# Implementing Avaya one-X® Client Enablement Services

Release 6.1 SP3
v1.0
October 2012

**Notice**

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

**Documentation disclaimer**

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

**Link disclaimer**

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

**Warranty**

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

**Licenses**

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

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

**License type(s)**

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

Shrinkwrap License (SR). Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”). (see “Third-party Components” for more information).

**Copyright**

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

**Third-party components**

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

The open source license text file, `OpenSourceLicense.txt`, is available in the Licenses folder on the Avaya one-X® Client Enablement Services server: `/Licenses/OpenSourceLicense.txt`.

**Preventing Toll Fraud**

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

**Avaya Toll Fraud Intervention**

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll

Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

**Trademarks**

Avaya, the Avaya logo, Avaya one-X® Client Enablement Services, Communication Manager, Modular Messaging, and Conferencing are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

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

**Downloading Documentation**

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

**Contact Avaya Support**

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

## Contents

# Chapter 1: Introduction

## Purpose of this document

This guide provides information for implementing Avaya one-X® Client Enablement Services.

Use this guide to:

- Install the Client Enablement Services Release 6.1 SP3 template
- Upgrade Client Enablement Services from any previous release to Release 6.1 SP3
- Install, configure, and upgrade the Handset Server
- Install, configure, and upgrade the Transcoding Server
- Troubleshoot issues that you encounter during the Client Enablement Services template installation

**Note:**

After you complete the template installation, you must setup Client Enablement Services. For more information, see *Administering Avaya one-X® Client Enablement Services*.

## Related documents

Use the appropriate user documentation to obtain specific information to plan, install, administer, troubleshoot, and maintain your Client Enablement Services system. You can download these documents from the Avaya Support Web site at http://www.avaya.com/support.

- *Avaya one-X® Client Enablement Services Overview*
- *Administering Avaya one-X® Client Enablement Services*
- *Avaya one-X® Client Enablement Services Online Help for administrators*
- *Avaya one-X® Communicator User Guide*
- *Avaya one-X® Communicator Online Help for users*
- *Avaya Online Help for centralized administration tool*
- *Avaya one-X® Mobile Android User Guide*

- *Avaya one-X® Mobile Blackberry User Guide (touch screen model)*
- *Avaya one-X® Mobile Blackberry User Guide (non-touch screen model)*
- *Avaya one-X® Mobile iPhone User Guide*

Before you install or upgrade Avaya products, check the Avaya Support Web site for the latest information.

# Avaya one-X® Client Enablement Services

Client Enablement Services is the first of a new series of next-generation applications that brings Unified Communications (UC) to your desktop and mobile handsets in a single tool. Use Client Enablement Services to access multiple Avaya UC capabilities, including Telephony, Messaging, Mobility, Conferencing, and Presence Services. With Client Enablement Services, you do not need multiple applications to access the features provided by Avaya Aura® Communication Manager, Avaya Aura® Presence Services, Avaya Modular Messaging or Avaya Aura® Messaging or Avaya Aura® Communication Manager Messaging, and Avaya Aura® Conferencing.

In Client Enablement Services, the UC clients of Avaya one-X® Communicator and Avaya one-X® Mobile work with a single server. The Client Enablement Services server delivers continuous subscriber data and provides a consistent user experience. Client Enablement Services supports a thick client and mobile interface to gain access to the functionality supported on the server.

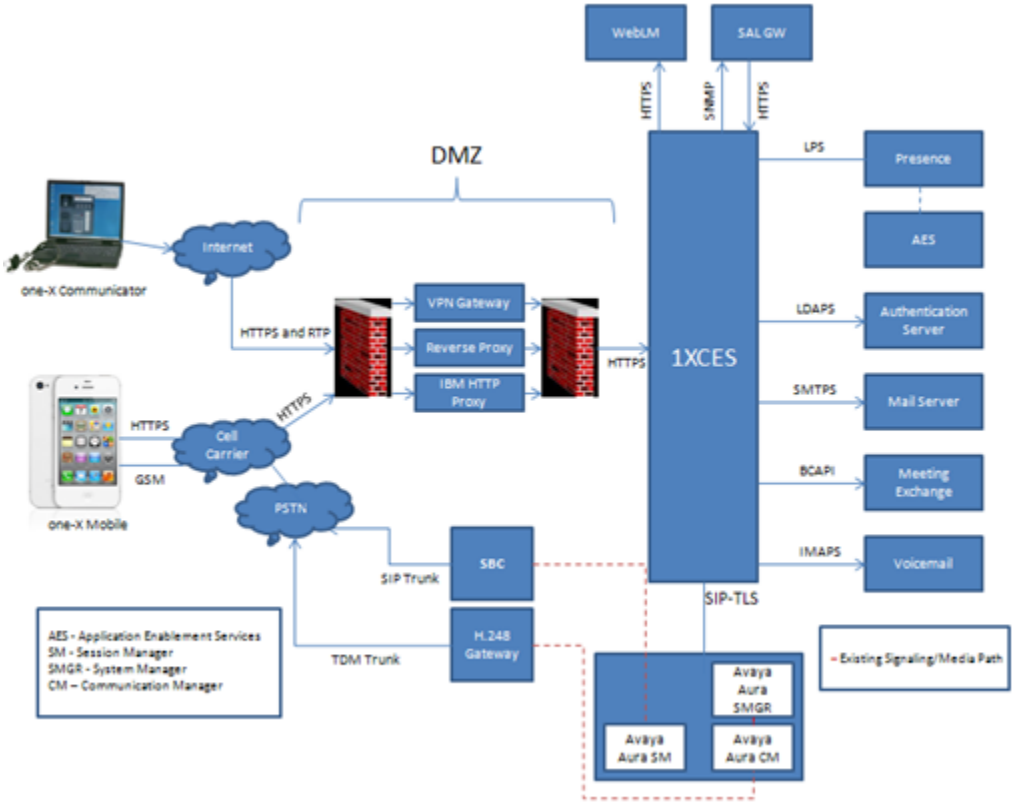
Avaya one-X® Communicator provides the softphone capability. Use Avaya one-X® Communicator to manage the communications tasks in your enterprise. Avaya one-X® Communicator provides a simple, intuitive access to your daily communications tools.

The UC features of Avaya one-X® Communicator include visual voice mail to filter and sort voice messages. Use the visual voice mail feature to respond to important messages quickly. Communication History logs help you trace the history of your enterprise calls and voice messages. Use Avaya one-X® Communicator to increase the productivity of your enterprise with tools that enhance collaboration, improve responsiveness, and lower costs for IT and end-user support.

Avaya one-X® Mobile provides seamless access to voice messaging and corporate directories while using a mobile device. Avaya one-X® Mobile equips your mobile phone with access to your office telephone system. Regardless of your work location, you can receive and make calls to and from your desk phone number, review voice mail messages, look up information in your enterprise directory, and even block calls.

# Avaya one-X® Client Enablement Services architecture

The architecture diagram shows the relationship between the Client Enablement Services server and the servers and clients with which Client Enablement Services integrates.




# Templates overview

Avaya offers product-specific templates to install different products on System Platform. A template is a definition of a set of one or more applications that you can install on System Platform. Client Enablement Services provides the following templates:

- `onexps_template_16GB.ovf`: If you are installing Client Enablement Services on a system that has 16 GB of RAM or more, you must use this template.
- `onexps_template_24GB.ovf`: If you are installing Client Enablement Services on a system that has 24 GB of RAM or more, you must use this template.

**Note:**

All templates have the same functionality. Select a template depending on the RAM of the system.

However, if you are using a Dell server with a minimum RAM of 24 GB, you must use the `onexps_template_24GB.ovf` template.

You can install the Client Enablement Services template from one of the following locations. Use the option that works best in a specific customer scenario.

- **Avaya Downloads (PLDS)**: The template files are located in Avaya PLDS. The list contains all templates to which your enterprise is entitled. Each line in the list begins with the *sold-to* number so that you can select the appropriate template for the site where you are installing Client Enablement Services. Hold the mouse pointer over the selection to view more information about the *sold-to* number. The PLDS are available at http://plds.avaya.com.
- **HTTP**: The template files are located on an http server. You can install the template files from the http server to several System Platform servers. You must enter the template URL information.
- **SP Server**: The template files can be copied to the `/vsp-template` file system in the Console Domain of the System Platform server.
- **SP CD/DVD**: The template files are located in the DVD supplied with the system or the DVD created onsite.

**Note:**

If you plan to install the Client Enablement Services template files from a DVD, then you must use a Double-Layer DVD media so that the template files fit into a single DVD.

- **SP USB Disk**: The template files are located in a USB flash drive connected to the server. The format of the USB flash drive must be ext3.

**Note:**

If you plan to install the Client Enablement Services template files from a USB, then you must ensure that the template files fit into a single USB.

# Deployment checklist

Use the following checklist to install Client Enablement Services. As you complete a task, make a check mark in the ✔ column.

| ✔ | Task | References | Notes |
|---|---|---|---|
| | Download required documentation. | See Related documents on page 9. | |
| | Gather preinstallation data. | See Preinstallation data gathering on page 21. | |
| | Verify that all equipments are on-site. | See Chapter 2: Prerequisites. | Do not rely on the packing slip for correct information. Instead, |

| ✔ | Task | References | Notes |
|---|---|---|---|
| | | | compare the inventory list of hardware and components that you ordered with the contents of the shipping boxes. If you find any discrepancy between the inventory list and the contents of the shipping boxes, immediately inform Avaya. |
| | Obtain one of the following servers, as appropriate:<br>• Dell™ PowerEdge™ R610 Server<br>• HP ProLiant DL360 G7 Server | See<br>• *Installing the Dell PowerEdge R610 Server*<br>• *Installing the HP DL360 G7 Server* | |
| | Obtain and install System Platform on the server. | For more information, see *Installing and Configuring Avaya Aura System Platform*. | |
| | Obtain the Client Enablement Services template. | See Templates overview on page 11. | |
| | Use the System Platform Web Console to install the Client Enablement Services template. | See Installing a solution template on page 50. | |
| | Set up Client Enablement Services. | For more information, see *Administering Avaya one-X® Client Enablement Services*. | |

# Chapter 2: Prerequisites

## Availability

**Note:**

Client Enablement Services is not customer installable. Only Avaya technicians or Avaya one-X® Client Enablement Services certified business partners are authorized to perform the installation of Client Enablement Services. For more information, please contact Avaya Support.

You can download the software-only solution of Client Enablement Services and the Avaya-provided complete solution through the Avaya Product Licensing and Delivery System (PLDS).

### Software-only solution

Avaya provides the following components:

- Internal Client Enablement Services database
- Client Enablement Services applications
- Avaya Aura® System Platform
- Avaya WebLM
- Secure Access Link Agent
- Secure Access Link Gateway

**Note:**

Client Enablement Services does not support any customer provided equipment (CPE) that meets the required hardware specifications. For the list of supported servers, see Hardware requirements on page 22.

### Avaya-provided complete solution

Avaya provides the following components:

- Dell R610 and HP DL360G7 servers
- Internal Client Enablement Services database
- Client Enablement Services applications
- Avaya Aura® System Platform

- Avaya WebLM
- Secure Access Link Agent
- Secure Access Link Gateway
- Handset Server
- IHS

## Avaya components

**Note:**

The versions of Avaya and third-party products mentioned in this guide are likely to change as Avaya tests and certifies later versions of supported products. To know about the latest versions of products that Client Enablement Services supports, see the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Client Enablement Services supports the following Avaya components:

| Avaya Components | Software or Hardware | Version |
|---|---|---|
| PBX | Communication Manager | 5.2.1 SP11 |
| | | 6.0* |
| | | 6.0.1 SP6 |
| | | 6.2 SP3 |
| Session Manager | Session Manager | 6.0 |
| | | 6.1 SP7 |
| | | 6.2 SP1 |
| System Manager | System Manager | 6.1 SP7 and 6.2 SP1 |
| System Platform | System Platform | 6.0 Build 6.0.3.0.3 with Patch 6.0.3.9.3 |
| Presence | Presence Services | 6.1 SP3 |
| Messaging | Avaya Modular Messaging | 5.2 SP6 |
| | Avaya Aura® Messaging | 6.0 |
| | | 6.0.1 |
| | | 6.1 SP1 |
| | | 6.2 |
| | Communication Manager Messaging | 6.2 |

| Avaya Components | Software or Hardware | Version |
|---|---|---|
| Conferencing | Avaya Aura Conferencing Standard Edition<br>In Release 5.2, Avaya Aura Conferencing Standard Edition was named as Avaya Meeting Exchange™ Enterprise Edition. | 5.2.1 |
| | | 6.0 |
| Speech | Avaya one-X® Speech | 5.2.x |
| SIP Hard Phones | Avaya SIP 2.6 | 9620 |
| | | 9620C |
| | | 9620L |
| | | 9630 |
| | | 9630G |
| | | 9640 |
| | | 9640G |
| | | 9650 |
| | | 9650C |
| | Avaya SIP 6.0 | 96x1 [9601, 9608, 9611G, 9621G, and 9641G] |
| | | 14xx and 16xx |
| H.323 Hard Phones | Avaya H.323 | 9620C |
| | | 9620L |
| | | 9630 |
| | | 9630G |
| | | 9640 |
| | | 9640G |
| | | 9650 |
| | | 9650C |
| | | 96x1 [9601, 9608, 9611G, 9621G, and 9641G] |
| | | 46xx |
| Avaya Soft Clients | Avaya one-X® Communicator | 6.1 SP5 |
| | Avaya one-X® Portal | 5.2 SP4 |

| Avaya Components | Software or Hardware | Version |
|---|---|---|
| | Avaya one-X® Mobile for iPhone | 6.1 SP3 |
| | Avaya one-X® Mobile for Android | 6.1.2 SP1 |
| | Avaya one-X® Mobile for BlackBerry | 6.1.2 SP1 |

**Note:**

* Client Enablement Services does not support Communication Manager 6.0 Feature Server implementation.

**Important:**

Limitations exist in the interoperability between Avaya one-X® Portal and Client Enablement Services clients. For information about interoperability, see the *one-X Client Enablement Services and one-X Portal Client Interoperability* section in the *Avaya one-X® Client Enablement Services Release Notes* document.

## Third-party components

**Note:**

The versions of Avaya and third-party products mentioned in this guide are likely to change as Avaya tests and certifies later versions of supported products. To know about the latest versions of products that Client Enablement Services supports, see the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

Client Enablement Services supports the following third-party components.

| Third-party Components | Software or Hardware | Version |
|---|---|---|
| Server OS | Linux | RHEL, part of the Client Enablement Services template. |
| Handset Server OS | Linux | RHEL 5.8 |
| Administration Browser | Microsoft Internet Explorer | 7.0 |
| | | 8.0 |
| | Mozilla Firefox | 3.6 |
| | Apple Safari | 5.x |
| LDAP | Microsoft Active Directory | 2003 R2 |
| | | 2008 R2 |

| Third-party Components | Software or Hardware | Version |
|---|---|---|
| | Microsoft ADAM | 2003 |
| | | 2008 – Active Directory Lightweight Directory Service (AD LDS) |
| | IBM Domino Server | 8.5.3 |
| | Novell eDirectory | 8.8 SP7 |
| | SUN Directory Server Enterprise Edition | 6.3.1 |
| | | 7.0 |
| Mobile Device Platforms | iPhone (Apple) | 4.3+, 5.0, and 6.0 |
| | BlackBerry (RIM) | 5.0+, 6.0+, and 7.0 |
| | Android | 2.2+ and 4.0 |
| Handsets | iPhone (Apple) | 3G, 3GS, 4, and 4S |
| | BlackBerry (RIM) | Bold - 9000, 9650, 97xx, and 99xx |
| | | Curve - 8520, 8530, 8900, and 9300 |
| | | Torch 9800 |
| | | Storm 9550 |
| | Android | Motorola - Droid 2, A953, and Atrix4G |
| | | HTC - MyTouch 4G, Desire HD, Desire S, and Evo 4G |
| | | LG - Revolution and Optimus 3D |
| | | Samsung - Galaxy, Galaxy S, Galaxy SII, and Nexus |
| | | Dell - Streak 5 and Venue |

# Preinstallation checklist

Use the following checklist to ensure that the prerequisites for installing Client Enablement Services are complete. As you ensure that a task is complete, make a check mark in the ✔ column.

| ✔ | Task | References | Notes |
|---|---|---|---|
| | Gather preinstallation data | See Preinstallation data gathering on page 21 | |
| | Check for environmental requirements | See Safety instructions on page 21 | |
| | | See Clearance requirements on page 22 | |
| | Check for hardware requirements | See Hardware requirements on page 22 | |
| | | See Avaya-provided equipment on page 24 | |
| | | See Customer-provided equipment on page 24 | |
| | Check for software requirements | See Software requirements on page 25 | |
| | | See Software requirements for features on page 25 | |
| | Check for network requirements | See Time synchronization requirements on page 28 | |
| | Check for licensing requirements | See Licensing requirements on page 29 | |
| | | See Location of the Avaya Web License Manager on page 29 | |
| | | See Product software and licenses on page 30 | |
| | | See Host ID on page 30 | |
| | Check for security requirements | See Security requirements on page 31 | |
| | | See Additional security information on page 32 | |
| | Configure Enterprise Directory | See Enterprise Directory integration guidelines on page 32 | |
| | Generate SMGR Enrollment Password | Generating the SMGR Enrollment Password on page 38 | |

# Preinstallation data gathering

You must fill data in several fields while installing and configuring Client Enablement Services. If you have the information required for these fields ahead of time, your installation will be faster and accurate.

Before you install Client Enablement Services:

- Distribute the appropriate checklists to your network administrator.
- Verify that your network infrastructure fulfills the hardware and software infrastructure prerequisites.

To ensure that you gather all the required data before the installation, fill out the installation worksheet for installing Client Enablement Services. SeeInstallation worksheet: information required by template installation on page 41.

# Environmental requirements

## Safety instructions

Use the following safety guidelines to ensure your own personal safety and to help protect your system and working environment from potential damage.

Observe the following precautions for rack stability and safety. Also refer to the rack installation documentation accompanying the rack for specific caution statements and procedures.

Systems are considered to be components in a rack. Thus, *component* refers to any system as well as to various peripherals or supporting hardware.

**⚠ Danger:**

- Before installing systems in a rack, install front and side stabilizers on stand-alone racks or the front stabilizer on racks that are joined to other racks. Failure to install stabilizers before installing systems in a rack could cause the rack to tip over, potentially resulting in bodily injury.
- After installing components in a rack, never pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in serious injury.
- Use caution when pressing the component rail release latches and sliding a component into or out of a rack because the slide rails can pinch your fingers.

**Note:**

- Your system is safety-certified as a free-standing unit and as a component for use in a rack cabinet using the customer rack kit. It is your responsibility to ensure that the final combination of system and rack complies with all applicable safety standards and local electric code requirements.
- System rack kits are intended to be installed in a rack by trained service technicians.

**Important:**

- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a component from the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack:
  - Do not block any air vents. Usually 15 cm (6 in.) of space provides proper airflow.
  - Install the server only in a rack cabinet with perforated doors.
  - Do not leave open spaces above or below an installed server in your rack cabinet. To help prevent damage to server components, always install a blank filler panel to cover the open space and to help ensure proper air circulation.
- Do not step on or stand on any component when servicing other components in a rack.
- Do not place any object on top of rack-mounted components.

## Clearance requirements

Install the server in a rack that meets the following requirements:

- Minimum depth of 70 mm (2.76 inches) between the front mounting flange and inside of the front door if the server is installed in a cabinet.
- Minimum depth of 157 mm (6.18 inches) between the rear mounting flange and inside of the rear door if the server is installed in a cabinet.
- Minimum depth of 718 mm (28.27 inches) and maximum depth of 762 mm (30 inches) between the front and rear mounting flanges to support the use of the cable-management arm.

# Hardware requirements

This section covers the minimum hardware requirements for the Client Enablement Services server. If you expect Client Enablement Services to handle a high volume of traffic, you must

provide hardware with more memory and a faster processor. Contact your Avaya representative or Avaya Business Partner representative for assistance with sizing a Client Enablement Services system.

The Client Enablement Services server must meet the following minimum hardware specifications:

**CPU** Dual quad-core processors (2.4 GHz or higher)

**Memory** 24 GB of RAM

**Hard drive** 4 * 146 GB (RAID 5)

**Network card** 100 Mbps / 1Gbps

**Optical drive** DVD/CD combination drive (Optional)

Client Enablement Services currently supports the Dell R610, HP DL360G7, and S8800 servers.

You must deploy Client Enablement Services on an Avaya provided common hardware platform to ensure optimal performance and hardware continuity for future software releases. Client Enablement Services supports older S8800 platforms provided you upgrade the S8800 server to meet the minimum specification outlined in the following table:

| Hardware requirements | Dell R610 | HP DL360G7 | S8800 (Upgrade required) |
|---|---|---|---|
| CPU | Dual quad-core processors of 2.4 Ghz. | Dual quad-core processors of 2.4 Ghz. | 2 * 2.2 Ghz or higher.<br>Single processor models are not supported. |
| Memory | 24 GB. | 24 GB. | 16 GB.<br>Requires 10 GB upgrade from the 6 GB default factory configuration. |
| Hard Drive | 4 * 146 GB RAID 5. | 3 * 300 GB RAID 5. | 4 * 146 GB.<br>Requires 2 * 146 GB upgrade from the 2 * 146 GB default factory configuration. |
| Network Card | 100 Mbps / 1Gbps. | 100 Mbps / 1Gbps. | 100 Mbps / 1Gbps. |
| Optical Drive | DVD/CD combination drive is optional. | DVD/CD combination drive is optional. | DVD/CD combination drive is optional. |

**Note:**

The versions of Avaya and third-party products mentioned in this guide are likely to change as Avaya tests and certifies later versions of supported products. To know about the latest versions of products that Client Enablement Services supports, see the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

## Avaya-provided equipment

Avaya provides the following equipment:

- Server and power cord
- Slide rails
- Cable management arm assembly
- Cable management arm stop bracket
- Cable management arm mounting bracket
- Cable management support arm
- Two 10–32 screws
- Four M6 screws
- Five small cable ties
- One large cable tie
- Other hardware as ordered, such as uninterruptible power source (UPS).

## Customer-provided equipment

The customer must provide the following equipment:

- Standard 19-inch four-post equipment rack that is properly installed and solidly secured. The rack must meet the following standards:
  - American National Standards Institute and Electronic Industries Association standard ANSI/EIA-310–D-92.
  - International Electrotechnical Commission standard IEC 297
  - Deutsche Industrie Norm standard DIN 41494
- Screws that come with the racks for installing the rails
- #2 cross-point (Phillips) screwdriver or 3/8 inch flathead screwdriver
- USB keyboard, USB mouse, and monitor must be available on the site for advanced installation or troubleshooting.
- Power from a nonswitched electrical outlet
- Access to the network

# Software requirements

Install the following software before installing Client Enablement Services:

**Note:**

The versions of Avaya and third-party products mentioned in this guide are likely to change as Avaya tests and certifies later versions of supported products. To know about the latest versions of products that Client Enablement Services supports, see the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

- Avaya Aura System Platform. For more information, see *Installing and Configuring Avaya Aura System Platform* guide.

  **Note:**

  You must install System Platform on the hardware on which Client Enablement Services is to be installed.

- Avaya Aura System Manager (Optional). For more information, see *Installing and Upgrading Avaya Aura System Manager* guide.

  **Note:**

  You must install System Manager only if you are using Presence Services.

- Avaya Aura Presence Services (Optional). For more information, see *Implementing Avaya Aura Presence Services* guide.

