

Configure SAML SSO on Cisco Unified Communications Manager with ADFS 3.0

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configuration Pre-Check](#)

[A Records](#)

[Pointer \(PTR\) Records](#)

[SRV Records are Needed to be in Place for Jabber Discovery Services](#)

[ADFS3 Initial Configuration](#)

[Configure SSO on CUCM with ADFS](#)

[LDAP Configuration](#)

[CUCM Metadata](#)

[Configure ADFS Relying Party](#)

[IDP Metadata](#)

[Configure SSO on CUC](#)

[CUC Metadata](#)

[Configure SSO on Expressway](#)

[Import Metadata to Expressway C](#)

[Export Metadata From Expressway C](#)

[Add a Relying Party Trust for Cisco Expressway-E](#)

[OAuth with Refresh Login](#)

[Authentication Path](#)

[SSO Architecture](#)

[On-Premise Login Flow](#)

[MRA Login Flow](#)

[OAuth](#)

[Access/Refresh Token](#)

[OAuth Authorization Code Grant Flow is better](#)

[Configure Kerberos](#)

[Select Windows Authentication](#)

[ADFS Supports both Kerberos NTLM](#)

[Configure Microsoft Internet Explorer](#)

[Add ADFS URL under Security > Intranet zones > Sites](#)

[Add CUCM, IMP, and Unity hostnames to Security > Trusted Sites](#)

[User Authentication](#)

[Jabber Login in SSO](#)

[Troubleshoot](#)

[Internet Explorer \(IE\)](#)

[Sites Adding to IE](#)

[Out of Sync Issue](#)

[Revoke a Token](#)

[Bootstrap File](#)

[SSO Failing Due MSIS7066](#)

Introduction

This document describes the steps to configure Single Sign-On with Active Directory Federation Service (ADFS 3.0) with the use of Windows 2012 R2 on Cisco Unified Communication Manage (CUCM), Cisco Unity Connection (CUC), Expressway products. Steps to configure Kerberos are also included in this document.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Single Sign-On (SSO) and Windows products.

Components Used

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

- CUCM 11.5
- CUC 11.5
- Expressway 12
- Windows 2012 R2 Server with these roles:
 - Active Directory Certificate Services
 - Active Directory Federation Services

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.

Configuration Pre-Check

Before you install ADFS3, these server roles need to already exist in the environment:

- Domain Controller and DNS
- All servers must be added as A Records along with their Pointer Record (a type of DNS record that resolves an IP address to a domain or hostname)

A Records

In fhlab.com. hosts cmpubhcsc, cmsubhcsc, cucpubhcsc, cucsubhcsc, expwyc, expwye, impubhcsc and imsubhcsc have been added.

| Name | Type |
|-------------------------|--------------------------|
| _msdcs | |
| _sites | |
| _tcp | |
| _udp | |
| DomainDnsZones | |
| ForestDnsZones | |
| (same as parent folder) | Start of Authority (SOA) |
| (same as parent folder) | Name Server (NS) |
| (same as parent folder) | Host (A) |
| ad | Host (A) |
| cmpubhcsc | Host (A) |
| cmsubhcsc | Host (A) |
| cucpubhcsc | Host (A) |
| cucsubhcsc | Host (A) |
| expwyc | Host (A) |
| expwye | Host (A) |
| imppubhcsc | Host (A) |
| impsubhcsc | Host (A) |

Pointer (PTR) Records

| Name | Type | Data | Timestamp |
|-------------------------|--------------------------|--|-----------------------|
| (same as parent folder) | Start of Authority (SOA) | [14], ad.fhlab.com, hostmaster.fhlab.co... | static |
| (same as parent folder) | Name Server (NS) | ad.fhlab.com. | static |
| 10.89.228.144 | Pointer (PTR) | expwyc.fhlab.com. | static |
| 10.89.228.145 | Pointer (PTR) | expwye.fhlab.com. | static |
| 10.89.228.146 | Pointer (PTR) | cmpubhcsc.fhlab.com. | static |
| 10.89.228.147 | Pointer (PTR) | cmsubhcsc.fhlab.com. | static |
| 10.89.228.148 | Pointer (PTR) | imppubhcsc.fhlab.com. | static |
| 10.89.228.150 | Pointer (PTR) | impsubhcsc.fhlab.com. | static |
| 10.89.228.151 | Pointer (PTR) | cucpubhcsc.fhlab.com. | static |
| 10.89.228.153 | Pointer (PTR) | cucsubhcsc.fhlab.com. | static |
| 10.89.228.154 | Pointer (PTR) | win10.fhlab.com. | 5/12/2020 10:00:00 AM |
| 10.89.228.226 | Pointer (PTR) | ad.fhlab.com. | 5/12/2020 11:00:00 AM |
| 10.89.228.227 | Pointer (PTR) | win10ext.fhlab.com. | 5/7/2020 4:00:00 PM |

SRV Records are Needed to be in Place for Jabber Discovery Services

The screenshot shows the DNS Manager console for the fhlab.com domain. The main pane displays a list of SRV records:

| Name | Type | Data | Timestamp |
|------------|------------------------|------------------------------------|-----------------------|
| _cisco-uds | Service Location (SRV) | [0][0][8443] cmsubhcsc.fhlab.com. | static |
| _cisco-uds | Service Location (SRV) | [0][0][8443] cmpubhcsc.fhlab.com. | static |
| _cuplogin | Service Location (SRV) | [0][0][8443] impsubhcsc.fhlab.com. | static |
| _cuplogin | Service Location (SRV) | [0][0][8443] imppubhcsc.fhlab.com. | static |
| _gc | Service Location (SRV) | [0][100][3268] ad.fhlab.com. | 5/12/2020 10:00:00 AM |
| _kerberos | Service Location (SRV) | [0][100][88] ad.fhlab.com. | 5/12/2020 10:00:00 AM |
| _kpasswd | Service Location (SRV) | [0][100][464] ad.fhlab.com. | 5/12/2020 10:00:00 AM |
| _ldap | Service Location (SRV) | [0][100][389] ad.fhlab.com. | 5/12/2020 10:00:00 AM |

An inset window titled "_cisco-uds Properties" shows the configuration for the SRV record:

- Service Location (SRV) Security
- Domain: fhlab.com
- Service: _cisco-uds
- Protocol: _tcp
- Priority: 0
- Weight: 0
- Port number: 8443
- Host offering this service: cmpubhcsc.fhlab.com.

- Root CA (assuming the certificates will be Enterprise CA-signed)

A Certificate Template needs to be created based on the Web Server Certificate Template, the former is duplicated, renamed and on the Extensions tab, Application Policies is modified adding a Client Authentication Application Policy. This template is needed to sign all internal certificates (CUCM, CUC, IMP and Expressway Core) in a LAB environment the internal CA can also sign the Expressway E Certificate Signing Requests (CSR).

The screenshot shows the Certificate Templates console for the AD.fhlab.com domain. A list of templates is visible on the left, including ClientServerAuth, Code Signing, and others. The main pane shows the "Properties of New Template" dialog with the "Extensions" tab selected. The "Extensions included in this template" list contains:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

The "Description of Application Policies" section lists:

- Server Authentication
- Client Authentication

An inset window titled "Edit Application Policies Extension" shows the configuration for the Application Policies extension, listing "Client Authentication" and "Server Authentication" as application policies.

The template created needs to be issued to be able to sign CSR.

The screenshot shows the Certificate Authority console for the local fhlab-AD-CA. The left pane shows the hierarchy: fhlab-AD-CA > Certificate Templates. The main pane displays a list of templates with their intended purposes:

| Name | Intended Purpose |
|----------------------------------|--|
| ClientServerAuth | Server Authentication, Client Authentic... |
| Directory Email Replication | Directory Service Email Replication |
| Domain Controller Authentication | Client Authentication, Server Authentic... |
| Kerberos Authentication | Client Authentication, Server Authentic... |
| EFS Recovery Agent | File Recovery |
| | Encrypting File System |
| | Client Authentication, Server Authentic... |
| | Client Authentication |

A context menu is open over the "Certificate Template to Issue" entry, showing options: "Manage", "New", and "Certificate Template to Issue".

On the CA certificate web, select the template that has been created previously.

Microsoft Active Directory Certificate Services -- fhlab-AD-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (Web server) in the Saved Request box.

