Configureer één SAML-verbinding/overeenkomst per cluster met ADSL versie 2.0

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren Stap 1: Exporteren van SP-metagegevens uit CUCM Stap 2: IDP-metagegevens van AD FS downloaden Stap 3. Voorziening-ID Stap 4: SAML SSO inschakelen Verifiëren Problemen oplossen

Inleiding

Dit document beschrijft hoe u de verbinding/overeenkomst per cluster met Active Directory Federation Service (AD FS) kunt configureren (SAML) Identity Provider (IDP).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Communications Manager (CUCM) 11.5 of hoger
- Cisco Unified Communications Manager IM and Presence versie 11.5 of hoger
- Active Directory Federation Service versie 2.0

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Active Directory Federation Service versie 2.0 als IDP
- Cisco Unified Communications Manager versie 11.5
- Cisco IM and Presence Server versie 11.5

Achtergrondinformatie

Voor SAML SSO moet een vertrouwenscirkel zijn tussen de serviceproviders (SP) en de IDP. Dit

vertrouwen wordt gecreëerd als onderdeel van SSO Enablement, wanneer trust (metagegevens) wordt uitgewisseld. Download de metagegevens van CUCM en uploadt deze naar IDP, en download de metagegevens van IDP eveneens en uploadt deze naar CUCM.

Eerder CUCM 11.5, het oorsprong knooppunt, genereert het metagegevensbestand en verzamelt ook de metagegevensbestanden van andere knooppunten in het cluster. Het voegt alle metagegevensbestanden aan één zip-bestand toe en legt deze vervolgens voor aan de beheerder. Administrator moet dit bestand opheffen en alle bestanden op de IDP zetten. Bijvoorbeeld, 8 metagegevensbestanden voor een 8 knooppunt cluster.

Eén SAML IDP-verbinding/overeenkomst per clusterfunctie wordt geïntroduceerd vanaf 11.5. Als onderdeel van deze functie genereert CUCM één metagegevensbestand voor serviceproviders voor alle CUCM- en IMP-knooppunten in de cluster. Het nieuwe naamformaat voor het metagegevensbestand is **<hostname>-single-agreement.xml**

Eén knooppunt maakt de metagegevens en duwt het naar andere SP-knooppunten in de cluster. Dit maakt het mogelijk voorzieningen, onderhoud en beheer te vergemakkelijken. Bijvoorbeeld, 1 meta-gegevensbestanden voor een 8 knooppunt cluster.

Het cluster brede metagegevensbestand maakt gebruik van een multiserver-to-cat-certificaat dat garandeert dat het sleutelpaar ook wordt gebruikt voor alle knooppunten in de cluster. Het metagegevensbestand heeft ook een lijst van Assertion Consumer Service (ACS) urls voor elke knooppunten in het cluster.

CUCM en Cisco IM and Presence versie 11.5 Ondersteunt zowel de SSO-modellen, de **clusterbrede** (één metagegevensbestand per cluster) en per knooppunt (bestaand model).

Dit document beschrijft hoe de clusterbrede modus van de SAML SER met AD FS 2.0 moet worden configureren.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Stap 1: Exporteren van SP-metagegevens uit CUCM

Open een webbrowser, logt u in bij CUCM als beheerder en navigeer **naar Systeem > SAML** Single Sign On.

Standaard wordt **Cluster Wide** radioknop geselecteerd. Klik op **Exporteren alle metagegevens.** Het metagegevensbestand dat aan de beheerder wordt gepresenteerd onder de naam **<hostname>-** single-agreement.xml



Stap 2: IDP-metagegevens van AD FS downloaden

Raadpleeg de link <u>https:// <FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml</u> om IDP-<u>metagegevens</u> te downloaden

Stap 3. Voorziening-ID

Zoals in de afbeelding wordt getoond, navigeer dan naar AD FS 2.0 Management/Trust Relation Ships/Relying Party trust. Klik op Add Relying Party Trust.

	_ [] ×
	_8×
Relying Party Trusts	Actions
Display Name	Relying Party Trusts
	Add Relying Party Trust
	View New Window from Here
1	G Refresh
4	Help
	Relying Party Trusts Display Name

De wizard Vertrouwend maken wordt toegevoegd zoals in de afbeelding weergegeven. Klik nu op **Start**.

