# Unity Connection版本10.5 SAML SSO配置示例

### 目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>網路時間協定(NTP)設定</u> <u>域名伺服器(DNS)安裝程式</u> <u>域名伺服器(DNS)安裝程式</u> <u>採用元件</u> <u>背景資訊</u> <u>設定</u> <u>網路圖表</u> <u>目錄設定</u> <u>啟用SAML SSO</u> <u>驗證</u> 疑難排解

# 簡介

本文說明如何為Cisco Unity Connection(UCXN)配置和驗證安全斷言標籤語言(SAML)單一登入 (SSO)。

## 必要條件

### 需求

#### 網路時間協定(NTP)設定

要使SAML SSO正常工作,必須安裝正確的NTP設定,並確保身份提供程式(IdP)和統一通訊應用程 式之間的時間差不超過三秒。有關同步時鐘的資訊,請參閱<u>Cisco Unified Communications作業系</u> <u>統管理指南</u>中的NTP設定部分。

#### 域名伺服器(DNS)安裝程式

統一通訊應用程式可以使用DNS將完全限定域名(FQDN)解析為IP地址。服務提供商和IdP必須由瀏 覽器解析。

必須安裝和配置Active Directory聯合身份驗證服務(AD FS)版本2.0才能處理SAML請求。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

• AD FS版本2.0作為IdP

• 作為服務提供商的UCXN

• Microsoft Internet Explorer版本10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

# 背景資訊

SAML是一種基於XML的開放式標準資料格式,用於資料交換。這是服務提供商用於驗證使用者身份的身份驗證協定。安全身份驗證資訊在IdP和服務提供商之間傳遞。

SAML是一種開放標準,它使客戶端能夠根據任何支援SAML的合作(或統一通訊)服務進行身份驗 證,而不管客戶端平台如何。

所有Cisco Unified Communication Web介面(如Cisco Unified Communications Manager(CUCM)或 UCXN)都使用SAML SSO功能中的SAML 2.0版協定。為了對輕量級目錄訪問協定(LDAP)使用者進 行身份驗證,UCXN將身份驗證請求委託給IdP。由UCXN生成的身份驗證請求是SAML請求。IdP驗 證並返回SAML斷言。SAML Assertion顯示Yes(authenticated)或No(authentication failed)。

SAML SSO允許LDAP使用者使用在IdP上進行身份驗證的使用者名稱和密碼登入客戶端應用程式。 啟用SAML SSO功能後,使用者登入統一通訊產品上任何受支援的Web應用,還可以訪問UCXN上 的這些Web應用(除CUCM和CUCM IM和線上狀態外):

Unity Connection使用者

#### Web應用程式

- UCXN管理
- Cisco UCXN可維護性
- Cisco Unified Serviceability

• 思科個人通訊助理

- Web收件箱
- •迷你Web收件箱(案頭版
  - 本)
- 思科個人通訊助理
- •Web收件箱

無管理員許可權的LDAP使用者

具有管理員許可權的LDAP使用者

- •迷你Web收件箱(案頭版 本)
- Cisco Jabber使用者端

設定

網路圖表



Figure :SAML Single sign SSO Call Flow for Collaboration Servers

### 目錄設定

- 1. 登入到UCXN管理頁面,然後選擇LDAP,然後按一下LDAP設定。
- 2. 選中Enable Synchronizing from LDAP Server,然後按一下Save。

LDAP System Configuration				
Save				
-Status				
G Status: Ready				
LDAP System Informati	on			
Enable Synchronizing from LDAP Server				
LDAP Server Type	Microsoft Active Directory			
LDAP Attribute for User ID	sAMAccountName			

Save

- 3. 按一下LDAP。
- 4. 按一下LDAP Directory Configuration。
- 5. 按一下「Add New」。

6. 配置以下專案:

LDAP目錄帳戶設定要同步的使用者屬性同步計畫LDAP伺服器主機名或IP地址和埠號

7. 如果要使用安全套接字層(SSL)與LDAP目錄通訊,請選中Use SSL。

**提示:**如果通過SSL配置LDAP,請將LDAP目錄證書上傳到CUCM。有關特定LDAP產品的帳 戶同步機制和LDAP同步的一般最佳實踐的資訊,請參閱<u>Cisco Unified Communications</u> <u>Manager SRND</u>中的LDAP目錄內容。

Cisco Unity Conne Cisco For Cisco Unified Commu	ection Administration	Navigation ucxnadmin	Cisco Unity Connection Administration 💌 🧕
Cisco Unity Connection For Cisco Unified Commun Cisco For Cisco Unified Commun Cisco Unified Commun Cisco Unity Connection Flugins Fax Server Flugins Fax Server Flugins Flug	LDAP Directory Configuration LDAP Directory Configuration EDAP Directory Configuration Ref Save Status Status: Ready LDAP Directory Information LDAP Configuration Name* LDAP Configuration Name* LDAP Manager Distinguished Name LDAP Password* Confirm Password* LDAP User Search Base* LDAP Custom Filter	LDAP  LDAP  CN-Administrator,CN-Users,DC-ciscolive,D  CN-Users,DC=ciscolive,DC=com  None >  Schedule	Search Documentation About Sign Ou tions > LDAP Directory Configuration (LDAP) DC-com 
Statisty     Tools     -Task Management     -Bulk Administration Tool     -Custom Keypad Mapping     B-Migration Utilities     -Grammar Statistics     -SMTP Address Search	Perform Sync Just Once Perform a Re-sync Every <sup>*</sup> Next Re-sync Time (YYYY-MM-DD h —Standard User Fields To Be Sy Cisco Unified Communications Mana	7 DAY 12015-01-18 00:00 nchronized ger User Fields LDAP Attribute	Cisco Unified Communications Manager U
-Show Dependencies -	User ID	sAMAccountName	First Name

8. 按一下Perform Full Sync Now。

Ц	
LDAP Server Information	
Host Name or IP Address for Server <sup>*</sup>	LDAP Port* Use SSL
adfs1.ciscolive.com	3268
Add Another Redundant LDAP Server	
Save Delete Copy Perform Full Sync Now Add New	

附註:按一下「儲存」之前,請確保在「可服務性」網頁中啟用了Cisco DirSync服務。

- 9. 展開Users並選擇Import Users。
- 10. 在Find Unified Communications Manager End Users清單中,選擇LDAP Directory。
- 11. 如果您希望僅匯入已整合UCXN的LDAP目錄中的使用者子集,請在搜尋欄位中輸入適用的規 範。

12. 選擇查詢。

13. 在「基於模板」清單中,選擇希望UCXN在建立所選使用者時使用的管理員模板。

**注意**:如果指定管理員模板,使用者將沒有郵箱。

14. 選中要為其建立UCXN使用者的LDAP使用者的覈取方塊,然後按一下Import Selected。

alula Cisco Unity Connection Administration		Navigation Cisco Unity Connection Administration 💌 Go		
CISCO For Cisco Unified Communications Solutions		ucxnadmin Search Documentation About Sign Out		
Cisco Unity Connection	Import Users	Import Users		
Users Users Import Users	Import Users Refresh Help Status			
Class of Service     Class of Service     Class of Service     Class of Service	Found 1 LDAP User(s)  Find			
Templates User Templates Call Handler Templates Contact Templates	Find End Users In LDAP Directory  Where Alias Begins With	Eind		
Contacts     Contacts	Import With Based on Template administratortemplate -			
Distribution Lists	Directory Search Results			
Call Management System Call Handlers	Import Selected Import All 25 Rows Per	r Page		
- Directory Handlers Interview Handlers - Custom Recordings				
El Roung → Mailbox Stores → Mailbox Stores Membership El - Mailbox Quotas RI - Messane Anion				

