AD为SAML SSO配置示例设置的FS版本2.0

目录

简介

本文描述如何配置活动目录联邦服务(AD FS)版本2.0为了启用安全断言标记语言(SAML)单一登录(SSO) Cisco协作产品的类似Cisco Unified Communications Manager (CUCM)， Cisco Unity Connection (UCXN)， CUCM IM和在线状态和Cisco头等协作。

先决条件

要求

AD必须安装和测试FS版本2.0。

> **Caution**:此安装指南根据实验室设置，并且AD FS版本2.0假设仅使用SAML SSO用Cisco协作产品。万一其他商业关键应用使用它，然后必要的自定义必须根据正式Microsoft文档完成。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- AD FS版本2.0
- 微软Internet Explorer 10
- CUCM版本10.5
- Cisco IM和Presence Server版本10.5

- UCXN版本10.5
- 思科设置10.5的最初协作

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

下载AD FS版本2.0标识供应商(IdP)元数据

为了下载IdP元数据，请运行在您的此链路浏览器：https:// ADFS>/FederationMetadata/2007-06/FederationMetadata.xml <FQDN。

下载Collaboration Server (SP)元数据

CUCM IM和在线状态服务

打开Web浏览器，登录CUCM作为管理员，并且导航对**系统> SAML单个符号**。

Unity Connection

打开Web浏览器，登录UCXN作为管理员，并且导航对**系统设置> SAML单个符号**。

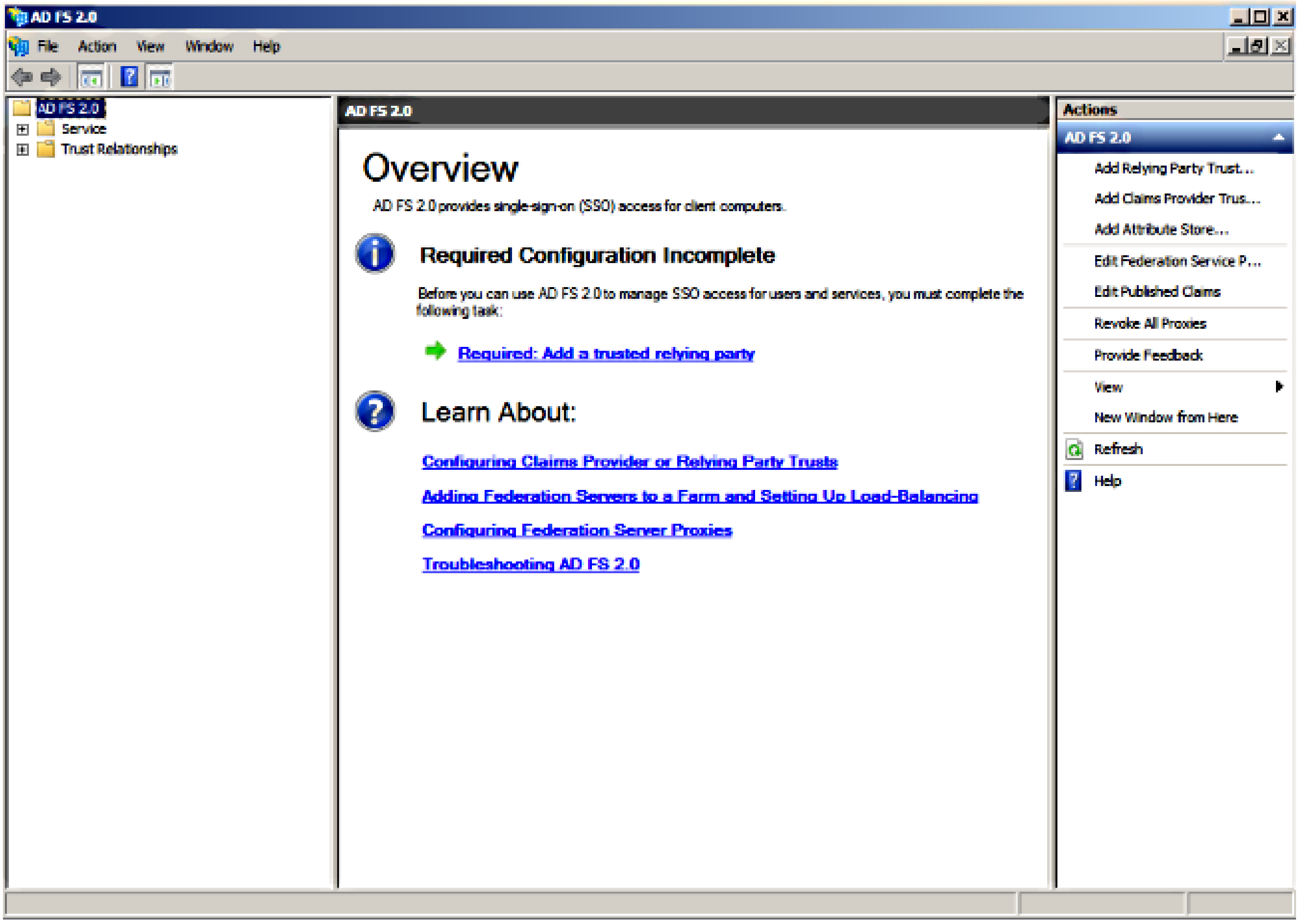
思科最初协作供应

打开Web浏览器，登录头等协作保证作为globaladmin，并且导航对**设置的管理>System >单个符号**。

添加CUCM，取决于Party托拉斯

1. 登录从Microsoft Windows**程序**菜单的AD FS服务器和启动AD FS版本2.0。

2. 选择**添加取决于Party托拉斯**。



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:

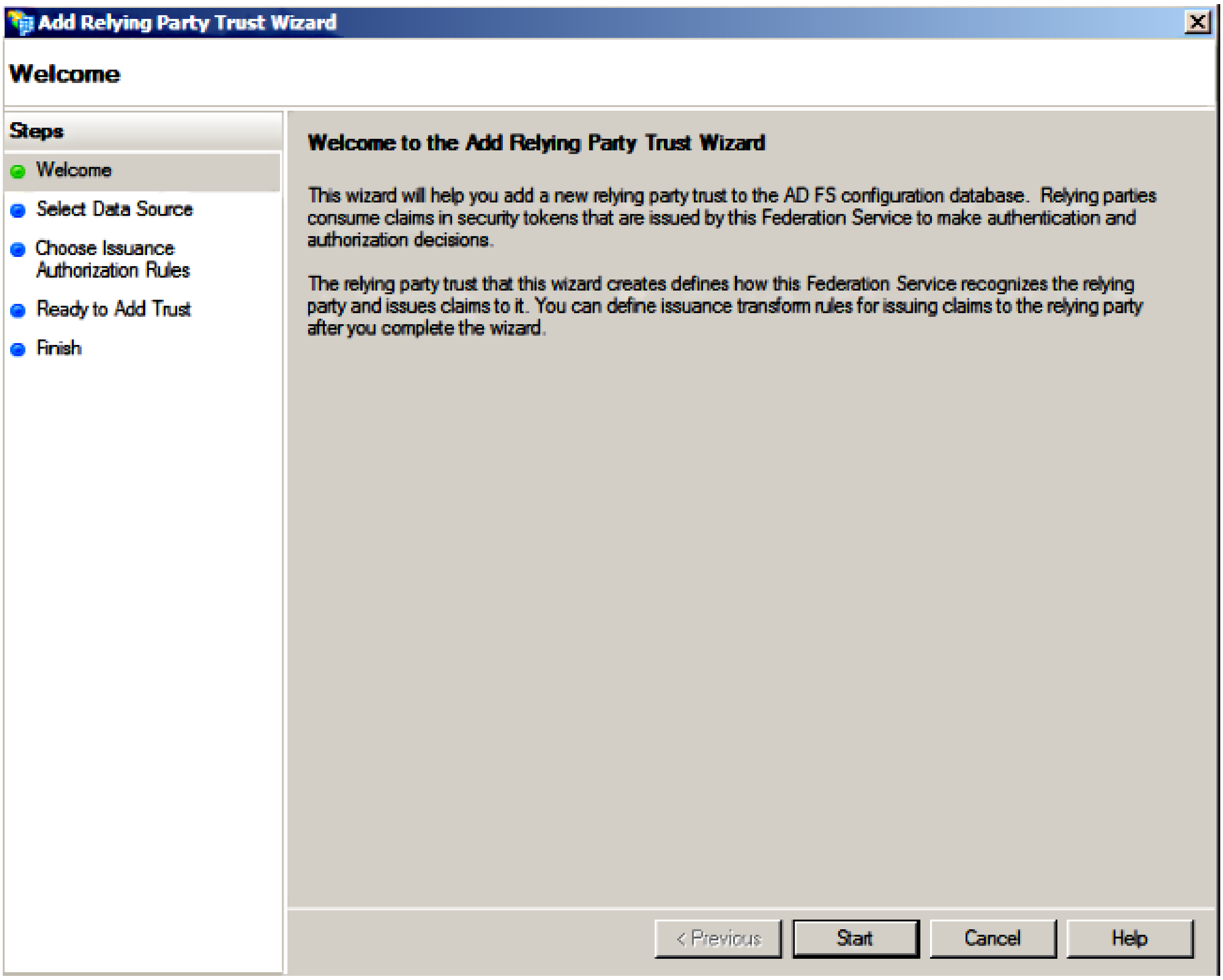
Configuring Claims Provider or Relying Party Trusts

