SAML SSO Configuration

SAML-Based SSO Prerequisites

The following system setup is required for SAML-Based SSO configuration:

- NTP Setup
- DNS Setup
- Directory Setup

NTP Setup

In SAML SSO, Network Time Protocol (NTP) enables clock synchronization between the Unified Communications applications and IdP. SAML is a time sensitive protocol and the IdP determines the time-based validity of a SAML assertion. If the IdP and the Unified Communications applications clocks are not synchronized, the assertion becomes invalid and stops the SAML SSO feature. The maximum allowed time difference between the IdP and the Unified Communications applications is 3 seconds.

Note For SAML SSO to work, you must install the correct NTP setup and make sure that the time difference between the IdP and the Unified Communications applications does not exceed 3 seconds.

DNS Setup

Domain Name System (DNS) enables the mapping of host names and network services to IP addresses within a network or networks. DNS server(s) deployed within a network provide a database that maps network services to hostnames and, in turn, hostnames to IP addresses. Devices on the network can query the DNS server and receive IP addresses for other devices in the network, thereby facilitating communication between network devices.

Unified Communications applications can use DNS to resolve fully qualified domain names to IP addresses. The service providers and the IdP must be resolvable by the browser. For example, when the administrator enters the service provider hostname (`http://www.cucm.com/ccmadmin`) in the browser, the browser must resolve the hostname. When the service provider redirects the browser to IdP (`http://www.idp.com/saml`) for SAML SSO, the browser must also resolve the IdP hostname. Moreover, when the IdP redirects back to the service provider ACS URL, the browser must resolve that as well.

Directory Setup

LDAP directory synchronization is a prerequisite and a mandatory step to enable SAML SSO across various Unified Communications applications. Synchronization of Unified Communications applications with an LDAP directory allows the administrator to provision users easily by mapping Unified Communications applications data fields to directory attributes.

Note To enable SAML SSO, the LDAP server must be trusted by the IdP server and supported by Unified Communications applications.

For more information, see the "Directory Integration and Identity Management" chapter of the *Cisco Collaboration System Solution Reference Network Designs* at:

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html

Certificate Management and Validation

Important Cisco strongly recommends that server certificates are signed for SAML SSO and that multiserver certificates are used where product support is available.

Note

- Common Names (CN) and Subject Alternative Names (SAN) are references to the IP address or Fully Qualified Domain Name (FQDN) of the address that is requested. For instance, if you enter https://www.cisco.com, then the CN or SAN must have “www.cisco.com” in the header.
- If the Unified Communications Manager is already in Mixed/Secure Mode and there are changes made to the certificates, then the CTL certificate must be updated using the secure USB token. Otherwise the Cisco Jabber client will not be able to acquire telephony capability. The CTL token update requires a Unified Communications Manager restart.

In SAML SSO, each entity participating in the SAML message exchange, including the user's web browser, must establish a seamless secure HTTPS connections to the required entities. Cisco strongly recommends that signed certificates issued by a trusted Certificate Authority be configured on each UC product participating in the SAML SSO deployment.

Unified Communications applications use certificate validation to establish secure connections with servers. Certificates are used between end points to build a trust/authentication and encryption of data. This confirms

that the endpoints communicate with the intended device and have the option to encrypt the data between the two endpoints.

When attempting to establish secure connections, servers present Unified Communications clients with certificates. If the client cannot validate a certificate, it prompts the user to confirm if they want to accept the certificate.

Certificates Signed by a Certificate Authority

Cisco recommends using server certificates that are signed by one of the following types of Certificate Authority (CA):

- **Public CA** - A third-party company verifies the server identity and issues a trusted certificate.
- **Private CA** - You create and manage a local CA and issue trusted certificates.

The signing process varies for each product and can vary between server versions. It is beyond the scope of this document to provide detailed steps for every version of each server. Refer the appropriate server documentation for detailed instructions on how to get certificates signed by a CA.

However, the following steps provide a high-level overview of the procedure:

Procedure

Step 1 Generate a Certificate Signing Request (CSR) on each product that can present a certificate to the client.

Step 2 Submit each CSR to the CA.

Step 3 Upload the certificates that the CA issues to each server.

