使用CUCM和AD FS 2.0配置单点登录

目录

简介

本文档介绍如何在Cisco Unified Communications Manager和Active Directory联合身份验证服务上配置单点登录(SSO)。

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)
- Active Directory联合身份验证服务(AD FS)的基本知识

要在您的实验环境中启用SSO，需要以下配置：

- 安装了AD FS的Windows Server。
- 配置了LDAP同步的CUCM。
- 已选择标准CCM超级用户角色的最终用户。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 带AD FS 2.0的Windows Server
- CUCM 10.5.2

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

提供了在Windows Server 2008 R2上使用AD FS 2.0的过程。这些步骤也适用于Windows Server 2016上的AD FS 3.0。

在Windows服务器上下载并安装AD FS 2.0

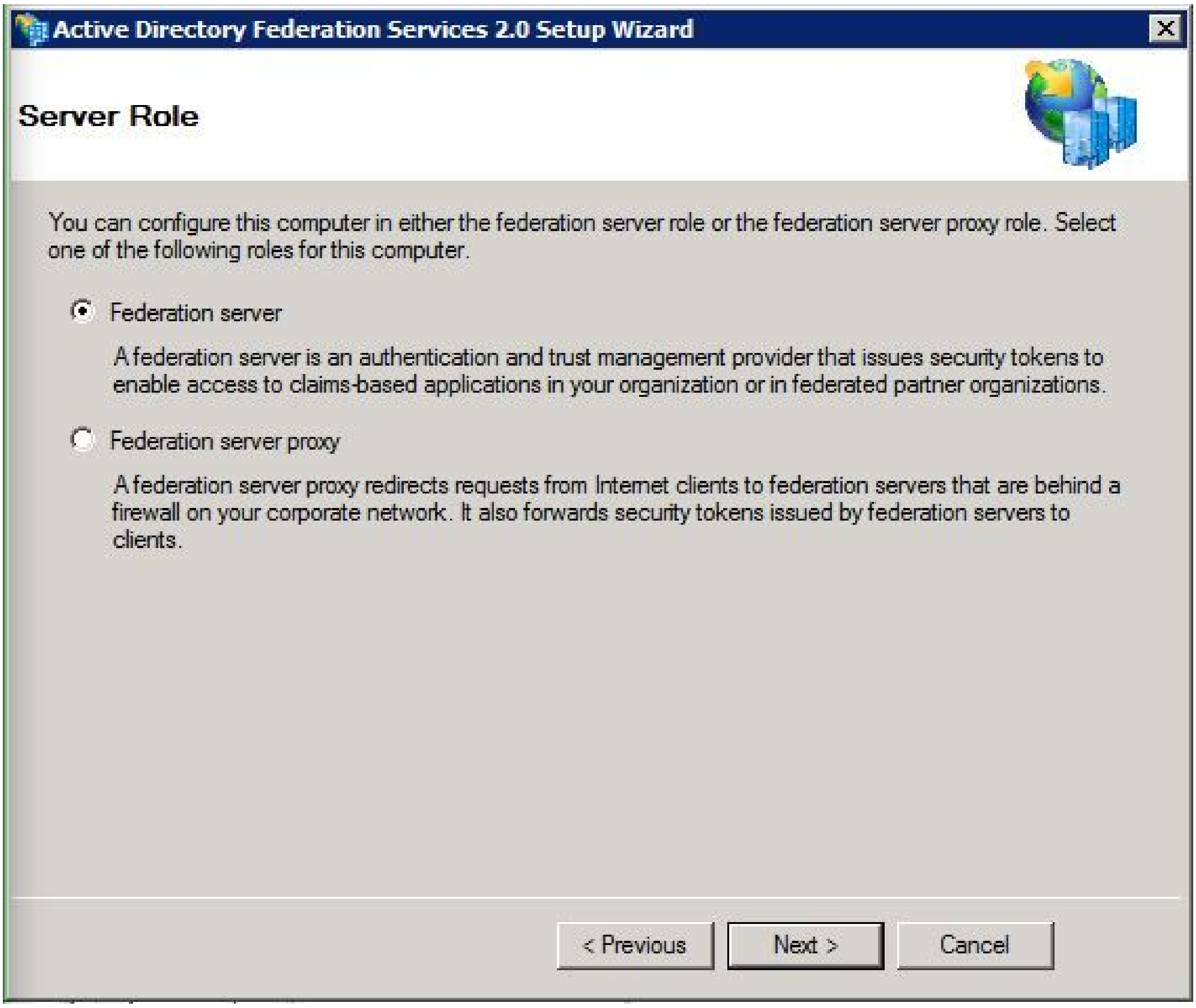
步骤1:导航至下载AD FS 2.0。

第二步：确保根据Windows Server选择适当的下载。

第三步：将下载的文件移动到Windows服务器。

第四步：继续安装：

第五步：出现提示时，选择联合服务器:



Active Directory Federation Services 2.0 Setup Wizard

Server Role

You can configure this computer in either the federation server role or the federation server proxy role. Select one of the following roles for this computer.

● Federation server

A federation server is an authentication and trust management provider that issues security tokens to enable access to claims-based applications in your organization or in federated partner organizations.

○ Federation server proxy

A federation server proxy redirects requests from Internet clients to federation servers that are behind a firewall on your corporate network. It also forwards security tokens issued by federation servers to clients.

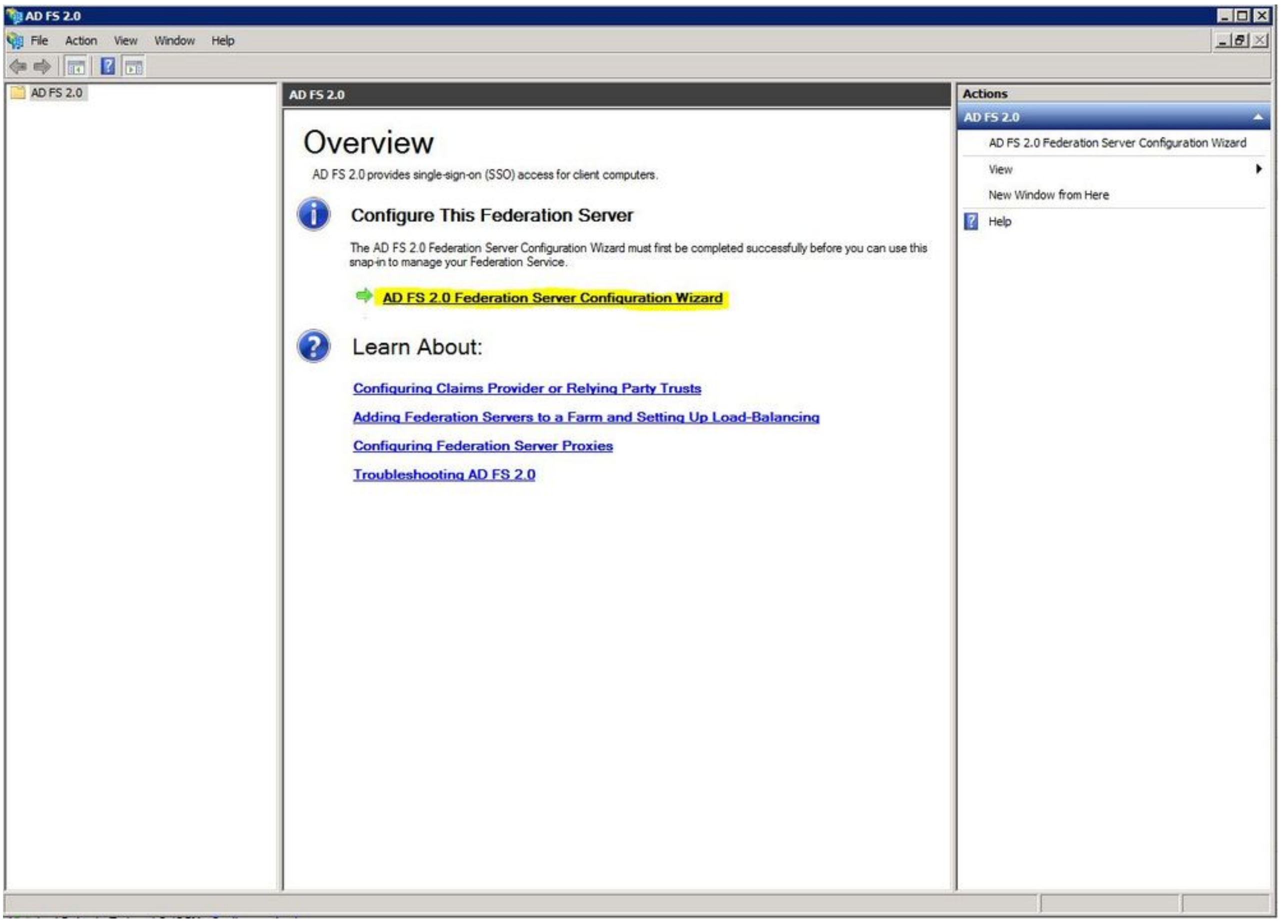
步骤6.自动安装某些依赖关系 — 完成后，单击完成。

现在您的服务器上已安装AD FS 2.0，您需要添加一些配置。

在Windows服务器上配置AD FS 2.0

步骤1:如果在安装后没有自动打开AD FS 2.0窗口，可以单击Start并搜索AD FS 2.0 Management以手动打开它。

第二步：选择AD FS 2.0联合服务器配置向导。



AD FS 2.0
File Action View Window Help
AD FS 2.0
AD FS 2.0
Actions
AD FS 2.0
AD FS 2.0 Federation Server Configuration Wizard
View
New Window from Here
Help

Overview

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

Configure This Federation Server

The AD FS 2.0 Federation Server Configuration Wizard must first be completed successfully before you can use this snap-in to manage your Federation Service.