Saved Request:

```
8V8mWY/9kjhqfnpBzAAW++to1GzBjnvqaT8StWM
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):
LA0dphF6LrurUeY2KLvMLmK1ft7aSy483yCsm0v1
OWQFzoLb3bS80ziW7fQEFWSaCg567DMQ8FkZt5N
10y/Ip60dzTdZE9w2p8rK3YxcbyovSt0iJiirh
AM/GjnzQ
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Additional Attributes:

- ✓ User
- Basic EFS
- Administrator
- EFS Recovery Agent
- Web Server
- Subordinate Certification Authority
- ClientServerAuth

CUCM, IMP and CUC Multi-Server CSR must be Generated and signed by the CA. The Certificate purpose must be tomcat.

Generate Certificate Signing Request

Generate Close

Status

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose** tomcat

Distribution* Multi-server(SAN)

Common Name* cmpubhcsc-ms.fhlab.com

Subject Alternate Names (SANs)

Auto-populated Domains

- cmpubhcsc.fhlab.com
- cmsubhcsc.fhlab.com
- imppubhcsc.fhlab.com
- impsubhcsc.fhlab.com

Parent Domain fhlab.com

Other Domains

Browse... No file selected.

Please import .TXT file only.
For more information please refer to the notes in the Help Section

Key Type** RSA

Key Length* 2048

Hash Algorithm* SHA256

Generate Close

CA Root Certificate must be uploaded to Tomcat Trust and the signed Certificate to tomcat.

Cisco Unified Operating System Administration

Navigation Cisco Unified OS Administration osadmin Search Documentation About Logout

Show Settings Security Software Upgrades Services Help

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

7 records found

Certificate List (1 - 7 of 7) Rows per Page 50

Find Certificate List where Certificate begins with tomcat Find Clear Filter

| Certificate | Common Name | Type | Key Type | Distribution | Issued By | Expiration | Description |
|--------------|------------------------|-------------|----------|---------------------|------------------------|------------|---|
| tomcat | cmouubhsc-ms.fhlab.com | CA-signed | RSA | Multi-server(SAN) | fhlab-AD-CA | 04/18/2022 | Certificate Signed by fhlab-AD-CA |
| tomcat-ECDSA | cmouubhsc-EC.fhlab.com | Self-signed | EC | cmouubhsc.fhlab.com | cmouubhsc-EC.fhlab.com | 04/02/2025 | Self-signed certificate generated by system |
| tomcat-trust | cmouubhsc-EC.fhlab.com | Self-signed | EC | imppubhsc.fhlab.com | imppubhsc-EC.fhlab.com | 04/02/2025 | Trust Certificate |
| tomcat-trust | cmouubhsc-EC.fhlab.com | Self-signed | EC | cmouubhsc.fhlab.com | cmouubhsc-EC.fhlab.com | 04/02/2025 | Trust Certificate |
| tomcat-trust | cmouubhsc-EC.fhlab.com | Self-signed | EC | cmouubhsc.fhlab.com | cmouubhsc-EC.fhlab.com | 04/02/2025 | Trust Certificate |
| tomcat-trust | fhlab-AD-CA | Self-signed | RSA | fhlab-AD-CA | fhlab-AD-CA | 04/18/2025 | Signed Certificate |

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

Certificate List (1 - 6 of 6) Rows per Page 50

Find Certificate List where Certificate begins with tomcat Find Clear Filter

| Certificate | Common Name | Type | Key Type | Distribution | Issued By | Expiration | Description |
|--------------|------------------------|-------------|----------|---------------------|------------------------|------------|---|
| tomcat | cucubhsc-ms.fhlab.com | CA-signed | RSA | Multi-server(SAN) | fhlab-AD-CA | 04/28/2022 | Certificate Signed by fhlab-AD-CA |
| tomcat-ECDSA | cucubhsc-EC.fhlab.com | Self-signed | EC | cucubhsc.fhlab.com | cucubhsc-EC.fhlab.com | 04/02/2025 | Self-signed certificate generated by system |
| tomcat-trust | fhlab-AD-CA | Self-signed | RSA | fhlab-AD-CA | fhlab-AD-CA | 04/18/2025 | Signed Certificate |
| tomcat-trust | cmouubhsc-EC.fhlab.com | Self-signed | EC | imppubhsc.fhlab.com | imppubhsc-EC.fhlab.com | 04/02/2025 | Trust Certificate |
