# Ejemplo de Configuración de Unity Connection Versión 10.5 SAML SSO

## Contenido

Introducción Prerequisites Requirements Configuración del protocolo de tiempo de red (NTP) Configuración del servidor de nombres de dominio (DNS) Componentes Utilizados Antecedentes Configurar Diagrama de la red Configuración del directorio Habilitar SAML SSO Verificación Troubleshoot

## Introducción

Este documento describe cómo configurar y verificar el lenguaje de marcado de aserción de seguridad (SAML) Single Sign-on (SSO) para Cisco Unity Connection (UCXN).

## Prerequisites

### Requirements

### Configuración del protocolo de tiempo de red (NTP)

Para que SAML SSO funcione, debe instalar la configuración NTP correcta y asegurarse de que la diferencia de tiempo entre las aplicaciones Identity Provider (IdP) y Unified Communications no exceda de tres segundos. Para obtener información sobre cómo sincronizar los relojes, vea la sección Configuración de NTP en la <u>Guía de Administración del Sistema Operativo de Cisco</u> <u>Unified Communications</u>.

### Configuración del servidor de nombres de dominio (DNS)

Las aplicaciones de Unified Communications pueden utilizar DNS para resolver los nombres de dominio completos (FQDN) a las direcciones IP. Los proveedores de servicios y el IdP deben ser resueltos por el navegador.

El servicio de federación de directorios activos (AD FS) versión 2.0 debe estar instalado y configurado para manejar las solicitudes SAML.

### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- AD FS versión 2.0 como IdP
- UCXN como proveedor de servicios
- Microsoft Internet Explorer versión 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.

## Antecedentes

SAML es un formato de datos basado en XML y estándar abierto para el intercambio de datos. Se trata de un protocolo de autenticación utilizado por los proveedores de servicios para autenticar a un usuario. La información de autenticación de seguridad se pasa entre un IdP y el Proveedor de servicios.

SAML es un estándar abierto que permite a los clientes autenticarse con cualquier servicio de colaboración (o Unified Communication) habilitado para SAML, independientemente de la plataforma del cliente.

Todas las interfaces web de Cisco Unified Communication, como Cisco Unified Communications Manager (CUCM) o UCXN, utilizan el protocolo SAML versión 2.0 en la función SAML SSO. Para autenticar al usuario del protocolo ligero de acceso a directorios (LDAP), UCXN delega una solicitud de autenticación en el IdP. Esta solicitud de autenticación generada por UCXN es una solicitud SAML. El IdP autentica y devuelve una afirmación SAML. La afirmación SAML muestra Sí (autenticado) o No (error de autenticación).

SAML SSO permite a un usuario LDAP iniciar sesión en aplicaciones cliente con un nombre de usuario y una contraseña que se autentican en el IdP. El usuario que inicia sesión en cualquiera de las aplicaciones web admitidas en productos de Unified Communication, después de habilitar la función SAML SSO, también obtiene acceso a estas aplicaciones web en UCXN (excepto CUCM y CUCM IM and Presence):

#### Usuarios de Unity Connection

#### Aplicaciones web

- Administración de UCXN
- Capacidad de servicio de Cisco UCXN
- Serviciabilidad de Cisco Unified
- Asistente de comunicaciones personales de Cisco
- Bandeja de entrada web
- Mini bandeja de entrada en la Web (versión de escritorio)
- Asistente de comunicaciones personales de Cisco
- Bandeja de entrada web
- Mini bandeja de entrada en la Web (versión de escritorio)
- Clientes de Cisco Jabber

Usuarios LDAP con derechos de administrador

#### Usuarios LDAP sin derechos de administrador

## Configurar

### Diagrama de la red



Figure :SAML Single sign SSO Call Flow for Collaboration Servers

### Configuración del directorio

Save

- 1. Inicie sesión en la página de administración de UCXN y seleccione LDAP y haga clic en Configuración de LDAP.
- 2. Marque Enable Synchronizing from LDAP Server y haga clic en Save.