  **Note:**

  If you are using Presence Services, then you must install Session Manager and System Manager.

You can gain access to all these documents and the interoperability matrix from the Avaya Support Web site at http://support.avaya.com.

# Software requirements for features

Client Enablement Services provides multiple features. Depending on the requirement, you can choose all the features or any combination. Certain features require additional or specific software to function properly.

For Client Enablement Services to function properly, you must:

- Implement Client Enablement Services with Modular Messaging 5.2 or Avaya Aura® Messaging 6.x or Communication Manager Messaging 6.2.

To implement Modular Messaging or Communication Manager Messaging, you do not require Session Manager and System Manager.

- Assign all users a voice mail resource as voice mail is mandatory in Client Enablement Services.
- Install Session Manager 6.1 if you use System Manager 6.1.

The following tables list the software that you must install for each feature. To use the feature listed in the *Feature* column, you must install the corresponding software indicated by a *Yes* in the software column.

**Avaya one-X® Mobile:**

| Feature | Communication Manager | Presence Services | System Manager | Session Manager |
|---|---|---|---|---|
| Telephony | Access Element. Yes (5.2.1) | No | Optional (6.1 and later) | Optional (6.0 and later) |
| | Evolution Server. Yes (6.0 and later) | No | Optional (6.1 and later) | Optional (6.0 and later) |
| | Feature Server. Yes (5.2.1 and later)* | No | Yes (6.1 and later) | Yes (6.0 and later) |
| Presence | Yes (5.2.1 and later) | Yes (6.1 and later) | Yes (6.1 and later) | Yes (6.0 and later) |
| Messaging | Yes (5.2.1 and later) | No | Yes (6.1 and later) | Yes (6.0 and later) |

**Note:**

*Client Enablement Services does not support Communication Manager 6.0 Feature Server implementation.

**Avaya one-X® Communicator - H.323:**

| Feature | Communication Manager | Presence Services | System Manager | Session Manager | Conferencing |
|---|---|---|---|---|---|
| Telephony (Non - Aura implementation) | Yes (5.2.1 and later) | No | Optional (6.1 and later) | Optional (6.0 and later) | No |
| Telephony | Access Element. Yes (5.2.1) | No | Yes (6.1 and later) | Yes (6.0 and later) | No |

| Feature | Communication Manager | Presence Services | System Manager | Session Manager | Conferencing |
|---|---|---|---|---|---|
| | Evolution Server. Yes (6.0 and later) | No | Yes (6.1 and later) | Yes (6.0 and later) | No |
| | Feature Server. Yes (5.2.1 and later)* | No | Yes (6.1 and later) | Yes (6.0 and later) | No |
| Presence | Yes (5.2.1 and later) | Yes (6.1 and later) | Yes (6.1 and later) | Yes (6.0 and later) | No |
| Conferencing | Yes (5.2.1 and later) | No | No | No | Yes (5.2.1 and later) |
| Messaging | Yes (5.2.1 and later) | No | Yes (6.1 and later) | Yes (6.0 and later) | No |

**Note:**

*Client Enablement Services does not support Communication Manager 6.0 Feature Server implementation.

**Avaya one-X® Communicator - SIP:**

| Feature | Communication Manager | Presence Services | System Manager | Session Manager | Conferencing |
|---|---|---|---|---|---|
| Telephony | Access Element. Yes (5.2.1) | No | Yes (6.1 and later) | Yes (6.0 and later) | No |
| | Evolution Server. Yes (6.0 and later) | No | Yes (6.1 and later) | Yes (6.0 and later) | No |
| | Feature Server. Yes (5.2.1 and later)* | No | Yes (6.1 and later) | Yes (6.0 and later) | No |
| Presence | Yes (5.2.1 and later) | Yes (6.1 and later) | Yes (6.1 and later) | Yes (6.0 and later) | No |
| Conferencing | Yes (5.2.1 and later) | No | Yes (6.1 and later) | Yes (6.0 and later) | Yes (5.2.1 and later) |
| Messaging | Yes (5.2.1 and later) | No | Yes (6.1 and later) | Yes (6.0 and later) | No |

**Note:**

*Client Enablement Services does not support Communication Manager 6.0 Feature Server implementation.

## Supported versions of third-party software

Avaya supports use of the documented software versions with the current release of this product. These software versions are the minimum versions that Avaya requires.

This release does not support operating systems, databases, Web servers, switches, or other software platforms that are not documented here, unless stated otherwise in a Product Support Notice.

Avaya will support subsequent updates and service packs that provide corrections for a bug, defect, or problem for the documented software versions. The support depends on the following:

- The manufacturer must guarantee that the updates and service packs are backwards compatible with the supported.
- The updates and service packs do not include changes to the core functionality or new features.

# Network requirements

## Time synchronization requirements

Time synchronization ensures that time stamps for all integrated systems are consistent.

**Note:**

If the time stamps are not synchronized, the secure SSL connections between the servers fail.

All servers that host integrated systems, such as Communication Manager, Messaging, System Manager, and Presence Services require NTP software for time synchronization.

# Licensing requirements

Before you install Client Enablement Services, you must obtain the UC All Inclusive total bundle license, which includes licenses for Client Enablement Services and all integrated components.

### UC All Inclusive total bundle licenses

You must obtain an end-user license from Avaya to provision users for Client Enablement Services. Unprovisioned users cannot gain access to Client Enablement Services.

This license file covers all Client Enablement Services users. An end-user license is consumed when a user is configured and activated for use.

The UC All Inclusive total bundle license has the license files for all Avaya components that you want to integrate with Client Enablement Services. For detailed information about the license requirements for these products, see the product documentation or consult your Avaya representative or Avaya Business Partner representative.

Depending on your system, the license requirements for integrated Avaya components must include the following:

| | |
|---|---|
| **Communication Manager** | Extension to Cellular (PBFMC and EC500), Avaya one-X® Communicator, and CTI Adjunct Links enabled. |
| **Messaging** | Message store platform, number of mailboxes, and maximum number of concurrent text to speech (TTS) sessions. |
| **Conferencing** | As required by your conference bridge version. |

The type of license consumed from Communication Manager depends on the system usage. The following licenses are present:

- Avaya one-X® Communicator license: One Avaya one-X® Communicator license is used for each user logging in using the VoIP (This Computer) mode.
- Public Fixed Mobile Convergence (PBFMC) license

# Location of the Avaya Web License Manager

You can install the Avaya Web License Manager (WebLM) in the following locations:

- Local WebLM: If WebLM of System Platform is used, use the Client Enablement Services pre-install plug-in page to select this option.
- Remote System Manager (SMGR) WebLM: If WebLM of remote System Manager is used, use the Client Enablement Services pre-install plug-in page to select this option.

You must install licenses for most Avaya products in a single location. You must use the WebLM of System Manager for Client Enablement Services.

Use the local WebLM server only if System Manager WebLM is not present.

# Product software and licenses

PLDS provides customers, Avaya Partners, distributors, and Avaya Associates with easy-to-use tools for managing asset entitlements and electronic delivery of software and related licenses. Using PLDS, you can perform activities such as license activation, license de-activation, license re-host, and software downloads.

**Note:**

To obtain a license from the PLDS Web site, you must have the Host ID of the computer.

For more information on downloading product software and obtaining licenses, see *Getting Started with Avaya PLDS* on the Avaya Support site.

# Host ID

You must provide a host ID of the computer that hosts license components for Client Enablement Services. The primary host ID is a software generated MAC address. The MAC address changes every time you reboot System Platform. Use the host ID to obtain a license from the PLDS Web site.

## Obtaining a host ID from a WebLM server co-resident on your Client Enablement Services server

If the WebLM server is co-resident on your Client Enablement Services server, follow this procedure.

### Procedure

1. Log in to the cdom Web admin console using `admin/admin01`.

   The cdom (Console Domain) IP address is the IP address that you configured in the **Static IP** field of the VSP Console Domain Network Configuration screen, during the installation of System Platform.
2. In the left pane, click **Server Management** > **License Management**.
3. Click **Launch WebLM License Manager**.
4. Log on to the WebLM server using your log-on credentials.

5. On the home page of the WebLM server, in the left pane, click the **Server Properties** link.
6. Note the **Primary Host ID**.

   For more information on installing and configuring an Avaya WebLM server, see *Installing and Configuring Avaya WebLM server* on the Avaya Support site.

   **Note:**

   You can obtain the LOCAL (cdom) WebLM URL from the Administration Web site.

### Obtaining a host ID from a System Manager's WebLM server

#### Procedure

1. Log in to the System Manager's Web admin console as `admin/admin01`.
2. Click **Services** > **Licenses**.
3. Select **Server Properties** and note the Primary Host ID.

# Security requirements

## Security requirements

Before implementing Client Enablement Services, ensure that the customer security staff reviews and approves the Client Enablement Services deployment. This means that customers must engage the expertise of their security staff early in the implementation process. The security staff must consider how they will incorporate Client Enablement Services into their routine maintenance of virus protection, patches, and service packs.

## Additional security information

Additional security information for all Avaya products, including Client Enablement Services, and Avaya components that integrate with Client Enablement Services, is available at http://support.avaya.com/security. For example, you can find information about the following:

- Avaya Product Security Vulnerability Response Policy
- Avaya Security Vulnerability Classification
- Security advisories for Avaya products
- Software patches for security issues
- Reporting a security vulnerability
- Automatic e-mail notifications of security advisories

You can also find additional information about security practices at http://www.nsa.gov/snac/.

# Configuring Enterprise Directory for Avaya one-X® Client Enablement Services

## Enterprise Directory integration guidelines

Client Enablement Services integrates with the following enterprise directory servers for user records, authentication, and authorization. Client Enablement Services also uses the enterprise directory to search contact information, that is, like an address book. You can integrate with an existing enterprise directory server, or you can use a dedicated enterprise directory server for Client Enablement Services.

- Microsoft Active Directory
- Microsoft ADAM
- IBM Domino Server
- Novell eDirectory
- SUN Directory Server Enterprise Edition

**Note:**

Client Enablement Services does not support enterprise data split between two or more enterprise directories. For example, you cannot create the User Domain on an Active Directory server and the Contact Domain on a Domino server. Also, Client Enablement Services supports only one enterprise directory attribute mapping. Therefore, the list of attributes must be the same for any enterprise directory you administer.

## Limitations on support for Active Directory domains

Each Client Enablement Services deployment can authenticate and authorize users from only one Active Directory domain. Depending upon the enterprise Active Directory policy, security groups for Client Enablement Services users can reside in the same domain or in a different domain. The domain that provides the users is the user domain. The domain that provides the security groups is the resource domain.

You can configure each deployment to access information about users in up to four additional Active Directory domains. However, Client Enablement Services considers the users in the additional domains to be contacts only and does not obtain anything other than the address book data from them. You cannot provision users from the additional domains, and those users cannot log in to the Client Enablement Services deployment.

If you want to provide the services of Client Enablement Services to users in more than one Active Directory domain, you must implement at least one Client Enablement Services deployment for each domain.

## Limitations on support for other Enterprise Directory domains

Only the LDAP server in the LDAP Domain on Client Enablement Services supports identity resolution on other supported enterprise directories.

## Supported Active Directory domain topologies

| Domain topology | Description |
|---|---|
| Combined domain | Users and security groups are in the same Active Directory domain.<br>For this topology, configure Client Enablement Services with the same domain for the user and the resource. |
| Split domain in same forest | Users and security groups are in separate Active Directory domains. These domains are in the same forest.<br>For this topology, the template installation presents you with Enterprise Directory configuration screens for the User and Group domains. |
| Split domain in different forest | Uses two Active Directory domains that are in different forests.<br>For this topology, the template installation presents you with Enterprise Directory configuration screens for the User and Group domains.<br>To ensure the required access, this topology requires a different service account and password for each forest when you install Client Enablement Services. |

### Required security groups

Before you install Client Enablement Services, you must create the following Enterprise Directory security groups:

- Client Enablement Services administrators
- Client Enablement Services users
- Client Enablement Services auditors

These security groups belong in the same resource domain where the enterprise maintains other security groups for Client Enablement Services users.

Client users must be a member of the Client Enablement Services users group. Administrators must be a member of the Administrative users group. Users who have both roles must be members of both groups.

If you plan to deploy more than one Client Enablement Services server in an environment, you must create unique User security groups across all Client Enablement Services servers. You must provision unique users on each Client Enablement Services server. This will restrict the number of users showing up in the unprovisioned list and will make them unique. Else, all Client Enablement Services servers will display all users as part of the User security group.

The Auditor and Administrator security groups can be the same across multiple Client Enablement Services servers. You cannot change the security groups assigned to a deployment without reinstalling Client Enablement Services.

### Naming conventions for security groups

You must follow existing corporate standards when you create security groups for Client Enablement Services. Each security group name must do the following:

- Be unique in the Active Directory domain.
- Identify the group as related to Client Enablement Services
- Identify the Client Enablement Services deployment
- Identify the purpose of the security group.

**Note:**

Do not use default security group names, such as Domain Users, for Client Enablement Services. These default groups do not function correctly with LDAP. For more information, see Microsoft Knowledge Base article number 275523.

For example, use the following naming conventions for security groups:

- <*deployment_name*> Client Enablement Services Users
- <*deployment_name*> Client Enablement Services Administrators
- <*deployment_name*> Client Enablement Services Auditors

Using this naming convention, you can identify the Client Enablement Services deployment associated with the security groups. Even if the system only includes one Client Enablement Services deployment, this naming convention ensures that the Active Directory integration can be expanded to include additional Client Enablement Services deployments.

# Determining the Active Directory domain topology

### About this task

After you install Client Enablement Services, you cannot change the Active Directory domain unless you reinstall Client Enablement Services. Hence, you must ascertain the domain topology that the Enterprise Active Directory uses.

### Procedure

1. Determine which of the following domain topologies the Enterprise Active Directory uses:
   - Combined domain
   - Split domain in same forest
   - Split domain in different forests
2. Identify the user domain that includes the users who access Client Enablement Services.
3. Identify the resource domain that defines the Client Enablement Services security groups.
4. If the user domain and resource domain are different, determine whether they are in the same forest.

**Related topics:**

Enterprise Directory integration guidelines on page 32

# Configuring Enterprise Directory security groups

**Note:**

Do not use default security group names, such as Domain Users, for Client Enablement Services. These default groups do not function correctly with LDAP. For more information, see Microsoft Knowledge Base article number 275523.

**Note:**

Do not change the Enterprise Directory security groups on the LDAP server once the installation is complete, as otherwise Client Enablement Services will not function properly.

### Procedure

1. In the resource domain, create Enterprise Directory security groups for the following groups of users in each Client Enablement Services deployment:
   - Administrative users who need access to the Administration application: Include the deployment in the group name, for example, Chicago Client Enablement Services Administrators.
   - Users who need access to Client Enablement Services: Include the deployment in the group name, for example, Chicago Client Enablement Services Users.
   - Auditors who need read-only access to the Administration application: Include the deployment in the group name, for example, Chicago Client Enablement Services Auditors.
2. (Optional) For *Active Directory* only, ensure that the configuration of each security group includes the following values:
   - The pre-Windows 2000 name has the same value as the group name.
   - The group type is Security.
   - For a split domain topology only, the group scope is Domain Local.
3. (Optional) For *Novell eDirectory* only, ensure that you add the Novell eDirectory administrator, who has the necessary roles and rights to perform administration on LDAP, to the Client Enablement Services administrators group.

**Related topics:**

Enterprise Directory integration guidelines on page 32

## Verifying Enterprise Directory user configuration

### About this task

Client Enablement Services accesses the user accounts in the Enterprise Directory for authentication and authorization. If Client Enablement Services can access an existing Enterprise Directory server, you do not need to create new user accounts.

Users can log in with their corporate log-in IDs and passwords. To ensure that enterprise users can access Client Enablement Services, verify that each user account meets the required criteria.

Client users must be a member of the Client Enablement Services users group. Administrators must be a member of the Administrative users group. Users who have both roles must be members of both groups.

### Procedure

For each Client Enablement Services user in the user domain, verify the following with regard to the Enterprise Directory user records.

- The domain that hosts Client Enablement Services has the Enterprise Directory user records.
- At least one Client Enablement Services security group is assigned the records to provide the user with the required administrative, user, or auditor privileges.
- The records have a pre-Windows 2000 log-on name that is identical to the Client Enablement Services log-on name.
- The records include a user password and the desired password options.

## Creating the Avaya one-X® Client Enablement Services administrative service account

### About this task

For Client Enablement Services create at least one administrative service account in the user domain of the Enterprise Directory. This administrative service account must be a member of the Client Enablement Services Administrators users group.

Client Enablement Services uses this service account to start and stop the Client Enablement Services server and perform other administrative functions.

If the Enterprise Directory uses a split domain topology with the user domain and resource domain in different forests, Client Enablement Services also requires a secondary service account in the resource domain.

For SUN Directory Server Enterprise Edition, the service account must be able to see the root of the directory.

**Note:**

Do not change the service account login and password on the LDAP server after the installation is complete, as otherwise Client Enablement Services does not function properly.

### Procedure

1. In the user domain, create a primary service account that meets the following criteria:
   - Password meets the requirements of IBM WebSphere. For example, the password cannot contain a space or special character such as $. The password must start with a number or letter, and must not start with an

underscore or other symbol. For more information, see the IBM WebSphere online documentation.

- Password does not expire. Select the **Password never expires** check box.

**Note:**

You can change the passwords of the user admin accounts that have rights to access the Client Enablement Services administration any time.

- Is a member of the Client Enablement Services administrator's security group.

2. The primary service account must be able to:
   - Get the Distinguish Name (DN) of the user based on the user's handle, so the system can validate the password of the user.
   - See the members of the security groups.
   - Read any information that Client Enablement Services wants to export, such as user phone numbers.
3. For Active Directory only, create a secondary service account in the resource domain that meets the same criteria specified in steps 1 and 2. This is only for a split domain topology with the user domain and resource domain in different forests.

**Note:**

To configure Client Enablement Services Enterprise Directories over SSL, refer to the Appendices in this document.

You can map Enterprise Directory attributes to the attributes used in Client Enablement Services using the **System** tab in Administration Web Client.

# Generating the SMGR Enrollment Password

If you want to integrate Presence Services with Client Enablement Services, then the order of installation is System Manager –> Presence Services –> Client Enablement Services.

**Important:**

If you are using System Manager, you must verify the certificates on System Manager before you install the Client Enablement Services template. For more information on managing certificates, see *Administering Avaya Aura® System Manager*.

Use this functionality to generate the simple certificate enrollment password (SCEP). The Client Enablement Services system requires the SCEP password to request certificates from Trust Management.

## Procedure

1. Log in to the System Manager Web console.
2. On the System Manager console, under **Services**, click **Security**.
3. Click **Certificates** > **Enrollment Password**.
4. On the Enrollment Password page, select the expiration of password in hours in the **Password expires in** field.
5. Click **Generate**.

   The password field displays the generated password.
6. Click **Commit**.

**Note:**

When you click **Commit**, the system updates the time displayed next to the **Time remaining** label with the value selected in the **Password expires in** field.

# Chapter 3: Installing

## Installation worksheet: information required by template installation

This worksheet lists the information that you need to install Client Enablement Services. The information and properties follow the same organization as the template installation.

### Installation configuration information

The values in the Example value column are only for guiding you on the format to use. For security purposes, use unique values when you configure Client Enablement Services.

| Property Name | Property values | | Notes |
|---|---|---|---|
| | Example value | Your value | |
| **Network Settings configuration** | | | |
| **One-X CES IP** | *###.###.###.###* | | IP address of the Client Enablement Services system. |
| **One-X CES FQDN** | *1xces.domain.xyzcorp.com* | | Fully qualified domain name of the Client Enablement Services system. |
| **NTP Server Details** | | | |
| **NTP Server1** | | | IP address or FQDN of the computer that hosts the NTP Server 1. This field is mandatory. |
| **NTP Server2** | | | IP address or FQDN of the computer that hosts the NTP Server 2. |
| **NTP Server3** | | | IP address or FQDN of the computer that hosts the NTP Server 3. |
| **LDAP information** | | | |
| **LDAP Type: Active Directory (Split Domain)** | | | If the Enterprise Directory has users defined in one domain and security groups defined in another domain, configure the |

| Property Name | Property values | | Notes |
|---|---|---|---|
| | Example value | Your value | |
| | | | user domain in the first section and the resource domain for security group in the second section. |
| **User LDAP Host** | *###.###.###.###* | | IP address of the computer that hosts the Enterprise Directory server.<br>The host value can also be the FQDN. |
| **User LDAP Port** | 389 | | Port that the Client Enablement Services computer will use to communicate with the Enterprise Directory server.<br>**Note:**<br>You must install the Client Enablement Services template over the non-secure port (389) for LDAP connection. If you want to establish a secure connection, this can be done later using the Client Enablement Services administration client. For more information, see the Appendices in this document. |
| **User LDAP Domain** | *users.domain.xyzcorp.com* | | The domain name of the user configured on the Enterprise Directory server. |
| **User LDAP UserName** | *admin_service_user* | | Enterprise Directory user that you created for the Client Enablement Services administrative service account.<br>**Note:**<br>The user must be a member of the Client Enablement Services administrator's security group created for this install. Client Enablement Services uses this user for assigning permissions to users for performing administrative tasks. |

| Property Name | Property values | | Notes |
|---|---|---|---|
| | Example value | Your value | |
| **User LDAP Password** | | | Password for the Client Enablement Services administrative service account. For password rules, see Creating the Avaya one-X Client Enablement Services administrative service account on page 37. |
| **Is Group LDAP on different forest?** | | | Select the check box if the Group LDAP is on a different forest. |
| **Group LDAP Host** | *###.###.###.###* | | IP address of the computer that hosts the Resource Enterprise Directory server.<br>The host value can also be the FQDN. |
| **Group LDAP Port** | 389 | | Port that the Client Enablement Services computer will use to communicate with the Resource Enterprise Directory server.<br>**Note:**<br>You must install the Client Enablement Services template over the non-secure port (389) for LDAP connection. If you want to establish a secure connection, this can be done later using the Client Enablement Services administration client. For more information, see the Appendices in this document. |
| **Group LDAP Domain** | *groups.domain.xyzcorp.com* | | The domain name of the group configured on the Enterprise Directory server. |
| **Group LDAP UserName** | *group_ldap_user* | | For same forest configuration, the user name is the Enterprise Directory user that you created for the Client Enablement Services administrative service account in the User LDAP. This user must also authenticate the Group LDAP.<br>For different forest configuration, the user name is the secondary |

| Property Name | Property values | | Notes |
|---|---|---|---|
| | Example value | Your value | |
| | | | Client Enablement Services administrative account that you created in the Group LDAP. |
| **Group LDAP Password** | | | Password for this user account. For password rules, see Creating the Avaya one-X Client Enablement Services administrative service account on page 37. |
| **Note:**<br>For information on other LDAPs such as Active Directory (Single Domain), Microsoft ADAM, SUN Directory Server Enterprise Edition, IBM Domino Server and Novell eDirectory, see LDAP Information field descriptions on page 125. | | | |
| **LDAP Configuration** | | | |
| **Admin Group DN** | cn=oneXCESAdmin,cn=users,dc=groups,dc=domain,dc=xyzcorp,dc=com | | The template installation uses the administrator security group to assign permissions to users who will administer Client Enablement Services in the Administration application. |
| **Audit Group DN** | cn=oneXCESAudit,cn=users,dc=groups,dc=domain,dc=xyzcorp,dc=com | | The template installation uses the auditor security group to assign permissions to users who will have read-only access to the Client Enablement Services configuration in the Administration application. Members of the auditor security group cannot make changes to the Client Enablement Services configuration in the Administration application. |
| **User Group DN** | cn=oneXCESUser,cn=users,dc=groups,dc=domain,dc=xyzcorp,dc=com | | The template installation uses the user security group to assign permissions to users who will access the Client Enablement Services application. |
| **SIP Local** | | | |
| **SIP Local Domain** | *sip.domain.xyzcorp.com* | | The local domain for SIP.<br>The value in this field must match the *Authoritative Domain* name in the Communication Manager ip- |

| Property Name | Property values | | Notes |
|---|---|---|---|
| | Example value | Your value | |
| | | | network-region form or the *Routing Domain* name in Session Manager. |
| **SIP Local Port** | 5060 | | The local port number for SIP.<br>**Note:**<br>If you select the **SIP Secure Port** check box, the port number is 5061. |
| **SIP Secure Port** | | | Check box to secure the SIP port. |
| **Handset Server/Service** | | | |
| **Install Handset Server** | | | Check box to install the Handset Server on the Co-resident Server, that is, on the same server on which you install Client Enablement Services.<br>The system installs IHS on the Co-resident Server irrespective of you selecting or clearing the check box. |
| **Use SSL** | | | Check box to secure connection between Handset Server and Handset Service. |
| **Handset Server Port** | 7777 | | Port on which the Handset Server listens for incoming connections from mobile clients. |
| **Handset Service Port** | 8888 | | The listening port of the Handset Service. |
| **Transcoding Server** | | | |
| **Transcoding Server Port** | 8090 | | Port on which the Transcoding Server listens for incoming connections. |
| **System Manager (SMGR) details** | | | |
| **SMGR Host** | ###.###.###.### | | IP address of the system hosting System Manager. |
| **SMGR Port** | 443 | | Port on which System Manager listens for trust management requests.<br>This is the port where Client Enablement Services contacts |

| Property Name | Property values | | Notes |
|---|---|---|---|
| | Example value | Your value | |
| | | | System Manager. The System Manager generates the Client Enablement Services' personal certificate. |
| **SMGR Enrollment Password** | | | Enrollment password for System Manager |
| **WebLM Details** | | | |
| **System Manager (SMGR) WebLM Port** | 52233 | | The port number for System Manager (SMGR) WebLM.<br>**Note:**<br>If the WebLM is local, the port is 8443. |

# Software download

## Software download checklist

Use the following checklist to download System Platform and Client Enablement Services software. As you complete a task, make a check mark in the ✔ column.

