# 統一通訊管理器10.5版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>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

本檔案介紹如何設定和驗證思科整合通訊管理員(CUCM)的安全宣告標籤語言(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。

如果CUCM和IdP之間存在時間不匹配,您將收到以下錯誤:"無效SAML響應。" 當CUCM和IdP伺 服器之間的時間不同步時,可能導致此錯誤。要使SAML SSO正常工作,必須安裝正確的NTP設定 ,並確保IdP和統一通訊應用程式之間的時間差不超過三秒。

有關如何同步時鐘的資訊,請參閱<u>Cisco Unified Communications作業系統管理指南</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。

#### 採用元件

本文中的資訊係根據以下軟體和硬體版本:

- •作為IdP的Active Directory聯合身份驗證服務(AD FS)版本2.0
- •作為服務提供商的CUCM 10.5版
- Microsoft Internet Explorer 10

**注意**:本文檔基於新安裝的CUCM。如果在已投入生產的伺服器上配置SAML SSO,則可能 必須相應地跳過某些步驟。在生產伺服器上執行這些步驟時,還必須瞭解服務影響。建議在非 工作時間執行此過程。

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是基於XML的開放式標準資料格式,使管理員能夠在登入到其中某個應用後,無縫訪問一組 已定義的思科合作應用。SAML SSO在作為IdP與服務提供商之間的調配過程的一部分交換後設資 料時建立信任圈(CoT)。服務提供商信任IdP的使用者資訊以提供對各種服務或應用的訪問。

**附註**:服務提供商不再參與身份驗證。SAML 2.0版將身份驗證從服務提供商處委託給IdP。客 戶端根據IdP進行身份驗證,IdP向客戶端授予斷言。客戶端向服務提供商顯示斷言。由於已建 立CoT,因此服務提供商信任宣告並授予對客戶端的訪問許可權。

### 設定

#### 網路圖表



Figure :SAML Single sign SSO Call Flow for Collaboration Servers

### 目錄設定

1. 選擇Cisco Unified CM Administration > System > LDAP > LDAP System。



- 2. 按一下「Add New」。
- 3. 配置輕量型目錄訪問協定(LDAP)伺服器型別和屬性。
- 4. 選擇Enable Synchronizing from LDAP Server。

LDAP System Configura	ation	
Save		
-Status		
i Status: Ready		
LDAP System Informat	tion	
Enable Synchronizing f	from LDAP Server	
LDAP Server Type	Microsoft Active Directory	-
LDAP Attribute for User ID	sAMAccountName	-
Save		

- 5. 選擇Cisco Unified CM Administration > System > LDAP > LDAP Directory。
- 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

LDAP Directory	
🔚 Save 🗶 Delete 🛅 Copy 👔	Perform Full Sync Now 🕂 Add New
Status	
Status Status: Ready	
-IDAR 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. 如果不想使用安全套接字層(SSL)與LDAP目錄通訊,請取消選中使用SSL。

**提示:**如果要通過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。

8. 按一下Save,然後按一下Perform Full Sync Now。

**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。** 

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

9. 導航到User Management > End User, 然後選擇要向其授予CUCM管理角色的使用者(此示例 選擇使用者SSO)。

System +	Call Routing 👻 Medi	a Resources 👻 Adva	anced Features 👻 Dev	rice + Application +	User Management 👻	Bulk Administration $\bullet$	Help 👻
Find and	l List Users						
🕂 Add	New Eselect All	🖽 Clear All   🙀 (	Delete Selected				
Status							
3 re	cords found						
-							
User	(1 - 3 of 3)						Rows p
User Find User	(1 - 3 of 3) r where First name		begins with 💽	]	Find Clear Filter	4	Rows p
User Find User	(1 - 3 of 3) r where First name User ID ^	First Name	Degins with 💽	Department	Find Clear Filter Directory U	₽ = RI	<i>Rows p</i> User Status
User Find User	(1 - 3 of 3) r where First name User ID ^ SSQ	First Name Saml	Last Name SSO	Department	Find Clear Filter Directory U	IRI Active LDA	<i>Rows p</i> User Status NP Synchronized User

