

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Network Time Protocol \(NTP\) Setup](#)

[Domain Name Server \(DNS\) Setup](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[Directory Setup](#)

[Enable SAML SSO](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how to configure and verify Security Assertion Markup Language (SAML) Single Sign-on (SSO) for Cisco Unified Communications Manager (CUCM).

Prerequisites

Requirements

Network Time Protocol (NTP) Setup

For SAML SSO to work, you must install the correct NTP setup and make sure that the time difference between the Identity Provider (IdP) and the Unified Communications applications does not exceed three seconds.

If there is a time mismatch between CUCM and IdP, you receive this error: "Invalid SAML response." This error might be caused when time is out of sync between the CUCM and IdP servers. 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 three seconds.

For information about how to synchronize clocks, refer to the NTP Settings section in [Cisco Unified Communications Operating System Administration Guide](#).

Domain Name Server (DNS) Setup

Unified Communications applications can use DNS in order to resolve Fully Qualified Domain Names (FQDNs) to IP addresses. The Service Providers and the IdP must be resolvable by the browser.

Components Used

The information in this document is based on these software and hardware versions:

- Active Directory Federation Service (AD FS) Version 2.0 as IdP
- CUCM Version 10.5 as Service Provider
- Microsoft Internet Explorer 10

Caution: This document is based on a newly-installed CUCM. If you configure SAML SSO on an already-in-production server, you might have to skip some of the steps accordingly. You must also understand the service impact if you perform the steps on the production server. It is recommended to perform this procedure during non-business hours.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

SAML is an XML-based, open-standard data format that enables administrators to access a defined set of Cisco collaboration applications seamlessly after they sign into one of those applications. SAML SSO establishes a Circle of Trust (CoT) when it exchanges metadata 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.

Note: Service Providers are no longer involved in authentication. SAML Version 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.

