AD FS Version 2.0 Setup for SAML SSO Configuration Example

Contents

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**.

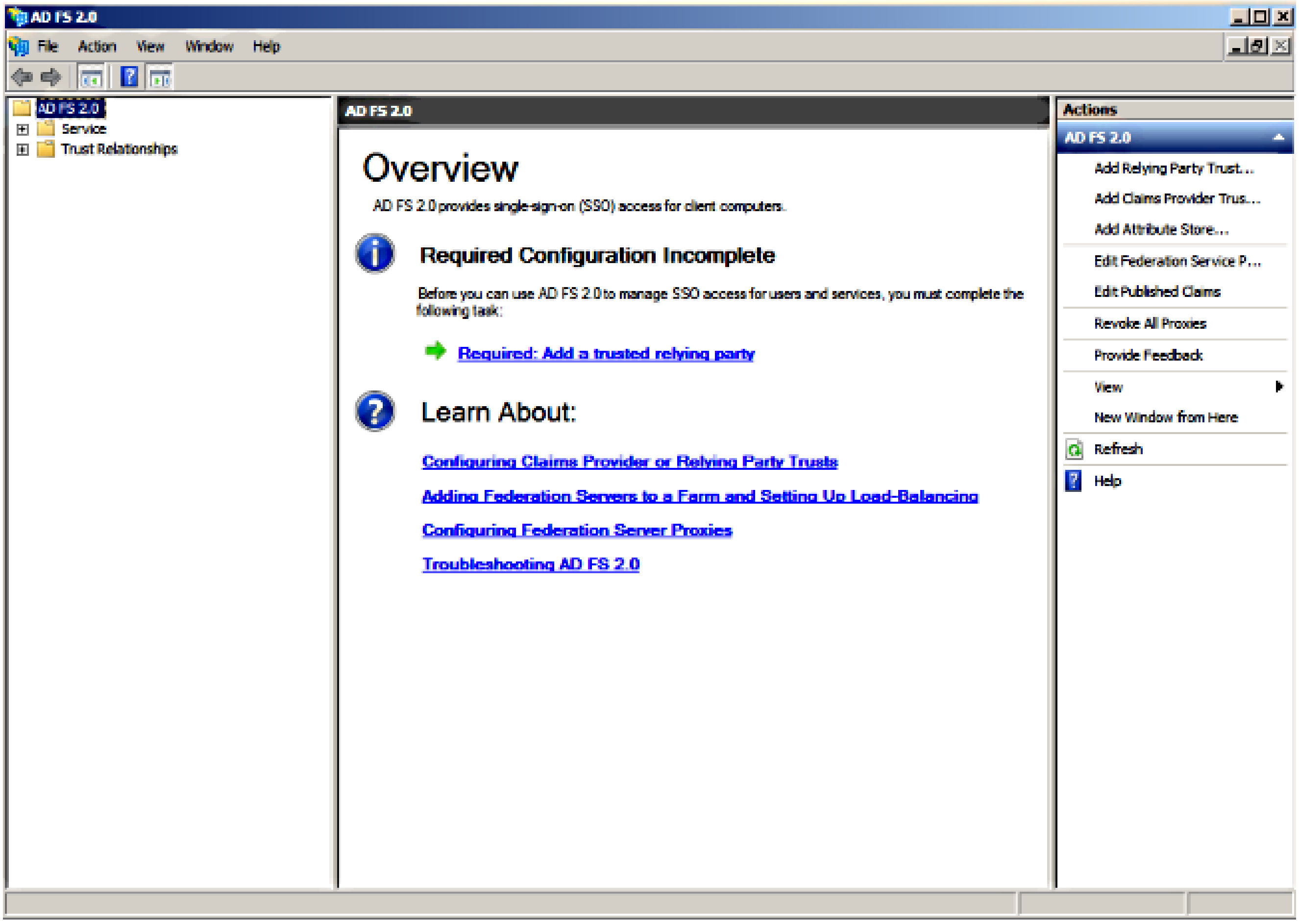
Cisco Prime Collaboration Provisioning

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**.



Overview

AD FS 2.0 provides single-sign-on (SSO) access for client computers.

Required Configuration Incomplete

Before you can use AD FS 2.0 to manage SSO access for users and services, you must complete the following task:

Required: Add a trusted relying party

Learn About:

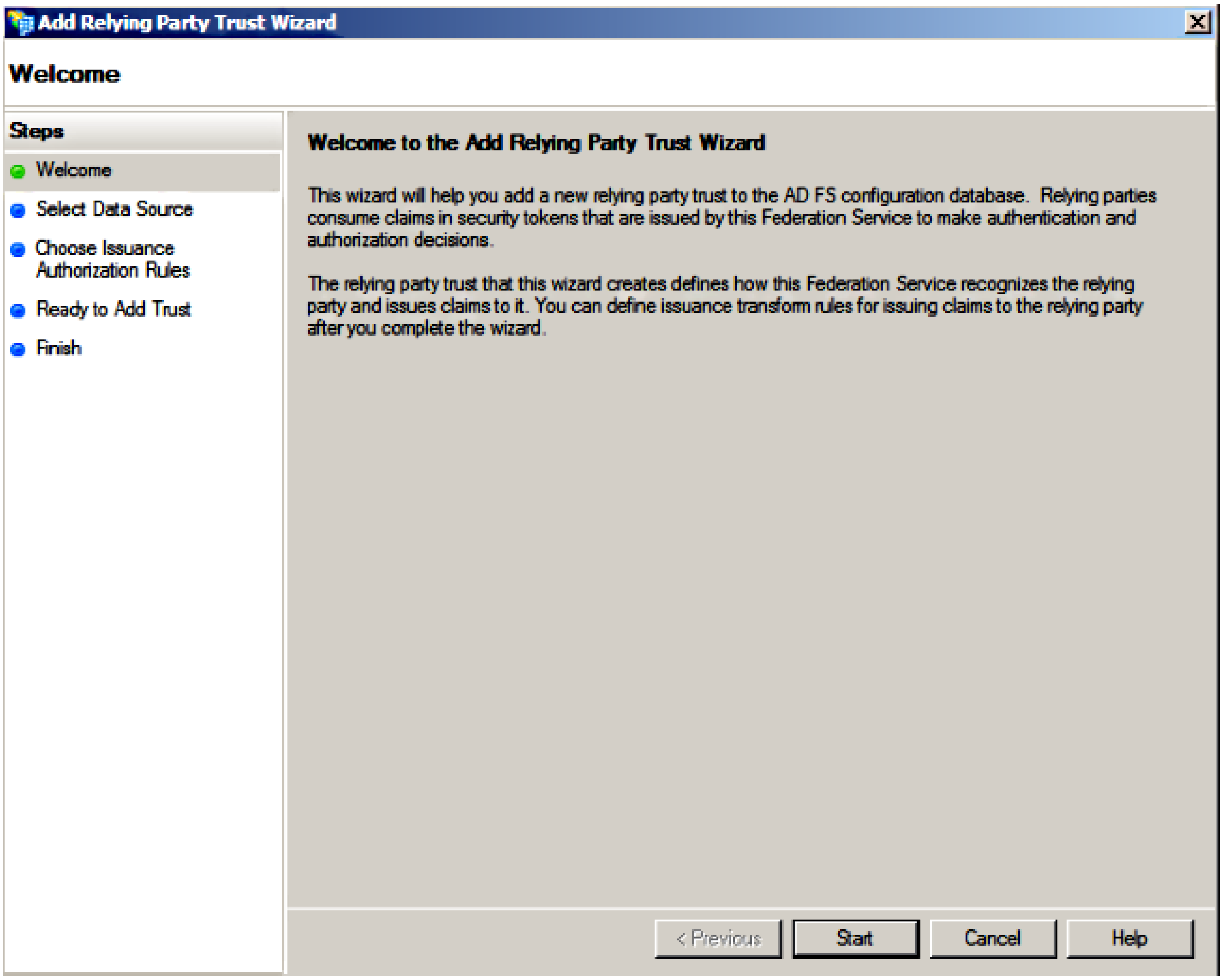
Configuring Claims Provider or Relying Party Trusts

