# Konfigurieren von SAML SSO auf Cisco Unified Communications Manager mit ADFS 3.0

## Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurationsvorprüfung A Datensätze PTR-Datensätze (Zeiger) Für Jabber Discovery Services müssen SRV-Datensätze vorhanden sein. Erstkonfiguration von ADFS3 Konfigurieren von SSO auf CUCM mit ADFS LDAP-Konfiguration **CUCM-Metadaten** Konfigurieren der ADFS-Relationship-Partei **IDP-Metadaten** Konfigurieren von SSO auf CUC **CUC-Metadaten** Konfigurieren von SSO auf Expressway Metadaten in Expressway C importieren Metadaten aus Expressway C exportieren Hinzufügen eines Vertrauens für eine vertrauenswürdige Partei für Cisco Expressway-E OAuth mit Refresh Login Authentifizierungspfad SSO-Architektur Anmeldungsablauf am Standort MRA-Anmeldeablauf OAuth Zugriffs-/Aktualisierungstoken Der Ablauf der OAuth-Autorisierungscodes für die Gewährung ist besser Konfigurieren von Kerberos Windows-Authentifizierung auswählen ADFS unterstützt beide Kerberos NTLM Konfigurieren von Microsoft Internet Explorer ADFS-URL unter Sicherheit > Intranetzonen > Standorte hinzufügen Hinzufügen von CUCM-, IMP- und Unity-Hostnamen zu Security > Trusted Sites Benutzerauthentifizierung Jabber-Anmeldung in SSO Fehlerbehebung Internet Explorer (IE)

<u>Sites, die zu IE hinzugefügt werden</u> <u>Problem bei fehlender Synchronisierung</u> <u>Aufrufen eines Tokens</u> <u>Bootstrap-Datei</u> <u>SSO fehlschlägt MSIS7066</u>

## Einführung

Dieses Dokument beschreibt die Schritte zur Konfiguration der einmaligen Anmeldung mit dem Active Directory Federation Service (ADFS 3.0) unter Verwendung von Windows 2012 R2 auf Cisco Unified Communication Manager (CUCM), Cisco Unity Connection (CUC) und Expressway-Produkten. Schritte zur Konfiguration von Kerberos sind ebenfalls in diesem Dokument enthalten.

## Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie mit Single Sign-On (SSO)- und Windows-Produkten vertraut sind.

#### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- CUCM 11,5
- CUC 11,5
- Expressway 12
- Windows 2012 R2 Server mit folgenden Rollen:
  - Active Directory-Zertifikatsdienste
  - Active Directory-Verbandsdienste

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konfigurationsvorprüfung

Vor der Installation von ADFS3 müssen diese Serverrollen bereits in der Umgebung vorhanden sein:

·Domänencontroller und DNS

·Alle Server müssen als A-Datensätze zusammen mit ihrem Zeigerdatensatz (ein DNS-Datensatz, der eine IP-Adresse in eine Domäne oder einen Hostnamen auflöst) hinzugefügt werden.

## A Datensätze

In fhlab.com. hosts cmpubhcsc, cmsubhcsc, cucpubhcsc, cucsubhcsc, expwyc, expwye, impubhcsc und imsubhcsc wurden hinzugefügt.



## PTR-Datensätze (Zeiger)

L DNS	Name	Туре	Data	Timestamp
AD AD	(same as parent folder)	Start of Authority (SOA)	[14], ad.fhlab.com., hostmaster.fhlab.co	static
a 📋 Forward Lookup Zones	(same as parent folder)	Name Server (NS)	ad.fhlab.com.	static
[] _msdcs.fhlab.com	10.89.228.144	Pointer (PTR)	expwyc.fhlab.com.	static
⊿ 🛐 fhlab.com	10.89.228.145	Pointer (PTR)	expwye.fhlab.com.	static
▷ []] _msdcs	10.89.228.146	Pointer (PTR)	cmpubhcsc.fhlab.com.	static
i _sites	10.89.228.147	Pointer (PTR)	cmsubhcsc.fhlab.com.	static
Dtcp	10.89.228.148	Pointer (PTR)	imppubhcsc.fhlab.com.	static
þ <u>□</u> _udp	10.89.228.150	Pointer (PTR)	impsubhcsc.fhlab.com.	static
DomainUnszones	10.89.228.151	Pointer (PTR)	cucpubhcsc.fhlab.com.	static
	10.89.228.153	Pointer (PTR)	cucsubhcsc.fhlab.com.	static
psues	10.89.228.154	Pointer (PTR)	win10.fhlab.com.	5/12/2020 10:00:00 AM
A 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

Für Jabber Discovery Services müssen SRV-Datensätze vorhanden sein.

2 DNS	Name	Type	Data	Ti	mestamp	
4 🗎 AD	cisco-uds	Service Location (SRV)	[0][0][8443] cmsubhcsc.fhl	ab.com. st	atic	
a 📋 Forward Lookup Zones	cisco-uds	Service Location (SRV)	[0][0][8443] cmpubhcsc.fhl	ab.com. st	atic	
[] _msdcs.fhlab.com	cuplogin	Service Location (SRV)	[0][0][8443] impsubhcsc.fh	lab.com. st	atic	
a 👸 fhlab.com	cuplogin	Service Location (SRV)	[0][0][8443] imppubhcsc.fh	lab.com. st	atic	
▷ []] _msdcs	ac .	Service Location (SRV)	[0][100][3268] ad.fhlab.com	n. 5/	12/2020 10:00:00 AM	
b Sites	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	[]_ldap	Service Location (SRV)	[0][100][389] ad.fhlab.com			
DomainUnsZones					_cisco-uds Properties	? X
A PorestUnszones				Contro Location (	CE10 0 0	
psites				Service Location (	SRV) Security	
A Beverse Lookup Zones				Domain:	fhlab.com	
228.89.10.in-addr.arp						
Trust Points				Service:	_cisco-uds	~
Conditional Forwarders				Protocol	ton	
b 🛐 Global Logs				riddood.	7.45	
				Priority:	0	
				Walaht	0	
				weight.	•	
				Port number:	8443	
				Host offering this	service:	
				emoublese filat	b.com.	

• Stammzertifizierungsstelle (vorausgesetzt, die Zertifikate werden von Enterprise CA signiert) Eine Zertifikatsvorlage muss auf der Grundlage der Vorlage für das Webserverzertifikat erstellt werden. Erstere wird dupliziert, umbenannt und auf der Registerkarte Erweiterungen werden Anwendungsrichtlinien geändert, um eine Richtlinie für die Clientauthentifizierung hinzuzufügen. Diese Vorlage wird benötigt, um alle internen Zertifikate (CUCM, CUC, IMP und Expressway Core) in einer LAB-Umgebung zu signieren. Die interne Zertifizierungsstelle kann auch die Expressway E Certificate Signing Requests (CSR) unterzeichnen.

Certificate Templates (AD.fhlab.	Template Display Name	Schem	a Version Versi Int Actions	
	CEP Encryption	1	Properties of New Template	V 🔹 V 😢
	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		
	IPSec	1		
	IPSec (Offline request)	1	Ede	
	Kerberos Authentication	2		
	Key Recovery Agent	2	Description of Application Policies:	Add Edit Remove
	CCSP Response Signing	3	Server Authentication	
	RAS and IAS Server	2	Client Authentication	Make this extension critical
	Root Certification Authority	1		

Die erstellte Vorlage muss ausgegeben werden, um CSR signieren zu können.



Wählen Sie im Zertifizierungsstellenzertifikat-Web die Vorlage aus, die zuvor erstellt wurde.

Microsoft Active	Directory Certificate Services fhlab-AD-CA	
Submit a Cert	ificate Request or Renewal Request	
To submit a sa Web server) in	ved request to the CA, paste a base-64-encode the Saved Request box.	d 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 LA0dphF6LrurUeY2KLwHLmKlft7aSy48JyCsm0v1 OWQFZoLb3bS80ziW7fgEFWSaCg567DM0Q8FkZt5N 10//Ip60DzTdZE9w2p8rK3YxccbypovSt0ijIirh AM/Gjnz0 END CERTIFICATE REQUEST	
Certificate Templ	ate:	
	d lines	

Basic EFS

Administrator EFS Recovery Agent Web Server

Subordinate Certification Authority

Additional Attril

Attributes

CUCM, IMP und CUC Multi-Server CSR müssen von der CA generiert und signiert werden. Der Zweck des Zertifikats muss "tomcat" sein.

