



Avaya Aura® Application Enablement Services Administration and Maintenance Guide

Release 6.1
Issue 2
February 2011

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its 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 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 Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its Hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: <http://support.avaya.com>. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/licenseinfo/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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 End User a license within the scope of the license types described below. 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 End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya 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 a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicate with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated by Avaya provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

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

Shrinkwrap License (SR). Customer 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"). (see "Third-party Components" for more information).

Copyright

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

the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

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 Web site: <http://support.avaya.com>. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

Avaya Aura is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and "Linux" is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: <http://support.avaya.com>.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://support.avaya.com>.

Contents

Chapter 1: Introduction to AE Services administration.....	13
Overview of AE Services administration.....	13
High level checklist for administering AE Services.....	13
Related documents.....	14
For information about AE Services security.....	15
Avaya support contact information.....	15
Chapter 2: Administering Communication Manager for AE Services.....	17
Communication Manager administrative checklists.....	17
Checklist - Communication Manager administration for a DMCC configuration that uses device and media control only.....	17
Checklist - Communication Manager administration for a DMCC with round-robin assignment of H.323 Gatekeepers.....	18
Checklist - Communication Manager administration for DMCC with Call Information Services.....	19
Checklist - Communication Manager administration for DMCC with call control.....	20
Checklist - Communication Manager administration for TSAPI and JTAPI.....	21
Checklist - Communication Manager administration for Telephony Web Services.....	22
Checklist - Communication Manager administration for CVLAN.....	22
Checklist - Communication Manager administration for DLG.....	23
Checklist - Communication Manager administration for AE Services Implementation with Microsoft LCS/OCS.....	24
Checklist - Communication Manager administration for AE Services Integration with IBM Sametime.....	24
Communication Manager administration for DMCC - network regions.....	25
Adding CLANs to the network.....	25
Enabling AE Services.....	27
Enabling Processor Ethernet.....	28
Administering UCIDs in Communication Manager (TSAPI and JTAPI applications).....	29
Administering a CTI Link for CVLAN.....	30
Administering a CTI Link for CVLAN (internal applications).....	30
Administering a CTI Link for DLG.....	31
Administering a CTI Link for TSAPI, JTAPI, DMCC with Call Control, Telephony Web Service, or an AE Services integration (Microsoft or IBM Sametime).....	31
Checking the status of a switch connection -- from Communication Manager to the AE Server.....	32
DMCC settings.....	32
DMCC station registration modes.....	32
Main dependency mode.....	33
Administering an extension exclusively for the DMCC softphone.....	33
Dependent and Independent dependency modes.....	34
Administering an extension number for the station that an application monitors.....	35
About Share Talk.....	35
Network regions for DMCC.....	36
Creating the DMCC codec set.....	37
Administering a region with a specific codec set.....	37
About signaling encryption.....	37
Administering security profiles for signaling encryption.....	38
Checking for media encryption.....	38
Methods for adding DMCC softphones to the network region.....	39
Guidelines for adding a media gateway to the network.....	39
Consulting the Communication Manager documentation.....	40

Adding a media processor circuit pack to the network.....	40
Sample Communication Manager and DMCC configuration.....	40
Sample Communication Manager administration screens.....	42
Setting up UCIDs for TSAPI and JTAPI applications.....	42
Checking for IP_API_A licenses.....	43
Adding stations.....	44
Configuring IP services - administering the transport link.....	46
Setting up a codec set.....	47
Administering a network region.....	48
Mapping IP addresses (for API softphones).....	50
Adding a media gateway.....	50
Adding a CLAN.....	51
Listing IP interfaces.....	54

Chapter 3: AE Services Administration.....55

About accessing AE Services.....	55
Before you access the AE Services Management Console - certificates and security alerts.....	57
If you are using the default server certificate.....	57
If you use your own Certificate Authority.....	57
Importing the CA certificate into your browser's certificate store.....	58
Logging in to AE Services as the system administrator.....	59
Checklists for administering the services that run on the AE Server.....	60
CVLAN - checklist.....	60
DLG - checklist.....	61
DMCC with device and media control only - checklist.....	62
DMCC with device and media control only (using a switch name for CLANs) - checklist.....	63
DMCC with Call Information Services - checklist.....	64
DMCC with Call Control Services - checklist.....	66
TSAPI (including JTAPI) - checklist.....	67
Telephony Web Services - checklist.....	68
System Management Service - checklist.....	69
AE Services integration for Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007 - checklist.....	70
AE Services integration for IBM Lotus Sametime - checklist.....	71
Enabling DMCC server ports for DMCC applications developed prior to AE Services 3.1.....	73
Administering the Local IP for a single NIC configuration.....	73
Administering the Local IP for a dual NIC configuration.....	74
Recommended AE Service IP (local IP) settings.....	75
Administering network interfaces with CVLAN - using the Any network setting.....	76
Adding a switch connection.....	77
Administering switch connections for DMCC applications that use device and media control only -- assigning H.323 IP addresses.....	78
Editing CLAN IPs.....	79
Editing a Processor Ethernet name or IP address.....	80
Checking the status of a switch connection -- from the AE Server to Communication Manager.....	80
CVLAN implementation guidelines.....	81
CVLAN applications and link management.....	81
Guidelines for setting up CVLAN links.....	81
Guidelines for setting up proprietary CVLAN links.....	82
Administering CVLAN links.....	82
Ensuring the CVLAN service is running.....	84
Testing a CVLAN link.....	84

Adding CVLAN clients.....	85
Administering DLG links.....	85
Administering TSAPI links.....	86
Setting DMCC media properties.....	88
Setting DMCC station properties.....	88
AE Services general maintenance.....	89
Backing up server data.....	89
Restoring the server data.....	89
Viewing log files.....	90
Downloading log files.....	91
Configuring network interface settings.....	92
Service Controller (start, stop, and restart services).....	93
Schematic view of an AE Services configuration.....	94

Chapter 4: User Management Administration.....99

User management for authentication.....	99
DMCC AA policy administration and bypassing user authentication.....	100
User Management for authorization.....	100
Logging into User Management.....	101
The cust account in User Management.....	102
Viewing the list of all users in the User Management database.....	102
Adding a user to User Management.....	102
Editing a user in User Management.....	103
Deleting a user from User Management.....	103
Searching for users in User Management.....	104
Modifying the default user - sample.....	104
Changing user passwords.....	106
Service Administration configuration files.....	106
attributesmap.properties.....	107
attributeacl.properties.....	107
sdbdistributor.properties.....	107
genericldap1.properties, genericldap2.properties, replicator1.properties.....	107
rbac.properties.....	108
ldapfilter.properties.....	108
log4j.properties.....	108
remoteldapauthenticator.properties.....	108
user.properties.....	109
ws_cus_bootstrap.properties.....	109
Re-initializing service configuration files.....	109
Editing the default user values file - sample scenario.....	110
Guidelines for synchronizing distributors.....	111

Chapter 5: Security Administration and Additional PAM Management.....113

About Security Administration and additional PAM management.....	113
Security administration.....	114
Account Management - Linux user accounts.....	115
Adding a local Linux account for an administrator - sample.....	115
Results of adding a local Linux account for an administrator - sample.....	117
Changing the properties of a Linux administrative account -- modify login.....	119
Results of changing role assignments for aesadmin3 - sample.....	120
Removing a Linux account - Remove Login.....	120
Locking or unlocking a Linux account - Lock/Unlock Login.....	121

PAM Management.....	122
Administering the PAM module configuration.....	122
Creating a PAM Issue (/etc/issue) message.....	123
Creating a PAM MOTD (/etc/motd) message.....	124
Adding PAM limits.....	125
Administering PAM time.....	125
Administering global password aging (etc/login.defs).....	126
Login reports.....	127
Displaying a login report for all Linux accounts.....	127
List Local Host Logins page field descriptions.....	127
Displaying a login report for a specific login ID.....	128
Display Login Information page field descriptions.....	128
Enabling a login audit.....	129
Unused Login Audit page field descriptions.....	130
Additional PAM management capabilities.....	130
Linux authentication.....	131
Enterprise directory settings in the AE Services Management Console.....	132
Enterprise directory configuration settings for AE Services integrations.....	133
Enterprise directory configuration settings with bridged appearance alert blocking.....	133
Enterprise directory user authorization policy for DMCC applications.....	133
Configuring AE Services to access an enterprise directory.....	134
Configuring an external LDAP server — Windows.....	136
User roles.....	137
Authentication with Microsoft Active Directory Services and Kerberos.....	138
Sample procedures for integrating AE Services with ADS using Kerberos.....	139
Creating an account for the AE Server on the Domain Controller.....	139
Generating a keytab file for the AE Server account on the Domain Controller.....	140
Installing the Kerberos5 RPMs on the AE Server.....	140
Editing the Kerberos 5 configuration file on the AE Server.....	141
Importing the keytab file on the AE Server.....	142
Changing from User Management Authentication to Active Directory Authentication on the AE Server.....	142
Chapter 6: The Security Database.....	145
APIs that use the Security Database.....	145
Enabling the Security Database - TSAPI, JTAPI, and Telephony Web Service.....	146
DMCC applications and SDB authorization.....	146
DMCC device services.....	147
DMCC session services.....	147
DMCC applications developed prior to AE Services 4.1.....	147
Enabling the SDB for DMCC applications.....	147
TSAPI properties.....	148
Editing TSAPI properties.....	149
About granting additional permissions.....	150
Extended worktop access.....	151
Access Rights options.....	152
Security Database objects.....	153
Tlinks.....	153
Tlink groups.....	154
Adding a Tlink group.....	155
Devices.....	155
Adding a device to the SDB.....	156

Device groups.....	156
Adding a device group.....	157
Worktops.....	157
Adding a worktop.....	158
Importing multiple worktops from a .CSV file.....	159
CTI Users.....	159
Administering CTI user settings.....	160
Sample SDB Administration scenario - setting up a permission scheme based on access rights.....	161
Initial settings for the sample help desk group.....	161
Access privileges for members of the help desk.....	161
Sample - creating a worktop for each user.....	162
Sample - creating a device group called help desk.....	162
Sample - administering Edward's user profile with greater privileges.....	163
Sample - verifying the settings of the help desk.....	164
Sample Configurations.....	164
Access privileges.....	164

Chapter 7: AE Services Administration from the Operating System Command Prompt171

Accounts for Avaya Services technicians.....	171
Changing the default passwords for sroot, craft, and rasaccess.....	172
Adding a Linux user.....	172
Using Tripwire.....	173
Reconfiguring the Tripwire database for administrative access.....	173
Routine administrative tasks for Tripwire.....	174
The dateconfig utility.....	175
Changing the date or time.....	176
Changing an NTP Server.....	177
The netconfig utility.....	177
Changing the server IP address – Bundled server.....	178
Changing the server IP address – Software-Only server.....	180
AE Services Tools and Linux commands.....	181
AE Services Linux based capabilities.....	181
Linux commands.....	183
Installation and upgrade logs and RPMs.....	186
Directory structure and file locations.....	186
AE Services disk partitioning scheme.....	187
Partitioning after an upgrade.....	187
Guidelines for creating directories.....	188
About the HMDC utility.....	188
Checking the status of the HMDC utility.....	189
Starting/stopping the HMDC utility.....	189
Scheduling data collection.....	189
Unscheduled data collection.....	192
Viewing configured schedules.....	192
Creating a metric data report.....	193
Cleaning up data immediately.....	194

Chapter 8: Administering SNMP.....195

Before you begin - SNMP basics.....	195
SNMP components for AE Services.....	196
Product ID administration.....	196
Configuring the SNMP Agent.....	196

About sending traps to an Avaya SSG	197
Administering SNMP trap receivers	198
Testing SNMP Traps	200
Working with alarm reports	202
AE Services alarm codes and messages	203
Chapter 9: Certificate management.....	209
Overview of certificate management.....	209
Server authentication.....	209
Client authentication.....	210
The AE Services default certificate.....	211
If you use certificates issued by a certificate authority.....	212
Certificate enrollment and installation.....	212
Overview of manual enrollment.....	213
Checklist for manual enrollment - server authentication.....	213
Overview of automatic enrollment.....	213
Checklist for automatic enrollment using SCEP.....	214
Checklist for installing your own certificates - server authentication.....	214
Checklist for installing your own certificates - client authentication.....	215
Enabling client authentication for DMCC Java clients.....	216
Enterprise server authentication.....	216
File conversion for DER and PKCS#12 files.....	216
Obtaining a trusted certificate for the AE Server.....	217
Importing the trusted certificate into AE Services.....	218
Creating a server certificate signing request for the AE Services server.....	220
Creating a server certificate for AE Services (generic procedure).....	222
Creating an AE Services server certificate (Microsoft-based procedure).....	222
Importing the server certificate into AE Services.....	223
About restarting the AE Server and the Web Server.....	225
Backing up certificates.....	225
Restoring certificates.....	225
Certificate renewal.....	225
Renewing certificates – creating the CSR.....	226
Renewing certificates – submitting the CSR to certificate authority (Microsoft example).....	226
Renewing certificates – replacing the old certificate with the new certificate.....	227
Chapter 10: Dial plan administration in AE Services.....	229
Configurations that require dial plan administration.....	229
Dial plan administration - converting E.164 numbers and dial strings.....	230
Dial plan processing requirements - TelURI formats that AE Services supports.....	230
Calling device and monitored device ID formats.....	231
Called device ID formats.....	231
General tips for setting up From TelURI conversion rules.....	231
General tips for setting up To TelURI conversion rules.....	231
Sample of setting up From TelURI conversion rules for a dial plan with fixed-length extensions.....	232
Example - From TelURI rules for fixed-length extensions.....	232
Example - how the From TelURI rules process numbers for fixed-length extensions.....	233
Sample of setting up To TelURI conversion rules for a dial plan with fixed-length extensions.....	234
Example - To TelURI rules for fixed-length extensions.....	234
Example - how the To TelURI rules process numbers for fixed-length extensions.....	234
Sample of setting up From TelURI conversion rules for a switch with variable length extensions.....	235
Example - From TelURI rules for variable length extensions.....	235

Example - how the From TelURI rules process numbers for variable length extensions.....	236
Sample of setting up To TelURI conversion rules for a switch with variable length extensions.....	237
Example - To TelURI rules for variable length extensions.....	237
Example - how the To TelURI rules process numbers for variable length extensions.....	238
Pattern matching -- using Pattern and RegEx (regular expressions).....	239
Pattern.....	239
RegEx.....	239
Tips for dial plan settings with networked switches.....	240
Methods for administering dial plan settings.....	241
Administering dial plan settings on a per-switch basis.....	241
Administering default dial plan settings.....	243
How different APIs or offers use the TelURI settings.....	245
From TelURI and ToTelURI operations for the DMCC service.....	245
From TelURI and ToTelURI operations for the AE Services implementation for LCS/OCS.....	247
Creating a backup of the dial plan.....	247
Importing a dial plan.....	248
Chapter 11: AE Services Administration for Web services-based applications.....	249
SMS Configuration.....	249
Changing SMS proxy port settings.....	250
Configuring SMS settings.....	250
Configuring TWS settings.....	252
Appendix A: Locations of AE Services log files.....	253
Device, Media, and Call Control Service.....	253
DLG Service.....	253
CVLAN Service.....	254
TSAPI Service.....	254
Telephony Web Service.....	254
System Management System Web Service.....	255
User Web Service.....	255
Appendix B: Upgrading System Platform.....	257
Upgrading System Platform.....	257
Upgrading System Platform.....	257
Commit and Rollback.....	258
Committing an upgrade.....	260
Rolling back an upgrade.....	260
Platform Upgrade field descriptions.....	260
Appendix C: AE Services network interfaces.....	263
Network interface configurations.....	263
Single NIC configurations.....	263
Dual NIC configurations.....	264
Network interface (NIC) settings.....	264
Editing the NIC configuration (optional).....	265
Appendix D: TCP ports and firewall settings on the AE Server.....	267
TCP ports and firewall settings.....	267
Appendix E: AE Services Management Console connectivity tests.....	271
Appendix F: AE Services administrative user accounts.....	273

AE Services administrative roles and access privileges (role based access control - RBAC).....	273
Default accounts and AE Services Management Console access privileges.....	275
Authenticating and authorizing administrators for AE Services Management Console and ssh access.....	277
Default AE Services accounts.....	277
Accounts installed with the Avaya Services package.....	278
The avaya account (User Management administrator).....	278
The cust accounts (Linux and User Management).....	279
The craft account.....	279
Changing the default password for the cust account in local Linux.....	280
Creating a new System Administrator account.....	281
Adding a Linux System Administrator account (if the Avaya Service Package is not installed).....	282
Changing the default password for the avaya account (User Management administrator).....	283
Changing the default password for the cust account in User Management.....	284
Creating a new User Management administrator account and removing the default avaya account from User Management.....	285
Creating a new System Administrator account and removing the default cust account from User Management.....	286

Appendix G: Sample Device, Media, and Call Control applications.....287

About the sample DMCC applications.....	287
Sample application files on the AES server.....	287
Preparing to run the sample application.....	288
Administering AE Services for the sample application.....	288
Administering Communication Manager for the sample application.....	289
Administering a station.....	289
Administering network region and gateway.....	289
Editing the tutorial properties file.....	289
Running the sample application.....	291
Troubleshooting the sample application.....	292

Appendix H: Avaya Computer Telephony and CVLAN migration.....295

TSAPI Client settings.....	295
Migrating Avaya Computer Telephony users to AE Services.....	295
Migrating the Avaya Computer Telephony SDB to AE Services.....	296
Importing the Avaya Computer Telephony SDB to the AE Services SDB.....	297
Use User Management to add a CTI user.....	297
Alternative migration strategies for Avaya Computer Telephony.....	297
Avaya Computer Telephony bronze level integration.....	298
Bronze level integration with Active Directory Services.....	299
Avaya Computer Telephony silver level integration.....	300
Silver level integration with Active Directory Services.....	301
Avaya Computer Telephony gold level integration.....	302
Gold level integration with Active Directory Services.....	303
Migrating CVLAN to AE Services.....	304
Migrating CVLAN Server for Linux (Releases 9.0 and 9.1) to AE Services.....	304
Migrating the MAPD-based CVLAN to AE Services.....	306

Glossary.....309



Index.....319

Chapter 1: Introduction to AE Services administration

Overview of AE Services administration

To administer Avaya Aura® Application Enablement Services (AE Services) you will need to perform administrative tasks on Communication Manager as well as the AE Services server (AE Server). The following checklist presents a high level view of AE Services administration.

High level checklist for administering AE Services

#	Description	Notes	✓
1	Administer Communication Manager	See Administering Communication Manager for AE Services on page 17.  Tip: Use Avaya Site Administration in terminal emulation mode (using System Administration Terminal, or SAT, commands).	
2	Administer the AE Services running on the AE Server	See AE Services Administration on page 55.  Tip: Review the checklists before you start administering specific services. See Changing the default password for the cust account in User Management on page 284.	
3	Administer Linux users in AE Services Management Console	See About Security Administration and additional PAM management on page 113.	
4	Administer user management	Optional. See User Management Administration on page 99.	

#	Description	Notes	✓
5	Administer SNMP	Optional. See Administering SNMP on page 195.	
6	Administer certificates	Optional. See Certificate management on page 209.	
7	Administer dial plan	Optional. See Dial plan administration in AE Services on page 229.	

Related documents

The following documents contain additional information about Communication Manager and AE Services.

- *Administering Avaya Aura®Communication Manager*, 03-300509
- *Administering Network Connectivity on Avaya Aura®Communication Manager*, 555-233-504
- *Implementing Avaya Aura®Application Enablement Services on Avaya Aura® System Platform*, 02-603468
- *Implementing Avaya Aura®Application Enablement Services in a Software-Only Environment*, 02-300355
- *Implementing Avaya Aura®Application Enablement Services for a Bundled Server*, 02-300356
- *Avaya Aura®Application Enablement Services Overview* , 02-300360
- *Avaya Aura®Application Enablement Services Implementation Guide for Microsoft Live Communications Server 2005 or Microsoft Office Communications Server 2007*, 02-601893

If you are administering the AE Services integration with *Microsoft Live Communications Server* or *Microsoft Office Communications Server 2007*, use this administration guide for general administrative tasks. For more information, see [Checklist - Communication Manager administration for AE Services Implementation with Microsoft LCS/OCS](#) on page 24. For other implementation-specific tasks see *Avaya Aura®Application Enablement Services Implementation Guide for Microsoft Live Communications Server 2005 or Microsoft Office Communications Server 2007*, 02-601893.

- *Avaya Aura®Application Enablement Services Integration Guide for IBM Lotus Sametime*, 02-602818

If you are administering the AE Services integration with *IBM Lotus Sametime*, you will need to use this administration guide for general administrative tasks. For more information, see [Checklist - Communication Manager administration for AE Services Integration with IBM Sametime](#) on page 24. For other implementation-specific tasks see

Avaya Aura® Application Enablement Services Integration Guide for IBM Lotus Sametime, 02-60818.

For information about AE Services security

For information about AE Services security, see *White-paper on Security in Application Enablement Services for Bundled and Software only solutions*. This document is located on the on the Avaya Support Center Web Site (<http://www.avaya.com/support>).

Avaya support contact information

For additional support, contact your Authorized Service Provider. Depending on your coverage entitlements, additional support may incur charges. Support is provided per your warranty or service contract terms unless otherwise specified.

Avaya Support Contact	Telephone
U.S. Remote Technical Services — Enterprise	800–242–2121
U.S. Remote Technical Services — Small Medium	800–628–2888
U.S. Remote Technical Services — BusinessPartners for Enterprise Product	877–295–0099
BusinessPartners for Small Medium Product	Contact you distributor.
Canada	800–387–4268
Caribbean and Latin America	786–331–0860
Europe, Middle East, and Africa	36–1238–8334
Asia Pacific	65–6872–8686

Chapter 2: Administering Communication Manager for AE 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 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 DMCC configuration that uses device and media control only

#	Description	Notes	✓
1	Check licensing	Use display system-parameters customer-options 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).  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 25. If you use a media server that uses Processor Ethernet, see Enabling Processor Ethernet on page 28.	

#	Description	Notes	✓
3	Add stations	See DMCC station registration modes on page 32. If an application uses “non-main dependency mode”, you do not need to administer a station for the application.	
4	Set up a network region	Requires network planning. See Network regions for DMCC on page 36.	
5	Add DMCC softphones to the network region	See Methods for adding DMCC softphones to the network region on page 39.	
6	Add a media gateway to the network	See Guidelines for adding a media gateway to the network on page 39.	
7	Add a media processor	See Adding a media processor circuit pack to the network on page 40.	

Checklist - Communication Manager administration for a DMCC with round-robin assignment of H.323 Gatekeepers

#	Description	Notes	✓
1	Check licensing	Use display system-parameters customer-options 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).  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 25. If you use a media server that uses Processor Ethernet, see Enabling Processor Ethernet on page 28.	
3	Enable AE Services	Required for the transport layer. See Enabling AE Services on page 27.	
4	Add stations	See DMCC station registration modes on page 32.	


#	Description	Notes	✓
		If an application uses “non-main dependency mode”, you do not need to administer a station for the application.	
5	Set up a network region	Requires network planning. See Network regions for DMCC on page 36.	
6	Add DMCC softphones to the network region	See Methods for adding DMCC softphones to the network region on page 39.	
7	Add a media gateway to the network	See Guidelines for adding a media gateway to the network on page 39.	
8	Add a media processor	See Adding a media processor circuit pack to the network on page 40.	

Checklist - Communication Manager administration for DMCC with Call Information Services

#	Description	Notes	✓
1	Check licensing	Not applicable. Licensed on AE Server.	
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 25. If you use a media server that uses Processor Ethernet, see Enabling Processor Ethernet on page 28.	
3	Enable AE Services	Required for the transport layer. See Enabling AE Services on page 27.	
4	Add stations	See DMCC station registration modes on page 32. If an application uses “non-main dependency mode”, you do not need to administer a station for the application.	
5	Set up a network region	Requires network planning. See Network regions for DMCC on page 36.	
6	Add DMCC softphones to the network region	See Methods for adding DMCC softphones to the network region on page 39.	
7	Add a media gateway to the network	See Guidelines for adding a media gateway to the network on page 39.	


#	Description	Notes	✓
8	Add a media processor	See Adding a media processor circuit pack to the network on page 40.	

Checklist - Communication Manager administration for DMCC with call control


#	Description	Notes	✓
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	<ul style="list-style-type: none"> • If you use a media server that uses CLANs, you must add CLANs to the network. See Adding CLANs to the network on page 25. • If you use a media server that uses Processor Ethernet, see Enabling Processor Ethernet on page 28. 	
3	Enable AE Services	Required for the transport layer. See Enabling AE Services on page 27.	
4	Add a CTI Link	DMCC applications that use Call Control require 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 31.	
5	Set up a network region	Requires network planning. See Network regions for DMCC on page 36.	
6	Add DMCC softphones to the network region	See Methods for adding DMCC softphones to the network region on page 39.	
7	Add a media gateway to the network	See Guidelines for adding a media gateway to the network on page 39.	

#	Description	Notes	✓
8	Add a media processor	See Adding a media processor circuit pack to the network on page 40.	

Checklist - Communication Manager administration for TSAPI and JTAPI


#	Description	Notes	✓
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 25. If you use a media server that uses Processor Ethernet, see Enabling Processor Ethernet on page 28.	
3	Enable AE Services	Required for the transport layer. See Enabling AE Services on page 27.	
4	Administering UCIDs	TSAPI and JTAPI applications that use predictive dialing must complete the tasks described in Setting up UCIDs for TSAPI and JTAPI applications on page 42.	
5	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 31.	

Checklist - Communication Manager administration for Telephony Web Services


#	Notes	Description	✓
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 25. If you use a media server that uses Processor Ethernet, see Enabling Processor Ethernet on page 28.	
3	Enable AE Services	Required for the transport layer. See Enabling AE Services on page 27.	
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 31.	

Checklist - Communication Manager administration for CVLAN


#	Notes	Description	✓
1	Check licensing	Use display system-parameters customer-options 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).	

#	Notes	Description	✓
		 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 25. If you use a media server that uses Processor Ethernet, see Enabling Processor Ethernet on page 28.	
3	Enable AE Services	Required for the transport layer. See Enabling AE Services on page 27.	
4	Add a CTI Link	See Administering a CTI Link for CVLAN on page 30 and Administering a CTI Link for CVLAN (internal applications) on page 30.	

Checklist - Communication Manager administration for DLG


#	Description	Notes	✓
1	Check licensing	Use display system-parameters customer-options to browse through the Optional Features and ASAI Enhanced Features screens. Confirm that you have ASAI Link Core Capabilities.  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 25. If you use a media server that uses Processor Ethernet, see Enabling Processor Ethernet on page 28.	
3	Enable AE Services	Required for the transport layer. See Enabling AE Services on page 27.	
4	Add a CTI Link	See Administering a CTI Link for DLG on page 31.	

Checklist - Communication Manager administration for AE Services Implementation with Microsoft LCS/OCS

#	Description	Notes	✓
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 25. If you use a media server that uses Processor Ethernet, see Enabling Processor Ethernet on page 28.	
3	Enable AE Services	Required for the transport layer. See Enabling AE Services on page 27.	
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 31.	

Checklist - Communication Manager administration for AE Services Integration with IBM Sametime

#	Description	Notes	✓
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.	

#	Description	Notes	✓
		 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 25. If you use a media server that uses Processor Ethernet, see Enabling Processor Ethernet on page 28.	
3	Enable AE Services	Required for the transport layer. See Enabling AE Services on page 27.	
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 31.	

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 for Avaya Aura® Communication Manager*, 555-233-504. See the “Network quality administration” chapter.
- *Administering Avaya Aura® Communication Manager*, 03-300509. See “IP Network Region” in the “Screen Reference” chapter.

Adding CLANs to the network

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.

**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](#) on page 25.

-
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](#) on page 52.
 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](#) on page 53.
 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 Address** field, type the gateway address for your network configuration.
 - e. In the **Enable Ethernet Port** 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 **Autofield**, 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](#) on page 52.

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`.

Enabling AE Services

Enabling AE Services refers to administering the transport link between Communication Manager and AE Services. You need to enable AE Services for the following applications.

- Device, Media, and Call Control (DMCC) applications that use Call Information Services
- DMCC applications that use Call Control Services
- Telephony Web Service
- JTAPI
- TSAPI
- CVLAN
- DLG (ASAI applications)

-
1. Type `change ip-services`.

Communication Manager displays the IP SERVICES form. For an example, see [Figure 8: Configuring IP services](#) on page 47.

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 S8300, S8400, S85xx, S87xx, and S88xx systems that use a processor ethernet interface, type `procr`.

 **Note:**

On the S8300 and S8400 Communication Manager media servers, Processor Ethernet support is enabled by default. On S85xx S87xx, and S88xx Communication Manager media servers, Processor Ethernet support is not enabled by default. To enable AE Services Processor Ethernet support, see [Enabling Processor Ethernet](#) on page 28.

- For DEFINITY Server Csi systems and Communication Manager S8400, S85xx, S87xx, and S88xx 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 (**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](#) on page 47.

