Application Enablement Services
Installation and Upgrade Guide for a Software-Only Offer Release 4.2

An Avaya MultiVantage® Communications Application
Notice
While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer
Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

Link disclaimer
Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty
Avaya Inc. provides a limited warranty on this product. 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 through the Avaya Support Web site: http://www.avaya.com/support

License
USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER’S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

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 Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)
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.

Database License (DL). Customer 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.

Copyright
Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use 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 identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:

http://support.avaya.com/ThirdPartyLicense/

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 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://www.avaya.com/support

Trademarks
Avaya, the Avaya logo, and MultiVantage are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

Microsoft is a registered trademark of Microsoft Corporation.

All other trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

COMPAS
This document is also available from the COMPAS database. The COMPAS ID for this document is 130916.

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 Support Web site: http://www.avaya.com/support

© 2005 - 2008 Avaya Inc.
All Rights Reserved.
# Contents

Chapter 1: Prerequisites for installation or upgrade .......................... 7  
  Intended audience ................................................................. 7  
  Reason for Reissue ................................................................. 7  
  Requirements for the AE Services server .................................... 7  
  Other computer requirements .................................................. 8  
    Client application computers ............................................... 8  
    Communication Manager and media servers ................................ 9  
  Platform and third-party software requirements .............................. 9  
    Software platform .............................................................. 9  
    Third-party software ......................................................... 9  
  Network requirements ........................................................... 11  
    Supported network interface configurations .............................. 12  
    Network latency requirements .............................................. 12  
    Network interface speed and duplex settings ............................. 13  
  IP Migration Readiness and Optimization analysis .......................... 13  
  Security considerations ......................................................... 14  

Chapter 2: Installing the Linux platform software ............................... 15  
  Optimizing the Linux software for AE Services .............................. 15  
  Administering SELinux .......................................................... 17  

Chapter 3: Installing the AE Services software .................................. 19  
  Obtaining the server software .................................................. 19  
  Installing the AE Services server software .................................. 20  
    Linux accounts created by AE Services when you install the Avaya Services package (cs-services) .............................................. 26  
    Linux account created by AE Services if you do not install the AE Services package ......................................................... 26  
  Installation problems ............................................................. 27  
  AE Services files and directories .............................................. 27  
  Location of installation/upgrade logs and RPMs .............................. 28  

Chapter 4: Installing licenses ....................................................... 29  
  Installing an AE Services license .............................................. 29  
    Starting WebLM and assigning a WebLM password ......................... 30  
    Removing an existing license file ......................................... 31  
    Installing the license file ................................................... 32  
    Restarting AE Services ....................................................... 33  
  Troubleshooting an AE Services license installation ......................... 34
Contents

Resolving error messages ................................................. 34
Obtaining a license file .................................................. 35
Identifying the MAC address ............................................. 35

Chapter 5: Initial administration for AE Services .................. 37

Chapter 6: Upgrading and updating the AE Services software .... 39
About the audience .......................................................... 39
Using the information in this chapter ................................ 40
Task summary for AE Services server upgrades ...................... 41
  Adding an Administrator to AE Services OAM - general reference for the Software-Only server without cs-services ........... 42
  Changing the default password for the User Management administrator (the avaya account) ........................................... 44
  Opening an ssh session to AE Services ................................ 45
  Logging into AE Services OAM ......................................... 46
  Getting the prerequisites for an upgrade or update to AE Services ................................................................. 47
    Downloading the software for an upgrade .......................... 49
    Downloading the AE Services Release 4.2 Release Notes ........ 50
    Getting DMCC login information ..................................... 51
  Obtaining a new AE Services license .................................. 51
  Recording the local IP settings ........................................ 52
  Backing up the AE Services server drive ............................ 53
  Backing up the AE Services database ................................ 53
  Manually backing up the LDAP database - Releases 3.0 and 3.0.1 only ................................................................. 54
  Upgrading AE Services software ....................................... 55
  Upgrading the Red Hat Enterprise Linux software .................. 63
  Validating the configuration settings ................................ 64
    Manually restoring the AE Services database ....................... 65
    Manually restoring the LDAP database - Releases 3.0 and 3.0.1 only ................................................................. 65
    Installing a new license ................................................. 65
  Updating the AE Services software - general reference ........... 67
About installing updates and patches - general reference .......... 68
Uninstalling updates and patches - general reference .............. 69
Changing the default password for the cust account on local Linux -- general reference .............................................. 70
Changing the default password for the cust account in User Management -- general reference .............................................. 71
## Contents

### Appendix A: Enterprise-wide licensing .......................... 73
- An overview of enterprise-wide licensing .......................... 73
- Licensing configuration examples ................................. 75
  - Standard licensing ............................................ 75
  - Enterprise wide licensing -- allocating licenses or features .... 76
  - Enterprise wide licensing -- pointing to a master license on a remote server .... 77
- Setting up a configuration for allocating licenses ............... 78
  - Installing the license file and configuring the Master WebLM Server .... 79
- Setting up a local WebLM server .................................. 81
- Setting up the Local WebLM Server in your configuration ......... 82
- Changing the allocations of a license file ......................... 84
- Verifying the license allocations on the Local WebLM Server ...... 86

### Appendix B: Configuring an LDAP server for User Management .... 87
- Configuring the LDAP server ...................................... 87
- Create an LDAP User account ...................................... 88

### Appendix C: Setting up remote access ............................ 91
- Setting up remote access on the AE Services server ............... 92
- Setting up a client to dial in to the server ....................... 94
  - Linux client .................................................. 94
  - Microsoft Windows client ..................................... 94
  - PPP connection requirements .................................. 94

### Index ................................................................. 95
Chapter 1: Prerequisites for installation or upgrade

This chapter describes prerequisites and requirements for an Application Enablement (AE) Services new software-only installation or a Release 4.2 upgrade.

Intended audience

This document is intended for two audience segments:

● Customers who are installing, upgrading or updating the AE Services software for themselves.

● Avaya Services Technicians or Avaya BusinessPartners who are upgrading or updating the AE Services Software-Only Server on behalf of customers.

Reason for Reissue

The Application Enablement Services Installation and Upgrade Guide for a Software-Only Offer Release 4.2, is reissued to include the following information.

● Revised instructions for upgrading and updating the AE Services software. For more information, see Chapter 6: Upgrading and updating the AE Services software.

● Information about setting up an AE Services configuration that uses enterprise-wide licensing. See Appendix A: Enterprise-wide licensing on page 73.

Requirements for the AE Services server

AE Services software requires a customer-provided server with the following minimum requirements:

● 3.0 GHz single-processor Pentium IV class processor with hyperthreading enabled

● 1GB RAM (system memory)
Prerequisites for installation or upgrade

Note:
Customers who require 10,000 simultaneous MOC/LCS users or a sustained processing rate of 720 TSAPI messages per second require 2 GB of RAM.

- 10 GB free disk space, after installing Linux

Note:
If you choose to set up the /var directory as a file system to improve reliability, Avaya recommends at least another 10 GB for the /var partition. For more information, see Optimizing the Linux software for AE Services on page 15.

- Hard disk drive with at least 7200 rpm rating
- 512 KB L2 cache
- 100 BaseT Ethernet NIC, must be set to full duplex
- DVD/CD-ROM drive

Other AE Services server considerations include:

- AE Services 4.x and later software supports Symmetrical Multiprocessing. However, AE Services is a network-centric application and not a processor-intensive application. Adding more processors will not necessarily increase the capacity or performance of the platform.
- The hostname of the AE Services server must be 15 or fewer characters. To determine the hostname associated with an AE Services server, run the following Linux command from the command line: `uname -n`.

Other computer requirements

This section describes requirements for other computers in an AE Services 4.2 configuration.

Client application computers

AE Services requires a customer-supplied computer for the AE Services client application.

- You can develop and run Device, Media, and Call Control applications on any computer that is capable of running the Java 2 Platform, Standard Edition (J2SE) 1.5.
- For requirements for other AE Services clients, see the Application Enablement Services TSAPI, JTAPI, and CVLAN Client and SDK Installation Guide (02-300543).
Communication Manager and media servers

To use AE Services Release 4.2, you must have the official Avaya Communication Manager Release 3.1.x, 4.x, or 5.x software running on an IP-enabled media server.

Note:
Only Communication Manager 3.1.x or later provides link bounce resiliency for the Application Enablement Protocol (AEP) transport links that AE Services uses.

AE Services supports all media servers and gateways that support Communication Manager Release 3.1.x, 4.x, or 5.x.

Platform and third-party software requirements

AE Services software requires the platform and third-party software described in this section.

Software platform

AE Services software requires Red Hat Enterprise Linux ES 4.0 update 6. The customer is responsible for obtaining an appropriate version of RHEL software.

Linux software considerations include:

- You must disable Security Enhanced Linux (SELinux) to support AE Services software. For more information, see Administering SELinux on page 17.

- Check the latest AE Services release notes to find the latest supported update. For a copy of the release notes, see the AE Services customer documents on the Avaya Support Web site: http://www.avaya.com/support.

Note:
The AE Services server is supported only on the English version of the Red Hat Linux OS. AE Services is not localized to other languages at this time.

Third-party software

The AE Services installation program installs and configures all of the required third-party packages. Avaya strongly recommends you accept this option when you install the AE Services.
Prerequisites for installation or upgrade

server software. **Table 1** shows a complete list of required packages for a software-only installation.

**Note:**
Customers are responsible for their license agreements with the companies of required third-party software.

**Table 1: Required third-party software**

<table>
<thead>
<tr>
<th>Name and minimum version for AE Services 4.2</th>
<th>Used for:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveMQ 4.0.1</td>
<td>System Configuration</td>
</tr>
<tr>
<td>apr 0.9.4-24.5 apr-util 0.9.4-21</td>
<td>Httpd</td>
</tr>
<tr>
<td>Axis 1.4</td>
<td>User Service, Telephony Service</td>
</tr>
<tr>
<td>compat-libcom_err 1.0-5</td>
<td>Postgres</td>
</tr>
<tr>
<td>Curl 7.12.1-8.rhel4</td>
<td>Installer</td>
</tr>
<tr>
<td>Dialog 1.0.20040731-3</td>
<td>Installer</td>
</tr>
<tr>
<td>distcache 1.4.5-6</td>
<td>Httpd</td>
</tr>
<tr>
<td>Ethereal 0.10.6-3</td>
<td>Avaya technical support if you have a Services contract</td>
</tr>
<tr>
<td>expect 5.42.1</td>
<td>OAM</td>
</tr>
<tr>
<td>gdb 6.3.0.0</td>
<td>Serviceability</td>
</tr>
<tr>
<td>httpd 2.0.52-28 httpd-suexec 2.0.52-28</td>
<td>OAM, SMS</td>
</tr>
<tr>
<td>JDK 1.5.0_10</td>
<td>Device, Media and Call Control, OAM</td>
</tr>
<tr>
<td>Kerberos (krb5): krb5-devel 1.3.4-27</td>
<td>TSAPI</td>
</tr>
<tr>
<td>krb5-libs 1.3.4-46 krb5-workstation 1.3.4-27</td>
<td></td>
</tr>
<tr>
<td>libidn 0.5.6</td>
<td>SMS</td>
</tr>
<tr>
<td>libpcap 0.8.3-10.rhel4</td>
<td>Ethereal</td>
</tr>
<tr>
<td>libxml2 2.6.16-6</td>
<td>SMS</td>
</tr>
<tr>
<td>mod_ssl 2.0.52-28</td>
<td>Apache</td>
</tr>
<tr>
<td>mon 0.99.2.6</td>
<td>Alarming services</td>
</tr>
</tbody>
</table>
### Table 1: Required third-party software (continued)

<table>
<thead>
<tr>
<th>Name and minimum version for AE Services 4.2</th>
<th>Used for:</th>
</tr>
</thead>
<tbody>
<tr>
<td>net-snmp 5.1.2-11</td>
<td>Alarming services</td>
</tr>
<tr>
<td>net-snmp-libs 5.1.2-11</td>
<td></td>
</tr>
<tr>
<td>nss_ldap 226-13</td>
<td>Security</td>
</tr>
<tr>
<td>openldap 2.2.13-6.4E</td>
<td>User Service</td>
</tr>
<tr>
<td>openldap-clients 2.2.13-6.4E</td>
<td></td>
</tr>
<tr>
<td>openldap-servers 2.2.13-6.4E</td>
<td></td>
</tr>
<tr>
<td>openssl 0.9.7a-43.10</td>
<td>SMS, Transport Layer</td>
</tr>
<tr>
<td>pam 0.77-66.17</td>
<td>Security</td>
</tr>
<tr>
<td>pam_krb5 2.1.8</td>
<td></td>
</tr>
<tr>
<td>perl-Time-HiRes 1.55-3</td>
<td>Alarming services (Mon)</td>
</tr>
<tr>
<td>pdksh 5.2.14-30.3</td>
<td>DLG, Call Control</td>
</tr>
<tr>
<td>PHP 5.1.6-3</td>
<td>SMS</td>
</tr>
<tr>
<td>php-cli 5.1.6-3</td>
<td></td>
</tr>
<tr>
<td>php-common 5.1.6-3</td>
<td></td>
</tr>
<tr>
<td>php-soap 5.1.6-3</td>
<td></td>
</tr>
<tr>
<td>PostgreSQL 8.1.8-1</td>
<td>All services</td>
</tr>
<tr>
<td>postgresql-libs 8.1.8-1</td>
<td></td>
</tr>
<tr>
<td>postgresql-jdbc 8.1.4-1</td>
<td></td>
</tr>
<tr>
<td>postgresql-server 8.1.8-1</td>
<td></td>
</tr>
<tr>
<td>tcl 8.4.7-2</td>
<td>OAM (Expect)</td>
</tr>
<tr>
<td>Tomcat 5.5.9</td>
<td>WebLM, OAM, User Service, Telephony</td>
</tr>
<tr>
<td><strong>Note</strong>: When you install third-party software using the installer, Avaya supplies the Tomcat RPM avaya-coreservices-tomcat 5.5.9</td>
<td>Web Service</td>
</tr>
<tr>
<td>Tripwire 2.3.1-21</td>
<td>Security</td>
</tr>
</tbody>
</table>

---

### Network requirements

This section describes supported network configurations, requirements, and settings.
Supported network interface configurations

You can configure the AE Software Only server to use one or more ethernet ports. Network topology and implementation requirements should dictate which configuration best serves your needs. In most cases the single NIC satisfies both the network and the implementation requirements.

