# 使用ADFS 3.0在Cisco Unified Communications Manager上配置SAML SSO

# 目录

简介 <u>先决条件</u> 要求 使用的组件 配置预检查 A记录 指针(PTR)记录 Jabber发现服务需要有SRV记录 ADFS3初始配置 使用ADFS在CUCM上配置SSO LDAP配置 CUCM元数据 配置ADFS信赖方 IDP元数据 在CUC上配置SSO CUC元数据 在Expressway上配置SSO 将元数据导入Expressway C 从Expressway C导出元数据 为Cisco Expressway-E添加信赖方信任 OAuth与刷新登录 身份验证路径 SSO架构 本地登录流 MRA登录流 OAuth 访问/刷新令牌 OAuth授权代码授予流程更好 配置Kerberos 选择Windows身份验证 ADFS支持两个Kerberos NTLM 配置Microsoft Internet Explorer 在"安全">"内部网区域">"站点"下添加ADFS URL 将CUCM、IMP和Unity主机名添加到Security > Trusted Sites 用户身份验证 Jabber在SSO中登录 故障排除 Internet Explorer(IE)

<u>添加到IE的站点</u> <u>不同步问题</u> <u>撤销令牌</u> <u>引导程序文件</u> SSO失败,应为MSIS7066

# 简介

本文档介绍在思科统一通信管理(CUCM)、思科统一连接(CUC)、Expressway产品上使用Windows 2012 R2配置使用Active Directory联合身份验证服务(ADFS 3.0)的单点登录的步骤。配置 Kerberos的步骤也包含在本文档中。

# 先决条件

## 要求

思科建议您了解单点登录(SSO)和Windows产品。

## 使用的组件

本文档中的信息基于以下软件和硬件版本:

- CUCM 11.5
- CUC 11.5
- Expressway 12
- Windows 2012 R2 Server具有以下角色:
  - Active Directory证书服务
  - Active Directory联合身份验证服务

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

# 配置预检查

在安装ADFS3之前,环境中需要已存在以下服务器角色:

·域控制器和DNS

·所有服务器都必须作为记录和指针记录一起添加(一种将IP地址解析为域或主机名的DNS记录)

## A记录

在fhlab.com中。hosts cmpubhcsc、cmsubhcsc、cucpubhcsc、cucsubhcsc、exwyc、expwye、 impubhcsc和imsubhcsc已添加。



## 指针(PTR)记录

A DNS	Name	Туре	Data	Timestamp
AD 🗎 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
þ 🛄 _tcp	10.89.228.148	Pointer (PTR)	imppubhcsc.fhlab.com.	static
▷udp	10.89.228.150	Pointer (PTR)	impsubhcsc.fhlab.com.	static
DomainUnsZones	10.89.228.151	Pointer (PTR)	cucpubhcsc.fhlab.com.	static
	10.89.228.153	Pointer (PTR)	cucsubhcsc.fhlab.com.	static
psues	10.89.228.154	Pointer (PTR)	win10.fhlab.com.	5/12/2020 10:00:00 AM
A C Reverse Lookup Zones	10.89.228.226	Pointer (PTR)	ad.fhlab.com.	5/12/2020 11:00:00 AM
228.89.10.in-addr.arp	10.89.228.227	Pointer (PTR)	win10ext.fhlab.com.	5/7/2020 4:00:00 PM

Jabber发现服务需要有SRV记录

& DNS	Name	Туре	Data	Т	imestamp	
A D	_cisco-uds	Service Location (SRV)	[0][0][8443] cmsubhcsc.fhla	b.com. s	tatic	
a 🔛 Forward Lookup Zones	_cisco-uds	Service Location (SRV)	[0][0][8443] cmpubhcsc.fhla	ab.com. st	tatic	
[] _msdcs.fhlab.com	cuplogin	Service Location (SRV)	[0][0][8443] impsubhcsc.fhl	ab.com. st	tatic	
⊿ 👸 fhlab.com	cuplogin	Service Location (SRV)	[0][0][8443] imppubhcsc.fhl	lab.com. st	tatic	
▷ []] _msdcs	gc	Service Location (SRV)	[0][100][3268] ad.fhlab.com	. 5	/12/2020 10:00:00 AM	
psites	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	
þ og udp	[]_ldap	Service Location (SRV)	[0][100][389] ad.fhlab.com		12/2020 10 02 00 111	
DomainDnsZones					_cisco-uds Properti	es ? X
a ForestUnszones				Control I contine	(20)	
psites				Service Location	(SRV) Security	
A Beverse Lookup Zones				Domain:	fhlab.com	
228.89.10.in-addr.arp						
Trust Points				Service:	_cisco-uds	~
Conditional Forwarders				Bestaval		
D Global Logs				Protocol.	_lcb	¥
_				Priority:	0	
					0	
				Weight:	0	
				Port number:	8443	
				Hart offering this		
				Post oilening the	s service.	
				chipubricsc ma	so.com.	

#### •根CA(假设证书将由企业CA签名)

需要根据Web服务器证书模板创建证书模板,前者是重复的、重命名的,在"扩展"(Extensions)选项 卡上,"应用策略"(Application Policies)被修改,添加客户端身份验证应用策略(Client Authentication Application Policy)。在实验室环境中,内部CA还可以签署Expressway E证书签名请求(CSR),在 签署所有内部证书(CUCM、CUC、IMP和Expressway核心)时,需要使用此模板。



#### 创建的模板需要发布才能签署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证书Web上,选择之前创建的模板。

#### 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多服务器CSR必须由CA生成和签名。证书用途必须是tomcat。

enerate Certificate Signing F	Request	
Generate 🖳 Close		
Status		
🔥 Warning: Generating a r	new CSR for a specific certificate type will overwrite	he existing CSR for that type
Cenerate Certificate Signing	Request	
Certificate Purpose**	tomcat	1
Distribution*	Multi-server(SAN)	
Common Name*	cmpublicsc-ms.fblab.com	
Subject Alternate Names (S	ANs)	
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* Hash Alcorithm*	RSA 2048	Add