| tomcat-trust | cucubhsc-EC.fhlab.com | Self-signed | EC | cucubhsc.fhlab.com | cucubhsc-EC.fhlab.com | 04/02/2025 | Trust Certificate |
| tomcat-trust | cucubhsc-EC.fhlab.com | Self-signed | EC | cucubhsc.fhlab.com | cucubhsc-EC.fhlab.com | 04/02/2025 | Trust Certificate |

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

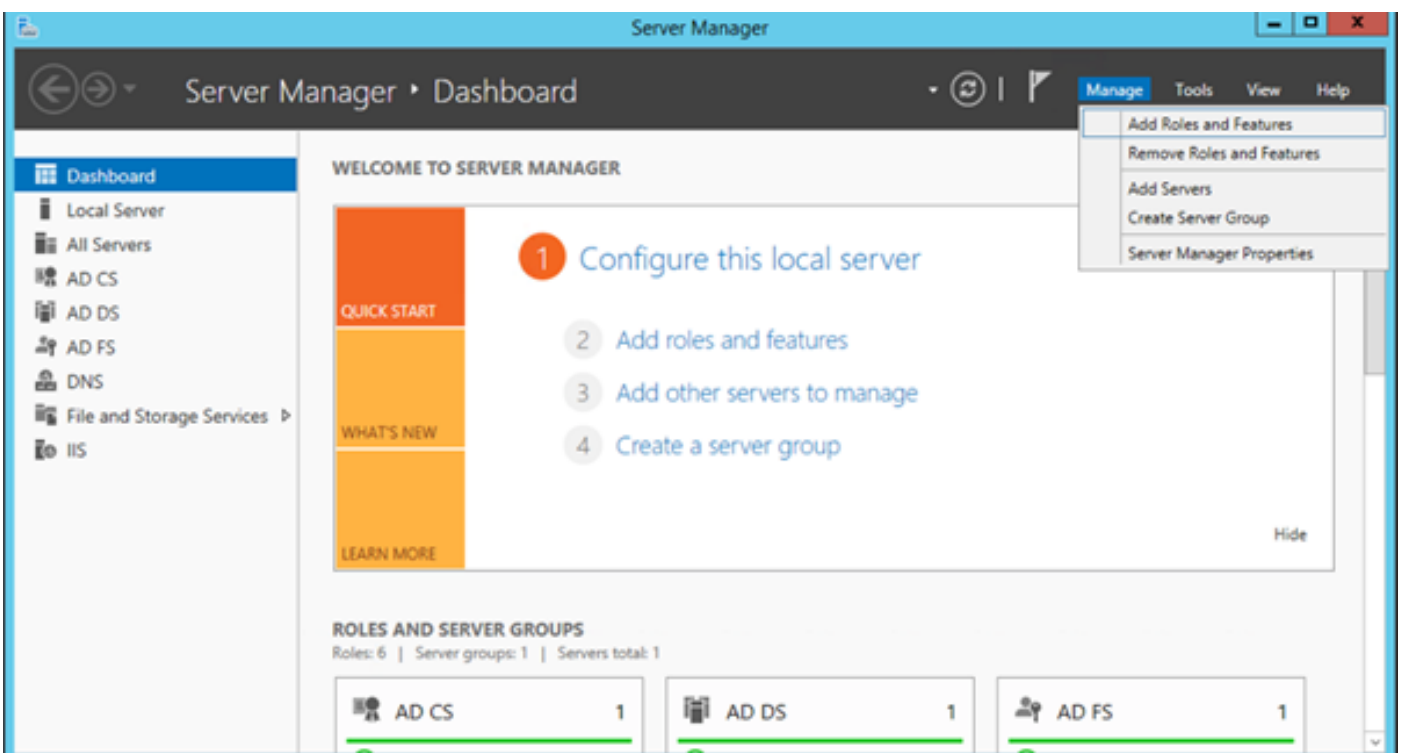
- IIS

If not, this section will go thru the installation of these roles. Otherwise, skip this section and proceed directly to the download of ADFS3 from Microsoft.

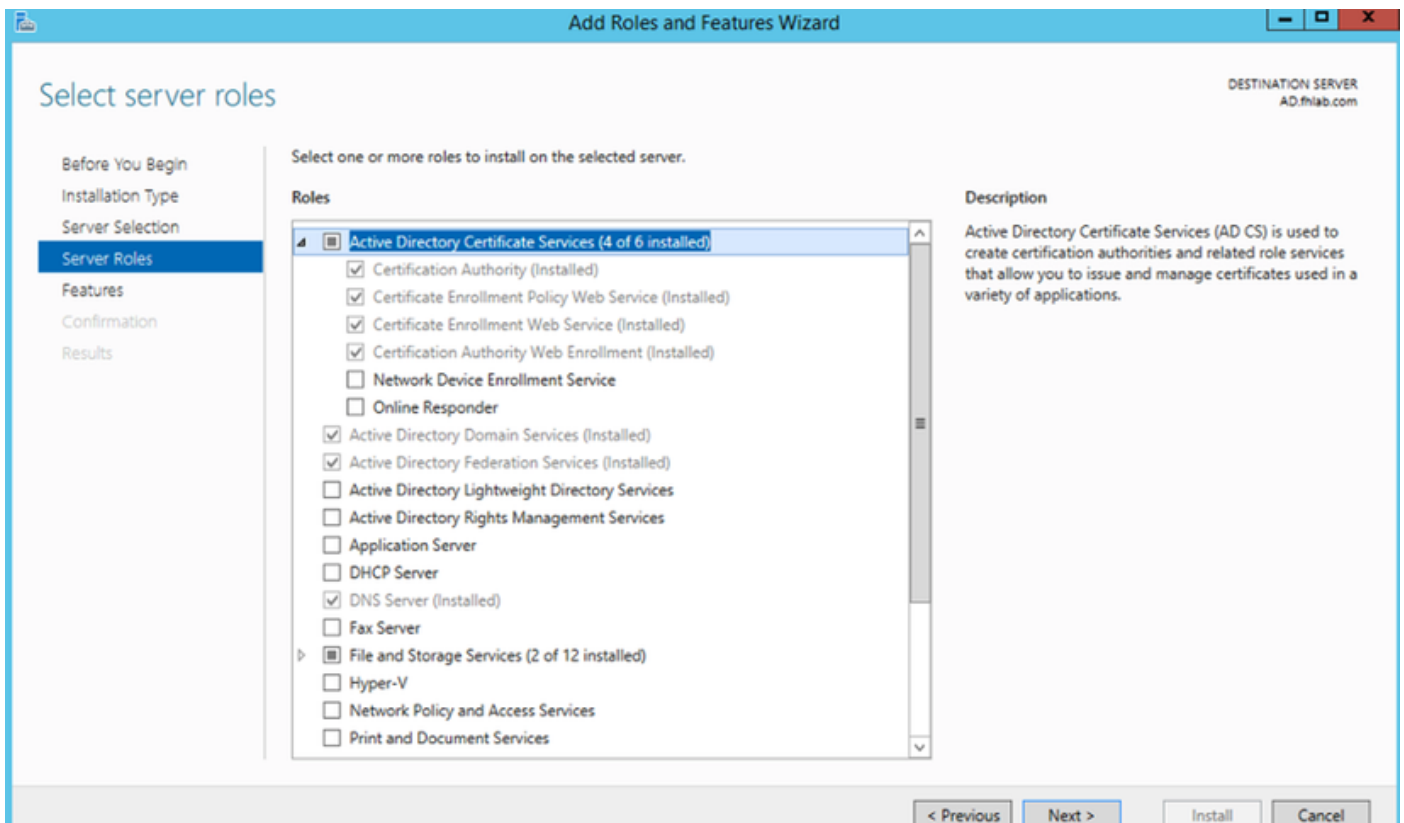
After you install Windows 2012 R2 with DNS, promote the server to a Domain Controller.

The next task will be to install Microsoft Certificate Services.

Navigate to Server Manager and add a new role:



Select the **Active Directory Certificate Services** role.



And deploy these services - Certificate Authority Certificate Enrollment Policy Web Service first. After those two roles are installed, configure them and then install **Certificate Enrollment Web Service** and **Certificate Authority Web Enrollment**. Configure them.

Additional role services and features required such as IIS will also be added, when the Certificate Authority is installed.

Depending on your deployment, you can select Enterprise or Standalone.



Specify Setup Type

Before You Begin

Server Roles

AD CS

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Web Server (IIS)

Role Services

Confirmation

Progress

Results

Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

- Enterprise
Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.
- Standalone
Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.

[More about the differences between enterprise and standalone setup](#)

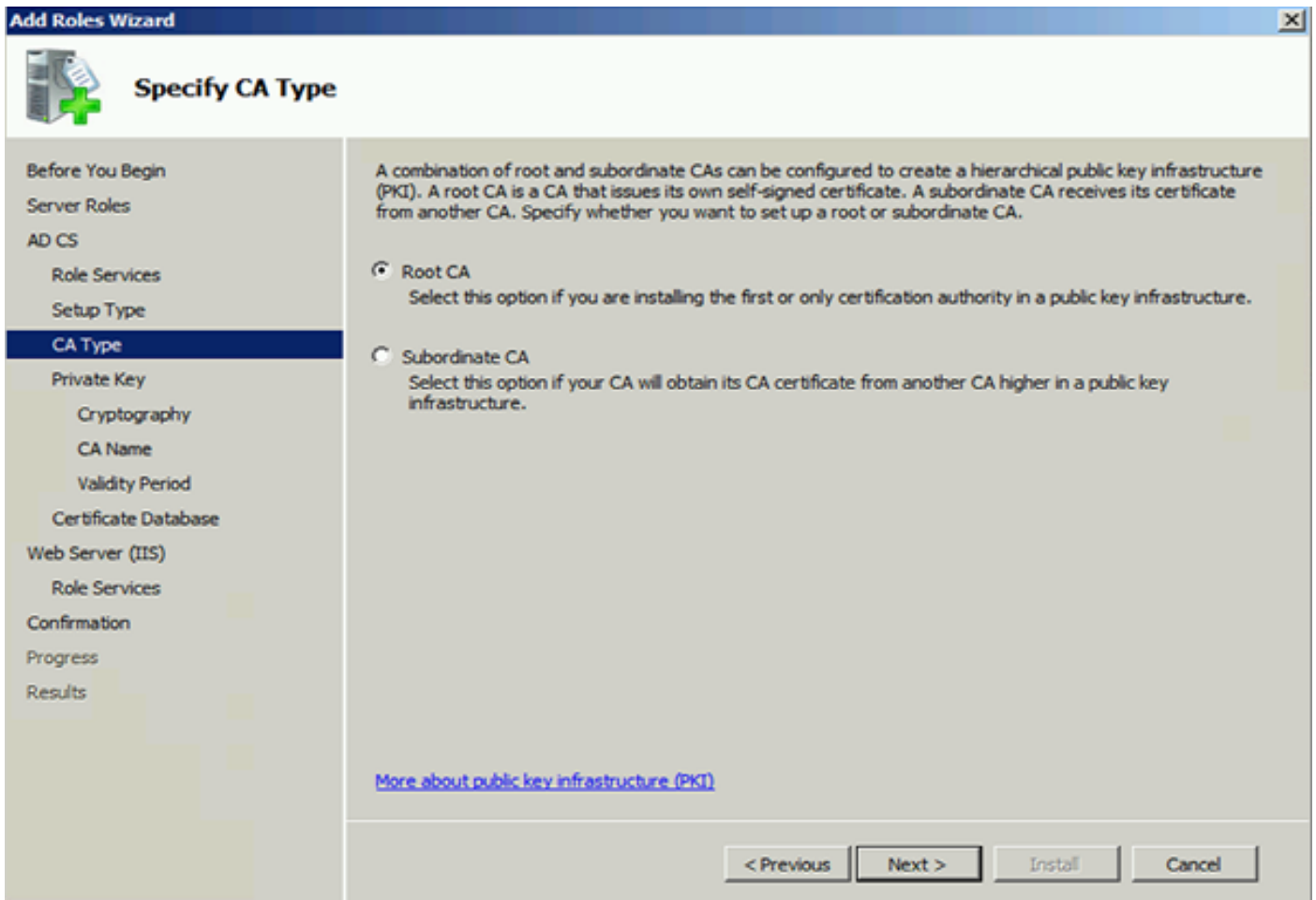
< Previous

Next >

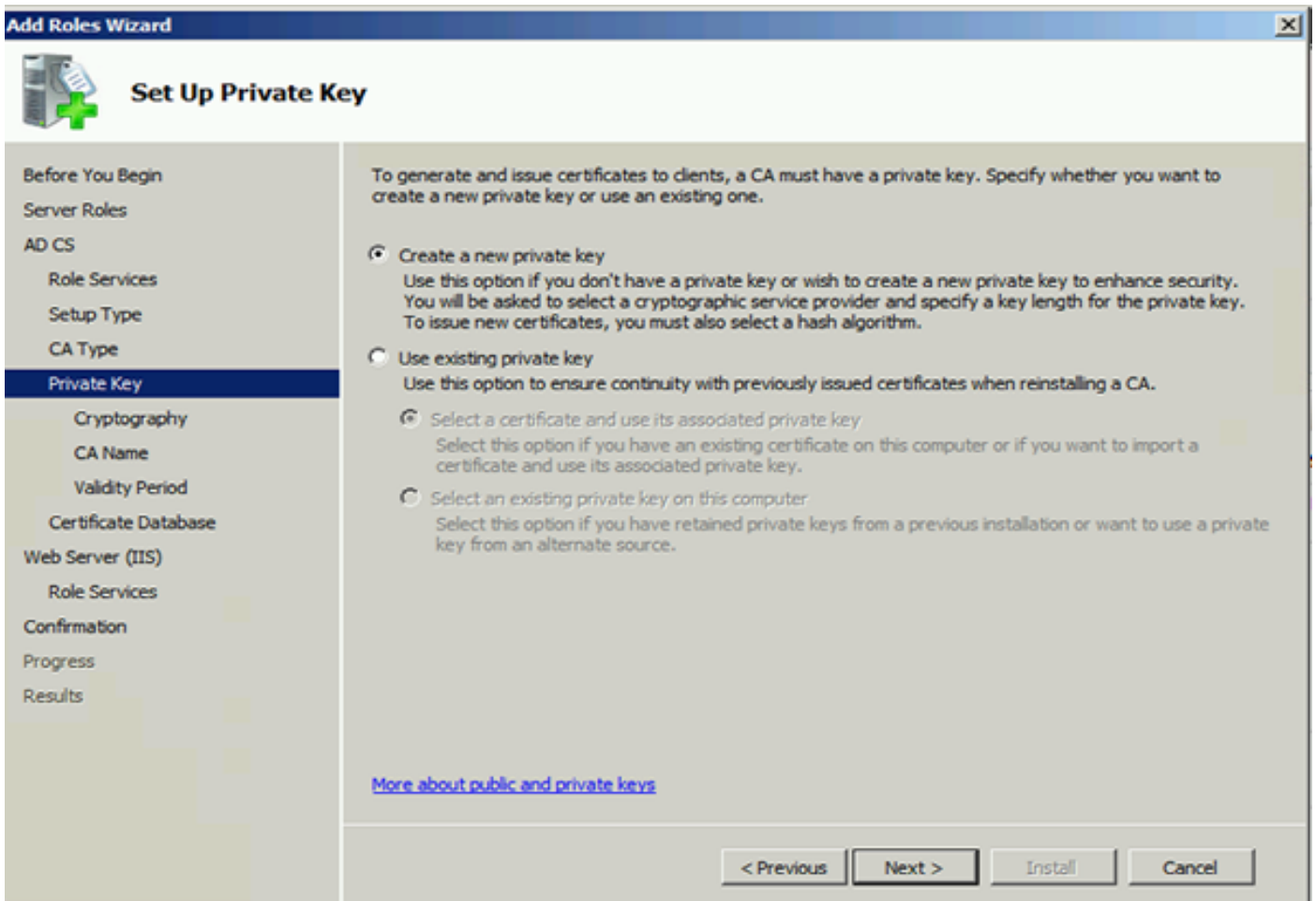
Install

Cancel

For the CA Type, you can select Root CA or Subordinate CA. If there is no other CA already running in the organization, select **Root CA**.

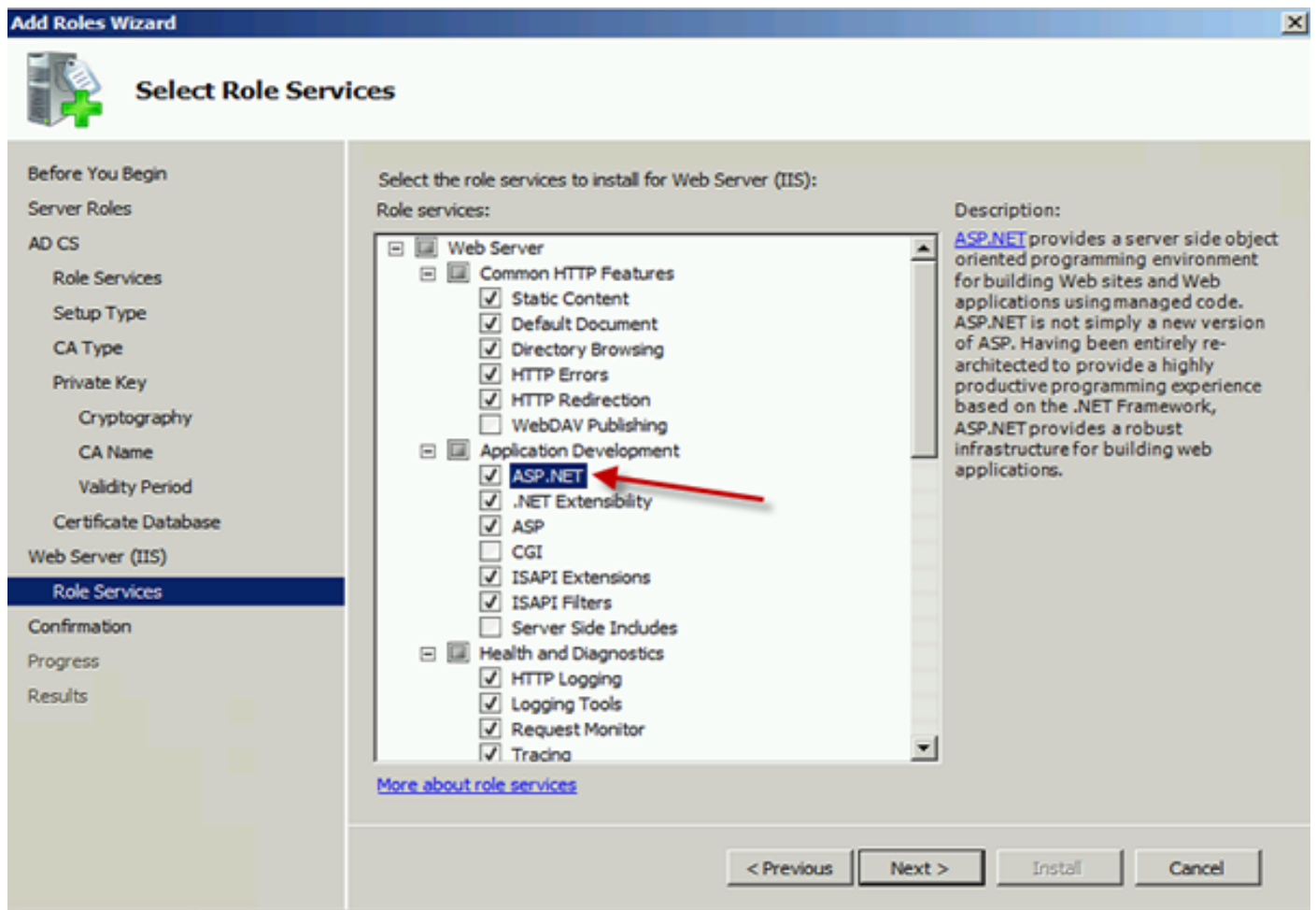


The next step is to create a private key for your CA.

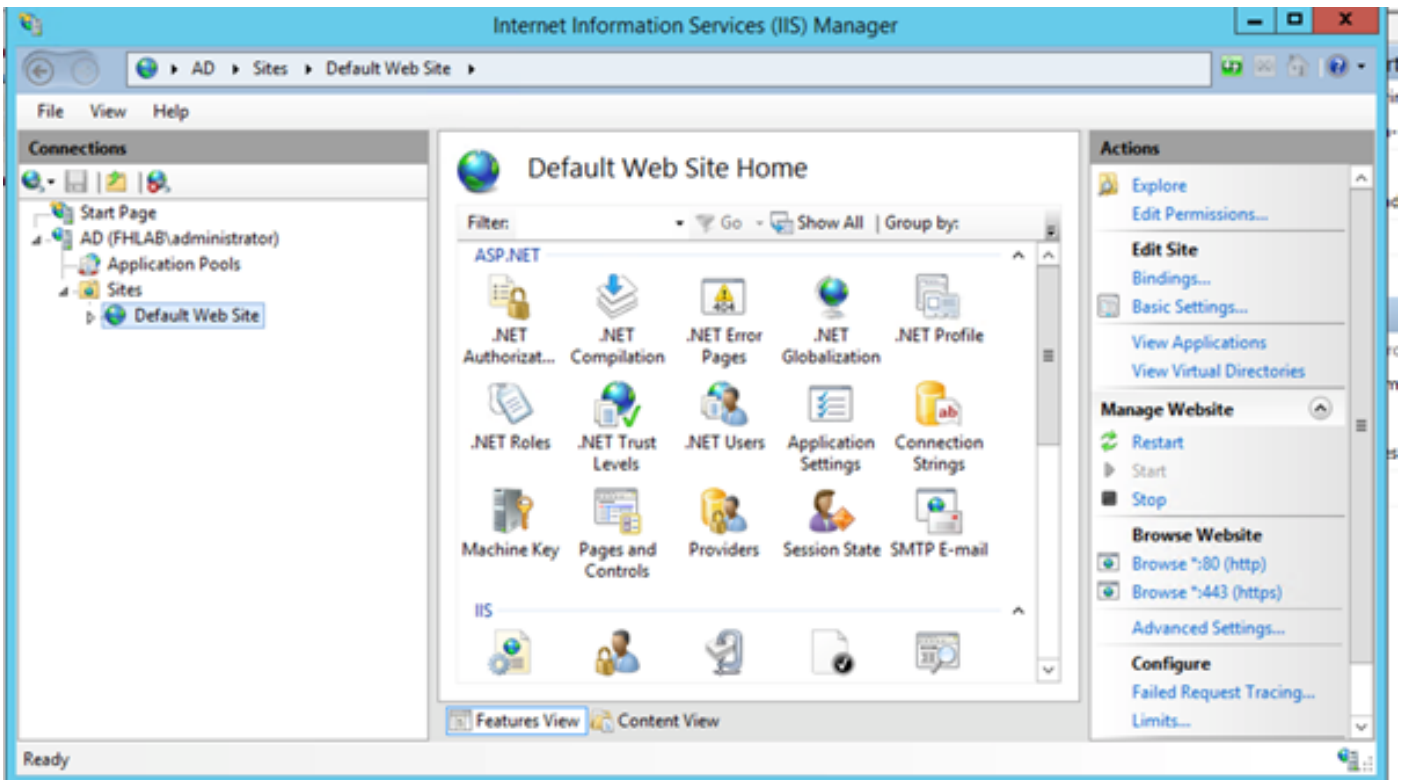


This step is only needed if you install the ADFS3 on a separate Windows Server 2012. After you

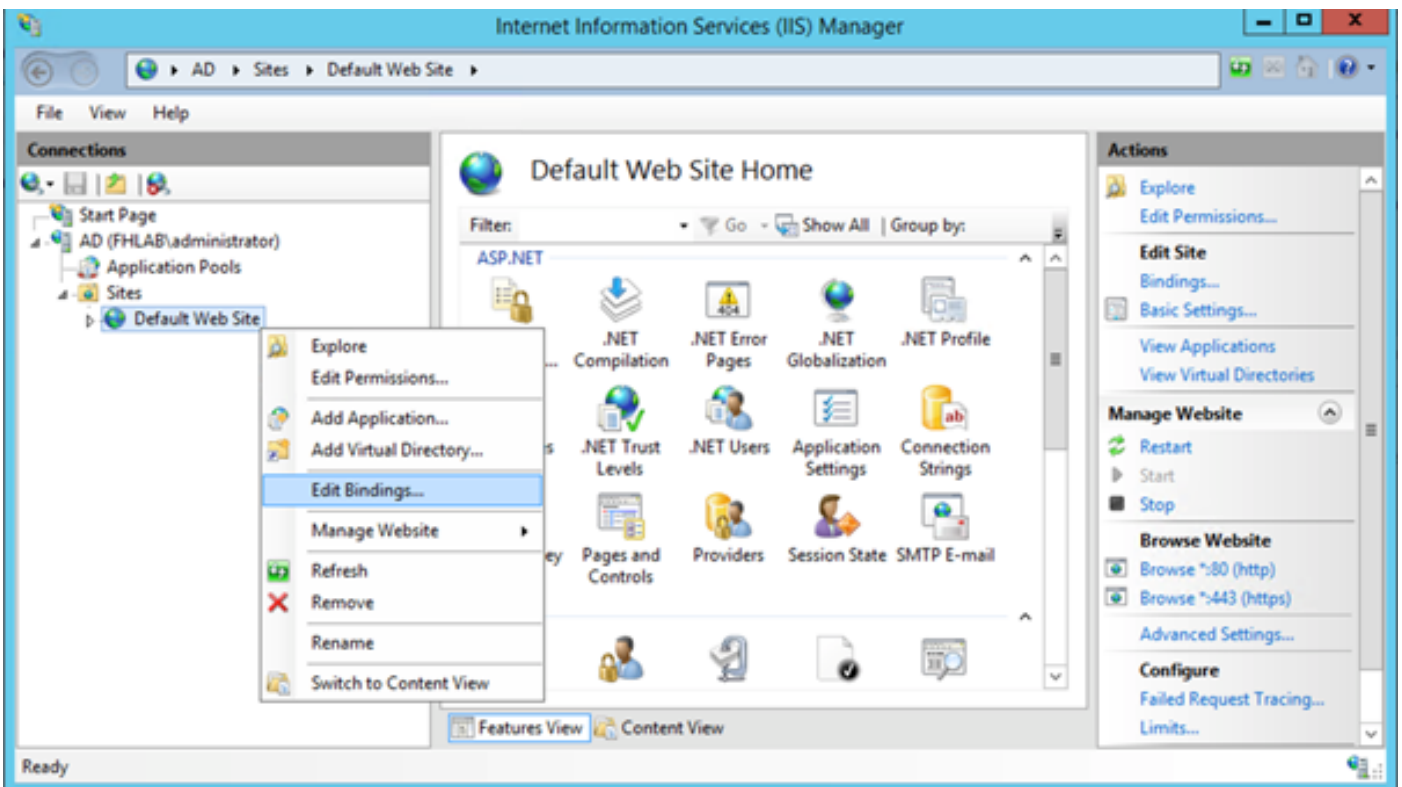
configure the CA, the Role Services for IIS needs to be configured. This is necessary for Web Enrollment on the CA. For most ADFS deployments, an extra Role in IIS, click on **ASP.NET** under Application Development is required.



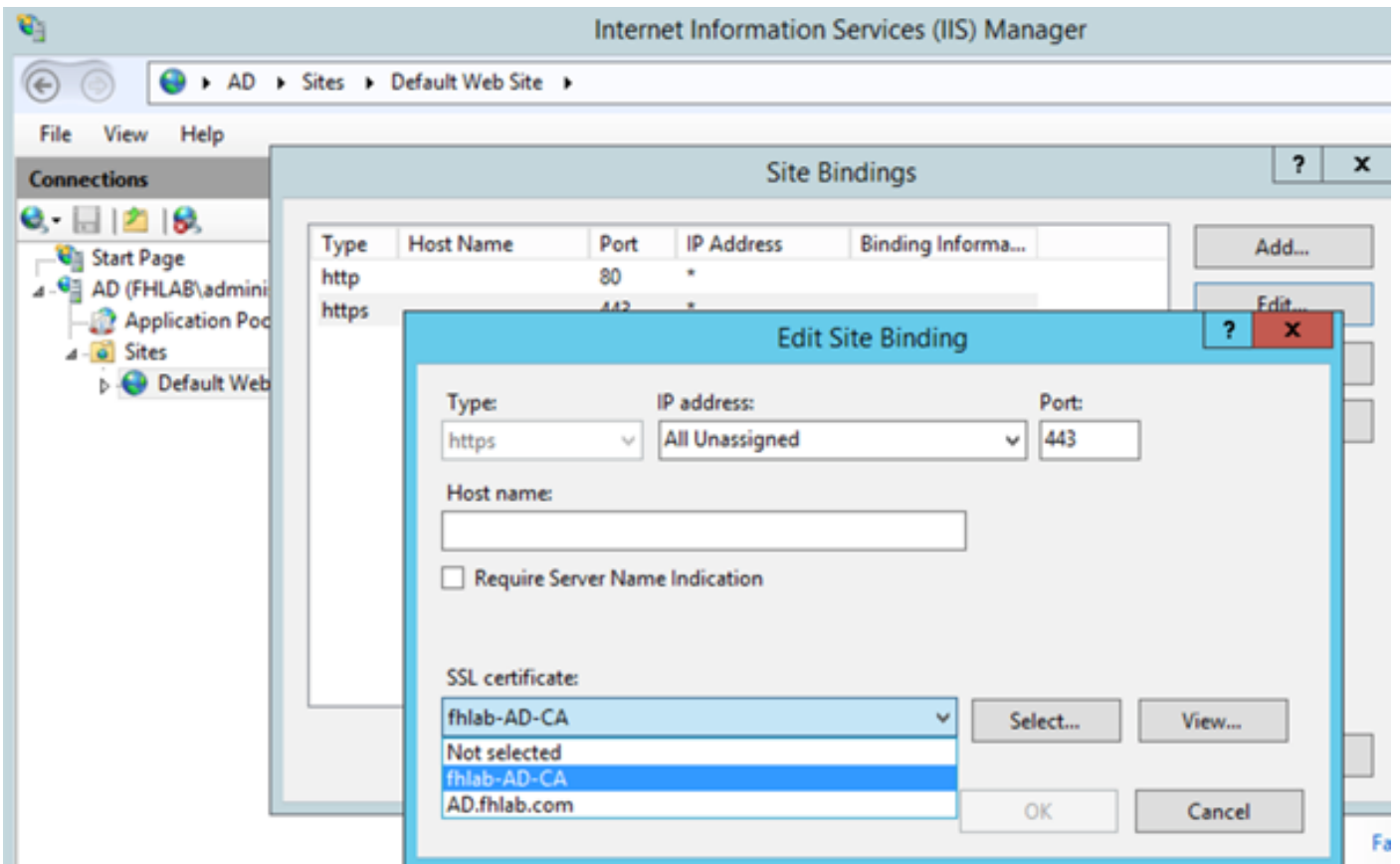
In Server Manager, click on **Web Server > IIS**, and then right-click on **Default Web Site**. The Binding needs to be changed to also allow HTTPS in addition to HTTP. This is done to support HTTPS.



Select **Edit Bindings**.

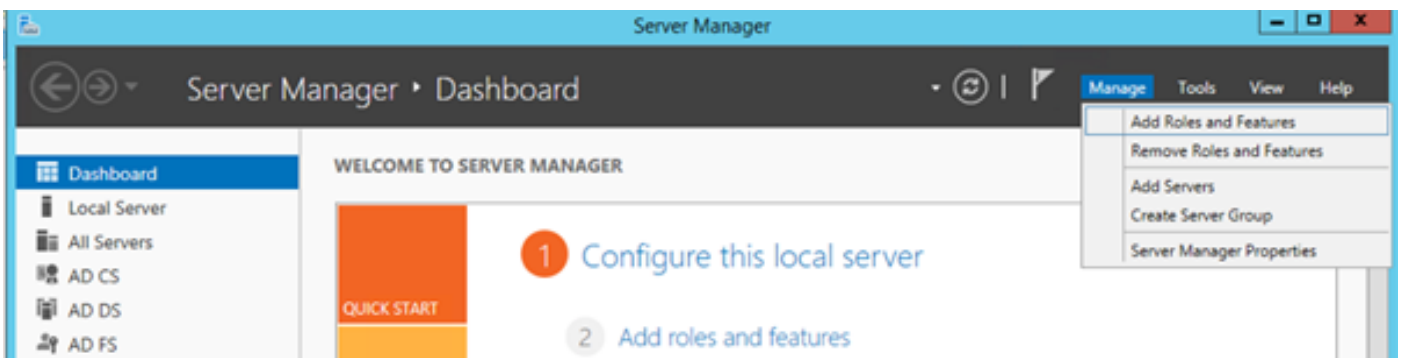


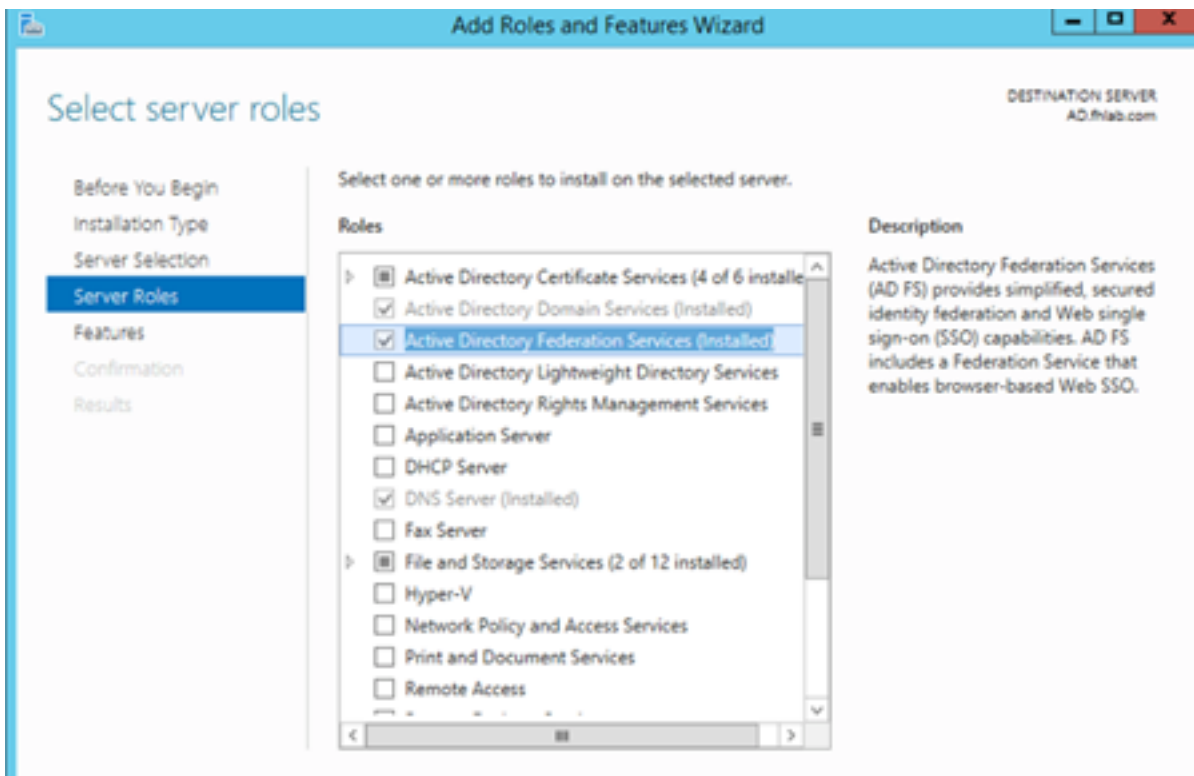
Add a new Site Binding and select **HTTPS** as the type. For the SSL certificate, pick the server certificate that should have the same FQDN as your AD server.



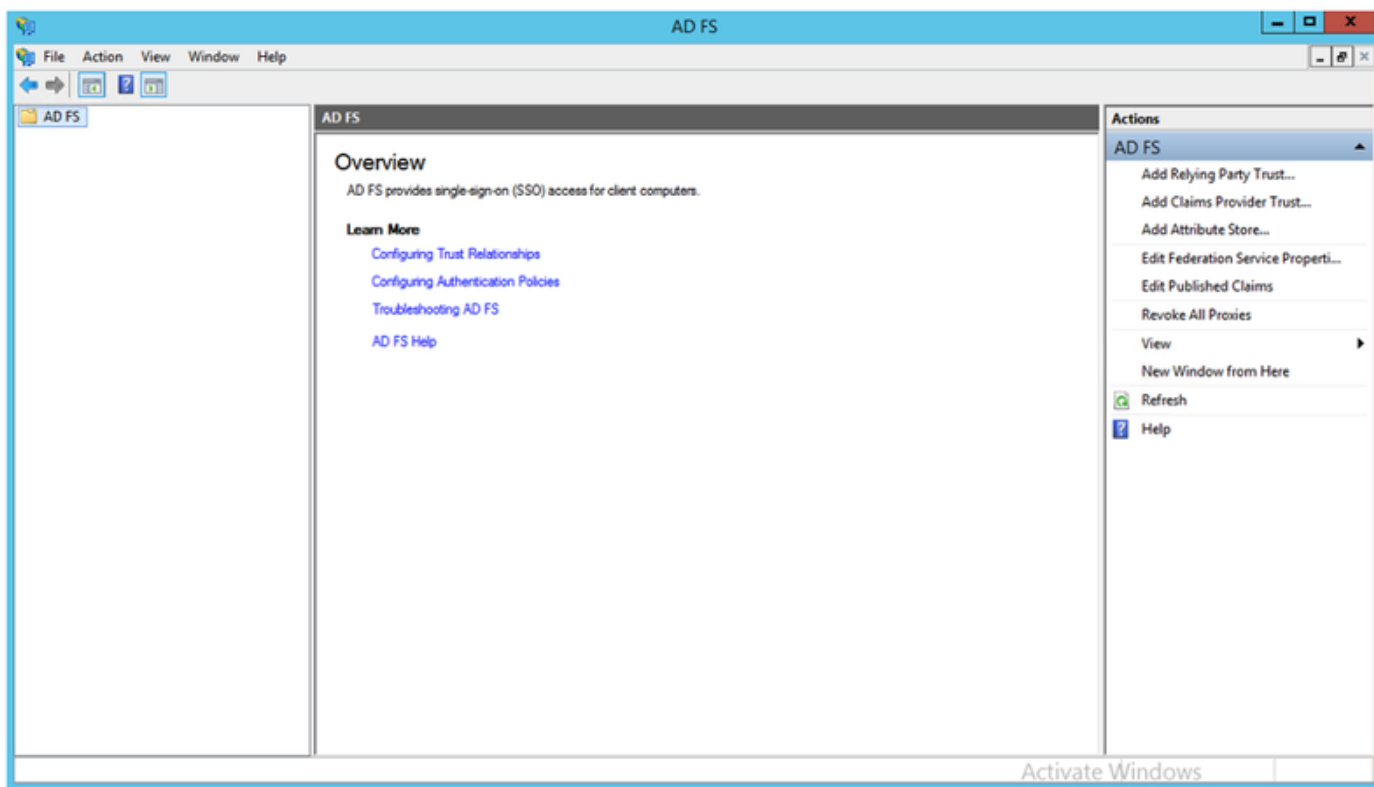
All the prerequisite roles are installed in the environment, so now you can proceed with the installation of ADFS3 Active Directory Federation Services (on Windows Server 2012).

For the Server Role, navigate to **Server Manager > Manage > Add Server Roles and Features** and then select **Active Directory Federation Services** if you install the IDP inside the customer network, on the private LAN.





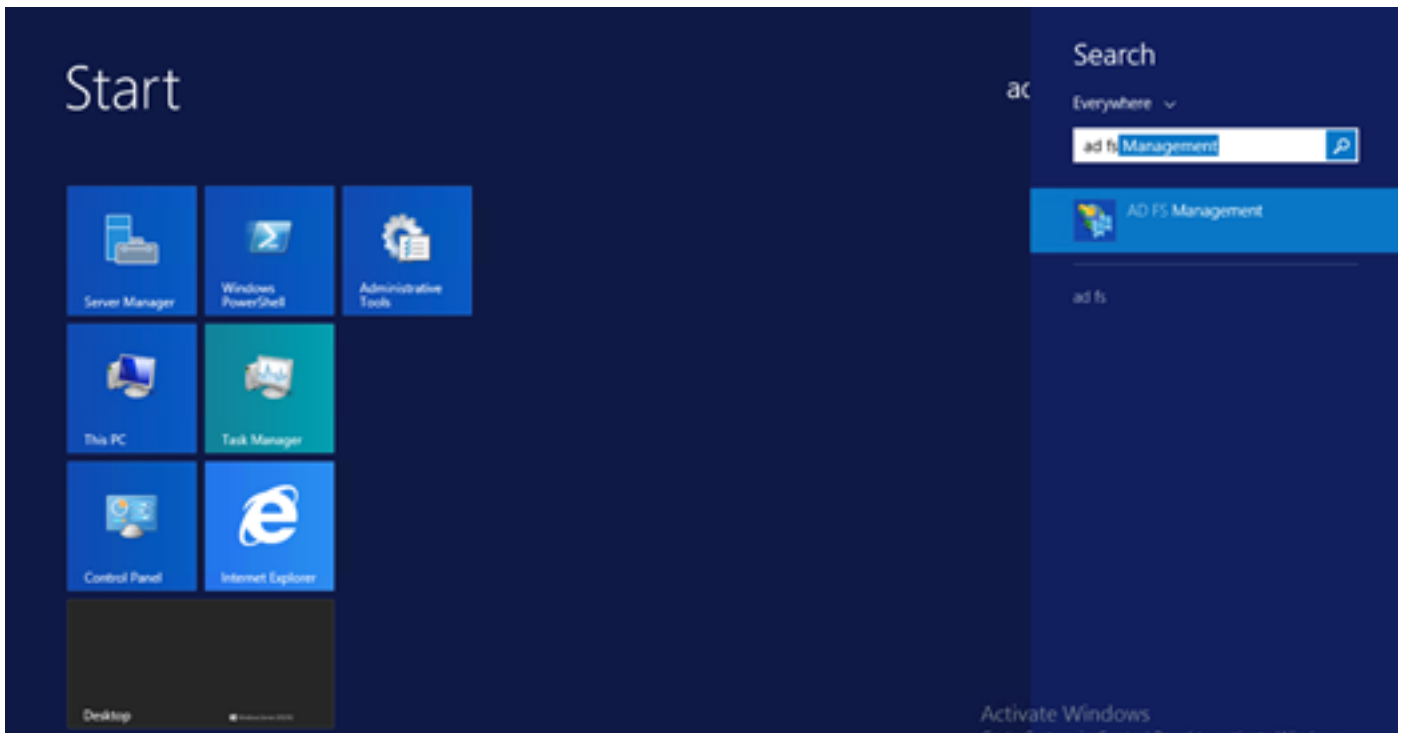