Adding Federation Servers to a Farm and Setting Up Load-Balancing

Configuring Federation Server Proxies

Troubleshooting AD FS 2.0

3. Click **Start**.

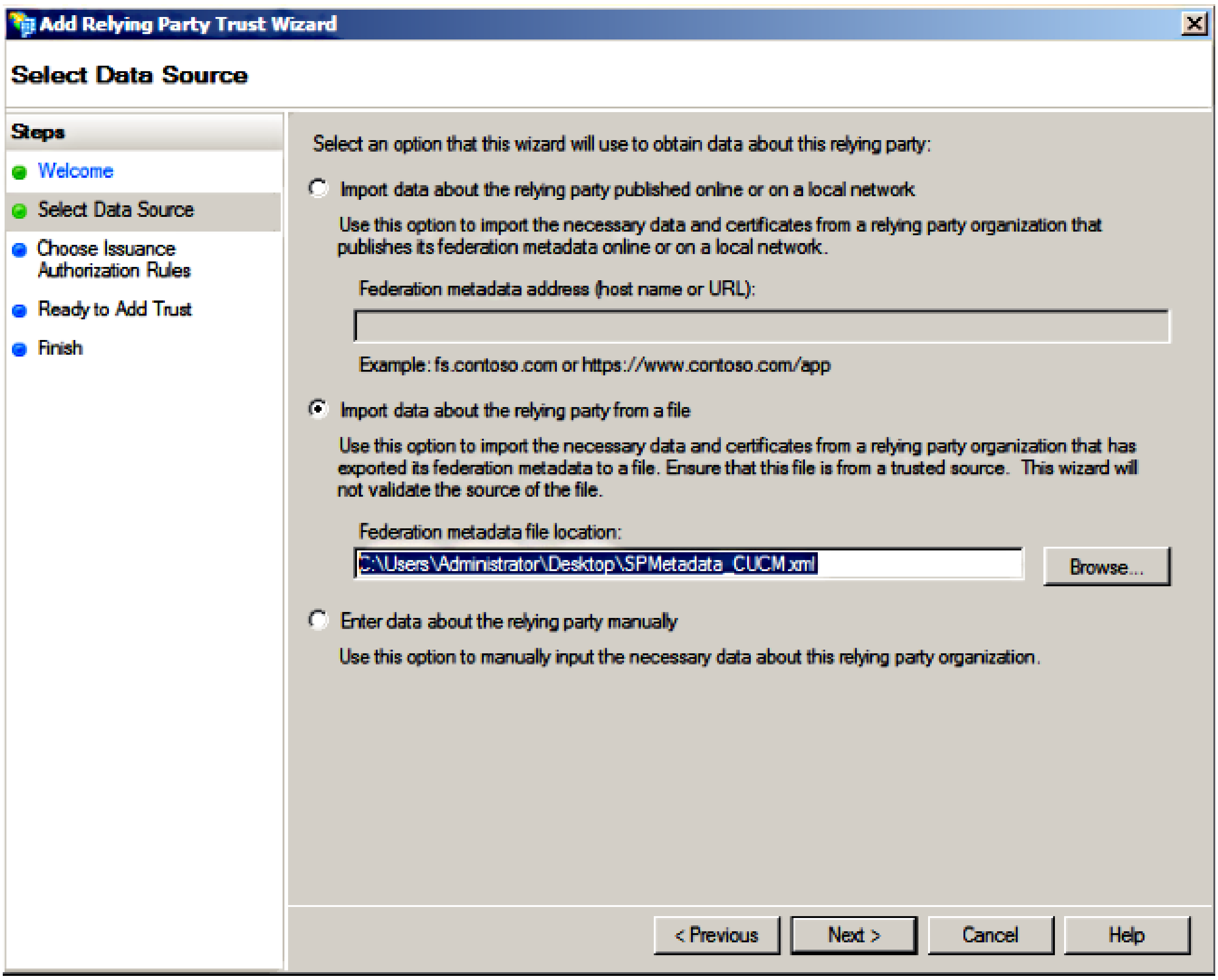


Welcome to the Add Relying Party Trust Wizard

This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.

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.**



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.

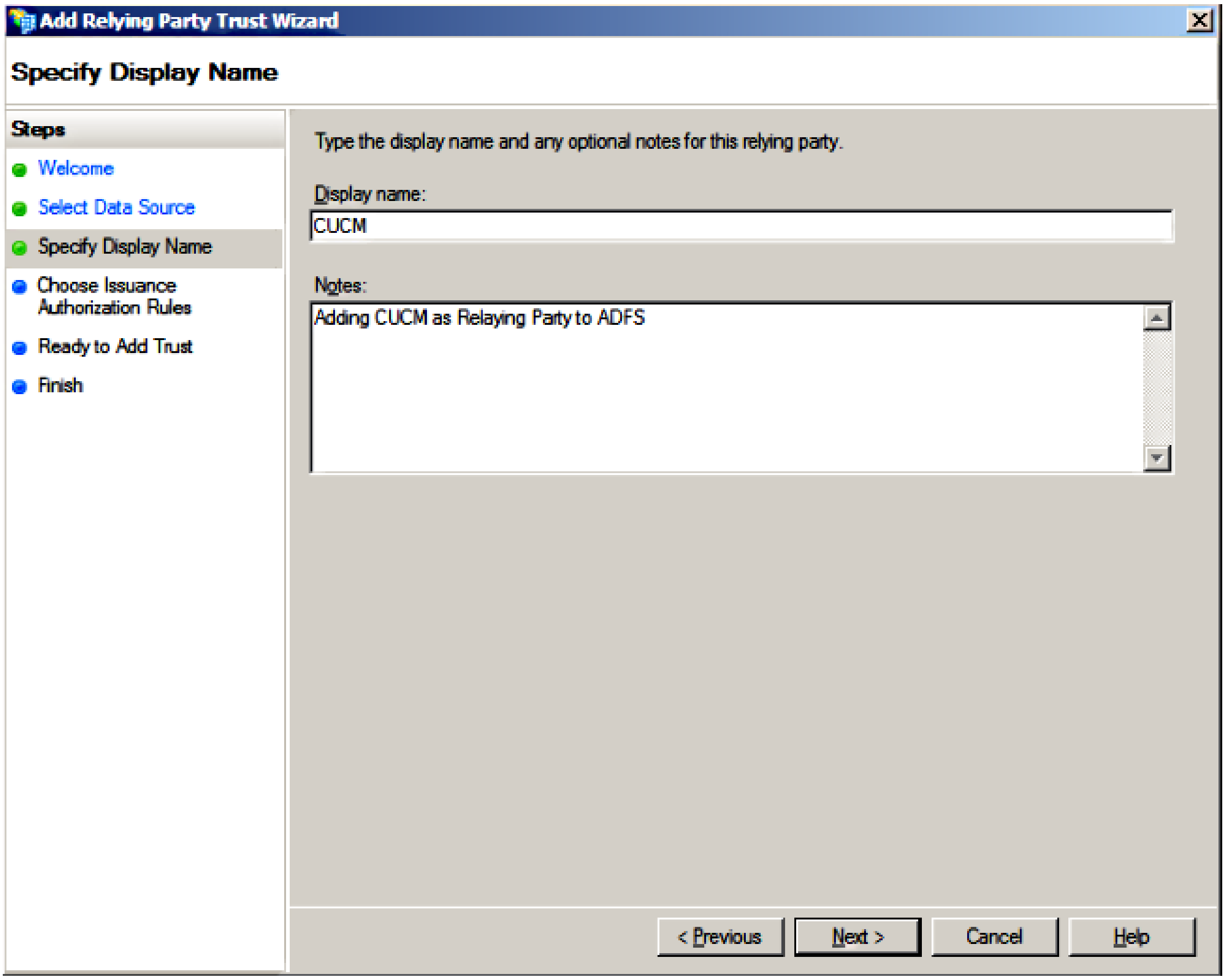
Federation metadata file location:

C:\Users\Administrator\Desktop\SPMetadata_CUCM.xml

○ Enter data about the relying party manually

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

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

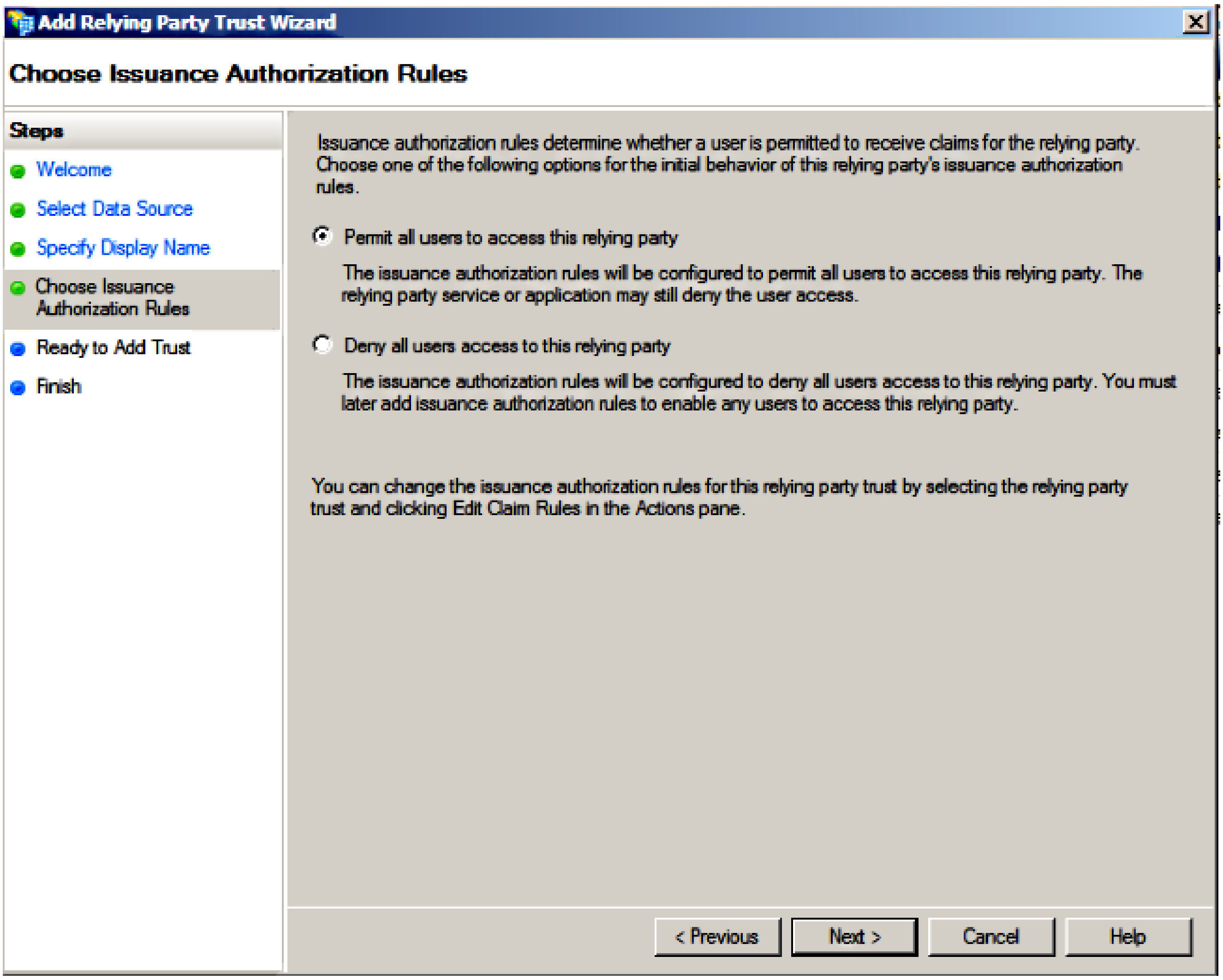


Type the display name and any optional notes for this relying party.

Display name: CUCM

Notes: Adding CUCM as Relaying Party to ADFS

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



Choose Issuance Authorization Rules

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

● Permit all users to access this relying party

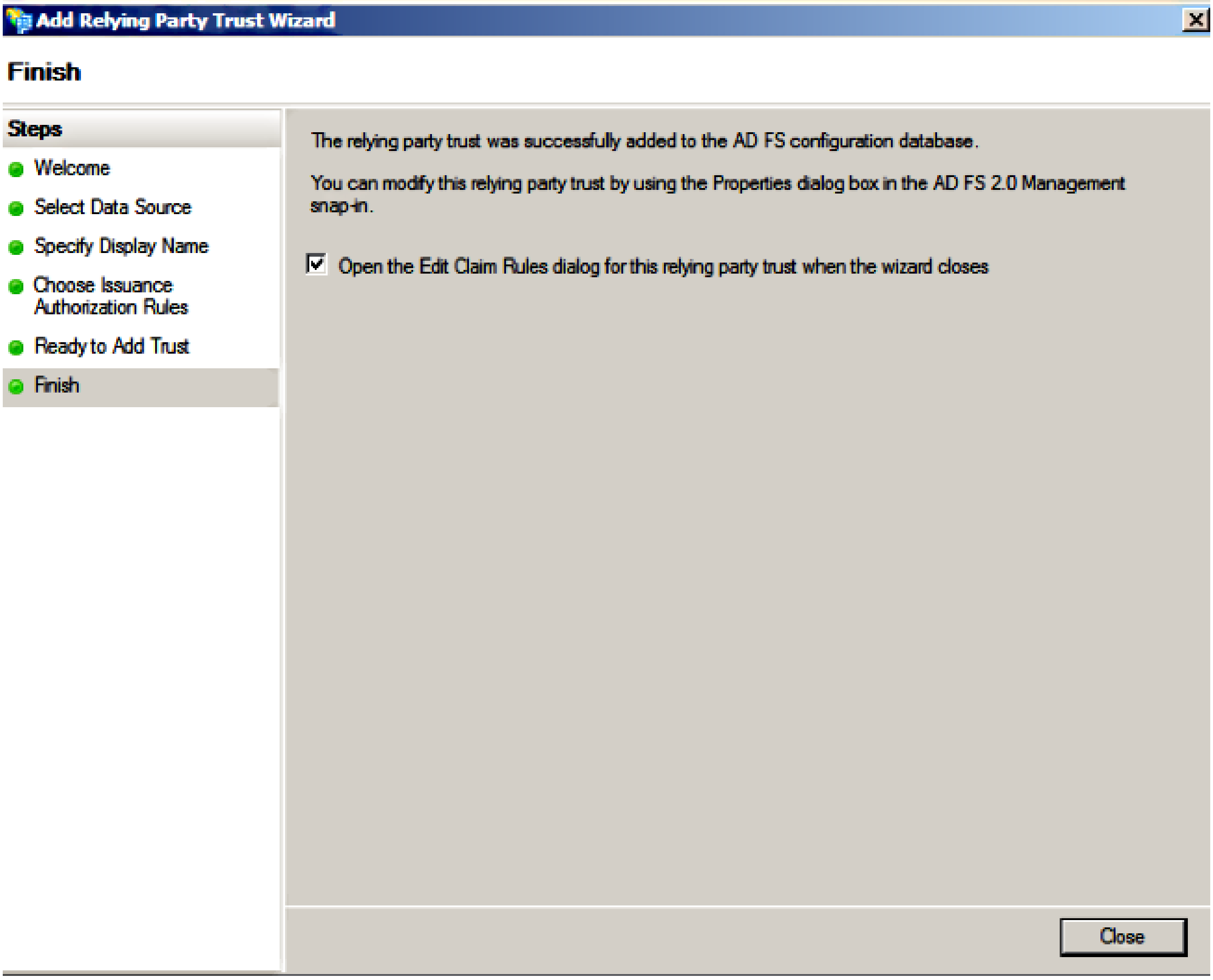
The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

