# Unified Communications Manager Version 10.5 SAML SSO - Konfigurationsbeispiel

### Inhalt

Einführung Voraussetzungen Anforderungen Network Time Protocol (NTP)-Einrichtung DNS-Einrichtung (Domain Name Server) Verwendete Komponenten Hintergrundinformationen Konfigurieren Netzwerkdiagramm Verzeichniseinrichtung SAML SSO aktivieren Überprüfen Fehlerbehebung

## Einführung

In diesem Dokument wird beschrieben, wie die SAML (Security Assertion Markup Language) Single Sign-On (SSO) für Cisco Unified Communications Manager (CUCM) konfiguriert und verifiziert wird.

### Voraussetzungen

### Anforderungen

#### Network Time Protocol (NTP)-Einrichtung

Damit SAML SSO funktioniert, müssen Sie die richtige NTP-Konfiguration installieren und sicherstellen, dass die Zeitdifferenz zwischen dem Identity Provider (IdP) und den Unified Communications-Anwendungen drei Sekunden nicht überschreitet.

Bei zeitlicher Abweichung zwischen CUCM und IdP wird folgender Fehler angezeigt: "Ungültige SAML-Antwort." Dieser Fehler kann auftreten, wenn die Zeit zwischen den CUCM- und IDP-Servern nicht synchronisiert ist. Damit SAML SSO funktioniert, müssen Sie die richtige NTP-Konfiguration installieren und sicherstellen, dass die Zeitdifferenz zwischen der IDP und den Unified Communications-Anwendungen drei Sekunden nicht überschreitet.

Weitere Informationen zur Synchronisierung von Uhren finden Sie im Abschnitt "NTP Settings" (NTP-Einstellungen) im <u>Administratorleitfaden für das Cisco Unified Communications-</u> <u>Betriebssystem</u>.

#### DNS-Einrichtung (Domain Name Server)

Unified Communications-Anwendungen können DNS verwenden, um vollständig qualifizierte Domänennamen (FQDNs) in IP-Adressen aufzulösen. Die Service Provider und die IdP müssen vom Browser auflösbar sein.

#### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Active Directory Federation Service (AD FS) Version 2.0 als IDP
- CUCM-Version 10.5 als Service Provider
- Microsoft Internet Explorer 10

**Vorsicht**: Dieses Dokument basiert auf einem neu installierten CUCM. Wenn Sie SAML SSO auf einem bereits in der Produktion befindlichen Server konfigurieren, müssen Sie möglicherweise einige der Schritte entsprechend überspringen. Wenn Sie die Schritte auf dem Produktionsserver durchführen, müssen Sie auch die Auswirkungen auf den Dienst verstehen. Es wird empfohlen, dieses Verfahren außerhalb der Geschäftszeiten durchzuführen.

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.

### Hintergrundinformationen

SAML ist ein XML-basiertes, auf offenen Standards basierendes Datenformat, das Administratoren den nahtlosen Zugriff auf bestimmte Cisco Collaboration-Anwendungen ermöglicht, nachdem sie sich bei einer dieser Anwendungen angemeldet haben. SAML SSO erstellt beim Austausch von Metadaten im Rahmen des Bereitstellungsprozesses zwischen dem IdP und dem Service Provider einen Circle of Trust (CoT). Der Service Provider vertraut den Benutzerinformationen der ID, um den Zugriff auf die verschiedenen Dienste oder Anwendungen zu ermöglichen.

**Hinweis**: Service Provider sind nicht mehr an der Authentifizierung beteiligt. SAML Version 2.0 delegiert die Authentifizierung von den Service Providern und den IdPs. Der Client authentifiziert sich anhand der IdP, und der IdP gewährt dem Client eine Assertion. Der Client stellt dem Dienstanbieter die Assertion dar. Da ein CoT eingerichtet ist, vertraut der Service Provider der Assertion und gewährt dem Client Zugriff.

### Konfigurieren

#### Netzwerkdiagramm



Figure :SAML Single sign SSO Call Flow for Collaboration Servers

### Verzeichniseinrichtung

1. Wählen Sie Cisco Unified CM Administration > System > LDAP > LDAP System aus.



- 2. Klicken Sie auf Neu hinzufügen.
- 3. Servertyp und -attribut für das Lightweight Directory Access Protocol (LDAP) konfiguriert.
- 4. Wählen Sie Synchronisierung vom LDAP-Server aktivieren aus.

