Configure Single Sign-On with CUCM and AD FS 2.0

Contents

Introduction

This document describes how to configure Single Sign-On (SSO) on Cisco Unified Communications Manager and Active Directory Federation Service.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Communications Manager (CUCM)
- Basic Knowledge of Active Directory Federation Service (AD FS)

In order to enable SSO in your lab environment, you need this configuration:

- Windows Server with AD FS installed.
- CUCM with LDAP sync configured.
- An End User with the Standard CCM Super Users role selected.

Components Used

The information in this document is based on these software and hardware versions:

- Windows Server with AD FS 2.0
- CUCM 10.5.2

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, ensure that you understand the potential impact of any command.

Background Information

The procedure for AD FS 2.0 with Windows Server 2008 R2 is provided. These steps also work for AD FS 3.0 on Windows Server 2016.

Download and Install AD FS 2.0 on your Windows Server

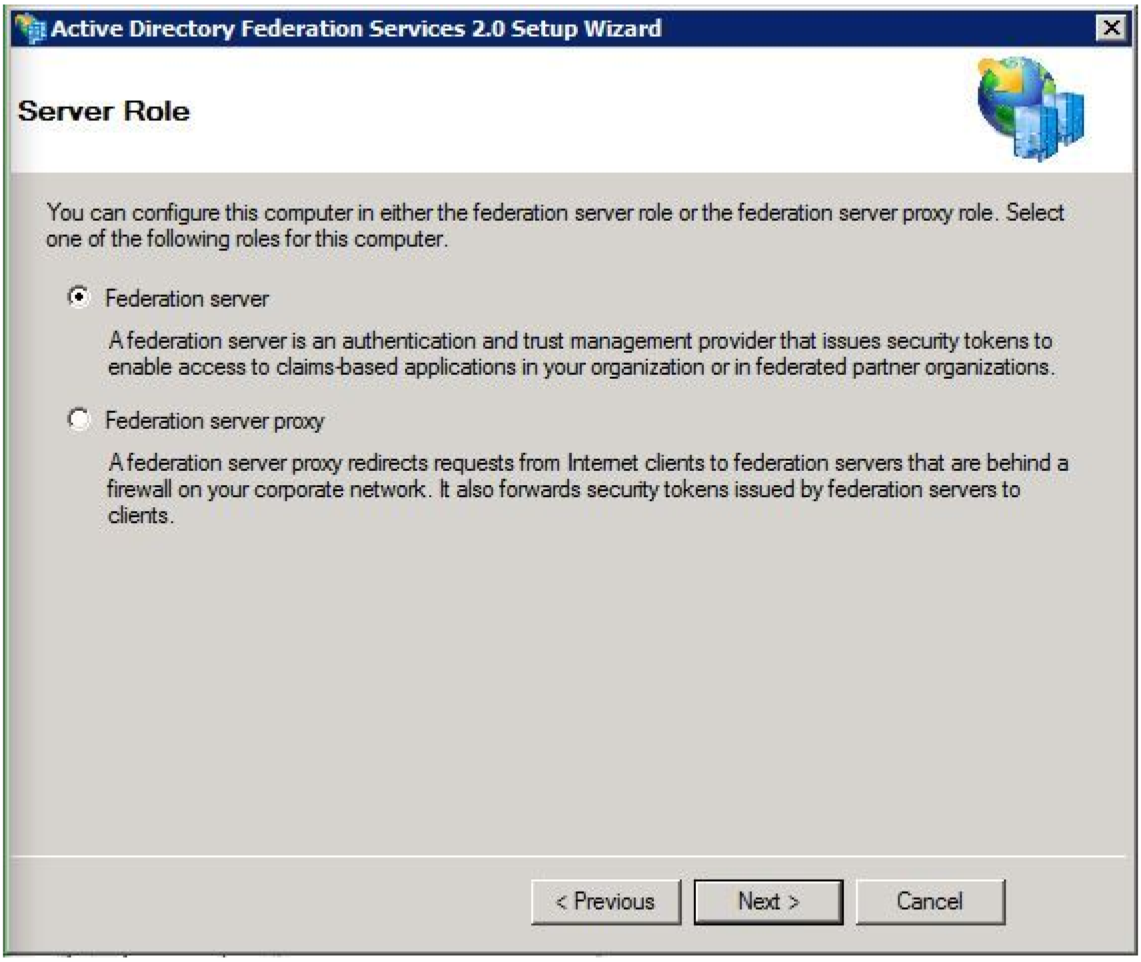
Step 1. Navigate to Download AD FS 2.0.

Step 2. Ensure that you select the appropriate download based on your Windows Server.

Step 3. **Move** the downloaded file to your Windows Server.

Step 4. Proceed with the installation:

Step 5. When prompted, choose **Federation Server**:



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.

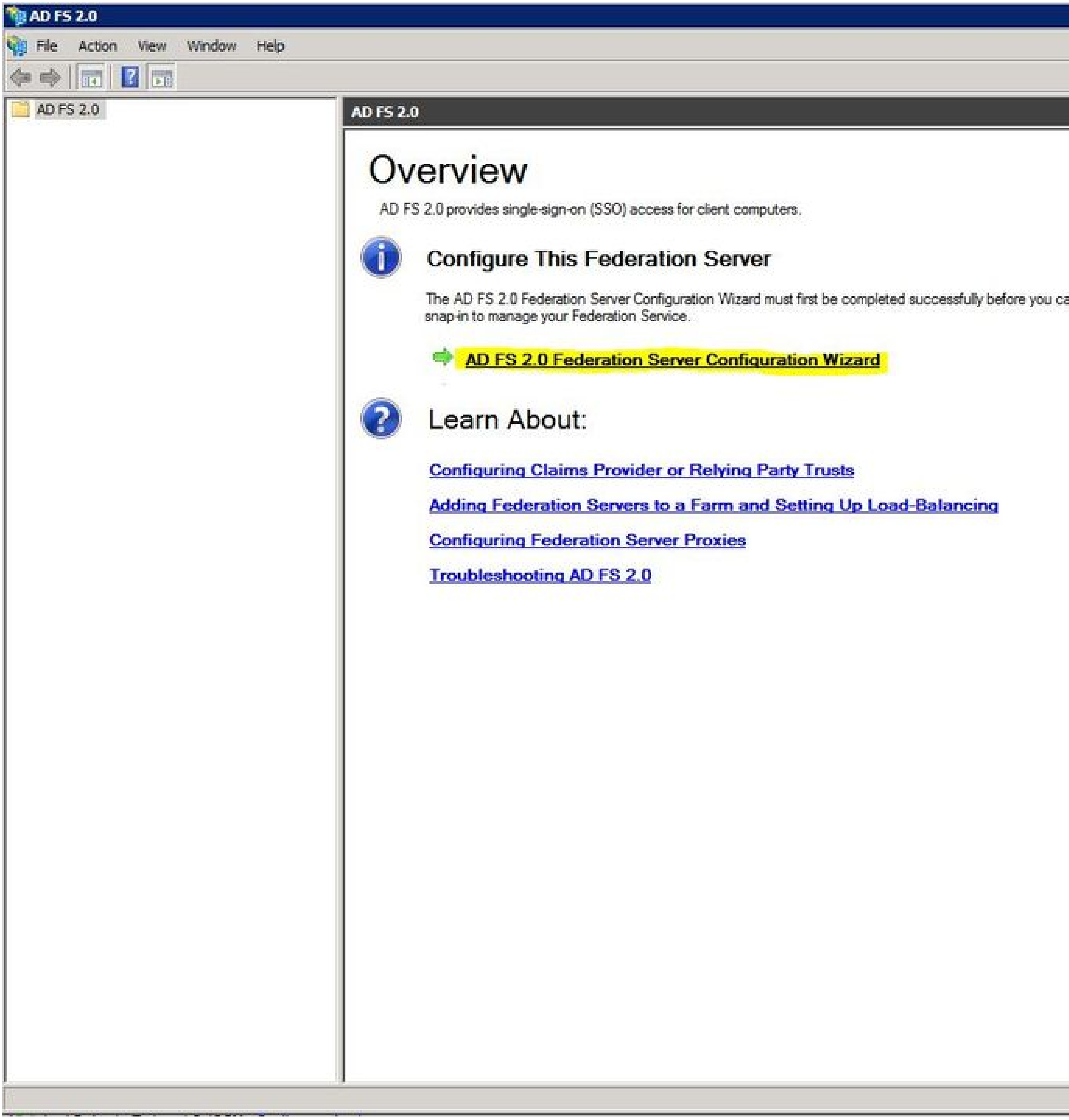
Step 6. Some dependencies are automatically installed - once that is done, click **Finish**.

