Avaya Aura® Application Server 5300 Configuration
© 2008-2017, 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 in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

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

Warranty
Avaya provides a limited warranty on Avaya hardware and software. 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: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if 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 an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in your service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service
THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCOMPLISHES 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 OF 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.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" 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 explicitly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. 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 set of Designated Processors that hosts (physically or virtually) 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
Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of 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), 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.

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

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

Virtualization
The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, 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: https://support.avaya.com/Copyright or such successor site as designated by Avaya.

Software License Terms
Instances of the same type of products, then two products of that type must be ordered.

Service Provider
The following applies to Avaya Channel Partner’s hosting of Avaya products or services. The product or Hosted Service may use Third Party Components subject to Third Party Terms and require a Service Provider to be independently licensed directly from the Third Party Supplier. An Avaya Channel Partner’s hosting of Avaya products must be authorized in writing by Avaya and if those hosted products use or embed certain third party software, including but not limited to Microsoft software or codecs, the Avaya Channel Partner is required to independently obtain any applicable license agreements, at the Avaya Channel Partner’s expense, directly from the applicable third party supplier.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML, THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

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

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

Avaya Toll Fraud intervention
If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, 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: https://support.avaya.com or such successor site as designated by Avaya.

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

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

Contact Avaya Support
See the Avaya Support website: https://support.avaya.com for product or 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: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

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

Avaya is a registered trademark of Avaya Inc.

AVAYA

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.

Java is a registered trademark of Oracle and/or its affiliates.
Contents

Chapter 1: New in this release ............................................................................................... 10
  Features ............................................................................................................................. 10
  Document changes since last issue .................................................................................... 10
  Other changes .................................................................................................................. 11

Chapter 2: Introduction ........................................................................................................ 15

Chapter 3: AS 5300 Element Manager Console overview ............................................. 17
  Software and hardware requirements and recommendations ........................................ 17
  AS 5300 Element Manager Console access ..................................................................... 18
  AS 5300 Element Manager Console layout ..................................................................... 19
    Title bar ......................................................................................................................... 19
    Menu bar ....................................................................................................................... 19
    Icon toolbar .................................................................................................................. 20
    Alarm summary bar ....................................................................................................... 20
    Configuration view ....................................................................................................... 21
    Work area .................................................................................................................... 21
    Logical and physical views ............................................................................................ 22
    Logical view .................................................................................................................. 23
    Physical view ................................................................................................................. 23
  AS 5300 Element Manager Console updates .................................................................... 23
  FIPS-compliant AS 5300 Element Manager Console ...................................................... 23

Chapter 4: AS 5300 Element Manager Console usage .................................................. 24
  Installing the AS 5300 Element Manager Console ........................................................ 24
  Uninstalling the AS 5300 Element Manager Console .................................................... 25
  Logging on to the AS 5300 Element Manager Console .................................................. 25
  Configuring DSCP marking before you log on ................................................................. 26
  Logging off from the AS 5300 Element Manager Console .............................................. 27

Chapter 5: Configuration fundamentals .......................................................................... 28
  Configuration management strategy ................................................................................. 28
  Network element instance configuration ......................................................................... 29
  OAMP strategy ................................................................................................................ 32
  Interoperability enhancements ......................................................................................... 32
    SIP Endpoint Protocol Profile ..................................................................................... 33
  Subscriber Lookup and Routing ...................................................................................... 33
  XMPP Gateway .............................................................................................................. 34
    Enabling the XMPP Gateway ...................................................................................... 34
  Network traffic separation ............................................................................................... 35
    AS 5300 Element Manager traffic .............................................................................. 36
    Accounting Manager and Fault Performance Manager traffic ..................................... 36
    Provisioning Manager traffic ...................................................................................... 36
### Chapter 6: System configuration
- System configuration tasks

### Chapter 7: Network data configuration
- Configuring the IPv4 address table
- Configuring the IPv6 address table
- Enabling a license key
- Reducing the number of subscriber licenses
- Configuring the Regional Patch Selector
- Configuring an SNMP profile
- Configuring a site
- Configuring an SMDI server
- Configuring an external node
- Configuring a trusted node
- Configuring an external SIP proxy
- Adding a SIP template
- Specifying a codec on the system
- Importing a new SIP Profile
- Adding a new SIP profile
- Configuring a new SIP profile from a copy
- Enabling SDP ANAT Support for a SIP profile
- Configuring OAMP channel cipher suites
- Configuring external OAMP cipher suites
- Configuring HTTPS cipher suites
- Configuring signaling cipher suites
- Configuring the DSCP marking value for SIP signaling
- Configuring the DSCP marking value for Operations, Administration, Maintenance and Provisioning
- Configuring the DSCP marking value for XMPP
- Configuration of the XMPP DSCP
- Configuring an EBC
- Configuring an SS Session Manager
- Configuring an LSC Session Manager
- Configuring failover group

### Chapter 8: Server configuration
- Configuring a server
- Configuring server alarm thresholds
- Starting the server monitor service
- Deleting a server

### Chapter 9: Database configuration
<table>
<thead>
<tr>
<th>Chapter Title</th>
<th>Start Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring database resource thresholds</td>
<td>86</td>
</tr>
<tr>
<td>Monitoring the database</td>
<td>87</td>
</tr>
<tr>
<td><strong>Chapter 10: Network element configuration</strong></td>
<td>88</td>
</tr>
<tr>
<td>Network element configuration tasks</td>
<td>88</td>
</tr>
<tr>
<td><strong>Chapter 11: Network element addition</strong></td>
<td>90</td>
</tr>
<tr>
<td>Network element addition procedures</td>
<td>90</td>
</tr>
<tr>
<td>Adding a network element</td>
<td>91</td>
</tr>
<tr>
<td>Adding a network element instance</td>
<td>92</td>
</tr>
<tr>
<td><strong>Chapter 12: AS 5300 Element Manager configuration</strong></td>
<td>93</td>
</tr>
<tr>
<td>Configuring AS 5300 Element Manager configuration parameters</td>
<td>93</td>
</tr>
<tr>
<td>Moving the AS 5300 Element Manager network element instance</td>
<td>96</td>
</tr>
<tr>
<td><strong>Chapter 13: Accounting Manager configuration</strong></td>
<td>98</td>
</tr>
<tr>
<td>Configuring Accounting Manager configuration parameters</td>
<td>98</td>
</tr>
<tr>
<td>Configuring the whole Accounting Manager network element</td>
<td>99</td>
</tr>
<tr>
<td>Moving the Accounting Manager network element instance</td>
<td>100</td>
</tr>
<tr>
<td><strong>Chapter 14: AS 5300 Session Manager configuration</strong></td>
<td>102</td>
</tr>
<tr>
<td>Configuring AS 5300 Session Manager configuration parameters</td>
<td>102</td>
</tr>
<tr>
<td>Configuring the whole AS 5300 Session Manager network element</td>
<td>119</td>
</tr>
<tr>
<td>Configuring the Master LSC functional role</td>
<td>121</td>
</tr>
<tr>
<td>Configuring the Slave LSC functional role</td>
<td>123</td>
</tr>
<tr>
<td>Configuring the SS functional role</td>
<td>124</td>
</tr>
<tr>
<td>Moving the AS 5300 Session Manager network element instance</td>
<td>125</td>
</tr>
<tr>
<td><strong>Chapter 15: Provisioning Manager configuration</strong></td>
<td>127</td>
</tr>
<tr>
<td>Configuring Provisioning Manager configuration parameters</td>
<td>127</td>
</tr>
<tr>
<td>Configuring the whole Provisioning Manager network element</td>
<td>135</td>
</tr>
<tr>
<td>Moving the Provisioning Manager network element instance</td>
<td>137</td>
</tr>
<tr>
<td>Configuring Personal Agent parameters</td>
<td>138</td>
</tr>
<tr>
<td><strong>Chapter 16: Avaya Media Server configuration</strong></td>
<td>139</td>
</tr>
<tr>
<td>Avaya MS cluster configuration</td>
<td>139</td>
</tr>
<tr>
<td>Adding an Avaya Media Server</td>
<td>140</td>
</tr>
<tr>
<td>Creating an Avaya MS cluster</td>
<td>142</td>
</tr>
<tr>
<td>Configuring database replication</td>
<td>143</td>
</tr>
<tr>
<td>Adding an Avaya MS SIP Route</td>
<td>144</td>
</tr>
<tr>
<td>Configuring Avaya Media Server configuration parameters</td>
<td>146</td>
</tr>
<tr>
<td>Configuring audio and video CODECs</td>
<td>148</td>
</tr>
<tr>
<td>Enabling and configuring audio CODEC settings</td>
<td>148</td>
</tr>
<tr>
<td>Removing an audio CODEC</td>
<td>149</td>
</tr>
<tr>
<td>Enabling and configuring video CODEC settings</td>
<td>149</td>
</tr>
<tr>
<td>Removing a video CODEC</td>
<td>150</td>
</tr>
<tr>
<td>Adding an Avaya MS license key</td>
<td>151</td>
</tr>
<tr>
<td>Locking the Avaya MS</td>
<td>151</td>
</tr>
<tr>
<td>Locking an Avaya MS with a pending lock</td>
<td>152</td>
</tr>
</tbody>
</table>
## Contents

**Chapter 17: MFSS and LSC configuration**  
MFSS and LSC configuration procedures ......................................................... 162

**Chapter 18: ASAC budget configuration**  
ASAC budget configuration procedures .......................................................... 164
- Configuring a directional audio profile .......................................................... 166
- Configuring a nondirectional audio profile ..................................................... 167
- Configuring a directional video profile .......................................................... 168
- Configuring a nondirectional video profile ..................................................... 169
- Configuring an ASAC budget ...................................................................... 169
- Configuring an ASAC budget for remote locations ...................................... 170

**Chapter 19: Commercial Cost Avoidance configuration**  
- Configuring the expiry timer for the routing cache ........................................ 173
- Configuring the routing cache size ................................................................. 173
- Configuring the cache audit period ............................................................... 174
- Configuring the LDAP connection audit interval .......................................... 174
- Configuring the query count ...................................................................... 175

**Chapter 20: Hybrid routing configuration** ....................................................... 176

**Chapter 21: Destination Code Controls configuration** .................................... 177

**Chapter 22: E911 Manager configuration** ....................................................... 178

**Chapter 23: Fault management configuration**  
Fault management configuration tasks ............................................................ 179

**Chapter 24: Packaged application configuration**  
- Configuring Ad Hoc conferencing ............................................................... 181
- Configuring Meet Me conferencing ............................................................. 182
- Configuring Recorder ............................................................................. 184
  - Configuring Recorder e-mail settings ...................................................... 185
- Configuring Announcements .................................................................... 186
- Configuring Instant Message Chat ............................................................. 187
- Configuring Music on Hold ...................................................................... 189
- Configuring Unified Communications ...................................................... 190

**Chapter 25: Log configuration**  
Log configuration procedures ..................................................................... 191
Configuring a simple log filter................................................................. 193
Configuring a composite log filter........................................................ 194
Configuring the log browser feed.......................................................... 195
Configuring log storage rules................................................................. 196
Configuring the log North-bound Server Feed rule.............................. 197
Configuring log FTP Push rules.............................................................. 199
Enabling and disabling log processing rules......................................... 200
Configuring debug logging.................................................................... 201

Chapter 26: SNMP configuration............................................................ 203
SNMP configuration procedures............................................................ 203
Configuring the SNMP Manager......................................................... 204
Configuring the SNMP Manager for the AS 5300 Element Manager...... 205
Associating an SNMP profile with a server......................................... 205

Chapter 27: Performance management configuration.......................... 207
OM configuration tasks........................................................................... 207
Configuring OM storage rules............................................................... 208
Configuring the OM North-bound Server Feed rule............................ 210
Configuring OM FTP Push rules............................................................ 211
Enabling and disabling OM processing rules....................................... 212

Chapter 28: Accounting records configuration..................................... 215
Accounting records configuration procedures..................................... 215
Configuring accounting storage rules................................................ 217
Configuring the accounting North-bound Server Feed rule................... 218
Configuring Accounting FTP Push rules............................................. 219
Enabling and disabling accounting processing rules........................... 220

Chapter 29: DNS configuration............................................................... 222
Configuring DNS................................................................................ 222

Chapter 30: Common procedures......................................................... 224
Starting a network element................................................................. 224
Stopping a network element............................................................... 225
Deploying a network element............................................................. 226
Undeploying a network element........................................................ 226
Restarting a network element............................................................. 227
Configuring an OSS server................................................................. 228
Configuring an OSS endpoint............................................................. 228
Configuring FTP Push destinations.................................................... 229
Chapter 1: New in this release

The following sections detail what is new in Avaya Aura® Application Server 5300 Configuration, NN42040-500 for Avaya Aura® Application Server 5300 Release 3.0.

Navigation

• Features on page 10
• Other changes on page 11

Features

For information about feature-related changes, see the following sections:

• XMPP Gateway on page 34
• Avaya Media Server configuration on page 139
• Packaged application configuration on page 181
• Enabling and configuring audio CODEC settings on page 148
• E911 Manager configuration on page 178

For information about the features that are new for this release, see Avaya Aura® Application Server 5300 Release Delta, NN42040-201.

Document changes since last issue

The following changes have been made to this document since it was issued for Application Server 5300 Release 3.0 in June, 2012:

• In Logging on to the AS 5300 Element Manager Console on page 25, added information for authentication using Common Access Card (CAC) when multiple certificates are available on the CAC

• Added information about Dual Tone Multi Frequency (DTMF) digit relay, in Configuring DTMF on page 154.
• Added information about the new XMPP Gateway, in the following sections: XMPP Gateway on page 34, Configuring the whole Accounting Manager network element job aid on page 100, and Configuring AS 5300 Session Manager configuration parameters job aid on page 103.

• Made changes to parameter tables in Configuring AS 5300 Session Manager configuration parameters job aid on page 103 and Configuring Provisioning Manager configuration parameters job aid on page 128.

• Updated Adding a SIP template job aid on page 58.

• Modified Destination Code Controls configuration on page 177 indicating that the DCC feature is activated for inter-LSC calls.

• Added a statement to Stopping a network element on page 225, indicating that in-progress conference recordings are lost when an Avaya MS NE is stopped.

• Added a statement to Adding a SIP template job aid on page 58 regarding P-Asserted Identity (PAI).

• Added a statement to Configuring Recorder on page 184, indicating that Recorder counts as a participant when used in conference calls.

• Removed references to SIP Firmware Web Manager.

• Added information about the new E911 Manager node in the following sections: Informational elements job aid on page 55 and E911 Manager configuration on page 178.

• Added support for MCPV5 format in the following sections: Configuring accounting storage rules job aid on page 217, Configuring the accounting North-bound Server Feed rule job aid on page 218, and Enabling and disabling accounting processing rules job aid on page 221.

### Other changes

#### Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2017</td>
<td>Updated the legal page for Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
<tr>
<td>September 2017</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0, Service Pack 14. Added support for new SNMP profiles and updated the following sections: * Configuring an SNMP profile on page 49  * Configuring an SNMP profile job aid on page 50  * Configuring AS 5300 Element Manager configuration parameters job aid on page 94  * Configuring the SNMP Manager on page 204</td>
</tr>
<tr>
<td>April 2017</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0, Service Pack 13.</td>
</tr>
</tbody>
</table>
### New in this release

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
</table>
| November 2016| Added support for MCPV5 in the following sections:  
  - [Configuring accounting storage rules job aid](#) on page 217  
  - [Configuring the accounting North-bound Server Feed rule job aid](#) on page 218  
  - [Enabling and disabling accounting processing rules job aid](#) on page 221                                                                 |
| March 2016   | This document is issued to support Avaya Aura® Application Server 5300 Release 3.0, Service Pack 12.  
  - Added new item to configure DSCP marking value for XMPP under the section [Configuring the DSCP marking value for XMPP](#) on page 75.  
  - Added new item to describe the configuration parameter of the XMPP DSCP under the section [Configuration of the XMPP DSCP](#) on page 75.  
  - Updated the description of the maximum number of ports in the section [Configuring Ad Hoc Conferencing job aid](#) on page 182. |
| July 2015    | This document is issued to support Avaya Aura® Application Server 5300 Release 3.0, Service Pack 11.  
  - Updated [Enabling the XMPP Gateway](#) on page 34.                                                                                                                     |
| December 2014| This document is issued to support Avaya Aura® Application Server 5300 Release 3.0, Service Pack 10.  
  - Added information about the HTTPConnector parameter group in the following sections: [Configuring AS 5300 Element Manager configuration parameters job aid](#) on page 94 and [Configuring Provisioning Manager configuration parameters job aid](#) on page 128. |
| September 2014| This document is issued to support Avaya Aura® Application Server 5300 Release 3.0, Service Pack 9.  
  - Added information about the E911 Manager node in the following sections: [Informational elements job aid](#) on page 55 and [E911 Manager configuration](#) on page 178. |
| April 2013   | Draft 04.20.AA. This document is issued to support Avaya Aura® Application Server 5300 Release 3.0, Feature Pack 1.  
  - Added information about XMPP Gateway in the following sections: [XMPP Gateway](#) on page 34, [Configuring the whole Accounting Manager network element job aid](#) on page 100, and [Configuring AS 5300 Session Manager configuration parameters job aid](#) on page 103. |

*Table continues…*
<table>
<thead>
<tr>
<th>Date</th>
<th>Standard</th>
<th>Document changes since last issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2013</td>
<td>04.09</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
<tr>
<td>March 2013</td>
<td>04.08</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0. Removed references to SIP Firmware Web Manager. Updated Adding a SIP template job aid on page 58.</td>
</tr>
<tr>
<td>February 2013</td>
<td>04.07</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0. Updated the following sections: <em>Logging on to the AS 5300 Element Manager Console</em> on page 25.</td>
</tr>
<tr>
<td>January 2013</td>
<td>04.06</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0. Updated Configuring Recorder on page 184.</td>
</tr>
<tr>
<td>January 2013</td>
<td>04.05</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0. Updated the following sections: <em>Configuring AS 5300 Session Manager configuration parameters job aid</em> on page 103.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added the following section: <em>Configuring DTMF</em> on page 154.</td>
</tr>
<tr>
<td>November 2012</td>
<td>04.04</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
<tr>
<td>September 2012</td>
<td>04.03</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0. Made editorial changes to the following section: <em>Fault management configuration tasks</em> on page 179.</td>
</tr>
<tr>
<td>June 2012</td>
<td>04.02</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0. Changed term System Management Console to Element Manager Console in document.</td>
</tr>
<tr>
<td>May 2012</td>
<td>04.01</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
<tr>
<td>August 2010</td>
<td>02.03</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 2.0. This document is updated after a review.</td>
</tr>
<tr>
<td>May 2010</td>
<td>02.02</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 2.0. This document is updated after a review.</td>
</tr>
<tr>
<td>April 2010</td>
<td>02.01</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 2.0.</td>
</tr>
</tbody>
</table>
New in this release

<table>
<thead>
<tr>
<th>Date</th>
<th>Standard 01.02. This document is issued to support Nortel Application Server 5300 Release 1.0.</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2008</td>
<td></td>
</tr>
<tr>
<td>May 2008</td>
<td>Standard 01.01. This document is new for Nortel Application Server 5300 Release 1.0.</td>
</tr>
</tbody>
</table>
Chapter 2: Introduction

This document contains the procedures required to configure the Avaya Aura® Application Server 5300 system. This document does not cover Primary Rate Interface (PRI) gateway, or integrated access device (IAD) configuration.

For information about Avaya Aura® Application Server 5300 administration and security (including certificate management), see Avaya Aura® Application Server 5300 Administration, NN42040-600 and Avaya Aura® Application Server 5300 Security, NN42040-601.

⚠️ Important:
Throughout this document, the term system refers to the Application Server 5300, unless otherwise noted.

Prerequisites
• Your completed Customer-Specific Information data sheet includes all server names and IP addresses. For a copy of this data sheet, see Avaya Aura® Application Server 5300 Planning and Engineering, NN42040-200.
  • The system installation is complete.
  • The security configuration for the system is complete. For more information about security configuration, see Avaya Aura® Application Server 5300 Security, NN42040-601.
  • You are familiar with the AS 5300 Element Manager Console.
    For more information about AS 5300 Element Manager Console, see AS 5300 Element Manager Console overview on page 17 and AS 5300 Element Manager Console usage on page 24.
  • You are familiar with the Avaya Aura® Application Server 5300 Provisioning Client.
    For more information about the Provisioning Client, see Avaya Aura® Application Server 5300 Security, NN42040-601.

Navigation
• AS 5300 Element Manager Console overview on page 17
• AS 5300 Element Manager Console updates on page 23
• Configuration fundamentals on page 28
• System configuration on page 40
• Network data configuration on page 43
• Server configuration on page 82
• **Database configuration** on page 86
• **Network element configuration** on page 88
• **Network element addition** on page 90
• **AS 5300 Element Manager configuration** on page 93
• **Accounting Manager configuration** on page 98
• **AS 5300 Session Manager configuration** on page 102
• **Provisioning Manager configuration** on page 127
• **MFSS and LSC configuration** on page 162
• **ASAC budget configuration** on page 164
• **Commercial Cost Avoidance configuration** on page 172
• **Hybrid routing configuration** on page 176
• **Fault management configuration** on page 179
• **Log configuration** on page 191
• **SNMP configuration** on page 203
• **Performance management configuration** on page 207
• **Accounting records configuration** on page 215
• **Common procedures** on page 224
Chapter 3: AS 5300 Element Manager
Console overview

This chapter provides an introduction to the AS 5300 Element Manager Console, a Java-based graphical user interface (GUI) that operates on a personal computer (PC), and which interacts with the AS 5300 Element Manager. Use the console to perform the following tasks:

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

The console includes mouse-over help.

Navigation

• Software and hardware requirements and recommendations on page 17
• AS 5300 Element Manager Console access on page 18
• AS 5300 Element Manager Console layout on page 19
• AS 5300 Element Manager Console updates on page 23
• FIPS-compliant AS 5300 Element Manager Console on page 23

Software and hardware requirements and recommendations

Avaya recommends that the management PC (the PC that you use to run the AS 5300 Element Manager Console) meet the minimum requirements described in the following table.

Table 1: Management PC requirements for the console

<table>
<thead>
<tr>
<th>Category</th>
<th>Minimum requirement</th>
<th>Recommended requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>600 MHz Pentium-class or equivalent processor</td>
<td>1.0 GHz (or higher) Pentium-class or equivalent processor</td>
</tr>
</tbody>
</table>

Table continues…
## Category | Minimum requirement | Recommended requirement
---|---|---
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, Microsoft Windows Vista, or Microsoft Windows XP | Microsoft Windows 7, Microsoft Windows Vista, or Microsoft Windows XP |
Network connectivity | 56 Kbps modem | 10Base-T or other fast network connection (such as DSL, Cable, or LAN) |
Internet browser | Microsoft Internet Explorer 6.0 Netscape Communicator 7.0 Mozilla FireFox 3.5 | Netscape Communicator 7.1 or better Microsoft Internet Explorer 6.0 or better Mozilla FireFox 3.5 or better |
Java | Sun JRE Version 1.6.0_05 | Sun JRE Version 1.6.0_05 or better |
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.

---

**AS 5300 Element Manager Console access**

Which system management tasks an administrator can perform depends on the role and permissions assigned to the administrator’s account.

Upon initial installation, an admin user account with secadmin role is created. At least one user with secadmin role must exist in the system at all times. Thus, to remove the default admin user account, you must first add another account with the secadmin role.

For the console, the admin account that has the secadmin role has total control and access to all services. The initial password is admin and the administrator must change this password during the initial log on. For more information about password security and hardening, see *Avaya Aura® Application Server 5300 Administration, NN42040-600* and *Avaya Aura® Application Server 5300 Security, NN42040-601*. 
**Important:**

If more than one person knows the admin (secadmin role) account password, system security is decreased.

The admin (secadmin role) must configure new roles, new accounts, and assign the new accounts roles. For more information, see *Avaya Aura® Application Server 5300 Administration, NN42040-600* and *Avaya Aura® Application Server 5300 Security, NN42040-601*.

---

**AS 5300 Element Manager Console layout**

The AS 5300 Element Manager Console interface consists of a title bar, a menu bar, an icon-based toolbar, a configuration view (left pane), and an editing area (right pane). On the icon-based toolbar, an alarm summary bar indicates the status of the network elements in the system.

**Navigation**

- **Title bar** on page 19
- **Menu bar** on page 19
- **Icon toolbar** on page 20
- **Alarm summary bar** on page 20
- **Configuration view** on page 21
- **Work area** on page 21
- **Logical and physical views** on page 22
- **Logical view** on page 23
- **Physical view** on page 23

---

**Title bar**

The title bar includes the following information:

- the name of the application
- the software version
- the login userid
- the IP address of the AS 5300 Element Manager

---

**Menu bar**

Use the menu bar to access the File, Views, Administration, Tools, and Help menus.
Not all menu options are available for every component or server. Unavailable menu options are disabled.

---

**Icon toolbar**

The icons on the toolbar are button shortcuts. Not all toolbar options are available for every component or server. Icons that appear dimmed are unavailable for the element selected in the configuration view.

*Figure 1: AS 5300 Element Manager Console icon toolbar* on page 20 shows the icon toolbar. The icons from left to right are:

- Alarm browser (appears dimmed until you select a network element)
- OM browser (appears dimmed until you select a network element)
- Log browser (appears dimmed until you select a network element)
- Logical view (opens the Logical View panel)
- Physical view (opens the Physical View panel)
- Refresh (refreshes the current view)

*Figure 1: AS 5300 Element Manager Console icon toolbar*

---

**Alarm summary bar**

This narrow horizontal bar, located below the toolbar, 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 each 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. For more information about managing alarms, see *Avaya Aura® Application Server 5300 Troubleshooting, NN42040-700*.

For information about alarms, see *Avaya Aura® Application Server 5300 Alarms and Logs Reference, NN42040-701*. 
Configuration view

The configuration view appears in the left pane of the AS 5300 Element Manager Console. After you select a leaf node in the tree, a new panel appears in the work area in the right pane. You can collapse and expand the tree structure.

⚠️ Important:

Not all leaf nodes have associated panels. For example, the Chassis and Network Elements root nodes do not have associated panels.

The configuration view is organized into the following five sections:

- Network Data and Mtc—Use this section to define information such as IP addresses, log report formats, Operational Support System (OSS) servers, and other data that does not change often, but must be reused during other configuration tasks. Enter the data in this section to avoid retyping, and typing errors, during other configuration tasks. Use this section to manage License keys for activating features.

- Servers—Use this section to configure servers and to monitor their hardware and operating systems.

- Chassis—Not used for Application Server 5300 configuration.

- Databases—Each Database has a folder. The folder contains the software load and configuration data so that AS 5300 Element Manager can connect to the database. The element manager can then distribute database connection information to other network elements that require database access.

- Network Elements—Use this section to configure all managed and monitored network elements. Each network element type has a folder, and each configured network element has a subfolder. After you select a network element folder, the Alarm Browser, Operational Measurements (OM) Browser, and Log Browser icons become active for that network element. Use this section to make changes to load deployment, configuration parameters, OM, log, and accounting record configuration. Use this section to perform maintenance tasks, such as start and stop, for network elements.

Work area

The work area is the right pane of the AS 5300 Element Manager Console. After you select a node from the configuration view pane, a panel appears in the work area. Panels in the work area display information about the selected node. Some configuration view nodes (Network Data and Mtc and Network Elements) have no associated panels.

Figure 2: Configuration panel icons on page 22 shows the icons that appear on panels that open in the work area. From left to right, the icons are:

- Add: add an element
• Edit: make changes to an existing element (appears dimmed until after you make a selection in the panel)
• Delete: remove an existing element (appears dimmed until after you make a selection in the panel)
• Refresh: update information in the configuration, logical, and physical views and in the configuration panels

Figure 2: Configuration panel icons

The NE Maintenance leaf node is available for each network element (expanded in the configuration view). Figure 3: NE maintenance panel icons on page 22 shows the icons that appear on the NE maintenance panels. From left to right the icons are:
• Deploy
• Undeploy
• Start
• Stop
• Restart
• Kill

Figure 3: NE maintenance panel icons

Logical and physical views

The Logical View and Physical View panels organize network elements (NE) by element type and location, respectively. You can use these panels to diagnose fault conditions. You open these views from the icon toolbar; for more information, see Figure 1: AS 5300 Element Manager Console icon toolbar on page 20.

Figure 4: Logical View and Physical View icons on page 22 shows the icons that appear on the Logical View and Physical View panels. These icons appear dimmed until after you select a network element.

Figure 4: Logical View and Physical View icons
The Icons, which appear are (from left to right):

- Alarm browser
- OM browser
- Log browser

Logical view

The logical view panel provides a graphical view of NEs, servers, and logical databases. In this view, you cannot determine which NEs are deployed on which servers.

Use this view to see the alarm conditions for all equipment, for each NE type. to enable The alarm, log and OM browser buttons appear dimmed until you select an NE instance, or a server. For Avaya Media Server (MS), only the Alarm and Log Browser buttons are available.

Logical View organizes the network element instances by type.

Physical view

The physical view panel provides a graphical view of the system. The elements are organized by site and server, and then by the network element applications deployed on the server.

Use this view to see alarm conditions for all monitored equipment, in each site. The alarm, log and OM browser buttons appear dimmed until you select an NE instance, or a server. For Avaya Media Server (MS), only the Alarm and Log Browser buttons are available.

AS 5300 Element Manager Console updates

After the initial installation, the software checks for updates each time you start it. If an update is available, the download and installation are automatic.

FIPS-compliant AS 5300 Element Manager Console

For a FIPS-compliant system, you can download a zip file from the AS 5300 Element Manager that contains the jar files and batch file required to run the AS 5300 Element Manager Console in FIPS mode.

For more information about how to install and update the FIPS-compliant AS 5300 Element Manager Console, see Avaya Aura® Application Server 5300 Security, NN42040-601.
Chapter 4: AS 5300 Element Manager Console usage

About this task
This chapter provides procedures for using the AS 5300 Element Manager Console.

Navigation
- Installing the AS 5300 Element Manager Console on page 24
- Uninstalling the AS 5300 Element Manager Console on page 25
- Logging on to the AS 5300 Element Manager Console on page 25
- Configuring DSCP marking before you log on on page 26
- Logging off from the AS 5300 Element Manager Console on page 27

Installing the AS 5300 Element Manager Console

About this task
The AS 5300 Element Manager Console uses Java Webstart technology. You must download the software to the management PC. Perform this procedure to install the AS 5300 Element Manager Console on the management PC.

Procedure
1. On the management PC, open Internet Explorer (IE).
2. In the IE address bar, enter: http://<IP address>:12120
   If HTTP port is disabled for the AS 5300 Element Manager, launch the AS 5300 Element Manager Console using: https://<IP address>:12121
3. On the <IP address>/index.html page, click Launch Element Manager Console.
   The AS 5300 Element Manager Console installs automatically. After the installation is complete, the log on dialog box appears.
Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP address&gt;</td>
<td>This value is the service IP address of the AS 5300 Element Manager.</td>
</tr>
</tbody>
</table>

Uninstalling the AS 5300 Element Manager Console

About this task
Perform this procedure to remove the AS 5300 Element Manager Console software from the management PC.

Procedure
1. On the management PC, open the Control Panel.
2. Double-click Add Remove Programs.
3. From the list of installed programs, select AS 5300 Element Manager - <IP address>, and click Remove.
4. To confirm the file deletion, click OK.

Logging on to the AS 5300 Element Manager Console

About this task
Perform this procedure to log on to the AS 5300 Element Manager Console. If your system supports security mode, you can use secure mode to connect to the AS 5300 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. For more information about DSCP configuration, see Configuring DSCP marking before you log on on page 26.

Prerequisites
- You have an account for the AS 5300 Element Manager Console.
Procedure

1. On the management PC, open Internet Explorer.
2. In the Address bar, type one of the following options, and press Enter.

<table>
<thead>
<tr>
<th>Choice Option</th>
<th>Choice Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP://&lt;IP address&gt;:12120</td>
<td>normal access</td>
</tr>
<tr>
<td>HTTPS://&lt;IP address&gt;:12121</td>
<td>secure access</td>
</tr>
</tbody>
</table>

3. If a certificate selection window appears, select a certificate, and click Apply. If you choose a certificate that is on a Common Access Card (CAC), you are prompted for a PIN. Enter the PIN associated with the CAC.
4. On the <IP address> page, click Launch Element Manager Console.
5. From the Service Address list on the Element Manager Console connection dialog box, select the IP address of the AS 5300 Element Manager.
6. Click Connect.
7. On the AS 5300 Element Manager Authentication dialog, select Accept the certificate for this session only, and click Apply.
8. A login dialog appears. Enter your UserID and Current Password. If you are already logged in on another session, select ForceOut.
9. Click OK.
10. A login banner appears. Read the security message and select the check box to acknowledge that you have read and understood the message.
11. Click Continue.

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP address&gt;</td>
<td>This value is the logical IP address of the AS 5300 Element Manager component.</td>
</tr>
</tbody>
</table>

Configuring DSCP marking before you log on

About this task

You can configure the 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.
Prerequisites

- You have an account for the AS 5300 Element Manager Console.

Procedure

1. On the management PC, open Internet Explorer (IE).
2. In the **IE Address** bar, enter:

<table>
<thead>
<tr>
<th>Access Type</th>
<th>Address Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal access</td>
<td>HTTP://&lt;IP address&gt;:12120</td>
</tr>
<tr>
<td>Secure access</td>
<td>HTTPS://&lt;IP address&gt;:12121</td>
</tr>
</tbody>
</table>

3. On the `<IP address>/index.html` page, click **Launch Element Manager Console**.
4. On the Element Manager Console dialog, click **Advanced**.
5. Use the right arrow to scroll through the tabs, and click the **DSCP Marking** tab.
6. Configure the values for the **High Throughput Data** and **Low Latency Data** parameters.
7. Click **Ok**.

### Configuring DSCP marking before you log on job aid

**About this task**

The following table lists and describes the DSCP marking parameters that you can configure offline, before you log on to the AS 5300 Element Manager Console.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Throughput Data</td>
<td>This parameter controls outgoing network packets</td>
</tr>
<tr>
<td></td>
<td>Range: 0-63</td>
</tr>
<tr>
<td></td>
<td>Default: 16</td>
</tr>
<tr>
<td>Low Latency Data</td>
<td>This parameter controls outgoing network packets</td>
</tr>
<tr>
<td></td>
<td>Range: 0-63</td>
</tr>
<tr>
<td></td>
<td>Default: 18</td>
</tr>
</tbody>
</table>

### Logging off from the AS 5300 Element Manager Console

**About this task**

After you finish working with the AS 5300 Element Manager Console, log off to end your session. Perform this procedure to log off the AS 5300 Element Manager Console.

**Procedure**

To terminate a session, from the AS 5300 Element Manager Console menu bar, select **File > Exit**.
Chapter 5: Configuration fundamentals

This section provides strategies and methodologies for the initial operational configuration of the Avaya Aura® Application Server 5300. For information about the day-to-day administration of the system, see Avaya Aura® Application Server 5300 Administration, NN42040-600. For information about security (configuration and administration), see Avaya Aura® Application Server 5300 Security, NN42040-601.

Navigation

- Configuration management strategy on page 28
- Network element instance configuration on page 29
- OAMP strategy on page 32
- Interoperability enhancements on page 32
- Subscriber Lookup and Routing on page 33
- XMPP Gateway on page 34
- Network traffic separation on page 35

Configuration management strategy

Avaya delivers preconfigured Session Initiated Protocol (SIP)-based IP network solutions. Process and tool development is geared to this strategy. As a result, custom engineering is offered only at an additional cost through Avaya Services.

After the installation and base commissioning are complete, the customer can use the following checklist to verify completion:

- All appropriate hardware equipment and software loads have been installed and loaded as follows:
  - The network is cabled and connected.
  - All cards are installed.
  - Grounding is implemented for safety.
- All network topology (physical characteristics) is implemented as planned.
- Installation validation procedures are complete and components are found to be operational. (For example, after you install and load software and power on pieces of equipment, you commission the equipment.)
Network element instance configuration

Configuration of a network element instance is a statement of intent; the act of configuration does nothing to bring the instance into being. The network element does not physically exist until it has been deployed. Deployment of an element is the act of populating a server's file system with the software load and data files needed by that element in order to run. Undeployment is the reverse operation; the file system is purged of the instance's software and data files. The NE daemon running on the server is responsible for carrying out these activities at the instigation of personnel.

After an instance has been deployed, the Start operation brings it into service in order to provide its intended function in the network. The Stop operation takes the instance out of service gracefully (allowing for system cleanup prior to shutdown). These maintenance activities are also carried out through the NE daemon running on the server. The Restart button is a shortcut for Stop followed by Start.

The NE daemon keeps track of instances that it has started and will restart them if they exit unexpectedly. If a restart attempt fails it will be repeated immediately. If it fails again a third attempt is made. If that attempt also fails, NE daemon waits five minutes and will then try three additional times. If those restart attempts also fail, NE daemon will continue to start the given instance indefinitely.

The Kill button forcibly terminates the instance by using the sigterm -9 signal. The instance immediately terminates, bypassing the shutdown process (no graceful cleanup).

Both deploying and starting an instance panel (and the reverse of these operations) are maintenance operations.