LDAP System Configurat	tion
Save	
- Status	
(1) Status: Ready	
-LDAP System Informati	ion —
🗹 Enable Synchronizing fr	rom LDAP Server
LDAP Server Type	Microsoft Active Directory
LDAP Attribute for User ID	sAMAccountName 💌
Save	

- 5. Wählen Sie Cisco Unified CM Administration > System > LDAP > LDAP Directory aus.
- 6. Konfigurieren Sie diese Elemente:

Kontoeinstellungen für LDAP-VerzeichnisseZu synchronisierende BenutzerattributeSynchronisierungsplanHostname oder IP-Adresse des LDAP-Servers und Portnummer

LDAP Directory	
🔚 Save 🗶 Delete 🗋 Copy 👔	Perform Full Sync Now 🕂 Add New
Status	
(i) Status: Ready	
LDAP Directory Information	
LDAP Configuration Name*	LDAP
LDAP Manager Distinguished Name*	CN=Administrator,CN=Users,DC=ciscolive,DC=com
LDAP Password*	•••••
Confirm Password*	•••••
LDAP User Search Base*	CN=Users,DC=ciscolive,DC=com
LDAP Custom Filter	< None >

7. Deaktivieren Sie **SSL verwenden**, wenn Sie Secure Socket Layer (SSL) nicht verwenden möchten, um mit dem LDAP-Verzeichnis zu kommunizieren.

**Tipp**: Wenn Sie LDAP über SSL konfigurieren möchten, laden Sie das LDAP-Verzeichniszertifikat auf CUCM hoch. Informationen zum Synchronisierungsmechanismus für bestimmte LDAP-Produkte und allgemeine Best Practices für die LDAP-Synchronisierung finden Sie im LDAP-Verzeichnisinhalt in <u>Cisco Unified Communications Manager SRND</u>.

 Klicken Sie auf Speichern und führen Sie die vollständige Synchronisierung jetzt aus. Hinweis: Vergewissern Sie sich, dass der Cisco DirSync-Dienst auf der Webseite Serviceability aktiviert ist, bevor Sie auf Save (Speichern) klicken.

	LUAP Port Ose 55L
adfs1.ciscolive.com	3268
Add Another Redundant LDAP Server	

 Navigieren Sie zu Benutzerverwaltung > Endbenutzer, und wählen Sie einen Benutzer aus, dem Sie die CUCM-Verwaltungsrolle zuweisen möchten (in diesem Beispiel wird SSO für Benutzer ausgewählt).

System +	Call Routing 👻 Med	ia Resources 👻 🗛	dvanced Features 👻	Device 👻	Application +	User Management 👻	Bulk Administration		•
Find and	l List Users								
🕂 Add	New Eslect All	🖽 Clear All 🙀	Delete Selected						
Status									
<b>()</b> 3 re	cords found								
User	(1 - 3 of 3)								Rows p
Find Use	r where First name		begins with 🖃			Find Clear Filter	4 -		
		First Name	Last Name		Department	Directory L	JRI		Upor Status
	User ID					, -			User Status
	550	Saml	SSO			,	Active	LDAP Synd	chronized User

10. Blättern Sie nach unten zu den Berechtigungsinformationen, und klicken Sie auf Zu Zugriffskontrollgruppe hinzufügen. Wählen Sie Standard CCM Super Users aus, klicken Sie auf Auswahl hinzufügen, und klicken Sie auf Speichern.

oups	Standard CCM Super Users		
			Add to Access Control Group
			Remove from Access Control Group
		View Details	
les	Standard AXL API Access		
	Standard Admin Rep Tool Admin		
	Standard CCM Admin Users		
	Standard CUReporting	View Details	
	Istandard Cokeporting	View Details	

