Installing Server Applications for Avaya one-X® Agent

Release 2.5.4 (H.323)
Issue 1
December 2013

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 may generally make available to users of its products and Hosted Services. 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 websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Software” means Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. “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. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type

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

Copyright

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya, the Avaya logo, one-X 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.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Avaya one-X Agent overview

Avaya one-X Agent is a desktop software for agents in a contact center. This desktop software enhances agent productivity regardless of agents working from the head office or the branch office. Avaya one-X Agent synchronizes with the deskphone to share the control of telephony and agent features. Agents can use the user interface to gain access to common agent features, including contact center capabilities, namely integrated video and instant messaging.

Avaya one-X Agent supports the agents to deliver superior customer contact features. Agents can:

- Use advanced contact handling features to serve the customer.
- Gain access to customer-specific information through Screen Pop.
- Contact experts throughout the enterprise by using the Supervisor Assist feature.

About server applications

The primary objective of the Avaya one-X Agent solution is collaboration and administration enhancement capabilities. Avaya one-X Agent introduces servers to support these capabilities. With these servers, Avaya one-X Agent can run new features on the client user interface. However, most of the server applications are optional and customers must buy appropriate licenses to use these features.

Server applications

You can use the following server components to deploy the Avaya one-X Agent solution:

- Communication Manager 2.x or later
- System Manager 6.1 SP1.1
- Session Manager 6.0 or later
- Presence Services 6.1
- Central Management 2.5

Note:

Communication Manager is an optional server application. Although, Avaya one-X Agent supports Communication Manager 2.x, 3.x, 4.x, 5.x, and 6.0, the application is tested with Communication Manager 6.0 and Communication Manager 6.2.

Server applications deployments

You must deploy System Manager, Presence Services, and Central Management on separate servers. Before deploying the Presence Services and Central Management applications, ensure that you installed the appropriate versions of the Linux operating system on each

server. For System Manager deployment, you must install System Manager 6.x on the server before you install the System Manager application.

You must install System Manager 6.1 SP1.1 first, and then install Central Management 2.5 or Presence Services 6.1 in any order. To use IM with Avaya one-X Communicator SIP endpoints, you must also install Session Manager 6.x.

Note:

You can deploy the server application on a separate physical server or a Virtual Machine (VM) created on the same application host. If you deploy the server application on a VM, ensure that the VM meets the minimum hardware and software requirements of the server application. However, you cannot install System Manager and System Platform on the VM environment. These servers must be installed on a physical server.

Note:

If you upgrade a Central Management 2.0 to Central Management 2.5:

- You must install and configure Presence Services on a separate server.
- You can still use System Manager 1.0.

To upgrade System Manager to System Manager 6.1 SP1.1, you must deploy System Manager 6.1 SP1.1 on a separate server.

Feature dependencies

This section describes the feature dependencies of Avaya one-X Agent on various server applications.

System Manager

You can configure Central Management to send logs and alarms to System Manager. Central Management uses a Secure Access Link (SAL) agent for delivering logs and alarms to System Manager. You must configure the SAL agent to read the Central Management logs and forward the information to System Manager.

Presence Services

Avaya one-X Agent depends on Presence Services for Instant Messaging (IM) and presence capabilities. If Presence Services is installed with the Microsoft Office Communicator (MOC) gateway that enables communication with the MOC client, agents can communicate with enterprise users.

Session Manager

Session Manager offers a core communication service that builds on existing equipment and adds a SIP-based architecture. You will require Session Manager if you are using IM with Avaya one-X Communicator Session Initiation Protocol (SIP) endpoints.

Central Management

Central Management provides a centralized administration for hot-desking, multi-location contact centers, multiple agents, and agent endpoints. Central Management provides a central storage, control, and delivery of the following Avaya one-X Agent features:

- Greeting messages
- User preferences
- System settings
- Agent profiles
- Call/IM logs
- Contact lists

User authentication

Avaya one-X Agent supports two types of authentication:

- Form-based authentication
- Single Sign-on (SSO)

Form-based authentication

Form-based authentication is a default authentication method. In form-based authentication, the system authenticates the user credentials separately against each server present in the deployment, namely, Central Management, Communication Manager, and Presence Services. Therefore, the authentication depends on the server applications present in the deployment. In Avaya one-X Agent, the following configurations are available:

- Telephony only (Avaya one-X Agent must be installed without selecting the **Enable Central storage of profile information** option during the installation process).
- Telephony and Central Management
- Telephony and Presence Services
- Telephony, Central Management, and Presence Services

SSO

You can configure Central Management to use the Windows Kerberos credentials and the Simple and Protected GSS-API Negotiation (SPNEGO) protocol for SSO. By doing so, users can bypass the user name and password authentication for each server component. In SSO, application uses the Windows logon credentials, and supplies those information for authentication. The system authenticates these credentials against Active Directory.

Deployment scenarios

There are four different scenarios to deploy the Avaya one-X Agent solution. Based on these scenarios, you can configure different ways to authenticate a user. The following sections explain different types of authentication mechanism.

Authentication for telephony only

The system with telephony is the basic configuration that consists of Communication Manager as the server application. The system authenticates the agent station ID and password against Communication Manager for signing in and license request. The authentication is similar to that of Avaya one-X Agent.

Authentication for telephony with Central Management

If you have a deployment for telephony with Central Management, the system requires Communication Manager and Central Management deployment in an environment. Therefore, the user must select the Central Management option and provide the IP address of the Central Management server during the Avaya one-X Agent client installation. The installer stores the server address in the registry.

The Avaya one-X Agent client sends the agent station ID and password to Central Management. The Central Management server passes the agent station ID and password to Active Directory for authentication. If the authentication is successful, the Central Management server sends one or more user profiles to the user, based on the user configuration. The profile sent to the user consists of the station ID, password, and the Avaya one-X Agent client settings that Central Management manages centrally. When a user chooses a profile, the system sends the associated station ID and password for user and license authentication against Communication Manager.

Authentication for telephony with Presence Services

If you have a deployment for telephony with Presence Services, the system authenticates the agent station ID and password against Communication Manager. If authentication is successful and the agent has sufficient licenses, the system authenticates the agent station ID and password against Presence Services. If the authentication is successful, the agent can use the IM and Presence Services features of Avaya one-X Agent. If the agent chooses the auto-login option during authentication, the system automatically authenticates Communication Manager followed by Presence Services authentication. If the Presence Services authentication fails, the agent cannot use the Presence features on the Avaya one-X Agent client. However, the agent can use the telephony features. For this type of authentication, the Avaya one-X Agent user must have installed the application without selecting the **Enable Central storage of profile information** option during the installation process.

Note:

Presence Services and Central Management have different user credential.

Authentication for telephony with Central Management and Presence Services

If you have telephony with Central Management and Presence Services, the system authenticates the Avaya one-X Agent client agent station ID and password with Central Management. The Central Management server passes the agent station ID and password to Active Directory for authentication. If the authentication is successful, Central Management sends one or more user profiles to the agent, based on the user configuration. The profile sent to the agent consists of the station ID and password. When the agent chooses a profile, the system sends the associated station ID and password for agent and license authentication with Communication Manager. If the agent obtains the sufficient license, then the system authenticates the agent station ID and password against Presence Services. In case of failure at any stage in authentication, agents cannot use the service.

Note:

Presence Services and Central Management have different user credential.

Minimum system requirements

Hardware requirements for Central Management installation

Following are the minimum hardware requirements for installing Central Management 2.5:

Processor	2.4 GHz dual-core processor For example: Dual-Core AMD Opteron Processor 2216 – 2.4 GHz
RAM	4 GB
NIC support	100 MB
Free disk space	40 GB

Software requirements

Following are the software requirements for installing Central Management 2.5:

Operating systems	• Red Hat Enterprise Linux (RHEL) 5.2, 5.3, or 5.4 32–bit The RHEL Operating System (OS) resolves its host name and the host name of all systems the OS works with. **Note:** Ensure that your installation environment does not have the Postgres and JDK software. The Central Management installation package will install the

	Postgres and JDK software for the application to function correctly.
Supported browsers	Internet Explorer 7.x Mozilla Firefox 3.5.x
Supported virtualization system	Central Management supports VMware ESXi. It is validated to operate with VMware ESXi Release 3.5.

Note:

For System Manager hardware and software system requirements, see *Installing and Upgrading Avaya Aura System Manager*, Release 6.1. Before installing System Manager, ensure that you have installed System Platform 6.x on the server. For System Platform hardware and software system requirements, see *Installing and Configuring Avaya Aura System Platform*, Release 6.x.

For Presence Services hardware and software system requirements, see *Implementing Avaya Aura Presence Services*, Release 6.1.

For Session Manager hardware and software system requirements, see *Installing and Configuring Avaya Aura Session Manager*, Release 6.x.

Server component installation checklist

As Central Management 2.5 interacts with many different products and services, you must plan for a successful deployment of server components. The following checklist ensures that you meet all requirements to complete the deployment of Central Management 2.5.

#	Task	Description	✔
1	Determine how your enterprise will deploy Central Management.	For deployment options, seeAbout server applications on page 7.	
2	Ensure that you have all product licenses.	For Product Licensing and Delivery System (PLDS), see Activating license entitlements on page 66.	
3	Download the software package from the Avaya Support Site.	The Central Management software package is available on the Avaya Support Site at http://www.avaya.com/support. For software requirements, see GUID-7FD3456A-1DA6-4423-828F-6A1A948C4684#GUID-7FD3456A-1DA6-4423-828F-6A1A948C4684.	

#	Task	Description	✔
4	Ensure that the end user and enterprise environments can support Central Management.	For the installation option, verify the following: • Is the required hardware in place? For hardware requirement, see Minimum system requirements on page 11. • Have all related Avaya software products been installed and administered correctly? For software requirements, see GUID-7FD3456A-1DA6-4423-828F-6A1A948C4684#GUID-7FD3456A-1DA6-4423-828F-6A1A948C4684. • Have all related third-party software products installed and administered correctly?	
4	Install System Manager 6.1 SP1.1.	Install System Manager only if you are installing Presence Services or Central Management. To install System Manager 6.1 SP1.1, see *Installing and Upgrading Avaya Aura System Manager,* Release 6.1.	
5	Install Presence Services 6.1.	Install Presence Services only if your enterprise is using the IM functionality. To install Presence Services 6.1, see *Implementing Avaya Aura Presence Services*, Release 6.1.	
6	Install Session Manager 6.x.	Use Session Manager as an optional installation only if your enterprise is using IM with Avaya one-X Communicator SIP endpoints. Install Session Manager to verify IM and Presence for Avaya one-X Communicator SIP endpoints. To install Session Manager 6.x, see *Installing and Configuring Avaya Aura Session Manager*, Release 6.x.	
7	Perform the post-installation configuration for System Manager 6.1.	To perform post-installation settings for System Manager 6.1, see Performing the post-installation	

#	Task	Description	✔
		settings for System Manager 6.1 on page 16.	
8	Complete the interoperability settings for Avaya one-X Agent with Avaya one-X Communicator.	To complete the setup, see Interoperability with Avaya one–X Communicator on page 17.	
9	Install Central Management 2.5.	To install Central Management, see Installing Central Management (GUI installation) on page 34.	
10	Complete the post-installation setting for Central Management 2.5.	After completing the installation, you must configure the Central Management settings. The administration settings are available in Creating a spreadsheet from Apache Directory Studio on page 43.	

Related documents

The following list contains additional documentation related to server components installation. These documents are available on the Avaya Support Site:

- *Using Central Management, Release 2.5*
- *Migrating Server Applications from Avaya one-X Agent from 2.0 to 2.5*
- *Installing and Upgrading Avaya Aura System Manager, Release 6.1 SP1*
- *Implementing Avaya Aura Presence Services, Release 6.1*
- *Installing and Configuring Avaya Aura Session Manager, Release 6.x*
- *Installing and Configuring Avaya Aura System Platform, Release 6.x.*

For more information about the migration process, go to www.avaya.com/support.