Now that you have AD FS 2.0 installed on your server, you need to add some configuration.

Configure AD FS 2.0 on Your Windows Server

Step 1. If the AD FS 2.0 window did not automatically open after the install, you can click **Start** and search for AD FS 2.0 Management to open it manually.

Step 2. Choose **AD FS 2.0 Federation Server Configuration Wizard**.



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 ca snap-in to manage your Federation Service.

AD FS 2.0 Federation Server Configuration Wizard

Learn About:

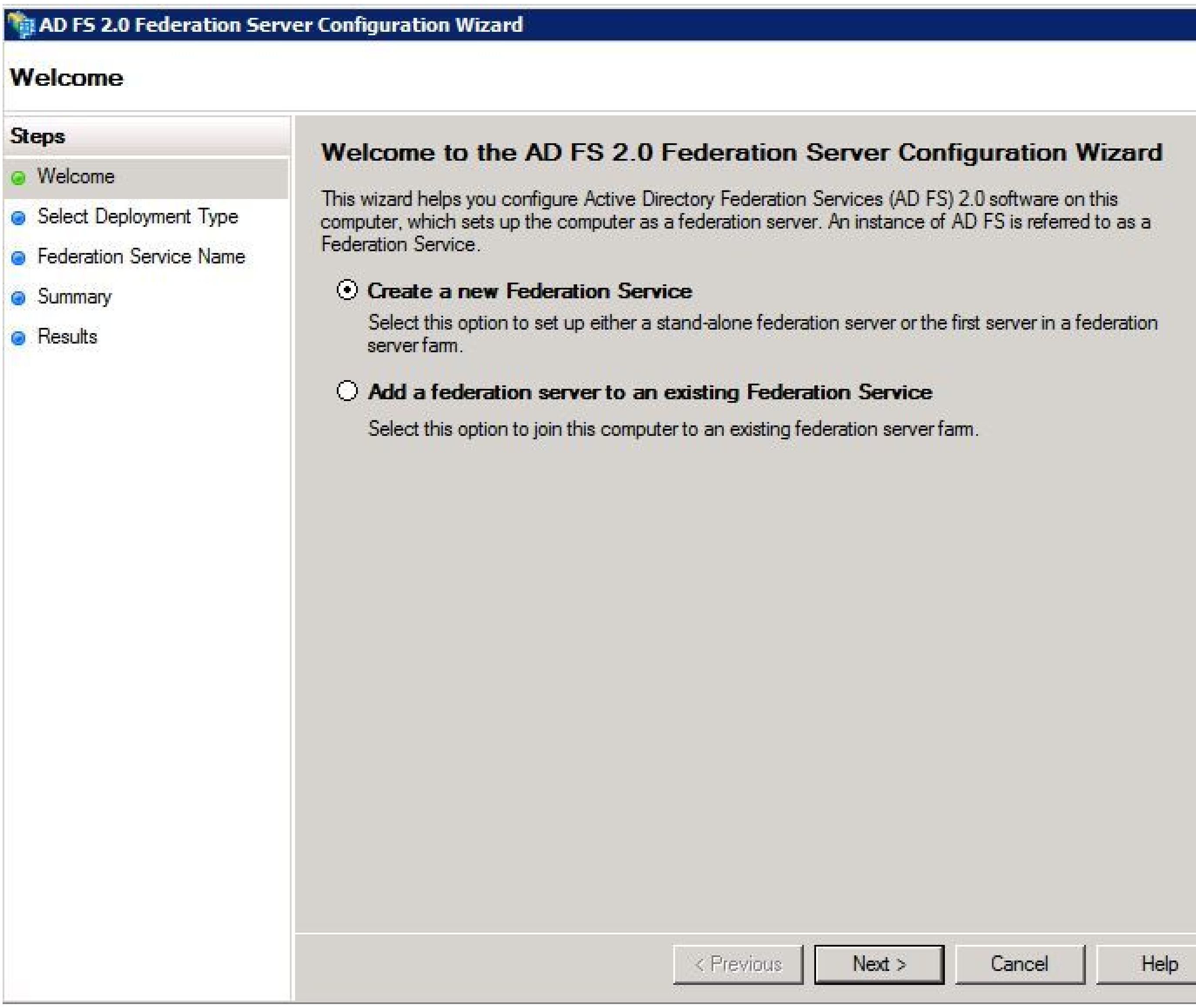
Configuring Claims Provider or Relying Party Trusts

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

Configuring Federation Server Proxies

Troubleshooting AD FS 2.0

Step 3. Next, click **Create a new Federation Service**.



AD FS 2.0 Federation Server Configuration Wizard

Welcome

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.