Configure

Network Diagram

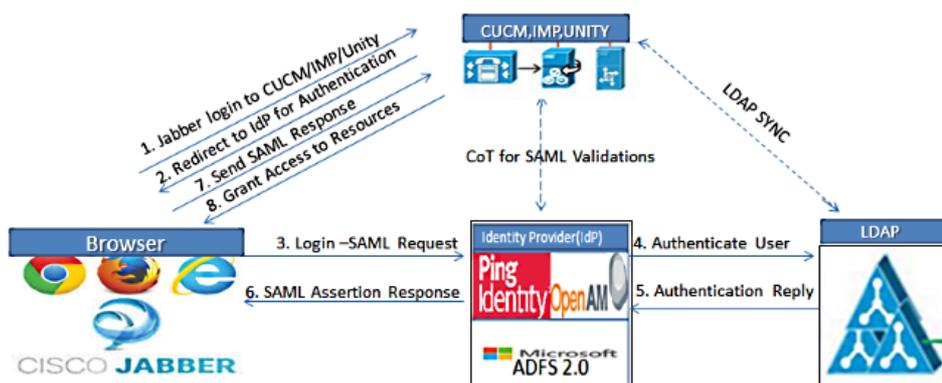
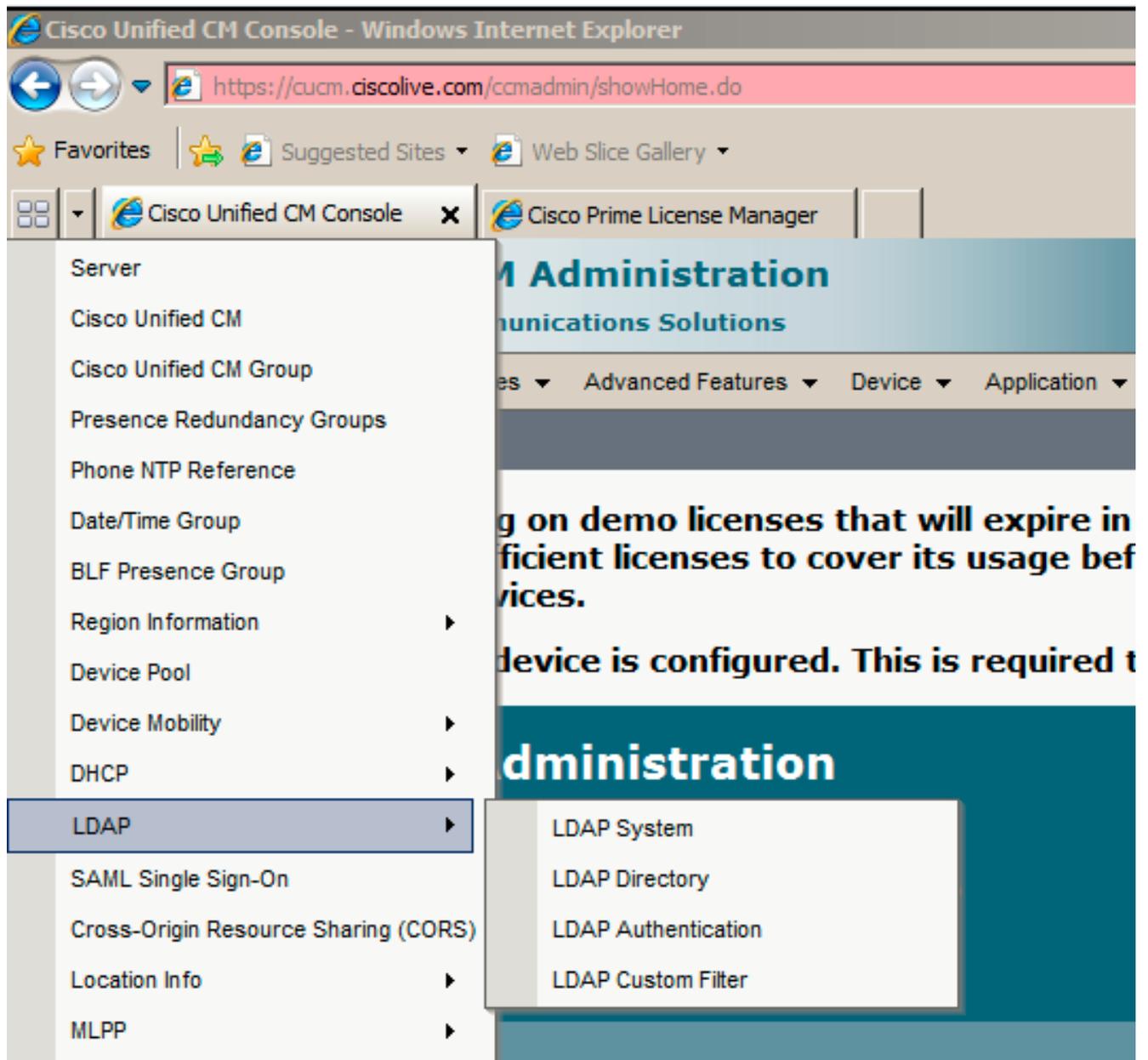


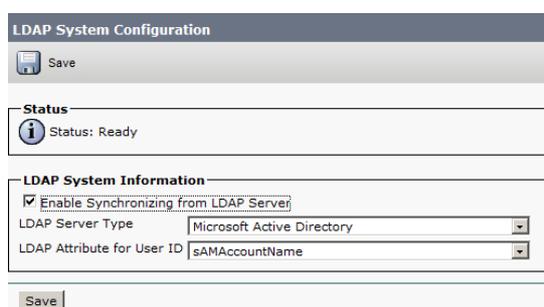
Figure :SAML Single sign SSO Call Flow for Collaboration Servers

Directory Setup

1. Choose **Cisco Unified CM Administration > System > LDAP > LDAP System**.



2. Click **Add New**.
3. Configure the Lightweight Directory Access Protocol (LDAP) server type and attribute.
4. Choose **Enable Synchronizing from LDAP Server**.



5. Choose **Cisco Unified CM Administration > System > LDAP > LDAP Directory**.

6. Configure these items:

LDAP directory account settings
User attributes to be synchronized
Synchronization schedule
LDAP server hostname or IP address and port number