10. 向下滾動到「Permissions Information(許可權資訊)」 ,然後按一下「Add to Access Control Group(新增到訪問控制組)」。選擇標準CCM超級使用者,按一下Add Selected,然後按一下Save。

IPS Standard CCM Super Users		
		Add to Access Control Group
		Remove from Access Control Group
	View Details	
Standard AXL API Access		
Standard Admin Rep Tool Admin	-	
Standard CCM Admin Users	-	
Standard CUReporting	View Details	

#### 啟用SAML SSO

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



3. 要在群集中啟用SAML SSO,請按一下Enable SAML SSO。

SAML Single Sign-O	'n					
V Enable SAML SSO	Export All Me	etadata 🔞 Update KIP I	Metadata File 🥜 Fix All D	isabled Servers		
-Status						
i SAML SSO disabl	ed					
SAML Single Sign-	0n (1-2 <i>o</i> f	2)				Rows per Page 50
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. 在「重置警告」視窗中,按一下繼續。

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 🖉 👘 🗸 Trusted sites   Protected Mode: Off 🛛 🖓 🔹 🔍 100% 🔹	//.

5. 在SSO螢幕上,按一下**Browse**,以使用**下載IdP後設資料**步驟匯入 IdP(**FederationMetadata.xml**)後設資料XML檔案。

System 👻	Call Routing 👻	Media Resources 👻	Advanced Features 👻	Device 👻	Application +	User Management 👻	Bulk Administration 👻	Help 🕶
SAML Sin	gle Sign-On	Configuration						
Next								
Chattan								
i Statu	is: Ready							
- Downloa To configu manually This	ad Identity pr ure the trust re obtain the file f is a manual st	ovider(IdP) Metad lationship between th from the IdP before y	data Trust File he IdP and your device you can upload it to yo	es, you mu our Collabo	ist first obtain t pration servers	rust metadata from y	your IdP and import it	to your servers. You will need to
1)Log in t	o your IdP and	download the metad	lata trust file to your l	ocal server	r.			
2)Click 'N	ext' once you h	nave this file availabl	e locally.					
Next	Cancel							
Next	Cancel							

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

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 IdD 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
Variable Import succeeded for all servers

7. 按一下**Download Trust Metadata File**(可選),將CUCM和CUCM IM and Presence後設資料 儲存到本地資料夾,並轉至<u>Add CUCM as Reliing Party Trust</u>。完成AD FS配置後,請繼續執 行步驟8。

V Import succeeded for all servers

Browse...

SAML Single Sign-On Configuration
de Back into Next
- Chalus
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 then skip the steps below and click Next. Otherwise follow the steps below to upload 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 Metadata has been imported to servers in this cluster
Download Server metadata and install on the for 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. 選擇SSO作為管理使用者,然後按一下運行SSO測試。

This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.

This action must be successful for at least the Publisher before moving on to the next task in this wizard.

1)Select the IdP Metadata Trust File

Import IdP Metadata

Next Cancel

2)Import this file to the Collaboration servers

Γ

System +	Call Routing	+ I	Vedia Resources 🔹	Advanced Features +	Device -	Application +	User Management 👻	Bulk Administration 👻	Help 🛨	
SAML SI	ngle Sign-O	n Co	onfiguration							
de Back										
Challens										-
	server meta	data	file must be inst	alled on the IdP before	this test is	run.				
- Test SS	0 Setup —									
This test SSO has	verifies that been enable	the n d. SS	netadata files ar O setup cannot	e correctly configured a be completed unless th	ind will allo is test is su	w SSO to start ccessful.	up on the servers. T	his test can be run or	any server for troubles	hooting once
1)Pick a	valid usernar	ne to	use for this test	:						
You must This user	already kno must have a	w the	a password for t histrator rights a	he selected username. nd also exist in the IdP						
🔥 Plea	ise use one o	of the	Usernames sho	wn below. Using any o	her Userna	me to log into	the IdP may result in	administrator lockou	ıt.	
Valid adn	ninistrator Us	erna	mes							
· · · ·										
2)Launch	SSO test pa	ge								
Run	SSO Test									
Back	Cancel									