Generate Close

CA根证书必须上传到Tomcat Trust,签名证书必须上传到Tomcat。

Show + Sempa + Security + Software Upgrades + Services + Help + Certificate List	Cisco Unified Operating System Administration For Cisco Unified Communications Solutions						opation Cisco Unified OS Administration sadmin Search Documentation About	Go Logout
Certificate List  Certificate  Certificate Certificate  Certificate	Show . Settings .	Security · Software Upgrades ·	· Services · Help ·					
Generate Self-signed     Dybed Centricate/Centricate CBR      Centrificate List     (1 - 7 of 7)     Rows per Page 50     Centrificate List     (1 - 6 of 6)     Rows per Page 50     Centrificate List     (1 - 6 of 6)     Rows per Page 50     Centrificate List     (1 - 6 of 6)     Rows per Page 50     Centrificate List     (1 - 6 of 6)     Rows per Page 50     Centrificate List     (2 - 6 of 6)     Rows per Page 50     Centrificate List     (2 - 6 of 6)     Rows per Page 50     Centrificate List     (2 - 6 of 6)     Rows per Page 50     Centrificate List     (2 - 6 of 6)     Rows per Page 50     Centrificate List     (2 - 6 of 6)     Rows per Page 50     Centrificate List     (2 - 6 of 6)     Rows per Page 50     Centrificate List     Rows per Page 50     Centrificate List     Rows per Page 50     Centrificate List     Rows per P	Certificate List							
Certificate List (1 - 7 of 7)     Rows per Page 50      Find Certificate List (1 - 7 of 7)     Rows per Page 50      Find Certificate List where Certificate      Legina with      torncat     compublescents     Comman Name     Type     Yes	Generate Self.siz	med 🕰 Upload Certificate/Certificat	te chain 👔 Generate CSR					
Image: Precords found       Rows per Page 50 ~         Find Certificate List where Certificate ~ begins with ~ tomcat       Find       Clear Filter       Image: Proceeding	0		×0					
Rows per Page 50 ~         Certificate List (1 - 7 of 7)       Rows per Page 50 ~         Find Certificate List where Certificate        begins with        tomcat       Find       Clear Filter       Image: Set Filter	7 records four	nd						í
Rows per Page 50 ~         Find Certificate List (1 - 7 of 7)       Rows per Page 50 ~         Find Certificate List where Certificate ~ begins with ~ tomcat       Find Clear Filter *       Image: Status -       Description         Construct -       Common Name       Tope       Key Type       Distribution       Exceed By       Exceed By       Exceed By       Exceed By       Exceed By       Centificate Signed Dy (Nab-AD-CA       Od/19/2022       Certificate Signed Dy (Nab-AD-CA       Od/19/2025       Trust Certificate Signed Dy (Nab-AD-CA       Od/19/2025       Trust Certificate Signed Dy Signed EC       Impubhosc-EC.//Nab.com       Od/00/2025       Trust Certificate       Impubhosc-EC.//Nab.com       Od/00/2025								
Find Certificate       Jegins with       tomcat       Find       Clear Filter       Image: Self-signed       Excitation       Description         tomcat       cmoublesc-mail/lab.com       CA-signed       RSA       Multi-server(SAN)       filleb-AD-CA       04/18/2022       Certificate Signed by filleb-AD-CA         tomcat       cmoublesc-filleb.com       Self-signed       RC       cmpublesc-filleb.com       04/02/2025       Self-signed orfif.cate generated by system         tomcat-trust       impeublesc-EC.filleb.com       Self-signed       EC       cmpublesc-filleb.com       04/02/2025       Trust Certificate         tomcat-trust       impeublesc-EC.filleb.com       Self-signed       EC       cmpublesc-filleb.com       04/02/2025       Trust Certificate         tomcat-trust       impeublesc-EC.filleb.com       Self-signed       EC       impeublesc-Filleb.com       04/02/2025       Trust Certificate         tomcat-trust       impeublesc-EC.filleb.com       04/02/2025       Trust Certificate       Self-signed       EC       impeublesc-Filleb.com       04/02/2025       Trust Certificate         tomcat-trust       filleb.AD-CA       Self-signed       RSA       filleb.com       ommethesc-EC.filleb.com       04/02/2025       Trust Certificate         Generate Self-signed       Uploed Certificate chain <td>Certificate List</td> <td>(1 - 7 of 7)</td> <td></td> <td></td> <td></td> <td></td> <td>Rows per Page 50</td> <td>~</td>	Certificate List	(1 - 7 of 7)					Rows per Page 50	~
Construct         Common Name         Type         Key Type         Distribution         Leaved By         Exercision         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         cmoubhcsc-EC.fhlab.com         Self-signed         EC         cmoubhcsc-fileb.com         04/02/2025         Self-signed certificate penerated by system           tomcat-trust         impeubhcsc-EC.fhlab.com         Self-signed         EC         cmoubhcsc-fileb.com         04/02/2025         Trust Certificate           tomcat-trust         imseubhcsc-EC.fhlab.com         Self-signed         EC         cmoubhcsc-fileb.com         04/02/2025         Trust Certificate           tomcat-trust         imseubhcsc-EC.fhlab.com         Self-signed         EC         impeubhcsc-fileb.com         04/02/2025         Trust Certificate           tomcat-trust         imseubhcsc-EC.fhlab.com         Self-signed         EC         impeubhcsc-fileb.com         04/02/2025         Trust Certificate           tomcat-trust         fhlab-AD-CA         fhlab-AD-CA         04/02/2025         Trust Certificate         E           Certificate List         (1 - 6 of 6)         Exercificate         E	Find Certificate List	where Certificate v begin	s with v torncat	Find Clear Filter	4 -			
tomcat       cmoubhcac-ms.fhlab.com       CA-signed       RSA       Multi-server(SAN)       fhlab-AD-CA       04/18/2022       Certificate Signed by fhlab-AD-CA         tomcat-ECDSA       cmoubhcac-EC.fhlab.com       Self-signed       EC       cmpubhcac-fhlab.com       04/02/2025       Self-signed certificate generated by system         tomcat-trust       impeubhcac-EC.fhlab.com       Self-signed       EC       cmpubhcac-fhlab.com       04/02/2025       Trust Certificate         tomcat-trust       cmsubhcac-EC.fhlab.com       Self-signed       EC       cmsubhcac-fLC.fhlab.com       04/02/2025       Trust Certificate         tomcat-trust       impeubhcac-EC.fhlab.com       Self-signed       EC       cmsubhcac-fLC.fhlab.com       04/02/2025       Trust Certificate         tomcat-trust       impeubhcac-EC.fhlab.com       04/02/2025       Trust Certificate       EC         tomcat-trust       fhlab-AD-CA       Self-signed       Self-signed       FC       cmsubhcac-fEC.fhlab.com       04/02/2025       Trust Certificate         tomcat-trust       fhlab-AD-CA       Self-signed       RSA       fhlab-AD-CA       04/18/2025       Signed Certificate         Certificate List       (1 - 6 of 6)       E       E       E       E       E       E       E       E       E <t< td=""><td>Contificate *</td><td>Common Name</td><td>Type Key 1</td><td>vee Distribution</td><td>Issued By</td><td>Expiration</td><td>Description</td><td></td></t<>	Contificate *	Common Name	Type Key 1	vee Distribution	Issued By	Expiration	Description	
tomaat-ECDSA <u>cmoubhase_EC_filab.com</u> Self-signed EC cmpubhase.Hisb.com cmpubhase_EC_filab.com 04/02/2025 Self-signed certificate generated by system tomaat-trust impubhase_EC_filab.com 04/02/2025 Trust Certificate tomat-trust filab.AD-CA Self-signed EC impubhase_EC_filab.com 04/02/2025 Trust Certificate tomat-trust filab.AD-CA Self-signed RSA filab-AD-CA filab-AD-CA 04/18/2025 Signed Certificate CSR Certificate List (1 - 6 of 6) Rows per Page 5/	tomcat	cmoublese-ms.fhlab.com	CA-signed RSA	Multi-server(SAN)	fhlab-AD-CA	04/18/2022	Certificate Signed by fhlab-AD-CA	
tomost-trust impeublices:EC.fhiab.com Self-signed EC impublices.filab.com impublices:FC.fhiab.com 04/02/2025 Trust Certificate tomost-trust impeublices:EC.fhiab.com Self-signed EC impublices.filab.com impublices:FC.fhiab.com 04/02/2025 Trust Certificate tomost-trust impeublices:EC.fhiab.com 04/02/2025 Trust Certificate tomost tomost-trust impeublice: EC.friate: EC	tomcat-ECDSA	cmoubhcsc-EC.Miab.com	Self-signed EC	cmpubhcsc.thiab.com	cmpublicsc-EC.thlab.com	04/02/2025	Self-signed certificate generated by system	-
tomoat-trust <u>emsubhase-EC_filiab.com</u> Self-signed EC emsubhase.Niab.com emsubhase-EC_filiab.com 04/02/2025 Trust Certificate tomoat-trust <u>emsubhase-EC_filiab.com</u> 04/02/2025 Trust Certificate tomoat-trust <u>hiab-AD-CA</u> Self-signed EC emsubhase.Niab.com emsubhase-EC_filiab.com 04/02/2025 Trust Certificate tomoat-trust <u>hiab-AD-CA</u> Self-signed RSA filiab-AD-CA filiab-AD-CA 04/18/2025 Signed Certificate Certificate List (1 - 6 of 6) Find Certificate List where Certificate ~ begins with ↓ tomoat tomoat _ ruse_Kery True <u>Find</u> Clear Filter ↓ Find Clear Filter ↓ Certificate List where Certificate _ begins with ↓ tomoat tomoat _ ruse_Kery True <u>Exert</u> <u>Find</u> Clear Filter ↓ Certificate List where Certificate _ Carigned RSA Multi-server(SAN) filiab-AD-CA 04/18/2022 Certificate Signed by filiab-AD-CA tomoat _ ruse_Kery True <u>Kery True</u> <u>Distribution</u> <u>Issued By</u> <u>Braintion</u> <u>Carificate Signed by filiab-AD-CA</u> 04/18/2025 Certificate Signed to the component of the compon	tomcat-trust	imppublicsc-EC.fhlab.com	Self-signed EC	imppublicsc.fhlab.com	imppublicsc-EC.fhlab.com	04/02/2025	Trust Certificate	
tomcat-trust imosublices:EC.fhiab.com Self-signed EC impsublices.CE.fhiab.com 04/02/2025 Trust Certificate impsublices:EC.fhiab.com CAVC2025 Trust Certificate impsublices:EC.	tomcat-trust	cmsubhcsc-EC.fhlab.com	Self-signed EC	cmsubhcsc.fhlab.com	cmsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate	
Longet Koust       Self-signed       SC/L cleaned       SC/L cleaned <ths< td=""><td>tomcat-trust</td><td>impsubhcsc-EC.fhlab.com</td><td>Self-signed EC</td><td>impsubhcsc.fhlab.com</td><td>impsubhcsc-EC.fhlab.com</td><td>04/02/2025</td><td>Trust Certificate</td><td></td></ths<>	tomcat-trust	impsubhcsc-EC.fhlab.com	Self-signed EC	impsubhcsc.fhlab.com	impsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate	
tomcat-trust     Mab-AD-CA     Self-signed     RSA     Mab-AD-CA     Mab-AD-CA     O4/18/2025     Signed Certificate       Generate Self-signed     Upload Certificate/Certificate chain     Generate CSR     Image: Control of Contro of Control of Control of Control of Control of Control of	Instant Install	consubheres \$C fields com	Eall signed EC	emerchhere fhish com	consubheres EC fieldsh com	04/03/3035	Toot Cadificate	
Generate Self-signed       Upload Certificate/Certificate chain       Generate CSR         Certificate List (1 - 6 of 6)       Rows per Page 5         Find Certificate List where Certificate $\checkmark$ begins with $\checkmark$ torncat       Find Clear Filter       Image: Certificate Self-signed       Rows per Page 5         Certificate $\checkmark$ begins with $\checkmark$ torncat       Find Clear Filter       Image: Certificate Self-signed       RSA       Multi-server(SAN)       Issued By       Exclusion       Certificate Signed by filab-AD-CA       Output: Self-signed       Certificate Signed Certificate       Self-signed       RSA       filab-AD-CA       Old/18/2025       Signed Certificate         torncat-trust       filab-cA       Old/18/2025       Signed Certificate	tomcat-trust	fhlab-AD-CA	Self-signed RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate	
Certificate List (1 - 6 of 6)       Rows per Page 5         Find Certificate List where Certificate is begins with is torncat       Find Clear Filter       Image 1       Image 1 <td>Generate Self-sig</td> <td>pned Upload Certificate/Certifi</td> <td>cate chain Generate CSI</td> <td>ł.</td> <td></td> <td></td> <td></td> <td>- 1</td>	Generate Self-sig	pned Upload Certificate/Certifi	cate chain Generate CSI	ł.				- 1
Certificate List (1 - 6 of 6)         Find Certificate List where Certificate v begins with v tomcat       Find Clear Filter       Image: Certificate v begins with v tomcat       Find Clear Filter       Image: Certificate v begins with v tomcat       Rows per Page S         Constituate *       Common Name       Trops       Key Trops       Distribution       Issued By       Exaination       Description         tomcat       Cuccubhoscients fileb.com       CA-signed       RSA       Multi-server(SAN)       Phab-AD-CA       04/28/2022       Certificate Signed by Fileb-AD-CA         tomcat-trust       Milab-AD-CA       Milab-AD-CA       04/18/2025       Signed Certificate	-							
Find Certificate List where Certificate     begins with     tomcat     Find     Clear Filter     Image: Certificate     Example to the certificate     Description       Constitues     Constitues     Constitues     Constitues     Distribution     Issued By     Example to the certificate     Description       tomcat     Cuccubhosc-ms.fblab.com     CA-signed     RSA     Multi-server(SAN)     fblab-AD-CA     04/28/2022     Certificate Signed by fblab-AD-CA       tomcat-trust     fblab-AD-CA     Self-signed     RSA     fblab-AD-CA     04/18/2025     Signed Certificate	Certificate List	(1 - 6 of 6)					Rows per Pag	e 50 v
Centrificate         Display with         Operation         Distribution         Issued By         Example         Description           Constituate         Constituate         Constituate         Distribution         Issued By         Example         Description           tomcat         Cuccubhacoms.fhilab.com         CA-signed         RSA         Multi-server(SAN)         Filab-AD-CA         04/28/2022         Certificate Signed by filab-AD-CA           tomcat-trust         filab-AD-CA         Self-signed         RSA         filab-AD-CA         04/18/2025         Signed Certificate	Fiel Codificate Link	-ben Castificate Liberia	www.human	fiel Class Elect	A			
Common Name         True         Key Type         Distribution         Issued By         Excitation         Description           tomcat         Cucoubbacems.fhilab.com         CA-signed         RSA         Multi-server(SAN)         Philab-AD-CA         04/28/2022         Certificate Signed by fhilab-AD-CA           tomcat-trust         fhilab-AD-CA         Self-signed         RSA         Philab-AD-CA         04/18/2025         Signed Certificate	Find Centricate List	where Certificate O Degin	is with Uptomcet	Find Clear Filter	<b>4</b>			
tomcat cucoubhosc-ms.fblab.com CA-signed RSA Multi-server(SAN) fblab-AD-CA 04/28/2022 Certificate Signed by fblab-AD-CA tomore trust fblab-AD-CA fblab-AD-CA fblab-AD-CA 04/18/2025 Signed Certificate	Castificate *	Common Name	Type Ke	Type Distribution	Issued By	Expiration	Description	_
tomcat-trust <u>fhlab-AD-CA</u> Self-signed RSA fhlab-AD-CA fhlab-AD-CA 04/18/2025 Signed Certificate	tomcat	cucpublicsc-ms.fhlab.com	CA-signed RSA	Multi-server(SAN)	fhlab-AD-CA	04/28/2022	Certificate Signed by fhlab-AD-CA	
tomost-orust miso-AD-CA 04/18/2025 Signed Certificate	termine and termine	Nub 40. CA	Collisional DCA	Alah AD CA	blab an ca	04/10/2025	Sanad Cart Lana	٦
	tomcat-trust	INISO-AU-LA	aer-signed RSA	miao-AD-CA	miao-AU-CA	04/18/2025	signed Certificate	
tempetation associated and the construction of	Inmediately	cursubbrac-EC (blab.com	Self-signed EC	cucsubbosc Blab.com	cursubhrac.EC Blab.com	04/02/2025	Tout contracte Windows	6
tomatives and the second second second second second second contraction of 22,203 that Catalogue Charlenge Contractions to activity Microsoft	tomcaturust	curpublices.EC.Blab.com	Self-signed EC	cucrubbosc fblab.com	currubbere-EC (blab.com	04/02/2025	Tost Certificate the activate Window	5
							and the second of the second to the second s	

