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

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。**

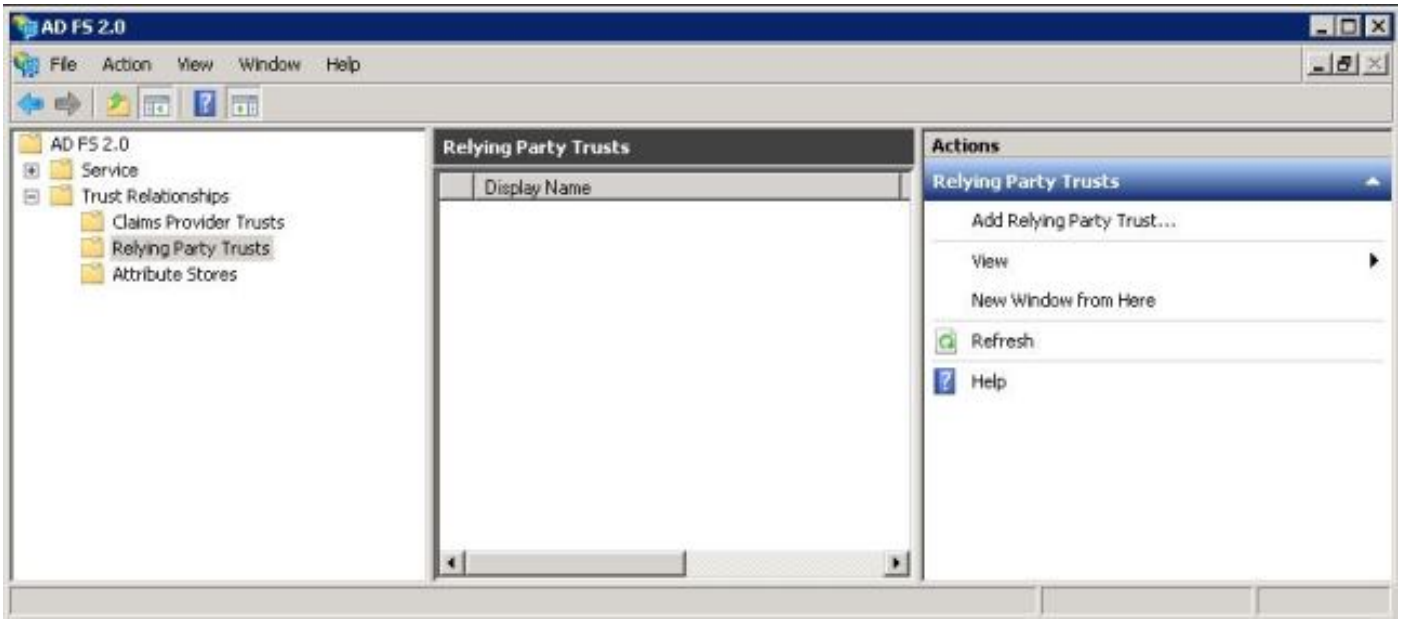
默认情况下，选**择"集群**范围"单选按钮。单击"导**出所有元数据"。**以名称<hostname>-single-agreement.xml向管理**员显示的元数据数据文件**

步骤2.从AD FS下载IDP元数据

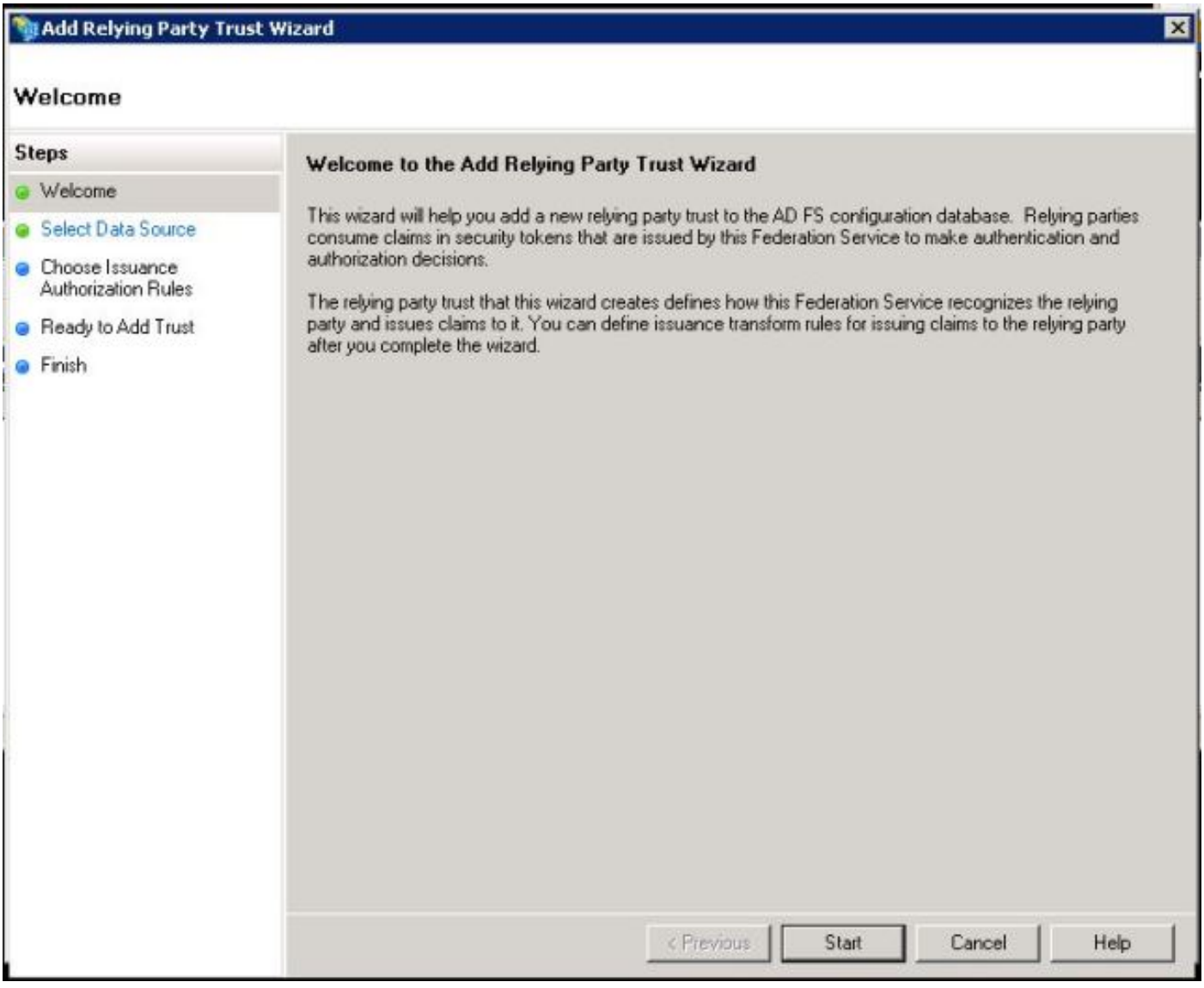
要下载IdP元数据，请参阅链接https:// <FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml

步骤3.调配IdP

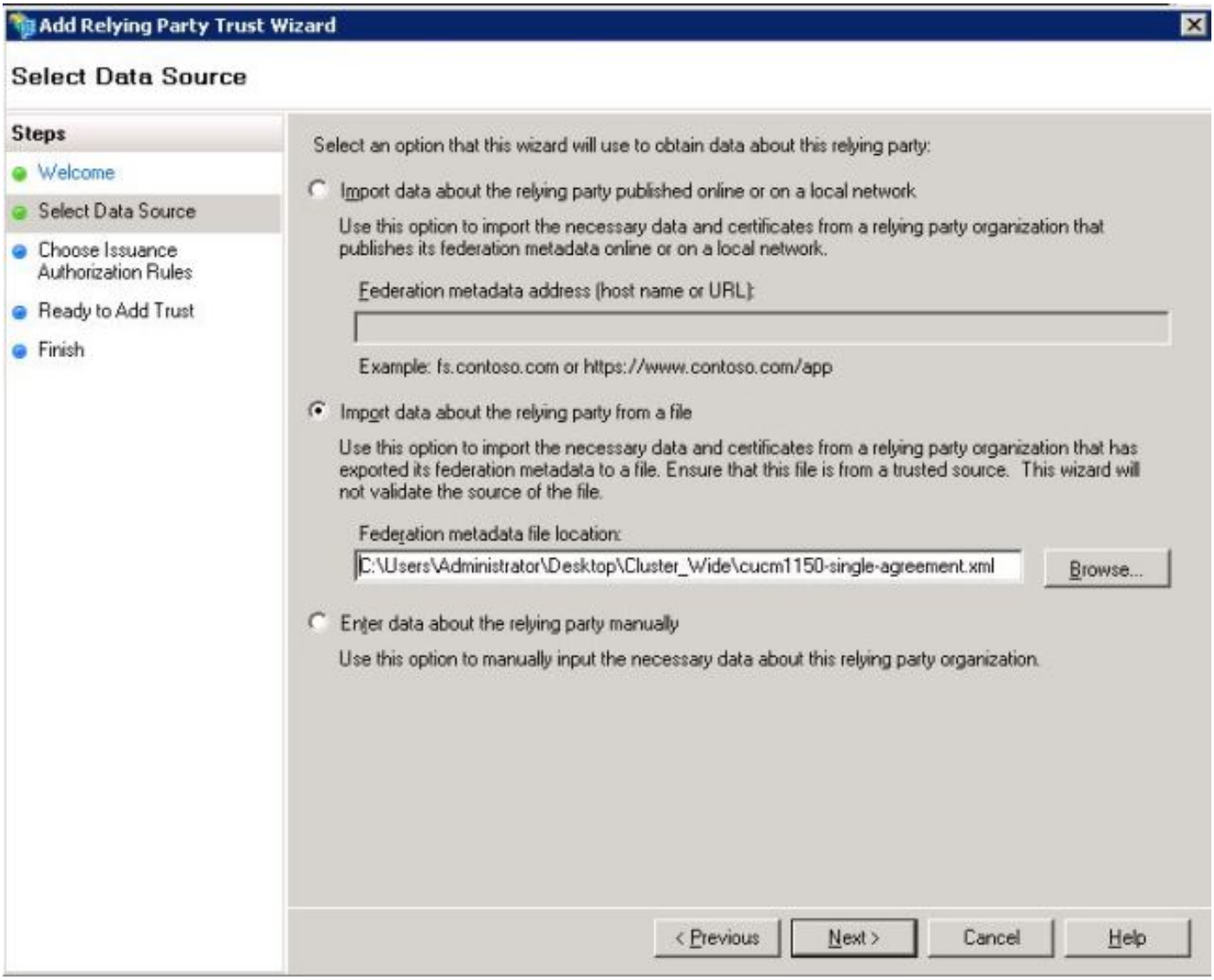
如图所示，导航至**AD FS 2.0管理/信任关系发运/信赖方信任。**单击"**添加信赖方信任**"。



