# SAML IOS configureren op Cisco Unified Communications Manager met ADFS 3.0

# Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Configuratie vooraf controleren Een register Pointer (PTR) records SRV-records moeten zijn geïnstalleerd voor Jabber-detectieservices ADFS3 Eerste configuratie SSO op CUCM configureren met ADFS LDAP-configuratie **CUCM-metagegevens** ADFS-relay configureren **IDP-metagegevens** SSO op CUC configureren **CUC-metagegevens** SSO op snelweg configureren Metagegevens invoeren in snelweg C Uitvoermetagegevens uit snelweg C Voeg een vertrouwen van de Relay Party in Cisco Expressway-E toe Handmatig met inloggen verversen Verificatiepad SSO-architectuur Login-flow op locatie **MRA-Login Flow** OAuth Toegang/verfrissing Token Goedkeuringscode Subsidie Flow beter Kerberos configureren Selecteer Windows-verificatie ADFS ondersteunt beide Kerberos NTLM Microsoft Internet Explorer configureren Voeg ADFS-URL toe onder Security > Intranet > sites > Voeg CUCM, IMP en Unity hostname toe aan Security > Trusted Sites Gebruikersverificatie Jabber-aanmelding bij SSO Problemen oplossen Internet Explorer (IE)

Plaatsen toegevoegd aan IE Niet sync-probleem Token intrekken Bootstrap-bestand SSO-defect MSIS7066

# Inleiding

Dit document beschrijft de stappen om Single Sign-On te configureren met Active Directory Federation Service (ADFS 3.0) met het gebruik van Windows 2012 R2 op Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (CUC) en Express-producten. De stappen om Kerberos te configureren zijn ook in dit document opgenomen.

# Voorwaarden

### Vereisten

Cisco raadt u aan kennis te hebben van Single aanmelding (SSO) en Windows-producten.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CUCM 11.5
- CUC 11.5
- Snelweg 12
- Windows 2012 R2-server met deze rollen:
  - Active Directory-certificaatservices
  - Services voor Active Directory Federation

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

# Configuratie vooraf controleren

Voordat u ADFS3 installeert, moeten deze serverrollen al in de omgeving bestaan:

Domain Controller en DNS

• Alle servers moeten als A Records worden toegevoegd samen met hun Pointer Record (een type DNS-record dat een IP-adres in een domein of hostname oplost)

### Een register

In Fhlab.com. er zijn ook gastheren cmpubhcsc , cmsubhcsc , cucpubhcsc , cucsubhcsc , expwyc , expwye , impubhcsc en imsubhcsc aan toegevoegd .



### Pointer (PTR) records

🍰 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
b in _sites	10.89.228.147	Pointer (PTR)	cmsubhcsc.fhlab.com.	static
þ 📃 _tcp	10.89.228.148	Pointer (PTR)	imppubhcsc.fhlab.com.	static
Danaia Danai	10.89.228.150	Pointer (PTR)	impsubhcsc.fhlab.com.	static
D UomainUnsZones D SecretDesZones	10.89.228.151	Pointer (PTR)	cucpubhcsc.fhlab.com.	static
2 PorestUnsZones	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 🚆 Reverse 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

SRV-records moeten zijn geïnstalleerd voor Jabber-detectieservices

8. DNS	Name	Type	Data	Т	imestamo	
A AD	Cisco-uds	Service Location (SRV)	[0][0][8443] cmsubhese.fhl	ab.com. st	tatic	
A C Forward Lookup Zones	cisco-uds	Service Location (SRV)	[0][0][8443] cmpubhcsc.fbl	ab.com. st	tatic	
msdcs.fhlab.com	Cuplosin	Service Location (SRV)	[0][0][8443] impsublese fb	lab.com st	tatic	
⊿ 👸 fhlab.com	cuplogin	Service Location (SRV)	[0][0][8443] impoublese fb	lab.com st	tatic	
▷ [] _msdcs		Service Location (SRV)	[0][100][3268] ad.fhlab.com	5	/12/2020 10:00:00 AM	
jsites	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 🔛 _udp	Idap	Service Location (SRV)	[0][100][389] ad.fhlab.com		(13/3030 10 00 00 414	
DomainDnsZones					_cisco-uds Properties	? X
⊿ ForestDnsZones					10010	
psites				Service Location	(SRV) Security	
A Reverse Lookup Zones				Domain:	fhlab.com	
228.89.10.in-addr.arp				Company.		
Trust Points				Service:	_cisco-uds	~
Conditional Forwarders				Pertagal	100	
b 🔂 Global Logs				Protocol.		¥
				Priority:	0	
				Mainht	0	
				wegn.	č	
				Port number:	8443	
				Host offering this	service:	
				cmpubhcsc fhla	b.com.	
			1			

• Root CA (ervan uitgaande dat de certificaten door Enterprise CA zijn ondertekend)

Er moet een certificaatsjabloon worden gemaakt op basis van de sjabloon voor webservercertificaat. De sjabloon moet worden gedupliceerd, een andere naam hebben en op het tabblad Uitbreidingen wordt het toepassingsbeleid gewijzigd door het toevoegen van een beleid voor clientverificatie. Deze sjabloon is nodig om alle interne certificaten (CUCM, CUC, IMP en Expressway Core) in een LAB-omgeving te tekenen. De interne CA kan ook de expressway E certificaatsignaleringsaanvragen (CSR) ondertekenen.

Certificate Templates (AD.fhlab.	Template Display Name	Schem	a Version Versi Int A 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 Cyptography Key Attestation	Edit Application Delision 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	Ede	
	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 critical
	Root Certification Authority	1		

De gecreëerde sjabloon moet worden uitgegeven om CSR te kunnen tekenen.



Selecteer in het CA-certificaatweb de sjabloon die eerder is gemaakt.

Microsoft Active Directory Certificate Services fhlab-AD-CA
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.

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	8V8mWY/9kjhqfnpeBzAAW++tolGzBjnvqaT8StWM LA0dphP6LrurUeY2KLwMLmKlft7aSy483yCsm0v1 00QF2cLbbS80ziM7dgPNsaCg567DM008PX2t5N 10y/Ip6oDzTd2E9w2p8rK3YxccbypovSt0ijIirh AM/Gjnz0 END CERTIFICATE REQUEST					
Certificate Templ	ato:					
Certificate Templ	ate: ✓ User					
Certificate Templ	ate: ✓ User Basic EFS					
Certificate Templ	✓ User Basic EFS Administrator					
Certificate Templ	v User Basic EFS Administrator EFS Recovery Agent					
Certificate Templ	ate: ✓ User Basic EFS Administrator EFS Recovery Agent Web Server					
Certificate Templ Additional Attribu	ate: V User Basic EFS Administrator EFS Recovery Agent Web Server Subordinate Certification Authority					

CSR op meerdere servers van CUCM, IMP en CUC moet worden gegenereerd en ondertekend door de CA. Het certificaat moet als doel hebben.

Generate Certificate Signing I	Request	
🔒 Generate 🖳 Close		
- Status		
Warning: Generating a	new CSR for a specific certificate type will overwrite the exi	sting 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**	RSA	Et Add
Key Length*	2048	
Hash Algorithm*	SHA256	
Generate Close		

CA Root Certificate moet worden geüpload naar Tomcat Trust en het ondertekende Certificaat om te kappen.

cisco For C	co Unified Operating	Navi	pation Cisco Unified OS Administration ~ sadmin Search Documentation About L				
Show - Settings -	Security · Software Upgrades	<ul> <li>Services - Help</li> </ul>	•				
ertificate List							
O Conservator S and a la	and D Habad Cartificate Cartific	ata chain 🛐 Garagat					
O Generate Sen-si	grea - g opean cermoale cermo	ale chain 60 General	e con				
<ol> <li>7 records four</li> </ol>	nd						
Certificate List	(1 - 7 of 7)						Rows per Page 50
find Certificate List	where Certificate v begi	ns with $\ \bigtriangledown$ torncat		Find Clear Filter	4 -		
Contificate *	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
omcat	cmpubhcsc-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/18/2022	Certificate Signed by fhlab-AD-CA
omcat-ECDSA	cmoubhcsc-EC.thlab.com	Self-signed	EC	cmpubhcsc.th/ab.com	cmpublicsc-EC.thlab.com	04/02/2025	Self-signed certificate generated by system
omcat-trust	imppublicsc-EC.fhlab.com	Self-signed	EC	imppublicsc.fhlab.com	imppublicsc-EC.fhlab.com	04/02/2025	Trust Certificate
omcat-trust	cmsubhcsc-EC.fhlab.com	Self-signed	EC	cmsubhcsc.fhlab.com	cmsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate
omcat-trust	impsubhcsc-EC.fhlab.com	Self-signed	EC	impsubhcsc.fhlab.com	impsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate
amont tourt	emashhara EC filsh com	Eall sissed	50	consultance (high com-	emashhere EC filsh com	04/03/3035	Tool Cadificate
omcat-trust	fhlab-AD-CA	Self-signed	RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate
Generate Self-sig	gned Upload Certificate/Certif	ficate chain Gener	ate CSR				
Certificate List	(1 - 6 of 6)						Rows per Page
find Certificate List	where Certificate v begi	ins with $\ \lor$ tormcet		Find Clear Filter	4 -		
Contificate *	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
omcat	cucpubhcsc-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/28/2022	Certificate Signed by fhlab-AD-CA
							The second
omcat-trust	fblab-AD-CA	Self-signed	RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate
CONTRACTOR OF BUILDING	CONTRACTOR CONTRACTOR	Con Agrico	11004	mana warver(awry	INGO NO CA		Astructo Mindows
omcat-trust	cucsubhose-EC.fhlab.com	Self-signed	EC	cucsubhcsc.fhlab.com	cucsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate (C VVIII d OWS
	the second	Call sinces		and the second delayer and the	successible and E.C. Balak anon	04/00/0000	The second se

