Konfiguration einer einzelnen SAML-IDP-Verbindung/Vereinbarung pro Cluster mit AD FS Version 2.0

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Schritt 1: SP-Metadaten aus CUCM exportieren Schritt 2: IDP-Metadaten von AD FS herunterladen Schritt 3: Bereitstellungs-IDP Schritt 4: SAML SSO aktivieren Überprüfen Fehlerbehebung

Einführung

In diesem Dokument wird beschrieben, wie die SAML (Single Security Assertion Markup Language) Identity Provider-Verbindung bzw. -Vereinbarung pro Cluster mit AD FS (Active Directory Federation Service) konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Unified Communications Manager (CUCM) 11.5 oder höher
- Cisco Unified Communications Manager IM und Presence, Version 11.5 oder höher
- Active Directory Federation Service Version 2.0

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

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

Hintergrundinformationen

Bei SAML SSO muss es sich um einen Vertrauenskreis zwischen dem Service Provider (SP) und dem IdP handeln. Diese Vertrauenswürdigkeit wird im Rahmen von SSO Enablement erstellt, wenn Vertrauenswürdigkeit (Metadaten) ausgetauscht wird. Laden Sie die Metadaten vom CUCM herunter und laden Sie sie auf IdP hoch, laden Sie die Metadaten ähnlich von IdP herunter und laden Sie sie in CUCM hoch.

Vor CUCM 11.5 generiert der Ausgangsknoten die Metadatendatei. Außerdem werden die Metadatendateien von anderen Knoten im Cluster gesammelt. Es fügt alle Metadatendateien einer einzelnen ZIP-Datei hinzu und präsentiert sie dann dem Administrator. Der Administrator muss diese Datei entpacken und alle Dateien auf der IDP bereitstellen. Beispielsweise 8 Metadatendateien für einen Cluster mit 8 Knoten.

Eine SAML-ID-Verbindung/Vereinbarung pro Cluster-Funktion wird ab 11.5 eingeführt. Im Rahmen dieser Funktion generiert CUCM eine einzige Metadatendatei für Service Provider für alle CUCMund IMP-Knoten im Cluster. Das neue Namensformat für die Metadatendatei ist **<hostname>**single-agreement.xml

Grundsätzlich erstellt ein Knoten die Metadaten und leitet sie an andere SP-Knoten im Cluster weiter. Dadurch wird die Bereitstellung, Wartung und Verwaltung vereinfacht. Beispiel: 1 Metadatendatei für einen Cluster mit 8 Knoten.

Die Metadatendatei für den Cluster verwendet ein Multiserver-Tomcat-Zertifikat, das sicherstellt, dass das Schlüsselpaar für alle Knoten im Cluster identisch ist. Die Metadatendatei verfügt außerdem über eine Liste von ACS-URLs (Assertion Consumer Service) für die einzelnen Knoten im Cluster.

CUCM und Cisco IM and Presence Version 11.5 unterstützen sowohl die SSO-Modi, **clusterweit** (eine Metadatendatei pro Cluster) und pro Knoten (vorhandenes Modell).

In diesem Dokument wird beschrieben, wie der clusterweite Modus der SAML SSO mit AD FS 2.0 konfiguriert wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Schritt 1: SP-Metadaten aus CUCM exportieren

Öffnen Sie einen Webbrowser, melden Sie sich als Administrator bei CUCM an, und navigieren Sie **zu System > SAML Single Sign On.**

Standardmäßig ist **das** Optionsfeld **Clusterweit** aktiviert. Klicken Sie auf **Alle Metadaten exportieren**. Die Metadatendatei wird dem Administrator im Namen **<hostname>-single-agreement.xml** präsentiert.



Schritt 2: IDP-Metadaten von AD FS herunterladen

Informationen zum Herunterladen von IdP-Metadaten finden Sie unter <u>https:// <FQDN des</u> <u>ADFS>/federationmetadata/2007-06/federationmetadata.xml</u>

Schritt 3: Bereitstellungs-IDP

Navigieren Sie, wie im Bild gezeigt, zu AD FS 2.0 Management/Trust Relation Ships/Relying Party Trust. Klicken Sie auf Vertrauenswürdige Partei hinzufügen.

