

Configureer één SAML-verbinding/overeenkomst per cluster met ADSL versie 2.0

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Stap 1: Exporteren van SP-metagegevens uit CUCM](#)

[Stap 2: IDP-metagegevens van AD FS downloaden](#)

[Stap 3. Voorziening-ID](#)

[Stap 4: SAML SSO inschakelen](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u de verbinding/overeenkomst per cluster met Active Directory Federation Service (AD FS) kunt configureren (SAML) Identity Provider (IDP).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Communications Manager (CUCM) 11.5 of hoger
- Cisco Unified Communications Manager IM and Presence versie 11.5 of hoger
- Active Directory Federation Service versie 2.0

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Active Directory Federation Service versie 2.0 als IDP
- Cisco Unified Communications Manager versie 11.5
- Cisco IM and Presence Server versie 11.5

Achtergrondinformatie

Voor SAML SSO moet een vertrouwenscirkel zijn tussen de serviceproviders (SP) en de IDP. Dit

vertrouwen wordt gecreëerd als onderdeel van SSO Enablement, wanneer trust (metagegevens) wordt uitgewisseld. Download de metagegevens van CUCM en uploadt deze naar IDP, en download de metagegevens van IDP eveneens en uploadt deze naar CUCM.

Eerder CUCM 11.5, het oorsprong knooppunt, genereert het metagegevensbestand en verzamelt ook de metagegevensbestanden van andere knooppunten in het cluster. Het voegt alle metagegevensbestanden aan één zip-bestand toe en legt deze vervolgens voor aan de beheerder. Administrator moet dit bestand opheffen en alle bestanden op de IDP zetten. Bijvoorbeeld, 8 metagegevensbestanden voor een 8 knooppunt cluster.

Eén SAML IDP-verbinding/overeenkomst per clusterfunctie wordt geïntroduceerd vanaf 11.5. Als onderdeel van deze functie genereert CUCM één metagegevensbestand voor serviceproviders voor alle CUCM- en IMP-knooppunten in de cluster. Het nieuwe naamformaat voor het metagegevensbestand is **<hostname>-single-agreement.xml**

Eén knooppunt maakt de metagegevens en duwt het naar andere SP-knooppunten in de cluster. Dit maakt het mogelijk voorzieningen, onderhoud en beheer te vergemakkelijken. Bijvoorbeeld, 1 meta-gegevensbestanden voor een 8 knooppunt cluster.

Het cluster brede metagegevensbestand maakt gebruik van een multiserver-to-cat-certificaat dat garandeert dat het sleutelpaar ook wordt gebruikt voor alle knooppunten in de cluster. Het metagegevensbestand heeft ook een lijst van Assertion Consumer Service (ACS) urls voor elke knooppunten in het cluster.

CUCM en Cisco IM and Presence versie 11.5 Ondersteunt zowel de SSO-modellen, de **clusterbrede** (één metagegevensbestand per cluster) en per knooppunt (bestaand model).

Dit document beschrijft hoe de clusterbrede modus van de SAML SER met AD FS 2.0 moet worden configureren.

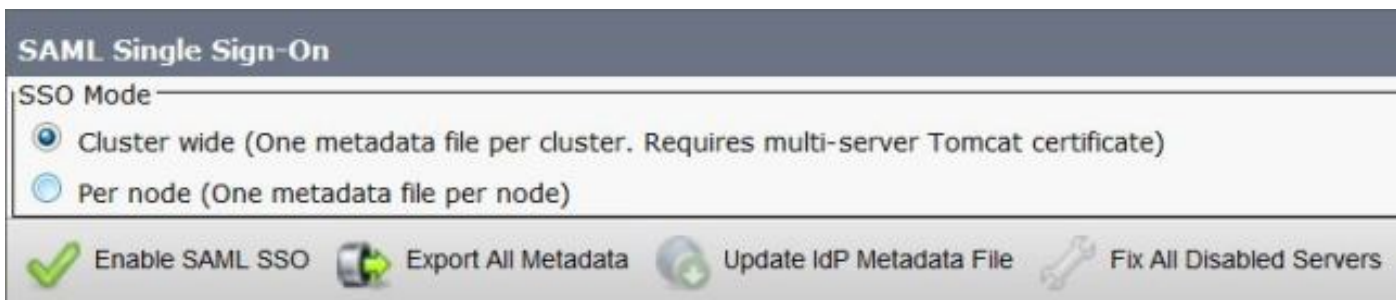
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Stap 1: Exporteren van SP-metagegevens uit CUCM

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

Standaard wordt **Cluster Wide** radioknop geselecteerd. Klik op **Exporteren alle metagegevens**. Het metagegevensbestand dat aan de beheerder wordt gepresenteerd onder de naam **<hostname>-single-agreement.xml**

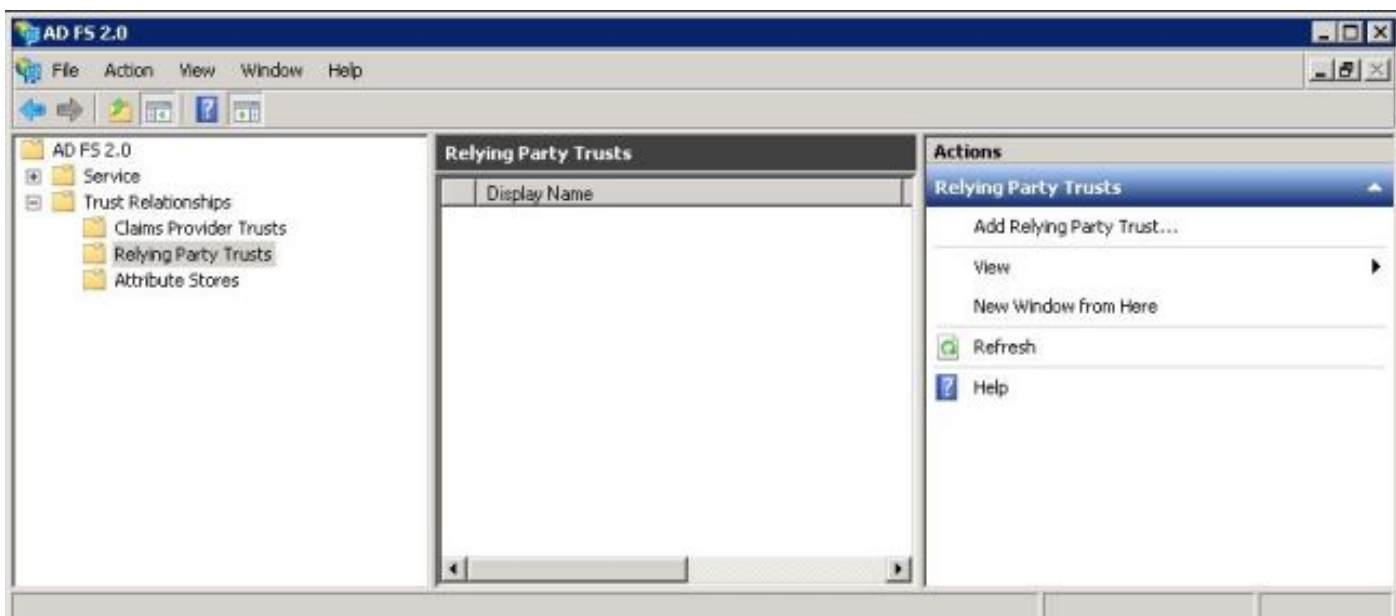


Stap 2: IDP-metagegevens van AD FS downloaden

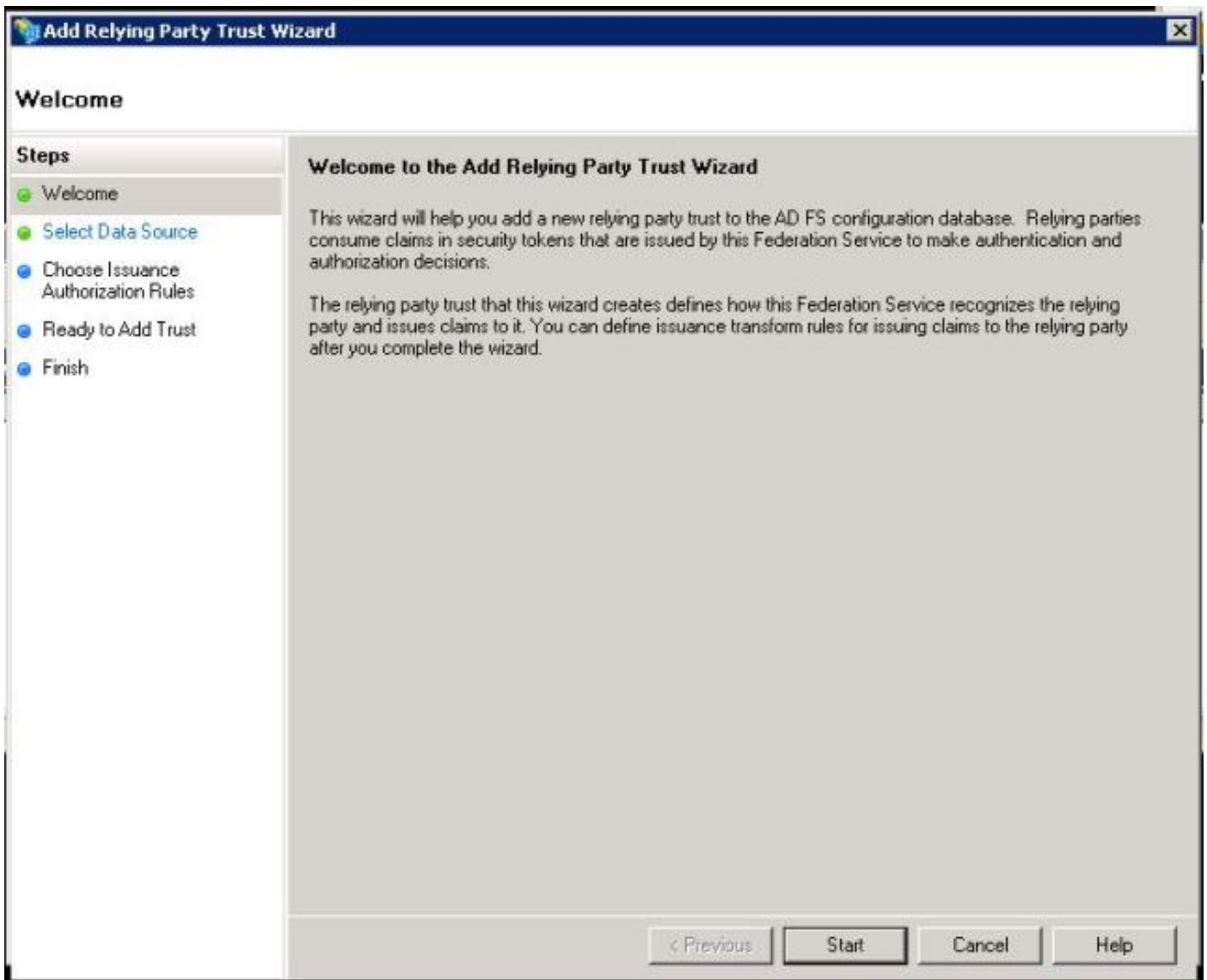
Raadpleeg de link [https:// <FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml](https://<FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml) om IDP-metagegevens te downloaden

