

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

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratie vooraf controleren](#)

[Een register](#)

[Pointer \(PTR\) records](#)

[SRV-records moeten zijn geïnstalleerd voor Jabber-detectieservices](#)

[ADFS3 Eerste configuratie](#)

[SSO op CUCM configureren met ADFS](#)

[LDAP-configuratie](#)

[CUCM-metagegevens](#)

[ADFS-relay configureren](#)

[IDP-metagegevens](#)

[SSO op CUC configureren](#)

[CUC-metagegevens](#)

[SSO op snelweg configureren](#)

[Metagegevens invoeren in snelweg C](#)

[Uitvoermetagegevens uit snelweg C](#)

[Voeg een vertrouwen van de Relay Party in Cisco Expressway-E toe](#)

[Handmatig met inloggen verversen](#)

[Verificatiepad](#)

[SSO-architectuur](#)

[Login-flow op locatie](#)

[MRA-Login Flow](#)

[OAuth](#)

[Toegang/verfrissing Token](#)

[Goedkeuringscode Subsidie Flow beter](#)

[Kerberos configureren](#)

[Selecteer Windows-verificatie](#)

[ADFS ondersteunt beide Kerberos NTLM](#)

[Microsoft Internet Explorer configureren](#)

[Voeg ADFS-URL toe onder Security > Intranet > sites >](#)

[Voeg CUCM, IMP en Unity hostname toe aan Security > Trusted Sites](#)

[Gebruikersverificatie](#)

[Jabber-aanmelding bij SSO](#)

[Problemen oplossen](#)

[Internet Explorer \(IE\)](#)

[Plaatsen toegevoegd aan IE](#)

[Niet sync-probleem](#)

[Token intrekken](#)

[Bootstrap-bestand](#)

[SSO-defect MSIS7066](#)

## Inleiding

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

## Voorwaarden

### Vereisten

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

### Gebruikte componenten

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

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

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

## Configuratie vooraf controleren

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

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

### Een register

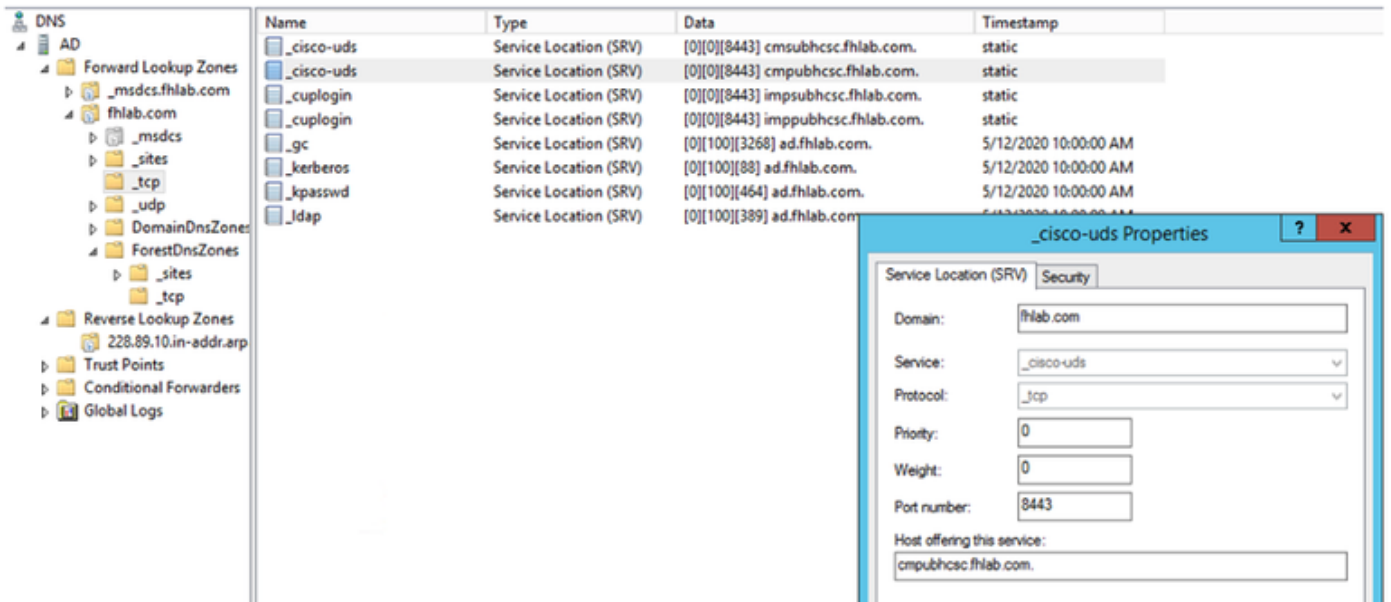
In Fhlab.com. er zijn ook gasteren cmpubhcsc , cmsubhcsc , cucpubhcsc , cucsubhcsc , expwyc , expwye , impubhcsc en imsubhcsc aan toegevoegd .

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)
impsubhcsc	Host (A)

## Pointer (PTR) records

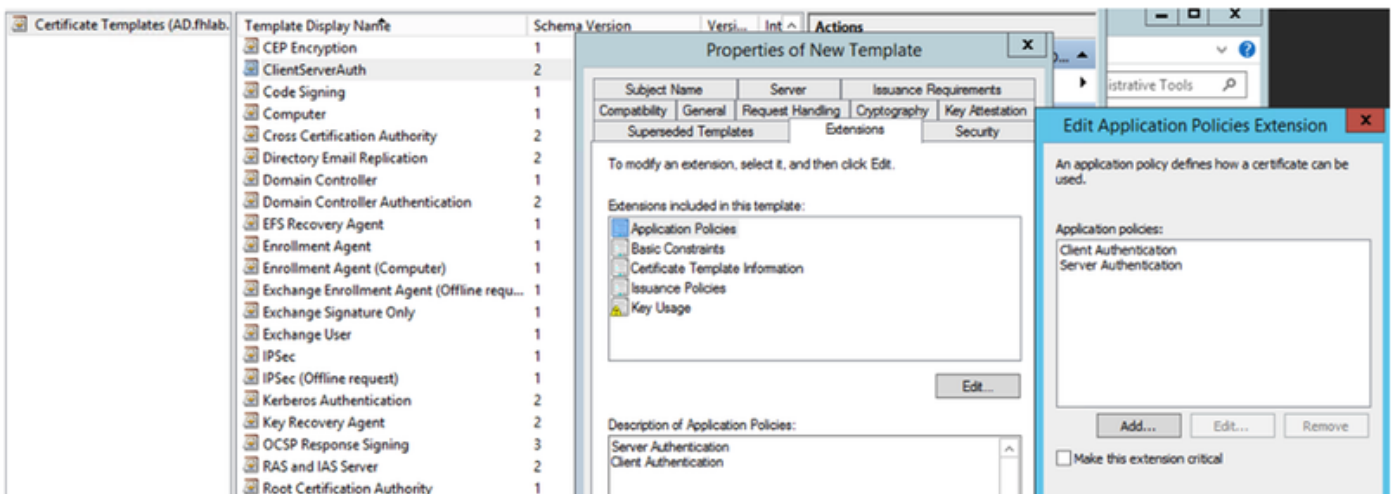
Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[14], ad.fhlab.com, hostmaster.fhlab.co...	static
(same as parent folder)	Name Server (NS)	ad.fhlab.com.	static
10.89.228.144	Pointer (PTR)	expwyc.fhlab.com.	static
10.89.228.145	Pointer (PTR)	expwye.fhlab.com.	static
10.89.228.146	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)	impsubhcsc.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

SRV-records moeten zijn geïnstalleerd voor Jabber-detectieservices



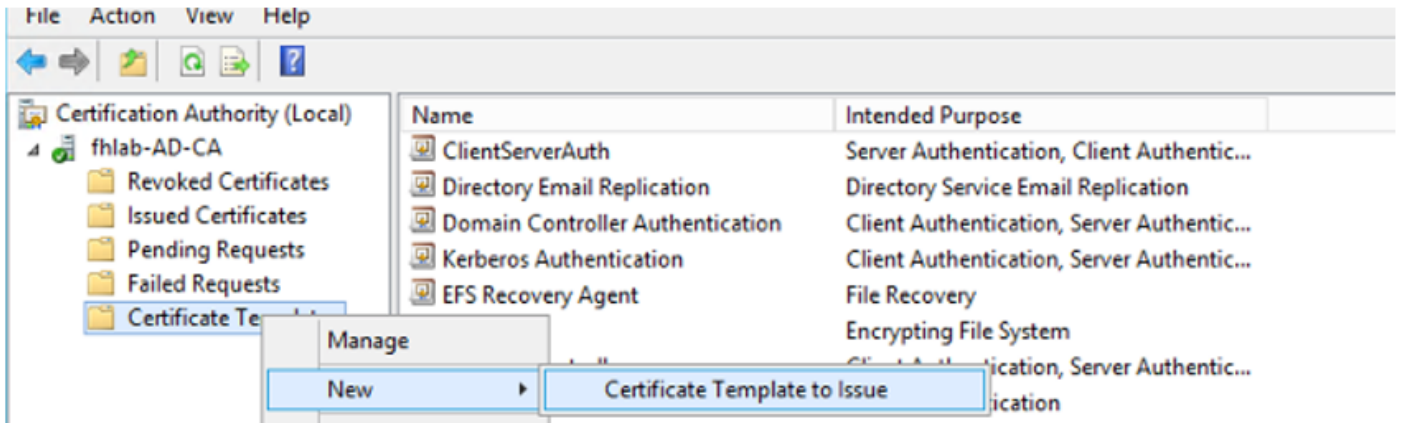
- Root CA (ervan uitgaande dat de certificaten door Enterprise CA zijn ondertekend)

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

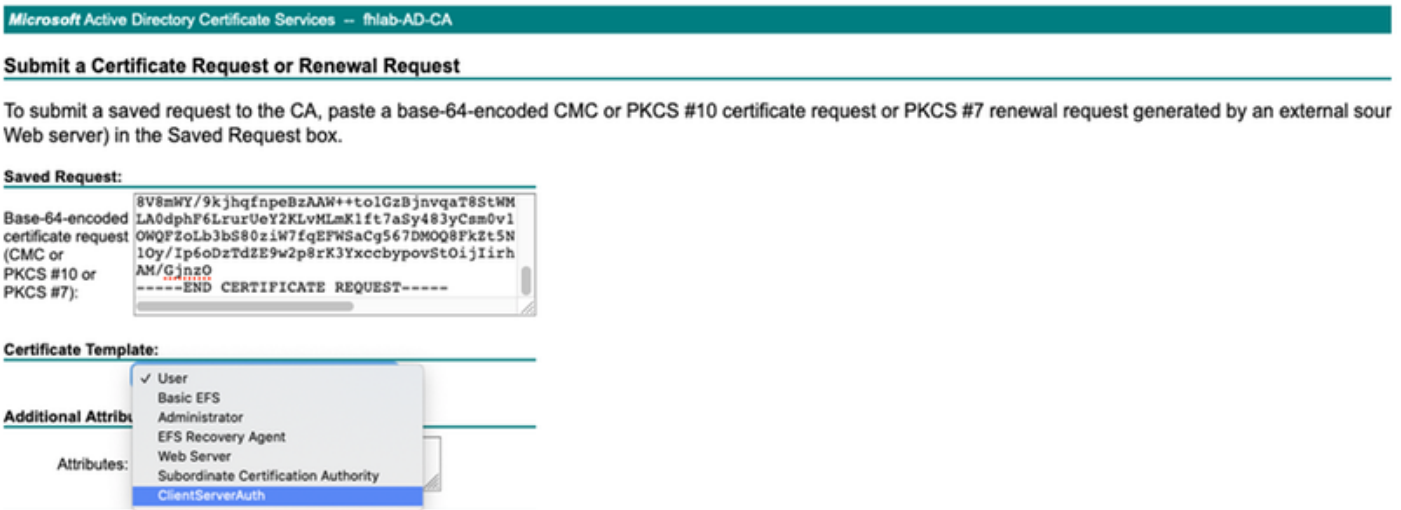


De gecreëerde sjabloon moet worden uitgegeven om CSR te kunnen tekenen.





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



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

### Generate Certificate Signing 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  
 impubhcsc.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

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

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

Certificate	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	cmpubhcsc-EC.fhlab.com	Self-signed	EC	cmpubhcsc.fhlab.com	cmpubhcsc-EC.fhlab.com	04/02/2025	Self-signed certificate generated by system
tomcat-trust	impubhcsc-EC.fhlab.com	Self-signed	EC	impubhcsc.fhlab.com	impubhcsc-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	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

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat	cmpubhcsc-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/28/2022	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	impubhcsc-EC.fhlab.com	Self-signed	EC	impubhcsc.fhlab.com	impubhcsc-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

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

- IS

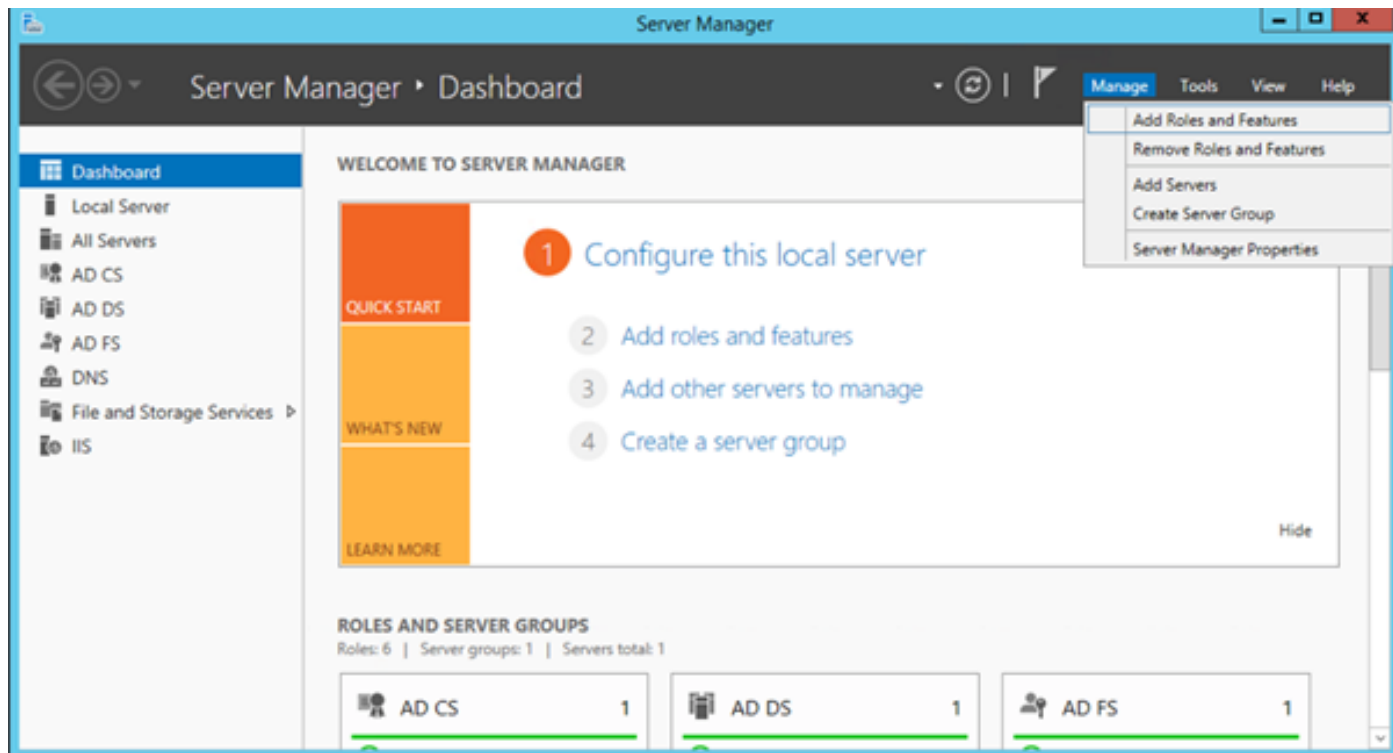
Als dit niet het geval is, wordt in dit gedeelte deze rollen geïnstalleerd. Anders slaat u deze sectie

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

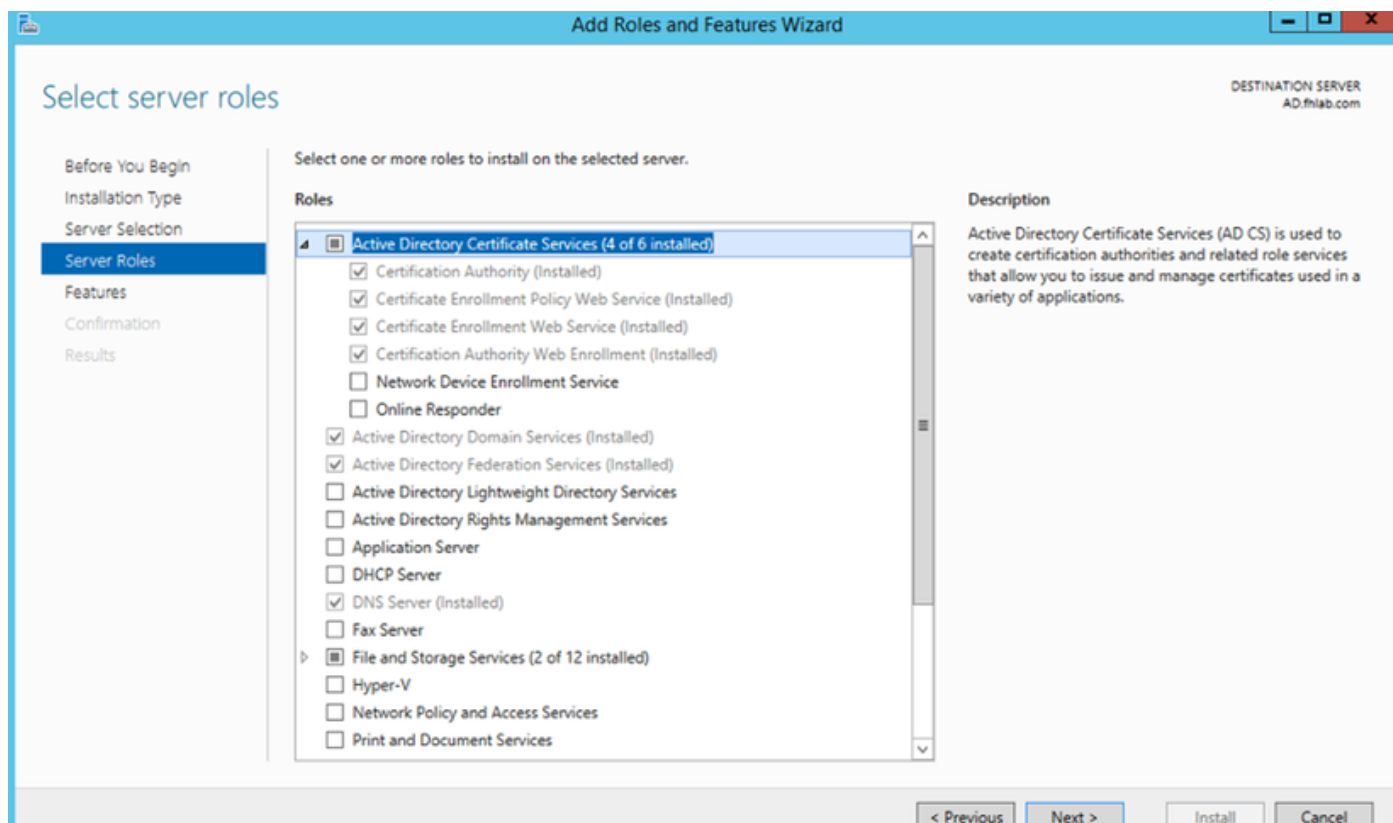
Nadat u Windows 2012 R2 met DNS hebt geïnstalleerd, promoot u de server aan een Domain Controller.

De volgende taak is het installeren van Microsoft certificaatservices.

Navigeren naar Server Manager en een nieuwe rol toevoegen:



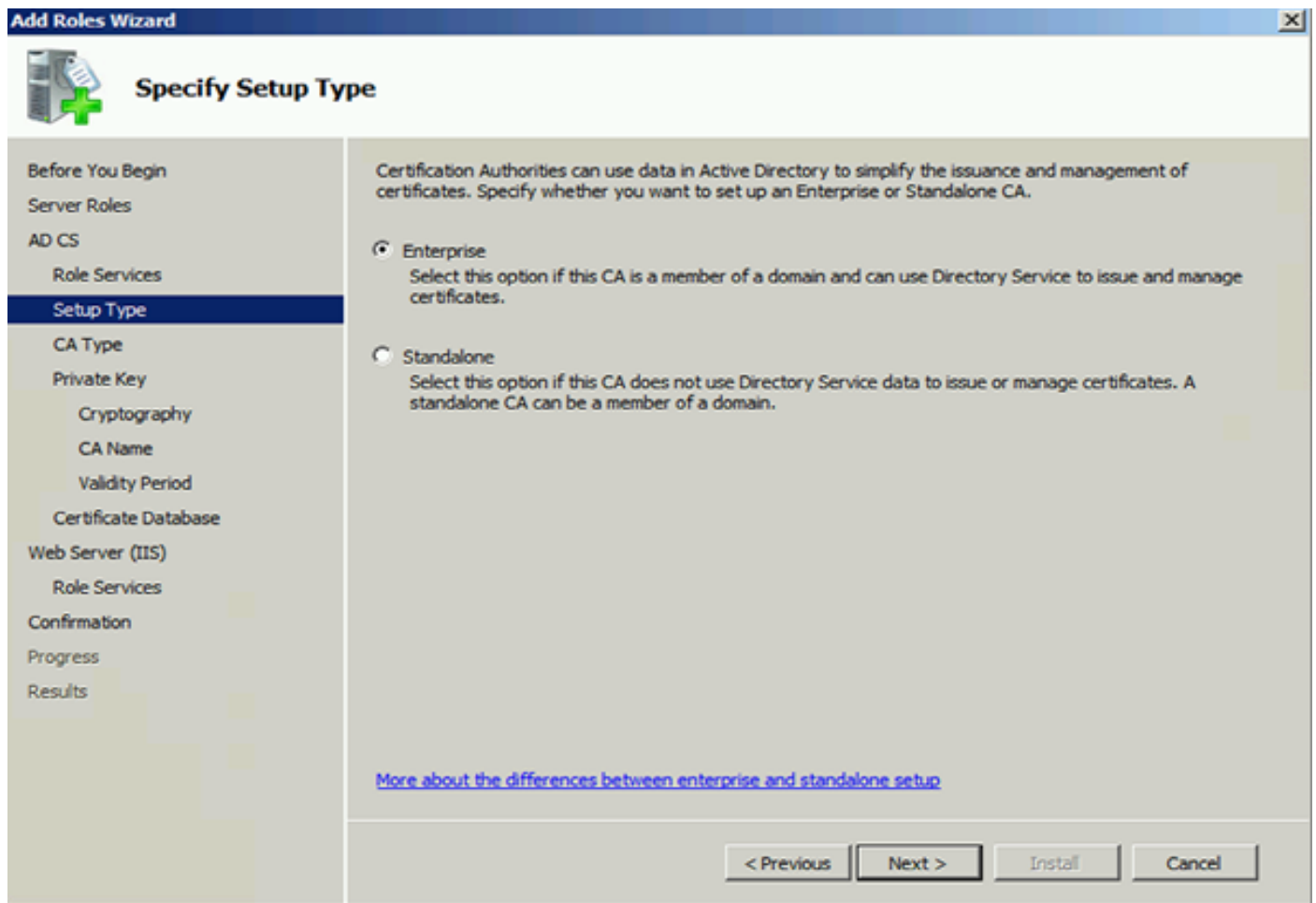
Selecteer de rol **Active Directory certificaatservices**.



