AD FS Version 2.0 Setup for SAML SSO Configuration Example

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Configure

- Download AD FS Version 2.0 Identity Provider (IdP) Metadata
- Download Collaboration Server (SP) Metadata
  - CUCM IM and Presence Service
  - Unity Connection
  - Cisco Prime Collaboration Provisioning
- Add CUCM as Relying Party Trust
- Add CUCM IM and Presence as Relying Party Trust
- AddUCXN as Relying Party Trust
- Add Cisco Prime Collaboration Provisioning as Relying Party Trust

Verify

Troubleshoot

Introduction

This document describes how to configure Active Directory Federation Service (AD FS) Version 2.0 in order to enable Security Assertion Markup Language (SAML) Single Sign-on (SSO) for Cisco Collaboration products like Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (UCXN), CUCM IM and Presence, and Cisco Prime Collaboration.

Prerequisites

Requirements

AD FS Version 2.0 must be installed and tested.

⚠ **Caution**: This installation guide is based on a lab setup and AD FS Version 2.0 is assumed to be used only for SAML SSO with Cisco Collaboration products. In case it is used by other business-critical applications, then necessary customization must be done as per official Microsoft Documentation.

Components Used

The information in this document is based on these software and hardware versions:

- AD FS Version 2.0

- Microsoft Internet Explorer 10
- CUCM Version 10.5
- Cisco IM and Presence Server Version 10.5
- UCXN Version 10.5
- Cisco Prime Collaboration Provisioning 10.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Download AD FS Version 2.0 Identity Provider (IdP) Metadata

In order to download IdP metadata, run this link on you browser: https://<FQDN of ADFS>/FederationMetadata/2007-06/FederationMetadata.xml.

Download Collaboration Server (SP) Metadata

CUCM IM and Presence Service

Open a web browser, log into CUCM as administrator, and navigate to **System > SAML Single Sign On**.

Unity Connection

Open a web browser, log into UCXN as administrator, and navigate to **System Settings > SAML Single Sign On**.

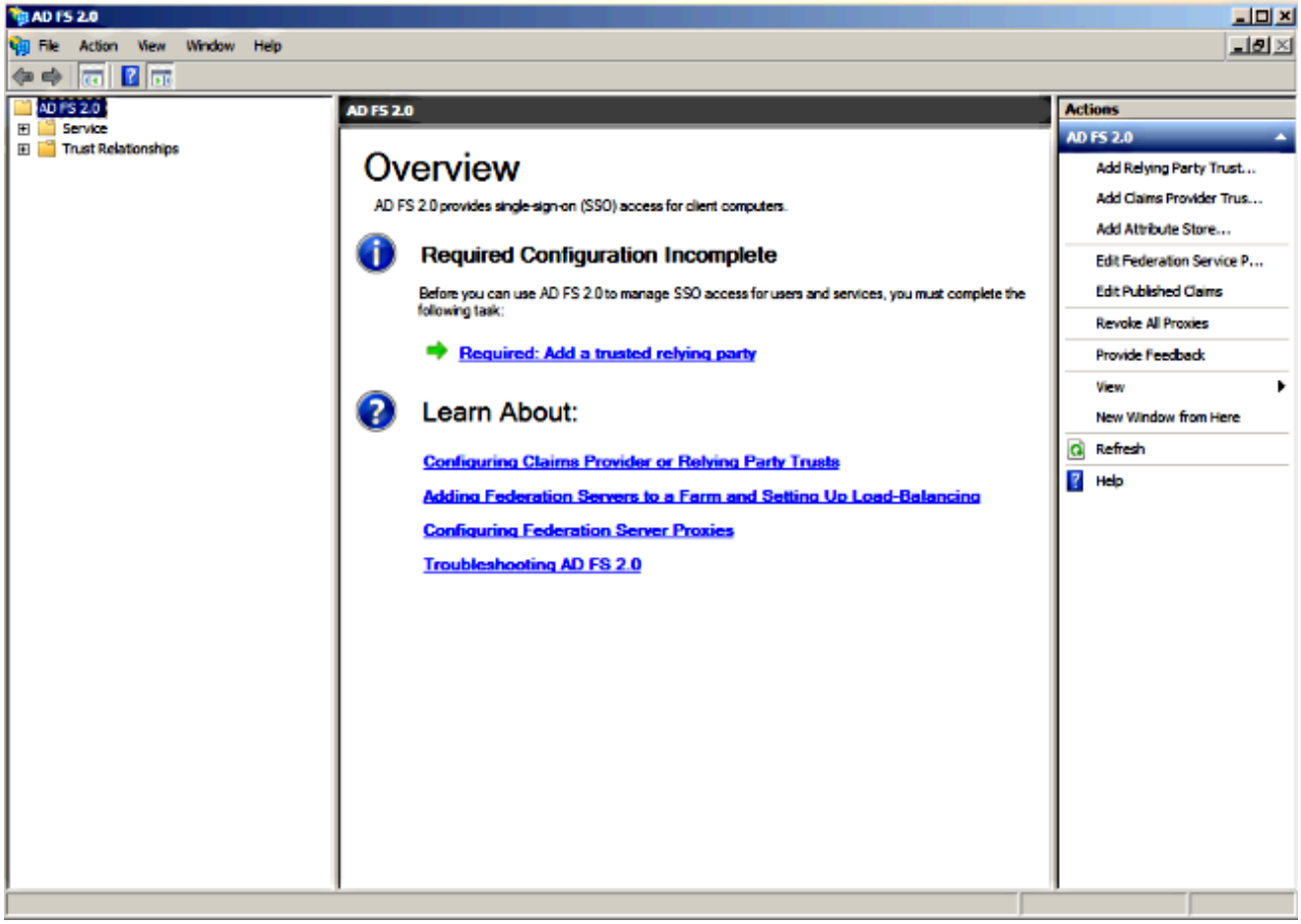
Cisco Prime Collaboration Provisioning

Open a web browser, log into Prime Collaboration Assurance as globaladmin, and navigate to **Administration > System Setup > Single Sign On**.