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



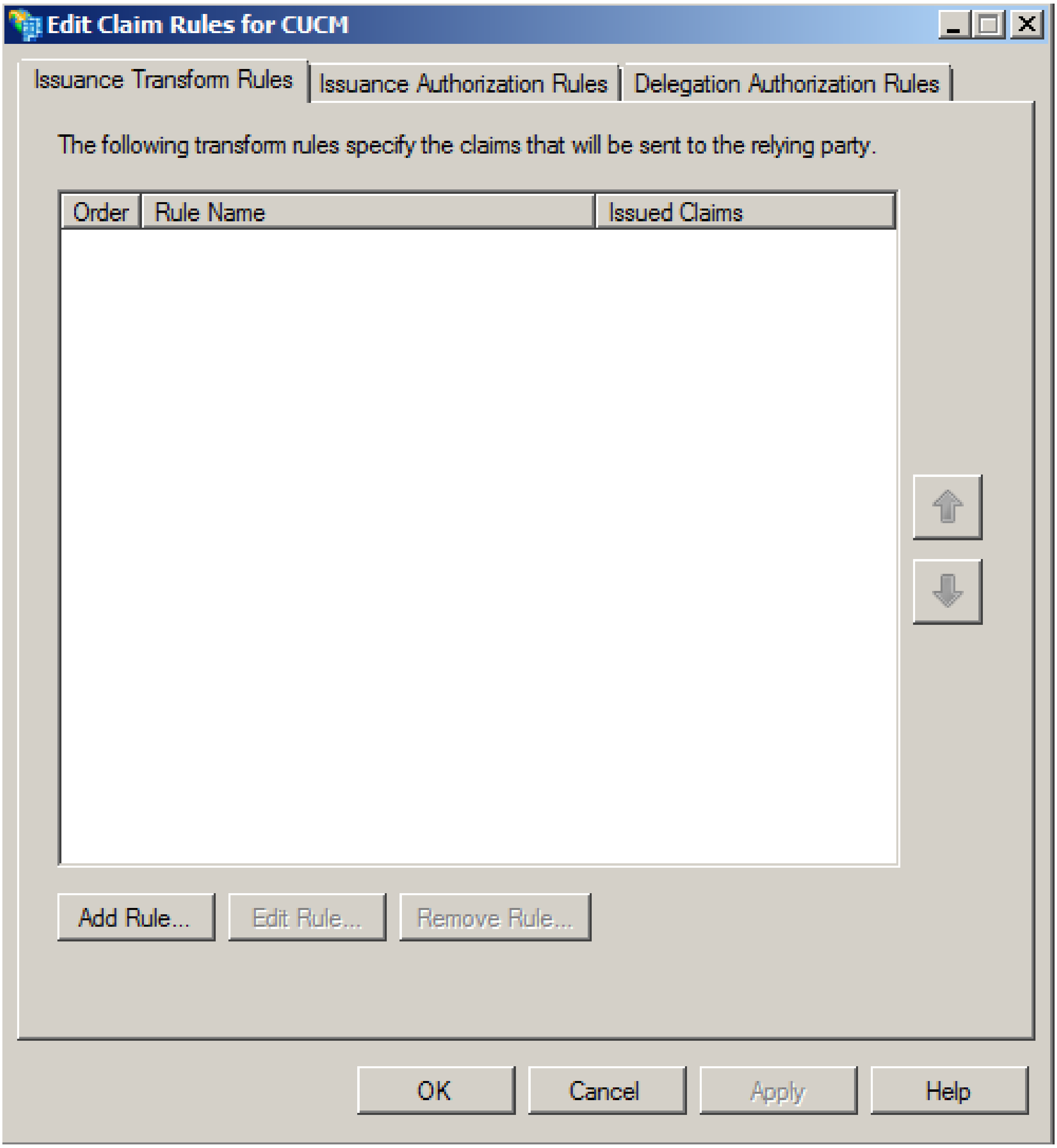
Finish

The relying party trust was successfully added to the AD FS configuration database.

You can modify this relying party trust by using the Properties dialog box in the AD FS 2.0 Management snap-in.

☑ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes

8. Click **Add Rule**.

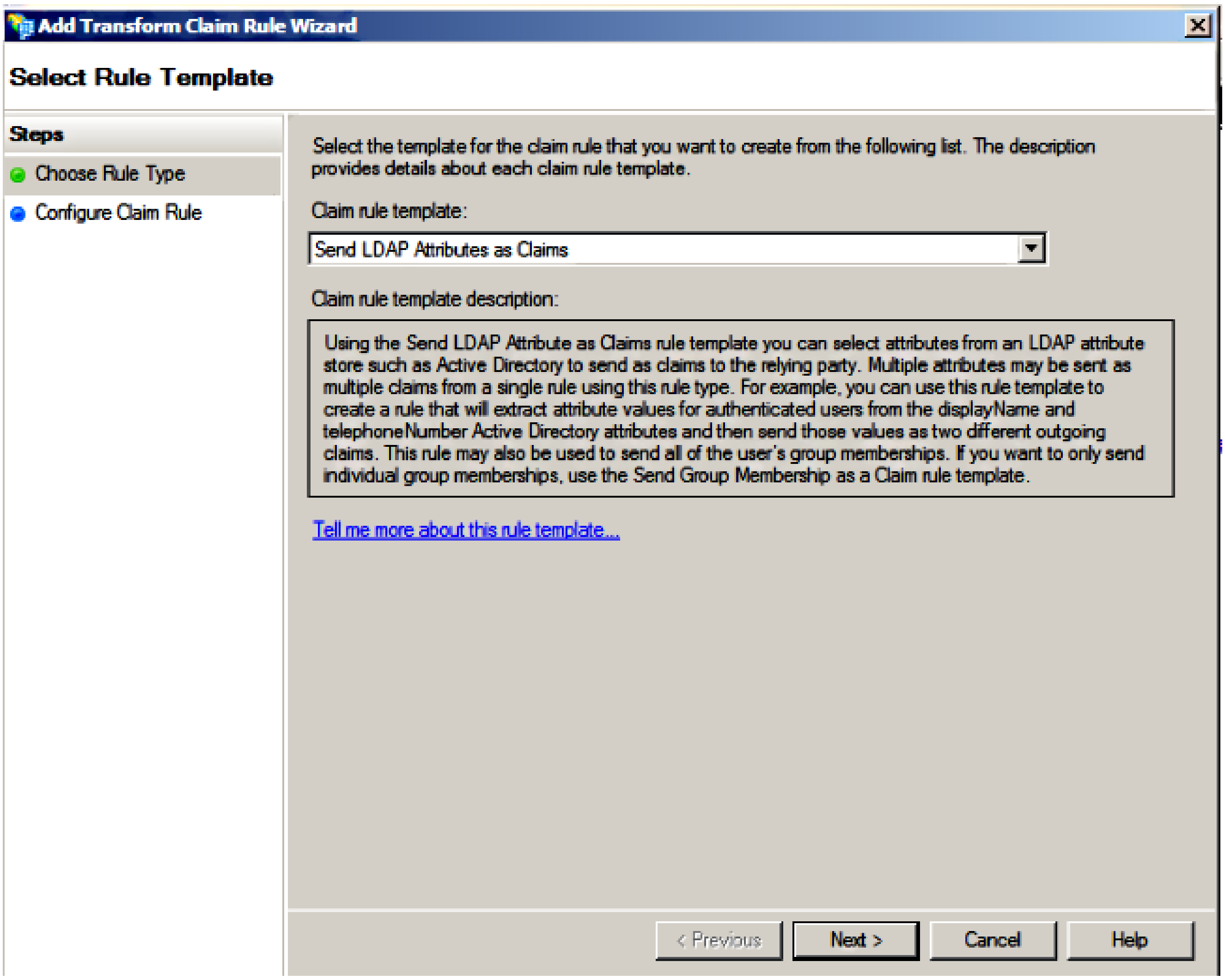


Edit Claim Rules for CUCM

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims

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



Add Transform Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send LDAP Attributes as Claims

