

# 使用AD FS版本2.0为每个集群配置单个SAML IdP连接/协议

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[步骤1.从CUCM导出SP元数据](#)

[步骤2.从AD FS下载IDP元数据](#)

[步骤3.调配IdP](#)

[步骤4.启用SAML SSO](#)

[验证](#)

[故障排除](#)

## 简介

本文档介绍如何使用Active Directory联合身份验证服务(AD FS)为每个集群配置单一安全断言标记语言(SAML)身份提供程序(IdP)连接/协议。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 思科统一通信管理器(CUCM)11.5或更高版本
- 思科统一通信管理器IM和在线状态版本11.5或更高版本
- Active Directory联合身份验证服务版本2.0

### 使用的组件

本文档中的信息基于以下软件版本：

- 作为IdP的Active Directory联合身份验证服务版本2.0
- 思科统一通信管理器11.5版
- 思科即时消息和在线状态服务器版本11.5

## 背景信息

对于SAML SSO，需要是服务提供商(SP)和IdP之间的信任圈。当交换信任（元数据）时，此信任

会作为SSO启用的一部分创建。从CUCM下载元数据并将其上传到IdP，同样从IdP下载元数据并将其上传到CUCM。

在CUCM 11.5之前，始发节点生成元数据文件，也从集群中的其他节点收集元数据文件。它将所有元数据文件添加到单个zip文件，然后向管理员显示。管理员必须解压此文件并在IdP上调配每个文件。例如，8个节点群集的8个元数据文件。

从11.5引入了单个SAML IdP连接/协议每个集群功能。作为此功能的一部分，CUCM为集群中的所有CUCM和IMP节点生成单个服务提供程序元数据文件。元数据文件的新名称格式为<hostname>-single-agreement.xml

基本上，一个节点创建元数据并将其推送到群集中的其他SP节点。这可简化调配、维护和管理。例如，8节点群集的1个元数据文件。

集群范围的元数据文件使用Multiserver tomcat证书，确保密钥对用于集群中的所有节点相同。元数据文件还包含集群中每个节点的断言使用者服务(ACS)URL列表。

CUCM和思科即时消息和在线状态版本11.5支持SSO模式、**集群范围**（每个集群一个元数据文件）和节点（现有模型）。

本文档介绍如何使用AD FS 2.0配置SAML SSO的集群范围模式。

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

### 步骤1.从CUCM导出SP元数据

打开Web浏览器，以管理员身份登录到CUCM，然后导航到**System >SAML Single Sign On**。

默认情况下，选择**“集群范围”**单选按钮。单击**“导出所有元数据”**。以名称<hostname>-single-agreement.xml向管理员显示的元数据数据文件

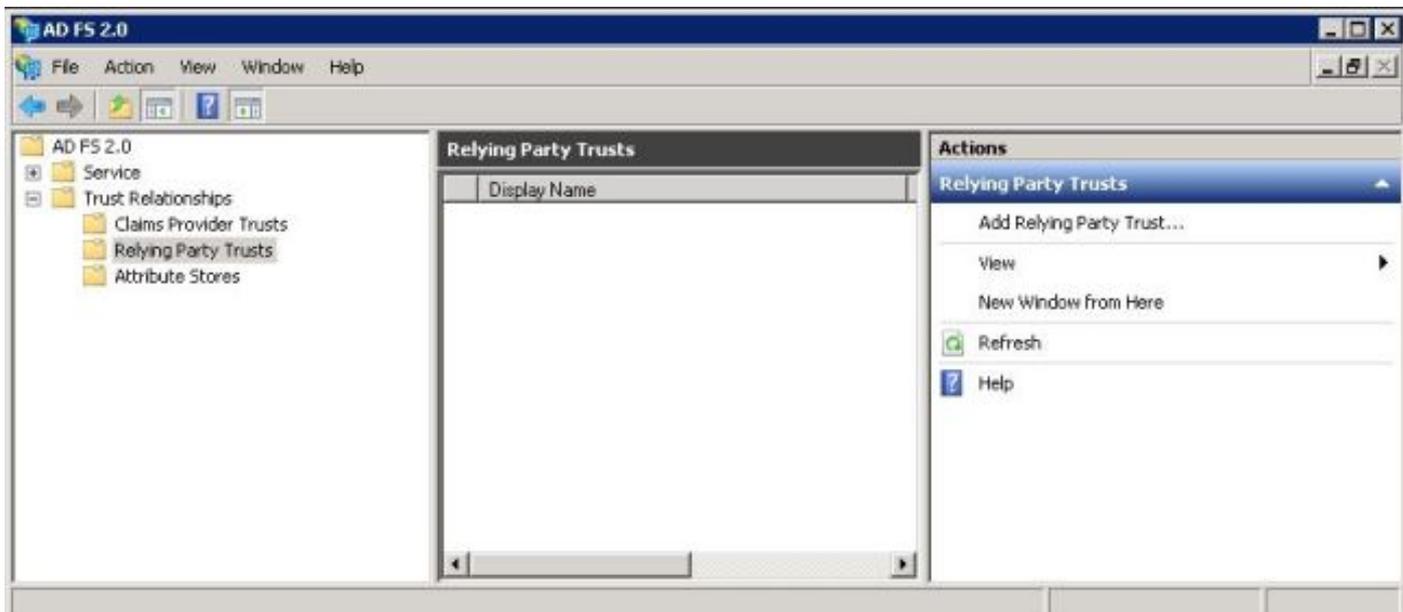


### 步骤2.从AD FS下载IDP元数据

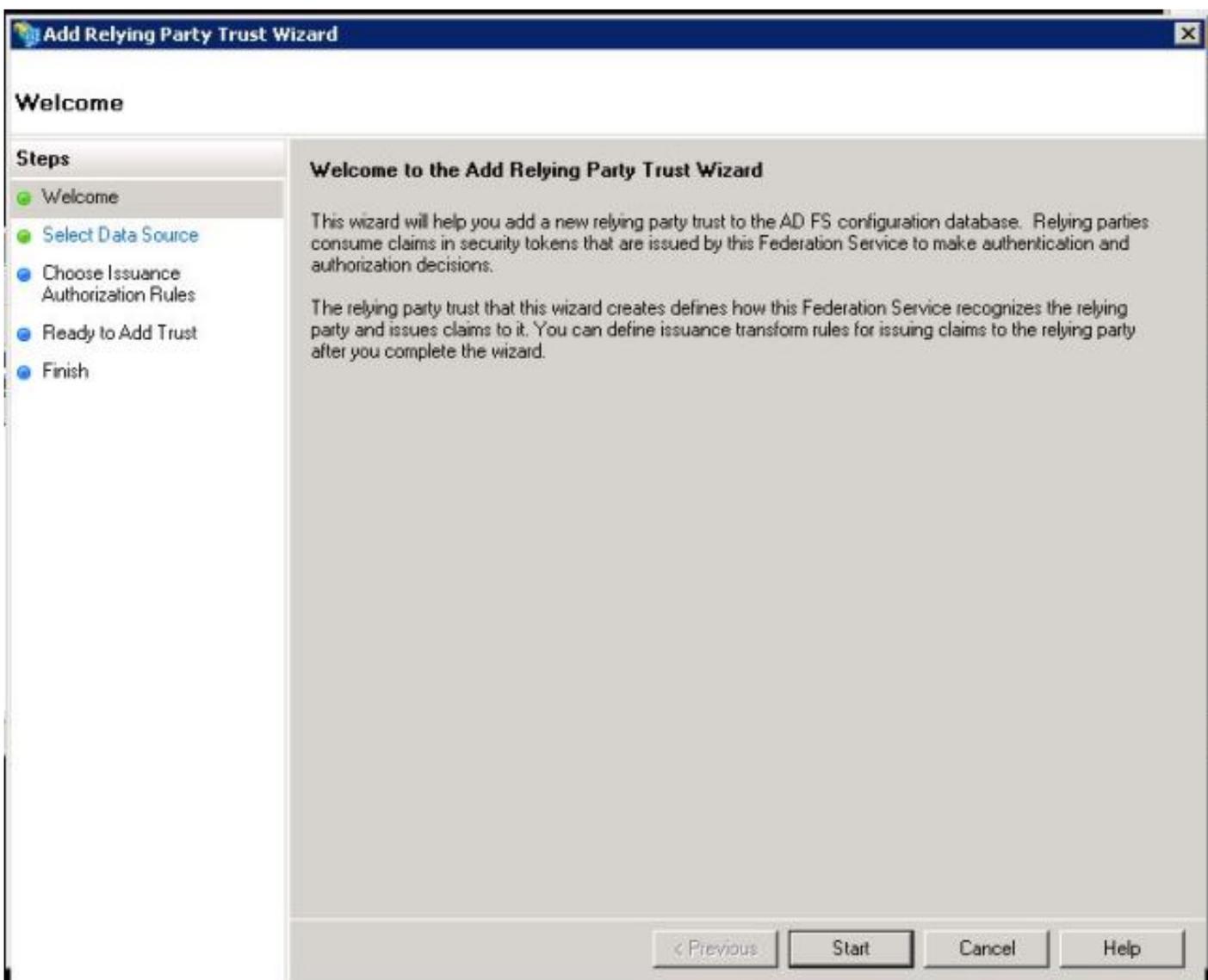
要下载IdP元数据，请参阅链接[https:// <FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml](https://<FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml)