Chapter 2: Prerequisites

This chapter provides instructions for installing server components as prerequisites for installing Central Management as part of Avaya one-X Agent solution deployment. This chapter also provides procedures to complete the post-installation settings for System Manager 6.1 and procedures you must complete for Avaya one-X Agent to inter-operate with Avaya one–X Communicator.

Installing server components

About this task

This section provides steps for installing server components as part of the Avaya one-X Agent solution deployment.

Use the following sequence to deploy server components:

Procedure

1. (Optional) Install System Manager 6.1 SP1.1 on a new computer if you are installing Presence Services or Central Management as part of the deployment.

   For system requirements and installation steps, see *Installing and Upgrading Avaya Aura System Manager,* Release 6.1.

   Note:

   Before installing System Manager, ensure that you have installed System Platform 6.x on the server. For system requirements and installation steps, see *Installing and Configuring Avaya Aura System Platform*, Release 6.x.

2. (Optional) Install Presence Services 6.1 on a new computer if your contact center is deploying Presence Services for Instant Messaging (IM) and Presence capabilities.

   For system requirements and installation steps, see *Implementing Avaya Aura Presence Services*, Release 6.1.

3. (Optional) Install Session Manager 6.x only if your enterprise is using IM with Avaya one-X Communicator SIP endpoints.

   For system requirements and installation steps, see *Installing and Configuring Avaya Aura Session Manager*, Release 6.x.

Next steps

After completing the installation of above applications, you must configure the System Manager 6.1 system. For steps, see Performing post installation settings for System Manager 6.1 on page 16.

Performing the post-installation settings for System Manager 6.1

This section provides a set of procedures to complete the post-installation settings for System Manager 6.1.

Related topics:

Adding a domain substitution rule for Presence Services on page 16
Modifying the System Presence ACL policy on page 17

Adding a domain substitution rule for Presence Services

About this task

The domain substitution rule defines how to convert a user login name into presence name. The system takes a user login name and the instances of **Domain Substitution Rule-From** string, and replaces it with the **Domain Substitute Rule-To** string.

For example, if the user name is Mike, the system with a rule *@global.com* as **Domain Substitution Rule-From** and *@pres* as **Domain Substitution Rule-To**, converts the login name of *mike@global.com* into the presence name of *mike@pres.example.com*.

Note:

Domain Substitution Rule Default can never overlap with **Domain Substitution Rule To** because the rule must be reversible.

Use the following steps to add a domain substitution rule for Presence Services.

Procedure

1. Log on to the System Manager 6.1 Web interface as administrator.
2. Click **Elements** > **Presence** > **Configuration**.
   The system displays the Presence panel.
3. On the **Configuration** panel, click **Edit** and perform the following steps:

a. For **Domain Substitution - From** field, enter a value for a user as `@<domain>.com`, where the <domain> is the domain name of System Manager.
b. For **Domain Substitution - To** field, enter the value for a presence user as `@pres<domain name>.com`.

Prefix `pres` before the Presence Services domain name to distinguish the domain names while installing Presence Services.

4. Click **Save**.

Modifying the System Presence ACL policy

About this task

You must change the System Presence ACL policy for the system to publish the presence policy document. This can result in Avaya one-X Agent not functioning properly with presence.

Use the following steps to change the System Presence ACL policy.

Procedure

1. Log on to the System Manager 6.1 Web interface as administrator.
2. Click **Users** > **User Management** > **System Presence ACLs**.
3. In the **System Presence ACL** panel, click the **Default Policy** tab.
4. In the **Default Policy** tab, ensure that **Access Level** is set to `Allow`.

   By doing so, the watchers can access the presence information associated with the corresponding access level. In the System Manager form, the Access Level Column has `All` and the Action Column has `Allow`.

Interoperability with Avaya one–X Communicator

Avaya one-X Agent supports integration with Avaya one-X Communicator 6.1. This section provides procedures you must complete for Avaya one-X Agent to inter-operate with Avaya one–X Communicator.

Related topics:

Installing Session Manager on page 18

Installing Session Manager

About this task

Use the following procedure to install Session Manager.

Procedure

1. Insert the kickoff-OS DVD and install OS on a machine where you want to install Session Manager.
2. Log on to the machine again as a sroot and password as sroot01 and run the following command to install Session Manager.

   ```
   home/craft/SMnetSetup
   ```

   You must provide the same IP address, gateway address, and domain as that of System Manager.
3. Insert the Session Manager DVD.
4. Log in as a sroot and at the prompt, run the following command:

   ```
   su - sroot
   ```
5. Mount the Session Manager DVD and perform an install (`install.sh`).

   ```
   [root@avaya-asm asm] mount -t iso9660 -o ro /dev/cdrom /cdrom
   [root@avaya-asm asm] cd /cdrom
   [root@avaya-asm cdrom] ./install.sh
   ```
6. Press **Enter** to begin the installation.

   The script prompts for Session Manager IP address or fully qualified domain name (FQDN) and enrollment password.
7. Provide the IP address or FQDN and enrollment password of Session Manager. Upon successful completion, Session Manager restarts automatically.

Configuring the IP address for software assets

Before you begin

- IP address or FQDN of System Manager 6.1 SP 1.1
- IP address of Communication Manager 4.0 or later. For Session Manager, ensure that you have Communication Manager 5.2.1 or later.
- IP address or FQDN of Session Manager 6.1

About this task

Use the followings steps to configure the FQDN or IP address of Session Manager and Communication Manager.

Procedure

1. Log on to the System Manager 6.1 Web interface as administrator.
2. Click **Elements** > **Routing** > **SIP Entities**.

   The system displays the SIP Entities page with a list of session initiation protocol (SIP) entities.
3. To add Session Manager as a SIP entity, click **New** and perform the following steps:
   a. In the **Name** field, enter a name for Session Manager, for example, `1XASessionManager`.

      You must choose a unique name with characters between 3 and 64.
   b. In the **FQDN or IP Address** field, enter the asset IP address of Session Manager.
   c. From the **Type** drop-down list, choose the entity type as `Session Manager`.
   d. In the **Location** drop-down list, specify the location of Session Manager.

      You can select from previously defined locations.
   e. In the **Time Zone** field, set the default time zone the Session Manager has to use.
   f. From the **SIP Link Monitoring** drop-down list, select `Use Session Manager Configuration` as a process for SIP Link Monitoring.
   g. Click **Commit** to add the Session Manager instance.
4. To add Communication Manager as a SIP entity and to configure the FQDN (or IP address), click **New** and perform the following steps:
   a. In the **Name** field, enter a name for Communication Manager, for example, `1XACM60`.

      You must choose a unique name with characters between 3 and 64.
   b. In the **FQDN or IP Address** field, enter the FQDN (or IP address) of Communication Manager.
   c. From the **Type** drop-down list, choose the entity type as `CM`.

d. In the **Location** drop-down list, specify the location of Communication Manager.

   You can select from previously defined locations.

e. In the **Time Zone** field, set the default time zone that Communication Manager has to use.

f. In the **SIP Timer /BF (In seconds)** field, enter the value of SIP timer in seconds.

g. In the **Call Detail Recording** field, ensure that the option is set to `None`.

h. From the **SIP Link Monitoring** drop-down list, select **Use Session Manager Configuration** as process for SIP Link Monitoring.

i. Click **Commit** to add the Communication Manager instance.

The system adds Session Manager and Communication Manager to the SIP entities list.

5. In **Port**, click **Add** and perform the following steps:

   a. Click **Add**, and in the **Port** field, type the port number as `5061`, and from the **Protocol** drop-down list, choose the protocol as `TLS`.

   b. Click **Add** and in the **Port** field, type the port number as `5060`, and from the **Protocol** drop-down list, choose the protocol as `TCP`.

6. To configure the SIP under **Entity Links**, perform the following steps:

   a. From the **SIP Entity 1** drop-down list, select the newly added Session Manager as an asset. For example, select `1XASessionManager` from the **SIP Entity 1** drop-down list, set the protocol as `TLS`, and set the listening port as `5061` in the **Port** field.

   b. From the **SIP Entity 2** drop-down list, select the newly added Communication Manager as an asset. For example, select `1XACM60` from the **SIP Entity 2** drop-down list, set the protocol as `TLS`, and set the listening ports as `5061` in the **Port** field.

7. Log on to Avaya Site Administration as an administrator and create SIP trunk with Communication Manager and Session Manager (with the asset IP).

8. Revert to the System Manager 6.1 Web interface, and select **Elements** > **Session Manager** > **Session Manager Administration**.

9. Click **New** to add a Session Manager instance and perform the following steps:

   a. In the **SIP Entity Name** field, enter a name for Session Manager.

   b. In the **Management Access Point Host Name/IP** field, provide the IP address of Session Manager.

   c. Ensure the **Direct Routing to Endpoints** option is set to `Enable`.

   d. In the **SIP Entity IP Address** field, provide the IP address of Session Manager.

      This IP address must be different from IP address assigned in step 9 a.

e. In the **Network Mask** field, enter the IP address of network as `255.255.255.0`.
f. In the **Default Gateway** field, enter the IP address of the default address.
g. Ensure that you do not change any values in the other fields.
h. Click **Commit**.

10. Go to **Elements** > **Session Manager** > **Dashboard**.

    The system displays the newly added Session Manager instance in the Dashboard panel.

11. In the **Dashboard** panel, click the **Service State** drop-down list and select `Accept New Service`.

12. Go to **Elements** > **Session Manager** > **System Status** > **Security Module Status** and select the **Connection Status** option.

    The system displays the Security Module Status page with status of each Session Manager Security Module.

Configuring SRE/URE on System Manager

About this task

Use the following procedure to configure SRE/URE on System Manager.

Procedure

1. Log on to the System Manager 6.1 Web interface as administrator.
2. To add a SIP domain, perform the following steps:
   a. Select **Elements** > **Routing** > **Domain**.
   b. In the **Name** field, enter the domain name of System Manager.
3. To add a location, perform the following steps:
   a. Go to **Elements** > **Routing** > **Locations**.
   b. In the **Locations** panel, click **New**.

      The system displays the Location Details.
   c. In the **Name** field, enter the name for Communication Manager, for example, `1XACM6.0`.
   d. Click **Add** and in the **IP Address Pattern** field, enter the IP address of Communication Manager.
   e. To view the newly added location, Go to **Elements** > **Routing** > **Locations**.
4. To add Routing Policies for Communication Manager, perform the following steps:
   a. Go to **Elements** > **Routing** > **Routing Policies**.

b. In the **Routing Policies** panel, click **New**.

The system displays the Routing Policy Details page.

c. In the **Name** field, enter the new name of Routing Policies for Communication Manager, for example, `1XCM6Policy`.

5. To add dial patterns for the numbers that a user must dial, perform the following steps:

a. Go to **Elements** > **Routing** > **Dial Patterns**.

b. In the **Dial Patterns** panel, click **New**.

The system displays the Dial Patterns page.

c. In the **Pattern** field, enter the dial pattern to match.

The dial pattern characters can be between 1 to 36.

d. In the **Min** field, enter the minimum number of digits that must match.

e. In the **Max** field, enter the maximum number of digits that must match.

f. Click **Add** to associate the Communication Manager policy as defined in step 4.

6. To add an application, perform the following steps:

a. Go to **Elements** > **Session Manager** > **Application Configuration** > **Applications**.

b. In the **Applications** panel, click **New**.

The system displays the Applications Details page.

c. In the **Name** field, enter a name for Communication Manager.

d. In the **SIP Entity** drop-down list, choose the newly created Communication Manager, for example, choose `1XACM6.0`.

e. To add the IP address of Communication Manager, click **View/Add CM Systems**.

A new Internet Explorer window appears with option to add a new instance of Communication Manager. In the **Application** tab, enter the name of Communication Manager as `CM6.0APP` in the **Name** field and choose `CM` from the **Type** drop-down list. Enter the IP address of Communication Manager in the **Node** field.

In the **Attribute** tab, enter the login name and password, and do not change any other default values.

Note:

You must create another user password in Communication Manager with administrator privilege using the following commands and provide these names in the fields.

```
cmuseradd super-user -C 18 <user name>
passwd <password>
```

f. In the **Description** field, enter the description for the application.

g. In the **Application Handle** field, enter the login name.