- Single NIC (one ethernet port): In most cases the single NIC satisfies both the network and implementation requirements. Avaya recommends that you use Ethernet interface 1 (eth0).

  In this configuration, the AE Services server, Communication Manager server, and client application computer all reside on a private LAN, virtual LAN (VLAN), or WAN.

- Multiple NIC (more than one ethernet port): For example, if you have an Avaya Services package, and your are using multiple NIC configuration, with four ethernet ports, use ports: eth0, eth2, or eth3 (eth1 is reserved for technicians). Multiple NICs can be used when two network segments are used (LAN, VLAN, or WAN). When the AE Server and the client application are on one network segment and the AE Server and Communication Manager are on another network segment, the client segment is referred to as the production network, and the Communication Manager segment is referred to as the private network segment.

Note:
When using multiple NICs, the NICs must be on separate network segments.

Always use the AE Services OAM Web pages to configure the network interface settings (Administration > Network Configuration > Local IP and Administration > Network Configuration > NIC Configuration).

Network latency requirements

Regardless of the type of network used (LAN, VLAN or WAN), set up the TCP/IP links (CTI links) between the AE Services server and Avaya Communication Manager with the following network latency characteristics:

- No more than a 200ms average round-trip packet delivery time, as measured with ping over every one-hour time period

- Periodic spiked delays of no more than 2 seconds while maintaining the 200ms average round-trip delivery time, as measured with ping over every one-hour time period

These requirements are necessary to maintain the AE Services communication channel with each Communication Manager C-LAN over a LAN/VLAN or WAN. Considerations include:

- If the CTI application will issue route requests, the associated “wait” step must have a value greater than the largest “periodic spiked delay”. With a maximum delay of 2
seconds, the wait step must be greater than 2 seconds. If you can guarantee “periodic spiked delays” of less than 2 seconds, you can reduce the wait step time-out accordingly.

● If the switch receives no response to a route select, the call will follow the remaining steps in this specific vector, so you must program the vector to deal with this condition. If you are using AE Services 3.1.x or later software and encounter “periodic spiked delays” greater than 2 seconds, messages are either:

- Stored and retransmitted after recovering from a short network outage, or
- Dropped during a long network outage

Note:

The communication channel between the AE Services server and the Communication Manager (C-LANs) requires a hub or data switch. Avaya does not support the use of a crossover cable.

Network interface speed and duplex settings

AE Services software has been tested at 100Base-T full duplex and these are the required speed and duplex settings. The CLAN board on the Communication Manager limits the maximum AE Services network speed to 100 Mbs. Verify the NIC settings before you install the AE Services software.

IP Migration Readiness and Optimization analysis

For Device, Media, and Call Control (DMCC) call recording solutions, Avaya recommends that you use the Avaya IP Migration Readiness and Optimization services to help you safely implement IP-based solutions in a stable, optimized infrastructure.

These services include a two-phased, detailed analysis of the entire network to help assess whether you can deploy a converged IP solution such as AE Services without adversely affecting your existing network applications and services.

The first phase of this analysis is the Customer Infrastructure Readiness Survey (CIRS). Certified Avaya engineers conduct a high-level evaluation of the local and wide area network infrastructure to identify any significant network issues that must be resolved prior to deploying the proposed IP solution.

Phase 2 of this analysis, Network Analysis/Network Optimization (NANO), is required when the CIRS indicates that the network cannot support the proposed IP solution at the desired performance levels. Starting with the information and data gathered for the CIRS, Avaya engineers perform problem diagnosis to get at the root causes of network issues. They also provide functional requirements and recommendations for a network design that optimizes all of the resources needed to support the IP solution.
Security considerations

For a complete discussion of the security considerations and guidelines for AE Services, see the White Paper on Security in Application Enablement Services for Bundled 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.
Chapter 2: Installing the Linux platform software

Before you can install AE Services software, you must first obtain and install the software for your Linux platform. Avaya does not provide Linux installation media with a software-only offer.

Linux considerations for AE Services software include:

- For AE Services Release 4.2, you must install Red Hat Enterprise Linux ES 4.0 update 6 (RHEL4 update 6). For more information, see Platform and third-party software requirements on page 9.
- Install Linux before you install the AE Service software, because the AE Services installation script also configures Linux for AE Services.

⚠️ CAUTION:
To prevent problems with the AE Services software, follow the Avaya-recommended guidelines described in this chapter.

---

Optimizing the Linux software for AE Services

Follow the instructions of the Red Hat installation utility to install the Linux operating system. In general, you can use the default options unless specifically noted otherwise.

To optimize the Linux installation for AE Services:

1. Boot to your Linux installation media.
2. Avaya strongly recommends doing a minimal installation of Linux. To access the Minimal option, run the Linux installation using the graphical mode.

⚠️ CAUTION:
The Linux software defaults to doing a complete installation. However, a complete installation can result in version conflicts with some of the third-party software packages that AE Services requires.

3. In the Linux installation program, set up disk partitioning:
   - You can use the Linux default partitioning, or
   - To improve system reliability, Avaya recommends that you set up the /var directory as a file system (partition). This change prevents the AE Services root directory from becoming filled with log messages. To set up a /var partition:
     a. On the Disk Partition Setup screen, select the partition method you prefer, such as Automatically partition. On the next screen, click New.
     b. Name the partition /var and complete the screen.
Installing the Linux platform software

c. Allocate about 40 percent of the disk drive space to create the /var partition if available. The /var partition must be at least 10 GB in size.

4. On the Firewall Configuration screen, the Security Enhanced Linux (SELinux) features are active by default. You must disable SELinux or AE Services will not work correctly. Locate the Enable SELinux option and select Disabled.

**CAUTION:**

If you fail to disable SELinux before you install the AE Services software, some AE Services will not start and other problems will occur. To resolve the AE Services problems, you must disable SELinux and then reboot the server.

For more information about SELinux, see Administering SELinux on page 17.

5. On the Package Installation Defaults screen, select a minimal installation of Linux:

   a. Click Customize software packages to be installed.
   
b. On the Package Group Selection screen, scroll down and select Minimal.

6. Complete the Linux installation and reboot the server.

   The time required for the software installation depends the options you selected and the server processing power. Allow several minutes.

7. After the reboot completes, verify that the /etc/hosts file contains the correct IP address for the AE Services server.

   a. Using the text editor of your choice, open the /etc/hosts file.
   
b. Verify that the AE Services server name is on a separate line with the correct IP address. For example:

```
127.0.0.1 localhost localhost.localdomain
10.9.30.106 aeserver1 aeserver1.mycompany.com
```
   
c. If needed, correct the AE server information and save the /etc/hosts file.

   **Note:**

   Apache HTTPD needs this line under some circumstances. If the /etc/hosts file contains an incorrect IP address for the AE Services server, AE Services will not start.

8. For security purposes, enable only the specific ports you require. Include all the ports that the AE Services software uses. For a list of required ports, see the White Paper on Security in Application Enablement Services for Bundled 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.

9. Add a kernel parameter to specify using the clock on the internal processor. RHEL4 update 4 defaults to using the power management clock, which degrades system performance.

   To specify the clock mechanism:

   a. In a command line interface window, change to the /boot/grub directory.
b. Open the file `grub.conf` and append `clock=hpet` to the line that starts with `kernel`.

**Note:**
Be sure to add a space between the previous parameter and the `clock=hpet` parameter.

c. Save the file and reboot the server.

---

**Administering SELinux**

The Linux software enables the Security Enhanced Linux (SELinux) feature by default. However, you must disable SELinux or the AE Services software will not work correctly.

- During a fresh Linux installation, disable SELinux on the Firewall Configuration screen. For this procedure, see [Optimizing the Linux software for AE Services](#) on page 15.
- If the Linux operating system is already installed, you must disable SELinux before you install the AE Services software.

⚠ **CAUTION:**
If you fail to disable SELinux before you install the AE Services software, some AE Services will not start and other problems will occur. To resolve the AE Services problems, you must disable SELinux and then reboot the server.

You can use the root user command `sestatus` to determine if SELinux is enabled or not.

1. Log in to the server as a user that has root privileges.
2. From the command line interface, type: `/usr/sbin/sestatus`

The response indicates if SELinux is **enabled** or **disabled**.

For more information about SELinux, see the Fedora Core 3 SELinux FAQ at [http://docs.fedoraproject.org/selinux-faq-fc3/index.html](http://docs.fedoraproject.org/selinux-faq-fc3/index.html). Information includes how to enable or disable SELinux.
Installing the Linux platform software
Chapter 3: Installing the AE Services software

This chapter describes how to install the AE Services server software and third-party software.

Obtaining the server software

Obtain the AE Services software from one of these sources:

- The software-only installation CD-ROM for Release 4.2, provided by Avaya
- The latest 4.2 software-only ISO image. To obtain an ISO image:
  - Customers that have a valid Software Support or Software Support plus Upgrades agreement can download the software from the Avaya Support Web site: [http://www.avaya.com/support](http://www.avaya.com/support).

To install from an ISO image, you can either:

- Create a CD-ROM from the ISO image and install from the CD, or
- Download and mount the ISO image and install from the mounted image
Installing the AE Services server software

You must install the AE Services server software from a window that emulates xterm or is recognized by Linux. If you try to install the server software from a DOS window, you might have display problems.

To mount the drive and start the installation program:

1. Open an ssh session to the AE Server and access an account with root privileges. For more information, see Opening an ssh session to AE Services on page 45.

2. From the command line interface, list the contents of /etc/fstab to find out the name of the media directory, such as /media/cdrom. The media directory will be your mountpoint for this procedure.

3. Follow Step a if you are installing from a CD-ROM; follow Step b if you are installing from an ISO image.

   a. (CD-ROM) Insert the disk into the DVD or CD-ROM drive on the server.
      - If the Autorun RPM is installed and configured on the server, the AE Services installation program starts automatically. Continue with Step 4.
      - If the installation program does not start automatically, mount the DVD or CD-ROM drive using the following command, and then continue with Step 4.

         \[
         \text{mount} \ \text{mountpoint}
         \]

         where \text{mountpoint} is the name of the media directory, such as /media/cdrom.

   b. (ISO image) Download the ISO image to the /tmp directory of the AE Services server.

      - Mount the image using the following command format:

         \[
         \text{mount} \ -t \text{iso9660} \ -o \text{loop} /\text{tmp/swonly-r4-1-0-18-20080903.iso} \text{mountpoint}
         \]

         where:

         - \text{swonly-r4-1-0-18-20080903.iso} is the file name of the ISO image for the AE Services software for a Software-Only offer. Note that the file name is subject to change.
         - \text{mountpoint} is the name of the media directory, such as /media/cdrom.
4. To start the installation program manually, type the following command (assuming the mountpoint is /media/cdrom): /media/cdrom/install

The installation program displays the navigation instructions.

5. Press Enter to continue with the server installation.

The installation program displays the Select Installation Media screen.

6. Select the media from which to install, then highlight the OK option and press Enter.

The installation program displays the Enter RPM URL screen.

7. Update the RPM location as follows:
   a. Change the path to use the mountpoint you used in the install command. For more information, see Installing the AE Services server software on page 20.
Installing the AE Services software

b. Highlight the **OK** option and press **Enter**.

The installation program displays the Select Release Version screen.

8. Verify the release you are installing, and then select **OK**.
   The installation program displays the Co-residency warning screen.

9. Select **Yes** to continue.
The installation program displays the Choose Installation Method screen.

![Choose Installation Method]

10. Verify that **Install** is selected, and then select **OK**.

   The installation program displays the Choose Installation Packages screen.

![Choose Installation Packages]

11. Verify that both packages are selected. Press **Enter** to select **OK**.

   The installation program displays the Optional Packages screen.

![Optional Packages]

12. Select the optional packages that you want to install.

   - **mvap-linuxconfig** - Installs the Linux configuration package (selected by default).
     
     Avaya strongly recommends that you install **mvap-linuxconfig**.
Installing the AE Services software

- **cs-cusldap** - Configures a Lightweight Directory Access Protocol (LDAP) directory in the default location of /etc/openldap (selected by default).

  Unless you are installing AE Services on a server that already has an implementation of LDAP installed, Avaya recommends that you configure LDAP for AE Services by selecting **cs-cusldap**.