### 步骤3.调配IdP

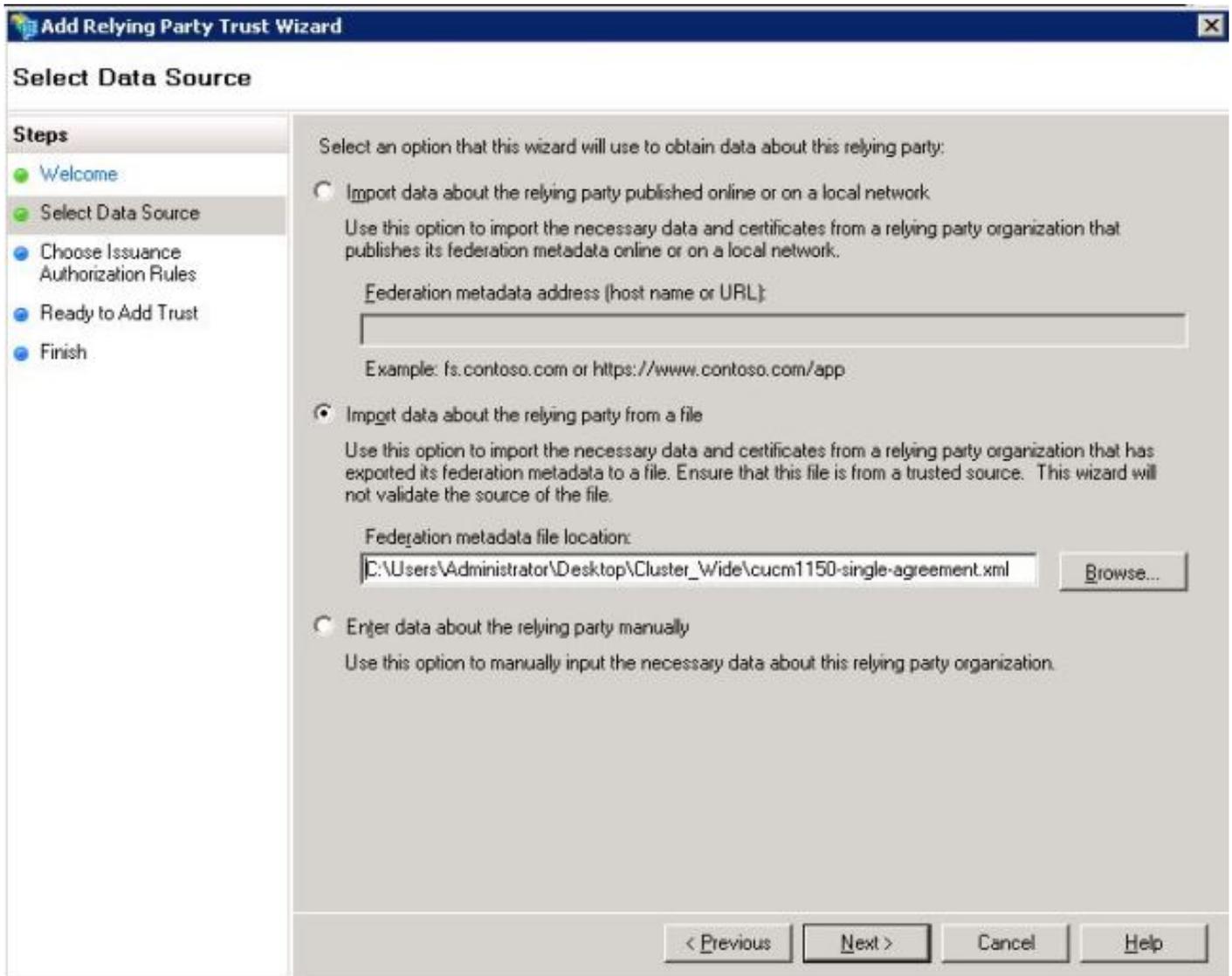
如图所示，导航至AD FS 2.0管理/信任关系发运/信赖方信任。单击**“添加信赖方信任”**。



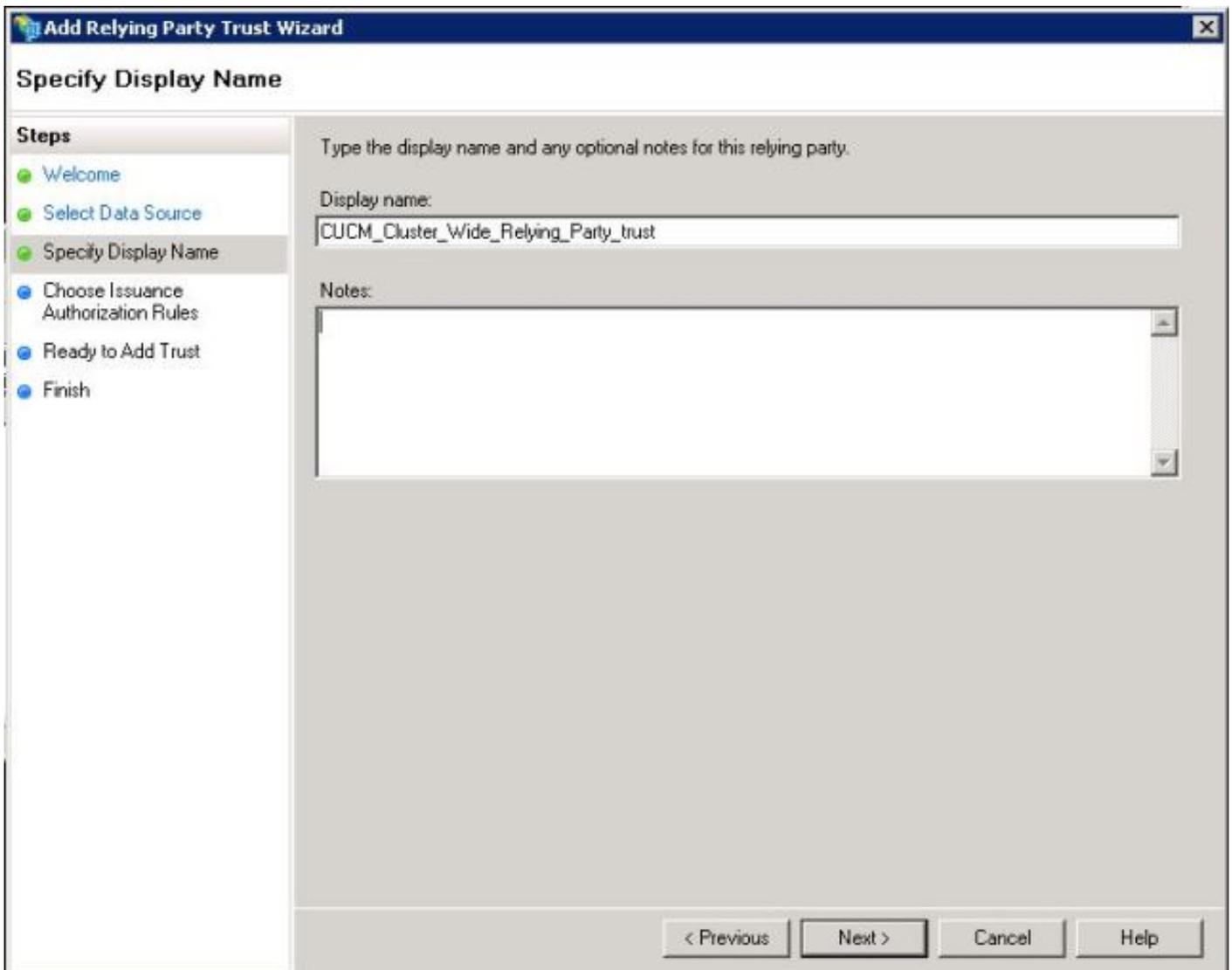
“添加信赖方信任向导”(Add Relying Party Trust Wizard)打开，如图所示，现在单击“开始”。