• IS

Als dit niet het geval is, wordt in dit gedeelte deze rollen geïnstalleerd. Anders slaat u deze sectie

over en gaat u direct naar het downloaden van ADFS3 vanuit Microsoft.

Nadat u Windows 2012 R2 met DNS hebt geïnstalleerd, promoot u de server aan een Domain Controller.

De volgende taak is het installeren van Microsoft certificaatservices.

Navigeren naar Server Manager en een nieuwe rol toevoegen:



### Selecteer de rol Active Directory certificaatservices.

2	Add Roles and Features Wizard		_ <b>D</b> X
Select server role	25		DESTINATION SERVER AD.fhlab.com
Before You Begin Installation Type	Select one or more roles to install on the selected server. Roles	D	escription
Server Selection Server Roles Features Confirmation Results	Active Directory Certificate Services (4 of 6 installed) Certification Authority (Installed) Certificate Enrollment Policy Web Service (Installed) Certificate Enrollment Web Service (Installed) Certification Authority Web Enrollment (Installed) Certification Authority Web Enrollment (Installed) Network Device Enrollment Service Online Responder Active Directory Federation Services (Installed) Active Directory Lightweight Directory Services Active Directory Rights Management Services Application Server DHCP Server DHCP Server INS Server (Installed) Fax Server Instand Storage Services (2 of 12 installed) Hyper-V Network Policy and Access Services Print and Document Services		ctive Directory Certificate Services (AD CS) is used to reate certification authorities and related role services nat allow you to issue and manage certificates used in a ariety of applications.
		< Previ	ous Next > Install Cancel

En stel deze services in - de dienst van het Web van de Inschrijving van het Certificaat van de Autoriteit voor het Beleid van het Web eerst. Nadat deze twee rollen zijn geïnstalleerd, configureer ze en installeer vervolgens **Web Service** en **Web Encapsulation certificaatinschrijving**. Configureer ze.

Er zullen ook aanvullende roldiensten en -functies worden toegevoegd, zoals IIS, wanneer de certificeringsinstantie is geïnstalleerd.

Afhankelijk van uw plaatsing, kunt u Enterprise of Standalone selecteren.

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 Validity Period Certificate Database Web Server (IIS) Role Services Confirmation Progress Results	<ul> <li>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.</li> <li>C Enterprise Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.</li> <li>C Standalone Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.</li> </ul>	
	More about the differences between enterprise and standalone setup	
	< Previous Next > Instal Cancel	

Voor het CA-type kunt u de optie Root CA of subordinaat CA selecteren. Als er nog geen andere CA actief is in de organisatie, selecteert u **Root CA**.

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 (PKD). 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	

De volgende stap is het maken van een privé sleutel voor uw CA.



Deze stap is alleen nodig als u ADFS3 op een afzonderlijke Windows Server 2012 installeert.

Nadat u CA vormt, moet de Rol Services voor IS worden gevormd. Dit is nodig voor een webinschrijving op de CA. Voor de meeste implementaties van ADFS, een extra rol in IS, klik op **ASP.NET** onder Toepassingsontwikkeling.



In Server Manager, klik op **Web Server > is**, en klik dan met de rechtermuisknop op **Standaard Website**. De binding moet worden gewijzigd om HTTPS ook toe te staan naast HTTP. Dit gebeurt ter ondersteuning van HTTPS.



### Selecteer Banden bewerken.

<i>8</i> ]	Interne	t Informatio	n Services	(IIS) Manage	er		_ <b>0</b> X	
AD > Sites > Default Web S	ite 🕨						🖬 🛛 🟠 🔞 •	,
File View Help								
Connections	0.00	6	Cite He				Actions	
🔍 • 🗟 🖄 😣	e De	erault web	Site Ho	me			🔉 Explore	2
Start Page	Filter		• 7 Go -	Show All	Group by:		Edit Permissions	
AD (FHLAB\administrator)	ASP.NET					A A	Edit Site	
A 😧 Sites	- E	1	404	9			Bindings Basic Settings	
Explore Edit Permissions		.NET Compilation	.NET Error Pages	.NET Globalization	.NET Profile	-	View Applications View Virtual Directories	
Add Application	h	- internet - 1	- <u>68</u> -	3	ab		Manage Website	
Add Virtual Direc	ctory s	.NET Trust	.NET Users	Application	Connection		🗢 Restart	1
Edit Bindings		Leves	<u></u>	secongs	oungs		Start	
Manage Website	e >	, 🖷	🥵 🌄	<b>&amp;</b>	🏖 💾		Browse Website	
22 Refresh	ey	Pages and Controls	Providers	Session State	SMTP E-mail		Browse *:80 (http)	
× Remove							Browse *:443 (https)	
Rename			Ð				Advanced Settings	
Switch to Conte	nt View		A	0	m)	~	Configure	4
	Features Vi	ew 💦 Conten	t View				Failed Request Tracing Limits	
Ready	Press						•1	- 

Voeg een nieuwe Site-binding toe en selecteer **HTTPS** als type. Kies voor het SSL-certificaat het servercertificaat dat dezelfde FQDN moet hebben als uw AD-server.

<b>e</b> j			Intern	et Information	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</li> <li>Application Poc</li> <li>Sites</li> <li>Default Web</li> </ul>	Type http https	Host Name Type: https Host name: Host name: SSL certificat fhlab-AD-Co AD.fhlab.com	Port 80 442 I v ierver Name te: A I A m	IP Address * Edit P address: All Unassigned Indication	Binding Infor	ma Port: V 443 Select	Add Fdit X View Cancel

Alle vereiste rollen zijn geïnstalleerd in de omgeving, zodat u nu kunt doorgaan met de installatie van ADFS3 Active Directory Federation Services (op Windows Server 2012).

Voor de Rol van de Server, navigeer aan Server Manager > Beheer > de Rollen en eigenschappen van de Server toevoegen en selecteer dan de Actieve Diensten van de Federatie van de Map als u IDP binnen het klantnetwerk, op het privé LAN installeert.

in .	Server Manager	_ <b>_</b> ×
€⊜∙	Server Manager • Dashboard • 🗵 l 🏲	Manage Tools View Help
Dashboard	WELCOME TO SERVER MANAGER	Remove Roles and Features Add Servers
Local Server	1 Configure this local server	Create Server Group Server Manager Properties
IIII AD CS IIII AD DS AP AD FS	QUICK START 2 Add roles and features	

	Add Roles and Features Wizard	
elect server roles		DESTINATION SERVER AD fhiab.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	El 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
	Active Directory Lightweight Directory Services	includes a Federation Service that
	Active Directory Rights Management Services	enables browser-based Web SSO.
	Application Server I	
	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	

Nadat de installatie is voltooid, kunt u deze openen in de taakbalk of in het startmenu.



# ADFS3 Eerste configuratie

Dit deel gaat over de installatie van een nieuwe, zelfstandige Federatie-server, maar het kan ook worden gebruikt om deze op een Domain Controller te installeren

Selecteer **Windows** en type **AD FS Management** om de ADFS-beheerconsole te starten zoals in de afbeelding wordt getoond.



Selecteer de optie **AD FS 3.0 Federation Server Configuration** om de ADFS-serverconfiguratie te starten. Deze screenshots vertegenwoordigen dezelfde stappen in AD FS 3.

