administrative tasks you can perform in Element Manager Console.

Note:

Unless instructed by Avaya Support, you should always log on to Element Manager Console using single sign-on access through Avaya Aura® System Manager.

Local logon access

For local logon access to Element Manager Console, you must have a local logon user ID. Element Manager Console provides the following local logon user IDs:

- admin

- admin1
- admin2
- admin3
- admin4
- admin5

Local logon user IDs have “expert privileges,” which enables a local logon user to have unrestricted administrative capabilities in Element Manager Console. When you log on to Element Manager Console with a local logon user ID, Element Manager Console controls password administration and login rules. Using a local logon user ID, you can access the Administration menu in Element Manager Console, which enables you:

- change the password for the local logon user IDs
- configure the password rules for the local logon user IDs
- configure the login rules for the local logon user IDs
- view the users currently logged on to Element Manager Console
- log out (force off) a user from Element Manager Console

Note:

The Administration menu is only available when you log on to Element Manager Console locally.

Warning:

Unless instructed by Avaya Support, you should always log on to Element Manager Console using single sign-on access through Avaya Aura® System Manager.

Related Links

Element Manager Console overview on page 39
Logging on to Element Manager Console via System Manager on page 45
Logging on to Element Manager Console Locally on page 46

Logging on to Element Manager Console via System Manager

Note:

This method of logging on to Element Manager only applies to Avaya Aura® deployments.

Before you begin

You must use the Avaya Aura® System Manager default administrator account or an alternative administrative account that is configured for accessing Avaya Aura® Conferencing. For more information on creating an administrative account that is configured for accessing Avaya Aura® Conferencing, see Checklist for creating an Avaya ®Aura Conferencing custom role on page 29.

Procedure

1. On the management PC, open the browser.
2. Go to the central login page for Single Sign-On for System Manager.
3. In the User ID box on the System Manager Log On page, enter your user name.

4. In the Password box, enter your password.
5. Click **Log On**.
6. In the Elements area on the System Manager console, click **Conferencing**.
7. In the Name column on the Conferencing Dashboard, click on the name of Element Manager Console.

   A new browser window appears and displays the Element Manager Console window.
8. If you want to configure initial Differentiated Services Code Point (DSCP) values for outgoing network packets (High Throughput Data Network packets and Low Latency Data Network packets) before you log on, perform the following steps:
   a. On the Element Manager Console window, click **Advanced**.
   b. Click the right arrow button next to the tabs to scroll to the **DSCP Marking** tab.
   c. Click the **DSCP Marking** tab.
   d. On the DSCP Marking tab, configure the settings.
   e. When finished, click the **Ok** button.
9. From the IPv4 Service Address box on the Element Manager Console window, select the IP address of the server running Element Management Console.
10. Click **Connect**.
11. On the Element Manager Authentication window, click **Accept the certificate for this session only**.
12. Click **Apply**.

    The Element Manager Console window appears.

Related Links

Logging on to Element Manager Console on page 44

Logging on to Element Manager Console Locally

About this task

Use this procedure to log on to Element Manager Console using a local logon user ID (for example, admin).

If your system supports security mode, you can use secure mode to connect to the Element Manager Console.

You can configure initial Differentiated Services Code Point (DSCP) values for outgoing network packets (High Throughput Data Network packets and Low Latency Data Network packets) before you log on.

Note:

If you have an Avaya Aura® deployment, you should only perform this procedure if you are unable to log onto Element Manager Console from Avaya Aura® System Manager. See Logging on to Element Manager Console via System Manager on page 45.

Procedure

1. On the management PC, open the browser.
2. In the Address box, enter the following address:
   - For normal access: `http://<IP address>:12120`

     where <*IP address*> is the EM Internal OAM Service IP address. (This is the logical IP address of the server running Element Manager Console.)
   - For secure access: `https://<IP address>:12121`

     where <*IP address*> is the EM Internal OAM Service IP address. (This is the logical IP address of the server running Element Manager Console.)
3. Press **ENTER** on your keyboard.
4. On the <IP address> page, click **Launch Element Manager Console**.

   The Element Manager Console window appears.
5. If you want to configure initial Differentiated Services Code Point (DSCP) values for outgoing network packets (High Throughput Data Network packets and Low Latency Data Network packets) before you log on, perform the following steps:
   a. On the Element Manager Console window, click **Advanced**.
   b. Click the right arrow button next to the tabs to scroll to the **DSCP Marking** tab.
   c. Click the **DSCP Marking** tab.
   d. On the DSCP Marking tab, configure the settings.
   e. When finished, click the **Ok** button.
6. From the IPv4 Service Address box on the Element Manager Console window, select the IP address of the server running Element Manager Console.
7. Click **Connect**.
8. On the Element Manager Authentication window, click **Accept the certificate for this session only**.
9. Click **Apply**.
10. In the UserID box on the Element Manager Console window, enter the local login name.
11. In the Current Password box, enter the password for the local login name.
12. (Optional) If you must end a previous session to log on, select the **ForceOut** check box.
13. Click **Ok**.

    The Element Manager Console window appears.

Related Links

Logging on to Element Manager Console on page 44

Logging off from Element Manager Console

Procedure

From the Element Manager Console menu bar, select **File > Exit**.

Related Links

Element Manager Console overview on page 39

Provisioning Client overview

Avaya Provisioning Client is a Web-based graphical user interface that enables you to set up and manage Avaya Aura® Conferencing. Using Provisioning Client, you can:

- add, modify, and delete users
- add, modify, and delete conference users
- add and delete System Manager domains
- add, modify, and delete locations
- assign media servers to locations
- add, modify, and delete conference access numbers
- add, modify, and delete video class of service
- add, modify, and delete conference class of service
- add, modify, and delete user templates
- view the list of operators

Related Links

Management Tools on page 23
Recommended PC hardware and software requirements for running Provisioning Client on page 48
Logging on to Provisioning Client on page 49
Logging off from Provisioning Client on page 52

Recommended PC hardware and software requirements for running Provisioning Client

Avaya recommends that the management PC (the PC that you use to run Provisioning Client) meet the requirements described in the following table.

Category	Minimum requirement	Recommended requirement
Processor	200 MHz Pentium-class or equivalent processor	300 MHz (or higher) Pentium-class or equivalent processor
Available RAM	No additional free RAM required. You must meet the minimum memory requirements of your browser. See your browser documentation for more information.	
Available hard disk space	No additional hard disk space required. Your web browser performs local caching of Web pages. See your browser documentation for more information about the minimum disk space requirements.	
Mouse	Optional	Recommended
Video graphics card	800 x 600 @16bpp [65,536 colors] VGA	1024x768 @16bpp [65,536 colors] VGA or better
Sound card	Not applicable	Not applicable
Operating system	Microsoft Windows 2000, 7.0, 8.0, or Server 2003	Microsoft Windows 2000, 7.0, 8.0, or Server 2003
Network connectivity	56 Kbps modem	10Base-T or other fast network connection (such as DSL, Cable, or LAN)
Internet browser	Microsoft Internet Explorer 7.0, 8.0, 9.0 and 10.0 Mozilla Firefox 10 Google Chrome 35	Microsoft Internet Explorer 7.0, 8.0, 9.0 and 10.0 Mozilla Firefox 10 or later Google Chrome 35
Java	Not applicable	Not applicable
Cookies	Enabled	Enabled
Javascript	Enabled	Enabled

Related Links

Provisioning Client overview on page 48

Logging on to Provisioning Client

There are two ways to log on to Provisioning Client:

- single sign-on access through Avaya Aura® System Manager (This applies to Avaya Aura® deployments only.)
- locally (This applies to both Avaya Aura® and Turnkey deployments.)

Single sign-on access through Avaya Aura® System Manager

For single sign-on access through Avaya Aura® System Manager, you must have an administrative account on Avaya Aura® System Manager that is configured for accessing Avaya Aura® Conferencing. To log on to Provisioning Client using single sign-on access, you must log into the central login page for Single Sign-On for System Manager. Once you log into System Manager successfully, you can access Provisioning Client from the Conferencing Dashboard in System Manager.

When you log on to Provisioning Client using single sign-on access through Avaya Aura® System Manager, System Manager controls password administration, session time limits, and the administrative tasks you can perform in Provisioning Client.

Note:

Unless instructed by Avaya Support, you should always log on to Provisioning Client using single sign-on access through Avaya Aura® System Manager.

Local logon access

For local logon access to Provisioning Client, you must have a local logon user ID. Provisioning Client provides the following local logon user IDs:

- admin
- admin1
- admin2
- admin3
- admin4
- admin5

Local logon user IDs have “expert privileges,” which enables a local logon user to have unrestricted administrative capabilities in Provisioning Client. When you log on to Provisioning Client with a local logon user ID, Element Manager Console controls password administration and login rules.

Note:

Unless instructed by Avaya Support, you should always log on to Provisioning Client using single sign-on access through Avaya Aura® System Manager.

Related Links

Provisioning Client overview on page 48
Logging on to Provisioning Client via System Manager on page 50
Logging on to Provisioning Client locally on page 51

Logging on to Provisioning Client via System Manager

Note:

This method of logging on to Provisioning Client only applies to Avaya Aura® deployments.

Before you begin

You have an administrative account on Avaya Aura® System Manager that is configured for accessing Provisioning Client.

About this task

Use this procedure to log on to Provisioning Client using your Avaya Aura® System Manager login (single sign-on).

Procedure

1. On the management PC, open the browser.
2. Go to the central login page for Single Sign-On for System Manager.
3. In the User ID box on the System Manager Log On page, enter your user name.
4. In the Password box, enter your password.
5. Click **Log On**.
6. In the Elements area on the System Manager console, click **Conferencing**.
7. In the Name column on the Conferencing Dashboard, click on the name of Provisioning Client you want to access.

   The Welcome to the Provisioning Client page appears for the system you selected.

Related Links

Logging on to Provisioning Client on page 49

Logging on to Provisioning Client locally

About this task

Use this procedure to log on to Provisioning Client using a local administrator login.

Note:

If you have an Avaya Aura® deployment, you should only perform this procedure if you are unable to log onto Provisioning Client from Avaya Aura® System Manager.

If your system supports security mode, you can use secure mode to connect to the Provisioning Client.

Procedure

1. On your PC, open the browser.
2. In the Address box, enter the following address:
   - For normal access: `http://<IP address>:8080/prov`

     where *<IP address>* is the logical IP address of the server running Provisioning Manager.
   - For secure access: `https://<IP address>:8443/prov`

     where *<IP address>* is the logical IP address of the server running Provisioning Manager.
3. Press **ENTER** on your keyboard.
4. In the Username box on the Provisioning Client Login window, enter your user name.
5. In the Password box, enter your password.

6. Click **Login**.

   The Welcome to the Provisioning Client page appears.

Related Links

Logging on to Provisioning Client on page 49

Logging off from Provisioning Client

Procedure

Click **Logout**.

Related Links

Provisioning Client overview on page 48

Chapter 3: Managing Users and Templates

This chapter describes how to

- add and manage Avaya Aura® Conferencing users
- add and manage user templates
- view the list of Avaya Aura® Conferencing users who are administered as operators

.

Related Links

Managing Users on page 53
Managing User Templates on page 74
Viewing the list of operators on page 77

Managing Users

This section describes how to manage Avaya Aura® Conferencing users. Use the procedures in this section to

- search for a user
- add users to Avaya Aura® Conferencing from Avaya Aura® System Manager (This applies to Avaya Aura® deployments only)
- add users to Avaya Aura® Conferencing from Provisioning Client
- modify multiple users at one time (that is, bulk provisioning)
- modify a user's conferencing settings

.

Related Links

Managing Users and Templates on page 53
Searching for a user on page 54
Adding a user from System Manager on page 55
Adding a user from Provisioning Client on page 63
Modifying a user on page 68
Modifying multiple users at one time on page 69
Modifying a user's conferencing settings on page 71

Deleting a user on page 73

Searching for a user

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to find a specific user.

Procedure

1. In the Provisioning Client window, select **User Management > Search Users**.
2. From the Search by box, select the user criterion you want to search.
3. In the Search for box, enter the appropriate search information for the user. You can use a wildcard character (*) in your search information.
4. Click **Search**.

   The users that match your search criteria are displayed.

Related Links

Managing Users on page 53
Advanced Search tab field descriptions on page 54

Advanced Search tab field descriptions

Name	Description
Search by	Specifies the user data field you want to search. Your choices are: • **Login Name**: This is the user's login name from System Manager. (in an Avaya Aura® deployment) • **Communication Profile**: This is the user's communication profile from System Manager. (in an Avaya Aura® deployment) • **Last Name** • **First Name** • **Phone Number**: This field includes the telephone numbers from the **Associated Phone Numbers** tab and the business, home, and cell phone numbers from the **Base data** tab. • **Status** • **Location**

Name	Description
	• **Moderator Collaboration Code** • **Participant Collaboration Code** • **Presenter Collaboration Code** • **Enterprise Identity**
Search for	Specifies the information you want to find.
Status	This field appears if you selected **Status** from the Search by box. Your choices are: • **ACTIVE** • **INACTIVE**
Add button	Adds more search criteria.
Remove button	Removes last criterion.
Clear button	Clears all criteria.

Name	Description
Login Name column	Displays the login names of all the users that match the search criteria you specified. Clicking on the login name of a user displays the data for that user.
Communication Profile column	Displays the communication profile from System Manager for the associated user.
Last Name column	Displays the last name of the associated user.
First Name column	Displays the first name of the associated user.
Participant Collaboration Code column	Displays the participant collaboration code for the associated user.
Moderator Collaboration Code column	Displays the moderator collaboration code for the associated user.
Presenter Collaboration Code column	Displays the presenter collaboration code for the associated user.

Related Links

Searching for a user on page 54

Adding a user from System Manager

You can only use System Manager to add a user if you have an Avaya Aura® deployment. This procedure does not apply to Turnkey deployments.

To use Avaya Aura® Conferencing, a System Manager user must be assigned the Conferencing Profile. The Conferencing Profile specifies conferencing parameters, such as participant and

moderator collaboration codes and pass codes, location, and conferencing user data template, for a user.

To add a user from System Manager, perform one of the following steps:

- If you want to assign the Conferencing Profile to an existing System Manager user, see Assigning the conferencing profile to existing System Manager users on page 56.
- If you want to assign the Conferencing Profile to a group of existing System Manager users, see Assigning the conferencing profile to a group of System Manager users on page 58.
- If you want to add a new System Manager user and assign the Conferencing Profile to that user, see Assigning the conferencing profile to new System Manager users on page 60.

Related Links

Managing Users on page 53
Assigning the conferencing profile to existing System Manager users on page 56
Assigning the conferencing profile to a group of System Manager users on page 58
Assigning the conferencing profile to new System Manager users on page 60

Assigning the conferencing profile to existing System Manager users

This procedure only applies to Avaya Aura® deployments. This procedure does not apply to Turnkey deployments.

To use Avaya Aura® Conferencing, a System Manager user must be assigned the conferencing profile. The conferencing profile specifies conferencing parameters, such as participant and moderator collaboration codes and pass codes, location, and conferencing user data template for a user. After you assign the conferencing profile to the System Manager user, the user is added into the Avaya Aura® Conferencing database and is available for editing in Provisioning Client.

Avaya Aura® Conferencing SIP users using SIP services require a Session Manager profile to be assigned.

Before you begin

- Ascertain if the user you are modifying is using a SIP endpoint or a non-SIP endpoint as this determines how to configure the Communication Profile.
- Ensure a Communication Profile has already been configured in System Manager for the existing user.

About this task

Use the following procedure to assign the conferencing profile to an existing System Manager user.

Note:

If you are using the LDAP directory integration feature, do not perform this feature. See *Managing LDAP directory integration*.

Procedure

1. On the System Manager console, click **Users** > **User Management**.
2. In the navigation pane, click **Manage Users**.
3. Select the check box for the user you want to assign the conferencing profile, and click **Edit**.

4. On the **Communication Profile** tab, select the **Conferencing Profile** check box.

   The Conferencing Profile section expands.

5. Complete the following fields:

   - **Select Auto-generated Code Length**: Modify the PIN length from 6 to 8 characters, default is 6.
   - **Auto Generate Participant Collaboration Code**: Select this check box if you want the system to automatically generate the collaboration codes for the participant.
   - **Participant Collaboration Code**: If you want to assign a specific participant collaboration code for this user, make sure the **Auto Generate Participant Collaboration Code** check box is not selected, and type the conference participant collaboration code for this user in the **Participant Collaboration Code** box.
   - **Auto Generate Moderator Collaboration Code**: Select this check box if you want the system to automatically generate the collaboration codes for the moderator.
   - **Auto Generate Participant Pass Code**: Select this check box if you want the system to automatically generate the pass codes for the participant.

     Note:

     Pass codes are like a second level of security. Participants must enter pass codes after they enter the collaboration code, in order to access the conference. Moderators must send the code to the participants.

   - **Auto Generate Moderator Pass Code**: Select this check box if you want the system to automatically generate the pass codes for the moderator.
   - **Location**: Select a location from the list. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users.

     Note:

     For SIP users, the location value is obtained from the Home Location field in the Session Manager profile (if an appropriate value was not selected in the Location field in the Conferencing Profile).

   - **Template**: Select the Avaya Aura® Conferencing template you want to assign to this user. The settings for the selected template display. If you are running System Manager 6.3.3 or earlier, you can click the Get Templates button. This button is no longer displayed on System Manager 6.3.4 and later.

6. Click **Commit & Continue**.
7. Repeat Steps 1 on page 56 through 6 on page 57 to assign the conferencing profile for every existing System Manager user.

Related Links

Adding a user from System Manager on page 55

Comments? infodev@avaya.com

Assigning the conferencing profile to a group of System Manager users

This procedure only applies to Avaya Aura® deployments. This procedure does not apply to Turnkey deployments.

To use Avaya Aura® Conferencing, a System Manager user must be assigned the conferencing profile. The conferencing profile specifies conferencing parameter such as moderator and participant collaboration codes and pass codes, location, and conferencing user data template for a user.

Avaya Aura® Conferencing SIP users using SIP services require a Session Manager profile to be assigned.

About this task

Use the following procedure to assign the conferencing profile to a group of System Manager users.

Note:

Avaya recommends using this procedure when assigning conferencing profiles to a large group of System Manager users.

Note:

If you are using the LDAP directory integration feature, do not perform this feature. See *Deploying Avaya Aura® Conferencing* at the Avaya Support website: http://support.avaya.com.

Procedure

1. On the System Manager console, click **Users** > **User Management**.
2. In the navigation pane, click **Manage Users** and ensure there is at least one user on this page.
3. In the **Communication Address** section, verify that at least one communication address is assigned.
4. In the **Session Manager Profile** section, verify that at least one Session Manager profile is assigned.
5. Log on to the System Manager as admin through ssh.
6. Run the following commands:
   - For System Manager 6.3:

     ```
     cd $MGMT_HOME/bulkadministration/exportutility
     ```

     and

     ```
     bash exportUpmUsers.sh
     ```
   - For System Manager 6.2:

     ```
     cd $MGMT_HOME/upm/bulkexport/exportutility
     ```

     and

```
bash exportUpmUsers.sh
```

Job:<filename> is created.

7. Copy the <filename>.zip, as shown in the previous step to your PC.
   - For System Manager 6.3, <filename>.zip is located in `$MGMT_HOME/bulkadministration/export`.
   - For System Manager 6.2, <filename>.zip is located in `$MGMT_HOME/upm/bulkexport`.
8. View `$AVAYA_LOG/mgmt/um_bulkexport/bulkexportTraceLog.log` file to check for error messages.
9. Extract the xml file(s) from <filename>.zip on your PC.
10. In the xml file(s), remove all users who are not affected.
11. In the xml file(s), locate the following information:

```
<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">
```

12. In the xml file(s), replace the information specified in Step 11 with the following information:

```
<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 ">
```

13. In the xml file(s), perform the following steps:
    a. Replace all instances of `<tns:user>` with `<tns:userDelta>`.
    b. Replace all instances of `</tns:user>` with `</tns:userDelta>`.
    c. Replace all instances of `<tns:users>` with `<tns:deltaUserList>`.
    d. Replace all instances of `</tns:users>` with `</tns:deltaUserList>`.
14. In the xml file(s), add the following xml segments between the lines `<commProfileList>` and `</commProfileList>` for users who have a conferencing profile:

```
<commProfile xsi:type="ns2:MmcsCommProfileType" xmlns:ns2="http://xml.avaya.com/
schema/import_mmcs">
<commProfileType>mmcsCommProfile</commProfileType>
<ns2:template>template</ns2:template>
<ns2:securityCode>123456</ns2:securityCode>
<ns2:moderatorPin>654321</ns2:moderatorPin>
<ns2:eventConfCode>222</ns2:eventConfCode>
<ns2:location>location</ns2:location>
<ns2:autoGeneratedCodeLength>6</ns2:autoGeneratedCodeLength>
</commProfile>
```

15. To create a conferencing profile from an existing template, copy the template and add the xml segments from the preceding step to the conferencing profile xml file.
16. Verify that all SIP users have values for `primarySM` and `homeLocation`.
17. Verify that all users have at least one handle in `commProfileSet > handleList`.

Comments? infodev@avaya.com

18. Complete the conferencing profile xml values:

    Where:

    - *template*: is an Avaya Aura® Conferencing user template name.
    - *securityCode*: is a Participant collaboration code. This is required if the autoGeneratedCodeLength parameter is not configured.
    - *moderatorPin*: is a Moderator collaboration code. This is required if the autoGeneratedCodeLength parameter is not configured.
    - *eventConfCode*: is a Presenter security code. This is required if the autoGeneratedCodeLength parameter is not configured.
    - *autoGeneratedCodeLength*: indicates if security codes must be auto generated and the required length for auto generated codes.
    - *location*: is an Avaya Aura® Conferencing user Location. The location is mandatory for non-SIP users without a configured Session Manager profile and optional for SIP users.

      Note:

      For SIP users, the value for the Avaya Aura® Conferencing user location is obtained from the Home Location parameter in the Session Manager profile (if the Location parameter in the Conferencing Profile is not configured).

19. Log on to System Manager as admin.
20. On the System Manager console, click **Bulk Import and Export**.
21. On the Import and export page, click **Import**.
22. On the Import page, click **User Management**.
23. On the Import - User and global settings page, click **Users**.
24. On the Import users page, click **Browse** to select the edited xml file.
25. In the General section on the Import users page, set Select import type to **Partial**.
26. Click **Import** to start the job.
27. In the **Manage job** section, click **Refresh** to view the status of your job.

    The status updates to indicate SUCCESSFUL or FAILED.

    Note:

    In case of a failure, under the **Job name** column, click the job number to see the error message.

Related Links

Adding a user from System Manager on page 55

Assigning the conferencing profile to new System Manager users

This procedure only applies to Avaya Aura® deployments. This procedure does not apply to Turnkey deployments.

To use Avaya Aura® Conferencing, a System Manager user must be assigned the conferencing profile. After you assign the conferencing profile to the System Manager user, the user is added into the Avaya Aura® Conferencing database and is available for editing in Provisioning Client.

Avaya Aura® Conferencing SIP users using SIP services require a Session Manager profile to be assigned.

The conferencing profile specifies conferencing parameters, such as participant and moderator collaboration codes and pass codes, location, and conferencing user data template for a user.

Before you begin

Ascertain if the new user you are adding is using a SIP endpoint or a non-SIP endpoint as this determines how to configure the Communication Profile.

About this task

Use the following procedure to assign the conferencing profile to a new System Manager user.

Note:

If you are using the LDAP directory integration feature, do not perform this feature. See *Deploying Avaya Aura® Conferencing* at the Avaya Support website: http://support.avaya.com.

Procedure

1. On the System Manager console, click **Users** > **User Management**.
2. In the navigation pane, click **User Management** > **Manage Users**.
3. On the User Management page, click **New**.

   The New User Profile page appears.
4. On the **Identity** tab, complete the required information, and then click **Commit & Continue**.
5. On the **Communication Profile** tab, complete the required information.
   a. **Name**: Type a name.
   b. **Default**: Select this check box.
   c. Complete the **Communication Address** section to add your E.164 or private enterprise numbering plan.
   d. Complete the **Session Manager Profile** section.
   e. Complete the following profiles as required for your users:
      - **CM Endpoint Profile**
      - **CS 1000 Endpoint Profile**
      - **Messaging Profile**
      - **CallPilot Messaging Profile**
      - **IP Office Endpoint Profile**
      - **Presence Profile**
   f. Complete the **Conferencing Profile** section, proceed to Step 6 on page 62.

6. On the **Communication Profile** tab, select the **Conferencing Profile** check box.

   The Conferencing Profile section expands.

7. Complete the following fields:

   - **Select Auto-generated Code Length**: Modify the PIN length from 6 to 8 characters, default is 6.
   - **Auto Generate Participant Collaboration Code**: Select this check box if you want the system to automatically generate the collaboration codes for the participant.
   - **Participant Collaboration Code**: If you want to assign a specific participant collaboration code for this user, make sure the **Auto Generate Participant Collaboration Code** check box is not selected, and type the conference participant collaboration code for this user in the **Participant Collaboration Code** box.
   - **Auto Generate Moderator Collaboration Code**: Select this check box if you want the system to automatically generate the collaboration codes for the moderator.
   - **Auto Generate Participant Pass Code**: Select this check box if you want the system to automatically generate the pass codes for the participant.

     Note:

     Pass codes are like a second level of security. Participants must enter pass codes after they enter the collaboration code, in order to access the conference. Moderators must send the code to the participants.

   - **Auto Generate Moderator Pass Code**: Select this check box if you want the system to automatically generate the pass codes for the moderator.
   - **Location**: Select a location from the list. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users.

     Note:

     For SIP users, the location value is obtained from the Home Location field in the Session Manager profile (if an appropriate value was not selected in the Location field in the Conferencing Profile).

   - **Template**: Select the Avaya Aura® Conferencing template you want to assign to this user. The settings for the selected template display. If you are running System Manager 6.3.3 or earlier, you can click the Get Templates button. This button is no longer displayed on System Manager 6.3.4 and later.

8. Click **Commit & Continue**.
9. Repeat Steps 1 on page 61 through 8 on page 62 for each new user you want to add to System Manager and assign the conferencing profile.

Result

Avaya Aura® Conferencing is assigned to a new System Manager user.

Related Links

Adding a user from System Manager on page 55

Adding a user from Provisioning Client

Before you begin

- You must be logged into Provisioning Client.
- Your login must have Expert mode privileges to perform this procedure.

Warning:

If you have an Avaya Aura® deployment, adding a user from Provisioning Client may cause the Provisioning Client data to become out of sync with the data in Avaya Aura® System Manager. You should only add users from the System Manager interface. This rule does not apply to a Turnkey deployment.

About this task

Use this procedure to add a user from Provisioning Client.

Procedure

1. In the Provisioning Client window, select **User Management > Add User**.
2. Complete this page. See Add User page field descriptions on page 64.
3. Click **Save**.
4. Click the **Communication Address** tab.
5. In the Communication Address box, enter the address for this user.
6. From the System Manager (or User) Domain box, select the User domain for this user.
7. Click **Add**.
8. Repeat Steps 5 through 7 to enter other communication addresses for this user (if necessary).
9. Click the **Password** tab, and complete this page. See Password tab field descriptions on page 66.
10. Click the **Aura user details** tab, and complete this page. See Aura user details tab field descriptions on page 67.
11. Click **Save**.
12. Click the **Actions** tab.
13. Click **Conferencing**.
14. Complete the Conferencing User page for this user. See Conferencing User page field descriptions on page 72.
15. Click **Save**.

Related Links

Managing Users on page 53
Add User page field descriptions on page 64

Base data tab field descriptions on page 65
Communication Address tab field descriptions on page 66
Password tab field descriptions on page 66
Associated Phone Numbers tab field descriptions on page 67
User details tab field descriptions on page 67
Actions tab field descriptions on page 67

Add User page field descriptions

Name	Description
Type	Your only option is **Conferencing**.
Login Name	This is the user's login name on System Manager in an Avaya Aura® deployment. In an Avaya Aura® Turnkey deployment, the values for **Login Name** and **Communication Profile** can be any value, as long as your entries adhere to the field alphanumeric rules. These fields perform no external validation against a PBX.
Communication Profile	This is the System Manager communication profile for this user in an Avaya Aura® deployment. In an Avaya Aura® Turnkey deployment, the values for **Login Name** and **Communication Profile** can be any value, as long as your entries adhere to the field alphanumeric rules. These fields perform no external validation against a PBX.
Password	This is the password for the user's account. This password is used for local authentication.
Confirm password	This is the password for the user's account.
User Template	This is the Provisioning Client user template that will be assigned to this account.
Status reason	Specifies the status for this account. Your choices are: • **ACTIVE** • **INACTIVE**
Location	Specifies the location for this user. This location should match an existing location in System Manager (or your PBX equivalent).
First name	You can enter alphanumeric characters.
Last name	You can enter alphanumeric characters.
Enterprise Identity	This is the identification (ID) of the user. This field is required for lightweight directory access protocol (LDAP) integration.

Name	Description
Enterprise Domain`	This is the domain of the enterprise directory. This field is required for LDAP integration.
E-mail	This is the user's email address.
Business phone	This is the user's business telephone number.
Home phone	This is the user's home telephone number.
Cell phone	This is the user's cell phone number.
Pager	This is the user's pager number.
Fax	This is the user's fax number.
Time zone	This is the time zone where the user is located.
Locale	This is the user's preferred written or spoken language.

Related Links

Adding a user from Provisioning Client on page 63

Base data tab field descriptions

Name	Description
Type	Your only option is **Conferencing**.
Login Name	This is the user's login name on System Manager in an Avaya Aura® deployment. In an Avaya Aura® Turnkey deployment, the values for **Login Name** and **Communication Profile** can be any value, as long as your entries adhere to the field alphanumeric rules. These fields perform no external validation against a PBX.
Communication Profile	This is the System Manager communication profile for this user in an Avaya Aura® deployment. In an Avaya Aura® Turnkey deployment, the values for **Login Name** and **Communication Profile** can be any value, as long as your entries adhere to the field alphanumeric rules. These fields perform no external validation against a PBX.
First name	You can enter alphanumeric characters.
Last name	You can enter alphanumeric characters.
Enterprise Identity	This is the identification (ID) of the user. This field is required for lightweight directory access protocol (LDAP) integration.
Enterprise Domain`	This is the domain of the enterprise directory. This field is required for LDAP integration.
E-mail	This is the user's email address.

Name	Description
Business phone	This is the user's business telephone number.
Home phone	This is the user's home telephone number.
Cell phone	This is the user's cell phone number.
Pager	This is the user's pager number.
Fax	This is the user's fax number.
Status reason	Specifies the status for this account. Your choices are: • **ACTIVE** • **INACTIVE**
Time zone	This is the time zone where the user is located.
Locale	This is the user's preferred written or spoken language.
Location	Specifies the location for this user. This location should match an existing location in System Manager (or your PBX equivalent).

Related Links

Adding a user from Provisioning Client on page 63

Communication Address tab field descriptions

Name	Description
Communication Address	Specifies the user's communication address. In an Avaya Aura® deployment, this address should be the same as on System Manager.
User Domain	Specifies the User domain. For a Turnkey solution, this is the SIP domain of the Avaya Aura® Conferencing server that you are using.
Communication Address column	Displays all of the user's communication addresses.
Launch Collaboration Agent column	Enables you to log into the user's Collaboration Agent account.
Delete column	Enables you to delete the associated communication address.

Related Links

Adding a user from Provisioning Client on page 63

Password tab field descriptions

Name	Description
New password	This is the password for the user's account. This password is used for local authentication.
Confirm password	This is the password for the user's account.

Related Links

Adding a user from Provisioning Client on page 63

Associated Phone Numbers tab field descriptions

Name	Description
Associated Phone Numbers column	Displays the telephone numbers that are permanently associated with the selected user. A user can have up to 10 associated telephone numbers.
Delete	Deletes the corresponding phone number that is associated with the selected user. **Note:** You can only view or delete the associated phone numbers. You cannot edit them.

Related Links

Adding a user from Provisioning Client on page 63

User details tab field descriptions

Name	Description
Login Name	This is the user's login name on System Manager in an Avaya Aura® deployment.
Localized Display Name	This is the localized name that is displayed for this user in a conference list.
Endpoint Display Name	This is the name that is displayed for this user's endpoint in a conference list.

Related Links

Adding a user from Provisioning Client on page 63

Actions tab field descriptions

Name	Description
Delete User	Deletes the selected user.
Conferencing	Displays the user's conferencing settings.
Clear Lockout	Clears the lock out condition for the user's login.

Related Links

Adding a user from Provisioning Client on page 63

Modifying a user

Before you begin

- You must be logged into Provisioning Client.
- Your login must have Expert mode privileges to perform this procedure.

Warning:

If you have an Avaya Aura® deployment, any changes you make may cause the Provisioning Client data to become out of sync with the data in Avaya Aura System Manager. You should only modify data to fix sync issues that cannot be resolved from the System Manager interface.

About this task

Use this procedure to modify an existing user.

Procedure

1. In the Provisioning Client window, select **User Management > Search Users**.
2. From the Search by box, select the user criterion you want to search.
3. In the Search for box, enter the appropriate search information for the user.
4. Click **Search**.
5. In the Login name column, click on the Login Name of the user.
6. On the Base data tab of the User page, make your changes. See Base data tab field descriptions on page 65.
7. Click the **Communication Address** tab, and make your changes. See Communication Address tab field descriptions on page 66.
8. If you want to delete the phone number that is permanently associated with this user, click the **Associated Phone Numbers** tab, and make your changes. See Associated Phone Numbers tab field descriptions on page 67.
9. Click the **Aura user details** tab, and make your changes. See Aura user details tab field descriptions on page 67.
10. Click the **Actions** tab.
11. Click **Conferencing**.
12. On the Conferencing User page, make your changes. See Conferencing User page field descriptions on page 72.
13. Click **Save**.

Related Links

Managing Users on page 53

Modifying multiple users at one time

Before you begin

- You must be logged into Provisioning Client.
- Your login must have Expert mode privileges to perform this procedure.

Warning:

If you have an Avaya Aura® deployment, any changes you make may cause the Provisioning Client data to become out of sync with the data in Avaya Aura System Manager. You should only modify data to fix sync issues that cannot be resolved from the System Manager interface.

About this task

Use this procedure to modify the conference class of service, video (enable/disable) setting, and recording (enable/disable) setting for multiple users at one time (that is, bulk provisioning). In this procedure, you will identify the list of users you want to modify by specifying search criteria.

Procedure

1. In the Provisioning Client window, select **User Management > Bulk Provisioning**.
2. From the Field box, select the user criterion you want to search.
3. From the Operation box, select the search operation you want to perform.
4. In the Value box, specify the appropriate search information for the users.
5. Click **Add Criteria**.
6. Repeat Steps 2 through 5 to specify any other search criteria.
7. When finished specifying your search criteria, click **Search**.

   The user's who match your search criteria are displayed.
8. Click the check box for each user you want to modify.
9. In the Actions area, select the check box for each setting you want to modify for all of the selected users, and then select the appropriate value. See Bulk Provisioning page field descriptions on page 69.
10. Click **Assign**.

Related Links

Managing Users on page 53
Bulk Provisioning page field descriptions on page 69

Bulk Provisioning page field descriptions

Name	Description
Field	Displays the field you want to search in the user data.

Name	Description
	Your choices are: • **Login Name** • **Communication Address Handle** • **Communication Address Domain** • **Last Name** • **First Name** • **Profile name** • **Directory Sync Status** There are three possible values for this field. - Pending (sync error or out of filter scope) - Synced from directory - Local user • **Video Enabled** • **Recording Enabled** • **Video Class**
Operation	Display the search operation you want to perform. Your choices are: • **Starts with** • **Contains** • **Equals**
Value	Displays the data you want to find in the specified user field.

Button	Description
Add Criteria	Adds the information you specified in the Field, Operation, and Value boxes into the search criteria list box.
Edit	Enables you to modify the selected search criterion .
Remove	Deletes the selected search criterion.
Remove all	Deletes all of the search criteria.
Search	Searches the user data using the displayed search criteria.
Commit	Saves the changes.

Name	Description
Directory Distinguished Name column	Displays an element which operates in conjunction with the search scope. It is the tree from which you

Name	Description
	would like to synchronize users. It is important to note that the domain part of the distinguished name is automatically based on the selected domain and cannot be changed. For example: `cn=Users,dc=example,dc=com display`.
Login name column	Displays the login name of each user.
Communication Profile	Displays the administered communications profile for each user.
Last Name	Displays the last name of each user.
First Name	Displays the first name of each user.

Name	Description
Conference Profile	Specify the conference class of service you want to assign to the selected users.
Enable Video	Specify whether video will be enabled or disabled for the selected users.
Enable Recording	Specify whether the Recording feature will be enabled or disabled for the selected users.
Delete User	Specify whether you would like to delete all selected users.

Related Links

Modifying multiple users at one time on page 69

Modifying a user's conferencing settings

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to modify the conferencing settings for a user.

Procedure

1. In the Provisioning Client window, select **User Management > Conferencing User**.
2. In the Select login name box, enter the login name for the user. Be sure to include the domain name (for example, yourname@company.com).
3. Click **>>**.
4. Make your changes. See Conferencing User page field descriptions on page 72.
5. Click **Save**.

Related Links

Managing Users on page 53
Conferencing User page field descriptions on page 72

Conferencing User page field descriptions

Name	Description
Select login name	Enables you to enter the login name of the conferencing user in which you are interested. You must include the domain with the user's login name (for example, jsmith@yourcompany.com).
Select comm profile	Enables you to select the communications profile for the user.
Class of service	Displays the conference class of service assigned to this user.
Enable Video	Specifies whether video is enabled for this user.
Enable Recording	Specifies whether conference recording is enabled for this user.
Enable operator control	Specifies whether this user has operator control privileges. **Note:** This setting is not available for an Event conference class of service.
Priority	Specifies the quality of service this user will receive. The higher the priority setting, the better the service. Your choices are: • **Business Critical**: The resolution, frame rate, or quality of sessions will not be reduced during high-usage network conditions. Sessions will proceed with the requested bandwidth at setup. • **High**: The resolution, frame rate, or quality of sessions may be reduced during high-usage network conditions or to accommodate Business Critical users. • **Medium**: The resolution, frame rate, or quality of sessions may be reduced during high-usage network conditions or to accommodate Business Critical and High priority users. Session reduction will occur for Medium priority users before High priority users. Also, session reduction will be greater for Medium priority users than High priority users.

Name	Description
	• **Low**: Sessions may lose video and fall back to audio-only during high-usage network conditions or to accommodate higher priority users.
Presenter Collaboration code	Specifies the code that a user must enter to become a presenter during the Event conference. **Note:** This setting is available for an Event conference class of service. This code is set by the Event conference host.
Participant Collaboration Code	Specifies the participant code that users must enter to log into this user's conference bridge. This value may consist of one to 20 numeric characters
Moderator Collaboration Code	Specifies the code that this user must enter to log into the conference bridge as a moderator. This value may consist of one to 20 numeric characters
Participant Pass code	Specifies the code that users must enter if a participant pass code is required for the conference bridge. This value may consist of one to 20 numeric characters
Moderator Pass code	Specifies the code that this user must enter if a moderator pass code is required for the conference bridge. This value may consist of one to 20 numeric characters

Related Links

Modifying a user's conferencing settings on page 71

Deleting a user

Before you begin

- You must be logged into Provisioning Client.
- Your login must have Expert mode privileges to perform this procedure.

Warning:

If you have an Avaya Aura® deployment, any changes you make may cause the Provisioning Client data to become out of sync with the data in Avaya Aura System Manager. You should only modify data to fix sync issues that cannot be resolved from the System Manager interface.

About this task

Use this procedure to delete a user's Avaya Aura® Conferencing account.

Procedure

1. In the Provisioning Client window, select **User Management > Search Users**.
2. From the Search by box, select the user criterion you want to search.
3. In the Search for box, enter the appropriate search information for the user.
4. Click **Search**.
5. In the Login name column, click on the Login Name of the user.
6. Click the **Actions** tab.
7. Click **Delete User**.
8. In the Confirmation window, enter your password, and click **Confirm**.

Related Links

Managing Users on page 53

Managing User Templates

This section describes how to add, modify, and delete templates for Avaya Aura® Conferencing users. A user template specifies the following settings for a user:

- the conference class of service
- whether video is enabled
- the quality of service the user will receive (that is, the priority)

If you have an Avaya Aura® deployment, you can apply a user template when you add an Avaya Aura® Conferencing user in Avaya Aura® System Manager or Provisioning Client. Avaya Aura® Conferencing provides a set of default templates that you can apply to users. You can “copy” the default templates to create custom templates that are based on the default templates.

Related Links

Managing Users and Templates on page 53
Adding a user template on page 75
Modifying a user template on page 76
Deleting a user template on page 77

Adding a user template

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to create a user template. You apply a user template when you add a conferencing user in Avaya Aura® System Manager (in an Avaya Aura® deployment) or Provisioning Client.

Procedure

1. In the Provisioning Client window, select **User Management > User Template**.
2. If you want to add a user template that is based on an existing user template, click **Copy** for the existing template you want to use.
3. In the Name box, enter the name for the video class you want to add.
4. Complete the fields as appropriate. See User Template page field descriptions on page 75.
5. Click **Save**.

Related Links

Managing User Templates on page 74
User Template page field descriptions on page 75

User Template page field descriptions

Name	Description
Name	Displays the name of the user template.
Conference class of service	Displays the conference class of service assigned to the user template.
Enable Video	Specifies whether video is enabled for the user.
Enable Recording	Specifies whether the Recording feature is enabled for the user.
Priority	Specifies the quality of service the user will receive. The higher the priority setting, the better the service. Your choices are: • **Business Critical**: The resolution, frame rate, or quality of sessions will not be reduced during high-usage network conditions. Sessions will proceed with the requested bandwidth at setup. • **High**: The resolution, frame rate, or quality of sessions may be reduced during high-usage network conditions or to accommodate Business Critical users.

Name	Description
	• **Medium**: The resolution, frame rate, or quality of sessions may be reduced during high-usage network conditions or to accommodate Business Critical and High priority users. Session reduction will occur for Medium priority users before High priority users. Also, session reduction will be greater for Medium priority users than High priority users. • **Low**: Sessions may lose video and fall back to audio-only during high-usage network conditions or to accommodate higher priority users.

Name	Description
Template Name column	Displays the user templates. Clicking on the name of a user template displays the associated settings.
Conference Class of Service column	Displays conference class of service that is assigned to the associated template.
Enable Video column	Displays whether video is enabled for the associated template.
Enable Recording column	Displays whether the Recording feature is enabled for the associated template.
Priority column	Displays the priority assigned to the associated template.
Copy column	Enables you to create a new user template that is based on the associated user template.
Delete column	Enables you to delete the associated user template. **Note:** You cannot delete a default user template.

Related Links

Adding a user template on page 75

Modifying a user template

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to modify an existing user template.

Note:

Any changes you make to an existing template are not applied to the users to which the template has already been assigned.

You cannot change the settings for a default user template.

Procedure

1. In the Provisioning Client window, select **User Management > User Template**.
2. Click the name of the user template you want to modify.
3. Make your changes. See User Template page field descriptions on page 75.
4. Click **Save**.

Related Links

Managing User Templates on page 74

Deleting a user template

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to delete a user template.

Note:

You cannot delete a default template.

Procedure

1. In the Provisioning Client window, select **User Management > User Template**.
2. Click **Delete** for the user template you want to delete.
3. In the Confirmation window, enter your password, and click **Confirm**.

Related Links

Managing User Templates on page 74

Viewing the list of operators

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to view the list users that are administered as operators. For these users, the **Enable operator control** check box is enabled in each user's conferencing settings. See Modifying a users conferencing settings on page 71.

Procedure

In the Provisioning Client window, select **Operator Management > Operators**.

Related Links

Managing Users and Templates on page 53
Operators page field descriptions on page 78

Operators page field descriptions

Name	Description
Login Name column	Displays the login names of all the users that have the Enable operator control check box enabled in the user's conferencing settings.
Communication Profile column	Displays the communication profile from System Manager for the associated user.
Last Name	Displays the last name of each user.
First Name	Displays the first name of each user.

Related Links

Viewing the list of operators on page 77

Chapter 4: Managing Loads and Patches

About loads and patches

Using Element Manager Console, you can

- view the information for a load or patch of Avaya Aura® Conferencing
- install a patch
- upgrade a network element instance

For detailed instructions on how to upgrade and patch Avaya Aura® Conferencing software, see "Upgrading and patching software" in *Deploying Avaya Aura® Conferencing 8.0*.

Viewing the information for a load or patch

About this task

Use this procedure to view the information for a load or patch.

Procedure

1. From the Tools menu in Element Manager Console, select **Patch/MR Manager**.
2. From the Load or Patch box in the Patch/MR Manager window, select the load or patch in which you are interested.
3. Click **Info**.

   The Load Information window displays information about the selected load or patch.
4. When finished, click **Ok**.

Installing a patch

About this task

Use this procedure to install a patch.

Procedure

1. From the Tools in Element Manager Console, select **Patch/MR Manager**.
2. From the Load or Patch box in the Patch/MR Manager window, select the patch you want to install.
3. Select the network element instance you want to patch.
4. Click **Patch**.
5. In the Confirmation dialog box, click **Yes**.

Upgrading a network element instance

About this task

Use this procedure to upgrade a network element instance.

Procedure

1. From the Tools menu in Element Manager Console, select **Patch/MR Manager**.
2. From the Load or Patch box in the Patch/MR Manager window, select the load or patch you want to install.
3. Select the network element instance that you want to upgrade.
4. Click **Upgrade**.
5. In the Confirmation dialog box, click **Yes**.

Viewing the version information for the Avaya Aura® Conferencing software installed on the server

Before you begin

You must be able to log into the server as the ntsysadm user or the ntappadm user.

About this task

Use this procedure to view the version information for the Avaya Aura® Conferencing software and Avaya Media Server software installed.

Procedure

1. Log into the server as the *ntsysadm* user or the *ntappadm* user.
2. Enter the command **`swversion`** and press ENTER.
3. If prompted, enter your password.

Chapter 5: Customizing Collaboration Agent

This chapter describes the procedures to customize Collaboration Agent. Avaya Aura® Conferencing provides a sample theme that you can download and customize for the pages in Collaboration Agent. This sample theme provides the following settings:

- the Avaya logo displayed on the Login page, Check-in page, and Pop-up blocker page
- a grayscale background for the Login page, Check-in page, and Collaboration Agent application window
- a grayscale background for the web collaboration area in the Collaboration Agent application window
- grayscale text on the Login page, Check-in page, and Collaboration Agent application window
- a grayscale background for buttons on the Login page and Check-in page
- a blue background for a button when you place the mouse over the button on the Check-in page
- grayscale text for the button labels on the Check-in page

You can create a custom theme and modify the default settings for the pages in Collaboration Agent. The following figures identify the components you can change on each page in Collaboration Agent.

