Configurar SAML SSO no Cisco Unified Communications Manager com ADFS 3.0

Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Pré-verificação da configuração A Records Registros de Ponteiro (PTR) É necessário que os registros SRV estejam em vigor para o Jabber Discovery Services Configuração inicial do ADFS3 Configurar SSO no CUCM com ADFS Configuração LDAP Metadados do CUCM Configurar entidade confiadora do ADFS Metadados IDP Configurar SSO no CUC Metadados CUC Configurar SSO no Expressway Importar metadados para o Expressway C Exportar Metadados Do Expressway C Adicione uma confiança de terceira parte confiável para o Cisco Expressway-E OAuth com login de atualização Caminho de autenticação Arquitetura SSO Fluxo de login no local Fluxo de login de MRA OAuth Token de acesso/atualização O fluxo de concessão do código de autorização OAuth é melhor **Configurar Kerberos** Selecionar autenticação do Windows O ADFS suporta o Kerberos NTLM Configurar o Microsoft Internet Explorer Adicione o URL do ADFS em Segurança > Zonas de Intranet > Sites Adicione nomes de host CUCM, IMP e Unity a Security > Trusted Sites Autenticação de usuário Login no Jabber em SSO Troubleshoot Internet Explorer (IE)

<u>Sites Adicionando ao IE</u> <u>Problema Fora de Sincronização</u> <u>Revogar um Token</u> <u>Arquivo de bootstrap</u> SSO com falha devido ao MSIS7066

Introduction

Este documento descreve as etapas para configurar o Single Sign-On com o Ative Diretory Federation Service (ADFS 3.0) com o uso do Windows 2012 R2 nos produtos Cisco Unified Communication Manage (CUCM), Cisco Unity Connection (CUC) e Expressway. As etapas para configurar o Kerberos também estão incluídas neste documento.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento dos produtos Single Sign-On (SSO) e Windows.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CUCM 11.5
- CUC 11.5
- Expressway 12
- Windows 2012 R2 Server com as seguintes funções:
 - Serviços de Certificados do Ative Diretory
 - Serviços de Federação do Ative Diretory

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Pré-verificação da configuração

Antes de instalar o ADFS3, estas funções de servidor já precisam existir no ambiente:

Domain Controller e DNS

Todos os servidores devem ser adicionados como Registros A junto com seu Registro de Ponteiro (um tipo de registro DNS que resolve um endereço IP para um domínio ou nome de host)

A Records

Em fhlab.com. os hosts cmpubhcsc, cmsubhcsc, cucpubhcsc, cucsubhcsc, expwyc, exwye,

impubhcsc e imsubhcsc foram adicionados.



Registros de Ponteiro (PTR)

🛔 DNS	Name	Туре	Data	Timestamp
⊿ 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
Dura Contraction	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 Beverse Lookun 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

Énecessário que os registros SRV estejam em vigor para o Jabber Discovery Services

🛔 DNS	Name	Туре	Data	Tir	mestamp	
A D	_cisco-uds	Service Location (SRV)	[0][0][8443] cmsubhcsc.fhl	ab.com. sta	ıtic	
a 🧮 Forward Lookup Zones	_cisco-uds	Service Location (SRV)	[0][0][8443] cmpubhcsc.fhl	ab.com. sta	itic	
[] _msdcs.fhlab.com	cuplogin	Service Location (SRV)	[0][0][8443] impsubhcsc.fh	lab.com. sta	tic	
⊿ 👸 fhlab.com	cuplogin	Service Location (SRV)	[0][0][8443] imppubhcsc.fh	lab.com. sta	tic	
b 🛐 _msdcs	gc	Service Location (SRV)	[0][100][3268] ad.fhlab.com	n. 5/1	12/2020 10:00:00 AM	
b	kerberos	Service Location (SRV)	[0][100][88] ad.fhlab.com.	5/1	12/2020 10:00:00 AM	
_tcp	kpasswd	Service Location (SRV)	[0][100][464] ad.fhlab.com.	5/1	12/2020 10:00:00 AM	
þ udp	Idap	Service Location (SRV)	[0][100][389] ad.fhlab.com			
DomainDisZones					_cisco-uds Properties	? X
A PorestUnszones				Control continue (000.0	
psites				Service Location (3	Security Security	
A C Reverse Lookup Zoper				Domain	fhlab.com	
228.89.10.in-addr.am				Coman.		
b Trust Points				Service:	_cisco-uds	~
Conditional Forwarders				Destaurali	-	
b 🔂 Global Logs				PTOLOCOL	Ticb	~
				Priority:	0	
				Weight:	U	
				Port number:	8443	
				Host offering this	service:	
				cmpublicsc fhlab	.com.	

• CA raiz (supondo que os certificados sejam assinados pela AC empresarial)

Um Modelo de Certificado precisa ser criado com base no Modelo de Certificado do Servidor Web, o primeiro é duplicado, renomeado e, na guia Extensões, as Políticas de Aplicativo são modificadas adicionando uma Política de Aplicativo de Autenticação de Cliente. Este modelo é necessário para assinar todos os certificados internos (CUCM, CUC, IMP e Expressway Core) em um ambiente de LAB, a CA interna também pode assinar as Solicitações de Assinatura de Certificado (CSR) do Expressway E.

Certificate Templates (AD.fhlab.	Template Display Name	Schem	a Version Versi Int Actions	
	CEP Encryption	1	Properties of New Template X	· · · · · · · · · · · · · · · · · · ·
	ClientServerAuth	2		
	Code Signing	1	Subject Name Server Issuance Requirements	istrative Tools
	Computer 2	1	Compatibility General Request Handling Cryptography Key Attestation	Edit Application Deligion Extension
	Cross Certification Authority	2	Superseded Templates Extensions Security	Edit Application Policies Extension
	Directory Email Replication	2	To modify an extension, select it, and then click Edit.	An application policy defines how a certificate can be
	Domain Controller	1		used.
	Domain Controller Authentication	2	Extensions included in this template:	
	EFS Recovery Agent	1	Application Policies	Application policies:
	Enrollment Agent	1	Basic Constraints	Client Authentication
	Enrollment Agent (Computer)	1	Certificate Template Information	Server Authentication
	Exchange Enrollment Agent (Offline requ	1	Issuance Policies	
	Exchange Signature Only	1	Key Usage	
	Exchange User	1		
	2 IPSec	1		
	IPSec (Offline request)	1	Edt	
	Kerberos Authentication	2		
	Key Recovery Agent	2	Description of Application Policies:	Add Edit Remove
	OCSP Response Signing	3	Server Authentication	
	RAS and IAS Server	2	Client Authentication	Make this extension chocal
	Root Certification Authority	1		

O modelo criado precisa ser emitido para poder assinar o CSR.



Na Web do certificado CA, selecione o modelo que foi criado anteriormente.