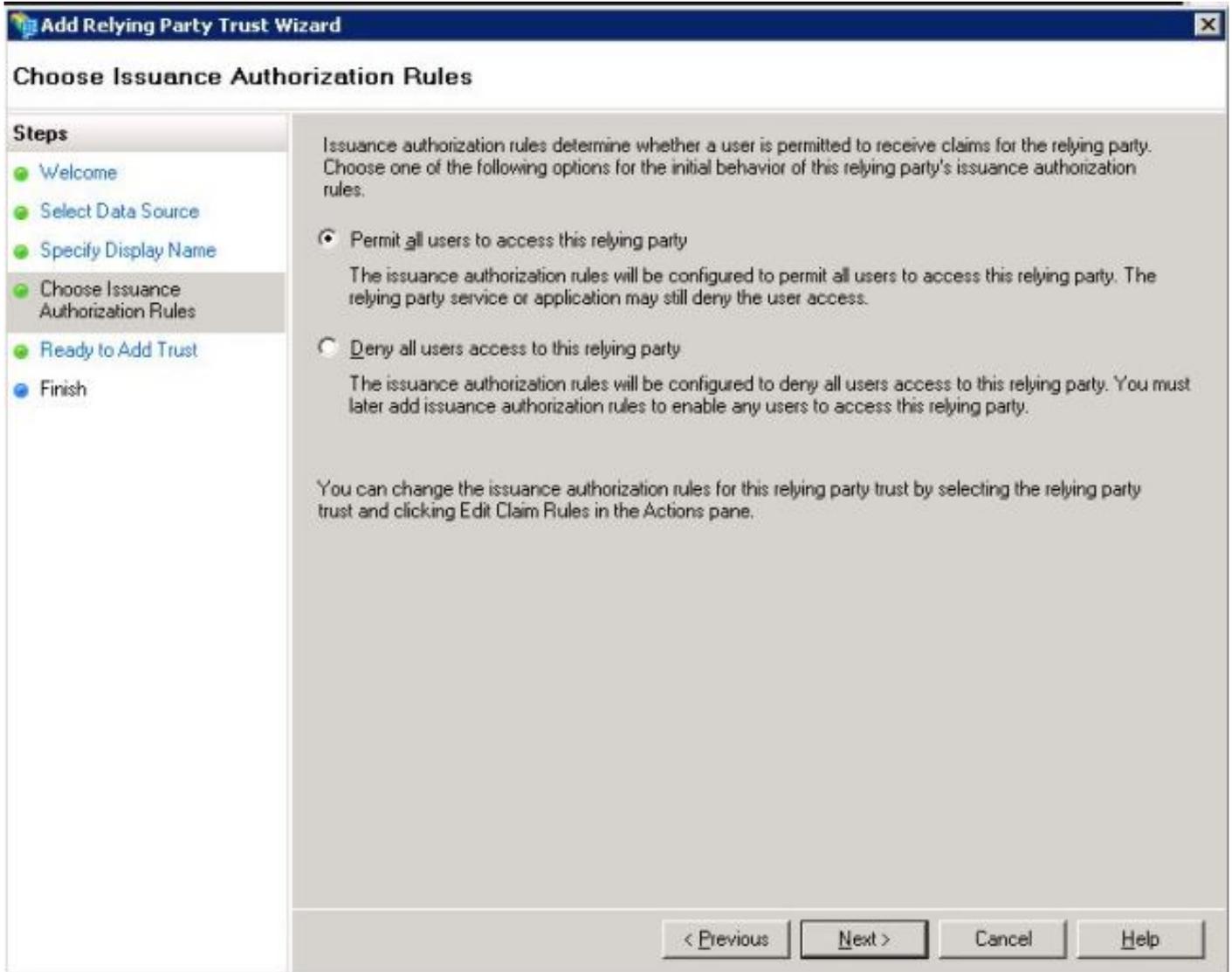
单击有关从文件中信赖方的导入数据。浏览从CUCM SAML SSO配置页下载的SP元数据。然后单击**Next**，如图所示：



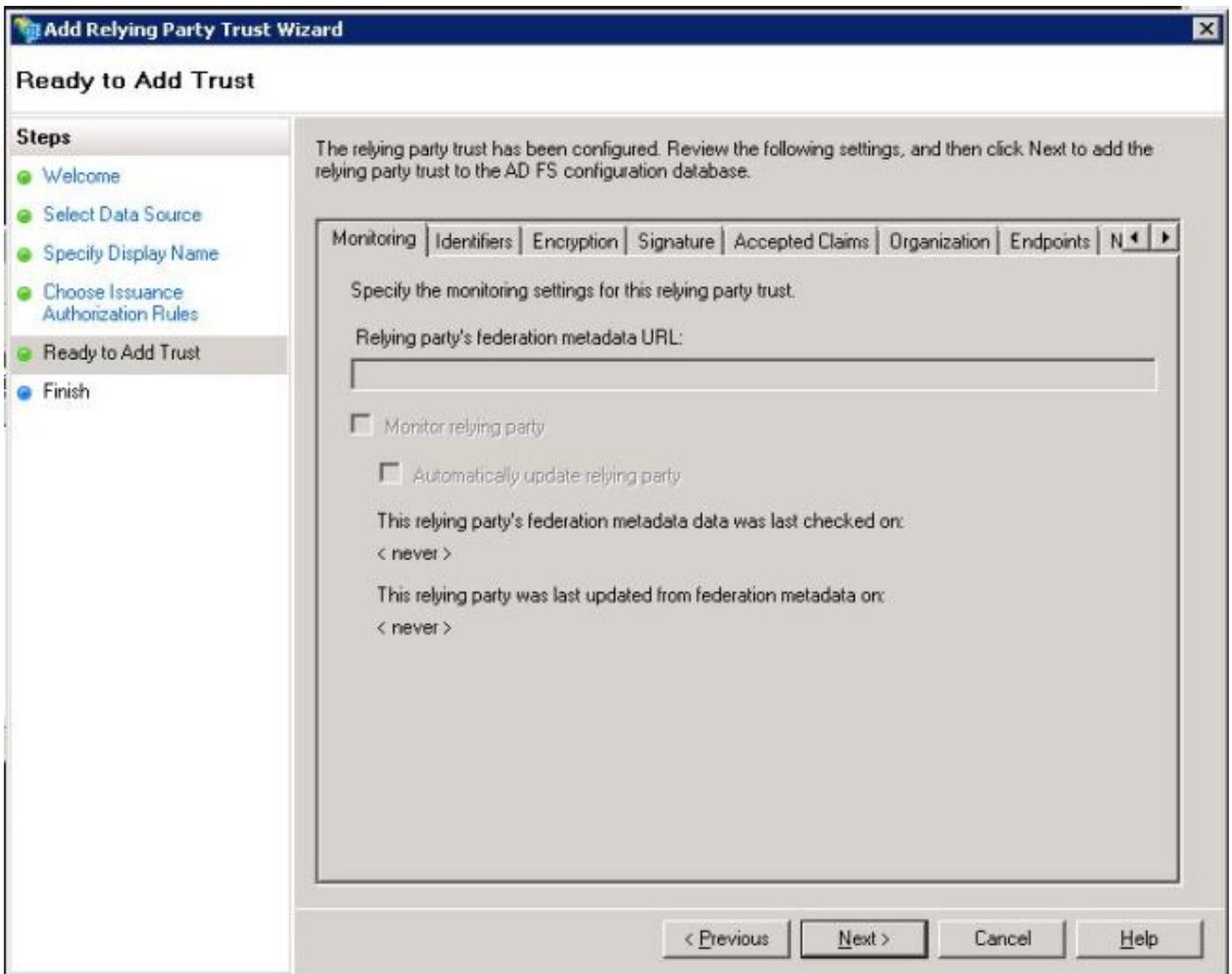
键入信赖方的显示名称和任何可选注释。单击**Next**，如图所示：



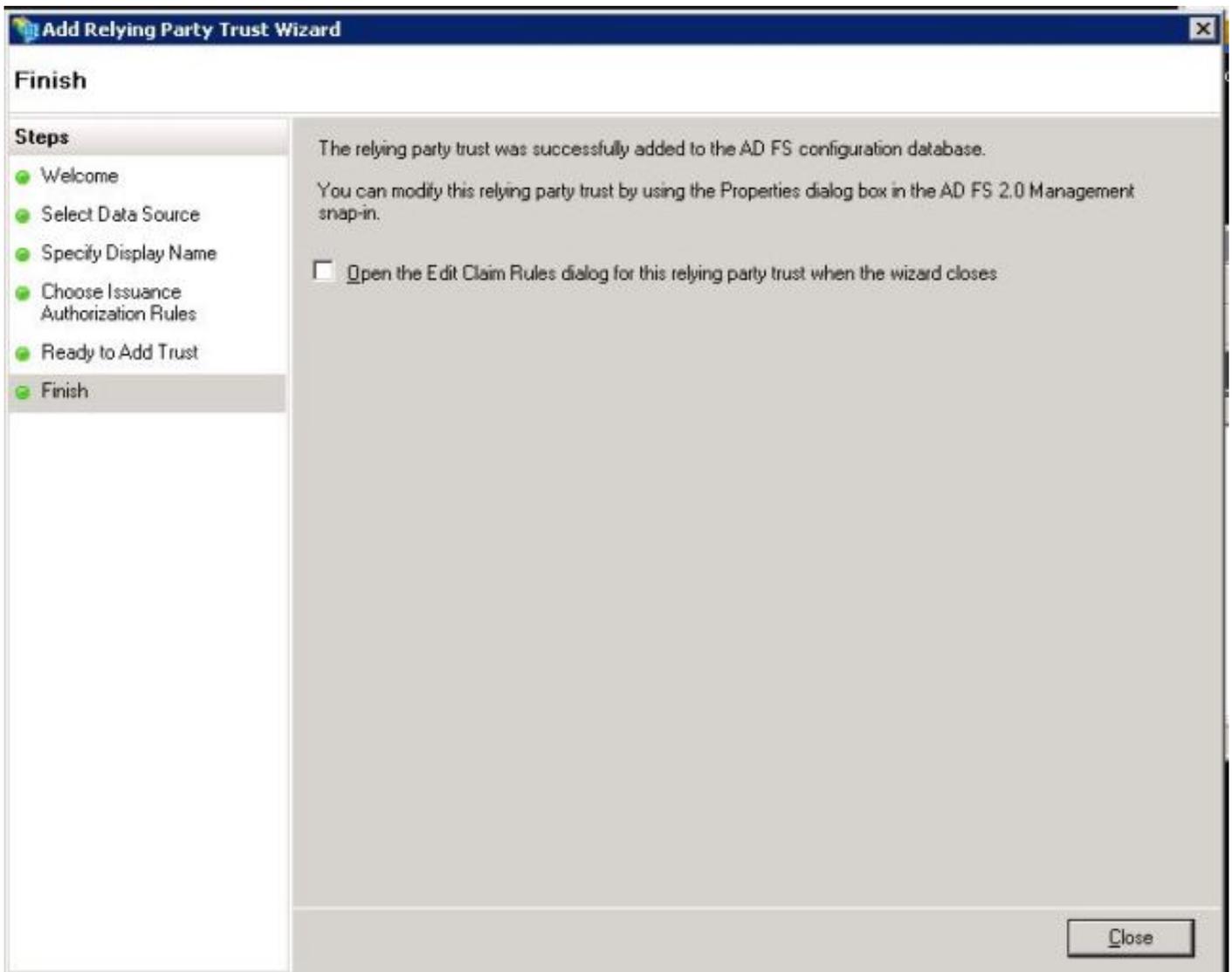
选择允许所有用户访问此信赖方以允许所有用户访问此信赖方，然后单击下一步，如图所示：