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

Configuring Federation Server Proxies

Troubleshooting AD FS 2.0

3. 单击开始。

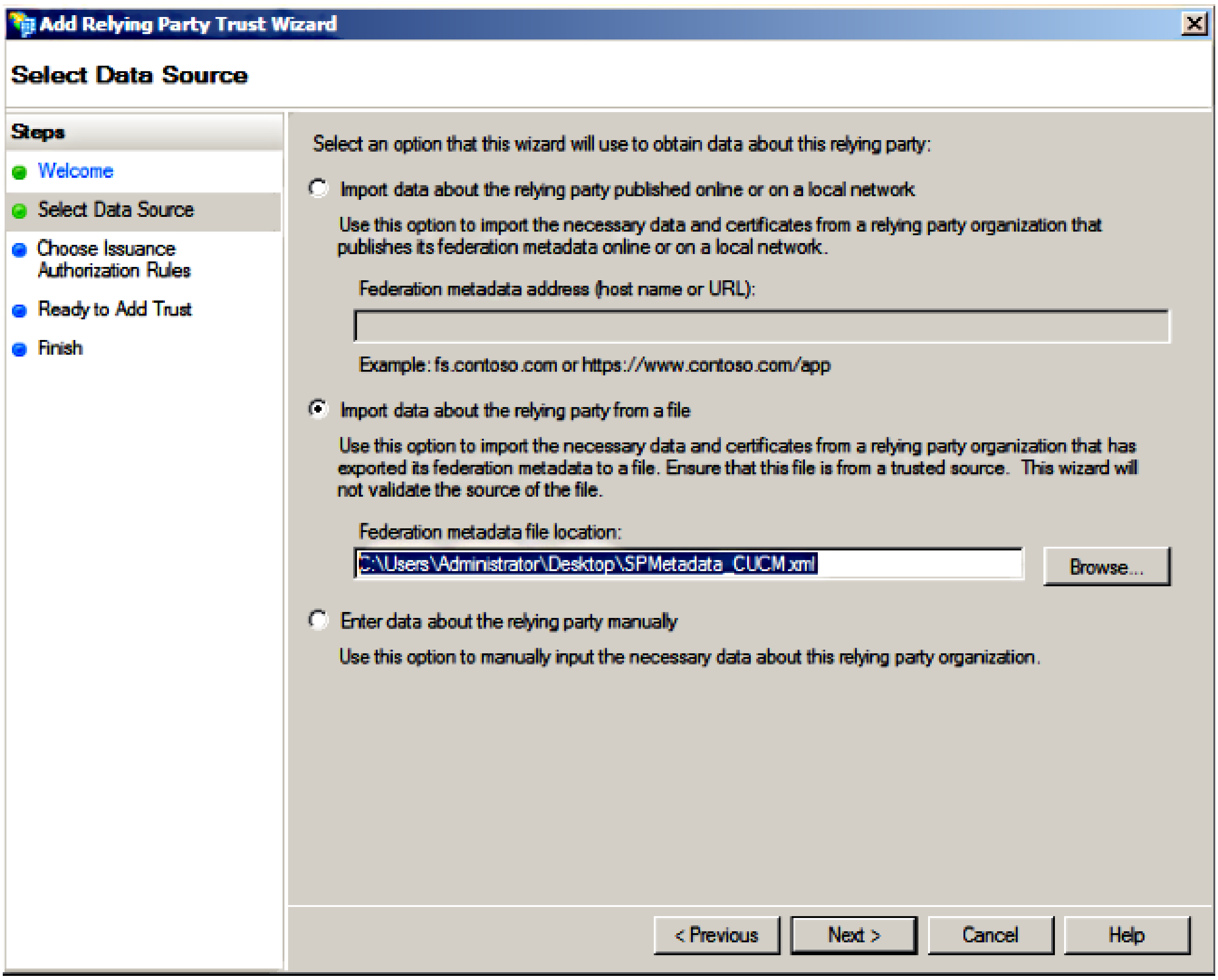


Welcome to the Add Relying Party Trust Wizard

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. 选择**关于取决于的当事人的导入数据从文件选项**，选择您从CUCM下载前的**SPMetadata_CUCM.xml元数据**文件，并且其次单击**。**



Select Data Source

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

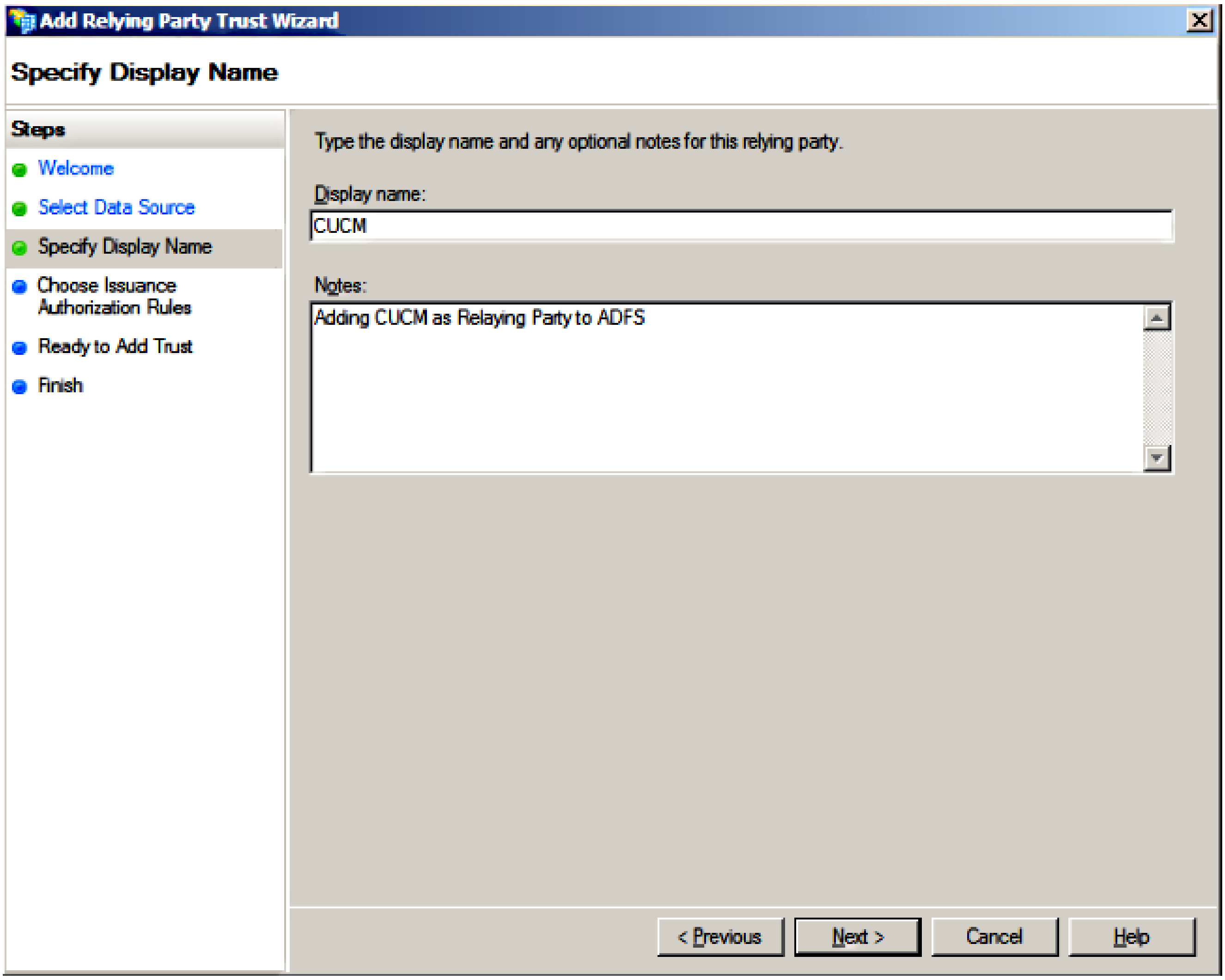
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