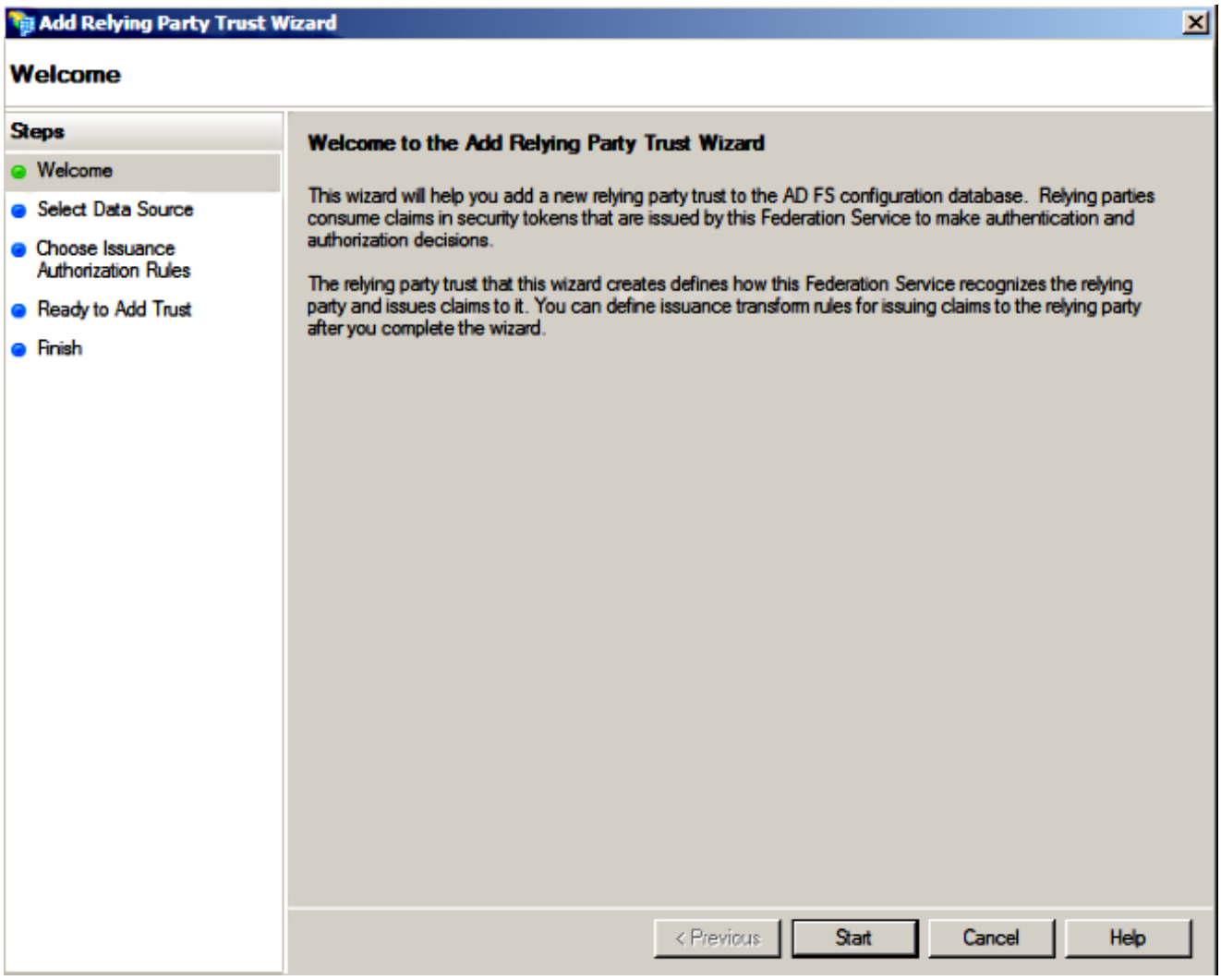
Add CUCM as Relying Party Trust

1. Log into the AD FS server and launch AD FS Version 2.0 from the Microsoft Windows **Programs** menu.

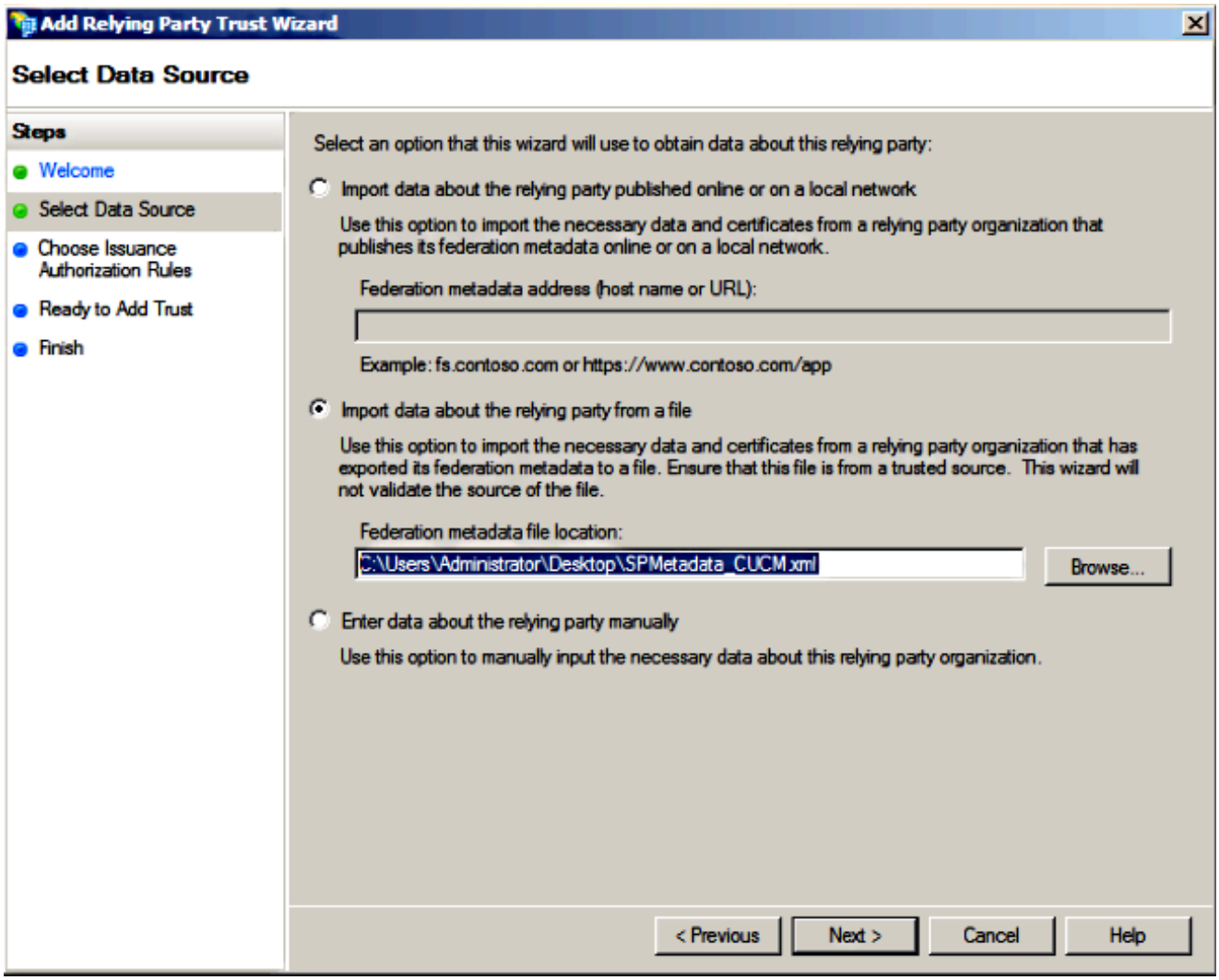
2. Select **Add Relying Party Trust**.



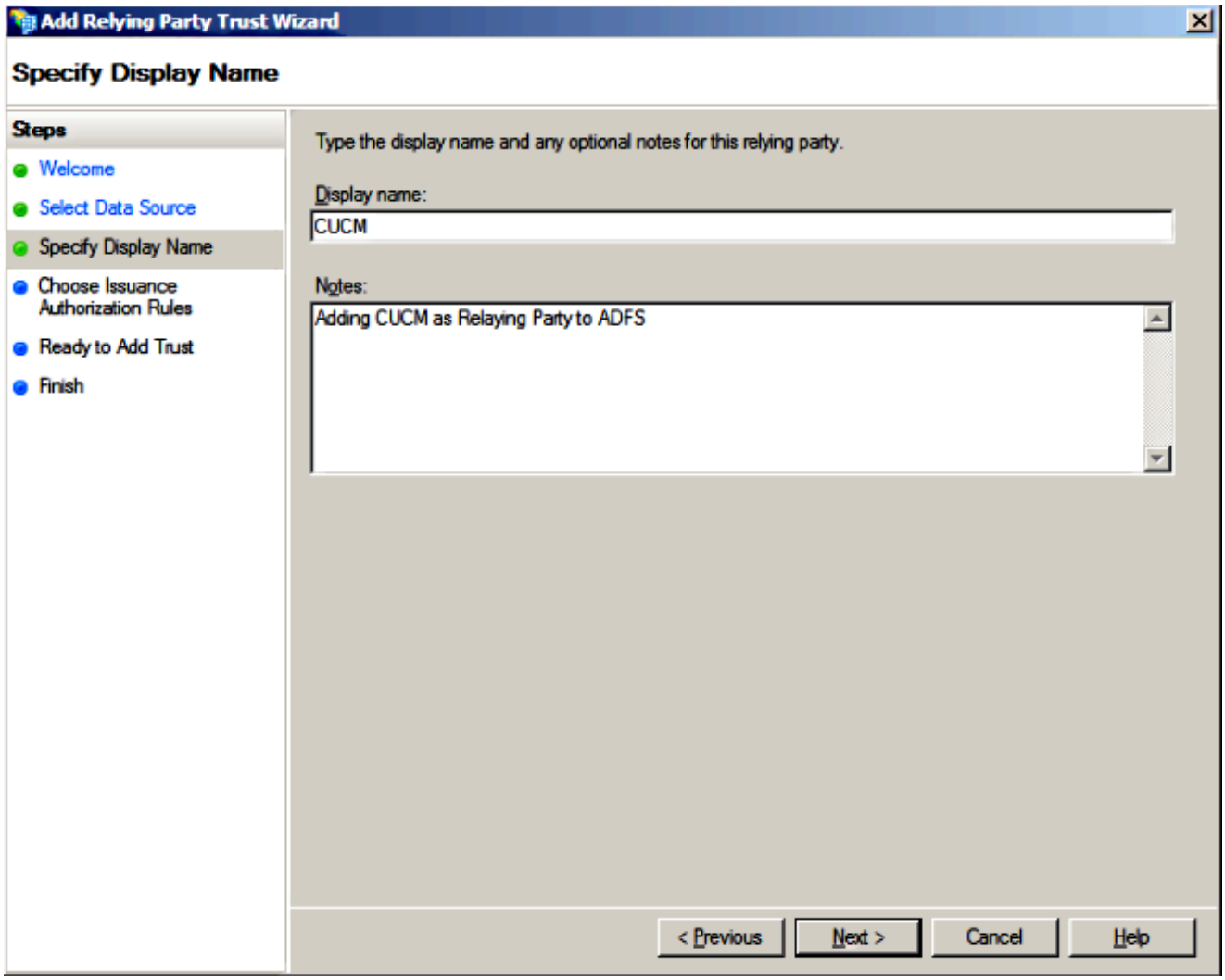
3. Click **Start**.



