Esempio di configurazione di Unified Communications Manager 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 Unified Communications Manager (CUCM).

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.

In caso di mancata corrispondenza tra CUCM e IdP, viene visualizzato il seguente messaggio di errore: "Risposta SAML non valida." Questo errore potrebbe essere causato da un tempo di sincronizzazione non corretto tra i server CUCM e IdP. Affinché SAML SSO funzioni, è necessario installare la corretta configurazione NTP e assicurarsi che la differenza di tempo tra l'IdP e le applicazioni Unified Communications non superi i tre secondi.

Per informazioni su come sincronizzare gli orologi, vedere la sezione relativa alle impostazioni NTP nel <u>manuale Cisco Unified Communications 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.

Componenti usati

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

- Active Directory Federation Service (ADFS) versione 2.0 come IdP
- CUCM versione 10.5 come provider di servizi
- Microsoft Internet Explorer 10

Attenzione: Questo documento si basa su un CUCM appena installato. Se si configura SAML SSO su un server già in produzione, potrebbe essere necessario ignorare alcuni passaggi. È inoltre necessario comprendere l'impatto del servizio se si eseguono le operazioni sul server di produzione. Si consiglia di eseguire questa procedura al di fuori dell'orario di lavoro.

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 basato su XML e basato su standard aperti che consente agli amministratori di accedere senza problemi a un insieme definito di applicazioni di collaborazione Cisco dopo aver eseguito l'accesso a una di tali applicazioni. L'SSO SAML stabilisce un Circle of Trust (CoT) quando scambia metadati come parte del processo di provisioning tra l'IdP e il provider di servizi. Il provider di servizi considera attendibili le informazioni utente dell'IdP per consentire l'accesso ai vari servizi o applicazioni.

Nota: I provider di servizi non sono più coinvolti nell'autenticazione. SAML versione 2.0 delega l'autenticazione ai provider di servizi e agli IdP. Il client esegue l'autenticazione in base all'IdP e l'IdP concede un'asserzione al client. Il client presenta l'asserzione al provider di servizi. Poiché è stato stabilito un CoT, il provider di servizi considera attendibile l'asserzione e concede l'accesso al client.

Configurazione

Esempio di rete



Figure :SAML Single sign SSO Call Flow for Collaboration Servers

Impostazione directory

1. Scegliere Cisco Unified CM Administration > System > LDAP > LDAP System.



- 2. Fare clic su Aggiungi nuovo.
- 3. Configurare il tipo e l'attributo del server Lightweight Directory Access Protocol (LDAP).
- 4. Scegliere Abilita sincronizzazione dal server LDAP.

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

- 5. Scegliere Cisco Unified CM Administration > System > LDAP > LDAP Directory.
- 6. Configurare gli elementi seguenti:

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

LDAP Directory	
🕞 Save 🗶 Delete 🛅 Copy 👔	Perform Full Sync Now 🕂 Add New
- Status	
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. Deselezionare **Usa SSL** se non si desidera utilizzare SSL (Secure Sockets Layer) per comunicare con la directory LDAP.

Suggerimento: Se si desidera configurare LDAP su SSL, caricare il certificato della directory LDAP in CUCM. Per informazioni sul meccanismo di sincronizzazione degli account per prodotti LDAP specifici e sulle best practice generali per la sincronizzazione LDAP, vedere il

contenuto della directory LDAP in Cisco Unified Communications Manager SRND.

8. Fare clic su **Save** (Salva), quindi su **Perform Full Sync Now (Esegui sincronizzazione completa)**.

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

Host Name or IP Address for Server	LDAP Port* Use SSL
adfs1.ciscolive.com	3268
Add Another Redundant LDAP Server	

9. Passare a **Gestione utente > Utente finale** e selezionare un utente al quale si desidera assegnare il ruolo amministrativo CUCM (in questo esempio viene selezionato **SSO** utente).

System +	Call Routing 👻 Medi	a Resources 👻 🗛	tvanced Features 👻	Device 👻	Application +	User Management 👻	Bulk Administration 👻	Help 👻
Find and	List Users							
🕂 Add	New Eselect All	🖽 Clear All 🙀	Delete Selected					
Status 3 re	ecords found							
User	(1 - 3 of 3)							Rows p
User Find Use	(1 - 3 of 3) r where First name		begins with 💽			Find Clear Filter		Rows p
User Find Use	(1 - 3 of 3) r where First name User ID *	First Name	begins with 💽		Department	Find Clear Filter	URI	Rows p User Status
User Find Use	(1 - 3 of 3) r where First name User ID ^ SSQ	First Name Saml	Last Name SSO		Department	Find Clear Filter Directory	URI Active LDA	<i>Rows p</i> User Status NP Synchronized User

