Installing Server Applications for Avaya one-X® Agent

Release 2.0
November 2009

Notice

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

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

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

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Web site: http://www.avaya.com/support

Licenses

License type

Copyright

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/ThirdPartyLicense/

Preventing toll fraud

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

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://www.avaya.com/support/

Suspected security vulnerabilities with Avaya Products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Downloading documents

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Avaya one-X Agent Release 2.0 is an integrated telephony softphone solution that provides seamless connectivity to at-home agents, remote agents, outsourced agents, contact center agents, and agents interacting with clients having vocal and hearing impairment. This is the second release of Avaya one-X Agent and has number of enhancements in addition to the features available in the Release 1.0.

Agent collaboration, supervisory support, and central administration capabilities are the main enhancements of Avaya one-X Agent Release 2.0. These enhancements are supported by Presence Services, System Manager, and Communication Manager. Avaya one-X Agent Release 2.0 also relies on the Call Center features of Communication Manager.

In addition to the features present in release 1.0, Avaya one-X Agent now supports new features such as instant messaging, hot-desking, supervisor monitoring, central management, TTY interaction, desktop sharing, and single sign on. The availability of new features depends on the type of Avaya one-X Agent license used for deployment.

All the enhancements are achieved maintaining the same user interface to help users adapt quickly to the new features presented in this release.

Related topics:

About server applications on page 5
Feature dependencies on page 7
User authentication on page 7
Minimum system requirements on page 10

About server applications

Agent collaboration and enhancing administrative capabilities of Avaya one-X Agent are the primary objectives of Release 2.0. To equip Avaya one-X Agent with these capabilities, a set of servers are added to Avaya one-X Agent setup. Various features of these server applications are leveraged to execute the new features on the client UI. However, most of the server applications are optional and clients need to buy licenses for the features that they want to be installed.

Server applications

Avaya one-X Agent Release 2.0 supports the following server applications:

- Communication Manager 2.x or later
- Aura System Manager 1.0
  - System log server
  - SAL Agent 1.0
- Presence Services 5.2
- Avaya Central Management

All the above server applications, except Communication Manager, are optional.

Server applications deployments

The server applications can be installed in the following combinations.

1. Single host — System Manager, Presence Services, and Central Management are installed on the same application host.
2. Multiple host — Coresident System Manager and Central Management and standalone Presence Services.

Note:

Standalone server application deployment can be a separate physical system or a virtual machine (VM) created on the same application host. In case the server application is deployed on a VM, the VM must satisfy the minimum hardware and software requirements prescribed for the server application.

Installation sequence

RHEL 5.1 or 5.2 — 32 bit must be installed on the system on which any or all of the server applications are getting installed. This is a primary requirement before you begin any installation.

For single host deployment, installation is performed in the following sequence:

1. System Manager 1.0
2. Presence Services 5.2
3. Avaya one-X Agent Central Management 2.0

For the multihost deployment, installation is performed in the following sequence:

1. System Manager 1.0 followed by Avaya one-X Agent Central Management 2.0 on the same host.
2. Presence Services 5.2 are installed on a separate application host.

Note:

Communication Manager is not included in this sequence as it is installed separately as a standalone installation.

Feature dependencies

This section briefly describes the feature dependencies of Avaya one-X Agent Release 2.0 on various server applications.

System Manager

Avaya one-X Agent depends on System Manager for logging. If the Avaya one-X Agent client is enabled for Central Logging, it sends syslog messages to a server. If the SAL agent on the server is configured to read the syslog messages, alarms can be generated.

Presence Services

Avaya one-X Agent depends on Presence Services for its Instant Messaging (IM) and Presence capabilities. If installed with MOC Gateway that enables communication with Microsoft OCS, agents can communicate with enterprise users.

Avaya one-X Agent Central Management

Avaya one-X Agent depends on Avaya Central Management for the hot-desking feature. Central Management provides a centralized control of multi-location contact centers, multiple agents, and agent end-points. It provides a central storage, control, and delivery of the following Avaya one-X Agent components:

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

User authentication

Avaya one-X Agent supports two types of authentication:

- Basic authentication
- Single sign on

Basic authentication

In basic authentication, the user credentials get authenticated separately against each server present in the deployment (such as Communication Manager, Presence Services, and Central

Management). Therefore, the authentication depends on the server applications present in the deployment. In Avaya one-X Agent Release 2.0, the following configurations are possible:

- Telephony only. (Avaya one-X Agent must be installed without selecting the **Enable Central storage of profile information** check box in the installer).
- Telephony with Central Management without Presence Services
- Telephony with Presence Services without Central Management
- Telephony with Central Management and Presence Services

Authentication for each of these configurations are explained further.

Single sign on

In single sign on, the user credentials get authenticated against Active Directory.

Central Management and Presence Services are the required server applications for single sign on. Since Communication Manager does not communicate with Active Directory, the user is authenticated against Central Management and Presence Services using a Kerberos token.

In case the single sign on does not succeed in authenticating a user, the user must resort to basic authentication, using one of the following options:

- Uninstall Avaya one-X Agent and then reinstall Avaya one-X Agent without selecting the **Use windows credentials to login to Central Management/Presence servers** option.
- Change value of *`UseSingleSignon`* property to `0` in the registry settings (Go to **HKLM** > **Software** > **Avaya** > **Avaya one-X Agent** > **Settings**)

Related topics:

Basic authentication for telephony only on page 8

Basic authentication for telephony with Central Management on page 8

Basic authentication for telephony with Presence Services on page 9

Basic authentication for telephony with Central Management and Presence Services on page 9

Basic authentication for telephony only

This is the most basic configuration that consists only of Communication Manager as the server application. Agent credentials are authenticated against the Communication Manager for signing in and for license request. The authentication is similar to that of Avaya one-X Agent 1.0.

Basic authentication for telephony with Central Management

In this authentication, Communication Manager and Central Management are the two server applications in such a deployment. Therefore, the user must select the Central Management check box and provide the IP address of the Central Management server during the Avaya one-X Agent client installation. The installer stores this server address in the registry. If the server address changes, the registry entries need to be changed or the client must be reinstalled.

In this configuration, the Avaya one-X Agent client sends the user credentials to the Central Management server. The Central Management server passes these user credentials 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 Avaya one-X Agent client settings that are centrally managed by the Central Management. When the user chooses a profile, the associated station ID and password are sent for user and license authentication against the Communication Manager.

Basic authentication for telephony with Presence Services

In this configuration, the user credentials are first authenticated against Communication Manager. If authentication is successful and a full license is obtained, the user can further authenticate against the Presence Services. If successful, the user can use the IM and Presence Services features of Avaya one-X Agent.

If auto-login is chosen during authentication, the Communication Manager authentication is automatically followed by Presence Services authentication. In any case the Presence Services authentication fails, the user cannot use the presence features on Avaya one-X Agent client, but the telephony features can still be used.

Important:

For this type of authentication, Avaya one-X Agent must be installed without selecting the **Enable Central storage of profile information** check box in the installer.

Basic authentication for telephony with Central Management and Presence Services

In this configuration, the Avaya one-X Agent client user credentials are first authenticated against Central Management. The Central Management server passes these user credentials 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 and password. When the user chooses a profile, the associated station ID and password are sent for user and license authentication against the Communication Manager. If the user authentication is successful and a full license is obtained, the user credentials are authenticated against Presence Services. In case of failure at any stage in authentication, the relevant service becomes unavailable for use.

Minimum system requirements

Hardware requirements for single application host deployment

A single application host deployment of the three server applications has the following minimum hardware requirements. This hardware requirement remains same even if Presence Server is installed on a separate application host.