**Note:**

Downloading software from PLDS is optional if you already have System Platform and Client Enablement Services software on the optical media.

| ✔ | Task | References | Notes |
|---|---|---|---|
| | Register for PLDS. | See Registering for PLDS on page 47. | |
| | Download System Platform and Client Enablement Services software from PLDS. | See Downloading software in PLDS on page 47. | |

# Registering for PLDS

### Procedure

1. Go to the Avaya Product Licensing and Delivery System (PLDS) Web site at https://plds.avaya.com.
   The PLDS Web site redirects you to the Avaya single sign-on (SSO) Web page.
2. Log in to SSO with your SSO ID and password.
   The PLDS registration page is displayed.
3. If you are registering:
   - as an Avaya Partner, enter the Partner Link ID. If you do not know your Partner Link ID, send an e-mail to prmadmin@avaya.com.
   - as a customer, enter one of the following:
     - Company Sold-To
     - Ship-To number
     - License authorization code (LAC)
4. Click **Submit**.
   Avaya will send you the PLDS access confirmation within one business day.

# Downloading software in PLDS

### Procedure

1. Type `http://plds.avaya.com` in your Web browser to access the Avaya PLDS Web site.
2. Enter your Login ID and password to log on to the PLDS Web site.
3. Select **Assets** from the Home page and select **View Downloads**.
4. Search for the available downloads using one of the following methods:
   - By Actual Download name
   - By selecting an Application type from the drop-down list
   - By Download type
   - By clicking **Search Downloads**
5. Click the download icon from the appropriate download.

6. When the system displays the confirmation box, select **Click to download your file now**.
7. If you receive an error message, click on the message, install Active X, and continue with the download.
8. When the system displays the security warning, click **Install**.

   When the installation is complete, PLDS displays a check mark next to the successfully completed download.

# Template installation

To install Client Enablement Services, you must first install System Platform and then install the Client Enablement Services (solution) template.

After installing the template, manage the template from the System Platform Web Console.

## Prerequisites for installing a solution template

Make sure that the IP addresses for the *avprivate* bridge do not conflict with any other IP addresses in your network.

Go to the Network Configuration Web page on the System Platform Web Console (**Server Management** > **Network Configuration**) to view the addresses that are allocated to avprivate. The range of IP addresses starts with System Domain's (Domain-0) interface on avprivate. Provide IP to Console Domain in the same subnet. If any conflicts exist, resolve them by assigning System Domain an IP address on a subnet that is unused in your network. The template you install will take additional addresses on the private bridge.

The avprivate bridge is an internal, private bridge that allows virtual machines to communicate with each other. This private bridge has no connection to your LAN. During installation, System Platform runs an algorithm to find a set of IP addresses that do not conflict with the addresses configured on the System Domain Network Configuration page. However, it is still possible that the addresses selected conflict with other addresses in your network. Since this private bridge is isolated from your LAN, this address conflict could result in the failure of System Platform or an installed template to route packets correctly.

## Downloading template files

### Procedure

1. To install the template by selecting the **SP Server** option, download the following .tar files:

- oneXCES_61_3.taraa
- oneXCES_61_3.tarab
- oneXCES_61_3.tarac
- oneXCES_61_3.tarad
- oneXCES_61_3.tarae
- oneXCES_61_3.taraf
- oneXCES_61_3.tarag

2. Copy the above files at location `/vsp-template/` on cdom.
3. Using the SSH terminal of cdom, extract or untar the template files using the command: **`cat oneXCES_61_3.tara* | (tar x)`** from the location `/vsp-template/`.

   The system creates the following files in a directory labeled with the version that you downloaded, for example, `/vsp-template/6.1.3.0.12`:

   - `backup_onexps.sh`
   - `lv_rhel.img.gz`
   - `onexps_template.mf`
   - `onexps_template_24GB.ovf`
   - `onexps_template_16GB.ovf`
   - `post_install.sh`
   - `preweb.war`
   - `restore_onexps.sh`
   - `patchplugin_onexps.sh`
   - `versioninfo_onexps.sh`

   You can verify the checksum of downloaded files using a sha1sum tool. The sha1sum tool is available as a freeware from Internet.
4. To verify the file checksum, use the command: **`sha1sum *`**

   Compare the results with the checksum information listed in the `onexps_template.mf` file.

# Installing a solution template

**Note:**

Restart the cdom using its Web administration console after you delete the existing template, before you install a new template.

### Before you begin

Complete all preinstallation and configuration worksheets and checklists, including the following:

- Installation worksheet: information required by template installation on page 41
- Configure NTP before proceeding with the Client Enablement Services installation

### Procedure

1. Log in to the System Platform Web Console as `admin/admin01`.
2. Click **Virtual Machine Management** > **Solution Template**.

   The system displays the Search Local and Remote Template Web page. Use this page to select the template that you want to install on System Platform.
3. Select a location from the list in the **Install Templates From** box.
   - Select **Avaya Downloads (PLDS)** and in the **Template Location** field, provide the PLDS URL.
   - Select **HTTP** and in the **Template Location** field, provide the URL of the HTTP server where the template files exist.
   - Select **SP Server** if the template files are copied to the `/vsp-template/` directory of the System Platform server and this option is used to install the Client Enablement Services template.
   - Select **SP CD/DVD**.

     **Note:**

     If you plan to install the Client Enablement Services template files from a DVD, then you must use a Double-Layer DVD media so that the template files fit into a single DVD.
   - Select **SP USB Disk**.

     **Note:**

     If you plan to install the Client Enablement Services template files from a USB, then you must ensure that the template files fit into a single USB.

4. Click **Search** to display a list of template descriptor files. Each available template has one template descriptor file.
5. On the Select Template Web page, select a template from following types, and then click **Select** to continue.
   - `onexps_template_16GB.ovf`. If the system on which you are installing Client Enablement Services has 16 GB or more RAM, use this template.
   - `onexps_template_24GB.ovf`. If the system on which you are installing Client Enablement Services has 24 GB or more RAM, use this template.

   **Note:**

   All templates have same functionality. Select a template based on the RAM of the system. If you are using a Dell server, you must use the `onexps_template_24GB.ovf` template.

   The system displays the Template Details Web page with information on the selected template and its Virtual Machines.
6. Click **Install** to start the template installation. Follow the installer prompts and enter the required information from the installation worksheet.

## Search Local and Remote Template field and button descriptions

| Field | Description |
|---|---|
| **Install Template From** | The locations from which you can select a template and install it on System Platform. The available options are:<br>• **Avaya Downloads (PLDS)**: The template files are located in the Avaya Product Licensing and Delivery System (PLDS) Web site. You must enter an Avaya SSO login and password. The list contains all the templates to which your enterprise is entitled. Each line in the list begins with the *sold-to* number to allow you to select the appropriate template for the site where you are installing. Hold the mouse pointer over the selection to view more information about the “sold-to” number.<br>• **HTTP**: The template files are located on an HTTP server. You must enter the template URL information.<br>• **SP Server**: The template files are located in the `/vsp-template` file system in the |

| Field | Description |
|---|---|
| | Console Domain of the System Platform server.<br>• **SP CD/DVD**: The template files are located on a DVD in the DVD drive on the server.<br>• **SP USB Disk**: The template files are located on a USB flash drive connected to the server. |
| **SSO Login** | Active only when you select the **Avaya Downloads (PLDS)** option to search for a template.<br>Login id for logging on to Single Sign On. |
| **SSO Password** | Active only when you select the **Avaya Downloads (PLDS)** option to search for a template.<br>Password for Single Sign On. |
| **Template Location** | Active only when you select the **HTTP** or **SP Server** option to search for a template. |
| **Search** | Searches for template descriptor files. Each available template has one template descriptor file. |

## Template Details field and button descriptions

| Name | Description |
|---|---|
| **Product ID** | Displays the Client Enablement Services template name. |
| **Product Vendor** | Displays the Client Enablement Services template vendor. |
| **Product Version** | Displays the Client Enablement Services template version. |
| **Install** | Installs the solution template. The system displays this button only if there is no template currently installed on System Platform. |
| **Cancel** | Cancels the installation of Client Enablement Services and discards all information entered in the template installation. |

# Avaya one-X® Client Enablement Services template installation screens

## Client Enablement Services template installation

**Note:**

Before you start the template installation, you must disable the pop-up blocker in the browser, as the pre-install plug-in will open as a pop-up.

The Client Enablement Services template installation includes the following configurations pages:

- **Network settings**
- **License**
- **NTP Server**
- **LDAP Details**
- **LDAP Groups**
- **SIP Local**
- **Handset Server**
- **Transcoding Server**
- **System Manager (SMGR)**
- **WebLM**
- **Summary**

You must enter all the details in the template installation. Skipping any details would result in improper installation/functioning of Client Enablement Services.

All the fields in the template installation are mandatory except the one for System Manager (SMGR), if System Manager is not present at the time of the Client Enablement Services installation.

**Note:**

If you want to integrate Presence Services with Client Enablement Services, then the order of installation is System Manager–> Presence Services–> Client Enablement Services. You must provide the System Manager credentials during the Client Enablement Services installation, as Presence Services will not function properly otherwise.

The following buttons are available on some or all of the template installation screens:

| Name | Description |
|---|---|
| **Cancel Installation** | Cancels the installation of Client Enablement Services and discards all information entered in the template installation. |
| **Previous Step** | Returns to the previous installer screen. However, the system does not discard the information entered in the current screen. |
| **Next Step** | Saves the information entered in the current screen and moves to the next installer screen. |

## Cancelling installation

### About this task

You can cancel the installation anytime by clicking on the **Cancel Pre-Install Plugin** link on any of the Client Enablement Services installation pages. The pre-install plug-in is nothing but the template installation mentioned in the previous pages.

### Procedure

1. On the Client Enablement Services template installation page, click the **Cancel Pre-Install Plugin** link on the left pane.
   The system displays the confirmation dialog.

   **Note:**

   If you cancel the installation, the plug-in does not install Client Enablement Services.

2. To abort the installation, click **OK**.
3. On System Platform Web Console, click **Cancel Installation**.

## Network Settings field descriptions

| Name | Description |
|---|---|
| **one-X CES IP** | Enter the IP address of the Client Enablement Services system. |
| **one-X CES FQDN** | Enter the Fully Qualified Domain Name of the Client Enablement Services system.<br>For example:<br>onexces100.sysucd.avaya.com |

## one-X CES License Agreement field descriptions

| Name | Description |
|---|---|
| **I accept the terms of license agreement** | Records that you have agreed to the terms of the agreement and continues with the Client Enablement Services installation. |

## NTP Server Details field descriptions

A NTP server provides the correct network time on your computer network using the Network Time Protocol (NTP). You can use NTP to synchronize the time on computers across a network.

| Name | Description |
|---|---|
| **NTP Server1** | IP address or FQDN of the computer that hosts the NTP Server 1. This field is mandatory. |
| **NTP Server2** | IP address or FQDN of the computer that hosts the NTP Server 2. |
| **NTP Server3** | IP address or FQDN of the computer that hosts the NTP Server 3. |

## LDAP Information field and button descriptions

The template installation uses this information to configure the connection between Client Enablement Services and the Enterprise Directory server.

If the Enterprise Directory has users defined in one domain and security groups defined in another domain, the template installation presents you with Enterprise Directory configuration screens for the User and Group domains. Configure the user domain in the first section and the resource domain for security group in the second section.

**Note:**

The split configuration is only supported and available with Microsoft Active Directory and not with other Enterprise Directories.

| Name | Description |
|---|---|
| **LDAP Type** | Select **Active Directory (Split Domain)** from the field. |

| Name | Description |
|---|---|
| | **Note:**<br>For information on other LDAPs such as Active Directory (Single Domain), Microsoft ADAM, SUN Directory Server Enterprise Edition, IBM Domino Server and Novell eDirectory, see LDAP Information field descriptions on page 125. |
| **User LDAP Host** | IP address of the computer that hosts the Enterprise Directory server.<br>The host value can also be the FQDN.<br>This is the user LDAP with all the administered users. |
| **User LDAP Port** | Port that Client Enablement Services uses to communicate with the Enterprise Directory server.<br>**Note:**<br>You must install the Client Enablement Services template over the non-secure port (389) for LDAP connection. If you want to establish a secure connection, you can perform this later using the Client Enablement Services administration client. For more information, see the Appendices in this document. |
| **User LDAP Domain** | The domain name of the user you configured on the Enterprise Directory server. |
| **User LDAP UserName** | Enterprise Directory user that you created for the Client Enablement Services administrative service account.<br>**Note:**<br>The user must be a member of the Client Enablement Services administrator's security group created for this install. Client Enablement Services uses this user for assigning permissions to users for performing administrative tasks. |
| **User LDAP Password** | Password for the Client Enablement Services administrative service account. |
| **Confirm** | Confirm password for the Client Enablement Services administrative service account. |

| Name | Description |
|---|---|
| **Is Group LDAP on different forest?** | Select the check box if the Group LDAP is on a different forest. |
| **Group LDAP Host** | IP address of the computer that hosts the Resource Enterprise Directory server.<br>The host value can also be the FQDN.<br>This is the group LDAP with all the administered Client Enablement Services security groups. |
| **Group LDAP Port** | Port that the Client Enablement Services computer will use to communicate with the Resource Enterprise Directory server.<br>**Note:**<br>You must install the Client Enablement Services template over the non-secure port (389) for LDAP connection. If you want to establish a secure connection, you can perform this later using the Client Enablement Services administration client. For more information, see the Appendices in this document. |
| **Group LDAP Domain** | The domain name of the group configured on the Enterprise Directory server. |
| **Group LDAP UserName** | For same forest configuration, the user name is the Enterprise Directory user that you created for the Client Enablement Services administrative service account in the User LDAP. This user must also authenticate the Group LDAP.<br>For different forest configuration, the user name is the secondary Client Enablement Services administrative account that you have created in the Group LDAP. |
| **Group LDAP Password** | Password for this user account. |
| **Confirm** | Confirm password for the Client Enablement Services administrative service account. |

## LDAP Configuration field and button descriptions

| Name | Description |
|---|---|
| **Admin Group DN** | Security group for Client Enablement Services administrators. |

| Name | Description |
|---|---|
| | Example values:<br>`cn=oneXCESAdmin,cn=users,dc=groups,dc=domain,dc=xyzcorp,dc=com` |
| **Auditor Group DN** | Security group for Client Enablement Services auditors.<br>Example values:<br>`cn=oneXCESAudit,cn=users,dc=groups,dc=domain,dc=xyzcorp,dc=com` |
| **User Group DN** | Security group for Client Enablement Services users.<br>Example values:<br>`cn=oneXCESUser,cn=users,dc=groups,dc=domain,dc=xyzcorp,dc=com` |

## SIP Local field descriptions

| Name | Description |
|---|---|
| **SIP Local Domain** | Enter the local domain for SIP.<br>The value in this field must match the *Authoritative Domain* name in the Communication Manager ip-network-region form or the *Routing Domain* name in Session Manager. |
| **SIP Local Port** | Enter the local port number for SIP.<br>The default port is 5060.<br>**Note:**<br>If you select the **SIP Secure Port** check box, the port number is 5061. |
| **SIP Secure Port** | Select the check box if the SIP port is secure. |

## Handset Server/Service field descriptions

| Name | Description |
|---|---|
| **Install Handset Server** | Select this check box to install the Handset Server on the Co-resident Server, that is, the same server on which you installed Client Enablement Services. |

| Name | Description |
|---|---|
| **Use SSL** | Select this check box to secure connection between Handset Server and Handset Service. |
| **Handset Server Port** | Enter the port on which the Handset Server listens for incoming connections from mobile clients.<br>The default port is 7777.<br>**Note:**<br>You can change this value later, if required, from the `handset_server.properties` file or from the Handset Configuration screen in the Client Enablement Services administration client.<br>For information on changing the value from the `handset_server.properties` file, see Handset Server configuration on page 73.<br>For information on changing the value from the administration client, see *Administering Avaya one-X® Client Enablement Services*. |
| **Handset Service Port** | Enter the listening port of the handset service.<br>The default port is 8888.<br>**Note:**<br>You can change this value later, if required, from the `handset_server.properties` file or from the Handset Configuration screen in the Client Enablement Services administration client.<br>For information on changing the value from the `handset_server.properties` file, see Handset Server configuration on page 73.<br>For information on changing the value from the administration client, see *Administering Avaya one-X® Client Enablement Services*. |

## Transcoding Server field descriptions

| Name | Description |
|---|---|
| **Transcoding Server Port** | Enter the port on which the Transcoding Server listens for incoming connections. The default port is 8090. |

## System Manager (SMGR) details field descriptions

**Note:**

This screen is optional. The details are required only for Session Manager and Presence Services integration.

| Name | Description |
|---|---|
| **SMGR Host** | Enter the network host address of System Manager. It can be defined either as FQDN or as an IP address. |
| **SMGR Port** | Enter the port on which the System Manager listens for trust management requests. This is the port where Client Enablement Services contacts System Manager. The System Manager generates the Client Enablement Services' personal certificate. The default port is 443. |
| **SMGR Enrollment Password** | Enter the enrollment password for System Manager. This is the password configured at System Manager in the security-certificates section. |
| **Confirm** | Confirm password for the SMGR enrollment. |

## WebLM Details field descriptions

| Name | Description |
|---|---|
| **Local WebLM** | Click this option if WebLM of System Platform is used. |

| Name | Description |
|---|---|
| | **Note:**<br>If you select this option, the **System Manager (SMGR) WebLM Port** field is not available. |
| **Remote System Manager (SMGR) WebLM** | Click this option if WebLM of remote System Manager is used. |
| **System Manager (SMGR) WebLM Port** | The port number for System Manager (SMGR) WebLM.<br>The default value is 52233. |

## Summary of Client Enablement Services installation

This screen summarizes the selections and configuration information that you entered in the template installation.

Review this summary carefully. To change any of the configuration information, click **Previous Step**.

## Completing the Client Enablement Services installation

### Procedure

Click **Install** to continue with the Client Enablement Services installation.
The system closes the summary page and the installation continues. Once the installation is complete, the system displays the following message: *Template Installation Completed Successfully*.

# Verifying the installation

### Procedure

1. Log in to the Client Enablement Services administration client using the credentials provided during the template installation in the **User LDAP UserName** and **User LDAP Password** fields.

   The default Web page address is `https://<one-X CES IP or FQDN>/admin`, where *one-X CES IP or FQDN* is the IP address or the Fully Qualified Domain Name (FQDN) of the server that hosts Client Enablement Services.

For example, if the name of the server that hosts Client Enablement Services is `oneXCES` and the domain is `xyzcorp.com`, the Web page address for your administration application is `https://oneXCES.xyzcorp.com/admin`.

**Note:**

If you use a third party reverse proxy with the Client Enablement Services server, you must enable the URL filtering on the reverse proxy to disable access to the administration application from outside the corporate network.

2. On the administration client, check whether the system displays the following tabs: **Home**, **Users**, **Servers**, **Scheduler**, **System**, and **Monitors**.
3. Click the **System** tab.
4. In the left pane, select **General**.

   The **Application Server Version** field displays the version of Client Enablement Services.

   If the version number matches the version of Client Enablement Services that you installed, the version match indicates that the system completed the installation correctly.

# Logging in to the Avaya one-X® Client Enablement Services server using SSH

## About this task

You can open an SSH session to the Client Enablement Services server. You can either use the user name `root` and password *root01* or the user name `craft` and password *craft01* to log in to the system. These are default passwords, and you can change them.

Craft is a general user; therefore, you must use the root login to perform system administration tasks.

To change the password of the user name root, perform the following tasks:

## Procedure

1. Log in to the Client Enablement Services server as `craft/craft01` and then switch the user to root using the command **`su - root`** and password *root01*.
2. In the command prompt, type the command **`passwd`**.
   The system displays the message: `Changing password for the user root`.
3. Enter the new password in the **New UNIX password** field.

4. Re-type the password in the **Retype new UNIX password** field.
   The system displays a message: `all authentication tokens updated successfully`.

**Note:**

Once you change the default password for the root user, use this password for subsequent tasks where you use the root login.

# Setting up Avaya one-X® Client Enablement Services

To configure the Client Enablement Services system, see *Administering Avaya one-X® Client Enablement Services*.

# Chapter 4: Installing, configuring, and upgrading the Handset Server

## Handset Server checklist

Use the following checklist to install, configure, and upgrade the Handset Server. You can also administer and uninstall the IBM HTTP Server. As you ensure that a task is complete, make a check mark in the ✔ column.

| ✔ | Task | References | Notes |
|---|---|---|---|
| | Install Standalone Handset Server | See Prerequisites on page 67 | |
| | | See Installing server with direct access on page 69 or see Installing server with only ssh access on page 70 | |
| | | See Connecting IBM HTTP Server with Client Enablement Services for downloading mobile applications from the Standalone system on page 71 | |
| | Install Co-resident Handset Server | See Installing on page 72 | |
| | Configure Handset Server | See Handset Server configuration on page 73 | |
| | Check Handset Server / IBM HTTP Server version | See Checking Handset Server / IBM HTTP Server version on page 78 | |
| | Upgrade the Handset Server | See Upgrading the Handset Server on page 78 | |

| ✔ | Task | References | Notes |
|---|---|---|---|
| | Administer the IBM HTTP Server | See IBM HTTP Server administration and maintenance on page 79 | |
| | Change the Handset Server configuration | See Change the Handset Server configuration on page 87 | |
| | Uninstall the Standalone Handset Server | See Uninstalling the Standalone Handset Server on page 90 | |
| | Uninstall the Standalone IBM HTTP Server | See Uninstalling the Standalone IBM HTTP Server on page 90 | |

# Handset Server installation

The Handset Server is required for functionality related to Avaya one-X® Mobile.

