Exemple de configuration d'Unity Connection version 10.5 SAML SSO

Contenu

Introduction Conditions préalables Conditions requises Configuration du protocole NTP (Network Time Protocol) Configuration du serveur de noms de domaine (DNS) Components Used Informations générales Configuration Diagramme du réseau Configuration du répertoire Activer SAML SSO Vérification Dépannage

Introduction

Ce document décrit comment configurer et vérifier l'authentification unique SAML (Security Assertion Markup Language) pour Cisco Unity Connection (UCXN).

Conditions préalables

Conditions requises

Configuration du protocole NTP (Network Time Protocol)

Pour que SAML SSO fonctionne, vous devez installer la configuration NTP correcte et vous assurer que la différence de temps entre le fournisseur d'identité (IdP) et les applications de communications unifiées ne dépasse pas trois secondes. Pour plus d'informations sur la synchronisation des horloges, reportez-vous à la section NTP Settings du <u>Guide d'administration du système d'exploitation Cisco Unified Communications</u>.

Configuration du serveur de noms de domaine (DNS)

Les applications de communications unifiées peuvent utiliser DNS afin de résoudre les noms de domaine complets (FQDN) en adresses IP. Les fournisseurs de services et l'IDP doivent pouvoir être résolus par le navigateur.

Le service de fédération Active Directory (AD FS) version 2.0 doit être installé et configuré pour gérer les requêtes SAML.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- AD FS version 2.0 en tant qu'IDP
- UCXN en tant que fournisseur de services
- Microsoft Internet Explorer version 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

SAML est un format de données basé sur XML et ouvert pour l'échange de données. Il s'agit d'un protocole d'authentification utilisé par les fournisseurs de services pour authentifier un utilisateur. Les informations d'authentification de sécurité sont transmises entre un IDP et le fournisseur de services.

SAML est une norme ouverte qui permet aux clients de s'authentifier contre tout service de collaboration (ou de communication unifiée) compatible SAML, quelle que soit la plate-forme du client.

Toutes les interfaces Web Cisco Unified Communications, telles que Cisco Unified Communications Manager (CUCM) ou UCXN, utilisent le protocole SAML version 2.0 dans la fonctionnalité SSO SAML. Afin d'authentifier l'utilisateur LDAP (Lightweight Directory Access Protocol), UCXN délègue une demande d'authentification à l'IDP. Cette requête d'authentification générée par l'UCXN est une requête SAML. L'IDP authentifie et renvoie une assertion SAML. L'assertion SAML affiche Oui (authentifié) ou Non (échec de l'authentification).

SAML SSO permet à un utilisateur LDAP de se connecter aux applications clientes avec un nom d'utilisateur et un mot de passe qui s'authentifient sur l'IdP. Une fois que vous avez activé la fonctionnalité SAML SSO, une connexion utilisateur à l'une des applications Web prises en charge sur les produits Unified Communication permet également d'accéder à ces applications Web sur UCXN (à l'exception de CUCM et CUCM IM and Presence) :

Utilisateurs Unity Connection

Applications Web

- Administration UCXN
- Facilité de maintenance de Cisco UCXN
- Cisco Unified Servicability
- Cisco Personal Communications
 Assistant
- Boîte de réception Web
- Mini boîte de réception Web (version bureau)
- Cisco Personal Communications
 Assistant
- Boîte de réception Web
- Mini boîte de réception Web (version bureau)

Utilisateurs LDAP avec droits d'administrateur

Utilisateurs LDAP sans droits d'administrateur

Clients Cisco Jabber

Configuration

Diagramme du réseau



Figure :SAML Single sign SSO Call Flow for Collaboration Servers

Configuration du répertoire

- 1. Connectez-vous à la page Administration UCXN et sélectionnez LDAP et cliquez sur Configuration LDAP.
- 2. Cochez Activer la synchronisation à partir du serveur LDAP et cliquez sur Enregistrer.

LDAP System Configurat	ion
Save	
Status	
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. Cliquez sur LDAP.

