Unified Communications Manager Version 10.5 SAML SSO Configuration Example

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 <u>Cisco</u> <u>Unified Communications Operating System Administration Guide</u>.

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.

| LDAP System Configurat | tion | |
|----------------------------|----------------------------|--|
| Save | | |
| | | |
| Status | | |
| i Status: Ready | | |
| | | |
| -LUAP System Informati | ion | |
| Enable Synchronizing fr | rom LDAP Server | |
| LDAP Server Type | Microsoft Active Directory | |
| LDAP Attribute for User ID | sAMAccountName | |
| | | |
| | | |
| Save | | |

- 5. Choose Cisco Unified CM Administration > System > LDAP > LDAP Directory.
- 6. Configure these items:

LDAP directory account settingsUser attributes to be synchronizedSynchronization scheduleLDAP server hostname or IP address and port number

| LDAP Directory | | | | | | | | | | |
|----------------------------------|---|--|--|--|--|--|--|--|--|--|
| 🕞 Save 🗙 Delete 📄 Copy 👔 | Perform Full Sync Now 🕂 Add New | | | | | | | | | |
| | | | | | | | | | | |
| Status: Ready | | | | | | | | | | |
| | | | | | | | | | | |
| LDAP Configuration Name* | LDAP | | | | | | | | | |
| LDAP Manager Distinguished Name* | CN=Administrator,CN=Users,DC=ciscolive,DC=com | | | | | | | | | |
| LDAP Password* | ••••• | | | | | | | | | |
| Confirm Password* | ••••• | | | | | | | | | |
| LDAP User Search Base* | CN=Users,DC=ciscolive,DC=com | | | | | | | | | |
| LDAP Custom Filter | < None > | | | | | | | | | |

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 <u>Cisco Unified Communications Manager</u> <u>SRND</u> 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.

| Host Name or IP Address for Server* | LDAP Port* Use SSI |
|-------------------------------------|--------------------|
| adfs1.ciscolive.com | 3268 |
| Add Another Redundant LDAP Server | |

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**).

| System + | Call Routing 👻 Medi | a Resources 👻 Advar | nced Features 👻 Device | Application | User Management 👻 | Bulk Administration 👻 | Help 👻 | | | |
|------------------|--|---------------------|------------------------|-------------|----------------------------------|-----------------------|---|--|--|--|
| Find and | l List Users | | | | | | | | | |
| | New Estect All | 🔛 Clear All 💥 D | elete Selected | | | | | | | |
| Status 3 re | Status 3 records found | | | | | | | | | |
| | | | | | | | | | | |
| User | (1 - 3 of 3) | | | | | | Rows p | | | |
| User Find Use | (1 - 3 of 3) r where First name | • Þ | egins with 💽 | 1 | Find Clear Filter | 4 - | Rows p | | | |
| User Find Use | (1 - 3 of 3) r where First name User ID * | First Name | egins with 💽 | Department | Find Clear Filter | | Rows p User Status | | | |
| User Find Use | (1 - 3 of 3) r where First name User ID • SSO | First Name Sami | egins with I | Department | Find Clear Filter Directory U | RI Active LDA | <i>Rows p</i> User Status P Synchronized User | | | |

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.

| Standard CCM Super Users | | |
|----------------------------------|--|---|
| | | Add to Access Control Group |
| | | Remove from Access Control Group |
| | View Details | |
| Standard AXL API Access | | |
| Standard Admin Rep Tool Admin | - | |
| Standard CCM Admin Users | _ | |
| Standard CURADMIN Administration | T Mary Datalla | |
| | Standard AXL API Access Standard Admin Rep Tool Admin Standard CCM Admin Users Standard CCMADMIN Administration Standard CUReporting | Standard AXL API Access Standard AXL API Access Standard Admin Rep Tool Admin Standard CCM Admin Users Standard CCMADMIN Administration Standard CUReporting View Details |

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-C | n | | | | | | | | | | |
|--------------------|--------------|------------------------|---------------------------|-----------------|--------------------------------|-----------------------|--|--|--|--|--|
| Enable SAML SSO | Export All M | etadata 🔞 Update KIP I | Aetadata File 🥜 Fix All D | isabled Servers | | | | | | | |
| -Status- | Status | | | | | | | | | | |
| (1) SAML SSO disab | led | | | | | | | | | | |
| | | | | | | | | | | | |
| 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.