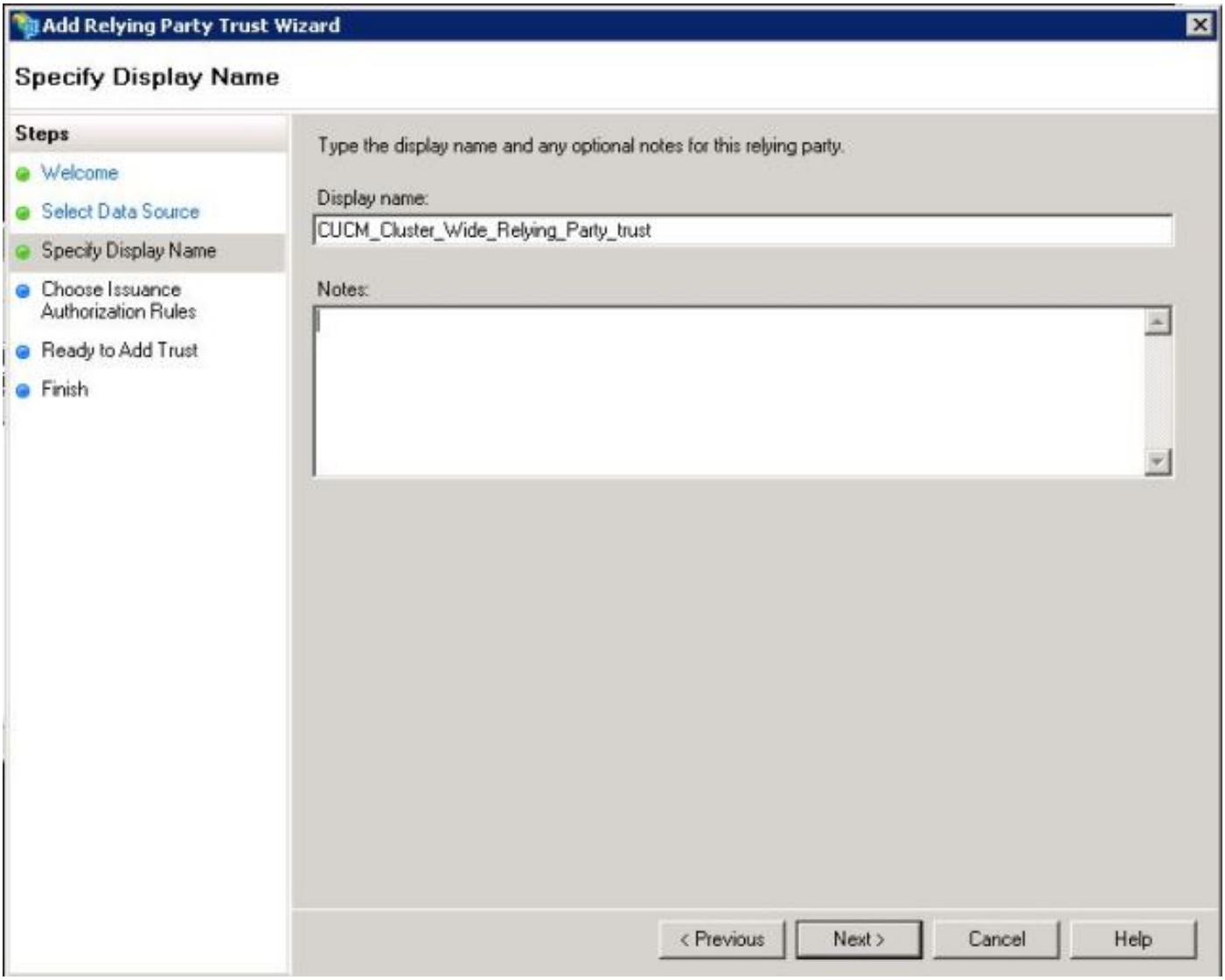
“添加信赖方信任向导”(Add Reling Party Trust Wizard)打开，如图所示，现在单击“**开始”**。



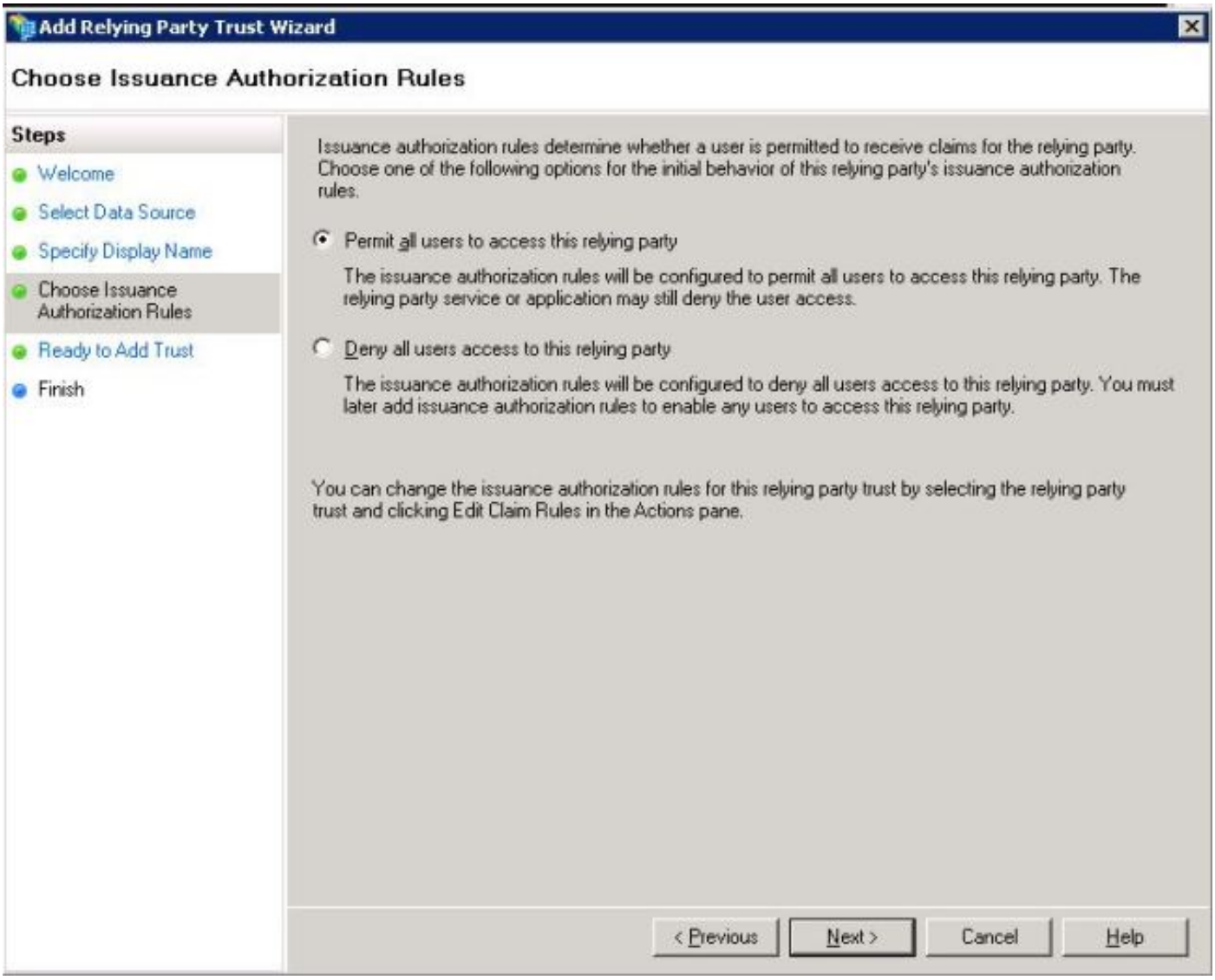
单击有关从文件中信赖方的导入数据。浏览从CUCM SAML SSO配置页下载的SP元数据。然后单击**Next**，如图所示：



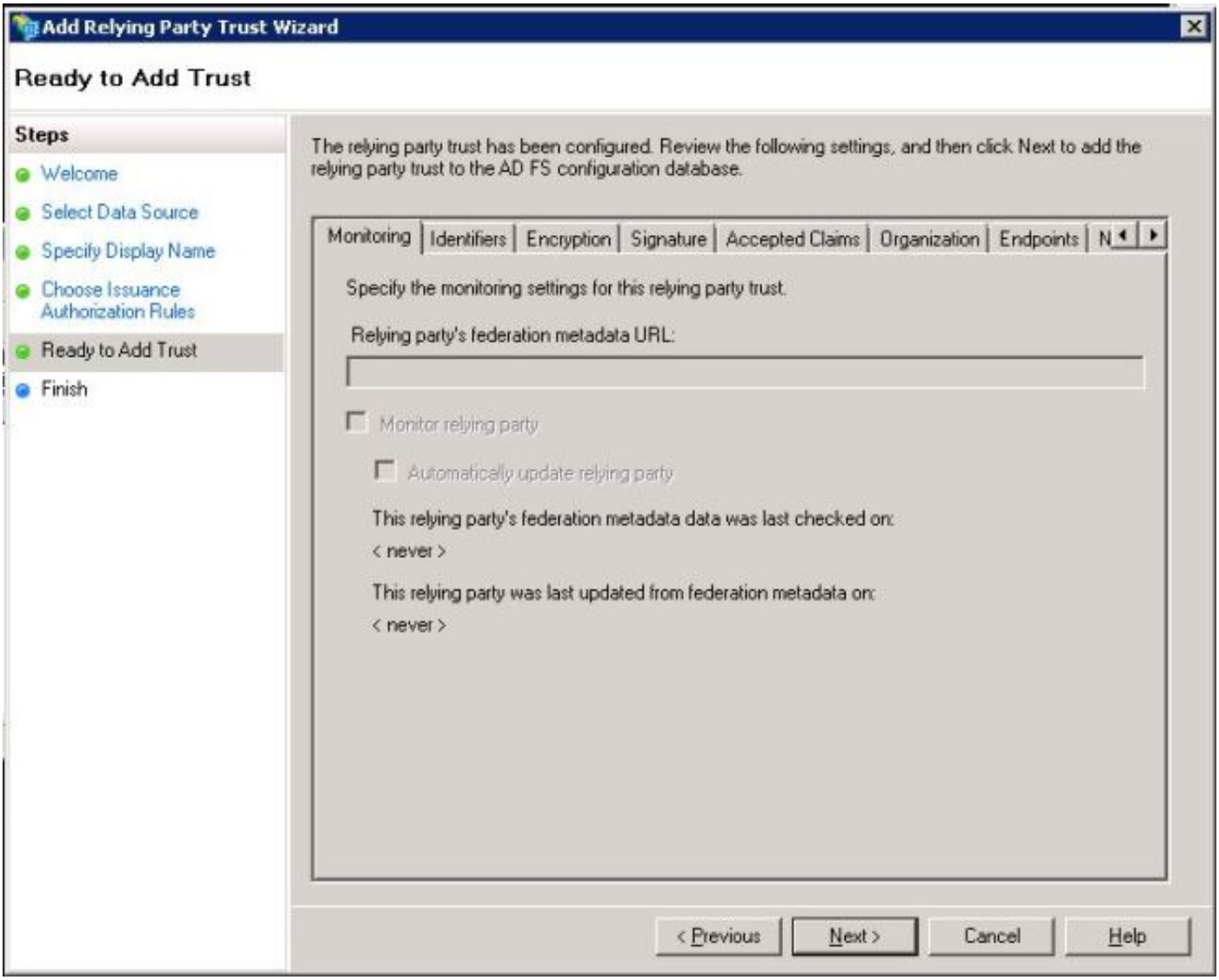
键入信赖方的显示名称和任何可选注释。单击**Next**，如图所示：



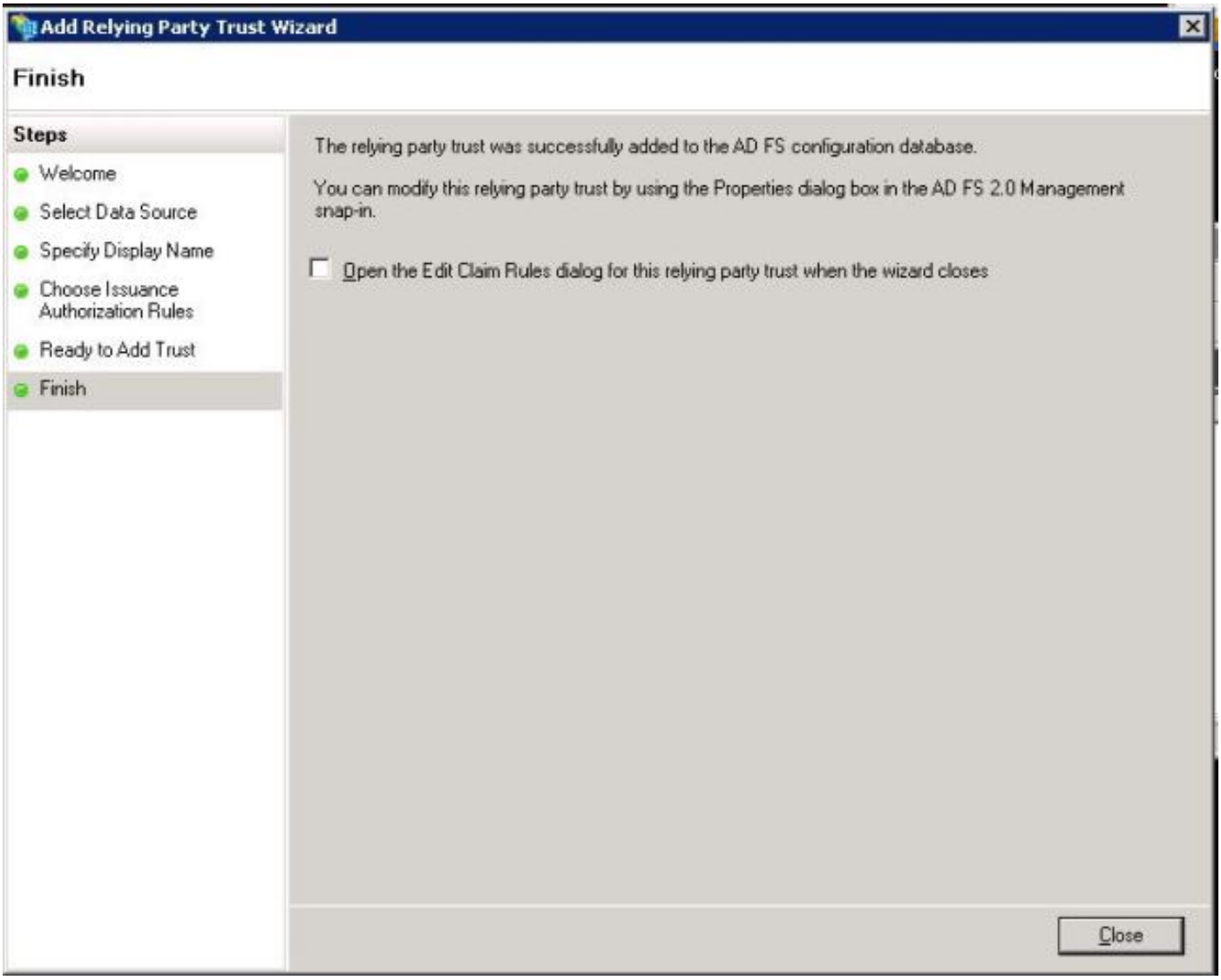
选择**允许所有用户访问此信赖方**以允许所有用户访问此信赖方，然后单击**下一步**，如图所示：