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

# Das CA-Stammzertifikat muss an Tomcat Trust und das signierte Zertifikat an Tomcat hochgeladen werden.

Cisco Unified Operating System Administration         Navigation         Cisco Unified OS Administration           Cisco Unified Communications Solutions         osadmin   Search Documentation   Ab								
how - Settings -	Security · Software Upgrades	· Services · Help	•					
ertificate List								
Canacata Califati	anad D. Haland Cartificate Cartifica	ta chain 🛐 Ganari	da CSP					
O Generale Sell-Si	gneu - g opoau cermoale/cermoa	de chan 60 Generi	Ne Con					
1 7 records fou	nd							
Certificate List	(1 - 7 of 7)						Rows per Page 50	
ind Certificate List	t where Certificate v begin	ns with $\sim$ torncat		Find Clear Filter	4 -			
Castificate *	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description	
omcat	cmoubhcsc-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/18/2022	Certificate Signed by fhlab-AD-CA	
mcat-ECDSA	cmpubhcsc-EC.thlab.com	Self-signed	EC	cmpubhcsc.th/ab.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	
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	
anal trust	consubheres \$7 fields com	Eall signad	50	cmoubless (hish com	consubheres EC faish com	04/03/3035	Tool Cadificate	
amcat-trust	fhlab-AD-CA	Self-signed	RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate	
Generate Self-si	gned Upload Certificate/Certifi	icate chain Gene	rate CSR					
-								
Certificate List	(1 - 6 of 6)						Rows per Page	
ind Certificate List	t where Certificate v begin	ns with $\sim$ torncet		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	
		P - 2					The second se	
omcat-trust	fhlab-AD-CA	Self-signed	RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate	
ALL DESCRIPTION OF ALL DESCRIPTI	CONTRACTOR OF THE OWNER OF THE	the segred		reason and a section of the section	INGO RO CR		- Activate Mindows	
omcat-trust	cucsubhcsc-EC./hlab.com	Self-signed	EC	cucsubhcsc.fhlab.com	cucsubhcsc-EC.fhlab.com	04/02/2025	Trust Ceitificate (C. VVIII GOWS	
	curpidblock, EC Blab com	Call rinnad	E.C.	and a shake a shake a same	contraction of the paper	0.000/0008	The set of	

• IIS

Andernfalls wird in diesem Abschnitt die Installation dieser Rollen beschrieben. Andernfalls

überspringen Sie diesen Abschnitt und fahren Sie direkt zum Download von ADFS3 von Microsoft.

Nach der Installation von Windows 2012 R2 mit DNS können Sie den Server auf einen Domänencontroller verweisen.

Die nächste Aufgabe besteht in der Installation von Microsoft Certificate Services.

Navigieren Sie zum Server Manager, und fügen Sie eine neue Rolle hinzu:



#### Wählen Sie die Rolle Active Directory-Zertifikatdienste aus.

<b>b</b>	Add Roles and Features Wiza	rd 🔄 🗖 🗙
Select server role	es	DESTINATION SERVER AD:fhlab.com
Before You Begin Installation Type	Select one or more roles to install on the selected server.	Description
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 Domain Services (Installed)     Active Directory Federation Services (Installed)     Active Directory Lightweight Directory Services     Active Directory Rights Management Services     Active Directory Rights Management Services     Active Directory Rights Management Services     DHCP Server     DNS Server (Installed)     Fax Server     B File and Storage Services (2 of 12 installed)	Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
	Hyper-V     Network Policy and Access Services     Print and Document Services	< previous Next > Install Cancel

Stellen Sie diese Dienste bereit - Webdienst für die Zertifizierungsstellen-Registrierung für Zertifikatszertifikate. Nachdem diese beiden Rollen installiert wurden, konfigurieren Sie sie, und installieren Sie dann den Webdienst für die Zertifikatregistrierung und die Webregistrierung der Zertifizierungsstelle. Konfigurieren Sie sie.

Wenn die Zertifizierungsstelle installiert ist, werden auch zusätzliche Rollendienste und Features hinzugefügt, die erforderlich sind, z. B. IIS.

Je nach Bereitstellung können Sie Enterprise oder Standalone auswählen.

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

Für den CA-Typ können Sie die Root CA oder die untergeordnete CA auswählen. Wenn keine andere CA in der Organisation bereits ausgeführt wird, wählen Sie **Root CA** (Stammzertifizierungsstelle) aus.

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

Im nächsten Schritt erstellen Sie einen privaten Schlüssel für Ihre CA.



Dieser Schritt ist nur erforderlich, wenn Sie ADFS3 auf einem separaten Windows Server 2012

installieren. Nachdem Sie die CA konfiguriert haben, müssen die Rollendienste für IIS konfiguriert werden. Dies ist für die Webregistrierung in der CA erforderlich. Für die meisten ADFS-Bereitstellungen ist eine zusätzliche Rolle in IIS erforderlich, wenn Sie unter Anwendungsentwicklung auf **ASP.NET** klicken.



Klicken Sie im Server Manager auf **Webserver > IIS**, und klicken Sie dann mit der rechten Maustaste auf **Standardwebsite**. Die Binding muss geändert werden, um zusätzlich zu HTTP auch HTTPS zuzulassen. Dies geschieht zur Unterstützung von HTTPS.



Wählen Sie Bindungen bearbeiten aus.

Internet Information Services (IIS) Manager								- • ×
AD > Sites > Default Web Si	te 🕨							₩ 20 🟠 🔞 •
File View Help								
Connections	0.0	6	Cite He				Actions	
Q,• 🔜 🖄 😣	e 🕑 De	erault web	Site Ho	me			Septore	^
Start Page	Filter		• 7 Go -	Show All	Group by:		Edit Permissi	ions
AD (FHLAB\administrator)	ASP.NET					A ^	Edit Site	
Sites     Default Web Site	- E		454	9	Ē.		Bindings Basic Setting	j5
Explore Edit Permissions		.NET Compilation	.NET Error Pages	.NET Globalization	.NET Profile	-	View Applica View Virtual	ations Directories
Add Application		<b></b>	d <b>e</b>	銅	ab		Manage Website	e 🔿 📲
Add Virtual Direc	tory s	.NET Trust	.NET Users	Application	Connection		C Restart	
Edit Bindings		(COVER)	<b>C</b>	e comp	Jonnys		Start	
Manage Website	•		6	<b>8</b>			Browse Web	bsite
22 Refresh	¢y	Pages and Controls	Providers	Session State	SMTP E-mail		Browse *:80 (	(http)
× Remove							Browse *:443	(https)
Rename			Ð			<u>^</u>	Advanced Se	ettings
Switch to Conter	nt View		Z	0	ЩQ	v	Configure	_
	Features Vi	ew 💦 Conten	t View				Failed Reque	est Tracing
Ready								•1.:

Fügen Sie eine neue Site Binding hinzu, und wählen Sie **HTTPS** als Typ aus. Wählen Sie für das SSL-Zertifikat das Serverzertifikat aus, das den gleichen FQDN wie Ihr AD-Server haben sollte.

<b>e</b> j			Intern	et Information	n Services (IIS) Manager	
🛞 💿 😜 🖌 AD 🕨	Sites 🔸	Default 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: Require S SSL certifica fhlab-AD-Co Not selected fhlab-AD-Co AD.fhlab.com	Port 80 442 I erver Name te: A I A m	IP Address * Edit P address: All Unassigned * Indication	Binding Informa t Site Binding Port: 443 Select OK	Add Fdit ? X

Alle erforderlichen Rollen sind in der Umgebung installiert, sodass Sie jetzt mit der Installation von ADFS3 Active Directory Federation Services (auf Windows Server 2012) fortfahren können.

