在帶有ADFS 3.0的Cisco Unified Communications Manager上配置SAML SSO

目錄

簡介 必要條件 需求 採用元件 組態預先檢查 A記錄 指標(PTR)記錄 需要為Jabber Discovery Services保留SRV記錄 ADFS3初始配置 使用ADFS在CUCM上配置SSO LDAP配置 CUCM後設資料 配置ADFS信賴方 IDP後設資料 <u>在CUC上配置SSO</u> CUC後設資料 在Expressway上配置SSO 將後設資料匯入到Expressway C 從Expressway C匯出後設資料 為Cisco Expressway-E新增信賴方信任 使用刷新登入的OAuth 驗證路徑 SSO架構 本地登入流程 MRA登入流 OAuth 存取/刷新權杖 OAuth授權代碼授權流程更好 配置Kerberos 選擇Windows身份驗證 ADFS同時支援Kerberos NTLM 配置Microsoft Internet Explorer 在Security > Intranet zones > Sites下新增ADFS URL 將CUCM、IMP和Unity主機名新增到Security > Trusted Sites 使用者驗證 SSO中的Jabber登入 疑難排解 Internet Explorer(IE)

<u>站點新增到IE</u> <u>不同步問題</u> <u>撤銷令牌</u> <u>載入程式檔案</u> 由於MSIS7066而導致SSO失敗

簡介

本文檔介紹在Cisco Unified Communication Manage(CUCM)、Cisco Unity Connection(CUC)和 Expressway產品上使用Windows 2012 R2使用Active Directory聯合身份驗證服務(ADFS 3.0)配置單 一登入的步驟。本文還包括配置Kerberos的步驟。

必要條件

需求

思科建議您瞭解一次登入(SSO)和Windows產品。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- CUCM 11.5
- CUC 11.5
- Expressway 12
- 具有以下角色的Windows 2012 R2 Server:
 - Active Directory證書服務
 - Active Directory聯合身份驗證服務

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。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

組態預先檢查

安裝ADFS3之前,環境中需要已經存在這些伺服器角色:

·域控制器和DNS

·所有伺服器必須作為A記錄與其指標記錄(將IP地址解析為域或主機名的一種DNS記錄)一起新增

A記錄

在fhlab.com。已新增主機cmpubhcsc、cmsubhcsc、cucpubhcsc、cucsubhcsc、expwyc、expwye、impubhcsc和imsubhcsc。



指標(PTR)記錄

8	DNS	Name	Туре	Data	Timestamp
4	AD	(same as parent folder)	Start of Authority (SOA)	[14], ad.fhlab.com., hostmaster.fhlab.co	static
	a 📔 Forward Lookup Zones	(same as parent folder)	Name Server (NS)	ad.fhlab.com.	static
	[] _msdcs.fhlab.com	10.89.228.144	Pointer (PTR)	expwyc.fhlab.com.	static
	⊿ 🛐 fhlab.com	10.89.228.145	Pointer (PTR)	expwye.fhlab.com.	static
	▷ [] _msdcs	10.89.228.146	Pointer (PTR)	cmpubhcsc.fhlab.com.	static
	i _sites	10.89.228.147	Pointer (PTR)	cmsubhcsc.fhlab.com.	static
▷ 2 _tcp▷ 2 _udp▷ 2 DomainDnsZone	⊳ 🚞 _tcp	10.89.228.148	Pointer (PTR)	imppubhcsc.fhlab.com.	static
	þ 📃 _udp	10.89.228.150	Pointer (PTR)	impsubhcsc.fhlab.com.	static
	DomainDnsZones	10.89.228.151	Pointer (PTR)	cucpubhcsc.fhlab.com.	static
	A ForestUnsZones	10.89.228.153	Pointer (PTR)	cucsubhcsc.fhlab.com.	static
	p 🔜 _sites	10.89.228.154	Pointer (PTR)	win10.fhlab.com.	5/12/2020 10:00:00 AM
		10.89.228.226	Pointer (PTR)	ad.fhlab.com.	5/12/2020 11:00:00 AM
	228.89 10 in-addr arn	10.89.228.227	Pointer (PTR)	win10ext.fhlab.com.	5/7/2020 4:00:00 PM
	E crossion and a contract				

需要為Jabber Discovery Services保留SRV記錄

L DNS	Name	Туре	Data	T	imestamp	
a 🗎 AD	cisco-uds	Service Location (SRV)	[0][0][8443] cmsubhcsc.fhla	ib.com. s	tatic	
a 🚞 Forward Lookup Zones	cisco-uds	Service Location (SRV)	[0][0][8443] cmpubhcsc.fhla	ab.com. s	tatic	
[] _msdcs.fhlab.com	cuplogin	Service Location (SRV)	[0][0][8443] impsubhcsc.fhl	ab.com. s	tatic	
⊿ 👸 fhlab.com	cuplogin	Service Location (SRV)	[0][0][8443] imppubhcsc.fhl	lab.com. s	tatic	
b [] _msdcs	gc	Service Location (SRV)	[0][100][3268] ad.fhlab.com	. 5	/12/2020 10:00:00 AM	
þsites	kerberos	Service Location (SRV)	[0][100][88] ad.fhlab.com.	5	/12/2020 10:00:00 AM	
tcp	kpasswd	Service Location (SRV)	[0][100][464] ad.fhlab.com.	5	/12/2020 10:00:00 AM	
budp	a _ldap	Service Location (SRV)	[0][100][389] ad.fhlab.com		100000000000000000000000000000000000000	
DomainUnszones					_cisco-uds Proper	ties Y
A Porestonszones				Contro Location	(CD)A	
psites				Service Location	(SHV) Securty	
A Beverse Lookup Zones				Domain:	fhlab.com	
228.89.10.in-addr.arp						
Trust Points				Service:	_cisco-uds	~
Conditional Forwarders				Pertagal	lee.	
Global Logs				Protocol.	300	¥
_				Priority:	0	
				Weight	0	
				weight.	•	
				Port number:	8443	
				Host offering this	a section.	
				consublices fbla	ah com	
				chipdonese ma	av	
	1					

•根CA(假設證書由企業CA簽署)

需要基於Web伺服器證書模板建立證書模板,複製證書模板,重新命名證書模板,並在「擴展」頁 籤上修改應用程式策略,新增客戶端身份驗證應用程式策略。在實驗室環境中簽署所有內部證書 (CUCM、CUC、IMP和Expressway核心)時需要使用此模板。內部CA還可以簽署Expressway E證書簽名請求(CSR)。



需要頒發建立的模板才能簽署CSR。

File Action View Help		
🗢 🔿 🙎 🙆 📓		
🙀 Certification Authority (Local)	Name	Intended Purpose
⊿ 👼 fhlab-AD-CA	ClientServerAuth	Server Authentication, Client Authentic
Revoked Certificates	Directory Email Replication	Directory Service Email Replication
Issued Certificates	Domain Controller Authentication	Client Authentication, Server Authentic
Pending Requests	Kerberos Authentication	Client Authentication, Server Authentic
Failed Requests	EFS Recovery Agent	File Recovery
Certificate Te Manag	je	Encrypting File System
New	Certificate Template t	ication

在CA證書Web上,選擇以前建立的模板。

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external sour Web server) in the Saved Request box.



CUCM、IMP和CUC多伺服器CSR必須生成並由CA簽名。證書用途必須為tomcat。

Generate Certificate Signing	l Request	
🥵 Generate 🖳 Close		
Status		
🔥 Warning: Generating a	new CSR for a specific certificate type will overwrite	the existing CSR for that type
Generate Certificate Signi	ng Request	
Certificate Purpose**	tomcat	1
Distribution*	Multi-server(SAN)	1
Common Name*	cmpubhcsc-ms.fhlab.com	
Subject Alternate Names	(SANs)	
Auto-populated Domains	cmpubhcsc.fhlab.com cmsubhcsc.fhlab.com imppubhcsc.fhlab.com impsubhcsc.fhlab.com	
Parent Domain	fhlab.com	
Other Domains		Browse No file selected. Please import .TXT file only. For more information please refer to the notes in the Help Section
Key Type** Key Length*	RSA 2048]
Hash Algorithm*	SHA256	