10. Scorrere fino a visualizzare le informazioni sulle autorizzazioni e fare clic su Aggiungi a gruppo di controllo di accesso. Selezionare Utenti privilegiati CCM standard, fare clic su Aggiungi selezionati, quindi fare clic su Salva.

oups St	andard CCM Super Users		
			Add to Access Control Group
			Remove from Access Control Group
		View Details	
les St	andard AXL API Access		
St	andard Admin Rep Tool Admin	-	
St	andard CCM Admin Users	_	
50	andard CURADMIN Administration	View Details	
1.00	andara conceporting	VIEW Decalls	

Abilita SAML SSO

1. Accedere all'interfaccia utente di amministrazione CUCM.

2. Scegliere **Sistema > SAML Single Sign-On** e viene visualizzata la finestra Configurazione SAML Single Sign-On.



3. Per abilitare l'SSO SAML nel cluster, fare clic su Abilita SSO SAML.

SAML Single Sign-C	n								
Enable SAML SSO	Export All M	etadata 🔞 Update IdP I	Aetadata File 🥜 Fix All D	isabled Servers					
-Status	Status								
SAML SSO disab	led								
SAML Single Sign-	SAMI Single Sign On (1 - 2 of 2)								
Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test			
CUCM	Disabled	N/A	Never	📥 File	March 30, 2011 7:57:56 PM CEST	Never Run SSO Test			

4. Nella finestra Reimposta avviso fare clic su Continua.

🔏 https://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	• //.

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

System 👻	Call Routing 👻	Media Resources 👻	Advanced Features 👻	Device 👻	Application +	User Management 👻	Bulk Administration 👻	Help 🕶
SAML Sin	gle Sign-On	Configuration						
Next								
-Status-								
() Statu	is: Ready							
- Downloa To configu manually	d Identity pr ure the trust re obtain the file	rovider(IdP) Metae lationship between t from the IdP before	data Trust File he IdP and your devic you can upload it to y	es, you must our Collabora	t first obtain t ation servers.	rust metadata from y	your IdP and import it	to your servers. You will need to
🔥 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. Una volta caricato il file di metadati, fare clic su **Import IdP Metadata** per importare le informazioni IdP in CUCM. Confermare che l'importazione è stata completata e fare clic su **Avanti** per continuare.

System 👻 Call Routing 👻 Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻 User Management 👻 Bulk Administration 👻 Help 👻
SAML Single Sign-On Configuration
Next
- Status
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
C:\Users\Administrator\Desktop\FederationMetadata.xml Browse
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
SAML Single Sign-On Configuration
Next
Status
V Import succeeded for all servers
- Tonand the TdD Netadata Toust Sile
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
2)Import this file to the Collaboration servers

Status	
✓ Import succeeded for all servers	
- Import the IdP Metadata Trust File	
This step uploads the file acquired from the IdP in the previous m	anual step to the Collaboration servers.
1)Select the IdP Metadata Trust File	
E.	Browse
2)Import this file to the Collaboration servers	
This action must be successful for at least the Publisher before me	oving on to the next task in this wizard.
Import IdP Hetadata	V Import succeeded for all servers
Next Cancel	

7. Fare clic su Scarica file metadati di trust (facoltativo) per salvare il CUCM e i metadati CUCM IM e Presenza in una cartella locale e passare a Aggiungi CUCM come attendibilità componente. Al termine della configurazione di AD FS, andare al passaggio 8.

SAML Single Sign-On Configuration
de Back 📫 Next
Status 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 Conver Matadata and install on the IdD
Download Server rectaulta and instant on the fur 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. Selezionare SSO come utente amministrativo e fare clic su Esegui test SSO.

System +	Call Routing 👻	Media Resources 👻	Advanced Features -	Device 👻 /	Application +	User Management 👻	Bulk Administration +	Help 🛨	
SAML SI	gle Sign-On	Configuration							
de Back									
-Status-									^*
The The	server metada	ta file must be insta	alled on the IdP before	this test is ru	n.				
- Test SS	0 Setup								
This test SSO has	verifies that the been enabled.	e metadata files are SSO setup cannot t	e correctly configured a be completed unless th	nd will allow is test is succ	SSO to start essful.	up on the servers. 1	This test can be run or	any server for troubles	shooting once
1)Pick a v	valid username	to use for this test							
You must This user	already know must have adr	the password for th ministrator rights ar	ne selected username. Ind also exist in the IdP.						
🔥 Plea	se use one of	the Usernames sho	wn below. Using any ot	her Usernam	e to log into t	he IdP may result i	n administrator lockou	ıt.	
Valid adm sso	ninistrator User	names							
2)Launch	SSO test page	1							
Run	SSO Test								
Back	Cancel								

9. Ignorare gli avvisi relativi ai certificati e continuare. Quando vengono richieste le credenziali, immettere il nome utente e la password per l'SSO utente e fare clic su OK.