Processor	3 GHz dual-core processor. For example: Intel Xeon Dual Core 3 GHz
RAM	8 GB
NIC support	100 MB
Free disk space	40 GB

Hardware requirements for Presence Services installation

The following table shows the minimum hardware requirements when Presence Services are installed independently on a separate application host or a VM.

Processor	Intel 2.66 GHz single quad core processor
RAM	8 GB
Front Side Bus (FDSB)	1333 MHz or equivalent
Network Interface	100/1000 full duplex Ethernet NIC
Hard disk	73 GB SAS (Serial Attached SCSI), 15000 RPM
Layer 2 cache	4 MB
Hyperthreading enabled/SMP Kernel 2.6	Yes/Yes

Software requirements

The following software requirements are applicable to all deployments:

Operating systems	Red Hat Enterprise Linux (RHEL) 5.1 or 5.2 — 32 bit RHEL must be installed on the system where System Manager, Presence Services, and Central Management are to be installed.
Supported browsers	Internet Explorer 7.0

	Mozilla Firefox 3.x
Supported virtualization system	Avaya one-X Agent supports VMware ESXi and has validated interoperability with Release 3.5.

Chapter 2: Installing System Manager

Prerequisites for installing System Manager

The installer contains the System Manager file in an ISO format. You must perform the following tasks before you proceed to install System Manager.

1. Download the System Manager ISO image from Avaya Licensing and Delivery System web site: https://www.plds.avaya.com.
2. In the `/etc/selinux/config` file, verify that SELinux is disabled by searching for the following option setting:

   ```
   SELINUX=disabled
   ```
3. Set the correct time and locale on the system on which you are planning to run the System Manager installer.
4. Disable firewall:

   ```
   service iptables stop
   chkconfig     --levels 2345 iptables off
   ```
5. The `/etc/hosts` file must contain the correct IP address and name of the application host the installation is to be carried on, otherwise installation will fail. For example, the correct format of this file must appear as shown here:

   ```
   127.0.0.1 localhost.localdomain localhost

   ::1 localhost.localdomain6 localhost6

   <IP Address> myhost.mydomain.com myhost
   ```

Installing System Manager using the ISO image

The installer installs System Manager, JBoss, SAL, and embedded PostgreSQL. If you download the ISO images of the installer files from PLDS and copy them to the System Manager application host using scp or winscp, you can run the installation with the following steps:

1. Login to a console on the system or SSH login with root privilege.
2. Transfer the System Manager ISO image to the System Manager server system.
3. Make sure the ISO image is stored in `/home/craft` directory.
4. Run the following commands from the command line:

   ```
   mkdir /iso
   mount -o ro,loop /home/craft/avmgmt-1.1.4.1.111015-
   installer.iso /iso

   cd /iso
   bash install.sh
   ```

5. When the installation is complete, run the following commands:

   ```
   cd /
   umount /iso
   ```

   This completes the System Manager installation.

Next steps

After a successful install, use the following URL to access the Common Console UI:

- HTTPS – https://<host >/IMSM
- HTTP – http://<host>/IMSM which directs you to the above URL.

The default username is `admin` and password is `admin123`.

Installing System Manager using a DVD

To install System Manager using a DVD:

1. Insert the System Manager DVD in the CD tray and mount the DVD using the following commands:

   ```
   mount /dev/cdrom /mnt
   cd /mnt
   ```

2. Copy the avmgmt-installer-<version>.zip file from the DVD to the host and unzip the file.
3. Run the installer with the following command within the directory where the zip file has been expanded:

```
./install.sh
```

The installation automatically continues for approximately 40 minutes without technician assistance. An indication is given when the installation is complete.

4. When the installation is complete, eject the DVD with the following commands:

```
cd /
eject
```

This completes the installation of the System Manager using a DVD.

Procedures after System Manager installation

Obtaining SAL login service details

Perform these steps after you have installed System Manager.

1. Log on to the System Manager console using the following URL and the following credentials:
   https://System Manager IP address/IMSM
   - User name: `admin`
   - User password: admin123
2. Click **Settings** > **Service Profile Management** > **SPIRIT 1.0** > **DataTransportConfig** .
3. Record the following details from the Data Transport page:
   - **Connection.AvayaProduction.FQDN** for SAL FQDN Name
   - **SpiritPlatformQualifier** for SAL Platform Qualifier Name
4. Exit the System Manager console.

Enrolling a password

Perform this procedure after you have installed System Manager.

1. Log on to the System Manager console
2. Click **Security** > **TrustManagement** > **Enrollment Password** .

   If a password has already been generated, copy it from the **Existing Password** box if the **Time Remaining** or the **Unused Certificates** fields are not set as zero.
3. If an existing password is not present or the time or count are not set to zero, select the expiration of password in days in the **Password expires in** field.
4. In the **Certificate allowed** field, select the number of certificates. Select at least ten certificates per System Manager instance.
5. Click **Generate** if you wish to use a randomly generated string as a password. The **Password** field displays the generated password. If you do not wish to use a randomly generated string, enter a password.
6. Click **Done**.

   Important:

   You must remember this password. You need to provide it as input at the time of installing Presence Server while entering details for the Trust Management Configuration screen.

Chapter 3: Installing Presence Services

Avaya Presence Services overview

Presence Services 5.2 supports Agent Instant Messaging (IM) functionality including agent to agent, and agent to resident expert. In order to provide rich functional advantage over SIMPLE / SIP MESSAGE, the resident expert presence and IM is based on Presence Services native eXtensible Messaging and Presence Protocol (XMPP) IM, which are driven by non-Avaya one-X Agent clients that are federated with Presence Services 5.2. This allows session-based versus message-based IM, enabling association of IM sessions with other communications channels for logging and reporting.

Presence Services 5.2 is designed primarily to support Avaya one-X Agent requirements, such as:

- XMPP IM and Presence
- XMPP IM federation with Microsoft OCS 2007 for IM and Presence
- LDAP directory for user authentication
- Integration with System Manager 1.0

Note:

Presence Services 5.2 integrates with Microsoft Office Communicator (MOC) clients using Microsoft Office Communications Server (OCS) 2007. Presence Services 5.2 is an instant messaging server, supporting Instant Messaging (IM) presence, and provides gateway to Microsoft Office Communications Server (OCS).

The Presence Services provide the following:

- Supports XMPP IM with One-X Agent, or with other standards-compliant XMPP clients.
- Provides bi-directional gateway for IM and Presence between XMPP clients like Avaya one-X Agent and Office Communicator clients over Microsoft Office Communicator Server (OCS) .
- Supports authentication of XMPP Clients through Kerberos.
- Improves serviceability by integrating with System Manager and Secure Access Layer (SAL)
- Converts the standard Syslog format logs to the Common Logging Format (for use by the SAL Agent).
- Monitors and tracks Logging and Alarming through System Manager Console.

Use the XCP controller web-based GUI on the local host for administration, life-cycle management, and configure these components of Presence Services. You can start, stop, and configure these Presence Components of Presence Services software.

Prerequisites for installing Presence Services

The following information needs to be collected after System Manager installation and configured before Installing the Presence Services:

Product	Required Information
Presence Services	Avaya service Login credentials
System Manager	• System Manager IP. • System Manager Host • System Manager Port. • SCEP Password **Note:** SCEP password is set by the System Manager under **Security** > **Trust Management** > **Enrollment Password** .
SAL	1. SAL FQDN (obtained after System Manager installation) 2. SAL Platform Qualifier Name (obtained after System Manager installation) 3. SAL Host Address 4. SAL Host Port 5. SNMP Receiver Host 6. SNMP Receiver Port **Note:** • SAL FQDN and Platform Qualifier Name can be found in the `/opt/Avaya/Mgmt/SALVERSION/SpiritEnterprise/config/DataTransportConfig.xml` file on the System Manager server. • Enter the hostname of the System Manager application host in the host file

	in `/etc` directory on the Presence Services application host.
OCS (If OCS integration is required)	• Login details for the OCS 2007 Access Edge server including domains and hostnames. • Login details for the DNS used by OCS-Edge server including domains and hostnames.

