

AD FS versie 2.0 Instellen voor SAML SFS-configuratievoorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[metagegevens over downloads en end-of-support versie 2.0 Identity Provider \(IDP\)](#)

[Metagegevens voor samenwerking met downloads \(Collaboration Server\)](#)

[CUCM IM and Presence Service](#)

[Unity Connection](#)

[Cisco Prime-provisioning voor samenwerking](#)

[CUCM toevoegen als vertrouwen van een betrouwbare partij](#)

[Voeg CUCM IM and Presence toe als Relay Party Trust](#)

[Voeg UCXN toe als vertrouwen van een betrouwbare partij](#)

[Voeg Cisco Prime Collaboration Provisioning toe als vertrouwen van derden](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u Active Directory Federation Service (AD FS) versie 2.0 kunt configureren om Security Association Markup Language (SAML) single aanmelding (SSO) mogelijk te maken voor Cisco Collaboration-producten zoals Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (UCXN), CUCM IM and Presence en Cisco Prime Collaboration.

Voorwaarden

Vereisten

AD FS versie 2.0 moet worden geïnstalleerd en getest.

Voorzichtig: Deze installatiehandleiding is gebaseerd op een labo-instelling en AD FS versie 2.0 wordt verondersteld alleen te worden gebruikt voor SAML SER met Cisco Collaboration-producten. Als de software door andere bedrijfskritieke toepassingen wordt gebruikt, moet de gewenste aanpassing plaatsvinden volgens de officiële Microsoft Documentatie.

Gebruikte componenten

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

- AD FS versie 2.0
- Microsoft Internet Explorer 1.0
- UCM versie 10.5
- Cisco IM and Presence Server versie 10.5
- UCXN versie 10.5
- Cisco Prime Collaboration Provisioning 10.5

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 live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

metagegevens over downloads en end-of-support versie 2.0 Identity Provider (IDP)

Als u IDP-metadata wilt downloaden, voert u deze link op uw browser uit: <https://<FQDN van ADFS>/FederationMetadata/2007-06/FederationMetadata.xml>.

Metagegevens voor samenwerking met downloads (Collaboration Server)

CUCM IM and Presence Service

Open een webbrowser, log in CUCM als beheerder en navigeer naar **Systeem > SAML Single Sign On**.

Unity Connection

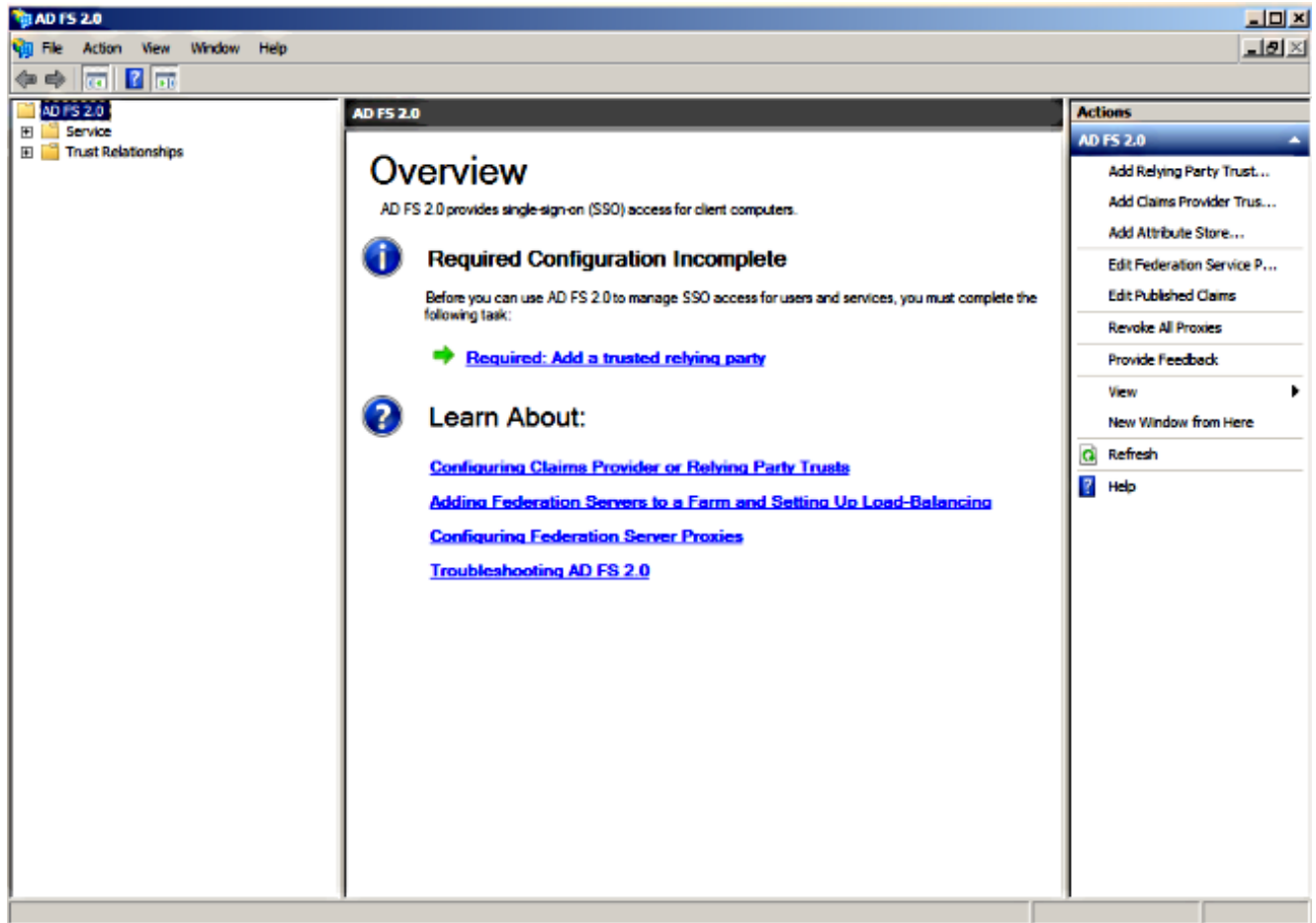
Open een webbrowser, log in UCXN als beheerder en navigeer naar **stelsysteeminstellingen > SAML Single Sign On**.