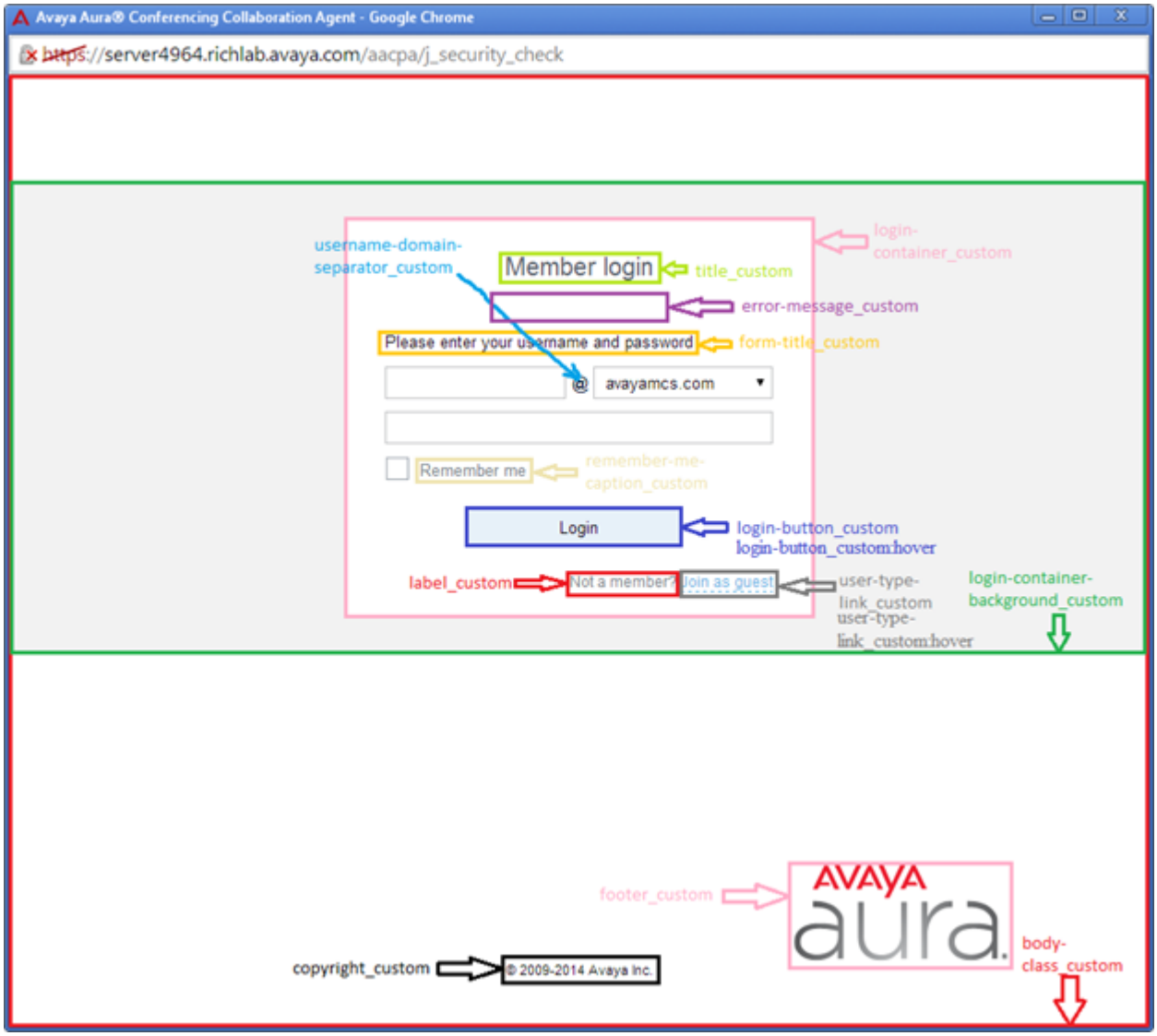


Figure 3: Components you can customize on the Collaboration Agent Login page

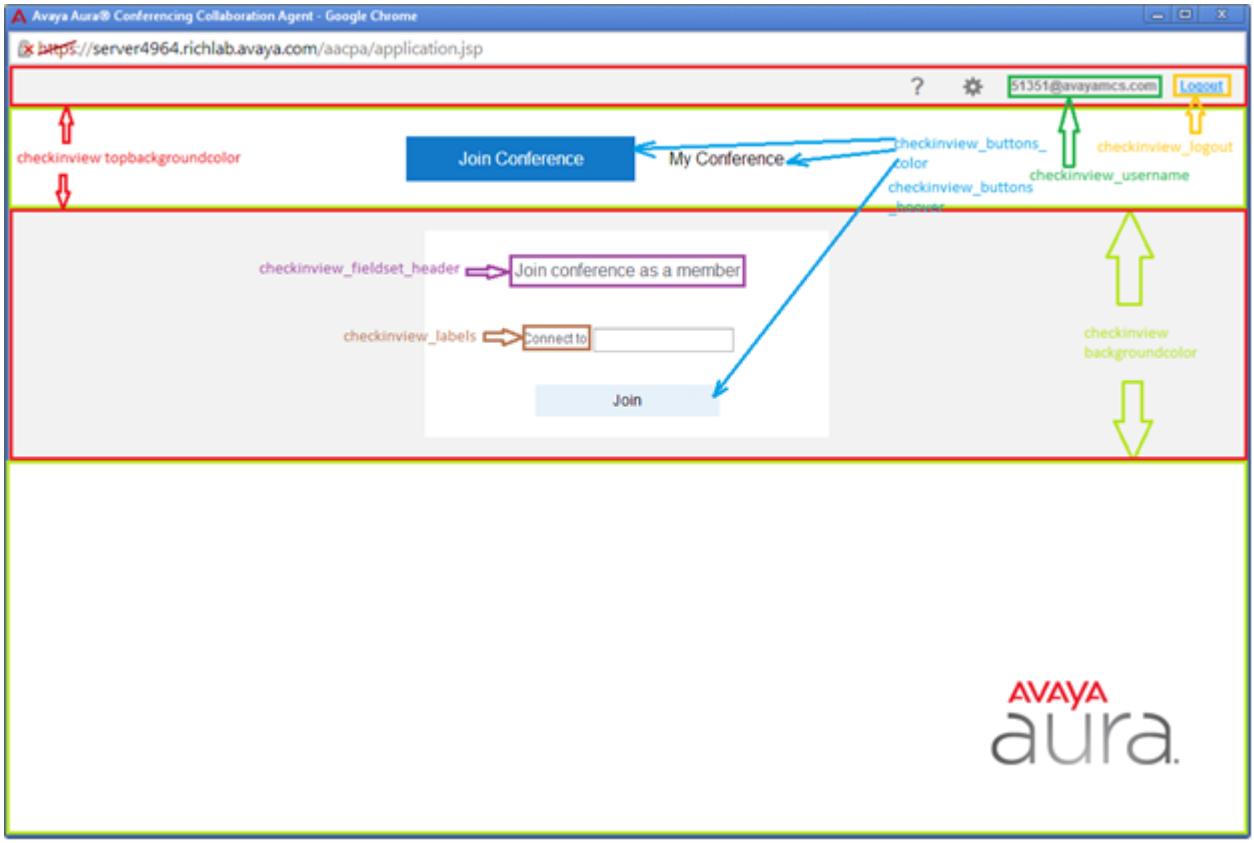


Figure 4: Components you can customize on the Collaboration Agent Check-in page

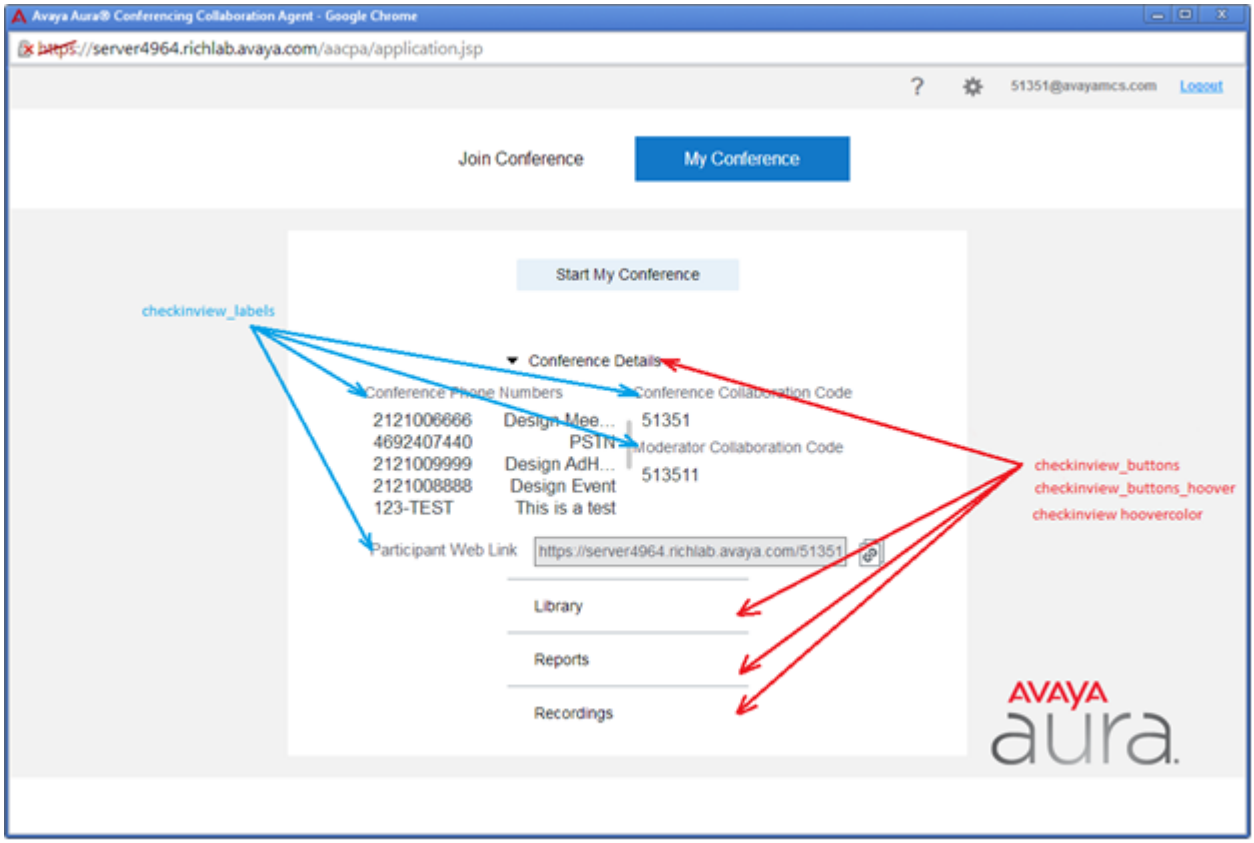


Figure 5: Components you can customize on the Collaboration Agent Check-in page 2

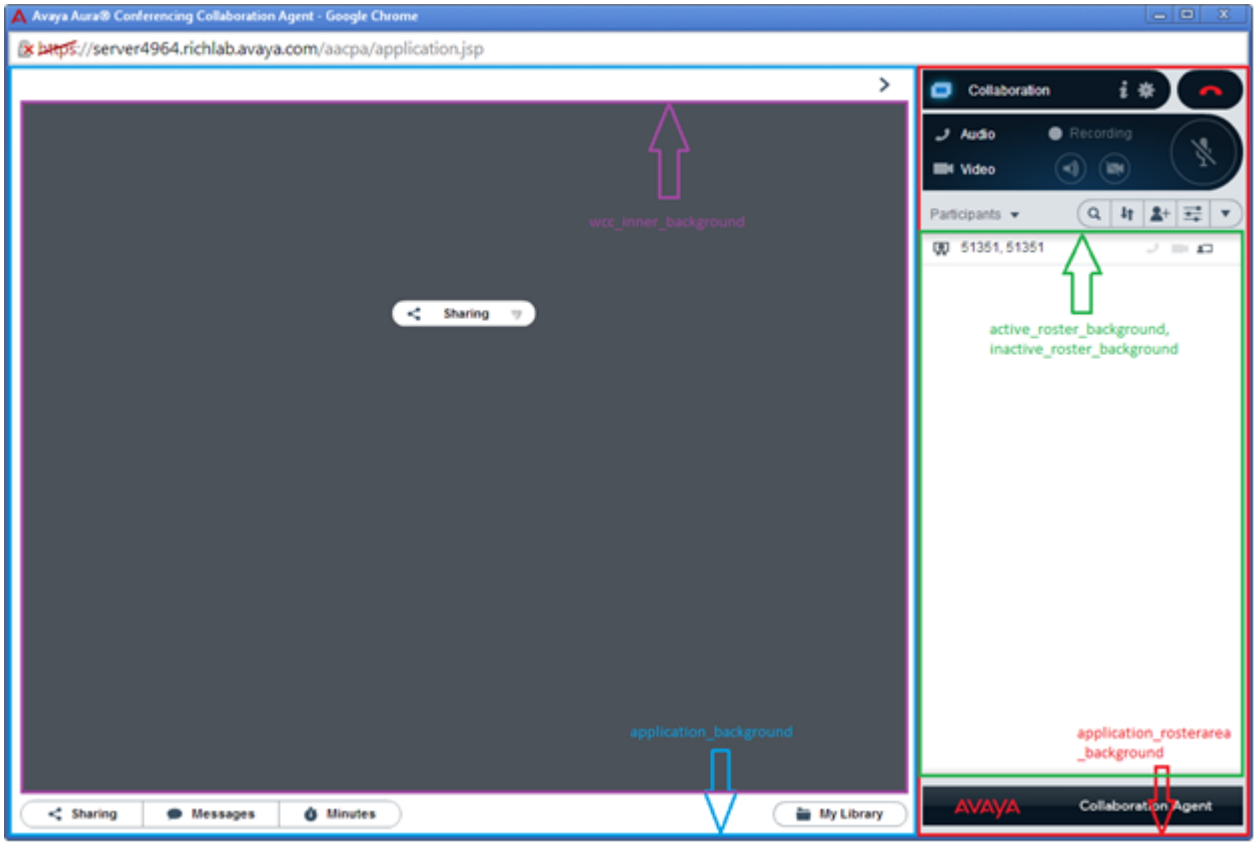


Figure 6: Components you can customize in the Collaboration Agent application window

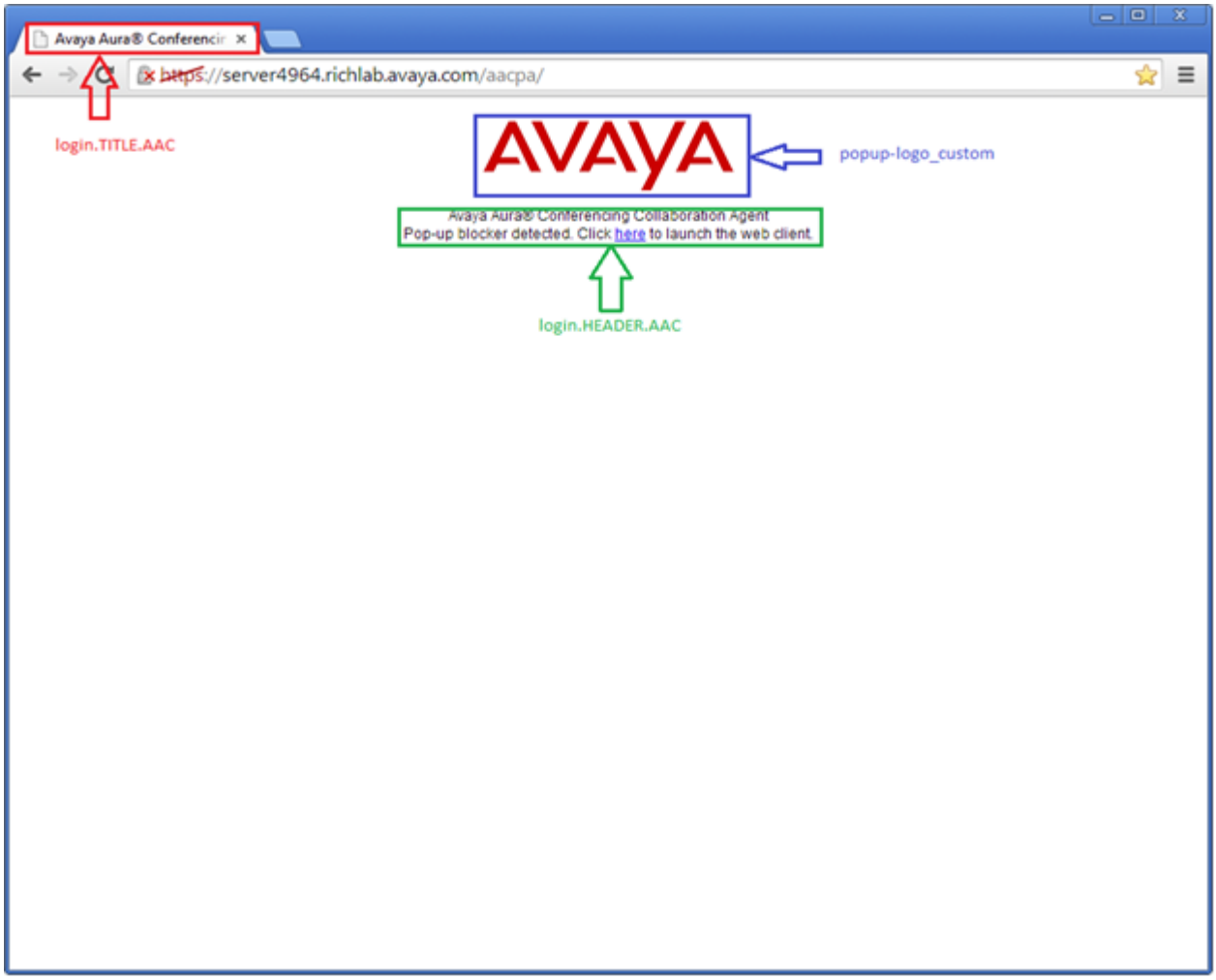


Figure 7: Components you can customize on the Collaboration Agent Pop-up Blocker page

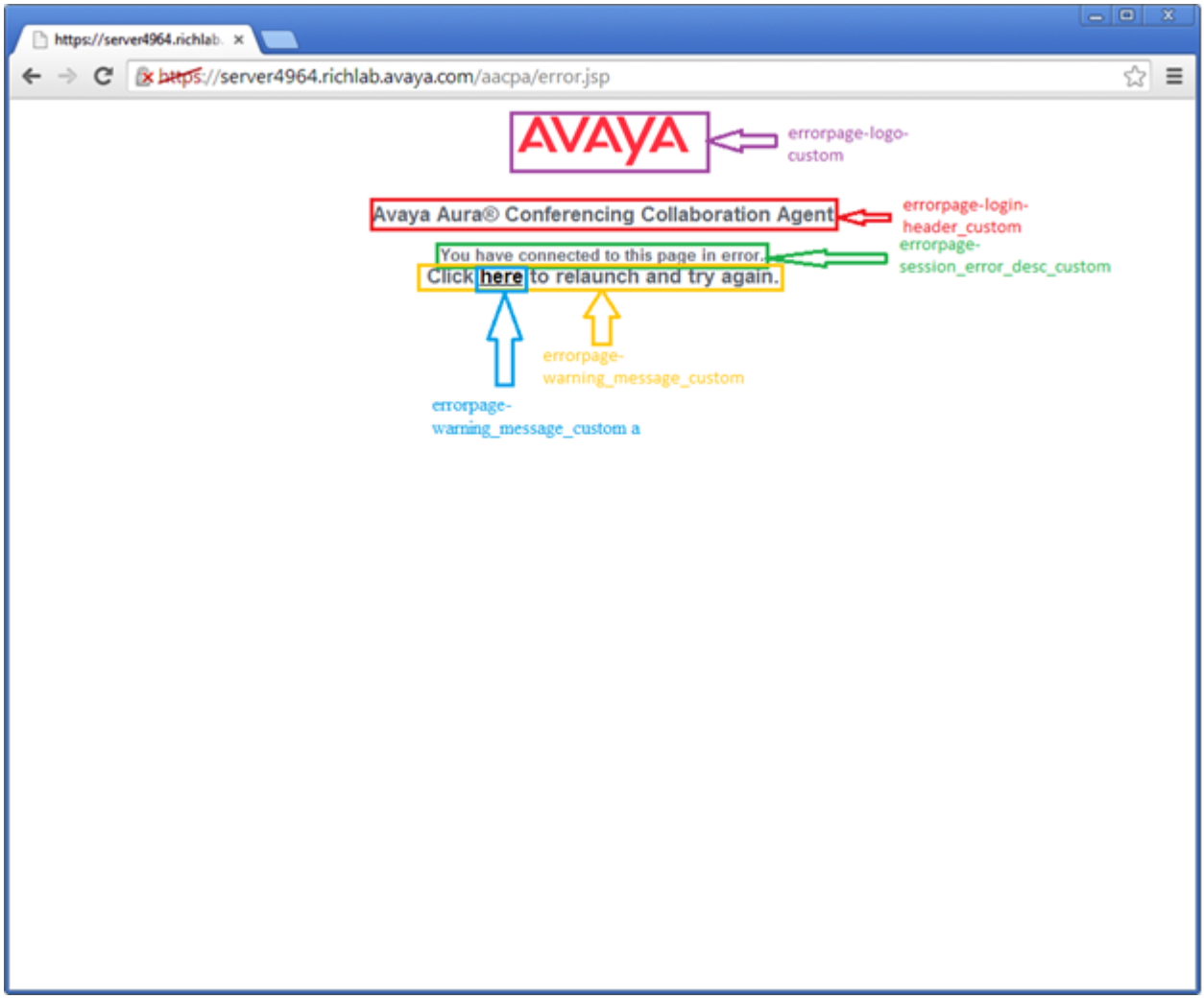


Figure 8: Components you can customize on the Collaboration Agent error page

Related Links

[Creating a custom theme for Collaboration Agent](#) on page 87
[Modifying a custom theme for Collaboration Agent](#) on page 94
[Applying a custom theme for Collaboration Agent](#) on page 94
[Replacing the custom theme for Collaboration Agent](#) on page 95
[Removing the custom theme for Collaboration Agent](#) on page 96
[Downloading the custom theme for Collaboration Agent](#) on page 97
[Forcing an update to the custom theme for Collaboration Agent](#) on page 98
[Retaining/restoring logo customizations during an upgrade](#) on page 99

Creating a custom theme for Collaboration Agent

About this task

Use this procedure to create a custom theme for Collaboration Agent. To create a custom theme, you must first download the sample theme via Element Manager Console. You will then modify the sample theme files that you downloaded to meet your needs. After you customize the appropriate files, you will upload your custom theme to Avaya Aura® Conferencing via Element Manager Console.

Note:

You can create multiple custom themes and save them on your PC. However, you can only upload one custom theme to Avaya Aura® Conferencing.

Procedure

1. Download the sample theme for Collaboration Agent from Avaya Aura® Conferencing and then extract that zipped file to a directory on your PC. See Downloading the sample theme on page 88.
2. Customize the theme colors for Collaboration Agent. See Modifying the theme colors for Collaboration Agent on page 89.
3. Customize the logos displayed in Collaboration Agent. See Modifying the logos for Collaboration Agent on page 91.
4. Customize the title and header displayed in Collaboration Agent. See Modifying the title and header for Collaboration Agent on page 92.
5. Create a zip file that contains the components of the custom theme in the appropriate structure. See Preparing the custom theme for upload on page 93.
6. Upload the custom theme zip file to Avaya Aura® Conferencing. See Applying a custom theme for Collaboration Agent on page 94.

Related Links

Customizing Collaboration Agent on page 81
Downloading the sample theme on page 88
Modifying the theme colors for Collaboration Agent on page 89
Modifying the logos for Collaboration Agent on page 91
Modifying the title and header for Collaboration Agent on page 92
Preparing the custom theme for upload on page 93

Downloading the sample theme

Before you begin

You can log into the server as `ntappadm`.

About this task

Use this procedure to download the sample theme for Collaboration Agent and extract the sample theme to a temporary directory.

Procedure

1. In the navigation pane of Element Manager Console, select **Custom Theme > Custom Theme**.
2. In the Custom Theme window, click **Add (+)**.
3. In the Add Custom Theme dialog box, click **Download** for Download Sample Theme.
4. In the FTP Login dialog box, enter `ntappadm` in the User box.
5. In the Password box, enter the password for ntappadm .
6. Click **Apply**.
7. In the Save dialog box, select the location where you want to save the sample theme zipped file. By default, the file is named theme.zip.
8. Click **Save**.

   The following message appears at the top of the Add Custom Theme dialog box: `Operation in progress. Please wait....`
9. After the sample theme zipped file is downloaded to your PC, click **OK** in the Download Complete message box.
10. Click **Apply**.
11. Extract the sample theme zipped file to a temporary directory.

Related Links

Creating a custom theme for Collaboration Agent on page 87

Modifying the theme colors for Collaboration Agent

Before you begin

Make sure you have downloaded and extracted the theme.

About this task

Use this procedure to modify the theme colors for Collaboration Agent.

To set the color for a page component in Collaboration Agent, you must specify the hexidecimal value for the color you want to use. For example, if you want to use bright red, you would enter `#FF0000`. If you wanted to use white, you would enter `#FFFFFF`. You can find the hexidecimal value for any color at http://www.colorschemer.com/online.html.

Procedure

1. Access the directory to which you extracted the theme.
2. Open the **css** directory.
3. Using a text editor such as Notepad, open the file `theme.css`.

The file `theme.css` enables you to specify the color for components on the Collaboration Agent Login page.

4. To change the color for a component, perform the following steps:
   a. Go to the section that contains the setting you want to modify. For example, if you want to change the background color of the Login page, you would go to the section `/** Collaboration Agent background color */`, which contains the component `body-class_custom`.
   b. Set `background-color:` to the hexadecimal number of the color you want to use.
5. Repeat Step 4 for each setting you want to modify. Refer to Components you can customize on the Log-in page on page 82 to determine what each setting controls.

   Note:

   The property `.errorpage-warning_message_custom a` is missing in the sample theme. If you would like to customize this property, you should replace `.errorpage-warning_message_custom {...}` with `.errorpage-warning_message_custom,.errorpage-warning_message_custom a{…}` in theme.css.
6. When finished, save your changes and exit the file.
7. Using a text editor such as Notepad, open the file `cawcctheme.css` in the **css** directory.

   The file `cawcctheme.css` enables you to specify:

   - the color for components on the Collaboration Agent Check-in page. See Components you can customize on the Check-in page on page 83.
   - the background color for the Collaboration Agent application window (`application_background`). See Components you can customize on the application window on page 85.
   - the background color for the web collaboration area in the Collaboration Agent application window (`wcc_inner_background`). See Components you can customize on the application window on page 85.
8. To change the color for a component, perform the following steps:
   a. Go to the section that contains the setting you want to modify. For example, if you want to change the background color of the Collaboration Agent application window, you would go to the section `/**Collaboration Agent application background color */`, which contains the component `application_background`.
   b. Set `color:` to the hexadecimal number of the color you want to use.
9. Repeat Step 8 for each setting you want to modify. Refer to Components you can customize on the Check-in page on page 83 and Components you can customize on the application window on page 85 to determine what each setting controls.
10. When finished, save your changes and exit the file.

Related Links

Creating a custom theme for Collaboration Agent on page 87

Modifying the logos for Collaboration Agent

Before you begin

Make sure you have downloaded and extracted the theme to a directory.

About this task

Use this procedure to specify the images you want to use as the logos in Collaboration Agent. You can set the logo that will be displayed on the following Collaboration Agent pages:

- Login page. See Components you can customize on the Log-in page on page 82.
- Check-in page. See Components you can customize on the Check-in page on page 83.
- Pop-up blocker page. See Components you can customize on the pop-up blocker window on page 86.
- Error page. See Components you can customize on the error page on page 87.

Note:

- The logo files you want to use must be in the PNG format.
- The logo file you want displayed on the Login page must have the file name `logo.png`. Avaya recommends that the image dimensions be 139 x 40 px.
- The logo file you want displayed on the Pop-up blocker page must have the file name `logo_white.png`. Avaya recommends that the image dimensions be 200 x 57 px.
- The logo file you want displayed on the Error page must have the file name `error-page-logo.png`. Avaya recommends that the image dimensions be 139 x 40 px. By default, Collaboration Agent uses the file `logo.png` for the logo on the Error page. If you want to use a different logo for the Error page, you must use the file name `error-page-logo.png`.
- You can also use custom image names. If you would like to use custom image names, you should change the names in appropriate css files as shown in the following example. Do not forget to use images with recommended dimensions. Avaya recommends using the height property to display images correctly.

Procedure

1. Rename the file you want to use as the logo in the Pop-up blocker page to `logo_white.png`.

   Note:

   The file you want to use as the logo on the Pop-up blocker page must have the file name `logo_white.png`.

2. Access the directory to which you extracted the theme.
3. Open the **img** directory.
4. Replace the existing file `logo_white.png` with the new file `logo_white.png`.

5. Rename the file you want to use as the logo on the Login page to `logo.png`.

   Note:

   - The file you want to use as the logo on the Login page must have the file name `logo.png`.
   - By default, Collaboration Agent will also use this file as the logo on the Error page.

6. In the **img** directory, replace the existing file `logo.png` with the new file `logo.png`.
7. If you want to use a different logo for the Error page:
   a. Rename the file you want to use as the logo for the Error page to `error-page-logo.png`.
   b. Save the file `error-page-logo.png` to the **img** directory.
   c. Access the **css** directory. The **css** directory appears in the directory to which you extracted the theme.
   d. Using a text editor such as Notepad, open the file `theme.css`.
   e. Go to the section `/** Logo on error page*/`
   f. Set `background-image:` to `url(../img/error-page-logo.png).`
   g. Save your changes and exit the file.

Related Links

Creating a custom theme for Collaboration Agent on page 87

Modifying the title and header for Collaboration Agent

Before you begin

Make sure you have downloaded and extracted the theme.

About this task

Use this procedure to modify the title and header for Collaboration Agent.

Procedure

1. Access the directory to which you extracted the theme.
2. Open the **props** directory.

   The **props** directory contains a number of `.properties` files. The name of each properties file is associated with the locale to which the file will be applied.

3. Using a text editor such as Notepad, open the properties file for the appropriate locale.
4. To configure the header for Collaboration Agent, set `login.HEADER.AAC` to the appropriate value. The value you enter will appear on the Login page (Components you can customize on the Log-in page on page 82) and the Error page (Components you can customize on the error page on page 87).

Note:

You may enter HTML special characters when entering the `login.HEADER.AAC` value (for example, `®`).

5. To configure the title for the Collaboration Agent pages (Components you can customize on the application window on page 85), set `login.TITLE.AAC` to the appropriate value.

Note:

You may enter Unicode characters when entering the `login.TITLE.AAC` value (for example, `\u00ae`).

6. When finished, save your changes and exit the file.
7. Repeat Steps 3 through 6 for the properties file of any other locales in which you are interested.

Related Links

Creating a custom theme for Collaboration Agent on page 87

Preparing the custom theme for upload

Before you begin

Make sure you have downloaded and extracted the theme and modified the appropriate settings.

About this task

Use this procedure to assemble the modified theme files for Collaboration Agent into a zipped file. The custom theme files must be stored in a zipped file before you can upload it to the Avaya Aura® Conferencing system.

Procedure

1. Access the directory to which you extracted the theme. This directory and the associated subdirectories contain the modified theme files.
2. Zip the contents of the directory (and subdirectories) to a file named `custom_theme.zip`.
3. Open the file `custom_theme.zip` and verify that the file contains the following directories and files:
   - **css** directory, which contains the following files:
     - `cawcctheme.css`
     - `theme.css`
   - **img** directory, which contains the following files:
     - `avaya_aura_alpha_logo.png`
     - `logo.png`
     - `logo_white.png`

Comments? infodev@avaya.com

- **props** directory, which contains `.properties` files for various locales

Related Links

Creating a custom theme for Collaboration Agent on page 87

Modifying a custom theme for Collaboration Agent

Before you begin

You have created and uploaded a custom theme previously for Collaboration Agent.

About this task

Use this procedure to modify a custom theme you created and uploaded previously for Collaboration Agent. After you make your changes, you will upload your modified custom theme to Avaya Aura® Conferencing via Element Manager Console.

Note:

You can create multiple custom themes and save them on your PC. However, you can only upload one custom theme to Avaya Aura® Conferencing.

Procedure

1. Download the custom theme for Collaboration Agent from Avaya Aura® Conferencing and then extract that zipped file to a folder on your PC. See Downloading the custom theme for Collaboration Agent on page 97.
2. Customize the theme colors for Collaboration Agent . See Modifying the theme colors for Collaboration Agent on page 89.
3. Customize the logos displayed in Collaboration Agent. See Modifying the logos for Collaboration Agent on page 91.
4. Customize the title and header displayed in Collaboration Agent. See Modifying the title and header for Collaboration Agent on page 92.
5. Create a zip file that contains the components of the custom theme in the appropriate structure. See Preparing the custom theme for upload on page 93.
6. Upload the custom theme zip file to Avaya Aura® Conferencing. See Replacing the custom theme for Collaboration Agent on page 95.

Related Links

Customizing Collaboration Agent on page 81

Applying a custom theme for Collaboration Agent

Before you begin

- You have created a zipped file that contains your custom theme.
- You can log into the server as `ntappadm`.

About this task

Use this procedure to apply a custom theme that you created for Collaboration Agent. During this procedure, you will upload via Element Manager Console the custom theme zipped file you created.

Procedure

1. In the navigation pane of Element Manager Console, select **Custom Theme > Custom Theme**.
2. In the Custom Theme window, click **Add (+)**.
3. In the Add Custom Theme dialog box, enter a name for the custom theme in the Theme Name box.
4. In the Theme Description box, enter a description of the custom theme.
5. Click **Browse**.
6. In the Select Custom Theme archive file dialog box, select the custom theme zipped file you want to upload, and click **Open**.
7. In the Message box, click **OK**.
8. In the Add Custom Theme dialog box, click **Upload**.
9. In the FTP Login dialog box, enter `ntappadm` in the User box.
10. In the Password box, enter the password for ntappadm .
11. Click **Apply**.

    The following message appears at the top of the Add Custom Theme dialog box: `Operation in progress. Please wait....`
12. After the custom theme zipped file is uploaded, click **OK** in the Upload Complete message box.
13. Click **Apply**.

Related Links

Customizing Collaboration Agent on page 81

Replacing the custom theme for Collaboration Agent

Before you begin

- You have created a zipped file that contains your custom theme.
- You can log into the server as `ntappadm`.

About this task

Use this procedure to replace the existing custom theme with a new custom theme..

Procedure

1. In the navigation pane of Element Manager Console, select **Custom Theme > Custom Theme**.
2. In the Custom Theme window, select the custom theme.
3. Click **Edit (+/-)**.
4. In the Edit Custom Theme dialog box, enter the name of the new custom theme in Theme Name box.
5. In the Theme Description box, enter a description of the new custom theme.
6. Click **Browse**.
7. In the Select Custom Theme archive file dialog box, select the custom theme zipped file you want to upload, and click **Open**.
8. In the Message box, click **OK**.
9. In the Edit Custom Theme dialog box, click **Upload**.
10. In the FTP Login dialog box, enter `ntappadm` in the User box.
11. In the Password box, enter the password for ntappadm .
12. Click **Apply**.

    The following message appears at the top of the Edit Custom Theme dialog box: `Operation in progress. Please wait....`
13. After the custom theme zipped file is uploaded, click **OK** in the Upload Complete message box.
14. Click **Apply**.

Related Links

Customizing Collaboration Agent on page 81

Removing the custom theme for Collaboration Agent

Before you begin

A custom theme has been uploaded previously to Avaya Aura® Conferencing.

About this task

Use this procedure to remove the custom theme that you created for Collaboration Agent from Avaya Aura® Conferencing. You can have only one custom theme loaded in Avaya Aura® Conferencing at a time.

Procedure

1. In the navigation pane of Element Manager Console, select **Custom Theme > Custom Theme**.
2. In the Custom Theme window, select the custom theme.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes** to delete the custom theme.

Related Links

Customizing Collaboration Agent on page 81

Downloading the custom theme for Collaboration Agent

Before you begin

- You have uploaded previously via Element Manager Console a zipped file that contains your custom theme.
- You can log into the server as `ntappadm`.

About this task

Use this procedure to download the custom theme for Collaboration Agent.

Procedure

1. In the navigation pane of Element Manager Console, select **Custom Theme > Custom Theme**.
2. In the Custom Theme window, select the custom theme.
3. Click **Edit (+/-)**.
4. In the Edit Custom Theme dialog box, click **Download** for Download Custom Theme.
5. In the FTP Login dialog box, enter `ntappadm` in the User box.
6. In the Password box, enter the password for ntappadm .
7. Click **Apply**.
8. In the Save dialog box, select the location where you want to save the custom theme zipped file. By default, the file is named theme.zip.
9. Click **Save**.

   The following message appears at the top of the Edit Custom Theme dialog box: `Operation in progress. Please wait....`
10. After the custom theme zipped file is downloaded to your PC, click **OK** in the Download Complete message box.
11. Click **Apply**.

12. If you want to modify the custom theme, extract the custom theme zipped file to a temporary directory.

Related Links

Customizing Collaboration Agent on page 81

Forcing an update to the custom theme for Collaboration Agent

Before you begin

- You have uploaded previously via Element Manager Console a zipped file that contains your custom theme.
- You can log into the server as `ntappadm`.

About this task

Use this procedure to force all conference agents and provisioning servers to redownload the current custom theme for Collaboration Agent.

Note:

It may take several minutes for all conference agents and provisioning servers to redownload the current custom theme.

Procedure

1. In the navigation pane of Element Manager Console, select **Custom Theme > Custom Theme**.
2. In the Custom Theme window, select the custom theme.
3. Click **Edit (+/-)**.
4. In the Edit Custom Theme dialog box, click **Force Update**.
5. In the Confirmation dialog box, click **Yes**.
6. In the Force Update message box, click **OK**.
7. Click **Apply**.

Related Links

Customizing Collaboration Agent on page 81

Retaining/restoring logo customizations during an upgrade

Before you begin

Ensure you have downloaded and extracted the theme.

About this task

Use this task when you are upgrading from Avaya Aura® Conferencing 7.2 to Avaya Aura® Conferencing 8.0 and you wish to retain and restore any customization that you made to the Collaboration Agent (CA) user interface.

Procedure

1. If you do not have a custom theme, then you must create one.

   For more information, see Creating a custom theme for CA on page 87.

2. Add each of the new additions that are in release 8.0 and not present in release 7.2.

   Avaya Aura® Conferencing 8.0 contains many new elements which were not present in the previous release. You must add these new items to your theme if you require them to be customized.

   Here is a list of the new additions:

Page	New elements
Login page	login-container_custom footer_custom title_custom form-title_custom username-domain-separator_custom remember-me-caption_custom label_custom a.user-type-link_custom a.user-type-link_custom:hover login-button_custom:hover error-message_custom errorpage-warning_message_custom a
Check-in page	checkinview topbackgroundcolor checkinview_buttons_color checkinview_logout checkinview_username checkinview_buttons_hoover

Comments? infodev@avaya.com

Page	New elements
Conference page	application_rosterarea_background active_roster_background inactive_roster_background

Here is the list of the modified elements:

Page	Modified elements <*old name*> — <*new name*>
Login page	div.login-container_custom — login-container_custom input.login-button_custom — login-button_custom
Log off/error page	div.errorpage-header_custom — div.errorpage-logo-custom errorpage-session_error_desc — errorpage-session_error_desc_custom errorpage-warning_message — errorpage-warning_message_custom errorpage-login-header_custom — div.errorpage-login-header_custom

Here is a list of elements that are no longer used in release 8.0:

Page	No longer used
Login page	user-type-selector_custom login-form-line-caption_custom user-type-selector-IE9_custom div.login-header_custom errorpage-error_info-div

Here is a list of the changes to the images in release 8.0:

- The Log off page uses logo.png.
- The Login and Check-in pages use avaya_aura_alpha_logo.png.
- Logo_white.png is used when pop-up blocker is enabled.
- The Login_button.png is not used anymore.

Use the figures (such as Components you can customize on the application window on page 85 and Components you can customize on the Check-in page on page 83) to understand the role of each new or modified item.

3. For more information on modifying your current theme, see Modifying a custom theme for CA on page 94.

Related Links

Customizing Collaboration Agent on page 81

Chapter 6: Managing the Avaya Aura® Conferencing Default Settings

This section describes how to set the following default conference settings for Avaya Aura® Conferencing:

- the URI that will be used to contact the operator for Avaya Aura® Conferencing
- the conference class that will be assigned to “guests” when they log in to a conference
- maximum number of attempts that a user is allowed to enter the correct participant/moderator code
- whether media cascading is on or off
- whether the conferencing Fast Start is on or off
- whether conference continuation is on or off
- whether bandwidth management is on or off
- whether Recording is on or off
- whether the user password is owned locally or not
- conference mode

.

Related Links

Configuring the system operator on page 103
Modifying the conference class of service for the guest login on page 103
Modifying the maximum participant/moderator code entry attempts setting on page 104
Modifying the media cascading setting on page 104
Modifying the conferencing fast start setting on page 105
Modifying the conferencing continuation setting on page 105
Modifying the bandwidth management setting on page 106
Modifying the recording setting on page 107
Modifying the user password owned locally setting on page 107
Modifying the Collaboration Agent plug-in setting on page 108
Modifying the Presentation Mode setting on page 109

Configuring the system operator

Before you begin

- You must be logged into Provisioning Client.
- You can only specify one URI for the operator.

About this task

Use this procedure to specify the URI that will be contacted when a participant requests the operator during a conference.

Procedure

1. In the Provisioning Client window, select **System Management > System Default Settings**.
2. In the Operator box, enter the URI of the operator. When a participant requests the operator during a conference, this URI will be contacted. For more information, see System Default Settings page field descriptions on page 109.
3. Click **Save**.

Related Links

Managing the Avaya Aura Conferencing Default Settings on page 102

Modifying the conference class of service for the guest login

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to change the conference class of service assigned to a participant who logs into a conference as “guest” (that is, uses the guest login).

Procedure

1. In the Provisioning Client window, select **System Management > System Default Settings**.
2. From the Guest conference class box, select the conference class of service that you want to assign to participant who logs into a conference as “guest.” For more information, see System Default Settings page field descriptions on page 109.
3. Click **Save**.

Related Links

Managing the Avaya Aura Conferencing Default Settings on page 102

Modifying the maximum participant/moderator code entry attempts setting

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to specify the maximum number of attempts a user has to enter the correct participant code or moderator code to access a conference.

Procedure

1. In the Provisioning Client window, select **System Management > System Default Settings**.
2. From the **Maximum number of attempt for Collaboration Code or Participant Passcodes entry** field and the **Maximum number of attempt for Moderator Passcode or Moderator Collaboration code entry** field, select the number of attempts a user may have to enter the correct participant codes or moderator codes for a conference. For more information, see System Default Settings page field descriptions on page 109.
3. Click **Save**.

Related Links

Managing the Avaya Aura Conferencing Default Settings on page 102

Modifying the media cascading setting

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to enable or disable the media cascading setting. Media cascading reduces WAN bandwidth usage and costs by optimizing audio and video streams to and from a location. You can benefit from media cascading for regular conferences and also for Event conferences. When media cascading is enabled, the setting on the video class will take effect.

Procedure

1. In the Provisioning Client window, select **System Management > System Default Settings**.
2. Perform one the following steps:
   - To enable media cascading, make sure the **Allow media cascading** check box is checked.
   - To disable media cascading, make sure the **Allow media cascading** check box is unchecked.

   For more information, see System Default Settings page field descriptions on page 109.

3. Click **Save**.

Related Links

Managing the Avaya Aura Conferencing Default Settings on page 102

Modifying the conferencing fast start setting

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to enable or disable the conferencing fast start feature for the system. When the recording feature is enabled for the system, users have the ability to use Fast Start for their conferences.

Procedure

1. In the Provisioning Client window, select **System Management > System Default Settings**.
2. Perform one the following steps:
   - To enable Fast Start and make it mandatory for all users, select **Force Enabled for all users** from the **Conferencing Fast Start** drop down list.
   - To disable Fast Start, select **Force Disabled for all users** from the **Conferencing Fast Start** drop down list.
   - To prevent users from enabling or disabling Fast Start, select **Allow users to enable/disable-default off** from the **Conferencing Fast Start** drop down list.
   - To enable users to enable or disable Fast Start, select **Allow users to enable/disable-default on** from the **Conferencing Fast Start** drop down list.

   For more information, see System Default Settings page field descriptions on page 109.
3. Click **Save**.

Related Links

Managing the Avaya Aura Conferencing Default Settings on page 102

Modifying the conferencing continuation setting

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to control the conference continuation experience for new users. When the conferencing continuation feature is enabled for the system, users have the ability to use enable/disable continuation.

Procedure

1. In the Provisioning Client window, select **System Management > System Default Settings**.
2. Perform one the following steps:
   - To provide users with the ability to enable/disable continuation participant entry and provide a default setting such that continuation is enabled, select **Allow users to enable/disable default on** from the **Conferencing Continuation** drop-down list.
   - To provide users with the ability to enable/disable continuation participant entry and provide a default setting such that continuation is disabled, select **Allow users to enable/disable default off** from the **Conferencing Continuation** drop-down list.

   For more information, see System Default Settings page field descriptions on page 109.
3. Click **Save**.

Related Links

Managing the Avaya Aura Conferencing Default Settings on page 102

Modifying the bandwidth management setting

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to enable or disable the bandwidth management setting. Bandwidth management helps increase session traffic and reduce costs while managing the quality of multimedia sessions. In a one-server campus deployment, you may want to disable bandwidth management.

Procedure

1. In the Provisioning Client window, select **System Management > System Default Settings**.
2. Perform one the following steps:
   - To enable bandwidth management, make sure the **Allow bandwidth management** check box is checked.
   - To disable bandwidth management, make sure the **Allow bandwidth management** check box is unchecked.

   For more information, see System Default Settings page field descriptions on page 109.
3. Click **Save**.

Related Links

Managing the Avaya Aura Conferencing Default Settings on page 102

Modifying the recording setting

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to enable or disable the Recording feature for the system. The Recording feature enables users to record audio, video, and web collaboration sessions. When the Recording feature is enabled for the system, you can then enable the Recording feature on a per user basis.

Procedure

1. In the Provisioning Client window, select **System Management > System Default Settings**.
2. Perform one the following steps:
   - To enable recording, make sure the **Allow recording** check box is checked.
   - To disable bandwidth management, make sure the **Allow recording** check box is unchecked.

   For more information, see System Default Settings page field descriptions on page 109.
3. Click **Save**.

Related Links

Managing the Avaya Aura Conferencing Default Settings on page 102

Modifying the user password owned locally setting

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to control whether the Avaya Aura® Conferencing system ‘owns’ the user password. If the Avaya Aura® Conferencing system owns the user password, it can be changed using Collaboration Agent and the password policy is applied when adding or modifying a user. The password policy is also applied when the password is changed. This also means that the user password is only pushed when users are added from external systems, such as System Manager in an Avaya Aura® deployment. If the password is not owned by the Avaya Aura® Conferencing system, and is owned by an external system, it cannot be changed using Collaboration Agent. It is synced from the external system in its current state and no password policy is applied.

Procedure

1. In the Provisioning Client window, select **System Management > System Default Settings**.
2. Perform one the following steps:
   - To ensure that the Avaya Aura® Conferencing system controls the password, select the **User Password Owned Locally** checkbox.
   - To ensure that an external system controls the password, do not select the **User Password Owned Locally** checkbox.

   For more information, see System Default Settings page field descriptions on page 109.
3. Click **Save**.

Related Links

Managing the Avaya Aura Conferencing Default Settings on page 102

Modifying the Collaboration Agent plug-in setting

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to enable or disable the Collaboration Agent plug-in setting for the system. This plug-in enhances the user experience when sharing data during conferences. It provides a more seamless collaboration experience with a secure and easy way of launching the screen sharing functionality.

If do not enable this checkbox, users can still access the existing collaboration functionality through the use of a Java Web applet invoked by the user's Web browser.

Procedure

1. In the Provisioning Client window, select **System Management > System Default Settings**.
2. Perform one the following steps:
   - To enable the download of the plug-in, make sure that the Allow collaboration plugin checkbox is checked.
   - To disable the download of the plug-in, make sure that the Allow collaboration plugin checkbox is unchecked.

   For more information, see System Default Settings page field descriptions on page 109.
3. Click **Save**.

Related Links

Managing the Avaya Aura Conferencing Default Settings on page 102

Modifying the Presentation Mode setting

In a conference with Presentation Mode, all participants join the web collaboration session as presenters. Presentation Mode enables any participant to start the web collaboration aspect of the conference. Presentation Mode means that participants do not have to wait for the moderator to start web collaboration before they can join a web collaboration session and begin sharing.

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to enable or disable the Presentation Mode feature for the system.

Procedure

1. In the Provisioning Client window, select **System Management > System Default Settings**.
2. Perform one the following steps:
   - To enable Presentation Mode, make sure the **Allow Presentation mode** check box is checked.
   - To disable Presentation Mode, make sure the **Allow Presentation mode** check box is unchecked.

   For more information, see System Default Settings page field descriptions on page 109.
3. Click **Save**.

Related Links

Managing the Avaya Aura Conferencing Default Settings on page 102
System Default Settings page field descriptions on page 109

System Default Settings page field descriptions

Name	Description
Operator	Displays the URI to which a conference participant will be forwarded when that person requests the operator.
Guest conference class	Displays the conference class of service that is assigned to a user who logs into a conference as “guest.”
Maximum number of attempts for Collaboration or Participant Pass codes entry	Displays the maximum number of attempts a user may have to enter the correct pass code for a conference. Your choices are 1 through 5.

Name	Description
Maximum number of attempts for Moderator Pass code or Moderator Collaboration code entry	Displays the maximum number of attempts the moderator may have to enter the correct moderator pass code for a conference. Your choices are 1 through 5.
Allow media cascading	Media cascading reduces WAN bandwidth usage and costs by optimizing audio and video streams to and from a location. When media cascading is enabled, the setting on the video class will take effect. If there are delays or issues in a room system, you may want to disable media cascading.
Conferencing fast start	Specify whether you want to allow users to have the ability to use the Fast Start feature for their conferences. • To enable Fast Start and make it mandatory for all users, select **Force Enabled for all users** from the **Conferencing Fast Start** drop down list. • To disable Fast Start, select **Force Disabled for all users** from the **Conferencing Fast Start** drop down list. • To prevent users from enabling or disabling Fast Start, select **Allow users to enable/disable-default off** from the **Conferencing Fast Start** drop down list. • To enable users to enable or disable Fast Start, select **Allow users to enable/disable-default on** from the **Conferencing Fast Start** drop down list.
Conference continuation	Use this feature to control the conference continuation experience for new users, as follows: • **Allow user to enable/disable, default on**: If you select this option, you provide users with the ability to enable/disable continuation and you provide a default setting such that continuation is enabled. • **Allow user to enable/disable, default off**: If you select this option, you provide users with the ability to enable/disable continuation and you provide a default setting such that continuation is disabled.
Allow bandwidth management	Bandwidth management helps increase session traffic and reduce costs while managing the quality of multimedia sessions. In a one-server campus deployment, you may want to disable bandwidth management.

Name	Description
Allow recording	Specify whether you want to allow users to have the ability to record audio, video, and web collaboration sessions. If you uncheck this check box, users will be unable to use the Recording feature.
User password owned locally	Specify whether the Avaya Aura® Conferencing system owns the password. If the Avaya Aura® Conferencing system owns the password, it can be changed using Collaboration Agent and the password policy is applied when adding or modifying a user. The password policy is also applied when changing the user password. This also means that the user password is only pushed from an external system, such as System Manager in an Avaya Aura® deployment, when a new user is added to that external system. If the password is owned by an external system, it cannot be changed using Collaboration Agent and is synced from the external system in its current state and no password policy is applied.
Allow collaboration plugin	Specify whether you want to allow users to have the ability to download the Collaboration Agent plug-in. This plug-in enhances the user experience when sharing data during conferences. It provides a more seamless collaboration experience with a secure and easy way of launching the screen sharing functionality. If do not enable this checkbox, users can still access the existing collaboration functionality through the use of a Java Web applet invoked by the user's Web browser.
Allow Presentation mode	Specify whether you want to allow users to enter the conference with the ability to start Web Collaboration. In Presentation mode, users of all levels can start web collaboration. If you do not enable this feature, users have to wait until the moderator starts web collaboration and gives them the presenter role before joining the web collaboration session and getting the ability to share.

Related Links

Modifying the Presentation Mode setting on page 109

Chapter 8: Managing Your Domains

This section describes how to view, add, modify, and delete Avaya Aura® user domains in Provisioning Client. If you have an Avaya Aura® deployment, Provisioning Client must contain all of the domains in System Manager. This section also describes how to view, modify, and delete enterprise domains in Provisioning Client. The enterprise domain is the Lightweight Directory Access Protocol (LDAP) domain. It is necessary for integration with an LDAP server.

Note:

Your login must have Expert mode privileges to add, modify, and delete domains.

Related Links

Viewing user domains on page 112
Viewing LDAP domains on page 113
Adding a user domain on page 113
Adding an LDAP domain on page 114
Deleting a domain on page 114

Viewing user domains

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to view the user domains.

If your login has Expert mode privileges, you can add and modify user domains.

Procedure

In the Provisioning Client window, select **System Management > User Domains**.

Related Links

Managing Your Domains on page 112
User Domains page field descriptions on page 113

User Domains page field descriptions

Name	Description
User Domain	Specifies the user domain that you want to add.
User Domain column	Displays the user domains that are currently administered for Avaya Aura® Conferencing.
Delete column	Enables you to delete the associated user domain.

Related Links

Viewing user domains on page 112

Viewing LDAP domains

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to view the Lightweight Directory Access Protocol (LDAP) domains.

If your login has Expert mode privileges, you can add and modify LDAP domains.

Procedure

In the Provisioning Client window, select **System Management** > **Enterprise Domains**.

Related Links

Managing Your Domains on page 112

Adding a user domain

Before you begin

- You must be logged into Provisioning Client.
- Your login must have Expert mode privileges to perform this procedure.

Warning:

If you have an Avaya Aura® deployment, any changes you make may cause the Provisioning Client data to become out of sync with the data in Avaya Aura System Manager. You should only modify data to fix sync issues that cannot be resolved from the System Manager interface.

About this task

Use this procedure to add a user domain. If you have an Avaya Aura® deployment, Provisioning Client must contain all of the domains in System Manager.

Procedure

1. In the Provisioning Client window, select **System Management > User Domains**.
2. In the User Domain box, enter the name of the domain you want to add.
3. Click **Add**.

Related Links

Managing Your Domains on page 112

Adding an LDAP domain

Before you begin

- You must be logged into Provisioning Client.
- Your login must have Expert mode privileges to perform this procedure.

Warning:

If you have an Avaya Aura® deployment, any changes you make may cause the Provisioning Client data to become out of sync with the data in Avaya Aura System Manager. You should only modify data to fix sync issues that cannot be resolved from the System Manager interface.

About this task

Use this procedure to add an LDAP domain.

Procedure

1. In the Provisioning Client window, select **System Management** > **Enterprise Domains**.
2. In the Enterprise Domain box, enter the name of the domain you want to add.
3. Click **Add**.

Related Links

Managing Your Domains on page 112

Deleting a domain

Before you begin

- You must be logged into Provisioning Client.
- Your login must have Expert mode privileges to perform this procedure.

Warning:

If you have an Avaya Aura® deployment, any changes you make may cause the Provisioning Client data to become out of sync with the data in Avaya Aura System Manager. You should only modify data to fix sync issues that cannot be resolved from the System Manager interface.