Installing the Presence Services

Prerequisites

- RHEL 5.1 (32 bit version) or higher must be installed
- No other software must be installed on the server.
- The server must be configured to your network
- Verify that 8 GB of disk space is available

Note:

The installation automatically checks the installed Red Hat Linux release.

Download the PS-05.02.00.00-0703.zip installer file from https://www.plds.avaya.com and copy the installer to the host where you want to install Presence Services.

To install Presence Services software:

1. Run the whoami command to verify that you are the root user.
   For example,

   ```
   whoami
   ```

2. If the firewall is running, enter the following command to stop the firewall:
   `service iptables stop`

3. Add Java configuration to environment variables by adding the following to `/etc/profile` directory.
   For example:

   ```
   JAVA_HOME=/usr/java/jdk1.6.0_11
   PATH=$JAVA_HOME/bin/:$PATH
   export PATH JAVA_HOME
   ```

4. Verify that the `/etc/hosts` file contains the following two lines:

```
Loop back_IP localhost.localdomain localhost
```

```
Machine_IP host_FQDN host_name
```

> **Important:**
>
> The system verifies these entries in `/etc/hosts` during the installation process. If these settings are not correctly set , the installation will fail.
>
> If you edit the hostname in the `/etc/hosts` file, you must run the service network restart command and verify the settings are properly set.
>
> You must also set the system static IP address and the fully-qualified domain name (FQDN) because these setting are used by the installer for naming purpose (specifically the hostname and hostname –s)

> **Note:**
>
> Changing the FQDN will require a system reboot for the changes to be applied system-wide.

5. Unzip the PS-05.02.00.00-0703.zip file with the following command

   ```
   unzip PS-05.02.00.00-0703.zip
   ```

   This is the single file required to install PS, provided you have the RHEL, JDK, and System Manager installed.

   The zip file contains the installer (.jar) and the install script (.sh) along with the system verification package (CAF.zip). The install script sets some configuration environment variables and performs some pre-installation tests before initiating the configuration auto framework.

6. Run the command:

   ```
   . /<PS_SP_SCRIPT_NAME>.sh -ci
   ```

   The system prompts you to provide the encryption key.

7. Enter the encryption key. You can enter any encryption key.

   > **Important:**
   >
   > Remember this encryption key as this is required for future installation and uninstallation.

   The system displays the welcome screen of the installation wizard for Presence Services installation.

8. Click **Next** on the welcome screen of the installer.
9. In the **Select the installation path** text field, retain the default path and click **Next**.

   If prompted with warning about overwriting installation directory, choose **OK**.
10. On the Select the packs you want to install screen, select the **PS SAL Configuration** and click **Next**.

Note:

If Presence Services 5.2 is installed on a dedicated application host where Postgres installation and SAL Agent are not shared between, then select **SAL Agent** check box.

SAL Agent pack includes a full SAL Agent installation with PS configuration. Moreover, the PS SAL Configuration includes just the configuration necessary for PS logging and alarming, and does not include the SAL Agent application.

11. On the Executing Task screen, click **Next**.
12. On **General Configuration** screen, perform any one of the following:
    - Select **Complete** option, complete the relevant information and click **Next**.
    - Select **XMPP-IM only** option, complete the relevant information and then click **Next**.
13. Complete the SAL Logging Service Details screen, and then click **Next**.
14. Complete the OCS Integration Details screen, and then click **Next**.

    This screen appears only if you select **Complete** installation option in step 12.
15. Complete the Trust Mgmt Service Configuration screen, and then click **Next**.
16. Click **Next** on the Summary screen with the installation path where the installation will proceed.

    After successful installation, the system displays the Installation Summary screen.
17. Click **Done** to exit the Installation wizard.

Next steps

1. If you have performed a single host installation, restart Jboss using the command:

   ```
   service jboss restart
   ```
2. Log on to the Presence Services console with the *https://<Presence Server IP address>:7300/admin* link in a browser on Presence Services host, using following credentials:
   - User ID: `craft`
   - Password: `craft01`

Make sure that all the components and routers are `Running` and displayed in green.

Procedures after Presence Services installation

Configuring an Active Directory component

Active Directory configuration determines the location of Active Directory (AD) in the network and which users in the Active Directory will be allowed to log on to Avaya one-X Agent.

Active Directory is configured through the XCP controller. After Presence Services are installed, the XCP can be accessed through your browser at *https://Presence Server IP:7300/admin*.

1. Log on to the XCP controller. If you are logging on for the first time after installation, you are prompted to accept a security certificate. Accept the new certificate and proceed to Active Directory configuration.
2. In the Components area on the XCP Controller's main page, select **Active Directory Component** in the list.
3. Click **Go** and then click **Detail** on the Directory Server section.
4. Enter the FQDN of the AD server in **Directory server hostname** field. This must be resolvable.
5. Enter the distinguished name of the Administrator in **Directory Server user**.
   For example:
   `cn=Administrator,cn=Users,dc=Subdomain,dc=mycompany,dc=com`
   where cn and dc can be in lower case.

   Moreover, if the FQDN does not contain Avaya, dc=subdomain or domain and dc=com.
6. Enter the Administrator password in **Password for directory server user** and **Confirm password** fields.
7. Click **Submit**.
8. On the Database section, click **Details**.
9. Scroll to **Base context for this LDAP class** field and enter the base context of the AD from where to allow users to log on.
   For example: For the OU 'Users' in the domain above (my.domain.com), this field must be cn=users,dc=my,dc=domain,dc=com
10. Click **Submit** twice to save the settings.
11. Click **Edit** on the Presence Session Manager component.
12. Clear the **mod_auth_plain** and **mod_auth_digest** check boxes and select the **mod_jds** check box.

13. Select **JDS Configuration** and clear **Registration Requirements** check boxes.
14. Click **Submit** and restart Presence Services by going to `/opt/Avaya/Presence/presence/bin` directory and run the stop script and then the start script.

Next steps

After the Presence Services are restarted, make sure that all the components are in running condition. This can be checked on the Presence Services console.

Configuring OCS

Prerequisites

To perform the Office Communication Server (OCS) setup, you must choose either a **Complete** installation or **XMPP-IM** when installing Presence Services 5.2, as this will create the required components. However there are additional post installation steps required for the secure connection configuration.

1. Perform the following procedures on the OCS:
   a. Copy `JABBER_HOME/certs/export-xxx.trusts` to Microsoft Edge (Could use WinSCP from MS Edge Server).
   b. Import to MS certificates as follows: Open Certificates Snap-in for Edge Server in MMC and then Open `Certificates/Trusted Root Certification Authorities/Certificates`.
   c. Right-click on Certificates in the left-hand pane and select **All Tasks/Import**. This will launch the Certificate Import Wizard. Follow through the steps of the wizard and browse for the export-xxx.trusts file you copied over from in step a.
2. For the Presence Services side, the OCS gateway component needs to trust the Certificate Authority (CA) of the OCS/EDGE. To do this perform the following steps:
   a. Download Microsoft root CA, <msroot>.cer.
      (download from *http://<ipofca>/certsrv/*)
   b. Copy to `/opt/Avaya/Presence/jabber/xcp/certs` (or equivalent).
   c. Run dos2unix <msroot>.cer.
   d. Append to .trusts file using:
      cat <msroot>.cer >>export-xxx.trusts
   e. Restart Presence Services and reboot Edge then run the following commands:

```
PRES_HOME/presence/bin/stop.sh
PRES_HOME/presence/bin/start.sh
```

Configuring Kerberos for single signon

1. Create an Active Directory user for the Presence XCP server. Keep the account options as simple as possible. Make sure that the user's password does not expire and that the user is not forced to change it the next time user logs in.
2. On the Active Directory server, use the KTPASS utility to generate a keytab for the Presence XCP user as follows:

   ```
   ktpass -princ xmpp/XCP_HOSTNAME@AD_REALM -pass XCP_PASSWORD
   -out krb5kt -mapuser XCP_USERNAME
   ```

   For Jabber XCP for Linux installations, name the output file as `krb5.keytab`.