The following figure shows the application area containing the network element instance maintenance panel.
Figure 5: Accounting Manager Instance Maintenance states

The Oper column in the preceding figure shows the maintenance state of the network element instance. It contains one of the values described in the following table.

Table 2: Network element states

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIGURED</td>
<td>The instance is configured but not yet deployed.</td>
</tr>
<tr>
<td>DEPLOYING</td>
<td>The Deploy operation puts the instance into this state, where it remains until deployment is complete. Successful deployment sets the state to OFFLINE; if deployment fails for any reason, the status returns to CONFIGURED.</td>
</tr>
<tr>
<td>OFFLINE</td>
<td>The instance is deployed but is not running.</td>
</tr>
<tr>
<td>STARTING</td>
<td>The Start operation puts the instance into this state. The instance remains in this state until the NE daemon has started the instance and the instance is able to communicate with the AS 5300 Element Manager.</td>
</tr>
<tr>
<td>CONNECTED</td>
<td>The instance progresses to this state when the instance initiates communication with the AS 5300 Element Manager</td>
</tr>
<tr>
<td>INITIALIZING</td>
<td>After you start a network element, it goes through this state to initialize all the subsystems that need to be activated.</td>
</tr>
<tr>
<td>SYNCHRONIZING</td>
<td>All network elements that are provisioned as a pair have an active and inactive node. When the second node is started, the &quot;Oper&quot; status shows the status of syncing. This indicates that the NE should not be failed over. Some feature functionality is not guaranteed to work if an NE is failed over while the inactive unit is still syncing.</td>
</tr>
<tr>
<td>HOT STANDBY</td>
<td>The instance progresses to this state after its subsystems initialize and synchronization with the active instance is complete and the system determines that the instance should be in standby mode</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTIVATING</td>
<td>The instance progresses to this state after it initializes and is ready to become ACTIVE. All the subsystems are activating as part of this phase.</td>
</tr>
<tr>
<td>ACTIVE</td>
<td>The instance progresses to this state after it is operational and capable of providing service.</td>
</tr>
<tr>
<td>STOPPING</td>
<td>The Stop operation puts the instance into this state. It remains in this state until the instance shuts itself down at which time it moves to the OFFLINE state.</td>
</tr>
<tr>
<td>ROGUE</td>
<td>The instance is running, but it is not managed by the AS 5300 Element Manager.</td>
</tr>
</tbody>
</table>

The Logical View panel also appears if an instance is in a running or a non-running state. Any state other than ACTIVE or HOT STANDBY is considered a non-running state. An instance with a non-running state appears in the Logical View panel with a gray down-arrow beside the instance name. See Figure 6: Running and non-running instances of Accounting Managers on page 31. After an instance is in ACTIVE or HOT STANDBY state, it is considered to be running. In the AS 5300 Element Manager Console, a green color circle next to the instance name indicates a running state.

If an instance is ACTIVE and if there are no alarms against that instance, the instance appears with a green circle beside it. If the instance is not running, it appears with a gray down-arrow. All the other states (yellow, red, orange, blue) indicate that the instance is running and has alarms against it.

The following figure shows a non-running instance of the Accounting Manager (AM1_0) and a running instance of the Accounting Manager (AM2_0).

![Logical View: Running and non-running instances of Accounting Managers](image)

Figure 6: Running and non-running instances of Accounting Managers
OAMP strategy

The system uses File Transfer Protocol (FTP) push or Secure File Transport Protocol (SFTP) pull to deliver formatted records to OSS servers. A formatted record file becomes a candidate for transfer to the Operation Support System (OSS) server after it closes (when it is no longer being written by the recording system).

You can configure the recording stream formats, if required.

Important:

If no FTP push is configured, it is assumed that the system retrieves records through SFTP pull. The system does not generate alarms for this scenario and records left on the disk past the seven-day retention period are deleted.

Interoperability enhancements

The system interacts with a variety of clients. Because of differences in SIP implementation and service configuration in each client and gateway, the system supports unique signaling for each endpoint. SIP Endpoint Protocol Profiles manage the actual SIP signaling between the system and external elements. The SIP Endpoint Protocol Profile/Template design provides the following capabilities:

- The SIP Endpoint Protocol Profile captures all information needed to determine how to manage the SIP messaging and how to determine when a particular profile should be used.
- The SIP Endpoint Protocol Profile component provides the system the ability to automatically create a messaging profile for new elements when they are connected.
- The SIP Endpoint Protocol Profile component provides a series of protocol templates that the operator can use to more easily populate a SIP Endpoint Protocol Profile when it is either manually or automatically created.
- The SIP Endpoint Protocol Profile component provides transparent conversion to the new system over upgrade from previous discriminator file based systems.
- The SIP Endpoint Protocol Profile component provides debugging assistance that helps the operator debug endpoint interoperation issues.

For more information about this feature, see the following procedures:

- Adding a SIP template on page 58
- Adding a new SIP profile on page 68
- Configuring a new SIP profile from a copy on page 69
SIP Endpoint Protocol Profile

A SIP Endpoint Protocol Profile captures all the information needed to determine how to manage the SIP messaging and to determine when a particular profile should be used. The AS 5300 Element Manager Console provides the interface for defining SIP protocol profiles.

By default, the system contains many defined profiles. The most commonly used profiles are:

- AudiocodesSipGateway
- AudiocodesSipGatewayMP
- AvayaMAS
- MASIPv6
- audiocodes
- audiocodesIPv6
- cs1kpbx
- genericpbx
- nortelipphone11xx
- nortelpcc7
- pri
- sipprigateway

Subscriber Lookup and Routing

With the Subscriber Lookup and Routing (SLR) feature, Application Server 5300 sites can share a single domain, which is called a multisite. This feature allows locating and routing messages to a subscriber on a multisite domain in a separate site. This function is performed through a query to the Lightweight Directory Access Protocol (LDAP) server. All provisioning details of sites in a multisite are stored both in the Database and LDAP.

This feature also allows Subscriber Mobility between the Application Server 5300 sites in a multisite domain. A user can gain access to their account from a client homed in another site. This feature does not require that the user changes the proxy information, but rather the user enters the user name and authentication information, and the system determines the location for that subscriber. Each subscriber (whether in single site or multisite domain) is associated directly with a home AS 5300 Session Manager as opposed to his domain being associated to the Server home.
XMPP Gateway

With an Extensible Messaging and Presence Protocol (XMPP) Gateway, subscribers can:

• exchange instant messages (IM) with external XMPP users or remote AS 5300 users.
• exchange presence updates with external XMPP users or remote AS 5300 users.
• DNS must be configured on all the Application Server 5300 servers hosting the Session Managers.

You must configure the DNS server, enable and configure the XMPP gateway, and ensure that certificates are installed for TLS. For more information about configuring the XMPP Gateway, see Configuring the whole AS 5300 Session Manager network element on page 119 and Enabling the XMPP Gateway on page 34.

The following prerequisites apply:

• A valid certificate must be available for establishing TLS connections
• DNS must be configured on the Application Server 5300 server.
• The port 5269 must be open in the Access Control List (ACL), thereby allowing XMPP packets. For more information, see the Method of Procedure 105.13 AS 5300 Security Hardening.

You must configure the following:

• Enable the AS 5300 Session Manager configuration parameter mutual authentication for XMPP TLS. For more information, see Configuring AS 5300 Session Manager configuration parameters on page 102.
  
  This feature supports XMPP with TLS only (not XMPP with TCP).

• Configure the DNS for Application Server 5300. For more information, see Configuring DNS on page 222.

• For each subscriber who uses this feature, you must assign the XMPP Gateway service, and configure an XMPP user name. For more information, see Application Server 5300 Using the Provisioning Client (NN42040–112) and Application Server 5300 Personal Agent (NN42040–105).

This feature is controlled by the Presence Subscriber license keycode.

Enabling the XMPP Gateway

About this task

Use the AS 5300 Element Manager Console to enable the XMPP Gateway for Session Managers.

Before you begin

• You can access the AS 5300 Element Manager Console.
• You have a valid client certificate.
**Note:**

A valid client certificate is required to establish TLS connections.

**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements >Session Managers**.

2. In the Session Managers window, select the entry for the network element to modify and click **Edit (+/-)**.

3. In the Edit <Session Manager instance> dialog box, in the Transport section, check the **Enable XMPP TLS** check box.

4. In the **SIP XMPP S2S Port** field, enter 5269.

5. In the **SIP XMPP C2S Port** field, enter 5222.

6. From the **Sesm XMPP Certificate** drop-down list, select a valid client certificate.

7. Click **Apply**.

---

**Network traffic separation**

To support traffic separation on the application side, server configuration includes Internal OAM (Default), External OAM, Signaling, and Media IP addresses. Server monitoring includes all physical Ethernet network interfaces that are configured as members of bonded interfaces.

You can separate traffic into (up to) four different subnets, based on traffic type.

**Table 3: Traffic separation by type**

<table>
<thead>
<tr>
<th>Traffic type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal OAMP</td>
<td>OAMP traffic internal to the Enclave</td>
</tr>
<tr>
<td></td>
<td>Example: AS 5300 Element Manager-NE, Local AS 5300 Element Manager-AS 5300</td>
</tr>
<tr>
<td></td>
<td>Element Manager, AS 5300 Element Manager/Provisioning Manager-Local Operational Support System (OSS) (such as Switch Expert)</td>
</tr>
<tr>
<td>External OAMP</td>
<td>OAMP traffic external to the Enclave</td>
</tr>
<tr>
<td></td>
<td>Example: AS 5300 Element Manager/Provisioning Manager-External Operational Support System (OSS) (such as ADIMSS)</td>
</tr>
<tr>
<td>Signaling</td>
<td>Call signaling and Personal Agent signaling</td>
</tr>
<tr>
<td></td>
<td>Example: All SIP signaling and service profile downloads</td>
</tr>
<tr>
<td>Media</td>
<td>Bearer traffic</td>
</tr>
<tr>
<td></td>
<td>Example: Avaya Media Server (MS) Real Time Protocol (RTP) streams</td>
</tr>
</tbody>
</table>
For more information about configuration for network traffic separation, see the following sections:

- AS 5300 Element Manager traffic on page 36
- Accounting Manager and Fault Performance Manager traffic on page 36
- Provisioning Manager traffic on page 36
- Avaya Media Server traffic on page 36
- OSS traffic on page 37
- VLAN tagging on page 37
- VLAN separation on page 38

---

**AS 5300 Element Manager traffic**

The Internal OAM service address that you configure in the AS 5300 Element Manager Console for the AS 5300 Element Manager, is the same as the Application Programming Interface (API) service address. You configure the HTTP port and X509 certificate for the External OAM service address in the same manner as that of the Internal OAM (default) service address except it is labeled external to differentiate the two. To configure the External OAM service address, you must first configure the Internal OAM service address. The AS 5300 Element Manager Console and OMI both reject the request to configure the External OAM service address if the Internal OAM service address is not already configured.

---

**Accounting Manager and Fault Performance Manager traffic**

The Internal OAM service address that you configure in the AS 5300 Element Manager Console for the Accounting Manager and the Fault Performance Manager, is the same as the API service address. To configure the External OAM service address, you must first configure the Internal OAM service address. The AS 5300 Element Manager Console and OMI both reject the request to configure the External OAM service address if the Internal OAM service address is not already configured.

---

**Provisioning Manager traffic**

A Provisioning Manager instance can run on a server with an External OAM server address. The AS 5300 Element Manager Console and OMI support the configuration of a separate certificate for external OAM access, for such instances.

---

**Avaya Media Server traffic**

Traffic separation requires the configuration of multiple IP addresses and to configure an Avaya MS you associate a server with the Avaya MS instead of an IP address. With this configuration, you can
configure Internal OAM (default), External OAM, Signaling and Media IP addresses for the Avaya MS.

### OSS traffic

The supported traffic types for communication between the Application Server 5300 system and the Operational Support System (OSS) servers are:

- North bound SNMP traps
- FTP push (accounting, OMs, logs)
- North bound log feeds

You can configure the local IP address that a network element uses to communicate with the OSS. For more information, see the following sections:

- [Fault management configuration](#) on page 179
- [Log configuration](#) on page 191
- [Performance management configuration](#) on page 207

### VLAN tagging

The Internal OAM (Default) network was previously known as the Service LAN. You must configure VLAN tagging before you can separate other traffic types (such as External OAM, signaling, and media).

The following figures depict the network before and after VLAN tagging.

[Figure 7: Before VLAN tagging](#)
VLAN separation

After you configure VLAN tagging, you can separate traffic by creating an external VLAN. The following figures depict the network before and after VLAN separation.

Figure 8: After VLAN tagging

Important:

VLAN ID 101 is used for demonstration purposes. Check with the network administrator for the VLAN ID assigned to your network.

For more information, see 105.1.1 AS5300 Network Separation.
Important:

VLAN ID 101 and 102 are used for demonstration purposes. Check with the network administrator for the VLAN IDs for your network.
Chapter 6: System configuration

This chapter provides an overview of the Avaya Aura® Application Server 5300 configuration.

System configuration tasks

About this task

This workflow provides the sequence of tasks that you perform to configure the Avaya Aura® Application Server 5300 system.
Figure 11: System configuration tasks

Navigation

- Network data configuration on page 43
- Server configuration on page 82
- Network element configuration on page 88
- Database configuration on page 86
System configuration

- **Fault management configuration** on page 179
- **Performance management configuration** on page 207
- **Accounting records configuration** on page 215
Chapter 7: Network data configuration

About this task
This chapter provides procedures that you use to configure network data. Network data is organized in the AS 5300 Element Manager Console under Network Data and Mtc.

Navigation
- Configuring the IPv4 address table on page 44
- Configuring the IPv6 address table on page 45
- Enabling a license key on page 46
- Reducing the number of subscriber licenses on page 48
- Configuring the Regional Patch Selector on page 49
- Configuring an SNMP profile on page 49
- Configuring a site on page 51
- Configuring an SMDI server on page 52
- Configuring an external node on page 53
- Configuring a trusted node on page 54
- Configuring an external SIP proxy on page 56
- Adding a SIP template on page 58
- Specifying a codec on the system on page 67
- Importing a new SIP Profile on page 67
- Adding a new SIP profile on page 68
- Configuring a new SIP profile from a copy on page 69
- Enabling SDP ANAT Support for a SIP profile on page 70
- Configuring OAMP channel cipher suites on page 71
- Configuring external OAMP cipher suites on page 71
- Configuring HTTPS cipher suites on page 72
- Configuring signaling cipher suites on page 72
- Configuring the DSCP marking value for SIP signaling on page 73
- Configuring the DSCP marking value for Operations, Administration, Maintenance and Provisioning on page 74
Configuring the IPv4 address table

About this task
Perform this procedure to add addresses to the IPv4 address table.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have AddressService privileges.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > Addresses > IPv4 Addresses.
2. On the IPv4 Addresses window, perform any of the following actions required:
   - To add a new IPv4 address, click Add (+)
   - To update an existing IPv4 address, select the address and click Edit (-/+)
   - To delete an existing IPv4 address, select the address and click Delete (-) and then click Yes to confirm
3. To add an IPv4 address, configure the Logical Name and IPv4 Address parameters on the Add IPv4 Address window.
   OR
   To update an IPv4 address, change the Logical Name and IPv4 Address parameters as required.
4. Click Apply.
5. Repeat 1 on page 44 to 4 on page 44 for each IPv4 address to add or update.

Configuring the IPv4 address table job aid

The following table lists and describes the parameters used to configure IPv4 address table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Name</td>
<td>Enter a logical name to identify the IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>Range: 1 – 20 alphanumeric characters</td>
</tr>
</tbody>
</table>

Table continues...
Configuring the IPv6 address table

About this task
Perform this procedure to add addresses to the IPv6 address table.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have AddressService privileges.
- Dual-Stack IPv4/IPv6 is present in the license key.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > Addresses > IPv6 Addresses**.
2. On the IPv6 Addresses window, perform any of the following actions required:
   - To add a new IPv6 address, click **Add (+)**
   - To update an existing IPv6 address, select the address and click **Edit (-/+)**
   - To delete an existing IPv6 address, select the address and click **Delete (-)** and then click **Yes** to confirm
3. If you chose to add an IPv6 address, configure the **Logical Name** and **IPv6 Address** parameters on the Add IPv6 Address window.
   OR
   If you chose to update an IPv6 address, change the **Logical Name** and **IPv6 Address** parameters as required.
4. Click **Apply**.
5. Repeat 1 on page 45 to 4 on page 45 for each IPv6 address to add or update.

Configuring the IPv6 address table job aid

The following table lists and describes the parameters used to configure IPv6 address table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Address</td>
<td>Enter a valid IPv4 address (written in four groups separated by periods in the format xxx.xxx.xxx.xxx, each group containing a value between 0 and 255).</td>
</tr>
</tbody>
</table>
## Parameter and Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Name</td>
<td>Enter a logical name to identify the IPv6 address. Range: 1 – 20 alphanumeric characters</td>
</tr>
</tbody>
</table>
| IPv6 Address       | Enter a valid IPv6 address (written in eight groups separated by colons in the format
|                    | You can enter any valid IPv6 address format here, including the format separated by :: to compress long strings of 0 values (for example, EE01::001). |

---

### Enabling a license key

**About this task**

Use this procedure to enable a license key.

A license key is used to activate specific features and services, (for example, Application Manager service and Network-based call log service) which require license keys for activation.

**Prerequisites**

- You can access the AS 5300 Element Manager Console.
- You have already downloaded the license keys using the Keycode Retrieval System (KRS). For more information, see the KRS documentation located at [http://www.avaya.com](http://www.avaya.com).

**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc >Licensekey**.
2. On the Licencekey window, do one of the following:
   - For a fresh install, click **Add (+)**.
   - To update an existing license key, click **Edit (-/+)**.
3. Navigate to the license key file on the local workstation, select the file, and then click **Open**.
4. Optional. Click the **Features** tab to see the list of enabled features.

### Enabling a license key job aid

This job aid provides a list of major Application Server 5300 services that are activated with their license keys. This is not a comprehensive list of license keys.

- Advanced Screening
• Network Call Log
• Presence
• Unified Communications
• Application Manager service
• SH Interface
• Vertical Service Codes
  - Call Forward Variants Subscribers
  - Do Not Disturb Subscribers
  - Anonymous Call Rejection Subscribers
  - Network Call Waiting Subscribers
  - Calling Line ID Restriction Subscribers
  - Call Return Subscribers
  - Short Dialing Codes Subscribers
  - Malicious Call Trace subscribers (existing)
• Call Type Based Screening and Selective Call Reject
  - Call Type Based
  - Deny All Calls service
  - Selective Reject service
• Embedded Web Service Gateway
  - Presence web service
  - Multimedia messaging web service
  - Third Party Call web service
  - E911 Public IP
• PBX Communicator Subscribers
• Session Policy Server
• Uniform Call Distribution (UCD)
• Avaya Aura® Application Server 5300 UC Client Control of SIP Terminal (PCCoST)
• SLR Mobility Subscribers
• Mobile Extension Subscribers
• Call Grabber Subscribers
• Hunt Group
• Equal Access Subscribers
Reducing the number of subscriber licenses

About this task
Use this procedure to reduce (decrement) the number of subscriber licences on the system.

Prerequisites:
- You have the Application Admin (AA) role.
- You can access the Element Manager Console.
- You have NEService privileges.
- A new license file is uploaded to the primary Element Management System (EMS) server.

Procedure
1. Log on to the AS 5300 Element Manager Console.
2. Stop all NEs except SESM NEs, AMS NEs, and primary EMS NE, by completing the steps in Stopping a network element on page 225.
3. Log on to the primary EMS server as a user with AA role (ntappadm).
4. Change directory: `cd /var/mcp/install`
5. Run the script to stop the primary AS 5300 Element Manager: `./emStop.pl`
6. Run the script to decrement licenses: `./licenseDecrement.pl`
7. At the script prompts, enter:
   a. The path to the new license key file (`-l` argument)
   b. The maximum value for SubscriberRefLimitKey (Subscribers) (`-s` argument)
   c. The maximum value for PresenceComboKey (Presence subscribers) (`-p` argument)
8. Run the script to start the primary AS 5300 Element Manager: `./emStart.pl`
9. For each NE that you shut down, start the NE by completing the steps in Starting a network element on page 224.
Reducing the number of subscriber licenses job aid

About this task

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-l</td>
<td>Path to the new license file.</td>
</tr>
<tr>
<td>-s</td>
<td>The maximum value for SubscriberRefLimitKey (Subscribers).</td>
</tr>
<tr>
<td>-p</td>
<td>The maximum value for PresenceComboKey (Presence subscribers).</td>
</tr>
</tbody>
</table>

Configuring the Regional Patch Selector

About this task

Perform this procedure to configure the Regional Patch Selector (RPS) to deliver patches.

Prerequisites

- You can access the AS 5300 Element Manager Console.
- You know the site name (as it appears in the RPS system).

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc**, Regional Patch Selector.
2. Select the **Integrate with Regional Patch Selector** check box.
3. In the **Site Name** box, type the site name (as it appears in the RPS system).
4. Click **Apply**.

Configuring an SNMP profile

About this task

Configure an Simple Network Management Protocol (SNMP) profile to establish consistent SNMP parameters that the AS 5300 Element Manager uses to monitor the condition of the operating system and server hardware for the managed and monitored network elements.

You can configure the following SNMP profiles:

- SNMPv2c
- SNMPv3

Prerequisites

- You can access the AS 5300 Element Manager Console.
You have SnmpProfileService privileges.

The license key is updated. For more information about how to update the license key, see Enabling a license key on page 46.

For more information about SNMP configuration, see SNMP configuration on page 203.

**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > SNMP Profiles.

2. Click **Add (+)**.

OR

Select an entry and click **Edit (-/+)**.

3. In the Add Server SNMP Profiles dialog box, perform the following:

   a. In **Profile Name**, type the name of the SNMP profile.

   b. In **Profile Version**, select SNMPv2c or SNMPv3.

      When you select **Profile Version**, the system displays the parameters associated with the SNMP profile. Fill the appropriate values in the parameters.

      • For **SNMPv2**, the system displays the Read Community String and Write Community String parameters.

      • For **SNMPv3**, the system displays the User Name, Security Level, Authentication Password, Authentication password confirmation, Authentication Protocol, Privacy Password, Privacy password confirmation, Privacy Protocol, and Engine ID Suffix parameters.

   c. Click **Apply**.

---

**Configuring an SNMP profile job aid**

**About this task**

The following table describes the parameters that you use to configure an SNMP profile.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>This (text) value is a unique name to identify the profile.</td>
</tr>
<tr>
<td>Profile Version</td>
<td>This value is the SNMP version that can be chosen from the <strong>Profile Version</strong> drop-down list. The options are: SNMPv3 and SNMPv2c. The default value is SNMPv3.</td>
</tr>
<tr>
<td>Read Community String</td>
<td>This (text) value is the name of the Read Community String. The default value is <strong>public</strong>.</td>
</tr>
<tr>
<td>Write Community String</td>
<td>This (text) value is the name of the Write Community String. The default value is <strong>private</strong>.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>This (text) value is the SNMPv3 user name. The default value is mcpUser.</td>
</tr>
<tr>
<td>Security Level</td>
<td>This value is the SNMPv3 security level that can be chosen from the Security Level drop-down list. The options are: authPriv, authNoPriv, and noAuthNoPriv. The default value is authPriv.</td>
</tr>
<tr>
<td>Authentication Password</td>
<td>This (text) value is the SNMPv3 authentication password.</td>
</tr>
<tr>
<td>Authentication password confirmation</td>
<td>This (text) value is the SNMPv3 authentication password confirmation.</td>
</tr>
<tr>
<td>Authentication Protocol</td>
<td>This value is the SNMPv3 authentication protocol. The options are: SHA1 and MD5. The default value is SHA1.</td>
</tr>
<tr>
<td>Privacy Password</td>
<td>This (text) value is the SNMPv3 privacy password.</td>
</tr>
<tr>
<td>Privacy password confirmation</td>
<td>This (text) value is the SNMPv3 privacy password confirmation.</td>
</tr>
<tr>
<td>Privacy Protocol</td>
<td>This value is the SNMPv3 privacy protocol. The options are: AES_CFB_128 and DES_CBC_128. The default value is AES_CFB_128.</td>
</tr>
<tr>
<td>Engine ID Suffix</td>
<td>This (text) value is the SNMPv3 Engine ID suffix. The default value is engineID.</td>
</tr>
</tbody>
</table>

**Important:**
To increase security, Avaya recommends that you configure the values other than the default values.

---

## Configuring a site

**About this task**

Use the following procedure to add or edit a site or site information on the servers.

**Prerequisites**

- You can access the AS 5300 Element Manager Console.
- You have PhysicalSiteService privileges.

**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > Physical Sites**.
2. To add a new site, click **Add (+)**.

   OR

   To modify an existing site, select an entry, and then click **Edit (-/+)**.
3. Configure the **Site Name, Zone, Easting**, and **Northing** parameters.
4. Click **Apply**.

---

### Configuring a site job aid

#### About this task

The following table lists and describes the parameters for configuring a site.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Site Name</strong></td>
<td>This parameter is a unique name identifying the site. Range: 1–20 alphanumeric characters</td>
</tr>
<tr>
<td><strong>Zone</strong></td>
<td>This parameter is the Universal Transverse Mercator (UTM) zone location of this site. Range: 1–3 alphanumeric characters</td>
</tr>
<tr>
<td><strong>Easting</strong></td>
<td>This parameter is the Easting of the site. Range: 1–7 digits For numbers greater than 1 100, do not enter spaces.</td>
</tr>
<tr>
<td><strong>Northing</strong></td>
<td>This parameter is the northing of the site. Range: 1–7 digits For numbers greater than 1 100, do not enter spaces.</td>
</tr>
</tbody>
</table>

---

### Configuring an SMDI server

#### About this task

Configure a Simplified Message Desk Interface (SMDI) server to specify Telnet session parameters for the Voicemail service.

#### Prerequisites

- You can access the AS 5300 Element Manager Console.
- You have SMDIServerService privileges.

#### Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > SMDI Servers**.
2. To add a new SMDI server, click **Add (+)**.
   
   OR
   
   To modify an existing SMDI server, select an entry, and then click **Edit (-/+)**.
3. Configure the **ShortName**, **LongName**, **Address**, **Session Manager**, **UserName**, **Password**, **Confirm Password**, **Port**, and **SmdVersion** parameters as required.
4. Click **Apply**.
Configuring an SMDI server job aid

About this task
The following table lists and describes the SMDI server configuration parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ShortName</td>
<td>A short name to identify the SMDI server.</td>
</tr>
<tr>
<td></td>
<td>Maximum: 6 alphanumeric characters</td>
</tr>
<tr>
<td>LongName</td>
<td>A longer more descriptive name to identify the SMDI server.</td>
</tr>
<tr>
<td></td>
<td>Maximum: 32 alphanumeric characters</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address (external node) for the SMDI server.</td>
</tr>
<tr>
<td>Session Manager</td>
<td>The AS 5300 Session Manager associated with the SMDI server. Select from the list.</td>
</tr>
<tr>
<td>UserName</td>
<td>The user name to establish the SMDI connection.</td>
</tr>
<tr>
<td></td>
<td>Maximum: 64 alphanumeric characters (special characters allowed)</td>
</tr>
<tr>
<td>Password</td>
<td>The password to establish the SMDI connection.</td>
</tr>
<tr>
<td></td>
<td>Maximum: 64 alphanumeric characters (special characters allowed)</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password to establish the SMDI connection.</td>
</tr>
<tr>
<td></td>
<td>Maximum: 64 alphanumeric characters (special characters allowed)</td>
</tr>
<tr>
<td>Port</td>
<td>The port to establish the SMDI connection.</td>
</tr>
<tr>
<td></td>
<td>A numeric value from 1–65 535</td>
</tr>
<tr>
<td>SmdiVersion</td>
<td>The version of SMDI.</td>
</tr>
<tr>
<td></td>
<td>The value must be 1 or 2.</td>
</tr>
</tbody>
</table>

Configuring an external node

About this task
Configure an external node to add multiple Informational Elements with the same IP address and different ports.

Prerequisites

- You can access the AS 5300 Element Manager Console.
- You have NodeService privileges.
- The IP address of the external node exists in the address table. For more information, see Configuring the IPv4 address table on page 44.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > External Nodes.
2. Click **Add (+)**

   OR

   Select an entry and click **Edit (-/+)**.

3. In the **Add External Node** or **Edit External Node** dialog box, configure the **Name**, **IPv4 Address**, and **IPv6 Address** parameters, as required.

4. Click **Apply**.

---

### Configuring an external node job aid

**About this task**

The following table lists and describes the parameters used to configure an external node.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the device (1–16 alphanumeric characters)</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>The IPv4 address of the device (select from the list). You must configure an IPv4 address for each node.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>The IPv6 address of the device (select from the list). This field is optional.</td>
</tr>
</tbody>
</table>

---

### Configuring a trusted node

**About this task**

Perform this procedure to configure an Informational Element, or trusted node, and to prevent the Session Initiation Protocol (SIP) Denial of Service (DoS) mitigation feature from blocking messages generated by the external SIP proxies or SIP test tools.

**Prerequisites**

- You can access the AS 5300 Element Manager Console.
- You have NodeService privileges.
- You have InfoElementService privileges.

**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > Addresses > IPv4 Addresses/IPv6 Addresses**.

2. In the IPv4/IPv6 Addresses window, click **Add (+)**.

3. Type the **Logical Name** and **IP Address**, and click **Apply**.

4. Select **External Nodes**.
5. In the External Nodes window, click **Add (+)**.

6. Type the **Name** of the external node, select an **IPv4 Address** for the external node, and optionally select an **IPv6 Address** for the external node.

7. Click **Apply**.

8. Select Informational Elements.

9. In the Informational Elements window, click **Add (+)**.

10. Configure the **ShortName**, **LongName**, **Trusted**, **ExemptDosProtection**, **Port**, and **Type** parameters.

11. In the Transport Information section, configure the **Node**, **Enable SIP UDP Port**, **SIP UDP Port**, **Enable SIP TCP Port**, **SIP TCP Port**, **Enable SIP TLS Port**, and **SIP TLS Port** parameters as required.

   **Important:**
   Systems that do not use Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) use UDP and RTP. The Audiocodes Mediant 3000 does not support best effort RTP/SRTP (mixed-mode). The configuration for all endpoints must be either secure or nonsecure for media.

12. Click **Apply**.

---

### Informational elements job aid

The following are the supported informational element types:

- **Gateway**: select for the IP address of a gateway such as the Communications Server 1000.
- **General**: select for an IP address that is not a gateway or Avaya Media Server (MS).
- **Avaya MS**: select for an address of an Avaya MS.
- **LDAP**: select for an address of a Lightweight Directory Access Protocol (LDAP) server.
- **Media Portal Resource**: select for the address of a Media Portal resource.
- **Pooled Media Resource**: select for the address of a Pooled Media resource.
- **E911 Manager**: select for the IP address of the E911 Manager server.

---

### Configuring a trusted node job aid

#### About this task

The following table lists and describes the parameters for trusted node configuration.
### Configuring an external SIP proxy

**About this task**

Perform this procedure to configure an external SIP proxy.

**Prerequisites**

- You can access the AS 5300 Element Manager Console.
- You have SipProxyService privileges

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ShortName</td>
<td>The name of the device. Maximum characters: 6</td>
</tr>
<tr>
<td>LongName</td>
<td>The long name of the device (same as the description of a long name parameter for a Network Element). Maximum characters: 32</td>
</tr>
<tr>
<td>Trusted</td>
<td>Specifies whether the informational element is trusted. The informational element is trusted for SIP communications only, not for any other protocol.</td>
</tr>
<tr>
<td>ExemptDoSProtection</td>
<td>Specifies whether the informational element is exempt from Denial of Service Protection.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the port. Range: 0–65534</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the informational element type.</td>
</tr>
<tr>
<td>Node</td>
<td>External node of the informational element.</td>
</tr>
<tr>
<td>Enable SIP UDP Port</td>
<td>Enables the SIP UDP port. Selected = enabled Not selected = disabled</td>
</tr>
<tr>
<td>SIP UDP Port</td>
<td>Specifies the UDP port for SIP. Example: 5060</td>
</tr>
<tr>
<td>Enable SIP TCP Port</td>
<td>Enables the SIP TCP port. Selected = enabled Not selected = disabled Example: 5060</td>
</tr>
<tr>
<td>SIP TCP Port</td>
<td>Specifies the TCP port for SIP. Example: 5060</td>
</tr>
<tr>
<td>Enable SIP TLS Port</td>
<td>Enables the SIP TLS port. Selected = enabled Not selected = disabled</td>
</tr>
<tr>
<td>SIP TLS Port</td>
<td>Specifies the TLS port for SIP. Example: 5061</td>
</tr>
</tbody>
</table>
Configuring an external SIP proxy job aid

About this task
The following table lists and describes the parameters for external SIP proxy configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Name</td>
<td>The short name of the external SIP proxy. Maximum of 6 characters.</td>
</tr>
<tr>
<td>Long Name</td>
<td>The long name of the external SIP proxy. Maximum of 32 characters.</td>
</tr>
<tr>
<td>Trusted</td>
<td>Specifies whether the element is trusted.</td>
</tr>
<tr>
<td></td>
<td>This check box is selected by default.</td>
</tr>
<tr>
<td></td>
<td>Selected = the element is trusted. Not selected = the element is not trusted.</td>
</tr>
<tr>
<td>ExemptDoS-Protection</td>
<td>Specifies whether the element is exempt from Denial of Service protection.</td>
</tr>
<tr>
<td></td>
<td>Selected = the element is protected. Not selected = the element is not protected.</td>
</tr>
<tr>
<td>Port</td>
<td>The SIP Port used by the external proxy. Range: 0–65 535</td>
</tr>
<tr>
<td>Node</td>
<td>The external node on which the element resides. (Select from the list.)</td>
</tr>
<tr>
<td>Enable SIP UDP Port</td>
<td>Enables the SIP UDP port.</td>
</tr>
<tr>
<td></td>
<td>This check box is selected by default.</td>
</tr>
<tr>
<td></td>
<td>Selected = enabled Not selected = disabled</td>
</tr>
<tr>
<td>SIP UDP Port</td>
<td>Specifies the UDP port for SIP.</td>
</tr>
</tbody>
</table>

Table continues…

Important:
Systems that do not use TCP/TLS and SRTP use UDP, TCP, and RTP.

5. Click Apply.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SIP TCP Port</td>
<td>Enables the SIP TCP port. Selected = enabled. Not selected = disabled. Example: 5060</td>
</tr>
<tr>
<td>SIP TCP Port</td>
<td>Specifies the TCP port for SIP. Example: 5060</td>
</tr>
<tr>
<td>Enable SIP TLS Port</td>
<td>Enables the SIP UDP port. Selected = enabled. Not selected = disabled.</td>
</tr>
<tr>
<td>SIP TLS Port</td>
<td>Specifies the TLS port for SIP. Example: 5061</td>
</tr>
</tbody>
</table>

Adding a SIP template

About this task
Use this procedure to add a SIP template.

Prerequisites

• You can access the AS 5300 Element Manager Console.
• You have Admin level access.
• You have SIPTemplateService privileges.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > SIP Templates > SIP Templates.
2. In the SIP Templates window, click Add (+).
3. In the Add SIP Template window, enter the Template Name and Template Description.
4. Adjust the template Signaling and Media attributes as required.
5. Click Apply.

