Esempio di configurazione di Unity Connection versione 10.5 SAML SSO

Sommario

Introduzione Prerequisiti Requisiti Installazione di Network Time Protocol (NTP) Installazione di DNS (Domain Name Server) Componenti usati Premesse Configurazione Esempio di rete Impostazione directory Abilita SAML SSO Verifica Risoluzione dei problemi

Introduzione

In questo documento viene descritto come configurare e verificare il protocollo SAML (Security Assertion Markup Language) Single Sign-on (SSO) per Cisco Unity Connection (UCXN).

Prerequisiti

Requisiti

Installazione di Network Time Protocol (NTP)

Affinché SAML SSO funzioni correttamente, è necessario installare l'installazione NTP corretta e assicurarsi che la differenza di tempo tra il provider di identità (IdP) e le applicazioni Unified Communications non superi i tre secondi. Per informazioni sulla sincronizzazione degli orologi, vedere la sezione relativa alle impostazioni NTP nel <u>manuale Cisco Unified Communications</u> <u>Operating System Administration Guide</u>.

Installazione di DNS (Domain Name Server)

Le applicazioni Unified Communications possono utilizzare il DNS per risolvere i nomi di dominio completi (FQDN) in indirizzi IP. I provider di servizi e l'IdP devono essere risolvibili dal browser.

Per gestire le richieste SAML, è necessario installare e configurare Active Directory Federation Service (ADFS) versione 2.0.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- AD FS versione 2.0 come IdP
- UCXN come provider di servizi
- Microsoft Internet Explorer versione 10

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

SAML è un formato di dati standard aperto basato su XML per lo scambio di dati. È un protocollo di autenticazione utilizzato dai provider di servizi per autenticare un utente. Le informazioni di autenticazione di protezione vengono passate tra un IdP e il provider di servizi.

SAML è uno standard aperto che consente ai client di eseguire l'autenticazione in base a qualsiasi servizio di collaborazione abilitato per SAML (o Unified Communications) indipendentemente dalla piattaforma client.

Tutte le interfacce Web di Cisco Unified Communications, quali Cisco Unified Communications Manager (CUCM) o UCXN, utilizzano il protocollo SAML versione 2.0 nella funzione SAML SSO. Per autenticare l'utente LDAP (Lightweight Directory Access Protocol), UCXN delega una richiesta di autenticazione all'IdP. Questa richiesta di autenticazione generata da UCXN è una richiesta SAML. IdP autentica e restituisce un'asserzione SAML. L'asserzione SAML visualizza Sì (autenticato) o No (autenticazione non riuscita).

SAML SSO consente a un utente LDAP di accedere alle applicazioni client con un nome utente e una password che vengono autenticati nel provider di identità. L'utente che accede a una delle applicazioni Web supportate nei prodotti Unified Communications, dopo aver abilitato la funzione SAML SSO, ottiene anche l'accesso a queste applicazioni Web in UCXN (a parte CUCM e CUCM IM e Presence):

Utenti Unity Connection

Applicazioni Web

- Amministrazione UCXN
- Manutenzione di Cisco UCXN
- Manutenzione unificata di Cisco
- Cisco Personal Communications Assistant
- Posta in arrivo Web
- Posta in arrivo Web minima (versione desktop)
- Cisco Personal Communications Assistant
- Posta in arrivo Web
- Posta in arrivo Web minima (versione desktop)
 - Client Cisco Jabber

Utenti LDAP senza diritti di amministratore

Utenti LDAP con diritti di amministratore

Configurazione

Esempio di rete



Figure :SAML Single sign SSO Call Flow for Collaboration Servers

Impostazione directory

- 1. Accedere alla pagina Amministrazione UCXN e selezionare LDAP, quindi fare clic su Configurazione LDAP.
- 2. Selezionare Abilita sincronizzazione dal server LDAP e fare clic su Salva.

LDAP System Configurat	tion
Save	
_	
Status	
(i) Status: Ready	
0	
	ion
Enable Synchronizing fr	om LDAP Server
LDAP Server Type	Microsoft Active Directory
LDAP Attribute for User ID	sAMAccountName

Save

- 3. Fare clic su LDAP.
- 4. Fare clic su Configurazione directory LDAP.
- 5. Fare clic su Aggiungi nuovo.
- 6. Configurare gli elementi seguenti:

Impostazioni account directory LDAPAttributi utente da sincronizzarePianificazione sincronizzazioneNome host o indirizzo IP del server LDAP e numero di porta

7. Selezionare **Usa SSL** se si desidera utilizzare SSL (Secure Sockets Layer) per comunicare con la directory LDAP.

Suggerimento: Se si configura LDAP su SSL, caricare il certificato della directory LDAP in CUCM. Fare riferimento al contenuto della directory LDAP in <u>Cisco Unified Communications</u> <u>Manager SRND</u> per informazioni sul meccanismo di sincronizzazione degli account per prodotti LDAP specifici e per le best practice generali per la sincronizzazione LDAP.