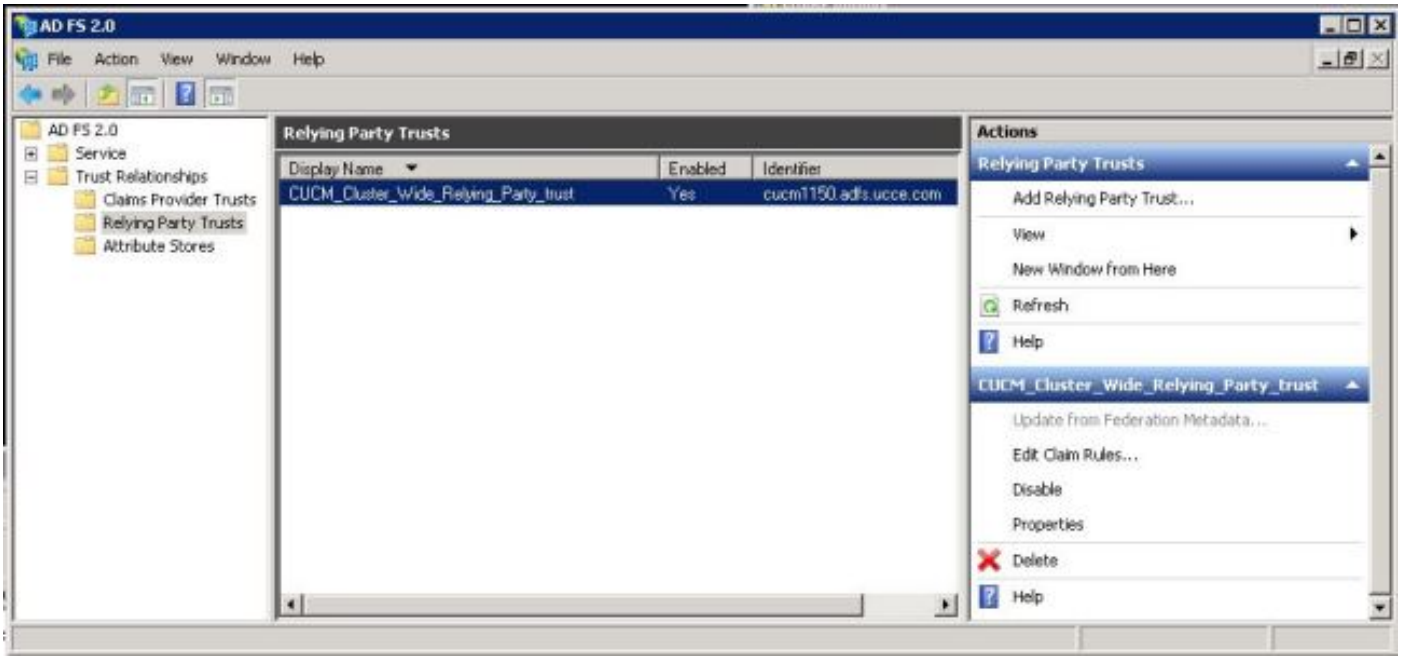
在“**准备添加信任”(Ready to Add Trust)页**面下，您可以查看已配置的信赖方信任的设置。现在单击**Next**，如图所示：



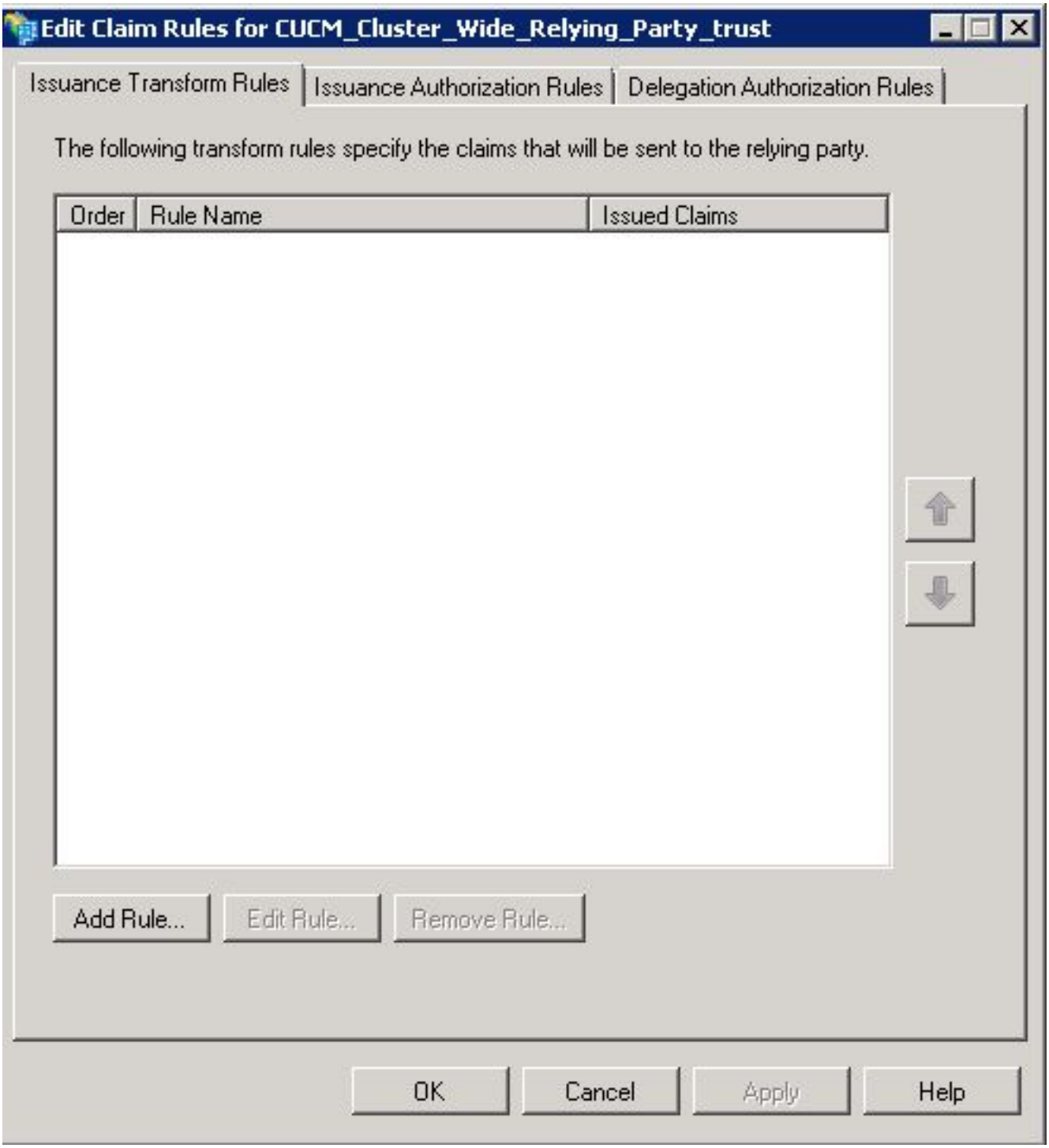
“完成”页确认信赖方信任已成功添加到AD FS配置数据库。取消选中“Box（框）”，然后单击“**Close（关闭）**”，如图所示：



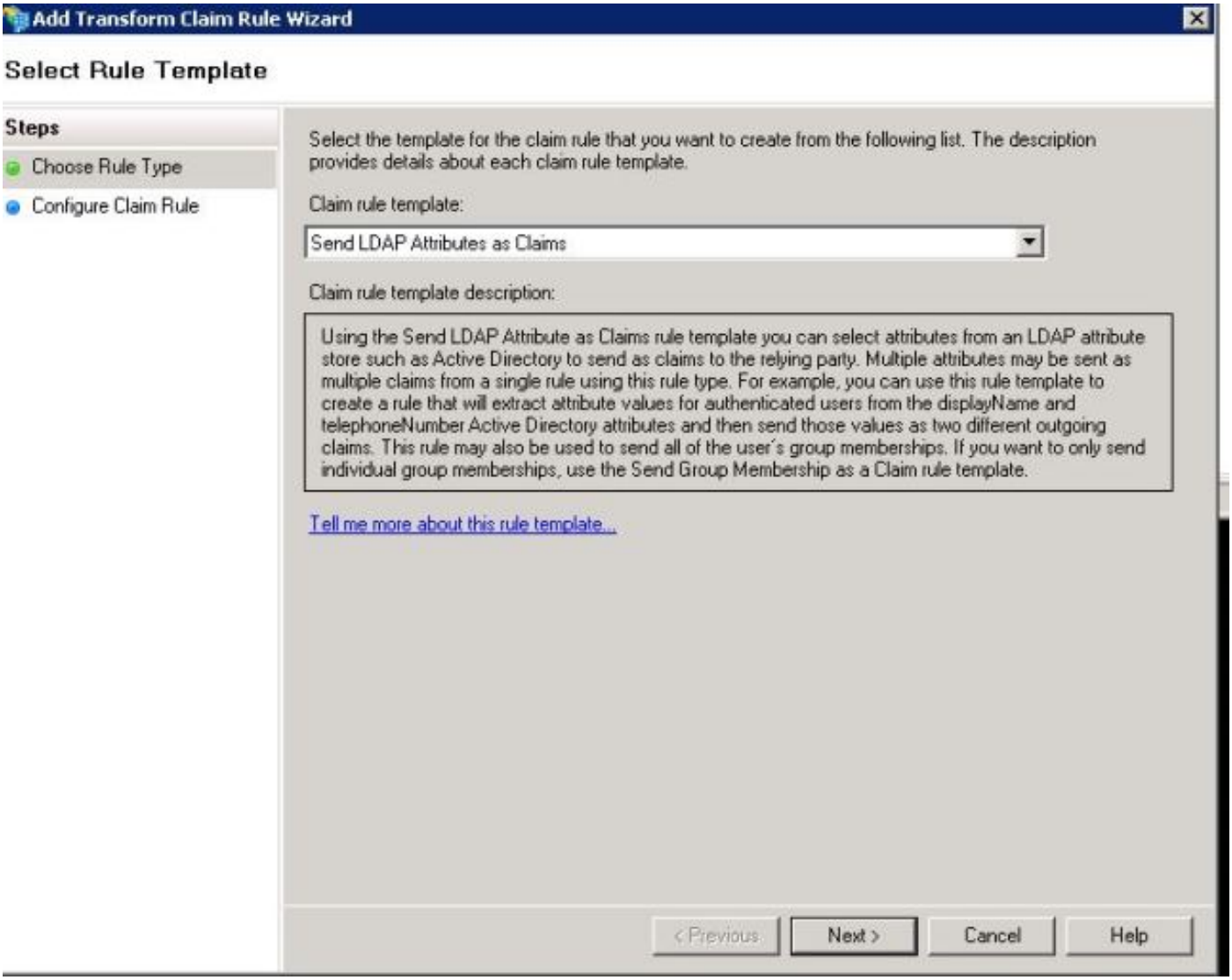
右键单击“信**赖方信任”**，然后单击“**编辑领款申**请规则”，如图所示：