Adding a SIP template job aid

About this task
The following table lists and describes the parameters for SIP template addition.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Subparameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
<td></td>
<td></td>
<td>The name of the template. The name must be unique. This field is required.</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
<td>The description of the template.</td>
</tr>
</tbody>
</table>
| Signaling               | Configure Request Allowed  | Check box | The type of requests the system permits to be sent to the device.  
1. Select the check box to enable this option.  
2. Click the **Configure Request Allowed** link to open the SIP Request Selection window.  
3. Select one or more requests from the Available Request list, and click **<<** to copy it to the Selected Request list.  
4. Click **Apply**. |
| Redirect Response       |                            | Check box | If not selected, calls from this device cannot receive a 302 response back.                                                                  |
| Header Selection        |                            | Check box | The headers supported by the client.  
1. Click the **Header Selection** link to open the Header Selection window.  
2. In the **Header Processing** list, make a selection.  
3. Select one or more headers from the Available Header list, and click **<<** to copy it to the Selected Header list.  
4. Click **Apply**. |
<p>| Tags Allowed            |                            | Check box | If selected, the system removes the From: tag from outgoing messages.  |
| Allow User Info Parameter |                            | Check box | If selected, the system allows User-Info parameters in the Request URIs destined to this device.  |
| Request Nortel Profile Header |                        | Check box | If selected, the system adds the x-nt-profile header into the outgoing message.  |
| Add Calling Party Display |                            | Check box | If selected, the system adds Calling Party Display to all Caller Identification fields when the Application Server 5300 owns the originating subscriber. |
| VIA IP                  |                            | Check box | If selected, the system adds the VIA header.                                                                                                 |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Subparameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Headers</td>
<td></td>
<td>Default: 200</td>
<td>The maximum number of headers to and from this device in a single SIP message.</td>
</tr>
<tr>
<td>Max Header Length</td>
<td></td>
<td>Default: 1024</td>
<td>The maximum length of a single header to or from this device.</td>
</tr>
<tr>
<td>Max Block Size</td>
<td></td>
<td>Default: 4096</td>
<td>Obsolete.</td>
</tr>
<tr>
<td>Hookflash URI</td>
<td>username</td>
<td>Check box</td>
<td>The value sent in the user part of the RequestURI to indicate that the hookflash has been received.</td>
</tr>
<tr>
<td>Digit Timeout URI</td>
<td>username</td>
<td>Check box</td>
<td>The time-out value used when collecting digit streams.</td>
</tr>
<tr>
<td>E911 Mid call reject</td>
<td></td>
<td>Check box</td>
<td>If selected, the Application Server 5300 does not permit calls terminating to an emergency server to be placed on hold.</td>
</tr>
<tr>
<td>User User Mode1</td>
<td></td>
<td>Check box</td>
<td>If selected, the system permits ISDN User-to-User information to be tunneled in a SIP header.</td>
</tr>
<tr>
<td>Require Priority</td>
<td>RingBack</td>
<td>Check box</td>
<td>If selected, and the Multi-Level Priority and Preemption feature is enabled, the Avaya Media Server (MS) is inserted into the voicepath to supply the priority ringback tones.</td>
</tr>
<tr>
<td>Play Announcements</td>
<td></td>
<td>Check box</td>
<td>If selected, the Application Server 5300 connects to the Avaya MS to play announcements for originating devices that cannot play announcements locally.</td>
</tr>
<tr>
<td>Unique Call IDs</td>
<td></td>
<td>Check box</td>
<td>If selected, each leg of a forked call has a unique call id assigned to it.</td>
</tr>
<tr>
<td>Ephemeral Source</td>
<td>port</td>
<td>Check box</td>
<td>If selected, the client uses ephemeral ports and the Application Server 5300 uses this value to route responses.</td>
</tr>
<tr>
<td>Allow P-Asserted</td>
<td>Identity Header</td>
<td>Check box</td>
<td>If selected for a non-trusted node (for example, a client), the system sends the P-Asserted Identity to the client.</td>
</tr>
<tr>
<td>PAI is applied as follows: The data for PAI is taken from: • PAI is added for new calls to other servers or systems. • For redirected calls, if PAI is present in the incoming call, it is updated from the ChargeID of the caller. • For interworking calls, PAI is added if available. PAI is added from Public...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Subparameter</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Charge ID, if available, otherwise from Remote-Party-ID (RPI), if available. For calls that come from an untrusted gateway, PAI is replaced by the string sip:<a href="mailto:anonymous@anonymous.invalid">anonymous@anonymous.invalid</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use Calling Party as From</td>
<td>Check box</td>
<td>If selected, the From: header is updated to match the value in the P-Asserted Identity.</td>
<td></td>
</tr>
<tr>
<td>Use Options</td>
<td>Check box</td>
<td>If selected, the Application Server 5300 uses the SIP OPTIONS method for long-call audits.</td>
<td></td>
</tr>
<tr>
<td>Consult Xfer SVC needed</td>
<td>Check box</td>
<td>If selected, the Consult transfer service is enabled for SSL subscribers only. If not selected, the system uses the standard method for consult transfers.</td>
<td></td>
</tr>
<tr>
<td>Presence Insertion</td>
<td>Check box</td>
<td>Obsolete.</td>
<td></td>
</tr>
<tr>
<td>Force Homed User</td>
<td>Check box</td>
<td>If selected, the client must register with the Application Server 5300 on which the subscriber is hosted, or a 404 Not Found is sent back.</td>
<td></td>
</tr>
<tr>
<td>Require Conference Parameter Swap</td>
<td>Check box</td>
<td>Select for clients that are not compliant to the SIP Refer specifications and therefore cannot copy the contents of the Refer-To: header to the resulting requestURI.</td>
<td></td>
</tr>
<tr>
<td>Require Refer To Privacy Swap</td>
<td>Check box</td>
<td>If selected, the Application Server 5300 reapplies any privacy settings on the Refer-To header when processing a Refer locally.</td>
<td></td>
</tr>
<tr>
<td>Delay Xfer202</td>
<td>Check box</td>
<td>If selected, the Application Server 5300 does not send out the 202 Accepted until after a response is received from the INVITE to the new party.</td>
<td></td>
</tr>
</tbody>
</table>
| Configure Alert Information set | Check box | The parameter values in the Alert-Info header.  
1. Select the check box to enable this option.  
2. Click the **Configure Alert Information set** link to open the Set AlertInfoParam window.  
3. Select one or more parameter from the Available AlertInfoParam list, and |

Table continues…
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Subparameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Subscribe Parameter</td>
<td>Check box</td>
<td>The valid parameters to include in a</td>
<td>The valid parameters to include in a SUBSCRIBE. Currently, only MWI is available for selection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SUBSCRIBE. Currently, only MWI is</td>
<td>1. Select the check box to enable this option.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>available for selection.</td>
<td>2. Click the <strong>Configure Subscribe Parameter</strong> link to open the SIP SubscribeParam Selection window.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. Select one or more parameter from the Available SubscribeParam list, and click &lt;&lt; to copy it to the Selected SubscribeParam list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4. Click <strong>Apply</strong>.</td>
</tr>
<tr>
<td>Require Alert Info Header</td>
<td>Check box</td>
<td>If selected, calls terminating to this</td>
<td>If selected, calls terminating to this device require the Alert-Info header.</td>
</tr>
<tr>
<td>Refer Response</td>
<td>Check box</td>
<td>If selected, the Application Server 5300</td>
<td>If selected, the Application Server 5300 hosts the Refer. This is the same as Handle Refer on AS, but it is specific to Communication Server 2000 Attached (SSL) subscribers.</td>
</tr>
<tr>
<td>Suppress Long call</td>
<td>Check box</td>
<td>If selected, long call audit, for calls</td>
<td>If selected, long call audit, for calls involving this device, is disabled.</td>
</tr>
<tr>
<td>Static Client Type</td>
<td>Check box</td>
<td>If selected, and the device is in use with</td>
<td>If selected, and the device is in use with the CS 2000 Attached (SSL) deployment, the device can monitored.</td>
</tr>
<tr>
<td>Refer To Substitution</td>
<td>Check box</td>
<td>When interworking with an enterprise</td>
<td>When interworking with an enterprise gateway, this setting will cause the replacement of the value in the Refer-To header with the private charge ID of the subscriber, plus add a &quot;phone-context=udp&quot; tag and a &quot;user=phone&quot; tag.</td>
</tr>
<tr>
<td>IN Session Authentication</td>
<td>Check box</td>
<td>If selected, the device must support in</td>
<td>If selected, the device must support in session challenges for any SIP message sent.</td>
</tr>
<tr>
<td>Use From Header For Subr Lookup</td>
<td>Check box</td>
<td>If selected, for SIP transactions that</td>
<td>If selected, for SIP transactions that originate from this client type, the From: header is used to locate a subscriber.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Subparameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Diversion Header</td>
<td>Check box</td>
<td></td>
<td>If selected, the system includes the Diversion header when a call terminates to a trusted node.</td>
</tr>
<tr>
<td>Use Request URI As TO</td>
<td>Check box</td>
<td></td>
<td>If selected, the system uses the URI contained in the RequestURI to encode the To: header.</td>
</tr>
<tr>
<td>Remove Unknown Paid</td>
<td>Check box</td>
<td></td>
<td>If selected, for calls from an unknown Calling Party, no P-Asserted Identity header is built.</td>
</tr>
<tr>
<td>Handle Refer On As</td>
<td>Check box</td>
<td></td>
<td>If selected, any REFER scenario involving this device is hosted on the Application Server 5300, and third party call control (INVITEs) is used to complete the REFER.</td>
</tr>
<tr>
<td>Use IP as FROM Domain</td>
<td>Check box</td>
<td></td>
<td>If selected, the system sends the IP address of the AS 5300 Session Manager that hosts the call, instead of the domain in the From field.</td>
</tr>
<tr>
<td>Remove Replaces Support</td>
<td>Check box</td>
<td></td>
<td>If selected, the system removes the Replaces header from the supported header for SIP messages to and from this device.</td>
</tr>
<tr>
<td>Remove NT-EndPoint from Request URI</td>
<td>Check box</td>
<td></td>
<td>If selected, the system removes the nt-endpt parameter from the Request URI.</td>
</tr>
<tr>
<td>Remove NT-EndPoint from Contact</td>
<td>Check box</td>
<td></td>
<td>If selected, the system removes the nt-endpt parameter from the content header.</td>
</tr>
<tr>
<td>Alteon 302 Redirection</td>
<td>Check box</td>
<td></td>
<td>If selected, the AS 5300 Session Manager sends a 302 Moved Temporarily when it would normally send a 301 Moved Permanently.</td>
</tr>
<tr>
<td>Allow DualCLI when Privacy header is Set</td>
<td>Check box</td>
<td></td>
<td>If selected, the DualCLI feature functions even if privacy is enabled on the call. Only enable for communication with a trusted node.</td>
</tr>
<tr>
<td>Require PRACK</td>
<td>Check box</td>
<td></td>
<td>If selected, the PRACK is required for all calls to this device. If PRACK is not supported, remove PRACK from the list of allowed headers.</td>
</tr>
<tr>
<td>Use UA-Profile Event Package for MWI</td>
<td>Check box</td>
<td></td>
<td>The Message Waiting notification method to send to the endpoint.</td>
</tr>
<tr>
<td>Override Host in From URI after Translation</td>
<td>Check box</td>
<td></td>
<td>If selected, the system changes the domain of the calling party fields to match that of the destination domain. This</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Subparameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>configuration forces the call back through the originators domain.</td>
</tr>
<tr>
<td>Set username for CLI unavailable</td>
<td>Check box</td>
<td>The value to use as the Display Name for calls with unknown display names.</td>
<td></td>
</tr>
<tr>
<td>Set username for CLI private</td>
<td>Check box</td>
<td>The value to use as the Display Name for calls with privacy enabled.</td>
<td></td>
</tr>
<tr>
<td>AS Provides Subsequent Ringback</td>
<td>Check box</td>
<td>If selected, the Application Server 5300 provides ringback for multiple early media sessions.</td>
<td></td>
</tr>
<tr>
<td>Do not Consider Device as Network Server</td>
<td>Check box</td>
<td>Disabled by default.</td>
<td></td>
</tr>
<tr>
<td>Disallow Sending 301</td>
<td>Check box</td>
<td>Disabled by default.</td>
<td></td>
</tr>
<tr>
<td>Microsoft Office Client Compatible (Microsoft Office Client is not supported)</td>
<td>Check box</td>
<td>Disabled by default.</td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td>Strip Audio Codecs</td>
<td>Check box and clickable link</td>
<td>List of audio codecs that are denied for the endpoint:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1. Select the check box to enable this option.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Click Strip Audio Codecs to open the SIP AudioCodec Selection window.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. Select one or more codecs from the Available Audio Codec list, and click &gt;&gt; to copy the codecs to the Selected Audio Codecs list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4. Click <strong>Apply</strong>.</td>
</tr>
<tr>
<td></td>
<td>Strip Video Codecs</td>
<td>Check box and clickable link</td>
<td>List of video codecs that are denied for the endpoint:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1. Select the check box to enable this option.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. Click Strip Video Codecs to open the SIP VideoCodec Selection window.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. Select one or more codecs from the Available Video Codec list, and click &gt;&gt; to copy it to the Selected Video Codecs list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4. Click <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Subparameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| Configure AudioPTime     | Check box        | Check box and clickable link   | 1. Select the check box to enable this option.  
2. Click the **Configure SIP AudioPTime** link to open the SIP AudioPTime Selection window.  
3. Select one or more values from the Available AudioPTime list, and click `<<` to copy it to the Selected AudioPTime list.  
4. Click **Apply**.                                                                 |
| Configure InsertPTime    | Check box        | Check box and clickable link   | 1. Select the check box to enable this option.  
2. Click the **Configure SIP InsertPTime** link to open the SIP InsertPTime Selection window.  
3. Select one or more values from the Available InsertPTime list, and click `<<` to copy it to the Selected InsertPTime list.  
4. Click **Apply**.                                                                 |
| Information Digit Negotiation | Check box | Check box                        | If enabled, the Application Server 5300 enables negotiation of the use of SIP INFO to send DTMF for the device.                                                                 |
| Codec Change             | Check box        |                                 | If disabled, the system disallows any changes to the originally negotiated codec.                                                                                                                            |
| Pivot Allowed            | Check box        |                                 | Not supported.                                                                                                                                  |
| Early Media              | Check box        |                                 | Specifies whether or not the client can support early media. This method is obsolete.                                                                                                                      |
| Multiple Provision       | Check box        |                                 | Specifies whether or not the device can support multiple provisional responses.                                                                                                                           |
| All Content              | Check box        |                                 | If not selected, the system sends only Audio and Video SDP connection information to this device.                                                                                                           |

*Table continues...*
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Subparameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfoDigit</td>
<td>Check box</td>
<td></td>
<td>Specifies whether support for the ability to send DTMF using the SIP INFO method is available.</td>
</tr>
<tr>
<td>Insert38Desc</td>
<td>Check box</td>
<td></td>
<td>Obsolete.</td>
</tr>
<tr>
<td>Hold Needed</td>
<td>Check box</td>
<td></td>
<td>If selected, the system sends a Hold (UPDATE or Re-INVITE) to this device prior to any renegotiation of the connection.</td>
</tr>
<tr>
<td>Use Network PTime</td>
<td>Check box</td>
<td></td>
<td>If selected and a configured Network Packet Time exists, all responses use the Network defined Ptime.</td>
</tr>
<tr>
<td>Remove SDP From PRACK</td>
<td>Check box</td>
<td></td>
<td>Select for devices that cannot accept SDP in a PRACK. If selected, the Application Server 5300 negotiates the connection information contained in the PRACK.</td>
</tr>
<tr>
<td>Allow Nortel Enterprise Content</td>
<td>Check box</td>
<td></td>
<td>Select for devices which do not support the negotiation of tunneled data from the Avaya Communication Server 1000 or Avaya Business Communication Manager.</td>
</tr>
<tr>
<td>Remove SRTP</td>
<td>Check box</td>
<td></td>
<td>Select to remove the Secure RTP Offer at the Application Server 5300 and to alter the SDP response to indicate SRTP is not supported.</td>
</tr>
<tr>
<td>SDP Anat Support</td>
<td>Check box</td>
<td></td>
<td>Disabled by default.</td>
</tr>
<tr>
<td>Remove Tcp</td>
<td>Check box</td>
<td></td>
<td>Select to remove the TCAP-related attribute from SDP for Clients that do not support TCAP. Disabled by default.</td>
</tr>
<tr>
<td>Remove Video</td>
<td>Check box</td>
<td></td>
<td>Select to remove all video capabilities from SDP for Client that do not support video. Disabled by default.</td>
</tr>
<tr>
<td>Set Early Media</td>
<td>Check box</td>
<td></td>
<td>Disabled by default.</td>
</tr>
</tbody>
</table>
Specifying a codec on the system

About this task
Use this procedure to specify the audio and video codecs that can be used for stripping from SDP in SIP Profile or use as preferred on a client (video codecs).

Before you begin
Ensure the following:

- You can access the AS 5300 Element Manager Console.
- You have administrator-level access.
- You have CodecService privileges.

Procedure
1. From the configuration view of the AS 5300 Element Manager console, select Network Data and Mtc > SIP Profiles > Audio (Video) Codecs.
2. Press + button.
3. Type the codec name that you want to add to the system.
4. Click Apply.

Importing a new SIP Profile

About this task
Use this procedure to import a new SIP profile.

Prerequisites

- You can access the AS 5300 Element Manager Console.
- You have Admin level access.
- You have SIPProfileService privileges.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > SIP Profiles > Import SIP Profiles.
2. In the Import file (required) field, click Choose.
3. Browse to the folder where the profile is located on your desktop, and click Open.
4. In the Result file (required) field, click Choose.
5. Browse to the folder where the profile is located on your desktop, and click Open.
6. In the Import Format field, select one of the options: Import All, or Import Selected.
Importing a new SIP profile job aid

The following table lists and describes the parameters for the Import Format parameter.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import All</td>
<td>Import all available SIP profiles and templates.</td>
</tr>
<tr>
<td>Import Selected</td>
<td>Import only the selected SIP profiles and templates.</td>
</tr>
<tr>
<td>Overwrite existing data</td>
<td>Overwrite the existing data</td>
</tr>
</tbody>
</table>

Adding a new SIP profile

About this task

Use this procedure to add a new SIP profile.

When an endpoint connects to the system that does not match any existing profile, and the device has a user-agent field, the system uses the Default Endpoint Protocol Profile in all messaging to and from the device. An Alarm is raised to signal that a profile for the device needs to be created. When an endpoint sends a message to the system and the system is unable to match the endpoint to a profile, and if the endpoint also has no user-agent header, the following actions are taken:

- The Unidentified Endpoint profile is used in all messaging to and from the device.
- A LOG is issued indicating that an unknown device has connected the IP address of that endpoint and the username, if known.

The system allows only a single log to be issued per user. Also, the system must ensure that an accidental deletion of a SIP Endpoint Protocol Profile does not result in an overflow of logs. Log throttling limits log generation in a one-minute period to 10 logs for any given root-level domain.

While configuring the profile, the following requirements must be met:

- The profile may either be a new profile or an existing profile copied and provided with a new name.
- Profiles must have unique names.
- The Matching Criteria provide the ability to differentiate endpoints by the User-Agent header. At least one of the Matching Criteria fields must be configured in order for a SIP Endpoint Protocol Profile to be created. Attempts to create profiles with empty matching criteria are rejected. Also, attempts to change an existing profile and remove all identification data are denied. A profile can be associated with any number of matching criteria.
- Protocol templates are selected from an existing list. When a protocol is selected, corresponding signaling and media values for the template are populated in the window. If Custom is selected from the list, custom values for signaling and media must be entered.
Prerequisites

• You must import a new SIP Profile before you can add it.
• You can access the AS 5300 Element Manager Console.
• You have Admin level access.
• You have SIPProfileService privileges.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > SIP Profiles > SIP Profiles.
2. In the SIP Profiles window, click Add (+).
3. On the Add Template Selection dialog box, from the list of templates, select the appropriate template.
4. Click Next.
5. Enter the Profile Name and Description.
6. Adjust the profile Signaling and Media attributes as required.
7. Click Apply.

Adding a new SIP profile job aid

About this task

The following table lists and describes the parameters for adding a new SIP profile.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>A unique name to identify the profile</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the profile you are adding</td>
</tr>
</tbody>
</table>

Configuring a new SIP profile from a copy

About this task

Use this procedure to configure a new SIP profile from a copy.

Prerequisites

• You can access the AS 5300 Element Manager Console.
• You have Admin level access.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > SIP Profiles > SIP Profiles.
2. From the list of SIP Profiles, select a profile to copy.
3. Click Edit (+/-).
4. In the Edit SIP Profile Default dialog box, click Copy.
5. Enter the Profile Name and Description.
6. Adjust the profile Signaling and Media attributes as required.
7. Click Apply.

---

### Adding a new SIP profile from a copy job aid

**About this task**
The following table lists and describes the parameters for adding a new SIP profile from a copy.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>A unique name to identify the profile</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the profile you are adding</td>
</tr>
</tbody>
</table>

---

### Enabling SDP ANAT Support for a SIP profile

**About this task**
Enable SDP ANAT Support to facilitate Session Description Protocol (SDP) Alternative Network Address Types (ANAT) communication between SDP ANAT capable endpoints and SDP ANAT incapable endpoints.

Enabling this option is the SIP Profiles of local clients, and in profiles for remote clients, allows simultaneous use of IPv4 and IPv6 addresses for calls. If this option is disabled, the server removes all IPv6 media related lines from SIP messages.

**Procedure**
1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > SIP Profiles > SIP Profiles.
2. From the list of SIP Profiles, select the profile for which you want to enable SDP ANAT Support.
3. Click Edit (+/-).
4. In the Edit SIP Profile Default dialog box, select the SDP ANAT Support check box.
5. Click Apply.

Configuring OAMP channel cipher suites

About this task
Configure Operations, Administration, Maintenance, and Provisioning (OAMP) cipher suites to specify the encryption type for OAMP communications.

For information about how to configure OAMP ciphers for FIPS-compliant system, see Avaya Aura® Application Server 5300 Security, NN42040-601.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have CipherSuiteService privileges.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > Cipher Suites > OAMP Channel Cipher Suites
2. In the OAMP Channel Cipher Suites window, select a cipher suite entry to configure.
3. Click Enable to enable the cipher suite, or Disable to disable the cipher suite.
4. Click Apply.

Configuring external OAMP cipher suites

About this task
Configure external Operations, Administration, Maintenance, and Provisioning (OAMP) cipher suites to specify the encryption for external OAMP communications.

For information about how to configure external OAMP ciphers for FIPS-compliant system, see Avaya Aura® Application Server 5300 Security, NN42040-601.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have CipherSuiteService privileges.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > Cipher Suites > External OAMP Cipher Suites
2. In the External OAMP Cipher Suites window, select a cipher suite entry to configure.
3. Click Enable to enable the cipher suite, or Disable to disable the cipher suite.
4. Click Apply.
Configuring HTTPS cipher suites

About this task
Configure Secure Hypertext Transfer Protocol (HTTPS) cipher suites to specify the encryption for HTTPS communications.

For information about how to configure HTTPS ciphers for FIPS-compliant system, see Avaya Aura® Application Server 5300 Security, NN42040-601.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have CipherSuiteService privileges.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > Cipher Suites > HTTPS Cipher Suites
2. In the HTTPS Cipher Suites window, select a cipher suite entry to configure.
3. Click Enable to enable the cipher suite, or Disable to disable the cipher suite.
4. Click Apply.

Configuring signaling cipher suites

About this task
Configure signaling cipher suites to specify the encryption for signaling communications.

For information about how to configure signaling ciphers for FIPS-compliant system, see Avaya Aura® Application Server 5300 Security, NN42040-601.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have CipherSuiteService privileges.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc, Cipher Suites, Signaling Cipher Suites
2. In the Signaling Cipher Suites window, select a cipher suite entry to configure.
3. Click Enable to enable the cipher suite, or Disable to disable the cipher suite.
4. Click Apply.
Configuring the DSCP marking value for SIP signaling

About this task
Perform this procedure to configure Differentiated Services Code Point (DSCP) marking value for SIP signaling.

Prerequisites
- You have QoS enabled in the service package configuration.
- You can access the AS 5300 Element Manager Console.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > DSCP Marking > Call Signaling DSCP Parameters.
2. Select callsignaling and click Edit (+/-).
3. In the SIP Signaling DSCP field, type the desired DSCP marking value.
4. Click Apply.
5. Click OK.

⚠️ Important:
The system raises an alarm; you must restart the network elements after you make DSCP configuration changes.

Avaya Aura® Application Server 5300 Web Client users logged on at the time of the changes, must log off, and then log back on to update the client configuration.

Configuring the DSCP marking value for SIP signaling job aid

About this task
This job aid lists and describes the Call Signaling DSCP parameter.

<table>
<thead>
<tr>
<th>Configurable Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP signaling</td>
<td>This parameter is used in outgoing IP packets. Range: 0-63 Default: 0</td>
</tr>
</tbody>
</table>
Configuring the DSCP marking value for Operations, Administration, Maintenance and Provisioning

About this task
Perform this procedure to configure new DSCP marking values for Operations, Administration, Maintenance and Provisioning (OAMP). The High Throughput Data and Low Latency Data DSCP values that you configure during this procedure, replace any DSCP marking values configured offline, during log on to the AS 5300 Element Manager Console.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have administrator access privileges

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > DSCP Marking > OAMP DSCP Parameters.
2. Select oamp and click Edit (-/+).
3. Enter the desired DSCP marking value in the High Throughput Data DSCP, Low Latency Data DSCP, and Network Signaling DSCP fields.
4. Click Apply.
5. Click OK.

Important:
The system raises an alarm; you must restart the network elements after you make DSCP configuration changes.

Configuring the DSCP marking value for OAMP job aid

About this task
This job aid lists and describes the OAMP for DSCP parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Throughput Data</td>
<td>This parameter controls outgoing network packets Range: 0-63 Default: 0</td>
</tr>
<tr>
<td>Low Latency Data</td>
<td>This parameter controls outgoing network packets Range: 0-63 Default: 0</td>
</tr>
<tr>
<td>Network Signaling</td>
<td>This parameter controls network signaling. Range: 0-63 Default: 0</td>
</tr>
</tbody>
</table>
Configuring the DSCP marking value for XMPP

Before you begin
Access the AS 5300 Element Manager Console. If MCP FIPS is:

- Enabled: Run `fips-mgmtconsole.bat`.
- Not enabled: Go to `https://AS5300 Element Manager Console IP:12121`.

Procedure
1. Log in with EM Admin credentials.
2. Click the expand button (+) next to Network Data and Mtc.
3. Click the expand button (+) next to DSCP Marking.
4. Click XMPP DSCP Parameters.
5. Select the `xmpp` row and click the expand or collapse button (+)/(-).
6. Set XMPP DSCP to XMPP DSCP value.
7. Click Apply.

The system generates the XMPP DSCP Configuration Change warning alarm. You can manually acknowledge or clear the alarm.

Configuration of the XMPP DSCP

This job aid lists the parameter group and describes the configuration parameter for AS 5300 Element Manager Console.

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMPP DSCP</td>
<td>DSCP values for XMPP network packets.</td>
</tr>
<tr>
<td></td>
<td>Range: 0 – 63</td>
</tr>
<tr>
<td></td>
<td>Default: 18</td>
</tr>
</tbody>
</table>

Configuring an EBC

About this task
Use the AS 5300 Element Manager Console to add each Edge Border Controller (EBC) to the AS 5300 Element Manager. Use this procedure if your system requires EBCs.

Prerequisites
- You can access the AS 5300 Element Manager Console.
• The IP address table contains the IP address for each EBC.
• Each EBC is already configured as an external node.
• You have ArtsElementService privileges

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > ARTS Integration > Edge Border Controllers.
2. On the Edge Border Controllers window, click Add (+).
3. On the Add Edge Border Controller window, configure the Short Name, Long Name, Trusted, ExemptDoSProtection, and Port parameters.
4. In the Transport Information section, configure the Node, Enable SIP UDP Port, SIP UDP Port, Enable SIP TCP, SIP TCP Port, Enable SIP TLS, and SIP TLS Port parameters as required by the system.
5. Click Apply.

Configuring an EBC job aid

About this task

The following table lists and describes the parameters used to configure an EBC.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Name</td>
<td>The short name of the element—maximum of 6 characters.</td>
</tr>
<tr>
<td>Long Name</td>
<td>The long name of the element—maximum of 32 characters.</td>
</tr>
<tr>
<td>Trusted</td>
<td>Specifies whether the element is trusted.</td>
</tr>
<tr>
<td>ExemptDoSProtection</td>
<td>Specifies whether the informational element is exempt from Denial of Service Protection.</td>
</tr>
<tr>
<td>Port</td>
<td>The element uses this port value on the external node. Range: 0-65535</td>
</tr>
<tr>
<td>Node</td>
<td>The external node on which the element resides. Select from the list.</td>
</tr>
<tr>
<td>Enable SIP UDP</td>
<td>(Check box) Select to enable the SIP UDP port.</td>
</tr>
<tr>
<td>SIP UDP Port</td>
<td>Specifies the UDP port for SIP. Example: 5060</td>
</tr>
<tr>
<td>Enable SIP TCP</td>
<td>(Check box) Select to enable the SIP TCP port.</td>
</tr>
<tr>
<td>SIP TCP Port</td>
<td>Specifies the TCP port for SIP. Example: 5060</td>
</tr>
<tr>
<td>Enable SIP TLS</td>
<td>(Check box) Select to enable the SIP TLS port.</td>
</tr>
<tr>
<td>SIP TLS Port</td>
<td>Specifies the TLS port for SIP. Example: 5061</td>
</tr>
</tbody>
</table>
Configuring an SS Session Manager

About this task
Use the AS 5300 Element Manager Console to add each softswitch (SS) Session Manager to the AS 5300 Element Manager.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- The IP address table contains the IP address for each SS Session Manager.
- Each SS Session Manager is already configured as an external node.
- You have ArtsElementService privileges

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, expand Network Data and Mtc > ARTS Integration > Multifunction Soft Switches.
2. On the Multifunction Soft Switches window, click Add (+).
3. On the Add Multifunction Soft Switch window, configure the Short Name, Long Name, Trusted, ExemptDoSProtection, and Port parameters.
4. In the Transport Information section, configure the Node, Enable SIP UDP Port, SIP UDP Port, Enable SIP TCP, SIP TCP Port, Enable SIP TLS, and SIP TLS Port parameters as required by the system.
5. Configure the Local Edge Border Controller, Remote Edge Border Controller Name, and Call Control Agent ID parameters.
6. Select the Paired MFSS check box if you want to configure the MFSS as a pair for the local SS for failover purposes.

    Note:
    This check box is enabled only if there is zero or one local SS profile on your system. This check box is disabled if a second SS profile is added to the system.

    You can have only one MFSS paired with the local SS. If you try to select a second MFSS as paired, the system displays a message indicating that an MFSS pair already exists in the system and asks for an override confirmation to replace the existing paired MFSS.

7. Click Apply.

Configuring an SS Session Manager job aid

About this task
The following table lists and describes the parameters used to configure an SS Session Manager.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Name</td>
<td>The short name of the element—maximum of six characters.</td>
</tr>
<tr>
<td>Long Name</td>
<td>The long name of the element—maximum of 32 characters.</td>
</tr>
<tr>
<td>Trusted</td>
<td>Specifies whether the element is trusted.</td>
</tr>
<tr>
<td>ExemptDoSProtection</td>
<td>Specifies whether the informational element is exempt from Denial of Service Protection.</td>
</tr>
<tr>
<td>Port</td>
<td>The element uses this port value on the external node. Range: 0-65535</td>
</tr>
<tr>
<td>Node</td>
<td>The external node on which the element resides. Select from the list.</td>
</tr>
<tr>
<td>Enable SIP UDP</td>
<td>(Check box) Select to enable the SIP UDP port.</td>
</tr>
<tr>
<td>SIP UDP Port</td>
<td>Specifies the UDP port for SIP. Example: 5060</td>
</tr>
<tr>
<td>Enable SIP TCP</td>
<td>(Check box) Select to enable the SIP TCP port.</td>
</tr>
<tr>
<td>SIP TCP Port</td>
<td>Specifies the TCP port for SIP. Example: 5060</td>
</tr>
<tr>
<td>Enable SIP TLS</td>
<td>(Check box) Select to enable the SIP TLS port.</td>
</tr>
<tr>
<td>SIP TLS Port</td>
<td>Specifies the TLS port for SIP. Example: 5061</td>
</tr>
<tr>
<td>Local Edge Border Controller</td>
<td>Local Edge Border Controller of the local switch.</td>
</tr>
<tr>
<td>Remote Edge Border Controller Name</td>
<td>Name of Remote Edge Border Controller fronting the MFSS.</td>
</tr>
<tr>
<td>Call Control Agent ID</td>
<td>Call Control Agent ID for ASAC purpose.</td>
</tr>
<tr>
<td>Paired MFSS</td>
<td>(Check box) Select to configure the MFSS as a pair for the local SS for failover purposes. This check box is enabled only if there is zero or one local SS profile on your system and is disabled if a second SS profile is added to the system. You can have only one MFSS paired with the local SS. If you try to select a second MFSS as paired, the system displays a message indicating that an MFSS pair already exists in the system and asks for an override confirmation to replace the existing paired MFSS.</td>
</tr>
</tbody>
</table>

**Configuring an LSC Session Manager**

**About this task**

Use the AS 5300 Element Manager Console to add each Local Session Controller (LSC) Session Manager to the AS 5300 Element Manager.

**Prerequisites**

- You can access the AS 5300 Element Manager Console.
- The IP address table contains the IP address for each LSC Session Manager.
- Each LSC Session Manager is already configured as an external node.
• You have ArtsElementService privileges

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, expand Network Data and Mtc > ARTS Integration > Local Session Controllers.
2. On the Local Session Controllers window, click Add (+).
3. On the Add Local Session Controller window, configure the Short Name, Long Name, Trusted, and Port parameters.
4. In the Transport Information section, configure the Node, Enable SIP UDP Port, SIP UDP Port, Enable SIP TCP, SIP TCP Port, Enable SIP TLS, and SIP TLS Port parameters as required by the system.
5. Configure the Local Edge Border Controller, Remote Edge Border Controller Name, and Call Control Agent ID parameters.
6. Click Apply.

---

**Configuring an LSC Session Manager job aid**

**About this task**

The following table lists and describes the parameters used to configure an LSC Session Manager.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Name</td>
<td>The short name of the element—maximum of six characters.</td>
</tr>
<tr>
<td>Long Name</td>
<td>The long name of the element—maximum of 32 characters.</td>
</tr>
<tr>
<td>Trusted</td>
<td>Specifies whether the element is trusted.</td>
</tr>
<tr>
<td>ExemptDoSProtection</td>
<td>Specifies whether the informational element is exempt from Denial of Service Protection.</td>
</tr>
<tr>
<td>Port</td>
<td>The element uses this port value on the external node. Range: 0-65535</td>
</tr>
<tr>
<td>Node</td>
<td>The external node on which the element resides. Select from the list.</td>
</tr>
<tr>
<td>Enable SIP UD</td>
<td>(Check box) Select to enable the SIP UDP port.</td>
</tr>
<tr>
<td>SIP UDP Port</td>
<td>Specifies the UDP port for SIP.</td>
</tr>
<tr>
<td>Enable SIP TCP</td>
<td>(Check box) Select to enable the SIP TCP port.</td>
</tr>
<tr>
<td>SIP TCP Port</td>
<td>Specifies the TCP port for SIP.</td>
</tr>
<tr>
<td>Enable SIP TLS</td>
<td>(Check box) Select to enable the SIP TLS port.</td>
</tr>
<tr>
<td>SIP TLS Port</td>
<td>Specifies the TLS port for SIP.</td>
</tr>
<tr>
<td>Local Edge Border Controller</td>
<td>Local Edge Border Controller of the local switch.</td>
</tr>
<tr>
<td>Remote Edge Border Controller Name</td>
<td>Name of Remote Edge Border Controller fronting the LSC.</td>
</tr>
<tr>
<td>Call Control Agent ID</td>
<td>Call Control Agent ID for ASAC purpose.</td>
</tr>
</tbody>
</table>
Configuring failover group

About this task
Use this procedure to configure a pair of primary/secondary Multifunction Softswitches (MFSS) on SS for failover group.

Procedure
1. Log on to the Provisioning Client with the secadmin, encadmin, or SuperUser role.
2. From the Provisioning Client menu bar, select Translations > Logical Entity to access the Service Node portlet.
3. In the list of logical entities, click the name of the logical entity to edit.
4. To add a route to the primary SS, click Add, and enter parameters for the new route.
5. Click Save to add the new route to the LE.
6. To add a route to the secondary SS, click Add, and enter parameters for the new route.
7. Click Save to add the new route to the LE.

Configuring failover group job aid

About this task
This job aid lists the parameters that you use to configure failover with a logical entity.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name the route in this field.</td>
</tr>
<tr>
<td>Node</td>
<td>Select the appropriate node from the list.</td>
</tr>
<tr>
<td>Parms</td>
<td>Select the appropriate element from the list:</td>
</tr>
<tr>
<td></td>
<td>• Trunk Group—This parameter associates a node with a trunk group.</td>
</tr>
<tr>
<td></td>
<td>• Facility Domain—This is the domain associated with the outgoing requested URL.</td>
</tr>
<tr>
<td></td>
<td>• User—The field is used in conjunction with SIP and PSTN-type gateways. The only option currently available in the list is phone. The phone is added to requested URL in the outgoing SIP INVITE.</td>
</tr>
<tr>
<td></td>
<td>• Locale—Select the language of the device. Populate the field to add a locale to the outgoing SIP message.</td>
</tr>
<tr>
<td>Weight (0-10)</td>
<td>Type a value between 0 and 10 for the route weight. The following guidelines apply for the weight field:</td>
</tr>
<tr>
<td></td>
<td>• Routes with a zero weight are disabled.</td>
</tr>
<tr>
<td></td>
<td>• At least one route must be defined before the logical entity can be added.</td>
</tr>
</tbody>
</table>

Table continues...
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• The total weight of all routes can be zero.</td>
</tr>
<tr>
<td></td>
<td>• The percentage of the total weight for each route is calculated automatically.</td>
</tr>
<tr>
<td></td>
<td>• Weight field has no meaning when Sequential Selection Algorithm is selected.</td>
</tr>
</tbody>
</table>
Chapter 8: Server configuration

About this task
This chapter contains procedures for Avaya Aura® Application Server 5300 server configuration.

• Configuring a server on page 82
• Configuring server alarm thresholds on page 83
• Starting the server monitor service on page 84
• Deleting a server on page 85

Configuring a server

About this task
The addition of new servers and server configuration typically occurs during installation and commissioning. For more information, see 102.1.1 AS5300 Server Installation, and 102.3.1 AS5300 Initial System Installation.