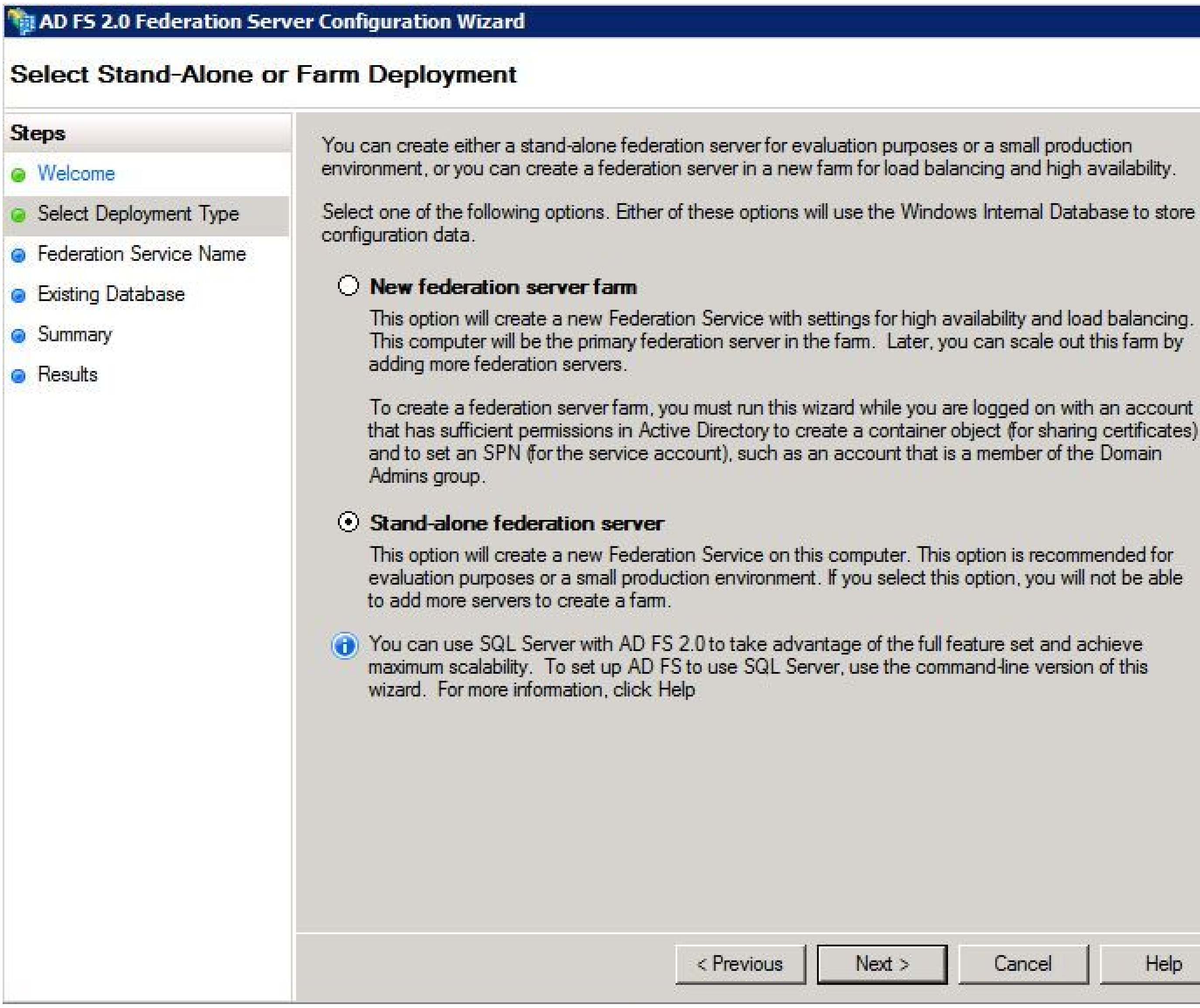
● Create a new Federation Service

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.

Step 4. For most environments, **Stand-alone federation server** is sufficient.



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.

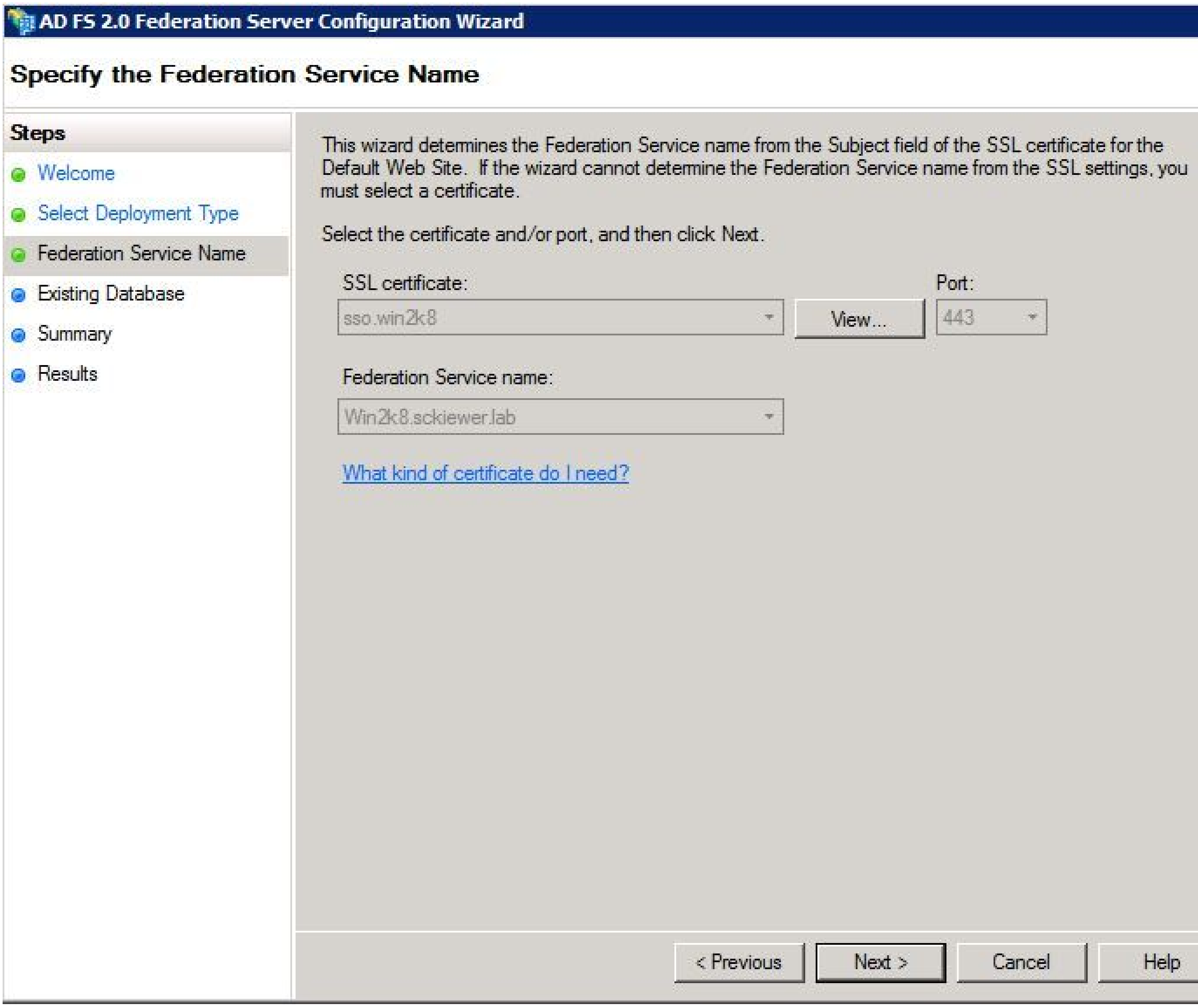
To create a federation server farm, you must run this wizard while you are logged on with an account that has sufficient permissions in Active Directory to create a container object (for sharing certificates) and to set an SPN (for the service account), such as an account that is a member of the Domain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

Step 5. Next, you are asked to choose a certificate. This field auto-populates as long as the server has a certificate.



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

Step 6. If you already have an AD FS database on the server, you need to remove it to continue.

Step 7. Finally, you are on a summary screen where you can click **Next**.

Import the Idp Metadata to CUCM / Download the CUCM Metadata

Step 1. Update the URL with your Windows server hostname/FQDN and download the metadata from your AD FS server - https://hostname/federationmetadata/2007-06/federationmetadata.xml

Step 2. Navigate to **Cisco Unified CM Administration** > **System** > **SAML Single Sign-On**.