Save

- 4. Cliquez sur Configuration du répertoire LDAP.
- 5. Cliquez sur Ajouter nouveau.
- 6. Configurez ces éléments :

Paramètres du compte d'annuaire LDAPAttributs utilisateur à synchroniserCalendrier de synchronisationNom d'hôte ou adresse IP du serveur LDAP et numéro de port

7. Cochez **Use SSL** si vous voulez utiliser SSL (Secure Socket Layer) afin de communiquer avec l'annuaire LDAP.

Astuce : Si vous configurez LDAP sur SSL, téléchargez le certificat d'annuaire LDAP sur CUCM. Reportez-vous au contenu de l'annuaire LDAP dans <u>Cisco Unified Communications</u> <u>Manager SRND</u> pour plus d'informations sur le mécanisme de synchronisation des comptes pour des produits LDAP spécifiques et les meilleures pratiques générales pour la synchronisation LDAP.

aliala Cisco Unity Conne	ection Administration	Navigatio	n 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 Configura	ations + LDAP Directory Configuration (LDAP)
Flugins Fax Server DDAP LDAP Setup	LDAP Directory Configuration Refr	esh Help	
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 Configuration Name*	LDAP	
SMTP Configuration Advanced	LDAP Manager Distinguished Name*	CN-Administrator, CN-Users, DC-ciscolive,	DC-com
Telephony Integrations Phone System	Confirm Password*	•••••••••••••••••••••••••••••••••••••	
- Port Group	LDAP User Search Base ⁴ LDAP Custom Filter	CN=Users,DC=ciscolive,DC=com < None >	×
- Trunk - Security	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 .	
Higration Utilities Grammar Statistics	Standard User Fields To Be Syn	chronized	Cisco Unified Communications Macrosov
SMTP Address Search Show Dependencies	User ID	sAMAccountName	First Name

8. Cliquez sur Exécuter la synchronisation complète maintenant.

Ц	
LDAP 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	

Note: Assurez-vous que **Cisco DirSync** est activé dans la page Web de maintenance avant de cliquer sur Enregistrer.

- 9. Développez Utilisateurs et sélectionnez Importer des utilisateurs.
- 10. Dans la liste **Rechercher les utilisateurs finaux de Unified Communications Manager**, sélectionnez **Répertoire LDAP**.
- 11. Si vous souhaitez importer uniquement un sous-ensemble des utilisateurs dans l'annuaire LDAP avec lequel vous avez intégré UCXN, saisissez les spécifications applicables dans les champs de recherche.
- 12. Sélectionnez Rechercher.
- 13. Dans la liste Basé sur le modèle, sélectionnez le **modèle Administrateur** que UCXN doit utiliser lorsqu'il crée les utilisateurs sélectionnés.

Attention : Si vous spécifiez un modèle administrateur, les utilisateurs ne disposeront pas

de boîtes aux lettres.

14. Cochez les cases correspondant aux utilisateurs LDAP pour lesquels vous souhaitez créer des utilisateurs UCXN et cliquez sur **Importer la sélection**.

aluda Cisco Unity Connection Administration			Navigation Cisco Unity Connection Administration 💌 G		
CISCO For Cisco Unified Comm	nunications Solutions		ucxna	dmin 📘 Search Documentat	ion About Sign (
Cisco Unity Connection	Import Users				Import Use
Users Users Import Users Synch Users	Import Users Refree Status Found 1 LDAP Us	sh Help er(s)			
Class of Service	-Find-	- (-)			
Templates User Templates Call Handler Templates Contact Templates B Notification Templates	Find End Users In U	DAP Directory • Begins With •	Eind		
Contacts Contacts	Based on Template	administratortemplate 💌			
Distribution Lists	Directory Search R	esults			
Call Management	Import Selected	Import All 25 💌	Rows Per Page		
Directory Handlers	Alias 🔺	First Name	Last Name	Phone Number	Extension
-Interview Handlers Custom Recordings El-Call Routing	Import Selected	Saml	SSO		
Message Storage Mailbox Stores Mailbox Stores Membership Mailbox Quotas Ressage Aning	ـــــــــــــــــــــــــــــــــــــ				

Activer SAML SSO

.

- 1. Connectez-vous à l'interface utilisateur UCXN Administration.
- 2. Choisissez **System > SAML Single Sign-on** et la fenêtre SAML SSO Configuration s'ouvre.

alude Cisco Unity Connection Administration		ation		Naviga	ation Cisco Unity Conn	co Unity Connection Administration 💌	
CISCO For Cisco Unified Comm	unications Sol	utions			ucxnadmin	Search Documenta	tion About Sign
Cisco Unity Connection	SAML Singl	e Sign on					SAML Single Sign
Plugins -Fax Server C-LDAP -LDAP Setup -LDAP Directory Configuration -LDAP Authentication -Phone Number Conversion -LDAP Custom Filter -SAML Single Sign on	SAML Single	Sign on Ri AML SSO	efresh Help Update IdP Metada	sta File 👔 Export All	i Metadata 🧳	Fix All Disabled Servers	
SMTP Configuration	SAML SI	igle Sign-On	(1 - 1 of 1)			1	Rows per Page 50 💽
E Advanced	Name	SSO	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
Telephony Integrations Phone System Port Group Port Speech Connect Port Trunk B-Security	Enable	Disabled SAML SSO	N/A Export Al	Never	🕁 File	Never	Never Run SSO Test
Tools Tools Task Management Bulk Administration Tool Custom Keypad Mapping G-Migration Utilities Grammar Statistics SMTP Address Search Show Dependencies	<u>.</u>						

- 3. Afin d'activer SAML SSO sur le cluster, cliquez sur Enable SAML SSO.
- 4. Dans la fenêtre Avertissement de réinitialisation, cliquez sur Continuer.