AD FS 2.0 Federation Server Configuration Wizard

Learn About:

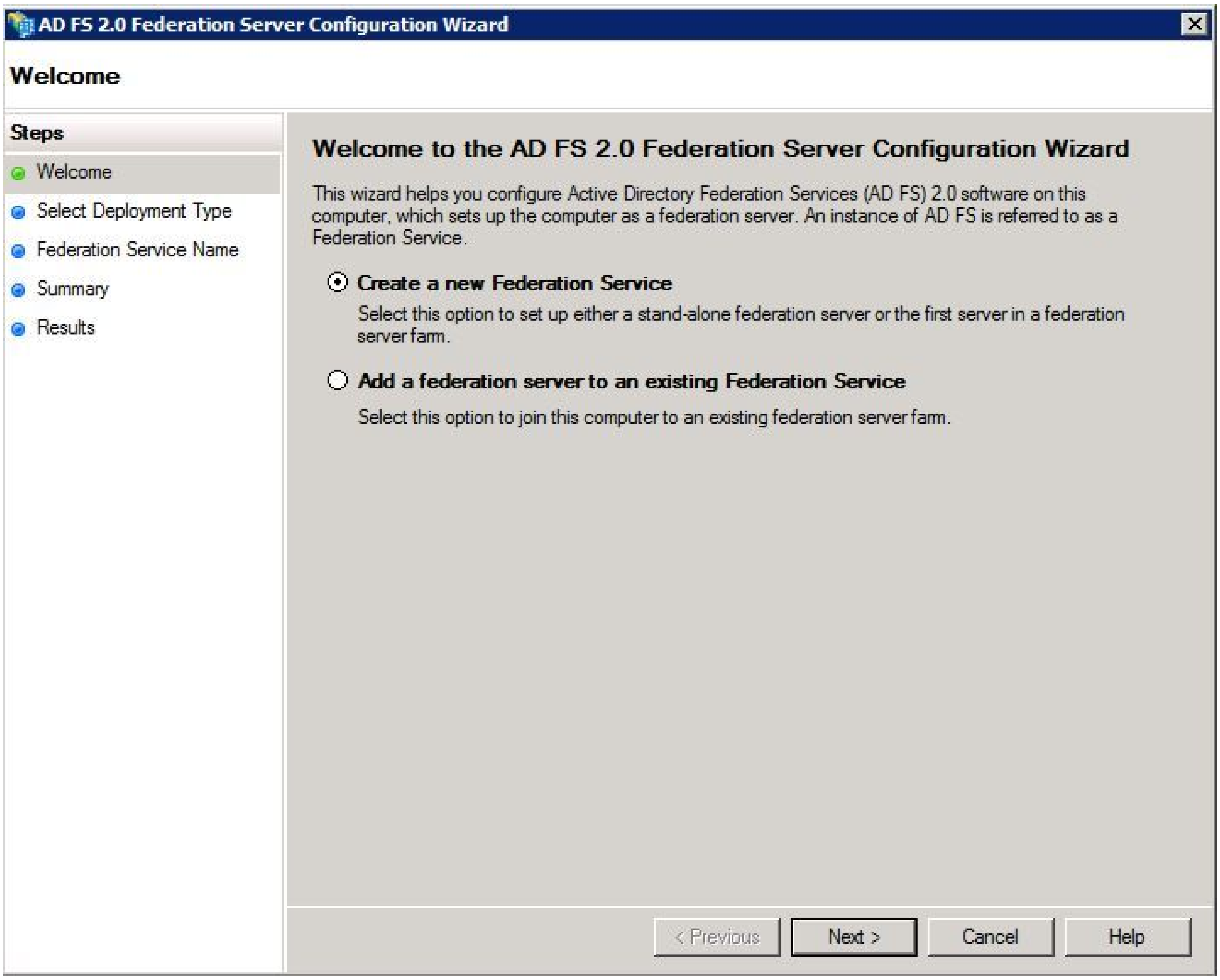
Configuring Claims Provider or Relying Party Trusts

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

Configuring Federation Server Proxies

Troubleshooting AD FS 2.0

步骤3.下一步，单击创建新的联合身份验证服务。



Welcome to the AD FS 2.0 Federation Server Configuration Wizard

This wizard helps you configure Active Directory Federation Services (AD FS) 2.0 software on this computer, which sets up the computer as a federation server. An instance of AD FS is referred to as a Federation Service.

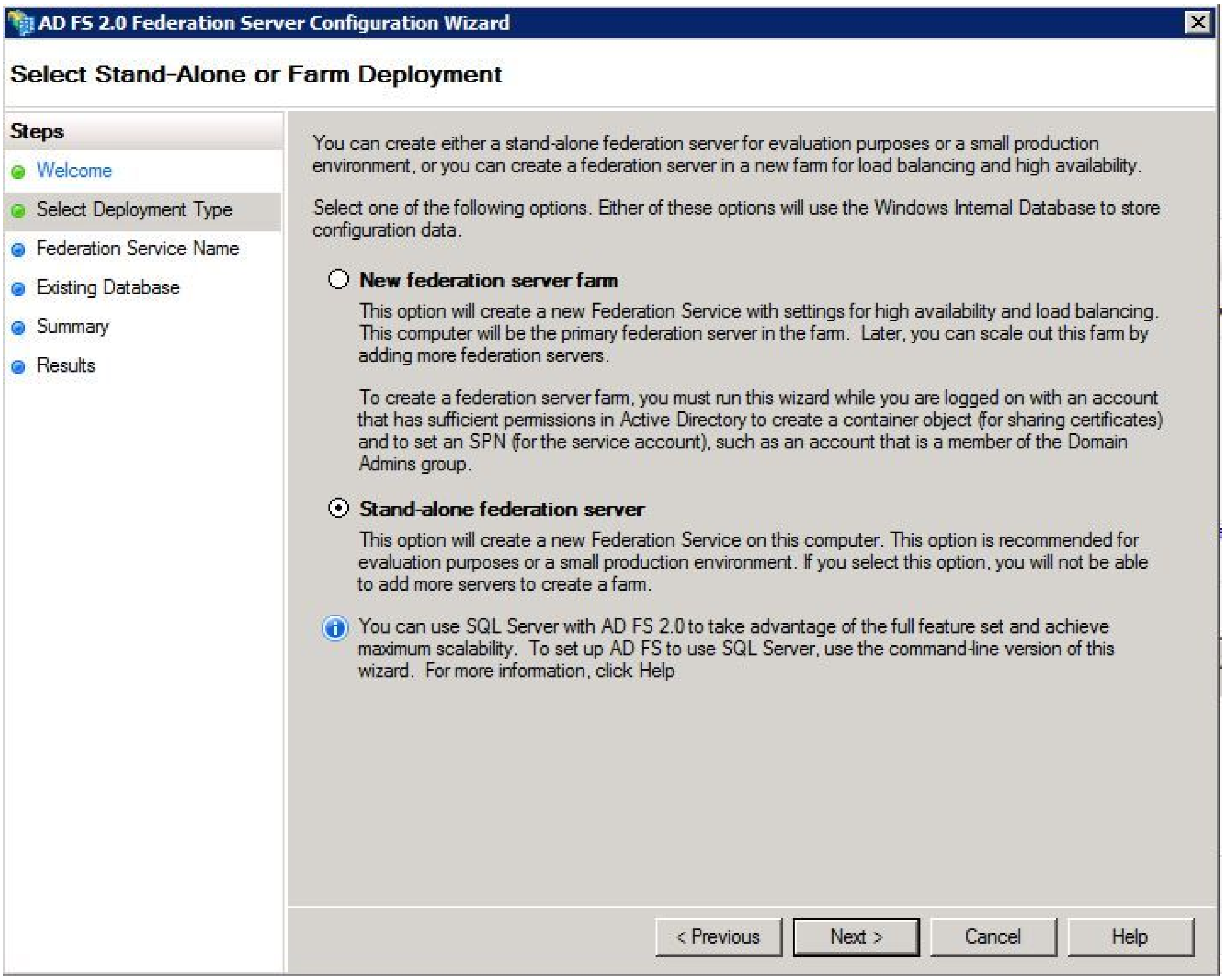
● Create a new Federation Service

Select this option to set up either a stand-alone federation server or the first server in a federation server farm.