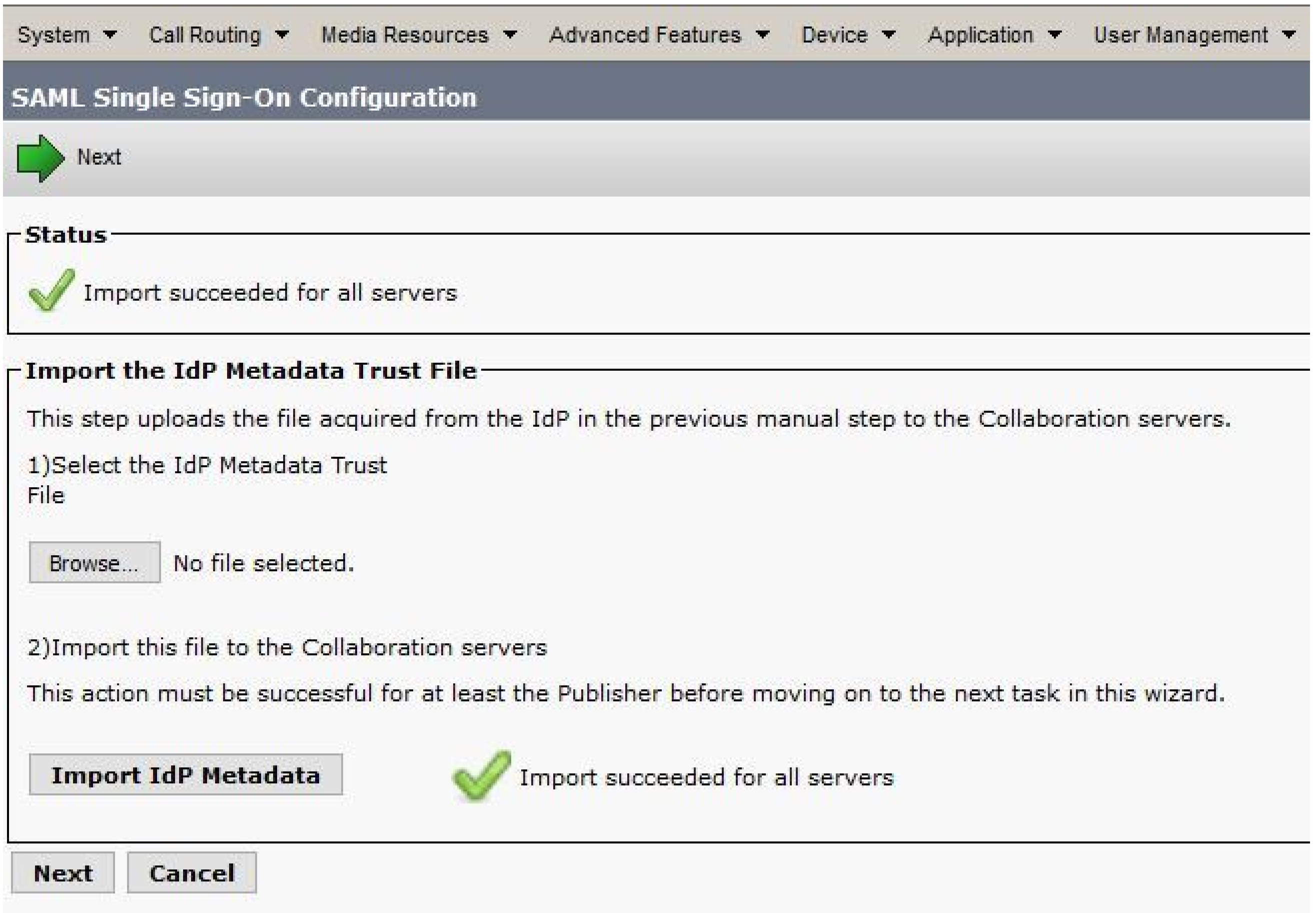
Step 3. Click **Enable SAML SSO**.

Step 4. If you receive an alert about Web Server Connections, click **Continue**.

Step 5. Next, CUCM instructs you to download the metadata file from your IdP. In this scenario, your AD FS server is the IdP, and you downloaded the metadata in Step 1, so click **Next**.

Step 6. Click **Browse** > **Select the .xml from Step 1** > Click **Import IdP Metadata**.

Step 7. A message indicates that the import was successful:



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

Step 8. Click **Next**.

Step 9. Now that you have the IdP metadata imported into CUCM, you need to import CUCM's metadata into your IdP.

Step 10. Click **Download Trust Metadata File**.

Step 11. Click **Next**.

Step 12. Move the .zip fileto your Windows Server and extract the contents to a folder.

Import CUCM Metatdata to AD FS 2.0 Server and Create Claim Rules

Step 1. Click **Start** and search for **AD FS 2.0 Management**.

Step 2. Click **Required: Add a trusted relying party**.

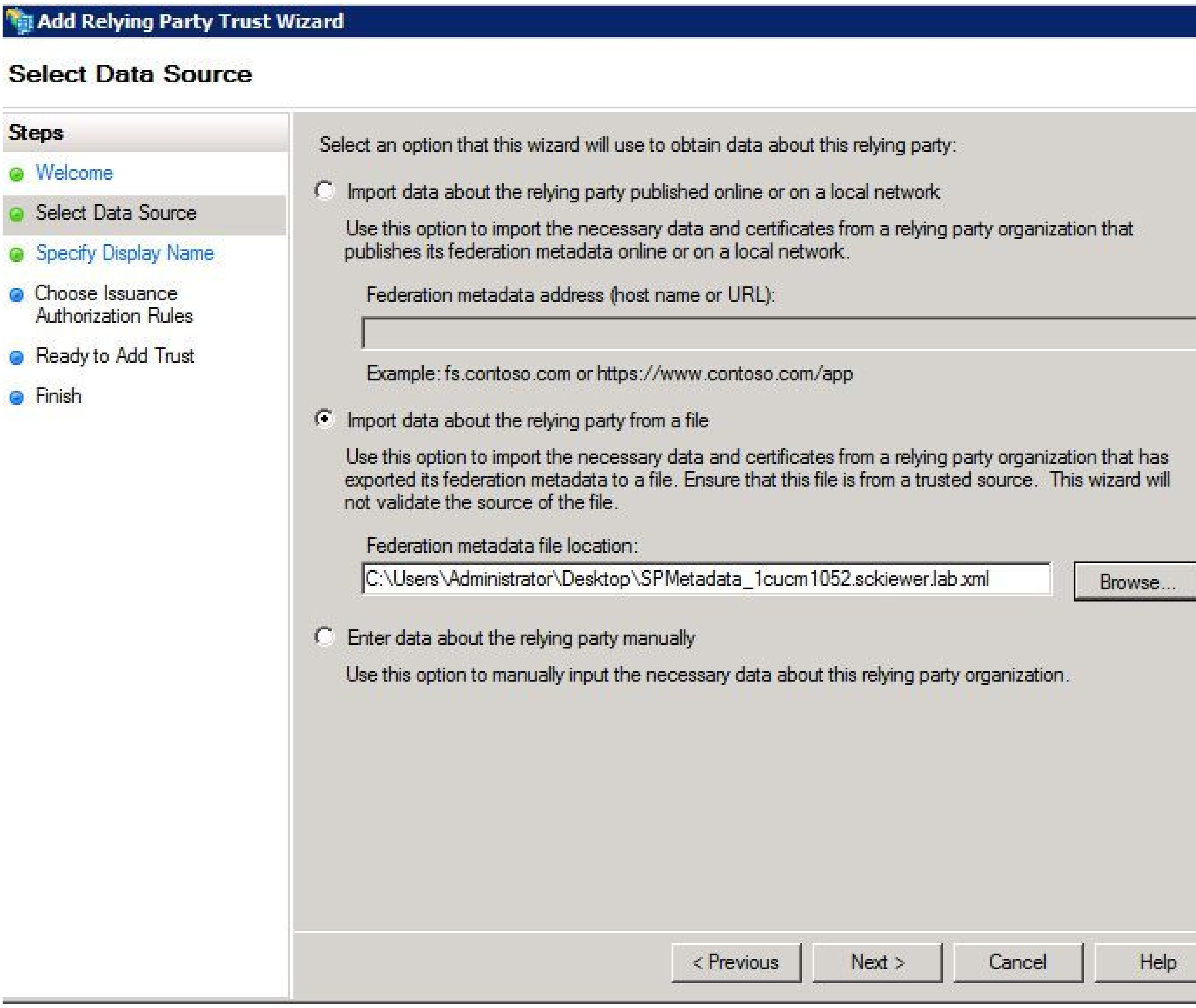
Note: If you do not see this option, you need to close the window and open it back up.

Step 3. Once you have the **Add Relying Party Trust Wizard** open, click **Start**.

Step 4. Here, you need to import the XML files that you extracted in step 12. Select **Import data**

about the relying party from a file and browse to the folder files and choose the XML for your publisher.

Note: Use the previous steps for any Unified Collaboration server on which you intend to utilize SSO.



Add Relying Party Trust Wizard

Select Data Source

Steps
- Welcome
- Select Data Source
- Specify Display Name
- 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_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.

Step 5. Click **Next**.