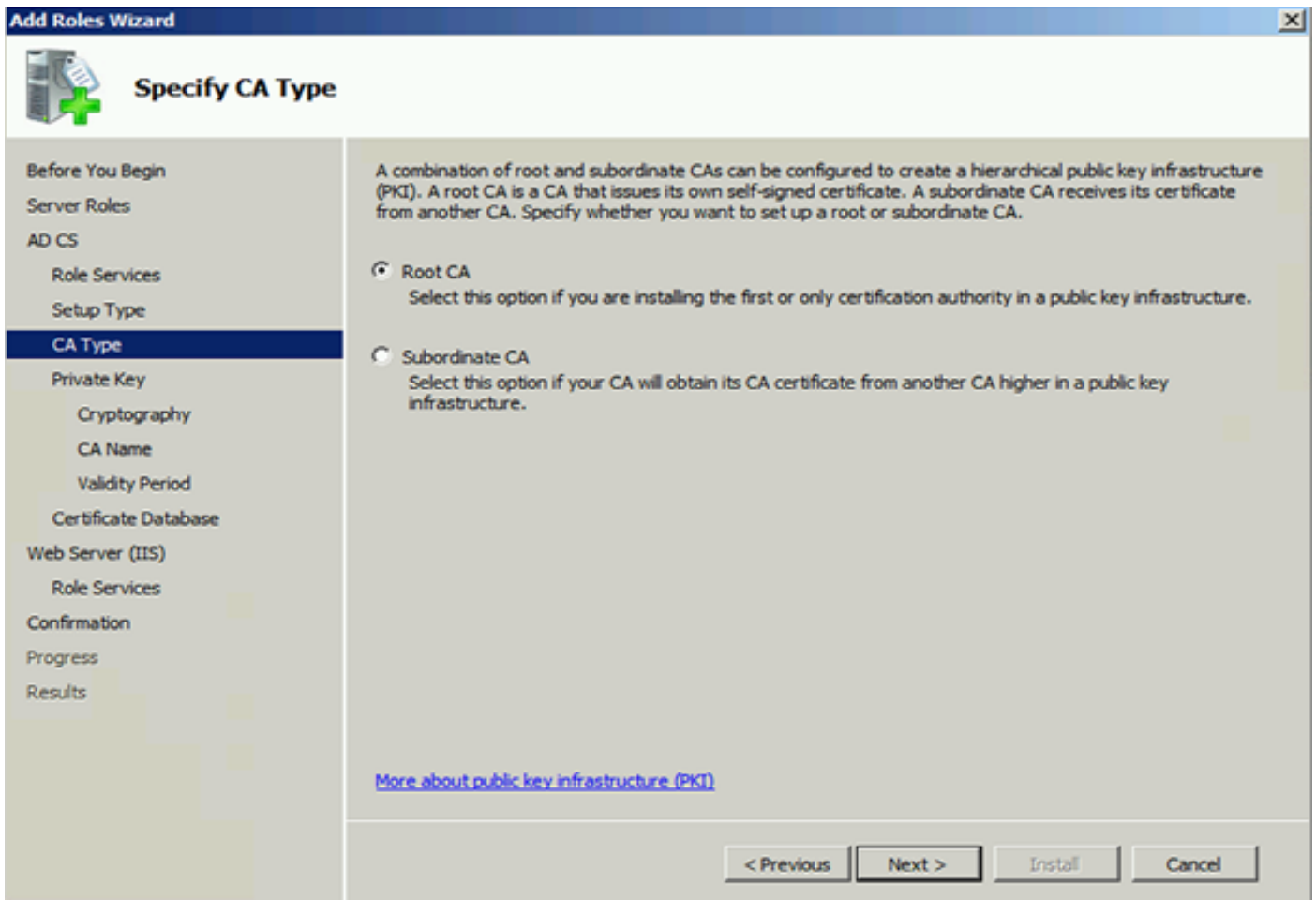
En stel deze services in - de dienst van het Web van de Inschrijving van het Certificaat van de Autoriteit voor het Beleid van het Web eerst. Nadat deze twee rollen zijn geïnstalleerd, configureer ze en installeer vervolgens **Web Service** en **Web Encapsulation certificaatschrijving**. Configureer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

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

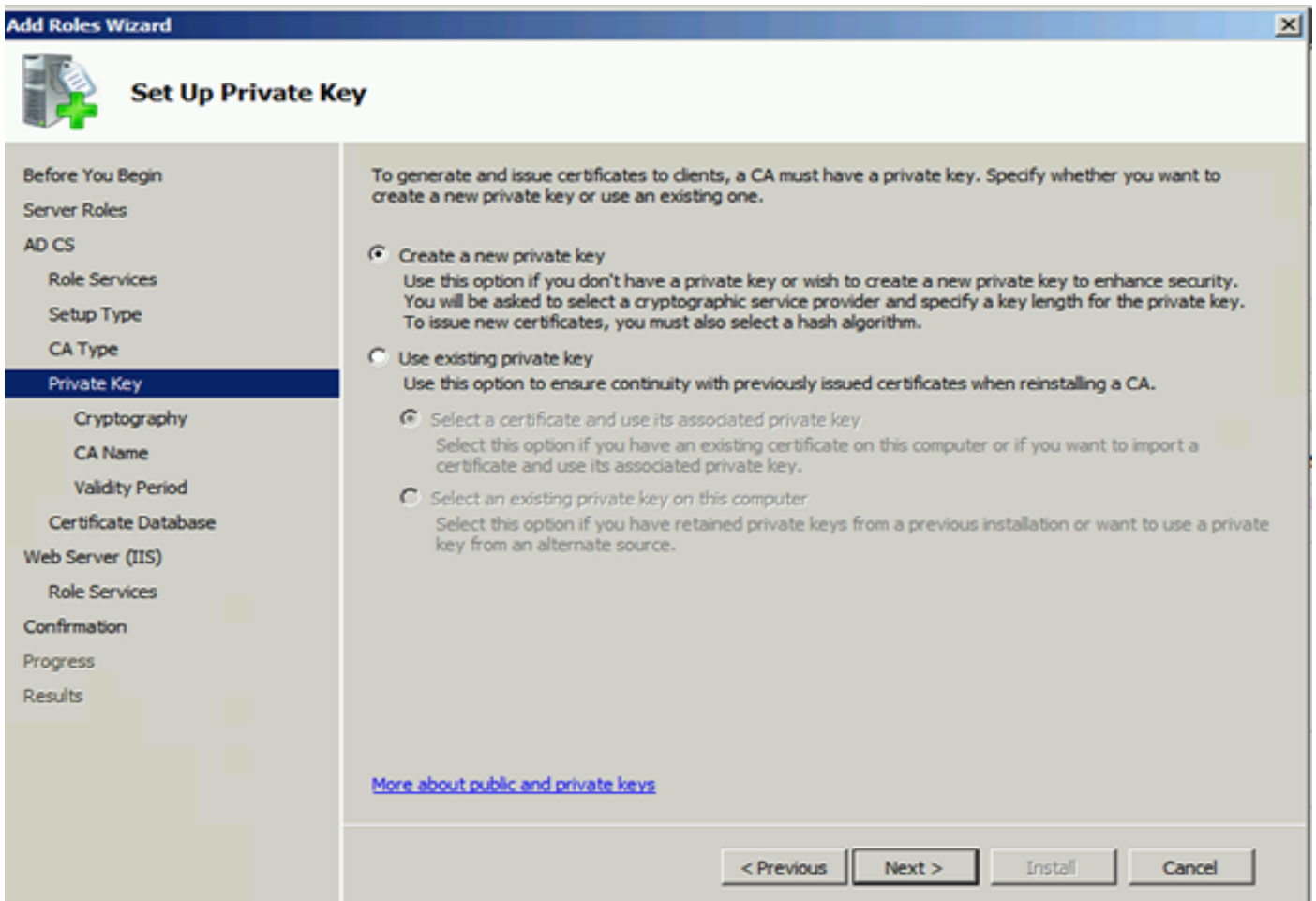
Afhankelijk van uw plaatsing, kunt u Enterprise of Standalone selecteren.



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

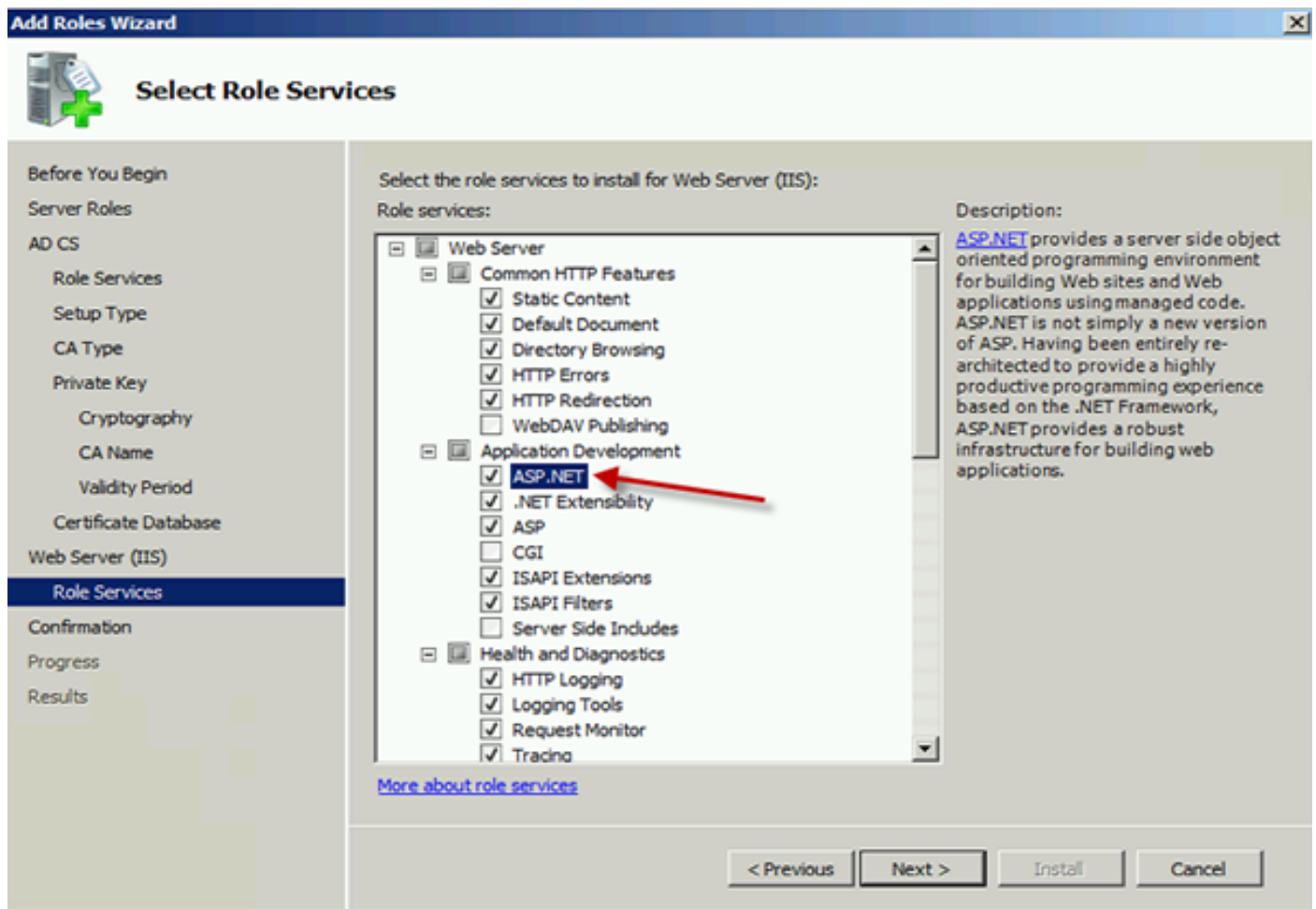


De volgende stap is het maken van een privé sleutel voor uw CA.



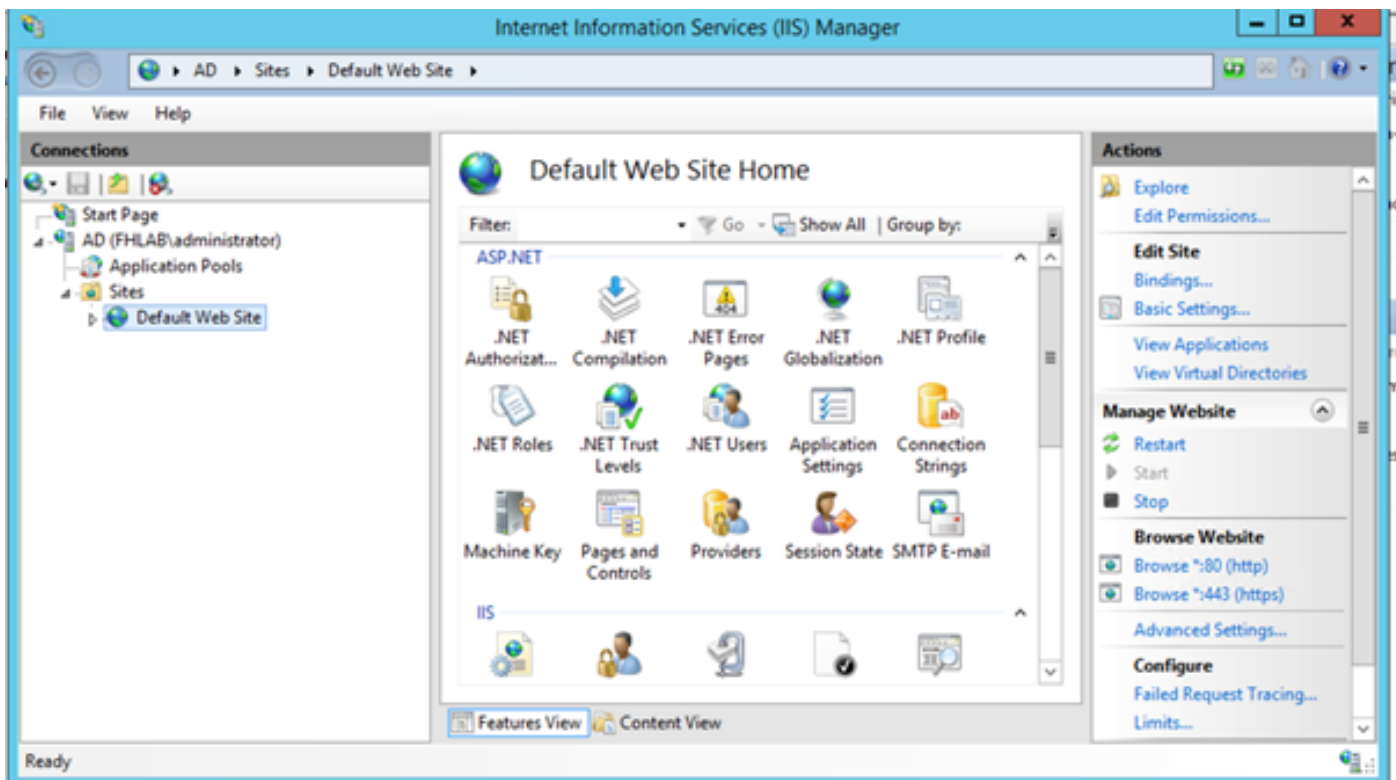
Deze stap is alleen nodig als u ADFS3 op een afzonderlijke Windows Server 2012 installeert.

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

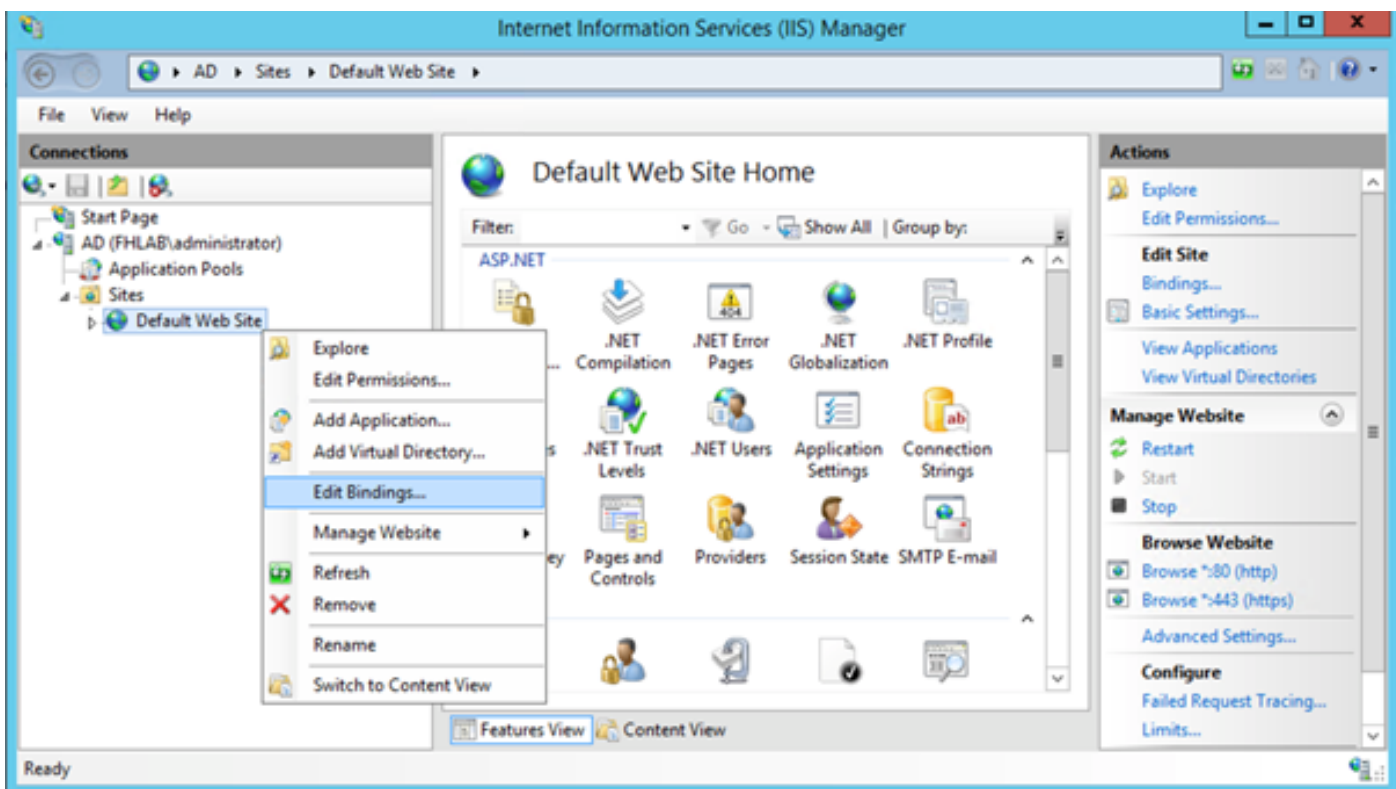


In Server Manager, klik op **Web Server > is**, en klik dan met de rechtermuisknop op **Standaard Website**. De binding moet worden gewijzigd om HTTPS ook toe te staan naast HTTP. Dit gebeurt ter ondersteuning van HTTPS.

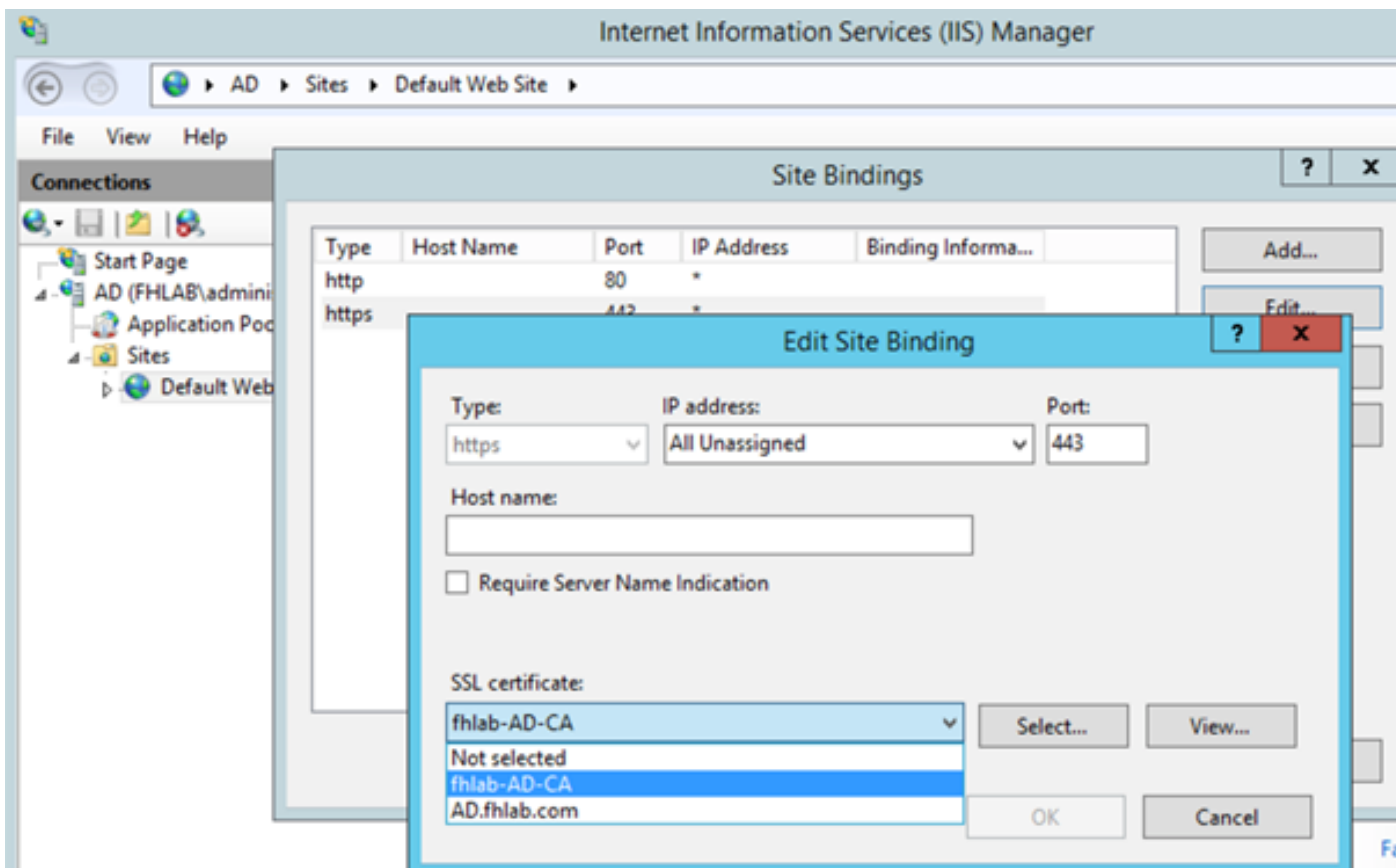




Selecteer **Banden bewerken**.

