

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-Autorisierungs-codes 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 \(IE\)](#)

[Sites, die zu IE hinzugefügt werden](#)
[Problem bei fehlender Synchronisierung](#)
[Aufrufen eines Tokens](#)
[Bootstrap-Datei](#)
[SSO fehlschlägt MSIS7066](#)

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.

The screenshot shows the DNS console for the AD domain. The left pane shows the hierarchy: DNS > AD > Forward Lookup Zones > fhlab.com. The right pane shows a list of records:

| Name | Type |
|-------------------------|--------------------------|
| _msdcs | |
| _sites | |
| _tcp | |
| _udp | |
| DomainDnsZones | |
| ForestDnsZones | |
| (same as parent folder) | Start of Authority (SOA) |
| (same as parent folder) | Name Server (NS) |
| (same as parent folder) | Host (A) |
| ad | Host (A) |
| cmpubhcsc | Host (A) |
| cmsubhcsc | Host (A) |
| cucpubhcsc | Host (A) |
| cucsubhcsc | Host (A) |
| expwyc | Host (A) |
| expwye | Host (A) |
| imppubhcsc | Host (A) |
| imsubhcsc | Host (A) |

PTR-Datensätze (Zeiger)

The screenshot shows the DNS console with the PTR records for the fhlab.com domain selected. The right pane shows a list of records with columns for Name, Type, Data, and Timestamp:

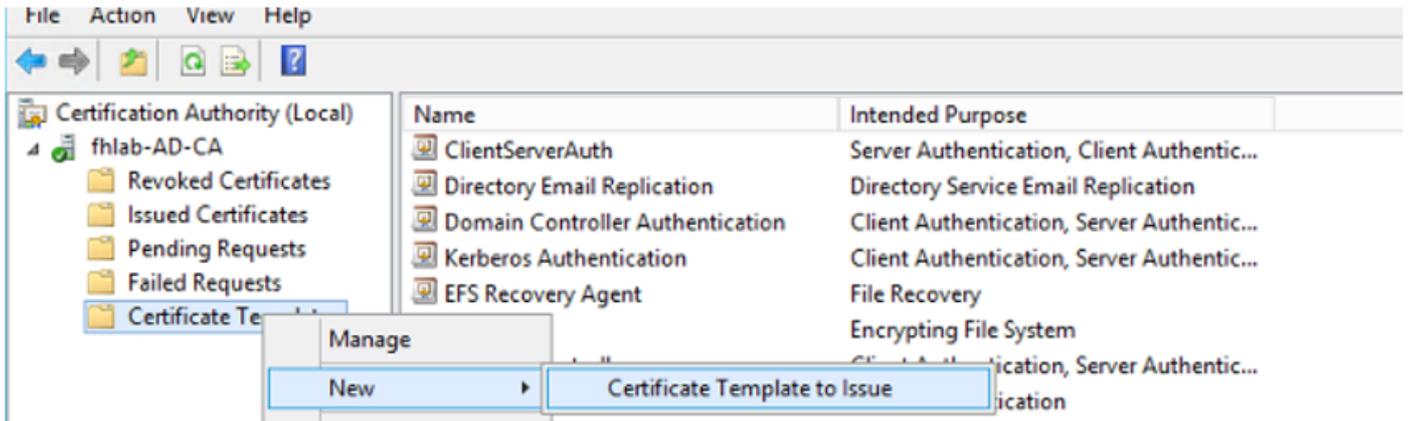
| Name | Type | Data | Timestamp |
|-------------------------|--------------------------|---|-----------------------|
| (same as parent folder) | Start of Authority (SOA) | [14], ad.fhlab.com., hostmaster.fhlab.co... | static |
| (same as parent folder) | Name Server (NS) | ad.fhlab.com. | static |
| 10.89.228.144 | Pointer (PTR) | expwyc.fhlab.com. | static |
| 10.89.228.145 | Pointer (PTR) | expwye.fhlab.com. | static |
| 10.89.228.146 | Pointer (PTR) | cmpubhcsc.fhlab.com. | static |
| 10.89.228.147 | Pointer (PTR) | cmsubhcsc.fhlab.com. | static |
| 10.89.228.148 | Pointer (PTR) | imppubhcsc.fhlab.com. | static |
| 10.89.228.150 | Pointer (PTR) | imsubhcsc.fhlab.com. | static |
| 10.89.228.151 | Pointer (PTR) | cucpubhcsc.fhlab.com. | static |
| 10.89.228.153 | Pointer (PTR) | cucsubhcsc.fhlab.com. | static |
| 10.89.228.154 | Pointer (PTR) | win10.fhlab.com. | 5/12/2020 10:00:00 AM |
| 10.89.228.226 | Pointer (PTR) | ad.fhlab.com. | 5/12/2020 11:00:00 AM |
| 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.

| Name | Type | Data | Timestamp |
|------------|------------------------|------------------------------------|-----------------------|
| _cisco-uds | Service Location (SRV) | [0][0][8443] cmsubhcsc.fhlab.com. | static |
| _cisco-uds | Service Location (SRV) | [0][0][8443] cmpubhcsc.fhlab.com. | static |
| _cuplogin | Service Location (SRV) | [0][0][8443] impsubhcsc.fhlab.com. | static |
| _cuplogin | Service Location (SRV) | [0][0][8443] impubhcsc.fhlab.com. | static |
| _gc | Service Location (SRV) | [0][100][3268] ad.fhlab.com. | 5/12/2020 10:00:00 AM |
| _kerberos | Service Location (SRV) | [0][100][88] ad.fhlab.com. | 5/12/2020 10:00:00 AM |
| _kpasswd | Service Location (SRV) | [0][100][464] ad.fhlab.com. | 5/12/2020 10:00:00 AM |
| _ldap | Service Location (SRV) | [0][100][389] ad.fhlab.com. | 5/12/2020 10:00:00 AM |

- 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.

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 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 source (Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```