Microsoft Active	Directory Certificate Services fhlab-AD-CA	
Submit a Cert	ificate Request or Renewal Request	
To submit a sav Web server) in	ved request to the CA, paste a base-64-encoded C the Saved Request box.	CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external sour
Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	8V8mWY/9kjhqfnpeBzAAW++tolGzBjnvqaT8StWM LA0dphF6LrurU0Y2KLvMLmKlft7aSy483yCsm0v1 OWQPZoLb3bS80ziW7fqEFWSaCg567DMOQ8FkZt5N 10y/Ip6oDzfdZE9w2p8rK3YxccbypovSt0ij1irh AM/Gjnz0 END CERTIFICATE REQUEST	
Certificate Templ	late:	
Additional Attribu	V User Basic EFS Administrator EFS Recovery Agent Web Server	

Attributes:

Subordinate Certification Authority

CUCM, IMP e CUC Multi-Server CSR devem ser gerados e assinados pela CA. A finalidade do certificado deve ser tomcat.

Generate Certificate Signing I	Request	
🔒 Generate 🖳 Close		
Status		
Warning: Generating a	new CSR for a specific certificate type will overwrite the e	xisting CSR for that type
Generate Certificate Signing	g Request	
Certificate Purpose**	tomcat	
Distribution*	Multi-server(SAN)	
Common Name*	cmpubhcsc-ms.fhlab.com	
Subject Alternate Names (S	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* Hash Algorithm*	RSA 2048 V SHA256 V	Add

O certificado raiz da CA deve ser carregado para o Tomcat Trust e o certificado assinado para tomcat.

cisco For Ci	sco Unified Communications	Solutions	ninistrat	ion		Navi	sadmin Search Documentation About L
how - Settings -	Security · Software Upgrades	· Services · Help	•				
ertificate List							
Connecto Salt ala	and D Habard Continues Continues	ata chain 🛐 Garacet					
0	per	are chain 60 deneral	e con				
 7 records foun 	vd						
Certificate List	(1 - 7 of 7)						Rows per Page 50
ind Certificate List	where Certificate v begi	ins with $\ arphi$ torncat		Find Clear Filter	4 -		
Contillante *	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
mcat	cmoubhcsc-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/18/2022	Certificate Signed by fhlab-AD-CA
mcat-ECDSA	cmoubhcsc-EC.thlab.com	Self-signed	EC	cmpubhcsc.thlab.com	cmpubhcsc-EC.thlab.com	04/02/2025	Self-signed certificate generated by system
mcat-trust	imppublicsc-EC.fhlab.com	Self-signed	EC	imppublicsc.fhlab.com	imppublicsc-EC.fhlab.com	04/02/2025	Trust Certificate
mcat-trust	cmsubhcsc-EC.fhlab.com	Self-signed	EC	cmsubhcsc.fhlab.com	cmsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate
mcat-trust	imosubhcsc-EC.fhlab.com	Self-signed	EC	impsubhcsc.fhlab.com	impsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate
and head	emoshkeen EC Blak com	Eall signed	50	emashhara fhish asm	emashhere EC filsh com	04/03/3035	Tout Cadificate
omcat-trust	fhlab-AD-CA	Self-signed	RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate
Generate Self-sig	pned Upload Certificate/Certil	ficate chain Genera	ate CSR				
-							
Certificate List	(1 - 6 of 6)						Rows per Page
ind Certificate List	where Certificate v begi	ins with $\ \bigtriangledown$ torncet		Find Clear Filter	4 -		
Contificate *	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
mcat	cucoubhose-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/28/2022	Certificate Signed by fhlab-AD-CA
	and a state of the second	********		and the second state and second	Contraction and the second		And a second and the second sector second sectors
mcat-trust	fhlab-AD-CA	Self-signed	RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate
THOM OF MAN	Sector and the sector sector sector	CH Agrico	1000	Here server(ever)	INGO AD CA		A structo Mindows
taund-brush	cucsubhcsc-EC.fhlab.com	Self-signed	EC	cucsubhcsc.fhlab.com	cucsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate te Windows
annound of stars							

• IIS

Caso contrário, esta seção passará pela instalação dessas funções. Caso contrário, ignore esta

seção e continue diretamente com o download do ADFS3 da Microsoft.

Depois de instalar o Windows 2012 R2 com DNS, promova o servidor para um controlador de domínio.

A próxima tarefa será instalar o Microsoft Certificate Services.

Navegue até Gerenciador de servidores e adicione uma nova função:



Selecione a função Serviços de Certificados do Ative Diretory.



E implante esses serviços - Serviço Web de Política de Registro de Certificado da Autoridade de Certificação primeiro. Depois que essas duas funções forem instaladas, configure-as e instale o **Serviço Web de Inscrição de Certificados** e **Inscrição na Web de Autoridade de Certificação**. Configure-os.

Os serviços e recursos de função adicionais necessários, como o IIS, também serão adicionados quando a Autoridade de Certificação estiver instalada.

Dependendo da sua implantação, você pode selecionar Empresa ou Independente.

Add Roles Wizard	×
Specify Setup Ty	pe
Before You Begin Server Roles AD CS Role Services Setup Type CA Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Veb 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

Para o tipo de CA, você pode selecionar CA raiz ou CA subordinada. Se não houver outra CA já em execução na organização, selecione **CA raiz**.

Add Roles Wizard		×
Specify CA Type		
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	 A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKQ). 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. 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	

A próxima etapa é criar uma chave privada para sua CA.



Esta etapa só é necessária se você instalar o ADFS3 em um Windows Server 2012 separado.

Depois de configurar a AC, os serviços de função do IIS precisam ser configurados. Isso é necessário para a inscrição na Web na CA. Para a maioria das implantações de ADFS, é necessária uma função extra no IIS, clique em **ASP.NET** em Desenvolvimento de Aplicativos.



No Server Manager, clique em **Web Server > IIS** e, em seguida, clique com o botão direito do mouse em **Default Web Site**. A associação precisa ser alterada para permitir também HTTPS além do HTTP. Isso é feito para suportar HTTPS.



Selecione Editar vínculos.

8]	Interne	et Informatio	n Services	(IIS) Manage	er		_	
AD > Sites > Default Web Si	te 🕨						10 8	1 in 10 •
File View Help								
Connections		fault Malak	Cite He				Actions	
🔍 • 🗟 🖄 😣		erault web	Site Ho	me			🔉 Explore	^
Start Page	Filter		• 7 Go -	Show All	Group by:		Edit Permissions	
AD (FHLAB\administrator)	ASP.NET					A A	Edit Site	
a 😧 Sites	E0	1	404	٠			Bindings Basic Settings	
Explore		.NET Compilation	.NET Error Pages	.NET Globalization	.NET Profile	=	View Applications View Virtual Direct	ories
Add Application		- internet - 1	- <u>68</u> -	3	ab		Manage Website	
Add Virtual Direc	tory s	.NET Trust	.NET Users	Application	Connection		💈 Restart	-
Edit Bindings		Leves	<u></u>	Secongs	oungs		Start	
Manage Website	•		198	8÷	1		Browse Website	
22 Refresh	9	y Pages and Controls	Providers	Session State	SMTP E-mail		Browse *:80 (http)	
× Remove		controla					Browse *:443 (http	s)
Rename			<i>.</i>		and the second	^	Advanced Setting:	kaa l
Switch to Conter	nt View	<u> </u>	Z	0	Ш <u>О</u>	~	Configure	
	Features V	iew 💦 Conten	t View				J Failed Request Tra Limits	cing
Ready								•1.:

Adicione uma nova associação de site e selecione **HTTPS** como o tipo. Para o certificado SSL, escolha o certificado do servidor que deve ter o mesmo FQDN do seu servidor AD.

e j			Intern	et Informatior	n Services (IIS) Manager	
💽 💿 💊 🕨 🖌 AD 🕨	Sites + D	efault Web Site	•			
File View Help						
Connections				Site	Bindings	? X
Image Image Image AD (FHLAB\admini Image AD (FHLAB\admini Image AD (FHLAB\admini Image AD (FHLAB\backson Poc Image Image Image	Type http https	Host Name Type: https Host name: Require S SSL certifica fhlab-AD-C Not selected fhlab-AD-C AD.fhlab.co	Port 80 442 I Server Name te: A d A m	IP Address * Edit P address: All Unassigned	Binding Informa Site Binding Port: 443 Select OK	Add Fdit X View Cancel

Todas as funções de pré-requisito estão instaladas no ambiente, por isso agora pode continuar com a instalação dos Serviços de Federação do Ative Diretory do ADFS3 (no Windows Server 2012).