Generate Close

必須將CA根證書上傳到Tomcat信任,並將簽名證書上傳到tomcat。

cisco For (co Unified Operating	Navi	pation Cisco Unified OS Administration sadmin Search Documentation About	Go Logout							
Show . Settings	Show + Settings + Security + Software Upgrades + Services + Help +										
Certificate List											
Generate Self-s	signed Dolbad Certificate/Certifica	ate chain Generate CSR									
0		0									
1 7 records for	und										
Certificate List	t (1 - 7 of 7)					Rows per Page 50	~				
Find Certificate Lis	st where Certificate 🗸 begi	ns with 🗸 tomcat	Find Clear Filter	4 -							
Contificate *	Common Name	Type Key Type	Distribution	Issued By	Expiration	Description	_				
tomcat	cmoubhcsc-ms.fhlab.com	CA-signed RSA	Multi-server(SAN)	fhlab-AD-CA	04/18/2022	Certificate Signed by fhlab-AD-CA					
tomcat-ECDSA	cmoubhcsc-EC./hlab.com	Self-signed EC	cmpubhcsc.thiab.com	cmpubhcsc-EC.thlab.com	04/02/2025	Self-signed certificate generated by system	-				
tomcat-trust	impoublese-EC.fhlab.com	Self-signed EC	imppublicsc.fhlab.com	imppublicsc-EC.fhlab.com	04/02/2025	Trust Certificate					
tomcat-trust	cmsubhcsc-EC.fhlab.com	Self-signed EC	cmsubhcsc.fhlab.com	cmsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate					
tomcat-trust	impsubhcsc-EC.fhlab.com	Self-signed EC	impsubhcsc.fhlab.com	impsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate					
Instant Instant	emoulahore EC falsh com	Roll classed BC	consultations (high com	consultance EC faish com	04/03/3035	Tout Cadificate	_				
tomcat-trust	fhlab-AD-CA	Self-signed RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate					
Generate Self-s	signed Upload Certificate/Certif	ficate chain Generate CSR					- 1				
-							_				
Certificate List	(1-6of6)					Rows per Pao	e 50				
		an water a large state	fied Class Shar	di m							
Find Continues 11	studens Castificate	os with support	Find Clear Filter								
Find Certificate Lis	st where Certificate v begi		Internet in the second								
Find Certificate Lis	st where Certificate v begi	Type Key Ty	Distribution	Issued By	Expiration	Description					
Find Certificate Lis Certificate * tomcat	Common Name cucpublicsc-ms.fhlab.com	Type Key Ty CA-signed RSA	e Distribution Multi-server(SAN)	Issued By fhlab-AD-CA	Expiration 04/28/2022	Description Certificate Signed by Rilab-AD-CA	3				
Find Certificate Lis	Common Name Common Name cucoubhosc-ma.fhiab.com	Type Key Ty CA-signed RSA Self-signed RSA	Bab AD-CA	Issued By fhlab-AD-CA	Expiration 04/28/2022	Description Certificate Signed by Phab-AD-CA Signed Certificate	2				
Find Certificate Lis	St where Certificate V begin Common Name cucpublicsc-ms.fhlab.com	Type Key Ty CA-signed RSA	Part Distribution Multi-server(SAN) Multi-server(SAN)	Issued By FNab-AD-CA FNab-AD-CA	Expiration 04/28/2022 04/18/2025	Description Certificate Signed by fhlab-AD-CA Signed Certificate					
Find Certificate Lis	Common Name Common Name Cucubhos-ms.Nab.com fhisb-AD-CA secondation.uncenteene	Type Key Ty CA-signed RSA Self-signed RSA Or synchronic RSA	Distribution Multi-server(SAN) fhlab-AD-CA rose Server(covy) cussubtase.fhlab.com	Issued By fhlab-AD-CA fhlab-AD-CA cutsubhase-EC.(hlab.com	04/28/2022 04/18/2025 04/02/2025	Description Certificate Signed by Mab-AD-CA Signed Certificate Trust Certificate Windows	3				

• IIS

如果沒有,本節將介紹這些角色的安裝。否則,請跳過此部分,直接從Microsoft下載ADFS3。

安裝帶有DNS的Windows 2012 R2後,將伺服器升級為域控制器。

下一個任務是安裝Microsoft證書服務。

導航到伺服器管理器並新增新角色:

6		Server Manager		_ _ X
Server Ma	anager • Dashb	oard	• © 🏲	Manage Tools View Help
Dashboard	WELCOME TO SERVER	t MANAGER		Add Koles and Features Remove Roles and Features Add Servers
All Servers	OU HOY START	1 Configure this local serve	r	Create Server Group Server Manager Properties
AD DIS AD AD FS AD DNS Elia and Storage Services D	Conce a sure	 Add roles and features Add other servers to manage 	e	
io IIS	WHAT'S NEW	4 Create a server group		
	LEARN MORE			Hide
	ROLES AND SERVER O Roles: 6 Server groups:	I Servers total: 1	1 2 4	ID FS 1
	-18 10 03			v 13

選擇Active Directory證書服務角色。

b	Add Roles and Features Wizard	_ X
Select server roles		DESTINATION SERVER AD:fnlab.com
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select one or more roles to install on the selected server. Roles	Description Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
	Network Policy and Access Services Print and Document Services	×
		< Previous Next > Install Cancel

並首先部署這些服務 — 證書頒發機構證書註冊策略Web服務。安裝這兩個角色後,請對其進行配 置,然後安裝**證書註冊Web服務**和**證書頒發機構Web註冊**。配置它們。

安裝證書頒發機構後,還會新增所需的其他角色服務和功能,例如IIS。

根據您的部署,您可以選擇企業或獨立。

Add Roles Wizard		×
Specify Setup Typ	pe	
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress Results	Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.	
	More about the differences between enterprise and standalone setup	
	< Previous Next > Install Cancel	

對於CA型別,您可以選擇根CA或從屬CA。如果組織中沒有其他CA正在運行,請選擇**根CA**。

Add Roles Wizard		×
Specify CA Type		
Before You Begin Server Roles AD CS Role Services Setup Type CA Type	A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA. C Root CA Select this option if you are installing the first or only certification authority in a public key infrastructure. C Scheerdnete C1	
Private Key Cryptography CA Name Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress Results	Subordinate CA Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.	
	More about public key infrastructure (PKI) Previous Next > Install Cancel	

Add Roles Wizard

Refore You Regin To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to	Set Up Private Key						
Server Roles In genetic and state for distance to distance a private key or use an existing one. AD CS Image: Create a new private key Role Services Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key to will be asked to select a cryptographic service provider and specify a key length for the private key CA Type Use existing private key Private Key Use existing private key CA Type Use existing private key Chyptography Select a certificate and use its associated private key. Ca Name Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key. Certificate Database Select this option if you have retained private keys from a previous installation or want to use a prive key from an alternate source.	vate						
Role Services Confirmation Progress Results More about public and private kevs							

×

只有在單獨的Windows Server 2012上安裝ADFS3時,才需要執行此步驟。配置CA後,需要配置 IIS的角色服務。這是在CA上進行Web註冊所必需的。對於大多數ADFS部署,在IIS中需要額外的角 色,請按一下「應用程式開發」下的ASP.NET。

Add Roles Wizard		×
Select Role Servi	ces	
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress Results	Select the role services to install for Web Server (IIS): Role services: Web Server Common HTTP Features Static Content Default Document Directory Browsing HTTP Errors HTTP Redirection WebDAV Publishing Application Development Met Extensibility ASP CGI Server Side Includes Health and Diagnostics HTTP Logging Logging Tools Request Monitor Tracho	Description: ASP.NET provides a server side object oriented programming environment for building Web sites and Web applications using managed code. ASP.NET is not simply a new version of ASP. Having been entirely rearchitected to provide a highly productive programming experience based on the .NET Framework, ASP.NET provides a robust infrastructure for building web applications.
	< Previous	Next > Instal Cancel

在伺服器管理器中,按一下**Web Server > IIS**,然後按一下右鍵**Default Web Site**。除了HTTP外 ,還需要更改繫結以允許HTTPS。這麼做是為了支援HTTPS。



選擇**編輯繫結**。

<i>8</i>]	Interne	t Informatio	n Services	(IIS) Manage	er		_ D X
AD > Sites > Default Web S	ite 🕨						🖬 🖾 🟠 😥 •
File View Help							
Connections	0.0		cite the				Actions
Q,- 🔒 🖄 😣	🥹 De	efault Web	Site Ho	me			🔉 Explore
Start Page	Filter		• 🐨 Go - 1	Show All	Group by:		Edit Permissions
AD (FHLAB\administrator)	ASP.NET					A A	Edit Site
a 🧕 Sites	En .	😓	A	۵			Bindings
Default Web Site		NET	NET Error	NET	NET Profile		Egg Basic Settings
Explore		Compilation	Pages	Globalization		=	View Applications View Virtual Directories
		A.	1	1	C		Manage Website
Add Application	stony 5	NET Trust	NET Users	Application	Connection		Restart
20 Not the one	coory	Levels		Settings	Strings		Start
Edit Bindings		and the second s					Stop
Manage Website	• •	Paper and	Providers	Service State	SMTP F-mail		Browse Website
E Refresh	~ ^'	Controls	rionacia	Season State	SHITT CHING		Browse *:80 (http)
× Remove						~	Browse ":443 (https)
Rename		~	Ð				Advanced Settings
Switch to Conte	nt View	0	H	0	لطه	\checkmark	Configure -
	Features Vi	ew 💦 Conten	t View				Limits V
Ready							•1.:

新增新的站點繫結並選擇**HTTPS**作為型別。對於SSL證書,選擇應與AD伺服器具有相同FQDN的伺 服器證書。

e 3			Intern	et Information	n Services (IIS) Manager	
€) AD →	Sites 🔸	Default Web Site	•			
File View Help						
Connections				Site	Bindings	? X
 Start Page AD (FHLAB\admini Application Poc Sites Default Web 	Type http https	Host Name Type: https Host name: Require S SSL certifica fhlab-AD-Co Not selected fhlab-AD-Co AD.fhlab.com	Port 80 442 I erver Name te: A I A m	IP Address * Edit P address: All Unassigned * Indication	Binding Informa t Site Binding Port: 443 Select OK	Add Fdit ? X