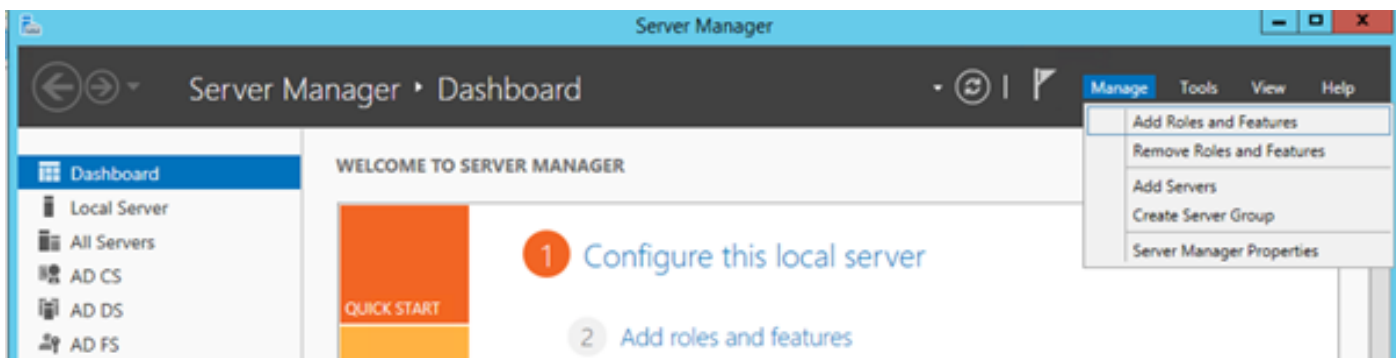


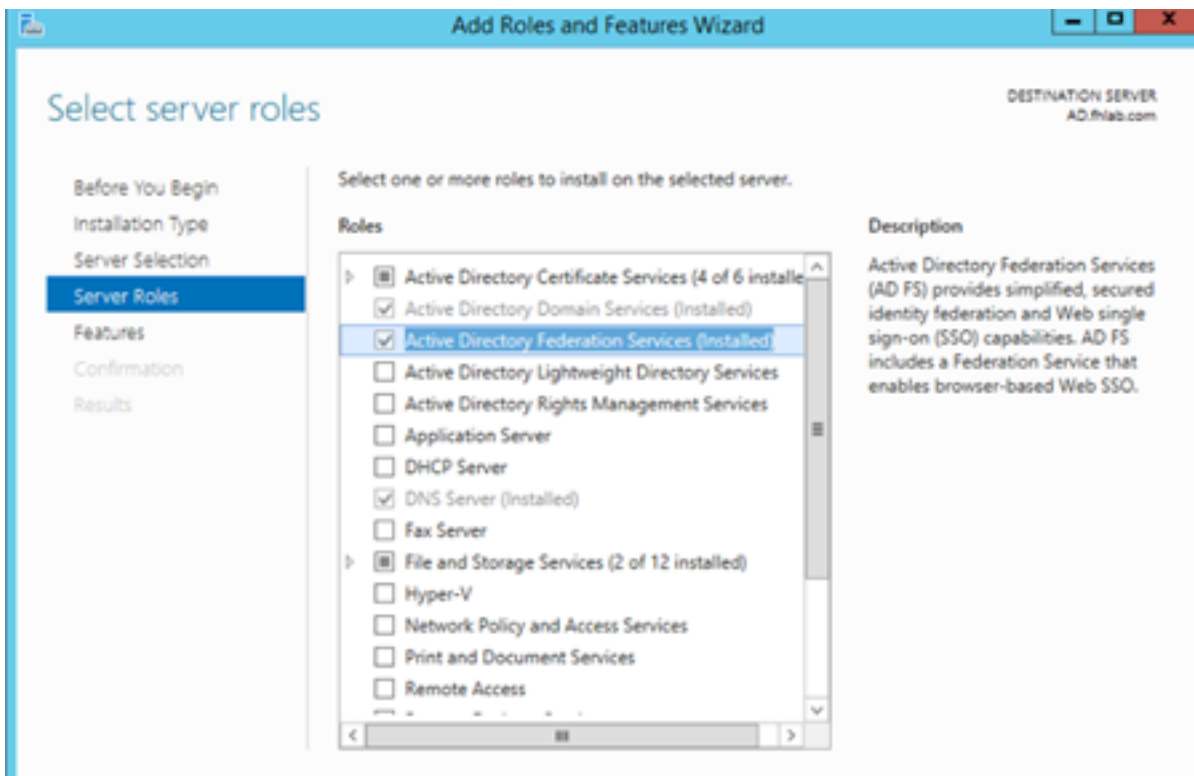
Voeg een nieuwe Site-binding toe en selecteer **HTTPS** als type. Kies voor het SSL-certificaat het servercertificaat dat dezelfde FQDN moet hebben als uw AD-server.



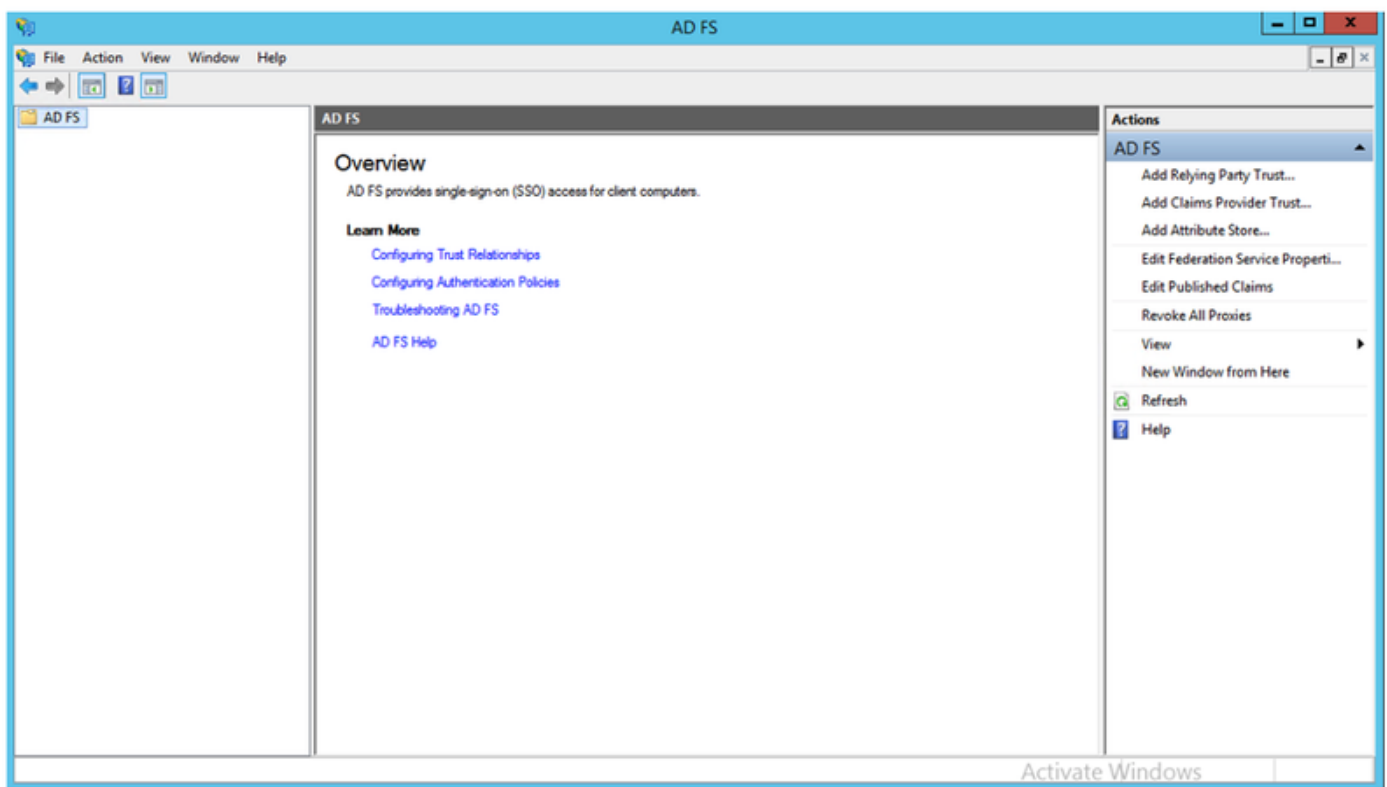
Alle vereiste rollen zijn geïnstalleerd in de omgeving, zodat u nu kunt doorgaan met de installatie van ADFS3 Active Directory Federation Services (op Windows Server 2012).

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





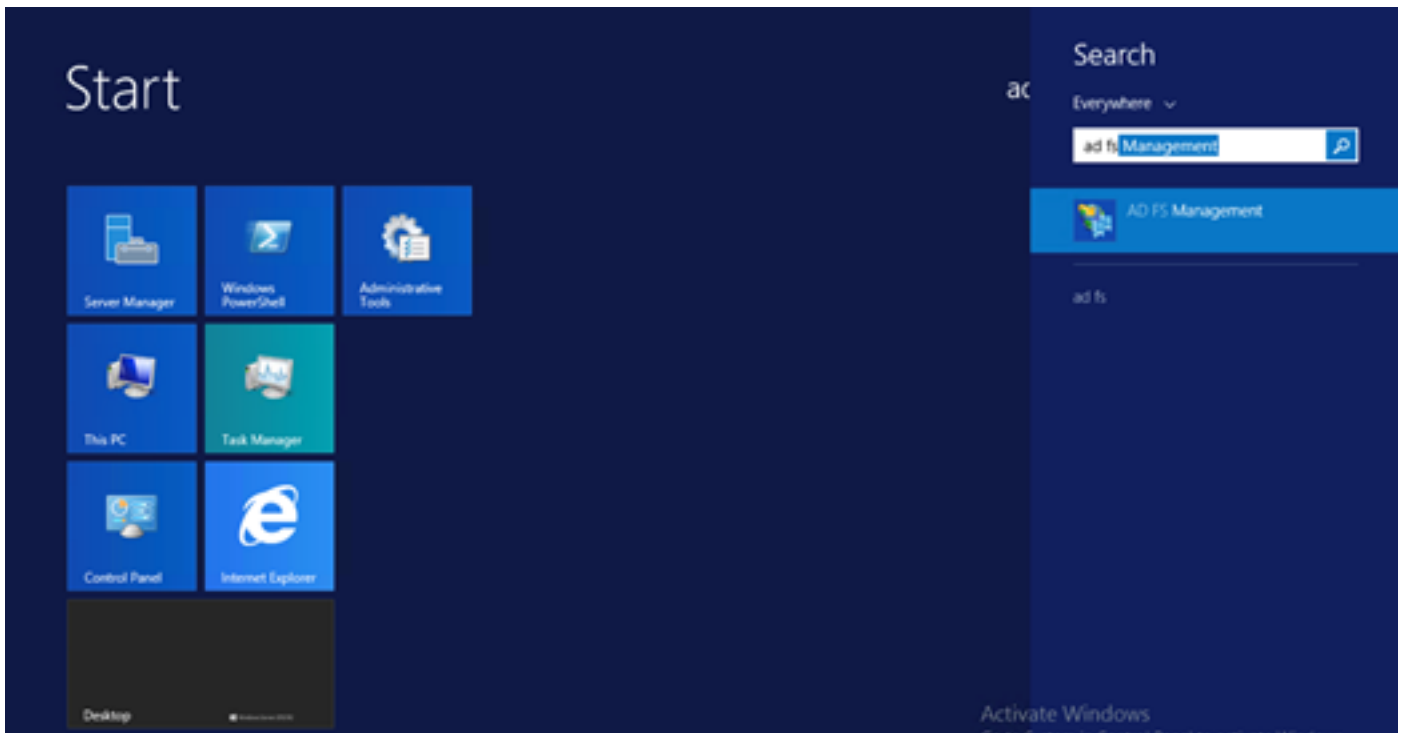
Nadat de installatie is voltooid, kunt u deze openen in de taakbalk of in het startmenu.



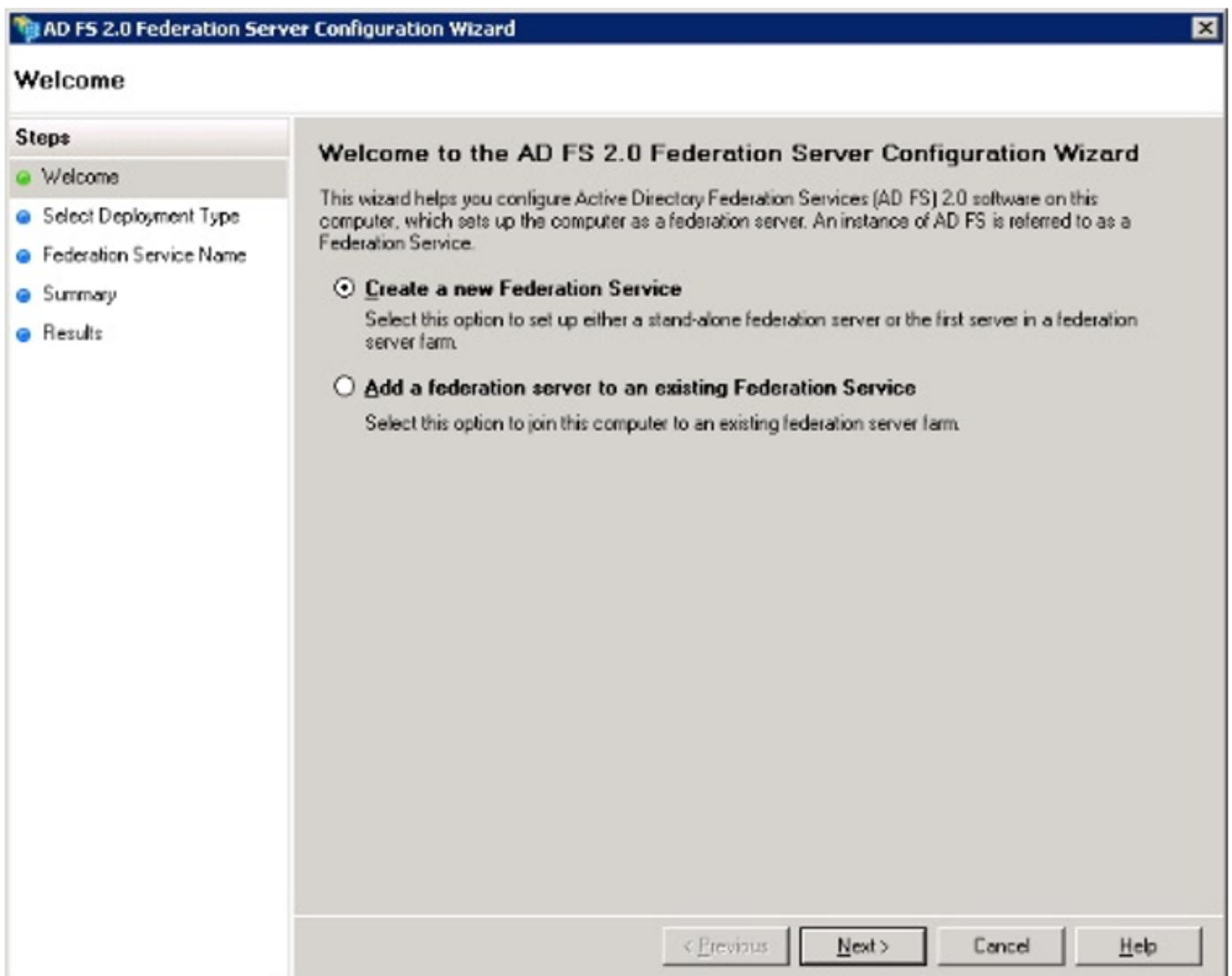
## ADFS3 Eerste configuratie

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

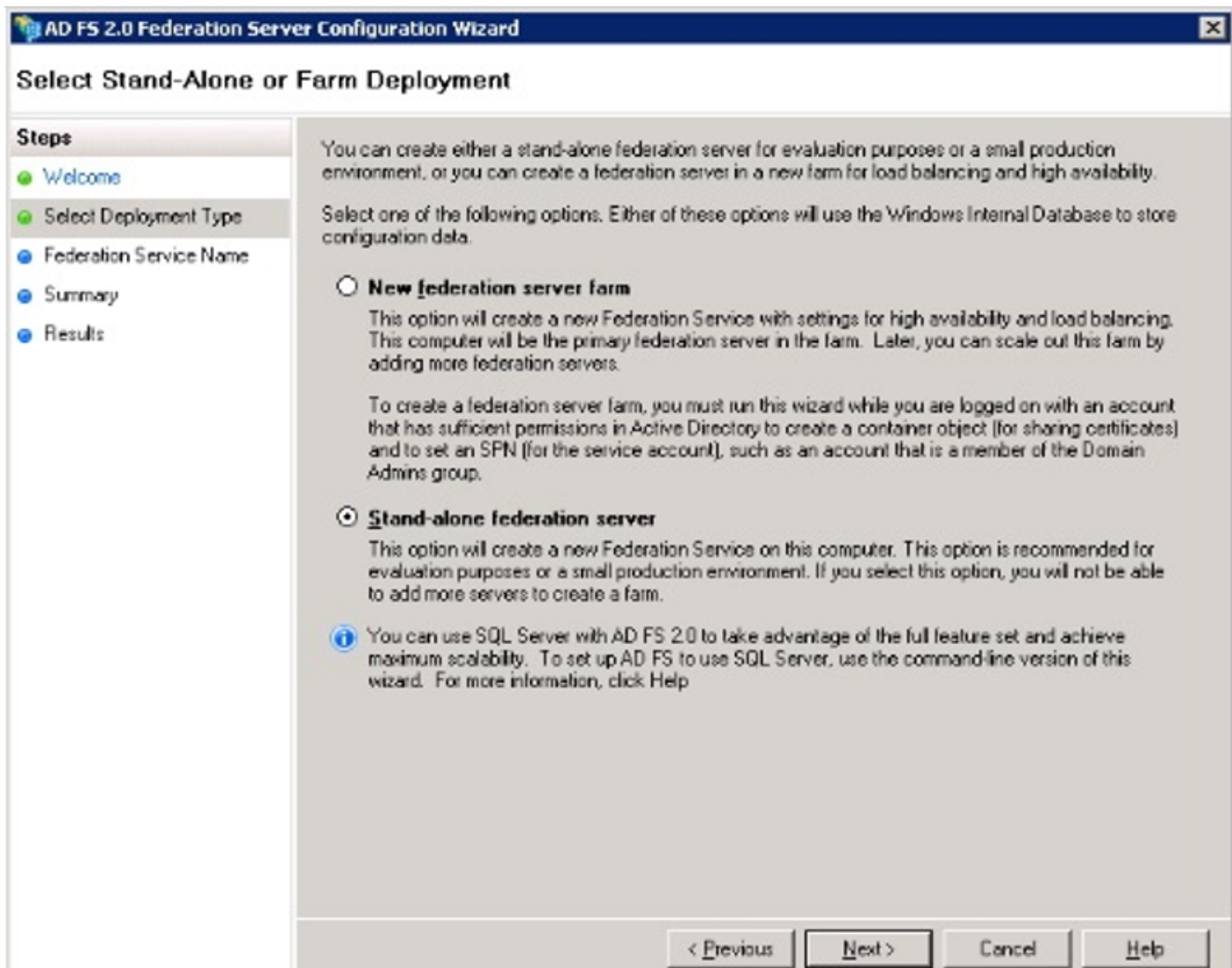
Selecteer **Windows** en type **AD FS Management** om de ADFS-beheerconsole te starten zoals in de afbeelding wordt getoond.



