Single Sign-On Configuration

July 2, 2014

Introduction

Cisco Unified Presence Release 8.6(4) and later supports Single Sign-On (SSO). SSO allows system administrators to log in to a Windows client machine on a Windows domain and use the following Cisco Unified Presence applications without being required to sign in again:

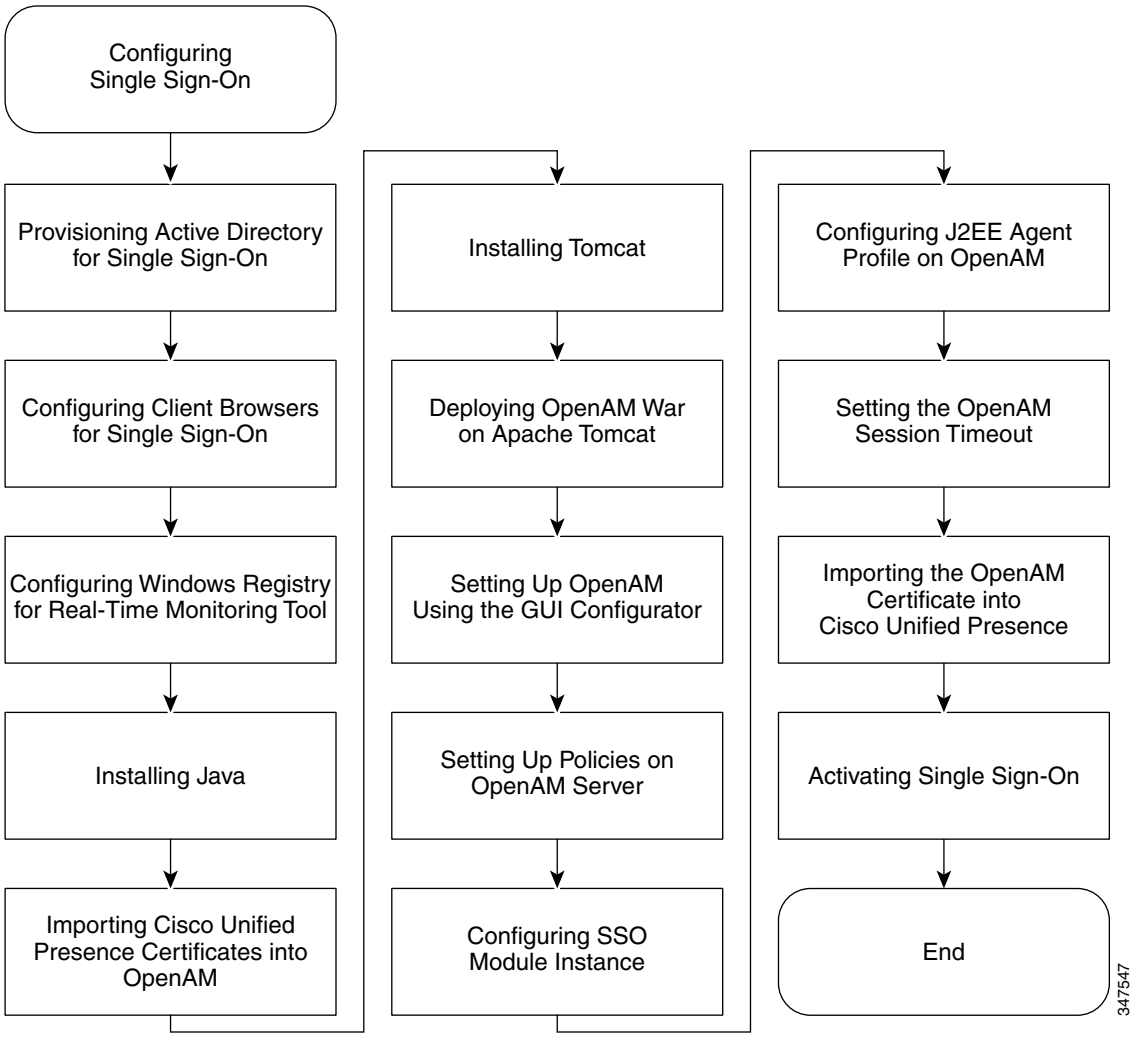
- Cisco Unified Presence User Options
- Cisco Unified Presence Administration
- Cisco Unified Serviceability
- Cisco Unified Reporting
- Disaster Recovery System
- Real-Time Monitoring Tool (RTMT) Administration
- Cisco Unified Operating System Administration
- Cisco UP Client Profile Agent - This option is only available in Cisco Unified Presence Release 8.6(5) and later and is only applicable to customers using Common Access Card (CAC) sign-on.

Task Flow for Single Sign-On Configuration

The following figure provides the sequence of tasks that are required to successfully configure SSO. Cisco recommends that you complete each task outlined in this flow in the order indicated, unless otherwise indicated. The following tasks are optional and do not fall within this task flow:

- Disable Single Sign-On, page 16-29
- Uninstall OpenAM, page 16-31
- Set the Debug Level, page 16-32

Figure 16-1 Task flow for Configuring Single Sign-On



System Requirements

The Single Sign-On (SSO) feature makes use of a third-party application from ForgeRock called OpenAM. Support for the OpenAM application is available only from ForgeRock. This section of the document outlines the software requirements and configuration guidelines to enable the SSO feature to work with OpenAM. This document describes the installation of OpenAM on a Windows Server environments.

Advanced OpenAM configurations such as deploying OpenAM behind load balancers or the use of session replication between OpenAM servers has not been validated. For information about these advanced features, see http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf.

The SSO feature requires the following third-party applications:

- Microsoft Windows Server 2008 R2
- Microsoft Active Directory
- ForgeRock Open Access Manager (OpenAM) Version 9.0

Note The SSO feature uses Active Directory and OpenAM in combination to provide SSO access to web-based client applications.

These third-party products must meet the following configuration requirements:

- Active Directory must be deployed in a Windows domain-based network configuration, not just as an LDAP server.
- The OpenAM server must be accessible on the network to all client systems and the Active Directory server.
- The Active Directory (Domain Controller) server, Windows clients, Cisco Unified Presence, and OpenAM must be in the same domain.
- DNS must be enabled in the domain.
- The clocks of all the entities that are participating in SSO must be synchronized.

See the third-party product documentation for more information about those products.

The following table provides a list of the software applications and versions that were used and tested in the procedures that appear in this chapter. In order for you to receive Cisco support, Cisco recommends that you adhere to these suggested requirements during your configuration.

Table 16-1 Software Versions

Component	Version
Active Directory	Windows Server 2008 R2 Enterprise
Desktop Operating System for end user clients	Windows 7 Professional (SP1)
Open Access Manager (OpenAM)	OpenAM Release 9.0: http://www.forgerock.org/downloads/openam_release9_20100207.zip For more information: https://wikis.forgerock.org/confluence/display/openam/OpenAM+Snapshot+9+Release+Notes
OpenAM underlying Operating System	Windows Server 2008 R2 Enterprise
Apache Tomcat on which OpenAM is loaded	Tomcat 6.0.2.0, Tomcat 7.0.29 http://archive.apache.org/dist/tomcat/tomcat-7/v7.0.29/bin
Java Development Kit (JDK) of OpenAM underlying Operating System	JDK 7 Update 3
Web browser	Internet Explorer 8, 9 and Mozilla Firefox 10, 11

Before You Begin

To help ensure that the configuration of SSO runs as smoothly as possible, Cisco recommends that you gather the following information before you configure SSO:

- Ensure that the installed base operating system (such as Windows server) for the OpenAM system is running.
- Make a note of the Fully Qualified Domain Name (FQDN) of the Windows Active Directory (AD) server to which the OpenAM will be integrating.
- Make a note of the FQDN of the Windows server on which OpenAM is to be installed.
- Ensure that the Cisco Unified Presence Web Application timeout is set consistently across all Cisco Unified Presence nodes in the cluster and make note of that timeout value. You can use the Cisco Unified Presence Administration CLI to verify the timeout value by entering the following command: `show webapp session timeout`. For more information, see the *Command Line Interface Reference Guide for Cisco Unified Presence Release 8,0, 8.5, and 8.6*.
- Ensure that Cisco Unified Communications Manager has been configured to sync users from Active Directory (AD) using "sAMAccountName" as the LDAP Attribute for User ID. For more information, see the "DirSync Service" section in the *Cisco Unified Communications Manager System Guide.*

Single Sign-On Configuration

Provision Active Directory for Single Sign-On

Prerequisite

Ensure that you have Windows Server 2008 support tools installed. Support tools are installed on Windows Server 2008 by default.