Para a Função de Servidor, navegue para Server Manager > Manage > Add Server Roles and Features e selecione Ative Diretory Federation Services se você instalar o IDP dentro da rede do cliente, na LAN privada.



	Add Roles and Features Wizard	
elect server roles		DESTINATION SERVER AD filab.com
Before You Begin	Select one or more roles to install on the selected server.	
Installation Type	Roles	Description
Server Selection		Active Directory Federation Services
Server Roles	Active Directory Certificate Services (4 of 6 installe	(AD FS) provides simplified, secured
Features	Active Directory Domain Services (Installed)	identity federation and Web single sign-on (SSO) canabilities, AD ES
	Artiva Directory Linktwaicht Directory Camicar	includes a Federation Service that
	Active Directory Eights Management Services	enables browser-based Web SSO.
	Application Server	
	DHCP Server	
	DNS Server (Installed)	
	Fax Server	
	File and Storage Services (2 of 12 installed)	
	Hyper-V	
	Network Policy and Access Services	
	Print and Document Services	
	Remote Access	
	< III >	

Quando a instalação for concluída, você poderá abri-la na barra de tarefas ou no menu Iniciar.



Configuração inicial do ADFS3

Esta seção passará pela instalação de um novo servidor de Federação independente, mas também poderá ser usada para instalá-lo em um Controlador de Domínio

Selecione **Windows** e digite **Gerenciamento do AD FS** para iniciar o console de Gerenciamento do ADFS como mostrado na imagem.



Selecione a opção **Assistente de Configuração do Servidor de Federação do AD FS 3.0** para iniciar a configuração do servidor ADFS. Essas capturas de tela representam as mesmas etapas no AD FS 3.

D F5 2.0 Federation Serv	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 viscard 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 selectation server. An instance of AD FS is referred to as a sever fam. 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. Ad a federation server to an existing Federation Service Select this option to join this computer to an existing federation server fam. 	
	Kext> Cancel Help	

Selecione Criar um novo Serviço de Federação e clique em Avançar.

AD FS 2.0 Federation Ser	ver Configuration Wizard	×
Select Stand-Alone or	r Farm Deployment	
Steps	You are cente aller a stand done federation are or for such ation propagation are small reachation.	
Welcome	environment, or you can create a federation server to evaluation purposes of a smart production 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	
	< <u>Previous</u> <u>Next</u> > Cancel <u>H</u> elp	

Selecione o Servidor de Federação Independente e clique em **Avançar** conforme mostrado na imagem.

Mathematical Serversion Serve	er Configuration Wizard				×
Specify the Federation	Service Name				
Steps Welcome Select Deployment Type Federation Service Name	This wizard determines the Federation Servi Default Web Site. If the wizard cannot dete must select a certificate. Select the certificate and/or port, and then o	ce name from t rmine the Fede click Next.	ne Subject field of ration Service nar	the SSL certific ne from the SSL	ate for the settings, you
 Summary Results 	SSL certificate: ad0a.identitylab.us ad0a.identitylab.us What kind of certificate do I need?	· ·	View	uft: 43 ↔	
		< Previous	Next >	Cancel	Help

Em certificado SSL, selecione o certificado autoassinado na lista. O nome do Serviço de Federação será preenchido automaticamente. Clique em Next.

Welcome	The following settings will be configured for AD FS 2.0:									
Select Deployment Type	 Stop AD FS server. Windows Internal Database service will be started and set to automatic startup. 									
 Select Deployment Type Federation Service Name Summary 	 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 correcting tion. 									
	 Network Service account will be given access to the database, to the certificate private keys and endroption and the service account will be given access to the database. 									
	 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 ad0a.identitylab.us Start AD FS server. 									
	To begin contiguring this computer with these settings, click Next.									

Revise as configurações e clique em **Avançar** para aplicar as configurações.

otope	The following settings are being contigured	
 Welcome Select Deployment Type Federation Service Name Summary Results 	Component Install Windows Internal Database Install Windows Internal Database Treate AD FS configuration database Configure service settings Deploy browser sign-in Web site Treate default claim set Create default Active Directory claim acceptance rul You have successfully completed the AD FS 2.0 Federa To close this wizard, click Close.	Status Configuration finished

Confirme se todos os componentes foram concluídos com êxito e clique em **Fechar** para encerrar o assistente e retornar ao console de gerenciamento principal. Isso pode levar alguns minutos.



O ADFS agora está efetivamente ativado e configurado como um provedor de identidade (IdP). Em seguida, você precisa adicionar o CUCM como um parceiro confiável. Antes de fazer isso, é necessário primeiro fazer alguma configuração na Administração do CUCM.

Configurar SSO no CUCM com ADFS

Configuração LDAP

O cluster precisa ser integrado ao LDAP com o Ative Diretory e a autenticação LDAP precisa ser configurada antes de prosseguir. Navegue até a **guia Sistema > Sistema LDAP** conforme mostrado na imagem.

LDAP System Configuration

Status								
Status								
Please Delete All LDAP Directories Before Making Changes on This Page								
i Please Disable LDAP A	uthentication Before Making Changes on This Page							
LDAP System Informatio	n							
🗹 Enable Synchronizing fr	om LDAP Server							
LDAP Server Type	Microsoft Active Directory	•						
LDAP Attribute for User ID	sAMAccountName	٥						

Em seguida, navegue até a guia Sistema > Diretório LDAP.

