Contents

Introduction Prerequisites Requirements Components Used Background Information Configure Step 1. Export SP metadata from CUCM Step 2. Download IDP metadata from AD FS Step 3. Provision IdP Step 4. Enable SAML SSO Verify Troubleshoot

Introduction

This document describes how to configure Single Security Assertion Markup Language (SAML) Identity Provider (IdP) connection/agreement per cluster with Active Directory Federation Service (AD FS).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Communications Manager (CUCM) 11.5 or later
- Cisco Unified Communications Manager IM and Presence version 11.5 or later
- Active Directory Federation Service version 2.0

Components Used

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

- Active Directory Federation Service version 2.0 as IdP
- Cisco Unified Communications Manager version 11.5
- Cisco IM and Presence Server version 11.5

Background Information

For SAML SSO, needs to be a circle of trust between the Service Provider (SP) and the IdP. This trust is created as part of SSO Enablement, when trust (metadata) is exchanged. Download the Metadata from CUCM and uploads it to IdP, similarly download the metadata from IdP and upload it to CUCM.

Prior CUCM 11.5, originating node generates the metadata file, also it collects the metadata files from other nodes in the cluster. It adds all Metadata files to a single zip file then presents to the administrator. Administrator has to unzip this file and provision each files on the IdP. For example, 8 metadata files for an 8 node cluster.

Single SAML IdP connection/agreement per cluster feature is introduced from 11.5. As part of this feature, CUCM generates a single Service Provider metadata file for all CUCM and IMP nodes in the cluster. The new name format for the metadata file is **<hostname>-single-agreement.xml**

Basically, one node creates the Metadata and pushes it to other SP nodes in the cluster. This enables ease of provisioning, maintenance and management. For example, 1 metadata files for an 8 node cluster.

The cluster wide metadata file make use of Multiserver tomcat certificate which ensures the key pair is used is same for all nodes in the cluster. The metadata file also have a list of Assertion Consumer Service (ACS) urls for each nodes in the cluster.

CUCM and Cisco IM and Presence version 11.5 Supports both the SSO Modes, **cluster-wide** (one metadata file per cluster) and per node (existing model).

This document describes how to configure the cluster-wide mode of the SAML SSO with AD FS 2.0.

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.

Configure

Step 1. Export SP metadata from CUCM

Open a web browser, log in to CUCM as administrator, and navigate to System >

By default, **Cluster Wide** radio button is selected. Click **Export All Metadata**. The metadata data file presented to administrator in the name **<hostname>-single-agreement.xml**



Step 2. Download IDP metadata from AD FS

In order to download IdP metadata, refer to the link <u>https:// <FQDN of</u> <u>ADFS>/federationmetadata/2007-06/federationmetadata.xml</u>

Step 3. Provision IdP

As shown in the image, navigate to AD FS 2.0 Management/Trust Relation Ships/ Relying Party trust. Click Add Relying Party Trust.

p.	×
Relying Party Trusts Display Name	Actions Relying Party Trusts
	Add Relying Party Trust View
	Refresh Help
	Relying Party Trusts Display Name

Add Relying Party Trust Wizard opens as shown in the image, now click on **Start**.

Madd Relying Party Trus	t Wizard
Welcome	
Steps Welcome Select Data Source Choose Issuance Authorization Rules Ready to Add Trust Finish	Welcome to the Add Relying Party Trust Wizard This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions. The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.
	CPrevious Start Cancel Help

Click the import data about relying party from a file. Browse the SP metadata downloaded from

CUCM SAML SSO Configuration Page. Then Click **Next**, as shown in the image:

📬 Add Relying Party Trus	it Wizard
Select Data Source	
 Steps Welcome Select Data Source Choose Issuance Authorization Rules Ready to Add Trust Finish 	Select an option that this wizard will use to obtain data about this relying party:
	< <u>Previous</u> <u>Next</u> Cancel <u>H</u> elp

Type the Display Name and any optional notes for the Relying Party. Click **Next**., as shown in the image:

📬 Add Relying Party Trust	Wizard	×
Specify Display Nam	e	
Steps	Type the display name and any optional notes for this relying party.	
Welcome	Display asses	
Select Data Source	CUCM Cluster Wide Belving Party trust	
Specify Display Name	looseferred upplicitieft adfant	
 Choose Issuance Authorization Rules 	Notes:	*
Ready to Add Trust		
 Finish 		-
	1	
	< Previous Next > Car	ncel Help

Select **Permit all users to access this relying party** to permit all users to access this relying party and then click **Next**, as shown in the image:

teps	leavance authorization ofer determine subather a coar is nervited to menice chiral for the relation mature
Welcome	Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.
Select Data Source	Permit all users to access this relying party
Choose Issuance Authorization Rules	The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.
Ready to Add Trust	C Deny all users access to this relying party
Finish	The issuance authorization rules to enable any users to access this relying party. You must later add issuance authorization rules to enable any users to access this relying party. You must You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