  **CAUTION:**

  If you are installing AE Services on a server that already has an implementation of LDAP installed, clear the selection for **cs-cusldap**. (Selecting the **cs-cusldap** option will overwrite your existing LDAP directory). To use your existing LDAP directory with AE Services you will need to manually configure your LDAP implementation for compatibility with AE Services User Management. For this procedure, see Appendix B: Configuring an LDAP server for User Management on page 87.

- **cs-service** - This choice installs the Avaya Services package for AE Services.

  Select this option only if you have a technical support contract with Avaya. This package provides specific customer accounts as well as Avaya Services accounts along with tools for Avaya support personnel. If you select this option

  The installation program displays the final warning screen.

  ![Last chance to abort -- Ready to Proceed?](image)

  13. Verify the installation command. If all options are correct, press **Enter** to select **Yes**.

  The software installation proceeds. The system displays the status of the installation on the screen. The final message for a successful installation is:

  Success
  Installation/Update completed

  **Note:**

  The time required to install the software varies depending on the packages you selected and the server processing power. Allow 5 to 10 minutes for the installation to complete.

  14. After the installation is complete, press **Enter** to select **Exit**.

  The installation program displays a final status screen, indicating the success or failure of the software installation.
For a successful installation, the installation program displays the following message. Select OK.

For an unsuccessful installation, the installation program displays a similar screen that states:

Installation/Update Failed

If the installation fails, check the installation log files for clues. See Location of installation/upgrade logs and RPMs on page 28.

15. Reboot the server to prepare for license installation.

16. You must install a valid license file before you can start the AE Services software. For this procedure, see Chapter 4: Installing licenses on page 29.
Linux accounts created by AE Services when you install the Avaya Services package (cs-services)

When you select cs-services and install the Avaya Services package, the installation program sets up the customer’s AE Server with **avaya** and **cust** accounts by default. It also adds service accounts, such as **craft**, for Avaya Service Technicians and Avaya BusinessPartners. Here is a summary of the **avaya**, **cust**, and **craft** accounts:

- **avaya** - The **avaya** account (default password is **avayapassword**) provides access to the User Management Service in Application Enablement Services Operations Administration and Maintenance.

  - The customer is responsible for changing the password for the **avaya** account after initially using it. For information about changing the password for the **avaya** account, see the following topic: *Changing the default password for the User Management administrator (the avaya account)* on page 44.

- **cust** - The **cust** account provides the customer with read-write access all to administrative domains in AE Services Web based administrative interface (referred to as Application Enablement Services Operations Administration and Maintenance, or AE Services OAM). The **cust** account also provides remote access, using a secure shell (ssh) client, to the Linux shell.

  - The customer is responsible for changing the password for the **cust** account after initially using it. For instructions about changing the password for the **cust** account see the following topics:
    - *Changing the default password for the cust account on local Linux -- general reference* on page 70
    - *Changing the default password for the cust account in User Management -- general reference* on page 71

- **craft** - The **craft** account provides Avaya Service Technicians and Avaya BusinessPartners with read-write access to all AE Services OAM administrative domains: CTI OAM Administration, User Management, and Security Administration.

Linux account created by AE Services if you do not install the AE Services package

If you did not install the Avaya Services package, AE Services provides the **avaya** account only.

For information about changing the password for the **avaya** account, see the following topic: *Changing the default password for the User Management administrator (the avaya account)* on page 44.
Installation problems

If you have problems installing the AE Services software, call 1-800-344-9670 or contact your local Avaya distributor.

AE Services files and directories

The installation program creates all required directories and files for AE Services during software installation. To locate all files and directories AE Services installed on the server:

1. Log in to the Operations, Administration, and Maintenance (OAM) home page on the AE Services server:
   a. From a web browser, type the fully qualified domain name or IP address of the AE Services server, for example:
   
   https://myaeserver.example.com
   
   b. On the Application Enablement Services welcome page, click AE Server Administration.
      The first time you try to access the AE Server, it presents a Security Alert for an SSL certificate. If the SSL certificate is not presented, verify that the URL shows the correct AE Services name or IP address, and that the browser shows https on the address line.
      c. Click Yes to accept the SSL certificate.
      Your browser display the Application Enablement Services welcome page.
      d. Log in using an appropriate user name and password.

2. From the OAM home page, click CTI OAM Administration > Help > About AE Services.
      The About AE Services screen lists all the AE Services-related RPMs installed on the server, along with their version numbers.

3. To find out where a particular RPM installs its files, use a command line interface and type:
   
   rpm -ql packagename
   
   where packagename is the name of the RPM, without the version number. For example, mvap-platform.
   The response displays the directories created and the files installed by the RPM.
Location of installation/upgrade logs and RPMs

You can use the installation logs to verify the success of an installation or upgrade, or to troubleshoot errors.

- Log files for an installation or upgrade are in:
  /var/disk/logs/update.out-yyyy-mmdd-tttt
  where yyyy-mmdd-tttt is a date and time stamp.
  For example, a log file could be named /var/disk/logs/update.out-2007-0309-0951.
- The system keeps copies of the Red Hat Package Manager (RPM) packages for each release that is installed, up to three releases. You can find the RPMs in:
  /var/disk/Releases/rx-nnn
  where rx-nnn is the release number.

Note:
For a list of all the RPMs that are installed, run swversion -a.
Chapter 4: Installing licenses

AE Services software requires you to install a valid license file for Release 4.2.

⚠️ CAUTION:
AE Services cannot start if the license file is missing or is from the wrong release.

Installing an AE Services license

Avaya sends the AE Services license file in an email message. If you did not receive a license file from Avaya, see Obtaining a license file on page 35.

1. Locate the email containing the AE Services license file.
2. Detach the license file from the email, and store it locally on a computer or flash drive.

   Note:
   You do not have to store the license file on the AE Services server.

3. Continue as appropriate:
   - If the server already has a license (for example, from an earlier version of the software), continue with Removing an existing license file on page 31.
   - If the server has no license, continue with Installing the license file on page 32.
Installing licenses

Starting WebLM and assigning a WebLM password

The Web License Manager (WebLM) provides you with the ability to manage Avaya product licenses.

Follow this procedure to start a WebLM session:

1. Log in to the computer that has the license file stored on it, or insert the flash drive that contains the license file.

2. Access the Web License Manager (WebLM) home page on AE Services server.
   a. From a web browser, type the fully qualified domain name or IP address of the AE Services server. For example:
      https://myaeserver.example.com
   b. On the Application Enablement Services welcome page, click WebLM Administration.

   The server changes the connection to a secure connection (https) and displays the Web License Manager Logon page.

   The first time you access this page, the server presents a Security Alert for an SSL certificate.

3. Accept the SSL certificate by clicking Yes.

   Note:
   If the SSL certificate is not presented, verify that the URL shows the correct AE Services name or IP address, and that the browser shows https on the address line. Some browsers indicate that they are running a secure connection by displaying the lock symbol somewhere on the browser window.

4. Log in to WebLM:
   a. Accept the default user name: admin.
   b. Type the default password for this account: webladmin.
   c. Click the arrow button to continue.

5. The first time you log in to WebLM, the server displays the Change Password page.
   Complete the fields on the Change Password page and click Submit.

   The password must contain 6 to 14 characters. White spaces are not permitted in the password, and the password itself must not be blank.

   Note:
   WebLM issues the Change Password page only the first time you log in to WebLM. You do not have to change your password the next time you log in.

   The server displays the Logon page.

6. Log in as admin with the correct password.
Removing an existing license file

Follow this procedure to remove an old AE Services license file from the server:

1. Log in to the computer that has the license file stored on it, or insert the flash drive that contains the license file.

2. From a web browser, type the fully qualified domain name or IP address of the AE Services server. For example:

   https://myaeserver.example.com

   Your browser displays the Application Enablement Services Welcome page.

3. From the Welcome page, click WebLM Administration.

   Your browser displays the Web License Manager Log on screen.

4. Enter your WebLM user name and password, and click the arrow.

   WebLM displays the main menu and the Install License page.

5. From the main menu, under Application_Enablement, click Uninstall Licenses.

   WebLM displays the Uninstall License page.

6. From the Uninstall License screen, select the check box for the Application_Enablement license, and click Uninstall.

7. Your browser displays a message asking if you want to continue. Click OK.
Installing licenses

Installing the license file

When you are ready to install the license on an AE Services server:

1. Log in to the computer that has the license file stored on it, or insert the flash drive that contains the license file.
2. From a web browser, type the fully qualified domain name or IP address of the AE Services server, for example:

   https://myaeserver.example.com

3. On the Application Enablement Services welcome page, click WebLM Administration.

   Your browser displays the Web License Manager Log on screen.

4. Enter your WebLM user name and password, and click the arrow.

   WebLM displays the main menu and the Install License page.

5. To install the license file:
   a. At Enter License Path, click Browse.
   b. Locate and select the AE Services license file.
   c. Verify that you selected the correct file for this server. Click Install.

   WebLM uploads the license file to the WebLM server. When the process is complete, the server displays the message: License file installed successfully.

   ! CAUTION: If you do not receive this message, see Troubleshooting an AE Services license installation on page 34.

6. Verify that the license settings are correct for this customer.
   a. Under Licensed Products, click Application Enablement.
   b. Verify that the correct license settings are enabled.

7. Log out of WebLM. Click Logout or the Logoff link.

Restarting AE Services

You must restart AE Services to use the capabilities of the new license.

You can restart AE Services from the command line or through the OAM interface.

- **From the command line:**
  1. Open an ssh session to the AE Server, by following Step a (for customers) or Step b (Avaya BusinessPartners or Services Technicians). If you are not familiar with opening an ssh session, see Opening an ssh session to AE Services on page 56.
    a. **(Customers)** log in as cust and access the root account by using the `su - root` command.
    b. **(Avaya Services Technicians or BusinessPartners)** log in as craft and access the root account by using the `su - sroot` command.
  2. Restart AE Services, using the following command: `/sbin/service mvap restart`
     The `restart` command stops AE Services, configures them, and then restarts the services. The restart process takes from 3 to 10 minutes.

- **From the Operations, Administration, and Maintenance (OAM) interface:**
  1. Access the OAM home page on AE Services server.
    a. From a web browser, type the fully qualified domain name or IP address of the AE Services server for example:
       ```
       https://myaeserver.example.com
       ```
    b. On the Application Enablement Services welcome page, click **AE Server Administration**.
       The server changes the connection to a secure connection (https).
  2. Log in using an appropriate user name and password
    a. **(Customers)** log in as cust and use the password for the cust user.
    b. **(Avaya Services Technicians or BusinessPartners)** log in as craft and use the password for the craft user.
  3. From the OAM home page, click **CTI OAM Administration > Maintenance > Service Controller**.
  4. On the Service Controller page, click **Restart AE Server**.
  5. On the Restart AE Server page, click **Restart**.
     After a pause, the server returns to the Service Controller page. A restart can take several minutes.
  6. Verify that all the correct licensed services are running.
Installing licenses

This completes the AE Services license installation. You can now:

- Log off the server, or
- Continue with server administration. For more information, see Chapter 5: Initial administration for AE Services on page 37.

Troubleshooting an AE Services license installation

Use the information in this section to troubleshoot problems you might encounter during license installation. Topics include:

- Resolving error messages
- Obtaining a license file on page 35

Resolving error messages

If your browser displays an error message, try to resolve the problem as shown in Table 2. If you cannot resolve the problem, contact your Avaya representative.

Table 2: Licensing error messages and resolution procedures

<table>
<thead>
<tr>
<th>Error message</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>License file is invalid or not created for this server. License file was NOT installed.</td>
<td>The file is corrupt or the MAC address in the license file does not match the MAC address in the server. To resolve this problem, see Identifying the MAC address on page 35.</td>
</tr>
<tr>
<td>Attempting to install a license file that is currently installed. License file was NOT installed</td>
<td>This license was already activated.</td>
</tr>
<tr>
<td>More than one license exists, the AE Server will not be started. Please have only one valid license and delete other licenses.</td>
<td>A valid license already exists due to an upgrade from an earlier release. You must remove the old license before you install the new 4.2 license. See Removing an existing license file on page 31.</td>
</tr>
<tr>
<td>No valid license file found</td>
<td>WebLM might display this message on the main page after AE Services reports &quot;License file installed successfully&quot;. To resolve this problem:</td>
</tr>
<tr>
<td></td>
<td>1. Verify you are using the AE Services server host name, and not the IP address.</td>
</tr>
<tr>
<td></td>
<td>2. If the host name is correct, contact your Avaya representative.</td>
</tr>
</tbody>
</table>
Obtaining a license file

If you did not receive the AE Services license file in an email from Avaya, contact your Avaya or Avaya Partner representative. To ensure that your request is processed as quickly as possible, be ready to provide the information listed in Table 3.

Note:

You must send a separate request for each license file.

Table 3: Required information for requesting a license file

<table>
<thead>
<tr>
<th>Required information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Return email address</td>
<td>Avaya emails the license file to you. You must provide a secure email address where you want to receive the license file.</td>
</tr>
<tr>
<td>MAC Address of the first NIC on the server. For servers with more than one NIC, use the first Ethernet interface.</td>
<td>Provide the unique 12-digit hexadecimal number for this server in the correct format. For more information, see Identifying the MAC address on page 35.</td>
</tr>
</tbody>
</table>

Identifying the MAC address

If AE Services software is already installed, you can use WebLM to identify the Media Access Control (MAC) address. Always use the first Ethernet interface of the first NIC on the server:

1. From a web browser, access the WebLM home page on the AE Services server. For example, you could type:
   
   https://aeserver/WebLM/

   where aeserver is the IP address or the fully qualified domain name of the AE Services server. If you use this form of the WebLM URL, you must supply a closing /.

