SAML-Based SSO Configuration

Prerequisites

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.

For information about synchronizing clocks, see the NTP Settings section in *Cisco Unified Communications Operating System Administration Guide*.

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 following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/collab10/directry.html

Certificate Management and Validation

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 Cisco 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 Cisco 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 CUCM 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.

High-Level Circle of Trust Setup

To enable SAML SSO across Unified Communications applications, the administrator must establish a Circle of Trust (CoT) between the Service Provider and the IdP. The following steps provide a high-level overview of the procedure.

Procedure

Step 1 Exchange of certificate between the IdP and the Service Provider:

a) Export a CA certificate from the Service Provider.

b) Go to the IdP server and import the CA certificate from the Service Provider.

c) Export a CA certificate from the IdP server.
d) Go to the Service Provider and import the CA certificate from the IdP server.

Note The administrator must ensure that the IdP trusts the certificate contained in the Service Providers metadata. In some instances importing the metadata to the IdP may be sufficient but in other cases the signing certs of the Service Provider certificate must be manually imported into the IdP's certificate trust store.

Step 2 Exchange of metadata between the IdP and the Service Provider:

a) Export the metadata from the IdP.
b) Import the metadata to the Service Provider.
c) Export the metadata from the Service Provider.
d) Go to the IdP server and provision the Service Provider by importing the metadata from the Service Provider.

Step 3 Configure the mandatory attribute uid on the IdP. This attribute must match the LDAP synchronized user id attribute that is used in Unified Communications applications.

Note uid is a mandatory attribute that IdP configures for a given Service Provider. Through this attribute, a Service Provider identifies the identity of an authenticated user. For information about configuring mandatory attribute mapping, refer the IdP product documentation.

Note For SAML SSO to work as expected, the Service Provider and the IdP must be in the same CoT.

Create a Circle of Trust

If there is no existing CoT to add Cisco Unified Communications Manager to, then a CoT must be created before SAML SSO becomes active.

This example uses OpenAM to create a CoT.

Procedure

Step 1 Log in to the OpenAM server user interface.

Step 2 Choose the **Federation** tab and in the Circle of Trust area, click the **New** button.

a) Create a circle of trust by giving a unique name for the IdP CoT. The Service Provider (in our case Cisco Unified Communications Manager) and the IdP should be in same CoT for SAML SSO to work.

Note You will assign the Service Provider and IdP to be in the same CoT in further steps.

Step 3 Create a SAMLv2 Identity Provider on the server.

a) Choose the **Common Tasks** tab and click the **Create Hosted Identity Provider** button to create a hosted IdP.
b) In the **Existing Circle of Trust** drop-down list, choose the CoT created in Step 2.
c) In the Attributes mapping area, set both **Name in Assertion** and **Local Attribute** values to be uid.
d) Click **Configure**.
e) Choose the **Federation** tab and click on the Hosted Entity Provider you created.
f) Browse to the Assertion Content section and in the Certificate Aliases area enter "test" as the **Signing** field value.

Note This is needed for signing SAML assertions with an alias.

Enable SAML SSO through the OpenAM IdP

SAML SSO Enablement

There are three required tasks and one optional task to enable SAML SSO regardless of the IdP used:

- Create a Circle of Trust
- Configure Cisco Unified Communications Manager for SAML SSO Activation
- Configure the IdP. In the following example we will configure OpenAM.
- [Optional] Verify the SAML SSO Configuration

Tip For SAML SSO to work, the Cisco Unified Communications Manager and the IdP (in this case OpenAM) clocks must be synchronized.

Configure Cisco Unified Communications Manager for SAML SSO Activation

Procedure

Step 1 Log in to the **Cisco Unified CM Administration** user interface.

Step 2 Choose **System** > **SAML Single Sign-On** and the **SAML Single Sign-On Configuration** window opens.

Step 3 To enable SAML SSO on the cluster, click on the **Enable SAML SSO** link.

Step 4 In the **Reset Warning** window, click **Continue**.

Note For SAML SSO, Cisco supports these IdPs:

- Microsoft Active Directory Federation Services (AD FS)
- Open Access Manager (OpenAM)
- Ping Federate

Leave the **SAML Single Sign-On Configuration** window open as you will return to it to save the **IdP Metadata Trust** file and to verify a successful configuration.

Open AM is used in the following example.