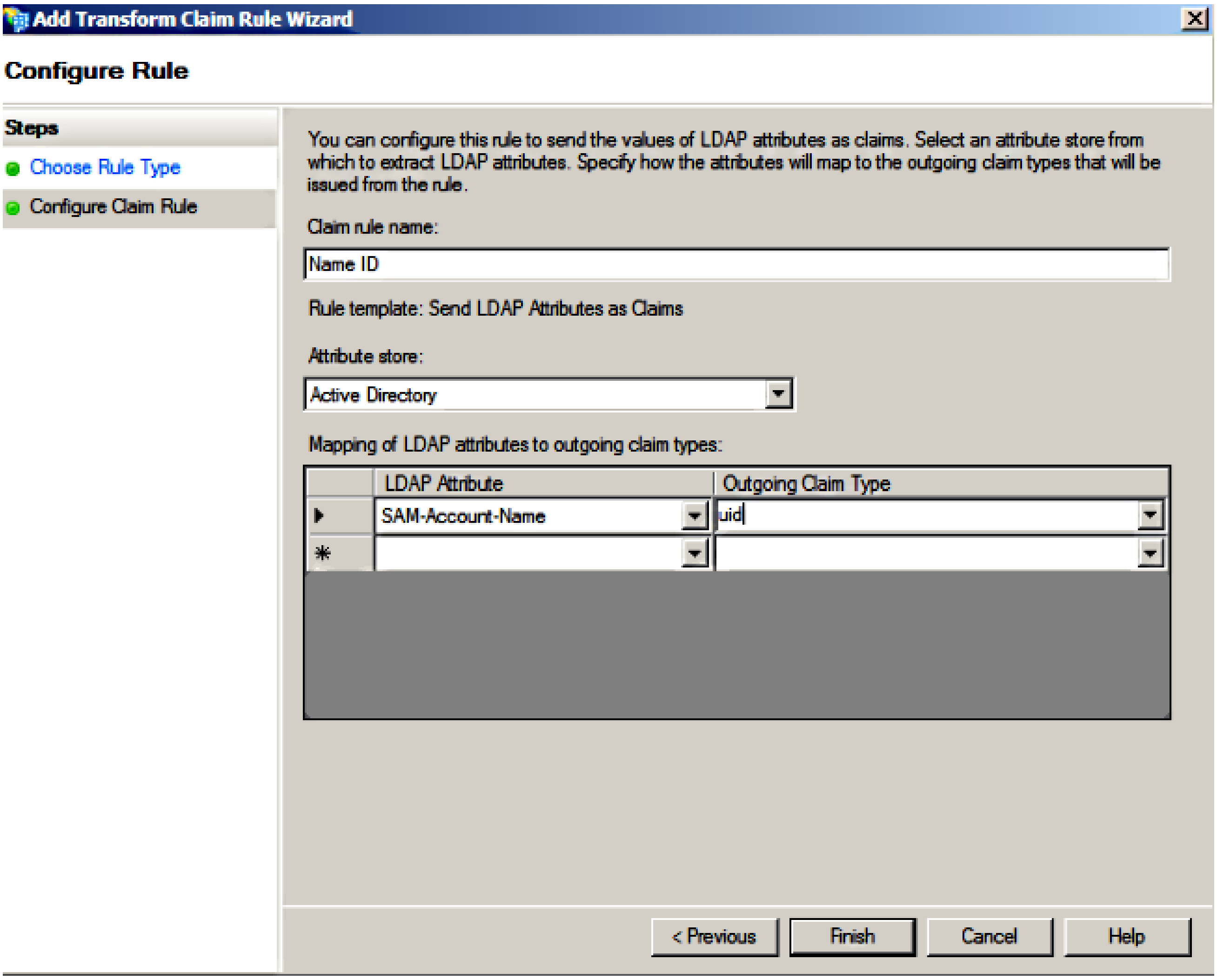
Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

Tell me more about this rule template...

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.



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

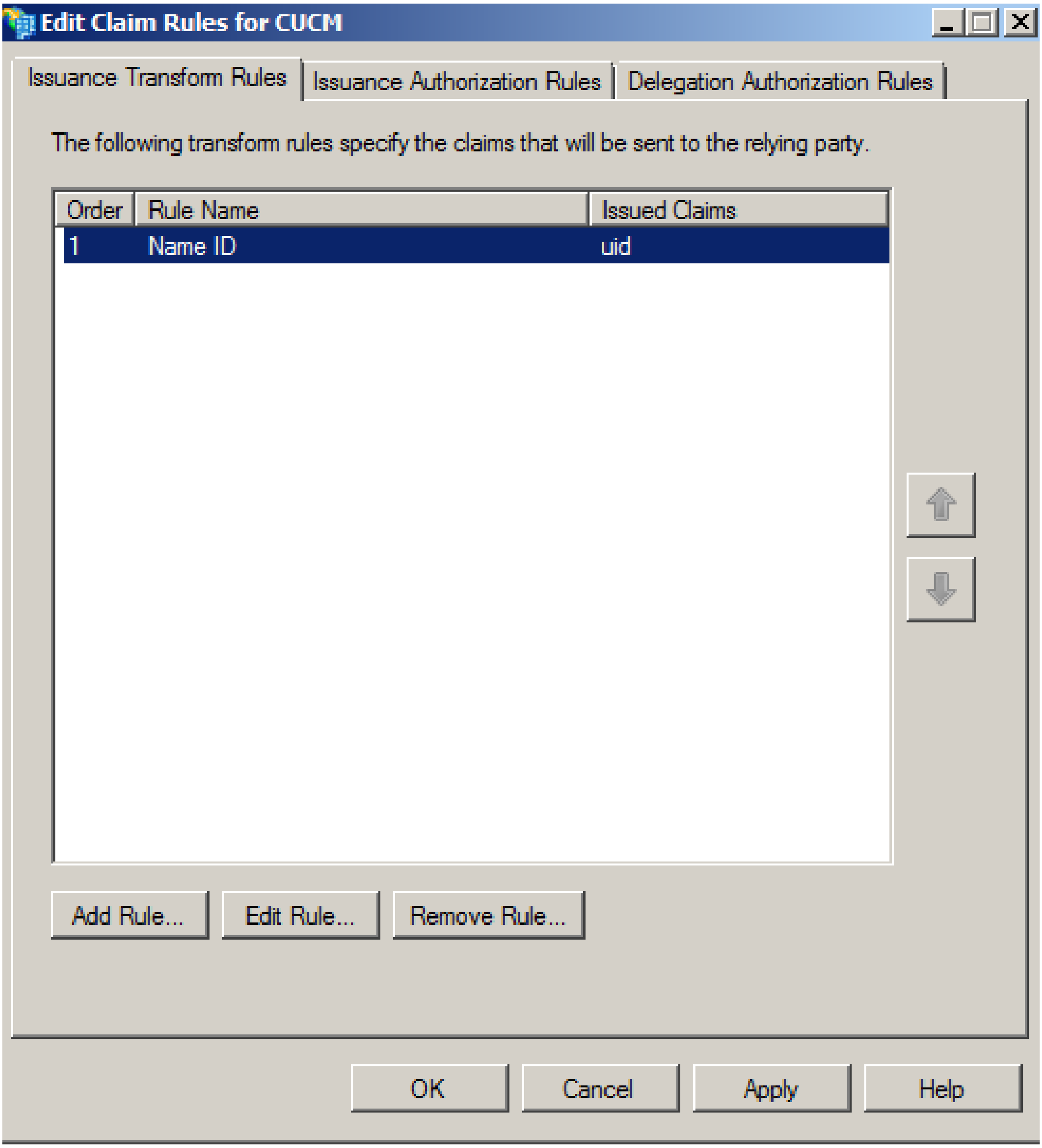
Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