Navigieren Sie für die Serverrolle zu Server Manager > Verwalten > Serverrollen und -funktionen hinzufügen, und wählen Sie Active Directory Federation Services aus, wenn Sie den IDP im Kundennetzwerk im privaten LAN installieren.

in .	Server Manager	_ <b>_</b> X
<u>ج</u> ي-	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
MI AD CS III AD DS AP AD FS	2 Add roles and features	

		DISTINATION SERVE
elect server roles		AD fhlab.com
Before You Begin	Select one or more roles to install on the selected server.	
Installation Type	Roles	Description
Server Selection	h - M Artin Directory Castificate Services (Lad & Install	Active Directory Federation Service
Server Roles	Active Directory Certificate Services (+ or o installed)     Active Directory Domain Services (Installed)	(AD FS) provides simplified, secured
Features	Active Directory Federation Services (Installed)	sign-on (SSO) capabilities. AD FS
	Active Directory Lightweight Directory Services	includes a Federation Service that
	Active Directory Rights Management Services	enables prowser-based web 330.
	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	
	v	

Sobald die Installation abgeschlossen ist, können Sie sie über die Taskleiste oder das Startmenü öffnen.

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

## **Erstkonfiguration von ADFS3**

In diesem Abschnitt wird die Installation eines neuen, eigenständigen Föderationsservers beschrieben. Dieser kann jedoch auch verwendet werden, um ihn auf einem Domänencontroller zu installieren.

Wählen Sie **Windows** aus, und geben Sie **AD FS Management** ein, um die ADFS Management Console wie im Bild gezeigt zu starten.



Wählen Sie die Option **AD FS 3.0 Federation Server Configuration Wizard** (Assistent zum Konfigurieren von AD FS-Servern) aus, um die ADFS-Serverkonfiguration zu starten. Diese Screenshots stellen die gleichen Schritte in AD FS 3 dar.

aD F5 2.0 Federation Serv	er Configuration Wizard	×
Welcome		
Welcome Welcome Select Deployment Type Federation Service Name Summary Results	<ul> <li>Welcome to the AD FS 2.0 Federation Server Configuration Wizard</li> <li>This wizard 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 rederation Service.</li> <li>C freate a 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>C Add a federation server to an existing Federation Service</li> <li>Select this option to join this computer to an existing federation server fam.</li> </ul>	
	< <u>Erevisus</u> <u>N</u> ext> Cancel <u>H</u> elp	

Wählen Sie Neuen Föderationsdienst erstellen aus, und klicken Sie auf Weiter.

AD FS 2.0 Federation Ser	ver Configuration Wizard	Ľ×
Select Stand-Alone o	r Farm Deployment	
Steps	You can create either a stand-alone federation server for evaluation numbers or a small conduction	
Welcome	environment, or you can create a federation server in a new farm for load balancing and high availability.	
Select Deployment Type	Select one of the following options. Either of these options will use the Windows Internal Database to store configuration data.	
Federation Service Name	O New federation server farm	
P 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.	
	⊙ 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	
	< <u>Previous</u> <u>Next&gt;</u> Cancel <u>H</u> elp	

Wählen Sie Standalone Federation Server (eigenständiger Föderationsserver) aus, und klicken Sie auf **Next (Weiter)**, wie im Bild gezeigt.

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 Service name f Default Web Site. If the wizard cannot determine the must select a certificate. Select the certificate and/or port, and then click Next.	rom the Subject field of the SSL certificate for the Federation Service name from the SSL settings, you	
<ul> <li>Summary</li> <li>Results</li> </ul>	SSL certificate: ad0a.identitylab.us ad0a.identitylab.us What kind of certificate do I need?	▼ View 443 ▼	
	< Previo	ous Next > Cancel Help	

Wählen Sie unter SSL-Zertifikat das selbst signierte Zertifikat aus der Liste aus. Der Name des Föderationsdiensts wird automatisch eingetragen. Klicken Sie auf **Weiter**.

AD FS 2.0 Federation Serv	ver Configuration Wizard
Ready to Apply Settin	gs
tep#	The following settings will be configured for AD FS 2.0:
Welcome	Stop AD FS server.
Select Deployment Type	<ul> <li>Windows Internal Database service will be started and set to automatic startup.</li> </ul>
Federation Service Name	<ul> <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 endpoints, and the service will run under this account.</li> </ul>
results	<ul> <li>Browser sign-in web site will be deployed to the 'Vadts/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 configuring this computer with these settings, click Next.
	< Previous Next > Cancel Help

Überprüfen Sie die Einstellungen, und klicken Sie auf **Weiter**, um die Einstellungen zu übernehmen.

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 configured           Component         Stop the AD FS 2.0 Windows Service           Install Windows Internal Database         Install Windows Internal Database           Start the Windows Internal Database service         Treate AD FS configuration database           Configure service settings         Deploy browser sign-in Web site           Deploy browser sign-in Web site         Treate default claim set           Create default claim set         Create default Active Directory claim acceptance rules	Status         Configuration finished         Status         Status

Bestätigen Sie, dass alle Komponenten erfolgreich abgeschlossen wurden, und klicken Sie auf **Schließen**, um den Assistenten zu beenden und zur Hauptverwaltungskonsole zurückzukehren. Dies kann einige Minuten dauern.



ADFS ist nun effektiv aktiviert und als Identitätsanbieter (Identity Provider, IDP) konfiguriert. Als Nächstes müssen Sie CUCM als zuverlässigen Partner hinzufügen. Bevor Sie dies tun können, müssen Sie zunächst eine Konfiguration in der CUCM-Verwaltung vornehmen.

## Konfigurieren von SSO auf CUCM mit ADFS

## LDAP-Konfiguration

Der Cluster muss LDAP-integriert in Active Directory sein, und die LDAP-Authentifizierung muss konfiguriert werden, bevor es weitergeht. Navigieren Sie zur **Registerkarte System > LDAP System** wie im Bild gezeigt.

## LDAP System Configuration

– Status		
	Directories Before Making Changes on This Page	
	therefore before Making changes on This Page	
Please Disable LDAP A	Ithentication 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	٥
LDAP Attribute for User ID	sAMAccountName	٥

Navigieren Sie anschließend zur **Registerkarte System > LDAP Directory (System > LDAP-**Verzeichnis).

LDAP Directory	
Save 🗙 Delete 🗋 Copy	Perform Full Sync Now 🕂 Add New
Status	
i 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*	Users Only O Users and Groups
LDAP Custom Filter for Groups	< None >
LDAP Directory Synchronization S	Schedule
Perform Sync Just Once	
Perform a Re-sync Every*	7 DAY ᅌ
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 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 3	Mail ID			mail		
Title	title	Home Number	r		homephone		
Mobile Number	mobile	Pager Number	r		pager		
Directory URI	mail	Display Name	1		displayName		
LDAP Server Information Host Name or IP Address for Server* LDAP Port* Use TLS							
10.89.228.226			389				
Add Another Redundant LDAP Server							
Save Delete Copy Perform Full Sync Now Add New							

Nachdem die Active Directory-Benutzer mit dem CUCM synchronisiert wurden, muss die LDAP-Authentifizierung konfiguriert werden.

Cisco Unified C	M Administration	Navigation Cisco Unified CM Administration v GO farfar Search Documentation About Locout
System - Call Routing - Media Resour	ces 👻 Advanced Features 👻 Device 👻 Application 👻 User Management 👻 Bulk Admi	istration 👻 Help 💌
LDAP Authentication		
Save		
c Status		
i Status: Ready		
LDAP Authentication for End Use	s	
Use LDAP Authentication for End	isers	
LDAP Manager Distinguished Name*	fhlab\Administrator	
LDAP Password*		
Confirm Password*		
LDAP User Search Base*	cn=users,dc=fhlab,dc=com	
LDAP Server Information		
Hor	Name or IP Address for Server* LDAP Port* Use 1	15
10.89.228.226	389	
Add Another Redundant LDAP Ser	ver	

Endbenutzer in CUCM müssen bestimmte Zugriffskontrollgruppen seinem Endbenutzerprofil zugewiesen haben. Die ACG sind Standard-CCM-Super-Benutzer. Der Benutzer wird zum Testen von SSO verwendet, wenn die Umgebung bereit ist.

End Use	er Configuration				Related Links: Back to Find List Use	ers 🗸 Go
Sav	e 🗙 Delete 🕂 Add Ne	ew				
Confirm MLPP Pr	MLPP Password recedence Authorization Lev	vel Default			~	^
CAPF I	nformation					
Associa	ted CAPF Profiles			∧ ✓ <u>View D</u>	Petails	
Permis	sions Information					
Groups	Standard CCM End Users Standard CCM Super User Standard CTI Allow Contro Standard CTI Enabled Standard AXL API Access Standard Admin Rep Tool Standard CCM Admin Use Standard CCM End Users Standard CCMADMIN Adm	rs ol of All Devices Admin rs ninistration	<ul> <li>View Details</li> <li>View Details</li> </ul>	Add to A Remove	from Access Control Group	
Conference Enable Meeting Attende	ence Now Information – ble End User to Host Confer Number 1001 es Access Code	rence Now				
Save	Delete Add New					

#### **CUCM-Metadaten**

In diesem Abschnitt wird der Prozess für den CUCM Publisher angezeigt.