Cisco Prime-provisioning voor samenwerking

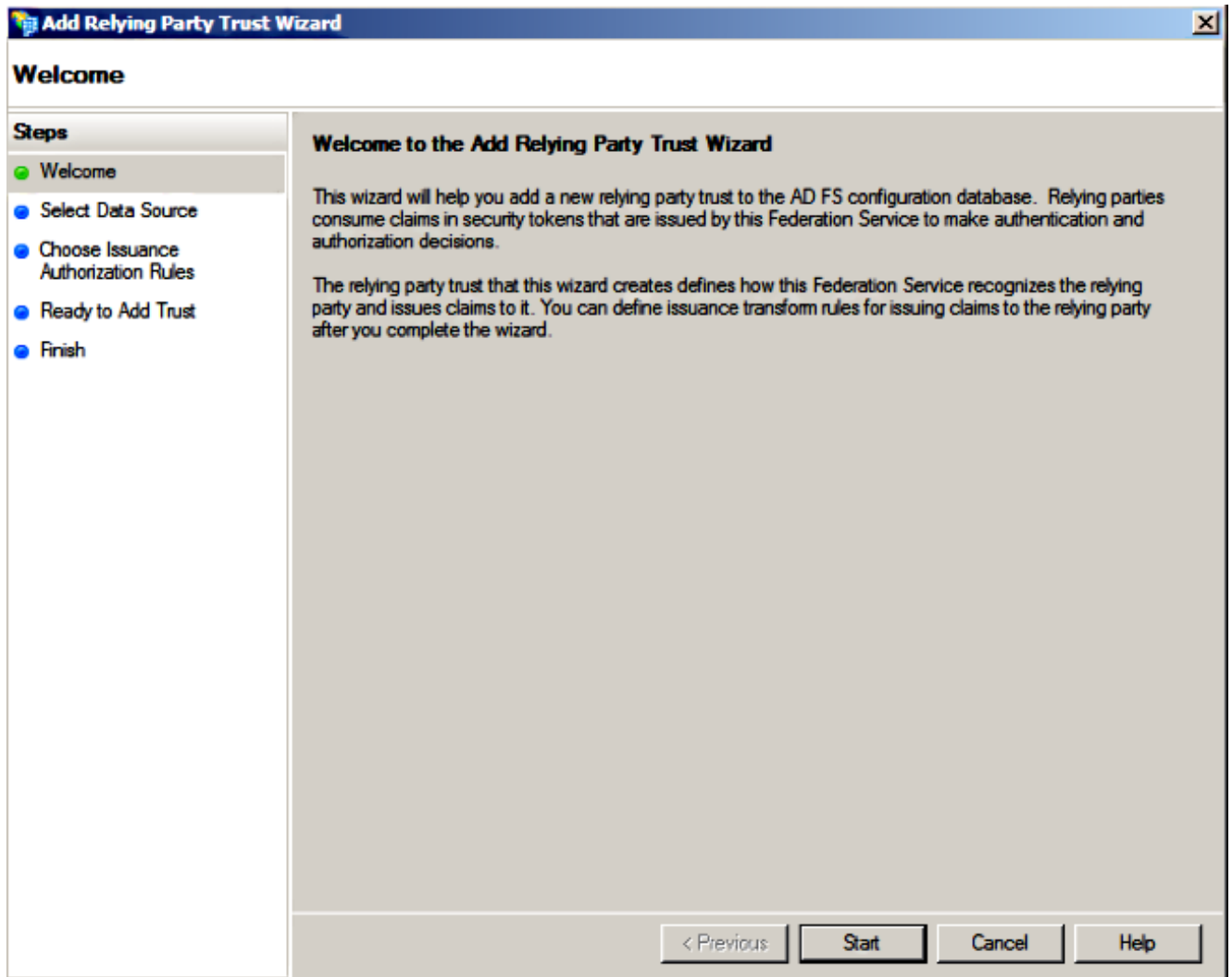
Open een webbrowser, log in Prime Collaboration Assurance als globaladmin en navigeer naar **Administration > System Setup > Single Sign On**.

CUCM toevoegen als vertrouwen van een betrouwbare partij

1. Meld u aan bij de AD FS-server en start u AD FS versie 2.0 in het menu **Programma's** van Microsoft Windows.
2. Selecteer **Toevoegen vertrouwen van derden**.



3. Klik op **Start**.



4. Selecteer de optie **Gegevens importeren over de vertrouwende partij uit een bestand** optie, kies het metagegevensbestand **SPMetmetadata_CUCM.xml** dat u eerder van CUCM hebt gedownload en klik op **Volgende**.

Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- 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 Help

5. Typ de naam van de weergave en klik op Volgende.

Add Relying Party Trust Wizard

Specify Display Name

Steps

- Welcome
- Select Data Source
- Specify Display Name**
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

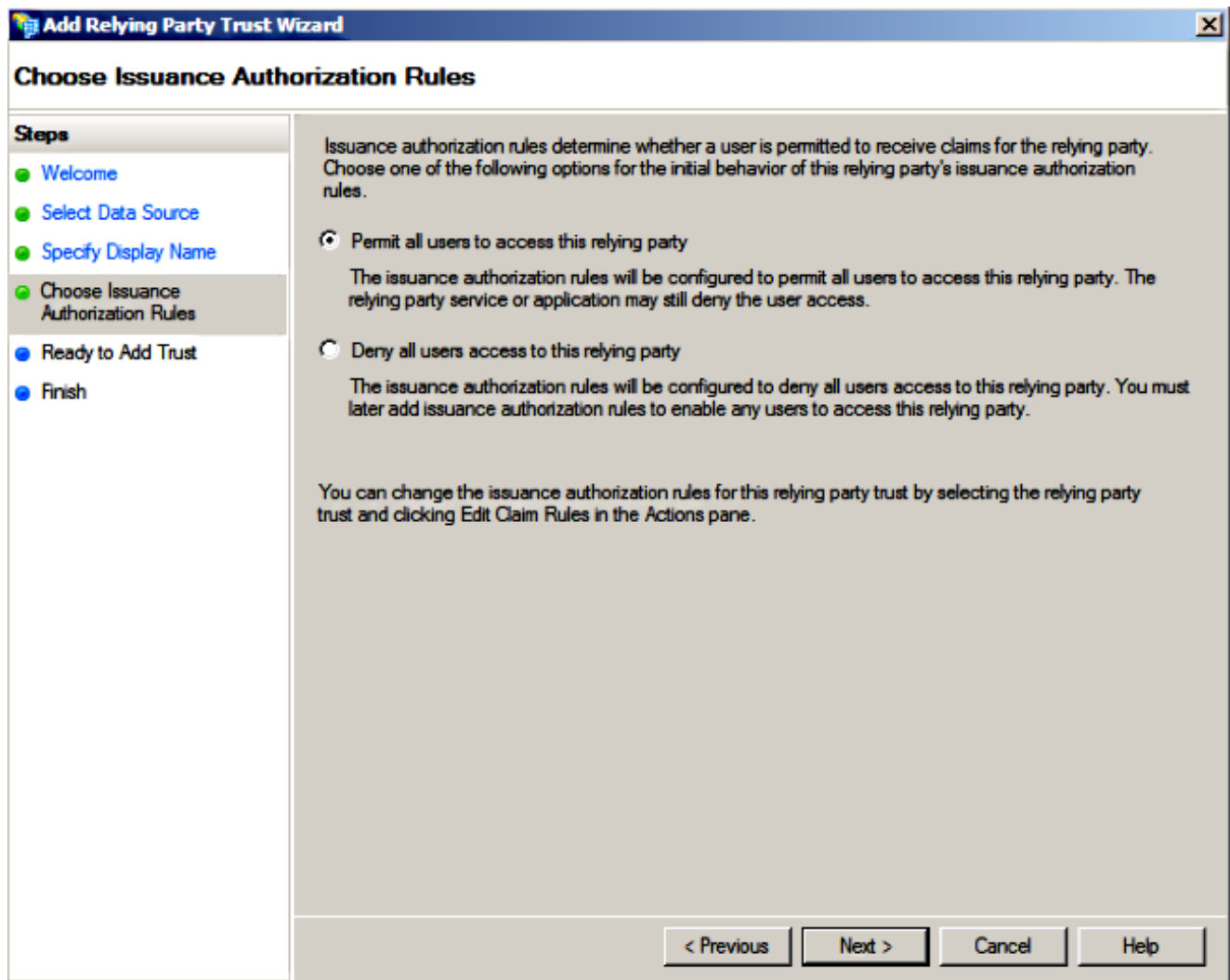
Type the display name and any optional notes for this relying party.

