Unity Connection-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 Unity Connection (UCXN) 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. Weitere Informationen zur Synchronisierung von Uhren finden Sie im Abschnitt "NTP Settings" (NTP-Einstellungen) im Administratorleitfaden für das Cisco Unified Communications-Betriebssystem.

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.

Active Directory Federation Service (AD FS) Version 2.0 muss installiert und konfiguriert werden, um SAML-Anfragen zu bearbeiten.

Verwendete Komponenten

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

- AD FS Version 2.0 als IdP
- UCXN als Service Provider
- Microsoft Internet Explorer Version 10

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, offenes Datenformat für den Datenaustausch. Es ist ein Authentifizierungsprotokoll, das von Service Providern zur Authentifizierung eines Benutzers verwendet wird. Die Informationen zur Sicherheitsauthentifizierung werden zwischen einem IdP und dem Service Provider weitergegeben.

SAML ist ein offener Standard, der es Clients ermöglicht, sich gegen jeden SAML-fähigen Collaboration- (oder Unified Communication-) Service zu authentifizieren, unabhängig von der Client-Plattform.

Alle Cisco Unified Communication-Webschnittstellen, wie z. B. Cisco Unified Communications Manager (CUCM) oder UCXN, verwenden das SAML Version 2.0-Protokoll in der SAML SSO-Funktion. Um den LDAP-Benutzer (Lightweight Directory Access Protocol) zu authentifizieren, delegiert UCXN eine Authentifizierungsanforderung an die IDP. Diese vom UCXN generierte Authentifizierungsanfrage ist eine SAML-Anforderung. Die IDP authentifiziert und gibt eine SAML-Assertion zurück. Die SAML-Assertion zeigt entweder Yes (authentifiziert) oder No (Authentifizierung fehlgeschlagen) an.

Mit SAML SSO kann sich ein LDAP-Benutzer mit einem Benutzernamen und einem Kennwort, die sich auf dem IdP authentifizieren, bei Client-Anwendungen anmelden. Wenn Sie die SAML SSO-Funktion aktiviert haben, erhalten Benutzer, die sich bei einer der unterstützten Webanwendungen für Unified Communication-Produkte anmelden, auch Zugriff auf diese Webanwendungen auf UCXN (außer CUCM und CUCM IM und Presence):

Unity Connection-Benutzer	Webanwendungen
-	 UCXN-Administration
	 Cisco UCXN-Benutzerfreundlichkeit
	 Cisco Unified Serviceability
LDAD Demutree wit Administrate we obtain	 Cisco Personal Communications
LDAP-Benutzer mit Administratorrechten	Assistant
	 Web-Posteingang
	 Mini-Web-Posteingang (Desktop-
	Version)
	Cisco Personal Communications

 Cisco Personal Communications Assistant

LDAP-Benutzer ohne Administratorrechte

• Web-Posteingang

- Mini-Web-Posteingang (Desktop-Version)
- Cisco Jabber-Clients

Konfigurieren

Netzwerkdiagramm



Figure :SAML Single sign SSO Call Flow for Collaboration Servers

Verzeichniseinrichtung

- 1. Melden Sie sich bei der UCXN-Administrationsseite an, wählen Sie LDAP aus, und klicken Sie auf LDAP Setup.
- 2. Aktivieren Sie die Option Synchronisierung vom LDAP-Server aktivieren, und klicken Sie auf Speichern.

LDAP System Configurat	ion
Save	
Status	
U Status: Ready	
-LDAP System Informati	on
Enable Synchronizing fr	om LDAP Server
LDAP Server Type	Microsoft Active Directory
LDAP Attribute for User ID	sAMAccountName

3. Klicken Sie auf LDAP.

Save

- 4. Klicken Sie auf LDAP-Verzeichniskonfiguration.
- 5. Klicken Sie auf Neu hinzufügen.
- 6. Konfigurieren Sie diese Elemente:

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

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

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

aliala Cisco Unity Conne	ection Administration	Navigation	Cisco Unity Connection Administration 💌 G
CISCO For Cisco Unified Commu	nications Solutions	ucxnadmin	Search Documentation About Sign Ou
Cisco Unity Connection	LDAP Directory Configuration	Find and List LDAP Directory Configural	tions 🕨 LDAP Directory Configuration (LDAP)
Fax Server	LDAP Directory Configuration Refr	esh Help	
LDAP Setup LDAP Directory Configuration LDAP Authentication Phone Number Conversion	Status Status: Ready		
LDAP Custom Filter SAML Single Sign on Cross-Origin Resource Sharing (C	LDAP Directory Information	LDAP	
SMTP Configuration Advanced	LDAP Manager Distinguished Name*	CN-Administrator, CN-Users, DC-ciscolive, D	0C-com
- Phone System	Confirm Password*		
- Port Group - Port - Speech Connect Port	LDAP User Search Base* LDAP Custom Filter	CN=Users,DC=ciscolive,DC=com < None >	
Trunk Trunk	LDAP Directory Synchronization Perform Sync Just Once	Schedule	
- Task Management - Bulk Administration Tool	Perform a Re-sync Every* Next Re-sync Time (YYYY-MM-DD hh	7 DAY	
- Custom Keypad Mapping - Migration Utilities - Grammar Statistics	Standard User Fields To Be Syn	chronized	
SMTP Address Search Show Dependencies	User ID	sAMAccountName	First Name

8. Klicken Sie auf Vollständige Synchronisierung jetzt durchführen.

DAP Server Information	
Host Name or IP Address for Server [*]	LDAP Port* Use SSL
adfs1.ciscolive.com	3268
Add Another Redundant LDAP Server	
Save Delete Copy Perform Full Sync Now Add New	

Hinweis: Vergewissern Sie sich, dass der **Cisco DirSync-**Dienst auf der Webseite Serviceability aktiviert ist, bevor Sie auf Save (Speichern) klicken.

- 9. Erweitern Sie Benutzer, und wählen Sie Benutzer importieren aus.
- 10. Wählen Sie in der Liste Endbenutzer für Unified Communications Manager suchen die Option LDAP-Verzeichnis aus.
- Wenn Sie nur eine Teilmenge der Benutzer im LDAP-Verzeichnis importieren möchten, mit dem Sie UCXN integriert haben, geben Sie die entsprechenden Spezifikationen in die Suchfelder ein.
- 12. Wählen Sie Suchen aus.
- 13. Wählen Sie in der Liste Basierend auf Vorlage die **Administratorvorlage** aus, die UCXN bei der Erstellung der ausgewählten Benutzer verwenden soll.

Vorsicht: Wenn Sie eine Administratorvorlage angeben, verfügen die Benutzer nicht über

Mailboxen.

14. Aktivieren Sie die Kontrollkästchen für die LDAP-Benutzer, für die Sie UCXN-Benutzer erstellen möchten, und klicken Sie auf **Import Selected (Ausgewählt importieren)**.

alada Cisco Unity Conr	nection Admin	istration		Navigation Cisco Unity Con	nection Administration 💌 Go
CISCO For Cisco Unified Comm	unications Solutions		ucxna	dmin Search Document	ation About Sign Out
 Cisco Unity Connection 	Import Users				Import Users
Users Users Import Users Synch Users Class of Service	Status	fresh Help ? User(s)			
Class of Service Class of Service Membership Templates Call Handler Templates	Find End Users In Where Alias	LDAP Directory • • Begins With •	Eind		
Contact Templates Notification Templates Contacts Distribution Lists	Import With Based on Templat	e administratortemplate 💌			
System Distribution Lists Call Management System Call Handlers	Import Select	Timport All 25 •	Rows Per Page	Phone Number	Extension
Directory Handlers Interview Handlers Custom Recordings ⊞-Call Routing	Import Select	Saml ted Import All	SSO		
Message Storage Mailbox Stores Mailbox Stores Membership Hailbox Quotas Ressage Anion	- <u></u>				

SAML SSO aktivieren

- 1. Melden Sie sich bei der UCXN Administration-Benutzeroberfläche an.
- 2. Wählen Sie **System > SAML Single Sign-on**, und das Fenster SAML SSO Configuration (SSO-Konfiguration für SAML) wird geöffnet.

alada Cisco Unity Conn	ection Administra	tion		Navig	ation Cisco Unity Co	nnection Administration 🗾 Go
CISCO For Cisco Unified Commu	nications Solutions			ucxnadmin	Search Docume	ntation About Sign Out
 Cisco Unity Connection 	SAML Single Sign on					SAML Single Sign on
Plugins	SAML Single Sign on Ref	resh Help				
	🔗 Enable SAML SSO (Update IdP Metad	ata File 🔐 Export All	Netadata 🧳	Fix All Disabled Servers	
LDAP Directory Configuration LDAP Authentication Phone Number Conversion LDAP Custom Filter	Status SAML SSO disabled					
Cross-Origin Resource Sharing (C	SAML Single Sign-On	(1 - 1 of 1)				Rows per Page 50 +
SMTP Configuration Advanced	Server SSO Name Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
Telephony Integrations Phone System Port Group Port Group	UCXN1 Disabled	N/A	Never	🏦 File	Never	Never Run SSO Test
- Speech Connect Port - Trunk B - Security	•- indicates required	item.	Meladata			
Tools Task Management Bulk Administration Tool Curtom Keyned Magning						
H-Migration Utilities Grammar Statistics						
Show Dependencies						

- 3. Um die SAML-SSO für den Cluster zu aktivieren, klicken Sie auf SAML-SSO aktivieren.
- 4. Klicken Sie im Fenster Warnung zurücksetzen auf Weiter.