Every server certificate should have an associated root certificate present in the trust store on client computers. Cisco UC applications validate the certificates that servers present against the root certificates in the trust store.

If you get server certificates signed by a public CA, the public CA should already have a root certificate present in the trust store on the client computer. In this case, you do not need to import root certificates on the client computers.

You should import root certificates if the certificates are signed by a CA that does not already exist in the trust store, such as a private CA.

In SAML SSO, the IdP and service providers must have CA signed certificates with the correct domains in the CN or SAN. If the correct CA certificates are not validated, the browser issues a pop up warning.

For example, when the administrator points the browser to `https://www.cucm.com/ccmadmin`; the Unified Communications Manager portal presents a CA certificate to the browser. When the browser is redirected to `https://www.idp.com/saml` , the IdP presents a CA certificate. The browser will check that the certificate presented by the servers contains CN or SAN fields for that domain, and that the certificate is signed by a trusted CA.

Alternatively, if the customer has their own private CA, then that CA must be installed as a root trust anchor on the computers that the administrator is launching their browser from.

Configure Multiserver SAN Certificates

Each Cisco product has its own process for generating multiserver SAN certificates. For information about the Cisco products that support multiserver SAN certificates see the relevant guide.

Related Topics

Release Notes for Cisco Unified Communications Manager, Release 10.5(1)
Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 10.x
Cisco Prime Collaboration

Deploy Certificate Issuer for Microsoft Edge Interoperability

An interoperability issue exists within SAML SSO deployments where the Microsoft Edge Browser is deployed. If the Edge Browser is deployed on an SSO-enabled machine, the Edge browser does not recognize the certificate issuer of the Unified Communications Manager certificate and does not provide access.

Use this procedure to fix this issue via the Group Policy Object (GPO) and Active Directory whereby you can push the certificate issuer of the Unified Communications Manager certificate to the Trusted Root Certification of local machines that use the Edge browser.

Note The "certificate issuer" depends on how your certificates are set up. For example, for third-party CA certificates, You may need to push the CA certificate only if the CA itself signs the Unified Communications Manager certificate. However, if an intermediate CA signs the Unified Communications Manager certificate, you may need to push the complete certificate chain, which will include the root certificate, intermediate certificate, and any leaf certificates.

Before you begin

Membership in the local **Administrators** group, or equivalent, of the local machine is the minimum required to complete this procedure

Procedure

Step 1 In Active Directory, Open Group Policy Management Console.

Step 2 Find an existing GPO or create a new GPO to contain the certificate settings. The GPO must be associated with the domain, site, or organizational unit whose users you want affected by the policy.

Step 3 Right-click the GPO, and select **Edit**.
The **Group Policy Management Editor** opens, and displays the current contents of the policy object.

Step 4 In the navigation pane, open **Computer Configuration** > **Windows Settings** > **Security Settings** > **Public Key Policies** > **Trusted Publishers**.

Step 5 Click the **Action** menu, and click **Import**.

Step 6 Follow the instructions in the **Certificate Import Wizard** to find and import the certificate.

Step 7 If the certificate is self-signed, and cannot be traced back to a certificate that is in the **Trusted Root Certification Authorities** certificate store, then you must also copy the certificate to that store. In the navigation

pane, click **Trusted Root Certification Authorities**, and then repeat steps 5 and 6 to install a copy of the certificate to that store.

Note For additional information on Managing Trusted Root Certificates in Active Directory, see https://technet.microsoft.com/en-us/library/cc754841(v=ws.11).aspx.

SAML SSO Configuration Task Flow

Complete these tasks to configure SAML SSO in your Cisco Collaboration environment. This process includes procedures for the following applications:

- Cisco Unified Communications Manager
- IM and Presence Service
- Cisco Unity Connection
- Cisco Expressway (with MRA Deployments)

Procedure

	Command or Action	Purpose
Step 1	Initiate SSO Configuration on Collaboration Applications, on page 5	In your Cisco Collaboration environment, initiate the SSO configuration and export UC metadata.
Step 2	Configure SAML SSO on Identity Provider, on page 8	On your Identity Provider: • Upload the UC metadata • Configure SAML SSO agreements • Export an IdP metadata file
Step 3	Enable SAML SSO for Cisco Collaboration Applications, on page 8	Import IdP metadata into your Cisco Collaboration environment and complete the configuration.

