Revised: April 2, 2024

SAML SSO Microsoft Entra ID Identity Provider

SAML SSO Microsoft Entra ID Identity Provider

Revision History

Date	Revision
April 02, 2024	Updated the document to include changes for enhancements to the Microsoft Entra ID Enterprise applications Catalog. • Configure Microsoft Entra ID Catalog Application, on page 4 • Enable SAML SSO for Collaboration Applications, on page 5
June 21, 2022	Added support for clusterwide agreements with Microsoft Entra ID for Unified CM, IM and Presence Service, Unity Connection, and Expressway.

Introduction

This document provides a configuration example of how to configure Microsoft Entra ID as the SAML SSO Identity Provider (IdP) for the following applications:

- Cisco Unified Communications Manager
- IM and Presence Service
- Cisco Unity Connection
- Cisco Expressway

Single sign-on (SSO) is a session or user authentication process that enables a user to provide credentials to access one or more applications. The process authenticates the user for all applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

For detailed information about the SAML SSO Solution, see the *SAML SSO Deployment Guide for Cisco Unified Communications Applications*.

Metadata Requirements

The following condition applies for metadata agreements with Microsoft Entra ID:

- Cisco Unified Communications Manager, IM and Presence Service, Cisco Unity Connection, and Cisco Expressway supports clusterwide agreement with Microsoft Entra ID.

Note Microsoft Entra ID officially supports only the cluster wide agreements and does not recommend per node agreements for SAML SSO.

Metadata Examples

Given the below UC deployment, see the following table for an example of the total number of metadata files that this deployment would give you for export. Note that the IM and Presence Service is deployed in a Standard Deployment, unless otherwise indicated.

- A five-node Cisco Unified Communications Manager cluster
- A three-node IM and Presence Service cluster (Standard deployment)
- A two-node Cisco Unity Connection cluster
- A three-node Expressway-C cluster
- A three-node Expressway-E cluster

Table 1: UC Metadata File Exported

With this type of deployment	These are the XML files that you get...
Expressway is in a Clusterwide agreement	**Example for Clusterwide agreement** You would export three metadata XML files in total: • One metadata XML file for the Unified CM cluster with Unified CM and IM and Presence Service nodes • One metadata XML file for the Unity Connection cluster • One metadata XML file for the Expressway-C cluster
IM and Presence Service is in a Centralized Deployment	If your IM and Presence Service nodes are in a Centralized Deployment, your IM and Presence metadata is exported separately from your Unified CM telephony cluster. This gives you an extra metadata XML file along with one extra metadata file for the standalone Unified CM node that is in the IM and Presence central cluster. This results in either 5 clusterwide XML metadata files in total, depending on the Expressway agreement type: • Unified CM zip contains one XML file (clusterwide) • For IM and Presence, one metadata XML file (clusterwide) and one metadata XML file for the Unified CM publisher node that is in the IM and Presence Service central cluster. • Unity Connection zip contains one XML file (clusterwide) • Expressway generates one Expressway metadata XML file (clusterwide)

Configure Microsoft Entra ID as Identity Provider

Complete these tasks to configure Microsoft Entra ID as your Identity Provider for Cisco Collaboration applications.

Before you begin

Perform a LDAP Directory synchronization. We do not recommend syncing users from the Microsoft Entra ID using LDAP. Instead, we suggest that you use the Cisco Webex Cloud-Connected UC Directory Services.

	Command or Action	Purpose
Step 1	Export UC Metadata File, on page 3	Export metadata file from your Cisco UC applications.
Step 2	Configure Microsoft Entra ID Catalog Application, on page 4	Import the UC metadata file into Microsoft Entra ID and configure Microsoft Entra ID to provide identity services. Export a Federation Metadata File from Microsoft Entra ID.
Step 3	Enable SAML SSO for Collaboration Applications, on page 5	Import the Microsoft Entra ID metadata file into your Cisco UC applications and complete the SSO configuration.

Export UC Metadata File

Before you configure Microsoft Entra ID, you must export UC metadata from your Cisco Collaboration deployment.

Step 1 Export UC metadata from Cisco Unified Communications Manager:

a) From Cisco Unified CM Administration, go to **System** > **SAML Single Sign On**.

b) For the **SSO Mode**, select **Cluster wide** agreement.

c) In the **Certificates** section, choose either **Use Tomcat certificate** or **Use system-generated self-signed certificate**.

d) Click **Export All Metadata** and download the metadata file.

Step 2 If you have deployed the Centralized Deployment for the IM and Presence Service, repeat the previous step on the Unified CM publisher node that is located within your IM and Presence central cluster.

Step 3 Export UC metadata from Cisco Unity Connection:

a) In Cisco Unity Connection Administration, choose **System Settings** > **SAML Single Sign On**.

b) For the **SSO Mode**, select **Cluster wide** agreement.

c) Click **Export All Metadata** and download the metadata file.

Step 4 Export UC metadata from Cisco Expressway.

a) On the Expressway-C primary peer, go to **Configuration** > **Unified Communications** > **Configuration**.

b) In the **MRA Access Control** section, set the **Authentication path** to either **SAML SSO authentication** or **SAML SSO or UCM/LDAP**.

c) Set **SAML Control** to **Cluster**.

d) Click **Export SAML data**.

e) **Download** the metadata file to a secure location.

