Administering Avaya Aura® Application Enablement Services
© 2015-2020, 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
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 any 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/

"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) for more information.

 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 expressly 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
Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order, or 2) up to the number of Instances of the Software as indicated in the order. Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User. You, through electronic means established by Avaya specifically for this purpose.

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

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

END USER AGREES TO INDUCE AND HOLD AVAYA, ITS AFFILIATES, ANY AVAYA CHANNEL PARTNER AND ANYONE ELSE USING OR SELLING THE SOFTWARE, THEIR AGENTS, SERVANTS AND EMPLOYEES, HARMLESS AGAINST ALL CLAIMS, LAWSUITS, DEMANDS AND JUDGMENTS ARISING OUT OF, OR IN CONNECTION WITH, THE USE OF THE SOFTWARE, OR INFRINGEMENT OF ANY THIRD PARTY RIGHTS ARISING OUT OF ANY USE OF THE SOFTWARE OR ANY PERFORMANCE THEREOF. END USER AGREES TO INDEMNIFY AND HOLD AVAYA, ITS AFFILIATES, ANY AVAYA CHANNEL PARTNER AND ANYONE ELSE USING OR SELLING THE SOFTWARE, THEIR AGENTS, SERVANTS AND EMPLOYEES, HARMLESS AGAINST ALL CLAIMS, LAWSUITS, DEMANDS AND JUDGMENTS ARISING OUT OF, OR IN CONNECTION WITH, THE USE OF 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. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"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. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product, in whole or in part, including any code and software. The Third Party Partner acknowledges and agrees the Avaya Channel Partner is responsible for any and all related fees and/or royalties. The H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, LLC. 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.

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

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.
Trade marks

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.

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

Chapter 1: Introduction .......................................................................................................... 15
  Purpose................................................................................................................................. 15
  Change history...................................................................................................................... 15

Chapter 2: Administering Application Enablement Services ...................................................... 18
  Administering Communication Manager for Application Enablement Services ................ 18
    Communication Manager administrative checklists.......................................................... 18
    Communication Manager administration for DMCC - network regions............................ 23
    Adding CLANs to the network............................................................................................ 24
    Enabling AE Services......................................................................................................... 25
    Enabling Processor Ethernet............................................................................................... 27
    Administering UCIDs in Communication Manager (TSAPI and JTAPI applications) .......... 27
    Administering a CTI Link for CVLAN............................................................................... 28
    Administering a CTI Link for CVLAN (internal applications)............................................. 28
    Administering a CTI Link for DLG.................................................................................... 29
    Administering a CTI Link for TSAPI, JTAPI, DMCC with Call Control, Telephony Web
    Service, or an AE Services integration............................................................................... 29
    Checking the status of a switch connection -- from Communication Manager to the AE
    Services server.................................................................................................................. 30
    DMCC settings................................................................................................................... 30
    DMCC station registration modes....................................................................................... 30
    Main dependency mode..................................................................................................... 31
    Administering an extension exclusively for the DMCC softphone.................................... 31
    Dependent and Independent dependency modes............................................................... 32
    Administering an extension number for the station that an application monitors............... 33
    Media Content and Media Tone Announcement for DMCC............................................... 33
    About Share Talk............................................................................................................... 34
    Network regions for DMCC............................................................................................... 34
    About signaling encryption............................................................................................... 36
    Adding a media processor circuit pack to the network....................................................... 38
    Sample Communication Manager and DMCC configuration............................................. 38
    Sample Communication Manager administration screens.............................................. 40

Chapter 3: AE Services administration ..................................................................................... 51
  AE Services Management Console - certificates and security alerts.................................... 53
  Browser security................................................................................................................. 54
  Using own Certificate Authority........................................................................................... 54
  Importing the CA certificate into your browser’s certificate store...................................... 55
  Logging in to AE Services as the system administrator......................................................... 55
  Checklists for administering the services that run on the AE Services server...................... 57
  CVLAN - checklist............................................................................................................. 57
Chapter 4: AE Services Secure Mode

AE Services secure mode

AE Services command line utilities for standard and secure mode

Enabling AE Services secure mode

Disabling AE Services secure mode
Chapter 5: Certificate Management ................................................................. 97
Certificate management ................................................................................. 97
Overview of certificate management .............................................................. 98
Using certificates issued by a certificate authority ........................................ 100
Certificate enrollment and installation .......................................................... 100
Certificate authentication between the AE Services server and Communication Manager .................................................. 118

Chapter 6: AE Services general maintenance ................................................... 120
Backing up the server data ........................................................................... 120
Restoring the server data ............................................................................. 121
Restoring the server data by using the command line interface ..................... 121
Logs ............................................................................................................ 122
Viewing log files ......................................................................................... 123
Downloading log files .................................................................................. 123
Service Controller (start, stop, and restart services) ..................................... 124
Schematic view of an AE Services configuration ........................................... 125
About stopping services .............................................................................. 126
Restarting the AE Services server and the web server .................................. 127
About rsyslog ............................................................................................... 128
About System Logging ................................................................................. 129
Configuring remote logging ........................................................................ 129
System Logging field descriptions ................................................................. 129
Configuring the trace or logging levels ......................................................... 130
About log and trace retention ...................................................................... 131
Retaining the log and trace files .................................................................. 132
Clearing the log files ................................................................................... 133
Clearing the trace files ............................................................................... 134
Retaining logs by using the command line interface ..................................... 134
Retaining traces by using the command line interface .................................. 135
Clearing logs by using the command line interface ..................................... 135
Clearing traces by using the command line interface .................................. 135

Chapter 7: User Administration ...................................................................... 136
User management for authentication .............................................................. 136
DMCC AA policy administration and bypassing user authentication ............. 137
User Management for authorization .............................................................. 137
Logging into User Management ................................................................... 138
The cust account in User Management ......................................................... 138
Viewing the list of all users in the User Management database ....................... 138
Adding a user to User Management ............................................................. 139
Editing a user in User Management ............................................................. 139
Chapter 8: Security Administration and Additional PAM Management

About Security Administration and additional PAM management........................................164
Security administration........................................................................................................164
Account Management - Linux user accounts......................................................................166
Adding a local Linux account for an administrator.............................................................166
Results of adding a local Linux account for an administrator - sample..............................168
Changing the properties of a Linux administrative account -- modify login.......................170
Contents

Results of changing role assignments for aesadmin3 - sample............................................... 170
Removing a Linux account - Remove Login.............................................................................. 171
Locking or unlocking a Linux account ...................................................................................... 172

PAM Management....................................................................................................................... 172
  Administering the PAM Password Manager.............................................................................. 173
  Creating a PAM Issue (/etc/issue) message............................................................................ 175
  Creating a PAM MOTD (/etc/motd) message......................................................................... 176
  Adding PAM limits................................................................................................................... 176
  Administering PAM time.......................................................................................................... 177

Support for Enhanced Access Security Gateway................................................................. 178
  Enabling or disabling EASG through the CLI interface........................................................ 178
  Enabling or disabling EASG through the AE Services Management Console interface....... 179
  Viewing the EASG certificate information.............................................................................. 180
  EASG product certificate expiration....................................................................................... 180
  EASG site certificate................................................................................................................ 180

Login reports............................................................................................................................... 181
  Displaying a login report for all Linux accounts................................................................. 182
  List Local Host Logins page field descriptions...................................................................... 182
  Displaying a login report for a specific login ID................................................................. 182
  Display Login Information page field descriptions.............................................................. 183
  Enabling a login audit............................................................................................................. 184
  Unused Login Audit page field descriptions.......................................................................... 184

AE Services client applications additional authentication methods.................................. 184
  Linux authentication............................................................................................................. 185
  Changing to Linux PAM Authentication for the AE Services client application............... 186
  Changing to User Management Authentication for the AE Services client application....... 186
  Enterprise directory settings in the AE Services Management Console............................. 186
  Enterprise directory configuration settings for AE Services integrations........................... 187
  Enterprise directory configuration settings with bridged appearance alert blocking............ 187
  Enterprise directory user authorization policy for DMCC applications.............................. 187
  Changing to Active Directory Authentication for the AE Services client application.......... 188

Configuring AE Services to access an enterprise directory.................................................. 189
  Configuring an external LDAP server — Windows............................................................... 190
  User roles............................................................................................................................... 191

Authentication with Microsoft Active Directory Services and Kerberos.......................... 192
  Sample procedures for integrating AE Services with ADS using Kerberos......................... 193
    Creating an account for the AE Services server on the Domain Controller....................... 193
    Generating a keytab file for the AE Server account on the Domain Controller................ 194
    Installing the Kerberos5 RPMs on the AE Server.............................................................. 194
    Editing the Kerberos 5 configuration file on the AE Server............................................. 195
    Importing the keytab file on the AE Server...................................................................... 196
  Administering the time-out period for console and HTTP sessions.................................. 196

Chapter 9: Data Encryption....................................................................................................... 198
Remote Key Server................................................................................................. 199
Data Encryption password policy........................................................................ 199
Data encryption commands................................................................................ 199
  encryptionPassphrase command...................................................................... 200
  encryptionRemoteKey command...................................................................... 202
Adding remote key server.................................................................................. 202
Removing remote key server............................................................................. 203
Displaying remote key server and slot assignment.......................................... 203
encryptionLocalKey command.......................................................................... 204
Enabling local key store..................................................................................... 204
Disabling local key store.................................................................................... 205
Viewing data encryption status.......................................................................... 205

Chapter 10: Fault Tolerance Configuration.......................................................... 206
Fault Tolerance.................................................................................................. 206
Fault Tolerance Configuration Checklist.......................................................... 206
Enabling Fault Tolerance.................................................................................... 207
Configuring Fault Tolerance on AE Services virtual machine............................ 207

Chapter 11: Security Database............................................................................ 209
The Security Database....................................................................................... 209
  APIs that use the Security Database............................................................... 209
  Enabling the Security Database - TSAPI, JTAPI, and Telephony Web Service.. 209
  DMCC applications and SDB authorization.................................................... 210
  Enabling the SDB for DMCC applications...................................................... 211
  TSAPI properties............................................................................................ 211
  Configuring TSAPI Properties....................................................................... 212
  About granting additional permissions......................................................... 213
  Security Database objects.............................................................................. 215
  Sample SDB Administration scenario - setting up a permission scheme based... 222
  Sample Configurations................................................................................... 225

Chapter 12: Licensing......................................................................................... 230
Licensing configurations..................................................................................... 230
Reserving unified desktop licenses.................................................................... 230
Reserving TSAPI user licenses.......................................................................... 232
Embedded Avaya WebLM Server....................................................................... 233
HTTPS, WebLM, and AE Services..................................................................... 234
Connecting to Avaya WebLM server.................................................................. 235
Reserving DMCC licenses.................................................................................. 236

Chapter 13: Administration from the operating system command prompt......... 238
AE Services Administration from the Operating System Command Prompt....... 238
  Accounts for Avaya Services technicians...................................................... 238
  Adding a Linux user....................................................................................... 239
  Using Tripwire............................................................................................... 240
Changing the default password for the cust account in User Management ............................... 333
Creating a new User Management administrator account and removing the default avaya account from User Management ........................................................................................................ 334
Creating a new System Administrator account and removing the default cust account from User Management ........................................................................................................ 335

Chapter 24: Sample Device, Media, and Call Control applications .................................. 337
Sample application files on the AE Services server ................................................................ 337
About the sample DMCC applications .................................................................................. 337
Preparing to run the sample application ............................................................................... 338
Administering AE Services for the sample application ......................................................... 338
Editing the tutorial properties file .......................................................................................... 339
Running the sample application ............................................................................................. 340
Troubleshooting the sample application ................................................................................ 341
Testing a DMCC configuration ............................................................................................... 342

Chapter 25: Avaya Computer Telephony and CVLAN migration ........................................... 343
TSAPI Client settings ............................................................................................................... 343
Migrating Avaya Computer Telephony users to AE Services ................................................ 343
Use User Management to add a CTI user ............................................................................. 344
Alternative migration strategies for Avaya Computer Telephony ........................................... 345
Avaya Computer Telephony bronze level integration ........................................................... 345
Bronze level integration with Active Directory Services ....................................................... 346
Avaya Computer Telephony silver level integration ............................................................. 347
Silver level integration with Active Directory Services ......................................................... 348
Avaya Computer Telephony gold level integration ............................................................... 349
Gold level integration with Active Directory Services ......................................................... 350
Migrating CVLAN to AE Services ......................................................................................... 351
Migrating CVLAN Server for Linux (Releases 9.0 and 9.1) to AE Services ......................... 351
Migrating the MAPD-based CVLAN to AE Services ............................................................ 352

Chapter 26: System Manager Trust Management ................................................................. 355
Using Avaya Aura® System Manager as a Certificate Authority (CA) to generate signed certificates ....................................................................................................................... 355
Creating the AE Services server certificate .......................................................................... 356
Downloading the SMGR CA certificate that signed the AE Services server certificate ............ 356
Importing the SMGR CA certificate into the AE Services server ....................................... 357
Importing the new AE Services server certificate into the AE Services server .................... 357
HTTPS, WebLM, and AE Services ......................................................................................... 357

Chapter 27: OpenSSL as a Certificate Authority (CA) ......................................................... 359
Using OpenSSL as a Certificate Authority (CA) to generate signed certificates .................... 359
Setting up the OpenSSL CA .................................................................................................. 359
Creating the certificate directory structure ......................................................................... 359
Configuring the OpenSSL configuration file ....................................................................... 360
Creating the CA root key and self-signed certificate ........................................................... 362
# Chapter 1: Introduction

## Purpose

This document describes administrative tasks you will need to perform on Communication Manager as well as the AE Services server.

This document is intended for people who perform AE Services administration tasks such as backing up, restoring, and managing users.

## Change history

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>July 2020</td>
<td>Updated the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- [Administering the Geo Redundant High Availability (GRHA)] on page 270</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <a href="#">Licensing configurations</a> on page 230</td>
</tr>
<tr>
<td>6</td>
<td>June 2020</td>
<td>Updated the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <a href="#">Reserving unified desktop licenses</a> on page 230</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <a href="#">AEServicesSNMPtrapsAlarmCodesAndMessages_Part1</a> on page 258</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <a href="#">Licensing configurations</a> on page 230</td>
</tr>
<tr>
<td>5</td>
<td>April 2020</td>
<td>Updated the <a href="#">Connecting to Avaya WebLM server</a> on page 235 section.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Summary of changes</th>
</tr>
</thead>
</table>
| 4     | January 2020 | Added the following sections:  
  • [About log and trace retention](#) on page 131  
  • [Retaining the log and trace files](#) on page 132  
  • [Retaining logs by using the command line interface](#) on page 134  
  • [Retaining traces by using the command line interface](#) on page 135  
  • [Clearing the log files](#) on page 133  
  • [Clearing the trace files](#) on page 134  
  • [Clearing logs by using the command line interface](#) on page 135  
  • [Clearing traces by using the command line interface](#) on page 135  
  • [Data Encryption](#) on page 198  
  • [Remote Key Server](#) on page 199  
  • [Data Encryption password policy](#) on page 199  
  • [encryptionPassphrase command](#) on page 200  
  • [Adding encryption passphrase](#) on page 200  
  • [Changing encryption passphrase](#) on page 200  
  • [Displaying encryption passphrase and slot assignment](#) on page 201  
  • [Removing encryption passphrase](#) on page 201  
  • [encryptionRemoteKey command](#) on page 202  
  • [Adding remote key server](#) on page 202  
  • [Removing remote key server](#) on page 203  
  • [Displaying remote key server and slot assignment](#) on page 203  
  • [encryptionLocalKey command](#) on page 204  
  • [Enabling local key store](#) on page 204  
  • [Disabling local key store](#) on page 205  
  • [Viewing data encryption status](#) on page 205  
Updated the following sections:  
  • [Administering the Geo Redundant High Availability (GRHA)](#) on page 270  

*Table continues...*
<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• <a href="#">AEServicesSNMPtrapsAlarmCodesAndMessages_Part2</a> on page 261</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">AEServicesSNMPtrapsAlarmCodesAndMessages_Part4</a> on page 266</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">User roles</a> on page 191</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Default accounts and AE Services Management Console access privileges</a> on page 324</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Default AE Services accounts</a> on page 327</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Restoring the server data by using the command line interface</a> on page 121</td>
</tr>
<tr>
<td>3</td>
<td>October 2019</td>
<td>Updated the following sections:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Using Tripwire</a> on page 240</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Administering the Geo Redundant High Availability (GRHA)</a> on page 270</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">The AE Services default certificate</a> on page 99</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Creating the certificate directory structure</a> on page 359</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Default AE Services accounts</a> on page 327</td>
</tr>
<tr>
<td>2</td>
<td>August 2019</td>
<td>Updated <a href="#">Restoring the server data by using the command line interface</a> on page 121 section.</td>
</tr>
<tr>
<td>1</td>
<td>June 2019</td>
<td>Release 8.1 document.</td>
</tr>
</tbody>
</table>
Chapter 2: Administering Application Enablement Services

Administering Communication Manager for Application Enablement Services

This chapter describes tasks that must be performed on Avaya Aura® Communication Manager to ensure that Communication Manager can communicate with the services running on the Application Enablement Services Server (AE Services Server).

🌟 Note:
To perform the tasks in this chapter use Avaya Site Administration in terminal emulation mode (using System Administration Terminal, or SAT, commands).

Communication Manager administrative checklists

Checklist - Communication Manager administration for a Device, Media and Call Control (DMCC) configuration that uses Registration Services and Call Information Services

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Check licensing</td>
<td>Use <code>display system-parameters customer-options</code> to browse through the Optional Features and ASAI Enhanced Features screens. Confirm that you have IP_STA and STA licenses (adding a station consumes these licenses).</td>
</tr>
</tbody>
</table>

🌟 Note:
If features are not enabled, contact your Avaya representative.
<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Add CLAN (or CLANs) or Enable Processor Ethernet</td>
<td>If you use a media server that uses CLANs, you must add CLANs to the network. See <a href="#">Adding CLANs to the network</a> on page 24. If you use a media server that uses Processor Ethernet, see <a href="#">Enabling Processor Ethernet</a> on page 27.</td>
</tr>
<tr>
<td>3</td>
<td>Enable AE Services</td>
<td>Required for the transport layer. See <a href="#">Enabling AE Services</a> on page 25</td>
</tr>
<tr>
<td>4</td>
<td>Add stations</td>
<td>See <a href="#">DMCC station registration modes</a> on page 30. If an application uses &quot;non-main dependency mode&quot;, you do not need to administer a station for the application.</td>
</tr>
<tr>
<td>5</td>
<td>Set up a network region</td>
<td>Requires network planning. See <a href="#">Network regions for DMCC</a> on page 34.</td>
</tr>
<tr>
<td>6</td>
<td>Add DMCC softphones to the network region</td>
<td>See <a href="#">Methods for adding DMCC softphones to the network region</a> on page 37.</td>
</tr>
<tr>
<td>7</td>
<td>Add a media gateway to the network</td>
<td>See <a href="#">Guidelines for adding a media gateway to the network</a> on page 37.</td>
</tr>
<tr>
<td>8</td>
<td>Add a media processor</td>
<td>See <a href="#">Adding a media processor circuit pack to the network</a> on page 38.</td>
</tr>
</tbody>
</table>

**Checklist - Communication Manager administration for a DMCC configuration that uses Call Control Services or 3rd party call control**

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1   | Check licensing                                         | Use `display system-parameters customer-options` to browse through the Optional Features and ASAI Enhanced Features screens. Confirm that you have Computer Telephony Adjunct Links and IP_STA and STA licenses.  

*Note:*  
If features are not enabled, contact your Avaya representative. |
| 2   | Add CLAN (or CLANs) or Enable Processor Ethernet         | • If you use a media server that uses CLANs, you must add CLANs to the network. See [Adding CLANs to the network](#) on page 24.  
• If you use a media server that uses Processor Ethernet, see [Enabling Processor Ethernet](#) on page 27. |

*Table continues…*
## Checklist - Communication Manager administration for Telephony Services Application Program Interface (TSAPI) and Java Telephony Application Programming Interface (JTAPI)

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Check licensing</td>
<td>Use <code>display system-parameters customer-options</code> to browse through the Optional Features and ASAI Enhanced Features screens. Confirm that you have Computer Telephony Adjunct Links. <strong>Note:</strong> If features are not enabled, contact your Avaya representative.</td>
</tr>
<tr>
<td>2</td>
<td>Add CLAN (or CLANs) or Enable Processor Ethernet</td>
<td>If you use a media server that uses CLANs you must add CLANs to the network. See <a href="#">Adding CLANs to the network</a> on page 24. If you use a media server that uses Processor Ethernet, see <a href="#">Enabling Processor Ethernet</a> on page 27.</td>
</tr>
<tr>
<td>3</td>
<td>Enable AE Services</td>
<td>Required for the transport layer. See <a href="#">Enabling AE Services</a> on page 25.</td>
</tr>
</tbody>
</table>

Table continues…
Administering UCIDs

TSAPI applications that use predictive dialing and JTAPI applications must complete the tasks described in Setting up UCIDs for TSAPI and JTAPI applications on page 40.

Note:

Administering UCIDs is also recommended when using AE Services in conjunction with the Avaya Aura® Contact Center (AACC) product.

Add a CTI Link

See Administering a CTI Link for TSAPI, JTAPI, DMCC with Call Control, Telephony Web Service, or an AE Services integration (Microsoft or IBM Sametime) on page 29.

Checklist - Communication Manager administration for Telephony Web Services

<table>
<thead>
<tr>
<th>#</th>
<th>Notes</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1 | Check licensing | Use display system-parameters customer-options to browse through the Optional Features and ASAI Enhanced Features screens. Confirm that you have Computer Telephony Adjunct Links.  
Note:  
If features are not enabled, contact your Avaya representative. |
| 2 | Add CLAN (or CLANs) or Enable Processor Ethernet | If you use a media server that uses CLANs you must add CLANs to the network. See Adding CLANs to the network on page 24.  
If you use a media server that uses Processor Ethernet, see Enabling Processor Ethernet on page 27. |
| 3 | Enable AE Services | Required for the transport layer. See Enabling AE Services on page 25. |
| 4 | Add a CTI Link | See Administering a CTI Link for TSAPI, JTAPI, DMCC with Call Control, Telephony Web Service, or an AE Services integration (Microsoft or IBM Sametime) on page 29. |
# Checklist - Communication Manager administration for Call Visor Local Area Network (CVLAN)

<table>
<thead>
<tr>
<th>#</th>
<th>Notes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Check licensing</td>
<td>Use <code>display system-parameters customer-options</code> to browse through the Optional Features and ASAI Enhanced Features screens. ASAI Link Core Capabilities and/or Computer Telephony Adjust Links are required, depending on the CVLAN application(s).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If features are not enabled, contact your Avaya representative.</td>
</tr>
</tbody>
</table>
| 2  | Add CLAN (or CLANs) or Enable Processor Ethernet | If you use a media server that uses CLANs, you must add CLANs to the network. See [Adding CLANs to the network](#) on page 24.  
If you use a media server that uses Processor Ethernet, see [Enabling Processor Ethernet](#) on page 27. |
| 3  | Enable AE Services | Required for the transport layer. See [Enabling AE Services](#) on page 25.                      |
| 4  | Add a CTI Link | See [Administering a CTI Link for CVLAN](#) on page 28 and [Administering a CTI Link for CVLAN (internal applications)](#) on page 28.  |

# Checklist - Communication Manager administration for Definity LAN Gateway (DLG)

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Check licensing</td>
<td>Use <code>display system-parameters customer-options</code> to browse through the Optional Features and ASAI Enhanced Features screens. Confirm that you have ASAI Link Core Capabilities.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If features are not enabled, contact your Avaya representative.</td>
</tr>
<tr>
<td>#</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>Add CLAN (or CLANs) or Enable Processor Ethernet</td>
<td>If you use a media server that uses CLANs, you must add CLANs to the network. See <a href="#">Adding CLANs to the network</a> on page 24.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you use a media server that uses Processor Ethernet, see <a href="#">Enabling Processor Ethernet</a> on page 27.</td>
</tr>
<tr>
<td>3</td>
<td>Enable AE Services</td>
<td>Required for the transport layer. See <a href="#">Enabling AE Services</a> on page 25.</td>
</tr>
<tr>
<td>4</td>
<td>Add a CTI Link</td>
<td>See <a href="#">Administering a CTI Link for DLG</a> on page 29.</td>
</tr>
</tbody>
</table>

### Checklist - Communication Manager administration for AE Services Implementation with Microsoft Lync Server

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Check licensing</td>
<td>Use <code>display system-parameters customer-options</code> to browse through the Optional Features and ASAI Enhanced Features screens. Confirm that you have Computer Telephony Adjunct Links.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✳ Note: If features are not enabled, contact your Avaya representative.</td>
</tr>
<tr>
<td>2</td>
<td>Add CLAN (or CLANs) or Enable Processor Ethernet</td>
<td>If you use a media server that uses CLANs you must add CLANs to the network. See <a href="#">Adding CLANs to the network</a> on page 24.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you use a media server that uses Processor Ethernet, see <a href="#">Enabling Processor Ethernet</a> on page 27.</td>
</tr>
<tr>
<td>3</td>
<td>Enable AE Services</td>
<td>Required for the transport layer. See <a href="#">Enabling AE Services</a> on page 25.</td>
</tr>
<tr>
<td>4</td>
<td>Add a CTI Link</td>
<td>See <a href="#">Administering a CTI Link for TSAPI, JTAPI, DMCC with Call Control, Telephony Web Service, or an AE Services integration</a> on Microsoft or IBM Sametime on page 29.</td>
</tr>
</tbody>
</table>

### Communication Manager administration for DMCC - network regions

When you administer a CLAN for AE Services, you must assign a network region based on your AE Services configuration. For example, if you are using DMCC, you might need to assign more
than one network region. For more information about administering network regions, see the following documents.

- *Administering Network Connectivity on Avaya Aura® Communication Manager*
- *Administering Avaya Aura® Communication Manager*

---

**Adding CLANs to the network**

**About this task**

If you are using a media server that uses CLANs, you must add the CLANs to the Communication Manager network.

⚠️ **Important:**

All CLANs dedicated to AE Services should be in a separate network region from those CLANs servicing endpoints. CLANs that provide connectivity for other endpoints should be in another network region.

CLAN used for ASAI should not be used for DMCC registrations or SMS traffic even if the CLAN originates from same AE Services server.

🌟 **Note:**

This example assumes a simple configuration with one network region. Some configurations will require more network regions, see Communication Manager administration for DMCC - network regions.

**Procedure**

1. **Type** `change node-names ip`.

   Communication Manager displays the IP NODE NAMES form. For an example, see Figure 18: Adding a CLAN - change node-names ip.

2. Complete the following fields on the IP NODE NAMES form.
   a. In the **Name** field, type the name you want to assign to this CLAN, for example **CLAN1**.
   b. In the **IP Address** field, type the IP address you want to assign to this CLAN.

3. **Type** `add ip-interface <board location>` (where **<board location>** is the board location for the CLAN, for example **1A06**).

   Communication Manager displays the IP INTERFACES form. For an example, see Figure 19: Adding a CLAN IP interface.

4. Complete the following fields on the IP INTERFACES form.
   a. In the **Node Name** field, type **<CLAN name>**, for example **CLAN1**.
   b. In the **IP Address** field, accept the default.
   c. In the **Subnet Mask** field, type the appropriate subnet mask for your network configuration.
d. In the **Gateway Node Name** field, type the name of the gateway node for your network configuration.

e. In the **Enable Interface** field, type `y`.

f. In the **Network Region** field, type `1`.

g. In the **VLAN** field, accept the default.

h. In the **Target socket load and Warning level** field, accept the default.

i. In the **Auto** field, type `y`.

5. Type `add data-module next`.

   Communication Manager displays the DATA MODULE form. For an example, see Figure 17: Adding a CLAN - add data-module.

6. Complete the following fields on the DATA MODULE form.

   a. In the **Data Extension** field, accept the default value.

   b. (Required) In the **Type** field, type `ethernet`.

   c. (Required) In the **Port** field, type the board location and port 17, for example `1D07017`.

   d. In the **Name** field, type the name you want to assign to the data module, for example `CLAN1DATA`. This name is not used for further administration. It is a name you use to help you identify the data module.

   e. In the **Network uses 1’s for Broadcast Addresses** field, type `y`.

**Related links**

- [Adding a CLAN](#) on page 47
- [Communication Manager administration for DMCC - network regions](#) on page 23

---

**Enabling AE Services**

**About this task**

Enabling AE Services refers to administering the transport link between Communication Manager and AE Services. You need to enable AE Services if any of the following AE Services features are to be employed.

- Device, Media, and Call Control (DMCC) applications that use Registration Services or Call Information Services (1st party call control)
- DMCC applications that use Call Control Services (3rd party call control)
- Telephony Web Service
- JTAPI
- TSAPI
- CVLAN
• DLG (ASAI applications)

**Procedure**

1. **Type** `change ip-services`.
   
   Communication Manager displays the IP SERVICES form. For an example, see Figure 8: Configuring IP services in Configuring IP services - administering the transport link.

2. Complete Page 1 of the IP SERVICES form as follows:
   
   a. In the **Service Type** field, type `AESVCS`.
   
   b. In the **Local Node** field, type the appropriate entry based on whether you are using a Processor Ethernet interface or a CLAN interface:
      
      - For Communication Manager S8300D, S8300E, and duplicated servers that use a processor ethernet interface, type `procr`.
      
      - For Communication Manager duplicated systems that use a CLAN interface, type `<nodename>`. Where `<nodename>` is the name of the CLAN.

      You can locate node names by typing `display node-names ip` and checking the **Local Node** field on the IP NODE NAMES form.
   
   c. In the **Local Port** field, accept the default value **8765**.

      If you are adding more than one CLAN for AE Services, repeat Step 2 for each CLAN you add.

3. Complete Page 3 of the IP SERVICES form as follows. For an example, see Figure 9: Configuring IP services - AE Services Administration in Configuring IP services - administering the transport link.

   a. In the **AE Services Server** field, type the name of the AE Services server.

      For example, `aeserver1`

      - **Note:**

      On the AE Services server you can obtain this name by typing `uname -n` at the command prompt. The name you use on Communication Manager must match the AE Services server name exactly.

   b. In the **Password** field, create a password that consists of 12 to 16 alphanumeric characters, for example `aespassword1`.
Important:

This is the password that the AE Services administrator must set on the AE Services server on Communication Manager Interface > Switch Connections > Edit Connection > Switch Password. The passwords must exactly match on both Communication Manager and the AE Services server.

c. Set the Enabled field to y.

Related links
- Enabling Processor Ethernet on page 27
- Configuring IP services - administering the transport link on page 43

---

Enabling Processor Ethernet

About this task

Processor Ethernet support on the duplicated Communication Manager media servers requires Communication Manager 3.1 or later. Use this procedure to enable Processor Ethernet on duplicated Communication Manager media servers.

Note:

On the S8300D and S8300E Communication Manager media servers, Processor Ethernet support is enabled by default.

Procedure

1. Type display system-parameters customer-options.
2. Verify that Processor Ethernet is enabled. You must perform this verification step before proceeding with the next step.
3. Type add ip-interface procr.

Note:

From AE Services Release 6.1, the Processor Ethernet interface provides a message rate of 1000 messages per second, full duplex, for duplicated media servers. For S8300D and S8300E media servers, the Processor Ethernet interface provides a message rate of 240 messages per second, full duplex.

---

Administering UCIDs in Communication Manager (TSAPI and JTAPI applications)

About this task

TSAPI applications that use predictive dialing and all JTAPI applications must be administered to use UCIDs. There is no charge to use these features, and they do not require any Avaya Product
Licensing and Delivery System (PLDS) changes. For more information about administering UCIDs, see *Administering Avaya Aura® Communication Manager*, 03-300509.

For examples of administrative screens used to administer UCIDs, see the following figures:

- Figure 1: Setting up UCIDs for TSAPI and JTAPI applications - create a UCID and assign a Node ID in Setting up UCIDs for TSAPI and JTAPI applications.
- Figure 2: Setting up UCIDs for TSAPI and JTAPI applications - send UCID to ASAI must be enabled in Setting up UCIDs for TSAPI and JTAPI applications.

**Procedure**

1. Type `change system-parameters features`.
2. Complete the following fields on the FEATURE-RELATED SYSTEM PARAMETERS form:
   a. In the Create Universal Call ID (UCID) field, type `y`.
   b. In the UCID Network Node ID field, type a node number that is unique to this switch in a network of switches.
   c. In the Send UCID to ASAI field, type `y`.
3. Submit the changes.

**Related links**

- *Setting up UCIDs for TSAPI and JTAPI applications* on page 40

---

**Administering a CTI Link for CVLAN**

**About this task**

Follow these steps from a Communication Manager SAT to administer a CTI link type ASAI-IP (CVLAN Link) for a CVLAN application.

**Procedure**

1. Type `add cti-link <link number>`, for example `add cti-link 3`.
2. Complete the CTI LINK form as follows:
   a. In the Extension field, type `<station extension>`, for example `20007`.
   b. In the Type field, type ASAI-IP.
   c. In the Name field, type `<name of AE Services server>`, for example `aeserver1`.

---

**Administering a CTI Link for CVLAN (internal applications)**

**About this task**

This procedure applies to Avaya Interaction Center (IC).

Follow these steps from a Communication Manager SAT to administer a CTI link type ADJ-IP (Proprietary CVLAN Link) for internal Avaya CVLAN applications.
Procedure

1. Type `add cti-link <link number>`, for example `add cti-link 3`.

2. Complete the CTI LINK form as follows:
   a. In the `Extension` field, type `<station extension>`, for example `30009`.
   b. In the `Type` field, type `ADJ-IP`.
   c. In the `Name` field, type `<name of AE Server>`, for example `aeserver1`.

Administering a CTI Link for DLG

About this task

Follow these steps from a Communication Manager SAT to administer a CTI link type ASAI-IP (DLG Link) for the DLG Service. The DLG service is for applications that are written to the ASAI communications interface.

Procedure

1. Type `add cti-link <link number>`, for example `add cti-link 4`.

2. Complete the CTI LINK form as follows:
   a. In the `Extension` field, type `<station extension>`, for example `40001`.
   b. In the `Type` field, type `ASAI-IP`.
   c. In the `Name` field, type `<name of AE Server>`, for example `aeserver1`.

Administering a CTI Link for TSAPI, JTAPI, DMCC with Call Control, Telephony Web Service, or an AE Services integration

About this task

If you are administering the AE Server for TSAPI, JTAPI, DMCC with Call Control, Telephony Web Service, or an AE Services integration (Microsoft), you must administer a CTI link from Communication Manager to AE Services. Keep in mind that all clients will share the same CTI link.

Follow these steps from a Communication Manager SAT to administer a CTI link type ADJ-IP.

Procedure

1. Type `add cti-link <link number>`, for example `add cti-link 5`.

2. Complete the CTI LINK form as follows:
   a. In the `Extension` field, type an unassigned station extension.
   b. In the `Type` field, type `ADJ-IP`.
   c. In the `Name` field, type `<name of AE Server>`, for example `aeserver1`.
Checking the status of a switch connection -- from Communication Manager to the AE Services server

About this task

Once you have added a switch connection on the AE Services server, you validate the switch connection by checking its status on both the AE Services server and on Communication Manager.

For information about checking the status of a switch connection from the AE Services server, see Checking the status of a switch connection -- from the AE Services to Communication Manager.

Procedure

To check the status of a switch connection on Communication Manager, type `status aesvcs link`.

Related links

- Checking the status of a switch connection from the AE Services server to Communication Manager on page 78

DMCC settings

This information applies if you are administering Communication Manager to work with DMCC applications. If you are administering Communication Manager to work with TSAPI, CVLAN, or DLG clients, you can skip this section.

DMCC station registration modes

Communication Manager and AE Services Release 8.0.1 and later allow up to ten endpoints to register to an extension. The endpoints can register in any of the permutations of dependency and media mode depicted in the following table.

If you are administering a release of Communication Manager that is prior to Release 5.0, only the permutations marked as “old” are allowed.

<table>
<thead>
<tr>
<th>Media Mode</th>
<th>Client</th>
<th>Telecommuter</th>
<th>Server</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependency Mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Main</td>
<td>(Old) Exclusive Control</td>
<td>(Old) Exclusive Control</td>
<td>(Old) Exclusive Control</td>
<td>New</td>
</tr>
<tr>
<td>• Dependent</td>
<td>New</td>
<td>Not allowed</td>
<td>New</td>
<td>(Old) Shared Control</td>
</tr>
<tr>
<td>• Independent</td>
<td>New</td>
<td>Not allowed</td>
<td>New</td>
<td>New</td>
</tr>
</tbody>
</table>
**Note:**

Only applications that use DMCC Registration Services need to administer these stations on Communication Manager.

**Caution:**

If the DMCC station is busyout in Communication Manager, AE Services might not send any notification or event message to the client application. This might cause potential loss of recording.

When the station is in release state in Communication Manager, Communication Manager will send a URQ unregister terminal notification to AE Services.

---

### Main dependency mode

When in main dependency mode, a DMCC application has full control of the extension number associated with the application. Main dependency mode must be used for any application that records and plays messages or detects DTMF digits. All the modes under main dependency mode are as follows. (Also see [DMCC station registration modes](#) on page 30.)

- client media mode
- server media mode
- telecommuter mode
- no media (media mode: none)

For more information about the types of media control, see the document *Avaya Aura® Application Enablement Services*, 02-300369.

---

### Administering an extension exclusively for the DMCC softphone

**About this task**

Follow these steps from a Communication Manager SAT to administer an extension exclusively for the DMCC softphone. For an example of the form, see [Adding stations](#) on page 41.

**Procedure**

1. Type `add station next` to add a station. Add as many stations as you need for your application.

2. Complete the STATION form as follows:
   a. In the **Type** field (for station type), choose an IP set type or a DCP set type, as appropriate.
   b. If you chose a DCP set type, in the **Port** field, do one of the following:
      - If it is an actual physical set, type `<port number>`.
• If it is not an actual physical set, type ×.

⚠️ **Note:**

If you chose an IP set type, the port automatically becomes IP.

c. In the **Security Code** field, type a `<numeric security code>`.

The security code can consist of four to eight digits. AE Services recommends that you use an eight digit code for maximum security. Additionally, AE Services recommends that you use a unique security code for each DMCC station. Whenever you provide a security code, make sure you maintain a secure record of it so you can use it again. You will need to use this security code when your application is registering with the DMCC softphone.

d. In the **IP SoftPhone** field, type y.

e. Administer any buttons necessary for your application. For example, to administer the share-talk feature, administer **share-talk** as one of the buttons.

---

**Dependent and Independent dependency modes**

The Dependent and Independent dependency modes (also referred to as non-main Dependency mode) allow the following media modes. (Also see DMCC station registration modes on page 30.)

- client
- server
- no media (media mode: none)

⚠️ **Note:**

Telecommuter mode is not allowed.

Non-main Dependency mode control of a DMCC extension number allows a DMCC application to monitor and control a physical digital phone or a physical/soft IP phone. All updates sent to the physical phone, such as lamp, ringer, or display updates, are also sent to the DMCC application. Additionally, either the DMCC application or the physical phone can perform actions on the physical phone such as go off-hook, go on-hook, and press buttons.

If the application uses non-main Dependency mode control, you do not need to administer any other extension number for the application other than that already administered for the main.

Each registration (whether for Main, Dependent, or Independent) requires a license. The license required is either a DMCC license from WebLM (if one is available) or an IP_API_A license from Communication Manager.

When you administer a station for an application that uses non-main Dependency Mode control, you must enable the IP_Softphone setting. When you administer a station for an application that uses the Dependent dependency mode (or Main mode) a physical phone is required. See Administering an extension number for the station that an application monitors on page 33.
Administering an extension number for the station that an application monitors

About this task

Follow these steps from a Communication Manager SAT to administer an extension number for the physical station the application is monitoring.

⚠️ Note:

Do not add stations.

Procedure

1. Type `change station nnnnn` (where `nnnn` is the extension number of the physical station the application is monitoring or controlling).

2. Check the settings on the STATION form. If the STATION form is not already administered this way, follow these steps:
   a. In the IP Softphone field, type `y`.
   b. In the Security Code field, type a `<numeric security code>`.

   The security code can consist of four to eight digits. AE Services recommends that you use an eight digit code for maximum security. Additionally, AE Services recommends that you use a unique security code for each DMCC station. Whenever you provide a security code, make sure you maintain a secure record of it so you can use it again. You will need to use this security code when your application is registering with the DMCC softphone.

   In non-main Dependency mode, the DMCC extension will be registered as long as the physical phone is connected to or registered with Communication Manager.

Media Content and Media Tone Announcement for DMCC

To support split stream recording for DMCC recorders starting from AE Services Release 8.0.1, two new parameters are added in `LoginInfo` of Register Terminal Request. Find below the details of these parameters.

**Media Content**

Media Content is used to specify from which specific parties terminal should receive the media content.

- **When MediaContent is set to FULL**, all parties present in the call provides a fully summed conference stream to the DMCC device. This is the default value for Media Content unless otherwise specified.
- **When MediaContent is set to MAIN_STATION_ONLY**, the media stream contains media from only the shared extension device with the current role of talker. This is usually the main station or the agent.
• When `MediaContent` is set to `ALL_BUT_MAIN_STATION`, the media stream excludes media from the shared extension device with the current role of talker. This is usually the main station or the agent. The media stream includes all other talking parties and any parties subsequently added to the call.

**Media Tones Announcement**

Media Tones Announcement specifies whether terminal should receive Communication Manager generated tones and announcements in media stream or not.

---

### About Share Talk

Share Talk enables multiple DCP or H323 IP endpoints that are registered to the same extension to share talk capability. Normally, when more than one endpoint requests RTP (Real Time Transport Protocol) media, only one of the endpoints (Base Set) is capable of talking and listening, while the other endpoints are connected in listen-only mode. This button allows all the endpoints that are associated with the extension to share the talk capability. Note that in Communication Manager 5.0, only AE Server DMCC (Device, Media, and Call Control) endpoints are capable of requesting RTP while they are sharing control of the extension. For more information about enabling this feature, see the following documents:

- **Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer’s Guide**, 02-300359
- **Avaya Aura® Application Enablement Services Device, Media, and Call Control XML Programmer’s Guide**, 02-300358

---

### Network regions for DMCC

From Release 8.0.1 and later, if any of the ten clients are using client or server media mode (see DMCC station registration modes on page 30), you must administer the network region for that extension.

If there is only one client application registered in telecommuter mode, or none of the client applications require media for this extension, you do not have to administer a codec set for that extension.

Setting up a network region requires some network planning. For a list of documents that contain information to assist you in planning see Communication Manager administration for DMCC - network regions on page 23.

You must set up DMCC softphones in an IP network region that supports the set of Audio Codecs that your application supports. For example, the IP network region must support one of the following codec sets:

- G.722
- G.711A
Applications can specify preferences for both the Audio Codec and the Media Encryption options that they use. The Audio Codec settings and Media Encryption settings that you administer in Communication Manager must be consistent with what your application supports.

- If your application supports media encryption, administer the Media Encryption setting on the IP Codec Set form with `aes` as the first preference and `none` as the second preference or `srtp` as the first preference, `aes` as the second preference, and `none` as the third preference.

- If your application does not support media encryption, administer the Media Encryption setting on the IP Codec Set form as `none`.

Additionally, there must be a media gateway or a media processor resource in the same network region or in an interconnected network region. Otherwise, there will be problems with the talkpath.

**Note:**

Using media encryption in server media mode can reduce capacity by 15%. Using media encryption in client media mode or no media mode will not impact server capacity.

### Creating the DMCC codec set

**About this task**

Use the `change ip-codec-set <codec set number>` command to create a codec set.

**Procedure**

1. Ensure that G.722, G.711A, G.711MU, G.729, G.729A, G.723, or G.726A are the only codecs administered.

   **Note:**

   - G.723 and G.726A codecs can only be used for DMCC applications, which use Client Media mode.
   - DMCC applications in Client Media mode can use the G.722 codec to record end-to-end High Definition Media Stream.

2. Verify that the Silence Suppression field is set to `n`.

3. It is recommended that you accept the default packet size.

   For an example of how to complete the form, see [Setting up a codec set](#) on page 43.
Administering a region with a specific codec set

About this task
Use the `change ip-network-region <region number>` command to administer a network region with the codec set.

Procedure
Specify the codec set and the UDP port range (minimum and maximum) for the network region you assigned to the DMCC softphones and to the media processor.

The Codec Set field reflects the codec set that must be used for connections between phones within this region or between phones and media processor boards within this region.

About signaling encryption
If you do not enable signaling encryption, you increase the risk of exposing sensitive information (such as credit card or other identification numbers) to the public in TCP/IP communications. For example, if you do not use signaling encryption, and your DMCC applications rely on button presses (to convey a credit card number, for example), these button presses are exposed, because DTMF digits are passed in the signaling channel.

⚠ Important:
AE Services strongly recommends that you enable signaling encryption, which is described in the next topic, Administering security profiles for signaling encryption on page 36.

Administering security profiles for signaling encryption

About this task
Use the `ip-network-region <region number>` command to administer signaling encryption. Communication Manager handles signaling encryption on a per ip network region basis. Choose from the following values when you administer the Allowed Security Profiles for an ip network region (see Figure 14: Administering a network region, IP NETWORK REGION screen, page 2 on page 46).

- `challenge (default)` — provides no H.232 signaling link encryption
  
  If a DMCC endpoint is registered to an ip network region that has challenge security profile selected, it means that no H.323 signaling link encryption is provided. The challenge setting is the default for all ip-network regions in Communication Manager.

- `pin-eke` — provides H.323 signaling link encryption

- `any-auth` — provides either pin-eke or challenge
  
  If a DMCC endpoint is registered to an ip network region that has any-auth or pin-eke selected, it means that H.323 signaling link encryption is provided.

The AE Server does not provide an administrative capability for either enabling or disabling encryption for DMCC Service endpoints. The only administrative interface for enabling or disabling signaling encryption is Communication Manager ip-network region administration.
Note: Using encryption can reduce the H.323 signaling capacity by 15%.

Checking for media encryption

About this task

The AE Server provides media encryption for DMCC applications that use Main Dependency Mode (see DMCC station registration modes on page 30 for a listing of registration modes). In this mode, the DMCC application is responsible for decrypting incoming media and encrypting outgoing media. The Media Encryption setting on the Communication Manager IP Codec Set form applies to both Client media mode and Server media mode.

- In the case of Server media mode, media is terminated on the AE Server. The AE Server encrypts and decrypts media.
- In the case of Client media mode, media is terminated on the application machine. The application is responsible for encrypting and decrypting media. AE Services also provides a media stack in the DMCC Java Client SDK that encrypts and decrypts media. The media stack can be used by applications that rely on client media mode.

To verify that media encryption is enabled on Communication Manager, use the following procedure.

Procedure

1. Type `change ip-codec-set <codec set number>`.
2. On the IP Codec Set form, verify that Media Encryption is set to `aes`.
   See Figure 11: Setting up a codec set - media encryption set to `aes` on page 44.

Methods for adding DMCC softphones to the network region

There are two ways to administer a network region for DMCC extensions. Use the method that you prefer.

- Let DMCC extensions get the network region for the CLAN (or Processor Ethernet) to which they are registering.
- Use the `change ip-network-map` command. On the IP ADDRESS MAPPING form, specify the IP address of the AE Server and assign a network region.

Guidelines for adding a media gateway to the network

If you are using a media server with a media gateway, you must add the media gateway to the Communication Manager network.

For information about adding a media gateway, see Consulting the Communication Manager documentation on page 38. Following are some general guidelines about adding a media gateway.

- Use the `add media-gateway` command to add the media gateway to the Communication Manager network.
• If you are adding this media gateway to the network region you created for DMCC, you must type that network region number in the NetRgn field.
  For an example, see Adding a media gateway on page 46.

Consulting the Communication Manager documentation
For more information about adding a media gateway, see the following documents.
• Administering Network Connectivity on Avaya Aura® Communication Manager
• Installing and Upgrading the Avaya S8300 Server.

★ Note:
If you need to add a CLAN to the network, see Adding CLANs to the network on page 24.

Adding a media processor circuit pack to the network

About this task
If you are using a media server that uses a media processor (MEDPRO) circuit pack, you must add the media processor circuit pack to the Communication Manager network.

Follow these steps to add a media processor to the network:

Procedure
1. Type change node-names ip.
   For an example, see Adding a CLAN - change node-names ip on page 47.
   For a screen reference, see “IP Node Names” in the “Screen Reference” chapter of Administering Avaya Aura® Communication Manager, 03-300509.
2. Type change ip-interface <board location> (where <board location> is the board location for the media processor, for example, 1A05).
   If you are adding this media processor to the network region you created for DMCC, you must type that network region number in the NetRgn field.
   For an example, see Adding a media processor on page 47.

Sample Communication Manager and DMCC configuration
To get an idea of how to administer Communication Manager to support this sample configuration, refer to the sample Communication Manager administration screens Figure 3: Checking for IP_API_A licenses on page 41 through Figure 22: Listing IP interfaces on page 50.
1. Communication Manager - Supported media server with a CLAN circuit card and a media processor circuit card
2. Communication Manager - G700 media gateway
3. AE Server
4. One or more DMCC softphones
5. DMCC application on separate computer
6. Network Region 1 (includes IP phones; supports code set, G.711A/MU and G.729)
7. Network Region 2 (Includes G700 media gateway, CLAN, media processor; supports codec sets G.711A/MU and G.729)
8. Network Region 3 (Includes Communication Manager API softphones; supports G.711A/MU and G.729)
Sample Communication Manager administration screens

Setting up UCIDs for TSAPI and JTAPI applications

TSAPI applications that use predictive dialing and JTAPI applications must enable the setting for creating UCIDs. Select a unique node number for the switch (see Figure 1), and enable the setting for Send UCID to ASAI (see Figure 2).

Checking for IP_API_A licenses

If your DMCC application uses DMCC to register one or more station endpoints, then you need licences. The preferred license type for this is the DMCC_DMC license available on the
Application Enablement Services WebLM server. However, if no DMCC_DMC licenses are available, then you can use the IP_API_A licenses of the Communication Manager. To verify that you have a sufficient number of licenses, type `display system-parameters customer-options`. Go to the MAXIMUM IP REGISTRATIONS BY PRODUCT ID screen and check the IP_API_A field. See Figure 3 on page 41.

<table>
<thead>
<tr>
<th>Product ID</th>
<th>Rel. Limit</th>
<th>Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_API_A</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>IP_Agent</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IP_Phone</td>
<td>1000</td>
<td>104</td>
</tr>
<tr>
<td>IP_RMCMax</td>
<td>50</td>
<td>15</td>
</tr>
<tr>
<td>IP_Soft</td>
<td>500</td>
<td>0</td>
</tr>
<tr>
<td>IP_eCons</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(NOTE: You must logoff & login to effect the permission changes.)

**Figure 3: Checking for IP_API_A licenses**

**Adding stations**

Add as many stations as you need for your DMCC based application. See the following:

- Figure 4: Adding a station, Page 1 of the STATION screen
- Figure 5: Adding a station, Page 2 of the STATION screen
- Figure 6: Adding a station, Page 3 of the STATION screen
- Figure 7: Adding a station, Page 4 of the STATION screen

**Figure 4: Adding a station, Page 1 of the STATION screen**
Figure 5: Adding a station, Page 2 of the STATION screen

Figure 6: Adding a station, Page 3 of the STATION screen
Configuring IP services - administering the transport link

Configuring IP services administers the transport link between Communication Manager and AE Services. Use the `change ip-services` command, and administer settings on the IP SERVICES screen (figure 8) and the AE Services Administration screen (figure 9).

**Note:**
For transport connections using CLANs, type the CLAN name as the Local Node. For transport connections using Processor Ethernet, type `procr` as the Local Node.

Setting up a codec set

Use the `change ip-codec set <codec set number>` command to set up a codec set that uses G.711A, G.711MU and/or G.729. See the figure on page 44.
Administering a network region

For this example network, you will administer the following codec connectivity within each network region and between network regions:

- network region 3 -> network region 1: codec 2
- network region 3 -> network region 2: codec 2
- network region 3 <-> network region 3: codec 3

See the figure on page 45 and the figure on page 45.
Mapping IP addresses (for API softphones)

Use the `change ip-network-map` command, and specify the IP address of the AE Server and assign a network region. See the figure on page 46.

Figure 15: Mapping IP addresses (for API softphones)

Adding a media gateway

If you are using a media server with a media gateway, you must add the media gateway to the Communication Manager network. For information about adding a media gateway, see Consulting the Communication Manager documentation on page 38.

* Note:

If you are using a media gateway, and your application needs media encryption, you must set `Encrypt Link?` to `y`. If you do not enable this setting, your application will not get a talk-path.
Adding a CLAN

When you are using a media server that uses CLANs, you must add the CLANs to the Communication Manager network. The procedure for adding a CLAN uses the following commands.

- **add data-module** see Figure 17
- **change node-names ip** see Figure 18
- **change ip-interface** - to add the following:
  - a CLAN see Figure 19
  - a MEDPRO circuit pack see Figure 20
  - a PROCR see Figure 21
Figure 17: Adding a CLAN - add data-module

![Data Module](image)

- Data Extension: **4444**
- Name: **CLAN1**
- Type: **ethernet**
- Port: **17D0717**

**Network uses 1's for Broadcast Addresses?**  Y

Figure 18: Adding a CLAN - change node-names ip

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLAN1</td>
<td>192.11.12.1</td>
<td>. . .</td>
<td>. . .</td>
</tr>
<tr>
<td>CLAN2</td>
<td>192.11.12.2</td>
<td>. . .</td>
<td>. . .</td>
</tr>
</tbody>
</table>
add ip-interface 1A06

IP INTERFACES

Type: C-LAN
Slot: 01A06
Code/Suffix: TN799 D
Node Name: sraychk-clan1
IP Address: 192.11 .12 .1
Subnet Mask: 255.255.255.0
Gateway Address: 135.9 .71 .254
Enable Ethernet Port? Y
Network Region: 1
VLAN: 0

Target socket load and Warning level: 400

Figure 19: Adding a CLAN IP interface

change ip-interface 1A17

IP INTERFACES

Type: MDFPRO
Slot: 01A17
Code/Suffix: TN2302
Node Name: sraychk-prw1
IP Address: 192.11 .12 .2
Subnet Mask: 255.255.255.0
Gateway Address: 135.9 .71 .254
Enable Ethernet Port? Y
Network Region: 1
VLAN: 0

Figure 20: Adding a media processor
Listing IP interfaces

Use the `list ip-interface all` command to view the IP interfaces you have administered, as illustrated in the figure on page 50.
Chapter 3: AE Services administration

The method you choose to access AE Services administration depends on the tasks you want to perform. Refer to Figure 23: AE Services and ssh authentication methods on page 52 and the figure on page 52 as you read the following descriptions of access methods.

**Web browser:** You must use a Web browser to access the Application Enablement Services Management Console (AE Services Management Console). Use the AE Services Management Console to configure the AE Services server. AE Services uses role-based access control (RBAC) to determine what tasks you are allowed to perform using the AE Services Management Console. For example, the default system administrator, cust, has read and write access to all of the administrative features in the AE Services Management Console. For more information about access privileges, see AE Services administrative roles and access privileges (role based access control - RBAC on page 321.

**Local or remote access to the Linux shell:** Administrators can access the AE Services Linux shell (command prompt) either locally using a system console or remotely using a secure shell (ssh) client. This access method applies primarily to AE Services Technicians (craft users) who perform specific tasks, such as viewing trace logs, installing patches, and so forth. If you plan to use the Linux shell for these kinds of maintenance tasks, see AE Services Administration from the Operating System Command Prompt on page 238.

**Important:**

The AE Services offers do not provide a web browser. To administer AE Services, you need a computer running a browser with network access to the AE Server.
Figure 23: AE Services and ssh authentication methods

*Note: PAM Management pages in the AE Services Management console apply only to the following:
- Local Linux accounts
- AE Services Management Console access, including RBAC
- Remote users with SSH access

Figure 24: AE Services client authentication methods

Related links
Logging in to AE Services as the system administrator on page 55
AE Services Management Console - certificates and security alerts

Use this section to understand the security alerts you might see when you attempt to access AE Services with your browser.

This section provides examples that are specific to Microsoft Internet Explorer (IE). Although the procedures might not be the same for other browsers, the same basic concepts apply.

The types of security alerts you receive and how to handle them, depend on whether you use the default AE Services server certificate CA, or if you use certificates issued by a trusted in-house or third-party certificate authority.

Using certificates issued by a trusted in-house or third-party certificate authority is also referred to as using your own certificates.
Note:
Some versions of IE has the Enhanced Security Configuration security feature enabled by default. In order to display the AE Services Management Console, you can add the AE Services Management Console URL to the Trusted Sites zone of the Windows Server Internet Explorer browser. Otherwise, you can disable the Enhanced Security Configuration security feature on the Internet Explorer browser.

For additional information about this feature, please see the Microsoft TechNet site [HTTP://TECHNET.MICROSOFT.COM/].

---

**Browser security**

If you use the default server certificate, your browser will issue two alerts. The first alert indicates that the certificate was issued by an invalid CA. The second alert indicates that the CN is invalid because the server name in the URL does not match the CN in the certificate. If you add the Avaya CA into your browser’s trust store the CN error will continue to occur.

If you are using the default server certificate, you cannot avoid this security alert. You will see this message each time you log in to AE Services, click Yes to use AE Services.

Note:
Do not use the default server certificates in a production environment. Avaya recommends that you must replace all the default installed certificates with new certificates.

---

**Using own Certificate Authority**

**About this task**

If you use your own certificates, note that your browser and the AE Server need to use the same trusted certificate. If your browser does not refer to the same trusted certificate as the AE Server, your browser will issue a security alert when you attempt to access AE Services. You can eliminate this security alert by following these steps.

**Procedure**

1. Obtain and install the CA certificate for the AE Server.
   For specific instructions, see [Obtaining a trusted certificate for the AE Server](#) on page 104.

2. Import the trusted certificate into AE Services.
   For specific instructions, see [Importing the trusted certificate into AE Services](#) on page 106.

3. Import the CA certificate in your browser’s certificate store.
   For specific instructions, see [Importing the CA certificate into your browser’s certificate store](#) on page 55.
Importing the CA certificate into your browser’s certificate store

About this task

Use this procedure to import the CA certificate into your browser’s certificate store. This procedure provides tasks specific to Microsoft Internet Explorer. Although the procedures might not be the same for other browsers, the same basic concepts apply.

Procedure

1. On your browser, click Tools > Internet Options.
2. In the Internet Options dialog box, click Content > Certificates.
3. In the Certificates dialog box, click the Trusted Root Certification Authorities tab.
4. In the list of Trusted Root Certification Authorities, click Import to start the Certificate Import Wizard.
5. In the File to Import dialog box, click Browse, and locate the certificate.
6. Click Next.
7. In the Certificate Store dialog box, click Browse.
8. In the Select Certificate Store dialog box, click Trusted Root Certification Authorities, and click OK.
9. Click Next.
10. In the Completing the Certificate Import Wizard dialog box, click Finish.
11. In the Import was successful dialog box, click OK to close the message.
12. Click Close to close the Certificates dialog box.
13. Click OK to close the Internet Options dialog box.

When you restart your browser and access AE Services, your browser will not display the security alert for an invalid CA.

Logging in to AE Services as the system administrator

About this task

Follow this procedure to log in to the AE Server as the default administrator (cust). Bear in mind that you can not log in to the AE Services Management Console as root.

Note:

For information about setting up administrative and user accounts, see AE Services administrative roles and access privileges (role based access control - RBAC).
Procedure

1. From your Web browser, type the address of the AE Server.
   You must use either the fully qualified domain name or the IP address of the AE Services Server. For example:
   aserver.example.com
   135.8.17.123 (An example of an IPv4 address)
   [2002:d5fe::1] (An example of an IPv6 address)

   Note:
   If you use an IPv6 address to connect to the AE Server, you must enclose the IPv6 address within square brackets ([ ] ) in the web browser (for example, https:// [2002:d5fe::1]).
   The first time you try to access the AE Server, your browser presents a Security Alert for an SSL certificate.

2. Click Yes to accept the SSL certificate.

   Note:
   If your browser does not display the SSL certificate, make sure that the URL begins with “https://” and the host name or IP address of the AE Services Server is correct.

3. On the Application Enablement Services welcome page, click Continue to Login.

   Tip:
   To change the message that appears on this Welcome screen, see Creating a PAM Issue (/etc/issue) message.

4. From the Application Enablement Services Management Console log in page, type the default login , and click Login.
   Your browser displays the Application Enablement Services Management Console home page for the cust administrator. The cust administrator has access to all AE Services Management Console menus. For more information about the access privileges assigned to administrative users, see AE Services administrative roles and access privileges (role based access control - RBAC).

Related links
AE Services administration on page 51
Creating a PAM Issue (/etc/issue) message on page 175
Administering the PAM Password Manager on page 173
Changing the default password for the cust account in local Linux on page 329
AE Services administrative roles and access privileges (role based access control - RBAC) on page 321
Checklists for administering the services that run on the AE Services server

Use the checklists in this section to plan and monitor your progress as you administer the services that run on the AE Services server.

For a high-level illustration of the services that run on the AE Services server, see Schematic view of an AE Services configuration 3.

Related links

- AE Services administration on page 51
- CVLAN - checklist on page 57
- DLG - checklist on page 58
- DMCC with device and media control only - checklist on page 58
- DMCC with device and media control only (using a switch name for CLANs) - checklist on page 60
- DMCC with Call Information Services - checklist on page 61
- DMCC with Call Control Services - checklist on page 63
- TSAPI (including JTAPI) - checklist on page 64
- Telephony Web Services - checklist on page 65
- System Management Service - checklist on page 66
- AE Services integration for Microsoft Lync Server 2010 and 2013 - checklist on page 67
- Schematic view of an AE Services configuration on page 125

CVLAN - checklist

Use this checklist if you are administering AE Services for CVLAN.

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 1 | Networking > AE Service IP (Local IP) | Required. Based on your AE Services configuration, see either of the following topics:  
  - Administering The Local IP for a single NIC configuration on page 70  
  - Administering The Local IP for a dual NIC configuration on page 71 |
| 2 | Networking > Ports | Not required. You can use the default settings. |
| 3 | Communication Manager Interface > Switch Connections | Required. See Adding a switch connection on page 73. |

Table continues…
## DLG - checklist

Use this checklist if you are administering AE Services for the DLG service. ASAI applications rely on the DLG service for communications to Communication Manager.

**Note:**

AE Services assigns port 5678 for DLG. You do not administer ports for DLG.

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Networking &gt; Network Configure</td>
<td>Required. See Configuring network interface settings on page 68.</td>
</tr>
</tbody>
</table>
| 2  | Networking > AE Services (Local IP)              | Required. Based on your AE Services configuration, see either of the following topics:  
|    |                                                  | • Administering The Local IP for a single NIC configuration on page 70.  
|    |                                                  | • Administering The Local IP for a dual NIC configuration on page 71.    |
| 3  | Communication Manager Interface > Switch Connections | Required. See Adding a switch connection on page 73.                  |
| 4  | AE Services > DLG > DLG Links > Add Link         | Required. See Administering DLG Links on page 83.                     |

### Related links

Checklists for administering the services that run on the AE Services server on page 57
<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Networking &gt; Network Configure</td>
<td>Required. See <a href="#">Configuring network interface settings</a> on page 68</td>
</tr>
<tr>
<td>2</td>
<td>Networking &gt; AE Services (Local IP)</td>
<td>Required. Based on your AE Services configuration, see either of the following topics:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Administering The Local IP for a single NIC configuration</a> on page 70.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Administering The Local IP for a dual NIC configuration</a> on page 71.</td>
</tr>
<tr>
<td>3</td>
<td>Networking &gt; Ports</td>
<td>Optional. You can use the default settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you have a firewall, you might need to change these settings. See <a href="#">TCP ports and firewall settings</a> on page 316.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Important:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you have a Release 3.0 DMCC application, see <a href="#">Enabling DMCC server ports for DMCC applications developed prior to AE Services 3.1</a> on page 69.</td>
</tr>
<tr>
<td>4</td>
<td>AE Services &gt; DMCC</td>
<td>Optional. You can use the default media and station properties. See <a href="#">Setting DMCC Media Properties</a> on page 85.</td>
</tr>
<tr>
<td>5</td>
<td>Security &gt; Certificate Management</td>
<td>Required if you are using link encryption. For more information, see <a href="#">Certificate management</a> on page 97.</td>
</tr>
<tr>
<td>7</td>
<td>Security &gt; Enterprise Directory</td>
<td>Optional. If you are using an external LDAP server (Microsoft Active Directory or Open Source LDAP) you must use the Enterprise Directory Configuration page in the AE Services Management Console. For more information, see <a href="#">Enterprise Directory settings in the AE Services Management Console</a> on page 186.</td>
</tr>
<tr>
<td>8</td>
<td>Security &gt; Host AA</td>
<td>Not applicable if you are not using encryption. It is optional if you are using link encryption. The DMCC service can be set up to provide far-end client authentication and authorization. For more information, see the Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer’s Guide, 02-300359.</td>
</tr>
</tbody>
</table>
## DMCC with device and media control only (using a switch name for CLANs) - checklist

Use this checklist if you are administering the DMCC service for applications that do not use Call Information Services or Call Control Services, but do use a switch name for round-robin assignment of H.323 Gatekeepers for administering AE Services.

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Networking &gt; Network Configure</td>
<td>Required. See <a href="#">Configuring network interface settings</a> on page 68</td>
</tr>
<tr>
<td>2</td>
<td>Networking &gt; AE Services (Local IP)</td>
<td>Required. Based on your AE Services configuration, see either of the following topics:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Administering The Local IP for a single NIC configuration</a> on page 70.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Administering The Local IP for a dual NIC configuration</a> on page 71</td>
</tr>
<tr>
<td>3</td>
<td>Networking &gt; Ports</td>
<td>Optional. You can use the default settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you have a firewall, you might need to change these settings. See <a href="#">TCP ports and firewall settings</a> on page 316.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Important:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you have a Release 3.0 DMCC application, see <a href="#">Enabling DMCC server ports for DMCC applications developed prior to AE Services 3.1</a> on page 69.</td>
</tr>
<tr>
<td>4</td>
<td>AE Services &gt; DMCC</td>
<td>Optional. You can use the default media and station properties. See <a href="#">Setting DMCC Media Properties</a> on page 85.</td>
</tr>
<tr>
<td>5</td>
<td>Communication Manager Interface &gt; Switch Connections</td>
<td>Required. The Switch Connection Name is used for round-robin assignment of H.323 Gatekeepers. You must edit the H.323 Gatekeeper. See <a href="#">Administering switch connections for DMCC applications that use device and media control only -- assigning H.323 IP addresses</a> on page 75.</td>
</tr>
</tbody>
</table>
Checklists for administering the services that run on the AE Services server

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Security &gt; Certificate Management</td>
<td>Not required if you are not using encryption. For more information, see Certificate management on page 97.</td>
</tr>
<tr>
<td>8</td>
<td>Security &gt; Enterprise Directory</td>
<td>Optional. For more information, see Enterprise Directory settings in the AE Services Management Console on page 186.</td>
</tr>
<tr>
<td>9</td>
<td>Security &gt; Host AA</td>
<td>Not applicable if you are not using encryption. It is optional if you are using link encryption. The DMCC service can be set up to provide far-end client authentication and authorization. For more information, see the Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer’s Guide, 02-300359.</td>
</tr>
</tbody>
</table>

Related links
Checklists for administering the services that run on the AE Services server on page 57

DMCC with Call Information Services - checklist

Use this checklist if you are administering the DMCC service for applications that use Call Information Services.

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Networking &gt; Network Configure</td>
<td>Required. See Configuring network interface settings on page 68</td>
</tr>
<tr>
<td>2</td>
<td>Networking &gt; AE Services (Local IP)</td>
<td>Required. Based on your AE Services configuration, see either of the following topics:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Administering The Local IP for a single NIC configuration on page 70.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Administering The Local IP for a dual NIC configuration on page 71.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 3  | Networking > Ports                   | Optionial. You can use the default settings.  
   |                                       | Note:  
   |                                       | If you have a firewall, you might need to change these settings. See TCP ports and firewall settings on page 316.  
   |                                       | Important:  
   |                                       | If you have a Release 3.0 DMCC application, see Enabling DMCC server ports for DMCC applications developed prior to AE Services 3.1 on page 69. |
| 4  | Communication Manager Interface > Switch Connections | Required. DMCC with Call Information Services uses the Transport Service. See Adding a switch connection on page 73.  
   |                                       | Optional. You have the option of using H.323 Gatekeepers when you administer a switch connection. See Administering switch connections for DMCC applications that use device and media control only -- assigning H.323 IP addresses on page 75. |
| 5  | Communication Manager Interface > Dial Plan | Optional. You must administer a dial plan if your DMCC clients use E.164ConversionServices. See Chapter 10: Dial plan administration in AE Services on page 281. |
| 6  | AE Services > DMCC                   | Optional. You can use the default media and station properties. See Setting DMCC Media Properties on page 85. |
| 8  | Security > Certificate Management    | Optional. if you are using link encryption, you must set up certificates. For more information, see Certificate management on page 97. |
| 9  | Security > Enterprise Directory      | Optional. If you are using an external LDAP Server (Microsoft Active Directory or Open Source LDAP), you must use the Enterprise Directory Configuration page in the AE Services Management Console. For more information, see Enterprise Directory settings in the AE Services Management Console on page 186. |
| 10 | Security > Host AA                   | Not applicable if you are not using encryption. It is optional if you are using link encryption. The DMCC service can be set up to provide far-end client authentication and authorization. For more information, see the Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer’s Guide, 02-300359. |
## DMCC with Call Control Services - checklist

Use this checklist if you are administering DMCC with Call Control Services.

