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

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 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 6	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	Verify the SAML SSO Configuration, on page 8	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 Cisco recommends 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.

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 Unified Communications Manager Administration Guide

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.

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.

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.

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. The CUCM downloads the regenerated metadata file and uploads to the IdP.