Procedure

Step 1 Log in to the Active Directory (AD) server.

Step 2 From the **Start** menu, choose **All Programs > Administration Tools > Active Directory Users and Computers**.

Step 3 Right-click **Users** and choose **New > User.**

Step 4 In the **User logon name** field, enter the OpenAM server hostname.

Note The OpenAM server hostname should not include the domain name.

Step 5 Click **Next**.

Step 6 Enter and confirm a password.

This password is required in Step 10.

Step 7 Uncheck the **User must change password at next login** check box.

Step 8 Click **Next**.

Step 9 Click **Finish** to finish creating the new user account.

Step 10 Create a keytab file on the AD server using the following command from the command prompt.

```
ktpass -princ HTTP/<hostname>.<domainname>@<DCDOMAIN> -pass
<password> -mapuser <userName> -out <hostname>.HTTP.keytab -ptype
KRB5_NT_PRINCIPAL -target <DCDOMAIN>
```

Value	Description	Example
hostname	The hostname (not the FQDN) of your OpenAM server	server1
domainname	The AD domain name	cisco.com
DCDOMAIN	The AD domain name, entered in block capitals	CISCO.COM
password	The password value that was specified when you created the user account for the OpenAM server earlier in this procedure.	
userName	The AD account name entered in Step 4; this value should be the OpenAM server hostname	server1

Example:

```
ktpass -princ HTTP/server1.cisco.com@CISCO.COM -pass cisco!123
-mapuser server1 -out server1.HTTP.keytab -ptype KRB5_NT_PRINCIPAL
-target CISCO.COM
```

Note Make a note of the *-princ* value for later procedures.

Step 11 After successful creation of the keytab file, copy the keytab file to a location on the OpenAM server; this path will later be specified in OpenAM configuration. Create a directory under C:\> and copy the above keytab file. For example, “C:/keytab/server1.HTTP.keytab”.

Client Browser Configuration for Single Sign-On

To use SSO for a browser-based client application, you must configure the web browser.

The following sections describe how to configure client browsers to use SSO:

- Configure Internet Explorer for Single Sign-On, page 16-5
- Configure Firefox for Single Sign-On, page 16-7

Configure Internet Explorer for Single Sign-On

The SSO feature supports Windows clients running Internet Explorer. Perform the following procedure to configure Internet Explorer to use SSO.

Note For a list of web browsers and supported versions, see Table 16-1.

Procedure

Step 1 Choose **Tools > Internet Options > Advanced** tab.

Step 2 Check **Enable Integration Windows Authentication**.

Step 3 Click **OK** to save the changes.

Step 4 Restart Internet Explorer.

Step 5 Choose **Tools > Internet Options > Security > Local Intranet** and click **Custom Level**.

Step 6 Under **User Authentication**, check **Automatic Logon Only in Intranet Zone**.

Step 7 Click **OK**.

Step 8 Click **Sites**.

Step 9 Check **Automatically detect intranet network**.

Step 10 Click **Advanced**.

Step 11 Fill in the **Add this website to the zone** field with the FQDN of the OpenAM server using the following format: https://OpenAM_FQDN.

Step 12 Click **Add**.

Step 13 Click **Close**.

Step 14 Click **OK**.

Step 15 Uncheck **Enable Protected Mode**.

Step 16 Click **Apply**.

Step 17 Click **OK**.

Step 18 Restart Internet Explorer.

Step 19 Open the Windows Registry Editor:

- For Windows XP or Windows 2008 - Choose **Start > Run** and type *regedit*.
- For Windows Vista and Windows 7.0 - Choose **Start** and type *regedit*. For Windows Vista, you must click **Continue**.

Step 20 Under registry key *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA*, right-click and choose New > DWORD (32-bit) value and rename it to be *SuppressExtendedProtection.*

Step 21 Right-click on the newly created DWORD, choose **Modify**.

Note Only an administrator can set the DWORD.

Step 22 Set the following values:

- Base: hexadecimal
- Value data: 002

Note The newly created DWORD will appear in the LSA directory list as follows:
Name: SuppressExtendedProtection
Type: REG_DWORD
Value: 0x00000002 (2)

Configure Firefox for Single Sign-On

The SSO feature supports Windows clients that are running Firefox.

Note For a list of web browsers and supported versions, see Table 16-1.

Procedure

Step 1 Open Firefox and enter the following URL page: **about:config**.

Step 2 Scroll down to **network.negotiate-auth.trusted-uris**.

Step 3 Right-click the Preference Name **network.negotiate-auth.trusted-uris**, and choose **Modify**.

Step 4 Set the string value to your domain (for example, cisco.com).

Step 5 Click **OK**.

Windows Registry Configuration for Real-Time Monitoring Tool

Configuring SSO for the Real-Time Monitoring Tool (RTMT) is optional. To achieve this configuration, you must create the following new registry key on your Desktop client (Windows XP or Windows 7).

Note An administrator must set the `allowtgtsessionkey` registry key entry for the Desktop client.

Procedure

Step 1 Go to either of the following locations, depending on your operating system:

- Windows XP: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos
- Windows Vista/Windows 7: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters

Step 2 Right-click the folder, choose **New > DWORD (32-bit) Value**, and rename it to be *allowtgtsessionkey.*

Step 3 Right-click the newly created registry key and choose **Modify**.

Step 4 In the **Value data:** field, enter *1*.

Install Java

OpenAM requires a Java Runtime Environment (JRE) to operate. The following procedure provides details for installing the JRE on your Windows server, forming the OpenAM base system.

Procedure

Step 1 Go to http://www.oracle.com/technetwork/java/archive-139210.html.

Step 2 Download the recommended version of the JDK installation file by choosing the executable file that corresponds to your server architecture (Windows x86 or Windows x64).

Note See Table 16-1 for a list of the recommended versions of software.

Step 3 Double-click the downloaded file to begin the installation of the JDK and accept the default values provided in the Installation wizard.

Note Make a note of the installation directory. This value indicates the location of the Java JRE and can be used to infer the JDK directory path. Example values may be as follows, depending on the JDK values that are used:

```
jre-path=C:\Program Files\Java\jre7
jdk-path=C:\Program Files\Java\jdk1.7.0_03
```

Step 4 A Java keystore and the associated security certificates are required to facilitate secure connections to the OpenAM server, which runs on Apache Tomcat. Choose one of the following options:

- If you use a self-signed security certificate for OpenAM/Tomcat, proceed to Step 5.
- If you use a Certificate Authority (CA) signed security certificate for OpenAM/Tomcat, proceed to Step 11.