1 AD F5 2.0 Federation Ser	ver Configuration Wizard
Welcome	
Steps Welcome Select Deployment Type Federation Service Name Summary Results	<ul> <li>Welcome to the AD FS 2.0 Federation Service (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 rederation Service.</li> <li>O freate new Federation Service</li> <li>Select this option to set up either a stand-alone federation server or the first server in a federation server fam.</li> <li>O dd a federation server to an existing Federation server lam.</li> <li>Select this option to join this computer to an existing federation server fam.</li> </ul>
	< <u>Previous</u> <u>Next&gt;</u> Cancel <u>H</u> elp

Selecteer Een nieuwe Federatie-service maken en klik op Volgende.

p AD FS 2.0 Federation Ser	ver Configuration Wizard	×
Select Stand-Alone o	r Farm Deployment	
Step:	You can create either a stand-alone federation server for evaluation purposes or a small production environment, or usu can create a federation server in a new term for lead balancing and high availability	
<ul> <li>Welcome</li> <li>Select Deployment Type</li> </ul>	Select one of the following options. Either of these options will use the Windows Internal Database to store	
Federation Service Name	configuration data.	
Summary	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 > Causel   Hab	1
	Clevious <u>Next</u> Cancel <u>H</u> ep	

Selecteer een zelfstandige Federatie Server en klik op Volgende zoals in de afbeelding.

http://www.commonscience.com	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 deter must select a certificate. Select the certificate and/or port, and then	ce name from t armine the Fede click Next.	he Subject field o ration Service na	of the SSL certific ame from the SSL	ate for the settings, you
<ul> <li>Summary</li> <li>Results</li> </ul>	SSL certificate: ad0a.identitylab.us Federation Service name: ad0a.identitylab.us <u>What kind of certificate do I need?</u>	·	View	Port: 443 ▼	
				Ŗ	
		< Previous	Next >	Cancel	Help

Selecteer onder SSL-certificaat het zelf-ondertekende certificaat in de lijst. De naam van de Federatieve Service zal automatisch worden ingevuld. Klik op **Volgende**.

B <b>p</b> \$	The following settings will be configured for AD FS 2.0:
Welcome	Cherry AD, FC, comment
Select Deployment Type	<ul> <li>Stop AD PS server.</li> <li>Windows Internal Database service will be started and set to automatic startup.</li> </ul>
Federation Service Name	<ul> <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> </ul>
Summary	<ul> <li>Network Service account will be given access to the database, to the certificate private keys and</li> </ul>
Results	<ul> <li>Default set of endpoints will be enabled.</li> <li>Browser sign-in web site will be deployed to the '/adfs/Is' virtual directory under the Default Web Site in IIS.</li> <li>Federation Service name is adDa.identitylab.us</li> <li>Start AD FS server.</li> </ul>
	To begin contiguring this computer with these settings, click Next.

Controleer de instellingen en klik op **Volgende** om de instellingen toe te passen.

Steps	The following settings are being continued	
<ul> <li>Welcome</li> <li>Select Deployment Type</li> <li>Federation Service Name</li> <li>Summary</li> <li>Results</li> </ul>	The following settings are being contigured           Component         Stop the AD FS 2.0 Windows Service           Install Windows Internal Database         Install Windows Internal Database           Start the Windows Internal Database service         Create AD FS configuration database           Configure service settings         Configure service settings           Deploy browser sign-in Web site         Start the AD FS 2.0 Windows Service           Start the AD FS 2.0 Windows Service         Create default claim set           Create default claim set         Create default Active Directory claim acceptance rules	Status Configuration finished

Bevestig dat alle onderdelen met succes zijn voltooid en klik op **Sluiten** om de wizard te beëindigen en naar de hoofdbeheerconsole terug te keren. Dit kan een paar minuten duren.



ADFS is nu effectief ingeschakeld en ingesteld als een Identity Provider (IDP). Daarna moet u CUCM als een vertrouwde partner toevoegen. Voordat u dit kunt doen, moet u eerst wat configuratie doen in CUCM Administration.

# SSO op CUCM configureren met ADFS

### LDAP-configuratie

Het cluster moet worden geïntegreerd met de actieve map en de LDAP-verificatie moet worden ingesteld voordat er verder wordt gegaan. Blader naar **systeemtabblad > Ldap-systeem** zoals in de afbeelding.

## LDAP System Configuration

_ Status								
	Directories Before Making Changes on This Page							
Please Disable LDAP A	uthentication Before Making Changes on This Page							
LDAP System Informatio	n							
Enable Synchronizing from the second seco	om LDAP Server							
LDAP Server Type	Microsoft Active Directory							
LDAP Attribute for User ID	sAMAccountName							

Vervolgens navigeer u naar **systeemtab > LDAP-map**.

LDAP Directory
🔚 Save 💢 Delete 📔 Copy ờ Perform Full Sync Now 🕂 Add New
Status Status: Ready
LDAP Directory Information
LDAP Configuration Name* LDAP1
LDAP Manager Distinguished Name* fhlab\administrator
LDAP Password*
Confirm Password*
LDAP User Search Base* cn=users,dc=fhlab,dc=com
LDAP Custom Filter for Users < None >
Synchronize* Olivers Only 🔘 Users and Groups
LDAP Custom Filter for Groups <pre>&lt; None &gt;</pre>
LDAP Directory Synchronization Schedule
Perform Sync Just Once
Perform a Re-sync Every* 7 DAY O
Next Re-sync Time (YYYY-MM-DD hh:mm)* 2020-05-24 00:00

Standard User Fields To Be Synchronized				
Cisco Unified Communications Manager User Fields	LDAP Attribute	Cisco Unified Communications M	lanager 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 Number		homephone
Mobile Number	mobile	Pager Number		pager
Directory URI	mail	Display Name		displayName
LDAP Server Information – Host Name or IP Addre	iss for Server*	LDAP Port	* Use TLS	
10.89.228.226		389		
Add Another Red	undant LDAP Server			
Save Delete Co	py Perform Full Sync Now Add New			

Nadat de actieve gebruikers van de folder met CUCM zijn gesynchroniseerd, moet de LDAP-verificatie worden ingesteld.

cisco	Cisco Un For Cisco Uni	ified Cl	M Administration	n					Navigati far	n Cisc rfar	to Unified CM Search Doc	Administration	ion About	✓ Go Logout
System +	Call Routing * M	ledia Resourc	es • Advanced Features •	Device *	Application •	User Management 👻	Bulk Administration +	Help 🔻						
LDAP Aut	hentication													
Save														
Status -									 					
(i) State	us: Ready													
LDAP Au	thentication for	End Users												
Use L	DAP Authenticatio	n for End Us	iers											
LDAP Mar	nager Distinguishe	ed Name* g	hlab\Administrator											
LDAP Pas	sword*	•			•••••									
Confirm P	Password*	•	•••••		•••••									
LDAP Use	r Search Base*	<	n=users,dc=fhlab,dc=com											
LDAP Se	rver Informatio													
		Host	Name or IP Address for Se	rver*		LDAP Po	et" Use TLS							
10.89.2	28.226					389								
Add A	nother Redundant	t LDAP Serv	er											

Een eindgebruiker in CUCM moet bepaalde toegangscontrolegroepen hebben toegewezen aan zijn/haar gebruikersprofiel. De ACG is standaard CCM supergebruikers. De gebruiker wordt gebruikt om de SSO te testen wanneer de omgeving klaar is.

End Use	er Configuration						Related Links	Back to Find List Users	✓ Go
🔚 Sav	ve 🗙 Delete 斗 .	Add New							
Confirm MLPP Pr	n MLPP Password recedence Authorizati	ion Level D	efault	_			~		
CAPF I	nformation								
Associa	ited CAPF Profiles					∧ ∨ <u>View D</u>	etails		
Permis	sions Information								
Groups	Standard CCM End U Standard CCM Supe Standard CTI Allow Standard CTI Enable Standard AXL API A Standard Admin Rep Standard CCM Admi Standard CCM End U Standard CCM ADMI	Users Control of A ed ccess o Tool Admin in Users Users N Administr	II Devices	< > < >	View Details	Add to A Remove	ccess Control G from Access Co	roup Introl Group	
Confer Enal Meeting Attende	ble End User to Host of Number 1001 tes Access Code Delete Add M	tion Conference L	Now				]		

### **CUCM-metagegevens**

In deze sectie wordt het proces voor de CUCM-uitgever getoond.

De eerste taak is de CUCM-metagegevens te verkrijgen, waarvoor u naar de URL moet bladeren; <CUCM Pub FQDN>:8443/ssosp/ws/fig/metadata/sp. of deze kan worden gedownload vanaf het tabblad System > SAML Single Sign-on. Dit kan worden gedaan per knooppunt of Cluster Wide. Dit kan het beste worden gebruikt bij dit Cluster Wide.