Once the installation completes, you can open it from the taskbar or start menu.



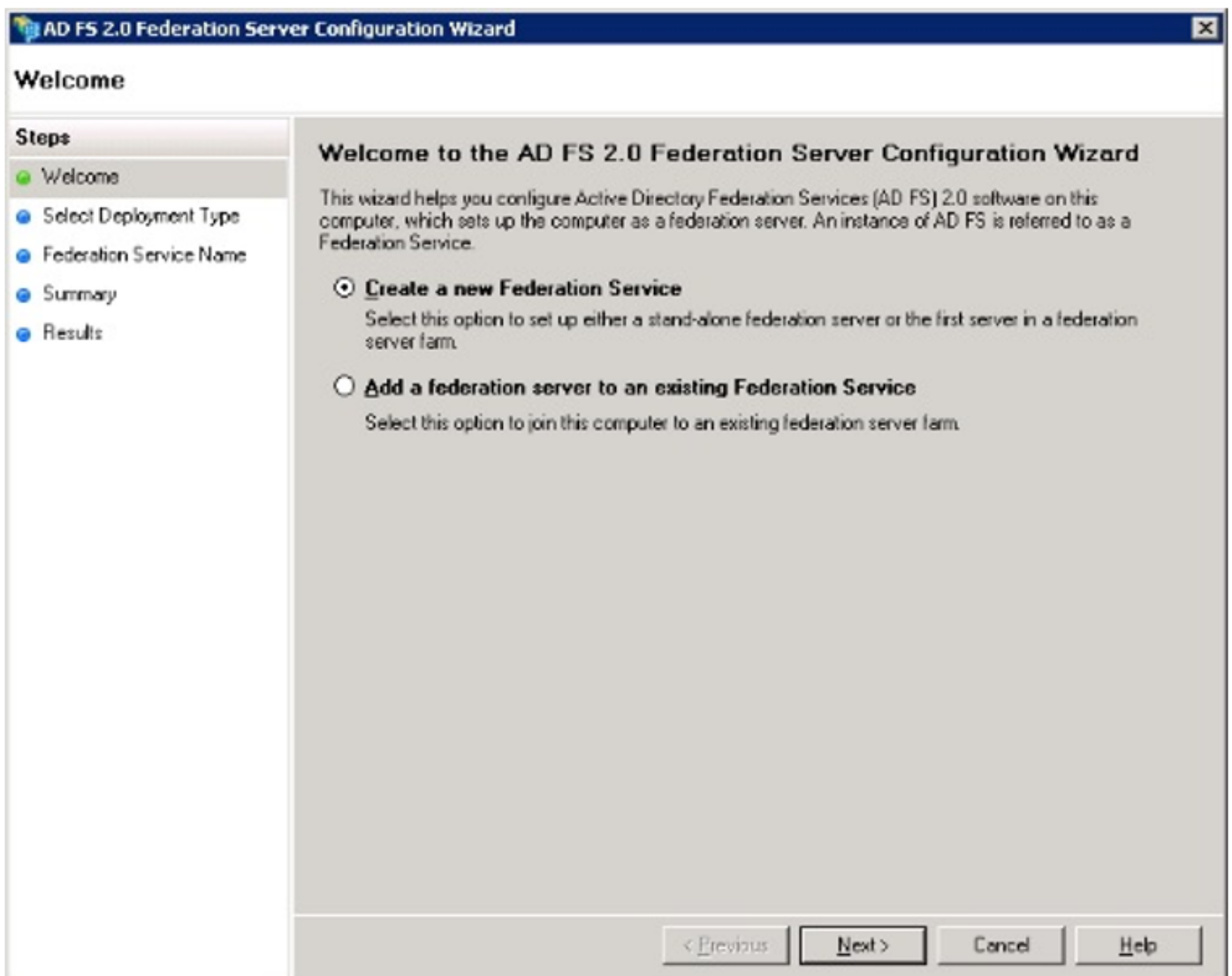
ADFS3 Initial Configuration

This section will go thru the installation of a new, Stand-alone Federation server but it can also be used to install it on a Domain Controller

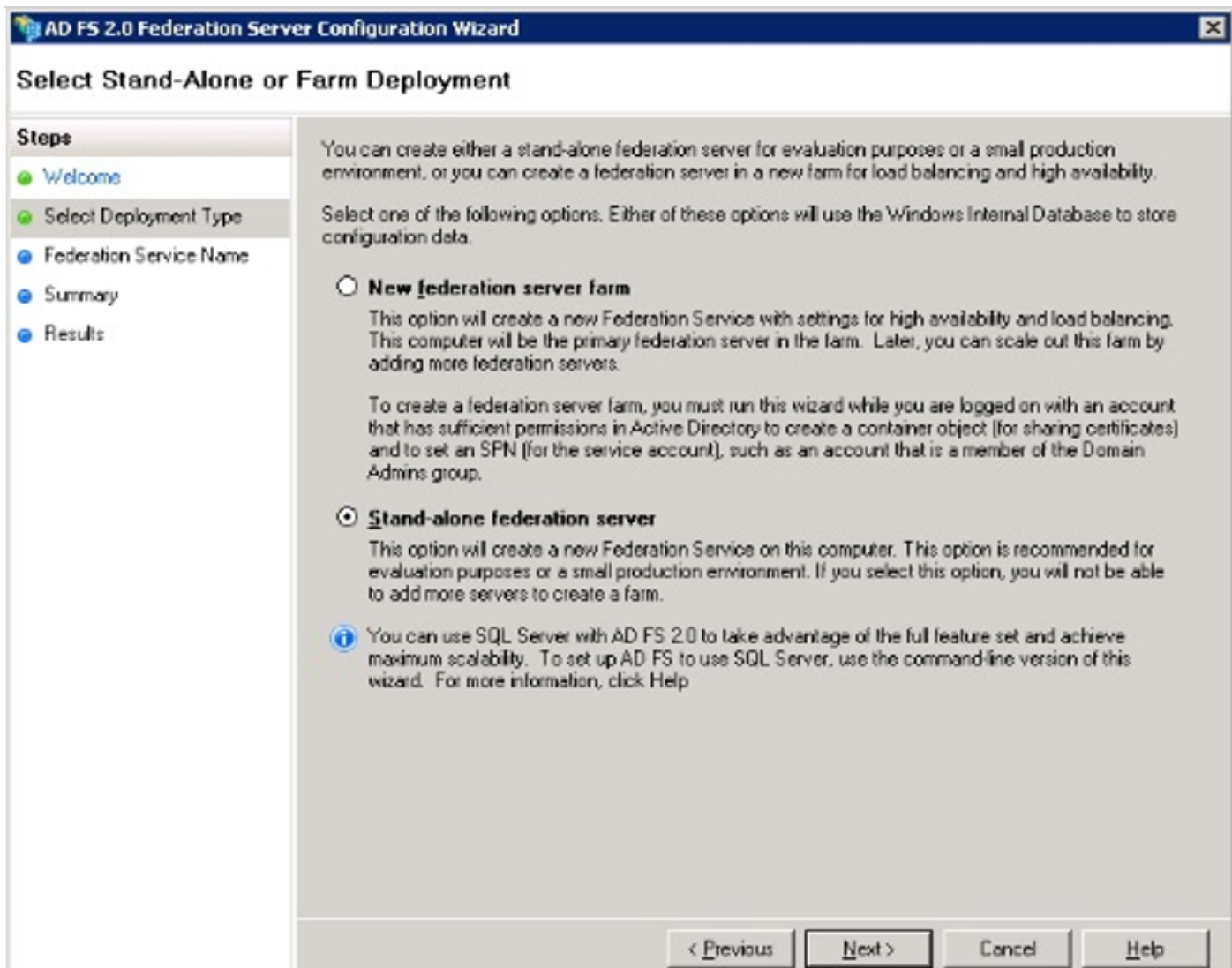
Select **Windows** and type **AD FS Management** in order to launch the ADFS Management console as shown in the image.



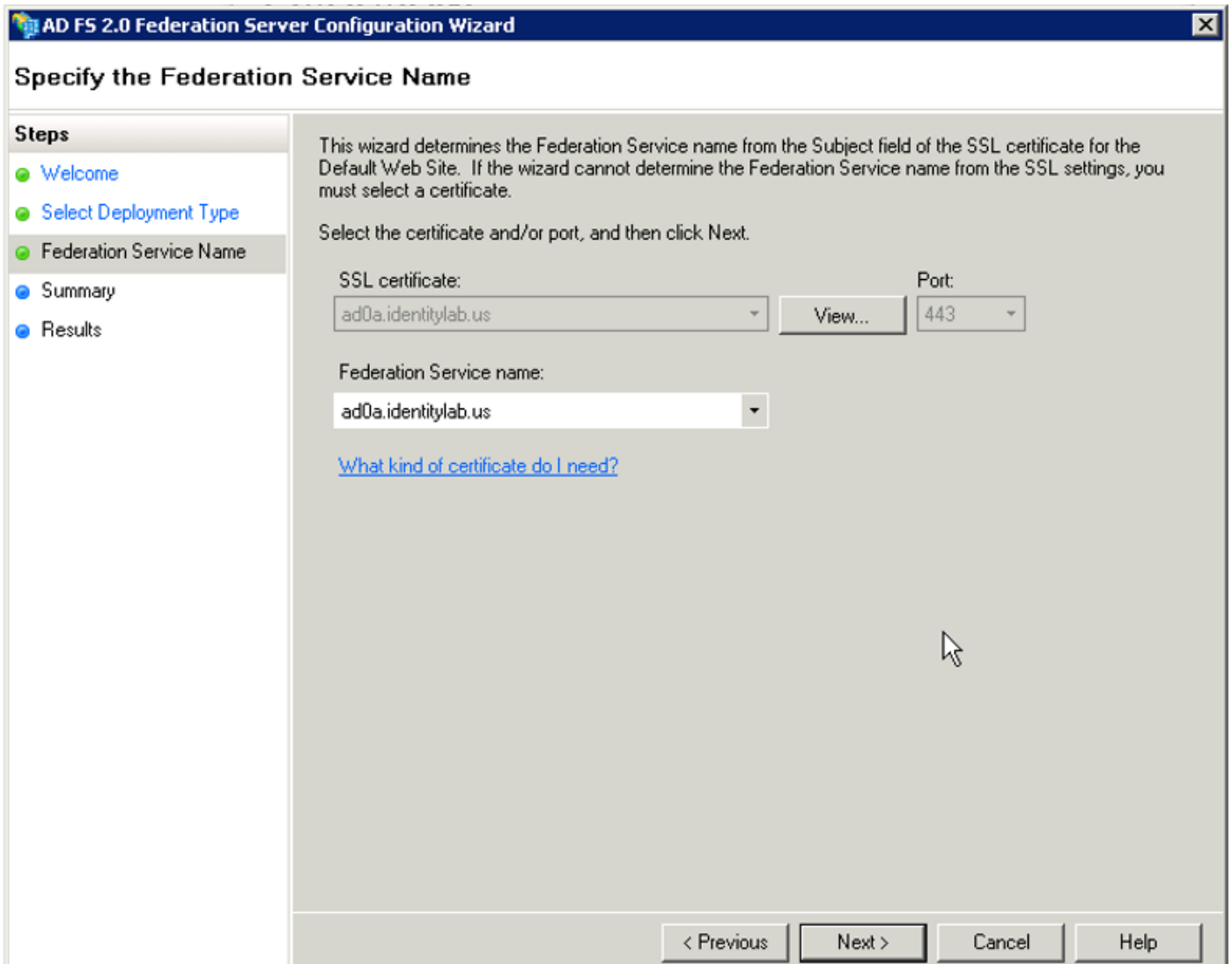
Select the **AD FS 3.0 Federation Server Configuration Wizard** option in order to start your ADFS server configuration. These screenshots represent the same steps in AD FS 3.



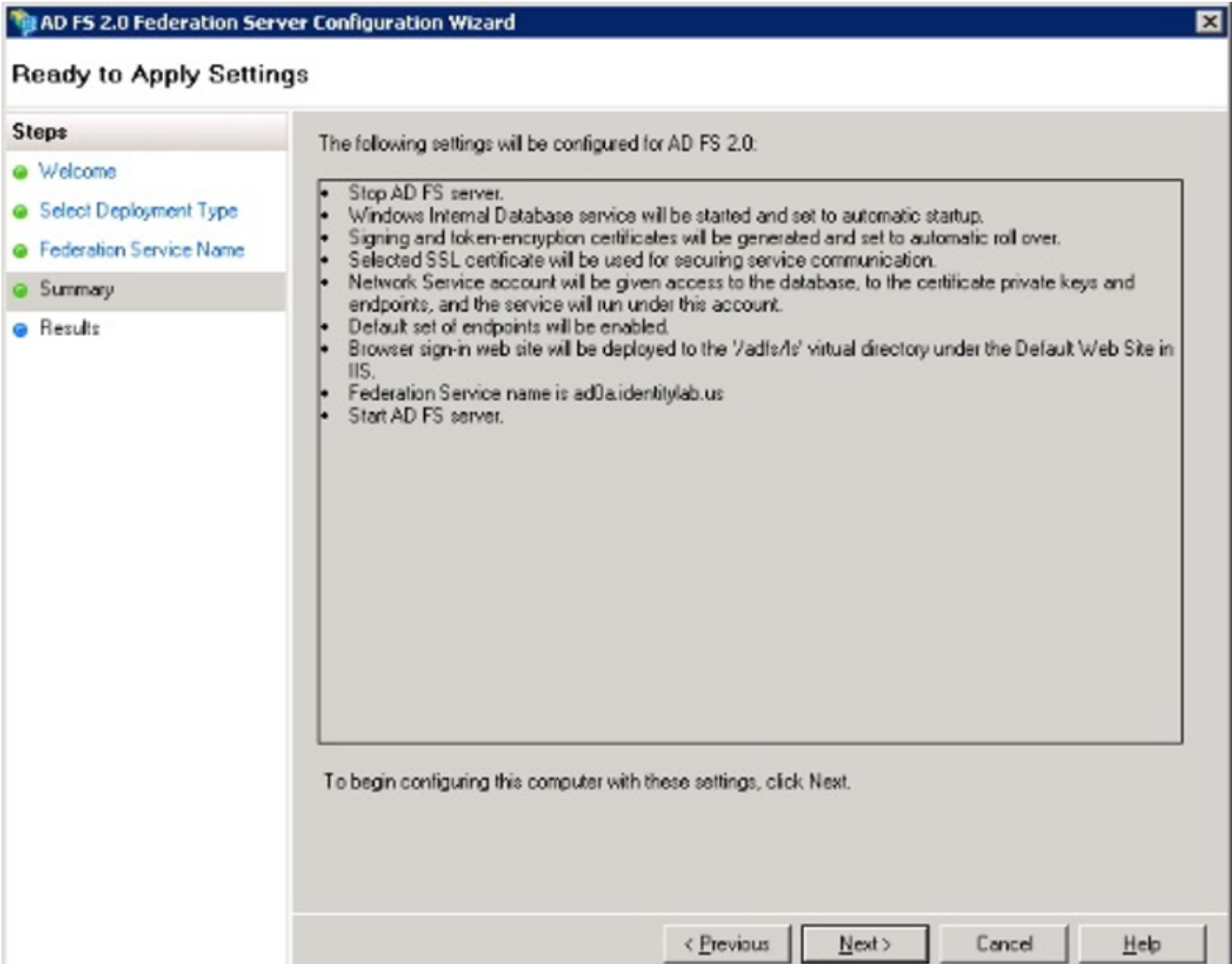
Select Create a new **Federation Service** and click **Next**.



Select Stand-alone Federation Server and click **Next** as shown in the image.



Under SSL certificate, select the self-signed certificate from the list. The Federation Service name will auto-populate. Click **Next**.



Review the settings and click **Next** in order to apply the settings.

AD FS 2.0 Federation Server Configuration Wizard

Configuration Results

Steps

- Welcome
- Select Deployment Type
- Federation Service Name
- Summary
- Results**

The following settings are being configured

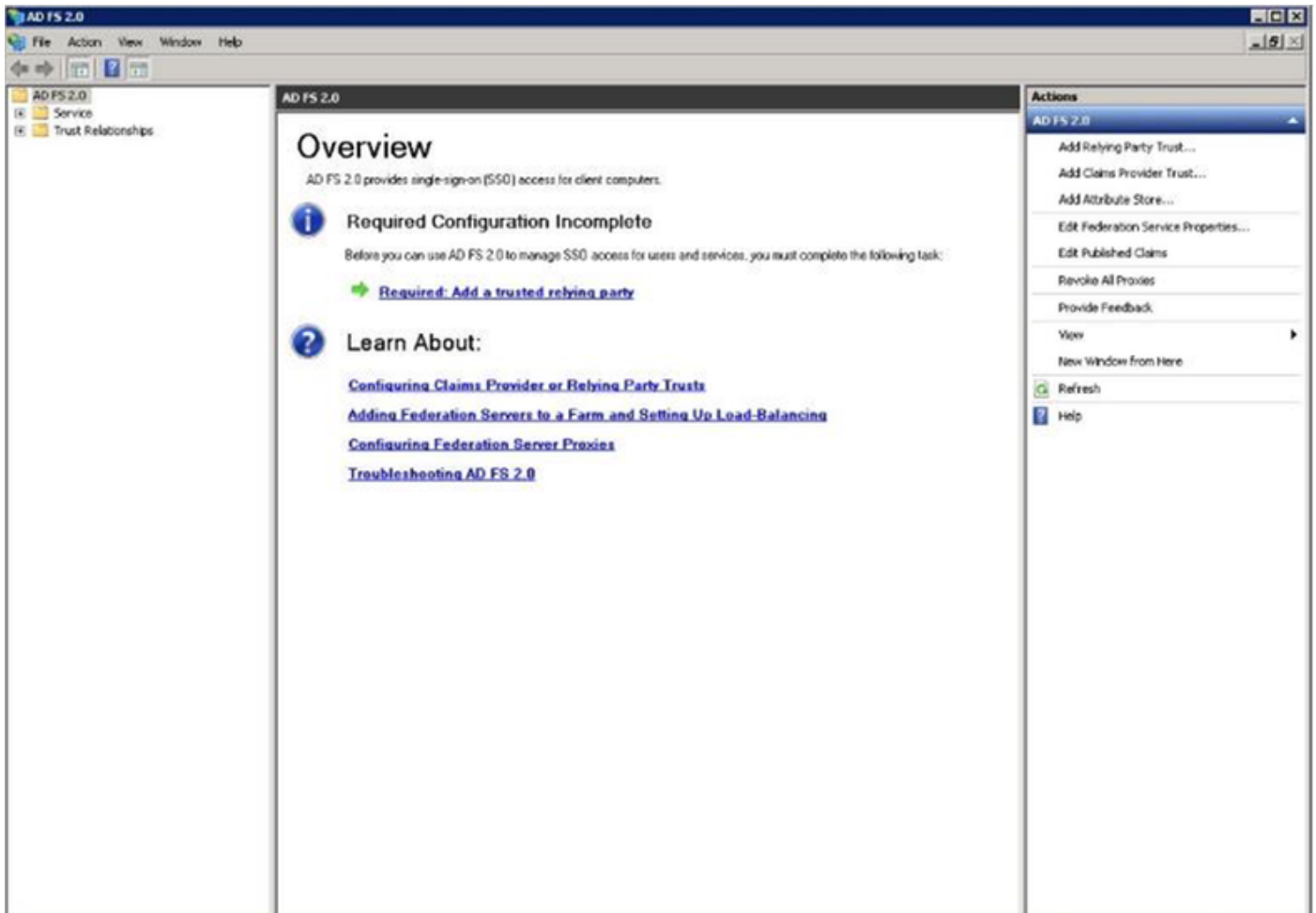
| Component | Status |
|--|------------------------|
| Stop the AD FS 2.0 Windows Service | Configuration finished |
| Install Windows Internal Database | Configuration finished |
| Start the Windows Internal Database service | Configuration finished |
| Create AD FS configuration database | Configuration finished |
| Configure service settings | Configuration finished |
| Deploy browser sign-in Web site | Configuration finished |
| Start the AD FS 2.0 Windows Service | Configuration finished |
| Create default claim set | Configuration finished |
| Create default Active Directory claim acceptance rules | Configuration finished |

You have successfully completed the AD FS 2.0 Federation Server Configuration Wizard.

To close this wizard, click Close.

Close

Confirm that all the components have completed successfully and click **Close** in order to end the wizard and return to the main management console. This might take a few minutes.



ADFS is now effectively enabled and configured as an Identity Provider (IdP). Next, you need to add CUCM as a trusted Relying partner. Before you can do this, you need to first do some configuration in CUCM Administration.

Configure SSO on CUCM with ADFS

LDAP Configuration

The cluster needs to be LDAP-integrated with Active Directory and LDAP authentication needs to be configured before going any further. Navigate to **System tab > LDAP System** as shown in the image.

LDAP System Configuration

Status



Please Delete All LDAP Directories Before Making Changes on This Page



Please Disable LDAP Authentication Before Making Changes on This Page

LDAP System Information

Enable Synchronizing from LDAP Server

LDAP Server Type

Microsoft Active Directory



LDAP Attribute for User ID

sAMAccountName



Then, navigate to **System tab > LDAP Directory**.

LDAP Directory



Save



Delete



Copy



Perform Full Sync Now



Add New

Status



Status: Ready

LDAP Directory Information

LDAP Configuration Name*

LDAP1

LDAP Manager Distinguished Name*

fhlab\administrator

LDAP Password*

.....

Confirm Password*

.....

LDAP User Search Base*

cn=users,dc=fhlab,dc=com

LDAP Custom Filter for Users

< None >

Synchronize*

Users Only Users and Groups

LDAP Custom Filter for Groups

< None >

LDAP Directory Synchronization Schedule