2. Log in to WebLM using an appropriate user name and password.

3. On the Server Properties page, the value for Primary Host ID is the MAC address.

You can alternatively use the Linux `ifconfig` command to identify the MAC address of the NIC. This method does not require the AE Services software to be installed:

1. From the Linux command prompt, type the command: `ifconfig`

   Linux displays the current information about the network interface. For example:

   ```
   eth0  Link encap:Ethernet  HWaddr 00:B0:D0:44:9F:A1
   inet addr:10.10.10 Bcast:10.255.255.255  Mask:255.0.0.0
   ```

   The MAC address corresponds to the HWaddr. In this example, the value is 00B0D0449FA1. When you specify the MAC address, do not include the colons.
Installing licenses

⚠️ Important:
If the server has a dual NIC or multiple NICs, provide the MAC address of the first Ethernet interface on the first NIC.

2. Provide the MAC address to your Avaya representative when you request a license.

Note:
If the NIC you used to generate the MAC address changes after initial installation, contact your local Avaya distributor. If you have a technical support agreement with Avaya, call 1-800-344-9670.
Chapter 5: Initial administration for AE Services

After you install the AE Services software and license, you must administer connectivity between Communication Manager and AE Services.

Note:
From this point forward, your primary reference is the Application Enablement Services Administration and Maintenance Guide (02-300357).

The basic administration tasks you must follow in the Application Enablement Services Administration and Maintenance Guide are:

1. Administer Communication Manager for connectivity to AE Services. Follow the procedures in Chapter 1, “Administering Communication Manager for AE Services”.

2. Administer AE Services for connectivity to Communication Manager. Follow the procedures in Chapter 2, “AE Services OAM Administration and CTI OAM Administration”.

3. Continue with any additional administration and testing procedures as directed by the Application Enablement Services Administration and Maintenance Guide until the system is ready for service. See Chapter 3 through Appendix A.
Initial administration for AE Services
Chapter 6: Upgrading and updating the AE Services software

This chapter is intended for two audience segments:

● Customers who are upgrading or updating the AE Services software for themselves. Customers are grouped as follows:
  - Customers who did not install the cs-service package when they installed AE Services (customers who do not have an Avaya Services contract). These customers do not have the default cust account. They will need to create a similar account, as described in Adding an Administrator to AE Services OAM - general reference for the Software-Only server without cs-services on page 42.
  - Customers who did install the cs-service package when they installed AE Services (customers who do have an Avaya Services contract). The cs-service package installs the default cust account.

● Avaya Services Technicians or Avaya BusinessPartners who are upgrading or updating the AE Services Software-Only Server on behalf of customers. The cs-service package installs the default craft account as well as other services accounts.

Note:
For more information about the cs-service package see Step 12 of "Installing the AE Services software," in Chapter 3.

All of the administrative tasks described in Table 2: Per-release task summary for upgrades on page 41 apply to both audience segments. The basic distinction between the audiences are the accounts they use for logging into AE Services. For more information see:

● Adding an Administrator to AE Services OAM - general reference for the Software-Only server without cs-services on page 42
● Opening an ssh session to AE Services on page 45
● Logging into AE Services OAM on page 46

About the audience

To carry out the procedures in this chapter you must have experience administering an AE Services server or a comparable Linux based server. Additionally this chapter assumes that you are familiar with AE Services CTI OAM administrative tasks, such as administering network connections, and other related tasks, For more information see the Avaya MultiVantage Application Enablement Services Administration and Maintenance Guide, 02-300357.
Using the information in this chapter

The primary purpose of this chapter is to describe the procedures for changing from a previous release of AE Services to the current release, AE Services, Release 4.2.

Note:
You can upgrade any release of AE Services software directly to Release 4.2 without having to install Release 4.0.

Table 1: AE Services releases

<table>
<thead>
<tr>
<th>Applicable releases</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>AE Services 4.0.1</td>
<td>Releases 4.0 and 4.0.1 are collectively referred to as 4.x.</td>
</tr>
<tr>
<td>AE Services 4.0</td>
<td>(When the third position is zero, it is implied. The notation &quot;4.0.0&quot; is not used.)</td>
</tr>
<tr>
<td>AE Services 3.1.4</td>
<td>Releases 3.0 through 3.1.4 are collectively referred to as 3.x.</td>
</tr>
<tr>
<td>AE Services 3.1.3</td>
<td>Notes: Release-specific notation is always used for Releases 3.0 and 3.0.1. Some information applies to both 3.0 and 3.0.1, and some information applies exclusively to either release (a reference to 3.0 means 3.0 only). 3.1.x: The notation 3.1.x refers to 3.1 through 3.1.4.</td>
</tr>
<tr>
<td>AE Services 3.1.2</td>
<td></td>
</tr>
<tr>
<td>AE Services 3.1.1</td>
<td></td>
</tr>
<tr>
<td>AE Services 3.1.0</td>
<td></td>
</tr>
<tr>
<td>AE Services 3.0</td>
<td></td>
</tr>
</tbody>
</table>
Task summary for AE Services server upgrades

Use the information in Table 2 as a checklist for performing upgrades to Release 4.2. Tasks are presented in sequential order. Some tasks are optional and some tasks are apply to specific releases. If the task does not apply, skip the task. In the table, R/O stands for required or optional. For an explanation of release notation, see Table 1: AE Services releases on page 40.

Table 2: Per-release task summary for upgrades

<table>
<thead>
<tr>
<th>Task</th>
<th>R/O</th>
<th>Applicable releases</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Getting the prerequisites for an upgrade or update to AE Services on page 47</td>
<td>Required</td>
<td>All releases -- 3.x and 4.x</td>
</tr>
<tr>
<td>2 Obtaining a new AE Services license on page 51</td>
<td>Required (3.x) Optional (4.x)</td>
<td>Required for all 3.x releases. Optional for 4.x - If you want the updated System Management Service functionality, you must install a new License file. Otherwise you do not need to install the new license file. See Obtaining a new AE Services license on page 51.</td>
</tr>
<tr>
<td>3 Recording the local IP settings on page 52</td>
<td>Optional</td>
<td>All releases -- 3.x and 4.x. A recommended precautionary procedure.</td>
</tr>
<tr>
<td>4 Backing up the AE Services server drive on page 53</td>
<td>Optional</td>
<td>All releases -- 3.x and 4.x. Important: Avaya recommends that you backup the entire contents of the AE Services server drive.</td>
</tr>
<tr>
<td>5 Backing up the AE Services database on page 53</td>
<td>Required</td>
<td>All releases -- 3.x and 4.x.</td>
</tr>
<tr>
<td>6 Manually backing up the LDAP database - Releases 3.0 and 3.0.1 only on page 54</td>
<td>Optional</td>
<td>Applies to releases 3.0 and 3.0.1 only.</td>
</tr>
<tr>
<td>7 Upgrading AE Services software on page 55</td>
<td>Required</td>
<td>All releases -- 3.x and 4.x.</td>
</tr>
<tr>
<td>8 Validating the configuration settings on page 64</td>
<td>Required</td>
<td>All releases -- 3.x and 4.x.</td>
</tr>
<tr>
<td>9 Installing a new license on page 65</td>
<td>Optional</td>
<td>Required for all 3.x releases. Optional for 4.x - If you want the updated System Management Service functionality, you must install a new License file. Otherwise you do not need to install the new license file. See Obtaining a new AE Services license on page 51.</td>
</tr>
</tbody>
</table>
Adding an Administrator to AE Services OAM - general reference for the Software-Only server without cs-services

To be able to carry out the procedures in this chapter, you must add a user to Linux, and set up that user with access privileges to the AE Services Web based administrative interface -- Application Enablement Services Operations Administration and Maintenance, often referred to as AE Services OAM. The root user can not access AE Services OAM.

This procedure assumes the following:

- You installed Linux using a Minimal installation and you disabled Security Enhanced Linux (see Chapter 2: Installing the Linux platform software on page 15).
- You installed the AE Services software, but you did not install the cs-service package. (Step 12 of "Installing the AE Services software," in Chapter 3).

Follow this procedure to add a user to Linux and to enable that user to access AE Services OAM. This procedure describes set up a user with access to CTI OAM, Security Management, and the User Service (equivalent to craft and cust).

Add a user to AE Services local Linux

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` to add a user with access to CTI OAM and Security Administration.
   
   For example: `useradd -g susers -G securityadmin cust00`

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.

Add the Linux user to User Management in OAM

6. From your web browser, type the fully qualified domain name or IP address of the AE Services server, for example: `myaserver.example.com`

   AE Services displays the Welcome page.
7. From the main menu, select **AE Server Administration**

AE Services displays the log in screen, with the message, "Please log on."

- In the Logon field, enter **avaya** (the User Management Administrator)
- In the Password field, enter **avayapassword** (the default).

⚠️ **SECURITY ALERT:**
Change this password immediately. For more information, see [Changing the default password for the User Management administrator (the avaya account)](page 44) on page 44.

8. AE Services OAM displays the Home page (User Management is the only item in the main menu).

9. Select **User Management**.

10. AE Services displays the User Management home page.

11. From the main menu, select **User Management > Add User**.

12. AE Services displays the Add User page.

13. Complete the fields on the Add User page for the cust00 user

   a. In the User Id: field, enter **cust00**
   b. In the Common Name field, enter the users first name, for example: **Jan**
   c. In the Surname field, enter the users first name, for example: **Green**
   d. In the User Password and Confirm Password fields, add the password that you established for the cust00 user in Step 4.
   e. In the Avaya Role field, select **userservice.useradmin** (when you select this attribute, this user has access to User Administration).
   f. Click **Apply**.

This new user will have access to the following AE Services OAM administrative domains:

- CTI OAM Administration
- Security Administration.
- User Management.
Changing the default password for the User Management administrator (the avaya account)

By default, AE Services installs an account called avaya for the Software Only server. The avaya account is installed even if you do not 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 Appendix C of the AE Services Administration and Maintenance Guide, 02-300357.

Follow this procedure to change the password for the default avaya account.

1. Log in to AE Services OAM as avaya with the default password.
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 CTI OAM, and Security Management, the password for the avaya account must be identical to the password for the Linux user you set up previously in Adding an Administrator to AE Services OAM - general reference for the Software-Only server without cs-services on page 42.
   b. In the Confirm New Password field, re-enter the new password.

Click Apply to put the change into effect.
Opening an ssh session to AE Services

To access AE services using an ssh client follow this procedure. This procedure assumes that you have a secure shell (ssh) client, such as PuTTY or PuTTYtel running on your administrative workstation.

1. Start your ssh client, and complete the information in the dialog box that it presents to open a session. For example, specify the following information to open a session to the AE Server.
   - Host Name (or IP address) - enter the host name or IP address of your AE Server, for example: myaserver.example.com
   - Port - 22
   - Connection type - SSH
   - Click Open
   The system displays the PuTTY window.

2. If you are a customer, follow Step a. If you are an Avaya Services Technician or BusinessPartner follow Step b.
   a. (Customer) Log in as follows:
      - At the Login as: prompt, enter root.
      - At the Password: prompt, enter the password for root.
   b. (Service Technician or BusinessPartner) Log in as follows:
      - At the Login as: prompt, enter craft.
      - At the Password: prompt, enter the password for craft.
      - At the command prompt, access a user account that has root privileges by using the command: su - sroot.

During an upgrade or update procedure, you might need to provide the full path name for a command, depending on how your Linux system is configured.
Logging into AE Services OAM

Many of the procedures in this chapter require you to log in to AE Services Operations Administration and Maintenance (OAM), the Web-based interface for managing the AE Server.

Keep in mind that you can not log in to OAM with a root account. Use the user account you created when you completed the procedure for Adding an Administrator to AE Services OAM - general reference for the Software-Only server without cs-services on page 42.

Follow this procedure to log in to AE Services OAM.

1. From your web browser, type the fully qualified domain name or IP address of the AE Services server, for example: myaserver.example.com
   AE Services displays the Welcome page.

2. From the main menu, select AE Server Administration
   AE Services displays the log in screen, with the message, "Please log on."

3. Enter a login and password for a user account with access to AE Services CTI OAM Administration. Select a, b, or c, as it applies to you.

   a. (Customers who did not install cs-service)
      - In the Logon field, enter the name of the user account you created in Adding an Administrator to AE Services OAM - general reference for the Software-Only server without cs-services on page 42.
      - In the Password field, enter the appropriate password for this user

   b. (Customers who did install cs-service) Complete the fields on the login screen as follows, and click Login.
      - In the Logon field, enter cust.
      - In the Password field, enter the appropriate password for the cust user

   c. (Service Technicians or BusinessPartners) Complete the fields on the login screen as follows, and click Login.
      - In the Logon field, enter craft.
      - In the Password field, enter the appropriate password for the craft user.

Note:
   For the craft (and other services accounts) to be available, the cs-service package must be installed (see Step 12 of "Installing the AE Services server software," in Chapter 3).

AE Services displays the AE Services OAM Home page.
Getting the prerequisites for an upgrade or update to AE Services

Before you start the upgrade procedures make sure you have the following items.

- **Administrative workstation** -- a computer or a laptop with network access to the AE Server. The computer must have the following software:
  - A browser (for access to AE Services OAM)
  - An ssh client (such as PuTTY) for access to the Linux operating system at the command prompt.