Step 5 Create the Java keystore by opening a Windows command prompt on the Windows Server, and executing the following command:

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -genkey -alias
tomcat -keyalg RSA -validity 1825 -keystore C:\keystore -ext
BC:c=ca:true
```

This command creates the Java keystore file at the following location: C:\keystore.
The keytool command is located in the <jdk-path>/bin directory, the exact path to the keytool command in the preceding command may vary depending on the JDK version used. For information about the keytool command, see http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html.

Note The keytool command with -ext option requires JDK 7. Using the -ext option with the above value results in an OpenAM/Tomcat certificate with the CA flag set to True. The CA flag must be set to True or the Cisco Unified Presence Operating System Administration interface may fail to upload the certificate into the tomcat-trust trust store. For more information, see Import the OpenAM Certificate into Cisco Unified Presence, page 16-25.

Step 6 When you are prompted for a keystore password, enter a valid keystore password. For example, “cisco!123”. Make a note of the keystore password as it is required to access the keystore.

Note Do not use example values on the production server; Use a unique password value for the keystore. This password will be visible in plain text in the Apache Tomcat configuration files and utilities.

Step 7 When you are prompted to enter the first name and last name, enter the FQDN (hostname.domainname) of the OpenAM server.
You also are prompted to enter your organization unit name, organization name, city or locality, state or province, and two-letter country code.

Step 8 When you are prompted for a Tomcat password, press RETURN to use the same keystore password value for the Tomcat private key. The Java keystore is created at the location specified in the keytool command. For example, C:\keystore.

Step 9 You can view the Tomcat certificate in the keystore using the following command:

Example:

```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -list -v
-alias tomcat -keystore C:\keystore
```

Step 10 *If you chose to use a self-signed security certificate for Tomcat, proceed to the end of this procedure and consider this task complete.*

Step 11 Create a Java keystore to store Certificate Authority (CA)-signed security certificates for OpenAM/Tomcat. Open a command prompt on the Windows Server and execute the following command:

Example:

```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -genkey -alias
tomcat -keyalg RSA -validity 1825 -keystore C:\keystore
```

This command creates the Java keystore file at the following location: C:\keystore.
The keytool command is located in the <jdk-path>/bin directory, the exact path to the keytool command in the example provided above may vary depending on the JDK version used. For information about the keytool command, see http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html.

Step 12 When you are prompted for a keystore password, enter a valid keystore password. For example, “cisco!123”. Make a note of the keystore password as it is required to access the keystore.

Note Do not use example values on the production server; Use a unique password value for the keystore. This password will be visible in plain text in the Apache Tomcat configuration files and utilities.

Step 13 When you are prompted to enter first name and last name, enter the FQDN (hostname.domainname) of your OpenAM server.
You also are prompted to enter your organization unit name, organization name, city or locality, state or province, and two-letter country code

Step 14 When you are prompted for a Tomcat password, press RETURN to use the same keystore password value for the Tomcat private key. The Java keystore is created at the location specified in the keytool command. For example, C:\keystore.

Step 15 You can view the Tomcat certificate in the keystore using the following command:

Example:

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -list -v
-alias tomcat -keystore C:\keystore
```

Step 16 Generate a certificate signing request (CSR) for this OpenAM/Tomcat instance. Open a command prompt on the Windows Server and execute the following command:

Example:

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -certreq
-keyalg RSA -alias tomcat -file certreq.csr -keystore C:\keystore
```

Note This command creates the CSR and writes it to a file called **certreq.csr**.

Step 17 Submit the CSR to your CA, request the CA to sign the CSR and create a certificate. Obtain and copy the following certificates to the Windows Server that is going to be the OpenAM server:

- CA signing or root certificate
- Intermediate signing certificates (if applicable)
- Newly signed OpenAM/Tomcat certificate

Note Refer to the CA documentation for instructions about completing these tasks.

Step 18 Import the CA signing or root certificate into the Java keystore that was created in Step 11. Open a command prompt on the Windows Server and execute the following command, answering “yes” to the prompt, “Trust this certificate?”:

Example:

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -import -alias
root -trustcacerts -file <filename_of_the_CA_root_certificate>
-keystore C:\keystore
```

Step 19 You can view the CA signing certificate in the keystore using the following command:

Example:

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -list -v
-alias root -keystore C:\keystore
```

Step 20 Import any other intermediate signing certificates (if applicable) into the Java keystore that was created in Step 11. Open a command prompt on the Windows Server and execute the following command, answering “yes” to the prompt, “Trust this certificate?”:

Example:

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -import -alias
inter01 -trustcacerts -file
<filepath_of_the_intermediate_signing_certificate> -keystore
C:\keystore
```

Note The -alias option must be updated with a value unique to the Java keystore, otherwise the import operation will result in an error similar to the following: “Certificate not imported, alias<inter01> already exists.”

Step 21 You can view any of the intermediate signing certificates in the keystore using the following command:

Example:

```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -list -v
-alias inter01 C:\keystore
```

Note The -alias option must be updated with the corresponding alias value for the intermediate certificates you wish to view. The above example uses a sample alias value of “inter01”.

Step 22 Import the newly signed certificate OpenAM/Tomcat certificate into the Java keystore that was created in Step 11. Open a command prompt on the Windows Server and execute the following command:

Example:

```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -import -alias
tomcat -file <new_certificate_filepath> -keystore C:\keystore
```

Step 23 You can view the new OpenAM/Tomcat certificate in the keystore using the following command:

Example:

```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -list -v
-alias tomcat -keystore C:\keystore
```

Note The issuer of this new Tomcat certificate is the CA or one of the intermediate CAs (if applicable).

Import Cisco Unified Presence Certificates into OpenAM

OpenAM must communicate with a J2EE Agent component that exists on each Cisco Unified Presence node for which SSO is enabled. This communication is over an encrypted channel and therefore the necessary security certificates must be imported onto OpenAM.

The OpenAM server must trust the security certificate presented by each Cisco Unified Presence node for the encrypted communication channel to be established. OpenAM trusts a security certificate by importing the required security certificates into the OpenAM keystore. A given Cisco Unified Presence node can present one of two types of security certificate:

- Self-signed certificate
- CA-signed certificate

Note The Cisco Unified Presence tomcat certificate and tomcat-trust trust store contain the security certificates of interest for secure communication with OpenAM. The other Cisco Unified Presence certificates and associated trust stores are not relevant for SSO (for example, cup, cup-xmpp, cup-xmpp-s2s or ipsec).

If your SSO-enabled Cisco Unified Presence deployment is configured to use self-signed certificates, each of the self-signed certificates must be imported into OpenAM.

If your SSO-enabled Cisco Unified Presence deployment is configured to use CA-signed certificates, the CA root certificate and any associated intermediate certificates must be imported into OpenAM. If you are also using a CA-signed certificate for your OpenAM/Tomcat instance, the required CA root and intermediate certificates may already be imported into the OpenAM keystore.

This procedure provides the details on how to identify the type of security certificate being used by the Cisco Unified Presence node and how to import the certificates into the OpenAM keystore that was created in Install Java, page 16-8.

Procedure

Step 1 Sign in to Cisco Unified Presence Operating System Administration for a given Cisco Unified Presence node for which SSO is to be enabled.

Step 2 Choose **Security > Certificate Management**.

Step 3 Click **Find**.

Step 4 Locate the entry with **Certificate Name** of **tomcat**.

Step 5 Examine the Description column of the tomcat certificate.

Step 6 If the description states that the tomcat certificate is **Self-signed certificate generated by system**, this indicates that the Cisco Unified Presence node is using a self-signed certificate. If this description is not present, a CA-signed certificate can be assumed.