Initiate SSO Configuration on Collaboration Applications

In your Cisco Collaboration environment, begin the SAML SSO configuration and export UC metadata for upload into your Identity Provider. Depending on the applications for which you are configuring SAML SSO, and the options chosen, you may have multiple download files.

Before you begin

Make sure that you plan beforehand what type of SAML SSO agreement you want (cluster wide or per node), along with the certificate type.

Procedure

Step 1 On Cisco Unified Communications Manager, export a UC metadata file:

a) From Cisco Unified CM Administration, choose **System** > **SAML Single Sign On**.
b) Select an **SSO Mode** option: **Cluster wide** or **Per Node**.
c) Select a **Certificate** option: **System generated self-signed certificate** or a **Cisco Tomcat** certificate.
d) Click **Export All Metadata** and save the metadata file to a secure location.
With cluster wide agreements, you will receive a single metadata file. With per node agreements, the zip file download contains a separate XML files for each cluster node. If you have IM and Presence Service deployed in a Standard deployment,

Step 2 IM and Presence Service—If you have a Centralized Deployment for the IM and Presence Service, repeat step 1 on the standalone Unified CM publisher node that is a part of your IM and Presence central cluster.

Note With IM and Presence Service Standard Deployments you can skip this task because the the metadata file that you downloaded from Unified Communications Manager in the previous step includes metadata for the IM and Presence Service cluster.

Step 3 On Cisco Unity Connection, export a metadata file:

a) From Cisco Unity Connection Administration, choose **System Settings** > **SAML Single Sign On**.
b) Select the **SSO Mode** option: **Cluster wide** or **Per node**.
c) Click **Export All Metadata**.

Step 4 On Cisco Expressway-C, export a metadata file:

a) On the Expressway-C primary peer, go to **Configuration** > **Unified Communications** > **Configuration**
b) In the **MRA Access Control** section, choose either of the following options for the **Authentication path**:

- **SAML SSO authentication**
- **SAML SSO and UCM/LDAP**—Allows either method.

c) Choose a **SAML Metadata** option: Cluster or Peer

- **Cluster**—Single metadata file for cluster
- **Peer**—Separate metadata files per node.

d) Click **Export SAML data**.

- For Cluster agreements, click **Generate Certificate** and then **Download** the certificate.
- For Peer agreements, **Download All**.

e) Save in a secure location.

At the completion of this procedure, you will have metadata files for each of your Collaboration applications. The number of metadata files depends on your configuration and deployment type.

Metadata Download Example

Refer to the following for an example of the number of file downloads you can expect from your Cisco Collaboration deployment. Assume that you are configuring SSO for the following applications:

- A five-node Cisco Unified Communications Manager cluster
- A three-node IM and Presence Service cluster
- A two-node Cisco Unity Connection cluster
- A three-node Expressway-C cluster accompanied with a 3-node Expressway-E cluster (MRA deployment)

The following table provides a breakdown of the total download files that you can expect depending on whether you are uisng cluster-wide agreements, and whether the IM and Presence Service is in a Standard Deployment or Centralized Deployment.

Table 1: Expected Metadata Downloads

Agreement Type	Total Files Downloaded when IM and Presence is in Standard Deployment	Total Files Downloaded when IM and Presence is in Centralized Deployment*
Cluster wide	Three metadata XML files representing following clusters: • Unfiied Communications Manager and IM and Presence Service cluster • Unity Connection cluster • Expressway-C cluster	Four metadata XML files representing following clusters: • Unfiied Communications Manager cluster • IM and Presence Service cluster • Unity Connection cluster • Expressway-C cluster
Per node	Three zip files containing 13 metadata XML files: • One zip file with eight XML files for Unified CM and IM and Presence nodes • One zip file with two XML files for Unity Connection nodes • One zip file with three XML files for Expressway-C nodes	Four zip files containing 14 metadata XML files: • One zip file with five XML files for Unified CM nodes • One zip file with three XML files for IM and Presence nodes and an extra XML file for the standalone Unified CM publisher node that is in the IM and Presence central cluster • One zip file with two XML files for Unity Connection nodes • One zip file with three XML files for Expressway-C nodes

Note With Standard Deployments, the IM and Presence Service is in the same cluster as Cisco Unified Communications Manager. Metadata for the IM and Presence Service is included in the metadata download from Cisco Unified Communications Manager.