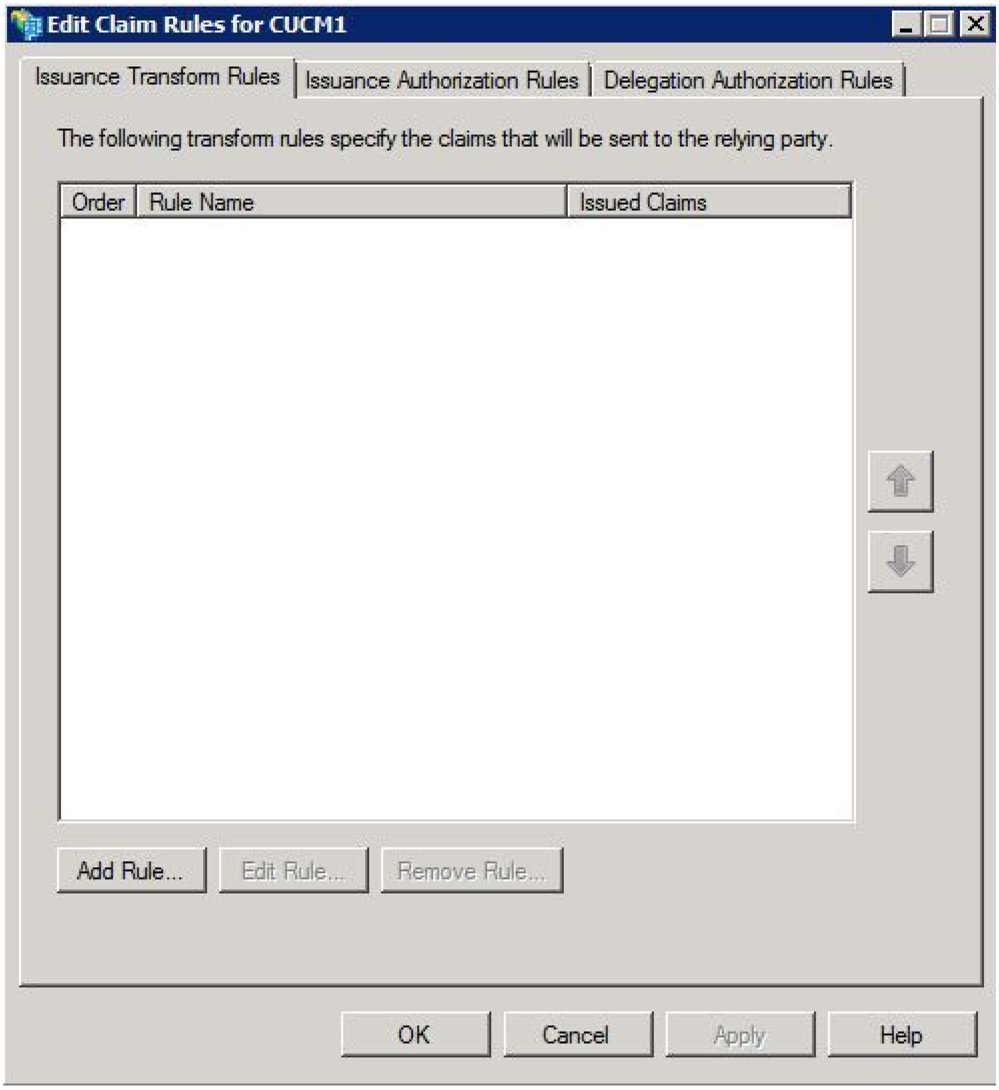
Step 6. Edit the **Display Name** and click **Next**.

Step 7. Choose **Permit all users to access this relying party** and click **Next**.

Step 8. Click **Next** again.

Step 9. On this screen, ensure that you have **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** checked, then click **Close**.

Step 10. The Edit Claim Rules window opens:



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

Step 11. In this window, click **Add Rule**.

Step 12. For **Claim rule template**, choose **Send LDAP Attributes as Claims** and click **Next**.

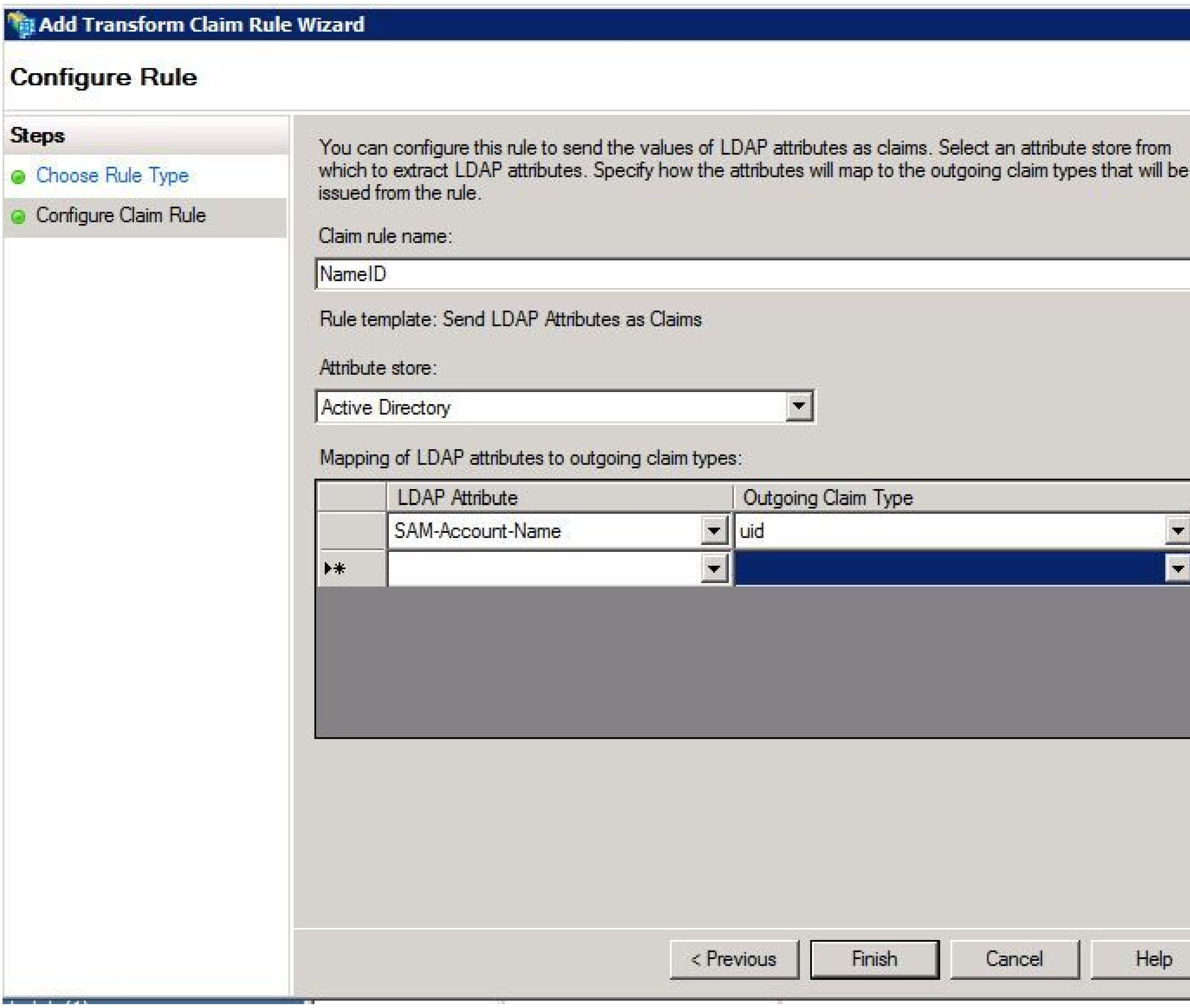
Step 13. On the next page, enter **NameID** for the **Claim rule name**.

Step 14. Choose **Active Directory** for the **Attribute store**.

Step 15. Choose **SAM-Account-Name** for the **LDAP Attribute**.

Step 16. Enter **uid** for **Outgoing Claim Type**.

Note: uid is not an option in the drop down list - it must be entered manually.



Add Transform Claim Rule Wizard

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
▸*		

Step 17. Click **Finish**.

Step 18. The first rule is now finished. Click **Add Rule** again.

Step 19. Choose **Send Claims Using a Custom Rule**.