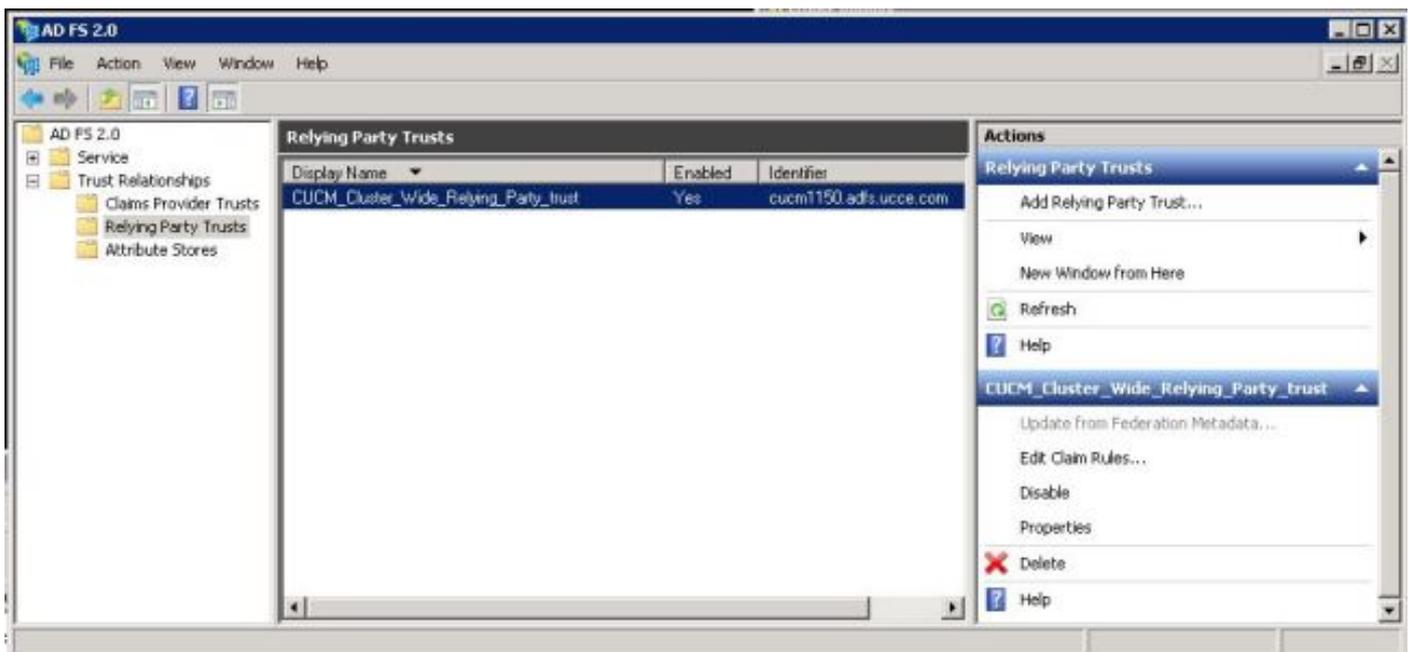
在“准备添加信任”(Ready to Add Trust)页面下，您可以查看已配置的信赖方信任的设置。现在单击 **Next**，如图所示：



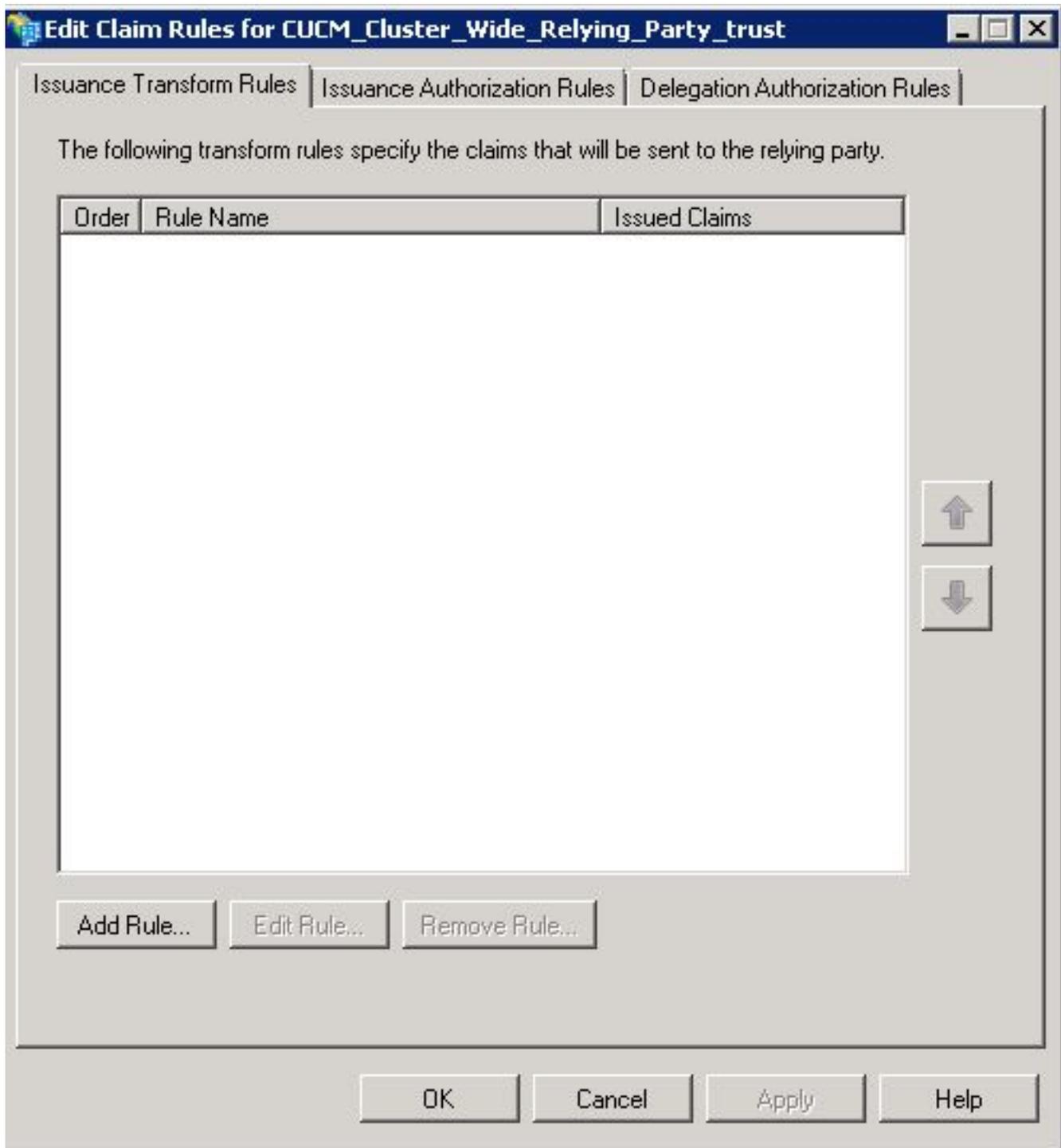
“完成”页确认信赖方信任已成功添加到AD FS配置数据库。取消选中“Box ( 框 )”，然后单击“Close ( 关闭 )”，如图所示：



