AD FS versie 2.0 Instellen voor SAML SFS-configuratievoorbeeld

Inhoud

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 **systeeminstellingen > SAML Single Sign On**.

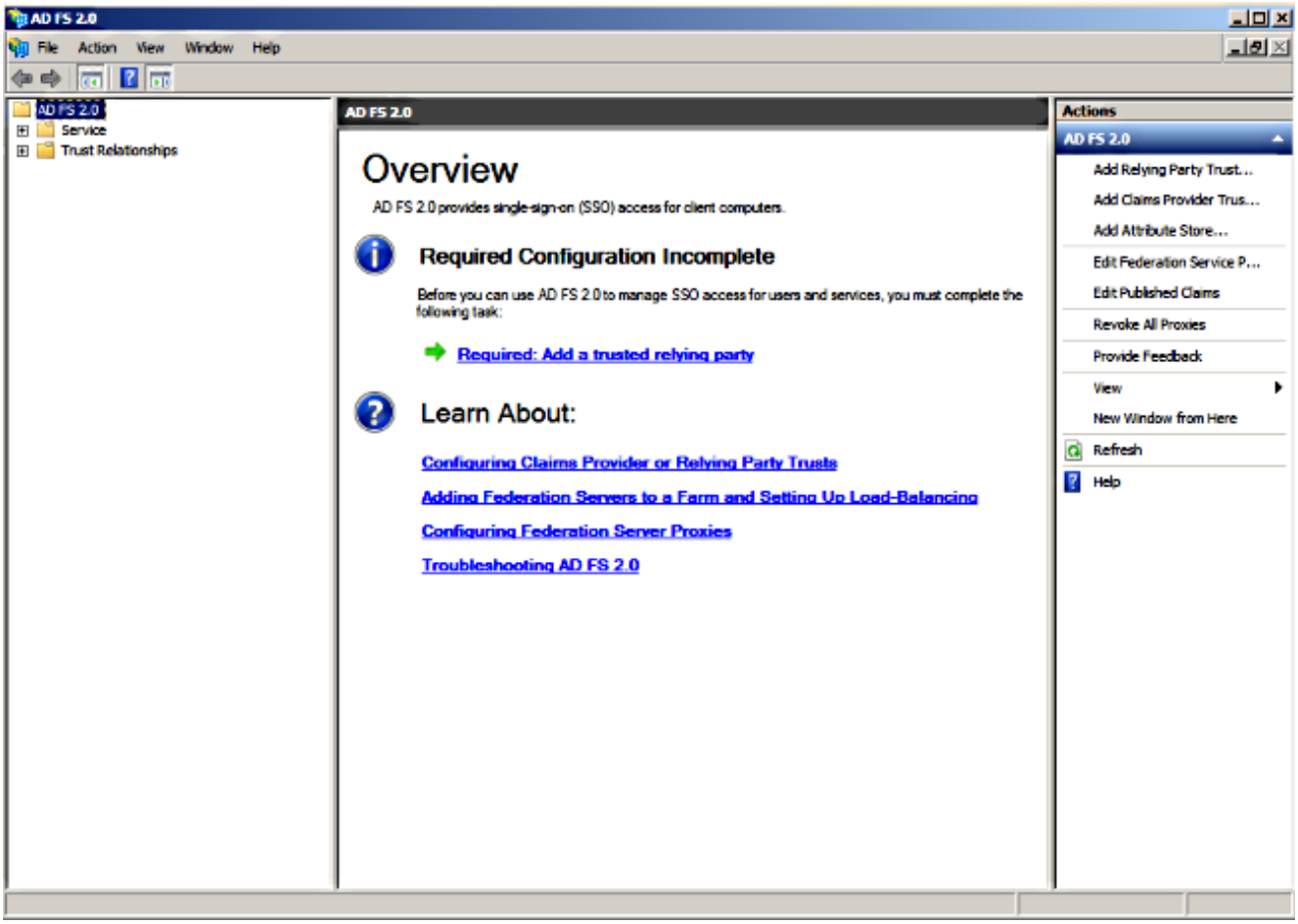
Cisco Prime-provisioning voor samenwerking

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

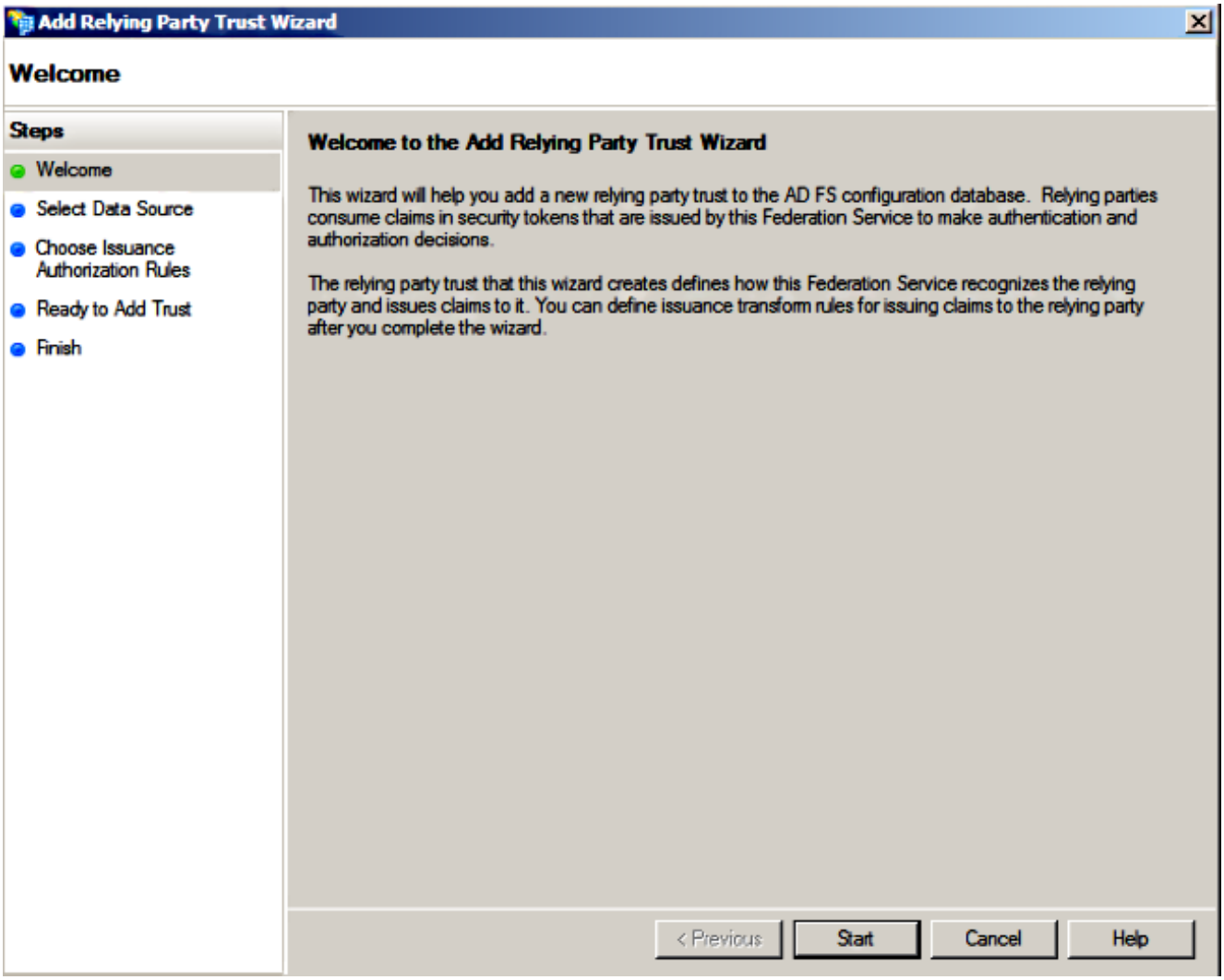
CUCM toevoegen als vertrouwen van een betrouwbare partij

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.