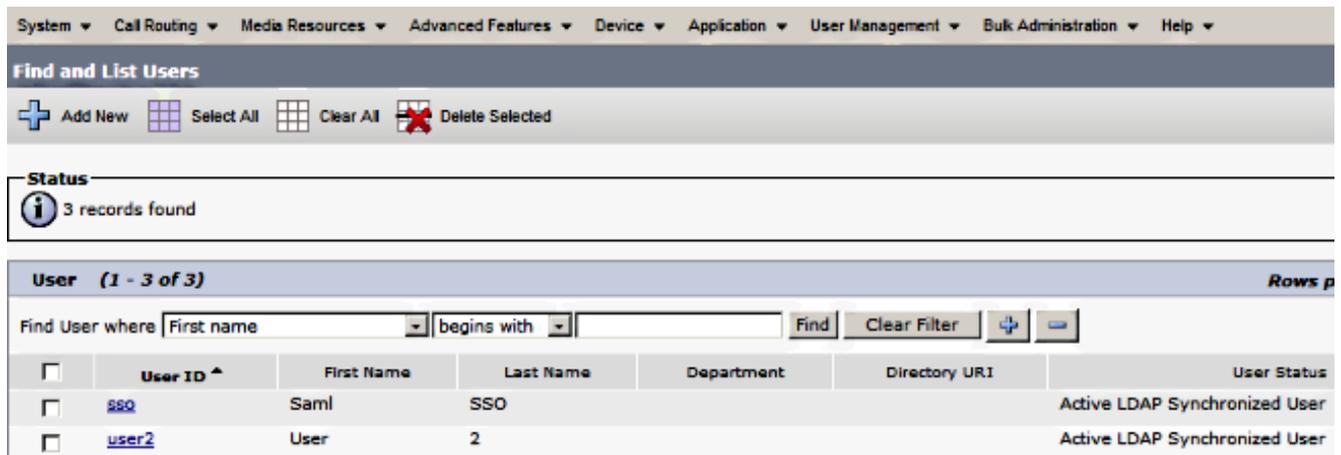
7. Uncheck **Use SSL** if you do not want to use Secure Socket Layer (SSL) in order to communicate with the LDAP directory.

Tip: If you want to configure LDAP over SSL, upload the LDAP directory certificate onto CUCM. See the LDAP directory content in [Cisco Unified Communications Manager SRND](#) for information about the account synchronization mechanism for specific LDAP products and general best practices for LDAP synchronization.

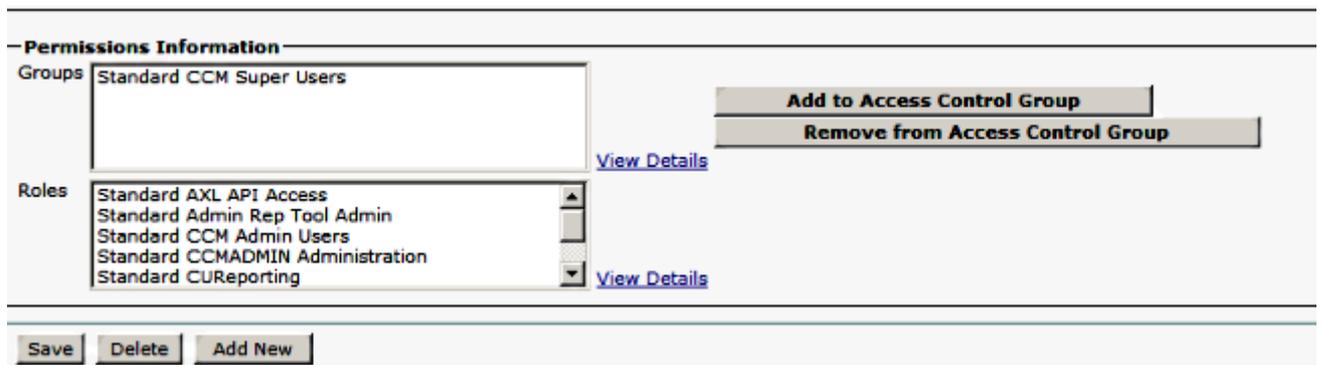
8. Click **Save** and then **Perform Full Sync Now**.

Note: Make sure **Cisco DirSync** service is enabled in the Serviceability web page before you click Save.

9. Navigate to **User Management > End User**, and select a user to whom you want to give the CUCM Administrative role (this example selects user **SSO**).