CAMI Cingle Cign-On							
SO Mode							
Churter wide (One me	and the file and the	star Bassime multi-see	Towned and Easte)				
Cluster wide (One me	cadata nie per ciu	ster, keguires multi-sen	ver iomcat certificate)				
Per node (One metada	ata file per node)						
🗙 Disable SAML SSO 🎧	Export All Metada	ta 🔗 Update kdP Metada	ata File // Fix All Disabled Servers				
Status							
(D							
RTMT is enabled for	SSO. You can cha	inge SSO for RTMT here	L				
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	inge SSO for RTMT <u>herr</u>					Rows per Pape 50
RTMT is enabled for     SAML SSO enabled  SAML Single Sign-On Server Name	SSO. You can cha (1 - 4 of 4) SSO Status	nge SSO for RTMT <u>herr</u> Re-Import Metadata	Last Metadata 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 cmpublicsc.fhiab.com	SSO. You can cha (1 - 4 of 4) SSO Status SAML	nge SSO for RTMT <u>here</u> 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	550 Test Passed - April 20, 2020 2:02:15 PM PDT	Rows per Page 50 Run SSO Test
RTMT is enabled for     AML SSO enabled     SAML SSO enabled     SAML Single Sign-On     Server Name     cmpubhcsc.fhlab.com     cmsubhcsc.fhlab.com	SSO. You can che (1 - 4 of 4) SSO Status SAML SAML	Re-Import Metadata N/A	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 Metadata Export April 18, 2020 8:05:38 PM PDT April 18, 2020 8:05:37 PM PDT	550 Teat 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     AML SSO enabled     SAML SSO enabled     SAML Single Sign-On     Server Name     cmpubhcsc.fhlab.com     imppubhcsc.fhlab.com	SSO. You can che (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 SSO Test Run SSO Test Run SSO Test

Sla de gegevens lokaal op met een betekenisvolle naam, zoals sp\_cucm0a.xml, nadat u deze nodig hebt.

### ADFS-relay configureren

Terug naar de AD FS 3.0 Management console.



Klik op Add Relying Party Trust Wizard.

<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>	<section-header>         Welcome to the Add Relying Party Trust Wizard         This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and autorization decisions.         The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party trust the wizard.         The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party are you complete the wizard.</section-header>

Klik op Start om verder te gaan

Selecteer het XML-bestand **met** metagegevens van de **federatie, medatada.xml** dat u eerder hebt opgeslagen en klik op **Volgende**.

<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.

Gebruik **CUCM\_Cluster\_Wide\_Relying\_Party\_trust** als de naam van de weergave en klik op **Volgende**.

<b>\$</b>	Add Relying Party Trust Wizard	5
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
<ul> <li>Welcome</li> </ul>	Display name:	
Select Data Source	CUCM_Cluster_Wide_Relying_Party_trust	]
Specify Display Name	Notes:	
<ul> <li>Configure Multi-factor Authentication Now?</li> </ul>	^	-
<ul> <li>Choose Issuance Authorization Rules</li> </ul>		
<ul> <li>Ready to Add Trust</li> </ul>		
<ul> <li>Finish</li> </ul>		_
	< Previous Next Activa (Canicel in)	de

Selecteer de eerste optie en klik op Volgende.

<b>\$</b>	Add Relying Party Trust Wizard
Steps Welcome	Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.
<ul> <li>Select Data Source</li> <li>Specify Display Name</li> </ul>	Multifactor Authentication Global Settings
Configure Multi-factor Authentication Now?	Requirements Users/Groups Not configured
<ul> <li>Choose Issuance Authorization Rules</li> </ul>	Device Not configured Location Not configured
Ready to Add Trust	
	<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 multifactor 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>
	< Previous Next Active Caripal in C

Selecteer Geef alle gebruikers toegang tot deze groep en klik op Volgende zoals in de afbeelding.

<b>\$</b>	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	<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>	
<ul> <li>Finish</li> </ul>	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 (Canipel/inde

Bekijk de configuratie en klik op Volgende zoals in de afbeelding.

<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.     Monitoring Identifiers   Encryption Signature   Accepted Claims Organization   Endpoints Not<    Specify the monitoring settings for this relying party trust.   Relying party's federation metadata   URL:   Monitor relying party Automatically update relying party This relying party's federation metadata data was last checked on: <never> This relying party was last updated from federation metadata on: <never></never></never>
	< Previous Allex V Caricel V S

Schakel het vakje uit en klik op Sluiten.

<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

Selecteer met de knop secondaire muis het **vertrouwen** van de **Relying Party** dat u in de afbeelding hebt gemaakt en **bewerkt de** configuratie **Eisen** voor de **claim** zoals weergegeven in de afbeelding.

<b>M</b>		AD FS		
Image: Service     Image: Service	w Help Relying Party Trusts			
<ul> <li>✓ Trust Relationships</li> <li>☐ Claims Provider Trusts</li> <li>☐ Relying Party Trusts</li> <li>☐ Attribute Stores</li> <li>▷ ☐ Authentication Policies</li> </ul>	Device Registration Service CUCM_Ouster_Wide Relving Party trus CUC_Ouster_W Update from Fe ExpwyC Edit Claim Rule Disable Properties Delete Help	Yes WS-Trust / SAM t Yes WS-Trust / SAM ederation Metadata s	ML / WS-Federation ML / WS-Federation L / WS-Federation L / WS-Federation	identifier um ms-drs:ad.fhlab.com cucpublicsc.fhlab.com cucpublicsc.fhlab.com fhlab.com-500D0F4107D76E57

Klik op Regel toevoegen zoals in de afbeelding weergegeven.

Section Claim Rules for CUCM_Cluster_Wide_Relying_Party		x
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Ru	ules	
The following transform rules specify the claims that will be sent to the relying party.		
Order Rule Name Issued Claims		
		1
	+	
Add Data Cath Data Data		
Add Rule Edit Rule Remove Rule		
OK Cancel	Apply	/

Selecteer LDAP-kenmerken als claims verzenden en klik op Volgende.

<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 provide	÷s	
Choose Rule Type	e 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 telephoneNumb Active Directory attributes and then send those values as two different outgoing claims. This rule may als 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.	e e e e e e e e e e e e e e e e e e e	
	< Previous Next > Cancel		

Configuratie van deze parameters:

Naam claimregel: NaamID

Beeld van kenmerken: Actieve Map (dubbelklik op de vervolgkeuzelijst)

LDAP-kenmerk: SAM-accountnaam

Type vordering: uid

Klik op FINISH/OK om verder te gaan.

Houd er rekening mee dat uid niet in het kleine geval is en niet reeds in het uitrolmenu bestaat. Typ het.

	Edit Rule - NamelD				
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 ssued from the rule.				
Claim ru	le name:				
NamelE	1				
Rule ter	mplate: Send LDAP Attributes as Claims				
Attribute	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	vid 🗸 🗸 Viu			
*	~	v			
14.					
View F	View Rule Language OK Cancel				

Klik nogmaals op **Regel toevoegen** om een andere regel toe te voegen.

💱 Edit C	laim Rules f	or CUCM_Clus	ter_Wid	e_Relying_Party	×		
Issuance	Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules						
The folk	owing transform n	ules specify the cla	ims that will	be sent to the relying p	xarty.		
Order	Rule Name			Issued Claims			
1	NameID			uid			
					1		
					4		
Add F	Rule Edit i	Rule Remov	e Rule				
			0	K Cancel	Apply		

Selecteer Vorderingen verzenden met een aangepaste regel en klik op Volgende.

<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 details about each claim rule template.					
Configure Claim Rule	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:  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 for use only in later rules Creating claims for use only in later rules					
	< Previous Next > Cancel					

Maak een aangepaste regel genaamd Cluster\_Side\_Claim\_Rule.

Kopieer en plak deze tekst direct vanuit dit regelvenster. Soms worden quotes gewijzigd indien bewerkt op een teksteditor die dan de regel mislukt wanneer u een SSO-test uitvoert:

c:[Type ==

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

Klik op Voltooien om verder te gaan.

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"] =&gt; 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	

U dient nu twee regels te hebben die zijn gedefinieerd als ADFS. Klik op **Toepassen** en **OK** om het regelvenster te sluiten.

🎨 Edit C	laim Rules f	or CUCM_Clus	ter_Wid	e_Relying_Party	×
Issuance	Transform Rules	Issuance Authori	zation Rules	Delegation Authoriza	tion Rules
The folk	owing transform n	les specify the cla	ims that will	be sent to the relying pa	aty.
Order	Rule Name			Issued Claims	
1	NameID			uid	
2	Cluster_Side_C	laim_Rule		<see claim="" rule=""></see>	
Add F	Rule	Remov	re Rule		*
			0	K Cancel	Apply

CUCM wordt nu toegevoegd als een betrouwbare vertrouwende partij bij ADFS.

