Configuration d'une connexion/d'un contrat SAML par cluster avec AD FS version 2.0

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Configuration Étape 1. Exporter les métadonnées SP de CUCM Étape 2. Télécharger les métadonnées PCI à partir d'AD FS Étape 3. IdP de provisionnement Étape 4. Activer SAML SSO Vérification Dépannage

Introduction

Ce document décrit comment configurer la connexion/l'accord de fournisseur d'identité (IdP) SAML (Single Security Assertion Markup Language) par cluster avec Active Directory Federation Service (AD FS).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Communications Manager (CUCM) 11.5 ou version ultérieure
- Cisco Unified Communications Manager IM and Presence version 11.5 ou ultérieure
- Service de fédération Active Directory version 2.0

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Service de fédération Active Directory version 2.0 en tant qu'IDP
- Cisco Unified Communications Manager version 11.5
- Cisco IM and Presence Server version 11.5

Informations générales

Pour SAML SSO, doit être un cercle de confiance entre le fournisseur de services (SP) et l'IDP. Cette approbation est créée dans le cadre de SSO Enablement, lorsque la confiance (métadonnées) est échangée. Téléchargez les métadonnées à partir de CUCM et téléchargez-les sur IdP, téléchargez les métadonnées à partir de IdP et téléchargez-les sur CUCM.

Avant CUCM 11.5, le noeud d'origine génère le fichier de métadonnées et collecte également les fichiers de métadonnées d'autres noeuds du cluster. Il ajoute tous les fichiers de métadonnées à un seul fichier zip puis les présente à l'administrateur. L'administrateur doit décompresser ce fichier et approvisionner chaque fichier sur l'IDP. Par exemple, 8 fichiers de métadonnées pour un cluster à 8 noeuds.

Une seule connexion/accord SAML IdP par fonction de cluster est introduite à partir de la version 11.5. Dans le cadre de cette fonctionnalité, CUCM génère un fichier de métadonnées unique pour le fournisseur de services pour tous les noeuds CUCM et IMP du cluster. Le nouveau format de nom du fichier de métadonnées est **<hostname>-single-agreement.xml**

En gros, un noeud crée les métadonnées et les transmet aux autres noeuds SP du cluster. Cela facilite le provisionnement, la maintenance et la gestion. Par exemple, 1 fichier de métadonnées pour un cluster à 8 noeuds.

Le fichier de métadonnées à l'échelle du cluster utilise un certificat multiserveur tomcat qui garantit que la paire de clés est utilisée de la même manière pour tous les noeuds du cluster. Le fichier de métadonnées contient également une liste d'URL ACS (Assertion Consumer Service) pour chaque noeud du cluster.

CUCM et Cisco IM and Presence version 11.5 prennent en charge les modes SSO, à l'échelle du cluster (un fichier de métadonnées par cluster) et par noeud (modèle existant).

Ce document décrit comment configurer le mode à l'échelle du cluster de SAML SSO avec 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.

Configuration

Étape 1. Exporter les métadonnées SP de CUCM

Ouvrez un navigateur Web, connectez-vous à CUCM en tant qu'administrateur et naviguez vers System >Single Sign On SAML.

Par défaut, le bouton radio **Cluster Wide** est sélectionné. Cliquez sur **Exporter toutes les métadonnées.** Fichier de données de métadonnées présenté à l'administrateur sous le nom **<hostname>-single-agreement.xml**



Étape 2. Télécharger les métadonnées PCI à partir d'AD FS

Pour télécharger les métadonnées IdP, consultez le lien <u>https:// <FQDN of</u> <u>ADFS>/federationmetadata/2007-06/federationmetadata.xml</u>

Étape 3. IdP de provisionnement

Comme l'illustre l'image, accédez à Gestion/Approbation des expéditions/Approbation de la partie de confiance AD FS 2.0. Cliquez sur Ajouter une approbation de partie de confiance.