7. To add an application sequence, perform the following steps:
   a. Go to **Elements** > **Session Manager** > **Application Configuration** > **Application Sequences**.
   b. In the **Applications Sequences** panel, click **New**.
      The system displays the Applications Sequences page.
   c. In the **Name** field, enter the application.
   d. Select the application and move the order using the **Move First** or **Move Last** buttons.
8. To Synchronize the Communication Manager data, perform the following steps:
   a. Go to **Elements** > **Inventory** > **Synchronization** > **Communication System**.
      The system displays the Synchronize CM Data and Configure Options page. The synchronization starts automatically.
   b. If synchronization does not start, then click **Launch Element Cut Through**.
   c. Select a Communication Manager from the list.
   d. Select the **Incremental Sync data for selected devices** option.
   e. Click **Now**.

   The system starts synchronizing the Communication Manager data for the selected devices with System Manager.

Creating a Presence Services entity

About this task

Use the following steps to configure the Presence Services entity to use Presence Services from Avaya one–X Communicator.

Procedure

1. Log on to the System Manager 6.1 Web interface as administrator.
2. Click **Elements** > **Routing** > **SIP Entities**.
   The system displays the SIP Entities page with a list of SIP entities.
3. To add Presence Services as a SIP entity, click **New** and perform the following steps:
   a. In the **Name** field, enter a name for Presence Services, for example, `1XAPS`.
      You must choose a unique name with characters between 3 and 64.
   b. In the **FQDN or IP Address** field, enter the FQDN or IP address of Presence Services.
   c. From the **Type** drop-down list, choose the entity type as `Other`.

d. In the **Location** drop-down list, specify the location of Presence Services.
e. In the **Time Zone** field, set the default time zone that Presence Services has to use.
f. From the **SIP Link Monitoring** drop-down list, select **Use Session Manager Configuration** as process for SIP Link Monitoring.
g. Click **Add** to add the Presence Services instance.

4. To create an entity link between Session Manager and Presence Services, perform the following steps:

a. From the **SIP Entity 1** drop-down list, select the newly added Session Manager as an asset. For example, `1XASessionManager`, set the protocol as `TLS` from the **Protocol** drop-down list, and set the listening port as `5060` in the **Port** field.
b. From the **SIP Entity 2** drop-down list, select the newly added Presence Services as an asset. For example, for `1XAPS`, set the protocol as `TLS` from the **Protocol** drop-down list, , and set the listening port as `5060` in the **Port** field.

Adding users in Active Directory

Before you begin

- For SIP mode, ensure that you have installed and configured Session Manager for IM and presence communication between Avaya one-X Agent and Avaya one-X Communicator SIP. You must also ensure that Presence Services is configured with Session Manager on System Manager.
- For H.323 mode, ensure that you have configured Presence Services on System Manager.

  Session Manager is an optional component for H.323 mode.
- Ensure that Presence Services is configured with System Manager for both Avaya one-X Communicator SIP and H.323 modes. For Avaya one-X Communicator SIP mode, you must perform additional configuration of Presence Services as SIP entity and then create link with Session Manager.

About this task

Use the following steps to add users for Avaya one-X Communicator and Avaya one-X Agent in Active Directory:

Procedure

1. To add the Avaya one-X Communicator users in Active Directory with user name and telephone number, use the following steps:

a. Add the Avaya one-X Communicator users in Active Directory with user name and telephone number.

   You can configure the e-mail address only if the e-mail address is mapped to the IM handle mapping and if the user is using Avaya one-X Communicator in the H.323 mode. The IM handle is a default option.

   Ensure that the telephone number appears in the E.164 format.

b. Modify the user details in Active Directory using the following steps:

   i. Add the telephone number in a E.164 format.

   ii. To add Avaya one-X Communicator H.323 users, ensure that the corresponding IM handle mapped field exists in Active Directory. By default, the system uses the e-mail ID of a contact, as mapped. To map to the e-mail ID in the H.323 extension mode, ensure that all other users have the corresponding e-mail address field required to add users in the H.323 user contact list.

   Note:

   Ensure that the mapped H.323 field and user account in Active Directory have the same value so that you can create a user account with the same field in System Manager.

   iii. If you are adding a SIP user, the **E-mail** field is optional. This is also the mapping field of the IM handle on H.323 endpoint of Avaya one-X Communicator.

2. Use the following steps to create Avaya one-X Agent users in Active Directory:

   a. Enter the login name that you want to use as the Presence Services login name.

   b. Open the corresponding user again, and add a telephone number (in E.164 format) in the **Telephone number** field.

   Important:

   The **Telephone number** field is a mandatory field. If you do not add the Telephone number, Avaya one-X Communicator will not add this contact to the contact list with IM and presence enabled contact.

   c. To add more users, use step 1 and 2.

   d. To inter-operate with the Avaya one-X Communicator H.323 mode, add the e-mail address in the **Email** field.

   By default, the system uses the email ID. You can add e-mail ID only if the **Email** field is used for IM handle mapping in Avaya one-X Communicator H.323 mode. However, you must to use the e-mail ID in SIP or H.323.

3. Use the following steps to import the user data from Active Directory to System Manager:

   a. Log on to the System Manager 6.1 Web interface as administrator.

b. Go to **Home** > **Users** > **Synchronize and Import**.

   The system displays the User Synchronization page.

c. On the User Synchronization page, select a data source from the table to synchronize the data source.

   If the data source is not available in the list, click **New** to create a new data source. see step 3 in Appendix B: Importing users from Active Directory to System Manager on page 49.

d. Click the **Active Synchronization Jobs** tab.

e. Click **Create New Job**.

   The system displays the New User Synchronization Job page.

f. From the **Datasource Name** field, choose the data source and click **Run Job**.

   The system creates a new job and starts the synchronization. You can check the job status on the scheduler dashboard at **Home** > **Services** > **Scheduler** > **Scheduler-Scheduler**.

4. Modify the profile of a user for Avaya one-X Communicator using the steps in Adding users for Avaya one-X Communicator on page 27.

5. To modify the user profile for Avaya one-X Agent, use the following steps:

   a. Log on to the System Manager 6.1 Web interface as administrator.

   b. Go to **Home** > **Users** > **User Management** > **Manager Users**.

      The system displays the Manager Users page with a list of new users.

   c. Select the corresponding Avaya one-X Agent profile and click **Edit**.

      The system displays the corresponding profile with details. Use the following steps to edit the profile:

      i. Click the **edit** link and specify the communication profile password in the corresponding fields as created for Avaya one-X Communicator.

         The system uses this password for Avaya one-X Agent extension to log in as a IM and presence user.

      ii. Click **New** to create a new E.164 handle as created for Avaya one-X Communicator.

         The E.164 handle must have the same value as entered in Active Directory telephone field. Otherwise, Avaya one-X Communicator will not add this as IM and presence enabled user.

      iii. (Optional) To create an H.323 extension for the corresponding user, create an endpoint profile.

         Do not create the Session Manager profile. The extension password will be the security code.

      iv. Click **Commit**.

Verify if the new extension is created in Communication Manager.

Adding users for Avaya one-X Communicator

Before you begin

- You must have a user database in Active Directory with user name and telephone number in the E.164 format for creating a user list for Avaya one-X Communicator. You can use the E.164 number to create an E.164 handle in System Manager. You must import users from Active Directory. For steps, seeImporting users from Active Directory to System Manager on page 49. Upon completing the Active Directory synchronization, user data will be present in System Manager.
- Ensure that you configure the domain substitution rule for Presence Services with Avaya one-X Agent. For steps, see Adding a domain substitution rule for Presence Services on page 16.
- For SIP mode, ensure that you install and configure Session Manager for Presence/IM communication between Avaya one-X Agent and Avaya one-X Communicator SIP. You must also ensure that Presence Services is configured with Session Manager on System Manager.
- For H.323 mode, ensure that you configure Presence Services on System Manager.

  Note:

  For H.323 users, you must have fields in Active Directory that are mapped with IM handle. You must create this field in System Manager while synchronizing with Active Directory.
- Ensure that Presence Services is configured with System Manager for both Avaya one-X Communicator SIP and H.323 modes. For Avaya one-X Communicator SIP mode, you must perform additional configuration of Presence Services as SIP entity and then create link with Session Manager.

About this task

Use the following steps to create new users or modify existing user details for Avaya one-X Communicator and map each user with the corresponding extension on Communication Manager.

Procedure

1. Log on to the System Manager 6.1 Web interface as administrator.
2. Go to **Home** > **Users** > **User Management** > **Manage Users**.

   The system displays the list of users in the User Management page. If users are already imported from Active Directory, choose a user and modify the login corresponding to the extension. If users are imported from Active Directory, then the users must modify their profile. Otherwise, you must create new users.

3. Select the corresponding Avaya one-X Communicator profile, and click **Edit**.
   The system displays the corresponding profile with details.
4. Click the **Communication Profile** tab, and perform the following steps:
   a. Click the **edit** link and specify the communication profile password in the corresponding fields.
      The system uses this password for Avaya one-X Communicator extension to log in as a SIP extension.
   b. Click **New** to create a new SIP handle if Avaya one-X Communicator is a SIP user.

      Important:

      You must use this field only for SIP users and not for H.323 users.
   c. Click **New** to create a new E.164 handle, and enter the full E.164 format extension number, for example, `49801`. You must enable the Avaya one–X Communicator presence extension, otherwise Avaya one–X Communicator will not add the user to its contact list. The E.164 number must be same as the Active Directory telephone number.
      Do not create a Jabber handle as Presence Services creates the Jabber handle.
   d. In the **Session Manager Profile** panel, click **New** and add the following:

Field name	Description
Primary Session Manager	Choose the newly added Session Manager, for example, `1XASessionManager`.
Home Location	Choose the newly added home location, for example, `1XACM`.

      Note:

      You can only configure Session Manager for SIP users.
   e. Select the **Endpoint Profile** panel, and add the following:

Field Name	Description
System	Select the newly added Communication Manager, for example, `CM6.0APP`.
Use Existing Stations	Select this option if the extension is already available on Communication Manager. If you want to create a new extension on Communication Manager, do not select this option.

Field Name	Description
	Type the extension number in the **Extension** field.
Extension	Type the first digit and a list of the available stations on Communication Manager appears. Select the required extension from the list. **Note:** The extension list appears only if you use existing extension. For new extension you must type the extension.
Security Code	Add the security code. **Note:** The security code is not the actual extension password for SIP extension, but an extension password that you enter for communication profile in the **Communication Profile** tab. The security code is the extension password for H.323 extension to match the Communication Profile password. The extension can be an existing or a new extension. If you select a new extension, click commit for this extension, the system creates the extension on Communication Manager. You must verify the new extension in Communication Manager.
Port	Do not update the **Port** field. The system updates the **Port** field automatically. **Note:** You must select `IP` from the **Port** drop-down list while creating the extension.

f. Click **Commit** to add the user.

The system make the necessary changes to System Manager and the corresponding user to Communication Manager.

5. Go to Avaya Site Administration, and click **save trans all** to save all numbers.

Adding the Avaya one-X Agent contacts to the Avaya one-X Communicator contact list

Before you begin

- For SIP mode, ensure that you have installed and configured Session Manager for presence and IM communication between Avaya one-X Agent and Avaya one-X Communicator SIP. You must also ensure that Presence Services is configured with Session Manager on System Manager. In addition, you must configure Communication Manager for SIP users.
- For H.323 mode, ensure that you have configured Presence Services on System Manager for presence and IM communication between Avaya one-X Agent and Avaya one-X Communicator H.323. You must configure Communication Manager to create an endpoint profile in System Manager.

  Note:

  Session Manager is an optional component for H.323 mode.
- Ensure that the user data are available in Active Directory or imported to System Manager.

About this task

Use the following steps to add an Avaya one-X Agent contact to the Avaya one-X Communicator contact list:

Procedure

1. Launch Avaya one-X Communicator 6.1 on your computer.
2. In the **General Settings** dialog box, click the **Telephony** panel and complete fields as appropriate.
3. If you are logging in as a SIP user, add the Session Manager ASSET IP in server list field, add Communication Manager IP address in case of a H.323 user.
4. In the **Domain** field, enter the domain name of System Manager.
5. In the **IM and Presence** panel, configure the IM settings as appropriate.
6. In the **Public Directory** panel, configure the public directory settings.