Stap 3. Voorziening-ID

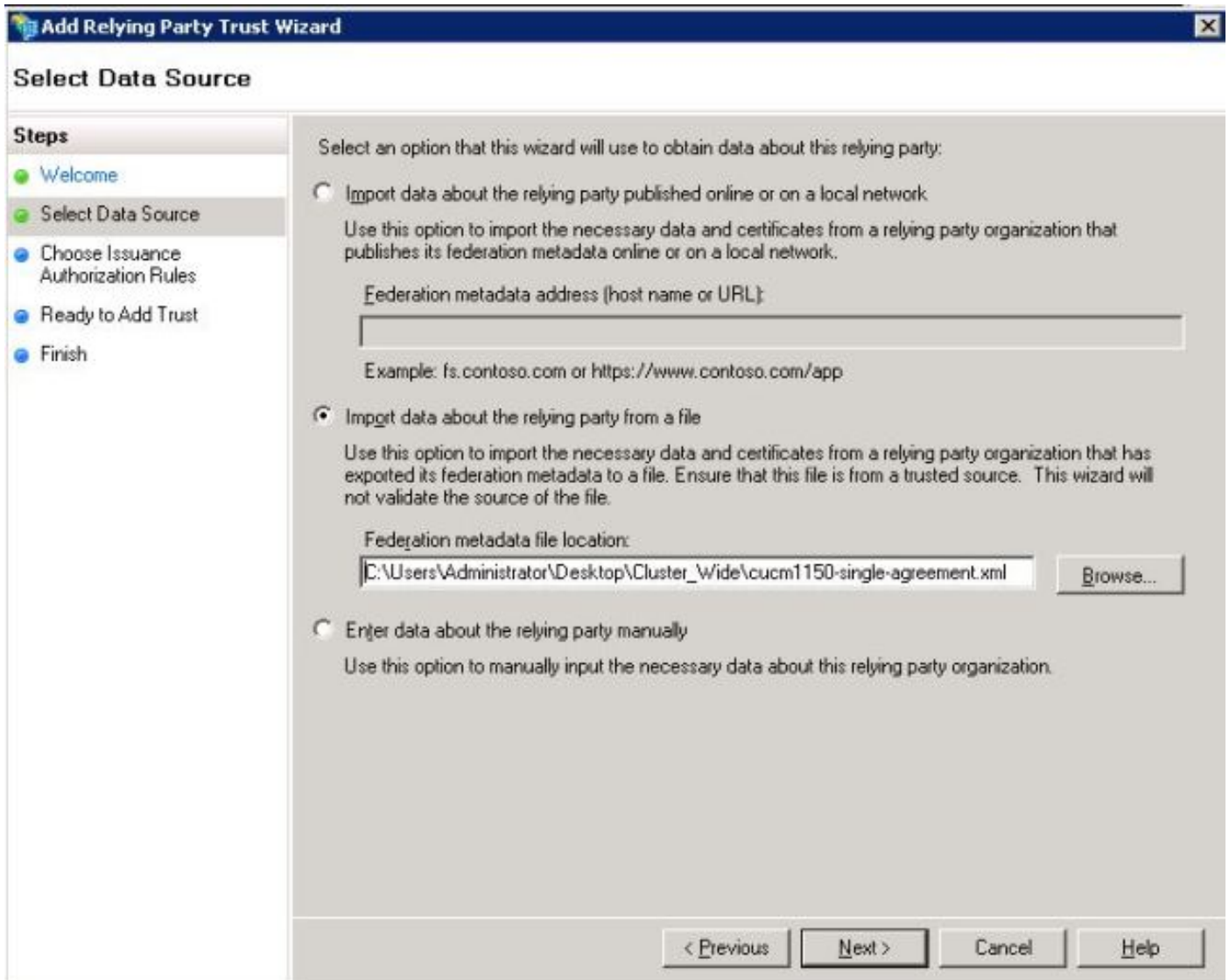
Zoals in de afbeelding wordt getoond, navigeer dan naar AD FS 2.0 Management/Trust Relationships/Relying Party trust. Klik op Add Relying Party Trust.



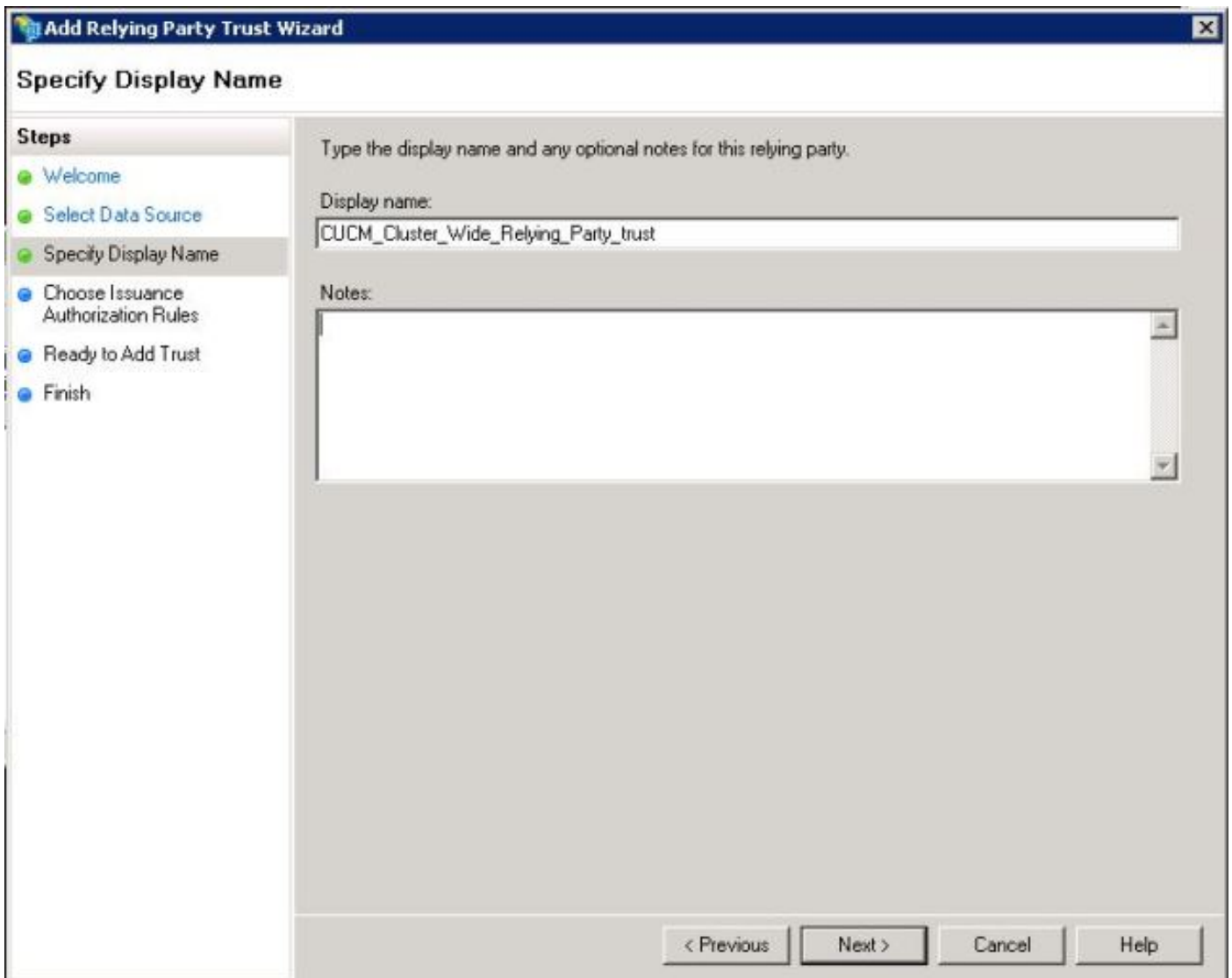
De wizard Vertrouwend maken wordt toegevoegd zoals in de afbeelding weergegeven. Klik nu op **Start**.