- **Recommended** -- a program for backing up the complete AE Services server drive. Use a program that allows you to copy the entire contents of the AE Services server drive. Avaya strongly recommends that you create a complete backup of the AE Services server drive before you upgrade the AE Services software.

- **For 3.0 and 3.0.1 upgrades only** -- you will need a means of transferring the LDAP database backup file from the AE Server to another computer. For example you can use pscp, or a third party client for secure file transfers, or a flash disk.

- **AE Services 4.2 Software** -- Required for upgrading all releases of AE Services. Get either of the following:
  - ISO file for the Application Enablement Services Server Software for the Software Only Solution, file name: `swonly-r4-1-0-31-2-20081118.iso`. To get the software, see [Downloading the software for an upgrade](#) on page 49.
  - The AE Services software-only installation CD-ROM for Release 4.2, provided by Avaya. The AE Services software-only installation CD-ROM can be ordered by contacting your Avaya representative or account executive.

- **Red Hat Enterprise Linux ES 4.0 update 6 software**. Recommended for upgrading all releases of AE Services.
  - If you are upgrading from AE Services 3.x to 4.2, follow the procedure, [Upgrading AE Services software](#) on page 55, before you upgrade Red Hat Enterprise Linux. At Step 10, you will be instructed upgrade Red Hat Enterprise Linux.
  - If you are upgrading from AE Services 4.0, 4.0.1, or 4.1 to 4.2 you can upgrade Red Hat Enterprise Linux either before you upgrade AE Services or after you upgrade AE Services.

- **AE Services License file for Release 4.2** -- Required for 3.x releases. It is required for 4.x releases only if you want to activate the new AE Services System Management Service (SMS).

**Note:**

If you need a new license, contact your Avaya representative well in advance of the day you plan to upgrade. For more information see [Obtaining a license file](#) on page 35.
Upgrading and updating the AE Services software

- **Release Notes** -- To get the release notes, see [Downloading the AE Services Release 4.2 Release Notes](#) on page 50.

- **(Optional) DMCC login information** -- if your upgrade involves the Device, Media, and Call Control API, see [Getting DMCC login information](#) on page 51 (note that prior to AE Services Release 3.1.1, the DMCC API was referred to as the Communication Manager API, or CMAPI).
**Downloading the software for an upgrade**

The software downloads for upgrading to AE Services 4.2 are as follows:

- **Application Enablement Services Server Software for the Software Only Solution**

Follow this procedure download the AE Services software downloads

1. From your administrative workstation, start your browser, and go to [support.avaya.com](http://support.avaya.com).
   
   Your browser displays the Avaya Support site "Support" page.

2. From the Support page, click **DOWNLOAD CENTER and UPDATES to AVAYA’S MANUFACTURER SUPPORT POLICY**

3. From the Online Service Manager Download Center page, click **Download My software**

4. On the Avaya SSO login page, enter your login ID and password, and click **Log In**.

5. From the Download Center page, select **Application Enablement Services**.
   
   Your browser displays the Application Enablement Services: Download Center page, which defaults to the latest release. Make sure the list box next to "Select a release" displays **4.2**.
   
   This page displays the Software Downloads table.

6. From the Software Downloads table, select **Application Enablement Services Server Software for the Software Only Solution**.
   
   Your browser displays the Application Enablement Services: Download Center page, for the Application Enablement Services Server Software for the Software Only Solution.

7. Click **Download** and save the file (**swonly-r4-1-0-31-2-20081118.iso**) to your administrative workstation.
Upgrading and updating the AE Services software

**Downloading the AE Services Release 4.2 Release Notes**

This procedure applies to all releases (see Table 2: Per-release task summary for upgrades on page 41).

Follow these steps to download the Application Enablement Services Release 4.2 Release Notes from the Avaya Support Web site (www.support.avaya.com).

1. From your browser, go to **support.avaya.com**. Your browser displays the Avaya Support site "Support" page.
2. From the Support page, click **FIND DOCUMENTATION and TECHNICAL INFORMATION by PRODUCT NAME**
3. From the Find Documentation and Downloads by Product Name page, select **Application Enablement Services**. Your browser displays the Application Enablement Services page for Release 4.2 by default.
5. Select **Application Enablement Services Release 4.2 Release Notes**. Your browser displays the Application Enablement Services: Release Notes & Software Update Notes page, which contains the following links: View PDF, and Download.
6. Select **Download** to download the Application Enablement Services Release 4.2 Release Notes file to your administrative workstation. Unzip and review the Release Notes before you start the upgrade procedure.
Getting DMCC login information

If you are upgrading an installation that uses DMCC, or its predecessor CMAPI, you will need to get the login and password that any DMCC or CMAPI applications are using.

- AE Services 3.x did not validate CMAPI logins or passwords, many applications and installers used whatever they wanted.
- AE Services 4.x does validate both CMAPI logins and passwords, if they are not right the CMAPI links will not start.
- AE Services 4.2 also enforces 8+char+num+special passwords, if an application is using something less you may have to turn off change the password rules on the AE Services PAM Module Configuration page in OAM. To access PAM Module Configuration, log in to AE Services OAM. From the home page, select Security Administration > PAM Management > PAM Module Config.

CMAPI applications that use Single Step Conference will also need "CT User" turned on for the CMAPI login.

Obtaining a new AE Services license

For an explanation of release notation, see Table 1: AE Services releases on page 40.

Obtaining a new license is required for upgrading all 3.x releases. A new license is not required if you are upgrading from 4.x, unless you want to activate the new AE Services System Management Service (SMS). Activating the new SMS feature requires a new license.

⚠️ Important:

If you need a new license, contact your Avaya representative well in advance of the day you plan to upgrade.

For information on obtaining a license file, see Chapter 4: Installing licenses on page 29.
Upgrading and updating the AE Services software

Recording the local IP settings

This procedure is recommended for upgrading all releases.

For AE Services, local IP settings are the IP addresses you have assigned to the Ethernet interfaces on the AE Server. It is recommended that you record them, and then verify them after the upgrade is complete.

Recording the local IP settings refers to maintaining a record of the settings that appear on the "Local IP" screen in the AE Services OAM interface. You can manually record the settings on paper, or you can create an electronic file and either type in the information or capture the screen.

Follow this procedure to record the local IP settings.

1. From your browser, log in to AE Services OAM with the appropriate user account and password. For more information, see Logging into AE Services OAM on page 46.

   AE Services displays the AE Services OAM Home page.

2. From the main menu, select CTI OAM Administration to access the CTI OAM home page.

3. For 4.x releases, follow Step a; for 3.x releases, follow Step b.

   a. (4.x) From the CTI OAM home page, click Administration > Network Configuration > Local IP.

   b. (3.x) From the CTI OAM home page, click Administration > Local IP.

4. From the Local IP page, record the Local IP settings for the Ethernet interfaces (Client Connectivity, Switch Connectivity, and Media Connectivity).
Backing up the AE Services server drive

This procedure is required for all releases.

Use an appropriate software program that allows you to perform a full system backup of the AE Services Server drive. Back up the entire contents of the AE Services server drive to another medium or device.

Backing up the AE Services database

This procedure is required for upgrading all releases.

Note:

If you are upgrading releases 3.0 and 3.0.1, you will need to manually back up the LDAP database. See Manually backing up the LDAP database - Releases 3.0 and 3.0.1 only on page 54

Follow these steps to back up the AE Services database.

1. From your browser, log in to AE Services OAM with the appropriate user account and password. For more information, see Logging into AE Services OAM on page 46.

   AE Services displays the AE Services OAM Home page.

2. From the main menu, select CTI OAM Administration to access the CTI OAM home page.

3. From the CTI OAM home page, click Maintenance > Backup Database.

   AE Services backs up the database, and displays the Database Backup page, which displays the following message:

   The backup file can be downloaded from here.

4. Click the here link.

   A file download dialog box is displayed, which allows you to either open or save the backup file (named as: mvapdbddmmyyyy.tar.gz, where ddmmyyyy is a date stamp).

5. Click Save, and download the backup file to a safe location that the upgrade will not affect. For example, save the file to your local computer or another computer used for storing backups.
Manually backing up the LDAP database - Releases 3.0 and 3.0.1 only

This procedure applies to Releases 3.0 and 3.0.1 only.

For Releases 3.0 and 3.0.1, you must backup and restore the LDAP database. Notice that you perform the backup procedure before the upgrade and the restore procedure after the upgrade.

Follow this procedure to manually back up the LDAP database before you upgrade the software. This procedure is an important precaution in case the upgrade fails.

1. Open an ssh session to the AE Server and access an account with root privileges. For more information, see Opening an ssh session to AE Services on page 45.

2. From the command line, follow these steps to backup the LDAP directory to a tar file
   a. Go to the directory containing the LDAP database: `cd /var/lib/ldap`
   b. Use the tar command to create a backup of the LDAP database:

   ```bash
   tar -cvf tar_file_name.tar *.dbb
   ```

   where `tar_file_name` is any name you want to give the file, such as `ldap.tar`.

3. Using `pscp`, or a third party client for secure file transfers, transfer the LDAP backup to your administrative workstation or another computer for safe storage.

⚠️ Important:

After you complete the upgrade, you must restore the LDAP database. See Manually restoring the LDAP database - Releases 3.0 and 3.0.1 only on page 65.
Upgrading AE Services software

This procedure applies to upgrading all releases of AE Services.

Use the following procedure to upgrade AE Services software and Linux. You can upgrade AE Services software from either a CD-ROM or from an ISO image.

1. Open an ssh session to the AE Server and access an account with root privileges. For more information, see Opening an ssh session to AE Services on page 45.

2. From the command line interface, list the contents of /etc/fstab to find out the name of the media directory. The media directory is the mountpoint for this procedure.

3. Follow Step a if you are installing from a CD-ROM; follow Step b if you are installing from an ISO image.

   a. (CD-ROM) Insert the disk into the DVD or CD-ROM drive on the AE Services server.
      
      ● If the Autorun RPM is installed and configured on the server, the AE Services installation program starts automatically and displays the navigation instructions. Continue with Step 5.
      
      ● If the installation program does not start automatically, mount the DVD or CD-ROM drive using the following command, and then continue with Step 4.
      
      ```bash
      mount mountpoint
      ```
      
      where `mountpoint` is the name of the media directory, such as `/media/cdrom`.

   b. (ISO image) Download the ISO image to the /tmp directory of the AE Services server.
      
      ● Mount the image using the following command format, and then continue with Step 4.
      
      ```bash
      mount -t iso9660 -o loop /tmp/swonly-r4-1-0-31-2-20081118.iso mountpoint
      ```
      
      where `mountpoint` is the name of the media directory, such as `/media/cdrom`.
4. To start the installation program manually, type the following command (assuming the mountpoint is `/media/cdrom`): `/media/cdrom/install`

The installation program displays the navigation instructions.

5. Press **Enter** to continue with the server software installation.

The installation program displays the Loss of Data Warning screen.

6. If you followed the procedure described in [Backing up the AE Services database](#) on page 53, press **Enter** to select **Yes**.
The installation program prompts you to back up the AE Services database to the AE Server.

7. Press Enter to select Yes.

If the installation program detects a previous release of AE Services software, .

8. Press Enter to select Yes.

Note: If you select No, the installation aborts.
The installation program continues with the process to uninstall the previous release of AE Services. When it completes, it prompts you to press Enter continue.

9. Press **Enter** to continue.

10. If the installation program displays the RHEL Upgrade Required screen, click **OK** to stop the installation. Then follow the procedure for Upgrading the Red Hat Enterprise Linux software on page 63. If the installation program does not display RHEL Upgrade Required screen, continue with Step 11.
11. If the installation program displays the Select Installation Media screen, click **OK**. Then continue with Step 12.

12. Select the media from which to install, then highlight the **OK** option and press **Enter**. The installation program displays the Enter RPM URL screen.

13. Update the RPM location as follows:
   a. Change the path to use the `mountpoint` (such as `/media/cdrom`) you used in the install command. For more information, see Step 4.
b. Highlight the OK option and press Enter.

The installation program displays the Select Release Version screen.

![Select Release Version window]

14. Verify the release you are installing, and then select OK.

The installation program displays the Co-residency warning screen.

![Co-residency warning window]

15. Select Yes to continue.

The installation program displays the Choose Installation Method screen.

![Choose Installation Method window]

16. Verify that Install is selected, and then select OK.
The installation program displays the Choose Installation Packages screen.

17. Verify that both packages are selected. Press **Enter** to select **OK**.

The installation program displays the Optional Packages screen.

18. Select the optional packages that you want to install.

   - **mvap-linuxconfig** - Installs the Linux configuration package (selected by default). Avaya strongly recommends that you accept the default.

   - **cs-cusldap** - Installs the LDAP configuration package for AE Services (selected by default). Accept the default unless you are using your own LDAP.
Upgrading and updating the AE Services software

⚠️ CAUTION:

If you are using your own implementation of LDAP, clear this selection. (Selecting the `cs-cusldap` option will overwrite your existing LDAP directory).

- **cs-service** - Select this option only if you have a technical support contract with Avaya. This package provides tools and information, including a Services login, to Avaya support personnel (not selected by default).

The installation program displays the final warning screen.

19. Verify the installation command. If all options are correct, press **Enter** to select **Yes**.

The software installation proceeds. The system displays the status of the installation on the screen. The final message for a successful installation is:

```
Success
Installation/Update completed
```

**Note:**

The time required to install the software varies depending on the packages you selected and the server processing power. Allow 5 to 10 minutes for the installation to complete.