Display name:
CUCM

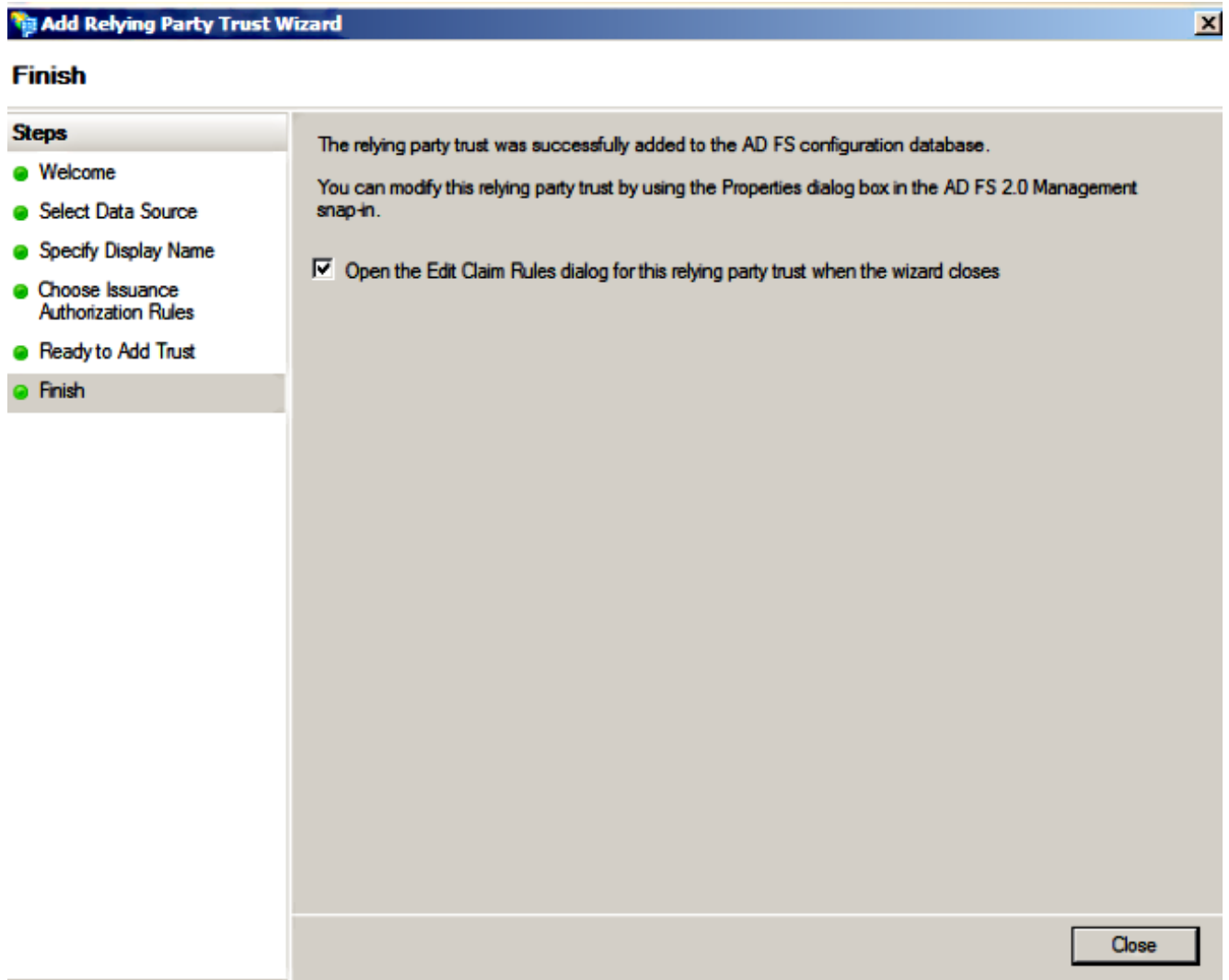
Notes:
Adding CUCM as Relaying Party to ADFS