	Service	:5				<u> </u>
File Action View Help						
(+ +) 🛅 🗟 🕞 📓 🖬 🕨 🖿						
Services (Local) Services (Local)						
Active Directory Federation	Name	Description	Status	Startup Type	Log On As	^
Services	Active Directory Certificate Services	Creates, manages, and removes	Running	Automatic	Local System	
	Active Directory Domain Services	AD DS Domain Controller servic	Running	Automatic	Local System	=
Stop the service	🔍 Active Directory Federation Services	Enables Active Directory Federa	Running	Automatic (Delayed Start)	FHLA8\administra	stor
MESTERS THE SERVICE	Active Directory Web Services	This service provides a Web Ser	Running	Automatic	Local System	
	App Readiness	Gets apps ready for use the first		Manual	Local System	
Description:	Application Experience	Processes application compatib		Manual (Trigger Start)	Local System	
Services to issue security tokens.	Application Host Helper Service	Provides administrative services	Running	Automatic	Local System	
	Application Identity	Determines and verifies the ide		Manual (Trigger Start)	Local Service	
	Application Information	Facilitates the running of intera		Manual (Trigger Start)	Local System	
	Application Layer Gateway Service	Provides support for 3rd party p		Manual	Local Service	
	Application Management	Processes installation, removal,		Manual	Local System	
	AppX Deployment Service (AppXSVC)	Provides infrastructure support		Manual	Local System	
	ASP.NET State Service	Provides support for out-of-pro		Manual	Network Service	
	Background Intelligent Transfer Service	Transfers files in the backgroun		Manual	Local System	
	Background Tasks Infrastructure Service	Windows infrastructure service	Running	Automatic	Local System	
	Base Filtering Engine	The Base Filtering Engine (BFE) i	Running	Automatic	Local Service	
	Certificate Propagation	Copies user certificates and roo	Running	Manual	Local System	
	CNG Key Isolation	The CNG key isolation service is	Running	Manual (Trigger Start)	Local System	
	G COM+ Event System	Supports System Event Notifica	Running	Automatic	Local Service	
	G COM+ System Application	Manages the configuration and	Running	Manual	Local System	
	Computer Browser	Maintains an updated list of co		Disabled	Local System	¥
	<					>
Extended (Standard /						
			A	Activate Windows	5	

Start voordat u verdergaat de ADFS-service opnieuw. Blader naar **Start Menu > Administratieve** hulpmiddelen > Services.

### **IDP-metagegevens**

U moet CUCM informatie geven over onze IDP. Deze informatie wordt uitgewisseld met behulp van XML-metagegevens. Zorg ervoor dat deze stap wordt uitgevoerd op de server waar ADFS is geïnstalleerd.

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

Eerst moet u verbinding maken met de ADFS (IDP) door een browser Firefox te gebruiken om de XML-metadata te downloaden. Open een browser naar https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml en SAVE de metagegevens naar een lokale map.

Blader nu naar de CUCM-configuratie in het systeemmenu > SAML Single Sign-On-menu.

	🗰 Find and List Cisco	o Unified CM × +	-		×
¢	) → ଫ ŵ	Image: Barrier State	ii\ C	) ®	-e
	Server Cisco Unified CM Cisco Unified CM Group Presence Redundancy Group Phone NTP Reference Date/Time Group BLF Presence Group Region Information	M Administration Navigation Cisco Unified CM Administrati nunications Solutions es  Advanced Features  Device  Application  User Management  Buk Admin ups ups anager Group	an Abou	R   L	Go ogout
	Device Pool Device Mobility DHCP	where Name begins with      Find Cle     active query. Please enter your search criteria using the options above.	ar Filter	9	-
	LDAP	•			
	SAML Single Sign-On				
	Cross-Origin Resource Shari (CORS)	ring			
	Location Info	•			
	MLPP	•			
	Physical Location				
	SRST				
	Enterprise Parameters				
	Enterprise Phone Configuration	tion			
	Service Parameters				
	Security	•			
	Application Server				
	Licensing	•			
	Geolocation Configuration				
	Geolocation Filter				
	E911 Messages				

https://cmpubhcsc.fhlab.com:8443/ccmadmin/samlSingleSignOn.do

Terug naar CUCM Management en selecteer SYSTEM > SAML Single aanmelding.

Firefox *							_ [ ] X
🕮 Find and List User	s	× SAML Single Sign-Cr	×	End and List LDAP Directories	× +		
+ A https://cu	cm0a/comadmin/samiSi	ngleSignOn.do		습 v	C' Scogle	۶ 🖬 -	+ #
cisco For	Cisco Unified Co	CM Administrations	on		Navigation Cisco Unifie admin Search Docum	d CM Administratio entation About	n 💌 Go Logout
System - Cal Ro	uting 👻 Media Reso	urces 👻 Advanced Features	- Device - Applicatio	on 👻 User Management 👻 B	ulk Administration 👻 Help 👻		
SAML Single Si	jn-On						
SAML S	ISO 🔥 Update kil	P Metadata File 👔 Export A	Metadata 🧳 Fix All Dis	sabled Servers			
- Status							
(i) SAML SSO	disabled						
SAML Single S	ign-On (1 - 1 a	of 1)				Rows per Pag	e 50 💌
Server Name	SSO Status	Re-Import Metadata	Last Metadata Imp	ort Export Metadata	Last Metadata Export	SSO TO	est
cucmua	Disabled	ny A	Never	ine rite	Never	Rever	un Test

Selecteer SAML SSO inschakelen.

Klik op **Doorgaan** om de waarschuwing te bevestigen.

Weset worning Prozino Firefox	
Https://cucmDa/ccmadmin/genericDialogWindow.do?windowtitlekey=generi	iccialogwindow.windowtitle.ssoenable 😭
Enabling SSO and importing the metadata will cause web servi of the wizard. All affected web applications will drop their conn to be logged into again.	ices to restart upon completion ection momentarily and need
Enabling SSO and importing the metadata will cause web servi of the wizard. All affected web applications will drop their conn to be logged into again.	ices to restart upon completion lection momentarily and need

FederatieMetagegevens.xml in te voeren dat u eerder hebt opgeslagen zoals in de afbeelding.

Firefox *					
Find and List Users ×	SAML Single Sign-On Configuration	× Find and List LDAP Directories	× +		
+ https://cucm0a/ccmadmin/samlSingleSig	nOnConfigurationWizard.do	습 = C	S * Google	₽ 🖸 •	+ #
Cisco Unified CM For Cisco Unified Commu	Administration		Navigation Cisco Unified CM dmin Search Documentatio	Administration	Go 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 m Identity Provider(IdP) Metadata Tru To configure the trust relationship between manually obtain the file from the IdP and IdP Metadata File Browse. No file s Initiate the Metadata In No file selected. This action must be successful for at lease Import IdP Metadata Next Cancel	etadata trust file to cluster servers  st File  an the IdP and your servers, you mus lupload it here.  elected.  t the Publisher before moving on to t	it first obtain trust metadata from your Io	dP and import it to your servers.	. You will need	to

Selecteer het XML bestand en klik op **Open** om het vanuit de downloads onder de favorieten naar CUCM te uploaden.

💽 File Upload					X
GO . Adminis	strator - Downloads				Search Downloads
Organize • New folder					j≡• 🗊 <b>0</b>
* Favortes	Name +	Date modified	Type	Size	
E Desktop	AdfsSetup	2013/09/09 06:10 PM	Application	24 518 KB	
Downloads	😁 Federation/Hetadata	2013/09/12 02:01 FM	396. Document	32 KB	
Concurrents  Concurrents  Concurrents  Concurrents  Concurrent  C	Seperation of the second secon	2013/09/12 11:09 444	Application	11 129×8	
File	e game: FederationMetadata				All Files
					<u>Open</u> Cancel

Klik na het uploaden op de Metagegevens van de Importeren IDP om de informatie IDP in CUCM te importeren. Bevestig dat de invoer geslaagd is en klik op Volgende om verder te gaan.