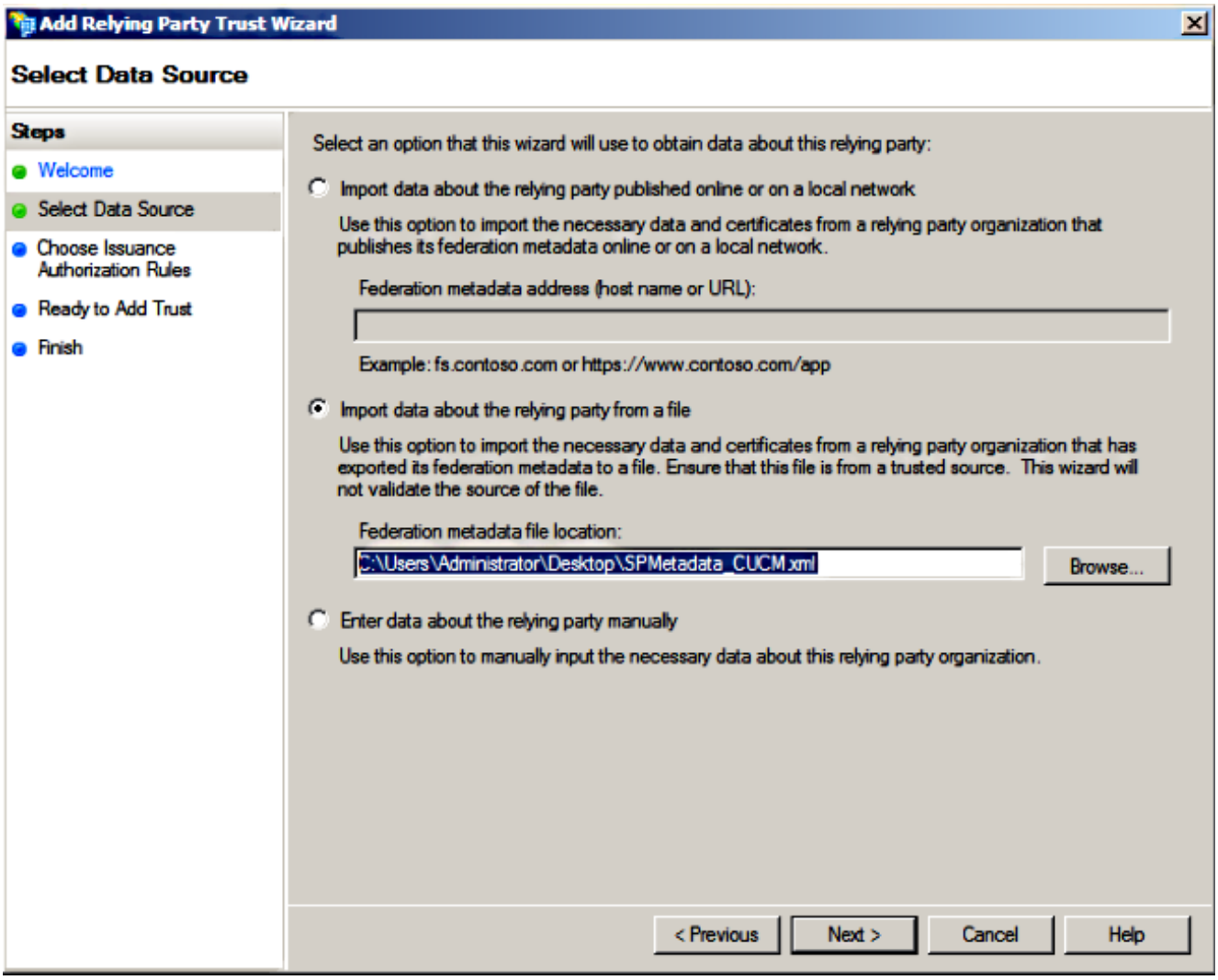
2. Selecteer **Toevoegen vertrouwen van derden**.



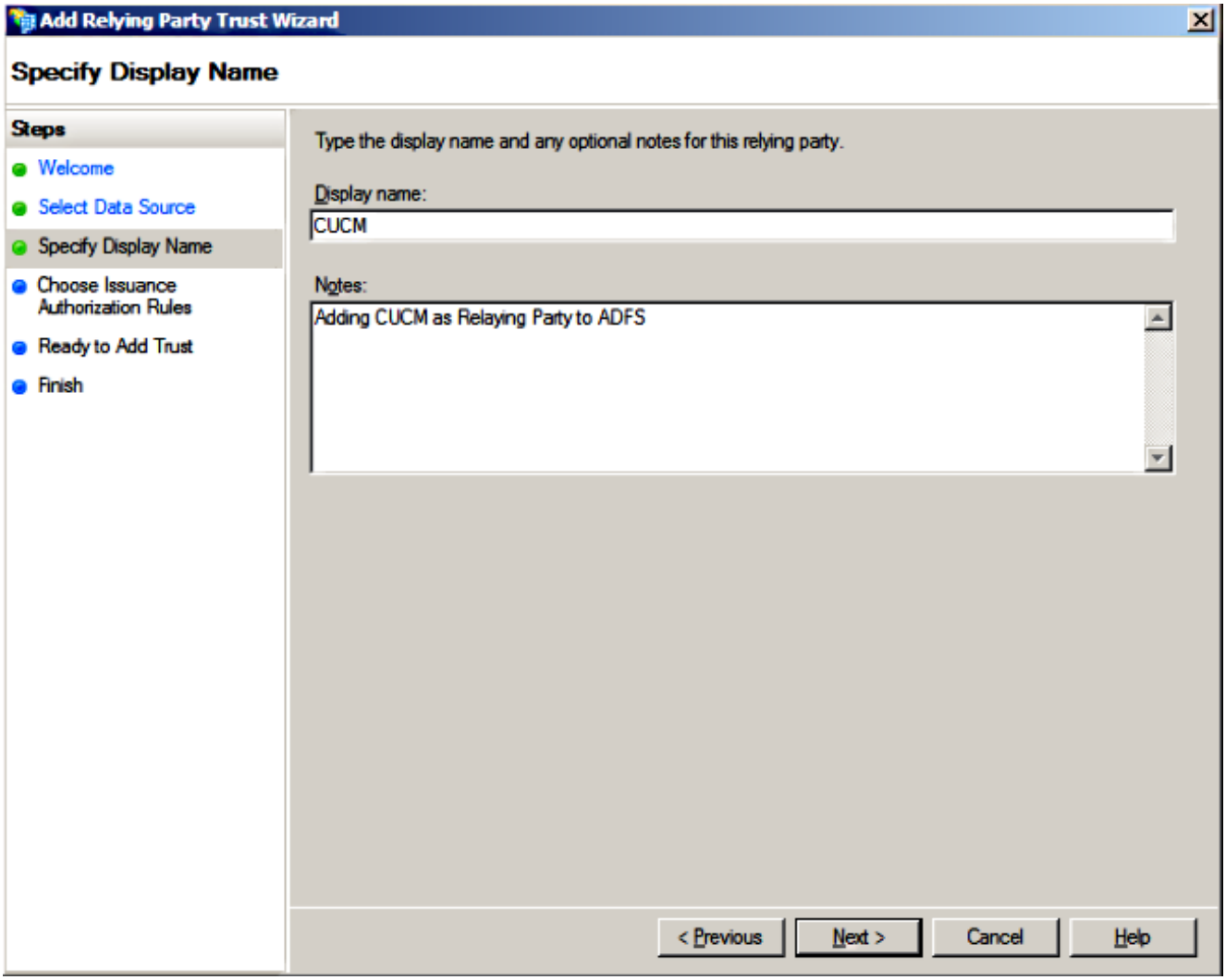
3. Klik op **Start**.