Under **Ready to Add Trust** page, you can review the settings for the Relying Party Trust, which has been configured. Now click **Next**, as shown in the image:

Add Relying Party Trus	t Wizard	E
leady to Add Trust		
teps	The relving party trust has been configured. Review the following settings, and then click Next to add the	
Welcome	relying party trust to the AD FS configuration database.	
Select Data Source		ī
Specify Display Name	Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints N.	
Choose Issuance Authorization Rules	Specify the monitoring settings for this relying party trust.	
Ready to Add Trust	Relying party's federation metadata URL:	
	 Monitor relying party Automatically update relying party This relying party's federation metadata data was last checked on: < never > This relying party was last updated from federation metadata on: < never > 	

Finish Page confirms that relying party trust was successfully added to the AD FS configuration Database. Uncheck the Box and Click **Close**, as shown in the image:

📬 Add Relying Party Trus	: Wizard	×
Finish		
 Steps Welcome Select Data Source Specify Display Name Choose Issuance Authorization Rules Ready to Add Trust Finish 	The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS 2.0 Management snap-in.	
		10

Right Click the **Relying Party Trusts** and click on **Edit Claim Rules**, as shown in the image:

1 AD FS 2.0			novieto constanti vita en	
File Action View Window	Help			
AD FS 2.0	Relying Party Trusts			Actions
Attribute Stores	CUCM_Cluster_Wide_Relying_Party_Inust	Enabled Yes	Identifier cucm1150.ad/s.ucce.com	Relying Party Trusts Add Relying Party Trust, View New Window from Here Refresh Help CUEM_Cluster_Wide_Relying_Party_trust Update from Federation Metadata Edit Claim Rules, Disable Properties X Delete Help

Now click on Add Rule., as shown in the image:

📴 Edit Clai	m Rules for CUCM	_Cluster_Wide_Rely	ving_Party_trust	_ 🗆 X
Issuance T	ransform Rules Issu	uance Authorization Ru	les Delegation Authorization	Rules
The follo	wing transform rules s	specify the claims that v	vill be sent to the relying party.	
Order	Rule Name		Issued Claims	1 I
				*
Add R	ule Edit Rule	Remove Rule	1	
			1	
		ок с	Cancel Apply	Help

When the Add Transform Claim Rule opens, click Next with the default claim rule template Send LDAP Attributes as Claims, as shown in the image:

Steps	Select the template for the claim rule that you want to create from the following list. The description
Choose Rule Type	provides details about each claim rule template.
 Configure Claim Rule 	Claim rule template:
	Send LDAP Attributes as Claims
	Claim rule template description:
	Use of a sind (LDM Anton as LDM and a feature as the more as you can also do distuble to the an UDM anton and the more association and LDM anton and the set of the anton and LDM anton and the set of the set of the anton and the set of the set
	Contract Contract Contract

Click **Configure Claim Rule** as shown in this image. LDAP Attribute must match with the LDAP Attribute in LDAP Directory configuration in the CUCM. Manage outgoing claim type as **uid**. Click **Finish**, as shown in the image:

🙀 Add Transform Claim Ri	ule Wizard				×
Configure Rule					
Steps Choose Rule Type Configure Claim Rule	You o which issuer Claim	an configure this rule to send the to extract LDAP attributes. Spe d from the rule. rule name:	e values of L cify how the	DAP attributes as claims. Select an attri attributes will map to the outgoing claim	bute store from types that will be
	Name Rule I Attribu	ID template: Send LDAP Attributes a ute store:	as Claims		
	Mapp	e Directory ing of LDAP attributes to outgoin	ıg claim type	*:	
		LDAP Attribute		Outgoing Claim Type	-
	*	Grant Cook A Mane	-		
			< Pr	evious Finish Cancel	Help

Add the custom rule for the relying party. Click **Add rule**. Select **Send Claims using a Custom Rule** and then click **Next**, as shown in the image:

 Choose Rule Type Configure Claim Rule 	provides details about each claim rule template.
Configure Claim Rule	
	Claim rule template:
	Send Claims Using a Custom Rule
	Claim rule template description:
	Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS 2.0 claim rule language. Capabilities that require custom rules include: • Sending claims from a SQL attribute store using a custom LDAP filter • Sending claims from a custom attribute store using a custom LDAP filter • Sending claims rule when 2 or more incoming claims are present • Sending claims only when 2 or more incoming claims are present • Sending claims only when 2 or more store • Sending claims store complex changes to an incoming claim value • Creating claims for use only in later rules Tell me more about this rule template