Cisco Unity Connection LDAP Directory Configuration Find and List LDAP Directory Configuration (LDAP) Hugins Fax Server + LDAP LDAP Directory Configuration Refresh + LDAP Setup LDAP Directory Configuration Refresh + LDAP Setup LDAP Configuration Save - LDAP Authentication Phone Number Conversion Status: Ready - LDAP Configuration DAP Directory Information DAP - Cross-Origin Resource Sharing (C) B Advanced IDAP Directory Information B Advanced - DAP Directory Synchronization Name* IDAP - Phone System - Port Group - DAP Custom Filter - Confirm Pessword* - Trunk Security Confirm Pessword* - Consolite Perform Synchronization Schedule Perform Sync Just Once - Perform Sync Just Once - Perform Sync Just Once - Perform Sync Just Once - Trunk - Standard User Fields To Be Synchronization CloaP Hencey Curry* - DAY * - Standard User Fields To Be Synchronization CloaP Attribute Cisco Unified Communications Manager User Fields CloaP Attribute - Standard User Fields To Be Synchronization CloaP Attribute Cisco Unified Communications Manager Us	Cisco Unity Conne Cisco For Cisco Unified Commun	ction Administration	Navigat ucxnadmin	ion Cisco Unity Connection Administration 💌 G
- LDAP Setup - LDAP Directory Configuration - LDAP Authentication - Mone Number Conversion - LDAP Custom Filter - Satus - SAML Single Sign on - Cross-Origin Resource Sharing (C - Cross-Origin Resource Sharing (C - Status B Advanced - LDAP Directory Information - Port Group - DAP Custom Filter - Port Group - Port Group - Port Group - DAP Directory Synchronization Schedule - Trask Management Bulk Administration Tool - Custom Keypad Mapping - Migration Ublities - Grammer Statistics - Standard User Fields To Be Synchronizations Manager User Fields LDAP Attribute - Standard User Fields To Be Synchronizations Manager User Fields LDAP Attribute Cisco Unified Communications Manager User Fields LDAP Attribute	Cisco Unity Connection Plugins Fax Server Ft.DAP	LDAP Directory Configuration LDAP Directory Configuration Refr	Find and List LDAP Directory Configuesh Help	rations > LDAP Directory Configuration (LDAP)
LDAP Custom Filter SAML Single Sign on Cross-Origin Resource Sharing (C SMTP Configuration DAP Configuration Name* LDAP LDAP Configuration Name* LDAP LDAP Manager Distinguished Name* (N=Administrator,CN=Users,DC=ciscolive,DC=com LDAP Manager Distinguished Name* Confirm Password* LDAP Password* Confirm Password* LDAP User Search Base* Confirm Password* LDAP Custom Filter Confirm Password* LDAP User Search Base* Confirm Password* LDAP Custom Filter Confirm Password* LDAP Directory Synchronization Schedule Perform Sync Just Once Perform a Re-sync Every* Tools Grammar Statistics Grammar Statistics SMTP Address Search SMTP Add	- LDAP Setup LDAP Directory Configuration LDAP Authentication Phone Number Conversion	Status Status: Ready		
B: Advanced LDAP Password* □ Telephony Integrations Confirm Password* □ Phone System DAP User Search Base* CN=Users,DC=ciscolive,DC=com □ Port DAP Custom Filter < None > □ Speech Connect Port IDAP Directory Synchronization Schedule □ Trunk DAP Directory Synchronization Schedule □ Tools □ □ Task Management □ □ Bulk Administration Tool □ □ Custom Keypad Mapping Perform a Re-sync Every* 7 ◎ Migration Utilities Standard User Fields To Be Synchronized □ Standard User Fields To Be Synchronized Cisco Unified Communications Manager □ Sup Particular Communications Manager SAMAccountName	LDAP Custom Filter SAML Single Sign on - Cross-Origin Resource Sharing (C 	LDAP Directory Information LDAP Configuration Name* LDAP Manager Distinguished Name*	LDAP CN-Administrator, CN-Users, DC-ciscolive	s,DC=com
-Port -Speech Connect Port -Trunk -Tr	Phone System Port Group	LDAP Password* Confirm Password* LDAP User Search Base*	CN=Users,DC=ciscolive,DC=com	
Tools T	- Port - Speech Connect Port - Trunk B- Security	LDAP Custom Filter	< None >	
Migration Utilities Grammar Statistics SMTP Address Search User TD SAMAccountName First Name	Tools Tools Task Management Bulk Administration Tool Custom Keypad Mapping	Perform a Re-sync Every* Next Re-sync Time (YYYY-MN-DD hi	7 DAY	3
	Higration Utilities Grammar Statistics SMTP Address Search Shaw Descentering	Standard User Fields To Be Syn Cisco Unified Communications Manag User ID	chronized er User Fields LDAP Attribute sAMAccountName	Cisco Unified Communications Manager U First Name