8V8mWY/9kjhgfnpeBzAAW++t0GzBjnvqaT8StWM
LA0dphF6LrurUeY2KLvMLmK1ft7aSy483yCsm0v1
OWQFzoLb3bS80ziW7fQEPWSaCg567DMOQ8PkZt5N
10y/Ip6oDzTdZE9w2p8rK3YxcbyfovStOijIirh
AM/GjnzQ
-----END CERTIFICATE REQUEST-----

```

Certificate Template:

Additional Attributes:

Attributes:

- User
- Basic EFS
- Administrator
- EFS Recovery Agent
- Web Server
- Subordinate Certification Authority
- ClientServerAuth

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 existing CSR for that type

Generate Certificate Signing 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** RSA

Key Length* 2048

Hash Algorithm* SHA256

Generate Close

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 Go

osadmin Search Documentation About Logout

Show Settings Security Software Upgrades Services Help

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

7 records found

Certificate List (1 - 7 of 7) Rows per Page 50

Find Certificate List where Certificate begins with tomcat Find Clear Filter

| Common Name | Type | Key Type | Distribution | Issued By | Expiration | Description |
|--------------------------------------|-------------|----------|----------------------|-------------------------|------------|---|
| tomcat cmpubhcsc-ms.fhlab.com | CA-signed | RSA | Multi-server(SAN) | fhlab-AD-CA | 04/18/2022 | Certificate Signed by fhlab-AD-CA |
| tomcat-ECDSA cmsubhcsc-EC.fhlab.com | Self-signed | EC | cmpubhcsc.fhlab.com | cmpubhcsc-EC.fhlab.com | 04/02/2025 | Self-signed certificate generated by system |
| tomcat-trust imppubhcsc-EC.fhlab.com | Self-signed | EC | imppubhcsc.fhlab.com | imppubhcsc-EC.fhlab.com | 04/02/2025 | Trust Certificate |
| tomcat-trust cmsubhcsc-EC.fhlab.com | Self-signed | EC | cmsubhcsc.fhlab.com | cmsubhcsc-EC.fhlab.com | 04/02/2025 | Trust Certificate |
| tomcat-trust impsubhcsc-EC.fhlab.com | Self-signed | EC | impsubhcsc.fhlab.com | impsubhcsc-EC.fhlab.com | 04/02/2025 | Trust Certificate |
| tomcat-trust cmpubhcsc-EC.fhlab.com | Self-signed | EC | cmpubhcsc.fhlab.com | cmpubhcsc-EC.fhlab.com | 04/02/2025 | Trust Certificate |
| tomcat-trust fhlab-AD-CA | Self-signed | RSA | fhlab-AD-CA | fhlab-AD-CA | 04/18/2025 | Signed Certificate |

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

Certificate List (1 - 6 of 6) Rows per Page 50

Find Certificate List where Certificate begins with tomcat Find Clear Filter

| Common Name | Type | Key Type | Distribution | Issued By | Expiration | Description |
|--------------------------------------|-------------|----------|----------------------|-------------------------|------------|-----------------------------------|
| tomcat cucpubhcsc-ms.fhlab.com | CA-signed | RSA | Multi-server(SAN) | fhlab-AD-CA | 04/28/2022 | Certificate Signed by fhlab-AD-CA |
| tomcat-trust fhlab-AD-CA | Self-signed | RSA | fhlab-AD-CA | fhlab-AD-CA | 04/18/2025 | Signed Certificate |
| tomcat-trust imppubhcsc-EC.fhlab.com | Self-signed | EC | imppubhcsc.fhlab.com | imppubhcsc-EC.fhlab.com | 04/02/2025 | Trust Certificate |
| tomcat-trust cmsubhcsc-EC.fhlab.com | Self-signed | EC | cmsubhcsc.fhlab.com | cmsubhcsc-EC.fhlab.com | 04/02/2025 | Trust Certificate |
| tomcat-trust cucpubhcsc-EC.fhlab.com | Self-signed | EC | cucpubhcsc.fhlab.com | cucpubhcsc-EC.fhlab.com | 04/02/2025 | Trust Certificate |

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

- IIS

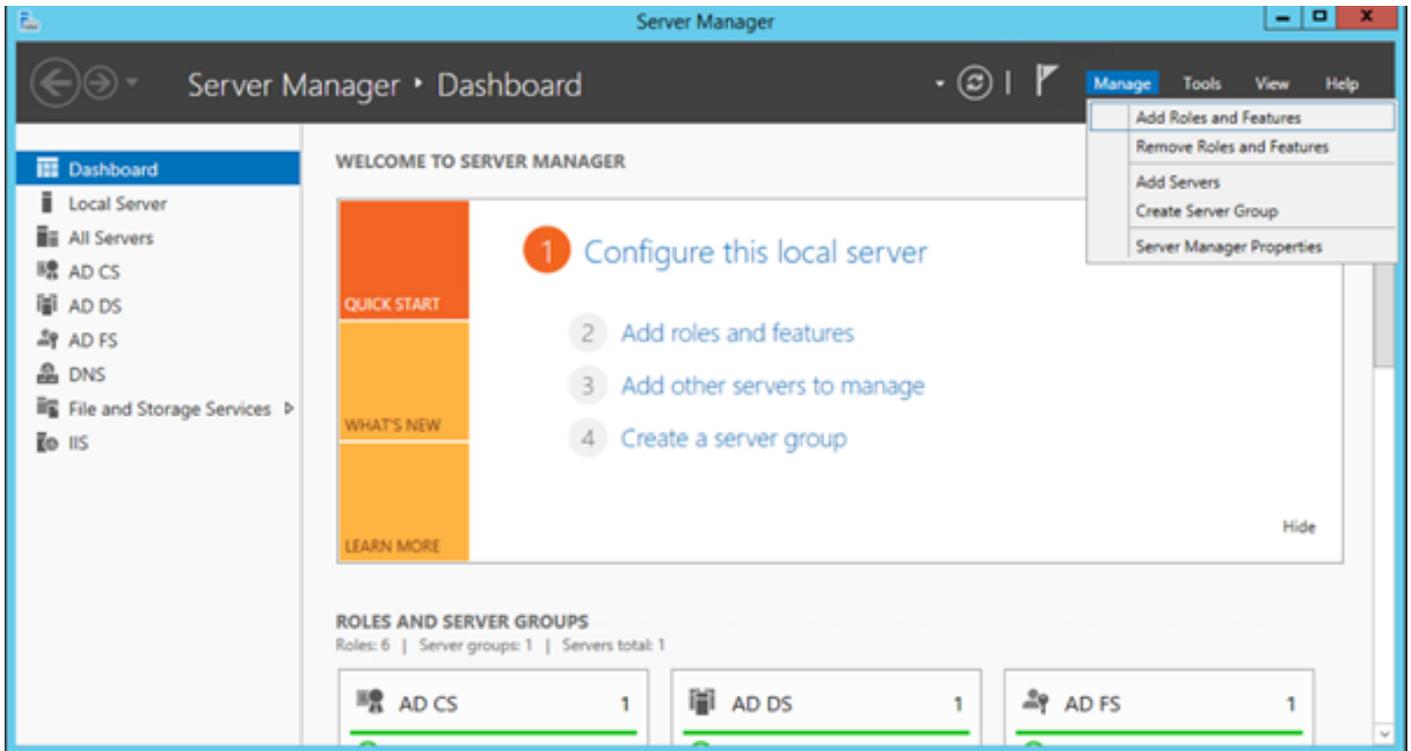
Andernfalls wird in diesem Abschnitt die Installation dieser Rollen beschrieben. Andernfalls

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

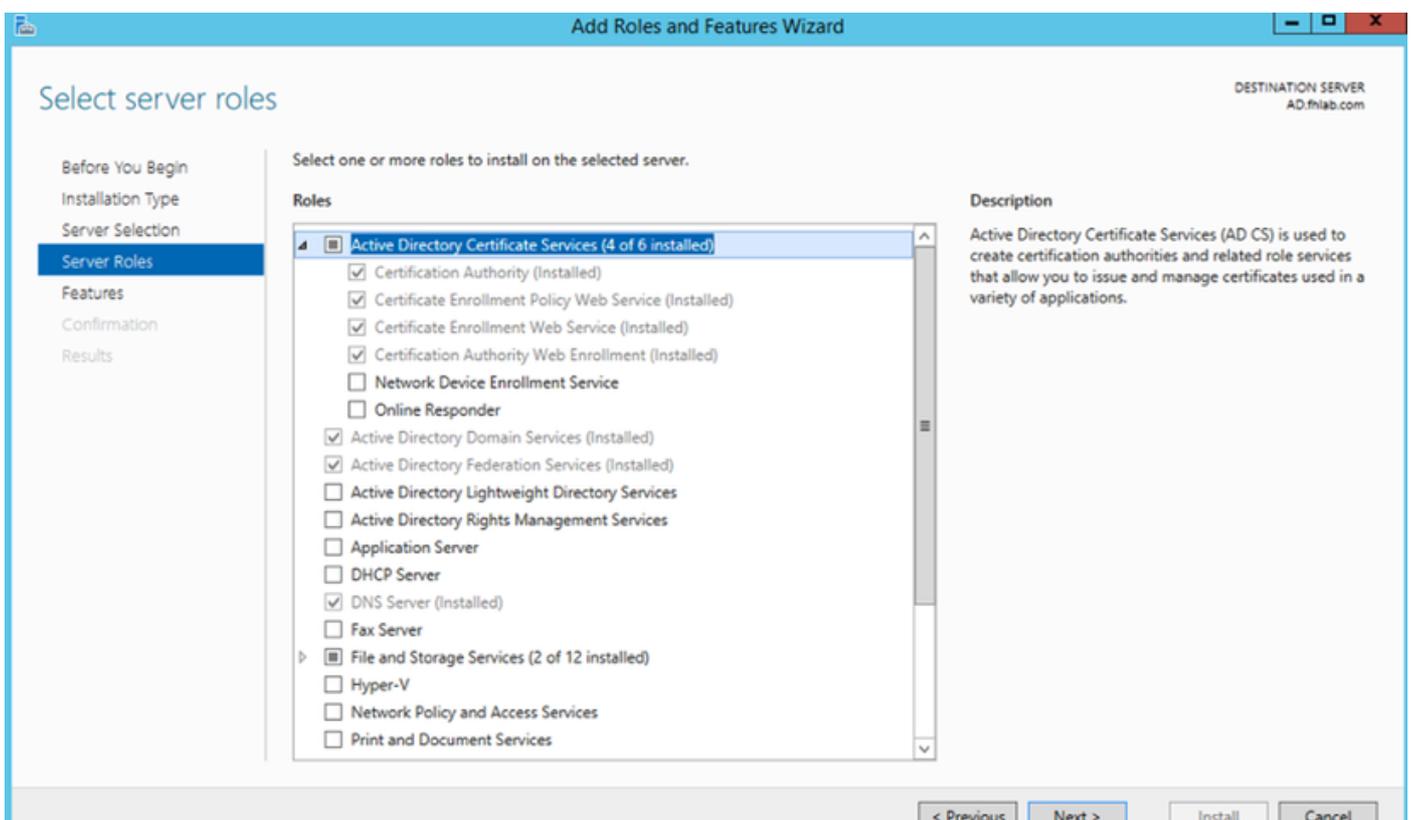
Nach der Installation von Windows 2012 R2 mit DNS können Sie den Server auf einen Domänencontroller verweisen.

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

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



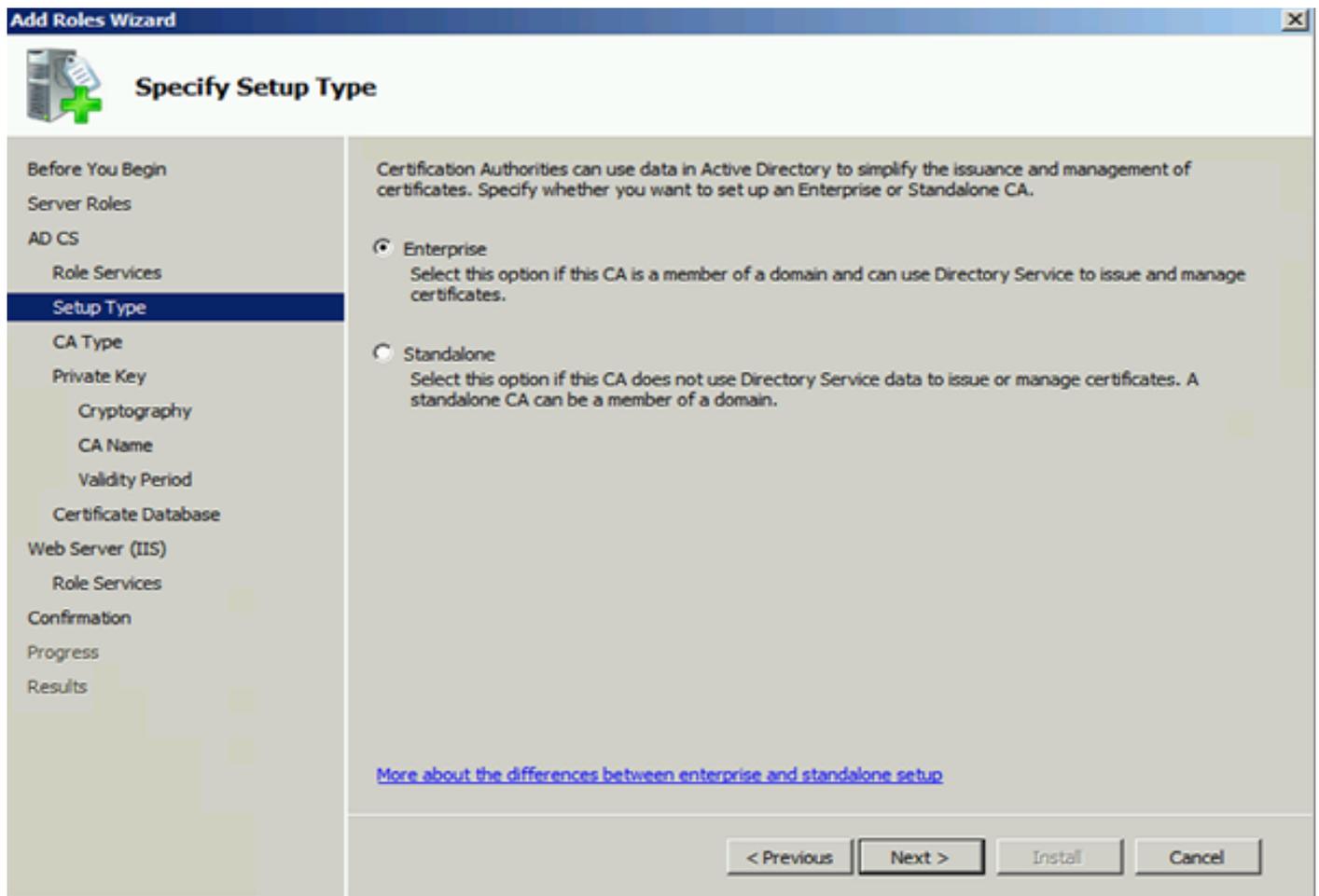
Wählen Sie die Rolle **Active Directory-Zertifikatdienste** aus.



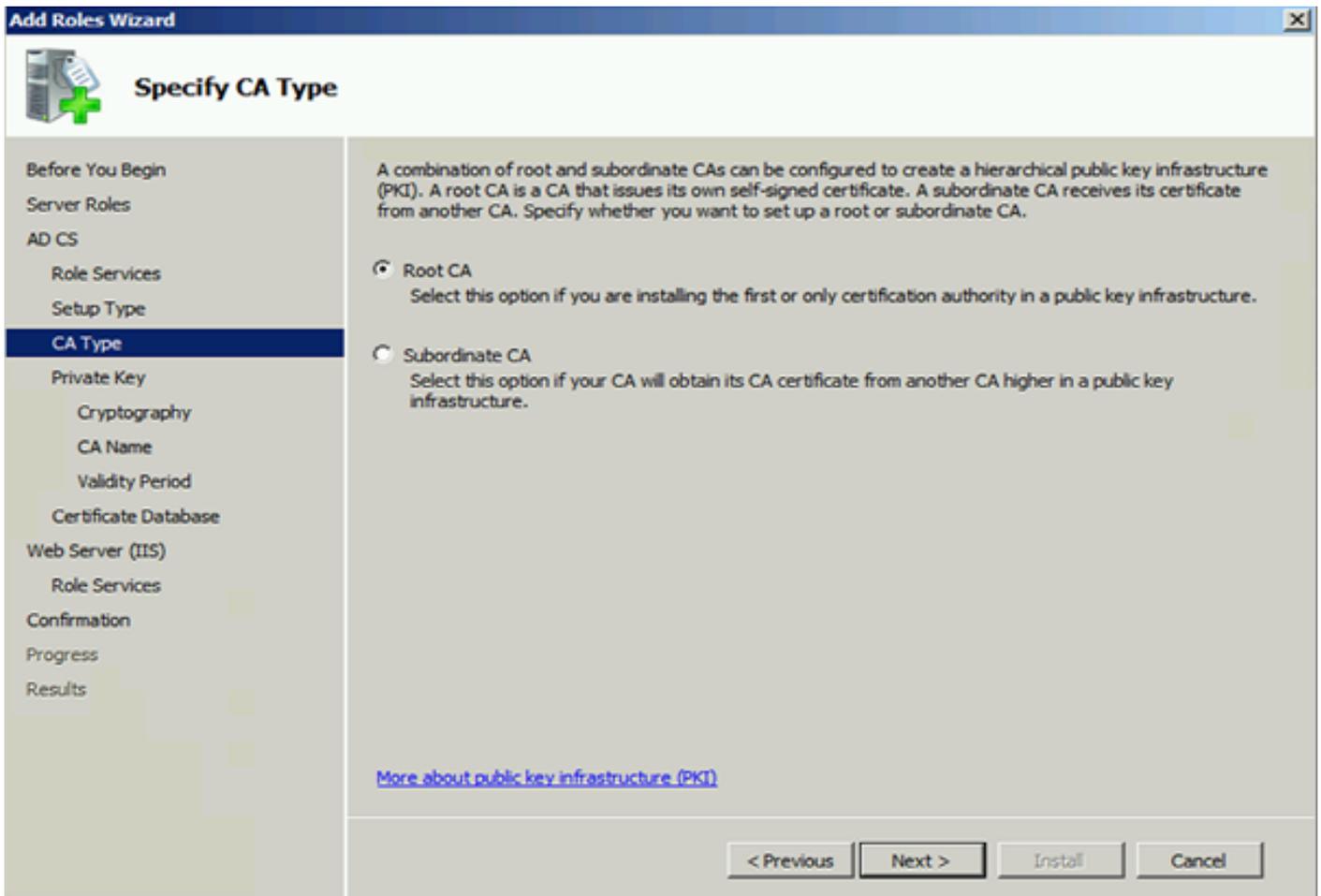
Stellen Sie diese Dienste bereit - Webdienst für die Zertifizierungsstellen-Registrierung für Zertifikatszertifikate. Nachdem diese beiden Rollen installiert wurden, konfigurieren Sie sie, und installieren Sie dann den **Webdienst für die Zertifikatregistrierung** und die **Webregistrierung der Zertifizierungsstelle**.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

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

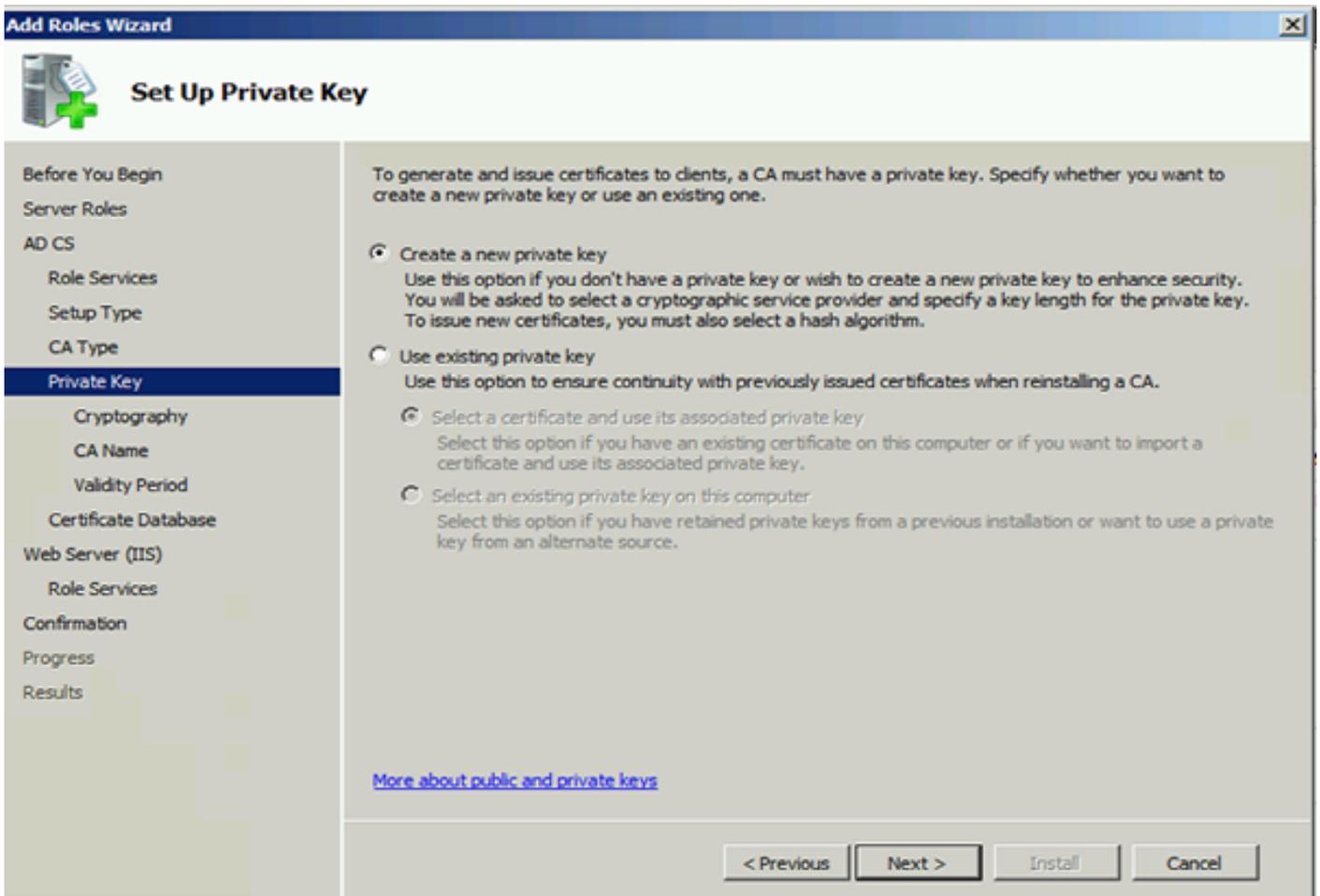
Je nach Bereitstellung können Sie Enterprise oder Standalone auswählen.



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.

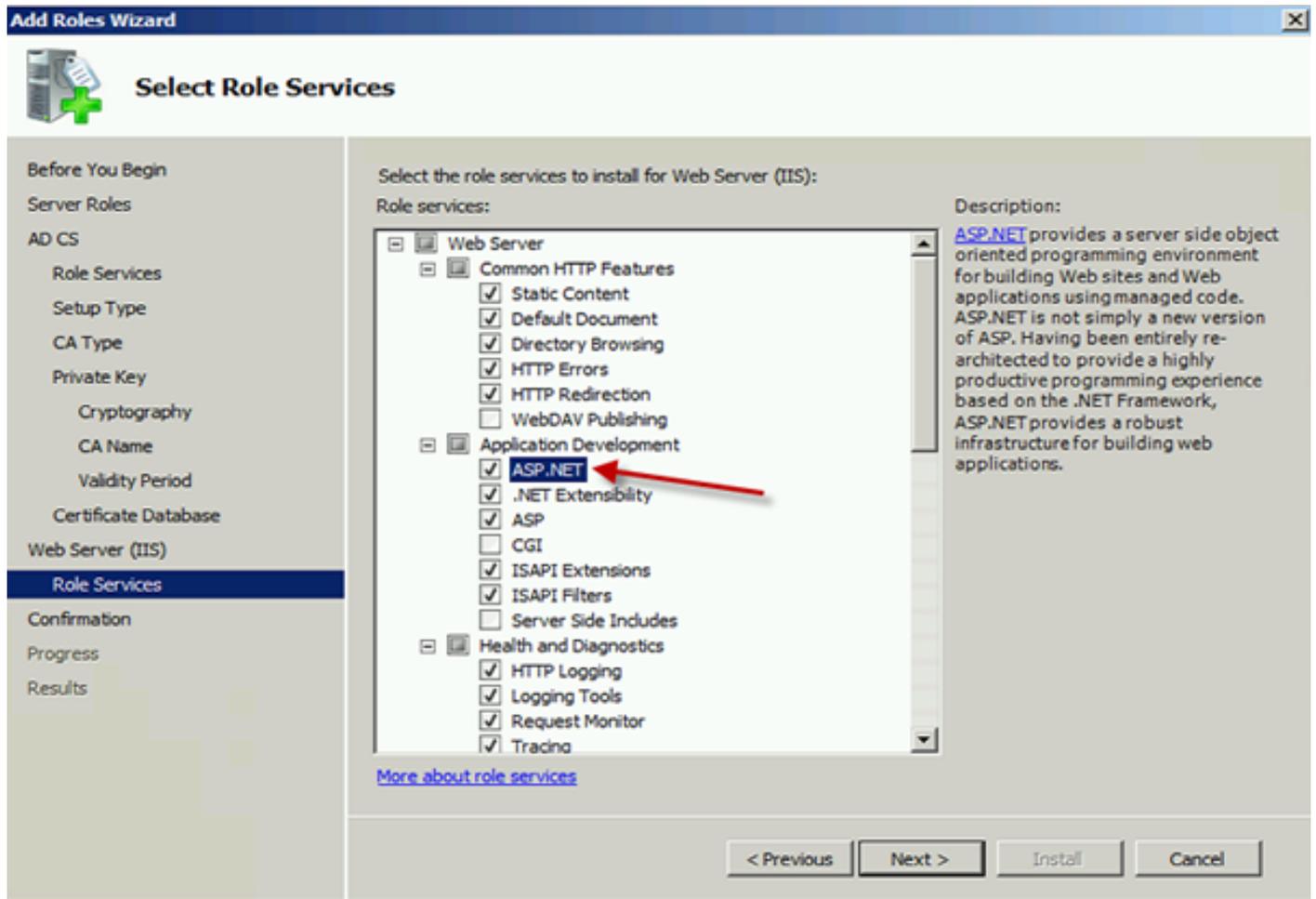


Im nächsten Schritt erstellen Sie einen privaten Schlüssel für Ihre CA.

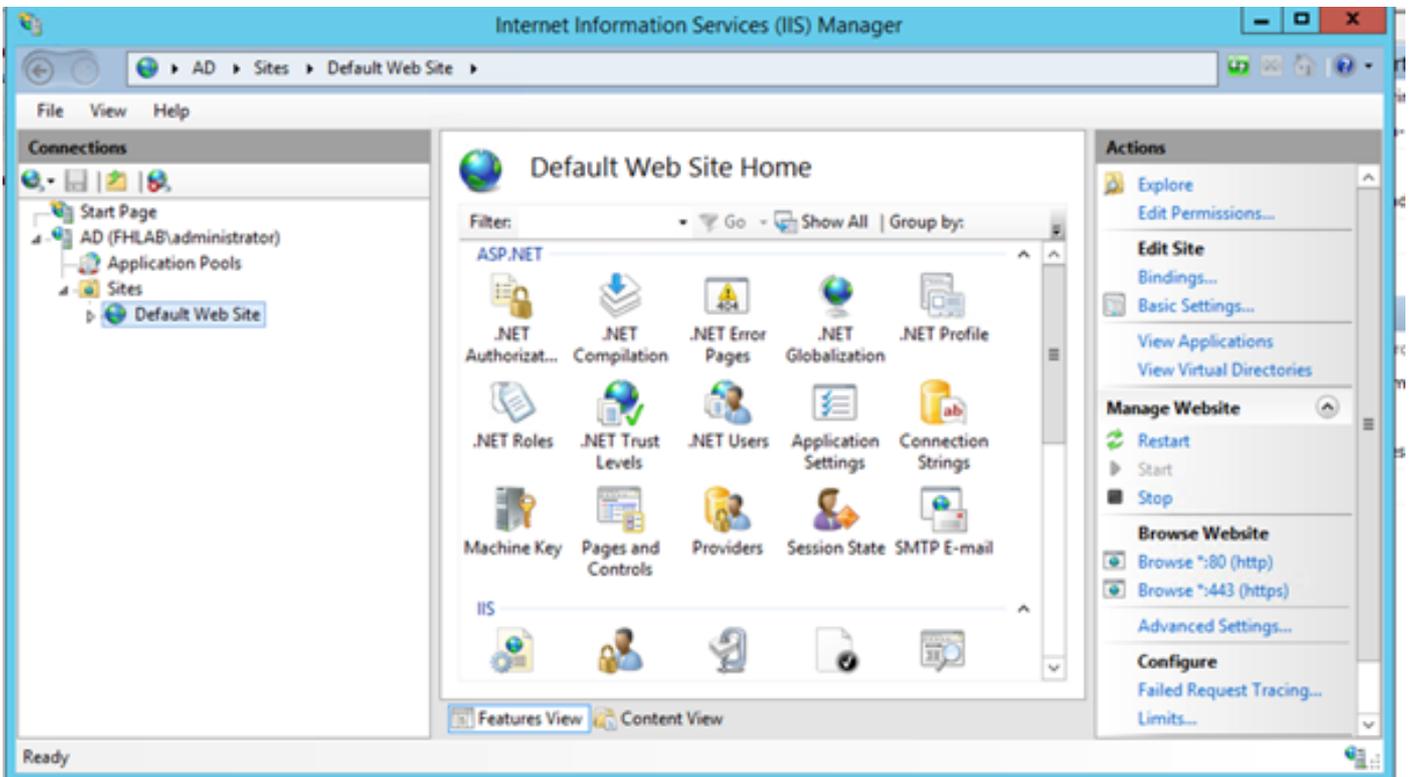


Dieser Schritt ist nur erforderlich, wenn Sie ADFS3 auf einem separaten Windows Server 2012