📬 AD F5 2.0		-0	×	
Rife Action View Window Help		_ <u></u>	×	
4 📫 🔁 🖬 🔛 🖬	Debine Dealer Treats	Actions	_	
Service Toust Relationships	Display Name	Relying Party Trusts	-	
Claims Provider Trusts		Add Relying Party Trust		
Relying Party Trusts		View New Window from Here	•	
	1	Refresh		
	•	Help		
J	(1974)			

Der Assistent für das Hinzufügen von Gruppenvertrauen wird geöffnet, wie im Bild gezeigt. Klicken Sie jetzt auf **Start**.

Madd Relying Party Tru	st Wizard	×
Welcome		
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

Klicken Sie auf Importdaten, die angeben, ob eine Partei aus einer Datei stammt. Durchsuchen Sie die von der CUCM SAML SSO-Konfigurationsseite heruntergeladenen SP-Metadaten. Klicken Sie anschließend auf **Weiter**, wie im Bild gezeigt:

📬 Add Relying Party Trus	t 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: 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. Federation 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: [C:\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>Previous</u> <u>Next</u> Cancel <u>H</u> elp	

Geben Sie den Display Name (Anzeigenamen) und alle optionalen Notizen für die Relying Party (Partei) ein. Klicken Sie auf **Weiter**, wie im Bild gezeigt:

📬 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:	×
	< Previnus Next > Car	acel [Help]

Wählen Sie **Zulassen aller Benutzer für den Zugriff auf diese vertrauliche Partei**, um allen Benutzern den Zugriff auf diese Partei zu gestatten, und klicken Sie dann auf **Weiter**, wie im Bild gezeigt:

📬 Add Relying Party Trust	: Wizard
Choose Issuance Au	thorization Rules
Steps 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 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.
	< Previous Next > Cancel Help

Auf der Seite **Ready to Add Trust (Bereit zum Hinzufügen von Vertrauenswürdigkeit)** können Sie die Einstellungen für die konfigurierte Relying Party Trust (Vertrauenswürdigkeit) überprüfen. Klicken Sie jetzt auf **Weiter**, wie im Bild gezeigt:

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 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 or: < never >

Finish Page (Abschließende Seite) bestätigt, dass die Vertrauenswürdigkeit der Partei erfolgreich der AD FS-Konfigurationsdatenbank hinzugefügt wurde. Deaktivieren Sie das Kontrollkästchen, und klicken Sie auf **Schließen**, wie im Bild gezeigt:

📬 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 snap-in.	

Klicken Sie mit der rechten Maustaste auf **Relying Party Trusts**, und klicken Sie auf **Edit Claim Rules** (Anspruchsregeln bearbeiten), wie im Bild gezeigt:

AD FS 2.0	Heb			- O ×
(* *) (2) (m) 🖸 (m)				
AD FS 2.0	Relying Party Trusts			Actions
Service Trust Relationships	Display Name 💌	Enabled	Identifier	Relying Party Trusts 🔺 🔺
Claims Provider Trusts	CUCM_Cluster_Wide_Relying_Party_trust	Yes	cucm1150.adls.ucce.com	Add Relying Party Trust
Relying Party Trusts				View
ACTING Stores	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
				Help
				1 -

Klicken Sie jetzt auf Regel hinzufügen, wie im Bild gezeigt:

Edit Claim Rules for CUCM_Cluster_Wide_R	telying_Party_trust	_ 🗆 🗙
Issuance Transform Rules Issuance Authorization	Rules Delegation Authorization R	ules
The following transform rules specify the claims th	at will be sent to the relying party.	
Order Dule Name	Loured Claims	
		1
Add Dula L Edit Dula L Damaus Dul		
	3	
 пк 1	Cancel Applu	Help
	Concor Appy	Пар

Wenn die **Regel für das Hinzufügen von Umwandlungsforderungen** geöffnet wird, klicken Sie auf **Weiter** mit der Standardlastenvorlage **LDAP-Attribute als Ansprüche senden**, wie im Bild gezeigt:

iteps	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 may be sent as nulliple 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.			
	C Previous Next > Cancel Help			