LDAP Directory	LDAP Directory							
🔚 Save 🗙 Delete 🗋 Copy 隆	Perform Full Sync Now 🚽 Add New							
Status Status: Ready								
LDAP Directory Information								
LDAP Configuration Name*	DAP1							
LDAP Manager Distinguished Name* fh	lab\administrator							
LDAP Password*								
Confirm Password*								
LDAP User Search Base* cn	=users,dc=fhlab,dc=com							
LDAP Custom Filter for Users	< None >							
Synchronize*	Users Only 🔵 Users and Groups							
LDAP Custom Filter for Groups	< None >							
LDAP Directory Synchronization Sch	nedule							
Perform Sync Just Once								
Perform a Re-sync Every*	7 DAY 🗘							
Next Re-sync Time (YYYY-MM-DD hh:m	m)* 2020-05-24 00:00							

Standard User Fields To Be Synchronized —					
Cisco Unified Communications Manager User Fields	LDAP Attribute	Cisco Unified C	Communications Man	ager User Fields	LDAP Attribute
User ID	sAMAccountName	First Name			givenName
Middle Name	middleName 😳	Last Name			sn
Manager ID	manager	Department		department	
Phone Number	telephoneNumber 😋	Mail ID			mail
Title	title	Home Numbe	e e e e e e e e e e e e e e e e e e e		homephone
Mobile Number	mobile	Pager Number	r		pager
Directory URI	mail	Display Name	1		displayName
LDAP Server Information	ee for Conuer*		IDAR Bost*		
Host Name of IP Addre	iss for Server		LUAP POR	Use ILS	
10.89.228.226			389		
Add Another Red	undant LDAP Server				
Save Delete Co	py Perform Full Sync Now Add New				

Após os usuários do Ative Diretory terem sido sincronizados com o CUCM, a autenticação LDAP precisa ser configurada.

ob	alo	Cisc	o U	nifi	ed (M /	\dm	inis	tra	tion	1												Na	vigatio	n Cis	ico Ur	nified (M Adm	inistratio	n	√ Go
cit	co	For Ci	sco U	Inifie	d Con	muni	catio	ns Sol	ution	15														far	far	Se	arch D	ocumer	tation	About	Logout
System	•	Call Routin	9 *	Media	Resou	rces +	Adv	ranced	Featur	es 🕶	Devi	ce 🕶	Appl	ication .	U	ser Mana	pement .	Bu	& Administration	- 1	Help 👻										
LDAP	Aut	henticati	ion																												
	Save																														
Stat																															
1	Statu	is: Ready																													
LDA	P Aut	henticat	tion f	or Er	d Use	rs -																									
Ø	se LC	AP Authe	inticat	ion fe	r End	Users																									
LDA	Man	ager Disti	inguis	hed f	ame*	fhlab	Admi	nistrat	or																						
LDA	Past	* brows				••••	••••	•••••	•••••	••••	••••	••••	•••••	••••																	
Conf	irm P	assword*	·			••••	••••	•••••	•••••	••••	••••	••••	•••••	••••																	
LDAS	User	r Search I	Base*			cn=u	sers,d	c=fhla	b,dc=	com			_																		
LDA	Ser	ver Info	rmat	ion -																											
					Ho	t Nam	e or I	P Add	ress fr	or Ser	ver*							ort"	Use TLS												
10	89.23	28.226															389														
A	dd Ar	other Re	dunda	int LD	AP Se	wer																									

Um usuário final no CUCM precisa ter determinados grupos de controle de acesso atribuídos ao seu perfil de usuário final. O ACG é o padrão para superusuários do CCM. O usuário será usado para testar o SSO quando o ambiente estiver pronto.

End Use	r Configuration	Related Links: Back to Find List Users 🧹	Go
Sav	e 🗙 Delete 👍 Add New		
Confirm MLPP Pr	MLPP Password	~	^
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	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 	
Confer	ence Now Information		
Meeting Attende	Number 1001 es Access Code		
Save	Delete Add New		

Metadados do CUCM

Esta seção mostrará o processo para o Editor do CUCM.

A primeira tarefa é obter os metadados do CUCM, para o que você precisa navegar até a URL; https://<CUCM Pub FQDN>:8443/ssosp/ws/config/metadados/sp ou pode ser baixado da guia System > SAML Single Sign-on. Isso pode ser feito por nó ou por cluster. Preferível fazer este cluster inteiro.

SAML Single Sign-On							
SSO Mode							
Cluster wide (One me	etadata file per clu	ster. Requires multi-serv	ver Tomcat certificate)				
O Per node (One metad	lata file per node)						
🗙 Disable SAML SSO 🧯	È Export All Metada	ta 🔞 Update KIP Metadi	ata File 🧳 Fix All Disabled Servers				
Status							
(i) RTMT is enabled for	r SSO. You can cha	ange SSO for RTMT here	L				
RTMT is enabled for SAML SSO enabled	r SSO. You can che	ange SSO for RTMT <u>here</u>	L.				
RTMT is enabled for SAML SSO enabled SAML Single Sign-On	r SSO. You can che (1 - 4 of 4)	ange SSO for RTMT <u>here</u>	L				Rows per Page 50
RTHT is enabled for SAML SSO enabled SAML Single Sign-On Server Name	(1 - 4 of 4)	nge SSO for RTMT here	Last Metedata Import	Export Metadata	Last Metadata Export	SSO Test	Rows per Page 50
RTMT is enabled for SAML SSO enabled SAML Single Sign-On Server Name cmpubhcsc.fhlab.com	r SSO. You can che (1 - 4 of 4) SSO Status SAML	Re-Import Metadata	Lest Metadata Import April 20, 2020 2:00:57 PM PDT	Export Metadata	Lest Metadate 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	r SSO. You can cha (1 - 4 of 4) SSO Status SAML SAML	Re-Import Metadata N/A MP IdP	Last Metadata Import April 20, 2020 2:00:57 PM PDT April 20, 2020 2:00:57 PM PDT	Export Metadata È File File	Last Metadeta Export April 18, 2020 8:05:38 PM PDT April 18, 2020 8:05:37 PM PDT	550 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 Single Sign-On Server Name cmpubhcsc.fhlab.com mppubhcsc.fhlab.com	r SSO. You can che (1 - 4 of 4) SSO Status SAML SAML SAML	Re-Import Metadata N/A M IdP 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 Metadate File File File File	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 Text 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 SSO Test. Run SSO Test. Run SSO Test.

Salve os dados localmente com um nome significativo como sp_cucm0a.xml, você precisará deles depois.

Configurar entidade confiadora do ADFS

Volte para o console de gerenciamento do AD FS 3.0.



Clique no Assistente para Adicionar Confiança de Terceiros Confiantes.

\$	Add Relying Party Trust Wizard
Welcome	
 Steps Welcome Select Data Source Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish 	<section-header><section-header><text><text></text></text></section-header></section-header>

Clique em Iniciar para continuar.

Selecione o arquivo XML de metadados **federationmedatada.xml** que você salvou anteriormente e clique em **Avançar**.

\$	Add Relying Party Trust Wizard
Select Data Source	
 Steps Welcome Select Data Source Configure Multi factor 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 is federation metadata online or on a local network. 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 fle Use this option to import the necessary data and certificates from a relying party organization that has evoluted to federation metadata to a fle. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Rederation metadata file location: Exture that about the relying party manually Use this option to manually input the necessary data about this relying party organization. Browse
	Chevious (in Marcalien)

Use **CUCM_Cluster_Wide_Relying_Party_trust** como o nome de exibição e clique em **Avançar**.

\$	Add Relying Party Trust Wizard
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?	<u>^</u>
 Choose Issuance Authorization Rules 	
 Ready to Add Trust 	
 Finish 	×
	< Previous Next & Ctive Canitel in d

Selecione a primeira opção e clique em Avançar.