About this task

Use this procedure to delete a user or LDAP domain.

Procedure

1. In the Provisioning Client window, select **System Management** > **User Domains** or **System Management** > **Enterprise Domains**, depending on the type of domain that you wish to delete.
2. In the Delete column, click **Delete** for the domain you want to delete.
3. In the Confirmation window, enter your password, and click **Confirm**.

Related Links

Managing Your Domains on page 112

Chapter 9: Managing Locations

This section describes how to

- add, modify, and delete locations in Provisioning Client
- configure pattern-matching of IP addresses for locations
- reduce the bandwidth usage for new and existing sessions during periods of high-bandwidth utilization at a location
- configure media stream cascading for a location
- configure a hosting location
- configure pattern-matching of IP addresses

Related Links

Adding a location on page 116
Modifying a location on page 117
Deleting a location on page 118
Modifying location settings on page 119
Configuring IP address patterns on page 119
Optimizing the bandwidth for a location on page 122
Configuring media stream cascading for a location on page 124
Configuring a hosting location on page 126
Configuring a regional cascading location on page 127
Configuring locations and media server clusters for recording on page 129

Adding a location

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to add a location.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Locations**.

2. Click **Add Location**.
3. In the Location Name box, enter the name of the location.

   If your deployment is an Avaya Aura® deployment, this name must match the location name in System Manager.
4. In the Location Description box, enter any pertinent information about the location.
5. Click **Save**.

Related Links

Managing Locations on page 116
Location page field descriptions on page 117
Add Location page field descriptions on page 117

Location page field descriptions

Name	Description
Add Location	Enables you to add a new location.
Location name	Enables you to modify the associated location.
Delete	Deletes the associated location.

Related Links

Adding a location on page 116

Add Location page field descriptions

Name	Description
Location Name	This is the name of a location in System Manager that you want to add to Provisioning Client. If your deployment is an Avaya Aura® deployment, this name must match the location name in System Manager.
Location Description	Any pertinent information you want to include about this location.

Related Links

Adding a location on page 116

Modifying a location

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to modify an existing location.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Locations**.
2. Click the name of the location you want to modify.
3. On the Modify Location tab, make your changes. See Modify Location page field descriptions on page 118.
4. Click **Save**.

Related Links

Managing Locations on page 116
Modify Location page field descriptions on page 118

Modify Location page field descriptions

Name	Description
Location Name	This is the name of a location in System Manager. If your deployment is an Avaya Aura® deployment, this name must match the location name in System Manager.
Location Description	Any pertinent information you want to include about this location.

Related Links

Modifying a location on page 117

Deleting a location

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to delete a location.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Locations**.

2. Click **Delete** for the location you want to delete.
3. In the Confirmation window, enter your password, and then click **Confirm**.

Related Links

Managing Locations on page 116

Modifying location settings

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to configure location specific conferencing settings.

Procedure

1. In the Provisioning Client window, select **System Management** > **Location Settings**.
2. Choose the name of the location you want to modify.
3. Make your changes.

   For more information, see Modify Location Settings page field descriptions on page 119.
4. Click **Save**.

Related Links

Managing Locations on page 116
Modify Location Settings page field descriptions on page 119

Modify Location Settings page field descriptions

Name	Description
AViCA enabled	Controls if Audio/Video in Collaboration Agent (AViCA) feature is enabled for selected location

Related Links

Modifying location settings on page 119

Configuring IP address patterns

Within each site location, you can configure Avaya Aura® Conferencing to match a single IP address, a range of IP addresses, a specified subnet, or you can configure a wildcard within an IP

address. So, for example, if your site contains all of the IP addresses from 192.168.0.0 to 192.168.0.50, you can configure Avaya Aura® Conferencing to successfully connect a call from any IP in this range.

If an IP address matches several patterns, selection is based on their type. Priority order from highest to lowest is as follows:

- Single address: For example, 192.168.0.3.
- Wildcard: For example, 192.168.0.x.
- Interval: For example, 192.168.0.0-192.168.0.50.
- Subnet: For example, 192.168.0.0/24.

Inside each type, patterns are sorted by the address range.

Tip:

Use only one pattern type if possible to avoid unexpected results when using multiple types.

Use 0.0.0.0/0 as global pattern with the lowest priority.

Related Links

Managing Locations on page 116
Location Address Patterns page field descriptions on page 120
Adding an IP address pattern on page 121
Copying an IP address pattern on page 121
Deleting an IP address pattern on page 122

Location Address Patterns page field descriptions

Name	Description
Select location	Displays the list of provisioned locations. For more information about adding a new location, see Adding a location on page 116.
IP Address Pattern	Specify the IP address pattern that you wish to match. For syntax examples, see Configuring IP address patterns on page 119.
Notes	Enter any free text notes relating to the IP address pattern.

Button	Description
Save	Saves the details of the IP address pattern.

Name	Description
IP Address Pattern column	Displays the IP address pattern.
Notes column	Displays any free text notes relating to the IP address pattern.

Name	Description
Copy column	Copies the corresponding IP address pattern so that you can use it as a base for the addition of another IP address pattern.
Delete column	Deletes the corresponding IP address pattern.

Related Links

Configuring IP address patterns on page 119

Adding an IP address pattern

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to add an IP address pattern.

Procedure

1. In the Provisioning Client window, click **System Management** > **Routing** > **Locations**
2. Click the **Location Address Patterns** tab.
3. From the **Select Location** drop-down menu, select a location.

   For more information about adding a new location, see Adding a location on page 116.
4. In the **IP Address Pattern** field, enter an IP address pattern.

   For syntax examples, see Configuring IP address patterns on page 119.
5. In the **Notes** field, enter any additional information relating to the IP address pattern.
6. Click **Save**.

Result

Avaya Aura® Conferencing adds the new IP address pattern.

Related Links

Configuring IP address patterns on page 119

Copying an IP address pattern

You can copy an IP address pattern to use as a starting point for adding a new IP address pattern. This functionality means that you do not have to type the entire address again. It is useful if the IP addresses are very similar.

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to copy an IP address pattern.

Procedure

1. In the Provisioning Client window, click **System Management** > **Routing** > **Locations**
2. Click the **Location Address Patterns** tab.
3. Click the **Copy** link that corresponds to the IP address pattern that you want to copy.

   The Provisioning Client displays the copied IP address pattern in the **IP Address Pattern** field. You can now modify it and click **Save** to add a new IP address pattern.

Result

Avaya Aura® Conferencing copies the IP address pattern.

Related Links

Configuring IP address patterns on page 119

Deleting an IP address pattern

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to delete an IP address pattern.

Procedure

1. In the Provisioning Client window, click **System Management** > **Routing** > **Locations**
2. Click the **Location Address Patterns** tab.
3. Click the **Delete** link that corresponds to the IP address pattern that you want to delete.

   The Provisioning Client displays a warning and requests you to enter your Provisioning Client password.
4. Enter your Provisioning Client password and click **Confirm** to delete the IP address pattern.

Result

Avaya Aura® Conferencing deletes the IP address pattern.

Related Links

Configuring IP address patterns on page 119

Optimizing the bandwidth for a location

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to reduce the bandwidth usage for new and existing sessions during periods of high-bandwidth utilization at a location.

Procedure

1. In the Provisioning Client window, select **System Management > Bandwidth Optimization**.
2. From the Select location box, select the appropriate location.
3. Complete the fields as appropriate. See Bandwidth Optimization page field descriptions on page 123.
4. Click **Save**.

Related Links

Managing Locations on page 116
Bandwidth Optimization page field descriptions on page 123

Bandwidth Optimization page field descriptions

Name	Description
Select location	Displays the configured locations.
High threshold	When the bandwidth at the selected location exceeds this setting, the bandwidth usage for new sessions will be reduced based on the priority settings of each user. Some users may receive lower video resolution, but new sessions will be able to start. Existing sessions are unaffected. This setting is also used to define the limit for stopping bandwidth optimization for all existing sessions after the Critical threshold is exceeded. The range is 75 to 100. When set to 100 percent, bandwidth optimization is disabled for all new and existing sessions.
Critical threshold	When the bandwidth at the selected location exceeds this setting, the bandwidth usage for all new and existing sessions will be reduced based on the priority settings of each user. Bandwidth optimization will continue for all new and existing sessions until the High Threshold limit is reached. Some users may receive lower video resolution, but new sessions will be able to start until the maximum allowed bandwidth is reached.

Name	Description
	The range is 75 to 100. When set to 100 percent, bandwidth optimization is disabled for existing sessions. This value should be greater than the High threshold setting.

Related Links

Optimizing the bandwidth for a location on page 122

Configuring media stream cascading for a location

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to configure media stream cascading for a location.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Stream Cascading** tab.
3. From the Select location box, select the appropriate location.
4. Complete the fields as appropriate. See Media Stream Cascading tab field descriptions on page 124.
5. Click **Save**.

Related Links

Managing Locations on page 116
Media Stream Cascading tab field descriptions on page 124

Media Stream Cascading tab field descriptions

Name	Description
Select location	Enables you to specify the location for which you want to configure media cascading.
Cascading is allowed when this location is hosting the conference	Specifies whether media cascading can occur for a conference hosted at this location.

Name	Description
Allowed number of video streams to a remote location	Specifies the maximum number of video streams sent from a host media server to a remote media server in a cascading media server environment. For example, if you set this value to 1, then only one video stream (of the active speaker) will be sent from the host media server to the remote media server. If you set this value to 4, then four video streams (showing the active speaker and the previous three active speakers) will be sent from the host media server to the remote media server. Your choices are 1 through 4. Changing this setting affects all conferences that use cascading media servers at the selected location.
Allowed number of video streams from a remote location	Specifies the maximum number of video streams sent from a remote media server to a host media server in a cascading media server environment. For example, if you set this value to 1, then only one video stream (of the active speaker) will be sent from the remote media server to the host media server. If you set this value to 4, then four video streams (showing the active speaker and the previous three active speakers) will be sent from the remote media server to the host media server. Your choices are 1 through 4. Changing this setting affects all conferences that use cascading media servers at the selected location.
Cascading is allowed when the conference is hosted remotely at another location	Specifies whether media cascading can occur for a conference that is hosted at another location.
Allowed number of video streams to a hosting location	Specifies the maximum number of video streams sent from a remote media server to a host media server in a cascading media server environment . For example, if you set this value to 1, then only one video stream (of the active speaker) will be sent from the remote media server to the host media server. If you set this value to 4, then four video streams (showing the active speaker and the previous three active speakers) will be sent from the remote media server to the host media server. Your choices are 1 through 4. Changing this setting affects all conferences that use cascading media servers at the selected location.
Allowed number of video streams from a hosting location	Specifies the maximum number of video streams sent from a host media server to a remote media server in a cascading media server environment . For example, if you set this value to 1, then only one

Name	Description
	video stream (of the active speaker) will be sent from the host media server to the remote media server. If you set this value to 4, then four video streams (showing the active speaker and the previous three active speakers) will be sent from the host media server to the remote media server. Changing this setting affects all conferences that use cascading media servers at the selected location.

Related Links

Configuring media stream cascading for a location on page 124

Configuring a hosting location

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to associate multiple locations with a hosting location. This hosting location will host conferences for the locations you specify.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Hosting Locations** tab.
3. From the Select Hosting Location box, select the hosting location you want to configure. For more information see, Hosting Locations tab field descriptions on page 126
4. From the Hostable Locations box, select the appropriate location(s), and then click **Copy**. If you want to assign all locations, click **Copy all**.
5. Click **Save**.

Related Links

Managing Locations on page 116
Hosting Locations tab field descriptions on page 126

Hosting Locations tab field descriptions

Name	Description
Select Hosting Location	Select the hosting location you want to configure.

Name	Description
Hostable Locations	Displays the locations that you can assign to the selected location. From this list box, you can select the location(s) that you want to assign to the selected hosted location.
Hosted Locations	Displays the locations that you want to assign to the selected hosted location.

Button	Description
Copy all	Moves all of the locations displayed in the Hostable Locations list box into the Hosted Locations list box.
Copy	Moves the selected location in the Hostable Locations list box into the Hosted Locations list box.
Remove	Moves the selected location in the Hosted Locations list box into the Hostable Locations list box.
Remove All	Moves all of the locations displayed in the Hosted Locations list box into the Hostable Locations list box.

Related Links

Configuring a hosting location on page 126

Configuring a regional cascading location

Before you begin

- You must be logged into Provisioning Client.
- Cascaded locations (that is, locations that cascade through a cascading location) must have a good-quality WAN link.
- Cascaded locations do not need to have media servers configured.
- A cascaded location can be assigned to only one cascading location (that is, the location that provides media cascading).
- A cascaded location and cascading location pair cannot be assigned as a hosted location and hosting location pair (and vice versa).
- A cascading location can be the same as the hosting location for a particular location.
- Cascading must be enabled for the Avaya Aura® Conferencing system, the user location, the cascading location, and the hosting location if you want to use regional cascading.
- For Event conferences, the hosting media servers are dedicated Event conference servers. The cascading media servers are not dedicated. In other words, any media servers that are assigned to serve a certain location can be used for media cascading.

About this task

Use this procedure to configure a regional cascading location, which provides media cascading to the remote locations you specify. The users at the specified locations will be able to call into the

regional cascading location instead of the joining the conference directly via the hosting media server. Regional cascading locations enable you to optimize WAN bandwidth usage.

Note:

Cascading must be allowed (enabled) for the Avaya Aura® Conferencing system, the user location, the cascading location, and the hosting location if you want to use regional cascading.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Cascading Locations** tab.
3. From the Select Cascading Location box, select the location that will provide media cascading for other locations.
4. From the Locations that have no Cascading Location assigned list box, select the location(s) that you want to assign to the selected cascading location, and then click **Copy**. If you want to assign all locations, click **Copy all**. For more information see, Media Cascading Locations tab field descriptions on page 128.
5. Click **Save**.

Related Links

Managing Locations on page 116
Media Cascading Locations tab field descriptions on page 128

Media Cascading Locations tab field descriptions

Name	Description
Select Cascading Location	Select the location that will provide media cascading for other locations.
Locations that have no Cascading Location assigned	Displays the locations that you can assign to the selected cascading location. From this list box, you can select the location(s) that you want to assign to the selected cascading location.
Locations that cascade through <*selected cascading location*>	Displays the locations that you want to assign to the selected cascading location. The selected cascading location is a variable/dynamic field, based on the **Select Cascading Location** field.

Button	Description
Copy all	Moves all of the locations displayed in the Locations that have no Cascading Location assigned list box into the Locations that cascade through list box.

Button	Description
Copy	Moves the selected location in the Locations that have no Cascading Location assigned list box into the Locations that cascade through list box.
Remove	Moves the selected location in the Locations that have no Cascading Location assigned list box into the Locations that cascade through list box.
Remove All	Moves all of the locations displayed in the Locations that cascade through list box into the Locations that have no Cascading Location assigned list box.

Related Links

Configuring a regional cascading location on page 127

Configuring locations and media server clusters for recording

Before you begin

- You must be logged into Provisioning Client.
- Media servers and media server cluster must be configured already on Element Manager Console.

About this task

Use this procedure to configure the location and media server cluster for recording. You can configure Recording by location or by media server cluster.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Cluster for Recording** tab.
3. If you want to configure Recording by location, perform the following steps:
   a. From the Select by box, select **Location**.
   b. From the Select Location box, select the location you want to assign to a recording cluster.
   c. From the Recording Cluster box, select the appropriate recording cluster.
   d. Click **Save**.
4. If you want to configure Recording by media server cluster, perform the following steps:
   a. From the Select by box, select **Media Server Cluster**.
   b. From the Select Recording Media Server Cluster box, select the recording cluster you want to assign to a location.

c. In the Select Locations area, select the check box for each location you want to assign to the selected recording cluster.

d. Click **Save**.

Related Links

Managing Locations on page 116

Chapter 10: Managing Conference Access Numbers

This section describes how to

- add, modify, and delete conference access numbers
- add, modify, and delete the conference access number displayed in Collaboration Agent

Managing Conference Access Numbers

Adding a conference access number

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to add an access number for users to dial into a conference. You can create access numbers for the following types of conferences:

- MeetMe
- Adhoc
- Event

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Service URI**.
2. In the Service URI box, enter the access number that you want to add.
3. From the Locale box, select the appropriate locale.
4. From the Conference Type box, select the type of conference for this access number. For more information, see Service URI page field descriptions on page 132.
5. Click **Save**.

Related Links

Managing Conference Access Numbers on page 131

Service URI page field descriptions on page 132

Service URI page field descriptions

Name	Description
Service URI	Specifies the access number that users must dial to access a conference.
Locale	Specifies the primary language used for the associated conference access number. Your choices are: • **English (United States)** • **Chinese (Simplified)** • **Japanese (Japan)** • **Korean (Korea)** • **French (France)** • **German (Germany)** • **Italian (Italy)** • **Russian (Russia)** • **English (United Kingdom)** • **Spanish (Mexico)** • **Portuguese (Brazil)** • **French (Canada)** • **English (Canada)**
Conference Type	Specifies the type of conference for this access number. Your choices are: • **MeetMe** • **Adhoc** • **Event**
Service URI column	Displays the service URI for each administered conference access number.
Conference Type column	Displays the conference type for the associated conference access number.
Locale column	Displays the language for the associated conference access number.
Delete column	Enables you to delete the associated conference access number.

Related Links

Adding a conference access number on page 131

Modifying a conference access number

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to change the service URI, locale, or conference type for an existing conference access number.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Service URI**.
2. In the Service URI column, click the access number you want to modify.
3. Make your changes. See Service URI page field descriptions on page 132.
4. Click **Save**.

Related Links

Managing Conference Access Numbers on page 131

Deleting a conference access number

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to delete a conference access number.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Service URI**.
2. In the Delete column, click **Delete** for the access number you want to delete.
3. In the Confirm window, enter your password, and click **Confirm**.

Related Links

Managing Conference Access Numbers on page 131

Managing Conference Access Numbers Displayed in Collaboration Agent

Adding a conference access number to be displayed in Collaboration Agent

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to add a conference access number to be displayed in Collaboration Agent.

To change the order in which the conference access numbers are displayed in Collaboration Agent, see Changing the order of conference access numbers displayed in Collaboration Agent on page 135.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Service URI**.
2. Click the **Display Numbers** tab.
3. In the Display Number box, enter the access number that you want to be displayed in Collaboration Agent. See Display Numbers page field descriptions on page 134.
4. In the Description box, enter a description for the corresponding access number.
5. Click **Save**.

Related Links

Managing Conference Access Numbers on page 131
Display Numbers page field descriptions on page 134

Display Numbers page field descriptions

Name	Description
Display Number	Specifies the conference access number displayed in Collaboration Agent.
Description	Describes the corresponding conference access number.
Display Number column	Lists the conference access numbers displayed in Collaboration Agent.
Description column	Displays the description for the corresponding conference access number.
Display Order column	Use **Move Up** and **Move Down** to change the order in which the conference access numbers are

Name	Description
	displayed in Collaboration Agent. When you click **Move Up** or **Move Down** for an entry, the order in which the conference access numbers are displayed changes accordingly.
Delete column	Enables you to delete the associated conference access number displayed in Collaboration Agent.

Related Links

Adding a conference access number to be displayed in Collaboration Agent on page 134

Modifying a conference access number displayed in Collaboration Agent

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to modify a conference access number that is displayed in Collaboration Agent.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Service URI**.
2. Click the **Display Numbers** tab.
3. In the Display Number column, click the access number displayed in Collaboration Agent that you want to modify.
4. Make your changes. See Display Numbers page field descriptions on page 134.
5. Click **Save**.

Related Links

Managing Conference Access Numbers on page 131

Changing the order of conference access numbers displayed in Collaboration Agent

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to change the order in which conference access numbers are displayed in Collaboration Agent.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Service URI**.
2. Click the **Display Numbers** tab.
3. In the Display Order column, use **Move Up** and **Move Down** to change the order in which the conference access numbers are displayed in Collaboration Agent. When you click **Move Up** or **Move Down** for an entry, the order in which the conference access numbers are displayed changes accordingly.

Related Links

Managing Conference Access Numbers on page 131

Deleting a conference access number displayed in Collaboration Agent

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to delete a conference access number that is displayed in Collaboration Agent.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Service URI**.
2. Click the **Display Numbers** tab.
3. In the Delete column, click **Delete** for the access number displayed in Collaboration Agent that you want to delete.

Related Links

Managing Conference Access Numbers on page 131

Chapter 11: Managing Video Class of Service

Adding a video class of service

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to create a new video class of service.

Procedure

1. In the Provisioning Client window, select **System Management > Video Class of Service**.
2. If you want to add a video class that is based on an existing video class, click **Copy** for the existing video class you want to use.
3. In the Name box, enter the name for the video class you want to add.
4. Complete the fields as appropriate. See Video Class of Service page field descriptions on page 137.
5. Click **Save**.

Related Links

Video Class of Service page field descriptions on page 137

Video Class of Service page field descriptions

Name	Description
Name	Displays the name of the video class of service.
Maximum average bandwidth per participant (kbps)	Displays the maximum average bandwidth allowed for each participant on the conference. The minimum setting depends on the codec class you select. The maximum setting is 12000 kbps.
Codec Class	Specifies the codec class for the video class of service.

Name	Description
	Clicking the arrow button next to this box displays the maximum resolution and the aspect ratio for the selected codec class.
Maximum resolution	Displays the maximum resolution for the selected codec class.
Aspect Ratio	Displays the aspect ratio for the selected codec class.
Base resolution	Specifies the base resolution for the video class of service.

Name	Description
Name column	Displays the existing video class of service. Clicking on the name of a video class of service displays the associated settings.
Maximum Bandwidth (kbps) column	Displays the maximum bandwidth (kbps) setting for the associated video class of service.
Maximum Resolution column	Displays the maximum resolution setting for the associated video class of service.
Codec Class column	Displays the codec class setting for the associated video class of service.
Copy column	Enables you to create a new video class of service that is based on the associated video class of service.
Delete column	Enables you to delete the associated video class of service. **Note:** You cannot delete a default video class of service.

Related Links

Adding a video class of service on page 137

Modifying a video class of service

Before you begin

You must be logged into Provisioning Client.

About this task

Perform this procedure to modify an existing video class of service.

Note:

You cannot modify the settings for a default video class of service.

Procedure

1. In the Provisioning Client window, select **System Management > Video Class of Service**.
2. Click the name of the video class you want to modify.
3. Make your changes. See Video Class of Service page field descriptions on page 137.
4. Click **Save**.

Deleting a video class of service

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to delete a video class of service.

Note:

You cannot delete a default video class of service.

Procedure

1. In the Provisioning Client window, select **System Management > Video Class of Service**.
2. Click **Delete** for the video class you want to delete.
3. In the Confirmation window, enter your password, and click **Confirm**.

Chapter 12: Managing Conference Class of Service

Adding a conference class of service

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to create a new conference class of service.

Procedure

1. In the Provisioning Client window, select **System Management > Conference Class of Service**.
2. If you want to add a new conference class of service that is based on an existing class of service, click **Copy** for the existing class of service you want to use.
3. In the Name box, enter the name for the class of service you want to add.
4. Complete the fields as appropriate. See Conference Class of Service page field descriptions on page 140.
5. Click **Save**.

Related Links

Conference Class of Service page field descriptions on page 140

Conference Class of Service page field descriptions

Name	Description
Name	Displays the name of the conference class of service.
Maximum number of participants	Displays the maximum number of participants that can participate on a conference call. This setting can be between 1 and 3000.
Event Conference	Specifies whether the chair person can host an event conference.

Name	Description
Allow dial out to participants	Specifies whether the chair person can invite new participants to the conference. It also specifies whether participants can dial out to their preferred audio devices. This setting does not impact the Conference Manager Plug-in for Microsoft Outlook functionality to dial out from the meeting appointment.
Conference Flow	Choices are: • collaboration_flow • passcode_flow
Participant Passcodes required	Specifies whether passcodes are required for conferences. This setting is only available if **Conference Flow** is set to **passcode_flow**.
Video class	Displays the video class assigned to this conference class of service. You may select a default video class or a custom video class that you previously created. The settings for the selected video class appear below the Video class box.

Name	Description
Name column	Displays the existing conference class of service. Clicking on the name of a conference class of service displays the associated settings.
Copy column	Enables you to create a new conference class of service that is based on the associated conference class of service.
Delete column	You cannot delete a default conference class of service.
Users column	Displays all of the users to which the associated conference class of service is assigned.

Related Links

Adding a conference class of service on page 140

Modifying a conference class of service

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to modify an existing conference class of service.

Note:

You cannot modify a default conference class of service.

Procedure

1. In the Provisioning Client window, select **System Management > Conference Class of Service**.
2. Click the name of the conference class of service you want to modify.
3. Make your changes. See Conference Class of Service page field descriptions on page 140.
4. Click **Save**.

Viewing the users assigned to a conference class of service

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to view all of the users assigned to a specific conference class of service.

Procedure

1. In the Provisioning Client window, select **System Management > Conference Class of Service**.
2. Click **Users** for the appropriate conference class of service.

Related Links

List of Users page field descriptions on page 142

List of Users page field descriptions

Name	Description
Login name column	Displays the login name of each user.
Communication Profile	Displays the administered communications profile for each user.

Related Links

Viewing the users assigned to a conference class of service on page 142

Deleting a conference class of service

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to delete a conference class of service.

Note:

You cannot delete a default conference class of service.

Procedure

1. In the Provisioning Client window, select **System Management > Conference Class of Service**.
2. Click **Delete** for the conference class of service you want to delete.
3. In the Confirmation window, enter your password, and click **Confirm**.

Chapter 13: Managing IP Addresses

Adding an IP address

Before you begin

You must know the IPv4 address of the server you want to add.

About this task

Use this procedure to add the IP address of a server.

Procedure

1. In the navigation pane of Element Manager Console, select **Addresses**.
2. In the Addresses window, click **Add (+)**.
3. In the Logical Name box in the Add IPv4 Address dialog box, enter the logical name for the IP address you want to add. The name can contain up to 16 alphanumeric characters.
4. In the IPv4 Address dialog box, enter the IPv4 address.
5. When finished, click **Apply**.

Modifying an IP address

About this task

Use this procedure to modify the IP address of a server.

You can modify only the IPv4 address.

Procedure

1. In the navigation pane of Element Manager Console, select **Addresses**.
2. In the Addresses window, select the IP address you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit IPv4 Address dialog box, make your changes.
5. When finished, click **Apply**.

Deleting an IP address

About this task

Use this procedure to delete the IP address of a server.

Procedure

1. In the navigation pane of Element Manager Console, select **Addresses**.
2. In the Addresses window, select the IP address you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Chapter 14: Managing External Nodes

Adding an external node

Before you begin

The IP address of the external node you want to add must exist in the Addresses window. See Adding an IP address on page 144 for more information.

About this task

Use this procedure to add multiple informational elements with the same IP address and different ports.

Procedure

1. In the navigation pane of Element Manager Console, select **External Nodes**.
2. In the External Nodes window, click **Add (+)**.
3. In the Name box in the Add External Node dialog box, enter the name for the external node. The name can contain up to 16 alphanumeric characters.
4. From the IPv4 Address box, select the logical name of the IPv4 address that you want to assign to this external node. The logical names displayed in the IPv4 Address box are configured in the Addresses window. For more information, see Add Edit External Node dialog box field descriptions on page 147.
5. When finished, click **Apply**.

Modifying an external node

About this task

Use this procedure to modify an external node.

You can modify only the IPv4 address of an external node.

Procedure

1. In the navigation pane of Element Manager Console, select **External Nodes**.
2. In the External Nodes window, select the external node you want to modify.
3. Click **Edit (-/+)**.

4. From the IPv4 Address box in the Edit External Node dialog box, select the appropriate IP address for the external node. For more information, see Add Edit External Node dialog box field descriptions on page 147.
5. When finished, click **Apply**.

Related Links

Add/Edit External Node dialog box field descriptions on page 147

Add/Edit External Node dialog box field descriptions

Name	Description
Name	The name of the device (1–16 alphanumeric characters)
IPv4 Address	The IPv4 address of the device (select from the list). You must configure an IPv4 address for each node.

Related Links

Modifying an external node on page 146

Deleting an external node

About this task

Use this procedure to delete an external node.

Procedure

1. In the navigation pane of Element Manager Console, select **External Nodes**.
2. In the External Nodes window, select the external node you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Chapter 15: Managing Avaya Aura System Manager Elements

Does this section apply?

This section only applies to Avaya Aura® deployments. This section does not apply to Turnkey deployments.

You do not manage Avaya Aura® System Manager or Session Manager elements if you have a Turnkey deployment.

Modifying the Avaya Aura® System Manager element

About this task

Use this procedure to modify the Avaya Aura® System Manager element.

You can modify the following parameters for the Avaya Aura® System Manager element:

- long name
- node

Procedure

1. In the navigation pane of Element Manager Console, select **Avaya Aura Core > System Manager**.
2. In the System Manager window, select the System Manager element you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit System Manager dialog box, make your changes.
5. When finished, click **Apply**.

Refreshing the Avaya Aura® System Manager element

About this task

Use this procedure to refresh the Avaya Aura® System Manager element.

Procedure

1. In the navigation pane of Element Manager Console, select **Avaya Aura Core > System Manager**.
2. In the System Manager window, select the System Manager element you want to refresh.
3. Click **Refresh**.

Chapter 16: Managing Avaya Aura Session Manager Elements

Does this section apply?

This section only applies to Avaya Aura® deployments. This section does not apply to Turnkey deployments.

You do not manage Avaya Aura® System Manager or Session Manager elements if you have a Turnkey deployment.

Adding an Avaya Aura® Session Manager element

About this task

Use this procedure to add an Avaya Aura® Session Manager element.

Procedure

1. In the navigation pane of Element Manager Console, select **Avaya Aura Core > Session Manager**.
2. In the Session Manager window, click **Add (+)** .
3. In the Add Session Manager dialog box, complete the fields as appropriate. For more information, see Add Edit Session Manager dialog box field descriptions on page 151.
4. When finished, click **Apply**.

Modifying an Avaya Aura® Session Manager element

About this task

Use this procedure to modify an Avaya Aura® Session Manager element.

You can modify the following parameters for an Avaya Aura® Session Manager element:

- long name

- trusted
- ExemptDoSProtection
- node
- SIP TCP port
- SIP TLS port

Procedure

1. In the navigation pane of Element Manager Console, select **Avaya Aura Core > Session Manager**.
2. In the Session Manager window, select the Session Manager element you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Session Manager dialog box, make your changes. For more information, see Add Edit Session Manager dialog box field descriptions on page 151.
5. When finished, click **Apply**.

Related Links

Add/Edit Session Manager dialog box field descriptions on page 151

Add/Edit Session Manager dialog box field descriptions

Name	Description
Short Name	The short name of the element—maximum of 6 characters.
Long Name	The long name of the element—maximum of 32 characters.
Trusted	Specifies whether the element is trusted.
ExemptDoSProtection	Specifies whether the informational element is exempt from Denial of Service Protection.
Port	Displays the port value that the element uses on the external node.
Node	The external node on which the element resides. Select from the list.
Enable SIP TCP	(Check box) Select to enable the SIP TCP port.
SIP TCP Port	Specifies the TCP port for SIP. Example: 5060
Enable SIP TLS	(Check box) Select to enable the SIP TLS port.
SIP TLS Port	Specifies the TLS port for SIP. Example: 5061

Related Links

Modifying an Avaya Aura Session Manager element on page 150

Deleting an Avaya Aura® Session Manager element

About this task

Use this procedure to delete an Avaya Aura® Session Manager element.

Procedure

1. In the navigation pane of Element Manager Console, select **Avaya Aura Core > Session Manager**.
2. In the Session Manager window, select the Session Manager element you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Refreshing an Avaya Aura® Session Manager element

About this task

Use this procedure to refresh an Avaya Aura® Session Manager element.

Procedure

1. In the navigation pane of Element Manager Console, select **Avaya Aura Core > Session Manager**.
2. In the Session Manager window, select the Session Manager element you want to refresh.
3. Click **Refresh**.

Chapter 17: Managing OAM Profiles

Managing OSS Servers

Adding an OSS server

About this task

Use this procedure to add an OSS server.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > OSS Servers**.
2. In the OSS Servers window, click **Add (+)**.
3. In the Add OSS Server dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Modifying an OSS server

About this task

Use this procedure to modify an OSS server.

You can modify the following parameters for an OSS server:

- node
- whether the OSS server uses an external OAM network

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > OSS Servers**.
2. In the OSS Servers window, select the OSS server you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit OSS Server dialog box, make your changes.
5. When finished, click **Apply**.

Deleting an OSS server

About this task

Use this procedure to delete an OSS server.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > OSS Servers**.
2. In the OSS Servers window, select the OSS server you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Refreshing an OSS server

About this task

Use this procedure to refresh an OSS server.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > OSS Servers**.
2. In the OSS Servers window, select the OSS server you want to refresh.
3. Click **Refresh**.

Managing OSS Endpoints

Adding an OSS endpoint

About this task

Use this procedure to add an OSS endpoint.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > OSS Endpoints**.
2. In the OSS Endpoints window, click **Add (+)**.
3. In the Add OSS Endpoint dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Modifying an OSS endpoint

About this task

Use this procedure to modify an OSS endpoint.

You can modify the following parameters for an OSS endpoint:

- server
- port

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > OSS Endpoints**.
2. In the OSS Endpoints window, select the OSS server you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit OSS Endpoint dialog box, make your changes.
5. When finished, click **Apply**.

Deleting an OSS endpoint

About this task

Use this procedure to delete an OSS endpoint.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > OSS Endpoints**.
2. In the OSS Endpoints window, select the OSS endpoint you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Refreshing an OSS endpoint

About this task

Use this procedure to refresh an OSS endpoint.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > OSS Endpoints**.

2. In the OSS Endpoints window, select the OSS endpoint you want to refresh.
3. Click **Refresh**.

Managing FTP Push Destinations

Adding an FTP push destination

About this task

Use this procedure to add an FTP push destination.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > FTP Push Destinations**.
2. In the FTP Push Destinations window, click **Add (+)**.
3. In the Add FTP Push Destination dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Modifying an FTP push destination

About this task

Use this procedure to modify an FTP push destination.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > FTP Push Destinations**.
2. In the FTP Push Destinations window, select the FTP push destination you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit FTP Push Destination dialog box, make your changes.
5. When finished, click **Apply**.

Deleting an FTP push destination

About this task

Use this procedure to delete an FTP push destination.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > FTP Push Destinations**.
2. In the FTP Push Destinations window, select the FTP push destination you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Refreshing an FTP push destination

About this task

Use this procedure to refresh an FTP push destination.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > FTP Push Destinations**.
2. In the FTP Push Destinations window, select the FTP push destination you want to refresh.
3. Click **Refresh**.

Managing Log Filters

Adding a log filter

About this task

Use this procedure to add a log filter.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > Log Filters**.
2. In the Log Filters window, click **Add (+)**.
3. In the Add Log Filter dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Modifying a log filter

About this task

Use this procedure to modify a log filter.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > Log Filters**.
2. In the Log Filters window, select the log filter you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Log Filter dialog box, make your changes.
5. When finished, click **Apply**.

Deleting a log filter

About this task

Use this procedure to delete a log filter.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > Log Filters**.
2. In the Log Filters window, select the log filter you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Refreshing a log filter

About this task

Use this procedure to refresh a log filter.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > Log Filters**.
2. In the Log Filters window, select the log filter you want to refresh.
3. Click **Refresh**.

Managing Log Browser Feeds

Modifying a log browser feed

About this task

Use this procedure to modify a log browser feed.

You can have only one log browser feed.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > Log Browser Feeds**.
2. In the Log Browser Feeds window, select the log browser feed.
3. Click **Edit (-/+)**.
4. In the Edit Log Browser Feed Configuration dialog box, make your changes.
5. When finished, click **Apply**.

Refreshing the log browser feed

About this task

Use this procedure to refresh the log browser feed.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > Log Browser Feeds**.
2. In the Log Browser Feeds window, select the log browser feed.
3. Click **Refresh**.

Managing SNMP Managers

Adding an SNMP manager

About this task

Use this procedure to add an SNMP manager.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > SNMP Managers**.
2. In the SNMP Managers window, click **Add (+)**.
3. In the Add SNMP Manager dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Modifying an SNMP manager

About this task

Use this procedure to modify an SNMP manager.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > SNMP Managers**.
2. In the SNMP Managers window, select the SNMP manager you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit SNMP Manager dialog box, make your changes.
5. When finished, click **Apply**.

Deleting an SNMP manager

About this task

Use this procedure to delete an SNMP manager.

Procedure

1. In the navigation pane of Element Manager Console, select **OAM Profiles > SNMP Managers**.
2. In the SNMP Managers window, select the SNMP manager you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Chapter 18: Security

Configuring Cipher Suites

Configuring OAMP channel cipher suites

About this task

Use this procedure to configure OAMP channel cipher suites.

Procedure

1. In the navigation pane of Element Manager Console, select **Security > Cipher Suites > OAMP Channel Cipher Suites**.
2. In the OAMP Channel Cipher Suites dialog box, select the setting you want to enable/disable.
3. Do one of the following:
   - If you want to enable the selected setting, click **Enable**.
   - If you want to disable the selected setting, click **Disable**.
4. Repeat steps 2 and 3 for each setting you want to enable/disable.
5. When finished, click **Apply**.

Configuring external OAMP cipher suites

About this task

Use this procedure to configure external OAMP cipher suites.

Procedure

1. In the navigation pane of Element Manager Console, select **Security > Cipher Suites > External OAMP Cipher Suites**.
2. In the External OAMP Cipher Suites dialog box, select the setting you want to enable/disable.

3. Do one of the following:
   - If you want to enable the selected setting, click **Enable**.
   - If you want to disable the selected setting, click **Disable**.
4. Repeat steps 2 and 3 for each setting you want to enable/disable.
5. When finished, click **Apply**.

Configuring HTTPS cipher suites

About this task

Use this procedure to configure HTTP cipher suites.

Procedure

1. In the navigation pane of Element Manager Console, select **Security > Cipher Suites > HTTPS Cipher Suites**.
2. In the HTTPS Cipher Suites dialog box, select the setting you want to enable/disable.
3. Do one of the following:
   - If you want to enable the selected setting, click **Enable**.
   - If you want to disable the selected setting, click **Disable**.
4. Repeat steps 2 and 3 for each setting you want to enable/disable.
5. When finished, click **Apply**.

Configuring signaling cipher suites

About this task

Use this procedure to configure signaling cipher suites.

Procedure

1. In the navigation pane of Element Manager Console, select **Security > Cipher Suites > Signaling Cipher Suites**.
2. In the Signaling Cipher Suites dialog box, select the setting you want to enable/disable.
3. Do one of the following:
   - If you want to enable the selected setting, click **Enable**.
   - If you want to disable the selected setting, click **Disable**.
4. Repeat steps 2 and 3 for each setting you want to enable/disable.
5. When finished, click **Apply**.

Managing Certificates

Creating a certificate for network elements

Before you begin

You must know the enrollment password.

Note:

If your Avaya Aura® Conferencing deployment is a Turnkey deployment, you must use an internal certificate authority. If your Avaya Aura® Conferencing deployment is an Avaya Aura® deployment, you must use the System Manager certificate authority.

About this task

Use this procedure to create trusted certificates and generate private keys for all of your network elements that are managed directly from the certificate authority, such as provisioning manager, element manager, media server, and the application server.

Procedure

1. In the navigation pane of Element Manager Console, select **Security > Certificate Management > Enrollment Request**.
2. In the Certificate Enrollment dialog box, complete the following fields:
   - Logical Name: Type a logical name for the certificate to be assigned to a specific managed network element, for example, the provisioning manager network element.
   - Certificate Authority: If you have an Avaya Aura® deployment, select System Manager. If you have a Turnkey deployment, select the internal certificate authority.
   - Bit length: Select 1024, 2048, or 4096 from the list. Determine the bit length by the security policy of your network
   - Common name: Type the FQDN, for example, prov2.avaya.com.
   - Enrollment password: This password must match the current enrollment password that is configured on the certificate authority.
3. Click **Submit**.
4. Repeat this procedure for the network elements that require a new certificate (for example, provisioning manager, element manager, media server, and the application server network elements that are not required to be in the DMZ).

Managing Keystore Certificates

Viewing a certificate in the keystore

Comments? infodev@avaya.com

About this task

Use this procedure to view a certificate in the keystore.

Procedure

1. In the navigation pane of Element Manager Console, select **Security > Certificate Management > Keystore**.
2. In the Keystore window, select the certificate you want to view.
3. Click **Edit (-/+)**.
4. When finished viewing the certificate, click **Cancel**.

Deleting a certificate from the keystore

Before you begin

The certificate must not be associated with a TLS port.

About this task

Use this procedure to remove a certificate from the keystore.

Note:

When you delete a certificate from the keystore, the private key is also deleted.

Procedure

1. In the navigation pane of Element Manager Console, select **Security > Certificate Management > Keystore**.
2. In the Keystore window, select the certificate you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Managing Truststore Certificates

Viewing a certificate in the truststore

About this task

Use this procedure to view a certificate in the truststore.

Procedure

1. In the navigation pane of Element Manager Console, select **Security > Certificate Management > Truststore**.
2. In the Truststore window, select the certificate you want to view.
3. Click **Edit (-/+)**.
4. When finished viewing the certificate, click **Cancel**.

Deleting a certificate from the truststore

About this task

Use this procedure to remove a CA root or intermediate certificate from the truststore.

Warning:

Use extreme caution when you perform this procedure. The removal of a trusted CA can disrupt service.

Procedure

1. In the navigation pane of Element Manager Console, select **Security > Certificate Management > Truststore**.
2. In the Truststore window, select the certificate you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Managing Certificate Revocation Lists

Adding a certificate revocation list

About this task

Use this procedure to add a certificate revocation list.

Procedure

1. In the navigation pane of Element Manager Console, select **Security > Certificate Management > Certificate Revocation List**.
2. In the Certificate Revocation List window, click **Add (+)**.
3. In the Select CRL File dialog box, select the appropriate certificate revocation list file.
4. Click **Open**.

Viewing a certificate revocation list

About this task

Use this procedure to view a certificate revocation list.

Procedure

1. In the navigation pane of Element Manager Console, select **Security > Certificate Management > Certificate Revocation List**.
2. In the Certificate Revocation List window, select the certificate revocation list you want to view.
3. Click **Edit (-/+)**.

4. When finished viewing the certificate revocation list, click **Cancel**.

Deleting a certificate revocation list

About this task

Use this procedure to delete a certificate revocation list.

Procedure

1. In the navigation pane of Element Manager Console, select **Security > Certificate Management > Certificate Revocation List**.
2. In the Certificate Revocation List window, select the certificate revocation list you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Modifying the SRTP settings

About this task

Use this procedure to modify the SRTP settings for audio and video.

Procedure

1. In the navigation pane of Element Manager Console, select **Security > SRTP Settings**.
2. In the SRTP Settings dialog box, make your changes. For more information, see SRTP Settings dialog box field descriptions on page 166.
3. When finished, click **Apply**.

Related Links

SRTP Settings dialog box field descriptions on page 166

SRTP Settings dialog box field descriptions

Name	Description
Security Policy	Select the type of media security policy you want to use. The security policy you specify dictates the type of media (audio and video)Avaya Aura® Conferencing will include in offer SDPs and how Avaya Aura® Conferencing generates answer SDP during SDP negotiation. Choices are: • **BEST EFFORT** When this option is selected, Avaya Aura® Conferencing will generate requests using SIPS and will offer both RTP and SRTP media using capability negotiation. If the request fails because SIPS is not supported by the endpoint,

Name	Description
	Avaya Aura® Conferencing will retry the request using SIP and RTP. Avaya Aura® Conferencing will accept and negotiate RTP-only offers, SRTP-only offers, and RTP/SRTP best effort offers. SRTP will be negotiated where allowed when a compatible SRTP crypto suite is offered. RTP will be negotiated for RTP-only offers and for RTP/SRTP best effort offers when a compatible SRTP crypto suite is not offered. • **SECURITY DISABLED** When this option is selected, Avaya Aura® Conferencing will support only RTP. Avaya Aura® Conferencing will accept and generate RTP offers/answers. Avaya Aura® Conferencing will negotiate to RTP when it receives a request that contains an SDP offer with RTP media or best-effort media. Avaya Aura® Conferencing will reject requests that contain an SDP offer with only SRTP media by replying with a 480 Temporarily Unavailable response. A local treatment will be played to the end user. • **SECURITY ENFORCED** When this option is selected, Avaya Aura® Conferencing will support only SRTP media. Avaya Aura® Conferencing will negotiate to SRTP media when it receives a request that contains an SDP offer with SRTP media or best-effort media and a compatible crypto suite. Avaya Aura® Conferencing will reject requests that contain an SDP offer with only RTP media by replying with a 480 Temporarily Unavailable response. A local treatment will be played to the end user. **Note:** The SECURITY ENFORCED option does not guarantee signaling security. To ensure full encryption, you must configure TLS for the Avaya Aura® Conferencing Application Server network element.
Encrypt RTCP	Select this check box to indicate that Avaya Aura® Conferencing supports encrypted SRTCP messages. When not selected, Avaya Aura® Conferencing indicates the preference to send and receive unencrypted SRTCP messages by including the UNENCRYPTED_SRTCP session parameter in outgoing offers. When selected, Avaya Aura® Conferencing supports sending and receiving encrypted SRTCP messages. Avaya Aura® Conferencing will not include the UNENCRYPTED_SRTCP session parameter in its offers. In either case, if the UNENCRYPTED_SRTCP session parameter is received in an offer, Avaya Aura® Conferencing will echo the UNENCRYPTED_SRTCP session parameter in its answer, and unencrypted SRTCP will be used in both directions. If the UNENCRYPTED_SRTCP session parameter is not received in an offer, Avaya Aura® Conferencing will not include the UNENCRYPTED_SRTCP session parameter in the answer and encrypted SRTCP is used in both directions.
Video Allowed For Security Enforced Calls	Select this check box if you want Avaya Aura® Conferencing to send secure audio and unsecure video while the **Security Policy** field is set to SECURITY ENFORCED.

Name	Description
	If this check box is not selected, Avaya Aura® Conferencing will disable the video port for calls with secure audio. This field only takes effect if the **Security Policy** field is set to SECURITY ENFORCED.
Enforce SIPS for Security Enforced Calls	Select this check box if you want to require incoming calls to use SIPS signaling to negotiate secure media for the call. In addition, Avaya Aura® Conferencing generated requests with SRTP-only media offers will use SIPS signaling.
Enable Video Encryption	Select this check box if you want to enable secure video for your configuration. If you do not select this check box, Avaya Aura® Conferencing does not provide secure video transmission. In other words, if you do not select this check box, Avaya Aura® Conferencing provides unencrypted video.
Mode	Select the encryption mode(s) you want to use. This is commonly referred to as the “crypto suite.“ Choices are **AES_CM_128_HMAC_SHA1_32** and **AES_CM_128_HMAC_SHA1_80**.
Priority	Select the priority for the associated mode. Choices are **0** to **9**. If you want to disable the encryption mode, select **0**. A non-zero value indicates the priority that should be applied to the crypto suite during media negotiation. **1** is the highest priority; **9** is the lowest priority.
Send Lifetime	Select this check box to indicate that Avaya Aura® Conferencing should include the Master Key Lifetime specified by the SRTP Master Key Lifetime option (below) in the key parameter of the SRTP crypto attribute during SRTP media negotiation. When not selected, the Master Key Lifetime field is not included in the key parameter of the SRTP crypto attribute during SRTP media negotiation. In this case, the default lifetime for the crypto suite is used for media negotiation.
SRTP Master Key Lifetime	Specify the maximum number of SRTP packets that will use a particular master key. Choices are **1** to **31**.
Key Derive Rate	Specify how frequently a new session key is derived from an SRTP master key. Choices are **0** to **24**.
Master Key Index Length	Specify the size of the Master Key Index/Identifier (MKI) field in the actual SRTP packets. Choices are **0** to **4**. An MKI is used to identify the master key from which the session key that authenticates the particular packet was derived. When set to **0**, Avaya Aura® Conferencing will not include an MKI value and its associated length in the key parameter of the SRTP crypto attribute during SRTP media negotiation, and an MKI field will not be included in the actual SRTP packets. When the Master Key Index Length is set to a value greater than **0**, Avaya Aura® Conferencing will include an MKI value, and its associated length in the key parameter of the SRTP crypto attribute during SRTP media negotiation and an MKI field will be included in the actual SRTP packets.

Related Links

Modifying the SRTP settings on page 166
Administering the SRTP settings for Avaya Aura Conferencing on page 333

Chapter 19: Managing Servers

Adding a server

About this task

Use this procedure to add a server.

Procedure

1. In the navigation pane of Element Manager Console, select **Servers**.
2. In the Servers window, click **Add (+)**.
3. In the Add Server dialog box, complete the fields as appropriate. For more information, see Add/Edit Server dialog box field descriptions on page 170.
4. When finished, click **Apply**.

Modifying a server

About this task

Use this procedure to modify a server.

Procedure

1. In the navigation pane of Element Manager Console, select **Servers**.
2. In the Servers window, select the server you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Server dialog box, make your changes. For more information, see Add Edit Server dialog box field descriptions on page 170.
5. When finished, click **Apply**.

Related Links

Add/Edit Server dialog box field descriptions on page 170

Add/Edit Server dialog box field descriptions

Name	Description
Short Name	This parameter is the unique name that identifies the server, for example, EMS1. You use this parameter to associate the network element application with the server.
Long Server Name	This parameter is the long name of the server, for example, EMS1Server.
Physical Site	This parameter (select from a list) specifies the location where the network elements are deployed for this server.
IPv4 Internal OAM (Default) Address	This parameter (select from a list), specifies the IPv4 address to use for traffic internal to the enclave.
IPv4 External OAM Address	This optional parameter (select from a list) specifies the IPv4 address to use for traffic external to the enclave.
IPv4 Signaling Address	This optional parameter (select from a list) specifies the IPv4 address to use for signaling traffic.
IPv4 Media Address	This optional parameter (select from a list) specifies the IPv4 address to use for bearer traffic.
Operating System	This parameter (select from a list) indicates the operating system running on the server. If the value is **windows**, memory information is not polled from the server. The system also uses this parameter to determine file paths.
Server Type	This parameter can only be set to the following value: **Other**.
SNMP Profile	This parameter (select from a list) specifies the SNMP profile the server uses. Ensure that the operating system SNMP daemon configuration matches the defined SNMP profile.

Related Links

Modifying a server on page 169

Deleting a server

About this task

Use this procedure to delete a server.

Procedure

1. In the navigation pane of Element Manager Console, select **Servers**.
2. In the Servers window, select the server you want to delete.
3. Click **Delete (-)**.

4. In the Confirmation dialog box, click **Yes**.

Configuring alarm thresholds for a server

About this task

Use this procedure to configure alarm thresholds for a server.

Procedure

1. In the navigation pane of Element Manager Console, select **Servers > <*Server name*> > Monitor**.
2. In the Server Monitor window, click **Configure Thresholds**.
3. In the Server Monitor Alarm Thresholds dialog box, select or clear the **Minor**, **Major**, and **Critical** check boxes for the CPU, RAM, Disk, and Interface sections as required.
4. Modify the threshold values for the CPU, RAM, Disk, and Interface sections as required.
5. When finished, click **OK**.