Klicken Sie auf **Anspruchsregel konfigurieren**, wie in diesem Bild gezeigt. Das LDAP-Attribut muss mit dem LDAP-Attribut in der LDAP-Verzeichniskonfiguration im CUCM übereinstimmen. Verwalten Sie den ausgehenden Anspruchtyp als **uid**. Klicken Sie auf **Fertig stellen**, wie im Bild gezeigt:

Add Transform Claim R	ule Wizard				2
Configure Rule					
Steps Choose Rule Type Configure Claim Rule	You o which issue Claim	an configure this rule to send the to extract LDAP attributes. Spe d from the rule. rule name:	e values of L city how the	DAP attributes as claims. Select an attribute store attributes will map to the outgoing claim types that	from will be
	Rule	template: Send LDAP Attributes ute store:	as Claims		
	Mapp	e Directory	ng claim type	• • • • • • • • • • • • • • • • • • •	
		LDAP Attribute		Dutgoing Claim Type	-
	*		-		-
			< Pre	evious Finish Cancel I	Help

Fügen Sie die benutzerdefinierte Regel für die vertrauende Partei hinzu. Klicken Sie auf **Regel hinzufügen**. Wählen Sie **Anträge mit einer benutzerdefinierten Regel senden aus,** und klicken Sie dann auf **Weiter,** wie im Bild gezeigt:

🃬 Add Transform Claim R	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 <u>Tell me more about this rule template</u>		
	< Brevious Next > Cancel Help		

Geben Sie in der Regel zur Anspruchskonfiguration einen Namen für eine Anspruchsregel ein, und kopieren Sie anschließend die angegebene und die Vergangenheit der Anspruchsregel im Feld Benutzerdefinierte Regel im Assistenten. Damit wird der Namensgleichrichter und der Spname-Qualifizierer in der Anspruchsregel geändert. Klicken Sie auf **Fertig stellen**, wie im Bild gezeigt:

Anspruchsregel:

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,
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =</pre>
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =</pre>
"http:// <fqdn adfs="" of="">/adfs/com/adfs/services/trust",</fqdn>
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =</pre>
" <entity id="" in="" metadata="" sp="" the="">");</entity>

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

Muu Transform Claim K			
Configure Rule			
iteps	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts		
Choose Rule Type	claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an insurance 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		

Klicken Sie, wie im Bild gezeigt, auf Übernehmen und dann auf OK.

Irder	Hule Name NamelD Cluster, Side, C	aim Bule	uid <see claim="" rule=""></see>	
				4
Vaa Di	le Edite	ule Bemove	Bule 1	

Schritt 4: SAML SSO aktivieren

Öffnen Sie einen Webbrowser, melden Sie sich als Administrator bei CUCM an, und navigieren Sie **zu System > SAML Single Sign On**.

Standardmäßig ist **das** Optionsfeld **Clusterweit** aktiviert. Klicken Sie auf **Saml SSO aktivieren**, wie im Bild gezeigt:



Wie im Bild gezeigt, benachrichtigt das Popup-Fenster die Warnung für den Neustart des Webservers und informiert, dass die clusterweite SAML SSO oder Per-Node SAML SSO gemäß idp ausgewählt wird. Klicken Sie auf **Weiter**.



Das Kriterium für die Aktivierung der clusterweiten SSO besteht darin, dass Sie bereits über ein Multiserver-Tomcat-Zertifikat verfügen müssen. Klicken Sie auf **Test for Multi-Server Tomcat Certificate**, wie im Bild gezeigt:

SAML Single Sign-On Configuration
Next
Status
Status: Ready
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 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
 Restart Tomcat service on all the nodes in the cluster
Restart TFTP service on all the TFTP nodes 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 certificate
Next Cancel

Nach der Bestätigung wird für alle Knoten das Multi-Server-Zertifikat angezeigt. Alle Knoten verfügen über das Multi-Server-Zertifikat, und klicken Sie dann auf Weiter, wie im Bild gezeigt:

SAML Single Sign-On Configuration
Next 1
_ Status
(i) 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 Tomost
4) decir Devinduoli da Indu-Server S) Cirk Cenerate
6) Download the CSR and set it skined 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

Klicken Sie, wie im Bild gezeigt, auf Weiter.