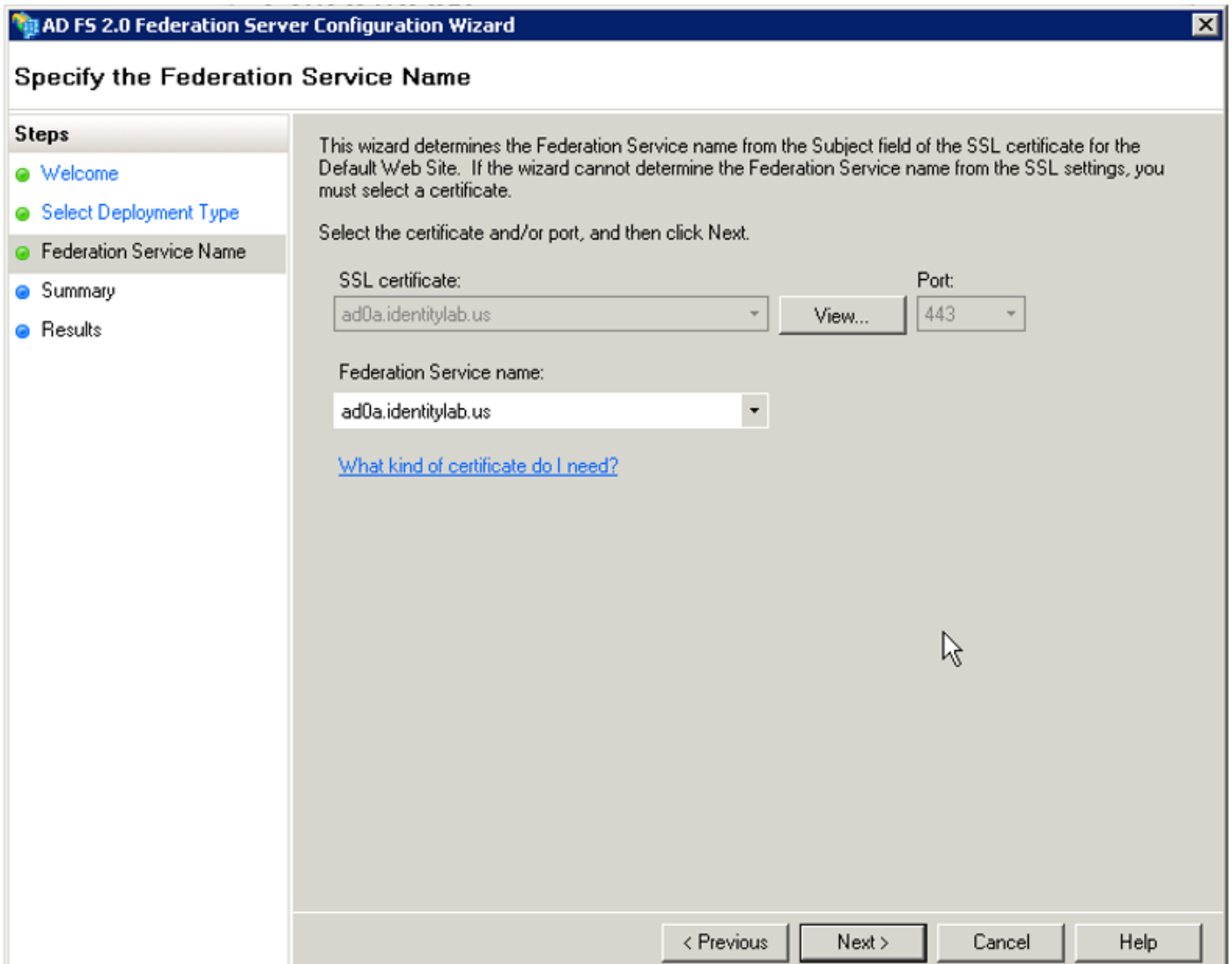
Selecteer de optie **AD FS 3.0 Federation Server Configuration** om de ADFS-serverconfiguratie te starten. Deze screenshots vertegenwoordigen dezelfde stappen in AD FS 3.



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

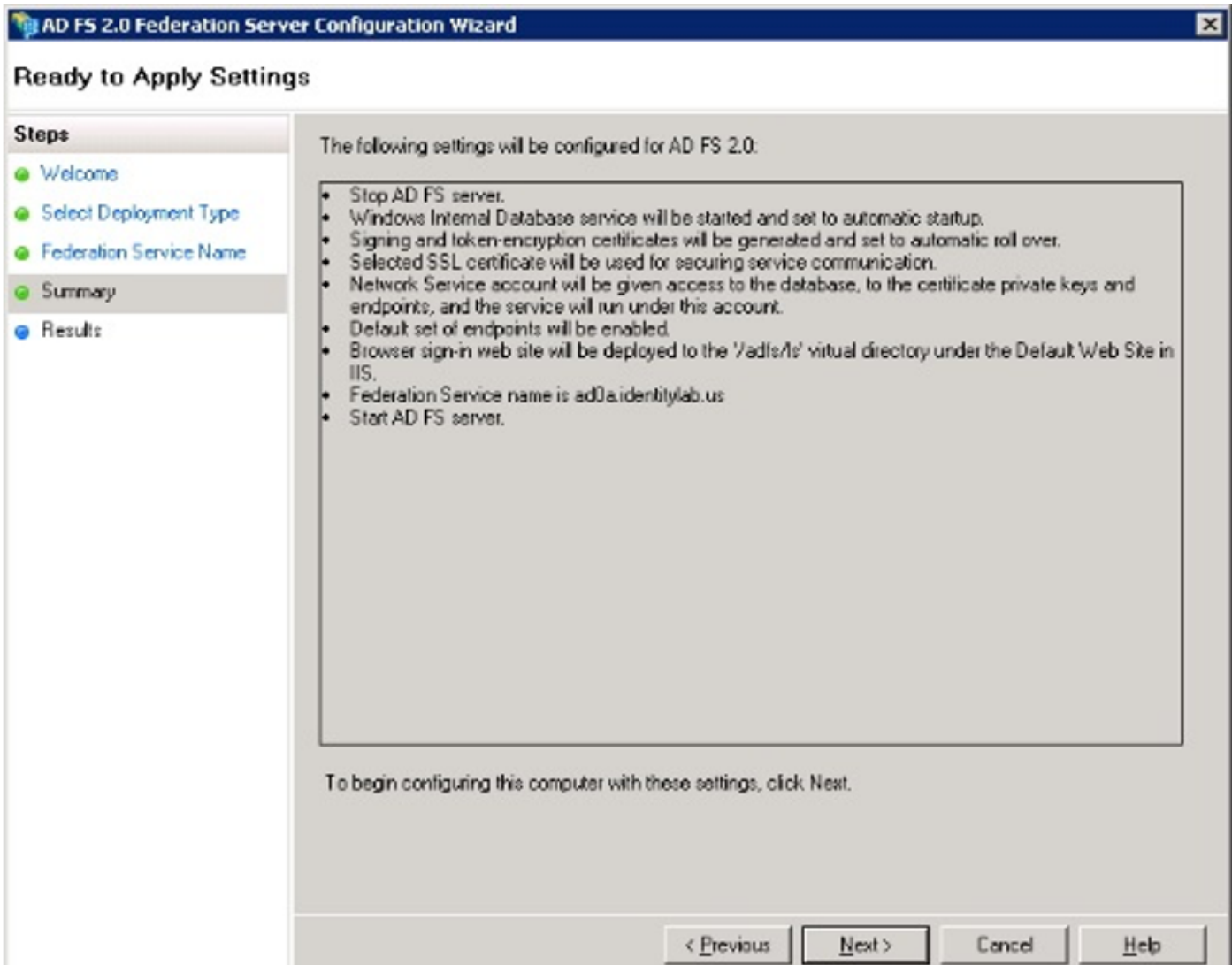


Selecteer een zelfstandige Federatie Server en klik op **Volgende** zoals in de afbeelding.



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





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

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

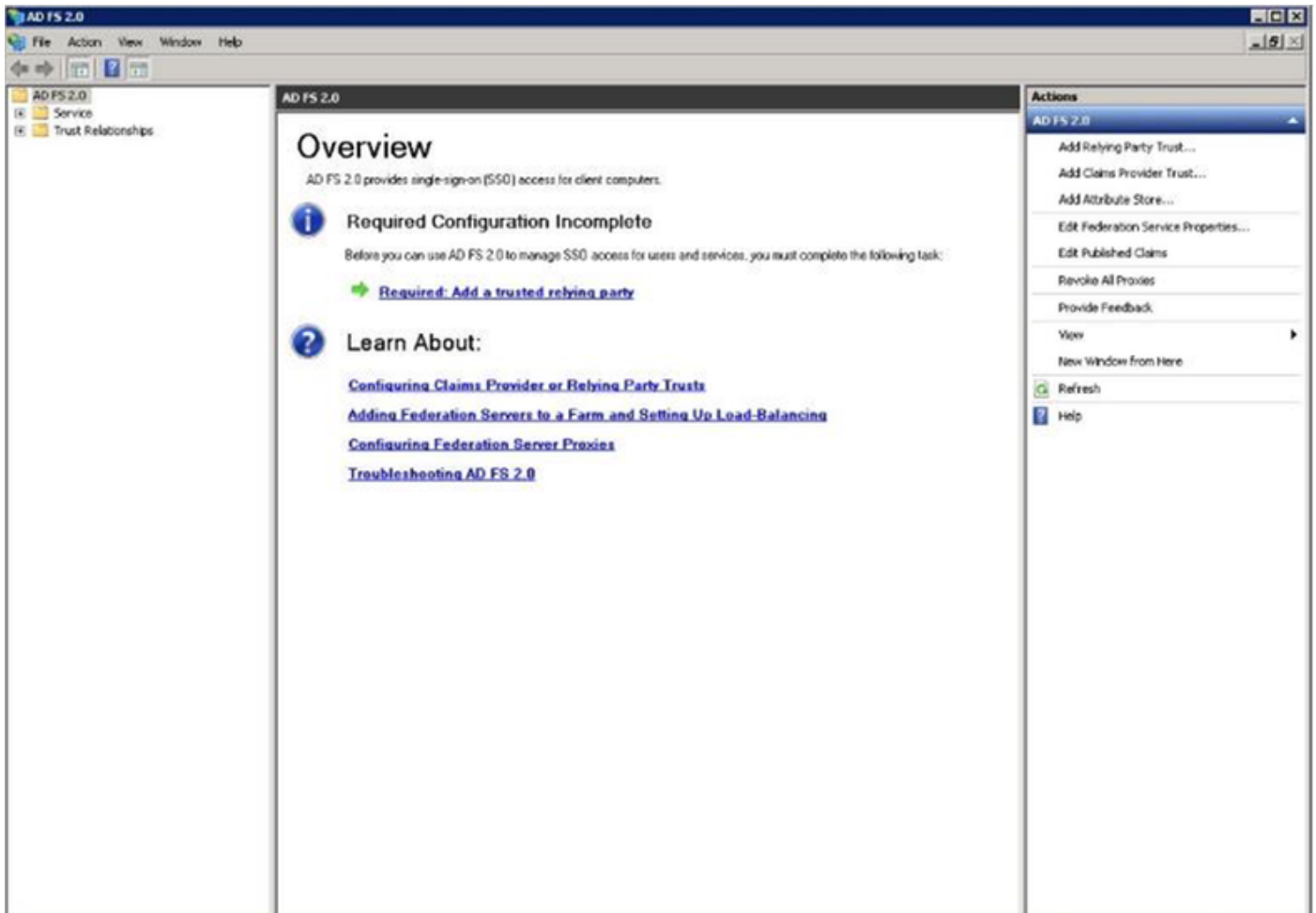
Component	Status
Stop the AD FS 2.0 Windows Service	Configuration finished
Install Windows Internal Database	Configuration finished
Start the Windows Internal Database service	Configuration finished
Create AD FS configuration database	Configuration finished
Configure service settings	Configuration finished
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

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



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

## SSO op CUCM configureren met ADFS

### LDAP-configuratie

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

## 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



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

## 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](#)

Save
Delete
Copy
Perform Full Sync Now
Add New

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

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration Go  
[farfar](#) | [Search Documentation](#) | [About](#) | [Logout](#)

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

**LDAP Authentication**

Save

**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](#)

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

**End 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-metagegevens

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

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

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

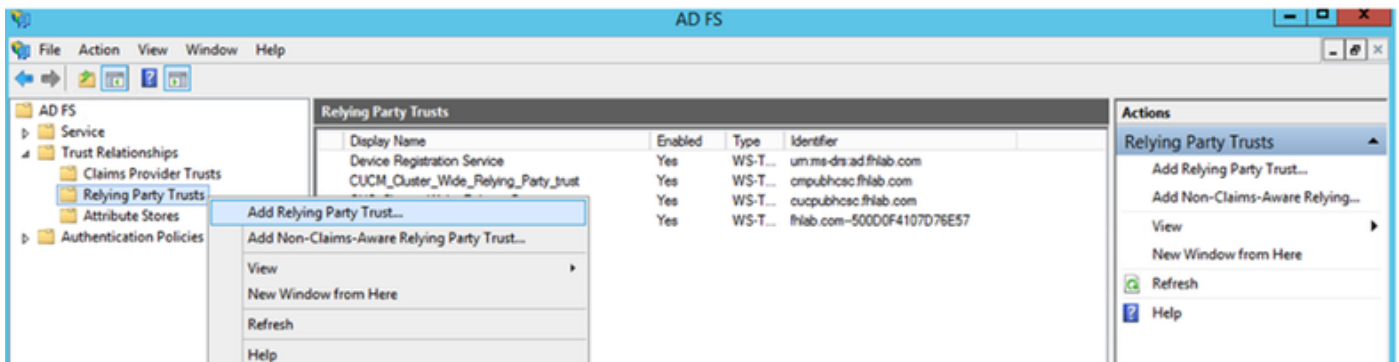
Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
cmpubhcsc.fhlab.com	SAML	N/A	April 20, 2020 2:00:57 PM PDT	<input type="button" value="File"/>	April 18, 2020 8:05:38 PM PDT	Passed - April 20, 2020 2:02:15 PM PDT <input type="button" value="Run SSO Test..."/>
cmsubhcsc.fhlab.com	SAML	<input type="button" value="IDP"/>	April 20, 2020 2:00:57 PM PDT	<input type="button" value="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	<input type="button" value="IDP"/>	April 20, 2020 2:00:57 PM PDT	<input type="button" value="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	<input type="button" value="IDP"/>	April 20, 2020 2:00:57 PM PDT	<input type="button" value="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..."/>

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

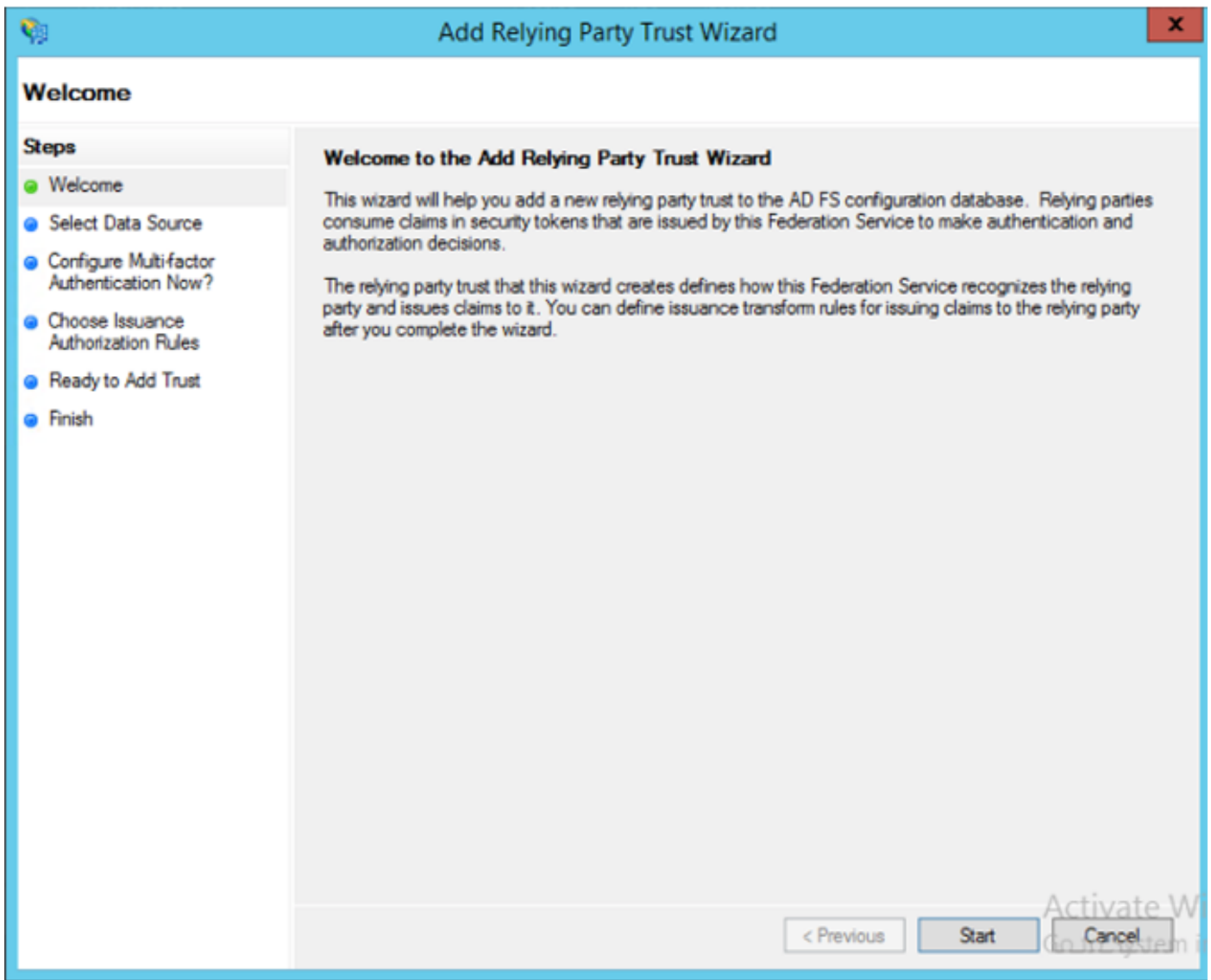
## ADFS-relay configureren

Terug naar de AD FS 3.0 Management console.





Klik op **Add Relying Party Trust Wizard**.



Klik op **Start** om verder te gaan

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

**Add Relying Party Trust Wizard**

### Select Data Source

**Steps**

- Welcome
- Select Data Source
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes 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:

Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

< Previous    Next >    Cancel

Gebruik `CUCM_Cluster_Wide_Relying_Party_trust` als de naam van de weergave en klik op **Volgende**.

**Add Relying Party Trust Wizard**

### Specify Display Name

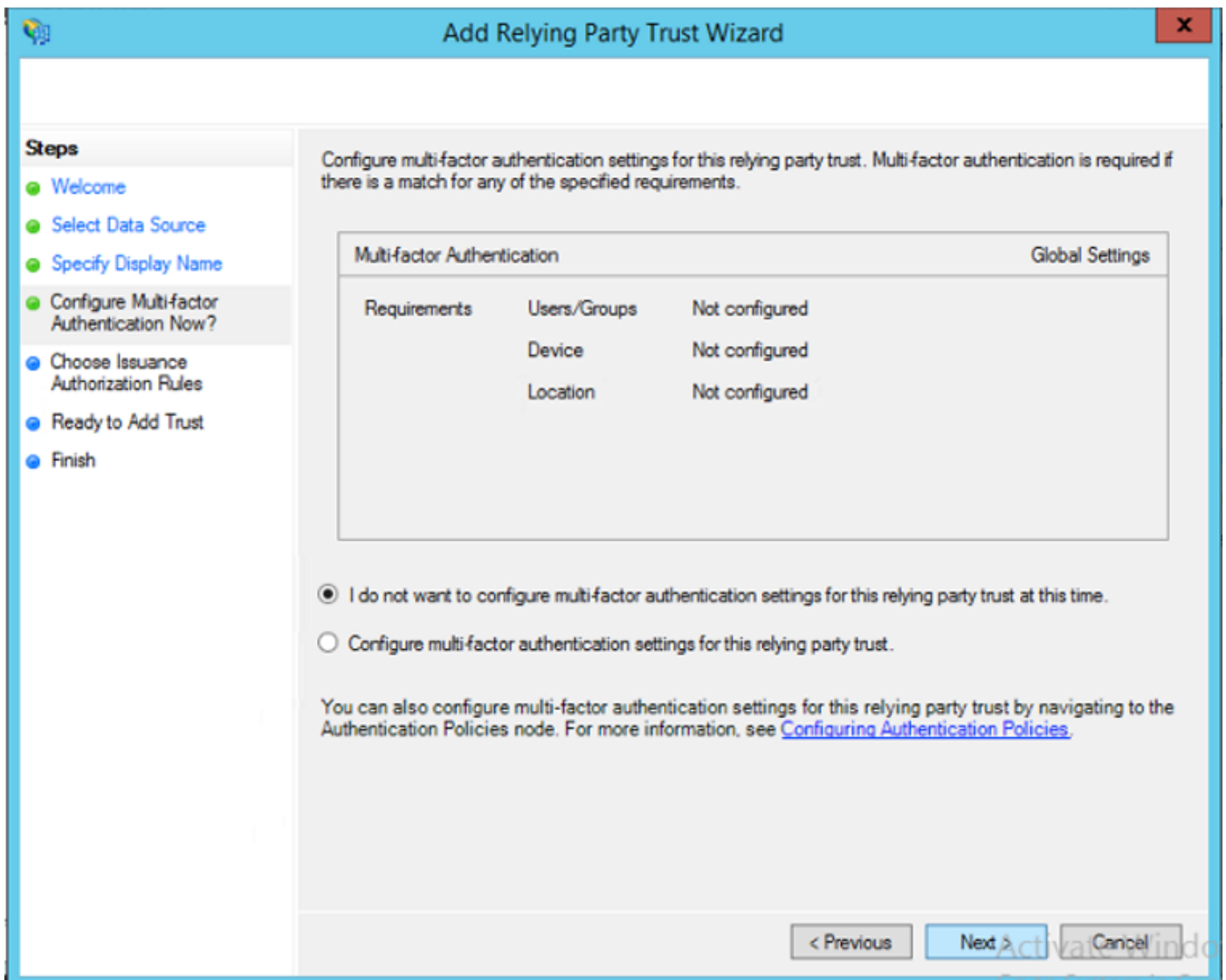
Enter the display name and any optional notes for this relying party.