Starting the monitor service for a server

About this task

Use this procedure to start the monitor service for a server.

The monitor service reports the following critical resource information about the server:

- CPU usage
- physical memory usage
- network I/O usage
- file system disk usage

Procedure

1. In the navigation pane of Element Manager Console, select **Servers > <*Server name*> > Monitor**.
2. In the Server Monitor window, look at the bottom of the window to verify that the server monitor is not running.
3. In the Server Monitor window, click **Start Monitor**.

   The following message appears at the bottom of the window: “The server monitor is running.”

Stopping the monitor service for a server

About this task

Use this procedure to stop the monitor service for a server.

Procedure

1. In the navigation pane of Element Manager Console, select **Servers > <*Server name*> > Monitor**.
2. In the Server Monitor window, look at the bottom of the window to verify that the server monitor is running.
3. In the Server Monitor window, click **Stop Monitor**.

   The following message appears at the bottom of the window: “The server monitor is not running.”

Generating an analysis of all servers

About this task

Use this procedure to generate an analysis of all servers.

You can save the server analysis information to a file.

Procedure

1. From the Tools menu, select **Server Analysis**.
2. In the Server Analysis window, click the tab of the server in which you are interested.
3. If you want to save the information for all of the servers to a file:
   a. From the File menu in the Server Analysis window, select **Save Server Analysis**.
   b. In the Save Server Analysis dialog box, specify the location and name of the file to which you want to save the server analysis data.
   c. Click **Save**.
4. When finished, click the **X** button to close the Server Analysis window.

Chapter 20: Managing SNMP Profiles

Adding an SNMP profile

About this task

Use this procedure to add an SNMP profile.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > SNMP Profiles**.
2. In the SNMP Profiles window, click **Add (+)**.
3. In the Add Server SNMP Profiles dialog box, complete the fields as appropriate. For more information, see Add Edit Server SNMP Profiles dialog box field descriptions on page 174.
4. When finished, click **Apply**.

Next steps

To associate the SNMP profile with a server, see Associating an SNMP profile with a server on page 174.

Modifying an SNMP profile

About this task

Use this procedure to modify an SNMP profile.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > SNMP Profiles**.
2. In the SNMP Profiles window, select the SNMP profile you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Server SNMP Profiles dialog box, make your changes. For more information, see Add Edit Server SNMP Profiles dialog box field descriptions on page 174.
5. When finished, click **Apply**.

Related Links

Add/Edit Server SNMP Profiles dialog box field descriptions on page 174

Add/Edit Server SNMP Profiles dialog box field descriptions

Name	Description
Profile Name	This (text) value is a unique name to identify the profile.
SNMP Port	This (read only) value is the SNMP port.
Read Community String	This (text) value is the name of the Read Community String. Default: public.
Write Community String	This (text) value is the name of the Write Community String. Default: private.

Important:

The default values are Public and Private. To increase security, Avaya recommends that you use values other than Public and Private.

Related Links

Modifying an SNMP profile on page 173

Deleting an SNMP profile

About this task

Use this procedure to delete an SNMP profile.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > SNMP Profiles**.
2. In the SNMP Profiles window, select the SNMP profile you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Associating an SNMP profile with a server

About this task

Use this procedure to associate an SNMP profile with a server.

Procedure

1. In the navigation pane of Element Manager Console, select **Servers**.
2. In the Servers window, select the server to which you want to associate an SNMP profile.
3. Click **Edit (-/+)**.
4. In the SNMP Profile box in the Edit Server dialog box, select the SNMP profile you want to associate with the server.
5. Click **Apply**.

Chapter 21: Managing the Database

Adding a database instance

About this task

Use this procedure to add a database instance.

You can have a maximum of two instances for the database.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Database > mcpdb > Configuration**.
2. In the mcpdb Configuration window, click **Add (+)**.
3. In the Add Database Instance dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Deleting a database instance

About this task

Use this procedure to delete a database instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Database > mcpdb > Configuration**.
2. In the mcpdb Configuration window, select the database instance you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Starting the monitor service for the database

About this task

Use this procedure to start the monitor service for the database.

The monitor service reports the data replication status for the mcpdb database.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Database > mcpdb > Monitor**.
2. In the mcpdb Monitor window, select the database instance for which you want to start the monitor service.
3. Click **Monitor**.
4. In the mcpdb Database Instance Monitor window, look at the bottom of the window to verify that the database monitor is not running.
5. In the mcpdb Database Instance Monitor window, click **Start Monitor**.

   The following message appears at the bottom of the window: “The database instance monitor is running.”

Stopping the monitor service for the database

About this task

Use this procedure to stop the monitor service for the database.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Database > mcpdb > Monitor**.
2. In the mcpdb Monitor window, select the database instance for which you want to stop the monitor service.
3. Click **Monitor**.
4. In the mcpdb Database Instance Monitor window, look at the bottom of the window to verify that the database monitor is running.
5. In the mcpdb Database Instance Monitor window, click **Stop Monitor**.

   The following message appears at the bottom of the window: “The database instance monitor is not running.”

Chapter 22: Managing the Element Manager

Modifying the element manager

About this task

Use this procedure to modify the element manager.

Note:

You can have only one element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager**.
2. In the Element Manager window, select the element manager.
3. Click **Edit (-/+)**.
4. In the Edit EM dialog box, make your changes.
5. When finished, click **Apply**.

Related Links

Add/Edit Element Manager dialog box field descriptions on page 178

Add/Edit Element Manager dialog box field descriptions

Name	Description
Internal OAM area	
IPv4 Service Address	The internal OAM (default) service address used by the network element.
HTTPS Certificate	The private key and certificate pair for the Element Manager server.
EM Service FQDN	Fully Qualified Domain Name (FQDN) for the service address of the Element Manager
External OAM area	

Name	Description
IPv4 external OAM service address	The external OAM service address used by the network element.
HTTPS Certificate	The private key and certificate pair for the external OAM service address used by the network element.

Related Links

Modifying the element manager on page 178

Modifying the configuration parameters of the element manager

About this task

Use this procedure to modify the configuration parameters of the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Configuration Parameters**.
2. From the **Parm Group** drop-down list box in the Element Manager Configuration Parameters window, select the group that contains the parameter you want to modify.
3. Select the appropriate parameter, and click **Edit (-/+)**.

   For more information, see Element Manager Configuration Parameters window field descriptions on page 179.
4. From the Edit Element Manager Config Parm dialog box, make your changes, and then click **Apply**.
5. Repeat Steps 2 through 4 for each parameter you want to modify.

Related Links

Element Manager Configuration Parameters window field descriptions on page 179

Element Manager Configuration Parameters window field descriptions

Parameter group	Configuration parameter	Description
EMAdminAudit	EnableAudit	This parameter enables monitoring for Admin accounts. Range: true or false Default: false

Comments? infodev@avaya.com

Parameter group	Configuration parameter	Description
TLSAuth	EnableCRL	This parameter enables CRL retrieval for certificate revocation status. Range: true or false Default: false
	EnableOCSP	This parameter enables OCSP retrieval for certificate revocation status. Range: true or false Default: false
	EnforceTLSMutual-AuthForHTTPS	This parameter enforces TLS Mutual Authentication for HTTP interface. Range: true or false Default: false
	PermitIfNoRevocationValidateResp	This parameter permits access, if no certificate revocation validation response. Range: true or false Default: true
FQDN	FQDNAuditInterval	This parameter determines the timeout to audit FQDNs Range: 30 – 1800 seconds Default: 90 seconds
Load	LoadAuditIntervalInMinutes	This parameter specifies the time interval (in minutes) for auditing loads on the local and remote Element Manager servers. The audit queries the loads present on an Element Manager and, if indicated, removes temporary files and directories left from previous load transactions. Default value is 50 minutes. Range: 1–2147483647. Default: 50 minutes
Metrics	HistoryStorage	This parameter is a Boolean parameter. It indicates if OM History should be persisted in the database or not. Default: true
Network	LowSpeedSiteLinks	This parameter is a Boolean parameter. It indicates if long timeout for NED operations (deploy NEI) is used. The default timeout is 600 seconds and the low speed timeout is 1200 seconds. Default: false (You should be set to true for slow networks.)

Parameter group	Configuration parameter	Description
SNMP	maxTimedOutRequests	This parameter specifies the number of timed out requests after which the “SNMP Agent Communication Failure” alarm is raised. Range: 0–10 Default: 3
	useProductDefaultMIBs	This parameter is a Boolean parameter. It controls which MIBs a product uses at boot. When it is true, the ALARM-MIB is used to report alarms. When it is false, the Nortel Reliable MIBs are used. Default: true
Cross-Domain Policy	AllowAccessFromDomains	This parameter specifies the list of domains to which Avaya Aura® Conferencing (AAC) permits access to its Adobe Flash-based features. If a domain is not in this list, the clients in this domain will not be able to access features such as Web Collaboration or the document library. By default, Avaya Aura® Conferencing permits access for any domain. However, if Avaya Aura® Conferencing administrators wish to harden their system, they can limit access, by specifying certain domains and/or IP addresses, with multiple values separated by a comma.
Security	DisableMtcLogs	This parameter is a Boolean parameter. It enable/disables OMI logs for maintenance operations. Default: false
	DisableReadLogs	This parameter is a Boolean parameter. It enable/disables OMI logs for read operations. Default: true
	DisableWriteLogs	This parameter is a Boolean parameter. It enable/disables OMI logs for write operations. Default: false

Related Links

Modifying the configuration parameters of the element manager on page 179

Managing element manager instances

Adding an element manager instance

About this task

Use this procedure to add an element manager instance.

You can have a maximum of two element manager instances.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Instance**.
2. In the Element Manager Instance window, click **Add (+)**.
3. In the Add Element Manager Instance dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Modifying an element manager instance

About this task

Use this procedure to modify an element manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Instance**.
2. In the Element Manager Instance window, select the Element Manager instance you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Element Manager Instance dialog box, make your changes. To change the Eng Parms, click **Advanced**.
5. When finished, click **Apply**.

Deleting an element manager instance

About this task

Use this procedure to delete an element manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Instance**.
2. In the Element Manager Instance window, select the element manager instance you want to delete.
3. Click **Delete (-)**.

4. In the Confirmation dialog box, click **Yes**.

Deploying an element manager instance

About this task

Use this procedure to deploy an element manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > NE Maintenance**.
2. In the Element Manager Maintenance dialog box, select the instance you want to deploy.
3. Click **Deploy**.

Undeploying an element manager instance

About this task

Use this procedure to undeploy an element manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > NE Maintenance**.
2. In the Element Manager Maintenance dialog box, select the instance you want to undeploy.
3. Click **Undeploy**.

Starting an element manager instance

About this task

Use this procedure to start an element manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > NE Maintenance**.
2. In the Element Manager Maintenance dialog box, select the instance you want to start.
3. Click **Start**.

Stopping an element manager instance

About this task

Use this procedure to stop an element manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > NE Maintenance**.
2. In the Element Manager Maintenance dialog box, select the instance you want to stop.
3. Click **Stop**.

Restarting an element manager instance

About this task

Use this procedure to restart an element manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > NE Maintenance**.
2. In the Element Manager Maintenance dialog box, select the instance you want to restart.
3. Click **Restart**.

Killing an element manager instance

About this task

Use this procedure to kill an element manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > NE Maintenance**.
2. In the Element Manager Maintenance dialog box, select the instance you want to kill.
3. Click **Kill**.

Viewing the details for an element manager instance

About this task

Use this procedure to view the details for an element manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > NE Maintenance**.
2. In the Element Manager Maintenance dialog box, select the instance for which you want to view the details.
3. Click **Details**.

Managing SNMP Managers for the element manager

Adding an SNMP Manager for the element manager

About this task

Use this procedure to add an SNMP manager for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Alarm Processing > SNMP Managers**.
2. In the Element Manager SNMP Managers window, click **Add (+)**.
3. In the Add Element Manager SNMP Manager Stream dialog box, select the appropriate SNMP manager.
4. When finished, click **Apply**.

Modifying an SNMP Manager for the element manager

About this task

Use this procedure to modify an SNMP manager for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Alarm Processing > SNMP Managers**.
2. In the Element Manager SNMP Managers window, select the SNMP manager that you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Element Manager SNMP Manager Stream dialog box, make your changes.
5. When finished, click **Apply**.

Deleting an SNMP Manager for the element manager

About this task

Use this procedure to delete an SNMP manager for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Alarm Processing > SNMP Managers**.
2. In the Element Manager SNMP Managers window, select the SNMP manager that you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Managing log processing rules for the element manager

Enabling a log rule for the element manager

About this task

Use this procedure to enable a log rule for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Log Processing > Log Rules Maintenance**.
2. In the Element Manager Log Processing Rules Maintenance window, click the tab that contains the log rule you want to enable. For more information, see Element Manager Log Processing Rules Maintenance window field descriptions on page 187.
3. Select the log rule you want to enable.
4. Click **Enable**.

Disabling a log rule for the element manager

About this task

Use this procedure to disable a log rule for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Log Processing > Log Rules Maintenance**.
2. In the Element Manager Log Processing Rules Maintenance window, click the tab that contains the log rule you want to disable. For more information, see Element Manager Log Processing Rules Maintenance window field descriptions on page 187.
3. Select the log rule you want to disable.
4. Click **Disable**.

Related Links

Element Manager Log Processing Rules Maintenance window field descriptions on page 187

Element Manager Log Processing Rules Maintenance window field descriptions

Name	Description
Name	This column contains the unique names of the processing rules.
Log Format	This column contains the names of the log formats associated with the processing rules.
Log Filter	This column contains the names of the log filters associated with the processing rules.
Admin	This column contains the administrative states of the rules. The value is either ENABLED or DISABLED.

Related Links

Disabling a log rule for the element manager on page 186

Managing log storage rules for the element manager

Adding a log storage rule for the element manager

About this task

Use this procedure to add a log storage rule for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Log Processing > Log Storage Rules**.
2. In the Element Manager Log Storage Rules window, click **Add (+)**.
3. In the Add Log Storage Rule dialog box, complete the fields as appropriate. For more information, see Add Edit Log Storage Rule dialog box field descriptions on page 188.
4. When finished, click **Apply**.

Modifying a log storage rule for the element manager

About this task

Use this procedure to modify a log storage rule for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Log Processing > Log Storage Rules**.
2. In the Element Manager Log Storage Rules window, select the log storage rule you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Log Storage Rule dialog box, make your changes. For more information, see Add Edit Log Storage Rule dialog box field descriptions on page 188.
5. When finished, click **Apply**.

Related Links

Add/Edit Log Storage Rule dialog box field descriptions on page 188

Add/Edit Log Storage Rule dialog box field descriptions

Name	Description
Name	A unique name that represents a log storage rule under the context of the Element Manager.
Log Format	This parameter (select from the list) specifies the format of logs under this rule. The supported formats are: MCP, STD, SCC2, STDEcore, SCC2Ecore, and ACL.
Log Filter	This parameter (select from the list of configured log filters) determines the particular set of logs stored by this rule.
Working Directory	This (read-only) parameter shows the working directory path for the storage of log files —based on the current configuration of the log storage rule.
Rotation Size Enabled	This parameter (check box) enables or disables rotation of log files by file size. Select the check box to enable rotation of log files by file size.
Rotation Size	This parameter specifies the file size for rotation in megabytes—available only if the Rotation Size Enable check box is selected.
Rotation Period Enabled	This parameter (check box) enables or disables rotation of log files by time period. Select the check box to enable rotation of log files by time period.
Rotation Period	This parameter specifies the number of minutes for rotation—available only if the Rotation Period Enable check box is selected.
Retention	This parameter (select from the list) specifies the number of days for which the system retains log files. The options are 1–7 days.
Secure	This parameter (check box) specifies the root directory path for log files storage. Selected—the path is: /var/mcp/oss/seclog Cleared—the path is: /var/mcp/oss/log
Compression	This parameter (check box) enables or disables compression of log files. Select the check box to enable compression of log files.

Related Links

Modifying a log storage rule for the element manager on page 188

Deleting a log storage rule for the element manager

About this task

Use this procedure to delete a log storage rule for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Log Processing > Log Storage Rules**.
2. In the Element Manager Log Storage Rules window, select the log storage rule you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Managing log north bound server feed rules for the element manager

Adding a log north bound server feed rule for the element manager

About this task

Use this procedure to add a log north bound server feed rule for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Log Processing > Log North Bound Server Feed Rules**.
2. In the Element Manager Log North Bound Server Feed Rules window, click the **Add (+)** button.
3. In the Add Log North Bound Server Feed Rule dialog box, complete the fields as appropriate. For more information, see Add Edit Log North Bound Server Feed Rule dialog box field descriptions on page 190.
4. When finished, click **Apply**.

Modifying a log north bound server feed rule for the element manager

About this task

Use this procedure to modify a log north bound server feed rule for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Log Processing > Log North Bound Server Feed Rules**.
2. In the Element Manager Log North Bound Server Feed Rules window, select the log north bound server feed rule you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Log North Bound Server Feed Rule dialog box, make your changes. For more information, see Add Edit Log North Bound Server Feed Rule dialog box field descriptions on page 190.
5. When finished, click **Apply**.

Related Links

Add/Edit Log North Bound Server Feed Rule dialog box field descriptions on page 190

Add/Edit Log North Bound Server Feed Rule dialog box field descriptions

Parameter	Description
Name	The unique name that represents a log North Bound Server Feed rule under the context of the Element Manager.
Log Format	This parameter (select from the list) specifies the format of logs under this rule. The supported formats are: MCP, STD, SCC2, STDEcore, SCC2Ecore, and ACL.
Log Filter	This parameter (select from the list of configured log filters) determines the particular set of logs stored by this rule.
Local Port	This (text) parameter specifies the TCP listening port in the EM for log forwarding to OSS servers.
ACL Validation	This parameter (check box) enables or disables access control list validation of OSS servers for log forwarding.
Available OSS Servers	This parameter lists the available OSS servers for log forwarding.
OSS Servers	This parameter specifies the authorized OSS servers for log forwarding.

Related Links

Modifying a log north bound server feed rule for the element manager on page 189

Deleting a log north bound server feed rule for the element manager

About this task

Use this procedure to delete a log north bound server feed rule for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Log Processing > Log North Bound Server Feed Rules**.

2. In the Element Manager Log North Bound Server Feed Rules window, select the log north bound server feed rule you want to delete.
3. Click **Delete (-)**.
4. Click **Yes**.

Managing log UDP client feed rules

Adding a log UDP client feed rule for the element manager

About this task

Use this procedure to add a log UDP client feed rule for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Log Processing > Log UDP Client Feed Rules**.
2. In the Element Manager Log UDP Client Feed Rules window, click **Add (+**.
3. In the Add Log UDP Client Feed Rule dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Modifying a log UDP client feed rule for the element manager

About this task

Use this procedure to modify a log UDP client feed rule for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Log Processing > Log UDP Client Feed Rules**.
2. In the Element Manager Log UDP Client Feed Rules window, select the log UDP client feed rule you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Log UDP Client Feed Rule dialog box, make your changes.
5. When finished, click **Apply**.

Deleting a log UDP client feed rule for the element manager

About this task

Use this procedure to delete a log UDP client feed rule for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Log Processing > Log UDP Client Feed Rules**.

2. In the Element Manager Log UDP Client Feed Rules window, select the log UDP client feed rule you want to delete.
3. Click **Delete (-)**.
4. Click **Yes**.

Managing log FTP push rules for the element manager

Adding a log FTP push rule for the element manager

About this task

Use this procedure to add a log FTP push rule for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Log Processing > Log FTP Push Rules**.
2. In the Element Manager Log FTP Push Rules window, click **Add (+)**.
3. In the Add Log FTP Push Rule dialog box, complete the fields as appropriate. For more information, see Add Edit FTP Push Rule dialog box field descriptions on page 193.
4. When finished, click **Apply**.

Modifying a log FTP push rule for the element manager

About this task

Use this procedure to modify a log FTP push rule for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Log Processing > Log FTP Push Rules**.
2. In the Element Manager Log FTP Push Rules window, select the log FTP push rule that you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Log FTP Push Rule dialog box, make your changes. For more information, see Add Edit FTP Push Rule dialog box field descriptions on page 193.
5. When finished, click **Apply**.

Related Links

Add/Edit FTP Push Rule dialog box field descriptions on page 193

Add/Edit FTP Push Rule dialog box field descriptions

Name	Definition
Name	This parameter (text) is a unique name to represent a log FTP Push rule under the context of the Element Manager.
Log Storage Rule	This parameter (select from the list) specifies a configured log storage rule and determines the source of log files to FTP push under this rule.
FTP Destination	This parameter (select from the list) specifies a configured Log FTP Push destination configured at the network level and provides the particular destination directory and access information required to perform the FTP push by this rule.

Related Links

Modifying a log FTP push rule for the element manager on page 192

Deleting a log FTP push rule for the element manager

About this task

Use this procedure to delete a log FTP push rule for the element manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Element Manager > Element Manager > Log Processing > Log FTP Push Rules**.
2. In the Element Manager Log FTP Push Rules window, select the log FTP push rule that you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Chapter 23: Managing Accounting Managers

Adding an accounting manager

About this task

Use this procedure to add an accounting manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers**.
2. In the Accounting Managers window, click **Add (+)**.
3. In the Add Accounting Manager dialog box, complete the fields as appropriate. For more information, see Add Edit Accounting Manager dialog box field descriptions on page 195.
4. When finished, click **Apply**.

Next steps

When you add a new network element, it is likely that you are also changing IP addresses and reconfiguring the NTP, DNS, and Syslog server. If you are making so many changes in your Avaya Aura® Conferencing system, you should always check if the Access Control List (ACL) is applied to the network element. The ACL manages the rules for internal and external system connections. If the ACL is applied to the network element, you should apply it to the new network element. For instructions on checking if it is applied and then applying it, see *Deploying Avaya Aura® Conferencing*, which is available from https://support.avaya.com/. The *Deploying Avaya Aura® Conferencing* guide also describes how to change IP addresses, reconfigure servers, and so on.

Modifying an accounting manager

About this task

Use this procedure to modify an accounting manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers**.

2. In the Accounting Managers window, select the accounting manager you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Accounting Manager dialog box, make your changes. For more information, see Add Edit Accounting Manager dialog box field descriptions on page 195.
5. When finished, click **Apply**.

Related Links

Add/Edit Accounting Manager dialog box field descriptions on page 195

Add/Edit Accounting Manager dialog box field descriptions

Parameter	Description
Short Name	(Read-only) The short name of the network element. Maximum of 6 characters.
Long Name	The long name of the network element. Maximum of 32 characters.
Base Port	A range of 100 ports reserved off the base port for use by the network element. Range: 1100-654000.
FPM	Displays **ElementManager**.
IPv4 internal OAM Service Address	The internal OAM (default) service address used by the network element.
IPv4 external OAM Service Address	The external OAM service address used by the network element.

Related Links

Modifying an accounting manager on page 194

Deleting an accounting manager

About this task

Use this procedure to delete an accounting manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers**.
2. In the Accounting Managers window, select the accounting manager you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Managing accounting manager instances

Adding an accounting manager instance

About this task

Use this procedure to add an accounting manager instance.

You can have a maximum of two instances for an accounting manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > Instance**.
2. In the Accounting Manager Instance window, click **Add (+)**.
3. In the Add Accounting Manager Instance dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Modifying an accounting manager instance

About this task

Use this procedure to modify an accounting manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > Instance**.
2. In the Accounting Manager Instance window, select the Accounting Manager instance you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Accounting Manager Instance dialog box, make your changes. To change the Eng Parms, click **Advanced**.
5. When finished, click **Apply**.

Deleting an accounting manager instance

About this task

Use this procedure to delete an accounting manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > Instance**.
2. In the Accounting Manager Instance window, select the accounting manager instance you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Starting an accounting manager instance

About this task

Use this procedure to start an accounting manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > NE Maintenance**.
2. In the Accounting Manager Maintenance dialog box, select the instance you want to start.
3. Click **Start**.

Stopping an accounting manager instance

About this task

Use this procedure to stop an accounting manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > NE Maintenance**.
2. In the Accounting Manager Maintenance dialog box, select the instance you want to stop.
3. Click **Stop**.

Restarting an accounting manager instance

About this task

Use this procedure to restart an accounting manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > NE Maintenance**.
2. In the Accounting Manager Maintenance dialog box, select the instance you want to restart.
3. Click **Restart**.

Deploying an accounting manager instance

About this task

Use this procedure to deploy an accounting manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > NE Maintenance**.
2. In the Accounting Manager Maintenance dialog box, select the instance you want to deploy.
3. Click **Deploy**.

Undeploying an accounting manager instance

About this task

Use this procedure to undeploy an accounting manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > NE Maintenance**.
2. In the Accounting Manager Maintenance dialog box, select the instance you want to undeploy.
3. Click **Undeploy**.

Killing an accounting manager instance

About this task

Use this procedure to kill an accounting manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > NE Maintenance**.

2. In the Accounting Manager Maintenance dialog box, select the instance you want to kill.
3. Click **Kill**.

Viewing the details for an accounting manager instance

About this task

Use this procedure to view the details for an accounting manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > NE Maintenance**.
2. In the Accounting Manager Maintenance dialog box, select the instance for which you want to view the details.
3. Click **Details**.

Managing accounting rules for an accounting manager

Enabling an accounting rule for an accounting manager

About this task

Use this procedure to enable an accounting rule for an accounting manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > RU Processing > Accounting Rules Maintenance**.
2. In the Accounting Manager Accounting Processing Rules Maintenance window, click the tab that contains the accounting rule you want to enable. For more information, see Accounting Manager Accounting Processing Rules Maintenance window field descriptions on page 200.
3. Select the accounting rule you want to enable.
4. Click **Enable**.

Disabling an accounting rule for an accounting manager

About this task

Use this procedure to disable an accounting rule for an accounting manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > RU Processing > Accounting Rules Maintenance**.
2. In the Accounting Manager Accounting Processing Rules Maintenance window, click the tab that contains the accounting rule you want to disable. For more information, see Accounting Manager Accounting Processing Rules Maintenance window field descriptions on page 200.
3. Select the accounting rule you want to disable.
4. Click **Disable**.

Related Links

Accounting Manager Accounting Processing Rules Maintenance window field descriptions on page 200

Accounting Manager Accounting Processing Rules Maintenance window field descriptions

Column name	Description
Name	This column contains the unique names of the processing rules.
Accounting Format	This column contains the names of the accounting formats associated with the processing rules (MCPV3 or MCPV4).
Admin State	This column contains the administrative states of the rules. The value is either ENABLED or DISABLED.

Related Links

Disabling an accounting rule for an accounting manager on page 199

Managing storage rules for an accounting manager

Adding an accounting storage rule for an accounting manager

About this task

Use this procedure to add an accounting storage rule for an accounting manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > RU Processing > Accounting Storage Rules**.
2. In the Accounting Manager Accounting Storage Rules window, click **Add (+)**.

3. In the Add Accounting Storage Rule dialog box, complete the fields as appropriate. For more information, see Add Edit Accounting Storage Rules dialog box field descriptions on page 201.
4. When finished, click **Apply**.

Modifying an accounting storage rule for an accounting manager

About this task

Use this procedure to modify an accounting storage rule for an accounting manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > RU Processing > Accounting Storage Rules**.
2. In the Accounting Manager Accounting Storage Rules window, select the accounting storage rule you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Accounting Storage Rule dialog box, make your changes. For more information, see Add Edit Accounting Storage Rules dialog box field descriptions on page 201.
5. When finished, click **Apply**.

Related Links

Add/Edit Accounting Storage Rules dialog box field descriptions on page 201

Add/Edit Accounting Storage Rules dialog box field descriptions

Name	Definition
Name	This parameter is the unique name that represents an accounting storage rule under the context of an Accounting Manager.
Accounting Format	This parameter (select from the list) specifies the format of accounting records under this rule. The supported formats are: MCPV3 and MCPV4.
Working Directory	This (read-only) parameter shows the working directory path for the storage of accounting files—based on the current configuration of the log storage rule.
Rotation Size Enabled	This parameter (check box) enables or disables rotation of accounting files by file size. Select the check box to enable rotation of accounting files by file size.
Rotation Size	This (text) value specifies the file size for rotation in megabytes—available only if the Rotation Size Enabled check box is selected.
Rotation Period Enabled	This parameter (check box) enables or disables rotation of accounting files by time period. Select the check box to enable rotation of accounting files by time period.

Name	Definition
Rotation Period	This parameter specifies the number of minutes for rotation—available only if the Rotation Period Enabled check box is selected.
Retention	This parameter (select from the list) specifies the number of days for which the system retains accounting files. The options are 1–7 days.
Compression	This parameter (check box) enables or disables compression of log files. Select the check box to enable compression of accounting files.

Related Links

Modifying an accounting storage rule for an accounting manager on page 201

Deleting an accounting storage rule for an accounting manager

About this task

Use this procedure to delete an accounting storage rule for an accounting manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > RU Processing > Accounting Storage Rules**.
2. In the Accounting Manager Accounting Storage Rules window, select the accounting storage rule you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Managing north bound server feed rules for an accounting manager

Adding an accounting north bound server feed rule for an accounting manager

About this task

Use this procedure to add an accounting north bound server feed rule for an accounting manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > RU Processing > Accounting North Bound Server Feed Rules**.
2. In the Accounting Manager Accounting North Bound Server Feed Rules window, click **Add (+)**.

3. In the Add Accounting North Bound Server Feed Rule dialog box, complete the fields as appropriate. For more information, see Add Edit Accounting North Bound Server Feed Rule dialog box field descriptions on page 203.
4. When finished, click **Apply**.

Modifying an accounting north bound server feed rule for an accounting manager

About this task

Use this procedure to modify an accounting north bound server feed rule for an accounting manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > RU Processing > Accounting North Bound Server Feed Rules**.
2. In the Accounting Manager Accounting North Bound Server Feed Rules window, click **Edit (-/+)**.
3. In the Edit Accounting North Bound Server Feed Rule dialog box, make your changes. For more information, see Add Edit Accounting North Bound Server Feed Rule dialog box field descriptions on page 203.
4. When finished, click **Apply**.

Related Links

Add/Edit Accounting North Bound Server Feed Rule dialog box field descriptions on page 203

Add/Edit Accounting North Bound Server Feed Rule dialog box field descriptions

Parameter	Description
Name	This parameter is the unique name that represents an accounting North Bound Server Feed rule under the context of an Accounting Manager.
Accounting Format	This parameter (select from the list) specifies the format of accounting records under this rule. The supported formats are: MCPV3 and MCPV4.
Local Port	This (text) parameter specifies the TCP listening port in the AM for forwarding to OSS servers.
ACL Validation	This parameter (check box) enables or disables access control list validation of OSS servers for forwarding accounting files.
Available OSS Servers	This parameter lists the available OSS servers for forwarding accounting files.
OSS Servers	This parameter specifies the authorized OSS servers for forwarding accounting files.

Related Links

Modifying an accounting north bound server feed rule for an accounting manager on page 203

Deleting an accounting north bound server feed rule for an accounting manager

About this task

Use this procedure to delete an accounting north bound server feed rule for an accounting manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > RU Processing > Accounting North Bound Server Feed Rules**.
2. In the Accounting Manager Accounting North Bound Server Feed Rules window, select the accounting north bound server feed rule you want to delete.
3. Click **Delete (-)**.
4. Click **Yes**.

Managing FTP push rules for an accounting manager

Adding an accounting FTP push rule for an accounting manager

About this task

Use this procedure to add an accounting FTP push rule for an accounting manager.

Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane of Element Manager Console, select **Addresses**.
3. In the Addresses window, click **Add (+)** .
4. In the Add IPv4 Address dialog box, complete the following fields:
   - **Logical Name**: Type the logical name of the FTP server.
   - **IPv4 Address**: Type the IP address for the FTP server.
5. Click **Apply**.
6. In the navigation pane, click **External Nodes**.
7. In the External Nodes window, click **Add (+)** .
8. In the Add External Node dialog box, complete the following fields:
   - **Name**: Type a logical name for the FTP server node.
   - **IPv4 Address**: Select the address added for the FTP server node.
9. Click **Apply**.
10. In the navigation pane, click **OAM Profiles** > **OSS Servers**.

11. In the OSS Servers window, click **Add (+)** .
12. In the Add OSS Server dialog box, complete the following fields:
    - **Name**: Type a logical name for the FTP OSS server.
    - **Node**: Select the node added for the FTP OSS server.
    - **Use External OAM Network**: Check this option only if you are using an external OAM Network.
13. Click **Apply**.
14. In the navigation pane, click **OAM Profiles** > **OSS Endpoints**.
15. In the OSS Endpoints window, click **Add (+)** .
16. In the Add OSS Endpoint dialog box, complete the following fields:
    - **Name**: Type a logical name for the FTP OSS endpoint.
    - **Server**: Select the node added for the FTP OSS endpoint.
    - **Port**: Type the FTP port to be used (for example: 21).
17. Click **Apply**.
18. In the navigation pane, click **OAM Profiles** > **FTP Push Destinations**.
19. In the FTP Push Destinations window, click **Add (+)** .
20. In the Add FTP Push Destination dialog box, complete the following fields:
    - **Name**: Type a logical name for the FTP push destination server.
    - **OSS Endpoint**: Select the OSS Endpoint added for the FTP push destination server.
    - **Root Directory**: Type a root address on the FTP server for file storage.

    Note:

    The User ID below must have write privileges for this directory. As an example: "./" could be entered to use the home directory of user on a Linux server.

    - **User ID**: Type the user ID to be used in the FTP sessions.
    - **Password**: Type the password to be used in the FTP sessions.
    - **Confirm Password**: Re-type the password to be used in the FTP sessions.
    - **Replicate**: Do not select this option.
21. Click **Apply**.
22. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > RU Processing > Accounting FTP Push Rules**.
23. In the Accounting Manager Accounting FTP Push Rules window, click **Add (+)**.
24. In the Add Accounting FTP Push Rule dialog box, complete the fields as appropriate. For more information, see Add Edit Accounting FTP Push Rule dialog box field descriptions on page 206.

25. When finished, click **Apply**.
26. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Accounting Managers** > **<*Accounting Managername*>** > **RU Processing** and perform the following actions:
    - **FTP Push**: Select the FTP Push tab at the top of the Accounting.
    - **Name**: Select the Accounting FTP Rules added above.
    - **Enable**: Click the **Enable** button to enable the rules.

Modifying an accounting FTP push rule for an accounting manager

About this task

Use this procedure to modify an accounting FTP push rule for an accounting manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > RU Processing > Accounting FTP Push Rules**.
2. In the Accounting Manager Accounting FTP Push Rules window, select the accounting FTP push rule that you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Accounting FTP Push Rule dialog box, make your changes. For more information, see Add Edit Accounting FTP Push Rule dialog box field descriptions on page 206.
5. When finished, click **Apply**.

Related Links

Add/Edit Accounting FTP Push Rule dialog box field descriptions on page 206

Add/Edit Accounting FTP Push Rule dialog box field descriptions

Name	Definition
Name	This parameter (text) is a unique name to represent an Accounting FTP Push rule under the context of an Accounting Manager.
Accounting Storage Rule	This parameter (select from the list) specifies a configured accounting storage rule and determines the source of accounting files to FTP Push under this rule.
FTP Push Destination	This parameter (select from the list) specifies a configured Accounting FTP Push destination configured at the network level and provides the particular destination directory and access information required to perform the FTP push by this rule.

Related Links

Modifying an accounting FTP push rule for an accounting manager on page 206

Deleting an accounting FTP push rule for an accounting manager

About this task

Use this procedure to delete an accounting FTP push rule for an accounting manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Accounting Managers > <*Accounting Manager name*> > RU Processing > Accounting FTP Push Rules**.
2. In the Accounting Manager Accounting FTP Push Rules window, select the accounting FTP push rule that you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Chapter 24: Managing Provisioning Managers

Adding a provisioning manager

About this task

Use this procedure to add a provisioning manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers**.
2. In the Provisioning Managers window, click **Add (+)**.
3. In the Add Provisioning Client Manager dialog box, complete the fields as appropriate. For more information, see Add Edit Provisioning Manager dialog box field descriptions on page 209.
4. When finished, click **Apply**.

Next steps

When you add a new network element, it is likely that you are also changing IP addresses and reconfiguring the NTP, DNS, and Syslog server. If you are making so many changes in your Avaya Aura® Conferencing system, you should always check if the Access Control List (ACL) is applied to the network element. The ACL manages the rules for internal and external system connections. If the ACL is applied to the network element, you should apply it to the new network element. For instructions on checking if it is applied and then applying it, see *Deploying Avaya Aura® Conferencing*, which is available from https://support.avaya.com/. The *Deploying Avaya Aura® Conferencing* guide also describes how to change IP addresses, reconfigure servers, and so on.

Modifying a provisioning manager

About this task

Use this procedure to modify a provisioning manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers**.
2. In the Provisioning Managers window, select the provisioning manager you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Provisioning Client Manager dialog box, make your changes. For more information, see Add Edit Provisioning Manager dialog box field descriptions on page 209.
5. When finished, click **Apply**.

Related Links

Add/Edit Provisioning Manager dialog box field descriptions on page 209

Add/Edit Provisioning Manager dialog box field descriptions

Name	Description
Short Name	(Read-only) The short name of the NE—maximum of 6 characters.
Long Name	The long name of the NE—maximum of 32 characters.
Base Port	A range of 100 ports reserved off the base port for use by the NE. Range: 1100–654000
FPM	Displays **ElementManager**.
Prov area	
Enable HTTP Port	(Check box) Select to enable the Provisioning HTTP port.
Internal OAM HTTPS Certificate	The private key and certificate pair for the Provisioning HTTPS server.
Prov Service FQDN	FQDN for the service address of the Provisioning Manager.
External OAM HTTPS Certificate	The private key and certificate pair for the Provisioning HTTPS server (external interface).
Directory Server Certificate	The logical name of the certificate used for communication between the Provisioning Manager and the LDAP server.
CA area	
Enable HTTP Port	(Check box) Select to enable the Collaboration Agent HTTP port.
HTTPS Certificate	The private key and certificate pair that the Collaboration Agent HTTPS server uses. (Select from the list.)
CA Service FQDN	FQDN for the service address of the Collaboration Agent Manager.
Enable SIP TCP Port	(Check box) Select to enable the SIP TCP port. Default: 5060
Enable SIP TLS Port	(Check box) Select to enable the SIP TLS port. Default: 5061
SIP Certificate	The logical name of the certificate that the system uses for secure SIP communication. (Select from the list.)

Name	Description
Lock Message Profile	The logical name of the lock message profile. (Select from the list).

Related Links

Modifying a provisioning manager on page 208

Deleting a provisioning manager

About this task

Use this procedure to delete a provisioning manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers**.
2. In the Provisioning Managers window, select the provisioning manager you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Modifying the configuration parameters of a provisioning manager

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers > <*Provisioning Manager name*> > Configuration Parameters**.
2. In the Provisioning Manager Configuration Parameters window, make your changes. Use the **Parm Group** drop-down list box to access the parameter(s) you want to modify. For more information, see Provisioning Manager Configuration Parameters window field descriptions on page 211.

Related Links

Provisioning Manager Configuration Parameters window field descriptions on page 211

Provisioning Manager Configuration Parameters window field descriptions

Parameter group	Configuration parameter	Description
HTTPDoS	Enable MMS DoS filter	This parameter enables or disables the HTTP Denial of Service protection feature for the Provisioning Manager. Range: true or false Default: false
	Enable PA Manager DoS filter	This parameter enables or disables the HTTP Denial of Service protection feature for the Collaboration Agent Manager. Range: true or false Default: false
	Enable Presence DoS filter	This parameter enables or disables the HTTP Denial of Service protection feature for Presence. Range: true or false Default: false
	Enable Prov Manager DoS filter	This parameter enables or disables the HTTP Denial of Service protection feature for the Provisioning Manager. Range: true or false Default: false
	Enable SOPI DoS filter	This parameter enables or disables the HTTP Denial of Service protection feature for Subscriber Open Provisioning Interface (SOPI). Range: true or false Default: false
	Enable TPCC DoS filter	This parameter enables or disables the HTTP Denial of Service protection feature for Third Party Call Control. Range: true or false Default: false
PersonalAgent	GenerateAuditLogs	This parameter enables or disables the generation of Audit Logs for the Collaboration Agent and Subscriber Open Provisioning Interface (OPI). Range: true, false
PROVAdminAudit	EnableAudit	This parameter enables monitoring for Admin accounts.

Comments? infodev@avaya.com

Parameter group	Configuration parameter	Description
		Range: true or false Default: false
	AuditStartTime	This parameter controls the time of day at which the system audits Admin accounts. Range: 0–23 hours Default: 0
SIPDoS	Enable DoS filter	This parameter enables or disables the SIP Denial of Service protection feature for the Provisioning Manager. Range: true or false Default: false
SIPStack	DEFAULT_MAX_-BUFFER_-SIZE	This parameter determines the maximum UDP message length. Range: 0–2 147 483 647 Default: 6144
SIPRespOMThresh	Info 500	This parameter indicates how many 500 error responses can be received for SIP Refer Requests before an alarm is raised. Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15
	Invite500	This parameter indicates how many 500 error responses can be received for SIP Invite Requests before an alarm is raised. Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15
	Message500	This parameter indicates how many 500 error responses can be received for SIP Message Requests before an alarm is raised. Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15
	Notify500	This parameter indicates how many 500 error responses can be received for SIP Notify Requests before an alarm is raised. Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15

Parameter group	Configuration parameter	Description
	Option500	This parameter indicates how many 500 error responses can be received for SIP Option Requests before an alarm is raised. Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15
	Publish500	This parameter indicates how many 500 error responses can be received for SIP Publish Requests before an alarm is raised. Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15
	Refer500	This parameter indicates how many 500 error responses can be received for SIP Refer Requests before an alarm is raised. Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15
	Register500	This parameter indicates how many 500 error responses can be received for SIP Register Requests before an alarm is raised. Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15
	Subscribe500	This parameter indicates how many 500 error responses can be received for SIP Subscribe Requests before an alarm is raised. Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15
	Service500	This parameter indicates how many 500 error responses can be received for SIP Service Requests before an alarm is raised. Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15
	Update500	This parameter indicates how many 500 error responses can be received for SIP Update Requests before an alarm is raised. Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100

Parameter group	Configuration parameter	Description
		Default: 5,10,15
SipTransport	InitialMaxHops	This parameter defines the maximum number of hops before a request is dropped. Range: 5–50 Default: 20
	InviteTimer	This parameter defines the maximum time to wait for an INVITE to receive a Final Response, after receiving a provisional response, in milliseconds. Range: 120 000–3 600 000 Default: 128 000
	MaxRedirections	This parameter defines the maximum number of redirections permitted before a request is dropped. Range: 3–10 Default: 5
	MaxTermAttempt	The maximum number of internal cpl loops allowed before a request is dropped. Range: 5–50 Default: 10
TLSAuth	EnableCRL	This parameter enables CRL retrieval for certificate revocation status. Range: true or false Default: false
	EnableOCSP	This parameter enables OCSP retrieval for certificate revocation status. Range: true or false Default: false
	EnforceTLSMutual-AuthForHTTPS	This parameter enforces TLS Mutual Authentication for HTTP interface. Range: true or false Default: false
	EnforceTLSMutual-AuthForSIP	This parameter enforces TLS Mutual Authentication for SIP interface. Range: true or false Default: false
	PermitIfNoRevocationValidateResp	This parameter permits access, if no certificate revocation validation response. Range: true or false

Parameter group	Configuration parameter	Description
		Default: true
	SyncOCSPForSIP	This parameter enables synchronous OCSP query for SIP interface. Range: true or false Default: false
	Disable hostname verifier	This parameter enables or disables hostname verification check on certificate validation. Range: true or false Default: false
TLSSession	AllowTLSsessionresumption	This parameter enables or disables TLS session resumption. Range: true, false
	Enforce renegotiation	The TLS connections between clients (especially peers) can exist for long durations. The longer a session key is in use, the greater the likelihood of compromise. To mitigate this risk, TLS supports renegotiating the session key for an existing connection. Range: true or false Default: false
WebServer	EnableAccessLogs	This parameter enables Tomcat Access/Error logs. Range: true, false
LDAP	PageSize	This parameter determines number of returned records on one page. Range: 1 - 2147483647 Default: 5
FQDN	FQDNAuditInterval	This parameter determines the timeout to audit FQDNs Range: 30 – 1800 seconds Default: 90 seconds

Related Links

Modifying the configuration parameters of a provisioning manager on page 210

Managing provisioning manager instances

Adding a provisioning manager instance

About this task

Use this procedure to add a provisioning manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers > <*Provisioning Manager name*> > Instance**.
2. In the Provisioning Manager Instance window, click **Add (+)**.
3. In the Add Provisioning Manager Instance dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Modifying a provisioning manager instance

About this task

Use this procedure to modify a provisioning manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers > <*Provisioning Manager name*> > Instance**.
2. In the Provisioning Manager Instance window, select the Provisioning Manager instance you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Provisioning Manager Instance dialog box, make your changes. To change the Eng Parms, click **Advanced**.
5. When finished, click **Apply**.

Deleting a provisioning manager instance

About this task

Use this procedure to delete a provisioning manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers > <*Provisioning Manager name*> > Instance**.
2. In the Provisioning Manager Instance window, select the provisioning manager instance you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Deploying a provisioning manager instance

About this task

Use this procedure to deploy a provisioning manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers > <*Provisioning Manager name*> > NE Maintenance**.
2. In the Provisioning Manager Maintenance dialog box, select the instance you want to deploy.
3. Click **Deploy**.

Undeploying a provisioning manager instance

About this task

Use this procedure to undeploy a provisioning manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers > <*Provisioning Manager name*> > NE Maintenance**.
2. In the Provisioning Manager Maintenance dialog box, select the instance you want to undeploy.
3. Click **Undeploy**.

Starting a provisioning manager instance

About this task

Use this procedure to start a provisioning manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers > <*Provisioning Manager name*> > NE Maintenance**.
2. In the Provisioning Manager Maintenance dialog box, select the instance you want to start.
3. Click **Start**.

Stopping a provisioning manager instance

About this task

Use this procedure to stop a provisioning manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers > <*Provisioning Manager name*> > NE Maintenance**.
2. In the Provisioning Manager Maintenance dialog box, select the instance you want to stop.
3. Click **Stop**.

Restarting a provisioning manager instance

About this task

Use this procedure to restart a provisioning manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers > <*Provisioning Manager name*> > NE Maintenance**.
2. In the Provisioning Manager Maintenance dialog box, select the instance you want to restart.
3. Click **Restart**.

Killing a provisioning manager instance

About this task

Use this procedure to kill a provisioning manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers > <*Provisioning Manager name*> > NE Maintenance**.
2. In the Provisioning Manager Maintenance dialog box, select the instance you want to kill.
3. Click **Kill**.

Viewing the details for a provisioning manager instance

About this task

Use this procedure to view the details for a provisioning manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Provisioning Managers > <*Provisioning Manager name*> > NE Maintenance**.
2. In the Provisioning Manager Maintenance dialog box, select the instance for which you want to view the details.
3. Click **Details**.

Chapter 25: Managing Collaboration Agent Managers

Adding a Collaboration Agent manager

About this task

Use this procedure to add a Collaboration Agent manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Collaboration Agent Managers**.
2. In the Collaboration Agent Managers window, click **Add (+)**.
3. In the Add Collaboration Agent Manager dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Next steps

When you add a new network element, it is likely that you are also changing IP addresses and reconfiguring the NTP, DNS, and Syslog server. If you are making so many changes in your Avaya Aura® Conferencing system, you should always check if the Access Control List (ACL) is applied to the network element. The ACL manages the rules for internal and external system connections. If the ACL is applied to the network element, you should apply it to the new network element. For instructions on checking if it is applied and then applying it, see *Deploying Avaya Aura® Conferencing*, which is available from https://support.avaya.com/. The *Deploying Avaya Aura® Conferencing* guide also describes how to change IP addresses, reconfigure servers, and so on.

Related Links

Add/Edit Collaboration Agent Manager dialog box field descriptions on page 220

Add/Edit Collaboration Agent Manager dialog box field descriptions

Name	Description
Short Name	(Read-only) The short name of the NE—maximum of 6 characters.
Long Name	The long name of the NE—maximum of 32 characters.

Name	Description
Base Port	A range of 100 ports reserved off the base port for use by the NE. Range: 1100–654000
FPM	Displays **ElementManager**.
Enable HTTP Port	(Check box) Select to enable the Collaboration Agent HTTP port.
CA HTTPS Certificate	The private key and certificate pair that the Collaboration Agent HTTPS server uses. (Select from the list).
CA Service FQDN	FQDN for the service address of the Collaboration Agent Manager.
Directory Server Certificate	The logical name of the certificate used for communication between the Collaboration Agent Manager and the LDAP server.
Enable SIP TCP Port	(Check box) Select to enable the SIP TCP port. Default: 5060
Enable SIP TLS Port	(Check box) Select to enable the SIP TLS port. Default: 5061
SIP Certificate	The logical name of the certificate that the system uses for secure SIP communication. (Select from the list.)
Lock Message Profile	The logical name of the lock message profile. (Select from the list).

Related Links

Adding a Collaboration Agent manager on page 220

Modifying a Collaboration Agent manager

About this task

Use this procedure to modify a Collaboration Agent manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Collaboration Agent Managers**.
2. In the Collaboration Agent Managers window, select the Collaboration Agent manager you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Collaboration Agent Manager dialog box, make your changes.
5. When finished, click **Apply**.

Deleting a Collaboration Agent manager

About this task

Use this procedure to delete a Collaboration Agent manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Collaboration Agent Managers**.
2. In the Collaboration Agent Managers window, select the Collaboration Agent manager you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Modifying the configuration parameters of a Collaboration Agent manager

About this task

Use this procedure to modify the configuration parameters of a Collaboration Agent manager.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Collaboration Agent Managers > <*Collaboration Agent Manager name*> > Configuration Parameters**.
2. In the Collaboration Agent Manager Configuration Parameters window, make your changes. Use the **Parm Group** drop-down list box to access the parameter(s) you want to modify.

Managing Collaboration Agent Managers instances

Adding a Collaboration Agent manager instance

About this task

Use this procedure to add a Collaboration Agent manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Collaboration Agent Managers > <*Collaboration Agent Manager name*> > Instance**.
2. In the Collaboration Agent Manager Instance window, click **Add (+)**.

3. In the Add Collaboration Agent Manager Instance dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Modifying a Collaboration Agent manager instance

About this task

Use this procedure to modify a Collaboration Agent manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Collaboration Agent Managers > <*Collaboration Agent Manager name*> > Instance**.
2. In the Collaboration Agent Manager Instance window, select the Collaboration Agent manager instance you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Collaboration Agent Manager Instance dialog box, make your changes. To change the Eng Parms, click **Advanced**.
5. When finished, click **Apply**.

Deleting a Collaboration Agent manager instance

About this task

Use this procedure to delete a Collaboration Agent manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Collaboration Agent Managers > <*Collaboration Agent Manager name*> > Instance**.
2. In the Collaboration Agent Manager Instance window, select the Collaboration Agent manager instance you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Deploying a Collaboration Agent manager instance

About this task

Use this procedure to deploy a Collaboration Agent manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Collaboration Agent Managers > <*Collaboration Manager name*> > NE Maintenance**.
2. In the Collaboration Agent Manager Maintenance dialog box, select the instance you want to deploy.
3. Click **Deploy**.