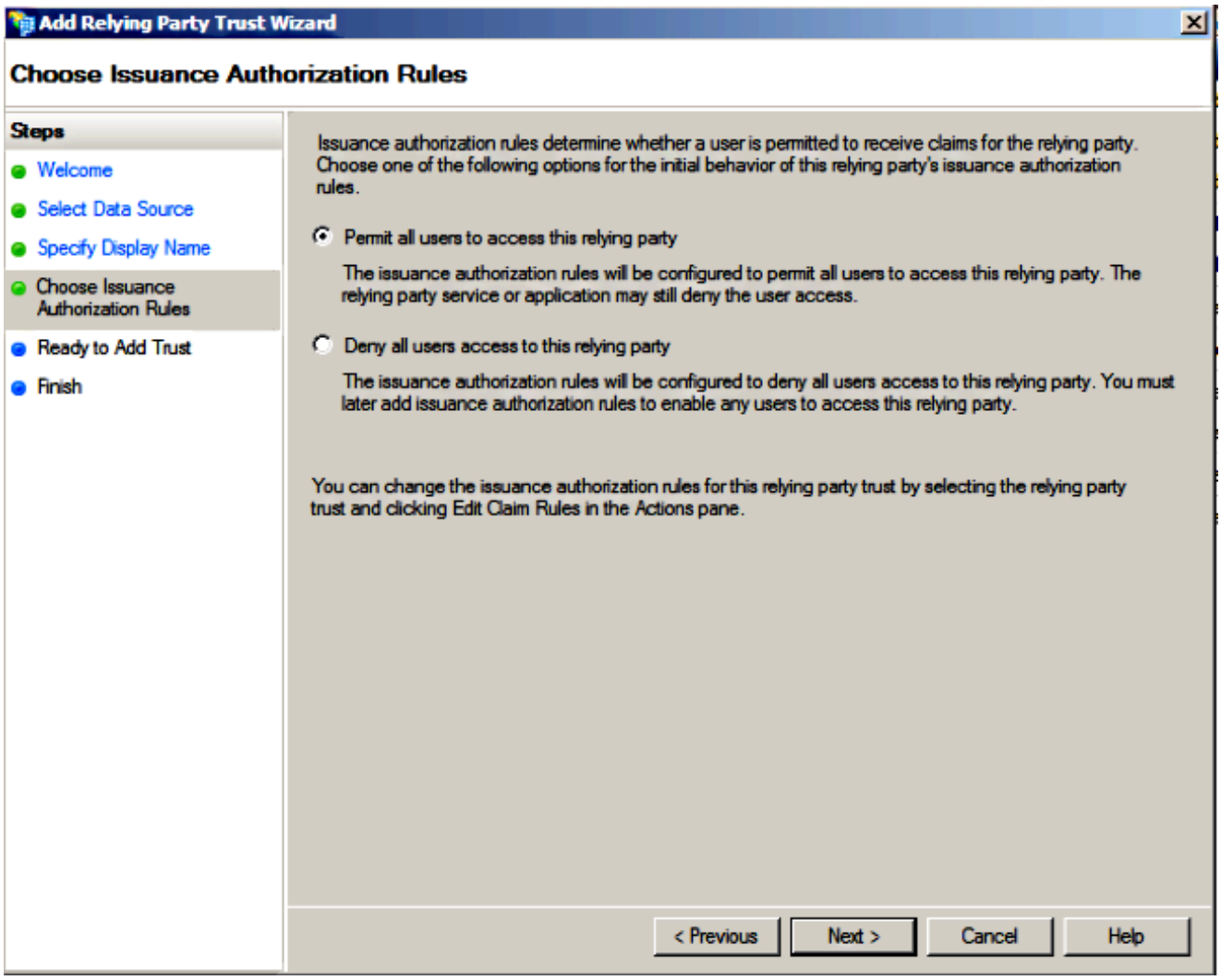
4. Select the **Import data about the relying party from a file** option, choose the **SPMetadata_CUCM.xml** metadata file that you downloaded from CUCM earlier, and click **Next.**



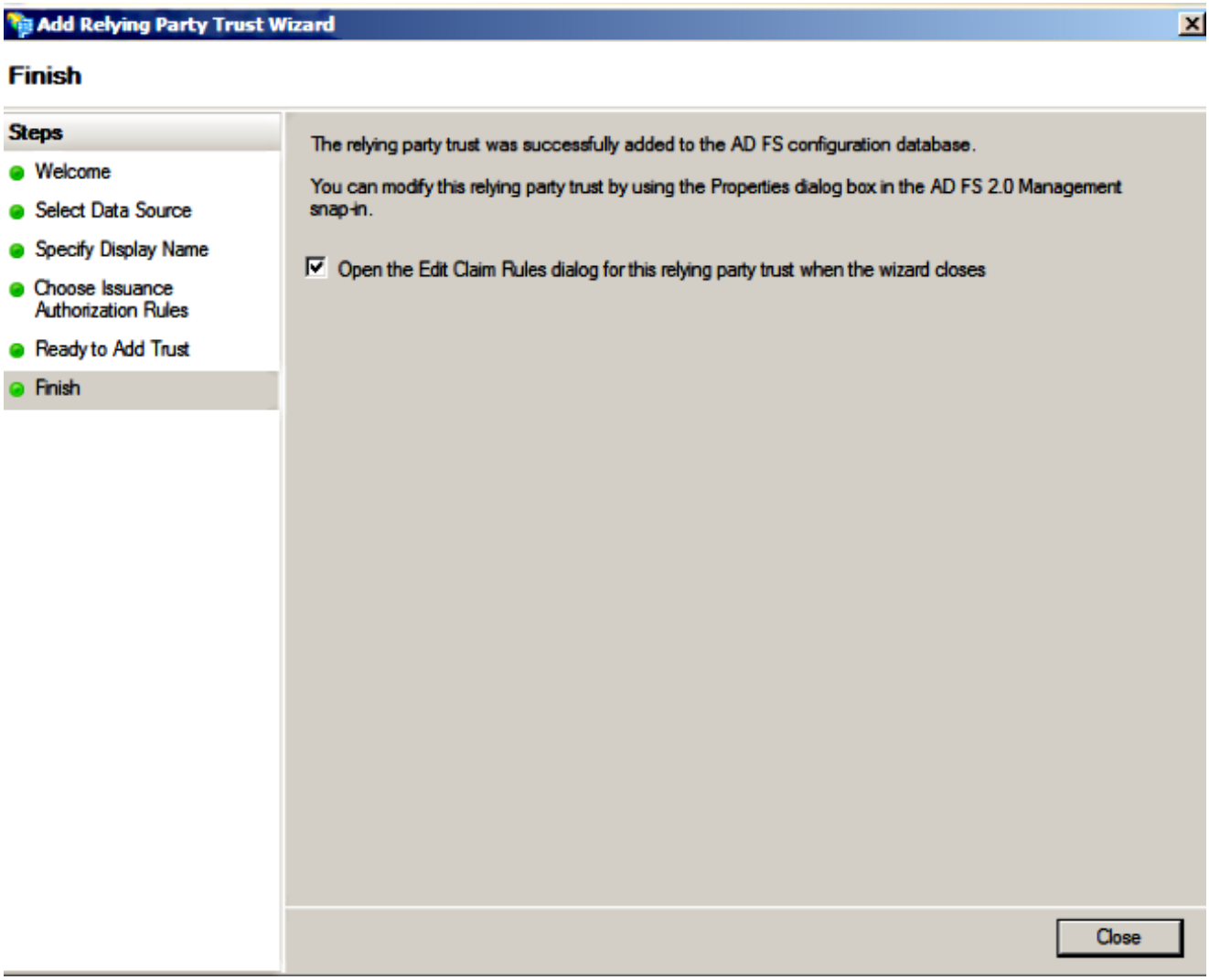
5. Enter **Display name** and click **Next**.