• IIS

否则,本节将介绍这些角色的安装过程。否则,请跳过此部分,直接从Microsoft下载ADFS3。

安装带DNS的Windows 2012 R2后,将服务器升级到域控制器。

下一个任务是安装Microsoft证书服务。

导航至服务器管理器并添加新角色:

<b>6</b>	Server Manag	ger	- • ×
Server Ma	nager • Dashboard	- 🕲   🏲 Manage	Tools View Help
Dashboard	WELCOME TO SERVER MANAGER	Rer Adv	move Roles and Features
All Servers	1 Configure thi	is local server	ver Manager Properties
簡 AD DS 와 AD FS 盈 DNS 聞 File and Storage Services ▷ 配 IIS	QUICK START  2 Add roles an  3 Add other se  WHAT'S NEW  4 Create a serv	id features ervers to manage ver group	
	LEARN MORE		Hide
	Roles: 6   Server groups: 1   Servers total: 1	D DS 1 AD FS	1

选择Active Directory证书服务角色。

<b>b</b>	Add Roles and Features Wizard	
Select server roles		DESTINATION SERVER AD fhiab.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           Image: Active Directory Certificate Services (4 of 6 installed)       Image: Certificate Services (4 of 6 installed)         Image: Certificate Enrollment Volicy Web Service (Installed)       Image: Certificate Enrollment Policy Web Service (Installed)         Image: Certificate Enrollment Veb Service (Installed)       Image: Certificate Enrollment Web Service (Installed)         Image: Certificate Enrollment Web Service (Installed)       Image: Certificate Enrollment Veb Service (Installed)         Image: Certificate Enrollment Services       Online Responder         Image: Certificate Directory Domain Services (Installed)       Image: Certificate Services (Installed)         Image: Certificate Directory Domain Services (Installed)       Image: Certificate Directory Services (Installed)         Image: Certificate Directory Rights Management Services       Active Directory Rights Management Services         Image: Certificate Directory Rights Management Services       Application Server         Image: DHCP Server       Image: DHCP Server         Image: DHCP S	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.
	]	< Previous Next > Install Cancel

并首先部署这些服务 — 证书颁发机构证书注册策略Web服务。安装这两个角色后,配置它们,然 后安**装证书注册Web**服务**和证书颁发机构Web注册**。配置它们。

安装证书颁发机构后,还将添加IIS等其他角色服务和功能。

根据部署,您可以选择企业或独立。

Add Roles Wizard		×
Specify Setup Ty	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	

## 对于CA类型,可以选择根CA或从属CA。如果组织中没有其他CA正在运行,请选择**根CA**。

Add Roles Wizard		×
Specify CA Type		
Before You Begin Server Roles AD CS Role Services Setup 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. © Root CA Select this option if you are installing the first or only certification authority in a public key infrastructure.	
Setup Type CA Type 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 > Instal Cancel	

下一步是为CA创建私钥。

#### Add Roles Wizard

Set Up Private Ke	2 <b>y</b>
Before You Begin Server Roles AD CS Role Services Setup Type CA Type	<ul> <li>To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.</li> <li>Create a new private key         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 issue new certificates, you must also select a hash algorithm.     <li>Use existing private key</li> </li></ul>
Private Key Cryptography CA Name Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress Results	Use this option to ensure continuity with previously issued certificates when reinstalling a CA.  Select a certificate and use its associated private key 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.  Select an existing private key on this computer Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.
	More about public and private keys           Amount of the second

X

只有在单独的Windows Server 2012上安装ADFS3时,才需要执行此步骤。配置CA后,需要配置 IIS的角色服务。在CA上进行Web注册时,这是必需的。对于大多数ADFS部署(即IIS中的额外角色 ),需要单击"应**用程序开**发"下的"ASP.NET"。

Add Roles Wizard		<u>×</u>
Select Role Servi	ices	
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         HTTP Redirection         WebDAV Publishing         NET Extensibility         ASP         CGI         ISAPI Filters         Server Side Includes         HTTP Logging         Logging Tools         Request Monitor         Tracing	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"服务器管理器"中,单**击"Web服务器">"IIS"**,然后右键单击"默认**网站"**。绑定需要更改,以便除 HTTP外还允许HTTPS。这是为了支持HTTPS。



选择"编**辑绑定**"。



添加新的"站点绑定"并**选择**HTTPS作为类型。对于SSL证书,选择应具有与AD服务器相同的 FQDN的服务器证书。

<b>8</b> 3			Intern	et Informatior	n Services (IIS) Manager	
€ ) AD →	Sites + D	efault Web Site	•			
File View Help						
Connections				Site	Bindings	? X
<ul> <li>Start Page</li> <li>AD (FHLAB\admini Application Poc a)</li> <li>Sites</li> <li>Default Web</li> </ul>	Type http https	Host Name Type: https Host name: Require S SSL certificat fhlab-AD-C/ Not selected fhlab-AD-C/ AD.fhlab.com	Port 80 442 I V ierver Name te: A I A m	IP Address * Edit P address: All Unassigned	Binding Informa t Site Binding Port: 443 443 Select OK	Add Fdit ? X View