Undeploying a Collaboration Agent manager instance

About this task

Use this procedure to undeploy a Collaboration Agent manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Collaboration Agent Managers > <*Collaboration Manager name*> > NE Maintenance**.
2. In the Collaboration Agent Manager Maintenance dialog box, select the instance you want to undeploy.
3. Click **Undeploy**.

Starting a Collaboration Agent manager instance

About this task

Use this procedure to start a Collaboration Agent manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Collaboration Agent Managers > <*Collaboration Manager name*> > NE Maintenance**.
2. In the Collaboration Agent Manager Maintenance dialog box, select the instance you want to start.
3. Click **Start**.

Stopping a Collaboration Agent manager instance

About this task

Use this procedure to stop a Collaboration Agent manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Collaboration Agent Managers > <*Collaboration Manager name*> > NE Maintenance**.
2. In the Collaboration Agent Manager Maintenance dialog box, select the instance you want to stop.
3. Click **Stop**.

Restarting a Collaboration Agent manager instance

About this task

Use this procedure to restart a Collaboration Agent manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Collaboration Agent Managers > <*Collaboration Manager name*> > NE Maintenance**.
2. In the Collaboration Agent Manager Maintenance dialog box, select the instance you want to restart.
3. Click **Restart**.

Killing a Collaboration Agent manager instance

About this task

Use this procedure to kill a Collaboration Agent Manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Collaboration Agent Managers > <*Collaboration Manager name*> > NE Maintenance**.
2. In the Collaboration Agent Manager Maintenance dialog box, select the instance you want to kill.
3. Click **Kill**.

Viewing the details for a Collaboration Agent manager instance

About this task

Use this procedure to view the details for a Collaboration Agent manager instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Collaboration Agent Managers > <*Collaboration Manager name*> > NE Maintenance**.
2. In the Collaboration Agent Manager Maintenance dialog box, select the instance for which you want to view the details.
3. Click **Details**.

Chapter 26: Managing Application Servers

Adding an application server

About this task

Use this procedure to add an application server

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers**.
2. In the Application Servers window, click **Add (+)**.
3. In the Add Application Server dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Next steps

When you add a new network element, it is likely that you are also changing IP addresses and reconfiguring the NTP, DNS, and Syslog server. If you are making so many changes in your Avaya Aura® Conferencing system, you should always check if the Access Control List (ACL) is applied to the network element. The ACL manages the rules for internal and external system connections. If the ACL is applied to the network element, you should apply it to the new network element. For instructions on checking if it is applied and then applying it, see *Deploying Avaya Aura® Conferencing*, which is available from https://support.avaya.com/. The *Deploying Avaya Aura® Conferencing* guide also describes how to change IP addresses, reconfigure servers, and so on.

Related Links

Add/Edit Application Server dialog box field descriptions on page 227

Add/Edit Application Server dialog box field descriptions

Name	Description
Short Name	(Read-only) The short name of the NE—maximum of 6 characters.
Long Name	The long name of the NE—maximum of 32 characters.
Base Port	A range of 100 ports reserved off the base port for use by the NE. Range: 1100–654000
FPM	Displays **ElementManager**.

Name	Description
IPv4 signalling service address	The internal OAM (default) service address used by the network element.
AM	The logical name of the Application Manager. (Select from the list).
Enable SIP TCP/SIP TCP Port	Enables the SIP TCP port and specifies the TCP Port.
Enable SIP TLS/SIP TLS Port	Enables the SIP TLS port and specifies the TLS Port.
SIP Certificate	Choose the security certificate to be used by SIP.
Directory Server Certificate	The logical name of the certificate used for communication between the Application Server and the LDAP server.

Related Links

Adding an application server on page 227

Modifying an application server

About this task

Use this procedure to modify an application server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers**.
2. In the Application Servers window, select the application server you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Application Server dialog box, make your changes.
5. When finished, click **Apply**.

Deleting an application server

About this task

Use this procedure to delete an application server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers**.
2. In the Application Servers window, select the application server you want to delete.

3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Modifying the configuration parameters of an application server

About this task

Use this procedure to modify the configuration parameters of an application server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers > <*Application Server name*> > Configuration Parameters**.
2. In the Application Server Configuration Parameters window, make your changes. Use the **Parm Group** drop-down list box to access the parameter group you want to modify. Use **Edit (+/-)** to modify the selected parameter.

   For more information, see Application Server Configuration Parameters window field descriptions on page 229.

Related Links

Application Server Configuration Parameters field descriptions on page 229

Application Server Configuration Parameters field descriptions

Parameter group	Configuration parameter	Description
Accounting	—	The accounting system provides a framework that enables the transport of accounting information from internal IMS components to the back-end billing system of a service provider. The IMS Accounting System provides: • Reliable transport of accounting information. • Persistent storage of accounting information. • Flexible and extensible formatting of accounting fields into an IPDR-like format.
	IMBillingActive	Enables and disables the capture of IM billing information. The default value is **true**.
	RegisterSuccessBilling	Accepts user registrations and stores the contact information of users to support user mobility.

Parameter group	Configuration parameter	Description
		This field creates a record for successful user registrations. The default value is **false**.
Authentication	AllowAdvancedAuthentication	Applies advanced digest authentication to enable and disable advanced authentication. The default value is **true**.
	AuthenticationWithIntegrity	The default value is **true**.
	GracePeriod	The grace period for advanced SIP authentication. The default value is **90000**.
	NCSequenceEnforcement	Enables and disables the nonce-count sequence enforcement. The default value is **false**.
	NonceUsageCount	The usage count value of a nonce used in advanced SIP authentication. The default value is **30000**.
	PrivateKey	The key used to uniquely generate authentication challenges. The default value is **MCP**.
BandwidthParms	EnableLocationSeparation	Splits a location into two locations such as Dallas and Dallas_AAC for bandwidth monitoring. The names of the two locations must be same, except for the suffix. Both the locations must be provisioned on System Manager. The default value is **false**.
	FailureConfirmationTimerDelay	The time delay, in seconds, after which Avaya Aura® Conferencing raises an alarm if a BW PUBLISH request fails. The default value is **60**.
	LocationSeparationSuffix	Specifies a string to use as the suffix. The field is used to determine the bandwidth consumption Avaya Aura® Conferencing from the total bandwidth consumption in a location. A suffix in the name of a location indicates that the location is used for the Avaya Aura® Conferencing bandwidth. Media Server must be assigned to the location names that contain a suffix such as **_AAC**.
ConfMonitoring	MaxSearchResults	Specifies the maximum number of search results for conferences and sessions in the Avaya Aura® Conferencing reports and monitoring application. The default value is **50**.

Parameter group	Configuration parameter	Description
	MonitorTimeoutSeconds	The monitor timeout, in seconds, after which Avaya Aura® Conferencing automatically aborts a monitor if the monitor is not refreshed within the timeout period. The default value is **60**.
ConferenceParms	ActiveSpeakerNotifyInterval	The minimum time delay after which Avaya Aura® Conferencing displays the active speaker notification in conferences. The range of values is 0 to 60 seconds. The default value is **4**. If you set a value of **0**, you can disable the active speaker notification in all conferences.
	CascadingActiveSpeakerTimer	The minimum time delay after which Avaya Aura® Conferencing displays the active speaker notification in cascaded conferences. The range of values is 0 to 60 seconds. The default value is **2**. If you set a value of **0**, you can disable the timer in all cascaded conferences.
	ConfEndWaitTime	Specifies the period, in minutes, that conferences remain active after the moderator disconnects. The range of values is 1 to 5. The default value is **2**.
	ConfMSReRouteHandling	Specifies the method of rerouting a participant to another Media Server. The values are **REFER**, **REINVITE**, or **PERALLOW**. Set the value to **REFER** if the signaling message contains `Allow:REFER`, otherwise set the value to **REINVITE**. The default value is **REINVITE**.
	SilenceTimeBeforeEnd	Specifies the minimum time delay, in hours, after which conferences automatically end. The range of values is 1 to 8. The default value is **8**.
	UseAcceptLanguage	Indicates whether the signaling message contains **Accept-Language** and **Request-URI**. A value of **true** indicates that the message contains **Accept-Language** and **Request-URI**. A value of **false** indicates that the message contains only **Request-URI**. The default value is **true**.
ConferenceSDP	VideoAuditTimer	Specifies the interval, in minutes, after which Avaya Aura® Conferencing starts the video audit timer. During the audit, Avaya Aura® Conferencing disconnects the unused receiving audio streams in conferences. The range of values is 0 to 30. The default value of the timer is **15**. If you set the value to

Parameter group	Configuration parameter	Description
		0, you can disable the video audit. The audit is disabled, by default.
DNS	AuditInterval	Specifies the interval, in minutes, after which Avaya Aura® Conferencing starts the DNS table audit. The range of values is 1 to 2147483647. The default value is **5**.
	MaxEntry	Specifies the maximum number of entries allowed for a record in the DNS table. The range of values if 1 to 3. The default value is **3**.
	MaxTuples	Specifies the maximum size of DNS tables. The value range is 0 to 10000. The default value is **10**.
	NegativeExpiry	Specifies the time delay, in minutes, after which unresolved DNS queries expire. The time delay ensures that repeated queries for nonexistent entries are not sent to DNS. The value is 1 to 2147483647. The default value is **60**.
	PositiveExpiry	Specifies the time delay after which DNS returns the unresolved DNS queries. The value range is 1 to 2147483647. The default value is **60**.
EarlyProgress	EarlyProgressTimer	Specifies the time delay, in seconds, for the early 180 progress signal. The value range is 0 to 30. The default value is **3**.
HungCall	HungUnstableCallAuditTimer	Specifies the interval, in minutes, after which Avaya Aura® Conferencing starts the audit to determine and disconnect unstable, hung connections. The value range is 0 to 30. The default value is **3**. If you set a value of **0**, you can disable the audit.
KPIAlarm	IsAlarmEnabled	Enables and disables the KPI threshold alarms. The default value is **false**. If the value is **false**, the threshold alarms are disabled.
KPI_CallDist	answer_Seizure_Ratio	Specifies the threshold value of the answer seizure ratio. The answer seizure ratios are **minor**, **major**, and **critical**. The values are 0 to 100. The default value is **90, 70, 60, NEG**.
	Call_Treated_Ratio	Specifies the threshold value of the call treated ratio. The call treated ratios are **minor**, **major**, and **critical**. The values are 0 to 100. The default value is **60, 70, 90, POS**.

Parameter group	Configuration parameter	Description
KPI_IncomingCall	Call_Abandon_Ratio	Specifies the threshold value of the call abandon ratio. The call abandon ratios are **minor**, **major**, and **critical**. The values are 0 to 100. The default value is **60, 70, 90, POS**.
	Call_Other_Ratio	Specifies the threshold value of the call other ratio. The call other ratios are **minor**, **major**, and **critical**. The values are 0 to 100. The default value is **60, 70, 90, POS**.
	Call_Success_Ratio	Specifies the threshold value of the call success ratio. The call success ratios are **minor**, **major**, and **critical**. The values are 0 to 100. The default value is **90, 70, 60, NEG**.
	Call_Treated_Ratio	Specifies the threshold value of the call treated ratio. The call treated ratios are **minor**, **major**, and **critical**. The values are 0 to 100. The default value is **60, 70, 90, POS**.
LDAP	PageSize	Specifies the page size of the list of users returned by the LDAP server. The default value is **5**.
LongCall	CheckpointAuditDuration	Specifies the endpoint audit timer override period, in seconds, for check-pointed calls. The value range is 0 to 2147483647. The default value is **300**. If you set a value of **0**, you can disable the timer override.
	Duration	Specifies the interval, in minutes, between endpoint audits. The endpoint audit detects abandoned calls. The value range is 0 to 2147483647. The default value is **5**. If you set a value of **0**, you can disable the endpoint audit.
	EmergencyDuration	Specifies the endpoint audit timer override period, in seconds, for emergency calls. The value range is 0 to 2147483647. The default value is **30**. If you set a value of **0**, you can disable the timer override.
	SipLinesDuration	Specifies the endpoint audit timer override period, in seconds, for SIP calls. The value range is 0 to 2147483647. The default value is **30**. If you set a value of **0**, you can disable the timer override.

Parameter group	Configuration parameter	Description
		Caution: Changing the value of **SipLinesDuration** might cause call processing outage. If you are not aware of the correct setting, contact your next level of support.
	TlsTcpCallAuditDuration	Specifies the endpoint audit timer override period, in seconds, for TCP/TLS check-pointed calls. The value range is 0 to 2147483647. The default value is **300**. If you set a value of **0**, you can disable the timer override.
MSQuery	MaxFailures	Specifies the maximum number of OPTIONS request failures after which Avaya Aura® Conferencing declares a Media Server instance out of service. The value range is 1 to 10. The default value is **3**.
	QueryInterval	Specifies the interval, in seconds, between OPTIONS requests to the Media Server. The value range is 0 to 2147483647. The default value is **5**. If you set a value of **0**, you can disable the OPTIONS request.
	ReleaseConferenceOnMSFailure	Enables and disables whether Avaya Aura® Conferencing ends the conferences on a Media Server instance if the Media Server is out of service. The default value is **true**.
OBSubscribe	MaxSubscribeAttempts	Specifies the maximum number of times that the re-subscribe is attempted. The range is 1-10 and the default value is **5**.
	MaximumExpires	Specifies the maximum allowable expiration value for a subscription request. The range (in seconds) is 60-86400 and the default value is **86400**.
	ReSubscribeDelay	Specifies the time between re-subscription attempts. The range (in seconds) is 60-600 and the default value is **60**.
	ReSubscribeOffset	Specifies how early to send subscription refresh before subscription expires. The range (in seconds) is 60-600 and the default value is **300**.
Publish	MaximumExpires	Specifies the maximum allowable publication duration, in seconds. The range is 60-86400 and the default value is **86400**.

Parameter group	Configuration parameter	Description
	MinimumExpires	Specifies the minimum allowable publication duration, in seconds. The range is 60-86400 and the default value is **60**.
QoSThresholds	audioRTDThreshold	Specifies the audio round trip delay threshold value in milliseconds for reporting QoS problems in the QoSTroubleStart record. The range is 0 to 10,000 and the default value is **500**.
	jitterThreshold	Specifies the jitter threshold value in milliseconds for reporting QoS problems in the QoSTroubleStart record. The range is 0 to 30 and the default value is **3**.
	rFactorThreshold	Specifies the rFactor threshold value for reporting QoS problems in the QoSTroubleStart record. The range is 0 to 100 and the default value is **70**.
Recording	ActiveSpeakerEnergyThreshold	Specifies the minimum energy level required to be considered as an active speaker, in dBm. The range is -40 to -5 dBm and the default value is **-18** dBm.
	MaxConcurrentActiveSpeakers	Specifies the maximum number of concurrent active speaker to be displayed in playback of a recording. The range is 1 to 5 and the default value is **2** Maximum Concurrent Active Speakers.
	MaxLength	Specifies the maximum allowed recording length, in minutes. The range is 1 to 1440 minutes and the default value is **660** minutes.
SIPDos	Enable DoS filter	Enables or disables SIP DoS protection. The default value is **false**.
SIPStack	AutoAnswerForBYE	If set to this value to true, the stack sends auto 200 OK to BYE request. The allowable values are true/false and the default value is **true**.
	DEFAULT_MAX_BUFFER_SIZE	Specifies the maximum send/receive buffer length. The range is 6144 to 2147483647 and the default value is **16384**.
SMQuery	QueryInterval	Specifies the value in seconds for the query interval (how often AppServer sends OPTIONS query to a session manager). The range (in seconds) is 0 - 2147483647 and the default is 30 seconds. If you set the value to 0, you can disable the setting. The default value is **30**.

Parameter group	Configuration parameter	Description
ScopiaParms	DigitModification	Specifies the number of digits from the right end of the inline access code to be used for matching. The range is 0 - 15 for each digit. Use a pair of digits like a,b where a>b. If you set the value to 0,0, you can disable the digit modification. The default value is **0,0**.
SessionTimer	MinSE	Specifies the minimum value (in seconds) that is accepted for the session interval. The range (in seconds) is 90 - 2147483647 and the default value is **90** seconds.
SignalSupport	HandleReferForHomeInitator	If you set this value to true, then REFER is handled by the application server if the REFER initiator is homed on the application server. The allowable values are true/false and the default value is **false**.
	HandleReferForeignParty	If you set this value to true, then REFER is handled by the application server if the REFER target is a foreign destination. The allowable values are true/false and the default value is **false**.
SIPBehavior	ConcealAuthFailureReason	If you set this value to true, you can send a 407 "Authorization Required" for an invalid userid. The allowable values are true/false and the default value is **true**.
	IncludeMessageAccountForMWI	If you set this value to TRUE, you can include the "Message-Account" header in the MWI Notify Message. The allowable values are true/false and the default value is **true**.
SIPRespOMThresh	Infor500	The alarm thresholds are minor,major,and critical. The setting shows the percentage of incoming responses to SIP INFO that are 500. The format is a,b,c where all are integers between 1 and 100 (%) and a < b < c. The default values are 5,10,15. ALL OTHER ARE SIMILAR.
	Invite500	Default: 5,10,15
	Message500	Default: 5,10,15
	Notify500	Default: 5,10,15
	Options500	Default: 5,10,15
	Publish500	Default: 5,10,15
	Refer500	Default: 5,10,15
	Register500	Default: 5,10,15
	Service500	Default: 5,10,15
	Subscribe500	Default: 5,10,15

Parameter group	Configuration parameter	Description
	Update500	Default: 5,10,15
SIPTransport	GatewayBehindNATSupport	Enables 'Behind NAT support' for gateways. The two possible values are true or false. The default value is **false**.
	InitialMaxHops	Specifies the maximum number of hops allowed before a request is dropped. The range is 5 to 50. The default value is **20**.
	InviteTimer	Specifies the maximum time to wait for an INVITE to receive a response. The values range from 120000 to 3600000 milliseconds. The default value is **128000**.
	MaxRedirections	Specifies the maximum number of redirections allowed before a request is dropped. The values range from 3 to 10. The default value is **5**.
	MaxTermAttempt	Specifies the maximum number of internal cpl loops allowed before a request is dropped The values range from 5 to 50. The default value is **10**.
	NetworkSupportedPacketization	Specifies the network supported ptimes when a CS2K is present. It consists of a comma separated list of ptimes in ms (milliseconds).
	RejectCallfNoRegDests	If you set this value to true, Avaya Aura® Conferencing rejects a call when there is no regdest for term user. The allowable values are true and false. The default value is **false**.
	ServiceNodeName	Specifies the host name to use in the CS2K Via header. It consists of the host name associated with the logical service address
SubscrThreshold	PerConferenceSubscrThreshold	Specifies the limit to subscriptions allowed per conference focus. The range is from 0 to 5000. The default is **5000**. Use 0 to disable all conference-info subscriptions.
Subscribe	MaximumExpires	Specifies the maximum allowable expiration value for a subscription request, in seconds. The values range from 60-86400. The default value is **86400**.

Parameter group	Configuration parameter	Description
	MinimumExpires	Specifies the minimum allowable expiration value for a subscription request, in seconds The values range from 60-86400. The default value is 60.
Syntax	BadSyntaxLogging	Specifies the logging level of alarms raised from RVStack. If this parm is 0 then Avaya Aura® Conferencing does not display anything. If this parm is 2 then Avaya Aura® Conferencing displays the genLog of each alarm. The default value is 1.
TLSAuth	Disable hostname verifier	This parameter enables or disables the hostname verification check on Certificate validation. It is disabled by default (**false**). The allowable values are true or false.
	EnableCRL	This parameter enables or disables CRL retrieval for certificate revocation status. It is disabled by default (**false**). The allowable values are true or false.
	EnableOCSP	This parameter enables or disables OCSP for certificate revocation status. It is disabled by default (**false**). The allowable values are true or false.
	EnforceTLSMutualAuthForHTTPS	This parameter enforces TLS Mutual Authentication for the HTTPS interface. It is disabled by default (**false**). The allowable values are true or false.
	EnforceTLSMutualAutForSIP	This parameter enforces TLS Mutual Authentication for SIP interface. Clients connecting directly are excluded. It is disabled by default (**false**). The allowable values are true or false.
	PermitIfNoRevocationValidateResp	This parameter permits access if no certificate revocation validation response. It is enabled by default (**true**). The allowable values are true or false.
	SyncOCSPForSIP	This parameter allows synchronous OCSP queries for the SIP interface. It is disabled by default (**false**). The allowable values are true or false.
TLSSession	Allow TLS session resumption	This parameter enables or disables session resumption. It is disabled by default (**false**). The allowable values are true or false.
	Enforce renegotiation	This parameter enables or disables session renegotiation. MS NE should be restarted in order to take effect. It is disabled by default (**false**). The allowable values are true or false.

Parameter group	Configuration parameter	Description
X2	QueueThresholdsHigh	This parameter sets the alarm threshold high value. An alarm will be raised if the X2 queue size reaches QueueThresholdsHigh: % of QueueSize. The values range from (in %) 75 to 95. The default is **90**.
	QueueThresholdsLow	• This parameter sets the alarm threshold low value. The alarm raised when X2 queue size reached QueueThresholdsHigh will be cleared if it reaches QueueThresholdsLow: % of QueueSize. • The values range from (in %) 5 to 25. The default value is **10**.

Related Links

Modifying the configuration parameters of an application server on page 229

Modifying the active speaker reporting interval

About this task

Use this procedure to modify the time interval at which the active speaker notification is reported to the client application (for example, Avaya Flare® Experience for Windows, Avaya Flare® Experience for iPad Devices, and Avaya Collaboration Agent).

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers > <*Application Server name*> > Configuration Parameters**.
2. From the Parm Group box in the Application Server Configuration Parameters window, select **ConferenceParms**.
3. Select **ActiveSpeakerNotifyInterval**.
4. Click **Edit (+/-)**.
5. In the Value box of the Edit Application Server ConferenceParms Config Parm dialog box, make your change. The range for this setting is 0 to 60 seconds. The default is 4.
6. Click **Apply**.

Specifying the Avaya Aura® Session Manager that manages bandwidth for an application server

About this task

Use this procedure to specify the primary and/or secondary Avaya Aura® Session Manager that manages bandwidth for an application server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers > <*Application Server name*> > Bandwidth Management ASM**.
2. In the Application Server Bandwidth Management ASM dialog box, select the appropriate Avaya Aura Session Manager(s).
3. Click **Apply**.

Managing application server instances

Adding an application server instance

About this task

Use this procedure to add an application server instance.

You can have a maximum of two instances for an application server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers > <*Application Server name*> > Instance**.
2. In the Application Server Instance window, click **Add (+)**.
3. In the Add Application Server Instance dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Modifying an application server instance

About this task

Use this procedure to modify an application server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers > <*Application Server name*> > Instance**.
2. In the Application Server Instance window, select the application server instance you want to modify.

3. Click **Edit (-/+)**.
4. In the Edit Application Server Instance dialog box, make your changes. To change the Eng Parms, click **Advanced**.
5. When finished, click **Apply**.

Deleting an application server instance

About this task

Use this procedure to delete an application server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers > <*Application Server name*> > Instance**.
2. In the Application Server Instance window, select the application server instance you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Deploying an application server instance

About this task

Use this procedure to deploy an application server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers > <*Application Server name*> > NE Maintenance**.
2. In the Application Server Maintenance dialog box, select the instance you want to deploy.
3. Click **Deploy**.

Undeploying an application server instance

About this task

Use this procedure to undeploy an application server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers > <*Application Server name*> > NE Maintenance**.

2. In the Application Server Maintenance dialog box, select the instance you want to undeploy.
3. Click **Undeploy**.

Starting an application server instance

About this task

Use this procedure to start an application server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers > <*Application Server name*> > NE Maintenance**.
2. In the Application Server Maintenance dialog box, select the instance you want to start.
3. Click **Start**.

Stopping an application server instance

About this task

Use this procedure to stop an application server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers > <*Application Server name*> > NE Maintenance**.
2. In the Application Server Maintenance dialog box, select the instance you want to stop.
3. Click **Stop**.

Restarting an application server instance

About this task

Use this procedure to restart an application server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers > <*Application Server name*> > NE Maintenance**.
2. In the Application Server Maintenance dialog box, select the instance you want to restart.
3. Click **Restart**.

Killing an application server instance

About this task

Use this procedure to kill an application server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers > <*Application Server name*> > NE Maintenance**.
2. In the Application Server Maintenance dialog box, select the instance you want to kill.
3. Click **Kill**.

Viewing the details for an application server instance

About this task

Use this procedure to view the details for an application server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Application Servers > <*Application Server name*> > NE Maintenance**.
2. In the Application Server Maintenance dialog box, select the instance for which you want to view the details.
3. Click **Details**.

Chapter 27: Managing Media Servers

Adding a media server

About this task

Use this procedure to add a media server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers**.
2. In the Media Servers window, click **Add (+)**.
3. In the Add Media Server dialog box, complete the fields as appropriate. For more information, see Add Edit Media Server dialog box field descriptions on page 245.
4. When finished, click **Apply**.

Next steps

When you add a new network element, it is likely that you are also changing IP addresses and reconfiguring the NTP, DNS, and Syslog server. If you are making so many changes in your Avaya Aura® Conferencing system, you should always check if the Access Control List (ACL) is applied to the network element. The ACL manages the rules for internal and external system connections. If the ACL is applied to the network element, you should apply it to the new network element. For instructions on checking if it is applied and then applying it, see *Deploying Avaya Aura® Conferencing*, which is available from https://support.avaya.com/. The *Deploying Avaya Aura® Conferencing* guide also describes how to change IP addresses, reconfigure servers, and so on.

Modifying a media server

About this task

Use this procedure to modify a media server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers**.
2. In the Media Servers window, select the media server you want to modify.

3. Click **Edit (-/+)**.
4. In the Edit Media Server dialog box, make your changes. For more information, see Add Edit Media Server dialog box field descriptions on page 245.
5. When finished, click **Apply**.

Related Links

Add/Edit Media Server dialog box field descriptions on page 245

Add/Edit Media Server dialog box field descriptions

Name	Description
ShortName	A short name to identify the Media Server. Maximum: 6 alphanumeric characters. Example: MS1, MS2.
LongName	A longer more descriptive name to identify the Media Server. Maximum: 32 alphanumeric characters
Base Port	The port the Media Server uses. A numeric value from 1–65 535
FPM	Displays **ElementManager**.
Transport tab	
Enable SIP TCP / SIP TCP Port	Enables SIP TCP port and specifies the TCP Port.
Enable SIP TLS / SIP TLS Port	Enables SIP TLS port and specifies the TLS Port.
SIP Certificate	Choose the security certificate to be used by SIP.
Soap Proxy Port	Port for the administration SOAP.
SOAP Port	TCP port for the SOAP.
SOAP TLS Port	TLS port for the SOAP.
Enable SOAP/TLS	Enables TLS for the SOAP port.
SOAP Certificate	Logical name of the certificate used for SOAP/TLS communication.

Related Links

Modifying a media server on page 244

Deleting a media server

About this task

Use this procedure to delete a media server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers**.
2. In the Media Servers window, select the media server you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Modifying the configuration parameters of a media server

About this task

Use this procedure to modify the configuration parameters of a media server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > Configuration Parameters**.
2. In the Media Server Configuration Parameters window, make your changes. Use the **Parm Group** drop-down list box to access the parameter(s) you want to modify.

   For more information, see Media Server Configuration Parameters window field descriptions on page 246.

Related Links

Media Server Configuration Parameters window field descriptions on page 246

Media Server Configuration Parameters window field descriptions

Parameter group	Configuration parameter	Description
TLSAuth	EnableCRL	This parameter enables CRL retrieval for certificate revocation status. Range: true or false Default: false
	EnableOCSP	This parameter enables OCSP retrieval for certificate revocation status. Range: true or false Default: false
	EnableTCPTLSTransport	This parameter is a Boolean parameter. If you enable it, TLS is used for all external TCP connections. You

Parameter group	Configuration parameter	Description
		should restart the media server network element in order for this parameter to take effect. Default: false
	EnforceTLSMutual-AuthForHTTPS	This parameter enforces TLS Mutual Authentication for HTTP interface. Range: true or false Default: false
	EnforceTLSMutual-AuthForSIP	This parameter enforces TLS Mutual Authentication for SIP interface. Range: true or false Default: false
	PermitIfNoRevocationValidateResp	This parameter permits access, if no certificate revocation validation response. Range: true or false Default: true
	SyncOCSPForSIP	This parameter enables synchronous OCSP query for SIP interface. Range: true or false Default: false
	Disable hostname verifier	This parameter enables or disables hostname verification check on certificate validation. Range: true or false Default: false
	TCPTLSSessionRenegotiation	This parameter is a Boolean parameter. It enables or disables session renegotiation. You should restart the media server network element in order for this parameter to take effect. Default: true
	OCSPPermitIfNoResponse	This parameter is a Boolean parameter. It allows TLS network connections when no OCSP response is received. You should restart the media server network element in order for this parameter to take effect. Default: true
FQDN	FQDNAuditInterval	This parameter determines the timeout to audit FQDNs Range: 30 – 1800 seconds Default: 90 seconds

Parameter group	Configuration parameter	Description
MS	MSFileStorageAuditInterval	This parameter specifies the media server file storage audit interval in seconds. The media server downloads audio prompts and music on wait files from Element Manager. This parameter shows how often the media server network element requests the current state of this process from the media server database (and raise alarms that the process is currently in progress or failed, if needed). Range: 1–1800 Default: 30 seconds
	MSFileStorageDownloadTimeout	This parameter specifies the maximum amount of time in seconds for getting a file (particularly audio prompts and music on wait files) from Element Manager. Range: 0–300 (A value of 0 disables the timeout) Default: 300
	MSServiceStatusPollInterval	This parameter specifies the media server service status audit interval in seconds. This parameter shows how often the media server network element requests the current status of the media server service and indicates if the media server service is started or not. An alarm is raised if the media server service has not started. Range: 0–300 seconds Default: 30
MSDBConf	AcquireRetryAttempts	This parameter specifies the number of reconnection attempts to the media server database. It is used to recover from temporary database outages, such as those which occur during a database restart or brief loss of network connectivity. Range: 0–2147483647 Default: 5
	AcquireRetryDelay	This parameter specifies the delay in milliseconds between reconnection attempts to the media server database. It is used together with the `AcquireRetryAttempts` parameter to recover from temporary database outages. Range: 1000–3600000 milliseconds Default: 5000
	Port	This parameter specifies the port which is used to connect to the media server database. Range: 1025–65535

Parameter group	Configuration parameter	Description
		Default: 3306
Cross-Domain Policy	AllowAccessFromDomains	This parameter specifies the list of domains to which Avaya Aura® Conferencing (AAC) permits access to its Adobe Flash-based features. If a domain is not in this list, the clients in this domain will not be able to access features such as Web Collaboration or the document library. By default, Avaya Aura® Conferencing permits access for any domain. However, if Avaya Aura® Conferencing administrators wish to harden their system, they can limit access, by specifying certain domains and/or IP addresses, with multiple values separated by a comma.

Related Links

Modifying the configuration parameters of a media server on page 246

Configuring logs for a media server

About this task

Use this procedure to

- enable or disable debugtrace for a media server. When debugtrace is enabled, the Avaya media server writes logs in the files *Debug.txt in the directory /var/mcp/ma/MAS/common/logs.
- enable or disable system diagnostic mode for a media server. When system diagnostic mode is enabled, the Avaya media server writes logs in the files *Debug.txt in the directory /var/mcp/ma/MAS/common/logs.

Note:

Enabling system diagnostic mode can reduce system performance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > Log Processing > Log Configuration**.
2. In the Media Server Log Configuration dialog box, select the **Enable debugtrace** check box if you want to enable debug traces.
3. Select the **Enable system diagnostic mode** check box if you want to enable system diagnostic mode.
4. Click **Apply**.

Downloading logs for a media server

About this task

Use this procedure to download the logs for a media server to a file. You can also download the debug trace logs for a media server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > Log Processing > Log Download**.
2. In the Media Server Log Download dialog box, select the **Include debug trace logs** check box if you want to download trace logs also.
3. Click **Download**.
4. In the Save dialog box, specify the location and file to which you want to download the media server log(s).
5. Click **Save**.

Accessing the session detail record browser for a media server

About this task

Use this procedure to access the session detail record browser for a media server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > Session Detail Record Browser**.
2. In the Session Detail Record Browser window, enter your query settings.
3. Click **Execute**.

Managing Media Server Instances

Adding a media server instance

About this task

Use this procedure to add a media server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > Instance**.
2. In the Media Server Instance window, click **Add (+)**.
3. In the Add Media Server Instance dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Modifying a media server instance

About this task

Use this procedure to modify a media server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > Instance**.
2. In the Media Server Instance window, select the media server instance you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Media Server Instance dialog box, make your changes. To change the Eng Parms, click **Advanced**.
5. When finished, click **Apply**.

Deleting a media server instance

About this task

Use this procedure to delete a media server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > Instance**.
2. In the Media Server Instance window, select the media server instance you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Deploying a media server instance

About this task

Use this procedure to deploy a media server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > NE Maintenance**.
2. In the Media Server Maintenance dialog box, select the instance you want to deploy.
3. Click **Deploy**.

Undeploying a media server instance

About this task

Use this procedure to undeploy a media server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > NE Maintenance**.
2. In the Media Server Maintenance dialog box, select the instance you want to undeploy.
3. Click **Undeploy**.

Starting a media server instance

About this task

Use this procedure to start a media server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > NE Maintenance**.
2. In the Media Server Maintenance dialog box, select the instance you want to start.
3. Click **Start**.

Stopping a media server instance

About this task

Use this procedure to stop a media server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > NE Maintenance**.
2. In the Media Server Maintenance dialog box, select the instance you want to stop.
3. Click **Stop**.

Restarting a media server instance

About this task

Use this procedure to restart a media server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > NE Maintenance**.
2. In the Media Server Maintenance dialog box, select the instance you want to restart.
3. Click **Restart**.

Killing a media server instance

About this task

Use this procedure to kill a media server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > NE Maintenance**.
2. In the Media Server Maintenance dialog box, select the instance you want to kill.
3. Click **Kill**.

Viewing the details for a media server instance

About this task

Use this procedure to view the details for a media server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > NE Maintenance**.
2. In the Media Server Maintenance dialog box, select the instance for which you want to view the details.
3. Click **Details**.

Locking the service maintenance of a media server

About this task

Use this procedure to lock the service maintenance for a media server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > Service Maintenance**.
2. In the Media Server Maintenance dialog box, select the media server you want to lock.
3. Click the **Lock** button.
4. In the Confirmation dialog box, click **Yes**.

Administering a pending lock on the service maintenance of a media server

About this task

Use this procedure to administer a pending lock on the server maintenance of a media server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > Service Maintenance**.
2. In the Media Server Maintenance dialog box, select the media server to which you want to administer a pending lock.

3. Click the **Pending Lock** button.
4. In the Confirmation dialog box, click **Yes**.

Unlocking the service maintenance of a media server

About this task

Use this procedure to unlock the service maintenance of a media server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Servers > <*Media Server name*> > Service Maintenance**.
2. In the Media Server Maintenance dialog box, select the media server you want to unlock.
3. Click the **Unlock** button.
4. In the Confirmation dialog box, click **Yes**.

Managing Custom Prompts

About custom prompts

Avaya Aura® Conferencing provides the ability for you to use custom prompts. Custom prompts are a single ZIP archive containing only the prompt files you want to customize. For example, if you want to customize only the introduction prompt, you would put only one file in the archive. The default prompts are played for all non-customized files. The file structure and file names in the custom prompts archive are fixed. It is the administrator's responsibility to put the correct file structure into the uploaded custom prompts archive.

The file names and file paths in the archive should be exactly the same as in the default prompts ZIP archive. You should use the default prompts ZIP archive as an example in order to correctly put the audio files into the custom prompts archive. To download the default prompts ZIP archive, see Downloading default prompts from the media servers on page 265.

If the Avaya Aura® Conferencing system is using the default prompt set, and no custom prompts have been created previously, download the default prompts ZIP archive and create your custom prompts archive.

After you configure the custom prompts archive, you must upload that file to the Avaya media servers. The custom prompts zip archive will be uploaded to the following directory on the server for the instance EM0 (that is, EMServer1): /var/mcp/media/audio/custom/. After the zip archive is uploaded to EM0, this file is then downloaded by every media server instance that is currently running in Element Manager Console. Custom prompt files are also downloaded to media server

instances when media server instances are started or deployed. To upload custom prompts, see Uploading custom prompts to the media servers on page 263.

Related Links

List of customizable prompts on page 256

List of customizable prompts

Note:

All files must be 16bit 8Khz pcm mono format. The file names are the same regardless of language used. The text can be modified for any of the supported languages.

Table 1: Verbal announcements

Filename	Text
IntroVidConf.wav	Avaya , Welcome to Avaya Video Conferencing
EnterAccess.wav	Please Enter your collaboration code followed by the pound Key
ReEnterAccess.wav	The collaboration code is invalid. Please reenter your collaboration code followed by the pound key
Admin.wav	Please contact your local administrator
InvalidChair.wav	The moderator pin you have provided is invalid. Please reenter the moderator PIN followed by the pound key
FastStart.wav	The Conference is now starting you are the first person to arrive.
ConfEndingNow.wav	The conference is now ending. Goodbye
ConfEnding.wav	The conference will end in one minute
MINUTES.wav	...minutes
CONF_END_PRE.wav	
ExitBleep.wav	<Bleep tone>
EnterBleep.wav	<Bleep tone>
EnterStar.wav	If you are the conference moderator, please enter the star key now
ConferenceUnlocked.wav	Conference unlocked.
ConferenceLocked.wav	Conference locked
ConferenceFull.wav	That conference you are attempting to join has reached the maximum allowed number of participants.
ChairNoTerminate.wav	The conference will be allowed to continue when you leave the conference
ChairTerminate.wav	The conference will be terminated when you leave the conference

Filename	Text
EntryExitOn.wav	Entry and exit notification enabled.
EntryExitOff.wav	Entry and exit notification disabled.
ChairCode.wav	Please Enter the moderator passcode followed by the pound key.
ChairEnter.wav	Please press one when you are ready to enter the conference.
OnlyPerson.wav	You are the only person in the conference.
ThereAre.wav	There are…
PartiesInThisConference.wav	Parties in this conference.
VideoMute.wav	Video paused
VideoUnmute.wav	Video resumed
UserAudioMuted.wav	Audio silenced
UserAudioUnmuted.wav	Audio unsilenced
UserMuted.wav	Audio silenced and video paused
UserUnmuted.wav	Audio unsilenced and video resumed
ConferenceFullMuted.wav	Conference Silenced and Video Paused.
ConferenceFullUnmuted.wav	Conference unsilenced and Video resumed.
ConfVideoMute.wav	Conference video paused
ConfVideoUnmute.wav	Conference video resumed
ConferenceAudioMuted.wav	Conference Muted
ConferenceAudioUnmuted.wav	Conference Unmuted
LectureOn.wav	Lecture mode started
LectureModeActive.wav	This operation is not allowed while lecture mode is active
LECTURE_ENTRANT.wav	You are entering a conference that is in lecture mode
LectureOff.wav	Lecture mode stopped
VideoDisabled.wav	Conference Video disabled
VideoEnabled.wav	Conference Video enabled
VideoUnavailable.wav	Video unavailable
DialoutConfirmation.wav	You have been invited to a conference. Press one to be placed into the conference.
DialoutConfirmationForModerator.wav	You have been invited to a conference as the moderator. Press one to be placed into the conference.
FailToAdd.wav	Dial out request to participate resulted in an error. Please try again
AddUnavailable.wav	The participant requested to join the conference is unavailable at this time.

Filename	Text
DialoutDisabled.wav	The dial out feature is not currently allowed.
LectureModeActive.wav	This operation is not allowed while lecture mode is active
DialOut.wav	Please enter the number of the participant you wish to dial followed by the pound key.
EventMode.wav	You are entering an event conference.
PanelDisabled.wav	Presentation mode stopped.
PanelEnabled.wav	Presentation mode started.
FeatureUnavailable.wav	This operation is not currently allowed.
DialoutFull.wav	The conference has reached its maximum amount of participants. Dial out is not allowed.
ConferenceIsLocked.wav	The conference you are attempting to join is locked.
ConferencePlacement.wav	You will now be placed into the conference.
WaitForChair.wav	You will be placed into conference when the moderator arrives.
ModeratorPresent.wav	A moderator is already present
InvalidModerator.wav	A moderator is already present
SetChair.wav	You are now the conference moderator.
UnSetChair.wav	You are not the conference moderator.
NoOperatorAdmin.wav	There is no operator is available, please contact your local administrator.
ConfirmConfKill.wav	Press one to confirm that you want the conference to end immediately.
PlaybackEnding.wav	Playback ending.
TRANSFER_TO_OPERATOR.wav	You are now being transferred to an operator.
ConfirmOperatorSupport.wav	Please press 1 to confirm that you want to be transferred to an operator
UserRaiseHand.wav	Your hand is raised.
UserLowerHand.wav	Your hand is lowered
ModeratorLowerHand.wav	The moderator has lowered your hand.
ResourceFailure.wav	Your call can not be completed at this time. Please try again later.
BandwidthFailure.wav	Network resources are not available to complete your call. Please try again later.
PasscodeRequired.wav	This conference requires a passcode. Please enter your passcode followed by the pound key.
PasscodeReEnter.wav	Please re-enter your passcode followed by the pound key.
ContactOwner.wav	Please contact the conference owner for passcode information.

Table 2: Announcements related to the recording feature

Filename	Text
ConferenceRecordingStarted.wav	Your conference is being recorded
ConferenceRecordingStopped.wav	Conference Recording has stopped
RecordingMenuStartRecording.wav	Press one to begin recording or any other key to cancel.
RecordingMenuStopRecording.wav	Press one to stop recording or any other key to cancel.
ConferenceRecorded.wav	The conference is now being recorded.
ConferenceRecordingUnavailable.wav	I'm sorry conference recording is not available.
Playbackprompt.wav	Press 1 if you would like to playback a recording portion you've missed.

Table 3: Announcements related to the help feature

Filename	Text
StarZeroMmcs.wav	Press star zero to dial out to an operator.
StarFiveMmcs.wav	Press star five to start and stop lecture mode.
StarSevenMmcs.wav	Press star seven to toggle the conference lock.
StarEightMmcs.wav	Press star eight to toggle muting of the conference audio and starting and stopping of the conference video.
StarEightOneMmcs.wav	Press star eight one to toggle muting of the conference participants.
StarEightTwoMmcs.wav	Press star eight two to toggle starting and stopping of video for the conference participants.
StarSixMmcs.wav	Press star six to toggle muting and starting and stopping of video.
StarSixOneMmcs.wav	Press star six one to toggle audio silencing.
StarSixTwoMmcs.wav	Press star six two to start and stop video.
StarFourMmcs.wav	Press star four to enable and disable entry and exit notification.
PoundPoundMmcs.wav	Press pound pound to immediately end the conference.
StarOneMmcs.wav	Press star one to initiate dial out in order to join a participant to the conference.
StarPoundMmcs.wav	Press star pound for the number of conference parties.
Star41RaiseHand.wav	Press star four one to raise your hand
Star42LowerHand.wav	Press star four two to lower your hand

Filename	Text
SetModeratorHelp.wav	Press star five one to assume moderator controls if no moderator is present.
StarNineEightMmcs.wav	Press star nine eight to start and stop conference continuation.
StarNineSixMx.wav	Press star nine six to toggle muting of the conference audio and starting and stopping of the conference video.

Note:

These are the current files used to build numbers for zero to three thousand. Each language has its own set of files and rules for building numbers that may be unique to that language.

Table 4: Number announcements

Filename
a-or-an.wav
and.wav
eight-five.wav
eight-hundred.wav
eight.wav
eighteen.wav
eighty-eight.wav
eighty-four.wav
eighty-nine.wav
eighty-one.wav
eighty-seven.wav
eighty-six.wav
eighty-three.wav
eighty-two.wav
eighty.wav
eleven.wav
fifteen.wav
fifty-eight.wav
fifty-five.wav
fifty-four.wav
fifty-nine.wav
fifty-one.wav
fifty-seven.wav
fifty-six.wav

Filename
fifty-three.wav
fifty-two.wav
fifty.wav
five-hundred.wav
five.wav
forty-eight.wav
forty-five.wav
forty-four.wav
forty-one.wav
forty-seven.wav
forty-six.wav
forty-three.wav
forty-two.wav
forty.wav
four-hundred.wav
four.wav
fourteen.wav
hundred.wav
nine-hundred.wav
nine.wav
nineteen.wav
ninety-eight.wav
ninety-five.wav
ninety-four.wav
ninety-nine.wav
ninety-one.wav
ninety-seven.wav
ninety-six.wav
ninety-three.wav
ninety-two.wav
ninety.wav
one-hundred.wav
one-thousand.wav
one.wav
seven-hundred.wav
seven-six.wav

Filename
seven.wav
seventeen.wav
seventy-eight.wav
seventy-five.wav
seventy-four.wav
seventy-nine.wav
seventy-one.wav
seventy-seven.wav
seventy-three.wav
seventy-two.wav
seventy.wav
six-hundred.wav
six.wav
sixteen.wav
sixty-eight.wav
sixty-five.wav
sixty-four.wav
sixty-nine.wav
sixty-one.wav
sixty-seven.wav
sixty.wav
ten.wav
thirteen.wav
thirty-eight.wav
thirty-five.wav
thirty-four.wav
thirty-nine.wav
thirty-one.wav
thirty-seven.wav
thirty-six.wav
thirty-three.wav
thirty-two.wav
thirty.wav
three-hundred.wav
three-thousand.wav
three.wav

Filename
twelve.wav
twenty-eight.wav
twenty-five.wav
twenty-four.wav
twenty-nine.wav
twenty-one.wav
twenty-seven.wav
twenty-six.wav
twenty-three.wav
twenty-two.wav
twenty.wav
two-hundred.wav
two-thousand.wav
two.wav
zero.wav

Related Links

About custom prompts on page 255

Uploading custom prompts to the media servers

Before you begin

You must know the password for the ntappadm login.

The custom audio prompt files must meet the following requirements:

- The files must have a .wav extension.
- The files must be in PCM audio format (8000 Hz, 16 bit, Mono).
- The files must stored and loaded as a single zip archive file.
- The file names and file paths in the archive should be exactly the same as in the default prompts ZIP archive.

Note:

You should use the default prompts ZIP archive as an example in order to correctly put the audio files into the custom prompts archive. To download the default prompts ZIP archive, see Downloading default prompts from the media servers on page 265.

About this task

Use this procedure to upload custom prompts to the Avaya media servers.

The custom prompts zip archive will be uploaded to the following directory on the server for the instance EM0 (that is, EMServer1): /var/mcp/media/audio/custom/. After the zip archive is uploaded

to EM0, this file is then downloaded by every media server instance that is currently running in Element Manager Console. Custom prompt files are also downloaded to media server instances when media server instances are started or deployed.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Custom Prompts**.
2. In the Custom Prompts dialog box, click **Browse**.
3. In the Select media archive file dialog box, select the custom prompts zip archive file that you want to upload.
4. Click **Open**.
5. In the Message box, click **OK**.

   The Upload custom Prompts box displays the path and name of the zip file you want to upload.
6. Click **Upload**.
7. In the FTP Login dialog box, enter your FTP login ID in the User box.
8. In the Password box, enter the password for your FTP login ID.
9. Click **Apply**.
10. In the Upload Complete message box, click **OK**.

Downloading custom prompts from the media servers

Before you begin

You must know the password for the ntappadm login.

About this task

Use this procedure to download custom prompts from the media servers.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Custom Prompts**.
2. For the Download custom Prompts setting in the Custom Prompts dialog box, click **Download**.
3. In the FTP Login dialog box, enter your FTP login ID in the User box.
4. In the Password box, enter the password for your FTP login ID.
5. Click **Apply**.
6. In the Save dialog box, specify the name and location for the custom prompts zip archive file that you want to download.

7. Click **Save**.
8. In the Download Complete box, click **OK**.

Downloading default prompts from the media servers

Before you begin

You must know the password for the ntappadm login.

About this task

Use this procedure to download default prompts from the media servers.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Custom Prompts**.
2. For the Download default Prompts setting in the Custom Prompts dialog box, click **Download**.
3. In the FTP Login dialog box, enter your FTP login ID in the User box.
4. In the Password box, enter the password for your FTP login ID.
5. Click **Apply**.
6. In the Save dialog box, specify the name and location for the default prompts zip archive file that you want to download.
7. Click **Save**.
8. In the Download Complete box, click **OK**.

Deleting custom prompts from the media servers

Before you begin

You must know the password for the ntappadm login.

About this task

Use this procedure to delete the custom prompts from the media servers.

If you delete the custom prompts, all of the media servers will use the default prompts. (The default prompts are restored automatically.)

Warning:

The custom prompts will be deleted from the EM Server. Before performing this procedure, create a backup copy of the existing custom prompts. See Downloading custom prompts from the media servers on page 264 to create a backup copy of the existing custom prompts.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Custom Prompts**.
2. In the Custom Prompts dialog box, click **Delete**.
3. In the Confirmation dialog box, click **Yes**.
4. Click **Apply**.
5. In the Delete Custom Prompts message box, click **OK**.

Managing Custom Music on Wait

About custom music on wait files

Avaya Aura® Conferencing provides the ability for you to use custom music on wait files. Custom music on wait files are stored and loaded as a single ZIP archive. The custom music on wait ZIP archive must contain the full set of audio files to be played for music on wait.

The custom music on wait files must meet the following requirements:

- The files must have a .wav extension.
- The files must be in PCM audio format (8000 Hz, 16 bit, Mono).

After you configure the custom music on wait ZIP archive, you must upload that file to the Avaya media servers. The custom music on wait ZIP archive will be uploaded to the following directory on the server for the instance EM0 (that is, EMServer1): /var/mcp/media/audio/custom/. After the ZIP archive is uploaded to EM0, this file is then downloaded by every media server instance that is currently running in Element Manager Console. Custom music on wait files are also downloaded to media server instances when media server instances are started or deployed. To upload the custom music on wait files, see Uploading custom music on wait files to the media servers on page 266.

The file structure and file names in the custom music on wait ZIP archive are not fixed.

If the Avaya Aura® Conferencing system is using the default music on wait files set, and no custom music on wait files have been created previously, download the default music on wait ZIP archive and create your custom music on wait ZIP archive.

Uploading custom music on wait files to the media servers

Before you begin

You must know the password for the ntappadm login.

The custom music on wait files must meet the following requirements:

- The files must have a .wav extension.
- The files must be in PCM audio format (8000 Hz, 16 bit, Mono).
- The files must be stored and loaded as a single ZIP archive.

About this task

Use this procedure to upload custom music on wait files to the media servers.

The custom music on wait ZIP archive will be uploaded to the following directory on the server for the instance EM0 (that is, EMServer1): /var/mcp/media/audio/custom/. After the ZIP archive is uploaded to EM0, this file is then downloaded by every media server instance that is currently running in Element Manager Console. Custom music on wait files are also downloaded to media server instances when media server instances are started or deployed.