   While configuring the settings, you must enter the Active Directory information and select the **Use Active directory GSS bind** option.
7. In the **Public Directory** panel, configure the public directory settings.
8. In the **Preference** panel, select `Active directory` under **Desktop integration** > **Name Look-Up**.

9. Log on to Avaya one-X Communicator using the SIP or H.323 extension and password.
10. Launch Avaya one-X Communicator with newly created Presence Services user.

    The user must be the one created in Active Directory, synchronized to System Manager, and modified in the profile. For Avaya one-X Communicator, if a user has a Presence Services account, then Avaya one-X Communicator logs the user on to the Presence Services server automatically.
11. Launch Avaya one-X Communicator with the newly created Presence Services user.

    For Avaya one-X Communicator, if a user has a Presence Services account, then Avaya one-X Communicator logs the user on to the Presence Services server automatically.
12. In Avaya one-X Communicator, search the user using the Active Directory search.

    Wait for the system to retrieve the contact.
13. Select a user and click **Add to Favorite** to add the user to the favorite list.
14. Initiate an IM session from Avaya one-X Communicator and Avaya one-X Agent to verify if the user is imported correctly.

Chapter 3: Installing, upgrading, and rolling back Central Management

This chapter provides instructions for installing, upgrading, and rolling back Central Management 2.5.

Installing Central Management

You can install Central Management using the Graphical User Interface (GUI) installation or silent installation mode.

With the GUI installation mode, you can use the installation setting through an installation wizard. The setup wizard prompts the administrator for relevant information during the installation process.

With the silent installation mode, the administrator can use the standard install settings through a command line interface (CLI). The setup utilizes the information to complete the installation procedure. You can also upgrade Central Management from 2.0 to 2.5 using the installation mode.

Note:

In Central Management 2.5, you can limit the rollover log files. However, if you have Central Management 2.0, SP1, SP2, or SP3 and are upgrading to Central Management 2.5, the rollover logs continue to grow on a daily basis.

Prerequisites

You must have:

- Working knowledge on LDAP, such as, using bindDN to configure Central Management service to communicate with the Active Directory server.
- System Manager 6.1 SP1.1 is installed in your environment.
- The installation environment does not have the Postgres and JDK software. The Central Management installation package installs the Postgres and JDK software for the application to function correctly.
- Red Hat Enterprise Linux (RHEL) 5.2, 5.3, or 5.4 32–bit is installed on the server.
- The time set on the server is the current date and time before running the Central Management Server installation setup.

- The SELINUX attribute is disabled, that is, **SELINUX=disabled** in the /etc/selinux/config file.
- The firewall is disabled with the following commands **chkconfig --level 2345 iptables off** or **service iptables stop**.

Related topics:

Installing Central Management (GUI installation) on page 34
Installing Central Management (silent installation) on page 36

Installing Central Management (GUI installation)

Before you begin

- Ensure that System Manager 6.1 SP1.1 is installed and configured.
- Download the oneXAgentCM-<version>.zip installer.
- Before connecting to the Linux server to install Central Management, ensure that the X Window System display (X11) variable is set on the Linux server to complete the Central Management installation.
- Check the following:
  - Ensure that the /etc/hosts file contains entries for host, Active Directory, and System Manager. Each entry must have the IP Address or FQDN hostname. For example:

```
127.0.0.1         localhost.localdomain localhost
::1             localhost6.localdomain6 localhost6
148.147.xx.xxx    cam25-hostname.domain-name.com    cam25-hostname # NIC
<eth0)
148.147.xx.xxx    AD-hostname.domain-name.com    AD-hostname
148.147.xxx.xxx    SMGR-hostname.domain-name.com    SMGR-hostname
```

  - Entries in the /etc/hosts file must not contain any spaces.
  - All fields, namely, IP Address or FQDN host name, in an entry in the /etc/hosts file must be separated by tabs. For example:

```
127.0.0.1         localhost.localdomain localhost
::1             localhost6.localdomain6 localhost6
148.147.xx.xxx    cam25-hostname.domain-name.com    cam25-hostname # NIC
<eth0)
148.147.xx.xxx    AD-hostname.domain-name.com    AD-hostname
148.147.xxx.xxx    SMGR-hostname.domain-name.com    SMGR-hostname
```

  - In the /etc/sysconfig/network file, ensure that the HOSTNAME=<FQDN> file is present, where FQDN is the host name. For example, **HOSTNAME=cam25-hostname.domain-name.com**.

- Ensure that the `/etc/sysconfig/network-scripts/ifcfg-eth0` file contains the following entries:

```
DNS=<IP address of DNS>
PEERDNS=yes
DOMAIN=<Domain name>
```

- Restart the network after making the updates by running the command:

```
service network restart
```

- Active Directory, System Manager, Presence Services, and Central Management must be in the same domain.

About this task

Use the following steps to install and configure the Central Management 2.5 server on the same server without System Manager:

Note:

If you start the installation in the directory which is writable only for a root user, an error message occurs during the installation of Central Management 2.5. In this case, the script cannot write the log information to the directory using “sudo”. Therefore, the system returns with the following message:

```
Could not change directory to "/root/Desktop/Cam-2.5/
oneXAgentCM-2.5.00356."
```

Ignore this warning message, as the error message does not have any impact during the installation process.

Procedure

1. Log on to the Linux server as root.
2. Open the directory where you have downloaded the `oneXAgentCM-<version>.zip` file on Linux, by running the command: `cd <directory name>`.
3. Extract the files by running the command:

   ```
   unzip oneXAgentCM-<version>.zip
   ```

   When you extract the `unzip oneXAgentCM-<version>.zip` file, the system creates a new folder called `oneXAgentCM-<version>`, and stores the files to this new folder.
4. Navigate to the `oneXAgentCM-<version>` folder, and run the following command to open the installer:

   ```
   chmod 777 oneXAgentCM-install.sh
   ./oneXAgentCM-install.sh
   ```

   After completing the prerequisite check, the system displays the **Set Encryption Key for secure data** message, and after entering password, the system initiates the installation process with a Welcome page.
5. Click **Next**.

6. Select the packs you want to install and click **Next**.
7. In the LDAP Information screen, perform the following steps:
   a. In the **LDAP.bindDN** and **LDAP.bindCredential** fields, enter the distinguished name and password provided while configuring an active directory component, respectively.
   b. In the **LDAP.url** and **LDAP.baseCtxDN** fields, enter the URL of the LDAP directory and the user name search context, respectively.

   The information on the LDAP Information screen consists of text strings. Obtain this information electronically to copy the text strings without causing any errors.
8. In the SMGR Information screen, perform the following steps and click **Next**:
   a. In the **SMGR-HOST_FQDN** field, enter the FQDN of System Manager.
   b. In the **SMGR-HOST_ PORT** field, enter the port number of System Manager.
   c. In the **ENROLLMENT_ PASSWORD** field, enter the password to register to the corresponding System Manager.

      To find the enrollment password on System Manager, log on to the System Manager 6.1 Web interface as administrator and navigate to **Home** > **Services** > **Security** > **Certificate** > **Enrollment Password**.

      For more information on enrollment password, see the *Administering Avaya Aura System Manager* Release 6.1 guide at http://www.avaya.com/support.
   d. In the **OXACM_ALARMID** field, enter the alarm ID for Central Management 2.5.

      For more information on alarm IDs, see the *Administering Avaya Aura System Manager* Release 6.1 guide at http://www.avaya.com/support.

   The system begins the installation process and returns the summary of installation upon successful completion of the Central Management installation.

Installing Central Management (silent installation)

Before you begin

- Ensure that System Manager 6.1 SP1.1 is installed and configured.
- Download the `oneXAgentCM-<version>.zip` installer.

- Before connecting to the Linux machine to install Central Management, ensure that the X11 DISPLAY variable is set on the Linux machine to complete the Central Management installation.
- Check the following:
  - Ensure that the `/etc/hosts` file contains entries for host, Active Directory, and System Manager. Each entry must have the IP Address or FQDN hostname. For example:

```
127.0.0.1         localhost.localdomain localhost
::1             localhost6.localdomain6 localhost6
148.147.xx.xxx    cam25-hostname.domain-name.com    cam25-hostname # NIC
<eth0)
148.147.xx.xxx    AD-hostname.domain-name.com    AD-hostname
148.147.xxx.xxx    SMGR-hostname.domain-name.com    SMGR-hostname
```

  - Entries in the `/etc/hosts` file must not contain any spaces.
  - All fields (namely, IP Address or FQDN host name) in an entry in the `/etc/hosts` file must be separated by tabs. For example:

```
127.0.0.1         localhost.localdomain localhost
::1             localhost6.localdomain6 localhost6
148.147.xx.xxx    cam25-hostname.domain-name.com    cam25-hostname # NIC
<eth0)
148.147.xx.xxx    AD-hostname.domain-name.com    AD-hostname
148.147.xxx.xxx    SMGR-hostname.domain-name.com    SMGR-hostname
```

  - In the `/etc/sysconfig/network` file, ensure that HOSTNAME=<FQDN > file, the FQDN entry is present, where FQDN is FQDN of the host. For example, **`HOSTNAME=cam25-hostname.domain-name.com`**.
  - Ensure that the `/etc/sysconfig/network-scripts/ifcfg-eth0` file contains the following entries:

```
DNS=<IP address of DNS>
PEERDNS=yes
DOMAIN=<Domain name>
```

  - Restart the network after making the updates by running the command:

```
service network restart
```

  - Active Directory, System Manager, Presence Services, and Central Management must be in the same domain.

About this task

Use the following steps to install and configure the Central Management 2.5 server in silent mode on the same machine without System Manager:

Procedure

1. Log on to the Linux machine as root.
2. Open the directory where you have downloaded the `oneXAgentCM-<version>.zip` file on Linux, using the `cd <directory name>` command.
3. Extract the files by running the command:

`unzip oneXAgentCM-<version>.zip`

When you extract the `unzip oneXAgentCM-<version>.zip` file, the system creates a new folder called `oneXAgentCM-<version>`, and extracts the files into this new folder.

4. Locate the `headless_install.properties.template` file, and copy the file to a new file named `headless_install.properties`.
5. Open the `headless_install.properties` file, and edit as following properties:

```
LDAP.bindCredential= <User credentials>
LDAP.url= ldap://<IP address>:389
LDAP.baseCtxDN= CN=Users,DC=Domain Name,DC=com
SMGR_HOST_FQDN= <System Manager Hostname>.<Domain Name>
SMGR_ENROLLMENT_PASSWORD= <Password>
OXACM_ALARMID= <Alarm id>
```

   To find the enrollment password on System Manager, log on to the System Manager 6.1 Web interface as administrator and navigate to **Home** > **Services** > **Security** > **Certificate** > **Enrollment Password**.

   For more information on enrollment password, see the *Administering Avaya Aura System Manager Release 6.1* guide.

6. Run the following command:

   `./oneXAgentCM-install.sh -h <install_configuration_file>`

   The `install_configuration_file` file in this case is the `headless_install.properties` file.

   The installer runs in the silent mode, and ensures the system meets the prerequisites for the setup. After completing the prerequisite check, the system displays the following message:

```
Set Encryption Key for secure data.
```

7. To complete the installation, enter a valid password for the encryption key.

   Avaya Installation Framework (AIF) uses the encryption key to protect sensitive information, such as, password used during the installation and preserving the information in files.

   Wait for the system to complete the installation. For any exceptions, you can verify the install log in the `/opt/Avaya/install_logs` directory.

Upgrading Central Management

Use the Central Management 2.5 installation to upgrade Central Management 2.0 installation to Central Management 2.5.

Before you begin

Download the `oneXAgentCM-<Version>.zip` installer.