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Networking &gt; Network Configure</td>
<td>Required. See <a href="#">Configuring network interface settings</a> on page 68</td>
</tr>
</tbody>
</table>
| 2  | Networking > AE Services (Local IP)                   | Required. Based on your AE Services configuration, see either of the following topics:  

- [Administering The Local IP for a single NIC configuration](#) on page 70.  
- [Administering The Local IP for a dual NIC configuration](#) on page 71. |
| 3  | Networking > Ports                                    | Optional. You can use the default settings.  

**Note:**  
If you have a firewall, you might need to change these settings. See [TCP ports and firewall settings](#) on page 316.  

**Important:**  
If you have a Release 3.0 DMCC application, see [Enabling DMCC server ports for DMCC applications developed prior to AE Services 3.1](#) on page 69. |
| 4  | Communication Manager Interface > Switch Connection   | Required. The Transport Layer is used. See [Adding a switch connection](#) on page 73. |
| 5  | CTI Link Admin                                         | Required (you must add a TSAPI Link).  
Applications that use DMCC with Call Control rely on the TSAPI Service. See [Administering TSAPI Links](#) on page 84. |
| 6  | AE Services > DMCC Configuration                       | Optional. You can use the default media properties. See [Setting DMCC Media Properties](#) on page 85. |
| 7  | Security > Security Database                          | Optional. If you are using the AE Service Security Database for controlling device access you must administer the TSAPI Configuration settings. See [Chapter 6: The Security Database](#) on page 209.|

Table continues…
<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Security &gt; Enterprise Directory</td>
<td>Optional. If you are using an external LDAP directory you will need to use the Enterprise Directory Configuration page. For more information, see Enterprise Directory settings in the AE Services Management Console on page 186.</td>
</tr>
<tr>
<td>9</td>
<td>Security &gt; Certificate Management</td>
<td>Optional. If you are using link encryption, you must set up certificates. For more information, see Certificate management on page 97.</td>
</tr>
<tr>
<td>10</td>
<td>Security &gt; Host AA</td>
<td>Not applicable if you are not using encryption. It is optional if you are using link encryption. The DMCC service can be set up to provide far-end client authentication and authorization. For more information, see the Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer’s Guide, 02-300359.</td>
</tr>
</tbody>
</table>

Related links

Checklists for administering the services that run on the AE Services server on page 57

---

**TSAPI (including JTAPI) - checklist**

Use this checklist if you are administering AE Services for TSAPI or JTAPI applications. AE Services JTAPI is a client side interface to the TSAPI service, and, as such it provides third party call control.

⚠️ **Note:**

Beginning with Release 4.1, AE Services provides the option of encrypted TSAPI links. If you are administering the TSAPI service for encrypted TSAPI links, you will need to administer the TSAPI links as encrypted. If you use encrypted links you will need to administer certificates.

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Networking &gt; Network Configure</td>
<td>Required. See Configuring network interface settings on page 68.</td>
</tr>
<tr>
<td>2</td>
<td>Networking &gt; AE Services (Local IP)</td>
<td>Required. Based on your AE Services configuration, see either of the following topics:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Administering The Local IP for a single NIC configuration on page 70.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Administering The Local IP for a dual NIC configuration on page 71.</td>
</tr>
<tr>
<td>#</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>----</td>
<td>------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>3</td>
<td>Networking &gt; Ports</td>
<td>Optional. You can use the default settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✳ Note:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you have a firewall, you might need to change these settings. See TCP ports and firewall settings on page 316.</td>
</tr>
<tr>
<td>4</td>
<td>Communication Manager Interface &gt; Switch Connection</td>
<td>Required. The Transport Layer is used. See Adding a switch connection on page 73.</td>
</tr>
<tr>
<td>5</td>
<td>CTI Link Administration</td>
<td>Required (TSAPI Link). See Administering TSAPI Links on page 84.</td>
</tr>
<tr>
<td>6</td>
<td>TSAPI Configuration</td>
<td>Optional. If you are using the AE Service Security Database for controlling device access you must administer the TSAPI Configuration settings. See Chapter 6: The Security Database on page 209.</td>
</tr>
<tr>
<td>8</td>
<td>Security &gt; Enterprise Directory</td>
<td>Optional. If you are using an external LDAP directory you will need to use the Enterprise Directory Configuration page. For more information, see Enterprise Directory settings in the AE Services Management Console on page 186.</td>
</tr>
<tr>
<td>9</td>
<td>Security &gt; Certificate Management</td>
<td>Optional. if you are using link encryption, you must set up certificates. For more information, see Certificate management on page 97.</td>
</tr>
</tbody>
</table>

Related links
- Checklists for administering the services that run on the AE Services server on page 57

## Telephony Web Services - checklist

When you administer AE Services for Telephony Web Services applications, you must add a TSAPI link. Use this checklist if you are administering AE Services for Telephony Web Services applications.

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Networking &gt; Network Configure</td>
<td>Required. See Configuring network interface settings on page 68.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 2  | Networking > AE Services (Local IP)              | Required. Based on your AE Services configuration, see either of the following topics:  
|    |                                                  | • **Administering The Local IP for a single NIC configuration** on page 70.  
|    |                                                  | • **Administering The Local IP for a dual NIC configuration** on page 71. |
| 3  | Networking > Ports                               | Optional. You can use the default settings.  
|    |                                                  | ✴️ **Note:**  
|    |                                                  | If you have a firewall, you might need to change these settings. See **TCP ports and firewall settings** on page 316. |
| 4  | Communication Manager Interface > Switch Connection | Required. See **Adding a switch connection** on page 73. |
| 5  | AE Services > TSAPI > TSAPI Link > Add TSAPI Links | Required. You must add a TSAPI Link.  
|    |                                                  | See **Administering TSAPI Links** on page 84. |
| 6  | Security > Enterprise Directory                  | Optional. For more information, see **Enterprise Directory settings in the AE Services Management Console** on page 186. |
| 7  | Security > Certificate Management                | Optional. If you are using link encryption, you must set up certificates. For more information, see **Certificate management** on page 97. |

**Related links**

[Checklists for administering the services that run on the AE Services server](#) on page 57

---

**System Management Service - checklist**

When you administer AE Services for System Management Service applications, you must add a link to the Communication Manager host. Use this checklist if you are administering AE Services for System Management Service applications.

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Networking &gt; Network Configure</td>
<td>Required. See <strong>Configuring network interface settings</strong> on page 68.</td>
</tr>
</tbody>
</table>

*Table continues...*
<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 2 | Networking > AE Services (Local IP)             | Required. Based on your AE Services configuration, see either of the following topics:  
|   |                                                 | • [Administering The Local IP for a single NIC configuration](#) on page 70.  
|   |                                                 | • [Administering The Local IP for a dual NIC configuration](#) on page 71. |
| 3 | Network Configuration > Ports                   | Optional. You can use the default settings.                          |
|   |                                                 | ★ Note:                                                               |
|   |                                                 | If you have a firewall, you might need to change these settings. See [TCP ports and firewall settings](#) on page 316. |
| 4 | SMS Configuration                               | Required. See [SMS Configuration](#) on page 298.                     |

**Related links**

[Checklists for administering the services that run on the AE Services server](#) on page 57

---

### AE Services integration for Microsoft Lync Server 2010 and 2013 - checklist


Use this checklist to plan and monitor your administrative tasks.

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Networking &gt; Network Configure</td>
<td>Required. See <a href="#">Configuring network interface settings</a> on page 68.</td>
</tr>
</tbody>
</table>
| 2  | Networking > AE Services (Local IP)             | Required. Based on your AE Services configuration, see either of the following topics:  
|    |                                                 | • [Administering The Local IP for a single NIC configuration](#) on page 70.  
|    |                                                 | • [Administering The Local IP for a dual NIC configuration](#) on page 71 |
| 3  | Networking > Ports                              | Required. You must enable the TR87 LCS Port (4723). By default this port is disabled in the AE Services Management Console. |

Table continues…
<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>AE Services &gt; DMCC Configuration</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>5</td>
<td>Communication Manager Interface &gt; Switch Connection</td>
<td>Required. The Transport Layer is used. See <a href="#">Adding a switch connection</a> on page 73.</td>
</tr>
<tr>
<td>6</td>
<td>CTI Link Administration</td>
<td>Required (TSAPI Link). See <a href="#">Administering TSAPI Links</a> on page 84.</td>
</tr>
<tr>
<td>10</td>
<td>Security &gt; Host AA</td>
<td>Optional. TR/87 applies to Microsoft Office Live Communications Server 2005, Microsoft Office Communications Server 2007, and Microsoft Lync Server 2010 and 2013. Setting to “Authenticate Client Cert with Trusted Certs” preset (activated). Enable “Enforce Host Authorization” to have the TR/87 service check the CN in the client certificate and verify that it matches one of the administered authorized hosts.</td>
</tr>
</tbody>
</table>

Related links

[Checklists for administering the services that run on the AE Services server](#) on page 57

---

### Configuring network interface settings

#### About this task

Use this procedure to configure network interface settings. In this procedure, you must use an explicit IPv4 address or an IPv6 address. Do not use IPv4 mapped or a compatible IPv6 address that combines the IPv4 and IPv6 formats.
Procedure

1. On the AE Services Management Console main menu, click **Networking > Network Configure**.
2. In the **Physical IP Address** field, type or modify the IP address for each network interface.
3. In the **Netmask** field, type an appropriate netmask address for each network interface.
4. Select the **Enable** check box for each network interface.
5. Click **Apply Changes**.
6. On the **Apply Changes to Network Configure** page, click **Apply**.
7. Log in to the AE Services Management Console by using the new IP address of the AE Services server.
8. On the AE Services Management Console main menu, click **Networking > AE Services IP (Local IP)** and set the new IP addresses for Client Connectivity, Switch Connectivity, and Media Connectivity.
9. On the AE Services Management Console main menu, click **Maintenance > Service Controller**.
10. On the **Service Controller** page, click **Restart AE Server**.
11. Ensure that all the services are in the **Running** state, and that the connection state to the switches is functional.

If you cannot access the AE Services Management Console, check the status of the httpd and tomcat processes. If they are not running, start them. For example:

```
/usr/bin/systemctl status httpd status
/usr/bin/systemctl start httpd start
/usr/bin/systemctl status tomcat status
/usr/bin/systemctl start tomcat start
```

Related links

AE Services administration on page 51

Enabling DMCC server ports for DMCC applications developed prior to AE Services 3.1

**About this task**

DMCC applications connect to a secure, encrypted port (4722) on the AE Server. The encrypted port is enabled by default.

**Important:**

If you have a DMCC application that was developed prior to AE Services 3.1 and it uses an unencrypted port, you must enable the unencrypted port (4721).
Procedure

1. From the AE Services Management Console main menu, select Networking > Ports.

2. From the Ports page, in the DMCC Server Ports section, locate the Unencrypted Port field, and select the option button for Enabled.

Related links

AE Services administration on page 51

Administering the Local IP for a single NIC configuration

About this task

Administering a Local IP refers to choosing the network interfaces that the AE Server uses for connectivity. For a single NIC configuration, it means that you will use one network interface for connectivity to Communication Manager and your clients. For more information, see Single NIC configurations on page 313.

Note:

If you are using CVLAN in combination with other services, see Administering network interfaces with CVLAN - using the Any network setting on page 72.

Note:

The ethN:IP address setting refers to a specific network interface on the server. If your AE Server uses four network interfaces, it can refer to eth0, eth2, or eth3 The Any setting uses the wild card IP address (0.0.0.0 if you are using IPv4 or :: if you are using IPv6), which means that all services on the AE Server will listen on all interfaces.

Procedure

1. From the AE Services Management Console main menu, select Networking > AE Service IP (Local IP).

2. From the AE Service IP (Local IP) page, complete the connectivity settings as follows:
   a. In the Client Connectivity field, select ethN:IP address or Any.
   b. In the Switch Connectivity field, select ethN:IP address or Any.
   c. In the Media Connectivity field, select ethN:IP address or Any.
   d. In the OAM Connectivity field, select ethN:IP address or Any.

   Note:

   For a summary of these settings, see Recommended AE Service IP (local IP) settings on page 72.

Related links

AE Services administration on page 51
Administering the Local IP for a dual NIC configuration

About this task

Administering a Local IP refers to specifying the network interfaces that the AE Server uses for connectivity. For a dual NIC configuration, it means that you will use two network interfaces. For more information, see Dual NIC configurations on page 314.

⚠️ Note:

The ethN:IP address setting refers to a specific network interface on the server. If your AE Server uses four network interfaces, it can refer to eth0, eth2, or eth3. For dual NIC configuration, one NIC is designated for client connectivity, and the other NIC is designated for switch connectivity. The Any setting uses the wild card IP address (0.0.0.0 if you are using IPv4 or :: if you are using IPv6), which means that all services on the AE Server will listen on all interfaces.

Procedure

1. From the AE Services Management Console main menu, select Networking > AE Service IP (Local IP).
2. From the AE Service IP (Local IP) page, complete the connectivity settings as follows:
   a. In the Client Connectivity field, select ethN:IP address.
      For a dual NIC configuration ethN:IP address refers to the network interface that connects to the client (also referred to as the production network connection).
   b. In the Switch Connectivity field, select ethN:IP address.
      For a dual NIC configuration ethN:IP address refers to the network interface that connects to Communication Manager (also referred to as the private network connection).
   c. In the Media Connectivity field, select one of the following:
      • Select ethN:IP address if you are administering AE Services for DMCC applications with media connectivity.
      • Select Any if you are administering AE Services for all other applications.
         ⚠️ Note: For a summary of these settings, see Recommended AE Service IP (local IP) settings on page 72.
   d. In the OAM Connectivity field, select one of the following:
      • Select eth N:IP address to restrict the OAM connectivity to the selected IP network.
      • Select Any to access OAM from all the networks.
         ⚠️ Note: For a summary of these settings, see Recommended AE Service IP (local IP) settings on page 72.
Recommended AE Service IP (local IP) settings

Use the following recommendations for the AE Service IP (local IP) settings in the AE Services Management Console.

⚠️ **Note:**

The **Any** setting uses the wild card IP address (0.0.0.0 if you are using IPv4 or :: if you are using IPv6), which means that all services on the AE Services Server will listen on all interfaces, or in the case of a single NIC, one interface.

<table>
<thead>
<tr>
<th></th>
<th>Single NIC</th>
<th>Dual NIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client connectivity</td>
<td>eth0:IP address or Any</td>
<td>eth0:IP address</td>
</tr>
<tr>
<td>(production network)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch connectivity</td>
<td>eth0:IP address or Any</td>
<td>eth2:IP address or eth3:IP address</td>
</tr>
<tr>
<td>(private network)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Connectivity</td>
<td>eth0:IP address or Any</td>
<td>eth0:IP address or Any</td>
</tr>
<tr>
<td></td>
<td>• Use eth0:IP address for DMCC applications</td>
<td>• Use Any for all other applications (TSAPI,</td>
</tr>
<tr>
<td></td>
<td>with media connectivity.</td>
<td>JTAPI, DMCC with Call Control, Web Services,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CVLAN, and DLG).</td>
</tr>
<tr>
<td>OAM Connectivity</td>
<td>ethN:IP address or Any</td>
<td>eth0:IP address or Any</td>
</tr>
<tr>
<td></td>
<td>• Use ethN:IP address to restrict the OAM</td>
<td>• Use Any to access OAM from all the</td>
</tr>
<tr>
<td></td>
<td>connectivity to the selected IP network.</td>
<td>networks.</td>
</tr>
</tbody>
</table>

**Related links**

AE Services administration on page 51

---

Administrating network interfaces with CVLAN - using the Any network setting

**About this task**

Use this procedure to use the **Any** setting for client connectivity.
The `/etc/hosts` file must contain the IP address of the host computer on which the CVLAN clients are on.

**Procedure**

1. Log in as root user.
2. On the command line interface run the following command:
   ```
   uname -n
   ```
   Linux displays the network node hostname which refers to the AE Server name, for example `aeserver1`. Make a note of the AE Server name.
3. Type `ifconfig eth0` to get the IP address of the host (this assumes that you are using eth0 for client connectivity).
   Make a note of the IP address of the AE Server. For example, `inet addr: 192.168.123.44`.
4. Use a text editor to open the `/etc/hosts` file.
   Make sure that the `/etc/hosts` file contains the AE Server name along with its IP address (see the figure on page 73).
5. If the `/etc/hosts` file does not contain this AE Server name and IP address entry, add it to the file.

   ```
   # Do not remove the following line, or various programs
   # that require network functionality will fail.
   127.0.0.1 localhost.localdomain localhost
   192.168.123.44 aeserver1
   192.168.123.64 anosrv
   ~
   ```

   *Figure 25: sample `/etc/hosts` file*

**Related links**

- [AE Services administration](#) on page 51

---

### Adding a switch connection

**About this task**

You must administer a switch connection for all applications except DMCC applications that use device and media control only.

If you have a DMCC application that uses device and media control only, and you want to administer a switch connection to use the gatekeeper feature, see Administering switch connections for DMCC applications that use Registration Services -- assigning H.323 IP addresses.
**Procedure**

1. From the AE Services Management Console main menu, select Communication Manager Interface > Switch Connections.
2. On the Switch Connections page, in the Add Connection field, type a switch connection name (for example Switch1).
   
The switch connection name can be any name you want to use, but it must consist of alphanumeric characters only.
3. Click Add Connection.
4. On the Connections Details page, do the following:
   a. In the Switch Password field, type the password that the Communication Manager administrator assigned when the node name of the AE Services Server on the IP-Services form was administered, see Enabling AE Services.
   b. In the Confirm Switch Password field, retype the password.
   c. In the Msg Period field, accept the default (30 minutes).
   d. For the Provide AE Services certificate to switch check box, do one of the following:
      • For Communication Manager Release 6.3.6 or later, accept the default (check box is checked).
      Ensure that the Communication Manager recognizes the Certificate Authority used by the AE Services certificate.
      • For any previous release of Communication Manager, clear the Provide AE Services certificate to switch check box.
   e. For the Secure H323 Connection check box, do one of the following:
      • For Communication Manager Release 6.3.6 or later and TLS for the H.323 Signaling Channel (normally associated with FIPS Mode), select the Secure H323 Connection check box.
      • For any previous release of Communication Manager without TLS for the H.323 Signaling Channel, clear the Secure H323 Connection check box.
      For information about Communication Manager media servers that support a Processor Ethernet connection, see Enabling AE Services.
   f. Click Apply.

AE Services adds the switch connection and returns you to the Switch Connections page. The new switch connection name appears in the Connection Name column.

**Related links**

AE Services administration on page 51
Administering switch connections for DMCC applications that use Registration Services - assigning H.323 IP addresses on page 75
Enabling AE Services on page 25
Administering switch connections for DMCC applications that use Registration Services - assigning H.323 IP addresses

About this task

When you are administering AE Services for DMCC applications that use Registration Services, you have the option of using H.323 Gatekeepers when you administer a switch connection.

If you want to use the round-robin assignment of IP addresses to softphones based on a Switch Connection name (highly recommended), then set up a Switch Connection and use the H.323 Gatekeeper feature to associate a list of H.323 Gatekeepers (GKs) with the Switch Connection name. Only the IP addresses of the CLANs in the appropriate network region should be included in the H.323 GK list. The Processor Ethernet (PE) IP address of the Main CM is automatically included as a gatekeeper if the address is entered in the Edit Processor Ethernet IP page.

⚠️ Caution:

The Processor Ethernet IP addresses of any ESS or LSP servers must not be included in the GK list. The PE IPs of ESS or LSP servers should only be included in the Survivability Hierarchy list.

Procedure

1. From the AE Services Management Console main menu, select Communication Manager Interface > Switch Connections
2. From the Switch Connections page, select the connection name you want to associate with the H.323 Gatekeeper.
3. Click Edit H.323 Gatekeeper.
4. On the Edit H.323 Gatekeeper page, in the Add Name or IP field, type the host name or IP address of the TN799DP CLAN you want to use.

🌟 Note:

You must use either an explicit IPv4 address or an IPv6 address. Do not use an IPv4-mapped/compatible IPv6 address that combines the IPv4 and IPv6 formats.

Do not add the Processor Ethernet IP addresses of any ESS or LSP servers to the H.323 Gatekeeper list. The PE IPs of the ESS or LSP servers should only be included in the Survivability Hierarchy list.
5. If you are adding multiple H.323 Gatekeepers (TN799DP CLANs), repeat Step 4 for each H.323 Gatekeeper.

When you add multiple H.323 Gatekeepers for a switch connection, each host name or IP address is added as the last item in the name or IP address list.

Related links
AE Services administration on page 51
Enabling AE Services on page 25
Logs on page 122
Viewing log files on page 123
Downloading log files on page 123
About rsyslog on page 128

---

Editing CLAN IPs

About this task
After you add a switch connection, you must associate the switch name with a CLAN host name or IP address. Use this procedure when you are setting up a switch connection with a Communication Manager media server that uses a CLAN connection to AE Services. If you are setting up a switch connection to a Communication Manager media server that uses a Processor Ethernet connection, see Editing a Processor Ethernet name or IP address on page 77.

Procedure

1. From the AE Services Management Console main menu, select Communication Manager Interface > Switch Connections.
2. On the Switch Connections page, select the connection name you just added (for example, Switch1).
3. Click Edit PE/CLAN IPs.
   
   Skip this step if you use Device, Media, and Call Control without Call Information Services.
4. In the Add Name or IP field, type the host name or IP address.
   
   ✪ Note:
   You must use either an explicit IPv4 address or an IPv6 address. Do not use an IPv4-mapped/compatible IPv6 address that combines the IPv4 and IPv6 formats.
5. Click Add/Edit Name or IP of the CLAN or the TN799DP CLAN.
6. For systems with multiple TN799DP CLANs, repeat Steps 4 and 5 for each TN799DP CLAN.
   
   When you add multiple TN799DP CLANs for a switch connection, each host name or IP address is added as the last item in the name or IP address list.
Editing a Processor Ethernet name or IP address

About this task
After you add a switch connection, you must associate the switch connection name with the Processor Ethernet host name or IP address. Use this procedure to edit a Processor Ethernet name or IP address.

Procedure
1. On the AE Services Management Console, navigate to Communication Manager Interface > Switch Connections.
2. On the Switch Connections page, select the connection name that you want to edit.
3. Click Edit PE/CLAN IPs.
4. Choose a processor ethernet.
5. On the Add/Edit Processor Ethernet IP page, in the Add/Edit Name or IP field, type the host name or the IP address of the Processor Ethernet.
   You must use either an IPv4 address or an IPv6 address. Do not use an IPv4 mapped or compatible IPv6 address that combines the IPv4 and IPv6 formats.
6. Click Add/Edit Name or IP.

Adding Communication Manager High Availability information

About this task
After you have associated a CLAN or Processor Ethernet host name or IP address with the switch connection, you may optionally populate the Survivability Hierarchy list. If your Communication Manager High Availability configuration employs the use of an Enterprise Survivable Server (ESS or survivable core server) or a Local Survivable Processor (LSP or survivable remote server), the ESS or the LSP should be added to the hierarchy. The Survivability Hierarchy list specifies the precedence of ESS or LSP nodes within the selected switch connection.
Procedure

1. From the AE Services Management Console main menu, select Communication Manager Interface > Switch Connections.
2. From the Switch Connections page, select the switch connection name you just added, for example, Switch2.
3. Click Survivability Hierarchy.
4. On the Survivability Hierarchy page, if you want to allow the main Communication Manager server to take over as soon as it is online, uncheck the Remain connected to current active ESS/LSP when Main comes back online box. The Remain connected to current active ESS/LSP when Main comes back online box is checked by default.
5. In the Cluster ID/MID field, type the cluster ID/MID of the new survivable node that you want to add to the Survivability Hierarchy table.
6. Click Append to add the new cluster ID/MID to the bottom of the hierarchy, or click Insert to add the new cluster ID/MID above the selected existing cluster ID/MID in the table.

🌟 Note:

Inserting the new cluster ID/MID implies that all nodes at and below the selected entry will have their priorities changed in the Survivability Hierarchy table. The priority of each node will be increased by 1.

7. Ensure that the correct cluster ID/MID is selected and click Edit PE IP.
8. In the provided field, add host name or IP address of the Processor Ethernet associated with the ESS or LSP.
9. Click Add/Edit Name or IP to save host name or IP address.
10. Click Back to return to the Survivability Hierarchy page.
11. Repeat steps 5-10 for each ESS or LSP to be added to the Survivability Hierarchy for this switch connection.
12. Once all of the ESS and LSP servers have been added, click Back to return to the Switch Connections page.

Related links

AE Services administration on page 51

Checking the status of a switch connection from the AE Services server to Communication Manager

About this task

Use this procedure to check the status of a switch connection from the AE Services server to Communication Manager.
procedure

1. On the AE Services Management Console, navigate to Status > Status and Control > Switch Connections Summary.
2. On the Switch Connections Summary page, select the switch connection that you just added.
3. Click Connection Details.
4. Review the information on the Connection Details page.
5. Verify that the connection is in the Talking state and the online or offline status of the connection is Online.

⚠️ Important:

After you complete this procedure, check the status of the switch connection from Communication Manager to the AE Services server. For more information see, Checking the status of a switch connection -- from Communication Manager to the AE Services server on page 30.

related links

AE Services administration on page 51
Guidelines for setting up CVLAN links

To set up a CVLAN link that allows multiple clients (up to 60) to share the same CVLAN link (signal), follow these guidelines.

• On Communication Manager, administer the CTI link as ASAI-IP, as described in Administering a CTI Link for CVLAN on page 28.

• In the AE Services Management Console, administer the CVLAN link with the Proprietary setting disabled, as described in Administering CVLAN Links on page 80.

• In the AE Services Management Console, administer the CVLAN clients (up to 60) for a specific CVLAN link, as described in Adding CVLAN Clients on page 82.

Guidelines for setting up proprietary CVLAN links

• On Communication Manager, administer the CTI link as ADJ-IP, as described in Administering a CTI Link for CVLAN (internal applications) on page 28.

• In the AE Services Management Console, administer the CVLAN link with the Proprietary setting enabled. See Administering CVLAN Links on page 80.

• In the AE Services Management Console, administer only one CVLAN client for each CVLAN link. See Adding CVLAN Clients on page 82.

AE Services provides proprietary links for Avaya applications. As a result, AE Services limits the way that proprietary links can be used. For example, AE Services allows only one proprietary link to be opened for one CVLAN client IP address.

Adding CVLAN Links

About this task

CVLAN links are used by external and internal applications. For example, Avaya Interaction Center is an internal application that uses CVLAN links.

⚠️ Note:

By default, the CVLAN service is not started on the AE Services server until you administer the first CVLAN link. After you administer the first CVLAN link, verify that the CVLAN service is running.

Procedure

1. On Application Enablement Services Management Console, click AE Services > CVLAN > CVLAN Links.

2. Click Add Link.
3. On the Add CVLAN Links page, perform the following:
   a. In the **Signal** field, select a signal number.
      The signal number used by the CVLAN link and the CVLAN application must match.
      
      **Note:**
      Prior to CVLAN R9 and AE Services 3.0, the range of CVLAN links was 1 through 8 instead of 1 through 16. If you select 9 through 16, ensure that your application is not hard coded to use signals 1 through 8 only.

   b. In the **Proprietary** check box, perform one of the following:
      - Clear the **Proprietary** check box if the CVLAN link is for an external application.
      - Select the **Proprietary** check box if the CVLAN link is for an internal application.
      By default, the **Proprietary** check box is clear.

   c. In the **Switch Connection** field, click a switch connection value.

   d. In the **Switch CTI Link Number** field, select the switch CTI link number administered on Communication Manager for this CVLAN Link.

   e. In the **ASAI Link Version** field, select the highest ASAI link version that the CVLAN application can support.
      CVLAN supports ASAI Link version from 1 through 10.
      The default value is version 4.

      **Warning:**
      If you change the ASAI Link version, all active clients might be dropped when you put the change into effect.

   f. In the **Heartbeat** check box, select the setting appropriate for the configuration:
      - Select **Heartbeat** to enable the setting to designate the CVLAN service as the ASAI Heartbeat server.
      - Clear **Heartbeat** to disable the setting to designate the CVLAN application as the ASAI Heartbeat server.

   g. Click **Apply Changes**.

4. On the Apply Changes to Link page, click **Apply**.

5. Restart the CVLAN Service for the changes to take effect. To restart the CVLAN Service, perform the following:
   a. On Application Enablement Services Management Console, click **Maintenance > Service Controller**.
   b. On the Service Controller page, select **CVLAN Service**.
   c. Click **Restart Service**.
Ensuring the CVLAN service is running

About this task
After you administer the first (or only) CVLAN link, follow this procedure to make sure that the CVLAN service is running.

Procedure

1. From the AE Services Management Console main menu, select Status > Status and Control > Services Summary.
2. On the Services Summary page, confirm that ONLINE appears as the CVLAN service status. If a status other than ONLINE appears, do one of the following:
   - If the status is STOPPED, follow these steps:
     a. From the AE Services Management Console main menu, select Maintenance > Service Controller.
     b. From the Service Controller page, check the CVLAN Service check box.
     c. Click Restart Service.
   - If the status is NO LICENSE, you will need to install the CVLAN license (assuming you have acquired one).

Testing a CVLAN link

Procedure

1. From the AE Services Management Console main menu, select Utilities > Diagnostics > AE Service > ASAI Test.
2. On the ASAI Test page, select a link number.
3. Click Test.
   The ASAI Test Result page indicates whether the test succeeded or failed.

Adding CVLAN clients

Procedure

1. From the AE Services Management Console main menu, select AE Services > CVLAN > CVLAN Links.
2. On the CVLAN Links page, select the signal (link) that you want to administer.
3. Click **Edit Client**.
4. On the **Edit Clients** page, in the **Add Client** field, type the IP address or host name of the CVLAN client.

   **Note:**
   You must use either an explicit IPv4 address or an IPv6 address. Do not use an IPv4-mapped/compatible IPv6 address that combines the IPv4 and IPv6 formats.

5. Click **Add Client**.
6. Repeat steps 4 and 5 for each client you want to add.

---

**Adding DLG Links**

**About this task**

DLG links are used by ASAI applications.

**Procedure**

1. On Application Enablement Services Management Console, go to **AE Services > DLG > DLG Links**.
2. Click **Add Link**.
3. On the Add DLG Links page, do the following:
   a. In the **Switch Connection** field, click a switch connection value.
   b. In the **Switch CTI Link Number** field, select the switch CTI link number administered on Communication Manager for this DLG link.
   c. In the **Client Hostname or IP** field, type the host name or IP address of the client application.

      **Note:**
      You must use either an explicit IPv4 address or an IPv6 address. Do not use an IPv4-mapped/compatible IPv6 address that combines the IPv4 and IPv6 formats.

   d. In the **Client Link Number** field, select the link number of the client application.
   e. Click **Apply Changes**.
4. On the Apply Changes to Link page, click **Apply**.
5. Restart the DLG Service for the changes to take effect. To restart the DLG Service, do the following:
   a. On Application Enablement Services Management Console, go to **Maintenance > Service Controller**.
   b. On the Service Controller page, select **DLG Service**.
c. Click Restart Service.

The DLG service has successfully restarted when the Controller Status displays Running.

Related links
AE Services administration on page 51

---

Adding TSAPI Links

About this task
TSAPI links are used by TSAPI applications, JTAPI applications, Telephony Web Service applications, DMCC applications that use Call Control, and DMCC applications that use Logical Device Feature Services. TSAPI links are also used for the AE Services integration for Microsoft Lync Server.

You can administer one TSAPI link for each switch connection.

Procedure
1. On Application Enablement Services Management Console, go to AE Services > TSAPI > TSAPI Links.
2. Click Add Link.
3. On the Add TSAPI Links page, do the following:
   a. In the Link field, select the link number.
   b. In the Switch Connection field, click a switch connection value.
   c. In the Switch CTI Link Number field, select the switch CTI link number administered on Communication Manager for this TSAPI link.
   d. In the ASAI Link Version field, select 10.

   ✔ Note:

   Link version 10 is only supported for Communication Manager 8.1 or 7.1.3.4 and later and AE Services 8.1 and later.

   e. In the Security field, select one of the following:
      • **Unencrypted**: To use unencrypted client connections.
      • **Encrypted**: To encrypt client connections for this TSAPI link.
      • **Both**: To use both encrypted and unencrypted client connections.

If you select the Both option, all TSAPI clients using the Encrypted Advertised TLINK require AE Services 4.1 or later.

Any TSAPI clients using the Unencrypted Advertised TLINK can work with AE Services 4.1 or earlier versions.
For the AE Services integration with Microsoft Lync, you must administer TSAPI links as encrypted. If your AE Server supports other TSAPI applications in addition to the integration with Microsoft Lync, and some of those applications use unencrypted TSAPI links, you must administer TSAPI links with the Both setting.

f. Click Apply Changes.

4. On the Apply Changes to Link page, click Apply.

5. Restart the TSAPI Service for the changes to take effect. To restart the TSAPI Service do the following:
   a. On Application Enablement Services Management Console, go to Maintenance > Service Controller.
   b. On the Service Controller page, select TSAPI Service.
   c. Click Restart Service.

The TSAPI service has successfully restarted when the Controller Status displays Running.

Related links

AE Services administration on page 51
Checking the status of a switch connection -- from Communication Manager to the AE Services server on page 30
Checking the status of a switch connection from the AE Services server to Communication Manager on page 78
Checklists for administering the services that run on the AE Services server on page 57

---

Setting Media Properties

About this task

If you use the DMCC service for media control, use the Media Properties webpage in the AE Services Management Console to change the default media properties.

Procedure

1. On Application Enablement Services Management Console, go to AE Services > DMCC > Media Properties
2. On the Media Properties page, review the default settings and make any necessary changes.
3. Click Apply Changes.
4. On the Apply Changes to Media Properties page, click Apply.
5. (Optional) Click Restore Defaults to restore the default settings.
6. Restart the DMCC Service for the changes to take effect. To restart the DMCC Service, perform the following:
   a. On Application Enablement Services Management Console, go to Maintenance > Service Controller.
   b. On the Service Controller page, select DMCC Service.
   c. Click Restart Service.

      The DMCC service has successfully restarted when the Controller Status displays Running.

Related links
AE Services administration on page 51

---

Setting DMCC Station Properties

About this task
If you use the DMCC service for media control, use the Station Properties webpage in the AE Services Management Console to change the default station properties.

Procedure
1. On Application Enablement Services Management Console, go to AE Services > DMCC > Station Properties.
2. On the Station Properties page, review the default settings and make any necessary changes.
3. Click Apply Changes.
4. On the Station Properties page, click Apply.
5. (Optional) Click Restore Defaults to restore the default settings.
6. Restart the DMCC Service for the changes to take effect. To restart the DMCC Service, perform the following:
   a. On Application Enablement Services Management Console, go to Maintenance > Service Controller.
   b. On the Service Controller page, select DMCC Service.
   c. Click Restart Service.

      The DMCC service has successfully restarted when the Controller Status displays Running.

Related links
AE Services administration on page 51
Administering Auto Hold

About this task
Use this procedure to enable or disable the Auto Hold feature for Microsoft Office Communicator clients and Microsoft Lync clients. When you enable the Auto Hold feature, a Microsoft Office Communicator client or Microsoft Lync client that is on an active call receives a notification or a toaster pop-up when a new call arrives.

Procedure
1. On Application Enablement Services Management Console, go to AE Service > DMCC > Auto Hold Configuration.
2. Do one of the following:
   • To enable the Auto Hold feature, select the Auto Hold check box.
   • To disable the Auto Hold feature, clear the Auto Hold check box.
3. Perform one of the following:
   • If you want AE Services to refuse holdCall requests from Microsoft Lync and Microsoft Office Communicator clients, select the Prevent Lync and Office Communicator clients from holding calls check box. When this feature is enabled, users can only place calls on hold using the device.
   • If you want AE Services to accept holdCall requests from Microsoft Lync and Microsoft Office Communicator clients, clear the Prevent Lync and Office Communicator clients from holding calls check box.
4. Click Apply Changes.
5. On the Apply Changes to Auto Hold Configuration page, click Apply.

Related links
AE Services administration on page 51

TCP or TLS Settings
Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message.

Under the TCP/TLS Settings options, TLSv1 Protocol Configuration options are presented. The options are as follows:
• Support TLSv1.0 Protocol.
• Support TLSv1.1 Protocol.
• Support TLSv1.2 Protocol.
Only the TSL1.2 option is checked by default. If you are upgrading to AE Services 7.x.x and have client applications that based on AE Services Release 6.3.x or older and using TLS, you will be unable to connect.

Enable TLS1.0 and/or TLS1.1, to avoid the potential risk associated with selecting a non-compatible option.

Related links
AE Services administration on page 51

Administering the TCP retransmission count

About this task
Use this procedure to set the TCP retransmission count.

⚠️ Important:
The TCP retransmission count setting applies to all TCP and TLS sockets on the AE Server.

Procedure
1. From the AE Services Management Console main menu, select Networking > TCP Settings.
2. On the TCP Settings page, perform one of the following steps:
   • If you want to set the TCP retransmission count to 15, click Standard Configuration. (This is the default setting.)
   • If you want to set the TCP retransmission count to 6, click TSAPI Routing Application Configuration.
3. Click Apply Changes.
4. On the Apply changes to TCP Retransmission Count page, click Apply to confirm your changes.

Related links
AE Services administration on page 51
Chapter 4: AE Services Secure Mode

AE Services secure mode

Federal Information Processing Standard Publication (FIPS) is the United States government specification to cover the levels of security in vendor products that are used by the Department of Defense or other government agencies. AE Services is based on the Red Hat Enterprise Linux (RHEL) operating system, and provides support for some of the recommendations as specified in FIPS Publication 140-2 for Security Level 1, including Annex A.

⚠️ Important:

- You must perform all database backup or restore operations before switching to AE Services secure mode.
- After switching over to secure mode, first login to the AE Services server using the management console before accessing the command line interface.
- Once secure mode is enabled, Avaya does not recommend switching over to non secure mode as some of the services might not function correctly. Reinstall is the recommended action.
- In secure mode, AE Services supports the account management only through the command line interface and not through the management console.
- In secure mode, AE Services does not support diagnostic tests using the management console (Utilities > Diagnostics).
- In secure mode, before configuring GRHA, the new Linux users that have been created on the primary server, must be created manually on the secondary server as well.
- Backup taken in non secure mode can only be restored on the AE Services server in non secure mode. Backup taken in secure mode can only be restored on the AE Services server in secure mode.

When AE Services secure mode is enabled, the following changes occur.

- The RHEL kernel is configured for kernel FIPS mode. In this mode, the kernel only uses FIPS approved ciphers. This change take effect after the server is rebooted.
- SSH is configured to use only FIPS approved ciphers.
- The Apache web server presents a valid identity certificate through a connecting browser or a client. The Apache web server known trusted root CA signs the identity certificate before the access to AE Services Management Console or Web Services is granted.
- The AE Services DMCC, TSAPI, and CVLAN requires a connecting client to present a valid identity certificate signed by a trusted root CA known by the respective AE Services before a TLS connection is allowed for service.
• The AE Services, DLG, is stopped.

• Non secure ports that is FTP (21) or DMCC (4721) are blocked by the firewall.

• All configured switch connections are updated to use the Secure H323 Connection option located on the Management Console screen, Communication Manager > Switch Connections > Add/Edit Connection. This option is used by DMCC to set the TLS authentication flag in the Gatekeeper Request (GRQ) message during a device registration process. After a successful Gatekeeper Confirmation (GCF) response is received, a TLS connection to Communication Manager is used for the signaling channel.

⚠️ Note:

If Secure Mode with FIPS is not enabled on Communication Manager or if Communication Manager does not support Secure Mode with FIPS (Communication Manager versions prior to 6.3.6 and Communication Manager version 6.3.6 and later that do not have the FIPS template installed). The DMCC H323 device registration request is rejected by Communication Manager. For each switch connection where Communication Manager is not in FIPS mode, the system administrator will need to disable the Secure H323 Connection option for DMCC registration to succeed.

• DMCC media encryption is configured to only support the SRTP ciphers based on AES128-HMAC32 and AES128-HMAC80 for authenticated and unauthenticated mode.

• All configured switch connections are updated to use the Provide AE Services certificate to switch option located on the Management Console screen, Communication Manager Interface > Switch Connections > Add/Edit Connection. When Secure Mode with FIPS is enabled for the AE Services, it is expected that Communication Manager is also functioning in FIPS mode. While in the FIPS mode, Communication Manager is expected to request an identity certificate from any connecting client requesting service. In this case the client is AE Services. The first installed AE Services identity certificate associated with the alias cmtls, aeservices or server, respectively, is used as the identity certificate and sent to Communication Manager when requested.

⚠️ Note:

If the switch connection is unable to be established, please verify that the CA certificate used to sign the AE Services identity certificate is in the Communication Manager trust store. In addition, verify that the CA certificate used to sign the Communication Manager identity certificate is in the AE Services trust store.

When AE Services secure mode is disabled, the following changes will occur. Any changes made during the enable phase that is not reverted back to its previous state will need to be changed by the system administrator.

• The RHEL kernel FIPS mode will be disabled. This change will take effect after the server is rebooted.

• The Apache web server will not require a connecting browser/client to present an identity certificate.

• DMCC will be configured to support all the available media encryption ciphers used by the DMCC SDK.

Related links
AE Services command line utilities for standard and secure mode on page 91
Enabling AE Services secure mode on page 92
AE Services command line utilities for standard and secure mode

<table>
<thead>
<tr>
<th>Security attribute</th>
<th>Description</th>
<th>Standard profile</th>
<th>Hardened profile</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set TLS versions</td>
<td>To enable or disable TLS versions 1.0 1.1, and 1.2</td>
<td>Yes</td>
<td>Yes</td>
<td>setTLSviaCLI [enable</td>
</tr>
<tr>
<td></td>
<td>You can also set the TLS versions using the AE Services management console.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SELinux</td>
<td>To set the SELinux mode of RHEL.</td>
<td>Disabled</td>
<td>Enforced</td>
<td>setSELinux [enforce</td>
</tr>
<tr>
<td>Kernel FIPS</td>
<td>To enable or disable FIPS mode for Kernel.</td>
<td>Disabled</td>
<td>Enabled</td>
<td>kernelFIPSmode [on</td>
</tr>
<tr>
<td>Database Auditing</td>
<td>To enable or disable the auditing of database actions.</td>
<td>Manual Enablement</td>
<td>Manual Enablement</td>
<td>DBAudit [enable</td>
</tr>
<tr>
<td>Tripwire (File Tampering Prevention)</td>
<td>To reconfigure Tripwire properties. You can also configure Tripwire properties using the AE Services management console.</td>
<td>Manual Enablement</td>
<td>Manual Enablement</td>
<td>setTripwire [reconfigure</td>
</tr>
</tbody>
</table>

Related links

AE Services secure mode on page 89
Enabling AE Services secure mode

About this task
Use this procedure to enable AE Services secure mode for FIPS.

The Apache web server requires a connecting browser or client to present a valid identity certificate. The identity certificate must be signed by a trusted root CA known by the Apache web server. Only after the identity certificate is signed you can access the AE Services Management Console or web services.

Before you begin

- Ensure that your browser is properly configured with an identity certificate.
- Ensure that The root CA certificate used to sign the identity certificate is imported into the AE Services server

Procedure

1. On the command line prompt, run the following command:
   ```
   /opt/mvap/bin/aesvcsSecureMode on
   ```
2. Enter relevant answers to the questions that follow.
3. After all the changes are successfully applied, reboot the server complete the process.

Related links

AE Services secure mode on page 89

Disabling AE Services secure mode

About this task
Use this procedure to disable AE Services secure mode for FIPS.

Procedure

1. On the command line interface, run the following command:
   ```
   /opt/mvap/bin/aesvcsSecureMode off
   ```
2. Enter relevant answers to the questions that follow.
3. After all the changes are successfully applied, the server is rebooted to complete the process.

Related links

AE Services secure mode on page 89
**Multifactor authentication**

The multifactor authentication is a two factor authentication process on the AE Services server. AE Services activates multifactor authentication when configured in the secure mode.

For AE Services management console, the required credentials are:

- Certificate authentication
- Password associated with the certified user

For AE Services command line interface, the required credentials are:

- Certificate authentication
- Username of the certified user

**Related links**

- [AE Services secure mode](#) on page 89
- [Enabling multifactor authentication](#) on page 93
- [Disabling multifactor authentication](#) on page 94

**Enabling multifactor authentication**

**About this task**

Use this procedure to enable multifactor authentication. AE Services enables multifactor authentication when configured in a secure mode.

**Before you begin**

Before you enable multifactor authentication, ensure the following:

- Ensure that your web browser is configured with the identity certificate.
- Create Root CA certificate and client certificate. See, [Using OpenSSL as a Certificate Authority (CA) to generate signed certificates](#) on page 359.
- The root CA certificate used to sign the identity certificate is imported into the AE Services server using the Management Console screen.
- On the web browser, import the client certificate. Note that, if you do not install certificates, enabling secure mode fails.
- Using the command line interface, create another root user on the AE Services server with same user name as on the client certificate.

**Procedure**

1. On the AE Services server command line interface, run the following command:
   ```bash
   /opt/mvap/bin/enableMFA on
   ```
2. When the system prompts, enter the required parameters.
   After the completion of the process, the server reboots for changes to take effect.
3. In the secure mode, log in first using the management console before logging in to the command line interface.
Do not use the default user name created during the deployment process.

Related links

- Multifactor authentication on page 93

Disabling multifactor authentication

About this task

Use this procedure to disable multifactor authentication. AE Services disables multifactor authentication when the secure mode is disabled.

Procedure

1. On the command prompt, run the following command:

   `/opt/mvap/bin/enableMFA off`

2. When the system prompts, enter the required parameters.

   After the completion of the process, the server reboots for changes to take effect.

Related links

- Multifactor authentication on page 93

Certificate revocation configuration

The AE Services supports certificate revocation configuration. The certificate revocation configuration is applicable for DMCC, TSAPI, and CVLAN client provided certificate validation and revocation check occurring on AE Services server.

Related links

- AE Services secure mode on page 89
- Certificate revocation configuration field descriptions on page 94

Certificate revocation configuration field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Revocation Validation</td>
<td>Specifies the validation method for revocation check on the certificate.</td>
</tr>
<tr>
<td></td>
<td>• <strong>NONE</strong>: No revocation check.</td>
</tr>
<tr>
<td></td>
<td>• <strong>BEST_EFFORT</strong>: Revocation check will be performed. Fails revocation check only if the certificate is REVOKED.</td>
</tr>
<tr>
<td></td>
<td>• <strong>MANDATORY</strong>: Revocation check will be performed. Allows revocation check only if the certificate is GOOD.</td>
</tr>
</tbody>
</table>

Table continues...
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCSP Local URI</td>
<td>Specifies local OCSP Responder URI. This field is mandatory if the OCSP URI Preference field is set to Local.</td>
</tr>
<tr>
<td>OCSP URI Preference</td>
<td>Specifies which OCSP Responder URL is used first for revocation check.</td>
</tr>
<tr>
<td></td>
<td>• CERT: From the certificate AuthorityInfoAccess extension.</td>
</tr>
<tr>
<td></td>
<td>• LOCAL: From OCSP Local URI.</td>
</tr>
</tbody>
</table>

Related links

Certificate revocation configuration on page 94

Certificate revocation for multifactor authentication

When AE Services is configured in secure mode, AE Services enables multifactor authentication and provides ability to enable certificate revocation check for client provided certificates.

When certificate revocation check is enabled, AE Services server checks the revocation status of client provided certificates using Online Certificate Status Protocol (OCSP) responder either provided in Certificate Authority Information Access (AIA) Extension or OCSP responder URL provided during configuration.

If client certificate is REVOKED or OCSP responder URL is unreachable or incorrect, AE Services rejects the secure connection request to AE Services OAM and the user cannot connect to the OAM interface.

If client certificate is GOOD, AE Services allows the secure connection request to the OAM interface and the user can connect to the OAM interface. Revocation check on client certificate is performed every time when new session request is created with the OAM interface.

Related links

AE Services secure mode on page 89

Enabling or disabling certificate revocation by using OCSP

About this task

Use this procedure to enable or disable the certificate revocation check for multifactor authentication. When configured in secure mode, AE Services provides an ability to enable certificate revocation check for client certificates.
Before you begin

Ensure the following:

- The OCSP responder is available from which the certificate revocation status can be obtained.
- The OCSP responder URL is provided in the certificate AIA extension or during the certificate revocation check for MFA configuration.
- The OCSP responder is running on Port 80, when secure mode is configured on AE Services.

Procedure

1. To enable the certificate revocation check, run the following command on the command line interface:
   ```bash
   mfaOCSPCheck enable
   ```

2. To disable the certificate revocation check, run the following command on the command line interface:
   ```bash
   mfaOCSPCheck disable
   ```

3. To check the status of a certificate revocation check, run the following command on the command line interface:
   ```bash
   mfaOCSPCheck status
   ```

Related links

[AE Services secure mode](#) on page 89
Chapter 5: Certificate Management

Certificate management

Install your own certificates signed by either your own PKI infrastructure or a third party PKI vendor. If such resources are not available immediately, use the temporary AE Services server self-signed certificate. It should be noted that this self-signed certificate is valid for only 1 year. It is expected that you deploy your own certificates before this certificate expires.

* Note: Do not use the default server certificates in a production environment.

For an upgrade from a previous AE Services 5.x or 6.x release to AE Services 7.x and later, any customer application relying on the old, Avaya provided server certificate for TLS will not be able to connect to the AE Services Release 7.x and 8.x server. If you have been using these certificates in a production environment, we strongly recommend that you prepare and execute a rollout plan, as soon as possible, to update your client applications and AE Services server with your own certificates.

Avaya strongly encourages customers to create this certificate prior to upgrading to the AE Services 8.x.

AE Services supports only one AE Services server certificate. Do not upload multiple third party server certificate on AE Services server.

* Note: For any AE Services release, where the installed AE Services server certificate has been replaced with a customer provided certificate, the client/server TLS connection will not be affected by the aforementioned certificate expiration or replacement.

Possible customer options to create the new AE Services server certificate:

- Use your own Private Key Infrastructure (PKI).
- Use Avaya Aura’s System Manager (SMGR) Trust Management PKI feature. See System Manager Trust Management in Appendix H.
- Use an Open Source PKI, for example EJBCA. Avaya does not endorse or require the use of this product or vendor. You may use any product or vendor of your choosing.
- Use a third party vendor, for example Verisign. Avaya does not endorse or require the use of this product or vendor. You may use any product or vendor of your choosing.
- Use OpenSSL to create your own Certificate Authority (CA). See the OpenSSL section in Appendix I.
If for some reason none of the above options fit your immediate need, please contact Avaya Services for additional assistance.

Overview of certificate management

This overview of certificate management is provided to help you understand the role of the AE Services administrator in terms of managing certificates and to explain some basic concepts about certificates. Two key concepts are server authentication and client authentication.

Server authentication

This section describes the server authentication process. This procedure is the same if you use certificates issued by a trusted in-house or third-party certificate authority — referred to as using your own certificates, or if you use the default certificate installed by AE Services.

1. The client sends a request to the server for a secure session
2. The server sends its server certificate to the client.
3. The client checks the server certificate to determine the following:
   a. If the server certificate is issued by a certificate authority that the client trusts. The client checks the name of the CA. To comply, the name of the certification authority (CA) on the certificate must match the name of the CA on the client’s trusted certificate.
   b. If the server certificate is within its validity window. The client checks to see if the current time falls between the Not Before and Not After dates in the server certificate.
   c. If the common name in the server certificate matches the name of the server to which the client is connected. If the names do not match, the client can not trust the certificate.

When all the security checks are satisfied the client and server can exchange secure messages.

In this situation the client trusts the server because the server presents a certificate issued by the CA that the client trusts.

![Server Authentication Diagram](image)

Figure 26: Server authentication
Client authentication

Client authentication is similar to server authentication, except that the roles are reversed. In the case of client authentication the server asks the client to provide the client certificate.

The process of client authentication occurs on the server, as follows:

1. The server sends a request to the client asking for the client certificate.
2. The client sends the client certificate to the server.
3. The server checks the client certificate to determine the following:
   a. If the client certificate is issued by a certificate authority that the server trusts. The server checks the name of the CA. To comply, the name of the certification authority (CA) on the certificate must match the name of the CA on the server's trusted certificate.
   b. If the client certificate is within its validity window. The server checks to see if the current time falls between the Not Before and Not After dates in the client certificate.

When all the security checks are satisfied the client and server can exchange secure messages.

In this situation the server trusts the client because the client presents a certificate issued by the CA that the server trusts.

Figure 27: Client Authentication

The AE Services default certificate

You can use the default certificates installed by AE Services in your lab environment if you have not installed your own certificates.

Note:

- AE Services installs a default certificate. You can delete the default certificate. But please install a third party certificate for AE Services to be able to continue using secure links. If no certificates are present, you can use only non-secured links.
- The AE Services server comes pre-installed with a set of default server certificates for lab use. These default server certificates should not be used in a production environment.
environment. It is highly recommended to replace all default installed certificates. See Certificate enrollment and installation on page 100. See Certificate management on page 97 to understand the certificate change and expiration policies.

The default server certificate (serverCert.pem) is located as follows:

/etc/opt/avaya/certs/private/serverCert.pem

Also, by default the AE Services client installation programs for DMCC, TSAPI, JTAPI, and CVLAN install the Avaya Product CA certificate on the client computer. Information about managing certificates on the clients is provided in the following documents.

- Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide, 02-300543
- Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer’s Guide, 02-300359
- Avaya Aura® Application Enablement Services — Device, Media and Call Control .NET API Programmer’s Guide 102-602658
- Avaya Aura® Application Enablement Services JTAPI Programmer’s Guide, 02-603488

Note:
The default configuration for DMCC, TSAPI, JTAPI, and CVLAN, requires no AE Services Management Console administration. The AE Services Certificate Management pages apply only if you are using your own certificates.

AE Services Server authentication and the AE Services Management Console

The AE Services Management Console relies on two software programs, Apache and Tomcat, which require certificates. By default, Apache and Tomcat use a self-signed certificate, which is different from the AE Services server certificate.

Note:
For production environment, it is highly recommended to replace the Apache and Tomcat default installed lab server certificate. See Certificate enrollment and installation on page 100.

Using certificates issued by a certificate authority

If you use certificates issued by a trusted in-house or third-party certificate authority, the AE Services Certificate Management Web pages provide you information to manage these certificates.

Certificate enrollment and installation

If you use your own certificates, AE Services supports both manual and automatic enrollment of certificates.
Overview of manual enrollment

The manual process requires you to manually carry out steps for obtaining and installing certificates. You submit a request to a CA, handle the receipt of the certificates, and then install the certificates. User intervention is required for each task. The Manual method includes the steps described in Checklist for manual enrollment - server authentication on page 101.

Checklist for manual enrollment - server authentication

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Install the Trusted CA's Certificate on client computer.</td>
<td>Browser - (not in the AE Services Management Console). The client user performs this procedure on the computer that the client is installed on.</td>
</tr>
<tr>
<td>2</td>
<td>Create a server certificate request for AE Services</td>
<td>AE Services Management Console - See Creating a server certificate signing request for the AE Services server on page 107.</td>
</tr>
<tr>
<td>3</td>
<td>Create an AE Services server certificate.</td>
<td>Browser - See Creating a server certificate for AE Services (generic procedure) on page 112.</td>
</tr>
<tr>
<td>4</td>
<td>Import the server certificate into AE Services.</td>
<td>AE Services Management Console - See Importing the server certificate into AE Services on page 113.</td>
</tr>
</tbody>
</table>

Overview of automatic enrollment

Automatic enrollment refers to using SCEP (Simple Certificate Enrollment Protocol) certificates. The automatic enrollment process does not require as much administrative intervention as manual enrollment.

With automatic enrollment, you complete the SCEP parameter information on the Add Server Certificate page. When you click Apply on the Add Server Certificate page, AE Services submits the request to the SCEP server. The AE Services Management Console tasks for the SCEP method are described in Checklist for automatic enrollment using SCEP on page 102.
### Checklist for automatic enrollment using SCEP

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a server certificate request (CSR) for AE Services</td>
<td>You are submitting the Certificate Request (CSR) to the CA’s SCEP Server for signing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• On successful execution of the SCEP command, AE Services receives the signed server certificate from the SCEP server. AE Services saves the certificates repository automatically.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In addition to the server certificate, the CA's public certificate is also added to the Trusted Certs repository (if it does not exist already).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• After successful completion of the SCEP command, the server certificate and its private key are bundled into PKCS#12 file. The java key store (JKS) is updated, and the CSR is deleted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✌️ Note: If for some reason, the SCEP command fails, then the CSR is still available and will be listed in the Pending Certificates page. You can choose automatic or manual enrollment for the pending certificates at a later time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See <a href="#">Creating a server certificate signing request for the AE Services server</a> on page 107.</td>
</tr>
<tr>
<td>2</td>
<td>Create an AE Services server certificate.</td>
<td>Browser - See <a href="#">Creating a server certificate for AE Services (generic procedure)</a> on page 112.</td>
</tr>
<tr>
<td>3</td>
<td>Import the server certificate into AE Services.</td>
<td>AE Services Management Console - See <a href="#">Importing the server certificate into AE Services</a> on page 113.</td>
</tr>
</tbody>
</table>

### Checklist for installing your own certificates - server authentication

If you are installing your own certificates, and you use server authentication, make sure that the Trusted CA’s certificate is installed on the client computer.

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(Client) Install the Trusted CA’s Certificate on client computer.</td>
<td>Browser - (Client web browser as opposed to the AE Services Management Console). The client user performs this procedure on the computer that the client is installed on.</td>
</tr>
</tbody>
</table>
Checklist for installing your own certificates - client authentication

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Install the Trusted CA's certificate on the AE server.</td>
<td>AE Services Management Console. See the following topics:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Obtaining a trusted certificate for the AE Server on page 104</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Importing The trusted certificate into AE Services on page 106.</td>
</tr>
<tr>
<td>2</td>
<td>Install the client computer's certificate (the client certificate)</td>
<td>Client Desktop - Client user perform this procedure on the computer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>that the client is installed on.</td>
</tr>
<tr>
<td>3</td>
<td>Add a trusted host. In the AE Services Management Console (Security &gt; Host AA &gt; Trusted Hosts &gt; Add Trusted Host).</td>
<td>AE Services Management Console. Only the application uses port 4723</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(this is TR87, and the AAC client) for client authentication.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(See Client authentication on page 99).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the DMCC client does not use client authentication.</td>
</tr>
</tbody>
</table>

Enabling client authentication for DMCC Java clients

About this task

Optionally, for the DMCC Java API clients only, the AE Server can provide client authentication by using the Service Settings (Security > Host AA > Service Settings).

Procedure

1. From the AE Services Management Console main menu, select Security > Host AA > Service Settings.
2. From the Service setting page, select the check boxes for Authenticate Client Cert with Trusted Certs and Require Trusted Host Entry.

For an explanation of these settings see Host AA Service settings on page 104.
3. Click **Apply Changes**.

4. From the **Apply Changes to Host AA service settings** page, click **Apply**.

**Host AA Service settings**

This section explains the Host AA service settings.

- **Authenticate Client Cert with Trusted Certs** — If this setting is enabled, AE Services issues a request for the client certificate and it rejects incoming connections if the client certificate is not signed by a trusted certificate authority (CA).

- **Enforce Host Authorization** — If this setting is enabled, AE Services checks the common name (CN) in the client certificate, and verifies that it matches one of the administered authorized hosts. If the CN matches one of the authorized hosts, the connection is permitted. If the CN does not match, the connection is rejected.

**Enterprise server authentication (LDAP Server)**

If your configuration uses an enterprise directory server (also referred to an external directory server), you will need to configure AE Services to access an enterprise directory and verify the enterprise directory server’s certificate.

To this you will need to complete the Enterprise Directory Configuration page in the AE Services Management Console and enable the setting for LDAP-S. See Configuring AE Services to access an enterprise directory on page 189.

**File conversion for DER and PKCS#12 files**

If your CA provides you with a certificate in a format other than PEM, you must convert it to PEM format before importing it into the AE Services Management Console. The following sections describe how to convert files using openssl tools, which are on the AE Server in `/usr/bin`.

**Converting a DER file to PEM**

**About this task**

If your Certificate Authority provides you with a DER-encoded certificate, you must convert it to PEM format before you can import it into the AE Services Management Console.

**Procedure**

To convert a DER file to PEM, from the command line type the following command:

```bash
openssl x509 -in <input>.cer -inform DER -out <output>.pem -outform PEM
```

**Obtaining a trusted certificate for the AE Services server**

**About this task**

This information is for general reference only. Follow the instructions on your CA Web site.

**Procedure**

1. From your browser, go to your Web page for CA and download the certificate chain.
Important:

You must import the entire certificate chain all the way back to the root certificate.

• The trusted certificate or certificate chain must be in text format (PEM or Base-64). If you are importing a certificate chain, it must be a text-based PKCS#7 file. Think of a PKCS#7 file as an envelope containing all trusted certificates.

• It is acceptable to import certificates in the chain individually if they are not available in PKCS#7 format, but all certificates must be in the trusted certificates store.

2. The certificate authority processes your request and issues a trusted certificate (or certificate chain) for you to download.

3. Download the entire certificate to the AE Services administrative workstation, and save it with a unique name (for example, C:\temp\aetrucert.cer).

4. Using a text editor, verify the header and trailer of the trusted certificate file.

• The header and trailer for a PEM or Base 64 file are as follows:
  
  ----BEGIN CERTIFICATE----- (header)
  ----END CERTIFICATE----- (trailer)

• The header and trailer for a PKCS#7 file are as follows:
  
  -----BEGIN PKCS7 ----- (header)
  -----END PKCS7----- (trailer)

Note:

The header and trailer in the imported certificate file must read as follows before you import the contents of the file into the AE Services Management Console.

-----BEGIN PKCS7-----
-----END PKCS7-----

or

-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----

If the header and trailer of your PKCS#7 file do not match either of these two forms, you must edit the header and trailer before you import the file into the AE Services Management Console.

Next steps

Continue with the following procedures:

• Importing The CA certificate into your browser’s certificate store on page 55.
• Importing the trusted certificate into AE Services on page 106.
Importing the trusted certificate into AE Services

**Procedure**

1. From the AE Services Management Console main menu, select **Security > Certificate Management > CA Trusted Certificates**.
2. From the **CA Trusted Certificates** page, click **Import**.
3. Complete the **Trusted Certificate Import** page, as follows:
   a. Click **Browse**.
   b. In the Choose File to Upload dialog box, select the certificate you want to import, and then click **Open**.
   c. In the **Certificate Alias** field, type an alias for the trusted certificate (for example `catrusted`).
      The trusted certificate alias can be arbitrary. It does not need to match any aliases for AE Services.
   d. Click **Apply**.

AE Services recommends that you verify the installation of the certificate. See [Verifying the installation of the trusted certificate in AE Services](#) on page 106.

Verifying the installation of the trusted certificate in AE Services

**About this task**

Use this procedure to verify the installation of the entire certificate chain (all the way back to the root certificate) in AE Services.

**Procedure**

1. From the AE Services Management Console main menu, select **Security > Certificate Management > CA Trusted Certificate**.
2. From the **CA Trusted Certificates** page, select the trusted certificate (`catrusted` based on this sample scenario), and click **View**.
3. From the **Trusted Certificate Details** page, verify that the information for the trusted certificate is correct.
   a. Verify that the entire chain of certificates exists, all the way back to a self-signed certificate.
   b. Verify that the **Issued To** field displays the name of the organization that the trusted certificate is issued to.
   c. Verify that the **Issued By** field indicates the name of the certificate authority that issued the trusted certificate (referred to as the issuer on the certificate).
      This issuer should be either the same issuer or an issuer in the same certificate chain.
   d. Verify that the **Expiration Date** indicates the date that the trusted certificate expires.
   e. Verify the information in the Details display. Make sure the Certificate Status is valid.
4. Click **Close** to exit the **Trusted Certificate Details** page.

**Creating a server certificate signing request for the AE Services server**

**About this task**

Use this procedure to create a server certificate request (also referred to as a certificate signing request, or CSR) for the AE Services server. This procedure generates a certificate signing request which includes a private key.

**Procedure**

1. From the AE Services Management Console main menu, select **Security > Certificate Management > Server Certificates**.
2. On the **Server Certificates** page, click **Add**.
3. Complete the **Add Server Certificate** page, as follows:
   a. In the **Certificate Alias** field, select the appropriate alias for the certificate.
      - Select **cmtls** for the Transport Service certificate
      - Select **aeservices** for the CVLAN, DLG, DMCC and TSAPI certificates. If **cmtls** is not specified, and the switch connection Provide AE Services certificate to switch option is enabled, this certificate will be used for the Transport Service.
      - Select **web** for the Apache and Tomcat certificates.
      - Select **ldap** for the LDAP certificate.
      - Select **server** to include all certificates (cmtls, aeservices, web, and ldap).
      - Select **rsyslog** for remote logging.
   b. Leave the **Create Self-Signed Certificate** check box unchecked (the default).
   c. In the **Enrollment Method** field, select the appropriate setting.
   d. In the **Encryption Algorithm** field, select **3DES**.
   e. In the **Password** field, type the password of your choice.
   f. In the **Re-enter Password** field, type the password of your choice.
   g. In the **Key Size** field, accept the value **2048** or higher
   h. In the **Certificate Validity** field, accept the default **1825**.
   i. In the **Distinguished Name** field, type the LDAP entries required by your CA.
      
      These entries must be in LDAP format and they must match the values required by your CA. If you are not sure what the required entries are, contact your CA.