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. 输入**显示名称**并且**其次**单击。



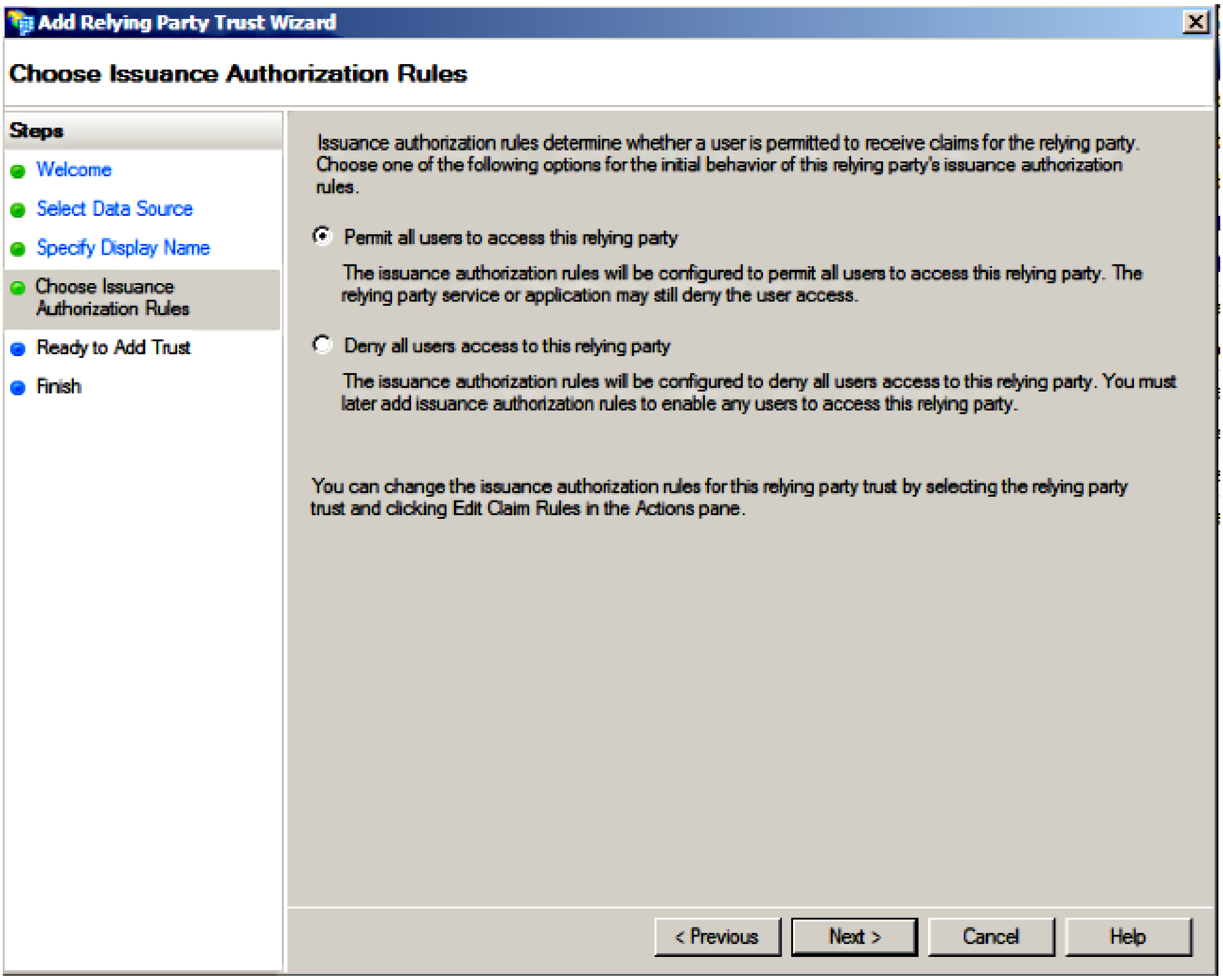
Specify Display Name

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

Display name: CUCM

Notes: Adding CUCM as Relaying Party to ADFS

6. 选择**Permit所有用户访问此取决于的当事人**并且**其次**单击。



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

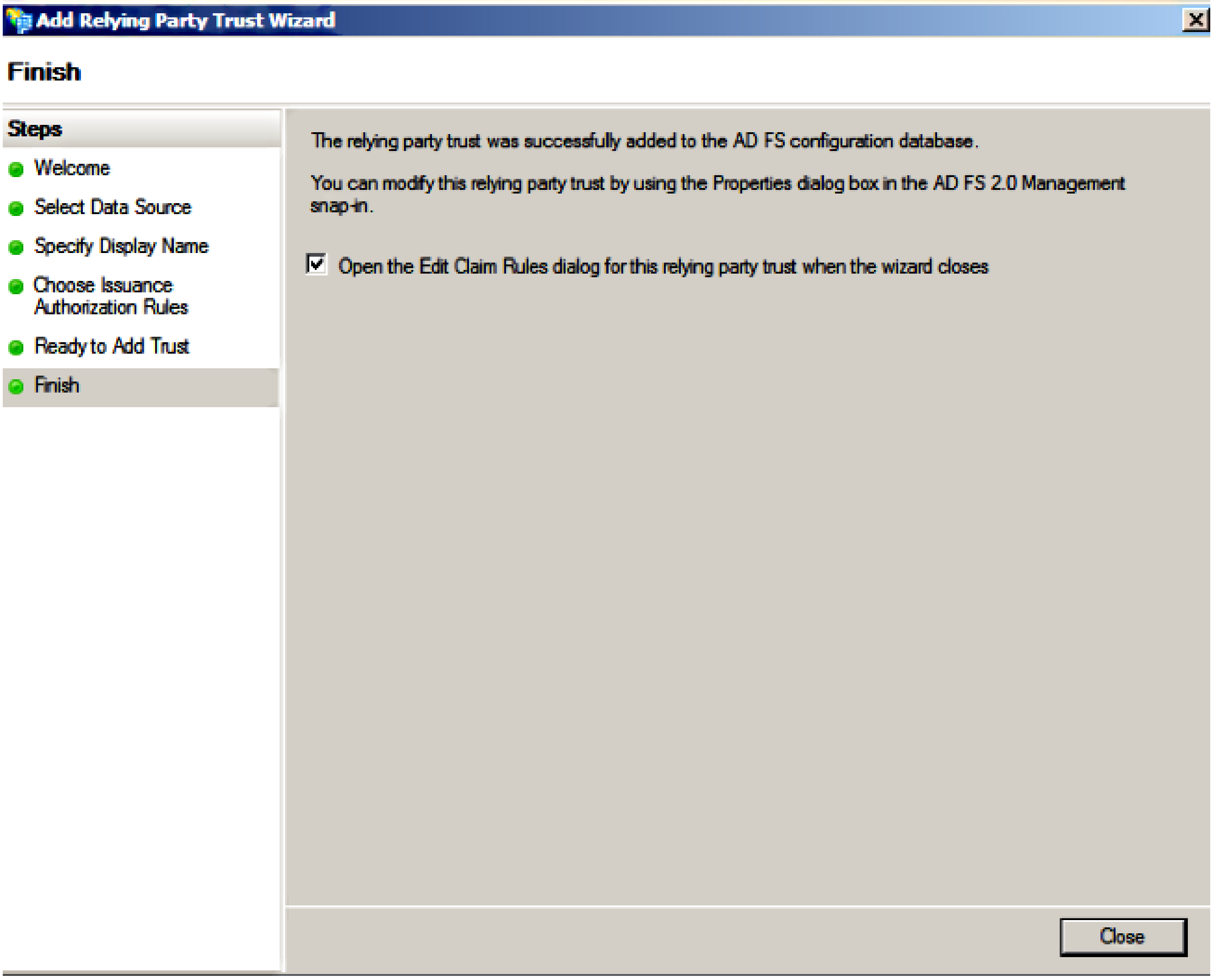
The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ 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. 选择**开放取决于当事人信任的thee的编辑声明规则对话，当向导关闭时**并且点击**Close。**