< Previous Next > Cancel Help

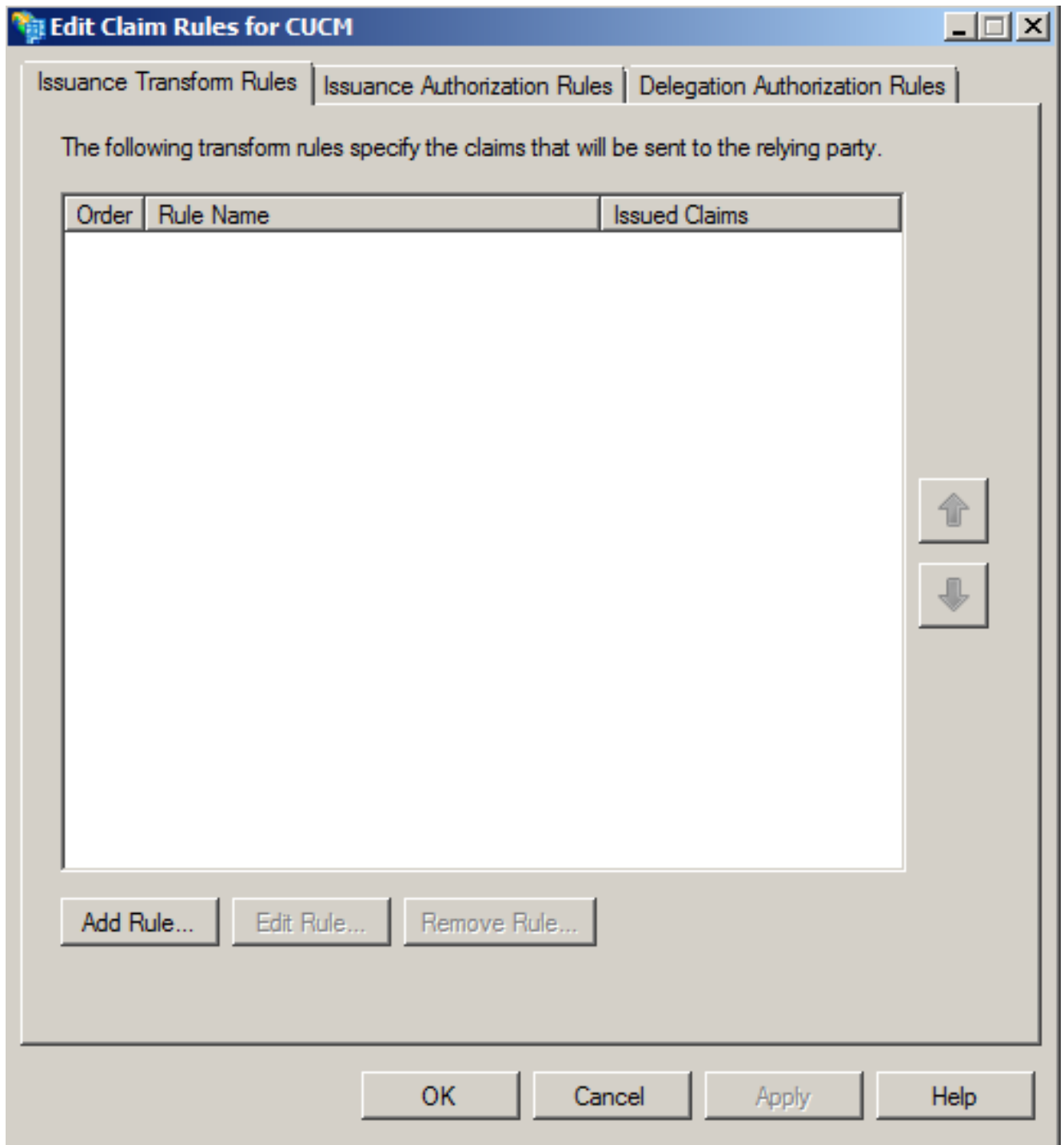
6. Kies **Toestaan alle gebruikers van deze groep** en klik op **Volgende**.



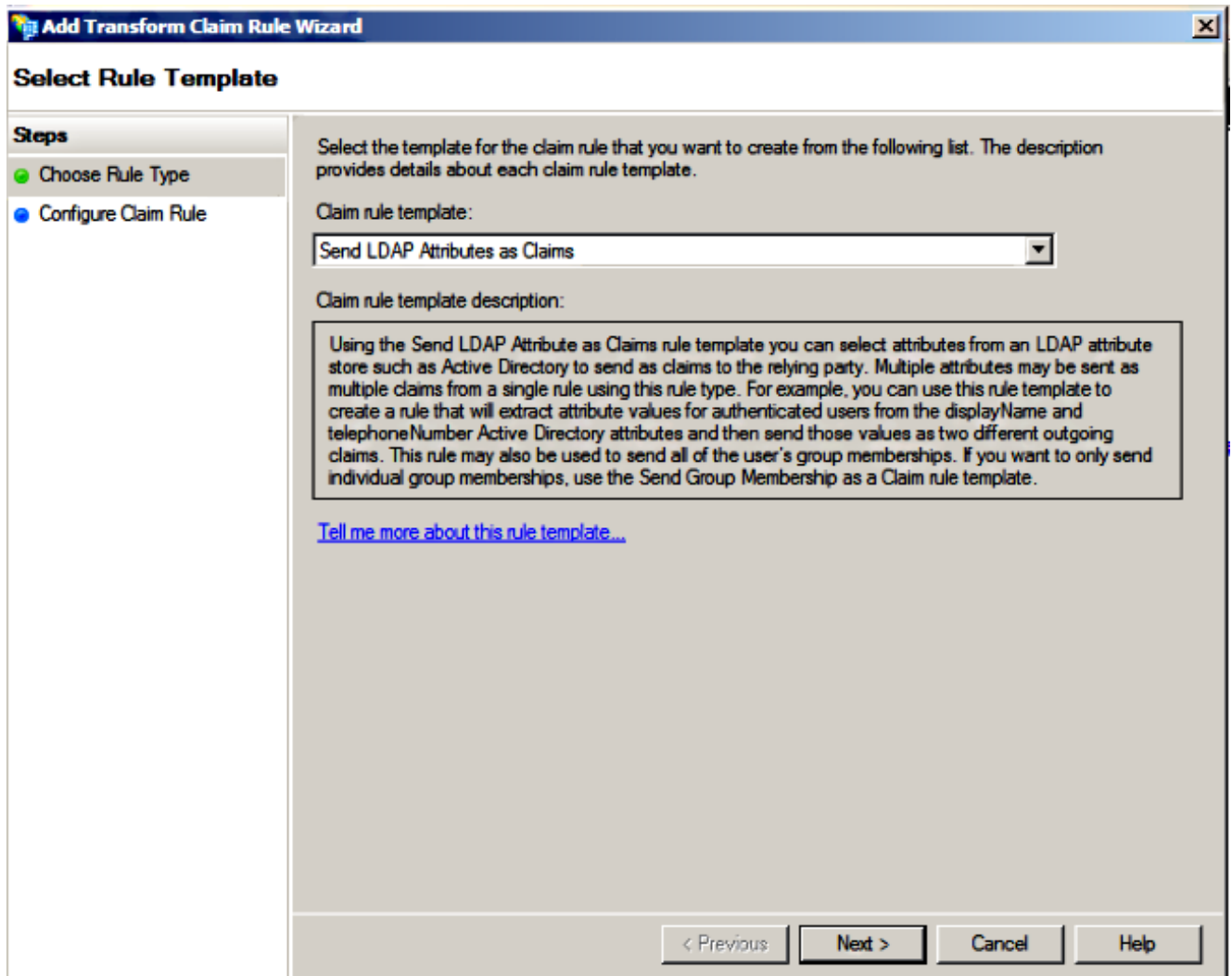
7. Selecteer het dialoogvenster FineReader-regels bewerken voor het vertrouwen van een betrouwbare partij wanneer de wizard sluit en klik op Sluiten.