#### SAML SSO aktivieren

1. Melden Sie sich bei der Benutzeroberfläche der CUCM-Verwaltung an.

2. Wählen Sie **System > SAML Single Sign-On**, und das Fenster SAML Single Sign-On Configuration wird geöffnet.

<u>@</u> c	isco Unified CM Console - Windows I	nternet Explorer						
G	🔿 🗢 💋 https://cucm. ciscolive.com	/ccmadmin/showHome.do	🔸 🗙 🖟					
	Favorites 👍 🍘 Suggested Sites 🕶	C Web Slice Gallery -						
6	Cisco Unified CM Console		🙆 -					
	Server	1 Administration	Navigation					
	Cisco Unified CM	unications Solutions	ccmadmin					
	Cisco Unified CM Group	es 👻 Advanced Features 👻 Device 👻 Application 👻 User Management 👻	Bulk Administra					
	Presence Redundancy Groups							
	Phone NTP Reference							
	Date/Time Group	g on demo licenses that will expire in 60 days. Add this systen ficient licenses to cover its usage before expiration in order to						
	BLF Presence Group							
	Region Information	vices.						
	Device Pool	levice is configured. This is required to recover your	system in					
	Device Mobility							
	DHCP	dministration						
	LDAP •	5						
	SAML Single Sign-On	el(R) Xeon(R) CPU E5-2690 0 @						
	Cross-Origin Resource Sharing (CORS)	6Mbytes RAM, Partitions aligned						
	Location Info	) ago						
	MLPP +							
	Obvisional Location							

3. Um die SAML-SSO für den Cluster zu aktivieren, klicken Sie auf SAML-SSO aktivieren.

SAML Single Sign-O	n								
🤣 Enable SAML SSD 🔀 Export All Netadata 🔞 Update KIP Metadata File 🥜 Fix All Disabled Servers									
-Status	- Status								
() SAML SSO disabl	ed								
SAML Single Sign-									
Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Text			
CUCM	Disabled	N/A	Never	📥 File	March 30, 2011 7:57:56 PM CEST	Never Run SSO Test			

4. Klicken Sie im Fenster Warnung zurücksetzen auf Weiter.

//cucm.ciscolive.com/?windowtitlekey=genericdialogwindow.windowtitle.ssoenablewindowtitle	- 🗆 🗡
	*
Web server connections will be restarted	
Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again.	
Click "Export All Metadata" button	
If the server metadata has not already been uploaded to the IdP, it can be done before running the wizard. You can obtain the server metadata by clicking the "Export All Metadata" button on the main page. Then go to the IdP and upload the file.	
Continue Cancel	
	-
Done	6 • <i>//</i> .

5. Klicken Sie auf dem SSO-Bildschirm auf **Durchsuchen**, um die XML-Datei IDP (FederationMetadata.xml)-Metadaten mit dem Schritt IdP-Metadaten zu importieren.

System +	Call Routing 👻	Media Resources 👻	Advanced Features 👻	Device 👻	Application +	User Management 👻	Bulk Administration +	Help 🕶	
SAML Sir	gle Sign-On	Configuration							
Next									
i Status	is: Ready								
- Downloa To config manually	- Download Identity provider(IdP) Metadata Trust File- To configure the trust relationship between the IdP and your devices, you must first obtain trust metadata from your IdP and import it to your servers. You will need to manually obtain the file from the IdP before you can upload it to your Collaboration servers.								
🔥 This	is a manual st	epi							
1)Log in t	o your IdP and	download the meta	data trust file to your l	ocal server					
2)Click 'N	ext' once you h	have this file availab	le locally.						
Next	Cancel								

6. Klicken Sie nach dem Hochladen der Metadatendatei auf **IDP-Metadaten importieren**, um die IDP-Informationen in CUCM zu importieren. Bestätigen Sie, dass der Import erfolgreich war, und klicken Sie auf **Weiter**, um fortzufahren.