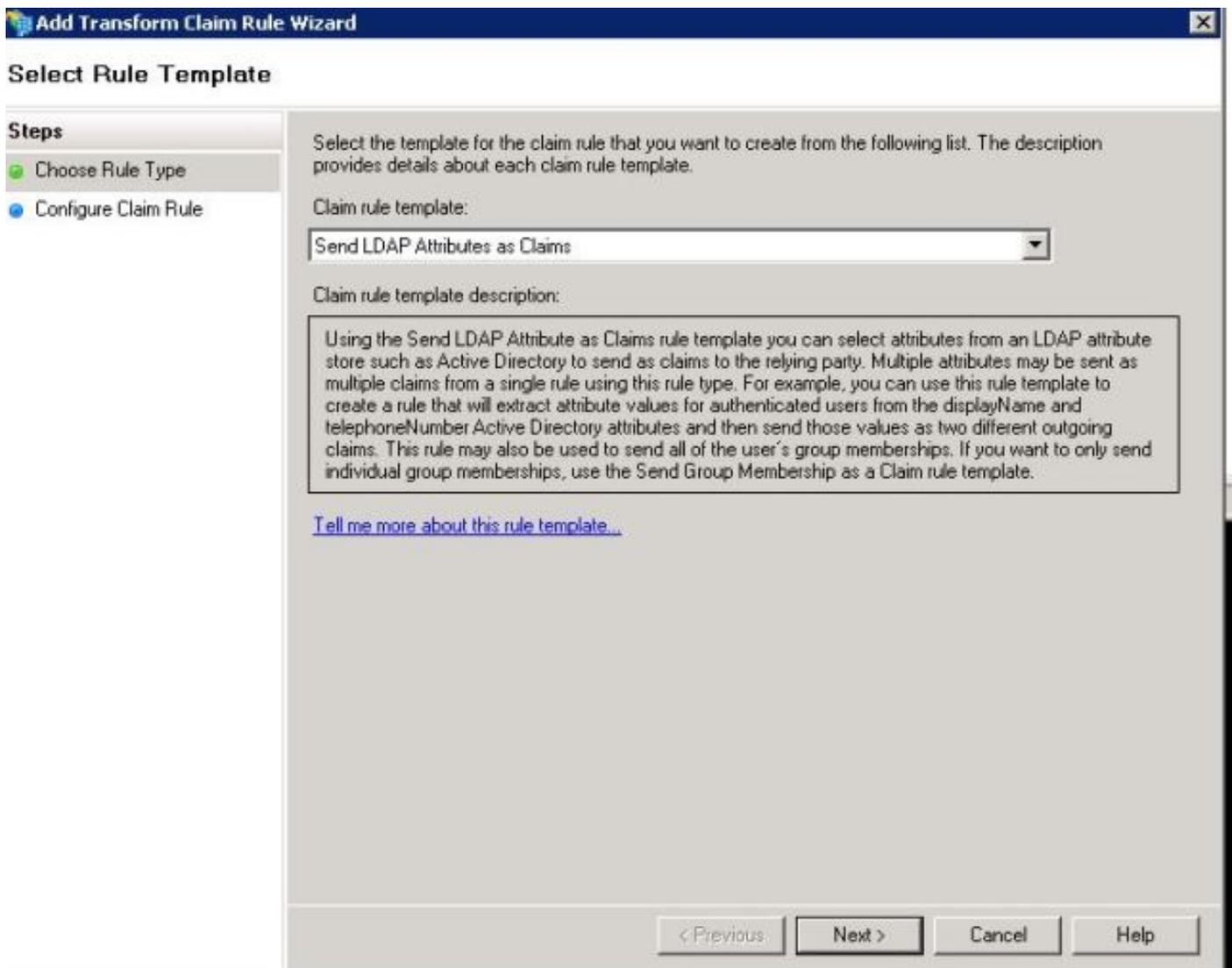
右键单击“信赖方信任”，然后单击“编辑领款申请规则”，如图所示：



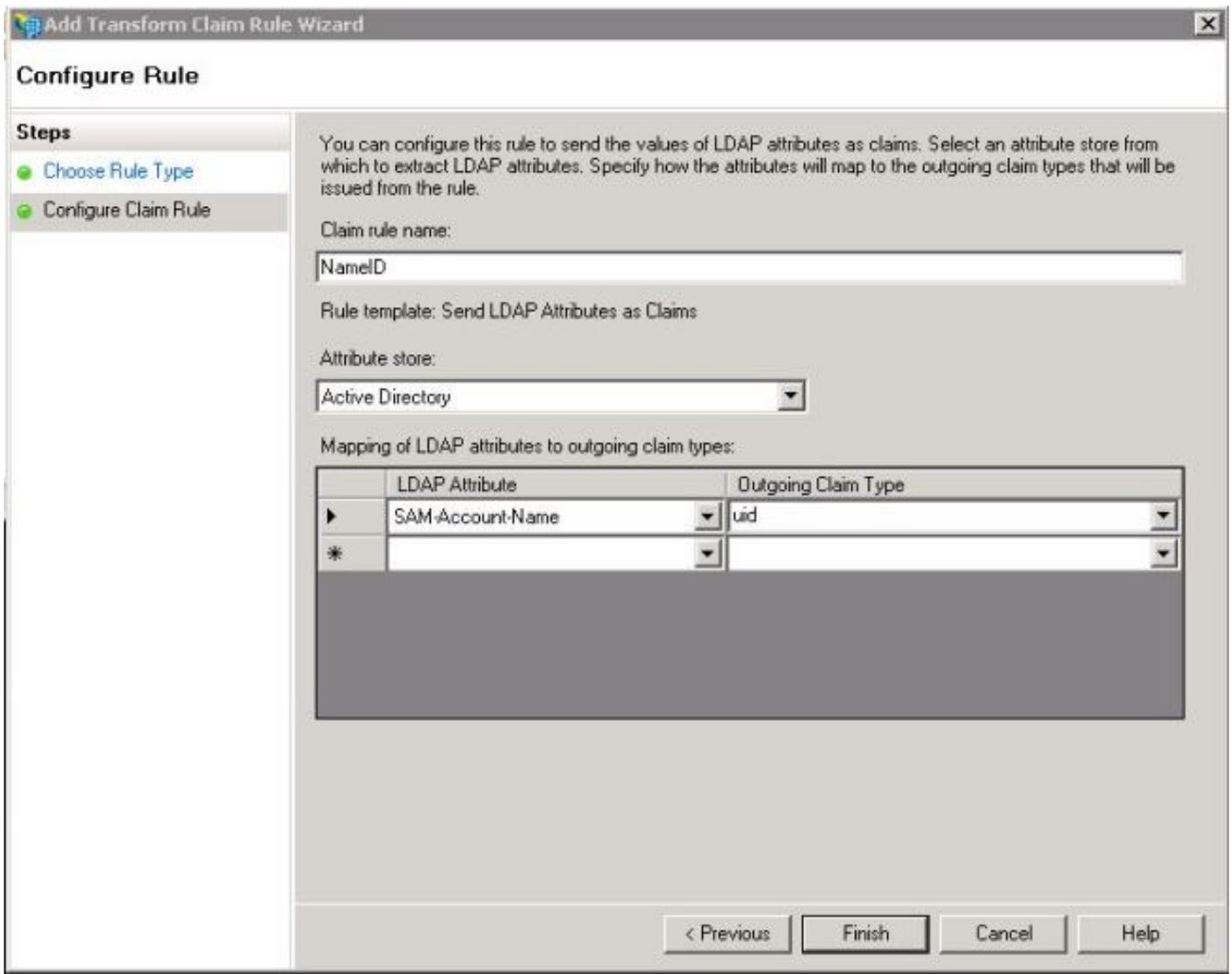
现在单击Add Rule，如图所示：



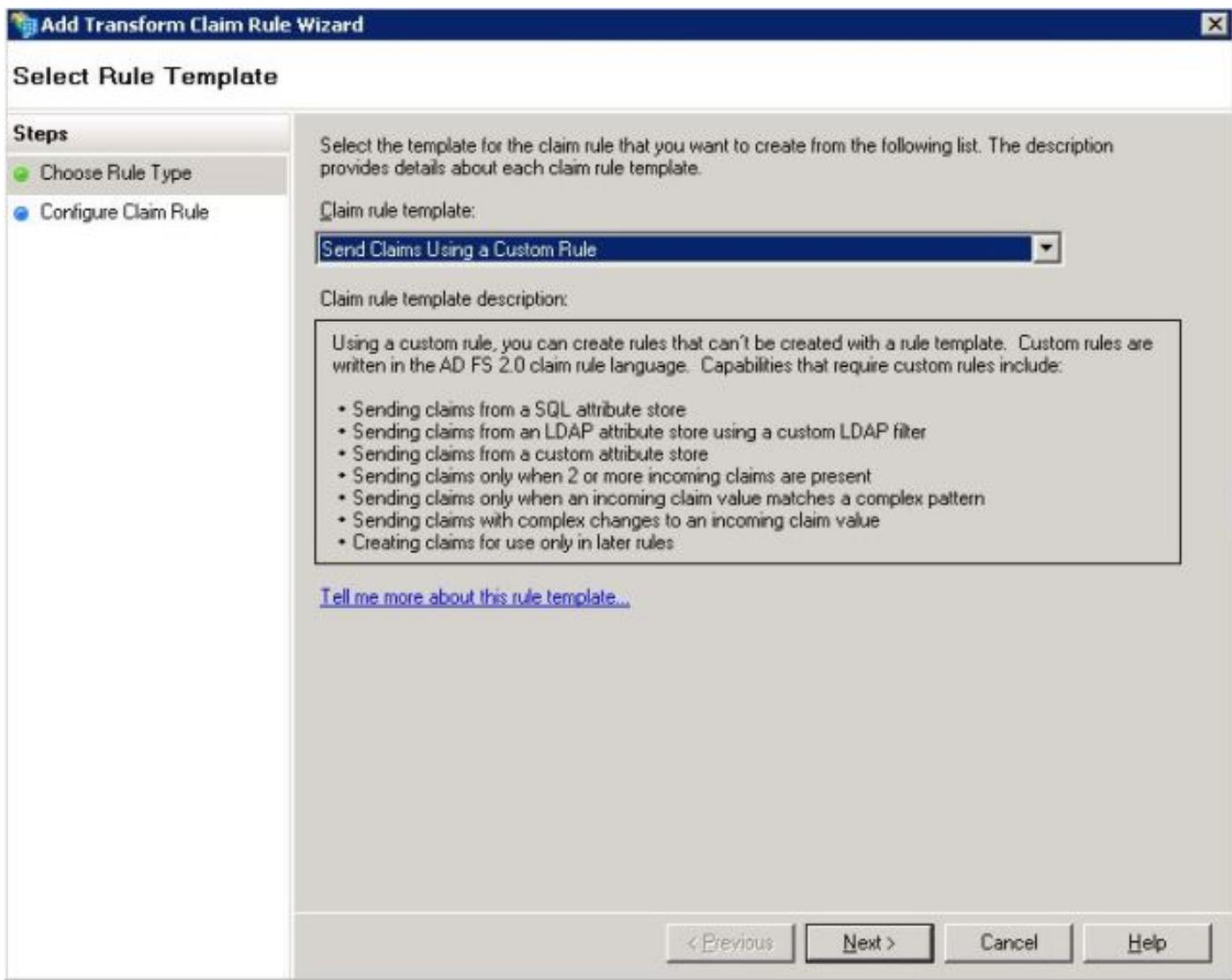
当“添加转换声明规则”(Add Transform Claim Rule)打开时，单击使用默认声明规则模板“将LDAP属性作为声明发送”(Send LDAP Attributes as Claims)的“下一步”(Next)，如图所示：