所有必备角色都安装在环境中,因此现在您可以继续安装ADFS3 Active Directory联合身份验证服务 (在Windows Server 2012上)。

对于"服务器角色",导航至**"服务器管理器">"管理">"添加服务器角色和功能"**,然后选择Active Directory**联合身份验证服务**(如果您在客户网络内部的专用LAN上安装IDP)。



安装完成后,您可以从任务栏或开始菜单打开它。

<b>%</b>	AD FS	_ <b>_</b> X
输 File Action View Window Help		_ 8 ×
← → □		
ad FS	AD FS	Actions
	Overview	AD FS Add Relying Party Trust
	AD FS provides single-sign-on (SSO) access for client computers.	Add Claims Provider Trust
	Learn More	Add Attribute Store
	Configuring Trust Relationships	Edit Federation Service Properti
	Configuring Authentication Policies	Edit Published Claims
	Troubleshooting AD FS	Revoke All Proxies
	AD FS Help	View 🕨
		New Window from Here
		G Refresh
		Help
	Activate	Windows

# ADFS3初始配置

本节将介绍新的独立联合服务器的安装过程,但也可用于在域控制器上安装该服务器

选择Windows并键入AD FS Management以启动ADFS管理控制台,如图所示。



选择AD FS 3.0联合服务器配置向导选项以启动ADFS服务器配置。这些屏幕截图代表AD FS 3中的相同步骤。

AD FS 2.0 Federation Ser	ver Configuration Wizard	×
Welcome		
Welcome  Welcome  Velcome  Select Deployment Type  Federation Service Name  Summary  Results	<ul> <li>Welcome to the AD FS 2.0 Federation Service Configuration Wizard</li> <li>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 sectoration Service</li> <li>C frate a new Federation Service</li> <li>Select this option to set up either a stand-alone federation Service</li> <li>Add a federation server to an existing Federation Service</li> <li>Select this option to join this computer to an existing federation server farm.</li> </ul>	
	< <u>Previous</u> <u>Next&gt;</u> Cancel <u>H</u> elp	

选择"创建新联合**身份验证服**务"并单**击"下一**步"。

AD FS 2.0 Federation Ser	ver Configuration Wizard	×
Select Stand-Alone o	r Farm Deployment	
Step:	You can create either a stand along federation ensure for such ratios prepared or a small reachestion	
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.	
<ul> <li>Summary</li> </ul>	O New federation server farm	
<ul> <li>Results</li> </ul>	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.	
	⊙ Stand-alone federation server	
	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	

选择Stand-alone Federation Server,然后单击**Next(下**一步),如图所示。

No. 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 Default Web Site. If the wizard cannot determi must select a certificate. Select the certificate and/or port, and then clic	name from ine the Feo k Next.	the Subject field o leration Service na	of the SSL certifica ime from the SSL :	ite for the settings, you
<ul> <li>Summary</li> <li>Results</li> </ul>	ad0a.identitylab.us Federation Service name: ad0a.identitylab.us What kind of certificate do I need?	*	View	443 ¥	
		Previous	Next	Gancel	Help
		i revious	INCAL /		

在SSL证书下,从列表中选择自签名证书。联合身份验证服务名称将自动填充。单击 Next。

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

查看设置并单击"下**一步"**以应用设置。

AD FS 2.0 Federation Serv	ver Configuration Wizard	×							
Configuration Results									
Steps @Welcome	The following settings are being configured								
<ul> <li>Welcome</li> <li>Select Deployment Type</li> <li>Federation Service Name</li> <li>Summary</li> <li>Results</li> </ul>	Component         Install Windows Internal Database         Install Windows Internal Database         Install Windows Internal Database         Install Windows Internal Database service         Install Windows Internal Database         Install Windows Internal Database         Install Windows Internal Database         Install Configure service settings         Install Deploy browser sign-in Web site         Install Deploy Browser Service         Install Deploy Browser Service         Install Deploy Browser Service         Install Deploy Browser Service         Install Deploy Browser Service </th <th>Status Configuration finished Server Configuration Wizard.</th>	Status Configuration finished Server Configuration Wizard.							
		<u>_</u> lose							

确认所有组件都已成功完成,然后单击**关闭**以结束向导并返回主管理控制台。这可能需要几分钟。

AD 15 2	0	Actions
	Verview           %S 20 provides angle-sign-on (SSO) access for client computers.           Required Configuration Incomplete           Before you can use AD FS 20 to manage SSO access for users and services, you must complete the following task:           Required: Add a trusted rebring party           Learn About:           Configuring: Claims Provider or Bebring Party Trusts           Adding Federation Servers to a Farm and Setting Up Load-Balancing           Configuring Claims Provider or Proxies           Troubleshooting AD FS 2.0	Actions AD FS 220 Add Relying Party Trust Add Clains Provider Trust Add Attribute Store Edit Federation Service Proper Edit Published Clains Revole Al Provides Provide Feedback. Yiger New Window from Here Refresh Provide Feedback Help

ADFS现在已有效启用并配置为身份提供程序(IdP)。 接下来,您需要将CUCM添加为可信赖的合作 伙伴。在执行此操作之前,您需要先在CUCM管理中执行一些配置。

# 使用ADFS在CUCM上配置SSO

## LDAP配置

群集需要与Active Directory进行LDAP集成,并且在进一步配置之前,需要配置LDAP身份验证。导 航至**系统选项卡> LDAP**系统,如图所示。

#### 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

然后,导航至"系统**"选项卡>"LDAP目录**"。

LDAP Directory							
🔚 Save 🗶 🕻	Delete 🗋 Copy	🏷 Pe	rform Full Sync No	w 🕂	Add New		
Status							
i Status: Read	dy						
LDAP Directory	Information						
LDAP Configurati	on Name*	LDAP1					
LDAP Manager Di	istinguished Name*	fhlab\a	administrator				
LDAP Password*		•••••	•••••	•••••	•••••		
Confirm Password	d*	•••••	•••••	•••••	•••••		
LDAP User Search	h Base*	cn=use	ers,dc=fhlab,dc=	com			
LDAP Custom Filt	er for Users	< Nor	ne >			٥	
Synchronize*		🖸 Us	ers Only 🔵 Us	ers and	Groups		
LDAP Custom Filt	er for Groups	< Nor	ne >			٢	
LDAP Directory	Synchronization S	chedu	le				
Perform Sync Jus	t Once						
Perform a Re-syn	ic Every*		7 DAY ᅌ				
Next Re-sync Tin	ne (YYYY-MM-DD hh:	:mm)*	2020-05-24 00	:00	]		
itandard User Fields To Be Synchro	nized						
isco Unified Communications Manager U Jser ID	sAMAccountName			Cisco Unified Co First Name	ommunications Manager User Field	givenName	
liddle Name	middleName 😌			Last Name		sn	
lanager ID	manager			Department		department	
hone Number	telephoneNumber ᅌ			Mail ID		mail	
itle	title			Home Number		homephone	
inertory LIRT	mobile			Pager Number		displayName	
	maii	<u>×</u>		Display Name		displaywame	
-LDAP Server Informa	tion						
Host Name or IP	Address for Server <sup>+</sup>				LDAP Port * Use TLS		
10.89.228.226 389							
Save Delete	Copy Perform Full	Sync Now	Add New				

在Active Directory用户与CUCM同步后,需要配置LDAP身份验证。

abab	Cisco Un	nified Cl	M Adı	ninistrati	on							Navigation	Cisc	to Unified CM A	Idministrati	on	√ Go
cisco	For Cisco Un	nified Comm	nunicati	ons Solutions								farfa	• 1	Search Docur	mentation	About	Logout
System *	Call Routing + N	Media Resource	es 👻 A	Ivanced Features	• Device •	Application •	User Mana	gement 👻	Bulk Administration 👻	Help 🕶							
LDAP Aut	thentication																
Seve																	
Status																	
() Stat	us: Ready																
LDAP AU	thentication for	r End Users															
Use L	DAP Authenticatio	on for End Us	ers														
LDAP Mar	nager Distinguish	ed Name* [	hlab\Adn	inistrator													
LDAP Pas	sword*	•	•••••			•••••											
Confirm I	Password*	•	•••••														
LDAP Use	er Search Base*	c	n=users	dc=fhlab,dc=co	m												
LDAP Se	rver Informatio	on															
		Host	Name or	IP Address for	Server*			LDAP Por	t" Use TLS								
10.89.2	28.226							389									
Add A	nother Redundan	t LDAP Serv	er														

#### CUCM中的最终用户需要将特定访问控制组分配给其最终用户配置文件。ACG是标准CCM超级用户 。当环境就绪时,用户将用于测试SSO。

End Use	r Configuration		Related Links: Back to Find List Users	Go Go
Sav	e 🗙 Delete 🕂 Add New			
Confirm	MLPP Password			1
MLPP Pr	recedence 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	<ul> <li>View Details</li> </ul>		
Conference Enate Meeting	ence Now Information ble End User to Host Conference Now Number 1001			
Attende	es Access Code			
Save	Delete Add New			

## CUCM元数据

本节将显示CUCM发布者的流程。

第一项任务是获取CUCM元数据,您需要浏览到URL;**https://<CUCM Pub** FQDN>:8443/ssosp/ws/config/metadata/sp,或者可以从System选项卡> SAML Single Sign-on下 载。这可以按节点或集群范围完成。首选执行此集群范围。

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.