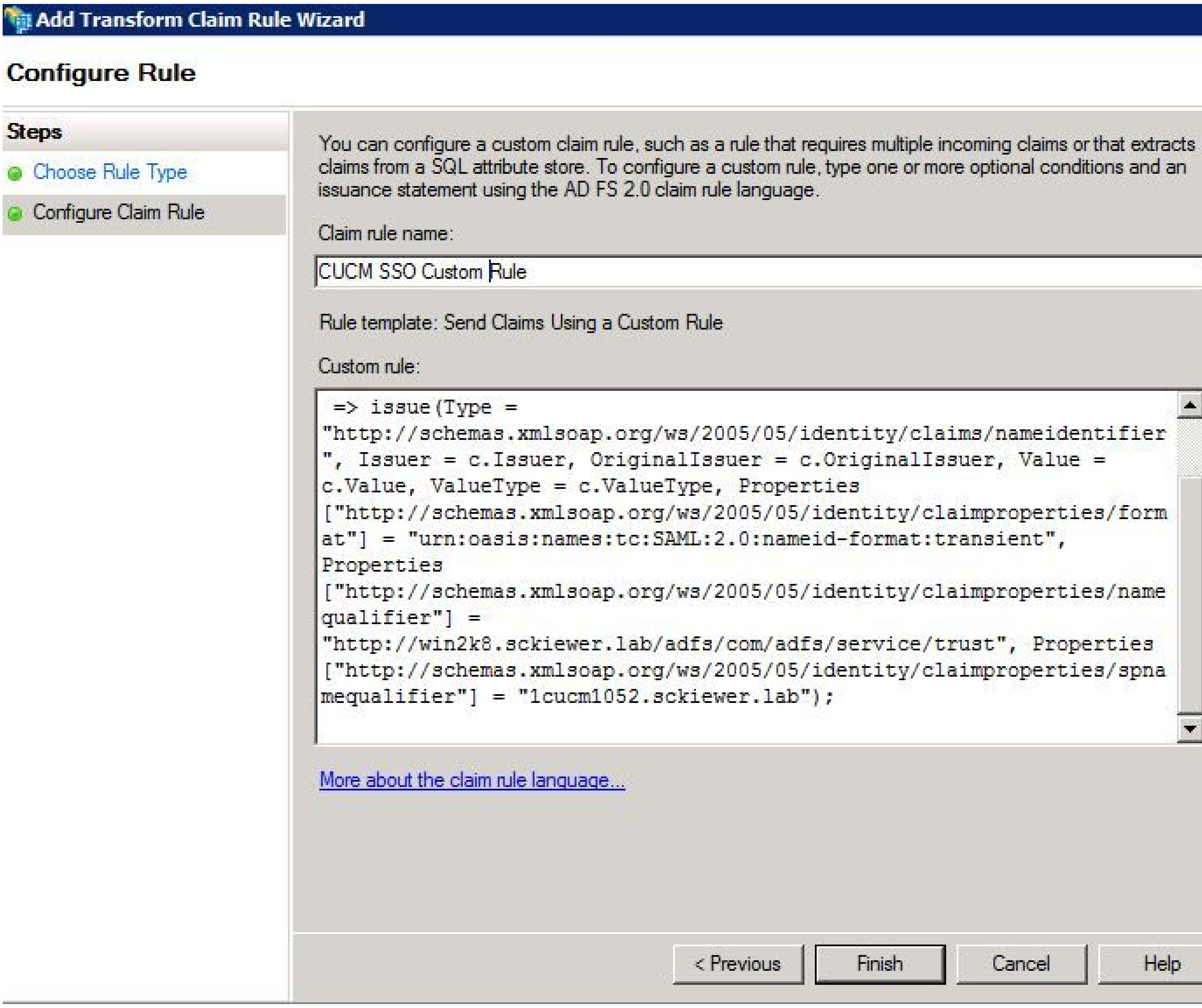
Step 20. Enter a **Claim rule name**.

Step 21. In the **Custom rule** field, paste this text:

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://ADFS_FEDERATION_SERVICE_NAME/com/adfs/service/trust", Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "CUCM_ENTITY_ID");

Step 22. Ensure that you change AD_FS_SERVICE_NAME and CUCM_ENTITY_ID to the appropriate values.

Note: If you are not sure about the AD FS Service Name, you can follow the steps to find it. The CUCM Entity ID can be pulled from first line in the CUCM metadata file. There is an entityID on the first line of the file that looks like this, entityID=1cucm1052.sckiewer.lab,. You need to enter the underlined value into the appropriate section of the claim rule.



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...

Step 23. Click **Finish**.

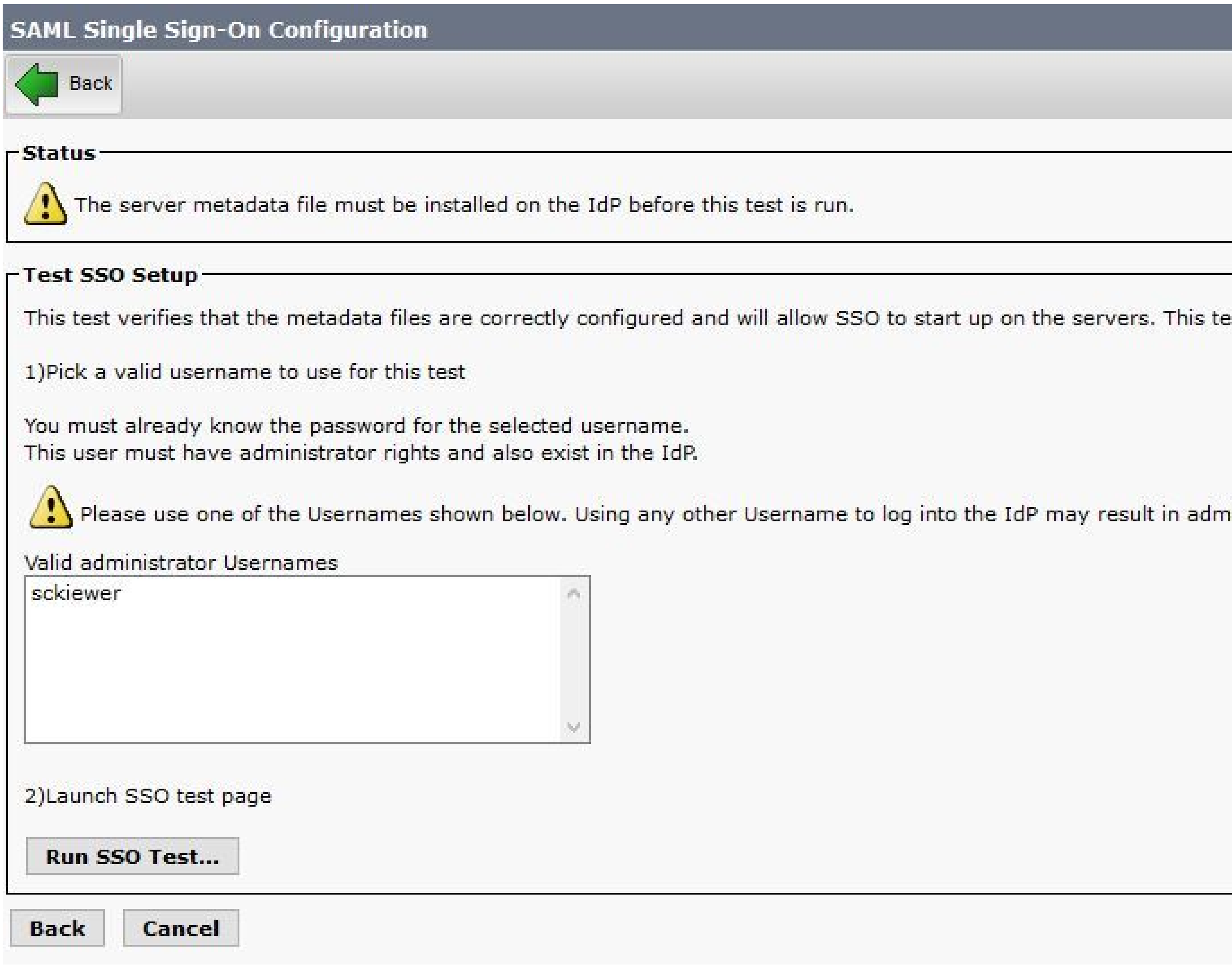
Step 24. Click **OK**.