What to Do Next

If you have not yet created a Circle of Trust, you can do it now or shift tasks while configuring OpenAM. We recommend that the Circle of Trust be created before you configure OpenAM for SAML SSO.

Related Topics

Supported IdPs

Configure OpenAM and Cisco Unified Communications Manager for SAML SSO

This task involves switching actions between the OpenAM IdP server and Cisco Unified Communication Manager nodes.

Before You Begin

Create a Circle of Trust (CoT)

Configure Cisco Unified Communications Manager for SAML SSO

Procedure

Step 1 Log in to the **OpenAM IdP** server and download the metadata trust file.

a) To download the **IdP Metadata Trust** file for the OpenAM IdP server enter one of the following URLs in a browser where *server.example.com* is the FQDN of the OpenAM server and 8443 is the default port number:

- If a single realm is defined on the OpenAM server:

  https://*server.example.com*:8443/openam/saml2/jsp/exportmetadata.jsp.

- If multiple realms are defined on the OpenAM server:

  https://*server.example.com*:8443/openam/saml2/jsp/exportmetadata.jsp?entityid=

  https://*server.example.com*:8443/openam&realm=realm-name

  Note The two lines above (combined), are the complete URL for multiple realms.

Step 2 Access the **Cisco Unified CM Administration** user interface, and perform the following tasks:

a) Save the **IdP Metadata Trust** file and import it to the Cisco Unified Communications Manager node. If the import is successful, the **SAML Single Sign-On Configuration** window opens.

1. In the Import the IdP Metadata Trust File area, click **Browse** to locate the IdP Metadata Trust file.
2. Click the **Import IdP Metadata** button.
   Note If the import is successful, check marks appear announcing that the import is successful for all nodes.
3. Click **Next**.

b) Download the **Server Metadata** for the Cisco Unified Communications Manager nodes in the cluster to a convenient place in the local file system.

1. Click the **Download Trust Metadata File** link, and the **Opening SPMetadata** dialog box opens.
2. Save the compressed files locally.

3 Unzip the Metadata file folder. When the folder is unzipped, there will be one Metadata file for each node in the cluster.

Step 3 Access the OpenAM server user interface and upload the Metadata files for each node in the cluster.

Note If there is no existing CoT, to which the Cisco Unified Communications Manager is to be added, then a CoT must be created before you proceed to the next steps. See the **Create a Circle of Trust** task.

Step 4 Once the CoT has been created, the Cisco Unified Communications Manager node(s) need to be added as Entity providers. To do this:

a) In the OpenAM server user interface, choose the **Federation** tab and in the Entity Providers section click the **Import Entity..** button to import the Cisco Unified Communications Manager metadata file (*server*.xml), where *server* is the name of the Cisco Unified Communications Manager node.

b) Click **Save**.

c) Click on the entity imported in Step 3a, go to the Assertion Processing section, and add a mapping attribute for uid as per the Directory and OpenAM settings.

Note uid is a mandatory attribute that has to be configured on the IdP for a given Service Provider. This is how the Service Provider identifies an Authenticated user. While adding the uid attribute, you must map it to the correct attribute depending on the Directory/User store settings.

d) Repeat steps 3a-3c for any other nodes in the cluster, which need to be SAML SSO enabled.

e) Choose the **Federation** tab and click the **Circle of Trust** you added.

f) In the Entity Providers section, move the IdP(OpenAm server) and any Cisco Unified Communications Manager entities from the Available to the Selected sections.

This assigns the IdP server and Cisco Unified Communications Manager node(s), to the same CoT.

Step 5 In the OpenAM server you will also need to add a user whose credentials match the administrator level user, which were used to enable SSO on the Cisco Unified Communications Manager.

a) Choose **Access Control** > **(Top Level Realm)Subject** and add the administrator level user.

Once the OpenAM server and Cisco Unified Communications Manager node(s) have been configured, you can verify a successful enablement of SAML SSO on the **Cisco Unified CM Administration** user interface.

What to Do Next

Verify the SAML SSO Configuration.

Verify the SAML SSO Configuration

Before You Begin

- You have installed the required server metadata files on the IdP.
- The **SAML Single Sign-On Configuration** window under the **Cisco Unified CM Administration** user interface shows that you have successfully imported the **IdP Metadata Trust** file.