\$	Add Relying Party Trust Wizard	X
Steps Welcome	Configure multi-factor authentication settings for this relying party trust. Multi-factor authentices a match for any of the specified requirements.	intication is required if
 Select Data Source Specify Display Name 	Multi-factor Authentication	Global Settings
Configure Multifactor 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 multifactor authentication settings for this relying party true Configure multifactor authentication settings for this relying party trust. You can also configure multi-factor authentication settings for this relying party trus Authentication Policies node. For more information, see <u>Configuring Authentication</u>	st at this time. t by navigating to the <u>Policies</u> .
	< Previous Next	ActivatCanpelindo

Selecione **Permitir que todos os usuários acessem esta terceira parte confiável** e clique em **Avançar** conforme mostrado na imagem.

\$	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 & ct Va (Canbel in do

Revise a configuração e clique em Avançar conforme mostrado na imagem.

\$	Add Relying Party Trust Wizard
Ready to Add Trust	
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 Avext > at Cancel / S

Desmarque a caixa e clique em Fechar.

\$	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	

Com o botão do mouse secundário, selecione a **Confiança da terceira parte confiável** que você acabou de criar e **edite a** configuração **das regras de reivindicação**, como mostrado na imagem.

\$			AD I	S		
翰 File Action View Windo	w Help					
🗢 🄿 🖄 📰 🚺 🗊						
AD FS	Relying Party Trusts					
Service	Display Name		Enabled	Туре		Identifier
Irust Relationships	Device Registration S	Service	Yes	WS-Trust / SAM	IL / 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
Kelying Party Trusts Attribute Stores	CUC_Cluster_W	Update from Fede	eration Meta	data	L / WS-Federation	cucpubhcsc.fhlab.com
	ExpwyC	Edit Claim Rules			L / WS-Federation	fhlab.com500D0F4107D76E57
		Disable				
		Properties				
		Delete				
		Help				
						1

Clique em Adicionar regra conforme mostrado na imagem.

Name and the second sec	×
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules	
The following transform rules specify the claims that will be sent to the relying party.	
Order Rule Name Issued Claims	
Add Rule Edit Rule Remove Rule	
	_
OK Cancel Apply	

Selecione Enviar atributos LDAP como reivindicações e clique em Avançar.

\$	Add Transform Claim Rule Wizard	X
Select Rule Template		
Steps	Select the template for the claim rule that you want to create from the following list. The description provide details about each claim rule template	s
Choose Rule Type		
 Contigure 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 telephoneNumbe 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.	н аг о
	< Previous Next > Cancel	

Configure estes parâmetros:

Nome da regra de reivindicação: NameID

Repositório de atributos: Ative Diretory (clique duas vezes na seta do menu suspenso)

Atributo LDAP: SAM-Account-Name

Tipo de solicitação de saída: uid

Clique em FINISH/OK para continuar.

Observe que o uid não está em minúsculas e ainda não existe no menu suspenso. Digite.

	Edit R	ule - NameID
You car which to issued fr	n configure this rule to send the values of L o extract LDAP attributes. Specify how the rom the rule.	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be
Claim ru	le name:	
NamelD	1	
Rule ter	nplate: Send LDAP Attributes as Claims	
Attribute	store:	
Active I	Directory	¥
Mapping	g of LDAP attributes to outgoing claim type	s:
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
•	SAM-Account-Name V	uid 🗸
*	~	×
View F	Rule Language	OK Cancel

Clique em Adicionar regra novamente para adicionar outra regra.

💱 Edit Claim	Rules for CUCM_Clust	er_Wide	_Relying_Party	- - X
Issuance Transf	orm Rules Issuance Authoriza	tion Rules	Delegation Authorization	n Rules
The following	transform rules specify the claim	ns that will b	e sent to the relying party	
Order Rule	e Name	k	ssued Claims	
1 Nan	nelD	U	id	
				*
Add Bule	Edit Rule Remove	Bule		-
10011010		110101		
		OK	Cancel	Apply

Selecione Enviar reivindicações usando uma regra personalizada e clique em Avançar.

\$	Add Transform Claim Rule Wizard
Select Rule Template	
Steps Ghoose Rule Type Configure Claim Rule	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:
	 ✓ ✓ ✓ 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: Sending claims from a SQL attribute store Sending claims from a custom attribute store using a custom LDAP filter Sending claims only when 2 or more incoming claims are present Sending claims only when an incoming claim value matches a complex pattern Sending claims for use only in later rules Oreating claims for use only in later rules
	< Previous Next > Cancel

Crie uma regra personalizada chamada Cluster_Side_Claim_Rule.

Copie e cole este texto na janela de regras diretamente daqui. Às vezes, os orçamentos são alterados se forem editados em um editor de texto e isso fará com que a regra falhe quando você testar o SSO:

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>
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
<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>
<pre>"<cucm fqdn="" pub="">");</cucm></pre>
c:[Type == " <u>http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname</u> "]
<pre>=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",</pre>
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
<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/namegualifier"] =</pre>
" <u>http://AD.fhlab.com/adfs/services/trust</u> ",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =

"cmpubhcsc.fhlab.com");

Clique em **Concluir** para continuar.

9	Add Transform Claim Rule Wizard	2
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	
	<pre>cusum nue: 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 "] = "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/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	

Agora você deve ter duas regras definidas no ADFS. Clique em Aplicar e em OK para fechar a janela de regras.

💱 Edit C	laim Rules fo	or CUCM_Clu	ster_Wid	e_Relying_Party	- • ×
Issuarice	Iransform Hules	Issuance Author	zation Hules	Delegation Authoriza	tion Hules
The folk	owing transform n	les specify the cla	sims 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	Aule Edt F	Remo	ve Rule		 ♠
			0	K Cancel	Apply

O CUCM foi adicionado com êxito como uma parte confiável ao ADFS.

9		Service	5				x
File Action View	Help						
🕈 🔿 🔝 🖬 🖬	🗟 📓 🔳 🕨 🖬 🕪						
Services (Local)	Services (Local)						
	Active Directory Federation Services	Name Active Directory Certificate Services Active Directory Domain Services	Description Creates, manages, and removes AD DS Domain Controller servic	Status Running Running	Startup Type Automatic Automatic	Log On As Local System Local System	^ II
	Stop the service Restart the service	Active Directory Federation Services	Enables Active Directory Federa	Running	Automatic (Delayed Start)	FHLA8\administra	tor
	Description: Enables Active Directory Federation Services to issue security tokens.	Active Directory Web Services App Readiness Application Experience Application Host Helper Service Application Information Application Information Application Layer Gateway Service Background Intelligent Transfer Service Background Tasks Infrastructure Service Getificate Propagation COM + Event System COM + System Application Computer Browser <	This service provides a Web Ser Gets apps ready for use the first Processes application compatib Provides administrative services Determines and verifies the ide Facilitates the running of intera Provides support for 3rd party p Processes installation, removal, Provides infrastructure support Provides support for out-of-pro Transfers files in the backgroun Windows infrastructure service The Base Filtering Engine (BFE) i Copies user certificates and roo The CNG key isolation service is Supports System Event Notifica Manages the configuration and Maintains an updated list of co	Running Running Running Running Running Running Running	Automatic Manual (Trigger Start) Automatic Manual (Trigger Start) Manual (Trigger Start) Manual Manual Manual Manual Automatic Automatic Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Manual Disabled	Local System Local System	v
	(Extended / Standard)				Letiusto Mindauu		_
				ŀ	Activate Windows		_

Antes de continuar, reinicie o serviço ADFS. Navegue até **Menu Iniciar > Ferramentas** Administrativas > Serviços.