- a. In the **AE Services Server** field, type the name of the AE Server, for example `aeserver1`.

 **Note:**

On the AE 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 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 Server (**Communication Manager Interface > Switch Connections > Edit Connection > Switch Password**). The passwords must exactly match on both Communication Manager and the AE Server.

- c. Set the **Enabled** field to `y`.

Enabling Processor Ethernet

Processor Ethernet support on the S85xx, S87xx, and S88xx Communication Manager media servers requires Communication Manager 3.1 or later. Follow this procedure to enable Processor Ethernet on S85xx, S87xx, and S88xx Communication Manager media servers.

**Note:**

On the S8300 and S8400 Communication Manager media servers, Processor Ethernet support is enabled by default.

-
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:**

With AE Services 6.1, the Processor Ethernet interface provides a message rate of 1000 messages per second, full duplex, for S8510, S87xx, and S88xx media servers. For the S8500 media server, the Processor Ethernet provides a message rate of 720 messages per second, full duplex. For S83xx and S84xx 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)

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](#) on page 43
- [Figure 2: Setting up UCIDs for TSAPI and JTAPI applications - send UCID to ASAI must be enabled](#) on page 43

-
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.
-

Administering a CTI Link for CVLAN

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

-
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 Server>*, for example `aeserver1`.
-

Administering a CTI Link for CVLAN (internal applications)

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.

-
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

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.

-
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 (Microsoft or IBM Sametime)

If you are administering the AE Server for TSAPI, JTAPI, DMCC with Call Control, Telephony Web Service, or an AE Services integration (Microsoft or IBM Sametime), 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.

-
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 *<station extension>*, for example 70001.
 - 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 Server

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

For information about checking the status of a switch connection from the AE Server, see [Checking the status of a switch connection -- from the AE Server to Communication Manager](#) on page 80.

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

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 5.0 and later allows up to three 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.

Media Mode	Client	Telecommuter	Server	None
Dependency Mode				
Main	(Old) Exclusive Control	(Old) Exclusive Control	(Old) Exclusive Control	New
Dependent	New	Not allowed	New	(Old) Shared Control

Media Mode	Client	Telecommuter	Server	None
Independent	New	Not allowed	New	New

**Note:**

DMCC applications that use the Call Control Services do not need to administer stations on Communication Manager.

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 32.)

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

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

Administering an extension exclusively for the DMCC softphone

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 44.

-
1. Type `add station` 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 `x`.



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 32.)

- 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 35.

Administering an extension number for the station that an application monitors

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.

-
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.

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

If any of the three clients are using client or server media mode (see [DMCC station registration modes](#) on page 32), 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 25.

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.711A
- G.711MU
- G.729
- G.729A

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.
- 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

Use the `change ip-codec-set <codec set number>` command to create a codec set that uses G.711A, G.711MU and G.729.

-
1. Ensure that G.711A, G.711MU, or G.729 are the only codecs administered.
 2. Verify that the **Silence Suppression** field is set to `n`.
 3. It is recommended that you accept the default packet size of 20 ms.

For an example of how to complete the form, see [Setting up a codec set](#) on page 47.

Administering a region with a specific codec set

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

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 38.

Administering security profiles for signaling encryption

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 50).

- **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-ek** — provides H.323 signaling link encryption
- **any-auth** — provides either pin-ek or challenge
If a DMCC endpoint is registered to an ip network region that has any-auth or pin-ek 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

The AE Server provides media encryption for DMCC applications that use Main Dependency Mode (see [DMCC station registration modes](#) on page 32 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.

-
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 48.
-

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 (S8300/S8500/S8700/S8710) with a G700/G350 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 40. Here 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 50.

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*, 555-233-504.
- *Installing and Upgrading the Avaya S8300 Server*, 555-234-100.



Note:

If you need to add a CLAN to the network, see [Adding CLANs to the network](#) on page 25.

Adding a media processor circuit pack to the network

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:

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

For an example, see [Adding a CLAN - change node-names ip](#).

For a screen reference, see “IP Node Names” in the “Screen Reference” chapter of *Administering Avaya Aura® Communication Manager*, 03-300509.

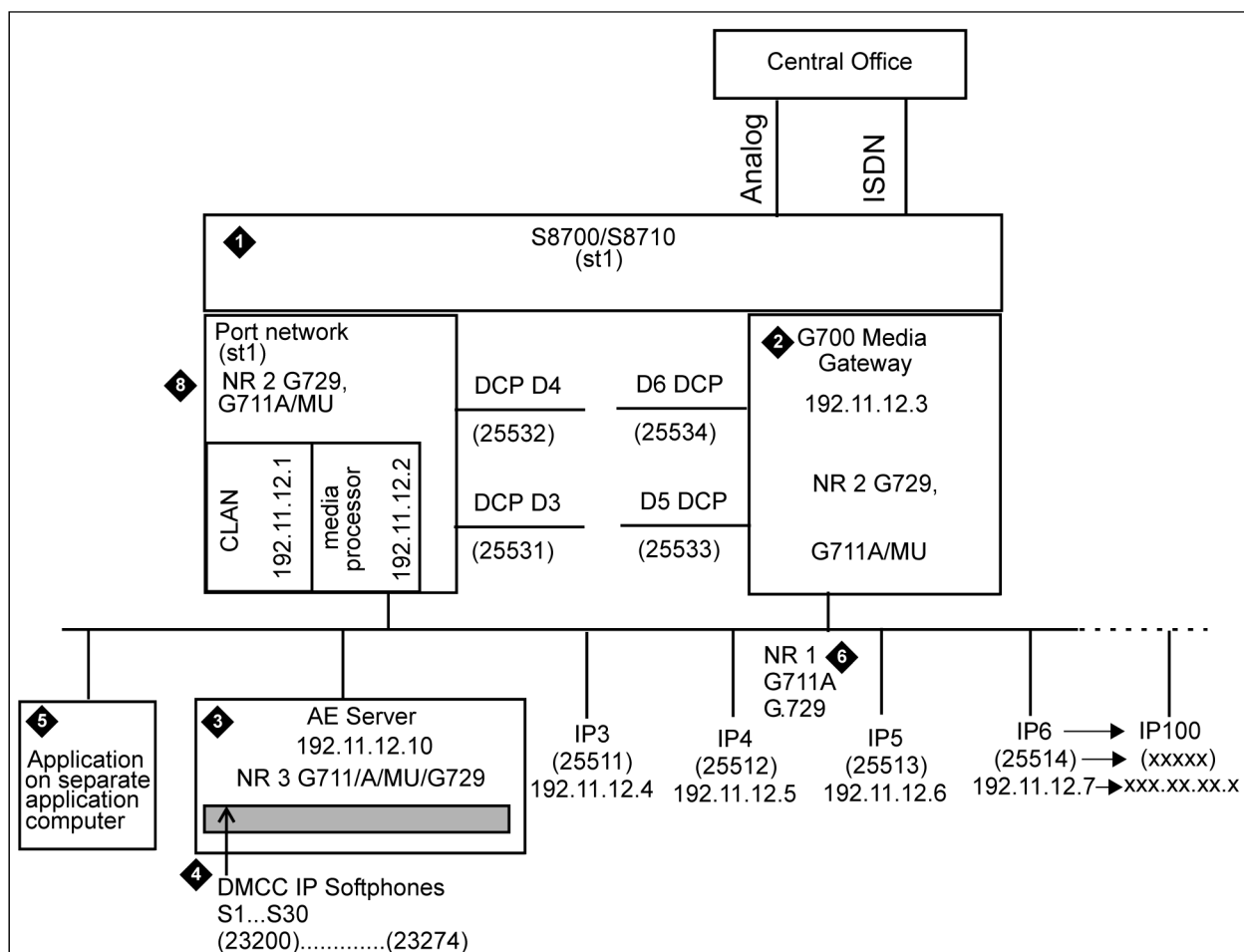
2. Type `change ip-interface <board location>` (where *<board location>* is the board location for the media processor, for example, 1A05).

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](#).

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 44 through [Figure 22: Listing IP interfaces](#) on page 54.



1. Communication Manager - S8700/8710 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.11A/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 must enable the setting for creating UCIDs. Select a unique node number for the switch (see [Figure 1: Setting up UCIDs for TSAPI and JTAPI applications - create a UCID and assign a Node ID](#) on page 43), and enable the setting for Send UCID to ASAI (see [Figure 2: Setting up UCIDs for TSAPI and JTAPI applications - send UCID to ASAI must be enabled](#) on page 43).

change system-parameters features Page 5 of 17

FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS:
 Endpoint: _____ Lines Per Page: 60

SYSTEM-WIDE PARAMETERS:
 Switch Name: _____

Emergency Extension Forwarding min): 10
 Enable Inter-Gateway Alternate Routing? n

MALICIOUS CALL TRACE PARAMETERS
 APPLY WCT Warning Tone? n MCT Voice Recorder Trunk Group: _____

SEND ALL CALLS OPTIONS
 Send All Call Applies to: station Auto Inspect on Send All Calls? n

UNIVERSAL CALL ID
Create Universal Call ID (UCID)? y UCID Network Node ID: 1

Figure 1: Setting up UCIDs for TSAPI and JTAPI applications - create a UCID and assign a Node ID

change system-parameters features Page 12 of 17

FEATURE-RELATED SYSTEM PARAMETERS

AGENT AND CALL SELECTION:
 MIA Across Splits or Skills? n
 ACW Agents Considered Idle? n
 Call Selection Measurement: current-wait-time
 Service Level Supervisor Call Selection Override? n
 Auto Reserve Agents: none

ASAI
 Copy ASAI UII During Conference/Transfer? n
 Call Classification After Answer Supervision? n
Send UCID to ASAI? y

CALL MANAGEMENT SYSTEM
 Reporting Adjunct Release:
 BCMS/VuStats LoginIDs? y
 BCMS/VuStats Measurement Interval: hour
 BCMS/VuStats Abandon Call Timer (seconds):
 Validate BCMS/VuStats Login IDs? n
 Clear VuStats Shift Data? on-login
 Remove Inactive BCMS/VuStats Agents? n

Figure 2: Setting up UCIDs for TSAPI and JTAPI applications - send UCID to ASAI must be enabled

Checking for IP_API_A licenses

You need an IP_API_A license if you are not using DMCC_DMC licenses via Application Enablement Services WebLM. 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: Checking for IP_API_A licenses](#) on page 44.

```
MAXIMUM IP REGISTRATIONS BY PRODUCT ID
```

Product ID	Rel. Limit	Used
IP_API_A	: 1000	0
IP_Agent	: 0	0
IP_Phone	: 1000	104
IP_ROMax	: 50	15
IP_Soft	: 500	0
IP_eCons	: 5	0
	: 0	0
	: 0	0
	: 0	0
	: 0	0
	: 0	0
	: 0	0
	: 0	0
	: 0	0
	: 0	0
	: 0	0

(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](#) on page 45
- [Figure 5: Adding a station, Page 2 of the STATION screen](#) on page 45
- [Figure 6: Adding a station, Page 3 of the STATION screen](#) on page 46
- [Figure 7: Adding a station, Page 4 of the STATION screen](#) on page 46

add station 23200 Page 1 of 5

STATION

Extension: 23200	Lock Messages? n	BCC: 0
Type: 4624	Security Code: *	TN: 1
Port: S00142	Coverage Path 1:	COR: 1
Name: cmapi ip-softphone 23200	Coverage Path 2:	COS: 1
	Hunt-to Station:	

STATION OPTIONS

Loss Group: 19	Personalized Ringing Pattern: 1
Speakerphone: 2-way	Message Lamp Ext: 23200
Display Language: english	Mute Button Enabled? y
	Media Complex Ext:
	IP SoftPhone? y

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

add station 23200 Page 2 of 5

STATION

FEATURE OPTIONS

LWC Reception: spe	Auto Select Any Idle Appearance? n
LWC Activation? y	Coverage Msg Retrieval? y
LWC Log External Calls? n	Auto Answer: none
CDR Privacy? n	Data Restriction? n
Redirect Notification? y	Idle Appearance Preference? n
Per Button Ring Control? n	Restrict Last Appearance? y
Bridged Call Alerting? n	
Active Station Ringing: single	
H.320 Conversion? n	Per Station CPN - Send Calling Number?
Service Link Mode: as-needed	
Multimedia Mode: enhanced	Audible Message Waiting? n
MWI Served User Type:	Display Client Redirection? n
AUDIX Name:	Select Last Used Appearance? n
	Coverage After Forwarding? s
IP Emergency Calls: extension	Direct IP-IP Audio Connections? y
Emergency Location Ext: 23200	IP Audio Hairpinning? y

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

add station 23200
Page 3 of 5

STATION

SITE DATA

Room: change sta
Headset? n

Jack:
Speaker? n

Cable:
Mounting: d

Floor:
Cord Length: 0

Building:
Set Color:

ABBREVIATED DIALING

List1:
List2:
List3:

BUTTON ASSIGNMENTS

1: call-appr
7:

2: call-appr
8:

3: call-appr
9:

4:
10:

5:
11:

6:
12:

Figure 6: Adding a station, Page 3 of the STATION screen

add station 23200
Page 4 of 5

STATION

FEATURE BUTTON ASSIGNMENTS

13:
19:

14:
20:

15:
21:

16:
22:

17:
23:

18:
24:

Figure 7: Adding a station, Page 4 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: Configuring IP services](#) on page 47) and the AE Services Administration screen ([Figure 9: Configuring IP services - AE Services Administration](#) on page 47).

change ip-services Page 1 of 3

			IP SERVICES		
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
SAT	y	st1-clan	9000	any	0
AESVCS	y	st1-clan	8765		

Figure 8: Configuring IP services

**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.

change ip-services Page 3 of 3

AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	aeserver1	aespassword1	y	
2:	_____	_____	—	
3:	_____	_____	—	

Figure 9: Configuring IP services - AE Services Administration

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 [Figure 10: Setting up a codec set - media encryption set to none](#) on page 48.

```

change ip-codec-set 3                                     Page 1 of 1

                                IP Codec Set

Codec Set: 3

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size(ms)
1: G.711MU      n           2         20
2: G.711A      n           2         20
3: G.729       n           2         20
4:
5:
6:
7:

Media Encryption: none

```

Figure 10: Setting up a codec set - media encryption set to none

```

change ip-codec-set 3                                     Page 1 of 1

                                IP Codec Set

Codec Set: 3

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size(ms)
1: G.711MU      n           2         20
2: G.711A      n           2         20
3: G.729       n           2         20
4:
5:
6:
7:

Media Encryption: aes

```

Figure 11: Setting up a codec set - media encryption set to aes

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 [Figure 12: Administering a network region, IP NETWORK REGION screen, page 1](#) on page 49 and [Figure 13: Administering a network region, IP NETWORK REGION screen, page 3](#) on page 49.

change ip-network-region 3 Page 1 of 19

IP NETWORK REGION

Region: **3**
 Location: Home Domain:
 Name:

Intra-region IP-IP Direct Audio: no
 Inter-region IP-IP Direct Audio: no
 IP Audio Hairpinning? n

AUDIO PARAMETERS
 Codec Set: **3**
 UDP Port Min: 2048
 UDP Port Max: 65535

RTCP Reporting Enabled? y
 RTCP MONITOR SERVER PARAMETERS
 Use Default Server Parameters? y

DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 34
 Audio PHB Value: 46

802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 7
 Audio 802.1p Priority: 6

H.323 IP ENPOINTS AUDIO RESOURCE RESERVATION PARAMETERS
 RSVP Enabled? n
 H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
 Keep-Alive Interval (sec): 5
 Keep-Alive Count: 5

Figure 12: Administering a network region, IP NETWORK REGION screen, page 1

change ip-network-region 3 Page 3 of 19

Inter Network Region Connection Management

src rgn	dst rgn	codec set	direct WAN	WAN-BW-limits	Intervening-regions	Dynamic CAC Gateway
3	1	2				
3	2	2	y	NoLimit		
3	3	3				
3	4					
3	5					
3	6					
3	7					
3	8					
3	9					
3	10					
3	11					
3	12					
3	13					
3	14					
3	15					

Figure 13: Administering a network region, IP NETWORK REGION screen, page 3

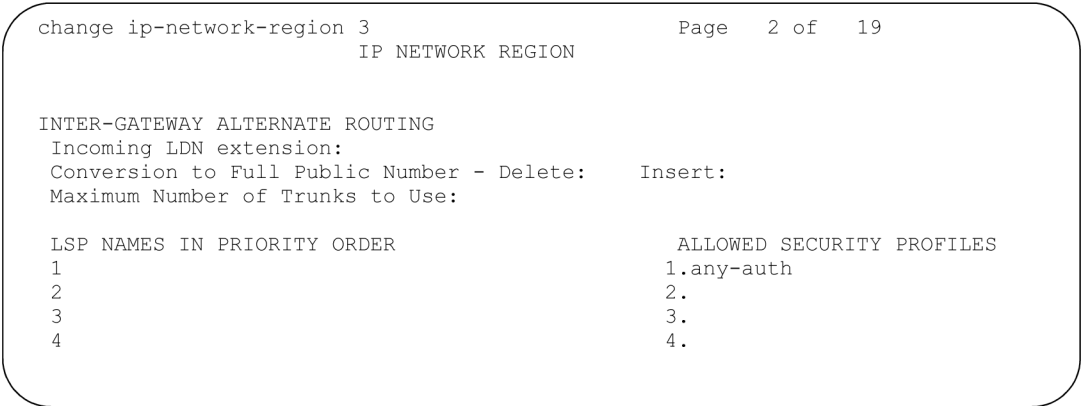


Figure 14: Administering a network region, IP NETWORK REGION screen, page 2

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 [Figure 15: Mapping IP addresses \(for API softphones\)](#) on page 50.

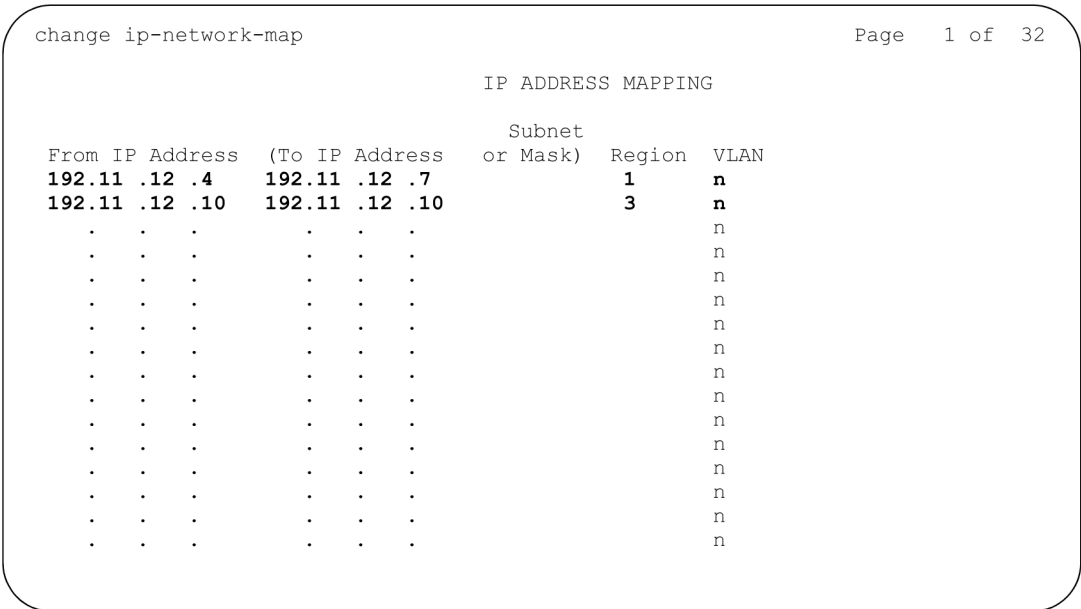


Figure 15: Mapping IP addresses (for API softphones)

Adding a media gateway

If you are using a media server (S8300/S8500/S8700/S8710) with a G700/G350 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 40.



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.

add media-gateway 1
Page 1 of 1

MEDIA GATEWAY

Number: 5 Type: g350 Name: ST1 MG1 30N73 Name: Denver Branch Serial Number: NNNNNNNNNNNNNNNN Network Region: 3 Registered? n	IP address: 192.11.12 .3 FW Version/HW Vintage: MAC address: Encrypt Link? y Location: 1 Controller IP Address: Site Data: Denver
---	---

Slot	Module Type	Name
V1:	S8300	ICC MM
V2:	MM710	DS1 MM
V3:		
V4:		
V5:		
V6:	MM312	DCP MM
V7:	virtual-analog	ANA VMM
V9:	gateway-announcements	ANA VMM

Figure 16: Adding a media gateway

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: Adding a CLAN - add data-module](#) on page 52)
- **change node-names ip** (see [Figure 18: Adding a CLAN - change node-names ip](#) on page 52)
- **change ip-interface** - to add the following:
 - a CLAN (see [Figure 19: Adding a CLAN IP interface](#) on page 53)
 - a MEDPRO circuit pack (see [Figure 20: Adding a media processor](#) on page 53)
 - a PROCR (see [Figure 21: Adding a processor CLAN \(procr\)](#) on page 54)

add data-module 44444

DATA MODULE

Page 1 of 1

Data Extension: **44444**

Name: **CLAN1**

Type: **ethernet**

Port: **17D0717**

Network uses 1's for Broadcast Addresses?

Y

Figure 17: Adding a CLAN - add data-module

change node-names ip

IP NODE NAMES

Page 1 of 1

Name	IP Address	Name	IP Address
CLAN1	192.11 .12 .1		.
CLAN2	192.11 .12 .2		.

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

add ip-interface 1A06

Page 1 of 1

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

Page 1 of 1

IP INTERFACES

Type: **MEDPRO**
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

change ip-interface procr

Page 1 of 1

IP INTERFACES

Type: **PROCR**

Node Name: **procr**

IP Address: **135.9 .71 .180**

Subnet Mask: **255.255.255.0**

Enable Ethernet Port? **y**

Network Region: **1**

Figure 21: Adding a processor CLAN (procr)

Listing IP interfaces

Use the `list ip-interface all` command to view the IP interfaces you have administered, as illustrated in [Figure 22: Listing IP interfaces](#) on page 54.

list ip-interface all

IP INTERFACES

ON	Type	Slot	Code	Sfx	Node Name	Subnet Mask	Gateway	Address	Net	Rgn	VLA
y	C-LAN	01A06	TN799	D	sraychk-clan1	255.255.255.0	135.9	.71 .254	1	n	
y	MEDPRO	01A17	TN2302		sraychk-prw1	255.255.255.0	135.9	.71 .254	1	n	
y	C-LAN	02A06	TN799	C	sraychk-clan1	255.255.255.0	135.9	.71 .254	1	n	
y	MEDPRO	01A16	TN2302		sraychk-prw2	255.255.255.0	135.9	.71 .254	1	n	

Figure 22: Listing IP interfaces

Chapter 3: AE Services Administration

About accessing AE Services

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 56 and [Figure 24: AE Services client authentication methods](#) on page 56 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 273.

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 171.



Important:

The AE Services Bundled Server does not provide a web browser, and the AE Services Software-Only solution does not assume that you will install one. To administer AE Services, you need a computer running a browser with network access to the AE Server.

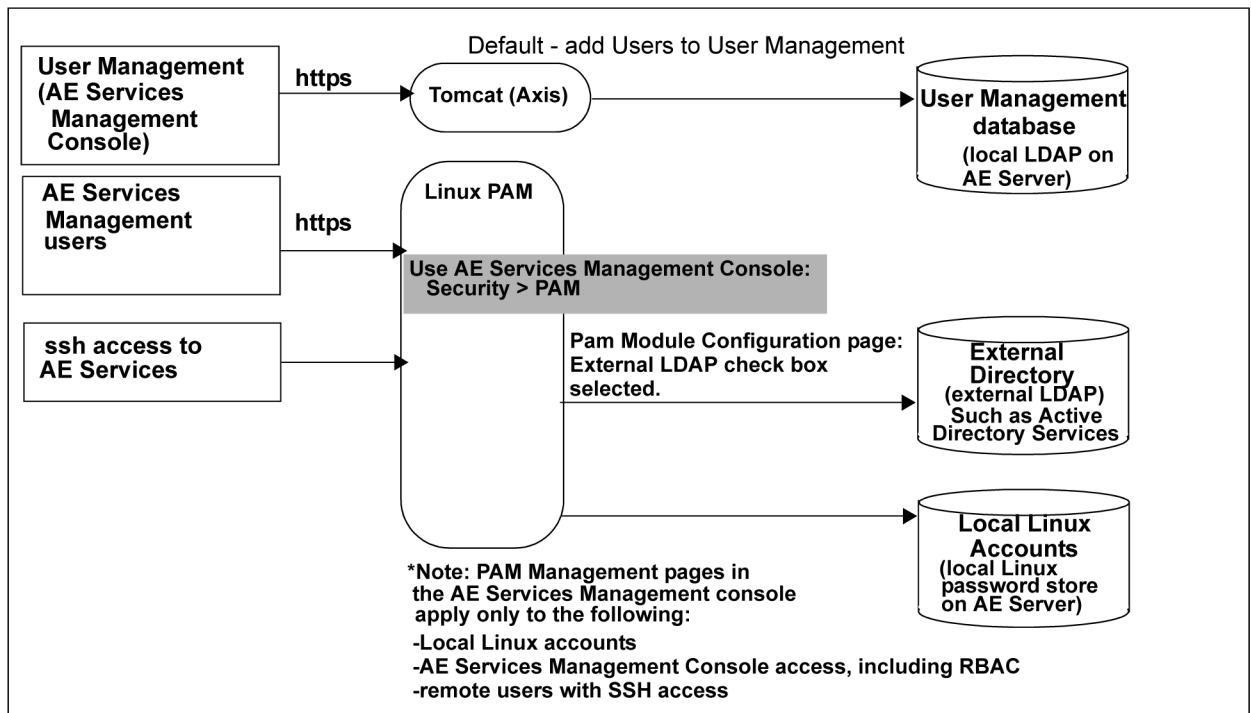


Figure 23: AE Services and ssh authentication methods

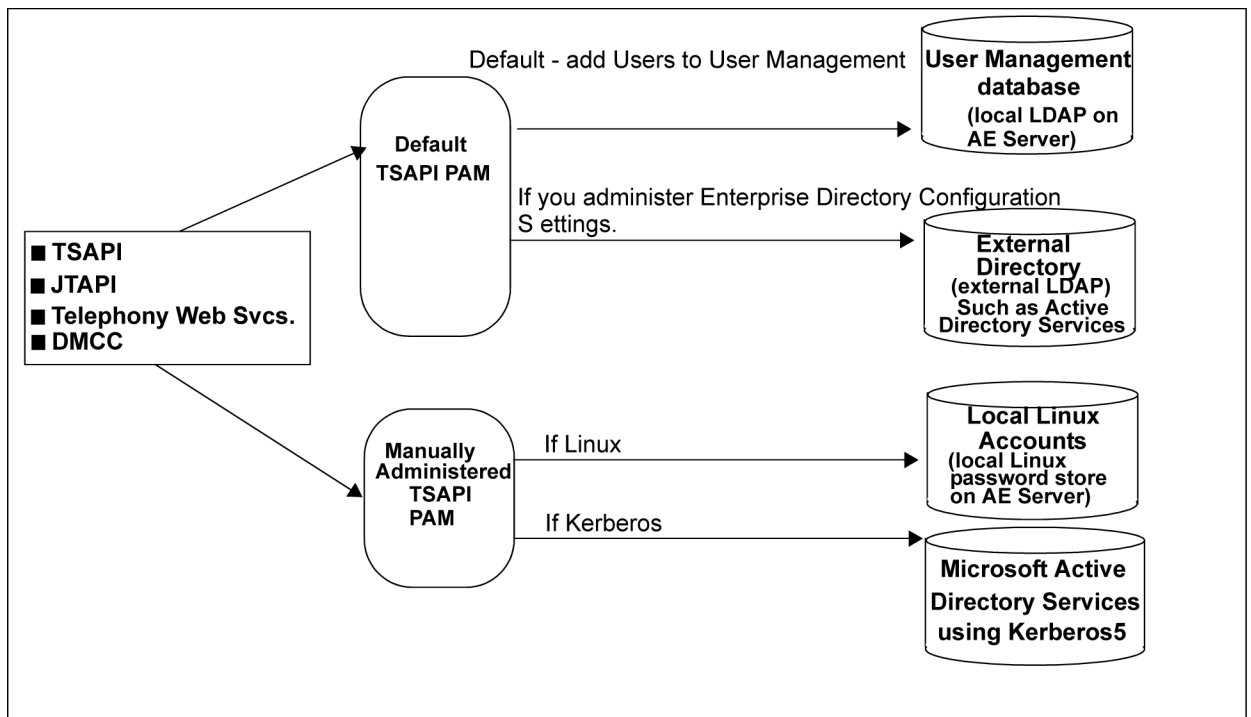


Figure 24: AE Services client authentication methods

Before you access the 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.

 **Note:**

This section provides examples that are specific to Microsoft Internet Explorer. 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 Avaya Product Root Certificate authority (the default) or if you use certificates issued by a trusted in-house or third-party certificate authority.