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

5. Klicken Sie auf dem SSO-Bildschirm auf **Durchsuchen**, um die XML-Datei **FederationMetadata.xml** Metadata mit dem Schritt **Idp Metadata herunterladen** zu importieren.

ahah Cisco Unity Conn	ection Administration	vigation Cisco Unity Connection Administration 💌 Go
CISCO For Cisco Unified Commu	nications Solutions ucxnade	nin Search Documentation About Sign Out
Cisco Unity Connection	SAML Single Sign on Configuration	SAML Single Sign on Configuration
- Fax Server	SAML Single Sign on Configuration Refresh Help	
LDAP	Next .	
LDAP Directory Configuration LDAP Authentication Phone Number Conversion LDAP Custom Filter	Status Ready to import Identity Provider metadata trust file to cluster serve	78
SAML Single Sign on Cross-Origin Resource Sharing (C B-SMTP Configuration B-Advanced	Import the IdP Metadata Trust File This step uploads the file acquired from the IdP in the previous manual ste 3)Select the IdP Metadata Trust File	p to the Collaboration servers.
Telephony Integrations Phone System Port Group	C:\Users\Administrator\Desktop\FederationMetadata.xml	Browse
Port	2)Import this file to the Collaboration servers	
Speech Connect Port	This action must be successful for at least the Publisher before moving on	to the next task in this wizard.
Trunk	Import IdP Metadata	
III Security	Navet Cancel	
Task Management	Tiext Cancer	
Bulk Administration Tool		
Custom Keypad Mapping		
Migration Utilities		
Grammar Statistics		
SMTP Address Search		
- Show Dependencies		
Done	Trush	ed sites Protected Mode: Off

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

cisco Unity Conr	ection Administration	Navigatio	Cisco Unity Connection	Administration 💌 G
For Cisco Unified Comm	unications Solutions	ucxnadmin	Search Documentation	About Sign Ou
Cisco Unity Connection	SAML Single Sign on Configuration		SAML Single :	Sign on Configuration
Plugins	SAML Single Sign on Configuration Refresh He	dp		
LDAP Setup	I Next			
LDAP Directory Configuration LDAP Authentication Phone Number Conversion LDAP Custom Filter	Status Import succeeded for all servers			
SAML Single Sign onCross-Origin Resource Sharing (CSMTP Configuration	This step uploads the file acquired from the IdP in 1)Select the IdP Metadata Trust File	the previous manual step to th	e Collaboration servers.	
Telephony Integrations			Browse	
Port Group	-			
Port	2)Import this file to the Collaboration servers			
Speech Connect Port	This action must be successful for at least the Public	isher before moving on to the	next task in this wizard.	
Trunk			0	
B-Security	Import IdP Metadata		all se	rvers
E Tools				
Task Management	Next Cancel			
Bulk Administration Tool				
R-Maration Utilities				
Grammar Statistics				
SMTP Address Search				
Show Dependencies				
())))))))))))))))))))))))))))))))))))				
one		Trusted sites	Protected Mode: Off	

7. Klicken Sie auf Trust Metadata Fileset herunterladen (nur wenn Sie ADFS noch nicht mit UCXN Metadata konfiguriert haben), um die UCXN-Metadaten in einem lokalen Ordner zu speichern, und gehen Sie zum <u>Hinzufügen von UCXN als Relay Party Trust</u>. Wenn die AD FS-Konfiguration abgeschlossen ist, fahren Sie mit Schritt 8 fort.