Before uploading custom music on wait files, note the following information:

- The custom music on wait zip archive must contain the full set of audio files to be played for music on wait.
- The file structure and file names in the custom music on wait zip archive are not fixed.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Custom Music on Wait**.
2. In the Custom Music on Wait dialog box, click **Browse**.
3. In the Select media archive file dialog box, select the custom music on wait zip archive file that you want to upload.
4. Click **Open**.
5. In the Message box, click **OK**.

   The Upload custom Music on Wait box displays the path and name of the zip file you want to upload.
6. Click **Upload**.
7. In the FTP Login dialog box, enter your FTP login ID in the User box.
8. In the Password box, enter the password for your FTP login ID.
9. Click **Apply**.
10. In the Upload Complete message box, click **OK**.

Downloading custom music on wait files from the media servers

Before you begin

You must know the password for the ntappadm login.

About this task

Use this procedure to download custom music on wait files from the media servers.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Custom Music on Wait**.
2. In the Custom Music on Wait dialog box, click **Download**.
3. In the FTP Login dialog box, enter your FTP login ID in the User box.
4. In the Password box, enter the password for your FTP login ID.
5. Click **Apply**.
6. In the Save dialog box, specify the name and location for the custom music on wait zip archive file that you want to download.
7. Click **Save**.
8. In the Download Complete box, click **OK**.

Deleting custom music on wait files from the media servers

Before you begin

You must know the password for the ntappadm login.

About this task

Use this procedure to delete the custom music on wait files from the media servers.

If you delete the custom music on wait files, all of the media servers will use the default music on wait files. (The default music on wait files are restored automatically.)

Warning:

The custom music on wait files will be deleted from the EM Server. Before performing this procedure, create a backup copy of the existing custom music on wait files. See Downloading custom music on wait files from the media servers on page 267 to create a backup copy of the existing custom music on wait files.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Custom Music on Wait**.
2. In the Custom Music on Wait dialog box, click **Delete**.
3. In the Confirmation dialog box, click **Yes**.
4. Click **Apply**.
5. In the Delete Custom Music on Wait message box, click **OK**.

Managing Media Server Resources

Associating a media server cluster with a location

Before you begin

- You must be logged into Provisioning Client.
- Media servers and media server clusters must be configured already on Element Manager Console.

About this task

Use this procedure to associate a media server cluster with a location. You may associate multiple locations to media server clusters. The media servers in the cluster will serve the associated locations.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Serving Locations** tab.
3. From the Media Server Cluster box, select the media server cluster you want to associate with a location.
4. In the Add locations area, select the check box of the location(s) to which you want to associate the selected media server cluster.
5. Click **Save**.

Related Links

Media Server Serving Locations tab field descriptions on page 269

Media Server Serving Locations tab field descriptions

Name	Description
Media Server Cluster	Specifies the media server cluster that you want to associate with a location. Only the media server clusters that are administered in Element Manager Console are displayed in this box.
Add locations	Displays the locations to which you can assign the selected media server cluster. A check mark next to a location indicates that the selected media server cluster is assigned to that location.

Related Links

Associating a media server cluster with a location on page 269

Assigning a media server cluster to a physical location (by location)

Before you begin

- You must be logged into Provisioning Client.
- Media servers and media server clusters must be configured already on Element Manager Console.

About this task

Use this procedure to associate a media server cluster with a physical location. This enables the conferencing server to select the appropriate media server cluster for media processing based on the end user's location.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Cluster Physical Location** tab.
3. From the Select by box, select **Location**.
4. From the Select Physical Location box, select the location to which you want to assign a media server cluster.
5. From the Available Media Server Clusters box, select the appropriate media server cluster, and then click **Copy**. If you want to assign all available media server clusters, click **Copy all**.
6. Click **Save**.

Media Server Cluster Physical Location tab field descriptions

Name	Description
Select by	Enables you to specify whether you want to manage the media server clusters by physical location or media server cluster name. Your choices: • **Location**: Enables you to manage the media server cluster by physical location. When you select this option, you can select the physical location for which you want to manage the media server clusters. • **Media Server Cluster**: Enables you to manage the media server cluster by name. When you select this option, you can select the media server cluster you want to manage.

Comments? infodev@avaya.com

Name	Description
Select Physical Location	Enables you to specify the physical location where you want to manage media server clusters. This field is displayed when you select **Location** from the Select by box.
Available Media Server Clusters	Displays the media server clusters that you can assign to the selected location. From this list box, you can select the media server cluster(s) that you want to assign to the selected location. This list box is displayed when you select **Location** from the Select by box.
Selected Media Server Clusters	Displays the media server clusters that you want to assign to the selected location. This list box is displayed when you select **Location** from the Select by box.
Select Media Server Cluster	Enables you to specify the media server cluster that you want to manage. This field is displayed when you select **Media Server Cluster** from the Select by box.
Physical Location	Enables you to specify the physical location to which you want to assign the selected media server cluster. This field is displayed when you select **Media Server Cluster** from the Select by box.

Button	Description
Copy all	Moves all of the media server clusters displayed in the Available Media Server Clusters list box into the Selected Media Server Clusters list box.
Copy	Moves the selected media server cluster in the Available Media Server Clusters list box into the Selected Media Server Clusters list box.
Remove	Moves the selected media server cluster in the Selected Media Server Clusters list box into the Available Media Server Clusters list box.
Remove All	Moves all of the media server clusters displayed in the Selected Media Server Clusters list box into the Available Media Server Clusters list box.

Related Links

[Assigning a media server cluster to a physical location (by media server cluster)](#) on page 272

Comments? infodev@avaya.com

Assigning a media server cluster to a physical location (by media server cluster)

Before you begin

- You must be logged into Provisioning Client.
- Media servers and media server clusters must be configured already on Element Manager Console.

About this task

Use this procedure to associate a media server cluster with a physical location. This enables the conferencing server to select the appropriate media server cluster for media processing based on the end user's location.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Cluster Physical Location** tab.
3. From the Select by box, select **Media Server Cluster**.
4. From the Select Media Server Cluster box, select the media server cluster you want to assign to a location.
5. From the Physical Location box, select the appropriate location.
6. Click **Save**.

Related Links

Media Server Cluster Physical Location tab field descriptions on page 270

Configuring media stream cascading for a location

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to configure media stream cascading for a location.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Stream Cascading** tab.
3. From the Select location box, select the appropriate location.

4. Complete the fields as appropriate. See Media Stream Cascading tab field descriptions on page 124.
5. Click **Save**.

Related Links

Managing Locations on page 116
Media Stream Cascading tab field descriptions on page 124

Event conferencing and media cascading

Event conferencing requires a dedicated Avaya Media Server and a dedicated Web Conferencing server. An event conference can support up to 2,000 active audio sessions per Avaya Media Server and 1,500 web sessions per Web Conferencing server. For example, you can host a single event conference with a maximum of 2,000 audio sessions and 1,500 web sessions using an Avaya Media Server and a Web Conferencing server, or you can host multiple event conferences with fewer participants simultaneously using an Avaya Media Server and a Web Conferencing server as long as the total number of audio sessions does not exceed the maximum of 2,000 and the total number of web sessions does not exceed 1,500.

You can add multiple Avaya Media Servers and Web Conferencing servers. However, a single event conference will still support a maximum of 2,000 audio sessions and 1,500 media.

You can also have multiple Avaya Media Servers in one location, enabling you to host multiple event conferences across multiple Avaya Media Servers in one location. In this scenario, once a conference starts on an Avaya Media Server, you are limited to the capacity of that Avaya Media Server. For example, if the first conference has 1,500 audio sessions, then the second conference that starts on that same Avaya Media Server will be limited to a maximum of 500 audio sessions.

The following table describes the capacities associated with event conferencing.

Table 5: Target capacities for Event conferencing

Servers (dedicated for Event conferencing)	Active audio sessions	Web sessions	Scalable by increasing the number of Event conferences only	Redundancy with an N+m configuration
Avaya Media Server	2,000 **Note:** Audio sessions are dedicated to a single server.	—	Yes **Note:** You can increase the number of simultaneous event conferences by adding additional servers. However, each server	Yes

Comments? infodev@avaya.com

Servers (dedicated for Event conferencing)	Active audio sessions	Web sessions	Scalable by increasing the number of Event conferences only	Redundancy with an N+m configuration
			supports a maximum of 2,000 audio sessions for all event conferences occurring on that server.	
Web Conferencing Server (primary and secondary)	—	1,500 **Note:** Web sessions are dedicated to a single server.	Yes **Note:** You can increase the number of simultaneous event conferences by adding additional servers.	Yes

Support for cascading

Media cascading reduces the number of media streams travelling across the WAN by consolidating these streams based by location. This technique is applied to both audio and video streams. Media cascading provides bandwidth optimization with no significant reductions in the quality of audio or video. Conferences are scalable with proper configuration and management which is fully transparent to end users. Media cascading is available for event conferences. The combination of these two features — event conferencing and media cascading — provides a very compelling solution for very large global conferences.

VMWare and cascading capcity

The following table shows the supported capacity for cascading Avaya Media Servers on VMWare for Avaya Aura® Conferencing 8.0

AAC on VMWare	Capacity (Audio Sessions)	Capacity (Video Sessions)	vCPU (Virtual CPU)	Virtual Memory (GB)	Virtual Storage (GB)	Minimum CPU Speed (GHz)/Per Core	vCPU Resource Reservation (GHz)
Cascading Avaya Media Servers (6 vCPUs)	540	160	6	16	150	2.893	17.358

In order to successfully support the cascading feature, an event conference requires a dedicated media server for hosting but does not require dedicated media servers at the cascading locations.

For more information on the available hardware options for cascading servers, see Supported hardware on page 21.

Media Stream Cascading tab field descriptions

Name	Description
Select location	Enables you to specify the location for which you want to configure media cascading.
Cascading is allowed when this location is hosting the conference	Specifies whether media cascading can occur for a conference hosted at this location.
Allowed number of video streams to a remote location	Specifies the maximum number of video streams sent from a host media server to a remote media server in a cascading media server environment. For example, if you set this value to 1, then only one video stream (of the active speaker) will be sent from the host media server to the remote media server. If you set this value to 4, then four video streams (showing the active speaker and the previous three active speakers) will be sent from the host media server to the remote media server. Your choices are 1 through 4. Changing this setting affects all conferences that use cascading media servers at the selected location.
Allowed number of video streams from a remote location	Specifies the maximum number of video streams sent from a remote media server to a host media server in a cascading media server environment. For example, if you set this value to 1, then only one video stream (of the active speaker) will be sent from the remote media server to the host media server. If you set this value to 4, then four video streams (showing the active speaker and the previous three active speakers) will be sent from the remote media server to the host media server. Your choices are 1 through 4. Changing this setting affects all conferences that use cascading media servers at the selected location.
Cascading is allowed when the conference is hosted remotely at another location	Specifies whether media cascading can occur for a conference that is hosted at another location.
Allowed number of video streams to a hosting location	Specifies the maximum number of video streams sent from a remote media server to a host media server in a cascading media server environment . For example, if you set this value to 1, then only one video stream (of the active speaker) will be sent from the remote media server to the host media server. If

Name	Description
	you set this value to 4, then four video streams (showing the active speaker and the previous three active speakers) will be sent from the remote media server to the host media server. Your choices are 1 through 4. Changing this setting affects all conferences that use cascading media servers at the selected location.
Allowed number of video streams from a hosting location	Specifies the maximum number of video streams sent from a host media server to a remote media server in a cascading media server environment . For example, if you set this value to 1, then only one video stream (of the active speaker) will be sent from the host media server to the remote media server. If you set this value to 4, then four video streams (showing the active speaker and the previous three active speakers) will be sent from the host media server to the remote media server. Changing this setting affects all conferences that use cascading media servers at the selected location.

Related Links

Configuring media stream cascading for a location on page 124

Configuring a hosting location

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to associate multiple locations with a hosting location. This hosting location will host conferences for the locations you specify.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Hosting Locations** tab.
3. From the Select Hosting Location box, select the hosting location you want to configure. For more information see, Hosting Locations tab field descriptions on page 126
4. From the Hostable Locations box, select the appropriate location(s), and then click **Copy**. If you want to assign all locations, click **Copy all**.
5. Click **Save**.

Related Links

Managing Locations on page 116
Hosting Locations tab field descriptions on page 126

Hosting Locations tab field descriptions

Name	Description
Select Hosting Location	Select the hosting location you want to configure.
Hostable Locations	Displays the locations that you can assign to the selected location. From this list box, you can select the location(s) that you want to assign to the selected hosted location.
Hosted Locations	Displays the locations that you want to assign to the selected hosted location.

Button	Description
Copy all	Moves all of the locations displayed in the Hostable Locations list box into the Hosted Locations list box.
Copy	Moves the selected location in the Hostable Locations list box into the Hosted Locations list box.
Remove	Moves the selected location in the Hosted Locations list box into the Hostable Locations list box.
Remove All	Moves all of the locations displayed in the Hosted Locations list box into the Hostable Locations list box.

Related Links

Configuring a hosting location on page 126

Configuring a regional cascading location

Before you begin

- You must be logged into Provisioning Client.
- Cascaded locations (that is, locations that cascade through a cascading location) must have a good-quality WAN link.
- Cascaded locations do not need to have media servers configured.
- A cascaded location can be assigned to only one cascading location (that is, the location that provides media cascading).
- A cascaded location and cascading location pair cannot be assigned as a hosted location and hosting location pair (and vice versa).
- A cascading location can be the same as the hosting location for a particular location.
- Cascading must be enabled for the Avaya Aura® Conferencing system, the user location, the cascading location, and the hosting location if you want to use regional cascading.

- For Event conferences, the hosting media servers are dedicated Event conference servers. The cascading media servers are not dedicated. In other words, any media servers that are assigned to serve a certain location can be used for media cascading.

About this task

Use this procedure to configure a regional cascading location, which provides media cascading to the remote locations you specify. The users at the specified locations will be able to call into the regional cascading location instead of the joining the conference directly via the hosting media server. Regional cascading locations enable you to optimize WAN bandwidth usage.

Note:

Cascading must be allowed (enabled) for the Avaya Aura® Conferencing system, the user location, the cascading location, and the hosting location if you want to use regional cascading.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Cascading Locations** tab.
3. From the Select Cascading Location box, select the location that will provide media cascading for other locations.
4. From the Locations that have no Cascading Location assigned list box, select the location(s) that you want to assign to the selected cascading location, and then click **Copy**. If you want to assign all locations, click **Copy all**. For more information see, Media Cascading Locations tab field descriptions on page 128.
5. Click **Save**.

Related Links

Managing Locations on page 116
Media Cascading Locations tab field descriptions on page 128

Media Cascading Locations tab field descriptions

Name	Description
Select Cascading Location	Select the location that will provide media cascading for other locations.
Locations that have no Cascading Location assigned	Displays the locations that you can assign to the selected cascading location. From this list box, you can select the location(s) that you want to assign to the selected cascading location.
Locations that cascade through <*selected cascading location*>	Displays the locations that you want to assign to the selected cascading location. The selected cascading location is a variable/dynamic field, based on the **Select Cascading Location** field.

Button	Description
Copy all	Moves all of the locations displayed in the Locations that have no Cascading Location assigned list box into the Locations that cascade through list box.
Copy	Moves the selected location in the Locations that have no Cascading Location assigned list box into the Locations that cascade through list box.
Remove	Moves the selected location in the Locations that have no Cascading Location assigned list box into the Locations that cascade through list box.
Remove All	Moves all of the locations displayed in the Locations that cascade through list box into the Locations that have no Cascading Location assigned list box.

Related Links

Configuring a regional cascading location on page 127

Configuring media server clusters for an Event conference

Before you begin

- You must be logged into Provisioning Client.
- Media server clusters must be configured already in Element Manager Console.

About this task

Use this procedure to associate a media server cluster with an Event conference.

Note:

The media server clusters you specify can only be used for Event conferences.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Clusters for Event Conference** tab.
3. From the Available Media Server Clusters box, select the appropriate media server cluster(s), and then click **Copy**. If you want to assign all media server clusters, click **Copy all**.
4. Click **Save**.

Related Links

Media Server Clusters for Event Conference field descriptions on page 279

Media Server Clusters for Event Conference field descriptions

Name	Description
Available Media Server Clusters	Displays the media server clusters that you can assign to the Event conference. From this list box, you can select the media server cluster(s) that you want to assign to the event conference.
Selected Media Server Clusters	Displays the media server clusters that you want to assign to the Event conference.

Button	Description
Copy all	Moves all of the media server clusters displayed in the Available Media Server Clusters list box into the Selected Media Server Clusters list box.
Copy	Moves the selected media server cluster in the Available Media Server Clusters list box into the Selected Media Server Clusters list box.
Remove	Moves the selected media server cluster in the Selected Media Server Clusters list box into the Available Media Server Clusters list box.
Remove All	Moves all of the media server clusters displayed in the Selected Media Server Clusters list box into the Available Media Server Clusters list box.

Related Links

Configuring media server clusters for an Event conference on page 279

Chapter 28: Managing Media Server Clusters

Adding a media server cluster

About this task

Use this procedure to add a media server cluster.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters**.
2. In the Media Server Clusters window, click **Add (+)**.
3. In the Add Media Server Cluster dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Related Links

Add/Edit Media Server Cluster dialog box field descriptions on page 281

Add/Edit Media Server Cluster dialog box field descriptions

Name	Description
Short Name	A short name to identify the Media Server cluster. Maximum: 6 alphanumeric characters. Example: MSC1, MSC2.
Long Name	A longer more descriptive name to identify the Media Server. Maximum: 32 alphanumeric characters
Primary Server	Select the Avaya Media Server network element. This list contains only the media server network elements that do not belong to any cluster. You must specify a primary server.
Secondary Server	If this cluster has two or more Avaya Media Servers, you must specify a secondary server. Otherwise, leave this field blank.
Role	Select role for this media server cluster. Choices are: • CONFERENCING ONLY • RECORDING ONLY

Name	Description
	• CONFERENCING AND RECORDING
Available	Displays the available media servers that can be added to this cluster. To add a media server to this cluster, select the media server you want to add, and then click **>>**.
Used	Displays the media servers that belong to this cluster. To remove a media server from this cluster, select the media server you want to remove, and then click **<<**.

Related Links

Adding a media server cluster on page 281

Modifying a media server cluster

About this task

Use this procedure to modify a media server cluster.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters**.
2. In the Media Server Clusters window, select the media server cluster you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Media Server Cluster dialog box, make your changes.
5. When finished, click **Apply**.

Deleting a media server cluster

About this task

Use this procedure to delete a media server cluster.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters**.
2. In the Media Server Clusters window, select the media server cluster you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Modifying the default media server cluster

About this task

Use this procedure to specify the default media server cluster.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Default Cluster**.
2. In the Media Server Default Cluster dialog box, select the default media server cluster.
3. When finished, click **Ok**.

Modifying the database replication settings for a media server cluster

About this task

Use this procedure to modify the database replication settings for a media server cluster.

Note:

If you have two or more media servers in one media server cluster, you must enable replication settings.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > Replication Settings**.
2. In the Media Server Cluster Replication Settings dialog box, enter the appropriate information.
3. When finished, click **Apply**.

Modifying the audio codec settings for a media server cluster

About this task

Use this procedure to modify the audio codec settings for a media server cluster.

Note:

To ensure compatibility for all of your clients, enable the G.711 codec. (This codec is enabled by default.)

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > Audio Codec Settings**.
2. In the Media Server Cluster Audio Codec Settings dialog box, administer the appropriate settings. For more information, see Media Server Cluster Audio Codec Settings dialog box field descriptions on page 284.
3. When finished, click **Apply**.

Related Links

Media Server Cluster Audio Codec Settings dialog box field descriptions on page 284

Media Server Cluster Audio Codec Settings dialog box field descriptions

Name	Description
Available	The list of available (but not enabled) audio codecs currently installed on the network. The media server supports the following audio codecs: ITU-T G.711 A-Law, ITU-T G.711 U-Law, ITU-T G.722, and ITU-T G.729.
Enabled	The list of audio codecs currently active on the network. **Note:** To ensure compatibility for all of your clients, enable the G.711 codec. (This codec is enabled by default.)
PTimes	The audio codec packet times (PTimes). You must select at least one PTimes value for each audio codec. For each codec type, the options are 10 ms, 20 ms, 30 ms, and 60 ms. The default PTime is 20 ms. You can change the default PTime for each codec.
Silence Suppression	Allows you to enable/disable silence suppression for the associated codec.

Related Links

Modifying the audio codec settings for a media server cluster on page 283

Modifying the recording trunk codec settings

About this task

Use this task to modify the recording trunk codec settings for all media servers clusters.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Recording Trunk Codec Settings**.
2. In the **Recording Trunk Codec Settings** dialog box, administer to the appropriate settings. For more information, see Recording Trunk Codec Settings dialog box field descriptions on page 285.
3. When finished, click **Apply**.

Related Links

Recording Trunk Codec Settings dialog box field descriptions on page 285

Recording Trunk Codec Settings dialog box field descriptions

Name	Description
Enabled	The list of recording trunk codecs currently active on the network.
Up button	Move up the selected codec in the list.
Down button	Move down the selected codec in the list.

Related Links

Modifying the recording trunk codec settings on page 285

Modifying the cascading trunk codec settings

About this task

Use this task to modify the cascading trunk codec settings for all media servers clusters.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Cascading Trunk Codec Settings**.
2. In the **Cascading Trunk Codec Settings** dialog box, administer to the appropriate settings. For more information, see Cascading Trunk Codec Settings dialog box field descriptions on page 286.
3. When finished, click **Apply**.

Related Links

Cascading Trunk Codec Settings dialog box field descriptions on page 286

Cascading Trunk Codec Settings dialog box field descriptions

Name	Description
Enabled	The list of cascading trunk codecs currently active on the network.
Up button	Move up the selected codec in the list.
Down button	Move down the selected codec in the list.

Related Links

Modifying the cascading trunk codec settings on page 285

Modifying the media port settings for a media server cluster

About this task

Use this procedure to modify the port range on each media server for audio, video, and conferencing.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > Media Ports Settings**.
2. In the Media Ports Settings dialog box, make your changes in the following fields:

   Start Port: Type a value from 6,000 to 26,798. Default value: 6,000.

   End Port: Type a value from 14,000 to 42,598. Default value: 42,598.

   Note:

   The total range must be greater than or equal to 15,800 ports. You cannot save a setting that is less than 15,800.
3. When finished, click **Apply**.

Modifying the DSCP settings for a media server cluster

About this task

Use this procedure to modify the DSCP settings for a media server cluster.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > DSCP Settings**.
2. In the DSCP Settings dialog box, make your changes.
3. When finished, click **Apply**.

Modifying the video settings for a media server cluster

About this task

Use this procedure to modify the video settings for a media server cluster.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > Video Settings**.
2. In the Media Server Cluster Video Settings dialog box, administer the appropriate settings. For more information, see Media Server Cluster Video Settings dialog box field descriptions on page 287.
3. When finished, click **Apply**.

Related Links

Media Server Cluster Video Settings dialog box field descriptions on page 287

Media Server Cluster Video Settings dialog box field descriptions

Name	Description
Dynamic Thinning	When this setting is enabled, the Avaya media server can “thin” SVC layers of video stream from the Avaya media server endpoints according to the input stream bit rate and estimated outgoing bandwidth.
H.264 AVC/SVC Relay	When this setting is enabled, the Avaya media server can relay video (AVC or SVC video) streams. When this setting is disabled, all conferences hosted on the Avaya media server will be audio only.

Related Links

Modifying the video settings for a media server cluster on page 287

Modifying the trace file history settings for a media server cluster

About this task

Use this procedure to set the trace file history for a media server cluster. The range for this setting is 0 to 20. By default, the Avaya media server cluster stores five debug log files. For example, if the trace file history is set to 5, and the current log file is VidMPDebug.txt, the history files are VidMPDebug.txt.0.bak, VidMPDebug.txt.1.bak, VidMPDebug.txt.2.bak, VidMPDebug.txt.3.bak, and VidMPDebug.txt.4.bak. Every time the media server cluster needs to store a new debug file in history, the oldest debug file is removed.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > Trace History Settings**.
2. In the Media Server Cluster Trace History Settings dialog box, select the appropriate setting from the Trace file history box, . The range is 0 to 20.
3. Click **Apply**.

Modifying the comfort noise setting for a media server cluster

About this task

Use this procedure to specify the amount of background noise you want Avaya Aura® Conferencing to provide when no one is talking during a conference.

Note:

After you modify the comfort noise setting, you must restart the media server network element instance for the change to take effect.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > Comfort Noise Settings**.
2. In the Media Server Cluster Comfort Noise Settings dialog box, select the appropriate comfort noise setting.
3. When finished, click **Apply**.

Related Links

Media Server Cluster Comfort Noise Settings dialog box field descriptions on page 289

Media Server Cluster Comfort Noise Settings dialog box field descriptions

Name	Description
Comfort Noise	Select the amount of background noise you want Avaya Aura® Conferencing to provide when no one is talking during a conference. Choices are **Off** (no background noise), **Low**, **Medium**, and **High**.

Related Links

Modifying the comfort noise setting for a media server cluster on page 288

Associating a media server cluster with a location

Before you begin

- You must be logged into Provisioning Client.
- Media servers and media server clusters must be configured already on Element Manager Console.

About this task

Use this procedure to associate a media server cluster with a location. You may associate multiple locations to media server clusters. The media servers in the cluster will serve the associated locations.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Serving Locations** tab.
3. From the Media Server Cluster box, select the media server cluster you want to associate with a location.
4. In the Add locations area, select the check box of the location(s) to which you want to associate the selected media server cluster.
5. Click **Save**.

Related Links

Media Server Serving Locations tab field descriptions on page 269

Media Server Serving Locations tab field descriptions

Name	Description
Media Server Cluster	Specifies the media server cluster that you want to associate with a location. Only the media server clusters that are administered in Element Manager Console are displayed in this box.
Add locations	Displays the locations to which you can assign the selected media server cluster. A check mark next to a location indicates that the selected media server cluster is assigned to that location.

Related Links

Associating a media server cluster with a location on page 269

Assigning a media server cluster to a physical location (by media server cluster)

Before you begin

- You must be logged into Provisioning Client.
- Media servers and media server clusters must be configured already on Element Manager Console.

About this task

Use this procedure to associate a media server cluster with a physical location. This enables the conferencing server to select the appropriate media server cluster for media processing based on the end user's location.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Cluster Physical Location** tab.
3. From the Select by box, select **Media Server Cluster**.
4. From the Select Media Server Cluster box, select the media server cluster you want to assign to a location.
5. From the Physical Location box, select the appropriate location.
6. Click **Save**.

Related Links

Media Server Cluster Physical Location tab field descriptions on page 270

Media Server Cluster Physical Location tab field descriptions

Name	Description
Select by	Enables you to specify whether you want to manage the media server clusters by physical location or media server cluster name. Your choices: • **Location**: Enables you to manage the media server cluster by physical location. When you select this option, you can select the physical location for which you want to manage the media server clusters. • **Media Server Cluster**: Enables you to manage the media server cluster by name. When you select this option, you can select the media server cluster you want to manage.
Select Physical Location	Enables you to specify the physical location where you want to manage media server clusters. This field is displayed when you select **Location** from the Select by box.
Available Media Server Clusters	Displays the media server clusters that you can assign to the selected location. From this list box, you can select the media server cluster(s) that you want to assign to the selected location. This list box is displayed when you select **Location** from the Select by box.
Selected Media Server Clusters	Displays the media server clusters that you want to assign to the selected location. This list box is displayed when you select **Location** from the Select by box.
Select Media Server Cluster	Enables you to specify the media server cluster that you want to manage. This field is displayed when you select **Media Server Cluster** from the Select by box.
Physical Location	Enables you to specify the physical location to which you want to assign the selected media server cluster. This field is displayed when you select **Media Server Cluster** from the Select by box.

Button	Description
Copy all	Moves all of the media server clusters displayed in the Available Media Server Clusters list box into the Selected Media Server Clusters list box.
Copy	Moves the selected media server cluster in the Available Media Server Clusters list box into the Selected Media Server Clusters list box.
Remove	Moves the selected media server cluster in the Selected Media Server Clusters list box into the Available Media Server Clusters list box.
Remove All	Moves all of the media server clusters displayed in the Selected Media Server Clusters list box into the Available Media Server Clusters list box.

Related Links

Assigning a media server cluster to a physical location (by media server cluster) on page 272

Assigning a media server cluster to a physical location (by location)

Before you begin

- You must be logged into Provisioning Client.
- Media servers and media server clusters must be configured already on Element Manager Console.

About this task

Use this procedure to associate a media server cluster with a physical location. This enables the conferencing server to select the appropriate media server cluster for media processing based on the end user's location.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Cluster Physical Location** tab.
3. From the Select by box, select **Location**.
4. From the Select Physical Location box, select the location to which you want to assign a media server cluster.
5. From the Available Media Server Clusters box, select the appropriate media server cluster, and then click **Copy**. If you want to assign all available media server clusters, click **Copy all**.
6. Click **Save**.

Configuring media server clusters for an Event conference

Before you begin

- You must be logged into Provisioning Client.
- Media server clusters must be configured already in Element Manager Console.

About this task

Use this procedure to associate a media server cluster with an Event conference.

Note:

The media server clusters you specify can only be used for Event conferences.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Clusters for Event Conference** tab.
3. From the Available Media Server Clusters box, select the appropriate media server cluster(s), and then click **Copy**. If you want to assign all media server clusters, click **Copy all**.
4. Click **Save**.

Related Links

Media Server Clusters for Event Conference field descriptions on page 279

Media Server Clusters for Event Conference field descriptions

Name	Description
Available Media Server Clusters	Displays the media server clusters that you can assign to the Event conference. From this list box, you can select the media server cluster(s) that you want to assign to the event conference.
Selected Media Server Clusters	Displays the media server clusters that you want to assign to the Event conference.

Button	Description
Copy all	Moves all of the media server clusters displayed in the Available Media Server Clusters list box into the Selected Media Server Clusters list box.
Copy	Moves the selected media server cluster in the Available Media Server Clusters list box into the Selected Media Server Clusters list box.

Button	Description
Remove	Moves the selected media server cluster in the Selected Media Server Clusters list box into the Available Media Server Clusters list box.
Remove All	Moves all of the media server clusters displayed in the Selected Media Server Clusters list box into the Available Media Server Clusters list box.

Related Links

Configuring media server clusters for an Event conference on page 279

Chapter 29: Managing Web Conferencing

A single document conversion server (DCS) or multiple DCSs?

You can add several Document Conversion Servers (DCSs) to your deployment, depending on your needs and the expected traffic. You can add, modify, and delete DCSs using the Element Manager interface. You can also use the Element Manager interface to start, stop, deploy, and undeploy each DCS instance, as you would any other network element.

The load balancing aspect of the DCS uses the concepts of locations and pools. These are optional configuration settings and are only relevant in a deployment with several DCS servers. You can assign a DCS to a particular location. You can also assign a DCS to a pool of DCSs. In addition, you can assign a particular DCS to be the default DCS for your system. When Avaya Aura® Conferencing chooses which DCS to use for a particular conference, it uses the following process:

- Avaya Aura® Conferencing checks if there is a DCS provisioned to serve the user (conference owner) in their location.
- If there are still no DCS available, Avaya Aura® Conferencing uses the default DCS.
- If there is no location DCS available and no default DCS available, Avaya Aura® Conferencing checks for an available DCS in the pool.

As an aside, the default DCS can be part of the pool of DCSs, but the selection rules still apply.

You can assign DCS instances to particular locations using the Provisioning Client interface. So, the typical order for managing your DCS is that you create and deploy DCS instances using Element Manager. Then you assign the deployed DCSs to particular locations using the Provisioning Client.

Managing document conversion servers

The document conversion server (DCS) is a Linux® server that converts Microsoft Word, Microsoft PowerPoint, Microsoft Excel, and other document types, such as .PDF and .TXT into a format for content sharing using web conferencing. The DCS also converts graphics, such as .PNG or .JPG images. Avaya Aura® Conferencing 8.0 hosts the document conversion server as a network element.

Use the procedures in this section to add, modify, and delete a document conversion server.

Note:

To upgrade the document conversion server, see *Upgrading Avaya Aura® Conferencing 8.0*, which is available from Avaya Support.

Related Links

Adding a web conferencing document conversion server on page 296
Modifying a web conferencing document conversion server on page 297
Modifying the configuration parameters of a document conversion server on page 297
Deleting a web conferencing document conversion server on page 300
Configuring the default document conversion server on page 300

Adding a web conferencing document conversion server

About this task

Use this procedure to add a web conferencing document conversion server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Document Conversion Servers**.
2. In the Document Conversion Servers window, click **Add (+)**.
3. In the Add Document Conversion Server dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Next steps

When you add a new network element, it is likely that you are also changing IP addresses and reconfiguring the NTP, DNS, and Syslog server. If you are making so many changes in your Avaya Aura® Conferencing system, you should always check if the Access Control List (ACL) is applied to the network element. The ACL manages the rules for internal and external system connections. If the ACL is applied to the network element, you should apply it to the new network element. For instructions on checking if it is applied and then applying it, see *Deploying Avaya Aura® Conferencing*, which is available from https://support.avaya.com/. The *Deploying Avaya Aura® Conferencing* guide also describes how to change IP addresses, reconfigure servers, and so on.

Related Links

Managing document conversion servers on page 295
Add/Edit Document Conversion Server field descriptions on page 296

Add/Edit Document Conversion Server field descriptions

Name	Description
ShortName	A short name to identify the DCS.
LongName	A longer, more descriptive name to identify the DCS.
Base Port	The port that the DCS uses (46000).

Name	Description
FPM	Displays **Element Manager**.
Access Key	
HTTPS Certificate	Choose the FQDN security certificate to be used by this DCS.
DCS Service FQDN	FQDN for the document conversion server.

Button	Description
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to clear your changes.

Related Links

Adding a web conferencing document conversion server on page 296

Modifying a web conferencing document conversion server

About this task

Use this procedure to modify a web conferencing document conversion server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Document Conversion Servers**.
2. In the Document Conversion Servers window, select the document conversion server you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Document Conversion Server dialog box, make your changes.
5. When finished, click **Apply**.

Related Links

Managing document conversion servers on page 295
Add/Edit Document Conversion Server field descriptions on page 296

Modifying the configuration parameters of a document conversion server

About this task

Use this procedure to modify the configuration parameters of a document conversion server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers** > ***<Document Conversion Server name>*** > **Configuration Parameters**.
2. In the Document Conversion Server Configuration Parameters window, make your changes. Use the **Parm Group** drop-down list box to access the parameter(s) you want to modify.

   For more information, see Document Conversion Server Configuration Parameters window field descriptions on page 298.

Related Links

Managing document conversion servers on page 295
Document Conversion Server Configuration Parameters window field descriptions on page 298

Document Conversion Server Configuration Parameters window field descriptions

Parameter group	Configuration parameter	Description
Dcs	dpi	This parameter specifies the resolution (dots per inch) of converted documents. Avaya recommends using the default settings. This parameter is used for Microsoft Excel, PDF and Microsoft Word document conversions. Default: 120
	pageLimit	This parameter specifies the limit of the number of document pages that can be uploaded to the Document Conversion Server (DCS). The DCS fails if a document with a greater number of pages is uploaded. Default: 300
	png_size_limit	This parameter specifies the maximum file size of shared images in the Portable Network Graphic (PNG) format on the Collaboration Agent interface. If a PNG file is greater than this size, Avaya Aura® Conferencing saves the file as a Joint Photographic Group (JPG) file. Default: 102400 bytes
	ppt_height	This parameter specifies the height of Microsoft Powerpoint slides that are displayed on the Collaboration Agent interface. Default: 768 pixels
	ppt_width	This parameter specifies the width of Microsoft Powerpoint slides that are displayed on the Collaboration Agent interface. Default: 1024 pixels

Parameter group	Configuration parameter	Description
TLSAuth	Disable hostname verifier	This parameter enables or disables hostname verification check on certificate validation. Range: true or false Default: false
	EnableCRL	This parameter enables CRL retrieval for certificate revocation status. Range: true or false Default: false
	EnableOCSP	This parameter enables OCSP retrieval for certificate revocation status. Range: true or false Default: false
	EnforceTLSMutualAuthForHTTPS	This parameter enforces TLS Mutual Authentication for HTTP interface. Range: true or false Default: false
	PermitNoRevocationValidateResp	This parameter permits access, if no certificate revocation validation response. Range: true or false Default: true
Cross-Domain Policy	AllowAccessFromDomains	This parameter specifies the list of domains to which Avaya Aura® Conferencing (AAC) permits access to its Adobe Flash-based features. If a domain is not in this list, the clients in this domain will not be able to access features such as Web Collaboration or the document library. By default, Avaya Aura® Conferencing permits access for any domain. However, if Avaya Aura® Conferencing administrators wish to harden their system, they can limit access, by specifying certain domains and/or IP addresses, with multiple values separated by a comma.
WebServer	EnableAccessLogs	This parameter enables Tomcat Access/Error logs. Range: true, false Default: false

Related Links

Modifying the configuration parameters of a document conversion server on page 297

Deleting a web conferencing document conversion server

In order to fully delete a document conversion server (DCS), you must delete the DCS instance and delete the DCS network element (NE).

About this task

Use this procedure to delete a web conferencing document conversion server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Document Conversion Servers** > ***<DCS name>*** > **Instance**.
2. Click **Delete (-)**.
3. In the Confirmation dialog box, click **Yes**.
4. Navigate to **Feature Server Elements** > **Document Conversion Servers**.
5. In the Document Conversion Servers window, select the document conversion server you want to delete from the list of document conversion servers.
6. Click **Delete (-)**.
7. In the Confirmation dialog box, click **Yes**.

Related Links

Managing document conversion servers on page 295

Configuring the default document conversion server

About this task

Use this procedure to configure a default document conversion server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Document Conversion Servers**.
2. Select **Default Document Conversion Server**.
3. From the **Document Conversion Server** drop-down list, select a document conversion server.
4. Click **Apply**.

Related Links

Managing document conversion servers on page 295

Managing document conversion server instances

You can also use the Element Manager interface to start, stop, deploy, and undeploy each document conversion server (DCS) instance, as you would any other network element.

Related Links

Deploying a document conversion server instance on page 301
Undeploying a document conversion server instance on page 301
Starting a document conversion server instance on page 302
Stopping a document conversion server instance on page 302
Restarting a document conversion server instance on page 302
Killing a document conversion server instance on page 303
Modifying a document conversion server instance on page 303

Deploying a document conversion server instance

About this task

Use this task to deploy a document conversion server instance.

Procedure

1. In the navigation pane of Element Manager console, select **Feature Server Elements** > **Document Conversion Servers** > ***<Document conversion server name>*** > **NE Maintenance**.
2. In the Document Conversion Server Maintenance dialog, select the instance that you want to deploy.
3. Click **Deploy**.

Related Links

Managing document conversion server instances on page 301

Undeploying a document conversion server instance

About this task

Use this task to undeploy a document conversion server instance.

Procedure

1. In the navigation pane of Element Manager console, select **Feature Server Elements** > **Document Conversion Servers** > ***<Document conversion server name>*** > **NE Maintenance**.
2. In the Document Conversion Server Maintenance dialog, select the instance that you want to undeploy.

3. Click **Undeploy**.

Related Links

Managing document conversion server instances on page 301

Starting a document conversion server instance

About this task

Use this task to start a document conversion server instance.

Procedure

1. In the navigation pane of Element Manager console, select **Feature Server Elements** > **Document Conversion Servers** > ***<Document conversion server name>*** > **NE Maintenance**.
2. In the Document Conversion Server Maintenance dialog, select the instance that you want to start.
3. Click **Start**.

Related Links

Managing document conversion server instances on page 301

Stopping a document conversion server instance

About this task

Use this task to stop a document conversion server instance.

Procedure

1. In the navigation pane of Element Manager console, select **Feature Server Elements** > **Document Conversion Servers** > ***<Document conversion server name>*** > **NE Maintenance**.
2. In the Document Conversion Server Maintenance dialog, select the instance that you want to stop.
3. Click **Stop**.

Related Links

Managing document conversion server instances on page 301

Restarting a document conversion server instance

About this task

Use this task to restart a document conversion server instance.

Procedure

1. In the navigation pane of Element Manager console, select **Feature Server Elements** > **Document Conversion Servers** > ***<Document conversion server name>*** > **NE Maintenance**.
2. In the Document Conversion Server Maintenance dialog, select the instance that you want to restart.
3. Click **Restart**.

Related Links

Managing document conversion server instances on page 301

Killing a document conversion server instance

About this task

Use this task to kill a document conversion server instance.

Procedure

1. In the navigation pane of Element Manager console, select **Feature Server Elements** > **Document Conversion Servers** > ***<Document conversion server name>*** > **NE Maintenance**.
2. In the Document Conversion Server Maintenance dialog, select the instance that you want to kill.
3. Click **Kill**.

Related Links

Managing document conversion server instances on page 301

Modifying a document conversion server instance

About this task

Use this procedure to modify a document conversion server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers** > ***<Document Conversion Server name>*** > **Instance**.
2. In the Document Conversion Server Instance window, select the server instance you want to modify.
3. Click **Edit (-/+)**.

4. In the Edit Document Conversion Server Instance dialog box, make your changes. To change the Eng Parms, click **Advanced**.
5. When finished, click **Apply**.

Example

This document does not contain an exhaustive description of each engineering parameter. Avaya recommends maintaining the parameter default values. For reference only, the following table describes the Dcs engineering parameters.

Parameter name	Value
DcsMaxTuples	This parameter specifies the maximum number of tuples that the DCS in memory database table can have. The default settings are: • For a small deployment: 1000 • For a medium deployment: 1500 • For a large deployment: 2000
graceful_shutdown_time	This parameter specifies the time allowed for the DCS to gracefully shutdown all running jobs (if any) before coming to a stop. The default setting is 5 seconds.
max_active_jobs	This parameter specifies the number of threads assigned to the DCS for conversion. The default settings is 4. This value is required for a large configuration but should be configured to 2 or 1 for a medium or small configuration. The default settings are: • For a small deployment: 1 • For a medium deployment: 2 • For a large deployment: 4
max_job_time	This parameter specifies the maximum time allowed by the DCS for a given conversion before it times out. The default setting is 1200000 seconds (20 minutes).
max_jobs	This parameter specifies the maximum number of active jobs that can run at any point in time. The default setting is 25.
upload_max_filesize	This parameter specifies the maximum upload file size allowed for conversion by the DCS. The default setting is 30720000 bytes (30Mb)

Parameter name	Value
	Note: This parameter does not apply to image uploads. For image uploads, for both PNG and JPG formats, the maximum file size limit is 12 Mb and the maximum resolution allowed is 23 mega pixels in total. This is not configurable through the DCS.

Note:

All changes to the Engineering Parameters require a restart.

Related Links

Managing document conversion server instances on page 301

Assigning document conversion servers to locations

For the purposes of load balancing, you must assign document conversion servers (DCSs) to locations. This way, you can insure that server selection is based on load performance factor and that Avaya Aura® Conferencing always distributes conversion requests in such a way as to minimize the conversion time.

You can assign a DCS to a location using the Provisioning Client. This functionality is located in the WCS Clusters section of the Provisioning Client. For more information, see:

- Assigning WCS clusters to serving locations on page 323
- WCS cluster/DCS serving locations tab field descriptions on page 323

Managing Web Conferencing Management Servers

Adding a web conferencing management server

About this task

Use this procedure to add a web conferencing management server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Management Servers**.
2. In the Web Conferencing Management Servers window, click **Add (+)**.

3. In the Add Web Conferencing Management Server dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Next steps

When you add a new network element, it is likely that you are also changing IP addresses and reconfiguring the NTP, DNS, and Syslog server. If you are making so many changes in your Avaya Aura® Conferencing system, you should always check if the Access Control List (ACL) is applied to the network element. The ACL manages the rules for internal and external system connections. If the ACL is applied to the network element, you should apply it to the new network element. For instructions on checking if it is applied and then applying it, see *Deploying Avaya Aura® Conferencing*, which is available from https://support.avaya.com/. The *Deploying Avaya Aura® Conferencing* guide also describes how to change IP addresses, reconfigure servers, and so on.

Related Links

Add/Edit Web Conferencing Management Server dialog box field descriptions on page 306

Add/Edit Web Conferencing Management Server dialog box field descriptions

Name	Description
Short Name	(Read-only) The short name of the network element — maximum of 6 characters.
Long Name	The long name of the network element — maximum of 32 characters.
Base Port	A range of 100 ports reserved off the base port for use by the network element. Range 1100–654000
FPM	Displays **Element Manager**.
Enable HTTP Port	(Checkbox) Select to enable the Web Conferencing Management Server HTTP port.
HTTP Listen Port	Specifies HTTP port.
HTTPS Listen Port	Specifies HTTPS port.
HTTPS Certificate	The private key and certificate pair that the Web Conferencing Management Server HTTPS server uses (select from the list).

Related Links

Adding a web conferencing management server on page 305

Modifying a web conferencing management server

About this task

Use this procedure to modify a web conferencing management server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Management Servers**.
2. In the Web Conferencing Management Servers window, select the web conferencing management server you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Web Conferencing Management Server dialog box, make your changes.
5. When finished, click **Apply**.

Deleting a web conferencing management server

About this task

Use this procedure to delete a web conferencing management server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Management Servers**.
2. In the Web Conferencing Management Servers window, select the web conferencing management server you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Modifying the configuration parameters of a web conferencing management server

About this task

Use this procedure to modify the configuration parameters of a web conferencing management server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Management Servers > <*Web conferencing management server name*> > Configuration Parameters**.
2. In the Web Conferencing Management Server Configuration Parameters window, make your changes. Use the **Parm Group** drop-down list box to access the parameter(s) you want to modify.

   For more information, see Web Conferencing Management Server Configuration Parameters window field descriptions on page 308.

Related Links

Web Conferencing Management Server Configuration Parameters window field descriptions on page 308

Web Conferencing Management Server Configuration Parameters window field descriptions

Parameter group	Configuration parameter	Description
HTTPDoS	Enable MMS DoS filter	This parameter enables or disables the HTTP Denial of Service protection feature for the WCMS. Range: true or false Default: false
TLSAuth	Disable hostname verifier	This parameter enables or disables hostname verification check on certificate validation. Range: true or false Default: false
	EnableCRL	This parameter enables CRL retrieval for certificate revocation status. Range: true or false Default: false
	EnableOCSP	This parameter enables OCSP retrieval for certificate revocation status. Range: true or false Default: false
	EnforceTLSMutual-AuthForHTTPS	This parameter enforces TLS Mutual Authentication for HTTP interface. Range: true or false Default: false
	EnforceTLSMutual-AuthForSIP	This parameter enforces TLS Mutual Authentication for SIP interface. Range: true or false Default: false
	PermitIfNoRevocationValidateResp	This parameter permits access, if no certificate revocation validation response. Range: true or false Default: true
	SyncOCSPForSIP	This parameter enables synchronous OCSP query for SIP interface. Range: true or false

Comments? infodev@avaya.com

Parameter group	Configuration parameter	Description
		Default: false
Cross-Domain Policy	AllowAccessFromDomains	This parameter specifies the list of domains to which Avaya Aura® Conferencing (AAC) permits access to its Adobe Flash-based features. If a domain is not in this list, the clients in this domain will not be able to access features such as Web Collaboration or the document library. By default, Avaya Aura® Conferencing permits access for any domain. However, if Avaya Aura® Conferencing administrators wish to harden their system, they can limit access, by specifying certain domains and/or IP addresses, with multiple values separated by a comma.
WebServer	EnableAccessLogs	This parameter enables Tomcat Access/Error logs. Range: true, false

Related Links

Modifying the configuration parameters of a web conferencing management server on page 307

Modifying the meeting event processor for a web conferencing management server

About this task

Use this procedure to modify the meeting event processor for a web conferencing management server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Management Servers > <*Web conferencing management server name*> > Meeting Event Processing**.
2. In the Web Conferencing Management Server Meeting Event Processing dialog box, select the appropriate meeting event processor.
3. Click **Apply**.

Managing Web Conferencing Management Server Instances

Adding a web conferencing management server instance

About this task

Use this procedure to add a web conferencing management server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Management Servers > <*Web conferencing management server name*> > Instance**.
2. In the Web Conferencing Management Servers Instance window, click **Add (+)**.
3. In the Add Web Conferencing Management Server Instance dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Modifying a web conferencing management server instance

About this task

Use this procedure to modify a web conferencing management server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Management Servers > <*Web conferencing management server name*> > Instance**.
2. In the Web Conferencing Management Server Instance window, select the web conferencing management server instance you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Web Conferencing Management Server Instance dialog box, make your changes. To change the Eng Parms, click **Advanced**.
5. When finished, click **Apply**.

Deleting a web conferencing management server instance

About this task

Use this procedure to delete a web conferencing management server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Management Servers > <*Web conferencing management server name*> > Instance**.
2. In the Web Conferencing Management Server Instance window, select the web conferencing management server instance you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Deploying a web conferencing management server instance

About this task

Use this procedure to deploy a web conferencing management server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Management Servers > <*Web conferencing management server name*> > NE Maintenance**.
2. In the Web Conferencing Management Server Maintenance dialog box, select the instance you want to deploy.
3. Click **Deploy**.

Undeploying a web conferencing management server instance

About this task

Use this procedure to undeploy a web conferencing management server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Management Servers > <*Web conferencing management server name*> > NE Maintenance**.
2. In the Web Conferencing Management Server Maintenance dialog box, select the instance you want to undeploy.
3. Click **Undeploy**.

Starting a web conferencing management server instance

About this task

Use this procedure to start a web conferencing management server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Management Servers > <*Web conferencing management server name*> > NE Maintenance**.
2. In the Web Conferencing Management Server Maintenance dialog box, select the instance you want to start.
3. Click **Start**.

Stopping a web conferencing management server instance

About this task

Use this procedure to stop a web conferencing management server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Management Servers > <*Web conferencing management server name*> > NE Maintenance**.
2. In the Web Conferencing Management Server Maintenance dialog box, select the instance you want to stop.
3. Click **Stop**.

Restarting a web conferencing management server instance

About this task

Use this procedure to restart a web conferencing management server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Management Servers > <*Web conferencing management server name*> > NE Maintenance**.
2. In the Web Conferencing Management Server Maintenance dialog box, select the instance you want to restart.
3. Click **Restart**.

Killing a web conferencing management server instance

About this task

Use this procedure to kill a web conferencing management server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Management Servers > <*Web conferencing management server name*> > NE Maintenance**.
2. In the Web Conferencing Management Server Maintenance dialog box, select the instance you want to kill.
3. Click **Kill**.

Viewing the details for a web conferencing management server instance

About this task

Use this procedure to view the details for a web conferencing management server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Management Servers > <*Web conferencing management server name*> > NE Maintenance**.

2. In the Web Conferencing Management Server Maintenance dialog box, select the instance for which you want to view the details.
3. Click **Details**.

Managing Web Conferencing Servers

Adding a web conferencing server

About this task

Use this procedure to add a web conferencing server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Servers and Clusters > Web Conferencing**.
2. In the Web Conferencing Servers window, click **Add (+)**.
3. In the Add Web Conferencing Server dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Next steps

When you add a new network element, it is likely that you are also changing IP addresses and reconfiguring the NTP, DNS, and Syslog server. If you are making so many changes in your Avaya Aura® Conferencing system, you should always check if the Access Control List (ACL) is applied to the network element. The ACL manages the rules for internal and external system connections. If the ACL is applied to the network element, you should apply it to the new network element. For instructions on checking if it is applied and then applying it, see *Deploying Avaya Aura® Conferencing*, which is available from https://support.avaya.com/. The *Deploying Avaya Aura® Conferencing* guide also describes how to change IP addresses, reconfigure servers, and so on.