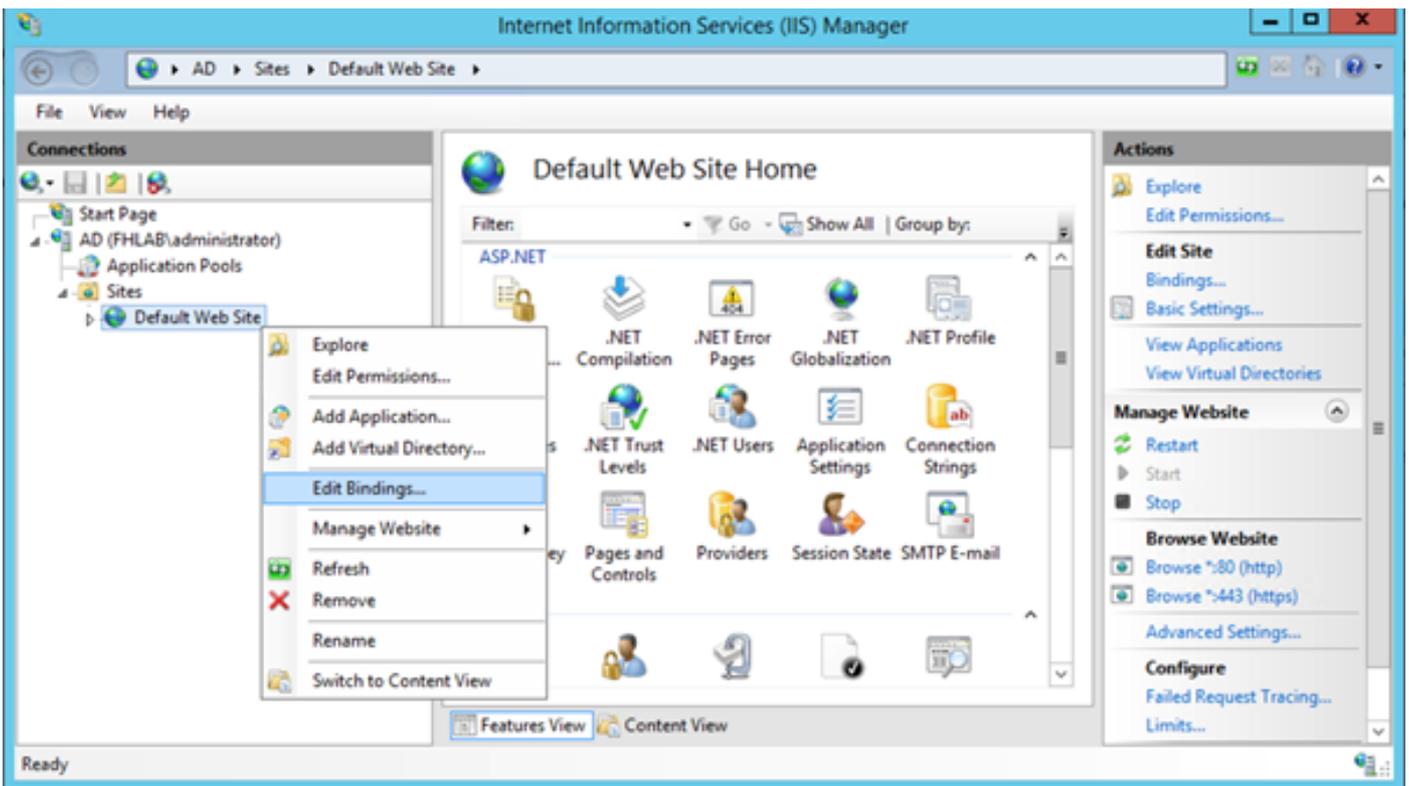
installieren. Nachdem Sie die CA konfiguriert haben, müssen die Rollendienste für IIS konfiguriert werden. Dies ist für die Webregistrierung in der CA erforderlich. Für die meisten ADFS-Bereitstellungen ist eine zusätzliche Rolle in IIS erforderlich, wenn Sie unter Anwendungsentwicklung auf **ASP.NET**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



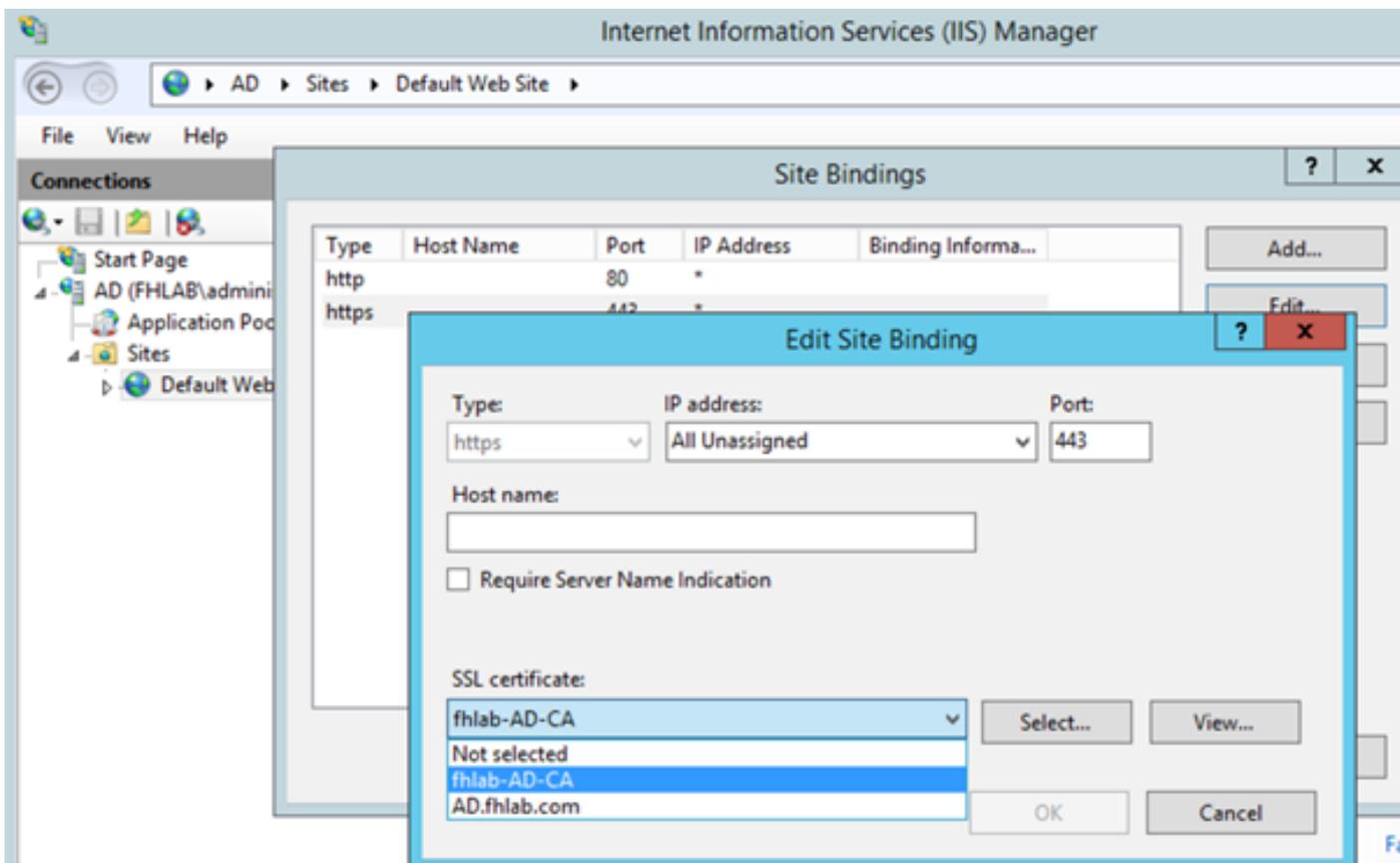
Klicken Sie im Server Manager auf **Webserver > IIS**, und klicken Sie dann mit der rechten Maustaste auf **Standardwebsite**. Die Binding muss geändert werden, um zusätzlich zu HTTP auch HTTPS zuzulassen. Dies geschieht zur Unterstützung von HTTPS.



Wählen Sie **Bindungen bearbeiten** aus.

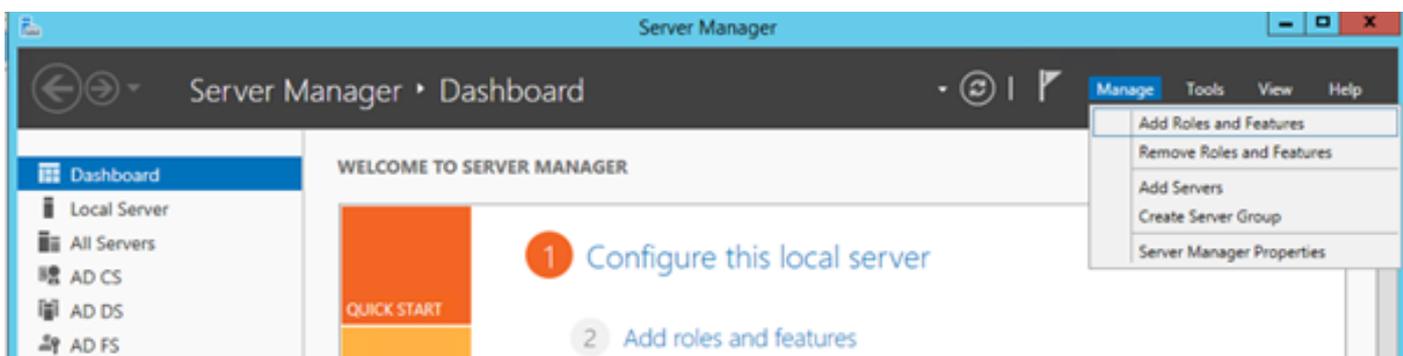


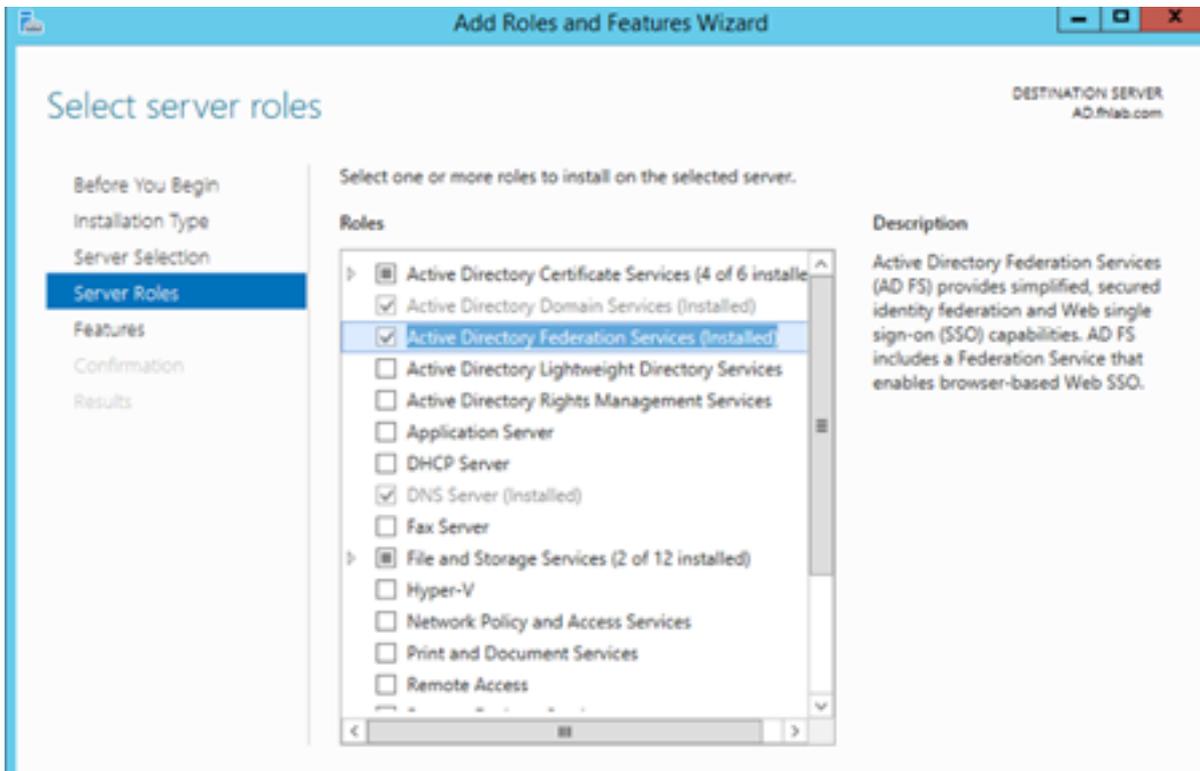
Fügen Sie eine neue Site Binding hinzu, und wählen Sie **HTTPS** als Typ aus. Wählen Sie für das SSL-Zertifikat das Serverzertifikat aus, das den gleichen FQDN wie Ihr AD-Server haben sollte.



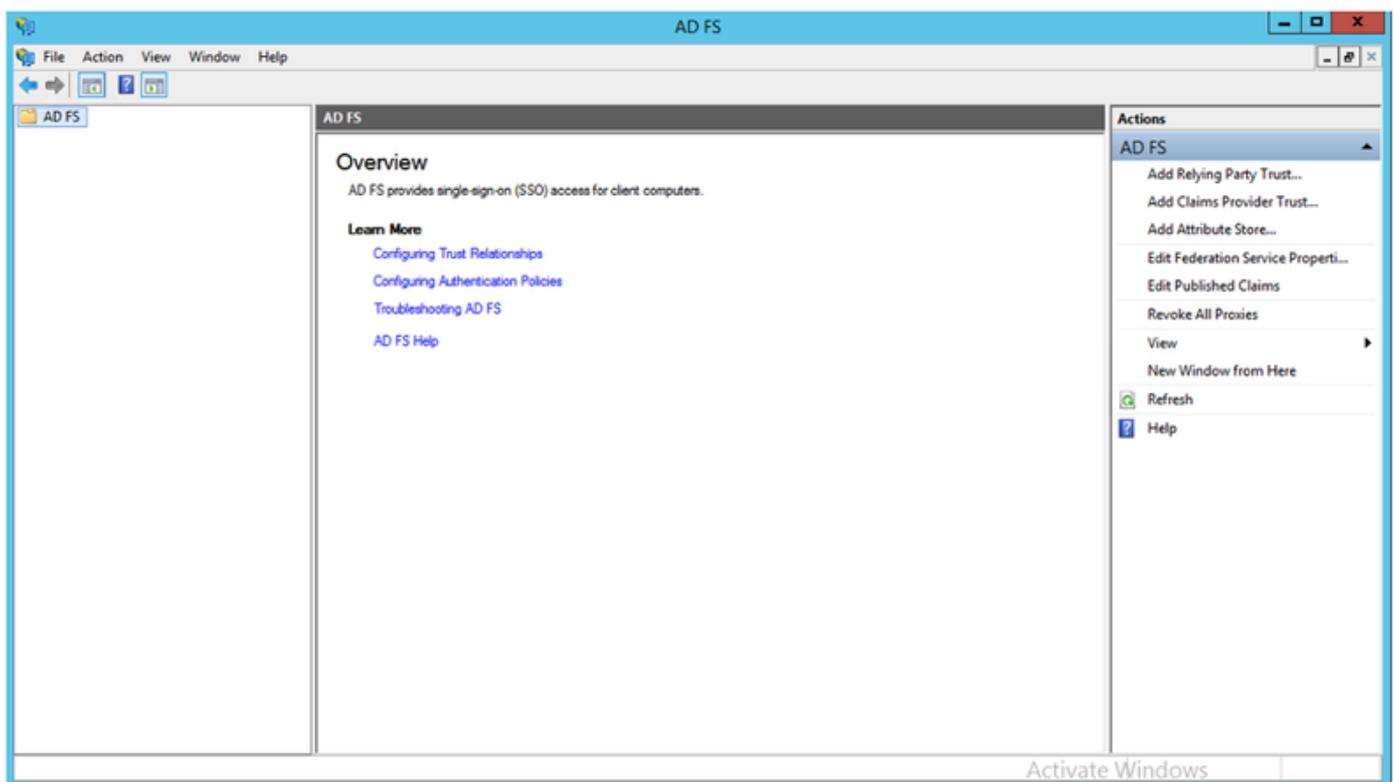
Alle erforderlichen Rollen sind in der Umgebung installiert, sodass Sie jetzt mit der Installation von ADFS3 Active Directory Federation Services (auf Windows Server 2012) fortfahren können.

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.





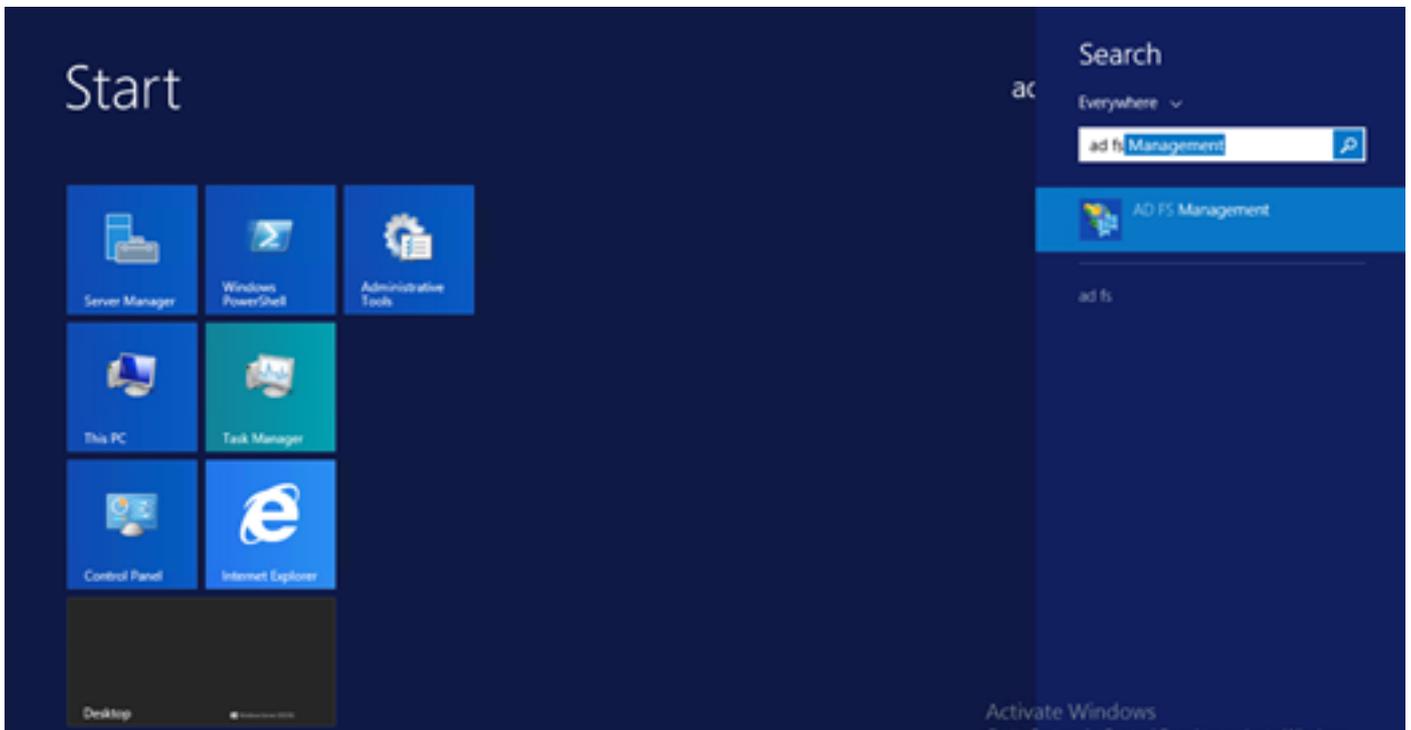
Sobald die Installation abgeschlossen ist, können Sie sie über die Taskleiste oder das Startmenü öffnen.



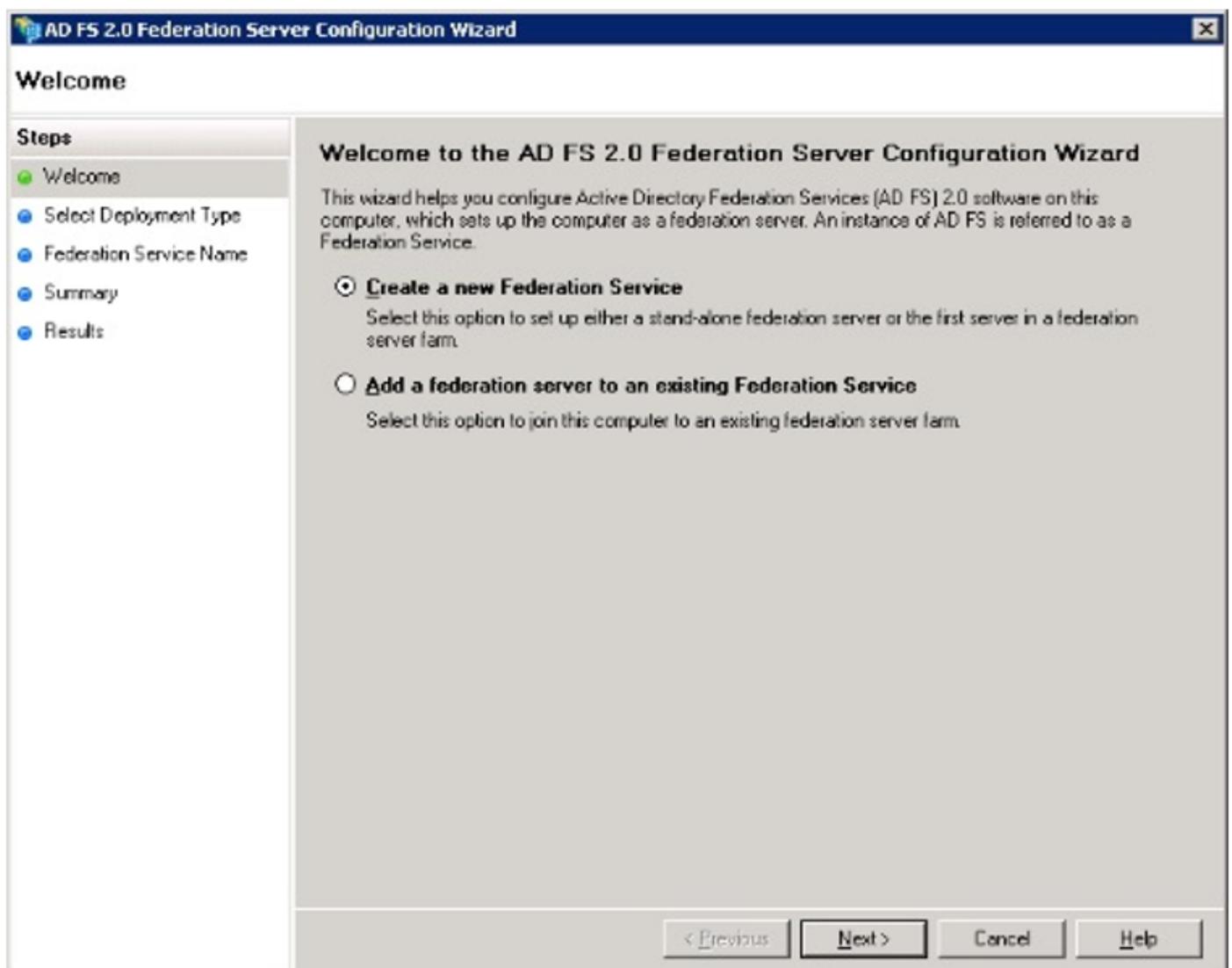
Erstkonfiguration von ADFS3

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

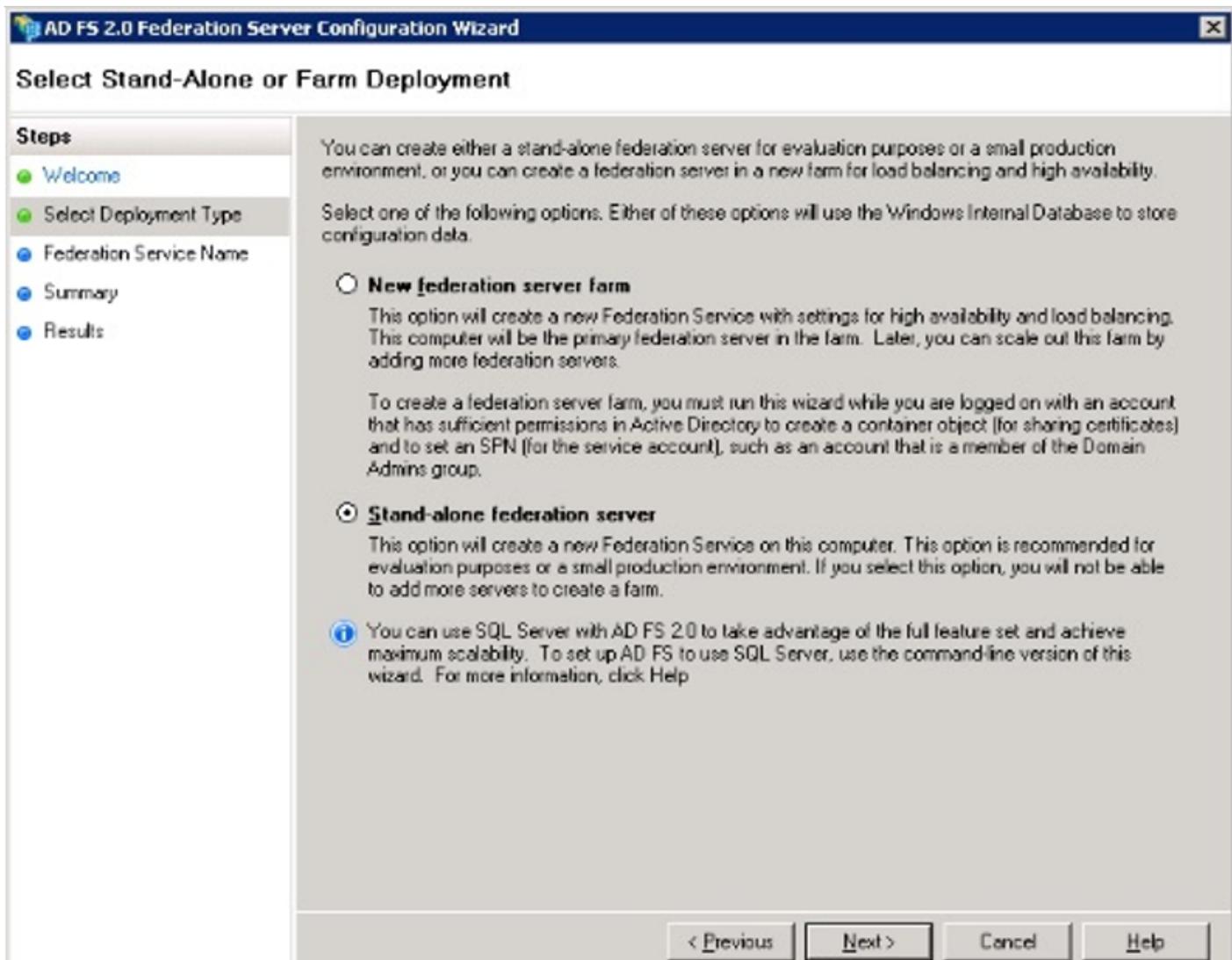
Wählen Sie **Windows** aus, und geben Sie **AD FS Management** ein, um die ADFS Management Console wie im Bild gezeigt zu starten.



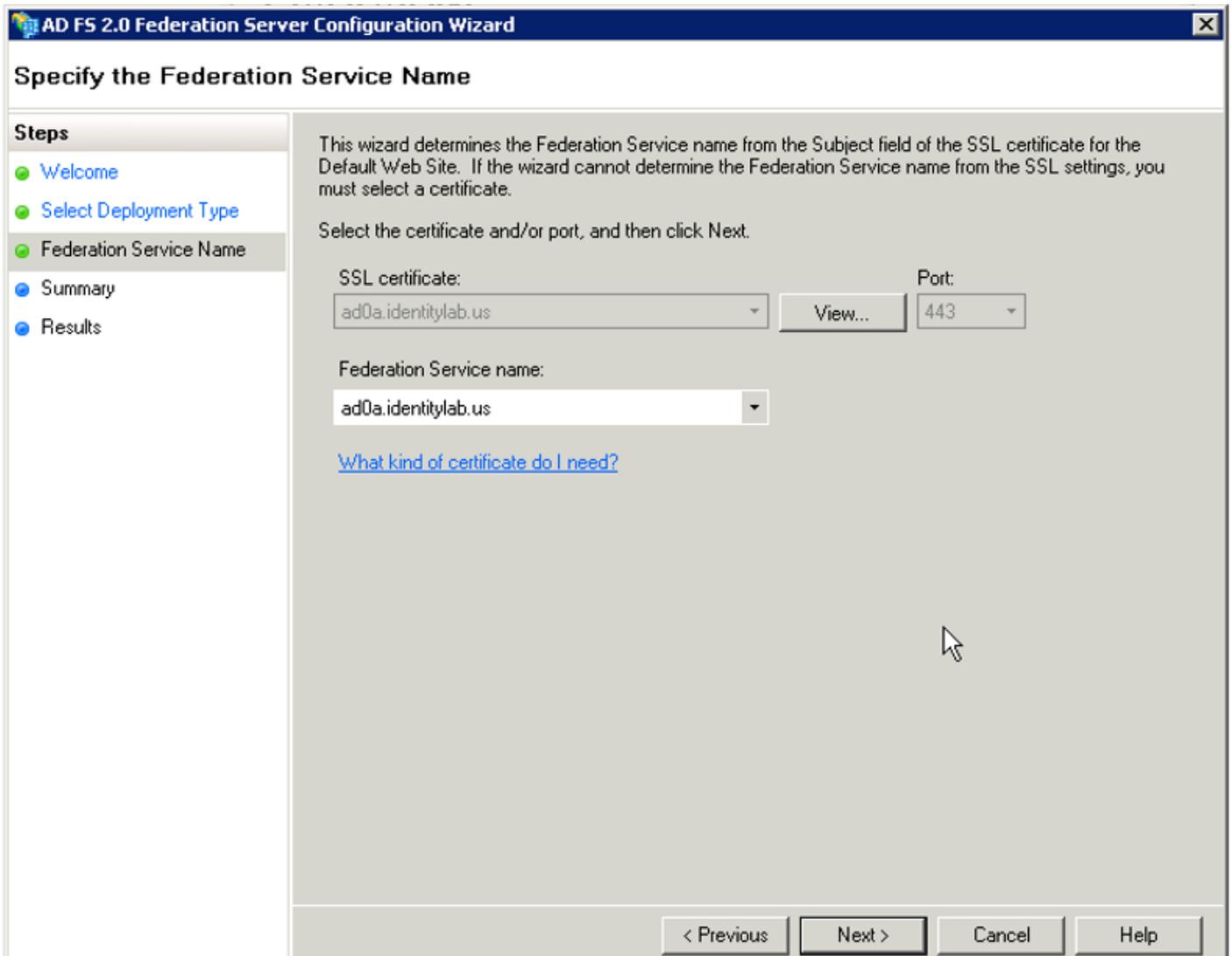
Wählen Sie die Option **AD FS 3.0 Federation Server Configuration Wizard** (Assistent zum Konfigurieren von AD FS-Servern) aus, um die ADFS-Serverkonfiguration zu starten. Diese Screenshots stellen die gleichen Schritte in AD FS 3 dar.



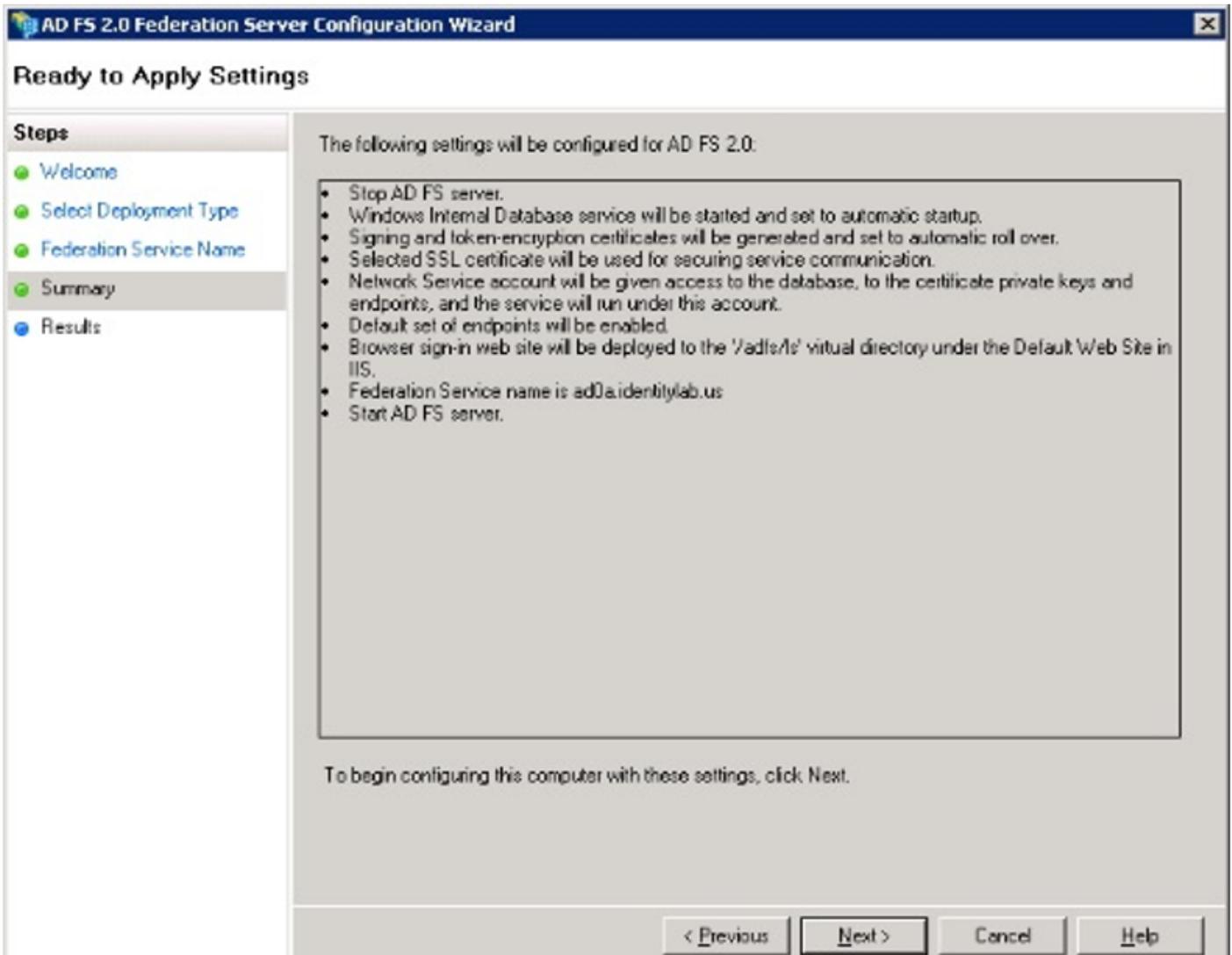
Wählen Sie **Neuen Föderationsdienst erstellen** aus, und klicken Sie auf **Weiter**.



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



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



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

AD FS 2.0 Federation Server Configuration Wizard

Configuration Results

Steps

- Welcome
- Select Deployment Type
- Federation Service Name
- Summary
- Results**

The following settings are being configured

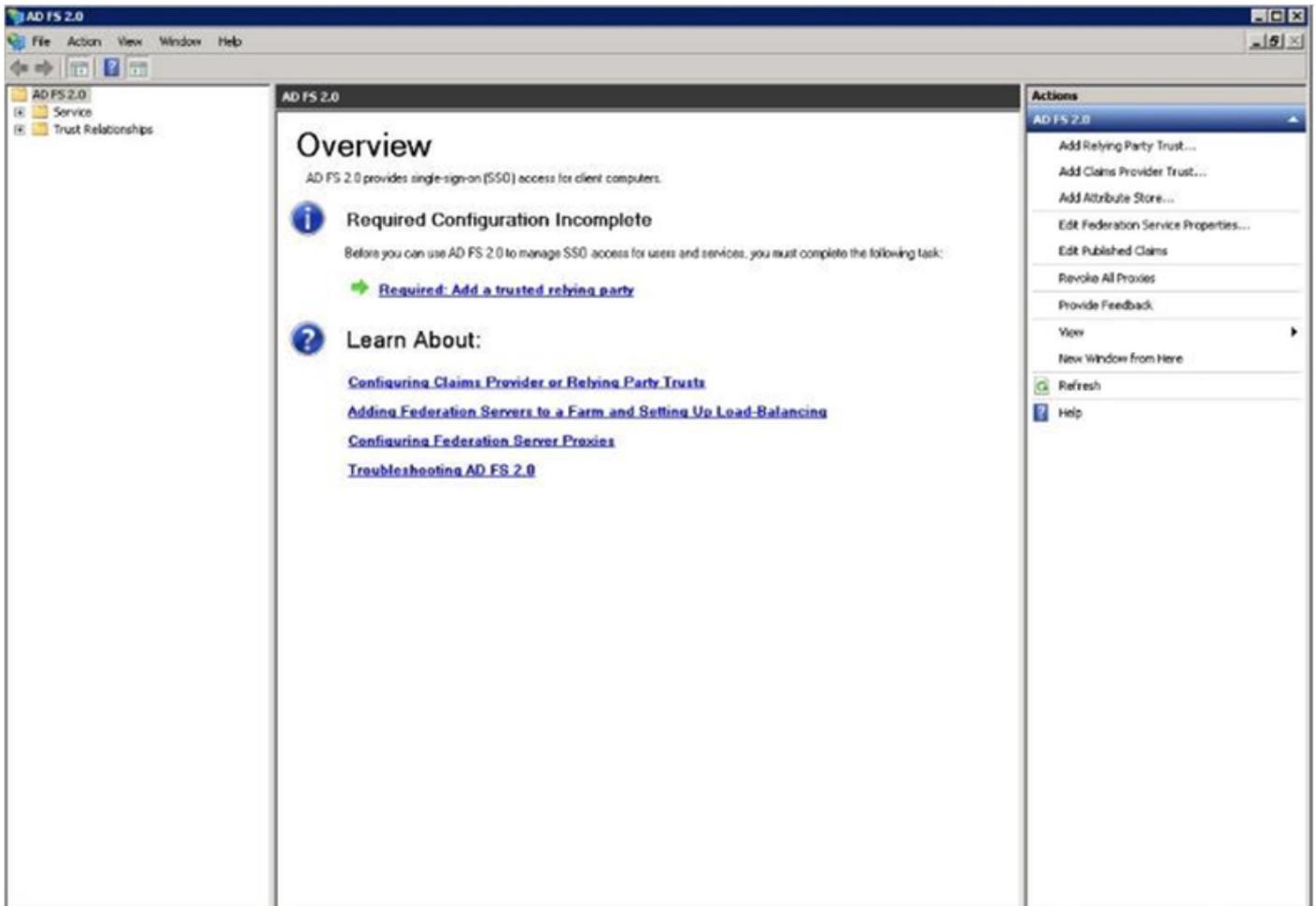
| Component | Status |
|--|------------------------|
| Stop the AD FS 2.0 Windows Service | Configuration finished |
| Install Windows Internal Database | Configuration finished |
| Start the Windows Internal Database service | Configuration finished |
| Create AD FS configuration database | Configuration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

You have successfully completed the AD FS 2.0 Federation Server Configuration Wizard.

To close this wizard, click Close.

Close

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



Please Delete All LDAP Directories Before Making Changes on This Page



Please Disable LDAP Authentication Before Making Changes on This Page

LDAP System Information

Enable Synchronizing from LDAP Server

LDAP Server Type

Microsoft Active Directory



LDAP Attribute for User ID

sAMAccountName



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

LDAP Directory



Save



Delete



Copy



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*



Users Only



Users and Groups

LDAP Custom Filter for Groups

< None >



LDAP Directory Synchronization Schedule

Perform Sync Just Once



Perform a Re-sync Every*

7

DAY



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 | |
| 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 Address for Server*
LDAP Port*
Use TLS

[Add Another Redundant LDAP Server](#)

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

The screenshot shows the Cisco Unified CM Administration web interface. The page title is "Cisco Unified CM Administration" and the navigation bar includes "Navigation Cisco Unified CM Administration" and "Go". The main menu includes "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The current page is "LDAP Authentication".

LDAP Authentication

Status

i Status: Ready

LDAP Authentication for End Users

Use LDAP Authentication for End Users

LDAP Manager Distinguished Name*

LDAP Password*

Confirm Password*

LDAP User Search Base*

LDAP Server Information

Host Name or IP Address for Server*
LDAP Port*
Use TLS

[Add Another Redundant LDAP Server](#)

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 User Configuration Related Links: [Back to Find List Users](#)