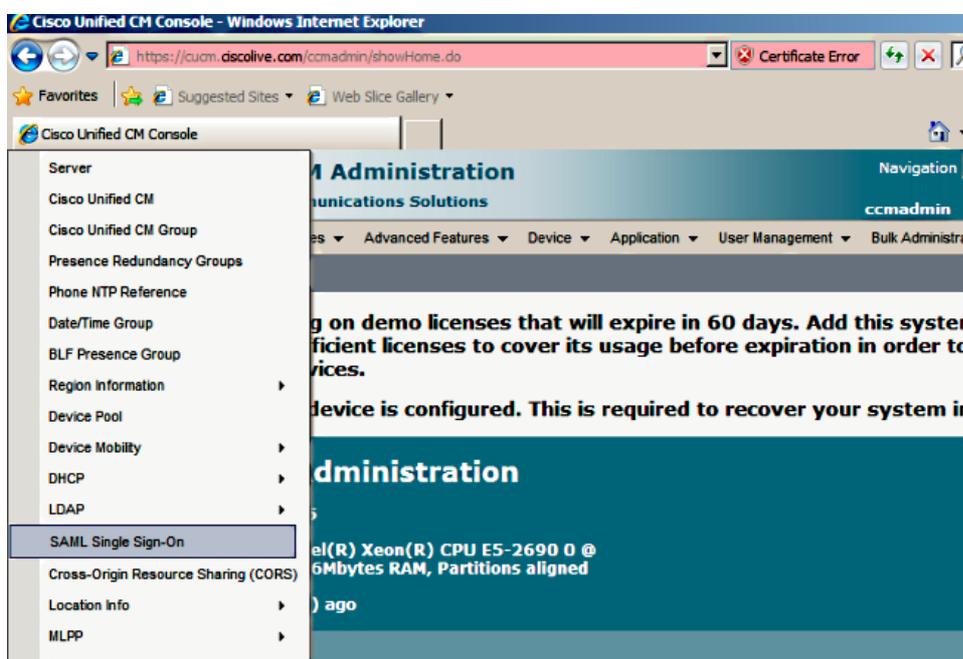


10. Scroll down to the Permissions Information and click **Add to Access Control Group**. Select **Standard CCM Super Users**, click **Add Selected**, and click **Save**.



Enable SAML SSO

1. Log into the CUCM Administration user interface.
2. Choose **System > SAML Single Sign-On** and the SAML Single Sign-On Configuration window opens.



3. In order to enable SAML SSO on the cluster, click **Enable SAML SSO**.

SAML Single Sign-On

Enable SAML SSO Export All Metadata Update IdP Metadata File Fix All Disabled Servers

Status

SAML SSO disabled

SAML Single Sign-On (1 - 2 of 2) Rows per Page: 50

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
CUCM	Disabled	N/A	Never	File	March 30, 2011 7:57:56 PM CEST	Never

Run SSO Test...

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

Web server connections will be restarted

Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again.

Click "Export All Metadata" button

If the server metadata has not already been uploaded to the IdP, it can be done before running the wizard. You can obtain the server metadata by clicking the "Export All Metadata" button on the main page. Then go to the IdP and upload the file.

Continue Cancel

5. On the SSO screen, click **Browse** in order to import the IdP (**FederationMetadata.xml**) metadata XML file with the **Download IdP Metadata** step.

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

SAML Single Sign-On Configuration

Next

Status

Status: Ready

Download Identity provider(IdP) Metadata Trust File

To configure the trust relationship between the IdP and your devices, you must first obtain trust metadata from your IdP and import it to your servers. You will need to manually obtain the file from the IdP before you can upload it to your Collaboration servers.

This is a manual step

1)Log in to your IdP and download the metadata trust file to your local server.
2)Click 'Next' once you have this file available locally.

Next Cancel

6. Once the metadata file is uploaded, click **Import IdP Metadata** in order to import the IdP information to CUCM. Confirm that the import was successful and click **Next** in order to continue.

System ▾ Cal Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

SAML Single Sign-On Configuration

Next

Status
Ready to import Identity Provider metadata trust file to cluster servers

Import the IdP Metadata Trust File
This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.
1) Select the IdP Metadata Trust File
C:\Users\Administrator\Desktop\FederationMetadata.xml

2) Import this file to the Collaboration servers
This action must be successful for at least the Publisher before moving on to the next task in this wizard.

Next

SAML Single Sign-On Configuration

Next

Status
Import succeeded for all servers

Import the IdP Metadata Trust File
This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.
1) Select the IdP Metadata Trust File

2) Import this file to the Collaboration servers
This action must be successful for at least the Publisher before moving on to the next task in this wizard.