8. Fare clic su Esegui sincronizzazione completa.

R	
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	

Nota: Prima di fare clic su Salva, verificare che il servizio **Cisco DirSync** sia abilitato nella pagina Web Serviceability.

- 9. Espandere Utenti e selezionare Importa utenti.
- 10. Nell'elenco Trova utenti finali di Unified Communications Manager selezionare LDAP Directory.
- 11. Se si desidera importare solo un sottoinsieme degli utenti nella directory LDAP con cui è stato integrato UCXN, immettere le specifiche applicabili nei campi di ricerca.
- 12. Selezionare Trova.
- 13. Nell'elenco In base a modello selezionare il **modello dell'amministratore** che si desidera utilizzare per la creazione degli utenti selezionati in UCXN.

Attenzione: Se si specifica un modello per l'amministratore, gli utenti non disporranno di cassette postali.

14. Selezionare le caselle di controllo relative agli utenti LDAP per i quali si desidera creare utenti UCXN e fare clic su **Importa selezionati**.

alialia Cisco Unity Connection Administration			ration		Navigation Cisco Unity Cor	nnection Administration 💌 Go
CISCO For Cisco Unified Com	munication	s Solutions		ucxn	admin 📕 Search Documen	tation About Sign Out
 Cisco Unity Connection 	Impor	Users				Import Users
Users Users Import Users Synch Users Class of Service	▲ Impor	t Users Refresh	(s)			
-Class of Service		_				
Class of Service Membership TemplatesUser TemplatesCall Handler TemplatesContact Templates BNotification Templates ContactsContact	Find Find When	e Alias In LDA e Alias In CDA ort With d on Template ad	AP Directory 💌 Begins With 💌	Eind	1	
Distribution Lists	Dire	tory Search Res	sults			
System Distribution Lists Call Management System Call Handlers		mport Selected	Import All 25 •	Rows Per Page	Phone Number	Extension
Directory Handlers		550	Sami	550		
Custom Recordings II-Call Routing		mport Selected	Import All			
H Message Storage Mailbox Stores Mailbox Stores Membership H-Mailbox Quotas	×					

Abilita SAML SSO

- 1. Accedere all'interfaccia utente di amministrazione UCXN.
- 2. Scegliere **Sistema > SAML Single Sign-on** e viene visualizzata la finestra Configurazione SAML SSO.

co Unity Conne	ection Adn	ninistration	1		Naviga	tion Cisco Unity Con	nection Administration 💌
isco Unified Commun	inications Soluti	ions			ucxnadmin	Search Document	ation About Sign C
nnection	SAML Single S	Sign on					SAML Single Sign o
1	SAML Single Si	gn on Refresh	Help				
ip I	🎸 Enable SAM	IL SSO 👩 Updat	le IdP Metadata	File 🚯 Export All	Metadata 🥜 F	ix All Disabled Servers	
ctory Configuration metrication mber Conversion tom Filter	Status SAML SSC	D disabled					
Resource Sharing (C	SAML Single	e Sign-On (1 ·	- 1 of 1)				Rows per Page 50 -
uration	Server	SSO Re Status Me	-Import etadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
rations n	UCXN1 0	Disabled	N/A	Never	🎂 File	Never	Never Run 550 Test
ect Port	Enable SA	ML SSO	Export All M	letadata			
	(i) *- indice	tes required item.					
ment tration Tool ed Mapping tiss stistics s Search Jencies	_						
ties Histics s Search Jencies	-						

- 3. Per abilitare l'SSO SAML nel cluster, fare clic su Abilita SSO SAML.
- 4. Nella finestra Reimposta avviso fare clic su Continua.

