Manage SAML Single Sign-On

SAML Single Sign-On Overview

Use SAML Single Sign-On (SSO) to access a defined set of Cisco applications 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 (such as Cisco Unified Communications Manager) to authenticate a user. With SAML, security authentication information is exchanged between an identity provider (IdP) and a service provider. The feature provides secure mechanisms to use common credentials and relevant information across various 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 user information of the IdP to provide access to the various services or applications.

The client authenticates against the IdP, and the IdP grants an Assertion to the client. The client presents the assertion to the service provider. Because a CoT established, the service provider trusts the assertion and grants access to the client.

Opt-In Control for Certificate-Based SSO Authentication for Cisco Jabber on iOS

This release of Cisco Unified Communications Manager introduces the opt-in configuration option to control Cisco Jabber on iOS SSO login behavior with an Identity provider (IdP). Use this option to allow Cisco Jabber to perform certificate-based authentication with the IdP in a controlled mobile device management (MDM) deployment.

You can configure the opt-in control through the **SSO Login Behavior for iOS** enterprise parameter in Cisco Unified Communications Manager.

Note Before you change the default value of this parameter, see the Cisco Jabber feature support and documentation at http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html to ensure Cisco Jabber on iOS support for SSO login behavior and certificate-based authentication.

To enable this feature, see the Configure SSO Login Behavior for Cisco Jabber on iOS, on page 3 procedure.

SAML Single Sign-On Prerequisites

- DNS configured for the Cisco Unified Communications Manager cluster
- An identity provider (IdP) server
- An LDAP server that is trusted by the IdP server and supported by your system

The following IdPs using SAML 2.0 are tested for the SAML SSO feature:

- OpenAM 10.0.1
- Microsoft® Active Directory® Federation Services 2.0 (AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIP-IP 11.6.0

The third-party applications must meet the following configuration requirements:

- The mandatory attribute “uid” must be configured on the IdP. This attribute must match the attribute that is used for the LDAP-synchronized user ID in Cisco Unified Communications Manager.
- The clocks of all the entities participating in SAML SSO must be synchronized. For information about synchronizing clocks, see “NTP Settings” in the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Manage SAML Single Sign-On

Enable SAML Single Sign-On

Note You cannot enable SAML SSO until the verify sync agent test succeeds.

Before you begin

- Ensure that user data is synchronized to the Unified Communications Manager database. For more information, see the *System Configuration Guide for Cisco Unified Communications Manager* at

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

- Verify that the Cisco Unified CM IM and Presence Service Cisco Sync Agent service successfully completed data synchronization. Check the status of this test by choosing **Cisco Unified CM IM and Presence Administration** > **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 successfully completed.
- Ensure that at least one LDAP synchronized user is added to the Standard CCM Super Users group to enable access to Cisco Unified CM Administration. For more information, see the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.
- 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.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On**.
Step 2 Click **Enable SAML SSO**.
Step 3 After you see warning message to notify you that all server connections will be restarted, click **Continue**.
Step 4 Click **Browse** to locate and upload the IdP metadata file.
Step 5 Click **Import IdP Metadata**.
Step 6 Click **Next**.
Step 7 Click **Download Trust Metadata Fileset** to download server metadata to your system.
Step 8 Upload the server metadata on the IdP server.
Step 9 Click **Next** to continue.
Step 10 Choose an LDAP synchronized user with administrator rights from the list of valid administrator IDs.
Step 11 Click **Run Test**.
Step 12 Enter a valid username and password.
Step 13 Close the browser window after you see the success message.
Step 14 Click **Finish** and allow 1 to 2 minutes for the web applications to restart.

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**.

Enable SAML Single Sign-On on WebDialer After an Upgrade

Follow these tasks to reactivate SAML Single Sign-On on Cisco WebDialer after an upgrade. If Cisco WebDialer is activated before SAML Single Sign-On is enabled, SAML Single Sign-On is not enabled on Cisco WebDialer by default.

Procedure

	Command or Action	Purpose
Step 1	Deactivate the Cisco WebDialer Service, on page 4	Deactivate the Cisco WebDialer web service if it is already activated.
Step 2	Disable SAML Single Sign-On, on page 5	Disable SAML Single Sign-On if it is already enabled.
Step 3	Activate the Cisco WebDialer Service, on page 5	
Step 4	Enable SAML Single Sign-On, on page 2	

Deactivate the Cisco WebDialer Service

Deactivate the Cisco WebDialer web service if it is already activated.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Servers** drop-down list, choose the Cisco Unified Communications Manager server that is listed.

Step 3 From **CTI Services**, uncheck the **Cisco WebDialer Web Service** check box.

Step 4 Click **Save**.

What to do next

Disable SAML Single Sign-On, on page 5

Disable SAML Single Sign-On

Disable SAML Single Sign-On if it is already enabled.

Before you begin

Deactivate the Cisco WebDialer Service, on page 4

Procedure

From the CLI, run the command **utils sso disable**.

What to do next

Activate the Cisco WebDialer Service, on page 5

Activate the Cisco WebDialer Service

Before you begin

Disable SAML Single Sign-On, on page 5

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Servers** drop-down list, choose the Unified Communications Manager server that is listed.

Step 3 From **CTI Services**, check the **Cisco WebDialer Web Service** check box.

Step 4 Click **Save**.

Step 5 From Cisco Unified Serviceability, choose **Tools** > **Control Center - Feature Services** to confirm that the CTI Manager service is active and is in start mode.

For WebDialer to function properly, the CTI Manager service must be active and in start mode.

What to do next

Enable SAML Single Sign-On, on page 2

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 Server Metadata After Deleting a Server

After a server is deleted from the cluster in a clusterwide SSO integration, re-import of metadata is mandatory to avoid index mismatch with IdP.

Before you begin

Note 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.

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"/>`