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

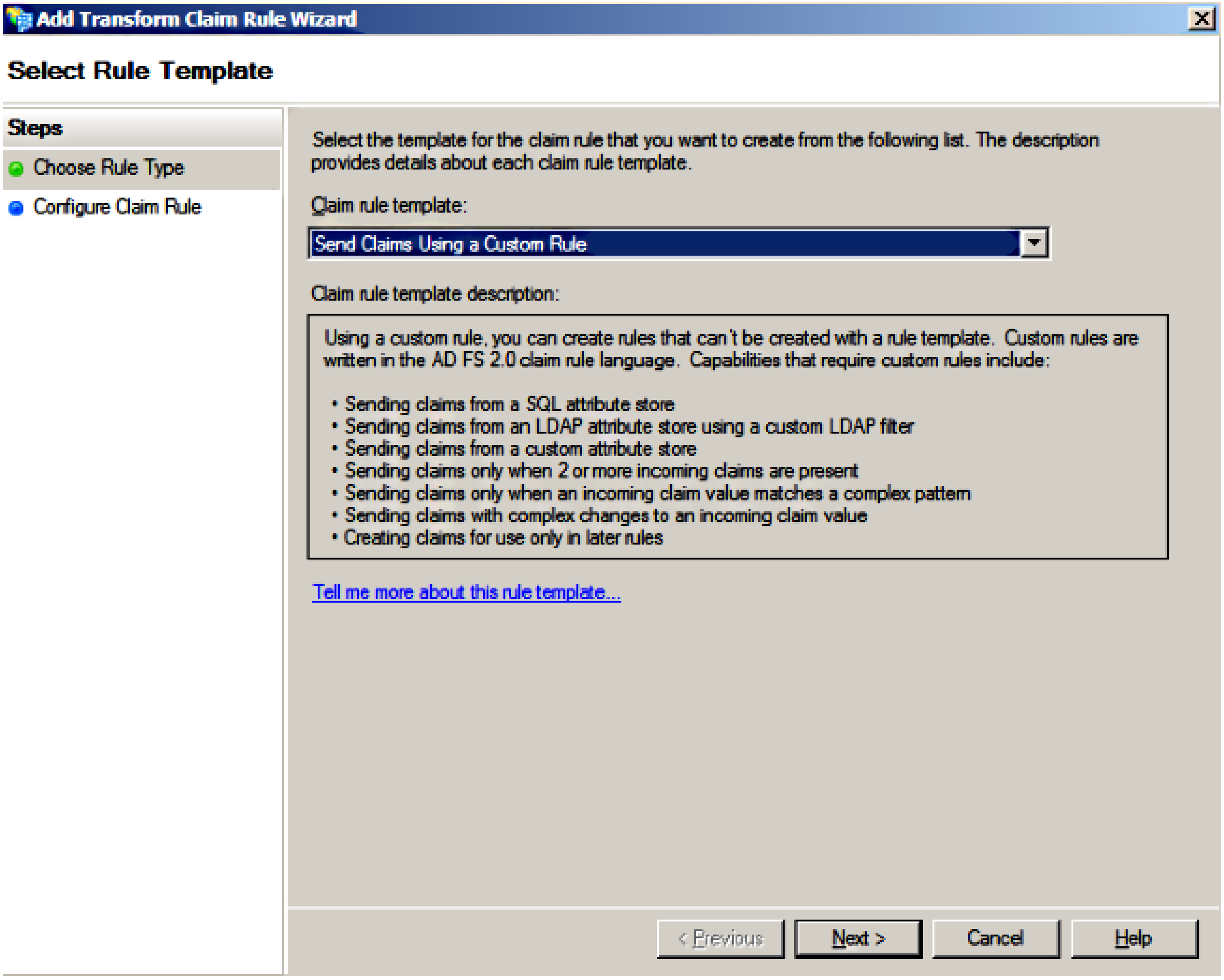
11. Click **Add Rule**, select **Send Claims Using a Custom Rule** as the claim rule template, and click **Next**.


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



Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send Claims Using a Custom Rule

Claim rule template description:

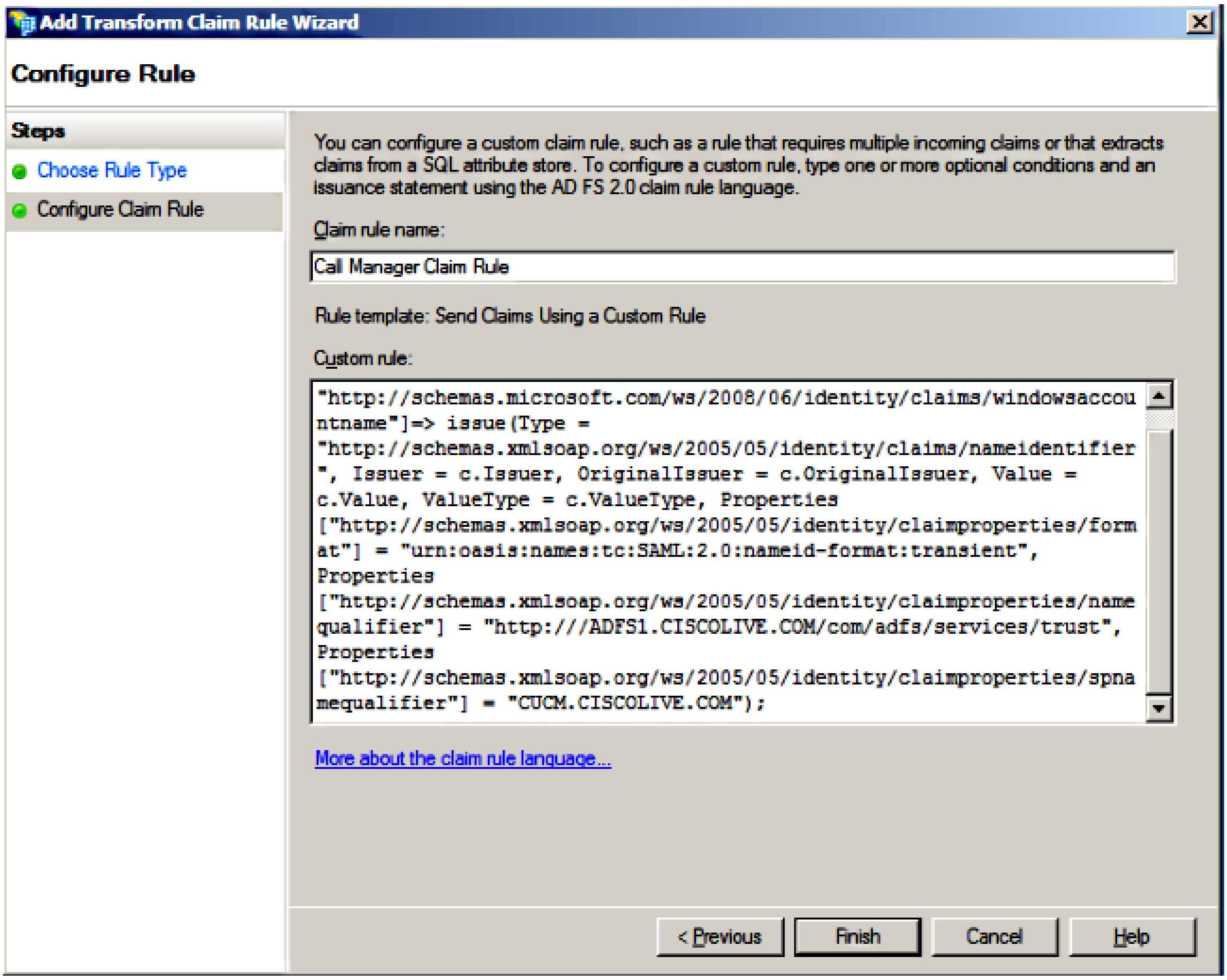
Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS 2.0 claim rule language. Capabilities that require custom rules include:

- Sending claims from a SQL attribute store
- Sending claims from an LDAP attribute store using a custom LDAP filter
- Sending claims from a custom attribute store
- Sending claims only when 2 or more incoming claims are present
- Sending claims only when an incoming claim value matches a complex pattern
- Sending claims with complex changes to an incoming claim value
- Creating claims for use only in later rules

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(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>");
```

(**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.)



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:

Call Manager Claim Rule

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccou
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"] = "CUCM.CISCOLIVE.COM");
```

More about the claim rule language...