SAML Single Sign-On Configuration - Windows Internet Explorer	
🚱 🕤 🗢 🎯 https://10.1.1.100/ccmadmin/s 🔎 💌 Ce 🗟 😏	🍯 SAML Single Sign-On Configu 🗙 👘 🔅
CISCO Cisco Unified CM Administration For Cisco Unified Communications Solutions	Navigation Cisco Unified CM Administration Search Documentation About Logout
System - Call Routing - Media Resources - Advanced Features - Help -	Device   Application  User Management  Bulk Administration
SAML Single Sign-On Configuration	
Next	
Status Import succeeded for all servers Identity Provider(IdP) Metadata Trust File To configure the trust relationship between the IdP and your servers to your servers. You will need to manually obtain the file from the IdP	s, you must first obtain trust metadata from your IdP and import it dP and upload it here.
IdP Metadata File C:\Users\bbanks\Downloads\FederationMetada	sta.xml Browse
Initiate the Metadata Import         This action must be successful for at least the Publisher before movi         Import IdP Metadata         Vext         Cancel	ing on to the next task in this wizard.

Selecteer de gebruiker die behoort tot de standaard CCM-gebruikers en klik op SSO-TEST uitvoeren.

🍅 SAML Single Sign-On Configuration - Mozilla Firefox	-	(		$\times$
🛛 🖨 📽 https://cmpubhcsc.fhlab.com:8443/ccmadmin/samlSingleSignOnConfigurationWizard3.do?server	•••	⊌	습	≡
SAML Single Sign-On Configuration				
Test SS0 Setup				
This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is suc	test (	can t II.	e run	on
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 a lockout.	dmini	strate	or	
Valid administrator Usernames				
2)Launch SSO test page				
Run SSO Test				
Cancel				

Meld u met de juiste gebruikersnaam en het juiste wachtwoord in bij een dialoogvenster voor gebruikersverificatie.

ڬ Sign In - Mozilla Firefox	-		$\times$
🛛 🔒 https://ad.fhlab.com/adfs/ls/?SAMLRequest=nZJPTwlxEMXvf	flpN77CIA	4NS0 •••	] ≡
			^
FS			
Sign in with your organizational account			
farfar@fhlab.com			
•••••			
Sign in			
			~

Als alles correct is ingesteld, kunt u een bericht zien waarin wordt gezegd dat de SSO-test is geslaagd!



Klik op SLUITEN en Voltooien om verder te gaan.

We hebben nu de basistaken voor configuratie voltooid om SSO op CUCM met ADFS mogelijk te maken.

# SSO op CUC configureren

Hetzelfde proces kan worden gevolgd om SSO in Unity Connection in te schakelen.

### LDAP integratie met CUC.



Configuratie van LBP-verificatie.

(← → ♂ @	🛛 🚔 🛱 https://cucpubhcsc.fhlab.com	m/cuadmin/home.do		🛛 🕻	2	III\ 🖸	۲ ک	=
cisco Unity Con For Cisco Unified Comm	nection Administration			Navigation Cisco farfar Sea	a Unity Connection Ac rch Documentation	iministratic About	n ∨ G Sign O	o ut
<ul> <li>Cisco Unity Connection</li> </ul>	LDAP Authentication					LDAP /	uthentical	tion
Video Services Accounts Status Dial Plan Partitions Search Spaces System Settings General Configuration Cluster Authentication Rules Restriction Tables Licenses Schedules Holiday Schedules Global Nicknames Subject Line Formats	COAP Authentication Refresh He     Save     Status     Coap Authentication Refresh He     DaP Authentication for End Use     DAP Authentication for End Use     DAP Manager Distinguished Name*     LDAP Password*     Confirm Password*     LDAP User Search Base*	p Users (hlab\Administrator (m=users,dc=fhlab,dc=com						
Attachment Descriptions Enterprise Parameters Service Parameters Plugins Rax Server CDAP LDAP Setup LDAP Directory Configuration LDAP Authentication	LDAP Server Information Ho 10.89.228.226 Add Another Redundant LDAP Se Save Fields marked with an asterisk (*) are	at Name or IP Address for Server* rver tree	LDAP Port <sup>®</sup> Use T	15				

Importeer de gebruikers van LDAP die voicemail hebben toegewezen en ook de gebruiker die zal dienen voor het testen van SSO.

Cisco Unity Connection	Import Users				Import L
E Users ^	Import Users Refresh Help				
Users					
Import Users	Status				
Synch Users	( Construction of the second s				
Class of Service	Found 1 LDAP User(s)				
Class of Service	r Find				
Class of Service Membership					
Templates	Find End Users In LDAP Director	<u> </u>			
User Templates	Where Alias  V Begins W	ith 🗸	Eind		
Call Handler Templates					
Contact Templates	Import With				
Notification Templates	Based on Template voicemailuse	rtemplate 🗸			
Contacts					
Contacts	Directory Search Results				
Distribution Lists	birectory search Results				
System Distribution Lists	Import Selected Import All	25 V Rows Per Page			
Call Management					
System Call Handlers	Alias A	First Name	Last Name	Phone Number	Extension
Directory Handlers	hugohugo	hugo	hugo	1002	1002
Interview Handlers	Encode Balantest   Encode All				
Custom Recordings	Import Selected Import All				

### Navigeer naar **gebruikers > Bewerken > Rollen** zoals in de afbeelding.

Cisco Unity Connection			
	Edit User	r Basics (hugohugo)	
Users	User E	Edit Refresh Help	
Synch Users	Save	User Basics	
Class of Service	- State	Password Settings	
Class of Service		Change Password	
Class of Service Membership	<b>U</b> 1	Roles	ectory
I Templates			
User Templates	Name	Message Waiting Indicators	
Call Handler Templates	Alias*	Transfer Rules	
Contact Templates	First N	Message Settings	
Notification Templates	Last N	Caller Input	
Contacts	Diselar	Mallhave	
E Distribution Liste	Dispia	Mailbox	
Sustem Distribution Lists	SMTP	Phone Menu	@cucpubhcsc.fhlab.com
Call Management	Initials	Playback Message Settings	
System Call Handlers	Title	Send Message Settings	
Directory Handlers	Employ	Message Actions	
-Interview Handlers		Grantiana	
Custom Recordings	LDAP	Greetings	
Call Routing		Post Greeting Recording	
Message Storage	Unt O	Notification Devices	
Mailboy Stores	O Do		

De testgebruiker de rol van systeembeheerder toewijzen.

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

### CUC-metagegevens

U hebt nu CUC-metadata gedownload, de Relying PartyTrust voor CUC gecreëerd en CUCmetagegevens geüpload en de regels i AD FS op ADFS 3.0 gemaakt



Ga naar SAML single-aanmelding en schakel SAML SSO in.

👛 saml :	_		$\times$					
0	🛛 🗎 📽 https://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?serverName							
SAML Sin	gle Sign on Configuration SAML Single S	Sign or	) Config	uration				
SAML Sin	gle Sign on Configuration Refresh Help							
Test SS This test on any s 1)Pick a You mus This use	O Setup verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This erver for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is s valid username to use for this test t already know the password for the selected username. r must have administrator rights and also exist in the IdP. ase use one of the Usernames shown below. Using any other Username to log into the IdP may result in ac	test ca access	an be ru iful. rator	n				
Valid adi farfar hugohu 2)Launci <b>Run S</b>	Valid administrator Usernames farfar hugohugo 2)Launch SSO test page Run SSO Test							
	na conferencia e Marilla Finder		- 0	L X				
🕑 🚔 🖙 http	se of Computation - Mobiles Friends			° ^ ⊛' ≡				
SAML Single Sig SAML Single Sig	n on Configuration SAML Single Sign on Configuration Navigation Cisco Unity Co on Configuration Refresh Help fartar Search Docur	nnection Ac	dministration	Go Sign Out				
Status			SAML Sin	gle Sign on				
	Test SAML - Mozilla Firefox							
Close	© ≜ ⅔ https://cucpubhcscfhlab.com/ssosp/pages/TestSSO.jsp?ssopage=true ····							
		Row	s per Page	50 v				
	Congratulations on a successful SAML SSO configuration test. Please close this window. File April 28, 2020 5:54:00 PM Passed - May 2 PDT PDT PASSED - April 28, 2020 5:54:00 PM Passed - April 2 PDT 11:05:37	SSO Test 4, 2020 PM PDT 9, 2020 AM PDT	Run SSC	Test				
	Close							

# SSO op snelweg configureren

### Metagegevens invoeren in snelweg C

Open een browser naar https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml en SAVE de metagegevens naar een lokale map

Upload naar Configuration > Unified Communications > IDP.

### Uitvoermetagegevens uit snelweg C

Ga naar configuratie -> Unified Communications -> IDP -> SAML-gegevens exporteren

Cluster mode gebruikt een zichzelf ondertekend certificaat (met lange levensduur) dat in SAML is opgenomen

metagegevens en gegevens die gebruikt worden voor het ondertekenen van SAML-verzoeken

- Voor de clusterbrede modus, om het enkele clusterbrede metagegevensbestand te downloaden, klikt u op Downloaden
- Op per-peer modus, om het metagegevensbestand voor een bepaald peer te downloaden, klikt u op Downloaden naast de peer. Als u alles in een .zip-bestand wilt exporteren, klikt u op Alles downloaden.