//ucxn1.ciscolive.com/?windowtitlekey=genericdialogwindow.windowtitle.ssoenablewindowtitl	×
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.	
i 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. Dans l'écran SSO, cliquez sur **Parcourir** afin d'importer le fichier XML de métadonnées **FederationMetadata.xml** à l'aide de l'étape **Télécharger les métadonnées Idp**.

alada Cisco Unity Conn	ection Administration Navigation Cisco Unity Connection Administration 💌 😡
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
Plugins	SAML Single Sign on Configuration Refresh Help
B-LDAP	Next .
LDAP Setup	
LDAP Directory Configuration	
LDAP Authentication	Status
Phone Number Conversion LDAP Custom Filter	Ready to import Identity Provider metadata trust file to cluster servers
-SAML Single Sign on	
Cross-Origin Resource Sharing (C	Import the IdP Metadata Trust File
SMTP Configuration	This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.
E Advanced	1)Select the JdP Metadata Trust File
E Telephony Integrations	C:\Users\Administrator\Desktop\FederationMetadata.xml Browse
Phone System	
Port Group	2)Import this file to the Collaboration servers
-Speech Connect Bort	This action must be successful for at least the Publisher before moving on to the next task in this wizard.
Trunk	Impact IdB Metodate
E Security	Import for Hetadata
E Tools	Next Cancel
- Task Management	
Bulk Administration Tool	
-Custom Keypad Mapping	
Migration Utilities	
Grammar Statistics	
- SMTP Address Search	1
Show Dependencies	1
Dane	💦 🗸 🖓 Trusted sites Protected Mode: Off

 Une fois le fichier de métadonnées téléchargé, cliquez sur Import IdP Metadata afin d'importer les informations IdP dans UCXN. Vérifiez que l'importation a réussi et cliquez sur Suivant pour continuer.

Cisco Unity Conr Cisco For Cisco Unified Comm	ection Administration	Navigation Cisco Unity Connection Administration 🗾 Go 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 Help	
Fax Server	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 B-SMTP Configuration B-Advanced	Timport the IdP Metadata Trust File This step uploads the file acquired from the IdP in the p 1)Select the IdP Metadata Trust file	revious manual step to the Collaboration servers.
Telephony Integrations Phone System	L.	Browse
Part Group Part Speech Connect Part	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.
Trunk	Terrard V dia Make data	 Import succeeded for
H-Security	Import IdP Hetadata	W all servers
	Next Cancel	
Migration Utilities Grammar Statistics		
SMTP Address Search		
Show Dependencies	•	
۱ (۱۱۱۲)		
Done		🖬 🗸 Trusted sites Protected Mode: Off

7. Cliquez sur Download Trust Metadata Fileset (effectuez cette opération uniquement si vous n'avez pas configuré ADFS déjà avec des métadonnées UCXN) afin d'enregistrer les métadonnées UCXN dans un dossier local et accédez à <u>Ajouter UCXN comme approbation</u> <u>de partie relais</u>. Une fois la configuration AD FS terminée, passez à l'étape 8.

Cisco Unity Conn Cisco Unified Commu	ection Administration	Navigation Cisco Unity Connection Administration 🚽 Go ucxnadmin Search Documentation About Sign Out
Cisco Unity Connection	SAML Single Sign on Configuration	SAML Single Sign on Configuration
- LDAP - LDAP Setup - LDAP Directory Configuration - LDAP Authentication - LDAP Authentication - LDAP Authentication	SAML Single Sign on Configuration Refresh Help	to IdP then skip the steps below and click Next. Otherwise follow the
- SATP Configuration	✓ steps below to upload the server metadata to JdP ✓ IdP Metadata has been imported to servers in this du ■ Download Server Metadata and install on the IdP.	ister File Download
-Advanced Telephony Integrations -Phone System -Port Group	Download the metadata trust file from Collaboration serv 1)Download the server metadata trust files to local storag Download Trust Metadata File	Do you want to open or save this file?
- Speech Connect Port - Trunk - Trunk - Tools	This is a manual step! 2)Log in to your IdP and upload the server metadata trus 3)Click 'Next' once you have installed the server metadat	Open Save Cancel
-Task Management Bulk Administration Tool Custom Keypad Mapping P-Migration Utilities	Back Next Cancel	While files from the internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. <u>What is the risk?</u>
Grammar Statistics SMTP Address Search Show Dependencies		