Madd Relying Party True	st Wizard	x
Welcome		
Welcome Velcome Steps Velcome 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	

Klik de invoergegevens over het vertrouwen van een partij in een bestand aan. Bladeren de SPmetadata die zijn gedownload van de CUCM SAML SSO Configuration Pagina. Klik vervolgens op **Volgende**, zoals in de afbeelding weergegeven:

http://www.commons.com/actions	st Wizard	×
Select Data Source		
 Add Relying Party Tru Select Data Source 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: Ignott 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.	
	< Previous Next > Cancel Help	

Typ de naam van het display en eventuele opmerkingen voor de betrokken partij. Klik op **Volgende**., zoals in de afbeelding wordt weergegeven:

📬 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_Helying_Party_trust	
 Choose Issuance Authorization Rules Ready to Add Trust Finish 	Notes:	×.
	< Previous Next > Can	cel Help

Selecteer **Toestaan alle gebruikers van deze vertrouwende partij** om alle gebruikers toe te staan om deze vertrouwende partij te benaderen en klik vervolgens op **Volgende**, zoals in de afbeelding:

Add Relying Party Trust	: Wizard
Choose Issuance Au	thorization Rules
 Steps Welcome 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 gli 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 later add issuance authorization rules to enable any users to access this relying party. 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.
	< <u>Previous</u> <u>N</u> ext > Cancel <u>H</u> elp

Onder **Ready to Add Trust** pagina, kunt u de instellingen voor het Relying Party Trust bekijken, die is geconfigureerd. Klik nu op **Volgende**, zoals in de afbeelding wordt weergegeven:

iteps	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	Helying party's federation metadata UHL:
	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 bevestigt dat het vertrouwen van een betrouwbare partij met succes is toegevoegd aan de AD FS configuratie Database. Schakel het vakje uit en klik op **Sluiten**, zoals in de afbeelding wordt weergegeven:

📬 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.

Klik met de rechtermuisknop op de **vertrouwenwekkende stoffen** van de **Betrouwer** en klik op **Bewerken** in de afbeelding.

AD FS 2.0	i Help				e ×
AD FS 2.0 Claims Provider Trusts Claims Provider Trusts Relying Party Trusts Attribute Stores	Relying Party Trusts			Actions Relying Party Trusts 🔶	
	CUCM_Cluster_Wide_Relying_Party_trust	Yes	cucm1150.adfs.ucce.com	Add Relying Party Trust View New Window from Here Refresh Help CUCM_cluster_Wide_Relying_Party_trust Update from Federation Metadata Edit Claim Rules	
	•			Disable Properties X Delete Help	

Klik nu op Add Rule ., zoals getoond in de afbeelding:

Bedit Claim Rules for CUCM_Cluster_Wide_ Issuance Transform Rules Issuance Authorization	_Relying_Party_trust on Rules Delegation Authorization R	ules
The following transform rules specify the claims	that will be sent to the relying party.	
Urder Rule Name	Issued Claims	
Add Rule Edit Rule Remove R	ule	
ОК	Cancel Apply	Help

Wanneer de **regel** Eis **toevoegen Omzetten** wordt geopend, klikt u op **Volgende** met de standaardclaimregelsjabloon **Verzend** LDAP-kenmerken als claims, zoals in de afbeelding wordt weergegeven:

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.		

Klik op **Claim Rule** zoals getoond in deze afbeelding. LDP-kenmerk moet overeenkomen met de LPDP-kenmerk in de configuratie van de LMBP-map in de CUCM. Uitgaande claim type als **uid** beheren. Klik op **Voltooien**, zoals in de afbeelding wordt weergegeven:

Add Transform Claim R	ule Wizard				×
Configure Rule					
Steps Choose Rule Type Configure Claim Rule	You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.				
	Name Rule Attrib	HD template: Send LDAP Attributes : ute store:	as Claims		
	Activ	e Directory ing of LDAP attributes to outgoin	ng claim type	• •	
		LDAP Attribute		Outgoing Claim Type	-
	*		-		-
			< Pre	evious Finish Cancel	Help

Voeg de aangepaste regel toe voor het vertrouwende partij. Klik op **Toevoegen**. Selecteer **Vorderingen verzenden met behulp van een Aangepaste regel** en klik vervolgens op **Volgende**, zoals in de afbeelding:

🍿 Add Transform Claim Ru	ule Wizard	×
Select Rule Templat	e	
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 • Tell me more about this rule template	
	< Erevious Next > Cancel Help]

In het configureren van de regel typt u een naam van de regel van de claim en kopieert u vervolgens de regel van de claim in het veld Aangepaste regel in het veld Aangepaste regel in de wizard die de naam en de SPANNER-kwaliteit wijzigt in de regel van de claim. Klik op **Voltooien**. zoals in de afbeelding wordt weergegeven:

Eis:

```
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.

oningure nule				
Steps Choose Rule Type Configure Claim Rule	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, type one or more optional conditions and an issuance statement using the AD FS 2.0 claim rule language.			
	Cluster_Side_Claim_Rule Rule template: Send Claims Using a Custom Rule Custom adu			
	<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			

Zoals in de afbeelding wordt weergegeven, klikt u op **Toepassen** en vervolgens **OK**.

Irder Hu Na	le Name melD des Cide Claime	Dula	Issued Claims uid	
Clu	ster_Side_Ulaim_i	Hule	<see claim="" rul<="" th=""><th>e></th></see>	e>
				4
	1	1	1	

Stap 4: SAML SSO inschakelen

Open een webbrowser, logt u in bij CUCM als beheerder en navigeer **naar Systeem > SAML** Single Sign On.

Standaard wordt **Cluster Wide** radioknop geselecteerd. Klik op **SSO** inschakelen zoals in de afbeelding:



Zoals in de afbeelding wordt getoond, waarschuwt het pop-up de waarschuwing voor het opnieuw opstarten van een webserver en informatie om de clusterbrede SAML SSO of Per-Node SAML SSO naar gelang idp te kiezen. Klik op **Doorgaan**.



De criteria om voor een Cluster-brede SSO beschikbaar te maken zijn dat u een multiservertomatecertificaat moet hebben dat al is ingevoerd. Klik op **Test voor Multi-Server om certificaat te verkrijgen**, zoals in de afbeelding wordt getoond:

Net Status Status: Ready Test for Multi-Server tomcat certificate
Status Status: Ready Test for Multi-Server tomcat certificate
Test for Multi-Server tomcat certificate
Test for Multi-Server tomcat certificate
The criteria for enabling dusterwide SSO is 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 Administration Page and Navigate to Certificate Management under Security Menu
2) Clck 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

Zodra dit bevestigd is, hebben alle knooppunten een multi-server certificaat weergegeven en **hebben alle knooppunten een multi-server certificaat** en klikt u vervolgens op **Volgende**, zoals in de afbeelding:

SAML Single Sign-On Configuration
Next 1
r Status
Status: Ready
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 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

Klik op Volgende zoals in de afbeelding.

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 meta import it to your servers. You will need to manually obtain the file from the IdP before you can upload servers.	idata from your IdP and 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.	

Bladeren en selecteer de gedownload IDP-metadata. Klik op **de Metagegevens van IDP importeren**, zoals in de afbeelding wordt getoond:

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

De pagina bevestigt dat Importeren voor alle servers is gelukt en vervolgens op **Volgende** klikt, zoals in de afbeelding:

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 VIII Import succeeded for all servers
Next Cancel

Zoals in de afbeelding wordt getoond, klikt u op **Volgende**, aangezien de SSP-metagegevens al zijn geëxporteerd vanuit de oorspronkelijke SAML SETH-configuratiescherm.

SAML Single Sign-On Configuration
Back Next
- Ctatus
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 IdD-
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 moet in sync zijn met de LDAP-map. De wizard geeft de geldige beheerder aan die in de LDAP-map is ingesteld. Selecteer de gebruiker en klik op **Test SSO uitvoeren**, zoals in de afbeelding:

AML Single Sign-On Configur	ration
Back	
Status The server metadata file mu	st be installed on the IdP before this test is run.
est SSO Setup	
This test verifies that the metada run on any server for troublesho successful.	ata files are correctly configured and will allow SSO to start up on the servers. This test can be oting once SSO has been enabled. SSO setup cannot be completed unless this test is
