Configure Single Sign-On

- About SAML SSO Solution, on page 1
- SAML SSO Configuration Task Flow, on page 2

About SAML SSO Solution

Important When deploying Cisco Jabber with Cisco Webex meeting server, Unified Communications Manager and the Webex meeting server must be in the same domain.

SAML is an XML-based open standard data format that enables administrators to access a defined set of Cisco collaboration applications seamlessly after signing into one of those applications. SAML describes the exchange of security related information between trusted business partners. It is an authentication protocol used by service providers (for example, Unified Communications Manager) to authenticate a user. SAML enables exchange of security authentication information between an Identity Provider (IdP) and a service provider.

SAML SSO uses the SAML 2.0 protocol to offer cross-domain and cross-product single sign-on for Cisco collaboration solutions. SAML 2.0 enables SSO across Cisco applications and enables federation between Cisco applications and an IdP. SAML 2.0 allows Cisco administrative users to access secure web domains to exchange user authentication and authorization data, between an IdP and a Service Provider while maintaining high security levels. The feature provides secure mechanisms to use common credentials and relevant information across various applications.

The authorization for SAML SSO Admin access is based on Role-Based Access Control (RBAC) configured locally on Cisco collaboration applications.

SAML SSO establishes a Circle of Trust (CoT) by exchanging metadata and certificates as part of the provisioning process between the IdP and the Service Provider. The Service Provider trusts the IdP's user information to provide access to the various services or applications.

Important Service providers are no longer involved in authentication. SAML 2.0 delegates authentication away from the service providers and to the IdPs.

The client authenticates against the IdP, and the IdP grants an Assertion to the client. The client presents the Assertion to the Service Provider. Since there is a CoT established, the Service Provider trusts the Assertion and grants access to the client.

SAML SSO Configuration Task Flow

Complete these tasks to configure Unified Communications Manager for SAML SSO.

Before you begin

SAML SSO configuration requires that you configure the Identity provider (IdP) at the same time that you configure Unified Communications Manager. For IdP-specific configuration examples, see:

- Active Directory Federation Services
- Okta
- Open Access Manager
- PingFederate

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

Procedure

	Command or Action	Purpose
Step 1	Export UC Metadata from Cisco Unified Communications Manager, on page 3	To create a trust relationship, you must exchange metadata files between Unified Communications Manager and the IdP.
Step 2	Configure SAML SSO on the Identity Provider (IdP)	Complete the following tasks: • Upload the UC metadata file that was exported from Unified Communications Manager in order to complete the Circle of Trust relationship. • Configure SAML SSO on the IdP • Export an IdP metadata file. This file will be imported into the Unified Communications Manager
Step 3	Enable SAML SSO in Cisco Unified Communications Manager	Import your IdP metadata and enable SAML SSO in Unified Communications Manager.
Step 4	Restart Cisco Tomcat Service, on page 5	Before and After you enable SSO, you must restart the Cisco Tomcat service on all cluster nodes where SSO is enabled.
Step 5	Verify the SAML SSO Configuration, on page 6	Verify that SAML SSO has been configured successfully.

Export UC Metadata from Cisco Unified Communications Manager

Use this procedure to export a UC metadata file from the Service Provider (Unified Communications Manager). The metadata file will be imported into the Identity Provider (IdP) in order to build a Circle of Trust relationship.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On**

Step 2 From the **SAML Single Sign-On** window, choose one of the options for the **SSO Mode** field:

- **Cluster wide**—A single SAML agreement for the cluster.

  Note
  If you choose this option, ensure that Tomcat servers for all the nodes in the cluster have the same certificate, which is the multi-server SAN certificate.

- **Per Node**—Each node has a separate SAML agreement.

Step 3 From the **SAML Single Sign-On** window, choose one of the options for the **Certificate** field.

- **Use system generated self-signed certificate**
- **Use Tomcat certificate**

Step 4 Click **Export All Metadata** to export the metadata file.

Note
If you choose the **Cluster wide** option in Step 3, a single metadata XML file appears for a cluster for download. However, if you choose the **Per Node** option, one metadata XML file appears for each node of a cluster for download.

What to do next

Complete the following tasks on the IdP:

- Upload the UC metadata file that was exported from Unified Communications Manager
- Configure SAML SSO on the IdP
- Export an IdP metadata file. This file will be imported into the Unified Communications Manager in order to complete the Circle of Trust relationship.