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

- 3. Haga clic en LDAP.
- 4. Haga clic en Configuración del directorio LDAP.
- 5. Haga clic en Agregar nuevo.
- 6. Configure estos elementos:

Configuración de la cuenta de directorio LDAPAtributos de usuario que se van a sincronizarProgramación de sincronizaciónNombre de host o dirección IP del servidor LDAP y número de puerto

7. Marque **Use SSL** si desea utilizar Secure Socket Layer (SSL) para comunicarse con el directorio LDAP.

**Consejo:** Si configura LDAP sobre SSL, cargue el certificado de directorio LDAP en CUCM. Refiérase al contenido del directorio LDAP en el <u>SRND de Cisco Unified Communications</u> <u>Manager</u> para obtener información sobre el mecanismo de sincronización de cuentas para productos LDAP específicos y prácticas recomendadas generales para la sincronización LDAP.

Cisco Unity Conn Cisco For Cisco Unified Commu	ection Administration		Navigation Cisc	o Unity Connection Administration 💌 G
<ul> <li>Cisco Unity Connection</li> </ul>	LDAP Directory Configuration	Find and List LDAP	Directory Configurations	LDAP Directory Configuration (LDAP)
Plugins     Fax Server     Construction     CDAP Setup     LDAP Directory Configuration     LDAP Authentication     Phone Number Conversion     -LDAP Coulom Filter     SAML Single Sign on     Cross-Origin Resource Sharing (C     SMTP Configuration     Advanced     Telephony Integrations     Phone System     Port Group     Port     Speech Connect Port     -Trunk	LDAP Directory Configuration Refi Save Status Status: Ready LDAP Directory Information LDAP Configuration Name* LDAP Manager Distinguished Name* LDAP Manager Distinguished Name* LDAP Password* Confirm Password* LDAP User Search Base* LDAP Custom Filter	LDAP CN-Administrator,CN-U CN-Users,DC-ciscolive, < None >	Isers,DC=ciscolive,DC=col DC=com	m
Security     Tools     -Task Management     -Bulk Administration Tool     -Custom Keypad Mapping     Migration Utilities	LDAP Directory Synchronizatio Perform Sync Just Once Perform a Re-sync Every* Next Re-sync Time (YYYY-MM-DD h	n Schedule 7 h:mm)* [2015-01-18 00:00]	DAY .	
-SMTP Address Search	Cisco Unified Communications Mana	ger User Fields LDAP Attri	bute	Cisco Unified Communications Manager U
-Show Dependencies	User ID	sAMAccoun	tName	First Name

8. Haga clic en Realizar sincronización completa ahora.

Host Na	ame or IP Address for Server*	LDAP Port* Use S
adfs1.	.ciscolive.com	3268
Add	Another Redundant LDAP Server	

**Nota:** Asegúrese de que el servicio **Cisco DirSync** esté habilitado en la página web Serviceability antes de hacer clic en Save (Guardar).

- 9. Expanda Users y seleccione Import Users.
- 10. En la lista **Buscar usuarios finales de Unified Communications Manager**, seleccione **Directorio LDAP**.
- 11. Si desea importar sólo un subconjunto de los usuarios en el directorio LDAP con el que ha integrado UCXN, introduzca las especificaciones aplicables en los campos de búsqueda.
- 12. Seleccione Find.
- 13. En la lista Basado en plantilla, seleccione la **plantilla de administrador** que desea utilizar UCXN cuando cree los usuarios seleccionados.

Precaución: Si especifica una plantilla de administrador, los usuarios no tendrán buzones.

14. Active las casillas de verificación de los usuarios LDAP para los que desea crear usuarios UCXN y haga clic en **Importar seleccionados**.

alight Cisco Unity Connection Administration			Navigation Cisco Unity Connection Administration 💽 Go		
CISCO For Cisco Unified Commu	unications Solutions		ucxna	dmin Search Document	ation About Sign Out
<ul> <li>Cisco Unity Connection</li> </ul>	Import Users				Import Users
E Users	Import Users Re	fresh Help			
Synch Users  Class of Service Class of Service Class of Service Membership	Found 1 LDAP	User(s)			
Templates     User Templates     Call Handler Templates     Contact Templates     Dividication Templates	Find End Users In Where Alias	LDAP Directory      Begins With	Eind		
Contacts	Based on Templat	e administratortemplate 💌			
Distribution Lists	Directory Searc	h Results			
Call Management	Import Select	ed Import All 25 .	Rows Per Page		
-Directory Handlers	Alias 🖌	First Name	Last Name	Phone Number	Extension
Interview Handlers Custom Recordings	M sso	Saml	SSO		
Con Roomy     Message Storage     Mailbox Stores     Mailbox Stores Membership     B-Mailbox Quotas     R Message Anion     ■	-				