单击**Configure Claim Rule**，如下图所示。LDAP属性必须与CUCM中LDAP目录配置中的LDAP属性匹配。将传出声明类型管理为uid。单击**完成**，如图所示：



为信赖方添加自定义规则。单击**Add rule**。选择**使用自定义规则发送声明**，然后单击下一步，如图所示：

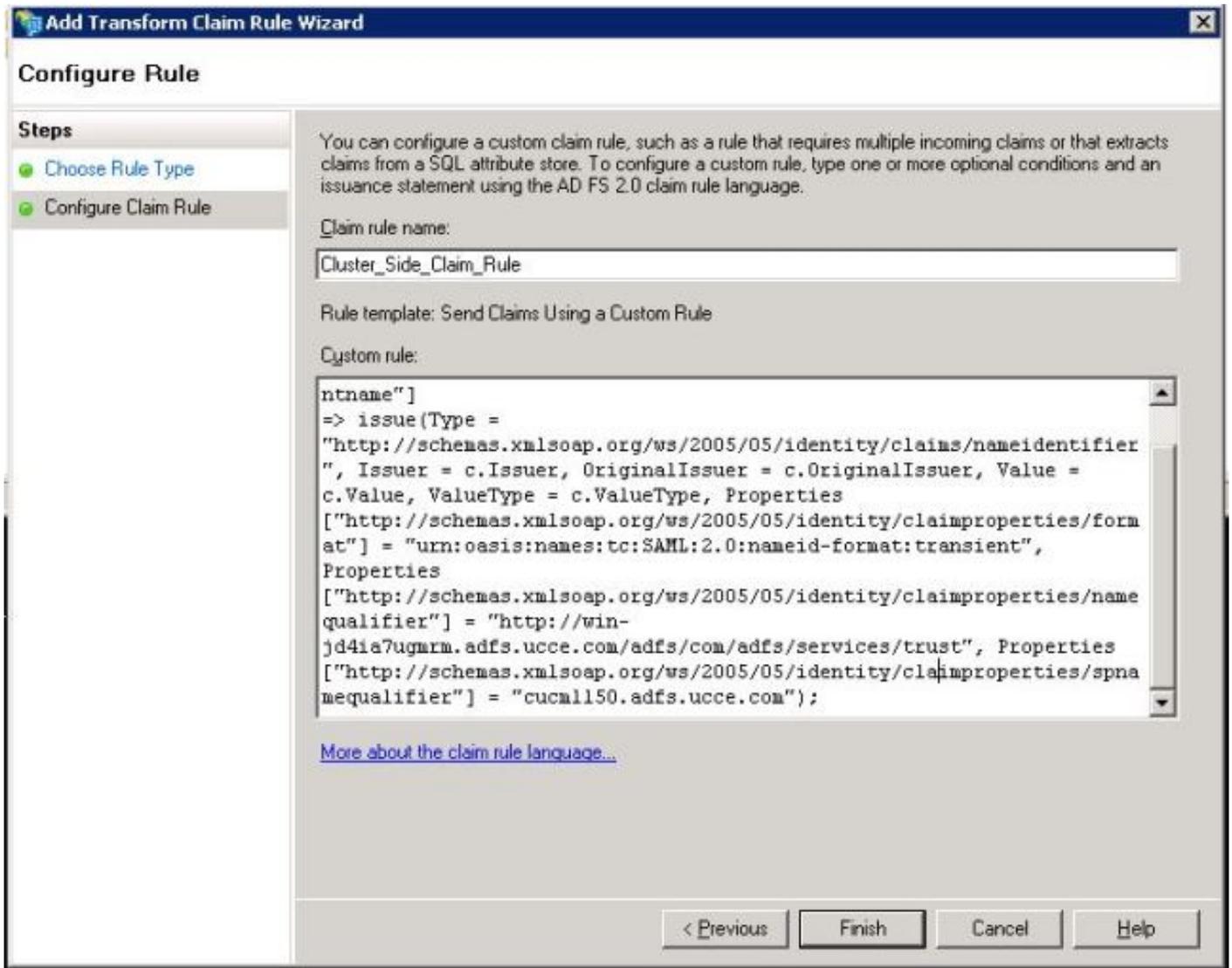


在配置领款申请规则中，键入领款申请规则名称，然后在修改领款申请规则中名称限定符和 spname 限定符的向导的“自定义规则”字段中，复制指定和过去的领款申请规则。单击**完成**，如图所示：