      Among the required entries will be the FQDN (fully qualified domain name) of the AE Server in LDAP format. Additionally you might need to provide your company name, your organization name and so on. Separate each LDAP entry with a comma, and do not use blank spaces, for example:
      
      ```
cn=aeserver.example.com,ou=myOrganizationalUnit,o=Examplecorp,L=Springfield,ST=Illinois,C=US
```
**Note:**

Currently the Add Server Certificate page in the AE Services Management Console does not support using commas within a DN attribute (for example o=Examplecorp, Inc).

j. In the **Challenge Password** field, type the challenge password of your choice.

k. In the **Re-enter Challenge Password** field, type the challenge password of your choice.

l. (Optional) From the **Key Usage** list, select the setting that is appropriate for your certificate:
   - Digital Signature
   - Non-repudiation
   - Key encipherment
   - Data encipherment
   - Key agreement
   - Key certificate sign
   - CRL sign
   - Encipher Only
   - Decipher Only

m. (Optional) From the **Extended Key Usage** list, select the setting appropriate for your certificate.

n. (Optional - applies to auto-enrollment) Complete the **SCEP Parameters** that apply to your certificate:
   - **SCEP Server URL** — specify the CA URL.
     
     An example of a Microsoft CA URL is http://ca.example.com/certsrv/mscep/mscep.dll. An example of an Enterprise Java Beans Certificate Authority (EJBCA) URL is http://ca.example.com:8080/ejbca/publicweb/apply/scep/pkiclient.exe.
   - **CA Certificate Alias** — enter the CA Alias to be used.
     
     The CA Certificate Alias refers to the name used to identify the CA Certificate.
   - **CA Identifier** — enter the CA ID to be used.
     
     The CA Identifier Used by CAs to identify which CA you are referring to in your SCEP request. Many CAs strictly match the CA Identifier string, while some ignore it. For example, with EJBCA you you need to match the CA Identifier string. This is used when the CA server acts as multiple CAs. This string is set by the CA Admin.

o. Click **Apply**.

AE Services displays the **Server Certificate Manual Enrollment Request** page, which displays the certificate alias and the certificate request itself in PEM (Privacy
Enhanced Mail) format. The certificate request consists of all the text in the box, including the header (-----BEGIN CERTIFICATE REQUEST -----) and the trailer (-----END CERTIFICATE REQUEST-----).

4. Copy the entire contents of the server certificate, including the header and the trailer. Keep the contents available in the clipboard for the next procedure.

Add Server Certificate field descriptions

<table>
<thead>
<tr>
<th>Add Server Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Certificate Alias</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Enrollment Method</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Certificate Key Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Encryption Algorithm</strong></td>
<td>The data encryption standard (DES) used to encrypt the private key.</td>
</tr>
<tr>
<td></td>
<td>The options are:</td>
</tr>
<tr>
<td></td>
<td>• The 3DES is the default setting.</td>
</tr>
<tr>
<td></td>
<td>• The DES is less secure than 3DES and uses a 56 bit key size.</td>
</tr>
<tr>
<td></td>
<td>The default is 3DES.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Certificate key or private key password which is used to lock the certificate key.</td>
</tr>
<tr>
<td><strong>Re-enter Password</strong></td>
<td>The certificate key password reentered.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Size</strong></td>
<td>The key length of the certificate key.</td>
</tr>
<tr>
<td></td>
<td>• 1024 specifies a key length of 1024 bits.</td>
</tr>
<tr>
<td></td>
<td>• 1536 specifies a key length of 1536 bits.</td>
</tr>
<tr>
<td></td>
<td>• 2048 specifies a key length of 2048 bits.</td>
</tr>
<tr>
<td></td>
<td>• 4096 specifies a key length of 4096 bits.</td>
</tr>
<tr>
<td></td>
<td>The default setting is 2048.</td>
</tr>
<tr>
<td><strong>Signature Algorithm</strong></td>
<td>The appropriate signature algorithm.</td>
</tr>
<tr>
<td></td>
<td>The default is sha256.</td>
</tr>
</tbody>
</table>

**Certificate Request Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Certificate validity</strong></td>
<td>The number of days that indicate the lifetime of the certificate.</td>
</tr>
<tr>
<td></td>
<td>The default is 1825 days or 5 years.</td>
</tr>
<tr>
<td><strong>Distinguished Name</strong></td>
<td>The LDAP entries required by your CA. These entries must be in LDAP format and they must match the values required by your CA. If you are not sure what the required entries are, contact your CA.</td>
</tr>
<tr>
<td></td>
<td>Among the required entries will be the FQDN of the AE Services Server in DNS format. Additionally you might need to provide your company name, your organization name and so on. Separate each LDAP attribute with a comma, and do not use blank spaces, for example:</td>
</tr>
<tr>
<td></td>
<td>cn=myaeserver.example.com,ou=myOrganizationalUnit, o=examplecorp,L=Springfield,ST=Illinois,C=US</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>If an LDAP name contains an attribute that has a comma within it, you must precede the comma with a backslash () when you enter the LDAP name in OAM.</td>
</tr>
<tr>
<td><strong>Challenge Password</strong></td>
<td>Certificate key or private key password which is used to lock the certificate request.</td>
</tr>
<tr>
<td><strong>Re-enter Challenge Password</strong></td>
<td>The certificate key password reentered for validation.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Usage</td>
<td>Key description contained in the certificate. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Digital Signature.</td>
</tr>
<tr>
<td></td>
<td>• Non-repudiation</td>
</tr>
<tr>
<td></td>
<td>• Key encipherment</td>
</tr>
<tr>
<td></td>
<td>• Data encipherment</td>
</tr>
<tr>
<td></td>
<td>• Key agreement</td>
</tr>
<tr>
<td></td>
<td>• Key certificate sign</td>
</tr>
<tr>
<td></td>
<td>• Key encipherment</td>
</tr>
<tr>
<td></td>
<td>• CRL sign</td>
</tr>
<tr>
<td></td>
<td>• Encipher only</td>
</tr>
<tr>
<td></td>
<td>• Decipher only</td>
</tr>
</tbody>
</table>

**Note:**
To deselect a Key Usage selection, use **Ctrl-Click**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Extended Key Usage</strong></td>
<td>Purpose of the certificate. Select one of the following:</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>To deselect an Extended Key Usage selection, use <strong>Ctrl-Click</strong>.</td>
</tr>
<tr>
<td></td>
<td>• SSL/TLS Web Server Authentication</td>
</tr>
<tr>
<td></td>
<td>• SSL/TLS Web Client Authentication</td>
</tr>
<tr>
<td></td>
<td>• Code Signing</td>
</tr>
<tr>
<td></td>
<td>• E-mail Protection (S/MIME)</td>
</tr>
</tbody>
</table>

**SCEP Parameters:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCEP Server URL</td>
<td>The URL of the CA's SCEP or Simple Certificate Enrollment Protocol Server.</td>
</tr>
<tr>
<td>CA Certificate Alias</td>
<td>The unique and descriptive name for the CA certificate. This can be a name that you assign or a name that the CA assigns. If the CA has assigned the name, use that name.</td>
</tr>
<tr>
<td>CA Identifier</td>
<td>The identification of the CA.</td>
</tr>
</tbody>
</table>
Creating a server certificate for AE Services (generic procedure)

About this task
If you are using a third-party certificate authority other than Microsoft Certificate Services, refer to this procedure. This procedure is provided as a guide only and should be used in conjunction with the instructions on your CA Web site.

Procedure
1. From your browser, go to your CA's Web page for requesting a server certificate.
2. Complete the required fields for enrollment.
   Usually you provide information such as your name, email address, the IP address of your server, your organizational unit (OU), and the type of server you have.
3. Paste the CSR into the appropriate field and submit or upload the request.
   (Paste the certificate request that you copied in the last step of the previous procedure Creating a server certificate signing request for the server on page 107.)
   The certificate authority processes your request and issues a server certificate for you to download.
4. Download the certificate to your AE Services administrative workstation, and save it with a unique name (for example C:\aescert.cer).

   ! Important:
   The certificate data you import into AE Services must be PEM-encoded (Base 64). If your CA issues certificates in DER format, you must convert it to PEM format before importing it into AE Services. See Converting a DER file to PEM on page 104 for more information.

Creating an AE Services server certificate (Microsoft-based procedure)

About this task
If you use Microsoft Certificate Services as the certificate authority, use this procedure as a guide for creating an AE Services server certificate.
Procedure

1. From your Web browser, type the URL of your certificate server. For example:
   http://<certificate_server.com>/certsrv

   where <certificate_server.com> is the domain name or IP address of your certificate server.

2. On the **Welcome** page of Microsoft Certificate Services, click **Request a certificate**.

3. On the **Request a Certificate** page, click **advanced certificate request**.

4. On the **Advanced Certificate Request** page, click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file** or **Submit a renewal request by using a base-64-encoded PKCS #7 file**.

   (AE Services uses a base-64-encoded CMC).

5. On the **Submit a Request or Renewal Request** page, paste the certificate request into the **Saved Request** field, and click **Submit**.

   (Paste the certificate request that you copied in the last step of the procedure **Creating a server certificate signing request for the server** on page 107.)

6. From the **Certificate Issued** page, select **Base 64 encoded**, and click **Download certificate**.

   ✤ **Note:**

   Some CAs are not set up to automatically grant certificates. In this case, you might have to wait until your administrator issues the certificate. Once your administrator issues the certificate, return to the Welcome page of Microsoft Certificate Services, and click **View the status of a pending certificate request** to get to the **Issued Certificate** page.

7. From the **File download** dialog box, save the certificate to your computer.

Importing the server certificate to AE Services

**About this task**

Use this procedure to import the AE Services server certificate to the AE Services management console.

**Before you begin**

Ensure that the server certificate is in PEM format. If not, see **File conversion for DER and PKCS#12 files** on page 104.

**Procedure**

1. On the AE Services management console main menu, navigate to **Security > Certificate Management > Server Certificates**.

2. On the Server Certificates page, click **Import**.
3. On the Server Certificate Import page, do the following:
   a. Click **Browse**.
   b. In the **Choose File to Upload** dialog box, select the server certificate that you want to import, and then click **Open**.
   c. Select the **Establish Chain of Trust** check box. By default, the check box is selected.
   d. In the **Certificate Alias** field, select the appropriate certificate alias, for example, aeservices, ldap, server, cmtls, rsyslog, or web.
   e. Click **Apply**.

**Server Certificate Import field descriptions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Path</td>
<td>The location of the certificate file.</td>
</tr>
<tr>
<td>Certificate Alias</td>
<td>The alias of the certificate file to import. The options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>aeservices</strong> refers to the AE Services: CVLAN, DLG, DMCC and TSAPI.</td>
</tr>
<tr>
<td></td>
<td>• <strong>web</strong> refers to Apache and Tomcat.</td>
</tr>
<tr>
<td></td>
<td>• <strong>cmtls</strong> refers to CM transport layer security</td>
</tr>
<tr>
<td></td>
<td>• <strong>ldap</strong> refers to LDAP.</td>
</tr>
<tr>
<td></td>
<td>• <strong>server</strong> refers to all aeservices, web, and ldap.</td>
</tr>
<tr>
<td></td>
<td>• <strong>rsyslog</strong> refers to TLS connection for remote logging.</td>
</tr>
<tr>
<td></td>
<td>The alias must match the alias you specified when you created the Certificate Signing Request (CSR). By default this field is blank.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browse</td>
<td>To locate the certificate file.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish Chain of Trust</td>
<td>To establish a chain of trust when you import a signed server certificate. Includes all certificates in the chain of trust, including the root CA, when you import the signed server certificate. By default this check box is selected. If your AE Services Implementation for Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007 does not use a CA hierarchy, you can clear this check box.</td>
</tr>
<tr>
<td>Apply</td>
<td>To import the server certificate to the AE Services certificate store.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong></td>
</tr>
<tr>
<td></td>
<td>After importing a server certificate you must restart the Web Server.</td>
</tr>
<tr>
<td>Close</td>
<td>To go back to the Server Certificates page.</td>
</tr>
</tbody>
</table>

Verifying the installation of the server certificate in AE Services

**About this task**

**Procedure**

1. From the AE Services Management Console main menu, select **Security > Certificate Management > Server Certificates**.
2. From the **Server Certificates** page, select the alias of the server certificate (aeservercert, based on this sample scenario), and click **View**.
3. From the **Server Certificate Details** page, verify that the information for the server certificate is correct.
   a. Verify that the **Issued To** field displays the fully qualified domain name of the AE Server.
   b. Verify that the **Issued By** field indicates fully-qualified domain name of the certificate authority that issued the server certificate.
   c. Verify that the **Expiration Date** indicates the date that the server certificate expires.
   d. Verify the information in the **Details** window. Make sure the Certificate Status is valid.
4. Click **Close** to exit the **Server Certificate Details** page.
About restarting the AE Services Server and the Web Server

About this task
Apache and Tomcat do not use the default server certificate. Instead they use self-signed certificates. If you install your own certificates, AE Services, Apache, and Tomcat must be restarted so that they all use the same certificate.

To restart these services, see Restarting the AE Server and the Web Server on page 127.

Backing up certificates

About this task
Use the AE Services Management Console Data Backup feature to back up the AE Services certificates. The data backup image includes the certificates that have been administered on the AE Server.

Procedure
To back up the AE Server data, which includes certificate files, see Backing up server data on page 120.

Restoring certificates

About this task
Use the AE Services Management Console Restore Data feature to restore the certificates. When you restore the AE Server data, the certificates are restored.

Procedure
To restore the AE Server data, which includes certificate files, see Restoring the server data on page 121.

Certificate renewal

Certificates are valid only for a certain period of time. To ensure that you have no service interruptions, you should request a certificate renewal from your certificate authority before the date that the certificate is set to expire. When you renew a certificate, you are replacing the expired certificate with a new certificate. The new certificate contains the same public key as the expired certificate.

The process for renewing a certificate involves the following activities.

- Select the certificate that is about to expire, and generate a certificate signing request (CSR) for the certificate. See Renewing certificates – creating the CSR on page 117.
- Submit the CSR to your certificate authority (CA). See Renewing certificates – submitting the CSR to certificate authority (Microsoft example) on page 117.
- Your certificate authority will processes the CSR and issue a new server certificate for you to download.
- Download the new certificate to your AE Services administrative workstation, and save it with a unique name (for example, C:\aescert.cer).
Important:

The certificate data you import into AE Services must be PEM-encoded (Base 64). If your CA issues certificates in DER format, you must convert it to PEM format before importing it into AE Services. See Converting a DER file to PEM on page 104.

- Replace the old certificate with the new certificate. See Renewing certificates – replacing the old certificate with the new certificate on page 118.

Renewing certificates – creating the CSR

Procedure

1. From the AE Services Management Console main menu, select Security > Certificate Management > Server Certificates.

2. From the Server Certificates page, select the check box next to the certificate you want to renew, and click Renew.

   Your browser displays the Server Certificate Renew Continue page, which contains a text box displaying the certificate signing request (CSR) for the certificate you requested.

3. Copy the CSR and paste it into a text editor. Be sure not to include any extra spaces or lines.

4. From the Server Certificate Renew Continue page, click Close.

   AE Services creates a Pending Server Certificate Request for the certificate you selected. Your next step is to submit the CSR to your certificate authority.

Renewing certificates – submitting the CSR to certificate authority (Microsoft example)

About this task

If you use Microsoft Certificate Services as the certificate authority, use this procedure as a guide for renewing an AE Services server certificate.

Procedure

1. From your Web browser, type the URL of your certificate server. For example:

   http://<certificate_server.com>/certsrv

   where <certificate_server.com> is the domain name or IP address of your certificate server.

2. On the Welcome page of Microsoft Certificate Services, click Request a certificate.

3. On the Request a Certificate page, click advanced certificate request.

4. On the Advanced Certificate Request page, click Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file or Submit a renewal request by using a base-64-encoded PKCS #7 file. (AE Services uses a base-64-encoded CMC.)

5. On the Submit a Request or Renewal Request page, paste the certificate request into the Saved Request field, and click Submit. (Paste the certificate request that you copied...
when you completed the procedure Renewing certificates – creating the CSR on page 117.)

6. From the Certificate Issued page, select Base 64 encoded, and click Download certificate.

   ✔ Note:

   Some CAs are not set up to automatically grant certificates. In this case, you might have to wait until your administrator issues the certificate. Once your administrator issues the certificate, return to the Welcome page of Microsoft Certificate Services, and click View the status of a pending certificate request to get to the Issued Certificate page.

7. From the File download dialog box, save the certificate to your computer.

Renewing certificates – replacing the old certificate with the new certificate

Procedure

1. From the AE Services Management Console main menu, select Security > Certificate Management > Server Certificates > Pending Requests.

2. From the Pending Server Certificate Requests page, select the certificate you want to renew, and click Manual Enroll.

3. From the Server Certificate Renew Continue page, click Renew.


5. From the Choose file dialog box, locate the server certificate you downloaded, and click Open.

6. From the Server Certificate Renew page, click Apply.

Certificate authentication between the AE Services server and Communication Manager

With AE Services 7.0, the AE Services Transport service will enforce validation of the Communication Manager identity certificate for all administered switch connections.

The connection to the Communication Manager is rejected if the AE Services server does not contain the CA certificate for Communication Manager. You can import the CA certificate used for Communication Manager by using the Management Console screen, Security > Certificate Management > CA Trusted Certificates. This new validation enforcement will affect all AE Services offer types regardless if secure mode with FIPS is enabled or disabled.

When in secure mode with FIPS, the AE Services server and Communication Manager exchange identity certificates and mutually authenticate the other side certificate.

If the AE Services server is not configured to send an identity certificate to Communication Manager and y option in the TLS Mutual Authentication for H.323 stations field is selected,
Communication Manager will not accept the security profile, H323TLS, in the Gatekeeper Confirmation (GCF).

If AE Services attempts to set up a TLS connection, Communication Manager will reject the TLS request. If the AE Services server is not configured to send an identity certificate to Communication Manager and an option in the **TLS Mutual Authentication for H.323 stations** field is selected, Communication Manager will allow the TLS connection to AE Services for H.323 registrations to proceed without an identity certificate.

The **Provide AE Services certificate to switch** field is used to configure the AE Services Transport service. The AE Services Transport services respond with a valid identity certificate to a Certificate Request message during the TLS handshake with Communication Manager. The first installed AE Services identity certificate associated with the alias cmtls, aeservices, or server is used as the identity certificate.
Chapter 6: AE Services general maintenance

Backing up the server data

About this task

Use this procedure to back up the AE Services server data, which includes configuration data files, AE Services user database, certificates, and the license file.

Backup taken in the non secure mode can only be restored in the non secure mode. Backup taken in the secure mode can only be restored in the secure mode.

The average size of AE Services full backup is 10 MB, but it can increase up to 1 GB depending on the size of Historical Metric Data Collector (HDMC). For information about HMDC, see Administering Avaya Aura® Application Enablement Services.

Procedure

1. On the AE Services Management Console main menu, click Maintenance > Server Data > Backup.

2. To encrypt the backup file, do one of the following:
   a. Select the Encrypt Backup File check box, and click Continue.
   b. In the Password field, enter the password you want to use for the encrypted backup file.

      This password must contain 15 to 256 characters. This password should not contain: apostrophe (‘), backslash (\), single quote (‘), double quote (“), and percent (%).
   c. In the Confirm Password field, re-enter the password.
   d. Click Continue.

3. On the Database Backup Continue page, click the here link to download the log file.
Restoring the server data

About this task
Restoring the AE Services server data involves restoring a copy of the AE Services database and restarting AE Services. The AE Services database includes configuration data files, the AE Services user database, certificates, and the license file.

Backup taken in the non secure mode can only be restored in the non secure mode. Backup taken in the secure mode can only be restored in the secure mode.

If the size of a backup file is greater than 10 MB, restore the server data using the Command Line Interface (CLI).

Procedure
1. In the AE Services Management Console main menu, click **Maintenance > Server Data > Restore**.
2. On the Restore Database Configuration page, click **Browse** and locate the AE Services database backup file that you intend to use. For example, `<hostname>_AES version>_aesvcsdb05052013.tar.gz.enc` if the file is encrypted or `<hostname>_AES version>_aesvcsdb05052013.tar.gz` if the file is not encrypted.
3. Click **Restore**.
4. On the Restore Database Configuration page, click **Restart Services**.

**Caution:**
If you make any changes in the AE Services Management Console in the interval between clicking **Restore** and **Restart Services**, the restore will not occur.

---

Restoring the server data by using the command line interface

About this task
You can restore the server data by using command line interface when the size of a backup file is greater than 10 MB.

Procedure
1. Log in to the AE Services as a root user.
2. Copy the backup file to the `/tmp` directory by using the following command:

   ```
   cp <backup file> to /tmp
   ```
3. Do the following:
   • Run the following command to restore with the GRHA configuration:
     `/opt/mvap/bin/Restore.sh -L </path/to/LargeAESBackupFile.tar.gz>`
   • Run the following command to restore without the GRHA configuration:
     `/opt/mvap/bin/Restore.sh -L -n </path/to/LargeAESBackupFile.tar.gz>`

4. Run the following commands to restart the services:

   ```
   systemctl restart DBService
   systemctl restart aesvcs
   systemctl restart iptables
   systemctl restart httpd
   systemctl restart snmpd
   systemctl restart subagent1
   ```

---

**Logs**

Use Logs to access the following types of log files that can be generated using AE Services:

- **Audit Logs** — Use Audit Logs to see administrative changes made through the OAM web interface.
- **Error Logs** — Use Error Logs to view CRITICAL, WARNING, and FYI messages generated by any of the call control services (DMCC, TSAPI, CVLAN, and DLG) you are licensed to use.
- **Install Logs** — Use Install Logs to verify the success of an installation or upgrade, or to troubleshoot problems.
- **Security Logs** — Use Security Logs to access the following logs:
  - Client Access Logs - Use client access logs to see information about client activity (CVLAN, DLG, TSAPI, and Transport).
  - Command Logs - Use command logs to see information about system activity and errors.
  - System Reset Logs - Use system reset logs to see a historical record of when the AE Services server was stopped and started.
- **Syslog (var log)** — Use Syslog to view various kinds of systems activity. Only the Security Administrator and System Administrator are able to access syslogs.
- **User Management Service logs** — Use User Management Service logs to view User Management Service activities and errors.

**Related links**

- [Viewing log files](#) on page 123
- [Downloading log files](#) on page 123
- [Administering switch connections for DMCC applications that use Registration Services - assigning H.323 IP addresses](#) on page 75
- [Enabling AE Services](#) on page 25
Viewing log files

Procedure
1. From the AE Services Management Console main menu, select Status > Logs > <log file> where <log file> can be:
   - Audit Logs
   - Error Logs
   - Install Logs
   - Security Logs > Client Access Logs
   - Security Logs > Command Logs
   - Security Logs > System Reset Logs
   - Syslog
   - Tripwire Logs
   - User Management Service Logs

Note:
Tripwire Logs are not available for the Software-Only server.

2. Click View.

Related links
Logs on page 122
Administering switch connections for DMCC applications that use Registration Services - assigning H.323 IP addresses on page 75
Enabling AE Services on page 25

Downloading log files

Procedure
1. From the AE Services Management Console main menu, select Status > Logs > <log file> where <log file> can be:
   - Audit Logs
   - Error Logs
   - Install Logs
   - Security Logs > Client Access Logs
   - Security Logs > Command Logs
   - Security Logs > System Reset Logs
• Syslog
• Tripwire Logs
• User Management Service Logs

🌟 Note:

Tripwire Logs are not available for the Software-Only server.

2. Select the check box(es) for the log file(s) you want to download.

3. Click **Download**.

4. On the **Download** page, click the **here** link to download the log file.

**Related links**

- [Logs](#) on page 122
- [Administering switch connections for DMCC applications that use Registration Services - assigning H.323 IP addresses](#) on page 75
- [Enabling AE Services](#) on page 25

---

**Service Controller (start, stop, and restart services)**

Use the Service Controller (**Maintenance > Service Controller**) to start, stop, and restart any of the following services:

- ASAI Link Manager
- DMCC Service (Device, Media, and Call Control)
- CVLAN Service
- DLG Service
- Transport Layer Service
- TSAPI Service

Additionally, the Service Controller provides the following capabilities:

- Restart AE Server - stops and starts (restarts) all services listed on the Service Controller page. Restarting the AE Server does not start and stop the Web Server.
- Restart Linux - stops and starts (restarts) the Linux operating system, as well as the AE Server (all services listed on the Service Controller page) and the Web Server.
- Restart Web Server - Stops and starts (restarts) Apache and Tomcat.

⚠️ Warning:

It is generally understood that stopping and starting (or restarting) a service is potentially disruptive to applications. Doing so can result in dropped connections and lost associations.
For an illustration of service dependencies, see Schematic view of an configuration on page 125.
About stopping services

The following table shows service dependencies and explains the effects of stopping the services listed on the Service Controller page.

**Note:**

A stopped AE Service will remain in a stopped state after a server reboot.

<table>
<thead>
<tr>
<th>Service</th>
<th>Impact of stopping the service</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMCC Service</td>
<td>If you stop the DMCC service, you lose functionality of the following:</td>
</tr>
<tr>
<td>(Device, Media, and Call Control)</td>
<td>• All DMCC services</td>
</tr>
<tr>
<td></td>
<td>All other AE Services continue to operate.</td>
</tr>
<tr>
<td>DLG Service</td>
<td>If you stop the DLG service, you lose DLG functionality, but all other AE Services continue to operate.</td>
</tr>
<tr>
<td>CVLAN Service</td>
<td>If you stop the CVLAN service, you lose CVLAN functionality, but all other AE Services continue to operate.</td>
</tr>
<tr>
<td>TSAPI Service</td>
<td>If you stop the TSAPI service, you lose TSAPI functionality and the following clients will not operate:</td>
</tr>
<tr>
<td></td>
<td>• TSAPI</td>
</tr>
<tr>
<td></td>
<td>• JTAPI</td>
</tr>
<tr>
<td></td>
<td>• Telephony Web Service</td>
</tr>
<tr>
<td></td>
<td>• DMCC with Call Control</td>
</tr>
<tr>
<td></td>
<td>All other AE Services continue to operate.</td>
</tr>
</tbody>
</table>

*Table continues…*
## Service Impact of stopping the service

<table>
<thead>
<tr>
<th>Service</th>
<th>Impact of stopping the service</th>
</tr>
</thead>
</table>
| ASAI Link Manager     | • If you stop the ASAI Link Manager, you lose ASAI link level functionality. DMCC with Call Information Services continues to communicate with Communication Manager. The TSAPI service and the CVLAN service continue to run, but they cannot communicate with the Transport Layer and Communication Manager.  
  - DLG applications and Device, Media, and Call Control applications that only use device and media control continue to communicate with Communication Manager.  
  - DMCC with Call Control can not communicate with Communication Manager.  
• If you restart the ASAI Link Manager you do not have to restart the TSAPI service, the CVLAN service, Telephony Web service, or the Device, Media, and Call Control service. These services will recover. All of their clients, however, would need to reconnect. |
| Transport Layer Service | • If you stop Transport Layer Services, the following services continue to run: the ASAI Link Manager, the TSAPI service, JTAPI, the CVLAN service, the DLG service, Device, Media, and Call Control with Call Information services, and Device, Media, and Call Control with Call Control services and Snapshot services, but they cannot communicate with Communication Manager.  
  - Device, Media, and Call Control applications that only use device and media control continue to operate and can communicate with Communication Manager.  
• If you restart the Transport Layer Service, you do not have to restart the ASAI Link Manager, the TSAPI service, the CVLAN service and the Device, Media, and Call Control service. These services will recover. You will, however, need to restart the DLG service. Also if you restart the Transport Layer service, clients of the following services would need to reconnect: TSAPI, Telephony Web service, Device, Media, and Call Control with Call Information services, Device, Media, and Call Control with Call Control services and Snapshot services, CVLAN, DLG. |

## Restarting the AE Services server and the web server

### About this task

Use this procedure to restart the AE Services server and the web server after you install your own certificates.

Apache and Tomcat do not use the default server certificate. Instead, they use self-signed certificates. If you install your own certificates, AE Services, Apache, and Tomcat must be restarted so that they all use the same certificate.

### Before you begin

Get system administration privileges to perform this task.
Procedure

1. On the AE Services Management Console main menu, click **Maintenance > Service Controller**.

2. On the Service Controller page, click **Restart AE Server**.
   The system restarts the ASAI Link Manager, the DMCC service, the CVLAN service, Transport Layer service, and the TSAPI service.

3. On the confirmation page, click **Restart** to restart the AE Services server.

4. On the AE Services Management Console main menu, click **Maintenance > Service Controller**.

5. On the Service Controller page, click **Restart Web Server**.
   The system restarts Apache and Tomcat.

6. On the Restart Web Server page, click **Restart** to restart the web server.

7. On the AE Services log in screen, log in to AE Services.

---

About rsyslog

All AE Services logs are recorded using rsyslog. 4DMCC, LCM, HMDC, snmp subagent, Tomcat and the AE Services OAM web services deployed on Tomcat use the log4j syslog adaptor (UDP).

TSAPI, TRANSPORT, CVLAN, DLG, ASAILINK and HTTPD record logs using glibc's syslog (/dev/syslog).

The rsyslog configuration for all the above mentioned services is present in `/etc/rsyslog.d/`. The file names are as follows:

- mavp.conf (TSAPI/TRANSPORT/CVLAN/DLG/ASAILINK)
- aesvcs.conf (DMCC, LCM)
- catalinaRsyslog.conf (tomcat, OAM)
- httpdRsyslog.conf (httpd).

**Note:**

Watchdog and ossicm logs are not logged via rsyslog

With rsyslog, log messages conform to Avaya CEC requirements.

See System Logging to learn how to send log data to a remote server.

**Related links**

- [Administrating switch connections for DMCC applications that use Registration Services - assigning H.323 IP addresses](#) on page 75
- [Enabling AE Services](#) on page 25
About System Logging

Using system logging, you can enable remote logging to specify the remote log server destination and port to forward the AE Services server log files. You can also configure trace and log levels by using the log manager.

⚠️ Note:
TSAPI logs are not forwarded to the remote log server.

Configuring remote logging

About this task
Use this procedure to configure forwarding of AE Services logs to a remote syslog server.

⚠️ Note:
TSAPI logs are not forwarded to the remote syslog server.

Before you begin
Configure a remote syslog server.

Procedure

1. On the AE Services Management Console main menu, click Status > Log Manager > System Logging.
3. Complete the other fields as required and then click Apply Changes.
   For more information about system logging field descriptions, see System Logging field descriptions on page 129.
4. Copy all files from the /etc/rsyslog.d/ directory on the AE Services server to the /etc/rsyslog.d directory on the remote syslog server.
5. Restart the remote syslog server.

System Logging field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Remote Logging</td>
<td>Enables or disables remote logging.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname (FQDN)/IP Address</td>
<td>IP Address or a fully qualified domain name. A blank value is not accepted.</td>
</tr>
<tr>
<td>Port</td>
<td>Value of the port. The value can either be 514, or in the range of 1024 to 65535.</td>
</tr>
<tr>
<td>Enable TLS Remote Logging</td>
<td>Enables TLS remote logging for secure and non secure connection between AE Services server and remote rsyslog server. You must install a client certificate with the certificate alias as rsyslog to enable TLS remote logging. Default value: No • <strong>NO</strong>: For non secure connection between AE Services server and remote rsyslog server. • <strong>YES</strong>: For secure connection between AE Services server and remote rsyslog server.</td>
</tr>
<tr>
<td>Common name of Remote Server Certificate</td>
<td>Common name of remote rsyslog server identity certificate. Default value: Blank When <strong>Enable TLS Remote Logging</strong> is set to <strong>YES</strong>, enter the common name of remote rsyslog server identity certificate in this field.</td>
</tr>
<tr>
<td>Facility</td>
<td>Value of a facility. The values can be in the range of local0 and local7.</td>
</tr>
</tbody>
</table>

**Configuring the trace or logging levels**

**About this task**

Use this procedure to configure the trace or logging levels by using the Log Manager for the following services:

- ASAI Link Manager
- CVLAN Service
- DLG Service
- Management Console
- Transport Layer Service
- TSAPI Service
- DMCC Service
The trace level setting might not correspond to any predefined choice on the Log Manager page. If so, the Log Manager page displays the exact string assigned to the service in the `tracemask` file. This entry is read only.

⚠️ Important:

Do not change the trace logging levels without consulting an Avaya engineer. Turning on traces or increasing logging levels might degrade system performance.

### Procedure

1. On the AE Services Management Console main menu, click **Status > Log Manager**.
2. On the Log Manager page, make your changes to the appropriate settings.
3. Click **Apply Changes**.
4. On the Log Manager Confirmation page, click **Apply**.

---

### About log and trace retention

You can set the period for retaining logs and traces from 0 to 180 days. AE Services deletes the retained log and trace files after the retention period is reached. The default retention period is 30 days. Post rotation, AE Services appends the following details to the file name: `<yyyy-mm-dd-timestamp>`. Here, the date is when the rotation took place and timestamp is the time after epoch.

You can retain the following trace files:

- `/var/log/avaya/aes/dmcc-nist.log`
- `/var/log/avaya/aes/dmcc-trace.log`
- `/var/log/avaya/aes/DLG/trace.out`
- `/var/log/avaya/aes/TSAPI/csta-trace`
- `/var/log/avaya/aes/common/trace.out`
- `/var/log/avaya/aes/TSAPI/g3trace.out`
- `/var/log/avaya/aes/ws-telsvc-trace.log`
- `/var/log/avaya/aes/trans-serv/trace.out`
- `/var/log/avaya/aes/asailink/trace.out`
- `/var/log/avaya/aes/CVLAN/trace.out`
- `/var/log/avaya/aes/ossicm.log`

You can retain the following log files:

- All files in `/var/log/sssd` folder
- `/var/log/httpd/error.log`
- `/var/log/avaya/aes/mvap.log`
- `/var/log/messages`
• /var/log/secure
• /var/log/tomcat/catalina.log
• /var/log/httpd/error.log
• /var/log/avaya/aes/oam-admin/audit.log
• /var/log/avaya/aes/oam-admin/login-auth.log
• /var/log/avaya/aes/sec.log
• /var/log/avaya/aes/dmcc-error.log
• /var/log/avaya/aes/ws-telsvc-error.log
• /var/log/avaya/aes/dmcc-jtapi-error.log
• /opt/mvap/lib/mgmt/logs/default.debug.log
• /var/log/avaya/aes/mgmt/logs/default.debug.log
• /var/log/tomcat/mgmt/logs/default.debug.log

alarm.log — You cannot retain this file. AE Services deletes the contents of this file within the day.

importsdb.log — You can retain this file. AE Services deletes the contents of the file post retention period.

📌 Note:
If the log disk is filled to more than 90% occupancy then AE Services deletes the mentioned logs and traces to 75% or below with the older files being deleted first.

Related links
Retaining the log and trace files on page 132
Clearing the log files on page 133
Clearing the trace files on page 134
Retaining logs by using the command line interface on page 134

Retaining the log and trace files

About this task
Use this procedure for log and trace retention by using the Log Manager:

Before you begin
Ensure that you have the datacontroller user role.

Procedure
1. On the AE Services Management Console main menu, click Status > Log Manager > Log and Trace Retention.
2. Enter the required Log and Trace Retention values between 0 to 180 in the corresponding fields.
The default value for which the logs and traces can be retained is 30 days.

3. Click **Set Retention**.
4. On the Log and Trace Retention Confirmation page, click **Apply**.
5. Click **Restore Defaults** for restoring the default values.
6. On the Restore Log and Trace Retention page, click **Restore**.
7. Click **Cancel Changes** to clear all the fields.

### Log and Trace Retention field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Retention</td>
<td>Log Retention period between 0–180 days. The default value is 30 days.</td>
</tr>
<tr>
<td>Trace Retention</td>
<td>Log Retention period between 0–180 days. The default value is 30 days.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Retention</td>
<td>To set the retention period you specified. OAM displays the Log and Trace Retention Confirmation page.</td>
</tr>
<tr>
<td>Restore Defaults</td>
<td>To restore defaults. OAM displays the Restore Log and Trace Retention page.</td>
</tr>
<tr>
<td>Cancel Changes</td>
<td>To cancel the changes.</td>
</tr>
</tbody>
</table>

### Clearing the log files

#### About this task

Use this procedure to clear log files by using the log manager.

**Note:**

When you are using High Availability, OAM can clear logs only from the active server. To clear logs from both the servers, use CLI individually on both servers.

#### Before you begin

Log in to AE Services Management Console using your data controller credentials.

#### Procedure

1. On the AE Services Management Console main menu, click **Status > Log Manager > Clear Logs**.
2. On the Clear Logs page, do one of the following:
   • Enter the number of days in Clear Logs Period field.
   • Click Clear Logs (days) to delete all the logs under retention policy older than the specified number of days.
   • Click Clear All Logs to delete all the logs under retention policy irrespective of the number of days.

3. On the Clear All Logs Confirmation page, click Apply.

---

### Clearing the trace files

**About this task**

Use this procedure to clear the trace files by using the log manager.

⚠️ **Note:**

When you are using High Availability, OAM can clear traces only from the active server. To clear traces from both the servers, use CLI individually on both servers.

**Before you begin**

Log in to AE Services Management Console using your data controller credentials.

**Procedure**

1. On the AE Services Management Console main menu, click Status > Log Manager > Clear Traces.
2. On the Clear Traces page, do one of the following:
   • Enter the number of days in Clear Traces Period field.
   • Click Clear Traces (days) to delete all the logs under retention policy older than the specified number of days.
   • Click Clear All Traces to delete all the logs under retention policy irrespective of the number of days.
3. On the Clear All Traces Confirmation page, click Apply.

---

### Retaining logs by using the command line interface

**Procedure**

1. Log in to the AE Services as a Data Controller user.
2. Use the following command for log retention: `retention -l <0–180>`. Here, 0–180 is the number of days for which you can retain the logs.
3. Use the following command to display the current log retention period: `retention -l`.

Comments on this document? infodev@avaya.com
4. Log out of AE Services.

Retaining traces by using the command line interface

Procedure
1. Log in to the AE Services as a Data Controller user.
2. Use the following command for trace retention: `retention -t <0–180>`.
   Here, 0–180 is the number of days for which you can retain the traces.
3. Use the following command to display the current trace retention period: `retention -t`.
4. Log out of AE Services.

Clearing logs by using the command line interface

Procedure
1. Log in to the AE Services as a Data Controller user.
2. Use the following command to clear the logs before the specified period: `logClear -l <0–180>`.
   The default value for clearing logs is 0. For the default value all logs except the currently written log will be cleared.
3. Log out of AE Services.

Clearing traces by using the command line interface

Procedure
1. Log in to the AE Services as a Data Controller user.
2. Use the following command to clear the traces before the specified period: `logClear -t <0–180>`.
   The default value for clearing traces is 0. For the default value all traces except the currently written trace will be cleared.
3. Log out of AE Services.
Chapter 7: User Administration

About this task

A Linux user or an Enterprise Directory User can access the AE Services Management Console. See Account Management - Linux user accounts on page 166.

To acquire the administrative role for User Management the user must have an administered account in the local LDAP data store with the Avaya role set to userservice.useradmin. (To set up the userservice.user administrative role, see Creating a new User Management administrator account and removing the default avaya account from User Management on page 334).

This chapter describes the capabilities provided by User Management. User Management refers to the local LDAP database on the AE Server. In the context of this chapter, local means located on the AE Services server.

AE Services users are authenticated by AE Services User Management (as opposed to Linux). AE Services users, as such, cannot log in to Linux. and they have limited access privileges in the AE Services Management Console.

Figure 28: AE Services User Management database

User management for authentication

User Management is the default user database that AE Services uses for user authentication (validating a user’s identity). If you use User Management as the user database for user authentication, all AE Services Management Console administrators are authenticated by User Management.
User Management service is the default authentication authority for TSAPI, JTAPI, DMCC, and Telephony Web Services users. You may also use any of the following authentication methods.

- Local Linux accounts
- External Directory service such as Active Directory Services or OpenLDAP
- Active Directory Services Using Kerberos (a specific implementation of an external directory)

For more information about these additional authentication methods, see Additional PAM management capabilities on page 184.

If you use these methods of user authentication, all AE Services Management Console administrators are authenticated by the method you use.

**DMCC AA policy administration and bypassing user authentication**

DMCC AA policy administration allows an administrator to provision security policies that are unique to an individual machine. The machine is identified and authenticated using a certificate. It is possible to specify a security policy that makes it unnecessary to provision a user for the application. This is done by indicating that the machine can bypass user authentication, and by specifying an LDAP or unrestricted access authorization policy.

**User Management for authorization**

In addition to user authentication, the User Management database provides you with the ability to designate a user as a CT User and thereby control their access rights (user authorization). You can use the User Management to authorize users who are authenticated by any of the following methods:

- User Management
- Local Linux accounts
- External Directory service such as Active Directory Services or OpenLDAP
- Active Directory Services using Kerberos (a specific implementation of an external directory)

To use AE Services User Management for authorization, you must follow these basic steps:

- Add each user to User Management (User Management > User Admin > Add User) and set the CT User field to Yes. See Adding a user to User Management on page 139.
- Enable the Security Database (SDB). See APIs that use the Security Database on page 209.
Logging into User Management

About this task
Use this procedure to log in to the AE Servicesserver as the default administrator (cust). You cannot log in to the AE Services management console as a root user.

Procedure
1. On your Web browser, type the fully qualified domain name or IP address of the AE Services server, for example, https://aserver.example.com.
2. On the Application Enablement Services welcome page, click Continue To Login.
3. In the Username field, type the default login ID.
4. Click Continue.
5. In the Password field, enter your password.
   If the Access Security Gateway (ASG) is present, your login ID is challenged by ASG. You must enter a proper response in the Response box to log in to the AE Servicesserver.
6. Click Login
   For more information about the access privileges assigned to administrative users, see AE Services administrative roles and access privileges (role based access control - RBAC) on page 321.

The cust account in User Management

For the Bundled Server and the Software-Only server set up with the Avaya Services Package (cs-service), AE Services installs the cust account in two places: in the local Linux password store and in User Management (local LDAP directory).

To change the password for the cust account in User Management, see Changing the default password for the cust account in User Management on page 333.

Viewing the list of all users in the User Management database

Procedure
From the AE Services Management Console main menu, select User Management > User Admin > List All Users.

Your browser displays the List All Users page, which contains a table displaying the User Id, Common Name, and Surname of each user in the User Management database.
Adding a user to User Management

About this task
Follow this procedure to add a user to the User Management (also referred to as the local LDAP database).

Note:
This example depicts adding a user who will be a member of the TSAPI Service SDB.

Procedure
1. From the AE Services Management Console main menu, select **User Management > User Admin > Add User**.
2. On the Add User page, complete following fields for the user you are adding.
   
   Note:
   The required fields are marked with an asterisk.
   a. In the **User id** field, type the user id you are assigning to the user (for example *jdoe*).
   b. In the **Common Name** field, enter the name the user prefers to use (for example *Jane Doe*).
   c. In the **Surname** field, type the surname (for example *Doe*).
   d. In the **User Password** field, type the password you are assigning to the user.
   e. In the **Confirm Password** field, re-type the assigned password.
   f. In the **CT User** field, do one of the following:
      • Accept the default *(no)* if the user is not a member of the SDB.
      • Select *yes* if the user is a member of the SDB.
   
   For more information about CT Users, see **CT User** in the Glossary.
3. Click **Apply**.
   
   The user you added has read-write access to User Management features in the AE Services Management Console.

Editing a user in User Management

Procedure
1. From the AE Services Management Console main menu, select **User Management > User Admin > List All Users**.
2. From the **List All Users** page, select the user id you want to edit.
3. Click **Edit**.
4. Edit the fields as appropriate.
5. Click **Apply**.
6. From the **Edit User confirmation** page, click **Apply Changes**.

---

### Deleting a user from User Management

**Procedure**

1. From the AE Services Management Console main menu, select **User Management > User Admin > List All Users**.
2. From the **List All Users** page, select the User Id you want to delete.
3. Click **Delete**.
4. From the **Delete User confirmation** page, click **Delete**.

---

### Searching for users in User Management

**Procedure**

1. From the AE Services Management Console main menu, select **User Management > User Admin > Search Users**.
2. On the **Search Users** page, in the **Search Attribute** field, select one of the following:
   - User ID
   - Surname
   - Common Name
3. In the **Search value** field, type the search value, as follows:
   - If you selected User ID, type a user ID (for example `jdoe`).
   - If you selected Surname, type the user’s last name (for example `doe`).
   - If you selected Common Name, type the user’s first name and last name (for example `Jane Doe`).

Your browser displays the Search Results page. If your search yields a match (or a list of matches), your browser displays the User ID, Common Name, and Surname of the user(s).
Search tips

Here are a few basic search tips.

- AE Services Management Console searches are not case sensitive. For example, you can use all lower case characters on a surname, such as doe, and get a successful result for Doe.
- Use the asterisk (or “wildcard”) when you know only part of the first or last name or User ID Usually, wildcard searches result in multiple names.

---

Modifying the default user - sample

About this task

The Modify Default User feature is closely tied to the Add User Web feature. When you have large groups of people who share common attributes, you can use the Modify Default User feature to simplify the process of adding users. Keep in mind, however, that if you do plan to use Modify Default User feature in this way, you must manage the process carefully.

Here is a simple example that demonstrates how the Modify Default User feature can be used to administer 60 users for two different departments, sales and support. Each department consists of 30 people.

Procedure

1. From the AE Services Management Console main menu, select User Management > User Admin > Modify Default User.
3. In the Department Number field, type 30756032100 (the department number for sales), and click Apply.
4. From the User Management menu select Add User.
5. On the Add User page, for each user in the sales department you would need to enter specific information for the required fields (User ID, Common Name, Surname, User Password, and Confirm Password), but the following fields, which you administered on the Modify Default User page, would already be complete.
   - Business Category Sales
   - Department Number 30756032100
6. Once you have completed the Add User page for each of the 30 users in the Sales group, select Modify Default User.
8. In the Department Number field, type 30747912100 (the department number for Support), and click Apply.
9. From the User Management menu select Add User.
10. On the **Add User** page, for each user in the Support department, you would need to enter specific information for the required fields (User ID, Common Name, Surname, User Password, and Confirm Password), but the following fields, which you administered on the Modify Default User page, would already be complete.

   - Business Category **Support**
   - Department Number 30747912100

11. Once you have completed the **Add User** page for all 30 users in the Support group, select **Modify Default User**.

12. On the **Modify Default User** page, clear the **Business Category** and **Department Number** fields, and click **Apply**.

**Important:**

When you use the **Modify Default User** page to administer groups of users with common settings, be sure to clear the settings once you have completed the process of administering all groups.

---

### Changing user passwords

**About this task**

Follow this procedure to change your User Management password.

**Procedure**

1. From the AE Services Management Console main menu, select **User Management > User Admin > Change User Password**.

2. On the **Change User Password** page, in the **User Id** field, type the user Id of the user you want to modify.

3. In the **New Password** field, type a new password.

   The default User Management password policy, which is based on a US standard keyboard, calls for a minimum of 8 characters, including a minimum of 1 upper-case, 1 lower-case, 1 alphanumeric, and 1 special character. The following characters are not permitted: $ (dollar sign), ' (apostrophe), " (quotation mark), \ (backslash), the space character, and any ASCII control-character.

4. In the **Confirm New Password** field, re-type the new password.

5. Click **Apply**.
Service Administration configuration files

Service Administration provides configuration files that enable you to control the local LDAP database. All configuration files contain parameters that are expressed as name-value pairs in the following format: `name=value`. For example, `cn=common name`.

⚠️ Caution:

Unless you are an advanced administrator, do not change any settings in these files.

attributesmap.properties

This file is used to map raw (LDAP oriented) user attribute names to friendly display names. For example, the file maps the attribute named “uid” to “User ID”.

There is no need to re-initialize the User Management if this file is edited.

attributeacl.properties

This file allows fine tuning of the attribute level Access Control List (ACL) enforced by User Management. This file is generally only altered for customization purposes.

For changes to this file to take effect, the User Management must be re-initialized. See Re-initializing service configuration files on page 145.

sdbdistributor.properties

This file is the configuration file for the SDB Distributor. This Distributor supports synchronization of the User Management with the Security Database.

For changes to this file to take effect, the User Management must be re-initialized. See Re-initializing service configuration files on page 145.

genericldap1.properties, genericldap2.properties, replicator1.properties

These three files are for reference only. The genericldap property files demonstrate two examples of configuring an LDAP distributor and serve as models for setting up an LDAP Distributor, post-installation.

Changes to these files are unnecessary unless a like named Distributor is configured to run in the user.properties file (distributors section).
When a corresponding Distributor is being run, and changes are made to its property file, the changes will not take effect until the User Management is re-initialized. See Re-initializing service configuration files on page 145.

Note:
The replicator1.properties file is a place holder for a replication Distributor that is not available in the current release of the User Management.

rbac.properties
This file maps User Management operation names to a list of roles that give access to the specified operation. It would be very unusual to reconfigure this file post-installation.

For changes to this file to take effect, the User Management must be re-initialized. See Re-initializing service configuration files on page 145.

ldapfilter.properties
This file configures the LDAP Authentication filter. When the User Management receives an operation request, the service validates the callers credentials against the LDAP service indicated in this file. The settings in this file should reflect the mode of authentication that the User Management is running in (see user.properties security section). For example, if the User Management is running with remote authentication, the ldapfilter.properties should be set to the same remote LDAP service. If the User Management is running with basic (local) authentication, then the properties should specify the User Management's underlying LDAP service.

For changes to this file to take effect, the User Management must be re-initialized. See Re-initializing service configuration files on page 145.

log4j.properties
This file is used to configure logging for the User Service using log4j.

remoteldapauthenticator.properties
If the User Management is running with remote authentication then this file specifies the location of the remote LDAP service. If this file is in use, the settings will normally match those of the ldapfilter.properties file.

For changes to this file to take effect, the User Management must be re-initialized. See Re-initializing service configuration files on page 145.
user.properties

This is the main configuration file for the User Management service. It controls:

- Primary LDAP interface settings
- Distributor settings
- Logging settings
- Supported attributes and their types
- The definition of "protected" users (from deletion during synchronizations)
- Security
- Advertising of internal user roles (for the AE Services Management Console)

For changes to this file to take effect, the User Management must be re-initialized. See Re-initializing service configuration files on page 145.

ws_cus_bootstrap.properties

This file contains the essential bootstrap parameters for the service, and is not normally altered post-installation. If the file is altered, it must be manually copied to the <TOMCAT_HOME>/webapps/axis/WEB-INF folder. Then, for changes to this file to take effect, the User Management must be re-initialized. See Re-initializing service configuration files on page 145.

Re-initializing service configuration files

About this task

After you edit the service configuration files, you need to reinitialize them to put your changes into effect. Re-initializing the service is a non-blocking feature. AE Services continues to operate when you use this feature.

Procedure

1. From the AE Services Management Console main menu, select User Management > Service Admin > Re-initialize Services.
2. On the Reinitialize Service page, click Reinitialize to re-initialize service configuration files.
Editing the default user values file

About this task

The default user values properties file defaultuservalues.properties determines which values appear as the default values on the Add User page in User Management. For more information on user management, see Adding a user to User Management on page 139.

All parameters in the defaultuservalues.properties file are expressed as name-value pairs in the following format: name=value, for example cn=common name.

Procedure

1. From the AE Services Management Console main menu, select User Management > Service Admin > Edit Services.
2. Select defaultuservalues.properties from the list of property files, and click Edit.
3. On the Edit Service Configuration page, add preferredlanguage=English as a user attribute, and click Apply.

   A message appears stating that if you edited service configuration, you may have to initialize the service for changes to be effective.

   ✨ Note:

   After you edit a service configuration file, you do not have to reinitialize the service.

4. To verify the default value for the preferred language is English, from the AE Services Management Console main menu, select User Management > User Admin > Add User.

   Your browser displays the Add User page which displays English in the preferredlanguage field.

5. To change the preferred language value (from English to Spanish, for example), from the AE Services Management Console main menu, select User Management > User Admin > Modify Default User.

6. From the Modify Default User page, change the value for the preferred language to Spanish.

7. Select User Management > Service Admin > Reinitialize Service.

8. Repeat Step 4 to verify the preferred language has change to Spanish.

Guidelines for synchronizing distributors

Distributors are components of User Management that propagate changes, such as additions, changes, or deletions, from an application to the AE Services User Service database. AE Services provides two distributors, the SDB distributor and the Generic LDAP distributor.

The Synchronize feature is used to trigger a synchronization of user data between the User Service database (LDAP based) and an application user space (for example, the TSAPI SDB)
through a Distributor connection. The Synchronize feature on the **Distributor List** page allows you to trigger an on-demand synchronization.

Following are a few situations that require an on-demand synchronization:

- Recovery of AE Services after a User Management failure or a maintenance shutdown. For information about shutting down services, see [Service Controller (start stop and restart services)] on page 124.
- Recovery of AE Services after a client application failure or a maintenance shutdown
- After adding a new client application that relies on the User Management capabilities

---

### Configuration using CLI

The following APIs allow you to configure AE Services by using the CLI. By using these APIs, you can configure AE Services without accessing the AE Services management console.

#### Common return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>&lt;No message&gt; Success.</td>
</tr>
<tr>
<td>1</td>
<td>The api has not been used correctly. Please check respective documentation for more details.</td>
</tr>
<tr>
<td>2</td>
<td>Restart aesvcs service manually using &quot;/usr/bin/systemctl restart aesvcs.service&quot; for changes to take effect.</td>
</tr>
<tr>
<td>3</td>
<td>The database query failed to execute.</td>
</tr>
</tbody>
</table>

**Note:**

All the utilities when run with -h or - -help option will display the usage of the respective utility. All the utilities must run using “root” user.

---

#### setWeblm

Allows you to set the IP address of the WebLM server.

**Syntax**

setWeblm -pri IPaddress:port -pssl [true|false] -sec IPaddress:port -sssl [true|false]

where:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-pri IPaddress:port</td>
<td>IP address of the primary WebLM server along with the port number.</td>
</tr>
</tbody>
</table>

[Table continues...]
### Argument Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-sec IPaddress:port</td>
<td>IP address of the secondary WebLM server along with the port number.</td>
</tr>
<tr>
<td>-pssl</td>
<td>The Secure Socket Layer connection to a primary WebLM server. By default this value is true.</td>
</tr>
<tr>
<td>-sssl</td>
<td>The Secure Socket Layer connection to a secondary WebLM server. By default this value is true.</td>
</tr>
</tbody>
</table>

### Return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Configuring of WebLM servers for GRHA failed.</td>
</tr>
<tr>
<td>6</td>
<td>The WebLM IP address is invalid.</td>
</tr>
<tr>
<td>7</td>
<td>Cannot use the non-secure WebLM Ports 80 or 8080 as WebLM Port, when SSL is true.</td>
</tr>
<tr>
<td>8</td>
<td>Cannot use the secure WebLM Ports 443 or 8443 as WebLM Port, when SSL is false.</td>
</tr>
<tr>
<td>9</td>
<td>The WebLM Port must be numeric.</td>
</tr>
<tr>
<td>10</td>
<td>The WebLM Port must be a valid port value in the range of 1024 to 65535 or 443 and 80.</td>
</tr>
</tbody>
</table>

---

### reservedLicenses

Allows you to configure and display the number of reserved licenses on AE Services for TSAPI basic user licenses, unified desktop licenses, and DMCC licenses.

**Syntax**

reservedLicenses reserve [ tsapi | desktop | dmcc ] [ number of licenses ]

reservedLicenses status [ tsapi | desktop | dmcc ]

For example, reservedLicenses reserve tsapi 500

where:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reserve</td>
<td>Reserves the required number of licenses.</td>
</tr>
<tr>
<td>status</td>
<td>Displays the current reserved licenses.</td>
</tr>
<tr>
<td>tsapi</td>
<td>This option corresponds to 'Reserved Tsapi Basic User Licenses' range of licenses that can be reserved: 1 - 25000.</td>
</tr>
<tr>
<td>desktop</td>
<td>This option corresponds to 'ReservedUnifiedDesktopLicenses' range of licenses that can be reserved: 1 – 25000.</td>
</tr>
<tr>
<td>dmcc</td>
<td>This option corresponds to 'Reserved DMCC Licenses' range of licenses that can be reserved: 1 – 1000.</td>
</tr>
</tbody>
</table>
Return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Invalid number of licenses entered.</td>
</tr>
</tbody>
</table>

importSDB

Allows you to import or upload an SDB backup file to AE Services server.

Syntax

importSDB [path_to_file]

For example, importSDB /tmp/backupsdb.txt

where:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>path_to_file</td>
<td>This is the path of the SDB backup file in txt format.</td>
</tr>
</tbody>
</table>

Return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>The file to import does not exist.</td>
</tr>
<tr>
<td>5</td>
<td>The file to import is not in correct format.</td>
</tr>
<tr>
<td>6</td>
<td>The file to import is too large. Cannot import.</td>
</tr>
<tr>
<td>7</td>
<td>There was an error in creating the temporary tar file.</td>
</tr>
<tr>
<td>8</td>
<td>Error in converting the tar file to DOS format.</td>
</tr>
<tr>
<td>9</td>
<td>Error importing SDB file. Check /var/log/avaya/aes/importsdb.log for more details.</td>
</tr>
</tbody>
</table>

setSDB

This will enable and disable Security Database for DMCC service, TSAPI service, JTAPI service and TWS.

Syntax

setSDB [ enable | disable ] [ dmcc | tsapi ]

For example, setSDB enable dmcc

where:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the SDB access for the respective services.</td>
</tr>
</tbody>
</table>
### hostAA

Allows you to set the service settings under HostAA properties.

**Syntax**

```
hostAA set [service name] [client authentication] [trusted host entry]
```

For example, `hostAA set dmcc true true`

where:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>Sets the authentication settings for respective services.</td>
</tr>
<tr>
<td>service name</td>
<td>This can be dmcc, tsapi, cvlan, or tr87.</td>
</tr>
<tr>
<td>client authentication</td>
<td>This is ‘true’ or ‘false’ for authenticating client with trusted CA certificate for respective servicename.</td>
</tr>
<tr>
<td>trusted host entry</td>
<td>This is ‘true’ or ‘false’ for enabling or disabling the “Require Trusted Host Entry” which checks the CN in the client certificate and verifies that it matches one of the administered authorized hosts.</td>
</tr>
</tbody>
</table>

**Return codes:**

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>The DMCC client authentication must be true if DMCC host authorization is true.</td>
</tr>
<tr>
<td>6</td>
<td>The TR87 client authentication cannot be set to false.</td>
</tr>
</tbody>
</table>

### trustedHosts

This will add a host as a trusted, authorized host under the HostAA configuration.

**Syntax**

```
trustedHosts add [certificateCN] [service type] [authentication policy] [authorization policy]
trustedHosts del [certificateCN] [service type]
trustedHosts edit [old certificateCN] [old service type] -n [new certificateCN] -s [new service type] -an [new authentication policy] -auth [new authorization policy]
```
For example, `trustedHosts add aesclient dmcc yes sdb` where:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Add the trusted host entry.</td>
</tr>
<tr>
<td>del</td>
<td>Delete the trusted host entry.</td>
</tr>
<tr>
<td>edit</td>
<td>Edit the trusted host entry.</td>
</tr>
<tr>
<td>certificateCN</td>
<td>The name that appears in the Subject Name or Common Name (CN) field of the client cert.</td>
</tr>
<tr>
<td>service type</td>
<td>'all', 'dmcc' or 'tr87'.</td>
</tr>
<tr>
<td>authentication policy</td>
<td>yes' or 'no' to apply authentication policy for the service.</td>
</tr>
</tbody>
</table>

Return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>The User Authentication Policy cannot be set to Required when the service type is TR/87.</td>
</tr>
<tr>
<td>5</td>
<td>Could not delete host. Possible reasons: The given combination of host and service type does not exist or the host was already deleted.</td>
</tr>
<tr>
<td>6</td>
<td>Possible duplication, CN already exists. Cannot add same CN for service type ALL.</td>
</tr>
<tr>
<td>7</td>
<td>Could not delete host. Possible reason: The host was already deleted. Not an error condition.</td>
</tr>
<tr>
<td>8</td>
<td>The specified host and/or service does not exist.</td>
</tr>
</tbody>
</table>

---

**trustCACertMgmt**

This API is used to manage trusted certificates.

**Syntax**

```
trustCACertMgmt list
trustCACertMgmt view [alias]
trustCACertMgmt import [alias] [uploadedfilename/path]
trustCACertMgmt export [alias]
trustCACertMgmt delete [alias]
```

For example, `trustCACertMgmt import DMCC /tmp/dmcc.txt` where:
<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>Lists all trusted CA certificates present on the server.</td>
</tr>
<tr>
<td>view</td>
<td>View details of mentioned trusted CA Certificate.</td>
</tr>
<tr>
<td>import</td>
<td>Imports the mentioned trusted CA Certificate.</td>
</tr>
<tr>
<td>export</td>
<td>Exports or displays pem text of mentioned trusted CA Certificate. It can be redirected to a file in</td>
</tr>
<tr>
<td></td>
<td>order to save it and can be used to import this certificate whenever and wherever required.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes the mentioned trusted CA Certificate.</td>
</tr>
<tr>
<td>alias</td>
<td>Suitable name for a trusted CA Certificate given by user.</td>
</tr>
<tr>
<td>uploadedfilename/path</td>
<td>File name or absolute path of the certificate user going to import.</td>
</tr>
</tbody>
</table>

Return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>No certificate with this name is present.</td>
</tr>
<tr>
<td>5</td>
<td>Error reading trusted certificate repository to list certificates.</td>
</tr>
<tr>
<td>6</td>
<td>Certificate with alias does not exist.</td>
</tr>
<tr>
<td>7</td>
<td>Alias name format error. Allowed values: Alphanumeric chars, underscore (_), and hyphen (-).</td>
</tr>
<tr>
<td></td>
<td>Max 31 chars.</td>
</tr>
<tr>
<td>8</td>
<td>The import file must be a PEM file.</td>
</tr>
<tr>
<td>9</td>
<td>The imported file does not exist.</td>
</tr>
<tr>
<td>10</td>
<td>Verification for the imported file failed.</td>
</tr>
<tr>
<td>11</td>
<td>Alias already exists.</td>
</tr>
<tr>
<td>12</td>
<td>Certificate already exists.</td>
</tr>
<tr>
<td>13</td>
<td>Switch to root user to execute the script</td>
</tr>
<tr>
<td>14</td>
<td>Deletion of default certificate is denied.</td>
</tr>
<tr>
<td>15</td>
<td>Keystore is not present.</td>
</tr>
</tbody>
</table>

**serverCertificates**

This API is used to manage server certificates.

**Syntax**

```
serverCertificates list
serverCertificates view [alias]
serverCertificates import [alias] [uploadedfilename/path]
[isChainOfTrust] [password]
serverCertificates delete [alias]
```

For example, `serverCertificates import DMCC /tmp/dmcc.txt true ahvc1234`
where:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>Lists server certificates present on the server.</td>
</tr>
<tr>
<td>view</td>
<td>View details of mentioned server certificate.</td>
</tr>
<tr>
<td>import</td>
<td>Imports mentioned server Certificate.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes mentioned server certificate.</td>
</tr>
<tr>
<td>alias</td>
<td>Suitable name for a server certificate given by user.</td>
</tr>
<tr>
<td>uploadedfilename/path</td>
<td>File name or absolute path of the certificate user going to import.</td>
</tr>
<tr>
<td>isChainOfTrust</td>
<td>Allowed values are true or false.</td>
</tr>
<tr>
<td>password</td>
<td>Password is optional depending on the type of certificate.</td>
</tr>
</tbody>
</table>

Return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Switch to root user to execute the script.</td>
</tr>
<tr>
<td>5</td>
<td>Error reading server certificate repository to list certificates.</td>
</tr>
<tr>
<td>6</td>
<td>Certificate does not exist.</td>
</tr>
<tr>
<td>7</td>
<td>Import failed. Certificate request not found.</td>
</tr>
<tr>
<td>8</td>
<td>Alias name should be one of aeservices,server,rsyslog,ldap,cmtls,web.</td>
</tr>
<tr>
<td>9</td>
<td>Certificate directory does not exist.</td>
</tr>
<tr>
<td>10</td>
<td>Certificate with this alias already exists.</td>
</tr>
<tr>
<td>11</td>
<td>Import file must be PEM or pfx file.</td>
</tr>
<tr>
<td>12</td>
<td>Establish chain of trust is required for importing pkcs12 file.</td>
</tr>
<tr>
<td>13</td>
<td>Certificate file is empty or unavailable.</td>
</tr>
<tr>
<td>14</td>
<td>Error importing certificate.</td>
</tr>
<tr>
<td>15</td>
<td>Error extracting PEM file.</td>
</tr>
<tr>
<td>16</td>
<td>Wrong Password entered.</td>
</tr>
<tr>
<td>17</td>
<td>Exception in deleting certificate request while overriding.</td>
</tr>
<tr>
<td>18</td>
<td>Certificate deletion failed.</td>
</tr>
</tbody>
</table>

---

**tsapiCti**

This API is used to query and edit information for cti link information for tsapi

**Syntax**

```bash
    tsapiCti add [switchname] [ctilink] [security] [linkversion]
    tsapiCti status [switchname]
    tsapiCti remove [switchname]
```

Following are the examples:

- tsapiCti add switchCM 4 both 9
- tsapiCti edit switchCM -s unencrypted

where:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Adds ctilink with given switch name.</td>
</tr>
<tr>
<td>status</td>
<td>Gets the status of the link.</td>
</tr>
<tr>
<td>remove</td>
<td>Removes the ctilink.</td>
</tr>
<tr>
<td>edit</td>
<td>Edit the information of link.</td>
</tr>
<tr>
<td>linkversion</td>
<td>Values range from 1 to 9 for Release 8.0.1 and 1 to 10 for Release 8.1.x.</td>
</tr>
<tr>
<td>ctilink</td>
<td>Values range from 1 to 64.</td>
</tr>
<tr>
<td>security</td>
<td>Can have the following values: encrypted, unencrypted, both.</td>
</tr>
</tbody>
</table>

Return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Switch does not exist in switch connections.</td>
</tr>
<tr>
<td>5</td>
<td>Invalid CTI link number.</td>
</tr>
<tr>
<td>6</td>
<td>Invalid Security mode/Encryption state.</td>
</tr>
<tr>
<td>7</td>
<td>TSAPI link already exists.</td>
</tr>
<tr>
<td>8</td>
<td>TSAPI link does not exist.</td>
</tr>
</tbody>
</table>

**switchConnection**

This API is used to add or edit Switch connections with Communication Manager.

*Syntax*

switchConnection add [switchName] [switchPassword] [msgPeriod] [isPe] [h323tls] [aesCert]

switchConnection update [switchName] -pw switchPassword -pe isPe -h h323tls -c aesCert

switchConnection editPECIan [switchName] [ip]

switchConnection editH323 [switchName] [ip]

switchConnection deleteConnection [switchName]

switchConnection deletePECIan [switchName] [ip]

switchConnection deleteH323 [ip]
Following are the examples:

- switchConnection add switchCM avaya12345avaya 30 true false false
- switchConnection deletePEClan switchCM 10.133.68.56

where:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Adds switch with corresponding switchname and other parameters.</td>
</tr>
<tr>
<td>update</td>
<td>Updates the parameters related to a particular switch.</td>
</tr>
<tr>
<td>editPEClan</td>
<td>Adds PE/CLAN IP for corresponding switch.</td>
</tr>
<tr>
<td>editH323</td>
<td>Adds H323 IP for switch.</td>
</tr>
<tr>
<td>deleteConnection</td>
<td>Deletes switch for given switch name.</td>
</tr>
<tr>
<td>deletePEClan</td>
<td>Deletes associated PE/CLAN IP.</td>
</tr>
<tr>
<td>deleteH323</td>
<td>Deletes associated H323 IP.</td>
</tr>
<tr>
<td>msgPeriod</td>
<td>Can have values from 1 to 72.</td>
</tr>
<tr>
<td>isPe, h323tls, aesCert</td>
<td>Can have the following values: true or false.</td>
</tr>
</tbody>
</table>

Return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Invalid msgPeriod.</td>
</tr>
<tr>
<td>5</td>
<td>Switch does not exist.</td>
</tr>
<tr>
<td>6</td>
<td>Max number of CLANs connections reached.</td>
</tr>
<tr>
<td>7</td>
<td>Cannot delete if there are active CLANs for the switch connection.</td>
</tr>
<tr>
<td>8</td>
<td>Cannot delete if there are links administered for the Switch Connection.</td>
</tr>
<tr>
<td></td>
<td>Remove the CLANs first.</td>
</tr>
<tr>
<td>9</td>
<td>Cannot delete if CLAN is active.</td>
</tr>
<tr>
<td>10</td>
<td>H323 Gatekeeper does not exist.</td>
</tr>
<tr>
<td>11</td>
<td>Switch already exist.</td>
</tr>
<tr>
<td>12</td>
<td>Maximum number of Switch Connections reached.</td>
</tr>
<tr>
<td>13</td>
<td>Invalid switch name.</td>
</tr>
<tr>
<td>14</td>
<td>Invalid password.</td>
</tr>
</tbody>
</table>

---

**stdResPorts**

This API is used to enable or disable the standard ports.

**Syntax**

stdResPorts -nm [service name] [enable|disable]

stdResPorts -no [port no] [enable|disable]
For example, stdResPorts -no 80 enable

where:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-nm [service name]</td>
<td>Accepts the name of service. It is case sensitive. All the values must be in lower case.</td>
</tr>
<tr>
<td>-no [port no]</td>
<td>Accepts the port number of service. If port number entered is 514, then the last argument should be [shell/syslog].</td>
</tr>
</tbody>
</table>

Return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Action is invalid. It should either be enable or disable.</td>
</tr>
<tr>
<td>5</td>
<td>Invalid service name.</td>
</tr>
<tr>
<td>6</td>
<td>Invalid port number.</td>
</tr>
</tbody>
</table>

enterpriseDirectory

This API is used to edit enterprise directory or view it.

Syntax to edit:

```
enterpriseDirectory baseDN hostFQDN primaryPort [options]
```

[options] are as follows:

- -udn (User DN for query authentication)
- -pw (Password)
- -sechost (Secondary hostname)
- -secport (Secondary port)
- -uid (User ID attribute name)
- -urole (User role attribute name)
- -cpwd (Change passowrd URL)
- -devid (Device ID attribute)
- -filter (Search filter attribute)

Syntax to view:

```
enterpriseDirectory view
```

For example, enterpriseDirectory cn=Users,dc=aes,dc=rnd,dc=avaya,dc=com lcs-dcl.aes.rnd.avaya.com 389

where:

The edit command will edit the enterprise directory.

The view command will display all the fields of enterprise directory.
Return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Could not change enterprise directory.</td>
</tr>
<tr>
<td>5</td>
<td>User DN for query authentication invalid</td>
</tr>
<tr>
<td>6</td>
<td>Base Search DN invalid</td>
</tr>
<tr>
<td>7</td>
<td>Primary/Secondary host should be in the form of FQDN.</td>
</tr>
<tr>
<td>8</td>
<td>Port value should be 389, 636, or within 1024 to 65535</td>
</tr>
<tr>
<td>9</td>
<td>User ID attribute name required except for TR/87 usage.</td>
</tr>
<tr>
<td>10</td>
<td>Password cannot contain backslash ()</td>
</tr>
<tr>
<td>11</td>
<td>Unable to locate Server Certificate.</td>
</tr>
<tr>
<td>12</td>
<td>Could not retrieve Enterprise directory Information.</td>
</tr>
</tbody>
</table>

**networkingPorts**

This API is used to set the range for AES networking ports, and enable or disable them.

**Syntax**

```bash
networkingPorts cvlan -uact [action] -eact [action] -e [portno]*
networkingPorts tsapi -spact [action] -umin [portno]* -umax [portno]* -emin [portno]* -emax [portno]*
networkingPorts sms -min [portno] -max [portno]
```

For example, `networkingPorts cvlan -eact enabled -e 9990`

where:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Sub-argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>-</td>
<td>Allowed values are enabled or disabled.</td>
</tr>
<tr>
<td>portno</td>
<td>-</td>
<td>Can have values between 1024 and 65535.</td>
</tr>
<tr>
<td>(*)</td>
<td>-</td>
<td>Indicates that the editing of port value is permitted only if action before it is “enabled”.</td>
</tr>
<tr>
<td>cvlan</td>
<td>-uact</td>
<td>Unencrypted port action.</td>
</tr>
<tr>
<td></td>
<td>-eact</td>
<td>Encrypted port action.</td>
</tr>
<tr>
<td></td>
<td>-e</td>
<td>Encrypted port number.</td>
</tr>
<tr>
<td>tsapi</td>
<td>-spact</td>
<td>TSAPI service port action.</td>
</tr>
</tbody>
</table>

Table continues…
Argument | Sub-argument | Description
--- | --- | ---
-umin |  | Unencrypted TLINK port no. minimum value.
-umax |  | Unencrypted TLINK port no. maximum value.
-emin |  | Encrypted TLINK port no. minimum value.
-emax |  | Encrypted TLINK port no. maximum value.
dmcc | -uact | Unencrypted port action.
-u |  | Unencrypted port number.
-eact |  | Encrypted port action.
e |  | Encrypted port number.
tact |  | Tr87 port action.
-tr87 |  | Tr87 port number.
h323 | -tmin | TCP minimum port number.
lumin |  | TCP maximum port number.
lumax |  | Local UDP minimum port number.
-smact |  | Local UDP maximum port number.
-rlumin |  | RTP local UDP minimum port number.
-rlumax |  | RTP local UDP maximum port number.
sms | -max | Minimum proxy port number.
-min |  | Maximum proxy port number.

Return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Port number or port range value should be between 1024 and 65535.</td>
</tr>
<tr>
<td>5</td>
<td>The action value is invalid. It should be enabled or disabled.</td>
</tr>
<tr>
<td>6</td>
<td>To change port value the respective action should be enabled.</td>
</tr>
</tbody>
</table>
| 7 | Exception occurred while trying to save SMS proxy ports to the configuration file. Either the file could not be found or you do not have write permissions. SMS changes have not been saved. For return code 7, all other values except SMS are saved successfully. For debugging purposes, please check and confirm for the below value. 