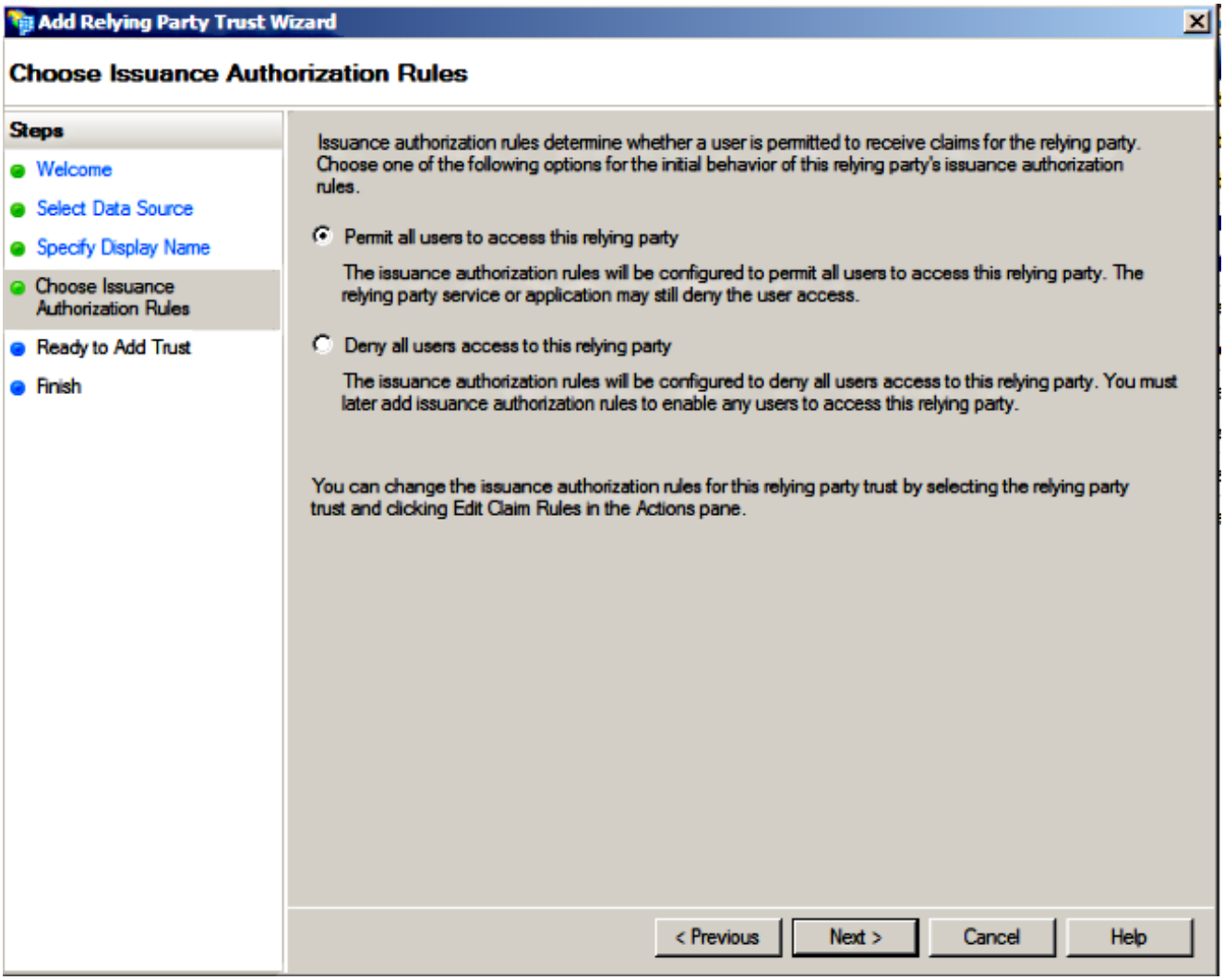
4. Selecteer de optie **Gegevens importeren over de vertrouwende partij uit een bestand** optie, kies het metagegevensbestand **SPMetmetadata_CUCM.xml** dat u eerder van CUCM hebt gedownload en klik op **Volgende.**



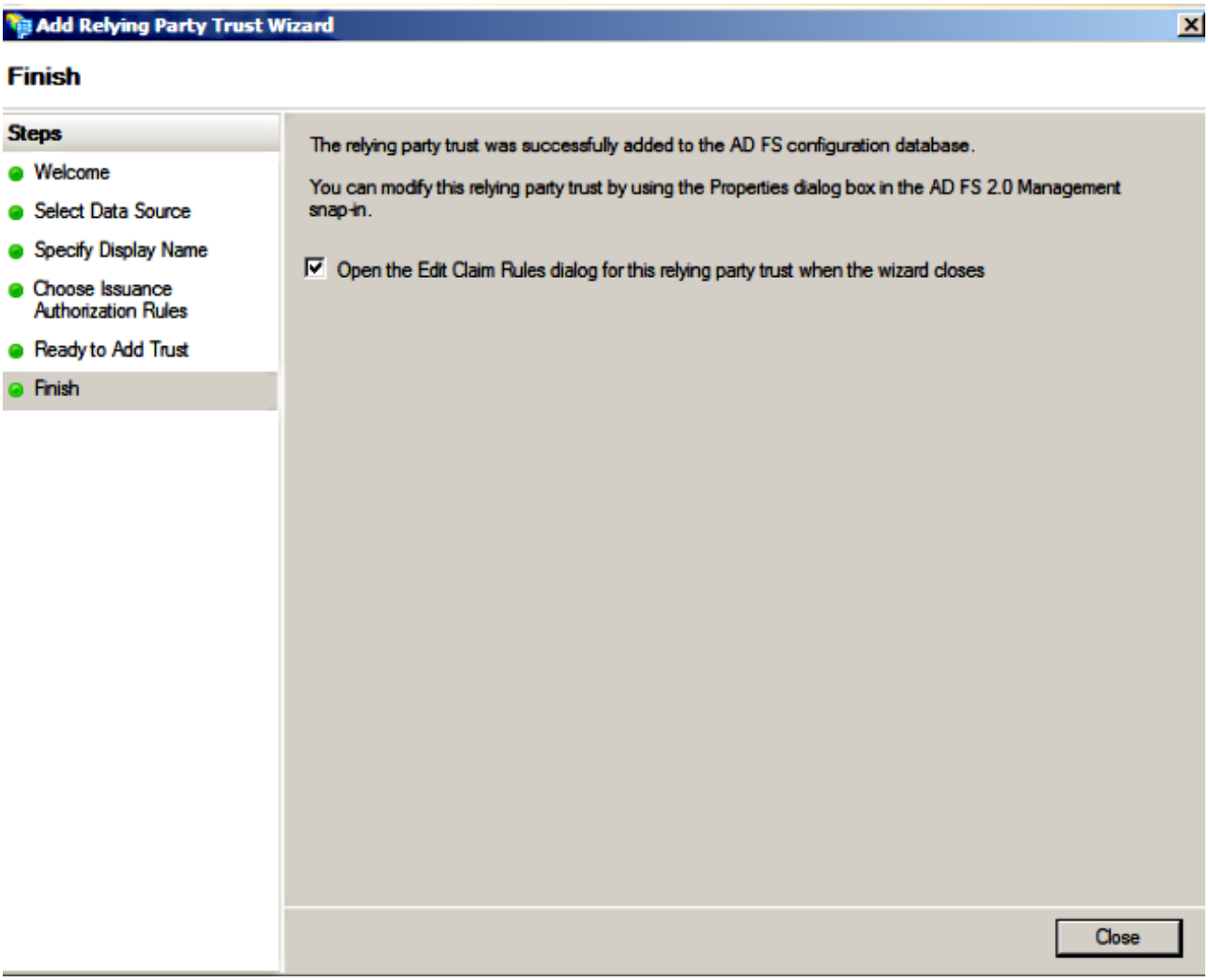
5. Typ **de naam van de weergave** en klik op **Volgende**.