There are two deployment options for Handset Server installation:

- Co-resident installation: The Handset Server is installed on the same server where Client Enablement Services is installed. This deployment option supports a Handset Server that is co-resident with Client Enablement Services on a System Platform template and supports Reverse Proxy deployment.

  By default, the system selects the **Install Handset Server** check box during the Client Enablement Services template installation. The Handset Server is installed at `/opt/avaya/HandsetServer`. The system installs the IHS on the Co-resident Server irrespective of you selecting or clearing the check box.

  Use the Co-resident IHS for handling internal HTTP traffic to the IHS, that is, the Client Enablement Services administration client and not the IBM console. Use the Standalone IHS for handling Internet traffic, that is, mobile application download. When the Handset Server is co-resident, the single Co-resident IHS plays both roles.

  On a Reverse Proxy deployment, if you upgrade Client Enablement Services and if the IHS has been hardened previously; the IHS must be re-hardened as the template upgrade does a fresh OS install.

- Standalone installation: The Standalone Server installation is performed on a separate server, typically located in the DMZ that is running the Handset Server service. To implement this, you must install and configure a separate RedHat server with an IP address. The IHS software is located on the Client Enablement Services server under `/opt/avaya` and the installation package is called `RHServer.bin`. You must copy this

package from the Client Enablement Services server to the target RedHat server that will host this application. Install `RHServer.bin` using the steps in the following section.

# Standalone Handset Server installation

You can install the standalone Handset Server using any of the following options:

- Server with direct access
- Server with only ssh access

**Note:**

If the Handset Server is standalone, you must install Client Enablement Services first and then the Handset Server. Installing Handset Server prior to installing Client Enablement Services will cause the Handset Server to time-out.

## Prerequisites

The server must meet the following prerequisites for installing Handset Server on a Standalone Server.

| | |
|---|---|
| **Operating System** | RHEL 5.8 (64 bit) |
| **CPU** | Dual quad-core processors (2.4 GHz or higher) |
| **Memory** | 4 GB of RAM |
| **Hard drive** | 2 * 146 GB (RAID 1) |
| **Network card** | 1 (maximum) |

**Note:**

The versions of Avaya and third-party products mentioned in this guide are likely to change as Avaya tests and certifies later versions of supported products. To know about the latest versions of products that Client Enablement Services supports, see the Avaya Support website at https://support.avaya.com/CompatibilityMatrix/Index.aspx.

### Open ports

Several ports have to be open for the DMZ HTTP and Handset Server to work.

**Note:**

For a new installation of Client Enablement Services, HTTP is disabled by default.

| Server | Open Port | Protocol | Required | Direction |
|---|---|---|---|---|
| HTTP Server | 443 | https | Yes | Open from Public Internet to HTTP Server |
| HTTP Server | 22 | ssh | Yes | Open from inside the corporate firewall of Client Enablement Services to HTTP Server |
| HTTP Server | 8008 | https | Yes | Open from inside the corporate firewall of Client Enablement Services to HTTP Server. The port must be open between the Client Enablement Services server and Standalone Handset Server. |
| Client Enablement Services | 9443 | https | Yes | Open from HTTP Server to Client Enablement Services |
| Handset Server | 7777. You can configure this port. | xSocket using SSL v3 | Yes | Open from Public Internet to Handset Server |
| Handset Server | 9999. You can configure this port. | JMX | Yes | Open from only the private network. |
| Client Enablement Services | 8888. You can configure this port. | xSocket using SSL v3 | Yes | Open from Handset Server to Client Enablement Services |

### Domain Name System

The IHS must resolve two fully qualified domain names (FQDNs). First, it has to resolve itself. Second, it has to resolve the domain name of the Client Enablement Services server. Either the Domain Name System (DNS) Servers must be accessible from the IHS Server, or the IHS

Server's `/etc/hosts` file has to have these two entries added. You need to add these two entries only if the DNS server cannot resolve the FQDN to IP.

An example of these `/etc/hosts` entries are:

### Example

```
198.152.10.235  dmzihsserver.example.com        dmzihsserver
192.168.1.100   onexCES.inside.example.com      onexCES
```

### Test whether the hosts are resolvable

To test if these hosts are resolvable, from the dmz server run: `hostname –long` and `wget https://<1xCESHostName>:9443/mobileapps`

For example, if `/etc/hosts` is setup up as in the `/etc/hosts` example above:

```
# hostname –long
dmzihsserver.example.com

#wget https:// onexCES:9443/mobileapps
--08:21:56--  https:// onexCES:9443/mobileapps
=> `mobileapps'
Resolving onexCES... 192.168.1.100
Connecting to onexCES |192.168.1.100|:9443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https:// onexCES:9443/mobileapps/ [following]
--08:21:57--  https:// onexCES:9443/mobileapps/
=> `index.html.1'
Reusing existing connection to onexps100:9443.
HTTP request sent, awaiting response... 200 OK
Length: 779 [text/html]

100%[======================================================>] 779         --.--
K/s

08:21:57 (61.91 MB/s) - `index.html.1' saved [779/779]
```

## Installing server with direct access

### Before you begin

- Log in to the shell as a *root* user.
- The Handset Server installer must have executable permissions. You can use the command `chmod +x RHServer.bin` to provide this permission.

### Procedure

1. Copy the `RHServer.bin` file to the`/tmp` directory on your system.

   The `RHServer.bin` file is available in the template provided with PLDS.

2. Launch the installer by using the command `./RHServer.bin`

   Enter the name of the installation directory.

3. In the **Handset Server IP** field, enter the IP address of the computer on which you are installing the Handset Server.

4. In the **Handset Server port** field, enter the port on which the Handset Server listens for incoming connections from mobile clients.

   The default value is 7777.

5. In the **Handset Services IP** field, enter the IP address of the Client Enablement Services server.
6. In the **Handset Services port** field, enter the listening port of the Handset Service.

   The default value is 8888.

7. Select the **Use SSL** check box to secure connection between Handset Server and Handset Service.
8. Click **Next** and complete the installation.

   **Note:**

   Once the installation of Handset Server is complete, exit and re-login the shell before starting the Handset Server.

## Installing server with only ssh access

### Before you begin

- Log in to the shell as a *root* user.
- The Handset Server installer must have executable permissions. You can use the command `chmod +x RHServer.bin` to provide this permission.

### Procedure

1. Copy the `RHServer.bin` file to the `/tmp` directory on your system.

   The `RHServer.bin` file is available in the template provided with PLDS.

2. Open ssh session with the server and navigate to the directory where the installer is located.
3. Launch the installer by using the command `./<RHServer.bin> -console`
4. In the **Handset Server IP** field, enter the IP address of the computer on which you are installing the Handset Server.
5. In the **Handset Server port** field, enter the port on which the Handset Server listens for incoming connections from mobile clients.

   The default value is 7777.

6. In the **Handset Services IP** field, enter the IP address of the Client Enablement Services server.

7. In the **Handset Services port** field, enter the listening port of the Handset Service.

   The default value is 8888.

8. Set the SSL value to *True*.
9. Complete the installation by following the system prompts.

   **Note:**

   Once the installation of Handset Server is complete, exit and re-login the shell before starting the Handset Server.

## Connecting IBM HTTP Server with Client Enablement Services for downloading mobile applications from the Standalone system

If you deploy the IHS on a Standalone system, you must perform the steps in this section for the Client Enablement Services server to interact with the IHS, before the mobile applications are available for download from the Standalone system.

You must perform the steps in this section each time you install or upgrade Client Enablement Services.

### Before you begin

Ensure that the Client Enablement Services server and the Standalone IHS are running.

### Procedure

1. Log in to the Client Enablement Services server using SSH terminal as user `craft/craft01` and then switch the user to root using the command **`su - root`** and password *root01*.
2. Change to the `/opt/avaya/1xp` directory using the `cd /opt/avaya/1xp` command.
3. Edit the `config.properties` file in the `/opt/avaya/1xp` directory to add the following property:

   - `dmz.ihs.host=<IP Address of the Standalone Handset Server>`

4. To configure the IHS on WAS, run the `run_config_httpservers_jython.pl` command in the `/opt/avaya/1xp` directory.
5. Copy the plug-in files from the Client Enablement Services server to the Standalone IHS using the `scp /opt/IBM/WebSphere/AppServer70/profiles/default/config/cells/<Host Name of the Client Enablement Services Server>Node01Cell/nodes/<IP Address of the Standalone Handset Server>-node/servers/dmzwebserver/plugin-* <Login User Name of the Standalone Handset Server>@<IP`

*Address of the Standalone Handset Server*>:/opt/IBM/HTTPServer/Plugins/config/dmzwebserver/ command.

6. In the SSH terminal session on the Standalone Handset Server, change the group of the plug-in files copied on the Standalone system to appsvr using the command: `chgrp appsvr /opt/IBM/HTTPServer/Plugins/config/dmzwebserver/*`
7. Restart the IHS service using the **`service ihs restart`** and **`service ihs_admin restart`** commands.
8. To download the active mobile applications on the Standalone system, access the `https://<IP Address of the Standalone Handset Server>/mobileapps/` Web site.

# Co-resident Handset Server installation

## Installing

During the installation of the Client Enablement Services template, the system installs the co-resident Handset Server on the same server on which you installed Client Enablement Services.

### Procedure

1. On the Handset Server / Service page of the Client Enablement Services template installation, ensure that the system selects the **Install Handset Server** check box by default.
2. Select the **Use SSL** check box to secure connection between Handset Server and Handset Service.
3. In the **Handset Server Port** field, enter the port on which the Handset Server listens for incoming connections from mobile clients.

   The default port is 7777.
4. In the **Handset Service Port** field, enter the listening port of the handset service.

   The default port is 8888.
5. Follow the installer prompts and enter the required information from the installation worksheet. For more information, see Installation worksheet: information required by template installation on page 41.

# Handset Server configuration

The Handset Server configuration is stored in the `handset_server.properties` file, which is located in the Handset Server installation directory, that is, `/opt/avaya/HandsetServer`. The `handset_server.properties` file is located on Handset Server irrespective of the server being Co-resident or Standalone.

During the installation, the system automatically populates this file with user input. Only the system administrator must modify this file.

The `handset_server.properties` file includes the following attributes.

**Note:**

If you make any changes in the `handset_server.properties` file, then you must stop and start Handset Server. For more information, see Stopping the Handset Server on page 76 and Starting the Handset Server on page 77.

| Name | Description |
|---|---|
| **hs_hostname** | The IP address or host name of the machine on which Handset Server is running. |
| **use_ssl** | To secure network connections, set this property to *true*.<br>The default value is *true*. |
| **port** | Handset Server listens for incoming connections from the mobile clients on this port.<br>The default value is *7777*. |
| **hss_hostname** | The IP address or host name of the Client Enablement Services server on which Handset Service runs. |
| **hss_port** | Handset Service listens to incoming connections from Handset Server on this port.<br>The default value is *8888*. |
| **hs.client.timeout** | The connection between the client and Handset Server can be idle for the specified period, after which the connection is disconnected.<br>The default value is *900* seconds. |
| **pipleline_idle_timeout** | The network connection can stay idle for the specified period, after which the network connection is disconnected. |

| Name | Description |
|---|---|
| | The default value is *20* seconds.<br>**Note:**<br>This parameter is very important. Any change in the parameter value can severely affect the performance of Handset Server. |
| **pipeline_count** | The total number of simultaneous network connections with Handset Services.<br>If you provision the server to support more number of simultaneous user connections, you must increase the pipeline count.<br>The default value is *10*.<br>**Note:**<br>This parameter is very important. Any change in the parameter value can severely affect the performance of Handset Server. |
| **pipeline_recovery_retry_delay** | Before attempting to reconnect to Handset Services, the system waits for the specified duration.<br>The default value is *60* seconds. |
| **log_client_io** | To log the client I/O information, set this property to true.<br>The default value is *false*.<br>The system logs the client I/O information in the `logs` directory.<br>**Note:**<br>You must use this property for debugging purpose only.<br>If you set this property to true, this property will negatively affect the performance of all I/O as the system dissects each data packet at the protocol level in order to log the information. |
| **tcp_keep_alive** | Use this property to enable socket-level tcp keep-alive for the pipeline that connects Handset Server and Handset Services.<br>The *tcp_keep_alive* property is useful in ensuring that the connection stays open through networking equipment that would otherwise close the connection during periods of inactivity.<br>The default value is *true*. |

| Name | Description |
|---|---|
| | **Note:**<br>This parameter is very important. Any change in the parameter value can severely affect the performance of Handset Server. |

## Handset Services properties

Handset Services use the Client API to provide Avaya one-X® Mobile users with access to their UC capabilities. Handset Services manages the cache data of the user session.

The Handset Services configuration is stored in the `HandsetServices.properties` file that is located in the `/opt/IBM/WebSphere/AppServer70/lib/ext` directory. In case of a Standalone Server, if you manually change the port information in the `HandsetServices.properties` file, then you must change the corresponding value in the `handset_server.properties` file that is located in the `/opt/avaya/HandsetServer` directory.

| Name | Description |
|---|---|
| **use_ssl** | For secure connections, set this property to true.<br>For non-secure connections, set this property to false.<br>The default value is *true*. |
| **port** | The port on which the Client Enablement Services server communicates with Handset Server.<br>The default value is *8888*. |
| The following parameters are very important. Changing these values can severely affect the system performance. | |
| **min_cache_size** | The minimum cache limit.<br>The default value is *50*. |
| **max_cache_size** | The maximum cache limit.<br>The default value is *6500*. |
| **server_idle_timeout** | The period of inactivity after which the connection is closed.<br>The default value is *20000*. |
| **cache_load_factor** | The cache load factor.<br>The default value is *0.75F.* |
| **maxClients** | The maximum number of clients that can connect to Handset Server. |

| Name | Description |
|---|---|
| | The default value is *2000*. |
| **vm_resource_status_change_handler_req_per_second** | Handset Services can handle the specified number of requests per second for every status change in the voice mail resource. The default value is *100*. |

# Verifying whether the Handset Server is running

## Procedure

1. Open terminal on the server where Handset Server is installed and run the command: **`ps -ef | grep HandsetServer`**.
2. If the Handset Server is running, the system displays its process.

## Example

```
# ps -ef | grep HandsetServer root 17788 1 0 Jun27 ? 00:26:35 /opt/avaya/
HandsetServer/_jvm/bin/java -jar -server -XX:+MaxFDLimit -
Dorg.xsocket.connection.server.ssl.sslengine.
enabledCipherSuites=TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_
AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA -Dcom.sun.management.config. file=/
opt/avaya/HandsetServer/hsjmx.properties /opt/avaya/HandsetServer/lib/
RoutingHandsetServer.jar
```

# Stopping the Handset Server

## Procedure

1. Log in to the Client Enablement Services server using SSH terminal as user `craft/craft01` and then switch the user to root using the command **`su - root`** and password *root01*.

   **Note:**

   In a Co-resident installation, you must log in to the Client Enablement Services server. However, in a Standalone installation, you must log in to the Handset Server.

2. On the shell prompt, type the **`service handset_server stop`** command to stop the Handset Server.
   This stops the Handset Server.

You can view the Handset Server logs in the `hs.log` file located in the `/opt/avaya/HandsetServer/logs` directory.

To check only the error information, view the `hs_errors.log` file located in the `/opt/avaya/HandsetServer/logs` directory.

## Starting the Handset Server

### Procedure

1. Log in to the Client Enablement Services server using SSH terminal as user `craft/craft01` and then switch the user to root using the command **`su - root`** and password *root01*.

   **Note:**

   In a Co-resident installation, you must log in to the Client Enablement Services server. However, in a Standalone installation, you must log in to the Handset Server.

2. On the shell prompt, type the **`service handset_server start`** command to start the Handset Server.
   This starts the Handset Server. If the server starts successfully, you will see the following output.

```
# service handset_server start
Starting handset_server:                                   [  OK  ]
```

## Testing the IBM HTTP Server on the Handset Service

### Procedure

You can test the IHS on the Handset Service using any of the following methods:

- Log in to the mobile applications client. The default Web page address is `https://<one-X CES IP or FQDN>/mobileapps`, where the Client Enablement Services Server is the IP address or the Fully Qualified Domain Name (FQDN) of the computer that hosts Client Enablement Services. The system must display a page containing mobile downloads.
- Check the `access_log` file using the command: `tail -f /opt/IBM/HTTPServer/logs/access_log`. The log file will include content that indicates your access to the mobile applications.

# Cipher Suite

A cipher suite is a named combination of authentication, encryption, and message authentication code (MAC) algorithms used to negotiate the security settings for a network connection using the Transport Layer Security (TLS) or Secure Sockets Layer (SSL) network protocol.

If your organization uses SSL Ciphers, you must modify the java command in the `handset_server` file to include a `Dorg` option. The `handset_server` file is located in the `/etc/rc.d/init.d` directory along with other services.

The cipher suite that works for both the Standalone and Co-resident Handset Server is: TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA ,TLS_RSA_WITH_AES_128_CBC_SHA

The command for enabling the Cipher Suite is

```
java -
Dorg.xsocket.connection.server.ssl.sslengine.enabledCipherSuites=TLS_DHE_R
SA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_
128_CBC_SHA -jar /opt/avaya/HandsetServer/lib/RoutingHandsetServer.jar
```

# Checking Handset Server / IBM HTTP Server version

### Procedure

1. To check the Handset Server version, view the `hs.log` file located in the `/opt/avaya/HandsetServer/logs` directory.
2. To check the IHS version, change to the `/opt/IBM/HTTPServer/bin` directory and then use the `./versionInfo.sh` command.

# Upgrading the Handset Server

**Note:**

To upgrade the Handset Server, you do not need to uninstall the earlier installation.

### Before you begin

Ensure that the Handset Server is not running. If the Handset Server is running, stop the Handset Server using the **`service handset_server stop`** command. For more information, see Stopping the Handset Server on page 76.

### Procedure

To upgrade the Handset Server on the:

- Standalone Server: Run the latest Handset Server installer, that is, `RHServer.bin`. Follow the installation prompts to complete the installation.
- Co-resident Server: Run the Client Enablement Services install. When you upgrade Client Enablement Services, the system automatically upgrades the Handset Server on the Co-resident Server.

# IBM HTTP Server administration and maintenance

The system configures IHS during installation.

You must generate a certificate-signing request as the request includes the distinguished name and the unique certificate label over which the certificate authority (CA) generates the certificate.

## Keystore certificates

A keystore is a repository of security certificates. A keystore is usually a file that contains trusted certificates and combinations of private keys with their corresponding certificates. Client applications use these keystores to verify the identity of a trusted server.

Client Enablement Services uses the following keystores:

- Keystore for WAS on port 9443. The keystore certificates must be in PCKS12 format.
- Keystore for IHS on port 443. The keystore certificates must be in CMS format. Avaya one-X® Communicator clients connect to Client Enablement Services using this keystore.
- Keystore for Handset Server on port 7777 or Handset Server Service on port 8888. The keystore certificates must be in JKS format.

The customer must choose one of the following models:

- Use the default certificate in each keystore.

**Security alert:**

Avaya recommends that you must not use the default certificate as the default certificate and the key pair is the same for all instances of Client Enablement Services.

- Replace the Client Enablement Services certificate with a self-signed certificate.
- Replace the Client Enablement Services certificate with a certificate signed by a third-party CA. For example, VeriSign.

# Generating a certificate signing request using GUI

## Before you begin

To work with certificates on your IBM server, IBM has a tool called IBM Key Management Utility (IKEYMAN). To install a certificate using a GUI interface, use the IKEYMAN tool available at `/opt/IBM/HTTPServer/bin/ikeyman`. You must run the IKEYMAN tool on Handset Server irrespective of the server being Co-resident or Standalone.

**Note:**

You can use the IKEYMAN tool only from the console, a remote graphical user interface (VNC), or remotely using x-windows.

## Procedure

1. Enter IKEYMAN on a command line on UNIX, or start the Key Management utility in the IBM HTTP Server folder on Windows.
2. From the main user interface, click **Key Database File** > **Open**.
   The system displays the Open dialog box.

   Ensure that the key database name is **CMS**.
3. Click **Browse** and navigate to the `/opt/IBM/HTTPServer` directory.
4. Select the `ihsserverkey_default.kdb` file.
5. Click **OK**.
6. In the Password Prompt dialog box, enter `WebAS` as the keystore password and click **OK**.
7. To create a certificate signing request, click **Create** > **New Certificate Request**.
   The system creates a new certificate request file that you must send to a CA to request a certificate.

   After you receive the signed certificate from your CA, put the signed certificate file into the IHS keystore using the **Receive** button.

   Ensure that when you receive the certificate, you configure the certificate as the default certificate.

8. To make the certificate default:
   a. In the **Key database content** area, click **Personal Certificates** and then select the certificate.
   b. Click **View/Edit**.
      The system displays the Key information for window.
   c. Select the **Set the certificate as the default** check box.
9. If the CA includes a signer certificate or intermediate CA certificates, you must add these to the Signer Certificates.
   a. In the **Key database content** area, click **Signer Certificates**.
   b. Click **Add**.
10. Click **Populate** to populate your CA Signer Certificates.

## Generating a certificate signing request using command line for Co-resident Handset Server

If you want to replace the default certificates in Client Enablement Services with a certificate signed by a third-party CA, you must follow the steps documented in this topic.

### Procedure

1. Log in to the Client Enablement Services server using SSH terminal as user `craft/craft01`.
2. Change the user to root using the command **`su - root`** and password *root01*.
3. Change to the Handset Server installation directory using the `cd /opt/avaya/IHS` command.
4. Create a certificate request using the `./gen_ihs_certificate_request.pl -pw=WebAS -dn=<distinquished_name> -label=<certificate_label>` command.
   - *distinquished_name*: The X.500 distinguished name. The distinguished name for the certificate must contain the Handset Server URL name. The value must be a quoted string in the following format that applies to your system: CN=common_name, OU=organization_unit, O=organization, L=location, ST=state, province, C=country. Only the CN attribute is mandatory, as the CN attribute is the subject name that appears on the certificate.
   - *certificate_label*: The label represents the certificate in the keystore and must be unique within the keystore. Renewal requests always require a unique non-default label.

For example: `./gen_ihs_certificate_request.pl -pw WebAS -dn "CN=ihsmachine.example.com, OU=Organization X, O=Example Inc, C=us" -label handsetservercert`

The system creates a new certificate request file, `certreq.arm`, in the `/opt/IBM/HTTPServer` directory that you must send to your CA to request a certificate.

5. After you receive the signed certificate from your CA, copy the signed certificate file along with the issuing root certificate and any intermediary certificates individually in to the IHS keystore using the `./receive_ihs_certificate.pl-pw WebAS -file=<filename_received certificate> -ca_file <filesname_ca_certificate> -format=<ascii | binary>` command.

   - *filename_received certificate*: The IHS certificate file name that you receive from your CA.
   - *filesname_ca_certificate*: The signer or intermediary certificate file name.
   - *ascii* | *binary*: The format of the certificate you receive from your CA.

   For example: `./receive_ihs_certificate.pl -pw WebAS -file ca_signed_cert.txt -ca_file ca_signer_certs.cer -format=ascii`

   If there are other intermediary or root certificate authorities in the trust chain, you must also import those certificates to the certificate store.