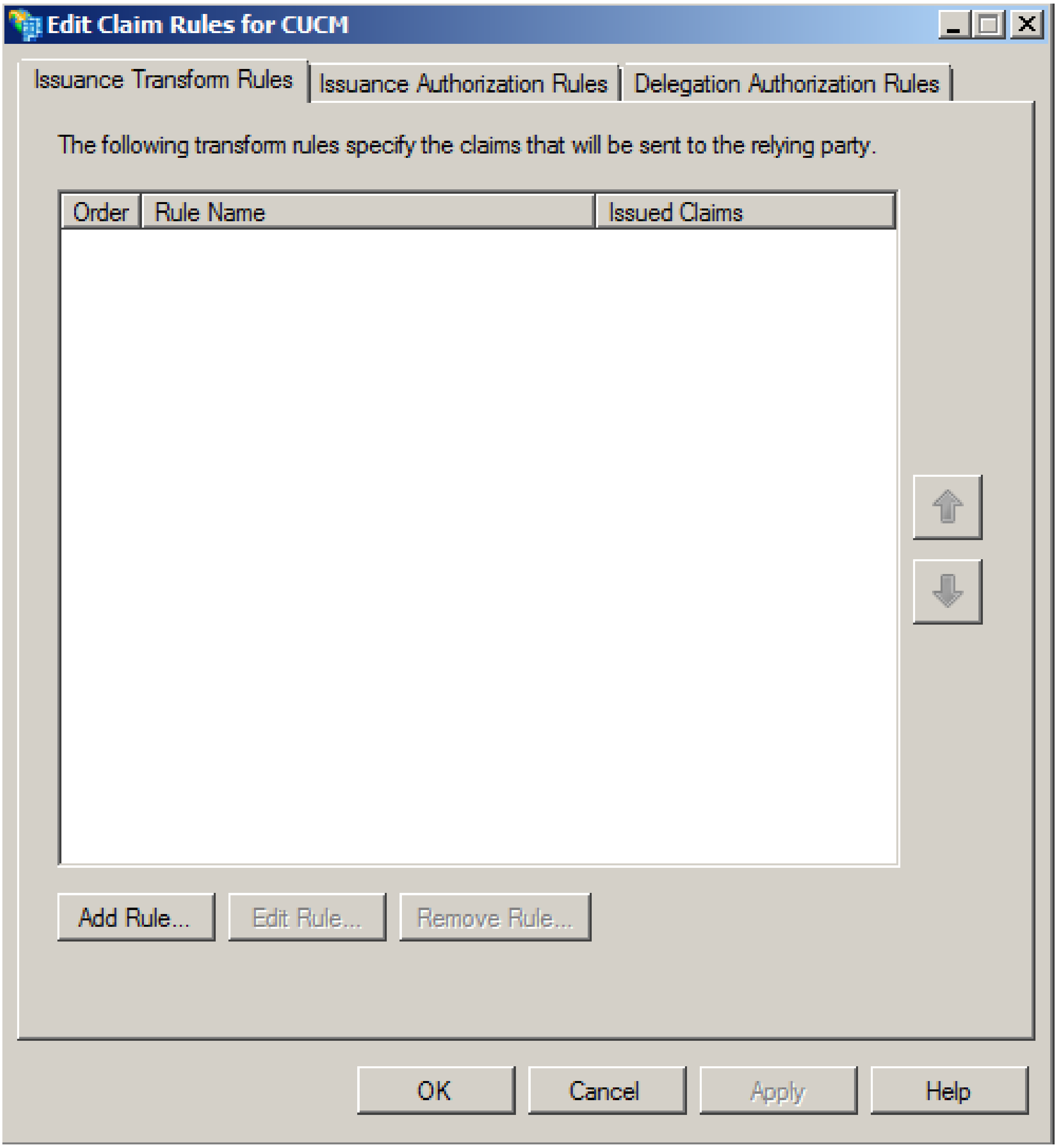


The relying party trust was successfully added to the AD FS configuration database.

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. 单击**增加规则**。



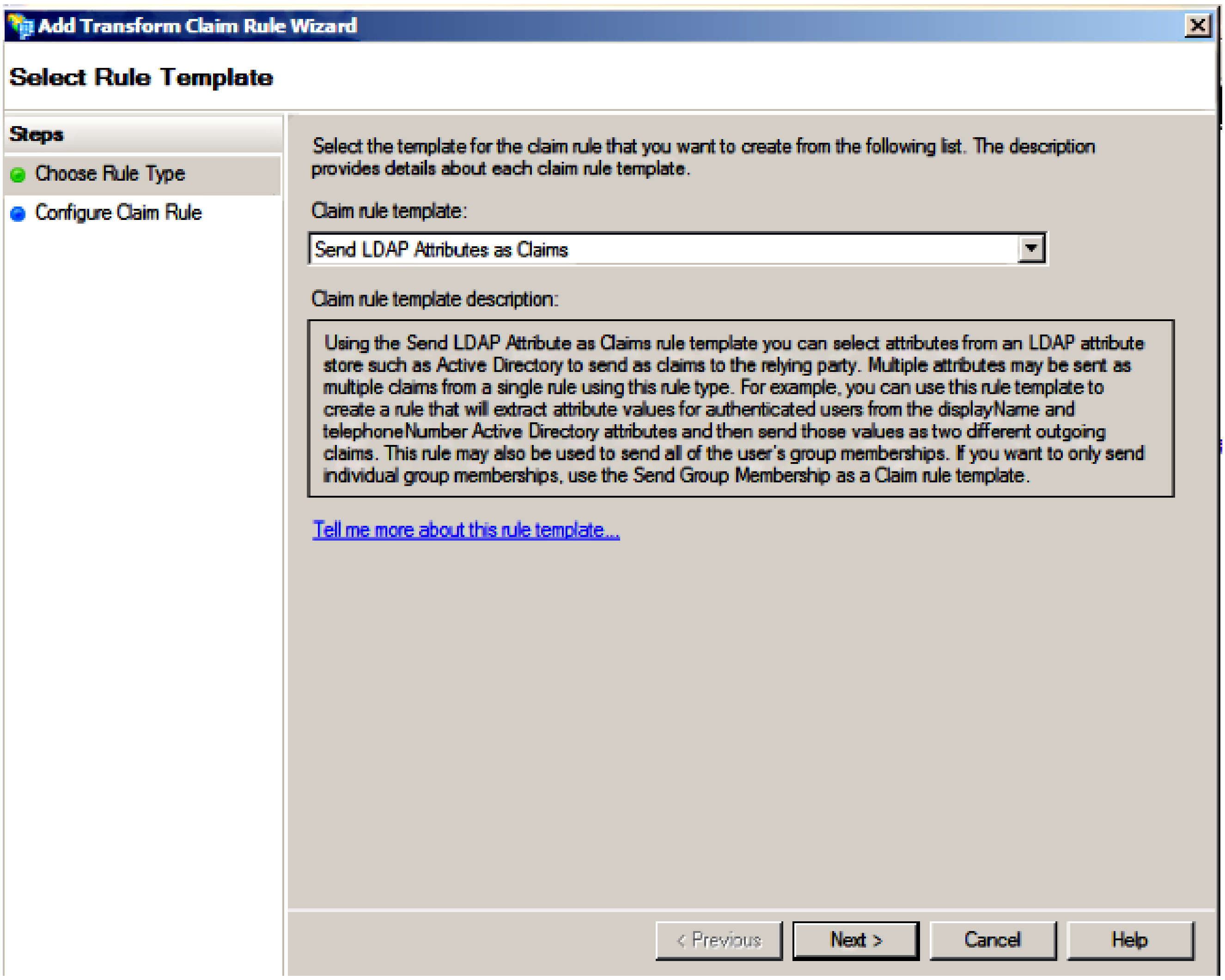
Edit Claim Rules for CUCM
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules

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

Order	Rule Name	Issued Claims

Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply
Help

9. 用默认声明设置的规则模板**其次**单击**发送LDAP属性作为要求**。



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.