With Centralized Deployments, the IM and Presence Service is in a different cluster from the Cisco Unified Communications Manager telephony cluster and metadata for the IM and Presence Service must be exported separately using the standalone, non-telephony Unified CM publisher node that is within the IM and Presence central cluster.

Configure SAML SSO on Identity Provider

On the Identity Provider, you need to:

- Import the UC metadata files that you downloaded from your Cisco Collaboration environment
- Configure SAML SSO agreements to your Cisco Collaboration applications
- Export an Identity Provider metadata file that you will later import into your Cisco Collaboration applications

Cisco provides the following Idp-specific configuration examples as a guide for you to use:

- Microsoft Active Directory Federation Services 2.0
- Microsoft Active Directory Federation Services 3.0
- Microsoft Active Directory Federation Services 4.0
- Microsoft Azure
- Okta
- Open AM
- PingFederate

Note The above links are examples only. Refer to your IdP documentation for official documentation.

Enable SAML SSO for Cisco Collaboration Applications

Procedure

Step 1 On Cisco Unified Communications Manager, complete the SSO configuration:

a) Restart the Cisco Tomcat server before enabling SAML SSO.
b) From Cisco Unified CM Administration, choose **System** > **SAML Single Sign On**.
c) Click **Enable SAML SSO**.

d) Click **Continue** and follow the prompts.
e) Cluster wide agreements only. Click **Test for Multi-server tomcat certificates.**
f) Click **Next**
g) **Browse** to select your IdP metadata file. After you have opened the file, click **Import IdP Metadata.**
h) Click **Next**.
i) Select an LDAP-synchronized whom has Standard CCM Super User permissions and **Run SSO test**.
j) Sign in with the user's credentials.
k) Click **Finish** to complete the SAML SSO setup.
l) Restart the Cisco Tomcat server.
m) Per node agreements only. Repeat this process on each Unified Communications Manager node.

Note If FIPS or ESM is enabled on the Unified Communications Manager, you need to set the SSO signing algorithm to sha256.

Run this command on admin CLI on all the nodes of Cisco Unified CM.

```
utils sso set signing-algorithm sha256
```

Step 2 IM and Presence Service—If you have a Centralized Deployment of the IM and Presence Service, repeat the previous step on the standalone Unified CM publisher node that is a part of the IM and Presence central cluster.

Step 3 On Cisco Unity Connection, complete the SAML SSO configuration:

a) Restart the Cisco Tomcat server before enabling SAML SSO.
b) In Cisco Unity Connection Administration, go to **System Settings** > **SAML Single Sign On**.
c) Click **Enable SAML Single Sign On**.
d) Click **Continue** and follow the prompts
e) Import the IdP metadata file into Cisco Unity Connection.
f) Test the SSO Connection.
g) Restart the Cisco Tomcat server.
h) Per node agreements only. Repeat this process for each cluster node.

Step 4 On the Expressway-C primary peer, complete the SAML SSO configuration:

a) Go to **Configuration** > **Unified Communications** > **Identity providers**.
b) Click **Import new IdP from SAML**.
c) Use **Import SAML file** control to locate the IdP metadata file.
d) Set the **Digest** to the required SHA hash algorithm.
e) Click **Upload**.

Note You can change the signing algorithm after you have imported the metadata, by going to **Configuration** > **Unified Communications** > **Identity Providers (IdP)** locating your IdP row then, in the Actions column, clicking **Configure Digest)**.

f) Verify that the IdP appears in the list of Identity Providers.
g) Click **Associate Domains** in the IdP row.
h) Check the domains that you want to assign to this Identity Provider.
i) Click **Save**.

Note If you are deploying Cisco Expressway with Active Directory Federation Services (ADFS) for SAML SSO, refer to Additional Expressway Configuration for ADFS, on page 10 for additional Expressway settings.

SAML SSO Additional Tasks

You can perform the following additional tasks to enable SAML SSO setup as per the requirement.

Restart Cisco Tomcat Service

Before and after enabling or disabling SAML Single Sign-On, restart the Cisco Tomcat service on all Unified CM and IM and Presence Service cluster nodes where Single Sign-On is running.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the `utils service restart Cisco Tomcat` CLI command.