Procedure

Step 1 On the **Cisco Unified CM Administration** user interface, 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, then SAML SSO has been successfully configured.

Reconfigure OpenAM SSO to SAML SSO

Cisco currently offers the following types of Single Sign-On (SSO) solutions:

- OpenAM SSO (Release 8.6 and later)
- SAML SSO (Release 10.0(1) and later)

Cisco collaboration applications favor SAML SSO over the proprietary OpenAM SSO solution because OpenAM is complex in nature and the deployment does not scale as per the customers' requirements.

Note From release 10.0(1) and later, Agent Flow SSO is not compatible with FIPS mode.

To reconfigure OpenAM SSO to SAML SSO, the administrator must create a new federation service and service account. For SAML SSO to work as expected, the service provider and IdP must be in the same Circle of Trust (CoT). The administrator needs to configure a trust relationship between the service provider and IdP. The following steps describe the configuration of OpenAM SSO to SAML SSO on Cisco Unified Communications Manager.

In this case, you continue to use OpenAM as the IdP, however OpenAM must be reconfigured to SAML.

Before You Begin

- Make sure the OpenAM SSO that is deployed using Agent Flow is installed and operational.
- For SAML SSO to work, the Cisco Unified Communications Manager and OpenAM clocks must be synchronized with each other.

Procedure

Step 1 Disable OpenAM Agent Flow mode of operation on all servers where it is enabled by using CLI commands.

Note Refer to the respective Cisco Unified Communications product documents to get the list of the required CLI commands.
You must disable a previously configured OpenAM SSO solution as only one SSO deployment is allowed at a time.

Step 2 Enable SAML SSO on those servers.
Note Refer to the respective Cisco Unified Communications product documents on how to enable SAML SSO.

Step 3 Log in to the OpenAM server user interface.

Step 4 Choose the **Federation** tab and under Circle of Trust, click **New**.

Step 5 Create a CoT by entering a unique name for the IdP Circle of Trust.

Step 6 To create a hosted IdP, choose the **Common Tasks** tab and click **Create hosted Identity Provider**.

Step 7 Use the default values for other parameters and click **Save**.
Note You can view the circle of trust that you created in the Circle of Trust section.

Step 8 Choose the **Federation** tab and under the Entity Providers section, click the **Hosted Identity Provider** you created.

Step 9 Choose the **Assertion Content** tab and under the Certificate Aliases section, enter <test> as an alias for signing SAML assertions in the **Signing** field .

Step 10 Choose the **Federation** tab, and in the Entity Providers section, click **Import Entity**.

Step 11 Upload the Cisco Unified Communications Manager metadata file (sp.xml), and click **Save**.
Note The metadata file upload fails if the metadata is signed. In such cases, add the Cisco Unified Communications Manager tomcat certificate to openAMKeystore. Follow the procedure below.

1. Download the tomcat certificate (tomcat.pem) from the **Cisco Unified Communications Manager OS Administration** page and the upload the certificate to a location in OpenAM server. For example, `/temp/tomcat.pem`
2. Run the following command in OpenAM:
   keytool -import -v -alias *aliasname* **-keystore**
   /root/openam/openam/keystore.jks -trustcacerts -file
   location_of_cucm_tomcat_cert
3. Enter the password as <changeit>.
4. A dialog box appears asking whether you trust the certificate, click **Yes**.
   The following message is displayed:
   ```
   Certificate was added to keystore
   [Storing /root/openam/openam/keystore.jks]
   ```
5. Restart the tomcat in OpenAM and try to upload the sp.xml metadata file again.
6. Choose **File** during Entity provider upload.

Note Cisco Unified Communications Manager supports metadata upload only through the File option.

Step 12 Choose the entity imported in Step 10.

Step 13 Choose the **Assertion Processing** tab and add a mapping attribute for uid as per the Directory and OpenAM settings.
Note While adding the uid attribute, map it to the correct attribute depending on the Directory/User store settings. For example, you can enter uid=sAMAccountName or uid=mail or uid=uid.

Step 14 Choose the **Federation** tab, and click **Circle of Trust**.

Step 15 To assign the IdP and the Cisco Unified Communications Manager to be in the same CoT: in the Entity Providers area, move the IdP (OpenAM server) and the Cisco Unified Communications Manager entities from the **Available** section to the **Selected** section.
The OpenAM server is successfully configured as IdP.