2	
Relying Party Trusts	Actions
Display Name	Relying Party Trusts
	Add Relying Party Trust
	View New Window from Here
1	G Refresh
*	Help
	Relying Party Trusts Display Name

L'Assistant Ajout d'approbation de partie de confiance s'ouvre comme indiqué dans l'image, cliquez maintenant sur **Démarrer**.

Madd Relying Party True	t Wizard	x
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.	
	< Previous Start Cancel Help	1

Cliquez sur les données d'importation relatives à la partie de confiance à partir d'un fichier. Parcourez les métadonnées SP téléchargées à partir de la page de configuration de CUCM SAML SSO. Cliquez ensuite sur **Suivant**, comme illustré dans l'image :

📬 Add Relying Party Trus	t Wizard	×
Select Data Source		
Steps Velcome 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: Igport data about the relying party published online or on a local network. Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network. Eederation metadata address (host name or URL): Example: fs. contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: D:\Users\Administrator\Desktop\Cluster_\Wide\cucm1150-single-agreement.xml Browse C Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization. 	
	< <u>P</u> revious <u>N</u> ext > Cancel <u>H</u> elp	

Tapez le nom d'affichage et toutes les notes facultatives pour la partie de confiance. Cliquez sur **Suivant**., comme illustré dans l'image :

add Relying Party Trust	Wizard	×
Specify Display Nam	e	
Steps	Type the display name and any optional notes for this relying party.	
 Welcome Select Data Source 	Display name:	
Specify Display Name	CUCM_Cluster_Wide_Relying_Party_trust	
 Choose Issuance Authorization Rules Ready to Add Trust Finish 	Notes:	X
	< Previous Next > Canc	el Help

Sélectionnez **Autoriser tous les utilisateurs à accéder à cette partie de confiance** pour autoriser tous les utilisateurs à accéder à cette partie de confiance, puis cliquez sur **Suivant**, comme illustré dans l'image :

Add Relying Party Trus	t Wizard
Choose Issuance Au	thorization Rules
 Velcome Select Data Source Specify Display Name Choose Issuance Authorization Rules Ready to Add Trust Finish 	 Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules. Permit all users to access this relying party 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. Deny all users access to this relying party The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party. You must rule add issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.
	< <u>P</u> revious <u>N</u> ext > Cancel <u>H</u> elp

Sous **la** page **Prêt à ajouter une approbation**, vous pouvez consulter les paramètres de l'approbation de partie de confiance, qui a été configurée. Cliquez maintenant sur **Suivant**, comme illustré dans l'image :

teps	The relying 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	
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 rederation 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 >

La page Finish confirme que l'approbation de partie de confiance a été ajoutée avec succès à la base de données de configuration AD FS. Décochez la case et cliquez sur **Fermer**, comme illustré dans l'image :

📬 Add Relying Party Trus	t 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 snapin.	

Cliquez avec le bouton droit de la souris sur les **approbations de la partie de confiance** et cliquez sur **Modifier les règles de demande**, comme illustré dans l'image :

		Another and structure	-	
Help			بلد [<u>el ×</u>
Relying Party Trusts			Actions	
Display Name 👻	Enabled	Identifier	Relying Party Trusts	•
CUCM_Cluster_Wide_Relying_Party_trust	Yes	cucm1150 adis ucce.com	Add Relying Party Trust	
			View	
1			New Window from Here	
1			G Refresh	
			👔 Help	
			CUCM_Cluster_Wide_Relying_Party_trust	
1			Update from Federation Metadata	-
1			Edit Claim Rules	
1			Disable	
1			Properties	
1			🔀 Delete	
4			Help	-
	Help Relying Party Trusts Display Name CUCM_Cluster_Wide_Relying_Party_trust	Relying Party Trusts Display Name Enabled CUCM_Cluster_Wide_Relying_Party_trust Yes	Relying Party Trusts Display Name * Enabled CUCM_Cluster_Wide_Relying_Party_Inust Yes cucm1150.adfs.ucce.com	Relying Party Trusts Actions Display Name * Enabled Identifier CUCM_Cluster_Wide_Relying_Party_Inust Yes cucm1150 adls ucce.com View New Window from Here @ Refresh @ Help CUCM_Cluster_Wide_Relying_Party_trust Update from Federation Metadata, Edx Claim Rules Disable Properties X Delete Y Help Y