Related Links

Add/Edit Web Conferencing Server dialog box field descriptions on page 313

Add/Edit Web Conferencing Server dialog box field descriptions

Name	Description
Short Name	(Read-only) The short name of the network element — maximum of 6 characters.
Long Name	The long name of the network element — maximum of 32 characters.
Base Port	A range of 100 ports reserved off the base port for use by the network element. Range 1100–654000

Name	Description
FPM	Displays **Element Manager**.
Service Address	The internal OAM (default) service address used by the network element.
Enable HTTP Port	(Checkbox) Select to enable the Web Conferencing Server HTTP port.
FQDN	FQDN for the Web Conferencing Server.

Related Links

Adding a web conferencing server on page 313

Modifying a web conferencing server

About this task

Use this procedure to modify a web conferencing server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Servers and Clusters > Web Conferencing**.
2. In the Web Conferencing Servers window, select the web conferencing server you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Web Conferencing Server dialog box, make your changes.
5. When finished, click **Apply**.

Deleting a web conferencing server

About this task

Use this procedure to delete a web conferencing server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Servers and Clusters > Web Conferencing**.
2. In the Web Conferencing Servers window, select the web conferencing server you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Modifying the configuration parameters of a web conferencing server

About this task

Use this procedure to modify the configuration parameters of a web conferencing server.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Servers and Clusters > Web Conferencing Servers > <*Web conferencing server name*> > Configuration Parameters**.
2. In the Web Conferencing Server Configuration Parameters window, make your changes. Use the **Parm Group** drop-down list box to access the parameter(s) you want to modify.

   For more information, see Web Conferencing Server Configuration Parameters window field descriptions on page 315.

Related Links

Web Conferencing Server Configuration Parameters window field descriptions on page 315

Web Conferencing Server Configuration Parameters window field descriptions

Parameter group	Configuration parameter	Description
HTTPDoS	Enable MMS DoS filter	This parameter enables or disables the HTTP Denial of Service protection feature for the WCS. Range: true or false Default: false
PlaybackServer	DownloadThrottlingKBPS	This parameter indicates throttling for downloading recordings. Default: 0 (Off/No throttling)
	MaxLength	This parameter specifies the length of the longest recording. It defaults to 8 hours and recording is stopped automatically once this limit is reached. The longest possible recording is 24 hours. Default: 8 hours
	StreamingThrottlingKBPS	This parameter indicates throttling for online playback. Default: 1024 kbps
TLSAuth	Disable hostname verifier	This parameter enables or disables hostname verification check on certificate validation. Range: true or false

Parameter group	Configuration parameter	Description
		Default: false
	EnableCRL	This parameter enables CRL retrieval for certificate revocation status. Range: true or false Default: false
	EnableOCSP	This parameter enables OCSP retrieval for certificate revocation status. Range: true or false Default: false
	EnforceTLSMutual-AuthForHTTPS	This parameter enforces TLS Mutual Authentication for HTTP interface. Range: true or false Default: false
	EnforceTLSMutual-AuthForSIP	This parameter enforces TLS Mutual Authentication for SIP interface. Range: true or false Default: false
	PermitIfNoRevocationValidateResp	This parameter permits access, if no certificate revocation validation response. Range: true or false Default: true
	SyncOCSPForSIP	This parameter enables synchronous OCSP query for SIP interface. Range: true or false Default: false
Cross-Domain Policy	AllowAccessFromDomains	This parameter specifies the list of domains to which Avaya Aura® Conferencing (AAC) permits access to its Adobe Flash-based features. If a domain is not in this list, the clients in this domain will not be able to access features such as Web Collaboration or the document library. By default, Avaya Aura® Conferencing permits access for any domain. However, if Avaya Aura® Conferencing administrators wish to harden their system, they can limit access, by specifying certain domains and/or IP addresses, with multiple values separated by a comma.
WebServer	EnableAccessLogs	This parameter enables Tomcat Access/Error logs. Range: true, false

Related Links

Modifying the configuration parameters of a web conferencing server on page 315

Managing Web Conferencing Server Instances

Adding a web conferencing server instance

About this task

Use this procedure to add a web conferencing server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Servers and Clusters > Web Conferencing Servers > <*Web conferencing server name*> > Instance**.
2. In the Web Conferencing Server Instance window, click **Add (+)**.
3. In the Add Web Conferencing Server Instance dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Modifying a web conferencing server instance

About this task

Use this procedure to modify a web conferencing server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Servers and Clusters > Web Conferencing Servers > <*Web conferencing server name*> > Instance**.
2. In the Web Conferencing Server Instance window, select the web conferencing server instance you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Web Conferencing Server Instance dialog box, make your changes. To change the Eng Parms, click **Advanced**.
5. When finished, click **Apply**.

Deleting a web conferencing server instance

About this task

Use this procedure to delete a web conferencing server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Servers and Clusters > Web Conferencing Servers > <*Web conferencing server name*> > Instance**.
2. In the Web Conferencing Server Instance window, select the web conferencing server instance you want to delete.
3. Click **Delete (-)**.
4. In the Confirmation dialog box, click **Yes**.

Deploying a web conferencing server instance

About this task

Use this procedure to deploy a web conferencing server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Servers and Clusters > Web Conferencing Servers > <*Web conferencing server name*> > NE Maintenance**.
2. In the Web Conferencing Server Maintenance dialog box, select the instance you want to deploy.
3. Click **Deploy**.

Undeploying a web conferencing server instance

About this task

Use this procedure to undeploy a web conferencing server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Servers and Clusters > Web Conferencing Servers > <*Web conferencing server name*> > NE Maintenance**.
2. In the Web Conferencing Server Maintenance dialog box, select the instance you want to undeploy.
3. Click **Undeploy**.

Starting a web conferencing server instance

About this task

Use this procedure to start a web conferencing server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Servers and Clusters > Web Conferencing Servers > <*Web conferencing server name*> > NE Maintenance**.
2. In the Web Conferencing Server Maintenance dialog box, select the instance you want to start.
3. Click **Start**.

Stopping a web conferencing server instance

About this task

Use this procedure to stop a web conferencing server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Servers and Clusters > Web Conferencing Servers > <*Web conferencing server name*> > NE Maintenance**.
2. In the Web Conferencing Server Maintenance dialog box, select the instance you want to stop.
3. Click **Stop**.

Restarting a web conferencing server instance

About this task

Use this procedure to restart a web conferencing server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Servers and Clusters > Web Conferencing Servers > <*Web conferencing server name*> > NE Maintenance**.
2. In the Web Conferencing Server Maintenance dialog box, select the instance you want to restart.
3. Click **Restart**.

Killing a web conferencing server instance

About this task

Use this procedure to kill a web conferencing server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Servers and Clusters > Web Conferencing Servers > <*Web conferencing server name*> > NE Maintenance**.

2. In the Web Conferencing Server Maintenance dialog box, select the instance you want to kill.
3. Click **Kill**.

Viewing the details for a web conferencing server instance

About this task

Use this procedure to view the details for a web conferencing server instance.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Web Conferencing > Web Conferencing Servers and Clusters > Web Conferencing Servers > <*Web conferencing server name*> > NE Maintenance**.
2. In the Web Conferencing Server Maintenance dialog box, select the instance for which you want to view the details.
3. Click **Details**.

Managing Web Conferencing Server Clusters

Web Conferencing Server (WCS) clusters

Within the Avaya Aura® Conferencing environment, the concept of a 'cluster' provides a mechanism for Avaya Aura® Conferencing administrators to provision a collection of servers as one single server. This mechanism reduces the number of configuration tasks but also maximizes load balancing between the servers. In the 8.0 release, Avaya Aura® Conferencing supports the concept of a media server (MS) cluster and a Web Conferencing Server (WCS) cluster. In the Avaya Aura® Conferencing 8.0 release, WCS clusters replace WCS groups from previous releases.

When Avaya Aura® Conferencing chooses which WCS cluster to use for a particular conference, it uses the following process:

- Avaya Aura® Conferencing checks if there is a WCS cluster provisioned to serve the user (conference owner) in their location.
- If there are no WCS clusters available in the same location as the user, Avaya Aura® Conferencing searches for WCS clusters serving the user's location, and selects the least loaded WCS from amongst those clusters.
- If there are still no WCS available, Avaya Aura® Conferencing uses the default WCS cluster.

There are additional options available if you wish to ensure that users from a particular location use the system resources in another location.

Avaya Aura® Conferencing follows this process:

- When it chooses which WCS to use for hosting a conference.
- When it chooses which WCS to use for recording a conference.

- When it chooses which WCS to use for playing back a conference.
- When it chooses which WCS to use for encoding a conference that does not include web collaboration.

Encoding, within this context, refers to the process of processing a conference recording to convert it to a playable format. If the conference contains web collaboration, Avaya Aura® Conferencing uses the hosting server for the encoding process.

You must also provision dedicated WCS clusters if you wish to support event conferences. For more information about event conferences, see Event conferencing and media cascading on page 273.

Related Links

WCS clusters and the upgrade process on page 321
WCS clusters and Application Delivery Controller (ADC) functionality on page 321
Creating a new WCS cluster on page 322
Configuring the default cluster on page 322
Assigning WCS clusters to serving locations on page 323
Assigning WCS clusters to physical locations on page 324
Assigning WCS clusters to hosting locations on page 326
Configuring WCS clusters for event conferences on page 327

WCS clusters and the upgrade process

During the upgrade process from Avaya Aura® Conferencing Release 7.2 to Avaya Aura® Conferencing Release 8.0, Avaya Aura® Conferencing creates a WCS cluster for each WCS in your deployment. After the upgrade is complete, you must combine the WCS clusters into an appropriate configuration for your deployment. Additionally, if your deployment supports event conferencing, in most cases, you must manually re-configure and re-assign the appropriate WCS clusters for event conferences. The only exception to this rule is if your deployment consists of a single WCS cluster for event conferencing and this WCS cluster is only assigned to a single location.

Related Links

Web Conferencing Server (WCS) clusters on page 320

WCS clusters and Application Delivery Controller (ADC) functionality

Avaya Aura® Conferencing supports the A10 Network AX Series Application Delivery Controller and the Barracuda Load Balancer Application Delivery Controller, which provide advanced load balancing as well as reverse proxies for Web Collaboration as well as for the Audio/Video in Collaboration Agent clients.

If your deployment supports a reverse proxy controller that uses web sockets[3], you must enter a WCS service address in the **Cluster FQDN** field on the **Add Web Conferencing Server Cluster** dialog when you are creating a new WCS cluster. The WCS Cluster Service address/Cluster FQDN is the fully qualified domain name of the WCS cluster.

For more information about the **Add Web Conferencing Server Cluster** dialog, see Creating a new WCS cluster on page 322.

[3] WebSocket is a protocol providing full-duplex communications channels over a single TCP connection.

Related Links

Web Conferencing Server (WCS) clusters on page 320

Creating a new WCS cluster

About this task

Use the following procedure to create a new Web Conferencing Server (WCS) cluster.

Note:

A WCS can only be a member of a single WCS cluster.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers and Clusters** > **Web Conferencing Server Clusters**.
2. In the Web Conferencing Server Clusters window, click **Add (+)**.
3. In the Add Web Conferencing Server Cluster dialog box, complete the following fields:
   - **Short Name**
   - **Long Name**
   - **Cluster FQDN**: If your deployment includes a reverse proxy server, you must enter a value in this field. If your deployment does not include a reverse proxy server, you must leave this field blank. Avaya supports the A10 Application Delivery Controller for reverse proxy functionality in Avaya Aura® Conferencing.
4. From the **Available** panel, select a WCS.
5. Click the arrow **>>** button.

   The WCS is displayed in the **Used** panel and becomes a member of the WCS cluster.
6. Repeat these steps to add additional WCSs to the cluster.
7. Click **Apply**.

Related Links

Web Conferencing Server (WCS) clusters on page 320

Configuring the default cluster

Avaya Aura® Conferencing uses a default WCS cluster if there is no cluster assigned to a location or if there are no system resources available on the assigned WCS clusters.

Before you begin

Create at least one WCS cluster. See Creating a new cluster on page 322.

About this task

Use this task to configure a default WCS cluster.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers and Clusters** > **Default Web Conferencing Server Cluster**.
2. In the Default Web Conferencing Server Cluster window, select a value from the Default Web Conferencing Server Cluster drop-down list.
3. Click **Ok**.

Related Links

Web Conferencing Server (WCS) clusters on page 320

Assigning WCS clusters to serving locations

Before you begin

- You must be logged into Provisioning Client.
- Create at least one WCS cluster. See Creating a new cluster on page 322.
- Configure at least one location. See Adding a location on page 116.

About this task

If your deployment contains only one WCS cluster, you simply need to configure a default WCS cluster. However, if your deployment contains multiple WCS clusters, you must assign the WCS clusters to a serving location for communication with other network elements. Use the following procedure to assign a particular WCS server cluster to a location.

Procedure

1. In the Provisioning Client window, select **System Management** > **Routing** > **Web Conferencing Server Resources**.
2. Click the **WCS cluster/DCS serving locations** tab.
3. Select a location from the **Location** drop-down list.
4. From the **Available WCS Clusters** box, select the appropriate WCS server cluster, and then click **Copy**. If you want to assign all available WCS server clusters, click **Copy all**.
5. Click **Save**.
6. Repeat Steps 3 through 6 for each location.

Related Links

Web Conferencing Server (WCS) clusters on page 320
WCS cluster/DCS serving locations tab field descriptions on page 323

WCS cluster/DCS serving locations tab field descriptions

Name	Description
Location	For any Location you have configured on System Manager, you must add it manually to Provisioning

Name	Description
	Client. A location can be a physical site office location or a virtual collective of users.
Available WCS Clusters	Displays a list of provisioned WCS clusters.
Selected WCS Clusters	Displays the WCS servers assigned to the selected WCS cluster.
Document Conversion Server	If there is a Document Conversion Server (DCS) assigned to this location, it is displayed here.
Document Conversion Server for Event Conference	If there is a specific Document Conversion Server (DCS) for an event conference assigned to this location, it is displayed here.

Button	Description
Copy all	Moves all of the WCS servers displayed in the **Available WCS Clusters** box to the **Selected WCS Clusters** box.
Copy	Moves the selected WCS server displayed in the **Available WCS Clusters** box to the **Selected WCS Clusters** box.
Remove	Moves the selected WCS server in the **Selected WCS Clusters** box to the **Available WCS Clusters** box.
Remove all	Moves all of the WCS servers displayed in the **Selected WCS Clusters** box to the **Available WCS Clusters** box.
Save	Click **Save** to apply your changes.

Related Links

Assigning WCS clusters to serving locations on page 323

Assigning WCS clusters to physical locations

When Avaya Aura® Conferencing chooses a WCS cluster, it checks the WCS clusters configured for the serving location of the conference. If there are several suitable WCS clusters available in the serving location, Avaya Aura® Conferencing checks the WCS clusters configured for the physical location of the conference.

Before you begin

- You must be logged into Provisioning Client.
- Create at least one WCS cluster. See Creating a new cluster on page 322.
- Configure at least one location. See Adding a location on page 116.

About this task

Use the following procedure to assign a particular WCS server cluster to a physical location.

Procedure

1. In the Provisioning Client window, select **System Management** > **Routing** > **Web Conferencing Server Resources**.
2. Click the **WCS Cluster Physical Location** tab.

   You can select WCS servers associated with a particular location or you can select WCS servers associated with a particular WCS cluster.
3. Choose a selection criteria.
   - If you choose to select from the WCS servers associated with a particular location, select **Location** from the **Select By** list. Provisioning Client displays a list of the WCS servers associated with that location in the **Select Physical Location** list.
   - If you choose to select from the WCS servers associated with a particular WCS cluster, select **WCS Cluster** from the **Select By** list. Provisioning Client displays a list of the WCS servers associated with that WCS cluster in the **Select Web Conferencing Cluster** list.
4. From the **Available WCS Clusters** box, select the appropriate WCS server cluster, and then click **Copy**. If you want to assign all available WCS server clusters, click **Copy all**.
5. Click **Save**.
6. Repeat Steps 3 through 6 for each location.

Related Links

Web Conferencing Server (WCS) clusters on page 320
WCS Cluster Physical Location tab field descriptions on page 325

WCS Cluster Physical Location tab field descriptions

Name	Description
Select by	Displays the two selection criteria for choosing a WCS. You can choose from a list of WCSs assigned to a location or a list of WCSs assigned to a WCS cluster.
Select Physical Location	Displays a list of the locations of WCSs.
Select Web Conferencing Cluster	Displays a list of the provisioned WCS clusters.
Available WCS Clusters	Displays a list of provisioned WCS clusters.
Selected WCS Clusters	Displays the WCS servers assigned to the selected WCS cluster.

Button	Description
Copy all	Moves all of the WCS servers displayed in the **Available WCS Clusters** box to the **Selected WCS Clusters** box.
Copy	Moves the selected WCS server displayed in the **Available WCS Clusters** box to the **Selected WCS Clusters** box.

Button	Description
Remove	Moves the selected WCS server in the **Selected WCS Clusters** box to the **Available WCS Clusters** box.
Remove all	Moves all of the WCS servers displayed in the **Selected WCS Clusters** box to the **Available WCS Clusters** box.
Save	Click **Save** to apply your changes.

Related Links

Assigning WCS clusters to physical locations on page 324

Assigning WCS clusters to hosting locations

You may wish to assign an alternative location to a particular group of users residing in a particular location. For example, your deployment may consist of a primary office site and a secondary office site. You may want the users in the secondary office site to use the Avaya Aura® Conferencing system resources from the primary office site. In other words, you may want the WCS cluster in the primary site to host a conference initiated by a user from the secondary site. You can use the concept of a hosting location to implement this functionality.

Before you begin

- You must be logged into Provisioning Client.
- Create at least one WCS cluster. See Creating a new cluster on page 322.
- Configure at least one location. See Adding a location on page 116.

About this task

Use this task to configure an alternative location for conferences.

Procedure

1. In the Provisioning Client window, select **System Management** > **Routing** > **Web Conferencing Server Resources**.
2. Click the **Hosting Locations** tab.
3. Select a hosting location from the **Select Hosting Location** list.

   For example, select a primary office site.
4. From the **Hostable Locations** box, select the appropriate location, and then click **Copy**. If you want to assign all available locations, click **Copy all**.

   For example, select a secondary office site.
5. Click **Save**.
6. Repeat Steps 3 through 6 for each location.

Related Links

Web Conferencing Server (WCS) clusters on page 320
Hosting Locations tab field descriptions on page 327

Hosting Locations tab field descriptions

Name	Description
Select Hosting Location	Displays the hosting location. This location will host the conferences for the locations listed in the **Hosted Locations** box.
Hostable Locations	Displays a list of provisioned locations.
Hosted Locations	Displays the locations assigned to the selected hosting location.

Button	Description
Copy all	Moves all of the locations displayed in the **Hostable Locations** box to the **Hosted Locations** box.
Copy	Moves the selected location displayed in the **Hostable Locations** box to the **Hosted Locations** box.
Remove	Moves the selected location in the **Hosted Locations** box to the **Hostable Locations** box.
Remove all	Moves all of the locations displayed in the **Hosted Locations** box to the **Hostable Locations** box.
Save	Click **Save** to apply your changes.

Related Links

Assigning WCS clusters to hosting locations on page 326

Configuring WCS clusters for event conferences

Event conferences are very large conferences that are used for gathering 100s or possibly 1000s of participants, often from multiple global locations. Event conferences are used for company announcements, town hall meetings, and so on. For more information about event conferences, see Event conferencing and media cascading on page 273 and Event conferencing considerations on page 329.

To configure event conferencing correctly, you must:

- Create and configure a WCS cluster that is dedicated to event conferencing, as described here.
- Assign a physical location to the WCS cluster, using the procedure in Assigning clusters to physical locations on page 324.
- Assign a user to the event location, using the procedure in Adding a user from Provisioning Client on page 63.
- Configure a media server cluster, as described in Configuring media server clusters for an Event conference on page 279.

Before you begin

- You must be logged into Provisioning Client.

Comments? infodev@avaya.com

- Create at least one WCS cluster. See Creating a new cluster on page 322.
- Configure at least one location. See Adding a location on page 116.

About this task

Use this task to configure a dedicated WCS cluster for event conferencing.

Procedure

1. In the Provisioning Client window, select **System Management** > **Routing** > **Web Conferencing Server Resources**.
2. Click the **WCS Clusters for Event Conference** tab.
3. From the **Available WCS Clusters** box, select a WCS cluster, and then click **Copy**. If you want to assign all available WCS clusters, click **Copy all**.
4. Click **Save**.

Related Links

Web Conferencing Server (WCS) clusters on page 320
WCS Clusters for Event Conference tab field descriptions on page 328
Event conferencing considerations on page 329

WCS Clusters for Event Conference tab field descriptions

Name	Description
Available WCS Clusters	Displays a list of clusters that are not assigned as serving a location for non-event conferences.
Selected WCS Clusters	Displays the WCS servers assigned to the selected WCS cluster.

Button	Description
Copy all	Moves all of the locations displayed in the **Available WCS Clusters** box to the **Selected WCS Clusters** box.
Copy	Moves the selected location displayed in the **Available WCS Clusters** box to the **Selected WCS Clusters** box.
Remove	Moves the selected location in the **Selected WCS Clusters** box to the **Available WCS Clusters** box.
Remove all	Moves all of the locations displayed in the **Selected WCS Clusters** box to the **Available WCS Clusters** box.
Save	Click **Save** to apply your changes.

Related Links

Configuring WCS clusters for event conferences on page 327

Event conferencing considerations

When considering the network deployment of Event conferencing resources, there are several factors that depend on the nature of the planned scenarios to be supported. These factors are specific to each situation as it occurs. For example, Event conferences that involve a large number of callers from the public require consideration for the point of entry into the network so that the required bandwidth capacities can be accommodated in the network. In this scenario, deployment of an Event conferencing Avaya Media Server that is collocated with PSTN gateways or session border controls (SBC) would minimize the WAN bandwidth requirements to support the expected calling patterns.

Reliability can also be a key requirement for Event conferences due to the impact of a system failure. Avaya recommends that you place the Event conferencing resources within a highly reliable location.

Related Links

Configuring WCS clusters for event conferences on page 327

Updating the host table entries

Note:

Perform this procedure only if the DNS client is not configured on the server.

The FQDN assigned to each Web Conferencing Service IP must be mapped to a corresponding IP address. Any server hosting a managed element instance that communicates with a Web Conferencing Service IP requires mapping.

Entries in the `/etc/hosts` table are managed by using the **`hostTableConfig`** alias. You must be logged on to an account with the SSA role (for example, ntsysadm).

Before you begin

- You must know the mapping of the service FQDN to IP address for each Web Conferencing Service IP.
- If the Web Conferencing Service IP is located within the DMZ, ping the IP address of each server to confirm communications between all components.

  Note:

  If your firewall blocks ICMP, you cannot verify communications between all components using ping.

About this task

Use the following procedure to create the mapping of FQDN to IP address on the Avaya Aura® Conferencing servers.

Comments? infodev@avaya.com

Procedure

1. Log on to the server hosting a Web Conferencing Server using an account with the SSA role (for example, ntsysadm).
2. Type `hostTableConfig -a <IP_Address> <FQDN>` for every IP address that requires mapping.

   Where IP_Address is the IP address to map to the specific Web Conference service FQDN.
3. Repeat Step 2 for each server hosting the following Network Elements:
   - Application Server
   - Provisioning Manager
   - Collaboration Agent Manager
   - Web Conferencing Management Server
   - Web Conferencing Server
   - Recording Server(s)

   Note:

   Systems external to Avaya Aura® Conferencing must be able to translate the Web Conferencing Server FQDN into an IP address for routing. Contact your network engineers to configure entries on your DNS servers.

Modifying the Collaboration Library settings

About this task

Use this procedure to modify the settings for the Collaboration Library.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Management** > **Collaboration Library**.
2. In the Collaboration Library dialog box, make your changes. For more information, see Collaboration Library dialog box field descriptions on page 331.
3. When finished, click **Apply**.

Related Links

Collaboration Library dialog box field descriptions on page 331

Collaboration Library dialog box field descriptions

Name	Description
Write Master	The web conferencing management server with library write access.
Snapshot Interval	The time interval (in seconds) between snapshots.
Snapshot Timeout	The amount of time (in seconds) allowed for a snapshot to complete.

Related Links

Modifying the Collaboration Library settings on page 330

Setting a web conferencing host name

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to specify the name of the web conferencing host.

Note:

You can have only one web conferencing host name.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Web Conferencing Host**.
2. In the Host Name box, type the name of the web conferencing host.
3. Click **Save**.

Related Links

Web Conferencing Host page field descriptions on page 331

Web Conferencing Host page field descriptions

Name	Description
Host Name	Specifies the name for the web conferencing host.

Related Links

Setting a web conferencing host name on page 331

Chapter 30: Managing Audio and Video SRTP

This section describes how to configure Audio and Video SRTP with Avaya Aura® Conferencing.

This feature enables users to conduct “secure” audio conferences if all participants in the conference are using SRTP audio. This feature also enables users to conduct “secure” video conferences if all participants in the conference are using SRTP video.

Endpoints supported with Audio SRTP

The following endpoints support Audio SRTP:

- Avaya 9600 Series IP Deskphones 96x1 H.323 Release 6.2
- Avaya 9600 Series IP Deskphones 96x1 H.323 Release 6.3
- Avaya 9600 Series IP Deskphones 96x1 SIP Release 6.2
- Avaya 9600 Series IP Deskphones 96x1 SIP Release 6.3
- Avaya Communicator Release 2.0 for Windows (TLS only)
- Avaya Communicator Release 2.0 for iPad Devices
- Avaya one-X Communicator Release 6.1
- Avaya one-X Communicator Release 6.1.1
- Avaya one-X Communicator Release 6.1.6
- Avaya one-X Communicator Release 6.2

Endpoints supported with Video SRTP

The following endpoints support Video SRTP:

- Avaya Flare Experience Release 1.2 for iPad Devices
- Avaya one-X Communicator Release 6.2

Related Links

Administering the SRTP settings for Avaya Aura Conferencing on page 333
Modifying Communication Manager settings for SRTP on page 336

Administering the SRTP settings for Avaya Aura Conferencing

About this task

Use this procedure to configure the SRTP settings for audio and video for Avaya Aura® Conferencing.

Here are the recommended Audio SRTP settings when configuring Avaya Aura® Conferencing in the Aura Solution:

- Security Policy - **BEST EFFORT**
- Encrypt RTCP - Disabled (that is, check box is not selected)
- Video Allowed For Security Enforced Calls - N/A
- Enforce SIPS for Security Enforced Calls - Enabled
- Enable Video Encryption - Enabled
- Mode - AES_CM_128_HMAC_SHA1_32:
  - Priority - **2**
  - Send Lifetime - Disabled (that is, check box is not selected)
  - SRTP Master Key Lifetime - **31**
  - Key Derive Rate - **0**
  - Master Key Index Length - **0**
- Mode - AES_CM_128_HMAC_SHA1_80:
  - Priority - **1**
  - Send Lifetime - Disabled
  - SRTP Master Key Lifetime - **31**
  - Key Derive Rate - **0**
  - Master Key Index Length - **0**

Procedure

1. In the navigation pane of Element Manager Console, select **Security > SRTP Settings**.
2. In the SRTP Settings dialog box, configure each setting. For more information, see SRTP Settings dialog box field descriptions on page 166.
3. When finished, click **Apply**.

Related Links

Managing Audio and Video SRTP on page 332
SRTP Settings dialog box field descriptions on page 166

Comments? infodev@avaya.com

SRTP Settings dialog box field descriptions

Name	Description
Security Policy	Select the type of media security policy you want to use. The security policy you specify dictates the type of media (audio and video)Avaya Aura® Conferencing will include in offer SDPs and how Avaya Aura® Conferencing generates answer SDP during SDP negotiation. Choices are: • **BEST EFFORT** When this option is selected, Avaya Aura® Conferencing will generate requests using SIPS and will offer both RTP and SRTP media using capability negotiation. If the request fails because SIPS is not supported by the endpoint, Avaya Aura® Conferencing will retry the request using SIP and RTP. Avaya Aura® Conferencing will accept and negotiate RTP-only offers, SRTP-only offers, and RTP/SRTP best effort offers. SRTP will be negotiated where allowed when a compatible SRTP crypto suite is offered. RTP will be negotiated for RTP-only offers and for RTP/SRTP best effort offers when a compatible SRTP crypto suite is not offered. • **SECURITY DISABLED** When this option is selected, Avaya Aura® Conferencing will support only RTP. Avaya Aura® Conferencing will accept and generate RTP offers/answers. Avaya Aura® Conferencing will negotiate to RTP when it receives a request that contains an SDP offer with RTP media or best-effort media. Avaya Aura® Conferencing will reject requests that contain an SDP offer with only SRTP media by replying with a 480 Temporarily Unavailable response. A local treatment will be played to the end user. • **SECURITY ENFORCED** When this option is selected, Avaya Aura® Conferencing will support only SRTP media. Avaya Aura® Conferencing will negotiate to SRTP media when it receives a request that contains an SDP offer with SRTP media or best-effort media and a compatible crypto suite. Avaya Aura® Conferencing will reject requests that contain an SDP offer with only RTP media by replying with a 480 Temporarily Unavailable response. A local treatment will be played to the end user. **Note:** The SECURITY ENFORCED option does not guarantee signaling security. To ensure full encryption, you must configure TLS for the Avaya Aura® Conferencing Application Server network element.
Encrypt RTCP	Select this check box to indicate that Avaya Aura® Conferencing supports encrypted SRTCP messages. When not selected, Avaya Aura® Conferencing indicates the preference to send and receive unencrypted SRTCP messages by including the UNENCRYPTED_SRTCP session parameter in outgoing offers. When selected, Avaya Aura® Conferencing supports sending and receiving encrypted SRTCP messages. Avaya Aura® Conferencing will not include the

Comments? infodev@avaya.com

Name	Description
	UNENCRYPTED_SRTCP session parameter in its offers. In either case, if the UNENCRYPTED_SRTCP session parameter is received in an offer, Avaya Aura® Conferencing will echo the UNENCRYPTED_SRTCP session parameter in its answer, and unencrypted SRTCP will be used in both directions. If the UNENCRYPTED_SRTCP session parameter is not received in an offer, Avaya Aura® Conferencing will not include the UNENCRYPTED_SRTCP session parameter in the answer and encrypted SRTCP is used in both directions.
Video Allowed For Security Enforced Calls	Select this check box if you want Avaya Aura® Conferencing to send secure audio and unsecure video while the **Security Policy** field is set to SECURITY ENFORCED. If this check box is not selected, Avaya Aura® Conferencing will disable the video port for calls with secure audio. This field only takes effect if the **Security Policy** field is set to SECURITY ENFORCED.
Enforce SIPS for Security Enforced Calls	Select this check box if you want to require incoming calls to use SIPS signaling to negotiate secure media for the call. In addition, Avaya Aura® Conferencing generated requests with SRTP-only media offers will use SIPS signaling.
Enable Video Encryption	Select this check box if you want to enable secure video for your configuration. If you do not select this check box, Avaya Aura® Conferencing does not provide secure video transmission. In other words, if you do not select this check box, Avaya Aura® Conferencing provides unencrypted video.
Mode	Select the encryption mode(s) you want to use. This is commonly referred to as the “crypto suite.“ Choices are **AES_CM_128_HMAC_SHA1_32** and **AES_CM_128_HMAC_SHA1_80**.
Priority	Select the priority for the associated mode. Choices are **0** to **9**. If you want to disable the encryption mode, select **0**. A non-zero value indicates the priority that should be applied to the crypto suite during media negotiation. **1** is the highest priority; **9** is the lowest priority.
Send Lifetime	Select this check box to indicate that Avaya Aura® Conferencing should include the Master Key Lifetime specified by the SRTP Master Key Lifetime option (below) in the key parameter of the SRTP crypto attribute during SRTP media negotiation. When not selected, the Master Key Lifetime field is not included in the key parameter of the SRTP crypto attribute during SRTP media negotiation. In this case, the default lifetime for the crypto suite is used for media negotiation.
SRTP Master Key Lifetime	Specify the maximum number of SRTP packets that will use a particular master key. Choices are **1** to **31**.
Key Derive Rate	Specify how frequently a new session key is derived from an SRTP master key. Choices are **0** to **24**.
Master Key Index Length	Specify the size of the Master Key Index/Identifier (MKI) field in the actual SRTP packets. Choices are **0** to **4**. An MKI is used to identify the master key from which the session key that authenticates the particular packet was derived. When set to **0**, Avaya Aura® Conferencing will not include an MKI value and its associated length in the key parameter of the SRTP crypto attribute during SRTP media negotiation, and an MKI field will not be included in the actual SRTP packets. When the Master Key Index Length is set to a value greater than **0**, Avaya Aura® Conferencing will include an MKI value, and its associated length in the key

Comments? infodev@avaya.com

Name	Description
	parameter of the SRTP crypto attribute during SRTP media negotiation and an MKI field will be included in the actual SRTP packets.

Related Links

Modifying the SRTP settings on page 166
Administering the SRTP settings for Avaya Aura Conferencing on page 333

Modifying Communication Manager settings for SRTP

About this task

Use the following procedure to modify Communication Manager settings to support Audio and Video SRTP. These settings are recommendations for “best effort.”

This section only applies to Avaya Aura® deployments. This section does not apply to Turnkey deployments.

Procedure

1. Log on to System Manager as admin.
2. On the System Manager console, click **Elements >** Communication Manager.
3. In the navigation pane, click **Parameters > System Parameters – Customer Options**.
4. On the System Parameters – Customer Options page, select the appropriate device, and click **View**.
5. Click **Next Page** to go to page 4.
6. On page 4, verify **Media Encryption Over IP** is set to **Y**.

   Note:

   If **Media Encryption Over IP** is set to **N**, contact Avaya support.
7. In the navigation pane, click **Parameters > System Parameters – Features**.
8. On the System Parameters – Features page, select the appropriate device, and click **New**.
9. Click **Prev Page** to go to page 19.
10. In the IP Parameters section, set **Initial INVITE with SDP for secure calls** to **Y**.
11. Press **Enter** to save your changes.
12. In the navigation pane, click **Network > Signaling Groups**.
13. Click the check box of the appropriate signaling group, and click **Edit**.
14. On Page 1, set **Enforce SIPS URI for SRTP** to **Y**.
15. Press **Enter** to save your changes.

16. Log off System Manager.
17. Open your Web browser and in the Address bar, type the IP address for the Communication Manager System Management Interface (SMI).
18. At the Logon ID prompt, type your Logon ID, and click **Logon**.
19. Type your password, and click **Logon**.
20. On the Administration menu, click **Native Configuration Manager**.
21. In the Server Login window, type your Logon ID, and click **OK**.
22. Type your password, and click **OK**.
23. In the Command field, type `change system-parameters ip-options`, and click **Send**.
24. On the IP-options system parameters page, click **NEXT PAGE** to navigate to page 2.
25. In the **Override ip-codec-set for SIP direct-media connections** field, type **n** if you are running Communication Manager 6.2 Feature Pack 3 or later.

    If you are running an earlier release of Communication Manager, type **y** in this field.
26. Click **Enter**.
27. In the Command field, type `change ip-codec-set #`, where `#` is the IP codec set you want to modify, and click **Send**.

    In default or new deployments, this is often `ip-codec-set 1` (and `ip-network-region 1`). If you are unsure, you should verify which IP network regions are being used in your deployment.
28. In the Media Encryption section on page 1 of IP Codec Set, perform the following steps:
    a. In field 1, type `1-srtp-aescm128-hmac80`.
    b. In field 2, type `2-srtp-aescm128-hmac32`.
    c. In field 3, type `none`.
29. Click **Enter**.
30. Repeat Steps 27 through 29 for each IP codec set.
31. When finished, close the Native Configuration Manager window.
32. In the Communication Manager system Management Interface (SMI) window, click **Logoff**.
33. Click **Log Off**.

Related Links

Managing Audio and Video SRTP on page 332
Communication Manager field descriptions on page 338

Communication Manager field descriptions

Name	Description
Media Encryption Over IP	This option enables media encryption over the IP network.
Initial INVITE with SDP for secure calls	Select this check box to ensure that Communication Manager sends out and accepts SIP INVITE messages with SDP Capability Negotiation.
Enforce SIPS URI for SRTP	Select this option to enforce SIPS URI for any incoming SIP message with descriptions (used for SRTP negotiation) in SDP. `Y` is the default value for this field.
Override ip-codec-set for SIP direct-media connections	Earlier versions of Communication Manager have mixed support for secure audio and video. Communication Manager 6.2 Feature Pack 3 fully supports secure audio and video. You must edit this parameter to accommodate the appropriate support level. When you enable `Override ip-codec-set for SIP direct-media connections`, Communication Manager overrides IP Codec Set preferences and uses SIP endpoint preferences. The default value is `N`.
ip-codec-set #	Page 1 of IP Codec Set enables you to configure the audio codec, the codec set, the frames per packet, the media encryption, the packet size, and the silence suppression. For the purposes of this task, you must enter information in the Media Encryption section.
IP Codec Set • 1-srtp-aescm128-hmac80 • 2-srtp-aescm128-hmac32 • none	**AES_CM_128_HMAC_SHA1_32** and **AES_CM_128_HMAC_SHA1_80** are the most commonly used encryption modes. They are commonly referred to as “crypto suites”. They are in ascending order of preference, in accordance with the **Priority** field on the SRTP Settings dialog on the Element Manager Console. These settings equate to the concept of **BEST EFFORT**. • **BEST EFFORT** When this option is selected, Avaya Aura® Conferencing will generate requests using SIPS and will offer both RTP and SRTP media using capability negotiation. If the request fails because SIPS is not supported by the endpoint, Avaya

Name	Description
	Aura® Conferencing will retry the request using SIP and RTP. Avaya Aura® Conferencing will accept and negotiate RTP-only offers, SRTP-only offers, and RTP/SRTP best effort offers. SRTP will be negotiated where allowed when a compatible SRTP crypto suite is offered. RTP will be negotiated for RTP-only offers and for RTP/SRTP best effort offers when a compatible SRTP crypto suite is not offered. • **SECURITY DISABLED** When this option is selected, Avaya Aura® Conferencing will support only RTP. Avaya Aura® Conferencing will accept and generate RTP offers/answers. Avaya Aura® Conferencing will negotiate to RTP when it receives a request that contains an SDP offer with RTP media or best-effort media. Avaya Aura® Conferencing will reject requests that contain an SDP offer with only SRTP media by replying with a 480 Temporarily Unavailable response. A local treatment will be played to the end user. • **SECURITY ENFORCED** When this option is selected, Avaya Aura® Conferencing will support only SRTP media. Avaya Aura® Conferencing will negotiate to SRTP media when it receives a request that contains an SDP offer with SRTP media or best-effort media and a compatible crypto suite. Avaya Aura® Conferencing will reject requests that contain an SDP offer with only RTP media by replying with a 480 Temporarily Unavailable response. A local treatment will be played to the end user. **Note:** The SECURITY ENFORCED option does not guarantee signaling security. To ensure full encryption, you must configure TLS for the Avaya Aura® Conferencing Application Server network element.

Related Links

Modifying Communication Manager settings for SRTP on page 336

Chapter 31: Managing the Recording feature

Configuring the system-wide Recording setting

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to enable the system-wide setting for the Recording feature. The Recording feature enables users to record audio and web collaboration sessions. When the Recording feature is enabled for the system, you can then enable the Recording feature on a per user basis.

Procedure

1. In the Provisioning Client window, select **System Management > System Default Settings**.
2. On the System Default Settings tab, select (check) the **Allow recording** check box.
3. Click **Save**.

Assign a Recording media server cluster to locations

About this task

Use this procedure to assign a Recording media server cluster to locations.

Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Cluster for Recording** tab.
3. From the Select by box, select **Media Server Cluster**.
4. From the Select Recording Media Server Cluster box, select the appropriate Recording media server cluster.
5. In the Select Locations area, select the check box for each location you want to assign to the selected Recording media server cluster.

6. Click **Save**.

Modifying a single user

Before you begin

You must be logged into Provisioning Client.

About this task

Use this procedure to configure the Recording feature for a user.

Note:

If you want to configure the Recording feature for multiple users at one time, you can use the Bulk Provisioning feature (**User Management > Bulk Provisioning**) in Provisioning Client.

Procedure

1. In the Provisioning Client window, select **User Management > Search Users**.
2. On the Advanced Search tab, click **Search** to view all provisioned users.
3. In the Login Name column, click on the Login Name of the user to whom you want to assign the Recording feature.
4. On the User page, click the **Actions** tab.
5. On the Actions tab, click **Conferencing**.
6. On the Conferencing User page, select (check) the **Enable Recording** check box.
7. Click **Save**.
8. Repeat Steps 2 through 7 for each user.

Scheduling a backup and/or purge of the Recording server

Before you begin

You have configured a Recording backup server. See Adding a backup location for the Recording server on page 346.

About this task

Use this procedure to schedule a backup and/or purge to be performed.

When a backup is performed, all recordings are stored on the backup server in folders named after each user's Avaya Aura ID (for example, `jsmith@yourcompany.com`). The individual recordings for each user are stored in subfolders for that user. These subfolders are named with the timestamp of the recording (for example, `20130621135839+0000`).

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > Recording > Backup/Purge Settings**.

   The Backup/Purge Settings dialog box appears.

2. Specify:
   - the time at which you want to run the backup and/or purge.
   - whether you want to run a backup, a purge, or both.
   - the location where you want to store the backup
3. When finished, click **Ok**.

Related Links

Backup/Purge Settings dialog box field descriptions on page 342

Backup/Purge Settings dialog box field descriptions

Name	Description
Schedule	Specify whether you want to schedule a backup and/or purge to be performed every day at a specific time. To schedule a daily backup and/or purge, click **Daily**, and specify the hour and minute (in 24-hour format) at which you want the backup and/or purge to be performed.
Actions	Click the check box of the process you want to schedule. If you want to schedule both a backup and a purge, select both the **Backup** check box and the **Purge** check box. If both the **Backup** check box and the **Purge** check box are checked, the purge process will delete only the recordings that have been backed up. If only the **Purge** check box is checked, the purge process will delete all recordings regardless of whether the recordings are backed up. A purge is triggered when the disk usage exceeds the critical threshold and continues deleting recordings until the retain threshold is reached. **Note:** • The purge process always deletes the oldest records first. • The timestamp is reset when recordings are restored to prevent the recordings from being immediately purged in the next purge process. • Changing the recording metadata (for example, by changing the title or by changing whether it is shared) will reset the backup flag and cause the file to be backed up again.
Location	Select the appropriate backup location.

Related Links

Scheduling a backup and/or purge of the Recording server on page 341

Backing up and/or purging the Recording server now

Before you begin

You have configured a Recording backup server. See Adding a backup location for the Recording server on page 346.

About this task

Use this procedure to back up and/or purge the Recording server.

When a backup is performed, all recordings are stored on the backup server in folders named after each user's Avaya Aura ID (for example, `jsmith@yourcompany.com`). The individual recordings for each user are stored in subfolders for that user. These subfolders are named with the timestamp of the recording (for example, `20130621135839+0000`).

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > Recording > Backup/Purge Settings**.

   The Backup/Purge Settings dialog box appears.

2. Specify:

   - whether you want to run a backup, a purge, or both.
   - the location where you want to store the backup

   For more information, see Backup/Purge Settings dialog box field descriptions on page 342.

3. When finished, click **Ok**.

4. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > Recording > Backup/Purge Maintenance**.

   The Backup/Purge Maintenance window appears.

5. Click **Start**.

   The Status column displays the current status of the operation. When the operation is complete, the Status column displays `Completed`.

   Note:

   If you want to stop the current operation, click **Stop**.

6. If you want to view the detailed status of the backup and/or purge, click **Details**.

Modifying the backup/purge settings for the Recording server

Before you begin

You have configured a Recording backup server. See Adding a backup location for the Recording server on page 346.

About this task

Use this procedure to:

- schedule a backup and/or purge
- modify the settings for a scheduled backup and/or purge

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > Recording > Backup/Purge Settings**.

   The Backup/Purge Settings dialog box appears.

2. Make your changes. For more information, see Backup/Purge Settings dialog box field descriptions on page 342.
3. When finished, click **Ok**.

Modifying the purge threshold settings for the Recording server

Before you begin

You have configured a Recording server.

About this task

Use this procedure to configure the thresholds at which an alarm will be triggered for disk space usage on the Recording media server recordings partition.

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > Recording > Purge Thresholds**.

   The Purge Thresholds dialog box appears.

2. Make your changes.
3. When finished, click **Ok**.

Related Links

Purge Thresholds dialog box field descriptions on page 345

Purge Thresholds dialog box field descriptions

Name	Description
Retain	Once a critical threshold is crossed, the purge job (if enabled) will start deleting the oldest recordings until disk space is freed at or below the Retain value you specify.
Major Threshold	Configure the threshold at which a major alarm will be triggered for disk space usage on the Recording media server recordings partition.
Critical Threshold	Configure the threshold at which a critical alarm will be triggered for disk space usage on the Recording media server recordings partition.

Related Links

Modifying the purge threshold settings for the Recording server on page 344

Restoring a backup to the Recording server

Before you begin

You have performed a backup previously.

About this task

Use this procedure to restore a backup to the Recording server. You can restore all recordings from a backup or only the recordings of a specific user. To restore the recordings of a specific user, you must know that user's Avaya Aura user ID (for example, `jsmith@yourcompany.com`).

Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > Recording > Restore Maintenance**.

   The Restore Maintenance window appears.

2. Click **Start**.
3. From the Location box in the Restore parameters dialog box, select the location of the backup you want to restore.
4. Perform one of the following steps:
   - If you want to restore all of the recordings in the backup location, go to Step 5.

Note:

Restoring all of the recordings in a backup location may take a long time.

- If you want to restore only the recordings of a specific user, enter the Avaya Aura ID of the user in the Subdirectory box (for example, `jsmith@yourcompany.com`). If you want to restore only that user's recordings for a specific month, enter the user's Avaya Aura ID and the year and month in which you are interested (`Avaya Aura user ID/yearmonth*`). For example, if you are interested in John Smith's recordings from June, 2013, you would enter `jsmith@yourcompany.com/201306*` where:
  - `jsmith@yourcompany.com` is the user's Avaya Aura user ID
  - `2013` is the year that contains the recording(s) in which you are interested
  - `06` is the month that contains the recording(s) in which you are interested
  - `*` is the wildcard character, which specifies that you want to restore all recordings for the user during the specified month

  .

Note:

To restore the recordings for an entire month, you must include the wildcard character (`*`) after the month in the Subdirectory box.

5. Click **Ok**.

Note:

If the Confirm empty path dialog box, appears, click **Yes**.

The Status column displays the current status of the operation. When the operation is complete, the Status column displays `Completed`.

Note:

If you want to stop the current operation, click **Stop**.

6. If you want to view the detailed status of the restore, click **Details**.

Managing Recording server backup locations

Adding a backup location for the Recording server

About this task

Use this procedure to specify a backup location for the Recording server.

Procedure

1. In the navigation pane of Element Manager Console, select **Recording > Backup Locations**.
2. In the Backup Locations window, click **Add (+)**.
3. In the Add Backup Locations dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

Related Links

Add/Edit Backup Locations dialog box field descriptions on page 347

Add/Edit Backup Locations dialog box field descriptions

Name	Description
Name	Enter the name of the backup server.
Node	Select the node for the backup server.
Path	Enter the absolute path under which recordings should be stored on the backup server.

Related Links

Adding a backup location for the Recording server on page 346

Modifying a backup location for the Recording server

About this task

Use this procedure to modify a backup location for the Recording server.

Procedure

1. In the navigation pane of Element Manager Console, select **Recording > Backup Locations**.
2. In the Backup Locations window, select the backup location you want to modify.
3. Click **Edit (+/-)**.
4. In the Edit Backup Locations dialog box, make your changes. For more information, see Add/Edit Backup Locations dialog box field descriptions on page 347.
5. When finished, click **Apply**.

Deleting a backup location for the Recording server

About this task

Use this procedure to delete a backup location for the Recording server.

Procedure

1. In the navigation pane of Element Manager Console, select **Recording > Backup Locations**.
2. In the Backup Locations window, select the backup location you want to delete.
3. Click **Delete (+/-)**.
4. In the Confirmation dialog box, click **Yes**.

Chapter 32: Managing LDAP directory integration

The LDAP directory integration feature enables an enterprise administrator to regularly synchronize the Avaya Aura® Conferencing database with LDAP directories. When Avaya Aura® Conferencing is integrated with LDAP directory servers, the conferencing subscriber data is managed in the LDAP directory. When a user logs into Avaya Aura® Conferencing via Collaboration Agent or a mobile client, the user will be authenticated directly against the password in the LDAP directory.

Note:

Avaya Aura® Conferencing supports any directory server that supports LDAP (for example, Microsoft® Active Directory 2003 and 2008 and OpenLDAP).

Related Links

Modifying the directory authentication timeouts on page 359
Configuring the directory access passcode on page 360
Configuring enterprise domain authentication on page 361
Configuring LDAP directory-synchronized users on System Manager on page 362

Managing the directory access servers

Modifying the connection credentials for directory access servers

Before you begin

You must know the distinguished name and password of a user with read access to the directory servers in each domain (for example, `cn=administrator,cn=Users,dc=ca,dc=canada,dc=com`).

About this task

Use the following procedure to modify the connection credentials for all directory access servers in the user domain.

Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Directory Servers**.
2. Click the **Connection Credentials** tab.
3. From the Select domain box, select the directory domain you want to modify. The Select domain box displays all the directory domains you have added.
4. In the Connection Principal box, enter the distinguished name of a user with read access to the directory servers in the selected domain (for example, `cn=administrator,cn=Users,dc=ca,dc=canada,dc=com`).
5. In the Connection Password box, enter the password of the user you entered in Step 4.
6. Click **Save**.

Related Links

Managing LDAP directory integration on page 349

Modifying the directory access servers for synchronization

About this task

Use the following procedure to modify the primary and secondary directory access servers in a domain for synchronization.

Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Directory Servers**.
2. Click the **Synchronization Servers** tab.
3. From the Select domain box, select the directory domain you want to configure.
4. From the Primary Server box, select the primary server used for synchronization.
5. Perform one of the following steps:
   - If there is a redundant server, select the redundant server from the Secondary Server box.
   - If there is not a redundant server, select **Not Selected** from the Secondary Server box.
6. Click **Save**.

Related Links

Managing LDAP directory integration on page 349

Modifying the directory access servers for user authentication

About this task

Use the following procedure to modify the list of directory access servers for a physical site in a user domain for user authentication.

Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Directory Servers**.
2. Click the **Authentication Servers** tab.
3. From the Select domain box, select the directory domain you want to modify.
4. If you want to configure the authentication server for a physical site:
   a. From the Physical Site box, select the physical site of the Application Server or Provisioning Manager server. (Both of these servers usually reside together on your intranet.)
   b. From the Authentication Server box, select the directory server that the Provisioning Manager server should try first for authentication for the domain.
   c. Click **Add**.

      The information you entered appears at the top of the table.