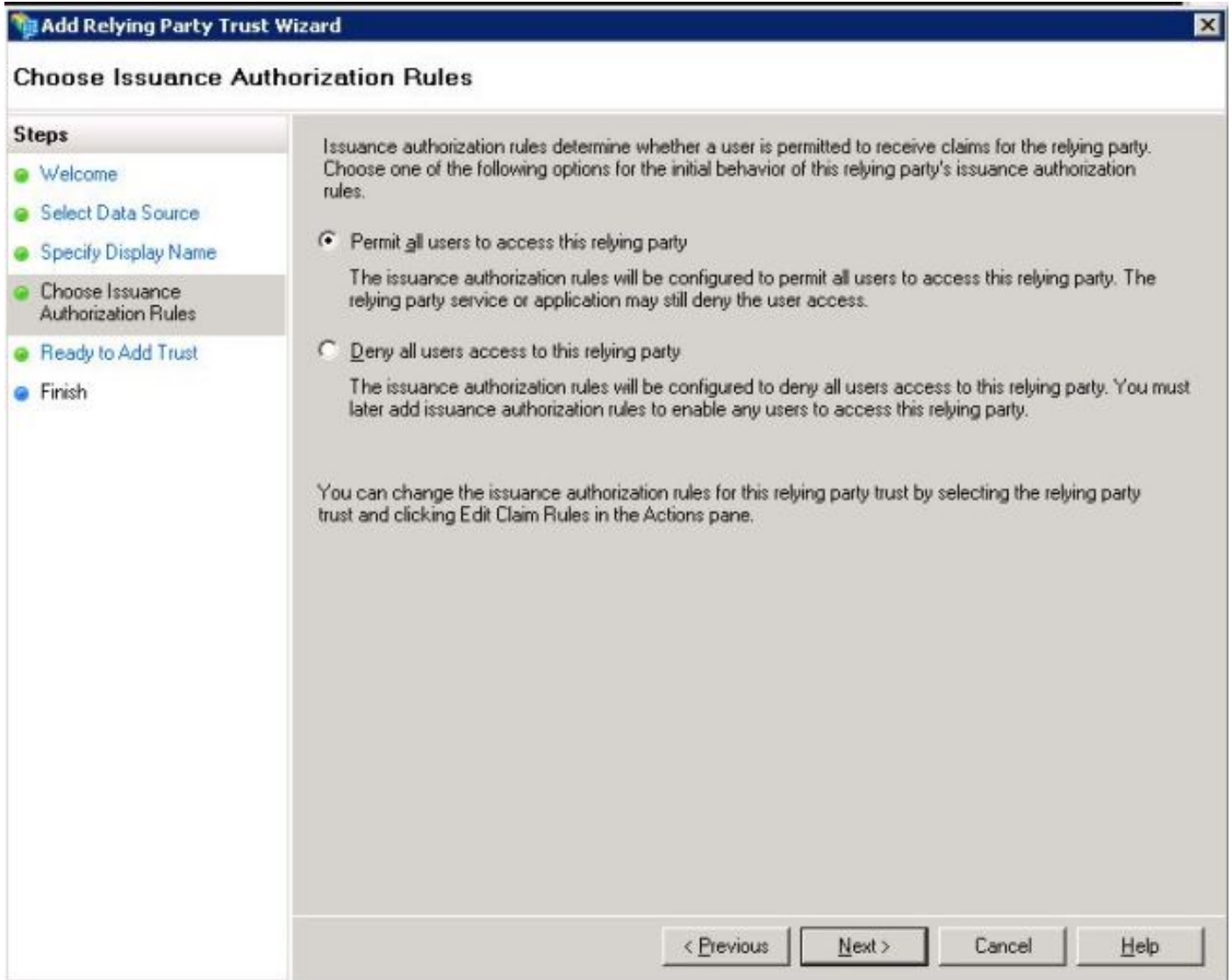
Klik de invoergegevens over het vertrouwen van een partij in een bestand aan. Bladeren de SP-metadata die zijn gedownload van de CUCM SAML SSO Configuration Pagina. Klik vervolgens op **Volgende**, zoals in de afbeelding weergegeven:



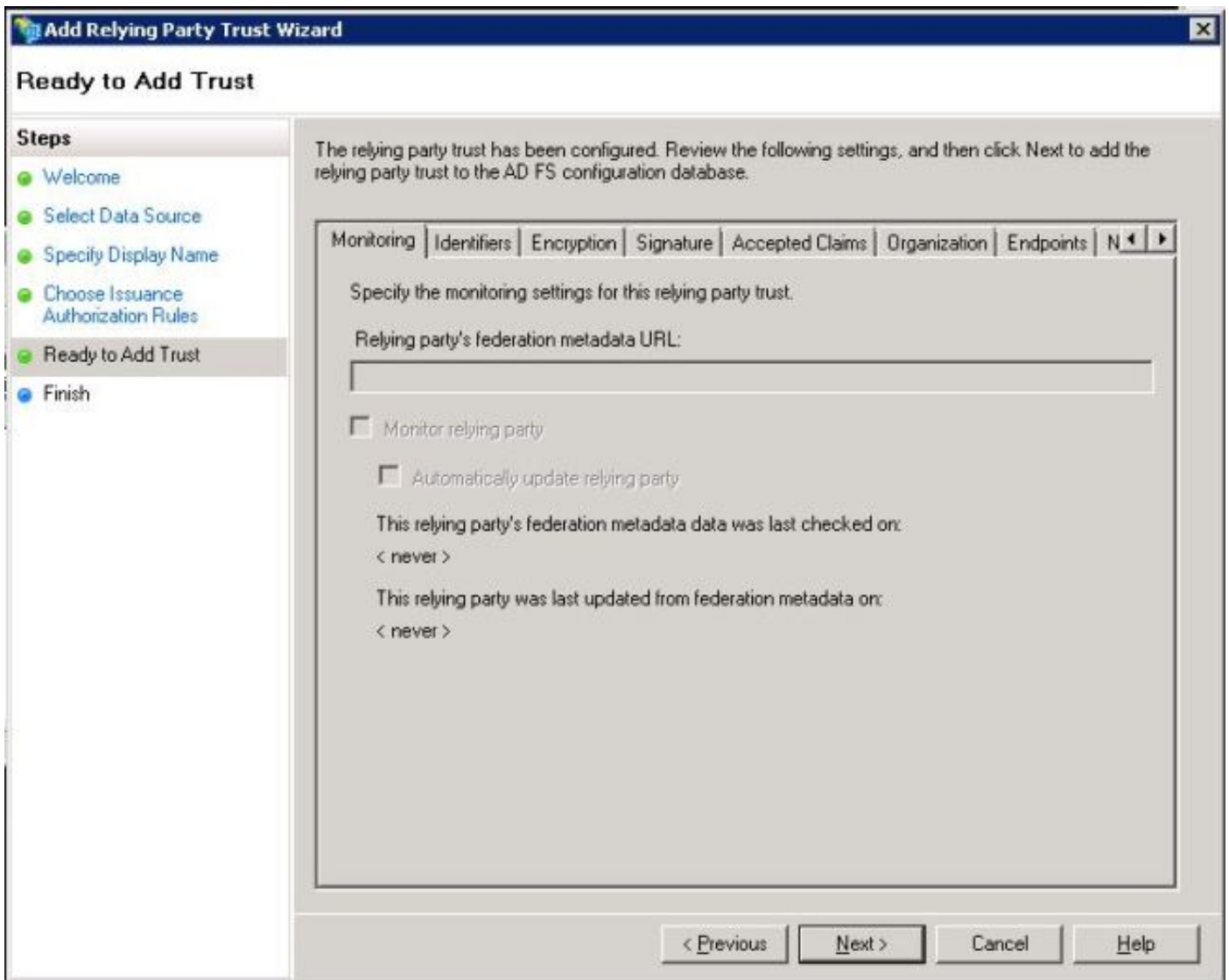
Typ de naam van het display en eventuele opmerkingen voor de betrokken partij. Klik op **Volgende.**, zoals in de afbeelding wordt weergegeven:



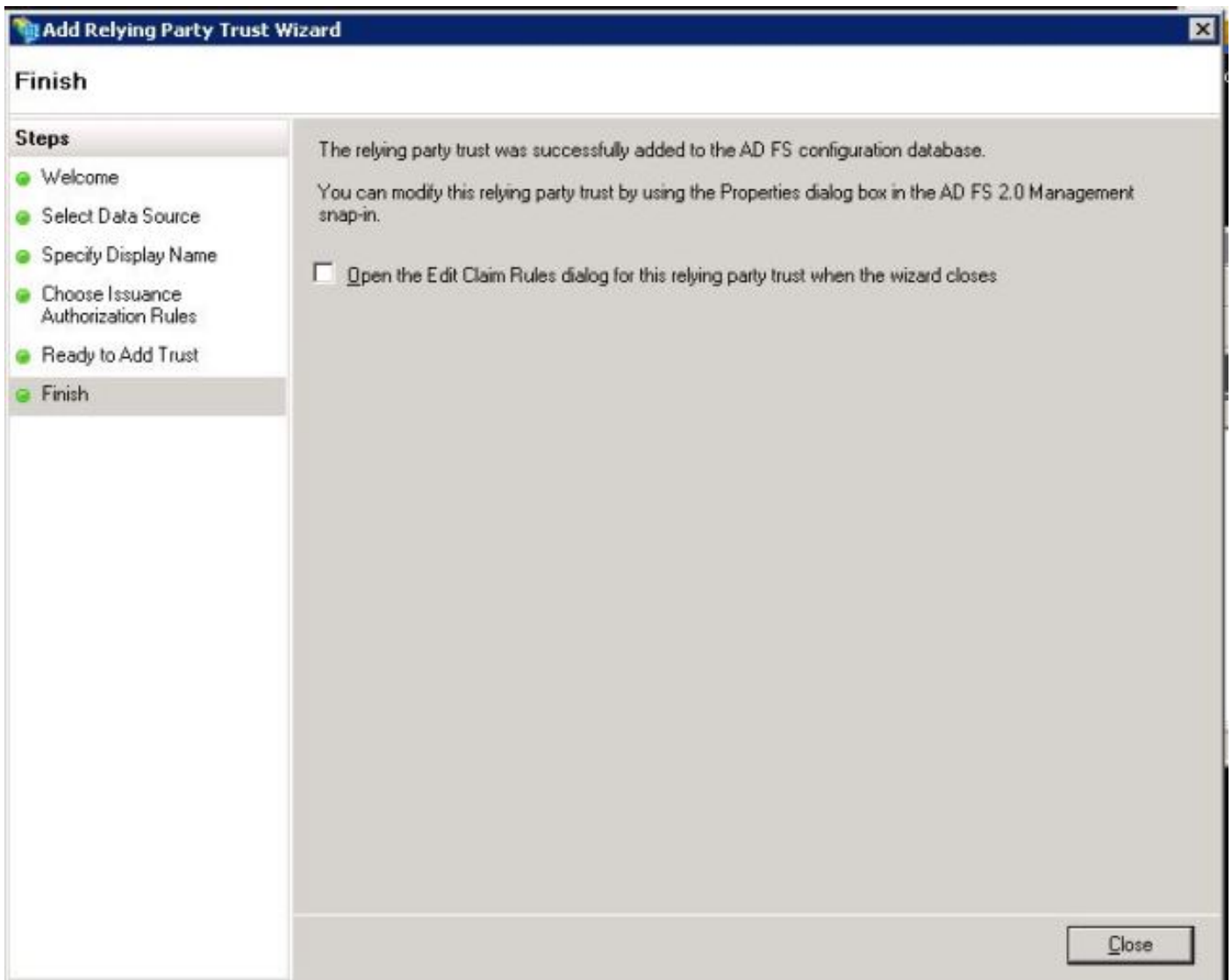
Selecteer **Toestaan alle gebruikers van deze vertrouwende partij** om alle gebruikers toe te staan om deze vertrouwende partij te benaderen en klik vervolgens op **Volgende**, zoals in de afbeelding:



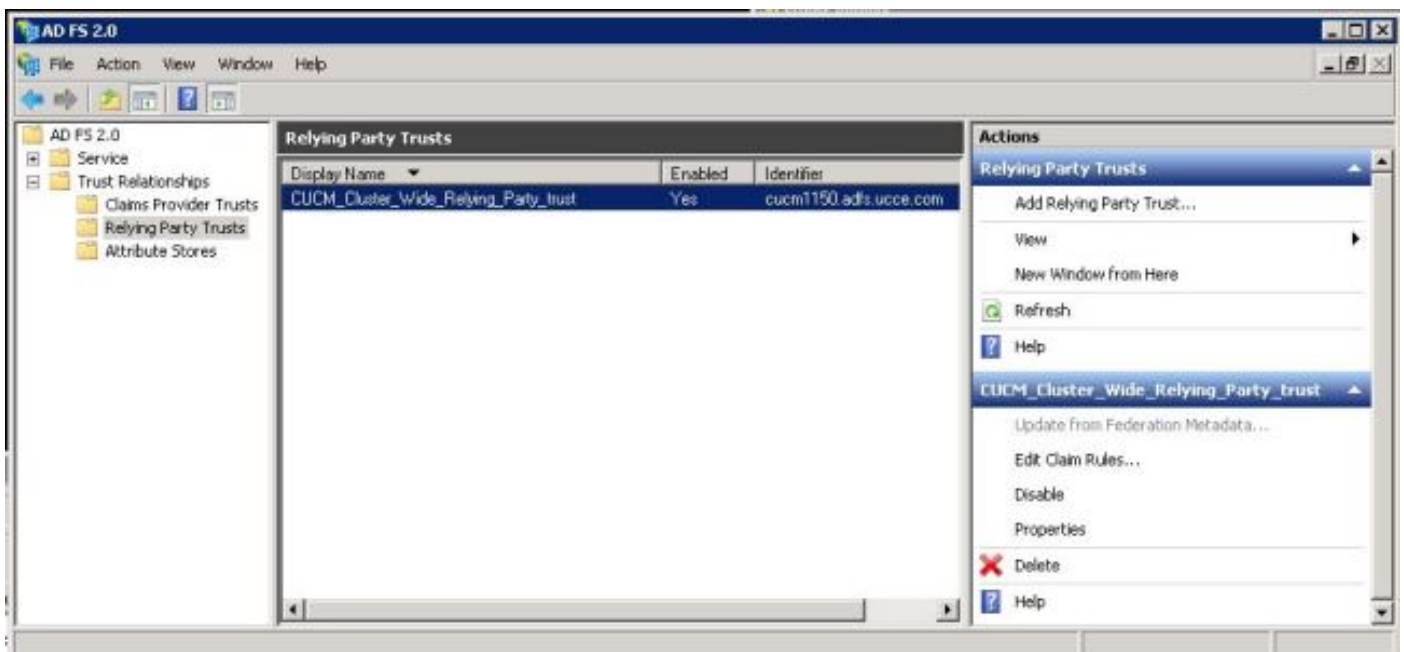
Onder **Ready to Add Trust** pagina, kunt u de instellingen voor het Relying Party Trust bekijken, die is geconfigureerd. Klik nu op **Volgende**, zoals in de afbeelding wordt weergegeven:



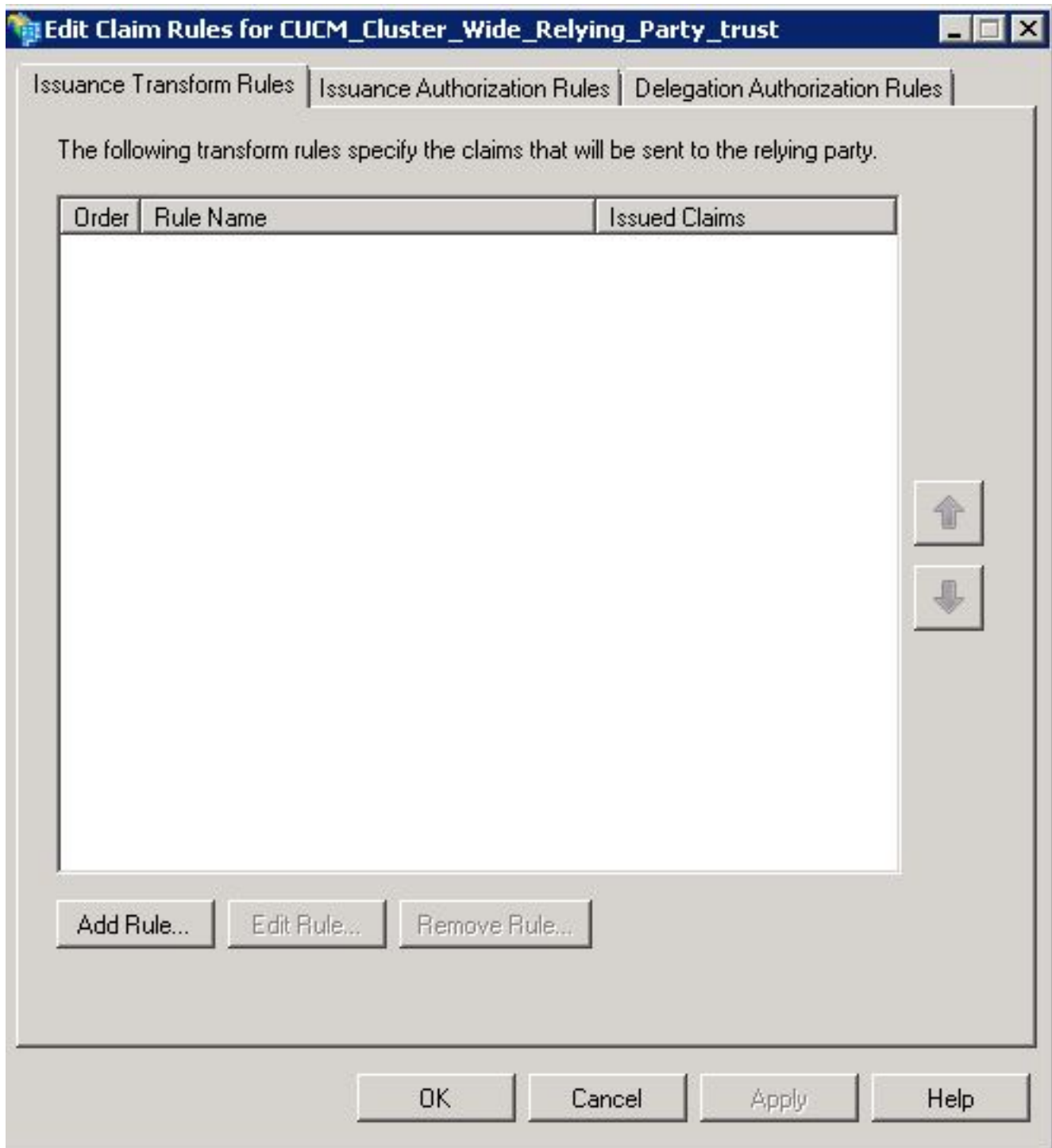
Finish Page bevestigt dat het vertrouwen van een betrouwbare partij met succes is toegevoegd aan de AD FS configuratie Database. Schakel het vakje uit en klik op **Sluiten**, zoals in de afbeelding wordt weergegeven:



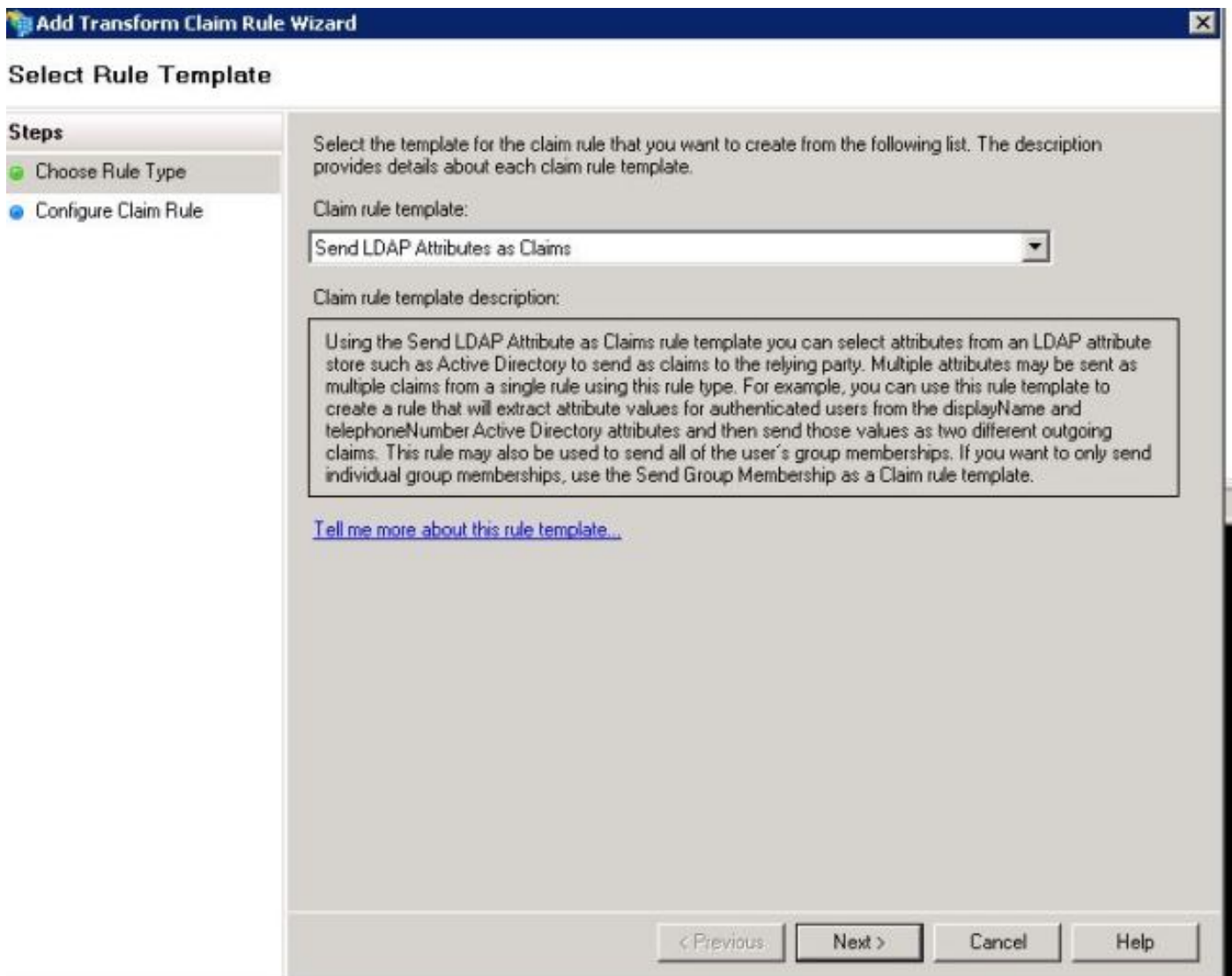
Klik met de rechtermuisknop op de **vertrouwenwekkende stoffen** van de **Betrouwer** en klik op **Bewerken** in de afbeelding.



Klik nu op **Add Rule** ., zoals getoond in de afbeelding:



Wanneer de regel **Eis toevoegen Omzetten** wordt geopend, klikt u op **Volgende** met de standaardclaimregelsjabloon **Verzend LDAP-kenmerken als claims**, zoals in de afbeelding wordt weergegeven:



Klik op **Claim Rule** zoals getoond in deze afbeelding. LDP-kenmerk moet overeenkomen met de LPDP-kenmerk in de configuratie van de LMBP-map in de CUCM. Uitgaande claim type als **uid** beheren. Klik op **Voltoeien**, zoals in de afbeelding wordt weergegeven:

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:

Rule template: Send LDAP Attributes as Claims

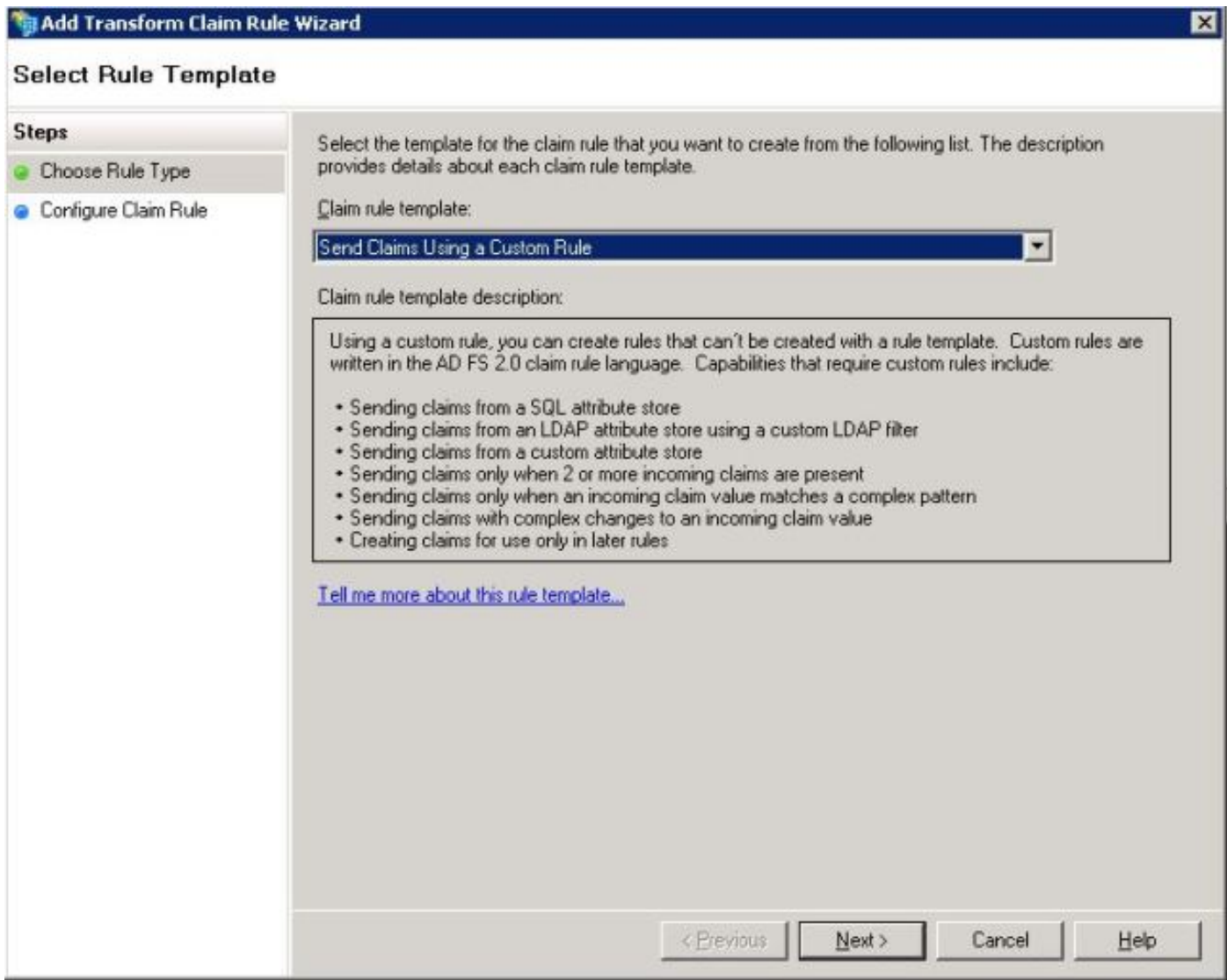
Attribute store:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
▶	<input type="text" value="SAM-Account-Name"/>	<input type="text" value="uid"/>
*	<input type="text"/>	<input type="text"/>

< Previous Finish Cancel Help

Voeg de aangepaste regel toe voor het vertrouwende partij. Klik op **Toevoegen**. Selecteer **Vorderingen verzenden met behulp van een Aangepaste regel** en klik vervolgens op **Volgende**, zoals in de afbeelding:

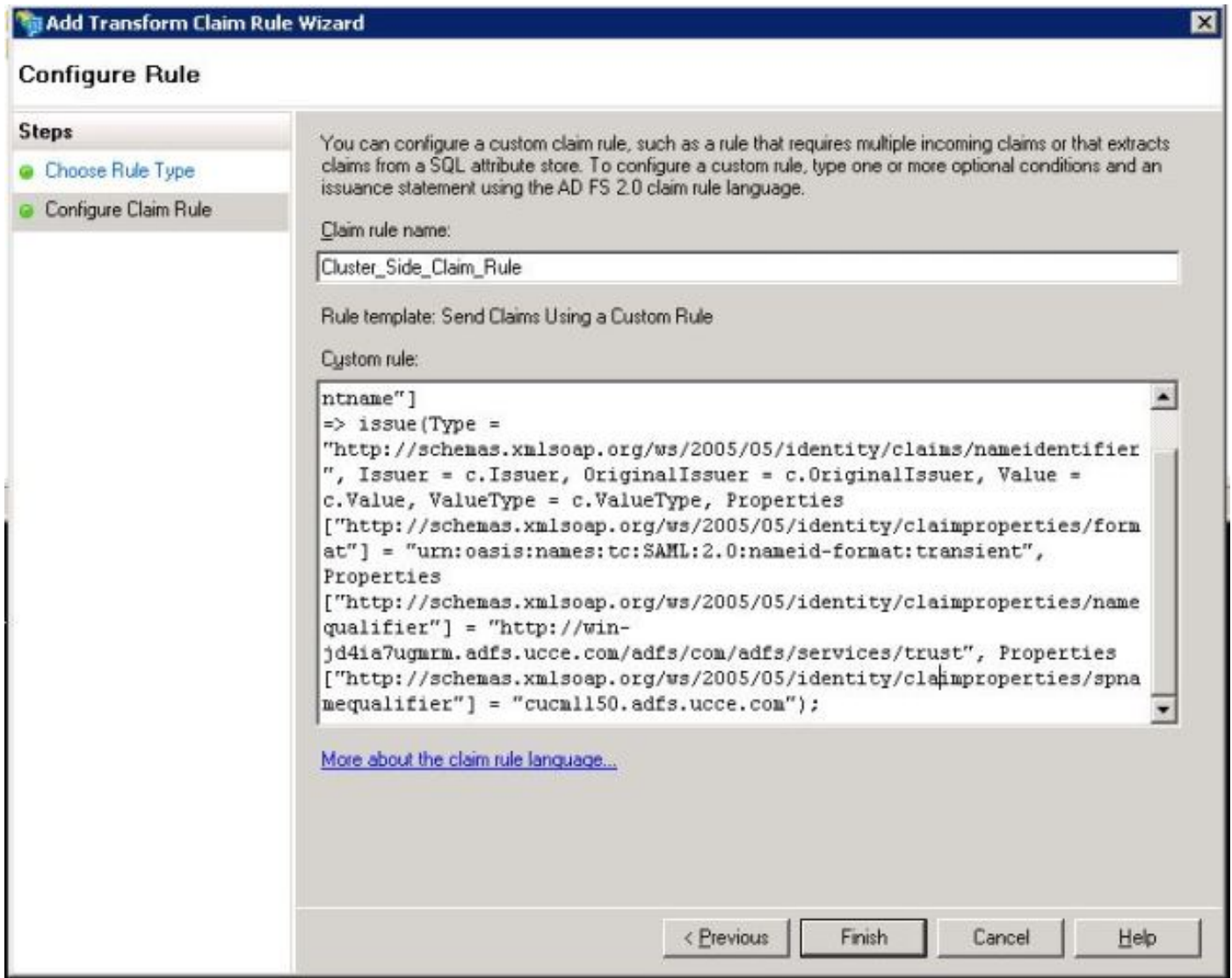


In het configureren van de regel typt u een naam van de regel van de claim en kopieert u vervolgens de regel van de claim in het veld Aangepaste regel in het veld Aangepaste regel in de wizard die de naam en de SPANNER-kwaliteit wijzigt in de regel van de claim. Klik op **Voltoeien**, zoals in de afbeelding wordt weergegeven:

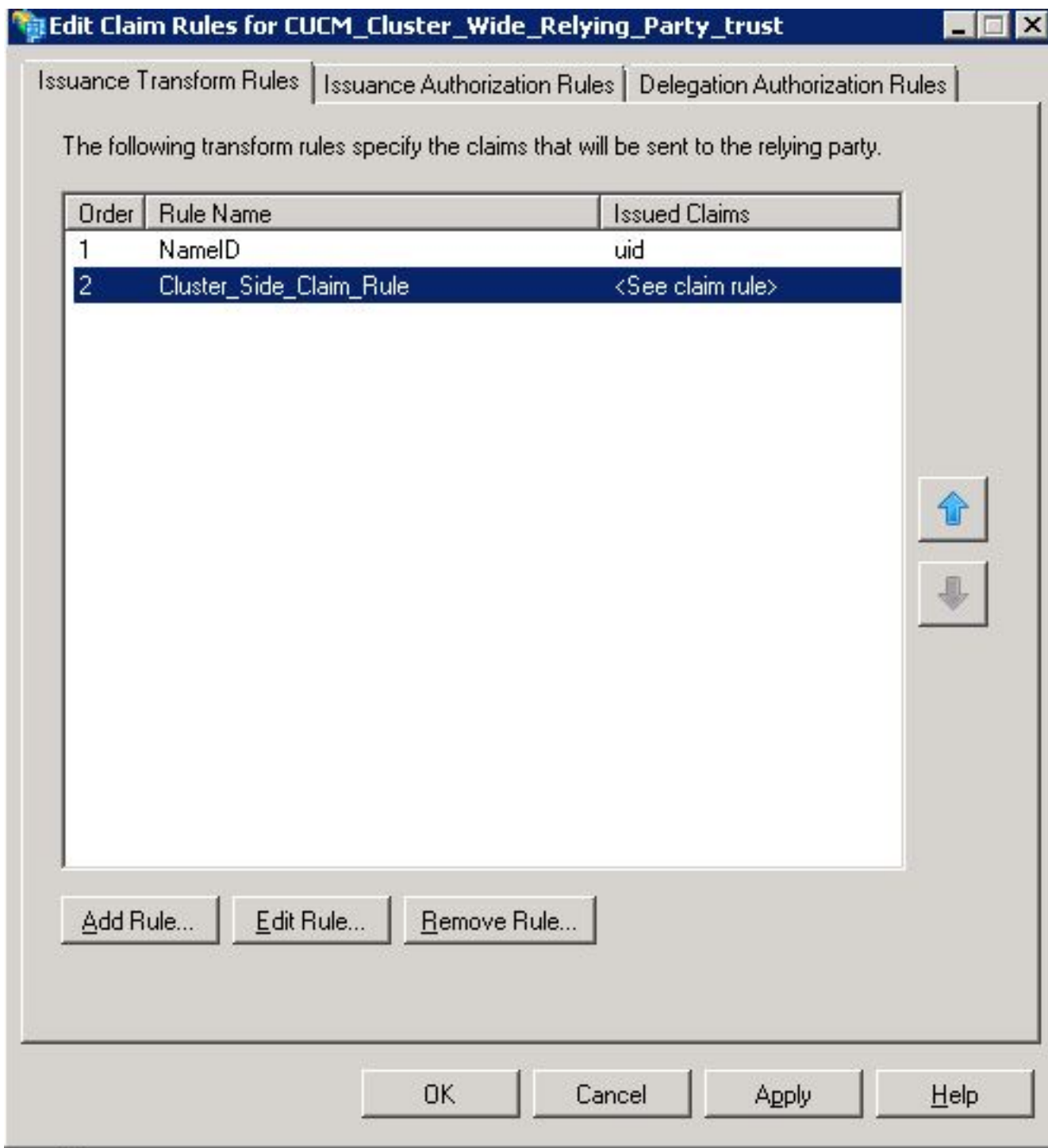
Eis:

```
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>/adfs/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"<Entity ID in the SP Metadata>");
```

Entity ID = Open the SP metadata and check the Entity ID. Basically, its the CUCM Publisher's FQDN.



Zoals in de afbeelding wordt weergegeven, klikt u op **Toepassen** en vervolgens **OK**.



Stap 4: SAML SSO inschakelen

Open een webbrowser, logt u in bij CUCM als beheerder en navigeer naar **System > SAML Single Sign On**.

Standaard wordt **Cluster Wide** radioknop geselecteerd. Klik op **SSO** inschakelen zoals in de afbeelding:

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)

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

Zoals in de afbeelding wordt getoond, waarschuwt het pop-up de waarschuwing voor het opnieuw opstarten van een webserver en informatie om de clusterbrede SAML SSO of Per-Node SAML SSO naar gelang idp te kiezen. Klik op **Doorgaan**.

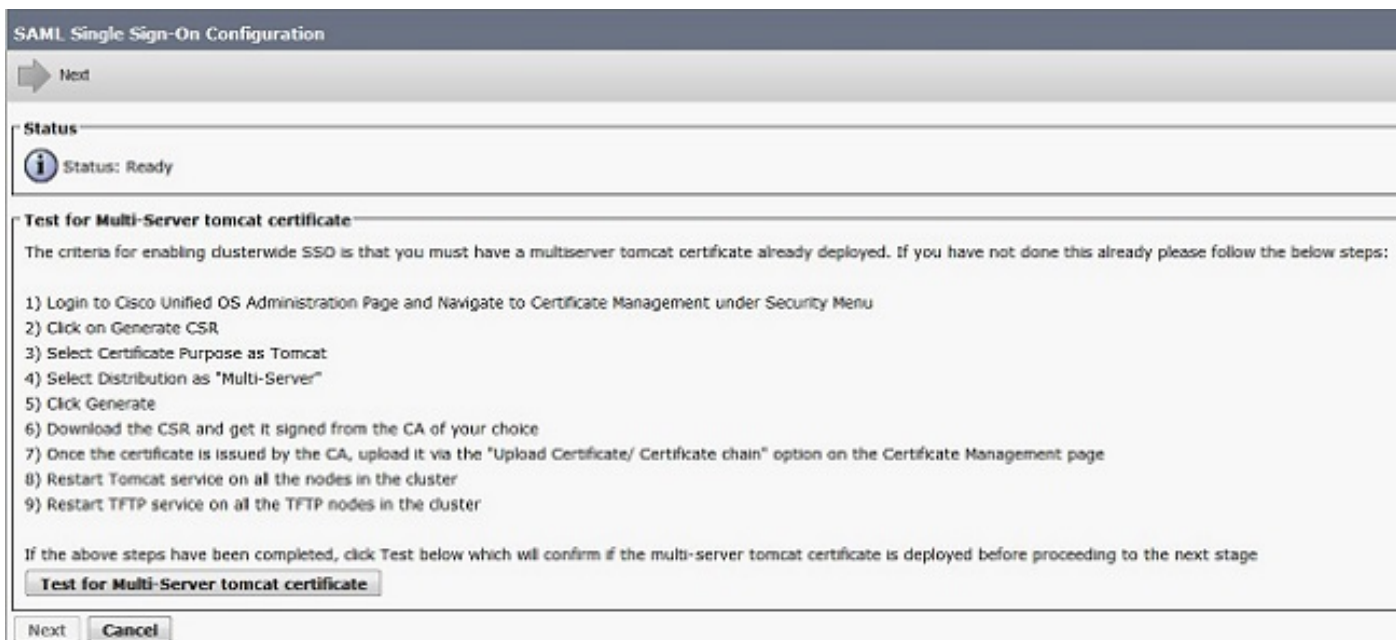
 **Web server connections will be restarted**

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.