```
ll /etc/sms.ini
lrwxrwxrwx 1 root root 25 Mar 13 12:00 /etc/sms.ini -> /opt/mvap/web/sms/saw.ini
```

----------

**ctiUser**

This API will create, view, or edit ctiUsers.

**Syntax**

ctiUser add [userid] [common-name] [surname] [password] [isCtiUser] -ar [avayaRole]
ctiUser delete [userid]
ctiUser view [userid]
ctiUser unrestricted [userid] [true|false]

For example, ctiUser modify user01 -n aesuser -s aes -c no

where:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>isCtiUser</td>
<td>Can have yes or no values.</td>
</tr>
<tr>
<td>avayaRole</td>
<td>Can have userservice, useradmin, or None values.</td>
</tr>
<tr>
<td>add</td>
<td>Adds user with given parameters.</td>
</tr>
<tr>
<td>modify</td>
<td>Modify the user with given userid.</td>
</tr>
<tr>
<td>delete</td>
<td>Delete the user with given userid.</td>
</tr>
<tr>
<td>view</td>
<td>Views information of the user with given userid.</td>
</tr>
<tr>
<td>unrestricted</td>
<td>Grants and rejects unrestricted access to a user, if it is a ctiUser</td>
</tr>
</tbody>
</table>

While viewing CTI user, if userid is not provided, list of all users are displayed.
The unrestricted option will enable or disable unrestricted SDB access for a given CTI user.

Return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Avaya Role is invalid.</td>
</tr>
<tr>
<td>5</td>
<td>Value of isCtiUser should be yes or no.</td>
</tr>
<tr>
<td>6</td>
<td>uid, cn or sn can contain [A-Z,a-z,0-9,_,.] and could be less than 32 characters.</td>
</tr>
<tr>
<td>7</td>
<td>Password should have at least one uppercase, one lowercase, one digit and one special character with minimum length of 8 characters.</td>
</tr>
<tr>
<td>8</td>
<td>User with this uid already exist.</td>
</tr>
<tr>
<td>9</td>
<td>User could not be &lt;action&gt; due to unknown reason.</td>
</tr>
<tr>
<td>10</td>
<td>The user with given uid does not exist.</td>
</tr>
<tr>
<td>11</td>
<td>The user is not a CTI user. Cannot modify unrestricted access.</td>
</tr>
</tbody>
</table>

**snmpAgent**

This API is used to view Product ID and configure snmp agent.

**Syntax**
snmpAgent view-product-id


Examples are as follows:

snmpAgent view-product-id

snmpAgent add -syslocation pune -contact 1234 -v1 true -communityname1 agent1 -v2c true -communityname2 agent1v2 -v3 true -username agent1v3 -authProtocol MD5 -authPassword abcd12345 -privacyProtocol AES -privacyPassword abcd1234 -ipaccess specificAccess -multipleIPaddr "1.0.0.1 1.2.3.4 1.0.9.6"

where:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>view-product-id</td>
<td>Displays the product ID.</td>
</tr>
<tr>
<td>add</td>
<td>Adds or updates an SNMP agent.</td>
</tr>
<tr>
<td>authProtocol</td>
<td>Allowed values are: None, MD5, and SHA.</td>
</tr>
<tr>
<td>authPassword</td>
<td>Password length need to be between 8-12 characters.</td>
</tr>
<tr>
<td>privacyProtocol</td>
<td>Allowed values – None, AES, and DES.</td>
</tr>
<tr>
<td>privacyPassword</td>
<td>Password length to be exactly 8 characters.</td>
</tr>
<tr>
<td>ipaccess</td>
<td>Allowed values – noAccess, specificAccess, and allAccess.</td>
</tr>
<tr>
<td>multipleIPaddr</td>
<td>Maximum of 5 IPs are allowed. If more then 1 ip is entered, make sure to enter in “x.x.x.x y.y.y.y”(within double quotes separated by space).</td>
</tr>
</tbody>
</table>

Return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>v1 , v2c, or v3 can either be true or false.</td>
</tr>
<tr>
<td>5</td>
<td>Community name or user name can not be left empty, if v1 ,v2c v3 is selected.</td>
</tr>
<tr>
<td>6</td>
<td>Password is required if protocol is not none.</td>
</tr>
<tr>
<td>7</td>
<td>Syslocation/contact/communityname1/communityname2c/username/ipadress format error. Allowed values: Alphanumeric chars, underscore (_), space, dot, coma, and hiphen (-). Maximum 255 characters are allowed.</td>
</tr>
<tr>
<td>8</td>
<td>Auth protocol can only be either 'None', 'MD5', 'SHA'.</td>
</tr>
<tr>
<td>9</td>
<td>Auth password length 8-12 characters and alphanumeric.</td>
</tr>
<tr>
<td>10</td>
<td>Privacy protocol can only be either 'None', 'DES', 'AES'.</td>
</tr>
<tr>
<td>11</td>
<td>Privacy password length exactly 8 characters and alphanumeric.</td>
</tr>
</tbody>
</table>

Table continues...
### snmpTrapReceiver

This API is used to configure SNMP Trap Receivers.

**Syntax**

```
snmpTrapReceiver list
snmpTrapReceiver add -enabled [true|false] -port [port number] -
    snmpversion [2c|3] -securityname [name] -authProtocol [None|MD5|SHA] -
    authPassword [password] -privacyProtocol [None|DES|AES] -privacyPassword
    [password] -ipaddr [ipaddress]
snmpTrapReceiver modify -id [id retrieved using list function] -enabled
    [true|false] -port [port no.] -snmpversion [2c|3] -securityname [name] -
    [None|DES|AES] -privacyPassword [password] -ipaddr [ipaddress]
snmpTrapReceiver delete -id [id retrieved using list function]
```

For example, `snmpTrapReceiver add -enabled true -port 162 -snmpversion 3 -
    securityname snmpTrap1 -authProtocol SHA -authPassword abcd1234 -
    privacyProtocol AES -privacyPassword abcd1234 -ipaddr 127.0.0.1`

where:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>Lists all the configured snmp trap receivers.</td>
</tr>
<tr>
<td>add</td>
<td>Adds a new snmp trap receiver.</td>
</tr>
<tr>
<td>modify</td>
<td>Modifies an already configured snmp trap receiver.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a snmp trap receiver.</td>
</tr>
</tbody>
</table>
| generate-agent-
    authfail-traps     | Generates agent authentication failure trap.     |
Return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>SNMP version can either be 2c or 3.</td>
</tr>
<tr>
<td>5</td>
<td>Version 2c is selected. Authorization protocol or privacy protocol are not applicable.</td>
</tr>
<tr>
<td>6</td>
<td>Password is required if protocol is not none.</td>
</tr>
<tr>
<td>7</td>
<td>&lt;Parameter name&gt; invalid value.</td>
</tr>
<tr>
<td>8</td>
<td>Auth protocol can only be either 'None', 'MD5', or 'SHA'.</td>
</tr>
<tr>
<td>9</td>
<td>Password length cant be less than 6 characters.</td>
</tr>
<tr>
<td>10</td>
<td>Privacy protocol can only be either 'None', 'DES' 'AES'.</td>
</tr>
<tr>
<td>11</td>
<td>Authorization protocol and password are required.</td>
</tr>
<tr>
<td>12</td>
<td>Switch to root user to execute the scrip.</td>
</tr>
<tr>
<td>13</td>
<td>Failed to restart service &lt;service name&gt;.</td>
</tr>
<tr>
<td>14</td>
<td>&lt;Script name&gt; script failed.</td>
</tr>
</tbody>
</table>

aesConnectivity

This API provides the ability to specify the NIC used for client, switch, or media connectivity.

**Syntax**

```
aesConnectivity [-oam|switch|-media|-client] [ipaddress] - If only one of the connectivity need to be changed or configured.
aesConnectivity [-oam|switch|-media|-client] [ipaddress] [-oam|-switch|-media|-client] [ipaddress] - If only one or more of the connectivity need to be changed or configured.
aesConnectivity -oam [ip address] -client [ip address] -switch [ip address] -media [ipaddress] - If all of the connectivity need to be changed or configured.
```

**Note:**

To allow connectivity from any ipaddress, enter '0.0.0.0' or '::' as ipaddress.

**For example,**

```
aesConnectivity -oam 0.0.0.0 -client 10.133.84.223 -switch 10.133.84.230 -media 10.133.84.230
```

where:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>oam</td>
<td>To set oam connectivity.</td>
</tr>
<tr>
<td>client</td>
<td>To set client connectivity.</td>
</tr>
<tr>
<td>switch</td>
<td>To set switch connectivity.</td>
</tr>
<tr>
<td>media</td>
<td>To set media connectivity.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>AES IP, virtual IP (incase if HA is configured or any (0.0.0.0)).</td>
</tr>
</tbody>
</table>
Return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Make sure CVLAN Service is offline. If not, user should stop service before changing the client facing IP.</td>
</tr>
<tr>
<td>5</td>
<td>Either invalid or not permissible IP address.</td>
</tr>
<tr>
<td>6</td>
<td>Execute with root user.</td>
</tr>
<tr>
<td>7</td>
<td>The command failed to execute.</td>
</tr>
<tr>
<td>8</td>
<td>Failed to restart service &lt;service name&gt;.</td>
</tr>
</tbody>
</table>
Chapter 8: Security Administration and Additional PAM Management

About Security Administration and additional PAM management

This chapter covers two major sections:

- **Security administration.** Security administration refers to managing the local Linux accounts on the AE Server and includes the following:
  - Account management
  - Pluggable Authentication Module (PAM) management
  - Login reports
  - Login audit

- **Additional PAM management capabilities.** PAM management capabilities describes authentication methods that apply to DMCC, TSAPI, JTAPI, and Telephony Web Services users. The information in this section does not apply to AE Services Management Console users or remote users with SSH access. PAM management includes the following:
  - Linux (using pam_unix)
  - LDAP (using pam_ldap)
  - AE Services User Management (using pam_ldap)
  - Active Directory w/ Kerberos (using pam_krb5)

**Note:**

The information in this chapter is not applicable to users of the following applications: DLG, CVLAN, and the System Management Service (SMS).

Security administration

The Security administration features can be accessed by the user assigned to the Security_Administrator role. For information about role assignments, see AE Services administrative roles and access privileges (role based access control - RBAC) on page 321.
The Security Administration feature (Account Management and PAM administration) affects the AE Services Management Console and access to the Linux server.

- **Account management**
  - Add Login
  - Modify Login
  - Remove Login
  - Lock/Unlock Login

- **PAM**
  - PAM Issue
  - PAM Limits
  - PAM MOTD
  - PAM Password Manager
  - PAM Time

- **Audit**
  - Login Reports
  - Login Audit

For an illustration of this administrative domain, see the figure on page 165.

---

**Figure 29: AE Services Security Administration and PAM management -- AE Services Management Console administrators**
Account Management - Linux user accounts

Account Management provides the following features for managing administrator logins and login groups.

- **Add Login** — lets you add a user account to Linux. For more information, see *Adding a local Linux account for an administrator - sample* on page 166.
- **Modify Login** — lets you change the Linux account attributes for an administrator. For more information, see *Changing the properties of a Linux administrative account -- Modify login* on page 170.
- **Remove Login** — lets you remove a Linux account. For more information, see *Removing a Linux account - Remove Login* on page 171.
- **Lock Unlock Login** — lets you block or grant access to the AE Services Management Console and the AE Server. For more information, see *Locking or unlocking a Linux account - Lock/Unlock Login* on page 172.

Adding a local Linux account for an administrator

**About this task**

Use this procedure to add a local Linux account for an administrator with the following roles:

- Auditor
- Backup_Restore
- Avaya_Maintenance

The following procedure is a sample scenario that depicts using a limited number of roles. AE Services also provides additional roles. For more information about roles and mapping to Linux groups, see *AE Services administrative roles and access privileges (role based access control - RBAC)* on page 321.

In Geo Redundant High Availability configuration, you must create any user on the primary server on the secondary server by using the command line interface.

**Procedure**

1. On the AE Services Management Console main menu, select **Security > Account Management > Add Login**.
2. On the Add Login page, in the **Login ID** field, enter a user name.
   
   A login ID can consist of up to 32 characters. The set of valid characters is: lowercase a through z; uppercase A-Z, the numbers 0 through 9, the dash (-), and the underscore (_).
3. Click **Continue**.
4. On the Add Login page, do the following:
   a. In the **Default Login Group** field, accept the default **users**.
The Default Login Group user maps to the Auditor role. You can have only one group name in the Default Login Group field.

b. In the Additional Login Groups field, type backuprestore, avayamaint.

You can have more than one group name in this field. When you enter more than one group name, separate each group name with a comma. Valid group names are:

- susers
- securityadmin
- backuprestore
- users
- avayamaint
- easg

c. In the Allow Linux Shell Access field, accept the default (unchecked) unless you want to provide Shell access to the user.

d. In the Lock Account check box, accept the default (unchecked).

e. In the Date on which account is disabled field, accept the default (blank) unless this is a temporary account that will be disabled within a specific time frame.

f. Under Password Authentication, in the Enter Password and Re-enter password fields, type the password based on the password policy.

The default Linux password policy, which is based on a US standard keyboard and the default password limits for PAM Module Configuration, calls for a minimum of 8 characters, with at least 1 uppercase character, 1 lowercase character, 1 alphanumeric character, and 1 special character. The following characters are not permitted: $ (dollar sign), ’ (apostrophe), “ (quotation mark), \ (backslash), the space character, and any ASCII control-character.

g. On the Force password change on first login dialog box, click No.

h. In the Maximum number of days a password may be used (PASS_MAX_DAYS) field, accept the default (99999).

i. In the Minimum number of days allowed between password changes (PASS_MIN_DAYS) field, accept the default (0).

j. In the Number of days warning given before a password expires (PASS_WARN_AGE) field, accept the default (7).

k. In the Days after password expired to lock account field, accept the default (0).

5. Reenter the cust password and click Apply.

See Results of adding a local Linux account for an administrator - sample on page 168 to see the access privileges administered for this user (aesadmin3).
Results of adding a local Linux account for an administrator - sample

The following table depicts the results of the sample scenario for adding the aesadmin3 user to the securityadmin and avayamaint groups. The aesadmin3 user now has privileges associated with the Security_Administrator role and the Avaya_Maintenance role in addition to the default privileges associated with the Auditor role. For more information about AE Services administrative roles, see AE Services administrative roles and access privileges (role based access control - RBAC on page 321.

<table>
<thead>
<tr>
<th>Role</th>
<th>Linux group</th>
<th>AE Services Management Console access privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor</td>
<td>users</td>
<td>Read-only access to the following menus:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Security -- access is limited to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Certificate Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Security Database &gt; CTI Users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Alarm Viewer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Logs -- access is limited to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Audit Logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Error Logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Install Logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User Management Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Status and Control - access is limited to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CVLAN Service Summary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DLG Service Summary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DMCC Service Summary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Switch Conn Summary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TSAPI Service Summary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Help</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Role</th>
<th>Linux group</th>
<th><strong>AE Services Management Console access privileges</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security_Administrator</td>
<td>securityadmin</td>
<td>Read and write access to the following menus in the AE Services Management Console:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Account Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Certificate Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- PAM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Security Database</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Tripwire Properties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Alarm Viewer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Status and Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Help</td>
</tr>
<tr>
<td>Avaya_Maintenance</td>
<td>avayamaint</td>
<td>Read and write access to the following menus in the AE Services Management Console:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Security Database</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Service Controller</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Server Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Certificate Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Security Database</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Alarm Viewer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Utilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Diagnostics</td>
</tr>
</tbody>
</table>
Changing the properties of a Linux administrative account -- modify login

About this task

Use the Modify Login feature to change the properties of a Linux administrative account. For example, assume that you want to restrict the administrative capabilities of the aesadmin3 account (created in Adding a local Linux account for an administrator - sample on page 166) to the Avaya Maintenance role only.

Procedure

1. From the AE Services Management Console main menu, select Security > Account Management > Modify Login.

AE Services displays the initial Modify Login page, which contains the Login ID text box.

2. On the Modify Login page, enter a user name in the Login ID field (for example aesadmin3).

3. Click Continue.

4. Complete the Modify Login page as follows:
   a. In the Default Login Group field, replace users with avayamaint.
   b. In the Additional login groups (optional) field, delete all entries (leave the field blank).
   c. For the remaining fields, keep the administered settings.

   ☀ Note:

   If you modify any of the password settings (such as PASS_MAX_DAYS or PASS_MIN_DAYS), the settings that you administer on this page take precedence for the particular user you are administering. The default password settings are read in from the PAM Management Global Password Aging page. Any password settings you change on the Modify Login page for a particular user have no effect on the PAM Management Global Password Aging page.

5. Reenter the cust password and click Apply.

See Results of changing role assignments for “aesadmin3” - sample on page 170 to see the modified access privileges for this user.

Results of changing role assignments for aesadmin3 - sample

The following table depicts the results of the sample scenario for changing aesadmin3 from the Auditor role to the Avaya_Maintenance role. For more information about AE Services administrative roles, see AE Services administrative roles and access privileges (role based access control - RBAC on page 321.
<table>
<thead>
<tr>
<th>Role</th>
<th>Linux group</th>
<th>AE Services Management Console access privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya_Maintenance</td>
<td>avayamaint</td>
<td>Read and write access to the following menus in the AE Services Management Console:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Security Database</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Service Controller</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Server Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Certificate Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Security Database</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Alarm Viewer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Utilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Diagnostics</td>
</tr>
</tbody>
</table>

**Removing a Linux account - Remove Login**

**About this task**

Use this procedure to delete a Linux administrative account.

**Note:**

If an application such as DMCC, TSAPI, JTAPI, or Telephony Web Services uses local Linux for authentication, the Remove Login action affects the application.

**Procedure**

1. On the AE Services Management Console main menu, select **Security > Account Management > Remove Login**.
2. On the Remove Login page, in the **Login ID** field, type the login ID of the administrative account that you want to remove.
3. Click **Continue**.
4. On the **Remove Login** page, verify the correct account is displayed.
5. Reenter the cust password and click **Apply**.
Locking or unlocking a Linux account

About this task

Use this procedure to lock or unlock an existing Linux account. Locking an account means prohibiting access to the AE Services Management Console.

* Note:

If an application such as DMCC, TSAPI, JTAPI, or Telephony Web Services uses local Linux for authentication, the application will also be affected by the Lock/Unlock action.

The Lock/Unlock Login feature acts as a toggle. If the account is locked, the Lock/Unlock feature lets you unlock the account; if the account is not locked, the Lock/Unlock feature lets you lock the account.

Procedure

2. On the Lock/Unlock Login page, in the Login ID field, type the login ID of the administrative account whose access you want to change.
3. Click Continue.
4. On the Lock/Unlock Login page, verify that the correct account is displayed.
5. Reenter the cust password and click Apply.
6. Do one of the following:
   - If the account is currently locked, to unlock the account, click Unlock.
   - If the account is currently unlocked, to lock the account, click Lock.

PAM Management

The AE Services Pluggable Authentication Module (PAM) Management Web pages enable you to set up the PAM authentication scheme for managing users who have access to the AE Services Management Console and the Linux server. PAM Management provides the following capabilities:

- The ability to define rules that require users to change their passwords periodically and how administrator accounts are authenticated and controlled. For more information, see Administering the PAM Password Manager on page 173.
- The ability to manage the login message. For more information, see Creating a PAM Issue (/etc/issue) message on page 175.
- The ability to display and change the message of the day (MOTD). For more information, see Creating a PAM MOTD (/etc/motd) message on page 176.
• The ability to limit the maximum number of simultaneous logins. For more information, see Adding PAM limits on page 176.

• The ability to restrict when (days of the week or times of day) a user can log in to AE Services. For more information see Administering PAM time on page 177.

---

Administering the PAM Password Manager

About this task

The PAM Password Manager allows you to define:

• rules that require users to change their passwords periodically. The settings on this page affect the settings in the /etc/login.defs file and are used by the Add Login and Modify Login pages.

🌟 Note:

Changes to the global password settings will only affect new users. Existing users will not be affected.

• how AE Services Management Console administrative accounts are authenticated and controlled.

Procedure

1. From the AE Services Management Console main menu, select Security > PAM > PAM Password Manager.

2. In the New global password configuration (etc/login.defs) section, perform the following steps:
   a. In the Maximum number of days a password may be used (PASS_MAX_DAYS) field, accept or change the default (60).
   b. In the Minimum number of days allowed between password changes (PASS_MIN_DAYS) field, accept or change the default (1).
   c. In the Number of days warning given before a password expires (PASS_WARN_AGE) field, accept or change the default (10).

3. In the Optional Additional Authentication Protocols section, perform one of the following steps:
   • If you authenticate users to an external LDAP server, select the External LDAP check box.
   • If you do not authenticate users to an external LDAP server, accept the default. By default, this option is disabled (that is, a check mark does not appear in the External LDAP check box). When this option is disabled, AE Services authenticates OAM administrative users to the local Linux password store on the AE Services server.
   • If you want to allow the Avaya Logins access to the server (Recommended), select the Enable EASG user access checkbox. This option also allow the ability to specify which of the Avaya Logins may or may not be granted access.
**Note:**
By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner. In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.

- If you want to block the Avaya Logins access to the server, select the **Enable EASG user access** checkbox.

**Note:**
By disabling Avaya Logins you are preventing Avaya access to your system. This is not recommended, as it impacts Avaya’s ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled.

4. In the **Password Limits** section, accept or change the default settings. These settings are described as follows:

- Enforce Password Limits check box indicates whether password limits are in effect for the user. This setting is enabled by default (the check box is selected), which, in turn, enables the following settings.
- Number of times user is prompted for a new password (retry). The default is 3.
- Number of characters in new password that must be different from old password (difok). The default is 2.
- Minimum length of a new password (minlen). The default is 8.
- Minimum credit in meeting required password length for digits in a password (dcredit). The default is 1.
- Minimum credit in meeting required password length for upper case characters in a password (ucredit). The default is 1.
- Minimum credit in meeting required password length for lower case characters in a password (lcredit). The default is 1.
- Minimum credit in a meeting required password length for other characters in a password (ocredit). The default is 1.
- Number of previous passwords that cannot be reused. The default is 5.
- Maximum number of same consecutive characters in a password. The default is 3.
- The algorithm used to encrypt the Linux password. The choices are **sha256** and **sha512**.
The following PAM rules are applicable only if you modify account using the command line interface:

- maxrepeat
- Number of previous passwords that cannot be reused

5. In the **Failed Login Response** section, accept or change the default settings. These settings are described as follows:
   - Enable account lockout with the following parameters check box. This check box is enabled by default, which, in turn, enables the following settings.
   - Lock out login after unsuccessful attempts to login (deny). The default is 3 attempts.
   - Lock account for seconds (lock_time). The default is 60 seconds.

6. Click **Apply Changes**.

---

**Creating a PAM Issue (/etc/issue) message**

**About this task**

Use the PAM Issue feature to display a message before you log in to the AE Services Management Console. The PAM Issue screen also contains a **Continue to Login** link.

The PAM Issue text is stored in `/etc/issue`. If the `/etc/issue` file does not exist, AE Services will not display a PAM Issue message.

**Note:**

If you access the AE Services Linux shell (command prompt) either locally using a system console or remotely using a secure shell (ssh) client, you will see the PAM Issue message.

**Procedure**

1. From the AE Services Management Console main menu, select **Security > PAM > PAM Issue**.

2. Follow these steps to complete the **PAM Issue** page.
   - Accept the default, **Display a message prior to login**.
   - Replace the default display (the Warning Notice) with the message of your choice.

**Tip:**

The text window on the page is 80 columns wide and 25 lines long. As you approach the 80 column limit, press Enter to force the start of the next line. If you do not force a new line, the text will extend beyond the 80 character boundary.

3. Click **Apply Changes**.
Creating a PAM MOTD (/etc/motd) message

About this task

Use the PAM Message of the Day (MOTD) feature to display a message of the day on the AE Services Management Console after the log-in screen is completed. The PAM MOTD screen also contains a Continue button.

The PAM MOTD text is stored in /etc/motd. If the etc/motd file does not exist, AE Services will not display a message of the day.

Note:

If you access the AE Services Linux shell (command prompt) either locally using a system console or remotely using a secure shell (ssh) client, you will see the PAM MOTD message.

Procedure

1. From the AE Services Management Console main menu, select Security > PAM > PAM MOTD.
2. Follow these steps to complete the PAM MOTD page.
   a. Select the check box for Display a message of the day after login.
   b. Type a message in the text box (for example, Hello System Administrator).
   c. Click Apply Changes.

   Tip:

   The text window on the page is 80 columns wide and 25 lines long. As you approach the 80 column limit, press Enter to force the start of the next line. If you do not force a new line, the text will extend beyond the 80 character boundary.

Adding PAM limits

About this task

Use the PAM Limits page to set the maximum number of simultaneous logins for a user. Keep in mind that the limit for the maximum number of simultaneous logins is a total of all access methods — AE Services Management Console access, shell access, and remote access.

Procedure

1. From the AE Services Management Console main menu, select Security > PAM > PAM Limits.
2. Follow these steps to complete the PAM Limits page.
   a. Accept the default to enable the setting, Limit the number of simultaneous logins.
   b. Accept the default setting (10) for Default Global Pam Limits.
c. In the New Configuration section, click Add.

3. Follow these steps to complete the Add PAM Limits page.
   a. In the Login ID field, enter a currently administered login ID or user name (for example `aesadmin3`).
   b. In the Value field, enter the maximum number of logins for this user (for example `3`).
   c. Click Apply Changes.
   d. On the Add PAM Limits warning screen, click Apply.

Administering PAM time

About this task
Use the PAM Time page to restrict access based on time of day and day of week. If you elect to configure PAM time for a user, you must prohibit a user from logging in for at least one 5-minute interval per week. To meet this minimum requirement, on the PAM Time page, you would select 1 day (for example Sunday) and 1 time interval (for example 00:05 to 00:10) for denying access.

Procedure

1. From the AE Services Management Console main menu, select Security > PAM > PAM Time.
2. Select the Limit logins by time of day check box.
   🔄 Note:
   The Limit logins by time of day check box must be checked for you to restrict access based on the day of the week or time of day.
3. If prompted to confirm that you want to limit logins by time of day, click OK.
4. On the PAM Time page, click Add.
   The Add PAM Time page appears.
5. In the Login field, enter the login ID or user name.
6. From the Access Rule drop-down menu, select Deny.
7. Select the check box(es) for the appropriate day(s) of the week.
8. Using the From box, select the appropriate hour and minutes for the beginning of the time interval.
9. Using the To box, select the appropriate hour and minutes for the end of the time interval.
10. Click Apply Changes.
Support for Enhanced Access Security Gateway

Application Enablement Services supports Enhanced Access Security Gateway (EASG). EASG provides a secure method for Avaya services personnel to access the Avaya Aura® AE Services remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

EASG can be enabled or disabled using the AE Services Management Console.

Related links
- Enabling or disabling EASG through the CLI interface on page 178
- Enabling or disabling EASG through the AE Services Management Console interface on page 179
- Viewing the EASG certificate information on page 180
- EASG product certificate expiration on page 180

Enabling or disabling EASG through the CLI interface

About this task
Avaya recommends enabling EASG. By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner. In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Refer to the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.

By disabling Avaya Logins you are preventing Avaya access to your system. This is not recommended, as it impacts Avaya’s ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled.

Procedure

1. Log on to the AE Services Management Console as an administrator associated with the Linux group, easg.
   
   If you log in to the AE Services as a craft with more than three invalid responses, your account gets locked due to PAM configuration. Also, if you run the EASGManage --listUsers command on the command line interface, the system displays the following output:
   
   Locked = No
   
   Both the features are different and does not have any relation with each other.

2. To check the status of EASG, run the following command: EASGStatus.
3. To enable EASG (Recommended), run the following command: EASGManage --enableEASG.

4. To disable EASG, run the following command: EASGManage --disableEASG.

Related links
Support for Enhanced Access Security Gateway on page 178

Enabling or disabling EASG through the AE Services Management Console interface

About this task
Avaya recommends enabling EASG. By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner. In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.

By disabling Avaya Logins you are preventing Avaya access to your system. This is not recommended, as it impacts Avaya’s ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled.

Note:

- If EASG is enabled during a fresh install, the Optional Additional Authentication Protocols section displays the Enable EASG check box as checked.
- Unchecking the Enable EASG checkbox disables access for the Avaya Logins craft and sroot.

Procedure

1. Log on to the Application Enablement Services OAM interface.
2. Go to Security > PAM > PAM Password Manager
3. In the Optional Additional Authentication Protocols section, check the Enable EASG box to enable EASG (Recommended). Additional settings are presented
4. Allow access for the Avaya Logins by checking the checkbox associated with the users craft and sroot.

Related links
Support for Enhanced Access Security Gateway on page 178
Viewing the EASG certificate information

About this task
Use this procedure to view information about the product certificate, which includes information about when the certificate expires.

Procedure
1. Log in to the Application Enablement Services CLI interface.
2. Run the following command: `EASGProductCert --certInfo`.

Related links
- [Support for Enhanced Access Security Gateway](#) on page 178

EASG product certificate expiration

Application Enablement Services raises an alarm if the EASG product certificate has expired or is about to expire in 365 days, 180 days, or 30 days. To resolve this alarm, the customer must apply the patch for a new certificate or upgrade to the latest release. Else, the customer loses the ability for Avaya to provide remote access support.

If the EASG product certificate expires, EASG access is still possible through the installation of EASG site certificate.

Related links
- [Support for Enhanced Access Security Gateway](#) on page 178

EASG site certificate

EASG site certificates are used by the onsite Avaya technicians who do not have access to the Avaya network to generate a response to the EASG challenge. The technician will generate and provide the EASG site certificate to the customer. The customer loads this EASG site certificate on each server to which the customer has granted the technician access. The EASG site certificate will only allow access to systems on which it has been installed, and will only allow access to the given Avaya technician and cannot be used by anyone else to access the system including other Avaya technicians. Once this is done, the technician logs in with the EASG challenge/response.

Managing site certificates

Before you begin
1. Obtain the site certificate from the Avaya support technician.
2. You must load this site certificate on each server that the technician needs to access. Use a file transfer tool, such as WinSCP to copy the site certificate to `/home/cust` directory,
where cust is the login ID. The directory might vary depending on the file transfer tool used.

3. Note the location of this certificate and use in place of installed_pkcs7_name in the commands.

4. You must have the following before loading the site certificate:
   - Login ID and password
   - Secure file transfer tool, such as WinSCP
   - Site Authentication Factor

**Procedure**

1. Log in to the AE Services CLI interface as an administrator associated with the Linux group, easg.

2. To install the site certificate:
   a. Run the following command: `sudo EASGSiteCertManage --add <installed_pkcs7_name>`.
   b. Save the Site Authentication Factor to share with the technician once on site.

3. To view information about a particular certificate: run the following command:
   - `sudo EASGSiteCertManage --list`: To list all the site certificates that are currently installed on the system.
   - `sudo EASGSiteCertManage --show <installed_pkcs7_name>`: To display detailed information about the specified site certificate.

4. To delete the site certificate, run the following command:
   - `sudo EASGSiteCertManage --delete <installed_pkcs7_name>`: To delete the specified site certificate.
   - `sudo EASGSiteCertManage --delete all`: To delete all the site certificates that are currently installed on the system.

---

**Login reports**

AE Services provides two types of login reports:

- A login report for all Linux accounts — see [Displaying a login report for all Linux accounts](#) on page 182.
- A login report for a particular login ID — see [Displaying a login report for a specific login ID](#) on page 182.
Displaying a login report for all Linux accounts

Procedure

1. From the AE Services Management Console main menu, select Security > Audit > Login Reports.

2. On the Login Reports page, in the List Local Host Logins field, accept the default (enabled), and click Continue.

AE Services displays the Login Reports - List Local Host Logins page. For a description of the fields on this page, see List Local Host Logins page field descriptions on page 182.

List Local Host Logins page field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Lists the name of the Linux login.</td>
</tr>
<tr>
<td>Group</td>
<td>Indicates the group name to which the login name is assigned.</td>
</tr>
<tr>
<td>Roles</td>
<td>Indicates the administrative role for a user, such as System_Administrator.</td>
</tr>
<tr>
<td>Lock</td>
<td>Yes or No to indicate if a lock exists for this account.</td>
</tr>
<tr>
<td>Shell Access</td>
<td>Yes or No to indicate whether the login name (account) has access to the Linux shell.</td>
</tr>
</tbody>
</table>

Displaying a login report for a specific login ID

Procedure

1. From the AE Services Management Console main menu, select Security > Audit > Login Reports.

2. On the Login Reports page, select Display Information for Local Host Login.

3. Enter the login ID for whom you want to generate a login report.

4. Click Continue.

AE Services displays the Login Reports - Display Login Information page. For a description of the fields on this page, see Display Login Information page field descriptions on page 183.
# Display Login Information page field descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information for Login:</td>
<td>Identifies the login name.</td>
</tr>
<tr>
<td>Group Name</td>
<td>Lists the Linux group name that the login ID is assigned to.</td>
</tr>
<tr>
<td>Other Groups</td>
<td>Lists other group names that the login ID is assigned to.</td>
</tr>
<tr>
<td>Roles</td>
<td>List the roles that are assigned to the login ID.</td>
</tr>
<tr>
<td>Shadow Locked</td>
<td>Indicates whether password shadowing is enabled or disabled.</td>
</tr>
<tr>
<td></td>
<td>• Yes - Indicates that password shadowing is enabled.</td>
</tr>
<tr>
<td></td>
<td>• No - Indicates that password shadowing is disabled.</td>
</tr>
<tr>
<td>Pam_Tally Locked</td>
<td>Indicates whether PAM tally limits are enabled or disabled.</td>
</tr>
<tr>
<td></td>
<td>• Yes - Indicates that the PAM tally is enabled.</td>
</tr>
<tr>
<td></td>
<td>• No - Indicates that the PAM tally is disabled.</td>
</tr>
<tr>
<td>Shell Access</td>
<td>Indicates whether the login name (account) has access to the Linux shell.</td>
</tr>
<tr>
<td></td>
<td>• Yes indicates that the login name has access to the Linux shell.</td>
</tr>
<tr>
<td></td>
<td>• No indicates that the login name does not have access to the Linux shell.</td>
</tr>
<tr>
<td>PW Min Days</td>
<td>Indicates the minimum number of days allowed between password changes, which is specified by the PASS_MIN_DAYS setting in the etc/login.defs file.</td>
</tr>
<tr>
<td>PW Max Days</td>
<td>Indicates the maximum number of days a password may be used, which is specified by the PASS_MAX_DAYS setting in the etc/login.defs file.</td>
</tr>
<tr>
<td>PW Warn Days</td>
<td>Indicates the number of days warning given before a password expires, which is specified by the PASS_WARN_AGE setting in the etc/login.defs file.</td>
</tr>
<tr>
<td>PW Last Changed</td>
<td>Indicates the date (MM DD YYYY) that the password was last changed.</td>
</tr>
<tr>
<td>PW Next Change Allowed</td>
<td>Indicates the first date that the next password change is permitted.</td>
</tr>
<tr>
<td>PW Expires</td>
<td>Indicates the date that the password expires.</td>
</tr>
<tr>
<td>Account Expires</td>
<td>Indicates the date that the login ID expires.</td>
</tr>
</tbody>
</table>
Enabling a login audit

About this task
Use the Login Audit feature to enable and configure an audit process for disabling an unused Linux account.

Procedure
1. From the AE Services Management Console main menu, select Security > Audit > Login Audit.
2. Use the settings on the Unused Login Audit page to enable the auditing process. (Alternatively, if you have an auditing process enabled, you can use this page to disable the audit.)

For a description of the fields on the Unused Login Audit page, See Unused Login Audit page field descriptions on page 184.

Unused Login Audit page field descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the Audit</td>
<td>• Select Yes to start the auditing process.</td>
</tr>
<tr>
<td></td>
<td>• Select No to stop the auditing process. No is the default setting.</td>
</tr>
<tr>
<td>Time to Begin Audit Each Day: (hour)</td>
<td>Select a start time to begin the audit, based on a 24-hour clock (select from 00 to 23).</td>
</tr>
<tr>
<td>Maximum Unused Time: (days, 3-365)</td>
<td>Enter a value from 3 to 365 to indicate the limit, in days, for maximum unused time. When the limit is reached the account is disabled.</td>
</tr>
<tr>
<td>Submit</td>
<td>Click Submit to start the audit process.</td>
</tr>
</tbody>
</table>

AE Services client applications additional authentication methods
User Management is the default user database that AE Services uses for user authentication (validating a user’s identity). for TSAPI, JTAPI, DMCC, and Telephony Web Services users. If you select not to use the User Management service, you can use any of the following authentication methods:
When Linux is the AE Services authentication authority, AE Services users are authenticated against the Linux accounts created on the AE Server.

⚠️ Caution:
This means that AE Services users have access rights to the AE Services Management Console and can log into the AE Server.

- If you want to use Linux instead of the User Management for AE Services authentication, you will need to carry out the following procedures:
  - Install the Linux PAM file instead of the User Management PAM file, see Instating the Linux PAM file on page 186.
  - Set up a Linux user account for each AE Services user, see Adding a Linux user on page 239.
  - Additionally, if you plan to use the Security Database, you will need to add each user to the User Management database. Although you are not using the User Management database for authentication, you must use it to populate the Security Database. See Adding a user to User Management on page 139.
- If you need to revert back to using User Management for authentication, you will need to re-instate the User Management PAM file, see Re-instating the User Management PAM file on page 186.
Changing to User Management Authentication for the AE Services client application

About this task
Use this procedure only if you are reverting back to the User Management.

Procedure
1. Log into AE Services and `su to root` or `sroot`.
2. From the Linux command line, type the following command:
   ```
   cp /opt/mvap/tsapi/tsapi_service.ldap /etc/pam.d/tsapi_service
   ```

Changing to Linux PAM Authentication for the AE Services client application

Procedure
1. Log into AE Services, and `su to root` or `sroot`.
2. From the Linux command line, type the following command:
   ```
   cp /opt/mvap/tsapi/tsapi_service.linux /etc/pam.d/tsapi_service
   ```

Changing to User Management Authentication for the AE Services client application

About this task
Use this procedure only if you are reverting back to the User Management.

Procedure
1. Log into AE Services and `su to root` or `sroot`.
2. From the Linux command line, type the following command:
   ```
   cp /opt/mvap/tsapi/tsapi_service.ldap /etc/pam.d/tsapi_service
   ```

Enterprise directory settings in the AE Services Management Console

An enterprise directory refers to an external LDAP directory server, such as OpenLDAP or Microsoft Active Directory Services. In AE Services, some form of a directory may be used by TSAPI, JTAPI, Telephony Web Services, and DMCC for authentication purposes only.
If you are planning to use an external LDAP directory for TSAPI, JTAPI, Telephony Web Services, and DMCC and you do not plan to use Microsoft Active Directory Services with Kerberos for authentication, you will need to administer the settings using the AE Services Management Console on the Security > Enterprise Directory Configuration page. For an illustration of this context, see Figure 30: AE Services client authentication -- additional PAM management on page 185.

Enterprise directory configuration settings for AE Services integrations

The enterprise directory configuration settings may apply to the AE Services implementation for Microsoft Lync Server 2010 and 2013. If you are administering AE Services for the integration of Microsoft Lync Server, see the Avaya Aura® Application Enablement Services Implementation Guide for Microsoft® Live Communications Server 2005, Microsoft Office Communications Server 2007, and Microsoft Lync® Server 2010 and 2013, 02-601893.

Enterprise directory configuration settings with bridged appearance alert blocking

The enterprise directory is used in conjunction with the bridged appearance alert blocking feature. This feature applies to DMCC applications as well as the AE Services integrations with Microsoft Office Live Communications Server, Microsoft Office Communications Server, and Microsoft Lync Server 2010 and 2013. DMCC applications that have requested the desktop call control filtering mode can take advantage of the bridged appearance alert blocking feature. For more information about setting up a DMCC application to use the call filtering mode, see the following documents:

- Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer's Guide, 02-300359
- Avaya Aura® Application Enablement Services Device, Media, and Call Control XML Programmer's Guide, 02-300358

Enterprise directory user authorization policy for DMCC applications

The enterprise directory user authorization policy relies on the LDAP enterprise directory for user authorization. DMCC applications can take advantage of this capability.
To implement the enterprise directory authorization policy you must administer the settings on the Enterprise Directory page in the AE Services Management Console. The following settings on the Enterprise Directory page are critical to this authorization method:

- **Search Filter Attribute Name** — This indicates the attribute name in the user record that corresponds to username. DMCC will attempt to match a username to the contents of this attribute. An example is “SAM-Account-Name” in Windows Active Directory.

- **Device ID Attribute** — This indicates the attribute name in the user record that corresponds to the device ID to be authorized for the user. A primary example here is an attribute such as “Phone Number” that contains a provisioned E.164 number for users.

When this authorization mechanism is selected, DMCC uses LDAP to query the user record for the provisioned device ID (such as the phone number). DMCC then caches the retrieved device ID. When DMCC attempts to authorize a request, it verifies that the device ID retrieved from the user record is a substring of the device ID specified in the request. This allows per-user authorization without per-user provisioning in AE Services. The substring match accounts for a very common scenario where a Tel URI is specified in the request (tel:+13035381234) but the user record contains an E.164 number (+13035381234) or extension (5380112).

For more information about leveraging advanced authentication (AA) policies from DMCC applications, see the following documents:

- *Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer's Guide*, 02-300359
- *Avaya Aura® Application Enablement Services Device, Media, and Call Control XML Programmer's Guide*, 02-300358

---

**Changing to Active Directory Authentication for the AE Services client application**

**About this task**

This procedure is performed by an administrator on the AE Services Server.

**Procedure**

1. Log into the AE Services Server as **root** or **sroot**.

2. At the command prompt, type the following command:
   
   ```
   cp /opt/mvap/tsapi/tsapi_service.ads /etc/pam.d/tsapi_service
   ```

   For more information, see [Re-instating the User Management PAM file](#) on page 186.
Configuring AE Services to access an enterprise directory

About this task
Use this procedure to configure AE Services to access the enterprise directory for a TSAPI, JTAPI, Telephony Web Services, or DMCC application that authenticates to an external LDAP server.

Procedure
2. On the Enterprise Directory Configuration page, provide the following information:
   a. In the User DN for Query Authentication field, type the DN for the user object that AE Services uses for accessing an external or enterprise directory. Based on how users are set up in an enterprise directory, the user object could refer to a full name, a display name, a user login, an application name, or a server name, for example, 
      cn=John Doe,cn=Users,dc=mycompany,dc=example,dc=com.
   b. In the Password field, type the password of the enterprise directory server.
   c. In the Confirm Password field, reenter the password.
   d. In the Base Search DN field, type the LDAP string that indicates where you want to start the search.
   e. In the Host FQDN field, type the FQDN of the enterprise directory server.
   f. In the Secondary HostName/IP Address field, type the IP address of the failover server if your configuration supports a failover server for the enterprise directory server.
   g. In the User ID Attribute Name field, accept the default, uid. You might need to change this setting to match your LDAP implementation. The default attribute names of some popular LDAP implementations are as follows:
      • AE Services User Management: uid
      • Microsoft Active Directory: samaccountname
      • IBM Lotus Domino: uid
   h. Ignore the User Role Attribute Name field. It does not apply to TSAPI, JTAPI, DMCC, and Telephony Web Services.
   i. In the Port field, type the port number used for enterprise directory access. The default port is 636.
   j. In the Secondary Port field, type the port number used for the failover server for the enterprise directory server.
   k. In the Change Password URL field, type the URL of your password change system.
   l. Ensure that the LDAP-S option is selected and is read-only.
Starting with AE Services Release 7.1, LDAP-S is required. The CA certificates used to sign the Enterprise Directory server identity certificate must be imported into the AE Services Management Console CA trust store.

3. Click **Apply Changes**.

---

**Configuring an external LDAP server — Windows**

**Procedure**

1. Install the Identity Management for UNIX component on Windows 2003 R2. This can be found under Add/Remove Windows Components, then double click on Active Directory Services.

2. Follow these steps to create an AES group.
   a. Click **Start > Run**.
   b. Type `dsa.msc`.
   c. Click **OK**.
   d. In the **Active Directory Users and Computers** dialog box, right click **Builtin > New > Group**.
   e. In the **New Object — Group** dialog box, in the **Group name** field, type **AES**.
   f. Click **OK**.
   g. Open the **AES** Group property, and click the **UNIX Attributes** tab.
   h. From the **NIS Domain** drop-down box, select the NIS domain this group belongs to.
      i. Click **OK**.

3. Follow these steps to configure the user's UNIX attributes.
   a. Create a user or use an existing user.
   b. Open the **User Properties** dialog box.
   c. Click the **UNIX Attributes** tab.
   d. In the **NIS Domain** field, select the appropriate NIS domain.
   e. From the **Primary group name/GID** drop-down box, select **AES**.
   f. Click **OK**.

4. Follow these steps to set up user roles. See **User roles** on page 191 for a list of user roles and corresponding privileges.
   a. Create an attribute or use an existing attribute on LDAP with the value `Security_administrator,Auditor`. 

Comments on this document? infodev@avaya.com
**Note:**

If the user has multiple roles, use a comma for the delimiter. For example: Audit, System_Administrator, Security_Administrator, Backup_restore.

b. In the `<user>SecurityAdmin Properties` dialog box, in the Description field, type Security_administrator,Auditor.

c. Click OK.

5. Follow these steps to configure Enterprise Directory.

   a. Log in to the AE Services Management Console as System Administrator.

   b. From the AE Services Management Console main menu, select **Security > Enterprise Directory**.

   c. On the **Enterprise Directory** page, in the **User Role Attribute Name** field, type description. This is the name of the user attribute, which contains the user’s roles in LDAP.

6. Follow these steps to enable external LDAP.

   a. Log in to the AE Services Management Console as System/Security Administrator.

   b. From the AE Services Management Console main menu, select **Security > PAM > PAM Module**.

   c. On the **PAM Module Configuration** page, select the External LDAP check box.

   d. Click **Apply**.

---

### User roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Privileges</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor</td>
<td>• View/List users (CTI, user-management)</td>
<td>Auditor</td>
</tr>
<tr>
<td></td>
<td>• View logs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• View certificates</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• View alarms</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• View status and control</td>
<td></td>
</tr>
<tr>
<td>Security_Administrator</td>
<td>• Key, certificate management</td>
<td>Security_Administrator</td>
</tr>
<tr>
<td></td>
<td>• Role-based access control administration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• View security logs</td>
<td></td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Role</th>
<th>Privileges</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>System_Administrator</td>
<td>Read/write access to all objects/operations except User Management and Security Administrator</td>
<td>System_Administrator</td>
</tr>
<tr>
<td>Backup_Restore</td>
<td>Backup and Restore</td>
<td>Backup_Restore</td>
</tr>
<tr>
<td>Avaya_Maintenance</td>
<td>• Access to maintenance</td>
<td>Avaya_Maintenance</td>
</tr>
<tr>
<td></td>
<td>• View logs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Access to utilities</td>
<td></td>
</tr>
<tr>
<td>User Management</td>
<td>• Manage user accounts</td>
<td>usrsvc_admin (or usrsvc_user)</td>
</tr>
<tr>
<td></td>
<td>• Configure user password policy</td>
<td>This feature is not available in Release 4.x.</td>
</tr>
<tr>
<td>EASG Administrator</td>
<td>Read and write access of the EASG option on the PAM Password Manager.</td>
<td>• Linux group: susers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Linux group ID: 510.</td>
</tr>
<tr>
<td>DataController</td>
<td>Execute all the functionalities related to log/trace retention and clearing</td>
<td>• Linux group: datacontroller</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Linux group ID: 560</td>
</tr>
</tbody>
</table>

### Authentication with Microsoft Active Directory Services and Kerberos

AE Services provides the ability to authenticate users using an external server such as Microsoft Active Directory Services (ADS) or OpenLDAP. If you use ADS, you can implement it with or without Kerberos. This section provides a sample scenario for integrating AE Services with ADS using Kerberos.

In a configuration with ADS and Kerberos, ADS is the AE Services authentication authority, and AE Services users are authenticated against a Domain Controller. This method of authentication requires integrating the AE Server into ADS as a Kerberos client (using Kerberos5).

- With this authentication method, AE Services users do not have access rights to the AE Services Management Console and cannot log into the AE Services Server (Linux).
- If the security database is enabled, the AE Services user must also have an account administered in User Management.
- The AE Services Server will authenticate using Kerberos5.

**Note:**

The time differential between the Domain Controller and the AE Services Server must be less than 2 minutes.
Sample procedures for integrating AE Services with ADS using Kerberos

The information in this section is provided as suggested practices. Although the procedures have been validated, they are simply recommendations. Additionally, the file locations, the commands, and the Kerberos related information are subject to change. Keep in mind that these examples assume that the Microsoft Active Directory Domain Controller supports Kerberos5. If you decide to use Kerberos, you must ensure the integrity of your system and maintain compliance with Kerberos on an ongoing basis.

The following tasks are performed by an AE Services administrator and a Windows Domain Controller administrator.

- Creating an account for The AE Server on the Domain Controller on page 193
- Generating a keytab file for The AE Server account on the Domain Controller on page 194
- Installing The Kerberos5 RPMs on the AE Server on page 194
- Editing The Kerberos 5 configuration file on the AE Server on page 195
- Importing The keytab file on the AE Server on page 196
- Changing from User Management Authentication to Active Directory Authentication on The AE Server on page 188

Creating an account for the AE Services server on the Domain Controller

About this task

On the Domain Controller, follow this procedure to create a user account where the AE Services server is designated as an Active Directory user.

Note:

To perform this procedure you must be a member of the Admin Group in Windows.

Procedure

1. From your desktop, select Start > Settings > Control Panel.
2. From the Control Panel, double-click Administrative Tools.
3. From Administrative Tools, double-click Active Directory Users and Computers.
4. Click Users in the left pane to display the list of users.
5. Move your cursor to the right pane, right-click, and select New > User.
6. Complete the New Object — User dialog box as follows:
   a. In the First name field, type a user name (for example aeserver).
b. Skip the **Initials** and **Last Name** fields.

c. In the **Full name** field, type **aeserver**.

d. In the first part of the **User Logon name** field, type **aeserver**.

e. In the next field, type the address of the Domain Controller (for example
   @dcserver1.xyz.com).

f. In the **User logon name** field (pre Windows 2000), type **aeserver**.

7. Click **Next**.

8. In the New Object — User dialog box, in the **Password** field, type **aespassword**.

9. In the **Confirm password** field, retype **aespassword**.

10. Click **Next**.

11. Click **Finish**.

---

**Generating a keytab file for the AE Server account on the Domain Controller**

### About this task

This procedure is performed by an administrator on the Windows Domain Controller.

After you create the AE Server account on the Windows Domain Controller, generate a keytab file
for the AE Server account.

⚠️ **Note:**

This example uses the aeserver user account name to generate a keytab file called
aeserver.keytab.

### Procedure

From the Windows command prompt type:

```
Ktpass -princ aeserver/aeserver@dcserver1.xyz.com -mapuser aeserver -pass aespassword -out aeserver.keytab
```

---

**Installing the Kerberos5 RPMs on the AE Server**

### About this task

This procedure is performed by an administrator on the AE Server.

Follow this procedure to determine if the pam_krb5 package and the krb5 workstation package are
installed on the AE Server.
**Procedure**

1. Login as `root` or `sroot` and type the following command:
   ```bash
   rpm -qa | grep krb
   ```
   If the Kerberos5 RPMs are installed, you will see output similar to the following:
   ```
   krb5-devel-1.6.1-70.el5_9.2
   pam_krb5-2.2.14-22.el5
   krb5-libs-1.6.1-70.el5_9.2
   krb5-workstation-1.6.1-70.el5_9.2
   ```

2. Download and install any missing Kerberos5 RPMs.

**Next steps**

Continue with the next procedure [Editing the Kerberos 5 configuration file on the AE Server](#) on page 195.

---

**Editing the Kerberos 5 configuration file on the AE Server**

**About this task**

This procedure is performed by an administrator on the AE Server.

After the Kerberos RPMs are properly installed, follow this procedure to edit the Kerberos 5 configuration file on AE Server (Kerberos 5 client):

**Procedure**

1. Log in as `root` or `sroot`, and type `cd /etc`.

2. With a text editor, open the `krb5.conf` file, for example: `vi krb5.conf`.

   The system displays the contents of `krb5.conf`.

3. Change the fields that are depicted in bold:

   ```
   [libdefaults]
   default_realm = dcservcer1.xyz.com
   dns_lookup_realm = true
   dns_lookup_kdc = true
   default_tkt_enctype = des-cbc-md5
   default_tgs_enctype = des-cbc-md5
   [realms]
   MNO.XYZ.COM = {
   kdc = dc-sername.dcservcer1.xyz.com:88
   kpasswd_server = dc-sername.dcservcer1.xyz.com:88
   [domain_realm]
   .xyz.com = MNO.XYZ.COM
   ```

4. Save your changes.

**Next steps**

Continue with the next procedure [Importing the keytab file on the AE Server](#) on page 196.
Importing the keytab file on the AE Server

About this task

This procedure is performed by an administrator on the AE Server.

After you configure the /etc/krb5.conf file, you must import the keytab file that was generated on the Windows Domain Controller (see Generating a keytab file for the AE Server account on the Domain Controller on page 194) to the AE Server.

Procedure

1. Log in as root or sroot.
2. From the command line, type /usr/kerberos/sbin/ktutil.
3. From the ktui prompt, type the following command to have the ktuility read in the keytab file.
   
rkt aeserver.keytab
   
   The ktuility reads in the keytab file, and upon completion, displays the ktutil prompt.
4. Type the following command to merge the imported key into the /etc/krb5.keytab file.
   
wkt /etc/krb5.keytab
5. Type q to exit ktutil.
6. From the command prompt, type kinit.

   This utility will obtain and cache the Kerberos ticket-granting ticket from the Domain Controller.

Next steps

Continue with the next procedure Changing from User Management Authentication to Active Directory Authentication on the AE Server on page 188.

Administering the time-out period for console and HTTP sessions

About this task

Use this procedure to specify the time-out period for the Linux console and HTTP sessions. When the time-out period is reached, the session expires.

Procedure

1. From the AE Services Management Console main menu, select Security > Session Timeouts.
2. In the Console Timeout field, enter the number of minutes at which the console session will expire. The range is 0 to 60 minutes. The default is 10 minutes. If you set this value to 0, the session will never expire.

3. In the HTTP Timeout field, enter the number of minutes at which the HTTP session will expire. The range is 0 to 60 minutes. The default is 10 minutes. If you set this value to 0, the session will never expire.

4. Click **Apply Changes**.

5. On the Apply changes to Session Timeouts page, click **Apply** to confirm your changes.
Chapter 9: Data Encryption

Note:

From Release 8.1.2, Application Enablement Services supports the file system data encryption feature with Release 8.1.2 OVA. The encryption can be enabled only at the time of deploying the AE Services 8.1.2 OVA. If you want to execute encryption commands, then you must deploy Release 8.1.2 OVA and then apply Release 8.1.2 patch.

With Release 8.1.2, you can enable or disable data encryption for Avaya Aura® applications at the time of deployment. Data Encryption is supported only for Appliance Virtualization Platform and VMware Virtualized Environment. Once you deploy the application with data encryption, you cannot disable data encryption after deployment.

By enabling Data Encryption, your Communication Product's certain Operational data and Log Files will be encrypted. You will be prompted to enter a passphrase that will be used to create or access an encryption key. You must remember the encryption passphrase, if not it can result in locking up the system. Secondly, you will be asked to configure the option for local key storage.

It is important to note that the encryption of the disk may have a performance impact. For further information, refer to the Avaya Product Administration guide(s). Before you select an encryption option, please read the Data Privacy Guideline so that you may better understand these options.

By disabling Data Encryption, your Communication Product's Operational data and Log Files will not be stored in encrypted partitions.

If encryption is enabled and the Require Encryption Pass-Phrase at Boot-Time check box is selected, you need to reenter the encryption passphrase whenever the application reboots.

During reboot, the application prompts you to enter the encryption passphrase on VM console at first boot and upon entering the correct encryption passphrase, the system mounts all the encrypted disks.

Note the following:

- If a common encryption passphrase is used for all the encrypted partitions, but an incorrect encryption passphrase is entered in first attempt, then you have to enter the correct encryption passphrase for every partition at least once.
- Multiple failures on encryption passphrase boots the system into the Maintenance/Emergency mode. To get the prompt again, you need to reboot the system.

If encryption is enabled and the Require Encryption Pass-Phrase at Boot-Time check box is not selected during OVA deployment, the application creates the Local Key Store and the system does not prompt you to type the encryption passphrase whenever the application reboots to mount the
encrypted disks. You can also set up the remote key server by using the `encryptionRemoteKey` command after the deployment of the application.

**Encryption of Application Enablement Services partitions**

When you enable data encryption for Application Enablement Services, the system encrypts the following partitions that have personal data.

- `/var/mvap/database`
- `/var/log`
- `/var/log/audit`
- `/var/lib/ldap`

---

**Remote Key Server**

When you enable data encryption for an application, you can set up remote key server. You can add multiple remote key servers. When you add a remote key server for the first time, the application disables the local key store. You can enable the local key store again after adding a remote key server. However, it is not recommended to enable local key store when the remote key server configuration exists.

If there is only one empty slot, then you cannot add a new remote key server or a new passphrase. The last empty slot is a “reserved” slot and you can use that only for changing the passphrase.

Application checks for the remote key server accessibility every 15 minutes. If any of the remote key server goes down, the application generates a Warning alarm. If all remote key servers are not accessible, then the application generates a Minor alarm.

---

**Data Encryption password policy**

The encryption passphrase must meet the following requirements:

- Must contain at least eight characters.
- Must contain at least one of each: an uppercase letter, a lowercase letter, a numerical, and a special character.

Ensure that you keep the encryption passphrase safe. You need the encryption passphrase later.

---

**Data encryption commands**

The following CLI commands are available to make changes to the Session Manager data encryption settings. For more details on administering data encryption, refer to *Administering Avaya Aura® Application Enablement Services*. 

Comments on this document? infodev@avaya.com
encryptionPassphrase command

Using the **encryptionPassphrase** command you can manage the encryption passphrase after deploying the application.

**Syntax**