8. Klik op **Regel toevoegen**.



9. Klik op **Volgende** met de standaardregelsjabloon voor claims ingesteld op **Verzend LDAP-kenmerken als claims**.



10. Typ in de regel Configureren de naam van de Claim Rule, selecteer **Actieve Map** als de winkel van Kenmerken, stel **LDAP-kenmerk** en **Uitgaande claimtype** in zoals in deze afbeelding weergegeven en klik op **Voltooien**.

Opmerking:

- De lichtgewicht Directory Access Protocol (LDAP) eigenschap moet overeenkomen met de Directory Sync eigenschap op CUCM.
- "uid" moet in het kleine geval staan.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

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:
Name ID

Rule template: Send LDAP Attributes as Claims

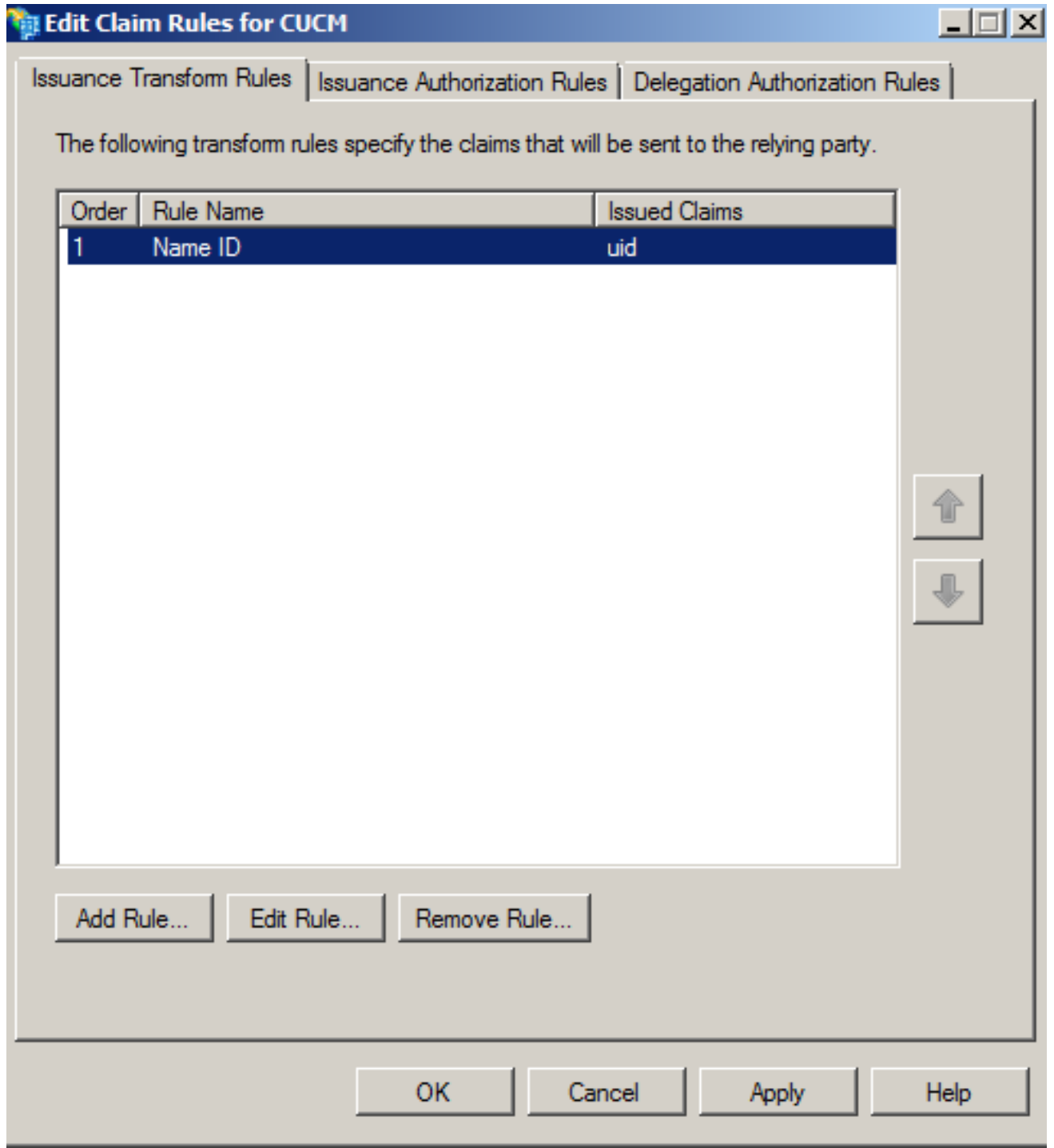
Attribute store:
Active Directory

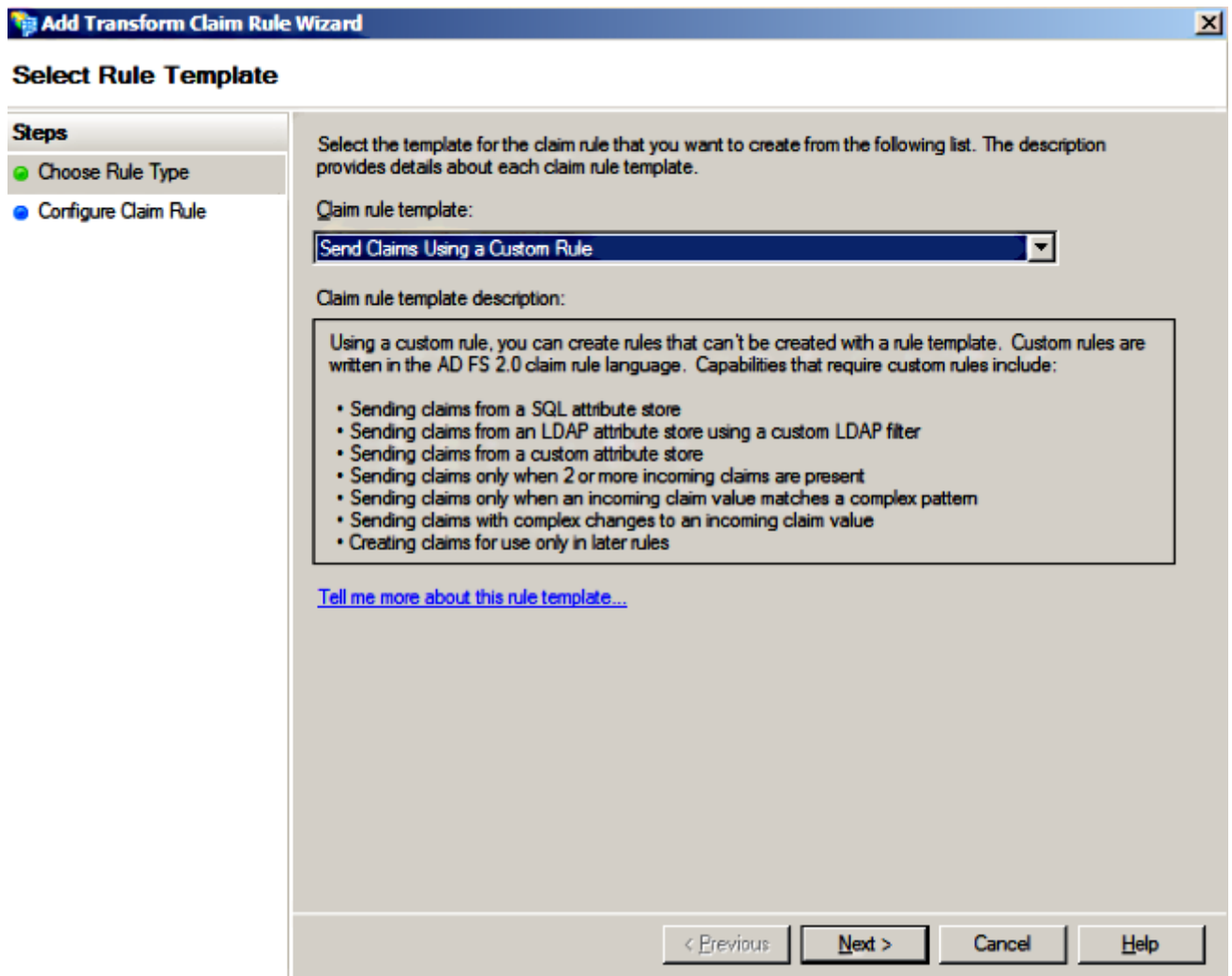