Enable SAML SSO in Cisco Unified Communications Manager

Use this procedure to enable SAML SSO on the Service Provider (Unified Communications Manager). This process includes importing the IdP metadata onto the Unified Communications Manager server.

Important We recommend that you restart Cisco Tomcat service after enabling or disabling SAML SSO.

Note The Cisco CallManager Admin, Unified CM IM and Presence Administration, Cisco CallManager Serviceability, and Unified IM and Presence Serviceability services are restarted after you enable or disable SAML SSO.

Note If the IdP server certificate and the Unified Communications Manager Tomcat certificate are signed by different certificate authorities (CAs), obtain the IdP certificate (or its root certificate) and upload it as tomcat-trust on the Unified CM servers.

Before you begin

Prior to completing this procedure, make sure of the following:

- You require an exported metadata file from your IdP.
- Make sure that the end-user data is synchronized to the Unified Communications Manager database.
- Verify that the Unified Communications Manager IM and Presence Cisco Sync Agent service has completed data synchronization successfully. Check the status of this test in **Cisco Unified CM IM and Presence Administration** by choosing **Diagnostics** > **System Troubleshooter** The "Verify Sync Agent has sync'ed over relevant data (e.g. devices, users, licensing information)" test indicates a "Test Passed" outcome if data synchronization has completed successfully.
- At least one LDAP synchronized user is added to the Standard CCM Super Users group to enable access to Cisco Unified Administration. For more information about synchronizing end-user data and adding LDAP-synchronized users to a group, see the "System setup" and "End user setup" sections in the Administration Guide for Cisco Unified Communications Manager.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On**.

Step 2 Click **Enable SAML SSO** and then click **Continue**.

A warning message notifies you that all server connections will be restarted.

Step 3 If you have configured the **Cluster wide** SSO mode, click the **Test for Multi-server tomcat certificate** button. Otherwise, you can skip this step.

Step 4 Click **Next**.

A dialog box that allows you to import IdP metadata appears. To configure the trust relationship between the IdP and your servers, you must obtain the trust metadata file from your IdP and import it to all your servers.

Step 5 Import the metadata file that you exported from your IdP:

a) **Browse** to locate and select your exported IdP metadata file.
b) Click **Import IdP Metadata**.
c) Click **Next**.

d) At the **Download Server Metadata and Install on IdP** screen, click **Next**.

Note
The **Next** button is enabled only if the IdP metadata file is successfully imported on at least one node in the cluster.

Step 6 Test the connection and complete the configuration:

a) In the **End User Configuration** window, choose a user that is LDAP-synchronized and has the permission as "Standard CCM Super User" from the **Permissions Information** list box.

b) Click **Run Test**.

The IdP login window appears.

Note
You cannot enable SAML SSO until the test succeeds.

c) Enter a valid username and password.

After successful authentication, the following message is displayed:

```
SSO Test Succeeded
```

Close the browser window after you see this message.

If the authentication fails, or takes more than 60 seconds to authenticate, a "Login Failed" message appears on the IdP login window. The following message is displayed on the SAML Single Sign-On window:

```
SSO Metadata Test Timed Out
```

To attempt logging in to the IdP again, select another user and run another test.

d) Click **Finish** to complete the SAML SSO setup.

SAML SSO is enabled and all the web applications participating in SAML SSO are restarted. It may take one to two minutes for the web applications to restart.

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.

Verify the SAML SSO Configuration

After you configure SAML SSO on both the Service Provider (Unified Communications Manager) and on the IdP, use this procedure on Unified Communications Manager to confirm that the configuration works.

Before you begin

Confirm the following:

- The **SAML Single Sign-On Configuration** window in Unified CM Administration shows that you have successfully imported the **IdP Metadata Trust** file.
- The Service Provider metadata files are installed on the IdP.

Procedure

Step 1 From the Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On** and the **SAML Single Sign-On Configuration** window opens, click **Next**.

Step 2 Choose an administrative user form the **Valid Administrator Usernames** area and click the **Run SSO Test…** button.

Note
The user for the test must have administrator rights and has been added as a user on the IdP server. The Valid Administrator Usernames area displays a list of users, which can be drawn on to run the test.

If the test succeeds, SAML SSO is successfully configured.