In Configure Claim rule, type a Claim Rule Name then Copy the Claim Rule given and past in the Custom Rule field in the wizard modifying the namequalifier and spname qualifier in the Claim rule. Click **Finish**., as shown in the image:

Claim Rule:

Add Transform Claim R	ule Wizard	1
Configure Rule		
Steps	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts	2
Choose Rule Type	claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD ES 2.0 claim rule language.	
Configure Claim Rule	Claim rule name:	
	Cluster_Side_Claim_Rule	
	Rule template: Send Claims Using a Custom Rule	
	Cystom rule:	
	<pre>ntname"] => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier ", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/form at"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/name qualifier"] = "http://win- jd4ia7ugmrm.adfs.ucce.com/adfs/com/adfs/services/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spna mequalifier"] = "cucml150.adfs.ucce.com");</pre>	
	More about the claim rule language	
	< <u>Previous</u> Finish Cancel <u>H</u> elp	_

As shown in the image, Click **Apply** then **OK**.

Drder	Rule Name NamelD		Issued Claims uid	
2	Cluster_Side_Clair	m_Hule	<see claim="" rule=""></see>	
				1
4 J J m.	a I carpu	- Pamaua P		

Step 4. Enable SAML SSO

Open a web browser, log in to CUCM as administrator, and navigate to System >.

By default, **Cluster Wide** radio button is selected. Click **Enable Saml SSO**, as shown in the image:



As shown in the image, the pop up notifies the warning for webserver restart and information to choose the cluster wide SAML SSO or Per-Node SAML SSO according to idp. Click **Continue**.



The criteria to enable Cluster-wide SSO is that you must have a multiserver tomcat certificate already deployed. Click **Test for Multi-Server tomcat Certificate**, as shown in the image:

SAML Single Sign-On Configuration	
Next	
_ Status	
i Status: Ready	
Test for Multi-Server tomcat certificate	0
The criteria for enabling dusterwide SSO i	s that you must have a multiserver tomcat certificate already deployed. If you have not done this already please follow the below step
1) Login to Cisco Unified OS Administratio	in Page and Navigate to Certificate Management under Security Menu
2) Click on Generate CSR	
3) Select Certificate Purpose as Tomcat	
4) Select Distribution as "Multi-Server"	
5) Click Generate	
6) Download the CSR and get it signed fr	om the CA of your choice
7) Once the certificate is issued by the CA	, upload it via the "Upload Certificate/ Certificate chain" option on the Certificate Management page
8) Restart Tomcat service on all the node	s in the cluster
9) Restart TFTP service on all the TFTP no	des in the duster
If the above steps have been completed,	click Test below which will confirm if the multi-server tomcat certificate is deployed before proceeding to the next stage
Test for Multi-Server tomcat certifica	ste

Once it is confirmed, all nodes have Multi Server Certificate displays an **All Nodes have Multi Server Certificate**, and then click **Next**, as shown in the image:

SAML Single Sign-On Configuration
Next .
- Status
Status Bearly
V All hodes have Multi Server Cercificate
Test for Multi-Server tomcat certificate
The criteria for enabling clusterwide SSO is that you must have a multiserver tomcat certificate already deployed. If you have not done this already please follow the below steps:
1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
2) Click on Generate CSR
3) Select Certificate Purpose as Tomcat
4) Select Distribution as "Multi-Server"
5) Click Generate
6) Download the CSR and get it signed from the CA of your choice
7) Once the certificate is issued by the CA, upload it via the "Upload Certificate/ Certificate chain" option on the Certificate Management page
B) Restart Tomcat service on all the nodes in the duster
9) Restart TFTP service on all the TFTP nodes in the cluster
If the above steps have been completed, click Test below which will confirm if the multi-server tomcat certificate is deployed before proceeding to the next stage
Test for Multi-Server tomcat certificate
Next Cancel

As shown in the image, click Next.

SAML Single Sign-On Configuration
Next
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

Browse and select the IdP metadata downloaded. Click **Import IdP Metadata**, as shown in the image:

SAML Single Sign-On Configuration
Next
Status
(i) Status: Ready
(1) 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
Browse) 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.
Import IdP Metadata
Next Cancel

The page confirms the Import succeeded for all servers and then click **Next**, as shown in the image:

SAML Single Sign-On Configuration
Next
Status
i Status: Ready
V 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
Browse No file selected.
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 IdP Metadata Vimport succeeded for all servers
Next Cancel

As shown in the image, click **Next**, since already exported the SP metadata from the initial SAML SSO configuration Page.

SAML Single Sign-On Configuration
Back Next
⊂ Status
i Status: Ready
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
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

CUCM has to be in sync with the LDAP Directory. Wizard shows the valid administrator users configured in the LDAP Directory. Select the user and click **Run SSO Test**, as shown in the image:

Abesporynuin assincerge i relikter fitingigas don block schoestesptiste plas woodd die wratie it for compatibiling SSO.