 **Note:**

Using certificates issued by a trusted in-house or third-party certificate authority is also referred to as using your own certificates.

If you are using the default server certificate

If you use the default server certificate (serverCert.pem), which is signed by the Avaya Product Certificate Authority (CA), 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 can not eliminate this security alert. You will see this message each time you log in to AE Services. Just click **Yes** to use AE Services.

If you use your own Certificate Authority

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.

-
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 217.

2. Import the trusted certificate into AE Services.

For specific instructions, see [Importing the trusted certificate into AE Services](#) on page 218.

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 58.

Importing the CA certificate into your browser's certificate store



Note:

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

1. From your browser, select **Tools > Internet Options**.
2. In the **Internet Options** dialog box, select the **Content** tab, and then click **Certificates**.
3. In the **Certificates** dialog box, select the **Trusted Root Certification Authorities** tab.
4. From 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.
(For example, **C:\templaetrucert.cer** based on the example in [Obtaining a trusted certificate for the AE Server](#) on page 217.)
6. Click **Next**.
7. In the **Certificate Store** dialog box, click **Browse**.
8. In the **Select Certificate Store** dialog box, select **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.

You have imported the CA certificate into your browser's certificate store. The next time you start 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

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 \(role based access control - RBAC\)](#) on page 273.

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 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 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](#) on page 123.

4. From the Application Enablement Services Management Console log in page, type the default login (**cust**) and default password (**custpw**), and click **Login**.



Tip:

To change to password settings (number of retries, length of password, and so forth), See [Administering the PAM module configuration](#) on page 122.

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 \(role based access control - RBAC\)](#) on page 273.



Security alert:

After you initially log in, change the default password for the cust account. See [Changing the default password for the cust account in local Linux](#) on page 280.

Checklists for administering the services that run on the AE Server

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

For a high-level illustration of the services that run on the AE Server, see [Schematic view of an AE Services configuration](#) on page 94.

CVLAN - checklist

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

#	Description	Notes	✓
1	Networking > AE Service IP (Local IP)	Required. Based on your AE Services configuration, see either of the following topics: <ul style="list-style-type: none"> • Administering the Local IP for a single NIC configuration on page 73 • Administering the Local IP for a dual NIC configuration on page 74 	
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 77.	
4	AE Services > CVLAN > CVLAN Links > Add CVLAN Link	Required (CVLAN Link). See Adding CVLAN clients on page 85.	
5	Security > Certificate Management	Optional. For more information, see Certificate management on page 209.	

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.

#	Description	Notes	✓
1	Networking > AE Services (Local IP)	Required. Based on your AE Services configuration, see either of the following topics: <ul style="list-style-type: none"> • Administering the Local IP for a single NIC configuration on page 73. • Administering the Local IP for a dual NIC configuration on page 74. 	
2	Communication Manager Interface > Switch Connections	Required. See Adding a switch connection on page 77.	
3	AE Services > DLG > DLG Links > Add Link	Required. See Administering DLG links on page 85.	

DMCC with device and media control only - checklist



Use this checklist If you are administering the DMCC service for applications that use device and media control only, (first party call control).

#	Description	Notes	✓
1	Networking > AE Services (Local IP)	Required. Based on your AE Services configuration, see either of the following topics: <ul style="list-style-type: none"> • Administering the Local IP for a single NIC configuration on page 73. • Administering the Local IP for a dual NIC configuration on page 74. 	
2	Networking > Ports	Optional. You can use the default settings. <p> Note: If you have a firewall, you might need to change these settings. See TCP ports and firewall settings on page 267.</p> <p> 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 73.</p>	
3	AE Services > DMCC	Optional. You can use the default media and station properties. See Setting DMCC media properties on page 88.	
4	Security > Certificate Management	Required if you are using link encryption. For more information, see Certificate management on page 209.	
5	Communication Manager Interface > Dial Plan	Optional. Dial plan administrating applies to DMCC clients using E164ConversionServices. See Dial plan administration in AE Services on page 229.	
6	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	

#	Description	Notes	✓
		settings in the AE Services Management Console on page 132.	
7	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 <i>Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer 's Guide</i> , 02-300359.	

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.

#	Description	Notes	✓
1	Networking > AE Services (Local IP)	Required. Based on your AE Services configuration, see either of the following topics: <ul style="list-style-type: none"> • Administering the Local IP for a single NIC configuration on page 73. • Administering the Local IP for a dual NIC configuration on page 74 	
2	Networking > Ports	Optional. You can use the default settings. <p> Note: If you have a firewall, you might need to change these settings. See TCP ports and firewall settings on page 267.</p> <p> 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 73.</p>	

#	Description	Notes	✓
3	AE Services > DMCC	Optional. You can use the default media and station properties. See Setting DMCC media properties on page 88.	
4	Communication Manager Interface > Switch Connections	Required. The Switch Connection Name is used for round-robin assignment of H.323 Gatekeepers. You must edit the H.323 Gatekeeper. See Administering switch connections for DMCC applications that use device and media control only -- assigning H.323 IP addresses on page 78.	
5	Security > Security Database	Optional. See The Security Database on page 145.	
6	Security > Certificate Management	Not required if you are not using encryption. For more information, see Certificate management on page 209.	
7	Security > Enterprise Directory	Optional. For more information, see Enterprise directory settings in the AE Services Management Console on page 132.	
8	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 <i>Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer's Guide</i> , 02-300359.	

DMCC with Call Information Services - checklist



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

#	Description	Notes	✓
1	Networking > AE Services (Local IP)	Required. Based on your AE Services configuration, see either of the following topics: <ul style="list-style-type: none"> • Administering the Local IP for a single NIC configuration on page 73. • Administering the Local IP for a dual NIC configuration on page 74. 	
2	Networking > Ports	Optional. You can use the default settings. <p> Note: If you have a firewall, you might need to change these settings. See TCP ports and firewall settings on page 267.</p> <p> 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 73.</p>	
3	Communication Manager Interface > Switch Connections	Required. DMCC with Call Information Services uses the Transport Service. See Adding a switch connection on page 77. 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 78.	
4	Communication Manager Interface > Dial Plan	Optional. You must administer a dial plan if your DMCC clients use E.164ConversionServices. See Dial plan administration in AE Services on page 229.	
5	AE Services > DMCC	Optional. You can use the default media and station properties. See Setting DMCC media properties on page 88.	
6	Security > Security Database	Optional. See The Security Database on page 145.	
7	Security > Certificate Management	Optional. If you are using link encryption, you must set up certificates. For more information, see Certificate management on page 209.	
8	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	

#	Description	Notes	✓
		Enterprise directory settings in the AE Services Management Console on page 132.	
9	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 <i>Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer's Guide</i> , 02-300359.	

DMCC with Call Control Services - checklist

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

#	Description	Notes	✓
1	Networking > AE Services (Local IP)	Required. Based on your AE Services configuration, see either of the following topics: <ul style="list-style-type: none"> • Administering the Local IP for a single NIC configuration on page 73. • Administering the Local IP for a dual NIC configuration on page 74. 	
2	Networking > Ports	Optional. You can use the default settings. <p> Note: If you have a firewall, you might need to change these settings. See TCP ports and firewall settings on page 267.</p> <p> 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 73.</p>	
3	Communication Manager Interface > Switch Connection	Required. The Transport Layer is used. See Adding a switch connection on page 77.	
4	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 86.	

#	Description	Notes	✓
5	AE Services > DMCC Configuration	Optional. You can use the default media properties. See Setting DMCC media properties on page 88.	
6	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 The Security Database on page 145.	
7	Security > Enterprise Directory	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 132.	
8	Security > Certificate Management	Optional. If you are using encrypted links, and you are using your own certificates you will need to use the Certificate Management pages. For more information, see Certificate management on page 209.	
9	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 <i>Avaya Aura® Application Enablement Services Device, Media, and Call Control Java Programmer's Guide</i> , 02-300359.	


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.

#	Description	Notes	✓
1	Networking > AE Services (Local IP)	Required. Based on your AE Services configuration, see either of the following topics: <ul style="list-style-type: none"> • Administering the Local IP for a single NIC configuration on page 73. • Administering the Local IP for a dual NIC configuration on page 74. 	
2	Networking > Ports	Optional. You can use the default settings. <div>  Note: If you have a firewall, you might need to change these settings. See TCP ports and firewall settings on page 267. </div>	
3	Communication Manager Interface > Switch Connection	Required. The Transport Layer is used. See Adding a switch connection on page 77.	
4	CTI Link Administration	Required (TSAPI Link). See Administering TSAPI links on page 86.	
5	TSAPI Configuration	Optional. If you are using the AE Service Security Database for controlling device access you must administer the TSAPI Configuration settings. See The Security Database on page 145.	
6	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 The Security Database on page 145.	
7	Security > Enterprise Directory	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 132.	
8	Security > Certificate Management	Optional. If you are using encrypted links, and you are using your own certificates you will need to use the Certificate Management pages. For more information, see Certificate management on page 209.	


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.

#	Description	Notes	✓
1	Networking > AE Services (Local IP)	Required. Based on your AE Services configuration, see either of the following topics: <ul style="list-style-type: none"> • Administering the Local IP for a single NIC configuration on page 73. • Administering the Local IP for a dual NIC configuration on page 74. 	
2	Networking > Ports	Optional. You can use the default settings. <div>  Note: If you have a firewall, you might need to change these settings. See TCP ports and firewall settings on page 267. </div>	
3	Communication Manager Interface > Switch Connection	Required. See Adding a switch connection on page 77.	
4	AE Services > TSAPI > TSAPI Link > Add TSAPI Links	Required. You must add a TSAPI Link. See Administering TSAPI links on page 86.	
5	Security > Enterprise Directory	Optional. For more information, see Enterprise directory settings in the AE Services Management Console on page 132.	
6	Security > Certificate Management	Optional. If you use encrypted links, and you use your own certificates you must configure Certificate Management in the AE Services Management Console. For more information, see Certificate management on page 209.	

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.

#	Description	Notes	✓
1	Networking > AE Services (Local IP)	Required. Based on your AE Services configuration, see either of the following topics: <ul style="list-style-type: none"> • Administering the Local IP for a single NIC configuration on page 73. • Administering the Local IP for a dual NIC configuration on page 74. 	
2	Network Configuration > Ports	Optional. You can use the default settings. <div>  Note: If you have a firewall, you might need to change these settings. See TCP ports and firewall settings on page 267. </div>	
3	SMS Configuration	Required. See SMS Configuration on page 249.	

AE Services integration for Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007 - checklist

When you administer AE Services for Microsoft Live Communications Server 2005 or Microsoft Office Communications Server 2007 you must add a TSAPI link.


Use this checklist to plan and monitor your administrative tasks.

#	Description	Notes	✓
1	Networking > AE Services (Local IP)	Required. Based on your AE Services configuration, see either of the following topics: <ul style="list-style-type: none"> • Administering the Local IP for a single NIC configuration on page 73. • Administering the Local IP for a dual NIC configuration on page 74 	
2	Networking > Ports	Required. You must enable the TR87 LCS Port (4723). By default this port is disabled in the AE Services Management Console.	
3	AE Services > DMCC Configuration	Not applicable.	

#	Description	Notes	✓
4	Communication Manager Interface > Switch Connection	Required. The Transport Layer is used. See Adding a switch connection on page 77.	
5	CTI Link Administration	Required (TSAPI Link). See Administering TSAPI links on page 86.	
6	Security > Certificate Management	Required. See the <i>Avaya Aura® Application Enablement Services Implementation Guide for Microsoft Live Communications Server 2005 or Microsoft Office Communications Server 2007</i> , 02-601893.	
7	Communication Manager Interface > Dial Plan	Required. See the <i>Avaya Aura® Application Enablement Services Implementation Guide for Microsoft Live Communications Server 2005 or Microsoft Office Communications Server 2007</i> , 02-601893.	
8	Security > Enterprise Directory	Required. See the <i>Avaya Aura® Application Enablement Services Implementation Guide for Microsoft Live Communications Server 2005 or Microsoft Office Communications Server 2007</i> , 02-601893.	
9	Security > Host AA	Optional. TR/87 applies to Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007. 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.	

AE Services integration for IBM Lotus Sametime - checklist

When you administer AE Services for IBM Lotus Sametime you must add a TSAPI link.

#	Description	Notes	✓
1	Networking > AE Services (Local IP)	Required. Based on your AE Services configuration, see either of the following topics: <ul style="list-style-type: none"> • Administering the Local IP for a single NIC configuration on page 73. • Administering the Local IP for a dual NIC configuration on page 74 	
2	Networking > Ports	Required. Verify that the DMCC Server Port , Encrypted Port 4722, is enabled.	
3	Communication Manager Interface > Switch Connection	Required. The Transport Layer is used. See Adding a switch connection on page 77.	
4	AE Services > TSAPI > TSAPI Links > Add TSAPI Link	Required (TSAPI Link). See Administering TSAPI links on page 86. <div>  Note: For the AE Services integration with IBM Sametime, you must administer TSAPI Links as Encrypted. If your AE Server supports other TSAPI applications in addition to the integration with Sametime, and some of those applications use unencrypted TSAPI links, you will need to administer TSAPI links with the Both setting (so it allows both encrypted and unencrypted). </div>	
5	User Management > User Admin > Add User	Required. You must add the IBM Lotus Sametime user account to AE Services User Management as a CT User (CT user set to Yes). When you set CT User to Yes the IBM Lotus Sametime user account is added to the AE Services Security Database.	
6	Security > Security Database > CTI Users > List All Users > Edit CTI User	Required. You must edit the IBM Lotus Sametime user account in the Security Database and enable unrestricted access (The Unrestricted Access check box must be checked on the Edit CTI User page.)	
7	Security > Certificate Management	Optional. See the <i>Avaya Aura® Application Enablement Services Integration Guide for IBM Lotus Sametime</i> , 02-602818.	
8	Communication Manager Interface > Dial Plan	Required. See the <i>Avaya Aura® Application Enablement Services Integration Guide for IBM Lotus Sametime</i> , 02-602818.	

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

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).

-
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**.
-

Administering the Local IP for a single NIC configuration

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 263.

 **Note:**

If you are using CVLAN in combination with other services, see [Administering network interfaces with CVLAN - using the Any network setting](#) on page 76.

 **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.

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**.



Note:

For a summary of these settings, see [Recommended AE Service IP \(local IP\) settings](#) on page 75.

Administering the Local IP for a dual NIC configuration

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 264.



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.

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 75.

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 Server will listen on all interfaces, or in the case of a single NIC, one interface.

	Single NIC	Dual NIC
Client connectivity (production network)	eth0:IP address or Any	eth0:IP address
Switch connectivity (private network)	eth0:IP address or Any	eth2:IP address or eth3:IP address
Media Connectivity	eth0:IP address or Any	eth0:IP address or Any <ul style="list-style-type: none"> • Use eth0:IP address for DMCC applications with media connectivity. • Use Any for all other applications (TSAPI, JTAPI, DMCC with Call Control, Web Services, CVLAN, and DLG).

Administering network interfaces with CVLAN - using the Any network setting

Keep this rule in mind if you are administering an AE Server configured with a single network interface that supports CVLAN and other services, and you want to use the **Any** setting for client connectivity.

 **Note:**

The `/etc/hosts` file must contain the IP address of the host computer that the CVLAN clients are on.

Follow this procedure to use the **Any** setting for client connectivity.

1. Log in as `root`.
2. From the command prompt, type `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 [Figure 25: sample /etc/hosts file](#) on page 76).
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

Adding a switch connection

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 device and media control only -- assigning H.323 IP addresses](#) on page 78.



Important:

AE Services recommends that you use a Processor Ethernet connection or at least two CLANs per switch connection.

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 Server on the IP-Services form was administered (see [Enabling AE Services](#) on page 27).
If you use Device, Media, and Call Control without Call Information Services and you are setting up a switch connection to use the round-robin assignment of H.323 Gatekeepers, a password is not required.
 - b. In the **Confirm Switch Password** field, re-type the password.
 - c. In the **Msg Period** field, accept the default (30 minutes).
 - d. For the **SSL** check box, do one of the following:
 - For all Communication Manager Servers except DEFINITY Server G3csi, accept the default (check box is checked).
 - For the DEFINITY Server G3csi, uncheck this check box. SSL is not supported by DEFINITY Server G3csi.
 - e. For the **Processor Ethernet** check box, do one of the following:

- If you are administering a switch connection to a Communication Manager media server that uses a CLAN connection to AE Services, accept the default (check box is not checked).
- If you are administering a switch connection to a Communication Manager media server that uses a Processor Ethernet connection to AE Services, check this check box.

For information about Communication Manager media servers that support a Processor Ethernet connection, see [Enabling AE Services](#) on page 27.

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.

Administering switch connections for DMCC applications that use device and media control only -- assigning H.323 IP addresses

When you are administering AE Services for DMCC applications that use Call Information 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 connection name, set up a connection and then use the H.323 Gatekeeper feature to associate a list of H.323 Gatekeepers with the switch connection name.

-
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 Processor Ethernet or 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.

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.

Editing CLAN IPs

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 80.

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

After you add a switch connection, you must associate the switch connection name with Processor Ethernet host name or IP address.

-
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 just added (for example, **Switch2**).
 3. Click **Edit PE/CLAN IPs**.
 4. 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.



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**.
-

Checking the status of a switch connection -- from the AE Server to Communication Manager

-
1. From the AE Services Management Console main menu, select **Status > Status and Control > Switch Conn Summary**.
 2. From the **Switch Connections Summary** page, select the switch connection you just added (for example, **Switch1**).
 3. Click **Connection Details**.
 4. Review the information on the **Connection Details** page. Verify that the connection state is **Talking** and the Online/Offline status is **Online**.

 **Important:**

After you complete this procedure, check the status of the switch connection from Communication Manager to the AE Server. See [Checking the status of a switch connection -- from Communication Manager to the AE Server](#) on page 32.

CVLAN implementation guidelines

When you are setting up CVLAN with AE Services, use the following guidelines based on your application requirements.

CVLAN applications and link management

Applications use separate links to avoid conflicts and control load. For example, by using two separate links you can avoid problems with two applications that register as routing servers.

When setting up a link, either a CVLAN link or a proprietary CVLAN link, bear in mind that only one application at a time can register as either a heartbeat server or a routing server. For more information about heartbeat messages and route requests, see the *Application Enablement Services CVLAN Programmer's Reference*, 02-300546.

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 30.
- In the AE Services Management Console, administer the CVLAN link with the Proprietary setting disabled, as described in [Administering CVLAN links](#) on page 82.
- 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 85.

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 30.
- In the AE Services Management Console, administer the CVLAN link with the Proprietary setting enabled. See [Administering CVLAN links](#) on page 82.
- In the AE Services Management Console, administer only one CVLAN client for each CVLAN link. See [Adding CVLAN clients](#) on page 85.

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.

Administering CVLAN links

CVLAN links are used by external and internal applications. (Avaya Interaction Center is an example of an internal application that uses CVLAN links). For more information about setting up CVLAN links, see [CVLAN implementation guidelines](#) on page 81. In the context of CVLAN links, the terms link and signal are synonymous.

 **Note:**

By default the CVLAN service is not started on the AE Server until you administer the first (or only) CVLAN link. After you administer the first CVLAN link, verify that the CVLAN service is running. For more information see [Ensuring the CVLAN service is running](#) on page 84.

-
1. From the AE Services Management Console main menu, select **AE Services > CVLAN > CVLAN Links**.
 2. On the **CVLAN Links** page, click **Add Link**.
 3. On the **Add CVLAN Links** page, do 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 signals (links) was 1 through 8 instead of 1 through 16. If you select 9 through 16, make sure your application is not hard coded to use signals 1 through 8 only.

- b. For the **Proprietary** check box, do one of the following:

- If the CVLAN link is for an external application, accept the default (unselected).
 - If the CVLAN link is for an internal application, check the **Proprietary** check box.
- c. In the **Switch Connection** field, select the switch connection that will be used (for example, **Switch1**).
 - 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 the CVLAN application will support.
 - f. In the **Heartbeat** check box, choose the setting appropriate for the configuration, as follows:
 - Enable the setting (checked) to designate the CVLAN service as the ASAI Heartbeat server.
 - Disable the setting (not checked) to designate the CVLAN application as the ASAI Heartbeat server.
 - g. Click **Apply Changes**.
4. In the **Apply Changes to Link** page, click **Apply**.
 5. Restart the CVLAN service as follows:
 - a. Select **Maintenance > Service Controller**.
 - b. From the **Service Controller** page, select **CVLAN Service**.
 - c. Click **Restart Service**.
The CVLAN service has successfully restarted when the Controller Status displays **Running**.
 6. Check the status of the link on Communication Manager and AE Services. See the following topics:
 - To check the status of the link on Communication Manager, see [Checking the status of a switch connection -- from Communication Manager to the AE Server](#) on page 32.
 - To check the status of the link on AE Services, see [Checking the status of a switch connection -- from the AE Server to Communication Manager](#) on page 80.
-

Ensuring the CVLAN service is running

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

-
1. From the AE Services Management Console main menu, select **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:
 - i. From the AE Services Management Console main menu, select **Maintenance > Service Controller**.
 - ii. From the **Service Controller** page, check the **CVLAN Service** check box .
 - iii. 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

-
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

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.
-

Administering DLG links

DLG links are used by ASAI applications.

1. From the AE Services Management Console main menu, select **AE Services > DLG > DLG Links**.
2. From the **DLG Links** page, click **Add Link**.
3. On the **Add DLG Links** page, do the following:
 - a. In the **Switch Connection** field, select the switch connection that you want to use (for example **Switch1**).
 - 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 Changes**.
5. Restart the DLG service as follows:
 - a. Select **Maintenance > Service Controller**.
 - b. From the **Service Controller** page, select **DLG Service**.
 - c. Click **Restart Service**.
The DLG service has successfully restarted when the Controller Status displays **Running**.
6. Check the status of the link on Communication Manager and AE Services. See the following topics:
 - To check the status of the link on Communication Manager, see [Checking the status of a switch connection -- from Communication Manager to the AE Server](#) on page 32.
 - To check the status of the link on AE Services, see [Checking the status of a switch connection -- from the AE Server to Communication Manager](#) on page 80.

Administering TSAPI links

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 Live Communications Server and the AE Services integration for IBM Lotus Sametime. For more information, see [Checklists for administering the services that run on the AE Server](#) on page 60).

You may administer one TSAPI link for each switch connection.

-
1. From the AE Services Management Console main menu, select **AE Services > TSAPI > TSAPI Links**.
 2. From the **TSAPI Links** page, 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, select the switch connection that you want to use.
 - 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 either **4** or **5**.

**Note:**

Link Version 5 is not supported prior to Avaya Communication Manager 5.0.

- 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. If you select **Encrypted**, all of the TSAPI clients using the Encrypted Advertised TLINK will require the AES 4.1 or later TSAPI client. Access to encrypted TSAPI links is not possible with earlier versions of the TSAPI client software.
 - **Both** – If your organization uses multiple applications, some applications can be set up with unencrypted links and others can be set up with encrypted links. If you select **Both**, all of the TSAPI clients using the Encrypted Advertised TLINK will require the AES 4.1 or later TSAPI client. Any TSAPI clients using the Unencrypted Advertised TLINK can be earlier versions.

**Note:**

For the AE Services integration with IBM Sametime, you must administer TSAPI links as encrypted. If your AE Server supports other TSAPI applications in addition to the integration with Sametime, and some of those applications use unencrypted TSAPI links, you will need to administer TSAPI links with the **Both** setting (so it allows both encrypted and unencrypted).

- f. Click **Apply Changes**.
4. On the **Apply Changes to a Link** page, click **Apply Changes**.
5. Restart the TSAPI service as follows:
 - a. Select **Maintenance > Service Controller**.
 - b. From the **Service Controller** page, select **TSAPI Service**.
 - c. Click **Restart Service**.

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

6. Check the status of the link on Communication Manager and AE Services. See the following topics:
 - To check the status of the link on Communication Manager, see [Checking the status of a switch connection -- from Communication Manager to the AE Server](#) on page 32.
 - To check the status of the link on AE Services, see [Checking the status of a switch connection -- from the AE Server to Communication Manager](#) on page 80.
-

Setting DMCC media properties

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

-
1. From the AE Services Management Console main menu, select **AE Services > DMCC > Media Properties**.
 2. On the **Media Properties** page, review the default settings and make any necessary changes.
-

Setting DMCC station properties

If you use the DMCC Service for media control, use the Media Properties Web page in the AE Services Management Console to change the default media properties if necessary.

-
1. From the AE Services Management Console main menu, select **AE Services > DMCC > Station Properties**.
 2. On the **Station Properties** page, review the default settings and make any necessary changes.
-

AE Services general maintenance

Backing up server data

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

1. From the AE Services Management Console main menu, select **Maintenance > Server Data > Backup**.
2. On the **Database Backup** page, click the **here** link.
3. In the **File Download** dialog box, click **Save**.
4. In the **Save As** dialog box, browse to the location on the computer where you want to store the AE Services server data backup.
5. Click **Save**.

 **Important:**

After your system saves the backup file, locate the file and verify that it has been saved with the .tar.gz extension. If it does not have the .tar.gz extension, rename the file and add the .tar.gz extension (for example, **<hostname>_<AES version>_aesvcsdb05052007.tar.gz**).

For information about restoring the server data, see [Restoring the server data](#) on page 89.

Restoring the server data

Restoring the database 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.

1. From the AE Services Management Console main menu, select **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>_aesvcsdb05052007.tar.gz**).

 **Important:**

Make sure that the database backup file has the .tar.gz extension as described in [Backing up server data](#) on page 89. If you did not rename the file when you ran the backup, be sure to rename it with the .tar.gz extension before you continue with the next step to restore the database.

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 during the interval between clicking **Restore** and **Restart Services**, the restore will not occur.

Viewing log files

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**.

Downloading log files

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



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.
5. From the **File Download** dialog box, click **Save**.
6. In the **Save As** dialog box, browse to the location on your local PC where you want to store the file(s).
7. Click **Save**.

The system stores the compressed error log file in the location you specified.

Configuring network interface settings

1. From the AE Services Management Console main menu, select **Networking > Network Configure**.
2. In the **Physical IP Address** field, type or modify the IP address for each network interface.

 **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.

3. In the **Netmask** field, type an appropriate netmask address for each network interface.
4. Check the **Enable** check box for each network interface.
5. Click **Apply Changes**.
6. From the **Apply Changes to Network Configure** page, click **Apply**.
7. Log into the AE Services Management Console using the new IP address of the AE Services server.

 **Note:**

If the AE Services Management Console does not respond within a reasonable amount of time, from the command prompt, type `service tomcat5 restart`. Then log into the AE Services Management Console again using the new IP address of the AE Services server.

8. From the AE Services Management Console main menu, select **Networking > AE Services IP (Local IP)** and set the new IP address(es) for Client Connectivity, Switch Connectivity, and Media Connectivity.
9. From the command line, execute the script `/opt/mvap/bin/setAlarmSvcUpgrade.sh`
10. From the AE Services Management Console main menu, select **Maintenance > Service Controller**.
11. From the **Service Controller** page, click **Restart AE Server**.
12. Confirm all services are in the **Running** state, and that the connection state to the switch(es) is functional.

 **Note:**

If you cannot access the AE Services Management Console, check the status of the `httpd` and `tomcat5` processes. If they are not running, start them. For example:

```
/sbin/service httpd status
/sbin/service httpd start
```

```
/sbin/service tomcat status  
/sbin/service tomcat start
```

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.