   Note:
   To use the ktpass command, you must first download and install Windows Server 2003 R2 support tools (or a version that matches your server). This is available from *Microsoft.com*. Once installed, the ktpass command can be executed from a DOS prompt.

3. Move the generated keytab file to the Presence Services server in the following location:

   `/etc/krb5.keytab`

4. Create the Kerberos configuration file as shown below:

   ```
   [libdefaults]
        default_realm = AD_REALM
        rnds = false
   [domain_realm]
        XCP_HOSTNAME = AD_REALM
   ```

   For example:

   ```
   [libdefaults]
        default_realm = CORP.EXAMPLE.COM
        rnds = false
   [domain_realm]
        example.com = CORP.EXAMPLE.COM
   ```

   For Linux installations, save the file as /etc/krb5.conf

5. You must complete the trust relationships on both sides:
   a. Go to **Active Directory Domains and trusts** on the Domain Controller under "**Administrative Tools**" on the start menu.
   b. Right-click on **AD Realm**, e.g. "example.domain" and go to properties.
6. Add a new rust entry under the **Trusts** tab. Entries that would work for the sample configuration would be:

- **Name**: XCP_HOSTNAME (For example, example.com)
- **Trust type**: Realm trust
- **Trust transitivity**: transitive
- **Direction**: Two way
- **Trust password**: <the password associated with the account that was created in Step 1>

7. Create the xmpp.conf file containing the following line:

   ```
   mech_list: gssapi
   ```

   For Linux installations, save the file in `JABBER_HOME/lib/sasl2`.
8. Change to the Presence XCP Controller's Advanced configuration view.
9. In the Router area on the Presence XCP Controller's main page, click **Edit** beside the Presence Session Manager.
10. In the Presence Session Manager Configuration page, scroll down to the **Hostnames for this Component** area, and make sure that the name specified in the **Host Filters** box matches the XCP_HOSTNAME specified in step 2.
11. Click **Submit** (or **Cancel** if you made no changes) to return to the Presence XCP Controller's main page.
12. In the **Components** area on the Presence XCP Controller's main page, click **Edit** beside the first Connection Manager.
13. In the Connection Manager Configuration page under **Add a New Command Processor**, click **Details** to edit the JSM Command Processor.
14. In the JSM Command Processor Configuration page under **Director Configuration**, click **Details** beside the first XMPP director.
15. Scroll to the bottom of the XMPP Director Configuration page, and select **SASL Settings**. Specify the AD_REALM from the krb5.conf file in the **SASL Realm** box.
16. Click **Submit** to save the director's configuration. You return to the JSM Command Processor Configuration page.
17. Under **Director Configuration**, click **Details** beside the second XMPP director, and repeat the previous two steps.
18. Click **Submit** on each configuration page until you have returned to the Presence XCP Controller's main page.
19. Restart the Presence XCP system.

Chapter 4: Installing Central Management

Prerequisites for installing Central Management

The Avaya one-X Agent Central Management 2.0 has an automatic installer.

Prerequisites to run the installer

- The installer assumes that you know the LDAP details such as the bindDN to be used to configure Jboss to communicate with the Active Directory Server.
- Installation will only succeed if System Manager has been installed.

Installing Avaya one-X Agent Central Management

Prerequisites

Make sure that the System Manager 1.0 and Presence Services 5.2 are already installed before attempting to install Avaya one-X Agent Central Management.

Tip:

In a multihost deployment where Presence Services are installed on a separate host, Central Management can be installed before Presence Services.

Download the oneXAgentCM-2.0.1012.0.zip installer file from https://support.avaya.com to a directory on the host where you want to install Central Management.

You can use this installation procedure for both fresh installation and upgrades. While performing an upgrade, the previously configured data is preserved.

1. Log on to the Linux application host as root.
2. Open the directory where you have downloaded the oneXAgentCM-2.0.1012.0.zip file on the Linux host, using the chdir <directory name> command.
3. Unzip the oneXAgentCM-2.0.1012.0.zip file.
4. Run the following command to open the installer:

```
chmod 754 oneXAgentCM-install.sh
./oneXAgentCM-install.sh
```

This starts the installer and displays the welcome page.

5. Click **Next** on the welcome page.
6. On the LDAP Information screen, perform one of the following:
    - Enter the distinguished name and password provided while configuring active directory component in the **LDAP.bindDN** and **LDAP.bindCredential** fields respectively.
    - Enter the URL of LDAP directory in **LDAP.url** and the user name search context in **LDAP.baseCtxDN**.

   The information provided on the LDAP Information screen consists of long text strings. You are advised to obtain this information electronically to be able to copy the text strings without causing any errors.
7. Click **Next**. Avaya Central Management is now installed .

Next steps

After a successful install, the following URL can be used to access the Avaya one-X Agent Central Management:

https://<host>/oneXAgentCM

The following default Administrator user is created:

User name	Password
onexagentcm	oxacm01
craft	craft01
sroot	sroot01

Note:

You can log on to Central Management using `onexagentcm`, `craft`, or `sroot` if System Manager and Central Management are on the same application host.

Other users can be imported from Active Directory as directed in the initial configuration.

Procedures after Central Management installation

Initial configuration after Central Management installation

At this stage of the installation, the web UI should be accessible and contain the details for the users called `onexagentcm`, `craft` and `sroot`. All other users need to have their details imported into the system using the bulk user import feature. Users can be imported using the defined spreadsheet format which can be produced by any means. The instructions below show a shortcut method of producing this spreadsheet directly from an LDAP browsing tool called “Apache Directory Studio”.

1. Download and install Apache Directory Studio.
2. Run Apache Directory Studio.
3. Create a new connection in the Connections window in the bottom left hand corner of the screen using right click **New Connection** menu item.
4. Navigate to the part of the LDAP tree containing the users which will be accessing Avaya one-X Agent Central Management.
5. Right-click at that point in the tree and select the **Export** > **Excel Export** submenu.
6. Open the export file in Excel.
7. Open the import template file https://<host>/oneXAgentCM/data/example.csv in Excel.
8. Copy the data from the export file into the appropriate columns in the import template file and save under a new filename on the local file system as comma separated values (csv).
9. Navigate to the *https://<host>/oneXAgentCM/pages/ImportUsersPage* page and import the new file.

Synchronizing Central Management with LDAP

LDAP Synchronization allows Central Management users to be synchronized with a given LDAP (Active Directory) server. The synchronization is performed via a timer that runs 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 fields that are updated on the LDAP server are changed in the Central Management database so that the Central Management field always has the same value as the LDAP field.

Mapping LDAP to Central Management

The entries from LDAP are mapped to Central Management attributes using the *ldapusermapping.properties* mapping file. You must restart JBoss for the changes made to the mapping file to take effect. The file is located in the `/opt/Avaya/OneXAgentCM/conf/` directory.

You can override the location of this file using the *cam.ldap.mapping.config.dir* system property.

If the file is not present in the directory then LDAP Sync will log a message and exit.

Disabling LDAP synchronization

By default, LDAP Sync is disabled. If after enabling LDAP Sync a user wants to later disable it, they must remove or rename the file ldapusermapping.properties.