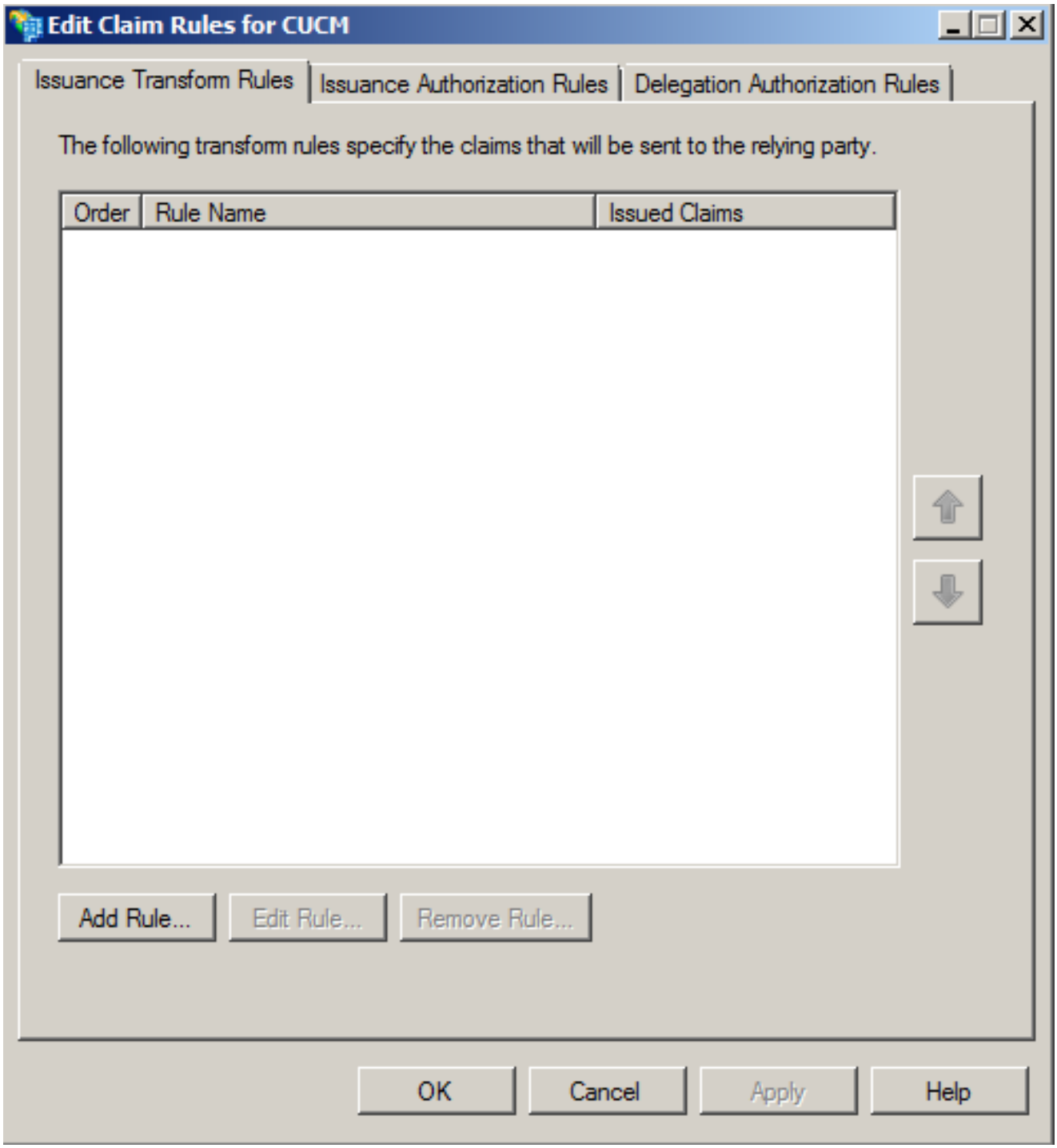
6. Choose **Permit all users to access this relying party** and click **Next.**



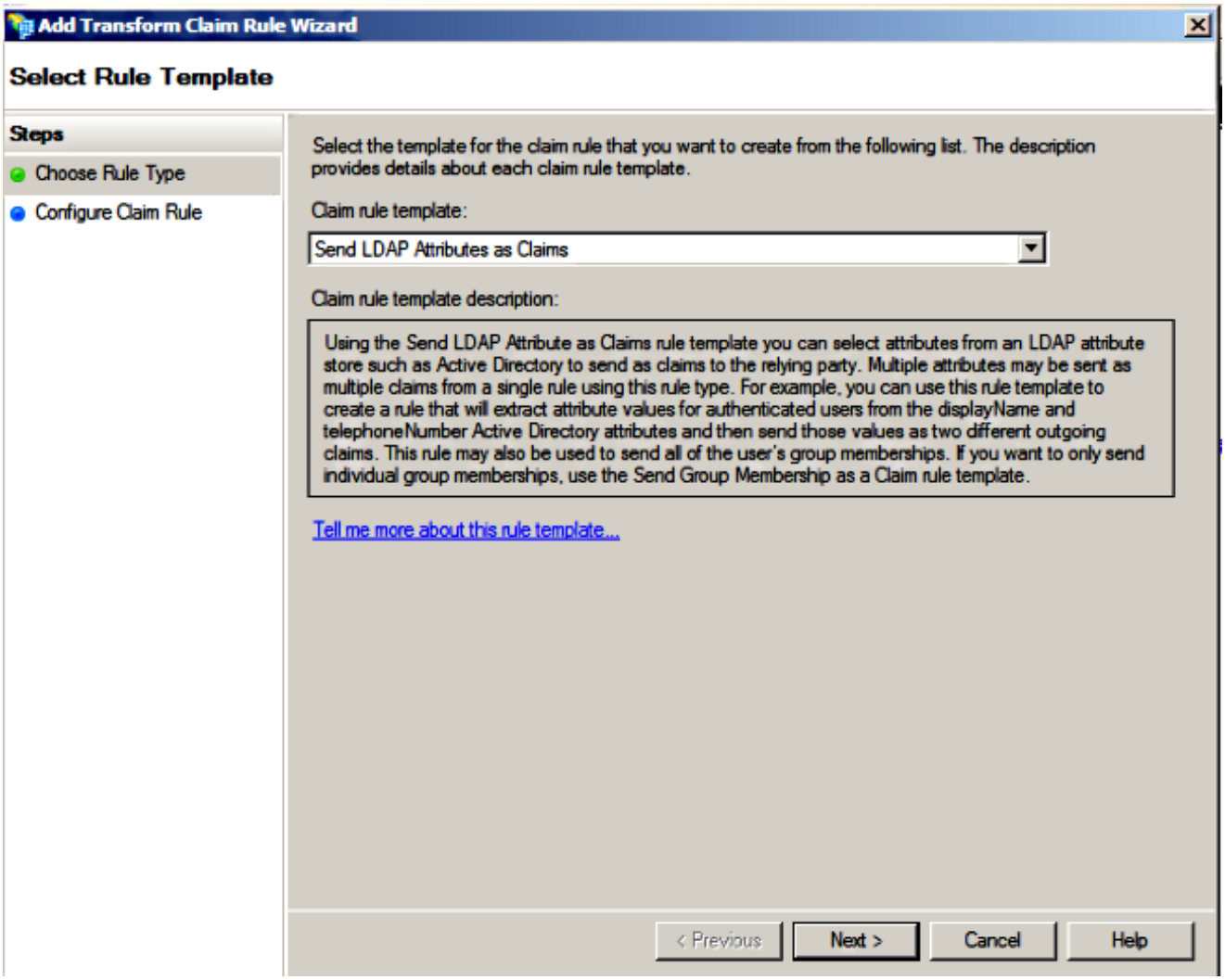
7. Select **Open the Edit Claim Rules dialog for thee relying party trust when the wizard closes** and click **Close.**