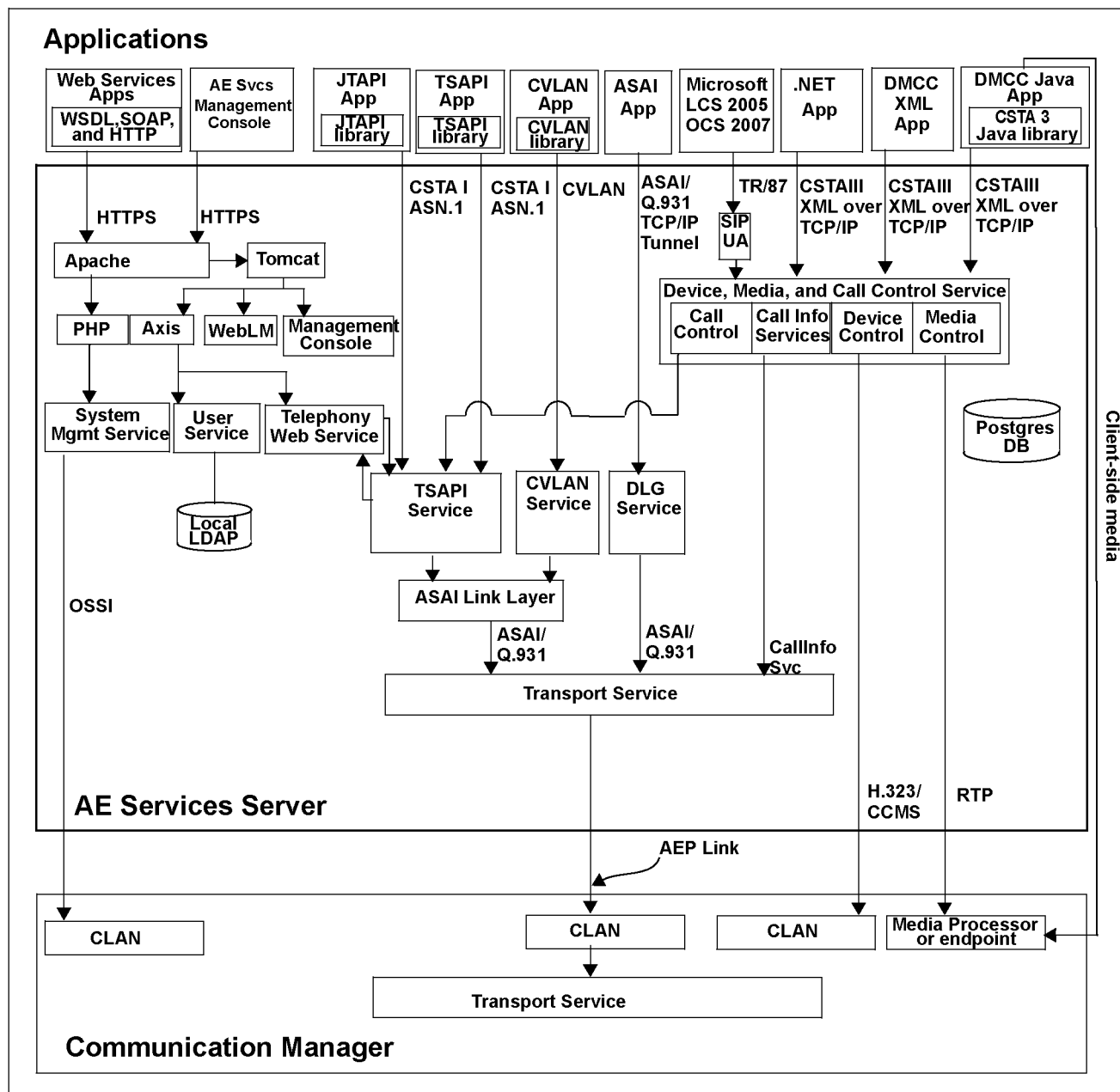


Warning:

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 AE Services configuration](#) on page 94.

Schematic view of an AE Services configuration



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.

Service	Impact of stopping the service
DMCC Service (Device, Media, and Call Control)	<p>If you stop the DMCC service, you lose functionality of the following:</p> <ul style="list-style-type: none"> • All DMCC services • AE Services Implementation of Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007. • Any IBM Sametime clients <p>All other AE Services continue to operate.</p>
DLG Service	<p>If you stop the DLG service, you lose DLG functionality, but all other AE Services continue to operate.</p>
CVLAN Service	<p>If you stop the CVLAN service, you lose CVLAN functionality, but all other AE Services continue to operate.</p>
TSAPI Service	<p>If you stop the TSAPI service, you lose TSAPI functionality and the following clients will not operate:</p> <ul style="list-style-type: none"> • TSAPI • JTAPI • Telephony Web Service • DMCC with Call Control • Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007 • IBM Sametime <p>All other AE Services continue to operate.</p>
ASAI Link Manager	<ul style="list-style-type: none"> • 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 can not communicate with the Transport Layer and Communication Manager. - DLG applications and Device, Media, and Call Control applications that only use device and media control can continue to communicate with Communication Manager.

Service	Impact of stopping the service
	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> • 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 can not 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 Server and the Web Server

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.

If you install your own certificates, follow this procedure. This procedure assumes that you have System Administration privileges.

1. From the AE Services Management Console main menu, select **Maintenance > Service Controller**.
2. From the **Service Controller** page, click **Restart Web Server**. (This restarts Apache and Tomcat.)
3. From the **Restart Web Server** page, click **Restart** to confirm that you want to restart the Web server.
4. From the AE Services log on screen, log in to AE Services again.

5. From the AE Services Management Console main menu, select **Maintenance > Service Controller**.
 6. From the **Service Controller** page, click **Restart AE Server**.
This restarts the ASAI Link Manager, the DMCC service, the CVLAN service, Transport Layer service and the TSAPI service.
 7. From the confirmation page, click **Restart** to confirm that you want to restart the AE server.
-

Chapter 4: User Management Administration

A Linux user or an Enterprise Directory User can access the AE Services Management Console. See [Account Management - Linux user accounts](#) on page 115.

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 285).

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, can not log in to Linux. and they have limited access privileges in the AE Services Management Console.

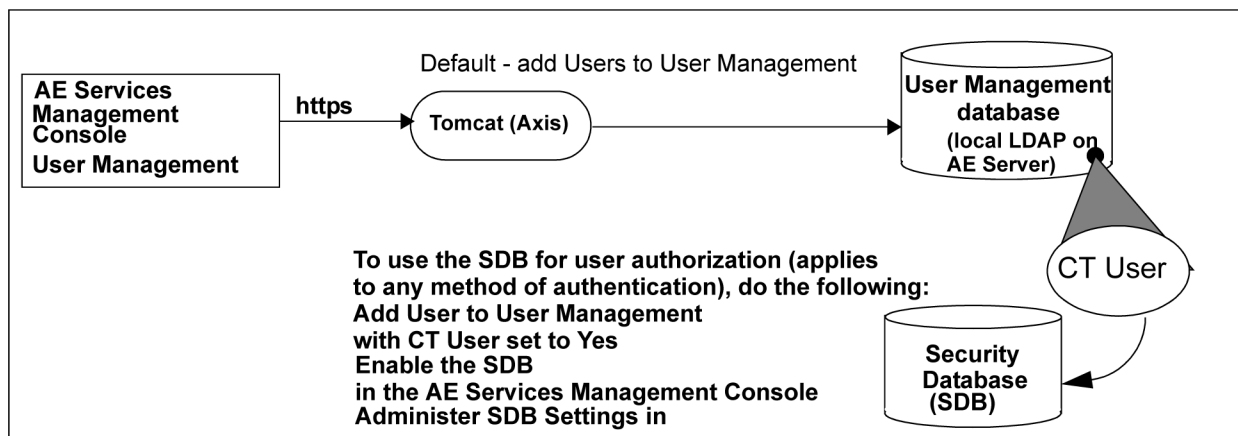


Figure 26: AE Services User Management database

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 130.

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 > Add User**) and set the **CT User** field to **Yes**. See [Adding a user to User Management](#) on page 102.
- Enable the Security Database (SDB). See [APIs that use the Security Database](#) on page 145.
- Administer the settings in the SDB. See [The Security Database](#) on page 145.

Logging into User Management

Follow this procedure to log on 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 user accounts](#).

-
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 Server. For example:
`aserver.example.com`
`135.8.17.123`
 2. From the Application Enablement Services Management Console login page, type the default user name and password, and click **Login**.
Your browser displays the Application Enablement Services Management Console home page for the User Management administrator.
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 273.



Security alert:

After you initially log in, change the default password for the cust and avaya accounts. See [Changing the default password for the avaya account \(User Management administrator\)](#) on page 283.

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 284.

Viewing the list of all users in the User Management database

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

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.

-
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

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

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

-
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

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.

-
1. From the AE Services Management Console main menu, select **User Management > User Admin > Modify Default User**.
 2. On the **Modify Default User** page, in the **Business Category** field, type *Sales*.
 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**.
 7. On the **Modify Default User** page, in the **Business Category** field, type *Support*.
 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

Follow this procedure to change your User Management password.

-
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 **Submit**.
-

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 109.

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 109.

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 109.

**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 109.

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 109.

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 109.

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 109.

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 109.

Re-initializing service configuration files

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.

-
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 - sample scenario

The default user values properties file (defaultuservalues.properties) determines which values appear as the default values on the Add User page in User Management (see [Adding a user to User Management](#) on page 102).

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

-
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 **Submit**.

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 93.
- 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

Chapter 5: 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:
 - Using Linux for authentication
 - Configuring AE Services to access an enterprise directory
 - Using Microsoft Active Directory Services and Kerberos for AE Services authentication
 - Procedures for Integrating AE Services with ADS using Kerberos



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 273.

The Security Administration feature (Account Management and PAM admin) affects the AE Services Management Console and access to the Linux server.

- Account management
 - Add Login
 - Modify Login
 - Remove Login
 - Lock Unlock Login
- PAM management
 - PAM Module Configuration
 - PAM MOTD
 - PAM Issue
 - PAM Limits
 - PAM Time
 - Global Password Aging
- Login Reports
- Login Audit

For an illustration of this administrative domain, see [Figure 27: AE Services Security Administration and PAM management -- AE Services Management Console administrators](#) on page 115.

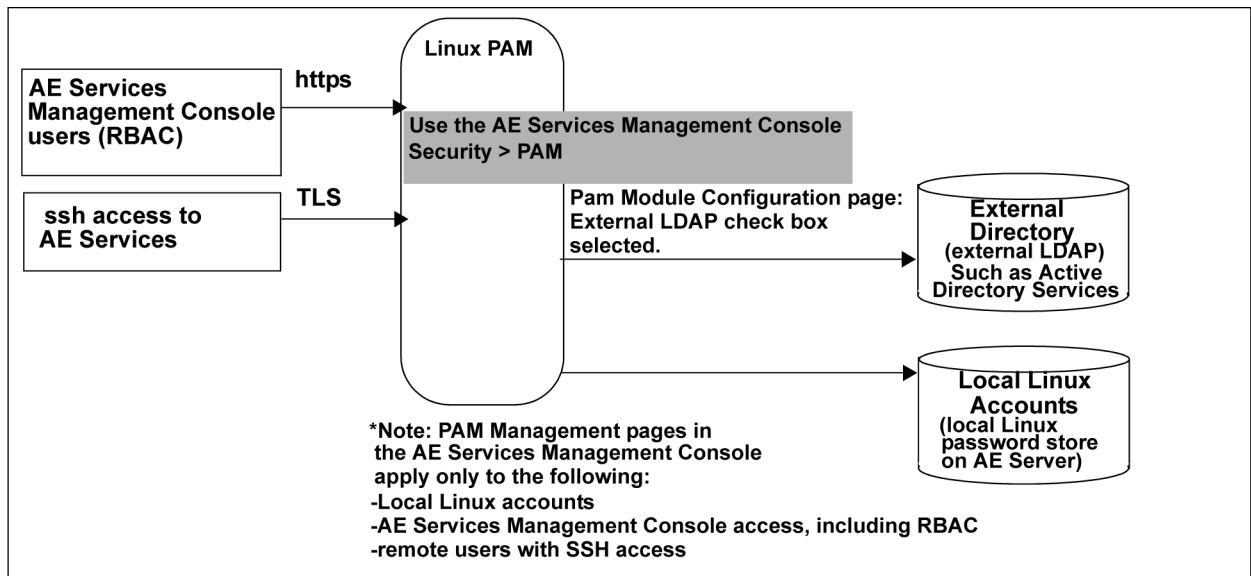


Figure 27: AE Services Security Administration and PAM management -- AE Services Management Console administrators

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 115.
- **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 119.
- **Remove Login** — lets you remove a Linux account. For more information, see [Removing a Linux account - Remove Login](#) on page 120.
- **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 121.

Adding a local Linux account for an administrator - sample

The following procedure is a sample scenario that depicts using a limited number of roles (AE Services provides additional roles). For more information about roles and how they map to Linux groups see [AE Services administrative roles and access privileges \(role based access control - RBAC\)](#) on page 273.

Follow these steps to add a local Linux account for an administrator with the following roles: Auditor, Backup_Restore, and Avaya_Maintenance.

-
1. From 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 (for example `aesadmin3`).
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. Complete the Add Login page as follows:
 - 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. For the **Additional Login Groups** field (optional), type `backuprestore,avayamaint`.
Note that 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`.
 - c. For the **Lock this account** check box, accept the default (unchecked).
 - d. For 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.
 - e. Complete the **Enter Password** and **Re-enter password** fields 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.

- f. For the **Force password change on first login** button accept the default (No).
 - g. In the **Maximum number of days a password may be used** (PASS_MAX_DAYS) field, accept the default (99999).
 - h. In the **Minimum number of days allowed between password changes** (PASS_MIN_DAYS) field, accept the default (0).
 - i. In the **Number of days warning given before a password expires** (PASS_WARN_AGE) field, accept the default (7).
 - j. In the **Days after password expired to lock account** field, accept the default (0).
5. Click **Add**.
- See [Results of adding a local Linux account for an administrator - sample](#) on page 117 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 273.

Role	Linux group	AE Services Management Console access privileges
Auditor	users	Read-only access to the following menus: <ul style="list-style-type: none"> • Security -- access is limited to: <ul style="list-style-type: none"> - Audit - Certificate Management - Security Database > CTI Users - Status - Alarm Viewer - Logs -- access is limited to: <ul style="list-style-type: none"> • Audit Logs • Error Logs

Role	Linux group	AE Services Management Console access privileges
		<ul style="list-style-type: none"> • Install Logs • User Management Service - Status and Control - access is limited to: <ul style="list-style-type: none"> • CVLAN Service Summary • DLG Service Summary • DMCC Service Summary • Switch Conn Summary • TSAPI Service Summary • Help
Security_Administrator	securityadmin	<p>Read and write access to the following menus in the AE Services Management Console:</p> <ul style="list-style-type: none"> • Security <ul style="list-style-type: none"> - Account Management - Audit - Certificate Management - PAM - Security Database - Tripwire Properties • Status <ul style="list-style-type: none"> - Alarm Viewer - Logs - Status and Control • Help
Avaya_Maintenance	avayamaint	<p>Read and write access to the following menus in the AE Services Management Console:</p> <ul style="list-style-type: none"> • Maintenance <ul style="list-style-type: none"> - Security Database - Service Controller - Server Data • Security <ul style="list-style-type: none"> - Audit

Role	Linux group	AE Services Management Console access privileges
		<ul style="list-style-type: none"> - Certificate Management - Security Database • Status <ul style="list-style-type: none"> - Alarm Viewer - Logs • Utilities <ul style="list-style-type: none"> Diagnostics

Changing the properties of a Linux administrative account -- modify login

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 115) to the Avaya Maintenance role only.

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. Click **Modify**.

See [Results of changing role assignments for aesadmin3 - sample](#) on page 120 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 aesamdin3 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 273.

Role	Linux group	AE Services Management Console access privileges
Avaya_Maintenance	avayamaint	<p>Read and write access to the following menus in the AE Services Management Console:</p> <ul style="list-style-type: none"> • Maintenance <ul style="list-style-type: none"> - Security Database - Service Controller - Server Data • Security <ul style="list-style-type: none"> - Audit - Certificate Management - Security Database • Status <ul style="list-style-type: none"> - Alarm Viewer - Logs • Utilities <ul style="list-style-type: none"> Diagnostics

Removing a Linux account - Remove Login

Use the Remove Login feature to delete a Linux administrative account.

**Note:**

If an application (DMCC, TSAPI, JTAPI, or Telephony Web Services) uses local Linux for authentication, the application will also be affected by the Remove Login action.

-
1. From 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. Click **Delete**.
-

Locking or unlocking a Linux account - Lock/Unlock Login

Use the Lock/Unlock Login feature to lock or unlock an existing Linux account. Locking an account means prohibiting access to the AE Services Management Console.

**Note:**

If an application (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.

-
1. From the AE Services Management Console main menu, select **Security > Account Management > Lock Unlock Login**.
 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 the correct account is displayed.
 5. 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 edit the PAM configuration file. For more information, see [Administering the PAM module configuration](#) on page 122.
- The ability to manage the login message. For more information, see [Creating a PAM Issue \(/etc/issue\) message](#) on page 123.
- 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 124.
- The ability to limit the maximum number of simultaneous logins. For more information, see [Adding PAM limits](#) on page 125.
- 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 125.
- The ability to set the global password aging policy. For more information, see [Administering global password aging \(etc/login.defs\)](#) on page 126.

Administering the PAM module configuration

The PAM Configuration Page allows you to determine how AE Services Management Console administrative accounts are authenticated and controlled.

In this sample procedure, the Linux PAM is configured to use an external LDAP server for authentication.

-
1. From the AE Services Management Console main menu, select **Security > PAM > PAM Module**.
 2. Follow these steps to complete the **PAM Module Configuration** page.
 - a. In the **Optional Additional Authentication Protocols** section, select the check box for **External LDAP**.
 - b. In the **Password Limits** section, accept the default settings. These settings are described as follows:
 - **Enforce password limits** - Indicates that password limits are in effect for the user. This setting is enabled by default (the check box is selected).

- 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 **4**.
- c. In the **Failed Login Response** section, accept the default settings. These settings are described as follows:
- Enable account lockout with the following settings. 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.

3. Click **Apply**.

Creating a PAM Issue (/etc/issue) message

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.

-
1. From the AE Services Management Console main menu, select **Security > PAM > PAM Issue**.
 2. Follow these steps to complete the **PAM Issue** page.
 - a. Accept the default, **Display a message prior to login**.
 - b. 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**.
-

Creating a PAM MOTD (/etc/motd) message

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.

-
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**.
-

Adding PAM limits

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.

-
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

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.

-
1. From the AE Services Management Console main menu, select **Security > PAM > PAM Time**.
 2. On the **PAM Time** page, complete the **New Configuration** settings as follows:
 - a. In the **Login** field, enter the login ID or user name.
 - b. From the **Access Rule** drop-down menu, select **Deny**.

- c. For **Days of Week**, select the check box(es) for the appropriate day(s).
 - d. For **Times of Day**, select a time interval as follows:
 - i. For the beginning of the time interval (**From**) select the appropriate hour and minutes.
 - ii. For the end of the time interval (**To**) select the appropriate hour and minutes.
 - e. Click **Apply**.
-

Administering global password aging (etc/login.defs)

The Global Password Aging page in the AE Services Management Console lets you define rules that require users to change their passwords periodically. The Global Password Aging page provides access to the settings in the `/etc/login.defs` file.



Note:

Changes to the global settings will only affect new users. Existing users will not be affected.

The settings you administer on this page are used by the Add Login and Modify Login pages.

-
1. From the AE Services Management Console main menu, select **Security > PAM > Global Password Aging**.
 2. On the **Global Password Aging** page, in the **Maximum number of days a password may be used** (PASS_MAX_DAYS) field, accept the default (**60**).
 3. In the **Minimum number of days allowed between password changes** (PASS_MIN_DAYS) field, accept the default (**1**).
 4. In the **Minimum acceptable password length** (PASS_MIN_LEN) field, accept the default (**8** characters).
 5. In the **Number of days warning given before a password expires** (PASS_WARN_AGE) field, accept the default (**10**).
 6. Click **Apply**.
-

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 127.
- A login report for a particular login ID — see [Displaying a login report for a specific login ID](#) on page 128.

Displaying a login report for all Linux accounts

-
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 127.

List Local Host Logins page field descriptions

Name	Description
Name	Lists the name of the Linux login.
Group	Indicates the group name to which the login name is assigned.
Roles	Indicates the administrative role for a user, such as System_Administrator. For a list of roles, see AE Services administrative roles and access privileges (role based access control - RBAC) on page 273.
Lock	Yes or No to indicate if a lock exists for this account.
Shell Access	Yes or No to indicate whether the login name (account) has access to the Linux shell.

Displaying a login report for a specific login ID

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 128.

Display Login Information page field descriptions

Field	Description
Information for Login:	Identifies the login name.
Group Name	Lists the Linux group name that the login ID is assigned to.
Other Groups	Lists other group names that the login ID is assigned to.
Roles	List the roles that are assigned to the login ID.
Shadow Locked	Indicates whether password shadowing is enabled or disabled. <ul style="list-style-type: none">• Yes - Indicates that password shadowing is enabled.• No - Indicates that password shadowing is disabled.
Pam_Tally Locked	Indicates whether PAM tally limits are enabled or disabled. <ul style="list-style-type: none">• Yes - Indicates that the PAM tally is enabled.• No - Indicates that the PAM tally is disabled.
Shell Access	Indicates whether the login name (account) has access to the Linux shell. <ul style="list-style-type: none">• Yes indicates that the login name has access to the Linux shell.• No indicates that the login name does not have access to the Linux shell.

Field	Description
PW Min Days	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.
PW Max Days	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.
PW Warn Days	Indicates the number of days warning given before a password expires, which is specified by the PASS_MIN_DAYS setting in the etc/login.defs file.
PW Last Changed	Indicates the date (Mon DD YYYY) that the password was last changed.
PW Next Change Allowed	Indicates the first date that the next password change is permitted.
PW Expires	Indicates the date that the password expires.
Account Expires	Indicates the date that the login ID expires.

Enabling a login audit

Use the Login Audit feature to enable and configure an audit process for disabling an unused Linux account.

-
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 130.

Unused Login Audit page field descriptions

Field	Description
Enable the Audit	<ul style="list-style-type: none">• Select Yes to start the auditing process.• Select No to stop the auditing process. No is the default setting.
Time to Begin Audit Each Day: (hour)	Select a start time to begin the audit, based on a 24-hour clock (select from 00 to 23).
Maximum Unused Time: (days, 3-365)	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.
Submit	Click Submit to start the audit process.

Additional PAM management capabilities

If you elect not to use the User Management service, you can authenticate TSAPI, JTAPI, Telephony Web Services, and DMCC clients using any of the following methods:

- Local Linux — see [Linux authentication](#) on page 131
- External LDAP — see [Enterprise directory settings in the AE Services Management Console](#) on page 132
- Microsoft Active Directory Services with Kerberos — see [Authentication with Microsoft Active Directory Services and Kerberos](#) on page 138

See [Figure 28: AE Services client authentication -- additional PAM management](#) on page 131 for a high-level view of the tasks involved when you administer TSAPI, JTAPI, and Telephony Web Services using these methods.

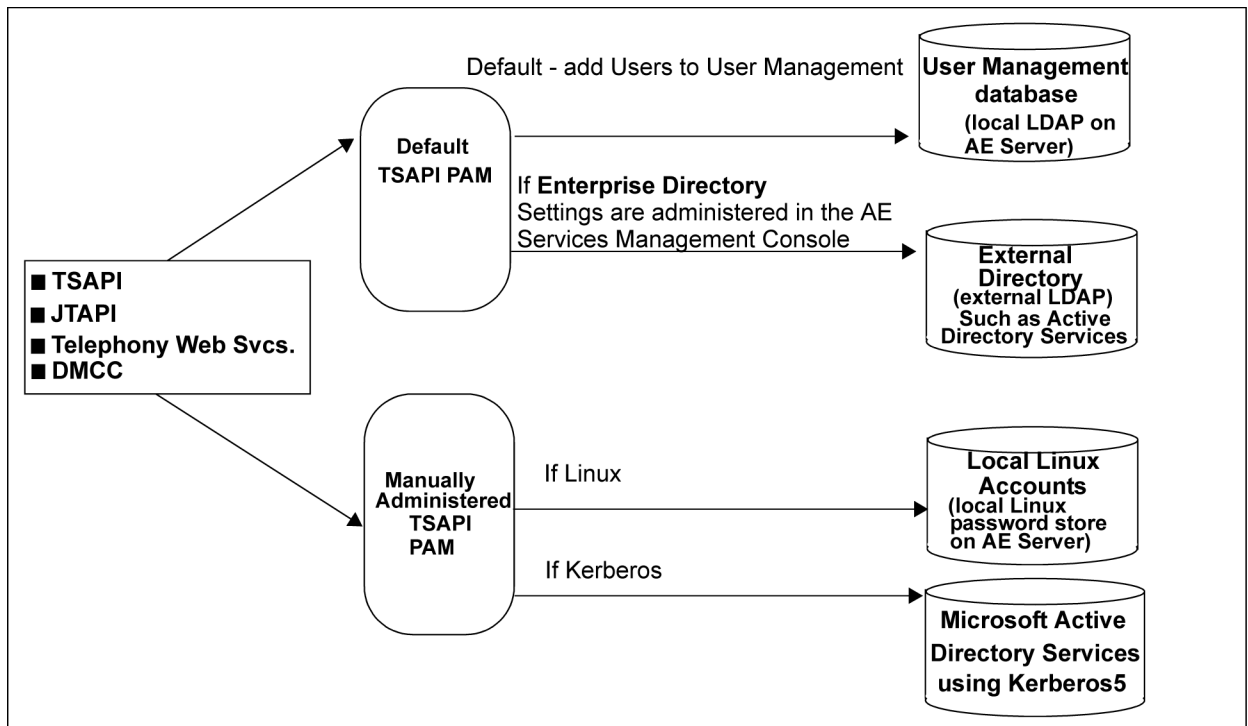


Figure 28: AE Services client authentication -- additional PAM management

Linux authentication

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:
 - Institute the Linux [PAM](#) file instead of the User Management PAM file, see [Instating the Linux PAM file](#) on page 132.
 - Set up a Linux user account for each AE Services user, see [Adding a Linux user](#) on page 172.
 - 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 102.

- 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 132.

Instating the Linux PAM file

-
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
```
-

Re-instating the User Management PAM file

Use this procedure only if you are reverting back to the User Management.

-
1. Log into AE Services and **su** to **root** or **sroot**.
 2. 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 on the Enterprise Directory Configuration page. For an illustration of this context, see [Figure 28: AE Services client authentication -- additional PAM management](#) on page 131.

Enterprise directory configuration settings for AE Services integrations

The enterprise directory configuration settings may apply to the AE Services Implementation for Microsoft Office Live Communications Server (LCS) 2005 or Microsoft Office Communications Server (OCS) 2007. If you are administering AE Services for the LCS/OCS integration, see the *Avaya Aura® Application Enablement Services Implementation Guide for Microsoft Live Communications Server 2005 or Microsoft Office Communications Server 2007*, 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. For AE Services 6.1, this feature applies to DMCC applications as well as the AE Services integrations with Microsoft Office Live Communications Server and Microsoft Office Communications Server. 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



Note:

The AE Services .NET DMCC client does not support client application certificates. As a result, .NET based applications are not able to take advantage of AA policy provisioning.

Configuring AE Services to access an enterprise directory

Follow this procedure to complete the Enterprise Directory Configuration page for a TSAPI, JTAPI, Telephony Web Services, or DMCC application that authenticates to an external LDAP server.

1. From the AE Services Management Console main menu, select **Security > Enterprise Directory**.
2. Complete the following fields on the Enterprise Directory Configuration Page as follows:
 - 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 for the enterprise directory server.
- c. In the **Confirm Password** field, retype the password you typed in the **Password** field.
- d. In the **Base Search DN** field, type the LDAP string that indicates where you want to start your search.
- e. In the **HostName/IP Address** field, type the IP address of the enterprise directory server.
- f. In the **Secondary HostName/IP Address** field, type the IP address of the failover server. (Complete this field only 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 may need to change this setting to match your LDAP implementation. The default attribute names for several 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 is 389 (the port assignment for LDAP).
- 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. Select the check box for **LDAP-S** if your configuration uses a TLS connection from AE Services to your enterprise directory server.

 **Note:**

If you enable LDAP-S, you must first create a server certificate with the alias or name of the LDAP server.

3. Click **Apply Changes**.
-

Configuring an external LDAP server — Windows

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 137 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`.



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

Role	Privileges	Parameters
Auditor	<ul style="list-style-type: none"> • View/List users (CTI, user-management) • View logs • View certificates • View alarms • View status and control 	Auditor
Security_Administrator	<ul style="list-style-type: none"> • Key, certificate management • Role-based access control administration • View security logs 	Security_Administrator

Role	Privileges	Parameters
System_Administrator	Read/write access to all objects/operations except User Management and Security Administrator	System_Administrator
Backup_Restore	Backup and Restore	Backup_Restore
Avaya_Maintenance	<ul style="list-style-type: none"> • Access to maintenance • View logs • Access to utilities 	Avaya_Maintenance
User Management	<ul style="list-style-type: none"> • Manage user accounts • Configure user password policy 	usrsvc_admin (or usrsvc_user) This feature is not available in Release 4.x.

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 can not log into the AE Server (Linux).
- If the security database is enabled, the AE Services user must also have an account administered in User Management.
- The AE Server will authenticate using Kerberos5.



Note:

The time differential between the Domain Controller and the AE 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 139
- [Generating a keytab file for the AE Server account on the Domain Controller](#) on page 140
- [Installing the Kerberos5 RPMs on the AE Server](#) on page 140
- [Editing the Kerberos 5 configuration file on the AE Server](#) on page 141
- [Importing the keytab file on the AE Server](#) on page 142
- [Changing from User Management Authentication to Active Directory Authentication on the AE Server](#) on page 142

Creating an account for the AE Server on the Domain Controller

On the Domain Controller, follow this procedure to create a user account where the AE Server is designated as an Active Directory user.



Note:

To perform this procedure you must be a member of the Admin Group in Windows.

-
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

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`.

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

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.

1. Login as **root** or **sroot** and type the following command:

```
rpm -qa | grep krb
```

If the Kerberos5 RPMs are installed, you will see output similar to the following:

```
krb5-devel-1.2.7-31.i386.rpm
krb5-libs-1.2.7-31.i386.rpm
krb5-workstation-1.2.7-31.i386.rpm
pam_krb5-1.73-1.i386.rpm
```

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 141.

Editing the Kerberos 5 configuration file on the AE Server

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):

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 = dcserver1.xyz.com
dns_lookup_realm = true
dns_lookup_kdc = true
default_tkt_enctypes = des-cbc-md5
default_tgs_enctypes = des-cbc-md5
[realms]
MNO.XYZ.COM= {
    kdc = dc-sename.dcserver1.xyz.com:88
    kpasswd_server = dc-sename.dcserver1.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 142.

Importing the keytab file on the AE Server

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 140) to the AE Server.

-
1. Log in as `root` or `sroot`.
 2. From the command line, type `ktutil`.
 3. From the `ktui` prompt, type the following command to have the `ktutility` read in the keytab file.