      Note:

      The order in which the information is displayed in the table indicates the order in which the authentication servers are queried. Be sure to prioritize the list of authentication servers for each physical site based on availability or network access.
5. If you want to change the priority of an entry in the list of servers to query, click **Move Up** or **Move Down** in the table for the appropriate entry.
6. If you want to delete an entry from the list of servers to query:
   a. In the table, click **Delete** for the entry you want to delete.
   b. In the Service Affecting dialog box, enter your password for Provisioning Client, and click **Confirm**.

Related Links

Managing LDAP directory integration on page 349

Managing the synchronization service

Modifying the directory synchronization timeouts

About this task

Use the following procedure to modify the following directory synchronization timeouts:

- connection timeout
- read timeout

Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Synchronization Service**.
2. Click the **Sync Configuration** tab.
3. From the Select Provision manager for sync box, select the Provisioning Manager network element that you want to perform the synchronization.
4. In the Connection Timeout (milliseconds) box, enter the connection timeout in milliseconds for synchronization. If the directory synchronization client cannot establish a connection within the period you specify, the client aborts the synchronization attempt.

   Note:

   If you enter **0**, the connection timeout is handled by TCP protocol.
5. In the Read Timeout (milliseconds) box, enter the read timeout in milliseconds for synchronization. If the directory synchronization client does not receive a read response within the period you specify, the client aborts the read attempt.

   Note:

   If you enter **0**, there is not timeout, and the system will wait for the read operation to complete.
6. Click **Save**.

Related Links

Managing LDAP directory integration on page 349

Configuring directory synchronization filters

About this task

Use the following procedure to configure directory filters for a specific user domain.

Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Synchronization Service**.
2. Click the **Sync Filter & Defaults** tab.

   Using the Sync Filter & Defaults tab, you can configure directory filters for a specific user domain.

   You must define one filter for each group of users you want to synchronize from the directory server. For example, if you want to synchronize users with the job title “engineer,” you may define the filter “title=engineer.” You can set a specific template for these users. Then, you may define a filter and default for managers. For example, this filter could be “title=manager” with a more advanced template “executive_passcodes.”

   Note:

   Keep in mind the following:

   - Synchronization will not occur unless at least one filter is configured.
   - A filter with an empty filter value is equivalent to “query all users”.

   The syntax of the filter string is defined by RFC 2254, The String Representation of LDAP Search Filters. This RFC may be used as a reference for constructing more complex filter strings.

   A filter is a UTF-8 formatted string that has the following syntax:

   (*attribute operator value*)

   or

   (*operator(filter1)(filter2)*)

   where *filter1* and *filter2* have the syntax displayed on the first line, and the operator is a string operator. The *attribute* corresponds to an LDAP attribute that exists in the directory, and value corresponds to the actual data value that is requested for the attribute. An example filter is `(&(ou=Austin)(sn=Miller))`. This filter returns all users whose last name is “Miller” and also have the organization unit “Austin.”

   An attribute specified in the filter can be any attribute that exists in the LDAP directory, and it is not required to be one of the attributes (specified in translation schema) that is imported by Provisioning Manager. The attribute is used only on the LDAP server to select data, and the corresponding entries will have a subset of their data imported (based on the translation schema).
3. To configure a new directory filter for a user domain, perform the following steps:
   a. From the Select domain box, select the directory domain you want to configure.
   b. In the Name box, enter the name for this filter.
   c. In the Filter box, enter the string representation of an LDAP search filter.

Comments? infodev@avaya.com

d. If you want to use a specific template, select the appropriate template from the Template box.

e. If you want to use a specific location, select the appropriate location from the Location box.

f. If you want to use a specific locale, select the appropriate locale from the Local box.

g. If you want to use a specific time zone, select the appropriate time zone from the Time zone box.

h. In the Communication profile box, enter the appropriate communication profile (for example, `Primary`).

i. Click **Save**.

The new filter appears at the bottom of the table.

Note:

The order in which the filters are displayed in the table indicates the order in which the filters are run.

4. To modify a directory filter, perform the following steps:
   a. From the Select domain box, select the directory domain you want to configure.
   b. In the table, click on the name of the directory filter you want to modify.
   c. Make your changes to the selected filter.
   d. When finished, click **Save**.
5. To change the priority of a directory filter, perform the following steps:
   a. From the Select domain box, select the directory domain you want to configure.
   b. In the table, click **Move Up** or **Move Down** for the appropriate filter.
6. To delete a directory filter, perform the following steps:
   a. From the Select domain box, select the directory domain you want to configure.
   b. In the table, click **Delete** for the filter you want to delete.
   c. In the Service Affecting dialog box, enter your password for Provisioning Client, and click **Confirm**.

Related Links

Managing LDAP directory integration on page 349

Configuring a directory synchronization schema

About this task

Use the following procedure to configure directory synchronization schema for a specific user domain.

Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Synchronization Service**.
2. Click the **Sync Schema** tab.

   Using the **Sync Schema** tab, you can configure a directory synchronization schema for a specific user domain.

   You must define one schema for each domain you want to synchronize from the directory server.
3. Select a domain from the **domain** drop-down list.
4. Make your changes.

   For more information, see Modify Sync Schema page field descriptions on page 355.
5. Click **Save**.

Related Links

Managing LDAP directory integration on page 349
Modify Sync Schema page field descriptions on page 355

Modify Sync Schema page field descriptions

Name	Description
Directory distinguished name	This is an element which works in conjunction with the search scope. It is the tree from which you want users to be synchronized. **Note:** The domain part of the distinguished name is automatically added based on the selected domain and cannot be changed. For example: cn=Users,dc=example,dc=com
Login name	The **Login name** field shows which directory attribute will be mapped into the login name. It is not a mandatory field. If you do not provide a mapping for **Login name**, or there is no such attribute in the directory, or the attribute value is null or an empty string, then **Communication address handle** is used as login name.
First name	First name of the user.
Last name	Last name of the user.
Display name	The **Display name** field shows which directory attribute will be mapped into the display name. It is not a mandatory field. If you do not provide a mapping for **Display name**, or there is no such attribute in the directory, or the attribute value is null or an empty string, then a combination of first name

Name	Description
	and last name is used as display name. For example, if the first name is Helena and the last name is Jensen, and **Display name** is empty, then display name will be Jensen, Helena.
Communication address handle	The Communication address handle field shows which directory attribute will be mapped into Communication address handle. **Note:** Only the handle part (without domain) is expected here. The omain part is added automatically during synchronization based on the selected domain. Example: 9026884452
Moderator Collaboration Code	The **Moderator Collaboration code** field shows which directory attribute will be mapped into the Moderator access code. It is not mandatory field. If you do not provide a mapping for **Moderator Collaboration code**, or there is no such attribute in the directory, or the attribute value is null or an empty string, then the Moderator Collaboration code will be autogenerated (random number).
Participant Collaboration Code	The **Participant Collaboration code** field shows which directory attribute will be mapped into Participant access code. It is not mandatory field. If you do not provide a mapping for **Participant Collaboration code**, or there is no such attribute in the directory, or the attribute value is null or an empty string, then the Participant Collaboration code will be autogenerated (random number).
Enterprise Identity	Directory Access Server identity for this user.
Moderator passcode	The **Moderator passcode** is synchronized with the directory only if the passcodes data source is LDAP. If the configured data source is the database, then **Moderator passcode** is not synchronized.
Participant passcode	The **Participant passcode** is synchronized with the directory only if the passcodes data source is LDAP. If the configured data source is the database, then **Participant passcode** is not synchronized.
Business phone Home phone Cell phone	Phone numbers of the user.
INACTIVE Status	For disabling users, in order to work across different types of directories (which may disable, lock or soft-delete a user), the **INACTIVE status** attribute requires a value specification. For example: if **INACTIVE Status** in schema is **isDeleted** and **Value**

Name	Description
	is **Y** and value of **isDeleted** attribute is **Y** for the appropriate user in directory, then the user is recognized as an INACTIVE user.

Related Links

Configuring a directory synchronization schema on page 354

Performing a directory synchronization now

About this task

Use the following procedure to perform a synchronization now.

Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Synchronization Service**.
2. Click the **Sync Scheduler** tab.
3. Click **Sync Now**.
4. To view the status of the synchronization, click the **Sync Status** tab.

Related Links

Managing LDAP directory integration on page 349
Directory Synchronization Status page field descriptions on page 357

Directory Synchronization Status page field descriptions

Name	Description
Domain	Name of the domain which users are synchronized
Users read	Number of synchronized users
Users added	Number of added users
Users modified	Number of modified users
Users deleted	Number of deleted users
Users failed	Number of users that cannot be synchronized
Users pending	Number of pending users to be synchronized
Status	Status of the synchronization

Related Links

Performing a directory synchronization now on page 357

Scheduling a directory synchronization

About this task

Use the following procedure to schedule a synchronization to be performed at a specific time and at a specific frequency (daily, weekly, and/or monthly).

Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Synchronization Service**.
2. Click the **Sync Scheduler** tab.
3. Click the **Enable scheduled sync** check box.
4. In the Time boxes, specify the time of day you want to run the synchronization.
5. If you want to schedule the synchronization to run on specific days of the week, select **Day of Week** from the Type box, and then click the check box of the appropriate day(s).
6. If you want to schedule the synchronization to run on a specific day of the month, select **Day of Month** from the Type box, and then select the appropriate day from the Perform sync every month at the following day box.

   Note:

   If the day number you specify exceeds the last day of a month, the synchronization will run on the last day of the month. For example, if you select **31**, the synchronization will run on the last day of the month in months that have less than 31 days.
7. When finished, click **Save**.

Related Links

Managing LDAP directory integration on page 349

Testing the directory synchronization connection and schema

About this task

Use the following procedure to verify the connection to the directory server and test the synchronization schema and filter configuration.

Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Synchronization Service**.
2. Click the **Query Test Tool** tab.

   Using Query Test Tool tab, you can test the connection and schema settings at any time.

3. In the Filter box, specify an LDAP filter. For example, you may try the filter “cn=*”. This filter will query all users under the base distinguished name you specified in the schema.
4. Click **Search**.

Related Links

Managing LDAP directory integration on page 349

Modifying the directory authentication timeouts

About this task

Use the following procedure to modify the following settings for the directory authentication service:

- connection timeout
- read timeout

Note:

Set these values based on the network and required user experience. Users logging into Collaboration Agent will experience the total amount of time configured here as the total amount of wait time before their login fails due to connection/read issues to the directory.

Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Authentication Service**.
2. Click the **Auth Configuration** tab.
3. In the Connection Timeout (milliseconds) box, enter the connection timeout in milliseconds for authentication. If the directory authentication client cannot establish a connection within the period you specify, the client aborts the connection attempt.

   Note:

   If you enter **0**, the connection timeout is handled by TCP protocol.
4. In the Read Timeout (milliseconds) box, enter the read timeout in milliseconds for authentication. If the directory authentication client does not receive a response within the period you specify, the client aborts the read attempt.

   Note:

   If you enter **0**, there is no timeout, and the system will wait for the authentication operation to complete.
5. Click **Save**.

Related Links

Managing LDAP directory integration on page 349

Configuring the directory access passcode

About this task

Use the following procedure to configure Directory Access passcode settings for a domain.

Procedure

1. In the Provisioning Client window, select **System Management** > **Directory Access Services** > **Authentication Service**.
2. Click the **Auth Passcode** tab.

   Using the **Auth Passcode** tab, you can configure the directory access passcode settings for a domain.

   You must define one schema for each domain you want to synchronize from the directory server.
3. Select a domain from the **domain** drop-down list.
4. Make your changes.

   For more information, see Modify Auth Passcode page field descriptions on page 360.
5. Click **Save**.

Related Links

Managing LDAP directory integration on page 349
Modify Auth Passcode page field descriptions on page 360

Modify Auth Passcode page field descriptions

Name	Description
Data source	The data source to use when authenticating passcodes.
Encoding Method	The encoding method when passcode authentication is performed using the LDAP.
Authentication Key Confirm Authentication Key	Authentication key string This field is required when an encoding method is selected. The authentication key uses an AES cypher with a key length of either 128 bits or 256 bits. The key should be provided in hexadecimal format. Example of 128 bits key: 0123456789ABCDEF0123456789ABCDEF.
Authentication Action	Action to perform when LDAP is unavailable to use for authentication.

Related Links

Configuring the directory access passcode on page 360

Configuring enterprise domain authentication

About this task

Use the following procedure to manage enterprise domain authentication.

Procedure

1. In the Provisioning Client window, select **System Management** > **Directory Access Services** > **Authentication Service**.
2. Click the **Auth Schema** tab.

   Using the **Auth Schema** tab, you can manage enterprise domain authentication.

   You must define one schema for each domain you want to synchronize from the directory server.
3. Select domain from the **domain** drop-down list.
4. Make your changes.

   For more information, see Modify Auth Schema page field descriptions on page 361.
5. Click **Save**.

Related Links

Managing LDAP directory integration on page 349
Modify Auth Schema page field descriptions on page 361

Modify Auth Schema page field descriptions

Name	Description
Directory distinguished name	Base directory name used for authentication
Enterprise identity	Enterprise identity attribute value

Related Links

Configuring enterprise domain authentication on page 361

Configuring LDAP directory-synchronized users on System Manager

About this task

Use the following procedure to provision manually on Avaya Aura® System Manager each user that you want synchronized from the LDAP directory. This section only applies to Avaya Aura® deployments. This section does not apply to Turnkey deployments.

Procedure

1. Log into Avaya Aura® System Manager.
2. On the System Manager console, click **Users** > **User Management**.
3. In the navigation pane, click **User Management** > **Manage Users**.
4. On the User Management page, click **New**.

   The New User Profile page appears.
5. On the **Identity** tab, complete the required information. When entering this information, perform the following steps:
   - Make sure the data you enter in the Last Name box matches the data in the schema you mapped to “Last name” on the Sync Schema tab in Provisioning Client.
   - Make sure the data you enter in the First Name box matches the data in the schema you mapped to “First name” on the Synch Schema tab in Provisioning Client.
6. When finished, click **Commit & Continue**.
7. On the **Communication Profile** tab, complete the required information:

   a. **Name**: Type a name.

   b. **Default**: Select this check box.

   c. Complete the **Communication Address** section to add the user’s communication address.

      Note:

      The user’s communication address consists of a handle and a domain (for example, 5522@avaya.com). When entering this information:

      - Make sure the data you enter for the handle matches the data in the schema you mapped to “Communication address handle” on the **Sync Schema** tab in Provisioning Client.
      - Make sure the data you enter for the domain matches the domain you selected on the **Sync Schema** tab in Provisioning Client.

   d. Complete the **Session Manager Profile** section.

   e. Complete the following profiles as required for your users:
      - **CallPilot Messaging Profile**

Comments? infodev@avaya.com

- **CM Endpoint Profile**
- **CS 1000 Endpoint Profile**
- **Messaging Profile**
- **B5800 Branch Gateway Endpoint profile**

Note:

Do not assign the Conferencing Profile to the user. The user will be synchronized into Avaya Aura Conferencing. If you assign the Conferencing Profile, you will receive errors either when saving the user on System Manager or during a subsequent LDAP synchronization because two sources will be trying to modify the same user data in Avaya Aura Conferencing.

8. Click **Commit & Continue**.
9. Repeat Steps 4 through 8 for each new user you want to add to System Manager.

Related Links

Managing LDAP directory integration on page 349

Chapter 33: Element Manager Console Local Logon Administration Tasks

This chapter describes how to:

- change the password for your “local” user ID for Element Manager Console. The local user ID is the user ID you use when you log onto Element Manager Console locally.
- change the password for other “local” user IDs for Element Manager Console. Element Manger Console provides six local user IDs.
- configure the password rules for the “local” user IDs for Element Manager Console.
- configure the login rules for the “local” user IDs for Element Manager Console and Provisioning Client.
- force off a user currently logged onto Element Manager Console.
- view the users currently logged onto Element Manager Console.

.

Note:

To perform the procedures in this section, you must be logged onto Element Manager Console locally.

Related Links

Changing the password for your local logon user ID for Element Manager Console on page 365
Changing the password for the other local logon user IDs for Element Manager Console on page 365
Configuring the password rules for the local logon user IDs for Element Manager Console on page 366
Configuring the login rules for the local logon user IDs for Element Manager Console and Provisioning Client on page 368
Forcing off a user logged into Element Manager Console on page 369
Viewing the users logged into Element Manager Console on page 370

Changing the password for your local logon user ID for Element Manager Console

Before you begin

You must be able to log onto Element Manager Console locally.

About this task

Use this procedure to change the password for your local logon user ID for Element Manager Console.

Procedure

1. Log onto Element Manager Console locally.
2. From the Administration menu, select **Password Administration > Change My Password**.
3. In the New Password box in the Change My Password dialog box, enter the new password for the selected user ID.
4. In the Password Confirm box, reenter the new password.
5. In the Current Password box, enter your old password.
6. Click **Apply**.

Related Links

Element Manager Console Local Logon Administration Tasks on page 364

Changing the password for the other local logon user IDs for Element Manager Console

Before you begin

You must be able to log onto Element Manager Console locally.

About this task

Use this procedure to change the password for any of the other local user IDs for Element Manager Console. Element Manager Console provides six local user IDs.

Procedure

1. Log onto Element Manager Console locally..
2. From the Administration menu, select **Password Administration > Set Administrator Password**.
3. From the User ID box in the Set Administrator Password dialog box, select the appropriate local administrator user ID.
4. In the New Password box, enter the new password for the selected user ID.

5. In the Password Confirm box, reenter the new password.
6. If you want the system to force a password change for this user ID, click the **Force Password Change** check box.
7. Click **Apply**.

Related Links

Element Manager Console Local Logon Administration Tasks on page 364

Configuring the password rules for the local logon user IDs for Element Manager Console

Before you begin

You must be able to log onto Element Manager Console locally.

About this task

Use this procedure to configure the complexity and aging rules for passwords for the local logon user IDs for Element Manager Console.

Procedure

1. Log into Element Manager Console locally.
2. From the Administration menu in Element Manager Console, select **Password Rules**.
3. In the Password Rules dialog box, complete the field as appropriate. For more information, see Password Rules dialog box field descriptions on page 366.
4. When finished, click **Apply**.

Related Links

Element Manager Console Local Logon Administration Tasks on page 364
Password Rules dialog box field descriptions on page 366

Password Rules dialog box field descriptions

Name	Description
Password Complexity Rules area	
Minimum Password Length	This parameter specifies the minimum number of total characters a password must contain. The range of values allowed is 4-32. Default: 8. The Minimum Password Length must be equal to or greater than the total of the Minimum Lowercase Characters, Minimum Uppercase Characters, Minimum Digit Characters, and Minimum Special

Name	Description
	Characters. If Check For Dictionary Words in Password is enabled, the Minimum Password Length value must be 6 or more.
Minimum Lowercase Characters	This parameter specifies the minimum number of lowercase characters (a–z) that the password must contain. The range of values allowed is 0-10. Default: 2
Minimum Uppercase Characters	This parameter specifies the minimum number of uppercase characters (A–Z) that the password must contain. The range of values allowed is 0-10. Default: 2
Minimum Digits	This parameter specifies the minimum number of digit characters (0–9) that the password must contain. The range of values allowed is 0-10. Default: 2
Minimum Special Characters	This parameter specifies the minimum number of special characters that the password must contain. Special Characters are: !#$%*. @ - _ {}& ‘ ^ ? ! ( ) , / \ : ; ~ = +. The range of values allowed is 0-10. Default: 0
Maximum Consecutive Characters	This parameter specifies the maximum number of times a given character can appear consecutively in a valid password. Configure the value to 0 (zero) to disable Maximum Consecutive Characters. The range of values allowed is 0-10. Default: 0
Minimum Characters Different from Previous Password	This parameter specifies the minimum number of characters by which the new password must differ from the previous password. The system ignores this value if either one half of the characters in the new password are different, or if there are more than 23 characters in the new password. The range of values allowed is 0-10. Default: 0
Password History	This parameter specifies the size of the password history maintained by the system for each user. The system rejects the reuse of any password found in the user's history. To disable password history validation, set this value to 0 (zero). The range of values allowed is 0-24. Default: 1
User ID or Reversed User ID Permitted in Password	Select this check box if you want to allow the password to include the user's ID or the user's ID reversed.
Check for Dictionary Words in Password	Select this check box if you want to prevent administrators from using passwords that are derived from dictionary words. When this setting is enabled, the system checks whether dictionary words are used in the password.
Password Aging Rules area	
Maximum Password Life (days)	This parameter specifies the maximum number of days that an administrator’s password can be used before it expires. After the specified number of days, the administrator must change the password to access the server. To disable password expiration, set this value to 0 (zero).

Name	Description
	The range of values allowed is 0-180 days. Default: 90
Minimum Password Life (hours)	This parameter specifies the minimum number of hours between password changes.This setting discourages administrators from immediately changing their passwords back to a previously used password (password flipping). To permit users to change their passwords as often as they want, set this value to 0 (zero). If not set to 0, the minimum password life must be less than the maximum password life. The range of values allowed is 0-480 hours (20 days). Default: 1
Expiry Notification (days)	This parameter specifies the number of days in advance that users receive a warning that their passwords will expire. To disable expiry notification, set this value to 0 (zero). If not set to 0, the expiry notification must be less than the maximum password life and greater than the minimum password life. The range of values allowed is 0-30 days. Default: 7

Related Links

Configuring the password rules for the local logon user IDs for Element Manager Console on page 366

Configuring the login rules for the local logon user IDs for Element Manager Console and Provisioning Client

Before you begin

You must be able to log onto Element Manager Console locally.

About this task

Use this procedure to configure the local login rules for:

- Element Manager Console
- Provisioning Client

Procedure

1. Log into Element Manager Console locally.
2. From the Administration menu in Element Manager Console, select **Login Rules**.
3. In the Login interface box in the Login Rules dialog box, specify whether you want to configure the login rules for Element Manager Console (**Configuration Management (OMI)**) or Provisioning Client (**Provisioning Management (PROV)**).
4. Complete the field as appropriate. For more information, see Login Rules dialog box field descriptions on page 369.

5. When finished, click **Apply**.

Related Links

Element Manager Console Local Logon Administration Tasks on page 364
Login Rules dialog box field descriptions on page 369

Login Rules dialog box field descriptions

Name	Description
Configuration Session Timeout (minutes)	This rule defines the maximum number of minutes a session can be idle before the user must reauthenticate. The range of values allowed is 0–120. Configure the value to 0 (zero) to disable session timeout. After a session times out, any write operations must be re-authenticated.
Provisioning Session Timeout (minutes)	This rule defines the maximum number of minutes a session can be idle before the user must reauthenticate. The range of values allowed is 0–120. You cannot disable session timeout for the Provisioning Client interface.
Failed Login Attempts before Lockout	This rule defines the maximum number of successive failed attempts to log on, allowed before the user's account is locked. The range of values allowed is 0–10. Configure the value to 0 (zero) to disable lockout and permit unlimited successive failed log on attempts. If not zero, the value represents an inclusive number of attempts. Therefore, if the value is 1 (one), a single failure causes the user's account is immediately locked. Until the account is unlocked, the system rejects further attempts to log on.
Lockout Duration (minutes)	This rule defines the number of minutes that a user's account remains locked after reaching the maximum number of successive failed attempts to log on. The range of values allowed is 1–60.
Account Inactivity Period (days)	This rule defines the number of consecutive days of inactivity (that is, the number of consecutive days that the user did not log onto the system) at which the user's account is locked.

Related Links

Configuring the login rules for the local logon user IDs for Element Manager Console and Provisioning Client on page 368

Forcing off a user logged into Element Manager Console

Before you begin

You must be logged into Element Manager Console locally.

About this task

Use this procedure to force off a user who is logged into Element Manager Console.

Procedure

1. Log into Element Manager Console locally.
2. From the Administration menu in Element Manager Console, select **User Display/Forceoff**.
3. In the Logged-In Users dialog box, select the user you want to force off.
4. Click **Force Off**.
5. In the Confirmation dialog box, click **Yes**.

Related Links

Element Manager Console Local Logon Administration Tasks on page 364

Viewing the users logged into Element Manager Console

Before you begin

You must be logged into Element Manager Console locally.

About this task

Use this procedure to view the users logged into Element Manager Console currently.

Procedure

1. Log into Element Manager Console locally.
2. From the Administration menu in Element Manager Console, select **User Display/Forceoff**.

   The Logged-in Users dialog box displays the users currently logged into Element Manager Console.

Related Links

Element Manager Console Local Logon Administration Tasks on page 364

Chapter 34: Importing and Exporting Data

Importing configuration data into Element Manager Console

Before you begin

You must know the user ID and password of an OS AA admin (ntappadm).

About this task

Use this procedure to import configuration data into Element Manager Console.

Procedure

1. From the Tools menu in Element Manager Console, select **DB Import**.
2. In the Import File area of the DB Import window, click **Choose**.
3. In the Open dialog box, select the file you want to import.
4. Click **Open**.
5. In the Result File area of the DB Import window, click **Choose**.
6. In the Save dialog box, specify the name and location for the log output file.
7. Click **Save**.
8. In the DB Import window, click **Import Now**.
9. In the FTP Login window, enter the AA (ntappadm) user name and password.
10. Click **Apply**.

Exporting configuration data from Element Manager Console

Before you begin

You must know the user ID and password of an OS AA admin (ntappadm).

About this task

Use this procedure to export the configuration data for Element Manager Console.

Procedure

1. From the Tools menu in Element Manager Console, select **DB Export**.
2. In the Export File area of the DB Export window, click **Choose**.
3. In the Save dialog box, select the file and location to which you want to save the configuration data.
4. Click **Save**.
5. Do one of the following:
   - If you want to export all of the service, click **Export All Services** in the Services area.
   - If you want to export selected services, click **Export Select Services** in the Services area, and then click on the services you want to export in the Services Available for Export list box. Press and hold the CTRL key on your keyboard to select multiple services.
6. Click **Export Now**.
7. In the FTP Login window, enter the AA (ntappadm) user name and password.
8. Click **Apply**.

Chapter 35: Deploying the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®

The Avaya Aura® Conference Manager Add-in for Microsoft Outlook® uses Outlook's Calendar Meeting feature to help users create and manage their conference invitations.

Note:

The Avaya Aura® Conference Manager Add-in for Microsoft Outlook® works with Microsoft Outlook 2007, Microsoft Outlook 2010, and Microsoft Outlook 2013.

You can use one of the following models for deploying the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®:

- ClickOnce deployment

  With the ClickOnce deployment, you must place the Avaya Aura® Conference Manager Add-in files on to a web server or other public location (like a network share) that Avaya Aura® Conferencing users can access. The users will then run the Avaya Aura® Conference Manager Add-in installer from that location. Once the users install the Avaya Aura® Conference Manager Add-in, updates will be applied automatically when available. For this deployment, each user must run the installer.

- Centralized software deployment

  With the centralized software deployment, you may configure a group policy so that individual computer configurations are updated. The Windows registry is modified to point to the Microsoft Outlook Add-in deployment manifest. When Microsoft Outlook is restarted, it will automatically download the Avaya Aura® Conference Manager Add-in from the specified location.

Note:

Once installed, the Avaya Aura® Conference Manager Add-in will check for updates every two weeks at the same location from which Avaya Aura® Conference Manager Add-in was installed. Make sure that location contains the latest version of the Avaya Aura® Conference Manager Add-in. To publish an updated version of the Avaya Aura® Conference Manager Add-in, remove the contents of the folder at that location, and then place the new files in that location.

Related Links

Implementing a ClickOnce deployment on page 374

Implementing a centralized software deployment on page 375

Implementing a ClickOnce deployment

Before you begin

- You must have the file *asu_version_date_time.zip* (for example, *asu_1.0.0.176_2012-12-13_15-44-20.zip*) , which is bundled with Collaboration Agent. The file *asu_version_date_time.zip* is located in `/var/mcp/media/prov_pa_installs/outlook/asu` on the server where Avaya Aura® Conferencing 8.0 is installed.
- To use the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®, a user must have:
  - Microsoft Outlook 2007 or Microsoft Outlook 2010 installed
  - an account (with a moderator code) on the Avaya Aura® Conferencing 8.0 system

About this task

Use this procedure to implement the Avaya Aura® Conference Manager Add-in for Microsoft Outlook using the ClickOnce deployment. With the ClickOnce deployment, each user must run the Avaya Aura® Conference Manager Add-in installer.

Procedure

1. Unzip the contents of the file *asu_version_date_time.zip* (for example, *asu_1.0.0.176_2012-12-13_15-44-20.zip*) on a web server that all users can access. The file *asu_version_date_time.zip* contains the installation files for the Avaya Aura® Conference Manager Add-in. The file *asu_version_date_time.zip* is located in `/var/mcp/media/prov_pa_installs/outlook/asu` on the server where Avaya Aura® Conferencing 8.0 is installed.
2. Open your web browser and make sure you can browse the folder on the web server that contains the files you unzipped in Step 1.
3. From the folder that contains the installation files for the Avaya Aura® Conference Manager Add-in, download the file *setup.exe* to a PC running Microsoft Windows.
4. On the Windows PC that contains the file *setup.exe* that you downloaded in Step 3, perform the following steps:
   a. Select **Start > All Programs > Accessories > Command Prompt**.
   b. In the Command Prompt window, type the following command:

      ```
      setup.exe -url="http://FQDN_or_IP_address_of_your_server/Outlook Add-In"
      ```

      where `"http://FQDN_or_IP_address_of_your_server/Outlook Add-In"` is the URL to the folder that contains the Avaya Aura® Conference Manager Add-in installation files.
   c. Upload the modified *setup.exe* file back to the folder that contains the installation files for the Avaya Aura® Conference Manager Add-in.

Comments? infodev@avaya.com

5. Make sure each user performs the following steps to install the Avaya Aura® Conference Manager Add-in:
   a. Open your web browser and go to the folder that contains the Avaya Aura® Conference Manager Add-in installation files.
   b. Click **setup.exe**.
   c. When prompted to run or save setup.exe, click **Run**.
   d. When prompted to confirm that you want to run this program, click **Run**.
   e. In the Avaya Aura Conference Manager Setup dialog box, read the license agreement.
   f. Click **Accept** to accept the terms of the license agreement.
   g. In the Microsoft Office Customization Installer dialog box, click **Install**.

      The Avaya Aura® Conference Manager Add-in is installed.
   h. When the installation is complete, click **Close**.
   i. Start Microsoft Outlook.

      The Avaya Aura dialog box should appear, prompting you to enter your user name, password, and service host.

      The service host is the name of the Web Conferencing Host that you entered in the Provisioning Client window. It must be the hostname, not the IP address.
   j. Enter your user name, password, and address of the service host, and then click **Save**.

Related Links

Deploying the Avaya Aura Conference Manager Add-in for Microsoft Outlook on page 373

Implementing a centralized software deployment

Before you begin

- To use the Avaya Aura® Conference Manager Add-in, the PC must contain the following software:
  - Microsoft Outlook 2007, 2010, and 2013.
  - Microsoft Windows Installer 3.1. (Typically, this is already present on a Windows PC.)
  - Microsoft .NET 4.0 Framework Client Profile
  - Microsoft VSTO 4.0 Runtime
  - Avaya Event Log Source. This software configures the source in the Windows System Event Log so that the Microsoft Outlook Add-in can log events under the name **Avaya Aura Outlook Conference Manager**.

  Microsoft Windows Installer 3.1, Microsoft .NET 4.0 Framework Client Profile, Microsoft VSTO 4.0 Runtime, and Avaya Event Log Source are available in the file *asu_version_date_time.zip* (for example, *asu_1.0.0.176_2012-12-13_15-44-20.zip*), which is bundled with Collaboration

Agent. The file *asu_version_date_time.zip* is located in `/prov_pa_installs/outlook/` on the server where Avaya Aura® Conferencing 8.0 is installed.

- You have Administrative privileges on the Windows PC. (You need to access the Windows Registry.)

About this task

Use this procedure to implement the Avaya Aura® Conference Manager Add-in for Microsoft Outlook using the centralized deployment. With the centralized deployment, you can configure your domain to remotely deploy software to client computers from a central location.

Procedure

1. Unzip the contents of the file *asu_version_date_time.zip* (for example, *asu_1.0.0.176_2012-12-13_15-44-20.zip*) to a folder. The file *asu_version_date_time.zip* contains the installation files for the Microsoft Outlook Add-in. The file *asu_version_date_time.zip* is located in `/prov_pa_installs/outlook/` on the server where Avaya Aura® Conferencing 8.0 is installed.
2. Modify the Windows Registry file *aacAddin.reg* to point to the location of the deployment manifest for the Avaya Aura® Conference Manager Add-in. An example of the manifest setting in the Windows Registry is:

   ```
   "Manifest"="http://localhost/Outlook Add-In v.1.0.0.141/
   Avaya.Aura.ConferenceManager.vsto"
   ```

3. On each client PC, perform the following steps:
   a. Install Microsoft VSTO 4.0 Runtime.
   b. Install Avaya Event Log Source.
   c. Install Microsoft .NET 4.0 Framework Client Profile.
   d. Download and save the file *aacAddin.reg* to your desktop.
   e. Right-click on *aacAddin.reg* and select **Merge**.
   f. Exit Microsoft Outlook.
   g. Restart Microsoft Outlook.
   h. In the Microsoft Office Customization Installer dialog box, click **Install**.

      The Avaya Aura dialog box should appear, prompting you to enter your user name, password, and service host.

      The service host is the name of the Web Conferencing Host that you entered in the Provisioning Client window. It must be the hostname, not the IP address.

   i. Enter your user name, password, and address of the service host, and then click **Save**.

Related Links

Deploying the Avaya Aura Conference Manager Add-in for Microsoft Outlook on page 373

Index

A

Access Control 25
accounting manager
adding 194
adding an accounting storage rule 200
adding an instance 196
deleting 195
deleting an accounting FTP push rule 207
deleting an accounting north bound server feed rule . 204
deleting an accounting storage rule 202
deploying an instance 198
disabling an accounting rule 199
enabling an accounting rule 199
killing an instance 198
modifying 194
modifying an accounting FTP push rule 206
modifying an accounting north bound server feed rule 203
modifying an accounting storage rule 201
modifying an instance 196
restarting an instance 197
starting an instance 197
stopping an instance 197
undeploying an instance 198
viewing the details for an instance 199
account manager
adding accounting north bound server feed rule 202
adding an accounting FTP push rule 204
Active Speaker
modifying the reporting interval 239
add
custom role 31
new role 31
role 31
adding custom role 31
adding IP 121, 122
Add Mapping 37, 39
Add New Role 36, 37
administration
related documentation 17
administration applications 23
administrator responsibilities 16
application servers
adding 227
adding an instance 240
deleting 228
deleting an instance 241
deploying an instance 241
killing an instance 243
modifying 228
modifying an instance 240
modifying the Active Speaker reporting interval 239
modifying the configuration parameters 229
restarting an instance 242
specifying the bandwidth management Session Manager 239
starting an instance 242
stopping an instance 242
undeploying an instance 241
viewing the details of an instance 243
assigning users to role 33
assign users 33
Assign Users 38
assign users to role 33
associated phone numbers
deleting 67
audio messages 256
Audio SRTP 336
configuring 332
modifying the settings 333
auth passcode 360
auth schema 361
Avaya Aura Conferencing
management tools 23
setting the default conference settings 102
Avaya Aura Conferencing software version
determining 80

B

bandwidth management setting
modifying 106
bandwidth optimization 122, 123
built-in roles 25
Built-in roles 25
bulk provisioning 69

C

cascading 124, 275
configuring a regional cascading location 127, 277
cascading trunk codec 285
certificate revocation list
adding 165
deleting 166
viewing 165
certificates
creating for network elements 163
cipher suites
configuring external OAMP cipher suites 161
configuring HTTPS cipher suites 162
configuring OAMP channel cipher suites 161
configuring signaling cipher suites 162
class of service
conference 103, 140, 141, 143

class of service *(continued)*
video ... 137–139
clusters
DCS ... 295
default value ... 322
event conferences ... 327
event conferencing ...
field descriptions ... 328
groups ... 320
hosting location
field descriptions ... 327
hosting locations ... 326
physical location
field descriptions ... 325
physical locations ... 324
reverse proxy ... 321
serving location
field descriptions ... 323
serving locations ... 323
upgrading ... 321
Collaboration Agent ... 81
applying a custom theme ... 94
changing the display order of conference access numbers ... 135
creating a custom theme ... 87
deleting the custom theme ... 96
displaying conference access numbers ... 134–136
downloading and extracting the sample theme ... 88
downloading the custom theme ... 97
forcing an update to the custom theme ... 98
modifying a custom theme ... 94
modifying the logos ... 91
modifying the theme colors ... 89
modifying the title and header ... 92
plug-in ... 108
preparing the custom theme for upload ... 93
replacing the custom theme ... 95
Collaboration Agent managers
adding ... 220
adding an instance ... 222
deleting ... 221
deleting an instance ... 223
deploying an instance ... 223
killing an instance ... 225
modifying ... 221
modifying an instance ... 223
modifying the configuration parameters of an instance ... 222
restarting an instance ... 225
starting an instance ... 224
stopping an instance ... 224
undeploying an instance ... 224
viewing the details for an instance ... 225
Collaboration Library
modifying the settings ... 330
Communication Manager ... 338
conference access numbers
adding ... 131
changing the display order in Collaboration Agent ... 135
deleting ... 133
displaying in Collaboration Agent ... 134–136
managing ... 131
modifying ... 133
conference class of service ... 140
adding ... 140
deleting ... 143
guest login ... 103
modifying ... 141
viewing assigned users ... 142
conferencing
setting the defaults for your system ... 102
conferencing continuation setting
modifying ... 105
conferencing fast start setting
modifying ... 105
conferencing profile ... 56, 58, 60
conferencing settings
modifying for a user ... 71, 72
configuring IP ... 119
continuation setting
modifying ... 105
copy
permission ... 39
Copy All From ... 39
Copy from Role ... 39
copying IP ... 121
copying permission mapping for a role ... 34
customizable prompts ... 256
customizations ... 99
custom music on wait files
about ... 266
deleting ... 268
downloading ... 267
uploading ... 266
custom prompts
about ... 255
deleting ... 265
downloading ... 264
uploading ... 263
custom role ... 29
add ... 31
delete ... 35
edit ... 35
custom roles ... 29
Custom roles ... 25

D

database
adding an instance ... 176
deleting an instance ... 176
starting the monitor service ... 176
stopping the monitor service ... 177
DCS ... 297

DCS *(continued)*
default ... 300
deploying ... 301
eng parm ... 303
instance ... 301
killing ... 303
locations ... 305
restarting ... 302
starting ... 302
stopping ... 302
undeploying ... 301
DCS clusters ... 295
DCS fields ... 296
default prompts
downloading ... 265
delete
role ... 35
delete custom role ... 35
deprecated locations ... 117
directory access server
authentication ... 351
directory access servers
connection credentials ... 349
synchronization ... 350
directory synchronization ... 354
directory synchronization timeouts ... 352
document conversion servers
adding ... 296
deleting ... 300
managing ... 295
modifying ... 297
modifying the Collaboration Library settings ... 330
domains ... 113
adding ... 113, 114
deleting ... 114
managing ... 112
viewing ... 112, 113

E

edit
custom role ... 35
element manager
adding a log FTP push rule ... 192
adding a log north bound server feed rule ... 189
adding a log storage rule ... 187
adding a log UDP client feed rule ... 191
adding an instance ... 181
adding an SNMP manager ... 185
deleting a log FTP push rule ... 193
deleting a log north bound server feed rule ... 190
deleting a log storage rule ... 189
deleting a log UDP client feed rule ... 191
deleting an instance ... 182
deleting an SNMP manager ... 186
deploying an instance ... 183
disabling a log rule ... 186
enabling a log rule ... 186
killing an instance ... 184
modifying ... 178
modifying a log FTP push rule ... 192
modifying a log north bound server feed rule ... 189
modifying a log storage rule ... 188
modifying a log UDP client feed rule ... 191
modifying an instance ... 182
modifying an SNMP manager ... 185
modifying configuration parameters ... 179
restarting an instance ... 184
starting an instance ... 183
stopping an instance ... 183
undeploying an instance ... 183
viewing the details for an instance ... 184
Element Manager Console
changing the password for local logon user IDs ... 365
changing the password for your local logon user ID ... 365
configuring password rules for local logon user IDs ... 366
configuring the login rules for local logon user IDs ... 368
exporting configuration data ... 371
forcing off a logged in user ... 369
importing configuration data ... 371
installing a patch ... 79
local logon ... 364
logging on to ... 44–46
logical view ... 42
Logical View window ... 42
overview ... 39
physical view ... 42
Physical View window ... 43
requirements ... 43
toolbar ... 41
upgrading a network element instance ... 80
viewing information for a load or patch ... 79
viewing users logged in ... 370
window components ... 40
enterprise domain ... 361
enterprise domains
viewing ... 113
Event conference
configuring media server clusters ... 279, 293
event conferencing ... 273, 327, 328
external nodes
adding ... 146
deleting ... 147
modifying ... 146

F

fast start setting
modifying ... 105
field descriptions
Add Mapping ... 37
Assigned Users ... 38
Roles ... 36
FTP push destinations

FTP push destinations *(continued)*
adding ... 156
deleting ... 156
modifying ... 156
refreshing ... 157

G

Group Name ... 37
guest login
modfiying the conference class of service ... 103

H

hosting locations ... 326
configuring ... 126, 276, 277
host tables ... 329
HP Proliant DL360 G8 ... 21
HTTPS cipher suites
configuring ... 162

I

implementation
related documentation ... 19
IP address
pattern-matching ... 119–122
IP addresses
adding ... 144
deleting ... 145
modifying ... 144

K

keystore
deleting a certificate ... 164
view a certificate ... 163

L

LDAP
passcode ... 360
schema ... 354
LDAP domains
viewing ... 113
LDAP integration ... 349–352, 357–359, 362
loads
overview ... 79
locations ... 124, 275
adding ... 116, 117
assigning a media server cluster ... 270, 272, 290, 292
associating a media server cluster ... 269, 289
configuring a hosting location ... 126, 276
configuring a regional cascading location ... 127, 277
configuring hosting locations ... 126, 277
configuring media cascading locations ... 128, 278
configuring media stream cascading ... 124, 272
configuring the media cluster for recording ... 129
deleting ... 117, 118
managing ... 116
modifying ... 117, 118
optimizing bandwidth ... 123
optimizing the bandwidth ... 122
location settings ... 119
log browser feed
refreshing ... 159
log browser feeds
modifying ... 159
log filters
adding ... 157
deleting ... 158
modifying ... 157
refreshing ... 158
logging off from Provisioning Client ... 52
logging on to Provisioning Client ... 50, 51
login rules ... 369
logo ... 99

M

map
permission ... 39
permission from template ... 39
map permission ... 34
map permissions
using templates ... 33
mapping
add ... 37
media cascading locations
configuring ... 128, 278
media cascading setting
modifying ... 104
media server cluster
configuring the location for recording ... 129
media server clusters ... 269, 289
adding ... 281
assigning a physical location (by location) ... 270, 292
assigning a physical location (by media server cluster) ... 272, 290
associating with a location ... 269, 289
configuring an Event conference ... 279, 293
configuring for an Event conference ... 279, 293
configuring trace file history settings ... 288
deleting ... 282
locations ... 270, 291
modifying ... 282
modifying the audio codec settings ... 283
modifying the comfort noise setting ... 288
modifying the database replication settings ... 283
modifying the default cluster ... 283
modifying the DSCP settings ... 286
modifying the media port settings ... 286
modifying the video settings ... 287

media servers 269, 289
about custom music on wait files 266
about custom prompts 255
accessing the session detail record browser 250
adding 244
adding an instance 250
administering a pending lock 254
configuring logs 249
deleting 245
deleting an instance 251
deleting custom music on wait files 268
deleting custom prompts 265
deploying an instance 252
downloading custom music on wait file 267
downloading custom prompts 264
downloading default prompts 265
downloading logs 250
killing an instance 253
locking the service maintenance 254
modifying 244
modifying an instance 251
modifying the configuration parameters 246
restarting an instance 253
starting an instance 252
stopping an instance 253
undeploying an instance 252
unlocking the service maintenance 255
uploading custom music on wait files 266
uploading custom prompts 263
viewing the details for an instance 254
media stream cascading 124, 272, 275
Microsoft Outlook Add-in
centralized software deployment 375
ClickOnce deployment 374
deploying 373
moderator code
modifying the maximum entry attempts setting 104
modifying 66
monitor service
configuring the alarm thresholds for a server 171
deleting the monitor service for the database 176
starting the monitor service for a server 171
starting the monitor service for the database 176
stopping the monitor service for a server 172
stopping the monitor service for the database 177
music on wait
custom files 266
deleting custom files 268
downloading custom files 267
uploading custom files 266

N

network element instance
upgrading 80
network elements
creating a certificate 163
new
role 36

O

OAMP channel cipher suites
configuring 161
OAMP cipher suites
configuring external OAMP cipher suites 161
OAM profiles
adding a log filter 157
adding an FTP push destination 156
adding an OSS endpoint 154
adding an OSS server 153
adding an SNMP manager 159
deleting a log filter 158
deleting an FTP push destination 156
deleting an OSS endpoint 155
deleting an OSS server 154
deleting an SNMP manager 160
modifying a log browser feed 159
modifying a log filter 157
modifying an FTP push destination 156
modifying an OSS endpoint 155
modifying an OSS server 153
modifying an SNMP manager 160
refreshing a log filter 158
refreshing an FTP push destination 157
refreshing an OSS endpoint 155
refreshing an OSS server 154
refreshing the log browser feed 159
online help 20
operator
modifying 103
operators
viewing 77, 78
OSS endpoints
adding 154
deleting 155
modifying 155
refreshing 155
OSS servers
adding 153
deleting 154
modifying 153
refreshing 154
overview
related documentation 18

P

panel mode 109
participant code
modifying the maximum entry attempts setting 104
password owned locally
modifying 107
password owned locally setting

password owned locally setting *(continued)*
modifying 107
patches
installing 79
overview 79
viewing the information 79
permission
copy 39
map 39
permission mapping 33, 39
physical locations 324
plug-in
modifying 108
presentation mode 109
prompts 256
custom prompts 255
deleting custom prompts 265
downloading custom prompts 264
downloading default prompts 265
uploading custom prompts 263
Provisioning Client
configuring the login rules for local logon user IDs 368
logging on to 49
overview 48
provisioning managers
adding an instance 215
deleting 210
deleting an instance 216
deploying an instance 217
killing an instance 218
modifying 208
modifying an instance 216
modifying configuration parameters 210
restarting an instance 218
starting an instance 217
stopping an instance 217
undeploying an instance 217
viewing the details for an instance 218
purge threshold settings
Recording server 344

R

RBAC 25
built-in roles 25
custom roles 29
recording
configuring the location and media server cluster 129
Recording 340
configuring for a user 341
Recording feature
backing up the Recording server 343
modifying the backup and purge settings for the Recording server 344
modifying the purge threshold settings 344
purging the Recording server 343
restoring a backup to the Recording server 345
scheduling a backup of Recording server 341
Recording server
adding a backup location 346
deleting a backup location 347
modifying a backup location 347
recording setting
modifying 107
Recording setting
configuring 340
recording trunk codec 285
regional cascading location
configuring 127, 277
related documentation
administration 17
implementation 19
overview 18
supporting 18
removing users from role 34
reverse proxy 321
role
add 36
assign users 33
copy permission mapping 34
delete 35
details 37
edit 35
new 36
unassign users 34
role based access control 25
Role Details 37
Role page 36
roles
built-in 25
RBAC 29
Service Provider Administrator 25
System Administrator 25
Tenant Administrator 25
Roles 25

S

security code
modifying the maximum entry attempts setting 104
servers
adding 169
configuring the alarm thresholds 171
deleting 170
generating an analysis 172
modifying 169
starting the monitor service 171
stopping the monitor service 172
service URI
adding 132
deleting 132
modifying 132
session detail record browser
viewing records 250

Session Manager element
adding ... 150
deleting ... 152
modifying ... 150
refreshing ... 152
setting the host name ... 331
signaling cipher suites
configuring ... 162
SNMP managers
adding ... 159
deleting ... 160
modifying ... 160
SNMP profile
deleting ... 174
SNMP profiles
adding ... 173
associating with a server ... 174
modifying ... 173
SRTP
modifying the audio settings ... 166, 333
modifying the settings ... 166
supporting
related documentation ... 18
synchronization status ... 357
sync schema ... 355
System default settings
modifying ... 109
System Manager
adding users ... 55
System Manager domains ... 113
adding ... 113, 114
deleting ... 114
System Manager element
modifying ... 148
refreshing ... 148

T

template
map permissions ... 33
Template for permission set ... 33, 39
templates for mapping permission ... 33
truststore
deleting a certificate ... 165
viewing a certificate ... 164

U

UDP
adding a log UDP client feed rule ... 191
deleting a log UDP client feed rule ... 191
modifying a log UDP client feed rule ... 191
unassign users
roles ... 34
user domains ... 113
adding ... 113, 114
deleting ... 114
managing ... 112
viewing ... 112
user roles
view ... 31
users ... 66, 142
adding ... 55, 64
adding from Provisioning Client ... 63
assign ... 38
associated phone numbers ... 67
bulk provisioning ... 69
clearing lockout ... 67
configuring the Recording feature ... 341
deleting ... 67, 73
managing ... 53
modifying ... 65, 67–69
modifying Aura settings ... 67
modifying conferencing settings ... 71, 72
modifying passwords ... 66
searching ... 54
viewing assigned conference class of service ... 142
viewing the list of operators ... 77
user templates
adding ... 75
deleting ... 75, 77
managing ... 74
modifying ... 75, 76

V

video class of service
adding ... 137
deleting ... 137, 139
modifying ... 137, 138
viewing
roles ... 31
user roles ... 31
viewing user roles ... 31

W

WCS clusters
default values ... 322
event conferences ... 327
field descriptions ... 323, 325, 327, 328
hosting locations ... 326
introduction ... 320
new ... 322
physical locations ... 324
reverse proxy ... 321
serving locations ... 323
upgrading ... 321
web conferencing
adding a document conversion server ... 296
adding a management server ... 305
adding a management server instance ... 309
adding a server ... 313
adding a server instance ... 317

serving location *(continued)*
clusters
default 322
deleting a management server instance 310
deleting a server instance 317
deleting document conversion servers 300
deleting management servers 307
deleting servers 314
deploying a management server instance 310
deploying a server instance 318
event conferences 327
event conferencing ....
field descriptions 328
hosting location
field descriptions 327
hosting locations 326
killing a management server instance 312
killing a server instance 319
managing a document conversion server 295
modifying a server instance 317
modifying document conversion servers 297
modifying management server instance 310
modifying management servers 306
modifying servers 314
modifying the Collaboration Library settings 330
modifying the configuration parameters for a management server 307
modifying the configuration parameters for a server .. 315
modifying the meeting event processor for a management server 309
physical location
field descriptions 325
physical locations 324
restarting a management server instance 312
restarting a server instance 319
reverse proxy 321
serving location
field descriptions 323
serving WCSs 323
starting a management server instance 311
starting a server instance 318
stopping a management server instance 311
stopping a server instance 319
undeploying a management server instance 311
undeploying a web conferencing instance 318
upgrade 321
viewing the details for a management server instance 312
viewing the details for a server instance 320
web conferencing host 331
web conferencing host name 331