Display name:

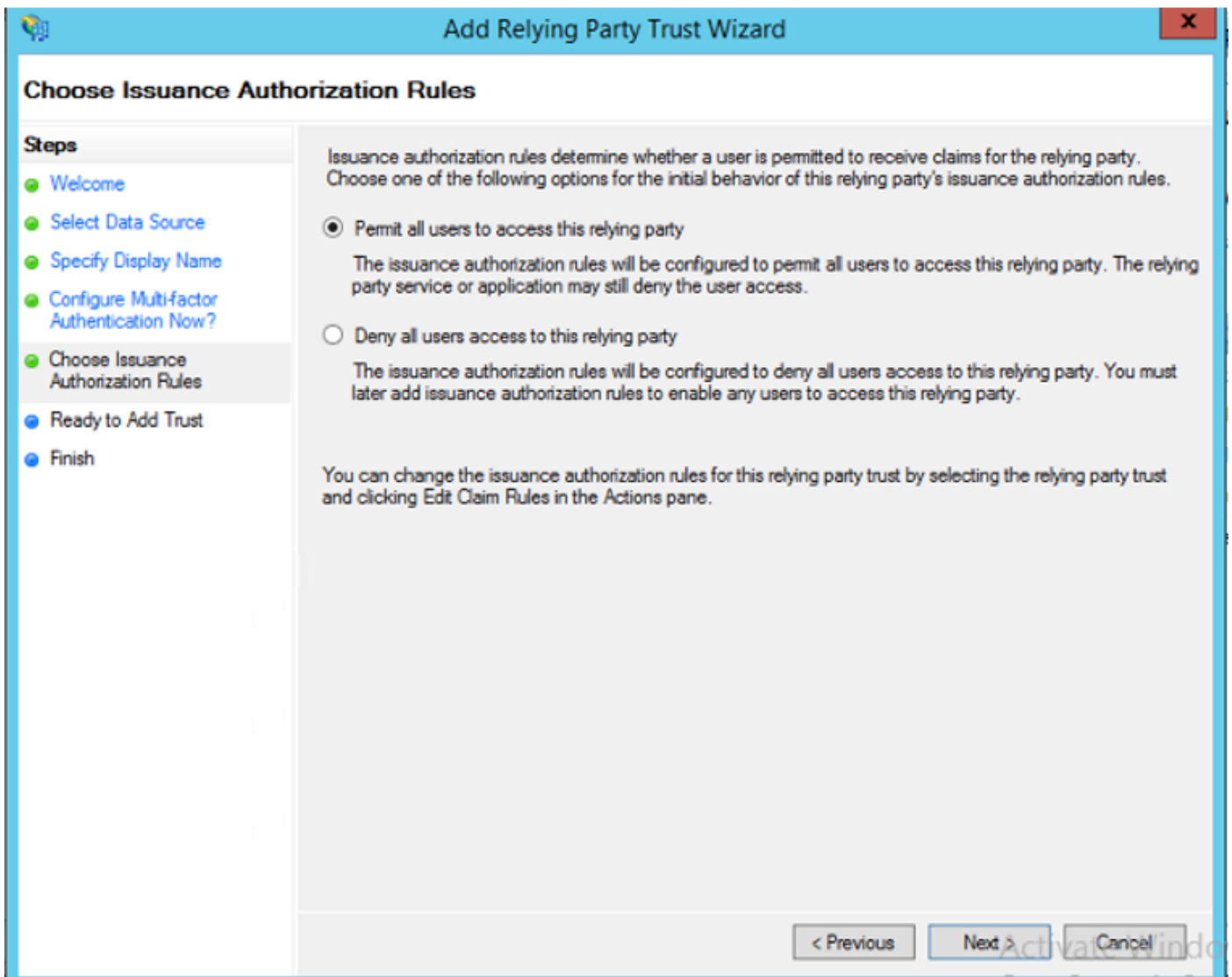
Notes:

< Previous   Next >   Cancel

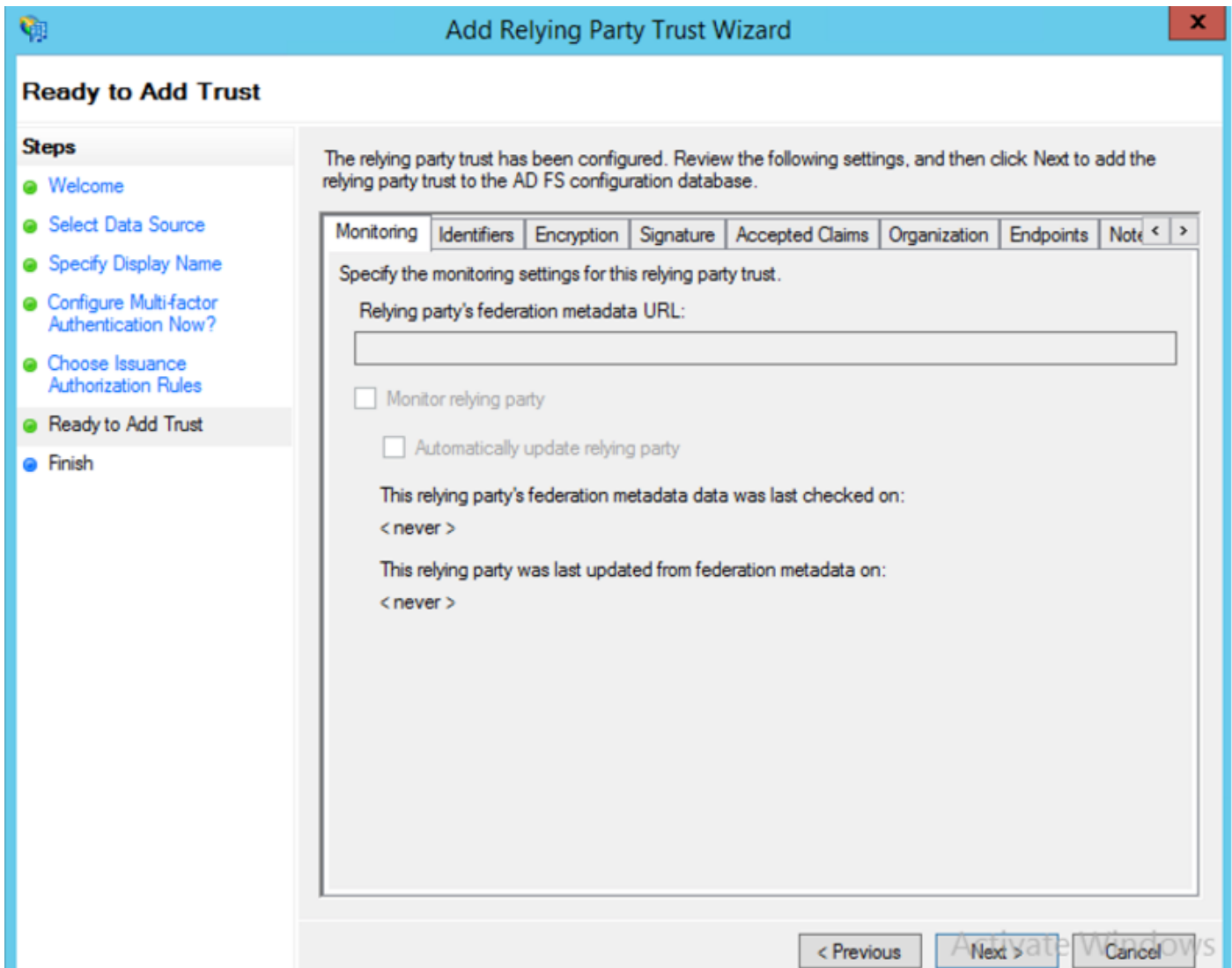
Selecteer de eerste optie en klik op **Volgende**.



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

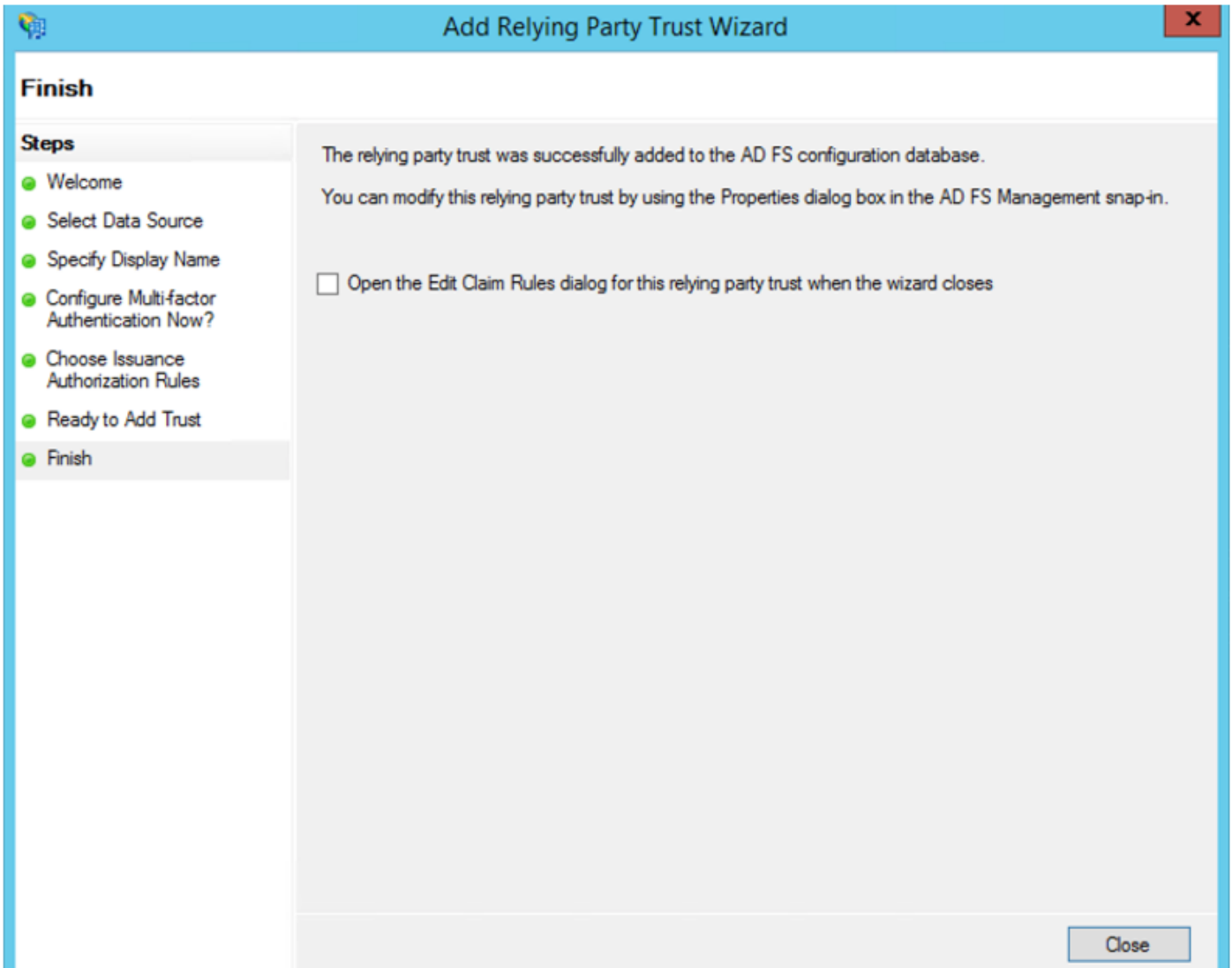


Bekijk de configuratie en klik op **Volgende** zoals in de afbeelding.

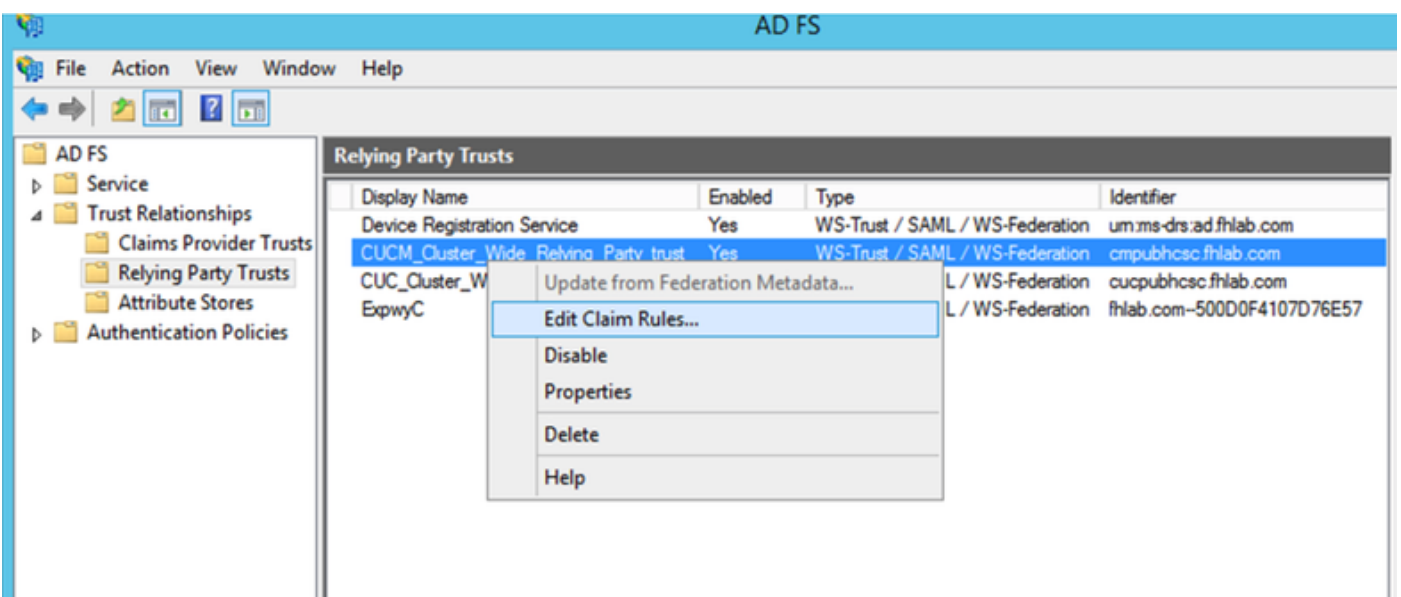


Schakel het vakje uit en klik op **Sluiten**.

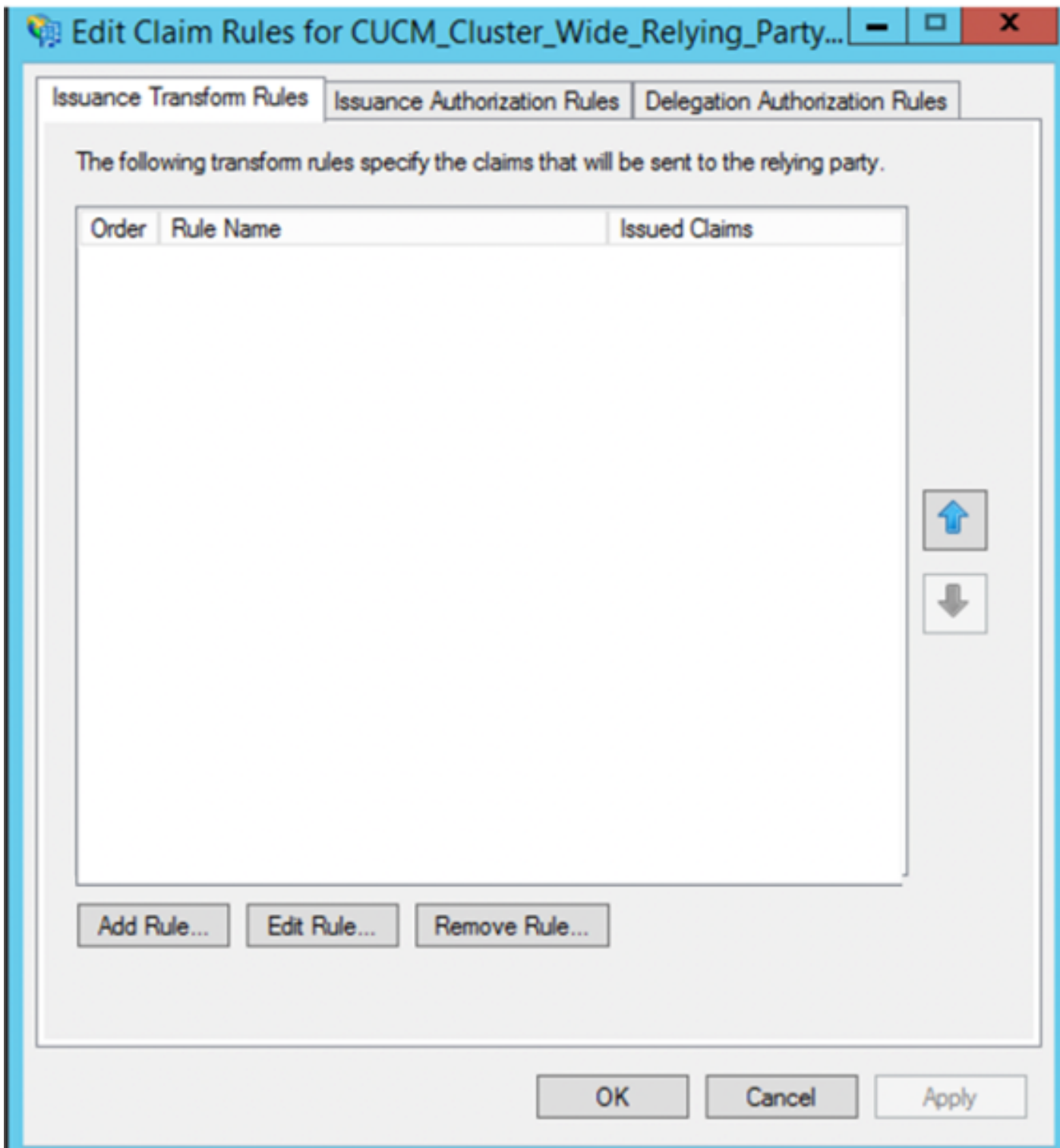




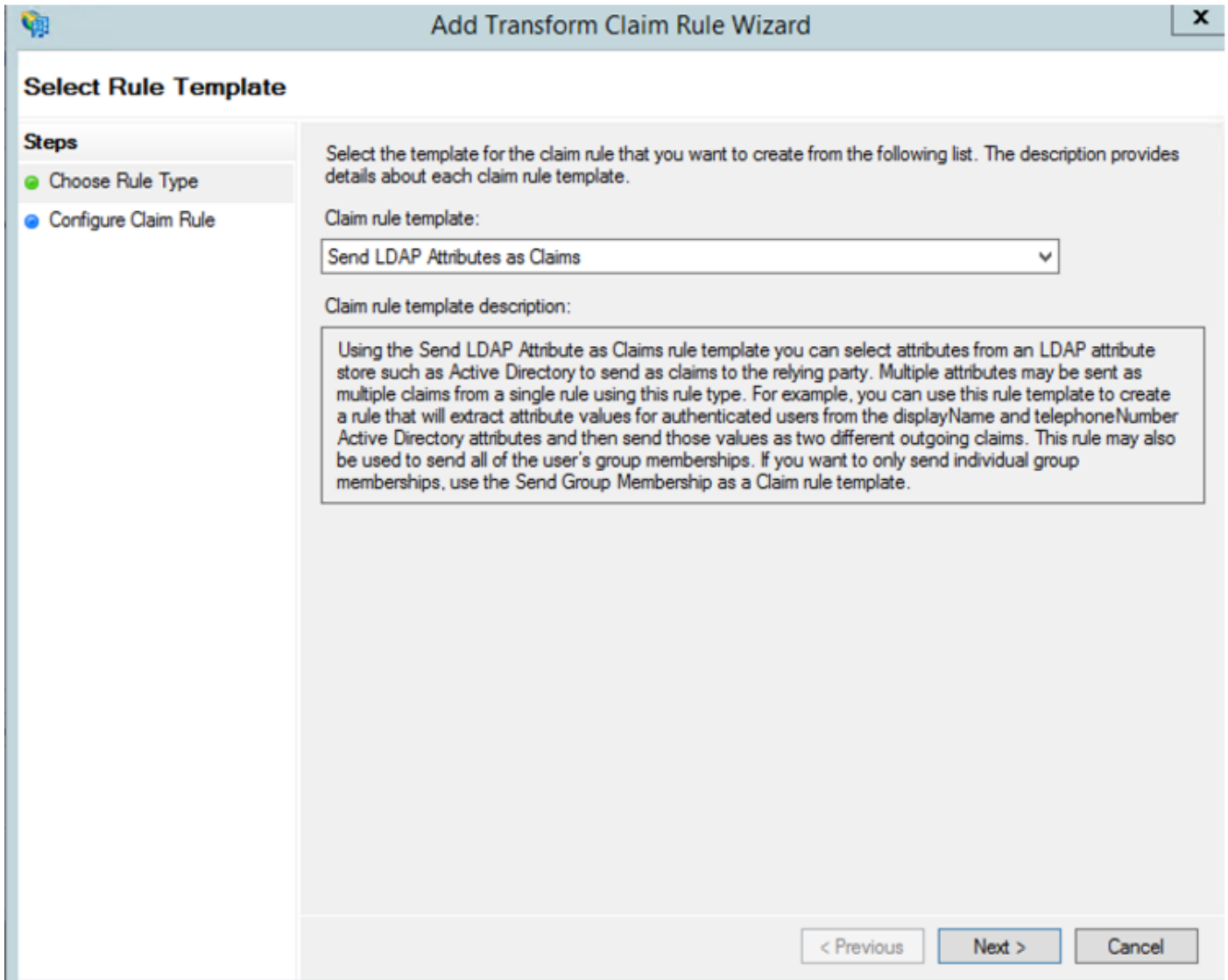
Selecteer met de knop secundaire muis het **vertrouwen** van de **Relying Party** dat u in de afbeelding hebt gemaakt en **bewerkt de configuratie Eisen** voor de **claim** zoals weergegeven in de afbeelding.



Klik op **Regel toevoegen** zoals in de afbeelding weergegeven.



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



Configuratie van deze parameters:

Naam claimregel: NaamID

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

LDAP-kenmerk: SAM-accountnaam

Type vordering: uid

Klik op **FINISH/OK** om verder te gaan.