System +	Call Routing 👻	Media Resources	<ul> <li>Advanced Features +</li> </ul>	Device 👻	Application +	User Management 👻	Bulk Administration 👻	Help 🕶
SAML Sin	gle Sign-On	Configuration						
Next								
-Status -								
(i) Read	y to import I	dentity Provider me	tadata trust file to clust	er servers				
-Import t	he IdP Meta	data Trust File-						
This step (	uploads the fi	le acquired from th	e IdP in the previous m	anual step to	the Collabora	tion servers.		
1)Select ti	he IdP Metad	ata Trust File						
C:\Users	Administrato	r\Desktop\Federati	onMetadata.xml		Browse			
2)Import (	this file to the	Collaboration serv	ers					
This action	n must be suc	cessful for at least	the Publisher before mo	wing on to th	e next task ir	this wizard.		
Imp	ort IdP Met	adata						
Next C	ancel							
SAML Sin	gle Sign-Or	n Configuration						
Next								
-Status-								
V Impo	ort succeeded	for all servers						
Tanaat	the IdD Met	adata Teust File-						
This step	uploads the f	ile acquired from the	e IdP in the previous m	anual step to	the Collabora	tion servers.		
1)Select t	he IdP Metad	ata Trust File						
					Browse			
2)Import	this file to the	Collaboration ser	vers					
This actio	n must be su	ccessful for at least	the Publisher before m	oving on to th	ie next task ir	this wizard.		
Im	oort IdP Met	adata				A import sur	ceeded for all server	5

7. Klicken Sie auf Trust Metadata File herunterladen (optional), um die CUCM- und CUCM IMund Presence-Metadaten in einem lokalen Ordner zu speichern, und gehen Sie zu Add <u>CUCM as Relying Party Trust</u>. Wenn die AD FS-Konfiguration abgeschlossen ist, fahren Sie mit Schritt 8 fort.

Next Cancel

SAML Single Sign-On Configuration
Hext Next
- Etalua
1 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 Service 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

8. Wählen Sie SSO als Administrator aus, und klicken Sie auf SSO-Test ausführen.

System +	Call Rout	ing 🛨	Media Resources	s <del>v</del> Advar	nced Features 👻	Device +	Application +	User Management 👻	Bulk Administration 👻	Help 🛨	
SAML SI	igle Sig	n-On	Configuration								
de Back											
- Status -											-
The	server m	etadal	ta file must be in	stalled on	the IdP before	this test is	run.				
- Test SS	0 Setup										
This test SSO has	verifies t been ena	hat the	e metadata files SSO setup cann	are correct ot be comp	ly configured a leted unless th	ind will allo is test is su	w SSO to start ccessful.	up on the servers. 1	This test can be run or	n any server for troub	leshooting once
1)Pick a v	valid user	name	to use for this t	est							
You must This user	already must ha	know l ve adr	the password fo ninistrator rights	r the select and also e	ed username. exist in the IdP.						
🔥 Plea	ise use o	ne of t	he Usernames s	hown belo	w. Using any ol	ther Userna	me to log into	the IdP may result i	n administrator lockou	ıt.	
Valid adm sso	ninistrato	r User	names								
2)Launch	SSO tes	t page									
Run	SSO Tes	t	1								
Back	Cancel	1									

 Zertifikatswarnungen ignorieren und weiter fortfahren Wenn Sie zur Eingabe der Anmeldeinformationen aufgefordert werden, geben Sie den Benutzernamen und das Kennwort für die Benutzer-SSO ein und klicken Sie auf OK.

	× Investored as white
Connecting to ADFS1.ciscolive.com.	ent website
	ercept any c
Domain: CISCOLIVE	
OK Cancel	

**Hinweis**: Dieses Konfigurationsbeispiel basiert auf selbstsignierten CUCM- und AD FS-Zertifikaten. Falls Sie Zertifikate der Zertifizierungsstelle (Certificate Authority, CA) verwenden, müssen entsprechende Zertifikate sowohl auf AD FS als auch auf CUCM installiert sein. Weitere Informationen finden Sie unter <u>Zertifikatsverwaltung und -validierung</u>.

 Nach Abschluss aller Schritte wurde der SSO-Test erfolgreich durchgeführt. wird angezeigt. Klicken Sie auf Schließen und Beenden, um fortzufahren. Sie haben nun die Konfigurationsaufgaben erfolgreich abgeschlossen, um SSO auf CUCM mit AD FS zu aktivieren.



11. Da CUCM IM und Presence wie der CUCM-Subscriber agieren, müssen Sie <u>CUCM IM und</u> <u>Presence als Relying Party Trust</u> konfigurieren und anschließend **SSO-Test ausführen**, um SAML SSO von der CUCM SAML-SSO-Seite selbst zu aktivieren.