```plaintext
encryptionPassphrase [add | change | remove | list]
```

- **add**
  Displays the prompts to add the encryption passphrase.
- **change**
  Displays the prompts to change the encryption passphrase.
- **remove**
  Removes the encryption passphrase.
- **list**
  Displays the encryption passphrase and slot assignment.

**Considerations**

You must deploy the application with data encryption.

**Adding encryption passphrase**

**About this task**

Use the **encryptionPassphrase add** command to add encryption passphrase.

You can add a maximum of seven encryption passphrases, if free slots are available.

**Procedure**

1. Log in to the application command line interface with administrator privileged credentials.
   - For Application Enablement Services, log in with root privileged credentials.
2. Type **encryptionPassphrase add**.
3. In **Enter existing passphrase**, type the encryption passphrase.
4. In **Enter new Passphrase**, type the new encryption passphrase.
5. In **Retype Passphrase**, retype the encryption passphrase.

**Changing encryption passphrase**

**About this task**

Use the **encryptionPassphrase change** command to change the existing encryption passphrase.
Procedure

1. Log in to the application command line interface with administrator privileged credentials.
   For Application Enablement Services, log in with root privileged credentials.

2. Type `encryptionPassphrase change`.

3. At the prompt, in **Current Passphrase**, type the encryption passphrase.

4. In **Enter new Passphrase**, type the new encryption passphrase.

5. In **Retype Passphrase**, retype the encryption passphrase.
   The application displays the following message.
   
   Passphrase successfully changed.

Displaying encryption passphrase and slot assignment

About this task

Use the `encryptionPassphrase list` command to list the slots assignment, encryption passphrase, and remote server details.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
   For Application Enablement Services, log in with root privileged credentials.

2. Type `encryptionPassphrase list`.

   The application displays the details based on the system configuration.

<table>
<thead>
<tr>
<th>Slot</th>
<th>Status</th>
<th>Passphrase/Remote Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Slot 0</td>
<td>ENABLED</td>
<td>Passphrase</td>
</tr>
<tr>
<td>Key Slot 1</td>
<td>ENABLED</td>
<td>Passphrase</td>
</tr>
<tr>
<td>Key Slot 2</td>
<td>ENABLED</td>
<td>Passphrase</td>
</tr>
<tr>
<td>Key Slot 3</td>
<td>ENABLED</td>
<td>Passphrase</td>
</tr>
<tr>
<td>Key Slot 4</td>
<td>ENABLED</td>
<td>Passphrase</td>
</tr>
<tr>
<td>Key Slot 5</td>
<td>Disabled</td>
<td>empty</td>
</tr>
<tr>
<td>Key Slot 6</td>
<td>Disabled</td>
<td>empty</td>
</tr>
<tr>
<td>Key Slot 7</td>
<td>Disabled</td>
<td>empty</td>
</tr>
</tbody>
</table>

Removing encryption passphrase

About this task

Use the `encryptionPassphrase remove` command to remove the existing encryption passphrase. You cannot remove all encryption passphrases, the application retains minimum one encryption passphrase.

If you attempt to delete the last encryption passphrase, the system displays the following message:

The last passphrase cannot be removed!
Procedure
1. Log in to the application command line interface with administrator privileged credentials. For Application Enablement Services, log in with root privileged credentials.
2. Type `encryptionPassphrase remove`.
3. At the prompt, in Passphrase to remove, type the existing encryption passphrase. The application displays the following message.
   Passphrase successfully removed.

---

encryptionRemoteKey command
Using the `encryptionRemoteKey` command you can manage the remote key server after deploying the application.

Syntax
```
encryptionRemoteKey [add | remove | list]
```
- **add** Displays the prompts to add the remote key server.
- **remove** Removes the remote key server.
- **list** Displays the remote key server and slot assignment.

Considerations
You must deploy the application with data encryption.

---

Adding remote key server

Before you begin
Ensure that the remote key server is configured and accessible.

Procedure
1. Log in to the application command line interface with administrator privileged credentials. For Application Enablement Services, log in with root privileged credentials.
2. Type `encryptionRemoteKey add <Address> <Port>`.
   Where:
   - **Address** is the IP address or FQDN of the remote key server.
Port is the port number of the remote key server. If you do not enter the port number the application uses the value of default port as 80.

3. In Enter existing passphrase, type the existing encryption passphrase.
   If the remote key server is not configured, the application displays the following message:
   Remote key server not found
   If the remote key server is configured, the application adds the remote key server. When you add a remote key server for the first time, the application disables the local key store.

Removing remote key server

About this task
Use the encryptionRemoteKey remove command to remove the existing remote key server.

Procedure
1. Log in to the application command line interface with administrator privileged credentials.
   For Application Enablement Services, log in with root privileged credentials.
2. Type encryptionRemoteKey remove <Address>.
   Where:
   Address is the IP address or FQDN of the remote key server.
   You must use the same IP address or FQDN value that you used to add the remote key server.
3. In Passphrase, type the existing encryption passphrase.
   The application removes the remote key server and displays the following message:
   RemoteKey successfully removed.

Displaying remote key server and slot assignment

About this task
Use the encryptionRemoteKey list command to list the slots assignment, encryption passphrase, and remote server details.

Procedure
1. Log in to the application command line interface with administrator privileged credentials.
   For Application Enablement Services, log in with root privileged credentials.
2. Type encryptionRemoteKey list.
The application displays the details based on the system configuration.

<table>
<thead>
<tr>
<th>Slot</th>
<th>Status</th>
<th>Passphrase/Remote Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Slot 0:</td>
<td>ENABLED</td>
<td>Passphrase</td>
</tr>
<tr>
<td>Key Slot 1:</td>
<td>ENABLED</td>
<td>&lt;IP Address of Remote Key Server&gt;</td>
</tr>
<tr>
<td>Key Slot 2:</td>
<td>ENABLED</td>
<td>Passphrase</td>
</tr>
<tr>
<td>Key Slot 3:</td>
<td>DISABLED</td>
<td>empty</td>
</tr>
<tr>
<td>Key Slot 4:</td>
<td>DISABLED</td>
<td>empty</td>
</tr>
<tr>
<td>Key Slot 5:</td>
<td>DISABLED</td>
<td>empty</td>
</tr>
<tr>
<td>Key Slot 6:</td>
<td>DISABLED</td>
<td>empty</td>
</tr>
<tr>
<td>Key Slot 7:</td>
<td>DISABLED</td>
<td>empty</td>
</tr>
</tbody>
</table>

---

**encryptionLocalKey command**

Using the `encryptionLocalKey` command you can enable or disable the local key store after deploying the application with data encryption.

**Syntax**

`encryptionLocalKey [enable | disable]`

**enable**

Enables the local key store.

**disable**

Disables the local key store.

**Considerations**

You must deploy the application with data encryption.

---

**Enabling local key store**

**About this task**

Use the `encryptionLocalKey enable` command to enable the local key store.

**Procedure**

1. Log in to the application command line interface with administrator privileged credentials.
   For Application Enablement Services, log in with root privileged credentials.
2. Type `encryptionLocalKey enable`.
3. At the prompt, in **Enter existing passphrase**, type the existing encryption passphrase.
   If the local key store is already enabled, the application displays the following message.
   
   Local key store is already enabled.
Disabling local key store

About this task

Use the `encryptionLocalKey disable` command to disable the local key store.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
   For Application Enablement Services, log in with root privileged credentials.
2. Type `encryptionLocalKey disable`.
   The application displays the following message.
   Local keystore removed
   Local Key Store is now disabled.

Viewing data encryption status

About this task

The `encryptionStatus` command displays information about encryption on the system.

Procedure

1. Log in to the application command line interface with administrator privileged credentials.
   For Application Enablement Services, log in with root privileged credentials.
2. Type `encryptionStatus`.
3. When the system prompts, type the password.
   For example, if the local key store is configured, the system displays the following status:
   ```
   Data Encryption: enabled
   Local Key Store: enabled
   Encryption Passphrase Required at Boot-time: no
   ```
   For example, if the remote key server is configured, the system displays the following status:
   ```
   Data Encryption: enabled
   Local Key Store: disabled
   Encryption Passphrase Required at Boot-time: yes
   remoteKeyServers: <remoteServer1: <remoteServerIPAddress> accessible>
   ```
Chapter 10: Fault Tolerance Configuration

Fault Tolerance

VMware Fault Tolerance provides continuous availability for virtual machines by creating and maintaining a secondary virtual machine that is identical to, and continuously available to replace the primary virtual machine in the event of a failover situation.

You can enable Fault Tolerance for the most critical virtual machines. A secondary virtual machine is created and runs in virtual lockstep with the primary virtual machine. VMware vLockstep captures inputs and events that occur on the primary virtual machine and sends them to the secondary virtual machine, which is running on another host. Using this information, the secondary virtual machine runs similar to that of the primary virtual machine. Because the secondary virtual machine is in virtual lockstep with the primary virtual machine, it can take over execution at any point without interruption, by providing fault tolerant protection.

Fault Tolerance Configuration Checklist

Use the following checklist to complete fault tolerance configuration:

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enable host certificate checking if you are upgrading from a previous version of vCenter server.</td>
<td>See, VMware documentation.</td>
</tr>
<tr>
<td>2</td>
<td>Configure networking for each host.</td>
<td>See, VMware documentation.</td>
</tr>
<tr>
<td>3</td>
<td>Create the VMware HA cluster, add hosts, and check compliance.</td>
<td>See, VMware documentation.</td>
</tr>
<tr>
<td>4</td>
<td>Enable fault tolerance.</td>
<td>See, Enabling Fault Tolerance on page 207</td>
</tr>
</tbody>
</table>
Enabling Fault Tolerance

About this task
Use this procedure to enable fault tolerance for virtual machines using the vSphere Client.

Before you begin
Ensure that you meet the following prerequisites:

- The two servers with the same hardware configuration must meet the VMware Fault Tolerance prerequisites.
- Locate the two servers, for example, two Dell R620 servers in the same rack.
- Install ESXi of the same version, vCenter Server, and vCenter Client on both the servers.
- Create a cluster and add two servers into the cluster.

For more information on installing VMware, vCenter Server, vCenter Client, creating a cluster, and adding servers to a cluster, see the VMware documentation.

Procedure
1. Connect vSphere Client to vCenter Server using administrator credentials.
2. On the vSphere Client, click the Hosts & Clusters view.
3. Right-click the single virtual machine, and click Fault Tolerance > Turn on Fault Tolerance.

You must enable the Fault Tolerance for one virtual machine at a time.

After the Fault Tolerance is on, the selected virtual machine acts as a primary virtual machine and secondary virtual machine is established on the another host.

Configuring Fault Tolerance on AE Services virtual machine

About this task
Use this procedure to configure fault tolerance on AE Services virtual machine.

Before you begin
Deploy AE Services profile 1 on the Server 1. For more information, see Deploying Avaya Aura® Application Enablement Services in Virtualized Environment

Procedure
1. Log in to the AE Services Management Console.
2. Select and right-click the AE Services virtual machine, and click Fault Tolerance > Turn On Fault Tolerance.
Fault Tolerance Configuration

3. After the Fault Tolerance is enabled, click **Fault Tolerance > Test Failover**.
Chapter 11: Security Database

The Security Database

The Application Enablement Services (AE Services) Security Database (SDB) provides the ability to control a user’s access privileges. The SDB stores information about Computer Telephony (CT) users and the devices they control. The DMCC service, the TSAPI service, and Telephony Web Services use this information for permission checking.

For an application to take advantage of the SDB, its users must be added to the AE Services User Management service as CT users, regardless of how users are authenticated. For example if you authenticate your DMCC users using the Active Directory Services, you must still add those users to the AE Services User Management service as CT users. By administering them as CT users, they are members of the SDB. See Adding a user to User Management on page 139.

APIs that use the Security Database

The following AE Services Application Programming Interfaces (APIs) use the Security Database for determining users’ access privileges.

⚠️ Important:

APIs that need to use the features of the security database must ensure that the SDB is enabled.

• TSAPI, JTAPI, and Telephony Web Service — see Enabling the Security Database - TSAPI, JTAPI, and Telephony Web Service on page 209.
• Device, Media, and Call Control (DMCC) — see Enabling the SDB for DMCC applications on page 211.

Enabling the Security Database - TSAPI, JTAPI, and Telephony Web Service

Procedure

1. From the AE Services Management Console main menu, select Security > Security Database > Control.

Comments on this document? infodev@avaya.com
2. From the SDB Control for DMCC, TSAPI, JTAPI, and Telephony Web Services page, select the check box for Enable SDB for TSAPI Service, JTAPI and Telephony Web Services (by default it is not selected).

3. Click Apply Changes.

4. Select Maintenance > Service Controller.

5. From the Service Controller page, select the check box for the TSAPI Service.

6. Click Restart Service.

7. From the Restart Service page, click Restart.

---

**DMCC applications and SDB authorization**

This section provides recommendations for DMCC applications that use the SDB for authorization. The procedure for enabling the SDB is described in [Enabling the SDB for DMCC applications](#) on page 211.

**Note:**

DMCC applications can use enterprise, or LDAP-based, authorization as an alternative to SDB authorization. For more information, see [Enterprise directory user authorization policy for DMCC applications](#) on page 187.

**DMCC device services**

For the DMCC API, you must enable the SDB if your applications use SDB authorization to take advantage of the DMCC device services enhancements introduced with AE Services 4.1. These enhancements allow a DMCC application to do the following:

- Get a list of the devices that are associated with a session
- Transfer a group of devices from one session to another session
- Share the control of a group of devices among multiple sessions

**DMCC session services**

Although DMCC session services will work with a disabled SDB, AE Services recommends that you enable it for security reasons.

**DMCC applications developed prior to AE Services 4.1**

If you are administering AE Services for DMCC applications that were developed prior to AE Services 4.1, you must retain the default setting and keep the SDB disabled.
Enabling the SDB for DMCC applications

About this task

Follow these steps to enable the SDB for DMCC applications that use the DMCC device series enhancements. This procedure is performed by a System Administrator from the AE Server.

**Note:**

When you change the SDB Control settings you must restart the affected service.

Procedure

1. From the AE Services Management Console main menu, select Security > Security Database > Control.
2. From the SDB Control for DMCC, TSAPI, JTAPI, and Telephony Web Services page, select the check box for Enable SDB for DMCC Service.
3. Click Apply Changes.
4. Select Maintenance > Service Controller.
5. From the Service Controller page, select the check box for the DMCC Service.
6. Click Restart Service.
7. From the Restart Service page, click Restart.

TSAPI properties

The TSAPI properties in the AE Services Management Console apply globally to the SDB. If you plan to assign worktops to each user and use the settings in the SDB to effect permission levels, it is recommended that you use the default TSAPI properties.

**Note:**

If you are administering DMCC applications to use the SDB, you do not have to administer the TSAPI properties.

The following list summarizes the TSAPI properties settings.

- **TCP Preferred Naming Format** — By default, this field is set to IP Address. You have the option of setting it to Host Name. This setting determines whether Auto Admin of LAN Addresses will use Host Names or IP addresses. This setting also determines the name of the field label that appears on the Add/Edit Worktop page.

- **Extended Worktop Access** — By default, this setting is disabled. This is a system-wide feature that affects all users. If you enable it, a CTI User can log in at any worktop and control...
all the devices on that worktop. For more information, see Extended worktop access on page 214.

- If you want most of your CTI users to be restricted to the devices assigned to their worktops, you would not enable this feature.

- If you have users who need additional access, you can use a permission scheme based on User Access Rights. For more information, see Sample SDB Administration scenario - setting up a permission scheme based on access rights on page 222.

• Auto Admin of LAN Addresses — By default, this setting is disabled. This means that you must administer an IP address (or Host Name) for each worktop.

- If your AE Services TSAPI configuration consists of a significant number of users, you can enable this setting, and AE Services will automatically add LAN addresses for all worktops. (The LAN address is either a host name or IP address, depending on what you selected for TCP Preferred Naming Format.)

- If you enable this setting, you can still override it on a per-worktop basis by typing an IP address (or host name) in the IP Address field on the Add/Edit Worktop page.

• Advanced Settings — Clicking this button enables you to administer the following TSAPI advanced settings:
  - TCP Send Wait Time
  - TCP Send Retries
  - Persistent AAOs
  - Persistent AAO Audit Interval
  - Persistent AAO Maximum Age
  - TSAP Service Advertising Mode (Advertise all Tlinks or Advertise only those Tlinks that are currently in service)

---

**Configuring TSAPI Properties**

**Procedure**

1. On Application Enablement Services Management Console, go to AE Services > TSAPI > TSAPI Properties.

2. On the TSAPI Properties page, in the TCP Preferred Naming Format field, select one of the following:
   - **IP Address** if your configuration uses fixed IP addresses for your clients.
   - **Host Name** if your configuration uses Dynamic Host Control Protocol or if the IP addresses of your clients frequently change.

3. In the Extended Worktop Access field, do one of the following:
   - Select the Extended Worktop Access check box if you want a CTI user to be able to log in to any worktop and control all the devices on that worktop.
• Clear the **Extended Worktop Access** check box if do not want to allow Extended Worktop Access.

4. In the **Auto Admin of LAN Addresses** field, do one of the following:
   • Select the **Auto Admin of LAN Addresses** check box if you want AE Services to automatically add LAN addresses for all worktops.
   • Clear the **Auto Admin of LAN Addresses** check box if do not want to allow Auto Admin of LAN Addresses.

5. Click **Apply Changes**.

6. On the Apply Changes to TSAPI Configuration Properties page, click **Apply**.

7. Restart the TSAPI Service for the changes to take effect. To restart the TSAPI Service do the following:
   a. On Application Enablement Services Management Console, go to **Maintenance > Service Controller**.
   b. On the Service Controller page, select **TSAPI Service**.
   c. Click **Restart Service**. The TSAPI service has successfully restarted when the Controller Status displays **Running**.

---

**About granting additional permissions**

The SDB provides you with the following ways to grant permissions to users.

⚠️ **Note:**

In the context of this chapter, the term user does not necessarily refer to a person. It can be an application that logs into the TSAPI service with its own login and password.

• Assign a worktop to a user. This is a typical method of assigning permissions to a user. By default a user assigned to a worktop has permission to access only the devices associated with that worktop for the following types of requests:
  - Call Origination and Termination
  - Device/Device monitoring requests

• Administer access rights for a user. The following access rights settings provide permission to access specific devices for each of the following types of requests.
  - Call Origination/Termination and Device Status
  - Device Monitoring
  - Call On A Device Monitoring
  - Call Monitoring
For a description of these access rights settings, see [Access Rights options](#) on page 214.

• Enable the **Extended Worktop Access** check box on the TS Configuration page. This allows users to roam to other worktops. For example, when a user logs in to another user’s workstation, the TSAPI service checks the Security Database for a worktop with the same LAN address as the workstation where the user is attempting to log in. If a match is found, the user is given Call Origination and Termination permissions and Device/Device monitoring permissions for any of the devices associated with that worktop.

**Extended worktop access**

Users can always control all the devices on their worktop and in their own call control Access Rights device group. Extended Worktop Access is a Security Database-wide administration setting that affects all users. This setting applies primarily to the contact center environment, where it is likely for users to move from one desktop to another. If this setting is enabled, a user can log in from any worktop and control the devices on that worktop.

**Note:**

LAN address information is used when the Extended Worktop Access setting is enabled. It enables the TSAPI service to determine from which worktop the user is logged in and which devices are associated with that worktop.

**If extended worktop access is disabled**

If the Extended Worktop Access setting is disabled, a user can control only the following devices:

• Primary device on the worktop
• Any device in the secondary device group associated with the worktop
• Any device in the call control Access Rights group

If a user logs in from another worktop while this option is disabled, the user cannot control the devices on that worktop. The user can still control the devices on his or her worktop and the devices in his or her call control Access Rights. See [Access Rights options](#) on page 214.

If most users should be restricted to the devices associated with their assigned worktop but specific users must control other devices, you can still disable the Extended Worktop Access feature. You can use user level access rights to allow these users to control additional devices. See [Sample SDB Administration scenario - setting up a permission scheme based on access rights](#) on page 222.

**Access Rights options**

For users who need additional access, you can use the following user level Access Rights permissions settings. Even with the Extended Worktop Access system option disabled, these users will be able to control the necessary devices. For settings that apply to these options, see [CTI Users](#) on page 221.

• **Call Origination and Termination**
Call Origination and Termination permissions include any operation that the user could perform manually, using their telephone. The user (or application) can originate calls and activate features such as call forwarding, call transfer, and so on. By default, all users have this permission for the devices associated with their worktop.

- **Device/Device Monitoring**

An application places a Device/Device monitor on a specific device so it can receive an event report any time an event occurs at that device. For example, if the device receives an incoming call or originates an outgoing call, the application receives an event report. Device/Device monitors are the most commonly used monitor. By default, all users have this permission for the devices associated with their worktop.

- **Call/Device Monitoring**

Call/Device monitors are placed to track events for a call once it reaches the device being monitored. Unlike Device/Device monitors, events for a call continue to be received even after the call leaves the device. A common usage of this monitor is to place it on the extension that incoming calls to a call center reach before being distributed to an agent. Once the call reaches this first extension, all further events (such as transfers to queues and disconnects) are sent to the application that requested the monitor. This type of monitor is commonly used by applications that track the efficiency of a call center operation. Supervisors may use this type of application to decide how to best allocate inbound call agents.

- **Call/Call Monitoring**

Call/Call monitors work differently from the device and call/device monitors previously mentioned. Those monitors are based on a device ID. Call/Call monitors are tracked based on a call ID (a unique identifier of the call being handled by Communication Manager). Users either have or do not have this permission; you do not need to create a device group for these Access Rights.

- **Routing**

When a routing application is started, it sends route registration requests to Communication Manager. Each request contains a device ID. This instructs Communication Manager to send all incoming calls for these devices to the TSAPI Service (and then on to the application) for routing. Communication Manager does not route these calls. Before the route registration request is passed to Communication Manager, the TSAPI Service checks that the user (in this case, the routing application) has permission to route calls for this device.

### Security Database objects

All the information that Telephony Services needs for routing messages and controlling access to the telephony network is stored in the Security Database in terms of the following objects.
**Note:**
If you are adding many new objects to the SDB, you may want to group the objects by object type and add them in the following order:

- **Tlinks** — Tlinks are created dynamically by the TSAPI service; you can not add them manually.
- **Tlink groups**
- **Devices**
- **Device groups**
- **Worktops**
- **Users**

### Tlinks

TSAPI links (Tlinks) are service identifiers (names) dynamically created by the TSAPI service. You can not manually add a Tlink group to the SDB.

The format of a Tlink name is as follows:

\[ \text{AVAYA}\#\text{switch\_connection\_name}\#\text{service\_type}\#\text{AE\_server\_name} \]

**where:**

- **AVAYA** is a fixed constant.
- **switch\_connection\_name** represents the switch connection name. You determine the switch connection name when you administer a switch connection in the AE Services Management Console, and the TSAPI service, in turn, gets the information from the database.
- **service\_type** refers to the CSTA service type. It can be either of the following:
  - CSTA — if you have administered the TSAPI link as unencrypted (nonsecure)
  - CSTA-S — If you have administered the TSAPI link as encrypted (secure)
- **AE\_server\_name** represents the AE Server name. The AE Server name is assigned by the person who performs the AE Services installation. The TSAPI service gets this information from the operating system.

An example of a Tlink name is as follows:

\[ \text{AVAYA}\#\text{CM1}\#\text{CSTA-S}\#\text{AESRV1} \]

### Tlink groups

A Tlink group is a name you assign to one or more Tlinks. If you have more than one switch, you can use Tlink groups to control access to a specific set of Tlinks (or switch connections).

When you associate a device with a Tlink group, a user can issue call control requests only for the device on a Tlink in the Tlink group.

If you do not need to restrict access to a specific switch connection, you can assign the default Tlink group, **Any**, to all devices as you add them to the SDB.
How Tlinks and Tlink groups are used

The TSAPI service uses Tlinks and Tlink groups to advertise (to clients) which switch connection or set of switch connections it supports. When a user starts an application at a client workstation, the application specifies which Tlink it should use. It may present a list of Tlinks to the user and prompt the user for a choice, or it may get the correct Tlink from an initialization file. The application then includes this Tlink in the request to establish a connection.

When the TSAPI service receives the establish connection request, it saves the Tlink name. Future application requests to control devices using this Tlink are checked by the TSAPI service. If the device can be accessed by this Tlink, the request goes through. If not, the request is rejected.

If you need this type of checking just described, you need to create groups of Tlinks. Each group is called a Tlink group. You then associate a particular Tlink group with each device, thus limiting access to the device to the Tlinks that are in that group. The following topics provide examples of how Tlink groups are used.

Tlink groups - a way to associate devices with a Switch Connection

The SDB lets you use Tlink groups as a way to associate devices with a particular switch connection (which represents a switch).

You can associate a group of devices to a Tlink group. This has two advantages:

- You know, by looking at the device object, which switch the device is associated with.
- If a user inadvertently selects the wrong Tlink when opening a connection, the TSAPI service returns an error immediately indicating that the Tlink cannot control the device. If this control were not in place, the request would be forwarded all the way to Communication Manager before the error could be detected.

Adding a Tlink group

About this task

The TSAPI service creates the default Tlink group, Any.

Procedure

1. From the AE Services Management Console main menu, select Security > Security Database > Tlink Groups.
2. On the Tlink Groups page, in the TLink Groups field, type the name that you want to assign to the Tlink group (for example newgroupA).
3. Click Add Tlink Group.
4. On the Add/Edit Tlink Group page, select the TLink(s) you want to add to this group.
5. Click Apply Changes.
6. On the Apply Changes to Tlink Group Properties page, click Apply.

Next steps

Continue with the procedure Adding a device to the SDB on page 218.
Devices

A device can be a telephone, a fax machine, a modem, an ACD, a VDN, or an agent ID that Communication Manager controls.

Devices can be associated with Tlink groups. Tlink groups are useful when you have a configuration that supports more than one switch connection. Tlink group names allow you to associate a device with a switch connection. For more information, see Sample SDB Administration scenario - setting up a permission scheme based on access rights on page 222.

For a sample procedure that depicts adding a device to the SDB, see Adding a Device to the SDB on page 218.

Adding a device to the SDB

Procedure

1. From the AE Services Management Console main menu, select Security > Security Database > Devices.
2. On the Devices page, in the Add Device field, type the extension number for a specific device, for example 7788.
3. Click Add Device.
4. Complete the Add/Edit Device page, as follows:
   a. In the Location field, type a location name, for example metro. (This field is optional).
   b. In the Device Type field, select the appropriate device type, for example PHONE.
   c. In the Tlink Group field, select the appropriate Tlink group, for example newgroupA. (The default is Any).
   d. Click Apply Changes.
5. On the Apply Changes to Device Properties page, click Apply.

Device groups

A device group refers to the name of a group and the devices that make up the group. A device group can refer to:

- A group of devices in a call center or help desk operation. In this environment, an application would
  - provide call routing for this device group
  - track incoming call statistics
- A device controlled by a user such as a fax or modem

A device group can be assigned to either a user or a worktop.

- You assign a device group to a user when you want to provide the user with permissions for controlling specific devices as well as assigning the type of control that the user can exert. This type of control is called Access Rights.
• Device groups are used in the worktop object to indicate resources that are shared among the worktop objects that contain the device group.

• A device group can be treated as an exception group. If the group is designated as an exception group, the TSAPI service treats the entire group as if it contained every device except for those devices in the device group.

Adding a device group

Procedure

1. From the AE Services Management Console main menu, select Security > Security Database > Device Groups.

2. On the Device Groups page, in the Add Device Group field, type the name of the device group you want to use, for example metrophone.

3. Click Add Device Group.

4. Complete the Add/Edit Device Group page as follows:
   a. Leave the Exception Group check box blank (the default setting).
   b. From the Device list, select the devices you want to include in this device group.
   c. Click Apply Changes.

5. On the Apply Changes to Device Group Properties page, click Apply.

Worktops

A worktop refers to a collection of devices. It can consist of a telephone (the primary device) and additional telephony devices, such as fax machines or modems (secondary devices). It is an abstraction of a user’s desktop devices. As such, the worktop associates the user’s workstation (computer) with the user’s telephone and any other telephony devices.

• Worktops are identified by a name and a TCP/IP network address (or a host name).

• Users can always control and monitor all the devices associated with their worktop, even if they are logged in from a different worktop.

• More than one user can be assigned to a worktop. For example, if your organization runs three shifts, and you want three different users to use the same worktop on a per-shift basis, you would assign all three users to the same worktop.

You can add a worktop manually or import multiple worktops from a .CSV file.

See Adding a Worktop on page 219 for more information.

Adding a worktop

Procedure

1. From the AE Services Management Console main menu, select Security > Security Database > Worktops.

2. From the Worktops page, in the Add Worktop field, type the name of the worktop you want to use, for example sgreen.
3. Click Add Worktop.
4. Complete the Add/Edit Worktop page as follows:
   a. In the **Primary Device ID** field, type the appropriate device ID for the worktop, for example 7788.
   b. In the **Secondary Device Group** field, select the appropriate device group, for example metrophone.
   c. In the **IP Address (or Host Name)** field, type the IP address (or Host Name) of the computer designated as the worktop.
   d. Click **Apply Changes**.
5. In the **Apply Changes to Worktop Properties** page, click **Apply**.

**Importing multiple worktops from a .CSV file**

**Before you begin**

To import multiple worktops from a .CSV file, you must have a .CSV file that contains information for each worktop in the following format: `worktop_name, ip_address, hostname, secondary_device_id, primary_device_id` where:

- **worktop_name**: This field must be numeric and should not be assigned to an existing worktop. This field cannot be null.
- **ip_address**: This field can be either null or a properly formatted IP address.
- **hostname**: This field can be either null or a resolvable hostname.
- **secondary_device_id**: This field should contain one of the following values:
  - **ANY**
  - **NONE**: This field cannot be null.
- **primary_device_id**: The value of this field must be equal to the “device_id” of an existing device. This field cannot be null.

**Procedure**

1. From the AE Services Management Console main menu, select **Security > Security Database > Worktops**.
2. From the Worktops page, click **Browse**.
3. From the Choose File to Upload dialog box, select the .CSV file that contains the information for the worktops you want to import, and then click **Open**.
   The path and file name of the .CSV file are displayed in the Upload worktops from file box.
4. Click **Upload**.
   The worktops and their associated information appear on the Worktops page.
CTI Users

A CTI user is a person (or an application) administered as a CT user in the AE Services User Management database who logs in and uses the TSAPI service. The settings in the TSAPI service Security Database determine what the user is allowed to do.

*Note:*

You cannot add or create users in the Security Database. You must use the User Management service to add or create users. For more information see Adding a user to User Management on page 139.

See Administering CTI User settings on page 221 for more information.

Administering CTI user settings

About this task

You cannot add or create users in the Security Database. You must use the User Management service to add or create users. For more information see Adding a user to User Management on page 139.

Procedure

1. From the AE Services Management Console main menu, select Security > Security Database > CTI Users > List All Users.
2. From the CTI Users page, select S. Green (the name of the worktop you created in Adding a worktop on page 219).
3. Click Edit.
4. Complete the Edit CTI User page as follows:
   a. In the Worktop Name field, select sgreen.
   b. Do not change the setting for Unrestricted Access. It is disabled by default (the button labeled Enabled puts unrestricted access into effect).
   c. In the Call Origination/Termination and Device Status field, select an appropriate device group, for example metrophone.
   d. In the Device Monitoring field, select an appropriate device group, for example metrophone.
   e. In the Calls On A Device field, select an appropriate device group, for example metrophone.
   f. In the Call Monitoring field, leave the check box unchecked.
   g. In the Allow Routing on Listed Device field, select an appropriate device group, for example metrophone.
5. Click Apply Changes.
6. In the Apply Changes to CTI User Properties page, click Apply.
Changes to User Permissions

If you make changes to a user’s permissions, the user must close any active applications and restart them before the changes take effect. This is because user permission information is saved in memory when the user’s application first opens a connection to the TSAPI Service. Any subsequent changes to the SDB are not reflected in the saved information.

Sample SDB Administration scenario - setting up a permission scheme based on access rights

About this task

If you have users who need additional access you can use a permission scheme (a simple hierarchy) based on User Access Rights. Here is an example that demonstrates how to administer different permission levels for different users, and allow one user greater access than others. This example achieves this by using the Access Rights settings at the user level (see Access Rights options on page 214).

Note:

Because this sample scenario assumes that you already have CTI users, and it does not include adding devices, it presents tasks in a different order than described in Security Database objects on page 215.

Initial settings for the sample help desk group

About this task

Assume that you have four CTI users (Edward, Michael, Sue, and Tom), who are initially administered with default profiles. From the AE Services Management Console main menu, if you were to select Security > Security Database > CTI Users > List All Users, and then select a user from the CTI Users page, the settings on the Edit CTI User page (for each user) would be identical except for the User ID and Common Name.

Access privileges for members of the help desk

Next, assume that you want to set up a simple help desk function for a supervisor (Edward) and the group of people he manages (Michael, Sue, and Tom).

You want Edward to be able to make calls and to receive calls from any of the phones in the help desk group, and you want him to be able to monitor and track calls associated with each of these phones.

You want Michael, Sue, and Tom to be able to use only the phones on their desktops.

Sample - creating a worktop for each user

About this task

The first procedure in this implementation scenario is to create a worktop for each user. Since the procedure is the same for each user, this example will depict setting up Edward’s worktop.
Procedure

1. From the AE Services Management Console main menu, select Security > Security Database > Worktops.
2. On the Worktops page, in the Add Worktop field, type Edward’s Wktp.
3. Click Add Worktop.
4. Complete the Add/Edit Worktop page as follows:
   a. In the Primary Device ID field, type 14088.
   b. Leave the Host Name (or IP Address) field as is (assume that Auto Admin of LAN Addresses is in effect).
   c. Click Apply Changes.
5. In the Apply Changes to Worktop Properties page, click Apply.
6. Repeat this procedure, for Michael, Sue, and Tom. Keep in mind that each user will have a different worktop name (Michael’s Wktp, Sue’s Wktp, and Tom’s Wktp) and a different Primary Device ID. (Michael’s Primary Device ID is 14124; Sue’s Primary Device ID is 14127, and Tom’s Primary Device ID is 14138).

Sample - creating a device group called help desk

About this task

The next procedure in this implementation scenario is to create a Device Group called HELP DESK.

Procedure

2. On the Device Groups page, type HELP DESK.
3. Click Add Device Group.
4. Complete the Add/Edit Device Group page, as follows:
   a. Leave the Exception Group check box unchecked.
   b. From the list of devices, select the following check boxes.
      • 14088 (Edward’s Primary Device ID)
      • 14124 (Michael’s Primary Device ID)
      • 14127 (Sue’s Primary Device ID)
      • 14138 (Tom’s Primary Device ID)
   c. Click Apply Changes.
5. On the Apply Changes to Device Group Properties page, click Apply.
Sample - administering Edward’s user profile with greater privileges

About this task
The next procedure in this implementation scenario is to administer Edward’s user profile with greater privileges. Recall that you want Edward to be able to make calls and to receive calls from any of the phones in the Help Desk group, and you want him to be able to monitor and track calls from each of their phones.

Procedure
1. From the AE Services Management Console main menu, select Security > Security Database > CTI Users > List All Users.
2. On the CTI Users page, select Edward.
3. Click Edit.
4. Complete the Edit CTI User page (for User ID Edward), as follows:
   a. In the Call Origination and Termination field, select HELP DESK. (This lets Edward make calls and receive calls from any of the phones in the Help Desk group).
   b. In the Device/Device field, select HELP DESK. (This lets Edward monitor calls that arrive at any of the phones in the Help Desk device group).
   c. In the Call/Device field, select HELP DESK. (This lets Edward track calls that are transferred to any of the phones in the Help Desk device group).
   d. Leave the check box for Call/Call unchecked.
   e. In the Allow Routing on Listed Device field, accept the default (None).
   f. Click Apply Changes.
5. In the Apply changes to CTI User Properties page, click Apply.

Sample - verifying the settings of the help desk

About this task
The last procedure is to verify the administration of the help desk you just put into effect.

Procedure
1. From the AE Services Management Console main menu, select Security > Security Database > Worktops.
2. On the Worktops page, click the heading Device Group to sort the listings in the device group column.
3. Verify that the Device Group lists HELP DESK as the Device Group for the Worktop name Edward’s Wktp (Device ID 14088).
Sample Configurations

This section describes operations at a fictional organization, the ACME company. It is a mail order company that sells seeds and garden equipment. Each of the following sections explores part of the operation and describes the administration required to implement it.

The ACME corporation has disabled the “Extended Worktop Access” feature. This limits each user to their own worktop, but as you will see, some users are given permission to monitor other devices or control calls at those devices. This is accomplished by creating device groups for these devices and associating those groups with each user.

Note:

The type of permissions you need to give each user depends on the applications that the user is running. Before you assign permissions, check your applications to see what permissions they require to work properly.

Access privileges

The ACME corporation has two inbound call groups: one group handles calls for the seed catalog and the second group handles calls for the tools catalog. Members of each group have their own desks and do not run TSAPI Service applications from any desk other than their own.

The basic permissions granted to a user are enough for these users, even with the “Extended Worktop Access” option disabled.

Table 1: Basic Permissions — Worktop Administration

<table>
<thead>
<tr>
<th>Worktop Name</th>
<th>Device ID</th>
<th>Secondary Device Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tools1</td>
<td>7701</td>
<td>Not applicable (N/A)</td>
</tr>
<tr>
<td>Tools2</td>
<td>7702</td>
<td>N/A</td>
</tr>
<tr>
<td>Seeds1</td>
<td>7711</td>
<td>N/A</td>
</tr>
<tr>
<td>Seeds2</td>
<td>7712</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table 2: Basic Permissions — User Administration

<table>
<thead>
<tr>
<th>User ID</th>
<th>Worktop Name</th>
<th>Call Orig&amp;Term</th>
<th>Device/Device Monitor</th>
<th>Call/Device Monitor</th>
<th>Routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Michael</td>
<td>Tools1</td>
<td>Not applicable (N/A)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Sally</td>
<td>Tools2</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Juan</td>
<td>Seeds1</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Marie</td>
<td>Seeds2</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Manager/Assistant Configuration

ACME has a president, two vice presidents, and a single assistant who handles all incoming calls to the executives (the president and vice presidents). The president and vice presidents handle only their own phones.

Since the president and vice presidents use only the phones at their desks, you do not need to grant additional access to these users. However, in order for their assistant to be able to control and monitor their phones, you must create a device group containing the device IDs of their telephones and assign this group to the assistant.

The following tables summarize the types of administration you can set up.

Table 3: Manager/Assistant — Device Group Administration

<table>
<thead>
<tr>
<th>Device Group Name</th>
<th>Device IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC LIST</td>
<td>7911, 7912, 7913</td>
</tr>
</tbody>
</table>

Table 4: Manager/Assistant — Worktop Administration

<table>
<thead>
<tr>
<th>Worktop Name</th>
<th>Device ID</th>
<th>Secondary Device Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRESIDENT WKTP</td>
<td>7911</td>
<td>Not applicable (N/A)</td>
</tr>
<tr>
<td>VP WKTP1</td>
<td>7912</td>
<td>N/A</td>
</tr>
<tr>
<td>VP WKTP2</td>
<td>7913</td>
<td>N/A</td>
</tr>
<tr>
<td>ASSISTANT WKTP</td>
<td>7914</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table 5: Manager/Assistant — User Administration

<table>
<thead>
<tr>
<th>User ID</th>
<th>Worktop Name</th>
<th>Call Orig&amp;Term</th>
<th>Device Monitoring</th>
<th>Call/Device Monitoring</th>
<th>Routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>President</td>
<td>PRESIDENT WKTP</td>
<td>Not applicable (N/A)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>VP1</td>
<td>VP WKTP1</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>VP2</td>
<td>VP WKTP2</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Exec Assistant</td>
<td>ASSISTANT WKTP</td>
<td>EXEC LIST</td>
<td>EXEC LIST</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

You can get the same results as the above example by assigning the EXEC LIST to the secondary device group on the assistant’s worktop.

Table 6: Manager/Assistant — Assistant Worktop Administration

<table>
<thead>
<tr>
<th>Worktop Name</th>
<th>Device ID</th>
<th>Secondary Device Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASSISTANT WKTP</td>
<td>7914</td>
<td>EXEC LIST</td>
</tr>
</tbody>
</table>
Table 7: Manager/Assistant — User Administration

<table>
<thead>
<tr>
<th>User ID</th>
<th>Worktop Name</th>
<th>Call Orig&amp;Term</th>
<th>Device Monitoring</th>
<th>Call/Device Monitoring</th>
<th>Routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exec Assistant</td>
<td>ASSISTANT WKTP</td>
<td>Not applicable</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Call Monitoring Application

The inbound call agents are monitored by their supervisor, Martha. Martha has one application that collects call handling statistics and a second application that lets her join a call in progress at an agent’s desk. To run these applications, Martha must be given call control privileges and Device/Device monitor, Call/Device monitor and Call/Call monitor privileges on the phones used by the agents. A device group containing the device IDs of the agents is created and entered in Martha’s user profile, and a worktop called ACD SUPV is created.

Table 8: Call Monitoring — Device Group Administration

<table>
<thead>
<tr>
<th>Device Group Name</th>
<th>Device IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACD AGENTS</td>
<td>7701,7702,7711,7712</td>
</tr>
</tbody>
</table>

Table 9: Call Monitoring — User Administration

<table>
<thead>
<tr>
<th>User ID</th>
<th>Worktop Name</th>
<th>Call Orig&amp;Term</th>
<th>Device Monitoring</th>
<th>Call/Device Monitoring</th>
<th>Call/Call Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Martha</td>
<td>ACD SUPV</td>
<td>ACD AGENTS</td>
<td>ACD AGENTS</td>
<td>ACD AGENTS</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

These permissions might also be required by applications that bill based on telephone usage.

Portion of User Community Shares Worktops

Two regular employees, Tom and Lalitha, normally sit at their own desks to perform their job, but may occasionally act as an in-bound call agent when a regular agent is out sick or on vacation. ACME handles this situation by creating a device group, ACD Substitutes, and assigning it to the worktops used by Tom and Lalitha.

Table 10: Shared Worktop — Device Group Administration

<table>
<thead>
<tr>
<th>Device Group Object</th>
<th>Device IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACD Substitutes</td>
<td>7701,7702,7711,7712</td>
</tr>
</tbody>
</table>

Table 11: Shared Worktop — Worktop Administration

<table>
<thead>
<tr>
<th>Worktop Name</th>
<th>Device ID</th>
<th>Secondary Device Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>WKTP1</td>
<td>7801</td>
<td>ACD Substitutes</td>
</tr>
<tr>
<td>WKTP2</td>
<td>7802</td>
<td>ACD Substitutes</td>
</tr>
</tbody>
</table>
Table 12: Shared Worktop — User Administration

<table>
<thead>
<tr>
<th>User ID</th>
<th>Worktop Name</th>
<th>Call Orig&amp;Term</th>
<th>Device Monitoring</th>
<th>Call/Device Monitoring</th>
<th>Routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tom</td>
<td>WKTP1</td>
<td>Not applicable (N/A)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Lalitha</td>
<td>WKTP2</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

As an alternative, you could allow Michael, Sally, Juan, and Marie (the inbound call agents) to switch desks by assigning the ACD Substitutes list to the secondary device group on each worktop or by assigning the list to the Call Origination and Termination group and Device groups in each of their user profiles.

ACME also shares a worktop in its shipping department where Louise, Frank, and Susan work. There is only one worktop in this department and all three share it.

Table 13: Shared Worktop — Secondary Device Worktop Administration

<table>
<thead>
<tr>
<th>Worktop Name</th>
<th>Device ID</th>
<th>Secondary Device Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shipping</td>
<td>7810</td>
<td>Not applicable (N/A)</td>
</tr>
</tbody>
</table>

Table 14: Shared Worktop — Secondary Device User Administration

<table>
<thead>
<tr>
<th>User ID</th>
<th>Worktop Name</th>
<th>Call Orig&amp;Term</th>
<th>Device Monitoring</th>
<th>Call/Device Monitoring</th>
<th>Routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Louise</td>
<td>SHIPPING</td>
<td>Not applicable (N/A)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Frank</td>
<td>SHIPPING</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Susan</td>
<td>SHIPPING</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Promoted Digits

ACME has a telephony-enabled application that can “pop-up” information about a customer using the customer’s account number. Customers call a vector directory number (VDN), where a recorded announcement prompts them to enter their account number on their touch tone phone. The call is then directed to a customer service representative. By monitoring the VDN, ACME’s application is able to retrieve the collected digits and display the customer information at the customer service representative’s computer.

The extension associated with the VDN is 7800. The application must perform both Device/Device monitoring (on the customer service representative’s phone) and call/device monitoring (on the VDN). Therefore, the customer service representatives must be given call/device monitoring permissions.

A device group, “CSR VDN,” is created containing the VDN. This device group is then assigned to the customer service representatives in their Access Rights options.
Table 15: Prompted Digits — Device Group Administration

<table>
<thead>
<tr>
<th>Device Group Name</th>
<th>Device IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSR VDN</td>
<td>7800</td>
</tr>
</tbody>
</table>

Table 16: Prompted Digits — User Administration

<table>
<thead>
<tr>
<th>User ID</th>
<th>Worktop Name</th>
<th>Call Orig&amp;Term</th>
<th>Dev/Device Monitoring</th>
<th>Call/Device Monitoring</th>
<th>Routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beth</td>
<td>WKTPA</td>
<td>Not applicable (N/A)</td>
<td>N/A</td>
<td>CSR VDN</td>
<td>N/A</td>
</tr>
<tr>
<td>Sally</td>
<td>WKTPB</td>
<td>N/A</td>
<td>N/A</td>
<td>CSR VDN</td>
<td>N/A</td>
</tr>
<tr>
<td>Dave</td>
<td>WKTPC</td>
<td>N/A</td>
<td>N/A</td>
<td>CSR VDN</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Call Routing

ACME has a server application that routes all calls to the call center based on the number called, the availability of agents and other criteria. The extension of the incoming calls are 7700 (seeds) and 7710 (tools).

The user in this case is the routing application (Routing App), not a person. The routing application logs in to the TSAPI Service just as a person would and has the same types of privileges. When the routing application begins, it sends a routing registration request to Communication Manager, requesting that incoming calls to extensions 7700 and 7710 be directed to it (the routing application). When the routing application determines which agent should get the call, it tells Communication Manager where to connect the call.

The routing application must be given routing permissions for devices 7700 and 7710. Notice that the user, Routing App, has no associated worktop.

Table 17: Call Routing — Device Group Administration

<table>
<thead>
<tr>
<th>Device Group Name</th>
<th>Device IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACD ROUTE</td>
<td>7700,7710</td>
</tr>
</tbody>
</table>

Table 18: Call Routing — User Administration

<table>
<thead>
<tr>
<th>User ID</th>
<th>Worktop Name</th>
<th>Call Orig&amp;Term</th>
<th>Dev/Device Monitoring</th>
<th>Call/Device Monitoring</th>
<th>Routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing App</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ACD ROUTE</td>
</tr>
</tbody>
</table>
Chapter 12: Licensing

Licensing configurations

In a typical AE Services configuration, a standard license file is installed on each AE Services server, and the licenses in that license file are acquired through a local WebLM server running on the AE Services server. However, the following configurations are also possible:

- Multiple AE Services may be configured to acquire their feature licenses from a single WebLM server where a standard license file is installed. In this configuration, feature licenses can pool from one AE Services server to another as they are needed.

- With enterprise-wide licensing, an enterprise license file is installed on a master WebLM server. Feature licenses can be allocated from the enterprise license file to multiple AE Services servers. The local WebLM server acquires the feature licenses from the AE Services servers. If any of the feature licenses from the enterprise license are not allocated to the individual AE Services servers, these licenses can also pool among the AE Services servers.

**Note:**

- If network delay is high in AE Services and WebLM server, then the use of pooled licensing for AE Services is not recommended. If you are using pooled licenses, adjust your WebLM configuration appropriately.

- When AE Services is configured for enterprise-wide licensing, the license cannot be removed until the local WebLM entries are removed. For more information, see the Enterprise Licensing topic in the *Administering standalone Avaya WebLM* guide.

- You cannot use Virtual IP address with enterprise-wide licensing in Geo Redundant High Availability (GRHA). You must configure the primary AE Services IP address on the WebLM server for enterprise licence to work properly.

  If standby or secondary AE Services server becomes the primary server, you must update the AE Services IP address on the WebLM server manually before the license grace period of 30 days expires.

Reserving unified desktop licenses

Unified desktop licenses are type of licenses used by TSAPI - typically for Microsoft Office Communicator (MOC) users. These users connect to AE Services via DMCC, but their licenses are controlled by TSAPI. Thus, like the TSAPI basic user licenses mentioned in the previous
Reserving unified desktop licenses

section, accessing the WebLM server for each license request can have a noticeable effect on performance. For example, if your Lync server initiates monitors for hundred MOCs, the TSAPI Service will normally acquire a license from the WebLM server, for each of these users, one at a time. You can reduce the time by reserving unified desktop licenses. When you reserve unified desktop licenses, the TSAPI Service acquires all of the reserved licenses at startup time by making a single request to the WebLM server. If more than the reserved amount of unified desktop licenses are used at any given time, TSAPI will acquire the extra licenses from the WebLM server, one at a time.

About this task
After installing or upgrading to AE Services 6.3 or later, use this procedure to:

- Ensure the TSAPI Service starts successfully after a system reboot.
- Optimize the performance of the TSAPI Service.

Procedure

1. Using a web browser, log into the AE Services Management Console.


   Alternatively, you can access Web License Manager using the Avaya WebLM IP address in your web browser.

   Important:
   If you are using a local Avaya WebLM server, then AE Services Management Console will redirect you to the Web License Manager page automatically for the WebLM configuration.

   If you are using a standalone WebLM server or Avaya Aura® System Manager WebLM server Release 8.0 and later then you have to manually log in to the WebLM server or Avaya Aura® System Manager for the WebLM configuration.

   Note:
   If the WebLM server displays a Cross-Site Request Forgery vulnerability warning, ignore it because the password is sent in encrypted form in a POST request.

3. On the Web License Manager page, log in to WebLM.

4. Click Application_Enablement to view the AE Services licensed features.

5. Note the number of Unified Desktop users that are licensed (VALUE_AES_AEC_UNIFIED_CC_DESKTOP).

6. Log out of WebLM.

7. From the AE Services Management Console main menu, select Licensing > Reserved Licenses. The Reserved Licenses page appears.

8. In the Reserved Unified Desktop Licenses box, enter the number of Unified Desktop users that are licensed. This is the value you noted in Step 5.
9. Click **Apply Changes**.
10. On the **Apply Changes to Reserved Licenses** page, click **Apply**.
11. Do one of the following:
    - If you need to reserve TSAPI User licenses, complete steps listed in Reserving TSAPI user licenses on page 232.
    - If you do not need to reserve TSAPI User licenses, continue to the next step.
12. From the **AE Services Management Console** main menu, select **Maintenance > Service Controller**.
13. On the **Service Controller** page, select the **TSAPI Service** check box.
14. Click **Restart Service**.
15. On the Restart Service page, click **Restart**.

---

**Reserving TSAPI user licenses**

**About this task**

After installing or upgrading to AE Services, perform this procedure to

- ensure the TSAPI Service starts successfully after a system reboot
- optimize the performance of the TSAPI Service.

The TSAPI Service acquires its licenses from the WebLM server. Depending on the nature of your TSAPI applications and the number of extensions under TSAPI control, accessing the WebLM server for each license request can have a noticeable effect on the performance of your application. For example, if your TSAPI application initiates monitors for several hundred extensions during its initialization, the TSAPI Service will normally acquire a license from the WebLM server for each of these extensions one at a time. You can reduce the time that it takes your TSAPI application to initialize by reserving TSAPI licenses. When you reserve TSAPI licenses, the TSAPI Service acquires all of the reserved licenses at startup time by making a single request to the WebLM server. If more than the reserved amount of TSAPI licenses are used at any given time, then TSAPI will acquire the extra licenses from the WebLM server one at a time.

**Procedure**

1. Using a web browser, log into the AE Services Management Console.
2. On the **AE Services Management Console** main menu, select **Licensing > WebLM Server Access**. A new browser window appears displaying the **Web License Manager** page.
   
   Alternatively, you can access Web License Manager using the Avaya WebLM IP address in your web browser.

3. On the **Web License Manager** page, log in to WebLM.
Note:
If the WebLM server displays a Cross-Site Request Forgery vulnerability warning, ignore it because the password is sent in encrypted form in a POST request.

4. Click **Application_Enablement** to view the AE Services licensed features.

5. Note the number of TSAPI simultaneous users that are licensed (VALUE_AES_TSAPI_USERS).

6. Log out of WebLM.

7. From the AE Services Management Console main menu, select **Licensing > Reserved Licenses**.

   The Reserved Licenses page appears.

8. In the Reserved TSAPI Basic User Licenses box, enter the number of TSAPI simultaneous users that are licensed. This is the value you noted in Step 5 of this procedure.

9. Click **Apply Changes**.

10. On the Apply Changes to Reserved Licenses page, click **Apply**.

11. From the AE Services Management Console main menu, select **Maintenance > Service Controller**.

12. On the Service Controller page, enable (check) the **TSAPI Service** check box.

13. Click **Restart Service**.

14. On the Restart Service page, click **Restart**.

---

**Embedded Avaya WebLM Server**

**Embedded Avaya WebLM Server and AE Services**

This feature is supported on all AE Services offers. The license file is deployed inside a AE Services server running on Tomcat.

The license file installed on the Embedded Avaya WebLM server uses the AE Services host ID.

Note:
If the eth0 IP address is changed, you must obtain a new license file.

**Embedded Avaya WebLM Server and Geographic Redundancy**

Obtain the Avaya WebLM host ID from both AE Services servers prior to configuring Geographic Redundancy.

- For the Geographic Redundancy feature to be activated, the license file generated for Embedded Avaya WebLM server requires host IDs of both AE Services servers within the license file.
If Geographic Redundancy is already configured, disable HA to get the Avaya WebLM host ID from each AE Services server.

**Embedded Avaya WebLM support by release**

Embedded Avaya WebLM is supported on all AE Services Software-Only offers.

Embedded Avaya WebLM is supported on AE Services 6.x System Platform and software-only offers only.

Embedded Avaya WebLM supports on AE Services VMWare offers from the Release 7.0.1.

**Extended Avaya WebLM service feature**

Extended Avaya WebLM service supports Avaya WebLM service deployed on System Manager or standalone Avaya WebLM server.

**Enterprise Wide Licensing**

In pooled mode, multiple AE Services servers share a pool of licenses installed on an external master Avaya WebLM server.

In allocation mode, a pool of licenses are subdivided and distributed to a local (or embedded) Avaya WebLM server from a master Avaya WebLM.

For a more responsive AE Services server, use allocation mode with Embedded Avaya WebLM servers.

---

**HTTPS, WebLM, and AE Services**

HTTPS is used for connecting a Master Avaya WebLM server and the AE Services Avaya WebLM client or embedded Local Avaya WebLM. The Master Avaya WebLM server can operate in an allocation mode or a pooled mode or both. For the allocation mode, the Master Avaya WebLM server acts as a client of the AE Services embedded Avaya WebLM to establish an HTTPS session and push a license file down to the AE Services embedded Local Avaya WebLM. For the pooled mode, the AE Services C++ and Java Avaya WebLM clients establish an HTTPS session to the Master Avaya WebLM server or the AE Services embedded Local Avaya WebLM to acquire a license.

During the TLS handshake, for an HTTPS client-server session, the server must send its identity certificate to the client and the client must validate the server’s identity certificate. For example, the Not Before date and the Not After date timeframe is valid, and the server identity certificate was signed by a trusted Certificate Authority (CA) known by the client. If the client is unable to validate the server’s identity certificate, the handshake connection is terminated.

**Note:**

- For the pooled mode, the Master Avaya WebLM CA certificates must be imported into the AE Services Trusted Certificate store using the AE Services Management Console.
- For the allocation mode, the AE Services Apache Web server CA certificates must be imported into the Master Avaya WebLM trust store.
While attempting to connect to Avaya WebLM from the AE Services server or from a Master Avaya WebLM to the AE Services embedded Local Avaya WebLM, the connection might not get established. The following are some troubleshooting suggestions:

- **Pooled mode:** Using the Management Console, verify that the CA certificate used to sign the Master Avaya WebLM server's identity certificate is in the AE Services Trusted Certificate store. For a default System Manager installation where the Master Avaya WebLM is also embedded, the System Manager’s embedded CA is used to sign the System Manager server identity certificate. Each System Manager deployment creates its own unique CA certificate with the same Common Name. Therefore, when validating whether the System Manager CA certificate is installed on the AE Services server, ensure that the System Manager CA certificate Serial ID matches the Serial ID of the System Manager CA certificate in the AE Services trust store.

- **Allocation mode:** Verify that the CA certificate used to sign the AE Services server identity certificate is in the Master Avaya WebLM trust store.

- Verify that the port is not blocked by a firewall.

- Verify that the Avaya WebLM server identity certificate has not expired.

- Check the AE Services log files for a TLS/SSL connection error, for example, using an unknown certificate.

### Connecting to Avaya WebLM server

#### About this task

Use this procedure to specify the IP address and port number of the Avaya WebLM server that Application Enablement Services uses for licensing.

Avaya WebLM also supports IPv6.

From the AE Services Release 7.1.3, do not enter Avaya WebLM credentials to log in to the Embedded Avaya WebLM interface. The change password link on the Avaya WebLM user interface does not work. If you changed the password, log out and log in again to Avaya WebLM. The Avaya WebLM login credentials are required only to log in to the external WebLM.

#### Procedure

1. On your web browser, log in to AE Services Management Console.

2. On the AE Services Management Console main menu, click **Licensing > WebLM Server Address**.

3. In the **WebLM IP Address** field, enter the IPv4 address of the remote Avaya WebLM server to point your AE Services server to the Avaya WebLM server.

   If AE Services requires to use the embedded Avaya WebLM server, enter the IP address 127.0.0.1.

4. Select the **SSL** check box to specify the appropriate setting for SSL.

   By default the **SSL** check box is selected.
5. In the **WebLM Port** field, enter the port number of the WebLM server.

**Note:**
If SMGR WebLM Server is used, import the SMGR CA certificate.

The configuration for Secondary WebLM is optional.

AE Services uses secondary WebLM server for licensing only if the primary WebLM server is not available and you have configured the **Secondary WebLM IP Address**.

6. In the **Secondary WebLM IP Address** field, enter the IPv4 address of the secondary WebLM server to point your AE Services server to the WebLM server.

7. Select the **Secondary SSL** check box to specify the appropriate setting for SSL.

8. In the **Secondary WebLM Port** field, enter the port number of the secondary WebLM server.

---

**Reserving DMCC licenses**

**About this task**
After installing or upgrading to AE Services 6.3 or later, perform this procedure to:

- make sure the DMCC Service starts successfully after a system reboot.
- optimize the use of the DMCC licenses.

Like the TSAPI Service, the DMCC License Service acquires its licenses from the WebLM server. DMCC licenses are used to register a DMCC endpoint (station) with Avaya Communication Manager for first-party call control. A DMCC license is required for each endpoint that is registered through DMCC.

Depending on the nature of your DMCC application and the number of endpoints it registers via DMCC, accessing the WebLM server for each license request can have a noticeable effect on the performance of your application. For example, if your DMCC application registers one or more endpoints for each of several hundred telephone extensions, the DMCC License Service will normally acquire a license from the WebLM server for each of these endpoints. Each license request to the WebLM server will be completed one license at a time.

You can reduce the time it takes your DMCC application to register these endpoints by reserving DMCC licenses. When you reserve DMCC licenses, the DMCC License Service acquires several licenses at the time of the first registration by making a single request to the WebLM server. One license will be allocated immediately for the initial registration, while the rest of the licenses will be held in reserve for future registrations. If more licenses than the specified reserve amount are required (that is, there are more concurrently registered endpoints than reserved licenses), then another increment of DMCC licenses (equal to the reserve amount) will be acquired from the WebLM server. License acquisition is performed in increments of the specified reserve amount up to the maximum number available on the WebLM server. Similarly, as endpoints are unregistered, the freed licenses will be released back to the WebLM server in similar increments (equal to the reserve amount). Note that when the last endpoint is unregistered, all of the remaining reserved DMCC licenses will be released back to the WebLM server.
Procedure

1. Estimate the maximum number of endpoints that will be registered via DMCC. If you are sure this is a firm limit, you can use this number as the value for the Reserved DMCC Licenses in the following steps. If this is not a firm limit, it may be wiser for you to use a smaller value for the Reserved DMCC Licenses in the following steps. DMCC will acquire and release licenses from the WebLM server in increments (chunks) equal to this reserve value.

For example, if you estimate the maximum number of registered endpoints to be 1000, then you can perform one of the following actions:

- Specify 1000 as the value for the Reserved DMCC Licenses. In this case, 1000 DMCC licenses will be acquired from the WebLM server on registration of the first endpoint. Note that no licenses will be released back to the WebLM server until the last endpoint is unregistered.

- Specify a smaller number (for example, 50) as the value. In this case, only 50 licenses will be acquired on registration of the first endpoint, another 50 licenses will be acquired on registration of the 51st concurrently-registered endpoint, etc. Note also that, in this case, as endpoints unregister and no longer need the DMCC licenses, the DMCC licenses will be released back to the WebLM server in chunks of 50 (for this example).

2. Using a web browser, log into the AE Services Management Console.

3. From the AE Services Management Console main menu, select Licensing > Reserved Licenses.

   The Reserved Licenses page appears.

4. In the Reserved DMCC Licenses box, enter the value you estimated in Step 1 of this procedure.

5. Click Apply Changes.

6. On the Apply Changes to Reserved Licenses page, click Apply.
Chapter 13: Administration from the operating system command prompt

AE Services Administration from the Operating System Command Prompt

This chapter describes AE Services Server (AE Server) administrative capabilities that you have through the Linux operating system at the command prompt.

⚠ Caution:
Do not attempt any of the commands listed in this chapter unless you have a thorough understanding of Linux administration.

Accounts for Avaya Services technicians

All accounts for Avaya Services technicians are exempt from password aging.

<table>
<thead>
<tr>
<th>Username</th>
<th>Linux Group</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>sroot</td>
<td>root</td>
<td>Created when you install AE Services. The AE Server can not be directly accessed through ssh.</td>
</tr>
<tr>
<td>craft</td>
<td>suser and securityadmin</td>
<td>Created when you install AE Services. Provides read and write access to all AE Services Management Console features.</td>
</tr>
<tr>
<td>rasaccess</td>
<td>remote</td>
<td>For inbound modem access The rasaccess account is for modem access only. This account is manually created by Avaya Services technicians when a user purchases a Service contract.</td>
</tr>
</tbody>
</table>

⚠ Security alert:
AE Services technicians should change the default passwords for the services accounts immediately. See administrative roles and access privileges (role based access control - RBAC) on page 321.
Changing the default passwords for sroot, craft, and rasaccess

About this task
This procedure is for service technicians, and it applies to either an AE Services VMWare server or Software-Only offer with the Avaya Services Package (cs-service) installed.

Procedure

1. If you have the Software-Only offer with the Avaya Services Package (cs-service) or one of the VMware offers, log in to the AE Services Server as root.
2. Type passwd username to display the password prompt. For example passwd root.
3. At the password prompt, type a password, and press Enter.
4. At the prompt to re-enter your password, type the password again, and press Enter.
5. To change the password for craft or rasaccess, repeat Steps 2 through 4.

Adding a Linux user

About this task
This procedure is provided as an alternative to using the AE Services Management Console to add a Linux user. AE Services recommends using the Security Administration pages. For more information see Adding a local Linux account for an administrator - sample on page 166.

Use this procedure add a Linux user with access privileges to AE Services Management Console. The user you add in this procedure will be added to two Linux groups, susers and securityadmin. As a result, this user will be assigned two roles: System Administrator and Security Administrator. For more information about access privileges, see AE Services administrative roles and access privileges (role based access control - RBAC on page 321.

Procedure

1. Do one of the following:
   a. If you have the Bundled Server offer, log in with your user account (username: cust; password custpw) and then become the superuser (su - sroot).
   b. If you have the Software-Only offer, log in as root.
2. Type useradd -g susers -G securityadmin username to add a user name with the same roles as the cust user.
   + Tip:
     The useradd and adduser commands are equivalent. You can use either command, and both commands accept the same arguments.
3. Type passwd username to display the password prompt.
4. At the password prompt, type a password, and press Enter.
5. At the prompt to re-enter your password, type the password again, and press Enter.
6. Log out, and then log in with the new user name and password.
7. From the command line, type `userdel cust` to delete the `cust` account.

---

**Using Tripwire**

Tripwire is configuration auditing software that is installed and initially configured on the AE Services Server. The Tripwire information provided in this section applies to all the AE Services offers except the Software-Only server. This section describes how to configure Tripwire for administrative access and how to use the Tripwire features.

*Note:*

System Platform and Bundled Server are not supported in AE Services Release 7.0. and later.

**Reconfiguring the Tripwire database for administrative access**

**About this task**

Because the Tripwire database is installed by an automated procedure, it is set up with passphrases that are not reusable. For administrative access to the Tripwire database, you must manually reinstall and reconfigure it.

**Procedure**

1. Log in as `root`.
2. Stop the Tripwire service by typing the following command: `service tripwire stop`.
3. Delete the Tripwire configuration file, the policy file, and all key files by typing the following commands:
   a. `rm /etc/tripwire/tw.cfg`
   b. `rm /etc/tripwire/tw.pol`
   c. `rm /etc/tripwire/*.*.key`
4. Delete the Tripwire database file by typing the following command: `rm /var/lib/tripwire/*.*.twd`
5. Configure Tripwire by typing the following command:
   `/etc/tripwire/cmds/twinstall.sh`
6. When prompted, type unique passphrases for the site key and the local key.
   - Each passphrase must consist of at least eight alphanumeric and symbolic characters (quotation marks should not be used). The maximum length of a passphrase is 1023 characters.
7. Reinitialize the tripwire database by typing the following command:
   `tripwire --init`
Note:
Ignore “No such file or directory” messages.

8. Start the tripwire service by typing the following command:

```
service tripwire start
```

Routine administrative tasks for Tripwire

Perform these routine administrative tasks from the command prompt as a root user.

Running an integrity check

About this task

AE Services runs a Tripwire integrity check daily at 4 a.m. If Tripwire detects any changes to the database files, it generates an alarm and creates a report file.

Procedure

To manually run an integrity check, type the command `tripwire --check`.

Tripwire displays the report on your terminal screen and prints a copy of the output in a report file that you can review when the integrity check is complete.

Printing reports

About this task

If Tripwire detects any database changes or security violations when it runs the integrity check, it generates a report, located in `/var/lib/tripwire/report`.

Procedure

To print a report, type the command `twprint -m r --twrfile /var/lib/tripwire/report/<filename>.twr`.

Changes to monitored files should be expected. File changes, additions, or deletions that are not expected could indicate a compromised system. Review the Tripwire report and investigate each file identified. If the change is not expected, take corrective action.

Updating the Tripwire database

About this task

Once a file monitored by Tripwire changes, it will be flagged in every integrity check until the Tripwire database is updated.

After you have taken the necessary corrective action, update the Tripwire database using the report file.

Procedure

1. Type `tripwire --check`, and press Enter
2. Type `tripwire -m u -twrfile /var/lib/tripwire/report/<filename>.twr`.
This updates the Tripwire database so the modified files are not flagged in the next integrity check.

Starting and Stopping Tripwire

About this task
When Tripwire is installed, it will be configured as a service. To start or stop Tripwire, simply treat it as any other service.

Procedure
1. To start Tripwire, type the following command:
   ```
   service tripwire start
   ```
2. To stop Tripwire, type the following command:
   ```
   service tripwire stop
   ```

The dateconfig utility

This information does not apply to the Software-Only server.

AE Services provides a customized version of the dateconfig utility, which is located in `/opt/mvap/bin`. The dateconfig utility lets you set the following:

- Date - sets the date used by the system
- Time - sets the time used by the system
- Time zone - sets the time zone used by the system
- NTP server IP address - sets the address of a time server that the system uses for synchronizing its time clock

⚠️ Warning:
Changing any of the dateconfig settings on a live AE Server can bring down a CTI link.

Changing the date or time

About this task
Changing the date or time of your system implies that it is not synchronized with a Network Time Protocol (NTP) server. If your server is synchronized with an NTP server, you can not change the system date and time unless you disable the NTP Server setting.

The following example depicts changing the date and time, and then disabling the NTP server setting.

Procedure
1. Log in as `root`.
2. Type `dateconfig`.
AE Service displays the Date/Time Initialization screen, with the first box of the Date field initially selected.

3. From the first box of the **Date** field, locate the appropriate month using the arrow up or arrow down keys.

   When you locate the appropriate month, press the **Tab** key to move to the next box and locate the appropriate value for the date. Continue through the **Year** and **Time** fields using the same method.

4. In the **Choose Timezone** field, use the arrow up and down keys to locate the appropriate timezone.

5. Use the space bar to make a selection, then press the **Tab** key to move to the **NTP Server** field.

6. From the **NTP Server** field, use the **Backspace** key to remove the host name or IP address of the NTP Server.

7. Press the space bar to enter a blank space in the **NTP Server** field.

   **Note:**
   To disable the NTP server you must enter a space in the **NTP Server** field.

8. Press the **Tab** key to move to the **OK** box.

9. Press **Enter** to select **OK**.

10. From the command prompt, type **date** to verify the date, year, and time.

### Changing an NTP Server

**About this task**
This example assumes that your server uses an NTP server for time synchronization.

**Note:**
If you change the NTP Server, or if you change the Timezone of an NTP Server, you must restart the ntpd service.

Follow this procedure to change the NTP server.

**Procedure**

1. Log in as **root**.

2. Type **dateconfig**.

   AE Service displays the **Date/Time Initialization** text box, with the first box of the **Date** field initially selected.

3. Press the **Tab** key to move to the **NTP Server** field.

4. Use the **Backspace** key to remove the current IP address and then type in the **<IP address>** or **<host name>** of another NTP server.

5. Press the **Tab** key to move to the **OK** box.
6. Press **Enter** to select **OK**.
7. At the command prompt, type `service ntpd restart`.

---

**The netconfig utility**

This information does not apply to the Software-Only server. The Software-Only server uses a different version of netconfig.

AE Services provides a customized version of the netconfig utility, which allows you to configure network information for the AE Server. The netconfig utility is located in `/opt/mvap/bin`. When you type `netconfig` AE Services displays a screen, which contains settings for the AE Server such as its: hostname, DNS Domain, DNS Server, network interface settings, and default gateway. Whenever you need to change these settings use the netconfig utility.

The table on page 244 provides an example of the Network Information Configuration screen settings for an AE Server with multiple network interfaces (eth0, eth1, eth2, and eth3).

**Table 19: The netconfig utility - Network Information Configuration settings**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Type</th>
<th>Address</th>
<th>Netmask</th>
<th>Enable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>eth0</strong></td>
<td>[ ]</td>
<td>192.168.123.43</td>
<td>255.255.255.0</td>
<td>[x]</td>
<td>eth0 is usually assigned the IP address for client access.</td>
</tr>
<tr>
<td><strong>eth1</strong></td>
<td>[ ]</td>
<td>192.168.123.42</td>
<td>255.255.255.0</td>
<td>[x]</td>
<td>eth1 is reserved for on-site technician use.</td>
</tr>
<tr>
<td><strong>eth2</strong></td>
<td>[ ]</td>
<td>192.168.123.41</td>
<td>255.255.255.0</td>
<td>[x]</td>
<td>eth2 is usually assigned the IP address for Communication Manager access (Private LAN).</td>
</tr>
<tr>
<td><strong>eth3</strong></td>
<td>[ ]</td>
<td></td>
<td></td>
<td></td>
<td>Reserved</td>
</tr>
<tr>
<td><strong>eth4</strong></td>
<td>[ ]</td>
<td></td>
<td></td>
<td></td>
<td>Reserved</td>
</tr>
</tbody>
</table>

| Default Gateway | 192.168.12.344 | The IP address of the network router. |

**Note:**

Instead of rebooting AE Services VM, the DB Service and AESVCS should be restarted. The AE Services cannot be rebooted without checking the status.
Changing the server IP address – Software-Only server

About this task
Follow this procedure to configure network interface settings for a Software-Only server.

Procedure

1. Log in as root.
2. From the command line, type the following command:
   
   /sbin/service mvap stop

   ✔️ Note:
   
   Avaya recommends using a Linux utility such as nmtui if you are using Red Hat Enterprise Linux 7.6

3. Update the /etc/hosts file with the new IP address(es) for the network interfaces.
4. From the command line, as a precautionary step, type /sbin/service network restart.
5. Log in to the AE Services Management Console again using the new IP address of AE Services server.

   ✔️ Note:
   
   If the AE Services Management Console is not responding in a reasonable amount of time, from the command prompt, type the following command: /sbin/service tomcat5 restart

6. From the AE Services Management Console main menu, select Administration > Network Configuration > Local IP.
7. On the AE Service IP (Local IP) page, verify that the IP address(es) for Client Connectivity, Switch Connectivity, and Media Connectivity is set to the new IP address(es) you entered in the /etc/hosts file.
8. From the command line, type the following command:
   
   /opt/mvap/bin/setAlarmSvcUpgrade.sh

9. From the AE Services Management Console main menu, select Maintenance > Service Controller.
10. From the Service Controller page, click Restart AE Server.
11. Make sure all services are in the Running state, and that the connection state to the switch(es) is functional.
Note:
If you can not access the AE Services Management Console, check the status of the httpd and tomcat5 processes. If they are not running, start them. For example, type the following commands:

- /sbin/service httpd status
- /sbin/service httpd start
- /sbin/service tomcat5 status
- /sbin/service tomcat5 start

AE Services Tools and Linux commands

This section describes AE Services Linux based capabilities and a few Linux commands that are available at the command prompt.

AE Services Linux based capabilities

AE Services provides the following Linux based capabilities.

dateconfig
Located in /opt/mvap/bin
Allows you to set the following values:
- Date
- Time
- Time zone
- NTP server IP address

statapp
This utility allows the user to check the status of commonly used services on AE Services and connectivity to the WebLM server.

You will see output similar to the following:

Example
[root@keystone2 cust]# statapp
AESVCS : active (running)
RSYSLOG : active (running)
DBSERVICE : active (running)
SNMPD : active (running)
AESVCS Spiritalgent : active (running)
HTTPD : active (running)
TOMCAT : active (running)
MON : active (running)
SLAPD : active (running)
SSSD : active (running)
NSLCD : active (running)
SUBAGENT1 : active (running)
SUBAGENT2 : active (running)
PRIMARY WEBLM : reachable

mvap.sh
Provides a way for system administrators to get a list of services running in the server and to start, stop and restart all services as a whole. Additionally, it can invoke any exposed methods on any individual service.

*Note:*
The AE Services Management Console Service Controller (Maintenance > Service Controller) provides equivalent functionality. Use the AE Services Management Console as your primary tool. It is recommended to use the mvap.sh utility judiciously and only when necessary, because using this utility might cause high CPU usage on AE Services Server.

Located in /opt/mvap/bin

Syntax

```
mvap.sh <command name> [<service name>] | <method name> <service name> <argument-list>
```

where:

<command name>

info - lists info name value pairs of <service name>
status - lists state of <service name>
start - invokes start on <service name>
stop - invokes stop on <service name>
restart - attempts to restart <service name>
suspend - attempts to suspend <service name>
resume - attempts to resume <service name>

CmapiService - Device, Media, and Call Control Service
CvlanService - CVLAN Service
TsapiService - TSAPI Service
Administration from the operating system command prompt

**D1gService** - DLG Service
**AsaILinkManager** - ASAI Link Manager
**TransportService** - Transport Service

**Note:**
If you omit the service name, the command assumes all service names.

*Example:*
```
mvap.sh info CvlanService
```

**netconfig**
Located in `/opt/mvap/bin`
Allows you to set the following values:

- Host name
- Domain name
- Domain name server
- IP address and network mask for eth0
- IP address and network mask for eth1
- IP address and network mask for eth2, if present
- IP address and network mask for eth3, if present
- Default Gateway IP address

**swversion**
Located in `/opt/mvap/bin`
There are three forms of the `swversion` command.

The first form, `swversion`, lists the following:

- Offer type
- Server type
- Patches installed
- Software version number
- Operating system (kernel) version

The second form, `swversion -a`, lists the following:

- Offer type
- Server type
- Patches installed
- Software version number
- Operating system (kernel) version
• List of AE Services RPMs
• List of third-party RPMs

The third form, `swversion -s`, lists the following:
• Application name
• Application version
• Application Deployment
• Virtualization Environment
• Current Application Size

**Linux commands**

This section describes Linux commands that are useful for working with AE Services.

**df**

Allows you to check the disk capacity and partitions of the AE Services server.

**ethtool**

Allows you to query or change the settings of an Ethernet device (a network interface device, sometimes referred to as a NIC, or Network Interface Card). Use `ethtool` to view or change the settings of the network interfaces on the AE Services server. When you use `ethtool` to change the network interface settings, the changed settings will not persist after rebooting the AE Services server. To specify new persistent settings for the network connection, you must use the AE Services Management Console. For more information about changing network settings, see *Editing the NIC configuration (optional)* on page 315.

The following list provides examples of using the `ethtool` command for AE Services.

```plaintext
• `ethtool eth0`
  Displays the settings of eth0.

• `ethtool -s eth0 autoneg on`
  Turns on auto-negotiation for eth0. This is the default setting for any interface unless it is changed.

• `ethtool -s eth0 autoneg off`
  Turns off auto-negotiation for eth0. When you want to change the settings of a network interface, such as the network speed or the duplex mode, you must turn off auto-negotiation first.

• `ethtool -s eth0 speed 100`
  Sets the network speed of eth0 to 100 Mbs. This is the required speed for AE Services.

• `ethtool -s eth0 duplex full`
  Sets the duplex mode to full for eth0. This is the required duplex mode for AE Services.