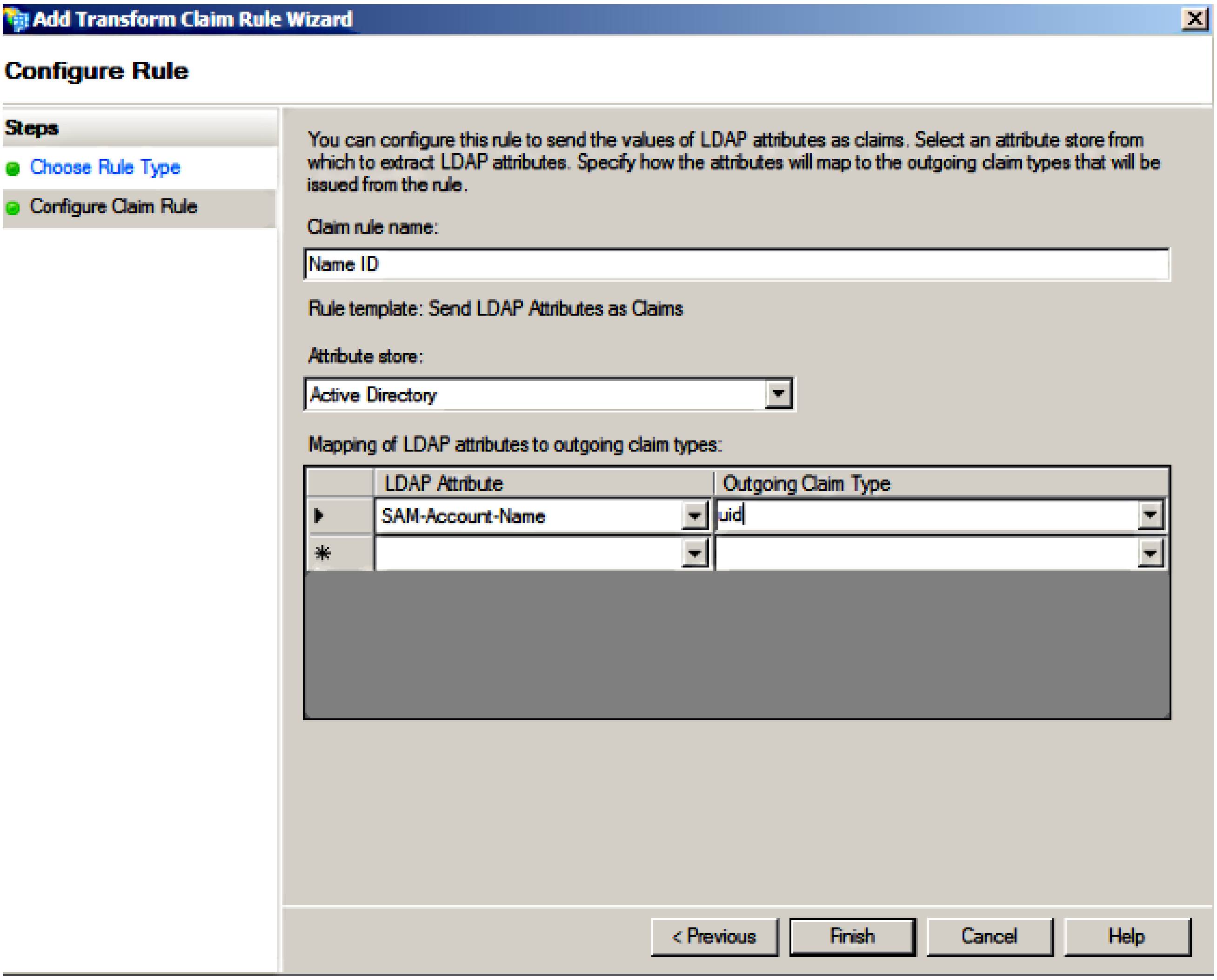
Claim rule template: Send LDAP Attributes as Claims

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.

10. 在请配置规则，输入声明规则名称，选择**活动目录，**当如此镜像所显示，属性存储，配置**LDAP属性**和**流出的声明类型**，并且点击**芬通社**。

    Note:
    -轻量级目录访问协议(LDAP)属性应该匹配在CUCM的目录同步属性。
    - “uid”应该用小写。



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

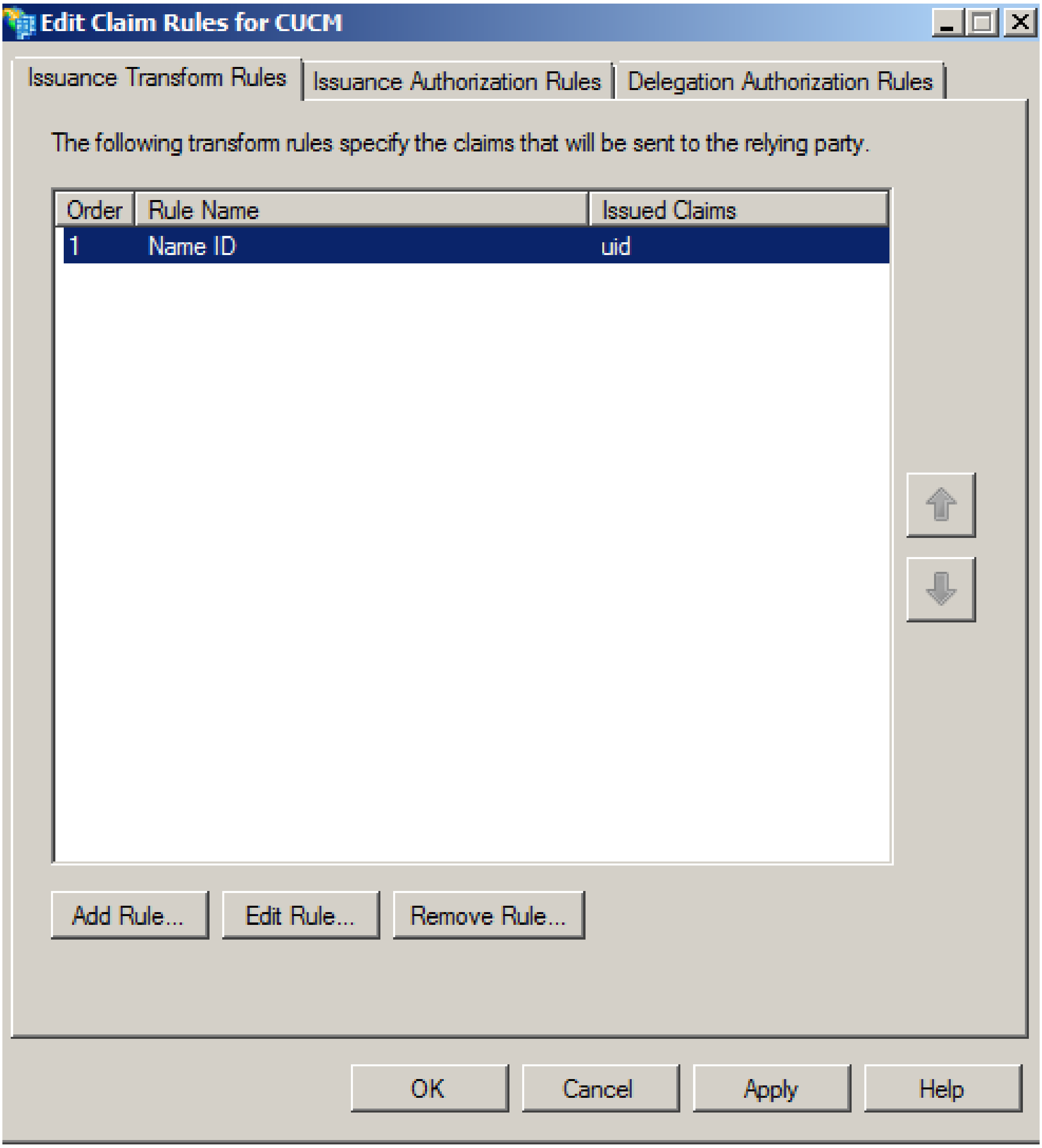
Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