Configuring Single Sign On (SSO) setup

Configuration for SSO must be completed after a regular installation of Avaya one-X Agent Central Management has been done and has been proven working. The steps described below assume a working system installed using the methods described in the main section of this document.

Avaya one-X Agent Central Management can be configured to use the Windows Kerberos credentials and the SPNEGO protocol for Single Sign On (SSO). This removes the need for users to enter a username and password combination each time they access the system Avaya one-X Agent Central Management makes use of a JBoss authentication module called “JBoss Negotiation” which integrates with JBoss container that Avaya one-X Agent Central Management runs on.

The detailed steps for configuring SSO are described in the document “User Guide for JBoss Negotiation” available from:

http://www.jboss.org/community/wiki/JBossNegotiation

You must read this document before you attempt to configure a system.

A summary example is shown below for a system with the following critical values:

Central Management Hostname: *vmcamdeployed.austest.avaya.com*

Active Directory domain (long form): *austest.avaya.com*

Active Directory domain (short form): *AUSTEST*

1. Run the following commands on the Active Directory server at the command prompt:

   ```
   setspn.exe -a host/vmcamdeployed.austest.avaya.com
   vmcamdeployed
   setspn.exe -a HTTP/vmcamdeployed.austest.avaya.com
   vmcamdeployed
   ktpass -princ host/vmcamdeployed@austest.avaya.com -pass * -
   mapuser AUSTEST\vmcamdeployed -out C:
   \vmcamdeployed.host.keytab
   ```

   This last command will generate a file `C:\vmcamdeployed.host.keytab` file

2. Transfer the generated file to a Windows machine with a JDK installed (as Active Directory server will rarely have a JDK) and run the following command:

   ```
   ktab -k vmcamdeployed.host.keytab -a
   vmcamdeployed@austest.avaya.com
   ```

   This command updates the generated file with some further information.

3. Transfer the generated file to the one-X Agent Central Management server and place it in the /etc directory

4. Ensure the Linux server has its time synchronized to the Active Directory server using NTP.

5. Ensure the Linux server hostname command returns the full machine name matching that used for the commands above.

6. Update the JBoss login configuration using the following steps

   ```
   service jboss stop
   ```

7. Copy the following section of the text :

   ```
   <application-policy name="host">
     <authentication>
       <login-module
   code="com.sun.security.auth.module.Krb5LoginModule"
   flag="required">
          <module-option name="storeKey">true<module-options>
           <module-option name="useKeyTab">true<module-options>
             <!-- It is CRITICAL that the domain name be in
   ```

```
UPPERCASE -->
          <module-option name="principal">host/
vmcamdeployed@AUSTEST.AVAYA.COM</module-option>
                <module-option name="principal">host/
vmcamdeployed@AUSTEST.AVAYA.COM</module-option>
                <module-option name="keyTab">/etc/
vmcamdeployed.host.keytab</module-option>
              <module-option name="doNotPrompt">true</module-
option>
                <module-option name="debug">true</module-
option>
            </login-module>
        </authentication>
    </application-policy>

<application-policy name="SPNEGO">
    <authentication>
        <login-module
code="org.jboss.security.negotiation.spnego.SPNEGOLoginModul
e" flag="requisite">
            <module-option name="password-
stacking">useFirstPass</module-option>
                </login-module>
                <login-module
code="org.jboss.security.auth.spi.UsersRolesLoginModule"
flag="required">
                <module-option name="password-
stacking">useFirstPass</module-option>
                <module-option name="usersProperties">props/
spnego-users.properties</moduleoption>
         <module-option name="rolesProperties">props/spnego-
roles.properties</moduleoption>
        </login-module>
    </authentication>
</application-policy>
```

8. Insert the copied text from above into the following file, directly after the opening <policy> tag:

   `/opt/Avaya/JBoss/4.3.0/jboss-eap-4.3/jboss-as/server/avmgmt/conf/login-config.xml`

9. Install the JBoss negotiation test application (jboss-negotiation-toolkit.war) into the directory: `/opt/Avaya/JBoss/4.3.0/jboss-eap-4.3/jboss-as/server/avmgmt`.

10. Restart the JBoss server.

    ```
    service jboss start
    ```

11. Debug the SSO setup using the JBoss Negotiate supplied tools and method documented in the *JBoss Negotiation document section 2.3 Negotiation Toolkit*.

12. After SSO has been proven to be working with the test application the configuration can then be extended to include the OXACM application.

Tip:

To avoid being locked out of the web application, new “Web Administrator” accounts should first be created using the full account name in the **Username** field e.g. `admin@austest.avaya.com`.

13. After the new administrator accounts have been created, the following command sequence should be used:

```
service jboss stop
/opt/Avaya/OneXAgentCM/bin/oxacmrepacksso.sh
```

The command above will make a copy of the HostedCCAll.ear and repackage a new version appropriate for SSO in the directory:

```
/opt/Avaya/OneXAgentCM
```

```
rm /opt/Avaya/JBoss/4.3.0/jboss-eap-4.3/jboss-as/server/
avmgmt/deploy/HostedCCAll.ear
```

```
cp /opt/Avaya/OneXAgentCM/HostedCCAll-{longstringofnumbers}-
sso.ear /opt/Avaya/JBoss/4.3.0/jboss-eap-4.3/jboss-as/
server/avmgmt/deploy/
```

```
service jboss start
```

Viewing software inventory

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

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

```
/opt/Avaya/OneXAgentCM/bin/oxacminvent.sh
```

The system displays the list of software deployed. A sample output is displayed in the subsequent example.

Example

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<avayaInstallInventory version="1.0">
```

```
<targetMachineDetails installPath="/opt/Avaya"
ipAddress="192.168.37.132" name="ozvmcfegan.austest.avaya.com"/>

<pack name="SAL Agent" id="SPIRIT">

<version date="09-Oct-09 15:23" id="1.0.17.0"/>

</pack>

<pack name="Postgres" id="PostgresID">

<version date="09-Oct-09 15:23" id="8.2.6.0"/>

</pack>

<pack name="JBoss" id="JBossID">

<version date="09-Oct-09 15:23" id="4.3.0.0"/>

</pack>

<pack name="System Manager" id="MgmtID">

<version date="09-Oct-09 15:23" id="1.0.17.0"/>

</pack>

<pack name="SIP A/S Management Console" id="Pack.SIPAS.console">

<version date="09-Oct-09 15:24" id="8.0.44.0"/>

</pack>

<pack name="ElementManager" id="Panther">

<patchversion date="09-Oct-09 15:31" id="1.1.4.1"/>

</pack>

<pack name="PS SAL Configuration" id="PS_SAL_Configuration">

<version date="09-Oct-09 16:11" id="1.0.18.0"/>

</pack>

<pack name="Presence Services" id="PS">

<version date="09-Oct-09 16:11" id="05.02-00-00-0703.0.0"/>

</pack>

<pack name="one-X Agent Central Management" id="OneXAgentCM">

<version date="09-Oct-09 16:26" id="2.0.1002.0"/>

</pack>

<avayaInstallInventory>
```

Chapter 5: Troubleshooting server applications

Common troubleshooting procedures

Troubleshooting JBoss

If JBoss is running, access to Central Management and System Manager must be possible. Run the following commands from the command line on the Linux host which has all the server applications installed if the respective UIs are returning errors on your browser.

- To check if JBoss is running:

  ```
  service jboss status
  ```

- To stop JBoss:

  ```
  service jboss stop
  ```

- To start JBoss:

  ```
  service jboss start
  ```

- To stop and start JBoss with a single command:

  ```
  service jboss 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 or System Manager before the startup is complete, the following message is displayed.