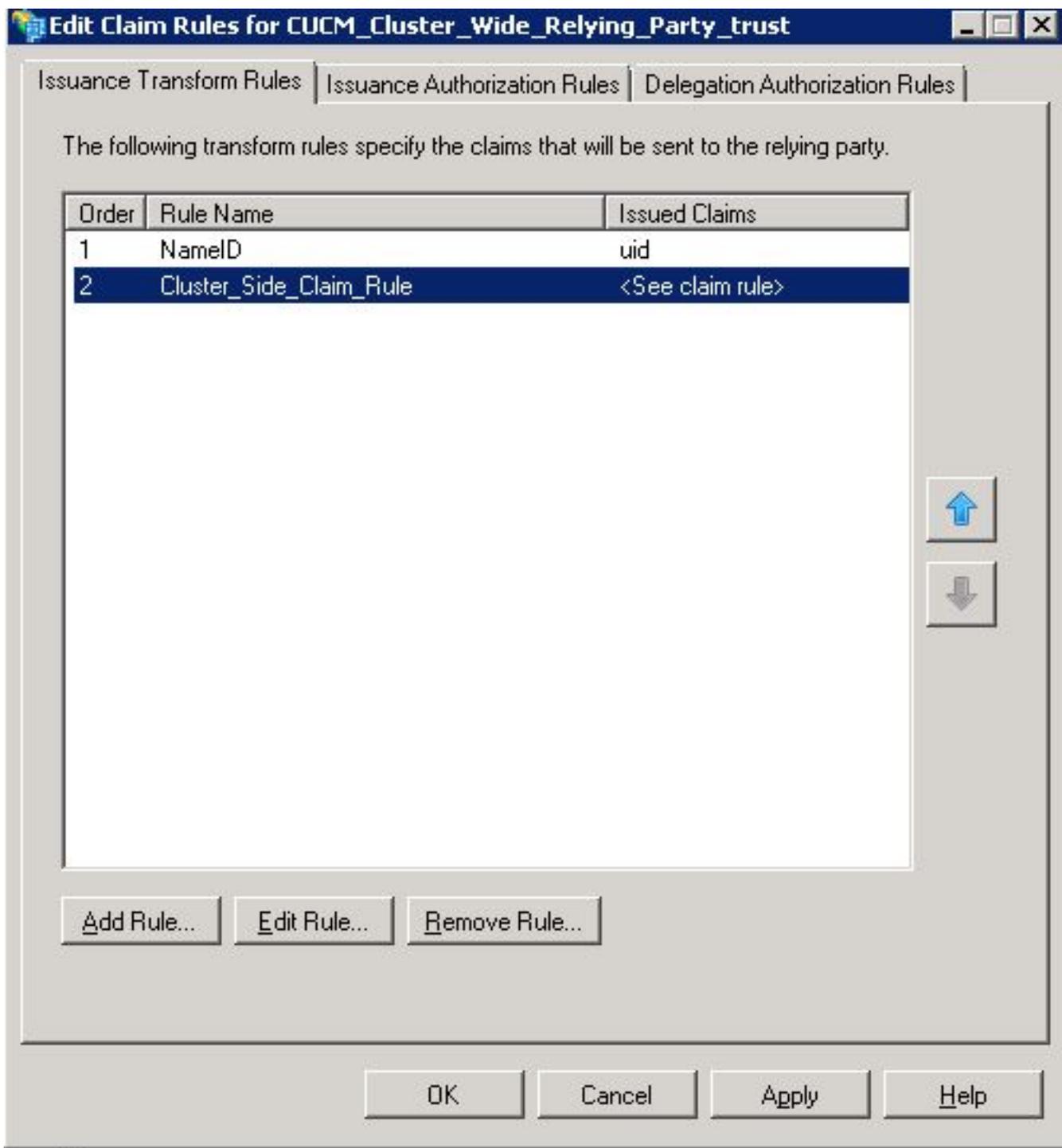
### 领款申请规则：

```
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.



如图所示，单击“应用”，然后单击“确定”。



#### 步骤4.启用SAML SSO

打开Web浏览器，以管理员身份登录CUCM，然后导航到**System >SAML Single Sign On**。

默认情况下，选择“**集群范围**”单选按钮。单击**Enable Saml SSO**，如图所示：

## 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

如图所示，弹出窗口会通知Web服务器重新启动的警告和信息，以根据idp选择集群范围的SAML SSO或每节点SAML SSO。单击 **Continue**。



### 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.

Continue

Cancel

启用集群范围SSO的条件是必须已部署多服务器Tomcat证书。单击**Test for Multi-Server Tomcat Certificate (测试多服务器Tomcat证书)**，如图所示：

## SAML Single Sign-On Configuration

Next

### Status

 Status: Ready

### Test for Multi-Server tomcat certificate

The criteria for enabling dusterwide SSO is that you must have a multiserver tomcat certificate already deployed. If you have not done this already please follow the below steps:

- 1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
- 2) Click on Generate CSR
- 3) Select Certificate Purpose as Tomcat
- 4) Select Distribution as "Multi-Server"
- 5) Click Generate
- 6) Download the CSR and get it signed from the CA of your choice
- 7) Once the certificate is issued by the CA, upload it via the "Upload Certificate/ Certificate chain" option on the Certificate Management page
- 8) Restart Tomcat service on all the nodes in the cluster
- 9) Restart TFTP service on all the TFTP nodes in the cluster

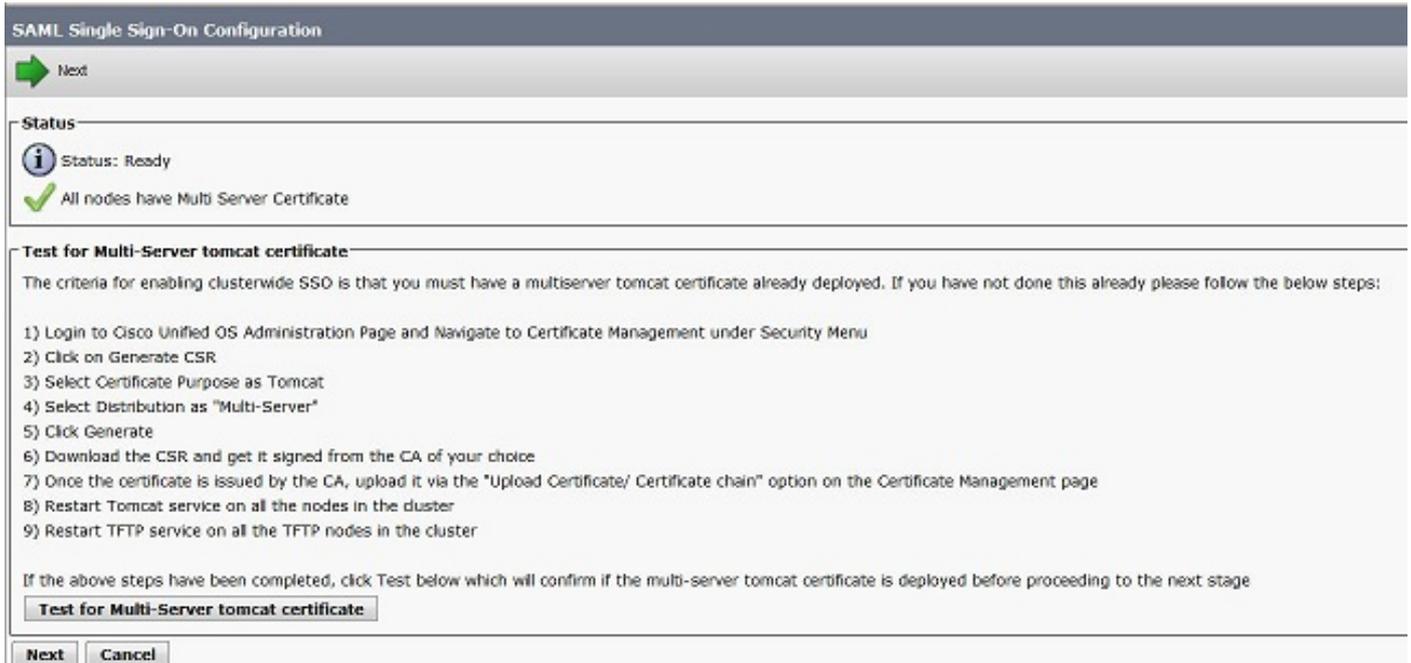
If the above steps have been completed, click Test below which will confirm if the multi-server tomcat certificate is deployed before proceeding to the next stage

Test for Multi-Server tomcat certificate

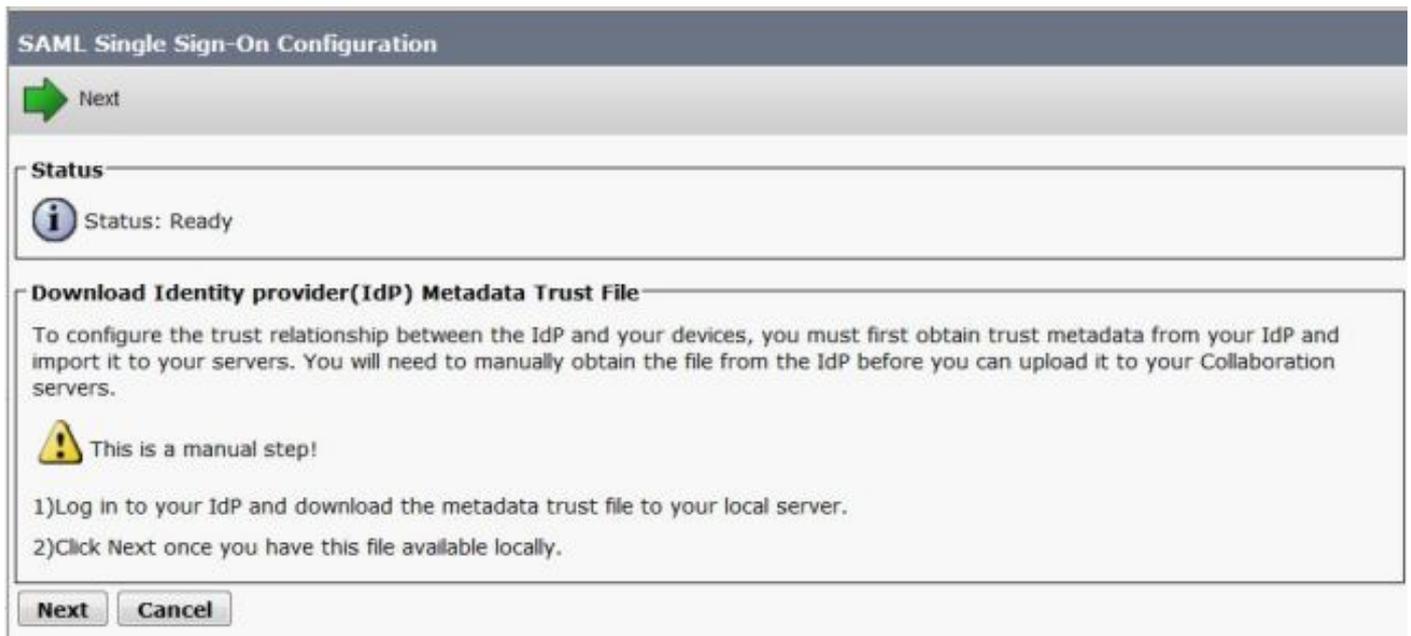
Next

Cancel

确认后，所有节点的“多服务器证书”(Multi Server Certificate)都会显示“所有节点都有多服务器证书”(All Nodes have Multi Server Certificate)，然后单击“下一步”(Next)，如图所示：