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

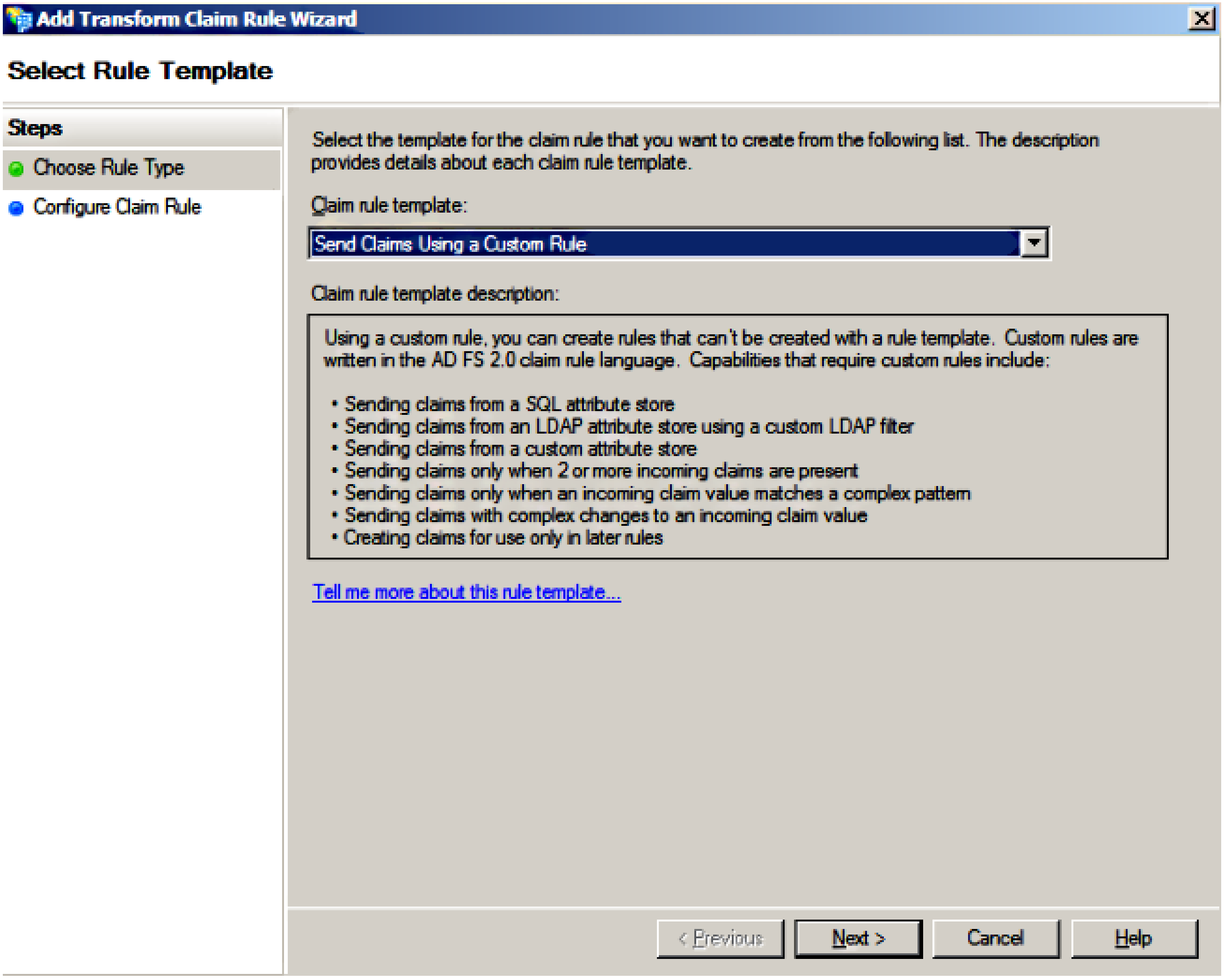
11. 单击**增加规则**，选择**发送要求使用海关规则，**声明规则模板，并且**其次**单击。



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
1	Name ID	uid



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:

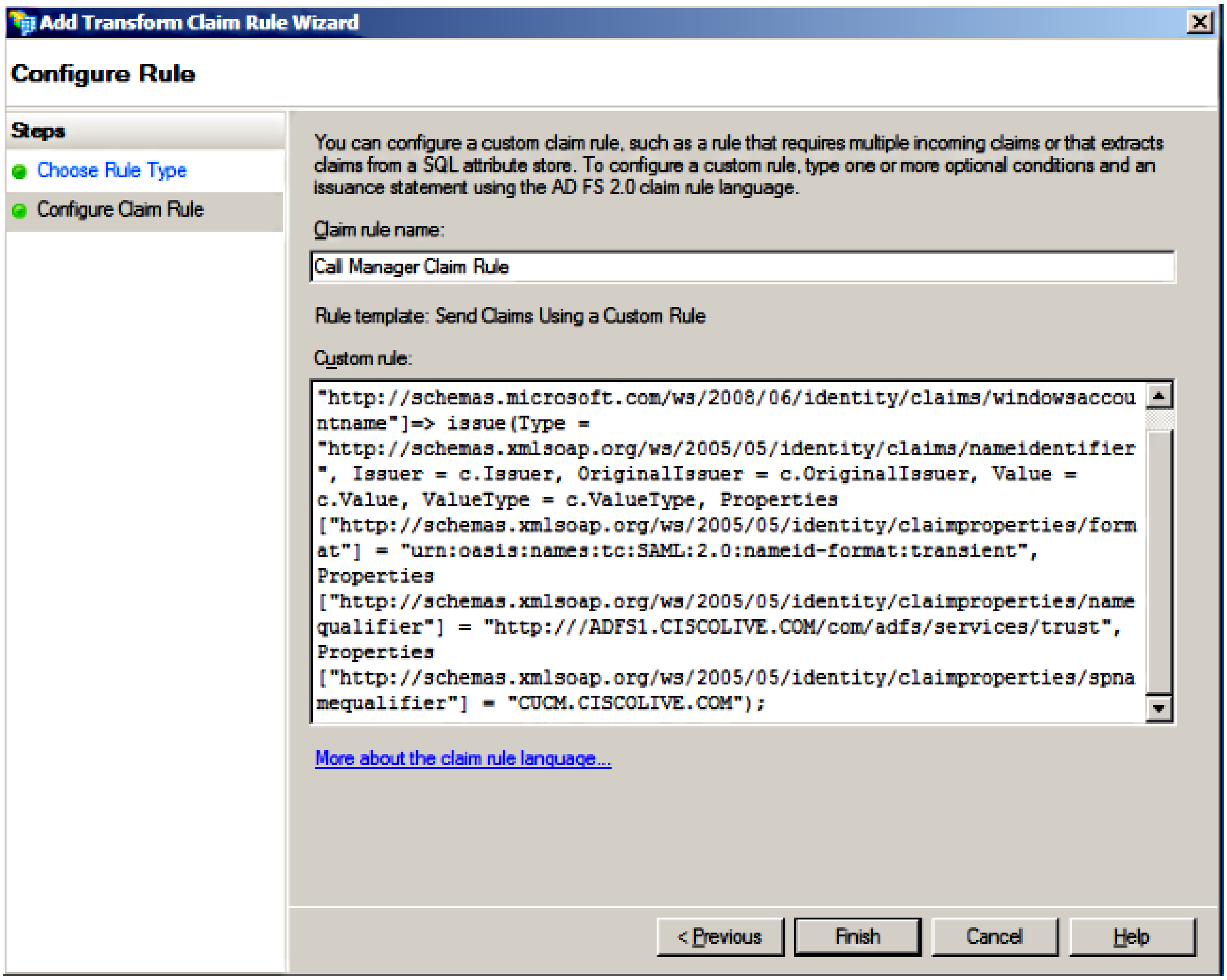
- Sending claims from a SQL attribute store
- Sending claims from an LDAP attribute store using a custom LDAP filter
- Sending claims from a custom attribute store
- Sending claims only when 2 or more incoming claims are present
- Sending claims only when an incoming claim value matches a complex pattern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

Tell me more about this rule template...