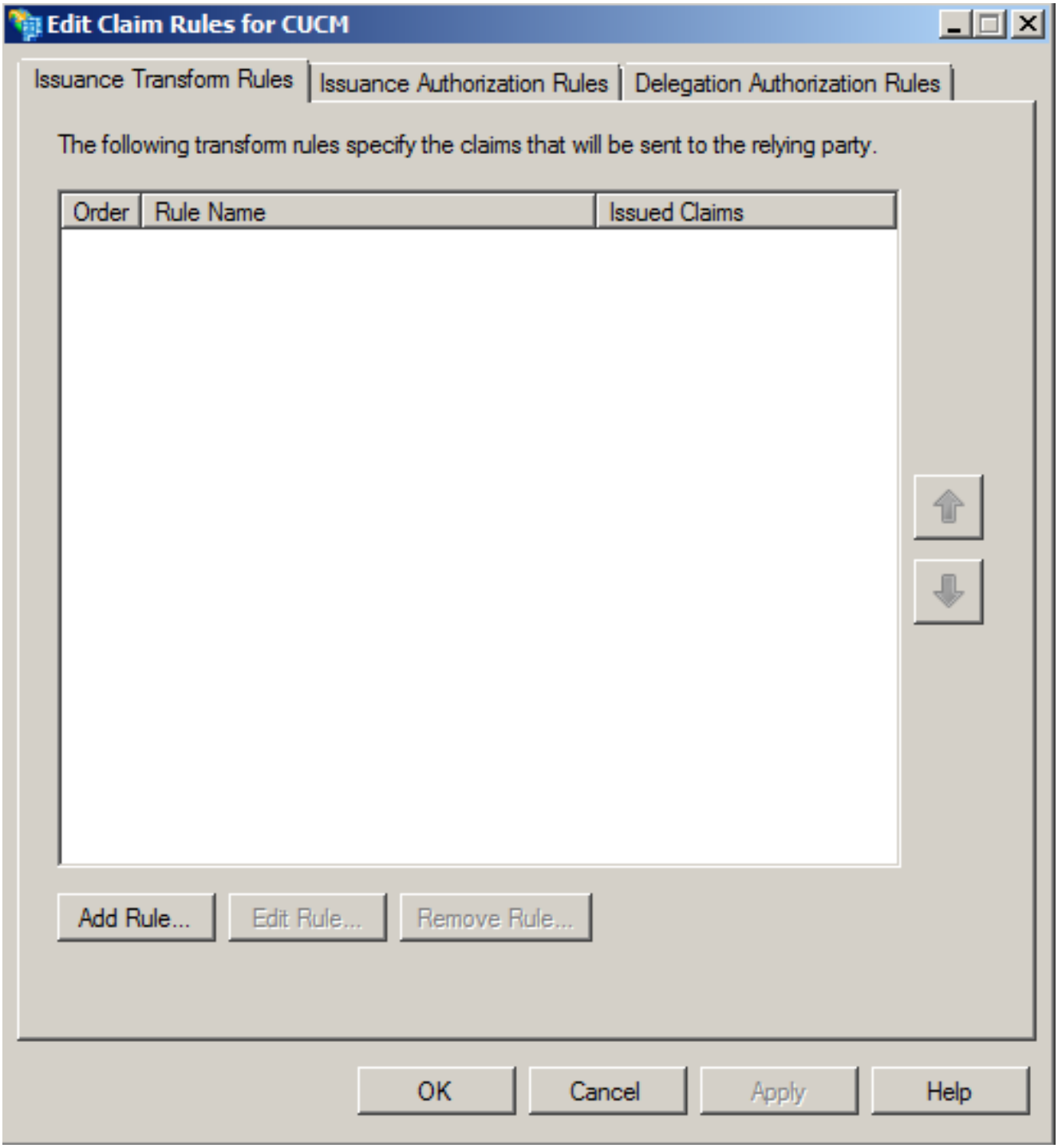
6. Kies **Toestaan alle gebruikers van deze groep** en klik op **Volgende.**



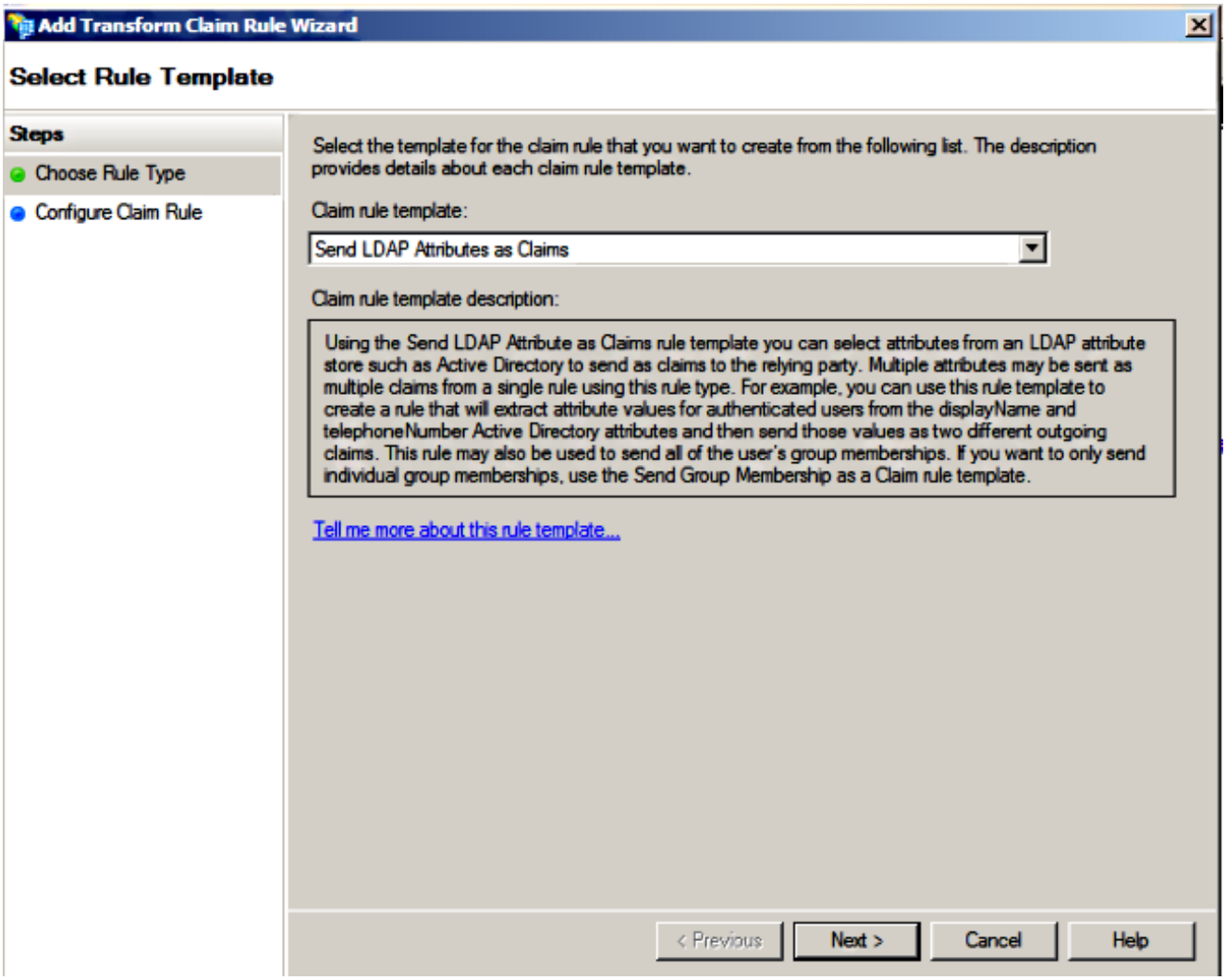
7. Selecteer **het dialoogvenster FineReader-regels bewerken voor het vertrouwen van een betrouwbare partij wanneer de wizard sluit** en klik op **Sluiten.**