Metadados IDP

Você precisa fornecer ao CUCM informações sobre nosso IdP. Essas informações são trocadas usando metadados XML. Certifique-se de executar esta etapa no servidor onde o ADFS está instalado.

Firefox T		_ 🗆 🗡
🔔 Untrusted Connection 🛛 🗙 😻 Mozilla Firefox Start Page 🛛 🛛	+	
🗲 🕲 ɔs://ad0a.identity 💫.us/FederationMetadata/2007-06/FederationMetadate 🏠 🔻 C	🛚 = Google 🛛 🔎 🔣 =	+ 🏦
Most Visited Getting Started Suggested Sites Web Slice Gallery		
Opening FederationMetadata.xml	but we can't confirm that your	<u> </u>
You have chosen to open:	dentification to prove that you ed.	
FederationMetadata.xml which is: XML Document from: https://ad0a.identitylab.us What should Firefox do with this file? Open with Internet Explorer (default) Save File Do this gutomatically for files like this from now on. OK Cancel Don't add an exception unless you know there's a good reason why the identification. Add Exception_	an that someone is trying to g this site's identification. Even ampering with your his site doesn't use trusted	
		-

Primeiro, você precisa se conectar ao ADFS (IdP) usando um navegador Firefox para baixar os metadados XML. Abra um navegador em https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml e SALVE os metadados em uma pasta local.

Agora, navegue até a configuração do CUCM até o **menu** do sistema **> menu de logon único SAML**.



Volte para a Administração do CUCM e selecione SYSTEM > SAML Single Sign-On.

Firefox *					_ [] ×
End and List Users	× # SAML Single Sign-On	× End and List LDAP Directories	× +		
+ https://cucm0a/ccmadmin/sami5i	ngleSignOn.do	습·	7 C ^e Scogle	۶ 🖬 ۲	+ +
Cisco Unified Cisco Unified Co	CM Administration		Navigation Cisco Unifie admin Search Docume	d CM Administratio	on 💌 Go Logout
System - Call Routing - Media Reso	urces - Advanced Features - Device -	Application - User Management - E	Bulk Administration 👻 Help 👻		
SAML Single Sign-On					
SAML SSO 👩 Update Id	P Metadata File 👔 Export All Metadata 🏑	Fix All Disabled Servers			
r Status					
(i) SAML SSO disabled					
SAML Single Sign-On (1 - 1 o	of t)			Rows per Pag	e 50 💌
Server Name SSO Status cucm0a Disabled	Re-Import Metadata Last Met N/A Never	adata Import Export Metadata	Last Metadata Export Never	SSO T Never	est

Selecione Ativar SSO SAML.

Clique em **Continuar** para confirmar o aviso.

😨 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

FederationMetadata.xml que você salvou anteriormente, como mostrado na imagem.

Firefox *					
Find and List Users ×	SAML Single Sign-On Configuration	× End and List LDAP Directories	× +		
A https://cucm0a/ccmadmin/samISingleS	ignOnConfigurationWizard.do	☆⊽C	S - Google	۵ م	• + +
Cisco Unified CM	Administration	a	Navigation Cisco Un dmin Search Doc.	ified CM Administra Imentation Abo	tion 💌 Go ut Logout
System - Call Routing - Media Resources	Advanced Features Device //	Application 👻 User Management 👻 Bulk A	dministration 👻 Help 👻		
SAML Single Sign-On Configuration					
Next					
Status Ready to import Identity Provider n Identity Provider(IdP) Metadata Tr To configure the trust relationship betwee manually obtain the file from the IdP an IdP Metadata File Browse. No file selected This action must be successful for at lead Import IdP Metadata Next Cancel	netadata trust file to cluster servers ust File en the 1dP and your servers, you must d upload it here. selected. st the Publisher before moving on to th	first obtain trust metadata from your Id	IP and import it to your	r servers. You will n	eed to

Selecione o arquivo XML e clique em **Abrir** para carregá-lo no CUCM em Downloads em Favoritos.

😧 File Upload						×
😋 🔾 = 🚺 • Adminis	trator + Downloads				Search Downloads	2
Organize - New folder					演• 🗊	2
* Favortes	Name -	Date modified	Type	Size		
E Desktop	AdfsSetup	2013/09/09 06:10 FM	Application	24 518 KB		
B Downloads	🖆 Federation/Hetadata	2013/09/12 02:01 PM	3ML Document	32 1/3		
2 Recent Places	🌍 picpick_inst	2013/09/12 11:09 AM	Application	11 129 KB		
Ubraries Documents Masic Pictures Videos Computer Network						
File	name: FederationMetadata				All Files	9
					<u>Q</u> pen Cancel	1

Depois de fazer o upload, clique em Importar metadados IdP para importar as informações do IdP para o CUCM. Confirme se a importação foi bem-sucedida e clique em Avançar para continuar.

SAML Single Sign-On Configuration - Windows Internet Explorer	
🚱 😔 🗢 🧭 https://10.1.1.100/ccmadmin/s 🔎 💌 😰 Ce 🖻 😏 🍏 🍏 SAML Single Sign-On Configu 🗙	A ★ ⊕
CISCO CISCO Unified CM Administration Navigation Cisco Unified CM For Cisco Unified Communications Solutions admin Search Docum	Administration Go
System - Call Routing - Media Resources - Advanced Features - Device - Application - User Ma	anagement 👻 Bulk Administration 👻
Help 🕶	
SAML Single Sign-On Configuration	
Next	
_ Status	
Import succeeded for all servers	
r Identity Provider(IdP) Metadata Trust File	
To configure the trust relationship between the IdP and your servers, you must first obtain trust metada	ata from your IdP and import it
to your servers. You will need to manually obtain the file from the IdP and upload it here.	
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	d.
Import IdP Metadata V Import succeeded for all servers	
Next Cancel	
Selecione o usuário que pertence ao CCM Super Users padrão e clique e	em RUN SSO TEST.
🍲 SAML Single Sign-On Configuration - Mozilla Firefox	- 🗆 ×

l	© ≙ ≏≂	https://cmpubhcsc.fhlab.com:8443/ccmadmin/samlSingleSignOnConfigurationWizard3.do?server 👓 😒 🏠	≡
s	AML Singl	le Sign-On Configuration	
г	Test SSO S	Setup-	
	This test ve any server	rifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test can be ru for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is successful.	in on
L	1)Pick a val	lid username to use for this test	
	You must al This user m	Iready know the password for the selected username. nust have administrator rights and also exist in the IdP.	
	Please lockou	e use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator ut.	
L	Valid admin	istrator Usernames	
	farfar		
L			
	2)Launch S	SO test page	
	Run SSO	Test	
Π	Cancel		

Quando apresentado com uma caixa de diálogo de autenticação de usuário, faça login com o nome de usuário e a senha apropriados.