🖉 https://ucxn1.ciscolive.com/?windowtitlekey=genericdialogwindow.windowtitle.ssoenablewindowtitl 💶 🗖	×
	4
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 🛛 🔰 👘 Trusted sites Protected Mode: Off 🛛 🖓 👻 🔍 100% 🔹	• //

5. Nella schermata SSO fare clic su **Sfoglia** per importare il file XML dei metadati **FederationMetadata.xml** con il passaggio **Download metadati IP**.

alada Cisco Unity Conn	ection Administration	Navigation Cisco Unity Connection Administration 💌 Go
CISCO For Cisco Unified Commu	nications Solutions	ucxnadmin Search Documentation About Sign Out
Cisco Unity Connection	SAML Single Sign on Configuration	SAML Single Sign on Configuration
- Fax Server E-LDAP	SAML Single Sign on Configuration Refresh Help	
LDAP Setup LDAP Directory Configuration LDAP Authentication Phone Number Conversion LDAP Custom Filter	Status Ready to import Identity Provider metadata trust file to	cluster servers
SAML Single Sign on Cross-Origin Resource Sharing (C SMTP Configuration Advanced	Import the IdP Metadata Trust File This step uploads the file acquired from the IdP in the previ 1)Select the IdP Metadata Trust file	ous manual step to the Collaboration servers.
Telephony Integrations Phone System Port Group	C:\Users\Administrator\Desktop\FederationMetadata.xml	Browse
Port Speech Connect Port	2)Import this file to the Collaboration servers This action must be successful for at least the Publisher before	are moving on to the next task in this wizard.
E Security	Import IdP Metadata	
Task Management Task Management Bulk Administration Tool Custom Keypad Mapping Migration Utilities Operation Utilities	MEXT LANCE	
-Grammar Statistics -SMTP Address Search -Show Dependencies		
Done		Trusted sites Protected Mode: Off

6. Una volta caricato il file di metadati, fare clic su **Import IdP Metadata** per importare le informazioni IdP in UCXN. Confermare che l'importazione è stata completata e fare clic su **Avanti** per continuare.

alialia Cisco Unity Con	nection Administration	Navigatio	Cisco Unity Connection	Administration 💌 Go
For Cisco Unified Comm	unications Solutions	ucxnadmin	Search Documentation	About Sign Out
 Cisco Unity Connection 	SAML Single Sign on Configuration		SAML Single :	Sign on Configuration
Plugins	SAML Single Sign on Configuration Refresh H	elp		
-LDAP -LDAP Setup	Next			
LDAP Directory Configuration LDAP Authentication Phone Number Conversion LDAP Custom Filter	Status Import succeeded for all servers			
SAML Single Sign on Cross-Origin Resource Sharing (C SMTP Configuration Advanced	Import the IdP Metadata Trust File This step uploads the file acquired from the IdP ir 1)Select the IdP Metadata Trust File	the previous manual step to the	e Collaboration servers.	
Telephony Integrations Phone System	[Browse	
Port Group	2)Import this file to the Collaboration servers			
Speech Connect Port	This action must be successful for at least the Put	lisher before moving on to the r	next task in this wizard.	
Trunk			A .	
⊞-Security	Import IdP Metadata		all se	rvers
E Tools				
Bulk Administration Tool	Next Cancel			
Custom Keypad Mapping				
Migration Utilities				
Grammar Statistics				
SMTP Address Search				
Show Dependencies	-			
<u>• </u>				
Done		🛛 🐘 🗸 Trusted sites	Protected Mode: Off	🖓 🔹 🔍 100% 🔹

7. Fare clic su Scarica set di file di metadati di attendibilità (eseguire questa operazione solo se ADFS non è già stato configurato con i metadati UCXN) per salvare i metadati UCXN in una cartella locale e passare a <u>Aggiungi UCXN come attendibilità parte di inoltro</u>. Al termine della configurazione di AD FS, andare al passaggio 8.