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

**Edit Rule - 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:

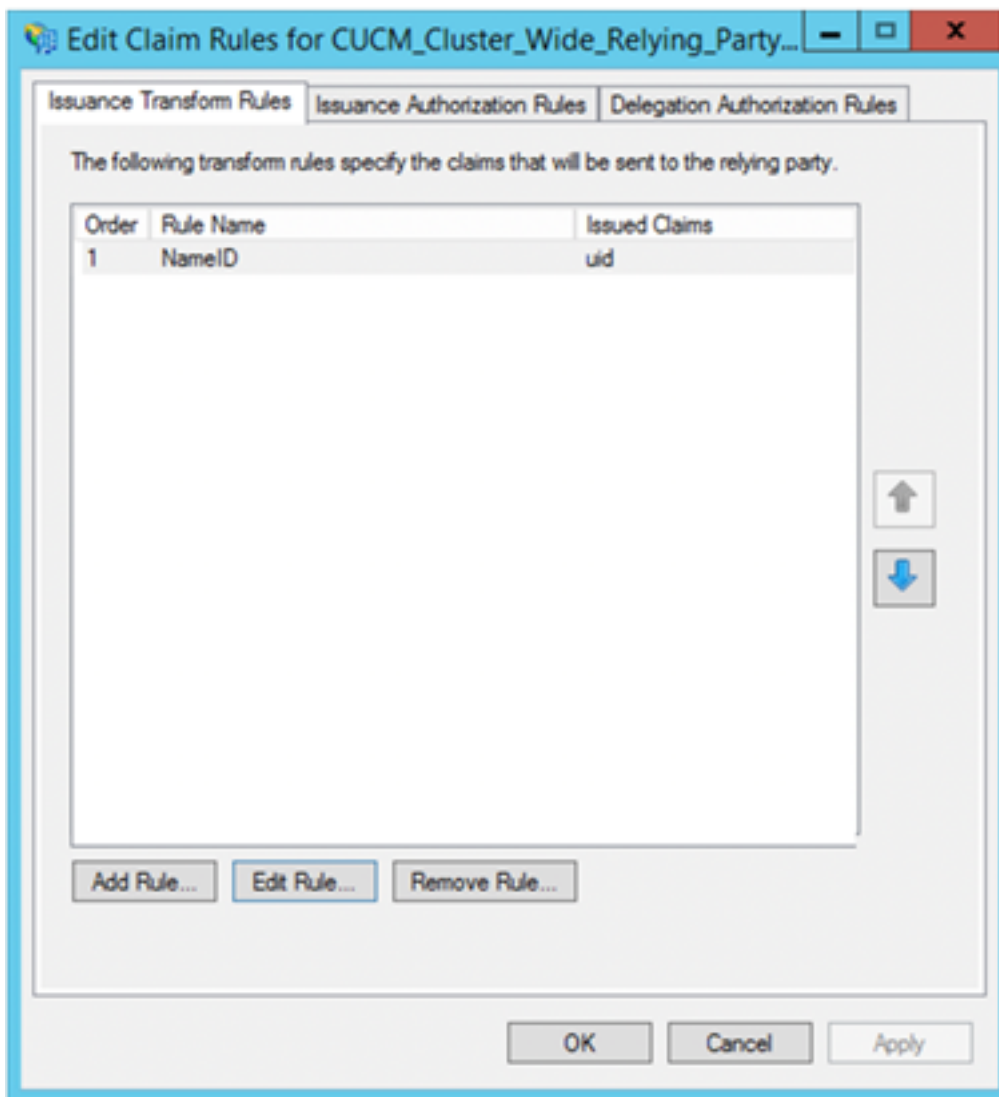
Rule template: Send LDAP Attributes as Claims

Attribute store:

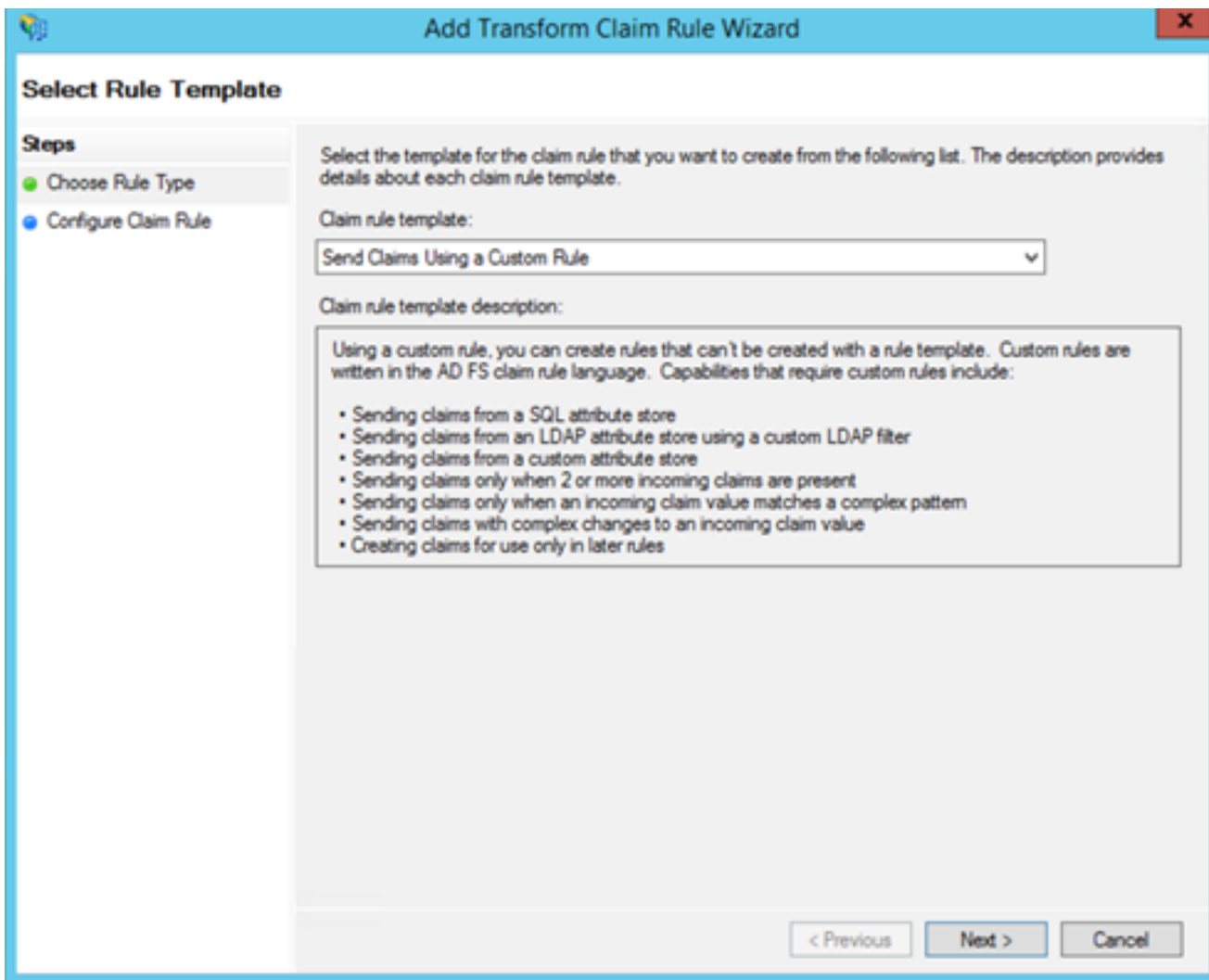
Mapping of LDAP attributes to outgoing claim types:

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

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



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



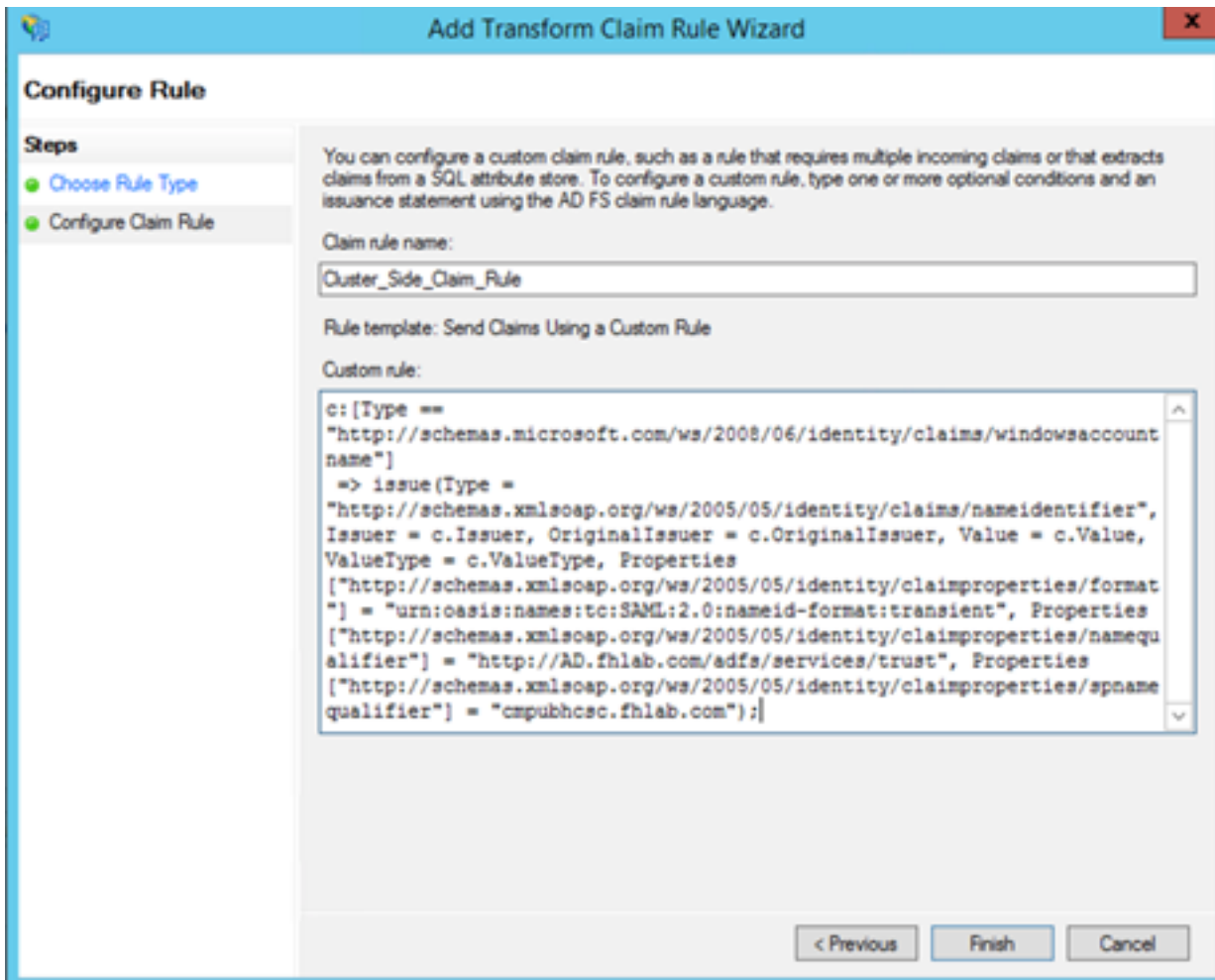
Maak een aangepaste regel genaamd Cluster\_Side\_Claim\_Rule.

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

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> 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>");