使用有意义的名称(如sp\_cucm0a.xml)将数据保存到本地,之后您将需要它。

# 配置ADFS信赖方

反向到AD FS 3.0管理控制台。

<b>\$</b> 0		AD FS	_ <b>_</b> ×
📬 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	CUCM Cluster Wide Rebino Party trust	Yes WS-T cmoubloss filab.com	Add Relying Party Trust
Relying Party Trusts	The Date Tout	Yes WS-T cucpublicsc fhlab.com	Add Non-Claims-Aware Relying
Attribute Stores Add Rey	Chiese Avera Babies Parts Tourt	Yes WS-T INab.com-50000F4107D76E57	View >
p Automotive Villes Add Non	-Claims-Aware neising Party Trust		New Window from Here
View New Win	dow from Here		@ Refresh
New With	dow nom Here		Help
Kefresh			
Help			

单击"添**加信赖方信任向导**"。

<b>\$</b>	Add Relying Party Trust Wizard	×
Welcome		
<ul> <li>Steps</li> <li>Welcome</li> <li>Select Data Source</li> <li>Configure Multi factor Authentication Now?</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	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 party consume 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 and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.	s te W

单击**Start(开**始)继续。

选择您**之前保存的**federationmedata.xml元数据XML文件,然后单击下一步。

<b>\$</b>	Add Relying Party Trust Wizard
Select Data Source	
<ul> <li>Steps</li> <li>Welcome</li> <li>Select Data Source</li> <li>Configure Multifactor Authentication Now?</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	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.         Federation 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\_Releing\_Party\_trust作为显示名称,然后单击Next。

Specify Display Name         Steps       Enter the display name         • Welcome       Display name:         • Select Data Source       CUCM_Cluster_Wid         • Specify Display Name       Notes:         • Configure Multifactor Authentication Now?       Image: Configure Name	me and any optional notes for this relying party. de_Relying_Party_trust
Steps     Enter the display name:          • Welcome      Display name:           • Select Data Source      CUCM_Cluster_Wid           • Specify Display Name      Notes:           • Configure Multi-factor       Authentication Now?         • Configure Multi-factor       Authentication Now?	me and any optional notes for this relying party.  de_Relying_Party_trust
Welcome     Display name:     Display name:     CUCM_Cluster_Wid     Specify Display Name     Configure Multi-factor     Authentication Now?     Configure Multi-factor     Authentication Now?	de_Relying_Party_trust
Select Data Source     CUCM_Cluster_Wid     Specify Display Name     Notes:     Configure Multifactor     Authentication Now?     Configure Authentication Now?	de_Relying_Party_trust
Specify Display Name     Notes:     Configure MultiFactor     Authentication Now?	<u>^</u>
Configure Multifactor     Authentication Now?	^
Authorization Rules	
Ready to Add Trust	
Finish	<u>~</u>
	< Previous Next & Canicel

选择第一个选项,然后单击"下**一步"**。

<b>\$</b>	Add Relying Party Trust Wizard	
Steps	Configure multifactor authentication settings for this relying party trust. Multifactor authentication is required if	
<ul> <li>Welcome</li> </ul>	there is a match for any of the specified requirements.	
Select Data Source		
Specify Display Name	Multi-factor Authentication Global Settings	
Configure Multi-factor Authentication Now?	Requirements Users/Groups Not configured	
Choose Issuance     Authorization Pulse	Device Not configured	
Ready to Add Trust	Location Not configured	
<ul> <li>Finish</li> </ul>		
	<ul> <li>I do not want to configure multifactor authentication settings for this relying party trust at this time.</li> <li>Configure multifactor authentication settings for this relying party trust.</li> <li>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>.</li> </ul>	de

选择**允许所有用户访问此信赖方,**然后单**击下**一步,如图所示。

<b>Q</b>	Add Relying Party Trust Wizard				
Choose Issuance Authorization Rules					
Steps	Issuance authorization rules determine whether a user is permitted to receive claims for the relying party.				
<ul> <li>Welcome</li> </ul>	Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.				
Select Data Source	<ul> <li>Permit all users to access this relying party</li> </ul>				
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				
<ul> <li>Choose Issuance Authorization Rules</li> </ul>	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.				
<ul> <li>Ready to Add Trust</li> </ul>					
• 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 (Canicel in do				

查看配置并单击Next(如图所示)。

<b>\$</b>	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.
	< Previous Allex Sate Caricel S

取消选中此框,然后单击"**关闭"**。

<b>\$</b>	Add Relying Party Trust Wizard	¢,
Finish		
<ul> <li>Steps</li> <li>Welcome</li> <li>Select Data Source</li> <li>Specify Display Name</li> <li>Configure Multi-factor Authentication Now?</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	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	

#### 使用鼠标辅助按钮选择您刚**创建的信**赖方信任和**编辑领款**申请规则配置,如图所示。

<b>\$</b>		AD FS		
翰 File Action View Window	w Help			
🗢 🄿 🖄 📰 📓 🗊				
🛗 AD FS	Relying Party Trusts			
Service	Display Name	Enabled Type		Identifier
	Device Registration Service	Yes WS-Trust / SAM	ML / WS-Federation	um:ms-drs:ad.fhlab.com
Claims Provider Trusts	CUCM_Cluster_Wide Relving Party trust	Yes WS-Trust / SAM	L / WS-Federation	cmpubhcsc.fhlab.com
Relying Party Trusts	CUC_Cluster_W Update from Fee	eration Metadata	L / WS-Federation	cucpubhcsc.fhlab.com
Attribute Stores	ExpwyC Edit Claim Rules		L / WS-Federation	fhlab.com500D0F4107D76E57
p Authentication Policies	Disable		1	
	Properties			
	riopenies			
	Delete			
	Help			
			-	
	I			

单击Add Rule(添加规则),如图所示。

翰 Edit Claim Rules	for CUCM_Cluster_Wid	le_Relying_Party	- • ×
Issuance Transform Rules	Issuance Authorization Rule	s Delegation Authoriza	ation Rules
The following transform	rules specify the claims that wi	I be sent to the relying p	arty.
Order Rule Name		Issued Claims	
			-
Add Rule Edit	Rule Remove Rule		
		OK Cancel	Apply

选择"**将LDAP属性作为声明发送**",然后**单击"**下一步"。

<b>\$</b>	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.
<ul> <li>Configure Claim Rule</li> </ul>	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

配置以下参数:

领款申请规则名称:名称ID

属性存储:Active Directory(双击下拉菜单箭头)

LDAP属性:SAM帐户名称

传出领款申请类型:uid

单击**完成/确**定继续。

请注意,uid不是小写的,并且下拉菜单中不存在。键入。

	Edit Ru	ule - NameID 🛛 🗙				
You car which to issued f	You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.					
Claim ru	le name:					
Namel	1					
Rule ter	mplate: Send LDAP Attributes as Claims					
Athbute	e store:					
Active	Directory	¥				
Mappin	g of LDAP attributes to outgoing claim type	8:				
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)				
•	SAM-Account-Name V	uid 🗸				
*	~	×				
View i	Rule Language	OK Cancel				

再次**单击Add Rule(添加规则)**以添加另一个规则。

🦚 Edit Cla	aim Rules fo	or CUCM_Clus	ter_Wid	e_Relying_Part	y 🗕	• x
Issuance Tr	ansform Rules	Issuance Authoriz	ation Rules	Delegation Autho	rization R	ules
The follow	ving transform n	les specify the clai	ins that will	be sent to the relyin	g party.	
Order	Rule Name			Issued Claims		
	NameID			uid		
						4
Add Ru	Je Edit F	Rule Remov	e Rule			
L						
			0	K Cance		Apply

<b>S</b>	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.
<ul> <li>Configure Claim Rule</li> </ul>	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: <ul> <li>Sending claims from a SQL attribute store</li> <li>Sending claims from a custom attribute store</li> <li>Sending claims only when 2 or more incoming claims are present</li> <li>Sending claims only when an incoming claim value matches a complex pattern</li> <li>Sending claims for use only in later rules</li> </ul>
	< Previous Next > Cancel

创建名为Cluster\_Side\_Claim\_Rule的自定义规则。

将此文本直接从此处复制并粘贴到规则窗口中。有时,如果在文本编辑器上编辑引号,则会更改引 号,这会使规则在测试SSO时失败:

c:[Type ==

"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] => 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/namegualifier"] = "http://<ADFS FQDN>/adfs/com/adfs/services/trust", Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "<CUCM Pub FQDN>"); c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] => 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/namequalifier"] = "http://AD.fhlab.com/adfs/services/trust", Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "cmpubhcsc.fhlab.com");

单击Finish(完成)继续。

<b>%</b>	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 == ^ "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
	<pre>"] = "urn:oasis:names:tc:SAML:2.0:nameId-format:translent", 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>