Procedure

1. Copy the latest build of `oneXAgentCM-<version>.zip` file into a directory on the Linux server.

   Note:

   For Avaya one-X Agent 2.0 and Avaya one-X Agent 2.0 SP1, Central Management supports only the Basic Authentication mode. For Avaya one-X Agent 2.0 SP2 and SP3, supports Central Management in the Basic Authentication, Form-base Authentication, and SSO modes. For AAvaya one-X Agent 2.5.x, there is no Basic Authentication support.

2. Log on to the Linux server as root.
3. Open the directory where you have downloaded the `oneXAgentCM-<version>.zip` file on Linux, by running the command:

   ```
   cd <directory name>
   ```

4. Extract the files by running the command: `unzip oneXAgentCM-<version>.zip`

   When you unzip the `unzip oneXAgentCM-<version>.zip` file, the system creates a new folder called `oneXAgentCM-<version>`, and extracts the files into this new folder.

5. Go to the `oneXAgentCM-<version>` folder, and at the command prompt, type:

   ```
   chmod 777 oneXAgentCM-install.sh
   ./oneXAgentCM-install.sh
   ```

   The setup does not complete the installation until you specify the encryption key. You must type a valid password, when the setup prompts for an encryption key.

6. Click **Next**.
7. Select the packs to install and click **Next** .
8. In the Delivery Options for log/alarms window, select **start usage of Remote System Manager** and click **Next**.

   The system begins the installation process and returns the summary of installation upon successful completion of the Central Management installation. Upon successful upgrade, the system saves the upgrade information to the `/tmp/Avaya/backup` folder.

9. In the SMGR Information window, perform the following actions and click **Next**:
   a. In the **SMGR_HOST_ FQDN** field, type the FQDN of System Manager.
   b. In the **SMGR_HOST_ PORT** field, type the port number of System Manager.
   c. In the **ENROLEMENT_ PASSWORD** field, type the password to register to the corresponding System Manager.

d. In the **OXACM_ALARMID** field, type the alarm ID for Central Management 2.5.

10. To update the System Manager information, at the command prompt, run the `<Central Management installation>/bin/oxacm4smgr.sh`, command, and perform the following actions:

    a. In the **SMGR_HOST_ FQDN** field, type the FQDN of System Manager.
    b. In the **SMGR_HOST_ PORT** field, type the port number of System Manager.
    c. In the **ENROLEMENT_ PASSWORD** field, type the password to register to the corresponding System Manager.
    d. In the **OXACM_ALARMID** field, type the alarm ID for Central Management 2.5.

Note:

The alarming service provides an interface for monitoring alarms that System Manager and other components generate. You can monitor alarms that Central Management generates through the System Manager console. For more information about alarms, see *Administering Avaya Aura® System Manager*.

Rolling back an upgrade

Before you begin

- Before upgrading Communication Manager 2.0 to Communication Manager 2.5, you must back up the Avaya Aura® Communication Manager 2.0 database. You can back up the database by running the script: `<Central Management installation>/bin/oxacmbackup.sh [<destination directory for dump files>]`. For more information about backing up the Communication Manager data, see *"Appendix A: Backup and restore data"* in *Using Avaya one-X Agent Communication Manager*.

About this task

Execute a rollback operation using Command Line Interface (CLI), if you find any errors or issues with Communication Manager 2.5 and to restore the Communication Manager 2.0 database.

Important:

Do not use the Communication Manager 2.5 GUI uninstaller for rolling back an upgrade, as the uninstaller does not provide support the rollback process.

Procedure

1. Go to the `/opt/Avaya/Uninstaller` directory.
2. Run the script:

   ```
   ./oxacmrollback.sh /tmp/Avaya/backup/2.0.xxxx.0:1
   ```

   The system saves the Communication Manager 2.5 environment into `/tmp/Avaya/backup/2.5.xxxxx.0`.

   Note:

   Once you successfully rollback to 2.0.xxxx.0 version, you can also upgrade to the 2.5 version by running the script:

   ```
   ./oxacmrollback.sh /tmp/Avaya/backup/2.5.xxxxx.0
   ```

   The system requires the location of Central Management 2.0 files for a rollback. You can find the Communication Manager 2.0 files at `/tmp/Avaya/backup/<release number>`, where `<release number>` corresponds to the following numbers depending on the versions:

Communication Manager release	Version number
Communication Manager 2.0	2.0.1012.0
Communication Manager 2.0 SP1	2.0.1017.0
Communication Manager 2.0 SP2	2.0.1901.0
Communication Manager 2.0 SP3	2.0.3102.0

   The system restores the Communication Manager database. You can also restore the Communication Manager database by running the script: `<Central Management installation>/bin/oxacmrestore.sh [<Full path to zipped backup>]`. For more information about backing up the Communication Manager data, see “*Appendix A: Backup and restore data*” in *Using Avaya one-X Agent Communication Manager*.

Chapter 4: Configuring the Central Management installation

This chapter provides steps for creating a spreadsheet using Apache Directory Studio. It also explains how to synchronize, map, and enable the LDAP synchronization with Central Management. It also explains how to view the software versions that are installed on the Central Management host.

Creating a spreadsheet from Apache Directory Studio

Before you begin

At this stage of the installation, the web interface must be accessible and have the user login details. The user login can be `onexagentcm`, `craft`, or `sroot`. All other users must have their details imported into the system using the bulk user import feature or by adding each user separately. You can import users using the defined spreadsheet format.

About this task

Use the following procedure to create a spreadsheet from an LDAP browsing tool, namely Apache Directory Studio.

Procedure

1. Download and install Apache Directory Studio.
2. Run Apache Directory Studio.
3. In the Connections window, right-click the **New Connection** menu item and select **Create a new connection**.
4. Go to the part of the LDAP tree containing the users gaining access to Central Management.
5. Right-click and select the **Export** > **Excel Export** submenu.
6. Open the export file in Microsoft Excel.
7. Log on to the Central Management web interface as an administrator, and import the template file in Excel.

   To perform a bulk import, the user data must be available in a tab-delimited file. A sample tab delimited file is also available on Central Management from the **example** link on the Import Users page. You must click the example link, save the Comma Separated Value (CSV) file to the computer as a Unicode Text file, and add the user

details to this file. The Unicode Text file saves the data in the tab-delimited format.

If you have already saved the user details to local computer as a CSV file, you can import users with the relevant data to Central Management by saving the CSV file as a Unicode Text file and importing the file. Do not delete or overwrite the header row of the Unicode Text file when you add data to the file.

8. Copy the data from the export file into the appropriate columns in the import template file, rename the file, and save the file as a CSV file on the computer.
9. From the Central Management navigation menu, click **Import Users**.
10. In the **File** field, click **Browse** to locate the Unicode Text file.
11. Click **Import** to import users listed in the Unicode Text file.

    For more information about importing users to Central Management, see *Chapter 3: User administration* in *Using Avaya one-X Agent Central Management*.

Synchronizing Central Management with LDAP

About this task

Note:

Throughout this document, LDAP and Active Directory are used interchangeably.

Use the LDAP Synchronization feature to synchronize the Central Management users with the Active Directory server. The system performs the synchronization for every 30 minutes.

The synchronization process reads a mapping file to determine:

- The location of the LDAP server
- The login credentials for the server
- The LDAP search criteria
- Description of which fields from the LDAP schema will map to the required user fields in the Central Management database.

The system changes the updated files on the LDAP server in the Central Management database. Therefore the Central Management field always has the same value as the LDAP field.

Mapping LDAP to Central Management

About this task

The system maps the entries from LDAP to Central Management attributes using the ldapusermapping.properties mapping file. The sample file ldapmapping.properties.sample is available in the `<Central Management installation>/conf/` folder.

Navigate to the ldapmapping.properties.sample file in the `<Central Management installation>/conf/` folder. Once the installation of Central Management completes, the system backs up the sample file as ldapmapping.properties.sample.orig and updates the ldapmapping.properties file with the LDAP information. You must ensure that the information in the sample file is correct. Do not modify any settings in the sample file. You must rename the sample file to ldapmapping.properties. Once you rename the ldapmapping.properties.sample file to ldapmapping.properties, ensure that the ldapmapping.properties file exists in the `<Central Management installation>/conf/` folder.

Enabling LDAP synchronization

By default, the LDAP Sync option is disabled. You must enable the LDAP synchronization to start the LDAP synchronization. You can restart the LDAP synchronization by renaming the sample file to ldapmapping.properties.

Viewing software inventory

About this task

The software inventory script displays the software versions installed on the Central Management host.

Procedure

1. To run the software inventory script, log on to the host as root.
2. Run the following commands for running software inventory script:

```
chmod 754 <Central Management Installation>/bin/oxacminvent.sh
./<Central Management Installation>/bin/oxacminvent.sh
```

The system displays a list of software deployed. Following is the sample output:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<avayaInstallInventory
version="1.0">    <targetMachineDetails installPath="/opt/Avaya"
ipAddress="xxx.xxx.xx.xxx" name="oxacm host name domain name"/>
  <pack name="one-X Agent Central Management JBoss" id="OneXAgentCMJBoss">
        <version date="25-Apr-11 13:53" id="2.5.00450.0"/>
 </pack>     <pack name="one-X Agent Central Management" id="OneXAgentCM">
        <version date="25-Apr-11 13:53" id="2.5.00450.0"/>
 </pack> </avayaInstallInventory>
```

Chapter 5: Uninstalling Central Management

About this task

Use the following steps to uninstall Central Management 2.5 in the silent uninstallation mode:

Procedure

1. Log on to the Linux machine as root.
2. Navigate to the `<Central Management installation>/utils/bin` directory.
3. Run the following command to install Central Management 2.5:

   ```
   chmod 777 oxacmuninstall.sh
   ./oxacmuninstall.sh
   ```

   The system returns with the following prompt:

   ```
   Do you want to proceed: [Y/N]
   ```

   Note:

   Pressing `N` aborts the Central Management 2.5 uninstallation process.

4. Type `Y`.

   The system initiates the Central Management uninstallation process.

5. Remove the script zip-up and backup the Central Management files under the `/tmp/AvayaBase/backup` directory.

   The system saves a copy of the database backup dump file in the `/tmp/AvayaBase/backupOneXAgentCM-2.5.xxxxx.0-<year>-<month>-<day>-<hour>-<minutes>.dump` directory. You can see the zipped up backup files, with `OneXAgent-backupfiles-<year>-<month>-<day>-<hour>-<minutes>.zip` in the `/tmp/Avaya/backup` directory.

Appendix A: Importing users from Active Directory to System Manager

Before you begin

- Ensure that user data is available in Active Directory or imported to System Manager.
- Ensure that System Manager and Presence Services are configured correctly.
- If an agent wants to communicate with SIP endpoints, the administrator has to configure Session Manager with System Manager and Presence Services.
- Ensure that the phone number in the **Phone Numbers** field is in the E.164 format for users in Active Directory. For example, +<Country Code>-<National Destination Code>-<Subscriber Number>.

About this task

To synchronize System Manager with Active Directory to import all existing users:

Procedure

1. Log on to the System Manager 6.1 Web page as administrator.
2. Click **Home** > **Users** > **Synchronize and import** > **Synch Users** > **New User Synchronization Datasource**.
3. On the New User Synchronization Datasource panel, perform the following steps:
   a. In the **Datasource Name** field, specify the data source name, for example, `UserNameAD`.
   b. In the **Host** field, enter the IP address of Active Directory.
   c. In the **Principal** field, enter the name of the user in Active Directory, for example, `<user name>@<domain name>.com`.
   d. In the **Password** field, enter the administrator password used in Active Directory.
   e. In the **Port** field, enter the port number `389`.
   f. In the **Base Distinguished Name** field, enter the name `cn=users,dc=domain name,dc=com`.
   g. In the **LDAP User Schema** field, enter the schema `inetOrgPerson`.
      The schema is case-sensitive.
   h. Click **Test Connection** to check the connection settings.
   i. Click **Save**.
4. On creating the Datasource, you must map the fields between Active Directory users and System Manager users. Ensure that you map the fields with the correct field types for synchronization to succeed. The following is an example of mapping fields between Active Directory users and System Manager users:

- Map the **userPrinicipleName** attribute of user in Active Directory to the **loginName** attribute of user in System Manager.
- Map the **sn** attribute of user in Active Directory to the **surname** attribute of user in System Manager.
- Map the **preferredLanguage** attribute of user in Active Directory to the **preferredLanguage** attribute of user in System Manager.
- Map the **objectGUID** attribute of user in Active Directory to the **sourceUserKey** attribute of user in System Manager. You must ensure that the type of field is binary.
- Map the **givenName** attribute of user in Active Directory to the **givenName** attribute of user in System Manager.
- Map the **displayName** attribute of user in Active Directory to the **displayName** attribute of user in System Manager.

5. To create a new job, click **Home** > **Users** > **Synchronize and import** > **Synchronize Users** > **Active Synchronization Jobs** > **Create a New Job**.
6. In the New User Synchronization Job page, perform the following steps:
   a. In the **Datasource Name** drop-down list, select the data source, for example, `UserNameAD`.
   b. Select the **Schedule job for future execution** option and set the date for scheduling the job.

      By default, the system uses the current date and time to schedule a job. Users can also schedule a job for immediate use.
   c. Click **Schedule job for future execution** to run the job.

      The system imports only the user information with a profile from Active Directory.

      Note:

      To view the status of the job, click **Services** > **Scheduler** from the System Manager Web console. Ensure that the system imported user data to System Manager. To view the job, click **Completed Job**. The system displays the Completed Job page.
7. To view the list of users imported to System Manager, click **Home** > **Users** > **User Management** > **Manage Users** and click **User Management**.

   The system displays the User Management page with a list of users.

   The system imports only the user information to System Manager and not the profile information. To import the profile information, use one of the following ways:

   - In the System Manager Webpage, go to each user details and update the profile information manually, or
   - Use an XML export and import facility to change the profile information.
8. To import the profile information using an XML file, perform the following steps:
   a. Log on to System Manager by using PuTTY or Telnet.

b. To export users, run the command **sh exportUpmUsers.sh** on $MGMT_HOME/upm/bulkexport/exportutility/exportUpmUsers.sh .

The system creates a zip file and stores the file to $MGMT_HOME/upm/bulkexport. The system unzips the file and creates an XML file.

The following is an example of an XML file that the system creates:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <tns:users xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ns3="http://
xml.avaya.com/schema/import_csm_mm" xmlns:ns4="http://xml.avaya.com/schema/
import_sessionmanager" xmlns:ns5="http://xml.avaya.com/schema/import_csm_agent"
xmlns:ns6="http://xml.avaya.com/schema/import_csm_cm" xmlns:ns7="http://
xml.avaya.com/schema/deltaImport" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:schemaLocation="http://xml.avaya.com/schema/import
userimport.xsd">
- <tns:user>
  <authenticationType>basic</authenticationType>
  <displayName>Default Administrator</displayName>
  <displayNameAscii>Default Administrator</displayNameAscii>
  <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
  <isEnabled>true</isEnabled>
  <isVirtualUser>false</isVirtualUser>
  <givenName>admin</givenName>
  <loginName>admin</loginName>
  <middleName>admin</middleName>
  <source>seeded</source>
  <sourceUserKey>seed data</sourceUserKey>
  <status>provisioned</status>
  <surname>admin</surname>
  <userName>admin</userName>
  <userPassword />
  <userType>administrator</userType>
- <roles>
  <role>System Administrator</role>
  <role>End-User</role>
  </roles>
- <commProfileSet>
  <commProfileSetName>Primary</commProfileSetName>
  <isPrimary>true</isPrimary>
  </commProfileSet>
  </tns:user>
```