Die erste Aufgabe besteht darin, die CUCM-Metadaten abzurufen, für die Sie zur URL navigieren müssen. https://<CUCM Pub FQDN>:8443/ssosp/ws/config/metadaten/sp oder kann von der Registerkarte System (System) > SAML Single Sign-on heruntergeladen werden. Dies kann pro Knoten oder Cluster-weit erfolgen. Diese Option ist clusterweit vorzuziehen.

SAML Single Sign-On							
ISO Mode							
Cluster wide (One me	tadata file per clu	ster. Requires multi-sen	ver Tomcat certificate)				
O Per node (One metad	ata file per node)						
🗙 Disable SAML SSO 🧃	Export All Metada	a 🚯 Update KP Metadi	ata File 🧳 Fix All Disabled Servers				
Status							
RTMT is enabled for	SSO. You can cha	nge SSO for RTMT here					
RTMT is enabled for     SAML SSO enabled	SSO. You can cha	nge SSO for RTMT <u>here</u>	L.				
RTMT is enabled for     SAML SSO enabled     SAML Single Sign-On	\$\$0. You can cha (1 - 4 of 4)	nge SSO for RTMT <u>her</u> s	L				Rows per Page 50
RTMT is enabled for     SAML SSO enabled  SAML Single Sign-On Server Name	SSO. You can che (1 - 4 of 4) SSO Status	nge SSO for RTMT <u>here</u> Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test	Rows per Page 50
RTHT is enabled for     SAML SSO enabled     SAML Single Sign-On     Server Name     cmpubhcsc.fhlab.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.
ATHT is enabled for     ATHT is 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	nge SSO for RTHT <u>berg</u> 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	Export Metadata Éxport Metadata File	Last Metadata 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.
ATHT is enabled for     ATHT is 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 PH PDT April 20, 2020 2:00:57 PH PDT April 20, 2020 2:00:57 PH PDT	Export Metadata 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 Teat 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.

Speichern Sie die Daten lokal mit einem aussagekräftigen Namen wie sp\_cucm0a.xml, danach benötigen Sie sie.

#### Konfigurieren der ADFS-Relationship-Partei

Kehren Sie zur Verwaltungskonsole AD FS 3.0 zurück.



Klicken Sie auf Assistent zum Hinzufügen von Vertrauenswürdigkeit.

<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         In swizard will help you add a new relying party trust to the AD FS configuration database. Relying parties oursource to inske authentication and autorization decisions.         The relying party trust that this wizard creates defines how this Federation Service to make authentication approximation database. The relying party trust that this wizard creates defines how this Federation Service to make authentication and autorization decisions.         The relying party trust that this wizard creates defines how this Federation Service to recognizes the relying party and issues claims to the relying to the relying party and issues claims to the relying party and issues claims to the relying to the relyi</section-header>

Klicken Sie auf Start, um fortzufahren.

Wählen Sie die zuvor gespeicherte XML-Datei **Federationmedatada.xml** aus, und klicken Sie auf **Weiter**.

<b>\$</b>	Add Relying Party Trust Wizard
Select Data Source	
Steps  Velcome  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 its 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 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:         Exture Vadministrator/Downloads/federationmetadata.om/         Browse         Cancel         Value this option to manually input the necessary data about this relying party organization.

Verwenden Sie **CUCM\_Cluster\_Wide\_Relying\_Party\_trust** als Anzeigenamen, und klicken Sie auf **Weiter**.

<b>\$</b>	Add Relying Party Trust Wizard	
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:	
Configure Multi-factor Authentication Now?	^	]
<ul> <li>Choose Issuance Authorization Rules</li> </ul>		
<ul> <li>Ready to Add Trust</li> </ul>		
<ul> <li>Finish</li> </ul>	×	J
	< Previous Next & Ctive Canipel in C	le

Wählen Sie die erste Option aus, und klicken Sie auf Weiter.

<b>\$</b>	Add Relying Party Trust Wizard
Steps	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.
Select Data Source	Mitifactor A theolication Global Settinge
Specify Display Name     Configure Multi-factor     Authentication Nam2	Requirements Users/Groups Not configured
Choose Issuance     Authorization Rules	Device Not configured
<ul> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	
<ul> <li>Hnish</li> </ul>	
	<ul> <li>I do not want to configure multi-factor authentication settings for this relying party trust at this time.</li> <li>Configure multi-factor authentication settings for this relying party trust.</li> <li>You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see <u>Configuring Authentication Policies</u>.</li> </ul>
	< Previous Next A ctive (Caripel in do

Wählen Sie **Zulassen aller Benutzer für den Zugriff auf diese vertrauliche Partei aus**, und klicken Sie auf **Weiter,** wie im Bild gezeigt.

<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.
<ul> <li>Welcome</li> </ul>	Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.
Select Data Source	<ul> <li>Permit all users to access this relying party</li> </ul>
Specify Display Name	The issuance authorization rules will be configured to permit all users to access this relying party. The relying
Configure Multi-factor Authentication Now?	Denvial users access to this relying party
<ul> <li>Choose Issuance Authorization Rules</li> </ul>	The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.
<ul> <li>Ready to Add Trust</li> </ul>	
<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 & ct Va (Canicel/in) do

Überprüfen Sie die Konfiguration, und klicken Sie auf Weiter, wie im Bild gezeigt.

<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:
	< Previous Avex yate WCaricelOV/S

Deaktivieren Sie das Kontrollkästchen, und klicken Sie auf Schließen.

<b>\$</b>	Add Relying Party Trust Wizard	x
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	]

Wählen Sie mit der zweiten Maustaste die **Relying Party Trust** aus, die Sie gerade erstellt haben, und **bearbeiten Sie** die Konfiguration der Anspruchsregeln, wie im Bild gezeigt.

<b>M</b>		AD FS		
翰 File Action View Windo	w Help			
🗢 🔿 🙎 📰 🛛 🖬				
🛗 AD FS	Relying Party Trusts			
Service	Display Name	Enabled Type		Identifier
Irust Kelationships     Claims Provides Trusts	Device Registration Service	Yes WS-Trust / S/	ML / WS-Federation	um:ms-drs:ad.fhlab.com
Rehing Party Trusts	CUCM_Cluster_Wide Relving Party trus	t Yes WS-Trust / S/	ML / WS-Federation	cmpubhcsc.fhlab.com
Attribute Stores	CUC_Cluster_W Update from Fe	deration Metadata	L / WS-Federation	cucpubhcsc.fhlab.com
Authentication Policies	ExpwyC Edit Claim Rule	5	L / WS-Federation	fhlab.com500D0F4107D76E57
	Disable			
	Properties			
	Delete			
	Help			

Klicken Sie auf Regel hinzufügen wie im Bild gezeigt.

👒 Edit Claim Rules for CUCM_Cluster_Wide_Relying_Party 💻 🗖 🗙
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
OK Cancel Apply

Wählen Sie LDAP-Attribute als Ansprüche senden aus, und klicken Sie auf Weiter.

<b>\$</b>	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	es
Choose Rule Type	details about each claim rule template.	
<ul> <li>Configure Claim Rule</li> </ul>	Claim rule template:	
	Send LDAP Attributes as Claims	
	Claim rule template description:	
	Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to created 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.	er O
	< Previous Next > Cancel	

Konfigurieren Sie diese Parameter:

Name der Anspruchsregel: NameID

Attributspeicher: Active Directory (doppelklicken Sie auf den Pfeil des Dropdown-Menüs)

LDAP-Attribut: SAM-Kontoname

Ausgehender Anspruchstyp: uid

Klicken Sie auf FERTIG/OK, um fortzufahren.

Bitte beachten Sie, dass uid nicht im Kleinbuchstaben angezeigt wird und nicht bereits im Dropdown-Menü vorhanden ist. Geben Sie es ein.