8. Sélectionnez SSO comme utilisateur administratif et cliquez sur Exécuter le test SSO.

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	Heck	4
FluginsFax ServerLDAPLDAP SetupLDAP Directory ConfigurationDAP AuthenticationDAP AuthenticationDAP Custom FilterSAML Single Sign onCross-Origin Resource Sharing (CSMTP ConfigurationConfiguration	Status The server metadata file must be installed Test SSO Setup This test verifies that the metadata files are con be run on any server for troubleshooting once S successful. 1)Pick a valid username to use for this test You must already know the password for the se This user must have administrator rights and als M Please use one of the Usernames shown b administrator lockout. Valid administrator Usernames SSO	on the 1dP before this test is run. rectly configured and will allow SSO to start up on the servers. This test can ISO has been enabled. SSO setup cannot be completed unless this test is lected username. so exist in the 1dP. elow. Using any other Username to log into the IdP may result in
Tools Tools Task Management Bulk Administration Tool Custom Keypad Mapping Migration Utilities Grammar Statistics SMTP Address Search Show Dependencies	2)Launch SSO test page Run SSO Test Back Cancel	

 Ignorez les avertissements de certificat et poursuivez. Lorsque vous êtes invité à saisir des informations d'identification, saisissez le nom d'utilisateur et le mot de passe de l'utilisateur SSO, puis cliquez sur OK.

		_
Windows Securit	γ.	usted certifi
Connecting to Al	DFS1.ciscolive.com.	ent website'
	sso	ercept any c
	Domain: CISCOLIVE Remember my credentials	e to this we
	OK Cancel	
•		F

Note: Cet exemple de configuration est basé sur des certificats autosignés UCXN et AD FS. Si vous utilisez des certificats d'autorité de certification, les certificats appropriés doivent être installés sur AD FS et UCXN. Référez-vous à <u>Gestion et validation des certificats</u> pour plus d'informations. 10. Une fois toutes les étapes terminées, vous recevez le « Test SSO réussi ! » message. Cliquez sur **Fermer** et **Terminer** pour continuer.



Vous avez maintenant terminé les tâches de configuration pour activer SSO sur UCXN avec AD FS.

Note obligatoire : Exécutez le test SSO pour UCXN Subscriber s'il s'agit d'un cluster afin d'activer SAML SSO. AD FS doit être configuré pour tous les noeuds d'UCXN dans un cluster.

Astuce : Si vous configurez les fichiers XML de métadonnées de tous les noeuds sur IdP et que vous commencez à activer l'opération SSO sur un noeud, SAML SSO sera activé automatiquement sur tous les noeuds du cluster.

Vous pouvez également configurer CUCM et CUCM IM and Presence pour SAML SSO si vous voulez utiliser SAML SSO pour les clients Cisco Jabber et offrir une véritable expérience SSO aux utilisateurs finaux.

Vérification

Ouvrez un navigateur Web et saisissez le nom de domaine complet d'UCXN. Une nouvelle option apparaît sous Applications installées, appelée **URL de récupération, pour contourner l'authentification unique (SSO)**. Une fois que vous avez cliqué sur le lien **Cisco Unity Connection**, les services AD FS vous demandent des informations d'identification. Une fois que vous avez entré les informations d'identification de l'utilisateur SSO, vous serez connecté correctement à la page Unity Administration, page Unified Serviceability.

Attps://ucon1.ciscolive.com/ - Winds	rws Internet Explorer			_ 8 ×
COO - M https://ucxn1.dscolive.com	m/	💌 🤤 Certificate Error	🔄 🗙 🔎 Bing	. م
🖕 Favorites 🛛 🙀 🙋 Suggested Sites 🔹	🖉 Web Sice Gallery 🔹			
🔠 🔹 💽 Certificate Error: Navigation	Chttps://ucxn1.ciscolive.c X		🏠 • 🔂 - 🖸 🖶 • Page	* Safety * Tools * 😧 *
cisco				×
Installed App	lications			
 Cisco Unity o Reco Cisco Prim Cisco Unifie 	Connection very URL to bypass Single Sign C e License Manager ad Serviceability)n (SSO)		
Platform App	lications			_
Disaster Re Cisco Unifie	ecovery System ed Communications OS Administr	ation		

Note: SAML SSO n'active pas l'accès à ces pages :

- Gestionnaire de licences Prime
- Administration du système d'exploitation
- Système de reprise après sinistre

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Référez-vous à <u>Dépannage SAML SSO pour les produits de collaboration 10.x</u> pour plus d'informations.