所有必備角色都安裝在環境中,因此現在您可以繼續安裝ADFS3 Active Directory聯合身份驗證服務 (在Windows Server 2012上)。

對於伺服器角色,導航到Server Manager > Manage > Add Server Roles and Features,然後在專 用LAN上在客戶網路中安裝IDP時選擇Active Directory Federation Services。



安裝完成後,您可以從工作列或「開始」選單開啟它。

Pile Action View Window Help Image: Constraint of the second seco	%	AD FS	_ _ X
Image: Contract of the service of t	🧌 File Action View Window Help		_ 8 ×
▲ AD FS Actions Overview AD FS provides single sign on (SSO) access for client computers. Add Relying Party Trust Learn More Configuing Trust Relationships Add Attribute Store Configuing Authentication Policies Troubleshooting AD FS AD FS Help View ND FS Help View Revice All Provides View Refresh Metershooting	(+ - +) 📰 🖬 🖬		
Overview AD FS ▲ Add Relying Party Trust Add Relying Party Trust Add Relying Party Trust Add Claims Provider Trust Learn More Configuring Trust Relationships Edit Federations Provider Trust Configuring Authentication Policies Edit Federations Edit Federations Troubleshooting AD FS Revoke All Provides Revoke All Provides AD FS Help View New Window from Here Refresh Help	ad FS	AD FS	Actions
keren keren		Overview AD FS provides single-sign-on (SSO) access for client computers. Learn More Configuring Trust Relationships Configuring Authentication Policies Troubleshooting AD FS AD FS Help	AD FS Add Relying Party Trust Add Relying Party Trust Add Claims Provider Trust Add Attribute Store Edit Federation Service Properti Edit Published Claims Revoke All Proxies View New Window from Here
Activate Windows		Activate	Windows

ADFS3初始配置

本節將介紹如何安裝新的獨立聯合伺服器,但也可以將其安裝在域控制器上

選擇Windows並鍵入AD FS Management以啟動ADFS管理控制檯,如下圖所示。



選擇AD FS 3.0 Federation Server Configuration Wizard 選項以啟動ADFS伺服器配置。這些截圖與 AD FS 3中的步驟相同。

AD FS 2.0 Federation Ser	ver Configuration Wizard	×
Welcome		
Steps Welcome Select Deployment Type Federation Service Name Summary Results	 Welcome to the AD FS 2.0 Federation Server Configuration Wizard This wixard helps you configure Active Directory Federation Services (AD FS) 2.0 software on this computer, which sets up the computer as a federation server. An instance of AD FS is referred to as a screation Service. C feate a new Federation Service Select this option to set up either a stand-alone federation server or the first server in a federation server fam. C Ad a federation server to an existing Federation Service Select this option to join this computer to an existing federation server fam. 	
	< <u>Erevisus</u> <u>N</u> ext> Cancel <u>H</u> elp	

選擇Create a new Federation Service並單擊Next。

AD FS 2.0 Federation Ser	ver Configuration Wizard	×
Select Stand-Alone or	r Farm Deployment	
Steps	You can create either a stand alone federation server for evaluation purposes or a small modulation	
Welcome	environment, or you can create a federation server in a new farm for load balancing and high availability.	
Select Deployment Type	Select one of the following options. Either of these options will use the Windows Internal Database to store	
Federation Service Name	coniguration data.	
Summary	O New federation server farm	
 Results 	This option will create a new Federation Service with settings for high availability and load balancing. This computer will be the primary federation server in the farm. Later, you can scale out this farm by adding more federation servers.	
	To create a federation server farm, you must run this wizard while you are logged on with an account that has sufficient permissions in Active Directory to create a container object (for sharing certificates) and to set an SPN (for the service account), such as an account that is a member of the Domain Admins group.	
	⊙ <u>Stand-alone federation server</u>	
	This option will create a new Federation Service on this computer. This option is recommended for evaluation purposes or a small production environment. If you select this option, you will not be able to add more servers to create a farm.	
	You can use SQL Server with AD FS 2.0 to take advantage of the full feature set and achieve maximum scalability. To set up AD FS to use SQL Server, use the command-line version of this wizard. For more information, click Help	
	< Previous Next > Cancel Help	

選擇Standalone Federation Server並按一下**Next**,如下圖所示。

Mail AD FS 2.0 Federation Serve	er Configuration Wizard	×
Specify the Federation	Service Name	
Steps Welcome Select Deployment Type Federation Service Name	This wizard determines the Federation Service name from the Subject field of the SSL certificate for the Default Web Site. If the wizard cannot determine the Federation Service name from the SSL settings, you must select a certificate. Select the certificate and/or port, and then click Next.	
 Summary Results 	SSL certificate: Port: ad0a.identitylab.us View 443 * Federation Service name: ad0a.identitylab.us * What kind of certificate do I need?	
	Yrevious Next > Cancel Help Xancel Help Xance	

在SSL certificate下,從清單中選擇自簽名證書。聯合身份驗證服務名稱將自動填充。按「**Next**」 (下一步)。

AD FS 2.0 Federation Ser	ver Configuration Wizard	×
Ready to Apply Settin	gs	
Steps	The following settings will be configured for AD FS 2.0:	
Welcome Select Deployment Type Federation Service Name Summary Results	 The following settings will be configured for AD FS 2.0. Stop AD FS server. Windows Internal Database service will be started and set to automatic startup. Signing and token-encryption certificates will be generated and set to automatic roll over. Selected SSL certificate will be used for securing service communication. Network Service account will be given access to the database, to the certificate private keys and endpoints, and the service will run under this account. Default set of endpoints will be enabled. Browser sign-in web site will be deployed to the Vadfs/Is' virtual directory under the Default Web Site in IIS. Federation Service name is adDatidentitylab.us Start AD FS server. 	
	To begin configuring this computer with these settings, click Next. < Previous	

檢查設定並按一下**下一步**以應用設定。

Configuration Results		
Step*	The following settings are being configured	
 Welcome Select Deployment Type Federation Service Name Summary Results 	Component Install Windows Internal Database Install Windows Internal Database Install Windows Internal Database Create AD FS configuration database Configure service settings Deploy browser sign-in Web site Ended of the AD FS 2.0 Windows Service Create default claim set Create default Active Directory claim acceptance rules You have successfully completed the AD FS 2.0 Federation To close this wizerd, click Close.	Status Configuration finished Server Configuration Wizard.
		Clare

Action View Window H	eb	
52.0	AD 15 2.0	Actions
ervice		AD F5 2.0
un resources	AD FS 2.0 provides single-sign-on (SSO) access for client computers.	Add Relying Party Trust Add Claims Provider Trust Add Attribute Store
	Required Configuration Incomplete Before you can use AD FS 2.0 to manage SS0 access for users and services, you must complete the following task:	Edit Federation Service Properties Edit Published Claims
	Pequired: Add a trusted rebring party	Revoke All Proxies Provide Feedback
	2 Learn About:	View New Window from Here
	Configuring Claims Provider or Belying Party Trusts	G Refresh
	Configuring Federation Server Proxies Configuring Federation Server Proxies Troubleshooting AD FS 2.0	E Pep

ADFS現在已有效地啟用並配置為身份提供程式(IdP)。 接下來,您需要將CUCM新增為可信賴合作 夥伴。在執行此操作之前,您需要先在CUCM管理中執行一些配置。

使用ADFS在CUCM上配置SSO

LDAP配置

群集需要與Active Directory進行LDAP整合,並且需要在進一步之前配置LDAP身份驗證。導覽至 System索引標籤> LDAP System,如下圖所示。

LDAP System Configuration

Status Please Delete All LDAP Directories Before Making Changes on This Page Please Disable LDAP Authentication Before Making Changes on This Page LDAP System Information Enable Synchronizing from LDAP Server LDAP Server Type Microsoft Active Directory SAMAccountName