The page shown in the image confirms that SAML SSO Enabling process is initiated on all servers.

SAML Single Sign-On Configuration

Status

SAML SSO enablement process initiated on all servers.

There will be a short delay while the applications are being updated on each server.

To verify the SSO status of each server, check the main SSO Configuration page.

Log out and log in back to CUCM using SAML SSO credentials. Navigate to **System >**. Click **Run SSO Test** for other nodes in the cluster, as shown in the image:

SAML Single Sign-On							
SSO Mode Cluster wide (One metadal Per node (One metadata fi	ta file per cluste le per node)	r. Requires n	nulti-server Tomcat certificate))			
🗙 Disable SAML SSO 🔐	Export Al Metada	ta 🔞 Upd	ale kiP Metadata File 🥢 Fix.	All Disabled Sen	vers		
Status RTMT is enabled for SSC SAML SSO enabled SAML Single Sign-On (2)). You can chan 1 - 3 of 3)	ge SSO for R	TMT <u>here.</u>			Row	s per Page 50 ¥
Server Name	SSO Status	Re-Import Metadata	Last Hetadata Import	Export Metadata	Last Metadata Export	550 Te	est
cucm1150.adfs.ucce.com	SAML	N/A	June 21, 2016 9:28:39 PM IST	🏄 File	June 21, 2016 7:46:56 PM IST	Passed - June 21, 2016 9:29:14 PM IST	Run SSO Test
cucm1150sub.adfs.ucce.com	SAML	🔶 IdP	June 21, 2016 9:28:39 PM IST	🏄 File	June 21, 2016 7:46:56 PM IST	Never	Run SSO Test
imp115.adfs.ucce.com	SAML	🔶 IdP	June 21, 2016 9:28:39 PM IST	🏄 File	June 21, 2016 7:46:56	Never	Run SSO Test

Verify

Use this section to confirm that your configuration works properly.

Confirm the SSO Test is succesful for the nodes which are SAML SSO enabled. Navigate to **System >**. Successful SSO tests shows the status Passed.

SAME Single Sign-On							
ISO Mode Cluster wide (One metadal Per node (One metadata fi	ta file per clu: le per node)	ster. Requires n	nulti-server Tomcat certificate)				
🗙 Disable SAML SSO 👔	Export All Meta	idata 🔞 Upd	iate IdP Metadata File 🥜 Fix /	All Disabled Ser	vers		
Status). You can ch	ange SSO for R	TMT <u>here.</u>				
(i) SAML SSO enabled SAML Single Sign-On (i)	1 - 3 of 3)					Rows	s per Page 50 🔻
(i) SAML SSO enabled SAML Single Sign-On (2) Server Name	I - 3 of 3) SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	Rows SSO To	s per Page 50 💌
SAML SSO enabled SAML Single Sign-On (2) Server Name cucm1150.adfs.ucce.com	1 - 3 of 3) SSO Status SAML	Re-Import Metadata N/A	Last Metadata Import June 20, 2016 9:57:30 AM IST	Export Metadata	Last Metadata Export June 20, 2016 10:06:27 PM IST	Rows SSO To Passed - June 20, 2016 9:59:02 PM IST	s per Page SD ▼ est Run SSO Test
SAML SSO enabled SAML Single Sign-On (2) Server Name cucm1150.adfs.ucce.com cucm1150sub.adfs.ucce.com	I - 3 of 3) SSO Status SAML SAML	Re-Import Metadata N/A IdP	Last Metadata Import June 20, 2016 9:57:30 AM IST June 20, 2016 10:15:46 PM IST	Export Metadata L File	Last Metadata Export June 20, 2016 10:06:27 PM IST June 20, 2016 10:06:26 PM IST	Rows SSO Te Passed - June 20, 2016 9:59:02 PM IST Passed - June 20, 2016 10:11:39 PM IST	s per Page 50 • est Run SSO Test Run SSO Test

Once the SAML SSO is activated, Installed Applications and Platform Applications are listed for CUCM login page, as shown in this image.

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

Once the SAML SSO is activated, Installed Applications and Platform Applications are listed for IM and Presence login page, as shown in this image:

Installed Applications

- Cisco Unified Communications Manager IM and Presence
 Recovery URL to bypass Single Sign On (SSO)
- Cisco Unified Reporting
- Cisco Unified Serviceability

Platform Applications

- Disaster Recovery System
- Cisco Unified Communications OS Administration

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

In order to set the SSO logs to debug, use command set samItrace level DEBUG

Collect the SSO logs Using RTMT or from **activelog /tomcat/logs/ssosp/log4j/*.log** location using CLI.

Example for SSO logs shows the metadata generated and sending to other nodes