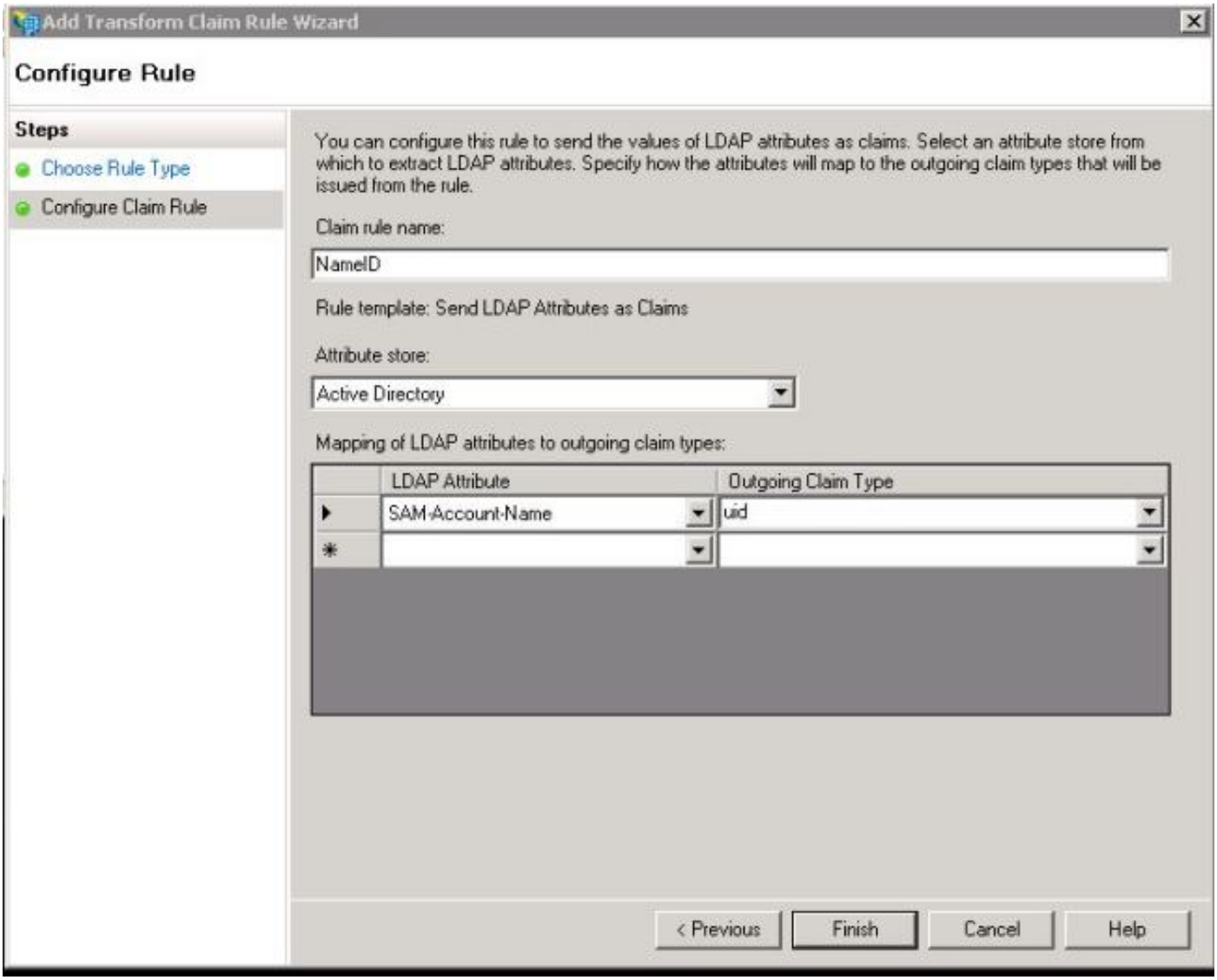
现在单击**Add Rule**，如图所示：



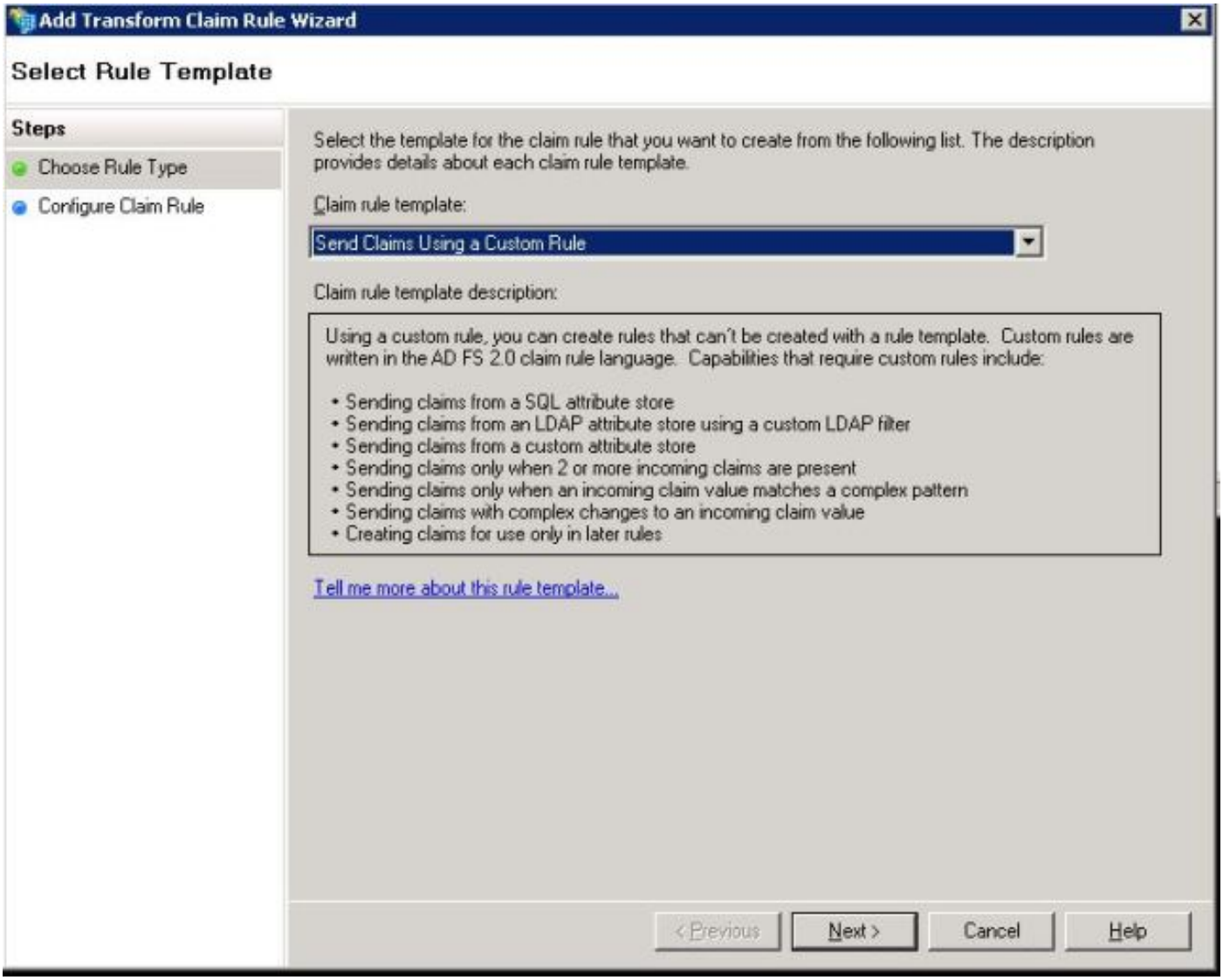
当“添**加转换声明规**则”(Add Transform Claim Rule)打开时，单**击使用默**认声明规则模板“**将LDAP属性作为声明发送”(Send LDAP Attributes as Claims)的“下一步”(Next)，如图所示：**



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：



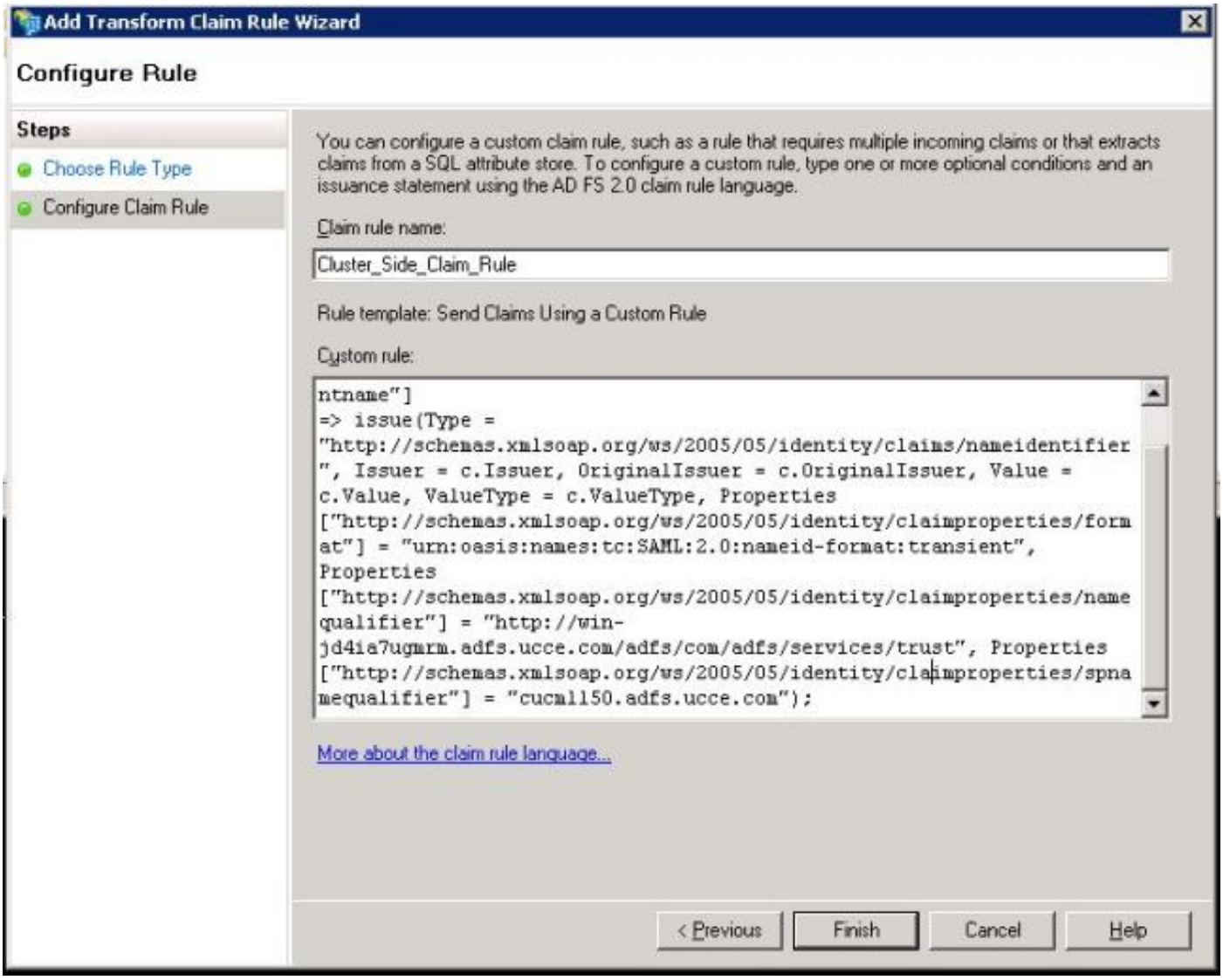
在配置领款申请规则中，键入领款申请规则名称，然后在修改领款申请规则中名称限定符和spname限定符的向导的“自定义规则”字段中，复制指定和过去的领款申请规则。单击**完成**，如图所示：