然後,導航到**System**頁籤> LDAP目錄。

Save X Delete Status Status: Ready LDAP Directory Info	rmation ame* uished Name*	Per LDAP1 fhlab\a	rform Full Sync Nov	• 🕂	Add New	
Status Status: Ready - LDAP Directory Info LDAP Configuration Na	rmation ame* uished Name*	LDAP1 fhlab\a				
Status: Ready LDAP Directory Info LDAP Configuration Na	rmation ame* uished Name*	LDAP1 fhlab\a				
- LDAP Directory Info LDAP Configuration Na	rmation ame* uished Name*	LDAP1 fhlab\a				
LDAP Configuration Na	ame* uished Name*	LDAP1 fhlab\a				
	uished Name*	fhlab\a				
LDAP Manager Disting			administrator			
LDAP Password*		•••••	•••••	•••••	•••••	
Confirm Password*		•••••	•••••	•••••	•••••	
LDAP User Search Bas	e* (cn=use	ers,dc=fhlab,dc=d	com		
LDAP Custom Filter for	r Users	< Nor	ne >			٥
Synchronize*		🖸 Use	ers Only 🔵 Use	rs and	Groups	
LDAP Custom Filter for	r Groups	< Nor	ne >			٥
LDAP Directory Sync	chronization S	chedu	le			
Perform Sync Just Ond	ce					
Perform a Re-sync Eve	ery*		7		DAY	2
Next Re-sync Time (Y)	YYY-MM-DD hh:	mm)*	2020-05-24 00:	00		
Standard User Fields To Be Synchronized						
Jisco Unified Communications Manager User Fields L Jser ID	LDAP Attribute sAMAccountName		F	Cisco Unified Cor First Name	mmunications Manager User F	divenName
Middle Name	middleName 🖸		L	Last Name		sn
Manager ID r	manager		c	Department		department
Phone Number	telephoneNumber 😌		P	Mail ID		mail
fobile Number	mobile		5	Pager Number		pager
Virectory URI	mail	0	c.	Display Name		displayName
-LDAP Server Information —						
Host Name or IP Addres	ss for Server*				DAP Port* Use TI	.s
10.89.228.226					389	
Add Another Redu	Indant LDAP Server	•				
Save Delete Con	Perform Full	Sync Now	Add New			

Active Directory使用者與CUCM同步後,需要配置LDAP身份驗證。

ababa	Cisco U	nified C	M Ad	ninistratio	n						Navigation	Cip	co Unified CM Administr	ation	√ Go
cisco	For Cisco U	Inified Com	municati	ons Solutions							farfa	er l	Search Documentatio	n About	Logout
System •	Call Routing 💌	Media Resource	ces 👻 A	dvanced Features 🔻	Device -	Application •	User Manag	ement 🕶	Bulk Administration 💌	Help 🕶					
LDAP Aut	hentication														
Save															
Status															
i) Stat	us: Ready														
LDAP AU	thentication f	or End User	s									_			
Use U	DAP Authenticat	tion for End U	isers												
LDAP Mar	nager Distinguis	hed Name*	fhlab\Adr	ninistrator											
LDAP Pas	sword*		•••••	•••••	•••••	•••••									
Confirm I	Password*		•••••		•••••	•••••									
LDAP Use	r Search Base	'	cn=users	,dc=fhlab,dc=com	h										
LDAP Se	rver Informat	ion													
		Host	t Name or	IP Address for Se	erver*			LDAP Por	rt" Use TLS						
10.89.2	28.226							389							
Add A	nother Redunda	Int LDAP Serv	ver												

CUCM中的終端使用者需要為其終端使用者配置檔案分配特定的訪問控制組。ACG是標準CCM超級 使用者。當環境準備就緒時,將使用使用者測試SSO。

End Use	r Configuration		Related Links: Back to Find List Users	√ Go
Sav	e 🗙 Delete 🕂 Add New			
Confirm	MLPP Password			^
MLPP Pr	ecedence Authorization Level Default		~	
CAPF I	nformation			
Associa	ted CAPF Profiles		 View Details 	
Permis	sions Information			
Groups	Standard CCM End Users	^		
	Standard CCM Super Users Standard CTI Allow Control of All Devices Standard CTI Enabled	View Details	Add to Access Control Group Remove from Access Control Group	
Roles	Standard AXL API Access Standard Admin Rep Tool Admin Standard CCM Admin Users Standard CCM End Users Standard CCMADMIN Administration	 View Details 		
Conference Enab Meeting Attende	ence Now Information ble End User to Host Conference Now Number 1001 es Access Code			
Save	Delete Add New			

CUCM後設資料

本節將介紹CUCM Publisher的流程。

第一個任務是獲取CUCM後設資料,為此您需要瀏覽到URL;**https://<CUCM Pub** FQDN>:8443/ssosp/ws/config/metadata/sp ,或者可以從「System(系統)」頁籤> SAML單一登 入下載。這可以按節點或集群範圍完成。最好在群集範圍內執行此操作。

AMI Single Sign-On							
SO Mode							
Chuster wide (One me	tadata file per chui	star Desuises multi-see	ar Tomrat cartificate)				
Cluster wide (one me	cauaca nile per ciu	solis regulates mais-self	ver romcat cercincave)				
Per node (One metad	ata file per node)						
💢 Disable SAML SSO 🏾 🗐	Export Al Metada	ta 🔞 Update kdP Metadi	ata File 🥜 Fix All Disabled Servers				
Status							
RTMT is enabled for	SSO. You can cha	inge SSO for RTMT here					
RTMT is enabled for	SSO. You can cha	inge SSO for RTMT here	L.				
RTMT is enabled for SAML SSO enabled	SSO. You can cha	inge SSO for RTMT here	L				
RTMT is enabled for SAML SSO enabled SAML Single Sign-On	\$\$0. You can che (1 - 4 of 4)	inge SSO for RTMT <u>herr</u>	L				Rows per Page 50
RTMT is enabled for SAML SSO enabled SAML Single Sign-On Server Name	SSO. You can che (1 - 4 of 4) SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Text	Rows per Page 50
RTHT is enabled for SAML SSO enabled SAML Single Sign-On Server Name cmpubhcsc.fhlab.com	(1 - 4 of 4) SSO Status SAML	Re-Import Metadata N/A	Last Metadata Import April 20, 2020 2:00:57 PM PDT	Export Metadata	Last Metadata Export April 18, 2020 8:05:38 PM PDT	SSO Test Passed - April 20, 2020 2:02:15 PM PDT	Rows per Page 50 Run SSO Test.
RTMT is enabled for SAML SSO enabled SAML Single Sign-On Server Name cmpubhcsc.fhlab.com msubhcsc.fhlab.com	SSO. You can cha (1 - 4 of 4) SSO Status SAML SAML	Re-Import Metadata N/A MP	Last Metadata Import April 20, 2020 2:00:57 PM PDT April 20, 2020 2:00:57 PM PDT	Export Metadata Å File File	Last Metadata Export April 18, 2020 8:05:38 PM PDT April 18, 2020 8:05:37 PM PDT	SSO Test Passed - April 20, 2020 2:02:15 PM PDT Passed - April 20, 2020 1:49:45 PM PDT	Rows per Page 50 Run SSO Test. Run SSO Test.
RTMT is enabled for SAML SSO enabled SAML SSO enabled SAML Single Sign-On Server Name ompubhcsc.fhlab.com mppubhcsc.fhlab.com	SSO. You can cha (1 - 4 of 4) SSO Status SAML SAML SAML	Re-Import Metadata N/A M IdP	Last Metadata Import April 20, 2020 2:00:57 PM PDT April 20, 2020 2:00:57 PM PDT April 20, 2020 2:00:57 PM PDT	Export Metadata	Last Metadata Export April 18, 2020 8:05:38 PM PDT April 18, 2020 8:05:37 PM PDT April 18, 2020 8:05:37 PM PDT	SSO Test Passed - April 20, 2020 2:02:15 PM PDT Passed - April 20, 2020 1:49:45 PM PDT Passed - May 24, 2020 12:02:56 PM PDT	Rows per Page 50 Run SS0 Test. Run SS0 Test. Run SS0 Test.

使用有意義的名稱(如sp_cucm0a.xml)在本地儲存資料,之後您將需要該名稱。

配置ADFS信賴方

回到AD FS 3.0管理控制檯。

\$ 0		AD FS		_ _ ×
📬 File Action View Window Help				_ 8 ×
🗢 🌩 🙎 📰 📓 🗊				
ad FS	Relying Party Trusts			Actions
Envice Service Trust Relationships	Display Name	Enabled Type Identifier		Relying Party Trusts
Claims Provider Trusts	Device Registration Service CLICM Queter Wide Belvice Party trust	Yes WS-T umms-drs:ad.fr Yes WS-T omoubloso.fbla	Aab.com	Add Relying Party Trust
Relying Party Trusts		Yes WS-T cucpubhcsc.fhi	lab.com	Add Non-Claims-Aware Relying
Attribute Stores Add Kelyn	Chiere Average Backing Darty Tourt	Yes WS-T INab.com-500	D0F4107D76E57	View 🕨
p Authentication Policies Add Non	-Claims-Aware Kelying Party Trust			New Window from Here
View	·			Q Refresh
New Win	dow from Here			Help
Refresh				-
Help				

按一下**新增信賴方信任嚮導**。

\$	Add Relying Party Trust Wizard	×
Welcome		
Steps Velcome Select Data Source Configure Multi factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Welcome to the Add Relying Party Trust Wizard This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties oursume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions. The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party after you complete the wizard. State	s e-W tem i

按一下**Start**繼續。

選擇之前儲存的federationmedatada.xml元資料XML檔案,然後按一下**下一步**。

Select Data Source Steps Select an option that this wizard will use to obtain data about this relying party: • Welcome Import data about the relying party published online or on a local network • Select Data Source Import data about the relying party published online or on a local network • Configure Multifactor Authentication Now? Import data about the relying party published online or on a local network. • Choose Issuance Authorization Rules Federation metadata address (host name or URL): • Ready to Add Trust Example: fs.contoso.com or https://www.contoso.com/app • Finish Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. • Federation metadata file location: Federation metadata file location:	\$	Add Relying Party Trust Wizard
Steps Select an option that this wizard will use to obtain data about this relying party: • Welcome Import data about the relying party published online or on a local network • Select Data Source Import data about the relying party published online or on a local network • Configure Multifactor Authentication Now? Federation metadata online or on a local network. • Choose Issuance Authorization Rules Federation metadata address (host name or URL): • Ready to Add Trust Example: fs.contoso.com or https://www.contoso.com/app • Finish Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. • Federation metadata file location: Federation metadata file location:	Select Data Source	
Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.	 Steps Welcome Select Data Source Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish 	Select an option that this wizard will use to obtain data about this relying party: Import data about the relying party published online or on a local network Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata address (host name or URL): Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Pederation metadata file location: Import data about the relying party manually Use this option to manually input the necessary data about this relying party organization.