○ Add a federation server to an existing Federation Service

Select this option to join this computer to an existing federation server farm.

第四步：对于大多数环境，独立联合服务器已足够。



AD FS 2.0 Federation Server Configuration Wizard

Select Stand-Alone or Farm Deployment

You can create either a stand-alone federation server for evaluation purposes or a small production environment, or you can create a federation server in a new farm for load balancing and high availability.

Select one of the following options. Either of these options will use the Windows Internal Database to store configuration data.

○ **New federation server farm**

This option will create a new Federation Service with settings for high availability and load balancing. This computer will be the primary federation server in the farm. Later, you can scale out this farm by adding more federation servers.

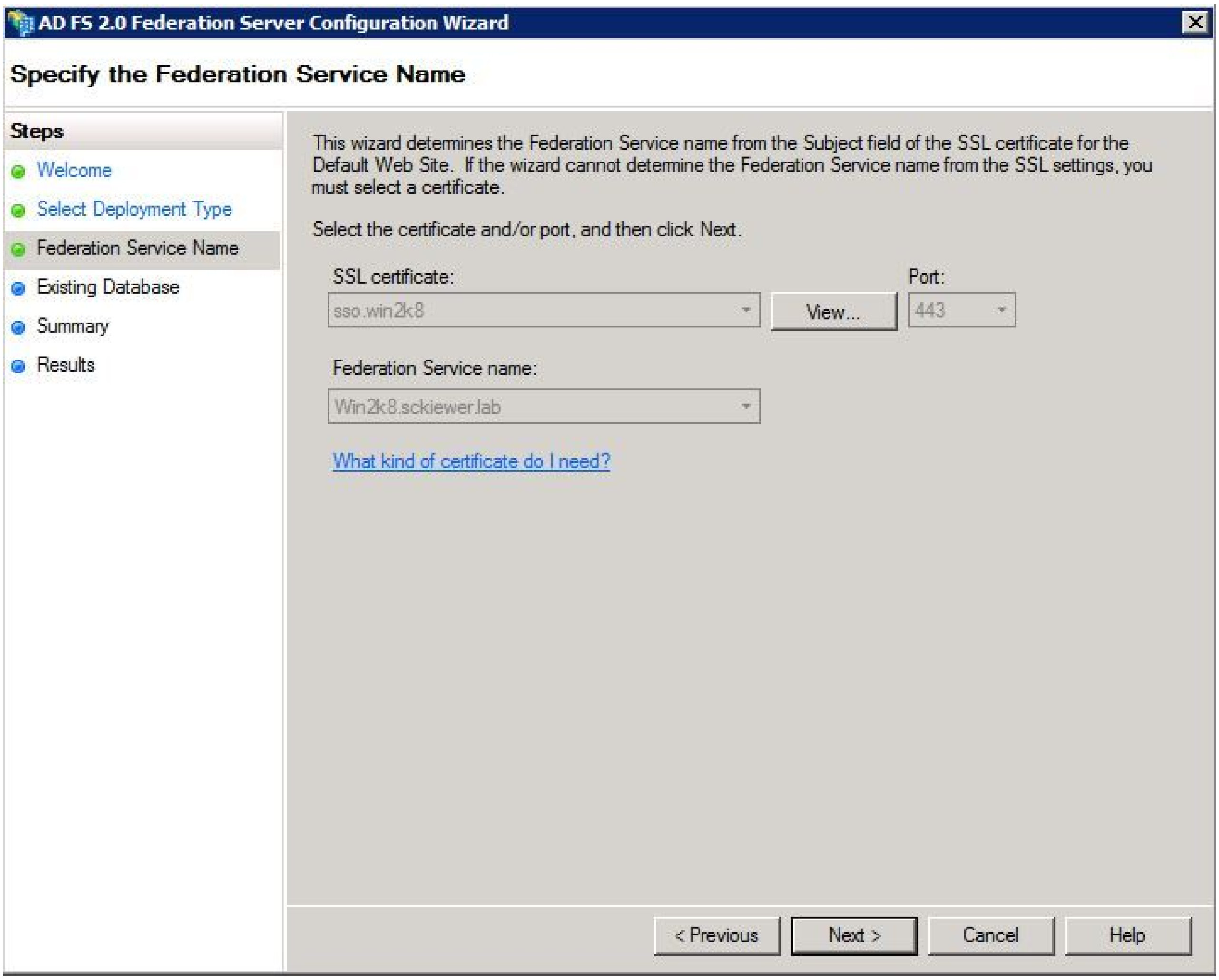
To create a federation server farm, you must run this wizard while you are logged on with an account that has sufficient permissions in Active Directory to create a container object (for sharing certificates) and to set an SPN (for the service account), such as an account that is a member of the Domain Admins group.

● **Stand-alone federation server**

This option will create a new Federation Service on this computer. This option is recommended for evaluation purposes or a small production environment. If you select this option, you will not be able to add more servers to create a farm.

You can use SQL Server with AD FS 2.0 to take advantage of the full feature set and achieve maximum scalability. To set up AD FS to use SQL Server, use the command-line version of this wizard. For more information, click Help

第五步：接下来，系统会要求您选择证书。只要服务器有证书，此字段就会自动填充。



AD FS 2.0 Federation Server Configuration Wizard

Specify the Federation Service Name

This wizard determines the Federation Service name from the Subject field of the SSL certificate for the Default Web Site. If the wizard cannot determine the Federation Service name from the SSL settings, you must select a certificate.

Select the certificate and/or port, and then click Next.

SSL certificate: sso.win2k8

Port: 443

Federation Service name: Win2k8.sckiewer.lab

What kind of certificate do I need?

第六步：如果服务器上已经有AD FS数据库，则需要将其删除才能继续。

步骤 7.最后，您将进入一个摘要屏幕，您可以在其中单击下一步。

将Idp元数据导入CUCM/下载CUCM元数据

步骤1:使用您的Windows服务器主机名/FQDN更新URL并从AD FS服务器下载元数据 — https://hostname/federationmetadata/2007-06/federationmetadata.xml

第二步：导航到Cisco Unified CM Administration > System > SAML Single Sign-On。

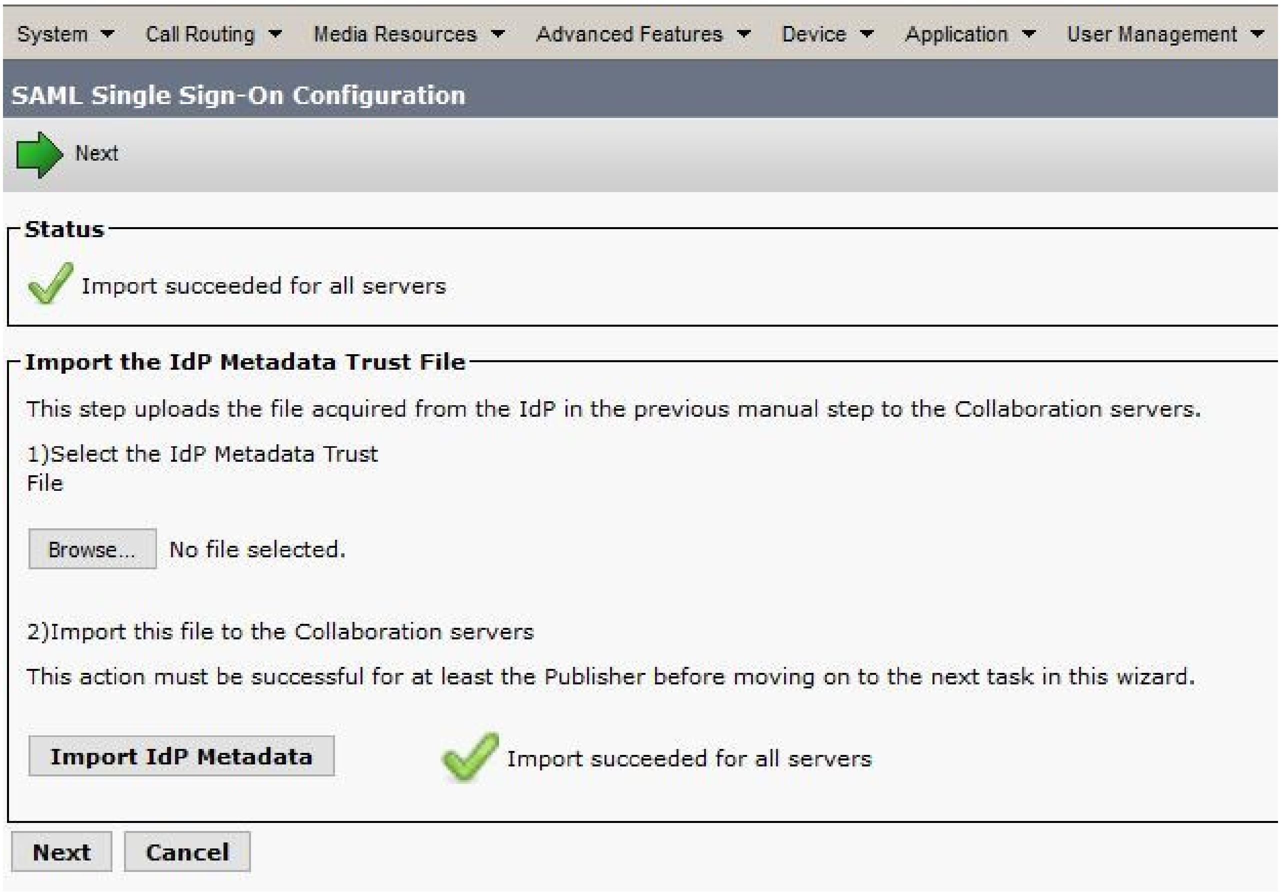
第三步：单击Enable SAML SSO。

第四步：如果收到有关Web服务器连接的警报，请单击Continue。

第五步：接下来，CUCM会指示您从IdP下载元数据文件。 在这种情况下，您的AD FS服务器是IdP，您在第1步中下载了元数据，因此单击下一步。

第六步：单击Browse > Select the .xml from Step 1 > 单击Import IdP Metadata。

步骤 7.消息表明导入成功：



SAML Single Sign-On Configuration

Status

✓ Import succeeded for all servers

Import the IdP Metadata Trust File

This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.