20. After the installation is complete, press **Enter** to select **Exit**.

The installation program displays a final status screen, indicating the success or failure of the software installation.

- For a successful installation, the installation program displays the following message. Select **OK**.

```
Installation Successful - Install/Upgrade Log file is in /var/disk/logs/
```
For an unsuccessful installation, the installation program displays a similar screen that states:

Installation/Update Failed

If the installation fails, check the installation log files for clues. See Location of installation/upgrade logs and RPMs on page 28

21. Reboot the server.

22. If you ran the AE Services upgrade from a CD-ROM, remove the CD from the AE Services server.

Upgrading the Red Hat Enterprise Linux software

Use this procedure only if the AE Services installation program stops and forces you to upgrade Red Hat.

1. Access the Red Hat Enterprise Linux ES 4.0 update 6 software. From the Linux main menu, select upgrade and follow the instructions of the Red Hat utility to upgrade the Linux operating system.

2. Add a kernel parameter to specify using the clock on the internal processor. RHEL4 update 6 defaults to using the power management clock, which degrades system performance.

   To specify the clock mechanism:
   
   a. In a command line interface window, change to the /boot/grub directory.

   b. Open the file grub.conf and append clock=hp et to the line that starts with kernel. Be sure to add a space between the previous parameter and the clock=hp et parameter.

   c. Save the file and reboot the server.

3. Go to Upgrading AE Services software on page 55, and complete all steps.
Validating the configuration settings

This procedure is required for all upgrades.

Follow this procedure to verify the upgrade. Recall that when the upgrade script completes and the AE Server reboots, your administrative workstation loses its connection to the AE Server. You must open an ssh session to the AE Server as directed in Step 1.

1. Open an ssh session to the AE Server, and access the root account. For specific information about opening an ssh session and accessing the root account, see Opening an ssh session to AE Services on page 45.

2. From the command line, run the command `swversion` and verify that the version number and build number are correct.

⚠️ **CAUTION:**

If the upgrade was not successful, do not continue with this procedure. Try to determine what the problem was before you attempt another upgrade.

3. From your browser, log in to AE Services OAM with the appropriate user account and password. For more information, see Logging into AE Services OAM on page 46.

   AE Services displays the AE Services OAM Home page.

4. From the main menu, select **CTI OAM Administration** to access the CTI OAM home page.

5. From the main menu, select **Administration > Network Configuration > Local IP**. Compare the settings on the Local IP page with the settings you recorded in Recording the local IP settings on page 52.

6. Select **NIC Configuration**, and verify that the NIC configuration settings are correct for AE Services. For more information, see Network interface speed and duplex settings on page 13.

7. Check all of the remaining OAM pages listed under **Administration**, and verify that the information is complete and correct.

8. From the main menu bar in the upper right section of the OAM screen, select **OAM Home** to display the top-level OAM Web pages. From the main menu select **User Management**, and check the User Management settings (local LDAP). If you are upgrading from 3.0 or 3.0.1 and you find problems with the User Management settings, you should manually restore the LDAP database. See Manually restoring the LDAP database - Releases 3.0 and 3.0.1 only on page 65.

9. From the main menu bar in the upper right section of the OAM screen, select **OAM Home** to display the top-level OAM Web pages. From the main menu select **Security Administration**, and check the Security Management settings (local Linux).

   If you find any problems with the settings on any of the AE Services OAM pages, you should manually restore the database. See Manually restoring the AE Services database on page 65.
Manually restoring the AE Services database

If you noticed any problems during the previous procedure, "Validating the configuration settings," continue with these steps to restore the AE Services database. This procedure applies to all releases.

1. From the main menu, select **AE Server Administration**
2. Log in using an appropriate user name and password.
3. From the OAM home page, click **CTI OAM Administration**.
4. On the CTI OAM home page, verify that all previously licensed services are running.
5. Manually restore the AE Services database.
   - a. From the CTI OAM home page, click **Maintenance > Restore Database**.

Locate the correct backup file for this server, and click **Restore**.

Manually restoring the LDAP database - Releases 3.0 and 3.0.1 only

If you noticed any problems during Step 8 of the previous procedure, "Validating the configuration settings," continue with these steps to restore the AE Services LDAP database. This procedure applies to Releases 3.0 and 3.0.1 only.

1. Open an ssh session to the AE Server and access an account with root privileges. For more information, see *Opening an ssh session to AE Services* on page 45.
2. Locate the tar file for the LDAP directory backup. (See Step 3 of *Manually backing up the LDAP database - Releases 3.0 and 3.0.1 only* on page 54).
3. Copy the tar file for the LDAP directory backup to /var/lib/ldap.
5. Extract the tar file in the ldap directory: `tar -xvf tar_file_name.tar`.
   where `tar_file_name` is the name of your saved tar file:
6. Restart the LDAP service using the following command: `service ldap restart`.
   - a. This completes the procedure to restore the LDAP database. After the LDAP service restarts, you can remove the tar file: `rm tar_file_name.tar`.

Installing a new license

For an explanation of release notation, see *AE Services releases* on page 40.

Installing a new license is required for upgrading all 3.x releases. If you are upgrading from 4.x, you need to install a license only if you want to activate the new AE Services System Management Service (SMS).

For the complete procedure, see *Chapter 4: Installing licenses* on page 29.
Upgrading and updating the AE Services software

**Note:**
You must restart AE Services after installing the license, as the procedure directs.
Updating the AE Services software - general reference

Avaya periodically provides updates and patches for the AE Services software.

- An update provides new features or enhancements to the AE Services system. An update might also include bug fixes. Avaya releases updates only on an as-needed basis for critical fixes. Updates are effected by the update command.

- A patch addresses a specific issue related to a specific component or a set of components in the AE Services system.

When you install an update or patch:

- The install script installs the new version of the RPMs in /var/disk/software.

- The update script backs up the current RPM before installing the new version of the RPM.

The /var/disk/software directory also contains all of the previous versions of the RPMs. To see all updates or patches installed on a server, use the command: swversion -a.
About installing updates and patches - general reference

Updates and patches consist of ZIP files of RPMs. You can apply multiple updates or patches to the system, using the `update` command.

Updates and patches are available on the Avaya Support Web site: [http://www.avaya.com/support](http://www.avaya.com/support). Check the Support site periodically to see if there is a new patch that applies to your system:

⚠️ **CAUTION:**

Always use the procedure described in this book, not an RPM command, to install AE Services updates or patches.

Follow this procedure to install an update or a patch:

1. From AE Services OAM, back up the server database before you install an update. See [Backing up the AE Services database](#) on page 53
2. Open an ssh session to the AE Server and access an account with root privileges. For more information, see [Opening an ssh session to AE Services](#) on page 45.
3. Download any new patch or update files to the current directory.
4. From the command line, type: `update -u xxxx.zip`
   
   where `xxxx` is the name of the downloaded file.

   The system displays the update or patch ID and the RPMs contained in the package. The system then prompts you to confirm the installation of the RPMs.

   - If you enter `y`, the installation of the update or patch proceeds. The system:
     - Stops AE Services, Tomcat service, and DBService.
     - Installs the RPMs contained in the package.
     - Restarts AE Services, Tomcat service, and DBService.
   - If you enter `n`, the installation of the update or patch aborts.

   To see all the updates or patches installed on the server, use the command: `swversion -a`. 
Uninstalling updates and patches - general reference

Note:
The directory /opt/mvap/resources/patch-update contains the patchnumber.txt files. These files list the RPMs that were installed in each update or patch.

Follow this procedure to uninstall updates or patches:

1. Open an ssh session to the AE Server and access an account with root privileges. For more information, see Opening an ssh session to AE Services on page 45.

2. From the command prompt, type swversion -a to find the number of the update or patch you want to remove.

3. At the command prompt, type: update -e patchnumber.
   The screen displays a list of all the RPMs to be uninstalled. The system prompts you for confirmation before it uninstalls these RPMs.
   - If you enter y, the system uninstalls the updates or patches. The system:
     - Stops AE Services, Tomcat service, and DBService.
     - Rolls back the RPMs specified in patchnumber.txt to the previous version.
     - Restarts AE Services, Tomcat service, and DBService.
   - If you enter n, the upgrade script exits.
Changing the default password for the cust account on local Linux -- general reference

This topic applies only to an AE Services Software Only sever with the Avaya Services package (cs-services) installed.

Follow these steps to create a new System Administrator account and delete the cust account.

Note:
If you require a greater level of security, see Appendix C, "Replacing the cust and avaya accounts," in the AE Services Administration and Maintenance Guide, 02-300357.

The current procedure describes how to change the default password for the cust account in local Linux. The local Linux cust account provides remote access to the Linux shell.

4. From a web browser, type the fully qualified domain name or IP address of the AE Services server. For example, myaes.example.com.
AE Services displays the Welcome page.

5. From the main menu, select AE Server Administration.
AE Services displays the log in screen, with the message, "Please log on."

6. Complete the log in screen:
   ● In the Logon field, enter the default user name for the system administrator: cust.
   ● In the Password field, enter the default password for the system administrator: custpw.
   ● Click Login.
AE Services displays the AE Services OAM Home page.

7. From the main menu, select Security Administration.
AE Services displays the Security Administration home page.

8. From the main menu, select Account Management > Modify Login.
AE Services displays the Modify Login page:

9. 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.

10. In the Re-enter passwords field, re-enter the new password.

11. Click Modify.
Changing the default password for the cust account in User Management -- general reference

This topic applies only to an AE Services Software Only sever with the Avaya Services package (cs-services) installed.

AE Services installs the cust account in two places: in the local Linux password store and in the User Management service (local LDAP directory). This topic describes changing the default password for the cust account in User Management (the local LDAP directory). The User Management cust account provides access to the User Management features in OAM.

Note:
If you require a greater level of security for this account, see Appendix C, "Replacing the cust and avaya accounts," in the AE Services Administration and Maintenance Guide, 02-300357.

Follow this procedure to change the default password for the cust account in User Management (the local LDAP directory).

1. From a web browser, type the fully qualified domain name or IP address of the AE Services server. For example, myaes.example.com.

AE Services displays the Welcome page.

2. From the main menu, select AE Server Administration.

AE Services displays the log in screen, with the message, "Please log on."

3. Complete the log in screen:
   - In the Logon field, enter the default user name for the system administrator: cust.
   - In the Password field, enter the default password for the system administrator: custpw.
   - Click Login.

AE Services displays the AE Services OAM Home page.

4. From the main menu, select User Management > List All Users.

5. From the List All Users page, select the option button for craft and click Edit.

6. 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.
Upgrading and updating the AE Services software

7. Click **Apply**.
Appendix A: Enterprise-wide licensing

Use this appendix if you are setting up an AE Services configuration that uses enterprise-wide licensing. This section contains an overview of enterprise wide licensing and some basic procedures for working with enterprise wide licenses.

- **Installing the license file and configuring the Master WebLM Server** on page 79. This procedure applies to both enterprise wide licensing examples described in this chapter.

- **Changing the allocations of a license file** on page 84. If you are using a configuration where the Master WebLM server allocates licenses to Local AE Servers, you will need to follow this procedure for each of your local AE Servers. If use a configuration where the AE Server points to the master server, this procedure is not applicable.

- **Changing the allocations of a license file** on page 84. If you are using a configuration where the Master WebLM server allocates licenses to Local AE Servers, you will need to follow this procedure when you want to change the allocation of license features from one AE Server to another. If use a configuration where the AE Server points to the master server, this procedure is not applicable.

An overview of enterprise-wide licensing

Starting with Release 4.2, AE services supports enterprise-wide Licensing. With enterprise wide licensing, AE Services customers will be able to purchase any number of licenses and then allocate those licenses to various AE Servers at their own discretion. This means that AE Services customers will be able to pool or share all AE Services features, and Rights To Use (RTU) among AE Servers.

- To compare standard licensing with enterprise-wide licensing, see Table 4.
Enterprise-wide licensing

- For examples of licensing configurations, see Licensing configuration examples on page 75.

Table 4: Comparison of Standard licensing and Enterprise-wide licensing

<table>
<thead>
<tr>
<th>Standard Licensing</th>
<th>Enterprise-wide licensing</th>
</tr>
</thead>
<tbody>
<tr>
<td>AE Services has used the standard license file since the introduction of the platform (Release 3.0). The standard license file continues to be used for standalone AE server licensing.</td>
<td>AE Services introduces support for enterprise-wide licensing with Release 4.2.</td>
</tr>
<tr>
<td>A Standard License is generated by Remote Feature Authorization (RFA) from the system record for an AE Server</td>
<td>Enterprise-wide licensing includes a master enterprise license file (ELF) and an allocation license file (ALF).</td>
</tr>
<tr>
<td>- The master enterprise license file (ELF) file is generated by RFA from the system record from the enterprise. The master license file can reside on an AE Server or a dedicated WebLM server.</td>
<td></td>
</tr>
<tr>
<td>- The allocation license file (ALF) is generated by WebLM, based on features in the master license file and user allocations on the AE Server. The ALF or ALFs can reside on one or more AE Servers.</td>
<td></td>
</tr>
<tr>
<td>The standard license file is installed on the AE Server. In a standard licensing arrangement, AE Services and the WebLM server must be co-resident.</td>
<td>With enterprise wide licensing, WebLM does not have to be co-resident with AE Services.</td>
</tr>
<tr>
<td>With standard licensing, a license can not be moved from one server to another, and capacities can not be reallocated.</td>
<td>With enterprise-wide licensing, you can reallocate enterprise capacities and features as desired.</td>
</tr>
<tr>
<td>The standard license file contains the Avaya root certificate used by DMCC, CVLAN, and TSAPI.</td>
<td>Enterprise Wide License File contains the Avaya root certificate used by DMCC, CVLAN, and TSAPI.</td>
</tr>
</tbody>
</table>
Licensing configuration examples

To provide you with an idea of how licensing configurations work, this section about enterprise wide licensing includes a description of standard licensing.