Prerequisites
• You can access the AS 5300 Element Manager.
• You have PhysicalServerService privileges.
• You have PhysicalSiteService privileges.
• You have IPAddressService privileges.
• You have SnmpProfileService privileges.

Procedure
1. From the configuration view of the AS 5300 Element Manager, select Servers.
2. Click Add (+).
3. In the Add Server dialog box, configure the parameters as required.
4. Click Apply.
   
   Use the new data to configure a network element instance.
Configuring a server job aid

About this task

This job aid lists and describes the parameters that appear on the Server dialog box. For more information about network traffic separation, see Network traffic separation on page 35.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>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.</td>
</tr>
<tr>
<td>Long Server Name</td>
<td>This parameter is the long name of the server, for example, EMS1Server.</td>
</tr>
<tr>
<td>Physical Site</td>
<td>This parameter (select from a list), specifies the location of the server.</td>
</tr>
<tr>
<td>IPv4 Internal OAM (Default) Address</td>
<td>This parameter (select from a list), specifies the IPv4 address to use for traffic internal to the enclave.</td>
</tr>
<tr>
<td>IPv4 External OAM Address</td>
<td>This optional parameter (select from a list) specifies the IPv4 address to use for traffic external to the enclave.</td>
</tr>
<tr>
<td>IPv4 Signaling Address</td>
<td>This optional parameter (select from a list) specifies the IPv4 address to use for signaling traffic.</td>
</tr>
<tr>
<td>IPv4 Media Address</td>
<td>This optional parameter (select from a list) specifies the IPv4 address to use for bearer traffic.</td>
</tr>
<tr>
<td>IPv6 Signaling Address</td>
<td>This optional parameter (select from a list) specifies the IPv6 address to use for signaling traffic.</td>
</tr>
<tr>
<td>IPv6 Media Address</td>
<td>This optional parameter (select from a list) specifies the IPv6 address to use for bearer traffic.</td>
</tr>
<tr>
<td>Operating System</td>
<td>This parameter (select from a list) indicates the operating system running on the server. Do not configure the value to windows. If the value is windows, memory information is not polled from the server. The system also uses this parameter to determine file paths.</td>
</tr>
<tr>
<td>Server Type</td>
<td>This legacy parameter can only be set to the following value: Other.</td>
</tr>
<tr>
<td>SNMP Profile</td>
<td>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.</td>
</tr>
<tr>
<td>Host Name</td>
<td>This parameter specifies the host name of the server.</td>
</tr>
</tbody>
</table>

Configuring server alarm thresholds

About this task

Configure alarm thresholds for CPU, memory, disk, and interface usage.
Server configuration

Prerequisites

- You have ServerMonitorConfigService privileges.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Servers > <server name> > Monitor.
2. On the <server name> Monitor window, click Configure Thresholds.
3. On the Server Monitor Alarm Threshold Configuration window, select or clear the Minor, Major, and Critical check boxes for the CPU, RAM, Disk, and Interface sections as required.
4. Modify the CPU, RAM, Disk, and Interface threshold values as required.
   You can edit the values only after you select the corresponding check box.
5. Click OK.

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;server_name&gt;</td>
<td>This value is the unique name that identifies the server.</td>
</tr>
</tbody>
</table>

Starting the server monitor service

About this task

To monitor the performance statistics for the server, you must use the AS 5300 Element Manager Console to start the server monitor.

Prerequisites

- You can access the AS 5300 Element Manager Console.
- You have PhysicalServerService privileges.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Servers > <server name> > Monitor.
   If the monitor is not already running, the status line at the bottom left of the server Monitor panel indicates “The server monitor is not running.”
2. Choose one of the tabs: Summary, Disk, Memory, CPU, or Interface.
3. Click Start Monitor to collect statistics for the server.
   The status line changes to indicate “The server monitor is running.”
Deleting a server

About this task

Use the following procedure to delete a server that does not host any network elements.

⚠ Important:

If you attempt to delete a server that has services deployed on it, the system rejects the request and indicates that the server is associated with NEInstanceData.

Prerequisites

• You can access the AS 5300 Element Manager Console.
• You have PhysicalServerService privileges.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Servers.
2. On the Servers window, select the server that you want to delete.
3. Click Delete (-).
4. Click Yes.

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Server Name&gt;</td>
<td>This value is the name of the server for which you want to start the monitor.</td>
</tr>
</tbody>
</table>
Chapter 9: Database configuration

About this task
This chapter contains the procedures that you require to configure the alarm thresholds for the database.
- Configuring database resource thresholds on page 86
- Monitoring the database on page 87

Configuring database resource thresholds

About this task
Perform this procedure to configure resource (disk space) thresholds for the database monitor control.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have DBMonitorConfigService privileges.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Database > <mcpdb name> > Monitor.
2. On the <mcpdb name> Monitor window, select an instance of the database.
3. Click Monitor.
4. On the <mcpdb name>_<instance> Database Instance Monitor window, click Configure Thresholds.
5. On the DB Monitor Alarm Threshold Configuration panel, select the corresponding check box for a threshold to enable the alarm.
   The corresponding configuration box is not available until you enable the alarm.
6. To change a default threshold, in the corresponding configuration box, type a new value for percent of disk space usage.
   The default thresholds are 80 for Minor, 90 for Major, and 100 for Critical.
7. Click OK.
Monitoring the database

About this task

Use this procedure to start the database monitor, and to view the capacity, disk space used, and status of the database.

Prerequisites

- You can access the AS 5300 Element Manager Console.
- Viewing the database monitor status requires an administrative role with DBMonitorService privilege.

Procedure

1. From the AS 5300 Element Manager Console configuration view, select Database > mcpdb > Monitor.
2. Select instance 0 or 1 from the mcpdb Monitor window and click Monitor.
3. Ensure that the status line at the bottom of the Monitor window indicates "The database instance monitor is running." If not, click Start Monitor.
Chapter 10: Network element configuration

This section provides the tasks that you perform to configure network elements.

Network element configuration tasks

About this task

This work flow shows the sequence of tasks that you perform to configure the network elements.

Navigation

- Network element addition on page 90
Network element configuration tasks

- **AS 5300 Element Manager configuration** on page 93
- **Accounting Manager configuration** on page 98
- **AS 5300 Session Manager configuration** on page 102
- **Provisioning Manager configuration** on page 127
Chapter 11: Network element addition

This section provides the procedures you perform to add a network element to the system during the initial configuration, to add redundancy, or to increase system capacity.

Network element addition procedures

About this task
This task flow shows you the sequence of procedures you perform to add a network element.

Navigation
- Adding a network element on page 91
Adding a network element

About this task
Perform this procedure to add network elements.

Important:
Installation of a network element on a server can generate a threshold alarm that indicates high CPU usage. The alarm clears after the installation is complete.

Prerequisites
• You can access the AS 5300 Element Manager Console.
• You have NEService privileges.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Elements ><NE type>.
   In the work area, a window for the selected network element type appears, displaying the existing network elements of this type.
2. In the network element window, click Add (+).
3. In the Add dialog box, type the configuration data.
   Different network element types require different configuration data. For help with property descriptions, move the pointer over the property name.
4. Click Apply.
   The Add dialog box closes and an entry appears in the network element type panel. The network element appears in the configuration view, but it does not have any associated servers or software.

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;NE type&gt;</td>
<td>This value is the name of the network element type, for example: Provisioning Managers,</td>
</tr>
</tbody>
</table>
Adding a network element instance

About this task
Perform this procedure to add an instance of a network element and associate the instance with a server.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have NEInstanceService privileges.

Procedure
1. In the configuration view of the AS 5300 Element Manager Console, expand Network Elements > <NE type> > <NE instance>.
2. Select Instance.
3. In the network element instance window, click Add (+) to add an instance of this network element and associate the instance with a server.
4. In the Add <NE instance> Instance dialog box, use the menus to associate a server, a software load, and an engineering profile with the instance.
   The engineering profile controls the initial size of the Java Virtual Machine and establishes engineering parameters appropriate for the hardware capabilities of the server.
5. Click Apply.
6. If the network element is fault tolerant, repeat 1 on page 92 to 5 on page 92 for the second unit.

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;NE type&gt;</td>
<td>This value is the name of the network element type, for example: Provisioning Managers,</td>
</tr>
<tr>
<td>&lt;NE instance&gt;</td>
<td>This value is the name of the network element instance, for example, PROV1.</td>
</tr>
</tbody>
</table>
Chapter 12: AS 5300 Element Manager configuration

About this task
This section provides the procedures that you perform to customize the AS 5300 Element Manager default configuration.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have NEService privileges.

Navigation
- Configuring AS 5300 Element Manager configuration parameters on page 93
- Moving the AS 5300 Element Manager network element instance on page 96

Configuring AS 5300 Element Manager configuration parameters

About this task
Perform this procedure to change the default configuration parameters for the AS 5300 Element Manager. You can modify configuration parameters while the network element is in service. Changes to these operating parameters apply to all network element instances of the network element and do not require a restart.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have ConfigParmService privileges.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Element Manager > Element Manager > Configuration Parameters.
2. In the Element Manager Configuration Parameters window, from the Parm Group list, select a parameter group.
3. Select the parameter to modify and click **Edit (-/+)**.

4. In the Edit dialog box, type or select a new value for the configuration parameter.

5. Click **Apply**.

   The system validates the new value. If the value is valid, the Edit Config Parm dialog closes and the configuration parameter updates.

---

### Configuring AS 5300 Element Manager configuration parameters job aid

**About this task**

This job aid lists the parameter groups and describes the configuration parameters for the AS 5300 Element Manager.

<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMAdminAudit</td>
<td>EnableAudit</td>
<td>This parameter enables checking for and automatic disabling of inactive Admin accounts. Default: false</td>
</tr>
<tr>
<td>HTTPConnector</td>
<td>ConnectionTimeout</td>
<td>This parameter controls the maximum number of seconds the HTTP Connector waits, after accepting a connection, for the request URI line to be presented. A value of 0 means no timeout. Default: 0</td>
</tr>
<tr>
<td></td>
<td>KeepAliveTimeout</td>
<td>This parameter controls the maximum number of seconds the HTTP Connector waits for another HTTP request before closing the connection. A value of 0 means no timeout. Default: 0</td>
</tr>
<tr>
<td>Load</td>
<td>LoadAuditIntervalInMinutes</td>
<td>This parameter controls the interval between checks of the AS 5300 Element Manager servers for loads and patches. This affects how often new loads and patches are detected and how often they are synchronized between the servers. Range: 2–60 Default: 5 minutes</td>
</tr>
<tr>
<td>Login</td>
<td>EnableLastLoginDisplay</td>
<td>This parameter enables or disables last login information. Range: true or false</td>
</tr>
<tr>
<td>Metrics</td>
<td>HistoryStorage</td>
<td>This parameter enables or disables the storage of historical information.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
|                  |                         | Range: true or false  
|                  |                         | Default: false |
| SNMP            | useProductDefaultMIBs   | This parameter determines whether the EM uses default MIBs.  
|                  |                         | Range: true or false  
|                  |                         | Default: true |
|                 | EmEngineIDforOSSLinks   | This parameter sets specific SNMPv3 engine ID for OSS servers.  
|                 | EmEngineIDforPlatformLinks | This parameter sets specific SNMPv3 engine ID for all internal AS 5300 servers.  
| Security        | DisableMtcLogs          | This parameter (if configured to true) disables the generation of SEC801 log reports for successful maintenance requests (such as opening the log browser).  
|                 |                         | Range: true or false  
|                 |                         | Default: false |
|                 | DisableReadLogs         | This parameter (if configured to true) disables the generation of SEC801 log reports for successful read requests (such as viewing values in the Network Data section of the AS 5300 Element Manager Console).  
|                 |                         | Range: true or false  
|                 |                         | Default: true |
|                 | DisableWriteLogs        | This parameter (if configured to true) disables the generation of SEC801 log reports for successful data change requests (such as changing Configuration Parameters).  
|                 |                         | Range: true or false  
|                 |                         | Default: false |
| TLSAuth         | EnableCRL              | This parameter enables CRL retrieval for certificate revocation status.  
|                 |                         | Default: false |
|                 | EnableOCSP             | This parameter enables OCSP retrieval for certificate revocation status.  
|                 |                         | Default: false |
|                 | EnforceTLSMutualAuthForHTTPS | This parameter enforces TLS Mutual Authentication for HTTP interface.  |
### Moving the AS 5300 Element Manager network element instance

#### About this task

After moving the AS 5300 Element Manager network element (NE) to another server, you specify the new server for the NE instance. Perform this procedure to move the NE Instance to a different server.

**Warning:**

This procedure is service-affecting. You must shut down the AS 5300 Element Manager to move it to another server.

**Caution:**

Engineering parameters must not be modified in the field. Modifying the engineering parameters for a network element instance can reduce the performance and services of the network element.

The only appropriate modifications to an NE Instance are to the load during an upgrade, or to move the NE Instance to a different server.

#### Prerequisites

- You can access the AS 5300 Element Manager Console.
- You have NEService privileges.
- You have NEInstanceService privileges.
- You have EngParmService privileges.
- You are familiar with the procedures to start, stop, deploy, and undeploy a network element. For more information, see [Common procedures](#) on page 224.

#### Procedure

1. Stop the AS 5300 Element Manager instance on the original server.
**Important:**

If this is the active AS 5300 Element Manager instance, the standby instance takes over activity and the connection to the AS 5300 Element Manager Console is lost.

2. Undeploy the AS 5300 Element Manager instance on the original server.

3. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Element Manager > Element Manager > Instance**.

4. On the Element Manager Instance window, select the Element Manager instance to modify and click **Edit (-/+)**.

5. From the **Server** list, select the server that hosts the Element Manager.

6. Click **Apply**.

7. Deploy the Element Manager instance on the new server.

8. Start the Element Manager instance on the new server.
Chapter 13: Accounting Manager configuration

About this task
This section provides the procedures that you perform to customize the Accounting Manager (AM) default configuration.

⚠️ Important:
Only one instance of the AM can be active at a time.

Prerequisites
• You can access the AS 5300 Element Manager Console.
• You are familiar with the procedure to restart a network element. See Restarting a network element on page 227.

Navigation
• Configuring Accounting Manager configuration parameters on page 98
• Configuring the whole Accounting Manager network element on page 99
• Moving the Accounting Manager network element instance on page 100

Configuring Accounting Manager configuration parameters

About this task
Perform this procedure to change the default configuration parameters for the Accounting Manager. You can modify configuration parameters while the network element is in service. Changes to these operating parameters apply to all network element instances of the network element and do not require a restart.

Prerequisites
• You can access the AS 5300 Element Manager Console.
• You have ConfigParmService privileges.
Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Accounting Managers > <Accounting Manager Instance> > Configuration Parameters**.
2. On the Config Parms window, from the **Parm Group** list, select **OM**.
3. Select **OfficeTransferPeriod** and click **Edit (-/+)**.
4. In the Edit dialog box, type a new value for the configuration parameter.
5. Click **Apply**.

   The system validates the new value. If the value is valid, the Edit dialog closes and the configuration parameter updates.

---

### Configuring Accounting Manager configuration parameters job aid

**About this task**

This job aid lists the parameter groups and describes the configuration parameters for the Accounting Manager.

<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OM</td>
<td>OfficeTransferPeriod</td>
<td>This parameter specifies the Fault Performance Manager polling period, in minutes. Range: 5, 15, 30, or 60 Default: 15</td>
</tr>
</tbody>
</table>

---

### Configuring the whole Accounting Manager network element

**About this task**

You can modify many options that are specific to each network element type, such as the base port of a network element application. You can also associate a different Fault Performance Manager with the network element.

**Prerequisites**

- You can access the AS 5300 Element Manager Console.
- You have NEService privileges.

**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Accounting Managers**.
2. In the Accounting Managers window, select the entry for the network element to modify and click Edit (-/+).

3. In the Edit <Accounting Manager instance> dialog box, modify the Long Name, Base Port, FPM, IPv4 internal OAM Service Address and IPv4 external OAM Service Address values as required.

4. Click Apply.

5. Restart the Accounting Manager instance.

### Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Accounting Manager instance&gt;</td>
<td>This value is the name of the Accounting Manager, such as AM1.</td>
</tr>
</tbody>
</table>

### Configuring the whole Accounting Manager network element job aid

**About this task**

This job aid lists and describes the fields on the Edit <Accounting Manager instance> dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Name</td>
<td>(Read-only) The short name of the NE; maximum of 6 characters</td>
</tr>
<tr>
<td>Long Name</td>
<td>The long name of the NE; maximum of 32 characters</td>
</tr>
<tr>
<td>Base Port</td>
<td>A range of 100 ports reserved off the base port for use by the NE Range: 1100–654000</td>
</tr>
<tr>
<td>Internal OAM Service Address</td>
<td>The internal OAM (Default) service address used by the NE</td>
</tr>
<tr>
<td>External OAM Service Address</td>
<td>The external OAM service address used by the NE</td>
</tr>
<tr>
<td>Acct Format Path</td>
<td>The name of the accounting format path</td>
</tr>
</tbody>
</table>

### Moving the Accounting Manager network element instance

**About this task**

After moving the Accounting Manager network element (NE) to another server, you specify the new server for the NE instance.
Warning:
This procedure is service-affecting. You must shut down the Accounting Manager to move it to another server.

Caution:
Engineering parameters must not be modified in the field. Modifying the engineering parameters for a network element instance can reduce the performance and services of the network element.

The only appropriate modifications to an NE Instance are to the load during an upgrade, or to move the NE Instance to a different server.

Prerequisites

- You can access the AS 5300 Element Manager Console.
- You have NEService privileges.
- You have NEInstanceService privileges.
- You have EngParmService privileges.
- You are familiar with the procedures to start, stop, deploy, and undeploy a network element. For more information, see Common procedures on page 224.

Procedure

1. Stop the Account Manager instance on the original server.
2. Undeploy the Account Manager instance on the original server.
3. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Accounting Managers > <Accounting Manager instance> > Instance
4. On the <Accounting Manager instance> Instance window, select the Accounting Manager instance to modify and click Edit (+/−).
5. From the Server list, select the server that hosts the Accounting Manager.
6. Click Apply.
7. Deploy the Account Manager instance on the new server.
8. Start the Account Manager instance on the new server.
Chapter 14: AS 5300 Session Manager configuration

About this task
This section provides the procedures that you perform to customize the AS 5300 Session Manager (SESM) default configuration.

Prerequisites
- You can access the AS 5300 Element Manager Console.

Navigation
- Configuring AS 5300 Session Manager configuration parameters on page 102
- Configuring the whole AS 5300 Session Manager network element on page 119
- Configuring the Master LSC functional role on page 121
- Configuring the Slave LSC functional role on page 123
- Configuring the SS functional role on page 124
- Moving the AS 5300 Session Manager network element instance on page 125

Configuring AS 5300 Session Manager configuration parameters

About this task
Perform this procedure to change the default configuration parameters for the AS 5300 Session Manager. You can modify configuration parameters while the network element is in service. Changes to these operating parameters apply to all network element instances of the network element and do not require a restart.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have ConfigParmService privileges.

Procedure
1. From the Configuration view of the AS 5300 Element Manager Console, select Network Elements > Session Managers > <SESM instance> > Configuration Parameters.
2. On the Configuration Parameters window, from the **Parm Group** list, select a parameter group.
3. Select the parameter to modify and click **Edit (-/+)**.
4. In the Edit Config Parm dialog box, type a new value for the configuration parameter.
5. Click **Apply**.

The system validates the new value. If the value is valid, the Edit Config Parm dialog closes and the configuration parameter updates.

---

### Configuring AS 5300 Session Manager configuration parameters job aid

**About this task**

This job aid lists the parameter groups and describes the configuration parameters for the AS 5300 Session Manager.

<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting</td>
<td>IMBillingActive</td>
<td>This parameter turns the capture of IM billing information on or off.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: true or false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: true</td>
</tr>
<tr>
<td></td>
<td>RegisterSuccessBilling</td>
<td>This parameter controls whether the system generates records for successful user registrations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: true or false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>ARTSFailover</td>
<td>LSCtoSSLinkRecoveryHoldOffPeriod</td>
<td>Time interval before the SIP traffic returns to the primary SS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 1 second – no upper limit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 60</td>
</tr>
<tr>
<td></td>
<td>LSCCSSOnMissedPingDelay</td>
<td>This parameter is not supported currently.</td>
</tr>
<tr>
<td></td>
<td>LSCtoSSPingInterval</td>
<td>Time interval between OPTIONS requests sent from LSC to SS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 35 seconds – no upper limit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 45</td>
</tr>
<tr>
<td></td>
<td>LSCtoSSPingIntervalOnFailure</td>
<td>Time interval between OPTIONS requests to failed SS upon failover.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 35 seconds – no upper limit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 60</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
|                 | LSCtoSSSuccessivePingNumber | Number of successive OPTIONS requests from LSC to SS before the failover is initiated.  
Range: 1 – no upper limit  
Default: 2 |
|                 | PingSecondarySS | This parameter indicates whether the secondary SS should be pinged or not.  
Range: true or false  
Default: true |
|                 | SSLSCMissedPingNumberToFailover | This parameter is not supported currently. |
|                 | SSLSCOnFailoverNoPingingTimeout | This parameter is not supported currently. |
|                 | SSLSCOnMissedPingDelay | This parameter is not supported currently. |
|                 | SSLSCOnSecondMissedPingDelay | This parameter is not supported currently. |
|                 | SSLSCPingPeriod | This parameter is not supported currently. |
|                 | SSLinkRecoveryHoldOffPeriod | Time interval before the SIP traffic returns to the recovered SS.  
Range: 1 second – no upper limit  
Default: 60 |
|                 | SSOnMissedPingDelay | This parameter is not supported currently. |
|                 | SSOnSecondMissedPingDelay | This parameter is not supported currently. |
|                 | SSOnPingInterval | Time interval between OPTIONS requests sent from an SS to another SS.  
Range: 35 seconds – no upper limit  
Default: 45 |
|                 | SSOnPingIntervalOnFailure | Time interval between OPTIONS requests to failed SS upon failover.  
Range: 35 seconds – no upper limit  
Default: 60 |
|                 | SSOnSuccessivePingNumber | Number of successive OPTIONS requests from an SS to another SS before the failover is initiated.  
Range: 1 – no upper limit |

Table continues…
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>AllowAdvancedAuthentication</td>
<td>This parameter enables or disables advanced authentication. Range: true or false. Default: true.</td>
</tr>
<tr>
<td></td>
<td>AuthenticationWithIntegrity</td>
<td>This parameter allows Session Managers to support the less secure Auth only authentication method when configured to false. AuthenticationWithIntegrity is a more secure authentication method. Range: true or false. Default: true.</td>
</tr>
<tr>
<td></td>
<td>GracePeriod</td>
<td>This parameter defines the grace period value of a nonce. This value is used in advanced SIP authentication. Default: 90,000.</td>
</tr>
<tr>
<td></td>
<td>NCSequenceeEnforcement</td>
<td>This parameter is a Boolean value that activates or deactivates the nonce-count value validation received from the user agent. Default: false.</td>
</tr>
<tr>
<td></td>
<td>NonceUsageCount</td>
<td>This parameter defines the usage count value of a nonce. This value is used in advanced SIP authentication. Default: 30,000.</td>
</tr>
<tr>
<td></td>
<td>PrivateKey</td>
<td>This parameter is the key the system uses to generate unique authentication challenges. Range: 0–256 characters. Default: MCP.</td>
</tr>
<tr>
<td></td>
<td>CPUCallsTimeToLive</td>
<td>Call Pickup Call's time to live on call queue (in seconds). Range: 60 to 900 seconds. Default: 120.</td>
</tr>
<tr>
<td>CallAcrossDomain</td>
<td>UseBlockCallsAcrossDomains</td>
<td>Parameter to block calls across domains. Range: true or false. Default: false.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| CallGrabber         | HoldBeforeGrabbing               | Configure this parameter to false to skip the hold before grabbing  
Range: true or false  
Default: true                                                   |
| CallReturn          | AnonymousCallback                | This parameter allows a subscriber to return a call even if the originating party has the Calling Line ID Restriction active. The subscriber must have Call Return service in the service set.  
Range: true or false  
Default: false                                                   |
| ConvergeMobility    | IMSInviteProvisionalTimer         | This parameter is not supported.                                                                                                           |
|                     | StandaloneInviteProvisionalTimer  | This parameter is not supported.                                                                                                           |
| DNS                 | AuditInterval                    | This parameter defines the audit interval (in minutes) for the DNS table.  
Range: 1–2,147,483,647  
Default: 5                                                        |
|                     | MaxEntry                         | The maximum number of entry placed in IMDNS cache for each DNS query.  
Range: 1-3  
Default: 3                                                        |
|                     | MaxTuples                        | The maximum size of the IMDNS table.  
Range: 1-10,000  
Default: 100                                                       |
|                     | NegativeExpiry                   | The time an invalid DNS entry (IP of an unknown domain not configured in DNS) remains in the IMDNS table.  
Range: 1 minute – no upper limit  
Default: 10 minutes                                                  |
|                     | PositiveExpiry                   | The duration in minutes a valid DNS entry (IP of unknown domain configured in DNS) remains in the IMDNS table.  
Range: 1 minute – no upper limit  
Default: 60 minutes                                                  |
| Diameter            | EnableListening                  | This parameter is not supported.                                                                                                           |
|                     | Port                             | This parameter is not supported.                                                                                                           |
|                     | Realm                            | This parameter is not supported.                                                                                                           |

Table continues…
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| EarlyProgress   | EarlyProgressTimer      | This parameter specifies the time for the early 180 progress signal.  
Range: 0–30 seconds  
Default: 3 |
| GCP             | Port                    | This parameter defines the UDP Port that the Communication Server 2000 / Avaya Aura® Application Server 5300 uses to communicate with the Gateway Controller using the GCP protocol. This port is used for call control signalling. Maintenance messages are always sent on the specified port + 1. For example, if the port specified is 7060, the message is sent on port 7061.  
Range: 1–2,147,483,647  
Default: 7,060 |
| 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 Personal 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.  
Range: true or false |
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Default: false</td>
<td></td>
</tr>
<tr>
<td>Enable TPCC DoS filter</td>
<td>This parameter enables or disables the HTTP Denial of Service protection feature for Third Party Call Control. Range: true or false Default: false</td>
<td></td>
</tr>
<tr>
<td>HungCall</td>
<td>HungUnstableCallAuditTimer</td>
<td>This parameter defines the time for releasing unstable hung transaction, in minutes. The value for this parameter needs to remain at 3 Default: 3</td>
</tr>
<tr>
<td></td>
<td>HungTimeout</td>
<td>This parameter is measured in seconds. The value is 190 or higher Default: 190</td>
</tr>
<tr>
<td>KPIAlarm</td>
<td>IsAlarmEnabled</td>
<td>Default: false</td>
</tr>
<tr>
<td>KPI_CallDist</td>
<td>answer_Seizure_Ratio</td>
<td>Default: 90,70,60,NEG</td>
</tr>
<tr>
<td></td>
<td>call_Treated_Ratio</td>
<td>Default: 60,70,90,POS</td>
</tr>
<tr>
<td>KPI_IncomingCall</td>
<td>Call_Abandon_Ratio</td>
<td>Default: 60,70,90,POS</td>
</tr>
<tr>
<td></td>
<td>Call_Other_Ratio</td>
<td>Default: 60,70,90,POS</td>
</tr>
<tr>
<td></td>
<td>Call_Success_Ratio</td>
<td>Default: 90,70,60,NEG</td>
</tr>
<tr>
<td></td>
<td>Call_Treated_Ratio</td>
<td>Default: 60,70,90,POS</td>
</tr>
<tr>
<td>LDAP</td>
<td>AuditInterval</td>
<td>This parameter defines the interval between two LDAP audit queries, in seconds. Range: 5–86,400 Default: 60 (one minute)</td>
</tr>
<tr>
<td></td>
<td>MaxThreadCount</td>
<td>Maximum number of threads for bulk operations. Range: 0-10 Default: 10</td>
</tr>
<tr>
<td></td>
<td>ThreadTimeOut</td>
<td>Idle timeout value in minutes for threads run during bulk operations Range: 10-60 Default: 10 (minutes)</td>
</tr>
<tr>
<td></td>
<td>TimeToLive</td>
<td>This parameter defines the expiration value for cached LDAP data, in seconds. Range: 1000–10 000 Default: 3,600 (one hour)</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
|                 | **TimeToLiveUnreliable**           | Expiration time of LDAP lookups stored in the IMLDAPAddrLookupTable which are marked as unreliable.  
Range: 0-10,000 seconds.  
Default is 300 seconds                                                                                                                                  |
| LongCall        | **CheckpointAuditDuration**        | This parameter controls the maximum amount of time that a checkpointed call takes to be audited after a failover. After the timer expires after a failover, an INFO message is sent to the clients to ensure the call is still active. A value of zero disables the audit.  
Range: 0–2,147,483,647 seconds  
Default: 30                                                                                                                                                |
| Duration        | **Duration**                       | This parameter determines the length of time, in minutes, between endpoint audits. Duration is used to detect abandoned calls. A value of zero deactivates the duration parameter.  
Range: 0–2,147,483,647 seconds  
Default: 60  
A call cannot be torn down if the long call audit is running and an abandoned call is detected. The Engineering parameter, MAX_AUDIT_FAILURE, controls how many audit failures occur before a call is torn down.  
Default: 3                                                                                                                                            |
|                 | **Emergency Duration**             | This parameter controls the long call audit duration for emergency calls.  
Range: 0–2,147,483,647 seconds  
Default: 30                                                                                                                                                |
|                 | **SipLinesDuration**               | SIP Lines is not supported.                                                                                                                                                                                                                                                                                                                  |
|                 | **TlsTcpCallAuditDuration**        | This parameter specifies the timer duration between retires to audit TLS/TCP calls after an EM failover.  
Range: 0–2,147,483,647 seconds  
Default: 300 seconds                                                                                                                                            |
| MLPP            | **ForwardingDiversionTimer**       | This parameter controls the number of seconds before diversion occurs, after a user forwards a call.  
Range: 0-45 seconds  
Default: 30                                                                                                                                                |
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>InitialDiversionTimer</td>
<td>This parameter controls the number of seconds before diversion occurs, after a user forwards a call (no call forward).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 15-45 seconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 45</td>
</tr>
<tr>
<td></td>
<td>StrictEnforcement</td>
<td>This parameter enforces the Resource-Priority tag within the Requires header. Configure to false to allow the AS 5300 Session Manager to remove the Resource-Priority tag to terminate to a client that does not support the tag.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: true or false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>Media Portal</td>
<td>BCPOptimizationSupport</td>
<td>This parameter toggles BCP Optimization on or off.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: true or false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td></td>
<td>DisableFirewallPortal–Strategy</td>
<td>Configure this parameter to TRUE when the firewall strategy for a client is disabled. Configure this parameter to TRUE if a Border Control Point or Media Portal server is NOT deployed as part of this system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: true or false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td></td>
<td>IgnorempRules</td>
<td>Configure this parameter to TRUE if a Border Control Point or Media Portal server is NOT deployed as part of this system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: true or false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td></td>
<td>InsertPortalWhenAnyBFW</td>
<td>This parameter inserts a portal if any client in the same domain is behind a firewall. This parameter applies only to programmatic rules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: true or false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td></td>
<td>LocationBasedInsertRules</td>
<td>This parameter controls whether activation location is based on media portal insertion rules. Medial Portal Insertion is not supported.</td>
</tr>
<tr>
<td>OBSSubscribe</td>
<td>MaxSubscribeAttempts</td>
<td>This parameter defines the maximum allowable subscription value, in seconds, for a subscription request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 1–10</td>
</tr>
<tr>
<td>Parameter group</td>
<td>Configuration parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 5</td>
</tr>
<tr>
<td></td>
<td>MaximumExpires</td>
<td>This parameter defines the number of times to attempt to subscribe before giving up. Range: 60–86,400 Default: 86,400</td>
</tr>
<tr>
<td></td>
<td>ResubscribeDelay</td>
<td>This parameter controls subscription delay, which the system uses for both local and remote overload. If it gets 408, 503 from the remote server, and there is no retry after header, the delay value is used as the delay before the subscription retry. If the AS 5300 Session Manager is in an overload state, the delay is the start-time for the next attempt. Range: 60–600 Default: 60</td>
</tr>
<tr>
<td></td>
<td>ResubscribeOffset</td>
<td>This field controls how many seconds before a Subscription expires that the system sends the refresh subscription to prevent the subscription from expiring. Range: 60–600 Default: 30</td>
</tr>
<tr>
<td>OverlapDialing</td>
<td>InterDigitTimer</td>
<td>Default: 4</td>
</tr>
<tr>
<td></td>
<td>SanityTimer</td>
<td>Default: 30</td>
</tr>
<tr>
<td>OM</td>
<td>OfficeTransferPeriod</td>
<td>This parameter specifies the Fault Performance Manager polling period, in minutes. Range: 5, 15, 30, or 60 Default: 15</td>
</tr>
<tr>
<td>Publish</td>
<td>MaximumExpires</td>
<td>This parameter defines the maximum allowable expiration value for a subscription request in seconds. Range: 60–86,400 Default: 86,400</td>
</tr>
<tr>
<td></td>
<td>MinimumExpires</td>
<td>This parameter defines the minimum allowable expiration value for a subscription request in seconds. Range: 60–86,400 Default: 60</td>
</tr>
<tr>
<td>Registrar</td>
<td>ActiveSubscriber</td>
<td>This parameter defines the maximum number of subscribers that can register. If EnforceActiveSubscriber is true and new registration request exceeds this value, the registration request is declined with the 603 “Active subscriber limit exceeded” SIP message.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
|                 |                         | Range: 1–2,147,483,647  
                       |                          | Default: 25,000 |
|                 | EnforceActiveSubscriber | This parameter enforces the registration count.  
                       |                          | Range: true or false  
                       |                          | Default: false |
|                 | MaximumExpires          | This parameter defines the maximum allowable registration duration, in seconds.  
                       |                          | Range: 60–86,400  
                       |                          | Default: 86,400 |
|                 | MinimumExpires          | This parameter defines the minimum allowable registration duration in seconds.  
                       |                          | Range: 60–86,400  
                       |                          | Default: 60 |
|                 | NATClientSupport        | If you configure this parameter to true, the system supports the storage of NAT binds in client registration.  
                       |                          | Range: true or false  
                       |                          | Default: true |
|                 | NATKeepAliveTimer       | Duration of registration expiration (used for NAT keepAlive).  
                       |                          | Range: 0 and 15-90 seconds  
                       |                          | Default: 0 |
|                 | SIPDoS                  | Enable DoS Filter  
                       |                          | This parameter enables or disables the SIP DoS protection feature.  
                       |                          | Range: enabled or disabled  
                       |                          | Default: disabled |
|                 | SIPPBX                  | AlarmTimer  
                       |                          | SIPPBX is not supported. |
|                 |                          | CallFailureTresholds  
                       |                          | SIPPBX is not supported. |
|                 |                          | CapacityTresholds  
                       |                          | SIPPBX is not supported. |
|                 | SIPStack                | AutoAnswerForBYE  
                       |                          | If you configure this parameter to true, the stack sends an auto 200 OK message in response to a BYE request.  
                       |                          | Range: true or false  
                       |                          | Default: true |
|                 |                          | DEFAULT_MAX_BUFFER_SIZE  
                       |                          | This parameter controls the maximum UDP message length.  
                       |                          | Range: 0–2,147,483,647 |