	Edi	t Ri	ule - NameID 🛛 🗙			
You ca which t issued f	You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.					
Claim n.	Claim rule name:					
Namel	0					
Rule te	mplate: Send LDAP Attributes as Claim	5				
Attribu A	a stora:					
Active	Disectory					
Acave	orrectory	-	Ť			
Mappin	g of LDAP attributes to outgoing claim	type	5.			
	LDAP Attribute (Select or type to add more)		Outgoing Claim Type (Select or type to add more)			
•	SAM-Account-Name	¥	uid 🗸			
*		۷	×			
		-				
View	Rule Language		OK Cancel			

Klicken Sie erneut auf **Regel hinzufügen**, um eine andere Regel hinzuzufügen.

🎙 Edit C	laim Rules fo	or CUCM_Clus	ter_Wide	e_Relying_Party	-	□ X
Issuance	Transform Rules	Issuance Authoriz	ation Rules	Delegation Authoriza	tion Ru	es
The foll	owing transform ru	les specify the clai	ims that will	be sent to the relying p	arty.	
Order	Rule Name			Issued Claims		
1	NameID			uid		
						1
Add F	Rule Edit R	ule Remov	e Rule			
			0	K Cancel		Apply

Wählen Sie Anträge mit einer benutzerdefinierten Regel senden aus, und klicken Sie auf Weiter.

<b>S</b>	Add Transform Claim Rule Wizard
Select Rule Template	
Steps	Select the template for the claim rule that you want to create from the following list. The description provides
Choose Rule Type	details about each claim rule template.
<ul> <li>Configure Claim Rule</li> </ul>	Claim rule template:
	Send Claims Using a Custom Rule 🗸
	Claim rule template description:
	Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include: • Sending claims from a SQL attribute store • Sending claims from a custom attribute store • 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 with complex changes to an incoming claim value • Creating claims for use only in later rules
	< Previous Next > Cancel

Erstellen Sie eine benutzerdefinierte Regel mit dem Namen Cluster\_Side\_Claim\_Rule.

Kopieren Sie diesen Text und fügen Sie ihn hier direkt in das Regelfenster ein. In manchen Fällen werden Kostenvoranschläge geändert, wenn sie in einem Texteditor bearbeitet werden. Dies führt dazu, dass die Regel beim Testen der SSO-Funktion fehlschlägt:

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

Klicken Sie auf Fertig stellen, um fortzufahren.

<b>S</b>	Add Transform Claim Rule Wizard
Configure Rule	
Reps a Choose Rule Type a Configure Claim Rule	You can configure a custom claim nule, such as a nule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom nule, type one or more optional conditions and an issuance statement using the AD FS claim nule language. Claim nule name: Quster_Side_Claim_Rule Rule template: Send Claims Using a Custom Rule Custom nule: C:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount name"] > issue (Type = "http://schemas.milooap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties ["http://schemas.milooap.org/ws/2005/05/identity/claimproperties/format "] = "urn:oasis:namestc:SAML:2.0:nameid-format:Tassient", Properties ["http://schemas.milooap.org/ws/2005/05/identity/claimproperties/format "] = "urn:oasis:namestc:SAML:2.0:nameid-format:Tassient", Properties ["http://schemas.milooap.org/ws/2005/05/identity/claimproperties/format "] = "urn:oasis:namestc:SAML:2.0:nameid-format:Tassient", Properties ["http://schemas.milooap.org/ws/2005/05/identity/claimproperties/format "] = "urn:oasis:namestc:SAML:2.0:nameid-format:Tassient", Properties ["http://schemas.milooap.org/ws/2005/05/identity/claimproperties/format multifier"] = "http://AD.fhlab.com"):]
	< Previous Finish Cancel

Sie sollten jetzt zwei Regeln für ADFS definieren. Klicken Sie auf **Übernehmen** und **OK**, um das Regelfenster zu schließen.

🎭 Edit C	laim Rules f	or CUCM_Clus	ster_Wid	e_Relying_Party	- • ×
Issuance	Transform Rules	Issuance Authori	zation Rule	Delegation Authoriza	tion Rules
The folk	owing transform n	ules specify the cla	ims that will	be sent to the relying pa	sty.
Order	Rule Name			Issued Claims	
1	NameID			uid	
2	Cluster_Side_C	laim_Rule		<see claim="" rule=""></see>	
Add F	Rule Edt 1	Rule	re Rule		<ul> <li>Image: Constraint of the second secon</li></ul>
			0	K Cancel	Apply

CUCM wird nun erfolgreich als vertrauenswürdiger vertrauender Partei zu ADFS hinzugefügt.

	Service	ES				x
File Action View Help						
Services (Local)						
Active Directory Federation Services Stop the service Restart the service Description: Enables Active Directory Federation Services to issue security tokens.	Name Active Directory Certificate Services Active Directory Certificate Services Active Directory Federation Services Active Directory Federation Services App Readiness Application Experience Application Information Application Information Application Information Application Management Application Management Application Experience Background Intelligent Transfer Service Background Tasks Infrastructure Service Base Filtering Engine	Description Creates, manages, and removes AD DS Domain Controller servic Enables Active Directory Federa 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 Provides support for 3rd party p Provides support for out-of-pro Transfers files in the backgroun Windows infrastructure service The Base Filtering Engine (BFE) i	Status Running Running Running Running Running	Startup Type Automatic Automatic Automatic (Delayed Start) Automatic Manual Manual (Trigger Start) Automatic Manual (Trigger Start) Manual Manual Manual Manual Manual Manual Manual Automatic Automatic	Log On As Local System Local System CHLASVadministre Local System Local System	ator
Extended (Standard /	Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Comparison Computer Browser C	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	Manual Manual (Trigger Start) Automatic Manual Disabled	Local System Local System Local Service Local System Local System	~

Bevor Sie fortfahren, starten Sie bitte den ADFS-Dienst neu. Navigieren Sie zu **Startmenü > Verwaltung > Dienste**.

#### **IDP-Metadaten**

Sie müssen dem CUCM Informationen zu unserem IDP geben. Diese Informationen werden mithilfe von XML-Metadaten ausgetauscht. Stellen Sie sicher, dass dieser Schritt auf dem Server ausgeführt wird, auf dem ADFS installiert ist.

Firefox T	
▲ Untrusted Connection × 🧶 Mozilla Firefox Start Page × +	
🗲 🕙 ɔs://ad0a. <b>identity\\us</b> /FederationMetadata/2007-06/FederationMetadata 🏠 🔻 😋 😫 🕶 Google	₽ 🖸 - 🖡 🏫
Most Visited Getting Started Suggested Sites Web Slice Gallery	
Opening FederationMetadata.xml	confirm that your
You have chosen to open: EederationMetadata.xml ed.	to prove that you
What should Firefox do with this file?	eone is trying to
Don't add an exception unless you know there's a good reason why this site doesn't identification.	use trusted
	<b>.</b>

Zuerst müssen Sie eine Verbindung mit dem ADFS (IdP) über einen Firefox-Browser herstellen, um die XML-Metadaten herunterzuladen. Öffnen Sie einen Browser unter https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml, und speichern Sie die Metadaten in einem lokalen Ordner.

Navigieren Sie jetzt zu CUCM-Konfiguration, und wählen Sie Menü > SAML Single Sign On (Menü für die einmalige Anmeldung) aus.



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

Kehren Sie zurück zu CUCM Administration, und wählen Sie **SYSTEM > SAML Single Sign-On** aus.

Firefox *								
🕮 Find and List User	s	× SAML Single Sign-O	n × 🖬	C Find and List LDAP Directories	× +			
+ A https://cu	cm0a/comadmin/sami5i	ingleSignOn.do		<u>⇔</u>	C Scogle	P 🗉	- +	Ĥ
cisco For	<b>Cisco Unified</b>	CM Administrati	on		Navigation Cisco Unifi admin Search Docum	ed CM Administr ientation Ab	ation 💌	Go ogout
System 👻 Call Roo	uting 👻 Media Reso	urces + Advanced Feature	e - Device - Application	n 👻 User Management 👻 B	ulk Administration 👻 Help 👻			
SAML Single Sig	n-On							
Cristie SAML S	ISO 🔥 Update Id	P Metadata File 👔 Export A	41 Metadata 🧳 Fix All Disc	abled Servers				
r Status								
() SAML SSO	disabled							
SAML Single S	ign-On (1 - 1 a	of 1)				Rows per l	Page 50	
Server Name cucm0a	SSO Status Disabled	Re-Import Metadata N/A	Last Metadata Impo Never	rt Export Metadata	Last Metadata Export Never	SS	o Test er Run Te	st

Wählen Sie SAML-SSO aktivieren aus.