Standard licensing

Prior to Release 4.2, AE Services supported Remote Feature Activation (RFA)-based Standard Licensing only. In a Standard Licensing configuration, the Standard license file (SLF) is installed on the AE Server and is controlled by the WebLM server running on the AE Server. For an illustration of Standard Licensing, see Figure 1.

If you use the standalone configuration, use the default settings on the WebLM Configuration page in AE Services OAM.

Figure 1: Standalone configuration (without enterprise Wide Licensing)

- AE Services OAM administration -- use default settings
- AE Services OAM administration -- use default settings

AE Server Administration
Administer WebLM IP address to point to local, standalone WebLM server
(use default - 127.0.0.1)

Standalone AE Server

AE Services acquire license

Local WebLM
127.0.0.1

Standard License File (SLF)
Enterprise-wide licensing -- allocating licenses or features

Starting with Release 4.2, AE Services expanded its licensing capabilities to include the RFA-based Enterprise Wide Licensing (EWL). With Enterprise Wide Licensing you have the flexibility to move capacities and features from one AE Sever to another. For example, prior to AE Services 4.2, if you had purchased 3 AE Servers with different licensing capacities, you could not move capacity purchased for one AE Server to another AE Server. With Enterprise wide licensing, you can move capacities or features from one server to another by using a Master WebLM Server to allocate license features to different AE Servers.

Because this configuration relies on a master enterprise license file (ELF), which generates allocation license files (ALF), it is referred to as an ELF/ALF configuration. Each ALF will reside on an AE Server with a Local WebLM Server. This is the recommended model for AE Services enterprise configurations. If you use the ELF/ALF model, you do not need to change the default settings on the WebLM Configuration page.

Figure 2: Enterprise licensing -- allocating licenses or features

Note: The IP addresses in this example are not valid IP address. They are used as examples only.

For information about setting up this type of configuration, see Setting up a configuration for allocating licenses on page 78.
Enterprise wide licensing -- pointing to a master license on a remote server

Another type of enterprise licensing configuration is referred to as an enterprise license file-only, (ELF) configuration.

In the ELF-only model, the enterprise license file resides on a master WebLM Server, and one or more AE Servers point to the IP Address of the master WebLM Server. No ALFs reside on AE servers.

If you use the ELF-only configuration, you must administer the WebLM Configuration page in AE Services OAM with the WebLM IP Address and WebLM Port number for the master WebLM Server that hosts the ELF.

The ELF-only configuration illustrated in Figure 3.

Figure 3: Enterprise wide licensing -- pointing to a master license on a remote server

Note: IP address 192.168.123.44 is used for purposes of this example. It is not a valid WebLM IP address.

⚠️ CAUTION: Using the ELF-only configuration is not recommended because network latency and outages can impact the AE Server’s ability to acquire licenses, and it creates a single point of failure for licensing.
Enterprise-wide licensing

Setting up a configuration for allocating licenses

Use the following procedures as an example for setting up a configuration for allocating licenses.

- Installing the license file and configuring the Master WebLM Server on page 79
- Changing the allocations of a license file on page 84
- Changing the allocations of a license file on page 84
Installing the license file and configuring the Master WebLM Server

This procedure applies to a configuration where the Master WebLM Server allocates licenses to Local AE Servers (see Figure 2: Enterprise licensing -- allocating licenses or features on page 76). You will need to use this procedure to install the master enterprise license (ELF) on the Master WebLM Server.

Follow these steps to install the enterprise license file (ELF) on the server that hosts the enterprise license file (ELF). This server can be an AE Server or a computer dedicated to WebLM.

1. Log in to the computer that has the license file stored on it.
2. From a web browser, type the fully qualified domain name or IP address of the AE Services server, for example:
   
   https://myaeserver.example.com

   In terms of this configuration example, the IP address would be 135.8.17.122.
3. On the Application Enablement Services welcome page, click WebLM Administration.
   
   Your browser displays the Web License Manager Log on screen.
4. Enter your WebLM user name and password, and click the arrow.
   
   WebLM displays the main menu and the Install License page.
5. Click Browse, which is next to the Enter License Path text box.
   
   Your system displays a dialog box that allows you to choose a file. Locate the license file and click Open. When you click Open, the file name will appear in the text box for Enter License Path box.
6. Click Install.
   
   WebLM uploads the license file to the WebLM server. When the process is complete, the server displays the message: License file installed successfully. Notice that the WebLM main menu, now displays Application_Enablement under Licensed Products.
7. From the WebLM main menu, select Application_Enablement > Configure Enterprise.
WebLM displays the Configure Enterprise page which provides settings for the enterprise license file (ELF).

8. Complete the Configure Enterprise page as follows:

   a. For the Master WebLM Configuration settings, which are required, accept the defaults.
      - Name: **Master WebLM Server**
      - Description: leave blank
      - IP Address: **127.0.0.1** (by default, it is set to the loopback address).

   b. For the Default Periodic Operation Settings settings, which are required, accept the defaults.

   c. For the SMTP Server Settings, which are optional, provide the name of the SMTP Server (Server Name), the user ID of the administrator (Admin Account), and the password of the administrator (Admin Password). These are the authentication settings for the SMTP server that sends email notifications for periodic operation failures.

   d. For the Email Notification Settings for Periodic Operation, complete the settings (Email Notification and Email Addresses) based on your operational requirements. By default, email notification is disabled (off).

   e. For the Default Periodic License Allocation Schedule, select the day and time, based on your operational requirements.

   f. For the Default Period Usage Query Schedule, select the day and time, based on your operational requirements.

   g. Click **Submit**.

This completes the procedure to set up the AE Server as the Master WebLM Server. After you have set up the Master WebLM Server, your next task is add a Local WebLM Server (or servers). Continue with **Adding a local WebLM server** on page 81.
Adding a local WebLM server

From the Master WebLM Server Web page, follow this procedure to add a Local WebLM Server.

**Note:**
You can allocate feature licenses only if the connection between the Master WebLM Server and the Local WebLM Server is validated and established.

1. From the WebLM main menu, select **Application Enablement**. Then select **Add Local WebLM**.

WebLM displays the Add Local WebLM page.

2. Complete the Add Local WebLM page as follows:

   - **Local WebLM Settings.**
     - Name: the `<name of the local AE Server>`, for example `lzbundled05`. (Although this name is required, it can be any name you choose).
     - Description: a descriptive term for the local AE Server (optional)
     - IP Address: `<IP address of the Local AE Server>`. For purposes of this example, the IP address is `135.8.17.123`.
     - Port: `443` (the default)
Enterprise-wide licensing

- Periodic License Allocation Schedule: Accept the defaults. Note that the default settings refer to the settings that you administered on the Master WebLM Server.
- Periodic Usage Query Schedule: Accept the defaults. Note that the default settings refer to the settings that you administered on the Master WebLM Server.

3. Click **Configure and Validate**.

This completes the procedure to add an AE Server as a Local WebLM Server.

Your next task is to log in to the Local WebLM Server and make sure that the WebLM Configuration page in AE Services OAM (CTI OAM > Administration > WebLM Configuration) is set up properly. Also, if this is the first time you are administering the Local WebLM Server, you will need to change the WebLM password. To carry out these tasks, see the next procedure, Setting up the Local WebLM Server in your configuration.

**Setting up the Local WebLM Server in your configuration**

Use the following procedure to change the default WebLM password and to verify the settings on the WebLM Configuration page in AE Services OAM.

1. From a web browser, type the fully qualified domain name or IP address of the WebLM server, and press **Enter**. For example:
   
   `https://myaeserver.example.com`
   
   In terms of this configuration example, the IP address would be **135.8.17.123**.

2. At the Security Alert, click **Yes** to accept the SSL certificate.

   Your browser displays the Application Enablement Services welcome page.

**WebLM Administration**

3. From the Welcome page, click **WebLM Administration**.

   Your browser displays the Web License Manager log in screen.

4. Log in to WebLM with default user name and password. The default user name is **admin**, and the default password is **weblmadmin**.

5. The first time you log in to WebLM, the WebLM server displays the Change Password page. Complete the fields on the Change Password page and click **Submit**.

   The password must contain 6 to 14 characters. White spaces are not permitted in the password, and the password itself must not be blank.

   The WebLM server displays the Web License Manager log in screen.

6. Log in as **admin** with the new password.

   WebLM displays the main menu and the Install License page.

7. From the main menu, select **Logout** to log out of WebLM.
AE Server Administration

8. Log on to the AE Services server (Local WebLM Server) again. For example, type the fully qualified domain name or IP address of the AE Services server, and press Enter.

   https://myaeserver.example.com

   In terms of this configuration example, the IP address would be 135.8.17.123.

9. At the Security Alert, click Yes to accept the SSL certificate.

   Your browser displays the Application Enablement Services welcome page.

10. From the Welcome page, click AE Server Administration.

    Your browser displays the AE Services log in screen.

11. Complete the log in screen and click Login.

    AE Services displays the OAM Home page.

12. From the main menu, select CTI OAM Administration.

    AE Services displays the CTI OAM Home page.

13. From the main menu, select Administration > WebLM Configuration.

    AE Services displays the CTI OAM Home page.

14. Verify that the WebLM Configuration page displays the following settings:

    ● WebLM IP Address: 127.0.0.1
    ● WebLM Port: 443

This completes the procedure to change the default WebLM password and to verify the WebLM Configuration settings on the Local WebLM Server.

Your next task is to log in to the Master WebLM Server, and allocate licenses to the Local WebLM Server. To carry out task, see Changing the allocations of a license file on page 84.
Changing the allocations of a license file

Master WebLM provides you with the ability to change license file allocations for your local WebLM Servers.

From the Master WebLM Server Web page, follow this procedure to change the license allocations.

1. From a web browser, type the fully qualified domain name or IP address of the WebLM server, and press Enter. For example:
   
   https://myaeserver.example.com
   
   In terms of this configuration example, the IP address would be 135.8.17.123.

2. At the Security Alert, click Yes to accept the SSL certificate.


   Your browser displays the Web License Manager Log on screen.

4. Enter your WebLM user name and password, and click the arrow.

   WebLM displays the main menu and the Install License page.

5. From the WebLM main menu, select Application Enablement. Then select Allocations.

6. WebLM displays the Allocations by Features page.

7. From the Allocations by Features page, click Change Allocations.
WebLM displays the Change Allocations page.

8. Enter an appropriate value in the New Allocation box and click Submit Allocations.

- For example, assume that you want to allocate 1 Application Enablement Connections license to the Local WebLM Server (lzbundled05 at IP address 135.17.123 in the example screen). Enter 1 in the New Allocations text box, and click Submit Allocations.

WebLM processes the allocation request, and displays the updated Allocations by Features page.

This completes the task to allocate license features to the Local WebLM Server.

Your final task is to log in to the Local WebLM Server, and verify that the license allocations that you administered are in effect. To accomplish this, see Verifying the license allocations on the Local WebLM Server on page 86.
Verifying the license allocations on the Local WebLM Server

Follow these steps to verify that the license allocations that you administered are in effect:

1. From a web browser, type the fully qualified domain name or IP address of the Local WebLM server, and press Enter. For example:
   
   https://myaeserver.example.com
   
   In terms of this configuration example, the IP address would be 135.8.17.123.

2. At the Security Alert, click Yes to accept the SSL certificate.
   
   Your browser displays the Application Enablement Services welcome page.

3. At the Security Alert, click Yes to accept the SSL certificate.
   
   Your browser displays the Application Enablement Services welcome page.

4. From the Welcome page, click WebLM Administration.
   
   Your browser displays the Web License Manager log in screen.

5. Log in to WebLM.
   
   WebLM displays the Install License page.

6. From the main menu, select Licensed Products > Application Enablement > Application Enablement.
   
   WebLM displays the license settings for the Local WebLM Server.

7. Verify that the Licensed Features on the Local WebLM server are consistent with the settings you administered on the Master WebLM Server.

   Note:
   
   The Allocation license is for valid up to 30 days. The master WebLM will push the ALF to the local WebLM based on the administered schedule (Periodic License Allocation Schedule).
Appendix B: Configuring an LDAP server for User Management

This appendix describes how to manually configure a Lightweight Directory Access Protocol (LDAP) server for User Management.

This appendix assumes the following:

- You have installed the AE Services server software, which installs the cs-userservice (to verify use `rpm -q cs-userservice`)
- During the software installation procedure you cleared the `cs-cusldap` option (see Step 11 of Installing the AE Services server software on page 20).
- Your LDAP implementation is based on an OPEN LDAP server of version 2.1.22-28 or later.