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
▶	SAM-Account-Name	uid
*		

< Previous Finish Cancel Help

11. Klik op **Regel toevoegen**, selecteer **Claims verzenden met een aangepaste regel** als de sjabloon voor de claimregel en klik op **Volgende**.

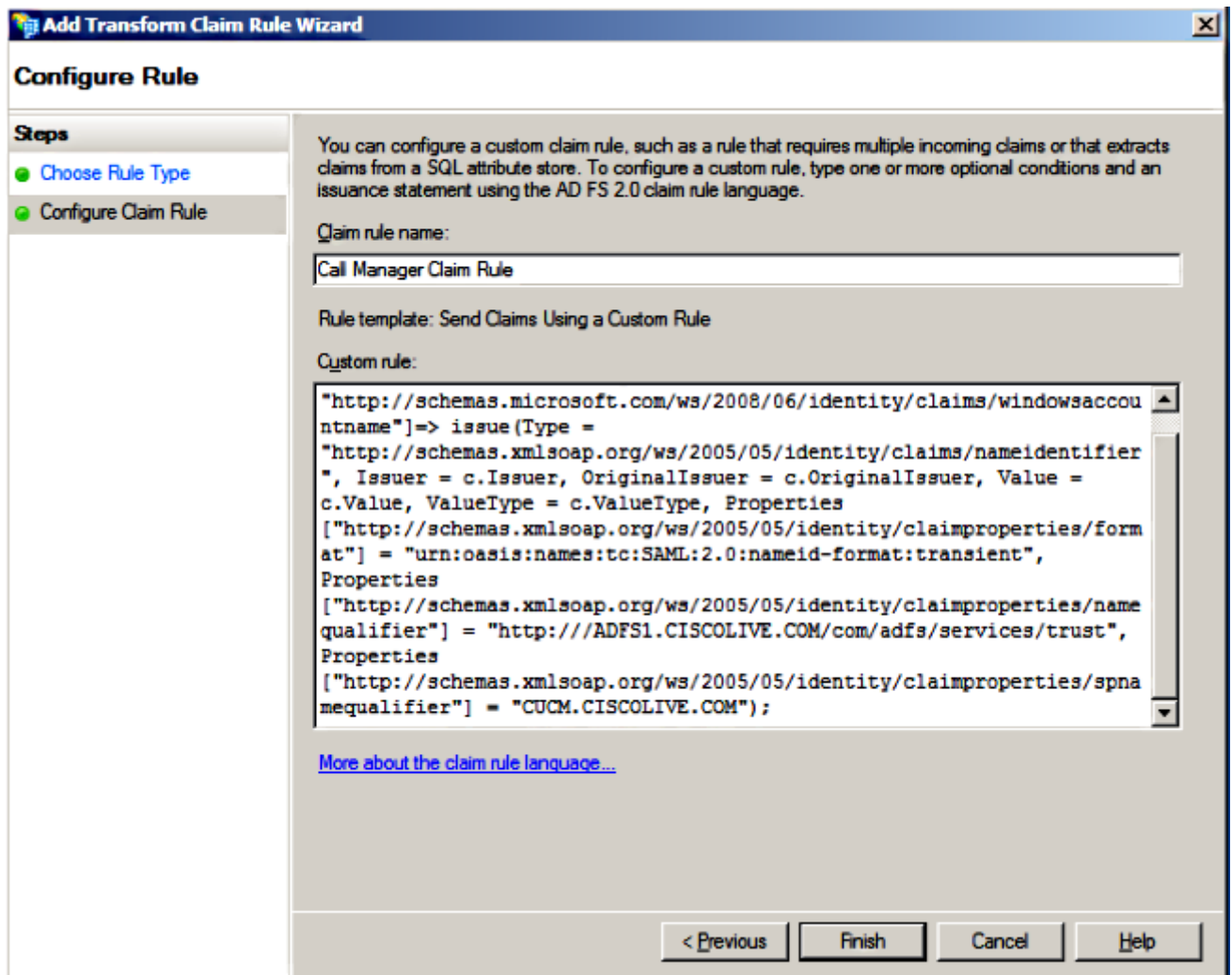




12. Voer een naam in voor de naam van de Claim-regel en kopieer deze syntaxis in de ruimte die onder Aangepaste regel wordt gegeven:

```
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://<FQDN of ADFS>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier
"] = "<FQDN of CUCM>");
```

(OPMERKING: Als u de tekst uit deze voorbeelden kopieert en kleeft, moet u er rekening mee houden dat bepaalde tekstverwerkingssoftware de ASCII-aanhalingstekens (") zal vervangen door de UNICODE-versies ("). De UNICODE-versies zullen ervoor zorgen dat de claimregel mislukt.)