   **Note:**

   If there is any white space in the certificate aliases or in the distinguished name, the gsk7cmd fails if IHS does not have the latest fix pack.

6. If the CA certificate includes several intermediary trusted CA certificates, you must add these certificates using the `./add_trusted_certs.pl -pw=<keystore_password> -file=<trusted certificate> -label=<trusted certificate label> -format=<ascii | binary>` command.

   - *keystore_password*: WebAS.
   - *trusted certificate*: The file name of the certificate copied to the server.
   - *trusted certificate label*: The label for the certificate as the label will appear in the keystore. The label is a unique alias for that certificate. All aliases in the certificate store must be unique.

   For example: ./add_trusted_certs.pl -pw *WebAS* -file *certfile* -label *certname* -format ascii

# Generating a certificate signing request using command line for Standalone Handset Server

If you want to replace the default certificates in Client Enablement Services with a certificate signed by a third-party CA, you must follow the steps documented in this topic.

### Procedure

1. Log in to Standalone Handset Server installed machine using SSH terminal as a root user.
2. Change to the Handset Server installation directory using the `cd $HSPATH` command.
3. Create a certificate request using the `./gen_ihs_certificate_request.pl -pw=WebAS -dn=<distinquished_name> -label=<certificate_label>` command.
   - *distinquished_name*: The X.500 distinguished name. The distinguished name for the certificate must contain the Handset Server URL name. The value must be a quoted string in the following format that applies to your system: CN=common_name, OU=organization_unit, O=organization, L=location, ST=state, province, C=country. Only the CN attribute is mandatory, as the CN attribute is the subject name that appears on the certificate.
   - *certificate_label*: The label represents the certificate in the keystore and must be unique within the keystore. Renewal requests always require a unique non-default label.

   For example: `./gen_ihs_certificate_request.pl -pw WebAS -dn "CN=ihsmachine.example.com, OU=Organization X, O=Example Inc, C=us" -label handsetservercert`

   The system creates a new certificate request file, `certreq.arm`, in the Handset Server installation directory that you must send to a CA to request a certificate.
4. After you receive the signed certificate from your CA, copy the signed certificate file along with the issuing root certificate and any intermediary certificates individually into the IHS keystore using the `./receive_ihs_certificate.pl-pw WebAS -file=<filename_received certificate> -ca_file <filesname_ca_certificate> -format=<ascii | binary>` command.
   - *filename_received certificate*: The IHS certificate file name that you receive from your CA.
   - *filesname_ca_certificate*: The signer or intermediary certificate file name.
   - *ascii* | *binary*: The format of the certificate you receive from your CA.

For example: `./receive_ihs_certificate.pl -pw WebAS -file ca_signed_cert.txt -ca_file ca_signer_certs.cer -format=ascii`

If there are other intermediary or root certificate authorities in the trust chain, you must also import those certificates to the certificate store.

**Note:**

If there is any white space in the certificate aliases or in the distinguished name, the gsk7cmd fails if IHS does not have the latest fix pack.

5. If the CA certificate includes several intermediary trusted CA certificates, you must add these certificates using the `./add_trusted_certs.pl -pw=<keystore_password> -file=<trusted certificate> -label=<trusted certificate label> -format=<ascii | binary>` command.
   - *keystore_password*: WebAS.
   - *trusted certificate*: The file name of the certificate copied to the server.
   - *trusted certificate label*: The label for the certificate as the label will appear in the keystore. The label is a unique alias for that certificate. All aliases in the certificate store must be unique.

   For example: ./add_trusted_certs.pl -pw *WebAS* -file *certfile* -label *certname* -format ascii

## Converting the existing SSL certificate to the PKCS12 format

To install a SSL certificate on the Microsoft Reverse Proxy server, you must convert the existing certificate on Handset Server to the PKCS12 format. The conversion script is located in the following directories:

- `/opt/avaya/HandsetServer` directory on Standalone Handset Server
- `/opt/avaya/IHS` directory on Co-resident Handset Server

### Procedure

Convert the existing SSL certificate to the PKCS12 format using the command:

- `./convert_ssl_pkcs12.pl -pw <password> -file /opt/avaya/HandsetServer/keystore.jks` on Standalone Handset Server
- `./convert_ssl_pkcs12.pl -pw <password> -file /opt/avaya/IHS/keystore.jks` on Co-resident Handset Server

where,

-pw <*password*> is the keystore password. The default password is *WebAS*.

-file <certificate file to be converted>. The Handset Server keystore file is located in the `/opt/avaya/HandsetServer` or `/opt/avaya/IHS` directory.

The system stores the certificate in the PKCS12 format in the `/opt/avaya/HandsetServer` or `/opt/avaya/IHS` directory.

## Importing the IBM HTTP Server keystore to the Handset Server keystore

Once the IHS keystore contains the new CA signed certificate, you must import the CA certificate to the Handset Server keystore.

If you want to use the trusted third-party certificates between Handset Server and Handset Services, you must perform these steps to export the keystore in JKS format.

### Procedure

1. Import the certificate to the Handset Server keystore using the `./migrate_ihs_keystore_to_handset_server.pl -pw WebAS` command. For example, on Co-resident Handset Server:

   ```
   # cd /opt/avaya/IHS
   # ./migrate_ihs_keystore_to_handset_server.pl –pw WebAS
   ```

   For example, on Standalone Handset Server:

   ```
   # cd /opt/avaya/HandsetServer
   # ./migrate_ihs_keystore_to_handset_server.pl –pw WebAS
   ```

2. If you are using Standalone Handset Server, copy the `keystore.jks` file using the SCP command to the Client Enablement Services server in the *tmp* directory.
3. On the Client Enablement Services server, copy the `keystore.jks` file from the
   - `/opt/avaya/HandsetServer` directory in case of Co-resident Handset Server
   - *tmp* directory in case of Standalone Handset Server

   to the `/opt/IBM/WebSphere/AppServer70/lib/ext` directory .
4. Restart the IHS service using the **`service ihs restart`** and **`service ihs_admin restart`** commands.
5. To view the active mobile applications that you can download, access the `https://<IP Address of IHS>/mobileapps/` website.

## Reimporting IBM HTTP Server certificates

Whenever the IHS certificate changes, you must reimport the IHS certificate in the Client Enablement Services WebSphere server by rerunning the `run_config_httpservers_jython.pl` script.

### Procedure

1. Log in to the Client Enablement Services server using SSH terminal as user `craft/craft01` and then change the user to root using the **`su - root`** command and password *root01*.
2. Change to the `/opt/avaya/1xp` directory using the `cd /opt/avaya/1xp` command.
3. Import the certificates using the `./run_config_httpservers_jython.pl` command.

## Renewing the IBM HTTP Server certificate

Certificates have a finite life, usually about a year. If the IHS certificate is the default, that is, you did not generate the third-party certificates using the GUI or command line, then the certificate you have is a self-signed certificate with a one-year life.

If you have a third-party certificate, that is, you generated the certificates using the GUI or command line; then the certificate expiry date depends on the CA, which is usually a year. Before the certificate expires, you must renew the certificate by obtaining a new certificate.

### Procedure

If you are using:

- a third-party party certificate, you must perform the steps provided in Generating a certificate signing request using GUI on page 80 or Generating a certificate signing request using command line for Co-resident Handset Server on page 81.
- the default self-signed certificate, run the following command from the Handset Server directory: `renew_self_signed_certificate.pl --pw=WebAS --label=<certificate_label>`

  *certificate_label*: The label represents the certificate in the keystore and must be unique within the keystore.

For example, on Co-resident Handset Server:

```
# cd /opt/avaya/IHS
# ./renew_self_signed_certificate.pl –pw WebAS --label=default_2
```

For example, on Standalone Handset Server:

```
# cd /opt/avaya/HandsetServer
# ./renew_self_signed_certificate.pl –pw WebAS --label=default_2
```

After renewing the certificate, either through a third-party CA or with a self-signed certificate, migrate the new certificate to Handset Server by following the instructions provided in Importing the IBM HTTP Server keystore to the Handset Server keystore on page 85. Check whether the label is unique. If the label is not unique, the `renew_self_signed_certificate.pl` command fails. You must use a different label.

## Restoring the default certificates

Use the steps in this section if you want to restore the default *CES_server* certificates to IHS.

**Security alert:**

Avaya recommends that you must not use the default certificate as the default certificate and the key pair is the same for all instances of Client Enablement Services.

### Procedure

Restore the default certificate to the Handset Server keystore using the `./restore_default_certs.pl` command.

For example, on Co-resident Handset Server:

```
# cd /opt/avaya/IHS
# ./restore_default_certs.pl
```

For example, on Standalone Handset Server:

```
# cd /opt/avaya/HandsetServer
## ./restore_default_certs.pl
```

The system restores the default *CES_server* certificates to IHS.

# Change the Handset Server configuration

During the Client Enablement Services template installation, you can select the Handset Server configuration to be Standalone or Co-resident.

However, once the installation is complete and if you want to change the Handset Server configuration from Co-resident to Standalone or Standalone to Co-resident, you must perform the steps documented in the following sections.

**Related topics:**

Changing the Handset Server configuration from Co-resident to Standalone on page 88
Changing the Handset Server configuration from Standalone to Co-resident on page 89

# Changing the Handset Server configuration from Co-resident to Standalone

## Procedure

1. On the CLI of the Co-resident Client Enablement Services system, stop Handset Server using the **`service handset_server stop`** command.
2. Ensure that Handset Server stops completely using the **`ps –ef | grep RoutingHandsetServer`** command.

   Ensure that there is no process id corresponding to the Handset Server process.
3. Disable the service by using the following commands:
   - **chkconfig handset_server off**
   - **chkconfig handset_server –del**
4. Rename the `/opt/Avaya/HandsetServer` folder to a temporary name.
   For example, – mv /opt/Avaya/HandsetServer /opt/Avaya/HandsetServer_test
5. Log in to the Client Enablement Services administration client application.
6. Click **Servers** > **Handset**.
7. In the **Handset server Host** field, change the IP address of Handset Server to that of the Standalone system.
8. To save the changes, click **Update**.
9. On the CLI of the Client Enablement Services system, restart WAS by running the **`service 1xp restart`** command.
10. If the system prompts for the administrator user name and password, enter the same.
11. Install Handset Server on the Standalone system.
12. Copy the `keystore.jks` certificate file from the Standalone system to the `/opt/IBM/WebSphere/AppServer70/lib/ext/` directory on the Client Enablement Services system.
13. On the Client Enablement Services administration client application, restart Handset Services by clicking **Monitors** > **Handset** > **Restart**.

14. On the Standalone system, restart Handset Server using the **service handset_server restart** command.
15. Once the Standalone system restarts, users can use the Standalone system IP address or FQDN to log in to the mobile clients.

## Changing the Handset Server configuration from Standalone to Co-resident

### Procedure

1. Log in to the CLI of the Standalone system and delete Handset Server. For more information, see *Administering Avaya one-X® Client Enablement Services*.
2. On the CLI of the Client Enablement Services system, stop WAS by running the **service 1xp stop** command.
3. If the system prompts for the administrator user name and password, enter the same.
4. Navigate to the `/opt/avaya` directory.

   The `RHServer.bin` file is located in the directory.
5. Start the installer by using the **./RHServer.bin** command.
6. Install Handset Server on the Client Enablement Services system.
7. On the CLI of the Client Enablement Services system, start WAS by running the **service 1xp start** command.
8. Once the Client Enablement Services system starts, log in to the Client Enablement Services administration client application.
9. Click **Servers** > **Handset**.
10. In the **Handset server Host** field, change the IP address of Handset Server to that of the Client Enablement Services system.
11. Restart Handset Services by clicking **Monitors** > **Handset** > **Restart**.
12. On the CLI of the Client Enablement Services system, restart Handset Server using the **service handset_server restart** command.
13. Once the Client Enablement Services system restarts, users can use the Co-resident system IP address or FQDN to log in to the mobile clients.

# Uninstalling the Standalone Handset Server and the IBM HTTP Server

## Uninstalling the Standalone Handset Server

### Before you begin

- If you have installed any third-party certificates like VeriSign, ensure that you back up the IHS keystores. The key stores are located in the `/opt/avaya/HandsetServer` directory.
- Ensure that the Handset Server is not running. If the Handset Server is running, stop the Handset Server using the **`service handset_server stop`** command. For more information, see Stopping the Handset Server on page 76.

### Procedure

1. Change to the `/opt/avaya/HandsetServer/_uninst` directory using the `cd /opt/avaya/HandsetServer/_uninst` command.
2. Uninstall the Handset Server using the `./uninstaller.bin –console` command.

## Uninstalling the Standalone IBM HTTP Server

If the Handset Server installation fails for a reason, you must uninstall the IHS.

### Before you begin

If you have installed any third-party certificates like VeriSign, ensure that you back up the IHS keystores. The key stores are located at `/opt/avaya/HandsetServer`.

### Procedure

1. Change to the `/opt/avaya/IHS` directory using the command: `cd /opt/avaya/IHS`
2. Uninstall the IHS using the command: `./uninstallIHS.sh`

# Chapter 5: Installing, configuring, and upgrading the Transcoding Server

## Transcoding Server checklist

Use the following checklist to install, configure, and upgrade the Transcoding Server. As you ensure that a task is complete, make a check mark in the ✔ column.

| ✔ | Task | References | Notes |
|---|---|---|---|
| | Install Transcoding Server | See Installing on page 92 | |
| | Perform postinstallation checks | See Performing postinstallation checks on page 92 | |
| | Configure Transcoding Server | See Transcoding Server configuration on page 93 | |
| | Stop the Transcoding Server | See Stopping the Transcoding Server on page 93 | |
| | Start the Transcoding Server | See Starting the Transcoding Server on page 93 | |
| | Verify whether the Transcoding Server is running | See Verifying whether the Transcoding Server is running on page 94 | |
| | Verify whether the Transcoding Service is able to connect and initialize the Transcoding Server | See Verifying whether the Transcoding Service is able to initialize the Transcoding Server on page 94 | |
| | Upgrade the Transcoding Server | See Transcoding Server upgrade on page 95 | |

# Transcoding Server installation

The Transcoding Server is required for the mobile client for downloading voice messages on the mobile device.

Use the Transcoding Server for converting the voice message from WAV format, that is, default voice message format, to a format that supported by the mobile client.

By default, the system installs the Transcoding Server with Client Enablement Services in the `/opt/avaya/1xp/transcodingserver` directory.

## Installing

### About this task

During the installation of the Client Enablement Services template, the system installs Transcoding Server on the same server on which you install Client Enablement Services.

### Procedure

1. On the Transcoding Server Web page of the Client Enablement Services template installation, in the **Transcoding Server Port** field, enter the port on which Transcoding Server listens for incoming connections.

   The default port is 8090.

2. Follow the installer prompts and enter the required information from the installation worksheet. For more information, see Installation worksheet: information required by template installation on page 41.

## Performing postinstallation checks

### Procedure

1. Log in to the Client Enablement Services server using SSH terminal as user `craft/craft01` and then switch the user to root using the command **`su - root`** and password *root01*.
2. Change to the `/opt/avaya/1xp` directory.
3. Check whether the `transcodingserver` folder exists in the `/opt/avaya/1xp` directory.

# Transcoding Server configuration

You can update the `TranscodingServer.properties` file to modify the properties of the Transcoding Server. You can find this file in the `opt/avaya/1xp/transcodingserver/config` directory.

This file contains the default server properties. By updating the `TranscodingServer.properties` file, you can only override the *transcoding.server.port* property. The Transcoding Server listens to the port specified in the *transcoding.server.port* property.

You can update all the other property values in the Audio Transcoding Web page of the Client Enablement Services administration Web site. The port specified in the properties file must be same as the port specified on the Client Enablement Services administration Web site.

# Stopping the Transcoding Server

### Procedure

1. Log in to the Client Enablement Services server using SSH terminal as user `craft/craft01` and then switch the user to root using the command **`su - root`** and password *root01*.
2. On the shell prompt, type the **`service transcoding_server stop`** command to stop the Transcoding Server.
   This stops the Transcoding Server. If the server stops successfully, you will see the following output.

```
# service transcoding_server stop
Stopping transcoding_server:                               [  OK  ]
```

# Starting the Transcoding Server

### Procedure

1. Log in to the Client Enablement Services server using SSH terminal as user `craft/craft01` and then switch the user to root using the command **`su - root`** and password *root01*.

2. On the shell prompt, type the **service transcoding_server start** command to start the Transcoding Server.
   This starts the Transcoding Server. If the server starts successfully, you will see the following output.

```
# service transcoding_server start
Starting transcoding_server:                               [  OK  ]
```

# Verifying whether the Transcoding Server is running

### Procedure

You can verify whether the Transcoding Server is running in the following ways:

- At the shell command prompt, run the command: **service transcoding_server status**. The system displays the status of the Transcoding Server.
- Open the `1x_transcoding.log` file from the `/opt/avaya/1xp/transcodingserver/logs` directory and check for the `transcoding server started on port XXXX` message.

  **Note:**

  XXXX defines the port mentioned in `TranscodingServer.properties` file.

- At the shell command prompt, run the command: **ps -ef | grep transcodingserver**. The system displays a process that runs on the Transcoding Server.

# Verifying whether the Transcoding Service is able to initialize the Transcoding Server

### Procedure

You can verify whether the Transcoding Service is able to connect and initialize the Transcoding Server in the following ways:

- On the Monitor Audio Transcoding Services Web page of the Client Enablement Services administration Web site, check whether the current status of the **State** field is set to **Available**.
- The Transcoding Service connects to the Transcoding Server and its state is Connected.
- Open the `1x_transcoding.log` file in the `/opt/avaya/1xp/transcodingserver/logs` directory and check for the following messages: `request received for server configuration` and `transcoding server starting with following properties`.

# Transcoding Server upgrade

When you upgrade the Client Enablement Services template, the system upgrades the Transcoding Server.

The default directory for the **Destination of converted audio messages** property on the Modify Audio Transcoding Web page of the Client Enablement Services administration Web site is `/tmp/transcoding`.

**Note:**

During the template upgrade, the system automatically creates the `transcoding` folder. If the system does not create the folder automatically, then you must manually create this folder before starting the Transcoding Server.

# Chapter 6: Upgrading to Release 6.1 SP3

## Introduction

### Upgrade overview

This chapter provides information on upgrading Client Enablement Services from any previous release to Release 6.1 SP3 on the following servers:

- Dell R610 Server
- HP DL360 G7 Server
- Avaya S8800 Server

### Templates overview

Avaya offers product-specific templates to install different products on System Platform. A template is a definition of a set of one or more applications that you can install on System Platform. Client Enablement Services provides the following templates:

- `onexps_template_16GB.ovf`: If you are installing Client Enablement Services on a system that has 16 GB of RAM or more, you must use this template.
- `onexps_template_24GB.ovf`: If you are installing Client Enablement Services on a system that has 24 GB of RAM or more, you must use this template.

**Note:**

All templates have the same functionality. Select a template depending on the RAM of the system.

You can install the Client Enablement Services template from one of the following locations. Use the option that works best in a specific customer scenario.

- **Avaya Downloads (PLDS)**: The template files are located in Avaya PLDS. The list contains all templates to which your enterprise is entitled. Each line in the list begins with the *sold-to* number so that you can select the appropriate template for the site where you are installing Client Enablement Services. Hold the mouse pointer over the selection to

view more information about the *sold-to* number. The PLDS are available at http://plds.avaya.com.

- **HTTP**: The template files are located on an http server. You can install the template files from the http server to several System Platform servers. You must enter the template URL information.
- **SP Server**: The template files can be copied to the `/vsp-template/` directory in the Console Domain (cdom) of the System Platform server.
- **SP CD/DVD**: The template files are located in the DVD supplied with the system or the DVD created onsite.

**Note:**

If you plan to install the Client Enablement Services template files from a DVD, then you must use a *Double-Layer* DVD media so that the template files fit into a single DVD.

- **SP USB Disk**: The template files are located in a USB flash drive connected to the server. The format of the USB flash drive must be ext3.

**Note:**

If you plan to install the Client Enablement Services template files from a USB, then you must ensure that the template files fit into a single USB.

## Servers overview

Client Enablement Services supports the following Avaya-provided hardware:

| Servers | Notes |
|---|---|
| Dell R610 Server | For the server installation instructions, see *Installing the Dell PowerEdge R610 Server*. |
| HP DL360 G7 Server | For the server installation instructions, see *Installing the HP DL360 G7 Server*. |
| S8800 Server | You must install Client Enablement Services on your existing S8800 server after upgrading the S8800 server with the upgrade kit. |

## Servers specifications

The following table includes the hardware requirements for the servers that Client Enablement Services supports.

| Hardware requirements | Dell R610 | HP DL360G7 | S8800 (Upgrade required) |
|---|---|---|---|
| CPU | Dual quad-core processors of 2.4 Ghz. | Dual quad-core processors of 2.4 Ghz. | 2 * 2.2 Ghz or higher.<br>Single processor models are not supported. |
| Memory | 24 GB. | 24 GB. | 16 GB.<br>Requires 10 GB upgrade from the 6 GB default factory configuration. |
| Hard Drive | 4 * 146 GB RAID 5. | 3 * 300 GB RAID 5. | 4 * 146 GB.<br>Requires 2 * 146 GB upgrade from the 2 * 146 GB default factory configuration. |
| Network Card | 100 Mbps / 1Gbps. | 100 Mbps / 1Gbps. | 100 Mbps / 1Gbps. |
| Optical Drive | DVD/CD combination drive is optional. | DVD/CD combination drive is optional. | DVD/CD combination drive is optional. |

# Preupgrade requirements

For a successful upgrade, you must perform the following functions before you begin:

- Download all the software.
- Ensure that there is enough space in the `/vsp-template/` folder. You need a minimum space of 6 GB for upgrade.

## Hardware requirements

You need the following hardware to complete the upgrade process.

- One of the following servers running Client Enablement Services:
  - Dell R610 Server
  - HP DL360 G7 Server
  - S8800 Server
- Required Ethernet CAT5 cables

## Software requirements

You must download the Client Enablement Services templates from PLDS. For more information, see Downloading software in PLDS on page 47.

## Preupgrade data gathering

You must fill data in several fields while upgrading and configuring Client Enablement Services. If you have the information required for these fields ahead of time, your upgrade will be faster and accurate.

Before you upgrade Client Enablement Services:

- Distribute the appropriate checklists to your network administrator.
- Verify that your network infrastructure fulfills the hardware and software infrastructure prerequisites.

To ensure that you gather all the required data before the upgrade, fill out the installation worksheet for upgrading Client Enablement Services. See Installation worksheet: information required by template installation on page 41.

## Upgrade checklist

Use the following checklist to upgrade Client Enablement Services. As you complete a task, make a check mark in the ✔ column.

| ✔ | Task | References | Notes |
|---|---|---|---|
| | Download the required documentation. | See Related documents on page 9. | |
| | Gather preupgrade data. | See Preupgrade data gathering on page 100. | |
| | Download the Client Enablement Services templates from PLDS. | See Downloading software in PLDS on page 47. | |
| | Backup Client Enablement Services. | See Backing up Avaya one-X Client Enablement Services on page 101. | |
| | Upgrade Client Enablement Services. | See Upgrading the Avaya one-X Client Enablement Services system on page 102. | |
| | Verify the Client Enablement Services upgrade. | See Verifying the upgrade on page 105. | |

| ✔ | Task | References | Notes |
|---|---|---|---|
| | Upgrade the Standalone Handset Server. | See Upgrading the Standalone Handset Server on page 106. | |
| | Verify that the IBM HTTP Server (IHS) is running. | See Verifying that the IBM HTTP Server is running post upgrade on page 107. | |
| | Upgrade the Transcoding Server. | See Transcoding Server upgrade on page 95. | |
| | Configure Client Enablement Services. | For more information, see *Administering Avaya one-X® Client Enablement Services*. | |

# Perform preupgrade tasks

## Backing up Avaya one-X® Client Enablement Services

You must backup the Client Enablement Services template files and database before you start the upgrade. For complete information, see Chapter 9, “Template and database backup and restore” in *Administering Avaya one-X® Client Enablement Services*.