### Voeg een vertrouwen van de Relay Party in Cisco Expressway-E toe

Maak eerst vertrouwen van de Relying Partij voor de Expressway-ES en voeg dan een claimregel toe om identiteit als UID attribuut te verzenden.



### Handmatig met inloggen verversen

Controleer in Cisco CUCM Enterprise-parameters of de parameter Loop met Vernieuwde inlogsnelheid is ingeschakeld. Ga naar **Cisco Unified CM-beheer > Enterprise-parameters > SSO en configuratie van derden**.

- SSO a	and OAuth Configuration		
OAuth	Token Expiry Timer (minutes) *	60	60
OAuth	Refresh Token Expiry Timer (days) *	60	] 60
Redire	ect URIs for Third Party SSO Client		]
<u>SSO L</u>	ogin Behavior for iOS *	Use embedded browser (WebView)	Use embedded browser (WebView)
OAuth	with Refresh Login Flow *	Enabled V	Disabled
Use S	SO for RTMT *	True 🗸	True

### Verificatiepad

# SAML SSO and UCM/LDAP ▼ None SAML SSO authentication UCM/LDAP basic authentication SAML SSO and UCM/LDAP

- Als de authenticatieweg is ingesteld op "SAML SSO authenticatie", dan kunnen alleen Jabber klanten die gebruik maken van een SSO-enabled Unified CM-cluster MRA op deze expressway gebruiken. Dit is alleen een SSO-configuratie.
- Ondersteuning van snelwegen bij MRA voor alle IP-telefoons, alle TelePresence-endpoints en alle Jabber-clients die zijn gestationeerd in een Unified CM-cluster die niet voor SSO zijn geconfigureerd, vereisen dat de authenticatieweg UCM/LDAP-verificatie omvat.
- Als een of meer van de Unified CM-clusters Jabber SSO ondersteunt, selecteert u de "SAML SSO en UCM/LDAP" zodat zowel de SSO als de basisverificatie mogelijk zijn.

# SSO-architectuur

SAML is een op XML gebaseerd open-standaard gegevensformaat dat beheerders in staat stelt om toegang te hebben tot een bepaalde reeks Cisco samenwerkingstoepassingen naadloos na het ondertekenen in één van die toepassingen. SAML SSO gebruikt het SAML 2.0-protocol om cross-domein en product single-aanmelding voor Cisco collaboration-oplossingen aan te bieden.

### Login-flow op locatie



Figure :SAML Single sign SSO Call Flow for Collaboration Servers



### **MRA-Login Flow**

### OAuth

OAuth is een standaard die autorisatie ondersteunt. Een gebruiker moet zijn gewaarmerkt voordat hij kan worden geautoriseerd. De vergunningscode Grant flow biedt een methode voor een cliënt om toegang te verkrijgen en penningen te verfrissen om toegang te krijgen tot een hulpbron (Unified CM, IM&P, Unity en Expressway-diensten). Deze stroom is ook gebaseerd op omleiding en vereist dus dat de client kan samenwerken met een HTTP user-agent (webbrowser) die door de gebruiker wordt gecontroleerd. De cliënt zal een eerste aanvraag indienen bij de vergunningserver met behulp van HTTPS. De OAuth server richt de gebruiker op een authenticatieservice. Dit kan uitgevoerd worden op Unified CM of een externe IDP als de SAML SSO is ingeschakeld. Afhankelijk van de authenticatiemethode die wordt gebruikt, kan een

webpagina-weergave aan de eindgebruiker worden aangeboden om zichzelf te authentificeren. (Kerberos-verificatie is een voorbeeld dat geen webpagina zou weergeven.) In tegenstelling tot de impliciete subsidiestroom zal een succesvolle subsidie-stroom van de authenticatiecode resulteren in de uitgifte van een "machtigingscode" door de OAuth-servers aan de webbrowser. Dit is een unieke code voor eenmalig gebruik die van korte duur is en vervolgens wordt doorgegeven van de webbrowser naar de client. De client verstrekt deze "Authorization Code" aan de autorisatieserver samen met een vooraf gedeeld geheim en ontvangt in ruil voor "Access Token" en een "Refresh Token". Het in deze stap gebruikte clientgeheim stelt de vergunningdienst in staat het gebruik te beperken tot geregistreerde en gewaarmerkte cliënten. De penningen worden gebruikt voor de volgende doeleinden:

### Toegang/verfrissing Token

Toegangstoken: Deze token wordt uitgegeven door de autorisatieserver. De client presenteert het token aan een resource server wanneer het toegang moet krijgen tot beschermde bronnen op die server. De resource server kan het token gebruiken en vertrouwt verbindingen met het token op. (Cisco Access Tokens standaard op een levensduur van 60 minuten)

Token verversen: Deze token wordt opnieuw uitgegeven door de autorisatieserver. De cliënt legt dit token voor aan de autorisatieserver samen met het clientgeheim wanneer het toegangstoken is verlopen of zal verlopen. Als het verfrissingstoken nog geldig is, geeft de autorisatieserver een nieuw toegangstoken op zonder dat een andere verificatie vereist is. (Cisco verfrist tokens standaard tot een levensduur van 60 dagen). Als de verfrissingstoken is verlopen, moet een nieuwe volledige OAuth autorisatie-code worden gestart om nieuwe penningen te verkrijgen.

### Goedkeuringscode Subsidie Flow beter

In de impliciete subsidie flow wordt het toegangstoken doorgegeven aan de Jabber client via een HTTP user agent (browser). In de vergunningscode gift flow wordt het toegangstoken rechtstreeks uitgewisseld tussen de licentieserver en de Jabber-cliënt. De token wordt gevraagd op de vergunningserver met behulp van een unieke vergunningscode voor een bepaalde tijd. Deze directe uitwisseling van het toegangspakket is veiliger en vermindert de blootstelling aan risico's.

De OAuth-autorisatiecode subsidie flow ondersteunt het gebruik van verfrissingspenningen. Dit levert een betere ervaring aan de eindgebruiker op omdat deze niet zo vaak opnieuw hoeft te authenticeren (standaard 60 dagen)

# Kerberos configureren

### Selecteer Windows-verificatie

# Internet Information Services (IS) Manager > Sites > Default Web Site > Verificatie > Windows Verificatie > Geavanceerde instellingen.

- 1. Schakel de verificatie van de Kernel-modus in.
- 2. Zorg ervoor dat uitgebreide bescherming is uitgeschakeld.



### ADFS ondersteunt beide Kerberos NTLM

Zorg ervoor dat AD FS versie 3.0 zowel het Kerberos-protocol als het NTLM-protocol (NT LAN Manager) ondersteunt omdat alle niet-Windows-clients Kerberos niet kunnen gebruiken en niet op NTLM kunnen vertrouwen.

In het rechter deelvenster selecteert u Providers en zorgt u ervoor dat er onder Ingeschakelde providers onderhandeling en NTLM aanwezig zijn:

Image: Start Page   Image: Start Page <th colspan="8">🛐 Internet Information Services (IIS) Manager 📃 🗖</th>	🛐 Internet Information Services (IIS) Manager 📃 🗖							
File View Help         Connections         Image: Start Page         Image: Start Page: Start Page         Image: Start Page: Start Page: Start Page         Image: Start Page: Start	€ Sites → Default Web Sites	te >				🖬 🗟 🟠 🔞 •		
Connections       Authentication         Start Page       Click here to learn how to configure Extended Protection.         AD (HLAB\administrator)       Application Pools         AD (HLAB\administrator)       Application Pools         A Difference       Starts         Providers       Disabled         Forms Authentication       Enabled         Move Up       Providers         Providers       X         Select a provider from the list of available providers and click Add to add to the enabled providers.         Configuration: 'localhost' applicationHost.config, <location "default<="" paths="" td="">         OK       Cancel</location>	File View Help							
Authentication       Authentication         Start Page       Group by: No Grouping       Image: Configure Extended Provides:         Application Pools       Application Pools       Start September 2000         Application Pools       Anonymous Authentication       Enabled         APAPNET Impersonation       Disabled       HTTP 302 Login/Redir         Windows Authentication       Enabled       HTTP 401 Challenge         Windows Authentication       Enabled       Providers:         Providers:       Nove Up         NILM       Move Up         Nove Down       Remove         Select a provider from the list of available providers and click Add       Move Up         Nove Down       Remove         Select a provider from the list of available providers.       Activity to 2000 Remove         Available Providers:       Activity to 2000 Remove         Configuration: 'localhost' applicationHost.config. <location <="" path="Default" td="">       Available Providers:         OK       Cancel       Windows Set</location>	Connections				Alerts			
Start Page         AD (FHLASkuministrator)         Application Pools         States         > Default Web Site         Forms Authentication         Function         Forms Authentication         Forms Authentication         Forms Authentication         Forms Authentication         Forms Authentication         Forms Authentication         Forma Authenticati	🔍 • 🔚 🖄 😣				A Click here	to learn how to		
Anonymous Authentication Enabled Asp. NET Impersonation Disabled Forms Authentication Enabled HTTP 302 Login/Redir Windows Authentication Enabled HTTP 401 Challenge Providers Providers ? X Enabled Providers: Negotiate NTLM Move Down Remove Select a provider from the list of available providers and click Add to add it to the enabled providers. Configuration: "localhost" applicationHost.config. <location path="Default">Actions Disable Advanced Settings Providers Providers: Negotiate NTLM Select a provider from the list of available providers and click Add to add it to the enabled providers. Available Providers: Configuration: "localhost" applicationHost.config. <location path="Default">Actions Disable Advanced Settings Providers: Negotiate NTLM Select a provider from the list of available providers and click Add to add it to the enabled providers. Configuration: "localhost" applicationHost.config. <location <br="" path="Default">(Configuration: "localhost" applicationHost.config. </location></location></location>	Start Page	Group by: No Grouping						
Anonymous Authentication Enabled ASP.NET Impersonation Disabled Forms Authentication Enabled HTTP 401 Challenge Providers. Providers Prov	Application Pools	Name ^	Status	Response Type	Actions			
Default Web Site     Advanced Settings     Providers     Configuration: 'localhost' applicationHost.config, <location a="" add="" advanced="" and="" available="" canced="" click="" down="" enabled="" from="" it="" list="" move="" of="" ok="" path="Default" provider="" providers="" providers.="" providers:="" remove="" select="" setting<="" settings="" td="" the="" to="" up="" windows=""><td>a 🐻 Sites</td><td>Anonymous Authentication</td><td>Enabled</td><td></td><td>Dicable</td><td></td></location>	a 🐻 Sites	Anonymous Authentication	Enabled		Dicable			
Windows Authentication       Enabled       HTTP 401 Challenge       Providers         Providers       ?       X         Enabled Providers:       Move Up       Move Up         Move Down       Remove       Select a provider from the list of available providers and click Add to add it to the enabled providers.         Configuration: 'localhost' applicationHost.config, <location default"<="" path="Default V&lt;/td&gt;       Available Providers:       Adactivate       Il 2 R2 ws         OK       Cancel       Windows Selection Path       OK       Vindows Selection Path       Windows Selection Path&lt;/td&gt;&lt;td&gt;Default Web Site&lt;/td&gt;&lt;td&gt;Forms Authentication&lt;/td&gt;&lt;td&gt;Disabled&lt;/td&gt;&lt;td&gt;HTTP 302 Login/Redir&lt;/td&gt;&lt;td&gt;Advanced&lt;/td&gt;&lt;td&gt;Settings&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Providers       ? ×         Enabled Providers:       Move Up         NTLM       Move Down         Remove       Select a provider from the list of available providers and click Add to add it to the enabled providers.         Configuration: 'localhost' applicationHost.config, &lt;location path=" td="">         Adactivate       12 R2 ws         Go to System in Control Period         Windows Set</location>		Windows Authentication	Enabled	HTTP 401 Challenge	Providers	Jettings		
Configuration: 'localhost' applicationHost.config, <location default="" path="Default W&lt;/td&gt;         Configuration: 'localhost' applicationHost.config, &lt;location path=" td="" w<="">         Available Providers:         OK         OK</location>				Providers	? X			
Configuration: 'localhost' applicationHost.config, <location default="" path="Default&lt;/td&gt;     Available Providers:     Available Providers:     Available Providers:     Attivate     Image: Cancel     OK     Cancel&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Configuration: 'localhost' applicationHost.config, &lt;location path=" td="" v<="">     Available Providers:     Attivate     Attivate     Move Up   Move Up   Move Down   Remove     Select a provider from the list of available providers and click Add   to add it to the enabled providers.     Attivate     Attivate     T2R2ws   So to System in Control Patheters     Windows Set</location>		Enable	d Providers:					
Image: Configuration: 'localhost' applicationHost.config, <location default="" path="Default V&lt;/td&gt;       Select a provider from the list of available providers and click Add to add it to the enabled providers.       Image: Configuration: 'localhost' applicationHost.config, &lt;location path=" td="" v<="">         Available Providers:       Image: Configuration: 'localhost' applicationHost.config, <location default="" path="Default V&lt;/td&gt;       Image: Configuration: 'localhost' applicationHost.config, &lt;location path=" td="" v<="">         Move Down       Remove       Image: Configuration: 'localhost' application path="Default V         Move Down       Remove       Image: Configuration: 'localhost' application path="Default V         Move Down       Remove       Image: Configuration: 'localhost' application path="Default V         Move Down       Remove       Image: Configuration: 'localhost' application path="Default V         Move Down       Remove       Image: Configuration: 'localhost' application path="Default V         Move Down       Remove       Image: Configuration: 'localhost' application path="Default V         Move Down       Remove       Image: Configuration: 'localhost' application path="Default V         Move Down       Remove       Image: Configuration: 'localhost' application path="Default V         Move Down       Remove       Image: Configuration: 'localhost' application path="Default V         Move Down       Remove       Image: Configuration: 'localhost' application path="Default V</location></location>		Negot	iate		Move Up			
Configuration: 'localhost' applicationHost.config, <location default="" path="Default V&lt;/td&gt;     Select a provider from the list of available providers and click Add to add it to the enabled providers.     Available Providers:     Addctivate     12 R2 ws     So to System in Control Path&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;NILM&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;Moure Down&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Configuration: 'localhost' applicationHost.config, &lt;location path=" td="" v<="">   Configuration: 'localhost' applicationHost.config, <location default="" path="Default V&lt;/td&gt;   Available Providers:   Available Providers:   Adactivate   Mindows Se   OK&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;movebount&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Configuration: 'localhost' applicationHost.config, &lt;location path=" td="" v<="">   Available Providers:   Available Providers:   Addttivate   Mindows Se   OK</location></location>					Remove			
Select a provider from the list of available providers and click Add to add it to the enabled providers.       Image: Configuration: 'localhost' applicationHost.config, <location <="" path="Default V" td="">         Available Providers:       Available Providers:       Image: Configuration: 'localhost' applicationHost.config, <location <="" path="Default V" td="">         Available Providers:       Adactivate       12 R2 ws         Go to System in Control Path       Mindows Select a providers</location></location>		<						
Configuration: 'localhost' applicationHost.config, <location default="" path="Default V&lt;br&gt;Available Providers:&lt;br&gt;Available Providers:&lt;br&gt;Available Providers:&lt;br&gt;Available Providers:&lt;br&gt;Addctivate&lt;br&gt;Addctivate&lt;br&gt;Addctivate&lt;br&gt;Addctivate&lt;br&gt;Mindowys:&lt;br&gt;Windows Se&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;Features View 👔 Select&lt;/td&gt;&lt;td&gt;a provider from the&lt;br&gt;it to the enabled pr&lt;/td&gt;&lt;td&gt;list of available providers and&lt;br&gt;oviders.&lt;/td&gt;&lt;td&gt;click Add&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Available Providers:&lt;br&gt;Available Providers:&lt;/td&gt;&lt;td&gt;Configuration: 'localhost' applicationHost.config , &lt;loc&lt;/td&gt;&lt;td&gt;ation path=" td="" v<=""><td></td><td></td><td></td><td>Q1.:</td></location>				Q1.:				
Go to System in Control Per Window/s. Windows Se		Availa	ble Providers:			12.00		
OK Cancel Windows Se				*	APRCTIVa Go to Si	Control D		
OK Cancel Windows Se					Window	S Windows S		
				OK	Cancel	windows Se		

### Microsoft Internet Explorer configureren

Zorg ervoor dat Internet Explorer > Advanced > Geïntegreerde Windows-verificatie inschakelen is ingeschakeld.

Internet (	Options						? <b>X</b>
General	Security	Privacy	Content	Connec	tions Pr	ograms	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 invited a security</li> <li>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 closed</li> <li>Enable DOM Storage</li> <li>Enable Integrated Windows Authentication*</li> </ul>						
•							•
*Takes effect after you restart Internet Explorer Restore 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		Cance		Apply

Voeg ADFS-URL toe onder Security > Intranet > sites >