### 啟用SAML SSO

- 1. 登入到UCXN管理使用者介面。
- 2. 選擇System > SAML Single Sign-on,此時將開啟SAML SSO Configuration視窗。

alialia Cisco Unity Conn	ection Adr	ninistra	tion		Navig	ation Cisco Unity Co	onnection Administration 🚽 Go
CISCO For Cisco Unified Commu	inications Solut	tions			ucxnadmin	Search Docume	ntation About Sign Out
<ul> <li>Cisco Unity Connection</li> </ul>	SAML Single	Sign on					SAML Single Sign on
Plugins	SAML Single S	lign on Re	fresh Help				
C-LDAP	🧹 Enable SAJ	VL \$\$0 ()	Update IdP Metada	sta File 🚯 Export Al	Netadata 🧳	Fix All Disabled Servers	
LDAP Directory Configuration LDAP Authentication Phone Number Conversion LDAP Custom Filter SAM Single Sign ad	Status SAML SS	O disabled					
Cross-Origin Resource Sharing (C	SAML Sing	le Sign-On	(1 - 1 of 1)				Rows per Page 50 +
SMTP Configuration     Advanced	Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
Telephony Integrations     Phone System     Port Group	UCXN1	Disabled	N/A	Never	🎂 File	Never	Never Run SSO Test
Port Speech Connect Port Trunk B-Security	Enable S	AML SSO	Export Al	l Metadata			
Tools     Task Management     Bulk Administration Tool     Custom Keypad Mapping     Grammar Statistics     SMTP Address Search     Show Dependencies							

- 3. 要在群集中啟用SAML SSO,請按一下Enable SAML SSO。
- 4. 在「重置警告」視窗中,按一下繼續。

https://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.	
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. 在SSO螢幕上,按一下Browse,以使用Download Idp Metadata步驟匯入 FederationMetadata.xml後設資料XML檔案。

ahah Cisco Unity Con	nection Administration	Navigation Cisco Unity Connection Administration 🗾 Go
CISCO 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
Hugins Fax Server	SAML Single Sign on Configuration Refresh Help	
LDAP Setup	Next Next	
LDAP Directory Configuration LDAP Authentication Phone Number Conversion LDAP Custom Filter	Status Ready to import Identity Provider metadata trust f	ile to cluster servers
SAML Single Sign on     Cross-Origin Resource Sharing (C     SMTP Configuration     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     Part Course	C:\Users\Administrator\Desktop\FederationMetadata.x	mi Browse
-Port	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.
Speech Connect Port	Import IdP Metadata	before merring on to are next case in and meaner
Tools     Tools     Tools     Bulk Administration Tool     Custom Keypad Mapping     Migration Utilities     Grammar Statistics     SNTP Address Search     Show Dependencies	Next Cancel	
<li>International International Internation</li>		Trusted sites   Protected Mode: Off

6. 上載後設資料檔案後,按一下Import IdP Metadata以將IdP資訊匯入UCXN。確認匯入成功 ,然後按一下**下一步**繼續。

ahah. Cisco Unity Con	nection Administration	Navigation Cisco Unity Connection Administration 🗾 Go
CISCO For Cisco Unified Com	munications Solutions	ucxnadmin Search Documentation About Sign Out
<ul> <li>Cisco Unity Connection</li> </ul>	SAML Single Sign on Configuration	SAML Single Sign on Configuration
Fax Server	SAML Single Sign on Configuration Refresh Help	
E-LDAP	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	Import the IdP Metadata Trust File This step uploads the file acquired from the IdP in the 1)Select the IdP Metadata Trust file	previous manual step to the 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 Publishe	r before moving on to the next task in this wizard.
Trunk		<b>0</b>
B-Security	Import IdP Metadata	all servers
Task Management Bulk Administration Tool	Next Cancel	
Custom Keypad Mapping		
Grammar Statistics		
SMTP Address Search		
Show Dependencies	<b>I</b>	
×		
Done		🐘 🗸 Trusted sites   Protected Mode: Off 🛛 🍕 🔹 🔍 100% 🔹