Import succeeded for all servers

Next

7. Click **Download Trust Metadata File** (optional) in order to save the CUCM and the CUCM IM and Presence metadata to a local folder and go to [Add CUCM as Relying Party Trust](#). Once the AD FS configuration is completed, proceed to Step 8.

SAML Single Sign-On Configuration

Back Next

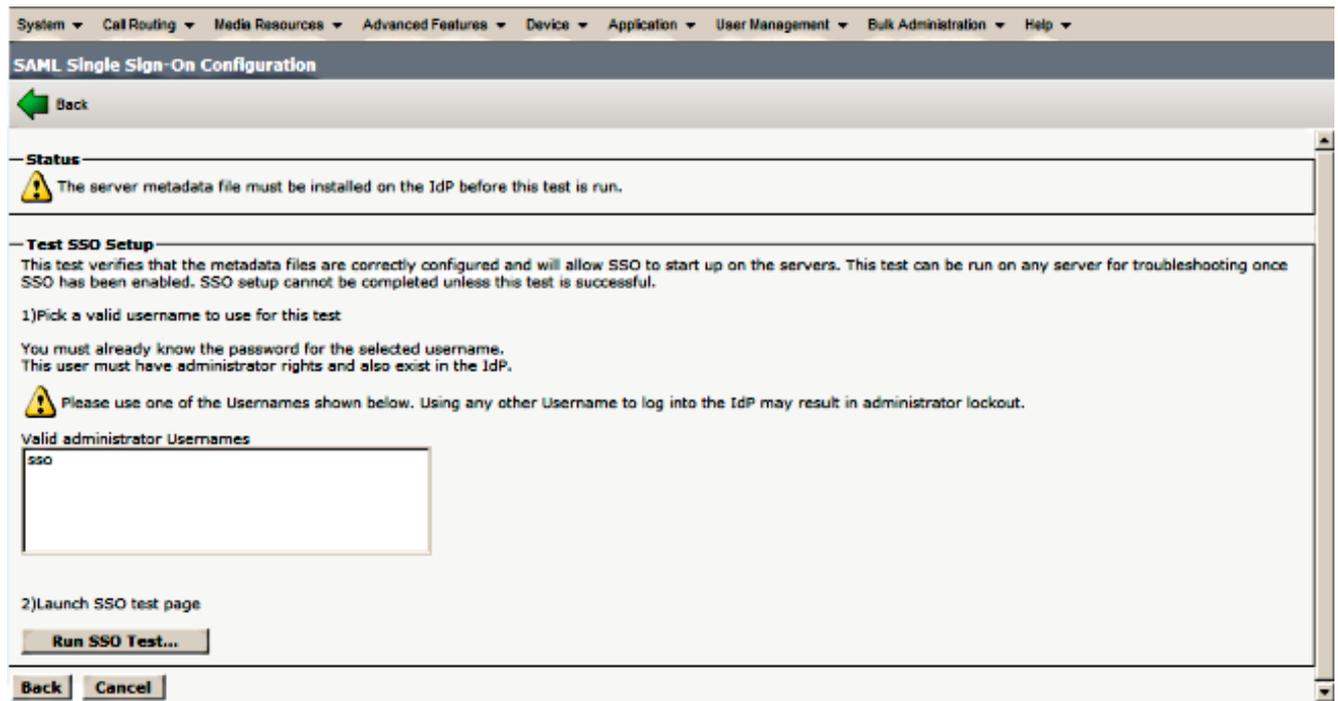
Status
If Admin has already uploaded the server metadata to IdP then skip the steps below and click Next. Otherwise follow the steps below to upload the server metadata to IdP
IdP Metadata has been imported to servers in this cluster

Download Server Metadata and install on the IdP
Download the metadata trust file from Collaboration servers and manually install it on the IdP server to complete SSO setup.
1) Download the server metadata trust files to local storage