8. Klik op **Regel toevoegen**.

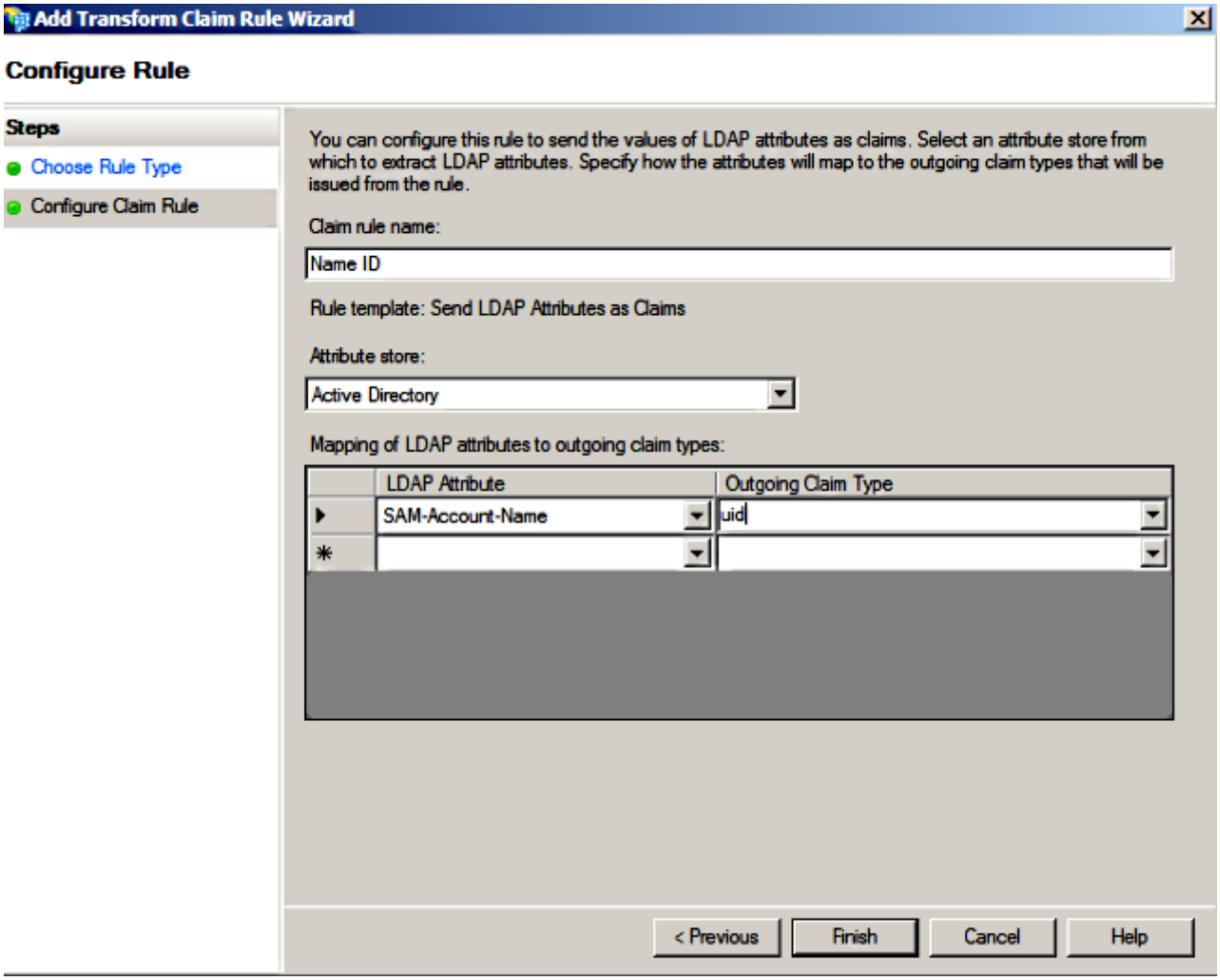


9. Klik op **Volgende** met de standaardregelsjabloon voor claims ingesteld op **Verzend LDAP-kenmerken als claims**.

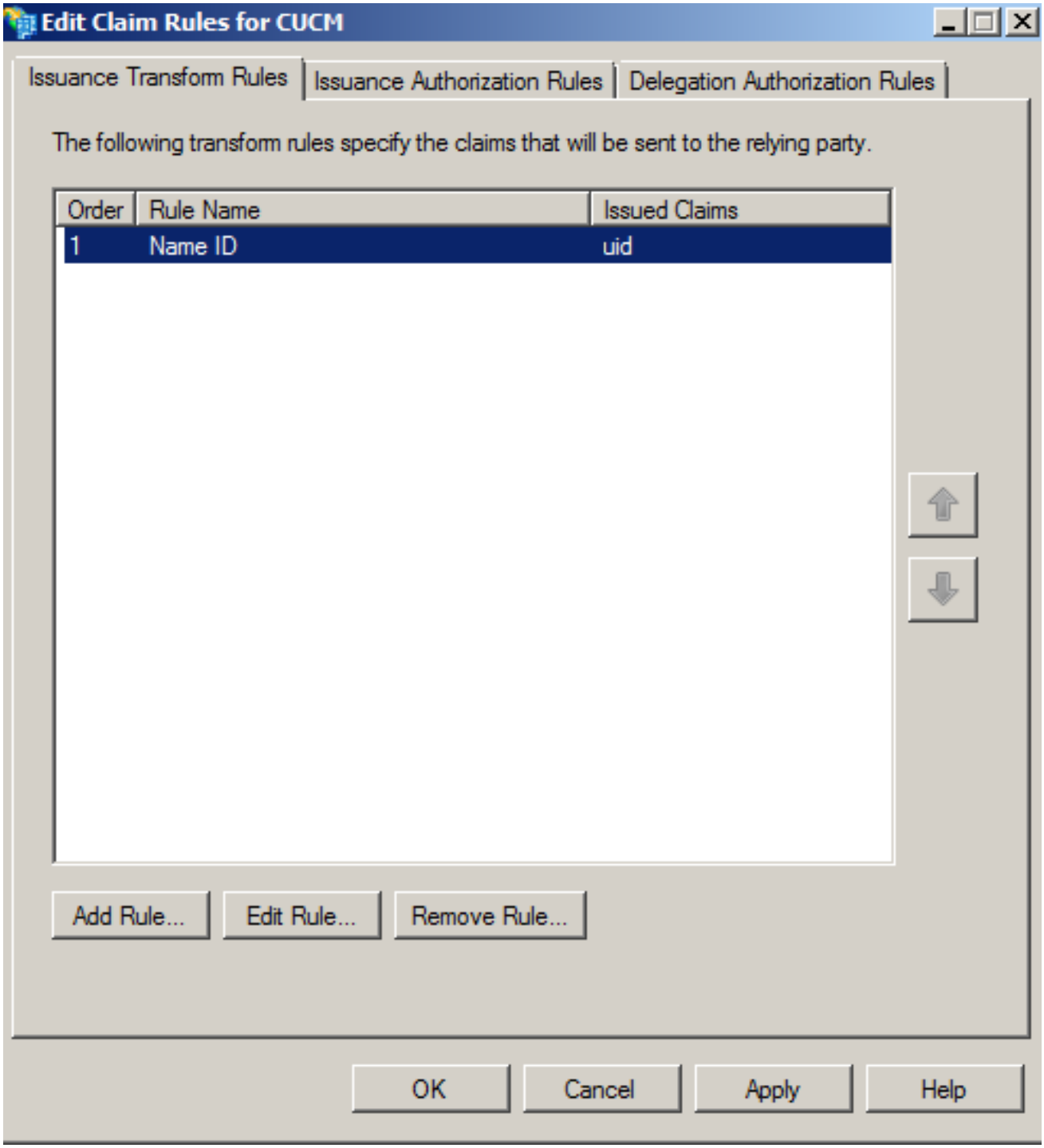