```
rkt aeserver.keytab
```

The `ktutility` 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 142.

Changing from User Management Authentication to Active Directory Authentication on the AE Server

This procedure is performed by an administrator on the AE Server.

-
1. Log into the AE 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
```
-

Chapter 6: 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 102.

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 146.
- Device, Media, and Call Control (DMCC) — see [Enabling the SDB for DMCC applications](#) on page 147.

Enabling the Security Database - TSAPI, JTAPI, and Telephony Web Service

-
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 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 147.



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 133.

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

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.

-
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 151.
 - 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 161.
- **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**)

Editing TSAPI properties

1. From the AE Services Management Console main menu, select **AE Services > TSAPI > TSAPI Properties**.
 2. On the **TSAPI Properties** page, in the **TCP Preferred Naming Format** field, select one of the following:
 - If your configuration uses fixed IP addresses for your clients, select **IP Address** (the default).
 - If your configuration uses Dynamic Host Control Protocol or if the IP addresses of your clients frequently change, select **Host Name**.
 3. In the **Extended Worktop Access** field, select one of the following:
 - If you want a CTI user to be able to log in to any worktop and control all the devices on that worktop, enable the check box.
 - If do not want to allow Extended Worktop Access, disable the check box (the default).
-  **Note:**
If you enable this setting,, see [Extended worktop access](#) on page 151 for more information.
4. In the **Auto Admin of LAN Addresses** field, select one of the following:
disabled.

- If you want AE Services to automatically add LAN addresses for all worktops, select **enabled**.
- If do not want to allow Auto Admin of LAN Addresses, select **disabled** (the default).

 **Note:**

If you enable this setting, see [TSAPI properties](#) on page 148 for more information.

5. Click **Apply Changes**.

6. On the **Apply Changes to TSAPI Configuration Properties** page, click **Apply**.

 **Note:**

You must restart the TSAPI service to put your changes into effect. For more information about restarting the TSAPI service, see [Service Controller \(start, stop, and restart services\)](#) on page 93.

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
 - Routing

For a description of these access rights settings, see [Access Rights options](#) on page 152.

- 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 can not 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 152.

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 161.

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 159.

- **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:

AVAYA#switch_connection_name#service_type#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:

```
AVAYA#CM1#CSTA-S#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

The TSAPI service creates the default Tlink group, **Any**.

-
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 156.

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 161.

For a sample procedure that depicts adding a device to the SDB, see [Adding a device to the SDB](#) on page 156.

Adding a device to the SDB

-
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

-
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 158 for more information.

Adding a worktop

-
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

Prerequisites

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.

-
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 can not 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 102.

See [Administering CTI user settings](#) on page 160 for more information.

Administering CTI user settings

You can not 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 102.

-
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 158).
 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

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 152).



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 153.

Initial settings for the sample help desk group

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

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.

-
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

The next procedure in this implementation scenario is to create a Device Group called HELP DESK.

-
1. From the AE Services Management Console main menu, select **Security > Security Database > Device Group**.
 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** (Sues' 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

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.

-
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

The last procedure is to verify the administration of the help desk you just put into effect.

-
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

Worktop Name	Device ID	Secondary Device Group
Tools1	7701	Not applicable (N/A)
Tools2	7702	N/A
Seeds1	7711	N/A
Seeds2	7712	N/A

Table 2: Basic Permissions — User Administration

User ID	Worktop Name	Call Orig&Term	Device/Device Monitor	Call/Device Monitor	Routing
Michael	Tools1	Not applicable (N/A)	N/A	N/A	N/A
Sally	Tools2	N/A	N/A	N/A	N/A
Juan	Seeds1	N/A	N/A	N/A	N/A
Marie	Seeds2	N/A	N/A	N/A	N/A

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

Device Group Name	Device IDs
EXEC LIST	7911, 7912, 7913

Table 4: Manager/Assistant — Worktop Administration

Worktop Name	Device ID	Secondary Device Group
PRESIDENT WKTP	7911	Not applicable (N/A)
VP WKTP1	7912	N/A

Worktop Name	Device ID	Secondary Device Group
VP WKTP2	7913	N/A
ASSISTANT WKTP	7914	N/A

Table 5: Manager/Assistant — User Administration

User ID	Worktop Name	Call Orig&Term	Device Monitoring	Call/Device Monitoring	Routing
President	PRESIDENT WKTP	Not applicable (N/A)	N/A	N/A	N/A
VP1	VP WKTP1	N/A	N/A	N/A	N/A
VP2	VP WKTP2	N/A	N/A	N/A	N/A
Exec Assistant	ASSISTANT WKTP	EXEC LIST	EXEC LIST	N/A	N/A

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

Worktop Name	Device ID	Secondary Device Group
ASSISTANT WKTP	7914	EXEC LIST

Table 7: Manager/Assistant — User Administration

User ID	Worktop Name	Call Orig&Term	Device Monitoring	Call/Device Monitoring	Routing
Exec Assistant	ASSISTANT WKTP	Not applicable (N/A)	N/A	N/A	N/A

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

Device Group Name	Device IDs
ACD AGENTS	7701,7702,7711,7712

Table 9: Call Monitoring — User Administration

User ID	Worktop Name	Call Orig&Term	Device Monitoring	Call/Device Monitoring	Call/Call Monitoring
Martha	ACD SUPV	ACD AGENTS	ACD AGENTS	ACD AGENTS	Enabled

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

Device Group Object	Device IDs
ACD Substitutes	7701,7702,7711,7712

Table 11: Shared Worktop — Worktop Administration

Worktop Name	Device ID	Secondary Device Group
WKTP1	7801	ACD Substitutes
WKTP2	7802	ACD Substitutes

Table 12: Shared Worktop — User Administration

User ID	Worktop Name	Call Orig&Term	Device Monitoring	Call/Device Monitoring	Routing
Tom	WKTP1	Not applicable (N/A)	N/A	N/A	N/A
Lalitha	WKTP2	N/A	N/A	N/A	N/A

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

Worktop Name	Device ID	Secondary Device Group
Shipping	7810	Not applicable (N/A)

Table 14: Shared Worktop — Secondary Device User Administration

User ID	Worktop Name	Call Orig&Term	Device Monitoring	Call/Device Monitoring	Routing
Louise	SHIPPING	Not applicable (N/A)	N/A	N/A	N/A
Frank	SHIPPING	N/A	N/A	N/A	N/A
Susan	SHIPPING	N/A	N/A	N/A	N/A

Prompted 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

Device Group Name	Device IDs
CSR VDN	7800

Table 16: Prompted Digits — User Administration

User ID	Worktop Name	Call Orig&Term	Dev/Device Monitoring	Call/Device Monitoring	Routing
Beth	WKTPA	Not applicable (N/A)	N/A	CSR VDN	N/A
Sally	WKTPB	N/A	N/A	CSR VDN	N/A
Dave	WKTPC	N/A	N/A	CSR VDN	N/A

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

Device Group Name	Device IDs
ACD ROUTE	7700,7710

Table 18: Call Routing — User Administration

User ID	Worktop Name	Call Orig&Term	Dev/Device Monitoring	Call/Device Monitoring	Routing
Routing App					ACD ROUTE

Chapter 7: 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.

Username	Linux Group	Comments
sroot	root	Created when you install AE Services. The AE Server can not be directly accessed through ssh .
craft	suser and securityadmin	Created when you install AE Services. Provides read and write access to all AE Services Management Console features.
rasaccess	remote	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.



Security alert:

AE Services technicians should change the default passwords for the services accounts immediately. See [AE Services administrative roles and access privileges \(role based access control - RBAC\)](#) on page 273.

Changing the default passwords for sroot, craft, and rasaccess

This procedure is for service technicians, and it applies to either an AE Services Bundled Server or a Software-Only server with the Avaya Services Package (cs-service) installed.

-
1. Do one of the following:
 - a. If you have the Software-Only offer with the Avaya Services Package (cs-service), log in to the AE Server as **root**.
 - b. If you have the Bundled Server offer with the Avaya Services Package (cs-service), log in to the AE Server with your user account and then become the superuser (**su sroot**).
 2. Type `passwd username` to display the password prompt. For example `passwd sroot`.
 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

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 115.

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 273.

-
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 Server. The Tripwire information provided in this section applies to the AE Services Bundled server; it does not apply to the Software-Only server. This section describes how to configure Tripwire for administrative access and how to use the Tripwire features.

For information about Tripwire for AE Services on System Platform, see *Implementing Avaya Aura® Application Enablement Services on Avaya Aura® System Platform*, 02-603468.

Reconfiguring the Tripwire database for administrative access

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.

-
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

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.

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

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`.

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

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.

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

When Tripwire is installed, it will be configured as a service. To start or stop Tripwire, simply treat it as any other service.

-
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

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.

-
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

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.

-
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.

[Table 19: The netconfig utility - Network Information Configuration settings](#) on page 178 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

		Comments	
Hostname	aeserver	Host name of the AE Server	
DNS Domain	example.com	Name of the DNS server	
DNS Server	192.168.123.44	IP address of the DNS server.	

Interface	Type	Address	Netmask	Enable	Comments
eth0	[]	192.168.123.43	255.255.255.0	[x]	eth0 is usually assigned the IP address for client access.
eth1	[]	192.168.123.42	255.255.255.0	[x]	eth1 is reserved for on-site technician use.
eth2	[]	192.168.123.41	255.255.255.0	[x]	eth2 is usually assigned the IP address for Communication Manager access (Private LAN).
eth3	[[]	Reserved
eth4	[]			[]	Reserved

		Comments	
Default Gateway	192.168.12.344	The IP address of the network router.	

Changing the server IP address – Bundled server

Follow this procedure to configure network interface settings for a Bundled server.

1. Log in as **root**.
2. From the command line, type `service mvap stop`.

3. Type the following command to bring up the network configuration screen in Linux:
`/opt/mvap/bin/netconfig`
4. Add or modify the IP address(es) for the network interfaces, and make sure the network interfaces are enabled (an **x** appears in the **Enabled** column).
5. Select **OK** and then press **Enter**.
6. Log in again as **sroot** with the new IP address if administering remotely.
7. From the command line, as a precautionary step, type `service network restart`.
8. 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`

9. From the AE Services Management Console main menu, select **Administration > Network Configuration > Local IP**.
10. 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.
11. From the command line, type the following command:
`/opt/mvap/bin/setAlarmSvcUpgrade.sh`
12. From the AE Services Management Console main menu, select **Maintenance > Service Controller**.
13. From the **Service Controller** page, click **Restart AE Server**.
14. 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`

Changing the server IP address – Software-Only server

Follow this procedure to configure network interface settings for a Software-Only server.

1. Log in as **root**.
2. From the command line, type the following command:
`/sbin/service mvap stop`

 **Note:**

AE Services strongly recommends using a Linux utility such as **/usr/bin/system-config-network** if you are using Red Hat Release 4.

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

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. Use `mvap.sh` only when necessary.

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>*

<service name>

CmapiService - Device, Media, and Call Control Service

CvlanService - CVLAN Service

TsapiService - TSAPI Service

DlgService - 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 two 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

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 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 Server. When you use `ethtool` to change the network interface settings, the changed settings will not persist after rebooting the AE 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 265.

The following list provides examples of using the `ethtool` command for AE Services.

- `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 Bundled 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:

- **mvap** — refers to all AE Services (ASAI Link Manager, CMAPI Service, CVLAN Service, DLG Service, TSAPI Service, and the Transport Layer Service).
- **DBService** — refers to the Postgres database.
- **tomcat5** — refers to the Tomcat Web application server.

shutdown -r now

Reboots the AE Server.

ssh

The **telnet** command is disabled on the Bundled 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.

tethereal

This tool is a sniffer that allows you to sniff packets to and from the AE Server. The **tethereal** command is very useful for debugging network traffic.

Located in `/usr/sbin/`

Example **tethereal** command lines:

```
tethereal -i eth0 -V -x > /tmp/sniff.out
```

Sniffs packets on the eth0 NIC in verbose mode and also dumps all the raw bytes into /tmp/sniff.out .

```
tethereal -i eth1 -V -x " -R ip.addr==136.1.1.1" > /tmp/sniff.out
```

Sniffs packets to and from IP address 136.1.1.1. on eth1 network interface in verbose mode and dumps all raw bytes into /tmp/sniff.out.

```
tethereal -i lo -V -x " -R (ip.addr==136.1.1.1) && (udp.port==6661 || tcp.port==7772) > /tmp/sniff.out:
```

Sniffs packets to and from IP address 136.1.1.1 and udp port 6661 or tcp port 7772 on NIC lo (loopback) in verbose mode and dumps all the raw bytes into /tmp/sniff.out.

tripwire

See [Using Tripwire](#) on page 173.

Installation and upgrade logs and RPMs

The Installation/upgrade logs are located in: `/var/disk/logs/upgrade.out-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`.

AE Services disk partitioning scheme

This section about disk partitioning applies to the Bundled Server only.

It is important to understand the disk partitioning scheme of the AE Server before you create directories or files on the AE Server. The AE Server has a SATA drive with an 80GB capacity. Once AE Services is installed, it has three disk partitions.

`/` - the active partition, with approximately 18.5 GB of space

`/root2` - the inactive or offline partition, with approximately 18.5 GB of space

`/var` - the common partition, with approximately 37 GB of space

The remaining space is allocated for cache and other uses.

Partitioning after an upgrade

The AE Services software is installed on the `/` partition when it is initially installed.

When an upgrade of AE Services software is performed, the upgrade script installs the new version of AE Services software on the `/root2` inactive partition first.

The upgrade script then reboots the AE Server server. Upon reboot the `/` and `/root2` partitions are switched. So, the new version of AE Services software is now on `/` the active partition and the old version is on the `/root2` partition.

Guidelines for creating directories

If you want to create directories or files on AE Server, it is strongly recommended that you create directories or files in the `/var` common partition. Otherwise any directory or file created in the `/` active partition will be moved to the `/root2` partition upon an upgrade of AE Services software. One exception is that any directory or file created in the `/home` directory under any of the logins such as `sroot`, `craft`, and so on, is always copied over during an upgrade. Because copying large files (such as media files or databases) is time consuming, it can delay the upgrade process if these files are stored in the `/home` directory of any login.

To summarize, it is highly recommended that any user level files including media files and databases be stored in the `/var` partition.

About the HMDC utility

The Historical Metric Data Collector (HMDC) utility enables you to collect, store, and display real-time and historic product-specific performance data. The HMDC utility is managed as a service and is administered via the Command Line Interface (CLI).

Note:

You must be a member of the group `suser` to administer the HMDC utility.

Using the HMDC utility, 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

Note:

The Command Line Interface (CLI) logs an entry in `MVAP_LOGS/hmdc/hmdc.log` for each HMDC command used.

Checking the status of the HMDC utility

The HMDC service is managed by `chkconfig`.

-
1. Log in with an account that is a member of the *suser* group.
 2. Type `chkconfig -list` and press **Enter**.
-

Starting/stopping the HMDC utility

After a fresh installation, the HMDC service is stopped by default.

-
1. Log in with an account that is a member of the *suser* group.
 2. Perform one of the following steps:
 - To stop the HMDC service, type `sudo service hmdc stop` and press **Enter**.
 - To start the HMDC service, type `sudo service hmdc start` and press **Enter**.
-

Scheduling data collection

Use this procedure to configure the HMDC utility to collect specific data. See [HMDC data](#) on page 190 for the data the HMDC utility can collect.

-
1. Log in with an account that is a member of the *suser* group.
 2. Type `hmdc schedule [-c cleanup-interval] [-s sampling-interval] [-m metric-group]`

where:

cleanup-interval is the time interval after which you want the data deleted. Choices are daily, weekly, monthly, and yearly. The default is weekly. This is an optional parameter.

sampling-interval is the time interval (in minutes) at which you want the sample collected. The default is 60 minutes. This is an optional parameter.

metric-group is the metric group data you want collected. Choices are system, transport, clvan, tsapi, dmcc, and dlg. By default, all metric group data will be collected. This is an optional parameter.

Example:

If you enter `hmdc schedule -m transport`, the data for the Transport group will be collected at a sampling interval of 60 minutes (the default setting). This data will also be deleted (that is, cleanup) weekly (the default setting).

If you enter `hmdc schedule -c yearly -s 10 -m cvlan`, the data for the CVLAN group will be collected at a sampling interval of 10 minutes. This data will also be deleted yearly.

3. Press **Enter**.

HMDC data

You can configure the HMDC utility to collect the data shown in the following table.

Metric Group	Metric Name	Description
System	SysCPU	Operating system total CPU utilization.
	SysMemory	Operating system memory usage.
	MvapNetRTT	IpAddress of AEP Link.
Transport	avAesaepLinkMsgSent	The number of messages sent for AEP Link in the last “window” minutes.
	avAesAepLinkMsgRcvd	The number of AEP messages received for AEP link in the last “window” minutes.
	avAesAepSessionsMsgSent	The number of messages sent for AEP session in the last “window” minutes.
	avAesAepSessionMsgRcvd	The number of messages received for AEP session in the last “window” minutes.
	avAesTciConnMsgSent	The number of TCI messages sent in the last “window” minutes.
	avAesTciConnMsgRcvd	The number of TCI messages received in the last “window” minutes.

Metric Group	Metric Name	Description
CVLAN	avAesCvlanCtiLinkMsgSent	The number of messages sent to Avaya Communication Manager in the last “window” minutes.
	avAesCvlanCtiLinkMsgRcvd	The number of messages received from Avaya Communication Manager in the last “window” minutes.
DLG	avAesDlgCtiLinkMsgSent	The count of messages sent to Avaya Communication Manager in the last “window” minutes.
	avAesDlgCtiLinkMsgRcvd	The count of messages received from Avaya Communication Manager in the last “window” minutes.
TSAPI	avAesTsapiCtiLinkMsgSent	The number of messages sent to Avaya Communication Manager in the last “window” minutes.
	avAesTsapiCtiLinkMsgRcvd	The number of messages received from Avaya Communication Manager in the last “window” minutes.
	avAesTsapiClientDeviceMonitors	The number of device monitors currently active.
	avAesTsapiClientCallMonitors	The number of call monitors currently active.
	avAesTsapiClientVdnMonitors	The number of VDN monitors currently active.
	avAesTsapiClientRegisteredRoutes	The number of route registrations currently active.
DMCC	avAesDmccActiveSessions	The number of active DMCC sessions.
	avAesDmccActiveDevices	The number of active devices.
	avAesDmccUsedMonitors	The number of monitors currently in use across the DMCC sessions.
	avAesDmccMaxMonitors	The number of monitors available to a DMCC service.

Unscheduler data collection

-
1. Log in with an account that is a member of the *suser* group.
 2. Type `hmdc unschedule [-m metric-group]`
where *metric-group* is the metric group data you want unscheduled. Choices are system, transport, clvan, tsapi, dmcc, and dlg. By default, all metric group data will be unscheduled. This is an optional parameter.
Example:
If you enter `hmdc unschedule -m tsapi`, data collection for the tsapi metric group is unscheduled.
If you enter `hmdc unschedule`, data collection for all metric groups is unscheduled.
 3. Press **Enter**.
-

Viewing configured schedules

Use this procedure to view the events you have scheduled.

-
1. Log in with an account that is a member of the *suser* group.
 2. Type `hmdc list [-m metric-group]`
where *metric-group* is the metric group data that will be collected. Choices are system, transport, clvan, tsapi, dmcc, and dlg. By default, all metric group data will be collected. This is an optional parameter.
Example:
If you enter `hmdc list -m transport`, the schedule details for the transport metric group are displayed..
If you enter `hmdc list`, the details are displayed for all metric groups that have been scheduled.
 3. Press **Enter**.
-

Creating a metric data report

By default, the HMDc utility automatically generates a predefined report in the .CSV format. This report is generated daily at 23:45 and stored in `/opt/mvap/hmdc/reports/report_<date>.csv`. The daily reports are kept for one week.

Each report displays the following information:

- Sample time
- Metric name
- Value
- IP address
- Link ID
- Link type
- Message period
- Switch name
- Tlink name

-
1. Log in with an account that is a member of the *suser* group.
 2. Type `hmdc report [-f from date [-t to date]] [-s sort by] [-m metric-group] filename`

where:

from date is the start date. Enter the date in the format mm/dd/yyyy. This is an optional parameter.

to date is the end date. Enter the date in the format mm/dd/yyyy. This is an optional parameter.

sort-by is sort criteria for the data. Choices are time (date of the data) and name (metric-group followed by metric name). The default is time. This is an optional parameter.

metric-group is the metric group data you want collected. Choices are system, transport, clvan, tsapi, dmcc, and dlq. By default, all metric group data will be collected. This is an optional parameter.

filename is the name of file to which the report will be saved. This is a mandatory parameter.

Example:

If you enter `hmdc report -m system /tmp/systemReport.csv`, a report containing the metrics collected for the system metric-group will be generated and saved to `/tmp/systemReport.csv`. This data will be sorted by time.

If you enter `hmdc report /tmp/allStatReport.csv`, a report containing the metrics collected for all configured metric groups will be generated and saved to `/tmp/allStatReport.csv`.

3. Press **Enter**.
-

Cleaning up data immediately

Use this procedure to delete collected data immediately.

-
1. Log in with an account that is a member of the *suser* group.
 2. Type `hmdc cleanup [-o date | [-f from date [-t to date]] [-m metric-group]`

where:

date is data older than the specified date. Enter the date in the format mm/dd/yyyy. This is an optional parameter.

from date is the start date. Enter the date in the format mm/dd/yyyy. This is an optional parameter.

to date is the end date. Enter the date in the format mm/dd/yyyy. This is an optional parameter.

metric-group is the metric group data. Choices are system, transport, clvan, tsapi, dmcc, and dlg. By default, all metric group data will be deleted. This is an optional parameter.

Example:

If you enter `hmdc cleanup -m system`, all of the data collected for the system metric group will be deleted.

If you enter `hmdc cleanup`, all of the data collected for all of the metric groups will be deleted.

3. Press **Enter**.
-

Chapter 8: 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) 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. The AE Services 6.1 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

The SNMP Agent incorporated into AE Services 6.1 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.

-
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 **None**, **HMAC-MD5**, or **SHA**.
 - c. If you selected either **HMAC-MD5** or **SHA**, in the **Authentication Password** field, enter an alphanumeric authentication password for authenticated SNMP v3 messages. This password can be a 6– to 32– character string.
 - d. From the **Privacy Protocol** drop down list box, select either **None**, **DES**, or **SHA**.
 - e. If you selected either **DES** or **SHA**, in the **Privacy Password** field, enter an alphanumeric privacy password for encrypted SNMP v3 messages. This password can be a 6– to 32– character string.
 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:**

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 SSG

If you have the AE Services Bundled Server, and you 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 and a local NMS

device. For more information about Secure Access and Control (SAC), see <http://support.avaya.com/sac>.

Traps sent to an SSG result in Initialization and Administrative System (INADS) notifications. INADS notifications, in turn, generate trouble tickets with Avaya Services.

 **Note:**

Traps such as tripwire notifications and login failures are not sent to an SSG. When you are administering the AE Server to send traps, you will want to send these traps to a local NMS.

If you do not have the SAC Offer

If you do not have the SAC Offer, you can send traps to a local NMS only. The SAC offer is available with the AE Services Bundled Server only. If you use the AE Services Software-Only server, the SAC 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

Follow this procedure to send traps from the AE Server to an SNMP manager, which can be either a local NMS device or an Avaya SSG.

-
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 traps to a remote NMS device (IBM *Tivoli* or HP *Openview*, for example). If you are administering a Software-Only server, the Device setting is restricted to NMS.

- Select **SSG** to send traps to an Avaya Secure Services Gateway. Keep in mind that only an SSG is capable of generating INADS notifications. This option is available only to Avaya Services accounts with **craft** log in access.
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 can not 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**, if any, that your SNMP managed network uses:
 - **None** indicates that the network does not perform authentication. This is the default.
 - **HMAC-MD5-96** indicates that the network uses the HMAC-MD5 authentication protocol.
 - **HMAC-SHA-96** indicates that the network uses the HMAC-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** ,if any, that your SNMP managed network uses:
 - **None** indicates that the network does not use a privacy protocol and does not perform any encryption. This is the default.

- **DES** indicates that the network uses the DES encryption protocol.
- **AES128** indicates that the network uses the AES128 encryption protocol.
- **AES192** indicates that the network uses the AES192 encryption protocol (not available for the Bundled Server).
- **AES256** indicates that the network uses the AES256 encryption protocol (not available for the Bundled Server).



Note:

AES192 and AES256 are not enabled during a standard OS installation and are controlled under U.S. federal export laws. For more information, see [Using AES 192 and AES 256](#) on page 200.

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.

Using AES 192 and AES 256

This information does not apply to the AE Services Bundled Server.

If you have the AE Services Software-Only Offer, and you plan to use Advanced Encryption Standard (AES)192 or AES 256 to encrypt SNMP message traffic, you will need to set up the AE Server to use these high encryption levels.

Follow these guidelines for setting up the AE Server to use AES 192 or AES 256.

- Install Third Party Software that provides the “Strong Encryption Package.” For information about getting the software, use the following links:

<http://www.gnupg.org/>

<http://www.jus.uio.no/lm/electronic.commerce/cryptography/encryption>

- Configure the AE Server's operating system to allow for these high encryption levels.
- Administer AE Services to use SNMP version 3 and a Privacy Protocol of either AES 192 or AES 256 by following the procedure described in [Administering SNMP trap receivers](#) on page 198.

Testing SNMP Traps

The following procedure provides you with a way to verify that you are able to receive a trap locally (on the AE Server) and remotely (on a remote NMS device).

 **Note:**

This procedure applies to AE Services 4.x through 6.1 configurations. If you are using AE Services 4.0 or 4.0.1, you must install the appropriate patch before you use this procedure for testing SNMP traps. If you are using 4.1 or 4.2, you do not need to install the patch. To get the patches, go to <http://support.avaya.com/download>, which requires Avaya Single Sign On (SSO), and download the appropriate patch:

- Application Enablement Services 4.0.1 Patch 1
- Application Enablement Services 4.0 Patch 2

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; customers use the **cust** user name and password).
4. From the AE Services Management Console main menu, select **Utilities > SNMP > 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 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.
 - h. Click **Apply**.
6. Click **Add Trap**.
7. As a root user on the AE Server, start the trap listener by typing the following command:


```
snmptrapd -fLo
```

8. Open another window as a root user on the AE Server and type the following command:

```
logger -t mon -i "High CPU"
```
 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. Use the AE Services Alarm Manager (**Status > Alarm Viewer**) to clear the alarms you just generated. For information about removing alarms, see [Working with alarm reports](#) on page 202.
-

Working with alarm reports

The following procedure demonstrates how to set up and generate a log report. For a listing of error codes that appear in an alarm report, see [AE Services alarm codes and messages](#) on page 203.



Note:

To view the Alarm Report, your browser must allow pop-ups from the AE Server.

1. From the AE Services Management Console main menu, select **Status > Alarms**.
2. From the **Alarm Manager** page, follow these steps:
 - a. In **System Name(s)** field, keep the default setting, **All Systems**.
For AE Services this is the default. It refers to the AE Server.
 - b. In the **Search Keyword(s)** field, enter a term that appears in the alarm message records, such as `CPU Utilization`, `login attempts`, and so forth.
You can also leave this field blank.
 - c. In the **Status** field, select the status indicator you want to use for setting up your report.
 - d. In the **Sort By** field, you can select to view alarms in terms of time, severity, category, status, or system name.
For example, to see a report that starts with the highest severity alarms, select **Severity: highest first**.
 - e. Use the **Date and Time** selections to determine the range of dates and times that are in your report.
For example, to see a report of errors in the last five days, select the option button for the **Last number of days**, and enter 5.

- f. Use **Categories and Severities** to determine whether your report includes platform errors, critical errors, major, errors, or minor errors.
For example, to see a report of critical platform alarms, select the check boxes for **Platform** and **Critical**, and uncheck the selections that you do not want in the report. You must select **Platform** and at least one severity level (**Critical**, **Major**, or **Minor**) to generate a report.
 - g. Click **OK** to generate a report.
Your browser displays the **Alarm Report** Web page with a display of all the types of alarms you specified on the **Alarm Manager** Web page.
3. On the **Alarm Report** page, review the alarms that are displayed.
Follow these steps to clear an alarm:
 - a. Go to the end of the **Alarm Report** page and locate the **Change Alarm Status** settings.
 - b. Select the option button for **Selected Alarms**.
 - c. In the check boxes to the left of the alarm, select the alarms you want to clear.
 - d. In the **New Status** field, select **RETIRED**, and click **SUBMIT**.
AE Services redisplay the **Alarm Report** page. The alarms you cleared are displayed as hyperlinks (RETIRED).
 - e. Click **RETIRED** to display the **Alarm History** page, which provides a history of the alarm.

**Note:**

Once you have cleared an alarm, you can not change its status. The RETIRED alarm will be cleared by the alarm service.

AE Services 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 columns labeled **INADS Trap** and **NMS Trap** are used to indicate which alarms will issue a trap to Avaya SSG (INADS) and/or a remote NMS.

Alarm Code	Alarm Message	INADS Trap	NMS Trap	Priority Level
AAES000	The AE Services POSTGRES service stopped unexpectedly	Yes	Yes	Minor
AAES001	The AE Services POSTGRES service started successfully	No	Yes	Minor

Alarm Code	Alarm Message	INADS Trap	NMS Trap	Priority Level
AAES002	The AE Services ASAI Link Manager service stopped unexpectedly	Yes	Yes	Minor
AAES003	The AE Services ASAI Link Manager service started successfully	No	Yes	Minor
AAES004	The AE Services CVLAN Server stopped unexpectedly	Yes	Yes	Minor
AAES005	The AE Services CVLAN Server started successfully	No	Yes	Minor
AAES006	The AE Services DLG Server stopped unexpectedly	Yes	Yes	Minor
AAES007	The AE Services DLG Server started successfully	No	Yes	Minor
AAES008	The AE Services Transport service stopped unexpectedly	Yes	Yes	Minor
AAES009	The AE Services Transport service started successfully	No	Yes	Minor
AAES010	The AE Services TSAPI service stopped unexpectedly	Yes	Yes	Minor
AAES011	The AE Services TSAPI service started successfully	No	Yes	Minor
AAES012	The AE Services DMCC stopped unexpectedly	Yes	Yes	Minor
AAES013	The AE Services DMCC service started successfully	No	Yes	Minor
AAES014	The AE Services Lifecycle Manager stopped unexpectedly	Yes	Yes	Minor
AAES015	The AE Services Lifecycle Manager service started successfully	No	Yes	Minor
AAES018	The AE Services ASAI Link Manager service cold started successfully	No	Yes	Minor
AAES019	The AE Services ASAI Link Manager service stopped successfully	No	Yes	Minor
AAES020	The AE Services CVLAN Server cold started successfully	No	Yes	Minor
AAES021	The AE Services CVLAN Server stopped successfully	No	Yes	Minor

Alarm Code	Alarm Message	INADS Trap	NMS Trap	Priority Level
AAES022	The AE Services DLG Server cold started successfully	No	Yes	Minor
AAES023	The AE Services DLG Server stopped successfully	No	Yes	Minor
AAES024	The AE Services Transport service cold started successfully	No	Yes	Minor
AAES025	The AE Services Transport service stopped successfully	No	Yes	Minor
AAES026	The AE Services TSAPI service cold started successfully	No	Yes	Minor
AAES027	The AE Services TSAPI service stopped successfully	No	Yes	Minor
AAES028	The AE Services DMCC service cold started successfully	No	Yes	Minor
AAES029	The AE Services DMCC stopped successfully	No	Yes	Minor
AAES030	The AE Services Lifecycle Manager service cold started successfully	No	Yes	Minor
AAES031	The AE Services Lifecycle Manager stopped successfully	No	Yes	Minor
AAES100	An AE Services TSAPI CTI link is down	No	Yes	Minor
AAES101	An AE Services TSAPI CTI link is up	No	Yes	Minor
AAES102	An AE Services CVLAN CTI link is down	No	Yes	Minor
AAES103	An AE Services CVLAN CTI link is up	No	Yes	Minor
AAES104	An AE Services DLG CTI link is down	No	Yes	Minor
AAES105	An AE Services DLG CTI link is up	No	Yes	Minor
AAES106	An AE Services AEP connection is down	No	Yes	Minor
AAES107	An AE Services AEP connection is up	No	Yes	Minor
AAES108	An AE Services Call Info connection is down	No	Yes	Minor
AAES109	An AE Services Call Info connection is up	No	Yes	Minor
AAES110	The WebLM connection is down	No	Yes	Minor
AAES111	The WebLM connection is up	No	Yes	Minor
AAES200	An AE Services TSAPI user authentication failure occurred	No	Yes	Minor

Alarm Code	Alarm Message	INADS Trap	NMS Trap	Priority Level
AAES201	An AE Services CVLAN user authentication failure occurred; the requested signal number was not valid for the client	No	Yes	Minor
AAES202	An AE Services CVLAN user authentication failure occurred	No	Yes	Minor
AAES203	An AE Services DLG user authentication failure occurred; the requested client link number was not valid for the client	No	Yes	Minor
AAES204	An AE Services DLG user authentication failure occurred	No	Yes	Minor
AAES205	The Server Certificate will expire in 30 days	No	Yes	Minor
AAES206	The Server Certificate will expire in 10 days	No	Yes	Minor
AAES207	The Server Certificate has expired	No	Yes	Major
AAES208	The AE Services Certificate will expire in 30 days	No	Yes	Minor
AAES209	The AE Services Certificate will expire in 10 days	No	Yes	Minor
AAES210	The AE Services Certificate has expired	No	Yes	Major
AAES211	The Web Server Certificate will expire in 30 days	No	Yes	Minor
AAES212	The Web Server Certificate will expire in 10 days	No	Yes	Minor
AAES213	The Web Server Certificate has expired	No	Yes	Major
AAES214	The LDAP Server Certificate will expire in 30 days	No	Yes	Minor
AAES215	The LDAP Server Certificate will expire in 10 days	No	Yes	Minor
AAES216	The LDAP Server Certificate has expired	No	Yes	Major
AAES217	OAM Login Failure	No	Yes	Minor
AAES218	Remote SSH Login Failure	No	Yes	Minor
AAES219	Local Console Login Failure	No	Yes	Major
AAES220	OAM Login Attempts Exceeded	No	Yes	Major
AAES221	SSH Login Attempts Exceeded	No	Yes	Major

Alarm Code	Alarm Message	INADS Trap	NMS Trap	Priority Level
AAES222	Local Console Login Attempts Exceeded	No	Yes	Major
AAES300	The AE Services license will expire in 30 days	No	Yes	Minor
AAES301	The AE Services license will expire in 10 days	No	Yes	Minor
AAES302	The AE Services license has expired	No	Yes	Minor
AAES303	DMCC entered 30 day grace period	No	Yes	Minor
AAES304	DMCC has 10 grace period days remaining	No	Yes	Minor
AAES305	DMCC entered restricted mode, 0 grace period days remain	No	Yes	Minor
AAES306	CVLAN entered 30 day grace period	No	Yes	Minor
AAES307	CVLAN has 10 grace period days remaining	No	Yes	Minor
AAES308	CVLAN entered restricted mode, 0 grace period days remain	No	Yes	Minor
AAES309	DLG entered 30 day grace period	No	Yes	Minor
AAES310	DLG has 10 grace period days remaining	No	Yes	Minor
AAES311	DLG entered restricted mode, 0 grace period days remain	No	Yes	Minor
AAES312	TSAPI entered 30 day grace period	No	Yes	Minor
AAES313	TSAPI has 10 grace period days remaining	No	Yes	Minor
AAES314	TSAPI entered restricted mode, 0 grace period days remain	No	Yes	Minor
ACORE00001	Disk: timed out getting disk status	Yes	Yes	Minor
ACORE00002	Disk: sda drive not ready	Yes	Yes	Minor
ACORE00003	Disk: reset timed out	Yes	Yes	Minor
ACORE00004	Disk: reset master error	Yes	Yes	Minor
ACORE00005	Disk: sda lost interrupt	Yes	Yes	Minor
ACORE00006	Disk: disk has failed	Yes	Yes	Minor
ACORE00007	Disk: status error	Yes	Yes	Minor
ACORE00008	Disk: disk usage exceeded 80%	Yes	Yes	Minor
ACORE00009	Disk: disk is full	Yes	Yes	Minor

Alarm Code	Alarm Message	INADS Trap	NMS Trap	Priority Level
ACORE00010	Disk: MBE detected	Yes	Yes	Minor
ACORE00021	CPU: CPU utilization exceeded 80%	Yes	Yes	Minor
ACORE00041	Security: There have been 3 unsuccessful login attempts. The account is locked out for 30 minutes	No	Yes	Minor
ACORE00043	Security: Linux login failure - access through illegal port (access denied)	No	Yes	Minor
ACORE00044	Security: a file has been modified illegally	No	Yes	Minor
ACORE00045	Security: a file has been removed illegally	No	Yes	Minor
ACORE00046	Security: a file has been added to the system in an illegal directory	No	Yes	Minor
ACORE00047	Security: tripwire failed to initialize the tripwire database	No	Yes	Minor
ACORE00070	Watchdog: Process is up	Yes	Yes	Minor
ACORE00071	Watchdog: Process is down	Yes	Yes	Minor
ACORE00072	Watchdog: Process is dead	Yes	Yes	Minor
ACORE00121	An upgrade has not been committed after 30 minutes of the last upgrade	Yes	Yes	Minor
ACORE00993	Link down (Network Interface(s))	Yes	Yes	Minor

Chapter 9: Certificate management

AE Services provides client connections over secure, encrypted links using Transport Layer Security (TLS). For secure communication to take place, AE Services and its clients rely on public key certificates. If you elect to use a secure link, you will need to use either the default certificate installed by AE Services or certificates issued by a trusted in-house or third-party certificate authority. The following clients and APIs can take advantage of secure links.

- AE Services Management Console
- TSAPI, JTAPI, DMCC, and the Telephony Web Service
- CVLAN
- System Management Service
- The AE Services Implementation for Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007

See the *Avaya Aura® Application Enablement Services Implementation Guide for Microsoft Live Communications Server 2005 or Microsoft Office Communications Server 2007*, 02-601893 for information about managing certificates in an AE Services and Microsoft Office Communications server environment.

- If your AE Services configuration includes an external directory server, you will need to validate the external directory server's certificate.



Note:

The Transport Service, which provides a secure link, does not use any of the certificates you administer in AE Services.

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. If you

are using the default certificate installed by AE Services, the trusted Certificate Authority (CA) is the Avaya Product Root CA.

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.

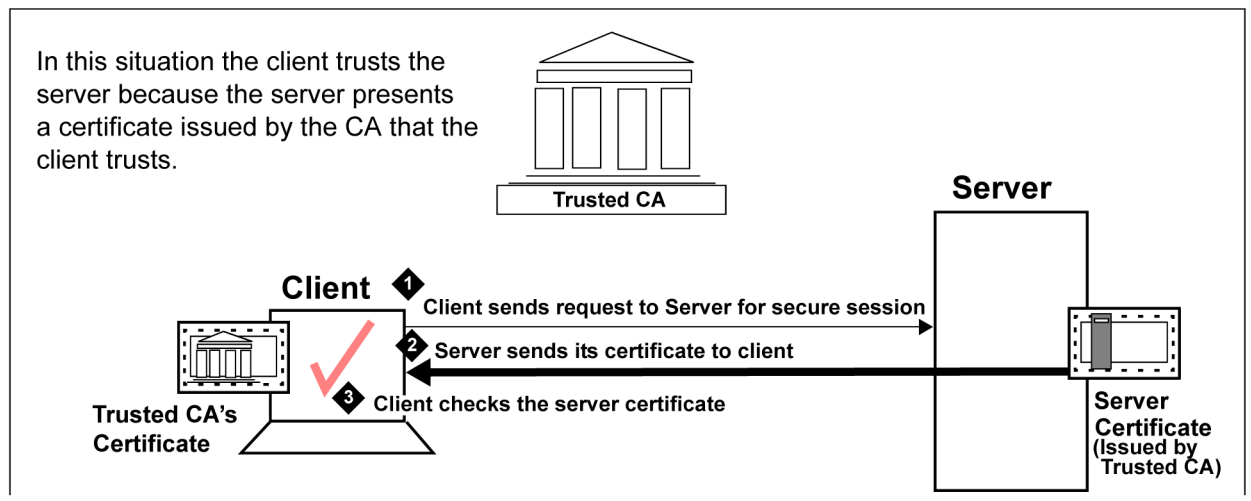


Figure 29: Server authentication

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.
 - c. If the common name in the client certificate matches the name of the client to which the server is connected. If the names do not match, the server can not trust the 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.

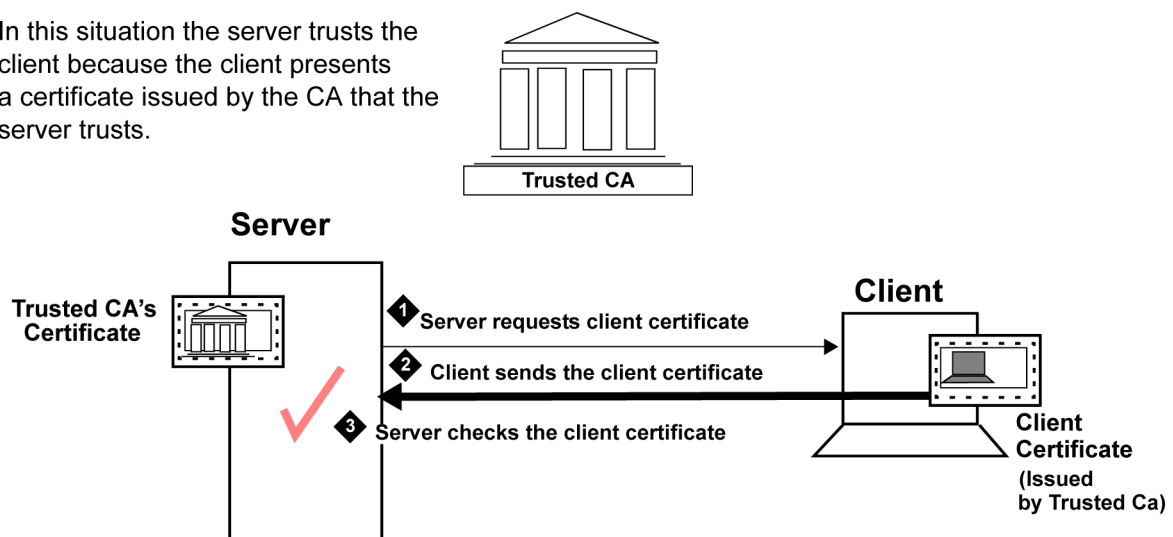


Figure 30: Client Authentication

The AE Services default certificate

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

The AE Services license file installs a default server certificate (serverCert.pem), which is signed by the Avaya Product Certificate Authority (CA). The default server certificate 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



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 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 separate, self-signed certificates, as follows:

- Tomcat - /usr/shared/tomcat5/conf/defaultkeystore
- Apache - /etc/httpd/conf/ssl.crt/Avaya.crt

If you use 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 with a way to manage these certificates.



Note:

If you are using the default certificates installed by AE Services, the AE Service Certificate Management Web pages do not apply

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 213.

Checklist for manual enrollment - server authentication


#	Description	Notes	✓
1	Install the Trusted CA's Certificate on client computer.	Browser - (not in the AE Services Management Console). The client user performs this procedure on the computer that the client is installed on.	
2	Create a server certificate request for AE Services	AE Services Management Console - See Creating a server certificate signing request for the AE Services server on page 220.	
3	Create an AE Services server certificate.	Browser - See Creating a server certificate for AE Services (generic procedure) on page 222.	
4	Import the server certificate into AE Services.	AE Services Management Console - See Importing the server certificate into AE Services on page 223.	

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 214.

Checklist for automatic enrollment using SCEP

#	Description	Notes	✓
1	Create a server certificate request (CSR) for AE Services	<p>You are submitting the Certificate Request (CSR) to the CA's SCEP Server for signing.</p> <ul style="list-style-type: none"> 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. 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). 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. <p> Note:</p> <p>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.</p> <p>See Creating a server certificate signing request for the AE Services server on page 220.</p>	
2	Create an AE Services server certificate.	Browser - See Creating a server certificate for AE Services (generic procedure) on page 222.	
3	Import the server certificate into AE Services.	AE Services Management Console - See Importing the server certificate into AE Services on page 223.	

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. For more information, see *Application Enablement Services Device, Media and Call Control API Java Programmers Guide*, 02-300359.

#	Description	Notes	✓
1	(Client) Install the Trusted CA's Certificate on client computer.	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.	
2	Create a server certificate request for AE Services	AE Services Management Console - See Creating a server certificate signing request for the AE Services server on page 220.	
3	Create an AE Services server certificate.	Browser - See Creating a server certificate for AE Services (generic procedure) on page 222.	
4	Import the server certificate into AE Services.	AE Services Management Console - See Importing the server certificate into AE Services on page 223.	

Checklist for installing your own certificates - client authentication

#	Description	Notes	✓
1	Install the Trusted CA's certificate on the AE server	AE Services Management Console. See the following topics: <ul style="list-style-type: none"> • Obtaining a trusted certificate for the AE Server on page 217 • Importing the trusted certificate into AE Services on page 218. 	
2	Install the client computer's certificate (the client certificate)	Client Desktop - Client user perform this procedure on the computer that the client is installed on.	
3	Add a trusted host. In the AE Services Management Console (Security > Host AA > Trusted Hosts > Add Trusted Host). Enable Authenticate Client Cert with Trusted Certs and Require Trusted Host Entry .	AE Services Management Console. Applies to a DMCC client that is using client authentication (see Client authentication on page 210). Not applicable to TSAPI, JTAPI, or CVLAN.	

Enabling client authentication for DMCC Java clients

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**).

-
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 216.
 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

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 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 134.

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

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.

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

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

Obtaining a trusted certificate for the AE Server

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

-
1. From your browser, go to your certificate authority's Web page 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\ae_trucert.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 58.
- [Importing the trusted certificate into AE Services](#) on page 218.

Importing the trusted certificate into AE Services

1. From the AE Services Management Console main menu, select **Security > Certificate Management > CA Trusted Certificates**.
2. From the **CA Trusted Certificates** page, select the certificate you want to import, and click **Import**.
3. Complete the **Trusted Certificate Import** page, as follows:
 - a. 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.

- b. For the **Certificate PEM**, you will need to provide an absolute path name for the CA Certificate file. Click **Browse**, and locate the CA's certificate file. After you have added the path name, click **Apply**.

If the import is successful, your browser displays the following message:
"Certificate Imported Successfully."

AE Services recommends that you verify the installation of the certificate. See [Verifying the installation of the trusted certificate in AE Services](#) on page 219.

Verifying the installation of the trusted certificate in AE Services

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

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

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.

1. From the AE Services Management Console main menu, select **Security > Certificate Management > Server Certificate**.
2. On the **Server Certificate** 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 **aeservices** for the CVLAN, DLG, DMCC and TSAPI certificates.
 - Select **web** for the Apache and Tomcat certificates.
 - Select **ldap** for the LDAP certificate.
 - Select **server** to include all certificates (aeservices, web, and ldap)
 - b. Leave the **Create Self-Signed Certificate** check box unchecked (the default).
 - c. In the **Encryption Algorithm** field, select **3DES**.
 - d. In the **Password** field, type the password of your choice.
 - e. In the **Key Size** field, accept the default **1024**.
 - f. In the **Certificate Validity** field, accept the default **1825**.
 - g. 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=Example corp,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`).

- h. In the **Challenge password** field, type the challenge password of your choice.
- i. (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
- j. (Optional) From the **Extended Key Usage** list, select the setting appropriate for your certificate.
- k. (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. With EJBCA 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.
- l. 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.

Creating a server certificate for AE Services (generic procedure)

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 the CA Web site.


-
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 AE Services server](#) on page 220.)
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 217 for more information.

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

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

-
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 AE Services server](#) on page 220.)
 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 into AE Services

Follow this procedure to import the AE Services server certificate into the AE Services Management Console. This procedure assumes that your certificate is in PEM format. If your certificate is in another format, see [File conversion for DER and PKCS#12 files](#) on page 216.

 **Note:**

Always install just the server certificate (as opposed to a PKCS7 certificate chain), but be sure to select **Establish Chain of Trust** as indicated in this procedure.

-
1. From the AE Services Management Console main menu, select **Security > Certificate Management > Server Certificates > Pending Requests**.
 2. From the **Server Certificates** page, click **Import**.
 3. Complete the **Server Certificate Import** page, as follows:
 - a. In the **Certificate Alias** field, select the appropriate certificate alias (aeservices, ldap, server, or web),
 - b. Accept the default for **Establish Chain of Trust** (by default the check box is selected).
 - c. Next to the **File Path** field, click **Browse** and locate the server certificate you want to import.
 - d. Click **Apply**.
-

Verifying the installation of the server certificate in AE Services

-
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 Server and the Web Server

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 96.

Backing up certificates

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.

To back up the AE Server data, which includes certificate files, see [Backing up server data](#) on page 89.

Restoring certificates

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

To restore the AE Server data, which includes certificate files, see [Restoring the server data](#) on page 89.

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 226.
- Submit the CSR to your certificate authority (CA). See [Renewing certificates – submitting the CSR to certificate authority \(Microsoft example\)](#) on page 226.
- Your certificate authority will process 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 217.


- Replace the old certificate with the new certificate. See [Renewing certificates – replacing the old certificate with the new certificate](#) on page 227.

Renewing certificates – creating the CSR

1. From the AE Services Management Console main menu, select **Security > 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)

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

-
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 226.)
 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

-
1. From the AE Services Management Console main menu, select **Security > 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**.
 4. From the **Server Certificate Renew** page, click **Browse**.

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**.
-

Chapter 10: 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 with IBM Sametime (the AE Services Integration with IBM Sametime uses From TelURI settings only; it does not use To TelURI settings.)
- AE Services Implementation with Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007 (AE Services Implementation for LCS/OCS)
- 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 245.

Dial plan administration - converting E.164 numbers and dial strings

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 231 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 231 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.

Format	Example
E.164	tel:+13031234567
E.164PlusExt	tel:+13031234567;ext=1234567
extOnly	tel:5389000;phone-context=<domain> where <domain> can be any organization's domain name tel:1234567;phone-context=example.com

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.

Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
11	11	1303538	4	(blank) ¹
11	11	1303	1	9
*	*	*	0	9011

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.

Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
7	7	538	0	1303
7	7	852	0	1732
10	10	*	0	1

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.

	Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
A	11	11	1303538	4	(blank) ¹
B	11	11	1732852	4	(blank)
C	11	11	1720444	4	(blank)
D	11	11	1303	1	9
E	11	11	1720	1	9
F	11	11	1	0	9

	Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
G	*	*	*	0	9011

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 232.

A	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.
B	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.
C	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.
D	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.
E	AE Services receives +17202891234,an 11-digit number. Because the number is within the minimum and maximum length requirements, and the first 4 digits (1720) are a pattern match, AE Services deletes the first digit (1),replaces it with a 9. The resulting number is 97202891234.
F	AE Services receives +18183891234, an 11-digit number. Because the number is within the minimum and maximum length requirements, and the first digit (1) is a pattern match, AE Services deletes no digits, and prepends a 9 to the number. The resulting number is 918183891234.
G	AE Services receives +4926892771234, a 13-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 and prepends 9011 to the number. The resulting number is 90114926892771234.

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.

	Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
A	7	7	538	0	1303
B	7	7	852	0	1732
C	7	7	444	0	1720
E	5	5	2	0	173285
F	5	5	4	0	172044
G	10	10	*	0	1

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 TelURI rules for fixed-length extensions](#) on page 234.

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 patternmatch, 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 patternmatch, AE Services deletes no digits, and prepends 1732 to the number. The resulting number is +17328521234.

C	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 patternmatch, AE Services deletes no digits, and prepends 1720 to the number. The resulting number is +17204441234.
D	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.
E	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 240). 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.
F	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 240). 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.
G	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.

	Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
A	8	11	49697100	7	(blank) ¹
B	8	11	49697101	7	(blank)
C	8	11	49697102	7	(blank)
D	8	11	49697103	7	(blank)
E	8	11	49697104	7	(blank)
F	8	11	49697105	7	(blank)
G	*	*	4969	4	0
H	*	*	49	2	00
I	9	9	46357	6	*8
J	*	*	*	0	000

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 - From TelURI rules for variable length extensions](#) on page 235.

A	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.
B	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.
C	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.
D	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.
E	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.
F	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.
G	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.
H	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.
I	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.
J	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.

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.

	Minimum Length	Maximum Length	Pattern Match	Delete Length	Replacement
A	1	4	*	0	4969710
B	*	*	00	2	(blank) ¹
C	*	*	0	1	49
D	*	*	*	0	4969

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 237.

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.
D	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.

	Min length	Max length	Pattern	Delete Length	Replacement
A			4969710([0-5]\\d{0,3})		\$1
B			4969(\\d{1,})		0\$1
C	*	*	49	2	00
C	*	*	*	1	000

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 239.

A	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).
B	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).
C	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.
D	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.

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 Office Communicator 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 241.
- You can administer default dial plan settings that are used for all switches. For more information, see [Administering default dial plan settings](#) on page 243.



Important:

In configurations with one AE Server supporting multiple switches, AE Services does not support Microsoft Office Communicator control of the same extension on more than one switch.

Administering dial plan settings on a per-switch basis

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 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 243. 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.

-
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 **aeslcswitch**, and click **Detail**.
 3. On the **Dial Plan Settings - Conversion Rules for aeslcswitch** page, in the **From TelURI** section, click **Add**.
 4. From the **Add Dial Plan - aeslcswitch** 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 15, 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 15, 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 15 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 aeslcs witch** page, in the **To TelURI** section, click **Add**.
6. From the **Add Dial Plan - aeslcs witch** 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 15, 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 15, 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 15 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).
- 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 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

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.

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:

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 15, 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 15, 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 15 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).
- 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 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:**

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 15, 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 15, 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 15 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).
- 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 LCS/OCS and Office Communication Server 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 handle the results of the conversion.

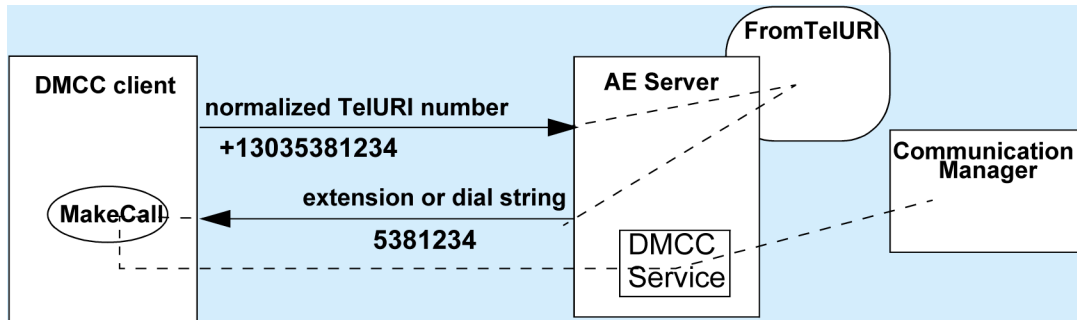
- To understand how the DMCC service uses the conversion rules, see [From TelURI and ToTelURI operations for the DMCC service](#) on page 245.
- To understand how the AE Services Implementation for Microsoft Live Communications Server and Office Communication Server uses the conversion rules, see [From TelURI and ToTelURI operations for the AE Services implementation for LCS/OCS](#) on page 247.

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 246 and [To TelURI operations for the DMCC service](#) on page 246.

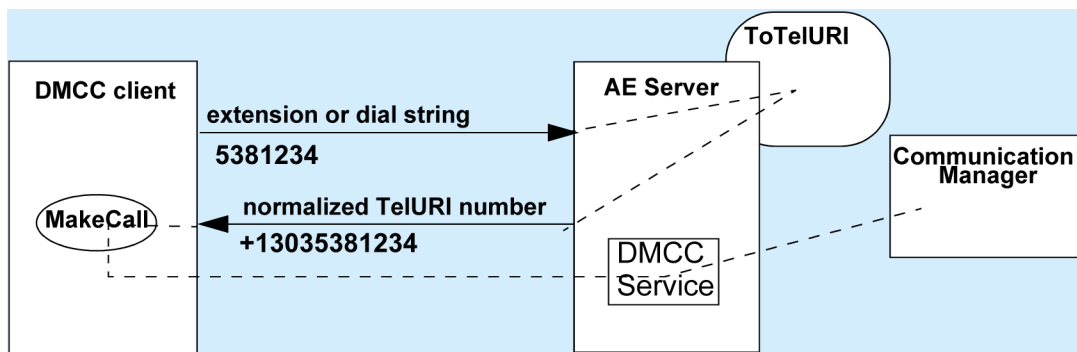
From TelURI operations for the DMCC service

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

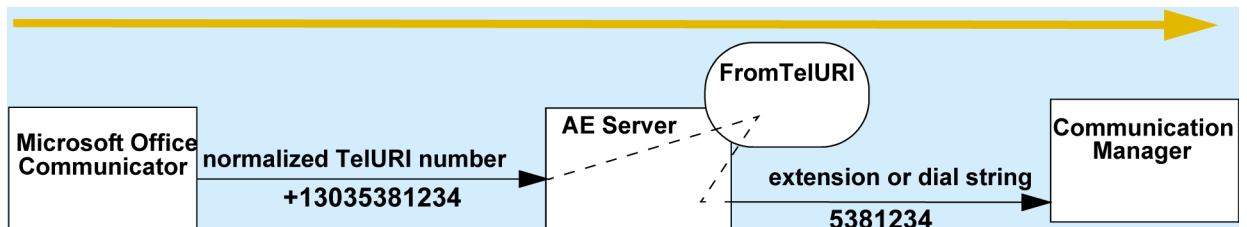
The DMCC application receives an event from Communication Manager, which includes an extension number. The DMCC application extracts the extension number and submits it to the E164 Conversion Service. The E164 Conversion Service converts the extension into a TelURI number. The application extracts the 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

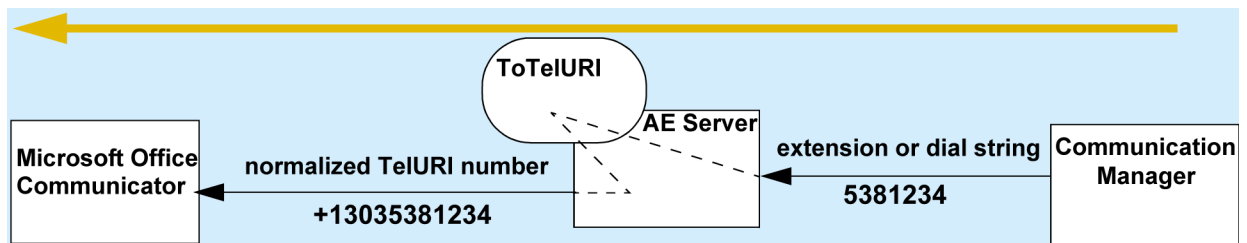
From TelURI operation for the AE Services implementation for LCS/OCS

For the AE Services implementation for LCS, From TelURI settings are used to convert normalized TelURI numbers, arriving from the Microsoft Office 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

For the AE Services implementation for LCS/OCS, 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.



Creating a backup of the dial plan

Use this procedure to export the dial plan to a backup file (comma separated values format).

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

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.

-
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 11: 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 249.

- 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

By default, AE Services assigns ports 4101 to 4116 for SMS proxy ports. If you need to change these settings follow this 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

-
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**.
 3. Complete the **SMS Configuration** 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 **OSSI3**, 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:
 - OSSI3 (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.
 - OSSI3. Exactly the same as OSSI3 except extension numbers do not contain punctuation.

Configuring TWS settings

-
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 > TWS**.
 3. Click **TWS Properties**.
 4. In the Session Timeout box, enter the appropriate value.
 5. When finished, click **Apply Changes**.
-

Appendix A: Locations 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 0 to 19)
- `dmcc-error.log.xx` (where `xx` is a number from 0 to 19)
- `dmcc-trace.log.xx` (where `xx` is a number from 0 to 19)
- `dmcc-wrapper.log.x` (where `x` is a number from 1 to 4. The first wrapper log, `mvap-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 `/var/log/avaya/aes`, as follows:

- Security (client) log (`sec.yyyymmdd`, for example `sec.20050622`)
- Error log (`log.yyyymmdd`, for example `log.20050622`)
- Command log (`cmd.yyyymmdd`, for example `cmd.20050622`)
- 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.yyyymmdd`, for example `sec.20050622`)
- Error log (`log.yyyymmdd`, for example `log.20050622`)
- Command log (`cmd.yyyymmdd`, for example `cmd.20050622`)
- 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.yyyymmdd`, for example `sec.20050622`)
- Error log (`log.yyyymmdd`, for example `log.20050622`)
- Command log (`cmd.yyyymmdd`, for example `cmd.20050622`)
- Reset log (`reset.log`)
- Trace log (`/var/log/avaya/aes/common/trace.out`)
- G3trace logs are located in `/var/log/avaya/aes/TSAPI`. This directory includes `g3trace-switchname-n.trace.out`, `csta_trace.n.out`, and `audit_trace` (where *switchname* is the name of your switch and *n* is a number).
- 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.

User Web Service

All logs are in `/var/log/avaya/aes/tomcat` , as follows:

- `ws_cus.log`
- `ws_cus_authentication.log`
- `ws_cus_cmd.log`
- `ws_cusdistributor_sdbdistributor.log`

Appendix B: Upgrading System Platform

Upgrading System Platform

Upgrading System Platform

1. Log in to System Platform Web Console.
2. Click **Server Management > Platform Upgrade**.
3. In the **Upgrade Platform From** field, select a location from where to download the System Platform image files for the platform upgrade. Options are:
 - **Avaya Downloads (PLDS)**
 - **HTTP**
 - **SP Server**
 - **SP CD/DVD**
 - **SP USB Device**
4. If you selected **HTTP** or **SP Server** in the **Upgrade Platform From** field, enter the platform upgrade URL.
5. Click **Search**.
The system searches for an upgrade description file that has an .ovf extension.
6. Select the appropriate description file for the platform upgrade, and then click **Select**.
The system displays the version and additional information for the current and the new platform (System Domain (Domain-0) or Console Domain, or both) on the Platform Upgrade Details page.
7. On the Platform Upgrade Details page, click **Upgrade**.

 **Important:**

As part of the upgrade process, the System Domain (Domain-0) and Console Domain are rebooted, and as a result, all other virtual machines will be rebooted. During the platform upgrade process, all operations on the System Platform Web Console are blocked and all links (including menu items) are disabled until the

system is booted up into the new platform for you to commit or rollback the upgrade.

8. Click **OK** in the dialog box that appears to confirm that the template has been qualified for the platform version to which you are upgrading and that both System Platform Web Console and Console Domain will reboot on completing the upgrade .
9. Click **OK** in the dialog box prompting you to confirm the upgrade.
At this stage, the upgrade process starts and the system displays the Platform Upgrade workflow status page.

 **Note:**

The System Domain (Domain-0) and Console Domain are rebooted at this stage. So the Platform Upgrade workflow status page does not show any updates until it reboots in the new Console Domain. After the Web Console is up, the system automatically redirects you to the login page. This can take approximately 20 minutes.

10. Log in to the System Platform Web Console.
At this stage, you can view the time remaining for Auto Rollback of the platform upgrade on the Commit or Rollback platform upgrade page. You can also check the Web Console to make sure that the upgrade process is running alright.
11. On the Commit or Rollback platform upgrade page, do one of the following:
 - Click **Commit** to continue the upgrade process by committing to the newly upgraded platform. See [Committing an upgrade](#) on page 260

 **Note:**

You are allowed a 4-hour period to log in to the System Platform Web Console. If you do not login during this period, the system will reboot using the previous release of System Platform. If a user logs in to System Platform Web Console within the 4-hour period, it is assumed that System Platform is reachable and the timer is cancelled. However, you still need to verify and commit the upgrade.

- Click **Rollback** to cancel the upgrade process and go back to the previous version of the software. See [Rolling back an upgrade](#) on page 260.

Commit and Rollback

System Platform upgrades should be committed before performing other operations. During an upgrade, after the system boots in the new platform release, the user is required to commit or rollback the upgrade. While the system is waiting for the user to either commit or rollback, Avaya advises not to perform any of the following operations:

- Delete a template
- Install a template
- Upgrade a template
- Reboot the System Platform Web Console

**Note:**

Rebooting System Platform Web Console before committing will roll back the system back to the previous release.

- Start High Availability Failover

**Note:**

System Platform does not prevent you from performing the above operations prior to selecting commit or rollback.

If you perform the above operations, the operations will actually take effect on the system. Thereafter, if rollback is performed, the new changes will be visible in the rolled back system. Committing an upgrade is unaffected by the changes made prior to committing the upgrade. If the template-related operations are performed and you want to recover after committing or rolling back the upgrade, you need to manually rollback the changes through System Platform Web Console. The upgrade rollback operation will not be able to roll the system back. A commit of the upgrade, on the other hand, is unaffected by the changes that you make prior to committing the System Platform upgrade.

Commit

You can execute a commit operation when you are satisfied that the new System Platform software is working without any issues. After executing a commit operation, you cannot go back to the older version of the System Platform software. If you do not log in to System Platform Web Console within 4 hours after the upgrade, the system performs an automatic rollback.

The system performs the following when you commit an upgrade:

- Disables the four hour timer that automatically performs a rollback.
- Performs a clean up operation (such as, removing state files and so on).
- Commits boot loader (grub) to boot up into the new platform from now on.
- Marks the Workflow as complete and indicates that on the Platform Upgrade Status page.

Rollback

You can execute a rollback operation if you find any errors or issues with the new System Platform software and want to go back to the older version of the software. Rollback can reboot the server.

The system performs the following when you roll back an upgrade:

- Disables the four hour timer that automatically performs a rollback.
- Commits boot loader (grub) to boot up into the old platform.
- Performs a clean up operation (such as, removing state files and so on).
- Prepares the system to notify the user of the reason for rollback after rebooting into the old platform.
- Reboots the platform to boot up into the old platform and restores access to System Platform Web Console.

Committing an upgrade

On the Commit or Rollback platform upgrade page, click **Commit** to continue the platform upgrade process.

Rolling back an upgrade

On the Commit or Rollback platform upgrade page, click **Rollback** to cancel the upgrade process and go back to the previous version of the software.



Note:



After a rollback, when you log on to the System Platform Web Console, the system displays the Rollback Acknowledge page that specifies the reason for rollback (either user initiated rollback or deadmans switch) based Auto rollback; or if the upgrade failed and the system rebooted to an older version of System Platform as part of fail-safe fallback mechanism.

Platform Upgrade field descriptions

Name	Description
Upgrade Location	Lets you specify the location from where to download or upload the template image files for the platform upgrade.

Name	Description
	<p>Options are:</p> <ul style="list-style-type: none"> • Avaya Downloads (PLDS) The files are located in the Avaya Product Licensing and Delivery System (PLDS) Web site. You must enter an Avaya SSO login and password. • HTTP The files are located on an HTTP server. You must specify the URL of the platform upgrade if you select this option. • SP Server The platform upgrade files are located in the <code>/vsp-template</code> directory in the System Platform Console Domain. You will need to copy the platform upgrade files in this directory using a file transfer program and change their permissions as follows: <code>chmod 644 <files-copied></code> • SP CD/DVD The files are located in a CD or DVD. • SP USB Device The files are located in a USB flash drive.

Button descriptions

Button	Description
Search	<p>Searches for a template description file that has an .ovf (Open Virtualization Format) extension at the location that you specify. Opens the Platform Upgrade Details page with the search results.</p> <p> Note: Open virtualization format (OVF) is an open standard for packaging and distributing software that runs on virtual machines.</p>
Select	Selects the required template description file.
Upgrade	Upgrades the system with the template description file.
Commit	<p>Commits an upgrade operation and upgrades the System Platform software to the latest version.</p> <p> Note: After executing a commit operation, you cannot go back to the older version of the System Platform software. If you do not execute a commit operation within 4 hours after the upgrade, the system performs an automatic rollback.</p>
Rollback	Cancels an upgrade operation, and the system goes back to the previous version of System Platform software.
Acknowledge	Lets you confirm the reason for the rollback operation.

Appendix C: AE Services network interfaces

Network interface configurations

The AE Services Bundled Server offer provide provides a hardware platform with four network interfaces (NICs): eth0, eth1, eth2, and eth3. For these offers, AE Services reserves eth1 for AE Services technicians (for on-site use).

You can configure the AE Server to use a single NIC configuration or a dual NIC configuration. Use the configuration that best suits your network topology and other characteristics of your network.



Note:

For information about network interface configurations for Application Enablement Services on System Platform, see *Implementing Avaya Aura® Application Enablement Services on Avaya Aura® System Platform*, 02-603468.

Single NIC configurations

In a single NIC configuration, you use one network interface. That is, the AE Server uses one NIC for client, switch and media connectivity.

In a single NIC configuration, the AE 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 Service 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 Server 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 most S8300, S8400, and S8500c 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.

Dual NIC configurations

In a dual NIC configuration, you use two network interfaces for connectivity to two separate network segments. If your hardware platform has four network interfaces, you can choose two of the three available network interfaces (eth0, eth2, or eth3; eth1 is reserved for technicians).

In a dual NIC configuration, you use one network segment for the AE Server and Communication Manager and another network segment for client and media connectivity (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 a dual NIC configuration for S8400, S8500c, S8700 Communication Manager media servers.

Network interface (NIC) settings

The NIC settings choices for eth0 and eth1 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 265 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 (optional)

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 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).

-
1. From the AE Services Management Console main menu, select **Networking > Network Configure**.
 2. From the Network Configure page, edit any of the settings that you need 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 Server will not reset any of the values.

Appendix D: TCP ports and firewall settings on the AE 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 Server. For information about security guidelines for the AE 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 the AE Services Bundled Server, a firewall is automatically configured and enabled by default.

Name				Description
CVLAN Ports	Unencrypted TCP Port	9999	Enabled/Disabled	The port number assignment for unencrypted (nonsecure) connections with CVLAN clients. This port assignment is enabled by default. You can enable and disable this port independently of the encrypted CVLAN port. When you enable or disable a CVLAN port, it does not affect CVLAN sessions that are already open.
	Encrypted TCP Port	9998	Enabled/Disabled	The port number assignment for encrypted (secure) connections with CVLAN clients. This port assignment is enabled by default. You can enable and disable this port independently of the unencrypted CVLAN port. When you enable or disable a CVLAN port, it does not affect CVLAN sessions that are already open.
DLG Port	TCP Port	5678	The DLG Service uses port 5678 for communication with clients. This is a fixed port number assignment.	

Name				Description
TSAPI Ports	TSAPI Service Port Note: If you disable Port 450, you must restart the TSAPI Service for the change to take effect.	450	Enable/Disable	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: <ul style="list-style-type: none"> • CSTA TLINK Ports for Non-Secured Clients • CSTA TLINK Ports for Secured Clients
	Local TLINK Ports	TCP Port Min	Reserved, port 1024	
		TCP Port Max	Reserved, port 1039	
	Unencrypted TLINK Ports. Note: You must restart the TSAPI Service for changes to the Tlink port assignments to take effect.	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 Administering TSAPI links on page 86.	
		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 Administering TSAPI links on page 86.	
	Encrypted TLINK Ports Note: You must restart the TSAPI Service for changes to the Tlink port assignments to take effect.	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 Administering TSAPI links on page 86.	
		TCP Port Max	The default minimum setting is 1081. 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 Administering TSAPI links on page 86. You must restart the TSAPI Service for changes to the Tlink port assignments to take effect.	
	DMCC Server Ports	Unencrypted Port	4721	Enabled/Disabled
				The DMCC Service uses port 4721 for unencrypted communication. By default the Unencrypted Port is disabled. It is

Name				Description
Note: If any of these 3 ports are enabled or disabled the DMCC service must be restarted.				provided for backward compatibility with applications that were developed prior to AE Services 3.1.
	Encrypted Port	4722	Enabled/Disabled	<p>The DMCC Service uses port 4722 for secure communication.</p> <ul style="list-style-type: none"> • 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	<p>The AE Server uses port 4723 for the AE Services implementation for Microsoft Live Communications Server. By default this port is disabled.</p> <p>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 24999. The DMCC Service uses this port for signaling.		
	Local UDP Port Min	The default minimum setting is 30000. The DMCC Service uses this port for Registration Administration and Status (RAS).		
	Local UDP Port Max	The default maximum setting is 34999. The DMCC Service uses this port for RAS.		
	RTP Local UDP Port Min	The default minimum setting is 40000. 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.		
SMS Proxy Ports	Proxy Port Min	<p>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.</p> <p>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.</p>		
	Proxy Port Max	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.		

TCP ports and firewall settings on the AE Server

Name		Description
		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.

Appendix E: AE Services Management Console connectivity tests

Use the following diagnostic utilities in AE Services Management Console to check connectivity:

- **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**)
- **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 and Microsoft Office Communications Server 2007. (**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.

Appendix F: AE Services administrative user accounts

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). All roles, except User Management, are mapped to Linux accounts.

Role	Linux group	AE Services Management Console access
System_Administrator	susers	<p>Read and write access to the following menus:</p> <ul style="list-style-type: none">• AE Services• Communication Manager Interface• Licensing• Maintenance• Networking• Security (the System_Administrator does not have access to Account Management, PAM, and Tripwire Properties)• Status• Utilities• Help <p> Note: The System_Administrator role does not have access to User Management.</p>

Role	Linux group	AE Services Management Console access
Security_Administrator	securityadmin	<p>Read and write access to the following menus in the AE Services Management Console:</p> <ul style="list-style-type: none"> • Security (the Security_Administrator does not have access to Enterprise Directory, Host AA, and Standard Reserved Ports) • Status • Help
Administrative role for User Management	Not associated with Linux.	<p>The default name for this account is avaya</p> <p>Read and write access to the following menus:</p> <p>User Management</p> <p> Note:</p> <p>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.</p>
Auditor	users	<p>Limited, read-only access to the following menus:</p> <ul style="list-style-type: none"> • Security — access is limited to: <ul style="list-style-type: none"> - Audit - Certificate Management - Security Database > CTI Users • Status <ul style="list-style-type: none"> - Alarm Viewer - Logs -- access is limited to: <ul style="list-style-type: none"> • Audit Logs • Error Logs • Install Logs • User Management Service Logs • Status > Status and Control — access is limited to: <ul style="list-style-type: none"> - CVLAN Service Summary - DLG Service Summary - DMCC Service Summary - Switch Conn Summary

Role	Linux group	AE Services Management Console access
		<ul style="list-style-type: none"> - TSAPI Service Summary • Help
Backup_Restore	backuprestore	Limited, read and write access to the following to the following menus: <ul style="list-style-type: none"> • Maintenance — access is limited to: <ul style="list-style-type: none"> - Server Data > Backup - Server Data > Restore • Help
Avaya_Maintenance	avayamaint	Limited, read and write access to the following menus in the AE Services Management Console: <ul style="list-style-type: none"> • Maintenance <ul style="list-style-type: none"> - Security Database - Service Controller - Server Data • Status <ul style="list-style-type: none"> Logs • Utilities <ul style="list-style-type: none"> Diagnostics • Help

Default accounts and AE Services Management Console access privileges



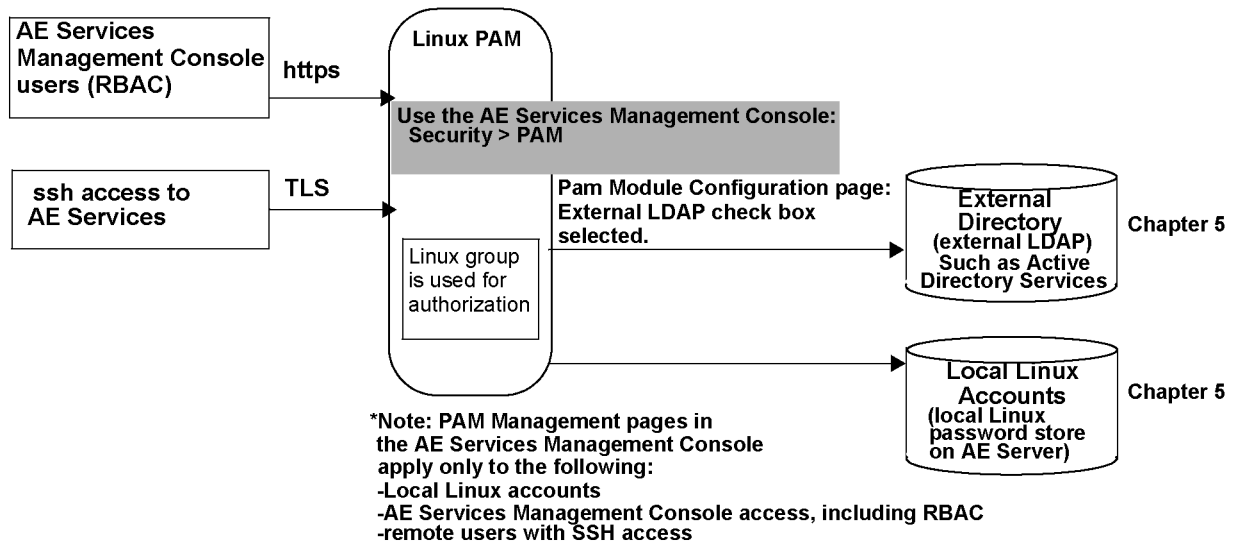
Security alert:

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 User Management](#).

Account name (log-in identifier)	Password	AE Services Management Console access privileges
craft (Avaya services account)	For service technicians only	Read and write access to the following menus: <ul style="list-style-type: none"> • AE Services • Communication Manager Interface

Account name (log-in identifier)	Password	AE Services Management Console access privileges
		<ul style="list-style-type: none"> • Licensing (you have access to this menu, but you must set up a separate WebLM password) • 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)
cust (customer account)	custpw	<p>Read and write access to the following menus:</p> <ul style="list-style-type: none"> • AE Services • Communication Manager Interface • Licensing (you have access to this menu, but you must set up a separate WebLM password) • Maintenance • Networking • Security (AE Services sets up the craft account with access to Security) • Status • User Management (AE Services sets up the craft account with access to Security) • Utilities
avaya (customer account)	avayapassword	<p>Read and write access to the User Management menu only</p>

Authenticating and authorizing administrators for AE Services Management Console and ssh access



Default AE Services accounts

Account name (log-in identifier)	Linux Group	Password	Access privileges
craft Available on: <ul style="list-style-type: none"> • AE Services Bundled Server • AE Services Software- Only Server only if you installed the Avaya Services package (cs-service) 	root	Contact your Avaya Business Partner or Business Partner representative.	Intended for Avaya services technicians. Provides local or remote access to the Linux shell. <ul style="list-style-type: none"> • 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)

Account name (log-in identifier)	Linux Group	Password	Access privileges
cust Available on: <ul style="list-style-type: none"> • AE Services Bundled Server • AE Services Software-Only Server only if you installed the Avaya Services package (cs-service) 	root	Contact your Avaya Business Partner or Business Partner representative.	Intended for customers. Provides local or remote access to the Linux shell. <ul style="list-style-type: none"> • Local - Log in from a local console as craft, and then access the root account (su - root) • Remote - Log in from a remote console with a secure shell client (ssh), as craft, and then access the root account (su - root)
avaya Available on: <ul style="list-style-type: none"> • AE Services Bundled Server • AE Services Software-Only Server only if you installed the Avaya Services package (cs-service) 	Not applicable	Contact your Avaya Business Partner or Business Partner representative.	User Management administration only. You do not have access to any other administrative menus.

Accounts installed with the Avaya Services package

When you install the Avaya Services package (cs-services), the installation program sets up the AE 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 281.

The avaya account (User Management administrator)

When you install the Avaya Services package (cs-services), the installation program sets up the AE 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 283.

The cust accounts (Linux and User Management)

When you install the Avaya Services package (cs-services), the installation program sets up the AE 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 280 and [Changing the default password for the cust account in User Management](#) on page 284.

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 273.
- 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 Server with the craft account by default. The craft account is equivalent to the cust account. See [Accounts for Avaya Services technicians](#) on page 171.

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

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](#) on page 286.

-
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](#) on page 278.
 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**.
-

Creating a new System Administrator account

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.

-
1. From your browser, log in to the AE Services Management Console as cust.
See [Accounts installed with the Avaya Services package](#) on page 278.
 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 273.

- 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)

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).

-
1. Log in to the AE 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 273.

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)

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 285.

-
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 278.
 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 282.

- 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

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 281.

-
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 278.
 2. From the main menu, select **User Management > List All Users**.
 3. From the **List All Users** page, select the option button for **craft** 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

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).

-
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`.
 - f. Click **Apply**.
 4. Log out of the AE Services Management Console (you are logging out as avaya).
 5. Log in to the AE Services Management Console again with the user identifier and password you created in Step 3 (`aesuseradmin`, based on this example).
 6. From the main menu, select **User Management > List All Users**.
 7. From the **List All Users** page, select the option button next to **avaya**, and click **Delete**.
 8. From the **Delete User** page, click **Delete**.
-

Creating a new System Administrator account and removing the default cust account from User Management

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.

-
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**.
-

Appendix G: Sample Device, Media, and Call Control applications

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, the Tutorial, in order 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 AES server/Communication Manager connectivity by running the tutorial application, you optionally can run the additional sample applications from a client application computer.



Note:

You can run the tutorial application directly on the AE Services server or on another computer. 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.

Sample application files on the AES 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/README.txt
```