Configuring the LDAP server

To manually configure your LDAP server for User Management:

1. Copy the mvapus schema file (`mvapus.schema`) from `/var/mvap/config/cus` to the LDAP schema directory (`/etc/openldap/schema`).
2. Edit the `/etc/openldap/schema/core.schema` file:
   a. Locate the `userid` attribute specification section.
   b. Add the following specification element:
      
      ```
      after the EQUALITY caseIgnoreMatch line, add
      ORDERING caseIgnoreOrderingMatch
      ```
   c. Save the schema file.
3. Edit the `/etc/openldap/slapd.conf` file.
   a. Add the following include statement to the already existing set of `\include statements`:
      ```
      include /etc/openldap/schema/mvapus.schema
      ```
   b. Note the suffix value used in the current slapd.conf file
   c. Save and close the slapd.conf file.
4. Modify the init.ldif file to match the chosen organizationalUnit for the \users and the existing suffix used by the enterprise:
   a. Eliminate the first entry in the init.ldif file.
   b. Revise the second entry to reflect the desired organizationalUnit (ex. ou=users)
   c. Revise the DN attribute of the next two entries to reflect the chosen organizationalUnit and suffix in use in the enterprise.
   d. Save and close the init.ldif file.
5. Restart the LDAP server.
6. Use the ldapadd tool or equivalent to add the entries in the ldif.init file into the LDAP server:

   ldapadd -x -D bind credentials DN -W -f init.ldif

---

### Create an LDAP User account

You must now create an LDAP user account for the user service. This account must have privileges to add, modify, and delete avayauser class entries in the specified region of the Directory Information Tree (DIT).

To create and administer an LDAP User account:

1. Open the /var/mvap/config/cus/user.properties file for editing.
2. Edit the LDAP storage section to reflect the LDAP configuration work completed in Configuring the LDAP server on page 87:
   a. Set the LDAP provider to the correct host and suffix combination.
   b. Set the userroot property to the suffix value in use.
   c. Set the principal to the DN of the LDAP you created in Configuring the LDAP server on page 87.
   d. Set the password attribute to the generated encrypted value.
      
      Run /usr/share/tomcat5/webapps/axis/WEB-INF/lib/makepassword.sh against the plain text password furnished by the enterprise LDAP administrator for the User account you created.
   e. Set the orgunit property to the organizationalUnit selected for the user data space.
3. Save and close the modified user.properties file.
4. Make identical changes to the corresponding properties in the var/mvap/config/cus/ldapfilter.properties file.
5. If the relevant Tomcat/Axis server has not already deployed the User Management service, deploy the service:
   a. Verify the Tomcat service is running.
   b. Go to:
      /usr/share/tomcat5/webapps/axis/WEB-INF/lib/
   c. Run the `org.apache.axis.client.AdminClient` application against the cusdeploy.wsdd file.
      For example:
      ```java
      java -classpath Axis jar files org.apache.axis.client.AdminClient cusdeploy.wsdd
      ```

6. Restart the Tomcat service that is the container for the user service.
Appendix C: Setting up remote access

Avaya technical support (Services) personnel require remote access to the AE Services server to do administration and maintainance. A remote access setup requires:

- a modem and supporting administration to be set up on the AE Services server
- a modem and suitable software to be installed on the client computer that is to access the AE Services server

Note:
This information in this appendix applies only to customers who have an Avaya maintenance or service contract for their AE Services server.

Information in this appendix includes:

- Setting up remote access on the AE Services server on page 92
- Setting up a client to dial in to the server on page 94

Figure 4 illustrates a remote access setup.

Figure 4: Remote access configuration
Setting up remote access on the AE Services server

This section describes how to set up an AE Services server to support remote access.

Note:
This section describes an example setup. You might need to modify these instructions depending on the type of modem you are using.

To set up a Linux computer to support remote access, you require:

- A Linux computer with the default Red Hat Enterprise Linux (RHEL) software components already installed
- A Red Hat Enterprise Linux-compatible modem
- The following software components to be installed before you continue:
  - ppp - Point-to-Point Protocol software
  - mgetty - a program that handles modem communications

To configure the Linux computer to support remote access:

1. Edit the /etc/inittab file:
   a. Using a text editor such as vi or emacs, open the /etc/inittab file.
   b. Add one line for each modem you plan to use. For example, you might type:

   ```
   S0:2345:respawn:/sbin/mgetty -D ttyS0
   ```

   where:
   -D is the parameter for a data modem.
   ttyS0 is the device identifier. This value varies according to your hardware. For example, ttyS0 is associated with COM1 and ttyS1 is associated with COM2.

   Note:
   ttyS0 identifies a serial modem. Modify these instructions as required if you are using a different type of modem.

2. Edit the login.config file:
   a. Open the /etc/mgetty+sendfax/login.config file.
   b. Edit the file by uncommenting the AutoPPP line. Edit the line to include a reference to the options file by specifying file /etc/ppp/options. For example:

   ```
   /AutoPPP/ - a_ppp /usr/sbin/pppd file /etc/ppp/options
   ```

3. Edit the pap-secrets file to set up Password Authentication Protocol (PAP) authentication:
   a. Open the /etc/ppp/pap-secrets file.
b. Edit the file so it consists of one line containing the following characters: * * " " *  
For example:

```
# Secrets for authentication using PAP
# client   server   secret    IP address
      *        *        "      "
```

These settings enable any registered user to log in. Alternatively, you could specify user names, passwords, and IP addresses.

4. Edit the options file for the modem to include a `<serverIP>:<clientIP>` entry:

a. Open the appropriate options file for your modem. For example, if your modem is connected to ttys0, open the `/etc/ppp/options.ttyS0` file.

b. Edit the options file to include a `<serverIP>:<clientIP>` entry for each tty. You must include the colon between the server IP address and the client IP address.

The default `<serverIP>:<clientIP>` entry for each tty is:

```
Server IP   Client IP
192.168.25.10:192.168.25.20
```

5. Verify PPP options:

a. Open the `/etc/ppp/options` file.

b. Verify that the client PPP supports the options specified in Table 5.

c. Edit the file if necessary.

### Table 5: PPP option settings for remote access

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lock</td>
<td>Creates a lock file that has exclusive access to a specific device.</td>
</tr>
<tr>
<td>-detach</td>
<td>Prohibits the pppd process from forking and becoming a background process.</td>
</tr>
<tr>
<td>modem</td>
<td>Sets up the server to use modem control lines. The client waits for a signal from the modem before opening a serial device (default behavior). You can change this handshake if necessary.</td>
</tr>
<tr>
<td>crtscts</td>
<td>Specifies hardware flow control.</td>
</tr>
<tr>
<td>proxyarp</td>
<td>Lets the client appear as if it is on the same LAN as its peers.</td>
</tr>
<tr>
<td>asyncmap 0</td>
<td>Prohibits the pppd process from setting up and using escape control sequences.</td>
</tr>
</tbody>
</table>
Setting up remote access

Setting up a client to dial in to the server

You must set up the remote computer to dial in to the AE Services server. The procedures vary depending on the type of client computer. This section contains tips for setting up the two most frequently used clients.

Linux client

To establish a PPP connection to the AE Services server from a Linux client, use either the GNOME or KDE Dialer. The specific procedure varies depending on the version of Linux you are using.

Microsoft Windows client

To establish a PPP connection to the AE Services server from a Microsoft Windows client, use the network connections setup appropriate for your version of Windows.

For example, to configure a dial-up connection in Windows XP:

1. Click Start > Control Panel > Network Connections.
2. Click Create a connection to the network at your office.
3. In the Location Information dialog box, enter the appropriate information. Click OK.
4. Click OK to close the Phone and Modem Options dialog box and start the New Connection wizard.
5. In the New Connection Wizard, click Dial-up connection, and then click Next.
6. Complete the wizard. When you are done, click Finish.

PPP connection requirements

Verify the PPP connection requirements and administer them accordingly. For example:

- For an AE Services software-only offer, you must administer a login and password on the AE Services server for the client connection. By default, no login and password are administered to support remote access.

- You must administer an IP address for the client connection. The default Client IP address is 192.168.25.20.
Index

A

About AE Services page .................................. 27
administering AE Services .............................. 37
AES server
    hostname ........................................ 8, 16, 34, 35
    remote access ................................... 92
    requirements ..................................... 7
    software installation ............................. 19
AES server software
    obtaining AES software ........................... 19
AES software
    administering for Communication Manager ... 37
    Ethernet ports required ........................ 16
    files, logs and directories ...................... 27
    installing ....................................... 20
    licensed services ................................ 32
    restarting ....................................... 33
    updating ......................................... 67
Application Enablement Services, see AES
    auto-negotiated settings ......................... 64

B

Backup Database page .................................. 53

C

CD
    AES software installation ........................ 20
    upgrade .......................................... 55
Change Password page in WebLM .................... 30, 82
Choose Installation Method screen ................ 23, 60
Choose Installation Packages screen ............. 23, 61
CIRS, see Customer Infrastructure Readiness Survey
    client application computer
        requirements .................................... 8
    client computer
        remote access setup .......................... 94
        requirements ................................ 91
    clock setting for AE Services .................. 16, 63
    commands
        ifconfig for MAC address ..................... 35
        updates ...................................... 68
Communication Manager
    administering for AE services ................. 37
    Processor Ethernet interface .................. 12
    requirements .................................. 9, 13

database
    back up .......................................... 53, 68
    LDAP ............................................. 54
    restore ......................................... 65
delays on communications channel ................. 12
dial in to server ................................ 94
dual-NIC configuration ............................... 35
duplex settings for AES ............................ 13

eclipse
    Enter RPM URL screen ............................ 21, 59
    error messages
        installation .................................. 28
        WebLM ....................................... 34
ethernet interfaces
    on SAMP ........................................ 33, 54, 55, 65, 68, 69
    on server ....................................... 8, 35
Ethernet ports required for AES .................. 16

F

files and directories for AE Services ............. 27

H

hardware
    MAC address ...................................... 35
    requirements .................................. 7, 8
Help page ............................................ 27

I

identifying the MAC address ......................... 35
installation
    AES software ................................... 19
Index

initial administration ........................................... 37
license file ...................................................... 29, 32
log files ......................................................... 25, 28
PPP connection ................................................... 94
prerequisites ....................................................... 7
required software ............................................... 15
requirements ..................................................... 7, 8
start installer program .......................................... 21
troubleshooting ................................................... 27
updates and patches .............................................. 67
installation screens
choose Installation Method screen ............................. 23, 60
Choose Installation Packages ................................ 23, 61
co-residency warning page ..................................... 22, 60
enter RPM URL .................................................... 21, 59
optional packages, including LDAP ......................... 23, 61
Select Installation Media ....................................... 21
select Release Version screen ................................. 22, 60
successful or failed screen ...................................... 25, 62
Installation/Update Successful or Failed screen ........... 25, 62
interface speed for AES ........................................ 13
IP Migration Readiness and Optimization analysis ......... 13
ISO image ......................................................... 20
mounting .......................................................... 20
obtaining .......................................................... 19

K
kernel parameter to specify clock ............................. 16, 63

L
laptop computer
connecting to server .............................................. 33, 54, 55, 65, 68, 69
LCS performance requirements ................................. 8
LDAP
configuring for User Management ............................ 87
creating a user account ......................................... 88
database ........................................................... 54
installing on server ............................................. 24
license file for AES
installing .......................................................... 29, 32
MAC address ...................................................... 35
obtaining .......................................................... 29, 35
removing an existing file ........................................ 30
required information ............................................ 35
requirements ....................................................... 25, 51, 65
troubleshooting ................................................... 34
upgrades .......................................................... 65
verify settings ..................................................... 32
WebLM ............................................................ 30
Licensed Products page for Application Enablement
licenses
AE Services ....................................................... 29, 37
third-party software ............................................. 10
Linux client, remote access setup ............................ 94
Linux commands
swversion ........................................................ 64, 67, 68
uname ............................................................ 6
Linux software
disk partitioning .................................................. 15
firewall configuration .......................................... 16
installing platform software .................................. 15
minimal installation ............................................. 15, 16
optimizing for AES ............................................. 15
required software ............................................... 15, 92
upgrading ........................................................ 63
version required ................................................ 9
log files
location .......................................................... 27, 28
troubleshooting ................................................... 25
log in
as user with root privileges ................................ 33
to OAM ........................................................... 27, 33, 42, 46
to WebLM ........................................................ 30, 35

M
MAC address for license file ................................... 35
media directory ................................................... 9, 20, 55
media server requirements ..................................... 9, 12, 13
Microsoft Windows client, remote access setup .......... 94
modem for remote access ....................................... 91
mount
CD ............................................................... 20, 55
ISO image ........................................................ 20

N
NANO, see network analysis ................................... 13
network
analysis .......................................................... 13
interface speed and duplex settings ......................... 13, 64
latency requirements .......................................... 12, 11
requirements ..................................................... 11
NIC
Ethernet interface for technician ......................... 33, 54, 55, 65, 68, 69
Ethernet interfaces ............................................. 8
manually adjust settings ....................................... 64
NIC Configuration page ........................................ 64

O
OAM
home page ........................................................ 27, 33, 42, 46
required software ............................................... 10
restarting AE Services ......................................... 33
operating system
Linux installation ............................................... 15

96  AE Services Installation and Upgrade Guide for Software-Only Offer R4.2
### Index

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>improve reliability</td>
<td>8</td>
</tr>
<tr>
<td>setup</td>
<td>15</td>
</tr>
</tbody>
</table>

**W**

WebLM

- error messages                      | 34   |
- logging in                          | 30, 35 |
- white paper on AES security         | 14, 16 |