Table continues…
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SendonlySupport</td>
<td>IsHoldBySendonly</td>
<td>Configure to true if for incoming re-INVITEs with the Sendonly Hold attribute.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: true or false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>Session Timer</td>
<td>Min-SE</td>
<td>The parameter indicates the minimum value that is accepted for the session interval (the keep-alive mechanism for SIP sessions), in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 90–2,147,483,647</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 90</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Only sessions established after configuration are affected by the new parameter value.</td>
</tr>
<tr>
<td>Sh</td>
<td>MaxMsgRetranmission</td>
<td>This parameter specifies the maximum number of times the system resends an Sh message.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 1–10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 3</td>
</tr>
<tr>
<td></td>
<td>QueueThresholdsHigh</td>
<td>This parameter specifies the queue alarm threshold high, as a percent of queue size.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 75–95</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 90</td>
</tr>
<tr>
<td></td>
<td>QueueThresholdsLow</td>
<td>This parameter specifies the queue alarm threshold low, as a percent of queue size.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 5–25</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 10</td>
</tr>
<tr>
<td>SignalSupport</td>
<td>AddUserEqualsPhoneForE164</td>
<td>Configure this parameter to true to add the user=phone parameter to any outgoing INVITE, for which the user portion of the Request URI uses the E. 164 format. (Required for some CSCF networks to route correctly.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: true or false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td></td>
<td>HandleReferForHomedInitiat</td>
<td>Configure this parameter to true to have the Application Server 5300 handle REFER as if the REFER initiator is homed on the Application Server 5300.</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td>Range: true or false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>Parameter group</td>
<td>Configuration parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>HandleReferForeignParty</td>
<td>Configure this parameter to true to have the Application Server 5300 handle REFER as if the REFER target is a foreign destination.</td>
<td>Range: true or false. Default: false</td>
</tr>
<tr>
<td>RouteByDefaultToICSCF</td>
<td>Configure this parameter to true to send call legs (for example, transfer legs) to the I-CSCF instead of the S-CSCF.</td>
<td>Range: true or false. Default: false</td>
</tr>
<tr>
<td>SipBehavior</td>
<td>ConcealAuthFailureReason</td>
<td>Range: true or false. Default: true</td>
</tr>
<tr>
<td></td>
<td>IncludeMessageAccountForMWI</td>
<td>Configure this parameter to true to include the Message-Account header in MWI Notify Message.</td>
</tr>
<tr>
<td>SIPRespOM-Thresh</td>
<td>Info500</td>
<td>This parameter indicates how many 500 error responses can be received for SIP Info Requests before an alarm is raised.</td>
</tr>
<tr>
<td></td>
<td>Invite500</td>
<td>This parameter indicates how many 500 error responses can be received for SIP Info Requests before an alarm is raised.</td>
</tr>
<tr>
<td></td>
<td>Message500</td>
<td>This parameter indicates how many 500 error responses can be received for SIP Message Requests before an alarm is raised.</td>
</tr>
<tr>
<td></td>
<td>Notify500</td>
<td>This parameter indicates how many 500 error responses can be received for SIP Notify Requests before an alarm is raised.</td>
</tr>
<tr>
<td>Parameter group</td>
<td>Configuration parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15</td>
</tr>
<tr>
<td>Options500</td>
<td></td>
<td>This parameter indicates how many 500 error responses can be received for SIP Options Requests before an alarm is raised. Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15</td>
</tr>
<tr>
<td>Publish500</td>
<td></td>
<td>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</td>
</tr>
<tr>
<td>Refer500</td>
<td></td>
<td>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</td>
</tr>
<tr>
<td>Register500</td>
<td></td>
<td>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</td>
</tr>
<tr>
<td>Service500</td>
<td></td>
<td>Default: 5,10,15</td>
</tr>
<tr>
<td>Subscribe500</td>
<td></td>
<td>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</td>
</tr>
<tr>
<td>Update500</td>
<td></td>
<td>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</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIPTransport</td>
<td>GatewayBehindNATSupport</td>
<td>This parameter toggles support for gateways behind NAT.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: true or false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td></td>
<td>InitialMaxHops</td>
<td>This parameter specifies the maximum number of hops allowed before the H.323 Gatekeeper drops the request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 5–50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 20</td>
</tr>
<tr>
<td></td>
<td>InviteTimer</td>
<td>This parameter controls the maximum time in seconds to wait for an INVITE to receive a final response, after receiving a provisional response.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 180–3,600</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 180</td>
</tr>
<tr>
<td></td>
<td>MaxRedirections</td>
<td>This parameter specifies the maximum number of redirections allowed before the system drops a request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 3–10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 5</td>
</tr>
<tr>
<td></td>
<td>MaxTermAttempt</td>
<td>This parameter specifies the maximum number of internal cpl loops allowed before the system drops a request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 5–50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 10</td>
</tr>
<tr>
<td></td>
<td>NetworkSupportedPacketization</td>
<td>This parameter specifies the network supported packet times when a CS 2000 is present. A comma-separated list of packet times in milliseconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: not configured</td>
</tr>
<tr>
<td></td>
<td>RejectCallIfNoRegDests</td>
<td>Configure this parameter to true to reject calls for which there is no regdest for term user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: true or false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td></td>
<td>ServiceNodeName</td>
<td>This parameter specifies the host name to use in a CS 2000 Via header. The value is the host name associated with the logical service address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: not configured</td>
</tr>
</tbody>
</table>
### Configuring AS 5300 Session Manager configuration parameters

<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscribe</td>
<td>CallParkMaximumExpires</td>
<td>This parameter defines the maximum allowable expiration value for a callpark subscription request, in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 60–86,400</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 86,400</td>
</tr>
<tr>
<td></td>
<td>MaximumExpires</td>
<td>This parameter defines the maximum allowable expiration value for a subscription request, in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 60–86,400</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 86,400</td>
</tr>
<tr>
<td></td>
<td>MinimumExpires</td>
<td>This parameter defines the minimum allowable expiration value for a subscription request, in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 60–86,400</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 60</td>
</tr>
<tr>
<td></td>
<td>PresenceMaximumExpires</td>
<td>This parameter defines the maximum allowable expiration value for a presence subscription request, in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 60–86,400</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 86,400</td>
</tr>
<tr>
<td>SubscriberOAM</td>
<td>MonitorRefreshRateSeconds</td>
<td>This parameter specifies the number of seconds between each refresh of the subscriber monitoring panel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 1 or more</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 5</td>
</tr>
<tr>
<td></td>
<td>StaticClientAuditStartHOD</td>
<td>This parameter specifies the hour of the day at which the static client audit starts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 0–23</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 3</td>
</tr>
<tr>
<td></td>
<td>UnreachableClientsThreshold</td>
<td>This parameter specifies the percentage of unreachable static clients encountered by an audit, after which the system raises an alarm.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 1–100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 100</td>
</tr>
<tr>
<td>Syntax</td>
<td>BadSyntaxLogging</td>
<td>This parameter controls whether the RV stack raises an alarm after the stack encounters an error.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Range: 0–2</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSAuth</td>
<td>EnableCRL</td>
<td>This parameter enables CRL retrieval for certificate revocation status. Default: false</td>
</tr>
<tr>
<td></td>
<td>EnableOCSP</td>
<td>This parameter enables OCSP retrieval for certificate revocation status. Default: false</td>
</tr>
<tr>
<td></td>
<td>EnforceTLSMutualAuthForSIP</td>
<td>This parameter enforces TLS Mutual Authentication for SIP interface. Default: false</td>
</tr>
<tr>
<td></td>
<td>EnforceTLSMutualAuthForXMPP</td>
<td>This parameter enforces TLS Mutual Authentication for XMPP connections. Default: false</td>
</tr>
<tr>
<td></td>
<td>PermitIfNoRevocation-ValidateResp</td>
<td>This parameter permits access, if no certificate revocation validation response. Default: true</td>
</tr>
<tr>
<td></td>
<td>SyncOCSPForSIP</td>
<td>This parameter enables synchronous OCSP query for SIP interface. Default: false</td>
</tr>
<tr>
<td>TLSSession</td>
<td>Allow TLS session resumption</td>
<td>Default: false</td>
</tr>
<tr>
<td></td>
<td>Enforce renegotiation</td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>XmppTLSHandshakeTimeout</td>
<td>This parameter specifies the amount of time (in milliseconds) the XMPP TLS handshake has to complete before timing out. Range: 1000–60000 Default: 2000</td>
</tr>
<tr>
<td>X2</td>
<td>QueueThresholdsHigh</td>
<td>This parameter specifies the queue threshold high value as a percent of QueueSize. Range: 75–95 Default: 90</td>
</tr>
</tbody>
</table>

Table continues...
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
|                 | QueueTresholdsLow       | This parameter specifies the queue threshold low value as a percent of QueueSize.  
Range: 5–25  
Default: 10 |
| XMPP            | EnableLogs             | This parameter enables extra logs for the XMPP feature.  
Default: false |
|                 | StreamIdleTimeout      | This parameter determines when an XMPP stream and connection is closed due to inactivity. Inactivity is defined as no XMPP data being exchanged for a given amount of time.  
Range: 10 minutes — 60 minutes  
Default: 15 minutes |
|                 | ConnectionFailureWindow| This parameter determines the time period in which failed XMPP connection attempts are counted. |
|                 | ConnectionBanPeriod    | This parameter determines the lockout period for failed XMPP connections that exceed the limit for failed connection attempts. |
|                 | ConnectionAttemptsForBan| This parameter determines the number of failed connection attempts after which, the peer XMPP server is locked out. |
|                 | ValidatePeerCertificate| This parameter enables peer server certificate validation according to XEP-0178. |
|                 | BindAttempts           | This parameter determines the number of times a client can try to bind resource to XMPP stream when initiating connection.  
Default: 2  
Range: 1-10 |

### Configuring the whole AS 5300 Session Manager network element

**About this task**

You can modify many options that are specific to each network element type, such as the base port of a network element application, or you can associate a different Fault Performance Manager with the network element.

For information about how to configure the AS 5300 Session Manager for a FIPS-compliant system, see *Avaya Aura® Application Server 5300 Security, NN42040-601*. 
Prerequisites

- You can access the AS 5300 Element Manager Console.
- You have NEService privileges.
- You are familiar with the procedure to restart a network element. See Restarting a network element on page 227.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Session Managers.
2. In the Session Managers window, select the entry for the network element to modify and click Edit (-/+).
3. In the Edit <Session Manager instance> dialog box, modify the parameters as required.
   
   **Important:**
   Systems that do not use TLS and SRTP use UDP and RTP. The Audiocodes Mediant 3000 does not support best effort RTP/SRTP (mixed-mode). The configuration for all endpoints must be either secure or nonsecure for media.

4. Click Apply.
5. Restart the network elements as required.

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Session Manager instance&gt;</td>
<td>This value is the name of the AS 5300 Session Manager, such as SESM1.</td>
</tr>
</tbody>
</table>

Configuring the whole AS 5300 Session Manager network element job aid

About this task

This job aid lists the fields on the Edit <Session Manager instance> dialog box.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Name</td>
<td>(Read-only) The short name of the network element (NE)—maximum of 6 characters.</td>
</tr>
<tr>
<td>Long Name</td>
<td>The long name of the NE—maximum of 32 characters.</td>
</tr>
<tr>
<td>Base Port</td>
<td>A range of 100 ports reserved off the base port for use by the NE. Range: 1100–654000</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPM</td>
<td>The FPM used by the NE.</td>
</tr>
<tr>
<td>IPv4 Signaling Service Address</td>
<td>The IPv4 Signaling Service Address used by the NE.</td>
</tr>
<tr>
<td>IPv6 Signaling Service Address</td>
<td>The IPv6 signaling service address used by the NE.</td>
</tr>
<tr>
<td>AM</td>
<td>The Accounting Manager to which the NE reports. (Select from the list.)</td>
</tr>
<tr>
<td>Call Park Id</td>
<td>(Read-only) The ID prepended to a call park number. This ID indicates the AS 5300 Session Manager, on which a call is parked.</td>
</tr>
<tr>
<td>Enable SIP UDP</td>
<td>Enables the SIP UDP port. Selected = enabled Not selected = disabled</td>
</tr>
<tr>
<td>SIP UDP Port</td>
<td>Specifies the UDP port for SIP. Example: 5060</td>
</tr>
<tr>
<td>Enable SIP TCP</td>
<td>Enables the SIP TCP port. Selected = enabled Not selected = disabled</td>
</tr>
<tr>
<td>SIP TCP Port</td>
<td>Specifies the TCP port for SIP. Example: 5060</td>
</tr>
<tr>
<td>Enable SIP TLS</td>
<td>Enables the SIP TLS port. Selected = enabled Not selected = disabled</td>
</tr>
<tr>
<td>SIP TLS Port</td>
<td>Specifies the TLS port for SIP. Example: 5061</td>
</tr>
<tr>
<td>Enable XMPP TLS</td>
<td>Enables the XMPP TLS port. Selected = enabled Not selected = disabled</td>
</tr>
<tr>
<td>XMPP S2S Port</td>
<td>Specifies the port used for XMPP S2S connections. Example: 5269</td>
</tr>
<tr>
<td>XMPP C2S ports</td>
<td>Specifies the port used for XMPP C2S connections. Example: 5222</td>
</tr>
<tr>
<td>SIP Certificate</td>
<td>The logical name of the certificate that the system uses for secure SIP communication. (Select from the list.)</td>
</tr>
<tr>
<td>Sesm LDAP Certificate</td>
<td>The logical name of the certificate that the AS 5300 Session Manager uses to communicate with the LDAP server. (Select from the list.)</td>
</tr>
<tr>
<td>Sesm XMPP Certificate</td>
<td>The logical name of the certificate that the AS 5300 Session Manager uses for secure XMPP communications. (Select from the list.)</td>
</tr>
</tbody>
</table>

**Note:**
Restart Session Manager after changing the Sesm XMPP certificate.

### Configuring the Master LSC functional role

**About this task**

Use the AS 5300 Element Manager Console to specify the AS 5300 Session Manager that functions as the Master Local Session Controller (LSC).

**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > ARTS Integration > Master LSC Profiles**.
2. On the Master LSC Profiles window, select the row that shows the Master LSC profile that you want to configure.

3. Click **Edit (-/+)**.

4. In the Edit Master LSC Profile dialog, configure the **Name**, **Call Control Agent ID**, **Enable ASAC**, **Primary Serving SS**, and **Secondary Serving SS** parameters.

5. Click **Apply**.

6. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Session Managers > <SESM instance> > ARTS Integration > Signalling Appliance Configuration**.

7. On the Signalling Appliance Configuration window, click **Add (+)**.

8. On the Add <SESM instance> Signaling Appliance Configuration dialog, in the **Name** field, type a name to identify the internal element.

9. From the **Profile** list, select the appropriate profile.

10. Click **Apply**.

---

### Configuring the Master LSC functional role job aid

**About this task**

The following table lists and describes the parameters used to configure the Master LSC Session Manager.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name for the internal element</td>
</tr>
<tr>
<td>CCA-ID</td>
<td>This string value specifies an ID to associate with an ASAC budget. Assign each SS and LSC Session Manager a unique CCA-ID. Default: blank</td>
</tr>
<tr>
<td>Type</td>
<td>This value (select from a list) is the functional role that the AS 5300 Session Manager performs. Values: Master LSC, LSC, SS, Default: LSC</td>
</tr>
<tr>
<td>Enable ASAC</td>
<td>This value (select from a list) specifies whether ASAC is enabled for the AS 5300 Session Manager. Values: true, false Default: false</td>
</tr>
<tr>
<td>Primary Serving SS</td>
<td>This value (select from the list of local and remote SSes) specifies the primary SS that serves the Master LSC.</td>
</tr>
<tr>
<td>Secondary Serving SS</td>
<td>This value (select from the list of local and remote SSes) specifies the backup SS to serve the Master LSC if the primary is down or unreachable.</td>
</tr>
</tbody>
</table>
Configuring the Slave LSC functional role

About this task
Use the AS 5300 Element Manager Console to specify an AS 5300 Session Manager that functions as a Slave Local Session Controller (LSC).

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > ARTS Integration > Slave LSC Profiles.
2. On the Slave LSC Profiles window, select the Slave LSC profile that you want to configure.
3. Click Edit (-/+).
4. In the Edit Slave LSC Profile dialog, configure the Name and Call Control Agent ID parameters.
5. Click Apply.
6. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Session Managers > <SESM instance> > ARTS Integration > Signalling Appliance Configuration.
7. On the Signalling Appliance Configuration window, click Add (+).
8. On the Add <SESM instance> Signaling Appliance Configuration dialog, in the Name field, type a name to identify the internal element.
9. From the Profile list, select the appropriate profile.
10. Click Apply.

Configuring the Slave LSC functional role job aid

About this task
The following table lists and describes the parameters used to configure an LSC Session Manager.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name for the internal element</td>
</tr>
<tr>
<td>CCA-ID</td>
<td>This string value specifies an ID to associate with an ASAC budget. Assign each SS and LSC Session Manager a unique CCA-ID. Default: blank</td>
</tr>
</tbody>
</table>
Configuring the SS functional role

About this task
Use the AS 5300 Element Manager Console to specify an AS 5300 Session Manager that functions as a soft switch (SS)

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > ARTS Integration > SS Profiles.
2. On the SS Profiles window, select the row that shows the SS profile that you want to configure.
3. Click Edit (-/+).
4. On the Edit SS Profile dialog, configure the Name, Call Control Agent ID, and Enable ASAC parameters.
5. From the Available ASAC Elements list, select the ASAC elements to assign, and then click >>.
6. Optional. To remove an assigned element, from the Assigned Elements list, select the element, and then click <<.
7. Click Apply.
8. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Session Managers > <SESM instance> > ARTS Integration > Signalling Appliance Configuration.
10. On the Add <SESM instance> Signaling Appliance Configuration dialog, in the Name field, type a name to identify the internal element.
11. From the Profile list, select the appropriate profile.
12. Click Apply

Configuring the SS functional role job aid

About this task
The following table lists and describes the parameters used to configure an SS Session Manager.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name for the internal element</td>
</tr>
<tr>
<td>CCA-ID</td>
<td>This string value specifies an ID to associate with an ASAC budget. Assign each SS and LSC Session Manager a unique CCA-ID. Default: blank</td>
</tr>
</tbody>
</table>

Table continues…
---

**Parameter** | **Description**  
--- | ---  
Enable ASAC | This value (select from a list) specifies whether ASAC is enabled for the AS 5300 Session Manager. Values: true, false  
Default: false  

---

### Moving the AS 5300 Session Manager network element instance

#### About this task

After moving the Session Manager network element (NE) to another server, you specify the new server for the NE instance.

⚠️ **Warning:**

This procedure is service-affecting. You must shut down the AS 5300 Session Manager to move it to another server.

⚠️ **Caution:**

Engineering parameters must not be modified in the field. Modifying the engineering parameters for a network element instance can reduce the performance and services of the network element.

The only appropriate modifications to an NE Instance are to the load during an upgrade, or to move the NE Instance to a different server.

#### Prerequisites

- You can access the AS 5300 Element Manager Console.
- You have NEService privileges.
- You have NEInstanceService privileges.
- You have EngParmService privileges.
- You are familiar with the procedures to start, stop, deploy, and undeploy a network element. For more information, see [Common procedures](#) on page 224.

#### Procedure

1. Stop the AS 5300 Session Manager instance on the original server.
2. Undeploy the AS 5300 Session Manager instance on the original server.
3. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Session Managers > [SESM instance] > Instance**
4. On the [SESM instance] Instance window, select the AS 5300 Session Manager instance to modify and click **Edit (-/+)**.
5. From the **Server** list, select the new server that hosts the AS 5300 Session Manager.

---

October 2017  
Avaya Aura® Application Server 5300 Configuration  
[Comments on this document? infodev@avaya.com](mailto:infodev@avaya.com)
6. Click **Apply**.
7. Deploy the AS 5300 Session Manager instance on the new server.
8. Start the AS 5300 Session Manager instance on the new server.
Chapter 15: Provisioning Manager configuration

About this task
This section provides the procedures that you perform to customize the Provisioning Manager default configuration.

Prerequisites
- You can access the AS 5300 Element Manager Console.

Navigation
- Configuring Provisioning Manager configuration parameters on page 127
- Configuring the whole Provisioning Manager network element on page 135
- Moving the Provisioning Manager network element instance on page 137
- Configuring Personal Agent parameters on page 138

Configuring Provisioning Manager configuration parameters

About this task
Perform this procedure to change the default configuration parameters for the Provisioning Manager, including Personal Agent parameters. You can modify configuration parameters while the network element is in service. Changes to these operating parameters apply to all network element instances of the network element and do not require a restart.

Before you begin
Ensure that:
- You can access the AS 5300 Element Manager Console.
- You have ConfigParmService privileges.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Provisioning Managers > <Provisioning Manager Instance> > Configuration Parameters.
2. In the Configuration Parameters window, from the **Parm Group** list, select a parameter group.
3. Select the parameter to modify and click **Edit (-/+)**.
4. In the Edit dialog box, enter a new value for the configuration parameter.
5. Click **Apply**.

The system validates the changes. If the changes are valid, the Edit Config Parm dialog closes and the configuration parameter updates.

---

**Configuring Provisioning Manager configuration parameters job aid**

**About this task**

This job aid lists the parameter groups and describes the configuration parameters for the Provisioning Manager.

<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Conf            | UrlPrefix              | This parameter defines the URL of the conference server for conferencing requests.  
|                 |                        | Default: sip:conference. |
| PasswordAudit   | EnableAudit            | This parameter enables Subscriber Password Expiry Audit, which runs once each day to check for expired subscriber passwords.  
|                 |                        | **Caution:**  
|                 |                        | If your system has more than one Provisioning Client, enable Subscriber Password Expiry Audit on only one Provisioning Client.  
|                 |                        | Range: true or false  
|                 |                        | Default: false  
|                 | AuditStartTime         | This parameter controls the time of day (in hours) at which Subscriber Password Expiry Audit runs. You must restart the Network Element Instance for changes to AuditStartTime to take effect.  
|                 |                        | Range: 0–23 (hours)  
| 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 |

Table continues…
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enable PA Manager DoS filter</td>
<td>This parameter enables or disables the HTTP Denial of Service protection feature for the Personal Agent Manager. Range: true or false Default: false</td>
</tr>
<tr>
<td></td>
<td>Enable Presence DoS filter</td>
<td>This parameter enables or disables the HTTP Denial of Service protection feature for Presence. Range: true or false Default: false</td>
</tr>
<tr>
<td></td>
<td>Enable Prov Manager DoS filter</td>
<td>This parameter enables or disables the HTTP Denial of Service protection feature for the Provisioning Manager. Range: true or false Default: false</td>
</tr>
<tr>
<td></td>
<td>Enable SOPI DoS filter</td>
<td>This parameter enables or disables the HTTP Denial of Service protection feature for Subscriber Open Provisioning Interface (SOPI). Range: true or false Default: false</td>
</tr>
<tr>
<td></td>
<td>Enable TPCC DoS filter</td>
<td>This parameter enables or disables the HTTP Denial of Service protection feature for Third Party Call Control. Range: true or false Default: false</td>
</tr>
<tr>
<td>HTTPConnector</td>
<td>ConnectionTimeout</td>
<td>This parameter controls the maximum number of seconds the HTTP Connector waits, after accepting a connection, for the request URI line to be presented. A value of 0 means no timeout. Default: 0</td>
</tr>
<tr>
<td></td>
<td>KeepAliveTimeout</td>
<td>This parameter controls the maximum number of seconds the HTTP Connector waits for another HTTP request before closing the connection. A value of 0 means no timeout. Default: 0</td>
</tr>
<tr>
<td>LDAP</td>
<td>AuditInterval</td>
<td>This parameter specifies the audit interval for LDAP servers. Range: 5–86 400</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MaxThreadCount</td>
<td>Maximum number of threads will be run during multiple multisite user add/delete operations. Range: 0-10</td>
</tr>
<tr>
<td></td>
<td>ThreadTimeOut</td>
<td>Idle timeout value in minutes for threads those run during multiple multisite user add/delete operations. Range: 10-60 minutes</td>
</tr>
<tr>
<td></td>
<td>TimeToLiveUnreliable</td>
<td>Expiration time of LDAP lookups stored in the iMLDAPAddrLookupTable that are marked as unreliable. Range: 0–10 000 seconds Default: 300 seconds</td>
</tr>
<tr>
<td>Login</td>
<td>EnableLastLoginDisplay</td>
<td>This parameter enables or disables the display of the Last Login information. Range: true, false</td>
</tr>
<tr>
<td>OM</td>
<td>OfficeTransferPeriod</td>
<td>This parameter specifies the Fault Performance Manager polling period, in minutes. Range: 5, 15, 30, or 60 Default: 15</td>
</tr>
<tr>
<td>PCAUserAgent</td>
<td>CtcCancelDelay</td>
<td>This parameter defines the click-to-call cancel delay value, in seconds. Range: 6–60 Default: 18</td>
</tr>
<tr>
<td></td>
<td>CtcPacketTime</td>
<td>This parameter defines the click-to-call packet time value, in seconds. Range: 10–60 Default: 30</td>
</tr>
<tr>
<td>PersonalAgent</td>
<td>GenerateAuditLogs</td>
<td>This parameter enables or disables the generation of Audit Logs for the Personal Agent and Subscriber Open Provisioning Interface (OPI). Range: true, false</td>
</tr>
<tr>
<td></td>
<td>MaxUserPictureSize</td>
<td>This parameter defines the maximum size for a user’s picture, in kilobytes. Range: 8–200 Default: 24</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 |
| SIPRespOM– Thresh| Info 500                  | This parameter indicates how many 500 error responses can be received for SIP Refer Requests before an alarm is raised.  
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.  
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.  
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.  
Default: 5,10,15 |
|                 | Option500                  | This parameter indicates how many 500 error responses can be received for SIP Option Requests before an alarm is raised.  
Default: 5,10,15 |
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publish500</td>
<td>This parameter indicates how many 500 error responses can be received for SIP Publish Requests before an alarm is raised.</td>
<td>Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15</td>
</tr>
<tr>
<td>Refer500</td>
<td>This parameter indicates how many 500 error responses can be received for SIP Refer Requests before an alarm is raised.</td>
<td>Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15</td>
</tr>
<tr>
<td>Register500</td>
<td>This parameter indicates how many 500 error responses can be received for SIP Register Requests before an alarm is raised.</td>
<td>Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15</td>
</tr>
<tr>
<td>Subscribe500</td>
<td>This parameter indicates how many 500 error responses can be received for SIP Subscribe Requests before an alarm is raised.</td>
<td>Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15</td>
</tr>
<tr>
<td>Update500</td>
<td>This parameter indicates how many 500 error responses can be received for SIP Update Requests before an alarm is raised.</td>
<td>Range: Minor alarm: 1–98 Major alarm: 2–99 Critical alarm: 3–100 Default: 5,10,15</td>
</tr>
<tr>
<td>SipTransport</td>
<td>InitialMaxHops</td>
<td>This parameter defines the maximum number of hops before a request is dropped.</td>
</tr>
<tr>
<td></td>
<td>InviteTimer</td>
<td>This parameter defines the maximum time to wait for an INVITE to receive a Final Response, after receiving a provisional response, in seconds.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
|                 | 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                                                               |
| TLSAuth         | EnableOCSP                   | This parameter enables OCSP retrieval for certificate revocation status.      |
|                 |                               | Range: true or false                                                        |
|                 |                               | Default: false                                                               |
| TLSAuth         | EnforceTLSMutual-AuthForHTTPS | This parameter enforces TLS Mutual Authentication for HTTP interface.       |
|                 |                               | Range: true or false                                                        |
|                 |                               | Default: false                                                               |
| TLSAuth         | EnforceTLSMutual-AuthForSIP   | This parameter enforces TLS Mutual Authentication for SIP interface.        |
|                 |                               | Range: true or false                                                        |
|                 |                               | Default: false                                                               |
| TLSAuth         | PermitIfNoRevocationValidateResp | This parameter permits access, if no certificate revocation validation response.  
|                 |                               | Range: true or false                                                        |
|                 |                               | Default: true                                                                |
| TLSAuth         | SyncOCSPForSIP               | This parameter enables synchronous OCSP query for SIP interface.            |
|                 |                               | Range: true or false                                                        |
|                 |                               | Default: false                                                               |
| TLSSession      | AllowTLSsessionresumption     | This parameter enables or disables TLS session resumption.                   |
|                 |                               | Range: true, false                                                           |

Table continues…
<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enforce renegotiation</td>
<td>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</td>
</tr>
<tr>
<td>WebClient</td>
<td>AudioRTPPort</td>
<td>This parameter defines the starting port address for RTP streams. Range: 0–65 535 Default: 50 000</td>
</tr>
<tr>
<td></td>
<td>AudioRTPPortRange</td>
<td>This parameter defines a range for the number of ports that can be used for RTP streams. Range: 1–10 000 Default: 100</td>
</tr>
<tr>
<td></td>
<td>ConnectionTimeout</td>
<td>This parameter defines how long the Provisioning Manager attempts to retry connecting to an AS 5300 Web Client before considering the connection timed out, in seconds. Range: 90–3600 Default: 360</td>
</tr>
<tr>
<td></td>
<td>PingInterval</td>
<td>This parameter determines the interval for pinging the Web client, in seconds. Range: 1–1200 Default: 120</td>
</tr>
<tr>
<td></td>
<td>PingTimeout</td>
<td>This parameter determines how long the Provisioning Manager waits for a ping response from the AS 5300 Web Client before considering the ping timed out, in seconds. Range: 1–3600 Default: 60</td>
</tr>
<tr>
<td></td>
<td>UseSSL</td>
<td>This parameter determines if the socket used to communicate with the AS 5300 Web Client uses Secure Sockets Layer technology. Range: true or false Default: false</td>
</tr>
<tr>
<td>WebServer</td>
<td>EnableAccessLogs</td>
<td>This parameter enables Tomcat Access/Error logs. Range: true, false</td>
</tr>
</tbody>
</table>

Table continues…
### Configuring the whole Provisioning Manager network element

**About this task**

You can modify many options that are specific to each network element type, such as the base port of a network element application, or you can associate a different Fault Performance Manager with the network element.

For information about how to configure the AS 5300 Session Manager for a FIPS-compliant system, see *Avaya Aura® Application Server 5300 Security, NN42040-601*.

**Prerequisites**

- You can access the AS 5300 Element Manager Console.
- You have NEService privileges.
- You are familiar with the procedure to restart a network element. See [Restarting a network element](#).

**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Provisioning Managers**.
2. In the Provisioning Managers window, select the entry for the network element to modify and click **Edit (-/+)**.

### Parameter group

<table>
<thead>
<tr>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RequestUserAvatar</td>
<td>This parameter enables or disables user avatar download from remote XMPP servers. Range: true or false Default: true</td>
</tr>
<tr>
<td>AvatarRequestTimeout</td>
<td>This parameter specifies number of seconds the server waits for response for user avatar request. Range: 5-60 Default: 15</td>
</tr>
<tr>
<td>EnableAudit</td>
<td>This parameter enables monitoring for Admin accounts. Range: true or false Default: false</td>
</tr>
<tr>
<td>AuditStartTime</td>
<td>This parameter controls the time of day at which the system audits Admin accounts. Range: 0–23 hours Default: 0</td>
</tr>
</tbody>
</table>

**Important:**

Systems that do not use TLS and SRTP use UDP and RTP. The Audiocodes Mediant 3000 does not support best effort RTP/SRTP (mixed-mode). The configuration for all endpoints must be either secure or nonsecure for media.

4. Click **Apply**.

5. Restart the Provisioning Manager network element.

---

### Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Provisioning Manager instance&gt;</td>
<td>This value is the name of the Provisioning Manager, such as PROV1.</td>
</tr>
</tbody>
</table>

### Configuring the whole Provisioning Manager network element job aid

#### About this task

This job aid lists and describes the fields on the Edit <Provisioning Manager instance> dialog box.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Name</td>
<td>(Read-only) The short name of the NE—maximum of 6 characters.</td>
</tr>
<tr>
<td>Long Name</td>
<td>The long name of the NE—maximum of 32 characters.</td>
</tr>
<tr>
<td>Base Port</td>
<td>A range of 100 ports reserved off the base port for use by the NE. Range: 1100–654000</td>
</tr>
<tr>
<td>FPM</td>
<td>The FPM used by the NE.</td>
</tr>
<tr>
<td>Enable HTTP Port</td>
<td>(Check box) Select to enable the Provisioning HTTP port.</td>
</tr>
<tr>
<td>Internal OAM Certificate</td>
<td>The private key and certificate pair for the Provisioning HTTPS server.</td>
</tr>
<tr>
<td>External OAM Certificate</td>
<td>The private key and certificate pair for the Provisioning HTTPS server (external interface).</td>
</tr>
<tr>
<td>LDAP Certificate</td>
<td>The logical name of the certificate used for communication between the Provisioning Manager and the LDAP server.</td>
</tr>
<tr>
<td>Enable HTTP Port</td>
<td>(Check box) Select to enable the Personal Agent HTTP port.</td>
</tr>
</tbody>
</table>

*Table continues...*
### Parameter | Description
--- | ---
HTTPS Certificate | The private key and certificate pair that the Personal Agent HTTPS server uses. (Select from the list.)
Enable SIP UDP Port | (Check box) Select to enable the SIP UDP port. Default: 5060
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.)
XMPP Certificate | The logical name of the certificate that the system uses for XMPP communication

---

## Moving the Provisioning Manager network element instance

### About this task

After moving the Provisioning Manager network element (NE) to another server, you must specify the new server for the NE instance.

⚠️ **Warning:**

This procedure is service-affecting. You must shut down the Provisioning Manager to move it to another server.

⚠️ **Caution:**

Engineering parameters must not be modified in the field. Modifying the engineering parameters for a network element instance can reduce the performance and services of the network element.

The only appropriate modifications to an NE Instance are to the load during an upgrade, or to move the NE Instance to a different server.

### Prerequisites

- You can access the AS 5300 Element Manager Console.
- You have NEService privileges.
- You have NEInstanceService privileges.
- You have EngParmService privileges.
- You are familiar with the procedures to start, stop, deploy, and undeploy a network element. For more information, see [Common procedures](#) on page 224.

### Procedure

1. Stop the AS 5300 Session Manager instance on the original server.
2. Undeploy the AS 5300 Session Manager instance on the original server.
3. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Provisioning Managers > <Provisioning Manager Instance> > Instance**.

4. On the Provisioning Manager Instance window, select the Provisioning Manager instance to modify and click **Edit (-/+)**.

5. From the **Server** list, select the server that hosts the Provisioning Manager.

6. Click **Apply**.

7. Deploy the AS 5300 Session Manager instance on the new server.

8. Start the AS 5300 Session Manager instance on the new server.

---

**Configuring Personal Agent parameters**

**About this task**

Use this procedure to configure Personal Agent.

**Procedure**

1. Select **Network Elements > Provisioning Managers > <Provisioning Manager instance> > Configuration Parameters**.

2. Select **Personal Agent** from the Parm Group list.

3. Select **MaxUserPictureSize** and then click **Edit (-/+)**.

4. On the Edit dialog, in the **Value** box, type a value between 8 and 200 (the number of KB), and then click **Apply**.

---

**Configuring Personal Agent parameters job aid**

The following provides additional information about Personal Agent parameters.

Calls that terminate to an AS 5300 UC Client can roll over to a voice mail system. Two options are available to the operator:

- Application Server 5300 users are routed to an Application Server 5300-based voice mail system.

Avaya recommends Application Server 5300-based voice mail. With Application Server 5300-based voice mail, the Personal Agent can search the user's other terminating devices before rolling over to voice mail. This configuration can require additional resources because the switching system sends all calls to the Application Server 5300 so that voice mail can be handled.

If the Application Server 5300 hosts the voice messaging system, the AS 5300 UC Client provides a voice mail indicator. The voice mail icon flashes when a new unread message is in the Inbox and remains flashing until the user retrieves the message. Note that the system does not provide the Voice Mail Waiting Indicator if voice mail is not hosted by the Application Server 5300.
Chapter 16: Avaya Media Server configuration

Use the information in this chapter to add Avaya Media Server (MS) and to configure Avaya MS clusters.

Navigation

- **Avaya MS cluster configuration** on page 139
- **Configuring Avaya Media Server configuration parameters** on page 146
- **Configuring audio and video CODECs** on page 148
- **Adding an Avaya MS license key** on page 151
- **Locking the Avaya MS** on page 151
- **Configuring QoS DSCP** on page 152
- **Configuring Media Ports** on page 153
- **Configuring Avaya MS Media Security** on page 155
- **Configuring DTMF** on page 154
- **Configuring Application Restrictions** on page 157
- **Configuring IP Traffic on** on page 157
- **Applying QFE patches** on page 158
- **Removing QFE patches** on page 160

---

**Avaya MS cluster configuration**

An Avaya MS cluster is a collection of Avaya MS nodes that work closely together, and can be treated as a single node. An Avaya MS cluster must contain at least one primary MS server. Optionally, you can add secondary or standard Avaya MS servers, to a maximum of eight servers in a cluster. An Avaya MS cluster shares a Simple Network Time Protocol (SNTP) server for clock synchronization, persistent content storage, and controller peer ring.

Use the information in this section to configure Avaya MS clusters.
Adding an Avaya Media Server on page 140
Creating an Avaya MS cluster on page 142
Adding an Avaya MS SIP Route on page 144
Configuring database replication on page 143

Adding an Avaya Media Server

About this task
When you install the Avaya MS, MS1 is automatically added, and uses port 15100. Use this procedure to add MS2.
Prerequisite: Install the Avaya MS.
Procedure

1. In the Configuration view of the AS 5300 Element Manager Console, navigate to Network Elements > Media Servers and Clusters > Media Servers.

2. Click Add (+).

3. Configure parameters as required.

4. Click Apply.

5. In the configuration view of the AS 5300 Element Manager Console, click Network Elements > Media Servers and Cluster > Media Servers > <server name> > Instance.

6. In the<server name> Instance window, click Add (+) to add an instance of this network element and associate the instance with a server.

7. In the Add <server name> Instance dialog box, use the menus to associate a server, a software load, and an engineering profile with the instance.

   The engineering profile controls the initial size of the Java Virtual Machine and establishes engineering parameters appropriate for the hardware capabilities of the server.

8. Click Apply.

9. In the Configuration view of the AS 5300 Element Manager Console, click Network Elements > Media Servers and Cluster > Media Servers > NE Maintenance.

10. In the Maintenance panel, select MS1 and click Deploy.

11. In the Maintenance panel, select MS2 and click Deploy.

12. Click Apply.

Adding an Avaya MS job aid

About this task

The following table lists and describes the Avaya MS configuration parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ShortName</td>
<td>Enter a short name to identify the Media Server.</td>
</tr>
<tr>
<td></td>
<td>Maximum: 6 alphanumeric characters. Example: MS1, MS2.</td>
</tr>
<tr>
<td>LongName</td>
<td>Enter a descriptive name to identify the Media Server.</td>
</tr>
<tr>
<td></td>
<td>Maximum: 32 alphanumeric characters</td>
</tr>
<tr>
<td>Base Port</td>
<td>Enter the port the Media Server uses. A numeric value from 1–65 535</td>
</tr>
<tr>
<td>FPM</td>
<td>From the list, select the Fault Performance Manager.</td>
</tr>
<tr>
<td>Enable SIP UDP /</td>
<td>Select the checkbox to enable SIP UDP, and enter a value for the UDP Port.</td>
</tr>
<tr>
<td>SIP UDP Port</td>
<td></td>
</tr>
</tbody>
</table>

Table continues…
### Creating an Avaya MS cluster

**About this task**

Use this procedure to create an Avaya MS cluster.