Confirm MLPP Password
 MLPP Precedence Authorization Level

CAPF Information

Associated CAPF Profiles [View Details](#)

Permissions Information

Groups:

- Standard CCM End Users
- Standard CCM Super Users**
- Standard CTI Allow Control of All Devices
- Standard CTI Enabled

[View Details](#)

Roles:

- Standard AXL API Access
- Standard Admin Rep Tool Admin
- Standard CCM Admin Users
- Standard CCM End Users
- Standard CCMADMIN Administration

[View Details](#)

Conference Now Information

Enable End User to Host Conference Now
 Meeting Number
 Attendees Access Code

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.

System > Call Routing > Media Resources > ... > Device > User Manager > ... > Administration

SAML Single Sign-On

SSO Mode

Cluster wide (One metadata file per cluster. Requires multi-server Tomcat certificate)
 Per node (One metadata file per node)

Status

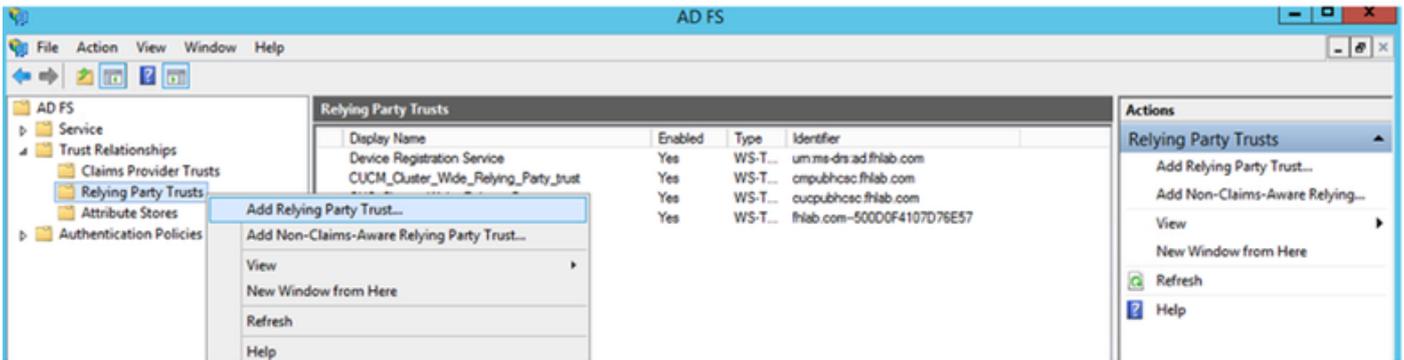
- RTMT is enabled for SSO. You can change SSO for RTMT [here](#).
- SAML SSO enabled

| Server Name | SSO Status | Re-Import Metadata | Last Metadata Import | Export Metadata | Last Metadata Export | SSO Test |
|----------------------|------------|--------------------|-------------------------------|-----------------|-------------------------------|---|
| cmpubhcsc.fhlab.com | SAML | N/A | April 20, 2020 2:00:57 PM PDT | File | April 18, 2020 8:05:38 PM PDT | Passed - April 20, 2020 2:02:15 PM PDT <input type="button" value="Run SSO Test..."/> |
| cmsubhcsc.fhlab.com | SAML | IdP | April 20, 2020 2:00:57 PM PDT | File | April 18, 2020 8:05:37 PM PDT | Passed - April 20, 2020 1:49:45 PM PDT <input type="button" value="Run SSO Test..."/> |
| imppubhcsc.fhlab.com | SAML | IdP | April 20, 2020 2:00:57 PM PDT | File | April 18, 2020 8:05:37 PM PDT | Passed - May 24, 2020 12:02:56 PM PDT <input type="button" value="Run SSO Test..."/> |
| impsubhcsc.fhlab.com | SAML | IdP | April 20, 2020 2:00:57 PM PDT | File | April 18, 2020 8:05:37 PM PDT | Passed - May 24, 2020 12:03:26 PM PDT <input type="button" value="Run SSO Test..."/> |

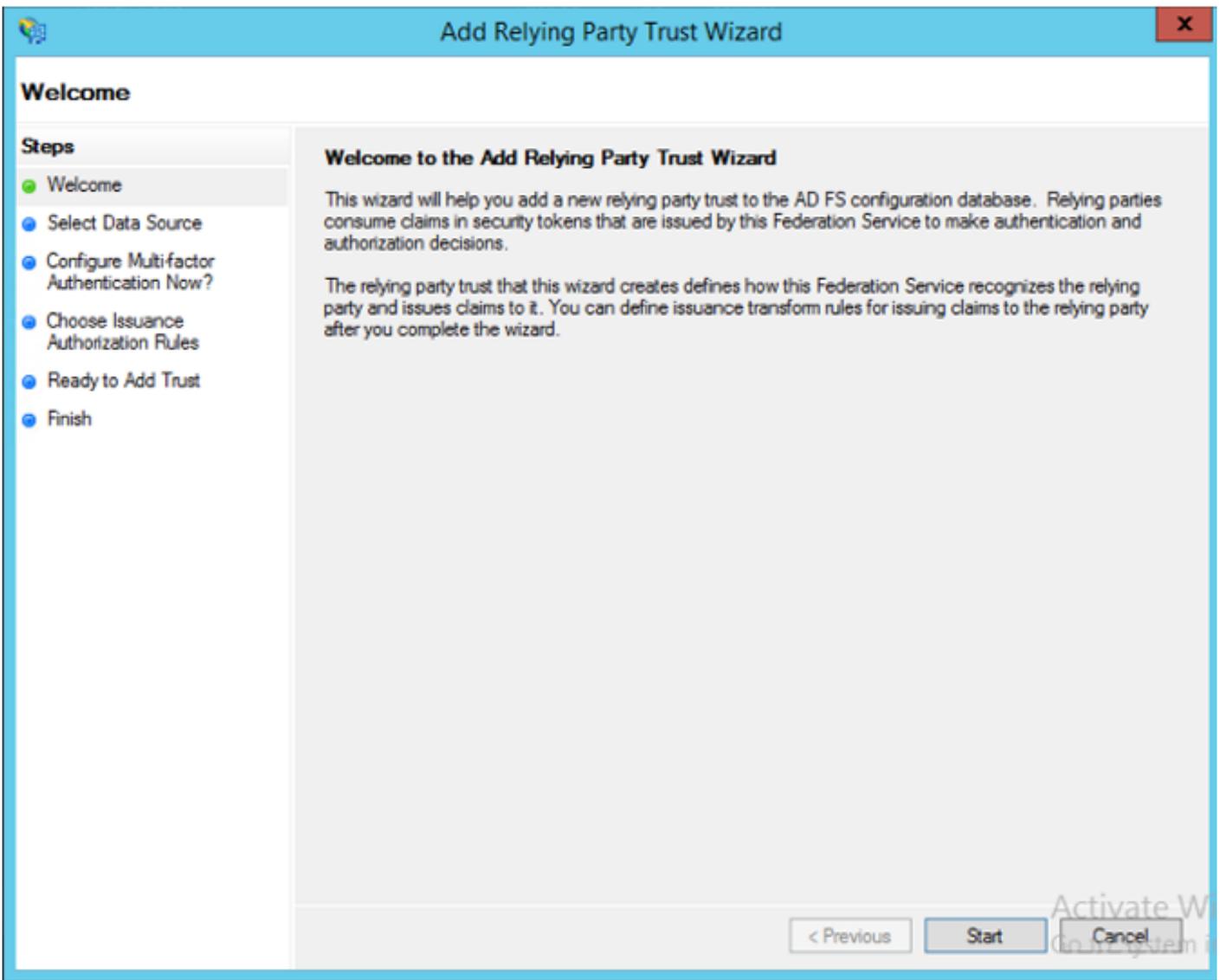
Speichern Sie die Daten lokal mit einem aussagekräftigen Namen wie sp_cucm0a.xml, danach benötigen Sie sie.

Konfigurieren der ADFS-Relationship-Partei

Kehren Sie zur Verwaltungskonsole AD FS 3.0 zurück.

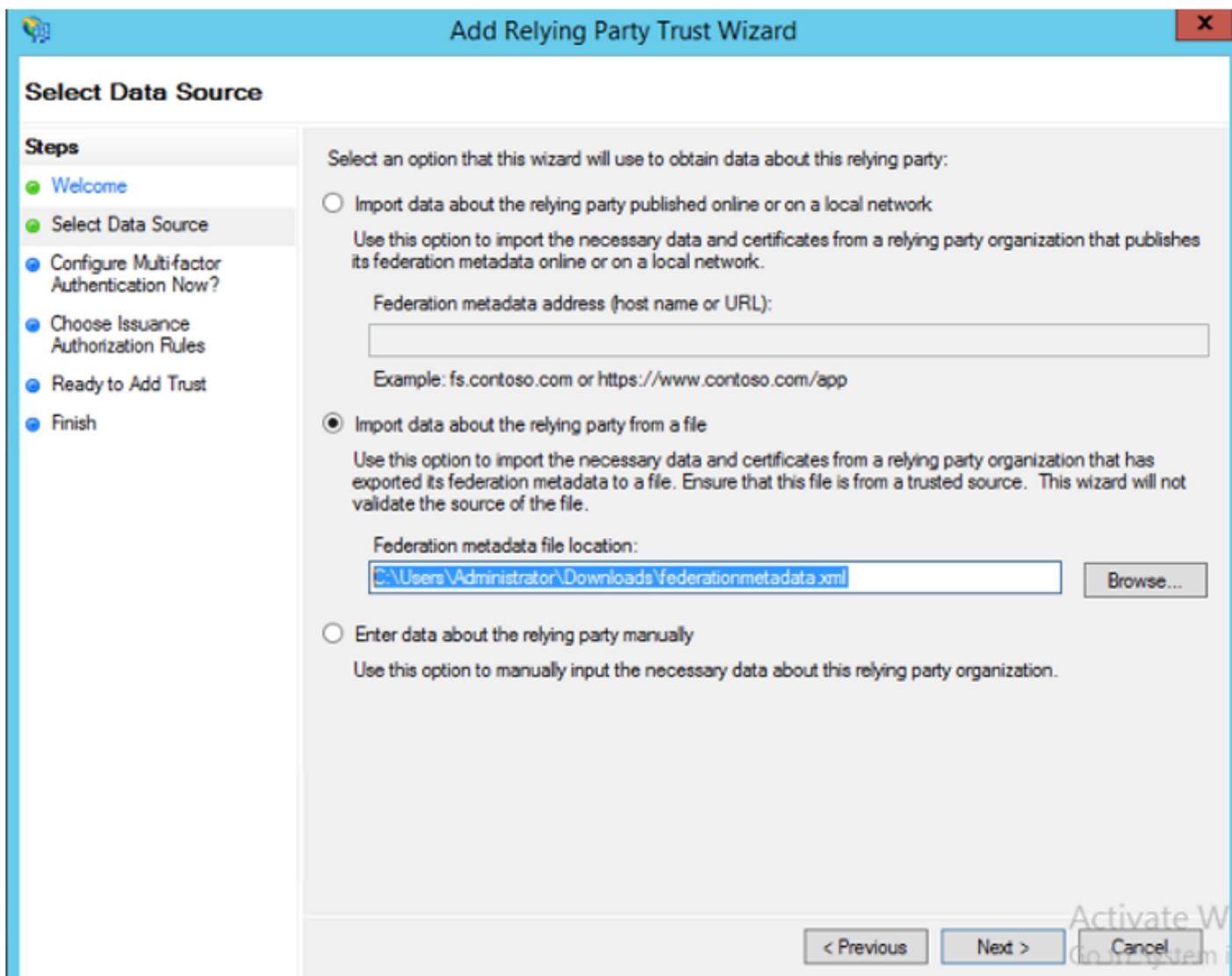


Klicken Sie auf **Assistent** zum Hinzufügen von Vertrauenswürdigkeit.



Klicken Sie auf **Start**, um fortzufahren.

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



Verwenden Sie CUCM_Cluster_Wide_Relying_Party_trust als Anzeigenamen, und klicken Sie auf Weiter.

Add Relying Party Trust Wizard

Specify Display Name

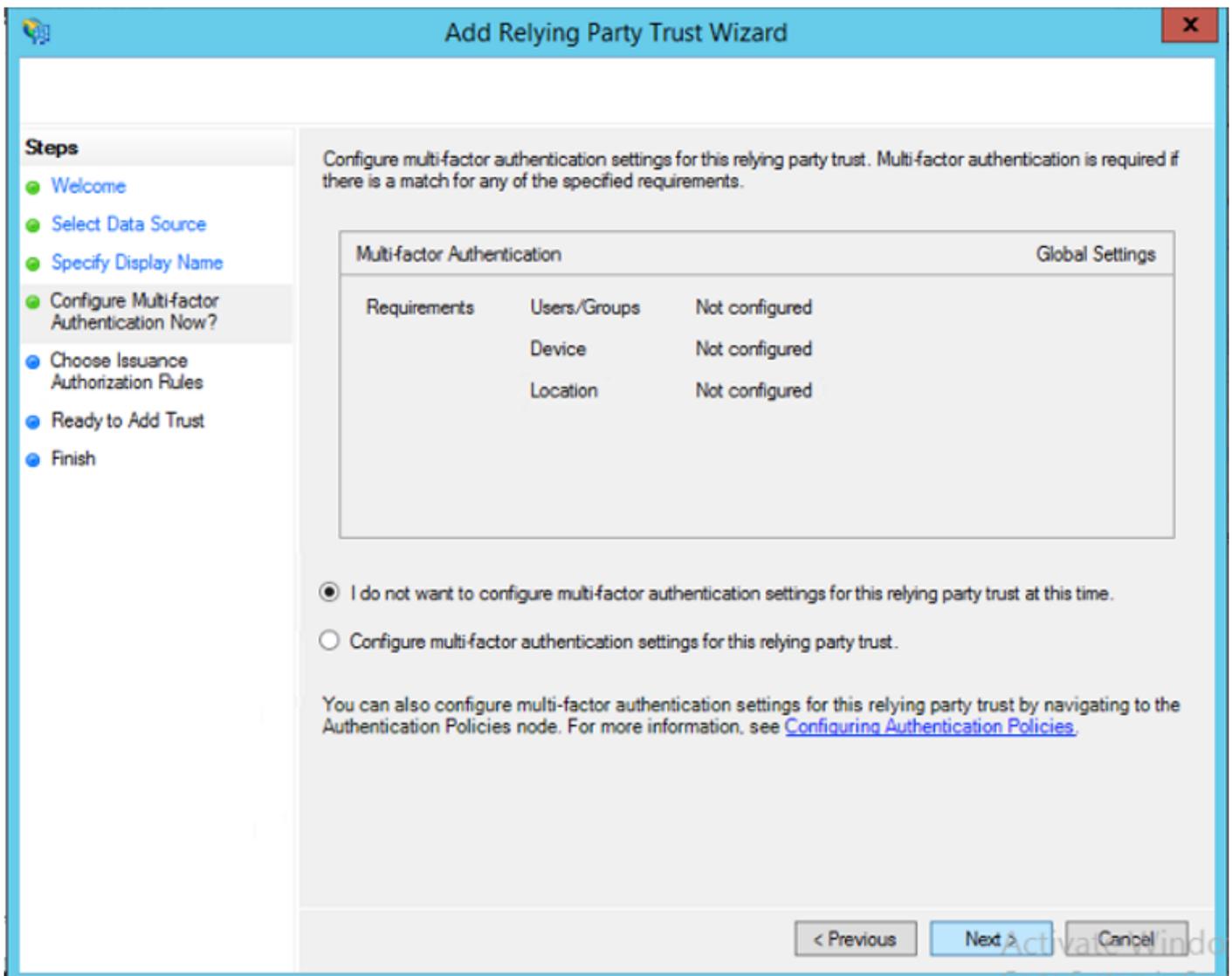
Enter the display name and any optional notes for this relying party.

Display name:

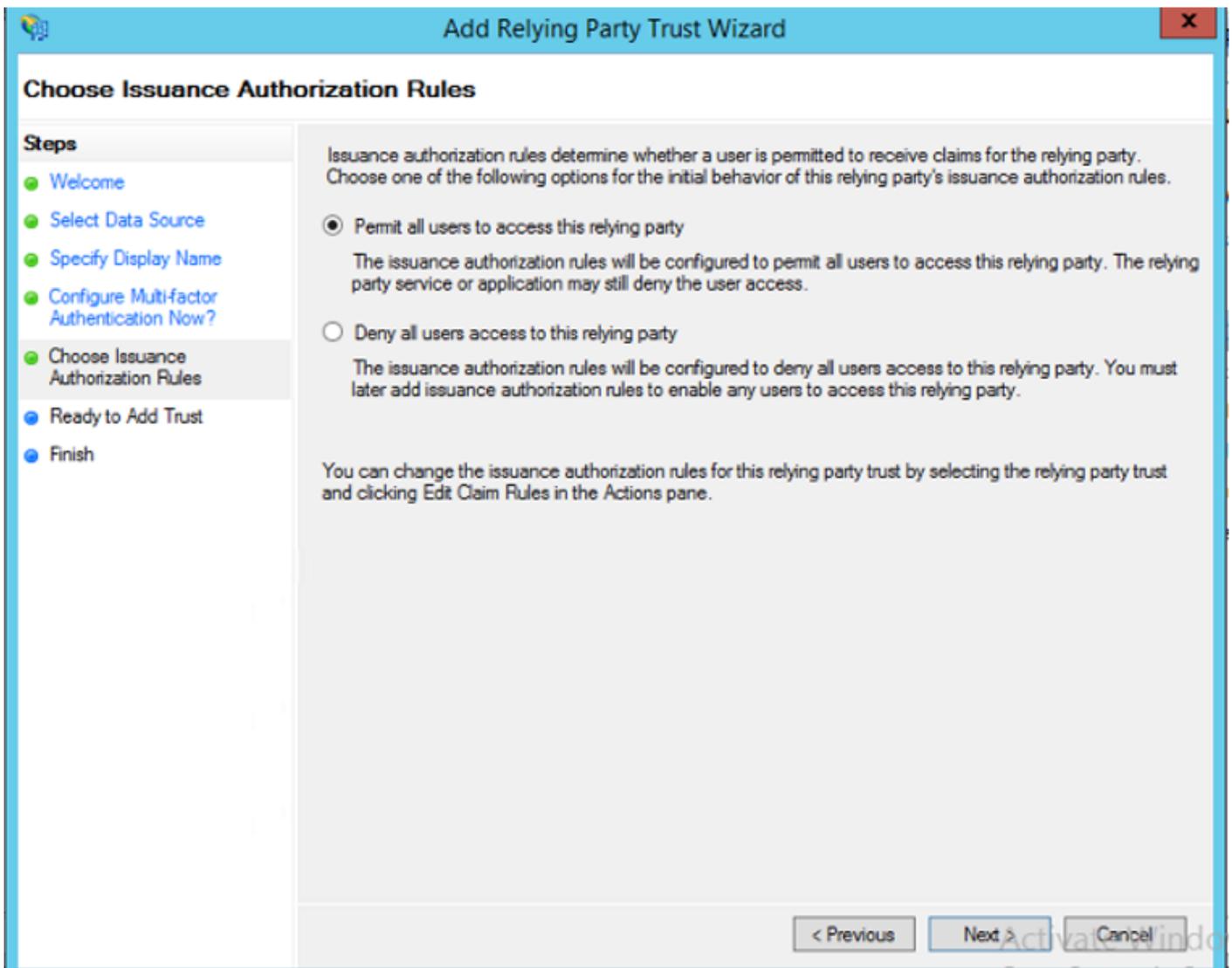
Notes:

< Previous Next > Cancel

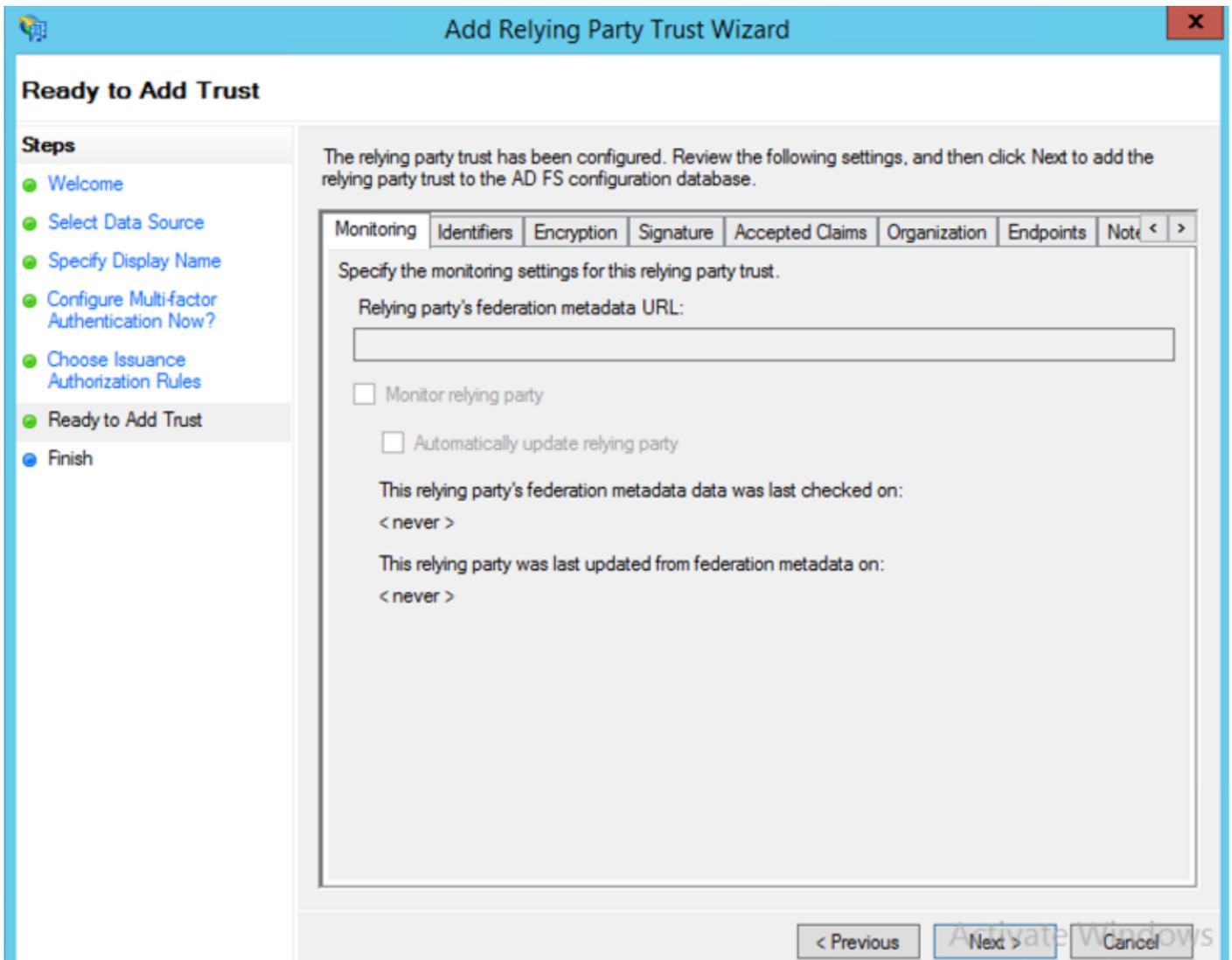
Wählen Sie die erste Option aus, und klicken Sie auf **Weiter**.



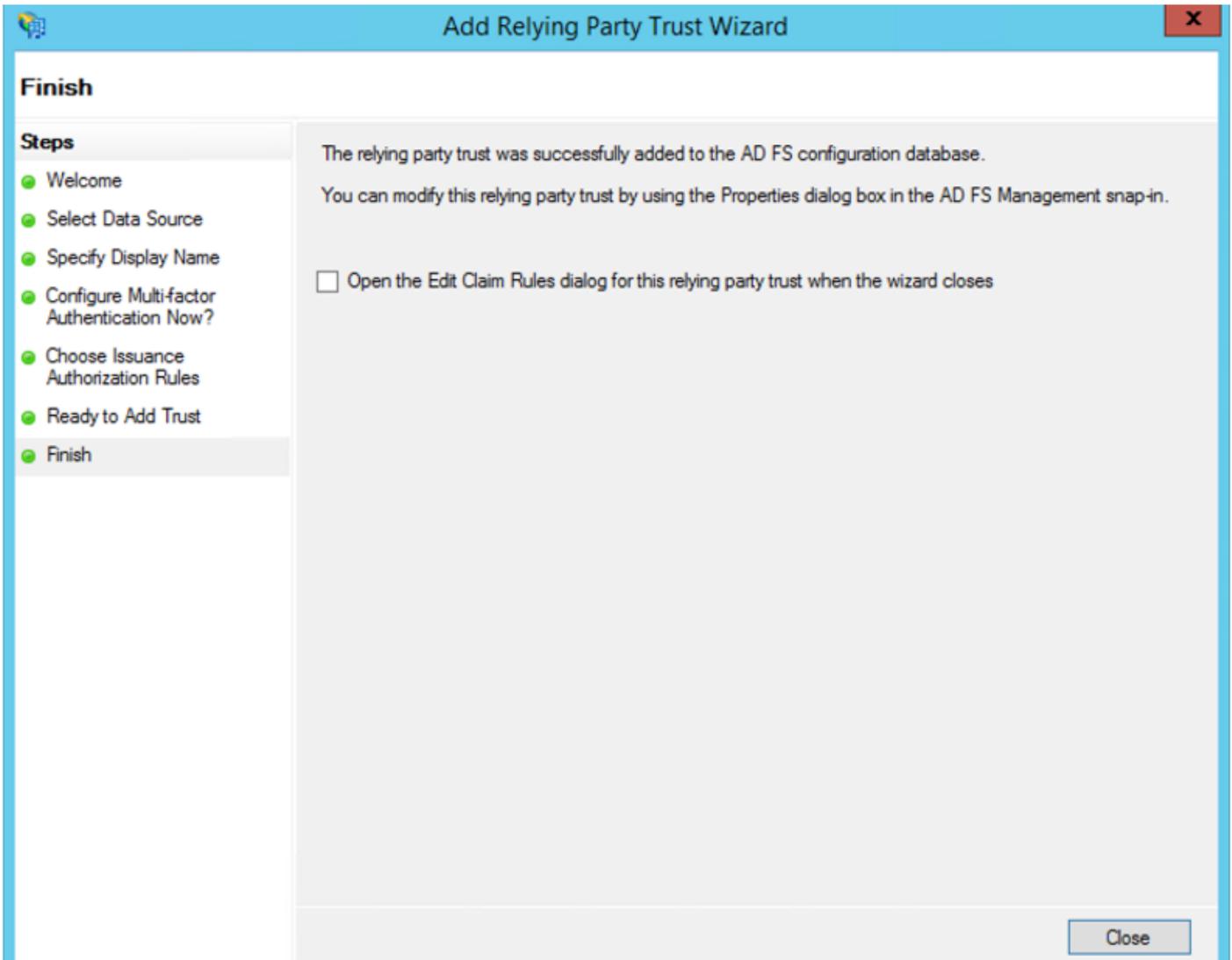
Wählen Sie **Zulassen aller Benutzer für den Zugriff auf diese vertrauliche Partei aus**, und klicken Sie auf **Weiter**, wie im Bild gezeigt.



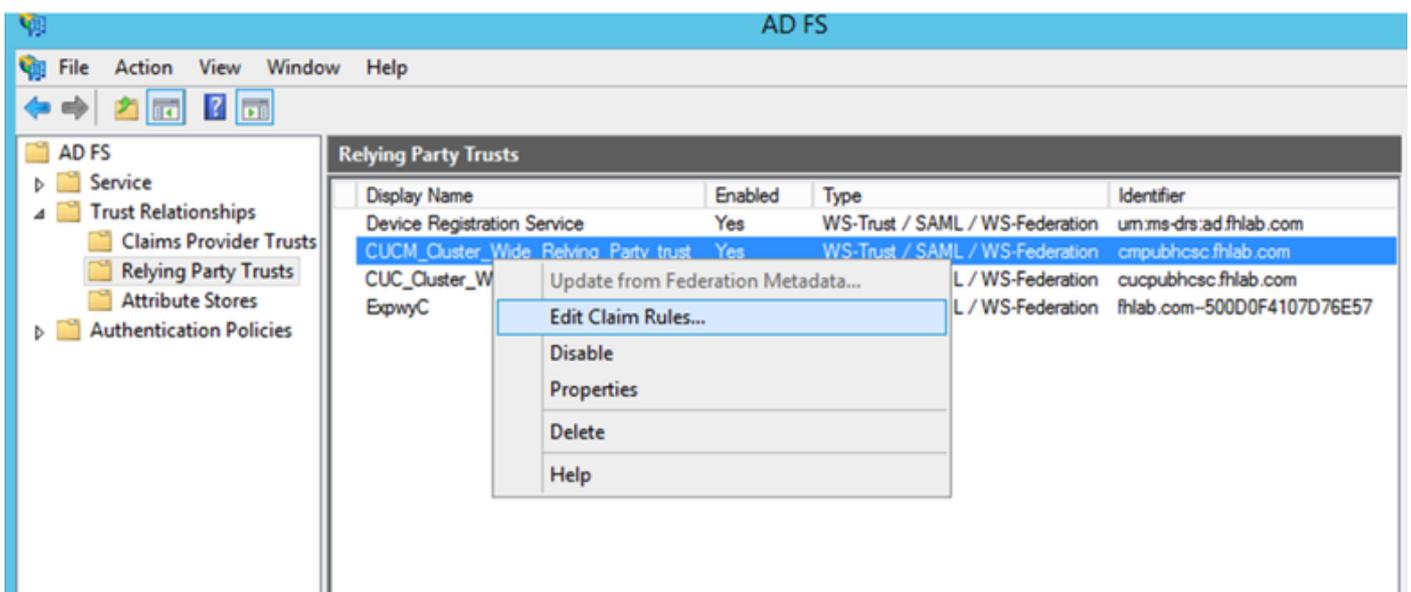
Überprüfen Sie die Konfiguration, und klicken Sie auf **Weiter**, wie im Bild gezeigt.



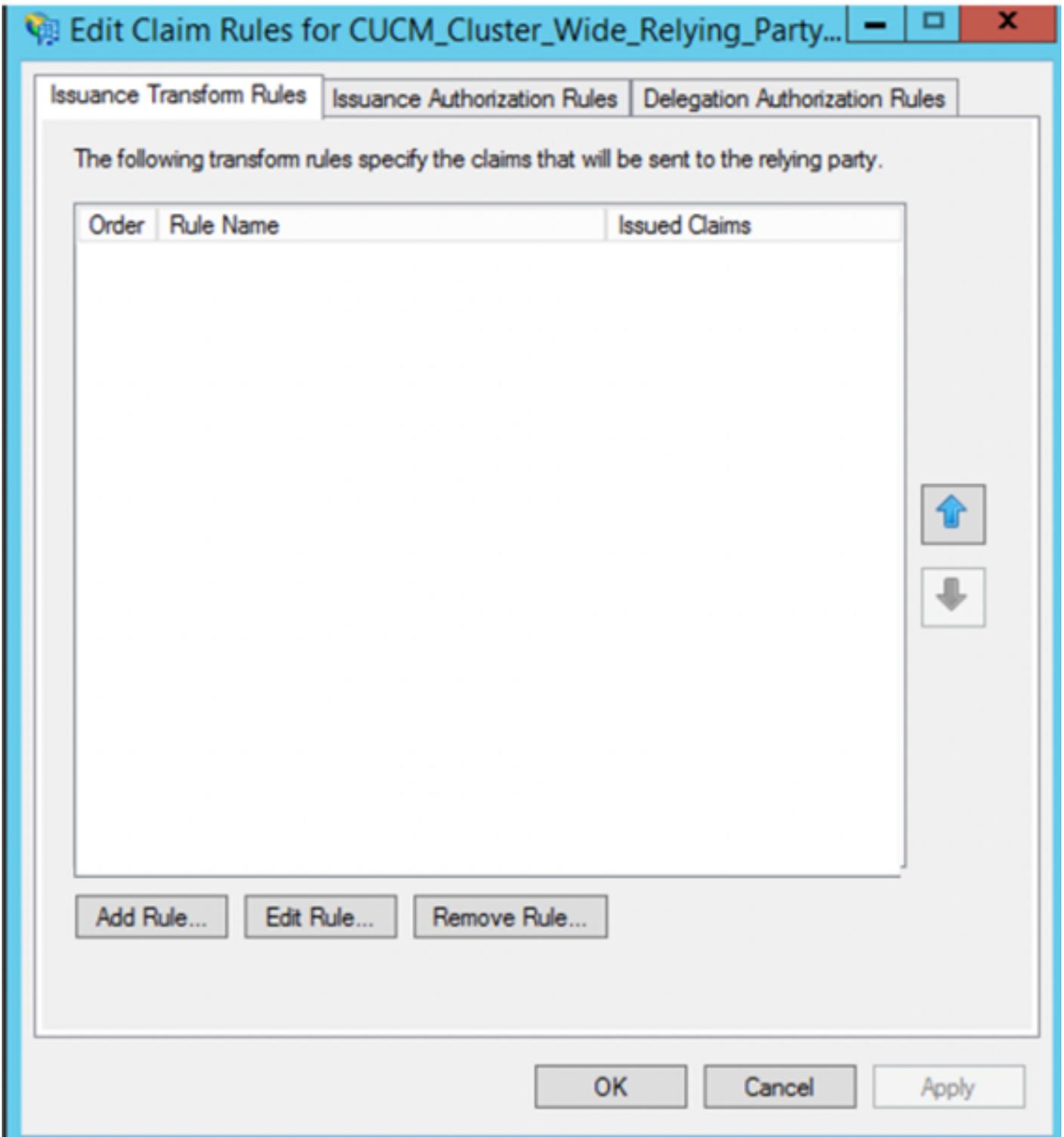
Deaktivieren Sie das Kontrollkästchen, und klicken Sie auf **Schließen**.



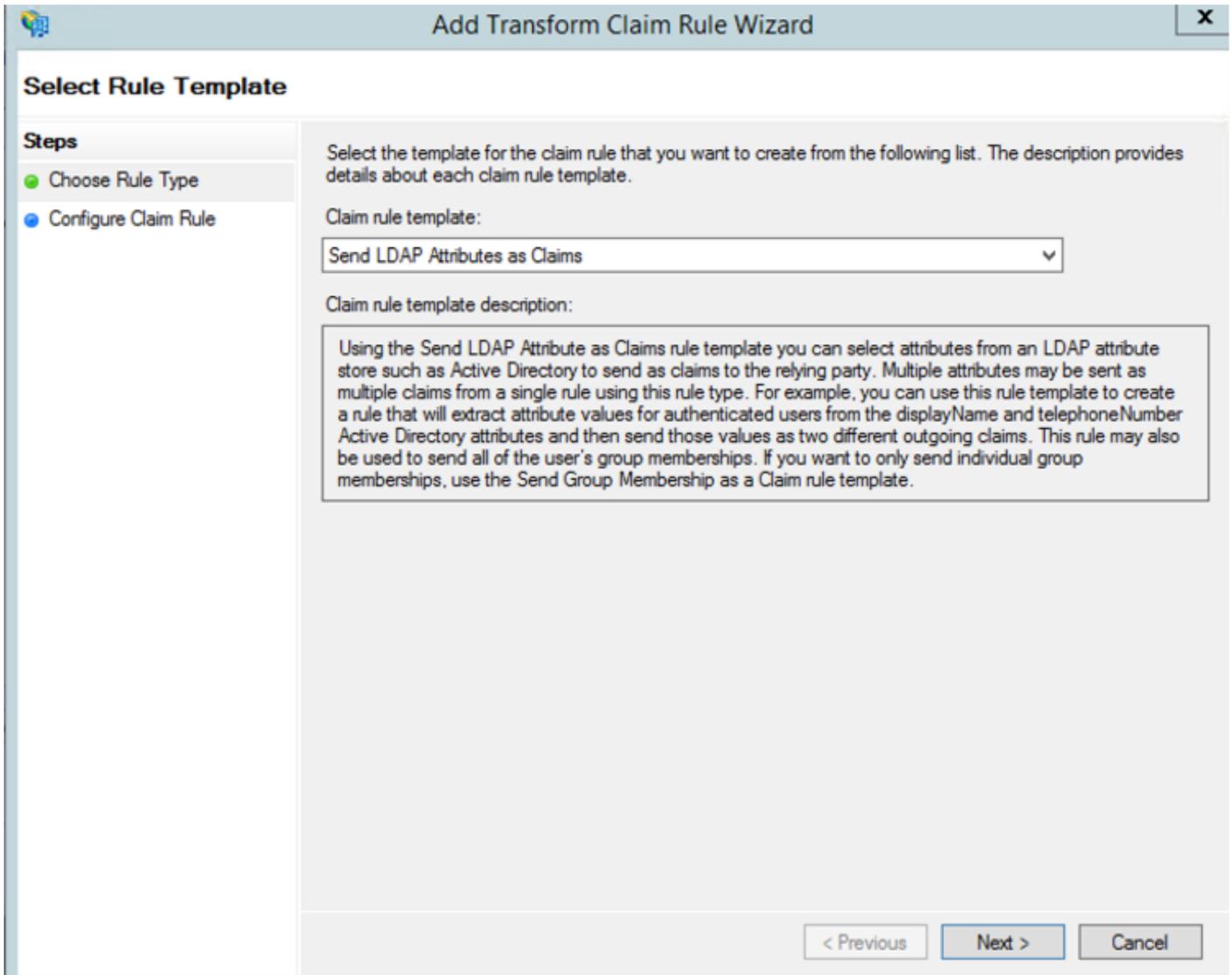
Wählen Sie mit der zweiten Maustaste die **Relying Party Trust** aus, die Sie gerade erstellt haben, und **bearbeiten Sie** die Konfiguration der Anspruchsregeln, wie im Bild gezeigt.



Klicken Sie auf **Regel hinzufügen** wie im Bild gezeigt.



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



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.

Edit Rule - NameID

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 rule name:

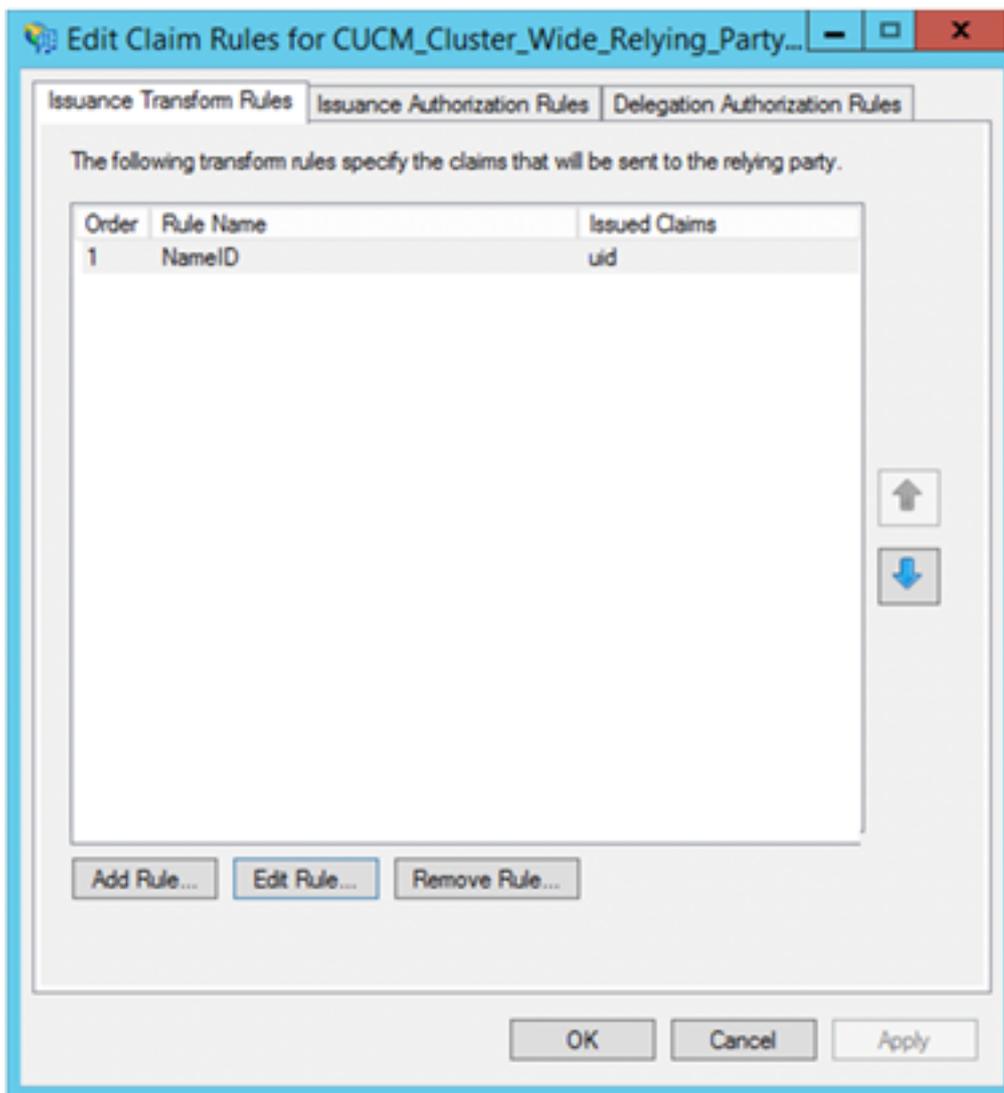
Rule template: Send LDAP Attributes as Claims

Attribute store:

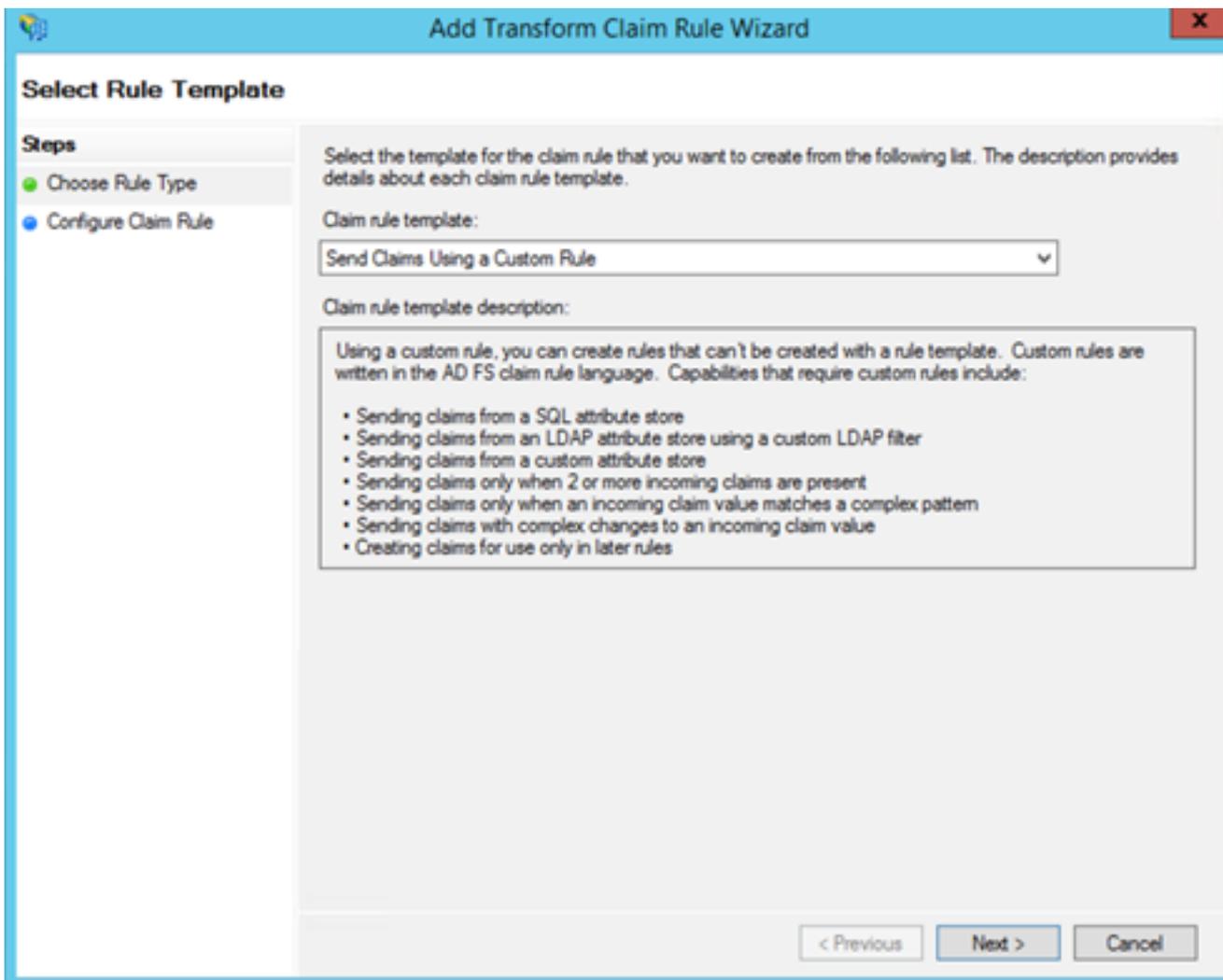
Mapping of LDAP attributes to outgoing claim types:

| | LDAP Attribute (Select or type to add more) | Outgoing Claim Type (Select or type to add more) |
|---|---|--|
| ▶ | SAM-Account-Name | uid |
| * | | |

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



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



Erstellen Sie eine benutzerdefinierte Regel mit dem Namen Cluster_Side_Claim_Rule.

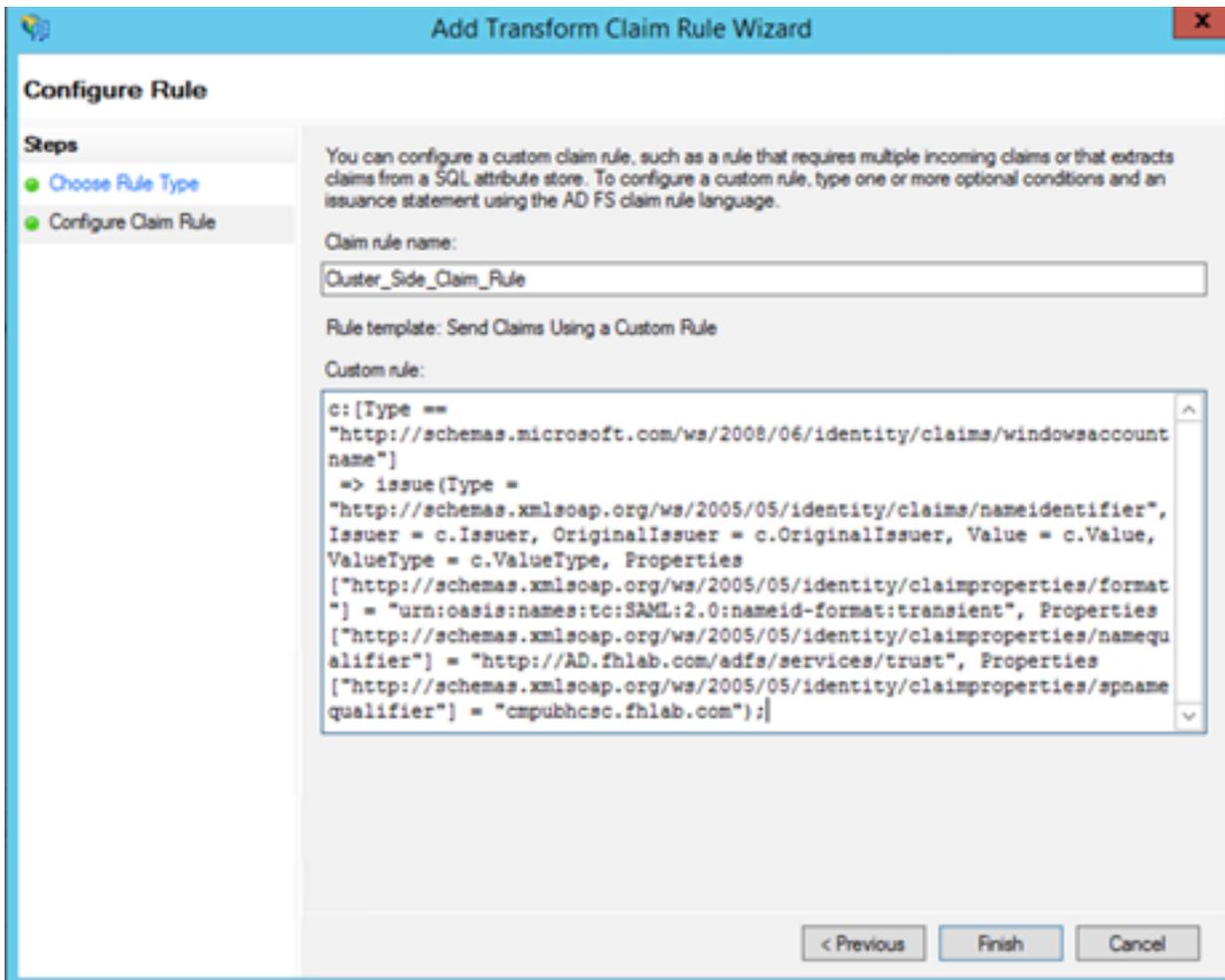
Kopieren Sie diesen Text und fügen Sie ihn hier direkt in das Regelfenster ein. In manchen Fällen werden Kostenvoranschläge geändert, wenn sie in einem Texteditor bearbeitet werden. Dies führt dazu, dass die Regel beim Testen der SSO-Funktion fehlschlägt:

```
c:[Type ==
```

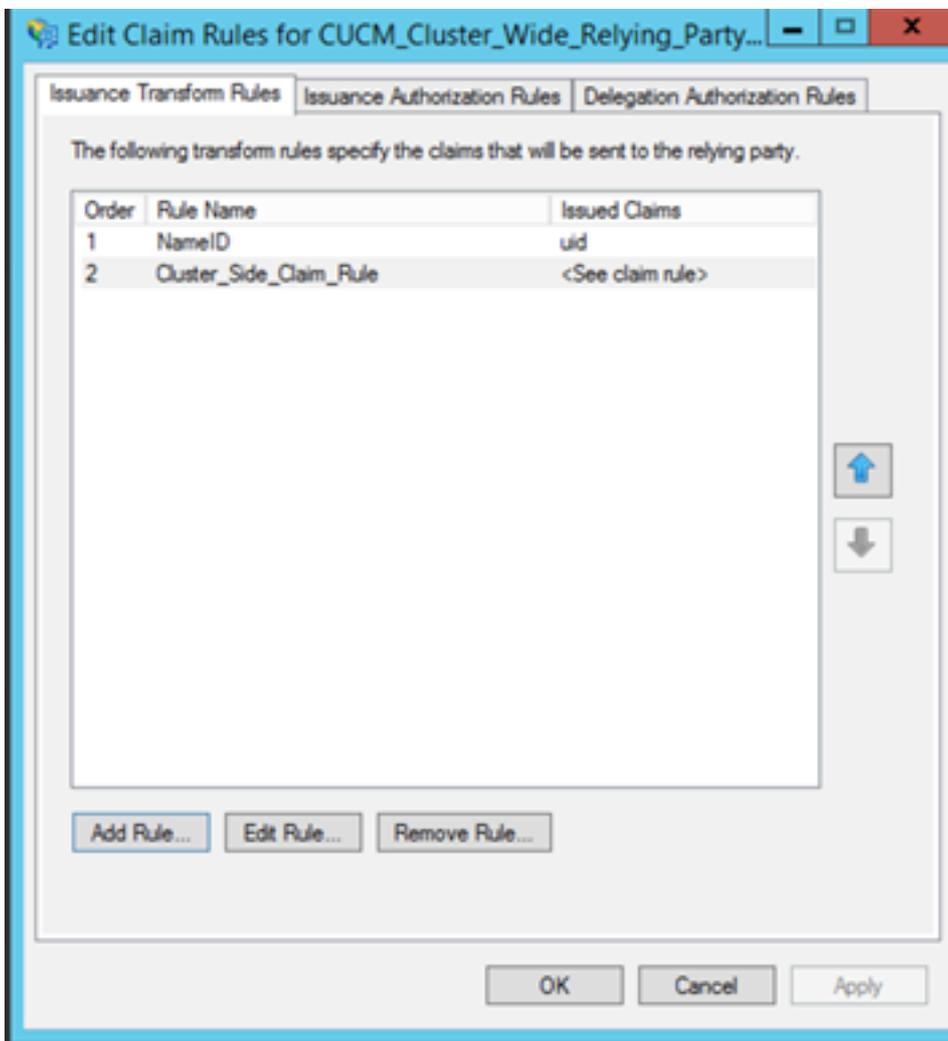
```
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]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