Step 3 Repeat this procedure on all cluster nodes where Single Sign-On is enabled.

Additional Expressway Configuration for ADFS

If you are deploying SAML SSO for Expressway with Active Directory Federation Services, complete these additional Expressway configurations:

Procedure

Step 1 In Windows PowerShell®, run the following command for each Expressway-E's <EntityName> once per Relying Party Trust created on ADFS:

```
Set-ADFSRelyingPartyTrust -TargetName "<EntityName>" -SAMLResponseSignatureMessageAndAssertion
```

where `<EntityName>` must be a display name for the Relying Party Trust of Expressway-E as set in ADFS.

Step 2 In ADFS, add a Claim Rule for Each Relying Party :

a) Open the **Edit Claims Rule** dialog, and create a new claim rule that sends AD attributes as claims.

b) Select the AD attribute to match the one that identifies OAuth users to the internal systems, typically email or SAMAccountName.

c) Enter **uid** as the Outgoing Claim Type.

Configure SSO Login Behavior for Cisco Jabber on iOS

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 To configure the opt-in control, in the SSO Configuration section, choose the **Use Native Browser** option for the **SSO Login Behavior for iOS** parameter:

Note The **SSO Login Behavior for iOS** parameter includes the following options:

- **Use Embedded Browser**—If you enable this option, Cisco Jabber uses the embedded browser for SSO authentication. Use this option to allow iOS devices prior to version 9 to use SSO without cross-launching into the native Apple Safari browser. This option is enabled by default.
- **Use Native Browser**—If you enable this option, Cisco Jabber uses the Apple Safari framework on an iOS device to perform certificate-based authentication with an Identity Provider (IdP) in the MDM deployment.

  Note We don't recommend to configure this option, except in a controlled MDM deployment, because using a native browser is not as secure as the using the embedded browser.

Step 3 Click **Save**.

Access the Recovery URL

Use the recovery URL to bypass SAML Single Sign-On and log in to the Cisco Unified Communications Manager Administration and Cisco Unified CM IM and Presence Service interfaces for troubleshooting. For example, enable the recovery URL before you change the domain or hostname of a server. Logging in to the recovery URL facilitates an update of the server metadata.

Before you begin

- Only application users with administrative privileges can access the recovery URL.
- If SAML SSO is enabled, the recovery URL is enabled by default. You can enable and disable the recovery URL from the CLI. For more information about the CLI commands to enable and disable the recovery URL, see *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Procedure

In your browser, enter `https://hostname:8443/ssosp/local/login`.

Update Server Metadata After a Domain or Hostname Change

After a domain or hostname change, SAML Single Sign-On is not functional until you perform this procedure.

Note If you are unable to log in to the **SAML Single Sign-On** window even after performing this procedure, clear the browser cache and try logging in again.

Before you begin

If the recovery URL is disabled, it does not appear for you to bypass the Single Sign-On link. To enable the recovery URL, log in to the CLI and execute the following command: **utils sso recovery-url enable**.

Procedure

Step 1 In the address bar of your web browser, enter the following URL:

`https://<Unified CM-server-name>`

where `<Unified CM-server-name>` is the hostname or IP address of the server.

Step 2 Click **Recovery URL to bypass Single Sign-On (SSO)**.

Step 3 Enter the credentials of an application user with an administrator role and click **Login**.

Step 4 From Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On**.

Step 5 Click **Export Metadata** to download the server metadata.

Step 6 Upload the server metadata file to the IdP.

Step 7 Click **Run Test**.

Step 8 Enter a valid User ID and password.

Step 9 After you see the success message, close the browser window.

Update IdP Metadata

Use this procedure to update the IdP Metadata Trust file on all the servers in the cluster.

Before you begin

If the recovery URL is disabled, it doesn't appear for you to bypass the Single Sign-On link. To enable the recovery URL, log in to the CLI and execute the following command: `utils sso recovery-url enable`.

Procedure

Step 1 In the address bar of your web browser, enter the following URL:

https://<Unified CM-server-name>

Where <Unified CM-server-name> is the hostname or IP address of the server.