, 使用CUCM_Cluster_Wide_Reliking_Party_trust作為顯示名稱,然後按一下**下一步**。

\$	Add Relying Party Trust Wizard	x
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
 Welcome 	Display name:	
Select Data Source	CUCM_Cluster_Wide_Relying_Party_trust	
Specify Display Name	Notes:	
Configure Multi-factor Authentication Now?		^
 Choose Issuance Authorization Rules 		
 Ready to Add Trust 		
 Finish 		<u> </u>
	< Previous Next & Caribel	inde
	< Previous Next > (Carical	indo

\$	Add Relying Party Trust Wizard			
Steps	Configure multifactor authentication settings for this relying party trust. Multifactor authentication is required if there is a match for any of the specified requirements.			
Select Data Source	Multi-factor Authentication Global Settings			
Configure Multi-factor Authentication Now?	Requirements Users/Groups Not configured			
 Choose Issuance Authorization Rules 	Device Not configured Location Not configured			
 Ready to Add Trust Finish 				
	 I do not want to configure multi-factor authentication settings for this relying party trust at this time. Configure multi-factor authentication settings for this relying party trust. 			
	You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see <u>Configuring Authentication Policies</u> .			
	< Previous Next A ct Va Canbel in do			

選擇**允許所有使用者訪問此信賴方**,然後按一下**下一步**,如下圖所示。

\$	Add Relying Party Trust Wizard
Choose Issuance Autho	prization Rules
Steps	Issuance authorization rules determine whether a user is permitted to receive claims for the relying party.
 Welcome 	Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.
Select Data Source	 Permit all users to access this relying party
Specify Display Name	The issuance authorization rules will be configured to permit all users to access this relying party. The relying
Configure Multi-factor Authentication Now?	Denvial users access to this relying party
 Choose Issuance Authorization Rules 	The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.
 Ready to Add Trust 	
 Finish 	You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.
	< Previous Next & Ctive Cangel in do

檢視設定,然後按一下Next,如下圖所示。

\$	Add Relying Party Trust Wizard
Ready to Add Trust	
Steps Welcome Select Data Source Specify Display Name Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database. Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Not(<) Specify the monitoring settings for this relying party trust. Relying party's federation metadata URL:
	< Previous Affect & at Provide OVS

取消選中該框並按一下Close。

\$	Add Relying Party Trust Wizard	x
Finish		
Steps Velcome Select Data Source Specify Display Name Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in. Open the Edit Claim Rules dialog for this relying party trust when the wizard closes	
	Close]

使用滑鼠輔助按鍵選擇剛建立的**信賴方信任**和「**編輯宣告規則**」配置,如下圖所示。

\$		AD FS		
File Action View Winds ← ➡ 2 □ □ □	ow Help			
 AD FS Service Trust Relationships Claims Provider Trusts Relying Party Trusts Attribute Stores Authentication Policies 	Relying Party Trusts Display Name Device Registration Service CUCM_Cluster_Wide_Relwino_Party_trust CUC_Cluster_W Update from Fed ExpwyC Edit Claim Rules. Disable Properties Delete Help	Enabled Type Yes WS-Trust / SA Yes WS-Trust / SA leration Metadata	ML / WS-Federation ML / WS-Federation L / WS-Federation L / WS-Federation	Identifier um ms-drs:ad.fhlab.com cucpublicsc.fhlab.com fhlab.com fhlab.com-500D0F4107D76E57

按一下「Add Rule」,如下圖所示。

Name and the set of th	x
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rule	s
The following transform rules specify the claims that will be sent to the relying party.	
Order Rule Name Issued Claims	
	_
	ŧ
Add Rule Edit Rule Remove Rule	
OK Cancel A	pply

選擇Send LDAP Attributes as Claims,然後按一下Next。

%	Add Transform Claim Rule Wizard
Select Rule Template	
Steps	Select the template for the claim rule that you want to create from the following list. The description provides
Choose Rule Type	details about each claim rule template.
 Configure Claim Rule 	Claim rule template:
	Send LDAP Attributes as Claims 🗸
	Claim rule template description:
	Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.
	< Previous Next > Cancel

配置以下引數:

宣告規則名稱 : 名稱ID

屬性儲存:Active Directory(按兩下下拉選單箭頭)

LDAP屬性:SAM-Account-Name

傳出宣告型別:uid

按一下FINISH/OK繼續。

請注意,uid大小寫不小,並且不在下拉選單中。打出來。

	Edit R	ule - NamelD	x
You car which to issued f	n configure this rule to send the values of I o extract LDAP attributes. Specify how the rom the rule.	LDAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be	
Claim ru	le name:		_
Namell			
Rule te	mplate: Send LDAP Attributes as Claims		
Attribute	e store:		
Active	Directory	*	
Mappin	g of LDAP attributes to outgoing claim type	85:	
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)	
•	SAM-Account-Name V	uid	¥.
*	Ý	·	~
			_
Vew	Rule Language	OK Cancel	l

再次按一下Add Rule以新增其他規則。

💱 Edit Claim	Rules for CUCM_Clust	ter_Wide_Rel	ying_Party	- 🗆 X
Issuance Transf	orm Rules Issuance Authoriz	ation Rules Dele	gation Authorizati	on Rules
The following	transform rules specify the clair	ns that will be sen	t to the relying par	ty.
Order Rule	e Name	Issued	Claims	
1 Nan	helD	uid		
				T
				+
Add Rule	Edit Rule Remove	Rule		
L				
		ОК	Cancel	Apply

Add Transform Claim Rule Wizard
Select the template for the claim rule that you want to create from the following list. The description provides
details about each claim rule template.
Claim rule template:
Send Claims Using a Custom Rule 🗸
Claim rule template description:
Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include: 9 Sending claims from a SQL attribute store 9 Sending claims from a custom attribute store using a custom LDAP fitter 9 Sending claims only when 2 or more incoming claims are present 9 Sending claims only when an incoming claim value matches a complex pattern 9 Sending claims for use only in later rules 10 Creating claims for use only in later rules 11 OF Previous 12 Previous 13 Previous 14 Previo

建立名為Cluster_Side_Claim_Rule的自定義規則。

從此處直接在規則視窗中複製並貼上此文本。有時,如果在文本編輯器中編輯引號,則會發生更改 ,這會導致測試SSO時規則失敗:

c:[Type ==

"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
<pre>=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",</pre>
<pre>Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,</pre>
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =</pre>
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
= "http:// <adfs fqdn="">/adfs/com/adfs/services/trust",</adfs>
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =</pre>
" <cucm fqdn="" pub="">");</cucm>
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
<pre>=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",</pre>
<pre>Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,</pre>
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =</pre>
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =</pre>
" <u>http://AD.fhlab.com/adfs/services/trust</u> ",
<pre>Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamegualifier"] =</pre>
"cmpubhcsc.fhlab.com");
按一下Finish以繼續。

\$ 1	Add Transform Claim Rule Wizard
Configure Rule	
Steps Choose Rule Type Configure Claim Rule	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language. Claim rule name: Cluster_Side_Claim_Rule Rule template: Send Claims Using a Custom Rule Custom rule: c: [Type ==
	<pre>"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount name"] "> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format "] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequ alifier"] = "http://AD.fhlab.com/adfs/services/trust", Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spname qualifier"] = "cmpubhcsc.fhlab.com");</pre>
	< Previous Finish Cancel

, 現在,您應該在ADFS上定義兩個規則。按一下**Apply**和**OK**關閉規則視窗。

🂱 Edit C	laim Rules f	or CUCM_Clus	ter_Wide	e_Relying_Party	-		x
Issuance 1	Transform Rules	Issuance Authoriz	ration Rules	Delegation Authoriza	tion Ru	les	
The folk	owing transform n	ules specify the cla	ins that will	be sent to the relying pa	arty.		
Order	Rule Name			Issued Claims			
1	NameID			uid			
2	Cluster_Side_C	laim_Rule		<see claim="" rule=""></see>			
Add F	Rule	Rule	e Rule			•]
			0	K Cancel		Apply	