Prerequisite: Make sure that one or more Avaya MS servers is configured and available.

**Procedure**

1. In the AS 5300 Element Manager Console, navigate to **Network Elements > Media Servers and Clusters > Media Server Clusters**
2. Click **Add (+)** to add a new Cluster.
3. Configure parameters as required.
4. Click **Apply**.

### Creating an Avaya MS cluster job aid

**About this task**

The following table lists and describes the Avaya MS cluster configuration parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ShortName</td>
<td>Enter a short name to identify the cluster. Maximum: 6 alphanumeric characters. Example: C1, C2.</td>
</tr>
<tr>
<td>LongName</td>
<td>Enter a descriptive name to identify the cluster. Maximum: 32 alphanumeric characters</td>
</tr>
<tr>
<td>Primary Server</td>
<td>From the list, choose the Primary Media Server for the cluster.</td>
</tr>
<tr>
<td>Secondary Server</td>
<td>(Optional) From the list, choose the Secondary Media Server for the cluster.</td>
</tr>
<tr>
<td>Standard Server</td>
<td>Perform this step only if you chose a Secondary Media Server in the previous step. (Optional) From the list, select a Standard Media Server for the cluster and click &gt;&gt; to move the server to the Used list.</td>
</tr>
</tbody>
</table>
Configuring database replication

About this task

Use this procedure to configure database replication for Avaya MS clusters.

Procedure

1. In the configuration view of the AS 5300 Element Manager Console, click **Network Elements > Media Servers and Clusters > Media Server Clusters > <clustename> > Replication Settings**.
2. Select **Enable Replication Account**.
3. Enter the **User Name**, **Password**, and **Confirm** the password of the Replication Account.
4. Click **Apply**.

Configuring database replication job aid

About this task

This job aid lists the parameters for the database replication account.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Enter the user name for the replication account.</td>
</tr>
</tbody>
</table>
| Password          | Enter the password for the replication account.  
                    The replication account password is protected by the following rules, which are controlled by the same parameters that control admin accounts on the AS 5300 Element Manager and Provisioning Client:  
                    • Minimum password length  
                    • Minimum lowercase characters  
                    • Minimum uppercase characters  
                    • Minimum digits  
                    • Minimum special characters  
                    • Maximum consecutive characters  
                    • User ID or reversed user ID permitted in password  
                    • Check for dictionary words in passwords  
                    For more information about these password rules, or to configure them, see *Avaya Aura® Application Server 5300 Security, NN42040-601*. |
| Confirm password  | Reenter the password for the replication account. |
Adding an Avaya MS SIP Route

About this task
Use this procedure to add a SIP Route for Avaya MS clusters.

Procedure
1. In the configuration view of the AS 5300 Element Manager Console, click **Network Elements > Media Servers and Clusters > Media Server Clusters > <clustername> > SIP Routes**.
2. Click +, and configure parameters as required.
3. Click **Apply**.

Adding an Avaya MS SIP Route job aid

About this task
This job aid lists the parameters for SIP Routes.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Node</td>
<td>Select the SIP node (sessMgr NE) from the list.</td>
</tr>
<tr>
<td>Served Domain</td>
<td>Enter the domain this route serves. Enter * to serve all domains.</td>
</tr>
<tr>
<td>SIP Transport</td>
<td>Select the SIP transport from the list.</td>
</tr>
<tr>
<td>priority</td>
<td>Enter the priority value for the route. The default value is 0. The range is from 0 to 65535 with the lowest value having the highest priority. The highest priority routes, which have lower values, are selected first.</td>
</tr>
<tr>
<td>weight</td>
<td>Enter the weight value for the route. The default is 10. The range is 0 to 65535. Weight is used to select routes within the same priority level.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select to enable a SIP route. Typically, routes are enabled; however, you can clear this check box to temporarily disable a route.</td>
</tr>
<tr>
<td>Proxy</td>
<td>Select to assign a proxy server role to this route. A SIP proxy server accepts Avaya MS requests and queries the SIP registrar server to obtain recipient addressing information.</td>
</tr>
<tr>
<td>IM Proxy</td>
<td>This is an advanced option; Avaya recommends that you use the default value.</td>
</tr>
<tr>
<td>Registrar</td>
<td>Select to assign a registrar server role to this route. A SIP registrar server is a database that contains the location of all user agents within a domain.</td>
</tr>
</tbody>
</table>
Managing Avaya MS SIP Routes

About this task
Use this procedure to add, modify, or delete SIP Routes for Avaya MS clusters.

Procedure
1. In the configuration view of the AS 5300 Element Manager Console, click **Network Elements > Media Servers and Clusters > Media Server Clusters > <clustername> > SIP Routes.**
2. Optionally, click **+** to add a route, and configure parameters as required.
3. Optionally, select a route from the list, click **–/+** to modify the route, and configure parameters as required.
4. Optionally, select a route from the list, and click **–** to delete a route.
5. Click **Apply.**

Managing Avaya MS SIP Routes job aid

About this task
This job aid lists the parameters for SIP Routes.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Node</td>
<td>Select the SIP node (sessMgr NE) from the list.</td>
</tr>
<tr>
<td>Served Domain</td>
<td>Enter the domain this route serves. Enter star (*) to serve all domains.</td>
</tr>
<tr>
<td>SIP Transport</td>
<td>Select the SIP transport from the list.</td>
</tr>
<tr>
<td>priority</td>
<td>Enter the priority value for the route. The default value is 0. The range is from 0 to 65535 with the lowest value having the highest priority. The highest priority routes, which have lower values, are selected first.</td>
</tr>
<tr>
<td>weight</td>
<td>Enter the weight value for the route. The default is 10. The range is 0 to 65535. Weight is used to select routes within the same priority level.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select to enable a SIP route. Typically, routes are enabled; however, you can clear this check box to temporarily disable a route.</td>
</tr>
<tr>
<td>Proxy</td>
<td>Select to assign a proxy server role to this route. A SIP proxy server accepts Avaya MS requests and queries the SIP registrar server to obtain recipient addressing information.</td>
</tr>
<tr>
<td>IM Proxy</td>
<td>This is an advanced option; Avaya recommends that you use the default value.</td>
</tr>
<tr>
<td>Registrar</td>
<td>Select to assign a registrar server role to this route. A SIP registrar server is a database that contains the location of all user agents within a domain.</td>
</tr>
</tbody>
</table>
Configuring Avaya Media Server configuration parameters

About this task
Perform this procedure to change the default configuration parameters for the Avaya Media Server network element. You can modify configuration parameters while the network element is in service. Changes to these operating parameters apply to all network element instances of the network element and do not require a restart.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have ConfigParmService privileges.

Procedure
1. From the configuration view of the console, select **Network Elements > Media Servers and Clusters > Media Servers > <your Avaya MS server> > Configuration Parameters**.
2. In the Configuration Parameters dialog box, from the **Parm Group** list, select a parameter group.
3. Select the parameter to modify and click **Edit (-/+)**.
4. In the Edit dialog box, select a new value for the configuration parameter.
5. Click **Apply**.

   The system validates the new value. If the value is valid, the Edit Config Parm dialog closes and the configuration parameter updates.

Configuring Avaya Media Server configuration parameters job aid

About this task
This job aid lists the parameter groups and describes the configuration parameters for the Avaya MS network element.

<table>
<thead>
<tr>
<th>Parameter group</th>
<th>Configuration parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS</td>
<td>MSServiceStatusPollInterval</td>
<td>This parameter controls how often the system polls the Avaya MS service status. In the range of 1 to 300. Default: 30</td>
</tr>
<tr>
<td>MSDBConf</td>
<td>AcquireRetryAttempts</td>
<td>This parameter controls how many times the system attempts to reconnect to the Avaya MS database. In the range of 0 to 2147483647. Default: 5</td>
</tr>
<tr>
<td></td>
<td>AcquireRetryDelay</td>
<td>This parameter controls how long the system waits before attempting to reconnect to the Avaya MS database. In the range of 1000 to 3600000.</td>
</tr>
<tr>
<td>Parameter group</td>
<td>Configuration parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Port</td>
<td>Default: 5000. This parameter controls the port the system uses to connect to the Avaya MS database. In the range of 1025 to 65535.</td>
</tr>
<tr>
<td>OM</td>
<td>OfficeTransferPeriod</td>
<td>Default: 15. This parameter controls Transfer Period.</td>
</tr>
<tr>
<td>TLSAuth</td>
<td>EnableCRL</td>
<td>Default: false. This parameter enables CRL retrieval for certificate revocation status.</td>
</tr>
<tr>
<td></td>
<td>EnableOCSP</td>
<td>Default: false. This parameter enables OCSP retrieval for certificate revocation status.</td>
</tr>
<tr>
<td></td>
<td>EnableTCPTLSTransport</td>
<td>Default: false. This parameter enables TLS for all external TCP connections.</td>
</tr>
<tr>
<td></td>
<td>EnforceTLSMutualAuthForHTTPS</td>
<td>Default: false. This parameter enforces TLS Mutual Authentication for HTTP interface.</td>
</tr>
<tr>
<td></td>
<td>EnforceTLSMutualAuthForSIP</td>
<td>Default: false. This parameter enforces TLS Mutual Authentication for SIP interface.</td>
</tr>
<tr>
<td></td>
<td>OCSPPermitNoResponse</td>
<td>Default: true. Allows TLS network connections when no OCSP response is received.</td>
</tr>
<tr>
<td></td>
<td>PermitIfNoRevocationValidateResp</td>
<td>Default: true. This parameter permits access, if no certificate revocation validation response.</td>
</tr>
<tr>
<td></td>
<td>SyncOCSPForSIP</td>
<td>Default: false. This parameter enables synchronous OCSP query for SIP interface.</td>
</tr>
<tr>
<td></td>
<td>TCPTLSSessionRenegotiation</td>
<td>Default: false. This parameter enables TCP TLS Session Renegotiation.</td>
</tr>
<tr>
<td>Media Preferences</td>
<td>LocalOffers</td>
<td>Default: IPv4 Preferred. The parameter controls the preferred IP address form for local offers. Accepted values are: IPv4 Preferred, IPv6 Preferred.</td>
</tr>
</tbody>
</table>

Table continues…
### Configuring audio and video CODECs

Configure the audio and video CODECs for the Avaya MS to allow the Avaya MS to compress and decompress audio and video data streams.

- Enabling and configuring audio CODEC settings on page 148
- Removing an audio CODEC on page 149
- Enabling and configuring video CODEC settings on page 149
- Removing a video CODEC on page 150

### Enabling and configuring audio CODEC settings

**About this task**

Use this procedure to enable and configure the audio CODECs supported on the server. The supported audio CODECs are G.722, G.729A, G.711–ALAW, and G.711–ULAW.

**Procedure**

1. In the Configuration view of the AS 5300 Element Manager Console, navigate to Network Elements > Media Servers and Clusters > Media Server Clusters > <clusternamex> > Audio Codec Settings.
2. To enable a CODEC on the Audio Codecs page, select the audio CODEC from the Available list.
3. Click >> to move the CODEC to the Enabled list.
4. To change the priority of a CODEC in the Enabled list, select the CODEC and click Up or Down to move the CODEC within the list.
5. For each CODEC that you add, select the PTimes (packet times).
6. Repeat step 2 through step 5 for each audio CODEC that you want to enable.
7. Click Apply.
Enabling and configuring Audio CODEC settings job aid

About this task

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>The list of available (but not enabled) audio CODECs currently installed on the network. The Avaya MS supports the following audio CODECs: G.722, G.711-ALAW, G.711-ULAW, and G.729A.</td>
</tr>
<tr>
<td>Enabled</td>
<td>The list of audio CODECs currently active on the network.</td>
</tr>
<tr>
<td>PTimes</td>
<td>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 EVRC-0 audio CODEC is available only with a 20 ms PTime. The default PTime is 20 ms.</td>
</tr>
</tbody>
</table>

Removing an audio CODEC

About this task

Use this procedure to remove an audio CODEC to withdraw support for the audio CODEC on the server.

Procedure

1. In the Configuration view of the AS 5300 Element Manager Console, navigate to Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <cluster name> > Audio Codec Settings.
2. Select the audio CODEC from the Enabled list.
3. Click << to move the CODEC to the Available list.
4. Click Apply.

Enabling and configuring video CODEC settings

About this task

Use this procedure to enable and configure the video CODECs supported on the server.

Procedure

1. In the Configuration view of the AS 5300 Element Manager Console, navigate to Network Elements > Media Servers and Clusters > Media Server Clusters > <clustername> > Video Codec Settings.
2. To enable a CODEC on the Video Codec Settings window, select the video CODEC from the Available list and click >> to move the CODEC to the Enabled list.
3. To change the priority of a CODEC in the **Enabled** list, select the CODEC and click **Up** or **Down** to move the CODEC within the list.

4. For each CODEC that you add, configure the **Frame Rates** parameters.

5. Repeat step 2 through step 5 for each video CODEC that you want to enable.

6. Click **Apply**.

### Enabling and configuring video CODEC settings job aid

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>The list of available (but not enabled) video CODECs currently installed on the network. The Avaya MS supports the following video CODECs: H.263++, H.263+, H.263, H264, and NNVC.</td>
</tr>
<tr>
<td>Enabled</td>
<td>The list of video CODECs currently active on the network.</td>
</tr>
<tr>
<td>Frame Rates</td>
<td>Select the allowed Frame Rates for the CODECs enabled.</td>
</tr>
<tr>
<td>Default</td>
<td>Select the desired Default Frame Rate for the CODECs enabled.</td>
</tr>
<tr>
<td>Format</td>
<td>Select the Preferred Format for the CODECs enabled.</td>
</tr>
<tr>
<td>Annex</td>
<td>Select the Annex Profile for the CODECs enabled.</td>
</tr>
<tr>
<td>Enforce Annex X</td>
<td>Select Enforce Annex X Profiles to enforce only the prescribed sets of annexes, as described in the annex X profile list, to be accepted by Avaya MS.</td>
</tr>
</tbody>
</table>

### Removing a video CODEC

**About this task**

Use this procedure to remove a video CODEC to withdraw support for the video CODEC on the server.

**Procedure**

1. In the Configuration view of the AS 5300 Element Manager Console, navigate to **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <cluster name> > Video Codec Settings**.

2. Select the video CODEC from the **Enabled** list.

3. Click **<<** to move the CODEC to the **Available** list.

4. Click **Apply**.
Adding an Avaya MS license key

About this task

Use this procedure to add a license key to the Avaya MS, thereby enabling services on the Avaya MS.

Prerequisites:

- Install the Avaya MS.
- Obtain a license key through the ordering system.

Procedure

1. In the Configuration view of the AS 5300 Element Manager Console navigate to Network Elements > Media Servers and Clusters > Media Servers > <server name> > License key.

2. In the <server name> License key window, paste the license key.

3. Click Apply.

4. Click OK.

5. Restart the Media Server network element.

Adding an Avaya MS license key job aid

About this task

Parameter | Description
--- | ---
License key | In this field, paste the license key for the Avaya MS.

Locking the Avaya MS

About this task

Use this procedure to lock the Avaya MS. If you lock the Avaya MS, all active sessions (existing calls) are terminated and no new requests are allowed.

When the system enters a locked state, existing sessions are terminated and the system redirects new traffic. You typically place the system into a Locked state when performing maintenance.

Prerequisite: Access the AS 5300 Element Manager Console.

Procedure

1. In the navigation pane, click Network Elements > Media Servers and Clusters > Media Servers > <server name> > Service Maintenance.

2. Click Lock.
3. Click **Yes** to confirm.

---

**Locking an Avaya MS with a pending lock**

**About this task**

Use the Pending Lock option to lock the Avaya MS, while allowing all active sessions (existing calls) to finish, but preventing new sessions. The Avaya MS is locked after all active sessions are completed.

Prerequisite: Access the AS 5300 Element Manager Console.

**Procedure**

1. In the navigation pane, click **Network Elements > Media Servers and Clusters > Media Servers > <server name> > Service Maintenance.**
2. Click **Pending Lock.** If a lock is already pending, the Pending Lock option is not available.
3. Click **Yes** to confirm.

---

**Unlocking an Avaya MS**

**About this task**

Use this procedure to unlock the Avaya MS. If the Avaya MS is locked, no applications or services can function. Normal call processing is performed after the system is unlocked.

**Prerequisites**

- Access the AS 5300 Element Manager Console.
- You can unlock the Avaya MS only if it is locked or pending locked.

**Procedure**

1. In the navigation pane, click **Network Elements > Media Servers and Clusters > Media Servers > <server name> > Service Maintenance.**
2. Click **Unlock.**
   
   If the Avaya MS is not locked, the Unlock option does not appear.

---

**Configuring QoS DSCP**

**About this task**

Use this procedure to configure Quality of Service (QoS) values for SIP, audio, and video streaming.
Procedure

1. In the Configuration view of the AS 5300 Element Manager Console, navigate to **Network Elements > Media Servers and Clusters > Media Server Clusters > <cluster name> > DSCP Settings**.
2. On the DSCP Settings page, enter a value in each field.
3. Click **Apply**.
4. Click **OK**.
5. Restart all Avaya MS network elements in the current cluster.

---

### Configuring QoS DSCP job aid

**About this task**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP QoS DSCP</td>
<td>The percentage of available bandwidth to reserve for SIP signalling. Valid range is 0–63.</td>
</tr>
<tr>
<td>Audio QoS DSCP</td>
<td>The percentage of available bandwidth to reserve for audio streaming. Valid range is 0–63.</td>
</tr>
<tr>
<td>Video QoS DSCP</td>
<td>The percentage of available bandwidth to reserve video streaming. Valid range is 0–63.</td>
</tr>
</tbody>
</table>

---

### Configuring Media Ports

**About this task**

Use the following procedure to configure the ports used for audio, video, and conferencing sessions.

**Procedure**

1. In the Configuration view of the AS 5300 Element Manager Console, navigate to **Network Elements > Media Servers and Clusters > Media Server Clusters > <cluster name> > Media Ports Settings**.
2. Configure parameters as required.
3. Click **Apply**.
Configuring Media Ports job aid

About this task

The following table lists and describes the Media Port configuration parameters. These parameters control the ports used by audio, video, and conference calls.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Port</td>
<td>The starting port for the media port range (two ports are used for each session). If you change this value you must restart the server for the change to take effect. This value corresponds to the AUDIO_START_PORT in the Avaya MS database. The default value is 6000. The range is between 6000 and 13998.</td>
</tr>
<tr>
<td>End Port</td>
<td>The end port for the media port range. If you change this value you must restart the server for the change to take effect. This value corresponds to the CONFERENCE_MAX_PORT in the Avaya MS database. The default value is 32598. The range is 14000 to 32598.</td>
</tr>
</tbody>
</table>

The Start Port and End Port values control the ports used by audio, video, and conference calls, which are divided as follows:

- 70% or the ports are used for conferencing.
- 30% of the ports are used for Interactive Voice Response (IVR).

⚠️ Note:

You must provide a total of at least 11500 ports, 8000 of which must be conference ports. Ensure that an even number of ports is reserved for conferencing, as two ports are used for each conferencing session.

Configuring DTMF

About this task

Use this procedure to configure Dual-Tone Multi-Frequency (DTMF) digit relay. The following DTMF relay methods are supported:

- INFO digits
- RFC2833/4733

Procedure

1. In the navigation pane, click Network Elements > Media Servers and Clusters > Media Server Clusters > <cluster> > Digit Relay (DTMF).
2. Enable or disable DTMF relay methods by selecting one of the methods in the Available or Enabled lists, and clicking >> or <<.
3. Configure the order of DTMF relay methods by selecting one of the enabled methods, and clicking **Up** or **Down**.

4. Optionally, configure the RFC2833 format type.

---

### Configuring DTMF job aid

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign RFC 2833 Format Type</td>
<td>Enable this option to dynamically assign the format type for RFC 2833. When this option is disabled, the value you enter in the Specify Type field is used. Default: Enabled</td>
</tr>
<tr>
<td>Specify Type</td>
<td>Enter the Format type to be used by RFC 2833. This parameter applies only when Assign RFC 2833 Format Type Dynamically is disabled. Default: None</td>
</tr>
</tbody>
</table>

---

### Configuring Avaya MS Media Security

**About this task**

Use this procedure to configure the media security policy to use for Session Description Protocol (SDP) negotiation.

The media security feature provides the ability to secure media streams with cryptographic protection based on the Secure Real-time Transport Protocol (SRTP). SRTP is a Real-time Transport Protocol (RTP) profile with symmetrical data encryption that provides the following security services: encryption, message integrity, and replay protection.

Secure Real-time Transport Control Protocol (SRTCP) provides encryption, message integrity, and replay protection to RTCP. SRTCP message authentication protects the RTCP fields that keep track of membership, provide feedback to RTP sends, or maintain packet sequence counters.

**Procedure**

1. In the Configuration view of the AS 5300 Element Manager Console, navigate to **Network Elements > Media Servers and Clusters > Media Server Clusters > <cluster name> > SRTP Settings**.
2. In the **Security Policy** list, select a policy.
3. If you selected the Best Effort policy, in the **Best Effort Mode** list, select a mode.
4. In the **Crypto Suites** section, configure parameters as required.
5. Click **Apply**.
## Configuring Avaya MS Media Security job aid

### About this task

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Policy</strong></td>
<td>Select the media security policy to use for SDP negotiation:</td>
</tr>
<tr>
<td></td>
<td>• BEST EFFORT</td>
</tr>
<tr>
<td></td>
<td>• SECURITY DISABLED (default)</td>
</tr>
<tr>
<td></td>
<td>• SECURITY ENFORCED</td>
</tr>
<tr>
<td><strong>Best Effort Mode</strong></td>
<td>Select the mode to use when Best Effort policy is enabled.</td>
</tr>
<tr>
<td></td>
<td>• DUAL M-LINE (default)</td>
</tr>
<tr>
<td></td>
<td>• CAPABILITY</td>
</tr>
<tr>
<td><strong>Priority</strong></td>
<td>Select the order of priority for Crypto Suites. The range of permitted values is: 1 (highest priority) to 9 (lowest priority).</td>
</tr>
<tr>
<td></td>
<td>To disable encryption mode (AES_CM_128_HMAC_SHA1_80 or AES_CM_128_HMAC_SHA1_32), select 0, or clear the Priority check box. To enable encryption mode, select the Priority check box.</td>
</tr>
<tr>
<td></td>
<td>Default: 1</td>
</tr>
<tr>
<td><strong>SRTP Master Key Lifetime</strong></td>
<td>Select the exponent of the number of packets between key renegotiations. The range of permitted values is: 1 to 31</td>
</tr>
<tr>
<td></td>
<td>Default: 31</td>
</tr>
<tr>
<td></td>
<td><strong>Caution:</strong> Do not change the Avaya MS SRTP Master Key Lifetime default value. Changing this value can result in unexpected call handling.</td>
</tr>
<tr>
<td><strong>Key Derive Rate</strong></td>
<td>Select the rate at which new keys are derived. The range of permitted values is: 0 to 24</td>
</tr>
<tr>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td><strong>Master Key Index Length</strong></td>
<td>Select the number of bytes in the Master Key Index, which is transmitted with each packet. The Master Key Index identifies which master key to use for decoding. The range of permitted values is: 0 to 4.</td>
</tr>
<tr>
<td></td>
<td>Default: 0</td>
</tr>
</tbody>
</table>
Configuring Application Restrictions

About this task
Use this procedure to control what applications are available on an Avaya MS Cluster. On initial install or upgrade, no applications are enabled in the Configuration window, so you must enable any applications you want to configure.

⚠️ Caution:
When you enable an application, the system configures the application to use default values. Therefore, if you disable and then reenable an application, any custom configuration values are cleared, and replaced by the default values.

Limitations:
• You can configure most applications in cluster mode, including Announcements, Ad hoc Conferencing, MeetMe Conferencing, Unified Communications, and Music on Hold. However, you must configure the Instant Message Chat application standalone; it cannot be coresident with other applications, and must be configured as a cluster with just one Avaya MS.
• You cannot manually enable Recorder. Recorder is automatically enabled or disabled when MeetMe Conferencing is enabled or disabled.

Procedure
1. In the Configuration view of the AS 5300 Element Manager Console, navigate to Network Elements > Media Servers and Clusters > <cluster name> > Application Configuration.
2. To enable an application, select the application in the Available list, and click >>.
3. To remove a restriction for an application, select the application in the Enabled list, and click <<.
4. Click Apply.

Configuring Application Restrictions job aid

About this task

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>This list contains applications that you can enable.</td>
</tr>
<tr>
<td>Enabled</td>
<td>This list contains applications that are currently enabled.</td>
</tr>
</tbody>
</table>

Configuring IP Traffic on Avaya Media Server

About this task
Use this procedure to configure the media server to use external IP addresses.
By default, the media server uses the Internal OAM Address for Signaling, Media, and Cluster, and the address 0.0.0.0 for External OAM.

**Procedure**

1. In the Configuration view of the AS 5300 Element Manager Console, select **Network Elements > Media Servers and Clusters > Media Servers > <server name> >NE Maintenance**.
2. In the <server name> Maintenance window, select the Avaya MS instance to stop, and click **Stop** to stop the server.
3. In the Configuration view of the console, select **Servers**.
4. In the Servers dialog box, configure the **IPv4 External OAM Address**, **IPv4 Signaling Address**, **IPv4 Media Address**, and **IPv6 Media Address**.
5. Click **Apply**.
6. Start the Avaya MS network element:
   - a. In the Configuration view of the EM Console, select **Network Elements > Media Servers and Clusters > Media Servers > <server name> >NE Maintenance**.
   - b. In the <server name> Maintenance window, select the network element to start, and click **Start**.

---

**Configuring IP Traffic on Avaya Media Server job aid**

**About this task**

The following table lists and describes the values you must configure to control IP Traffic for the Avaya MS.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 External OAM Address</td>
<td>From the list, select the IPv4 address to use for traffic external to the enclave.</td>
</tr>
<tr>
<td>IPv4 Signaling Address</td>
<td>From the list, select the IPv4 address to use for signaling traffic.</td>
</tr>
<tr>
<td>IPv4 Media Address</td>
<td>From the list, select the IPv4 address to use for bearer traffic.</td>
</tr>
<tr>
<td>IPv6 Media Address</td>
<td>From the list, select the IPv6 address to use for bearer traffic.</td>
</tr>
</tbody>
</table>

---

**Applying QFE patches**

**About this task**

Use this procedure to apply Quick Fix Engineering (QFE) patches, also referred to as Hot Fixes, to Avaya Media Server (MS).
Caution:
If multiple QFE patches are available for the installed software version, you must install them in order of creation. For example, install QFEplatform- 7.5.0.230-0001 before you install QFE-platform 7.5.0.230-0002.

Note:
• If you have an Avaya MS cluster configuration, apply each QFE to one node at a time, while other nodes handle service requests.
• If your system includes High Availability server pairs, apply the QFE to the Backup server, and then to the Active server.

Prerequisites:
• The system is backed up.
• The latest software version of Avaya MS is installed. To install or upgrade Avaya MS, see the installation, upgrade, and patch Method of Procedures, delivered with the software load.

Procedure

1. Download the required QFE patch, using the download instructions provided by the Avaya technical support engineer, and transfer the QFE to the following folder on the target server:
   • Linux: //ma/MAS/qfe (e.g. /var/mcp/ma/MAS/qfe) (root permission required)
   • Windows: Avaya/multimedia-applications/MAS/QFE

2. In the AS 5300 Element Manager Console, navigate to Network Elements > Media Servers and Clusters > Media Servers > <target server> > Monitoring > Active Sessions. Depending on whether active sessions are listed, perform one of the following actions:
   • If any sessions are active, navigate to Network Elements > Media Servers and Clusters > Media Servers > <target server> > Service Maintenance, and click Pending Lock. Wait for the active sessions to terminate before continuing. If you continue while sessions are active, those sessions are terminated.
   • If no active sessions are listed, navigate to Network Elements > Media Servers and Clusters > Media Servers > <target server> > Service Maintenance, and click Lock.

3. (Optional) If you are applying more than one QFE, stop the Media Server NE using the steps in Stopping a network element on page 225. Avaya recommends that you stop the media server when applying multiple QFE patches in sequence, thereby preventing services from stopping and starting unnecessarily between each QFE application.

4. To retrieve the name of the patch, open the command line interface, and enter: maspatch list all. Information about the patch appears in table form; note the patch name, which appears in the QFE column. Note that this name can be different from the file name.

5. To apply the patch, enter: maspatch <patch name> apply

6. To verify that the patch is activated, enter: maspatch list all

7. If you stopped the Media Server NE, start it by following the steps in Starting a network element on page 224.
8. Navigate to **Network Elements > Media Servers and Clusters > Media Servers > <target server> > Service Maintenance**, and click **Unlock**.

9. Verify that the Avaya MS is functioning correctly:
   a. In the AS 5300 Element Manager Console, check for service-impacting alarms.
   b. Place a call involving an Avaya MS service.

---

### Applying QFE patches job aid

**About this task**

This job aid lists parameters used to apply QFE patches.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;target server&gt;</td>
<td>The Avaya MS on which to apply the QFE patch.</td>
</tr>
<tr>
<td>&lt;patch name&gt;</td>
<td>The name of the patch to apply. Note that this can be different from the patch file name.</td>
</tr>
<tr>
<td>maspatch</td>
<td>The command line tool used to apply, manage, and remove QFE patches, with the following syntax: `maspatch &lt;apply</td>
</tr>
</tbody>
</table>

---

### Removing QFE patches

**About this task**

Use this procedure to remove QFE from Avaya MS, and revert the system to the pre-patch state.

⚠️ **Caution:**

If multiple QFE patches are installed, you must remove them in reverse order of application. For example, if QFE-platform-7.5.0.230-0001 and QFE-platform-7.5.0.230-0002 are both installed on your system, you must remove QFE-platform-7.5.0.230-0002 before you remove QFEMAS-7.5.0.230-0001.

🌟 **Note:**

- If you have an Avaya MS cluster configuration, remove each QFE one node at a time, while other nodes handle service requests.
- If your system includes High Availability server pairs, first remove the QFE from the Backup server, then from the Active server.
Procedure

1. In the AS 5300 Element Manager Console, navigate to **Network Elements > Media Servers and Clusters > Media Servers > <target server> > Monitoring > Active Sessions**. Depending on whether active sessions are listed, perform one of the following actions:

   - If any sessions are active, navigate to **Network Elements > Media Servers and Clusters > Media Servers > <target server> > Service Maintenance**, and click **Pending Lock**. Wait for the active sessions to terminate before continuing. If you continue while sessions are active, those sessions are terminated.
   
   - If no active sessions are listed, navigate to **Network Elements > Media Servers and Clusters > Media Servers > <target server> > Service Maintenance**, and click **Lock**.

2. (Optional) If you are removing more than one QFE, stop the Media Server NE using the steps in **Stopping a network element** on page 225. Avaya recommends that you stop the media server when removing multiple QFE patches in sequence, thereby preventing services from stopping and starting unnecessarily between each QFE removal.

3. To retrieve the name of the patch, open the command line interface, and enter: `maspatch list all`. Information about the patch appears in table form, including the patch name in the QFE column. Note that this name can be different from the file name.

4. To remove the patch, enter: `maspatch remove <patch name>`

5. To verify that the patch is removed, enter: `maspatch list all` 

6. If you stopped the Media Server NE, start it by following the steps in **Starting a network element** on page 224.

7. Navigate to **Network Elements > Media Servers and Clusters > Media Servers > <target server> > Service Maintenance**, and click **Unlock**.

8. Verify that the Avaya MS is functioning correctly:
   
   a. In the AS 5300 Element Manager Console, check for service-impacting alarms.
   b. Place a call involving an Avaya MS service.

---

**Removing QFE patches job aid**

**About this task**

This job aid lists parameters used to remove in QFE patches.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;target server&gt;</td>
<td>The Avaya MS from which to remove the QFE patch.</td>
</tr>
<tr>
<td>&lt;patch name&gt;</td>
<td>The name of the patch to remove. Note that this can be different from the patch file name.</td>
</tr>
<tr>
<td>maspatch</td>
<td>The command line tool used to apply, manage, and remove QFE patches, with the following syntax: maspatch &lt;apply</td>
</tr>
</tbody>
</table>
Chapter 17: MFSS and LSC configuration

Configure Session Managers to perform the function of either a MultiFunction SoftSwitch (MFSS) or a Local Session Controller (LSC).

The SoftSwitch (SS), MFSS, LSCs, and Edge Border Controllers (EBC) support the Assured Services Access Control feature.

Prerequisites

- You must have the appropriate licence key for each AS 5300 Session Manager.

MFSS and LSC configuration procedures

About this task

The following task flow shows the sequence of procedures that you perform to configure each AS 5300 Session Manager as either an SS, a Master LSC, or an LSC.
MFSS and LSC configuration procedures

Navigation

- Configuring the IPv4 address table on page 44
- Configuring an external node on page 53
- Configuring an EBC on page 75
- Configuring an SS Session Manager on page 77
- Configuring an LSC Session Manager on page 78
- Configuring the Master LSC functional role on page 121
- Configuring the Slave LSC functional role on page 123
- Configuring the SS functional role on page 124
Configure Assured Services Access Control (ASAC) budgets to control resource consumption by audio and video calls.

# ASAC budget configuration procedures

**About this task**

The following task flow shows the sequence of procedures that you perform to configure an ASAC budget.
Navigation

- [Configuring a directional audio profile](#) on page 166
- [Configuring a nondirectional audio profile](#) on page 167
- [Configuring a directional video profile](#) on page 168
- [Configuring a nondirectional video profile](#) on page 169
- [Configuring an ASAC budget](#) on page 169
Configuring a directional audio profile

About this task
Configure a directional audio profile for ASAC to specify separate call counts for incoming and outgoing audio calls.

Prerequisites
- You can access the AS 5300 Element Manager Console.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console select **Network Data and Mtc > ARTS Integration > Audio Budget Profiles**.
2. On the Audio Budget Profiles window, click **Add (+)**.
3. On the Add ASAC Audio Count Profile dialog, configure the **Name**.
4. Select **Directional**.
5. Configure the **Inbound** and **Outbound** parameters.
6. Click **Apply**.

Configuring a directional audio profile job aid

About this task
The following table lists and describes the parameters you use to configure a directional audio profile.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This string value is the name that identifies the audio profile.</td>
</tr>
<tr>
<td>Type</td>
<td>This value specifies the type of call count for the profile. Radio buttons: Option buttons: select Directional</td>
</tr>
<tr>
<td>Inbound</td>
<td>This value specifies the number of incoming calls. This parameter is available only after you configure the Call Count to Directional.</td>
</tr>
<tr>
<td>Outbound</td>
<td>This value specifies the number of outgoing calls. This parameter is available only after you configure the Call Count to Directional.</td>
</tr>
</tbody>
</table>
Configuring a nondirectional audio profile

About this task
Configure a nondirectional audio profile for ASAC to specify the total call count for incoming and outgoing audio calls.

Prerequisites

• You can access the AS 5300 Element Manager Console.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > ARTS Integration > Audio Budget Profiles.
2. On the Audio Budget Profiles window, click Add (+).
3. On the Add ASAC Audio Count Profile dialog, configure the Name parameter.
4. Select Non-Directional.
5. In the Total field, type the numerical value for the maximum number of calls allowed before ASAC occurs.
6. Click Apply.

Configuring a nondirectional audio profile job aid

About this task
The following table lists and describes the parameters you use to configure a nondirectional audio profile.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This string value is the name that identifies the audio profile.</td>
</tr>
<tr>
<td>Type</td>
<td>This value specifies the type of call count for the profile. Options buttons: select Non-Directional</td>
</tr>
<tr>
<td>Total</td>
<td>This value specifies the number of calls (incoming and outgoing). This parameter is available only after you configure the Call Count to Total.</td>
</tr>
</tbody>
</table>
Configuring a directional video profile

About this task
Configure a directional video profile for ASAC to specify separate call counts (in video service units) for incoming and outgoing video calls.

⚠️ Important:
Higher bandwidth video CODECs reduce the number of video service units (VSU) available at any one time more than lower bandwidth CODECs.

Prerequisites
- You can access the AS 5300 Element Manager Console.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > ARTS Integration > Video Budget Profiles.
2. On the Video Budget Profiles window, click Add (+).
3. On the Add ASAC Video Call Count Profile window, configure the Name parameter.
4. Select Directional.
5. Configure the Inbound and Outbound parameters.
6. Click Apply.