# Perform upgrade tasks

## Downloading template files

To download and extract the Client Enablement Services template files before proceeding with the upgrade:

### Procedure

1. To upgrade the template by selecting the **SP Server** option, download the following .tar files:
   - oneXCES_61_3.taraa

- oneXCES_61_3.tarab
- oneXCES_61_3.tarac
- oneXCES_61_3.tarad
- oneXCES_61_3.tarae
- oneXCES_61_3.taraf
- oneXCES_61_3.tarag

2. Copy the above files at the `/vsp-template/` location on cdom.
3. Using the SSH terminal of cdom, extract or untar the template files using the **`cat oneXCES_61_3.tara* | (tar x)`** command from the `/vsp-template/` location.

   The system creates the following files in a directory labeled with the version that you downloaded, for example, `/vsp-template/6.1.3.0.12`:

   - `backup_onexps.sh`
   - `lv_rhel.img.gz`
   - `onexps_template.mf`
   - `onexps_template_24GB.ovf`
   - `onexps_template_16GB.ovf`
   - `post_install.sh`
   - `preweb.war`
   - `restore_onexps.sh`
   - `patchplugin_onexps.sh`
   - `versioninfo_onexps.sh`
4. To verify the file checksum, use the **`sha1sum *`** command.

   Compare the results with the checksum information listed in the `onexps_template.mf` file.

# Upgrading the Avaya one-X® Client Enablement Services system

## Procedure

1. Log in to the System Platform Web Console using the advanced administrator login and password.
2. Click **Virtual Machine Management** > **Solution Template**.

The system displays the Search Local and Remote Template Web page. Use this page to select the template that you want to install on System Platform.

3. Select a location from the list in the **Install Templates From** box.
   - Select **Avaya Downloads (PLDS)**, and in the **Template Location** field provide the PLDS URL.
   - Select **HTTP**, and in the **Template Location** field provide the URL of the HTTP server where the template files exist.
   - Select **SP Server** if the template files are copied to the `/vsp-template/` directory of the System Platform server and this option is used to upgrade the Client Enablement Services template.
   - Select **SP CD/DVD**.

     **Note:**

     If you plan to install the Client Enablement Services template files from a DVD, then you must use a Double-Layer DVD media so that the template files fit into a single DVD.
   - Select **SP USB Disk**.

     **Note:**

     If you plan to install the Client Enablement Services template files from a USB, then you must ensure that the template files fit into a single USB.
4. Click **Upgrade**.
   The system displays a confirmation dialog.
5. Click **OK** to continue.
   The system displays the Select Template Web page.
6. Select the template file, and then click **Select** to continue.

   The template file size must correspond to the RAM deployed on the machine.

   The system displays the Template Details Web page with information on the selected template and its Virtual Machines.

   Confirm whether the template that you selected is for Client Enablement Services 6.1 SP3.
7. Click **Upgrade** to start the template upgrade over the currently installed template.
   The system displays the Pre-install configuration details Web page.
8. Click **Next** to continue.
   The system displays the Network Settings Web page. This page is read-only.

   To enter the required information in the template upgrade screens, see the installation worksheet. For more information, see Installation worksheet: information required by template installation on page 41.

9. Click **Next** to continue.
   The system displays the one-X CES License Agreement Web page.
10. Accept the license agreement, and click **Next** to continue.
    The system displays the NTP Server Details Web page.
11. Verify the details, and click **Next** to continue.
    The system displays the LDAP Information Web page.
12. Verify the details in the **User LDAP UserName**, **User LDAP Password**, and **Confirm** fields.

    The remaining fields are read-only.
13. Click **Next** to continue.
    The system displays the LDAP Configuration Web page. This page is read-only.
14. Click **Next** to continue.
    The system displays the SIP Local Web page.
15. Verify the details, and click **Next** to continue.
    The system displays the Handset Server/Service Web page.
16. In the **Handset Service Port** field, enter the value *8888*.
17. Verify the details in the remaining fields, and click **Next** to continue.
    The system displays the Transcoding Server Web page.
18. Verify the details, and click **Next** to continue.
    The system displays the System Manager (SMGR) Web page.
19. Verify the details, and click **Next** to continue.
    The system displays the WebLM Details Web page.

    You cannot modify the WebLM configuration on this page.

    Use the Client Enablement Services administration Web page to modify the WebLM configuration.
20. Click **Next** to continue.
    The system displays the Summary Web page.
21. Confirm the details, and click **Upgrade** to continue with the Client Enablement Services template upgrade.
    The system closes the Summary Web page and the upgrade process continues.
22. Once the upgrade process is complete, click **Commit** to finalize the upgrade.

    If you do not commit the changes, the template will revert to the previous build.

## Verifying the upgrade

### Procedure

1. Log in to the Client Enablement Services administration client using the credentials provided during the template upgrade in the **User LDAP UserName** and **User LDAP Password** fields.

   The default Web page address is `https://<one-X CES IP or FQDN>/admin`, where *one-X CES IP or FQDN* is the IP address or the Fully Qualified Domain Name (FQDN) of the server that hosts Client Enablement Services.

   For example, if the name of the server that hosts Client Enablement Services is `oneXCES` and the domain is `xyzcorp.com`, the Web page address for your administration application is `https://oneXCES.xyzcorp.com/admin`.

   **Note:**

   If you use a third party reverse proxy with the Client Enablement Services server, you must enable the URL filtering on the reverse proxy to disable access to the administration application from outside the corporate network.

2. On the administration client, check whether the system displays the following tabs: **Home**, **Users**, **Servers**, **Scheduler**, **System**, and **Monitors**.
3. Click the **System** tab.
4. In the left pane, select **General**.

   The **Application Server Version** field displays the version of Client Enablement Services.

   If the version number matches the version of Client Enablement Services that you upgraded, the version match indicates that the system completed the upgrade correctly.

# Handset Server upgrade

To upgrade the Handset Server, you do not need to uninstall the earlier installation.

Ensure that the Handset Server is not running. If the Handset Server is running, stop the Handset Server using the **`service handset_server stop`** command. For more information, see Stopping the Handset Server on page 76.

To upgrade the Handset Server on the:

- Standalone Server: Run the latest Handset Server installer, that is, `RHServer.bin`. Follow the installation prompts to complete the installation.
- Co-resident Server: Run the Client Enablement Services install. When you upgrade Client Enablement Services, the system automatically upgrades the Handset Server on the Co-resident Server.

**⚠ Caution:**

The system retains the third-party certificates installed prior to the Handset Server upgrade. Do not reinstall or upgrade the third-party certificates using any additional scripts as this might result in IHS not functioning properly. For instructions on modifying the certificate, see IBM HTTP Server administration and maintenance on page 79.

# Upgrading the Standalone Handset Server

## Before you begin

Copy the `RHServer.bin` file from the `/opt/avaya` directory on the upgraded Client Enablement Services server to Standalone Handset Server.

## Procedure

1. Log in to Handset Server using the SSH terminal.
2. Backup the `keystore.jks` file located in the `/opt/avaya/HandsetServer` directory on Standalone Server.

   If you have installed any third-party certificates like VeriSign, ensure that you back up the IHS keystores first and then restore the keystores after the installation.

   The keystores are located in the`/opt/IBM/HTTPServer` directory.
3. Ensure that Handset Server is not running. If Handset Server is running, stop Handset Server using the **`service handset_server stop`** command.
4. Upgrade Handset Server using the latest Handset Server installer, that is, `RHServer.bin`.

   Follow the installation prompts to complete the installation.
5. Exit the SSH terminal and relogin using SSH on Handset Server.
6. Restore the `keystore.jks` file from your backup location.
   a. Copy the `keystore.jks` file to the `/opt/avaya/HandsetServer` directory.
   b. Start Handset Server using the **`service handset_server start`** command.
7. To verify that Handset Server is running, run the **`service handset_server status`** command.

- If Handset Server is running, the system displays the Handset Server process.
- If Handset Server is not running, start Handset Server using the **service handset_server start** command.

Alternatively, you can verify the status of Handset Server using the **ps -ef | grep RoutingHandsetServer** command.

8. Restart Handset Services from the Client Enablement Services Web administration application.

## Verifying that the IBM HTTP Server is running post upgrade

### Procedure

1. For Co-resident Handset Server deployments:
   a. Log in to the Client Enablement Services server using the SSH terminal.
   b. To verify that the IHS is running, run the **ps -ef | grep HandsetServer** command.
      - If the IHS is running, the system displays the IHS process ID.
      - If the IHS is not running, start the IHS using the **service ihs start** and **service ihs_admin start** commands.
2. For Standalone Handset Server deployments:
   a. Log in to the Handset Server machine using the SSH terminal.
   b. To verify that the IHS is running, run the **ps -ef | grep HandsetServer** command.
      - If the IHS is running, the system displays the IHS process ID.
      - If the IHS is not running, start the IHS using the **service ihs start** and **service ihs_admin start** commands.

# Transcoding Server upgrade

When you upgrade the Client Enablement Services template, the system upgrades the Transcoding Server.

The default directory for the **Destination of converted audio messages** property on the Modify Audio Transcoding Web page of the Client Enablement Services administration Web site is `/tmp/transcoding`.

**Note:**

During the template upgrade, the system automatically creates the `transcoding` folder. If the system does not create the folder automatically, then you must manually create this folder before starting the Transcoding Server.

# Setting up Avaya one-X® Client Enablement Services

To configure the Client Enablement Services system, see *Administering Avaya one-X® Client Enablement Services*.

# Chapter 7: Troubleshooting and maintenance

## Troubleshooting the Avaya one-X® Client Enablement Services installation

### About this task

If you have a problem when you install Client Enablement Services, perform the following actions:

### Procedure

1. Review the topics in the following sections for possible resolutions to your problem.
2. Retry the action. Carefully follow the instructions in the documentation.
3. Retrieve the log files and review all applicable error messages.
4. Note the sequence of steps and events that led to the problem and the messages that the system displays.
5. If possible, capture screen shots that show what happens when the issue occurs.

**Tip:**

If the proposed solutions do not resolve your problem or if your problem is not included in this section, follow your corporate process to obtain support.

## Unable to access System Platform Web Console

You cannot reach System Platform Web Console. Also, when you try to ping Console Domain, you do not get a response.

# Troubleshooting steps

At the **xm list** command, the system displays information about the virtual machines that are currently running on a Linux operating system.

The system displays only three virtual machines: System Domain shown as `Domain-0`, Client Enablement Services shown as `onexps`, and Console Domain shown as `udom`.

A state of `r` indicates that the virtual machine is running. A state of `b` indicates that the virtual machine is blocked.

**Note:**

The blocked state does not indicate a problem with the virtual machine but that the virtual machine is currently not using any CPU time.

Other possible virtual machine states are:

- p: paused
- s: shutdown
- c: crashed

If the virtual machine is in the p, s, or c state, you cannot reach System Platform Web Console. Therefore, you cannot ping Console Domain.

For more information, see *Installing and Configuring Avaya Aura™ System Platform*.

### Procedure

1. Log in to System Domain (Domain-0) as `admin/admin01`.
2. Enter **su -** to log in as root.
3. At the prompt, type **xm list**.
4. On the Linux screen, type `exit` to log off as root.
5. Type `exit` again to log off from System Domain (Domain-0).
6. If the state of Console Domain is not `r` or `b`, then you must reinstall System Platform and ensure that Console Domain is accessible.

# Template installation fails

The template installation can fail for any of the following reasons:

- **Checksum mismatch**: The system returns this error on the initial pages during the installation when the system cannot verify the *Checksum* of image files.
- **Memory allocation error**: The system returns this error on the initial pages during the installation due to insufficient memory. The system displays the following error message: `Insufficient resources to install this template (Insufficient memory. Requested 8192MB (more), available free space 6488MB).`
- **Kernel mismatch**: The system returns this error on the last page during the installation.
- **Post-install plug-in failed**: The system returns this error on the last page during the installation or when the installation is stuck at this step.
- The template installation plug-in is stuck at the last stage for more than an hour.

## Troubleshooting steps

### Procedure

Select the solution that matches the reason for template failure:

- **Checksum mismatch**: Download the template files again.
- **Memory allocation error**: Check the available RAM on the system and then install the Client Enablement Services template.
- **Kernel mismatch**: Reboot Domain-0 from System Platform Web Console. In the left pane, click **Server Management** > **Server Reboot/Shutdown** and then click **Reboot**.
- **Post-install plug-in failed**: Reboot cdom from System Platform Web Console. In the left pane, click **Virtual Machine Management** > **Manage**. Click the **cdom** link and then click **Reboot** and try the installation again.
- If the plug-in is stuck during the installation of the template and the in-progress status does not change, check if you can reach the Client Enablement Services IP address using the ping command. If the ping command indicates that the Client Enablement Services IP address is not reachable, cancel the existing template installation. Reboot cdom from System Platform Web Console and try the installation again.

- If you do not know the reason for template failure, perform the following actions:
  - Check if all the required files are downloaded.
  - Check if the file permissions are correct.
  - Check if the System Manager server and the Client Enablement Services server are having the same time stamp.
  - Ensure that Client Enablement Services can access System Manager
  - Ensure that LDAP is functional.
  - Check if the LDAP service account password includes the special character $. If the password includes the special character $, and you install the Client Enablement Services template, the template installation is stuck at the last stage for a long time.

# Template installation pauses indefinitely

The Client Enablement Services template installation pauses indefinitely. Additionally, the `post_install_config.log` file in the `/opt/vsp/log` directory on the system on which you are installing the template logs the following error:

```
./runinstallapps.sh /opt/IBM/WebSphere/AppServer /opt/avaya/1xp avaya ****** < /opt/
vsp/bin/input.txt
WASX7023E: Error creating "SOAP" connection to host "localhost"; exception
information:
com.ibm.websphere.management.exception.ConnectorNotAvailableException:
[SOAPException: faultCode=SOAP-ENV:Client; msg=Error opening socket:
javax.net.ssl.SSLHandshakeException: com.ibm.jsse2.util.g: PKIX path building
failed: java.security.cert.CertPathBuilderException: PKIXCertPathBuilderImpl could
not build a valid CertPath.; internal cause is:
java.security.cert.CertPathValidatorException: The certificate issued by O=AVAYA,
OU=MGMT, CN=default is not trusted; internal cause is:
java.security.cert.CertPathValidatorException: Certificate chaining error;
targetException=java.lang.IllegalArgumentException: Error opening socket:
javax.net.ssl.SSLHandshakeException: com.ibm.jsse2.util.g: PKIX path building
failed: java.security.cert.CertPathBuilderException: PKIXCertPathBuilderImpl could
not build a valid CertPath.; internal cause is:
java.security.cert.CertPathValidatorException: The certificate issued by O=AVAYA,
OU=MGMT, CN=default is not trusted; internal cause is:
java.security.cert.CertPathValidatorException: Certificate chaining error]
```

# Troubleshooting steps

### Before you begin

If you are using System Manager, you must verify the certificates on System Manager before you install the Client Enablement Services template.

### Procedure

1. Revisit the expiry date of the System Manager certificates.
2. Regenerate the certificates on System Manager.
3. Cancel the current Client Enablement Services template installation.
4. Reboot cdom from System Platform Web Console.
5. Start the Client Enablement Services template installation.

## Template installed but Avaya one-X® Client Enablement Services does not run

Even after the installation of the template is complete, Client Enablement Services might not run due to any of the following reasons:

- Input error
- Unexpected syntax in input
- Post-install plug-in failed
- Cdom not restarted after you delete the existing template

## Troubleshooting steps

### Procedure

Perform the following:

- Log in to the System Platform Web Console and ensure that the Client Enablement Services virtual machine is running.
- Log in to the CLI of the Client Enablement Services virtual machine as an administrator. If login fails, reboot the Client Enablement Services virtual machine using the System Platform Web Console and try logging in again.
- Log in to the CLI of the Client Enablement Services virtual machine as a root user and execute the `service 1xp restart` command.
- Check the vsp logs in the `/opt/vsp/log` directory for any failure.
  - `post_install_config.log`: Logs the results of the installation
  - `restore_template.log`: Logs the results of the template restore. The system performs the restore after installation upgrades.

- Check the Client Enablement Services `trace.log` file in the `/opt/IBM/WebSphere/AppServer/profiles/default/logs/server1` directory.
- If the plug-in is stuck during the installation of the template, and the in-progress status does not change, you must reboot the cdom using the System Platform Web Console and try the installation again.
- Check if the LDAP service account password includes the special character $. If the password includes the special character $, when you log in to the Client Enablement Services administration application, the system displays an error message.
- If you are installing a new template, you must restart the cdom using the System Platform Web Console after you delete the existing template.

# Out-of-memory error

If you reinstall the template by deleting and installing the template multiple times, the system might display an out-of-memory space permanent generation (PermGen) error.

The system displays the error if you did not reboot the cdom using the System Platform Web Console, after you delete the existing template.

# Troubleshooting steps

### About this task

Perform the troubleshooting steps given here to ensure that a PermGen error does not occur.

### Procedure

1. Delete the template.
2. Restart Tomcat by performing the following steps:
   a. Log in to the cdom as `admin/admin01`.
   b. Enter **su -** to log in as root.
   c. At the prompt, type `/sbin/service tomcat restart`
3. Log in to the System Platform Web Console.
4. Install the template.

# Unable to log in to the Avaya one-X® Client Enablement Services Web administration portal

You cannot log in to the Client Enablement Services Web administration portal, or you get a 500 internal error on login.

## Troubleshooting steps

### Procedure

Perform the following:

- Ensure that the LDAP server is connected and running.
- Ensure that the user name and password are correct.
- Ensure that the user name is part of the Administrator Security Group.
- Ensure that the database is running.
  - If the database is not running, log in to the CLI of the Client Enablement Services server as root user.
  - Switch to dbinst user using the `su – dbinst` command.
  - Run the `db2start` command.
  - Switch to the root user and restart WAS by using the `service 1xp restart` command.

# Unable to log in to the Avaya one-X® Mobile client

You have installed the Handset Server. However, the user is unable to log in to the Avaya one-X® Mobile client.

## Troubleshooting steps

### Procedure

1. Log in to the CLI of the server on which you installed the Handset Server.
2. Check the `handset_server.properties` file in the `/opt/avaya/HandsetServer` directory to ensure all the values are correct.
3. Check if the Handset Server is running using the `ps –ef | grep HandsetServer` command.
   - If the Handset Server is not running, start the Handset Server using the `service handset_server start` command.
   - If the Handset Server is running, restart the Handset Server using the `service handset_server restart` command. Restart the Handset Service from the Client Enablement Services administration client using the Monitors tab, and then update the user to log in to the Avaya one-X® Mobile client.
4. If the user is still unable to login, perform the following:
   a. Quit the currently running Handset Server process using the command `Kill -9 <PID>`.
   b. Start the Handset Server.
   c. Restart the Handset Service from the Client Enablement Services administration client using the **Monitors** tab, and then update the user to log in to the Avaya one-X® Mobile client.

## Transcoding Service cannot connect to the Transcoding Server

On the Monitor Audio Transcoding Services Web page of the Client Enablement Services administration website, check whether the status of the **State** field is set to **Unavailable**.

The status indicates that the Transcoding Service is unable to connect to the Transcoding Server or the Transcoding Server configuration has a problem.

## Troubleshooting steps

### Procedure

Perform the following:

- Check whether the Transcoding Server is running as mentioned in Verifying whether the Transcoding Server is running on page 94.
- Open the `TranscodingServer.properties` file from the `opt/avaya/1xp/transcodingserver/config` directory. Ensure that the value of the *transcoding.server.port* property is the same as the value specified in the **Transcoding Server Address: Port** field on the Modify Audio Transcoding Web page of the Client Enablement Services administration website.
- Check whether the system creates the `/tmp/transcoding` directory for the **Destination of converted audio messages** property on the Modify Audio Transcoding Web page of the Client Enablement Services administration website. This directory must be present on the server.
- Check the host IP address at **Servers** > **Audio Transcoding** > **Transcoding Server Address**. By default, the address is the same as the loopback IP address. The Transcoding Server can function on both the loopback and the Client Enablement Services IP address.

# Secure SSL connection between servers fails

If you do not synchronize the time stamps, the secure SSL connection between the servers fails.

Time synchronization ensures that time stamps for all integrated systems are consistent.

## Troubleshooting steps

### Procedure

1. Log in to the cdom and the Client Enablement Services systems using the SSH terminal as user `craft/craft01` and then switch the user to root using the **`su - root`** command and *root01* password.
2. Check the date on both the systems using the `date` command.

If the time zone differs, you must use NTP for both cdom and Client Enablement Services to correct this mismatch.

# Trace errors using log files

This topic lists the log files that you can use to trace errors during the troubleshooting process.

### Console domain log files

- Log files in the `/var/log/vsp` directory
- Files in the `/vspdata/template/onexps_template` directory

### Client Enablement Services domain log files

- Log files in the `/opt/vsp/log` directory
- IBM log files in the `/opt/IBM/WebSphere/AppServer/profiles/default/logs/server1` directory

### Client Enablement Services domain files that are updated during the template installation

- `/opt/avaya/1xp/AcpInstallationConfig.sql`
- `/opt/avaya/1xp/AcpInstallationWebLM.sql`
- `/opt/avaya/1xp/config.properties`
- `/opt/avaya/1xp/installapps.py`
- `/opt/avaya/1xp/SIP_local_update.sql`
- `/opt/avaya/HandsetServer/handset_server.properties`

### Handset Server log files

The Handset Server log files are located in the `/opt/avaya/HandsetServer/logs` directory.

- To check all logs, view the `hs.log` file.
- To check only the error information, view the `hs_errors.log` file.
- To check only the I/O logging information, view the `hs_io.log` file.

To view the properties for the Handset Server log files, check the `log4j.properties` file located in the `/opt/avaya/HandsetServer` directory.

# Commands for use in Avaya one-X® Client Enablement Services

- To start the Client Enablement Services server, on the shell prompt, type the **service 1xp start** command.
- To stop the Client Enablement Services server, on the shell prompt, type the **service 1xp stop** command. The system prompts you to enter your user name and password when the system tries to stop the server.
- To restart the Client Enablement Services server, on the shell prompt, type the **service 1xp restart** command. The system prompts you to enter your user name and password when the system tries to stop the server.
- If you fail to access the `https://<one-X CES IP or FQDN>/mobileapps` page from Avaya one-X® Mobile or a browser, you must check the `access_log` file using the `tail -f /opt/IBM/HTTPServer/logs/access_log` command.

# Enabling VNC server for maintenance

### Before you begin

You must stop or configure the firewall (iptables) to allow VNC access. If the iptables are running or not configured to allow a VNC connection, you cannot access the system using VNC.

### Procedure

1. Log in to the Client Enablement Services server using SSH terminal as user `craft/craft01` and then change the user to root using the **su - root** command and *root01* password.
2. Start the VNC server using the `vncserver` command.

   **Note:**

   When you run this command for the first time, you must set a password.

   a. To allow access to the desktop, you must edit the `xstartup` file. This file is located in the home directory of the user in the `~/.vnc/xstartup` path.

      Uncomment the following lines, that is, remove the # sign:

      - `#unset SESSION_MANAGER`
      - `#exec /etc/X11/xinit/xinitrc`

b. To change the access password, type `vncpasswd`.