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

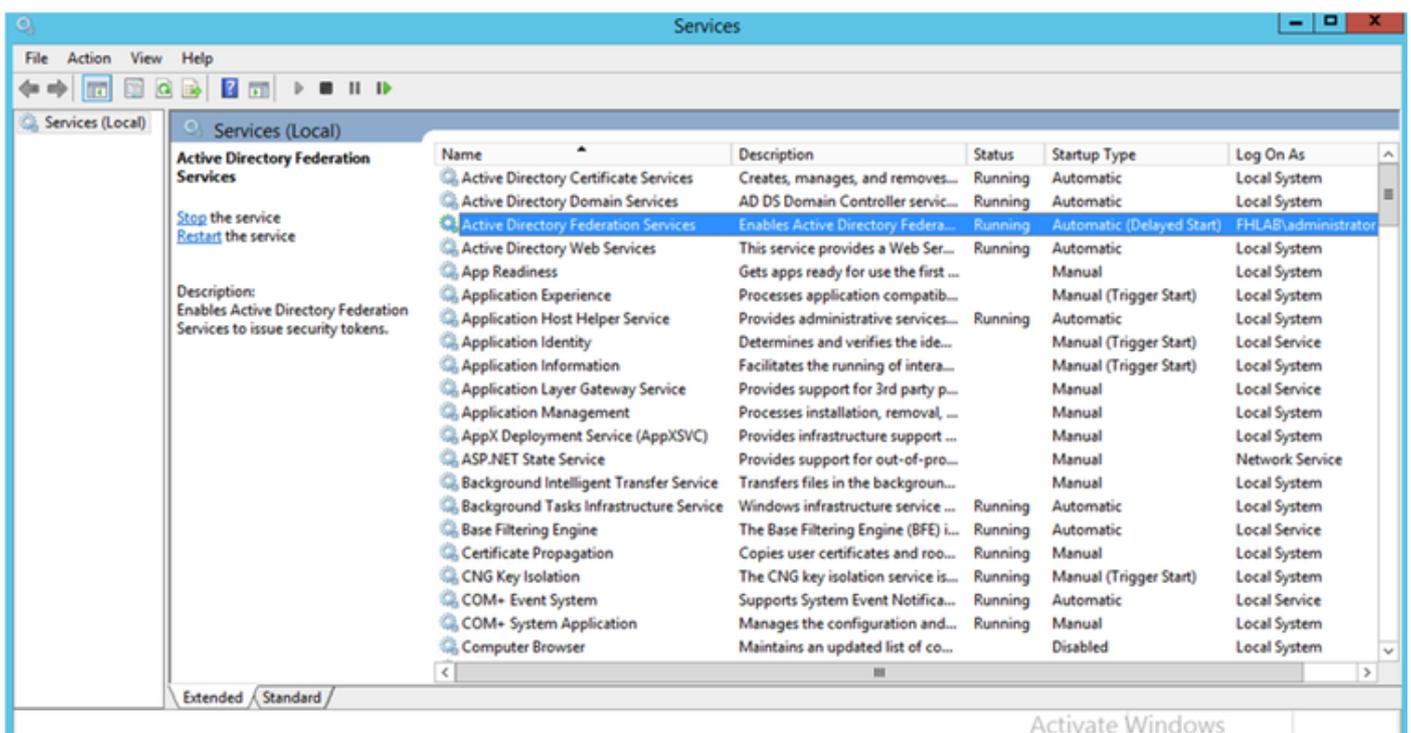
Klicken Sie auf **Fertig stellen**, um fortzufahren.



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



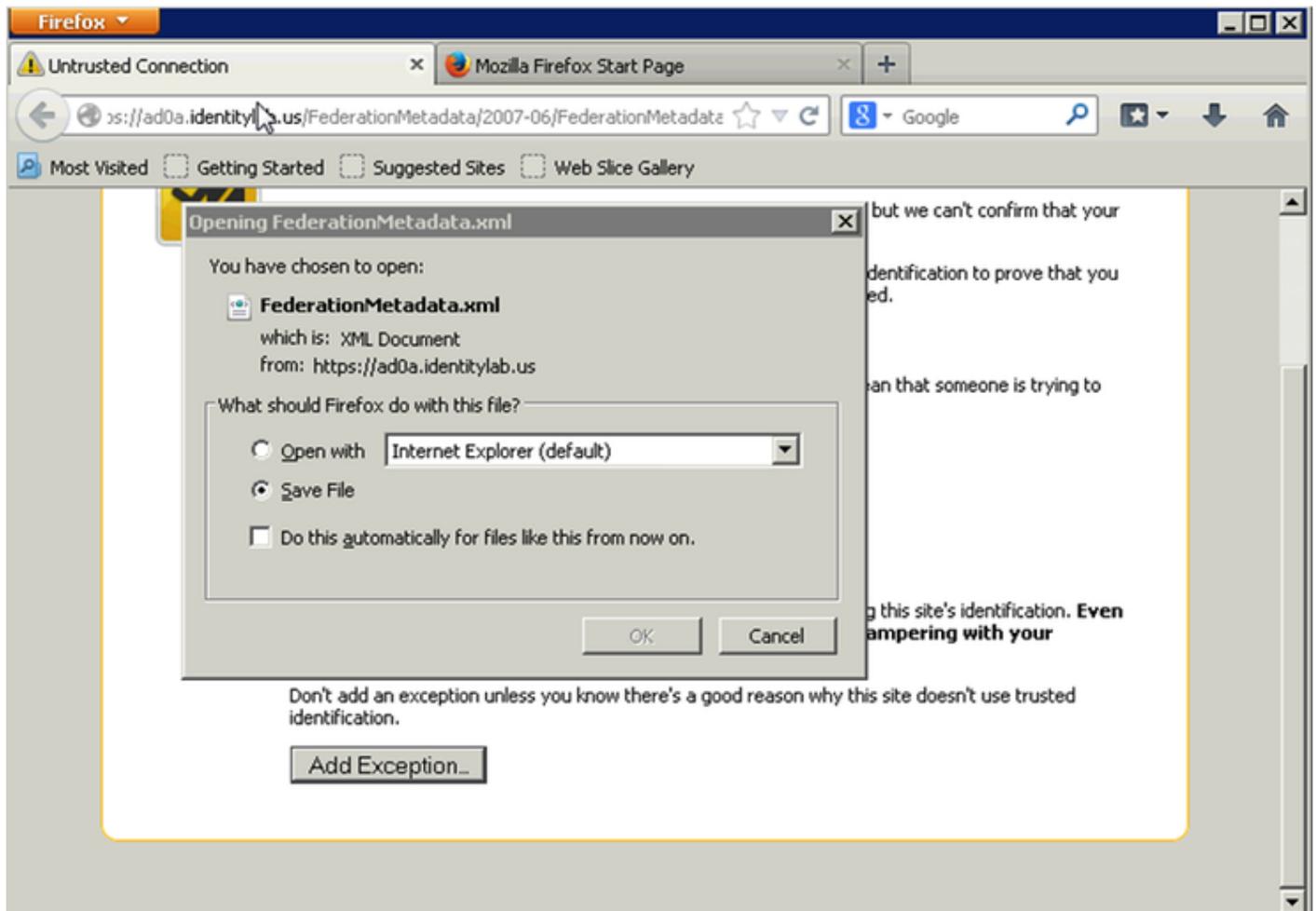
CUCM wird nun erfolgreich als vertrauenswürdiger vertrauender Partei zu ADFS hinzugefügt.



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

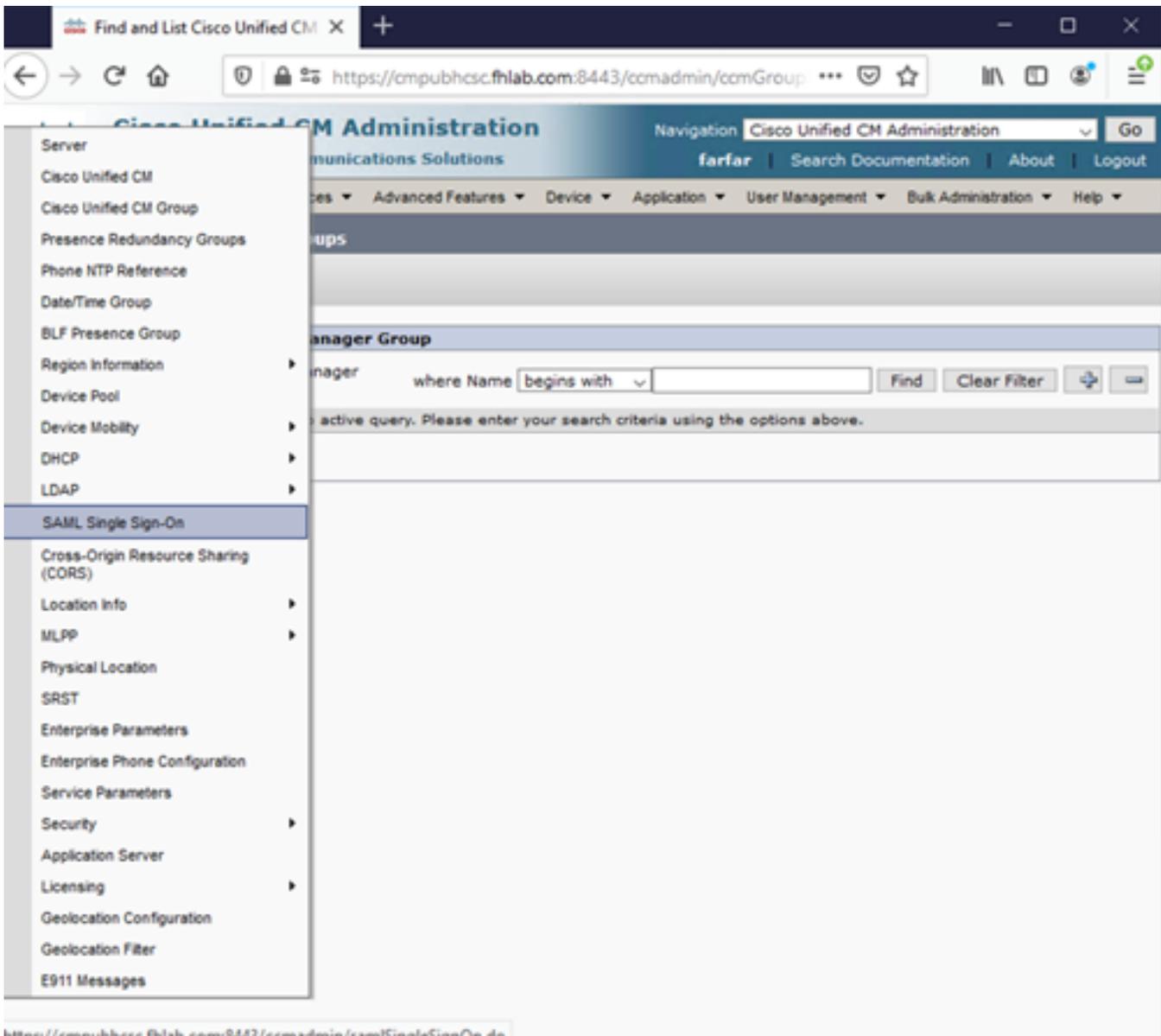
IDP-Metadaten

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.



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://cnpubhsc.fhlab.com:8443/ccadmin/samlSingleSignOn.do>

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

Firefox

Find and List Users | SAML Single Sign-On | Find and List LDAP Directories

https://cucm0a/ccmadmin/samlSingleSignOn.do

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go

admin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

SAML Single Sign-On

Enable SAML SSO | Update IdP Metadata File | Export All Metadata | Fix All Disabled Servers

Status

SAML SSO disabled

SAML Single Sign-On (1 - 1 of 1) Rows per Page: 50

| Server Name | SSO Status | Re-Import Metadata | Last Metadata Import | Export Metadata | Last Metadata Export | SSO Test |
|-------------|------------|--------------------|----------------------|-----------------|----------------------|----------|
| cucm0a | Disabled | N/A | Never | File | Never | Never |

Run Test...

Wählen Sie **SAML-SSO aktivieren** aus.

Klicken Sie auf **Weiter**, um die Warnung zu bestätigen.

Reset Warning - Mozilla Firefox

https://cucm0a/ccmadmin/genericDialogWindow.do?windowTitleKey=genericDialogWindow.windowTitle.ssoenable

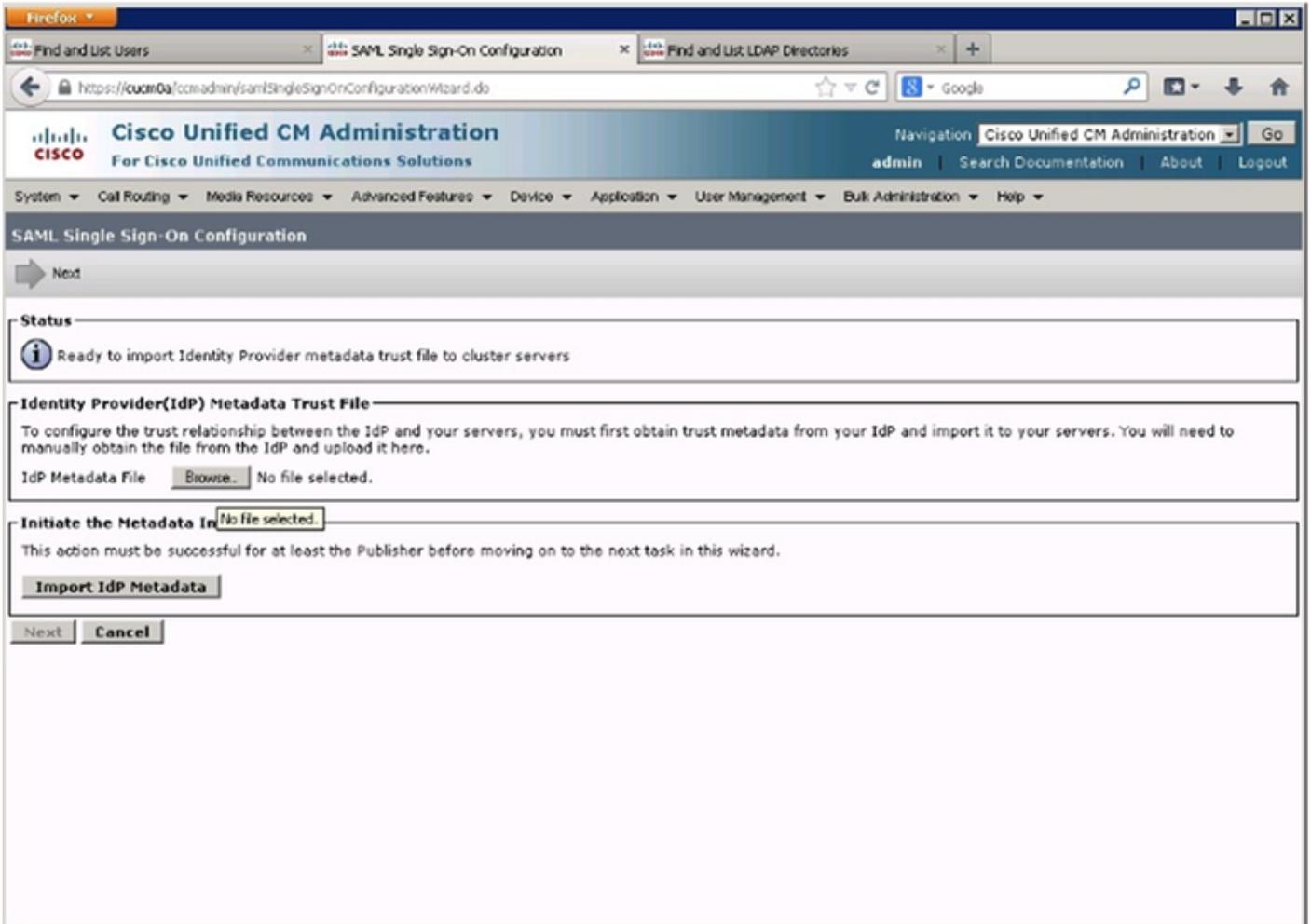
Web server connections will be restarted

Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again.