Cliquez maintenant sur Ajouter une règle, comme l'illustre l'image :

Edit Claim Rules for CUCM_Cluster_Wide_Rel	ying_Party_trust	
Issuance Transform Rules Issuance Authorization Ru	ules Delegation Authorization R	ules
The following transform rules specify the claims that	will be sent to the relying party.	
Order Rule Name	Lesued Claime	
		1
		4
Add Rule Edit Rule Remove Rule]	
	-	
OK	Cancel Apply	Help

Lorsque la **règle Ajouter une revendication de transformation** s'ouvre, cliquez sur **Suivant** avec le modèle de règle de revendication par défaut **Envoyer les attributs LDAP en tant que revendications**, comme illustré dans l'image :

teps	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:
	Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template. Tell me more about this rule template
	CPrevious Next Cancel Help

Cliquez sur **Configurer la règle de revendication** comme indiqué dans cette image. L'attribut LDAP doit correspondre à l'attribut LDAP dans la configuration de l'annuaire LDAP dans CUCM. Gérer le type de revendication sortante comme **uid**. Cliquez sur **Terminer**, comme l'illustre l'image :

🙀 Add Transform Claim R	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 attribute stor attributes will map to the outgoing claim types th	e from at will be
	Name Rule Attrib	ID template: Send LDAP Attributes : ute store:	as Claims		
	Mapp	e Directory ing of LDAP attributes to outgoin	ıg claim type		
		LDAP Attribute		Outgoing Claim Type	
		SAM-Account-Iname			
			< Pre	evious Finish Cancel	Help

Ajoutez la règle personnalisée pour la partie de confiance. Cliquez sur **Ajouter une règle**. Sélectionnez **Envoyer des revendications à l'aide d'une règle personnalisée** puis cliquez sur **Suivant,** comme illustré dans l'image :

Add Transform Claim Ru	le Wizard	×
Select Rule Template		
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 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 • Sending claims from an LDAP attribute store using a custom LDAP filter • Sending claims from a custom attribute store • Sending claims only when 2 or more incoming claims are present • Sending claims only when an incoming claim value matches a complex pattern • Sending claims with complex changes to an incoming claim value	
	Creating claims for use only in later rules <u>Tell me more about this rule template</u> (Brevious Next > Cancel Help	

Dans Configurer la règle de revendication, tapez un nom de règle de revendication, puis Copiez la règle de revendication donnée et passée dans le champ Règle personnalisée de l'Assistant modifiant l'équaliseur de noms et le qualificateur de nom dans la règle de revendication. Cliquez sur **Terminer**., comme l'illustre l'image :

Règle de revendication :