12. 输入一名称对于声明规则名称并且复制在根据海关规则给的空间的此语法：

```
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>");
```

(注意: 如果复制和插入从这些示例的文本，请注意若干文字处理软件将替代ASCII引号(")与UNICODE版本("")。 UNICODE版本将导致声明规则发生故障。)



Configure 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:

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和ADFS完全合格的域名(FQDN)事前填充与实验室CUCM和AD FS在本例中，并且必须修改匹配您的环境。
- CUCM/ADFS FQDN区分大小写，并且必须用元数据文件匹配。

13. 单击 **完成**。

14. 依次单击应用和确定。

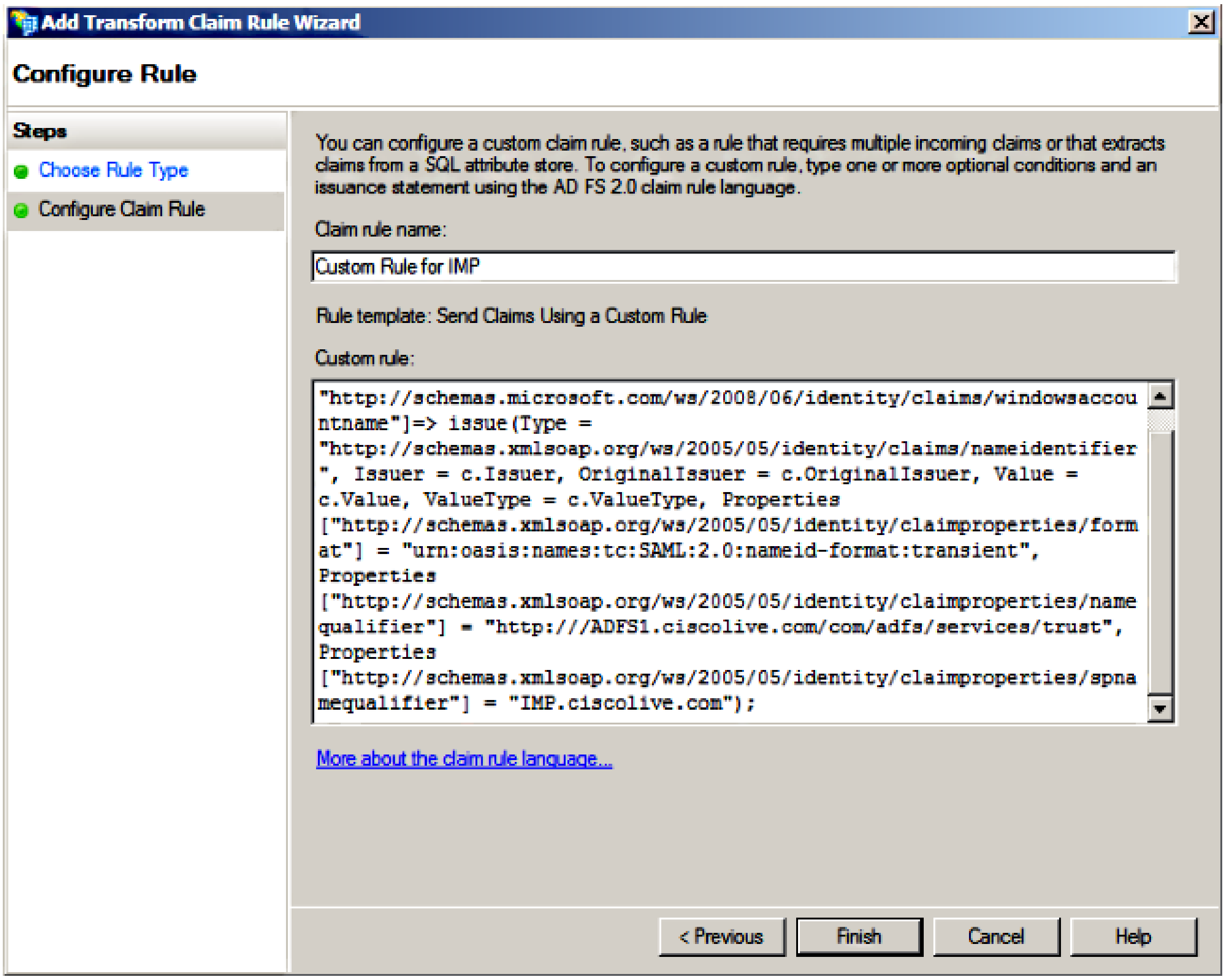
15. 重新启动从**Services.msc的**AD FS版本2.0服务。

添加CUCM IM和在线状态，取决于Party托拉斯

1. 重复步骤1到11如描述为**Add CUCM，取决于Party托拉斯**并且继续对步骤2。

2. 输入一名称对于声明规则名称并且复制在根据海关规则给的空间的此语法：

```
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");
```

注意IM和在线状态和AD FS FQDN事前填充与实验室IM和在线状态和AD FS在本例中，并且必须修改匹配您的环境。

3. 单击 **完成**。

4. 依次单击应用和确定。

5. 重新启动从**Services.msc的**AD FS版本2.0服务。

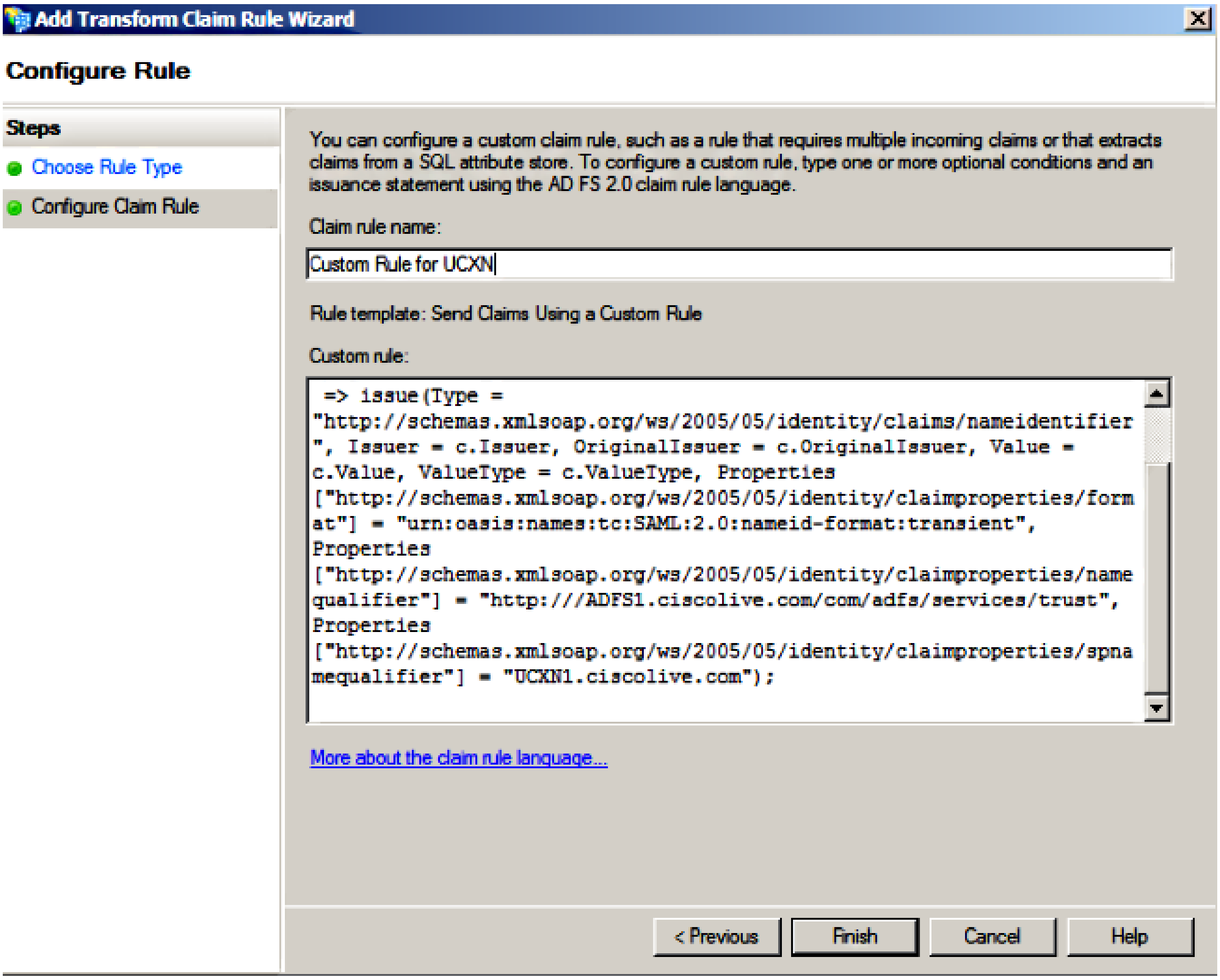
添加UCXN，取决于Party托拉斯

1. 重复步骤1到12如描述为**Add CUCM，取决于Party托拉斯**并且继续对步骤2。

2. 输入一名称对于声明规则名称并且复制在根据海关规则给的空间的此语法：

```
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");
```

More about the claim rule language...