领款申请规则：

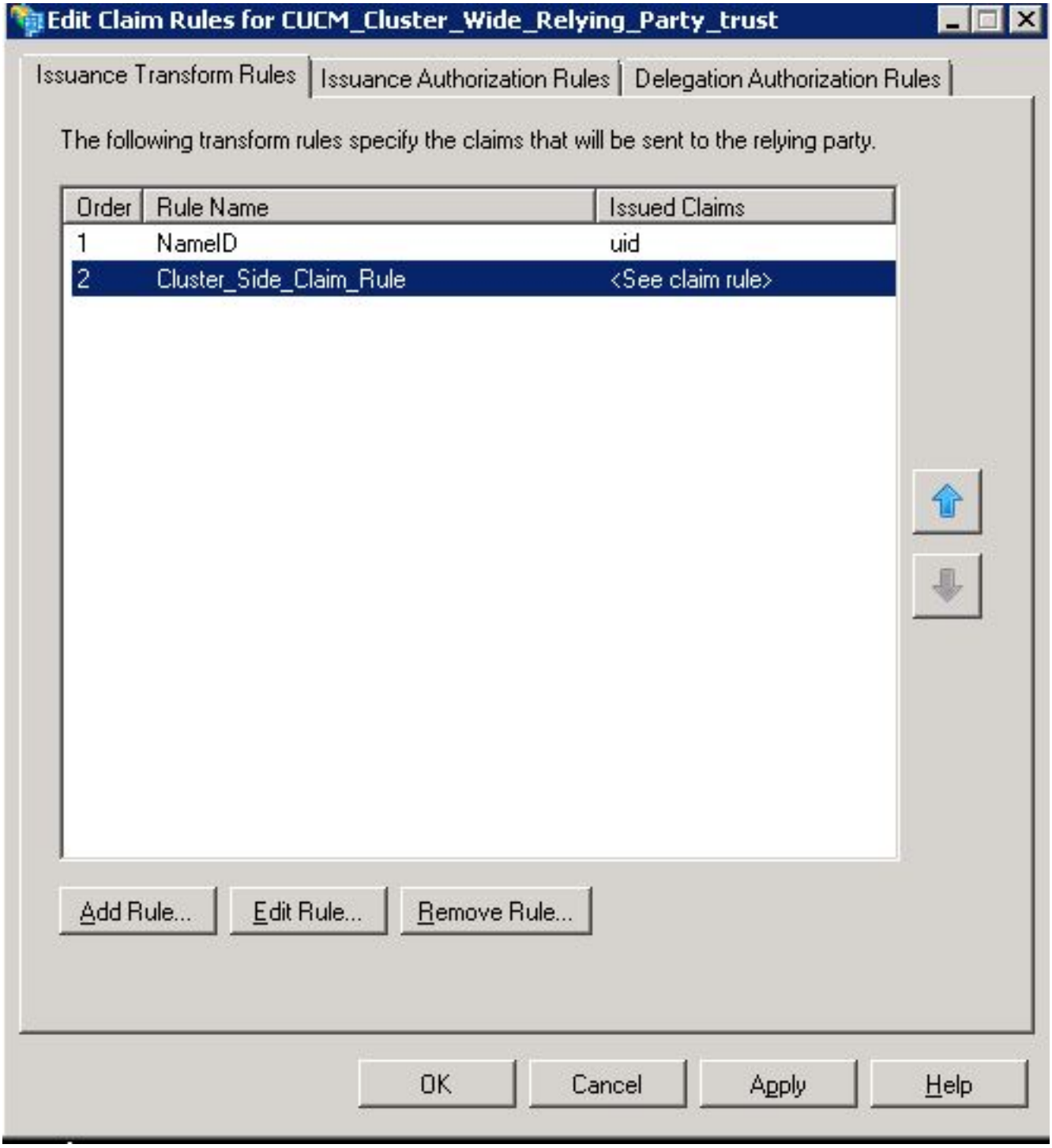
```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]

=> 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”**。

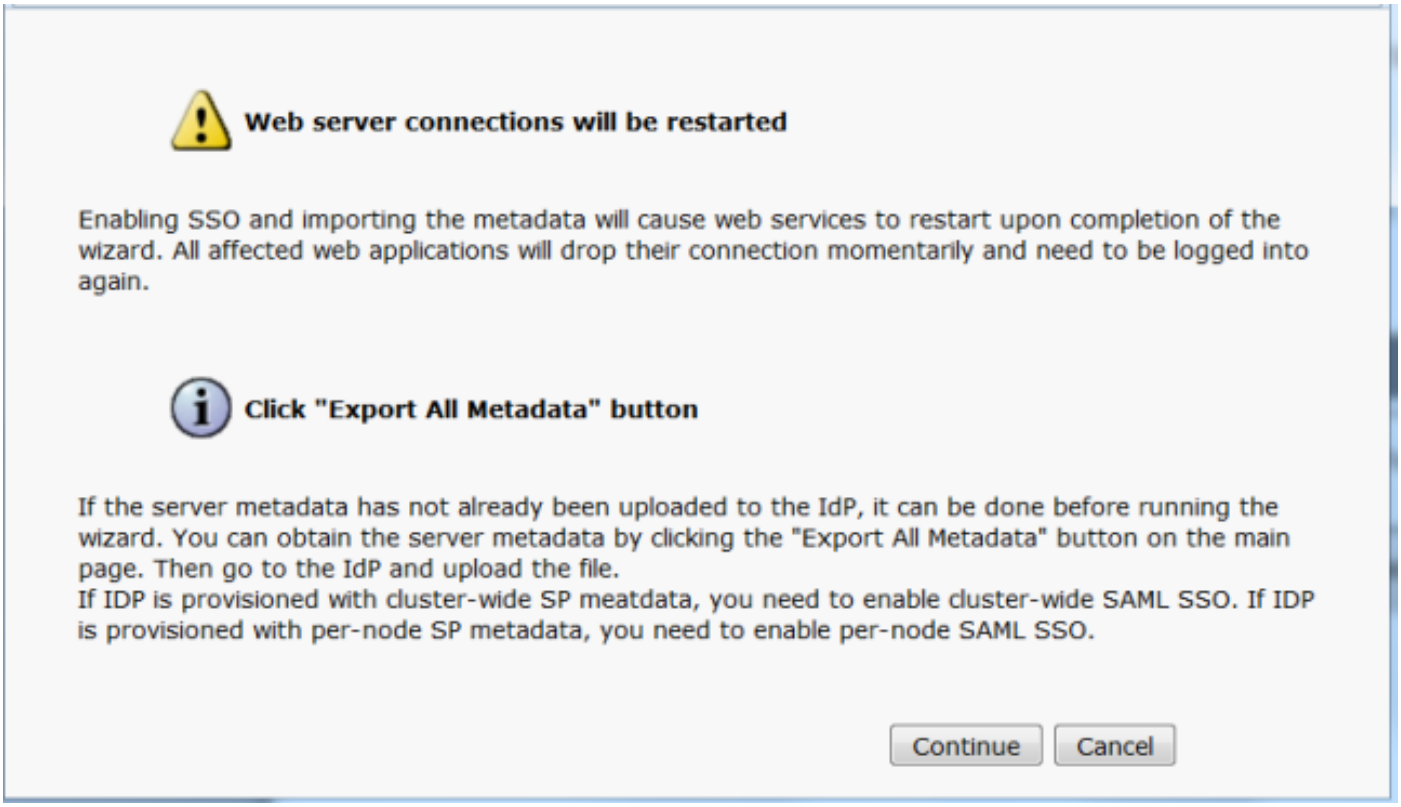


步骤4.启用SAML SSO

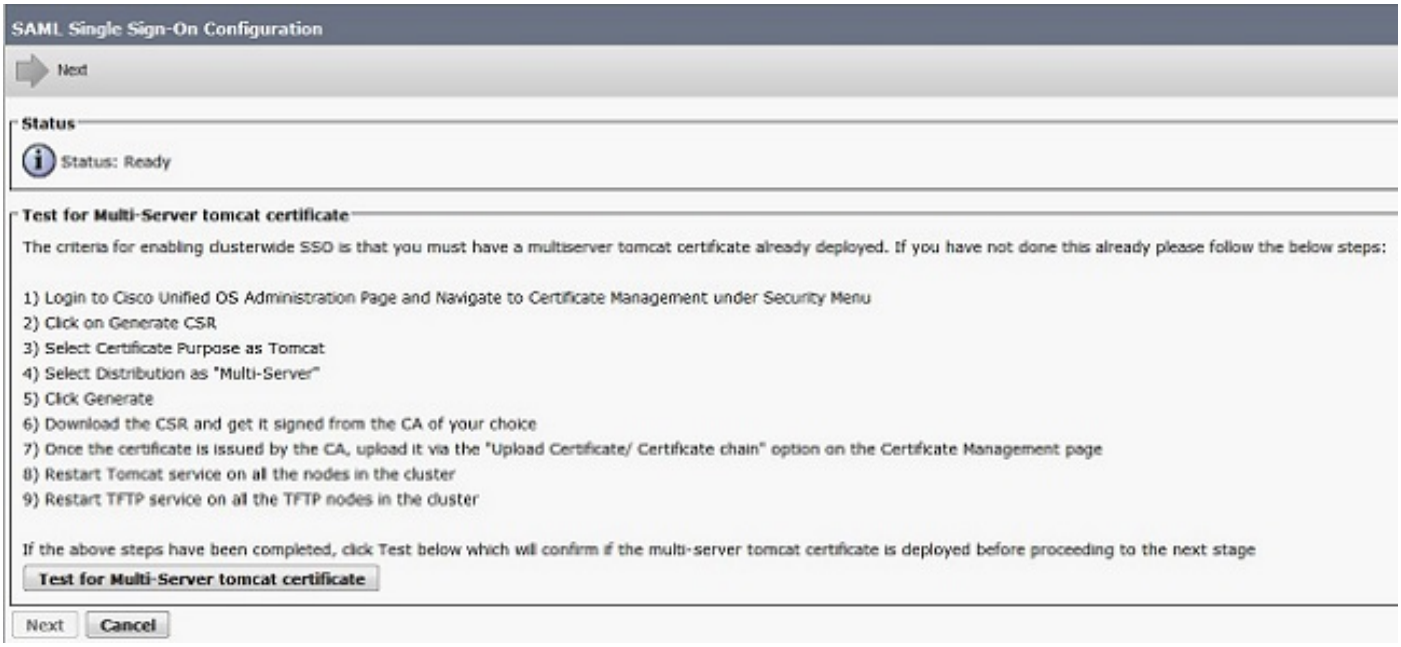
打开Web浏览器，以管理员身份登录CUCM，然后导航到**System >SAML Single Sign On**。

默认情况下，选**择"集群**范围"单选按钮。单击**Enable Saml SSO**，如图所示：

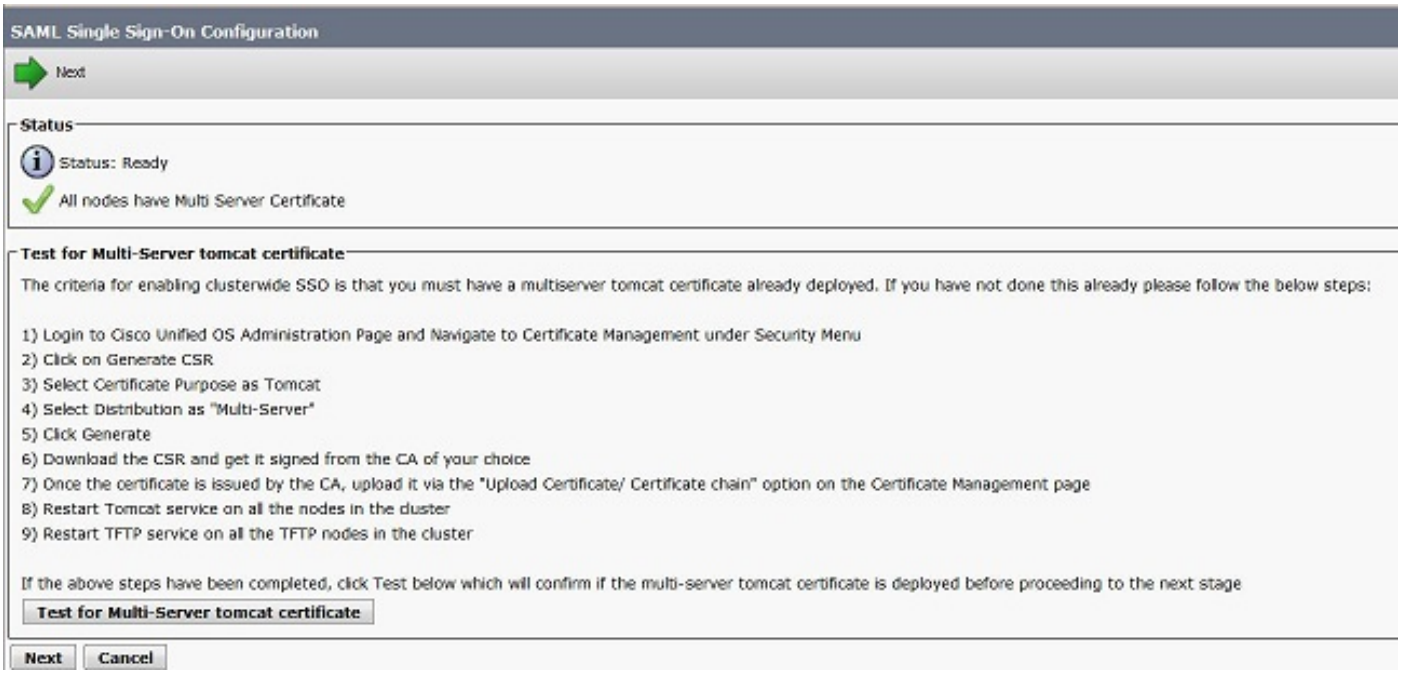
如图所示，弹出窗口会通知Web服务器重新启动的警告和信息，以根据idp选择集群范围的SAML SSO或每节点SAML SSO。单击 **Continue**。