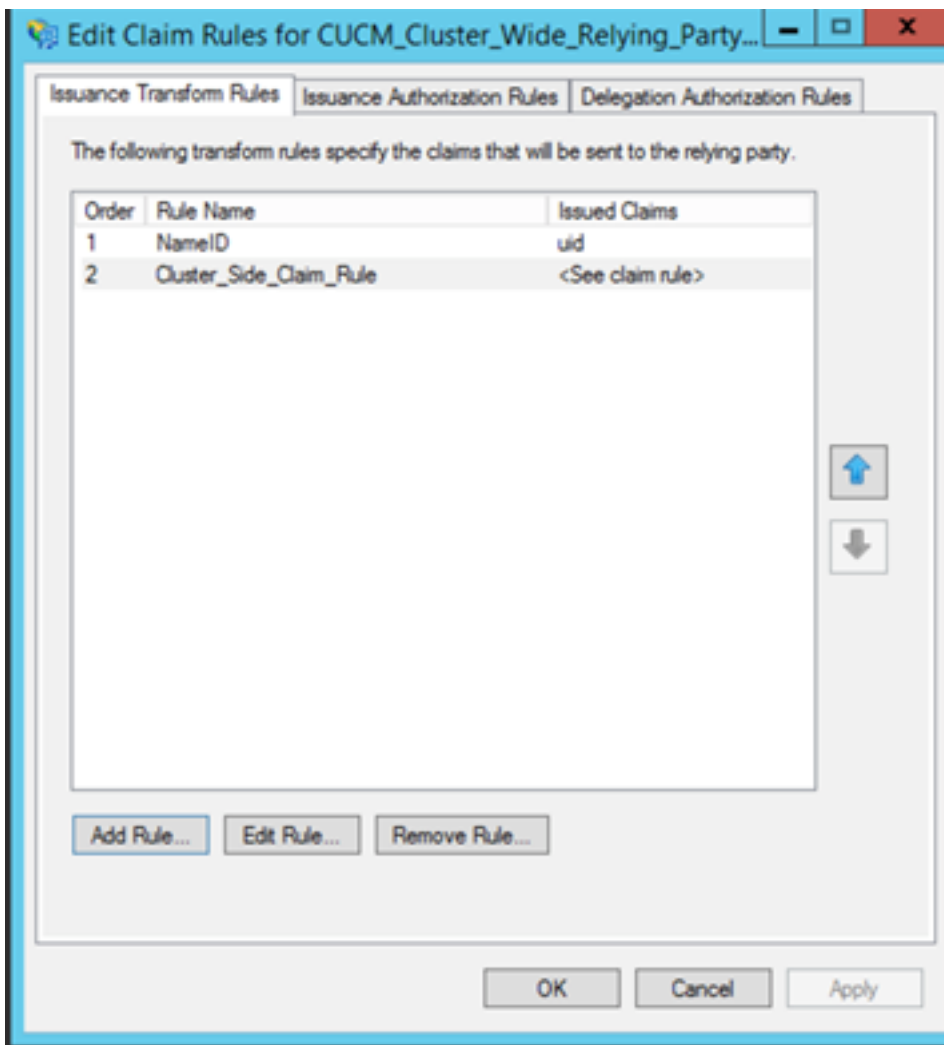
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"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");
```

Klik op **Voltoeien** om verder te gaan.

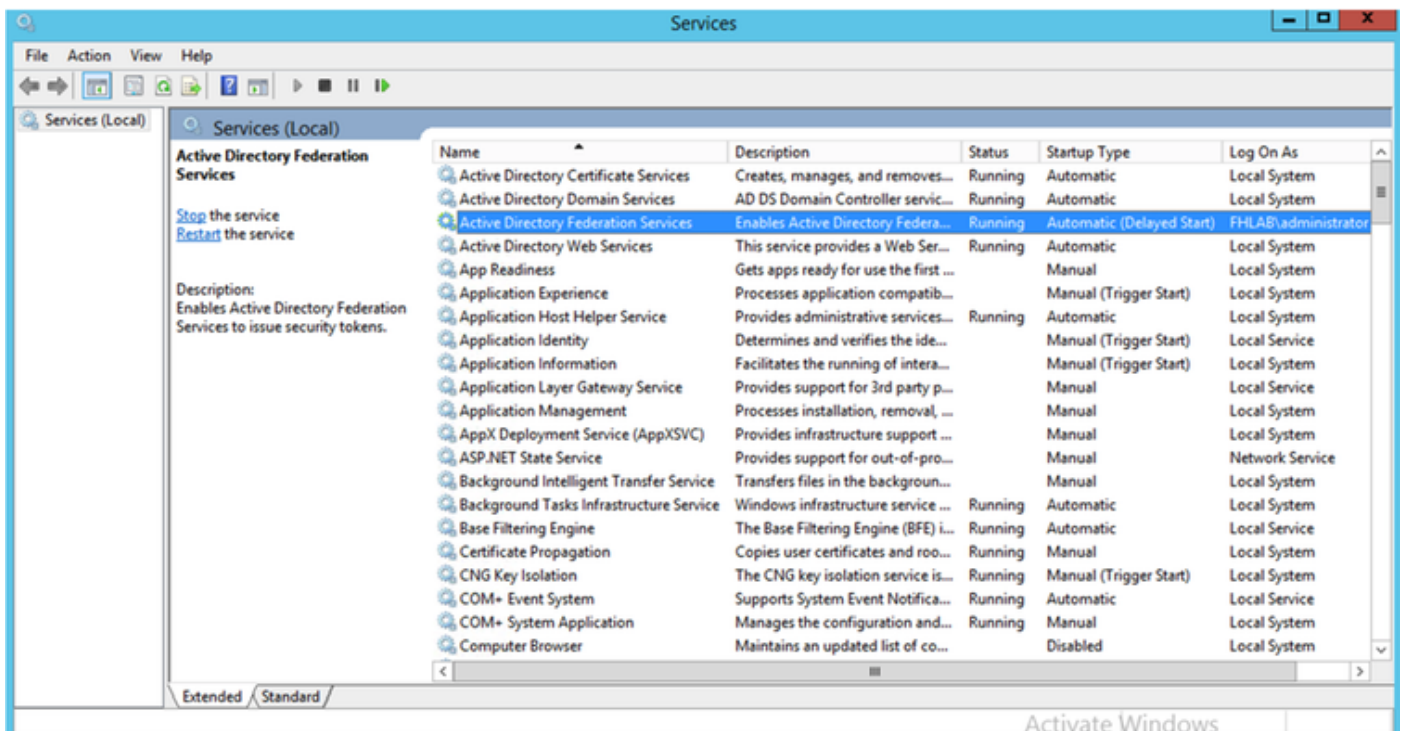


U dient nu twee regels te hebben die zijn gedefinieerd als ADFS. Klik op **Toepassen** en **OK** om het regelvenster te sluiten.





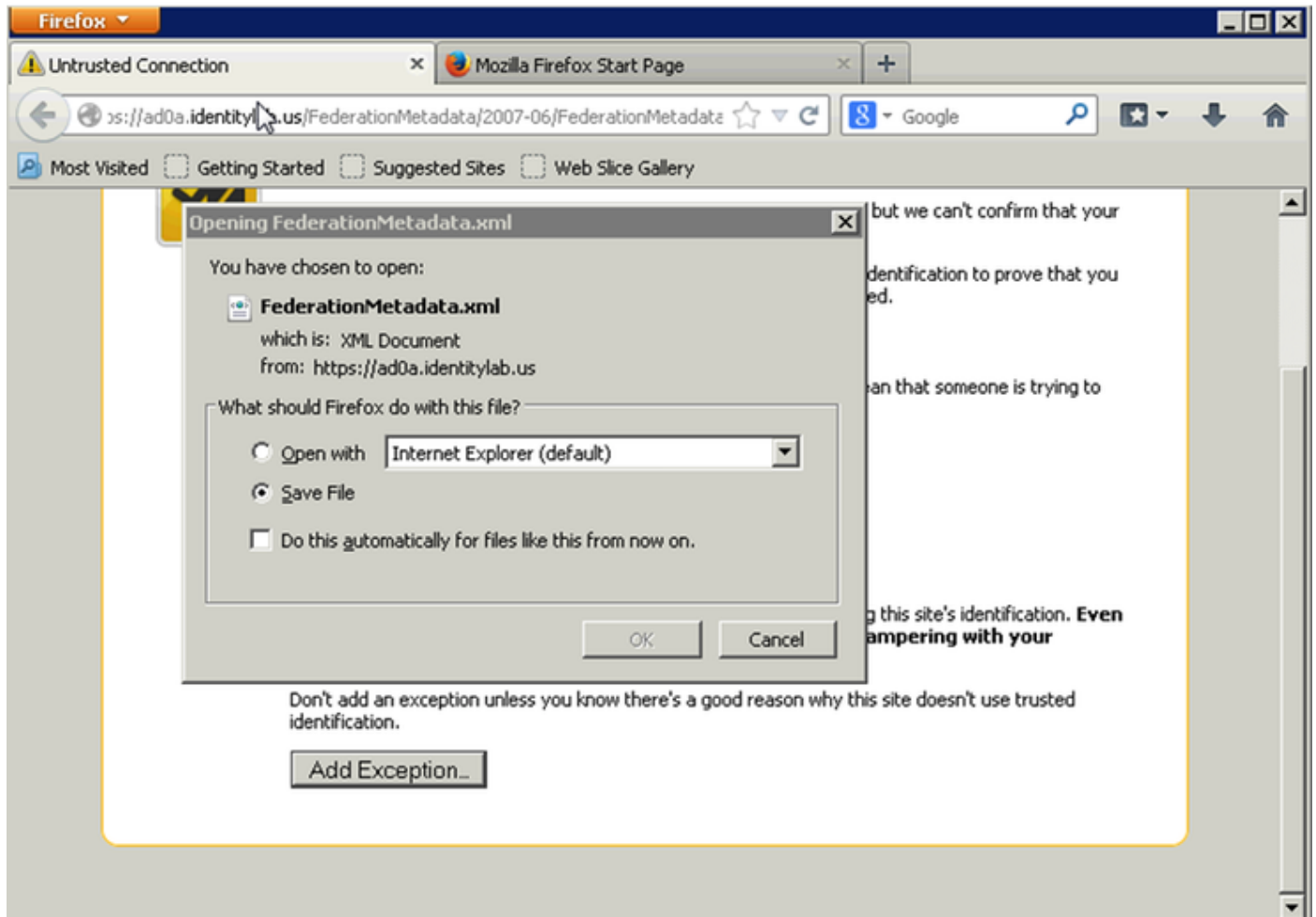
CUCM wordt nu toegevoegd als een betrouwbare vertrouwende partij bij ADFS.



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

## IDP-metagegevens

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



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

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

The screenshot shows the Cisco Unified CM Administration web interface. The navigation menu is open, displaying a list of categories. The 'SAML Single Sign-On' option is highlighted. The main content area shows a search filter for 'Manager Group' with a dropdown set to 'begins with' and a 'Find' button. The URL in the address bar is <https://cmubhsc.fhlab.com:8443/ccadmin/ccmGroup>.

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

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...

Selecteer **SAML SSO inschakelen**.

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

Reset Warning - Mozilla Firefox

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

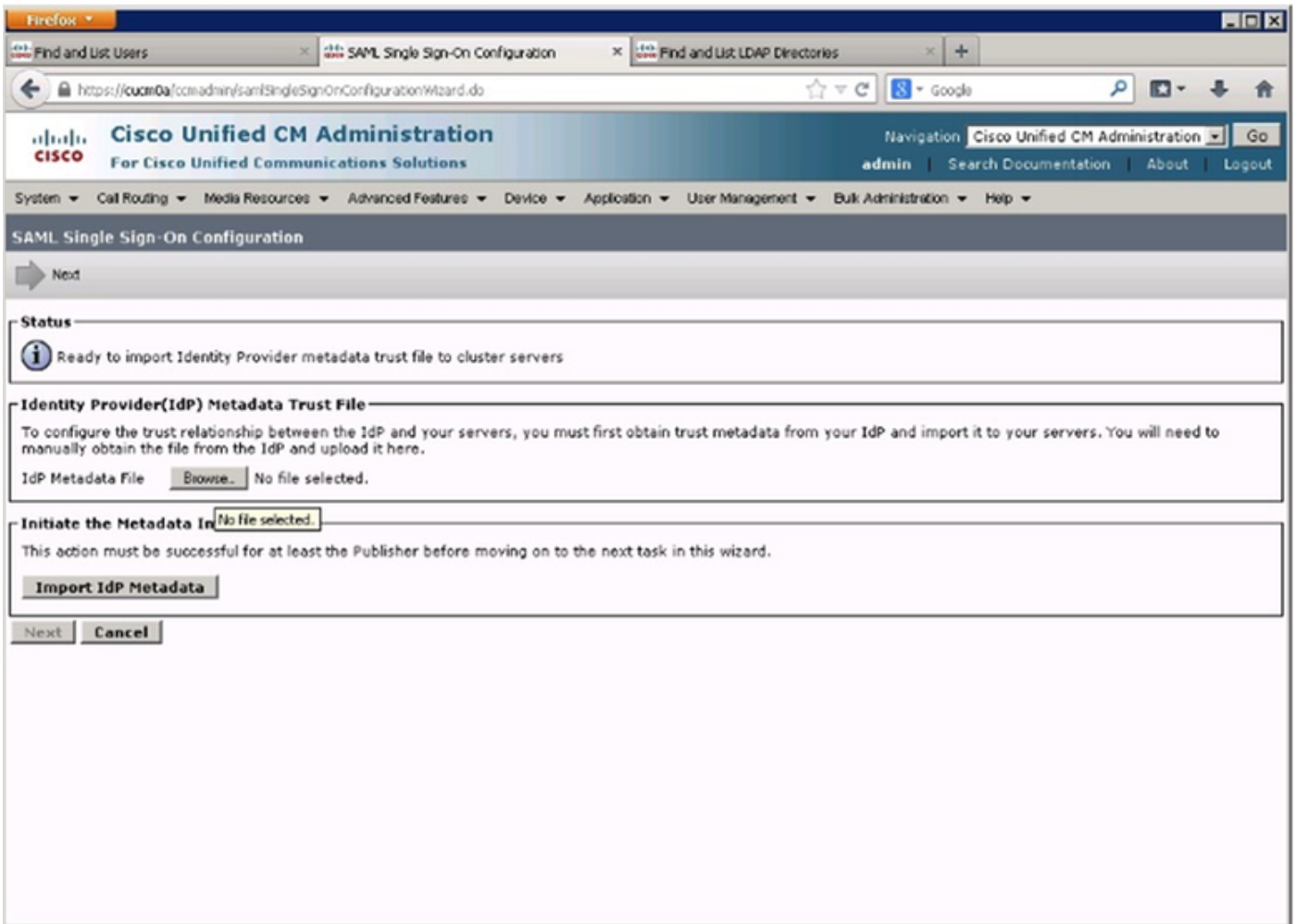
 **Web server connections will be restarted**

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.

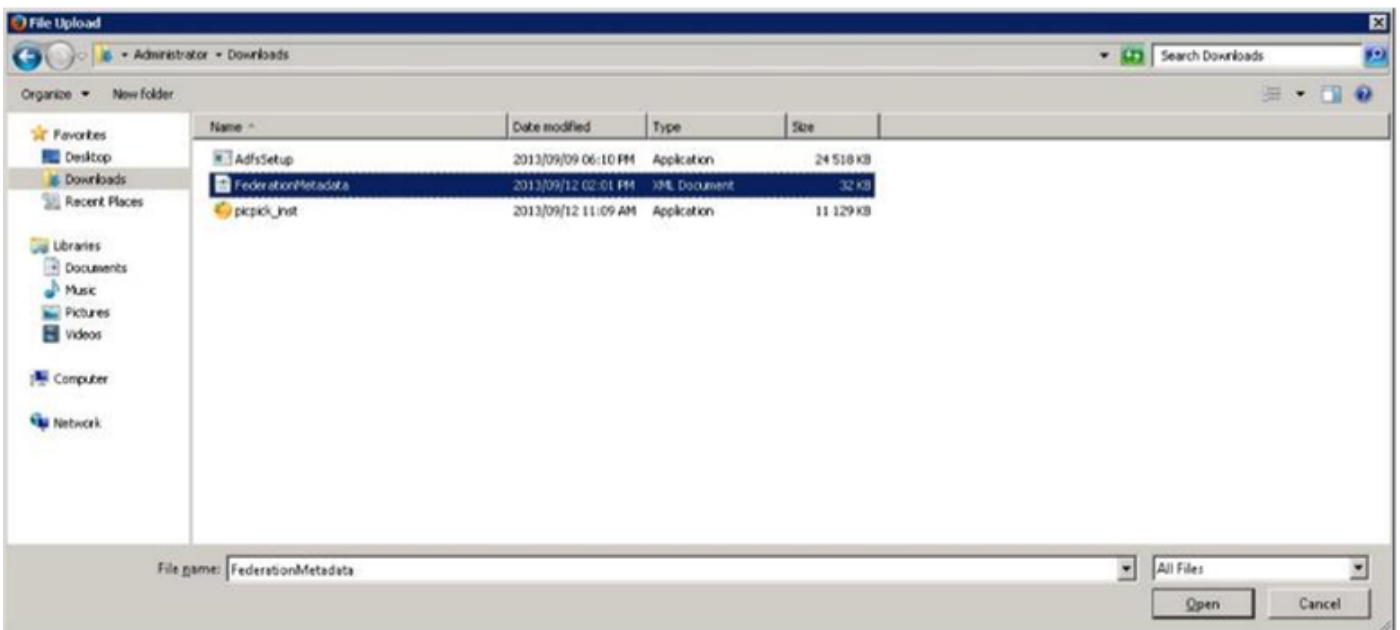
Continue Cancel

Op het SSO-scherm en klik op **Bladeren..** om het XML-bestand met de metagegevens

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



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



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


SAML Single Sign-On Configuration - Windows Internet Explorer

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

**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

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



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

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

Sign In - Mozilla Firefox

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

# FS

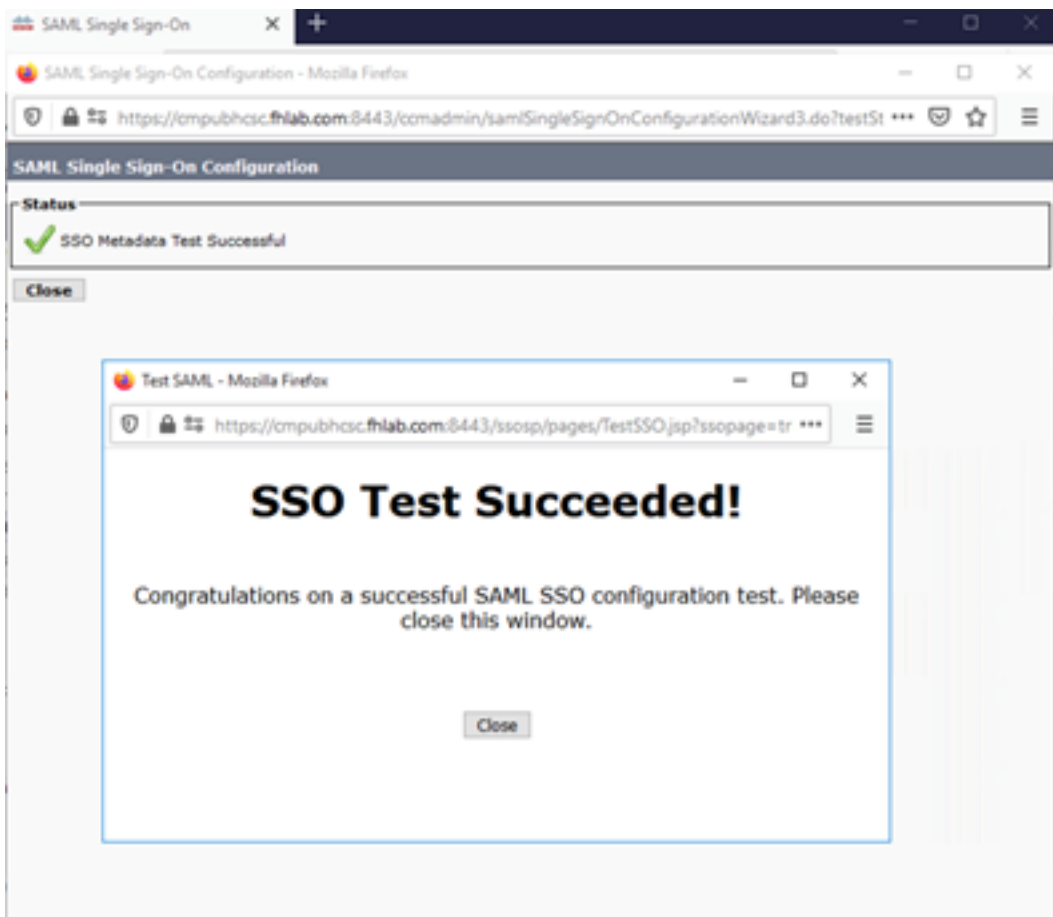
Sign in with your organizational account

farfar@fhlab.com

.....

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





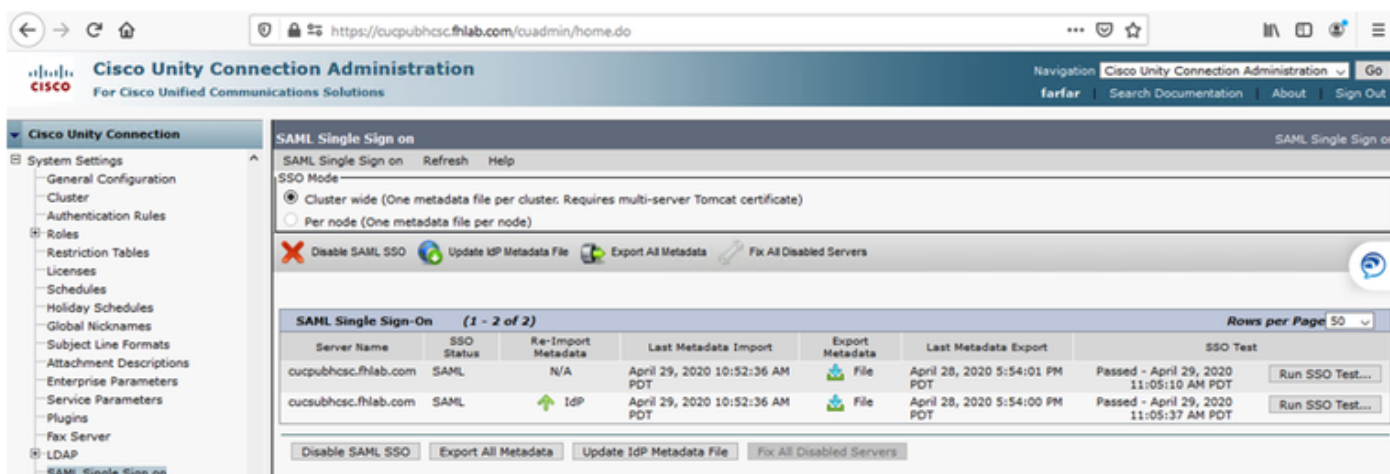
Klik op SLUITEN en Voltoeien om verder te gaan.

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

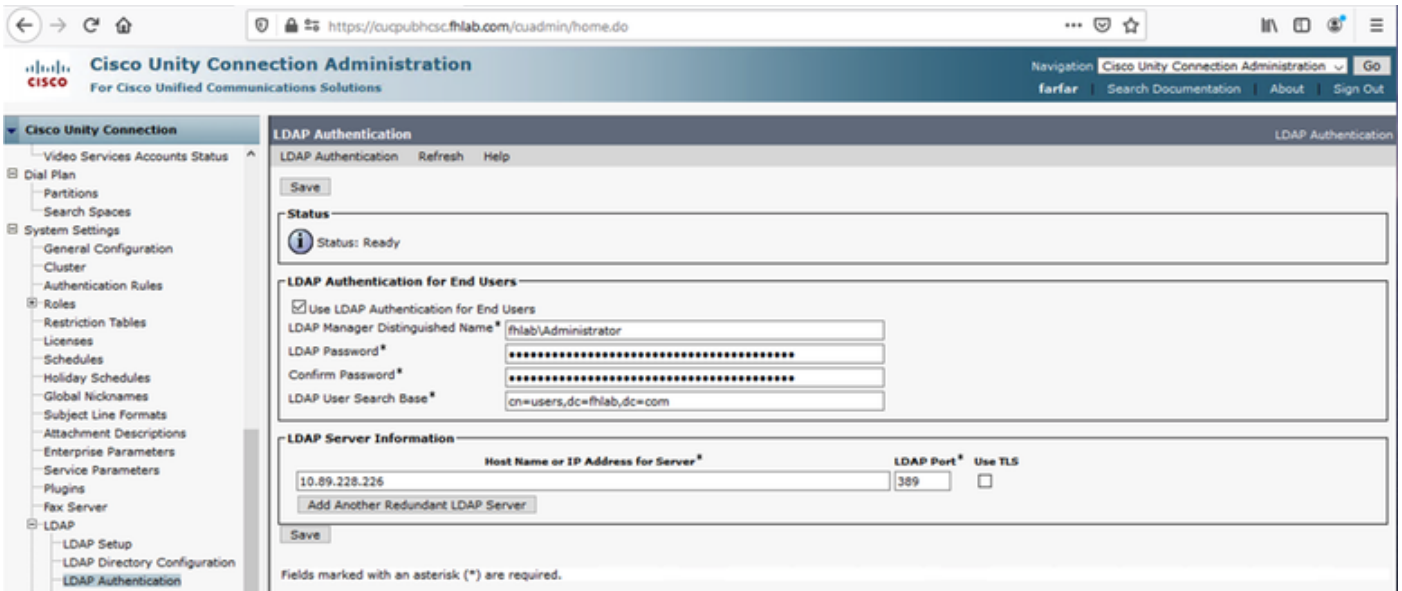
## SSO op CUC configureren

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

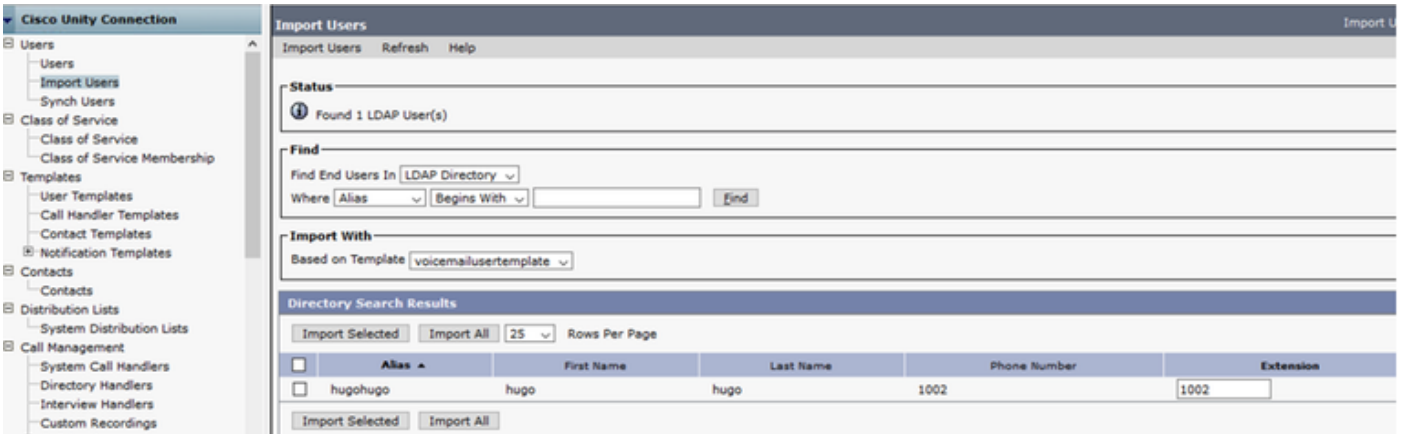
LDAP integratie met CUC.



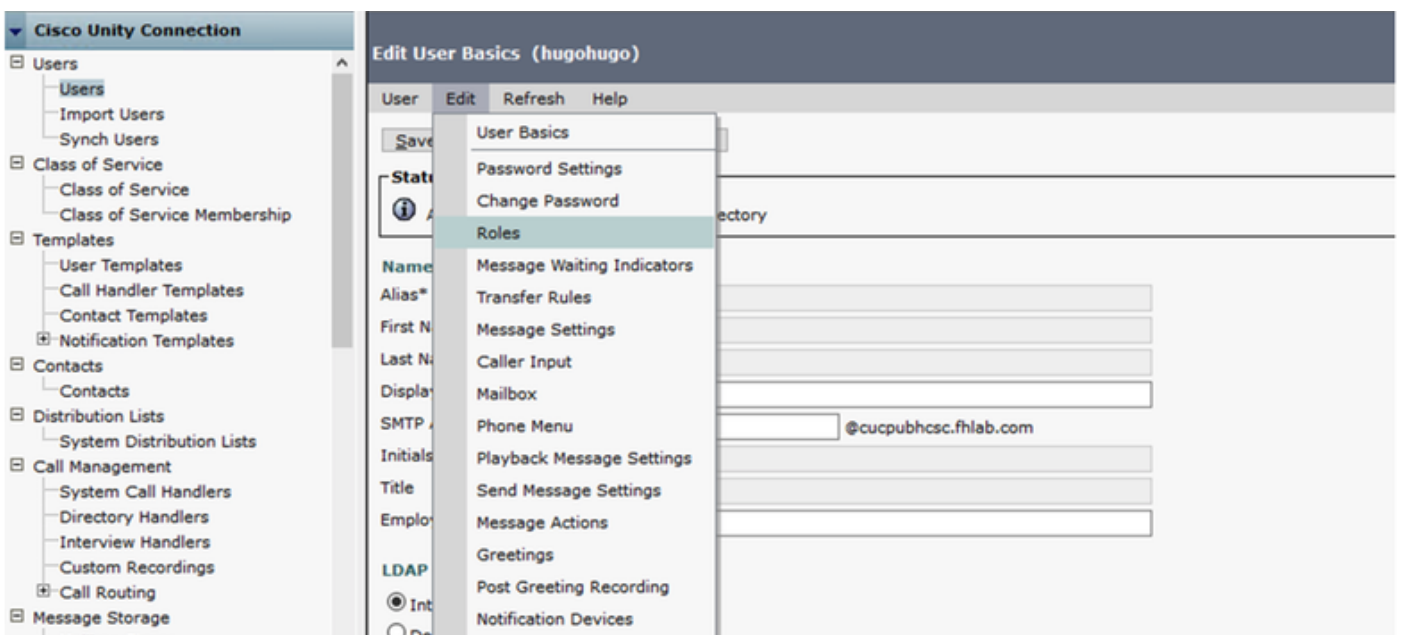
Configuratie van LBP-verificatie.



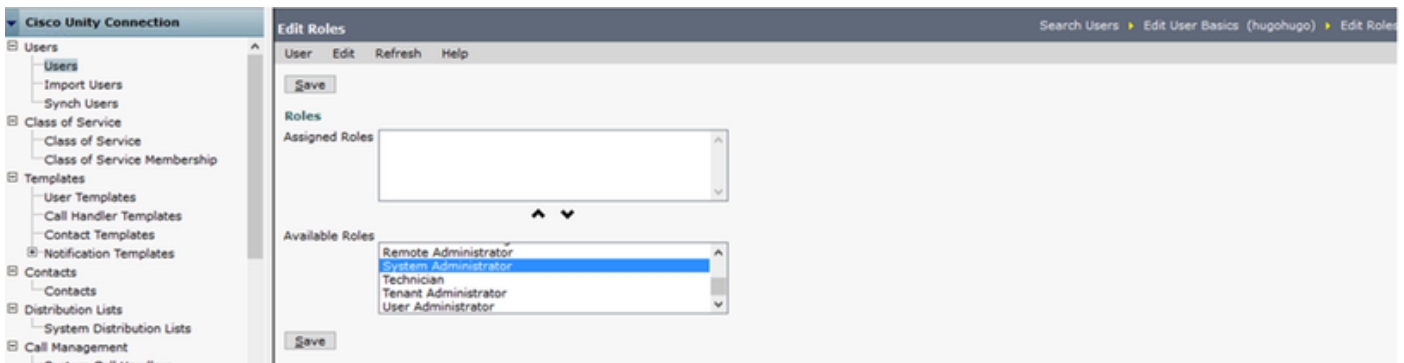
Importeer de gebruikers van LDAP die voicemail hebben toegewezen en ook de gebruiker die zal dienen voor het testen van SSO.



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

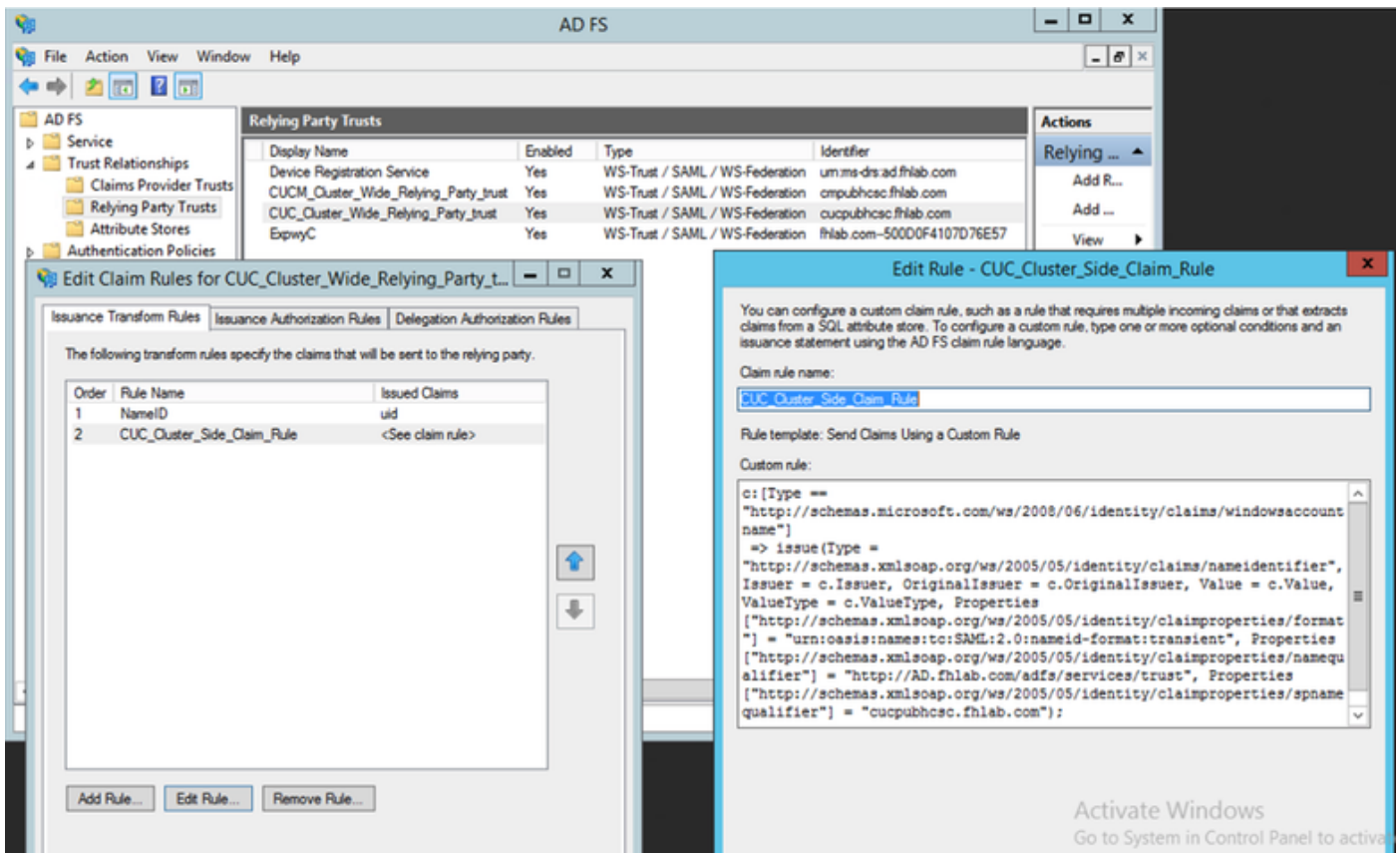


De testgebruiker de rol van systeembeheerder toewijzen.



## CUC-metagegevens

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



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

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 <b>Run SSO Test...</b>