- If the certificate is self-signed, proceed to Step 7.
- If the certificate is CA-signed, proceed to Step 13.

Step 7 Choose the **tomcat.pem** link.

Step 8 Click **Download** to download the tomcat.pem file.

Step 9 Copy the **tomcat.pem** file to the OpenAM server.

Step 10 Import the **tomcat.pem** file into the keystore (created in Install Java, page 16-8) on the OpenAM server as a trusted certificate. Open a command prompt on the Windows server (OpenAM) and execute the following command, updating the command with the values for your keytool command path and keystore location as applicable for your environment, and answer “yes” to the prompt “Trust this certificate?”:

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keystool.exe" -import
-alias cup01 -trustcacerts -file <full_filepath_of_the_tomcat.pem>
-keystore C:\keystore
```

Note The -alias option must be updated with a value unique to the Java keystore, otherwise the import operation will result in an error similar to the following: “Certificate not imported, alias <cup01> already exists.”

Step 11 You can view the **tomcat.pem** in the keystore using the following command, updating the command with the values for your keytool command path and keystore location as applicable for your environment:

```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keystool.exe -list -v
-alias cup01 -keystore C:\keystore
```

Note The -alias option must match the value used in Step 10, otherwise the keystore entry may not be found.

Step 12 Skip to Step 16.

Step 13 Identify the CA root certificates and any intermediate certificates that were used to sign your Cisco Unified Presence Tomcat certificate. Download the required certificates (CA root certificates and any intermediate certificates) from your CA to your OpenAM server.

Step 14 Import these certificates into the keystore on the OpenAM server as trusted certificates. Open a command prompt on the Windows server (OpenAM) and execute the following command for *each* downloaded certificate, updating the command with the values for your keytool command path and keystore location as applicable for your environment, and answer "yes" to the prompt "Trust this certificate?".

```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -import -alias
root_ca -trustcacerts -file <full_filepath_of_the_certificate>
-keystore C:\keystore
```

Note The -alias option must be updated with a value unique to the Java keystore, otherwise the import operation will result in an error similar to the following: "Certificate not imported, alias <root_ca> already exists."

Step 15 You can view the certificate in the keystore using the following command, updating the command with the values for your keytool command path and keystore location as applicable for your environment:

```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keystool.exe -list -v
-alias root_ca -keystore C:\keystore
```

Note The -alias option must match the value used in Step 14, otherwise the keystore entry may not be found.

Step 16 Repeat this procedure for each Cisco Unified Presence node for which SSO is to be enabled.

Note In the case of CA-signed certificates used on the Cisco Unified Presence node, it is not necessary to import the same CA and/or intermediate certificate into the OpenAM keystore more than once. If you find that a Cisco Unified Presence node has been signed by the same CA and/or intermediate certificate, there is no need to import those certificates into the OpenAM keystore again.

Install Tomcat

OpenAM requires that the Apache Tomcat Web Container be installed on the OpenAM Windows server base system. This procedure provides details on how to install Apache Tomcat on the OpenAM Windows server base system. See the following table for descriptions of the variables referred to in this procedure.

Table 16-2 Variable Descriptions

Variable	Description
<certstore-path>	The file path to the Java keystore used by Java applications and Apache Tomcat. Trusted server public certificates are stored in this keystore. See Steps 5 or 11 of Install Java, page 16-8 to determine the file path for the Java keystore.
<certstore-password>	The password used to access the Java keystore located at <certstore-path>. See Step 6 or 12 of Install Java, page 16-8 to determine the value used for the Java keystore password.

Procedure

Step 1 Download the recommended version of Apache Tomcat to your Windows server that forms the OpenAM base system.

Note See Table 16-1 for a list of the recommended versions of software.

Note Download the 32bit/64bit Windows Service Installer executable file.

Step 2 Double-click the downloaded file to begin the installation of Apache Tomcat.

Step 3 From the Apache Tomcat Setup wizard, click **Next**.

Step 4 In the **License Agreement** dialog box, click **I Agree**.

Step 5 In the **Choose Components** dialog box, Click **Minimum** as the type of install and click **Next**.

Step 6 In the **Configuration** dialog box, accept the default settings and click **Next**.

Step 7 In the **Java Virtual Machine** dialog box, ensure the installed JRE path is set to the value of **jre-path**. See Step 3 of Install Java, page 16-8.

Note If you are using the recommended version of Java, the path will display by default. If you are not using the recommended version of Java, ensure that the path chosen reflects the path chosen in Step 3 of Install Java, page 16-8.

Step 8 Click **Next**.

Step 9 In the **Choose Install Location** dialog box, accept the default settings and click **Install**. Note the Tomcat install location, because it is required later.

Note The installation location is referred to as **tomcat-dir** later in this procedure.

Step 10 Click **Finish**.

Step 11 Configure Apache Tomcat to start automatically:

a. Choose **Start > All Programs > Apache Tomcat 7.0 Tomcat7 > Configure Tomcat**.

b. From the **General** tab, set the **Startup type** as **Automatic**.

c. Click **Apply**.

d. Click **OK**.

Step 12 Configure the Apache Tomcat runtime parameters:

a. Choose **Start > All Programs > Apache Tomcat 7.0 Tomcat7 > Configure Tomcat**.

b. From the **Java** tab, add the following Java options:

```
-Djavax.net.ssl.trustStore=<certstore-path>
-Djavax.net.ssl.trustStorePassword=<certstore-password>
-XX:MaxPermSize=256m
```

Note See Table 16-2 for descriptions of the above variables.

Example:

```
-Djavax.net.ssl.trustStore=C:\keystore
-Djavax.net.ssl.trustStorePassword=cisco!123
-XX:MaxPermSize=256m
```

c. Set the **Initial memory pool** to 512.

d. Set the **Maximum memory pool** to 1024.

e. Click **Apply**.

f. Click **OK**.

Step 13 Using a Text Editor, open the server.xml file under <tomcat-dir>\conf folder. See Step 9 to determine the value for <tomcat-dir>. An example value is `"C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf"`.

Step 14 Comment out the 8080 connector port. Enter the code as follows:

Example:

```
<!-- <Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" /> -->
```

Step 15 Uncomment the 8443 connector port; Remove <!-- code at the beginning and --> at the end of the 8443 connector. You must add three more attributes to the connector configuration:

- keystoreFile (location of the keystore file that was created in section Install Java, page 16-8. In this example, it was created under C:\keystore)
- keystorePass
- keystoreType

Enter the code as follows:

Example:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="<certstore-path>"
keystorePass="<certstore-password>"
keystoreType"JKS"/>
```

Note See Table 16-2 for descriptions of the above variables.

Step 16 Save the server.xml file.

Step 17 Start the Tomcat service:

a. Choose **Start > All Programs > Apache Tomcat 7.0 Tomcat7 > Configure Tomcat**.

b. From the **General** tab, click **Start**. If the Tomcat service was already running, click **Stop**, then **Start**.

Step 18 To test the configuration, launch a web browser on the Windows Server that contains the Tomcat instance and go to https://localhost:8443/tomcat.gif. The web browser may present warning dialogs about insecure connections because the web browser does not trust the security certificates that are presented by the Tomcat instance. Either examine the certificates and add them to your local certificate store so that the browser trusts them or proceed to the web application (less secure option) using the available browser controls. If the configuration is correct, the Tomcat logo appears in the web browser window.