1)Select the IdP Metadata Trust File

No file selected.

2)Import this file to the Collaboration servers

This action must be successful for at least the Publisher before moving on to the next task in this wizard.

✓ Import succeeded for all servers

步骤 8单击 Next。

步骤 9现在您已将IdP元数据导入CUCM，您需要将CUCM的元数据导入IdP。

步骤 10单击下载信任元数据文件。

步骤 11单击 Next。

步骤 12将.zip文件移动到Windows Server并将内容解压到文件夹中。

将CUCM元数据导入AD FS 2.0服务器并创建声明规则

步骤1:单击Start并搜索AD FS 2.0 Management。

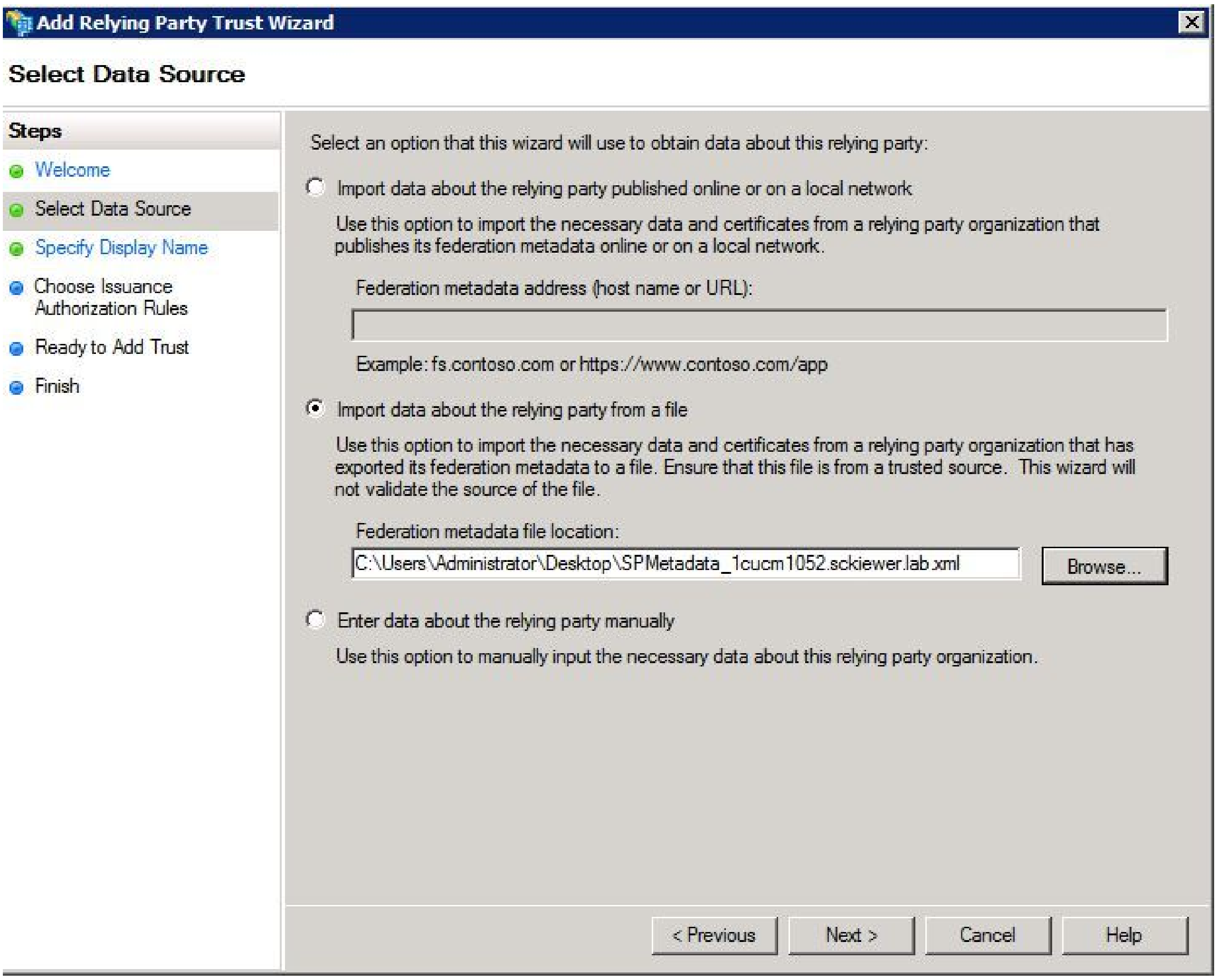
第二步：单击Required: Add a trusted relying party。

注：如果未看到此选项，您需要关闭窗口并重新打开它。

第三步：打开Add Relisting Party Trust Wizard后，单击Start。

第四步：在此，您需要导入在步骤12中提取的XML文件。选择Import data about the relying party from a file，浏览到文件夹文件，然后为发布者选择XML。