Klicken Sie auf Weiter, um die Warnung zu bestätigen.

😔 Reset Warning - Mozilla Firefox 📃 🗖	×
https://cucmDa/ccmadmin/genericDialogWindow.do?windowtitlekey=genericdialogwindow.windowtitle.ssoenable	2
Web server connections will be restarted Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again. Continue Cancel	

FederationMetadata.xml-Metadaten zu importieren, die Sie zuvor wie im Bild gezeigt gespeichert haben.

Firefox *	_ D ×
🕮 Find and List Users × 🕮 SAML Single Sign-On Configuration × 🛤 Find and List LDAP Dire	ectories × +
A https://cucm0a/comadmin/saml9ingleSignOnConfigurationWtzard.do	습 국 C 🗧 - Google 👂 🖬 - 🖡 🏫
Cisco Unified CM Administration For Cisco Unified Communications Solutions	Navigation Cisco Unified CM Administration 💽 Go admin Search Documentation About Logout
System 👻 Cell Routing 👻 Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻 User Management	t - Bulk Administration - Help -
SAML Single Sign-On Configuration	
Next .	
Status Ready to import Identity Provider metadata trust file to cluster servers Identity Provider(IdP) Metadata Trust File To configure the trust relationship between the IdP and your servers, you must first obtain trust metadata fm manually obtain the file from the IdP and upload it here. IdP Metadata File Browse. No file selected. Initiate the Metadata In No file selected. This action must be successful for at least the Publisher before moving on to the next task in this wizard. Import IdP Metadata Next Cancel	rom your IdP and import it to your servers. You will need to

Wählen Sie die XML-Datei aus, und klicken Sie auf **Öffnen**, um sie unter "Favoriten" aus den Downloads in CUCM hochzuladen.

File Upload					E
G · Admire	strator - Downloads				🔹 👪 Search Downloads 🛃
Organize - New folder	e				三 • 🗊 0
* Favortes	Name -	Date modified	Type	Size	
E Desktop	AdfsSetup	2013/09/09 06:10 FM	Application	24 518 KB	
& Downloads	😁 FederationMetadata	2013/09/12 02:01 PM	XML Document	32 KB	
Ubraries Documents Music Pictures Videos Computer Network	S picpick inst	2012/09/12 11:09 44	Application	11 12943	
Få	e game: FederationMetadata				All Files
					<u>Open</u> Cancel

Klicken Sie nach dem Hochladen auf Import IdP Metadata (IDP-Metadaten importieren), um die IDP-Informationen in CUCM zu importieren. Bestätigen Sie, dass der Import erfolgreich war, und

klicken Sie auf Weiter, um fortzufahren.

🗧 SAML Singl	le Sign-On Configuration - Windows Internet Explorer 📃 🗖
<b>G</b> • [	🍘 https://10.1.1.100/ccmadmin/s 🔎 💌 😰 Ce 🖹 😏 🧔 SAML Single Sign-On Configu 🗙 👘 🏠 😭 😭
cisco	Cisco Unified CM Administration         Navigation         Cisco Unified CM Administration         Image: Comparison         Image:
System - C Help -	Call Routing   Media Resources   Advanced Features   Device   Application   User Management   Bulk Administration
SAML Singk	e Sign-On Configuration
Next	
Status Import Identity Pro To configure to your serv	succeeded for all servers rovider(IdP) Metadata Trust File e the trust relationship between the IdP and your servers, you must first obtain trust metadata from your IdP and import it vers. You will need to manually obtain the file from the IdP and upload it here.
IdP Metadat	ta File C:\Users\bbanks\Downloads\FederationMetadata.xml Browse
Initiate the This action r Import Io Next Ca	e Metadata Import must be successful for at least the Publisher before moving on to the next task in this wizard. dP Metadata Import succeeded for all servers

Wählen Sie den Benutzer aus, der dem Standard-CCM-Super-Benutzer angehört, und klicken Sie auf SSO-TEST AUSFÜHREN.

🍅 SAML Single Sign-On Configuration - Mozilla Firefox	-		×					
🛛 🖨 😂 https://cmpubhcsc.fhlab.com:8443/ccmadmin/samlSingleSignOnConfigurationWizard3.do?server	···· (	9 G	≡					
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 test can be run on any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is successful.								
1)Pick a valid username to use for this test								
You must already know the password for the selected username. This user must have administrator rights and also exist in the IdP.								
Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in a lockout.	dminist	rator						
Valid administrator Usernames farfar								
2)Launch SSO test page								
Run SSO Test								
Cancel								

Wenn ein Dialogfeld zur Benutzerauthentifizierung angezeigt wird, melden Sie sich mit dem entsprechenden Benutzernamen und Kennwort an.

ڬ Sign In - Mozilla Firefox	_		$\times$
🛛 🔒 https://ad.fhlab.com/adfs/ls/?SAMLRequest=nZJPTwIxEMXvflpN77C	IAi4NS	50 •••	≡
			^
FS			
Sign in with your organizational account			
	_		
farfar@fhlab.com			
•••••			
Sign in			
			~

Wenn alles korrekt konfiguriert wurde, sollte die Meldung angezeigt werden, dass der SSO-Test erfolgreich durchgeführt wurde.



Klicken Sie auf SCHLIESSEN und FERTIG, um fortzufahren.

Die grundlegenden Konfigurationsaufgaben zur Aktivierung von SSO auf CUCM mithilfe von ADFS wurden jetzt erfolgreich abgeschlossen.

## Konfigurieren von SSO auf CUC

Zum Aktivieren von SSO in Unity Connection kann derselbe Prozess ausgeführt werden.

#### LDAP-Integration mit CUC.

€ → ୯ û	💿 🚔 😂 https://cucpub	hcsc.fhlab.co	m/cuadmin/hom		·· 🖂 🗘	III\ 🗊	\$ ≡		
Cisco Unity Co For Cisco Unified Con	nnection Administr	ation				Naviga farfa	ion Cisco Unity Connection A Search Documentation	dministration About	✓ Go Sign Ou
Cisco Unity Connection	SAML Single Sign on							SAML Sin	igle Sign
System Settings General Configuration Cluster Authentication Rules Restriction Tables Ucenses Schedules	SAML Single Sign on     SSO Mode     Otater wide (One m     Per node (One meta     Classes SAML SSO	Refresh He netadata file p idata file per i O Update KP	er cluster. Require node) Metadata File 👔	s multi-server Tomcat certificate) Export Al Metadala 🥜 Fix Al Disa	bled Servers				e
- Holiday Schedules	SAML Single Sign-0	m (1-2	of 2)				Roi	vs per Page	50 v
Subject Line Formats	Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Te	ıt	
Enterprise Parameters	cucpubhcsc.fhlab.com	SAML	N/A	April 29, 2020 10:52:36 AM PDT	📩 File	April 28, 2020 5:54:01 PM PDT	Passed - April 29, 2020 11:05:10 AM PDT	Run SSC	Test
Service Parameters         cucsubhcsc.fhlab.com         SAML         April 29, 2020 10:52:36 AM         April 29, 2020 5:54:00 PM         Passed - April 29, 2020         Run S           Plugins         PDT         PDT         PDT         PDT         PDT         PDT         Run S								Run SSC	Test
B LDAP SAML Single Sign on	Disable SAML SSO	Export All	Metadata Upd	ate IdP Metadata File Fix All D	isabled Server	5			

Konfigurieren der LDAP-Authentifizierung

← → ♂ ☆	A      https://cucpubhcsc.fhlab.com/cuadn	in/home.do		⊡ ☆	li\ ⊡ 📽 ≡
cisco Unity Con For Cisco Unified Comm	nection Administration			lavigation Cisco Unity Con farfar Search Docum	nection Administration 🐱 😡
Cisco Unity Connection	LDAP Authentication				LDAP Authentication
Video Services Accounts Status Dial Plan Partitions Search Spaces System Settings General Configuration Cluster Authentication Rules Restriction Tables Ucenses Schedules Global Nicknames Schedules	LDAP Authentication Refresh Help Save Status Status: Ready LDAP Authentication for End Users LDAP Manager Distinguished Name <sup>®</sup> (hiabUA LDAP Password <sup>®</sup> LDAP User Search Base <sup>®</sup> (n=use	śministrator			
Attachment Descriptions Enterprise Parameters Service Parameters Plugins Rax Server CDAP LDAP Setup UDAP Directory Configuration LDAP Authentication	LDAP Server Information Host Name 10.89.228.226 Add Another Redundant LDAP Server Save Fields marked with an asterisk (*) are require	pr IP Address for Server* d.	LDAP Port <sup>*</sup> Use TL5		

Importieren Sie die Benutzer aus LDAP, denen Voicemail zugewiesen ist, sowie den Benutzer, der für das Testen von SSO verwendet wird.