Step 19 Configure Windows firewall to allow incoming connections to Apache Tomcat:

a. Choose **Start > Administrative Tools > Windows Firewall and Advanced Security**.

b. Choose **Windows Firewall and Advanced Security > Inbound Rules**.

c. Right-click **Inbound Rules**.

d. Click **New Rule**.

e. From the **What type of rule would you like to create** list of options, choose **Port**.

f. Click **Next**.

g. From the **Does this rule apply to TCP or UDP?** list of options, choose **TCP**.

h. From the **Does this rule apply to all local ports or specific local ports?** list of options, choose **Specific local ports**.

i. Enter 8443 and click **Next**.

j. From the **What action should be taken when a connection matches the specified conditions?** list of options, choose **Allow the connection**.

k. Click **Next**.

l. From the **When does the rule apply?** list of options, choose **Domain** only.

m. Click **Next**.

n. Enter a name and description of your choosing and click **Finish**.

Step 20 To test the configuration, log in to another host on the network, launch a web browser on the Windows server that contains the Tomcat instance and go to https://<openam-fqdn>:8443/tomcat.gif, where <openam-fqdn> is the Fully Qualified Domain Name of the Windows Server that contains the Tomcat instance. The web browser may present warning dialogs about insecure connections because the web browser does not trust the security certificates that are presented by the Tomcat instance. Either examine the certificates and add them to your local certificate store so that the browser trusts them or proceed to the web application anyway (this is less secure) using the available browser controls. If the configuration is correct, the Tomcat logo appears loaded into the web browser window.

Deploy OpenAM War on Apache Tomcat

Procedure

Step 1 Download the recommended OpenAM release from the ForgeRock website, as indicated in Table 16-1Software Versions, page 16-3.

Step 2 Extract the .zip file and locate the opensso.war file that is contained within it.

Step 3 Copy the WAR file to the Windows server that is to be your OpenAM server. This Windows server should be running the previously configured Tomcat service.

Step 4 Stop the Apache Tomcat service if it is running:

a. Choose **Start > All Programs > Apache Tomcat 7.0 Tomcat7 > Configure Tomcat**.

b. From the **General** tab, click **Stop**.

Step 5 Deploy the WAR file on the Windows server that contains the Tomcat instance by copying the WAR file to the following location: <tomcat-dir>\webapps. See Install Tomcat, page 16-13 for a description of the <tomcat-dir> variable.

Example:

```
C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps
```

Step 6 Start the Apache Tomcat service:

a. Choose **Start > All Programs > Apache Tomcat 7.0 Tomcat7 > Configure Tomcat**.

b. From the **General** tab, click **Start**.

Note The WAR file will fully deploy within a couple minutes. Under the webapps folder, a new folder is created with the same name as the WAR file but with the .war extension removed.

Step 7 Verify your configuration by launching a web browser and entering https://<openam-fqdn>:8443/<war-file-name>, where <openam-fqdn> is the FQDN of the Windows server that contains the OpenAM/Tomcat instance and <war-file-name> is the name of the OpenAM WAR file with the .war extension removed. If the configuration is correct, the OpenAM administration interface should load in the web browser window.

Set up OpenAM using the GUI Configurator

The following procedure specifies a method of configuring OpenAM. If you have an existing OpenAM server or a solid understanding of OpenAM, you can configure the server differently.

OpenAM server and J2EE Policy Agents require FQDNs for the hostname of the machines on which you will perform your installations. To avoid problems with installation, configuration, and usage, Cisco highly recommends that you avoid using hostnames like “localhost” or numeric IP addresses like “192.168.1.2”.

OpenAM provides a web-based administration interface that must be accessed using a web browser, for example Mozilla Firefox. When accessing OpenAM for the first time, you must use the FQDN of the OpenAM server in the URL, for example, https://server1.cisco.com:8443/opensso, where the sample URL value assumes that the OpenAM WAR file is deployed as “opensso”.

OpenAM configuration and logging information is typically stored in two directories that can be found in the home directory of the user running the OpenAM/Tomcat instance, for example:

- `C:\opensso` (where the folder name matches the deployed URI for the OpenAM WAR file. For example, opensso.)
- `C:\.openssocfg`

If a problem occurs during the configuration, the Configurator displays an error message. If possible, correct the error and retry the configuration. The following log file directories may provide useful information:

- Tomcat Web Container logs: `tomcat-dir\logs`
- OpenAM Install log: `C:\opensso` (where the folder name matches the deployed URI for the OpenAM WAR file. For example, opensso.)

By default, OpenAM is deployed under C:\opensso on Windows platforms.

Procedure

Step 1 Open the web browser and navigate to the OpenAM server using the following URL: https://<fqdn of openam server>:8443/<WAR filename>.

Example:

https://server1.cisco.com:8443/opensso

Note When you access OpenAM for the first time, you are directed to the Configurator to perform the initial configuration of the OpenAM. The Configuration Options window appears when you access the OpenAM for the first time.

Step 2 Choose **Create Default Configuration**.

Note If you encounter an error, repeating steps 1 and 2 on your local machine. Windows 2008, for example, may not trust this site, even if it is listed as a trusted sites.

Step 3 In the **OpenSSO Configurator** window, specify and confirm passwords for the OpenAM administrator (amAdmin) and the default policy agent user (UrlAccessAgent). The default policy agent user is not used later in this example configuration; amAdmin is used each time you log in to OpenAM to change the configuration.

Step 4 Click **Create Configuration**.

You are notified when the configuration is complete.

Step 5 Click **Proceed to Login**.

Step 6 Log in to your deployed OpenAM web application using the previously configured username and password for “amAdmin”.

Step 7 From the **Access Control** tab, click **/(Top Level Realm)**.

Step 8 From the **Authentication tab,** click **Core**.

Step 9 Click **All Core Settings**.

Step 10 Set the **User Profile** to **Ignored**.

Step 11 Click **Save** to update the profile.

Step 12 Log out of the OpenAM GUI.

Set up Policies on OpenAM Server

Set up policies on the OpenAM server using the policy rules detailed in the following table.

Table 16-3 Policy Rules

Service Type	Name	Resource Name	Action
URL Policy Agent (with resource name)	<hostname>-01	https://<CUP FQDN>/*	Enable GET, Value = Allow Enable POST , Value = Allow
	<hostname>-02	https://<CUP FQDN>/*?*	
	<hostname>-03	https://<CUP FQDN>/*?*?*	
	<hostname>-04	https://<CUP FQDN>:8443/*	
	<hostname>-05	https://<CUP FQDN>:8443/*?*	
	<hostname>-06	https://<CUP FQDN>:8443/*?*?*	

When you apply the policy rules as defined in this procedure, the Cisco Unified Presence Administration/User interfaces can only be accessed with the web browser using the following URL formats:

- https://<CUP FQDN> - For example, https://CUP-Node-01.cisco.com
- https://<CUP FQDN>:8443 - For example https://CUP-Node-01.cisco.com:8443/

It is *not* possible to access the Cisco Unified Presence Administration/User interface using a URL that only specifies a hostname such as https://<CUP HOSTNAME> (for example, https://CUP-Node-01/).

Procedure

Step 1 Log in to the OpenAM Administration interface using the credentials you specified in section Set up OpenAM using the GUI Configurator, page 16-17.

Step 2 From the **Access Control** tab, click **/ (Top Level Realm)**.

Step 3 From the **Policies** tab, click **New Policy**.

Step 4 In the **Name** field, enter the PolicyName (for example, CUPPolicy) and click **OK**.

CUPPolicy is only a suggested value. You can use any valid name value. This value is not required later in this configuration.

Step 5 Choose the new policy, CUPPolicy, for editing.

Step 6 Click **Rules**.