8. Selezionare SSO come utente amministrativo e fare clic su Esegui test SSO.

alada Cisco Unity Conn	ection Administration Navigation Cisco Unity Connection Administration 💽 G
CISCO For Cisco Unified Commu	nications Solutions ucxnadmin Search Documentation About Sign Out
Cisco Unity Connection	Ver Beck
- Plugins - Fax Server - LDAP - LDAP Setup - LDAP Directory Configuration - LDAP Authentication - LDAP Custom Filter - SAML Single Sign on - Cross-Origin Resource Sharing (C - SMTP Configuration B Advanced Telephony Integrations - Phone System - Port Group - Port - Speech Connect Port - Trunk B Security - Port - - Por	Status Image: Status The server metadata file must be installed on the 1dP 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 1dP. Image: Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator Usernames Yalid administrator Usernames
Tools Tools Task Management Bulk Administration Tool Custom Keypad Mapping Migration Utilities Grammar Statistics SMTP Address Search Show Dependencies	2)Leunch SSO test page Run SSO Test Back Cancel

9. Ignora avvisi certificato e continua. Quando vengono richieste le credenziali, immettere il nome utente e la password di SSO utente e fare clic su **OK**.

Windows Security	usted certifi
Connecting to ADFS1.ciscolive.com.	ent website'
	ercept any o
SSO	
	e to this we
Remember my credentials	
OK Cancel	
▲	Þ

Nota: Questo esempio di configurazione è basato sui certificati autofirmati UCXN e AD FS. Se si utilizzano certificati dell'Autorità di certificazione (CA), è necessario installare i certificati appropriati sia in ADFS che in UCXN. Per ulteriori informazioni, fare riferimento a <u>Gestione e convalida certificati</u>.

10. Al termine di tutti i passaggi, si riceve il messaggio "Test SSO riuscito!" messaggio. Per continuare, fare clic su **Close** (Chiudi) e **Finish** (Fine).

https://ucxn1.ciscolive.com/?ssopage=true - Test SAML - Windows Internet Explorer	
SSO Test Succeeded!	Ă
Congratulations on a successful SAML SSO configuration test. Please close this window.	
Close	
Done	

Le attività di configurazione per l'abilitazione dell'SSO su UCXN con AD FS sono state completate.

Nota obbligatoria: Eseguire il test SSO per il sottoscrittore UCXN se si tratta di un cluster

per abilitare l'SSO SAML. AD FS deve essere configurato per tutti i nodi di UCXN in un cluster.

Suggerimento: Se si configurano i file XML dei metadati di tutti i nodi in IdP e si avvia l'abilitazione dell'operazione SSO su un nodo, l'SSO SAML verrà automaticamente abilitato su tutti i nodi del cluster.

È inoltre possibile configurare CUCM e CUCM IM e Presence per SAML SSO se si desidera utilizzare SAML SSO per i client Cisco Jabber e offrire agli utenti finali un'esperienza di SSO reale.

Verifica

Aprire un browser Web e immettere il nome di dominio completo (FQDN) di UCXN. In Applicazioni installate verrà visualizzata una nuova opzione denominata **URL di ripristino per ignorare Single Sign-On (SSO)**. Dopo aver fatto clic sul collegamento **Cisco Unity Connection**, all'utente vengono richieste le credenziali da ADFS. Dopo aver immesso le credenziali dell'utente SSO, verrà eseguito correttamente l'accesso alla pagina Unity Administration, Unified Serviceability.

// https://ucxn1.ciscolive.com/ - Windows Internet Explorer					-	8 ×
😋 😔 💌 https://ucxn1.dscolive.com/	💌 😵 Certificate Error	🐓 🗙 🔎 Bing				۰۹
😭 Favorites 🛛 🙀 🔊 Suggested Sites 🔹 🖉 Web Sice Gallery 🔹						
🙁 🔹 💽 Certificate Error: Navigation 🥻 https://ucxn1.ciscolive.c 🗙		💁 • 🗟 🕤	🗅 🖶 🔹 Page -	Safety +	Tools +	0٠
cisco						4
Installed Applications				-		
 Cisco Unity Connection Recovery URL to bypass Single Sign On (SSO) Cisco Prime License Manager Cisco Unified Serviceability 						
Platform Applications						
 Disaster Recovery System Cisco Unified Communications OS Administration 						

Nota: SAML SSO non consente l'accesso a queste pagine:

- Prime Licensing Manager
- Amministrazione del sistema operativo
- Sistema di disaster recovery

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Per ulteriori informazioni, fare riferimento a <u>Risoluzione dei problemi di SSO SAML per i prodotti</u> <u>Collaboration 10.x</u>.