Configuring a directional video profile job aid

About this task
The following table lists and describes the parameters you use to configure a directional video profile.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This string value is the name that identifies the video profile.</td>
</tr>
<tr>
<td>Type</td>
<td>This value specifies the type of call count for the profile. Option buttons: select Directional</td>
</tr>
<tr>
<td>Inbound</td>
<td>This value specifies the number of incoming VSUs. This parameter is available only after you configure the Call Count to Directional.</td>
</tr>
<tr>
<td>Outbound</td>
<td>This value specifies the number of outgoing VSUs. This parameter is available only after you configure the Call Count to Directional.</td>
</tr>
</tbody>
</table>
Configuring a nondirectional video profile

About this task
Configure a nondirectional video profile for ASAC to specify the total call count for incoming and outgoing video calls.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > ARTS Integration > Video Budget Profiles**.
2. On the Video Budget Profiles window, click **Add (+)**.
3. On the Add ASAC Video Call Count Profile window, configure the **Name** parameter.
4. Select **Non-Directional**.
5. In the **Total** field, type the numerical value for the maximum number of VSUs allowed before ASAC occurs.
6. Click **Apply**.

Configuring a nondirectional video profile job aid

About this task
The following table lists and describes the parameters you use to configure a nondirectional video profile.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This string value is the name that identifies the video profile.</td>
</tr>
<tr>
<td>Type</td>
<td>This value specifies the type of call count for the profile. Option buttons: select Non-Directional</td>
</tr>
<tr>
<td>Total</td>
<td>This value specifies the number of VSUs (incoming and outgoing). This parameter is available only after you configure the Call Count to Total.</td>
</tr>
</tbody>
</table>

Configuring an ASAC budget

About this task
Configure an ASAC budget to assign to the nodes to which you want to apply the specified budget profiles.

Prerequisites
- You can access the AS 5300 Element Manager Console.
• A configured audio budget profile exists.
• A configured video budget profile exists.

Procedure

1. From the Network Element view of the AS 5300 Element Manager Console, select **Network Elements > Session Managers > <Session Manager instance> > ARTS Integration > ASAC Budget**.
2. On the ASAC Budget window, click **Add (+)**.
3. On the Add ASAC Budget window, configure the **ASAC Budget** parameter.
4. From the **Audio Budget Profile** list, select a configured audio budget profile.
5. From the **Video Budget Profile** list, select a configured video budget profile.
6. To assign the ASAC budget to a node, from the **Available ASAC Elements** list, select the node and then click **>>**.
7. To remove a node assignment, from the **Assigned ASAC Elements** list, select the node and then click **<<**.
8. Click **Apply**.

---

**Variable Definitions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;Session Manager instance&gt;</code></td>
<td>This value is the instance of the AS 5300 Session Manager (for example, SESM1).</td>
</tr>
</tbody>
</table>

---

**Configuring an ASAC budget for remote locations**

**Before you begin**

• You can access the AS 5300 Element Manager Console.
• A configured audio budget profile exists.
• A configured video budget profile exists.

**About this task**

Configure an ASAC budget to count the calls made by Type 3 users according to their location.

**Procedure**

1. From the Network Element view of the AS 5300 Element Manager Console, select **Network Data and Mtc > ARTS Integration > ASAC Budget for Remote Locations**.
2. On the ASAC Budget for Remote Locations window, click **Add (+)**.
3. On the Add ASAC Budget for Remote Locations window, configure the ASAC Budget parameter.

4. In the Remote Location Profile Name field, type a name of the ASAC budget for a remote location.

5. From the Audio Budget Profile list, select a configured audio budget profile.

6. From the Video Budget Profile list, select a configured video budget profile.

7. Select the Count intra-location sessions check box if you want ASAC to count the calls that originate and terminate at the same location.

8. Click Apply.
Chapter 19: Commercial Cost Avoidance configuration

About this task
Configure the Commercial Cost Avoidance (CCA) feature so that subscribers can dial a public number and have the call routed across the private network if the public number maps to a private one. For information about provisioning tasks for the CCA feature, see *Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040-112*.

⚠️ Important:
The CCA feature shares some configuration with hybrid routing feature. For more information, see [Hybrid routing configuration](#) on page 176.

Prerequisites

- Add the LDAP server as an information element (trusted node). For more information, see [Configuring a trusted node](#) on page 54.
- Obtain and install the Certificate Authority (CA) and LDAP certificates. Use the AS 5300 Element Manager Console to import them into the key store and the trust store for Avaya Aura® Application Server 5300. For more information, see *Avaya Aura® Application Server 5300 Security, NN42040-601*. To import the certificates into the key store and trust store for the LDAP server, see the server documentation.
- Configure the LDAP certificate for the AS 5300 Session Manager. For more information, see [Configuring the whole AS 5300 Session Manager network element](#) on page 119.
- Configure the LDAP certificate for the Provisioning Manager. For more information, see [Configuring the whole Provisioning Manager network element](#) on page 135.

Navigation
- [Configuring the expiry timer for the routing cache](#) on page 173
- [Configuring the routing cache size](#) on page 173
- [Configuring the cache audit period](#) on page 174
- [Configuring the LDAP connection audit interval](#) on page 174
- [Configuring the query count](#) on page 175

Comments on this document? infodev@avaya.com
Configuring the expiry timer for the routing cache

About this task
Configure the expiry timer for the routing cache to determine the length of time to retain resolved LDAP lookups stored in the IMLDAPAddrLookupTable. The hybrid routing feature also uses this parameter.

Procedure
1. From the Network Element view of the AS 5300 Element Manager Console, select Network Elements > Session Managers > <Session Manager Instance> > Configuration Parameters.
2. From the Parm Group list, select LDAP.
3. Select TimeToLive and click Edit (+/−).
4. In the Value box, type a value in seconds.
   Range: 0–10000, Default: 3600 (one hour)
5. Click Apply.

Configuring the routing cache size

About this task
Configure the routing cache size to specify the maximum number of LDAP query results, and to specify the initial size of the IMDB table. The hybrid routing feature also uses this parameter.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Session Managers > <Session Manager instance> > Instance.
2. Select the appropriate AS 5300 Session Manager instance and then click Edit (+/−).
3. On the dialog, click Advanced.
4. From the Parm Group list, select IMDB.
5. Select IMLDAPAddrLookupMaxTuples and click Edit (+/−).
6. In the Value field, type a value in seconds.
   Range: 100–10000, Default: 1020
7. Click Apply.
Configuring the cache audit period

**About this task**
Configure the cache audit period to specify how long the system stores cached subscriber information in the database. The hybrid routing feature also uses this parameter.

**Procedure**
1. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Session Managers > <Session Manager instance> > Instance**.
2. Select the appropriate AS 5300 Session Manager instance and then click **Edit (-/+)**.
3. On the dialog, click **Advanced**.
4. From the **Parm Group** list, select IMDB.
5. Select **IMSubscriberCacheSyncInterval** and click **Edit (-/+)**.
6. In the **Value** field, type a value in seconds.
   - Range: 60–3600, Default: 60
7. Click **Apply**.

Configuring the LDAP connection audit interval

**About this task**
Configure the LDAP connection audit to determine the length of time between connectivity checks with the LDAP database.

**Procedure**
1. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Session Managers > <Session Manager instance> > Configuration Parameters**.
2. From the **Parm Group** list, select LDAP.
3. Select **AuditInterval** and click **Edit (-/+)**.
4. In the **Value** box, type a value in seconds.
   - Range: 5–86 400, Default: 60
5. Click **Apply**.
6. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Provisioning Managers > <PROV> > Configuration Parameters**.
7. Repeat 2 on page 174 to 5 on page 174 for each <PROV>. 
Configuring the query count

About this task
Configure the query count to specify the number of successful and unsuccessful audits before the system raises an alarm.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Session Managers > <Session Manager instance> > Instance.
2. Select the appropriate AS 5300 Session Manager instance and then click Edit (-/+).
3. On the dialog, click Advanced.
4. From the Parm Group list, select IMDB.
5. Select IMSSubscriberCacheSyncInterval and click Edit (-/+).
6. In the Value box, type a value in seconds.
   Range: 60–3600, Default: 60
7. Click Apply.
8. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Provisioning Managers > <PROV> > Instance.
9. Select the appropriate Provisioning Manager instance and then click Edit (-/+).
10. Repeat 3 on page 175 to 7 on page 175 for the Provisioning Manager.
Chapter 20: Hybrid routing configuration

About this task
Configure the hybrid routing feature so that the Avaya Aura® Application Server 5300 can identify IP and TDM routes, and then route them appropriately.

⚠ Important:
The hybrid routing feature shares some configuration with the Commercial Cost Avoidance (CCA) feature. For more information, see Commercial Cost Avoidance configuration on page 172.

Navigation
• Configuring an SS Session Manager on page 77
• Configuring an LSC Session Manager on page 78
• Configuring the Master LSC functional role on page 121
• Configuring the Slave LSC functional role on page 123
• Configuring the SS functional role on page 124
• Configuring the expiry timer for the routing cache on page 173
• Configuring the routing cache size on page 173
• Configuring the cache audit period on page 174
Chapter 21: Destination Code Controls configuration

About this task

Configure Destination Code Controls (DCC) feature to restrict subscribers from making calls to specific destinations that have been designated as difficult or impossible to reach. DCC controls the traffic to the enclaves and regions, and allows only precedence traffic to be passed to the destination.

For information about provisioning tasks for the DCC feature, see Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040-112.

Important:

The DCC feature is activated for inter-LSC calls only. DCC does not block incoming calls to the LSC. For Commercial Cost Avoidance (CCA) calls, the subscriber dials a public number and the call is routed using the private number mapped to the dialed public number. To block CCA calls, configure DCC to block both the private and the public numbers.

Navigation

• Configuring an SS Session Manager on page 77
• Configuring an LSC Session Manager on page 78
• Configuring the Master LSC functional role on page 121
• Configuring the Slave LSC functional role on page 123
• Configuring the SS functional role on page 124
Chapter 22: E911 Manager configuration

About this task

Configure E911 Manager to enable communication with the E911 Manager server node. E911 Manager is used to determine the real physical location of the user. AS 5300 uses this functionality to select the appropriate ERL when a user makes an emergency call according to the ELIN that was retrieved from E911 Manager.

Note:

E911 Manager should be a part of the deployment to enable this feature.

Procedure

To enable communication with E911 Manager, add the E911 Manager server as an information element (trusted node) with the Type parameter set to E911 Manager.

For more information, see Configuring a trusted node on page 54. Repeat the configuration steps if any redundant node of E911 Manager exists.

For information about provisioning tasks for the E911 Manager feature, see Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040-112.

To get more information about the E911 Manager feature, see:

• Avaya Aura® Application Server 5300 Overview, NN42040-100
• Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040-112
• Avaya Aura® Application Server 5300 Features Reference, NN42040–118
• Avaya Aura® Application Server 5300 Planning and Engineering, NN42040-200
• Avaya Aura® Application Server 5300 R3.0 - AS5300 Release Delta, NN42040-201
• Avaya Aura® Application Server 5300 Configuration, NN42040-500
• Avaya Aura® Application Server 5300 Alarms and Logs Reference, NN42040-701
• Avaya Aura® Application Server 5300 Operational Measurements Reference, NN42040-702
Chapter 23: Fault management configuration

This chapter contains the tasks that you use to configure logs and alarms for the system. Logs and alarms provide information that you can use to troubleshoot system faults.

Prerequisites

- A configured OSS server exists. For more information, see Configuring an OSS server on page 228 and Configuring an OSS endpoint on page 228.

Fault management configuration tasks

About this task

This work flow shows the sequence of tasks that you perform to configure logs and alarms for the system.
Fault management configuration

Navigation

- [Log configuration](#) on page 191
- [Alarm configuration](#) on page 83
- [SNMP configuration](#) on page 203
Chapter 24: Packaged application configuration

About this task

Configure packaged applications to ensure that subscribers can access and use packaged applications according to business requirements.

- Configuring Ad Hoc conferencing on page 181
- Configuring Meet Me conferencing on page 182
- Configuring Recorder on page 184
- Configuring Announcements on page 186
- Configuring Instant Message Chat on page 187
- Configuring Music on Hold on page 189
- Configuring Unified Communications on page 190

Configuring Ad Hoc conferencing

About this task

Use this procedure to configure Ad Hoc Conferencing.

Prerequisites

- Log on to AS 5300 Element Manager Console.
- On initial install or upgrade, all applications are restricted from operating. Before you can configure Ad Hoc conferencing, you must first configure Application Restrictions to allow the Ad Hoc conferencing feature to operate. See Configuring Application Restrictions on page 157.

Procedure

1. In the navigation pane, click Network Elements > Media Servers and Clusters > Media Server Clusters > <cluster> > Applications > AdHoc Conferencing.

2. On the AdHoc Conferencing window, edit the fields as required.

3. Click Apply.
Configuring Ad Hoc Conferencing job aid

About this task

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry Exit Tones</td>
<td>When enabled, plays entry and exit tones for all Ad Hoc conferences. When disabled, the ONT Entry Exit Tones configuration setting applies for Ad Hoc conferences originated by Optical Network Terminals (ONT). Default is disabled.</td>
</tr>
<tr>
<td>Maximum Call Duration</td>
<td>Specifies the maximum call duration in minutes allowed for an Ad Hoc session. Valid range is 0 to 10 080. Default is 1440.</td>
</tr>
<tr>
<td>Maximum Number of Ports</td>
<td>Specifies the maximum number of users who can join an Ad Hoc conference. If this value is set to zero (0), the number of maximum ports is set up for each user in Ad Hoc Conferencing Service System Profile in Provisioning Client. If this value not equal to zero (1-999), this value sets the number of maximum ports for all users on system regardless of Provisioning Client settings. Default is 0.</td>
</tr>
<tr>
<td>ONT Entry Exit Tones</td>
<td>When enabled, plays entry and exit tones for Ad Hoc conferences originated by ONT. When disabled, the Entry Exit Tones configuration setting applies. Default is enabled.</td>
</tr>
<tr>
<td>ONT Originator Release Ends Conference</td>
<td>When enabled, an Ad Hoc conference originated by an ONT ends when the originator hangs up. When disabled, the Originator Release Ends Conference configuration setting applies. Default is enabled.</td>
</tr>
<tr>
<td>Originator Release Ends Conference</td>
<td>When enabled, ends an Ad Hoc Conference when the originator hangs up. When disabled, the ONT Originator Release Ends Conference configuration setting applies for Ad Hoc Conferences originated by ONT. Default is disabled.</td>
</tr>
<tr>
<td>Send Accounting Info</td>
<td>When enabled, sends SIP INFO messages to the AS 5300 Session Manager to convey accounting information. Default is enabled.</td>
</tr>
<tr>
<td>Video Capability Negotiation</td>
<td>When enabled and properly licensed allows video conferencing. Default is disabled.</td>
</tr>
</tbody>
</table>

Configuring Meet Me conferencing

About this task

Use this procedure to configure Meet Me Conferencing.
Prerequisites

- Log on to AS 5300 Element Manager Console
- On initial install or upgrade, all applications are restricted from operating. Before you can configure Meet Me conferencing, you must first configure Application Restrictions to allow the Meet Me conferencing feature to operate. See Configuring Application Restrictions on page 157.

Procedure

1. In the navigation pane, click Network Elements > Media Servers and Clusters > Media Server Clusters > <cluster> > Applications > Meetme conferencing.
2. On the Meetme conferencing window, edit the fields as required.
3. Click Apply.

Configuring Meet Me Conferencing job aid

About this task

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Passcodes</td>
<td>When enabled, allows a chairperson to require that participants enter both a pass code and the conference access code. If this option is disabled, the following fields are dimmed: Maximum Participant Access Code Attempts, and Maximum Chairperson Pin Attempts.</td>
</tr>
<tr>
<td>Allow Video Capability</td>
<td>When enabled and properly licensed, allows video in conferences. Default is disabled.</td>
</tr>
<tr>
<td>Answer Delay</td>
<td>Specifies the number of rings before an incoming SIP call is answered. 0 rings implies immediate answer. Valid range is 1 to 100. Default is 1 ring.</td>
</tr>
<tr>
<td>Audio Recording</td>
<td>When enabled, allows a chairperson to record conferences. Default is enabled.</td>
</tr>
<tr>
<td>Chat Capability</td>
<td>When enabled, allows a chairperson to start a chat room when in conference. Default is enabled.</td>
</tr>
<tr>
<td>Default Domain</td>
<td>Specifies the primary domain for stand alone Meet Me.</td>
</tr>
<tr>
<td>Default Locale</td>
<td>Specifies the default language to use for Meet Me announcements. The drop-down list contains all available locales.</td>
</tr>
<tr>
<td>First Digit Timer</td>
<td>Specifies the duration in milliseconds to wait for the first DTMF tone from the caller. Valid range is 1,000 to 300,000 milliseconds. Default is 7,000.</td>
</tr>
<tr>
<td>Instant Messages</td>
<td>When enabled, allows the system to send Instant Messages (IM) to the conference chairperson. Default is enabled.</td>
</tr>
<tr>
<td>Instant Messages From User</td>
<td>Specifies the name to display when sending an IM. Valid characters are: a-z A-Z 0-9 _ . ! ~ * ( ) + = and -. No spaces are permitted. Default is MeetMeConf.</td>
</tr>
<tr>
<td>Inter Announcements Wait Time</td>
<td>Specifies the time duration between “chair has not yet arrived” messages. The valid range is 5,000 to 7,200,000 milliseconds. Default is 120,000.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Inter Digit Timer</td>
<td>Specifies the duration in milliseconds to wait between DTMF tones before timing out. Valid range is 1,000 to 300,000 milliseconds. Default is 5,000.</td>
</tr>
<tr>
<td>Maximum Call Duration</td>
<td>Specifies the maximum duration (in minutes) that a Meet Me session is allowed. The minimum value is 1 and the maximum is 10,080. The default value is 1,440.</td>
</tr>
<tr>
<td>Maximum Chairperson PIN Attempts</td>
<td>Specifies the number of attempts allowed for chairperson PIN entry. The valid range is 3 to 26. Default value is 3.</td>
</tr>
<tr>
<td>Maximum Participant Access Code Attempts</td>
<td>Specifies the number of attempts permitted for access code entry. The valid range is 3 to 26. Default value is 3.</td>
</tr>
<tr>
<td>Maximum Participant Pass Code Attempts</td>
<td>Specifies the number of attempts permitted for pass code entry. The valid range is 3 to 26. Default value is 3.</td>
</tr>
<tr>
<td>Maximum Wait Segments</td>
<td>Specifies the number of times to play &quot;chair has not yet arrived&quot; message before disconnecting. The valid range is 1 to 100. Default is 10.</td>
</tr>
<tr>
<td>Send accounting info</td>
<td>When enabled, sends SIP INFO messages to the AS 5300 Session Manager to convey accounting information.</td>
</tr>
<tr>
<td>Star First Digit Timer</td>
<td>Specifies the duration in milliseconds to wait for the caller to press the star (*) key. Valid range is 1,000 to 300,000 milliseconds. Default is 3,000</td>
</tr>
<tr>
<td>Star Inter Digit Timer</td>
<td>Specifies the duration in milliseconds to wait for the caller to press the next key. Valid range is 1,000 to 300,000 milliseconds. Default is 3,000</td>
</tr>
<tr>
<td>Use Default Domain</td>
<td>Indicates if the default domain is the only domain in use. Default is disabled. The following field is dimmed when disabled: Default Domain.</td>
</tr>
</tbody>
</table>

## Configuring Recorder

### About this task

Use this procedure to configure the Recorder values that are used by applications when subscribers record calls. The chairperson uses Personal Agent to specify the e-mail address used by this feature, and to enable or disable the feature. The chairperson may record all or part of a conference by pressing "+9 to toggle recording on or off.

**Note:**

When a conference is recorded, the system counts the Recorder as a participant in the conference. For example, if three parties are in a call and the call is being recorded, the system reports that there are four parties in the call.

### Prerequisites

- Log on to AS 5300 Element Manager Console.

### Procedure

1. In the navigation pane, click **Network Elements > Media Servers and Clusters > Media Server Clusters > <cluster> > Applications > Recorder.**
2. On the Recorder window, edit the fields as required.

3. Click Apply.

### Configuring Recorder job aid

**About this task**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Recording Collection Interval</td>
<td>The Meet Me conferencing service breaks the audio recordings into manageable chunks, and sends the recordings (as .wav files) to the chairperson through e-mail. This option specifies the maximum size of the recorded segments, in the range of 10–30 minutes. Default is 30.</td>
</tr>
<tr>
<td>Maximum Recording Time</td>
<td>This option specifies the maximum length of a recording session, in the range of 30–600 minutes. Default is 600.</td>
</tr>
</tbody>
</table>

### Configuring Recorder e-mail settings

**About this task**

Use this procedure to configure the values that are used by Meet Me to send recorded conversations by e-mail.

**⚠️ Note:**

The chairperson uses Personal Agent to specify the e-mail address used by this feature, and to enable or disable the feature. The chairperson may record all or part of a conference by pressing *9 to toggle recording on or off.

**Prerequisites**

- Log on to the Provisioning Client.

**Procedure**

1. Select **Services > Call Termination > Unified Communications**.
2. Click the Domain Properties tab.
3. In the **Default SMTP server** field, type the SMTP server.
4. In the **Email attachment size** field, choose the quality and size.
5. Click **Apply**.
Configuring Recorder e-mail settings job aid

About this task

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default SMTP server</td>
<td>The name of the default SMTP server.</td>
</tr>
<tr>
<td>Email attachment size</td>
<td>This value controls the size and quality of email attachments, and hence limits the length of recordings that Meet Me can transmit.</td>
</tr>
</tbody>
</table>

Configuring Announcements

About this task

Use this procedure to configure Announcements.

Prerequisites

- Log on to AS 5300 Element Manager Console.
- On initial install or upgrade, all applications are restricted from operating. Before you can configure Announcements, you must first configure Application Restrictions to allow the Announcements feature to operate. See Configuring Application Restrictions on page 157.

Procedure

1. In the navigation pane, click Network Elements > Media Servers and Clusters > Media Server Clusters > <clusternname> > Applications > Announcements Configuration.
2. On the Announcements window, edit the fields as required.
3. Click Apply.

Configuring Announcements job aid

About this task

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Answer Delay</td>
<td>Specifies the number of rings before an incoming SIP call is answered. Valid range is 0 to 100 rings. Zero implies immediate answer. Default is 0.</td>
</tr>
<tr>
<td>Maximum Call Duration</td>
<td>Specifies the maximum allowed duration in minutes for an announcement session. Valid range is 0 to 10 080 minutes. Default is 1440.</td>
</tr>
</tbody>
</table>
Configuring Instant Message Chat

About this task
Use this procedure to customize Instant Message Chat.

Prerequisites

- Log on to AS 5300 Element Manager Console.
- On initial install or upgrade, all applications are restricted from operating. Before you can configure Instant Message Chat, you must first configure Application Restrictions to allow the Instant Message Chat feature to operate. See Configuring Application Restrictions on page 157.

Procedure

1. In the navigation pane, click Network Elements > Media Servers and Clusters > Media Server Clusters > <cluster> > Applications > Chat > Configuration.
2. On the Configuration window, edit the fields as required.
3. Click Apply.
4. In the navigation pane, click Network Elements > Media Servers and Clusters > Media Server Clusters > <cluster> > Applications > Chat > Administrators.
5. On the Administrators window, click Add (+).
6. In the Add Administrator window, enter the name for the new chat administrator.
7. Click Apply.
8. In the navigation pane, click Network Elements > Media Servers and Clusters > Media Server Clusters > <cluster> > Applications > Chat > System rooms.
10. In the Add Room window, enter the name for the new chat room.
11. Click Apply.

Configuring Instant Message Chat job aid

About this task

<table>
<thead>
<tr>
<th>Configuration page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
<td></td>
</tr>
<tr>
<td>Maximum Rooms</td>
<td>The maximum number of chat rooms. The minimum value is 1 and the maximum value is 250. Default is 100.</td>
</tr>
</tbody>
</table>

Table continues…

Comments on this document? infodev@avaya.com
### Configuration page

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Participants Per Room</td>
<td>The maximum number of participants allowed in a single chat room. The minimum value is 2 and the maximum value is 250. Default is 100.</td>
</tr>
<tr>
<td>Idle Timeout</td>
<td>Maximum time, in milliseconds, for which a session is permitted to remain active without joining a room. After this duration, the session terminates. The minimum value is 60 000 and the maximum value is 1 800 000. Default is 300 000 ms.</td>
</tr>
<tr>
<td>Inactivity Timeout</td>
<td>Maximum session idle time, in milliseconds, in a chat room. The session terminates when there is no activity in the room for this duration. The minimum value is 60 000 and the maximum value is 60 480 000. Default is 43 200 000 ms.</td>
</tr>
<tr>
<td>Invitation Response Timeout</td>
<td>Maximum time, in milliseconds, to wait for a response to a chat invitation. The minimum value is 60000 and the maximum value is 1 800 000. Default is 120 000 ms.</td>
</tr>
<tr>
<td>Maximum Call Duration</td>
<td>Use the default value for this option. This option is not used by the Instant Chat application, and is not enforced.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>Select to route Chat messages through the SIP Core’s AS 5300 Session Manager (proxy), which, when configured, provides added security. Default is disabled.</td>
</tr>
</tbody>
</table>

### Cluster Administrators page

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators</td>
<td>List of chat administrators in the format: user@domain. Default is none.</td>
</tr>
<tr>
<td>Add Administrator / Admin Name</td>
<td>Enter the name of the new chat administrator. Minimum Admin Name length is 3 (1 character for name, 1 for ‘@’, 1 for domain) and maximum length is 85 (20 characters for name, 1 for ‘@’, 64 for domain).</td>
</tr>
</tbody>
</table>

### System Rooms page

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Rooms</td>
<td>Is a list of names of predefined chat rooms (room@domain) that are always available to all users. The maximum domain length is 64 characters. The maximum total length (for all room names) is 1024 characters.</td>
</tr>
</tbody>
</table>

*Table continues…*
### Configuring Music on Hold

**About this task**

Use this procedure to configure Music On Hold.

**Prerequisites**

- Log on to AS 5300 Element Manager Console.
- On initial install or upgrade, all applications are restricted from operating. Before you can configure Music on Hold, you must first configure Application Restrictions to allow the Music on Hold feature to operate. See [Configuring Application Restrictions](#) on page 157.

**Procedure**

1. In the navigation pane, click **Network Elements > Media Servers and Clusters > Media Server Clusters > <cluster> > Applications > Music on hold**.
2. On the Music on hold window, edit the fields as required.
3. Click **Apply**.

---

### Configuring Music on Hold job aid

**About this task**

The following table describes the parameters used in configuring Music on Hold.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Answer Delay</strong></td>
<td>Specifies the number of rings before an incoming SIP call is answered. Valid range is 0 to 100 rings. Zero implies immediate answer. Default is 0.</td>
</tr>
<tr>
<td><strong>Maximum Call Duration</strong></td>
<td>Specifies the maximum allowed duration in minutes for a MOH session. Valid range is 0 to 10 080 minutes. Default is 1440.</td>
</tr>
</tbody>
</table>
Configuring Unified Communications

About this task
Use this procedure to configure Unified Communications.

Prerequisites
- Log on to AS 5300 Element Manager Console.
- On initial install or upgrade, all applications are restricted from operating. Before you can configure Unified Communications, you must first configure Application Restrictions to allow the Unified Communications feature to operate. See Configuring Application Restrictions on page 157.

Procedure
1. In the navigation pane, click Network Elements > Media Servers and Clusters > Media Server Clusters > <cluster> > Applications > Unified Communications.
2. On the Unified Communications window, edit the fields as required.
3. Click Apply.

Configuring Unified Communications job aid

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Locale</td>
<td>Default Locale Specifies the default language to use for UCOMM announcements. The drop-down list contains all available locales.</td>
</tr>
<tr>
<td>Deposit SIP URI User #1</td>
<td>Directs calls with matching SIP Request URI users to Message Deposit.</td>
</tr>
<tr>
<td>Deposit SIP URI User #2</td>
<td>Directs calls with matching SIP Request URI users to Message Deposit.</td>
</tr>
<tr>
<td>Express SIP URI User #1</td>
<td>Directs calls with matching SIP Request URI users to Express Messaging.</td>
</tr>
<tr>
<td>Express SIP URI User #2</td>
<td>Directs calls with matching SIP Request URI users to Express Messaging.</td>
</tr>
<tr>
<td>PA Location</td>
<td>Populates the e-mail template so that http links (to picture IDs and images) are resolved to a public hostname or IP address of the Personal Agent web server. The Personal Agent web server delivers these images.</td>
</tr>
<tr>
<td>Retrieve SIP URI User #1</td>
<td>Directs calls with matching SIP Request URI users to Message Retrieval.</td>
</tr>
<tr>
<td>Retrieve SIP URI User #2</td>
<td>Directs calls with matching SIP Request URI users to Message Retrieval.</td>
</tr>
<tr>
<td>Send Accounting Info</td>
<td>When enabled, sends SIP INFO messages to the Application Server 5300 Session Manager, conveying accounting information. Default is enabled.</td>
</tr>
<tr>
<td>Use Custom Email Templates</td>
<td>When enabled, uses custom e-mail templates. Default is disabled.</td>
</tr>
</tbody>
</table>
Chapter 25: Log configuration

Configure how the system handles and stores system operation logs. Logs provide information that is useful for troubleshooting.

Avaya Media Server (MS) debug logging is described in Configuring debug logging on page 201.

Prerequisites

• A configured OSS server exists. For more information, see Configuring an OSS server on page 228 and Configuring an OSS endpoint on page 228.

Log configuration procedures

About this task

This task flow shows the sequence of procedures you perform to configure logs for the Application Server 5300 system.
Configuring a simple log filter on page 193
Configuring a composite log filter on page 194
Configuring the log browser feed on page 195
Configuring log storage rules on page 196
Configuring the log North-bound Server Feed rule on page 197
Configuring log FTP Push rules on page 199
Configuring a simple log filter

About this task
Configure simple log filters to categorize logs according to log severities and types.

Prerequisites
• You can access the AS 5300 Element Manager Console.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > OAM Profiles > Log Filters.
2. Click Add (+).
   OR
   Select an existing log filter and click Edit (-/+).
3. In the Add Log Filter window, configure Name and Filter Type.
4. In the Log Criteria tab, select the check boxes for the Event Severities and Event Types that you want to include.
5. Clear the check boxes for the Event Severities and Event Types that you do not want to include.
6. Click Apply.

Configuring a simple log filter job aid

About this task
This job aid lists and describes the parameters that you use to configure a simple log filter.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name that represents the Log Filter in the system.</td>
</tr>
<tr>
<td>Filter Type</td>
<td>This parameter (select SIMPLE from the list) specifies the log type.</td>
</tr>
<tr>
<td>Event Severities</td>
<td>This parameter (select or clear check boxes) specifies logs to include according to severity. Event severities include: ALARM, INFO, and ALERT.</td>
</tr>
<tr>
<td>Event Types</td>
<td>This parameter (select or clear check boxes) specifies logs to include according to event type. Event types include: COMMUNICATION RESOURCE AUDIT DEBUG THRESHOLD ABNORMAL ADMIN QOS UNCATEGORIZED SECURITY</td>
</tr>
</tbody>
</table>
Default log filters job aid

This job aid lists the filters that a fresh installation creates. These filters appear in the Log filters panel.

<table>
<thead>
<tr>
<th>Filter name</th>
<th>Filter type</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>all logs</td>
<td>SIMPLE</td>
<td>This filter contains all logs.</td>
</tr>
<tr>
<td>security</td>
<td>SIMPLE</td>
<td>This filter contains all security and audit logs, regardless of severity.</td>
</tr>
<tr>
<td>debug</td>
<td>SIMPLE</td>
<td>This filter contains all debug logs, regardless of severity.</td>
</tr>
<tr>
<td>alarm</td>
<td>SIMPLE</td>
<td>This filter contains all alarm logs, regardless of severity.</td>
</tr>
<tr>
<td>non-security</td>
<td>COMPOSITE</td>
<td>This filter contains all logs except security or audit logs.</td>
</tr>
<tr>
<td>iems</td>
<td>COMPOSITE</td>
<td>This filter contains all of the logs defined in the non-security filter except alarm logs.</td>
</tr>
</tbody>
</table>

Configuring a composite log filter

About this task

Configure composite log filters to categorize logs according to log severities and types by using combinations of existing simple and composite filters.

Prerequisites

- You can access the AS 5300 Element Manager Console.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > OAM Profiles > Log Filters**.
2. Click **Add (+)**.
3. In the Add Log Filter dialog, configure the **Name** and select the **Filter Type** as COMPOSITE.
4. In the **Filter Composition** section, configure the **Start Log Filter** parameter.
5. From the **Available Log Filters** list, select a log filter and click **>>** to move the filter to the **Subtracted Log Filters** list.
6. From the **Subtracted Log Filters** list, select a log filter and click **<<** to move the filter to the **Available Log Filters** list.
7. Repeat 2 on page 194 to 6 on page 194 for each log filter, to create the list of filters that you want to subtract from the start filter.
8. Click **Apply**.
Configuring a composite log filter job aid

About this task

This job aid lists and describes the parameters that appear on the Add log filter dialog box.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name that represents the Log Filter in the system.</td>
</tr>
<tr>
<td>Filter Type</td>
<td>This parameter (select COMPOSITE from the list) specifies the log type.</td>
</tr>
<tr>
<td>Start Log Filter</td>
<td>This parameter (select from the list) determines the simple or composite filter from which to begin filtering.</td>
</tr>
<tr>
<td>Available Log Filters</td>
<td>This parameter is a list of all filters already configured (simple and composite), which are not selected as the start filter in this dialog, and which are not moved to subtracted filters list.</td>
</tr>
<tr>
<td>Subtracted Log Filters</td>
<td>This parameter is a list of filters for which the resulting logs are subtracted from start set of logs (Start Log Filter).</td>
</tr>
</tbody>
</table>

Default log filters job aid

This job aid lists the log filters that a fresh installation creates.

<table>
<thead>
<tr>
<th>Filter name</th>
<th>Filter type</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>all logs</td>
<td>SIMPLE</td>
<td>This filter contains all logs.</td>
</tr>
<tr>
<td>security</td>
<td>SIMPLE</td>
<td>This filter contains all security and audit logs, regardless of severity.</td>
</tr>
<tr>
<td>debug</td>
<td>SIMPLE</td>
<td>This filter contains all debug logs, regardless of severity.</td>
</tr>
<tr>
<td>alarm</td>
<td>SIMPLE</td>
<td>This filter contains all alarm logs, regardless of severity.</td>
</tr>
<tr>
<td>non-security</td>
<td>COMPOSITE</td>
<td>This filter contains all logs except security or audit logs.</td>
</tr>
<tr>
<td>iems</td>
<td>COMPOSITE</td>
<td>This filter contains all of the logs defined in the non-security filter except alarm logs.</td>
</tr>
</tbody>
</table>

Configuring the log browser feed

About this task

Configure the log browser feed to have the AS 5300 Element Manager send only a subset of logs to the AS 5300 Element Manager Console log browser, for security purposes.

Prerequisites

- You can access the AS 5300 Element Manager Console.
**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > OAM Profiles > Log Browser Feeds**.
2. In the Log Browser Feeds window, configure the **Log Format** and **Log Filter** values.
3. Click **Apply**.

---

**Configuring the log browser feed job aid**

**About this task**

This job aid lists and describes the fields that appear on the Log Browser Feed panel.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Format</strong></td>
<td>This parameter (select from the list) specifies the format of logs forwarded to the AS 5300 Element Manager Console log browser. The supported formats are: MCP, STD, STDEcore, SCC2 and SCC2Ecore.</td>
</tr>
<tr>
<td><strong>Filter</strong></td>
<td>This parameter (select from the list of configured log filters) determines the particular set of logs forwarded to the AS 5300 Element Manager Console log browser.</td>
</tr>
</tbody>
</table>

---

**Configuring log storage rules**

**About this task**

Configure log storage rules to specify how the system stores formatted log record files and to ensure the access control of security log files.

**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Element Manager > Element Manager > Log Processing > Log Storage Rules**.
2. On the ElementManager Log Storage Rules window, click **Add (+)**.
3. In the Add Log Storage Rule window, configure the **Name**, **Log Format**, **Log Filter**, and **Working Directory** parameters.
4. In the **Storage Policy Group** section, configure the **Rotation Size Enabled**, **Rotation Size**, **Rotation Period Enabled**, **Rotation Period**, **Retention**, **Secure**, and **Compression** values.
5. Click **Apply**.
# Configuring log storage rules job aid

## About this task

This job aid lists and describes the parameters that appear on the Add Log Storage Rule dialog.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name that represents a log storage rule under the context of a AS 5300 Element Manager or a Fault Performance Manager.</td>
</tr>
<tr>
<td>Log Format</td>
<td>This parameter (select from the list) specifies the format of logs under this rule. The supported formats are: MCP, STD, STDEcore, SCC2 and SCC2Ecore.</td>
</tr>
<tr>
<td>Log Filter</td>
<td>This parameter (select from the list of configured log filters) determines the particular set of logs stored by this rule.</td>
</tr>
<tr>
<td>Working Directory</td>
<td>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.</td>
</tr>
<tr>
<td>Rotation Size Enable</td>
<td>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.</td>
</tr>
<tr>
<td>Rotation Size</td>
<td>This parameter specifies the file size for rotation in megabytes—available only if the Rotation Size Enable check box is selected.</td>
</tr>
<tr>
<td>Rotation Period Enable</td>
<td>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.</td>
</tr>
<tr>
<td>Rotation Period</td>
<td>This parameter specifies the number of minutes for rotation—available only if the Rotation Period Enable check box is selected.</td>
</tr>
<tr>
<td>Retention</td>
<td>This parameter (select from the list) specifies the number of days for which the system retains log files. The options are 1–7 days.</td>
</tr>
<tr>
<td>Secure</td>
<td>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</td>
</tr>
<tr>
<td>Compression</td>
<td>This parameter (check box) enables or disables compression of log files. Select the check box to enable compression of log files.</td>
</tr>
</tbody>
</table>

# Configuring the log North-bound Server Feed rule

## About this task

Configure the destinations of log records forwarded over a TCP connection to ensure that the AS 5300 Element Manager and Fault Performance Manager (FPM) forward secured log records to the authorized OSS server destinations only.