注意：对于要在其上使用SSO的任何Unified Collaboration服务器，请使用上述步骤。



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_1cucm1052.sckiewer.lab.xml

○ Enter data about the relying party manually

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

第五步：单击 Next。

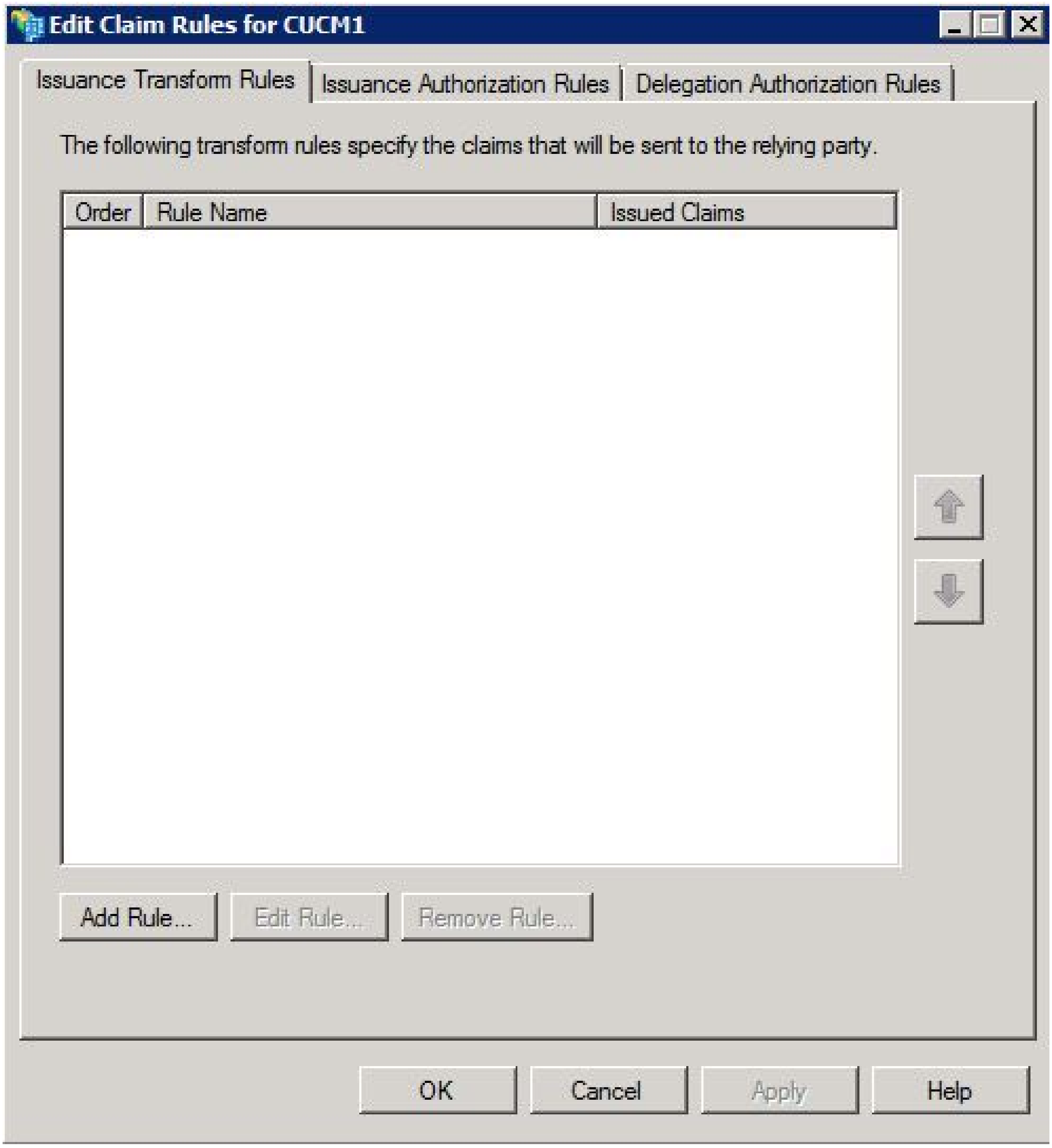
第六步：编辑显示名称，然后单击下一步。

步骤 7.选择Permit all users to access this relying party，然后单击Next。

步骤 8再次单击Next。

步骤 9在此屏幕上，请确保选中Open the Edit Claim Rules dialog for this relying party trust when the wizard closes，然后单击Close。

步骤 10“编辑领款申请规则”(Edit Claim Rules)窗口打开：



Edit Claim Rules for CUCM1
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

步骤 11在此窗口中，单击Add Rule。

步骤 12对于Claim rule template，选择Send LDAP Attributes as Claims，然后单击Next。

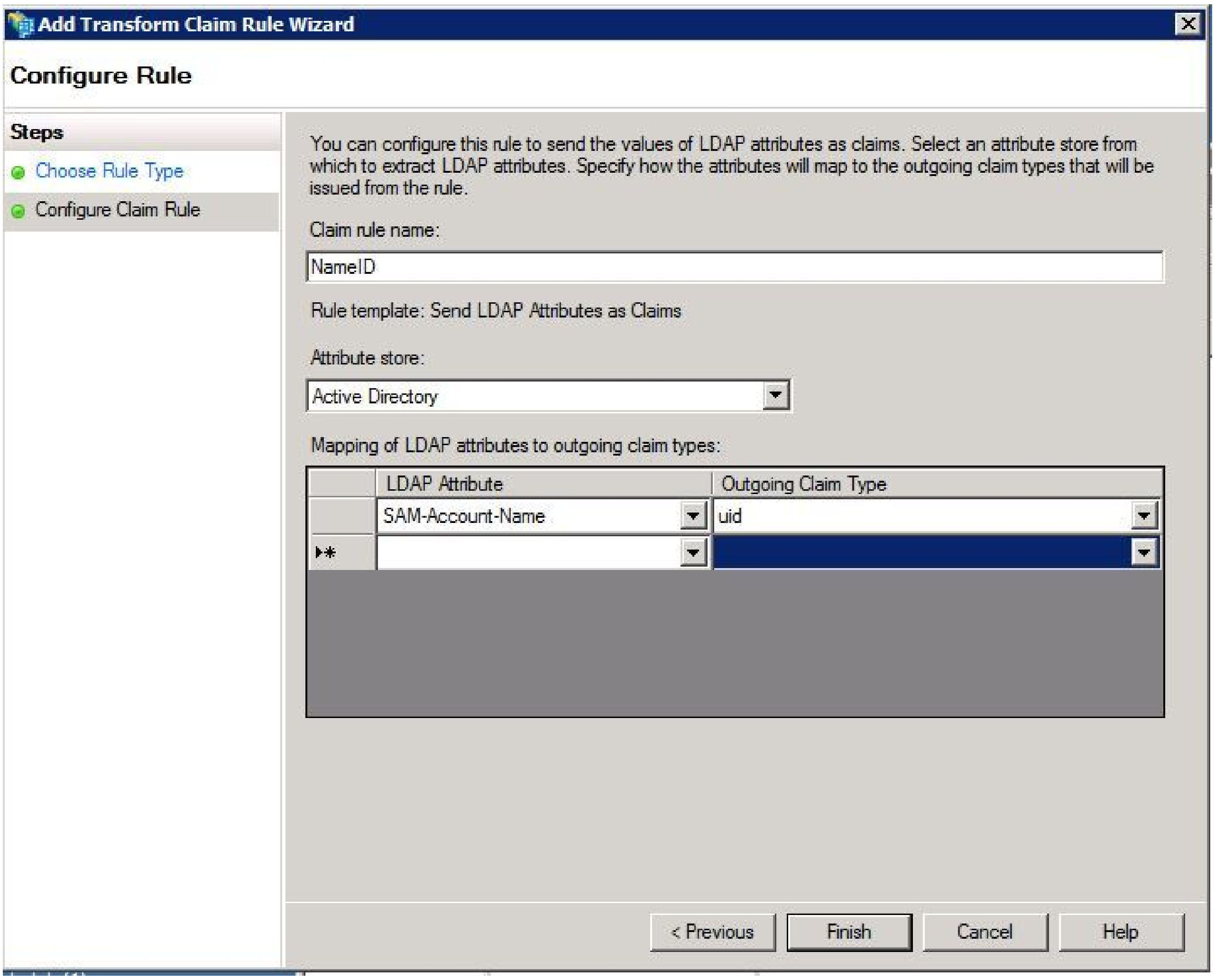
步骤 13在下一页上，输入NameID作为领款申请规则名称。

步骤 14选择Attribute store的Active Directory。

步骤 15为LDAP Attribute选择SAM-Account-Name。

步骤 16为传出声明类型输入uid。

注:uid不是下拉列表中的选项 — 必须手动输入。



Configure Rule

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:

NameID

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
▸*		

步骤 17单击 完成。

步骤 18.第一条 规则现已完成。再次单击Add Rule。

步骤 19.选择Send Claims Using a Custom Rule。

步骤 20.输入领款申请规则名称。

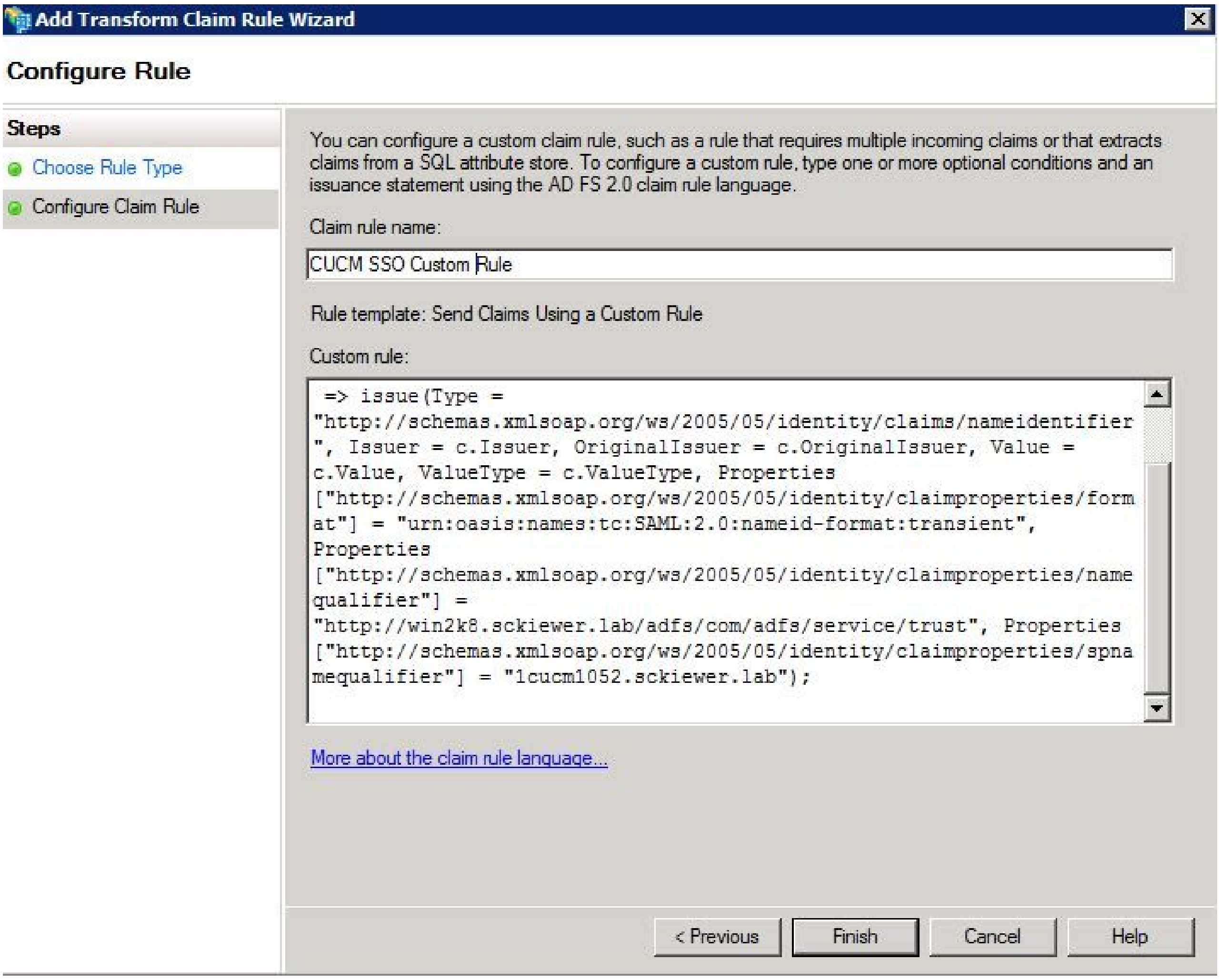
步骤 21.在Custom rule字段中，粘贴以下文本：

c:[键入== "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] =>问题(类型= "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/claimperties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient"，属性 ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimperties/namequalifier"] = "http://ADFS_FEDERATION_SERVICE_NAME/com/adfs/service/trust"，属性 ["http://schemas.xmlsoap.org/ws/2005/05/标识/属性/名称限定符"] = "CUCM_ENTITY_ID");