Note: Claim rules are needed for any Unified Collaboration server on which you intend to utilize SSO.

Finish SSO Enablement On CUCM And Run The SSO Test

Step 1. Now that the AD FS server is fully configured, you can go back to CUCM.

Step 2. You left off at the final configuration page:


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 te

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 adm

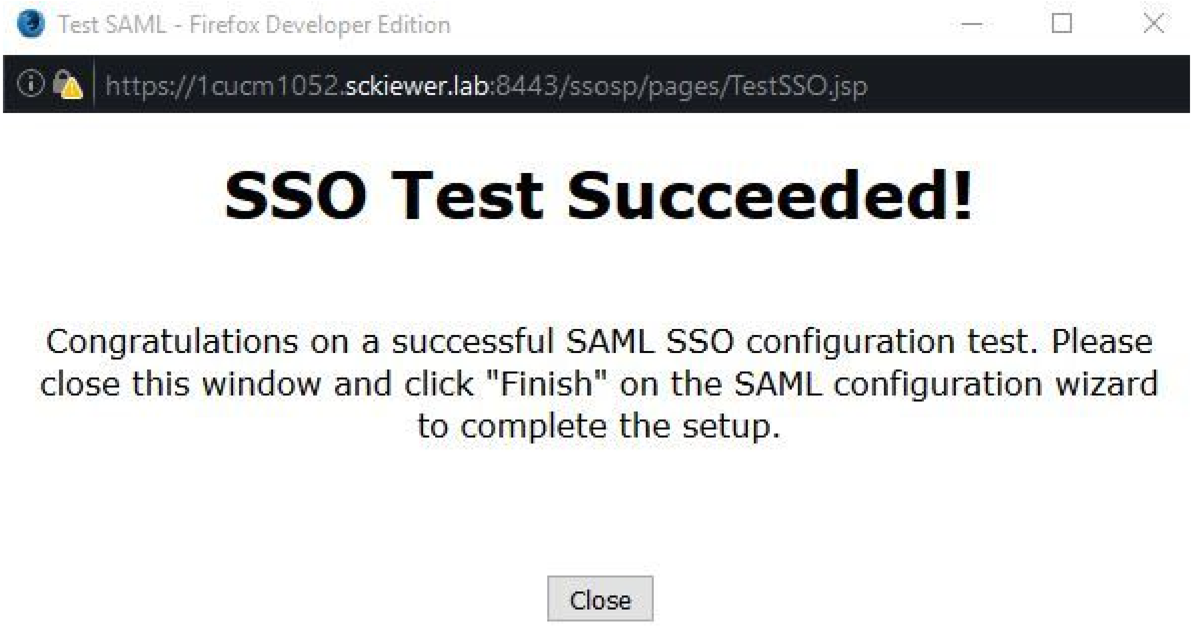
Valid administrator Usernames

sckiewer

2)Launch SSO test page

Step 3. Select your End User which has the **Standard CCM Super Users** role selected and click **Run SSO Test...**

Step 4. Ensure that your browser allows pop-ups, and enter your credentials into the prompt.


Test SAML - Firefox Developer Edition
https://1cucm1052.sckiewer.lab:8443/ssosp/pages/TestSSO.jsp
Close

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.

Step 5. Click **Close** on the pop-up window, and then **Finish**.

Step 6. After a brief restart of the web applications, SSO is enabled.

Troubleshoot

Set SSO Logs to Debug

To set the SSO logs to debug, you have to run this command in the CLI of the CUCM: **set samltrace level debug**

The SSO logs can be downloaded from RTMT. The name of the log set is **Cisco SSO**.

Find The Federation Service Name

To find the federation service name, click **Start** and search for **AD FS 2.0 Management**.

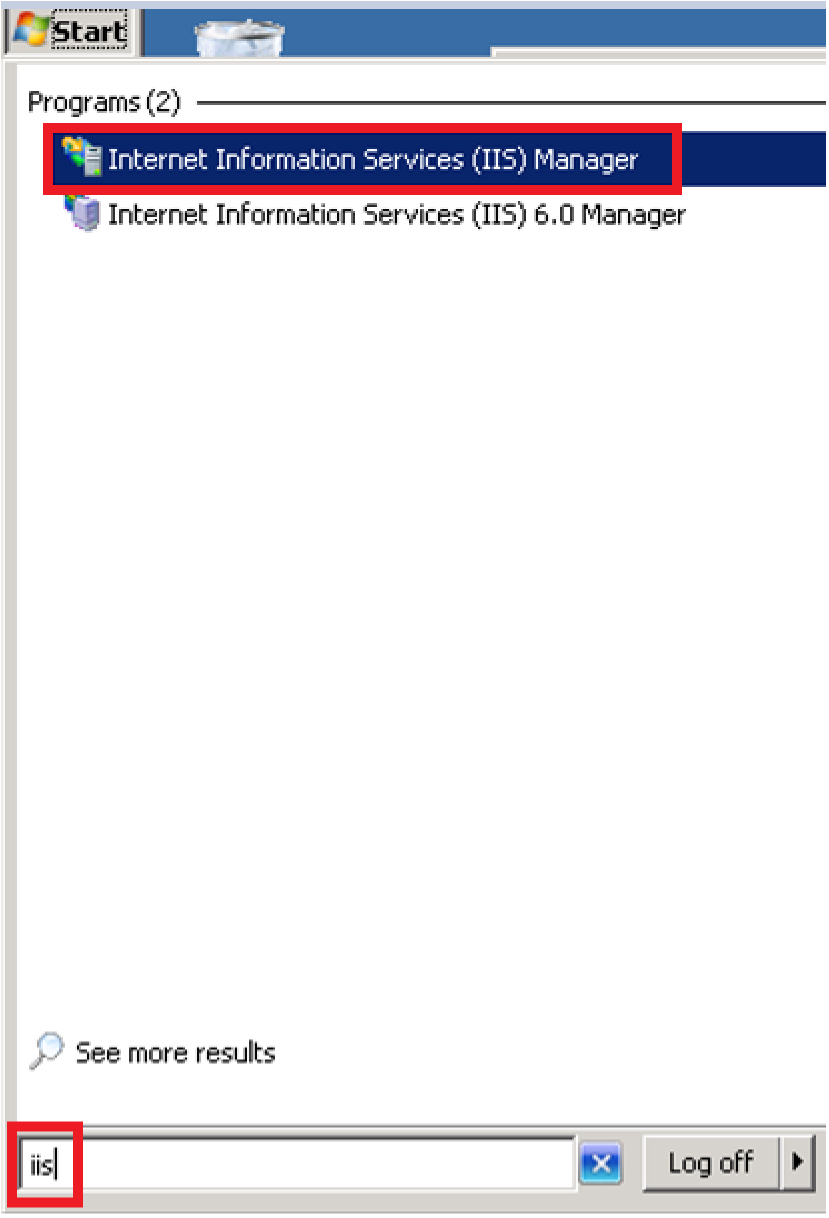
â€¢ Click on Edit **Federation Service Propertiesâ€¦**
â€¢ While on the General tab, look for **Federation Service name**

Dotless Certificate And Federation Service Name

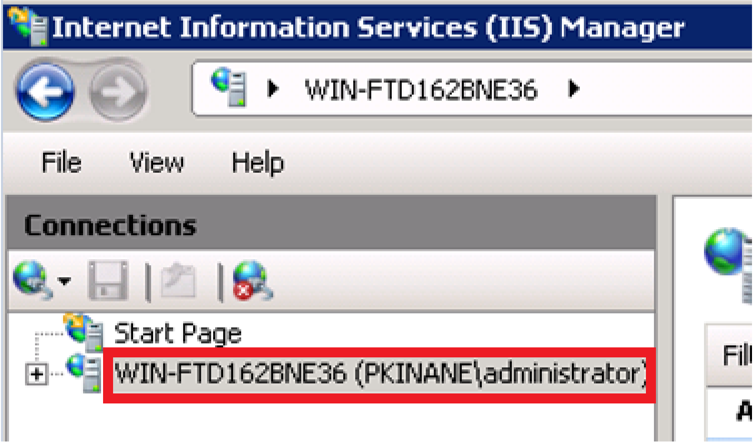
If you receive this error message in the AD FS configuration wizard, you need to create a new certificate.