| https://cucm.ciscolive.com/?windowtitlekey=genericdialogwindow.windowtitle.ssoenablewindowtitle 💻 🗖 | × |
|--|-------|
| | - |
| 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 | |
| | - |
| Done 🖉 👘 🗸 Trusted sites Protected Mode: Off 🛛 🖓 👻 🔍 100% | • //. |

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 Sir | gle Sign-On | Configuration | | | | | | | | |
| Next | | | | | | | | | | |
| -Status- | | | | | | | | | | |
| (i) State | us: Ready | | | | | | | | | |
| - Downloa To config manually | - 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 upoled it to your Collaboration servers. | | | | | | | | | |
| 🔥 This | is a manual st | epi | | | | | | | | |
| 1)Log in t | o your IdP and | download the meta | data trust file to your l | ocal server. | | | | | | |
| 2)Click 'N | lext' once you h | have this file availab | le 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 Resourc | es 🔻 | Advance | ed Features | - Devic | * * | Application + | User | Nanagement + | Bulk Administration | • | Help 🛨 |
|------------|--------|------------|-------|------------------|----------|------------|----------------|----------|----------------|---------------|---------------|-------------------------|---------------------|---|--------|
| SAML Sin | ngle | Sign-C |)n C | onfiguratio | n | | | | | | | | | | |
| Next | | | | | | | | | | | | | | | |
| r | | | | | | | | | | | | | | | |
| -Status- | | | | | | | | | | | | | | | |
| Read | dy to | import | Ide | ntity Provider | meta | idata trus | t file to clus | ter serv | ers | | | | | | |
| -Import | the | IdP Me | tad | ata Trust Fi | e— | | | | | | | | | | |
| This step | uplo | ads the | file | acquired from | n the | IdP in the | e previous r | nanual s | tep to | o the Collabo | ration s | ervers. | | | |
| 1)Select t | the I | dP Meta | data | a Trust File | | | | | | | | | | | |
| C:\Users | s∖Adn | ninistrat | or\[| Desktop\Fede | ration | Metadata | uxmi | | | Browse | | | | | |
| 2)Import | this | file to th | ie C | ollaboration : | erve | rs | | | | | | | | | |
| This actio | on mu | ust be s | ucce | assful for at le | ast th | he Publish | er before n | noving o | n to t | he next task | in this v | vizard. | | | |
| Im | port | IdP Me | tad | lata | | | | | | | | | | | |
| Next | Cane | el | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |
| SAML Si | ngle | Sign-(|)n (| Configuratio | n | | | | | | | | | | |
| Next | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |
| Status | | | | | | | | | | | | | | | |
| V Imp | port s | ucceede | ed fo | or all servers | | | | | | | | | | | |
| Transat | the | | t a d | ata Trust Fi | Ia — | | | | | | | | | | |
| This step | o uplo | ads the | file | acquired from | n the | IdP in the | e previous i | manual s | tep to | o the Collabo | ration s | ervers. | | | |
| 1)Select | the I | dP Meta | dəti | a Trust File | | | | | | | | | | | |
| | | | | | | | | | | Browse | | | | | |
| | | | | | | | | | | | | | | | |
| 2)Import | t this | file to t | he C | Collaboration | serve | rs | | | | | in the second | | | | |
| This actio | on m | ust De s | uco | essiul for at le | seist ti | ne Publisi | ver berore r | noving o | n to t | me next task | in this v | vizard. | | | |

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 <u>Add CUCM as Relying Party Trust</u>. Once the AD FS configuration is completed, proceed to Step 8.

Import succeeded for all servers

| SAML Single Sign-On Configuration |
|--|
| de Back 🕪 Next |
| - Ctatur |
| 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 then skip the steps below and click Next. Otherwise follow the steps below to upload 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 Metadata has been imported to servers in this cluster |
| - Download Sapvar Matadata 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 |
| Download Trust Metadata File |
| 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 Next Cancel |