• `ethtool -s eth0 speed 100 duplex full`
  Sets the network speed and duplex mode for eth0 with a single command entry.
```
For more information about `ethtool` command syntax, see the Linux manual page for `ethtool`.

**route**

Allows you to administer static routes.

To use this command, log in as `root` or `sroot`. Then type `route` to view or configure IP routes. For information on the different options of the `route` command, see the Linux manual page for `route`.

**scp and sftp**

Use the `scp` and `sftp` commands to copy files to and from the AE Services server.

**service <name> start/stop/restart**

Log in as `root` or `sroot` to use the service command.

**Syntax**

```
service <name> [start | stop | restart | status]
```

where `<name>` is:

- `DBService` — refers to the Postgres database.
- `tomcat5` — refers to the Tomcat Web application server.

**shutdown -r now**

Reboots the AE Services server.

**ssh**

The `telnet` command is disabled on the VMWare server for both incoming and outgoing connections. Use the `ssh` command instead. `ssh` uses port 22. If you are using a Windows machine to connect to the server, use a secure shell SSH client such as PuTTY to connect.

**tripwire**

See [Using Tripwire](#) on page 240.

**Installation and upgrade logs and RPMs**

For the Bundled offer, the installation/upgrade logs are located in: `/var/disk/logs/cinstall-xxxxxxxx-xxxxxx`.

For the other AE Services offers, the installation/upgrade logs are located in: `/var/disk/logs/update.out-xxxx-xxxx-xxxx`.

(Applies exclusively to Software-Only server) Copies of RPMs for each release that is installed (up to 3 installs) are located in:

`/var/disk/Releases/r<aes ISO version>`
Directory structure and file locations

The AE Services root directory /opt/mvap contains the following subdirectories

- **asailink** — ASAI specific files
- **bin** — executables and scripts
- **cmapi** — Device, Media, and Call Control specific files
- **conf** — User Management files
- **config** — configuration files
- **cvlan** — CVLAN specific files
- **deploy** — CMAPI hot deploy directory
- **dlg** — DLG specific files
- **dms** — Database Monitoring Service specific files
- **lib** — shared libraries, jars
- **licenses** — license files
- **logs** — log files including call control trace files. Starting with AE Services Release 4.1, logs is logical link to the /var/log/avaya/aes directory.
- **transport** — Transport Service specific files
- **tsapi** — TSAPI specific files
- **web** — Web Service files
- **alarming** — alarm log files
- **resources** — system and user resource files

**postgres data files**

The default directory for postgres data files is /var/mvap/database.

**External scripts**

External scripts, tools or binary executables are in /opt/mvap/bin.

**Environment variables**

Environment variables are set at login and defined in /etc/profile.d/mvap.sh.
Chapter 14: Administering SNMP

Administering SNMP

Use this chapter to set up the AE Server in an SNMP managed network.

Before you begin - SNMP basics

If you are not familiar with Simple Network Management Protocol (SNMP), read this section to learn a few basic concepts.

**Simple Network Management Protocol (SNMP).** SNMP is a standard network management protocol that is used to remotely monitor and manage network-capable devices such as computers, switches, and gateways. SNMP provides a way for monitored objects (SNMP agents) and monitoring objects (SNMP managers) to exchange status messages.

**SNMP Agents.** SNMP agents collect and store status information and make it available to SNMP NMS/Managers. In terms of the AE Services implementation, the AE Server contains an SNMP agent which supports SNMP protocols v1, v2c, and v3. The AE Server also has the ability to issue SNMP based Traps/Notifications. Whenever a significant event such as a service failure occurs, the SNMP agent sends a notification to the SNMP NMS. Notifications can be sent using either the SNMP *trap* command or the SNMP *inform* command.

- Notifications sent with the *trap* command do not require a confirmation from the receiver. All versions of SNMP support trap notifications.
- Notifications sent with the *inform* command require a confirmation from the receiver. Only SNMP versions 2c and 3 support inform notifications.

By default, AE Services uses the *trap* command to send notifications. In general usage, the term trap refers to an unsolicited notification from an SNMP agent to an SNMP manager.

**SNMP managers.** SNMP managers collect and store status information received from SNMP agents. In terms of the AE Services implementation, SNMP managers are either Avaya Secure Services Gateways (SSG), Avaya Secure Access Link (SAL), or Network Management System (NMS) devices (IBM Tivoli or HP OpenView, for example). SNMP managers get information by either issuing a request (solicited information) or by receiving a notification whenever an event occurs (unsolicited information). Traps (whether generated by the *trap* or *inform* command) are unsolicited notifications.
Management Information Base (MIB). The MIB defines (by way of data structures) the information an SNMP agent is capable of reporting. AE Services MIBs are available through the Product Licensing and Delivery System (PLDS).

SNMP components for AE Services

In terms of SNMP, the AE Server has three configuration areas in the AE Services Management Console under **Utilities > SNMP**.

- Product ID (also referred to as Alarm ID)
- SNMP Agent
- SNMP Trap Receivers

Product ID administration

The Product ID is used to identify an AE Server. This ID is also referred to as the Alarm ID. The ID is a 10–digit number that is included in each SNMP trap issued by the AE Server. In order to configure this value from the AE Services Management Console, from the main menu navigate to **Utilities > SNMP > Product ID**. The default AE Server Product ID is 4000000000.

Configuring the SNMP Agent

**About this task**

The SNMP Agent incorporated into AE Services 6.2 supports SNMP v1, v2c, and v3. This agent provides access to SNMP related system performance and metrics associated with the AE Server and AE Services (TSAPI, CVLAN, DLG, DMCC and the Transport Layer).

The agent is configured from the AE Services Management Console. By default all external access to the agent is disabled.

**Procedure**

1. From the AE Services Management Console main menu, select **Utilities > SNMP > SNMP Agent**.

2. In the **MIB II System Group Data** section, do the following:
   a. In the **Location** field, enter the physical location of the AE Server. For example LabB1Area2cRack5. **Up to 255 characters are permitted.**
   b. In the **Contact** field, enter the name of the person or organization to contact in regards to managing the AE Server. For example John Smith 555–1234 jsmith@example.com. **Up to 255 characters are permitted.**

   These values are used to configure the MIB II OIDs sysLocation and sysContact.

3. In the **SNMP Protocol Access** section, select one of the following settings to specify the SNMP protocol allowed to access the agent:
   - For SNMP v1 access, select the check box labeled **Enable SNMP Version 1** and provide a community string. For example allowV1Access.
• For SNMP v2 access, select the check box labeled **Enable SNMP Version 2** and provide a community string. For example `allowV2Access`.

• For SNMP v3 access, select the check box labeled **Enable SNMP Version 3**.

4. If you checked **Enable SNMP Version 3**, do the following:
   a. In the **User Name** field, enter the login name to be used. For example `JohnSmith`.
   b. From the **Authentication Protocol** drop down list box, select either MD5, or SHA.
   c. In the **Authentication Password** field, enter an alphanumeric authentication password for authenticated SNMP v3 messages. This password can be 6 to 32 character strings.
   d. From the **Privacy Protocol** drop down list box, select either DES, or AES.
      You must define a **Privacy Protocol** for SNMP Version 3 to work properly.
   e. In the **Privacy Password** field, enter an alphanumeric privacy password for encrypted SNMP v3 messages. This password can be a 6 to 32 character strings.

5. In the **Authorized IP Addresses for SNMP Access** section, select one of the following settings to provide the IP addresses of the NMSs that are allowed to access the AE Server SNMP Agent:
   • Select **No Access** to block all access. This is the default setting.
   • Select **Any IP Addresses** to allow anyone access.
   • Select **Following IP Addresses** to allow access for only 1 to 5 NMSs.

   ![Note:](image)
   There are no IP access restrictions on Software-Only for SNMP v3.

6. Select **Apply Changes**.

7. On the confirmation screen, select **Apply**.

### About sending traps to an Avaya INADS (SSG or SAL) and NMS

If you have the AE Services Server, and have purchased an agreement with Avaya Technical Services for either the Secure Access and Control Basic Offer or the Secure Access and Control Premium Offer, you can send traps to an SSG device or SAL and a local NMS device. For more information about Secure Access and Control (SAC), see [http://support.avaya.com/sac](http://support.avaya.com/sac).

Traps sent using the SSG or SAL device type as specified on the AE Services Management Console screen, **Utilities > SNMP > SNMP Trap Receivers**, result in Initialization and Administrative System (INADS) notifications. INADS notifications, in turn, generate trouble tickets with Avaya Services. Only a subset of the available traps issued by the AE Services server is published to a SNMP trap destination using INADS. This option is only available to Avaya Service accounts.

All available traps issued by the AE Services server are published to a SNMP trap destination when the NMS device type is specified.
Note:

Traps such as tripwire notifications and login failures are not sent to an SSG or SAL. When you are administering the AE Services Server to send traps, you will want to send these traps to a local NMS. SAL can act as an INADS or an NMS device type.

If you do not have the SAC–SSG or SAL Offer, you can send traps to a NMS device only. The SAC-SSG or SAL offer is available with the AE Services VMware offer only. If you use the AE Services Software-Only server, the SAC-SSG or SAL offer does not apply.

If you do not have the SAC-SSG or SAL Offer

If you do not have the SAC–SSG or SAL Offer, you can send traps to a local NMS only. The SAC-SSG or SAL offer is available with the AE Services VMware offer only. If you use the AE Services Software-Only server, the SAC-SSG or SAL offer does not apply.

If you provide Technical Services with modem access to the AE Server

If you provide Technical Services with modem access to the AE Server for maintenance, there is no provision for alarming. You must contact Avaya Services to report problems.

Administering SNMP trap receivers

About this task

Follow this procedure to send traps from the AE Server to an SNMP manager, which can be either a local NMS device, an Avaya SSG, or an Avaya SAL.

Procedure

1. From the AE Services Management Console main menu, select Utilities > SNMP Traps > SNMP Trap Receivers.
2. From the SNMP Traps Web page, select Add and complete the Add SNMP Trap page.
   If you are using SNMP Version 1 or 2c, complete Steps 3 through 10. If you are using SNMP Version 3, complete Steps 3 through 15.
3. Leave the Enabled check box selected (the default).
4. In the Device field, select the type of monitoring device that is to receive traps.
   - Select NMS to send all traps to an SNMP trap destination, for example, IBM Tivoli, HP Openview, or SAL. If you are administering a Software-Only server, the Device setting is restricted to NMS.
   - Select SSG/SAL to send INADS notifications to an Avaya Secure Services Gateway or Secure Access Link. Keep in mind that only an SSG or SAL is capable of generating INADS notifications. This option is available only to clients who have purchased an Avaya Services contract.
5. In the IP address field, type the host name IP address of the device to receive the traps.
6. In the Port field type the TCP/UDP port number that AE Services is to use for sending traps.
Keep in mind that the port number you specify must match the port number administered on the SNMP manager that is to receive the notification. The default is 162.

7. In the Notification Type field, select Trap (the default).

8. Select the SNMP Version that is appropriate for your SNMP managed network. The default is 3. If you are sending traps to an SSG, select 2c.

9. Type the Security Name that is appropriate for your SNMP network, as follows:
For devices that use SNMP version 1 or 2c, type the community name that the SNMP administrative domain uses for authentication. For devices that use SNMP version 3, type the security name that the SNMP administrative domain uses for authentication. You cannot leave this field blank or use the terms public or private.

10. Based on the version of SNMP you are using, do one of the following:
   • If you are using SNMP version 1 or 2c, click Apply to put your settings into effect. (You have completed all the necessary fields, and the procedure is complete.)
   • If you are using SNMP version 3, you must complete Steps 11 through 15.

11. Select the option for the Authentication Protocol that your SNMP managed network uses:
   • MD5 indicates that the network uses the MD5 based authentication protocol.
   • SHA indicates that the network uses the SHA authentication protocol.

12. Type an Authentication Password.
   This password can be a 6- to 32-character string. Validate the Authentication Password by retyping it in the Confirm Password field.

13. Select the option for the Privacy Protocol that your SNMP managed network uses:
   • DES indicates that the network uses the DES encryption protocol.
   • AES indicates that the network uses the AES encryption protocol.

14. Type a Privacy Password.
   This password can be a 6- to 32-character string. Validate the Privacy Password by retyping it in the Confirm Password field.

15. Click Apply to put your settings into effect.

Testing SNMP Traps

About this task
The following procedure is a method to verify that you are able to receive a trap locally on the following locations:
   • Local: AE Services Server
   • Remote: On a remote NMS device.
**Note:**
To get the patches, go to [http://support.avaya.com/download](http://support.avaya.com/download), which requires Avaya Single Sign On (SSO), and download the appropriate patch.

**Procedure**

1. From a web browser, type the fully qualified domain name or IP address of the AE Services server. For example `aeserver.example.com`.
2. From the main menu, select **Continue**.
3. Complete the log in screen with the appropriate log in information.
   - Avaya Services Technicians: use the **craft** user name and password.
   - Avaya customers: use the **cust** user name and password.
4. From the AE Services Management Console main menu, select **Utilities > SNMP > Trap Receivers**.
5. From the SNMP Trap Receivers page, select **Add**, and complete the Add SNMP Trap page by following these steps:
   a. Leave the **Enabled** check box selected (the default).
   b. In the **Device** field, select **NMS**.
   c. In the **IP address** field, type one of the following:
      - Host name (for example `aeserver.example.com`)
      - IP address (for example `192.168.123.44`)
      - Loop back IP address of the AE Services Server, which is `127.0.0.1`
   d. In the **Port** field, type the port number that AE Services is to use for sending traps. The default is `162`.
   e. In the **Notification Type** field, select **Trap**.
   f. In the **SNMP Version** field, select **2c**.
   g. In the **Security Name** field, type the name that the network uses for authentication. For devices that use SNMP Version 1 or 2c, this name corresponds to the community name. Enter a name for the test and click **Apply**.
6. Click **Add Trap**.
7. As a root user on the AE Services Server, start the trap listener by typing the following command:
   ```
   snmptrapd -fLo
   ```
8. Open another window as a root user on the AE Services Server and type the following command:
   ```
   logger -t mon -i "File Removed"
   logger -t mon -i "File Added"
   ```
9. Verify in the listener xterm window that the SNMP notification is received.
10. Verify that your remote SNMP Manager received the same trap.
11. Click **Status > Alarm viewer** to view the alarms you just generated.

**AE Services SNMP traps, alarm codes and messages**

AE Services provides the following alarm codes and messages. Each of the specified alarms will result in the generation of an SNMP trap:

- The **INADS Trap** and **NMS Trap** columns indicate which alarms will issue a trap to Avaya SSG (INADS) and/or a remote NMS.
- The **Alarm Severity** column represents the severity of the generated alarm and the SNMP trap.
- The **AES Release** column identifies the initial AE Services release which provides support for the specified SNMP trap and alarm.

**AEServicesSNMPtrapsAlarmCodesAndMessages_Part1**

**SNMP Object Name:** avAesServiceDown  
**SNMP OID:** .1.3.6.1.4.1.6889.2.27.2.2.2.1.0.1  
**SNMP Object Description:** AES Service died unexpectedly  
**Remediation Suggestions:** Review each service log file to determine the reason why the service stopped.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES000</td>
<td>The AE Services POSTGRES service stopped unexpectedly</td>
<td>Yes</td>
<td>Yes</td>
<td>Major</td>
</tr>
<tr>
<td>AAES001</td>
<td>The AE Services POSTGRES service started successfully</td>
<td>No</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
<tr>
<td>AAES002</td>
<td>The AE Services ASAI Link Manager service stopped unexpectedly</td>
<td>Yes</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES003</td>
<td>The AE Services ASAI Link Manager service started successfully</td>
<td>No</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
<tr>
<td>AAES004</td>
<td>The AE Services CVLAN Server stopped unexpectedly</td>
<td>Yes</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES005</td>
<td>The AE Services CVLAN Server started successfully</td>
<td>No</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
<tr>
<td>AAES006</td>
<td>The AE Services DLG Server stopped unexpectedly</td>
<td>Yes</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES007</td>
<td>The AE Services DLG Server started successfully</td>
<td>No</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
<tr>
<td>AAES008</td>
<td>The AE Services Transport service stopped unexpectedly</td>
<td>Yes</td>
<td>Yes</td>
<td>Minor</td>
</tr>
</tbody>
</table>

*Table continues…*
### Alarm Codes and Messages

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES009</td>
<td>The AE Services Transport service started successfully</td>
<td>No</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
<tr>
<td>AAES010</td>
<td>The AE Services TSAPI service stopped unexpectedly</td>
<td>Yes</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES011</td>
<td>The AE Services TSAPI service started successfully</td>
<td>No</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
<tr>
<td>AAES012</td>
<td>The AE Services DMCC stopped unexpectedly</td>
<td>Yes</td>
<td>Yes</td>
<td>Major</td>
</tr>
<tr>
<td>AAES013</td>
<td>The AE Services DMCC service started successfully</td>
<td>No</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
<tr>
<td>AAES014</td>
<td>The AE Services Lifecycle Manager stopped unexpectedly</td>
<td>Yes</td>
<td>Yes</td>
<td>Major</td>
</tr>
<tr>
<td>AAES015</td>
<td>The AE Services Lifecycle Manager service started successfully</td>
<td>No</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
</tbody>
</table>

### SNMP Object Name: `avAesServiceColdStart`

**SNMP OID:** `.1.3.6.1.4.1.6889.2.27.2.2.2.1.0.2`

**SNMP Object Description:** AES Service start request received.

**Remediation Suggestions:** N/A

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES018</td>
<td>The AE Services ASAI Link Manager service cold started successfully</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
<tr>
<td>AAES020</td>
<td>The AE Services CVLAN Server cold started successfully</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
<tr>
<td>AAES022</td>
<td>The AE Services DLG Server cold started successfully</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
<tr>
<td>AAES024</td>
<td>The AE Services Transport service cold started successfully</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
<tr>
<td>AAES026</td>
<td>The AE Services TSAPI service cold started successfully</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
<tr>
<td>AAES028</td>
<td>The AE Services DMCC service cold started successfully</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
<tr>
<td>AAES030</td>
<td>The AE Services Lifecycle Manager service cold started successfully</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
</tbody>
</table>

### SNMP Object Name: `avAesServiceStopped`

**SNMP OID:** `.1.3.6.1.4.1.6889.2.27.2.2.2.1.0.3`

**SNMP Object Description:** AES Service stop request received.

**Remediation Suggestions:** If this was planned, do nothing. Otherwise, investigate the log files to determine why the service was stopped.
<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES019</td>
<td>The AE Services ASAI Link Manager service stopped successfully</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
<tr>
<td>AAES021</td>
<td>The AE Services CVLAN Server stopped successfully</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
<tr>
<td>AAES023</td>
<td>The AE Services DLG Server stopped successfully</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
<tr>
<td>AAES025</td>
<td>The AE Services Transport service stopped successfully</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
<tr>
<td>AAES027</td>
<td>The AE Services TSAPI service stopped successfully</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
<tr>
<td>AAES029</td>
<td>The AE Services DMCC stopped successfully</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
<tr>
<td>AAES031</td>
<td>The AE Services Lifecycle Manager stopped successfully</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** avAesAuditServiceError

**SNMP OID:** .1.3.6.1.4.1.6889.2.27.2.2.1.0.4

**SNMP Object Description:** The audit service experienced an error.

**Remediation Suggestions:** The Linux Audit service (auditd) logs to the file /var/log/audit. Review the audit log file for additional information associated with the error.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES032</td>
<td>The audit service experienced an error</td>
<td>Yes</td>
<td>Yes</td>
<td>Minor</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** avAesAuditServiceLoggingIssue

**SNMP OID:** .1.3.6.1.4.1.6889.2.27.2.2.1.0.5

**SNMP Object Description:** The audit service experienced a logging issue.

**Remediation Suggestions:** The Linux Audit service (auditd) logs to the file /var/log/audit. Review the audit log file for additional information associated with the service logging issue.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES033</td>
<td>The audit service experienced a logging issue</td>
<td>Yes</td>
<td>Yes</td>
<td>Minor</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** avAesHaServiceIssue

**SNMP OID:** .1.3.6.1.4.1.6889.2.27.2.2.1.0.6

**SNMP Object Description:** The AE Services HA service experienced an issue.

**Remediation Suggestions:** Execute 'sohctl -lh' on the Linux shell or view the log file /opt/mvap/logs/ha.log for more information.
### Alarm Code

#### AAES034
The HA service experienced an error, please run `sohctl -lh` on the Linux shell or view the log file `/opt/mvap/logs/ha.log` for more information.

<table>
<thead>
<tr>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Minor</td>
</tr>
</tbody>
</table>

#### AAES035
The HA service cleared an error, please run `sohctl -lh` on the Linux shell or view the log file `/opt/mvap/logs/ha.log` for more information.

<table>
<thead>
<tr>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
</tbody>
</table>

#### AAES036
The HA service issued a failover, please run `sohctl -lh` on the Linux shell or view the log file `/opt/mvap/logs/ha.log` for more information.

<table>
<thead>
<tr>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Minor</td>
</tr>
</tbody>
</table>

### SNMP Object Name:

**avAesTsapiPbxDriverError**

### SNMP OID:

`.1.3.6.1.4.1.6889.2.27.2.2.2.1.0.7`

### SNMP Object Description:

TSAPI PBX Driver is not responding.

#### Remediation Suggestions:

Collect log files by running the `getlogs.sh` command. Copy the log files generated by running the `getlogs.sh` command and the core files generated at `/opt/mvap/logs/crash.tsrv.<pid>.tar.gz` path to a different server. Share the copied files at the server with Avaya support.

Do one of the following to restart the TSAPI service:

- Log in to the AE Services OAM interface and navigate to **Maintenance > Services Controller > Restart TSAPI service**.
- On the Command Line Interface, run the `mvap.sh restart TsapiService` command

Restarting the TSAPI service may impact your ongoing services.

### Note:

Application Enablement Services supports **avAesTsapiPbxDriverError** alarm from Release 8.1.2.1 and later.

### AEServicesSNMPtrapsAlarmCodesAndMessages_Part2

#### SNMP Object Name:

**avAesCtiLinkDown**

#### SNMP OID:

`.1.3.6.1.4.1.6889.2.27.2.2.2.0.1`

#### SNMP Object Description:

The CTI Link is down.

#### Remediation Suggestions:

If the link remains down, review each service log file and use the AE Services Management Console Status screen related to the affected service to review the CTI link information.
### Alarm Code

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES100</td>
<td>An AE Services TSAPI CTI link is down</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES101</td>
<td>An AE Services TSAPI CTI link is up</td>
<td>No</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
<tr>
<td>AAES102</td>
<td>An AE Services CVLAN CTI link is down</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES103</td>
<td>An AE Services CVLAN CTI link is up</td>
<td>No</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
<tr>
<td>AAES104</td>
<td>An AE Services DLG CTI link is down</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES105</td>
<td>An AE Services DLG CTI link is up</td>
<td>No</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
<tr>
<td>AAES108</td>
<td>An AE Services Call Info connection is down</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES109</td>
<td>An AE Services Call Info connection is up</td>
<td>No</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** avAesAepConnLinkDown  
**SNMP OID:** .1.3.6.1.4.1.6889.2.27.2.2.2.0.2  
**SNMP Object Description:** An AEP Connection link is down.  
**Remediation Suggestions:** If the link remains down, review the transport service log file and use the AE Services Management Console Status screen related to the Switch Connection service to review the link information.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES106</td>
<td>An AE Services AEP connection is down</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES107</td>
<td>An AE Services AEP connection is up</td>
<td>No</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** avAesWebLMConnLinkDown  
**SNMP OID:** .1.3.6.1.4.1.6889.2.27.2.2.2.0.3  
**SNMP Object Description:** The WebLM Connection link is down.  
**Remediation Suggestions:** If the link remains down, review the WebLM service log file, determine if the server is experiencing network related issues, and attempt to connect to the WebLM service.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES110</td>
<td>The WebLM connection is down</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES111</td>
<td>The WebLM connection is up</td>
<td>No</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** avAesRemoteKeyServerDown  
**SNMP OID:** .1.3.6.1.4.1.6889.2.27.2.2.2.0.4  
**SNMP Object Description:** The Remote Key Server[s] is/are down.  
**Remediation Suggestions:** Check accessibility to the Remote Key Server.
<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES326</td>
<td>The Remote Key Server &lt;Remote Key Server IP&gt; is not accessible</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
<tr>
<td>AAES327</td>
<td>The Remote Key Server &lt;Remote Key Server IP&gt; is reachable</td>
<td>No</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
<tr>
<td>AAES328</td>
<td>All remote key servers are not reachable</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES329</td>
<td>One or more remote key server is up</td>
<td>No</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
</tbody>
</table>

**AEServicesSNMPtrapsAlarmCodesAndMessages_Part3**

**SNMP Object Name:** avAesClientLoginFailure

**SNMP OID:** .1.3.6.1.4.1.6889.2.27.2.2.2.3.0.1

**SNMP Object Description:** An AES Client tried to log in but was not authenticated.

**Remediation Suggestions:** Verify the credentials used.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES200</td>
<td>An AE Services TSAPI user authentication failure occurred</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES201</td>
<td>An AE Services CVLAN user authentication failure occurred; the requested signal number was not valid for the client</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES202</td>
<td>An AE Services CVLAN user authentication failure occurred</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES203</td>
<td>An AE Services DLG user authentication failure occurred; the requested client link number was not valid for the client</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES204</td>
<td>An AE Services DLG user authentication failure occurred</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** avAesCertificateFailure

**SNMP OID:** .1.3.6.1.4.1.6889.2.27.2.2.2.3.0.2

**SNMP Object Description:** Specifies if a certificate is about to expire or has expired.

**Remediation Suggestions:** Replace or renew the affected certificate.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES205</td>
<td>The Server Certificate will expire in 30 days</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES206</td>
<td>The Server Certificate will expire in 10 days</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES207</td>
<td>The Server Certificate has expired</td>
<td>No</td>
<td>Yes</td>
<td>Major</td>
</tr>
</tbody>
</table>

*Table continues...*
<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES208</td>
<td>The AE Services Certificate will expire in 30 days</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES209</td>
<td>The AE Services Certificate will expire in 10 days</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES210</td>
<td>The AE Services Certificate has expired</td>
<td>No</td>
<td>Yes</td>
<td>Major</td>
</tr>
<tr>
<td>AAES211</td>
<td>The Web Server Certificate will expire in 30 days</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES212</td>
<td>The Web Server Certificate will expire in 10 days</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES213</td>
<td>The Web Server Certificate has expired</td>
<td>No</td>
<td>Yes</td>
<td>Major</td>
</tr>
<tr>
<td>AAES214</td>
<td>The LDAP Server Certificate will expire in 30 days</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES315</td>
<td>The EASG Certificate has expired</td>
<td>No</td>
<td>Yes</td>
<td>Major</td>
</tr>
<tr>
<td>AAES316</td>
<td>The EASG Certificate will expire in 30 days</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES317</td>
<td>The EASG Certificate will expire in 180 days</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES318</td>
<td>The EASG Certificate will expire in 365 days</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** avAesLoginFailure  
**SNMP OID:** .1.3.6.1.4.1.6889.2.27.2.2.2.3.0.3  
**SNMP Object Description:** Indicator of login failures.  
**Remediation Suggestions:** If the failure is excessive, either use the information contained in the SNMP Trap/Notification, or review the Linux server security log to determine the offending user and IP address to take appropriate action.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES217</td>
<td>OAM Login Failure</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES218</td>
<td>Remote SSH Login Failure</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES219</td>
<td>Local Console Login Failure</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** avAesLoginAttemptsExceeded  
**SNMP OID:** .1.3.6.1.4.1.6889.2.27.2.2.2.3.0.4  
**SNMP Object Description:** Indicator of login failure attempts exceeded.  
**Remediation Suggestions:** If the failure is excessive, either use the information contained in the SNMP Trap/Notification, or review the Linux server security log to determine the offending user and IP address to take appropriate action.
### Alarm Codes and Messages

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES220</td>
<td>OAM Login Attempts Exceeded</td>
<td>No</td>
<td>Yes</td>
<td>Major</td>
</tr>
<tr>
<td>AAES221</td>
<td>SSH Login Attempts Exceeded</td>
<td>No</td>
<td>Yes</td>
<td>Major</td>
</tr>
<tr>
<td>AAES222</td>
<td>Local Console Login Attempts Exceeded</td>
<td>No</td>
<td>Yes</td>
<td>Major</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** avAesLicenseFailure  
**SNMP OID:** .1.3.6.1.4.1.6889.2.27.2.2.2.4.0.1  
**SNMP Object Description:** Specifies if a license is about to expire or has expired.  
**Remediation Suggestions:** Replace or renew the expired license.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES300</td>
<td>The AE Services license will expire in 30 days</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES301</td>
<td>The AE Services license will expire in 10 days</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES302</td>
<td>The AE Services license has expired</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** avAesGracePeriodFailure  
**SNMP OID:** .1.3.6.1.4.1.6889.2.27.2.2.2.4.0.2  
**SNMP Object Description:** Specifies if a license grace period is about to expire or has expired.  
**Remediation Suggestions:** Install a valid license.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES303</td>
<td>DMCC entered 30 day grace period</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES304</td>
<td>DMCC has 10 grace period days remaining</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES305</td>
<td>DMCC entered restricted mode, 0 grace period days remain</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES306</td>
<td>CVLAN entered 30 day grace period</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES307</td>
<td>CVLAN has 10 grace period days remaining</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES308</td>
<td>CVLAN entered restricted mode, 0 grace period days remain</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES309</td>
<td>DLG entered 30 day grace period</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES310</td>
<td>DLG has 10 grace period days remaining</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES311</td>
<td>DLG entered restricted mode, 0 grace period days remain</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES312</td>
<td>TSAPI entered 30 day grace period</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES313</td>
<td>TSAPI has 10 grace period days remaining</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>AAES314</td>
<td>TSAPI entered restricted mode, 0 grace period days remain</td>
<td>No</td>
<td>Yes</td>
<td>Minor</td>
</tr>
</tbody>
</table>

Table continues…
### Alarm Codes and Messages

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES322</td>
<td>DMCC entered normal license mode</td>
<td>No</td>
<td>Yes</td>
<td>Clear</td>
</tr>
<tr>
<td>AAES323</td>
<td>TSAPI entered normal license mode</td>
<td>No</td>
<td>Yes</td>
<td>Clear</td>
</tr>
<tr>
<td>AAES324</td>
<td>CVLAN entered normal license mode</td>
<td>No</td>
<td>Yes</td>
<td>Clear</td>
</tr>
<tr>
<td>AAES325</td>
<td>DLG entered normal license mode</td>
<td>No</td>
<td>Yes</td>
<td>Clear</td>
</tr>
</tbody>
</table>

### SNMP Traps

AEServicesSNMPtrapsAlarmCodesAndMessages_Part4

**SNMP Object Name:** csDiskUsageThreshold

**SNMP OID:** .1.3.6.1.4.1.6889.2.18.1.1.1.0.8

**SNMP Object Description:** Disk usage has exceeded.

**Remediation Suggestions:** Use the Linux df command to narrow down the affected partition and then perform clean up. For example, the removal of core files or old log files.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACORE00008</td>
<td>Disk: disk usage exceeded 80%</td>
<td>Yes</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>ACORE00010</td>
<td>Log disk exceeded 90% storage</td>
<td>Yes</td>
<td>Yes</td>
<td>Minor</td>
</tr>
<tr>
<td>ACORE00011</td>
<td>Log disk automatically cleared upto 70%</td>
<td>Yes</td>
<td>Yes</td>
<td>Cleared</td>
</tr>
</tbody>
</table>

**Note:** Application Enablement Services supports the alarm code ACORE00010 and ACORE00011 of csDiskUsageThreshold alarm from Release 8.1.2 and later.

**SNMP Object Name:** csDiskFull

**SNMP OID:** .1.3.6.1.4.1.6889.2.18.1.1.1.0.9

**SNMP Object Description:** Disk is full.

**Remediation Suggestions:** Use the Linux df command to narrow down the affected partition and then perform clean up. For example, remove core files or old log files.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACORE00009</td>
<td>Disk: disk is full</td>
<td>Yes</td>
<td>Yes</td>
<td>Major</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** csCPUUtilization

**SNMP OID:** .1.3.6.1.4.1.6889.2.18.1.1.2.0.1

**SNMP Object Description:** CPU utilization is at least 80%.

**Remediation Suggestions:** Using the information in the SNMP Trap/Notification and possible the Linux top command to investigate and determine the service or services that is using an excessive amount of the CPU time. This maybe a service not operating correctly or the load on the server may need to be distributed.
### Alarm Code

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACORE00021</td>
<td>CPU: CPU utilization exceeded 80%</td>
<td>Yes</td>
<td>Yes</td>
<td>Minor</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** csSecurityFileModified  
**SNMP OID:** .1.3.6.1.4.1.6889.2.18.1.1.3.0.4  
**SNMP Object Description:** File modified.  
**Remediation Suggestions:** Review the Tripwire report to determine the modified file to take the appropriate corrective action. Afterwards update the Tripwire database.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACORE00044</td>
<td>Security: a file has been modified illegally</td>
<td>No</td>
<td>Yes</td>
<td>Minor, Major, or Critical</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** csSecurityFileRemoved  
**SNMP OID:** .1.3.6.1.4.1.6889.2.18.1.1.3.0.5  
**SNMP Object Description:** File Removed.  
**Remediation Suggestions:** Review the Tripwire report to determine the deleted file to take the appropriate corrective action. Afterwards update the Tripwire database. For log and trace files refer the log and trace retention policy list.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACORE00045</td>
<td>Security: a file has been removed illegally</td>
<td>No</td>
<td>Yes</td>
<td>Minor, Major, or Critical</td>
</tr>
<tr>
<td>ACORE00048</td>
<td>Logs are deleted manually.</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
<tr>
<td>ACORE00049</td>
<td>Traces are deleted manually.</td>
<td>No</td>
<td>Yes</td>
<td>Warning</td>
</tr>
</tbody>
</table>

**Note:**  
Application Enablement Services supports the alarm code ACORE00048 and ACORE00049 of csSecurityFileRemoved alarm from Release 8.1.2 and later.

**SNMP Object Name:** csSecurityFileAdded  
**SNMP OID:** .1.3.6.1.4.1.6889.2.18.1.1.3.0.6  
**SNMP Object Description:** File Added.  
**Remediation Suggestions:** Review the Tripwire report to determine the added file to take the appropriate corrective action. Afterwards update the Tripwire database.
### AEServicesSNMPtrapsAlarmCodesAndMessages_Part5

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACORE00046</td>
<td>Security: a file has been added to the system in an illegal directory</td>
<td>No</td>
<td>Yes</td>
<td>Minor, Major, or Critical</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** csSecurityInitFailed

**SNMP OID:** 1.3.6.1.4.1.6889.2.18.1.1.3.0.7

**SNMP Object Description:** Failed initialization of Tripwire database.

**Remediation Suggestions:** Review the Tripwire logs and take the appropriate actions.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACORE00047</td>
<td>Security: tripwire failed to initialize the tripwire database</td>
<td>No</td>
<td>Yes</td>
<td>Major</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** csWatchdogProcessUp

**SNMP OID:** 1.3.6.1.4.1.6889.2.18.1.1.4.0.10

**SNMP Object Description:** Process is up.

**Remediation Suggestions:** N/A

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES319</td>
<td>Started [watched] &lt;service name&gt;</td>
<td>Yes</td>
<td>Yes</td>
<td>Minor</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** csWatchdogProcessDown

**SNMP OID:** 1.3.6.1.4.1.6889.2.18.1.1.4.0.11

**SNMP Object Description:** Process is down.

**Remediation Suggestions:** If stopping the process was planned, do nothing. Otherwise, review the watchdog logs, review the logs of the affected service and take the appropriate actions to start the service.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Alarm Message</th>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES320</td>
<td>Unit: &lt;service name&gt; entered failed state</td>
<td>Yes</td>
<td>Yes</td>
<td>Major</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** csWatchdogProcessDead

**SNMP OID:** 1.3.6.1.4.1.6889.2.18.1.1.4.0.12

**SNMP Object Description:** Process is dead.

**Remediation Suggestions:** Review the watchdog logs, the logs of the affected service and take the appropriate actions to start the service.
### Alarm Code: AAES321

**Alarm Message:** Start request repeated too quickly for `<service name>`

<table>
<thead>
<tr>
<th>INADS Trap</th>
<th>NMS Trap</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Minor</td>
</tr>
</tbody>
</table>

**SNMP Object Name:** avAesUserAccountModified

**SNMP OID:** .1.3.6.1.4.1.6889.2.27.2.2.2.3.0.5

**SNMP Object Description:** Indicator of user account modification.

**Remediation Suggestions:** If the failure is excessive, either use the information contained in the SNMP trap or notification, or review the Linux server security log to determine the offending user and IP address to take appropriate action.

<table>
<thead>
<tr>
<th>Alarm Code</th>
<th>Event ID</th>
<th>Alarm Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAES113</td>
<td>O_AACCOUNT-00001</td>
<td>New user account created.</td>
</tr>
<tr>
<td>AAES114</td>
<td>O_AACCOUNT-00002</td>
<td>User account locked or unlocked.</td>
</tr>
<tr>
<td>AAES115</td>
<td>O_AACCOUNT-00003</td>
<td>User account modified.</td>
</tr>
<tr>
<td>AAES116</td>
<td>O_AACCOUNT-00004</td>
<td>User account removed.</td>
</tr>
</tbody>
</table>
Chapter 15: Administering Geo High Availability

Administering the Geo Redundant High Availability (GRHA)

This chapter describes how to configure and manage the GRHA feature. GRHA is a high availability solution that works across two datacenters with a pair of servers connected over a routable network. When the standby AE Services server is activated, AE Services will start providing service approximately a minute after the failure detection interval is over. However, all AE Services clients, other than DMCC clients have to re-establish all monitors/registrations as if they are working with an AE Services server that just came up after a reboot.

⚠️ Important:

- Before configuring GRHA, new Linux users that are created on the primary server must be created on the secondary server as well.

- You must log in to the OAM using the customer credentials and reset the user password because AE Services 7.1 does not restore the Linux password after migration.

- When upgrading from pre–7.1.x, AE Services does not restore the `/etc/shadow` file which results in the login issue with the cust and the root passwords. If you face the login issue, you must log in to the AE Services virtual machine using command line interface after the deployment and reset the cust and the root password to the previous AE Services values and then perform the restore operation. Alternately, you can set the cust and root passwords on the previous AE Services version to the values you set during the 7.1.x and 8.x deployment and perform the backup and restore the `/etc/shadow` file on the AE Services 7.1.x and 8.x virtual machine.

- The active and standby servers should have the same encryption setting. That is either both servers should be encrypted or both should be not encrypted.

🌟 Note:

- The IP network round trip time between two AE Services servers must be less than 100 milliseconds.

- GRHA is now supported in the AE Services Release 7.0 and later for VMware only. The use of Machine Preserving High Availability (MPHA) and Fast Reboot High Availability (FRHA) modes are not supported in the AE Services Release 7.0.
To use the GRHA feature, perform the following steps:

1. Make sure you have the appropriate information for the GRHA feature. See Configuration worksheet for Geo Redundant High Availability on page 272.
2. Configure and start GRHA, see Configuring Geo Redundant High Availability on page 275.

**Note:**

- You cannot change the AE Services IP address or hostname once GRHA is enabled. To change the hostname or IP address on either AE Services server, you must first disable GRHA.

- If you performed a backup when Geo Redundant High Availability was enabled and then restored that backup file when GRHA is removed, you must remove the GRHA configuration from the AE Services Management Console to be able to enable HA. See Removing Geo Redundant High Availability on page 279.

- You cannot change the AE Services Virtual IP addresses once GRHA is enabled. To change the Virtual IP addresses on either AE Services server, you must first disable GRHA.

- You cannot use Virtual IP address with enterprise-wide licensing. You must configure the primary AE Services IP address on the WebLM server for enterprise licence to work properly.

If standby or secondary AE Services server becomes the primary server, you must update the AE Services IP address on the WebLM server manually before the license grace period of 30 days expires.

For more information, see the Enterprise Licensing topic in the Administering standalone Avaya WebLM guide.

- The Virtual IP addresses and both AE Services server IP addresses must be in the same subnet. For two data centers with different subnets, one possible solution is to use an extended subnet between the data centers.

- For GRHA configuration both active and standby servers must be on the same platform and profile. For example, if the active AE Services server is on VMware with profile 1, the standby AE Services server must also be on VMware with profile 1.

Related links

- Configuration worksheet for Geo Redundant High Availability on page 272
- About Eth0 Virtual IP Address on page 274
- Configuring Geo Redundant High Availability on page 275
- Adding ping targets for Geo Redundant High Availability on page 276
- Starting Geo Redundant High Availability on page 277
- Stopping Geo Redundant High Availability on page 277
- Synchronizing Geo Redundant High Availability on page 277
- Switching to the standby server in Geo Redundant High Availability (interchange) on page 278
- Suspending Geo Redundant High Availability on page 278
- Unsuspending Geo Redundant High Availability on page 279
Configuration worksheet for Geo Redundant High Availability

To configure the Geo Redundant High Availability feature for AE Services, you must have the information listed in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local AE Server HostName</td>
<td>This is a display only field. The host name is configured when AE Services application is installed. The host name of the local AE Server.</td>
</tr>
<tr>
<td>Local AE Server IP Address</td>
<td>This is a display only field. The IP address is configured when AE Services application is installed. The IP address of the AE Server.</td>
</tr>
<tr>
<td>Remote AE Server IP Address</td>
<td>IP address of the remote AE Services server.</td>
</tr>
<tr>
<td>Remote AE Server User Name</td>
<td>User name of any user who is a part of the super user group and has access to linux shell. The default is cust.</td>
</tr>
<tr>
<td>Remote AE Server User Password</td>
<td>The password of the remote user.</td>
</tr>
<tr>
<td>Eth0 Virtual IP Address (optional)</td>
<td>The virtual IP address, which is used by the active AE Server. This field is optional.</td>
</tr>
<tr>
<td>Eth1 Virtual IP Address (optional)</td>
<td>The virtual IP address, which is used by the active AE Server. This field is optional.</td>
</tr>
<tr>
<td>Eth2 Virtual IP Address (optional)</td>
<td>The virtual IP address, which is used by the active AE Server. This field is optional.</td>
</tr>
<tr>
<td>Failure Detection Interval</td>
<td>The Failure Detection Interval determines how long you want AE Services to wait before the standby AE Services server becomes active if the standby AE Services server cannot reach the current active AE Services server. The range is 1 - 3600 seconds. The default value is 600 seconds.</td>
</tr>
</tbody>
</table>
### Field Description

**Preferred Active Node (optional)**
The IP address of the preferred active node. The default value is empty.

If Preferred Active Node is administered, during split brain resolution the preferred node will be chosen as the active AE Services server. If Preferred Active Node is not administered, the current active AE Services server remains active. Split brain is a condition when both AE Services servers are running in active mode due to network failure. When the network between the AE Services servers comes up, you must keep only one AE Services server active.

This field is optional.

**System Type**
The system type is based on the number of individual licenses allocated for this AE Services server. The system depends on the number of other AE Services licenses used on the AE Services server based on the following table. Choices are Small, Medium, and Large.

<table>
<thead>
<tr>
<th></th>
<th>HA Small License</th>
<th>HA Medium License</th>
<th>HA Large License</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLG (on/off)</td>
<td>NA</td>
<td>NA</td>
<td>HA Large required</td>
</tr>
<tr>
<td>CVLAN (on/off)</td>
<td>NA</td>
<td>NA</td>
<td>HA Large required</td>
</tr>
<tr>
<td>AE Services Advanced Small Switch</td>
<td>HA Small required</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>AE Services Advanced Medium Switch</td>
<td>NA</td>
<td>HA Medium required</td>
<td>OK</td>
</tr>
<tr>
<td>AE Services Advanced Large Switch</td>
<td>NA</td>
<td>NA</td>
<td>HA Large required</td>
</tr>
<tr>
<td>TSAPI Simultaneous Users</td>
<td>&lt;= 1000</td>
<td>&gt; 1000 and &lt;= 5000</td>
<td>&gt; 5000</td>
</tr>
<tr>
<td>Unified CC API Desktop Edition</td>
<td>&lt;= 1000</td>
<td>&gt; 1000 and &lt;= 5000</td>
<td>&gt; 5000</td>
</tr>
<tr>
<td>Device Media and Call Control</td>
<td>&lt;= 500</td>
<td>&gt; 500 and &lt;= 1000</td>
<td>&gt; 1000</td>
</tr>
</tbody>
</table>

**Note:**

If an application exceeds the use of AE Services individual licenses for a configured Geo Redundant High Availability system size, AE Services Geo Redundant High Availability will enter the Geo Redundant High Availability license violation state. Once in the Geo Redundant High Availability license violation state, Geo Redundant High Availability will prohibit failover for any reason until the license violation state is cleared. There are two ways to clear the license violation state:

- Acquire and install a higher level Geo Redundant High Availability license that is appropriate to AE Services individual license usage.
Call Avaya Services to clear the violation state.

Reducing the usage of AE Services individual licenses after the license violation state is reached will not clear the license violation state.

Related links

Administering the Geo Redundant High Availability (GRHA) on page 270

About Eth0 Virtual IP Address

AE Services Server supports a virtual IP address for each of the `eth0`, `eth1` and `eth2` interfaces. To be able to administer a virtual IP address, these interfaces must have a valid IP address. AE Services continues to support HA configuration without any virtual IP addresses configured. In such a configuration, the AE Services Server client applications connect one of the two IP addresses associated with each of AE Services Servers’ client connectivity interfaces. This is dependant on the AE Services Server that is active.

GRHA is enhanced with the following changes:

1. Registration states are replicated, as they happen over a newly created socket (TLS) connection between active and standby AE Services server.

2. Registration states are kept in memory in the `/dev/shm/resq` directory.

   **Note:**

   `/dev/shm` is a memory file system.

3. Virtual IP addresses can be configured for public, private and OOBM interfaces.

Since GRHA performs a synchronous update for session states, it can be used in place of FRHA.

Using virtual IP addresses have significant advantages:

- The client application can use the same IP address to connect to the active AE Services GRHA server. The client application does not have to maintain two different AE Services Server IP addresses
- If a virtual IP address is also used for Switch and Media Connectivity, any DMCC associations that are currently in place at the time of a GRHA fail-over will be automatically recovered by the new active AE Services Services server. The associations include the following:
  - DMCC client sessions
  - DMCC devices and device monitors
  - DMCC station registrations
  - DMCC call associations
  - DMCC system registrations.

Related links

Administering the Geo Redundant High Availability (GRHA) on page 270
Configuring Geo Redundant High Availability

About this task
Follow this procedure to configure and start the Geo Redundant High Availability feature.

Procedure

1. From the AE Services Management Console, select High Availability.
2. On the High Availability Status page, click Configure HA.
   
   The High Availability Configuration page appears.

3. In the Remote AE Services Server IP Address field, enter the IP address of the remote AE Services server.

4. In the Remote AE Services Server User Name field, enter the user name of the AE Services server.

5. In the Remote AE Services Server User Password field, enter the password.

6. In the Eth0 Virtual IP Address—optional field, enter the virtual IP address, which is used by the active AE Services server. This field is optional.

7. In the Eth1 Virtual IP Address—optional field, enter the virtual IP address, which is used by the active AE Services server. This field is optional, and can be configured to be used for private network.

8. In the Eth2 Virtual IP Address—optional field, enter the virtual IP address, which is used by the active AE Services server. This field is optional, and can be configured to be used for out of band network.

9. In the Failure Detection Interval field, enter the number of seconds for the Failure Detection Interval. The Failure Detection Interval determines how long you want AE Services to wait before the standby AE Services server becomes active if AE Services cannot reach the current active AE Services server. The range is 1-3600 seconds. The default value is 600 seconds.

10. In the Preferred Active Node—optional field, enter the IP address of the preferred active node. The default value is empty (none). This field is optional.

11. In the System Type area, select the appropriate system type. The system type is based on the number of individual licenses allocated for this AE Services server. The system depends on the number of other AE Services licenses used on the AE Services server based on the table in Configuration worksheet for Geo Redundant High Availability on page 272.

12. Click Apply Changes.


15. On the Start HA Confirmation page, click Apply.
Adding ping targets for Geo Redundant High Availability

About this task
Follow this procedure to add ping targets for the Geo Redundant High Availability feature. Ping targets are used to determine the health of a specific network up to a specific network node. Using ping targets, you can gauge the health of the network and determine which AE Services server should be active.

Adding ping targets is an optional procedure.

Procedure

1. From the AE Services Management Console, select **High Availability**.
2. On the High Availability Status page, click **Configure HA**.
   The High Availability Configuration page appears.
3. In the Ping Targets area, click **Add Ping Target**.
   A new, blank row appears for the ping target you want to add.
4. Click the check box next to the new ping target.
5. In the Ping Target (IP Address/Hostname) box, enter the IP address or hostname of the appropriate network node.

   **Note:**
   Only IPv4 addresses are supported.
6. In the Interval (sec) box, enter the interval. The default is 60 seconds.
7. In the Timeout (sec) box, enter the timeout interval for this target. The default is 600 seconds.
8. In the Interval AFF (sec) box, enter the interval after first failure value. The default is 60 seconds.
9. If you want to add additional ping targets, repeat steps 3 through 8.
10. When finished adding ping targets, click **Apply Changes**.
11. On the High Availability Configuration Confirmation page, click **Apply**.

Related links

- [Administering the Geo Redundant High Availability (GRHA)](on page 270)
Starting Geo Redundant High Availability

Before you begin
Geo Redundant High Availability is configured and in the stopped state.

About this task
Follow this procedure to start Geo Redundant High Availability.

Procedure
1. From the AE Services Management Console, select High Availability.
2. On the High Availability Status page, click Start.
3. On the Start HA Confirmation page, click Apply.

Related links
Administering the Geo Redundant High Availability (GRHA) on page 270

Stopping Geo Redundant High Availability

Before you begin
Geo Redundant High Availability must be running.

About this task
Follow this procedure to stop Geo Redundant High Availability.

Procedure
1. From the AE Services Management Console, select High Availability.
2. On the High Availability Status page, click Stop.
3. On the Stop HA Confirmation page, click Apply.

Related links
Administering the Geo Redundant High Availability (GRHA) on page 270

Synchronizing Geo Redundant High Availability

Before you begin
Geo Redundant High Availability is configured and running.

About this task
Follow this procedure to synchronize the active and standby servers configured for Geo Redundant High Availability.
Note:

• You may want to synchronize the active and standby servers after you make changes to the AE Services configuration.

• Synchronization is performed automatically after Geo Redundant High Availability is started and every minute after that.

• Configuration changes are copied automatically to the standby server every two minutes.

• DMCC active session states are copied to the standby instantaneously.

Procedure

1. From the AE Services Management Console, select **High Availability**.
2. On the High Availability Status page, click **Synchronize**.
3. On the High Availability Synchronize Confirmation page, click **Apply**.

Related links

[Administering the Geo Redundant High Availability (GRHA)](page 270)

Switching to the standby server in Geo Redundant High Availability (interchange)

Before you begin
Geo Redundant High Availability is configured and running.

About this task
Follow this procedure to make:

• the current active AE Services server become the standby AE Services server
• the current standby AE Services server become the active AE Services server

Procedure

1. From the AE Services Management Console, select **High Availability**.
2. On the High Availability Status page, click **Interchange**.
3. On the High Availability Interchange Confirmation page, click **Apply**.

Related links

[Administering the Geo Redundant High Availability (GRHA)](page 270)

Suspending Geo Redundant High Availability

Before you begin
Geo Redundant High Availability is configured and running.
About this task
Follow this procedure to suspend Geo Redundant High Availability.

Procedure
1. From the AE Services Management Console, select High Availability.
2. On the High Availability Status page, click Suspend.
3. On the Suspend HA Confirmation page, click Apply.

Related links
Administering the Geo Redundant High Availability (GRHA) on page 270

Unsuspending Geo Redundant High Availability

Before you begin
Geo Redundant High Availability is in the suspended state.

About this task
Follow this procedure to unsuspend Geo Redundant High Availability.

Procedure
1. From the AE Services Management Console, select High Availability.
2. On the High Availability Status page, click Unsuspend.
3. On the Unsuspend HA Confirmation page, click Apply.

Related links
Administering the Geo Redundant High Availability (GRHA) on page 270

Removing Geo Redundant High Availability

Before you begin
Geo Redundant High Availability is configured or in the running state.

About this task
Follow this procedure to remove Geo Redundant High Availability.

Note:
If Geo Redundant High Availability is running when you perform this procedure, Geo Redundant High Availability will first be stopped, and then the configuration will be removed.

Procedure
1. From the AE Services Management Console, select High Availability.
2. On the High Availability Status page, click Remove HA.
3. On the Remove HA Confirmation page, click **Apply**.

**Related links**

[Administering the Geo Redundant High Availability (GRHA)](#) on page 270
Chapter 16: Dial plan administration in AES

Dial plan administration in AE Services

Configurations that require dial plan administration

Dial Plan settings apply to the following types of configurations only:

- AE Services integration is not supported with IBM Sametime due to software limitations and security concerns.
- AE Services implementation with Microsoft Lync Server 2010 and 2013 (AE Services implementation for Microsoft Lync Server)
- AE Services with DMCC clients using E.164ConversionServices
- AE Services with DMCC applications working in TelURI mode. For more information, see the following documents:
  - Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer’s Guide, 02-300359
  - Avaya Aura® Application Enablement Services Device, Media, and Call Control XML Programmer’s Guide, 02-300358
  - Avaya Aura® Application Enablement Services Device, Media and Call Control API .NET Programmer’s Guide, 02-602658

★ Note:
For more information about the From and To TelURI operations, see How different APIs or offers use the TelURI settings on page 294.

★ Note:
AE Services integration with Microsoft Office Live Communications Server 2005 and Microsoft Office Communications Server 2007 support is stopped as Microsoft has ended its support for Microsoft Office Live Communications Server 2005 on 01/09/2018 and Microsoft Office Communications Server 2007 on 07/10/2007.
Dial plan administration in AE Services refers to setting up tables that convert TelURI numbers and dial strings for a switch connection. TelURI is an abbreviation for Telephony Uniform Resource Identifier.

- The AE Services Dial Plan pages in the Management Console use the From TelURI table to convert Tel URI phone numbers to dial strings. See General tips for setting up From TelURI conversion rules on page 283 for more information.
- The AE Services Dial Plan pages in the Management Console use the To TelURI table to convert dial strings to TelURI numbers. General tips for setting up To TelURI conversion rules on page 283 for more information.

**Important:**

To administer the dial plan settings in AE Services, you need to know how the dial plan is administered on Communication Manager. If you do not know what the dial plan settings are for a particular switch or set of switches, contact the Communication Manager administrator.

### Dial plan processing requirements - TelURI formats that AE Services supports

AE Services support the following TelURI formats. The preferred format is E.164, except in cases where the extension bears no resemblance to the E.164 numbers.

<table>
<thead>
<tr>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>E.164</td>
<td>tel:+13031234567</td>
</tr>
<tr>
<td>E.164PlusExt</td>
<td>tel:+13031234567;ext=1234567</td>
</tr>
<tr>
<td>extOnly</td>
<td>tel:5389000;phone-context=&lt;domain&gt;</td>
</tr>
<tr>
<td></td>
<td>where &lt;domain&gt; can be any organization’s domain name</td>
</tr>
<tr>
<td></td>
<td>tel:1234567;phone-context=example.com</td>
</tr>
</tbody>
</table>

**Calling device and monitored device ID formats**

AE Services requires the calling device and monitored devices to be in either E.164PlusExt format or E.164 format. The extOnly format should be used only if there is no correlation between the E.164 number and the extension.

**Called device ID formats**

Called device IDs can be in either E.164 format or E.164PlusExt format; called device IDs will not be in E.164PlusExt format.
General tips for setting up From TelURI conversion rules

The **From TelURI** table determines the way that AE Services processes inbound E.164 numbers. Generally speaking, AE Services applies matching criteria to the incoming number. When the number satisfies the matching criteria, AE Services manipulates the digits and provides the results to the requester (only one rule is applied for each number). When setting up the From TelURI settings, you can specify up to 200 rules. Each row in the table represents a rule. The rules are processed in order from top to bottom.

If you have a rule that contains a wildcard (* - asterisk) for the Minimum Length, Maximum Length, and Pattern match, it always must be the last rule in the list, and it must be a single asterisk (by itself). If you need to treat the asterisk as a literal in either the Pattern Match or the Replacement fields, you must precede it with a backslash, for example: \\
*. Also, if your dial plan uses a number sign and you need to treat it as a literal in the Pattern Match field, you must precede it with a backslash.

<table>
<thead>
<tr>
<th>Minimum Length</th>
<th>Maximum Length</th>
<th>Pattern Match</th>
<th>Delete Length</th>
<th>Replacement</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>11</td>
<td>1303538</td>
<td>4</td>
<td>(blank)(^1)</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>1303</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>*</td>
<td>*</td>
<td>*</td>
<td>0</td>
<td>9011</td>
</tr>
</tbody>
</table>

1. Blank means the replacement field is empty.

General tips for setting up To TelURI conversion rules

The **To TelURI** table determines the way that the AE Services processes outbound E.164 numbers. Generally speaking, AE Services applies matching criteria to the outgoing number. When the number satisfies the matching criteria, AE Services manipulates the digits and provides the results to the requestor (only one rule is applied for each number). When setting up the To TelURI settings, you can specify up to 200 rules. Each row in the table represents a rule. The rules are processed in order from top to bottom.

If you have a rule that contains a wildcard (* - asterisk) for the Minimum Length, Maximum Length, and Pattern match, it always must be the last rule in the list, and it must be a single asterisk (by itself). If you need to treat the asterisk as a literal in either the Pattern Match or the Replacement fields, you must precede it with a backslash, for example: \\
*. Also, if your dial plan uses a number sign and you need to treat it as a literal in the Pattern Match field, you must precede it with a backslash.

<table>
<thead>
<tr>
<th>Minimum Length</th>
<th>Maximum Length</th>
<th>Pattern Match</th>
<th>Delete Length</th>
<th>Replacement</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>7</td>
<td>538</td>
<td>0</td>
<td>1303</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>852</td>
<td>0</td>
<td>1732</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>*</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
Sample of setting up From TelURI conversion rules for a dial plan with fixed-length extensions

The following example depicts From TelURI conversion rules for a switch that uses fixed-length-extensions in its dial plan. This sample switch supports three different extension prefixes: 538, 852, and 444. The 538 prefix is used for extensions hosted on that switch, and the other two prefixes are used for switches connected via QSIG.

Example - From TelURI rules for fixed-length extensions

The following table contains sample conversion rules.

<table>
<thead>
<tr>
<th>Minimum Length</th>
<th>Maximum Length</th>
<th>Pattern Match</th>
<th>Delete Length</th>
<th>Replacement</th>
</tr>
</thead>
<tbody>
<tr>
<td>A 11</td>
<td>11</td>
<td>1303538</td>
<td>4</td>
<td>(blank)¹</td>
</tr>
<tr>
<td>B 11</td>
<td>11</td>
<td>1732852</td>
<td>4</td>
<td>(blank)</td>
</tr>
<tr>
<td>C 11</td>
<td>11</td>
<td>1720444</td>
<td>4</td>
<td>(blank)</td>
</tr>
<tr>
<td>D 11</td>
<td>11</td>
<td>1303</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>E 11</td>
<td>11</td>
<td>1720</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>F 11</td>
<td>11</td>
<td>1</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td>G *</td>
<td>*</td>
<td>*</td>
<td>0</td>
<td>9011</td>
</tr>
</tbody>
</table>

1. Blank means the replacement field is empty.

Example - how the From TelURI rules process numbers for fixed-length extensions

The following table describes how From TelURI rules process numbers for fixed length extensions in Example - From TelURI rules for fixed-length extensions on page 284.

<table>
<thead>
<tr>
<th></th>
<th>AE Services receives +13035381234, an 11-digit number. Because the number is within the minimum and maximum length requirements, and the first 7 digits (1303538) are a pattern match, AE Services deletes the first 4 digits (1303) and does not prepend any digits. The resulting number is 5381234.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>AE Services receives +17328521234, an 11-digit number. Because the number is within the minimum and maximum length requirements, and the first 7 digits (1732852) are a pattern match, AE Services deletes the first 4 digits (1732) and does not prepend any digits. The resulting number is 8521234.</td>
</tr>
<tr>
<td>B</td>
<td>AE Services receives +17204441234, an 11-digit number. Because the number is within the minimum and maximum length requirements, and the first 7 digits (1720444) are a pattern match, AE Services deletes the first 4 digits (1720) and does not prepend any digits. The resulting number is 4441234 to the switch.</td>
</tr>
<tr>
<td>C</td>
<td>AE Services receives +13036791234, an 11-digit number. Because the number is within the minimum and maximum length requirements, and the first 4 digits (1303) are a pattern match, AE Services deletes the first digit (1), and prepends 9 to the number. The resulting number is 93036791234.</td>
</tr>
</tbody>
</table>

Table continues…
Sample of setting up To TelURI conversion rules for a dial plan with fixed-length extensions

The following example depicts To TelURI conversion rules for a switch that uses fixed-length-extensions in its dial plan. This switch supports three different extension prefixes: 538, 852, and 444. The 538 prefix is used for extensions hosted on that switch, and the other two prefixes are used for switches connected via QSIG.

Example - To TelURI rules for fixed-length extensions

The following table contains sample conversion rules.

<table>
<thead>
<tr>
<th></th>
<th>Minimum Length</th>
<th>Maximum Length</th>
<th>Pattern Match</th>
<th>Delete Length</th>
<th>Replacement</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>7</td>
<td>7</td>
<td>538</td>
<td>0</td>
<td>1303</td>
</tr>
<tr>
<td>B</td>
<td>7</td>
<td>7</td>
<td>852</td>
<td>0</td>
<td>1732</td>
</tr>
<tr>
<td>C</td>
<td>7</td>
<td>7</td>
<td>444</td>
<td>0</td>
<td>1720</td>
</tr>
<tr>
<td>E</td>
<td>5</td>
<td>5</td>
<td>2</td>
<td>0</td>
<td>173285</td>
</tr>
<tr>
<td>F</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>0</td>
<td>172044</td>
</tr>
<tr>
<td>G</td>
<td>10</td>
<td>10</td>
<td>*</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Example - how the To TelURI rules process numbers for fixed-length extensions

The following table describes how To TelURI rules process numbers for fixed length extensions in Example - To URI rules for fixed-length extensions on page 285.

A  | AE Services receives 5381234, a 7 digit number. Because the number is within the minimum and maximum length requirements, and the first three digits (538) are a pattern match, AE Services deletes no digits, and prepends 1303 to the number. The resulting number is +13035381234.

B  | AE Services receives 8521234, a 7 digit number, from the switch. Because the number is within the minimum and maximum length requirements, and the first three digits (852) are a pattern match, AE Services deletes no digits, and prepends 1732 to the number. The resulting number is +17328521234.

Table continues…
AE Services receives 4441234, a 7-digit number, from the switch. Because the number is within the minimum and maximum length requirements, and the first three digits (444) are a pattern match, AE Services deletes no digits, and prepends 1720 to the number. The resulting number is +17204441234.

AE Services receives *510, from the switch. Because the number is within the minimum and maximum length requirements, and the first character in the dial string will be an asterisk, you must precede it with a backslash. AE Services does not delete or replace any characters. The resulting dial string is *510.

AE Services will sometimes receive a 5-digit extension from a networked switch, even if the local dial plan is 7 digits (see Tips for dial plan settings with networked switches on page 290). In this case, AE Services receives a 5-digit number 21234. Based on the matching pattern of 2 at the beginning, AE Services prepends 173285 to the number. The resulting number is +17328521234.

AE Services will sometimes receive a 5-digit extension from a networked switch, even if the local dial plan is 7 digits (see Tips for dial plan settings with networked switches on page 290). In this case, AE Services receives a 5-digit number 41234. Based on the matching pattern of 4 at the beginning, AE Services prepends 172044 to the number. The resulting number is +17204441234.

AE Services receives a 10-digit number, 2126711234. Based on the matching pattern of any 10-digit string, AE Services deletes no digits and prepends 1 to the number. The resulting number is +1212671123.

Sample of setting up From TelURI conversion rules for a switch with variable length extensions

The following example depicts From TelURI settings for a switch that uses variable length extensions in its dial plan. This example assumes the following:

- The customer owns numbers +49697100 through +49697105 in the dial plan, but does not own +49697106 and higher.
- The dial plan accommodates 1- to 4-digit extensions
- The ARS code is 0, the inter-region code is 0, and the international dial code is 00. The ARS code, which in this case is 0, is always included before the inter-region code and international dial code.

Example - From TelURI rules for variable length extensions

The following table contains sample conversion rules.

<table>
<thead>
<tr>
<th>Minimum Length</th>
<th>Maximum Length</th>
<th>Pattern Match</th>
<th>Delete Length</th>
<th>Replacement</th>
</tr>
</thead>
<tbody>
<tr>
<td>A 8</td>
<td>11</td>
<td>49697100</td>
<td>7</td>
<td>(blank)¹</td>
</tr>
<tr>
<td>B 8</td>
<td>11</td>
<td>49697101</td>
<td>7</td>
<td>(blank)</td>
</tr>
<tr>
<td>C 8</td>
<td>11</td>
<td>49697102</td>
<td>7</td>
<td>(blank)</td>
</tr>
<tr>
<td>D 8</td>
<td>11</td>
<td>49697103</td>
<td>7</td>
<td>(blank)</td>
</tr>
<tr>
<td>E 8</td>
<td>11</td>
<td>49697104</td>
<td>7</td>
<td>(blank)</td>
</tr>
</tbody>
</table>

Table continues…
Example - how the From TelURI rules process numbers for variable length extensions

The following table describes how From TelURI rules process numbers for fixed length extensions in Example - how the From TelURI rules process numbers for variable length extensions on page 286.

<table>
<thead>
<tr>
<th>Minimum Length</th>
<th>Maximum Length</th>
<th>Pattern Match</th>
<th>Delete Length</th>
<th>Replacement</th>
</tr>
</thead>
<tbody>
<tr>
<td>F 8</td>
<td>11</td>
<td>49697105</td>
<td>7</td>
<td>(blank)</td>
</tr>
<tr>
<td>G *</td>
<td>*</td>
<td>4969</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>H *</td>
<td>*</td>
<td>49</td>
<td>2</td>
<td>00</td>
</tr>
<tr>
<td>I 9</td>
<td>9</td>
<td>46357</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>J *</td>
<td>*</td>
<td>*</td>
<td>0</td>
<td>000</td>
</tr>
</tbody>
</table>

1. Blank means the replacement field is empty.

Example - how the From TelURI rules process numbers for variable length extensions

The following table describes how From TelURI rules process numbers for fixed length extensions in Example - how the From TelURI rules process numbers for variable length extensions on page 286.

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>AE Services receives +49697100, an 8-digit number. Because the number is within the minimum and maximum length requirements, and the number is an exact pattern match, AE Services deletes the first 7 digits (4969710) and does not prepend any digits to the number. The resulting number is 0.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>AE Services receives +49697101988, an 11-digit number. Because the number is within the minimum and maximum length requirements, and the first 8 digits (49697101) are a pattern match, AE Services deletes the first 7 digits and does not prepend any digits to the number. The resulting number is 1988.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>AE Services receives +4969710211, a 9-digit number. Because the number is within the minimum and maximum length requirements, and the first 8 digits (49697102) are a pattern match, AE Services deletes 7 digits and does not prepend any digits to the number. The resulting number is 211.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>AE Services receives +496971034, a 9-digit number. Because the number is within the minimum and maximum length requirements, and the first 8 digits (49697103) are a pattern match, AE Services deletes 7 digits and does not prepend any digits to the number. The resulting number is 34.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>AE Services receives +4969710494, a 10-digit number. Because the number is within the minimum and maximum length requirements, and the first 8 digits (49697104) are a pattern match, AE Services deletes 7 digits and does not prepend any digits to the number. The resulting number is 494.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>AE Services receives +4969710598, a 10-digit number. Because the number is within the minimum and maximum length requirements, and the first 8 digits (49697105) are a pattern match, AE Services deletes 7 digits and does not prepend any digits to the number. The resulting number is 598.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>AE Services receives +496971060, a 9-digit number. Because the wild card (*) permits a number of any length, and the first 4 digits (4969) are a pattern match, AE Services deletes the first 4 digits and prepends 0 to the number. The resulting number is 071060.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H</td>
<td>AE Services receives +49306441234, an 11-digit number from Communicator. Because the wild card (*) permits a number of any length, and the first 2 digits (49) are a pattern match, AE Services deletes the first 2 digits and prepends 00 to the number. The resulting number is 00306441234.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I</td>
<td>AE Services receives +4635746262, a 9-digit number from Communicator. Because the first 6 digits are a pattern match, AE Services deletes the first 6 digits and prepends *9 to the number.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>J</td>
<td>AE Services receives +17328521234, an 11 digit number. Because the minimum length, maximum length, and pattern match are set up with the wild card, any number is permitted. AE Services deletes no digits, prepends 000. The resulting number is 00017328521234.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Sample of setting up To TelURI conversion rules for a switch with variable length extensions

The following example depicts To TelURI conversion rules for a dial plan that uses variable-length extensions in its dial plan. The set of rules in this example assumes the following:

- All numbers less than or equal to 4 digits are extensions. This assumption allows the table to have one rule, rather than 6, for all extension starts. In some cases, it might be necessary to be more specific.
- International numbers start with 00, and inter-region numbers start with 0. Any digits other than 0 or 00 are assumed to be local digits. AE Services prepends 4969, which represents country or city codes. Keep in mind that you must carefully analyze your dial plan before you attempt to apply a catch-all rule such as this.

Example - To TelURI rules for variable length extensions

The following table contains sample conversion rules.

<table>
<thead>
<tr>
<th>Minimum Length</th>
<th>Maximum Length</th>
<th>Pattern Match</th>
<th>Delete Length</th>
<th>Replacement</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1</td>
<td>4</td>
<td>*</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>*</td>
<td>*</td>
<td>00</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>*</td>
<td>*</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>D</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>0</td>
</tr>
</tbody>
</table>

1. Blank means the replacement field is empty.

Example - how the To TelURI rules process numbers for variable length extensions

The following table describes how To TelURI rules process numbers for fixed length extensions in Example - To TelURI rules for variable length extensions on page 288.

| A | AE Services receives 1234, a 4-digit number. Because the number is within the minimum and maximum length requirements, and the wild card (*) permits a match of any 1- to 4-digit number, AE Services deletes no digits and prepends 4969710 to the number. The resulting number is 49697101234. |
| B | AE Services receives 0017328524321, a 13-digit number. Because the number is not within the range specified by the 1- to 4-digit rule (A) it satisfies this rule (B), which permits a number of any length where first two digits (00) are a pattern match. AE Services deletes the first 2 digits, prepends nothing to the number. The resulting number is 17328524321. |
| C | AE Services receives 0306441234, a 10-digit number. Because the number is not within the range specified by the 1- to 4-digit rule (A) it satisfies this rule (C), which permits a number of any length where first digit (0) is a pattern match. AE Services deletes the first digit, prepends 49 to the number. The resulting number is 49306441234. |