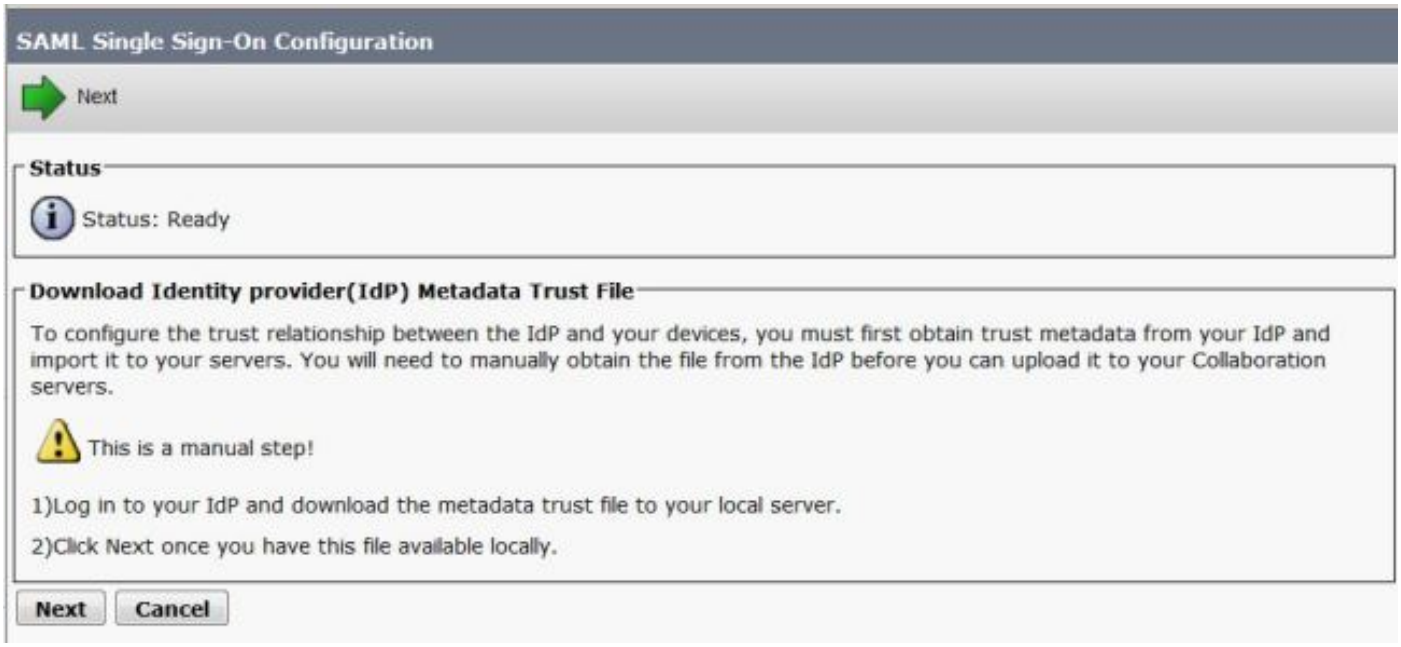
启用集群范围SSO的条件是必须已部署多服务器Tomcat证书。单击**Test for Multi-Server Tomcat Certificate（测试多服务器Tomcat证书）**，如图所示：



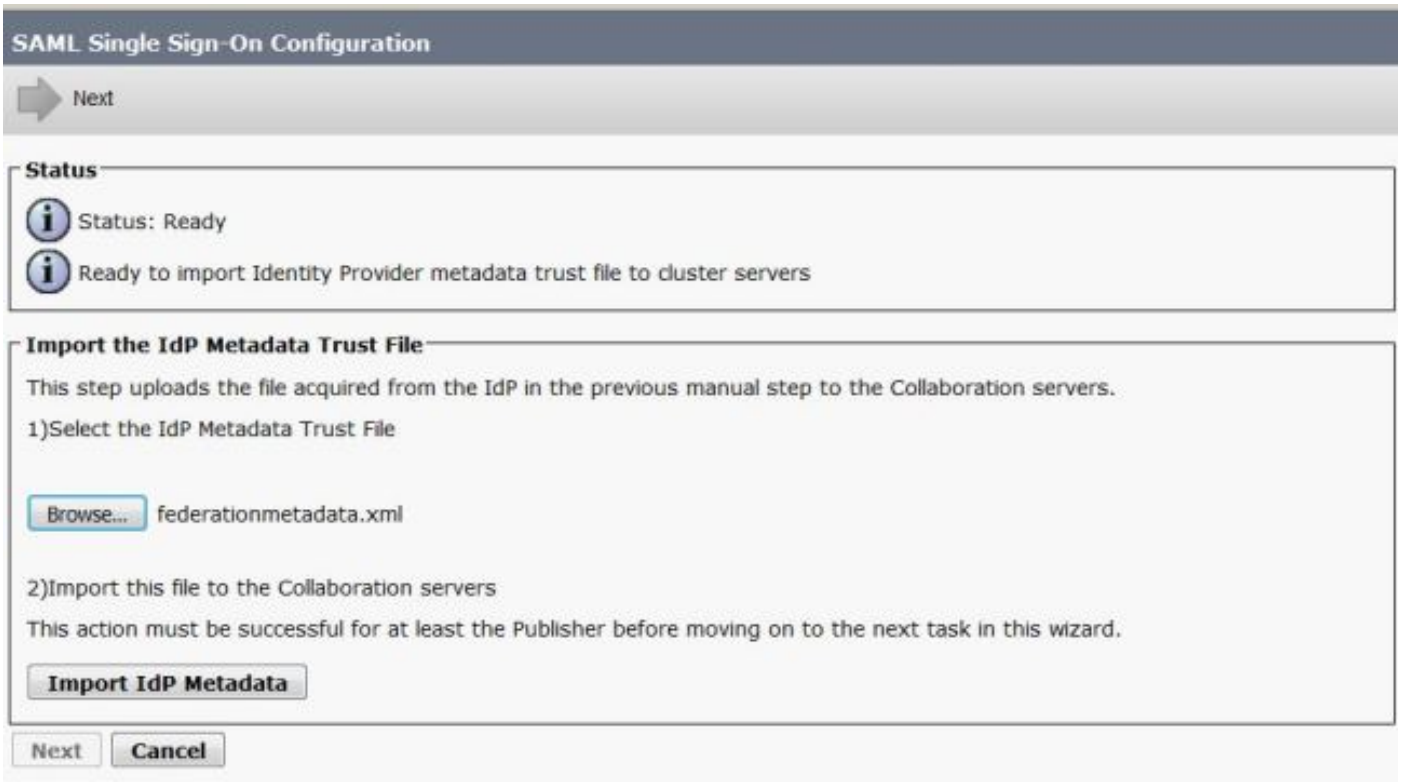
确认后，所有节点的“多服务器证书”(Multi Server Certificate)都会显示“**所有节点都有多服务器证书”(All Nodes have Multi Server Certificate)**，然后单击**“下一步”(Next)，如图所示：**



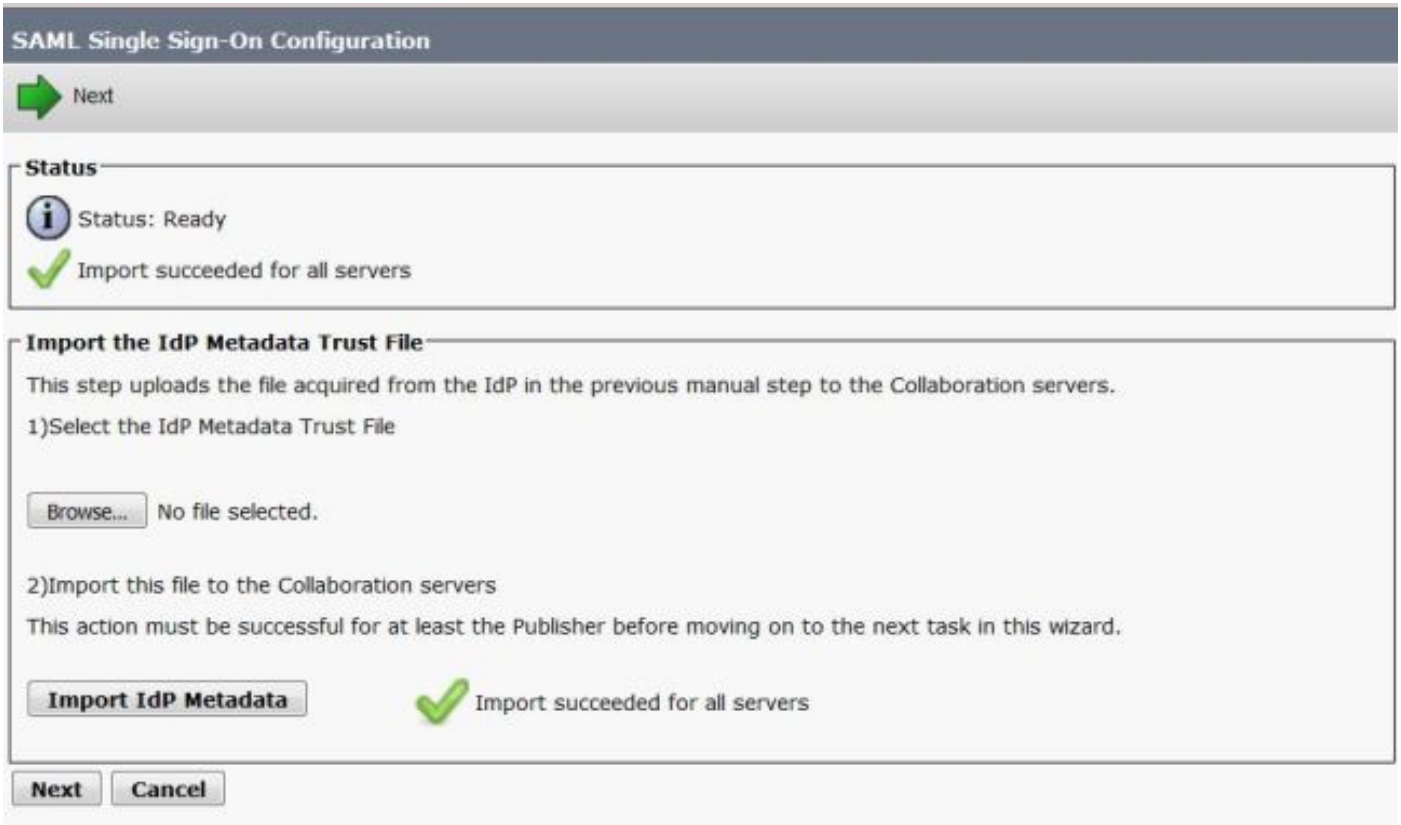
如图所示，单击“下一**步”**。



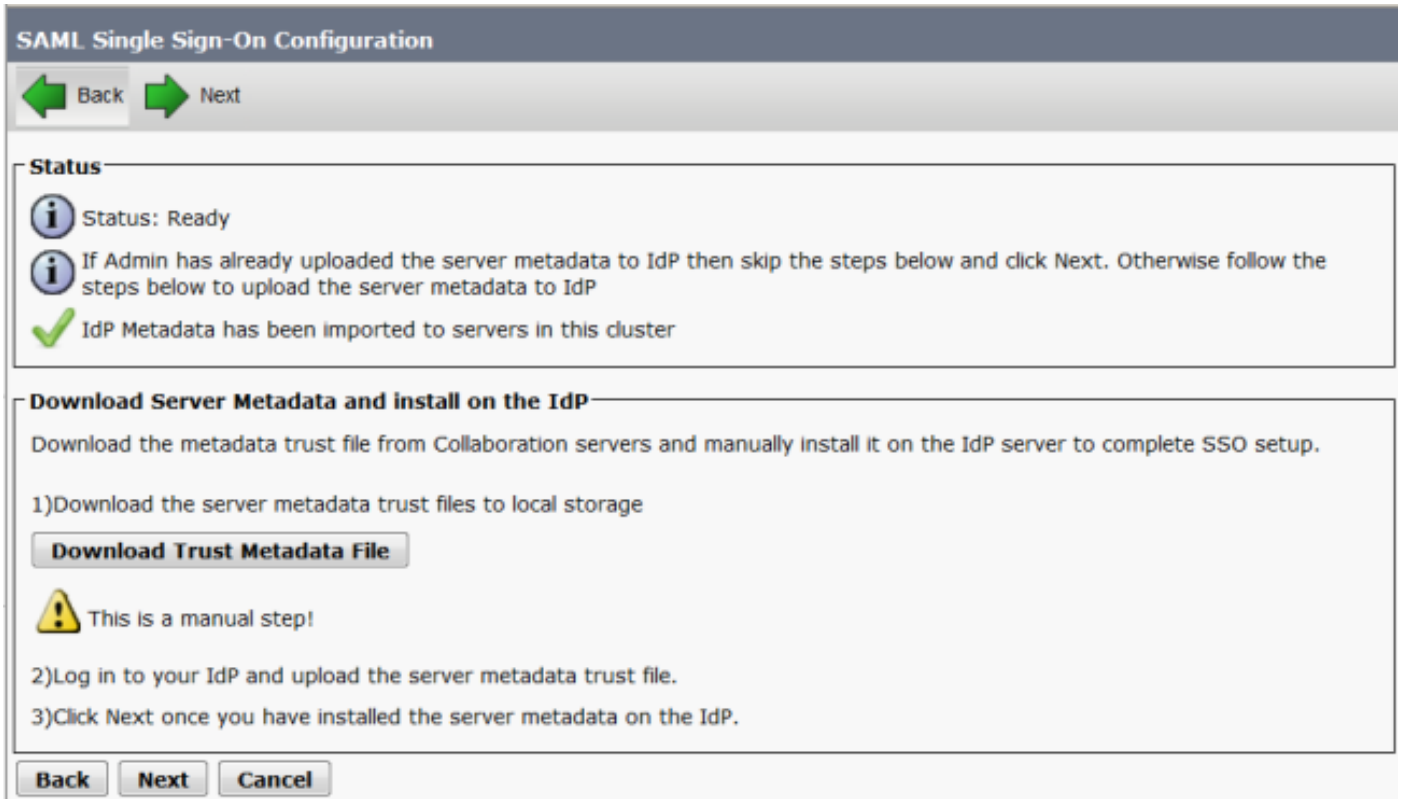
浏览并选择下载的IdP元数据。单击**导入IdP元数据**，如图所示：