Perform Sync Just Once

Perform a Re-sync Every*

7

DAY



Next Re-sync Time (YYYY-MM-DD hh:mm)*

2020-05-24 00:00

| Standard User Fields To Be Synchronized | | | |
|--|-----------------|--|----------------|
| Cisco Unified Communications Manager User Fields | LDAP Attribute | Cisco Unified Communications Manager User Fields | LDAP Attribute |
| User ID | sAMAccountName | First Name | givenName |
| Middle Name | middleName | Last Name | sn |
| Manager ID | manager | Department | department |
| Phone Number | telephoneNumber | Mail ID | mail |
| Title | title | Home Number | homephone |
| Mobile Number | mobile | Pager Number | pager |
| Directory URI | mail | Display Name | displayName |

LDAP Server Information

Host Name or IP Address for Server* LDAP Port* Use TLS

[Add Another Redundant LDAP Server](#)

Save
Delete
Copy
Perform Full Sync Now
Add New

After Active Directory users have been synchronized with CUCM, LDAP authentication needs to be configured.

The screenshot shows the Cisco Unified CM Administration web interface. The page title is "Cisco Unified CM Administration" and the sub-header is "LDAP Authentication". The status is "Ready". Under "LDAP Authentication for End Users", the checkbox "Use LDAP Authentication for End Users" is checked. The "LDAP Manager Distinguished Name" is "fhlab/Administrator", the "LDAP Password" and "Confirm Password" are masked with asterisks, and the "LDAP User Search Base" is "cn=users,dc=fhlab,dc=com". The "LDAP Server Information" section shows the "Host Name or IP Address for Server" as "10.89.228.226", the "LDAP Port" as "389", and "Use TLS" is unchecked. There is an "Add Another Redundant LDAP Server" button.

An end-user in CUCM needs to have certain Access Control Groups assigned to his/her end-user profile. The ACG is Standard CCM Super Users. The user will be used to test SSO when the environment is ready.

End User Configuration Related Links: [Back to Find List Users](#)

Confirm MLPP Password
 MLPP Precedence Authorization Level

CAPF Information

Associated CAPF Profiles [View Details](#)

Permissions Information

Groups:

- Standard CCM End Users
- Standard CCM Super Users**
- Standard CTI Allow Control of All Devices
- Standard CTI Enabled

[View Details](#)

Roles:

- Standard AXL API Access
- Standard Admin Rep Tool Admin
- Standard CCM Admin Users
- Standard CCM End Users
- Standard CCMADMIN Administration

[View Details](#)

Conference Now Information

Enable End User to Host Conference Now
 Meeting Number
 Attendees Access Code

CUCM Metadata

This section will show the process for the CUCM Publisher.

The first task is to get the CUCM metadata, for that you need to browse to the URL; <https://<CUCM Pub FQDN>:8443/ssosp/ws/config/metadata/sp> or it can be downloaded from **System tab > SAML Single Sign-on**. This can be done per node or Cluster Wide. Preferable to do this Cluster Wide.

System > Call Routing > Media Resources > ... > Device > User Manager > ... > SAML Administration

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)

Status

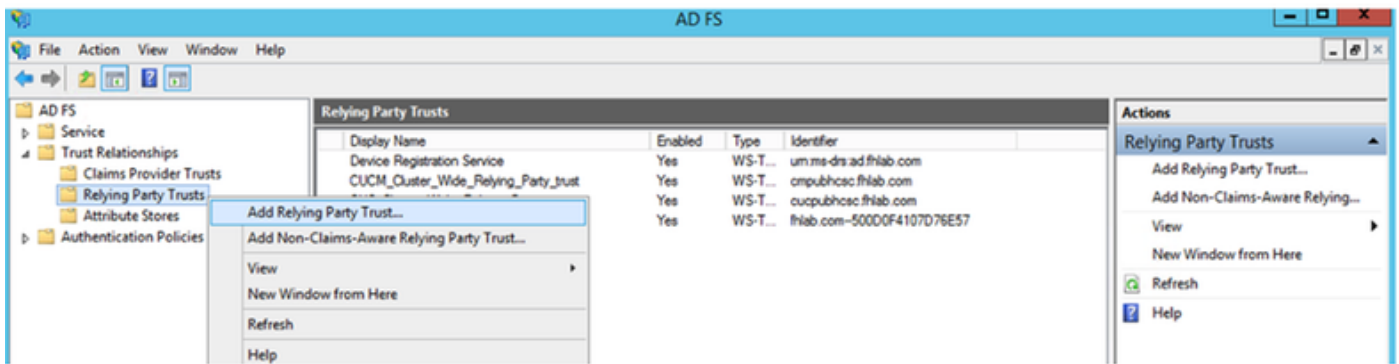
RTMT is enabled for SSO. You can change SSO for RTMT [here](#).
 SAML SSO enabled

| Server Name | SSO Status | Re-Import Metadata | Last Metadata Import | Export Metadata | Last Metadata Export | SSO Test |
|----------------------|------------|--------------------|-------------------------------|-----------------|-------------------------------|---|
| cmpubhcsc.fhlab.com | SAML | N/A | April 20, 2020 2:00:57 PM PDT | File | April 18, 2020 8:05:38 PM PDT | Passed - April 20, 2020 2:02:15 PM PDT <input type="button" value="Run SSO Test..."/> |