CUCM現在已成功新增為ADFS的受信任信賴方。

9		Service	5				x
File Action View	Help						
💠 🔿 📅 🔯 🖉	à 🗟 📘 🕨 🖬 🕪						
Services (Local)	Services (Local)						
	Active Directory Federation Services	Name	Description Creates, manages, and removes	Status Running	Startup Type Automatic	Log On As Local System	^
	Stop the service Restart the service	Active Directory Domain Services	AD DS Domain Controller servic Enables Active Directory Federa	Running	Automatic Automatic (Delayed Start)	FHLAB\administra	ator
	Duraities	G Active Directory Web Services	This service provides a Web Ser Gets apps ready for use the first	Running	Automatic Manual	Local System Local System	
	Enables Active Directory Federation Services to issue security tokens.	Application Experience Application Host Helper Service	Processes application compatib Provides administrative services	Running	Manual (Trigger Start) Automatic Manual (Trigger Start)	Local System Local System	
		Application Identity	Facilitates the running of intera Provides support for 3rd party p		Manual (Trigger Start) Manual (Trigger Start) Manual	Local System	
		Application Management AppXSVC)	Processes installation, removal, Provides infrastructure support		Manual Manual	Local System	
		ASP.NET State Service	Provides support for out-of-pro Transfers files in the backgroun		Manual Manual	Network Service	
		Background Tasks Infrastructure Service	Windows infrastructure service The Base Filtering Engine (BFE) i	Running Running	Automatic	Local System	
		Certificate Propagation	Copies user certificates and roo The CNG key isolation service is	Running	Manual Manual (Tripper Start)	Local System	
		COM+ Event System	Supports System Event Notifica Manages the configuration and	Running	Automatic	Local Service	
		Computer Browser	Maintains an updated list of co		Disabled	Local System	~
		3					>
	Extended Standard			A	Activate Windows		

繼續之前,請重新啟動ADFS服務。導航到**開始選單>管理工具>服務**。

IDP後設資料

您需要向CUCM提供有關我們的IdP的資訊。使用XML後設資料交換此資訊。確保在安裝ADFS的伺服器上執行此步驟。

Firefox 🔽	
▲ Untrusted Connection × 🥹 Mozilla Firefox Start Page × +	
(♦) 🕲 >s://ad0a.identity 💫.us/FederationMetadata/2007-06/FederationMetadata 🏠 ⊽ 😋 😫 ▼ Google 🛛 🔎	↓ ∧
Most Visited Getting Started Suggested Sites Web Slice Gallery	
Opening FederationMetadata.xml	-
You have chosen to open: PederationMetadata.xml dentification to prove that you ed.	
which is: XML Document from: https://ad0a.identitylab.us What should Firefox do with this file? Qpen with Internet Explorer (default) Save File Do this gutomatically for files like this from now on. OK Cancel of this site's identification. Even ampering with your	
Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.	
	•

首先,您需要使用Firefox瀏覽器連線到ADFS(IdP)以下載XML後設資料。開啟瀏覽器到 https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml,並將後設資料儲存 到本地資料夾。

現在,導航至CUCM配置至system Menu > SAML Single Sign-On選單。

	🗱 Find and List Cisco U	Unified CM × +	-		×
¢) → ୯ 🏠 🛛 🖸	🖸 🖴 😂 https://cmpubhcsc.fhlab.com:8443/ccmadmin/ccmGroup 🚥 😒 🟠	lin C) ®	-9
	Server Cisco Unified CM Cisco Unified CM Group Presence Redundancy Groups Phone NTP Reference Date/Time Group	Administration Navigation Cisco Unified CM Administration nunications Solutions farfar Search Documentation ces Advanced Features Device Application User Management Buk Adm s Ups	ition About the state of the st	v at I L • Help	Go ogout
	BLF Presence Group	anager Group			
	Region Information Device Pool	nager where Name begins with v Find C	lear Filter	4	-
	Device Mobility	active query. Please enter your search criteria using the options above.			
	DHCP	•			
	LDAP	•			
	SAML Single Sign-On				
	Cross-Origin Resource Sharing (CORS)	ng l			
	Location Info	•			
	MLPP	•			
	Physical Location				
	SRST				
	Enterprise Parameters				
	Enterprise Phone Configuration	n			
	Service Parameters				
	Security	•			
	Application Server				
	Licensing	•			
	Geolocation Configuration				
	Geolocation Filter				
	E911 Messages				

https://cmaulelecenters/and/indexianCondo 切換回CUCM管理並選擇SYSTEM > SAML Single Sign-On。

Firefox *							- 🗆 ×
🕮 Find and List User	s	× SAML Single Sign-Or	×	Find and List LDAP Directories	× +		
+ A https://cu	cm0a/comadmin/sami5i	ingleSignOn.do		<u>⇔</u>	C Scogle	۶ 🖸 -	+ +
cisco For	Cisco Unified	CM Administrations	on		Navigation Cisco Unifie admin Search Docume	d CM Administration entation About	Go Logout
System - Cal Ro	uting 👻 Media Reso	surces + Advanced Features	- Device - Application	• User Management • B	ulk Administration 👻 Help 👻		
SAML Single Si	jn-On						
SAML S	ISO 🔥 Update ki	P Metadata File 👔 Export A	I Metodoto 🧳 Fix All Dise	abled Servers			
- Status							
() SAML SSO	disabled						
SAML Single S	ign-On (1 - 1 c	of 1)				Rows per Page	50 💌
Server Name	SSO Status Disabled	Re-Import Metadata	Last Metadata Impo	rt Export Metadata	Last Metadata Export	SSO Test	
Cocinida	Libbled		Never		Never	Rur	Test

選擇**啟用SAML SSO**。

按一下「Continue」以確認警告。

😨 Reset Warning - Mozilla Firefox 📃 🗖	×
Https://cucmDa/ccmadmin/genericDialogWindow.do?windowtitlekey=genericdialogwindow.windowtitle.ssoenabler	2
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. Continue Cancel	

下圖所示。

Find and List Users X Attraction Status Attraction Status Status Status Attraction Identity Provider metadata trust file to cluster servers			
A https://cuanDa/comedmin/santSingleSignOnConfigurationWiteard.do Cisco Unified CM Administration For Cisco Unified Communications Solutions System * Call Routing * Media Resources * Advanced Features * Device * Application * User Management * Bulk Administration * Help * SAML Single Sign=On Configuration Status (i) Ready to import Identity Provider metadata trust file to cluster servers			
Cisco Unified CM Administration Navigation Cisco Unified CM Administration For Cisco Unified Communications Solutions admin Search Documentation System + Cal Routing + Media Resources + Advanced Features + Device + Application + User Management + Buk Administration + Hep + SAML Single Sign-On Configuration Image: Status Image: Ready to import Identity Provider metadata trust file to cluster servers	•	÷	ft
System Cal Routing Media Resources Advanced Features Device Application User Management Buk Administration Help SAML Single Sign-On Configuration Next Status Status Ready to import Identity Provider metadata trust file to cluster servers	istration About	Log	Go gout
SAML Single Sign-On Configuration Next Status Ready to import Identity Provider metadata trust file to cluster servers			
Status Status Image: Ready to import Identity Provider metadata trust file to cluster servers			
Status			
Identity Provider(IdP) Metadata Trust File To configure the trust relationship between the IdP and your servers, you must first obtain trust metadata from your IdP and import it to your servers. You manually obtain the file from the IdP and upload it here. IdP Metadata File Browse. No file selected. Initiate the Metadata In No file selected. This action must be successful for at least the Publisher before moving on to the next task in this wizard. Import IdP Metadata Next	will need t	20	

選擇XML檔案,然後按一下**開啟**,以便從「收藏夾」下的「下載」中將其上載到CUCM。

💽 File Upload					X
G · Adminis	strator - Downloads				👻 🚺 Search Downloads 🗾
Organize • New folder					j≡ • 🗊 0
* Favortes	Name +	Date modified	Туре	Size	
E Desktop	AdfsSetup	2013/09/09 06:10 PM	Application	24 518 KB	
B Downloads	🖆 FederationMetadata	2013/09/12 02:01 PM	XML Document	32 KB	
21 Recent Places	Spicpick_inst	2013/09/12 11:09 AM	Application	11 129 88	
Documents Documents Music Pictures Videos Computer Network					
Fil	e game: FederationMetadata				All Files