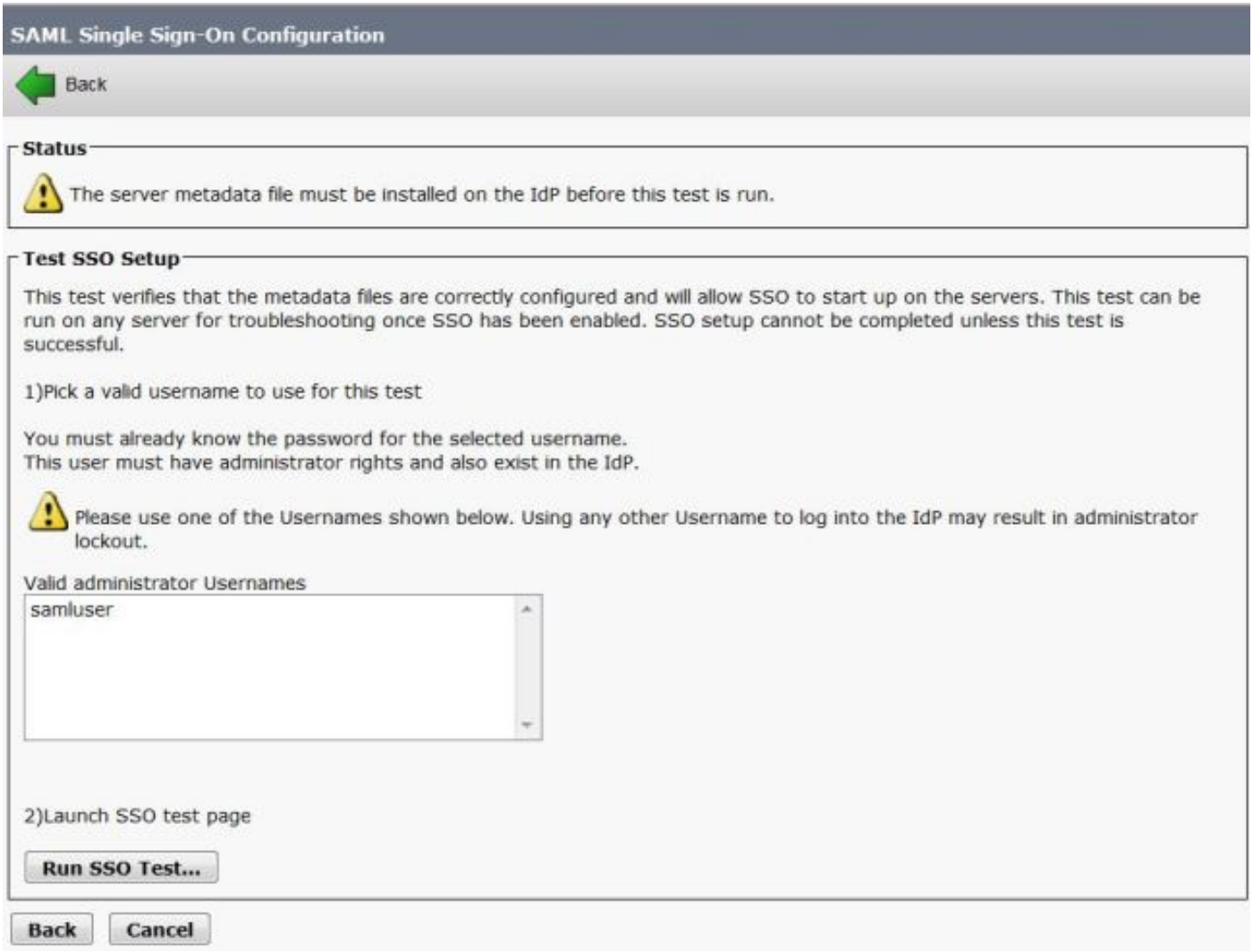
该页确认Import succeeded for all servers，然后单击**Next**，如图所示：



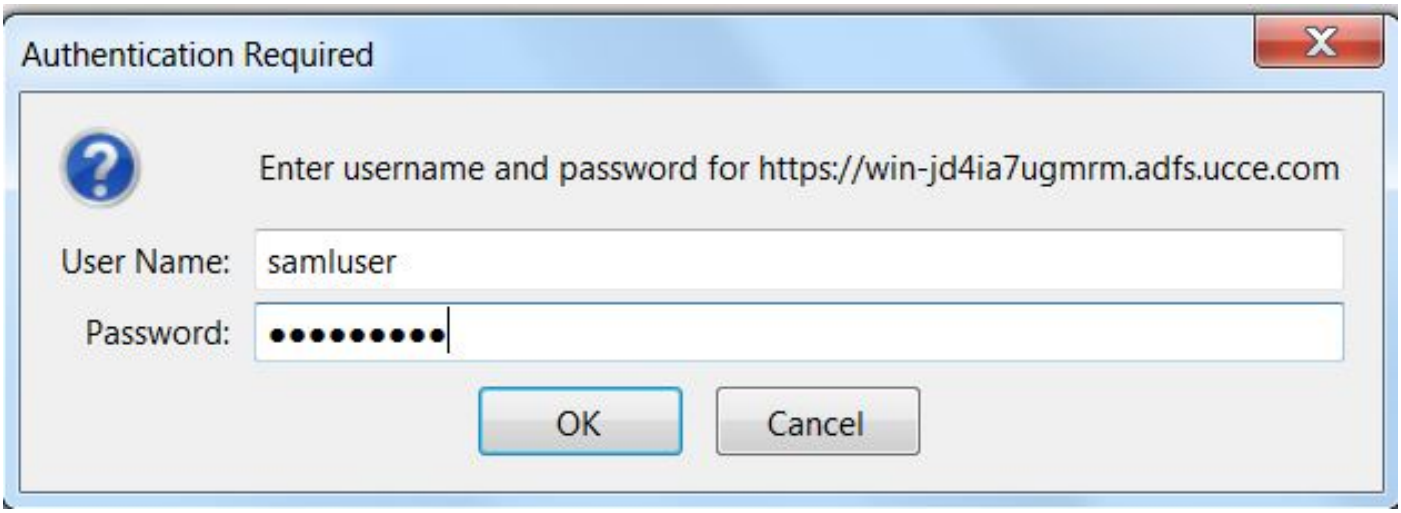
如图所示，单击**Next**，因为已从初始SAML SSO配置页导出SP元数据。



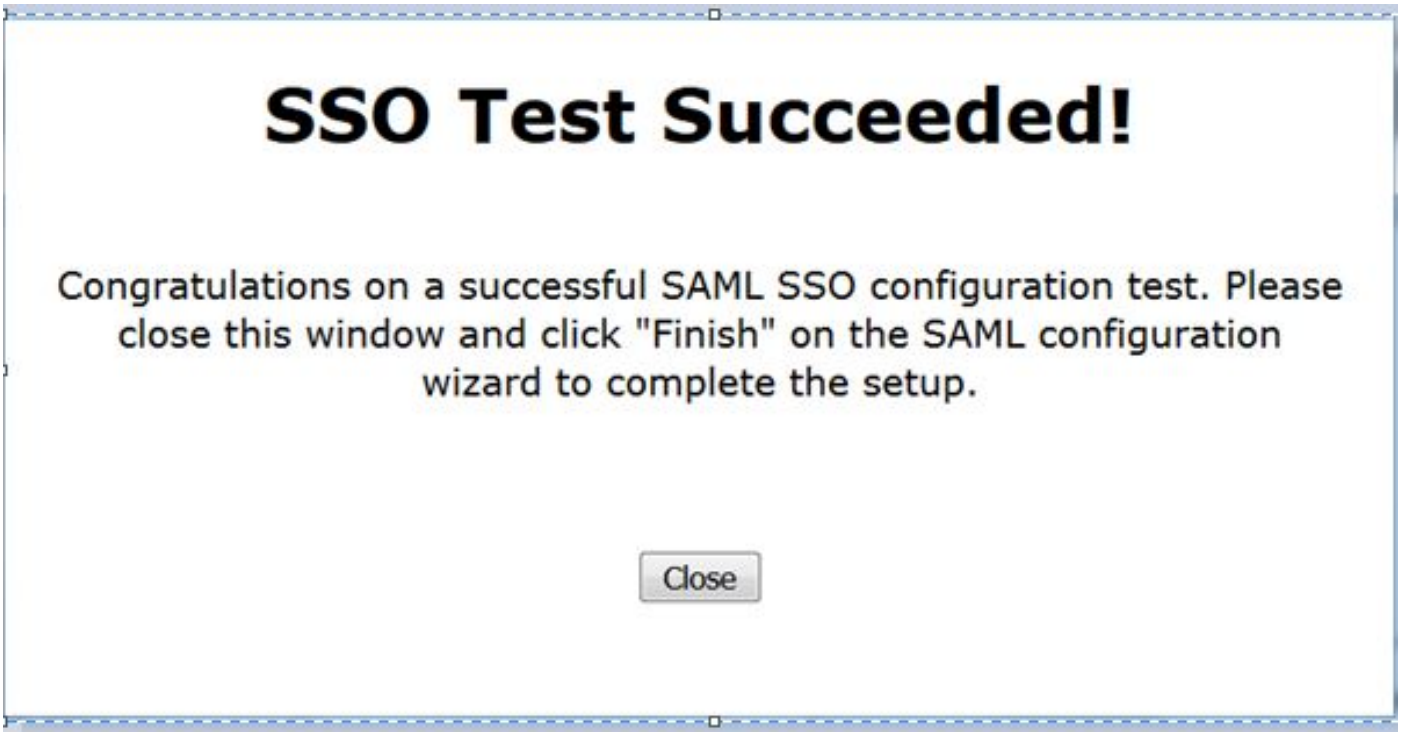
CUCM必须与LDAP目录同步。向导显示在LDAP目录中配置的有效管理员用户。选择用户，然后单击**运行SSO测**试，如图所示：



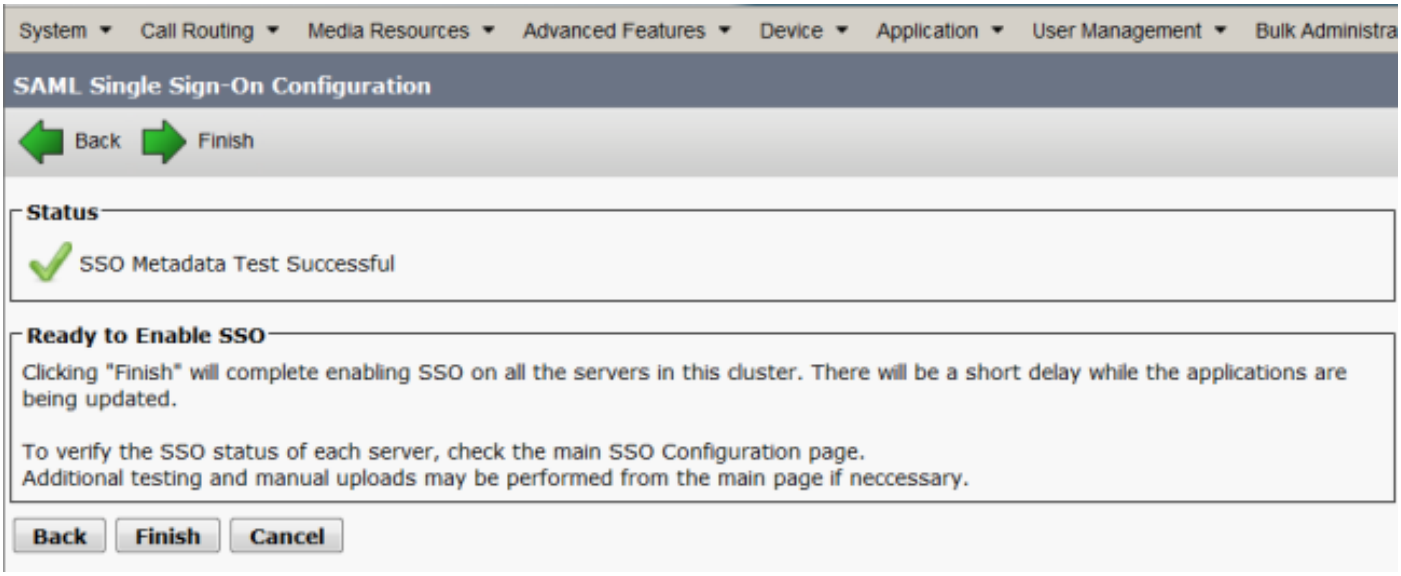
如图所示，在提示后输入用户ID和相应的密码。



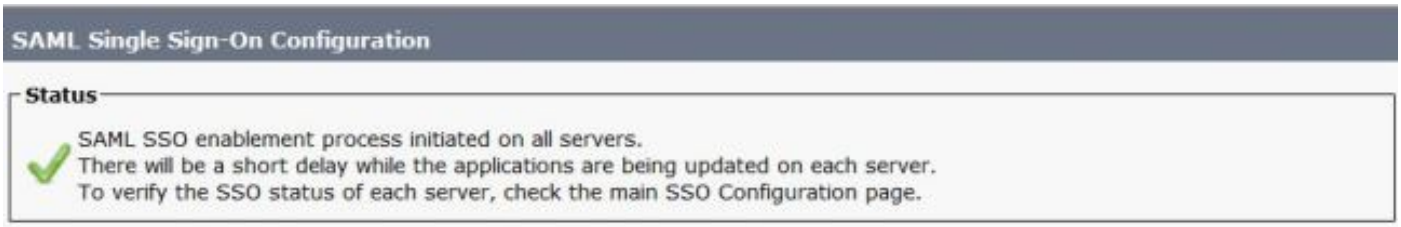
弹出窗口（如图所示）确认测试成功。



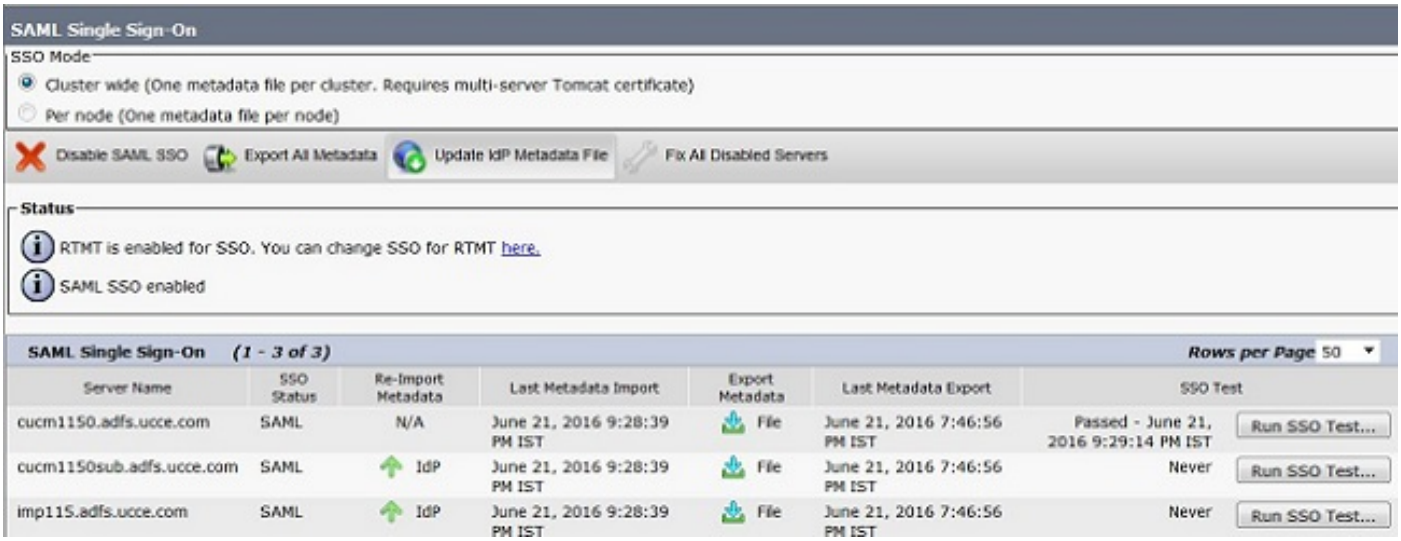
如图所示，单击**完成**以完成启用SSO的配置。