现在,您应在ADFS上定义两个规则。单击**Apply**和**OK**以关闭规则窗口。

🂱 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现在已成功添加为ADFS的可信信赖方。

9		Service	5				x
File Action View	Help						
💠 🔿 🔝 🖬 🕼	2 🕞 🛛 🖬 🕨 🖬 🕪						
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	Active Directory Domain Services	AD DS Domain Controller servic Enables Active Directory Federa	Running	Automatic Automatic (Delayed Start)	FHLAB\administra	ator
	Restart the service	Active Directory Web Services	This service provides a Web Ser Gets apps ready for use the first	Running	Automatic Manual	Local System Local System	ור
	Description: 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	Local System	
		Application Identity	Facilitates the running of intera Provides support for 3rd party p		Manual (Trigger Start) Manual (Trigger Start) Manual	Local System Local System	
		Application Management AppX Deployment Service (AppXSVC)	Processes installation, removal, Provides infrastructure support		Manual Manual	Local System Local System	
		ASP.NET State Service Background Intelligent Transfer Service	Provides support for out-of-pro Transfers files in the backgroun		Manual Manual	Network Service Local System	
		Background Tasks Infrastructure Service	Windows infrastructure service The Base Filtering Engine (BFE) i Conjectures certificates and roo.	Running Running Running	Automatic Automatic Magual	Local System Local Service	
		CNG Key Isolation	The CNG key isolation service is	Running	Manual (Trigger Start)	Local System	
		COM+ System Application	Manages the configuration and	Running	Manual	Local System	
		Secomputer Browser	Maintains an updated list of co		Disabled	Local System	~
	Canada (Canada)	٢					2
	Lotended / Standard /			4	Activate Windows	s	_

在继续之前,请重新启动ADFS服务。导航至"开**始"菜单>"管理工具">"服务**"。

## IDP元数据

您需要向CUCM提供有关我们IdP的信息。此信息使用XML元数据交换。确保在安装了ADFS的服务 器上执行此步骤。

Untrusted Connection x Mozila Firefox Start Page 4 Most Visited	Firefox 🔽	
Most Visited Getting Started Stars Web Slice Gallery          Image: Comparison of the start	🔔 Untrusted Connection 🛛 🗙 😼 Mozilla Firefox Start Page 🛛 🕹 +	
Most Visited Getting Started Suggested Sites Web Slice Gallery	(♦) 🕲 >s://ad0a.identity(us/FederationMetadata/2007-06/FederationMetadata ☆ マ ৫) 😣 - Google 🖉 🖌	+ 🏦
Opening FederationMetadata.xml       but we can't confirm that your         You have chosen to open:       dentification to prove that you         Image: PederationMetadata.xml       which is: XML Document         from: https://a00a.identitylab.us       an that someone is trying to         Image: PederationMetadata.xml       an that someone is trying to         Image: PederationMetadata.xml       Image: PederationMetadata.xml         which is: XML Document       Image: PederationMetadata.xml         Image: PederationMetadata.xml       an that someone is trying to         Image: PederationMetadata.xml       Image: PederationMetadata.xml         Image: PederationMetadata.xml       Image: PederationMetadata.xml         Image: PederationMetadata.xml       Image: PederationMetadata.xml         Image: PederationMetadata.xml       Image: PederationMetadata.xml         Image: PederationMetadata.xml       Image: PederationPederatio	Most Visited Getting Started Suggested Sites Web Slice Gallery	
You have chosen to open:       dentification to prove that you         Image: PederationMetadata.xml       which is: XML Document         from: https://ad0a.identitylab.us       an that someone is trying to         Image: I	Opening FederationMetadata.xml	<u> </u>
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. Mathematical for files like this files like this for files like this files	You have chosen to open: FederationMetadata.xml  dentification to prove that you ed.	
Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.	which is: XML Document from: https://ad0a.identitylab.us What should Firefox do with this file?	
	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浏览器连接到ADFS(IdP)以下载XML元数据。打开浏览器到https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml并将元数据保存到本地文件夹。

现在,导航至CUCM配置到系统菜单> SAML单点登录菜单。

	🗰 Find and List Cisco	o Unified CM × +	-		×
¢	) → ሮ ✿	Image: Barrier State	11/ 0	3	-9
	Server Cisco Unified CM Cisco Unified CM Group Presence Redundancy Grou Phone NTP Reference Date/Time Group	MAdministration Navigation Cisco Unified CM Administration nunications Solutions farfar Search Documentation ces • Advanced Features • Device • Application • User Management • Bulk Admin ups ups	on Abo stration	vt   L • Help	Go ogout
	BLF Presence Group	anager Group			
	Region Information	nager where Name begins with v Find Cle	ar Filte	r 🌵	-
	Device Mobility	active query. Please enter your search criteria using the options above.			
	DHCP	•			
	LDAP	•			
	SAML Single Sign-On				
	Cross-Origin Resource Shar (CORS)	ring			
	Location Info	•			
	MLPP	•			
	Physical Location				
	SRST				
	Enterprise Parameters				
	Enterprise Phone Configurat	ton			
	Service Parameters				
	Security	•			
	Application Server				
	Licensing	•			
	Geolocation Configuration				
	Geolocation Filter				
	E911 Messages				

https://moubbesc.fblab.com/##1/comadmin/sambinaleSianOn.do 反向到CUCM Administration并选择SYSTEM > SAML Single Sign-On。

	dtt: SAML Single Sign-O comadmin/samiSingleSignOn.do Unified CM Administrati o Unified Communications Solution: • Media Resources • Advanced Feature	on × the Fn	d and List LDAP Directories 습 포	× + C S - Google Navigation Cisco Unified	P E -	♣ ♠ Go
A https://cum0a/ cisco For Cisco System - Cal Routing SAML Single Sign-O	comadmin/samiSingleSignOn.do Unified CM Administrati o Unified Communications Solution • Media Resources • Advanced Feature	on s	습 <del>*</del>	C S - Google Navigation Cisco Unified	P CM Administration	♣ ♠ G0
SAML Single Sign-O	Unified CM Administrations Solution • Unified Communications Solution • Media Resources • Advanced Feature	on		Navigation Cisco Unified	d CM Administration	• Go
System - Cal Routing	Media Resources      Advanced Feature	- Daviso - Andication -		admin Search Docume	ntation   About	Logout
SAML Single Sign-O		с сенсе мариовани с	User Management + Bul	k Administration 👻 Help 👻		
	n					
SAML SSO	🚯 Update kiP Metadata File 👔 Export /	Al Metadata 🧳 Fix Al Disabled	Servers			
- Status						
() SAML SSO disabl	led					
SAML Single Sign-	On (1 - 1 of 1)				Rows per Page	50 💌
Server Name S	SO Status Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Tes	e
cuemua Dis	abled N/A	Never	rite rite	Never	Ru	n Test

选择Enable SAML SSO。

## 单击Continue以确认警告。

🥹 Reset Warning - Mozilla Firefox 📃 🗖	×
Https://cucmDa/ccmadmin/genericDialogWindow.do?windowtitlekey=genericdialogwindow.windowtitle.ssoenable	
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	

=-	_	
PЛ	朩	0

Firefox *	-0
🗱 Find and List Users × 🗱 SAML Single Sign-On Configuration × 🗱 Find and List LDAP Direct	ectories × +
A https://cucm0a/comadmin/sam/SingleSignOnConfigurationWizard.do	습 후 C 🗧 • Google 👂 🖬 • 🖡 🏦
Cisco Unified CM Administration For Cisco Unified Communications Solutions	Navigation Cisco Unified CM Administration 💌 Go admin Search Documentation About Logou
System 👻 Call Routing 👻 Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻 User Management	t ▼ Bulk Administration ▼ Help ▼
SAML Single Sign-On Configuration	
Next .	
Status	rom your IdP and import it to your servers. You will need to

## 选择XML文件,然后单击**打开**,以便从"收藏夹"下的"下载"中将其上传到CUCM。

File Upload						×
🗿 🖓 - Adminis	strator - Downloads				Search Downloads	12
Organize - New folder					清 • 🗊	
* Favortes	Name *	Date modified	Туре	5420		
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		
2 Recent Places	🍪 picpick_inst	2013/09/12 11:09 AM	Application	11 129 KB		
Ubraries Documents Music Pictures Videos Computer Network						
Fab	e game: FederationMetadata				All Files Qpen Cancel	•

上传后,点击Import IdP Metadata(导入IdP元数据),将IdP信息导入CUCM。确认导入成功,然 后单击"下一步"继续。

🗧 SAML Sir	ngle Sign-On Configuration - Windows Internet Explorer		_ [	IX
00.	🙆 https://10.1.1.100/ccmadmin/s 🔎 💌 😵 Ce 🖻 😏 🔏 SAML Single Sign-On Configu 🗙		$\odot$	<ul><li>(i)</li></ul>
cisco	Cisco Unified CM Administration         Navigation         Cisco Unified CM Administration           For Cisco Unified Communications Solutions         admin         Search Documentation	on Abou	t Logo	30 out
System 👻	Call Routing - Media Resources - Advanced Features - Device - Application - User Management -	Bulk /	Administrati	ion 👻
Help 👻				
SAML Sin	gle Sign-On Configuration			
Next				
Status —				_
√ Impo	ort succeeded for all servers			
Identity	Provider(IdP) Metadata Trust File			_
To configu to your se	ure the trust relationship between the IdP and your servers, you must first obtain trust metadata from you ervers. You will need to manually obtain the file from the IdP and upload it here.	ır IdP ar	nd import	it
IdP Metad	lata File C:\Users\bbanks\Downloads\FederationMetadata.xml Browse			
– Initiate t	he Metadata Import			=
This actio	n must be successful for at least the Publisher before moving on to the next task in this wizard.			
Import	IdP Metadata Vimport succeeded for all servers			
Next	Cancel			_
选择属于	F标准CCM超级用户的用户,然后点击RUN SSO TEST。			
😆 SAML S	Single Sign-On Configuration - Mozilla Firefox	_		×
0	https://cmpubhcsc.fhlab.com:8443/ccmadmin/samlSingleSignOnConfigurationWizard3.do?serv	rei ***	⊌ ☆	Ξ
SAML Sin	gle Sign-On Configuration			
Test SS0	) Setup			
This hash	The back is a set of the first set of the set of the set of the first set of the set of			