| cmsubhcsc.fhlab.com | SAML | IdP | April 20, 2020 2:00:57 PM PDT | File | April 18, 2020 8:05:37 PM PDT | Passed - April 20, 2020 1:49:45 PM PDT <input type="button" value="Run SSO Test..."/> |
| imppubhcsc.fhlab.com | SAML | IdP | April 20, 2020 2:00:57 PM PDT | File | April 18, 2020 8:05:37 PM PDT | Passed - May 24, 2020 12:02:56 PM PDT <input type="button" value="Run SSO Test..."/> |
| impsubhcsc.fhlab.com | SAML | IdP | April 20, 2020 2:00:57 PM PDT | File | April 18, 2020 8:05:37 PM PDT | Passed - May 24, 2020 12:03:26 PM PDT <input type="button" value="Run SSO Test..."/> |

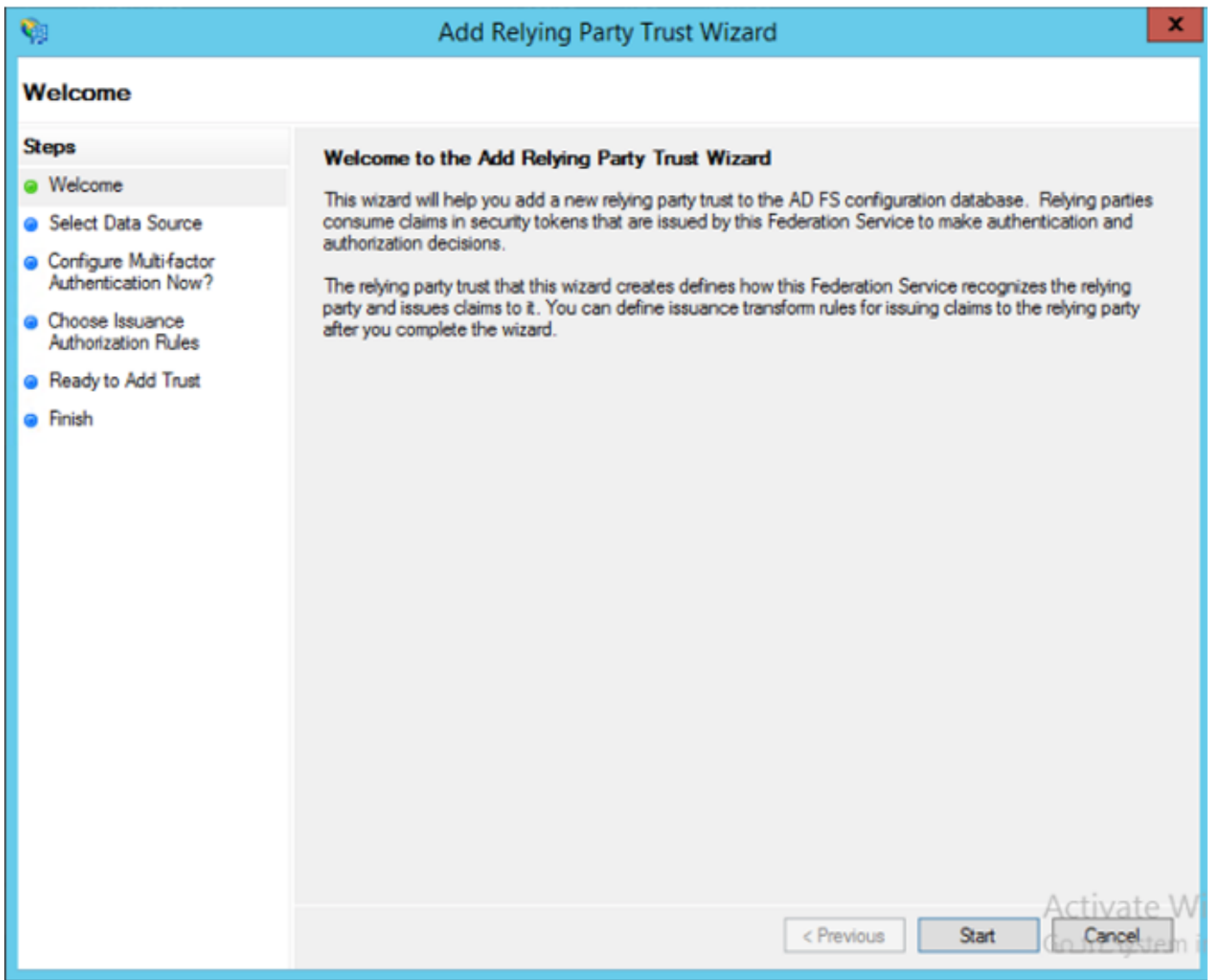
Save the data locally with a meaningful name such as sp_cucm0a.xml, you are going to need it after.

Configure ADFS Relying Party

Flip back to the AD FS 3.0 Management console.

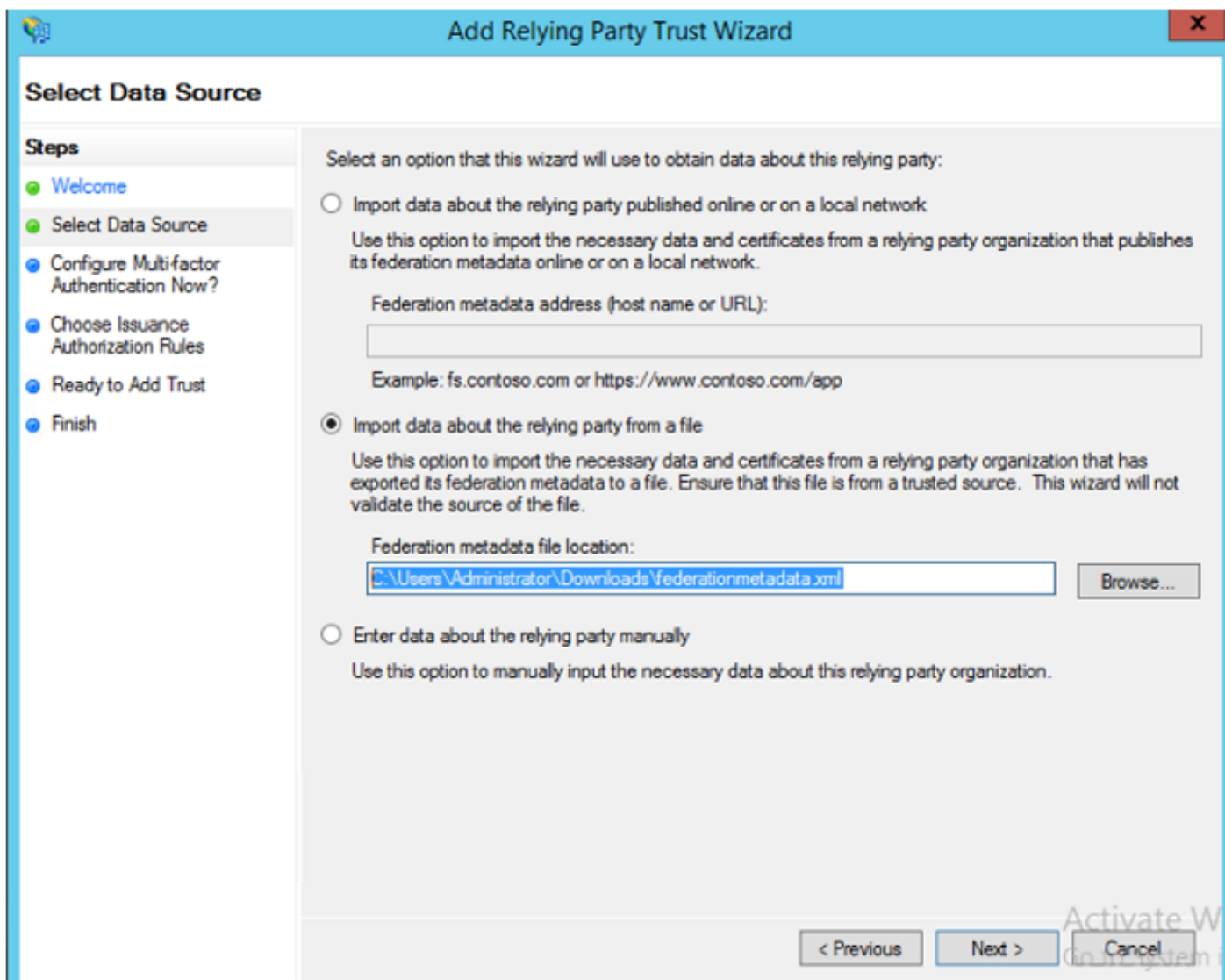


Click on **Add Relying Party Trust Wizard**.

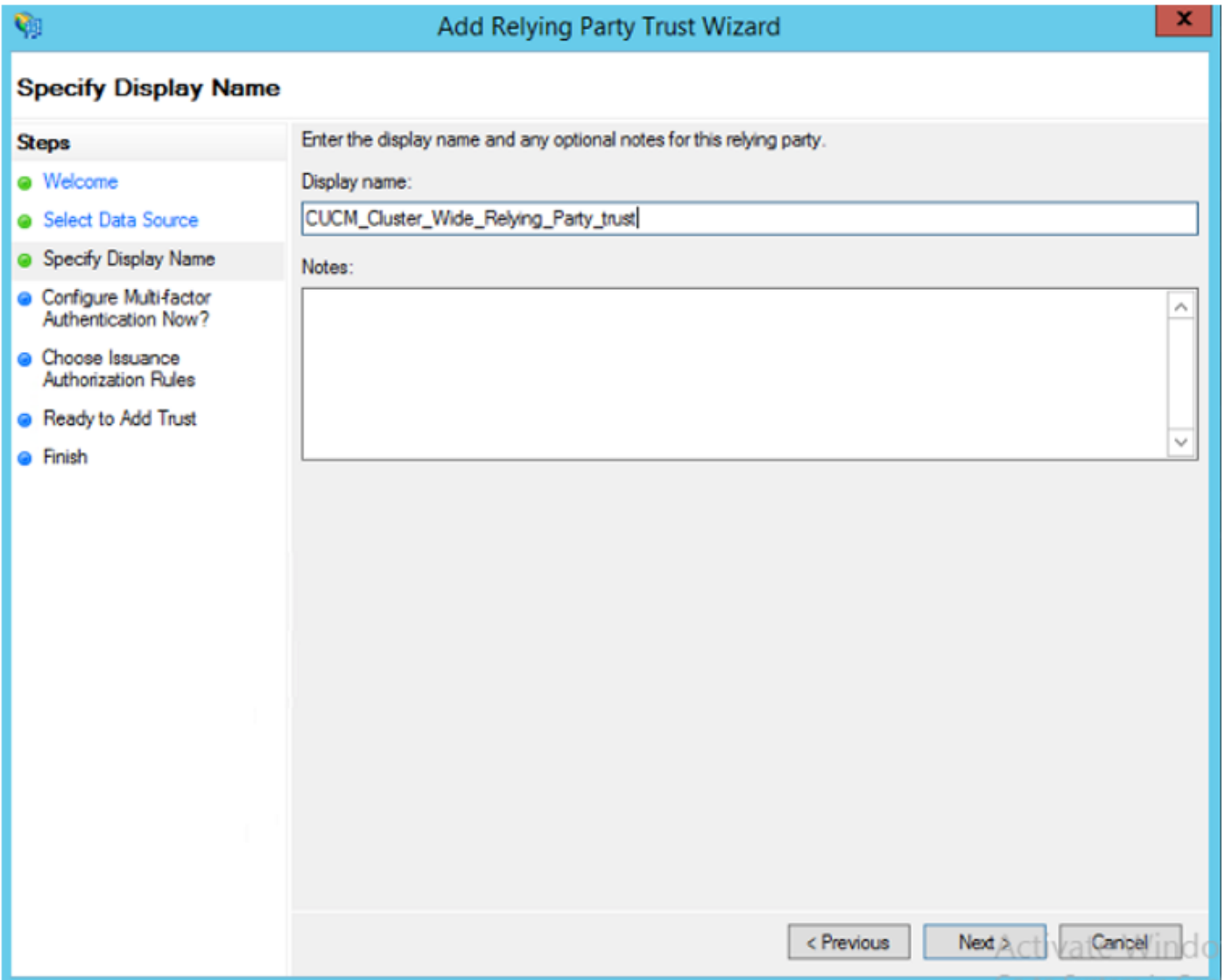


Click **Start** to continue.

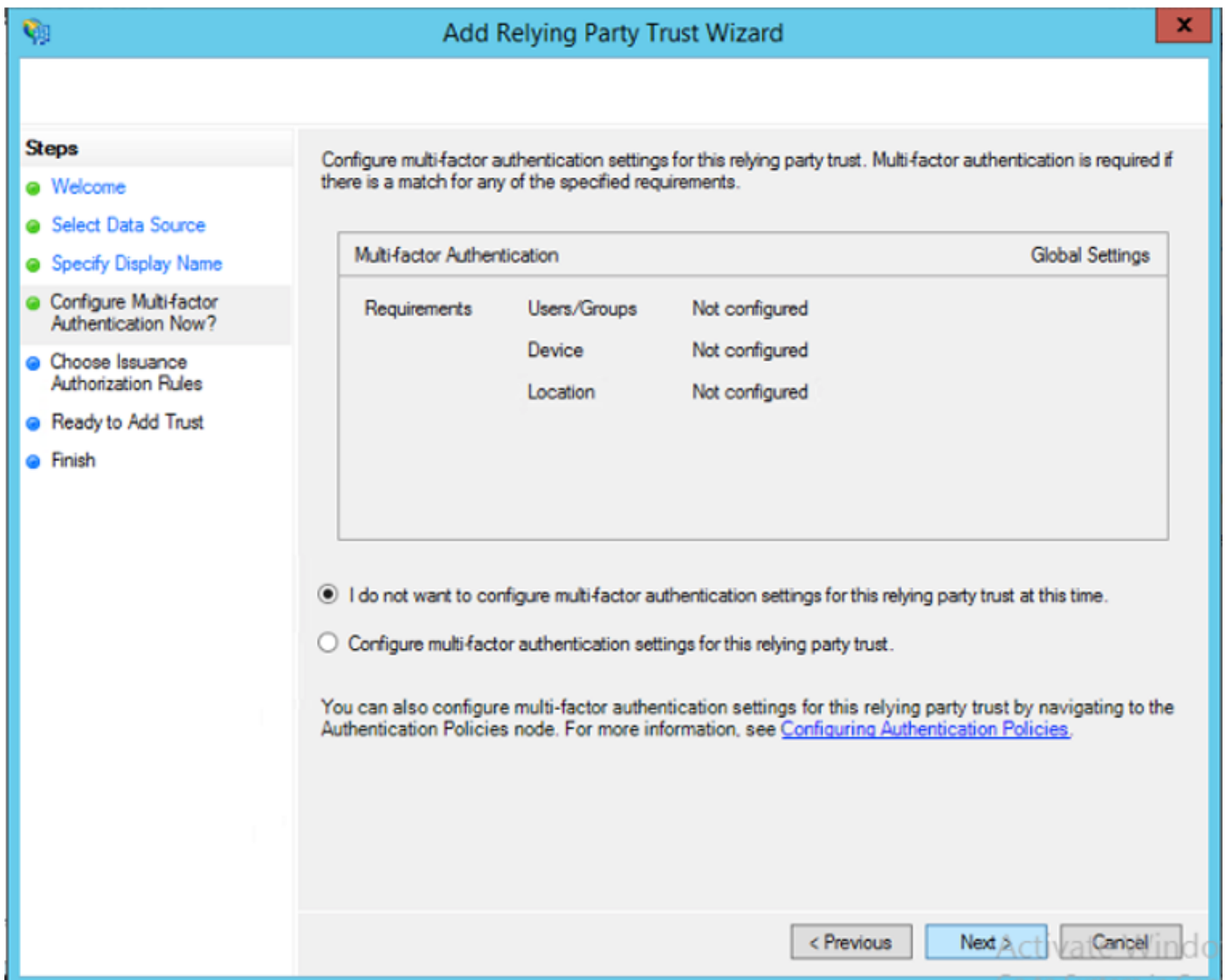
Select the **federationmetadata.xml** metadata XML file that you saved earlier and click **Next**.



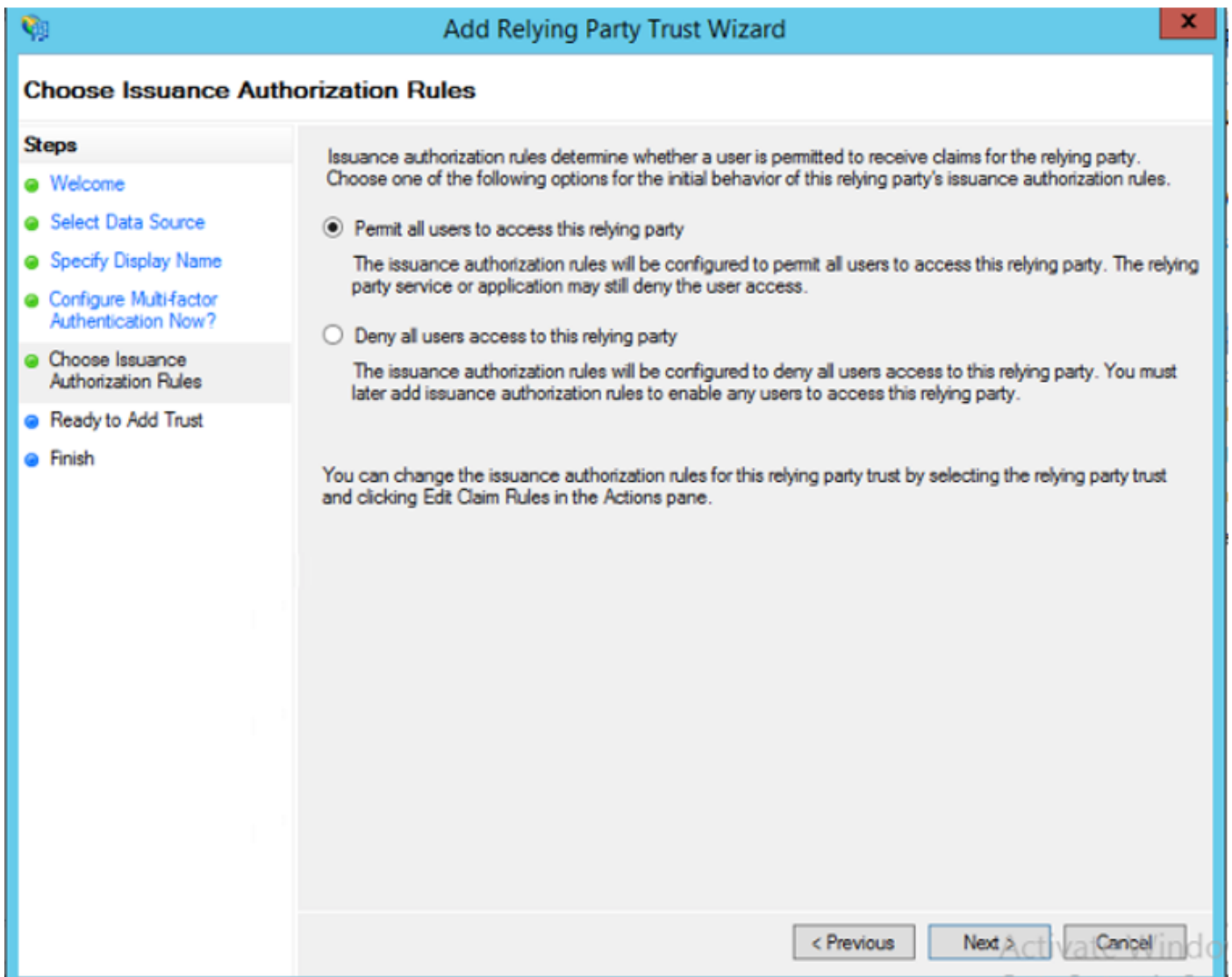
Use **CUCM_Cluster_Wide_Relying_Party_trust** as the display name and click **Next**.



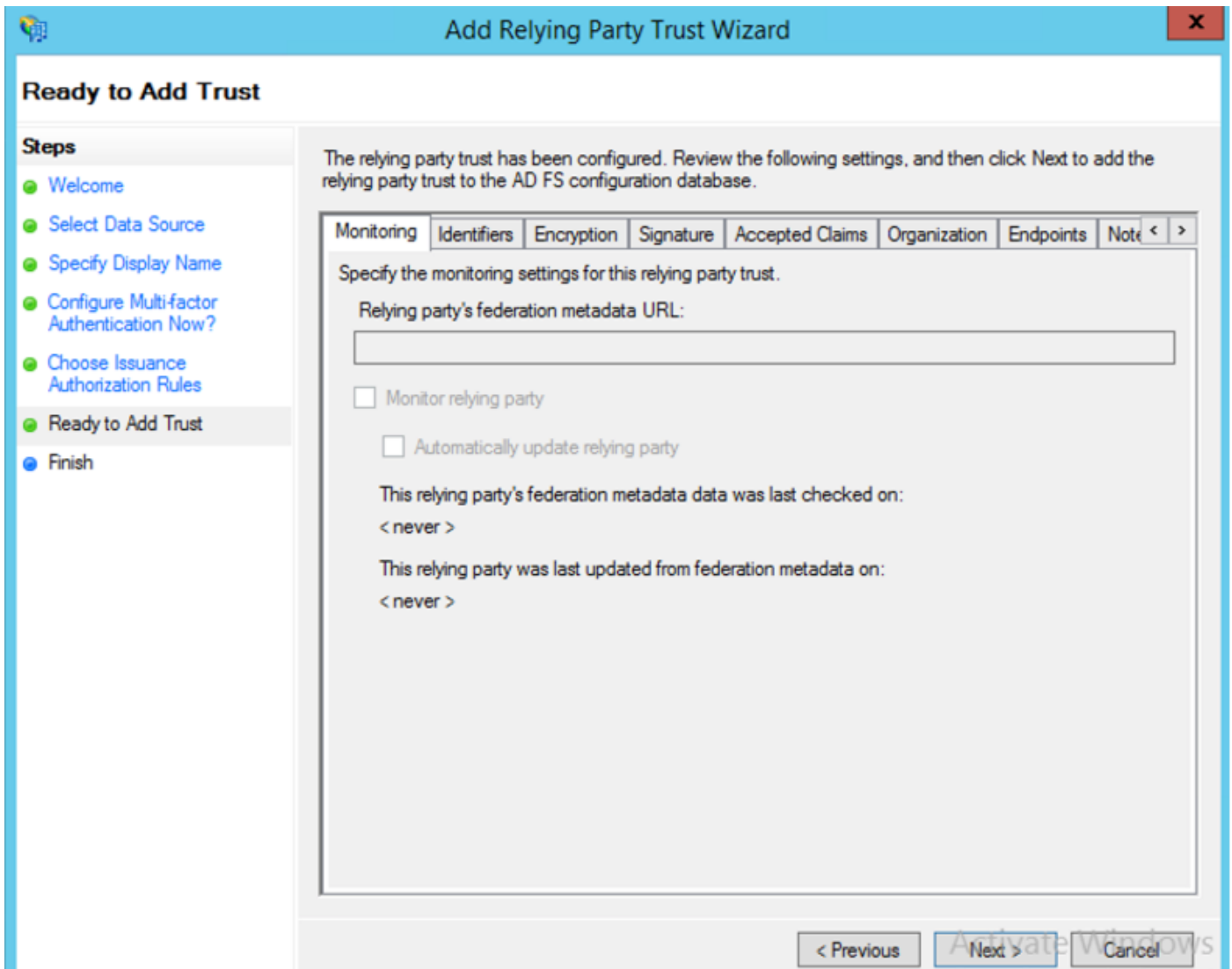
Select the first option and click **Next**.



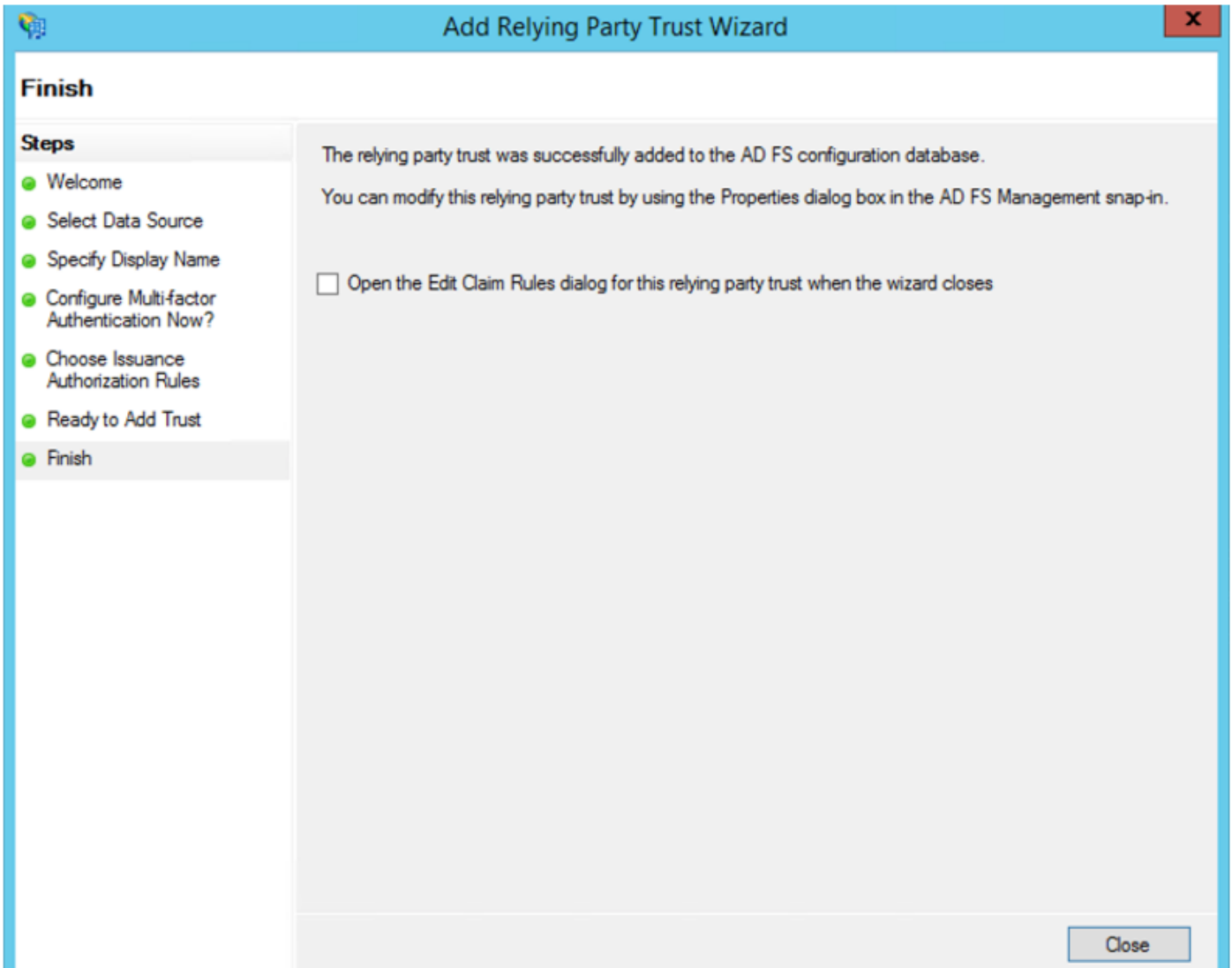
Select **Permit all users to access this relying party** and click **Next** as shown in the image.



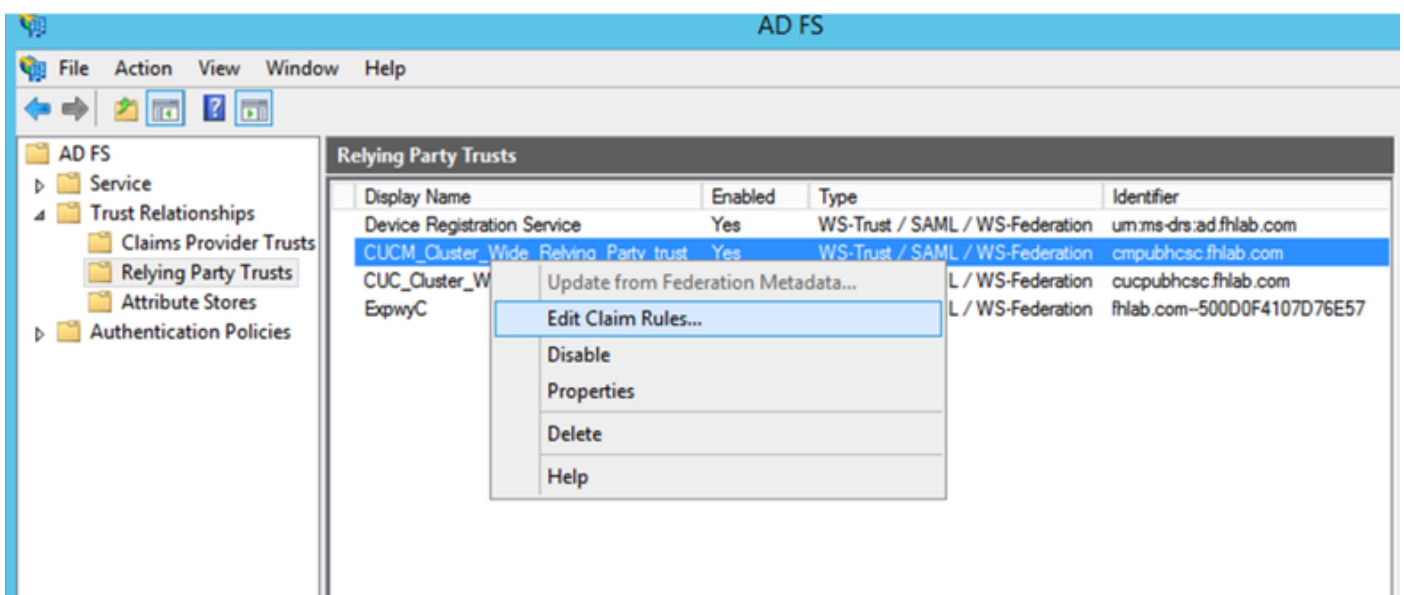
Review the configuration and click **Next** as shown in the image.



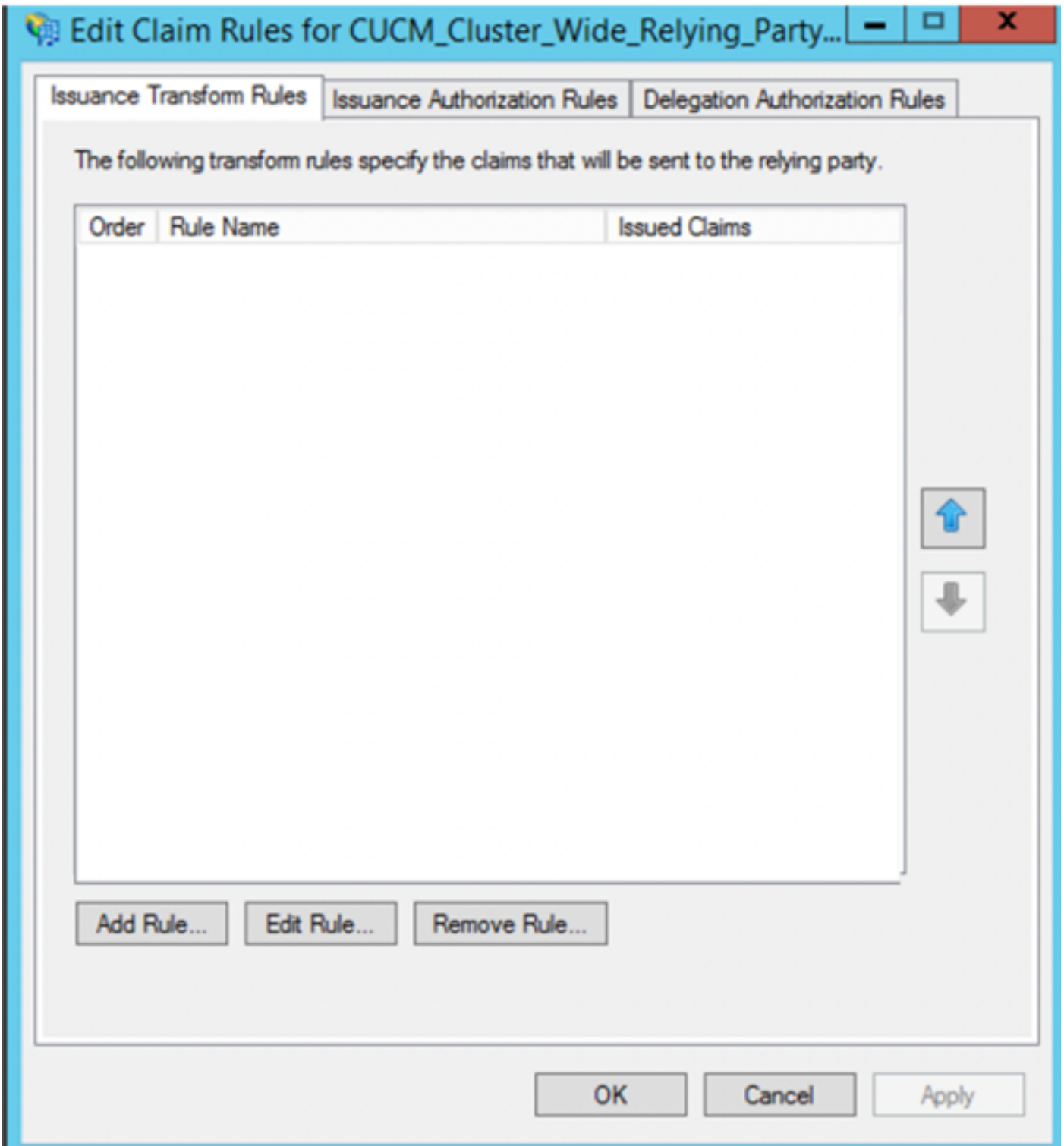
Uncheck the box and click **Close**.



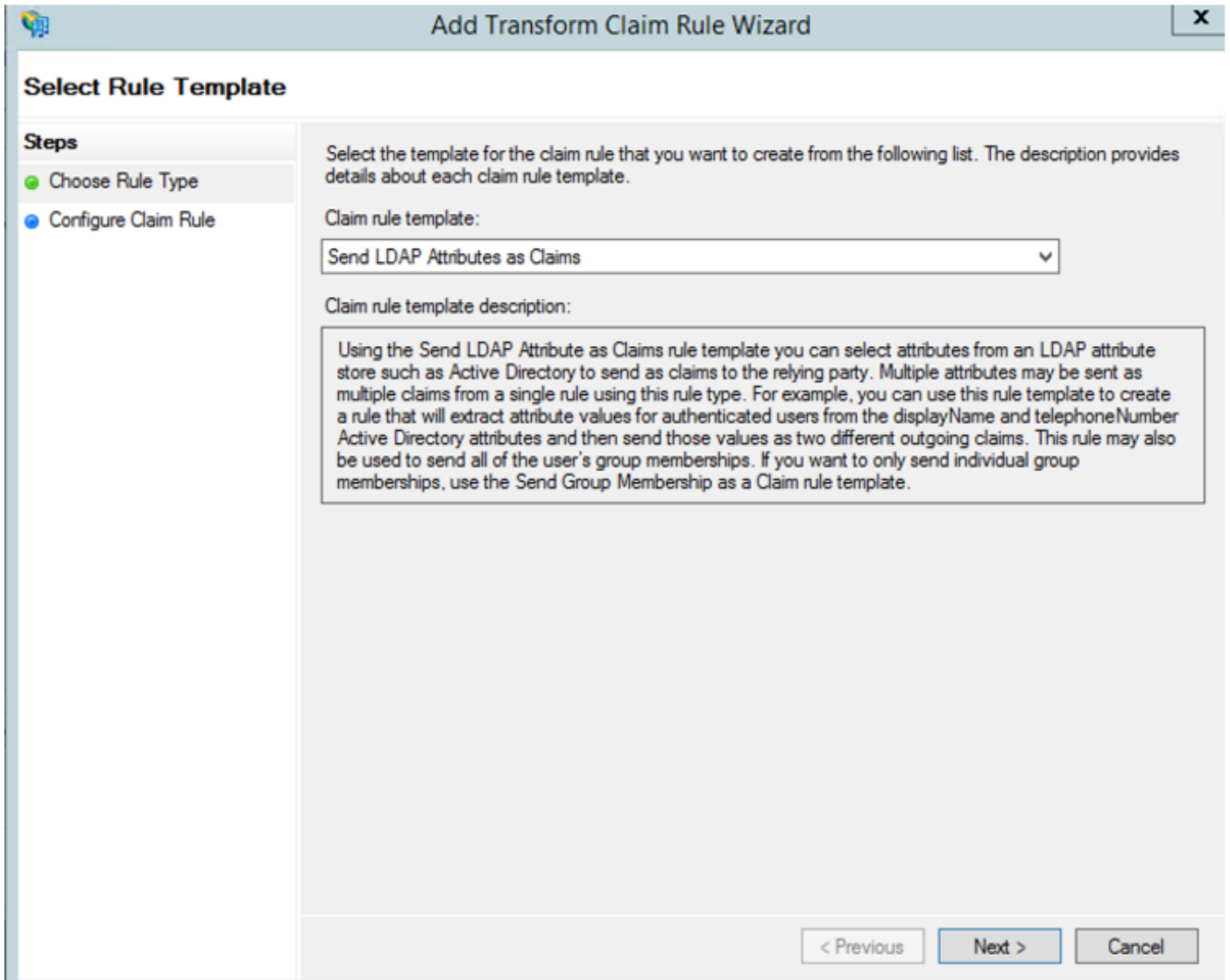
With the secondary mouse button select the **Relying Party Trust** you just created and **Edit Claim Rules** configuration as shown in the image.



Click **Add Rule** as shown in the image.



Select **Send LDAP Attributes as Claims** and click **Next**.



Configure these parameters:

Claim Rule Name: NameID

Attribute Store: Active Directory (double Click the drop-down menu arrow)

LDAP Attribute: SAM-Account-Name

Outgoing Claim Type: uid

Click **FINISH/OK** to continue.

Please note that uid is not in lower case and does not already exist in the drop-down menu. Type it.

Edit Rule - NameID

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:

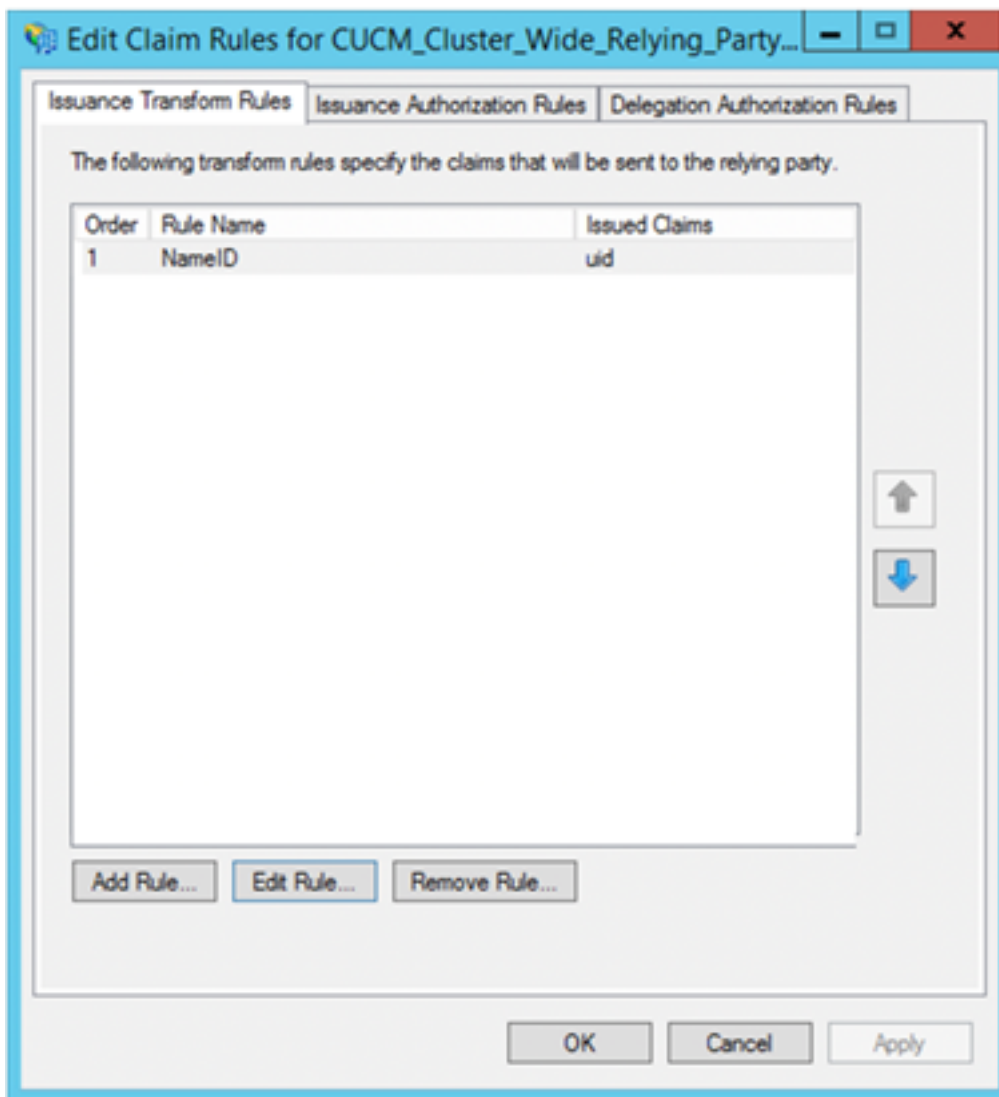
Rule template: Send LDAP Attributes as Claims

Attribute store:

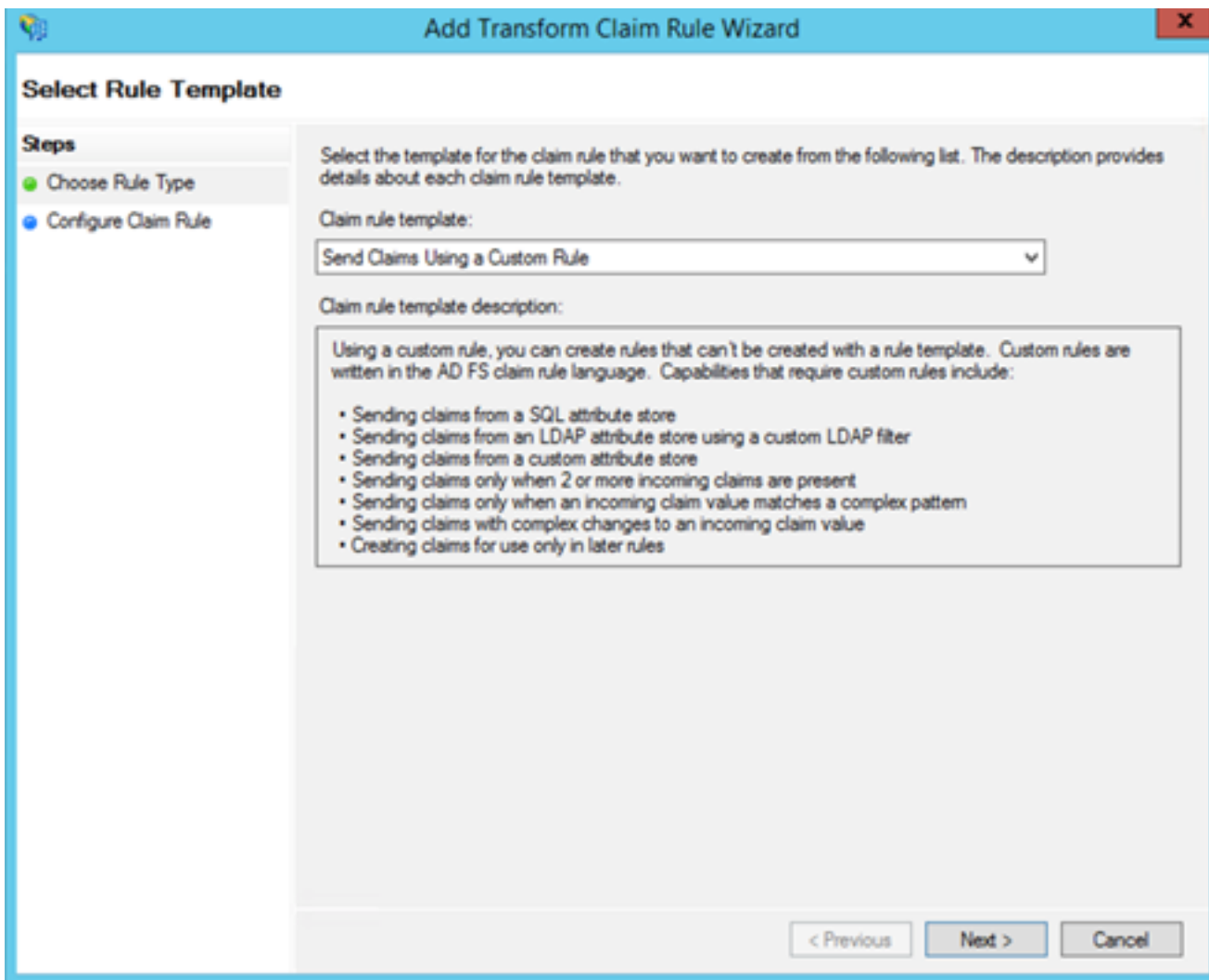
Mapping of LDAP attributes to outgoing claim types:

| | LDAP Attribute (Select or type to add more) | Outgoing Claim Type (Select or type to add more) |
|---|---|--|
| ▶ | SAM-Account-Name | uid |
| * | | |

Click **Add Rule** again in order to add another rule.



Select **Send Claims Using a Custom Rule** and click **Next**.



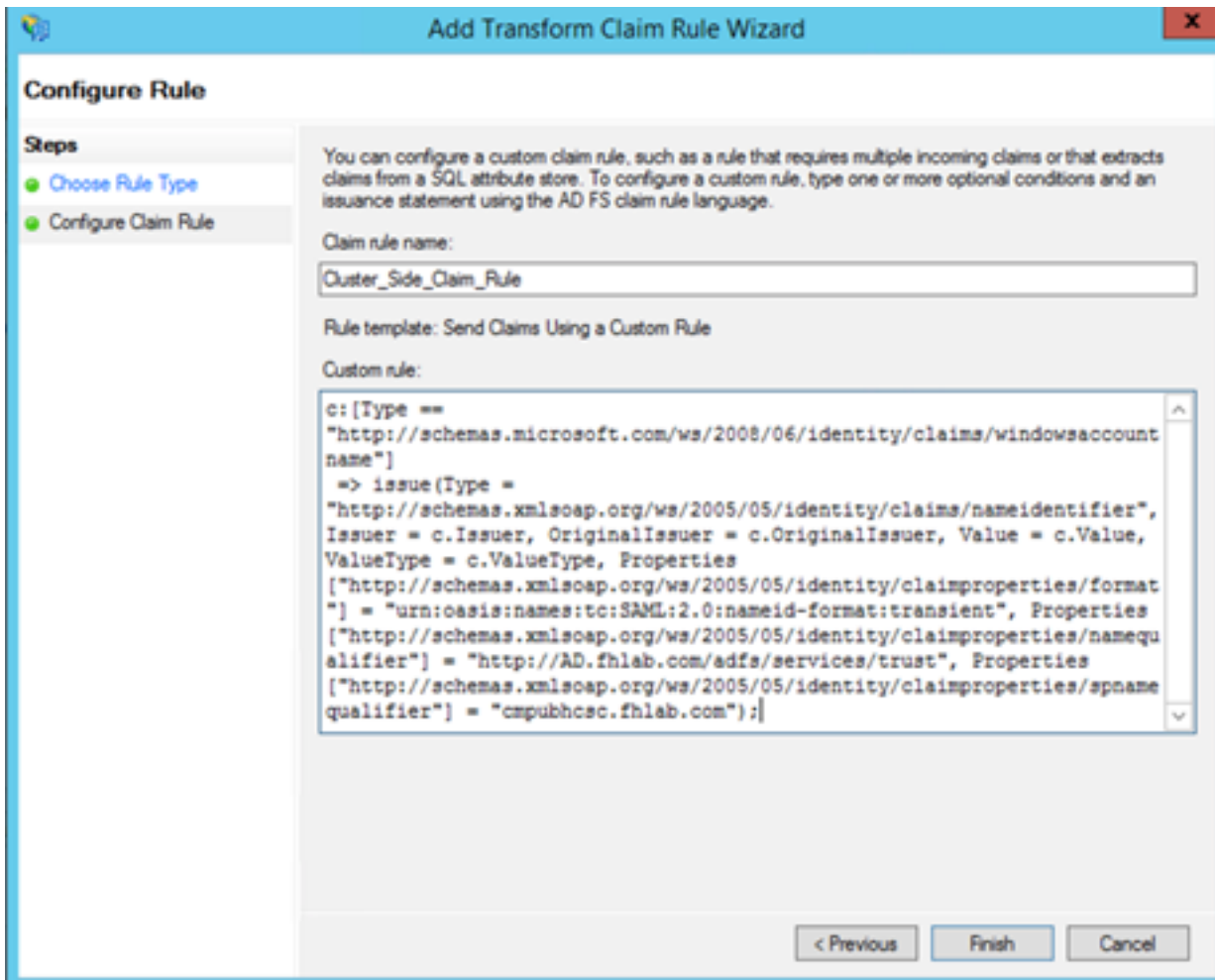
Create a custom rule called Cluster_Side_Claim_Rule.

Copy and paste this text in the rule window directly from here. Sometimes, quotes are changed if edited on a text editor and that will make the rule to fail when you test SSO:

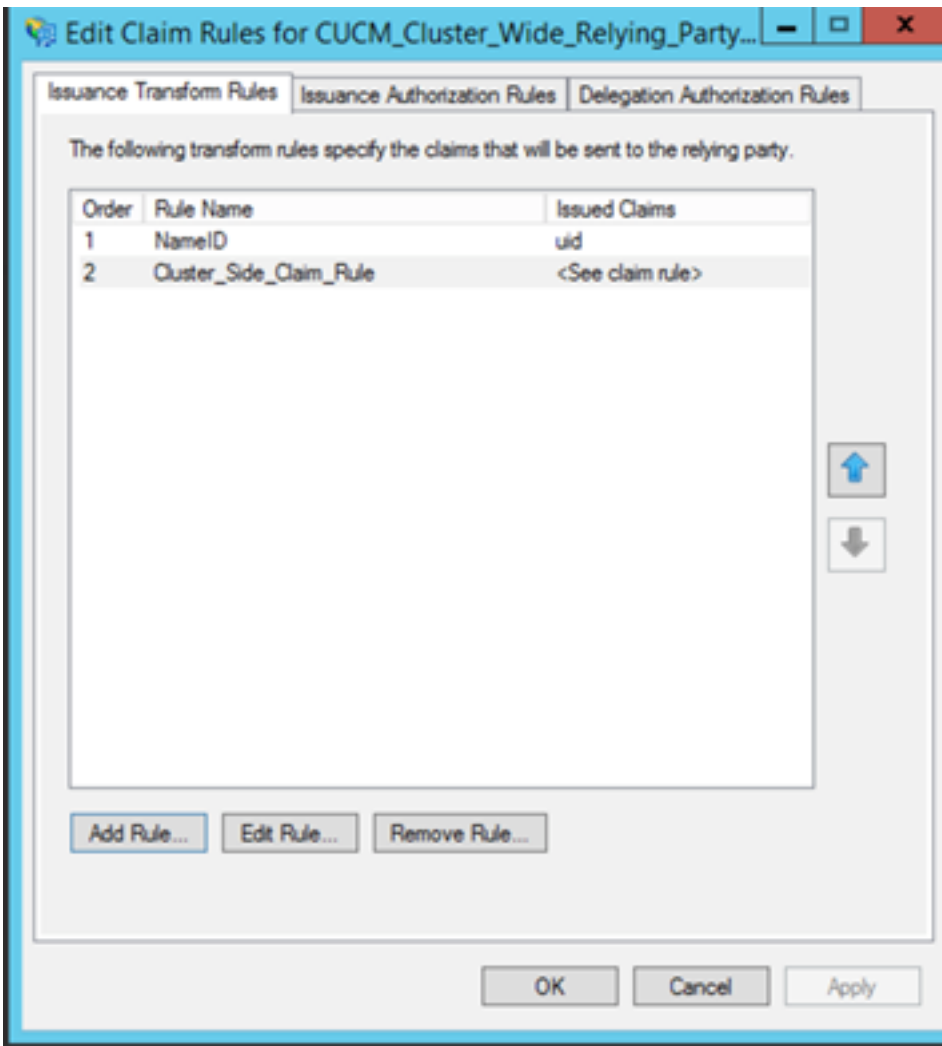
```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties[ "http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format" ] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties[ "http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier" ] =
"http://<ADFS FQDN>/adfs/com/adfs/services/trust",
Properties[ "http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier" ] =
"<CUCM Pub FQDN>");