Preparing to run the sample application

1. Administer AE Services. See [Administering AE Services for the sample application](#) on page 288.
2. Administer Communication Manager. See [Administering Communication Manager for the sample application](#) on page 289.



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 289.

Administering AE Services for the sample application

1. From the AE Services Management Console, select **AE Services > DMCC > Media Properties**.
2. On the **Media Properties** page, in the **Player Directory** field and the **Recorder Directory** field, type `/tmp`.
(/tmp is the default directory.)
3. Accept the defaults for the remaining fields, and click **Apply Changes**.
4. 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 AES server](#) on page 287.

Administering Communication Manager for the sample application

-
1. Administer a station to use with the application. See [Administering a station](#) on page 289.
 2. Administer out-of-band digit detection, if needed.
 3. Configure the network region and gateway, if not already configured. See [Administering network region and gateway](#) on page 289.
-

Administering a station

Use the Communication Manager `add station` command to add a station. For instructions on adding a station, see [Administering an extension exclusively for the DMCC softphone](#) on page 33 and [Adding stations](#) on page 44.

Administering network region and gateway

You must configure the network region and gateway, if these elements are not already configured. For more information, see [Administering a network region](#) on page 48 and [Adding a media gateway](#) on page 50.

Editing the tutorial properties file

Before you can run the sample application, you must edit the tutorial properties file (tutorial.properties) to provide information specific to your configuration.

1. Using the text editor of your choice, open tutorial.properties:

```
/opt/mvap/cmapl/cmapijava-sdk/examples/resources/
tutorial.properties
```

In Release 4.1, 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
cmapil.server_ip=nnn.nnn.nnn.nnn
cmapil.username=username
cmapil.password=password
cmapil.server_port=4722
# Legal values for cmapil.secure are true and false.
cmapil.secure=true
#cmapil.trust_store_location=sdh/build/mvshd/cmapijava-sdk/examples/
resources/avaya.jks
#if you do not know cmapil.trust_store_password, leave it default
#cmapil.trust_store_password=nnnn
#cmapil.key_store_location=nnnn.jks
#cmapil.key_store_password=nnnn
#cmapil.certificate_validation=true
#pattern xxx-yyy,ppp-qqq,rrr-sss....
#extensions=41400-41599,50001-50200,51000-51060
# by default getButtonInfo value is 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 S8300, S8400, S85xx, S87xx, and S88xx systems that use a Processor Ethernet (procr) this is the IP address of the media server.
 - For DEFINITY Server Csi systems and Communication Manager S8400, S85xx, S87xx, and S88xx 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.
See [Administering a station](#) on page 289.
 - c. For **password**, type the security code you administered for that station.
3. Add a **user_id** and **user_password** for the `cmapil.username` and `cmapil.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. Uncomment the last line about the `cmapi.trust_store_location` because you are using Port 4722.
 5. Save and close the tutorial.properties file.
-

Running the sample application

 **Note:**

The AE Services server must be running before you can run an application.

1. **ssh** into the AE Services server.
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 **Ant** on the tutorial application:

```
./ant.sh runTutorial
```

The application starts running. This application acts as a softphone and waits for calls. When the extension is called from any other phone, it answers with a recorded greeting that prompts you to record a message.

4. Experiment with this application:
 - 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. For this location, see [Administering AE Services for the sample application](#) on page 288.

Troubleshooting the sample application

If the application does not run as expected:

1. View the log files on the AE Services server.

Starting with AE Services Release 4.1, the log files reside in `/var/log/avaya/aes`:

- `mvap-error.log.x`
- `mvap-api.log.x`
- `mvap-trace.log.x`
- `mvap-wrapper.log`

When checking for exceptions, AE Services recommends that you use the `mvap-error.log.0` file. The `.0` file is the latest log file.

2. See [Table 20: Troubleshooting error messages for the sample application](#) on page 292 for help resolving the application error messages.

Table 20: Troubleshooting error messages for the sample application

Application error message	Troubleshooting procedure
Registration failed because Gatekeeper Reject reason: terminalExcluded	Verify that the extension number in <code>tutorial.properties</code> corresponds to a correctly administered extension number in Communication Manager.
Registration failed because Gatekeeper Reject reason: securityDenial	Verify that the password in <code>tutorial.properties</code> matches the password administered in Communication Manager for the station.
Registration failed because Protocol Timeout: reason: GRQ timer, tried 3 times	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.
Connection refused	<ul style="list-style-type: none"> • Verify that the IP address of the AE Services server is correct in the <code>tutorial.properties</code> file. • 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. • 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 <code>localhost</code> line.

For more information about creating and deploying Device, Media, and Call Control applications for AE Services, see:

- *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 Java Programmer's Reference* (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)
- *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 XML Programmer 's Reference* (an HTML document available on the Web only at the Avaya Support Site or Avaya DevConnect Site)

Appendix H: 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

Follow this procedure to migrate your Avaya Computer Telephony SDB to AE Services. This is a one-time only procedure that you run when you are ready to migrate all members. See [Importing the Avaya Computer Telephony SDB to the AE Services SDB](#) on page 297 for an illustration of the procedure.