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

If the UI continues to return an error, check the log file from the following location:

```
/opt/Avaya/JBoss/4.3.0/jboss-eap-4.3/jboss-as/server/avmgmt/log/
server.log
```

Troubleshooting Postgres and Presence Services—XCP

If Postgres is down, there will be no UI access for Presence Services, System Manager or Central Management Server. Run the following commands on the application host where the server applications are installed.

- To check if Postgres is running or stopped:

```
service postgresql status
```

- To start Postgres:

```
service postgresql start
```

- To stop postgres

```
service postgresql stop
```

- To stop and start with a single command

```
service postgresql restart
```

The XCP controller must also be running to access the Presence Services UI. You can start and stop various components from the Presence Services UI.

- To check XCP status:

```
/opt/Avaya/Presence/jabber/xcp/bin/runcontroller status
```

- To start XCP:

```
/opt/Avaya/Presence/jabber/xcp/bin/runcontroller start
```

- To stop xcp

```
/opt/Avaya/Presence/jabber/xcp/bin/runcontroller stop
```

Troubleshooting Jabber and Presence Services

Jabber must be running for Presence Services components to work. Run the following commands on the host where Presence Services are installed.

- To check the Jabber status:

```
/opt/Avaya/Presence/jabber/xcp/bin/runjabber status
```

- To start the Jabber:

```
/opt/Avaya/Presence/jabber/xcp/bin/runjabber start
```

- To stop the Jabber:

```
/opt/Avaya/Presence/jabber/xcp/bin/runjabber stop
```

To check whether the presence processes are running as expected:

```
ps -ef | grep presence
```

Validating Central Management and Active Directory connection

1. Log into the Central Management using the user name and password as `craft` and `craft01` respectively.
2. Add a user that exists in the Active Directory and assign that user the Web Administrator role.
3. Close your browser to log out of Central Management.
4. Log into the Central Management using the newly provisioned Web Administrator user name and password.

   If your log in is successful, the connectivity to Active Directory is established.
5. If the Central Management administration login fails, perform the following steps to verify that the AD connection and search criteria that was entered during Central Management installation is correct.

   > Using an LDAP browser such as Apache Directory Studio, create a new connection to the service account entered during Central Management installation using the same syntax for the bindDN
6. If using the LDAP browser to connect to the Apache Directory using the bindDN and password fails, backup the files you require to edit and perform the following procedures:
   a. Review the bindDN information in the login-config.xml file in the `/opt/Avaya/JBoss/4.3.0/jboss-eap-4.3/jboss-as/server/avmgmt/conf` directory and make the necessary changes to the bindDN , bindCredential or LDAP url.

   b. If using the LDAP browser succeeds in connecting to the defined service account then review the baseCTXDN defined in the login-config.xml in the `/opt/Avaya/JBoss/4.3.0/jboss-eap-4.3/jboss-as/server/avmgmt/conf` directory.

   This is to determine that the location at which the search root begins includes all the possible paths within the Active Directory structure and contains all potential users that will get authenticated via the Central Management. Using the LDAP browser connect provides the view of the Active Directory structure and the necessary information for guiding changes to the configuration that was entered during Central Management installation.

   c. Once the changes are applied, run the following command to restart JBoss application server:

```
service jboss restart
```

Note:

You must allow sufficient time for JBoss to restart as it takes several minutes to completely restart.

Testing communication between Active Directory and Presence Services

1. Follow the Presence Services documentation to set up Presence Services to use Active Directory for authentication.
2. Create a user in the Active Directory. Use this user credentials to log in to Avaya one-X Agent.
3. Start the Avaya one-X Agent client in any of the three modes.
4. Open **System Options** > **System Settings** and in the **Login** menu, click the **IM** tab.
5. Configure the Presence Services details on the **IM** tab.
6. Log on to Avaya one-X Agent client. Avaya one-X Agent client

   If the Active Directory details are configured correctly on the presence server, you must be able to log in to the Presence Services.
7. Once logged in, you can see the status of any other users in the system and be able to send and receive instant messages and search for existing users registered with this presence server.

If you still not able to log in, check the `/opt/Avaya/Presence/jabber/xcp/var/log/presence_stats.log` file logs.

Testing communication between System Manager and Presence Services

1. Make sure that Presence Services are running.
2. Open the **Monitoring** tab on the System Manager console and view the logs and alarms from the Presence Services.
3. Check for the logs of start and stop actions of Presence Services that are displayed as logs/alarms on the System Manager console

If no logs or alarms are displayed on the System Manager console, check the SAL documentation for configuration.

Testing communication between System Manager and Central Management

1. Make sure that Central Management is running.
2. Open the **Monitoring** tab on the System Manager console and view the logs and alarms from the Central Management.
3. Check for the logs of start and stop actions of Central Management that are displayed as logs/alarms on the System Manager console

If no logs or alarms are displayed on the System Manager console, check the SAL documentation for configuration.

Testing communication between Central Management and database

Start the Central Management UI using https://<IP Address>/oneXAgentCM.

If the database not running, an error page is displayed.

Check the `/opt/Avaya/JBoss/4.3.0/jboss-eap-4.3/jboss-as/server/avmgmt/log/server.log` file for Central Management logs.

You can also run the following command to check if the database is not responding:

```
service postgresql status
```

Testing communication between System Manager and database

Start the System Manager console using https://<IP Address>/IMSM.

If the database not running, an error page is displayed.

Check the `/opt/Avaya/JBoss/4.3.0/jboss-eap-4.3/jboss-as/server/avmgmt/log/server.log` file for System Manager logs.

You can also run the following command to check if the database is not responding:

```
service postgresql status
```

Testing communication between Presence Services and database

Start the Presence Services UI using https://<IP Address>/:7300/admin.

If the database not running, an error page is displayed.

Check the `/opt/Avaya/Presence/jabber/xcp/var/log` directory for Presence Services logs.

You can also run the following command to check if the database is not responding:

```
service postgresql status
```

Alarms and logging for server applications

You can access logs and alarms through SAL and System Manager. Refer to System Manager documentation for details on how to access alarms and logs.

Central Management creates alarms when it logs error messages. The alarm ID is issued by ART registration process.

Related topics:
Accessing logs and changing log levels on page 40

Accessing logs and changing log levels

1. To access log data:
    a. Log on to the System Manager console.
    b. Go to **Monitoring** > **Logging** from the navigation menu.
    c. Filter on the product type and find com.avaya.onexagentcm. You can refer the Presence Services documentation for the Presence Services logs.
2. To change logging levels:
    a. On the System Manager console, go to **Settings** > **Logging Configuration**
    b. Select the appropriate logger from the list and click **Edit**
    c. On the Edit Logger page, set the level in **Log level** field.

Troubleshooting System Manager

No matter whatever encryption key I enter, it always throws an error "Invalid encryption key"

You might be using java 1.4 version.

Proposed Solution

Ensure that you are using Java 1.6 or higher version.

SAL Agent does not start on Sparc -64

This issue occurs because of conflict in ports.

Proposed Solution

For the port conflict issue, it is possible that the SAL agent has not started.

1. Do the following changes in the $SPIRIT_HOME/wrapper.config file to confirm that there is a port issue:
   a. Set wrapper.debug to "true".
   b. Set wrapper.logfile.loglevel to "ALL"
   c. Restart the SAL agent.

   The log file $SPIRIT_HOME/logging/wrapper.log should get generated and should indicate that either "wrapper.port" or "wrapper.jvm.port" is already in use.
2. To resolve conflicting ports:

a. Add the entry for wrapper.port with value greater than 32000 for changing the wrapper port. This is the default value.

b. Set wrapper.jvm.port.min and wrapper.jvm.port.max to a value greater than 32000. The default values are "31000" and "31999" respectively. Do not assign the port that you have assigned to wrapper.port.