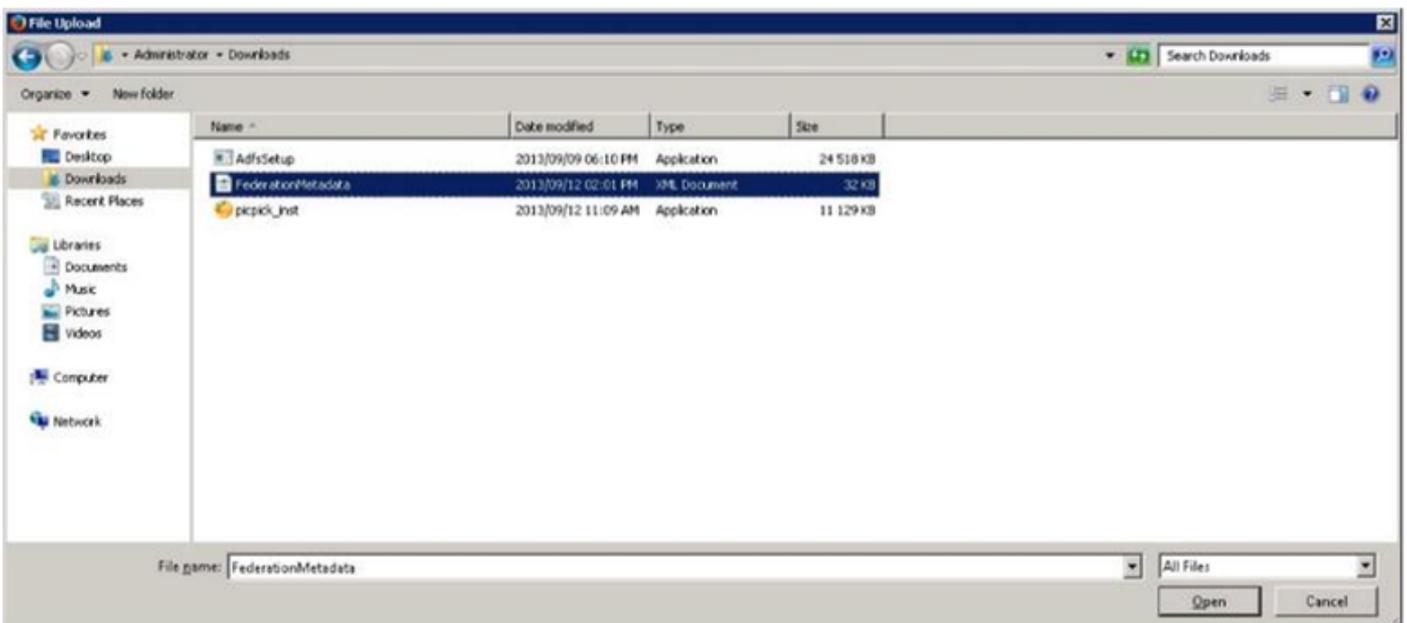
Continue Cancel

Klicken Sie auf dem SSO-Bildschirm auf **Durchsuchen..** um die XML-Datei

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



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



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 Single Sign-On Configuration - Windows Internet Explorer

Navigation Cisco Unified CM Administration Go

admin | Search Documentation | About | Logout

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

SAML Single Sign-On Configuration

Next

Status

✓ Import succeeded for all servers

Identity Provider(IdP) Metadata Trust File

To configure the trust relationship between the IdP and your servers, you must first obtain trust metadata from your IdP and import it to your servers. You will need to manually obtain the file from the IdP and upload it here.

IdP Metadata File Browse...

Initiate the Metadata Import

This action must be successful for at least the Publisher before moving on to the next task in this wizard.

✓ Import 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?servei ...

SAML Single Sign-On Configuration

Test SSO Setup

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test can be run on any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is successful.

1) Pick a valid username to use for this test

You must already know the password for the selected username.
This user must have administrator rights and also exist in the IdP.

 Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.

Valid administrator Usernames

farfar

2) Launch SSO test page

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

Sign In - Mozilla Firefox

https://ad.fhlab.com/adfs/ls/?SAMLRequest=nZJPTwIxEMXvflpN77CIAi4NS0 ...

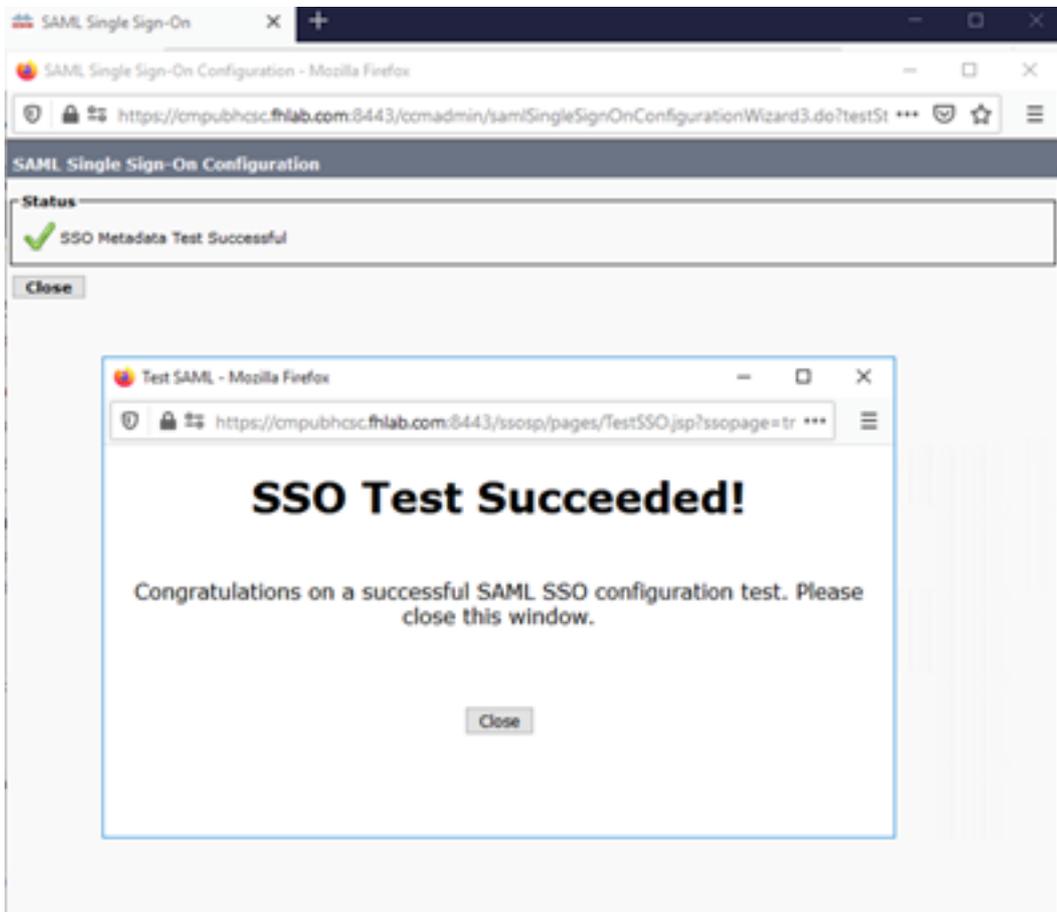
FS

Sign in with your organizational account

farfar@fhlab.com

.....

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



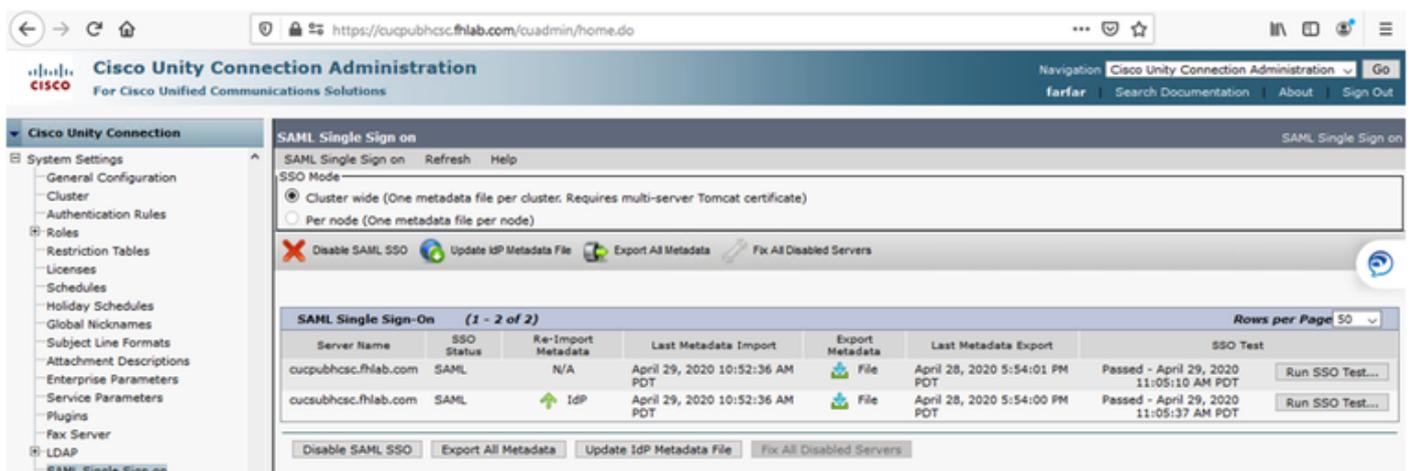
Klicken Sie auf SCHLIESSEN und FERTIG, um fortzufahren.

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

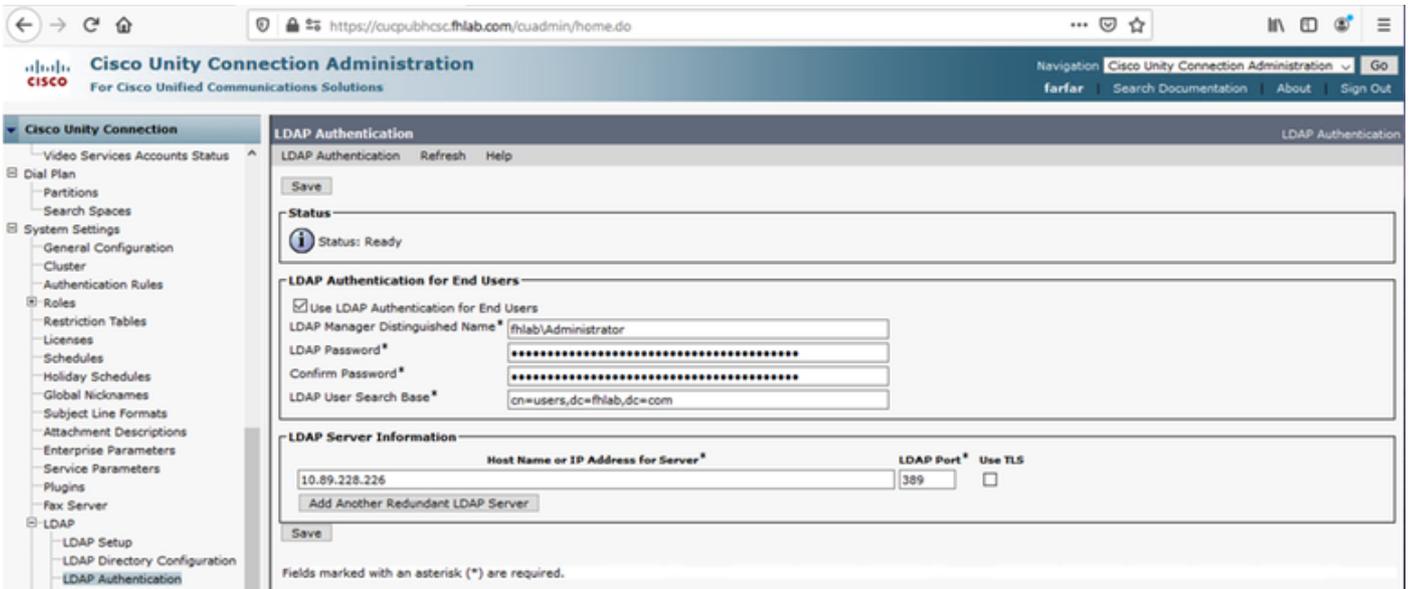
Konfigurieren von SSO auf CUC

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

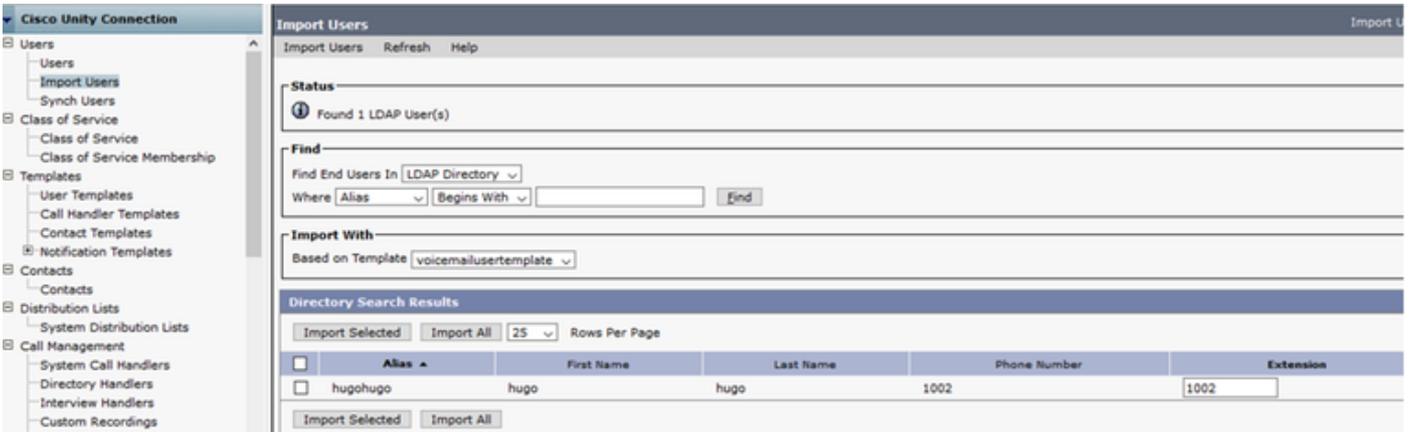
LDAP-Integration mit CUC.



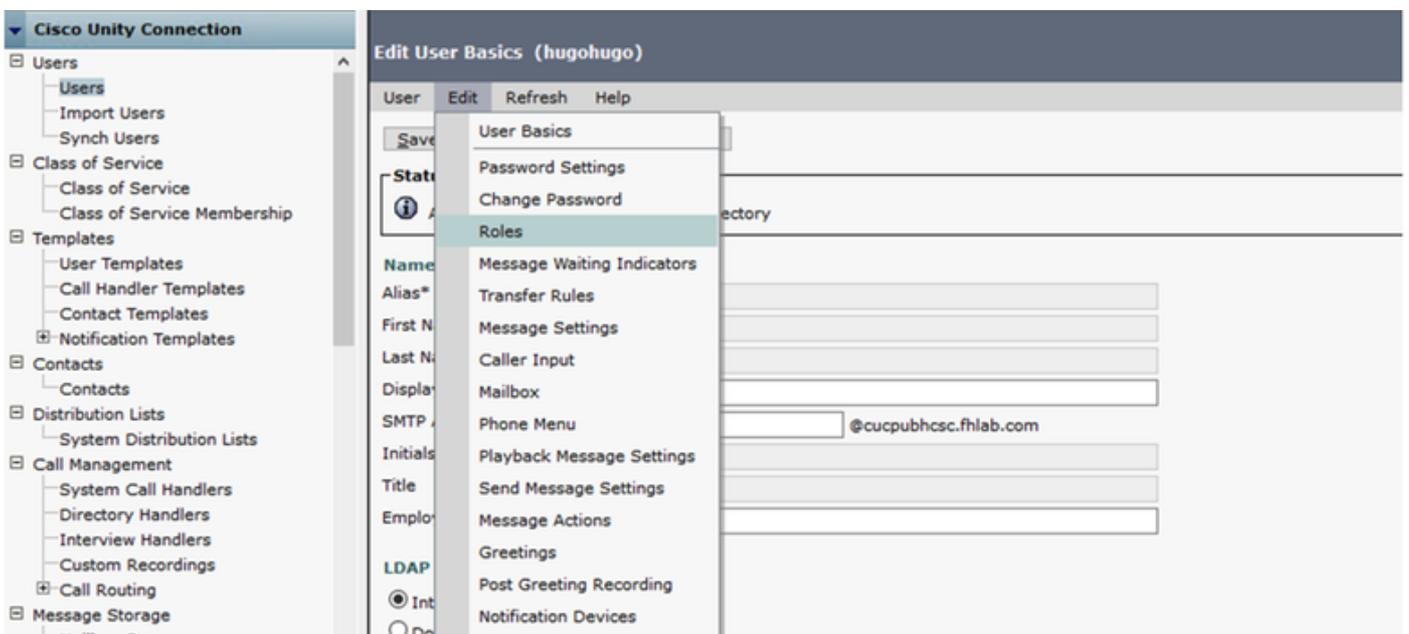
Konfigurieren der LDAP-Authentifizierung



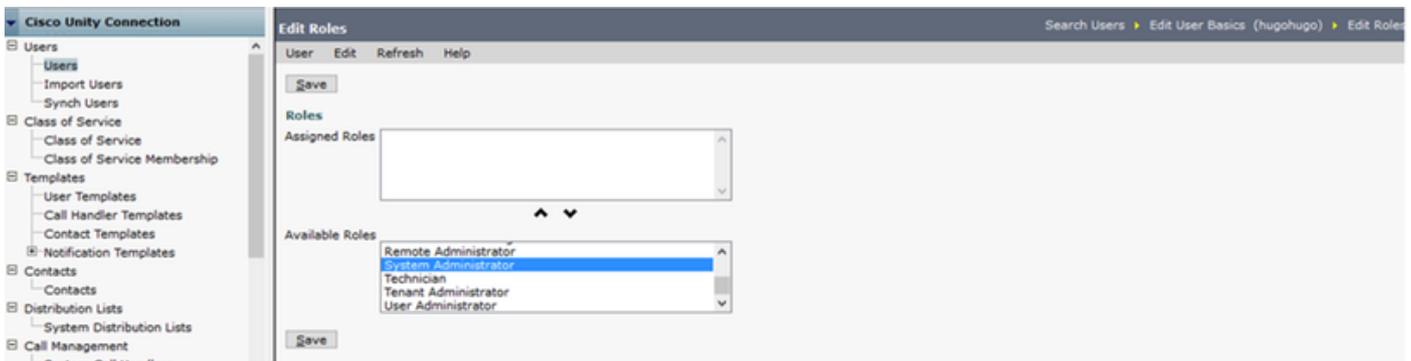
Importieren Sie die Benutzer aus LDAP, denen Voicemail zugewiesen ist, sowie den Benutzer, der für das Testen von SSO verwendet wird.



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

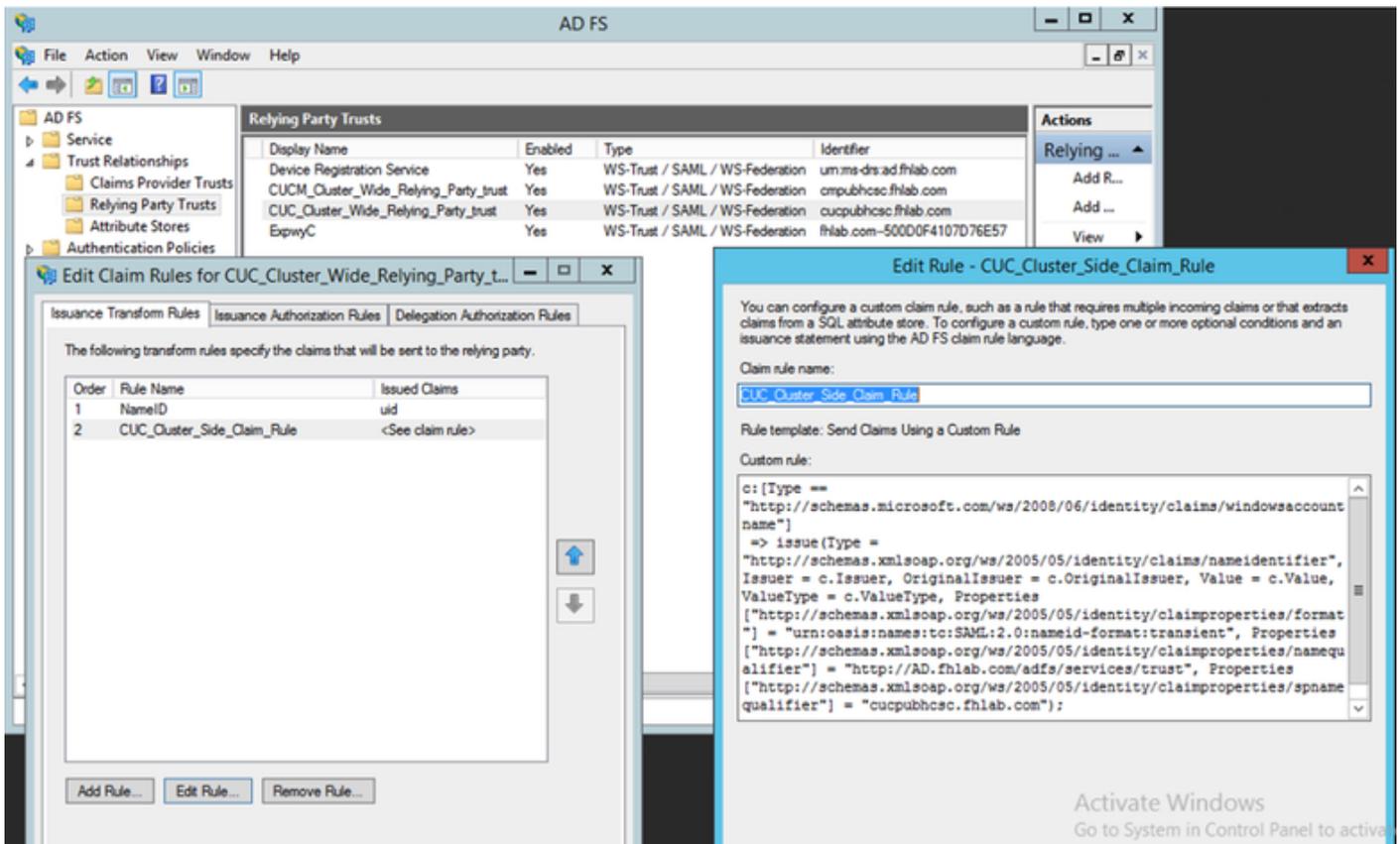


Weisen Sie dem Testbenutzer die Rolle des Systemadministrators zu.