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test can be run on any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is successful.						
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 administrator lockout.						
Valid administrator Usernames						
2)Launch SSO test page						
Run SSO Test						
Cancel						

## 当显示用户身份验证对话框时,使用适当的用户名和密码登录。

ign In - Mozilla Firefox	-		×
🛛 🔒 https://ad. <b>fhlab.com</b> /adfs/ls/?SAMLRequest=nZJPTwlxEMX	vflpN77ClAi	4NS0 •••	≡
			^
FS			
Sign in with your organizational account			
farfar@fhlab.com			
Sign in			~

## 如果所有配置都正确,您应看到一条消息,说SSO测试成功!

## SAMLS	ingle Sign-On X 🕂	=	D	×
😆 SAML S	ingle Sign-On Configuration - Mozilla Firefox	-		×
0 4:	https://cmpubhcsc.fhlab.com:8443/ccmadmin/samlSingleSignOnConfigurationWizard3.do?testSt	•••	⊠ ☆	≡
SAML Sin	gle Sign-On Configuration			
Status				
🗸 550	Metadata Test Successful			
Close				
	📦 Test SAML - Mozilla Firefox – 🗆 🗙	1		
	⑦ ▲ \$\prod \$			
	SSO Test Succeeded!			
	Congratulations on a successful SAML SSO configuration test. Please			
	close this window.			
	Close			

单击"关闭"和"完成"继续。

现在,我们已成功完成基本配置任务,以使用ADFS在CUCM上启用SSO。

# 在CUC上配置SSO

在Unity Connection中启用SSO时,可遵循相同的流程。

#### LDAP与CUC集成。

€ → ୯ û	💿 🔒 😂 https://cucpub	hoso.fhlab.co	m/cuadmin/home	•	· 🛛 🕁	II\ 🖸 📽	≡		
Cisco Unity Con Cisco For Cisco Unified Com	munications Solutions	ation				Naviga farfa	ion Cisco Unity Connection A Search Documentation	dministration 🗸 About Sig	Go ph Out
Cisco Unity Connection	SAML Single Sign on							SAML Single	Sign on
General Configuration Cluster Authentication Rules Roles Restriction Tables Licenses Schedules Holiday Schedules Global Nicknames	SSO Mode Cluster wide (One m Per node (One meta Disable SAML SSO SAML Single Sign-O	etadata file p data file per r O Update kdP n (1 - 2	er cluster. Require node) Metadata File 👔	s multi-server Tomcat certificate) Export Al Metadata 🧷 Fix Al Disa	bled Servers		Ro	rs per Page 50	0
Subject Line Formats	Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Te	ıt	
Attachment Descriptions cucpublicsc.fhlab.com SAML N/A April 29, 2020 10:52:36 AM 📩 File April 28, 2020 5:54:01 PM Passed - April 29, 2020 Run PDT 11:05:10 AM PDT							Run SSO Ter	st	
Service Parameters Plugins Fax Server B-LDAP SAM Single Sing on	cucsubhcsc.fhlab.com Disable SAML SSO	SAML Export All	1dP	April 29, 2020 10:52:36 AM PDT te IdP Metadata File	isabled Server	April 28, 2020 5:54:00 PM POT	Passed - April 29, 2020 11:05:37 AM PDT	Run SSO Te	đ

#### 配置 LDAP 验证.

← → ♂ ☆	🔞 🖨 🛱 https://cucpubhcsc.fhlab.com/cuadmin/home.do	
Cisco Unity Con For Cisco Unified Com	nection Administration nunications Solutions	Navigation Cisco Unity Connection Administration 🥪 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 Cluster Authentication Rules Restriction Tables Licenses Schedules Global Nicknames Global Nicknames	<ul> <li>▲ LDAP Authentication Refresh Help</li> <li>Save</li> <li>Status</li> <li>Status</li> <li>Status</li> <li>Status</li> <li>Status</li> <li>Use LDAP Authentication for End Users</li> <li>LDAP Manager Distinguished Name* [fhlab\Administrator</li> <li>LDAP Password*</li> <li>Confirm Password*</li> <li>LDAP User Search Base*</li> <li>Cn=users,dc=fhlab,dc=com</li> </ul>	
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 <sup>®</sup> 10.89.228.226 Add Another Redundant LDAP Server Save Fields marked with an asterisk (*) are required.	Port <sup>*</sup> Use TLS

从分配了语音邮件的LDAP导入用户,以及将用于测试SSO的用户。

Cisco Unity Connection	Import Users				Import L					
E Users ^	Import Users Refresh Help	Import Users Refresh Help								
Users Import Users	c Status	- Chatur								
Synch Users										
E Class of Service	Found 1 LDAP User(s)									
Class of Service Class of Service Membership	Find									
Templates	Find End Users In LDAP Directory	· ~								
User Templates	Where Alias V Begins Wi	th v	Find							
Call Handler Templates										
Contact Templates	_ Import With									
Notification Templates	Based on Template unicemailure	template								
E Contacts		template o								
Contacts										
Distribution Lists	Directory Search Results									
System Distribution Lists	Import Selected Import All	25 V Rows Per Page								
Call Management										
System Call Handlers	Alias 🔺	First Name	Last Name	Phone Number	Extension					
Directory Handlers	hugohugo	hugo	hugo	1002	1002					
Interview Handlers										
Custom Recordings	Import Selected Import All	1								

## 导航到**用户>编辑>角**色,如图所示。

Cisco Unity Connection	r.t.u.	an Bacias (humahuma)			
E Users	Eart Us	er Basics (hugonugo)			
Users	User	Edit Refresh Help			
-Import Users		User Basics	h.		
Synch Users	Save		μ		
E Class of Service	- State	Password Settings	L		
Class of Service		Change Password			
Class of Service Membership		Roles	ectory		
User Templates	Name	Message Waiting Indicators			
Call Handler Templates	Alias*	Transfer Pules			
Contact Templates	E	Transfer Rules	-		
Notification Templates	First N	Message Settings			
Contacts	Last N	Caller Input			
Contacts	Display	Mailbox			
Distribution Lists	SMTP	Phone Menu		@cucpubhcsc.fhlab.com	
System Distribution Lists	Initials	Playback Message Settings		]	
Call Management	This	Playback Hessage Settings	-		
System Call Handlers	litie	Send Message Settings			
Directory Handlers	Employ	Message Actions			
-Interview Handlers		Greetings			
Custom Recordings	LDAP	Post Creation Recording			
E Call Routing	<ul> <li>Int</li> </ul>	Post Greeting Recording			
Message Storage	0.00	Notification Devices			
Mailboy Stores					

#### 为测试用户分配系统管理员的角色。

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		
Class of Service	Roles	
Class of Service	Assigned Roles	
Class of Service Membership		
Templates		
User Templates	M	
Call Handler Templates	A V	
Contact Templates	Available Roles	
Notification Templates	Remote Administrator	
B Contacts	System Administrator	
Contacts	Technican Tenant Administrator	
Distribution Lists	User Administrator V	
System Distribution Lists		
E Call Management	Save	

## CUC元数据

现在,您应该已经下载了CUC元数据,为CUC创建了RelingPartyTrust,并上传了CUC元数据,并 在ADFS 3.0上创建了规则I AD FS



😂 SAML Single Sign on Configuration - Mozilla Firefox	_		$\times$
🛛 🖨 😁 https://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?serverName=	··· 6	ס ₪	≡
SAML Single Sign on Configuration SAML Single	Sign or	n Config	uratior
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. This 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	s test c success dminist	an be ru sful. trator	μn
farfar         hugohugo         2)Launch SSO test page         Run SSO Test			

Sign on Configuration - Mozilla Firefox	-		$\times$				- 0	×
tps://cucpubhcsc. <b>fhlab.com</b> /cuadmin/samlSingleSignOnConfigurationWizard3.do?testStatus	-1 ***	⊠ ⊀	7 ≡			· 🖂 🗘		\$ ≡
ign on Configuration SAML Sing yn on Configuration Refresh Help	gle Sign	on Cor	figuratio		Navigat farfa	ion Cisco Unity Connection Search Documentation	Administration	GO Gign Out
idata Test Successful							SAML Singl	le Sign on
😻 Test SAML - Mozilla Firefox — 🗆	×	]						
Image: SSO Test Succeeded!	=			vers				
				port	Last Metadata Export	SSO Te	st	
Congratulations on a successful SAML SSO configuration test. Ple close this window.	ase			File File	April 28, 2020 5:54:01 PM PDT April 28, 2020 5:54:00 PM	Passed - May 24, 2020 3:17:04 PM PDT Passed - April 29, 2020	Run SSO T	Test
Close				Server	POT	11:05:37 AM POT		
	ign on Configuration - Mozilla Firefox gn on Configuration Refresh Help data Test Successful	ign on Configuration - Mozilla Firefox	ign on Configuration - Mosilla Firefox — □ ↓ ps://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?testStatus=1 *** ♥ ↓ gn on Configuration sAML Single Sign on Con n on Configuration Refresh Help data Test Successful ♥ Test SAML - Mosilla Firefox — □ ↓ ♥ Test SAML - Mosilla Firefox — □ ↓ SSO Test Succeeded! Congratulations on a successful SAML SSO configuration test. Please close this window.	ign on Configuration - Mosilia Firefox — □ × ps://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?testStatus=1 •••	ign on Configuration - Mosilia Firefox - C × ps://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?testStatus=1 •••	ign on Configuration - Mozilla Firefox - □ × pt://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?testStatus=1 *** ⓒ ☆ ≡ •** gn on Configuration Refresh Help for the status of the status o	ign on Configuration - Mozilia Firefox × pro://cucpubhcsc:fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do/testStatus=1 ···· ♥ ♠	ign on Configuration - Modila Firefox ×