The selected certificate cannot be used to determine the Federation Service name because the selected certificate has a dotless (short-named) Subject name. Select another certificate without a dotless (short-named) Subject name, and then try again.

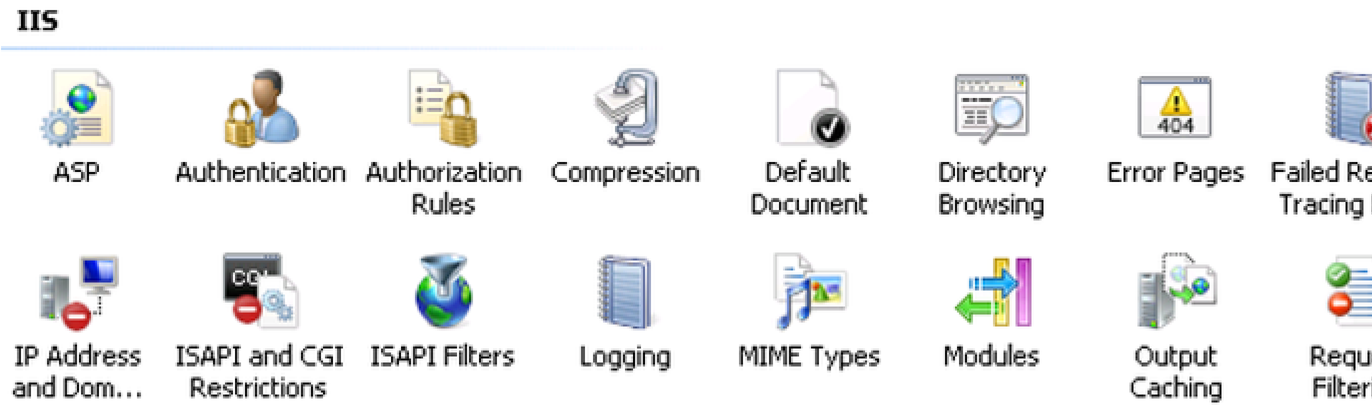
Step 1. Click Start and search for iis, then open Internet Information Services (IIS) Manager


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

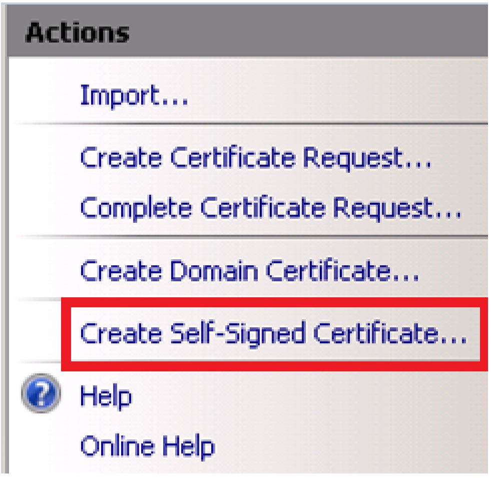
Step 2. Click your server's name.


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

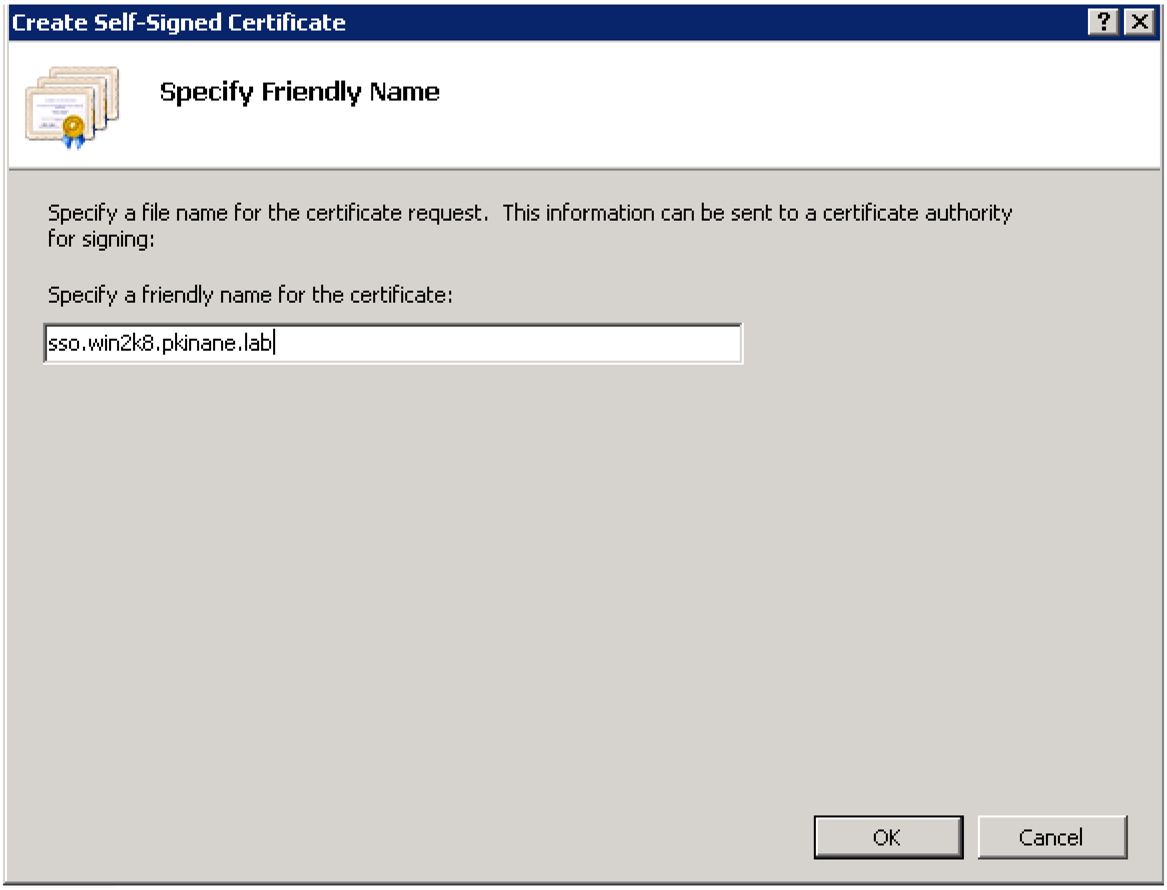
Step 3. Click Server Certificates.



Step 4. Click Create Self-Signed Certificate.


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

Step 5. Enter the name you want for the alias of your certificate.



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

Time is Out of Sync between the CUCM and IDP Servers

If you receive this error when you run the SSO test from CUCM, you need to configure the Windows Server to use the same NTP server(s) as the CUCM.

Invalid SAML response. This can be caused when time is out of sync between the Cisco Unified Communications Manager and IDP servers. Please verify the NTP configuration on both servers. Run "utils ntp status" from the CLI to check this status on Cisco Unified Communications Manager.

Once the Windows Server has the correct NTP servers specified, you need to perform another SSO test and see if the issue persists. In some instances, it is necessary to skew the validity period of the assertion. More detail on that process here.

Related Information

- Technical Support & Documentation - Cisco Systems