ڬ Sign lı	n - Mozilla Firefox -	-		×
0	https://ad. fhlab.com /adfs/ls/?SAMLRequest=nZJPTwIxEMXvflpN77Cl/	Ai4NS	50 •••	≡
				^
	FS			
	Sign in with your organizational account			
	farfar@fhlab.com			
	•••••			
	Sign in			
				~

Se tudo estiver configurado corretamente, você deverá ver uma mensagem informando Teste SSO bem-sucedido!



Clique em FECHAR e CONCLUIR para continuar.

Agora concluímos com êxito as tarefas básicas de configuração para ativar SSO no CUCM usando ADFS.

Configurar SSO no CUC

O mesmo processo pode ser seguido para ativar SSO no Unity Connection.

Integração LDAP com CUC.



Configure a autenticação LDAP.

€ → ୯ û	(1) ▲ \$\$ https://cucpubhcsc.fhlab.com/cuadmin/home.do (2) ☆ III (1) (1)				
Cisco Unity Con For Cisco Unified Comm	nection Administration unications Solutions	Navipation Cisco Unity Connection Administration 🥪 Go farfar Search Documentation About Sign Out			
Cisco Unity Connection Video Services Accounts Status Dial Plan Partitions Search Spaces System Settings General Configuration -Cluster Authentication Rules Restriction Tables Licenses Schedules Global Nicknames Subject Line Formats Attachment Descriptions Enterprise Parameters Senter Descriptions		tartar Search Locumentation About Sign Out LDAP Authentication			
Plugins Fax Server B-LDAP -LDAP Setup -LDAP Directory Configuration -LDAP Authentication	10.89-228-226 389 Add Another Redundant LDAP Server 389 Save Fields marked with an asterisk (*) are required.				

Importe os usuários do LDAP que terão correio de voz atribuído e também o usuário que servirá para testar o SSO.

Cisco Unity Connection	Import Users				Import U					
E Users	Import Users Refresh Help	Import Users Refresh Help								
Users Import Users	r Status									
Synch Users	0	A								
Class of Service	Found 1 LDAP User(s)									
Class of Service	Find									
E Templates	Find End Users In LDAP Directory		_							
User Templates	Where Alias V Begins Wi	èh ↓	Eind							
Call Handler Templates										
Contact Templates	Import With									
B Notification Templates	Based on Template voicemailuse	rtemplate 🗸								
E Contacts										
Contacts	Directory Search Results									
Distribution Lists	birectory search Results									
System Distribution Lists	Import Selected Import All	25 V Rows Per Page								
E Call Management										
System Call Handlers	Alias A	First Name	Last Name	Phone Number	Extension					
Directory Handlers	hugohugo	hugo	hugo	1002	1002					
Interview Handlers	Terrora Balantest Terrora All	1								
Custom Recordings	Import Selected Import All	1								

Navegue até Usuários > Editar > Funções como mostrado na imagem.

Cisco Unity Connection		Edit User Basics (hugohugo)						
E Users								
Users	User	Edit	Refresh Help					
-Import Users		114	ar Basics	h.				
Synch Users	Save	re		μ				
E Class of Service	Stat	ta Pa	assword Settings	L				
Class of Service		Change Password						
Class of Service Membership		Ro	oles	ectory				
User Templates	Nam	e Me	essage Waiting Indicators	1				
Call Handler Templates	Alias*	То	ansfer Rules					
Contact Templates	Einet							
Notification Templates	First	* Me	essage Settings					
Contacts	Last	4 CI	aller Input					
Contacts	Displ	Ma	ailbox					
Distribution Lists	SMTR	Ph	none Menu		@cucpubhcsc.fhlab.com			
System Distribution Lists Call Management	Initia	s Pla	ayback Message Settings					
System Call Handlers	Title	Se	end Message Settings					
Directory Handlers	Empl	Me Me	essage Actions					
-Interview Handlers			reations			_		
Custom Recordings	LDA		recungs					
Call Routing		Po	ost Greeting Recording					
Message Storage		No	otification Devices					
Mailhov Stores	100	0		1				

Atribua ao usuário de teste a função de Administrador do sistema.

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		
E Templates		
User Templates	×	
Call Handler Templates	A ¥	
Contact Templates	Available Roles	
Notification Templates	Remote Administrator A	
E Contacts	System Administrator	
Contacts	Tecnnican Tenant Administrator	
Distribution Lists	User Administrator V	
System Distribution Lists		
Call Management	Save	

Metadados CUC

Você já deve ter baixado os metadados do CUC, criado o ConyingPartyTrust para CUC e carregado os metadados do CUC e criado as regras do AD FS no ADFS 3.0



Vá para SAML Single Sign-On (Logon único SAML) e ative SAML SSO.

i SAML Single Sign on Configuration - Mozilla Firefox	_		ב	\times
🛛 🖴 😁 https://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?serverName	: ***	${\boxtimes}$	☆	≡
SAML Single Sign on Configuration SAML Single	e Sign	n on Co	onfigu	ration
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. The on any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is	is tes succ	t can t essful.	be run	•
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 lockout.	admir	nistrato	or	
Valid administrator Usernames				
2)Launch SSO test page				
Run SSO Test				
Cancel				

📦 SAML Single Si	gn on Configuration - Mozilla Firefox	- 0	\times				– ø ×	
🖲 🚔 🖘 http	$os://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?testStatus=1 \bullet table and the set of the set o$	⊠ ☆	≡			· ⊠ ☆	II\ ⊡ 📽 Ξ	
SAML Single Sig SAML Single Sign	on Configuration SAML Single S on Configuration Refresh Help	ign on Con	iguration		Navigat farfar	ion Cisco Unity Connection A Search Documentation	dministration 🥌 Go About Sign Out	
Status	lata Test Successful						SAML Single Sign on	
Close	👋 Test SAML - Mozilla Firefox — 🗆 🔿	×						
		=		ers				
	550 Test Succeeded:			Rows per Page 50 V				
	Congratulations on a successful SAMI SSO configuration test. Places			ort data	Last Metadata Export	SSO Test		
	close this window.			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			Servers				

Configurar SSO no Expressway

Importar metadados para o Expressway C

Abra um navegador em https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml e SALVE os metadados em uma pasta local

Carregar para Configuração > Comunicações Unificadas > IDP.

Exportar Metadados Do Expressway C

Vá para a configuração -> Unified Communications -> IDP -> Export SAML Data

O modo cluster usa um certificado autoassinado (com longa duração) que está incluído no SAML

metadados e usados para assinar solicitações SAML

- No modo de cluster-wide, para fazer o download do único arquivo de metadados para cluster, clique em Download
- No modo por peer, para baixar o arquivo de metadados de um peer individual, clique em Download ao lado do peer. Para exportar tudo em um arquivo .zip, clique em Baixar tudo.

Adicione uma confiança de terceira parte confiável para o Cisco Expressway-E

Primeiro, crie Confianças de terceira parte para o Expressway-Es e, em seguida, adicione uma regra de declaração para enviar identidade como atributo UID.