图中显示的页面确认SAML SSO启用进程在所有服务器上启动。



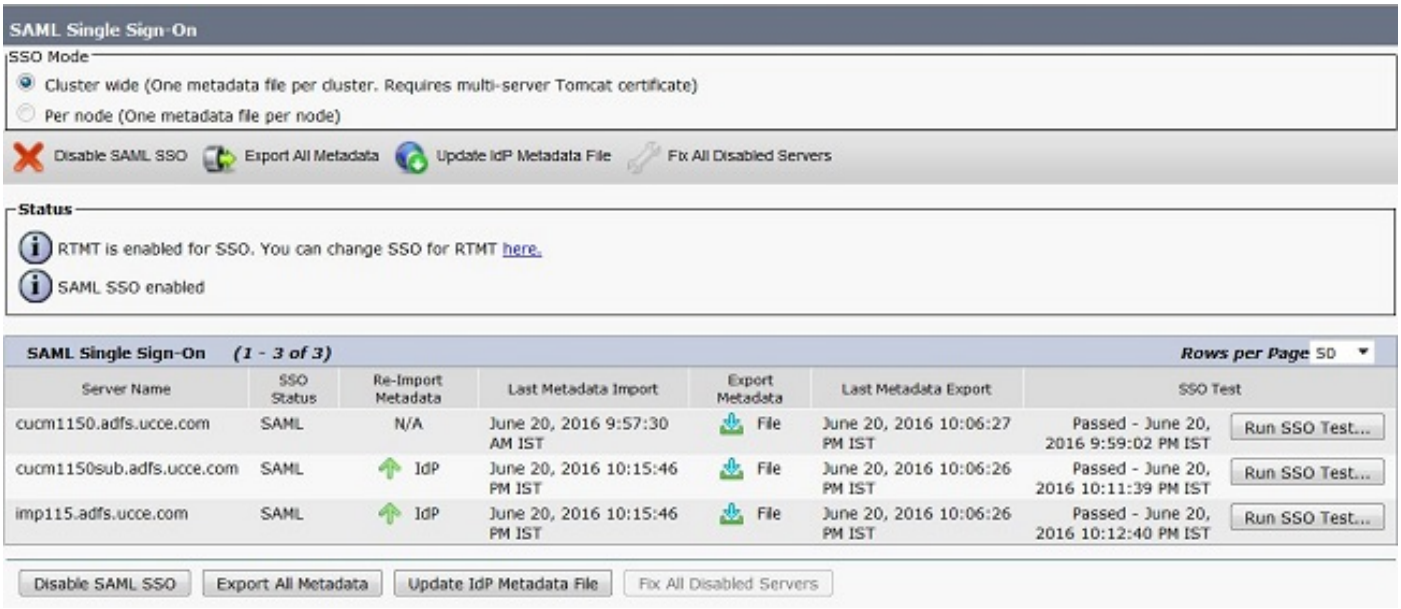
使用SAML SSO凭证注销并重新登录CUCM。导航至**系统>SAML单点登录。**单击运行**SSO测试**以查找群集中的其他节点，如图所示：



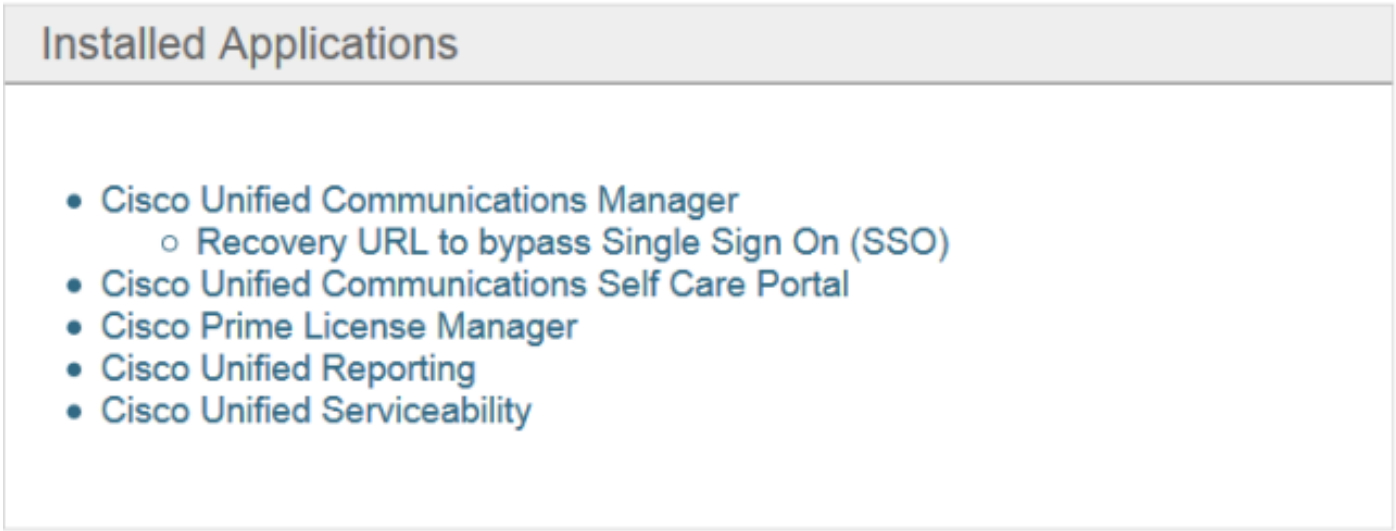
验证

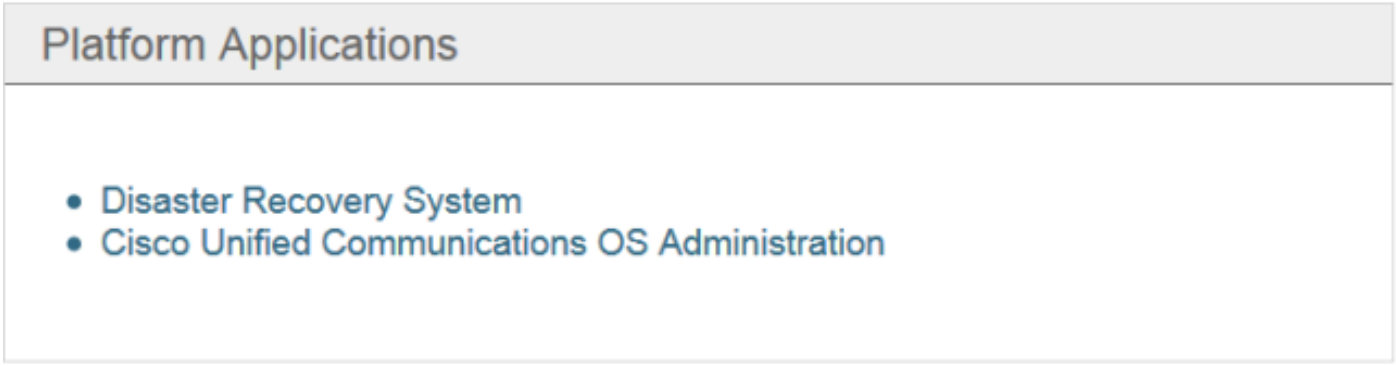
使用本部分可确认配置能否正常运行。

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。



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。





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：

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
```