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://cucpubhscsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?serverName: ...

SAML Single Sign on Configuration

SAML Single Sign on Configuration Refresh Help

Test SSO Setup

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test can be run on any server for troubleshooting once SSO has been enabled. SSO setup cannot be completed unless this test is successful.

1) Pick a valid username to use for this test

You must already know the password for the selected username. This user must have administrator rights and also exist in the IdP.

⚠ Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.

Valid administrator Usernames

- farfar
- hugo hugo

2) Launch SSO test page

Run SSO Test...

Cancel

SAML Single Sign on Configuration - Mozilla Firefox

https://cucpubhscsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?testStatus=1 ...

SAML Single Sign on Configuration

SAML Single Sign on Configuration Refresh Help

Status

✔ SSO Metadata Test Successful

Test SAML - Mozilla Firefox

https://cucpubhscsc.fhlab.com/ssosp/pages/TestSSO.jsp?ssopage=true

SSO Test Succeeded!

Congratulations on a successful SAML SSO configuration test. Please close this window.

Close

Navigation Cisco Unity Connection Administration Go

farfar Search Documentation About Sign Out

SAML Single Sign on

Rows per Page 50

| port data | Last Metadata Export | SSO Test | |
|-----------|-------------------------------|---|-----------------|
| File | April 28, 2020 5:54:01 PM PDT | Passed - May 24, 2020 3:17:04 PM PDT | Run SSO Test... |
| File | April 28, 2020 5:54:00 PM PDT | Passed - April 29, 2020 11:05:37 AM PDT | Run SSO Test... |

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 Metadatenfile.
- Klicken Sie im Peer-Modus neben dem Peer auf Herunterladen, um die Metadatenfile 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.

The screenshot displays the Cisco Expressway configuration interface. On the left, a tree view shows the configuration hierarchy: AD FS > Service > Trust Relationships > Relying Party Trusts. The main area is divided into two panes. The top pane, titled 'Relying Party Trusts', contains a table with the following data:

| Display Name | Enabled | Type | Identifier |
|---------------------------------------|---------|---------------------------------|----------------------------|
| Device Registration Service | Yes | WS-Trust / SAML / WS-Federation | um.ms-drs.ad.fhlab.com |
| CUCM_Cluster_Wide_Relying_Party_trust | Yes | WS-Trust / SAML / WS-Federation | cmpubhcsc.fhlab.com |
| CUC_Cluster_Wide_Relying_Party_trust | Yes | WS-Trust / SAML / WS-Federation | cucpubhcsc.fhlab.com |
| ExpwyC | Yes | WS-Trust / SAML / WS-Federation | fhlab.com-50000F4107076E57 |

The bottom pane, titled 'Edit Claim Rules for ExpwyC', shows the configuration for a specific rule named 'NameID'. It includes a table of 'Issued Claims' with one entry:

| Order | Rule Name | Issued Claims |
|-------|-----------|---------------|
| 1 | NameID | uid |

Below this table are buttons for 'Add Rule...', 'Edit Rule...', and 'Remove Rule...'. The right side of the 'Edit Rule - NameID' pane contains configuration options: 'Claim rule name' (NameID), 'Rule template: Send LDAP Attributes as Claims', 'Attribute store' (Active Directory), and a 'Mapping of LDAP attributes to outgoing claim types' table:

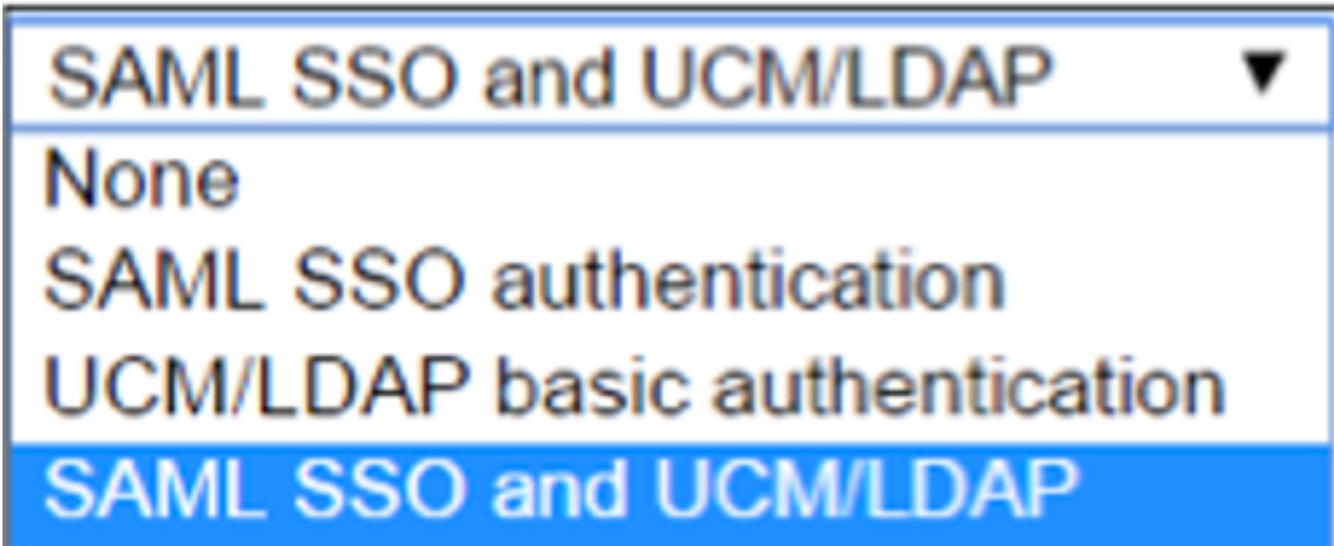
| LDAP Attribute (Select or type to add more) | Outgoing Claim Type (Select or type to add more) |
|---|--|
| SAM-Account-Name | uid |
| * | |

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

Authentifizierungspfad



- 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

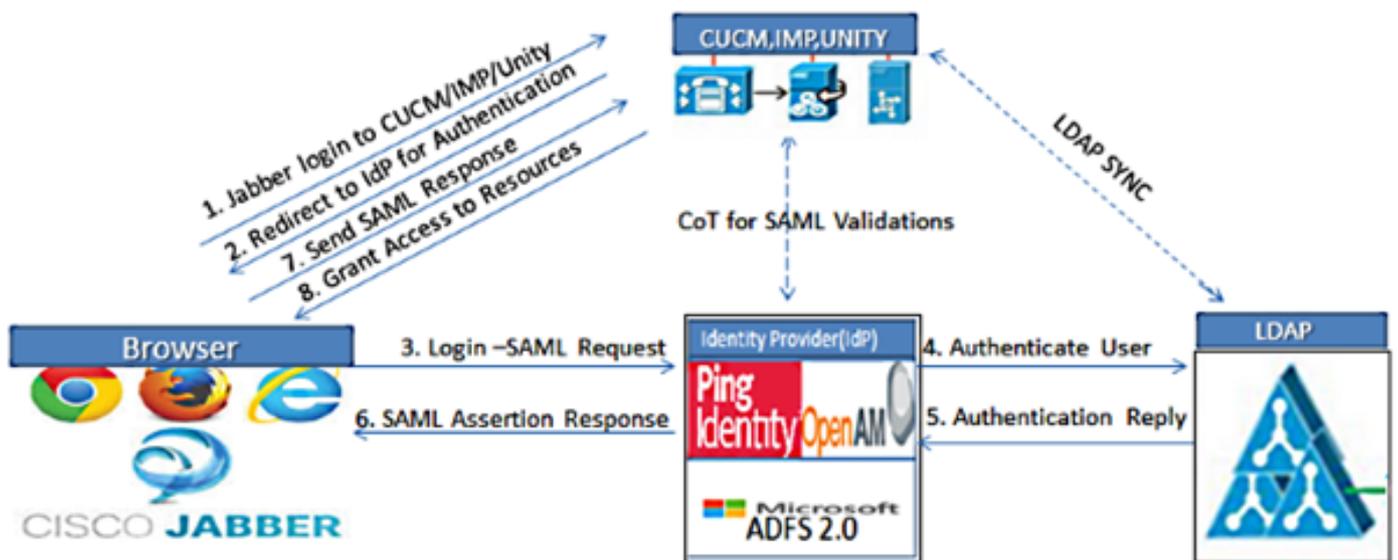
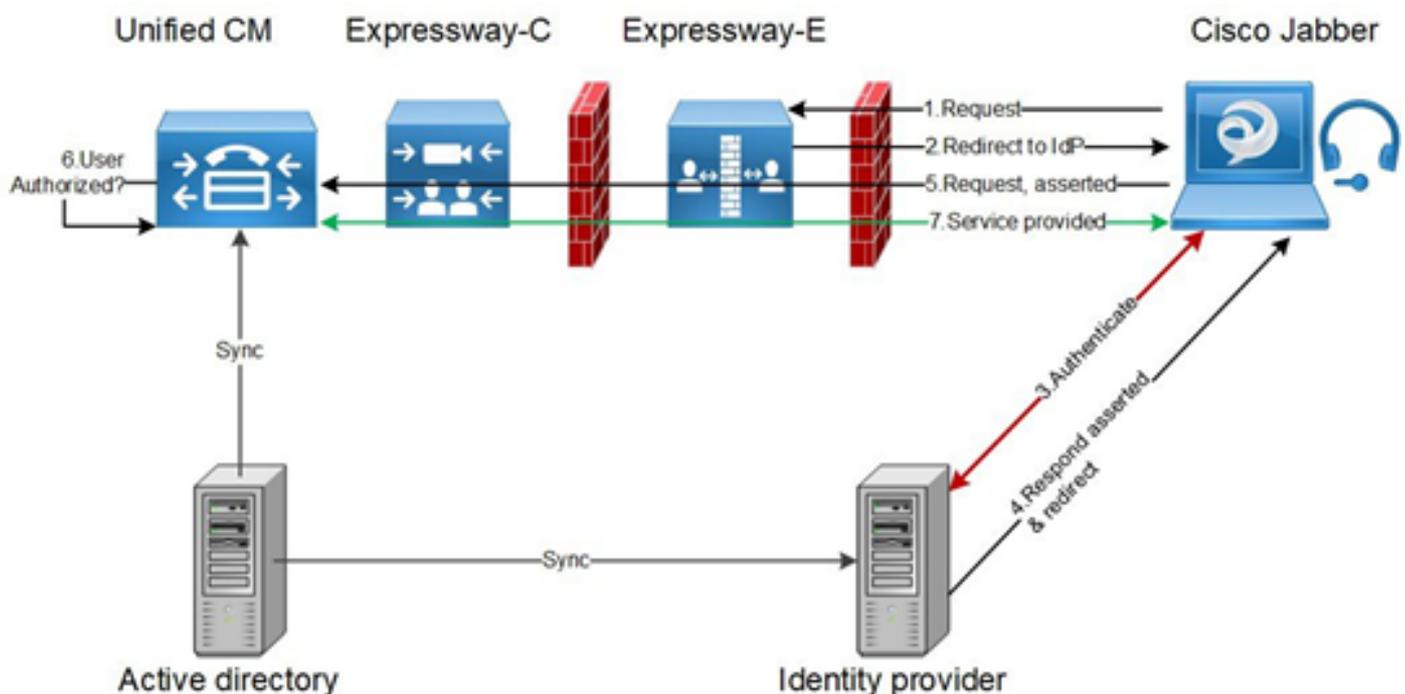


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

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 Aktualisierungstoken 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-Autorisierungscode 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 Autorisierungscode vom Autorisierungsserver angefordert. Dieser direkte Austausch des Zugriffs-Tokens ist sicherer und reduziert das Risiko.

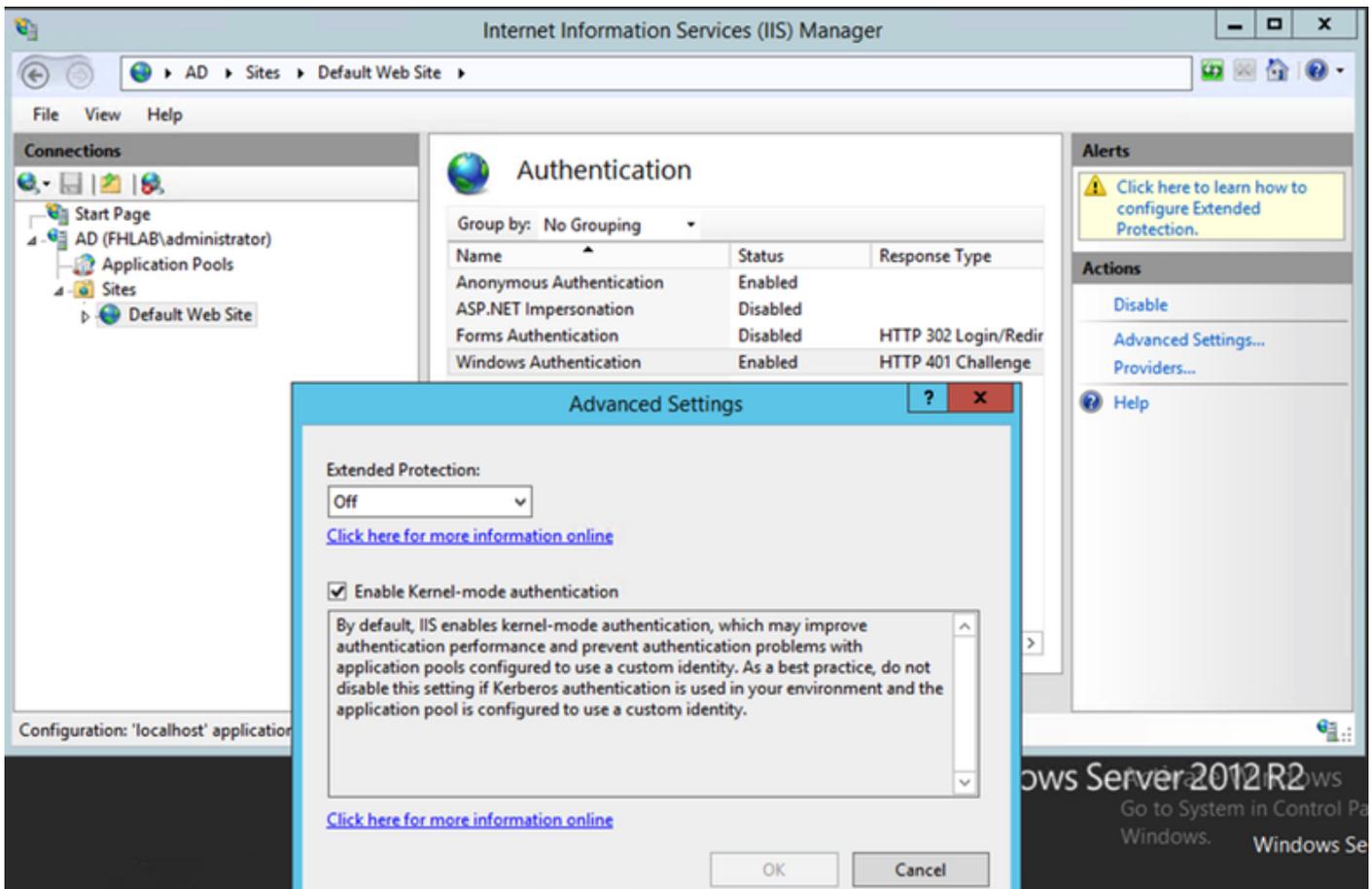
Der OAuth-Autorisierungscode-Grant-Fluss unterstützt die Verwendung von Aktualisierungstoken. Dies verbessert die Benutzerfreundlichkeit, da die Benutzer sich nicht so häufig erneut authentifizieren müssen (standardmäßig 60 Tage).

Konfigurieren von Kerberos

Windows-Authentifizierung auswählen

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

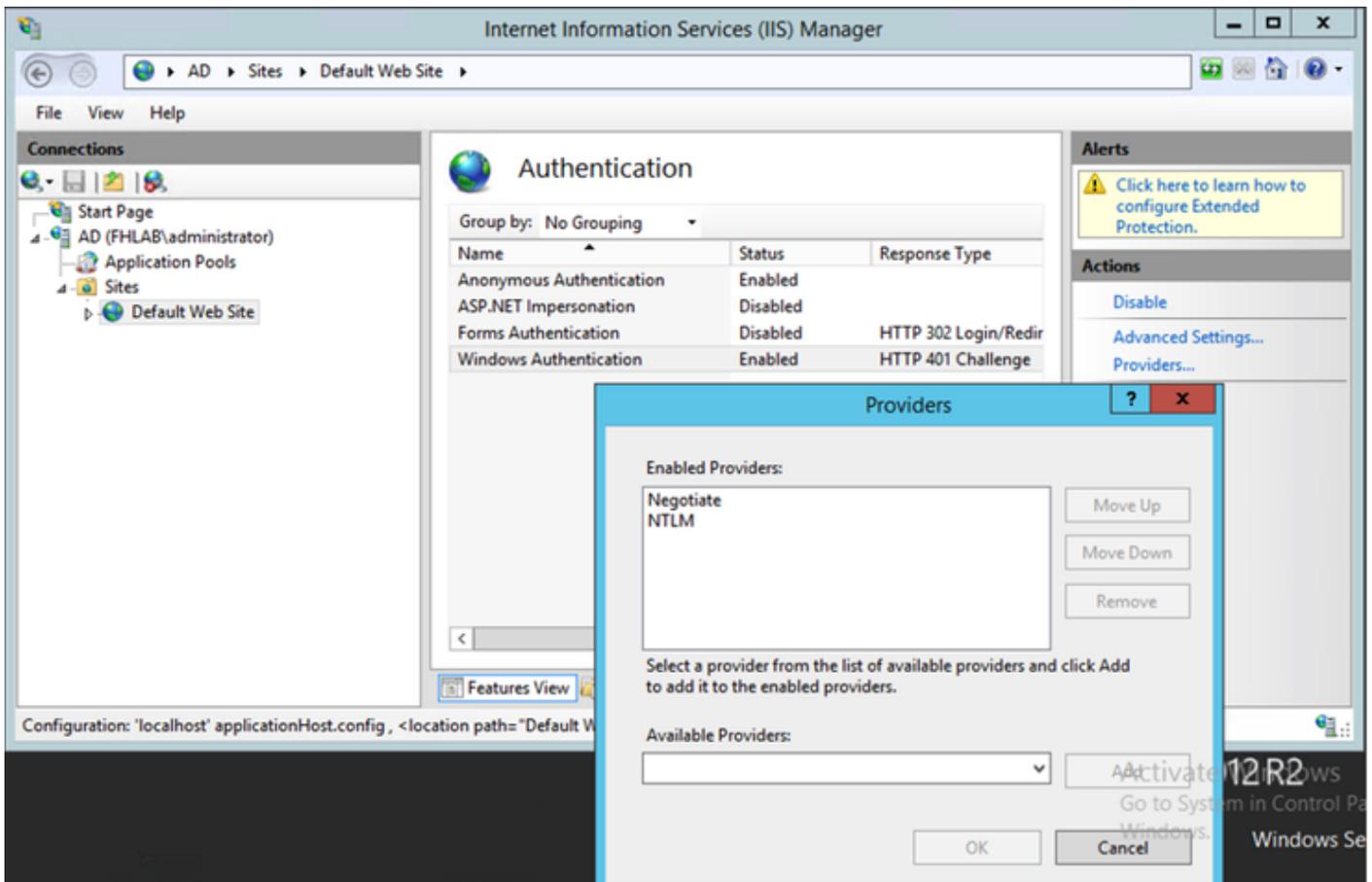
1. Deaktivieren Sie Kernel-Modus-Authentifizierung aktivieren.
2. Stellen Sie sicher, dass der erweiterte Schutz deaktiviert ist.



ADFS unterstützt beide Kerberos NTLM

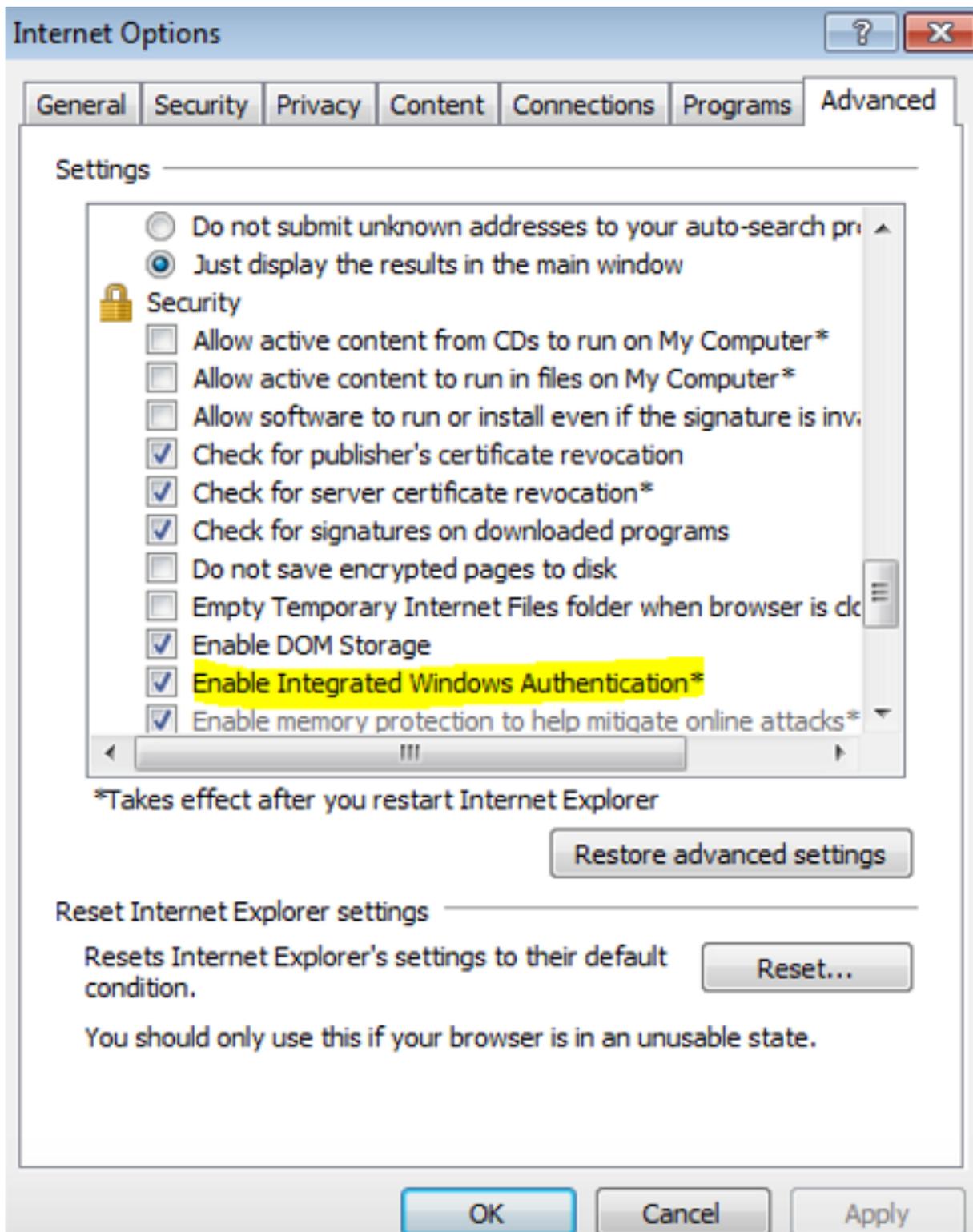
Stellen Sie sicher, dass AD FS Version 3.0 sowohl das Kerberos-Protokoll als auch das NT LAN Manager-Protokoll (NTLM) unterstützt, da alle Nicht-Windows-Clients Kerberos nicht verwenden können und sich auf NTLM verlassen.

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



Konfigurieren von Microsoft Internet Explorer

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



ADFS-URL unter Sicherheit > Intranetzonen > Standorte hinzufügen