Configure Microsoft Entra ID Catalog Application

Complete the following procedure for clusterwide agreements in your Cisco Unified Communications Manager, IM and Presence Service, Cisco Unity Connection, and Cisco Expressway deployment.

Step 1 In Microsoft Entra ID at **Enterprise applications | All applications**, click **New Application**.

Step 2 In the **New Application** window, do the following:

a) From the **Gallery Application**, select one of the following products: Cisco Unified Communications Manager, Cisco Unity Connection, or Cisco Expressway.

Note To enable SAML SSO on IM and Presence Service, ensure that you add the IM and Presence Service node to the Unified Communications Manager cluster.

b) Enter the **Name** of your new application (for example, `UnifiedCM_Publisher, UnityConnection_Publisher, or Expressway_cluster`) and click **Create**.

Step 3 In the left navigation bar, click **Single sign-on**.

Step 4 Click **SAML**.
The Set up Single Sign-On with SAML window appears.

Step 5 Click **Upload metadata file** and then browse to the UC metadata XML file for the server for which you are configuring an agreement. After you select and open the file, click **Add**.
The **Basic SAML Configuration** populates with Identifier (EntityID) and Reply URL (Assertion customer service URL) for the Collaboration server.

Step 6 Click **Save**.

Step 7 If necessary, **Edit** the **User Attributes & Claims** section.

Note If the value of **user.onpremisessamaccountname** doesn't match the value that you choose for the **User ID** in the Cisco Unified Communications Manager or Cisco Unity Connection, then you must find a suitable attribute in Entra ID to reflect your chosen value. For example, if **User ID** in Cisco Unified Communications Manager is the Telephone Number, then you must change it to **user.telephoneNumber**.

a) Under **Required claim**, click on **uid**.
b) Leave the **Namespace** field blank.
c) For **Source**, check the **Attribute** radio button.
d) Choose the right attribute from Entra ID for your Cisco Unified Communications Manager or Cisco Unity Connection systems.
e) Click **Save**.

Step 8 Click **SAML-based Sign-on** to return to the SAML summary.

Step 9 **Download** the **Federation Metadata XML** file.

Note You need to do download metadata from the IdP once only for your UC deployment. You can import the same IdP metadata file into all your applications.

Step 10 Enable the Application in Microsoft Entra ID and Assign Users:

Note Microsoft Entra ID provides you with the ability to assign individual users for SSO with Microsoft Entra ID, or all users. For this example, it is assumed that you are enabling SSO for all users.

a) In the left navigation bar, select **Manage** > **Properties**.
b) Set **Enabled for users to sign in?** to **Yes**.
c) Set **Visible to users?** to **No**.

d) Click **Save**.

Enable SAML SSO for Collaboration Applications

Complete the SAML SSO configuration in your Cisco Collaboration environment.

Step 1 Enable SAML SSO on Cisco Unified Communications Manager:

a) From Cisco Unified CM Administration, navigate to **System** > **SAML Single Sign On**.
b) Click **Enable SAML SSO**, then click **Continue** and follow the prompts.
c) Import the IdP Metadata file into the Cisco Unified Communications Manager.
d) Test the SSO connection.
e) Repeat the SSO test connection on each Cisco Unified Communications Manager cluster node.

Step 2 If you have an IM and Presence Centralized Deployment, repeat Step 1 on the Unified CM publisher node that is located in the IM and Presence central cluster.

Step 3 Enable SAML SSO on Cisco Unity Connection:

a) In Cisco Unity Connection Administration, go to **System Settings** > **SAML Single Sign On**.
b) Click **Enable SAML Single Sign On**.
c) Click **Continue** and follow the prompts.
d) Import the IdP metadata file into Cisco Unity Connection.
e) Test the SSO Connection.
f) Repeat the SSO test connection on each Cisco Unity Connection node.

Step 4 Enable SAML SSO on Expressway:

a) On the Expressway-C primary peer, navigate to **Configuration** > **Unified Communications** > **Identity providers (IdP)**.
b) Click **Import new IdP from SAML**.
c) Locate and select the metadata file.
d) Set **Digest** to the required SHA algorithm and click **Upload**.
e) Verify that your Identity Provider appears.
f) Click **Associate domains**.
g) Check each of the domains that you want to associate to this IdP.
h) Click **Save**.

Troubleshooting

For debugging purposes, use a tool like the SAML tracer.

Make sure that the X.509 Certificate data that is sent as part of the SAML assertion matches with the certificate present in your Microsoft Entra ID enterprise application.

Check the ssosp logs for errors. Following is an example of a certificate issue that might appear in the ssosp logs:

```
2020-09-21 05:45:39,131 ERROR [http-bio-8443-exec-51] fappend.SamlLogger - FMSigProvider.verify: The cert
```

```
contained in the document is NOT the same as the one being passed in.
2020-09-21 05:45:39,134 ERROR [http-bio-8443-exec-51] authentication.SAMLAuthenticator - Error while processing
 saml response The signing certificate does not match what's defined in the entity metadata.
com.sun.identity.saml2.common.SAML2Exception: The signing certificate does not match what's defined in the
entity metadata.
at com.sun.identity.saml2.xmlsig.FMSigProvider.verify(FMSigProvider.java:334)
at com.sun.identity.saml2.assertion.impl.AssertionImpl.isSignatureValid(AssertionImpl.java:651)
```