### Prerequisites

- You can access the AS 5300 Element Manager Console.
Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Element Manager > Log Processing > Log North-bound Server Feed Rules.

2. On the ElementManager Log North-bound Server Feed Rules window, click Add (+).

3. In the Add Log North-bound Server Feed Rule dialog, configure the Name, Log Format, and Log Filter values.

4. In the North Bound Server Feed Rule section, configure the Local Port and ACL Validation values.

5. Click >> to move a selected available OSS server to the OSS Servers pane.

6. Click << to remove a selected OSS server.

7. Click Apply.


10. In the Add Log North-bound Server Feed Rule dialog, configure the Name, Log Format, and Log Filter values.

11. In the North Bound Server Feed Rule section, configure the Local Port and ACL Validation values.

12. Click >> to move a selected available OSS server to the OSS Servers pane.

13. Click << to remove a selected OSS server.

14. Click Apply.

Configuring the log North-bound Server Feed rule job aid

About this task

This job aid lists and describes the parameters that appear on the Add Log North-bound Server Feed Rule dialog box.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name that represents a log North-bound Server Feed rule under the context of a AS 5300 Element Manager or a Fault Performance Manager.</td>
</tr>
<tr>
<td>Log Format</td>
<td>This parameter (select from the list) specifies the format of logs under this rule. The supported formats are: MCP, STD, STDEcore, SCC2 and SCC2Ecore.</td>
</tr>
<tr>
<td>Log Filter</td>
<td>This parameter (select from the list of configured log filters) determines the particular set of logs stored by this rule.</td>
</tr>
</tbody>
</table>

Table continues…
### Configuring log FTP Push rules

#### About this task

Configure log FTP Push rules to specify the destinations of FTP Push and ensure that the system forwards security log files to the authorized OSS destinations only.

#### Prerequisites

- You can access the AS 5300 Element Manager Console.

#### Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Element Manager > Element Manager > Log Processing > Log FTP Push Rules**.
2. On the ElementManager Log FTP Push Rules window, click **Add (+)**.
3. In the Add Log FTP Push Rule dialog, configure the **Name**, **Log Storage Rule**, and **FTP Destination** values.
4. Click **Apply**.

---

### Configuring log FTP Push rules job aid

#### About this task

This job aid lists and describes the parameters that appear on the Add Log FTP Push Rule dialog box.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This parameter (text) is a unique name to represent a log FTP Push rule under the context of a AS 5300 Element Manager or a Fault Performance Manager.</td>
</tr>
<tr>
<td>Log Storage Rule</td>
<td>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.</td>
</tr>
<tr>
<td>FTP Destination</td>
<td>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.</td>
</tr>
</tbody>
</table>
Enabling and disabling log processing rules

About this task
Enable or disable log processing rules to determine which rules apply.

Prerequisites
- You can access the AS 5300 Element Manager Console.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Element Manager > Element Manager > Log Processing > Log Rules Maintenance.
2. On the Log Processing Rules Maintenance window, select a tab.

<table>
<thead>
<tr>
<th>To enable or disable</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log storage rules</td>
<td>Select the Storage tab.</td>
</tr>
<tr>
<td>Log North-bound Server Feed rules</td>
<td>Select the North-bound Server Feed tab.</td>
</tr>
<tr>
<td>Log FTP Push rules</td>
<td>Select the FTP Push tab.</td>
</tr>
</tbody>
</table>
3. Select a rule.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the selected rule.</td>
<td>Click Enable.</td>
</tr>
<tr>
<td>Disable the selected rule.</td>
<td>Click Disable.</td>
</tr>
</tbody>
</table>
5. On the Log Processing Rules Maintenance window, select a tab.

<table>
<thead>
<tr>
<th>To manage</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log storage rules</td>
<td>Select the Storage tab.</td>
</tr>
<tr>
<td>Log North-bound Server Feed rules</td>
<td>Select the North-bound Server Feed tab.</td>
</tr>
<tr>
<td>Log FTP Push rules</td>
<td>Select the FTP Push tab.</td>
</tr>
</tbody>
</table>
6. Select a rule.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the selected rule.</td>
<td>Click Enable.</td>
</tr>
<tr>
<td>Disable the selected rule.</td>
<td>Click Disable.</td>
</tr>
</tbody>
</table>
Enabling and disabling log processing rules job aid

About this task

The following table lists and describes the columns that appear on the Log Processing Maintenance panel.

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This column contains the unique names of the processing rules.</td>
</tr>
<tr>
<td>Log Format</td>
<td>This column contains the names of the log formats associated with the processing rules.</td>
</tr>
<tr>
<td>Log Filter</td>
<td>This column contains the names of the log filters associated with the processing rules.</td>
</tr>
<tr>
<td>Admin</td>
<td>This column contains the administrative states of the rules. The value is either ENABLED or DISABLED.</td>
</tr>
</tbody>
</table>

Configuring debug logging

About this task

Use this procedure to configure debug logging, which is used for system support. Debug logging is enabled from the Avaya Media Server (MS) debug port, which you access using SSH.

Prerequisites

- You have a valid admin account on the Avaya MS.

Procedure

1. Using an SSH client, log on to the Avaya MS server.
2. Enter `telnet <localhost> <MS baseport>` to connect to the MS debug port.
3. At the Username prompt, enter your user name.
4. At the Password prompt, enter your password.
5. At the Debug prompt, enter `cd MS`.
6. At the Debug/root/MS prompt, enter `debugtrace`.
7. At the Debug/root/MS prompt, enter one of the following:
   - `debugtrace on` to enable debug logging.
   - `debugtrace off` to disable debug logging.
   - `debugtrace status` to view the status of debug logging.
8. Enter `quit`. 
Log configuration

9. Enter `su - root`
10. Enter `logcapture -t -f <filename>`

---

Configure debug logging job aid

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;localhost&gt;</code></td>
<td>The Avaya MS server IP address.</td>
</tr>
<tr>
<td><code>&lt;MS baseport&gt;</code></td>
<td>The Avaya MS server debug port.</td>
</tr>
<tr>
<td><code>&lt;filename&gt;</code></td>
<td>The name of the file in which to save the log data.</td>
</tr>
</tbody>
</table>
Chapter 26: SNMP configuration

Create Simple Network Management Protocol (SNMP) profiles to configure consistent SNMP parameters to assign to servers.

SNMP configuration procedures

About this task
This task flow shows you the sequence of procedures you perform to configure SNMP.

Navigation
- Configuring the SNMP Manager on page 204
Configuring the SNMP Manager

About this task

To start forwarding traps (alarm generating event reports) to an existing Network Management Layer (NML) manager, configure an SNMP Manager to associate with the AS 5300 Element Manager and all Fault Performance Managers. Perform this procedure to configure the SNMP Manager.

You can configure the following SNMP profiles:

- SNMPv2c
- SNMPv3

Prerequisites

- You can access the AS 5300 Element Manager Console.
- You have FPOssProfileService privileges.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > OAM Profiles > SNMP Managers**.
2. On the SNMP Managers window, click **Add (+)**.
3. In the Add SNMP Manager dialog box, perform the following:
   a. In **Profile Name**, type the name of the SNMP profile.
   b. In **Server**, select **OSSWin**.
   c. In **Profile Version**, select **SNMPv2c** or **SNMPv3**.
      - When you select **Profile Version**, the system displays the parameters associated with the SNMP profile. Fill the appropriate values in the parameters.
      - For **SNMPv2**, the system displays the **Community** parameter.
   d. In **Trap Port**, type the port value.
   e. Click **Apply**.
Configuring the SNMP Manager for the AS 5300 Element Manager

About this task
To start forwarding traps (alarm generating event reports) to an existing Network Management Layer (NML) manager, associate the SNMP Manager with the AS 5300 Element Manager. Perform this procedure to configure the SNMP Manager for the AS 5300 Element Manager.

Prerequisites
- You can access the AS 5300 Element Manager Console.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Element Managers > Element Manager > Alarm Processing > SNMP Managers.
2. On the ElementManager SNMP Managers window, click Add (+).
3. In the Add ElementManager SNMP Managers dialog, from the SNMP Manager list, select the name of the SNMP Manager profile.
4. Click Apply.

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Element Manager instance&gt;</td>
<td>This value is the instance of the AS 5300 Element Manager.</td>
</tr>
</tbody>
</table>

Associating an SNMP profile with a server

About this task
Associate an SNMP profile to a server so that the AS 5300 Element Manager can monitor the server.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have SnmpProfileService privileges.
- You have PhysicalServerService privileges.
- You have PhysicalSiteService privileges.
- You have IPAddressService privileges.
**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Servers**.
2. Select a server entry and click **Edit (-/+)**.
3. In the Edit Server dialog box, configure the **Long Server Name, Physical Site, Internal OAM (Default) Address, External OAM Address, Signaling Address, Media Address, Operating System, Server Type, SNMP Profile, and Host Name**, parameters.
4. Click **Apply**.

---

**Variable Definitions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Server&gt;</td>
<td>This value is the server with which you want to associate an SNMP profile.</td>
</tr>
</tbody>
</table>

---

**Associating an SNMP profile with a server job aid**

This job aid lists and describes the parameters that you configure to associate an SNMP profile with a server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>(Read only) The name of the server—maximum of 6 characters.</td>
</tr>
<tr>
<td>Long Server Name</td>
<td>The descriptive long name of the server—maximum of 16 characters.</td>
</tr>
<tr>
<td>Physical Site</td>
<td>The physical site. (Select from the list.)</td>
</tr>
<tr>
<td>Internal OAM (Default) Address</td>
<td>This parameter (select from a list), specifies the address to use for traffic internal to the enclave.</td>
</tr>
<tr>
<td>External OAM Address</td>
<td>This optional parameter (select from a list) specifies the address to use for traffic external to the enclave.</td>
</tr>
<tr>
<td>Signaling Address</td>
<td>This optional parameter (select from a list) specifies the address to use for signaling traffic.</td>
</tr>
<tr>
<td>Media</td>
<td>This optional parameter (select from a list) specifies the address to use for bearer traffic.</td>
</tr>
<tr>
<td>Operating System</td>
<td>The operating system. (Select from the list.)</td>
</tr>
<tr>
<td>Server Type</td>
<td>The server type. (Select from the list.)</td>
</tr>
<tr>
<td>SNMP Profile</td>
<td>The server profile. (Select from the list.)</td>
</tr>
<tr>
<td>Host Name</td>
<td>The host name for the server.</td>
</tr>
</tbody>
</table>
Chapter 27: Performance management configuration

Operational measurements (OM) provide statistical information about the server operations and performance. This section provides the procedures you perform to configure OMs for the system.

Prerequisites

- A configured OSS server exists. For more information, see Configuring an OSS server on page 228 and Configuring an OSS endpoint on page 228.

OM configuration tasks

About this task

This task flow shows the sequence of procedures you perform to configure OMs for the system.
Configure OM storage rules to specify how the system stores OM record files.

Prerequisites

- You can access the AS 5300 Element Manager Console.
### Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Element Manager > Element Manager > OM Processing > OM Storage Rules**.

2. On the ElementManager OM Storage Rules window, click **Add (+)**.

3. In the Add OM Storage Rule dialog, configure the **Name** and **OM Type** values.


5. Click **Apply**.

6. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Fault Performance Manager > Fault Performance Manager Instance > OM Processing > OM Storage Rules**.

7. On the Fault Performance Manager OM Storage Rules window, click **Add (+)**.

8. In the Add OM Storage Rule dialog, configure the **Name** and **OM Type** values.


10. Click **Apply**.

### Configuring OM storage rules job aid

#### About this task

This job aid lists and describes the parameters that appear on the Add OM Storage Rule dialog box.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This parameter is the unique name that represents an OM storage rule under the context of a AS 5300 Element Manager or a Fault Performance Manager.</td>
</tr>
<tr>
<td>OM Type</td>
<td>This parameter (select from the list) specifies the format of OMs under this rule. The supported formats are: OTP and TRAFFIC. The OM data of OTP type are collected according to the Office Transfer Period. The OM data of TRAFFIC type are collected every 5 minutes.</td>
</tr>
<tr>
<td>Working Directory</td>
<td>This (read-only) parameter shows the working directory path for the storage of OM files—based on the current configuration of the log storage rule.</td>
</tr>
<tr>
<td>Rotation Size Enable</td>
<td>This parameter (check box) enables or disables rotation of log files by file size. Select the check box to enable rotation of OM files by file size.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rotation Size</td>
<td>This (text) value specifies the file size for rotation in megabytes—available only if the Rotation Size Enable check box is selected.</td>
</tr>
<tr>
<td>Rotation Period Enable</td>
<td>This parameter (check box) enables or disables rotation of OM files by time period. Select the check box to enable rotation of OM files by time period.</td>
</tr>
<tr>
<td>Rotation Period</td>
<td>This parameter specifies the number of minutes for rotation—available only if the Rotation Period Enable check box is selected.</td>
</tr>
<tr>
<td>Rotation OTP Enable</td>
<td>This parameter (check box) enables or disables rotation of OM files according to the configured office transfer period.</td>
</tr>
<tr>
<td>Rotation OTP</td>
<td>This (text) value specifies the office transfer period for OM file rotation—available only if the Rotation OTP Enable check box is selected.</td>
</tr>
<tr>
<td>Retention</td>
<td>This parameter (select from the list) specifies the number of days for which the system retains OM files. The options are 1–7 days.</td>
</tr>
<tr>
<td>Compression</td>
<td>This parameter (check box) enables or disables compression of log files. Select the check box to enable compression of OM files.</td>
</tr>
</tbody>
</table>

---

### Configuring the OM North-bound Server Feed rule

**About this task**

Configure the destinations of operational measurements (OM) records forwarded over a TCP connection to ensure that the AS 5300 Element Manager and Fault Performance Manager (FPM) forward secured OM records to the authorized OSS destinations only.

**Prerequisites**

- You can access the AS 5300 Element Manager Console.

**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Element Manager > Element Manager > OM Processing > OM North-bound Server Feed Rules**.
2. On the ElementManager OM North-bound Server Feed Rules window, click **Add (+)**.
3. In the Add OM North-bound Server Feed Rule dialog, configure the **Name** and **OM Type** values.
4. In the **North Bound Feed Rule** section, configure the **Local Port** and **ACL Validation** values.
5. Click **>>** to move selected available OSS servers to the **OSS Servers** pane.
6. Click **<<** to remove selected OSS servers.
7. Click **Apply**.
8. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Fault Performance Manager > Fault Performance Manager > , OM Processing > OM North-bound Server Feed Rules.**

9. On the FaultPerformance OM North-bound Server Feed Rules window, click **Add (+).**

10. In the Add OM North-Bound Server Feed Rule dialog, configure the **Name** and **OM Type** values.

11. In the **North Bound Feed** section, configure the **Local Port** and **ACL Validation** values.

12. Click **>>** to move selected available OSS servers to the **OSS Servers** pane.

13. Click **<<** to remove selected OSS servers.

14. Click **Apply.**

---

**Configuring the OM North-bound Server Feed rule job aid**

*About this task*

This job aid lists and describes the fields that appear on the Add OM North-bound Server Feed Rule dialog box.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This parameter is the unique name that represents a log North-bound Server Feed rule under the context of a AS 5300 Element Manager or a Fault Performance Manager.</td>
</tr>
<tr>
<td>OM Type</td>
<td>This parameter (select from the list) specifies the format of OMs under this rule. The supported formats are: OTP and TRAFFIC. The OM data of type OTP are collected for each Office Transfer Period. The OM data of type TRAFFIC are collected every 5 minutes.</td>
</tr>
<tr>
<td>Local Port</td>
<td>This (text) parameter specifies the TCP listening port in the AS 5300 Element Manager or FPM for OM forwarding to OSS servers.</td>
</tr>
<tr>
<td>ACL Validation</td>
<td>This parameter (check box) enables or disables access control list validation of OSS servers for log forwarding.</td>
</tr>
<tr>
<td>OSS Servers</td>
<td>This parameter specifies the authorized OSS servers for log forwarding.</td>
</tr>
<tr>
<td>Available OSS Servers</td>
<td>This parameter lists the available OSS servers for log forwarding.</td>
</tr>
</tbody>
</table>

---

**Configuring OM FTP Push rules**

*About this task*

Configure OM FTP Push rules to specify the destinations of FTP Push and ensure that the system forwards OM files to the authorized OSS destinations only.
Prerequisites

- You can access the AS 5300 Element Manager Console.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Element Manager > Element Manager > OM Processing > OM FTP Push Rules.
3. In the Add OM FTP Push Rule dialog, configure the Name, OM Storage Rule, and FTP Push Destination values.
4. Click Apply.
5. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Fault Performance Manager > Fault Performance Manager > OM Processing > OM FTP Push Rules.
7. In the Add OM FTP Push Rule dialog, configure the Name, OM Storage Rule, and FTP Push Destination values.
8. Click Apply.

Configuring OM FTP Push rules job aid

About this task

This job aid lists and describes the parameters that appear on the Add OM FTP Push Rule dialog box.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This parameter (text) is a unique name to represent an OM FTP Push rule under the context of a AS 5300 Element Manager or a Fault Performance Manager.</td>
</tr>
<tr>
<td>OM Storage Rule</td>
<td>This parameter (select from the list) specifies a configured OM storage rule and determines the source of OM files to FTP Push under this rule.</td>
</tr>
<tr>
<td>FTP Push Destination</td>
<td>This parameter (select from the list) specifies a configured OM 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.</td>
</tr>
</tbody>
</table>

Enabling and disabling OM processing rules

About this task

Enable or disable Operational Measurement (OM) processing rules to determine which rules apply.
Prerequisites

- You can access the AS 5300 Element Manager Console.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Element Managers > Element Manager > OM Processing > OM Rules Maintenance**.

2. On the Element Manager OM Processing Rules Maintenance window, select a tab.

<table>
<thead>
<tr>
<th>To enable or disable</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>OM storage rules</td>
<td>Select the Storage tab.</td>
</tr>
<tr>
<td>OM North-bound Server Feed rules</td>
<td>Select the North-bound Server Feed tab.</td>
</tr>
<tr>
<td>OM FTP Push rules</td>
<td>Select the FTP Push tab.</td>
</tr>
</tbody>
</table>

3. Select a rule.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the selected rule.</td>
<td>Click Enable.</td>
</tr>
<tr>
<td>Disable the selected rule.</td>
<td>Click Disable.</td>
</tr>
</tbody>
</table>

4. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Fault Performance Managers > Fault Performance Manager > OM Processing > OM Rules Maintenance**.

5. On the OM Processing Rules Maintenance window, select a tab.

<table>
<thead>
<tr>
<th>To manage</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>OM storage rules</td>
<td>Select the Storage tab.</td>
</tr>
<tr>
<td>OM North-bound Server Feed rules</td>
<td>Select the North-bound Server Feed tab.</td>
</tr>
<tr>
<td>OM FTP Push rules</td>
<td>Select the FTP Push tab.</td>
</tr>
</tbody>
</table>

6. Select a rule.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the selected rule.</td>
<td>Click Enable.</td>
</tr>
<tr>
<td>Disable the selected rule.</td>
<td>Click Disable.</td>
</tr>
</tbody>
</table>

---

**Enabling and disabling OM processing rules job aid**

**About this task**

The following table lists and describes the columns that appear on the OM Processing Maintenance panel.
<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This column contains the unique names of the processing rules.</td>
</tr>
<tr>
<td>OM Type</td>
<td>This column contains the names of the OM types associated with the processing rules.</td>
</tr>
<tr>
<td>Admin</td>
<td>This column contains the administrative states of the rules. The value is either ENABLED or DISABLED.</td>
</tr>
</tbody>
</table>
Chapter 28: Accounting records configuration

Network elements generate accounting records for events that occur during service and session processing. This section provides the procedures that you perform to configure how the system manages accounting records.

Prerequisites

- A configured OSS server exists. For more information, see Configuring an OSS server on page 228 and Configuring an OSS endpoint on page 228.

Accounting records configuration procedures

About this task

This task flow shows the sequence of procedures you perform to configure how the system manages accounting records for the system.
Accounting records configuration

Navigation

- Configuring accounting storage rules on page 217
- Configuring the accounting North-bound Server Feed rule on page 218
- Configuring Accounting FTP Push rules on page 219
- Configuring FTP Push destinations on page 229
- Enabling and disabling accounting processing rules on page 220
Configuring accounting storage rules

About this task
Configure accounting storage rules to specify how the system stores accounting record files.

Prerequisites
• You can access the AS 5300 Element Manager Console.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Accounting Managers > <Accounting Manager Instance> > RU Processing > Accounting Storage Rules.
2. On the <Accounting Manager Instance> Accounting Storage Rules window, click Add (+).
3. In the Add Accounting Storage Rule dialog, configure the Name and Accounting Format values.
4. In the Storage Policy section, configure the Rotation Size Enabled, Rotation Size, Rotation Period Enabled, Rotation Period, Retention, and Compression values.
5. Click Apply.

Configuring accounting storage rules job aid

About this task
This job aid lists and describes the parameters that appear on the Add Accounting Storage Rule dialog box.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This parameter is the unique name that represents an accounting storage rule under the context of an Accounting Manager.</td>
</tr>
<tr>
<td>Accounting Format</td>
<td>This parameter (select from the list) specifies the format of accounting records under this rule. The supported formats are: MCPV3, MCPV4, and MCPV5.</td>
</tr>
<tr>
<td>Working Directory</td>
<td>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.</td>
</tr>
<tr>
<td>Rotation Size Enable</td>
<td>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.</td>
</tr>
<tr>
<td>Rotation Size</td>
<td>This (text) value specifies the file size for rotation in megabytes—available only if the Rotation Size Enable check box is selected.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rotation Period Enable</td>
<td>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.</td>
</tr>
<tr>
<td>Rotation Period</td>
<td>This parameter specifies the number of minutes for rotation—available only if the Rotation Period Enable check box is selected.</td>
</tr>
<tr>
<td>Retention</td>
<td>This parameter (select from the list) specifies the number of days for which the system retains accounting files. The options are 1–7 days.</td>
</tr>
<tr>
<td>Compression</td>
<td>This parameter (check box) enables or disables compression of log files. Select the check box to enable compression of accounting files.</td>
</tr>
</tbody>
</table>

### Configuring the accounting North-bound Server Feed rule

**About this task**

Every network element (NE) that generates accounting records reports to an Accounting Manager (AM). Configure the destinations of accounting records forwarded over a TCP connection.

**Before you begin**

- You can access the AS 5300 Element Manager Console.

**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Accounting Manager > [Accounting Manager Instance] > RU Processing > Accounting North-bound Server Feed Rules**.
2. On the **<Accounting Manager Instance> Accounting North-bound Server Feed Rules** window, click **Add (+)**.
3. In the **Add Accounting North-bound Server Feed Rule** dialog, configure the **Name** and **Accounting Format** values.
4. In the **North Bound Server Feed Rule** section, configure the **Local Port** and **ACL Validation** values.
5. Click **>>** to move selected available OSS servers to the **OSS Servers** pane.
6. Click **<<** to remove selected OSS servers.
7. Click **Apply**.

### Configuring the accounting North-bound Server Feed rule job aid

**About this task**

This job aid lists and describes the parameters that appear on the Add Accounting North-bound Server Feed Rule dialog box.
### Configuring Accounting FTP Push rules

#### About this task

Configure Accounting FTP Push rules to specify the destinations of FTP Push and ensure that the system forwards Accounting files to the authorized OSS destinations only.

#### Prerequisites

- You can access the AS 5300 Element Manager Console.

#### Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Accounting Manager > <Accounting Manager Instance> > RU Processing > Accounting FTP Push Rules**.
2. On the Accounting FTP Push Rules window, click **Add (+)**.
3. In the Add Accounting FTP Push Rule dialog, configure the **Name**, **Accounting Storage Rule**, and **FTP Destination** values.
4. Click **Apply**.

---

### Configuring Accounting FTP Push rules job aid

#### About this task

This job aid lists and describes the parameters that appear on the Add Accounting FTP Push Rule dialog box.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This parameter is the unique name that represents an accounting North-bound Server Feed rule under the context of an Accounting Manager.</td>
</tr>
<tr>
<td>Accounting Format</td>
<td>This parameter (select from the list) specifies the format of accounting records under this rule. The supported formats are: MCPV3, MCPV4, and MCPV5.</td>
</tr>
<tr>
<td>Local Port</td>
<td>This (text) parameter specifies the TCP listening port in the AM for forwarding to OSS servers.</td>
</tr>
<tr>
<td>ACL Validation</td>
<td>This parameter (check box) enables or disables access control list validation of OSS servers for forwarding accounting files.</td>
</tr>
<tr>
<td>OSS Servers</td>
<td>This parameter specifies the authorized OSS servers for forwarding accounting files.</td>
</tr>
<tr>
<td>Available OSS Servers</td>
<td>This parameter lists the available OSS servers for forwarding accounting files.</td>
</tr>
</tbody>
</table>
### Parameter Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This parameter (text) is a unique name to represent an Accounting FTP Push rule under the context of an Accounting Manager.</td>
</tr>
<tr>
<td>Accounting Storage Rule</td>
<td>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.</td>
</tr>
<tr>
<td>FTP Push Destination</td>
<td>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.</td>
</tr>
</tbody>
</table>

## Enabling and disabling accounting processing rules

### About this task

Enable or disable accounting processing rules to determine which rules apply.

### Prerequisites

- You can access the AS 5300 Element Manager Console.

### Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Elements > Accounting Managers > <Accounting Manager> > RU Processing > Accounting Rules Maintenance**.

2. On the Accounting Processing Rules Maintenance window, select a tab.

<table>
<thead>
<tr>
<th>To enable or disable</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting storage rules</td>
<td>Select the Storage tab.</td>
</tr>
<tr>
<td>Accounting North-bound Server Feed</td>
<td>Select the North-bound Server Feed tab.</td>
</tr>
<tr>
<td>Accounting FTP Push rules</td>
<td>Select the FTP Push tab.</td>
</tr>
</tbody>
</table>

3. Select a rule.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the selected rule.</td>
<td>Click Enable.</td>
</tr>
<tr>
<td>Disable the selected rule.</td>
<td>Click Disable.</td>
</tr>
</tbody>
</table>

### Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Accounting Manager&gt;</td>
<td>This value is the name of Accounting Manager element for which you want to enable or disable accounting processing rules. Example: AM1</td>
</tr>
</tbody>
</table>
Enabling and disabling accounting processing rules job aid

About this task

The following table lists and describes the columns that appear on the Accounting Processing Maintenance panel.

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This column contains the unique names of the processing rules.</td>
</tr>
<tr>
<td>Accounting Format</td>
<td>This column contains the names of the accounting formats associated with the processing rules.</td>
</tr>
<tr>
<td>Admin State</td>
<td>This column contains the administrative states of the rules. The value is either ENABLED or DISABLED.</td>
</tr>
</tbody>
</table>
Chapter 29: DNS configuration

About this task
You must configure DNS on all the AS 5300 servers hosting the Session Managers, Provisioning Managers and Personal Agents if XMPP Gateway feature is enabled.

Related links
Configuring DNS on page 222

Configuring DNS
Use this procedure to configure the DNS for the system to support the XMPP Gateway.

Note:
The DNS configuration files are backed up and restored as part of regular AS 5300 server backup and restore operations.

Before you begin
You must be the root user or a user with SSA role with sudo privileges.

Procedure
1. Log in using the ntsysadm credentials.
2. Type su root.
3. At the command prompt, type updateDNSSettings.
   The system displays the following menu:
   DNS Management Options:
   [1] Show DNS configuration
   [2] Modify DNS configuration
   [3] Save DNS configuration
   [4] Exit
4. Type 2.
   The system displays: Do you want to configure DNS Suffixes? (Y/N).
5. Type Y.
   The system displays the following menu:
   Please select one of the following actions:
   - [A]dd Domain Suffix(es)
   - Accept the Domain Suffix(es) and [C]ontinue with nameserver configuration

6. Type A.

7. Enter the domain suffix.
   The system displays the following menu:
   Please select one of the following actions:
   - [A]dd Domain Suffix(es)
   - [R]emove Domain Suffix(es)
   - Accept the Domain Suffix(es) and [C]ontinue with nameserver configuration

8. Type C.
   The system displays: Do you want to configure DNS Servers? (Y/N).

9. Type Y.
   The system displays the following:
   DNS server(s):
   1. not configured
   2. not configured
   3. not configured
   Please select one of the following actions:
   - [M]odify DNS server
   - Accept the nameserver configuration and [D]one with the DNS Client configuration

10. Type M to modify the DNS servers.

11. Enter IP addresses for the primary, secondary, and tertiary DNS servers.

12. Save the DNS configuration.

Related links
    DNS configuration on page 222
Chapter 30: Common procedures

About this task

The following sections describe common procedures that you use to configure the system.

- Starting a network element on page 224
- Stopping a network element on page 225
- Deploying a network element on page 226
- Undeploying a network element on page 226
- Restarting a network element on page 227
- Configuring an OSS server on page 228
- Configuring an OSS endpoint on page 228
- Configuring FTP Push destinations on page 229

Starting a network element

About this task

Perform this procedure to start a network element instance.

Prerequisites

- You can access the AS 5300 Element Manager Console.
- You have NEService privileges.

Procedure

1. In the configuration view of the AS 5300 Element Manager Console, select Network Elements > <NE type> > <NE instance> > NE Maintenance.
2. In the Maintenance panel, select the network element to start, and click Start.
   The time required to complete the process depends on the network element type and the hosting server.
3. (Optional) To view the maintenance and operational states of the transition, click Details.
### Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;NE type&gt;</code></td>
<td>This value is the type of network element, such as Accounting Managers.</td>
</tr>
<tr>
<td><code>&lt;NE instance&gt;</code></td>
<td>This is the network element, such as the Accounting Manager.</td>
</tr>
</tbody>
</table>

### Stopping a network element

Perform this procedure to stop a network element instance.

**Important:**

- When the AS 5300 Element Manager stops, your AS 5300 Element Manager Console window closes.
- When an Avaya Aura® MS NE stops, any conference recordings that are in progress, are lost.

**Before you begin**

- You can access the AS 5300 Element Manager Console.
- You have NEService privileges.

**Procedure**

1. In the configuration view of the AS 5300 Element Manager Console, select **Network Elements > `<NE type>` > `<NE instance>` > NE Maintenance.**
2. In the Maintenance panel, select the network element to stop, and click **Stop.**
   
   The time required to complete the process depends on the network element type and the hosting server.

### Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;NE type&gt;</code></td>
<td>This value is the type of network element, such as Accounting Managers.</td>
</tr>
<tr>
<td><code>&lt;NE instance&gt;</code></td>
<td>This is the network element, such as the Accounting Manager.</td>
</tr>
</tbody>
</table>
Deploying a network element

About this task
Perform this procedure to deploy a network element instance.

Prerequisites
• An NE must be OFFLINE before you can deploy it.
• You can access the AS 5300 Element Manager Console.
• You must have NEService privileges.

Procedure
1. In the configuration view of the AS 5300 Element Manager Console, select Network Elements > <NE type> > <NE instance> > NE Maintenance.
2. In the Maintenance window, select the network element, and then click Deploy.
   The time required to complete the process depends on the network element type and the hosting server.

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;NE type&gt;</td>
<td>This value is the type of network element, such as Accounting Managers.</td>
</tr>
<tr>
<td>&lt;NE instance&gt;</td>
<td>This is the network element, such as the Accounting Manager.</td>
</tr>
</tbody>
</table>

Undeploying a network element

About this task
Perform this procedure to undeploy a network element instance.

Prerequisites
• An NE must be OFFLINE before you can undeploy it.
• You can access the AS 5300 Element Manager Console.
• You must have NEService privileges.

Procedure
1. In the configuration view of the AS 5300 Element Manager Console, select Network Elements > <NE type> > <NE instance> > NE Maintenance.
2. In the Maintenance window, select the network element, and then click Undeploy.
   The time required to complete the process depends on the network element type and the hosting server.
**Variable Definitions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;NE type&gt;</td>
<td>This value is the type of network element, such as Accounting Managers.</td>
</tr>
<tr>
<td>&lt;NE instance&gt;</td>
<td>This is the network element, such as the Accounting Manager.</td>
</tr>
</tbody>
</table>

---

**Restarting a network element**

**About this task**

The Restart operation performs a combined stop and start. During the period of the restart, the network element instance does not provide service. There is no difference between performing a restart, or stopping and starting a network element (NE) instance. Restart a network element instance to apply configuration changes, or as a troubleshooting step.

⚠️ **Important:**

You cannot restart the active AS 5300 Element Manager from the AS 5300 Element Manager Console. To restart the active AS 5300 Element Manager, you must use the command line interface. When the AS 5300 Element Manager stops, your AS 5300 Element Manager Console window closes.

**Prerequisites**

- You can access the AS 5300 Element Manager Console.

**Procedure**

1. In the configuration view of the AS 5300 Element Manager Console, select **Network Elements > <NE type> > <NE instance> > NE Maintenance**.
2. From the Maintenance panel, select the instance to restart, and click **Restart**.
3. To confirm the restart, click **Yes**.

---

**Variable Definitions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;NE type&gt;</td>
<td>This value is the type of network element, such as Accounting Managers.</td>
</tr>
<tr>
<td>&lt;NE instance&gt;</td>
<td>This is the network element, such as the Accounting Manager.</td>
</tr>
</tbody>
</table>
Configuring an OSS server

About this task
Perform this procedure to configure an Operational Support System (OSS) server, to ensure that the system forwards log, OM, and accounting records to authorized OSS destinations.

Prerequisites
- You can access the AS 5300 Element Manager Console
- The OSS server is operational.
- The address of the OSS server exists in the address table.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > OAM Profiles > OSS Servers.
2. On the OSS Servers window, click Add (+).
3. On the Add OSS Server dialog, configure the Name, Node and Use External OAM Network parameters.
4. Click Apply.

Configuring OSS servers job aid

About this task
This job aid lists and describes the parameters that appear on the Configuring OSS servers dialog box.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the OSS server (between 1–16 characters).</td>
</tr>
<tr>
<td>Address</td>
<td>The logical name associated with the address of the OSS server.</td>
</tr>
</tbody>
</table>

Configuring an OSS endpoint

About this task
Perform this procedure to configure an OSS endpoint.

Prerequisites
- You can access the AS 5300 Element Manager Console
- A configured OSS server exists. For more information, see Configuring an OSS server on page 228.
- The OSS server is operational.
Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > OAM Profiles > OSS Endpoints**.
2. In the OSS Endpoints window, click **Add (+)**.
3. In the Add OSS Endpoint dialog, configure the **Name**, **Server**, and **Port** parameters.
4. Click **Apply**.

### Configuring an OSS endpoint job aid

**About this task**

This job aid lists and describes the OSS Endpoints parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name to represent the OSS endpoint (1–16 characters).</td>
</tr>
<tr>
<td>Server</td>
<td>The name of a configured OSS server (select from the list).</td>
</tr>
<tr>
<td>Port</td>
<td>The port number for the endpoint.</td>
</tr>
</tbody>
</table>

### Configuring FTP Push destinations

**About this task**

Configure log FTP Push destinations to specify the destinations of FTP Push and ensure that the system forwards security log files to the authorized OSS destinations only.

**Prerequisites**

- You can access the AS 5300 Element Manager Console
- A configured OSS endpoint exist. For more information, see **Configuring an OSS endpoint** on page 228.

**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > OAM Profiles > FTP Push Destinations**.
2. On the **FTP Push Destinations** window, click **Add (+)**.
4. Click **Apply**.
Configuring log FTP Push destinations job aid

About this task

This job aid lists and describes the parameters that appear on the Add FTP Push Destinations dialog box.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This parameter (text) is a unique name to represent an FTP Push Destination under the context of AS 5300 Element Manager.</td>
</tr>
<tr>
<td>OSS Endpoint</td>
<td>This parameter (select from the list) is a configured OSS endpoint. This determines the destination IP address and port to use with FTP push.</td>
</tr>
<tr>
<td>Root Directory</td>
<td>This parameter (text) specifies the destination directory on the OSS server, in which to place records.</td>
</tr>
<tr>
<td>User ID</td>
<td>This parameter (text) is a valid account for the OSS server.</td>
</tr>
<tr>
<td>Password</td>
<td>This parameter (text) is the password for FTP log on.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>This parameter (text) is the password for FTP log on—repeated to reduce typing error issues.</td>
</tr>
<tr>
<td>Replicate</td>
<td>This parameter (check box) specifies whether to replicate the source directory structure at the destination.</td>
</tr>
</tbody>
</table>