**Hinweis**: Wenn Sie alle XML-Metadaten-Dateien aller Knoten auf IdP konfigurieren und die SSO-Operation auf einem Knoten aktivieren, ist die SAML SSO auf allen Knoten im Cluster aktiviert.

AD FS muss für alle Knoten von CUCM und CUCM IM und Presence in einem Cluster als Relay Party (Weiterleitungsgruppe) konfiguriert werden.

**Tipp**: Sie sollten auch Cisco Unity Connection und CUCM IM and Presence für SAML SSO konfigurieren, wenn Sie die SAML SSO-Erfahrung für Cisco Jabber-Clients verwenden möchten.

# Überprüfen

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

- 1. Öffnen Sie einen Webbrowser, und geben Sie den FQDN für CUCM ein.
- 2. Klicken Sie auf Cisco Unified Communications Manager.
- 3. Wählen Sie die Webanwendung (CM Administration/Unified Serviceability/Cisco Unified Reporting) aus, und drücken Sie Go, um vom AD FS zur Eingabe der Anmeldeinformationen aufgefordert zu werden. Sobald Sie die Anmeldeinformationen des Benutzers SSO eingegeben haben, werden Sie erfolgreich bei der ausgewählten Webanwendung angemeldet (CM Administration-Seite, Unified Serviceability-Seite, Cisco Unified Reporting).

Chttp://cucm.ciscolive.com/ - Windows Internet Explorer	_ # X
Coo ▼ title http://cucm.ciscolive.com/	ρ-
🖕 Favorites 🛛 🙀 🙆 Suggested Sites 🔹 🙋 Web Sice Gallery 🔹	
ádz http://cucm.ciscolive.com/	e + Safety + Tools + 🔞 +
	-
alala.	
CISCO	
cisco	
Installed Applications	
Cisco Unified Communications Manager     Description (PD)	
Cisco Unified Communications Self Care Portal	
Cisco Prime License Manager     Cisco United Reporting	
Cisco Unified Reporting     Cisco Unified Serviceability	
	_
Platform Applications	
Director Decourse Sustem	
Cisco Unified Communications OS Administration	

Hinweis: SAML SSO ermöglicht keinen Zugriff auf folgende Seiten:

- Prime Licensing Manager
- Betriebssystemverwaltung
- Disaster Recovery System

### Fehlerbehebung

Wenn Sie SAML nicht aktivieren können und sich nicht anmelden können, verwenden Sie die neue Option unter Installierte Anwendungen mit dem Namen **Recovery URL, um Single Sign-on (SSO)** zu umgehen, die verwendet werden kann, um sich mit den Anmeldeinformationen anzumelden, die während der Installation erstellt wurden, oder mit lokal erstellten CUCM Administrative Benutzern.

🔏 Cisco Unii	fied CM Console - Windows Internet Explorer			_ # ×
00-	https://cuam.dscolive.com/camadmin/showRecovery.do	💌 😨 Certificate Error	🕂 🗙 🔎 Bing	- م
🚖 Favorites	😘 🔊 Suggested Sites 🔹 🖉 Web Silce Gallery =			
🔏 Cisco Unif	fied CM Console		🚹 • 🖾 - 🖬 🖷 • I	Page - Safety - Tools - 🔞 -
cisco	Cisco Single Sign On Recovery Administration For Cisco Unified Communications Solutions	on		
Cisco This par running This par	o Single Sign On Recovery Administr ge will validate credentials locally, allowing access only to applic on this server, and will not leverage SAML SSO authentication. ge can be disabled through the CLL	ation ations that are	Username comadmin Password Login Reset	
Copyright @ All rights re:	9 1999 - 2015 Cisco Systems, Inc. served.			_
This product	t contains cryptographic features and is subject to United States and local of	ountry laws governing impo	ort, export, transfer and use. Deli	ivery of Cisco cryptographic

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Report web site.

For information about Cisco Unified Communications Manager please visit our <u>Unified Communications System Documentation</u> web site.

For Cisco Technical Support please visit our Technical Support web site.

Weitere Informationen zur Fehlerbehebung finden Sie unter <u>Problembehandlung bei SAML SSO</u> <u>für Collaboration-Produkte 10.x</u>.