Step 7 Add the rules in the following order:

a. Under the **Rules** section, click **New**.

b. Choose **Service Type** as **URL Policy Agent (with resource name)**.

c. Click **Next**.

d. In the **Name** field, enter the suggested rule Name from Table 16-3Policy Rules, page 16-19, replacing <hostname> with the actual hostname of the Cisco Unified Presence node.

e. In the **ResourceName** field provided, enter the corresponding Resource Name for this rule, replacing <CUP FQDN> with the actual Fully Qualified Domain Name of the Cisco Unified Presence node.

f. Check the **GET** action with a value of **Allow**.

g. Check the **POST** action with a value of **Allow**.

h. Click **Finish** to complete the rule update.

i. Click **Save** to save the policy update.

j. Repeat this entire step for each rule in Table 16-3Policy Rules, page 16-19 then click **Finish**.

You must add this set of six rules for each Cisco Unified Presence node that is enabled for SSO.

Step 8 You must add a single Subject to the policy. Add the Subject as follows:

a. Under the **Subjects** section, click **New**.

b. Choose **Authenticated Users** as Subject Type.

c. Click **Next**.

d. Enter CUPSubject as the **Name** value.
CUPSubject is only a suggested value. You can use any valid value. This value is not required later in this configuration.

e. Click **Finish** to complete the Subject update.

f. Click **Save** to save the policy update.

Only a single Subject is required for this policy even if multiple Cisco Unified Presence nodes are enabled for SSO.

Step 9 You must add a single Condition to the policy. Add the Condition as follows:

a. Under the **Conditions** section, click **New**.

b. Choose **Active Session Time** as Condition Type.

c. Click **Next**.

d. Enter CUPTimeOutCondition as the **Name** value.
CUPTimeOutCondition is only a suggested value. You can use any valid name value. This value required later in this configuration.

e. Enter 120 as the **Maximum Session Time (minutes)**.

f. Ensure the **Terminate Session** field is set to **No**.

g. Click **Finish** to complete the Subject update.

h. Click **Save** to save the policy update.

Note that only a single Condition is required for this policy, even if multiple Cisco Unified Presence nodes are enabled for SSO.

Configure Single Sign-On Module Instance

This single module instance can be shared by multiple Cisco Unified Presence nodes that are configured for SSO as long as the same Active Directory domain is used throughout the deployment. Deployment scenarios involving more than one Active Directory domain are not covered in this documentation.

Procedure

Step 1 Log in to the OpenAM administration interface using the credentials you specified in Set up OpenAM using the GUI Configurator, page 16-17.

Step 2 From the **Access Control** tab, click **Top Level Realm**.

Step 3 From the **Authentication** tab, click **Module Instances**.

Step 4 In the **Module Instances** window, click **New**.

Step 5 Enter a name for the new login module instance (for example, CUPKRB) and choose **Windows Desktop SSO** from the **Type** list.

Step 6 Click **OK**.

Note This module instance name will be used later when enabling SSO on the Cisco Unified Presence server.

Step 7 Click **Save**.

Step 8 In the **Module Instances** window, choose the name of the new login module (for example, CUPKRB) and provide the following information:

Parameter	Description	Sample Value
Service Principal	This value should exactly match the value specified in Provision Active Directory for Single Sign-On, page 16-4. For example, -princ value.	HTTP/server1.cisco.com@CISCO.COM (using openAM server name and domain)
Keytab File Name	This value should be the location of the keytab file that was created in Provision Active Directory for Single Sign-On, page 16-4 copied to the OpenAM server in Step 11.	C:\keytab\server1.HTTP.keytab (on Windows platform)
Kerberos Realm	Domain for OpenAM server	CISCO.COM
Kerberos Server Name (Active Directory)	Provide the FQDN of the AD server. The AD server is normally the Kerberos Domain Controller. If multiple Kerberos Domain Controllers exist for failover purposes, all Kerberos Domain Controllers can be set using a colon (:) as the separator.	ad.cisco.com

Parameter	Description	Sample Value
Return Principal with Domain Name	Uncheck the **Enabled** check box.	
Authentication Level		22

Step 9 Click **Save**.

The module instance is created and called CUPKRB.

Step 10 Validate that the SSO Module is working correctly by logging in to a Windows Desktop session as a valid Windows user (a valid end user that exists in the AD; do not use the Administrator account). Access the following URL:

Note The browser must be configured for SSO.

```
https://<openam-FQDN>:8443/<war-file-name>/UI/Login?module=<SSO_Module>
```

Where:

<openam-FQDN> is the FQDN of the OpenAM server
<war-file-name> is the name of the deployed OpenAM WAR file, for example “opensso”
<SSO_Module> is the name of the WindowsDesktopSSO module.

A screen notifies you that login was successful.

Configure J2EE Agent Profile on OpenAM

The J2EE Agent is an internal component that is instantiated on each Cisco Unified Presence node with SSO enabled. You must configure an associated J2EE Agent Profile on the OpenAM server for each J2EE Agent. As such, a J2EE Agent Profile is required for every Cisco Unified Presence node with SSO enabled. If multiple nodes are to be configured for SSO, a J2EE Agent Profile must be created for each additional node.

Procedure

Step 1 Log in to the OpenAM Administration interface using the credentials you specified in section Set up OpenAM using the GUI Configurator, page 16-17.

Step 2 From the **Access Control** tab, click **/(Top Level Realm)**.

Step 3 From the **Agents** tab, choose the **J2EE** tab.

Step 4 In the Agents section, click **New**.

Step 5 Enter values for the following fields:

Parameter Name	Description	Value
Name	Name of the J2EE Policy Agent	cupnode01-j2ee-agent **Note** The Agent name will be used later when you enable SSO on Cisco Unified Presence.
Password	Password of the J2EE Policy Agent **Note** The password will be used when you enable SSO on Cisco Unified Presence.	
Configuration	Controls where the J2EE Policy Agent configuration is stored.	Choose **Centralized**
Server URL	The complete URL of the OpenAM server	https://<OpenAM FQDN>:8443/opensso where opensso is the name of the OpenAM WAR file with the .war extension removed
Agent URL	The URL of the J2EE Policy Agent to which OpenAM publishes notifications	https://<CUP FQDN>:8443/agentapp **Note** The value “agentapp” is the key item from the sample URL above. If you use the “agentapp” value, enter “agentapp” when prompted to **Enter the relative path where the policy agent should be deployed** in Step 3 of Enable Single Sign-On, page 16-28.

Step 6 Click **Create**.
A J2EE Agent with the name of <hostname-j2ee-agent> is created.

Step 7 Choose the J2EE agent that you created.

Step 8 From the **Application** tab, under the **Login Processing** section, add the Login Form URIs for each web GUI application on Cisco Unified Presence as follows:

Application	Sample Value
Cisco Unified Presence Administration	/cupadmin/WEB-INF/pages/logon.jsp
Cisco Unified Serviceability	/ccmservice/WEB-INF/pages/logon.jsp
Cisco Unified Reporting	/cucreports/WEB-INF/pages/logon.jsp

Application	Sample Value
Cisco Unified OS Administration	/cmplatform/WEB-INF/pages/logon.jsp
Disaster Recovery System	/drf/WEB-INF/pages/logon.jsp
Real-Time Monitoring Tool (RTMT)	/ast/WEB-INF/pages/logon.jsp
Cisco Unified Presence User Options	/cupuser/WEB-INF/pages/logoncontrol.jsp
Cisco UP Client Profile Agent	ssoservlet/WEB-INF/pages/logon.html **Note** This option is only available in Cisco Unified Presence Release 8.6(5) and later and is only applicable to customers using Common Access Card (CAC) sign-on.

Step 9 Click **Save**.