### Habilitar SAML SSO

- 1. Inicie sesión en la interfaz de usuario de Administración de UCXN.
- 2. Elija System > SAML Single Sign-on y se abrirá la ventana SAML SSO Configuration.

alada Cisco Unity Conne	ection Administrat	tion		Naviga	tion Cisco Unity Conne	ction Administration 🗾 Go
CISCO For Cisco Unified Commu	nications Solutions			ucxnadmin	Search Documentat	ion About Sign Out
<ul> <li>Cisco Unity Connection</li> </ul>	SAML Single Sign on					SAML Single Sign on
Plugins	SAML Single Sign on Ref	resh Help				
G-LDAP LDAP Setup	🎸 Enable SAML SSO ( 👌	Update IdP Metada	ita File 🔒 Export All	Netadata 🥜 f	ix 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)			R	ows per Page 50 -
SMTP Configuration     E-Advanced	Server SSO Name Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
Telephony Integrations     Phone System     Date System	UCXN1 Disabled	N/A	Never	🎂 File	Never	Never Run SSO Test
-Port Group -Port -Speech Connect Port	Enable SAML SSO	Export Al	l Metadata			
Trunk B-Security	(i) *- indicates required	item.				
E Tools						
Custom Keypad Mapping						
B-Migration Utilities						
-Grammar Statistics						
SMTP Address Search						
Show Dependencies						
× •						

- 3. Para habilitar SAML SSO en el clúster, haga clic en Habilitar SAML SSO.
- 4. En la ventana Restablecer advertencia, haga clic en Continuar.

https://ucxn1.ciscolive.com/?windowtitlekey=genericdialogwindow.windowtitle.ssoenablewindowtitl	
	<u> </u>
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.	3
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.	ð
Continue Cancel	
Done	<u>▼</u> % <b>▼</b> //:

5. En la pantalla SSO, haga clic en **Examinar** para importar el archivo XML de metadatos **FederationMetadata.xml** con el paso **Descargar metadatos Idp**.

uludu Cisco Unity Conn	ection Administration	Navigation Cisco Unity Connection	Administration 💌 Go
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
Plugina	SAML Single Sign on Configuration Refresh Help		
Fax Server	4		
H-LDAP	Next .		
LDAP Setup			-
LDAP Directory Configuration			
LDAP Authentication	Status	_	
Phone Number Conversion	Ready to import Identity Provider metadata trust file to c	luster servers	
LDAP Custom Filter	L		
SAML Single Sign on	- Import the IdP Metadata Tourt File		
Cross-Origin Resource Sharing (C	This step uploads the file acquired from the IdP in the previou	s manual step to the Collaboration servers.	
B-Advanced	1)Select the IdP Metadata Trust File		
Auvanceu     Telesbergy Integrations			
Bhone Surtem	C:\Users\Administrator\Desktop\FederationMetadata.xml	Browse	
Port Group			
Port	2)Import this file to the Collaboration servers		
-Speech Connect Port	This action must be successful for at least the Publisher before	a moving on to the next task in this wizard.	
Trunk	Impact IdP Metadata	-	
E Security	Import for Hetadata		
E Tools	Next Cancel		
Task Management			
-Bulk Administration Tool			
-Custom Keypad Mapping			
Migration Utilities			
Grammar Statistics			
-SMTP Address Search			
-Show Dependencies			
4			
lane		🚴 📝 Trusted sites   Protected Mode: Off	

6. Una vez cargado el archivo de metadatos, haga clic en **Importar metadatos IdP** para importar la información de IdP a UCXN. Confirme que la importación se ha realizado correctamente y haga clic en **Siguiente** para continuar.