8. Click **Add Rule**.

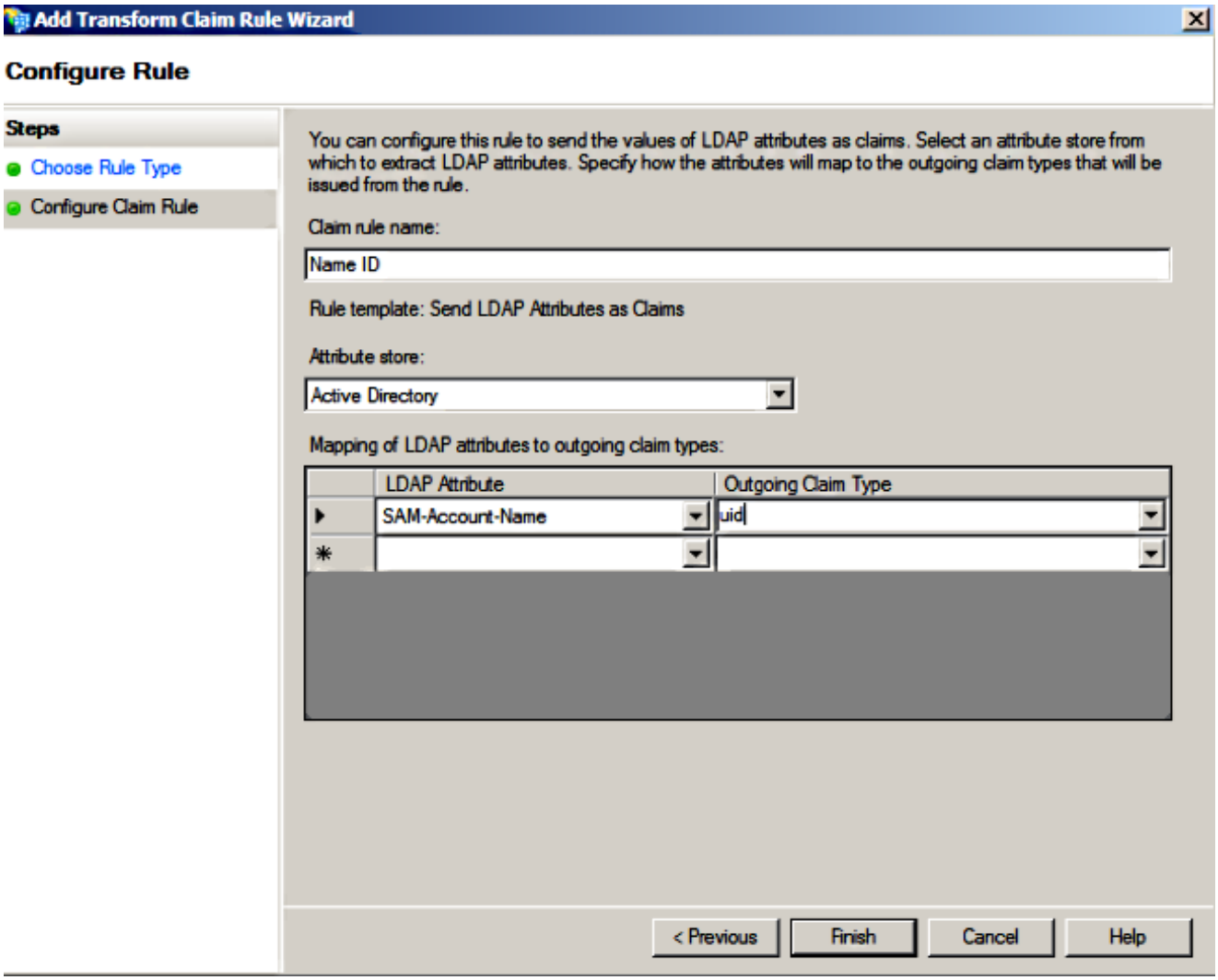


9. Click **Next** with default Claim rule template set to **Send LDAP Attributes as Claims**.

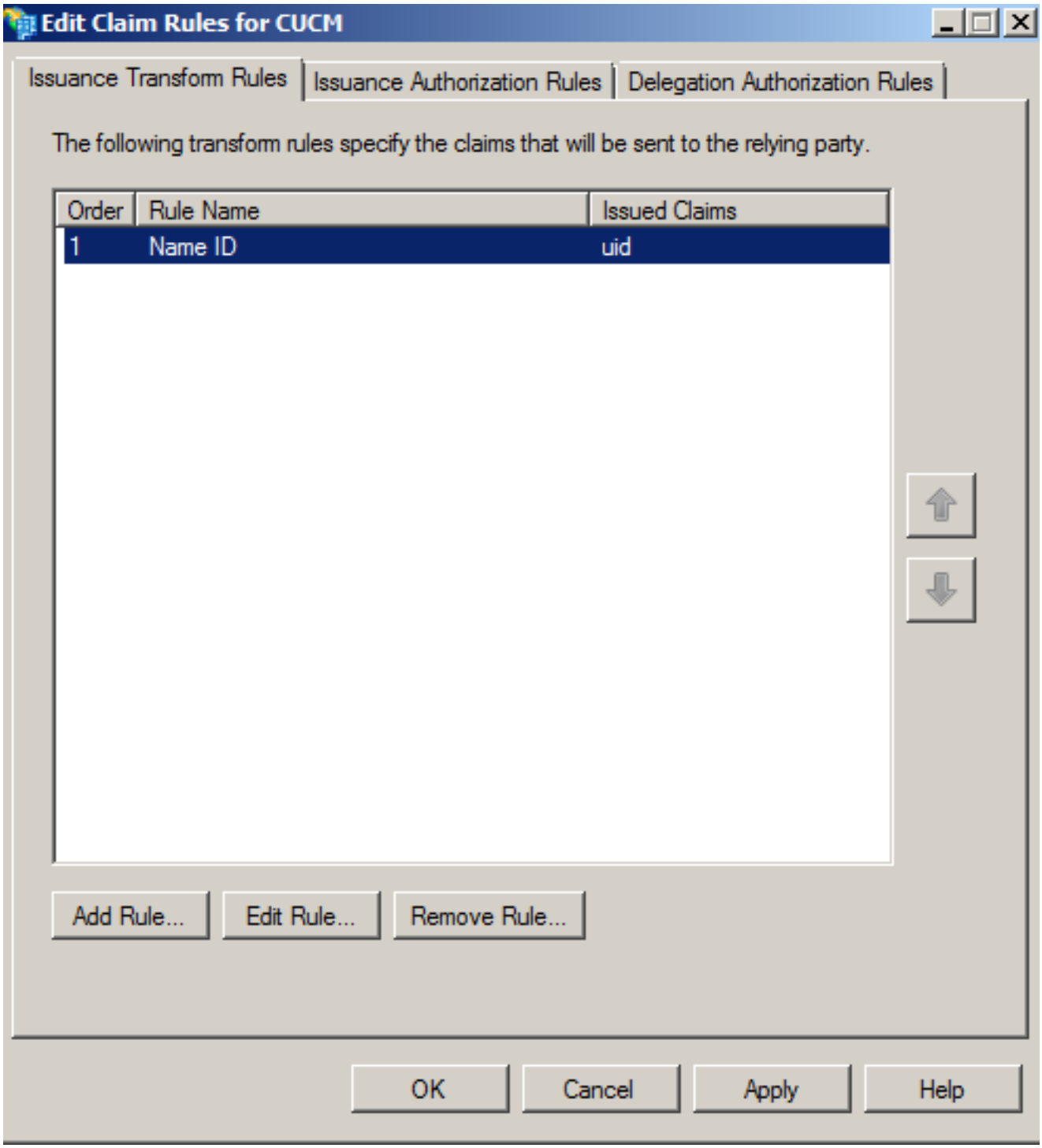


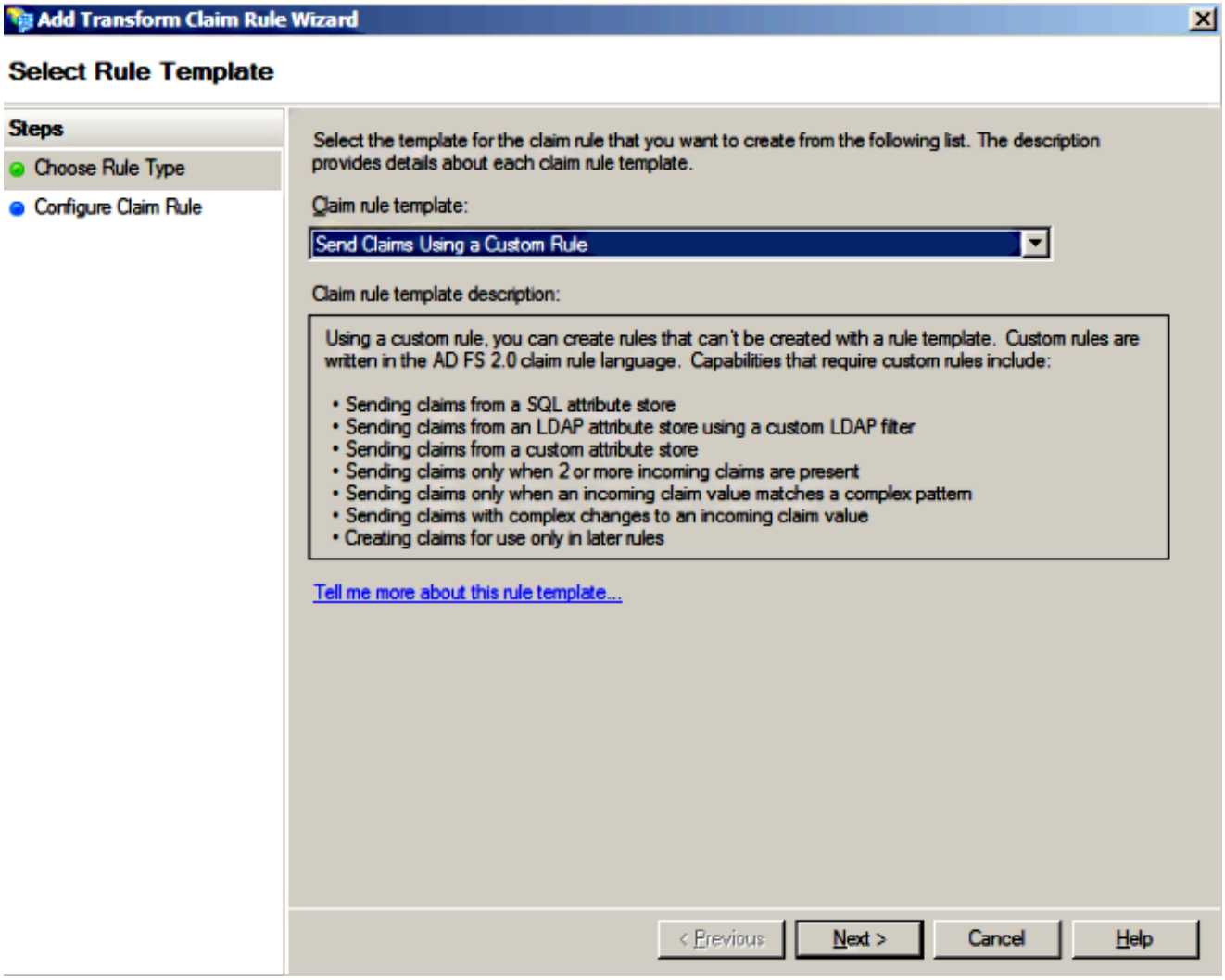
10. In Configure Rule, enter the Claim rule name, select **Active Directory** as the Attribute store, configure **LDAP Attribute** and **Outgoing Claim Type** as shown in this image, and click **Finish**.

Note:
- The Lightweight Directory Access Protocol (LDAP) attribute should match the Directory Sync attribute on CUCM.
- "uid" should be in lower case.