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 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

Durchsuchen und wählen Sie die heruntergeladenen IdP-Metadaten aus. Klicken Sie auf **Import IdP Metadata**, wie im Bild gezeigt:

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

Die Seite bestätigt den für alle Server erfolgreich importierten Import, und klicken Sie dann auf **Weiter**, wie im Bild gezeigt:

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 VIII Import succeeded for all servers
Next Cancel

Klicken Sie, wie im Bild gezeigt, auf **Weiter**, da die SP-Metadaten bereits von der ersten SAML SSO-Konfigurationsseite exportiert wurden.

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 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 muss mit dem LDAP-Verzeichnis synchronisiert sein. Der Assistent zeigt die gültigen, im LDAP-Verzeichnis konfigurierten Administratorbenutzer an. Wählen Sie den Benutzer aus, und klicken Sie auf **SSO-Test ausführen**, wie im Bild gezeigt:

AML Single Sign-On Configuration	
Back	
Status The server metadata file must be insta	alled on the IdP before this test is run.
Test SSO Setup	
This test verifies that the metadata files are run on any server for troubleshooting once successful.	e correctly configured and will allow SSO to start up on the servers. This test can be a SSO has been enabled. SSO setup cannot be completed unless this test is
1)Pick a valid username to use for this test	
You must already know the password for the This user must have administrator rights an Please use one of the Usernames sho lockout.	he selected username. nd also exist in the IdP. wwn 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	
Back Cancel	

Geben Sie, wie im Bild gezeigt, die Benutzer-ID und das entsprechende Kennwort ein, sobald Sie dazu aufgefordert werden.

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

Wie im Bild gezeigt, bestätigt das Popup-Fenster, dass der Test erfolgreich war.



Klicken Sie, wie im Bild gezeigt, auf **Fertig stellen**, um die Konfiguration für die Aktivierung der SSO abzuschließen.

System 🔹 Call Routing 👻 Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻 User Management 👻 Bulk Administra
SAML Single Sign-On Configuration
Back Finish
Ctatue
Status
SSO Metadata Test Successful
Ready to Enable SSO
Clicking "Einich" will complete enabling SSO on all the centers in this cluster. There will be a short delay while the applications are
being updated.
To verify the SSO status of each server, check the main SSO Configuration page.
Additional testing and manual uploads may be performed from the main page if neccessary.
Back Finish Cancel

Die im Bild angezeigte Seite bestätigt, dass der SAML SSO-Aktivierungsprozess auf allen Servern initiiert wird.



Melden Sie sich mit SAML SSO-Anmeldeinformationen ab, und melden Sie sich wieder beim CUCM an. Navigieren Sie zu System >SAML Single Sign On. Klicken Sie auf SSO-Test für andere Knoten im Cluster ausführen, wie im Bild gezeigt:

SAML Single Sign-On							
SSO Mode Cluster wide (One metadat 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	a 🔞 Upd	ale kdP Metadata File 🥜 Fix	All Disabled Ser	vers		
ATMT is enabled for SSO SAML SSO enabled SAML Single Sign-On (1)	 You can chan t - 3 of 3) 	ge SSO for R	ITMT <u>here.</u>			Row	s per Page 50 🔻
Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test	
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

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestätigen Sie, dass der SSO-Test für die Knoten erfolgreich ist, für die SAML SSO aktiviert ist. Navigieren Sie zu **System >SAML Single Sign On**. Erfolgreiche SSO-Tests zeigen den Status Bestanden an.

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		

Nach Aktivierung der SAML SSO werden installierte Anwendungen und Plattformanwendungen für die CUCM-Anmeldeseite aufgelistet, wie in diesem Bild gezeigt.

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

Nach Aktivierung der SAML SSO werden installierte Anwendungen und Plattformanwendungen für die Anmeldeseite IM und Presence aufgelistet, wie in diesem Bild gezeigt:

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

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Um die SSO-Protokolle auf Debuggen festzulegen, verwenden Sie den Befehl **SampleTrace Level DEBUG.**

Erfassen Sie die SSO-Protokolle mithilfe von RTMT oder vom Speicherort **activelog** /tomcat/logs/ssosp/log4j/*.log mithilfe der CLI.

Beispiel für SSO-Protokolle zeigt die generierten und an andere Knoten gesendeten Metadaten

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