上傳後,點選Import IdP Metadata將IdP資訊匯入CUCM。確認匯入成功,然後按一下「下一步」繼續。

SAML Single Sign-On Configuration - Windows Internet Explorer	
🔄 💿 💌 🎯 https://10.1.1.100/ccmadmin/s 🔎 💌 😰 Ce 🖻 🖅 🧭 SAML Single Sign-On Configu 🗙	☆☆ @
Cisco Unified CM Administration Navigation Cisco Unified CM Administration	Go About Logout
System - Call Routing - Media Resources - Advanced Features - Device - Application - User Management -	Bulk Administration 👻
Help 👻	
SAML Single Sign-On Configuration	
Next	
Status	
Import succeeded for all servers	
Identity Provider(IdP) Metadata Trust File	
To configure the trust relationship between the IdP and your servers, you must first obtain trust metadata from your I to your servers. You will need to manually obtain the file from the IdP and upload it here.	dP and import it
IdP Metadata File C:\Users\bbanks\Downloads\FederationMetadata.xml Browse	
- Initiate the Metadata Import	
This action must be successful for at least the Publisher before moving on to the next task in this wizard.	
Import IoP Metadata V Import succeeded for all servers	
Next Cancel	
選擇屬於「標準CCM超級使用者」的使用者,然後按一下「運行SSO測試」。	
🗉 SAML Single Sign-On Configuration - Mozilla Firefox	- 🗆 ×
☑	⊠ ☆ ≡
SAML Single Sign-On Configuration	
- Test SSO Setup	
This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is succ	test can be run on essful.
1)Pick a valid username to use for this test	
You must already know the password for the selected username. This user must have administrator rights and also exist in the IdP.	
Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in ad lockout.	Iministrator
Valid administrator Usernames	
2)Launch SSO test page	
Run SSO Test	

Cancel

出現使用者身份驗證對話方塊時,使用相應的使用者名稱和密碼登入。

ۏ Sign	n - Mozilla Firefox	_		\times
0	https://ad. fhlab.com /adfs/ls/?SAMLRequest=nZJPTwIxEMXvflpN77Cl	Ai4N	SO •••	≡
				^
	FS			
	Sign in with your organizational account			
	farfar@fhlab.com			
	Turtu emusiconi			
	•••••			
	Sign in			~
	FS Sign in with your organizational account farfar@fhlab.com ••••••			

如果所有配置都正確,您應該會看到一條消息,指示SSO測試成功!

## SAMLS	ngle Sign-On X +			×
😆 SAML S	ngle Sign-On Configuration - Mozilla Finefox	-		×
0 🔒 =	https://cmpubhcsc.fhlab.com:8443/ccmadmin/sam/SingleSignOnConfigurationWizard3.do?testSt	••• (9 ¢	≡
SAML Sing	le Sign-On Configuration			
Status				
🗸 550	Metadata Test Successful			
Close				
	😻 Test SAML - Mozilla Firefox — 🗆 🗙	1		
	① ▲ \$\pm https://cmpubhcsc.fhlab.com:8443/ssosp/pages/TestSSO.jsp?ssopage=tr ···· Ξ			
	SSO Test Succeeded!			
	Congratulations on a successful SAML SSO configuration test. Please			
	close this window.			
	Close			
		1		

按一下「關閉」和「完成」繼續。

我們現在已成功完成使用ADFS在CUCM上啟用SSO的基本配置任務。

在CUC上配置SSO

在Unity Connection中啟用SSO的過程相同。

LDAP與CUC整合。



配置LDAP身份驗證。

(←) → C @	🔞 🖨 😂 https://cucpubhcsc.fhlab.com/cuadmin/home.do	⊡☆ ॥\ ⊡ © ≡
Cisco Unity Con For Cisco Unified Comm	nection Administration nunications Solutions	Navigation Cisco Unity Connection Administration V Go farfar Search Documentation About Sign Out
Cisco Unity Connection	LDAP Authentication	LDAP Authentication
Video Services Accounts Status Dial Plan Partitions Search Spaces System Settings General Configuration Clutter Authentication Rules Restriction Tables Schedules Holiday Schedules Global Nicknames Subject Line Formats	▲ LDAP Authentication Refresh Help Save Status Uae LDAP Authentication for End Users LDAP Authentication for End Users LDAP Manager Distinguished Name* [fhilab\Administrator LDAP Password* Confirm Password* LDAP User Search Base*	
- Attachment Descriptions - Enterprise Parameters - Service Parameters - Plugins - Fax Server - LDAP - LDAP Setup - LDAP Directory Configuration - LDAP Authentication	LDAP Server Information Host Name or IP Address for Server* 10.89.228.226 Add Another Redundant LDAP Server Save Fields marked with an asterisk (*) are required.	LDAP Port* Use TLS

從LDAP匯入將分配語音郵件的使用者以及將用於測試SSO的使用者。

Cisco Unity Connection	Import Users				Import U					
E Users ^	Import Users Refresh Help									
Users										
Import Users	Status	Status								
Synch Users	0									
Class of Service	Found 1 LDAP User(s)									
Class of Service	End									
Class of Service Membership	Find									
Templates	Find End Users In LDAP Directory									
User Templates	Where Alias ~ Begins Wi	th v	End							
Call Handler Templates										
Contact Templates	- Import With									
Notification Templates	Based on Template Jusics mailture	template								
Contacts	Voicemailuse	template V								
Contacts										
Distribution Lists	Directory Search Results									
System Distribution Lists	Import Selected Import All	25 Pours Par Page								
Call Management	Import Delected Import Par	ab o Rons Fer Feye								
System Call Handlers	Alias A	First Name	Last Name	Phone Number	Extension					
Directory Handlers	hugohugo	hugo	hugo	1002	1002					
Interview Handlers										
Custom Recordings	Import Selected Import All									

導覽至Users > Edit > Roles,如下圖所示。

Cisco Unity Connection	e 10 a		
Users	Edit U	iser Basics (hugohugo)	
Users	User	Edit Refresh Help	
-Import Users		User Basics	h.
Synch Users	Sav		
E Class of Service	_ Sta	Password Settings	
Class of Service		Change Password	
Class of Service Membership		Roles	ectory
liempiates		Massage Waiting Indicators	
Coll Handlas Tamalatas	Nam	e Message waiting Indicators	
Call Handler Templates	Alias	Transfer Rules	
Contact Templates	First I	Message Settings	
Notification Templates	Lack I	the Collection of	
□ Contacts	Last	Caller Input	
Contacts	Displa	Mailbox	
Distribution Lists	SMTP	Phone Menu	@cucpubhcsc.fhlab.com
System Distribution Lists	Initial	S Disuback Message Settings	
Call Management	ATTICION OF	Playback Message Settings	
System Call Handlers	Title	Send Message Settings	
Directory Handlers	Emple	Message Actions	
-Interview Handlers		Constitution of the second sec	
Custom Recordings	LDAP	Greetings	
Call Routing		Post Greeting Recording	
E Message Storage	In	Notification Devices	
Mailhoy Stores	I O D	0	

為測試使用者分配系統管理員角色。

Cisco Unity Connection	Edit Roles	Search Users + Edit User Basics (hugohugo) + Edit Role
E Users	User Edit Refresh Help	
Users		
-Import Users	Save	
Synch Users	Refer	
Class of Service	Koles	
Class of Service	Assigned Roles	
Class of Service Membership		
Templates		
User Templates	×	
Call Handler Templates	A ¥	
Contact Templates	Available Roles	
Notification Templates	Remote Administrator	
E Contacts	System Administrator	
Contacts	Tenant Administrator	
Distribution Lists	User Administrator	
System Distribution Lists		
Call Management	Save	

CUC後設資料

現在,您應該已經下載了CUC後設資料,為CUC建立了ReliingPartyTrust並上載了CUC後設資料 ,並在ADFS 3.0上建立了規則I AD FS



🔹 SAML Single Sign on Configuration - Mozilla Firefox	-		\times
🛛 🖴 😁 https://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?serverName=	···· (פ לי	≡
SAML Single Sign on Configuration SAML Single	Sign o	n Config	guration
SAML Single Sign on Configuration Refresh Help			
Test SSO Setup This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. Thi on any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is 1)Pick a valid username to use for this test You must already know the password for the selected username. This user must have administrator rights and also exist in the IdP. Image: Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in a lockout. Valid administrator Usernames farfar hugohugo 2)Launch SSO test page Run SSO Test	s test o succes	an be risful.	un

🛑 SAML Single	Sign on Configuration - Mozilla Firefox	-		\times				- a	x v
🖲 🖴 🖬	ttps://cucpubhcsc. fhlab.com /cuadmin/samlSingleSignOnConfigurationWizard3.do?testStatus=1	(9 ¢	≡			· 🖂 🗘		\$ ≡
SAML Single S SAML Single Si	sign on Configuration SAML Single gn on Configuration Refresh Help	Sign o	in Config	puration		Navigat farta	ion Cisco Unity Connection A Search Documentation	Administration	Go Sign Out
Status	adata Test Successful							SAML Sin	gle Sign o
Close	🍟 Test SAML - Mozilla Firefox 🦳 🗆	×							
	© ≜ thttps://cucpubhcscfhlab.com/ssosp/pages/TestSSO.jsp?ssopage=true ···· SSO Test Succeeded!	Ξ			ers				
			port data	Last Metadata Export	SSO Te	st	50 0		
	Congratulations on a successful SAML SSO configuration test. Pleas close this window.	se			File	April 28, 2020 5:54:01 PM PDT	Passed - May 24, 2020 3:17:04 PM PDT	Run SSO	Test
					File	April 28, 2020 5:54:00 PM PDT	Passed - April 29, 2020 11:05:37 AM PDT	Run SSO	Test
	Close				Serven	1			
	1								

在Expressway上配置SSO

將後設資料匯入到Expressway C

開啟瀏覽器到https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml,並將後設資料儲存到本地資料夾