Cisco Unity Connection	Import Users				Import U			
E Users ^	Import Users Refresh Help	port Users Refresh Help						
Users Import Users	e Clature							
Synch Users	atatus							
Class of Service	Found 1 LDAP User(s)							
Class of Service	r Find							
Class of Service Membership	Find End Users In LDAP Director	( ~						
User Templates	Where Alias V Begins W	ith u	Find					
Call Handler Templates								
Contact Templates	- Import With							
B Notification Templates	Based on Template Unicemailuse	demolate w						
Contacts								
Contacts	Directory Cornels Decults							
Distribution Lists	Directory search Results							
System Distribution Lists	Import Selected Import All	25 V Rows Per Page						
Call Management								
System Call Handlers	Alias 🔺	First Name	Last Name	Phone Number	Extension			
Directory Handlers	hugohugo hugo hugo 1002 1002							
Interview Handlers								
Custom Recordings	Import Selected Import All							

#### Navigieren Sie zu Benutzer > Bearbeiten > Rollen wie im Bild gezeigt.

Cisco Unity Connection								
B Users Edit User Basics (hugohugo)								
Users	User E	dit Refresh Help						
Import Users	Court	User Basics						
Class of Service	Save	Decemard Settinge						
Class of Service	State	Password Settings						
Class of Service Membership	🗌 🛈 🚣	Change Password	ectory					
Templates		Roles						
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     Contacts	Disala							
E Distribution Lists	Displa	Mailbox						
System 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						
		Greetings						
Custom Recordings	LDAP	Dest Creation Decedies						
E-Call Routing	<ul> <li>Int</li> </ul>	Post Greeting Recording						
Message Storage	ODo	Notification Devices						

Weisen Sie dem Testbenutzer die Rolle des Systemadministrators zu.

*	Cisco Unity Connection	Edit Roles	Search Users + Edit User Basics (hugohugo) + Edit Role
Ξ	Users ^	User Edit Refresh Help	
	Users		
	Import Users	Save	
	Synch Users		
Ξ	Class of Service	Roles	
	Class of Service	Assigned Roles	
	Class of Service Membership		
Ξ	Templates		
	User Templates	M	
	Call Handler Templates	^ <b>v</b>	
	Contact Templates	Available Roles	
	Notification Templates	Remote Administrator	
Ξ	Contacts	System Administrator	
	Contacts	Technican Technicat	
E	Distribution Lists	User Administrator V	
	System Distribution Lists		
E	Call Management	Save	

## **CUC-Metadaten**

Sie sollten jetzt CUC-Metadaten heruntergeladen, RelyingPartyTrust für CUC erstellt, CUC-Metadaten hochgeladen und die Regeln erstellt haben, die I AD FS für ADFS 3.0 darstellt.



Gehen Sie zu SAML Single Sign-On und aktivieren Sie SAML SSO.

🗉 SAML Single Sign on Configuration - Mozilla Firefox								-		×
🗊 🖴 📽 https://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?serverName: •							verName: ••• 🕻	ጋ 습	≡	
SAML S	ngle Sign on Configuratio	n					SA	AML Single Sign o	n Config	uration
SAML S	ngle Sign on Configuration	Refresh	Help							
Test S	SO Setup									
This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test on any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is succ							ervers. This test of this test of this test is success	can be ru sful.	IN	
1)Pick	a valid username to use for t	this test								
You m This us	ust already know the passwor er must have administrator r	rd for the s rights and a	elected userna also exist in the	me. IdP.						
	lease use one of the Usernan ockout.	nes shown	below. Using a	ny othe	er Usern	ame to lo	og into the IdP may	result in adminis	trator	
Valid a	dministrator Usernames									
farfar hugol	ugo		^							
			~							
2)Laur	ch SSO test page									
Run	SSO Test									
Kun	550 1050									
Cance	21									
SAML Sing	e Sign on Configuration - Mozilla Firefox					×			- 0	ı ×
	ttps://cucpubhcsc. <b>fhlab.com</b> /cuadmin/samlSin	gleSignOnConfig	urationWizard3.do?test	Status=1 •	© ☆	=		• ⊠ ☆	lin 🖸	: ≡
SAME Single	ign on Configuration Refresh Help		SA	ML Single Si	ign on Contig	uration	Navigat farfar	ion Cisco Unity Connection	Administration	Go Sign Out
Status									SAML Sir	gle Sign on
SSO M	tadata Test Successful				-					
Close	Test SAML - Mozilla Firefox      A 25. https://guopubless.fblab.com	/ssoso/pages/Tes	=		=					
		t and a high and a set	1330 gsp 1330 pege - 11 de		-	ers				
	SSO Tes	t Succ	eeded!							
						sort	Last Metadata Export	Ro SSO Te	ws per Page	50 V
	Congratulations on a successi close	ful SAML SSO e this window	configuration test	t. Please		File	April 28, 2020 5:54:01 PM PDT	Passed - May 24, 2020 3:17:04 PM PDT	Run SSC	Test
						File	April 28, 2020 5:54:00 PM PDT	Passed - April 29, 2020 11:05:37 AM PDT	Run SSC	) Test
		Close				Servers	£			

## Konfigurieren von SSO auf Expressway

#### Metadaten in Expressway C importieren

Öffnen Sie einen Browser unter https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml, und speichern Sie die Metadaten in einem lokalen Ordner.

#### Upload to **Configuration > Unified Communications > IDP**.

## Metadaten aus Expressway C exportieren

Gehen Sie zu configuration -> Unified Communications -> IDP -> SAML-Daten exportieren.

Der Cluster-Modus verwendet ein selbstsigniertes Zertifikat (mit langer Lebensdauer), das in der SAML enthalten ist.

Metadaten und werden zum Signieren von SAML-Anforderungen verwendet

- Klicken Sie im clusterweiten Modus auf Herunterladen der einzelnen clusterweiten Metadatendatei.
- Klicken Sie im Peer-Modus neben dem Peer auf Herunterladen, um die Metadatendatei für einen einzelnen Peer herunterzuladen. Um alle Dateien in eine ZIP-Datei zu exportieren, klicken Sie auf Alle herunterladen.

# Hinzufügen eines Vertrauens für eine vertrauenswürdige Partei für Cisco Expressway-E

Erstellen Sie zunächst Relying Party Trusts für die Expressway-ES, und fügen Sie dann eine Anspruchsregel hinzu, um Identität als UID-Attribut zu senden.



#### OAuth mit Refresh Login

Überprüfen Sie in Cisco CUCM Enterprise-Parametern, ob der Parameter OAuth with Refresh login flow aktiviert ist. Gehen Sie zu **Cisco Unified CM Administration > Enterprise Parameters > SSO and OAuth Configuration**.

	-SSO and OAuth Configuration		
I	550 and orlatil configuration		
l	OAuth Token Expiry Timer (minutes) *	60	]60
l	OAuth Refresh Token Expiry Timer (days) *	60	] 60
l	Redirect URIs for Third Party SSO Client		]
l	SSO Login Behavior for iOS *	Use embedded browser (WebView)	Use embedded browser (WebView)
l	OAuth with Refresh Login Flow *	Enabled	Disabled
l	Use SSO for RTMT *	True 🗸	True
L.			