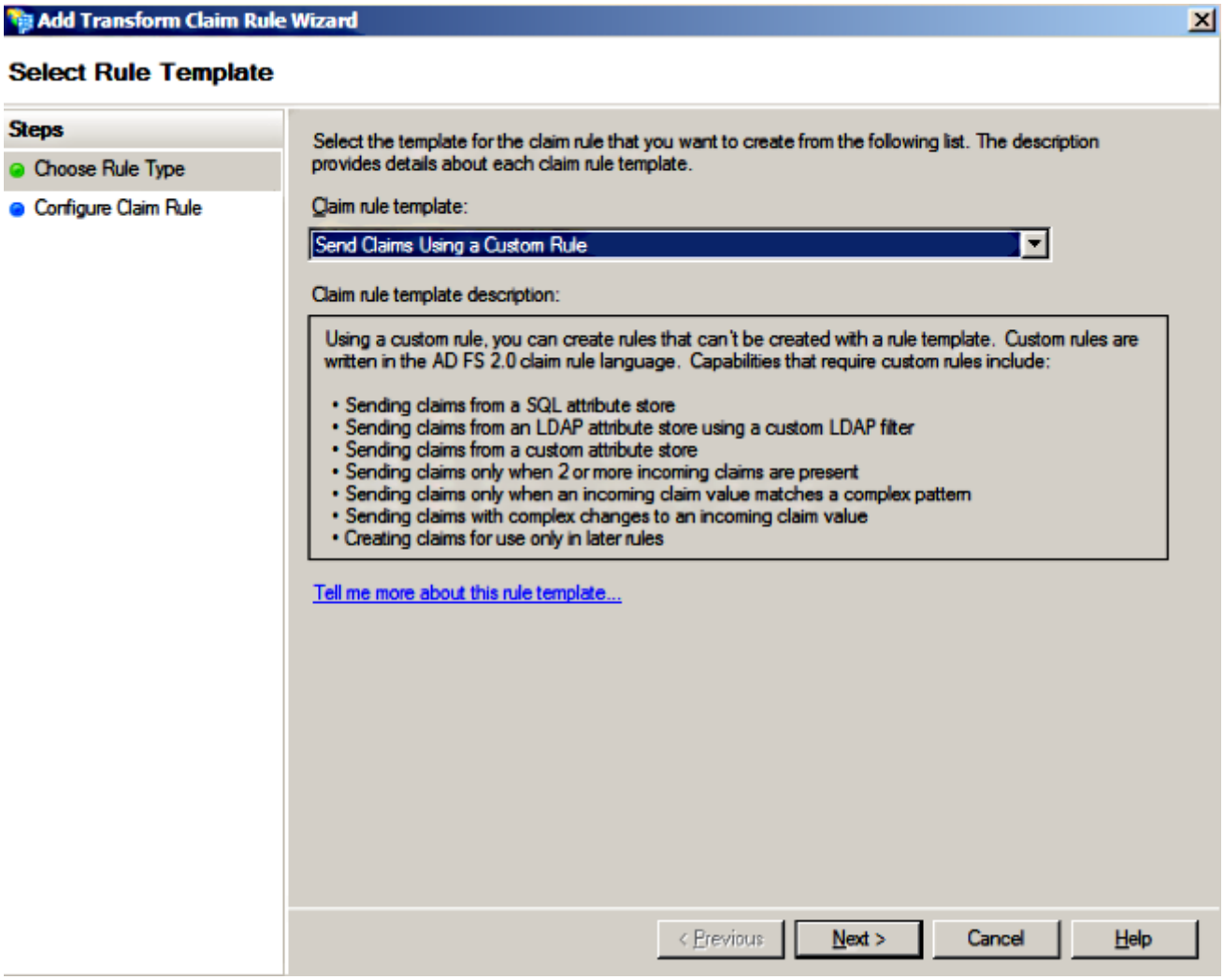
10. Typ in de regel Configureren de naam van de Claim Rule, selecteer **Actieve Map** als de winkel van Kenmerken, stel **LDAP-kenmerk** en **Uitgaande claimtype in** zoals in deze afbeelding weergegeven en klik op **Voltooien**.