3. Stop the VNC server using the `vncserver –kill :1` command.

# Appendix A: Port usage

| Server | Network or Application Protocol | Destination Port(s) | Source Port(s) | Comments |
|---|---|---|---|---|
| Messaging | TCP or SMTP | 25 | 1024-65535 | SMTP for sending e-mail and SMS |
| | SSL or SMTP | 465 | 1024-65535 | SMTP for sending e-mail and SMS |
| | SSL or IMAP4 | 993 | 1024-65535 | IMAP for retrieving voicemails and faxes for display, and audio playback for user |
| | TCP or LDAP | 389 or 636 | 1024-65535 | LDAP for Messaging |
| Conferencing | TCP | 2002 | 1024-65535 | Protocol for communicating with Meeting Exchange |
| | TCP or BCAPI | 5040 with auto-increment | 1024-65535 | BCAPI protocol for communicating with Meeting Exchange |
| | UDP or BCAPI | 5040 with auto-increment | 1024-65535 | BCAPI protocol for communicating with Meeting Exchange |
| Presence Services | SIP over MLTS | 5061 - SIP<br>9072 - LPS Consumer Port<br>9070 - LPS Supplier Port<br>2009 - RMI | 1024-65535 | Presence updates for a contact |
| WebLM | SSL or HTTP | If the WebLM is local, the port is 8443.<br>If WebLM is on System Manager, the port is 52233. | 1024-65535 | Communication with Avaya Licensing |

| Server | Network or Application Protocol | Destination Port(s) | Source Port(s) | Comments |
|---|---|---|---|---|
| Enterprise Directory | TCP or LDAP | 389 | 1024-65535 | Enterprise contacts and security group information |
| | SSL or LDAP | 636 | 1024-65535 | Enterprise contacts and security group information |
| Client Enablement Services administration client | SSL or HTTP | 443 and 9443 | 1024-65535 | Communication with the administration client |
| Command Line Interface (CLI) | SSH | 22 | 1024-65535 | Open from inside the Client Enablement Services corporate firewall to HTTP server |
| Management Nodes | SNMP | 162 | 1024-65535 | SNMP traps |
| System Manager | SCEP | 443 | 1024-65535 | Communication with System Manager for trust management |
| Client Enablement Services | xSocket using SSL v3 | 8888. You can configure this port. | 1024-65535 | Open from Handset Server to Client Enablement Services |
| Handset Server | xSocket using SSL v3 | 7777. You can configure this port. | 1024-65535 | Open from public Internet to Handset Server |
| Handset Server | JMX | 9999. You can configure this port. | 1024-65535 | Open from only the private network. |
| Handset Device | SSL or HTTP | 443 | 1024-65535 | Download mobile binaries package |
| Session Manager or Communication Manager | SIP | 5060 or 5061 | 1024-65535 | Communication with Session Manager or Communication Manager |

| Server | Network or Application Protocol | Destination Port(s) | Source Port(s) | Comments |
|---|---|---|---|---|
| HTTP | HTTPS | 8008 | 1024-65535 | Open from inside the Client Enablement Services corporate firewall to HTTP server. The port must be open between the Client Enablement Services server and Standalone Handset Server. |

# Appendix B: LDAP Information field descriptions

| Property Name | Property values | | Notes |
|---|---|---|---|
| | Example value | Your value | |
| **LDAP information** | | | |
| **LDAP Type: Active Directory (Single Domain)** | | | |
| **LDAP Host** | *###.###.###.###* | | IP address of the computer that hosts the Enterprise Directory server. The host value can also be the FQDN. |
| **LDAP Port** | 389 | | Port that the Client Enablement Services computer will use to communicate with the Enterprise Directory server.<br>**Note:**<br>You must install the Client Enablement Services template over the non-secure port (389) for LDAP connection. If you want to establish a secure connection, this can be done later using the Client Enablement Services administration client. For more information, see the Appendices in this document. |
| **LDAP Domain** | *users.domain.xyzcorp.com* | | Fully qualified domain name configured on the Enterprise Directory server. |
| **LDAP UserName** | *admin_service_user* | | Enterprise Directory user that you created for the Client Enablement Services administrative service account.<br>**Note:**<br>The user must be a member of the Client Enablement Services administrator's security group |

| Property Name | Property values | | Notes |
|---|---|---|---|
| | Example value | Your value | |
| | | | created for this install. Client Enablement Services uses this user for assigning permissions to users for performing administrative tasks. |
| **LDAP Password** | | | Password for the Client Enablement Services administrative service account. |
| **Confirm** | | | Confirm password for the Client Enablement Services administrative service account. |
| **LDAP Type: Active Directory Application Mode (ADAM)** | | | |
| **LDAP Host** | ###.###.###.### | | IP address of the computer that hosts the Enterprise Directory server. The host value can also be the FQDN. |
| **LDAP Port** | 389 | | Port that the Client Enablement Services computer will use to communicate with the LDAP server.<br>**Note:**<br>You must install the Client Enablement Services template over the non-secure port (389) for LDAP connection. If you want to establish a secure connection, this can be done later using the Client Enablement Services administration client. For more information, see the Appendices in this document. |
| **Base DN** | dc=sysucd,dc=avaya,dc=com | | The domain name of the LDAP Server in the form: dc=<name>,dc=<organization>,dc=com |
| **Bind DN** | cn=onexces,ou=users,dc=sysucd,dc=avaya,dc=com | | The bind domain name. This field is used to validate the user with the LDAP server.<br>**Note:**<br>The user must be a member of the Client Enablement Services administrator's security group created for this install. Client |

| Property Name | Property values | | Notes |
|---|---|---|---|
| | Example value | Your value | |
| | | | Enablement Services uses this user for assigning permissions to users for performing administrative tasks. |
| **LDAP Password** | | | Password for the Client Enablement Services administrative service account. |
| **Confirm** | | | Confirm password for the Client Enablement Services administrative service account. |
| **LDAP Type: SUN Directory Server Enterprise Edition** | | | |
| **LDAP Host** | ###.###.###.### | | IP address of the computer that hosts the Enterprise Directory server. The host value can also be the FQDN. |
| **LDAP Port** | 389 | | Port that the Client Enablement Services computer will use to communicate with the LDAP server.<br>**Note:**<br>You must install the Client Enablement Services template over the non-secure port (389) for LDAP connection. If you want to establish a secure connection, this can be done later using the Client Enablement Services administration client. For more information, see the Appendices in this document. |
| **Base DN** | dc=Avaya,dc=com | | The base domain name. |
| **Bind DN** | cn=onexces,ou=users,dc=sysucd,dc=avaya,dc=com | | The bind domain name. This field is used to validate the user with the LDAP server.<br>**Note:**<br>The user must be a member of the Client Enablement Services administrator's security group created for this install. Client Enablement Services uses this user for assigning permissions to |

| Property Name | Property values | | Notes |
|---|---|---|---|
| | Example value | Your value | |
| | | | users for performing administrative tasks. |
| **LDAP Password** | | | Password for the Client Enablement Services administrative service account. |
| **Confirm** | | | Confirm password for the Client Enablement Services administrative service account. |
| **LDAP Type: IBM Domino Server and Novell eDirectory** | | | |
| **LDAP Host** | ###.###.###.### | | IP address of the computer that hosts the Enterprise Directory server. The host value can also be the FQDN. |
| **LDAP Port** | 389 | | Port that the Client Enablement Services computer will use to communicate with the LDAP server.<br>**Note:**<br>You must install the Client Enablement Services template over the non-secure port (389) for LDAP connection. If you want to establish a secure connection, this can be done later using the Client Enablement Services administration client. For more information, see the Appendices in this document. |
| **Bind DN** | cn=onexces,ou=users,dc=sysucd,dc=avaya,dc=com | | The bind domain name. This field is used to validate the user with the LDAP server.<br>**Note:**<br>The user must be a member of the Client Enablement Services administrator's security group created for this install. Client Enablement Services uses this user for assigning permissions to users for performing administrative tasks. |
| **LDAP Password** | | | Password for the Client Enablement Services administrative service account. |

| Property Name | Property values | | Notes |
|---|---|---|---|
| | Example value | Your value | |
| **Confirm** | | | Confirm password for the Client Enablement Services administrative service account. |
| **LDAP Configuration** | | | |
| Microsoft ADAM **Admin Group** | cn=oneXCESAdmin,cn=users,dc=groups,dc=domain,dc=xyzcorp,dc=com | | The template installation uses the administrator security group to assign permissions to users who will administer Client Enablement Services in the Administration application. |
| SUN Directory Server Enterprise Edition **Admin Group** | | | |
| IBM Domino Server **Admin Group** | | | |
| Novell eDirectory **Admin Group** | | | |
| Microsoft ADAM **Audit Group** | cn=oneXCESAudit,cn=users,dc=groups,dc=domain,dc=xyzcorp,dc=com | | The template installation uses the auditor security group to assign permissions to users who will have read-only access to the Client Enablement Services configuration in the Administration application. |
| SUN Directory Server Enterprise Edition **Audit Group** | | | |
| IBM Domino Server **Audit Group** | | | |
| Novell eDirectory **Audit Group** | | | |
| Microsoft ADAM **User Group** | cn=oneXCESUser,cn=users,dc=groups,dc=domain,dc=xyzcorp,dc=com | | The template installation uses the user security group to assign permissions to users who will access the Client Enablement Services application. |
| SUN Directory Server Enterprise Edition **User Group** | | | |
| IBM Domino Server **User Group** | | | |
| Novell eDirectory **User Group** | | | |

# Appendix C: Configuring Microsoft Active Directory

## Configure secure LDAP connection for Microsoft Active Directory

You can configure Client Enablement Services communication with Active Directory using Lightweight Directory Access Protocol (LDAP) over Secure Socket Layer (SSL), also known as LDAPS, using the procedures described in this section. The configuration involves the following steps:

1. Configuring Active Directory SSL
2. Configuring WebSphere
3. Configuring Client Enablement Services for LDAPS

### Prerequisite

Install Client Enablement Services using LDAP and then configure WebSphere with the Active Directory certificate authority (CA) to communicate using SSL.

## Configuring Active Directory SSL

If you have not configured Active Directory to use SSL, you must perform the following.

### Before you begin

- Install Certificate Authority (CA) on a Windows 2003 server or on a Windows 2008 server.
- Active Directory must be present on a Windows 2003 server or on a Windows 2008 server.

### About this task

Use the following steps to configure Active Directory to enable communication-using SSL.

### Procedure

1. Obtain a root certificate using the following steps:
   a. Open certificate authority Web page in your browser using the *http://<CA-server>/certsrv* link.
   b. When the system prompts you for a user service and a password, use an account with Administrator privileges on the CA server.
   c. Click **Download a CA certificate, certificate chain, or CRL** link.
   d. Select **Base-64** and then click **Download CA certificate**.
   e. Use download function of your browser to save the certificate as a file with a .cer extension.

   **Note:**

   All root certificates from the same certificate authority are functionally the same. You can download a certificate once and use it repeatedly until it expires.

2. Open the certificate manager using the following steps:
   a. Click **Start** > **Run** on your desktop and type `mmc` in the Run window.
   b. On Microsoft Management Console, click **File** > **Add/Remove Snap-in**. This displays the Add/Remove Snap-in window.
   c. On Add/Remove Snap-in window, select the **Standalone** tab and click **Add**. This displays the Add Standalone Snap-in window.
   d. Select certificates from the Add Standalone Snap-in window and click **Add**.
   e. Select a computer account and click **Next**.
   f. Select a local computer and click **Finish**.
   g. Click **Close** on the Add Standalone Snap-in window.
   h. Click **OK** on the Add/Remove Snap-in window

3. Install the root certificate for the Certificate Authority using the following steps on the Microsoft Management Console:
   a. On the left pane, open the `Certificates (Local Computer)\Trusted Root Certificate Authorities\Certificates` folder.
   b. Click **Action** > **Tasks** > **Import**.
   c. On the Certificate Import wizard, click **Next**.
   d. Click **Browse**, select the root certificate file, and click **Open** > **Next**.
   e. Click **Next**.
   f. Select **Place all certificates in the following store**.
   g. Click **Browse**, select **Trusted Root Certificate Authorities**, and click **OK**.
   h. Click **Next**.
   i. Click **Finish**.
   j. On the right pane, select the new certificate you just imported.
   k. Click **Action** > **Properties**.
   l. Enter a name that identifies the CA.

m. Click **OK**.

4. Generate a policy file for the Domain Controller on the DC machine using the following steps:
   a. Obtain a copy of the reqdccert.vbs script. This is available on the Web at several locations.
   b. From the command prompt, run the **`reqdccert.vbs`** script.
   c. Verify if the system creates the following files:
      - `<dc-name>.inf`
      - `<dc-name>-req.bat`
      - `<dc-name>-vfy.bat`
5. Edit `<dc-name>.inf` with a text editor using the following steps:
   a. Under the line that says [NewRequest], add a line:

      `Subject="CN=<dc-fqdn>"`

      where, <dc-fqdn> is the fully qualified domain name (FQDN) of the DC. You can view the FQDN of the DC from **Start** > **Control Panel** > **System** > **Computer Name**, where it is displayed as **Full Computer name**. Do not forget to add the prefix `CN=` and put the whole subject in quotes.
   b. Delete the line that says **Critical=2.5.29.17**. WebSphere does not recognize this extension.
   c. Save the file.
6. Create the certificate request on the Domain Controller using the following steps:
   a. Open the directory where the `<dc-name>.inf` is located and run the command:

      `certreq –new <dc-name>.inf <dc-name>.req`
   b. Copy the `<dc-name>.req` and `<dc-name>-req.bat` files to the CA machine.
7. Create the domain controller certificate using the following steps:
   a. . Open the command prompt, and go to the directory where the system copied the files.
   b. Run the BAT file`<dc-name>-req`.
   c. When prompted, select the CA and click **OK**. The script prompts you to save the `<dc-name>.cer` file.

      **Note:**

      In Window Server 2008, if you get an error at this step, you can use the certificate request file `<dc-name.req>` to request a certificate from the CA, and obtain a certificate file <dc-name.cer> directly.
   d. Log on to the CA, and open the Certification Authority application from **Start** > **Administrative Tools** > **Certification Authority**.

e. Open the **Pending Requests** folder.
f. Accept the request for <dc-name>.
g. Open the **Issued Certificates** folder.
h. Open the new certificate.
i. Click the **Detail** tab and click **Copy to file**.
j. Select a `Base-64.cer` file and export it.

8. Install the Domain Controller Certificate on the Domain Controller using the following steps:
   a. Copy the .cer file from CA to the DC machine.
   b. In the directory where the `<dc-name>.cer` file is located, run the command:
      ```
      certreq –accept <dc-name>.cer
      ```
   c. Open the certificate manager for the local system as described in step 2.
   d. In the left pane, open the **Certificates** folder from the `<local drive>\Personal\Certificates` folder and make sure the certificate is installed.
   e. (Optional) Rename the certificate. For example, Enable LDAPS.
   f. Reboot the Domain Controller.

# Configuring WebSphere

### About this task

After configuring the Active Directory for LDPS, use the IBM WebSphere console to configure WebSphere. To configure WebSphere:

### Procedure

1. Log on to the IBM WebSphere console using the Client Enablement Services administrative credentials. The address for the IBM administrative console is `https://<oneXCESMachine>:9043/ibm/console`.
2. Under the **Security** section, click the **SSL certificate and key management** link.
3. On the SSL certificate and key management page, go to **Key stores and certificates** > **NodeDefault** > **Signer certificates**, and click **Retrieve from port**.
4. Enter the **Host**, **Port** and **Alias** information. The **Host** is the IP Address of your DC machine, and the **port** is the port for the LDAPS service. Port 636 is the default port.
5. Click **Retrieve signer information**.
6. Click **OK** and save the configuration.

7. Use the IBM console to verify the connection with the LDAP server. This test does not use Client Enablement Services code, so it is a good validation for the environment setup. To perform validation on the IBM console:
   a. Click **Security** > **Secure administration, applications, and infrastructure**.
   b. If your system is already set up to talk to a single AD environment, the **Available realm definitions** field must be set to Standalone LDAP registry.
   c. Click **Configure**.
   d. Configure the parameters for your Active Directory. If the system is configured to communicate with Active Directory, change the **Port** to `636` and the **SSL Settings** to enable SSL.
   e. Click **Test connection**. If the test is successful, the system displays the following message:
   `<LDAP IP Address> on port 636 was successful`

      **Note:**

      If the test is not successful, you must take a corrective action based on the error message.
   f. Log out of the IBM Console.

      **Important:**

      Do not change the configuration here, since changing the configuration on Client Enablement Services also changes this configuration. Do not save the connection at WAS.

# Configuring Avaya one-X® Client Enablement Services for LDAPS

### Procedure

1. Log on to Client Enablement Services administration client: `https://<oneXCESServer>:9443/admin`.
2. Open the **System** tab and click **Enterprise Directory**.
3. Select the domain for which you must set the LDAPS configuration.
4. Change **Port** value to `636` and the select **Secure Port**.
5. Save the configuration.

6. Restart Client Enablement Services.

# Appendix D: Configuring Microsoft ADAM

## Configure secure LDAP connection for Microsoft ADAM

**Important:**

Client Enablement Services does not support integration with the Presence Services server if you are using Microsoft Active Directory Application Mode (ADAM) as the enterprise directory.

You can configure Client Enablement Services communication with Active Directory Application Mode (ADAM) using Lightweight Directory Access Protocol (LDAP) over Secure Socket Layer (SSL), also known as LDAPS, using the procedures described in the following sections. The configuration involves the following steps:

1. Configuring ADAM SSL
2. Configuring WebSphere
3. Configuring Client Enablement Services for LDAPS

### Prerequisite

Install Client Enablement Services using LDAP and then configure WebSphere with the Active Directory certificate authority (CA) to communicate using SSL.

## Configuring ADAM SSL

Use the procedure documented in the following section as an example and a reference. The procedure describes how to use Microsoft Certificate Services to create and issue the certificate that ADAM uses. For complete instructions on how to set up ADAM to use SSL, see the Microsoft documentation for ADAM.

### Before you begin

- Before you install Microsoft Certificate Services CA, you must install Internet Information Server (IIS).
- Once you install and configure IIS, install and use the Certificates Services to enable SSL for ADAM.

## Procedure

1. Install Certificate Services by clicking **Add or Remove Programs** > **Add/Remove Windows Components**.

   If your operating system is Windows 2003 or 2008 server only, that is, you have not configured Active Directory, select **Stand-alone CA**.

   **Important:**

   Choose the name of the certification authority carefully, because you cannot change the name after the CA setup is complete. When you specify the name of the root CA certificate, do not specify the fully qualified domain name of the workstation host name if you have installed Active Directory on the same workstation as the Certificate Authority services workstation.

   The ADAM certificate requires the name to be the fully qualified domain name of the workstation on which ADAM runs. ADAM cannot have a certificate with the same name as the CA root certificate.

2. For the ADAM system to trust the newly installed Certificate Authority, you must install the root CA certificate onto the system as a trusted root:

   a. Use a Web browser on the workstation running ADAM and go to `http://`*`CA_server_machine`*`/certsrv` to install the CA certificate.

   b. Click **Download a CA certificate, certificate chain or CRL** > **Install this CA certificate chain**.

      If this is the first time you have installed the root CA certificate on the system, the system displays a security warning. Click **Yes** to install the root CA certificate onto the system as a trusted root.

   c. Request a certificate for use with ADAM SSL by using the Web browser and going to `http://`*`CA_server_machine`*`/certsrv`.

   d. Click **Request a Certificate** > **Advanced Certificate Request** > **Create and Submit a request to this CA**.

   e. In the **Name** field, enter the fully qualified domain name of the ADAM system exactly the same way the system displays the name in **My Computer** > **Properties** > **Computer Name**.

   f. Complete the *Advanced Certificate Request* information as per the requirements of your organization.

   g. Select **Server Authentication Certificate** as the type of certificate needed.

   h. Select **Create new key set** as a key option.

   i. Select **Store certificate in the local computer certificate store**.

      You can retain the default values in the other fields unless otherwise required by your organization.

   j. Click **Submit**.

      Ensure you record the *RequestID* number for use in the next step.

3. Use the *Certification Authority* tool to issue the certificate request:

a. Click **Start** > **Administrative Tools** > **Certification Authority**.
b. Expand the Certification Authority CA and click the **Pending Requests** folder.
c. Select the certificate request with the same *RequestID* number from Step 2j.
d. To issue the certificate, right-click the *RequestID* number and click **All Tasks** > **Issue**.
In the *Certification Authority* tool, the system moves the request from the *Pending Request* folder to the *Issued Certificates* folder.

4. Install the issued certificate:
   a. Open a Web browser and enter `http://CA_server_machine/certsrv`.
   b. Select **View the status of a pending certificate request**.
   c. Select the request and click **Install this certificate**.
   The system displays a warning about installing a certificate on the system.
   d. To install the certificate into the system key store, click **Yes**.
5. To install the certificate for use by ADAM, use *Microsoft Management Console*:
   a. Run **mmc.exe** and click **File** > **Add/Remove Snap-in**.
   b. Click **Add...** and select **Certificates snap-in**.
   c. Click **Add**.
   d. On the Certificate Snap-in panel, select **Service Account** and click **Next**.
   e. Select the workstation you want to manage and click **Next**.
   f. On the Service account panel, scroll to locate and select the ADAM instance service name and click **Finish**.
   g. On the Add Standalone Snap-in panel, select **Certificates snap-in** and click **Add**.
   h. Select **Computer Account** and click **Next**.
   i. Select the workstation you want to manage and click **Next**.
   j. Close the Add Standalone Snap-in panel.
   k. To add the snap-ins, click **OK**.
   l. Click **Certificates (Local Computer)** > **Personal** > **Certificates folder** and verify that the system installed the certificate.
   m. Double-click the certificate and confirm that the **General** tab includes the following statement: `You have a private key that corresponds to this certificate.`
   n. Click **OK** to close the Certificate information panel.
6. Use the following steps to assign read permission for the ADAM service account to read the keystore of the certificate:
   a. On the command line, run the **`certutil -store my`** command to identify the Key Container of the ADAM certificate.
   b. Use Microsoft Explorer to navigate to `Documents and Settings\AllUsers\Application Data\Microsoft\Crypto\RSA\MachineKeys` and match the Key Container name you determined in Step 6a with the file in this folder.

c. Right-click the file and click **Properties**.
d. On the **Security** tab, click **Add** > **Advanced** > **Find Now** and choose the service account under which ADAM is running.
e. Click **OK** twice to add read permission to the certificate keystore for the ADAM service account.

# Configuring WebSphere

### About this task

After configuring the Active Directory for LDAPS, use the IBM WebSphere console to configure WebSphere.

### Procedure

1. Log on to the IBM WebSphere console using the Client Enablement Services administrative credentials. The address for the IBM administrative console is `https://<oneXCESMachine>:9043/ibm/console`.
2. In the **Security** area, click the **SSL certificate and key management** link.
3. In the **Configuration settings** area, click **Manage endpoint Security configurations**.
4. In the **Outbound/nodes** area, click the appropriate node: *<servername>.comNode01(NodeDefaultSSLSettings)*.
5. In the **Related Items** area, click **Keystores and Certificates**.
6. Select **NodeDefaultTrustStore**.
7. In the **Additional Properties** area, select **Signer certificate**.
8. Select **Retrieve from port**.
9. In the **Host** field, enter the IP address of the ADAM server.
10. In the **Port** field, enter the SSL port that you configured on the ADAM server.
11. In the **Alias** field, enter the fully qualified domain name of the ADAM server.
12. Select **Retrieve signer information**.
13. Click **OK** and **Apply**.