Step 2 Click **Recovery URL to bypass Single Sign-On (SSO)**.

Step 3 Enter the credentials of an application user with an administrator role and click **Login**.

Step 4 From Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On**.

Step 5 Click **Update IdP Metadata File** to import the IdP Metadata trust file.

Step 6 Click **Browse** to select the IdP Metadata trust file and click **Import IdP Metadata** to import the file to collaboration servers.

Step 7 Click **Next**.

Step 8 Select an LDAP-synchronized who has Standard CCM Super User permissions to verify whether the metadata file is configured appropriately and **Run SSO Test**.

Step 9 Sign in with the valid user's credentials.

Step 10 Click **Finish** to enable the SAML SSO setup on all the servers in the cluster.

Note When the applications are updated, there will be a short delay. The "Cisco Tomcat" services restart on all nodes in the cluster if the SSO mode is "cluster-wide". Otherwise, the services restart on the particular node where IDP metadata is updated.

Manually Provision Server Metadata

To provision a single connection in your Identity Provider for multiple UC applications, you must manually provision the server metadata while configuring the Circle of Trust between the Identity Provider and the Service Provider. For more information about configuring the Circle of Trust, see the IdP product documentation.

The general URL syntax is as follows:

```
https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>
```

Procedure

To provision the server metadata manually, use the Assertion Customer Service (ACS) URL.

Example:

Sample ACS URL: `<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com" index="0"/>`

Reconfigure OpenAM SSO to SAML SSO Following an Upgrade

As of Release 11.0(1), Unified Communications Manager no longer offers the OpenAM SSO solution. If you have upgraded from an earlier release with the Open AM SSO solution configured, you must reconfigure your system to use the SAML SSO solution using one of the supported IdPs. Use the configurations that are documented in this guide to reconfigure your system to use SAML SSO.

Note Do not confuse the OpenAM SSO solution with a SAML SSO solution that uses OpenAM for the identity provider as they are different solutions. When you reconfigure your system to use SAML SSO, you can use any of the IdPs that are listed in this document.

Re-Provisioning Cluster After Network Migration

For SSO login to work properly, ensure that you re-provision the cluster post network migration.

Note This procedure is applicable only for Network migration clusters with SSO enabled. This procedure is not applicable for Simple migration.

Before you begin

- Only application users with administrative privileges can access the recovery URL.
- If SAML SSO is enabled, the recovery URL is enabled by default. You can enable and disable the recovery URL from the CLI. For more information about the CLI commands to enable and disable the recovery URL, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Procedure

Step 1 In the address bar of your web browser, enter the following URL: https://<*Unified CM-server-name*>, where <*Unified CM-server-name*> is the hostname or IP address of the server.

Step 2 Click **Recovery URL to bypass Single Sign-On (SSO)**.

Step 3 Enter the credentials of an application user with an administrator role and click **Login**.

Step 4 From Cisco Unified CM Administration, choose **System > SAML Single Sign-On**.

Step 5 Click **Export All Metadata** to download the server metadata for upload into your Identity Provider.

Step 6 Click **Update IdP Metadata File** to import the IdP Metadata trust file.

Step 7 Click **Browse** to select the IdP Metadata trust file and click **Import IdP Metadata** to import the file to collaboration servers. Click **Next**.

Step 8 Select an LDAP-synchronized who has Standard CCM Super User permissions to verify whether the metadata file is configured appropriately and click **Run Test**.

Step 9 Click **Finish** to enable the SAML SSO setup on all the servers in the cluster.

When the applications are updated, there will be a short delay. The "Cisco Tomcat", "Cisco SSOSP Tomcat" and "Cisco UDS Tomcat" services restart on all nodes in the cluster if the SSO mode is 'cluster-wide'.

SAML SSO Deployment Interactions and Restrictions

Feature	Feature Interaction
Tomcat Certificate Regeneration	If you regenerate the Tomcat Certificates, generate a new metadata file on the Service Provider and upload that metadata file to the IdP.
Metadata Regeneration	The metadata file regenerates if you perform one of the following: • Change Self-Signed Certificates to Tomcat Certificates and vice-versa. • Regenerate Tomcat Certificates to ITL Recovery Certificates. Cisco Unified Communications Manager downloads the regenerated metadata file and uploads to the IdP.