-
1. From your Avaya Computer Telephony administrative workstation, use TSA 32 to create a flat file from the Avaya Computer Telephony SDB, as follows: Select **Admin > Bulk Admin > Create Flat file from SDB**.
 2. From the AE Services Management Console main menu, select **Maintenance > Security Database > Import**.
 3. From the **Import SDB** page, click **Browse**.
 4. Browse to the location of your Avaya Computer Telephony SDB backup file, and select **Open**.
 5. Click **Import**.

AE Services does the following:

- It updates the AE Services User Management database with your users (in effect, it adds your users with the **CT User** flag set to **yes**).
- It updates the SDB with the permission settings for worktops, devices, device groups, and Tlink groups. It does not, however, import user passwords and Tlinks.



Note:

Because Tlinks are not imported, the Tlink Groups are empty. Continue with this procedure to administer them in AE Services.

6. From AE Services Management Console main menu, select **Security Database > Tlink Groups**.
 7. From the **Tlink Groups** page, select a Tlink Group, and click **Edit Tlink Group**.
 8. From the **Add/Edit Tlink Group** page, select the Tlinks that you want to add to the Tlink Group, and click **Apply Changes**.
 9. From the **Apply Changes to Tlink Group properties** page, click **Apply**.
-

Importing the Avaya Computer Telephony SDB to the AE Services SDB

image missing, wrong image was in this file.

INSERT IMAGE

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 102.

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 160.

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 102.

 **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

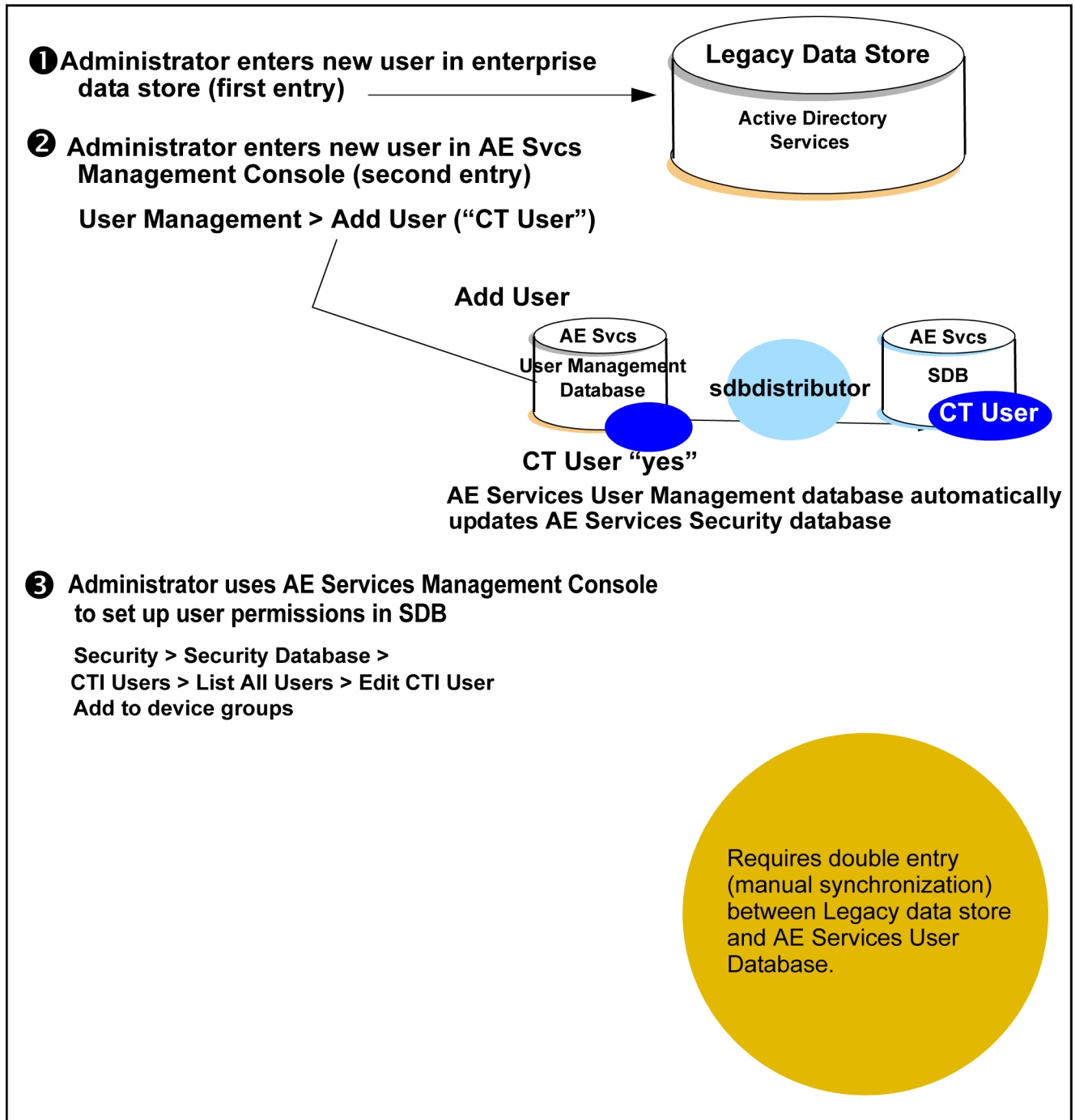
Bronze level integration is the lowest level of integration. Essentially it requires manually maintaining two sets of the same data.

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 299.

- 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



Avaya Computer Telephony silver level integration

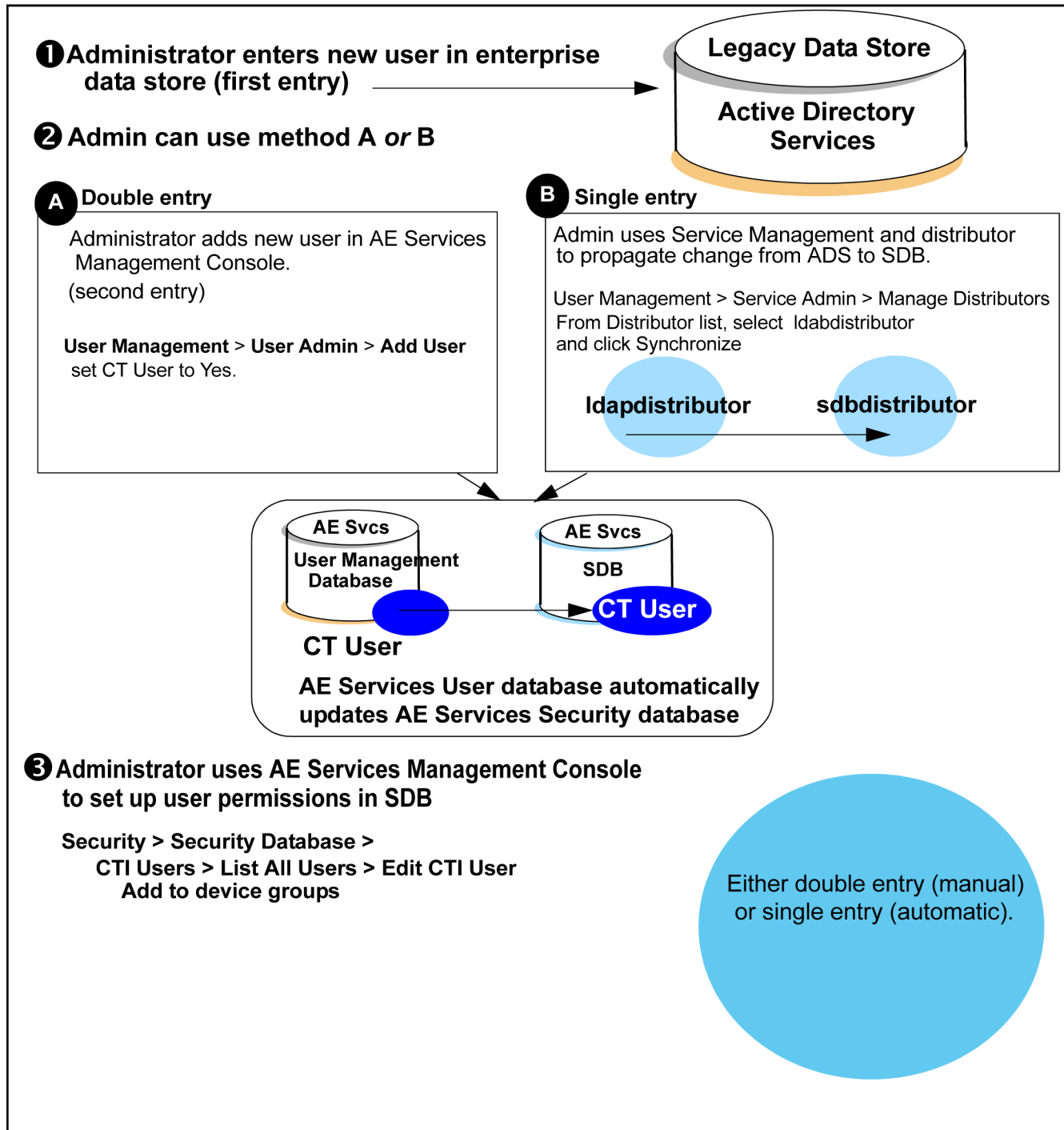
Silver level integration represents a tighter coupling between your enterprise database (Windows Active Directory Services) and AE Services User Management database.

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 301.

- 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



Avaya Computer Telephony gold level integration

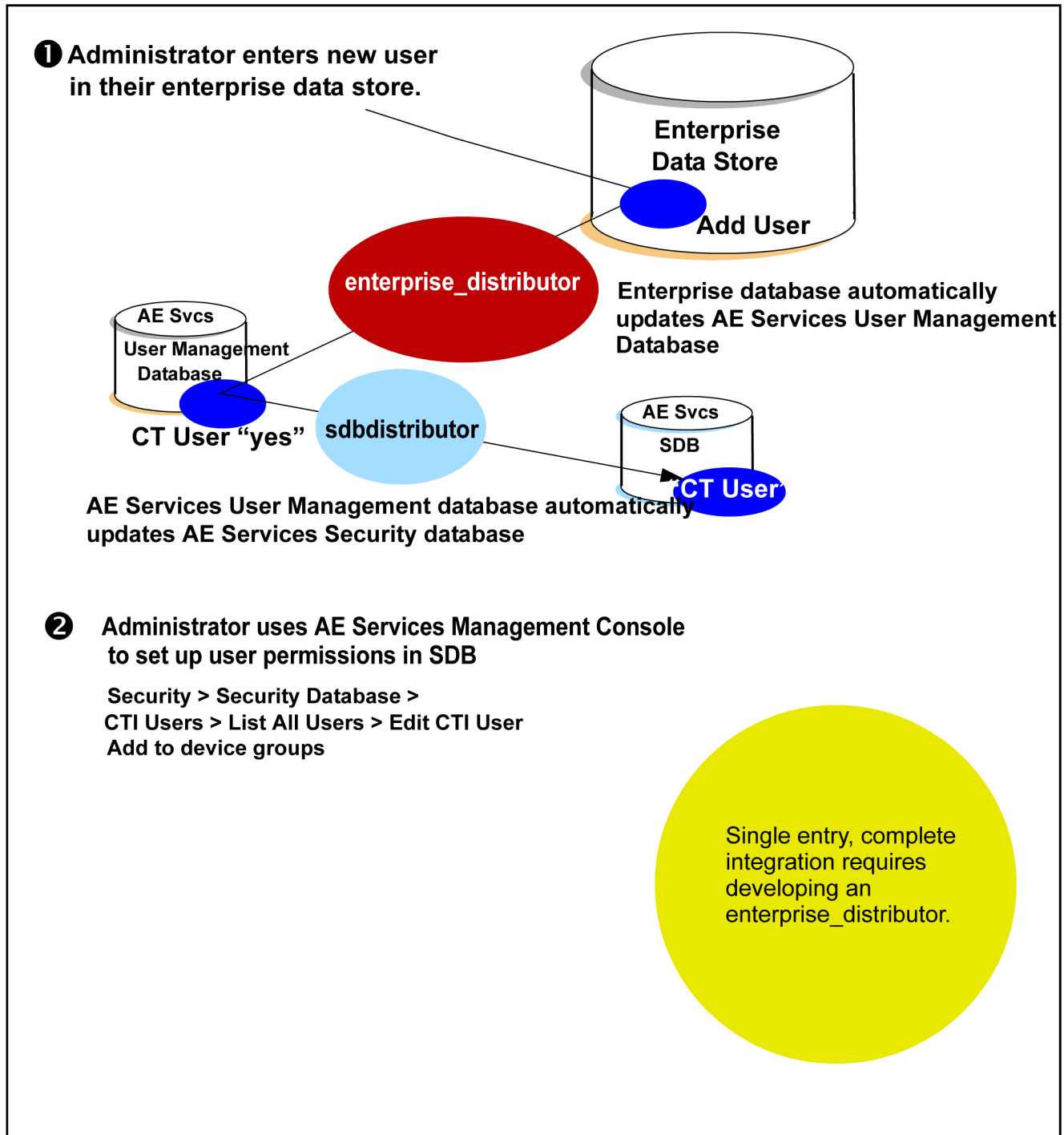
Gold level integration means complete integration between your enterprise database, and AE Services. A single entry in your enterprise database automatically results in an entry in the AE Services SDB. Gold level integration, however, does require that you develop a solution. In effect you develop your 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 303.

- 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



Migrating CVLAN to AE Services

Migrating CVLAN Server for Linux (Releases 9.0 and 9.1) to AE Services

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 9.1 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.

-
1. Obtain the CVLAN settings on Communication Manager.
See [Obtaining the CVLAN settings from Communication Manager](#) on page 304.
 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 305.
 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 305.
-

Obtaining the CVLAN settings from Communication Manager

On Communication Manager, follow these steps to obtain the settings for the CTI link number and corresponding client link number for CVLAN.

-
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 the AE Services Management Console when you administer the CVLAN Service. (See [Administering the CVLAN Settings on the AE Server](#) on page 305.)

Obtaining the CVLAN settings from the CVLAN R9.0 or R9.1 Server for Linux

On the CVLAN Server (R9.0 or R9.1), follow these steps to obtain the name or IP address of each CVLAN client.

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 Server

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.

1. Administer the NICs. See [Administering the Local IP for a single NIC configuration](#) on page 73.
 2. Administer the switch connections. See [Adding a switch connection](#) on page 77.
 3. Administer the CVLAN links. See [Administering CVLAN links](#) on page 82.
When perform 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 84.
 5. Administer the CVLAN clients. See [Adding CVLAN clients](#) on page 85.
When you perform this procedure, use the CVLAN client information you noted in Step 2.
-

Migrating the MAPD-based CVLAN to AE Services

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.

-
1. Obtain the CVLAN settings from the MAPD.
See [Obtaining the CVLAN settings from the MAPD](#) on page 306.
 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 306.
-

Obtaining the CVLAN settings from the MAPD

-
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_oam` to start the CV/LAN screens.
 4. From the main menu, select **CV/LAN Administration**.
 5. From the **CV/LAN 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

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

-
1. Administer the NIC. See [Administering the Local IP for a single NIC configuration](#) on page 73.
 2. Administer the switch connection. See [Adding a switch connection](#) on page 77.
 3. Administer the CVLAN links. See [Administering CVLAN links](#) on page 82.
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 306.)
 - 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 306.)
 4. Test the CVLAN Links. See [Testing a CVLAN link](#) on page 84.
 5. Administer the CVLAN clients. See [Adding CVLAN clients](#) on page 85. When you perform this procedure, use the CVLAN client information you noted in Step 2.
-

Glossary

AES	Advanced Encryption Standard. The Advanced Encryption Standard (AES) is a Federal Information Processing Standard (FIPS) Publication (FIPS-197) that specifies a cryptographic algorithm for use by U.S. Government organizations to protect sensitive (unclassified) information. The AES specifies three key sizes: 128, 192 and 256 bits.
Alphanumeric	A character string that is a combination of letters of the alphabet and numbers.
API	Application Programming Interface. Software that applications use to interact with network services, telephony services, and so forth.
ASAI	Adjunct Switch Application Interface. ASAI is a protocol that enables software applications to access call processing capabilities provided by Avaya Communication Manager.
Association	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.
Authentication	The process of validating the identity of a user by means of user profile attributes.
Authorization	The process of granting a user the ability to carry out certain activities based on permissions.
Automatic Call Distribution	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.
Breadcrumb	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 Logs Audit Logs.
Call/call monitor	<p>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).</p> <p>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.</p>

Contrast with device monitors and device/device monitors, which are based on a device ID.

Call/device monitor

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.

Call control

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 TSAPI Service (which includes the Telephony Web Service and JTAPI) provide client applications with call control capabilities.

Call Information Services

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.

Certificate authority (CA)

A certificate authority is an organization that issues and manages security credentials, including digitally signed certificates containing public keys for message encryption and decryption.

CN

Common name. See [Common name](#).

Common name

In terms of [LDAP](#) 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.

Common User Store

The pool of shared user profile attributes maintained in the Lightweight Directory Access Protocol ([LDAP](#)) database. In other words, a common repository of user profiles. See also, [Profile](#).

Communication Manager API

The [Device, Media, and Call Control](#) 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.

Computer Telephony Integration

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.

Connection name	See Switch Connection Name .
CTI link	<p>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).</p> <p>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.</p>
CTI User	Computer Telephony Integration user (synonymous with CT User). See CT User .
CT User	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.
CUS	Common User Store. See Common User Store .
DES	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.
Device	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 Device ID), Location, Device Type, and Tlink Group.
Device/device	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.

Device group

Device group	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.
Device ID	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.
Device, Media, and Call Control	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.
Distinguished name	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.
Distributors	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 .
DMCC	See Device, Media, and Call Control .
DN	Distinguished Name. See Distinguished name .
Domain controller	Microsoft Windows based term for computer running XP Server that uses a common directory for storing account information for a complete domain.
DTMF	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.
Exception group	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

First party call control

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.

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

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). ACT 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 synchronization behavior of a particular Distributor. See also, [Distributors](#).

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.

User profile

A set of attributes that represent a specific user in the local LDAP database.

Vector Directory Number (VDN)

A VDN is an extension that provides access to the vectoring feature on the switch. Vectoring allows a customer to specify the treatment of incoming calls based on the dialed number.

Workstation

In general usage, a workstation, or an administrative workstation, refers to a computer running a browser with network access to the AE Server.

In terms of the AE Services Security Database (SDB), a workstation is the client computer that has either a Host Name or an IP address. It is represented in the Security Database by a host name or IP address.

Worktop

An SDB term. A worktop is a Security Database entity (object) that refers to a device, or a collection of devices, that are associated with the host name or IP address of a workstation. A worktop can consist of a client telephone (the worktop's primary device) and any number of additional telephony devices (such as fax machines or modems), which are specified through the worktop's secondary device list. The telephone

Worktop

extension is usually the Primary Device ID attribute in the Worktop object.

Index

A

add data-module command [25](#)
Adding a CLANs [25](#)
adding a station [289](#)
Adding AE Services users
 Users, AE Services, adding [102](#)
Administering a CTI link for an ASAI application [31](#)
Administering a CTI link for CVLAN [30](#)
Administering a CTI link for internal Avaya CVLAN
 applications [30](#)
Administering a network region [48](#)
Administering a switch connection. [77](#)
Administering CVLAN links [82](#)
Administering default dial plan [243](#)
Administering dial plan settings [241](#)
Administering DLG links [85](#)
Administering local IP [73](#)
Administering Local IP [74](#)
Administering Switch Connections [77](#)
Administering the PAM module [122](#)
administering UCIDs in Communication Manager [29](#)
AE Server, restarting [93](#)
AE Services Management Console
 home page [59](#), [101](#)
AE Services server data, restoring [89](#)
AE Services users, adding [102](#)
AE Services users, editing [103](#)
AES server
 hostname [183](#)
AES Web services) [249](#)
alarm codes and messages [203](#)
Alarms, clearing [202](#)
APIs that use the Security Database [145](#)
Application, and device monitoring [152](#)
ASAI application, administering a CTI link [31](#)
Asterisk, when treated as a wildcard [231](#)
attributeacl.properties [107](#)
attributesmap.properties [107](#)
authentication [99](#)
Authentication with Microsoft Active Directory Services
 and Kerberos [138](#)
auto-negotiated settings [184](#)
Avaya Services technicians, accounts [171](#)
Avaya support contact information [15](#)

B

Backing up certificates [225](#)
backup, AE Services server data. backing up [89](#)
Bundled server IP address, changing [178](#)

C

Call Control service setup [287](#)
Call monitoring application, sample configuration [166](#)
Call routing, in sample configuration [169](#)
Call/call monitors [152](#)
Call/device monitor [152](#)
Certificate administration
 importing the trusted certificate into AE Services [218](#)
 verifying installation of entire certificate chain in AE
 Services [219](#)
Certificate management
 importing the server certificate into AE Services [223](#)
Certificate management, Microsoft-based procedure for
 creating a server certificate for AE Services [222](#)
Certificate management, overview [209](#)
Certificate renewal [225](#)
change ip-codec-set command [37](#)
change ip-interface command [40](#)
change ip-network-region command [37](#)
change node-names ip command [25](#), [40](#)
CLAN, adding [25](#)
Clearing alarms [202](#)
client application computer
 running sample applications [287](#)
Client authentication [210](#)
codec set
 administering a region with [37](#)
codec set, that uses (G.711A,G.711U and G.729) [37](#)
Commit [258](#)
Communication Manager
 adding stations [289](#)
 administering for AE Services [17](#)
 administering for sample application [289](#)
 connectivity testing [287](#)
 IP address [289](#)
 network region and gateway [289](#)
Communication Manager and DMCC configuration,
 sample [40](#)
Configuring IP services [27](#)
connectivity testing

sample application	287
control modes	
exclusive	33
Converting a DER file to PEM	217
craft, changing default password	172
Creating a backup of the dial plan	247
Creating a server certificate for AE Services	222
Creating a server certificate request for AE Services	220
Creating an account for the AE Server on the Domain Controller	139
CT User field	102
CTI link for TSAPI, JTAPI, Telephony Web Service, DMCC with Call Control, or an AE Services integration (Microsoft or IBM Sametime)	31
CTI user settings, administering	160
CTI Users	159
CVLAN applications and link management	81
CVLAN clients, adding	85
CVLAN implementation guidelines	81
CVLAN Link, testing	84
CVLAN links, administering	82
CVLAN service, ensuring it is running	84
CVLAN, administering a CTI link	30
CVLAN, Local IP administration and the Any setting	76

D

database	
User Service	289
dateconfig command	181
dateconfig utility	175
default server certificate	57
Delete AE Services user	103
Dependent/independent dependency mode	34
Device and Media Control codec set	37
Device and Media Control extensions, administering a network region	39
Device group, adding	157
Device groups	156
Device service setup	287
device, adding	156
Device/device monitoring	152
df command	184
Dial plan administration, converting E.164 numbers and dial strings	230
dial plan for testing	288
Display Login Information page field descriptions	128
distributors	111
DLG links, administering	85
DMCC AA policy administration, bypassing user authentication	100
DMCC applications and SDB authorization	146

DMCC device services	147
DMCC media properties, setting`	88
DMCC Session Services	147
DMCC Station Properties, setting`	88
DMCC station registration modes	32
DMCC with device and media control only	62
DMCC with device and media control only (using a switch name for CLANs)	63
duplex settings for AES	184

E

Enabling DMCC server ports for DMCC applications prior to AE Services 3.1	73
Enabling Processor Ethernet	28
exclusive control	33
Exporting the dial plan	247
Extended worktop access	
and LAN address information	151
if disabled	151

F

field descriptions	
Platform Upgrade page	260
From TelURI settings	231 , 235

G

Gatekeeper list (for DMCC APIs that use device and media control)	78
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, JTAPI, CVLAN, and DLG)	77
genericldap1.properties	107
global password aging, administering	126

H

header and trailer of PEM (Base 64) certificate file	217
header and trailer of PKCS#7 trusted certificate file	217
Historical Metric Data Collector utility	188
HMDC utility	
checking the status	189
cleaning up data	194
collectable data	190
creating a metric data report	193
scheduling data collection	189

starting/stopping	189
unscheduling data collection	192
viewing configured schedules	192

I

Importing a dial plan	248
installation logs	186
interface speed for AES	184
IP services, configuring	27

L

LAN address information, and Extended Worktop	
Access	151
ldapfilter.properties	108
legal notices	2
Links, CVLAN	85
Links, TSAPI	86
Linux account, removing	120
Linux administrative account, changing properties	119
Linux commands	181–186
dateconfig	181
df	184
ethtool	184
mvap.sh	182
netconfig	183
route	185
scp	185
service start/stop/restart	185
sftp	185
shutdown	185
ssh	185
swversion	183
tetherreal	185
tripwire	186
Linux, restarting	93
List Local Host Logins page field descriptions	127
Local IP, administering	73, 74
locking a Linux account	121
log files, downloading	91
log files, viewing	90
log in	
to AE Services Management Console	59, 101
login audit, enabling	129
login report for a specific login ID, displaying	128
login report for all Linux accounts, displaying	127
login reports	127

M

Main dependency mode	33
----------------------------	--------------------

media encryption	38
media gateway, adding	39
media processor, adding	40
Media service setup	287
Modify default user	104
mvap.sh command	182

N

netconfig utility	177
network	
administering region and gateway	289
interface speed and duplex settings	184
monitor packets	185
network interface settings, configuring	92
network region	
adding softphones	39
Network regions for DMCC	36
Network regions, administering	25
NIC	
manually adjust settings	184
NIC Configuration page	184
NIC configuration, editing	265
NIC, recommended settings	264
notices, legal	2
NTP server, changing	177

O

OAM	
changing network settings	184

P

PAM issue (/etc/issue) message, creating	123
PAM limits, adding	125
PAM management	113, 122
PAM management capabilities	130
PAM MOTD (/etc/motd) message, creating	124
PAM time, administering	125
Password policy	
Linux	115, 280–282
User Management (local LDAP)	106, 283–286
Password, User Management	106
passwords	
user management	289
Platform Upgrade page	
field descriptions	260
Procedure 3a - Verifying the installation of the trusted certificate in AE Services	219

Procedure 6 - Importing the server certificate into AE Services OAM	223	SNMP manager, NMS or SSG	197
Processor Ethernet name or IP address, editing	80	SNMP trap receivers, administering	198
Processor Ethernet, enabling	28	SNMP traps, testing	200
Product ID administration	196	SNMP, AE Server as agent	196
		SNMP, basic information	195
R		softphones	
rasaccess, changing default password	172	adding to network region	39
rbac.properties	108	Software-only server IP address, changing	180
reboot AES server	185	sroot, changing default password	172
Recommended AE Service IP (local IP) settings	75	Switch connection status	32
Reinitializing User Management	109	Switch Connection status (AE Services)	80
Renewing certificates	226, 227	Switch connection, administering	77
replicator1.properties	107	Switch Connections, administering	77
Restarting the AE Server and the Web Server	96, 225	System Platform	
Restoring certificates	225	upgrading	257
RETIRED alarm status, clearing alarms	202		
Rollback	258	T	
Routing application, when started	152	Tlink group	
Routing, when a routing application is started	152	defined	161
RPMS	186	Tlink group, adding	155
		Tlink groups	154
S		To TelURI settings	231, 237
sample application		Tripwire	
administering on server	288	running an integrity check	174
files on server	287	Tripwire (AE Services on Bundled Server only)	
properties file	287, 289	reconfiguring for administrative access	173
running	287, 291	updating the database	175
Sample configuration		Tripwire (AE Services on System Platform and Bundled Server only)	
assigning permissions	164	printing a report	174
call monitoring	166	tripwire command	186
manager/assistant	165	Tripwire software	173
sdbdistributor.properties	107	Troubleshooting the sample application	292
Search user, feature	104	TSAPI links	153
Secure Services Gateway (SSG) sending traps to	197	TSAPI links, administering	86
Security administration	113	TSAPI properties	148
Server authentication	209	TSAPI properties, editing	149
server data backup	89	tutorial application, see sample application	287
server data restore	89	tutorial properties file	289
service start/stop/restart command	185		
service dependencies	95	U	
setting up CVLAN links	81	unlocking a Linux account	121
Share Talk	35	Unused Login Audit page field descriptions	130
Shared control mode	34	upgrade logs	186
Shared worktop device group administration	167	upgrading	
SMS proxy port settings, changing	250	System Platform	257
SNMP agent	195	User Management database, viewing the list of users	102
SNMP Agent, configuring	196	User Management page	289
SNMP manager	195	User Management, password	106

User Management, reinitializing	109	Verifying the installation of the server certificate in AE Services	224
User permissions changes to	160		
User, AE Services, deleting.	103	W	
user.properties	109		
Users, AE Services, editing	103		
<hr/>			
V			
VDN (vector directory number), usage example	168	worktop, adding	158 , 159
		worktop, importing	159
		Worktops	157
		ws_cus_bootstrap.properties	109