Step 10 From the **OpenSSO Services** tab, under Login URL, add OpenSSO Login URL as https://<OpenAM FQDN>:8443/<war-file-name>/UI/Login?module=<SSO_Module>.

Note Replace the place holders OpenAM FQDN, war-file-name and SSO_Module with the correct values where SSO_Module should be the same value as the one you created in Configure Single Sign-On Module Instance, page 16-21. For example, https://server1.cisco.com:8443/opensso/UI/Login?module=CUPKRB

Step 11 In the text area, remove all URLs other than the Login URL. Only the Login URL specified in the previous step should be listed in the text area.

Step 12 Click **Save**.

Step 13 Click **Back to Main Page**.

Step 14 Repeat Steps 4 through 13 to create a J2EE Profile Agent for every other Cisco Unified Presence node to be enabled for SSO.

Set the OpenAM Session Timeout

The OpenAM session timeout must be set to a value that is higher than the session timeout parameter that is set on the Cisco Unified Presence server. To determine the session timeout value on the Cisco Unified Presence server, enter the following command using the CLI:

```
show webapp session timeout
```

Procedure

Step 1 Log in to the OpenAM Administration interface using the credentials you specified in section Set up OpenAM using the GUI Configurator, page 16-17.

Step 2 From the **Configuration** tab, choose **Global.**

Step 3 **Click Session.**

Step 4 **Click Dynamic Attributes**

Step 5 Enter a value in the **Maximum Idle Time** field.

Step 6 Click **Save**.

Import the OpenAM Certificate into Cisco Unified Presence

Cisco Unified Presence nodes with SSO communicate with the OpenAM server over an encrypted channel. Establishing an encrypted communication channel requires each Cisco Unified Presence node with SSO to trust the security certificate presented by the OpenAM server. A Cisco Unified Presence node trusts a security certificate by importing the required security certificates into the tomcat-trust trust store.

The required procedure is dependent on the security configuration used when creating the Java keystore for the OpenAM Server in section Before You Begin, page 16-4:

- Use a self-signed security certificate for OpenAM/Tomcat instance
- Use a CA-signed security certificate for OpenAM/Tomcat instance

Caution Importing OpenAM certificates affects service; Cisco highly recommends that you import the OpenAM certificates during a maintenance window.

Note For information about importing certificates, see *Cisco Unified System Maintenance Guide for Cisco Unified Presence*.

Procedure

Step 1 Sign in to the Cisco Unified Presence Administration for a given Cisco Unified Presence publisher node that is to be enabled with SSO.

Step 2 Choose **System > Security > Certificate Import Tool**.

Step 3 Choose **Tomcat Trust** as the **Certificate Trust Store**.

Step 4 Enter the Fully Qualified Domain Name of the OpenAM server as the **Peer Server**.

Step 5 Enter 8443 as the **Peer Server Port**.

Step 6 Click **Submit**.

The Certificate Import Tool executes two tests:

- **Verify reachability of the specified certificate server (pingable)** - checks that the OpenAM server is reachable by this Cisco Unified Presence node. If this test fails, it may be due to the firewall on the OpenAM base Windows system blocking the ping operation. See the following link for further information about how to allow a ping through a Windows firewall: http://technet.microsoft.com/en-us/library/cc749323(WS.10).aspx
- **Verify SSL connectivity to the specified certificate server** - checks if this Cisco Unified Presence node can securely connect to the OpenAM server. If this test fails due to “Missing certificates”, the required certificates are missing and a secure connection can not be established. If this test fails, proceed to the next step. If this test passes, proceed to Step 15.

Note If this test fails with the following error "The Troubleshooter has encountered an internal error", proceed with Certificate Failure, page 23-6 and then continue with the next step.

Step 7 Click **Configure** to open the Certificate Viewer. The Certificate Viewer provides a visual representation of the certificate chain presented by OpenAM during a TLS connection handshake. This indicates which certificates must be imported into this Cisco Unified Presence node.

Step 8 Inspect the certificates in the chain and ensure that you trust the issuers.

Step 9 Check **Accept Certificate Chain** and click **Save**.

The required certificates from the chain are now imported into the tomcat-trust trust store of this Cisco Unified Presence node.

Step 10 Click **Close**.

The Certificate Import Tool reports that the "Certificates verified successfully".

Step 11 Restart the Cisco UP Intercluster Sync Agent service on this node using the following CLI command: `utils service restart Cisco UP Intercluster Sync Agent`.

Step 12 Restart the Tomcat service on this node using the following CLI command: `utils service restart Cisco Tomcat`.

Step 13 Repeat Steps 11 and 12 for each subscriber node in this cluster.

Step 14 Verify the secure connection by using the Certificate Import Tool on each subscriber node in this cluster.

a. Sign in to Cisco Unified Presence Administration for a given Cisco Unified Presence subscriber node that is being configured with SSO.

b. Choose **System > Security > Certificate Import Tool**.

c. Choose **Tomcat Trust** as the **Certificate Trust Store**.

d. Enter the FQDN of the OpenAM server as the **Peer Server**.

e. Enter **8443** as the **Peer Server Port**.

Step 15 Repeat this procedure for all Cisco Unified Presence clusters for which you will be enabling SSO.

Activate Single Sign-On

When enabling SSO, you must perform the following tasks in the order indicated.

- Configure Access Permissions Before Enabling Single Sign-On, page 16-27
- Enable Single Sign-On, page 16-28

Caution Enabling SSO affects service; Cisco highly recommends that you enable SSO during a maintenance window.

Configure Access Permissions Before Enabling Single Sign-On

It is important to understand the user access permissions that should be in place before and after SSO is enabled. Understanding the permissions can help avoid situations in which users have incorrect permissions when accessing the Cisco Unified Presence applications.

Application	Notes
Cisco Unified Presence Administration (Cisco Unified Presence Administration, Cisco Unified Presence Serviceability, Cisco Unified Presence Reporting)	Before enabling SSO, ensure that an end user who is a member of the necessary User Groups exists in order to facilitate administration access. The default administrator application user that was created at the time of installation has the following: Groups: • Standard Audit Users • Standard Cisco Unified Presence Super Users • Standard RealtimeAndTraceCollection Roles: • Standard AXL API Access • Standard Audit Log Administration • Standard CCM Admin Users • Standard CCMADMIN Administration • Standard CUReporting • Standard RealtimeAndTraceCollection* • Standard SERVICEABILITY Administration Any end user that is a member of the above User Groups with those Roles will have full access rights to Cisco Unified Presence, similar to that of the default administrator To view the default application user on Cisco Unified Presence, choose **Cisco Unified Presence Administration > User Management > Application User > Find**. Choose the default application user (that was created during installation) to view their details. To assign an end user to these groups on Cisco Unified Presence, choose **Cisco Unified Presence Administration > User Management > User Groups > Find**. Choose a group and click **Add End Users**. Search for the desired end user, choose the user, and click **Add Selected**.
Cisco Unified Presence User Options	Ensure that the end users are members of the Standard CCM End User group on the corresponding Cisco Unified Communications Manager node.

Application	Notes
Cisco Unified Presence Operating System Administration (Cisco Unified Presence Operating System Administration, Cisco Unified Presence Disaster Recovery System)	Normally, the default administrator application user does not have access to these web applications. These web applications are only accessible by the Cisco Unified Presence Operating System administrator. This administrator has access to the Administration CLI in addition to these web applications. After SSO is enabled for these applications, the applications are accessible by any end user that has the same permissions as the default administrator application user.
Real-Time Monitoring Tool	Before enabling SSO, ensure that an end user exists that is a member of the necessary user groups to allow administrative access to the Real-Time Monitoring Tool. Refer to the note for Cisco Unified Presence Administration above.