c. Open the XML file and update the profile information in the XML file, namely, Endpoint Profile and Session Manager Profile.

The following is a sample XML file to add profile information. You must add multiple profiles:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <imp:users xmlns:imp="http://xml.avaya.com/schema/import">
- <imp:user>
  <authenticationType>BASIC</authenticationType>
  <givenName>Robin</givenName>
  <loginName>59036@sipdomain.com</loginName>
  <surname>Forman</surname>
- <roles>
  <role>End-User</role>
  </roles>
+ <commProfileSet>
  </imp:user>
- <imp:user>
  <authenticationType>BASIC</authenticationType>
  <givenName>Simon</givenName>
  <loginName>59056@sipdomain.com</loginName>
  <surname>Woollett</surname>
- <roles>
```

```
  <role>End-User</role>
  </roles>
- <commProfileSet>
  <commProfileSetName>Primary</commProfileSetName>
  <isPrimary>true</isPrimary>
- <commProfileList>
- <commProfile xsi:type="imp:xmlStationProfile" xmlns:imp="http://xml.avaya.com/
schema/import_csm_cm" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <commProfileType>CM</commProfileType>
  <imp:cmName>CommunicationManager1</imp:cmName>
  <imp:useExistingExtension>false</imp:useExistingExtension>
  <imp:extension>59056</imp:extension>
  <imp:setType>9640</imp:setType>
  <imp:port>IP</imp:port>
  </commProfile>
- <commProfile xsi:type="imp:SessionManagerCommProfXML" xmlns:imp="http://
xml.avaya.com/schema/import_sessionmanager" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
  <commProfileType>SessionManager</commProfileType>
  <imp:primarySM>SessionManager1</imp:primarySM>
  <imp:homeLocation>Location1</imp:homeLocation>
  </commProfile>
- <commProfile xsi:type="imp:xmlMessagingProfile" xmlns:imp="http://
xml.avaya.com/schema/import_csm_mm" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
  <commProfileType>Messaging</commProfileType>
  <imp:messagingName>Messaging</imp:messagingName>
  <imp:useExisting>false</imp:useExisting>
  <imp:messagingTemplate>DEFAULT_CMM_6_0</imp:messagingTemplate>
  <imp:mailboxNumber>59056</imp:mailboxNumber>
  <imp:password>1</imp:password>
  </commProfile>
  </commProfileList>
  </commProfileSet>
  </imp:user>
  </imp:users>
```

The following is a sample XML file that the system displays after updating the profile information

```
<?xml version="1.0" encoding="UTF-8" ?>
- <imp:users xmlns:imp="http://xml.avaya.com/schema/import">
- <imp:user>
  <authenticationType>basic</authenticationType>
  <givenName>PankajMigrationDemo</givenName>
  <loginName>Pankimos@avaya.com</loginName>
  <surname>Hirlekar</surname>
  <userName>Panky</userName>
  <userPassword>admin123</userPassword>
  <commPassword>admin123</commPassword>
- <!--
authenticationType>BASIC</authenticationType>
    <givenName>Robin</givenName>
    <loginName>59036@sipdomain.com</loginName>
    <surname>Forman</surname
  -->
- <!--
roles>
      <role>End-User</role>
    </roles
  -->
- <commProfileSet>
  <commProfileSetName>Primary</commProfileSetName>
  <isPrimary>true</isPrimary>
- <handleList>
```

```
- <handle>
  <handleName>sip:pankaj12@6xadc.com</handleName>
  <handleType>sip</handleType>
- <!--
 <handleSubType>sip</handleSubType>
  -->
  </handle>
  </handleList>
- <commProfileList>
- <commProfile xsi:type="imp:xmlAgentProfile" xmlns:imp="http://xml.avaya.com/
schema/import_csm_agent" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <commProfileType>CM</commProfileType>
  <commProfileSubType>Agent</commProfileSubType>
  <imp:cmName>ACM187</imp:cmName>
  <imp:useExistingAgent>false</imp:useExistingAgent>
  <imp:loginIdExtension>2005</imp:loginIdExtension>
- <!--
imp:setType>9620</imp:setType
  -->
  <imp:template>DEFAULT_AGENT_CM_6_0</imp:template>
  </commProfile>
- <commProfile xsi:type="imp:SessionManagerCommProfXML" xmlns:imp="http://
xml.avaya.com/schema/import_sessionmanager" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
  <commProfileType>SessionManager</commProfileType>
  <imp:primarySM>asset</imp:primarySM>
  <imp:homeLocation>AssetPune</imp:homeLocation>
  </commProfile>
- <!--
commProfile xsi:type="imp:xmlMessagingProfile" xmlns:imp="http://xml.avaya.com/
schema/import_csm_mm" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
          <commProfileType>Messaging</commProfileType>
          <imp:messagingName>MSGR</imp:messagingName>
          <imp:useExisting>false</imp:useExisting>
          <imp:messagingTemplate>DEFAULT_MM_5_2</imp:messagingTemplate>
          <imp:mailboxNumber>59036</imp:mailboxNumber>
          <imp:password>1</imp:password>
        </commProfile
  -->
  </commProfileList>
  </commProfileSet>
  </imp:user>
  </imp:users>
```

d. To add another user, repeat Step 1 to Step 8.

9. To import the XML file to System Manager:

   a. Click **Synchronization** and select **Import** > **Import Users**.

      The system displays the Import Users page.

   b. In the **File Selection** field, click **Browse** and find the XML file to be imported to System Manager.

   c. In the General panel, select the following options:

In	Choose option
Select Error Configuration	`Continue processing other records`
Select import type	`Complete`

In	Choose option
If a matching records already exists	`Merge`

d. In the Job Schedule panel, select **Schedule Job as Run immediately**.
e. Click **Save**.

The system imports the XML file. On importing the users, ensure that the system applies the profiles.

10. To view the list of users imported with profiles to System Manager, select **Home** > **Users** > **User Management** > **Manage Users** and click **User Management**.
11. On the User Management page, click a user in the list.
The system displays the Communication Profile page with user details and the corresponding profile information.

Appendix B: Troubleshooting server applications

This section provides information that assist you in troubleshooting general issues associated with server applications and Central Management. The section is divided into topic areas to locate information that you need as quickly as possible.

Common troubleshooting procedures

This section has common troubleshooting procedures for Central Management entities and components. This section also provides steps for testing connection between Central Management and other entities.

Related topics:

Troubleshooting the Central Management JBoss on page 55
Testing connection to Central Management user interface on page 56
Validating the Central Management and Active Directory connection on page 57
Alarms and logging for server applications on page 59

Troubleshooting the Central Management JBoss

If JBoss is running, access to Central Management must be possible. Run the following commands from CLI on the Linux host if the respective user interfaces are returning errors on your browser. The Linux host has all the server applications.

- To check if Central Management is running in the JBoss container:

```
service oxacm status
```

- To stop Central Management:

```
service oxacm stop
```

- To start Central Management:

```
service oxacm start
```

- To restart Central Management with a single command:

```
service oxacm restart
```

Tip:

You must allow sufficient time for JBoss to complete the startup whenever you start or restart JBoss. If you attempt to access Central Management before the startup is complete, the following message appears.