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.**

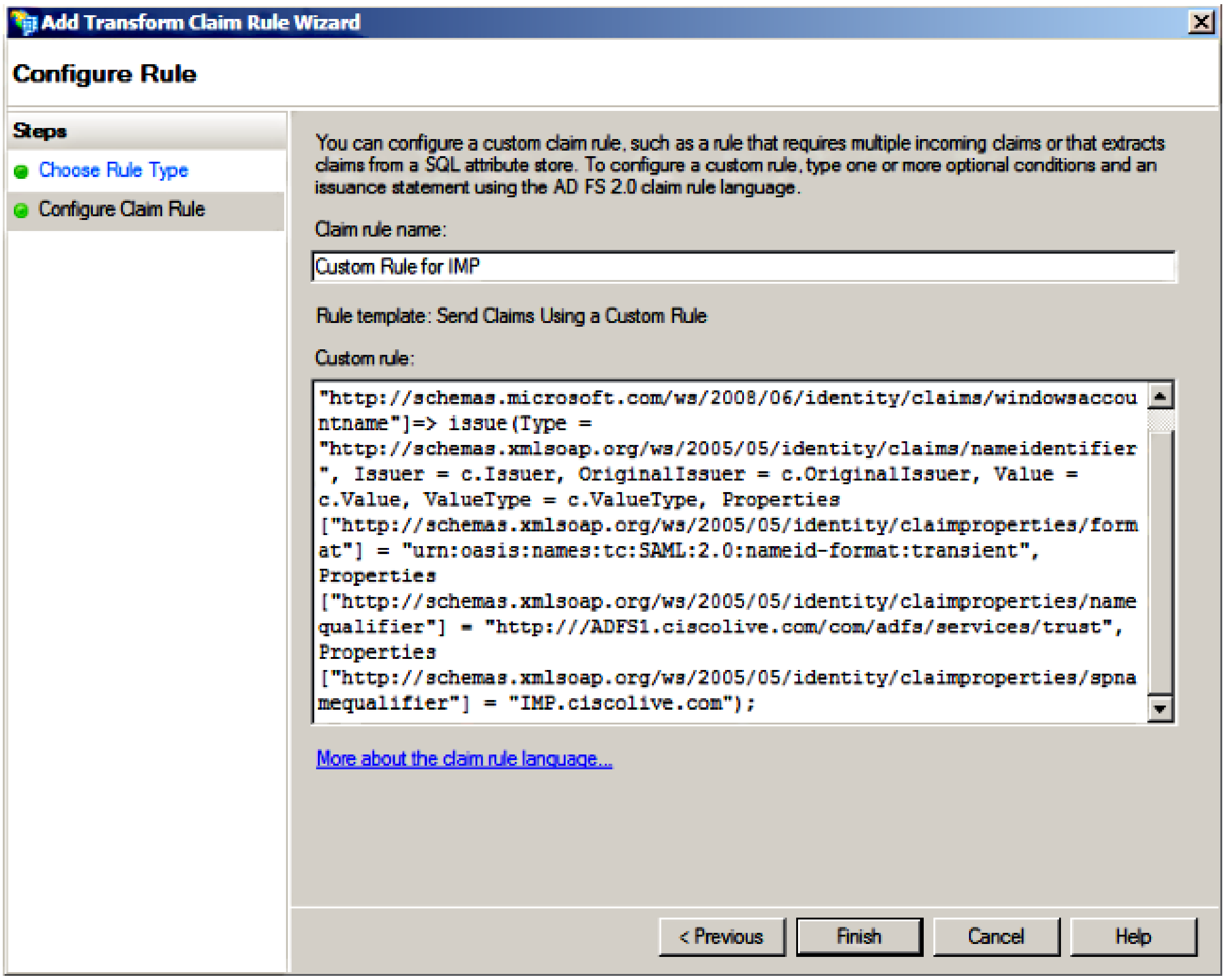
15. Restart the AD FS Version 2.0 service from **Services.msc**.

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(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>");
```



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 IMP

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccou
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"] = "IMP.ciscolive.com");
```

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.**

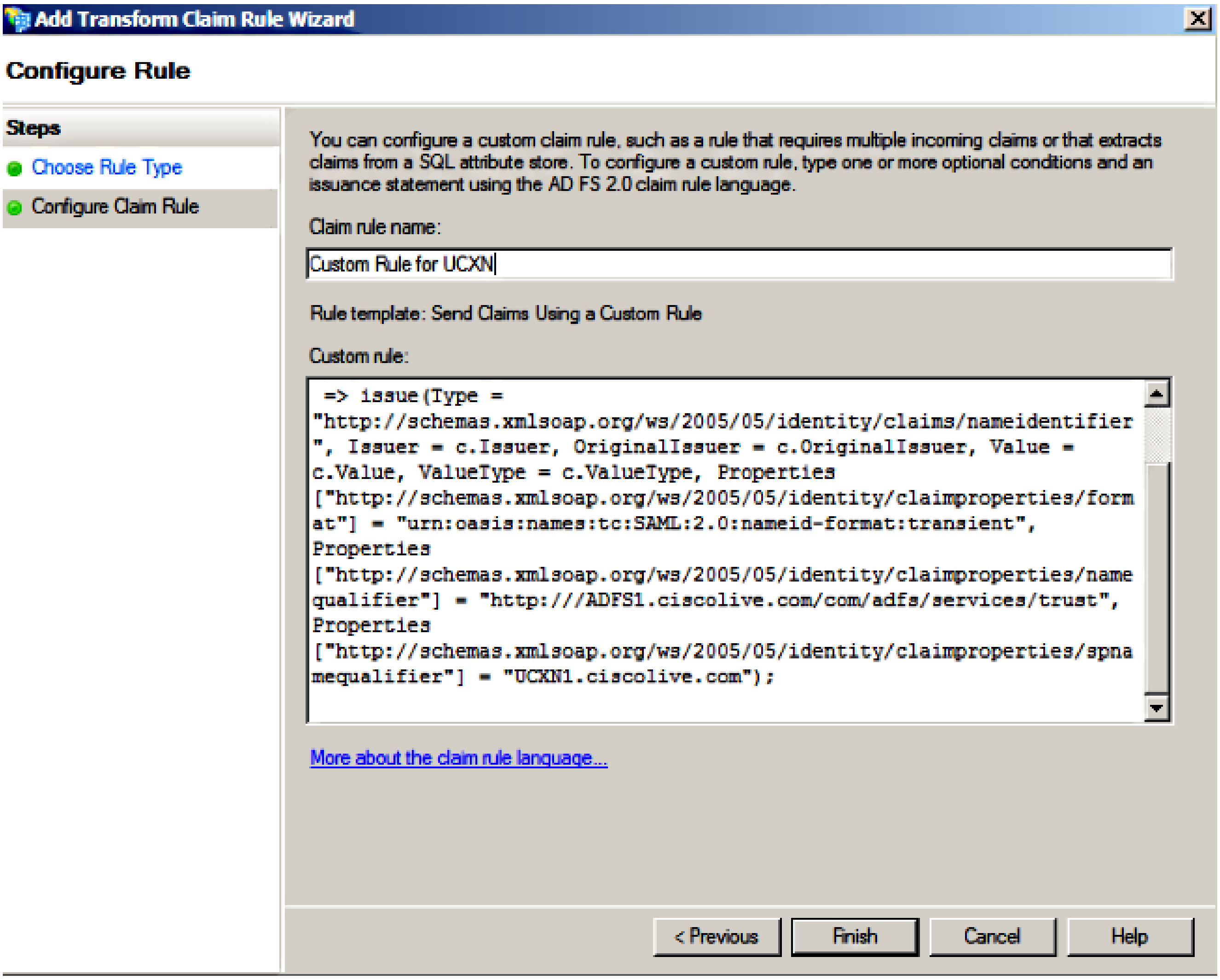
5. Restart the AD FS Version 2.0 service from **Services.msc.**

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(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>");
```



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 UCXN

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
 => 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"] = "UCXN1.ciscolive.com");
```

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**.