🗢 🌩 🙎 🗊 📓 🗊							
AD FS		Relying Party Trusts					Actions
AD FS Service Endpoints Cetificates Claim Descriptions Claims Provider Trusts Relying Party Trusts Attribute Stores Authentication Policies	Issuance Transfo The following to Order Rule 1 Name	Relying Party Trusts Daplay Name Device Registration Service CUCM_Ouster_Wide_Relying_Party_trust Euclide Relying_Party_trust Deprov Edit Claim Rules for Expw Edit Claim Rules for Expw Issuance Authorization Rules Issuance Authorization Rules Deleptransform rules specify the claims that will be sent Name Issued 0	Enabled Yes Yes Yes yyC pation Authorit to the relying Daims	Type WS-Trust / SAM WS-Trust / SAM WS-Trust / SAM WS-Trust / SAM cation Rules party.	L / WS-Federation L / WS-Federation L / WS-Federation L / WS-Federation Which to extract issued from the Claim rule name Ztametic Rule template: S Attribute store: Active Directory Mapping of LDAP add m SAMA *	Identifier ummedis ad fihiab.com cmpubhcsc fihiab.com cuspubhcsc fihiab.com Ihiab.com-50000F4107076E57 Edit Rui re this rule to send the values of LD LDAP attributes. Specify how the a ule. iend LDAP Attributes as Claims P attributes to outgoing claim types National (Select or type to ret) coount-Name v	Actions Relying Party Trusts Add Relying Party Trust Add Non-Claims-Aware Relying Part View Interview Claims Select an attribute store from tributes will map to the outgoing claim types that will be Cutgoing Claim Type (Select or type to add more) ad v
	Add Rule	Edt Rule Remove Rule					Activate windows Go to System in Control Panel to activate Windows.

OAuth com login de atualização

Em Parâmetros do Cisco CUCM Enterprise, Verifique se OAuth com parâmetro de fluxo de login de atualização está ativado. Vá para Cisco Unified CM Administration > Enterprise Parameters > SSO and OAuth Configuration.

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

Caminho de autenticação



• Se o caminho de autenticação estiver definido como "autenticação SSO SAML", somente os

clientes Jabber que usam um cluster Unified CM habilitado para SSO poderão usar MRA neste Expressway. Esta é uma configuração somente SSO.

- O suporte de MRA do Expressway para todos os telefones IP, todos os endpoints do TelePresence e todos os clientes Jabber associados a um cluster do Unified CM não configurado para SSO exigirão que o caminho de autenticação inclua a autenticação UCM/LDAP.
- Se um ou mais clusters do Unified CM oferecerem suporte a Jabber SSO, selecione "SAML SSO e UCM/LDAP" para permitir SSO e autenticação básica.

Arquitetura SSO

O SAML é um formato de dados padrão aberto baseado em XML que permite que os administradores acessem um conjunto definido de aplicativos de colaboração da Cisco de forma transparente após se conectarem a um desses aplicativos. O SAML SSO usa o protocolo SAML 2.0 para oferecer login único entre domínios e produtos para soluções de colaboração da Cisco.

Fluxo de login no local



Figure :SAML Single sign SSO Call Flow for Collaboration Servers

Fluxo de login de MRA



OAuth

OAuth é um padrão que suporta autorização. Um usuário deve ser autenticado antes de ser autorizado. O fluxo de concessão de código de autorização fornece um método para que um cliente obtenha acesso e atualize tokens para acessar um recurso (serviços Unified CM, IM&P, Unity e Expressway). Esse fluxo também é baseado no redirecionamento e, portanto, exige que o cliente possa interagir com um agente de usuário HTTP (navegador da Web) controlado pelo usuário. O cliente fará uma solicitação inicial ao servidor de autorização usando HTTPS. O servidor OAuth redireciona o usuário para um serviço de autenticação. Isso pode ser executado no Unified CM ou em um IdP externo se o SSO SAML estiver habilitado. Dependendo do método de autenticação usado, uma exibição de página da Web pode ser apresentada ao usuário final para se autenticar. (A autenticação Kerberos é um exemplo que não exibiria uma página da Web.) Ao contrário do fluxo de concessão implícito, um fluxo de concessão de código de autenticação bem-sucedido fará com que os servidores OAuth emitam um "Código de autorização" para o navegador da Web. Este é um código exclusivo de uso único e de vida curta que é então passado de volta do navegador para o cliente. O cliente fornece este "Código de autorização" ao servidor de autorização juntamente com um segredo pré-compartilhado e recebe em troca um "Token de acesso" e um "Token de atualização". O segredo do cliente usado nesta etapa permite que o serviço de autorização limite o uso somente para clientes registrados e autenticados. Os tokens são usados para as seguintes finalidades:

Token de acesso/atualização

Token de acesso: Este token é emitido pelo servidor de autorização. O cliente apresenta o token a um servidor de recursos quando precisa acessar recursos protegidos nesse servidor. O servidor de recursos pode validar o token e confiar em conexões usando o token. (Os tokens de acesso da Cisco têm como padrão uma vida útil de 60 minutos)

Atualizar token: Este token é emitido novamente pelo servidor de autorização. O cliente apresenta esse token ao servidor de autorização juntamente com o segredo do cliente quando o token de acesso expirou ou está prestes a expirar. Se o token de atualização ainda for válido, o servidor de autorização emitirá um novo token de acesso sem exigir outra autenticação. (Os tokens de atualização da Cisco têm como padrão uma vida útil de 60 dias). Se o token de atualização expirou, um novo fluxo de concessão de código de autorização OAuth completo deve ser iniciado

para obter novos tokens.

O fluxo de concessão do código de autorização OAuth é melhor

No fluxo de concessão implícito, o token de acesso é passado ao cliente Jabber através de um agente de usuário HTTP (navegador). No fluxo de concessão do código de autorização, o token de acesso é trocado diretamente entre o servidor de autorização e o cliente Jabber. O token é solicitado ao servidor de autorização usando um código de autorização único limitado por tempo. Essa troca direta do token de acesso é mais segura e reduz a exposição ao risco.

O fluxo de concessão de código de autorização OAuth suporta o uso de tokens de atualização. Isso proporciona uma melhor experiência ao usuário final, pois ele não precisa se autenticar novamente com a mesma frequência (por padrão, 60 dias)

Configurar Kerberos

Selecionar autenticação do Windows

Gerenciador dos Serviços de Informações da Internet (IIS) > Sites > Site Padrão > Autenticação > Autenticação do Windows > Configurações Avançadas.

- 1. Desmarque Ativar autenticação no modo Kernel.
- 2. Verifique se a proteção estendida está desativada.



O ADFS suporta o Kerberos NTLM

Certifique-se de que o AD FS Versão 3.0 suporta o protocolo Kerberos e o protocolo NT LAN Manager (NTLM) porque todos os clientes não Windows não podem usar Kerberos e dependem do NTLM.

No painel direito, selecione Provedores e verifique se Negociar e NTLM estão presentes em Provedores Habilitados:



Configurar o Microsoft Internet Explorer

Verifique se Internet Explorer > Advanced > Enable Integrated Windows Authentication está marcado.

Internet Options							
General	Security	Privacy	Content	Connect	ions Programs	Advanced	
Setting	s]	
	 Do not submit unknown addresses to your auto-search pri 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* 						
•		. memory	III	to nep m		4	
*Ta	kes effect a	after you i	restart Inte	ernet Exp Re	lorer store advanced	settings	
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	

Adicione o URL do ADFS em Segurança > Zonas de Intranet > Sites