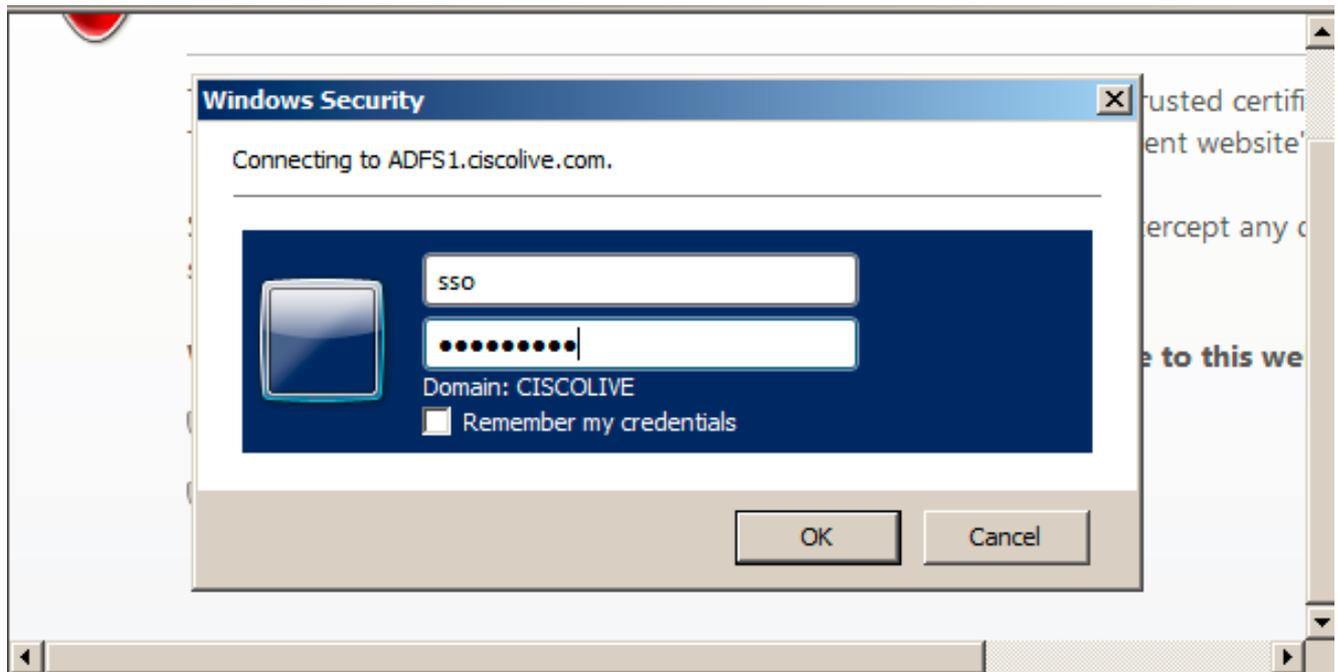
⚠ This is a manual step!
2) Log in to your IdP and upload the server metadata trust file.
3) Click 'Next' once you have installed the server metadata on the IdP.