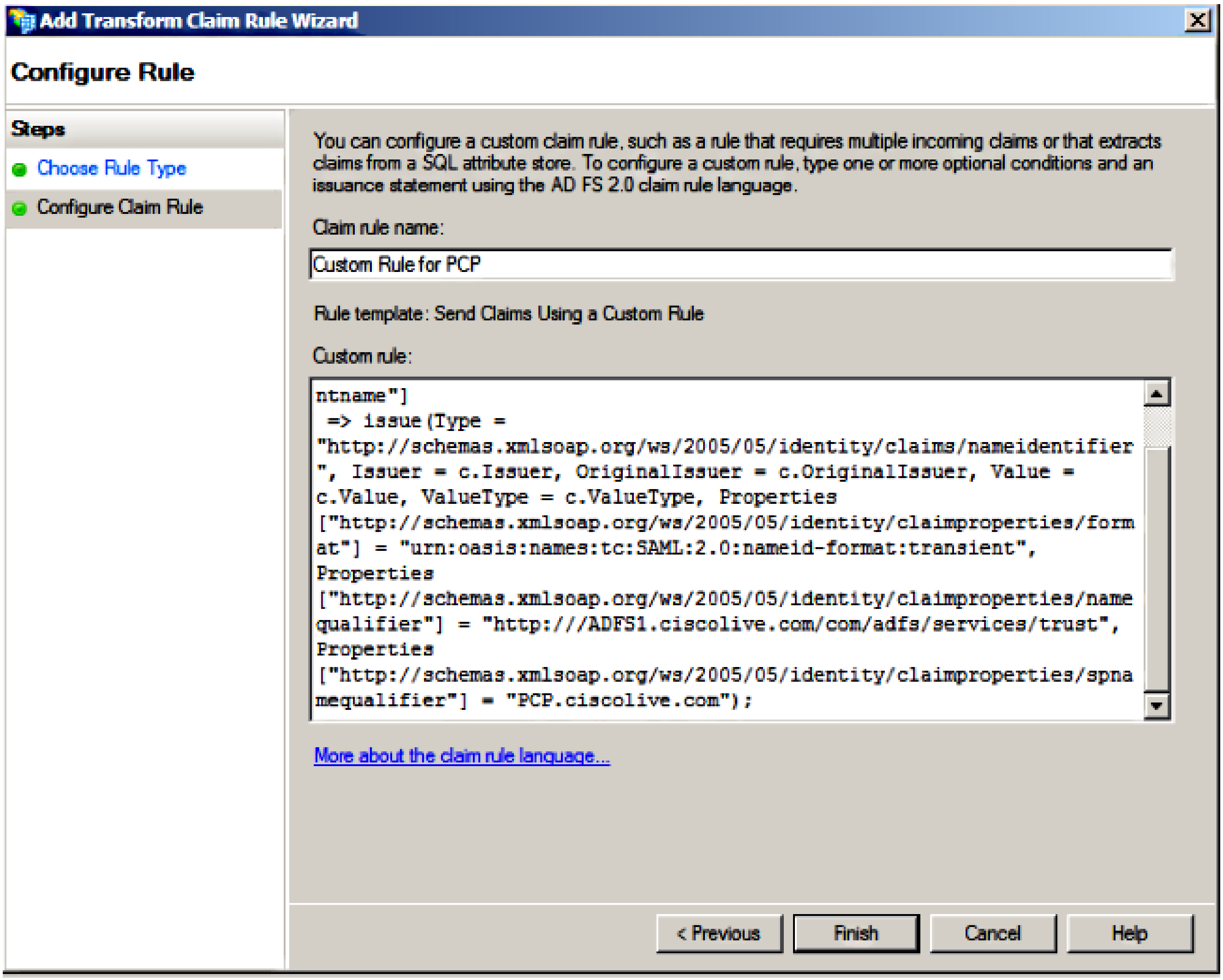
5. Restart the AD FS Version 2.0 service from **Services.msc.**

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(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>");
```



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");
```

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.

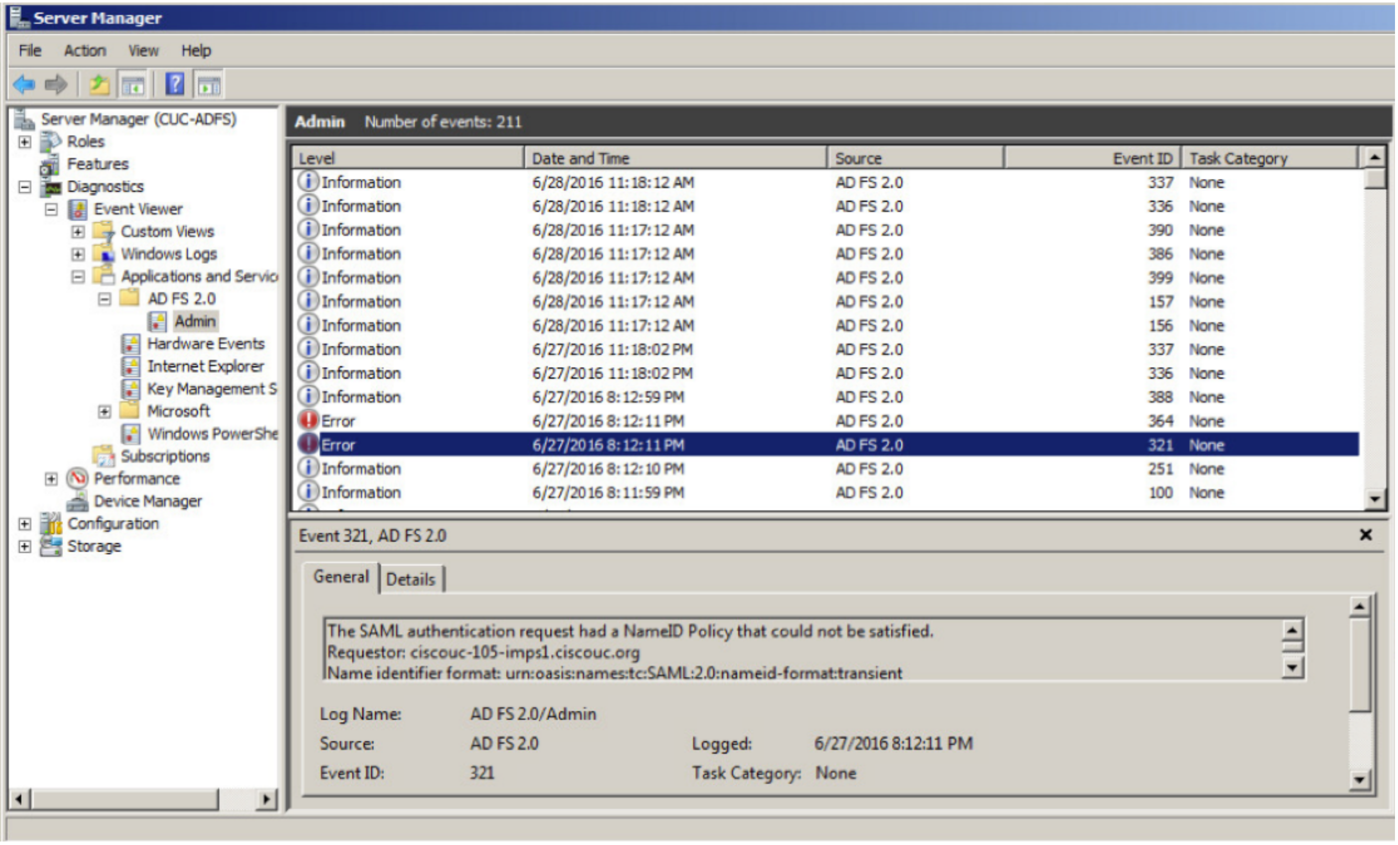
Verify

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



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

```
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