步骤 22.确保将AD_FS_SERVICE_NAME和CUCM_ENTITY_ID更改为相应的值。

注：如果您不确定AD FS服务名称，可以按照步骤进行查找。 CUCM实体ID可以从CUCM元

数据文件中的第一行提取。 文件第一行有一个entityID，如下所示，entityID=1cucm1052.sckiewer.lab。您需要在索赔规则的相应部分输入带下划线的值。



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:

CUCM SSO Custom Rule

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://win2k8.sckiewer.lab/adfs/com/adfs/service/trust", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spna
mequalifier"] = "1cucm1052.sckiewer.lab");
```

More about the claim rule language...

步骤 23.单击 完成。

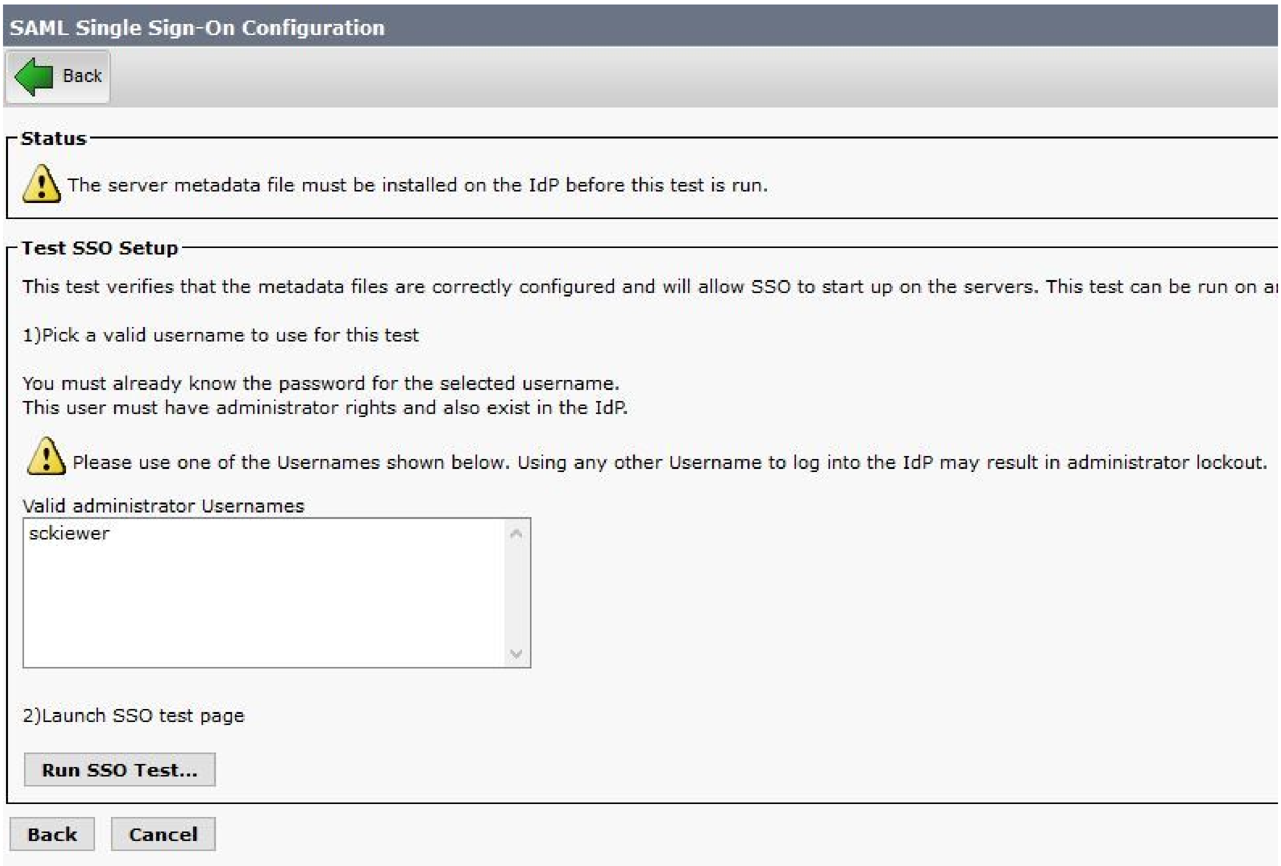
步骤 24Click OK.

注意：对于要在其上使用SSO的任何Unified Collaboration服务器，都需要声明规则。

完成CUCM上的SSO启用并运行SSO测试

步骤1:现在，AD FS服务器已完全配置，您可以返回到CUCM。

第二步：您在最终配置页面上关闭：



SAML Single Sign-On Configuration

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 a

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.

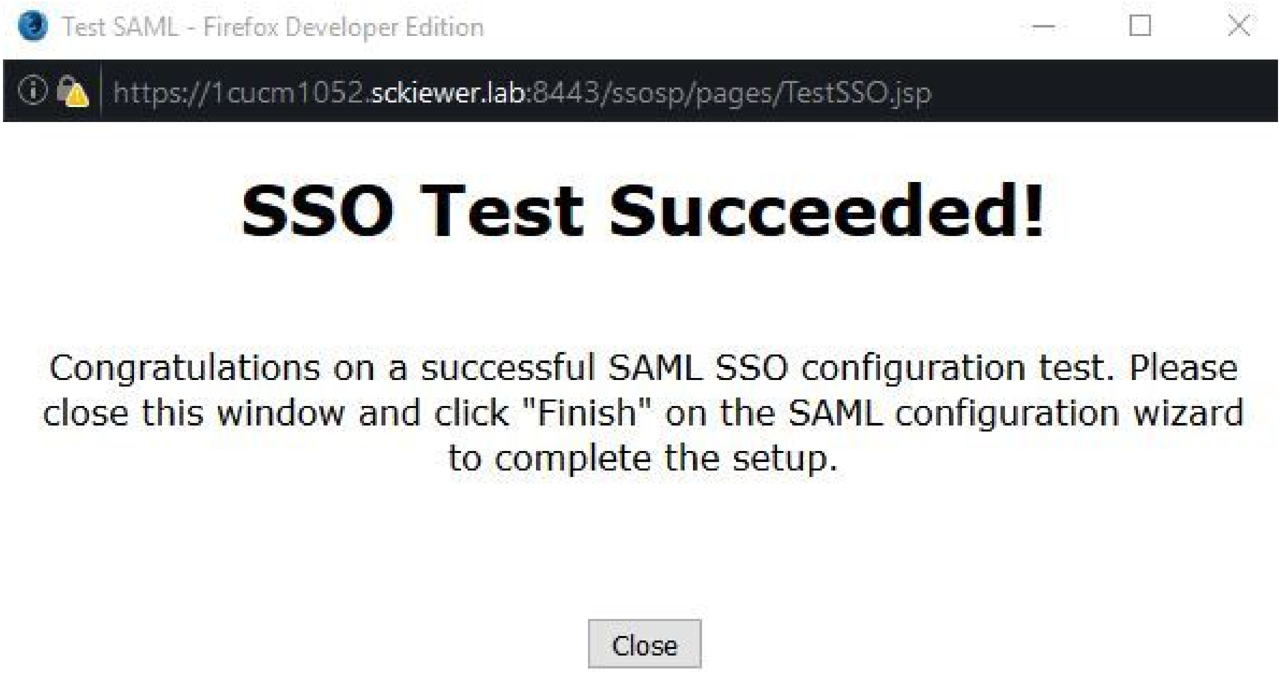
Valid administrator Usernames

sckiewer

2)Launch SSO test page