Opmerking:

- CUCM en ADFS Full Qualified Domain Name (FQDN) is in dit voorbeeld vooraf ingevuld met het laboratorium CUCM en AD FS en moet worden aangepast om uw omgeving aan te passen.
- FQDN van CUCM/ADFS is hoofdlettergevoelig en moet met de metagegevensbestanden overeenkomen.

13. Klik op **Voltooien**.

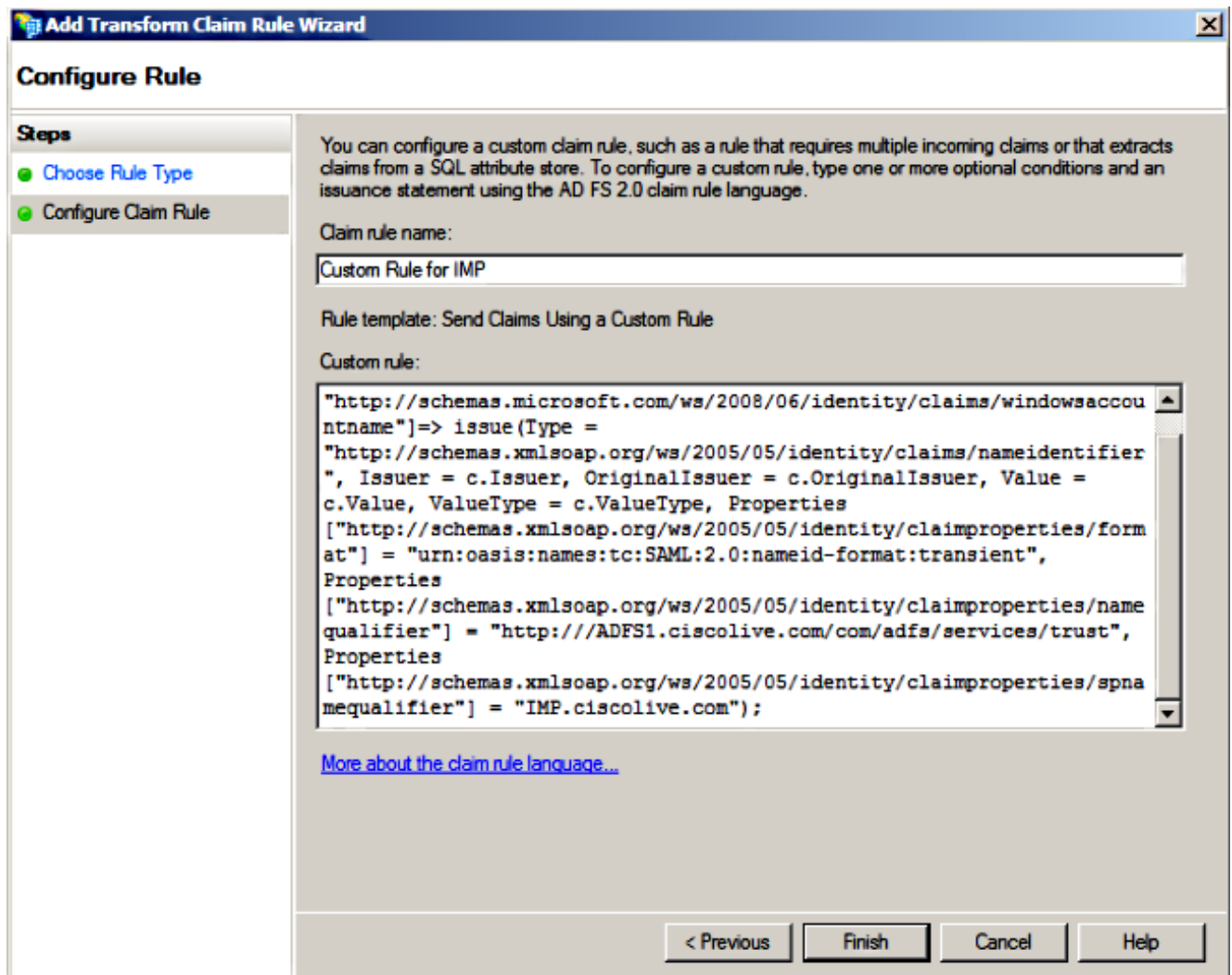
14. Klik op **Toepassen** en vervolgens op **OK**.

15. Start de AD FS versie 2.0 opnieuw vanaf **Services.msc**.

Voeg CUCM IM and Presence toe als Relay Party Trust

1. Herhaal stap 1 tot en met 11 zoals beschreven voor **Add CUCM als Relying Party Trust** en ga naar stap 2.
2. Voer een naam in voor de naam van de Claim-regel en kopieer deze syntaxis in de ruimte die onder Aangepaste regel wordt gegeven:

```
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://<FQDN of ADFS>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of IMP>");
```