Cisco Unity Con For Cisco Unified Com	nection Administration	Navigation Cisco Unity Connection Administration
Cisco Unity Connection	SAML Single Sign on Configuration	SAML Single Sign on Configuration
Plugins	SAML Single Sign on Configuration Refresh He	
Fax Server		*
	Next 💭	
LDAP Setup		
LDAP Directory Configuration		
-LDAP Authentication	Status	
Phone Number Conversion	Import succeeded for all servers	
CAMI Single Sign on		
-Cross-Origin Resource Sharing (C	Import the IdP Metadata Trust File	
H-SMTP Configuration	This step uploads the file acquired from the IdP in t	the previous manual step to the Collaboration servers.
B:Advaged	1)Select the IdP Metadata Trust File	
E Telephony Integrations		
Phone System		Browse
Port Group		
Port	2)Import this file to the Collaboration servers	
Speech Connect Port	This action must be successful for at least the Publ	isher before moving on to the next task in this wizard.
Trunk		
B-Security	Import IdP Metadata	Import succeeded for
E Tools		all servers
Task Management	In the second se	
Bulk Administration Tool	Next Cancel	
Custom Keypad Mapping		
B-Migration Utilities		
Grammar Statistics		
SMTP Address Search		
Show Dependencies	×	
۰ ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (		
Done		💦 🗸 Trusted sites   Protected Mode: Off 🛛 🍕 🔹 💐 100% 🔹

7. Haga clic en Descargar conjunto de archivos de metadatos de confianza (sólo si no ha configurado el ADFS ya con metadatos UCXN) para guardar los metadatos UCXN en una carpeta local y vaya a <u>Agregar UCXN como confianza de parte reactiva</u>. Una vez completada la configuración de AD FS, continúe con el paso 8.

Cisco Unity Conn	ection Administration	Navigation Cisco Unity Connection Administration 💽 Go
For Cisco Unified Commu	nications Solutions	ucxnadmin Search Documentation About Sign Out
<ul> <li>Cisco Unity Connection</li> </ul>	SAML Single Sign on Configuration	SAML Single Sign on Configuration
Cisco Unity Connection     Plugins     Fax Server     C-LDAP     LDAP Setup     LDAP Directory Configuration     LDAP Authentication     LDAP Custom Filter     SAML Single Sign on     Cross-Origin Resource Sharing (C     SMTP Configuration     Advanced     Telephony Integrations     Phone System     Port Group     Part     Speech Connect Port     Trunk     B - Security     Tools	SAML Single Sign on Configuration Refresh Help Back Next Status Tf Admin has already uploaded the server metadata steps below to upload the server metadata to IdP V IdP Metadata has been imported to servers in this di Download Server Metadata and install on the IdP- Download the metadata trust file from Collaboration server	to IdP then skip the steps below and click Next. Otherwise follow the uster File Download Do you want to open or save this file?
	1)Download the server metadata trust files to local storag Download Trust Metadata File  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 metadata	Name: SPMetadata.zp Type: Compressed (zpped) Folder, 1.57KB From: ucxn1.ciscolive.com Open Save Cancel
Task Management     Bulk Administration Tool     Custom Keypad Mapping     Migration Utilities     Grammar Statistics     SMTP Address Search     Show Dependencies	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. What is the risk?

8. Seleccione SSO como usuario administrativo y haga clic en Ejecutar prueba SSO.

Cisco Unified Communications Solutions       uccnade         ▼ Cisco Unity Connection       ■ Beck         ■ Fax Server       ■ CDAP         ■ LDAP Setup       ■ DAP Directory Configuration         ■ LDAP Authentication       ■ Phone Number Conversion         ■ DAP Custom Filter       ■ Satus         ■ SAML Single Sign on       ■ Cross-Origin Resource Sharing (Cisto System         ■ Advanced       ■ Telephony Integrations         ■ Phone System       ■ Phone System         ■ Port       ■ Speech Connect Port         ■ Speech Connect Port       ■ Trunk	
	Search Documentation About Sign
-Plugins         -Fax Server         -LDAP         -LDAP Directory Configuration         -LDAP Authentication         -Phone Number Conversion         LDAP Custom Filter         -SAML Single Sign on         -Cross-Origin Resource Sharing (C         SAMP Configuration         B Advanced         Telephony Integrations         -Phone System         -Port Group         -Port         -Speech Connect Port         -Trunk	
Security	run. w SSO to start up on the servers. This test can ietup cannot be completed unless this test is me to log into the IdP may result in
Tools Task Management Bulk Administration Tool Custom Keypad Mapping Migration Utilities Grammar Statistics SMTP Address Search Sharp Decendencies	