9. 忽略證書警告並繼續。當系統提示您輸入憑據時,請輸入使用者SSO的使用者名稱和密碼,然 後按一下**確定**。

Windows Security usted certification Connecting to ADFS1.ciscolive.com.
Connecting to ADFS1.ciscolive.com.
ercept any c
sso •••••••• Domain: CISCOLIVE Remember my credentials
OK Cancel

附註:此配置示例基於CUCM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CUCM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,「SSO測試成功!」 顯示消息。按一下**Close**和**Finish**以繼續。您現在已成功完成配置任務,以便在CUCM上啟用SSO with AD FS。



11. 由於CUCM IM and Presence與CUCM使用者類似,您必須將<u>Add CUCM IM and Presence</u> <u>as Relisting Party Trust</u>配置,然後運行**Run SSO Test**,以便從CUCM SAML SSO頁面本身 啟用SAML SSO。

**附註**:如果在IdP上配置所有節點的後設資料XML檔案,並且在一個節點上啟用SSO操作,則 集群中的所有節點上都會啟用SAML SSO。

必須將群集中CUCM和CUCM IM and Presence的所有節點配置為中繼方。

**提示:**如果您希望對Cisco Jabber客戶端使用SAML SSO體驗,則還應配置Cisco Unity Connection以及CUCM IM and Presence for SAML SSO。

### 驗證

使用本節內容,確認您的組態是否正常運作。

- 1. 開啟Web瀏覽器並輸入CUCM的FQDN。
- 2. 按一下「Cisco Unified Communications Manager」。
- 3. 選擇Web應用(CM管理/統一可維護性/Cisco Unified Reporting)並按Go,AD FS將提示您輸入憑 據。輸入使用者SSO的憑證後,您即成功登入到選定的Web應用(CM管理頁面、Unified Serviceability頁面、Cisco Unified Reporting)。

// http://cucm.ciscolive.com/ - Windows Internet Explorer		_ # X
🚱 🕢 🗢 🛱 http://cucm.discolive.com/	🗾 🔂 🗙 🔎 Bing	. م
🚖 Favorites 🛛 🚔 👩 Suggested Sites 🔹 👩 Web Slice Gallery	•	
did: http://cucm.ciscolive.com/	🎦 + 🔂 - 🖃 🖶 - Page - 1	Safety - Tools - 🔞 -
		-
ahaha		
CISCO		
Installed Applications		
<ul> <li>Cisco Unified Communication</li> <li>Recovery URL to bypa</li> <li>Cisco Unified Communication</li> <li>Cisco Prime License Manag</li> <li>Cisco Unified Reporting</li> <li>Cisco Unified Serviceability</li> </ul>	ns Manager iss Single Sign On (SSO) ins Self Care Portal er	
Platform Applications		
Disaster Recovery System     Cisco Unified Communication	ns OS Administration	

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

如果您無法啟用SAML且無法登入,請使用名為**Recovery URL的已安裝應用程式下的新選項繞過單 點登入(SSO)**,該選項可用於使用在安裝期間建立的憑據或本地建立的CUCM管理使用者登入。

🚰 Cisco Unif	ied CM Console - Windows Internet Explorer			_ 8 ×
00-	https://cucm.dscolive.com/ccmadmin/showRecovery.do	🔹 😨 Certificate Error	😝 🗙 🔎 Bing	۹.
👉 Favorites	🝰 🙋 Suggested Sites 🔹 🙋 Web Silce Gallery 🔹			
🏉 Cisco Unifi	led CM Console		💁 • 🖾 · 🖃 🖶 •	Page + Safety + Tools + 🔞 +
cisco	Cisco Single Sign On Recovery Administration For Cisco Unified Communications Solutions			
Cisco This pag running This pag	o Single Sign On Recovery Administrat ge will validate credentials locally, allowing access only to applicatio on this server, and will not leverage SAML SSO authentication. ge can be disabled through the CLI.	ion ns that are	Username ccmadmin Password Login Reset	
Copyright @	) 1999 - 2015 Cisco Systems, Inc.			

All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

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

For information about Cisco Unified Communications Manager please visit our <u>Unified Communications System Documentation</u> web site.

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

如需進一步的疑難排解,請參閱適用於合作產品10.x的SAML SSO疑難排解。