11. Click **Add Rule**, select **Send Claims Using a Custom Rule** as the claim rule template, and click **Next**.

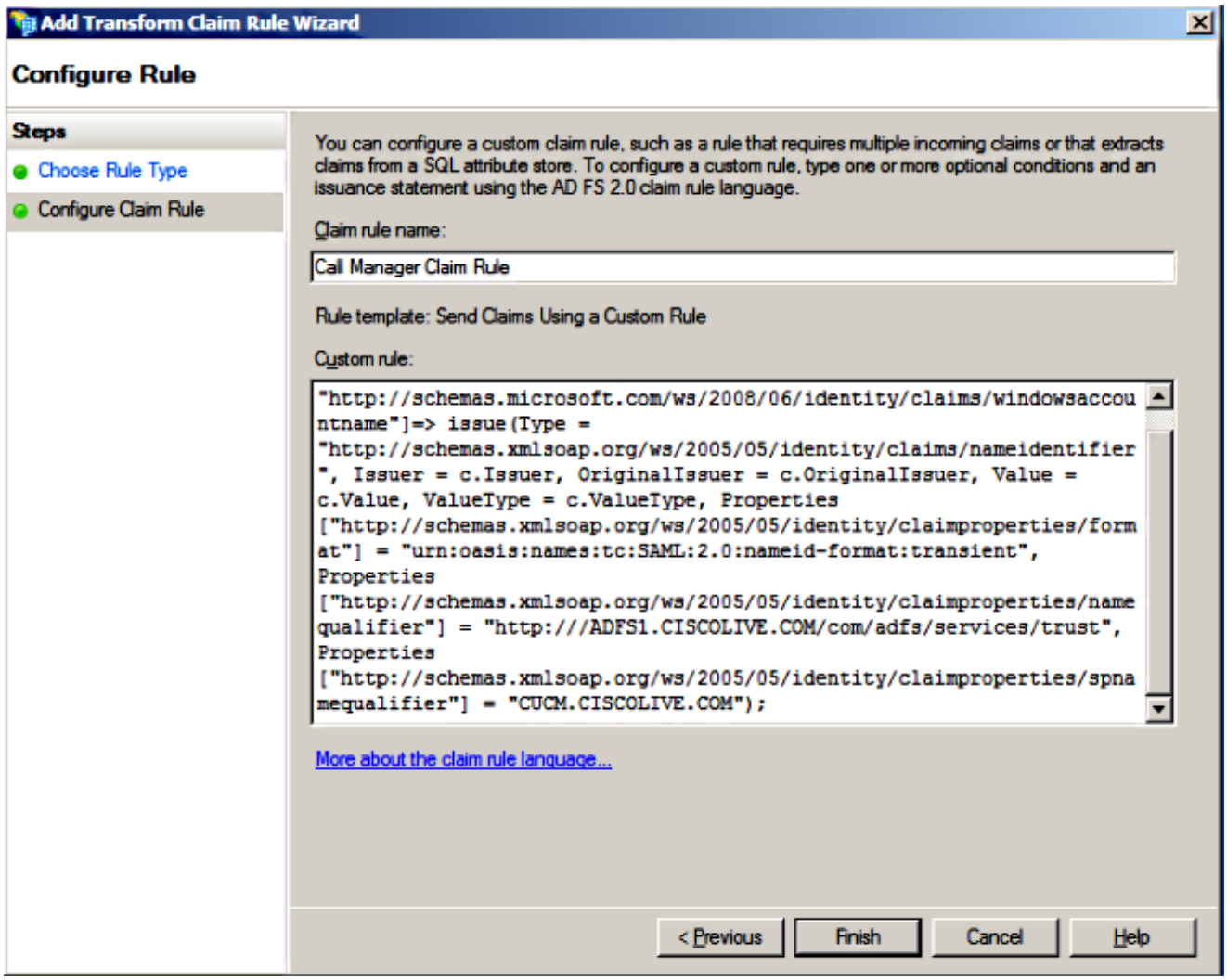

Edit Claim Rules for CUCM
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
The following transform rules specify the claims that will be sent to the relying party.
Order
Rule Name
Issued Claims
1
Name ID
uid
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply
Help



12. Enter a name for Claim rule name and copy this syntax in the space given under Custom rule:

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

(**NOTE:** If you copy and paste the text from these examples, be aware that some word processing software will substitute the ASCII quotation marks (") with the UNICODE versions (“”). The UNICODE versions will cause the claim rule to fail.)



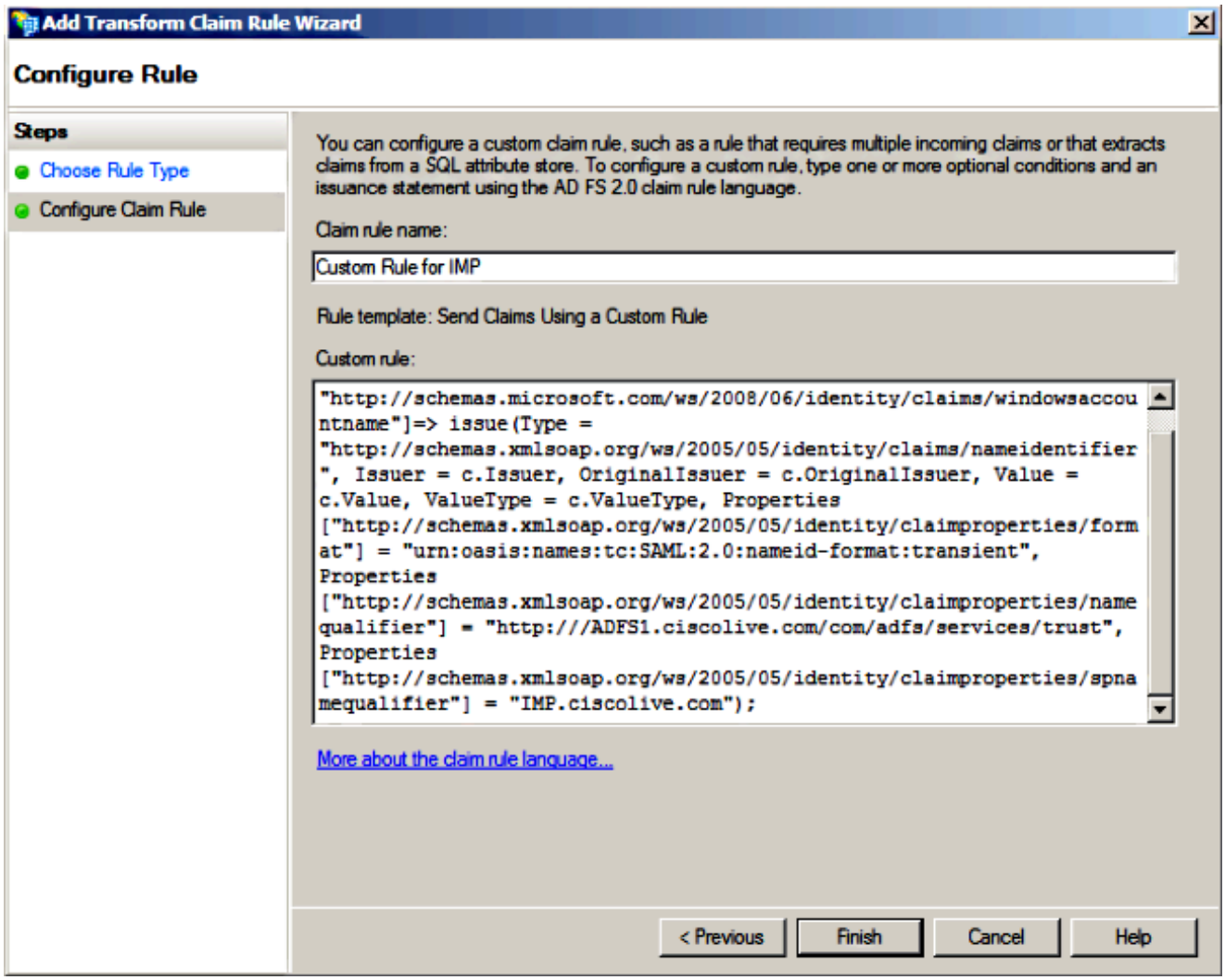
Note:
- CUCM and ADFS Fully Qualified Domain Name (FQDN) is prepopulated with the lab CUCM and AD FS in this example and must be modified to match your environment.
- FQDN of CUCM/ADFS are case-sensitive and must match with the metadata files.

13. Click **Finish**.
14. Click **Apply** and then **OK.**
15. Restart the AD FS Version 2.0 service from **Services.msc**.

Add CUCM IM and Presence as Relying Party Trust

1. Repeat Steps 1 to 11 as described for **Add CUCM as Relying Party Trust** and proceed to Step 2.
2. Enter a name for Claim rule name and copy this syntax in the space given under Custom rule:

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



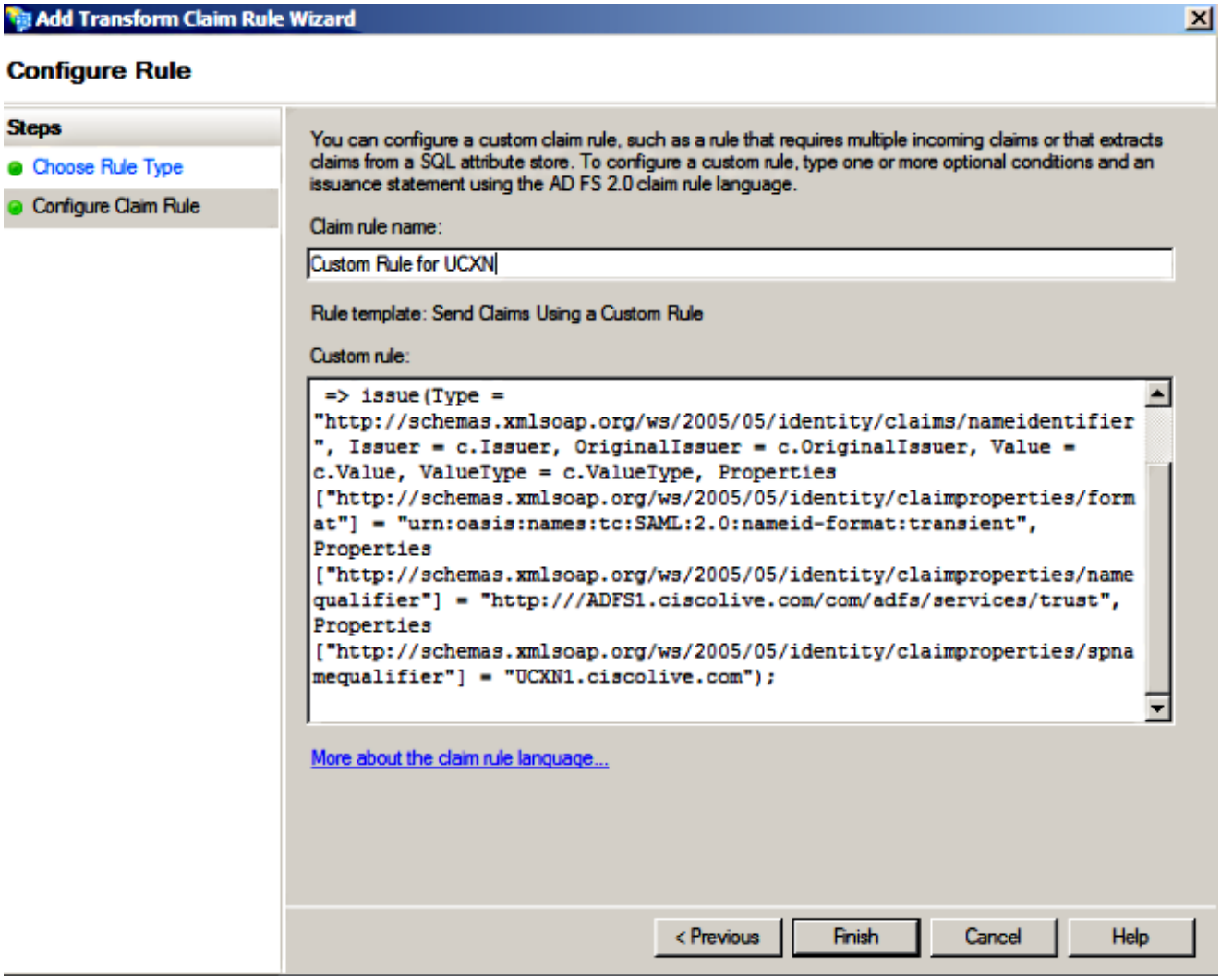
Notice that IM and Presence and AD FS FQDN is prepopulated with the lab IM and Presence and AD FS in this example and must be modified to match your environment.

3. Click **Finish**.
4. Click **Apply** and then **OK.**
5. Restart the AD FS Version 2.0 service from **Services.msc.**

Add UCXN as Relying Party Trust

1. Repeat Steps 1 to 12 as described for **Add CUCM as Relying Party Trust** and proceed to Step 2.
2. Enter a name for Claim rule name and copy this syntax in the space given under Custom rule:

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



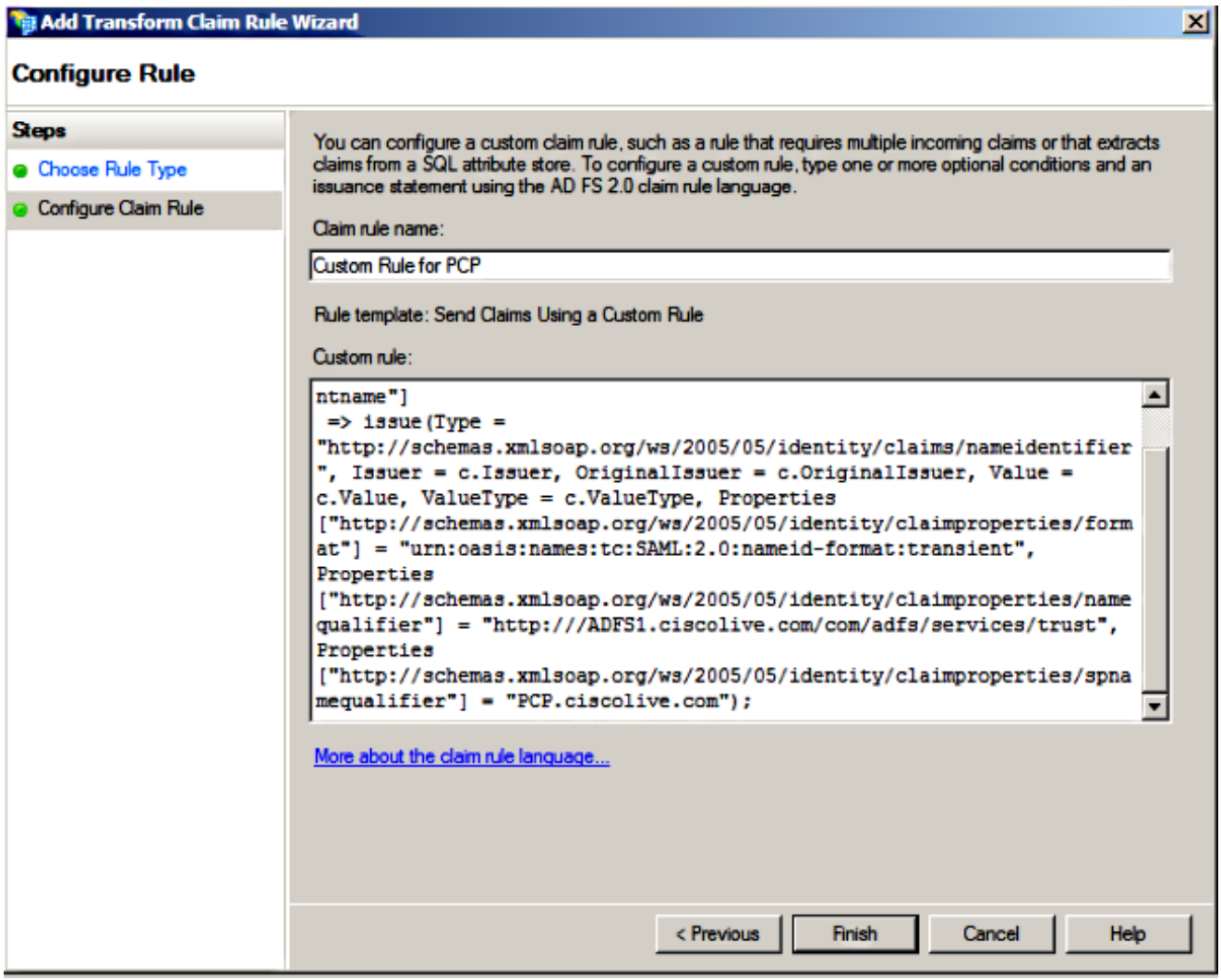
Notice that UCXN and AD FS FQDN is prepopulated with the lab UCXN and ADFS in this example and must be modified to match your environment.

3. Click **Finish**.
4. Click **Apply** and then **OK**.
5. Restart the AD FS Version 2.0 service from **Services.msc.**

Add Cisco Prime Collaboration Provisioning as Relying Party Trust

1. Repeat Steps 1 to 12 as described for **Add CUCM as Relying Party Trust** and proceed to Step 2.
2. Enter a name for Claim rule name and copy this syntax in the space given under Custom rule:

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



Notice that Prime Provisioning and AD FS FQDN is prepopulated with the lab Prime Collaboration Provisioning (PCP) and AD FS from this example and must be modified to match your environment.

3. Click **Finish**.
4. Click **Apply** and then **OK**.
5. Restart the AD FS Version 2.0 service from **Services.msc**.

Once you set up AD FS Version 2.0, proceed to enable SAML SSO on Cisco Collaboration products.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

AD FS logs diagnostic data to the system Event Log. From Server Manager on the AD FS server open **Diagnostics -> Event Viewer -> Applications and Services -> AD FS 2.0 -> Admin**

Look for errors logged for AD FS activity