第三步：选择已选择标准CCM超级用户角色的最终用户，然后单击运行SSO测试……

第四步： 确保您的浏览器允许弹出窗口，并在提示符中输入您的凭证。



Test SAML - Firefox Developer Edition

https://1cucm1052.sckiewer.lab:8443/ssosp/pages/TestSSO.jsp

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.

第五步：在弹出窗口中单击Close，然后单击Finish。

第六步：在短暂重新启动Web应用程序后，SSO已启用。

故障排除

将SSO日志设置为调试

要将SSO日志设置为调试，您必须在CUCM的CLI中运行此命令：set samltrace level debug

可以从RTMT下载SSO日志。日志集的名称为Cisco SSO。

查找联合身份验证服务名称

要查找联合身份验证服务名称，请单击Start并搜索AD FS 2.0 Management。

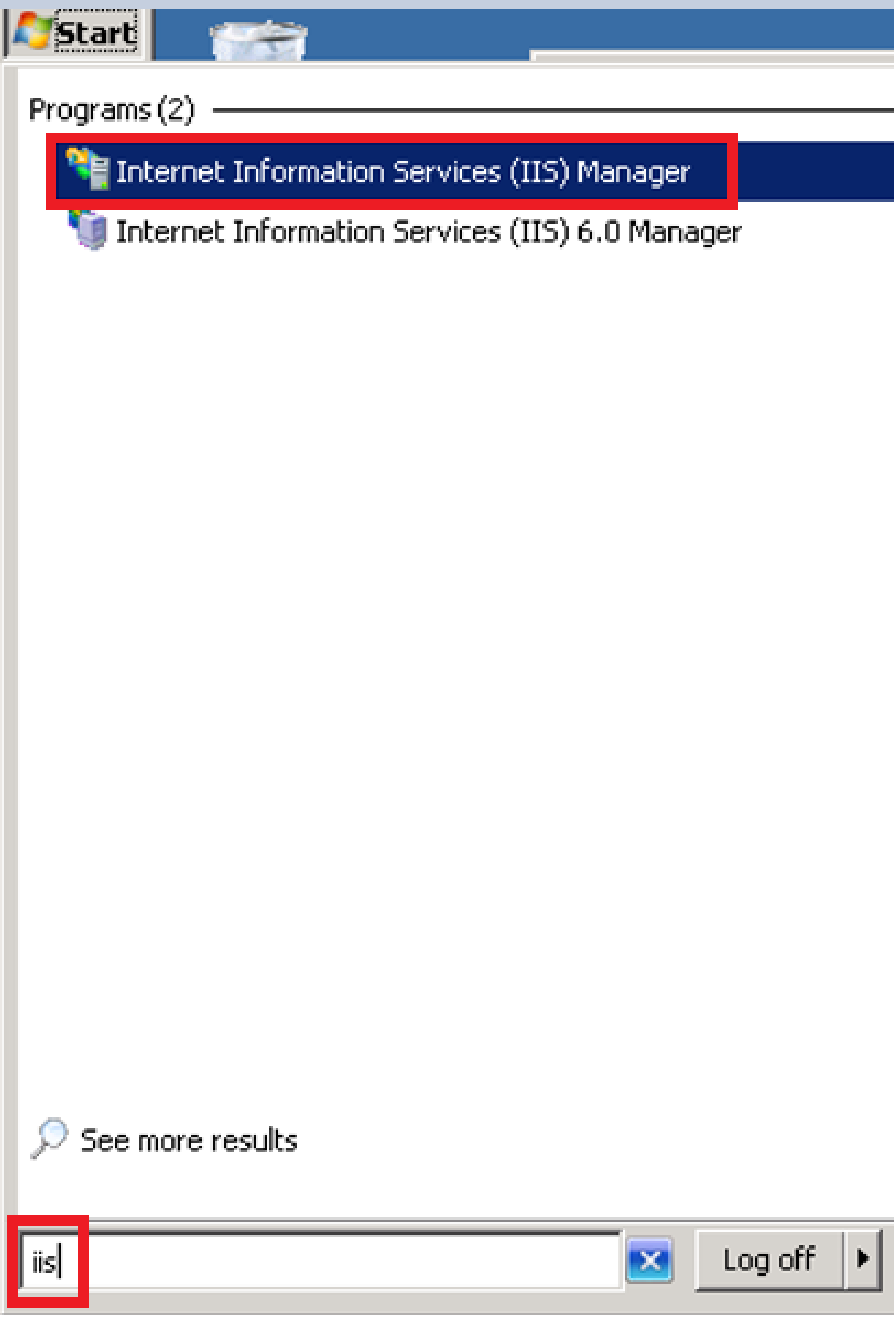
·点击Edit Federation Service Properties...
·在“常规”选项卡上，查找联合身份验证服务名称

无点证书和联合身份验证服务名称

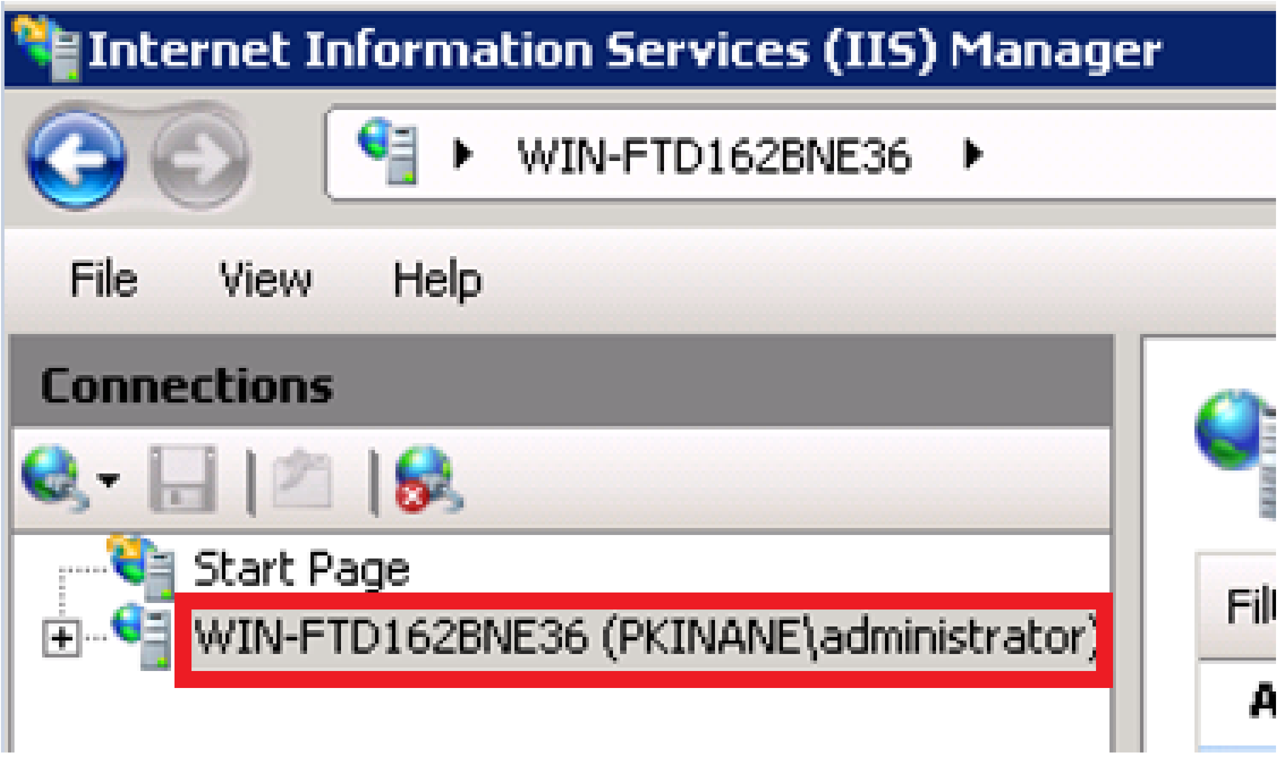
如果在AD FS配置向导中收到此错误消息，则需要创建新证书。

所选证书不能用于确定联合身份验证服务名称，因为所选证书具有无点（短名称）使用者名称。请选择另一个没有无点（短名称）使用者名称的证书，然后重试。

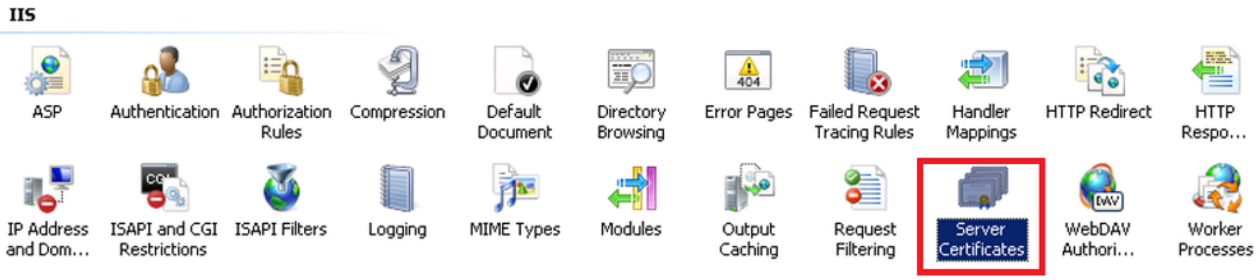
步骤1:单击开始并搜索iis，然后打开Internet信息服务(IIS)管理器


Start
Programs (2)
Internet Information Services (IIS) Manager
Internet Information Services (IIS) 6.0 Manager
See more results
iis
Log off