Back

8. Select **SSO** as the administrative user and click **Run SSO Test**.

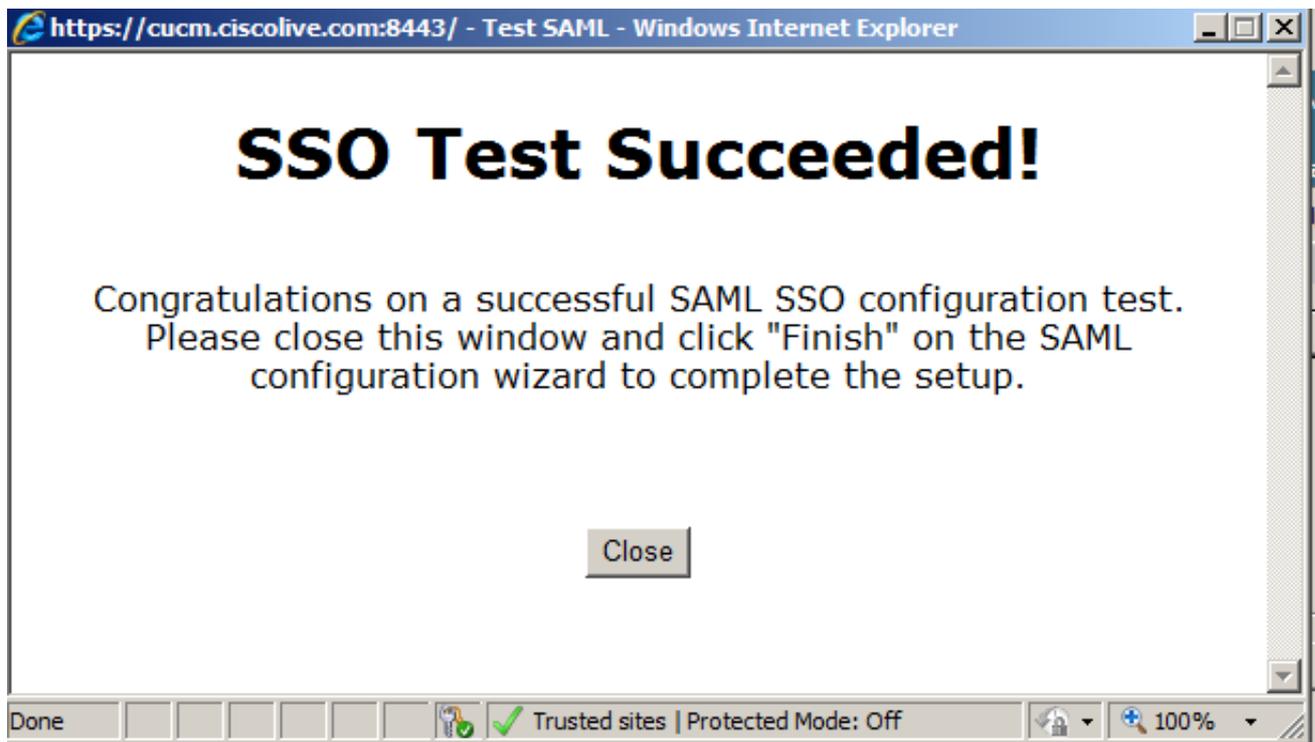


9. Ignore Certificate Warnings and proceed further. When you are prompted for credentials, enter the username and password for user **SSO** and click **OK**.



Note: This configuration example is based on CUCM and AD FS self-signed certificates. In case you use Certificate Authority (CA) certificates, appropriate certificates must be installed on both AD FS and CUCM. Refer [Certificate Management and Validation](#) for more information.

10. After all steps are complete, the "SSO Test Succeeded!" message displays. Click **Close** and **Finish** to continue. You have now successfully completed the configuration tasks in order to enable SSO on CUCM with AD FS.



11. Since CUCM IM and Presence acts like the CUCM Subscriber, you must configure [Add CUCM IM and Presence as Relying Party Trust](#) and then run **Run SSO Test** in order to enable SAML SSO from the CUCM SAML SSO page itself.

Note: If you configure all nodes' metadata XML files on IdP and you enable SSO operation on one node, then SAML SSO is enabled on all of the nodes in the cluster.

AD FS must be configured for all of the nodes of CUCM and CUCM IM and Presence in a cluster as Relaying Party.

Tip: You should also configure Cisco Unity Connection and CUCM IM and Presence for SAML SSO if you want to use the SAML SSO experience for Cisco Jabber Clients.

Verify

Use this section in order to confirm that your configuration works properly.

1. Open a web browser and enter the FQDN for CUCM.
2. Click **Cisco Unified Communications Manager**.
3. Select the webapp (**CM Administration/Unified Serviceability/ Cisco Unified Reporting**) and press **Go**, then you should be prompted for credentials by the AD FS. Once you enter the credentials of user **SSO**, you are successfully logged into the selected webapp (**CM Administration pag , Unified Serviceability page, Cisco Unified Reporting**).



Note: SAML SSO does not enable access to these pages:

- Prime Licensing Manager
- OS Administration
- Disaster Recovery system

Troubleshoot

If you are not able to enable SAML and you are not able to log in, use the new option under Installed Applications called **Recovery URL to bypass Single Sign-on (SSO)**, which can be used in order to log in with the credentials created during installation or locally-created CUCM Administrative users.

Cisco Unified CM Console - Windows Internet Explorer

https://cucm.discofive.com/ccadmin/showRecovery.do Certificate Error Bing

Cisco Unified CM Console

Cisco Single Sign On Recovery Administration
For Cisco Unified Communications Solutions

Cisco Single Sign On Recovery Administration

This page will validate credentials locally, allowing access only to applications that are running on this server, and will not leverage SAML SSO authentication.

This page can be disabled through the CLI.

Username
ccadmin

Password

Login Reset

Copyright © 1999 - 2015 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.

For further troubleshooting, refer to [Troubleshooting SAML SSO for Collaboration Products 10.x](#).