Table continues…
AE Services receives 45427, a 5-digit number. Because the number is not within the range specified by the 1- to 4-digit rule (A) it satisfies this “catch-all” rule that permits a number of any length and any pattern of digits. AE Services deletes no digits, prepends 4969 to the number. The resulting number is 496945427.

Pattern matching -- using Pattern and RegEx (regular expressions)

Pattern

Use Pattern when you want to use a digit string as a way of detecting the presence of a specific sequence of digits in an incoming dial string. When you select Pattern you can create a matching string based on literal digits (0 through 9), one character literal (the #), and one special character, the asterisk (*) which will match any digit or sequence of digits. If you select Pattern, valid dial string characters are: all digits (0-9), the number sign (#), and the asterisk (*).

RegEx

Use RegEx (regular expression) when you want to use a Java regular expression to analyze an incoming dial string. Regular expressions rely on symbolic notation - grouping of digits and special characters for analyzing incoming dial strings. For example, ([0-5]\d{0,3}) is a regular expression which matches extensions that start with digits 0 - 5, and are 1 to 4 digits in length.

Note:

You can mix rule types. You can create a From TelURI table that uses rules based on Pattern and rules based on RegEx.

Example - To TelURI rules that use RegEx

The following table contains sample conversion rules that include regular expression rules and simple pattern match rules.

<table>
<thead>
<tr>
<th>Min length</th>
<th>Max length</th>
<th>Pattern</th>
<th>Delete Length</th>
<th>Replacement</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td>4969710([0-5]\d{0,3})</td>
<td>$1</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td>4969(\d{1,})</td>
<td>0$1</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>*</td>
<td>49</td>
<td>2</td>
<td>00</td>
</tr>
<tr>
<td>C</td>
<td>*</td>
<td>*</td>
<td>1</td>
<td>000</td>
</tr>
</tbody>
</table>

Example - How the To TelURI rules process numbers that use RegEx

The following table describes how To TelURI rules process numbers that use RegEx in Example - To TelURI rules that use RegEx on page 289.
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A</strong></td>
<td>This rule uses a RegEx pattern to specify that Call Control Services is to look for a string starting with 4969710, matching an extension that starts with 0 through 5 and is 1 to 4 digits in length. The parentheses around the extension indicate a group, which is correlated with the $1 in the replacement string. The $1 says to replace the matching string (the entire E.164 number) with the group designated by the parentheses (the extension).</td>
</tr>
<tr>
<td><strong>B</strong></td>
<td>This rule uses a RegEx pattern to specify that Call Control Services is to look for a string starting with 4969, followed by 1 or more digits. The parentheses again correlate with the $1 in the replacement string, which says to take the group (the E.164 number without country code or city code) and to add a 0 in front of it (the ARS code).</td>
</tr>
<tr>
<td><strong>C</strong></td>
<td>This rule uses a simple pattern match. The asterisk in the Min and Max length permits a number of any length. The pattern indicates that Call Control Services is to look for a string starting with 49. When it detects 49, it deletes the first 2 digits, and replaces them with 00.</td>
</tr>
<tr>
<td><strong>D</strong></td>
<td>This rule uses a wildcard pattern match. The asterisk in the Min and Max length permits a number of any length, and the asterisk in the pattern permits pattern of digits. When any number that does not satisfy the first 3 rules (A,B, and C) is detected, Call Control Services deletes the first digit and replaces it with 000.</td>
</tr>
</tbody>
</table>

---

**Tips for dial plan settings with networked switches**

When switches are networked together using ISDN QSIG tie trunks or ISDN tie trunks, in some call scenarios Communication Manager sends extension numbers from the networked switch to the AE Server. The format of these extension numbers may be different than the format of local extension numbers.

To optimize the experience of Microsoft Lync users, be sure to administer “To TelURI” rules for the networked switch, or switches, as well as the local switch. Additionally, if the networked switch has a different extension length than the local switch, extensions might be reported with both the local extension length and the networked extension length. Be sure to administer “To TelURI” rules that can successfully convert both extension lengths for the networked switch.

Also, you might need multiple entries in the To TelURI rules for the networked switch if that switch has a different extension length than the local switch.

---

**Methods for administering dial plan settings**

In AE Services you can use either of the following methods to administer dial plan settings.

- You can administer the dial plan settings for one switch at a time. For more information, see [Administering dial plan settings on a per-switch basis](#) on page 291.
- You can administer default dial plan settings that are used for all switches. For more information, see [Administering default dial plan settings](#) on page 293.
Important:
In configurations with one AE Server supporting multiple switches, AE Services does not support Microsoft Office Communicator/Microsoft Lync control of the same extension on more than one switch.

Administering dial plan settings on a per-switch basis

About this task
AE Services uses the dial plan information to convert E.164 phone numbers to switch extensions (From TelURI) and switch extensions to E.164 phone numbers (To TelURI).

Note:
If your AE Services and Microsoft LCS/Lync configuration uses a number of switches that all have the same dial plan, use the procedure described in Administering default dial plan settings on page 293. By using the default settings, you enter the dial plan settings only once.

Follow this procedure to administer the dial plan settings for a switch connection you have already administered in AE Services.

Procedure
1. From the AE Services Management Console main menu, select Communication Manager Interface > Dial Plan > Switch Administration.
2. From the Switch Dial Plan Administration page, select the connection name for the switch you want to administer, for example aeslcsswitch, and click Detail.
3. On the Dial Plan Settings - Conversion Rules for aeslcsswitch page, in the From TelURI section, click Add.
4. From the Add Dial Plan - aeslcsswitch page, follow these steps to complete the From TelURI settings, based on your dial plan.

Important:
Refer to online help in the AE Services Management Console as you complete these fields.

a. In the Pattern Type check box, select Pattern or RegEx based on your dial plan rules. Pattern is the default.

b. In the Minimum length field, type a number from 1 to 21, or an asterisk (*) for any number, to specify the minimum number of characters expected in the telephone number (dial string).

c. In the Maximum Length field, type a number from 1 to 21, or an asterisk (*) for any number, to specify the maximum number of characters expected in the number (dial string).

d. In the Matching Pattern field, type a string of valid characters that you expect at the beginning of a dial string.
Valid characters are all digits (0-9), the number sign (#), and the asterisk (*). You can not specify a blank space or the plus sign (+) in this field.
e. In the **Delete length** field, type a number from 1 to 21 to specify the number of characters to delete from the beginning of the number (dial string).

f. In the **Replacement String** field, type a string of characters to be prepended to the number (dial string).

g. Click **Apply Changes**.

h. On the Add Dial Plan page, click **Apply**.

**Note:**

You have added one From TelURI conversion rule. If you want to add another From TelURI conversion rule, repeat Step 4.

5. On the **Dial Plan Settings - Conversion Rules for aeslcswitch** page, in the **To TelURI** section, click **Add**.

6. From the **Add Dial Plan - aeslcswitch** page, follow these steps to complete the **To TelURI** settings, based on your dial plan.

**Important:**

Refer to online help in the AE Services Management Console as you complete these fields.

a. In the **Pattern Type** check box, select **Pattern** or **RegEx** based on your dial plan rules. **Pattern** is the default.

b. In the **Minimum length** field, type a number from 1 to 21, or an asterisk (* ) for any number, to specify the minimum number of characters expected in the telephone number (dial string).

c. In the **Maximum Length** field, type a number from 1 to 21, or an asterisk (* ) for any number, to specify the maximum number of characters expected in the number (dial string).

d. In the **Matching Pattern** field, type a string of valid characters that you expect at the beginning of a dial string.

   Valid characters are all digits (0-9), the number sign (#), and the asterisk (*). You cannot specify a blank space or the plus sign (+) in this field.

e. In the **Delete length** field, type a number from 1 to 21 to specify the number of characters to delete from the beginning of the number (dial string).

f. In the **Replacement String** field, type string of characters to be prepended to the number (dial string).

Note: Click **Apply Changes**.

h. On the **Add Dial Plan** page, click **Apply**.

**Note:**

You have added one To TelURI conversion rule. If you want to add another To TelURI conversion rule, repeat Step 6.
Result
The changes you made to your dial plan settings are in effect. You do not have to restart the AE Server.

Administering default dial plan settings

About this task
If you use more than one switch in your AE Services and Microsoft for Live Communications Server configuration, and all the switches have the same dial plan settings, you can use the Default Dial Settings page as a template. When you add a switch connection, the dial plan settings that you have administered on the Default Dial Plan settings page are applied to that switch connection.

Procedure
1. From the AE Services Management Console main menu, select Communication Manager Interface > Dial Plan > Default Settings.
2. On the Dial Plan Settings - Conversion Rules for default page, in the From TelURI section, click Add.
3. From the Add Dial Plan - default page, follow these steps to complete the From TelURI settings, based on your dial plan.
   
   Important:
   See the online help in the AE Services Management Console as you complete these fields.
   a. In Pattern Type, select Pattern or RegEx based on your dial plan rules.
   b. In Minimum length, type a number from 1 to 21, or an asterisk (\* ) for any number, to specify the minimum number of characters expected in the telephone number (dial string).
   c. In Maximum Length, type a number from 1 to 21, or an asterisk (\* ) for any number, to specify the maximum number of characters expected in the number (dial string).
   d. In Matching Pattern, type a string of valid characters that you expect at the beginning of a dial string.
      Valid characters are all digits (0-9), the number sign (#), and the asterisk (*). You can not specify a blank space or the plus sign (+) in this field.
   e. In Delete length, type a number from 1 to 21 to specify the number of characters to delete from the beginning of the number (dial string).
   f. In Replacement String, type string of characters to be prepended to the number (dial string).
   g. Click Apply Changes.
   h. On the Add Dial Plan page, click Apply.
Note:
You have added one From TelURI conversion rule. To add another From TelURI conversion rule, repeat Step 3.

4. On the Dial Plan Settings - Conversion Rules for default page, in the To TelURI section, click Add.

5. From the Add Dial Plan - default page, follow these steps to complete the To TelURI settings, based on your dial plan.

Important:
See online help in the AE Services Management Console as you complete these fields.

a. In Pattern Type, select Pattern or RegEx based on your dial plan rules. Pattern is the default.

b. In Minimum length, type a number from 1 to 21, or an asterisk (*) for any number, to specify the minimum number of characters expected in the telephone number (dial string).

c. In Maximum Length, type a number from 1 to 21, or an asterisk (*) for any number, to specify the maximum number of characters expected in the number (dial string).

d. In Matching Pattern, type a string of valid characters that you expect at the beginning of a dial string.
   Valid characters are all digits (0-9), the number sign (#), and the asterisk (*). You can not specify a blank space or the plus sign (+) in this field.

e. In Delete length, type a number from 1 to 21 to specify the number of characters to delete from the beginning of the number (dial string).

f. In Replacement String, type string of characters to be prepended to the number (dial string).

g. Click Apply Changes.

h. On the Add Dial Plan page, click Apply.

Note:
You have added one To TelURI conversion rule. If you want to add another To TelURI conversion rule, repeat Step 5.

Result
Changes you made to your dial plan settings are in effect. You do not have to restart the AE Server.

How different APIs or offers use the TelURI settings
Both the DMCC API and the AE Services implementation for Microsoft Lync Server 2010 and 2013 use the From TelURI and the ToTelURI settings to convert between E.164 numbers and dial
strings. There are differences, however, in the way that the DMCC API and the AE Services implementation for LCS/OCS and Microsoft Lync Server handle the results of the conversion.

- To understand how the DMCC service uses the conversion rules, see From TelURI and ToTelURI operations for the DMCC service on page 295.
- To understand how the AE Services implementation for Microsoft Lync Server 2010 and 2013 uses the conversion rules, see From TelURI and ToTelURI operations for the AE Services implementation for LCS/OCS and Lync on page 296.

From TelURI and ToTelURI operations for the DMCC service

An application can not work in TelURI mode with AE Services. That is, an application must explicitly request conversion (from a dial string to a TelURI or from a TelURI to a dial string) from E164 conversion services as described in the two following topics, From TelURI operations for the DMCC service on page 295 and To TelURI operations for the DMCC service on page 295.

From TelURI operations for the DMCC service

The DMCC application receives a TelURI number from a directory. The DMCC application then submits the TelURI number to the E164 Conversion Service. The E164 Conversion Service provides a response, which includes a dial string. The application extracts the dial string from response and uses it in its next request, which is usually GetDeviceId.

To TelURI operations for the DMCC service

The DMCC application receives an event from Communication Manager, which includes an extension number. The DMCC application extracts the extension number and submits it to the E164 Conversion Service. The E164 Conversion Service converts the extension into a TelURI number. The application extracts the TelURI from the response, and uses it to resolve a number to a user or to display the TelURI number.
From TelURI and ToTelURI operations for the AE Services implementation for LCS/OCS and Lync

From TelURI operation for the AE Services implementation for LCS/OCS and Lync

For the AE Services implementation for LCS and Lync, From TelURI settings are used to convert normalized TelURI numbers, arriving from the Microsoft Office/Lync client, into dial strings. AE Services hands off the dial strings to the switch (Communication Manager).

To TelURI operations for the AE Services implementation for LCS/OCS and Lync

For the AE Services implementation for LCS/OCS and Lync, To TelURI settings are used to convert dial strings, arriving from the switch (Communication Manager) into normalized TelURI numbers. AE Services hands off the normalized TelURI numbers to Microsoft Office Communicator/Lync.

Creating a backup of the dial plan

About this task

Use this procedure to export the dial plan to a backup file (comma separated values format).
**Procedure**

1. From the AE Services Management Console main menu, select **Communication Manager Interface > Dial Plan > Export**.
2. On the **Export Dial Plan** page, click **Here**.

---

**Importing a dial plan**

**About this task**

Use this procedure to import (upload) a dial plan (comma separated values) backup file to AE Services. AE Services imports the dial plan backup file and updates the AE Services switch connection and teluri tables in the database.

**Procedure**

1. From the AE Services Management Console main menu, select **Communication Manager Interface > Dial Plan > Import**.
2. On the **Import Dial Plan** page, click **Browse**.
3. In the **Choose File to Upload** dialog box, select the dial plan backup file you want to import, and then click **Open**.
4. Click **Upload**.
Chapter 17: Administering for Web services-based applications

AE Services Administration for Web services-based applications

Application Enablement Services Web Services provides the ability for data application developers to interface to Communication Manager through standard Web Services methods. AE Services provides the following Web services based interfaces:

- **User Management** — a service component enabling the management of user profile data in the local LDAP database.

  🌟 **Note:**

  Effective with AE Services 4.1, AE Services had discontinued support for the User Service on AE Services 3.x and 4.0. Applications written to the User Service will continue to work on AE Services 3.x and 4.0, but AE Services will not support applications written to the User Service.

- **System Management Service (SMS)** — a web service that exposes selected management features of Communication Manager. SMS enables SOAP (Simple Object Access Protocol) clients to display, list, add, change and remove specific managed objects on Communication Manager.

  For information about SMS configuration settings, see [SMS Configuration](#) on page 298.

- **Telephony Web Service** — a high level interface to a small subset of call control services. You can configure the Session Timeout setting for TWS in the AE Services Management Console.

  For more information about the Web Services, see the *Avaya Aura® Application Enablement Services Web Services Programmer's Guide*, 02-300362.

---

**SMS Configuration**

The SMS Configuration pages in the AE Services Management Console let you edit the saw.ini file using the Management Console pages. Because SMS Configuration a part of the AE Services Management Console, the saw.ini file will be backed up whenever a you use the Backup Database feature to backup the AE Server.
Effective administration of the SMS configuration settings assumes that you are working with SMS application development to configure the AE Server for SMS. Here are a few guidelines for completing the SMS Configuration Page.

### Changing SMS proxy port settings

**About this task**

By default, AE Services assigns ports 4101 to 4116 for SMS proxy ports. If you need to change these settings follow this procedure.

**Procedure**

1. Log in to the AE Services Management Console with System Administrator privileges.
2. From the AE Services Management Console main menu, select **Networking > Ports**.
3. From the **Ports** page, locate the SMS Proxy Ports settings. The default settings are:
   - Proxy Port Min **4101**
   - Proxy Port Max **4116**
4. Change the port assignments to port numbers that are appropriate for your configuration.

**Note:**

SMS can use up to 16 ports. If you change any of the SMS port assignments, make sure that there are no conflicts with other ports.

### Configuring SMS settings

**Procedure**

1. Log in to the AE Services Management Console with System Administrator privileges.
2. From the AE Services Management Console main menu, select **AE Services > SMS > SMS Properties**.
3. Complete the **SMS Properties** page.

   The following list describes the SMS configuration settings and provides some guidelines for configuring SMS.

   - **Default CM Host Address** — If you administer a Communication Manager Host Address, SMS will attempt to connect to this Communication Manager host address, as long as no host address is explicitly specified in the authorization header of a client request. If this field is blank, all SMS requests must explicitly include the target Communication Manager host address.
   - **Default CM Admin Port** — By default the System Management Service will use 5022 to connect to a Communication Manager server. The Default Communication Manager Admin Port is a default setting that can be overridden at any time by an SMS request. If you manually administer a port number, make sure that there are no conflicts with other ports.
   - **CM Connection Protocol** — The Communication Manager Connection Protocol setting and the Default Communication Manager Admin Port are interdependent.
Note:
If you change the **CM Connection Protocol**, you may need to change the **Default CM Admin Port**. The default TUI (or SAT) ports on Communication Manager are as follows:
SSH Port=5022
Telnet Port=5023

- **SMS Logging** — Use the default setting **Normal** unless you are debugging. Changing this setting to **Verbose** could result in a high volume of read and write operations.
- **SMS Log Destination** — Use the default apache, unless you are debugging. The syslog setting is for debugging only.
- **CM Proxy Trace Logging** — Use the default **None**, unless you are debugging. The **Normal** and **Verbose** settings are for debugging only.
- **Proxy Log Destination** — Use the default destination `/var/log/avaya/aes/ossicm.log` for the CM Proxy Trace logs on the AE Server.
- **Max Sessions per CM** — This is a safety setting that prevents SMS from consuming all of the TUI processes on Communication Manager. By default the setting is 5. You can specify from 1 to 5 sessions. The maximum number of sessions that SMS allows open on a single Communication Manager is 5.
- **Proxy Shutdown Timer(s)** — Use the default **1800 seconds**, unless you are developing an SMS application that requires modifying this setting.
- **SAT Login Keepalive(s)** — Use the default **180 seconds**, unless you are developing an SMS application that requires modifying this setting.
- **CM Terminal Type** — Use the default **OSSIZ**, unless you have the need to remove punctuation from extensions on list operations or security requirements. This setting allows for the ossicm proxy to change its default terminal type. Select from the following options:
  - **OSSIZ** (the default). Any customer-related superuser login to CM will be able to read as well as write station security codes.
  - **OSSI3**. Only the “init” user can read station security codes.
  - **OSSIE**. Exactly the same as OSSIZ except extension numbers do not contain punctuation.

---

**Configuring TWS Properties**

**Procedure**

1. On Application Enablement Services Management Console, click **AE Services > TWS > TWS Properties**.
2. In the Session Timeout field, type the appropriate value.
3. Click **Apply Changes**.
4. On the TWS Properties page, click **Apply**.
5. **(Optional)** Click **Restore Defaults** to restore the default settings.
Chapter 18: Using the Historical Metric Data Collector (HMDC)

Using the Historical Metric Data Collector (HMDC)

The Historical Metric Data Collector (HMDC) enables you to collect, store, and display real-time and historic product-specific performance data.

Using HMDC you can:

- Schedule metric-group(s) data to be collected
- Specify how long you want to keep collected data
- Generate reports with the collected data
- Delete collected data.

Related links

- Scheduling data collection on page 302
- Unscheduling data collection on page 304
- Viewing configured schedules on page 305
- Modifying a scheduled data collection on page 305
- Enabling and disabling data collection on page 306
- Creating a metric data report on page 307
- Cleaning up data immediately on page 308

Scheduling data collection

About this task

Use this procedure to configure HMDC to collect specific data. See HMDC data on page 303 for a description of the metric data HMDC can collect.

Procedure

1. From the AE Services Management Console main menu, select Utilities >HMDC>Configuration.
2. From the field at the top of the Historical Metric Data Collection Configuration page, select the metric group data you want to collect.
3. Click **Schedule**.

4. On the Add/Edit Metric Group page, perform the followings steps:
   a. In the Configurable Metrics area, select the check box of the metric data you want to collect. By default, all of the check boxes are selected. See [HMDC data](#) on page 303 for a description of the metric data HMDC can collect.
   b. From the Sampling Interval field, select the time interval at which you want to collect the data sample.
   c. In the Cleanup Interval area, select the time interval after which you want the data deleted.
   d. Click **Apply Changes**.
   e. On the Edit HMDC metric group page, click **Apply**.

Related links

- [Using the Historical Metric Data Collector (HMDC)](#) on page 302
- [HMDC data](#) on page 303

**HMDC data**

You can configure the HMDC utility to collect the data shown in the following table.

<table>
<thead>
<tr>
<th>Metric Group</th>
<th>Metric Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>SysCPU</td>
<td>Operating system total CPU utilization.</td>
</tr>
<tr>
<td></td>
<td>SysMemory</td>
<td>Operating system memory usage.</td>
</tr>
<tr>
<td></td>
<td>MvapNetRTT</td>
<td>Ping time for each AEP link configured on AE Services.</td>
</tr>
<tr>
<td>Transport</td>
<td>avAesaepLinkMsgSent</td>
<td>The number of messages sent for AEP Link in the last “window” minutes.</td>
</tr>
<tr>
<td></td>
<td>avAesAepLinkMsgRcvd</td>
<td>The number of AEP messages received for AEP link in the last “window” minutes.</td>
</tr>
<tr>
<td></td>
<td>avAesAepSessionsMsgSent</td>
<td>The number of messages sent for AEP session in the last “window” minutes.</td>
</tr>
<tr>
<td></td>
<td>avAesAepSessionMsgRcvd</td>
<td>The number of messages received for AEP session in the last “window” minutes.</td>
</tr>
<tr>
<td></td>
<td>avAesTciConnMsgSent</td>
<td>The number of TCI messages sent in the last “window” minutes.</td>
</tr>
<tr>
<td></td>
<td>avAesTciConnMsgRcvd</td>
<td>The number of TCI messages received in the last “window” minutes.</td>
</tr>
<tr>
<td>CVLAN</td>
<td>avAesCvlanCtiLinkMsgSent</td>
<td>The number of messages sent to Avaya Communication Manager in the last “window” minutes.</td>
</tr>
</tbody>
</table>
### Using the Historical Metric Data Collector (HMDC)

<table>
<thead>
<tr>
<th>Metric Group</th>
<th>Metric Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>avAesCvlanCtiLinkMsgRcvd</td>
<td>The number of messages received from Avaya Communication Manager in the last “window” minutes.</td>
</tr>
<tr>
<td>DLG</td>
<td>avAesDlgCtiLinkMsgSent</td>
<td>The count of messages sent to Avaya Communication Manager in the last “window” minutes.</td>
</tr>
<tr>
<td></td>
<td>avAesDlgCtiLinkMsgRcvd</td>
<td>The count of messages received from Avaya Communication Manager in the last “window” minutes.</td>
</tr>
<tr>
<td>TSAPI</td>
<td>avAesTsapiCtiLinkMsgSent</td>
<td>The number of messages sent to Avaya Communication Manager in the last “window” minutes.</td>
</tr>
<tr>
<td></td>
<td>avAesTsapiCtiLinkMsgRcvd</td>
<td>The number of messages received from Avaya Communication Manager in the last “window” minutes.</td>
</tr>
<tr>
<td></td>
<td>avAesTsapiClientDeviceMonitors</td>
<td>The number of device monitors currently active.</td>
</tr>
<tr>
<td></td>
<td>avAesTsapiClientCallMonitors</td>
<td>The number of call monitors currently active.</td>
</tr>
<tr>
<td></td>
<td>avAesTsapiClientVdnMonitors</td>
<td>The number of VDN monitors currently active.</td>
</tr>
<tr>
<td></td>
<td>avAesTsapiClientRegisteredRoutes</td>
<td>The number of route registrations currently active.</td>
</tr>
<tr>
<td>DMCC</td>
<td>avAesDmccActiveSessions</td>
<td>The number of active DMCC sessions.</td>
</tr>
<tr>
<td></td>
<td>avAesDmccActiveDevices</td>
<td>The number of active devices.</td>
</tr>
<tr>
<td></td>
<td>avAesDmccUsedMonitors</td>
<td>The number of monitors currently in use across the DMCC sessions.</td>
</tr>
<tr>
<td></td>
<td>avAesDmccMaxMonitors</td>
<td>The number of monitors available to a DMCC service.</td>
</tr>
</tbody>
</table>

**Related links**

[Scheduling data collection](#) on page 302

---

**Unscheduling data collection**

**About this task**

Use this procedure to unschedule an HDMC collection.

**Procedure**

1. From the AE Services Management Console main menu, select **Utilities** > **HMDC** > **Configuration**.
2. Select the appropriate metric group.
3. Click **Unschedule**.
4. On the Unschedule HMDC metric group page, click **Apply**.

Related links
- [Using the Historical Metric Data Collector (HMDC)](#) on page 302

---

### Viewing configured schedules

**About this task**
Use this procedure to view the events you have scheduled.

**Procedure**
From the AE Services Management Console main menu, select **Utilities >HMDC>Configuration**.

The Historical Metric Data Collection Configuration page appears and displays the scheduled events.

**Note:**
If the Current Status column displays **Disabled** for a scheduled metric group, data collection for that group will not occur, but clean up of already collected data will continue according to the configured schedule.

Related links
- [Using the Historical Metric Data Collector (HMDC)](#) on page 302

---

### Modifying a scheduled data collection

**About this task**
Use this procedure to modify a scheduled HMDC data collection event. See [HMDC data](#) on page 303 for a description of the metric data HMDC can collect.

**Procedure**
1. From the AE Services Management Console main menu, select **Utilities >HMDC>Configuration**.
2. On the Historical Metric Data Collection Configuration page, select the metric group data collection event you want to modify.
3. Click **Edit**.
4. On the Add/Edit Metric Group page, perform the followings steps:
   a. In the Configurable Metrics area, select the check box of the metric data you want to collect. By default, all of the check boxes are selected. See HMDC data on page 303 for a description of the metric data HMDC can collect.
   b. From the Sampling Interval field, select the time interval at which you want to collect the data sample.
   c. In the Cleanup Interval area, select the time interval after which you want the data deleted.
   d. Click Apply Changes.
   e. On the Edit HMDC metric group page, click Apply.

Related links
Using the Historical Metric Data Collector (HMDC) on page 302

Enabling and disabling data collection

About this task
Use this procedure to temporarily enable or disable an HMDC data collection event.

Procedure
1. From the AE Services Management Console main menu, select Utilities >HMDC>Configuration.
2. On the Historical Metric Data Collection Configuration page, select the metric group data collection event you want to enable or disable.
   *The Current Status column displays whether the selected data collection event is enabled or disabled.
3. Perform one of the following steps:
   - If you want to enable the selected data collection event, click Enable.
   - If you want to disable the selected data collection event, click Disable.
4. On the Disable HMDC metric group page, click Apply to confirm your action.
   *The Current Status column displays the updated status for the selected data collection event.

Related links
Using the Historical Metric Data Collector (HMDC) on page 302
Creating a metric data report

About this task
Use this procedure to generate a metric data report. You can download and save this report in the .CSV format.

Procedure
1. From the AE Services Management Console main menu, select Utilities >HMDC>Reporting.
2. From the Select Metric Group field, select the metric group data you want displayed in the report.
3. In the Select the metrics for reporting area, select the check box of the metric data you want displayed in the report. By default, all the check boxes are selected.
4. If you want to generate a historical report, perform the following steps:
   a. In the Report type area, click Historical Report.
   b. Click the Calendar button next to the From field.
   c. On the Calendar, select the starting date and time.
   d. Click Apply.
   e. Click the Calendar button next to the To field.
   f. On the Calendar, select the ending date and time.
   g. Click Apply.
      All collected data that fall in the range you specified will be displayed in the report.
5. If you want to generate a report that contains a “snapshot” of current data, click Current Snapshot in the Report type area.
6. Click Generate report.
   The Report page appears and displays the data.
7. If you want to save this data to a .CSV file, perform the following steps:
   a. Click Save Report.
   b. In the File Download dialog box, click Save.
   c. In the Save As dialog box, specify the folder and name of the file, and then click Save.
   d. In the Download complete dialog box, click Close.

Related links
Using the Historical Metric Data Collector (HMDC) on page 302
Cleaning up data immediately

About this task

Use this procedure to delete collected data immediately.

Procedure

1. From the AE Services Management Console main menu, select **Utilities > HMDC > Cleanup**.
2. From the Select Metric Group field, select the metric group data you want to delete.
3. In the Select the metrics for cleanup area, select the check box of the metric data you want to delete. By default, all the check boxes are selected.
4. If you want to delete all of the logs, click **All logs** in the Remove area.
5. If you want to delete logs older than a specific date and time, perform the following steps:
   a. In the Remove type, click **Logs older than**.
   b. Click the **Calendar** button next to the Older than field.
   c. On the Calendar, select the date and time.
   d. Click **Apply**.
6. If you want to delete logs from a specific time period, perform the following steps:
   a. In the Remove area, click **Logs between**.
   b. Click the **Calendar** button next to the From field.
   c. On the Calendar, select the starting date and time.
   d. Click **Apply**.
   e. Click the **Calendar** button next to the To field.
   f. On the Calendar, select the ending date and time.
   g. Click **Apply**.
7. Click **Cleanup**.
8. On the Cleanup HMDC metric group page, click **Apply** to confirm your action.

Related links

- [Using the Historical Metric Data Collector (HMDC)](Using%20the%20Historical%20Metric%20Data%20Collector%20(HMDC)) on page 302
Chapter 19: Location of AE Services log files

Device, Media, and Call Control Service

All logs are in /var/log/avaya/aes, as follows:

- dmcc-api.log.xx (where xx is a number from 1 to 20. The first dmcc-api.log is not numbered.)
- dmcc-error.log.xx (where xx is a number from 1 to 20. The first dmcc-error.log is not numbered.)
- dmcc-trace.log.xx (where xx is a number from 1 to 20. The first dmcc-trace.log is not numbered.)
- dmcc-nist.log.xx (where xx is a number from 1 to 20. The first dmcc-nist.log is not numbered.)
- dmcc-wrapper.log.x (where x is a number from 1 to 4. The first wrapper log, dmcc-wrapper.log, is not numbered.)
- database.log
- reset.log

DLG Service

AE Services provides the same logs that were provided with the MAPD-based DLG. All logs except the trace log are in the /var/log/avaya/aes directory, as follows:

- Security (client) log: sec.log
- Error log: mvap.log
- Command log: cmd.log
- Reset log: reset.log
- Trace log: /var/log/avaya/aes/common/trace.out
CVLAN Service

AE Services provides the same logs that were provided with the MAPD-based CVLAN and CVLAN Release 9 and Release 9.1 for Linux.

All logs except the trace log are in /var/log/avaya/aes, as follows:

- Security (client) log: sec.log
- Error log: mvap.log
- Command log: cmd.log
- Reset log: reset.log
- Trace log: /var/log/avaya/aes/common/trace.out

TSAPI Service

All logs, except the trace log and the G3trace log, are in /var/log/avaya/aes, as follows:

- Security (client) log: sec.log
- Error log: mvap.log
- Command log: cmd.log
- Reset log: reset.log
- Trace log: /var/log/avaya/aes/common/trace.out
- G3trace logs are located in the /var/log/avaya/aes/TSAPI directory. This directory includes g3trace.out and csta_trace.out.
- Import SDB log: importsdb.log

Telephony Web Service

The Telephony Web Service infrastructure includes Tomcat, Axis, and the TSAPI Service. Any major failure in either Tomcat or the TSAPI Service will affect the Telephony Web Service.

All logs are in /var/log/avaya/aes/tomcat, as follows:

- ws-telsvc-api.log
- ws-telsvc-error.log
- ws-telsvc-trace.log
System Management System Web Service

The System Management Service uses the Linux syslog and Apache logs.
Chapter 20: AE Services network interfaces

Out of Band Management

Out of Band Management provides the ability to move the AE Services Management Console Web based management and configuration traffic of the server to a dedicated subnetwork.

Table 20: Application Enablement Services Out of Band Management

<table>
<thead>
<tr>
<th>Component</th>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMCC Service</td>
<td>Eth0 (public IP)</td>
<td>The Device, Media, and Call Control (DMCC) service provides both, first-party and third-party call control features using a Java API. It also provides XML and .NET interfaces. Additionally, DMCC provides the integration for Microsoft Lync 2010, and Lync 2013. TCP/IP, TLS and SIP protocols may be used to connect a DMCC Client to DMCC.</td>
</tr>
<tr>
<td>DLG Service</td>
<td>Eth0 (public IP)</td>
<td>The DEFINITY LAN Gateway (DLG) service tunnels messages over TCP/IP. That is, the DLG service supports a set of TCP/IP connections for the communications channel between Avaya Aura® Communication Manager and AE Services. The DLG service is also used for transporting ASAI/Q.931 messages.</td>
</tr>
<tr>
<td>CVLAN Service</td>
<td>Eth0 (public IP)</td>
<td>The CallVisor LAN (CVLAN) service is a C/C++ based API that enables applications to exchange ASAI messages with the AE Services server. CVLAN provides a full complement of third-party call control capabilities such as controlling specific calls or stations, completing routing of incoming calls, receiving notifications of events, invoking features, and querying Avaya Aura® Communication Manager for information.</td>
</tr>
<tr>
<td>TSAPI Service</td>
<td>Eth0 (public IP)</td>
<td>The Telephony Services API (TSAPI) is a C/C++ based API that provides a full complement of third party call control capabilities. The Java Telephony API (JTAPI) is a client side interface to the TSAPI service. It provides third party call control.</td>
</tr>
<tr>
<td>Transport Service</td>
<td>Eth0 (public IP) Eth1 (private IP)</td>
<td>The Transport link is a secure TCP/IP connection between the AE Services server and Avaya Aura® Communication Manager. The default interface is eth0</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Component</th>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Management Service</td>
<td>Eth0 (public IP), or Eth2 (Out of Band Mgmt IP)</td>
<td>Listens on port 443 for HTTPS connection to provide users a web interface to enable SOAP-based access to Avaya Aura® Communication Manager administration functions. The default interface is eth0, unless Out-of-Band Management has been configured.</td>
</tr>
<tr>
<td>Telephony Web Service</td>
<td>Eth0 (public IP), or Eth2 (Out of Band Mgmt IP)</td>
<td>Listens on port 8443 and 443 for HTTPS connection to provide users a web interface that enables high level call control functionality over standard web services interfaces (SOAP/XML). The default interface is “eth0”, unless Out-of-Band Management has been configured.</td>
</tr>
<tr>
<td>AES Management Console</td>
<td>Eth0 (public IP) or Eth2 (Out of Band Mgmt IP)</td>
<td>The Application Enablement Services Management Console listens on port 443 for HTTPS connections, and provides an Operations, Administration and Management interface for maintenance of the AE Services server. The default interface is eth0, unless Out-of-Band Management has been configured.</td>
</tr>
</tbody>
</table>

**Network interface configurations**

You can configure the AE Services Server to use a single NIC, two NICs or three NIC configuration. The second and third NIC can be used for creating a private network between the AE Services server and Communication Manager, or for out of band management. Use the configuration that best suits your network topology and other characteristics of your network.

**Single NIC configurations**

In a single NIC configuration, you use one network interface. That is, the AE Services server uses one NIC for client, switch and media connectivity.

In a single NIC configuration, the AE Services server, Communication Manager, and the client application computer must reside on a private LAN, a virtual LAN (VLAN), or a WAN. In terms of setting up the AE Services IP (Local IP), this means you are using one NIC for client, switch, and media connectivity.

In a single NIC configuration, you must configure the IP interface for the AE Services server to be publicly accessible for the registration of IP endpoints. Always use eth0 for a single NIC configuration (eth1 is reserved for Avaya service technicians).

AE Services recommends a single NIC configuration for connectivity to S8300D and S8300E Communication Manager media servers.
Note:
The S8300 media server does not use a CLAN as a network interface, it uses a processor ethernet (procr) instead.

Two NIC configurations

In a two NIC configuration, you use two network interfaces for connectivity to two separate network segments.

In a dual NIC configuration, you use one network segment for the AE Services Server and Communication Manager and another network segment for client and media connectivity, that is LAN, VLAN, or WAN. The NICs must be on separate network segments. In a dual NIC configuration, the client segment is referred to as the production network, and the Communication Manager segment is referred to as the private network segment.

AE Services supports using two NIC configurations for duplicated Communication Manager media servers.

The second NIC can also be used for out of band management if network separation between Communication Manager and AE Services Server client applications.

Three NIC configurations

A third NIC can be configured for out of band management, if the first two NICs are used for non management related traffic, as described above.

Network interface (NIC) settings

The NIC settings choices for eth0, eth1 and eth2 are as follows:

- Auto-Negotiate:
  - Gigabit interfaces: Auto-negotiation (auto-neg) - on
    In this case, you must administer 1000-Mbps / full / auto-neg at each end of the Ethernet link.
  - 100-Mbps interfaces: Auto-negotiation (auto-neg) - on
    In this case, you must administer 100-Mbps / full / auto-neg at each end of the Ethernet link.

- Lockdown: 100-Mbps interfaces
  100-Mbps interfaces: Lockdown (auto-neg) - off
    In this case, you must administer 100-Mbps / full / Lockdown at each end of the Ethernet link.
Important:

AE Services defaults to auto-negotiation mode; it negotiates the network speed and duplex mode with the Ethernet switch. Both ends of the Ethernet link must be set to the same mode. Otherwise, a duplex mismatch will occur. Verify that both ends of the Ethernet link operate at the same desired speed and duplex settings.

Keep in mind the following:

- Auto-neg is highly desired for Gigabit links.
- Auto-neg or Lockdown is acceptable for 100-Megabit links.
- Lockdown for Gigabit links is highly discouraged.
- 10-Megabit and/or half-duplex operation is never acceptable and should be corrected.

See Editing the NIC configuration (optional) on page 315 to set up the server NICs. For detailed information about using auto-negotiation and Lockdown, see Ethernet Link Guidelines at https://support.avaya.com/css/P8/documents/100121639.

---

Editing the NIC configuration

About this task

Network interfaces are configured during the AE Services installation process on the Configure Network Information page.

Use this procedure only if you need to change the NIC settings from Auto-Negotiate to Lockdown (100M links only).

The values that are initially displayed on the Network Configure page reflect the negotiated values between the NICs on the AE Services server and the Ethernet switch on your network.

Important:

AE Services has been tested at 1000BaseT full duplex and 100BaseT full duplex. These are the required speed and duplex mode settings for both network interfaces eth0 and eth1.

Procedure

1. On the AE Services Management Console, click Networking > Network Configure.
2. On the Network Configure page, edit any of the settings that you want to change, and click Apply Changes.

Note:

Changing the settings for a NIC will cause the NIC to restart. Once you change the settings, they remain in effect until you reset them. Rebooting the AE Services server will not reset any of the values.
Chapter 21: TCP ports and firewall settings on the AE Services server

TCP ports and firewall settings

If you use a firewall, you must make sure that the TCP port settings on your firewall are consistent with the TCP port settings on the AE Services Server. For information about security guidelines for the AE Services Server, see the White Paper on Security in Application Enablement Services for Bundled, AES on System Platform and Software Only Solutions. This white paper is available with the AE Services customer documents on the Avaya Support Web site: http://www.avaya.com/support.

Note:

For all AE Services servers, except the Software-Only server, a firewall is automatically configured and enabled by default.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVLAN Ports</td>
<td>The port number assignment for unencrypted connections with CVLAN clients.</td>
</tr>
<tr>
<td>UnencryptedTCP Port</td>
<td>9999</td>
</tr>
<tr>
<td>DLG Port</td>
<td>The DLG Service uses port 5678 for communication with clients. This is a fixed port number assignment.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>TCP Port Min</th>
<th>TCP Port Max</th>
</tr>
</thead>
</table>
| TSAPI Ports         | The port number assignment for the TSAPI listener. By default TSAPI port 450 is enabled. When you disable TSAPI 450, you also disable following TSAPI Port settings:  
• CSTA TLINK Ports for Non-Secured Clients  
• CSTA TLINK Ports for Secured Clients | 450          |              |
| Note:              | If you disable Port 450, you must restart the TSAPI Service for the change to take effect. | Enable/Disable |              |
| Local TLINK Ports   | TCP Port Min Reserved, port 1024                                            | TCP Port Min | TCP Port Max |
|                     | TCP Port Max Reserved, port 1039                                            |              |              |
| Unencrypted TLINK Ports | TCP Port Min The default minimum setting is 1050. If you elect to use another port assignment as the minimum, it can not conflict with another port number. For information about administering TSAPI Links as either secure (Encrypted) or nonsecure (Unencrypted), see Administrating TSAPI Links on page 84. | The default minimum setting is 1050. If you elect to use another port assignment as the minimum, it can not conflict with another port number. For information about administering TSAPI Links as either secure (Encrypted) or nonsecure (Unencrypted), see Administrating TSAPI Links on page 84. | TCP Port Min | TCP Port Max |
|                     | TCP Port Max The default maximum setting is 1065. If you elect to use another port assignment as the minimum, it can not conflict with another port number. For information about administering TSAPI Links as either secure (Encrypted) or nonsecure (Unencrypted), see Administrating TSAPI Links on page 84. | The default maximum setting is 1065. If you elect to use another port assignment as the minimum, it can not conflict with another port number. For information about administering TSAPI Links as either secure (Encrypted) or nonsecure (Unencrypted), see Administrating TSAPI Links on page 84. | TCP Port Min | TCP Port Max |
| Encrypted TLINK Ports | TCP Port Min The default minimum setting is 1066. If you elect to use another port assignment as the minimum it can not conflict with another port number. For information about administering TSAPI Links as either secure (Encrypted) or nonsecure (Unencrypted), see Administrating TSAPI Links on page 84. | The default minimum setting is 1066. If you elect to use another port assignment as the minimum it can not conflict with another port number. For information about administering TSAPI Links as either secure (Encrypted) or nonsecure (Unencrypted), see Administrating TSAPI Links on page 84. | TCP Port Min | TCP Port Max |

Table continues…
## Name | Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>to take effect.</td>
<td>TCP Port Max</td>
</tr>
<tr>
<td>DMCC Server Ports</td>
<td>Unencrypted Port</td>
</tr>
</tbody>
</table>
| Note: | Encrypted Port | 4722 | Enabled/Disabled | The DMCC Service uses port 4722 for secure communication.  
- By default the secure, Encrypted Port setting is enabled.  
- The default port number for encrypted DMCC communications is 4722. |
| | TR/87 Port | 4723 | Enabled/Disabled | The AE Services Server uses port 4723 for the AE Services implementation for Microsoft Live Communications Server. By default this port is disabled.  
- You must enable this port if you are integrating AE Services with Microsoft Live Communications Server. |
<p>| H.323 Port | TCP Port Min | The default minimum setting is 20000. The DMCC Service uses this port for signaling. |
| | TCP Port Max | The default maximum setting for this range is 29999. The DMCC Service uses this port for signaling. |
| | Local UDP Port Min | The default minimum setting is 20000. The DMCC Service uses this port for Registration Administration and Status (RAS). |
| | Local UDP Port Max | The default maximum setting is 29999. The DMCC Service uses this port for RAS. |
| | RTP Local UDP Port Min | The default minimum setting is 30000. The DMCC Service uses this port for the Media Real Time Protocol (RTP) sessions. |
| | RTP Local UDP Port Max | The default maximum setting for this range is 49999. The DMCC Service uses this port for Media RTP sessions. |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS Proxy Ports</td>
<td>Enter a Communication Manager proxy port range of up to 16 proxy ports. By default, the Communication Manager Proxy Port Range is 4101 to 4116.</td>
</tr>
<tr>
<td>Proxy Port Min</td>
<td>Note: SMS can use up to 16 ports. If you change any of the SMS port assignments, make sure that there are no conflicts with other ports.</td>
</tr>
<tr>
<td>Proxy Port Max</td>
<td>Note: SMS can use up to 16 ports. If you change any of the SMS port assignments, make sure that there are no conflicts with other ports.</td>
</tr>
</tbody>
</table>
Chapter 22: AE Services Management

Console connectivity tests

Use the following diagnostic utilities in AE Services Management Console to check connectivity:

**Note:**

When AE Services server is configured in the secure mode, AE Services does not support tests under **Utilities > Diagnostics > AE Services**.

- **ASAI Test** — Use the ASAI Test utility to determine if the AE Server is communicating with Communication Manager. The ASAI Test utility sends a heartbeat message over any of the CVLAN or TSAPI links you have configured between the AE Server and Communication Manager. ([Utilities > Diagnostics > AE Service > ASAI Test](#))

- **Ping Host** — Use the Ping Host utility to determine if the hostname or IP address you specify exists and is accepting requests. ([Utilities > Diagnostics > Server > Ping Host](#))

- **DMCC Test** — Use the DMCC Test to test the DMCC configurations. ([Utilities > Diagnostics > AE Service > DMCC Test](#))

- **TSAPI Test** — TSAPI Test is a simple test application that makes a call between two stations, primarily to verify that the client is set up correctly and the TSAPI Service has been administered correctly. TSAPI Test applies to TSAPI, JTAPI, and Telephony Web Service applications. ([Utilities > Diagnostics > AE Service > TSAPI Test](#))

- **TR/87 Test** — Use the TR/87 Test utility to run tests for DMCC applications and the AE Services implementation for Microsoft Office Live Communications Server 2005, Microsoft Office Communications Server 2007, and Microsoft Lync Server 2010 and 2013. ([Utilities > Diagnostics > AE Service > TR/87 Test](#)). Some of the tests may require you to administer the dial plan in AE Services before you can execute some of the TR/87 tests.

**Note:**

The Host AA settings for AE Services (**Security > Host AA**) have an effect on the TR/87 Test utility. If you enable host authorization, the authorized hosts list must include the Peer Certificate CN (which is the Server Certificate Subject Name). Because the TR/87 Test utility depends on the Host AA settings and uses the same certificate that is used by Tomcat, you must restart the Web Server after adding a server certificate.
## AE Services administrative roles and access privileges (role based access control - RBAC)

AE Services provides role-based access control (RBAC), which establishes the following roles for AE Services administrators (AE Services Management Console access and ssh access). The AE Services server uses the reserved Linux user ID range 500-599 and the reserved Linux group ID range 500-599 for the default AE Services server users and groups.

<table>
<thead>
<tr>
<th>Role</th>
<th>Linux group</th>
<th>Linux group ID</th>
<th>AE Services Management Console access</th>
</tr>
</thead>
<tbody>
<tr>
<td>System_Administrator</td>
<td>susers</td>
<td>555</td>
<td>Read and write access to the following menus:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• AE Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Communication Manager Interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Licensing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Networking</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Security (the System_Administrator does not have access to Account Management, PAM, and Tripwire Properties)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Status</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Utilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Help</td>
</tr>
</tbody>
</table>

⚠️ **Note:**

The System_Administrator role does not have access to User Management.

Table continues…
<table>
<thead>
<tr>
<th>Role</th>
<th>Linux group</th>
<th>Linux group ID</th>
<th>AE Services Management Console access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security_Administrator</td>
<td>securityadmin</td>
<td>505</td>
<td>Read and write access to the following menus in the AE Services Management Console:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Security (the Security_Administrator does not have access to Enterprise Directory,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Host AA, and Standard Reserved Ports)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Status</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Help</td>
</tr>
<tr>
<td>UserSvc_Admin</td>
<td>usrsvc_admin</td>
<td>508</td>
<td>Read and write access to the following menus:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• User Management</td>
</tr>
</tbody>
</table>

**Note:**
To acquire the Administrative role for User Management, a user must have an administered account in User Admin (the local LDAP data store) with the Avaya role set to userservice.useradmin.

*Table continues…*
<table>
<thead>
<tr>
<th>Role</th>
<th>Linux group</th>
<th>Linux group ID</th>
<th>AE Services Management Console access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor</td>
<td>users</td>
<td>100</td>
<td>Limited, read-only access to the following menus:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Security — access is limited to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Certificate Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Security Database &gt; CTI Users</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Status</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Alarm Viewer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Logs -- access is limited to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Audit Logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Error Logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Install Logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• User Management Service Logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Status &gt; Status and Control — access is limited to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- CVLAN Service Summary</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- DLG Service Summary</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- DMCC Service Summary</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Switch Conn Summary</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- TSAPI Service Summary</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Help</td>
</tr>
<tr>
<td>Backup_Restore</td>
<td>backuprestore</td>
<td>507</td>
<td>Limited, read and write access to the following menus:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Maintenance — access is limited to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Server Data &gt; Backup</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Server Data &gt; Restore</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Help</td>
</tr>
</tbody>
</table>

*Table continues…*
### AE Services administrative roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Linux group</th>
<th>Linux group ID</th>
<th>AE Services Management Console access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya_Maintenance</td>
<td>avayamaint</td>
<td>506</td>
<td>Limited, read and write access to the following menus in the AE Services Management Console:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Security Database</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Service Controller</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Server Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Status</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Utilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Diagnostics</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Help</td>
</tr>
<tr>
<td>EASG Administrator</td>
<td>easg</td>
<td>510</td>
<td>Read and write access of the EASG option on the PAM Password Manager.</td>
</tr>
</tbody>
</table>

### Default accounts and AE Services Management Console access privileges

⚠️ **Security alert:**

You must change the password for the `cust` account after initially using it.
<table>
<thead>
<tr>
<th>Account name (log-in identifier)</th>
<th>Linux Group</th>
<th>AE Services Management Console access privileges</th>
</tr>
</thead>
</table>
| **craft**  (Avaya services account) | susers securityadmin | Read and write access to the following menus:  
- AE Services  
- Communication Manager Interface  
- Licensing (you have access to this menu)  
- Maintenance  
- Networking  
- Security (AE Services sets up the craft account with access to Security)  
- Status  
- Utilities  
- User Management (AE Services sets up the craft account with access to Security)  
- Help |
| **cust**  (customer account) | susers securityadmin usrsvc_admin easg datacontroller | Read and write access to the following menus:  
- AE Services  
- Communication Manager Interface  
- Licensing (you have access to this menu)  
- Maintenance  
- Networking  
- Security (AE Services sets up the cust account with access to Security)  
- Status  
- User Management (AE Services sets up the cust account with access to Security)  
- Utilities  
- Help |
| **avaya**  (customer account) | Not applicable | Read and write access to the following menus:  
- User Management  
- Help  
- **Status > Logs > User Management Service** |
| **Available on:** | |  
- AE Services Software - Only Server only if you enabled EASG at the time of installation.  
- AE Services using VMware® in the Virtualized Environment |
<table>
<thead>
<tr>
<th>Account name (log-in identifier)</th>
<th>Linux Group</th>
<th>AE Services Management Console access privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>datacontroller (customer account)</td>
<td>datacontroller</td>
<td>Read and write access to the following menus:</td>
</tr>
<tr>
<td>• AE Services Software-Only Server</td>
<td></td>
<td>• Help</td>
</tr>
<tr>
<td>• AE Services using VMware® in the Virtualized Environment</td>
<td></td>
<td>• Status &gt; Log Manager</td>
</tr>
</tbody>
</table>

**Authenticating and authorizing administrators for AE Services Management Console and ssh access**

*Note: PAM Management pages in the AE Services Management Console apply only to the following:*
- Local Linux accounts
- AE Services Management Console access, including RBAC
- remote users with SSH access
# Default AE Services accounts

<table>
<thead>
<tr>
<th>Account name (log-in identifier)</th>
<th>Linux Group</th>
<th>Access privileges</th>
</tr>
</thead>
</table>
| **craft**                        | susers      | Intended for Avaya services technicians. Provides local or remote access to the Linux shell.  
• Local - Log in from a local console as craft, and then access the root account (su - sroot)  
• Remote - Log in from a remote console with a secure shell client (ssh), as craft, and then access the root account (su - sroot) |
| Available on AE Services Software-Only Server only if you enabled EASG at the time of installation. | securityadmin | |
| **cust**                         | susers      | Intended for customers. Provides local or remote access to the Linux shell.  
• Local - Log in from a local console as cust, and then access the root account (su - root)  
• Remote - Log in from a remote console with a secure shell client (ssh), as cust, and then access the root account (su - root) |
| Available on AE Services Software-Only Server. | securityadmin | |
| **avaya**                        | Not applicable | User Management administration only.  
You do not have access to any other administrative menus. |
| Available on AE Services Software-Only Server. | | |
| **datacontroller**               | datacontroller | Log and trace retention and clearing logs and traces only.  
You do not have access to any other administrative menus. |
| Available on AE Services Software-Only Server. | | |

## Accounts installed with the Avaya Services package

When you install the Avaya Services package (cs-services), the installation program sets up the AE Services server with avaya and cust accounts by default. It also adds service accounts, such as craft, for Avaya Service Technicians and Avaya BusinessPartners.

⚠️ **Note:**

If you did not install the Avaya Services package, skip this section and see [Creating a new System Administrator account](#) on page 330.
The avaya account (User Management administrator)

When you install the Avaya Services package (cs-services), the installation program sets up the AE Services server with the avaya account in the local LDAP store (User Management) by default. It is not a Linux account. You must install the AE Services license in order to access Application Enablement Services Management Console with the avaya account.

The avaya account provides access to the User Management Service in the Application Enablement Services Management Console. The avaya user is the User Management administrator.

⚠️ Security alert:

The customer is responsible for changing the password for the avaya account after initially using it. To learn about changing the password for the avaya account, see Changing the default password for the avaya account (User Management administrator) on page 332.

The cust accounts (Linux and User Management)

When you install the Avaya Services package (cs-services), the installation program sets up the AE Services server with the cust account by default.

⚠️ Security alert:

You are responsible for changing the password for the cust account after initially using it. See Changing the default password for the cust account in local Linux on page 329 and Changing the default password for the cust account in User Management on page 333.

AE Services installs the cust account in two places: the local Linux password store and the local LDAP directory (User Management Service). As a result, the cust account has read-write access to all AE Services Management Console features.

• The Linux cust account provides remote access, using a secure shell (ssh) client, to the Linux shell. The Linux cust account belongs to two login groups: susers and security admin. As a result, the cust account has system administration privileges and security administration privileges. To see how administrative roles map to Linux groups in AE Services, refer to AE Services administrative roles and access privileges (role based access control - RBAC) on page 321.

• The User Management Service cust account provides access to the User Management Service. You must install the AE Services license in order to log in to Application Enablement Services Management Console with the User Management Service cust account.
The craft account

When you install the Avaya Services package (cs-services), the installation program sets up the AE Services server with the craft account by default. The craft account is equivalent to the cust account. See Accounts for Avaya Services technicians on page 238.

The craft account provides Avaya Service Technicians and Avaya Business Partners read-write access to all administrative functions using either the Linux command line or the AE Services Management Console.

You must install the AE Services license in order to access Application Enablement Services Management Console with the craft account.

Changing the default password for the cust account in local Linux

About this task

Follow this procedure to change the default password for the cust account in local Linux. The local Linux cust account provides remote access to the Linux shell. This procedure applies only to an AE Services Software Only server with the Avaya Services package (cs-services) installed.

Note:

If you require a greater level of security, see Creating a new System Administrator account and removing the default cust account from User Management.

Procedure

1. From your browser, log in to the AE Services Management Console as cust with the default password (custpw).
   See Accounts installed with the Avaya Services package.
2. From the main menu, select Security Administration.
3. From the Security Administration home page, select Account Management > Modify Login.
4. From the Modify Login page, in the Password authentication Enter password field, enter a new password.
   The default Linux password policy, which is based on a US standard keyboard and the default password limits for PAM Module Configuration, calls for a minimum of 8 characters, with at least 1 uppercase character, 1 lowercase character, 1 alphanumeric character, and 1 special character. The following characters are not permitted: $ (dollar sign), ' (apostrophe), " (quotation mark), \ (backslash), the space character, and any ASCII control-character.
5. In the **Re-enter password** field, re-enter the new password.

6. Click **Modify**.

Related links

- Creating a new System Administrator account and removing the default cust account from User Management on page 335
- Accounts installed with the Avaya Services package on page 327
- The avaya account (User Management administrator) on page 328
- The cust accounts (Linux and User Management) on page 328
- The craft account on page 329

---

## Creating a new System Administrator account

### About this task

Follow these steps to create a new System Administrator account and delete the cust account. This procedure applies to the AE Services Bundled Server and the AE Services Software-Only Server with the Avaya Services Package (cs-service) installed.

**Note:**

In the AE Services secure mode, the **Account Management** tab under the **Security** tab is disabled.

### Procedure

1. From your browser, log in to the AE Services Management Console as cust.

   See Accounts installed with the Avaya Services package on page 327.

2. From the main menu, select **Security > Account Management > Add Login**.

3. Complete the **Add Login** page as follows:

   **Note:**

   These settings assume that you want to set up the new system administrator with the same administrative roles that were set up for the cust account.

   a. In the **Login ID** field, enter a new username for the system administrator, for example `aesadmin`, and click **Continue**.

   b. In the **Default login group** field, type `susers` (the `susers` Linux group maps to the System_Administrator role).

   c. In the **Additional login groups** field, type `securityadmin` (the `securityadmin` Linux group maps to the Security_Administrator role).
Note:

When completing the Default login group and Additional login groups fields, you must use the group names for RBAC assignments described in AE Services administrative roles and access privileges (role based access control - RBAC) on page 321.

d. Complete the Password authentication fields. Enter a password, and re-enter the password to confirm it.

The default Linux password policy, which is based on a US standard keyboard and the default password limits for PAM Module Configuration, calls for a minimum of 8 characters, with at least 1 uppercase character, 1 lowercase character, 1 alphanumeric character, and 1 special character. The following characters are not permitted: $ (dollar sign), ' (apostrophe), " (quotation mark), \ (backslash), the space character, and any ASCII control-character.

e. In the remaining fields, either accept the defaults, or complete the fields according to your business requirements, and click Add.

4. From the navigation bar, click Logout (you are logging out as cust).

5. Log into the AE Services Management Console again with the new system administrator account (aesadmin, based on this example).

6. From the main menu, select Security > Account Management > Remove Login.

7. From the Remove Login page, in the Login ID field, enter cust and click Continue.

8. On the Remove Login page, verify that you are removing the appropriate login (cust), and click Delete.

Adding a Linux System Administrator account (if the Avaya Service Package is not installed)

About this task

If you did not install the cs-services package when you installed the AE Services Software-Only server, you initially have only one account (the avaya account).

Note:

The root user can not access the AE Services Management Console.

Follow this procedure to add a user to Linux with system administration privileges (system_administrator) and security administration privileges (security_administrator).

Procedure

1. Log in to the AE Services Server as root using the password you assigned to root during the Linux installation.
2. Type `useradd -g susers -G securityadmin username`.
   
   For example: `useradd -g susers -G securityadmin cust00`

   **Note:**
   
   To administer a user with system administrator privileges in AE Services Management Console, you must add the user to the susers group in Linux. If you want this user to have access to the security menu in the Management Console, you must add the user to the securityadmin group as well. To see how administrative roles map to Linux groups in AE Services, refer to AE Services administrative roles and access privileges (role based access control - RBAC) on page 321.

3. Type `passwd username` to display the password prompt.

4. At the password prompt, type a password, and press Enter.
   
   The default Linux password policy, which is based on a US standard keyboard and the default password limits for PAM Module Configuration, calls for a minimum of 8 characters, with at least 1 uppercase character, 1 lowercase character, 1 alphanumeric character, and 1 special character. The following characters are not permitted: $ (dollar sign), ’ (apostrophe), " (quotation mark), \ (backslash), the space character, and any ASCII control-character.

5. At the prompt to re-enter your password, type the password you just created and press Enter.

---

**Changing the default password for the avaya account (User Management administrator)**

**About this task**

By default, AE Services installs an account called avaya for the Software-Only server. The avaya account is created for all installations of AE Services. That is, it is created regardless of whether you install the Avaya Services package (cs-services). The avaya account provides you with administrative access to User Management. The default password for this account is set to avayapassword.

**Security alert:**

After you initially log on using the avaya account, immediately change the password. If you require a greater level of security for this account, see Creating a new User Management administrator account and removing the default avaya account from User Management on page 334.

**Procedure**

1. Log in to the AE Services Management Console as avaya with the default password.
   
   See Accounts installed with the Avaya Services package on page 327.
2. From the main menu, select **User Management > List All Users**.

3. From the **List All Users** page, select the option button for **avaya** and click **Edit**.

4. Update the password settings as follows:
   a. In the **New Password** field, enter a new password.
      
      The default User Management password policy, which is based on a US standard keyboard, calls for a minimum of 8 characters, including a minimum of 1 upper case, 1 lower case, 1 alphanumeric, and 1 special character. The following characters are not permitted: $ (dollar sign), ' (apostrophe), " (quotation mark), \ (backslash), the space character, and any ASCII control-character.

      **Note:**

      If you want the avaya user to be able to access all administrative domains, the password for the avaya account must be identical to the password for the Linux user described in **Adding a Linux System Administrator account (if the Avaya Service Package is not installed)** on page 331.

   b. In the **Confirm New Password** field, re-enter the new password.

5. Click **Apply**.

---

**Changing the default password for the cust account in User Management**

**About this task**

This topic applies only to an AE Services Software-Only server with the Avaya Services package (cs-services) installed.

AE Services installs the cust account in two locations — in the local Linux password store and in the User Management service (local LDAP directory).

**Note:**

If you require a greater level of security for this account, see **Creating a new System Administrator account** on page 330.

**Procedure**

1. From your browser, log in to the AE Services Management Console as cust with the default password.

   See **Accounts installed with the Avaya Services package** on page 327.

2. From the main menu, select **User Management > List All Users**.

3. From the **List All Users** page, select the option button for **cust** and click **Edit**.
4. Update the password settings as follows:
   a. In the **New Password** field, enter a new password.

   The default User Management password policy, which is based on a US standard keyboard, calls for a minimum of 8 characters, including a minimum of 1 upper case, 1 lower case, 1 alphanumeric, and 1 special character. The following characters are not permitted: $ (dollar sign), ' (apostrophe), " (quotation mark), \ (backslash), the space character, and any ASCII control-character.

   b. In the **Confirm New Password** field, re-enter the new password.

5. Click **Apply**.

---

**Creating a new User Management administrator account and removing the default avaya account from User Management**

**About this task**

Follow these steps to create a new User Management administrator account and delete the avaya account (avaya is the default User Management administrator account). This procedure applies to the Bundled Server, the Software-Only offer with the Avaya with services package (cs-service), and the Software-Only offer without the Avaya services package (cs-service).

**Procedure**

1. From your browser, log in to the AE Services Management Console as avaya with the default password (avayapassword).

2. From the main menu, select **User Management > Add User**.

3. Complete the **Add User** page as follows:
   a. In the **User Id** field, enter a user ID, for example **aesuseradmin**.
   b. In the **Common Name** field, enter the name the user prefers to use, for example **Pat Adams**.
   c. In the **Surname** field, enter the users last name, for example **Adams**.
   d. In the **User Password** field, enter a password.

   The default User Management password policy, which is based on a US standard keyboard, calls for a minimum of 8 characters, including a minimum of 1 upper case, 1 lower case, 1 alphanumeric, and 1 special character. The following characters are not permitted: $ (dollar sign), ' (apostrophe), " (quotation mark), \ (backslash), the space character, and any ASCII control-character.

   e. In the **Avaya Role** field, select **userservice.useradmin**.
Creating a new System Administrator account and removing the default cust account from User Management

About this task

For the Bundled Server and the Software-Only server with the Avaya Services Package (cs-service), AE Services installs the cust account in two locations — in the local Linux password store and in User Management (local LDAP directory).

If you do not want to use the User Management cust account, you can create a new User Management account that is equivalent to cust, and then remove the cust account from User Management.

Procedure

1. From your browser, log in to the AE Services Management Console as cust with the default password (custpw).

2. From the main menu, select User Management > User Admin > Add User.

3. Complete the Add User page as follows:
   a. In the User Id field, enter a user identifier, for example aesadmin.
   b. In the Common Name field, enter the name the user prefers to use, for example Jan Green.
   c. In the Surname field, enter the user's last name, for example Green.
   d. In the User Password field, enter a password.
      The default User Management password policy, which is based on a US standard keyboard, calls for a minimum of 8 characters, including a minimum of 1 upper case, 1 lower case, 1 alphanumeric, and 1 special character. The following characters are not permitted: $ (dollar sign), ' (apostrophe), " (quotation mark), \ (backslash), the space character, and any ASCII control-character.
   e. In the Avaya Role field, select userservice.useradmin.
   f. Click Apply.
4. Log out of the AE Services Management Console (you are logging out as cust).

5. Log in to the AE Services Management Console again with the user identifier and password you created in Step 3.

6. From the main menu, select **User Management > User Admin > List All Users**.

7. From the **List All Users** page, select the option button next to **cust**, and click **Delete**.

8. From the **Delete User** page, click **Delete**.
Chapter 24: Sample Device, Media, and Call Control applications

Sample application files on the AE Services server

An AE Services server includes following sample application-related files:

- The application properties file for the sample application (the tutorial properties file):
  /opt/mvap/cmapi/cmapijava-sdk/examples/resources/tutorial.properties
- The sample application media files including:
  /opt/mvap/cmapi/cmapijava-sdk/examples/media/0001.wav
  /opt/mvap/cmapi/cmapijava-sdk/examples/media/0002.wav
  /opt/mvap/cmapi/cmapijava-sdk/examples/media/0003.wav
  /opt/mvap/cmapi/cmapijava-sdk/examples/media/0004.wav
- A README file containing a description of how to set up and run the sample application:
  /opt/mvap/cmapi/cmapijava-sdk/examples/bin/SampleAppsReadme.txt

About the sample DMCC applications

To help support users of the Device, Media, and Call Control capabilities of AE Services, the AE Services software automatically installed several sample applications. This section describes how to administer and run one sample application to:

- Test connectivity between AE Services and Communication Manager
- Perform various tasks involved in running an application
- Learn which files are involved in running an application
- See some of the capabilities of an AE Services Device, Media, and Call Control application

The AE Services server also installs other sample applications. After you have checked the AE Services server and Communication Manager connectivity by running the tutorial application, you optionally can run the additional sample applications from a client application computer.
As an initial test, run the tutorial application directly on the AE Services server or on another computer. In general, run all other applications on a different computer from the AE Services server so you do not affect server performance. AE Services does not support co-resident applications.

Preparing to run the sample application

Procedure
1. Administer AE Services. See Administering AE Services for the sample application on page 338.
2. Administer Communication Manager.
   
   Note:
   You must also know the dial plan and which Communication Manager extensions are available.
3. Edit the tutorial properties file. See Editing the tutorial properties file on page 339.

Administering AE Services for the sample application

Procedure
1. From the AE Services Management Console, select AE Services > DMCC > Media Properties.
   (/tmp is the default directory.)
3. Accept the defaults for the remaining fields, and click Apply Changes.
5. On the Ports page, ensure that the DMCC Server Ports > Unencrypted Port is enabled.
6. If you enabled the Unencrypted Port, then select Maintenance > Service Controller and restart the DMCC service.
7. From the Linux command line, copy the application media files into the directory you specified in Step 2.
   For a list of media files, see Sample application files on the AE Services server on page 337.
Editing the tutorial properties file

About this task

Before you can run the sample application, you must edit the tutorial properties file (tutorial.properties) to provide information specific to your configuration.

Procedure

1. Using the text editor of your choice, open tutorial.properties:

   /opt/mvap/cmaipi/cmapi/java-sdk/examples/resources/tutorial.properties

   In Release 8.1.1, the tutorial.properties file contains the following text:

   ```
   # tutorial.properties
   #
   # Copyright (c) 2002-2007 Avaya Inc. All rights reserved.
   #
   # IP address of the call server (i.e, CLAN/PROCR/Gatekeeper), which AE Server
   # would
   # use to register the device (extension) to Communication
   # Manager
   callserver=nnn.nnn.nnn.nnn
   extension=xxxx
   password=yyyy
   