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> 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/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
"http://<FQDN of ADFS>/adfs/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"<Entity ID in the SP Metadata>");
```

Entity ID = Open the SP metadata and check the Entity ID. Basically, its the CUCM Publisher's FQDN.

📬 Add Transform Claim R	ule Wizard	×				
Configure Rule						
Steps	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, ture one or more optional conditions and an					
Choose Hule Type	issuance statement using the AD FS 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	1				

Comme le montre l'image, cliquez sur Apply, puis sur OK.

Jraer Hui Nar Clu:	e Name nelD ster_Side_Claim_F	lule	uid <see claim="" rule:<="" th=""><th>×</th></see>	×
				4

Étape 4. Activer SAML SSO

Ouvrez un navigateur Web, connectez-vous à CUCM en tant qu'administrateur et naviguez **vers** System >Single Sign On SAML.

Par défaut, le bouton radio **Cluster Wide** est sélectionné. Cliquez sur **Enable Saml SSO**, comme illustré dans l'image :



Comme l'illustre l'image, la fenêtre contextuelle avertit l'avertissement de redémarrage du serveur Web et les informations permettant de choisir l'SSO SAML ou SSO SAML par noeud à l'échelle du cluster, conformément à idp. Cliquez sur **Continue**.



Le critère d'activation de l'authentification unique à l'échelle du cluster est que vous devez disposer d'un certificat tomcat multiserveur déjà déployé. Cliquez sur **Test for Multi-Server Tomcat Certificate**, comme illustré dans l'image :

AML Single Sign-On Configuration
Next
Status
i Status: Ready
Test for Multi-Server tomcat certificate
The criteria for enabling dusterwide SSD 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
8) Restart Tomcat service on all the nodes in the cluster
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

Une fois la confirmation obtenue, tous les noeuds ont un certificat multi-serveur affiche un **certificat multi-serveur pour tous les noeuds**, puis cliquez sur **Suivant**, comme illustré dans l'image :

SAML Single Sign-On Configuration
Next .
e Statue
Actor
U Status: Ready
V All nodes have Multi Server Certificate
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

Comme le montre l'image, cliquez sur Suivant.

SAML Single Sign-On Configuration	
Next	
Status	
(i) 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 me import it to your servers. You will need to manually obtain the file from the IdP before you can uploat servers.	etadata from your IdP and ad it to your Collaboration
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.	

Parcourez et sélectionnez les métadonnées IdP téléchargées. Cliquez sur **Importer les métadonnées IdP**, comme indiqué dans l'image :

SAML Single Sign-On Configuration
Next .
Status
(i) Status: Ready
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

La page confirme que l'importation a réussi pour tous les serveurs, puis cliquez sur **Suivant**, comme illustré dans l'image :

SAML Single Sign-On Configuration
Next
Status
(i) Status: Ready
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 Import succeeded for all servers
Next Cancel

Comme l'illustre l'image, cliquez sur **Suivant**, car les métadonnées SP ont déjà été exportées à partir de la page de configuration initiale SAML SSO.

SAML Single Sign-On Configuration
Back Next
r 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 doit être synchronisé avec l'annuaire LDAP. L'Assistant affiche les utilisateurs administrateur valides configurés dans l'annuaire LDAP. Sélectionnez l'utilisateur et cliquez sur **Exécuter le test SSO**, comme illustré dans l'image :

SAML Single Sign-On Configuration	on
de Back	
Status The server metadata file must b	e installed on the IdP before this test is run.
Test SSO Setup	
This test verifies that the metadata f run on any server for troubleshootin successful.	iles are correctly configured and will allow SSO to start up on the servers. This test can be g once SSO has been enabled. SSO setup cannot be completed unless this test is
1)Pick a valid username to use for th	is test
You must already know the passwor This user must have administrator n Please use one of the Usernam lockout.	d for the selected username. ghts and also exist in the IdP. es shown below. Using any other Username to log into the IdP may result in administrator
Valid administrator Usernames	
samluser	
2)Launch SSO test page Run SSO Test	

Comme l'illustre l'image, entrez l'ID utilisateur et le mot de passe respectifs une fois qu'il l'invite.

Authentication	Required				