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

Cisco Processon About Sign Out • Cisco Unity Connection • Biox • Cisco Unity Connection • Different connection • Different connection • Different connection • Cisco Unity Connection • Cisco Unity Connection • Cisco Unity Connection • Situs • Cisco Unity Connection • Situs • Cisco Unity Configuration • Cisco Configuration • Different configurati	alada Cisco Unity Conn	ection Administration Navigation Cisco Unity Connection Administration	Go
✓ Cisco Unity Connection Pligins Fax Server LDAP LDAP Setup LDAP Directory Configuration DAP Authentication DAP Context Pitter SMID Signal Sign on Cross-Origin Resource Sharing (C SMTP Configuration Phone System Phone System Phont Group Port Group Port Group Port Security Trask Management Build Administration Tool Custom Keypa Mapping Migration Utilities Grammar Statistics Muscond State page Run SSD Test Back Claunch SSO test page Run SSD Test Claunch SSO test page Run SSD Test	CISCO For Cisco Unified Commu	nications Solutions ucxnadmin Search Documentation About Sign	Out
Program Fax Server CLDAP LDAP Directory Configuration LDAP Authentication Phone Number Conversion LDAP Controm Filter SAML Singla Sign on Cross-Ongin Resource Sharing (C SMTP Configuration B Advanced IT talephony Integrations Phone System Port Spech Connect Port Trunk B Security IT tools Custom Keypad Mapping B Migration Utilities B Migration Utilities B Migration Utilities	Cisco Unity Connection	Beck	ł
Tools Task Management Bulk Administration Tool Custom Keypad Mapping Migration Utilities Grammar Statistics Run SSO Test	PluginsFax ServerLDAPLDAP SetupLDAP Directory ConfigurationDAP AuthenticationDAP AuthenticationDAP Custom FilterSAML Single Sign onCross-Origin Resource Sharing (CSMTP Configuration BAdvanced Telephony IntegrationsPone SystemPort GroupPortSpeech Connect PortTrunkSecurity	Status Image: Status The server metadata file must be installed on the IdP before this test is run. Test SSO Setup This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test can be run on any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is successful. 1)Pick a valid username to use for this test You must already know the password for the selected username. This user must have administrator rights and also exist in the IdP. Image: Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator Usernames You did administrator Usernames	
SMTP Address Search	Tools Tools -Task Management -Bulk Administration Tool -Custom Keypad Mapping B-Migration Utilities -Grammar Statistics SMTP Address Search -Show Dependencies	2)Launch SSO test page Run SSO Test Back Cancel	

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

	1
Windows Security	usted certifi
Connecting to ADFS1.ciscolive.com.	ent website'
	ercept any c
sso	
	to this we
Domain: CISCOLIVE	e to this we
Remember my credentials	
OK Cancel	
	•

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

10. Nachdem alle Schritte abgeschlossen sind, erhalten Sie den "SSO-Test erfolgreich durchgeführt". Nachricht. Klicken Sie auf **Schließen** und **Beenden**, um fortzufahren.

https://ucxn1.ciscolive.com/?ssopage=true - Test SAML - Windows Internet Explorer	_ I ×
SSO Test Succeeded!	*
Congratulations on a successful SAML SSO configuration tes Please close this window.	st.
Close	
Done	100% -

Sie haben nun die Konfigurationsaufgaben erfolgreich abgeschlossen, um SSO auf UCXN mit AD FS zu aktivieren.

Obligatorische Anmerkung: Führen Sie den SSO-Test für UCXN-Teilnehmer aus, wenn es

sich um ein Cluster zur Aktivierung von SAML SSO handelt. AD FS muss für alle UCXN-Knoten in einem Cluster konfiguriert werden.

Tipp: Wenn Sie die XML-Metadaten aller Knoten auf IDs konfigurieren und die SSO-Operation auf einem Knoten aktivieren, wird die SAML SSO auf allen Knoten im Cluster automatisch aktiviert.

Sie können CUCM und CUCM IM and Presence für SAML SSO auch konfigurieren, wenn Sie SAML SSO für Cisco Jabber-Clients verwenden und Endbenutzern eine echte SSO-Erfahrung bieten möchten.

Überprüfen

Öffnen Sie einen Webbrowser, und geben Sie den FQDN von UCXN ein. Unter Installierte Anwendungen sehen Sie eine neue Option namens **Recovery URL, um Single Sign-on (SSO)** zu **umgehen**. Wenn Sie auf den Link **Cisco Unity Connection** klicken, werden Sie vom AD FS zur Eingabe der Anmeldeinformationen aufgefordert. Nachdem Sie die Anmeldeinformationen des Benutzer-SSO eingegeben haben, werden Sie erfolgreich bei der Seite Unity Administration (Unity-Administration), Unified Serviceability (Unified Serviceability), angemeldet.



Hinweis: SAML SSO ermöglicht keinen Zugriff auf folgende Seiten:

- Prime Licensing Manager
- Betriebssystemverwaltung
- Disaster Recovery System

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

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