Troubleshooting presence services

Access to the XCP controller fails

If access to the XCP controller fails after installation, run the following commands to check the status of the XCP controller and Jabber:

```
/opt/Avaya/Presence/jabber/xcp/bin/runcontroller status
/opt/Avaya/Presence/jabber/xcp/bin/runjabber status
```

If the status shows neither to be running they can be started as follows:

```
/opt/Avaya/Presence/jabber/xcp/bin/runcontroller start
/opt/Avaya/Presence/jabber/xcp/bin/runjabber start
```

If any of the above steps fail, check the system logs to find out the cause of the problem.

Presence services installer error

The PS installer checks for the presence of PostgreSQL rpms and other dependent rpms. If an attempt at an installation results in the following error:

```
./PS-05.02.00.00-0703.sh -ci

error: Failed dependencies: libpq.so.4 is needed by (installed)

apr-util-1.2.7-6.i386

ERROR: Found Postgres packages with dependencies, please remove them
and their dependencies
```

Remove apr-util-1.2.7-6.i386 using the –nodeps option. Installation should then proceed to completion. Ensure no errors are recorded in the instillation log files which are found at `/opt/Avaya/install_logs/` directory.

SMGR common console UI error after a Presence services installation

When logging into a SMGR Common Console UI, the following error may appear after a PS install:

```
Login failed. System could not process the request - exception:
UPMLoginModule: Could not verify against UPM database. Failed to get
database connection.
```

Presence services install scripts may have overwritten some configuration values used by SMGR. To fix this, run the command:

```
/opt/Avaya/Postgres/8.2.13/utils/securePostgres
```

You may see the following error when you run the script:

```
mv: cannot stat `/opt/Avaya/Mgmt/1.0.18/utils/mgmt-postgres-ssl-
ds.xml': No such file or directory
```

The script updates `/var/lib/pgsql/data/postgresql.conf`.

Ensure that there are no double entries in the section of “Security and Authentication”. In addition the line, “hostssl all all 127.0.0.1/32 md5” should appear in `/var/lib/pgsql/data/ pg_hba.conf` for a successful login to the SMGR Common Console UI. Restart posgreSQL and JBoss Servers after this.

Troubleshooting Central Managment

Internal server error when starting Avaya one-X Agent Central Management UI

If JBoss is started and the Avaya one-X Agent Central Management tables are not created, ensure that you have created the databases “camdb” and “jboss” with owner “camuser” and password “camuser” before deploying the Avaya one-X Agent Central Management. The log file pgstartup.log found at `/var/lib/pgsql` can be used to check if errors were logged during an attempt at table creation.

Cannot access System Manager, Presence Services UI, or Central Management UI

Assuming you have typed in the correct URLs to access the UIs, check if JBoss is running:

```
service jboss status
```

This should show whether JBoss is running or stopped. If it has stopped then restart JBoss

```
service jboss restart
```

If access to System Manager UI, Presence Services UI, or Central Management UI still fails, check if PostgreSQL is running:

```
service potgresql status
```

This should show whether JBoss running or stopped. If it has stopped restart postgreSQL.

```
service postgresql start
```

403 error from Central Management

If you start the Avaya one-X Agent Central Management UI and get a 403 unauthorized error, ensure the user you are trying to log in, is in both the Avaya one-X Agent Central Management database and Active Directory database, and has a role authorizing the user to get the requested resource.

Central Management unavailable message

Once you deploy the Avaya one-X Agent Central Management application and start the Web UI, 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 instead of the desktop client.

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

The following is an example of what you see after entering the user name and password, you see following information:

```
Timestamp: 2009-08-10T06:02:56.763Z

Remote address: 135.27.66.163

Remote host: ozcfegan-a0.auslabs.avaya.com

Username: craft
```

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 and corresponding location details on the Manage Locations page of the Avaya one-X Agent Central Management UI, check the users proxy settings.

If you are working in an environment that has a Web proxy, ensure it is NOT used for traffic going to the Avaya one-X Agent Central Management server. To do this, set an exception in the **Proxy Server** settings of Internet Explorer. Go to the menu **Tools** > **Internet Options** > **Connections** > **Lan Settings** > **Advanced** and make sure that hostname of the Avaya one-X Agent Central Management appears in the **Exceptions** list.

Go to the menu **Tools** > **Options** > **Network** > **Lan Settings** > **Advanced** and make sure that hostname of the Avaya one-X Agent Central Management appears in the **Exceptions** list.

Use the following procedure for Mozilla Firefox:

1. Click **Tools** > **Options** .
2. On Options window, click **Network** tab.
3. Click **Settings**.
4. Make sure that Central Management hostname 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 is displayed. Ensure the Avaya one-X Agent user has been assigned a profile on the Manage Users page, on the Avaya one-X Agent Central Management UI.

No connection between Central Management and JBoss and Postgres

To determine whether the connection between CAM/JBoss and Postgres is broken or not working properly, you can review the logs. The logs contain errors about not being able to write to the database.

Central Management does not work after installation

Reinstall Central Management and ensure all prerequisite software are in place.

Appendix A: PLDS Licensing

Overview

Downloading product software and licenses

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

Installation software applications for different products are available as ISO files on PLDS. After activating the license entitlements, installation administrators must 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.

Always review the PLDS to determine if a later service pack or release is available. If updates do exist, you should refer to the appropriate upgrade procedures, contact Avaya, or contact the Avaya BusinessPartner Service representative.

Obtaining licenses

You should have a license code with you before you install a product. Using PLDS, you can activate the license entitlements and download the products.

After you buy a product, an Avaya BusinessPartner or an Avaya Associate who has permissions in PLDS for your site or sales order can access PLDS and generate license entitlements for you. You must provide the MAC address of the WebLM server to generate license entitlements in the form of License Activation Codes (LACs). The LAC will help you identify the product among other Avaya products you hold licenses for, keep track of the number of downloads, and automatically download patches and upgrades - all the while keeping the required groups and coordinators informed, through e-mail messages. The LAC e-mail recipients must be identified during the order placement process by providing their e-mail addresses.

With the LACs in hand, you can use the Quick Activation screen to activate the LACs and download the product.

Activating entitlements

Use this functionality to activate one or more entitlements for a product using the license activation code. You may choose to activate all the licenses or specify the number of licenses that you want to activate from the total number of licenses associated with the entitlements.

On successful activation of the entitlements, PLDS sends an Activation Record to the customer registered with the entitlements by an e-mail. The Activation Record provides details of the number of activated licenses, the Host ID of the computer on which licenses are activated, and the complete link of the product download. The e-mail also contains the license file. You need to install the license on the License Host (WebLM server) to use the licenses.

Prerequisites

To activate a license entitlement, you must have License Activation Codes (LACs) and the Host ID of the computer on which you want to install the licenses.

1. Type `http://plds.avaya.com` in your web browser to access the Avaya PLDS Web site.
2. Enter the Login ID and password to log on to the PLDS Web site.
3. Enter the License activation code (LAC) that you have received through an e-mail in the **LAC(s)** field in the Quick Activation section.

   Note:

   If you do not have an e-mail with your LAC ID, follow the steps in the Searching for Entitlements section and make a note of the appropriate LAC ID from the LAC column. The Quick Activation automatically assumes you want to activate all entitlements on LAC, and gives the option to remove line items, and enter amount of each license to activate (full or partial amount).
4. Enter the host information.
5. Click **Next** to validate the registration detail.
6. Enter WebLM Host Server Information.