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://AD.fhlab.com/adfs/services/trust",
Properties[ "http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier" ] =
"cmpubhcsc.fhlab.com");
```

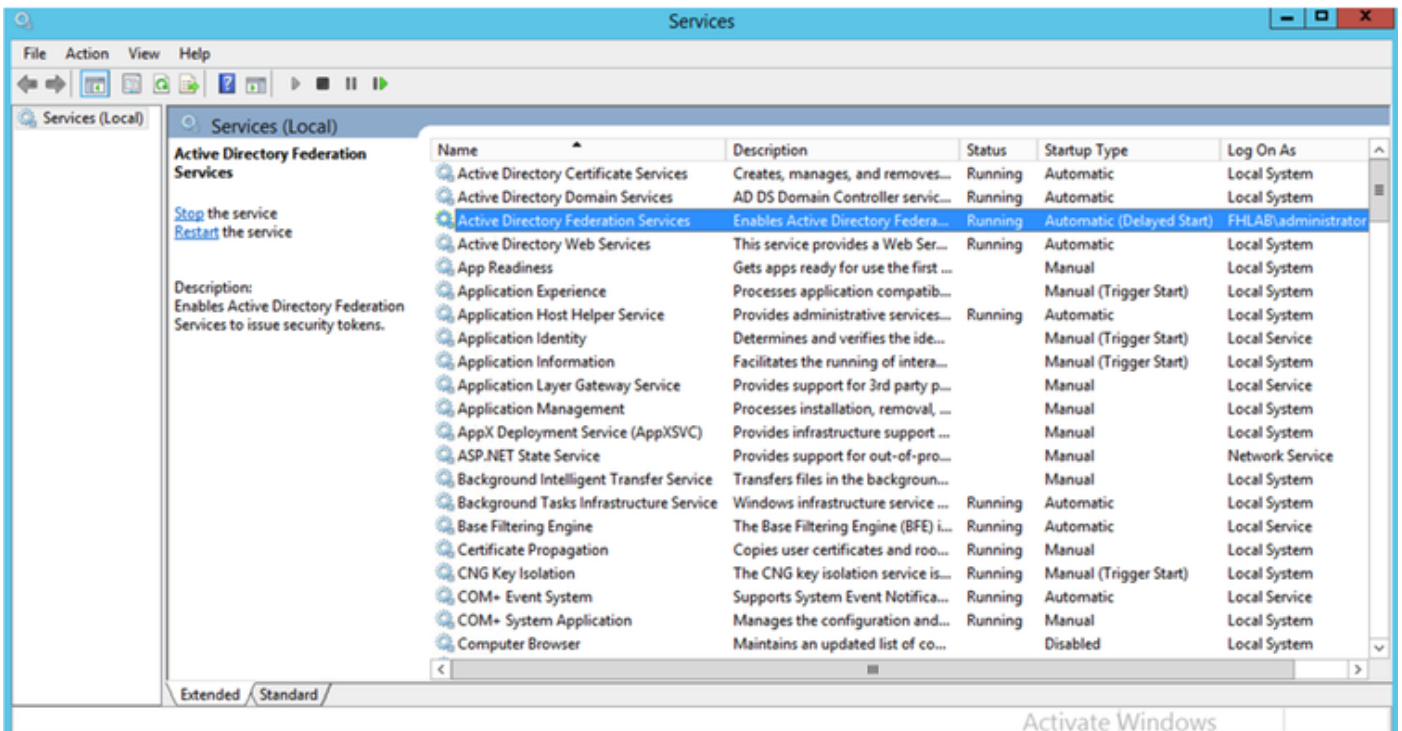
Click **Finish** to continue.



You should now have two rules defined on ADFS. Click **Apply** and **OK** to close the rules window.



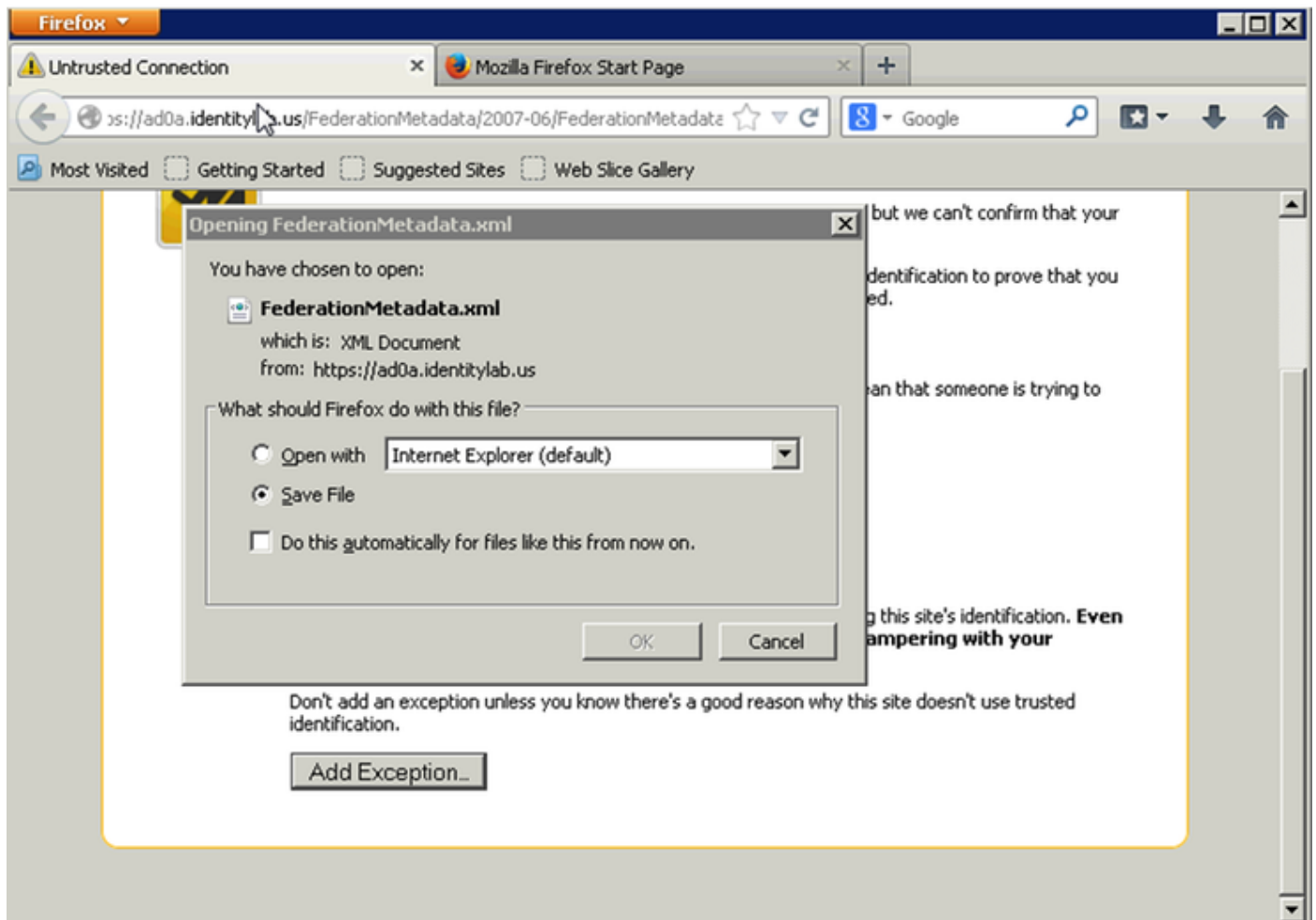
CUCM is now successfully added as a trusted relying party to ADFS.



Before you continue, please Restart the ADFS service. Navigate to **Start Menu > Administrative Tools > Services**.

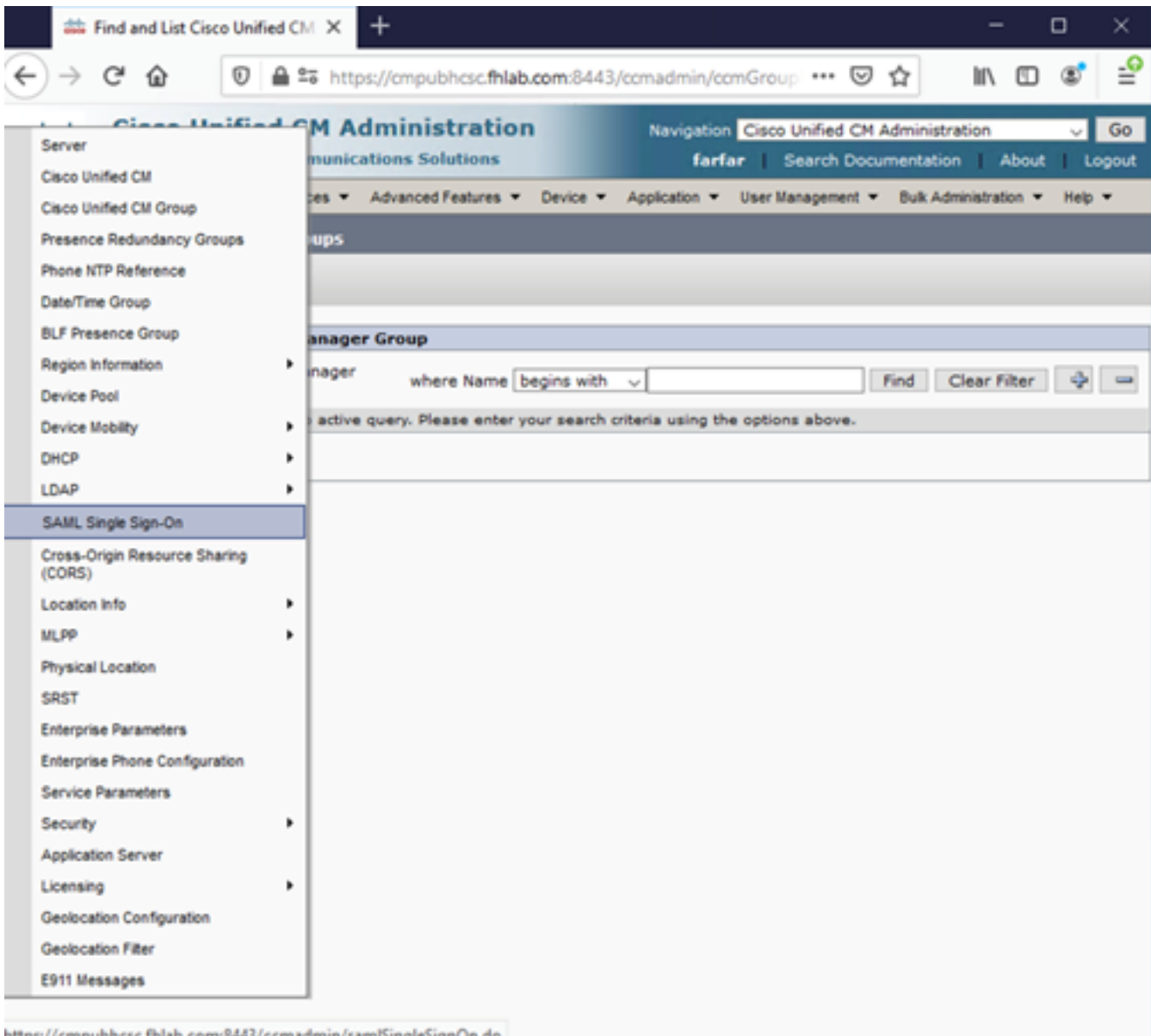
IDP Metadata

You need to provide CUCM with information about our IdP. This information is exchanged using XML metadata. Ensure to perform this step on the server where ADFS is installed.



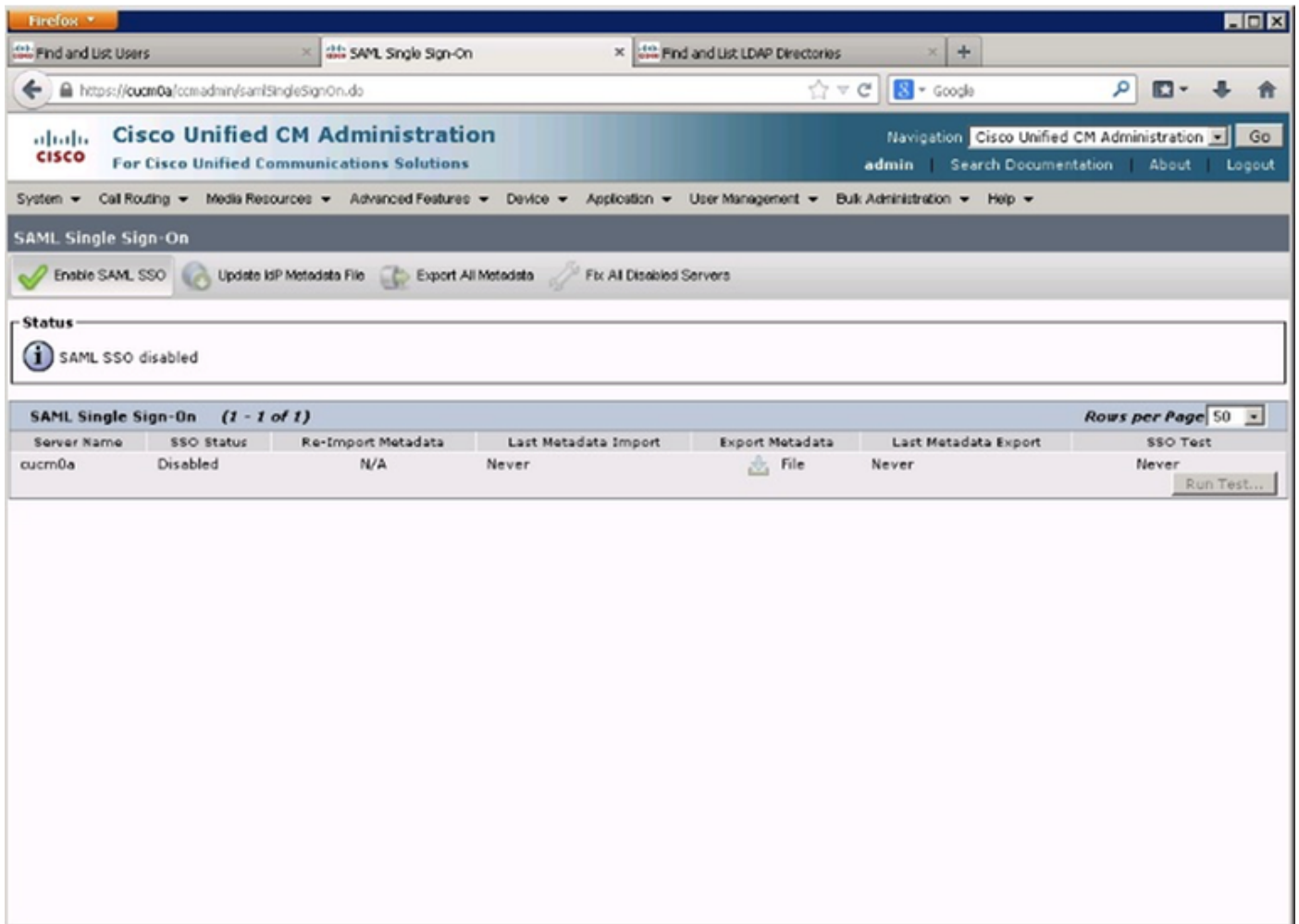
First, you need to connect to the ADFS (IdP) using a Firefox browser to download the XML metadata. Open a browser to <https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml> and SAVE the metadata to a local folder.

Now, navigate to CUCM configuration to the system **Menu > SAML Single Sign-On menu**.



<https://cmubhsc.fhlab.com:8443/ccadmin/samlSingleSignOn.do>

Flip back to the CUCM Administration and select **SYSTEM > SAML Single Sign-On**.



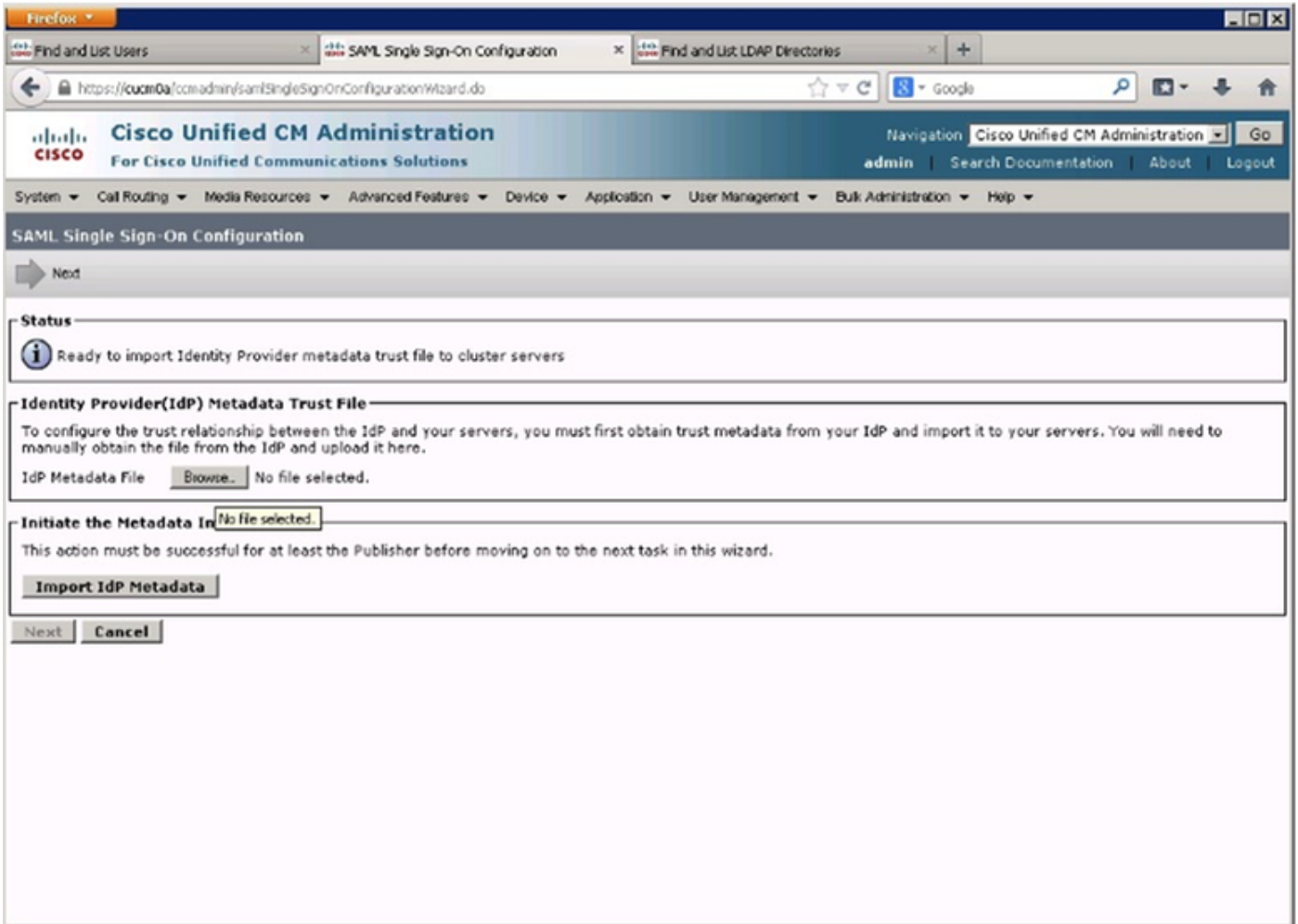
Select **Enable SAML SSO**.

Click **Continue** in order to acknowledge the warning.

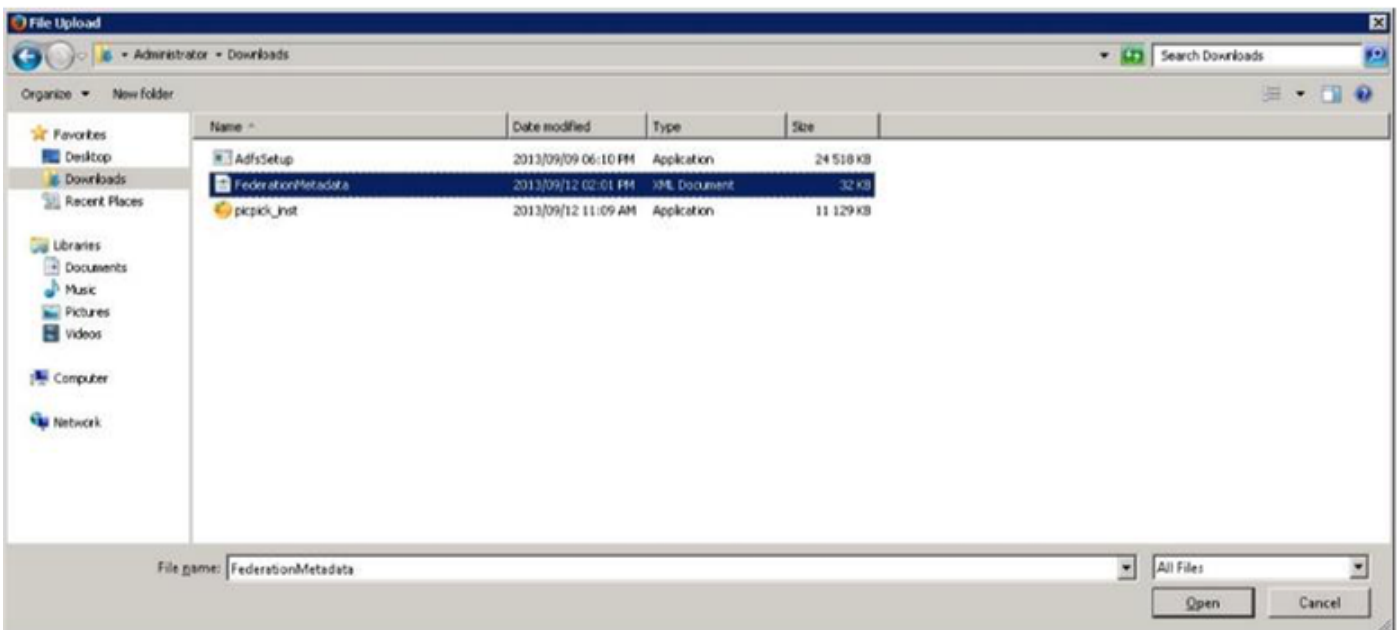


On the SSO screen and click on **Browse..** in order to import the FederationMetadata.xml

metadata XML file you saved earlier as shown in the image.



Select the XML file and click **Open** in order to upload it to CUCM from the Downloads under Favourites.



Once uploaded click on Import IdP Metadata to import the IdP information to CUCM. Confirm the import was successful and click Next to continue.

SAML Single Sign-On Configuration - Windows Internet Explorer

Navigation Cisco Unified CM Administration admin | Search Documentation | About | Logout

System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help

SAML Single Sign-On Configuration

Next

Status

Import succeeded for all servers

Identity Provider(IdP) Metadata Trust File

To configure the trust relationship between the IdP and your servers, you must first obtain trust metadata from your IdP and import it to your servers. You will need to manually obtain the file from the IdP and upload it here.

IdP Metadata File Browse...

Initiate the Metadata Import

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

Select the user belonging to the Standard CCM Super Users and click RUN SSO TEST.

SAML Single Sign-On Configuration - Mozilla Firefox

https://cmpubhcsc.fhlab.com:8443/ccadmin/samlSingleSignOnConfigurationWizard3.do?serve...


SAML Single Sign-On Configuration

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

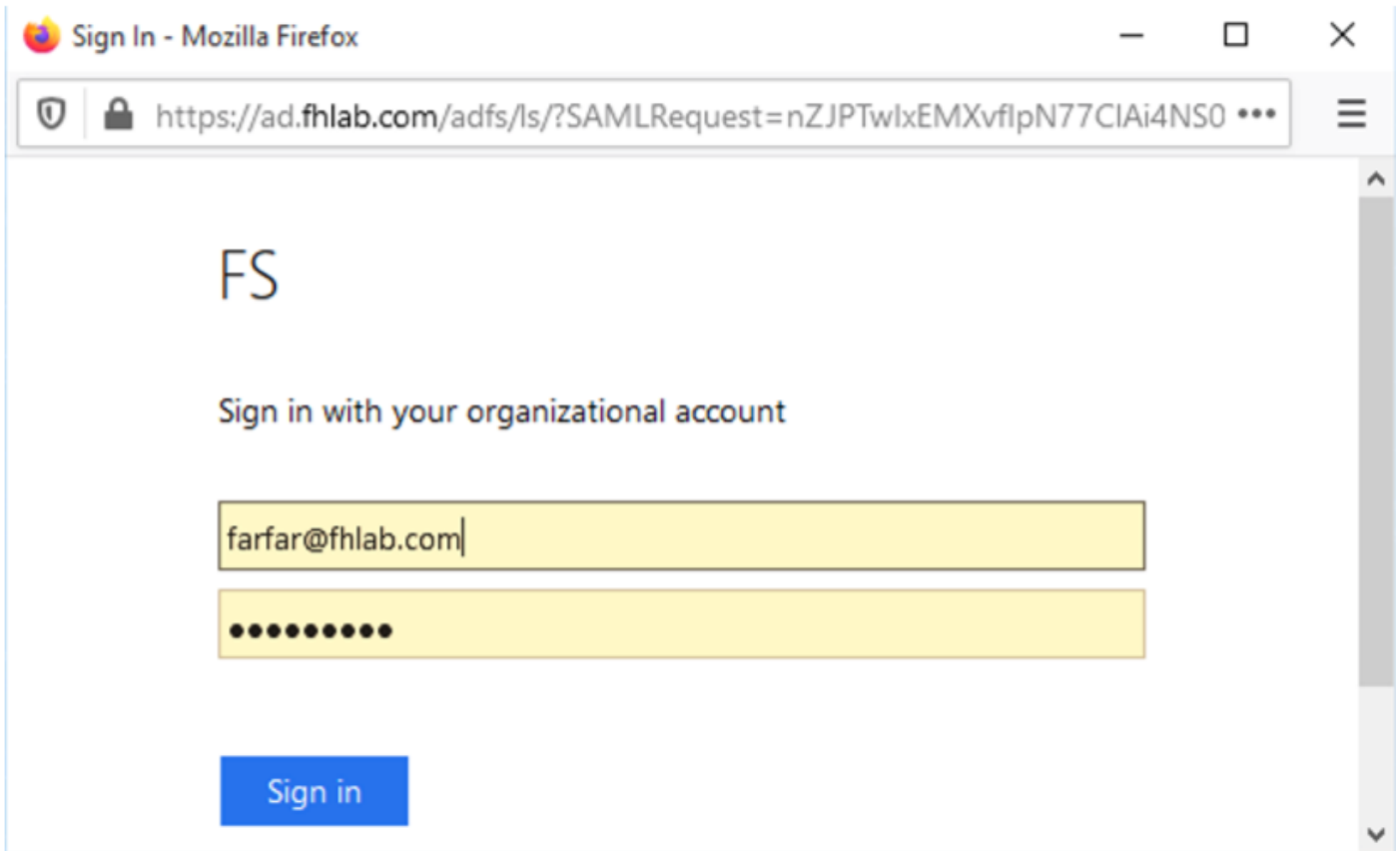
You must already know the password for the selected username. This user must have administrator rights and also exist in the IdP.

 Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.

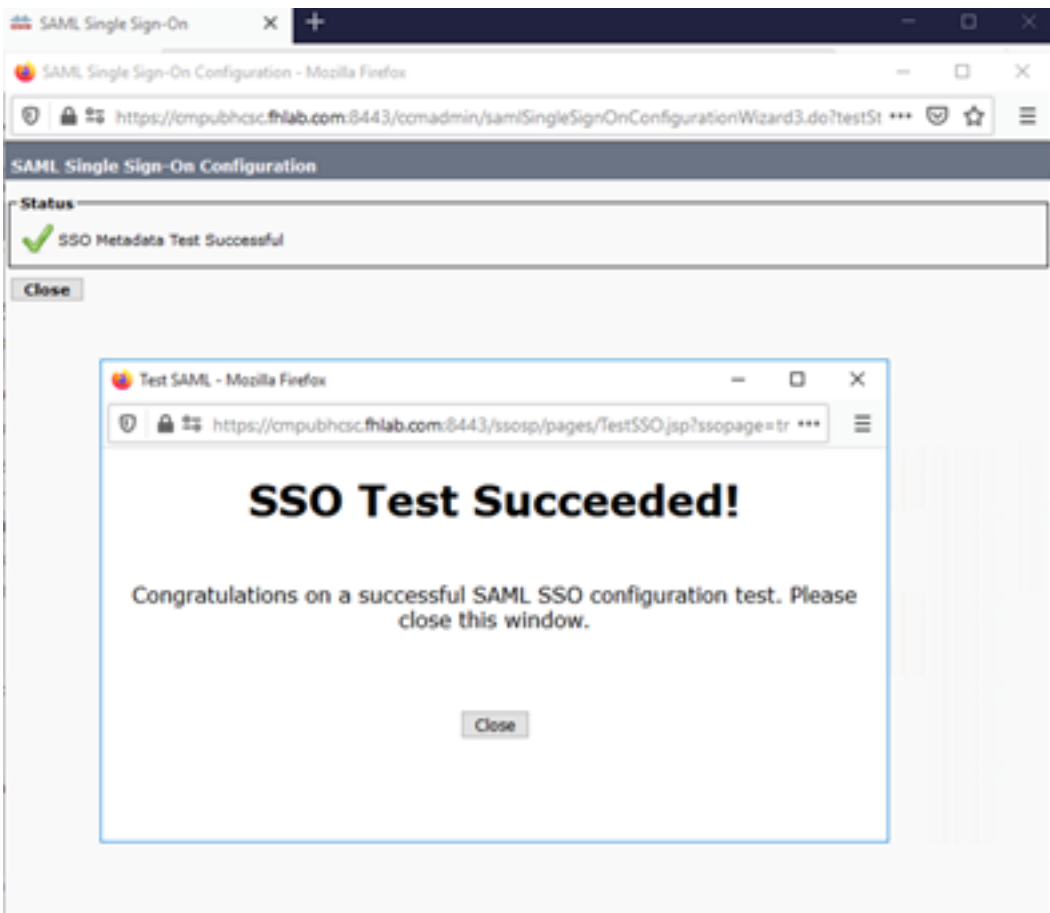
Valid administrator Usernames

2) Launch SSO test page

When presented with a user authentication dialogue box login with the appropriate username and password.