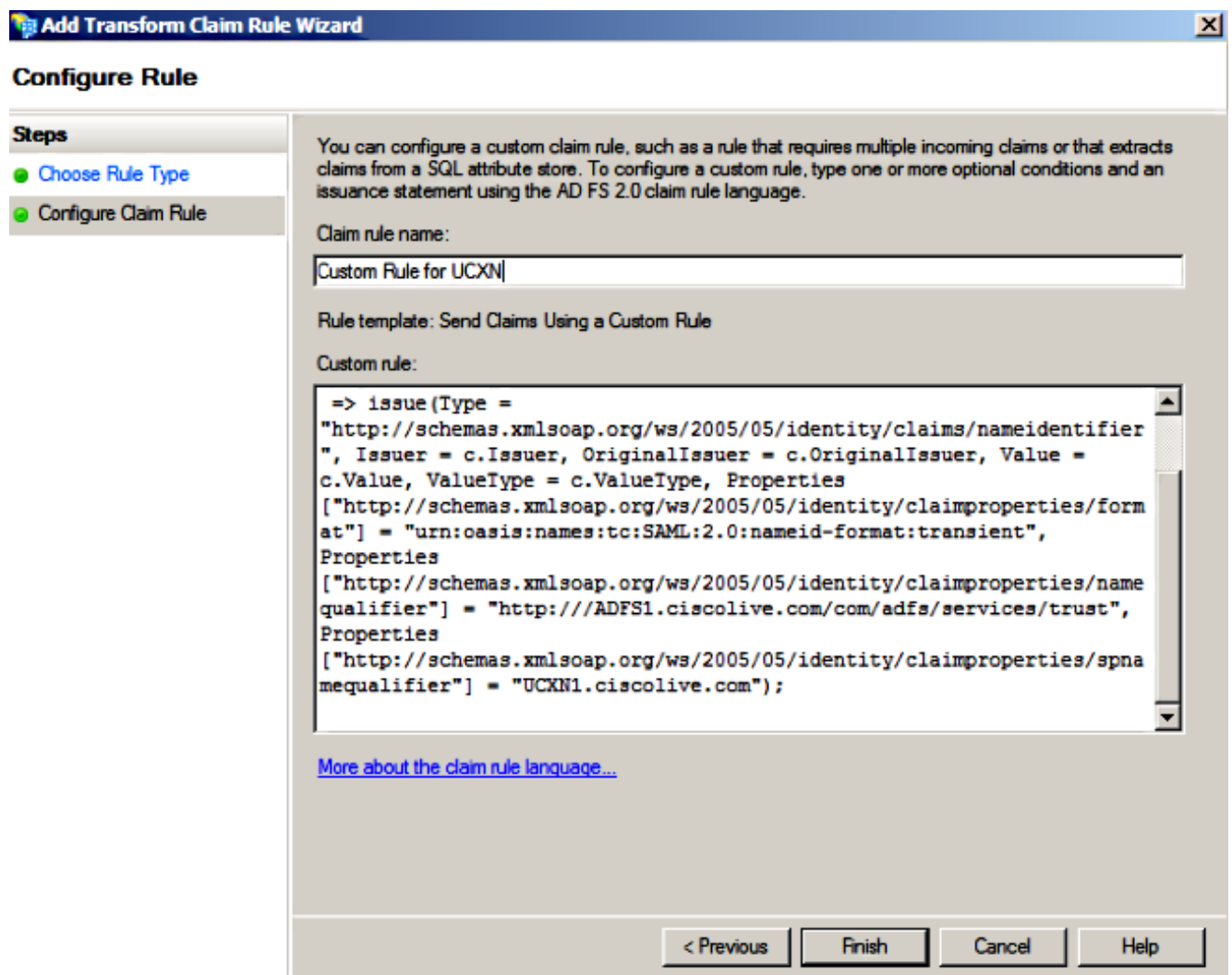
Merk op dat IM and Presence en AD FS FQDN in dit voorbeeld met het laboratorium IM and Presence en AD FS zijn voorbevolkt en moeten worden aangepast om uw omgeving aan te passen.

3. Klik op **Voltooien**.
4. Klik op **Toepassen** en vervolgens op **OK**.
5. Start de AD FS versie 2.0 opnieuw vanaf **Services.msc**.

Voeg UCXN toe als vertrouwen van een betrouwbare partij

1. Herhaal stap 1 tot en met 12 zoals beschreven voor **Add CUCM als Relying Party Trust** en ga naar stap 2.
2. Voer een naam in voor de regelnaam van de claim en kopieer deze syntaxis in de ruimte die onder Aangepaste regel wordt gegeven:

```
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://<FQDN of ADFS>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of UCXN>");
```



Merk op dat UCXN en AD FS FQDN in dit voorbeeld voorbevolkt is met het lab UCXN en ADFS en moet worden aangepast om uw omgeving aan te passen.

3. Klik op **Voltoeien**.
4. Klik op **Toepassen** en vervolgens op **OK**.

5. Start de AD FS versie 2.0 opnieuw vanaf **Services.msc**.

Voeg Cisco Prime Collaboration Provisioning toe als vertrouwen van derden

1. Herhaal stap 1 tot en met 12 zoals beschreven voor **Add CUCM als Relying Party Trust** en ga naar stap 2.
2. Voer een naam in voor de regelnaam van de claim en kopieer deze syntaxis in de ruimte die onder Aangepaste regel wordt gegeven:

```
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://<FQDN of ADFS>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of PCP>");
```

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule**

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS 2.0 claim rule language.

Claim rule name:
Custom Rule for PCP

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
ntname"]
=> 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/form
at"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/name
qualifier"] = "http://ADFS1.ciscolive.com/com/adfs/services/trust",
Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spna
mequalifier"] = "PCP.ciscolive.com");
```

[More about the claim rule language...](#)

< Previous Finish Cancel Help

Merk op dat Prime Provisioning en AD FS FQDN wordt voorbevolkt met de lab Prime

Collaboration Provisioning (PCP) en AD FS uit dit voorbeeld en moet worden gewijzigd om uw omgeving te evenaren.

3. Klik op **Voltooien**.
4. Klik op **Toepassen** en vervolgens op **OK**.
5. Start de AD FS versie 2.0 opnieuw vanaf **Services.msc**.

Nadat u versie 2.0 van de AD90 hebt ingesteld, schakelt u de SAML SETO in op Cisco Collaboration-producten.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

AD FS registreert diagnostische gegevens aan het systeemEvent Log. Vanaf Server Manager op AD FS server open **Diagnostics -> Event Viewer -> Toepassingen en services -> AD FS 2.0 -> Admin**

Kijk naar fouten die zijn vastgelegd voor AD FS-activiteit

Level	Date and Time	Source	Event ID	Task Category
Information	6/28/2016 11:18:12 AM	AD FS 2.0	337	None
Information	6/28/2016 11:18:12 AM	AD FS 2.0	336	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	390	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	386	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	399	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	157	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	156	None
Information	6/27/2016 11:18:02 PM	AD FS 2.0	337	None
Information	6/27/2016 11:18:02 PM	AD FS 2.0	336	None
Information	6/27/2016 8:12:59 PM	AD FS 2.0	388	None
Error	6/27/2016 8:12:11 PM	AD FS 2.0	364	None
Error	6/27/2016 8:12:11 PM	AD FS 2.0	321	None
Information	6/27/2016 8:12:10 PM	AD FS 2.0	251	None
Information	6/27/2016 8:11:59 PM	AD FS 2.0	100	None

Event 321, AD FS 2.0

General | Details

The SAML authentication request had a NameID Policy that could not be satisfied.
Requestor: ciscouc-105-imps1.ciscouc.org
Name identifier format: urn:oasis:names:tc:SAML:2.0:nameid-format:transient

Log Name: AD FS 2.0/Admin
Source: AD FS 2.0 Logged: 6/27/2016 8:12:11 PM
Event ID: 321 Task Category: None