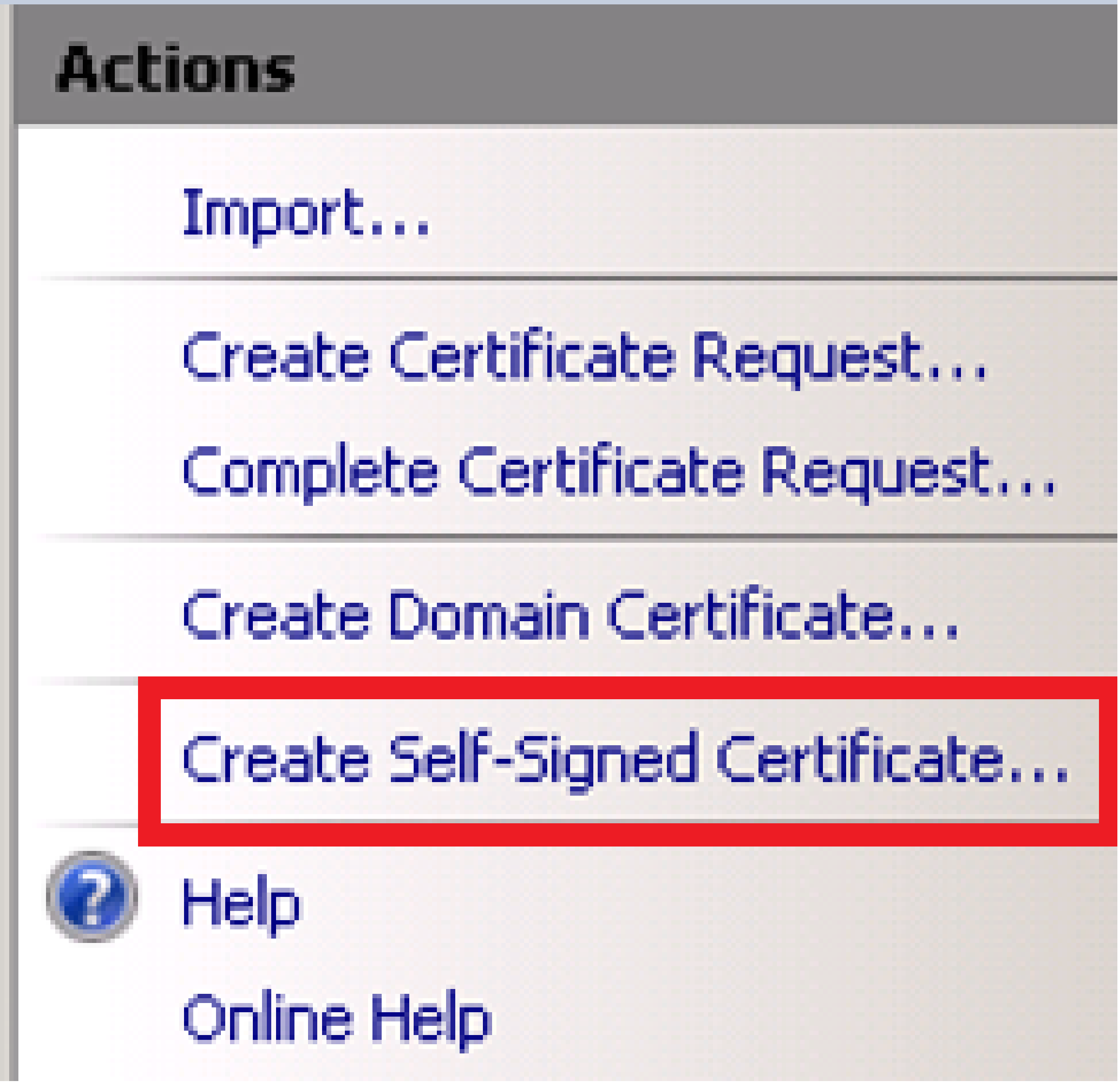
第二步：单击服务器的名称。


Internet Information Services (IIS) Manager
WIN-FTD162BNE36
File
View
Help
Connections
Start Page
WIN-FTD162BNE36 (PKINANE\administrator)

第三步：点击Server Certificates。

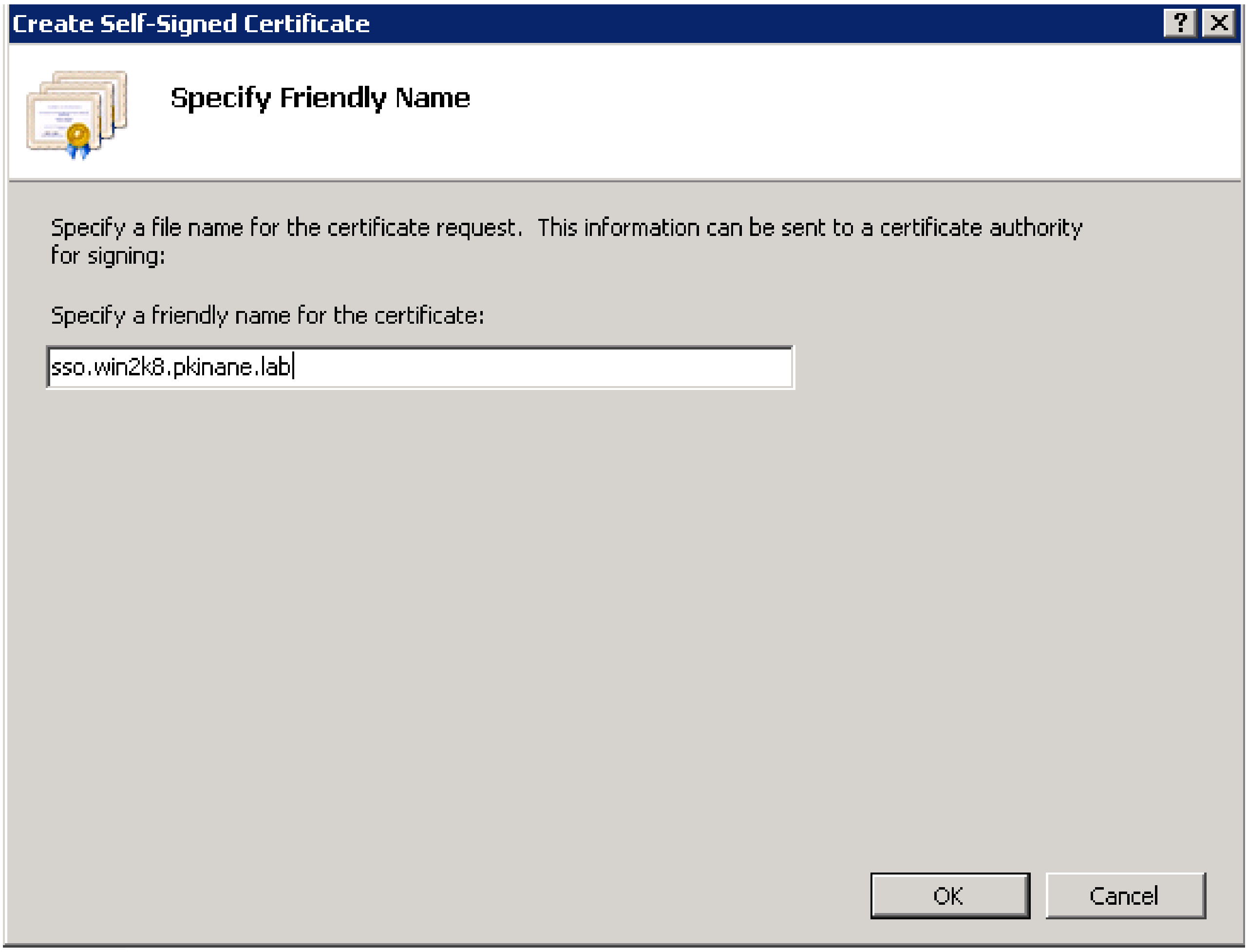


第四步：点击Create Self-Signed Certificate。



Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Help
Online Help

第五步：输入证书别名的名称。



Create Self-Signed Certificate

Specify Friendly Name

Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

Specify a friendly name for the certificate:

sso.win2k8.pkinane.lab

CUCM和IDP服务器之间的时间不同步

如果在从CUCM运行SSO测试时收到此错误，则需要将Windows Server配置为使用与CUCM相同的NTP服务器。

无效的SAML响应。当Cisco Unified Communications Manager和IDP服务器之间的时间不同步时，可能会出现这种情况。请验证两台服务器上的NTP配置。从CLI运行“utils ntp status”以检查Cisco Unified Communications Manager上的此状态。

在Windows Server指定了正确的NTP服务器后，您需要执行另一个SSO测试并查看问题是否仍然存在。 在某些情况下，有必要歪曲声明的有效期。 有关这一过程的更多详细信息。

相关信息

- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。