Windows Securi	ty	usted certifi
Connecting to A	DFS1.ciscolive.com.	ent website'
	sso	ercept any c
	Domain: CISCOLIVE	e to this we
	OK Cancel	
•		

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

10. Dopo il completamento di tutti i passaggi, il "Test SSO riuscito!" viene visualizzato un messaggio. Fare clic su Close (Chiudi) e su Finish (Fine) per continuare. Le attività di configurazione necessarie per abilitare l'SSO in CUCM con ADFS sono state completate.



11. Poiché CUCM IM e Presence funzionano come il sottoscrittore CUCM, è necessario configurare <u>Aggiungi CUCM IM e Presenza come attendibilità componente</u> e quindi eseguire **Esegui test SSO** per abilitare l'SSO SAML dalla stessa pagina SAML SSO CUCM.

Nota: Se si configurano i file XML dei metadati di tutti i nodi su IdP e si abilita l'operazione SSO su un nodo, l'SSO SAML viene abilitato su tutti i nodi del cluster.

AD FS deve essere configurato come relaying party per tutti i nodi di CUCM, CUCM IM e Presenza in un cluster.

Suggerimento: È inoltre necessario configurare Cisco Unity Connection, CUCM IM e Presence per SAML SSO se si desidera utilizzare l'esperienza SAML SSO per i client Cisco Jabber.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

- 1. Aprire un browser Web e immettere il nome FQDN per CUCM.
- 2. Fare clic su Cisco Unified Communications Manager.
- Selezionare l'app Web (Amministrazione CM/Servizi unificati/Cisco Unified Reporting) e fare clic su Vai, quindi verranno richieste le credenziali da ADFS. Dopo aver immesso le credenziali di SSO utente, si è connessi correttamente all'app Web selezionata (pagina Amministrazione CM, pagina Manutenzione unificata, Cisco Unified Reporting).

C http://cucm.ciscolive.com/ - Windows Internet Explorer		X
G 🕢 🗢 🖾 http://cucm.ciscolive.com/		. م
👷 Favorites 😫 😰 Suggested Sites - 😰 Web Slice Galery -	🐴 = 🔂 - 🖃 📾 = Page = Sal	fety + Tools - 🔞 +
ahaha		
CISCO		
Installed Applications		
Cisco Unified Communications Manager Decovery LIPL to by asso Single Single	00(550)	
Cisco Unified Communications Self Care Provide Disputs Self Care	lortal	
Cisco Prime Dense Manager Cisco Unified Reporting		
Gisco Unitied Serviceability		
Platform Applications		
Disaster Recovery System Class Unified Communications CO Administ	trafina	
 Cisco Unitied Communications US Adminis 	trauon	
1		

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

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

Risoluzione dei problemi

Se non è possibile abilitare SAML e non è possibile eseguire l'accesso, utilizzare la nuova opzione in Applicazioni installate denominata **URL di ripristino per ignorare Single Sign-On (SSO)**, che può essere utilizzata per accedere con le credenziali create durante l'installazione o con gli utenti amministrativi CUCM creati localmente.

🔏 Cisco Uni	fied CM Console - Windows Internet Explorer			_ # ×
00-	https://cucm.dscolive.com/comadmin/showRecovery.do	💌 😺 Certificate Error	😝 🗙 🔎 Bing	ρ.
👍 Favorites	🙀 🙋 Suggested Sites 🔹 🙋 Web Sike Gallery 🔹			
🏉 Cisco Uni	fied CM Console		💁 • 🔂 • 💷 🖶 • P	lage + Safety + Tools + 📦 +
cisco	Cisco Single Sign On Recovery Administration For Cisco Unified Communications Solutions			<u>^</u>
Cisc This pa running This pa	to Single Sign On Recovery Administration of the second structure of the secon	ion ns that are	Username comadmin Password Login Reset	
Copyright (All rights re This produc products do U.S. and lo product imm	© 1999 - 2015 Cisco Systems, Inc. eserved. It contains cryptographic features and is subject to United States and local count bes not imply third-party authority to import, export, distribute or use encryption cal country laws. By using this product you agree to comply with applicable laws mediately.	try laws governing impo . Importers, exporters, and regulations. If you	rt, export, transfer and use. Deli distributors and users are respo are unable to comply with U.S. a	very of Cisco cryptographic sible for compliance with and local laws, return this

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

For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.

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

Per ulteriori informazioni sulla risoluzione dei problemi, consultare il documento sulla <u>risoluzione</u> dei problemi di SAML SSO per i prodotti Collaboration versione 10.x.