# 在Expressway上配置SSO

## 将元数据导入Expressway C

打开浏览器到https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml,并将 元数据保存到本地文件夹

上传到Configuration > Unified Communications > IDP。

## 从Expressway C导出元数据

转至配置 — >统一通信 — > IDP ->导出SAML数据

集群模式使用SAML中包含的自签名证书(具有长生命期)

元数据,用于对SAML请求签名

- 在集群范围模式下,要下载单个集群范围的元数据文件,请点击Download
- 在每对等模式下,要下载单个对等体的元数据文件,请点击对等体旁边的下载。要在.zip文件中 导出所有内容,请点击Download All。

#### 为Cisco Expressway-E添加信赖方信任

首先,为Expressway Es创建信赖方信任,然后添加声明规则以将身份作为UID属性发送。

💠 🔶 🙇 📰 📓 🗊						
🛗 AD FS	Relying Party Trusts					Actions
AD FS  A DFS  Claim Descriptions  Claim Descriptions  A Trust Relationships  Claims Provider Trusts  Attribute Stores  Attribute Stores  Attribute Stores  Attribute Stores  New York Authentication Policies  The following to  Creder Rule  New York Rule  Attribute Store  Attribute Store	Relying Party Trusts           Display Name         Device Registration Service           CUCM_Ouster_Wide_Relying_Party_trust         CUC_Ouster_Wide_Relying_Party_trust           Experiment         Edit Claim Rules for Express           Edit Claim Rules for Express         Issuance Authorization Rules           Issuance Authorization Rules         Deleg           ranaform rules specify the claims that will be sent         Name           eID         uid	Enabled Yes Yes Yes yC gation Authoriz to the relying p Daims	Type WS-Trust / SAI WS-Trust / SAI WS-Trust / SAI WS-Trust / SAI ation Rules party.	AL / WS-Federation AL / WS-Federation AL / WS-Federation AL / WS-Federation AL / WS-Federation AL / WS-Federation AL / WS-Federation which to extract issued from the Claim rule name Claim ru	Identifier       n ummedias ad fitiab.com       n ompublicat fitiab.com       n ompublicat fitiab.com       n units dias ad fitiab.com       n dias ad fitiab.com       <	Actions Relying Party Trusts Add Relying Party Trust. Add Non-Claims-Aware Relying Part View Ule - NameID X DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be Cutgoing Claim Type (Select or type to add more) Uld v
Add Rule	Edt Rule Remove Rule					Go to System in Control Panel to activate Windows.

## OAuth与刷新登录

在Cisco CUCM企业参数中,启用了使用刷新登录流参数验证OAuth。转到**Cisco Unified CM管理 >企业参数> SSO和OAuth配置**。

ſ	-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 🗸	True

## 身份验证路径



• 如果身份验证路径设置为"SAML SSO身份验证",则只有使用启用SSO的Unified CM集群的 Jabber客户端才能在此Expressway上使用MRA。这是仅SSO配置。

- 对所有IP电话、所有网真终端和驻留在未配置SSO的Unified CM集群上的任何Jabber客户端的 Expressway MRA支持将需要身份验证路径以包括UCM/LDAP身份验证。
- 如果一个或多个Unified CM集群支持Jabber SSO,请选择"SAML SSO和UCM/LDAP"以允许 SSO和基本身份验证。

# SSO架构

SAML是基于XML的开放标准数据格式,使管理员能够在登录到其中一个应用后无缝访问一组定义的思科协作应用。SAML SSO使用SAML 2.0协议为思科协作解决方案提供跨域和跨产品单点登录。

#### 本地登录流



Figure :SAML Single sign SSO Call Flow for Collaboration Servers

MRA登录流



#### OAuth

OAuth是支持授权的标准。用户必须经过身份验证才能获得授权。授权码授权流为客户端提供获取 访问和刷新令牌以访问资源(Unified CM、IM&P、Unity和Expressway服务)的方法。此流程也基 于重定向,因此要求客户端能够与用户控制的HTTP用户代理(Web浏览器)交互。客户端将使用 HTTPS向授权服务器发出初始请求。OAuth服务器将用户重定向到身份验证服务。如果启用了 SAML SSO,则此操作可能在Unified CM或外部IdP上运行。根据所使用的验证方法,网页视图可呈 现给最终用户以验证自己。(Kerberos身份验证是不显示网页的示例。)与隐式授权流不同,成功 的身份验证代码授权流将导致OAuth服务器向Web浏览器发出"授权代码"。这是一次性、短暂的唯一 代码,然后从Web浏览器传回客户端。客户端将此"授权代码"连同预共享密钥一起提供给授权服务 器,并接收"访问令牌"和"刷新令牌"交换。此步骤中使用的客户端密钥使授权服务能够将使用限制为 仅允许注册和经过身份验证的客户端使用。令牌用于以下目的:

#### 访问/刷新令牌

访问令牌:此令牌由授权服务器颁发。当客户端需要访问该服务器上的受保护资源时,会将令牌呈 现给资源服务器。资源服务器能够验证令牌并信任使用该令牌的连接。(思科访问令牌默认为60分 钟的生命周期)

刷新令牌:授权服务器再次发出此令牌。当访问令牌过期或到期时,客户端将此令牌连同客户端密 钥一起呈现给授权服务器。如果刷新令牌仍然有效,则授权服务器将发出新的访问令牌,而无需进 行其他身份验证。(思科刷新令牌默认为60天。)如果刷新令牌已过期,则必须启动新的完整 OAuth授权码授权流以获取新令牌。

#### OAuth授权代码授予流程更好

在隐式授权流中,访问令牌通过HTTP用户代理(浏览器)传递到Jabber客户端。 在授权代码授权 流中,访问令牌直接在授权服务器和Jabber客户端之间交换。使用限时唯一授权码从授权服务器请 求令牌。这种访问令牌的直接交换更安全,并降低了风险。

OAuth授权代码授予流支持使用刷新令牌。这为最终用户提供了更好的体验,因为他们不需要像以前那样频繁地重新进行身份验证(默认为60天)

# 配置Kerberos

## 选择Windows身份验证

#### Internet信息服务(IIS)管理器>站点>默认网站>身份验证> Windows身份验证>高级设置。

- 1. 取消选中Enable Kernel-mode authentication。
- 2. 确保"扩展保护"已关闭。



## ADFS支持两个Kerberos NTLM

确保AD FS版本3.0同时支持Kerberos协议和NT LAN Manager(NTLM)协议,因为所有非 Windows客户端都无法使用Kerberos并依赖NTLM。

在右窗格中,选择提供程序,并确保协商和NTLM在已启用的提供程序下:

Vi Internet Information Services (IIS) Manager								
Image: Optimized State     Image: Optimized State								
File View Help								
Connections		Alerts						
🔍 - 🔚   🖄   🔗	Authentication	Click here to learn how to						
Start Page	Group by: No Grouping -				configure Extended Protection.			
AD (FHLAB\administrator)	Name	Status	Response Type	Actions				
⊿ - i Sites	Anonymous Authentication	Enabled		Dishla				
Default Web Site	ASP.NET Impersonation	Disabled	HTTP 302 Login/Redir	Disable	C-11/2-12			
	Windows Authentication	Enabled	HTTP 401 Challenge	Providers	Settings			
		Description		? X				
			Providers					
	Enabled Providers:							
	Negot	iate		Move Up				
	NTLM	NTLM						
				Move Down				
				Remove				
	<							
	Select a provider from the list of available providers and click Add							
Configuration: "Incollection plantic plantic and a star "Default II								
configuration: focarios: application host config, vioca	Availal	ble Providers:			12.220			
			~	Adactiva	ite <b>N2</b> iR2ows			
				Go to Sy	ystem in Control Pa			
			OK	Cancel	Windows Se			

## 配置Microsoft Internet Explorer

确保选中Internet Explorer > Advanced > Enable Integrated Windows Authentication。

Internet C	Options					? 💌		
General	Security	Privacy	Content	Connect	ions Programs	Advanced		
Setting	js —					]		
<ul> <li>Do not submit unknown addresses to your auto-search provide a security</li> <li>Allow active content from CDs to run on My Computer*</li> <li>Allow active content to run in files on My Computer*</li> <li>Allow software to run or install even if the signature is involved to check for publisher's certificate revocation</li> <li>Check for server certificate revocation*</li> <li>Check for signatures on downloaded programs</li> <li>Do not save encrypted pages to disk</li> <li>Empty Temporary Internet Files folder when browser is clear to be provided to the provided tother provided to the provided to the provided to the provide</li></ul>								
*Takes effect after you restart Internet Explorer								
Restore advanced settings								
Reset Internet Explorer settings								
Resets Internet Explorer's settings to their default Reset								
			OK		Cancel	Apply		

在"安全">"内部网区域">"站点"下添加ADFS URL