```
Temporarily Unavailable. The server is temporarily unable to
service your request due to maintenance downtime or capacity
problems. Please try again later.
```

If the user interface continues to display an error, check the log file from the following location:

```
<Central Management installation>/jboss-4.2.3.GA/server/
default/log/server.log
```

Testing connection to Central Management user interface

You must enter the Central Management FQDN when accessing the Central Management Web console. Alternatively, you can enter the IP address Central Management.

Before you begin

- If you have a problem accessing `https://<CAM FQDN> :8643/oneXAgentCM` from your machine, ensure that you have the registered machine in the same domain as Central Management. Also, ensure that you have added Central Management FQDN entry in the Internet Explorer local intranet settings.
- Use the following steps to change the Internet Explorer security settings.
    a. Navigate to **Tools** > **Internet Options** > **Security tab**, and select **Local intranet**.
    b. Select **Sites** and click **Advanced**.
    c. In the **Add this website to the zone** field, prefix `https://` before `CAM FQDN` and click **Add**.
    d. Click **Close**.

Note:

You must register the machine from which you are accessing the Central Management URL into the same domain as the Central Management server. However, this does not apply if you are not using SSO.

About this task

Use the following steps if you are using SSO:

Procedure

1. Right-click **My Computer** to select the **Properties** option.

2. In the **System Properties** dialog box, select the **Computer Name** tab and click **Change**.
3. In the **Member of** section, select the **Domain** option, and enter your domain.

   Enter the user name and password in the **Computer Name Changes** dialog box if the system prompts you to validate your user credentials.
4. Restart your machine, after the registration with your domain is successful.
5. Log into the client machine.
6. Click **Start** > **My Network Places**, and select the **Properties** option.
7. In **Network Connections**, right-click **Local Area Connection** > **This connection uses the following items** > **Internet Protocol (TCP/IP)**.
8. Click **Properties** and ensure that the **Use the following DNS server addresses** option is checked and the IP address appears in the **Preferred DNS server** field.

   If the IP address is not appearing in the **Preferred DNS server** field, ensure to enter a valid IP address.
9. Click **Advanced** and select the **DNS** tab.
10. Ensure that you have entered a valid DNS server address in the **DNS** field.
11. Ensure that you have selected the **Append these DNS suffixes (in order):** option. Click **Add** and enter your DNS suffix, that is, your domain name.
12. Ensure that you have selected the **Register this connection's addresses in DNS** option.
13. Click **OK**.
14. Restart the client machine.
15. When logging into the client machine after restarting, select your domain name from the **Log on to** drop-down list, and log in as the user you specified in step 3.

Validating the Central Management and Active Directory connection

Procedure

1. Log on to the Central Management Web console using the user name and password as `craft` and `craft01`, respectively.

   You can also log on to Central Management using the user name and password as `sroot` and `sroot01` respectively.

2. Add a user that exists in the Active Directory and assign a Web Administrator role to this user.
3. Close your browser to log out of Central Management.
4. Log on to the Central Management using the newly provisioned Web Administrator user name and password.
5. If the Central Management administration login fails, perform the following steps to verify that the Active Directory connection and the search criteria that you entered during Central Management installation is correct.
   - Create a new connection to the service account using an LDAP browser. You can create a new connection using Apache Directory Studio while installing Central Management with the same syntax for bindDN.
6. If the LDAP browser (that you connect to the Apache Directory using the bindDN) and the password fails, you must back up the files to edit, and perform the following steps:
   a. Review the bindDN information in the login-config.xml file in the `<Central Management installation>/jboss-4.2.3.GA/server/default/conf` directory and make the necessary changes to the bindDN, bindCredential, or LDAP URL.
   b. If the LDAP browser succeeds in connecting to the service account, then review the base CTXDN configuration that is defined in the `login-config.xml` in the `<Central Management installation>/jboss-4.2.3.GA/server/default/conf` directory.

      You must review the base CTXDN configuration to determine that the location at which the search root begins. The base CTXDN configuration also includes all the possible paths within the Active Directory structure and contains all potential users that get authenticated through Central Management. Using the LDAP browser, the base CTXDN configuration provides the view of the Active Directory structure and the necessary information for guiding changes to the configuration that was entered during the Central Management installation.
   c. Once the system applies the changes, run the following command to restart the JBoss application server:

      ```
      service oxacm restart
      ```

      Note:

      You must wait for JBoss to restart, as it takes several minutes to restart.

Alarms and logging for server applications

You can access logs and alarms through SAL and System Manager. For details on how to access alarms and logs, see the System Manager documentation.

Central Management creates alarms when it logs error messages. The ART registration process issues the alarm ID.

Related topics:

Accessing logs and changing the log levels on page 59
Accessing alarms on page 59

Accessing logs and changing the log levels

Procedure

1. To access the log information, log on to the System Manager Web console as a Web administrator and perform the following steps:
   a. On the System Manager Web console, under **Services**, click **Events**.
   b. In the left navigation pane, click **Logs** > **Log Viewer**.
   c. Filter the product type, and find *com.avaya.onexagentcm*.
      For more information on Presence Services logs, see the *Administering Presence Services XCP Controller* guide at http://www.avaya.com/support.
2. To change logging levels:
   a. On the System Manager Web console, under **Services**, click **Events**.
   b. In the left navigation pane, click **Logs** > **Log Viewer**.
   c. Select the appropriate logger from the list, and click **Edit**.
   d. On the Edit Logger page, set the level in the **Log level** field.

Accessing alarms

About this task

Use the following steps to access alarms generated by Central Management.

Procedure

1. Log on to the System Manager 6.1 Web interface as administrator.

2. On the System Manager Web interface, go to **Home** > **Services**, and click **Events**.
3. On the left navigation pane, click **Alarms** > **Alarming (Alarm List)**.
4. In **Host Name/Sys Name or Source IP Address** field, filter the Central Management list by entering the host name or IP address of Central Management.

   The system lists the alarms if any, corresponding to Central Management.

Troubleshooting Central Management

The section has troubleshooting procedures relating to Central Management.

Related topics:

Internal server error when starting Central Management on page 60
403 error from Central Management on page 60
401 HTTP Authentication error from Central Management on page 61
401 unknown user error from Central Management on page 61
Central Management unavailable message on page 61
Hot-desking feature not working on page 62
No agent profile on desktop on page 62
No connection between Central Management and Postgres on page 62
Central Management 2.5 cannot be registered on System Manager on page 62
TMClientLibException appears during Central Management installation or when the oxacm4smgr.sh script is run manually on page 63

Internal server error when starting Central Management

If the system has started the oxacm service and the Central Management tables are not created, ensure that you have created the **camdb** and **camjbossdb** databases before deploying Central Management. To check if errors were logged during an attempt at table creation, use the log file **pgstartup.log** at `/var/lib/pgsql`.

403 error from Central Management

If you start the Central Management user interface and get a 403 unauthorized error, that the user you are trying to log on with exists in both the Central Management database and Active

Directory. Also, ensure that you have a role authorizing the user to get the requested resource.

401 HTTP Authentication error from Central Management

Central Management returns the following 401 error when trying to access the Web user interface with SSO authentication:

```
This request requires HTTP authentication
```

To resolve this problem:

- Ensure the Central Management host machine has its time synchronized against the Active Directory server.
- Ensure that you can access the Active Directory server through its FQDN from the Central Management host machine.

401 unknown user error from Central Management

Central Management returns the following 401 error when trying to access the Web user interface with SSO authentication:

```
Unknown user: <user>@DOMAIN.COM
```

To resolve this problem you can add a user with the user name <user>@DOMAIN.COM Central Management.

Note:

You must provide the domain name of the user in uppercase.

Central Management unavailable message

Once you deploy the Central Management application and start the Web user interface, you get the following message:

```
Temporarily Unavailable The server is temporarily unable to service
your request due to maintenance downtime or capacity problems. Please
try again later.
```

Try accessing the Central Management server with a standard Web browser.

https://<hostname>:8643/oneXAgentCM/client/login?protocol=1.4

Following is an example you will see after entering the agent user name and password:

```
Timestamp:      2011-01-27T07:37:20.596Z
Protocol:       2.5
Username:       agent1
Remote host:    135.105.6.73
Remote address: 135.105.6.73
Preferred:       agent_template
AutoLogin:       false
ReadOnly:       false
```

Hot-desking feature not working

If the hot-desking feature is not working for a valid Avaya one-X Agent user with a known profile, check the proxy settings of the user.

If you are working in an environment that has a Web proxy, ensure that the Web proxy is not used for traffic going to the Central Management server. To do this, set an exception in the **Proxy Server** settings of Internet Explorer. Go to the Internet Explorer menu **Tools** > **Internet Options** > **Connections** > **LAN Settings** > **Advanced**, and ensure that the host name of Central Management appears in the **Exceptions** list.

For Mozilla Firefox, click **Tools** > **Options**, and in the Options window, click **Network** > **Settings**. Ensure that Central Management host name appears in the **No Proxy for** list.

No agent profile on desktop

If the Avaya one-X Agent client has no profile assigned at start up, an error message appears when an agent logs in to the Agent one-X Agent desktop.

To resolve this, on the Manage Users page of Central Management user interface, ensure the Avaya one-X Agent user is assigned with a template.

No connection between Central Management and Postgres

Review the logs to determine if the connection between Central Management and Postgres is broken or not working properly. The logs contain errors on database. You can find the server logs on the Central Management host machine at `<CAM install location>jboss-.2.3.GA/server/default/log .`

Central Management 2.5 cannot be registered on System Manager

Central Management 2.5 must be registered on System Manager 6.1 and Enrollment Password must be correct. Due to connection between SAL Agent 6.1 and System Manager

6.1, the two machines must have similar protocols to identify and communicate with each other. For instance, if the host of SAL Agent 6.1 is set to IP address and the host of System Manager 6.1 is FQDN, SAL Agent 6.1 converts the FQDN of System Manager 6.1 to IP address.

Ensure that the protocol for each server for identifying and communicating with each other is same and that each machine has same information on etc/hosts.

TMClientLibException appears during Central Management installation or when the oxacm4smgr.sh script is run manually

If TMClientLibException appears during the installation or when the oxacm4smgr.sh script under the `<Central Management installation>/bin` folder is run manually. Check one or all of the following conditions:

- Ensure that the enrollment password is configured in System Manager.
- Ensure that the enrollment password has not expired in System Manager.
- Ensure that the enrollment password assigned as an input during the Central Management server installation matches with the one that is configured in System Manager.
- Ensure that System Manager is configured with Central Management to recognize each other.

Appendix C: PLDS Licensing

PLDS Overview

The Avaya Product Licensing and Delivery System (PLDS) provides customers, Avaya Partners, distributors, and Avaya Associates with tools for managing license entitlements and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads.

Installation software packages for Avaya products are available as ISO files on PLDS. Users can download the ISO images to a PC, and choose to either burn a DVD for installation or transfer the ISO file to the target server for installation.

You can check PLDS to determine if a later service pack or software release is available. If updates do exist, see the appropriate upgrade procedures, contact Avaya, or contact the Avaya Partner Service representative.

When you place an order for a PLDS-licensed software product, the license entitlements on the order are automatically created in PLDS. Once these license entitlements are created, you receive an e-mail notification from PLDS. This e-mail notification includes a license activation code (LAC). Using the LAC, you can quickly find and activate the newly purchased license entitlements in PLDS. You can then download the license file.

Important:

You must provide the WebLM host ID to activate the license file in PLDS. The primary WebLM host ID is the MAC address of a physical network interface card (NIC) on the server.

Examples of license management tasks that you can perform in PLDS include:

- Adding more license entitlements to an existing activation
- Upgrading a license file to a new major release
- Moving license entitlement activations between license hosts
- Regenerating a license file with an new host ID

Activating license entitlements

Before you begin

You know the Host ID of the License Host if you are activating license entitlements on a new License Host.

About this task

Use the License Activation Code (LAC) to activate one or more license entitlements. You can activate all of the licenses, or you can specify a number of licenses to activate from the quantity available. Upon successful activation of the license entitlements, PLDS creates an Activation Record and sends an Activation Notification e-mail message to the customer who is registered with the entitlements. The Activation Record and Activation Notification provide details on the number of activated licenses and the License Host. The license file can be accessed on the License/Keys tab of the Activation Record in PLDS and is also an attachment to the Activation Notification e-mail message. You must install the license file on WebLM to use the licenses.

Procedure

1. Type http://plds.avaya.com in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS Web site.
3. In the **LAC(s)** field of the Quick Activation section, enter the LAC that you received in an e-mail message.

   Note:

   If you do not have an e-mail message with your LAC, follow the steps in the Searching for Entitlements section and make a note of the appropriate LAC from the LAC column.

   Note:

   The Quick Activation automatically activates all license entitlements on the LAC. However, you can remove line items or specify a number of licenses to activate from the quantity available.
4. Enter the License Host information.

   You can either create a new license host or use an existing license host.
5. Click **Next** to validate the registration detail.
6. Enter the License Host Information.

   The Host ID is the MAC address of the server hosting the WebLM server. The Host ID is obtained from the Server Properties page of the WebLM server where the license file is installed.

7. Enter the number of licenses to activate.
8. Review the Avaya License Agreement and accept the agreement if you agree.
9. Perform the following steps to send an activation notification e-mail message:
   a. In the **E-mail to** field, enter the e-mail addresses of the additional activation notification recipients.
   b. Enter the comments or special instructions in the **Comments** field.
   c. Click **Finish**.
10. Click **View Activation Record**.
    - The **Overview** tab displays a summary of the license activation information.
    - The **Ownership** tab displays the registration information.
    - The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file will be generated for each application. From the **License/Key** tab, you can view and download the license file. Install each license file on the WebLM server associated with the License Host.

Searching for license entitlements

About this task

Use this functionality to search for an entitlement by using any one or all of the following search criteria:

- Company name
- Group name
- Group ID
- License activation code

In addition to these search criteria, PLDS also provides other additional advanced search criteria for searching license entitlements.

Note:

Avaya associates or Avaya Partners can search license entitlements only by company name.

For more information on downloading license entitlements, see Downloading software from PLDS on page 72.

Procedure

1. Type http://plds.avaya.com in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS Web site.
3. Click **Assets** > **View Entitlements**.

   The system displays Search Entitlements page.
4. To search license entitlements by *company name*, enter the company name in the **%Company: field**. To see a complete list of companies before searching for their corresponding entitlements, do the following:

   a. Click the **magnifying glass** icon.
   b. Enter the name or several characters of the name and a wildcard (%) character.
   c. Click **Search Companies**.
   d. Select the desired company name from the list of options.

   Tip:

   You can use a wildcard (%) character if you do not know the exact name of the company you are searching for. For example, if you enter `Av%`, the system searches for all the company names starting with the letter Av. You can enter a wildcard character at any position in the search criteria.
5. To search license entitlements by *group name*, enter the appropriate information in the **%Group name:** or **%Group ID:** fields.

   Group Names or IDs are specific to Functional Locations and Sold-To's that define the actual location of equipment and software.

   Tip:

   You can use a wildcard character if you do not know the exact name of the group you are searching for. For example, if you enter `Gr%`, the system searches for all the groups starting with the characters Gr. You can enter a wildcard character at any position in the search criteria.
6. To search license entitlements by *LAC*, enter the specific LAC in the **%LAC:** field.

   Tip:

   You can use a wildcard character if you do not know the exact LAC you are searching for. For example, if you enter `AS0%`, the system searches for all the LACs starting with AS0. You can enter a wildcard character at any position in the search criteria.

   You will receive LACs in an e-mail if you have supplied the e-mail address to your sales order. If you do not have this code, search by using one of the other search criteria.

7. To search license entitlements by *application*, *product* or *license status*, select the appropriate application, product, and/or status from the field.
8. Click **Search Entitlements**.

Result

All corresponding entitlement records appear at the bottom of the page.

Moving activated license entitlements

Before you begin

Host ID or License Host name of the move from/to License Host.

About this task

Use this functionality to move activated license entitlements from one License Host to another. You can chose to move all or a specified quantity of license entitlements.

Note:

If you move a specified number of activated license entitlements from one host to another by using the Rehost/Move transaction in PLDS, two new license files are generated:

- One license file reduces the number of license entitlements on the License Host from which you are moving license entitlements.
- One license file increases the number of license entitlements on the License Host to which you are moving license entitlements.

Install each of these license files on the appropriate server.

If you move all activated license entitlements, only one license file is generated. Install this new license file on the License Host to which you are moving license entitlements. Remove the license file from the License Host from which you are moving all license entitlements.

Procedure

1. Type http://plds.avaya.com in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS Web site.
3. Click **Activation** > **Rehost/Move** from the Home page.
4. Click **View Activation Record information** to find and select licenses to rehost or move.

   You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.

Note:

If you are an Avaya associate or Avaya Partner, enter the search criteria and click **Search Activation Records**.

5. Select **Rehost/Move** for the License Host from which you are moving license entitlements.
6. In the **Search License Hosts** field, enter the License Host to which you are moving license entitlements.

   Alternatively, you can click **Add a License Host** to select an existing License Host.
7. Validate the Registration Detail, and click **Next**.
8. Enter the License Host Information.

   The Host ID is the MAC address of the server hosting the WebLM server. The Host ID is obtained from the Server Properties page of the WebLM server where the license file is installed.
9. Enter the number of Licenses to move in the **QTY column** field and click **Next**.
10. Accept the Avaya Legal Agreement.
11. Perform the following steps to send an activation notification e-mail message:
    a. In the **E-mail to** field, enter the e-mail addresses of the additional activation notification recipients.
    b. Enter the comments or special instructions in the **Comments** field.
    c. Click **Finish**.
12. Click **View Activation Record**.

    - The **Overview** tab displays a summary of the license activation information.
    - The **Ownership** tab displays the registration information.
    - The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file will be generated for each application. From the **License/Key** tab, you can view and download the license file. Install each license file on the WebLM server associated with the License Host.

Regenerating a license file

Procedure

1. Type http://plds.avaya.com in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS Web site.
3. Click **Activation** > **Regeneration** from the Home page.
4. Search License Activations to Regenerate.

   You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.
5. Click **Regenerate** from the appropriate record.
6. Validate the Registration Detail, and click **Next**.
7. Validate the items that will regenerate and click **Next**.
8. Accept the Avaya Legal Agreement.
9. Perform the following steps to send an activation notification e-mail message:
   a. In the **E-mail to** field, enter the e-mail addresses of the additional activation notification recipients.
   b. Enter the comments or special instructions in the **Comments** field.
   c. Click **Finish**.
10. Click **View Activation Record**.
    - The **Overview** tab displays a summary of the license activation information.
    - The **Ownership** tab displays the registration information.
    - The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file will be generated for each application. From the **License/Key** tab, you can view and download the license file. Install each license file on the WebLM server associated with the License Host.

Downloading software from PLDS

About this task

Note:

You can download product software from http://support.avaya.com also.

Procedure

1. Type http://plds.avaya.com in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS Web site.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. 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**
6. Click the download icon from the appropriate download.
7. When the system displays the confirmation box, select **Click to download your file now**.
8. If you receive an error message, click on the message, install Active X, and continue with the download.
9. When the system displays the security warning, click **Install**.

   When the installation is complete, PLDS displays the downloads again with a checkmark next to the downloads that are completed successfully.

Adding a host

About this task

You can define a new License Host on which to activate the license entitlements.

Procedure

1. Click **Add a License Host**.
2. Enter License Host name.
3. Click **Save**.

Searching for a host

About this task

Use this functionality to search for a License Host associated with one or more entitlements.

Procedure

1. Enter a few characters of the Host name in the **%License Host** field.

   Note:

   You can use a wildcard (%) character if you do not know the exact name of the License Host you are searching for. For example, if you enter `Ho%`, the system searches for all the host names starting with the characters Ho. You can enter a wildcard character (%) at any position in the search criteria.

2. Click **Search License Hosts**.

Appendix D: Connecting to another System Manager

The administrator can connect to another System Manager server using the following script:

```
<Central Management installation>/bin/oxacm4smgr.sh
```

The system prompts for the following parameters:

Note:

The following script, with the parentheses, prints the default value set during the installation. Do not leave the enrollment password field empty.

```
--- Set System Manager machine FQDN (scsmgr61b.sv.avaya.com): [Type here new FQDN or "Enter"
to use default ]
Input FQDN <echoed input>--- Set System Manager HTTPS port (443): [Type here new Port or
"Enter" to use default ]
Input PORT <echoed input>

--- To connect SMGR set Enrollment Password:**********): [Type here new FQDN or "Enter" to use
default ]
Starts will be printed , no actual echo of input

---Set OXACM Alarm ID (1234567890):: [Type here new Alarm ID or "Enter" to use default ]
Input Alarm ID <echoed input>
PROD-SMGR-HOST=<echoed input>
PROF-SMGR-IPADDR=<Script recognized IP Address from FQDN>
PROD-SMGR-PORT=<echoed input>
PROD-ALARMID=<echoed input>
Updating the SPIRIT Supported Products file to add support for OneX Agent Central management
(OXACM)
SPIRITHOME=<found installed SAL Agent home directory>
```

```
Prepare to update /opt/spirit//config/agent/SPIRITAgent_1_0_supportedproducts_orig.xml
Looking for OXACM product marked as onexagentcm
Trying to update Inventory file /opt/spirit//inventory/default_product_inventory.xml
Updating the SPIRIT Agent Base Configuration file to provide log tailing support.
SPIRITHOME=</opt/spirit/>
LOG_LOCATION=/var/log/Avaya/mgmt/OneXAgentCM/spiritOperationalAppender.log
Updating the SPIRIT Agent Base Configuration file to provide log tailing support.
SPIRITHOME=</opt/spirit/>
LOG_LOCATION=/var/log/Avaya/mgmt/OneXAgentCM/spiritAuditAppender.log
Updating the SPIRIT Agent Base Configuration file to provide log tailing support.
SPIRITHOME=</opt/spirit/>
LOG_LOCATION=/var/log/Avaya/mgmt/OneXAgentCM/spiritSecurityAppender.log
SPIRITHOME=</opt/spirit/>
=== Running /opt/spirit//scripts/configureSALAgent.sh -s 0987654321 scsmgr61b.sv.avaya.com
443 ********* Enterprise-scsmgr61b.sv.avaya.com ===
   result=<empty - meaning connection is good, or error message>
Stopping SPIRIT Agent Application 6.1-1.0.0.108.208...
SPIRIT Agent Application 6.1-1.0.0.108.208 was not running.
Starting SPIRIT Agent Application 6.1-1.0.0.108.208...
```

In case of error messages, check the parameters and try again.

Appendix E: Connecting to another LDAP server

The administrator can connect to another LDAP server using the following script:

```
<Central Management installation>/bin/oxacm4ldap.sh
```

The system prompts for the following parameters:

Note:

The following script, with the parentheses, prints the default value set during the installation. You cannot leave the LDAP password field empty.

```
---Set URL of the LDAP server in form ldap://<Host FQDN><port>(ldap://148.147.18.172:389):
[Type here new URL or "Enter" to use default ]
---Set LDAP Distinguished Name used to bind and check user credentials with
(CN=binduser,CN=Users,DC=subdomain,DC=mycompany,DC=com): [Type here new Distributed Name or
"Enter" to use default ]
---Set password to use in combination with the bind DN: [Type here LDAP password]
--- Set LDAP Distinguished Name (DN) used as a base to combine with usernames when checking
user credentials ():[Type here new DN or "Enter" to use default ]
```

In case of error messages, check the parameters and try again. Restart the oxacm service to apply the changes to the settings.

Central Management is set to use LDAP with parameters as entered above.

Appendix F: Distributed third party software

Package name	Version	License type	License URL
Silk Icons	1.3	Creative Commons Attribution 2.5 License	http://www.famfamfam.com
Apache Wicket	1.4	Apache License version 2.0	http://wicket.apache.org
JDK	1.6	Sun License	http://java.sun.com
JBoss EAP	4.3.2	GPL	http://www.jboss.com/downloads/
PostgreSQL	8.3	BSD	http://www.postgresql.org/
Slf4J	1.5.3	MIT License	http://www.slf4j.org/
Hibernate	3.4	LGPL	https://www.hibernate.org
Spring Framework	2.5.6	Apache License version 2.0	http://www.apache.org/licenses
Ehcache	1.7	Apache License version 2.0	http://ehcache.org
Xerces	2.7	Apache License version 2.0	http://www.apache.org/licenses
JSR	3.0.5	Apache License version 2.0	http://www.apache.org/licenses
Java CSV Library	1.0	LGPL	http://www.csvreader.com
pwauth	2.3.8	BSD	http://olex.openlogic.com/packages/pwauth/2.3.8
JBoss Kerberos/ SPNEGO Toolkit	*	GPL	http://www.jboss.com
Kunststoff Look&Feel	2.1	LGPL	http://sourceforge.net/projects/kunststoff-laf
Metouia Look&Feel	2.1	LGPL	http://mlf.sourceforge.net

Package name	Version	License type	License URL
NanoXML	2.2.3	NanoXML zlib/libpng License	http://sourceforge.net/projects/nanoxml
JGoodies	*	BSD	http://www.jgoodies.com
Log4j	1.2	Apache License version 2.0	http://www.apache.org/licenses
LiquidLnF	2.6	LGPL	https://liquidlnf.dev.java.net
IzPack	2.0	Apache License version 2.0	http://www.apache.org/licenses
XML Security Library	1.4.2	MIT License	http://www.aleksey.com/xmlsec/index.html
GUICE	1.0	Apache License version 2.0	http://code.google.com/p/google-guice

Index