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



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

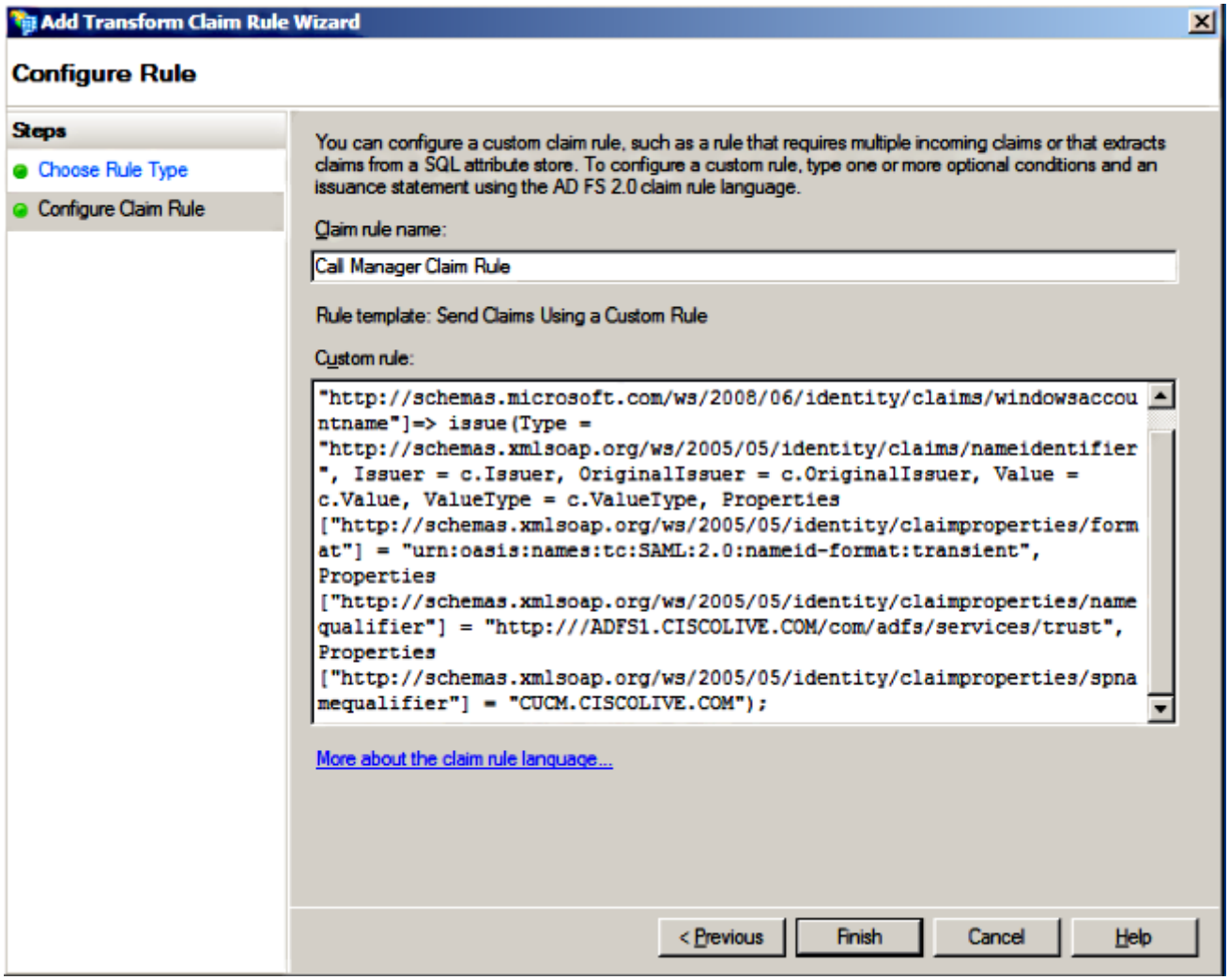

Edit Claim Rules for CUCM
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
The following transform rules specify the claims that will be sent to the relying party.
Order
Rule Name
Issued Claims
1
Name ID
uid
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply
Help



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.**

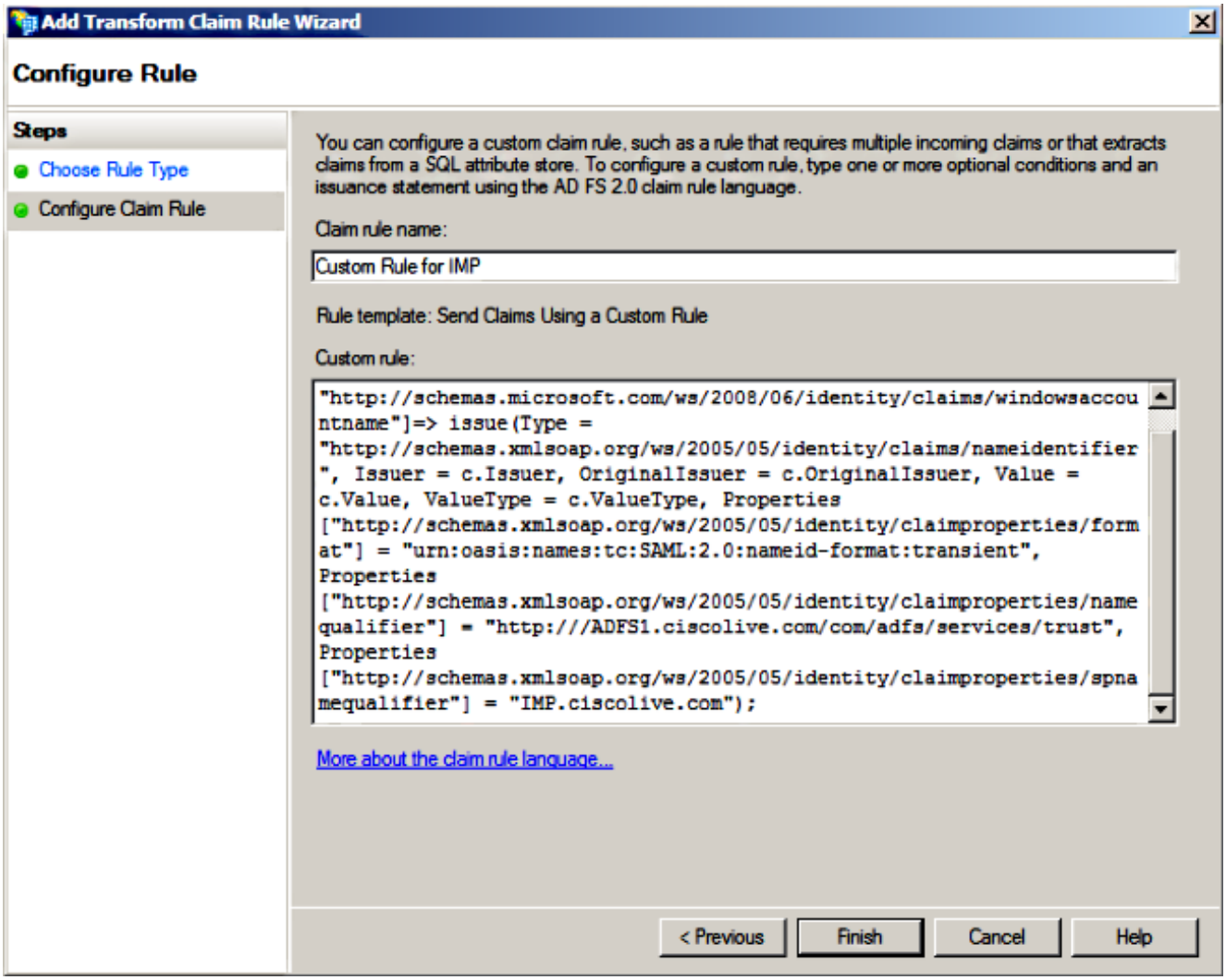
15. Start de AD FS versie 2.0 opnieuw vanaf **Services.msc**.

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.