如图所示，单击“下一步”。



浏览并选择下载的IdP元数据。单击导入IdP元数据，如图所示：



该页确认Import succeeded for all servers，然后单击Next，如图所示：



如图所示，单击Next，因为已从初始SAML SSO配置页导出SP元数据。

### 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必须与LDAP目录同步。向导显示在LDAP目录中配置的有效管理员用户。选择用户，然后单击**运行SSO测试**，如图所示：

### 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

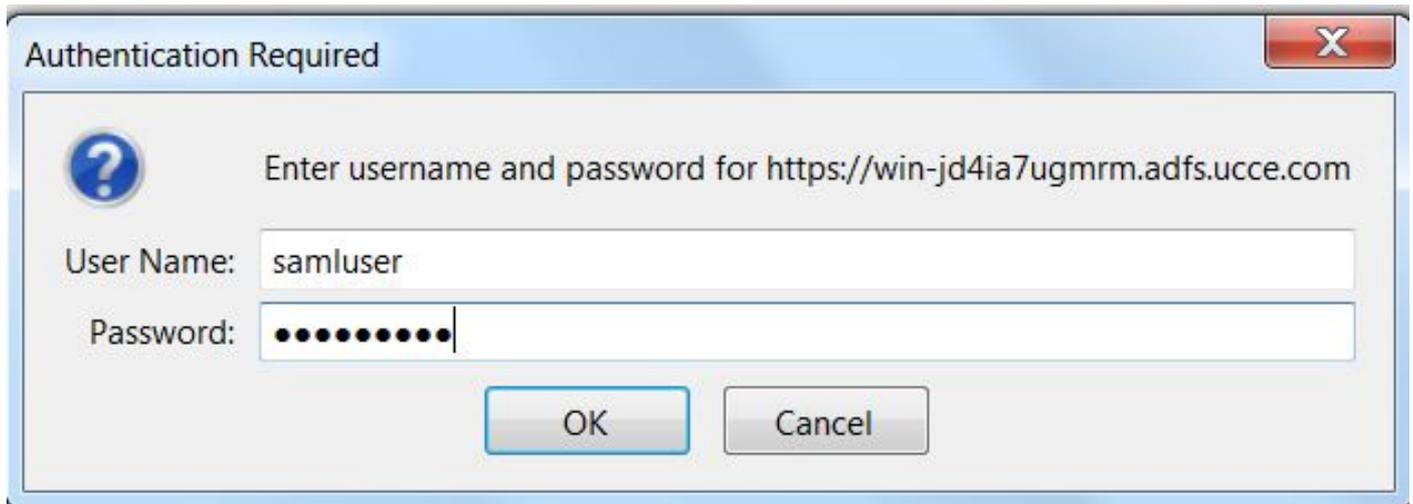
samluser
----------

2)Launch SSO test page

**Run SSO Test...**

**Back**    **Cancel**

如图所示，在提示后输入用户ID和相应的密码。



Authentication Required

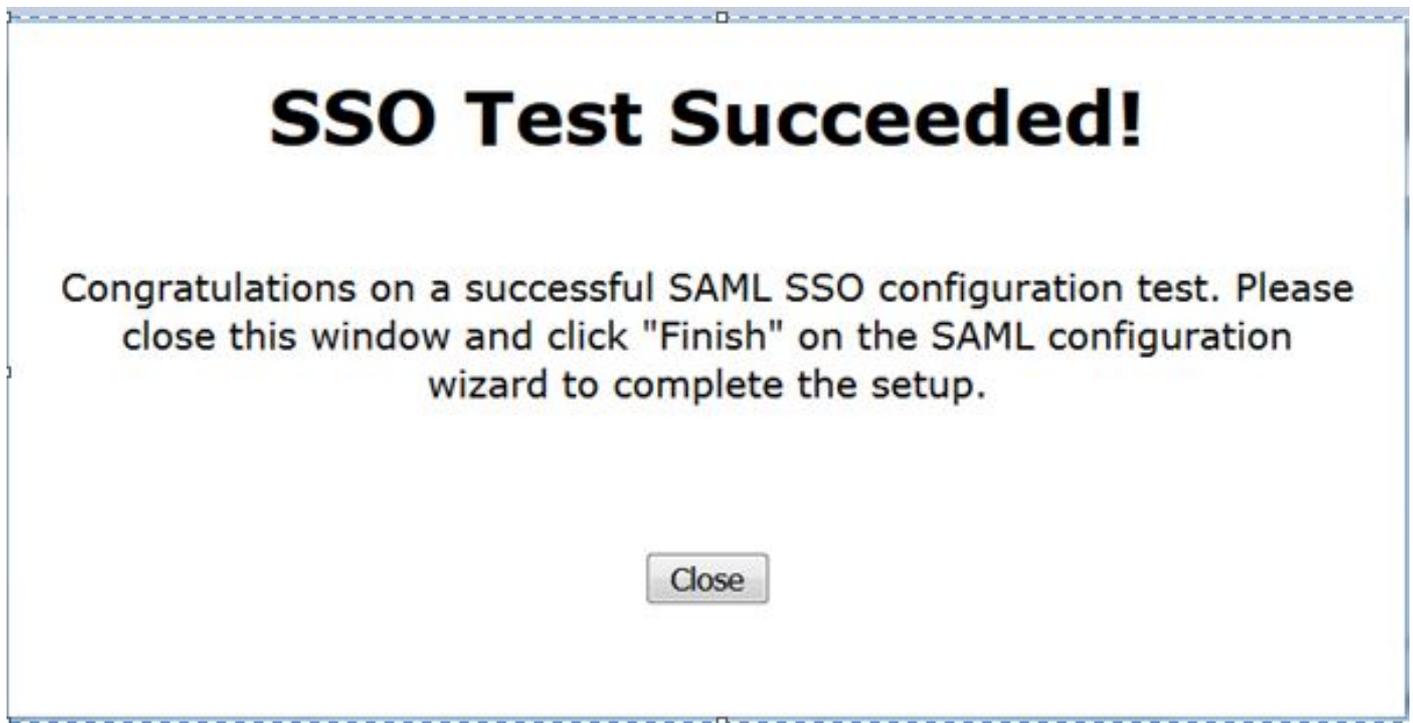
Enter username and password for https://win-jd4ia7ugmrm.adfs.ucce.com

User Name:

Password:

OK Cancel

弹出窗口（如图所示）确认测试成功。



**SSO Test Succeeded!**

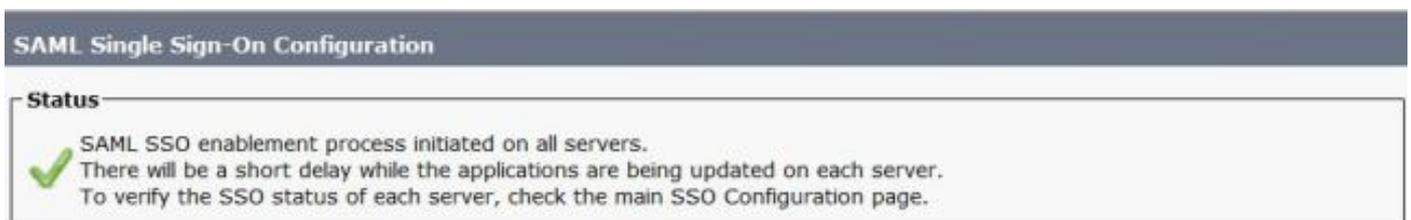
Congratulations on a successful SAML SSO configuration test. Please close this window and click "Finish" on the SAML configuration wizard to complete the setup.

Close

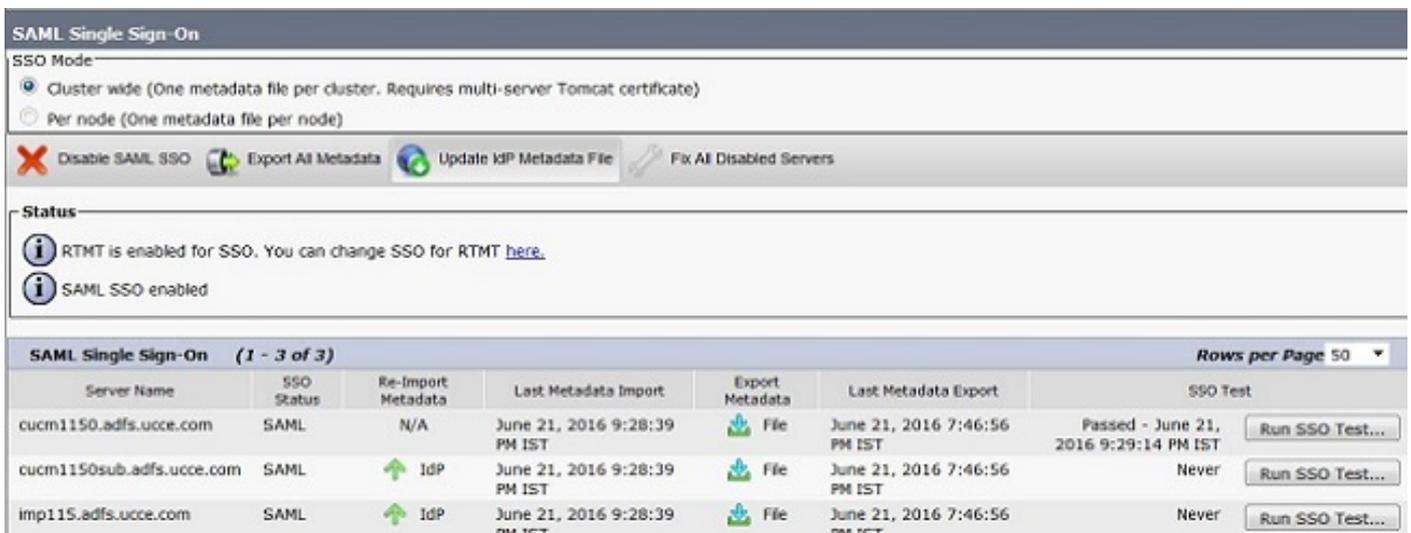
如图所示，单击**完成**以完成启用SSO的配置。



图中显示的页面确认SAML SSO启用进程在所有服务器上启动。



使用SAML SSO凭证注销并重新登录CUCM。导航至系统>SAML单点登录。单击运行SSO测试以查找群集中的其他节点，如图所示：



## 验证

使用本部分可确认配置能否正常运行。

确认已启用SAML SSO的节点的SSO测试成功。导航至System >SAML Single Sign On。成功的SSO测试显示状态已通过。

**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

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

激活SAML SSO后，将为CUCM登录页列出已安装的应用和平台应用，如下图所示。

**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

激活SAML SSO后，会为IM and Presence登录页列出Installed Applications和Platform Applications，如下图所示：

## 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

## 故障排除

本部分提供的信息可用于对配置进行故障排除。

要将SSO日志设置为调试，请使用命令set **samltrace level DEBUG**

使用RTMT或从活动日志/tomcat/logs/ssosp/log4j/\*.log位置使用CLI收集SSO日志。

SSO日志示例显示生成的元数据并发送到其他节点

```
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
```