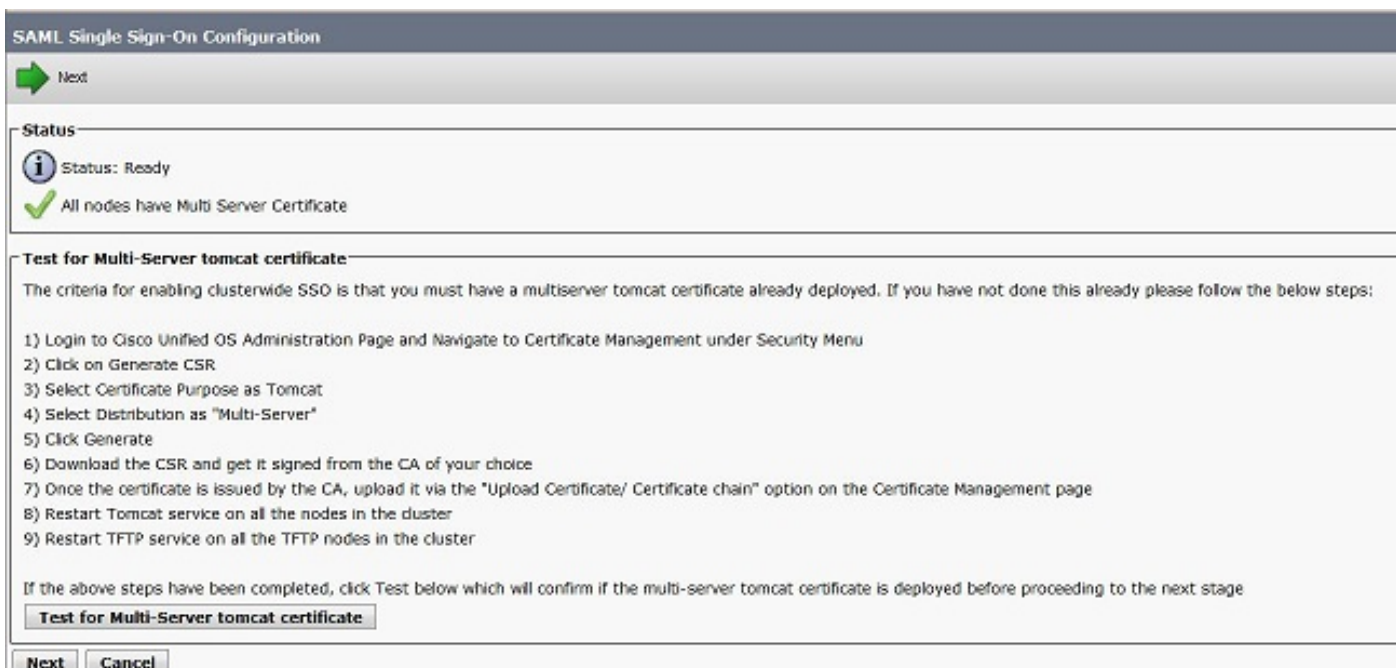
 **Click "Export All Metadata" button**

If the server metadata has not already been uploaded to the IdP, it can be done before running the wizard. You can obtain the server metadata by clicking the "Export All Metadata" button on the main page. Then go to the IdP and upload the file.
If IDP is provisioned with cluster-wide SP metadata, you need to enable cluster-wide SAML SSO. If IDP is provisioned with per-node SP metadata, you need to enable per-node SAML SSO.

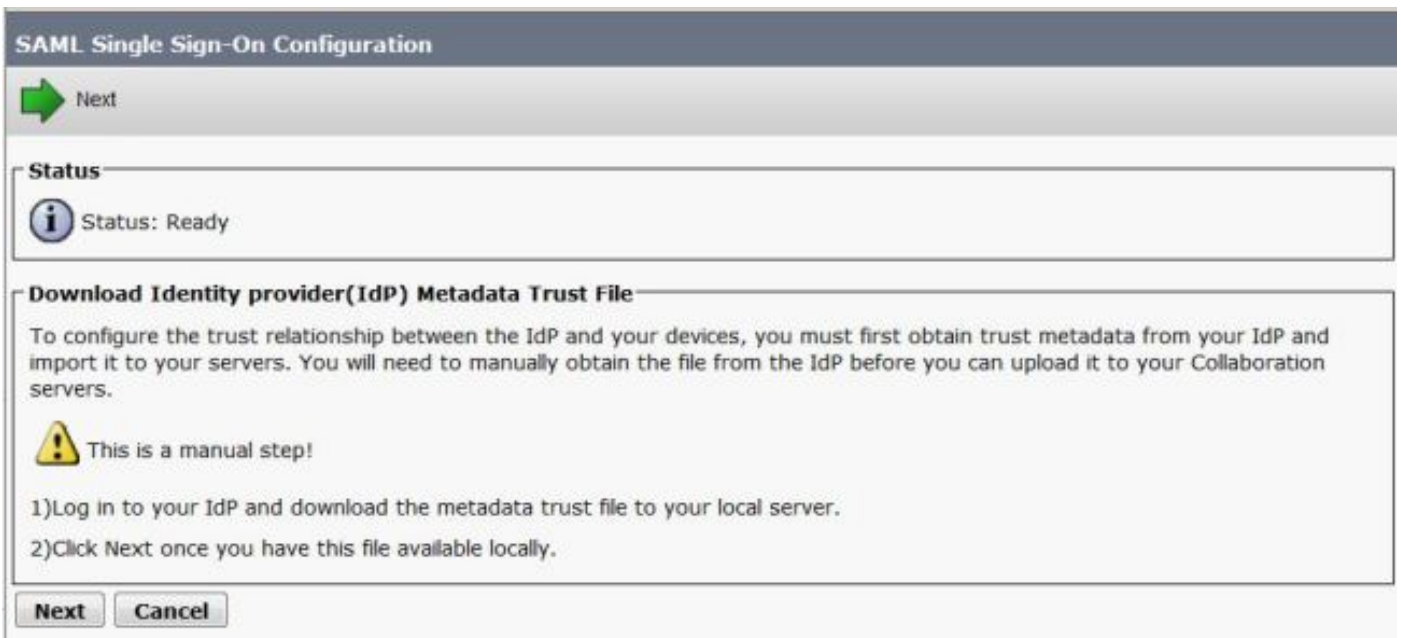
De criteria om voor een Cluster-brede SSO beschikbaar te maken zijn dat u een multiserver-tomatecertificaat moet hebben dat al is ingevoerd. Klik op **Test voor Multi-Server om certificaat te verkrijgen**, zoals in de afbeelding wordt getoond:



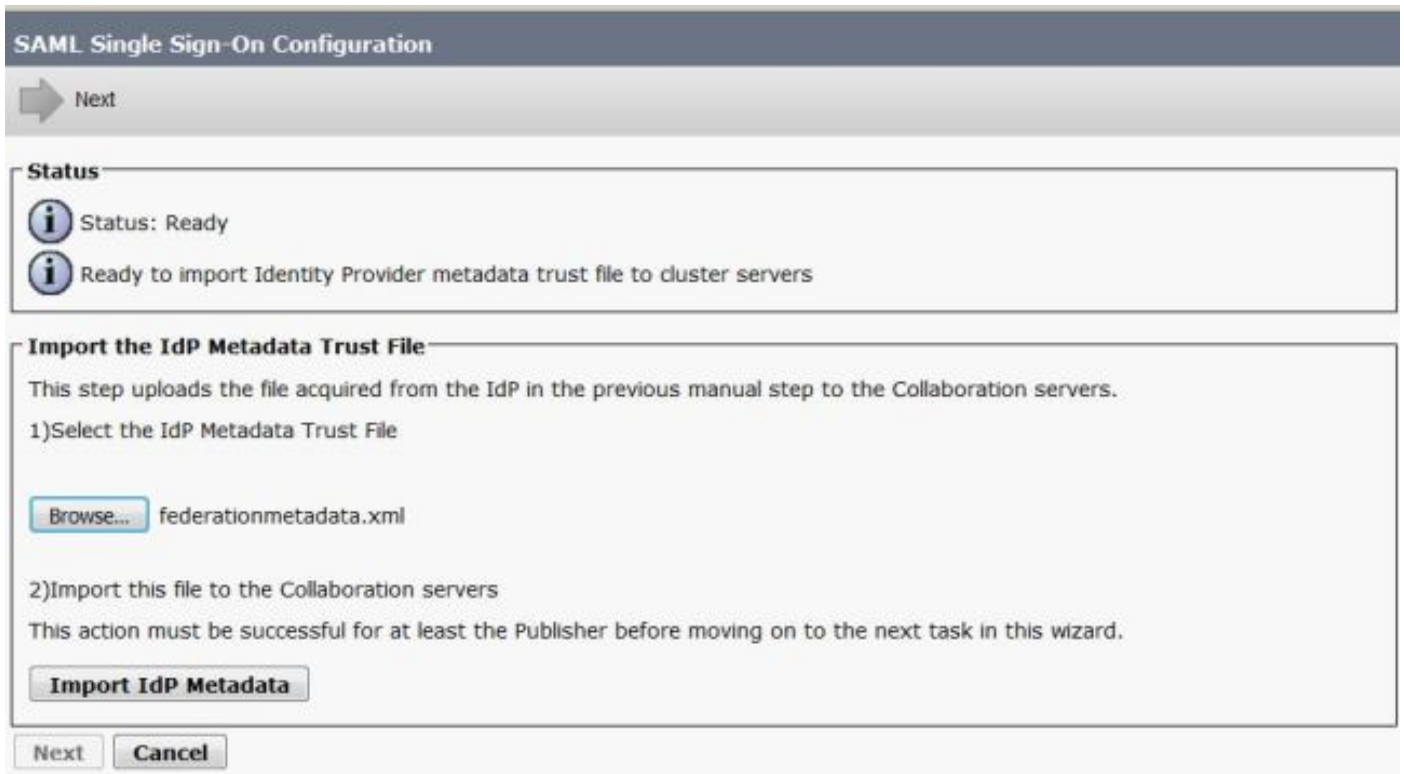
Zodra dit bevestigd is, hebben alle knooppunten een multi-server certificaat weergegeven en hebben alle knooppunten een multi-server certificaat en klikt u vervolgens op **Volgende**, zoals in de afbeelding:



Klik op **Volgende** zoals in de afbeelding.



Bladeren en selecteer de gedownload IDP-metadatas. Klik op **de Metagegevens van IDP importeren**, zoals in de afbeelding wordt getoond:



De pagina bevestigt dat Importeren voor alle servers is gelukt en vervolgens op **Volgende** klikt, zoals in de afbeelding:

SAML Single Sign-On Configuration

Next

Status

- Status: Ready
- Import succeeded for all servers

Import the IdP Metadata Trust File

This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.

1) Select the IdP Metadata Trust File

Browse... No file selected.

2) Import this file to the Collaboration servers

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

Import IdP Metadata

Import succeeded for all servers

Next Cancel

Zoals in de afbeelding wordt getoond, klikt u op **Volgende**, aangezien de SSP-metagegevens al zijn geëxporteerd vanuit de oorspronkelijke SAML SETH-configuratiescherm.

SAML Single Sign-On Configuration

Back Next

Status

- Status: Ready
- If Admin has already uploaded the server metadata to IdP then skip the steps below and click Next. Otherwise follow the steps below to upload the server metadata to IdP
- IdP Metadata has been imported to servers in this cluster

Download Server Metadata and install on the IdP

Download the metadata trust file from Collaboration servers and manually install it on the IdP server to complete SSO setup.

1) Download the server metadata trust files to local storage

Download Trust Metadata File

! This is a manual step!


2) Log in to your IdP and upload the server metadata trust file.

3) Click Next once you have installed the server metadata on the IdP.


Back Next Cancel

CUCM moet in sync zijn met de LDAP-map. De wizard geeft de geldige beheerder aan die in de LDAP-map is ingesteld. Selecteer de gebruiker en klik op **Test SSO uitvoeren**, zoals in de afbeelding:

SAML Single Sign-On Configuration

 Back

Status

 The server metadata file must be installed on the IdP before this test is run.

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

samluser

2) Launch SSO test page

Voer, zoals in de afbeelding, de gebruiker-ID en het bijbehorende wachtwoord in nadat deze is gevraagd.

Authentication Required

 Enter username and password for <https://win-jd4ia7ugmrm.adfs.uce.com>

User Name:

Password:

De pop-up, zoals in de afbeelding wordt getoond bevestigt dat de test succesvol is.

SSO Test Succeeded!

Congratulations on a successful SAML SSO configuration test. Please close this window and click "Finish" on the SAML configuration wizard to complete the setup.

Close

Zoals in de afbeelding wordt weergegeven, klikt u op **Voltooien** om de configuratie voor het inschakelen van de SSO te voltooien.

The screenshot shows the 'SAML Single Sign-On Configuration' page in a web interface. At the top, there is a navigation menu with items like 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', 'Application', 'User Management', and 'Bulk Administration'. Below the menu, the page title is 'SAML Single Sign-On Configuration'. There are two navigation buttons: 'Back' (left arrow) and 'Finish' (right arrow). The 'Status' section shows a green checkmark and the text 'SSO Metadata Test Successful'. Below this, the 'Ready to Enable SSO' section contains instructions: 'Clicking "Finish" will complete enabling SSO on all the servers in this cluster. There will be a short delay while the applications are being updated.' and 'To verify the SSO status of each server, check the main SSO Configuration page. Additional testing and manual uploads may be performed from the main page if necessary.' At the bottom, there are three buttons: 'Back', 'Finish', and 'Cancel'.

De pagina in de afbeelding bevestigt dat het SAML SSO-instelproces op alle servers is gestart.

The screenshot shows the 'SAML Single Sign-On Configuration' page. The 'Status' section shows a green checkmark and the text: 'SAML SSO enablement process initiated on all servers. There will be a short delay while the applications are being updated on each server. To verify the SSO status of each server, check the main SSO Configuration page.'

Log in op CUCM met SAML SSO-referenties. Navigeer naar **Systeem > SAML single aanmelding**. Klik op **SSO Test** om andere knooppunten in de cluster te testen, zoals in de afbeelding:

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)

Disable SAML SSO Export All Metadata Update IdP Metadata File Fix All Disabled Servers

Status

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

SAML SSO enabled

SAML Single Sign-On (1 - 3 of 3) Rows per Page 50

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
cucm1150.adfs.ucce.com	SAML	N/A	June 21, 2016 9:28:39 PM IST	File	June 21, 2016 7:46:56 PM IST	Passed - June 21, 2016 9:29:14 PM IST
cucm1150sub.adfs.ucce.com	SAML	IdP	June 21, 2016 9:28:39 PM IST	File	June 21, 2016 7:46:56 PM IST	Never
imp115.adfs.ucce.com	SAML	IdP	June 21, 2016 9:28:39 PM IST	File	June 21, 2016 7:46:56 PM IST	Never

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Controleer of de SSO-test succesvol is voor de knooppunten die zijn geactiveerd met de SAML SSO. Blader naar **stelsysteem > SAML single aanmelding**. Een succesvolle SSO-test toont de status die is goedgekeurd.

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)

Disable SAML SSO Export All Metadata Update IdP Metadata File Fix All Disabled Servers

Status

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

SAML SSO enabled

SAML Single Sign-On (1 - 3 of 3) Rows per Page 50

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
cucm1150.adfs.ucce.com	SAML	N/A	June 20, 2016 9:57:30 AM IST	File	June 20, 2016 10:06:27 PM IST	Passed - June 20, 2016 9:59:02 PM IST
cucm1150sub.adfs.ucce.com	SAML	IdP	June 20, 2016 10:15:46 PM IST	File	June 20, 2016 10:06:26 PM IST	Passed - June 20, 2016 10:11:39 PM IST
imp115.adfs.ucce.com	SAML	IdP	June 20, 2016 10:15:46 PM IST	File	June 20, 2016 10:06:26 PM IST	Passed - June 20, 2016 10:12:40 PM IST

Nadat het SAML SSP-systeem is geactiveerd, worden de geïnstalleerde toepassingen en de Platform-toepassingen vermeld voor de CUCM-inlogpagina, zoals in deze afbeelding wordt weergegeven.

Installed Applications

- Cisco Unified Communications Manager
 - Recovery URL to bypass Single Sign On (SSO)
- Cisco Unified Communications Self Care Portal
- Cisco Prime License Manager
- Cisco Unified Reporting
- Cisco Unified Serviceability

Platform Applications

- Disaster Recovery System
- Cisco Unified Communications OS Administration

Nadat de SAML SSO is geactiveerd, worden de geïnstalleerde toepassingen en de Platform-toepassingen vermeld voor IM and Presence inlogpagina, zoals in deze afbeelding wordt weergegeven:

Installed Applications

- Cisco Unified Communications Manager IM and Presence
 - Recovery URL to bypass Single Sign On (SSO)
- Cisco Unified Reporting
- Cisco Unified Serviceability

Platform Applications

- Disaster Recovery System
- Cisco Unified Communications OS Administration

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Om de SSO-logbestanden te debug in te stellen, gebruikt u de opdracht **om BEELDNIVEAU DEBUG in te stellen**

Verzamel de SSO-bestanden met RTMT of **activelog /tomcat/logs/ssosp/log4j/*.log** locatie met behulp van CLI.

Voorbeeld van SSO-logs toont de metagegevens die zijn gegenereerd en naar andere knooppunten worden verzonden

```
2016-05-28 14:59:34,026 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Call GET API to generate Clusterwide SP Metadata in the Local node.
2016-05-28 14:59:47,184 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Call to post the generated SP Metadata to other nodes
2016-05-28 14:59:47,185 INFO [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Begin:postClusterWideSPMetadata
2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Nodes [cucm1150, cucm1150sub.adfs.ucce.com]
2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post ClusterWideSPMetadata to the cucm1150
2016-05-28 14:59:47,187 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post ClusterWideSPMetadata to the cucm1150sub.adfs.ucce.com
```