注意UCXN和AD FS FQDN事前填充与在本例中的实验室UCXN和ADFS，并且必须修改匹配您的环境。

3. 单击 **完成**。

4. 依次单击应用和确定。

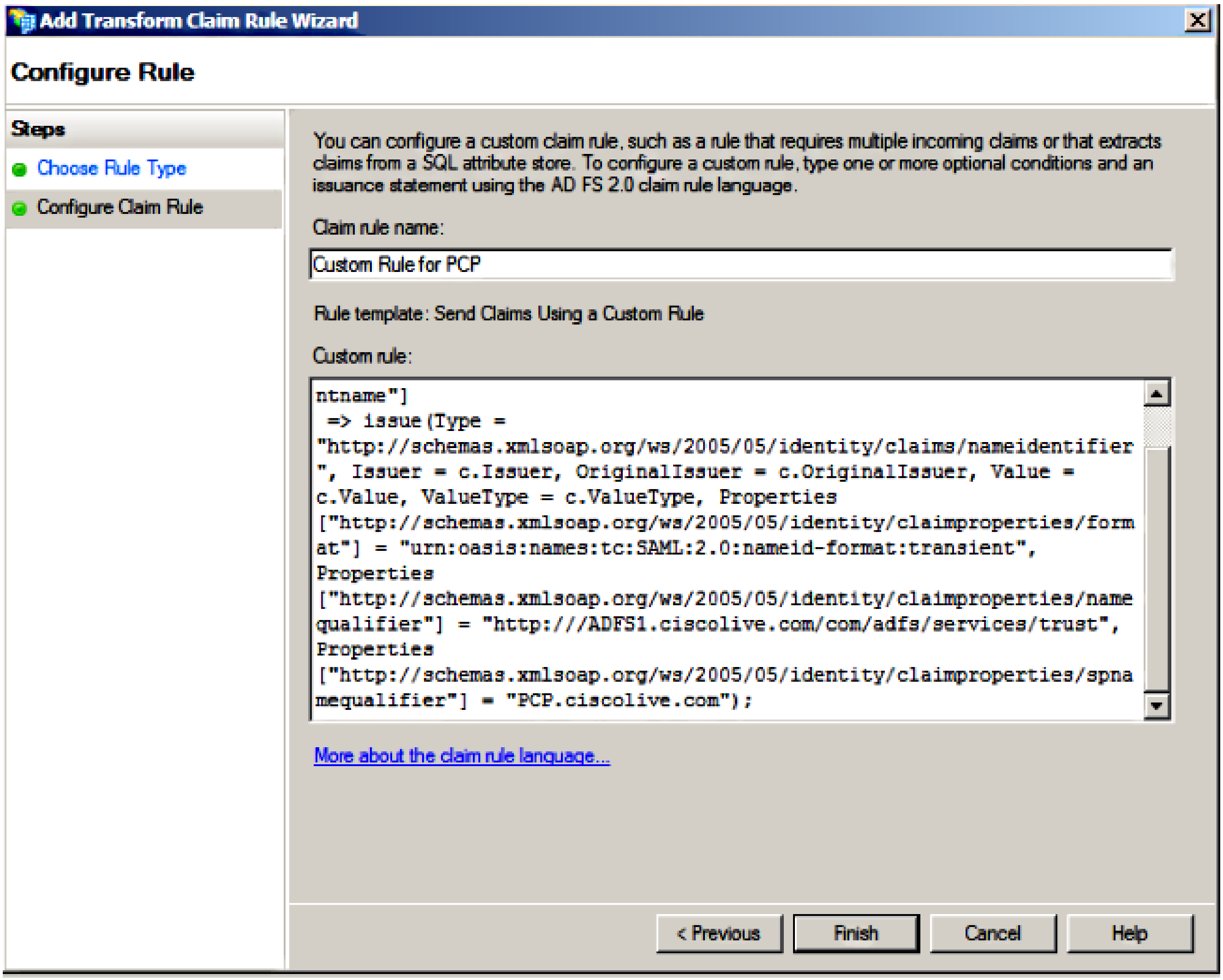
5. 重新启动从**Services.msc的**AD FS版本2.0服务。

添加思科头等协作供应，取决于Party托拉斯

1. 重复步骤1到12如描述为**Add CUCM，取决于Party托拉斯**并且继续对步骤2。

2. 输入一名称对于声明规则名称并且复制在根据海关规则给的空间的此语法：

```
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...

注意最初供应和AD FS FQDN事前填充与实验室最初协作供应(PCP)和从此示例的AD FS，并且必须修改匹配您的环境。

3. 单击 **完成**。

4. 依次单击应用和确定。

5. 重新启动从**Services.msc的**AD FS版本2.0服务。

一旦设置AD FS版本2.0，请继续对enable (event)在Cisco协作产品的SAML SSO。

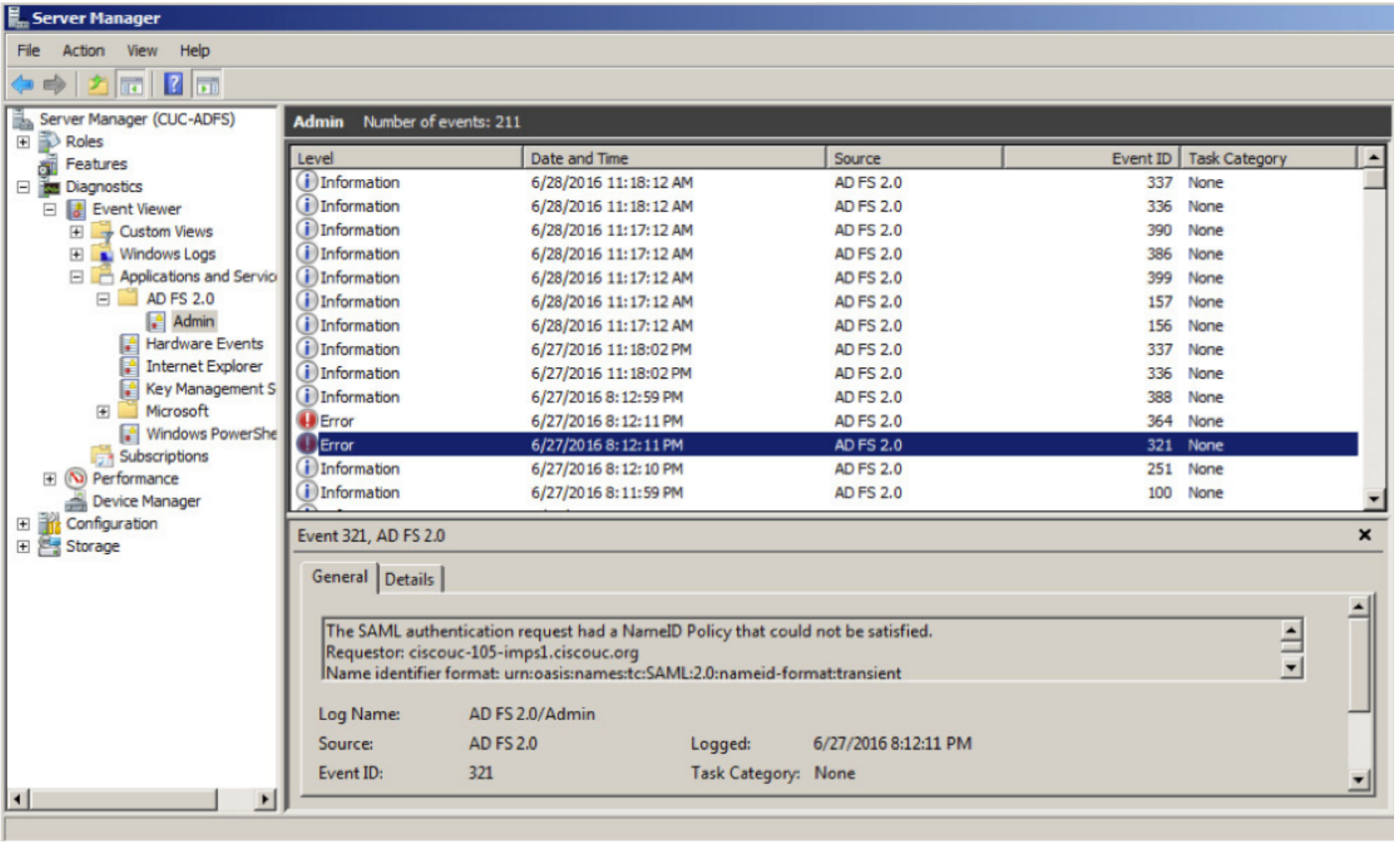
验证

当前没有可用于此配置的验证过程。

故障排除

AD FS记录诊断数据对系统事件日志。 从AD FS服务器的服务器管理器请打开**诊断- > Event Viewer - >应用程序和服务- > AD FS 2.0 - > Admin**

寻找为AD FS活动记录的错误



Admin Number of events: 211

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

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