# Configuring Avaya one-X® Client Enablement Services for LDAPS

### Procedure

1. Log on to the Client Enablement Services administration client: `https://<oneXCESServer>:9443/admin`.
2. Open the **System** tab and click **Enterprise Directory**.
3. Select the domain for which you must set the LDAPS configuration.
4. Change the **Port** value to `636` and then select **Secure Port**.
5. Save the configuration.
6. Restart Client Enablement Services.

# Appendix E: Configuring Novell eDirectory

## Configure secure LDAP connection for Novell eDirectory

This section describes the steps to configure Client Enablement Services communication with Novell eDirectory using LDAP over SSL. You must have simultaneous access to WebSphere and Novell iManager utility to create, exchange, and configure server certificates.

### Prerequisites

Install the following utilities on the system that you want to use to administer Novell eDirectory:

- Novell iManager. To administer Novell eDirectory.
- Certificate Manager add–in. To obtain the Novell Certificate Server configurable from Novell iManager.
- LDAP plug-in. To administer LDAP Server from Novell iManager.

Perform the following steps to configure Client Enablement Services and Novell eDirectory setup over SSL.

## Creating a trusted root container on iManager

### About this task

Open the iManager utility in your browser and perform the following steps.

### Procedure

1. Click **Novell Certificate Server** > **Create Trusted Root Container**.
2. Specify a container name of your choice in the **Container** field.
3. Click **Object selector** and set **Context** as Security.
4. Click **OK**.

# Exporting Novell CA self-signed certificate as a DER file

### About this task

**Important:**

Do not export the private key when you export.

### Procedure

1. On iManager, click **Novell Certificate Server** > **Configure Certificate Authority**.
2. On the **Certificates** tab, select **Self Signed Certificate** and click **Export**.
3. Clear the **Export private key** check box.
4. Select the **DER** format and click **Next**.
5. Save the file.

# Adding the self-signed certificate as a trusted root

### Before you begin

First export the self-signed certificate as a DER file. For more information, see Exporting Novell CA self-signed certificate as a DER file on page 144

### Procedure

1. On iManager, click **Novell Certificate Server** > **Create Trusted Root**.
2. Enter a name for the trusted root.
3. Select `<trusted root container>.Security` file that you exported in the previous step.

# Exporting WebSphere certificate from Avaya one-X® Client Enablement Services server and importing into Novell

### Procedure

1. In WebSphere Web console, click **Security** > **SSL certificate and key management** > **Key stores and certificate**.
2. On the Key stores and Certificates page, click **NodeDefaultKeyStore** > **Personal Certificates** links.
3. Select the default certificate, and click **Extract**.
4. Save the certificate as a DER file on the Client Enablement Services file system, and transfer that file to the machine where you installed iManager.

# Adding WebSphere certificate as a trusted root on Novell eDirectory

### Procedure

1. On iManager, click **Novell Certificate Server** > **Create Trusted Root** links.
2. Enter a name for the trusted root.
3. Select **Security** container as created in previous steps.
4. Browse and select the DER file that you received from WebSphere.
5. Configure the LDAP Server Connection using the following steps:
   a. Set the **Client Certificate** = Requested, and the **Trusted Root Containers** = <trusted root container>.Security.
   b. Click **Save** and then **Refresh**.

# Importing Novell CA certificate into WebSphere

## Procedure

1. In WebSphere Web console, click **Security** > **SSL Certificate and key management** > **Key stores and certificates** > **NodeDefaultTrustStore** > **Signer certificates**.
2. Select the certificate and click **Retrieve from port**.
3. Enter the Novell eDirectory IP Address in **Host** and SSL LDAP port (usually 636) in **Port** fields. Do not save the configuration yet. Use the Client Enablement Services administration user interface to save this configuration as described in step 8.
4. In the WebSphere Web console, select **Security** > **Secure administration, applications, and infrastructure**.
5. Make sure you select the **Standalone LDAP** registry, and click **Configure**.
6. Change the **Port** to be the SSL LDAP port (usually 636).
7. Select the **SSL Enabled** check box to enable SSL and click **Test connection**.

   **Caution:**

   Do not click **Apply** or **Save** at this step.
8. Log on to the Client Enablement Services administration client.
9. On the **System** tab, select **Enterprise Directory**.
10. Select the Novell eDirectory domain, and change the configuration to use the SSL LDAP port.
11. Select the **Secure Port** check box.
12. Save the configuration and restart WebSphere.

# Appendix F: Configuring SUN Directory Server Enterprise Edition

## Configure secure LDAP connection for SUN Directory

You must use your own certificate authority to enable SSL on a SUN directory server, since SUN directory does not have an integrated Certificate Authority (CA). You must have a custom Certificate Authority environment, and it is out of the scope of this document to describe the details for any particular environment.

This section describes how to configure Client Enablement Services communication with SUN directory using LDAP over SSL.

**Note:**

In the SUN directory server, in the Client Control Settings, the default Size Limit is 2000 and the default Lookthrough Limit is 5000. These limits restrict the total number of records processed using LDAP queries and the total number of records visible by the Client Enablement Services server synchronization. Set these limits greater than the total number of user records you want to import to Client Enablement Services server.

## Requesting the certificate using the console

### About this task

You must create the request for server certificate from the SUN directory, process the request for server certificate on CA, and then get the certificate back from CA.

### Procedure

1. On the SUN Directory Service Control Center, click **Directory Servers** >**Servers**.
2. From the list of **Directory Servers**, select a server.
3. Click **Security** > **Certificates**.
4. Click **Request CA-Signed**.

5. On the **Request CA-Signed Certificate** section, enter the following information:

| Field | Description |
|---|---|
| **Common Name** | Fully qualified host name of the Directory Server as it is used in DNS lookups. |
| **Organization** | The legal name of your company or institution. Most CAs require you to verify this information with legal documents such as a copy of a business license. |
| **Organizational Unit** (optional) | Descriptive name for your division or business unit within the company. |
| **City/Locality** (optional) | Name of your city. |
| **State/Province** | Name of your state or province. |
| **Country** | Two-character abbreviation for your country name in ISO format. The country code for the United States is US. For a list of ISO country codes, see *Appendix C: Directory Internationalization* in the *Sun Directory Server Reference Manual*. |

   Click **OK** to proceed to the next page.

6. Enter the password of your security device, and then click **Next**. This is the password set in Creating a Certificate Database.
7. Select **Copy to Clipboard** or click **Save to File** to save the certificate request information in a text file that you must send to the Certificate Authority.

# Installing the server certificate

### Procedure

1. Send the server certificate request information to your Certificate Authority, according to prescribed procedures.

   For example, the CA will ask you to send the certificate request in an e-mail, or you will be able to enter the request through the CA Website.
2. Wait for the CA to respond with your certificate.

Response time for your request varies. For example, if your CA is internal to your company, it will only take a day or two to respond to your request. If your selected CA is external to your company, the response time can be longer.

3. When CA sends a response, save the information in a text file.

   The PKCS #11 certificate in PEM format appears similar to the example.

### Example

```
BEGIN CERTIFICATE

MIICjCCAZugAwIBAgICCEEwDQYJKoZIhKqvcNAQFBQAwfDELMAkGA1UEBhMCVVMx
IzAhBgNVBAoGlBhbG9a2FWaWxsZGwSBXaWRnZXRzLCBJbmMuMR0wGwYDVQQLExRX
aWRnZXQgTW3FrZXJzICdSJyBVczEpMCcGAx1UEAxgVGVzdCBUXN0IFRlc3QgVGVz
dCBUZXN0IFlc3QgQ0EswHhcNOTgwMzEyMDIzMzUWhcNOTgwMzI2MDIzMpzU3WjBP
MQswCYDDVQQGEwJVUzEoMCYGA1UEChMfTmV0c2NhcGUgRGlyZN0b3J5VIFB1Ymxp
Y2F0aW9uczEWMB4QGA1UEAxMNZHVgh49dq2tLNvbjTBaMA0GCSqGSIb3DQEBAQUA
A0kAMEYkCQCksMR/aLGdfp4m0OiGgijG5KgOsyRNvwGYW7kfW+8mmijDtZaRjYNj
jcgpF3VnlbxbclX9LVjjNLC5737XZdAgEDozYwpNDARBglghkgBhvhCEAQEEBAMC
APAwHkwYDVR0jBBgwFAU67URjwCaGqZHUpSpdLxlzwJKiMwDQYJKoZIhQvcNAQEF
BQADgYEAJ+BfVem3vBOPBveNdLGfjlb9hucgmaMcQa9FA/db8qimKT/ue9UGOJqL
bwbMKBBopsDn56p2yV3PLIsBgrcuSoBCuFFnxBnqSiTS7YiYgCWqWaUA0ExJFmD6
6hBLseqkSWulk+hXHN7L/NrViO+7zNtKcaZLlFPf7d7j2MgX4Bo=

END CERTIFICATE
```

### Next steps

You must back up the certificate data in a safe location. If your system ever loses the certificate data, you can reinstall the certificate using your backup file. Once you have your server certificate, you are ready to install it in the certificate database of your server.

# Installing server certificate using the console

### Procedure

1. On the SUN Directory Service Control Center, click **Directory Servers** >**Servers**.
2. From the list of **Directory Servers**, select a server.
3. Click **Security** > **Certificates**.
4. On the Add Certificate page, enter a name of the certificate in the **Certificate Name** field and copy the text from the CA certificate received in the **Certificate** field.
5. Click **OK**.
6. Verify the certificate by providing the password that protects the private key. Use the same password that you provided for Creating a Certificate Database.

7. Click **Done** to close the wizard.

   Your new certificate must appear in the list on the **Server Certs** tab. Your server is now ready for SSL activation.

8. Reboot the Directory Server.

# Trusting the Certificate Authority using the console

### About this task

After securing the CA certificate, you can use the Certificate Install Wizard to configure the Directory Server to trust the Certificate Authority.

### Procedure

1. Perform one of the following steps to begin:
   - On the **Tasks** tab of the Directory Server console, click **Manage Certificates**.
   - On the top-level **Tasks** tab of the Directory Server console, select the **Manage Certificates** from the **Console** > **Security** menu.

   This displays the Manage Certificates window.
2. On Manage Certificates window, select the **CA Certs** tab and click **Install**. This opens the Certificate Install Wizard window.
3. Perform one of the following steps to submit the certificate:
   - If you saved the certificate to a file, enter the path in the field provided and click **Next**.
   - If you received the certificate through e-mail, copy and paste the certificate including the headers into the text field provided and click **Next**.
4. Verify that the certificate information displayed is correct for your CA and then click **Next**.
5. Specify the certificate name, and then click **Next**.
6. Select the purpose of trusting this CA from the following choices. You can select one or both depending on your corporate requirement and policy:
   - **Accepting connections from clients (Client Authentication)**. Select this check box if your LDAP clients perform certificate-based client authentication by presenting certificates issued by this CA.

- **Accepting connections to other servers (Server Authentication)**. Select this check box if your server functions in a replication supplier role over SSL with another server that has a certificate issued by this CA.

7. Click **Done** to close the wizard.

# Activating SSL on SUN Directory Server

### About this task

Activate SSL on SUN Directory Server and configure SSL to use the new server certificate. The following procedure activates SSL communications and enables encryption mechanisms in the directory server:

### Procedure

1. On the top-level **Configuration** tab of the Directory Server console, select the root node with the server name, and then select the **Encryption** tab in the right panel. The **Encryption** tab displays the current server encryption settings.
2. Select the **Enable SSL for this Server** check box to enable encryption.
3. Select **Use this Cipher Family** check box.
4. Select the certificate that you want to use from the drop-down menu.
5. Click **Cipher Settings** and select the ciphers you want to use in the Cipher Preference dialog.
6. Set your preferences for client authentication. Select one of the following preferences:
   - **Allow client authentication**. This is the default setting. With this option, authentication is performed on the clients request.
   - **Use SSL in SUN Server Console**. Select this option if you want the console to use SSL when communicating with Directory Server.
7. Click **Save** or set the secure port you want the server to use for SSL communications in both LDAP and DSML-over-HTTP protocols.

   **Note:**

   All connections to the secure port must use SSL regardless of whether you configure the secure port. After you activate SSL, clients can use the Start TLS operation to perform SSL encryption over the non-secure port.

8. Restart the directory server.

# Adding server certificate in WebSphere

### About this task

To import the SUN Directory Server certificate into WebSphere:

### Procedure

1. Go to the WebSphere (WAS) console by using the *https://<onexp server ip>:9043/ibm/console* link.
2. In WebSphere Web console, select **Security** > **SSL Certificate and key management** > **Key stores and certificates** > **Node Default Trust Store** > **Signer certificate**.
3. Select **Retrieve from port**.
4. Specify the SUN Directory Server IP address and SSL LDAP port (usually 636).
5. Enter an **Alias** for the certificate. For example, `sunonecert`.
6. Click **Retrieve Signer information**.
7. Click **OK**.

**Important:**

Do not save the connection here. Use Client Enablement Services administration application to save the configuration.

# Testing connection from WebSphere to SUN Directory Server

### About this task

Test the LDAP connection to see if it works but do not save it. Use Client Enablement Services administration UI to save this configuration.

### Procedure

1. In the WebSphere Web console, select **Security** > **Secure administration, applications, and infrastructure** and select the **Standalone LDAP registry** check box.

2. Click **Configure**.
3. Change the port to make it an SSL LDAP port (usually 636).
4. Select **SSL enabled** check box to enable SSL.
5. Click **Test Connection**. The system must return a success message.

# Changing Avaya one-X® Client Enablement Services configuration for secure connection

### Procedure

1. Log in to the Client Enablement Services administration client.
2. Select **System** tab and click **Enterprise Directory**.
3. Choose the SUN Directory Server domain, and change the configuration to use the SSL LDAP port.
4. Select the **Secure Port** check box.
5. Save the configuration and restart WebSphere.

# Appendix G: Configuring IBM Domino Server

## Configure secure LDAP connection for IBM Domino Directory

You must use your Certificate Authority (CA) to enable SSL on a Domino directory since Domino does not have an integrated CA. You can have a custom CA environment, but it is out of the scope of this document to describe the details for a particular environment. This section describes how to configure Client Enablement Services to enable communication with the Domino directory using LDAP over SSL.

## Registering an Internet certifier

### Procedure

1. Launch the Domino Administrator client by using the Administrator ID file.
2. Select the correct domain and server.
3. Click **Configuration** to go to the **Configuration** tab.
4. From the menu, click **Configuration** > **Registration** > **Internet Certifier**.
5. Select **I want to register a new Internet certifier that uses the CA process**, and click **OK**.
6. In the **Register a New Internet Certifier** dialog box, click **Create Certifier Name** and fill in a common name such as `MyCompany CA`, and click **OK**.
7. Select the server on which you want to put the certifier for the CA.
8. You can use the default Issued Certificate List (ICL) database name or modify it. For example, icl\icl_MyCompany.nsf.
9. Select one of the following options for the **Encrypt Certifier ID with** settings:
    - Encrypt ID with Server ID: lowest security, no password required

- Encrypt ID with Server ID and Require password to activate certifier
- Encrypt ID with Locking ID and choose the person whose ID will be used to secure the new CA

10. Click **OK**.
    The system displays a success message.

### Next steps

Run the certificate authority task.

# Running the CA task

### Procedure

1. On the **Configuration** tab of the Domino Administrator client, perform one of the following actions:
   - Type **load** *ca* if the task is not running.
   - Type **tell** *ca refresh* if the CA task is running.
2. To ensure that the new CA is ready for use, type **tell** *adminp process all*.
3. Type **tell** *ca stat*.
   If your new CA does not show up in the list, type **tell** *adminp process all*.
4. Type **tell** *ca refresh*.
   The system displays the new CA, if included in the list.
5. To verify that the new CA is initialized, type **tell** *ca stat*.
6. To activate your password when your CA is not active, type **tell** *ca activate certifier number password*
7. To obtain the actual value for certifier number, type **tell** *ca stat*.
   The system lists each CA with a number preceding it. Use this number to identify a **tell** command.

### Next steps

Creating and setting up the certification request database

# Creating and setting up the certification request database

### Procedure

1. On the Domino Administrator client, select **File** > **Database** > **New**, then select your server.
2. In the **Specify New Database Name and Location** section of the **New database** page, enter a title for the database. For example, enter `Western CA database`.
3. Enter a name for the database file, for example, `certreq.nsf`.

   Each Internet Certifier requires a unique Certificate Requests database. If you are going to create additional Internet CAs in future, provide a unique title for the associated CAs in the Certificate Requests database. For example, you can provide the title `Cert Req MyCompany`, and a file name such as `CR_myco.nsf`. Keep the file name short so that it is easier to enter as part of a URL in a Web browser.
4. In the **Specify Template for New Database** section of the **New database** page, ensure that the template server is set to **server**, and not to **local**.
5. Select **Show Advanced Templates** and select the template name **Certificate Requests (6)** with the file name `certreq.ntf`.
6. To create the Certificate Requests database, click **OK**.
   The system creates the database.
7. Close the **About...** document.

   The system displays the **Database Configuration** form.

   - Select the administration server.

     This server runs the CA process for the supported CA.
   - Select the CA you created in the Configuring Domino SSL topic.
   - Select the intended purpose of this CA:
     - **Server Certificates Only**
     - **Both Client and Server Certificates**

   Do not select **Client Certificates Only** if you want to create a server key ring for SSL.
8. From the **Processing Method** drop-down list, select one of the following processing methods:

   - **Automatic**
   - **Automatic Transfer Server (optional)**

If you select the **Automatic** method, the person designated as an RA must be listed amongst those who can select **Run unrestricted methods and operations** in the Administration Server's server document.

RA is often the same person who creates the Certificate Requests database, that is, `certreq.nsf`. To verify this or to make changes, open the Domino Directory, navigate to the **Server/Servers** view, open the appropriate server document, and navigate to the **Security** section to see the **Processing Method** field.

If you do not set the **Processing Method** field properly, you will not be able to run the agents in the Certificate Requests database.

9. Select whether you want the applicant to receive the confirmations.
10. Click **Save & Close**.

### Next steps

Creating a key ring

# Creating a key ring

### Procedure

1. Open the Domino administration client.
2. On **Files** tab, open the Certification Requests database.
3. Select **Domino Key Ring Management** >**Create Key Ring**.
   The system displays the **Create Key Ring** form.
4. In the **Key Ring File Name** field, enter a file name for the key ring file without the .kyr extension.
5. In the **Password** and **Confirm Password** fields, enter identical passwords.
6. From the **Key Size** drop-down list, select a key size.
7. In the **Common Name** field, enter the common name of the server.

   The common name of the server must be a fully qualified host name, for example, server.company.com.
8. In the **Organization** field, enter the organization name.

   All other fields are optional.
9. Click **Create Key Ring**.
10. To automatically add your CA as a trusted root and to generate a certificate request for your server, in the **Key Ring Created** dialog box, verify the information and click **OK**.

11. In **Merge Trusted Root Certificate Confirmation** dialog box, verify the information and click **OK**.
    The system displays the **Certificate received into key ring and designated as trusted root** confirmation screen.
12. Click **OK**.
    The system displays the **Certificate Request Successfully Submitted for Key Ring** dialog box.
13. To dismiss the message, click **OK**.

### Next steps

Approving a key ring request

# Approving a key ring request

### Procedure

1. Open the Certificate Requests database.
2. To refresh the view, on the **Pending/Submitted Requests** view, press F9 if you do not find your request.
3. If the status of the request is **Submitted to Administration Process**, go to step 5. If the status of the request is **Pending Submission**, select the request and click **Submit Selected Requests**. The system displays the **Successfully submitted 1 request(s) to the Administration Process** message.
4. Click **OK**.
   Keep the Certificate Requests database open.
5. Open the Administration Requests database `Admin4.nsf`, go to the **Certification Authority Requests/Certificate Requests** view, and find your new request.
6. Double-click the request to open it, click **Edit Request**, and verify the information of the request.
7. Once you have verified the information and finished making any optional changes, click **Approve Request**.
8. Press F9 till the state of the request changes from the **New** state to the **Issued** state.
   The request state might change to **Approved** state before changing to the **Issued** state.

### Next steps

Checking the status of a key ring request

# Configuring a port

### Procedure

1. In the **Server/Servers** view of the Domino directory, find the server document.
2. Open the server document and click **Edit Server**.
3. In the **Ports - Internet Ports** section, enter the name of the new key ring file.
   Do not enter the full path of the key ring file.
4. Scroll down the page and locate the **SSL Port Status** field, and change it from **Disabled** to **Enabled**.
5. To enable SSL on the server, on the server console, type **`tell`** *`http restart`* if HTTP is running.
6. To verify that the HTTP server is now listening on port 443, on the server console, type **`show`** *`task`*.

### Next steps

Establishing a secure session over SSL by using Internet Explorer.

# Establishing a secure session over SSL using IE

### Procedure

1. To confirm that SSL works on the server, open a browser and type https://<server>.<company>.com/<CR_myco.nsf>.
   The system displays the **Security Alert** screen.
2. Click **View Certificate**.
3. Click **Install Certificate**.
4. On the **Certificate Import Wizard** screen, click **Next**.
5. On the **Certificate Store** screen, retain the default selection **Automatically select the certificate store based on the type of certificate**, and click **Next**.

6. On the **Completing the Certificate Import Wizard** screen, click **Finish**.
   The system displays **The import was successful** message.
7. Click **OK**.
8. On the **Security Alert** screen, click **Yes**.
   If the system displays a secured padlock near the top of the Internet Explorer window, it means you have successfully established a secure session over SSL.

### Next steps

Configuring the WebSphere server.

# Configuring the WebSphere server

### Procedure

1. Log in to the IBM WebSphere Administrative Console by using the administrative credentials.
   The address for IBM WebSphere Administrative Console is `https://<oneXCESMachine>:9043/ibm/console`.
2. In the **Security** section, select **SSL certificate and key management**.
3. Navigate to **Key stores and certificates** >**NodeDefaultTrustStore** > **Signer certificates** and click **Retrieve from port**.
4. In the **Host**, **Port**, and **Alias** fields, enter the host, port, and alias.
   The host is the IP address of the Domain Controller (DC) machine, and the port is the port for the LDAPS service. The default port is 636.
5. Click **Retrieve signer information**.
6. To save the configuration, click **OK**.
7. To verify the connection, check whether you can connect to the LDAP server by using the IBM Console. This test does not use any Client Enablement Services code, so it is a good validation for the environment setup.
8. On the administrative console, navigate to **Security > Secure administration, applications, and infrastructure**.
   If your system is already set up to communicate with a single LDAP environment, the **Available realm definitions** option must be already set to **Standalone LDAP registry**.
9. Click **Configure** and configure the LDAP parameters.
   Do not save any information now.

10. If you configure the system to communicate with LDAP, change the port to 636, and select the **SSL Enabled** check box in the **SSL Settings** section.
11. Click **Test connection**.

### Next steps

Configuring Client Enablement Services for LDAPS

# Configuring Avaya one-X® Client Enablement Services for LDAPS

### Procedure

1. Log in to the Client Enablement Services administration client.
2. Click the **System** tab.
   The system displays the **System** tab.
3. Click **Enterprise Directory**.
4. Select the domain for which you must set the LDAPS configuration.
5. Change the port value to 636.
6. Select **Secure Port**.
7. To save the configuration, click **Save**.
8. Restart Client Enablement Services.

# Index

## Numerics



## A



## B



## C



## D

## E



## G



## H



## I



## K



## L

## M



## N



## O



## P



## R



## S

## T

## U



## V



## W