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

Import IdP Metadata

Next Cancel

| System + | Call Routing | • | Media Resources | a - A | dvanced Features | Device | Application | User Manageme | int 🛨 | Bulk Administration 👻 | Help | • | |
|-----------------------|------------------------------|-------------|--------------------------------------|----------------------|---------------------------------------|--------------------------------|---------------------------------|-------------------|---------|-----------------------|---------|---------------------------|--------|
| SAML SI | gle Sign-(|)n C | onfiguration | | | | | | | | | | |
| dack Back | | | | | | | | | | | | | |
| - Status - | | | | | | | | | | | | | |
| The The | server meta | dətə | a file must be in | stalled | on the IdP befor | e this test i | s run. | | | | | | |
| - Test SS | 0 Setup — | | | | | | | | | | | | |
| This test SSO has | verifies that been enable | the d. S | metadata files SO setup canno | are cor ot be co | meetly configured ompleted unless | and will all this test is a | low SSO to star successful. | t up on the serve | ers. Th | his test can be run o | n any s | erver for troubleshooting | g once |
| 1)Pick a v | valid userna | me t | to use for this t | est | | | | | | | | | |
| You must This user | already kno must have | adm | he password for inistrator rights | r the se ; and al | lected username so exist in the Id | P. | | | | | | | |
| 🔥 Plea | se use one | of th | e Usernames s | hown b | elow. Using any | other Userr | name to log intr | the IdP may re- | sult in | administrator lockou | ıt. | | |
| Valid adm sso | ninistrator U | sem | ames | | | | | | | | | | |
| | | | | | | | | | | | | | |
| 2)Launch | SSO test pa | ige | | | | | | | | | | | |
| Run | SSO Test | | | | | | | | | | | | |
| Back | Cancel | | | | | | | | | | | | - |

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

| | | _ |
|------------------|-------------------------|---------------|
| Windows Securit | γ | usted certifi |
| Connecting to Al | DFS1.ciscolive.com. | ent website' |
| | | ercept any o |
| | sso | |
| | •••••• | e to this we |
| | Domain: CISCOLIVE | |
| (| Remember my credentials | |
| (| | |
| | OK Cancel | |
| | | |
| | | |
| | | ▶ |

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 <u>Certificate Management and Validation</u> 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 <u>Add</u> <u>CUCM IM and Presence as Relying Party Trust</u> 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.
- 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).

| Chttp://cucm.ciscolive.com/ - Windows Internet Explorer | | _ @ × |
|--|----------------------------|-----------------|
| COO - Mile http://cucm.discolive.com/ | 💌 🔸 🗙 🖓 Bing | ρ- |
| 😭 Favorites 🛛 🙀 💋 Suggested Sites 🔹 💋 Web Sice Gallery 🔹 | | |
| 结: http://cucm.ciscolive.com/ | 🏠 + 🔂 - 🖃 🖶 + Page + Safet | y - Tools - 🔞 - |
| | | <u>^</u> |
| ahaha | | |
| CISCO | | |
| | | |
| Installed Applications | | |
| | | |
| Cisco Unified Communications Manager | | |
| Recovery URL to bypass Single Sign On (SSO) Cisco Unified Communications Self Care Portal |) | |
| Cisco Prime License Manager | | |
| Cisco Unified Reporting Cisco Unified Serviceability | | |
| | | |
| | | |
| | | |
| Platform Applications | | |
| | | |
| Disaster Recovery System | | |
| Cisco Unified Communications OS Administration | | |
| | | |
| | | |

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 Unif | fied CM Console - Windows Internet Explorer | | | X |
|---|--|---------------------------|---|----------------------------|
| 00- | https://cucm.discolive.com/ccmadmin/showRecovery.do | 💌 😵 Certificate Error | 😝 🗙 🔎 Bing | P - |
| 🚖 Favorites | 🙀 🙋 Suggested Sites 🛛 🙋 Web Sice Gallery | | | |
| 🄏 Cisco Unif | fied CM Console | | 🚹 • 🔂 - 🖬 🖶 • N | age 🔹 Safety 👻 Tools 👻 🔞 🔹 |
| cisco | Cisco Single Sign On Recovery Administratio For Cisco Unified Communications Solutions | n | | <u>^</u> |
| Cisc This par running This par | o Single Sign On Recovery Administra ge will validate credentials locally, allowing access only to applica g on this server, and will not leverage SAML SSO authentication. ge can be disabled through the CLI. | tions that are | Username comadmin Password Login Reset | |
| Copyright @ All rights re | 8 1999 - 2015 Cisco Systems, Inc. Iserved. | | | _ |
| This produc | t contains cryptographic features and is subject to United States and local co | untry laws governing impo | ort, export, transfer and use. Deliv | ery of Cisco cryptographic |

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 <u>Unified Communications System Documentation</u> 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.