## Authentifizierungspfad

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

- Wenn der Authentifizierungspfad auf "SAML SSO Authentication" gesetzt ist, können nur Jabber-Clients, die ein SSO-fähiges Unified CM-Cluster verwenden, MRA auf diesem Expressway verwenden. Hierbei handelt es sich um eine Konfiguration, die nur für SSOs gilt.
- Die Expressway-MRA-Unterstützung für alle IP-Telefone, alle TelePresence-Endpunkte und alle Jabber-Clients, die an ein Unified CM-Cluster weitergeleitet werden, das nicht für SSO konfiguriert ist, erfordert den Authentifizierungspfad, um die UCM-/LDAP-Authentifizierung einzuschließen.
- Wenn ein oder mehrere Unified CM-Cluster Jabber SSO unterstützen, wählen Sie "SAML SSO and UCM/LDAP" aus, um sowohl SSO als auch grundlegende Authentifizierung zuzulassen.

## SSO-Architektur

SAML ist ein XML-basiertes, auf offenen Standards basierendes Datenformat, mit dem Administratoren nach der Anmeldung bei einer dieser Anwendungen problemlos auf bestimmte Cisco Collaboration-Anwendungen zugreifen können. SAML SSO verwendet das SAML 2.0-Protokoll, um domänenübergreifende und produktübergreifende einmalige Anmeldung für Cisco Collaboration-Lösungen zu ermöglichen.

## Anmeldungsablauf am Standort



Figure :SAML Single sign SSO Call Flow for Collaboration Servers



#### MRA-Anmeldeablauf

## OAuth

OAuth ist ein Standard, der die Autorisierung unterstützt. Ein Benutzer muss authentifiziert werden, bevor er autorisiert werden kann. Der Autorisierungscode-Grant-Flow stellt eine Methode bereit, mit der ein Client auf Zugriffs- und Aktualisierungs-Token zugreifen kann, um auf eine Ressource zuzugreifen (Unified CM-, IM&P-, Unity- und Expressway-Dienste). Dieser Datenfluss basiert auch auf Umleitung und erfordert daher, dass der Client mit einem vom Benutzer gesteuerten HTTP-User-Agent (Webbrowser) interagieren kann. Der Client stellt eine erste Anforderung an den Autorisierungsserver über HTTPS. Der OAuth-Server leitet den Benutzer an einen Authentifizierungsdienst um. Diese kann auf Unified CM oder einer externen IDP ausgeführt werden, wenn SAML SSO aktiviert ist. Je nach verwendeter Authentifizierungsmethode kann dem

Endbenutzer eine Webseitenansicht zur Selbstauthentifizierung angezeigt werden. (Die Kerberos-Authentifizierung ist ein Beispiel, das keine Webseite anzeigen würde.) Im Gegensatz zum impliziten Grant-Flow führt ein erfolgreicher Grant-Fluss dazu, dass die OAuth-Server dem Webbrowser einen "Autorisierungscode" ausgeben. Hierbei handelt es sich um einen einmaligen, kurzlebigen eindeutigen Code, der dann vom Webbrowser an den Client zurückgegeben wird. Der Client stellt dem Autorisierungsserver diesen "Autorisierungscode" zusammen mit einem vorinstallierten geheimen Schlüssel zur Verfügung und erhält im Austausch ein "Zugriffstoken" und ein "Aktualisierungstoken". Der in diesem Schritt verwendete Clientgeheim ermöglicht es dem Autorisierungsdienst, die Verwendung auf registrierte und authentifizierte Clients zu beschränken. Die Token werden für folgende Zwecke verwendet:

### Zugriffs-/Aktualisierungstoken

Zugriffs-Token: Dieses Token wird vom Autorisierungsserver ausgegeben. Der Client stellt das Token einem Ressourcenserver zur Verfügung, wenn er auf geschützte Ressourcen auf diesem Server zugreifen muss. Der Ressourcenserver kann das Token validieren und Verbindungen mithilfe des Tokens vertrauen. (Cisco Access Token haben standardmäßig eine Lebensdauer von 60 Minuten.)

Aktualisierungstoken: Dieses Token wird erneut vom Autorisierungsserver ausgegeben. Der Client stellt dieses Token zusammen mit dem Clientgeheimnis dem Autorisierungsserver zur Verfügung, wenn das Zugriffstoken abgelaufen ist oder abläuft. Wenn das Aktualisierungstoken noch gültig ist, gibt der Autorisierungsserver ein neues Zugriffstoken aus, ohne dass eine weitere Authentifizierung erforderlich ist. (Die Standardeinstellung der Cisco Refresh Tokens beträgt 60 Tage.) Wenn das Aktualisierungstoken abgelaufen ist, muss ein neuer vollständiger OAuth-Autorisierungscode-Fluss initiiert werden, um neue Token zu erhalten.

#### Der Ablauf der OAuth-Autorisierungscodes für die Gewährung ist besser

Im impliziten Grant-Flow wird das Zugriffstoken über einen HTTP-Benutzer-Agent (Browser) an den Jabber-Client übergeben. Im Berechtigungscode-Grant-Fluss wird das Zugriffstoken direkt zwischen dem Autorisierungsserver und dem Jabber-Client ausgetauscht. Das Token wird mithilfe eines zeitlich begrenzten eindeutigen Autorisierungscodes vom Autorisierungsserver angefordert. Dieser direkte Austausch des Zugriffs-Tokens ist sicherer und reduziert das Risiko.

Der OAuth-Autorisierungscode-Grant-Fluss unterstützt die Verwendung von Aktualisierungstoken. Dies verbessert die Benutzerfreundlichkeit, da die Benutzer sich nicht so häufig erneut authentifizieren müssen (standardmäßig 60 Tage).

## Konfigurieren von Kerberos

#### Windows-Authentifizierung auswählen

# Internetinformationsdienste-Manager (IIS) > Sites > Default Web Site > Authentication > Windows Authentication > Advance Settings.

- 1. Deaktivieren Sie Kernel-Modus-Authentifizierung aktivieren.
- 2. Stellen Sie sicher, dass der erweiterte Schutz deaktiviert ist.



## ADFS unterstützt beide Kerberos NTLM

Stellen Sie sicher, dass AD FS Version 3.0 sowohl das Kerberos-Protokoll als auch das NT LAN Manager-Protokoll (NTLM) unterstützt, da alle Nicht-Windows-Clients Kerberos nicht verwenden können und sich auf NTLM verlassen.

Wählen Sie im rechten Teilfenster Anbieter aus, und stellen Sie sicher, dass Negotiate und NTLM unter Enabled Providers (Aktivierte Anbieter) vorhanden sind:

<b>S</b>	Internet Information Se	ervices (IIS) Man	ager		_ 🗆 X
€ ● AD → Sites → Default Web Site	: •				🖬 🗟 🏠 🔞 •
File View Help					
Connections	Authorities			Alerts	
🔍 - 🗔 🖄 😥	Authentication			A Click here	to learn how to
Start Page	Group by: No Grouping			configure Protection	Extended
AD (FHLAB\administrator)	Name	Status	Response Type	Actions	
4 - 🙆 Sites	Anonymous Authentication	Enabled		Dicable	
Default Web Site	ASP.NET Impersonation Forms Authentication	Disabled	HTTP 302 Login/Redir	Advanced	Cattings
	Windows Authentication	Enabled	HTTP 401 Challenge	Providers	secongs
			Providers	? X	
			Tiondels		
	Enable	d Providers:			
	Negot	iate		Move Up	
	NTLM			L Marrie David	
				Move Down	
				Remove	
	<				
	Select Teatures View 🙀 to add	a provider from the it to the enabled pr	list of available providers and oviders.	click Add	
Configuration: 'localhost' applicationHost.config , <loca< td=""><td>tion path="Default W Availal</td><td>ble Providers:</td><td></td><td></td><td>•<u>1</u>.:</td></loca<>	tion path="Default W Availal	ble Providers:			• <u>1</u> .:
			~	Additiva	10 POWS
				Go to S	stem in Control P
			04	Window	S. Windows Se
			UK	Cancel	

## Konfigurieren von Microsoft Internet Explorer

Stellen Sie sicher, dass Internet Explorer > Erweitert > Integrierte Windows-Authentifizierung aktivieren aktiviert ist.

Internet (	Options					? <mark>- X-</mark>				
General	Security	Privacy	Content	Connecti	ons Programs	Advanced				
Setting	Settings									
	<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 of the signature is invited for publisher's certificate revocation</li> <li>Check for publisher's 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 determined for the signature of the signa</li></ul>									
•						Þ				
*Ta Reset Res	*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		Cancel	Apply				

ADFS-URL unter Sicherheit > Intranetzonen > Standorte hinzufügen