Enable Single Sign-On

This application is split into three components:

- Status
- Server Settings
- Select Applications

Status

A warning message displays indicating that the change in SSO settings causes Tomcat to restart.

The following error messages may display when you enable the SSO application:

- Invalid Open Access Manager (OpenAM) server URL - This error message displays when you enter an invalid OpenAM server URL.
- Invalid profile credentials - This error message displays when you enter a wrong profile name or wrong profile password or both.
- Security trust error - This error message displays when this Cisco Unified Presence node does not trust the certificate chain presented by the OpenAM server.

Note If you see any of the above error messages while enabling SSO, then the status changes to that error.

Server Settings

You can edit the server settings only when SSO is disabled for all applications.

Select Applications

You can enable or disable SSO on any of the following applications:

- Cisco Unified Presence Administration - Enables SSO for Cisco Unified Presence Administration, Cisco Unified Serviceability, and Cisco Unified Reporting
- Cisco Unified Presence User Options - Enables SSO for End User Options
- Cisco Unified Operating System Administration - Enables SSO for Cisco Unified Operating System Administration and Disaster Recovery System

- RTMT - Enables the web application for the Real-Time Monitoring Tool
- Cisco UP Client Profile Agent - Enables SSO for the Cisco UP Client Profile Agent service. This option is only available in Cisco Unified Presence Release 8.6(5) and later and is only applicable to customers using Common Access Card (CAC) sign-on.

Note You can enable SSO using either the GUI, as described in this procedure, or the CLI. For information about how to enable SSO using the CLI, see the `utils sso enable` command in the *Command Line Interface Guide for Cisco Unified Presence Release 8.0, 8.5, and 8.6*.

Procedure

Step 1 Navigate to the Cisco Unified Presence Operating System Administration page and choose **Security > Single Sign On**.

Step 2 Enter the URL of the OpenAM server.

Example:

https://server1.cisco.com:8443/opensso

Step 3 Enter the relative path where the policy agent should be deployed. The relative path must be alphanumeric, such as *agentapp*, for example. See Configure J2EE Agent Profile on OpenAM, page 16-22.

Step 4 Enter the name of the profile that is configured for this policy agent, for example "cupnode01-j2ee-agent". See Configure J2EE Agent Profile on OpenAM, page 16-22.

Step 5 Enter the password of the profile name. See Configure J2EE Agent Profile on OpenAM, page 16-22.

Step 6 Enter the login Module instance name that is configured for Windows Desktop SSO, such as CUPKRB, for example. See Configure Single Sign-On Module Instance, page 16-21.

Step 7 Click **Save**.

Step 8 In the **Confirmation** dialog box, click **OK** to restart Tomcat.

Disable Single Sign-On

If you choose to disable SSO, you must perform the following tasks in the order indicated.

- Configure Access Permissions Before Disabling Single Sign-On, page 16-29
- Disable Single Sign-On, page 16-30

Configure Access Permissions Before Disabling Single Sign-On

If SSO is disabled for any Cisco Unified Presence web application that supports SSO, all users accessing that application need to provide a username and password. Cisco recommends that if you are a Cisco Unified Presence administrator intending to disable SSO for any Cisco Unified Presence web applications, ensure that users can access the application after SSO is disabled. This action is important to avoid inadvertently locking out the active Cisco Unified Presence administration account.

Application	Notes
Cisco Unified Presence Administration (Cisco Unified Presence Administration, Cisco Unified Presence Serviceability, Cisco Unified Presence Reporting	Before disabling SSO, ensure that an application users exists with a known username/password and that this user is a member of the necessary User Groups. The default administrator application user that was created at the time of installation has the following: Groups: • Standard Audit Users • Standard Cisco Unified Presence Super Users • Standard RealtimeAndTraceCollection Roles: • Standard AXL API Access • Standard Audit Log Administration • Standard CCM Admin Users • Standard CCMADMIN Administration • Standard CUReporting • Standard RealtimeAndTraceCollection* • Standard SERVICEABILITY Administration Any application user that is a member of the above User Groups with those Roles will have full access rights to Cisco Unified Presence if SSO is disabled. To view the application users on Cisco Unified Presence, choose **Cisco Unified Presence Administration > User Management > Application User > Find**. Choose a user to view their details.
Cisco Unified Presence User Options	Ensure that passwords exist for the end users and that they are aware of their password values. This information is required by each end user to access the application.
Cisco Unified Presence Operating System Administration (Cisco Unified Presence Operating System Administration, Cisco Unified Presence DRS)	Before disabling SSO, ensure that an OS Administration user exists with a known username/password and that this user has access to Cisco Unified Presence Operating System Administration CLI. After SSO is disabled, this user has access rights to the Cisco Unified Presence Operating System Administration GUIs.
Real-Time Monitoring Tool	Before disabling SSO, ensure that an application user with a known username/password exists and that this user has the same access rights as the user specified for Cisco Unified Presence Administration (Cisco Unified Presence Administration, Cisco Unified Presence Serviceability, and Cisco Unified Presence Reporting).

Disable Single Sign-On

You can disable SSO using either the GUI, as described in this procedure, or the CLI. For information

about how to disable SSO using the CLI, see the `utils sso disable` command in the *Command Line Interface Guide for Cisco Unified Presence Release 8.0, 8.5, and 8.6*.

Procedure

Step 1 Navigate to the Cisco Unified Presence Operating System Administration page and choose **Security > Single Sign On**.

Step 2 Uncheck all applications that were previously enabled for SSO.

Step 3 Click **Save**.

Step 4 In the **Confirmation** dialog box, click **OK** to restart Tomcat.

Uninstall OpenAM

Prerequisites

Ensure that you have completed the following tasks before you uninstall OpenAM:

- Configure Access Permissions Before Disabling Single Sign-On, page 16-29
- Disable Single Sign-On, page 16-29

Procedure

Step 1 Access the OpenAM server Windows desktop and choose **Start > All Programs > Apache Tomcat 7.0 Tomcat 7 > Configure Tomcat**.

Note This menu path assumes you are using Tomcat 7.

Step 2 From the **General** tab, click Stop to stop the Tomcat service if it is running on the OpenAM server.

Step 3 Delete the OpenAM configuration data. This data is typically stored in two directories that can be found in the home directory of the user running the Tomcat instance. For example, C:\opensso (where the folder name matches the deployed URI for the OpenAM WAR file such as opensso) and C:\.openssocfg.

Step 4 Delete the deployed OpenAM WAR file and the WAR file itself from the following location on the OpenAM/Tomcat instance: tomcat-dir\webapps. See Install Tomcat, page 16-13 for a description of the tomcat-dir variable.

Example:

```
C:\Program Files\Apache Software Foundation\Tomcat 7\webapps
```

Step 5 Access the Windows desktop of the OpenAM server and choose **Start > All Programs > Apache Tomcat 7.0 Tomcat 7 > Configure Tomcat**.

Step 6 From the **General** tab, click **Start** to start the Tomcat service.

Set the Debug Level

You can gather additional debug information the Cisco Unified Presence node by setting the log level for the J2EE Policy Agent accordingly. The log level for this component is configured on the OpenAM server itself. The default log level is Error. You can change the log level to Message to provide additional debug information. Cisco recommends that you use the Message log level only for short periods of time, because the associated log files can grow quite large.

Procedure

Step 1 Sign in to OpenAM (https://<OpenAM FQDN>:8443/opensso) from your web browser (for example, Mozilla Firefox).

Step 2 From the Access Control menu, choose **Top Level Realm > Agents > J2EE**.

Step 3 Under the **General** heading, choose **Agent Debug Level**.