7. 按一下Download Trust Metadata Fileset(僅當尚未使用UCXN Metadata配置ADFS時才執行 此操作)以將UCXN後設資料儲存到本地資料夾,並轉至Add UCXN as Relaying Party Trust。完成AD FS配置後,請繼續執行步驟8。



8. 選擇SSO作為管理使用者,然後按一下運行SSO測試。

alada Cisco Unity Conn	ection Administration	Navigation Cisco Unity Connection Administration 💌 🤇
CISCO For Cisco Unified Commu	nications Solutions	ucxnadmin Search Documentation About Sign O
Cisco Unity Connection	Heck	
Plugins -fax Server -LDAP -LDAP Setup -LDAP Directory Configuration -DAP Authentication -DAP 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	Status The server metadata file must be installed Test SSO Setup This test verifies that the metadata files are cor be run on any server for troubleshooting once 3 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 al M Please use one of the Usernames shown to administrator lockout. Valid administrator Usernames 30	I on the IdP before this test is run. rrectly configured and will allow SSO to start up on the servers. This test can SSO has been enabled. SSO setup cannot be completed unless this test is elected username. Iso exist in the IdP. below. 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	

忽略證書警告並繼續操作。當系統提示您輸入憑據時,輸入使用者SSO的使用者名稱和密碼,然後按一下OK。

		-
Windows Security	<b>y</b>	usted certifi
Connecting to AD	PFS1.ciscolive.com.	ent website'
		ercept any c
	SSO	
		e to this we
	Remember my credentials	
	OK Cancel	
•		Þ

**附註**:此配置示例基於UCXN和AD FS自簽名證書。如果使用證書頒發機構(CA)證書,必須在 AD FS和UCXN上安裝適當的證書。如需詳細資訊,請參閱<u>憑證管理和驗證</u>。

10. 完成所有步驟後,您將收到「SSO測試成功!」 消息。按一下「Close」和「Finish」以繼續。

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

現在,您已成功完成配置任務,以便在UCXN上啟用SSO(使用AD FS)。

**必需附註**:如果UCXN訂戶是集群,請運行SSO測試以啟用SAML SSO。必須為群集中 UCXN的所有節點配置AD FS。

提示:如果在IdP上配置所有節點的後設資料XML檔案,並且開始在一個節點上啟用SSO操作

,則將自動在群集中的所有節點上啟用SAML SSO。

如果您希望對Cisco Jabber客戶端使用SAML SSO,並為終端使用者提供真正的SSO體驗 ,您還可以為SAML SSO配置CUCM和CUCM IM和線上狀態。

### 驗證

開啟Web瀏覽器並輸入UCXN的FQDN,您會看到「已安裝的應用程式」(稱為「**Recovery URL」**)下有一個新選項,用於繞過單點登入(SSO)。 按一下Cisco Unity Connection連結後, AD FS會提 示您輸入憑證。輸入使用者SSO的憑據後,您將成功登入到Unity Administration頁面Unified Serviceability頁面。

Chttps://ucon1.ciscolive.com/ - Windows Internet Explorer		_ 8 ×
C C + Ittps://ucm1.dscolive.com/	Certificate Error 🐓 🗙 🔎 Bing	. م
🙀 Favorites 🛛 🙀 🙋 Suggested Sites 🔹 🙋 Web Sice Gallery 🔹		
🙁 🔹 🖸 Certificate Error: Navigation Chttps://ucxn1.ciscolive.c 🗙	han e na e	afety + Tools + 😢 +
alada		Î
CISCO		
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>		

附註:SAML SSO不允許訪問以下頁面:

- Prime Licensing Manager
- 作業系統管理
- 災難恢復系統

### 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

如需詳細資訊,請參閱適用於協同合作產品10.x的SAML SSO疑難排解。