File	April 28, 2020 5:54:00 PM PDT	Passed - April 29, 2020 11:05:37 AM PDT <b>Run SSO Test...</b>

Servers

## SSO op snelweg configureren

### Metagegevens invoeren in snelweg C

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

Upload naar **Configuration > Unified Communications > IDP.**

## Uitvoermetagegevens uit snelweg C

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

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

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

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

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

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

The screenshot displays the configuration interface for adding a claim rule. The main window is titled 'Edit Claim Rules for ExpywC' and shows a table of transform rules:

Order	Rule Name	Issued Claims
1	NameID	uid

The 'Edit Rule - NameID' sub-dialog is open, showing the following configuration:

- Claim rule name: NameID
- Rule template: Send LDAP Attributes as Claims
- Attribute store: Active Directory
- 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
*	

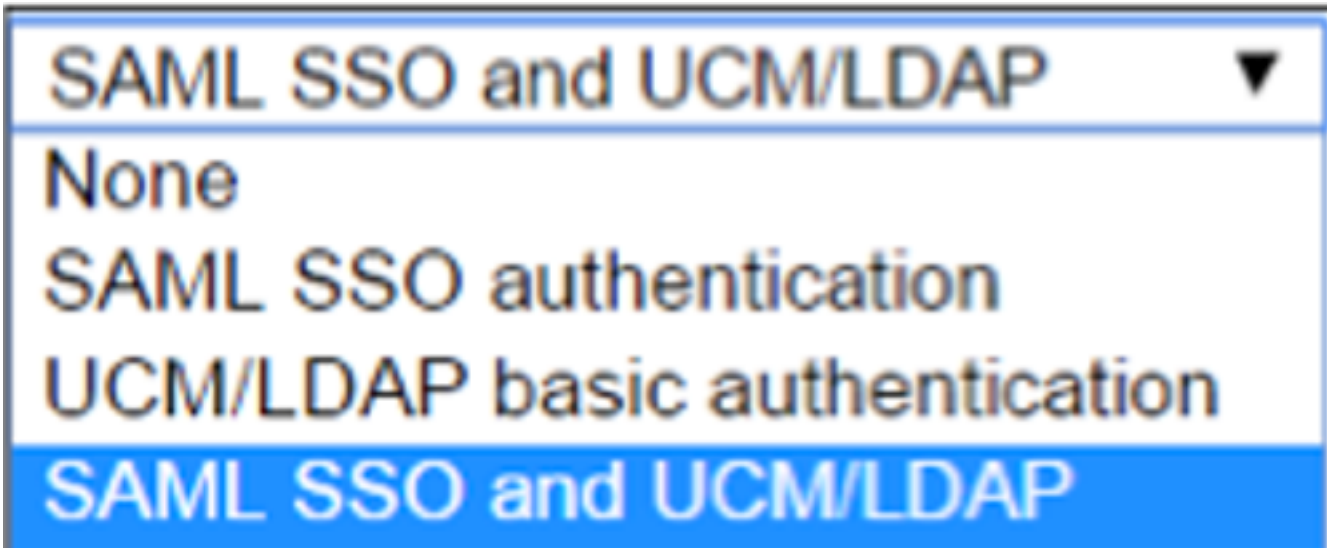
## Handmatig met inloggen verversen

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



SSO and OAuth Configuration		
<a href="#">OAuth Token Expiry Timer (minutes) *</a>	60	60
<a href="#">OAuth Refresh Token Expiry Timer (days) *</a>	60	60
<a href="#">Redirect URIs for Third Party SSO Client</a>		
<a href="#">SSO Login Behavior for iOS *</a>	Use embedded browser (WebView)	Use embedded browser (WebView)
<a href="#">OAuth with Refresh Login Flow *</a>	Enabled	Disabled
<a href="#">Use SSO for RTMT *</a>	True	True

## Verificatiepad



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

## SSO-architectuur

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

## Login-flow op locatie

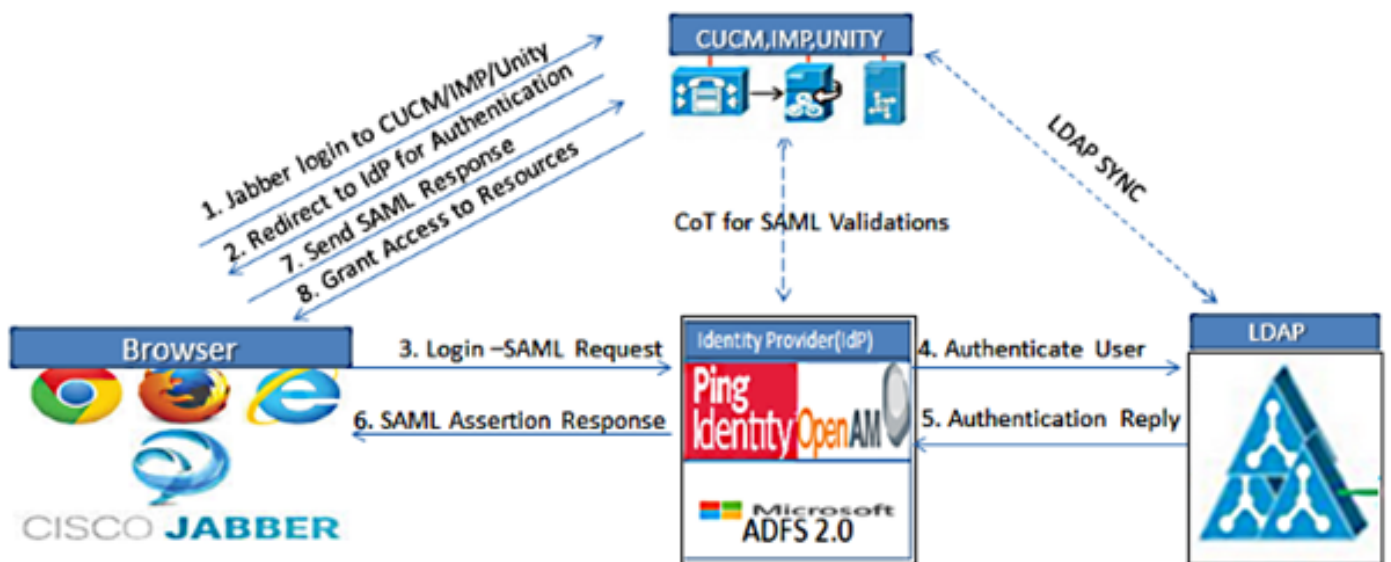
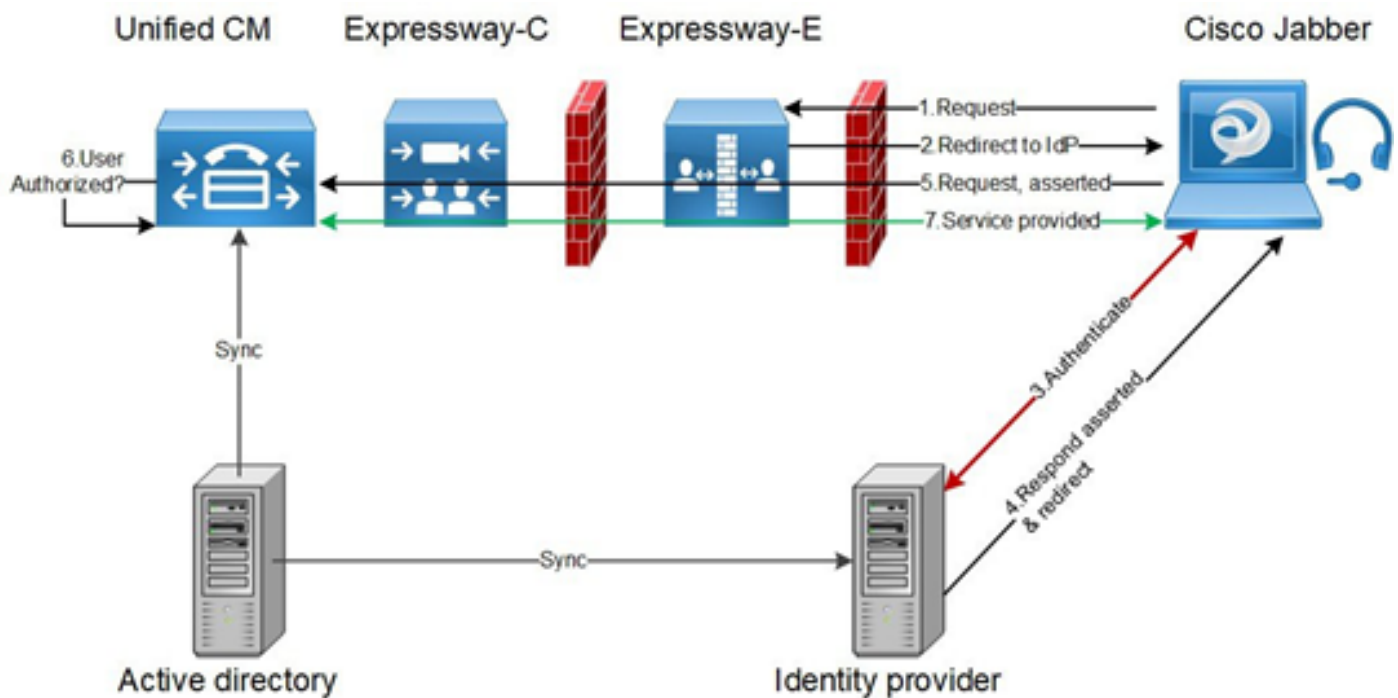


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

## MRA-Login Flow



## OAuth

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



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

## **Toegang/verfrissing Token**

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

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

## **Goedkeuringscode Subsidie Flow beter**

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

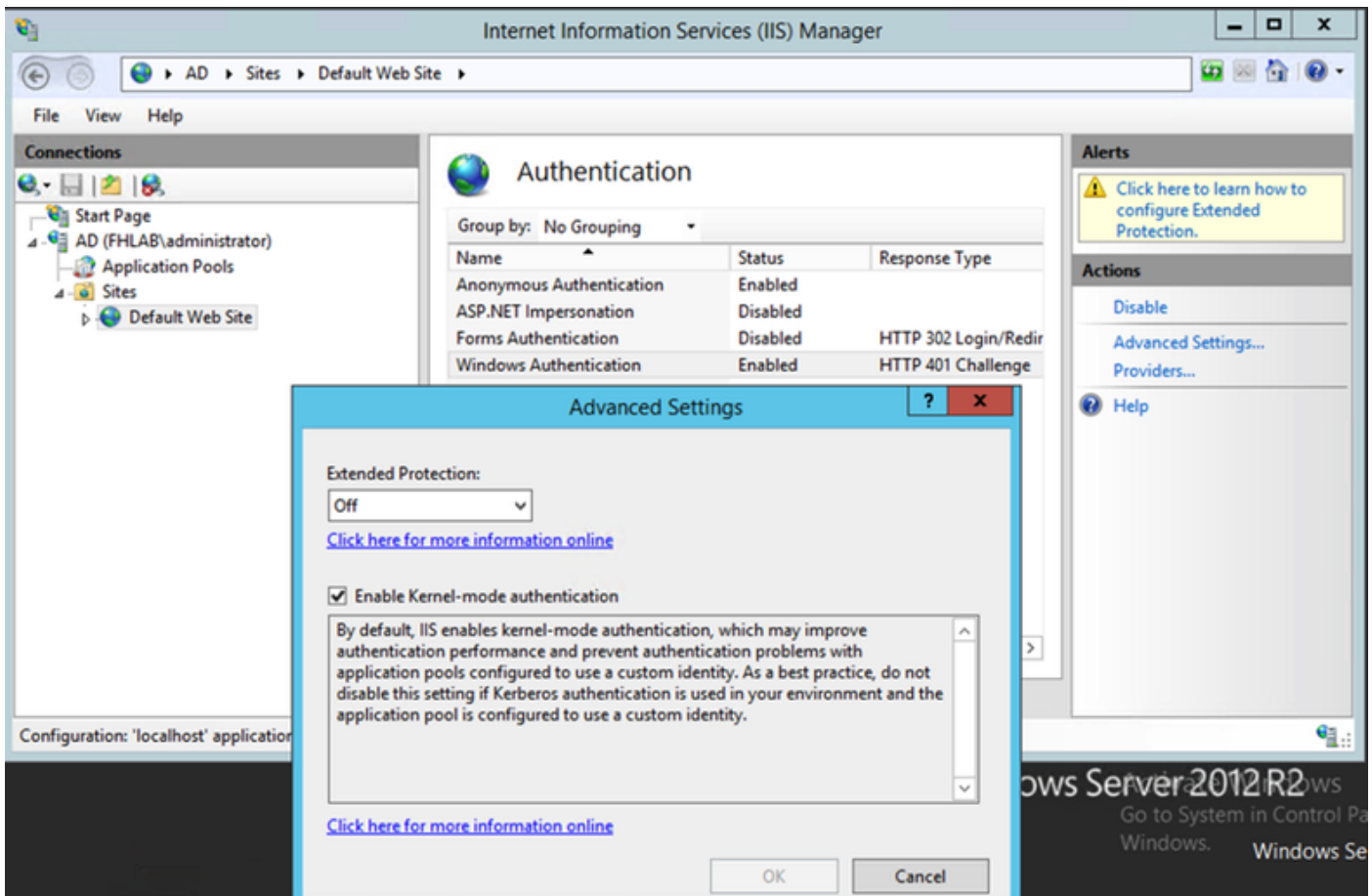
De OAuth-autorisatiecode subsidie flow ondersteunt het gebruik van verfrissingspenningen. Dit levert een betere ervaring aan de eindgebruiker op omdat deze niet zo vaak opnieuw hoeft te authenticeren (standaard 60 dagen)

## **Kerberos configureren**

### **Selecteer Windows-verificatie**

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

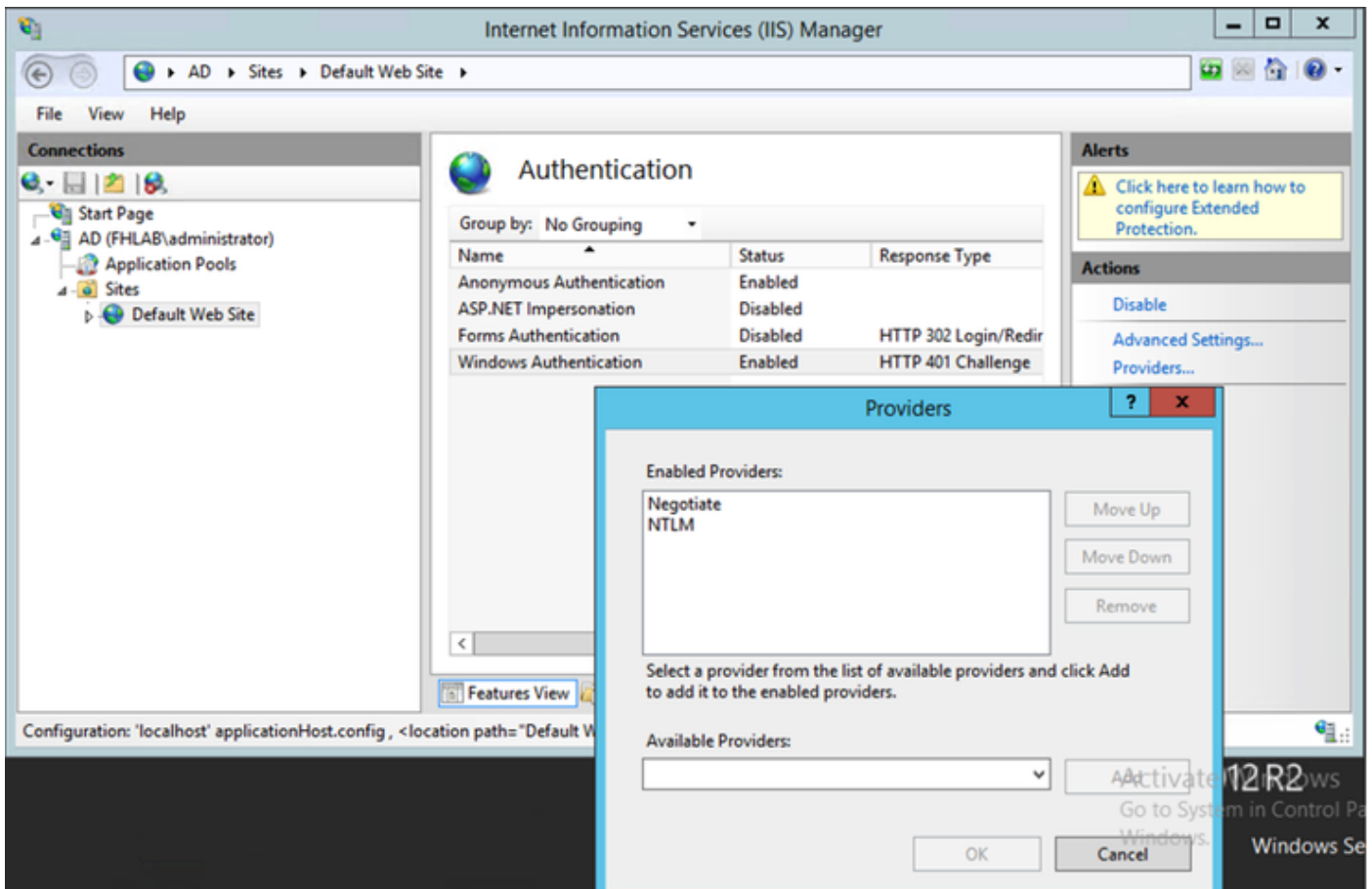
1. Schakel de verificatie van de Kernel-modus in.
2. Zorg ervoor dat uitgebreide bescherming is uitgeschakeld.



## ADFS ondersteunt beide Kerberos NTLM

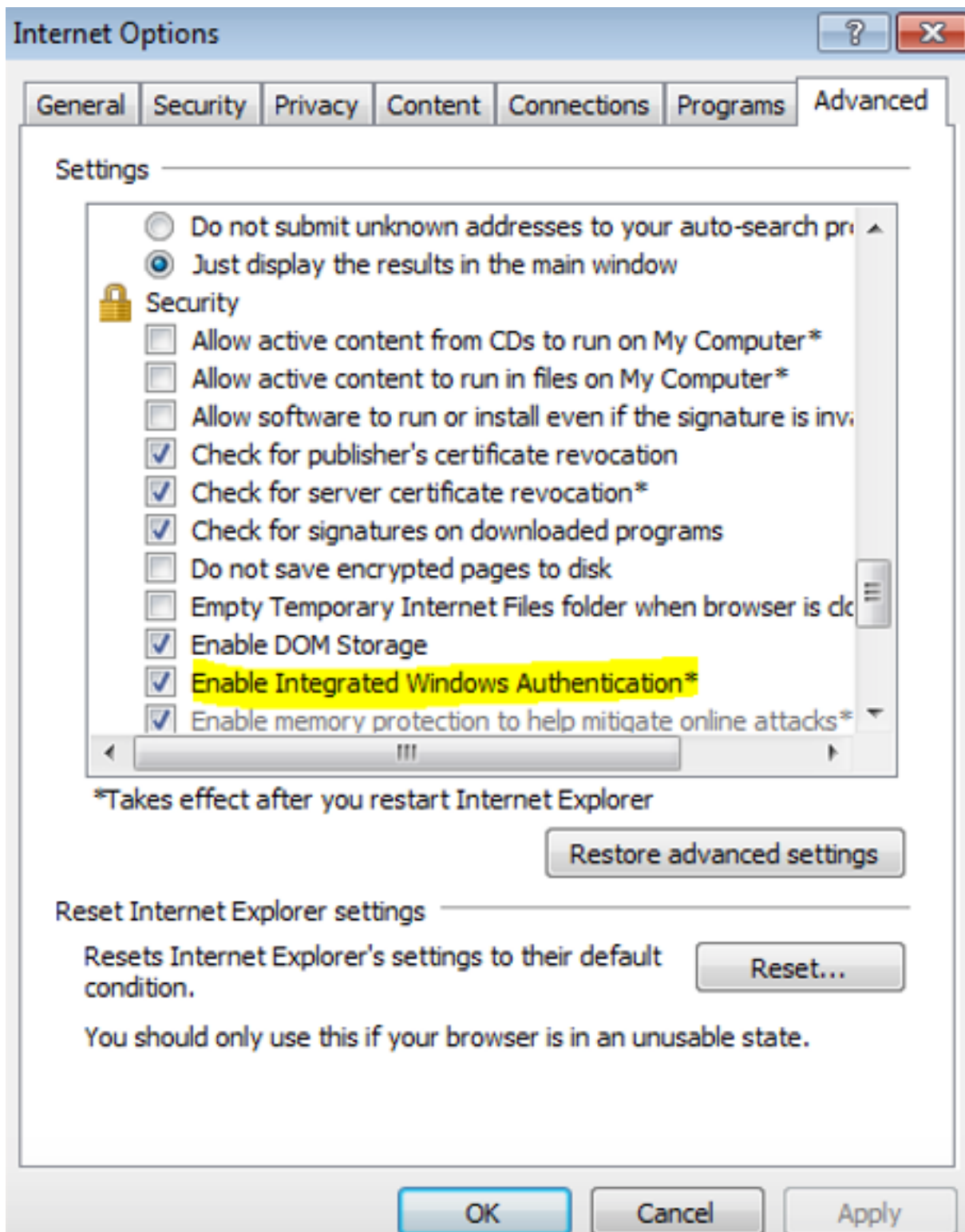
Zorg ervoor dat AD FS versie 3.0 zowel het Kerberos-protocol als het NTLM-protocol (NT LAN Manager) ondersteunt omdat alle niet-Windows-clients Kerberos niet kunnen gebruiken en niet op NTLM kunnen vertrouwen.

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



## Microsoft Internet Explorer configureren

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



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