上傳到Configuration > Unified Communications > IDP。

從Expressway C匯出後設資料

轉到配置 — >統一通訊 — > IDP->匯出SAML資料

群集模式使用包含在SAML中的自簽名證書(壽命長)

用於對SAML請求進行簽名的後設資料

- 在群集範圍模式下,要下載單個群集範圍後設資料檔案,請按一下「下載」
- 在每對等體模式下,要下載單個對等體的後設資料檔案,請按一下該對等體旁邊的Download。
 要全部匯出到.zip檔案,請按一下「全部下載」。

為Cisco Expressway-E新增信賴方信任

首先,為Expressway-Es建立信賴方信任,然後新增宣告規則以傳送標識作為UID屬性。

🗢 🌩 🖄 📰 📓 🗊						
AD FS	Relying Party Trusts					Actions
A UPS Endpoints Certificates Claim Descriptions Claims Provider Trusts Relying Party Trusts Attribute Stores Authentication Policies		Enabled Type Service Yes WS-Trust / SA Pelying_Party_trust Yes WS-Trust / SA Pelying_Party_trust Yes WS-Trust / SA Yes WS-Trust / SA N Rules for ExpwyyC It Rules for ExpwyyC It Rules Delegation Authorization Rules Issued Claims		/ WS-Federation / WS-Federatio	Identifier um ms-dm ad fhilab.com cwpubhcsc fhilab.com cwpubhcsc fhilab.com fhilab.com-500D0F4107D76E57 Edit Ru re this rule to send the values of LD LDAP attributes. Specify how the a de	Actions Relying Party Trusts Add Relying Party Trust Add Non-Claims-Aware Relying Part View Image: Select an attribute store from tributes will map to the outgoing claim types that will be
	1 NamelD uid		Ŷ	Rule template: Si Attribute store: Active Directory Mapping of LDAI	end LDAP Attributes as Claims P attributes to outgoing claim types Natibute (Select or type to	
	Add Rule Edt Rule Remove Rule		+	sAM-Ac	re) count-Name v	Activate Windows.

使用刷新登入的OAuth

在Cisco CUCM Enterprise Parameters中,啟用Verify OAuth with Refresh login flow引數。轉到 **Cisco Unified CM管理>企業引數> SSO和OAuth配置**。

SSO and OAuth Configuration		
OAuth Token Expiry Timer (minutes) *	60	60
OAuth Refresh Token Expiry Timer (days) *	60	60
Redirect URIs for Third Party SSO Client		
SSO Login Behavior for iOS *	Use embedded browser (WebView)	Use embedded browser (WebView)
OAuth with Refresh Login Flow *	Enabled V	Disabled
Use SSO for RTMT *	True V	True

驗證路徑



•如果身份驗證路徑設定為「SAML SSO身份驗證」,則只有使用啟用了SSO的Unified CM集群 的Jabber客戶端才能在此Expressway上使用MRA。這是僅SSO配置。

- •對於所有IP電話、所有網真終端和駐留在未配置SSO的Unified CM集群上的任何Jabber客戶端 ,Expressway MRA支援都需要身份驗證路徑以包括UCM/LDAP身份驗證。
- 如果有一個或多個Unified CM集群支援Jabber SSO,請選擇「SAML SSO和UCM/LDAP」以允許SSO和基本身份驗證。

SSO架構

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程式後無縫訪問一 組已定義的思科合作應用程式。SAML SSO使用SAML 2.0協定為思科合作解決方案提供跨域和跨產 品單點登入。

本地登入流程



Figure :SAML Single sign SSO Call Flow for Collaboration Servers

MRA登入流



OAuth

OAuth是一個支援授權的標準。使用者必須經過驗證才能獲得授權。授權碼授權流程為客戶端提供 獲取訪問權杖和刷新權杖以訪問資源(Unified CM、IM&P、Unity和Expressway服務)的方法。此 流程也基於重定向,因此需要客戶端能夠與使用者控制的HTTP使用者代理(Web瀏覽器)互動。 客戶端將使用HTTPS向授權伺服器發出初始請求。OAuth伺服器將使用者重定向到身份驗證服務。 如果啟用SAML SSO,則此操作可能在Unified CM或外部IdP上運行。根據所使用的認證方法,網頁 檢視可能呈現給終端使用者以認證其自身。(Kerberos驗證是不顯示網頁的範例。)與隱式授予流 程不同,成功的身份驗證代碼授予流程將導致OAuth伺服器向Web瀏覽器發出「授權代碼」。這是 一個一次性使用的短暫唯一代碼,然後從Web瀏覽器傳回客戶端。使用者端將這個「授權碼」與預 先共用密碼一起提供到授權伺服器,並交換接收「存取權杖」和「刷新權杖」。在此步驟中使用的 客戶端密碼使授權服務可以將使用限製為僅註冊和經過身份驗證的客戶端。令牌用於以下用途:

存取/刷新權杖

訪問令牌:此令牌由授權伺服器頒發。當客戶端需要訪問資源伺服器上的受保護資源時,向資源伺 服器呈現令牌。資源伺服器能夠驗證該令牌並信任使用該令牌的連線。(思科訪問令牌的生存時間 預設為60分鐘)

刷新令牌:授權伺服器再次發出此令牌。當訪問令牌已過期或即將過期時,客戶端將此令牌與客戶 端金鑰一起提供給授權伺服器。如果刷新令牌仍然有效,則授權伺服器將頒發新的訪問令牌,而無 需其他身份驗證。(思科刷新令牌的生存期預設為60天)。如果刷新令牌已過期,則必須啟動新的 完整OAuth授權代碼授予流程以獲取新令牌。

OAuth授權代碼授權流程更好

在隱式授予流程中,訪問令牌通過HTTP使用者代理(瀏覽器)傳遞到Jabber客戶端。 在授權碼授 權流程中,訪問令牌直接在授權伺服器和Jabber客戶端之間交換。使用時間限制的唯一授權碼從授 權伺服器請求令牌。這種直接交換訪問令牌更加安全並且減少了風險。

OAuth授權代碼授予流程支援使用刷新令牌。這可以為終端使用者提供更好的體驗,因為他們不需 要頻繁地重新進行身份驗證(預設情況下為60天)

配置Kerberos

選擇Windows身份驗證

Internet資訊服務(IIS)管理器>站點>預設網站>身份驗證> Windows身份驗證>高級設定。

- 1. 取消選中Enable Kernel-mode authentication。
- 2. 確保已關閉擴展保護。



ADFS同時支援Kerberos NTLM

確保AD FS版本3.0同時支援Kerberos協定和NT LAN Manager(NTLM)協定,因為所有非 Windows客戶端都不能使用Kerberos並依賴NTLM。

在右窗格中,選擇Providers(提供程式),並確保Negotiate and NTLM出現在Enabled Providers(已啟用提供程式)下:

Vi Internet Information Services (IIS) Manager							
€) AD → Sites → Default Web Sit	e 🕨				📅 🖂 🏠 🔞 •		
File View Help							
Connections				Alerts			
🔍 - 🔚 🖄 😥	Authentication			A Click here	to learn how to		
Start Page	Group by: No Grouping			configure Protection	Extended		
AD (FHLAB\administrator)	Name	Status	Response Type	Actions			
⊿ - i Sites	Anonymous Authentication	Enabled		Disable	_		
Default Web Site	ASP.NET Impersonation	Disabled	HTTP 302 Login/Redir	Disable	C-11/2-12		
	Windows Authentication	Enabled	HTTP 401 Challenge	Providers	Settings		
			Drouidare	? X			
			Providers				
	Enable	d Providers:					
	Negot	iate		Move Up			
	NTLM						
				Move Down			
				Remove			
	<						
	Select	a provider from the it to the enabled pro	list of available providers and oviders.	click Add			
Configuration: 'localhort' applicationHort configclos	tion nath-"Default W				61.		
configuration: focarios: application host config, vioca	Availal	ble Providers:			10.000		
			~	Adactiva	ite N2 iR2ows		
				Go to Sy	ystem in Control Pa		
			OK	Cancel	Windows Se		

配置Microsoft Internet Explorer

確保選中Internet Explorer > Advanced > Enable Integrated Windows Authentication。

Internet Options							
Genera	Security	Privacy	Content	Connec	tions Prog	grams	Advanced
Settings							
 Do not submit unknown addresses to your auto-search pro Just display the results in the main window Security Allow active content from CDs to run on My Computer* Allow active content to run in files on My Computer* Allow software to run or install even if the signature is invi Check for publisher's certificate revocation Check for server certificate revocation* Check for signatures on downloaded programs Do not save encrypted pages to disk Empty Temporary Internet Files folder when browser is ck Enable DOM Storage Enable Integrated Windows Authentication* 							
•	Enable memory protection to help mitigate online attacks*						
*Takes effect after you restart Internet Explorer							
Reset Internet Explorer settings Resets Internet Explorer's settings to their default Condition. You should only use this if your browser is in an unusable state.							
			OK		Cancel		Apply

在Security > Intranet zones > Sites下新增ADFS URL