1)Pick a valid username to use fo	or this test
You must already know the pass This user must have administrate Please use one of the Userr lockout.	word for the selected username. or rights and also exist in the IdP. names shown below. Using any other Username to log into the IdP may result in administrator
/alid administrator Usernames	
samluser	
2)Launch SSO test page Run SSO Test	

Voer, zoals in de afbeelding, de gebruiker-ID en het bijbehorende wachtwoord in nadat deze is gevraagd.

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

De pop-up, zoals in de afbeelding wordt getoond bevestigt dat de test succesvol is.



Zoals in de afbeelding wordt weergegeven, klikt u op **Voltooien** om de configuratie voor het inschakelen van de SSO te voltooien.

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administra
SAML Single Sign-On Configuration
Back Finish
- Statue
Status
SSO Metadata Test Successful
Ready to Enable SSO
Clicking "Finish" will complete enabling SSO on all the servers in this cluster. There will be a short delay while the applications are
being updated.
To walf the CCO status of each server shall the said CCO Configuration and
Additional testing and manual uploads may be performed from the main page if percessary.
readenar cesting and manade aprovabiliting be performed from the main page if neccessary.
Back Finish Cancel

De pagina in de afbeelding bevestigt dat het SAML SSO-instelproces op alle servers is gestart.



Log in op CUCM met SAML SSO-referenties. Navigeer naar **Systeem > SAML single aanmelding**. Klik op **SSO Test** om andere knooppunten in de cluster te testen, zoals in de afbeelding:

SAML Single Sign-On							
SSO Mode Cluster wide (One metadat Per node (One metadata fi	ta file per cluster. le per node)	Requires m	ulti-server Tomcat certificate))			
🗙 Disable SAML SSO 👔	Export All Metadata	🔞 Upda	nie klip Metadata File 🧳 Fix	All Disabled Sen	vers		
RTMT is enabled for SSO SAML SSO enabled SAML Single Sign-On	 You can change You can change<th>e SSO for R</th><th>TMT <u>here.</u></th><th></th><th></th><th>Row</th><th>s per Page 50 🔻</th>	e 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

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Controleer of de SSO-test succesvol is voor de knooppunten die zijn geactiveerd met de SAML SSO. Blader naar **systeem > SAML single aanmelding**. Een succesvolle SSO-test toont de status die is goedgekeurd.

SAML Single Sign-On							
SSO Mode Cluster wide (One metadai Per node (One metadata fi	ta file per clu le per node)	ster. Requires n	nulti-server Tomcat certificate))			
🗙 Disable SAML SSO 👔	Export All Metz	idata 👩 Upd	iate IdP Metadata File 🧳 Fix.	All Disabled Ser	vers		
RTMT is enabled for SSO SAML SSO enabled). You can ch	ange SSO for R	ITMT <u>here.</u>			Baue	nar Dana SD. 💌
Server Name	SSO Status	Re-Import Netadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test	
cucm1150.adfs.ucce.com	SAML	N/A	June 20, 2016 9:57:30 AM IST	🏄 File	June 20, 2016 10:06:27 PM IST	Passed - June 20, 2016 9:59:02 PM IST	Run SSO Test
cucm1150sub.adfs.ucce.com	SAML	🔶 IdP	June 20, 2016 10:15:46 PM IST	🎂 File	June 20, 2016 10:06:26 PM IST	Passed - June 20, 2016 10:11:39 PM IST	Run SSO Test
imp115.adfs.ucce.com	SAML	star 💠 🕂	June 20, 2016 10:15:46 PM IST	🎂 File	June 20, 2016 10:06:26 PM IST	Passed - June 20, 2016 10:12:40 PM IST	Run SSO Test
Disable SAML SSO Exp	ort All Metad	ata Update	IdP Metadata File Fix All I	Disabled Serve	rs		

Nadat het SAML SSP-systeem is geactiveerd, worden de geïnstalleerde toepassingen en de Platform-toepassingen vermeld voor de CUCM-inlogpagina, zoals in deze afbeelding wordt weergegeven.

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

Nadat de SAML SSO is geactiveerd, worden de geïnstalleerde toepassingen en de Platformtoepassingen vermeld voor IM and Presence inlogpagina, zoals in deze afbeelding wordt weergegeven:

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

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Om de SSO-logbestanden te debug in te stellen, gebruikt u de opdracht **om BEELDNIVEAU DEBUG in te stellen**

Verzamel de SSO-bestanden met RTMT of activelog /tomcat/logs/ssosp/log4j/*.log locatie met behulp van CLI.

Voorbeeld van SSO-logs toont de metagegevens die zijn gegenereerd en naar andere knooppunten worden verzonden

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