?	Enter username and password for https://win-jd4ia7ugmrm.adfs.ucce.com				
User Name:	samluser				
Password:	••••••				
	OK Cancel				

La fenêtre contextuelle, comme le montre l'image, confirme que le test est réussi.



Comme l'illustre l'image, cliquez sur Terminer afin de terminer la configuration pour activer SSO.

System • C	all Routing 🔻	Media Resources 💌	Advanced Features 💌	Device •	Application •	User Management	Bulk Administra
SAML Single	e Sign-On Co	onfiguration					
Back	Finish						
Status	etadata Test S	Guccessful					
Ready to Er Clicking "Finis being update To verify the Additional tes	nable SSO sh" will comple ed. SSO status o sting and man	te enabling SSO on a f each server, check ual uploads may be p	all the servers in this clu the main SSO Configur performed from the ma	uster. There ration page. iin page if n	e will be a short eccessary.	: delay while the app	lications are
Back	nish Can	cel					

La page illustrée dans l'image confirme que le processus d'activation SAML SSO est lancé sur tous les serveurs.



Déconnectez-vous et reconnectez-vous à CUCM à l'aide des informations d'identification SAML SSO. Accédez à **System >SAML Single Sign On**. Cliquez sur **Exécuter le test SSO** pour les autres noeuds du cluster, comme illustré dans l'image :

SAML Single Sign-On							
SSO Mode Cluster wide (One metadat Per node (One metadata fi	ta file per cluster. le per node)	Requires m	nulti-server Tomcat certificate)				
🗙 Disable SAML SSO 👔	Export All Metadata	🔞 Upda	ale klP Metadata File 🧳 Fix	All Disabled Sen	vers		
RTMT is enabled for SSO SAML SSO enabled SAML Single Sign-On). You can change t - 3 of 3)	: SSO for R	TMT <u>here.</u>			Row	s per Page 50 🔻
Server Name	SSO Status	te-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 PM IST	Never	Run SSO Test

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Confirmez que le test SSO a réussi pour les noeuds qui sont activés SSO SAML. Accédez à **System >SAML Single Sign On**. Les tests SSO réussis indiquent l'état Passé.

 O Mode Cluster wide (One metadat: Per node (One metadata fil 	a file per clus e per node)	ster. Requires n	nulti-server Tomcat certificate))			
🗙 Disable SAML SSO 👔 E	Export All Meta	data 🔞 Upd	late IdP Metadata File 🥜 Fix /	All Disabled Ser	vers		
Status							
RTMT is enabled for SSO.	. You can chi	ange SSO for R	TMT here.				
CAMI SEO anablad							
SAME SSO enabled							
SAMI Single Sign-On (7	- 3 of 3)					Rows	ner Page 50 ¥
SAML Single Sign-On (1 Server Name	- 3 of 3) SSO Status	Re-Import Netadata	Last Metadata Import	Export Metadata	Last Metadata Export	Rows SSO Te	s per Page 50 💌
SAML Single Sign-On (1 Server Name	- 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 Te Passed - June 20, 2016 9:59:02 PM IST	s per Page 50 ▼ est Run SSO Test
SAML Single Sign-On (1 Server Name sucm1150.adfs.ucce.com	sso status SAML SAML	Re-Import Metadata N/A 1dP	Last Metadata Import June 20, 2016 9:57:30 AM IST June 20, 2016 10:15:46 PM IST	Export Metadata L Fie L Fie	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 V est Run SSO Test Run SSO Test

Une fois l'OSS SAML activé, les applications installées et les applications de plate-forme sont répertoriées pour la page de connexion CUCM, comme illustré dans cette 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

Une fois le SSO SAML activé, les applications installées et les applications de plate-forme sont répertoriées pour la page de connexion IM and Presence, comme illustré sur cette 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

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Afin de définir les journaux SSO sur debug, utilisez la commande set samltrace level DEBUG

Collectez les journaux SSO à l'aide de RTMT ou à partir de l'emplacement **activelog** /tomcat/logs/ssosp/log4j/*.log à l'aide de l'interface de ligne de commande.

Exemple pour les journaux SSO montre les métadonnées générées et envoyées à d'autres noeuds

2016-05-28 14:59:34,026 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Call GET API to generate Clusterwide SP Metadata in the Local node. 2016-05-28 14:59:47,184 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Call to post the generated SP Metadata to other nodes 2016-05-28 14:59:47,185 INFO [http-bio-443-exec-297] cluster.SAMLSSOClusterManager -Begin:postClusterWideSPMetaData 2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Nodes [cucm1150, cucm1150sub.adfs.ucce.com] 2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post ClusterWideSPMetadata to the cucm1150 2016-05-28 14:59:47,187 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post ClusterWideSPMetadata to the cucm1150