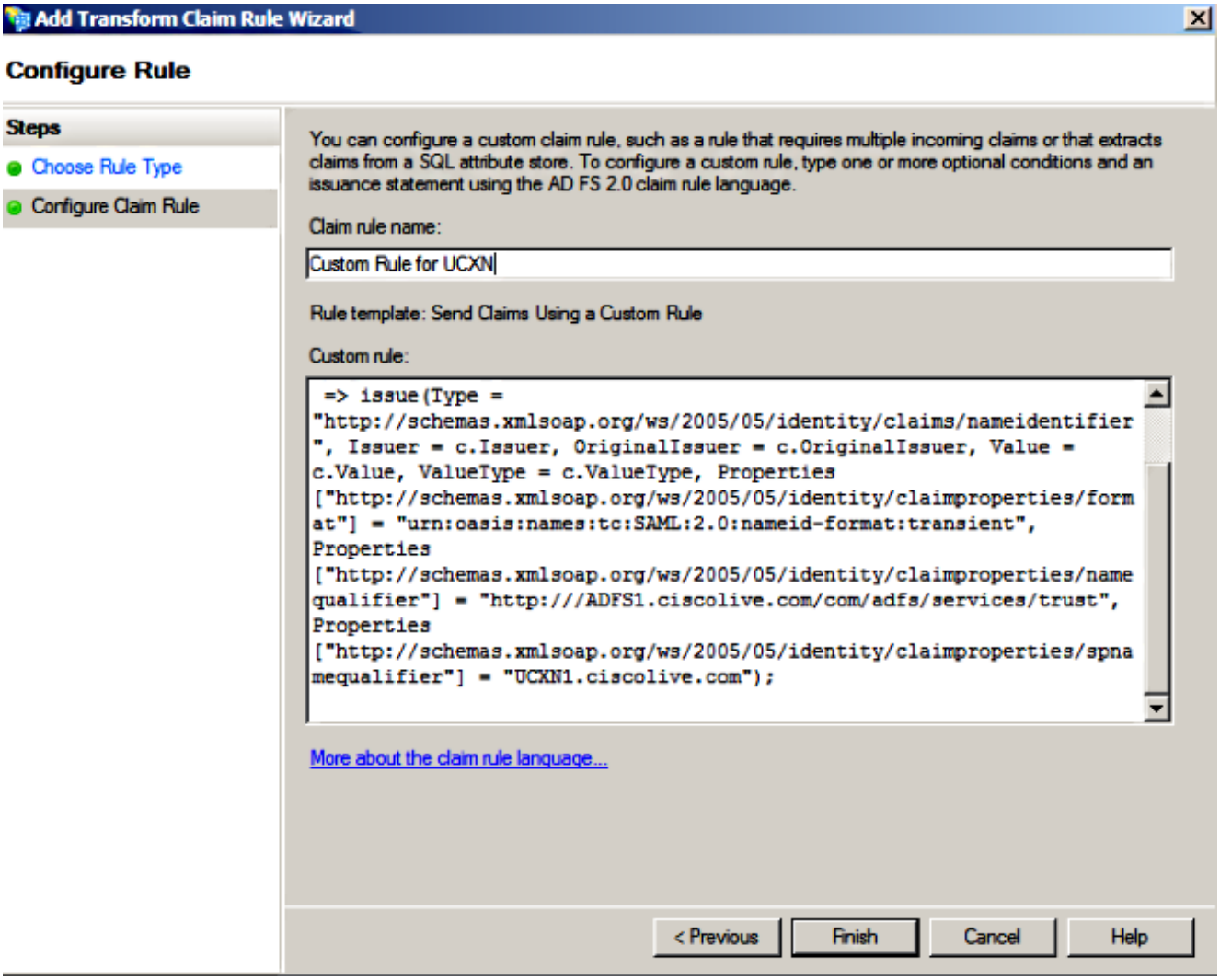
3. Klik op **Voltooien**.
4. Klik op **Toepassen** en vervolgens op **OK.**
5. Start de AD FS versie 2.0 opnieuw vanaf **Services.msc.**

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 **Voltooien**.

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

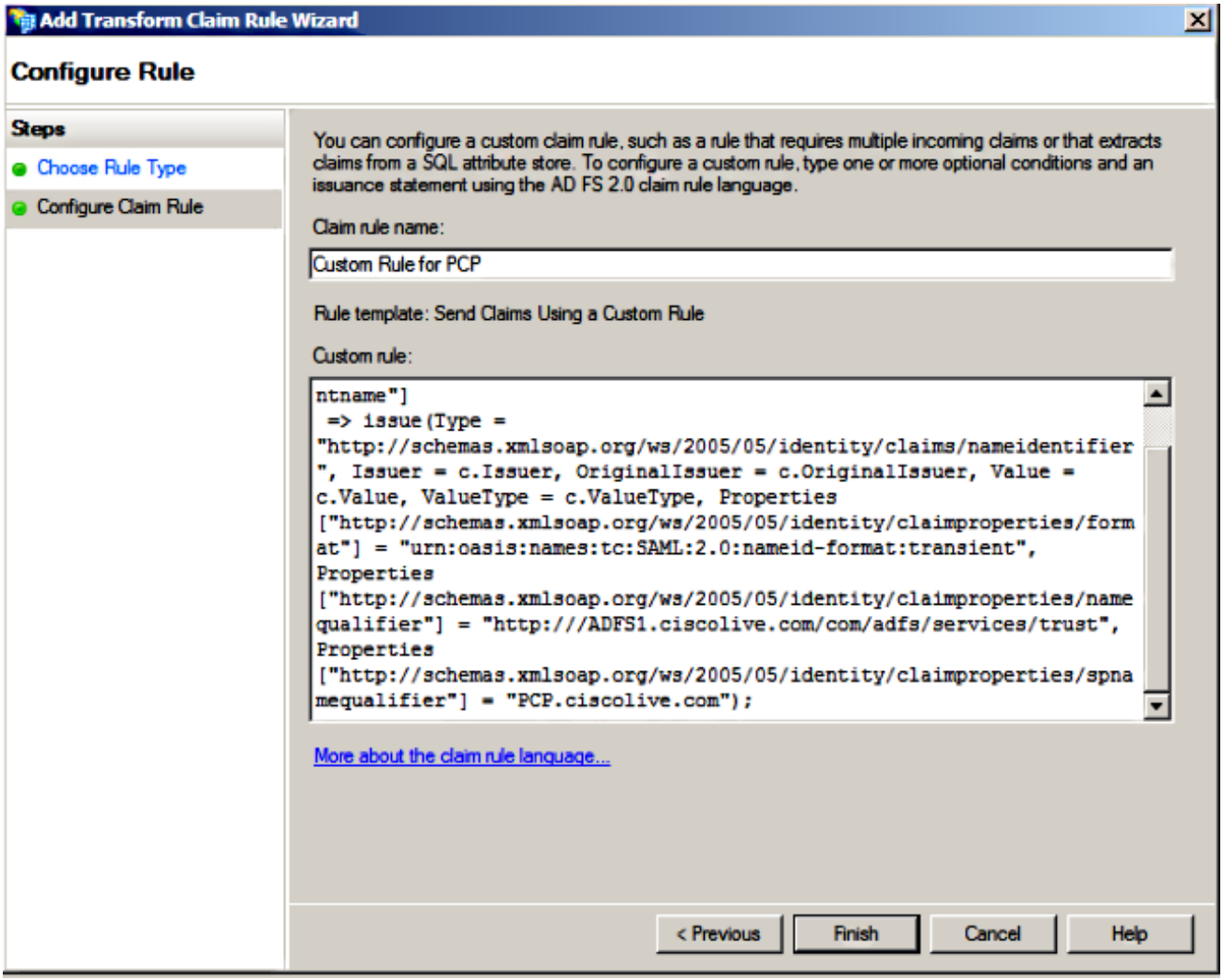
5. Start de AD FS versie 2.0 opnieuw vanaf **Services.msc.**

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>");
```



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