   The Host ID is the MAC address from the machine hosting the WebLM server. Click on the **Help** link and follow the instructions on how to obtain the MAC address.
7. Enter the number of licenses you want to Activate.
8. Read and accept the Avaya Legal Agreement.
9. Perform the following steps, to send a confirmation e-mail:

   a. Enter any additional certificate recipients e-mail addresses in the **E-mail to:** field.

   b. Enter Comments.

   c. Click **Finish**.
10. Click **View Activation Record**.
    - The **Overview** tab displays a record of the key activation information.
    - The **Ownership** tab confirms the registration information.
    - The **License/Key** tab displays the actual license files which allow x number of users to use the software. A single license file will be generated for each

product line. From **License/Key** tab, you can select options to view activation details, and installation instructions.

Searching for entitlements

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

1. Type `http://plds.avaya.com` in your web browser to access the Avaya PLDS Web site.
2. Enter the Login ID and password to log on to the PLDS Web site.
3. Enter the company name in the **%Company: field**. If you would like to see a complete list of possible companies before searching for their corresponding entitlements, do the following:
    a. Click **Search**.
    b. Enter the name or several characters of the name and a wildcard (%) character.

       Company names are case sensitive. Search using both upper and lower case characters to ensure that you have visibility into all possible records.

    c. Click **Search Companies**.

    ⊕ **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 except at the beginning. If you enter %av as the search criteria, the page displays an error.

4. 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 except at the beginning. If you enter %av as the search criteria, the page displays an error.

5. Enter the specific license activation code (LAC) ID in the **%LAC:** field.

   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 `AS0%`, the system searches for all the LACs starting with AS0. You can enter a wildcard character (%) at any position in the search criteria except at the beginning. If you enter %AS0 as the search criteria, the page displays an error.

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

6. Select the application, product, license type and status from the drop-down field.
7. Click **Search Entitlements**.

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

Rehosting

Use this functionality to move or swap out the activated items from the host on which the licenses are installed to another host or computer if the current License Host fails or does not work properly. You may chose to move either all or specified quantities of activated items from one License Host to another License Host. For rehosts or moves:

- Use the LAC to search for the License Host to rehost/move from
- Provide the Host ID or License Host for the License Host to rehost/move to

1. Type `http://plds.avaya.com` in your web browser to access the Avaya PLDS Web site.
2. Enter the 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.

5. Select **Rehost/Move** from the appropriate record which will display.
6. Enter the new host information in the **Enter New Host Information** field.
7. Validate the Registration Detail and click **Next**.

8. Enter WebLM Host Server Information.

   The Host ID is the MAC address from the machine hosting the WebLM server. Click on the **Help** link and follow the instructions on how to obtain the MAC address.

9. Enter the number of Licenses to Activate in the **QTY column** field and click **Next**.

10. Accept the Avaya Legal Agreement.

11. Perform the following steps, to send a confirmation e-mail:

    a. Enter any additional certificate recipients e-mail addresses in the **E-mail to:** field.

    b. Enter Comments.

    c. Click **Finish**.

12. Click **View Activation Record**.

    - The **Overview** tab displays a record of the key activation information.
    - The **Ownership** tab confirms the registration information.
    - The **License/Key** tab displays the actual license files which allow x number of users to use the software. A single license file will be generated for each product line. From **License/Key** tab, you can select options to view activation details, and installation instructions.

Regenerating a license file

Use this functionality to regenerate the License/Key on a selected License Host. During the regenerate process, you are able to change the activation details, except for the Host ID.

1. Type `http://plds.avaya.com` in your web browser to access the Avaya PLDS Web site.

2. Enter the 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 a confirmation e-mail:

a. Enter any additional certificate recipients e-mail addresses in the **E-mail to:** field.

b. Enter Comments.

c. Click **Finish**.

10. Click **View Activation Record**.

    - The **Overview** tab displays a record of the key activation information.
    - The **Ownership** tab confirms the registration information.
    - The **License/Key** tab displays the actual license files which allow x number of users to use the software. A single license file will be generated for each product line. From **License/Key** tab, you can select options to view activation details, and installation instructions.

Downloading software in PLDS

1. Type http://plds.avaya.com in your web browser to access the Avaya PLDS Web site.
2. Enter the Login ID and password to log on to the PLDS Web site.
3. Select **Assets** from the Home page and select **View Downloads**.
4. Search for the downloads available using one of the following methods:
    - By Actual Download name
    - By selecting an Application type from the drop-down list
    - By Download type
    - By clicking **Search Downloads**
5. Click the download icon from the appropriate download.
6. When the confirmation box displays, select **Click to download your file now**.
7. If you receive an error message, click on the message, install Active X, and continue with the download.
8. When the security warning displays, click **Install**.

    When the install is complete, PLDS displays the downloads again with a checkmark next to the downloads which have been completed successfully.

Adding a host

You can define a brand new License host to activate entitlements on this License host.

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

Searching for a host

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

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 except at the beginning. If you enter %ho as the search criteria, the page displays an error.

2. Click **Search License Hosts**.

Appendix B: Distributed third party software

Package name	Version	License type	License URL
jinja	1.2	Jinja 1.2 License	http://jinja.pocoo.org/1/
pgAdmin	III	pgAdmin III License	http://www.pgadmin.org/download/
Hudson	1.255	MIT License	https://hudson.dev.java.net/servlets/ProjectDocumentList
sphinx	0.4.3	BSD	http://pypi.python.org/pypi/Sphinx
jMock	2.5.1	jMock Project License	http://www.jmock.org/download.html
junit	4.5	Common Public License Version 1.0	http://sourceforge.net/project/showfiles.php?group_id=15278&package_id=12472
Silk Icons	1.3	Creative Commons Attribution 2.5 License	http://www.famfamfam.com/lab/icons/silk&/
Pygments	0.11	BSD	http://pygments.org/download/
simpleJSON	2.0.5	MIT License	http://pypi.python.org/pypi/simplejson
Docutils	0.5	DocUtils 0.5 License	http://docutils.sourceforge.net/
H2 Database Engine	1.1	H2 License	http://www.h2database.com/html/download.html
cygwin	1.5	GNU GPL	http://cygwin.com/
jython	2.5	Jython License	http://www.jython.org/Project/download.html
cobertura	1.9	GNU GPL	http://cobertura.sourceforge.net/download.html
Apache Commons	*	Apache License	http://commons.apache.org/
Mylyn	3.1	Eclipse Public License	http://www.eclipse.org/mylyn/downloads/
Apache Wicket	1.4	Apache License	http://wicket.apache.org/getting-wicket.html
Java SE	1.6.0	Sun License	http://java.sun.com/javase/downloads/index.jsp

Package name	Version	License type	License URL
JBoss EAP	*	GPL	http://www.jboss.com/downloads/
GUICE	1	Apache License	http://code.google.com/p/google-guice/
Apache Log4J	1.2	Apache License	http://logging.apache.org/log4j/1.2/index.html
PostgreSQL	8.2	BSD	http://www.postgresql.org/
CSSHover	3	LGPL	http://www.xs4all.nl/~peterned/csshover.htm
Checkstyle	5	LGPL	http://checkstyle.sourceforge.net/
Eclipse IDE	3.4	Eclipse Public License	http://www.eclipse.org/
Slf4J	1.5.3	SLF4J 1.5.3 License	http://www.slf4j.org/
hibernate	3.4	LGPL	https://www.hibernate.org
FindBugs	1.3.8	LGPL	http://findbugs.sourceforge.net/downloads.html
Apache Ivy	2	Apache License	http://ant.apache.org/ivy/download.cgi
Apache Ant	1.7.0	Apache License	http://ant.apache.org/
EclEmma	1.4.1	Eclipse Public License	http://www.eclemma.org/installation.html
Spring Framework		Apache License	http://www.apache.org/licenses/LICENSE-2.0

Index