   # codec choices: g711U, g711A, g729, g729A
   codec=g711U
   
   # encryption choices: aes, none
   encryption=none
   
   cmapi1.server_ip=nnn.nnn.nnn.nnn
   cmapi1.username=username
   cmapi1.password=password
   cmapi1.server_port=4722
   
   # Legal values for cmapi1.secure are true and false.
   cmapi1.secure=true
   
   #cmapi.trust_store_location=sdk/build/mvsm/cmapi/java-sdk/examples/resources/avaya.jks
   #if you do not know cmapi.trust_store_password, leave it default
   #cmapi.trust_store_password=nnnn
   
   #cmapi.key_store_location=nnnn.jks
   #cmapi.key_store_password=nnnn
   
   #cmapi.certificate_validation=true
   #pattern xxx-yyyy,ppp-qqq,rrr-sss....
   extensions=41400-41599,50001-50200,51000-51060
   
   # by default getButtonInfo value is true.
   getButtonInfo=true
   #getButtonInfo=false
   
   # Legal values for cmapi1.secure are true and false.
   cmapi1.secure=true
   
   #cmapi.trust_store_location=sdk/build/mvsm/cmapi/java-sdk/examples/resources/avaya.jks
   #if you do not know cmapi.trust_store_password, leave it default
   #cmapi.trust_store_password=nnnn
   
   #cmapi.key_store_location=nnnn.jks
   #cmapi.key_store_password=nnnn
   
   #cmapi.certificate_validation=true
   #pattern xxx-yyyy,ppp-qqq,rrr-sss....
   extensions=41400-41599,50001-50200,51000-51060
   
   # by default getButtonInfo value is true.
   getButtonInfo=true
   #getButtonInfo=false
   ```

2. Replace the variables in the first three fields with the following values:

   a. For **callserver**, type the IP address of the media server for Communication Manager.
      
      • For Communication Manager S8300D, S8300E, and duplicated systems that use a
        Processor Ethernet (procr) this is the IP address of the media server.
      
      • For Communication Manager, duplicated systems that use a CLAN interface, this is
        the IP address of the CLAN.

   b. For **extension**, type the extension number of the station that you administered for this
      application.
c. For **password**, type the security code you administered for that station.

3. Add a user_id and user_password for the `cmapi1.username` and `cmapi1.password` properties.

   By default, these values are the username and password stored in the User Management database (local LDAP).

   ✪ **Note:**

   To see a list of these users, log in to the AE Services Management Console, and select **User Management > User Admin > List All Users**.

4. Set the `cmapi1.server_port=4721` and the `cmapi1.secure=false`.

5. Save and close the tutorial.properties file.

---

**Running the sample application**

**About this task**

Use this procedure to run the sample application.

**Before you begin**

The AE Services server must be running before you can run an application.

**Procedure**

1. Log in to the AE Services server using the SSH session.

2. On the AE Services server, change to the directory where the demonstration application run script resides:

   ```
   cd /opt/mvap/cmapi/cmapijava-sdk/examples/bin
   ```

3. Run the following command on the tutorial application:

   ```
   ./ant.sh runTutorial
   ```

   The application starts running. This application works as a softphone and waits for calls. When you call the extension from any other phone, the application answers with a recorded greeting that prompts you to record a message.

4. On the application, do the following:

   a. Call the extension and listen to the recorded greeting.

   b. Follow the prompts to record a message and have the system play it back to you.

   ✪ **Note:**

   The sample application can play only the last recorded message on a given call. If you make a new call, you can not hear a recording from a previous call. All the
recorded files are saved in the directory you specified as the location of the recorded files.

**Troubleshooting the sample application**

If the application does not run as expected:

1. View the following log files from `/var/log/avaya/aes` on the AE Services server:
   - `dmcc-error.log`
   - `dmcc-api.log`
   - `dmcc-trace.log`
   - `dmcc-wrapper.log`

   Use the `dmcc-error.log` file to check exceptions. The `dmcc-error.log` file is the latest log file.

2. See the following table for resolving the application error messages.

<table>
<thead>
<tr>
<th>Application error message</th>
<th>Troubleshooting procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration failed because Gatekeeper Reject reason: terminalExcluded</td>
<td>Verify that the extension number in <code>tutorial.properties</code> corresponds to a correctly administered extension number in Communication Manager.</td>
</tr>
<tr>
<td>Registration failed because Gatekeeper Reject reason: securityDenial</td>
<td>Verify that the password in <code>tutorial.properties</code> matches the password administered in Communication Manager for the station.</td>
</tr>
<tr>
<td>Registration failed because Protocol Timeout reason: GRQ timer, tried 3 times</td>
<td>Verify that the IP address in <code>tutorial.properties</code> for the call server (media server) is correct. Try to ping the media server from the AE Services server to verify connectivity.</td>
</tr>
<tr>
<td>Connection refused</td>
<td>• Verify that the IP address of the AE Services server is correct in the <code>tutorial.properties</code> file.</td>
</tr>
<tr>
<td></td>
<td>• Check for network problems between the client application computer and the AE Services server. For example, ping the AE Services server from the client application server.</td>
</tr>
<tr>
<td></td>
<td>• View the <code>/etc/hosts</code> files. Verify that you included a line that explicitly lists the IP address of the AE Services server, in addition to the localhost line.</td>
</tr>
<tr>
<td></td>
<td>• Verify that the <code>cmapi1.server_port=4721</code> is listed in the <code>tutorial.properties</code> file. Further verify that port 4721 is listening for incoming TCP connections. Use <code>netstat</code> command on the AE Services server.</td>
</tr>
</tbody>
</table>
Testing a DMCC configuration

About this task
You can test first party calls and third party calls.

Procedure

1. From the AE Services Management Console main menu, select **Utilities > Diagnostics > AE Service > DMCC Test**.
2. In the User box on the **DMCC Test** page, enter the user ID to log into AE Services.
3. In the User Password box, enter the password to log into AE Services.
4. Uncheck the **TLS** box.
5. From the Switch Name box, select the appropriate switch.
6. From the Switch IP box, select the IP address of the switch (optional).
7. In the Caller Extension box, enter the caller extension.
8. In the Caller Extension Password box, enter the password for the caller extension.
9. In the Callee Extension box, enter the callee extension.
10. In the Callee Extension Password box, enter the password for the callee extension.
11. Perform one of the following steps:
   • If you want make a first party call, click **Make First Party Call**.
     The First Party Call Test Result Page appears, displaying the results of the test.
   • If you want make a third party call, click **Make Third Party Call**.
     The Third Party Call Test Result Page appears, displaying the results of the test.
Chapter 25: Avaya Computer Telephony and CVLAN migration

TSAPI Client settings

If you are migrating from Avaya Computer Telephony, and you are using an IP address for the AE Services Server (AE Server) that is different than the IP address you used for the Avaya Computer Telephony Windows-based server, you must make sure that your clients can access the AE Services Server.

Depending on how you implemented your configuration, you might have to change your client configuration files. For information about editing client configuration files see the Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide, 02-300543.

Note:

If you are editing client template files (TSLIB.INI file for Windows or tslibrc for Linux) make sure that the address in the template file uses the externally facing IP address of your firewall instead of the IP address of the AE Server. For information about editing client configuration files see the Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide, 02-300543.

Migrating Avaya Computer Telephony users to AE Services

The AE Services Import SDB capability is designed to use the flat file created by backing up the Avaya Computer Telephony SDB. For more information about creating a flat file and backing up the Avaya Computer Telephony SDB, refer to Chapter 5, “Bulk Administration,” in the Avaya Computer Telephony 1.3, Telephony Services Administration and Maintenance Guide (this document is not included with AE Services, it is included with Avaya Computer Telephony Releases 1.2 and 1.3).
Migrating the Avaya Computer Telephony SDB to AE Services

About this task

Use this procedure to migrate your Avaya Computer Telephony SDB to AE Services. This is a one-time task that you perform when you are ready to migrate all members.

Procedure

1. On the Avaya Computer Telephony administrative workstation, navigate to Admin > Bulk Admin > Create Flat file from SDB.

   Use TSA 32 to create a flat file from the Avaya Computer Telephony SDB.


3. On the Import SDB page, click Choose File.

4. Select the Avaya Computer Telephony SDB backup file and click Open.

5. Click Import.

   AE Services updates the following:
   - The AE Services User Management database with your users. AE Services adds the users with the CT User flag set to yes.
   - The SDB file with the permission settings for worktops, devices, device groups, and Tlink groups. AE Services imports user passwords and Tlinks.

   The Tlink Groups are empty because Tlinks are not imported.


7. On the Tlink Groups page, select a Tlink Group, and click Edit Tlink Group.

8. On the Add/Edit Tlink Group page, select the Tlinks that you want to add to the Tlink Group, and click Apply Changes.

9. On the Apply Changes to Tlink Group properties page, click Apply.

Use User Management to add a CTI user

When you want to add a CTI user to AE Services, you must use the User Management Menu in the AE Services Management Console. That is, the AE Services Management Console Security menu (Security > Security Database) does not allow you to add a CTI User. See Adding a user to User Management on page 139.

Service Management (which controls User Management) periodically runs a synchronization process to update the Security Database. When the newly added user appears in the Security
Database, you can assign user permissions for the newly added user. See Administering CTI User settings on page 221.

---

### Alternative migration strategies for Avaya Computer Telephony

If you plan to use another source of authority (Windows Active Directory Services) for user authentication, but you want to use the TSAPI Service Security Database (SDB) for user authorization, you will need to add your users to the AE Services User Management database. The AE Services User Management database is the means for populating the SDB. For information about adding users to the AE Services User Management database, see Adding a user to User Management on page 139.

*Note:* If you plan to use Active Directory Services for user authentication and you do not plan to use the SDB, you can skip this section.

In terms of integrating with AE Services, the strategies are presented from the lowest level of integration to the highest. Bronze represents the lowest level of integration, Silver represents intermediate integration, and Gold represents complete integration.

---

### Avaya Computer Telephony bronze level integration

Bronze level integration is the lowest level of integration. Essentially it requires manually maintaining two sets of the same data.

**How bronze level integration works**

Here is a high-level description of how bronze level integration works for adding a new user. For an illustration see, Bronze Level Integration with Active Directory Services on page 346.

- **Provisioning:**
  - Add the user to the authoritative source (Windows Active Directory Services).
  - Add the user to AE Services User Management database with the CT User flag set to **yes**. This will effect an update to the AE Services SDB.

- **Authentication:**
  - A user attempts to log in (as a client of the TSAPI Service).
  - The user is authenticated against the Windows Active Directory Services based User Management.
  - User permissions are derived from the AE Services SDB.
Bronze level integration with Active Directory Services

1. Administrator enters new user in enterprise data store (first entry)

2. Administrator enters new user in AE Svcs Management Console (second entry)
   User Management > Add User (“CT User”)

3. Administrator uses AE Services Management Console to set up user permissions in SDB
   Security > Security Database >
   CTI Users > List All Users > Edit CTI User
   Add to device groups

Requires double entry (manual synchronization) between Legacy data store and AE Services User Database.
Avaya Computer Telephony silver level integration

Silver level integration represents a tighter coupling between your enterprise database (Windows Active Directory Services) and AE Services User Management database.

How silver level integration works

Here is a high-level description of how silver level integration works for adding a new user. For an illustration see Silver Level Integration with Active Directory Services on page 348.

- Provisioning:
  - Add the user to the authoritative source (Windows Active Directory Services).
  - Do either of the following:
    - Add the user to AE Services User Management database with the **CT User** flag set to **yes**. This will effect an update to the AE Services SDB (double-entry).
    - From User Management run `ldapdistributor`, which imports the user information from Windows Active Directory Services (manual synchronization).

- Authentication:
  - A user attempts to log in (as a client of the TSAPI Service).
  - The user is authenticated against Windows Active Directory services based User Management.
  - User permissions are derived from the AE Services SDB (which is created by virtue of either double-entry or synchronization).
Silver level integration with Active Directory Services

1. Administrator enters new user in enterprise data store (first entry)

2. Admin can use method A or B

   A. Double entry
   - Administrator adds new user in AE Services Management Console.
   - User Management > User Admin > Add User
     - set CT User to Yes.

   B. Single entry
   - Admin uses Service Management and distributor to propagate change from ADS to SDB.
     - User Management > Service Admin > Manage Distributors
     - From Distributor list, select Idapdistributor and click Synchronize.

3. Administrator uses AE Services Management Console to set up user permissions in SDB
   - Security > Security Database
     - CTI Users > List All Users > Edit CTI User
     - Add to device groups

Either double entry (manual) or single entry (automatic).
Avaya Computer Telephony gold level integration

Gold level integration means complete integration between your enterprise database, and AE Services. A single entry in your enterprise database automatically results in an entry in the AE Services SDB. Gold level integration, however, does require that you develop a solution. In effect you develop your own distributor.

How gold level integration works

Here is a high-level description of how gold level integration works for adding a new user. For an illustration see, Gold Level Integration with Active Directory Services on page 350.

• Provisioning:
  - Add the user to your enterprise user management system.
  - Your enterprise system contacts AE Services User Management via Simple Object Access Protocol (SOAP) interface, as a normal processing activity, to provide the update.
    • Your “enterprise_distributor” updates the AE Services User Management database.
    • The AE Services sdbdistributor updates the SDB.

• Authentication:
  - A user attempts to log in (as a client of the TSAPI Service).
  - The user is authenticated against the enterprise user management system.
  - User permissions are derived from the AE Services SDB.
Gold level integration with Active Directory Services

1. Administrator enters new user in their enterprise data store.

   enterprise_distributor

   AE Services User Management database automatically updates AE Services User Management Database

   CT User “yes”

   sdd_distributor

   AE Services User Management database automatically updates AE Services Security database

2. Administrator uses AE Services Management Console to set up user permissions in SDB

   Security > Security Database >
   CTI Users > List All Users > Edit CTI User
   Add to device groups

Single entry, complete integration requires developing an enterprise_distributor.
Migrating CVLAN to AE Services

Migrating CVLAN Server for Linux (Releases 9.0 and 9.1) to AE Services

About this task

AE Services does not provide a tool for migrating CVLAN Server for Linux (Releases 9.0 and 9.1) to AE Services. Migrating CVLAN Server R9.0 or R9.1 means that you are replacing a CVLAN R9.0 or R9.1 Server with the AE Services CVLAN Service for connectivity to Communication Manager 3.0, or later. You must manually obtain the CVLAN settings from Communication Manager and the CVLAN server, and then administer them on the AE Server.

Follow these steps to migrate CVLAN R9.0 or R9.1 to AE Services 3.1.

Procedure

1. Obtain the CVLAN settings on Communication Manager.
   See Obtaining the CVLAN settings from Communication Manager on page 351.

2. Obtain the CVLAN settings on the CVLAN Server.
   See Obtaining the CVLAN settings from the CVLAN R9.0 or R9.1 Server for Linux on page 352.

3. Administer the settings, which you obtained from Communication Manager and the CVLAN Server, on the AE Server.
   See Administering the CVLAN Settings on the AE Server on page 352.

Obtaining the CVLAN settings from Communication Manager

About this task

On Communication Manager, follow these steps to obtain the settings for the CTI link number and corresponding client link number for CVLAN.

Procedure

1. From the System Administration Terminal, type `change ip-services`.
2. From the IP Services screen, go to the DLG Administration screen.
3. Make a note of the CTI Link number and the corresponding Client Link number.

You administer this information to the AE Services Management Console when you administer the CVLAN Service. (See Administering the CVLAN Settings on the AE Server on page 352.)
Obtaining the CVLAN settings from the CVLAN R9.0 or R9.1 Server for Linux

About this task
On the CVLAN Server (R9.0 or R9.1), follow these steps to obtain the name or IP address of each CVLAN client.

Procedure
1. From your CVLAN Server (R9.0 or R9.1) select Administration > Links.
2. Select each link and click Edit Clients.
3. From the Edit Clients page, make a note of the Name or IP Address of each client associated with the CVLAN Link you selected.

Administering the CVLAN Settings on the AE Services Server

About this task
From the AE Server with an active license for the CVLAN service, administer the CVLAN Service for connectivity to Communication Manager by following these steps.

Procedure
1. Administer the NICs. See Administering the Local IP for a single NIC configuration on page 70.
2. Administer the switch connections. See Adding a switch connection on page 73.
3. Administer the CVLAN links. See Administering CVLAN Links on page 80.
   While performing this procedure from the AE Services Management Console, follow these steps:
   a. In the Signal field, use the Client Link number you noted on the Communication Manager 2.x DLG Administration Screen in Step 1.
   b. In the Switch CTI Link number field, use the CTI Link number you noted on the Communication Manager 2.x DLG Administration Screen in Step 1.
4. Test the CVLAN links. See Testing a CVLAN link on page 82.
5. Administer the CVLAN clients. See Adding CVLAN clients on page 82.
   When you perform this procedure, use the CVLAN client information you noted in Step 2.

Migrating the MAPD-based CVLAN to AE Services

About this task
AE Services does not provide a tool for migrating the MAPD-based CVLAN to AE Services. Migration for the MAPD-based CVLAN means that you are replacing a MAPD-based CVLAN Server with the AE Services 3.1 CVLAN Service for connectivity to Communication Manager 3.0.
To migrate the MAPD-based CVLAN from AE services, you must manually obtain the settings on the MAPD and then administer them on the AE Server.

**Procedure**

1. Obtain the CVLAN settings from the MAPD.
   
   See [Obtaining the CVLAN settings from the MAPD](#) on page 353.

2. Administer the CVLAN settings, which you obtained from the MAPD, on the AE Server.
   
   See [Administering the settings for CVLAN on the AE Server](#) on page 353.

**Obtaining the CVLAN settings from the MAPD**

**Procedure**

1. Log in to the MAPD.
   
   For example, `telnet <host name or IP address of MAPD>`

2. Enter the MAPD log in and password.

3. From the system prompt, type `eth_cam` to start the CVLAN screens.

4. From the main menu, select **CVLAN Administration**.

5. From the **CVLAN Administration** screen, follow these steps:
   
   a. From the **Node ID** column, make a note of the signal numbers (signal01, signal02, and so on).

   b. From the **Number of Clients** column, select each client number (1, 2, and so on), and make a note of the IP address of each client.

**Administering the settings for CVLAN on the AE Server**

**About this task**

Follow these steps to administer the CVLAN settings, which you obtained from the MAPD, on an AE Server with an active license for the CVLAN service

**Procedure**

1. Administer the NIC. See [Administering the Local IP for a single NIC configuration](#) on page 70.

2. Administer the switch connection. See [Adding a switch connection](#) on page 73.

3. Administer the CVLAN links. See [Administering CVLAN Links](#) on page 80.

   When you perform this procedure from the AE Services Management Console, follow these steps:
   
   a. In the **Signal** field, use the signal number you obtained on the MAPD. (See [Obtaining the CVLAN settings from the MAPD](#) on page 353.)

   b. In the **Switch CTI Link Number** field, use the client number you obtained on the MAPD. (See [Obtaining the CVLAN settings from the MAPD](#) on page 353.)
4. Test the CVLAN Links. See Testing a CVLAN Link on page 82.

5. Administer the CVLAN clients. See Adding CVLAN Clients on page 82. When you perform this procedure, use the CVLAN client information you noted in Step 2.
Chapter 26: System Manager Trust Management

Using Avaya Aura® System Manager as a Certificate Authority (CA) to generate signed certificates

About this task

Use this procedure to use the System Manager Trust Management feature as your PKI and create an End Entity for the AE Services server.

Procedure

1. On the System Manager web console, click Services > Security > Certificates > Authority > Add End Entity.
2. Under RA functions, click Add End Entity.
3. In the End Entity Profile field, click INBOUND_OUTBOUND_TLS.
4. Type a username and password. This password is used to encrypt the P12 trust store file, as shown below.
5. Complete the fields that you want in your certificate as follows:
   - mail address: labmanager@yourcompany.com
   - CN: Common name: aeshostname.yourcompany.com
   - OU: Organizational Unit: IT
   - O: Organization: Your Company Name
   - L: Locality: Denver
   - ST: State or Province: CO
   - C: Country: US
6. In the Certificate Profile drop down list, select ID_CLIENT_SERVER.
7. In the CA drop down list select tmdefaultca.
8. In the Token drop down list select P12 file.
9. Click Add.
**Creating the AE Services server certificate**

**Procedure**

1. Using the SMGR Web console, under Services, navigate to Security > Certificates > Authority
2. In the left hand navigation pane near the bottom of the screen, click on Public Web
3. On the Public Web screen click on create key store
   a. Enter the user name and password of the End Entity and click OK
   b. Select the certificate key length. 2048 is recommended
   c. Click on Enroll
   d. Save the server certificate to a known location.

*Note:*
This is the signed server certificate you have to import into the AE Services server.

**Downloading the SMGR CA certificate that signed the AE Services server certificate**

**Procedure**

1. Using the SMGR web console navigate to the Public Web page as described previously. Click Fetch CA certificates
2. Click Download PEM chain on the line starting with CA certificate chain
3. Save the CA certificate to a known location.
   This is the CA certificate that needs to be imported into the AE Services server.
Importing the SMGR CA certificate into the AE Services server

Procedure

1. Using the AE Services Management Console navigate to Security > Certificate Management > CA Trusted Certificates.
2. Click on the Import button and upload the SMGR CA certificate you downloaded previously. Give it an alias name, for example caSMGR.
3. Click the Apply button.

🌟 Note:
You need to import this CA before you can import the AE Services server certificate.

Importing the new AE Services server certificate into the AE Services server

Procedure

2. Click on the Import button and upload the new AE Services server certificate you created previously. Select an alias, for example server from the drop down menu and Click Apply.
3. Enter the password you used while creating the End Entity.
4. Click the Apply button and then click the Apply button again on the following page.

🌟 Note:
You need to import the CA before you can import the AE Services server certificate.

HTTPS, WebLM, and AE Services

HTTPS is used for connecting a Master Avaya WebLM server and the AE Services Avaya WebLM client or embedded Local Avaya WebLM. The Master Avaya WebLM server can operate in an allocation mode or a pooled mode or both. For the allocation mode, the Master Avaya WebLM server acts as a client of the AE Services embedded Avaya WebLM to establish an HTTPS session and push a license file down to the AE Services embedded Local Avaya WebLM. For the pooled mode, the AE Services C++ and Java Avaya WebLM clients establish an HTTPS session to the Master Avaya WebLM server or the AE Services embedded Local Avaya WebLM to acquire a license.
During the TLS handshake, for an HTTPS client-server session, the server must send its identity certificate to the client and the client must validate the server’s identity certificate. For example, the Not Before date and the Not After date timeframe is valid, and the server identity certificate was signed by a trusted Certificate Authority (CA) known by the client. If the client is unable to validate the server’s identity certificate, the handshake connection is terminated.

**Note:**
- For the pooled mode, the Master Avaya WebLM CA certificates must be imported into the AE Services Trusted Certificate store using the AE Services Management Console.
- For the allocation mode, the AE Services Apache Web server CA certificates must be imported into the Master Avaya WebLM trust store.

While attempting to connect to Avaya WebLM from the AE Services server or from a Master Avaya WebLM to the AE Services embedded Local Avaya WebLM, the connection might not get established. The following are some troubleshooting suggestions:

- **Pooled mode:** Using the Management Console, verify that the CA certificate used to sign the Master Avaya WebLM server’s identity certificate is in the AE Services Trusted Certificate store. For a default System Manager installation where the Master Avaya WebLM is also embedded, the System Manager’s embedded CA is used to sign the System Manager server identity certificate. Each System Manager deployment creates its own unique CA certificate with the same Common Name. Therefore, when validating whether the System Manager CA certificate is installed on the AE Services server, ensure that the System Manager CA certificate Serial ID matches the Serial ID of the System Manager CA certificate in the AE Services trust store.

- **Allocation mode:** Verify that the CA certificate used to sign the AE Services server identity certificate is in the Master Avaya WebLM trust store.

- Verify that the port is not blocked by a firewall.

- Verify that the Avaya WebLM server identity certificate has not expired.

- Check the AE Services log files for a TLS/SSL connection error, for example, using an unknown certificate.
Chapter 27: OpenSSL as a Certificate Authority (CA)

Using OpenSSL as a Certificate Authority (CA) to generate signed certificates

The following steps use a key size, cipher, and a single-level CA, instead of a multi-level CA infrastructure, that may be considered inefficient to support your IT security requirements. It is recommended that you review the OpenSSL commands and make the necessary changes to meet or exceed your certificate security requirements. These commands are provided as is, use at your own risk, with no guarantee that they will protect your network from a possible intrusion.

The OpenSSL package is available on all Linux distributions, Windows, for example cygwin and is available for download from the OpenSSL Web site.

On a Linux server, use the man command, for example man genrsa to find out additional information on the openssl commands like genrsa, req, x509, ca, and pkcs12.

The following steps are based on the Linux® Operating System and explain how to create a single-level CA.

Setting up the OpenSSL CA

Creating the certificate directory structure

Procedure

1. Create a directory to serve as your certificate home directory, by typing the command, mkdir certificates.
2. Change directory to the certificates home directory, by typing the command cd certificates.
3. From the Linux® Operating System command line interface (CLI), run the following commands:
   • mkdir CA
   • mkdir CA/certs
   • mkdir CA/crl
   • mkdir CA/newcerts
   • mkdir CA/private
   • touch CA/index.txt
   • touch CA/private/cakey.pem
   • touch CA/serial

---

**Configuring the OpenSSL configuration file**

**Procedure**

1. Determine the location of OpenSSL's default openssl.cnf file. On RHEL, it is at /etc/pki/tls/openssl.cnf. If not, use the find command to locate the file, that is find / -name openssl.cnf

2. Copy the openssl.cnf file to the certificates home directory, for example cp /etc/pki/tls/openssl.cnf /certificates

3. Change directories to the certificates home directory, for example cd /certificates

4. Edit the copied version of the openssl.cnf file with the following changes, for example vi /certificates/openssl.cnf
   - Modify the following line in the section [ CA_default ]
     Change from:
     dir = ../../CA
     Change to:
     dir = ./CA
   - Comment out the two appearances of the following line:
     Change from:
     nsComment = "OpenSSL Generated Certificate"
     Change to:
     #nsComment = "OpenSSL Generated Certificate"
   - Uncomment the following line and add v3_req to extensions.
     Change from:
# X.509v3 extensions to use:
extensions =

Change to:

# X.509v3 extensions to use:
extensions = v3_req

• Uncomment the following line.

Change from:

# req_extensions = v3_req # The extensions to add to a certificate request.
Change to:

req_extensions = v3_req # The extensions to add to a certificate request.

• Change the following line in the [ v3_req ] section.

Change from:

keyUsage = nonRepudiation, digitalSignature, keyEncipherment
Change to:

keyUsage = nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment

• Add the following line to the [ v3_req ] section.

extendedKeyUsage=serverAuth,clientAuth

• Add the following line to the [ usr_cert ] section.

Change from:

# These extensions are added when 'ca' signs a request.
Change to:

# These extensions are added when 'ca' signs a request.

keyUsage = nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage=serverAuth,clientAuth

• Change string_mask in the [ req ] section to the following:

- string_mask = MASK:0x2002

• If you want to use a message digest higher than sha1, for example sha256, change the option default_md in the [ req ] section.

5. Save changes to the openssl.cnf file.
Creating the CA root key and self-signed certificate

Procedure

1. Change directories to the certificates home directory, for example: cd /certificates

2. Create the CA key by operating the following command:

   openssl genrsa -des3 -out cakey.pem 2048

   You will be asked for a password to encrypt the CA root key, and then you will be asked to provide that password again as verification. The key will be encrypted using triple des, for example: des3. You will be asked for this password when signing the CSR. The size of the key will be 2048 bits. The key will be saved to the file cakey.pem.

3. Run the following command to create the CA public certificate signed by the CA key:

   openssl req -new -x509 -days 3650 -key cakey.pem -out cacert.pem -config openssl.cnf

   You will be asked for the CA root key password. The public CA certificate will expire in 10 years. In order to change the expiration, modify the –days option. The certificate will be saved in the file cacert.pem. The openssl.cnf will be used to apply some configuration values. You will be asked to enter information that will be incorporated into your certificate request. Leave the Email Address field blank.

   An example:

   • Country Name (2 letter code) [GB]:US
   • State or Province Name (full name) [Berkshire]:CO
   • Locality Name (eg, city)[Newbury]:Denver
   • Organization Name (eg, company) [My Company Ltd]:Your Company Name
   • Organizational Unit Name (eg, section) []:IT
   • Common Name for example your name or your server's hostname) []:YourCompanyName Root CA
   • Email Address []:

4. Move the generated CA root key to the CA/private directory, that is mv cakey.pem ./CA/private/

5. Move the generated CA public certificate to the CA directory, that is mv cacert.pem ./CA/

6. You can view the contents of the CA public certificate with the following command:

   openssl x509 -in ./CA/cacert.pem -text -noout
Note:
Your CA is now configured and ready to issue certificates. This CA can be used to create all your AE Services server certificates. Only the CA certificate will need to be imported into your clients trust certificate store.

Generating a server certificate for each AE Services server

Creating a Certificate Signing Request (CSR) and key for each of your AE Services server

Procedure

1. Login to the AE Services Management console of the server for which you need to create the certificate

   a. To select the Certificate Alias, select either server or aeservices from the drop down menu.
   b. To select the Enrollment Method, select Manual from the drop down menu
   c. To select the Encryption Algorithm, select 3DES from the drop down menu
   d. Enter a password in the Password field. This password will be used to encrypt the private key associated with the certificate. The encrypted private key will be kept on the AE Services server. Re-enter the password for verification
   e. To select the Key Size, select 2048 from the drop down menu
   f. Under Signature Algorithm, select sha256 from the drop down menu. If your client does not support sha256, select sha1
   g. For the Certificate Validity, enter the number of days you want this certificate to be valid. For example, for 5 years, it would be 1825 days.
   h. To select a Distinguished Name (DN), enter as per the below hints:
      • C=US
      • ST=CO
      • L=yourCity
      • O=YourCompanyName
      • OU=yourOrg
• **CN=aeshostname**

**Note:**

The **C** value US, the **ST** value CO and the **O** value that is **YourCompany** must match the country name, state name and the company name of the CA certificate for the CA certificate to be able to sign the CSR.

i. Modify the **Key Usage** by holding down the **Ctrl** key on the keyboard. Select the **Digital Signature**, **Non-repudiation**, **Key encipherment**, and **Data encipherment** options.

j. To set the **Extended Key Usage**, hold the **Ctrl** key down on the keyboard. Select the **SSL/TSL Web Server Authentication** and **SSL/TLS Web Client Authentication** options. Leave all other fields empty.

k. Click **Apply**

3. From the **Server Certificate Manual Enrollment Request** page, copy the CSR certificate in the window starting with **-----BEGIN CERTIFICATE REQUEST-----** and ending with **-----END CERTIFICATE REQUEST-----**. Save the CSR to a file named **myserver.req** in the /certificate directory on the server where the CA certificate was created.

---

**Signing the AE Services server CSR**

**About this task**

By using the server where the CA certificate was created, sign the AE Services server CSR as follows:

**Procedure**

1. Change directories to the certificates home directory, for example `cd /certificates`

2. Create a serial number for the certificate by using the following command:
   ```bash
   tr -c -d 0-9 < /dev/urandom | head -c 10 > ./CA/serial
   ```

3. Sign the CSR by using the following command:
   ```bash
   openssl ca -config openssl.cnf -days 730 -out myserver.crt -infiles myserver.req
   ```

   The `openssl.cnf` file will be used to apply some configuration options. The signed public certificate will expire in 2 years. In order to change the expiration modify the option –days. The certificate will be saved in the file `myserver.crt`. The CSR is in the file `myserver.req`. You will be asked for the CA root key password to sign the CSR and confirmation to sign and commit the request.

4. View the contents of the newly signed public server certificate with the following command:
   ```bash
   openssl x509 -in ./ myserver.crt -text -noout
   ```
Importing the public CA certificate into the AE Services trust certificate store

Procedure

1. Import the public CA certificate into the AE Services trust certificate store using the AE Services Management Console as follows:
   
   a. Using the AE Services Management Console navigate to Security > Certificate Management > CA Trusted Certificates
   
   b. Click the Choose File button and upload the OpenSSL-generated CA certificate you created above. Give it an alias name, for example `myCA` and click Apply

   🔄 Note:
   
   The CA certificate must be imported before the signed server certificate can be imported into the AE Services server in the next step.

2. Import the `myserver.crt` file created in the previous step into the AE Services server using the AE Services Management Console.

   a. Using the AE Services Management Console, navigate to Security > Certificate Management > Server Certificates
   
   b. Click the Choose File button and upload the new AE Services server certificate, that is `myserver.crt` you created above. Select the alias you chose when creating the CSR, that is `server` or `aeservices` from the drop down menu and click Apply

   🔄 Note:
   
   Make sure that the AE Services server and the server where the CA was created are properly time synchronized to an NTP server.

3. Import the public CA certificate into the AE Services related clients trust certificate stores.

   🔄 Note:
   
   Repeat the CSR creation and subsequent steps for different AE Services servers and use the same CA to sign each of the CSRs. This way all the AE Services clients only need to know one CA certificate, that signed all the AE Services server certificates.
# Chapter 28: Resources

## Application Enablement Services documentation

The following table lists the documents related to Application Enablement Services. Download the documents from the Avaya Support website at [http://support.avaya.com](http://support.avaya.com).

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Design</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya Aura® Application Enablement Services Overview and Specification</td>
<td>Understand high-level product features and functionality.</td>
<td>Customers and sales, services, and support personnel</td>
</tr>
<tr>
<td>Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide</td>
<td>Installing TSAPI and CVLAN Client and SDK</td>
<td>Customers and sales, services, and support personnel</td>
</tr>
<tr>
<td><strong>Using</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upgrading Avaya Aura® Application Enablement Services</td>
<td>Upgrading Application Enablement Services applications.</td>
<td>System administrators and IT personnel</td>
</tr>
<tr>
<td>Administering Avaya Aura® Application Enablement Services</td>
<td>Administering Application Enablement Services applications and install patches on Application Enablement Services applications.</td>
<td>System administrators and IT personnel</td>
</tr>
<tr>
<td><strong>Implementation</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deploying Avaya Aura® Application Enablement Services for Microsoft® Lync Server Products</td>
<td>Deploy Application Enablement Services applications in Microsoft Lync Server Products</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td>Deploying Avaya Aura® Application Enablement Services in Virtual Appliance</td>
<td>Deploy Application Enablement Services applications in Virtual Appliance</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td>Deploying Avaya Aura® Application Enablement Services in Virtualized Environment</td>
<td>Deploy Application Enablement Services applications in Virtualized Environment</td>
<td>Implementation personnel</td>
</tr>
</tbody>
</table>

Table continues…
## Related links

- Finding documents on the Avaya Support website on page 367
- Accessing the port matrix document on page 368
- Avaya Documentation Portal navigation on page 368

## Finding documents on the Avaya Support website

**Procedure**

1. Go to [https://support.avaya.com](https://support.avaya.com).
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product > Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.
   - The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.
   - For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

**Related links**

- Application Enablement Services documentation on page 366
Accessing the port matrix document

Procedure

2. Log on to the Avaya website with a valid Avaya user ID and password.
4. In Enter Your Product Here, type the product name, and then select the product from the list of suggested product names.
5. In Choose Release, select the required release number.
6. In the Content Type filter, select one or more of the following categories:
   • Application & Technical Notes
   • Design, Development & System Mgt
     The list displays the product-specific Port Matrix document.
7. Click Enter.

Related links

Application Enablement Services documentation on page 366

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com.

⚠ Important:

For documents that are not available on the Avaya Documentation Portal, click Support on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Portal, you can:

• Search for content in one of the following ways:
  - Type a keyword in the Search field.
  - Type a keyword in Search, and click Filters to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
• Find a document from the Publications menu.
• Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
• Add content to your collection by using My Docs (⭐).
Navigate to the My Content > My Docs menu, and do any of the following:

- Create, rename, and delete a collection.
- Add content from various documents to a collection.
- Save a PDF of selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive content that others have shared with you.

* Add yourself as a watcher by using the Watch icon (👀).

Navigate to the My Content > Watch list menu, and do the following:

- Set how frequently you want to be notified, starting from every day to every 60 days.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

🌟 Note:

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

Related links

Application Enablement Services documentation on page 366

---

**Training**

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

<table>
<thead>
<tr>
<th>Course code</th>
<th>Course title</th>
</tr>
</thead>
<tbody>
<tr>
<td>20980W</td>
<td>What's New with Avaya Aura® Release 8.1</td>
</tr>
</tbody>
</table>

---

**Viewing Avaya Mentor videos**

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.
About this task
Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

• To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In Search, type Avaya Mentor Videos, click Clear All and select Video in the Content Type.
  - In Search, type the product name. On the Search Results page, click Clear All and select Video in the Content Type.
  The Video content type is displayed only when videos are available for that product.
  In the right pane, the page displays a list of available videos.
• To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

★ Note:
Videos are not available for all products.

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

Related links
Using the Avaya InSite Knowledge Base on page 370

Using the Avaya InSite Knowledge Base
The Avaya InSite Knowledge Base is a web-based search engine that provides:
• Up-to-date troubleshooting procedures and technical tips
• Information about service packs
• Access to customer and technical documentation
• Information about training and certification programs
• Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

2. Log on to the Avaya website with a valid Avaya user ID and password.
   The system displays the Avaya Support page.
3. Click **Support by Product > Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press **Enter**.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Related links

[Support](#) on page 370
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alphanumeric</td>
<td>A character string that is a combination of letters of the alphabet and numbers.</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface. Software that applications use to interact with network services, telephony services, and so forth.</td>
</tr>
<tr>
<td>ASAI</td>
<td>Adjunct Switch Application Interface. ASAI is a protocol that enables software applications to access call processing capabilities provided by Avaya Communication Manager.</td>
</tr>
<tr>
<td>Association</td>
<td>A communication channel between the adjunct and switch for messaging purposes. An active association is an existing call in the Communication Manager call processing domain or an extension on the call.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The process of validating the identity of a user by means of user profile attributes.</td>
</tr>
<tr>
<td>Authorization</td>
<td>The process of granting a user the ability to carry out certain activities based on permissions.</td>
</tr>
<tr>
<td>Automatic Call Distribution</td>
<td>A feature that answers calls, and then depending on administered instructions, delivers messages appropriate for the caller and routes the call to an agent when one becomes available.</td>
</tr>
<tr>
<td>Breadcrumb</td>
<td>Refers to the part of the navigation bar on a Web site that shows the location of the current web page relative to the site hierarchy. For example: Server Status</td>
</tr>
<tr>
<td>Call control</td>
<td>Call control refers to the group of services that enable a telephony client application to control a call or connection on Communication Manager. These services are typically used for placing calls from a device and controlling any connection on a single call as the call moves through Communication Manager. The CVLAN Service, the DLG Service and the</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TSAPI Service (which includes the Telephony Web Service and JTAPI)</td>
<td>provide client applications with call control capabilities.</td>
</tr>
<tr>
<td><strong>Call Information Services</strong></td>
<td>Avaya Call Information Services is a collection of services that allows applications to get detailed call information (such as VDN number, agent ID, and so forth) and to determine the status of the AE Services call information link.</td>
</tr>
<tr>
<td><strong>Call/call monitor</strong></td>
<td>An SDB term. A call/call monitor is software that tracks call activity on the basis of a call ID (a unique identifier of the call being handled by Communication Manager). Users either have or do not have call/call monitoring permission; you do not need to create a device group for call/call monitoring access rights. Contrast with device monitors and device/device monitors, which are based on a device ID.</td>
</tr>
<tr>
<td><strong>Call/device monitor</strong></td>
<td>An SDB term. Call/device monitors are used to track events for a call once it reaches the device being monitored. Unlike device/device monitors, events for a call continue to be received even after the call leaves the device.</td>
</tr>
<tr>
<td><strong>Certificate authority (CA)</strong></td>
<td>A certificate authority is an organization that issues and manages security credentials, including digitally signed certificates containing public keys for message encryption and decryption.</td>
</tr>
<tr>
<td><strong>CN</strong></td>
<td>Common name. See <a href="#">Common name</a> on page 373.</td>
</tr>
<tr>
<td><strong>Common name</strong></td>
<td>In terms of <a href="#">LDAP</a> on page 376 it can refer to the name a user prefers to use (such as a first name, a middle name, a nickname, a first and last name, and so forth). It can also refer to the name of a resource, such as a computer.</td>
</tr>
<tr>
<td><strong>Common User Store</strong></td>
<td>The pool of shared user profile attributes maintained in the Lightweight Directory Access Protocol (<a href="#">LDAP</a> on page 376) database. In other words, a common repository of user profiles. See also, <a href="#">Profile</a> on page 377.</td>
</tr>
<tr>
<td><strong>Communication Manager API</strong></td>
<td>The <a href="#">Device, Media, and Call Control</a> on page 374 API supersedes Communication Manager API (or CMAPI). Communication Manager API is the former name of a service that provided connectivity between applications (that provide device and media control) and Communication Manager.</td>
</tr>
<tr>
<td><strong>Computer Telephony Integration</strong></td>
<td>CTI. CTI is the integration of services provided by a computer and a telephone. In simplest terms it means connecting a computer to a communications server (or switch) and having the computer issue commands that control calls.</td>
</tr>
</tbody>
</table>
### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection name</strong></td>
<td>See <a href="#">Switch connection names</a> on page 378.</td>
</tr>
<tr>
<td><strong>CT User</strong></td>
<td>An abbreviation for Computer Telephony User. A user (or an application) administered in the AE Services User Management (local LDAP) as a CT User derives authorization from the Security Database. CT Users include the following users or applications: TSAPI Service users (including JTAPI users), Telephony Web Service users, and DMCC users who use Call Control Services.</td>
</tr>
<tr>
<td><strong>CTI link</strong></td>
<td>The term CTI link refers to a generic link type that is used in the context of Communication Manager administration. As a generic link type, it can refer to any of the following AE Services links: CVLAN Links, DLG links, and TSAPI links (the Call Control Services, the Telephony Web Service, and JTAPI use the TSAPI Service). On an AE Services Management Console page, such as the TSAPI Services Summary, the column heading for Switch CTI link ID refers to a TSAPI link as it is administered on Communication Manager.</td>
</tr>
<tr>
<td><strong>CTI User</strong></td>
<td>Computer Telephony Integration user (synonymous with CT User). See <a href="#">CT User</a> on page 374.</td>
</tr>
<tr>
<td><strong>CUS</strong></td>
<td>Common User Store. See <a href="#">Common User Store</a> on page 373.</td>
</tr>
<tr>
<td><strong>DES</strong></td>
<td>Data Encryption Standard. DES is a United States Government Sanctioned encryption algorithm described in Federal Information Processing Standards Publication, FIPS PUB 46-1 or ANSI Standard X3.92. DES uses 64 bit keys of which 56 bits are used by the algorithm and 8 are used for error detection.</td>
</tr>
<tr>
<td><strong>Device</strong></td>
<td>An SDB term. A device can be a telephone, a FAX, an ACD, a VDN, or an agent ID that Communication Manager controls. In the Security Database, a device has the following attributes: Device ID (which is administered on Communication Manager, see <a href="#">Device ID</a> on page 374), Location, Device Type, and Tlink Group.</td>
</tr>
<tr>
<td><strong>Device group</strong></td>
<td>An SDB term. A device group refers to a named list of devices in the Security Database. You can assign device groups to users and worktops.</td>
</tr>
<tr>
<td><strong>Device ID</strong></td>
<td>An SDB term. A Device ID is a 2 to 13-digit number for a phone, fax, modem, ACD, VDN, or agent id that is administered on Communication Manager. This is not the full 7 or 10 digit number used by the public network.</td>
</tr>
<tr>
<td><strong>Device, Media, and Call Control</strong></td>
<td>Device, Media, and Call Control (DMCC) refers to the service that provides first party call control (Device and Media control or Device and Media Control with Call Information Services) as well as third party call control (Device and Media Control and Call Control Services. Call Control services provides an extended set of third party call control services.</td>
</tr>
<tr>
<td><strong>Device/device</strong></td>
<td>An SDB term. Device/device refers to either a device/device monitor or a device/device monitoring group in the Security Database. An application places a device monitor on a specific device so it can receive an event report any time an event occurs at that device. For example, if the device receives an incoming call or originates an outgoing call, the application receives an event report. Device monitors are the most commonly used monitor. By default, all have this permission for the devices associated with their worktop.</td>
</tr>
<tr>
<td><strong>Distinguished name</strong></td>
<td>An LDAP protocol term. A distinguished name (DN) is unique identifier for an entry in a directory. A distinguished name is a hierarchical identifier, and as such, a distinguished name can consist of a series of relative distinguished names.</td>
</tr>
<tr>
<td><strong>Distributors</strong></td>
<td>Components of User Management that propagate changes, such as additions, changes or deletions from an application to the local LDAP database. The AE Services provides two distributors, the SDB distributor and the Generic LDAP distributor. See also Synchronize on page 378.</td>
</tr>
<tr>
<td><strong>DMCC</strong></td>
<td>See Device, Media, and Call Control on page 374.</td>
</tr>
<tr>
<td><strong>DN</strong></td>
<td>Distinguished Name. See Distinguished name on page 375.</td>
</tr>
<tr>
<td><strong>Domain controller</strong></td>
<td>Microsoft Windows based term for computer running XP Server that uses a common directory for storing account information for a complete domain.</td>
</tr>
<tr>
<td><strong>DTMF</strong></td>
<td>Dual-Tone Multi-Frequency. DTMF is a generic term for the method of pushbutton signaling from voice terminals using the voice transmission path. The code for DTMF Signaling provides 16 distinct signals, each composed of 2 voiceband frequencies (one from each of 2 mutually exclusive frequency groups of 4 frequencies each). DTMF tones are commonly known as touch tones.</td>
</tr>
<tr>
<td><strong>Exception group</strong></td>
<td>An SDB term. An exception group is a way of managing a large list by using the principle of exclusion. An exception group contains only the excluded members or the exceptions. For example, suppose Mary is a supervisor with permission to control all of the phones in the organization, except those that belong to the president and the vice president. Instead of setting up a device group that contains all of the devices except the president’s phone and the vice-president’s phone, you could set up an exception group and assign it to Mary. This exception group would contain the phones of the president and vice president.</td>
</tr>
<tr>
<td><strong>First party call control</strong></td>
<td>First party call control refers to the application acting as the user to operate a telephone. The application invokes operations such as “Go off-hook”, “Press button,” and so forth, until the switch collects enough digits to initiate the call.</td>
</tr>
</tbody>
</table>
Fully Qualified Domain Name (FQDN)

FQDN is the complete domain name of a computer in an Internet Protocol network. The FQDN includes all higher level domains.

Heartbeat

The heartbeat capability allows a client to query the server for the status of a CTI link. Heartbeat is a two-way capability. Communication Manager (as the client) can issue the heartbeat to the AE Server, or the AE Server (as the client) can issue a heartbeat to Communication Manager. Additionally, an AE Services client, such as TSAPI, JTAPI, or CVLAN can initiate a heartbeat to the AE Server.

In the AE Services Management Console you can set heartbeat state to Off or On. If heartbeat is set to off, Communication Manager initiates a heartbeat request. If the heartbeat is set to on, AE Server initiates the heartbeat request.

Host name

A name you assign to a host computer such as an AE Server. A Host name can consist of only the following characters: a through z (uppercase or lower case), the digits 0 through 9, and the hyphen. Host names must begin with a character from a through z, and they must end in either a character or a number. AE Services assumes that host names are mapped to IP addresses and can be validated by DNS.

JTAPI

Java Telephony Application Programming Interface. JTAPI is an API that provides access to the complete set of Third Party call control features provided by the TSAPI Service. JTAPI uses the TSAPI Service for communication with Avaya Communication Manager.

Kerberos

Kerberos is a network authentication protocol that lets users authenticate themselves using a secure server.

Keystore

A file that contains public and private keys.

LDAP

Lightweight Directory Access Protocol. LDAP defines a standard protocol for organizing directory hierarchies and a standard interface for clients to access directory servers.

MIB

Management Information Base. MIB is a component of SNMP. It defines what information a device’s SNMP agent is capable of reporting. It is a list of all the types of information an SNMP manager can poll an SNMP agent for, as well as the traps an SNMP agent can send to an SNMP manager. The Application Enablement Services MIB resides on the AE Server.

Monitor

An SDB term. A monitor is a TSAPI Service capability that watches for activity on a call or a device. A monitor placed on a device or a call causes reports of changes in the status of the device or call to be sent to the client requesting the monitor. If your application places a device monitor on your phone, your application is notified of any change in your phone’s status (for example an incoming call has been received, a call...
has ended, and so forth). Many applications rely on monitors to provide this type of information.

**OAM**
Operations, Administration, and Maintenance. This term is superseded by the term Application Enablement Services Management Console (AE Services Management Console).

**PAM**
Pluggable Authentication Module. PAM is software that accommodates different authentication methods.

**PKI**
Public key Infrastructure. PKI is a system or framework that provides users of a non-secure public network to securely and privately exchange data through the use of a cryptographic key pair that is provided by a trusted authority, typically a certificate authority. A public key infrastructure includes a certificate authority (CA), a registration authority (RA) and a means of managing certificates.

**Primary device ID**
An SDB term. The primary device ID is the primary device at a user’s worktop. Usually it is the extension of the telephone on the worktop.

**Private data**
A TSAPI term. Private data is a switch-specific software implementation that provides value added services.

**Profile**
A set of attributes that represents a specific user in AE Services User Management.

**Routing**
In the sense of adjunct routing, routing is a capability for selecting an appropriate path for a call. When a routing application is started, it sends route registration requests, which contain a device ID, to Communication Manager. Routing requests instruct Communication Manager to send all incoming calls to these device IDs (in the TSAPI Service). The TSAPI Service sends the call to the application for routing. Communication Manager does not route these calls. Also referred to as adjunct routing.

In terms of access privileges (Allow Routing on Listed Device), routing refers to the ability to register with Communication Manager to route calls (as in adjunct routing). A CT User (or an application) can perform routing for a device or a device group. Routing privileges can be granted only by administering access privileges (Allow Routing on Listed Device).

**SATA**
Serial Advanced Technology Attachment (Serial ATA).

**Secondary device group**
An SDB term. A group of devices (in addition to the primary device) that are associated with the worktop or are shared among worktops. Users assigned to this worktop have permission to control and monitor all devices in this group.

**Security Database (SDB)**
SDB is a database that stores information about CT Users and the devices they control. The TSAPI Service uses this information in its permission checking. Administrators can control user access to the
TSAPI Service by placing restriction on the types of request users can make. The TSAPI Service uses the Postgres database for the SDB.

**Server Certificate**
Certificate generated on the server, which have both the private and public key pairs. Server Certificates are stored in both certificate form and PKCS12 form. Server Certificates are typically used as identity certificates by the server applications. For example, a web server would use a PKCS12 file (certificate) for establishing SSL.

**Service administration**
A set of functions in the AE Services Management Console that provide you with the ability to manage the User Management Service.

**Simple Network Management Protocol (SNMP)**
SNMP is a standard network management protocol that is used to remotely monitor and manage network-capable devices such as computers, switches, and gateways. SNMP provides a way for monitored objects (SNMP agents) and monitoring objects (SNMP managers) to exchange status messages.

**SNMP agent**
The component in an SNMP managed network that collects and stores status information and makes it available to the SNMP manager. One of its capabilities is to send traps (alarm notifications) to an SNMP agent when a device failure occurs.

**SNMP manager**
The SNMP manager is the component in an SNMP managed network that communicates with SNMP agents. It can issue requests for information and it can receive unsolicited notifications from SNMP agents. Unsolicited notifications are referred to as traps.

**Switch connection names**
A Switch Connection Name is a term that refers to either of the following:

- For the TSAPI Service, the Telephony Web Service, the CVLAN Service, and the DLG Service, a collection of host names or IP addresses associated with one (and only one) switch.

  **Important:**
  
  If you use multiple switch connection names, the total number of IP addresses and host names can not exceed 64 for a given AE Services Server. That is, if you use two switch connection names, SCA and SCB, the total number of names and IP addresses (or host names) can not exceed 64.

- For the DMCC Service, a collection of H.323 Gatekeepers that are associated with one (and only one) switch.

**Synchronize**
In the context of User Management, the Synchronize feature is used to trigger a synchronization of user data between the local LDAP database and an application user space (for example, the Security Database) through a Distributor connection. The Synchronize button on the Distributor List page provides administrators with a way to trigger the
Telephony Web Service

The Telephony Web Service is an API that provides access to basic subset of Third Party call control features of Communication Manager. It relies on the TSAPI Service to communicate with Communication Manager.

Third-party call control

Third-party call control means that, rather than acting as the user, the application is making requests on the behalf of the user. A third-party make call says “Make a call from extension X to extension Y”.

Tlink

A Tlink is a service identifier that is created when the administrator adds a TSAPI link in the AE Services Management Console. A Tlink refers to a switch connection between a specific switch and a specific AE Server.

TLS

Transport Layer Security. TLS is a protocol that guarantees privacy and data integrity between client and server components communicating over the Internet.

Transport link

A transport link is a secure TCP/IP connection between the AE Services server and a CLAN on Communication Manager. When the AE Services Transport Service starts up, it establishes the transport link between the AE server and the Communication Manager server, based on administering a switch connection in the AE Services Management Console.

The CLAN IP addresses that you administer from the Edit CLAN IPs page in the AE Services Management Console are used to set up TLS connections between AE Services and Communication Manager. These are TLS connections called transport links.

Trusted Certificate

A Trusted Certificate, typically, belongs to the root or subordinate root Certificate Authority (CA), a third party that an organization trusts. It validates the identity of the trusted third party. For example, if SampleCA certificate is in the trusted certificate repository, then a user presenting SampleCert - that is issued by SampleCA - can be trusted to be a valid user.

TSAPI Service

The CSTA-based third-party call control services provided by AE Services.

User

A person or an application administered in the local LDAP database. For example, a TSAPI application would be administered as an AE Services user with the CT User field set to Yes.

User Management

AE Services Management Console service that provides you with capabilities for managing AE Services user profiles. User Management relies on the local LDAP database to authenticate users.
<table>
<thead>
<tr>
<th><strong>Glossary</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User profile</strong></td>
</tr>
<tr>
<td><strong>Vector Directory Number (VDN)</strong></td>
</tr>
<tr>
<td><strong>Workstation</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Worktop</strong></td>
</tr>
</tbody>
</table>
Index

A
Access ................................................................. 189
accessing port matrix ............................................. 368
add data-module command ..................................... 24
adding
   CVLAN links .................................................... 80
   encryption passphrase ...................................... 200
media gateway ................................................... 37
remote key server ............................................... 202
TSAPI Links ....................................................... 84
Adding a CLANs .................................................. 24
Adding AE Services users ................................. 24
Users, AE Services, adding ............................... 139
Add Server Certificate ........................................ 109
administering
   AE services .................................................. 51
Auto Hold ......................................................... 87
CVLAN links .................................................... 80
TSAPI Links ....................................................... 84
Administering a CTI link for an ASAI application ... 29
Administering a CTI link for CVLAN ................... 28
Administering a CTI link for internal Avaya CVLAN applications ........................................... 28
Administering a network region ........................... 44
Administering a switch connection ....................... 73
Administering default dial plan ............................ 293
Administering dial plan settings ............................ 291
Administering local IP ......................................... 70
Administering Local IP ........................................ 71
Administering Switch Connections ....................... 73
Administering the console session timeout period .... 196
Administering the HTTP session timeout period .... 196
Administering the PAM Password Manager ............ 173
Administering the TCP retransmission count .......... 88
administering UCIDs in Communication Manager .... 27
aeConnectivity .................................................. 162
AE Server, restarting .......................................... 124
AE Services configuration .................................... 125
AE Services logs ............................................... 128
AE Services Management Console ...................... 55, 138
home page ....................................................... 55
AE Services ServerCSRCertificate Signing Requestkey ........................................... 363
AE Services server data, restoring ......................... 121
AE Services trust certificate storeimportpublic CA certificate ........................................... 365
AE Services users, adding ................................... 139
AE Services users, editing ................................... 139
AES server
   hostname ....................................................... 248
AES server certificateImporting ............................ 357
AES Web services) ............................................ 298
APIs that use the Security Database ....................... 209
Application, and device monitoring ...................... 214
ASAI application, administering a CTI link .......... 29
Asterisk, when treated as a wildcard ...................... 283
attributeacl.properties ....................................... 143
attributesmap.properties .................................... 143
authentication ................................................. 136
Authentication with Microsoft Active Directory Services and Kerberos ............................. 192
Auto Hold
   administering ................................................ 87
   configuring ................................................... 87
auto-negotiated settings ....................................... 249
Avaya Computer Telephony SDB
   migrating ..................................................... 344
Avaya Services technicians, accounts .................... 238
Avaya support website ....................................... 370
Avaya WebLM .................................................. 233

B
backing up, AE Services server data ...................... 120
Backing up certificates ...................................... 116

C
Call/call monitors .............................................. 214
Call/device monitor .......................................... 214
Call Control service setup .................................... 337
Call monitoring application, sample configuration .... 227
Call routing, in sample configuration ..................... 229
CA Trusted Certificate ........................................ 114
field descriptions ............................................. 114
certificate
   revocation configuration ................................... 94
Certificate administration
   importing the trusted certificate into AE Services .... 106
   verifying installation of entire certificate chain in AE Services ............................. 106
Certificate management
   importing the server certificate to AE Services ....... 113
Certificate management, Microsoft-based procedure for creating a server certificate for AE Services ........................................... 112
Certificate management, overview ........................ 97
Certificate renewal ............................................ 116
certificate revocation ......................................... 95
certificate revocation configuration ...................... 94
certificate revocation configuration field description ........................................... 94
change ip-codec-set command ............................ 35
change ip-interface command .............................. 38
change ip-network-region command ..................... 36
change node-names ip command .......................... 24, 38
changing

July 2020

Administering Avaya Aura® Application Enablement Services

Comments on this document? infodev@avaya.com

381
## Index

### Administering Avaya Aura® Application Enablement Services

### F
- fault tolerance ................................................................. 206
- enabling ........................................................................ 206
- fault tolerance configuration
  - checklist .................................................................. 206
- field descriptions
  - log retention
    - trace retention .................................................. 133
- finding content on documentation portal ...................... 368
- finding port matrix ...................................................... 368
- FIPS ........................................................................... 89
- From TelURI settings .................................................. 283, 286

### G
- Gatekeeper list (for DMCC APIs that use device and media control) ............................................. 75
- Gateway list (as opposed to H.323 Gatekeeper list), creating a switch connection name for a named list of CLAN IP addresses (for APIs that use the transport layer - DMCC, TSAPI, JTAI, CVLAN, and DLG) ......................... 73
- genericlcp1.properties .................................................. 143
- Geo Redundant High Availability
  - adding ping targets .................................................. 276
  - configuration worksheet ....................................... 272
  - configuring ............................................................... 275
  - interchanging .......................................................... 278
  - removing .................................................................... 279
  - starting ....................................................................... 277
  - stopping ..................................................................... 277
  - suspending .................................................................. 278
  - switching to the standby server ................................. 278
  - synchronizing ........................................................... 277
  - unsuspending ............................................................ 279
- Geo Redundant High Availability
  - GRHA ....................................................................... 270
  - overview ..................................................................... 270

### H
- header and trailer of PEM (BAse 64) certificate file .................. 104
- header and trailer of PKCS#7 trusted certificate file .............. 104
- Historical Metric Data Collector ........................................... 302
- HMDC
  - cleaning up data ......................................................... 308
  - disabling data collection ........................................... 306
  - enabling data collection ............................................. 306
  - scheduling data collection ......................................... 302, 305
  - unscheduling data collection ...................................... 304
  - viewing configured schedules .................................... 305
- HMDC utility
  - collectable data .......................................................... 303
  - creating a metric data report ...................................... 307
  - hostAA ........................................................................ 150
- HTTPS .......................................................................... 234, 357

### E
- EASG ............................................................................. 178
- disabling ....................................................................... 178
- enabling ........................................................................ 178
- OAM ............................................................................. 179
- EASG certificate information ......................................... 180
- EASG product certificate expiration ............................... 180
- EASG site certificate ..................................................... 180
- editing
  - Processor Ethernet name or IP address ....................... 77
- Editing
  - default user values file .............................................. 146
- Embedded Avaya WebLM Server ..................................... 233
- enabling ....................................................................... 95
- fault tolerance .............................................................. 207
- local key store ................................................................ 204
- multifactor authentication ............................................ 93
- enabling AE Services secure mode .................................. 92
- Enabling DMCC server ports for DMCC applications prior to AE Services 3.1 .......................................................... 69
- Enabling Processor Ethernet .......................................... 27
- encryptionLocalKeY ...................................................... 204
- encryptionPassphrase .................................................. 200
- encryptionRemoteKey .................................................. 202
- Enhanced Access Security Gateway ............................... 178
- enterpriseDirectory ....................................................... 156
- Enterprise Directory ...................................................... 189
- Eth0 ............................................................................. 274
- exclusive control .......................................................... 31
- Exporting the dial plan .................................................. 296
- Extended worktop access
  - and LAN address information .................................... 214
  - if disabled .................................................................... 214
Index

I

importing
  server certificate to AE Services .................................................... 113
Importing a dial plan ................................................................. 237
importSDB .................................................................................. 149
InSite Knowledge Base ............................................................... 370
installation logs ........................................................................... 250
interface speed for AES .............................................................. 249
IP services, configuring ............................................................... 25

L

LAN address information, and Extended Worktop Access ........ 214
ldapfilter.properties .................................................................. 144
licenses
  reserving DMCC licenses ......................................................... 236
  reserving TSAPI user licenses .................................................. 232
Licensing .................................................................................... 233
Licensing configurations ............................................................. 230
Links, CVLAN ........................................................................... 82
Linux, restarting ........................................................................ 124
Linux account, removing ........................................................... 171
Linux administrative account, changing properties ................. 170
Linux commands
  dateconfig ............................................................................. 246
df ............................................................................................. 249
ethtool ....................................................................................... 249
mvap.sh .................................................................................... 247
netconfig .................................................................................. 248
route ......................................................................................... 250
scp ........................................................................................... 250
service <name> start/stop/restart .............................................. 250
sftp ......................................................................................... 250
shutdown .................................................................................. 250
ssh .......................................................................................... 250
svversion ................................................................................ 248
tripwire ..................................................................................... 250
listing
  slots assignment and encryption passphrase ......................... 201
  slots assignment and remote key server ............................... 203
  slots assignment and remote server ..................................... 201
List Local Host Logins page field descriptions ......................... 182
Local IP, administering .............................................................. 70, 71
locking a Linux account ............................................................... 172
log4j
  properties ............................................................................... 144
log files, downloading ............................................................... 123
log files, viewing ......................................................................... 123
logging
  remote logging ...................................................................... 129
log in
to AE Services Management Console .................................... 55, 138
login audit, enabling ................................................................. 184
login report for all Linux accounts, displaying ......................... 182
login report for a specific login ID, displaying ......................... 182
login reports ............................................................................. 182
logs
  client access
    command .............................................................................. 122
    syslog ................................................................................. 122
M

Main dependency mode ................................................................. 31
Management Console security alerts certificates ...................... 53
media content and media tone announcement for DMCC ............ 33
media encryption ...................................................................... 37
media processor, adding ............................................................. 38
Media Properties
  configuring ............................................................................. 85
  setting ................................................................................... 85
Media service setup .................................................................. 337
MFA ............................................................................................ 93
migrating
  Avaya Computer Telephony SDB to AE Services ..................... 344
  Modify default user ................................................................. 141
  multifactor authentication ..................................................... 93
    disabling ............................................................................ 94
    enabling ............................................................................ 93
mvap.sh command .................................................................. 247
My Docs .................................................................................... 368

N

netconfig utility ......................................................................... 244
network
  interface speed and duplex settings ....................................... 249
  networkingPorts .................................................................... 157
  network interface settings, configuring ................................ 68
  network region
    adding softphones ................................................................ 37
    Network regions, administering .......................................... 23
    Network regions for DMCC .................................................. 34
NIC
  manually adjust settings ........................................................... 249
  NIC, recommended settings ..................................................... 314
NICConfiguration ...................................................................... 313
NIC configuration, editing .......................................................... 315
NIC Configuration page .............................................................. 249
NIC configurations
  NICThree NIC ....................................................................... 314
  NTP server, changing ............................................................. 243
  Two NIC ................................................................................ 249

O

OAM
  changing network settings ......................................................... 249
  online certificate status protocol ............................................. 95
OpenSSLCertificate Authority .................................................... 359
OpenSSL certificate directory structure .................................. 359
OpenSSLConfiguringConfigureconfiguration file ......................... 360
Retaining (continued)
trace files ................................................................. 132
retaining, clearing, logs, traces ..................................... 134
retaining, traces .......................................................... 135
retention
log files ......................................................................... 131
trace files ...................................................................... 131
root keysigned certificate ................................................ 362
Routing, when a routing application is started .................. 214
Routing application, when started .................................... 214
RPMs ........................................................................... 250
rsyslog .......................................................................... 128, 129

S
sample application
administering on server .................................................. 338
files on server ............................................................... 337
properties file ................................................................... 337, 339
running ........................................................................... 337, 340
Sample configuration
assigning permissions ...................................................... 225
call monitoring ............................................................... 227
manager/assistant .......................................................... 226
sd distributor.properties .................................................. 143
searching for content ...................................................... 368
Search user, feature ........................................................ 140
Secure Access Link (SAL) sending traps to ..................... 254
secure mode ..................................................................... 89
command line utilities ..................................................... 91
Secure Services Gateway (SSG) sending traps to .......... 254
Security administration .................................................... 164
Server authentication ...................................................... 98, 100
server certificate ............................................................ 356
importing ........................................................................ 113
serverCertificates .......................................................... 152
data backup .................................................................... 120
data restore ..................................................................... 121
Service <name> start/stop/restart command .................. 250
service dependencies ...................................................... 126
setSDB ............................................................................ 149

ing setting
Media Properties ............................................................. 85
Station Properties ............................................................ 86
TWS Properties ............................................................... 300
set up CVLAN links ........................................................ 80
setWeblm ......................................................................... 147
Shared control mode ....................................................... 32
Shared workstation device group administration ............ 227
Share Talk ....................................................................... 34
sharing content .............................................................. 368
signed certificates System ManagerCertificate AuthoritySystem Manager .................................................. 355
site certificate
add ............................................................................... 180
delete ............................................................................. 180
manage .......................................................................... 180

Out of Band Management
Application Enablement Services .................................... 312
Network interface configurations ..................................... 312
own certificate authority .................................................... 54
P
reserved Licenses .............................................................
Restarting the AE Service server and the Web Server .........

PAM issue (/etc/issue) message, creating ....................... 175
PAM limits, adding .......................................................... 176
PAM management ......................................................... 164, 172
PAM management capabilities ........................................... 184
PAM MOTD (/etc/motd) message, creating ....................... 176
PAM time, administering .................................................. 177
Password, User Management ............................................ 142
Password policy
Linux .............................................................................. 166, 329–331
User Management (local LDAP) ........................................... 142, 332–335
passwords
user management .................................................................. 339
ping targets
adding for Geo Redundant High Availability .................... 306
port matrix ......................................................................... 368
Procedure 3a - Verifying the installation of the trusted
certificate in AE Services ............................................. 106
Processor Ethernet, enabling ............................................. 27
Processor Ethernet name or IP address
editing ............................................................................... 77
Product ID administration ................................................... 253
R
rasaccess, changing default password .............................. 239
rbac.properties ............................................................... 144
reboot AES server ............................................................ 250
Recommended AE Service IP (local IP) settings ................... 72
Reinitializing User Management .......................................... 145
remote logging
configuring ....................................................................... 129
removing
encryption passphrase ..................................................... 201
remote key server ............................................................. 203
removing Geo Redundant High Availability ....................... 279
Renewing certificates ......................................................... 117, 118
replicator1.properties ........................................................ 143
reserved Licenses ............................................................. 146
reserving unified desktop licenses ..................................... 230
Restarting the AE Service server and the Web Server ........... 116
Restarting the AE Services server and the Web Server ........... 127
restore default
TWS Properties ................................................................. 300
Restoring certificates ........................................................ 116
restoring the server data
using CLI .......................................................................... 121
restoring the server data using CLI .................................... 121
retaining
log files ........................................................................... 132
Retaining

July 2020
Administering Avaya Aura® Application Enablement Services 385
Comments on this document? infodev@avaya.com
V
VDN (vector directory number), usage example ..........228
Verifying the installation of the server certificate in AE
Services .................................................................115
videos .................................................................369
viewing
data encryption status ........................................205
Virtual IP Address ..................................................274
VMware fault tolerance .........................................206

W
watch list ...............................................................368
WebLM ...............................................................234, 357
WebLM server
  connecting .........................................................235
worktop, adding .................................................219, 220
worktop, importing .............................................220
Worktops ............................................................219
ws_cus_bootstrap.properties ...............................145