9. Ignore las advertencias del certificado y continúe. Cuando se le pida las credenciales, ingrese el nombre de usuario y la contraseña del SSO del usuario y haga clic en **Aceptar**.

		•
Windows Securi	ty	usted certifi
Connecting to A	DFS1.ciscolive.com.	ent website'
1		ercept any c
	SSO	
	••••••	e to this we
	Domain: CISCOLIVE	
(		
	OK Cance	4
		•

**Nota:** Este ejemplo de configuración se basa en certificados autofirmados UCXN y AD FS. En caso de que utilice certificados de autoridad certificadora (CA), deben instalarse los certificados adecuados tanto en AD FS como en UCXN. Refiérase a <u>Administración y</u> <u>Validación de Certificados</u> para obtener más información.

10. Después de completar todos los pasos, recibirá la "Prueba de SSO satisfactoria". mensaje. Haga clic en **Cerrar** y **Finalizar** para continuar.

https://ucxn1.ciscolive.com/?ssopage=true - Test SAML - Windows Internet Explorer	<u> </u>
SSO Test Succeeded!	4
Congratulations on a successful SAML SSO configuration test. Please close this window.	
Close	
Done	▼ % ▼ //.

Ya ha completado correctamente las tareas de configuración para habilitar SSO en UCXN con AD FS.

**Nota obligatoria**: Ejecute la prueba SSO para el suscriptor UCXN si es un clúster para habilitar SAML SSO. AD FS se debe configurar para todos los nodos de UCXN en un clúster.

**Consejo:** Si configura los archivos XML de metadatos de todos los nodos en IdP y comienza a habilitar la operación SSO en un nodo, SAML SSO se activará automáticamente en todos los nodos del clúster.

También puede configurar CUCM y CUCM IM and Presence para SAML SSO si desea utilizar SAML SSO para clientes Cisco Jabber y ofrecer una verdadera experiencia de SSO a los usuarios finales.

## Verificación

Abra un navegador web e introduzca el FQDN de UCXN y verá una nueva opción en Aplicaciones instaladas llamada **URL de recuperación para omitir el inicio de sesión único (SSO)**. Una vez que haga clic en el enlace **Cisco Unity Connection**, el AD FS le solicitará las credenciales. Después de ingresar las credenciales del usuario SSO, se conectará correctamente a la página Unity Administration (Administración de Unity), página Unified Serviceability (Serviciabilidad unificada).

C https://ucon1.ciscolive.com/ - Windows Internet Explorer		_ 8 ×
🚱 😔 🖷 https://ucxn1.ciscolive.com/	😵 Certificate Error  😽 🗡 Bing	ρ.
😭 Favorites 🛛 🎭 🔊 Suggested Sites 🔹 🖉 Web Sice Gallery 🔹		
🙁 🔹 🖸 Certificate Error: Navigation Ehttps://ucxn1.ciscolive.c 🗙	🤷 🛪 🔂 🛪 🖂 👼 🛪 Page x Safe	iety + Tools + 😧 +
cisco		Î
Installed Applications		
<ul> <li>Cisco Unity Connection <ul> <li>Recovery URL to bypass Single Sign On (SSO)</li> <li>Cisco Prime License Manager</li> <li>Cisco Unified Serviceability</li> </ul> </li> </ul>		
Platform Applications		
<ul> <li>Disaster Recovery System</li> <li>Cisco Unified Communications OS Administration</li> </ul>		-

Nota: SAML SSO no permite el acceso a estas páginas:

- Prime Licensing Manager
- Administración del SO
- Sistema de recuperación ante desastres

## Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Refiérase a <u>Troubleshooting de SAML SSO para Productos de Colaboración 10.x</u> para obtener más información.