If everything was correctly configured you should see a message saying SSO Test Succeeded!



Click CLOSE and FINISH to continue.

We have now successfully completed the basic configuration tasks to enable SSO on CUCM using ADFS.

Configure SSO on CUC

The same process can be followed to enable SSO in Unity Connection.

LDAP integration with CUC.

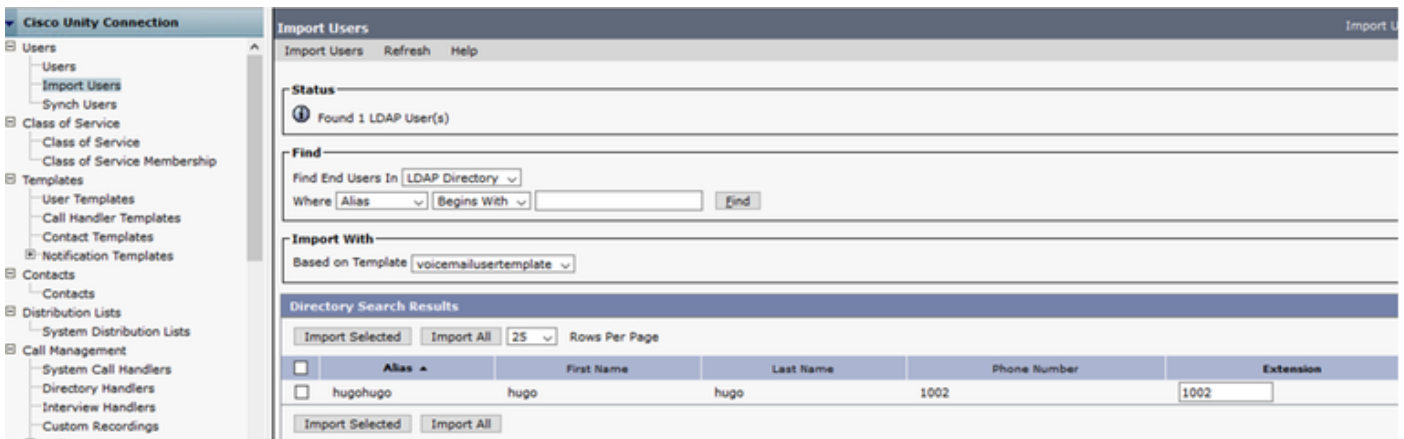
The screenshot shows the Cisco Unity Connection Administration interface for SAML Single Sign on. The left sidebar lists various system settings, with 'SAML Single Sign on' selected. The main content area has a 'SAML Single Sign on' header and a 'Refresh' button. Below the header, there are two radio buttons for 'SSO Mode': 'Cluster wide (One metadata file per cluster. Requires multi-server Tomcat certificate)' (selected) and 'Per node (One metadata file per node)'. There are three buttons: 'Disable SAML SSO' (with a red X), 'Update IdP Metadata File', and 'Export All Metadata'. Below this is a table titled 'SAML Single Sign-On (1 - 2 of 2)' with columns for Server Name, SSO Status, Re-Import Metadata, Last Metadata Import, Export Metadata, Last Metadata Export, and SSO Test. The table contains two rows of data for servers 'cucpubhsc.fhlab.com' and 'cucsubhsc.fhlab.com'. At the bottom, there are buttons for 'Disable SAML SSO', 'Export All Metadata', 'Update IdP Metadata File', and 'Fix All Disabled Servers'.

| Server Name | SSO Status | Re-Import Metadata | Last Metadata Import | Export Metadata | Last Metadata Export | SSO Test |
|---------------------|------------|--------------------|--------------------------------|-----------------|-------------------------------|---|
| cucpubhsc.fhlab.com | SAML | N/A | April 29, 2020 10:52:36 AM PDT | File | April 28, 2020 5:54:01 PM PDT | Passed - April 29, 2020 11:05:10 AM PDT Run SSO Test... |
| cucsubhsc.fhlab.com | SAML | IdP | April 29, 2020 10:52:36 AM PDT | File | April 28, 2020 5:54:00 PM PDT | Passed - April 29, 2020 11:05:37 AM PDT Run SSO Test... |

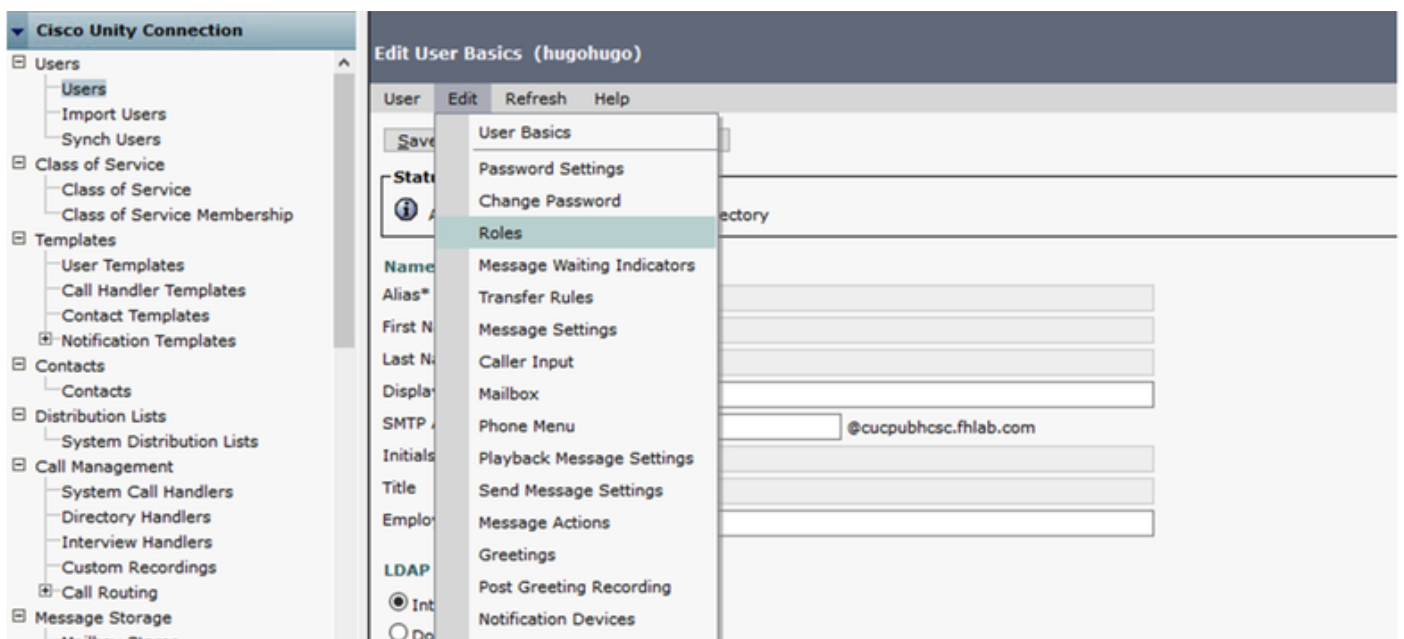
Configure LDAP Authentication.

The screenshot shows the Cisco Unity Connection Administration interface for LDAP Authentication. The left sidebar lists various system settings, with 'LDAP Authentication' selected. The main content area has a 'LDAP Authentication' header and a 'Refresh' button. Below the header, there is a 'Save' button and a 'Status' section showing 'Status: Ready'. The 'LDAP Authentication for End Users' section has a checked box for 'Use LDAP Authentication for End Users' and fields for 'LDAP Manager Distinguished Name*' (fhlab/Administrator), 'LDAP Password*', 'Confirm Password*', and 'LDAP User Search Base*' (cn=users,dc=fhlab,dc=com). The 'LDAP Server Information' section has fields for 'Host Name or IP Address for Server*' (10.89.228.226), 'LDAP Port*' (389), and 'Use TLS' (checkbox). There is an 'Add Another Redundant LDAP Server' button and a 'Save' button. A note at the bottom states 'Fields marked with an asterisk (*) are required.'

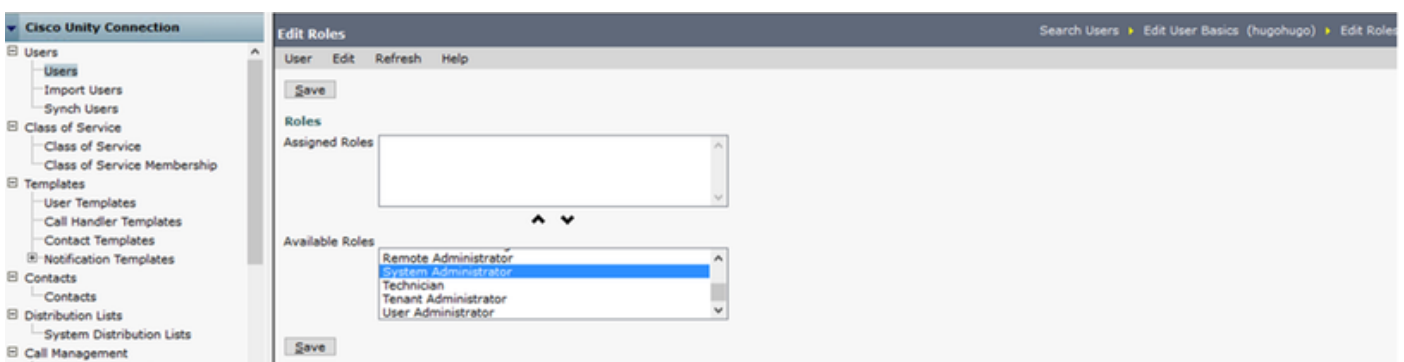
Import the Users from LDAP that will have voicemail assigned and also the user that will serve for testing SSO.



Navigate to **Users > Edit > Roles** as shown in the image.

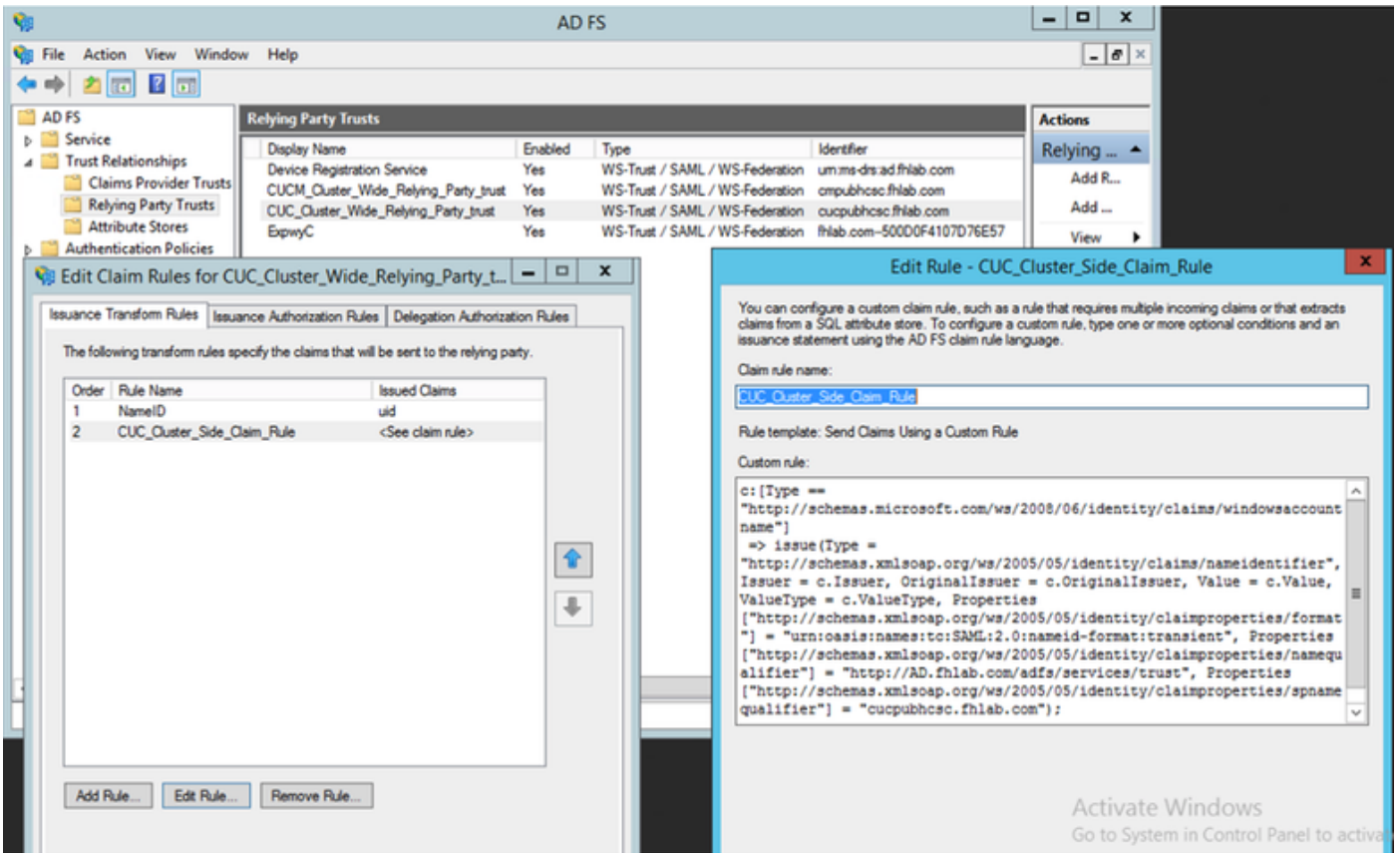


Assign the testing user the role of System Administrator.

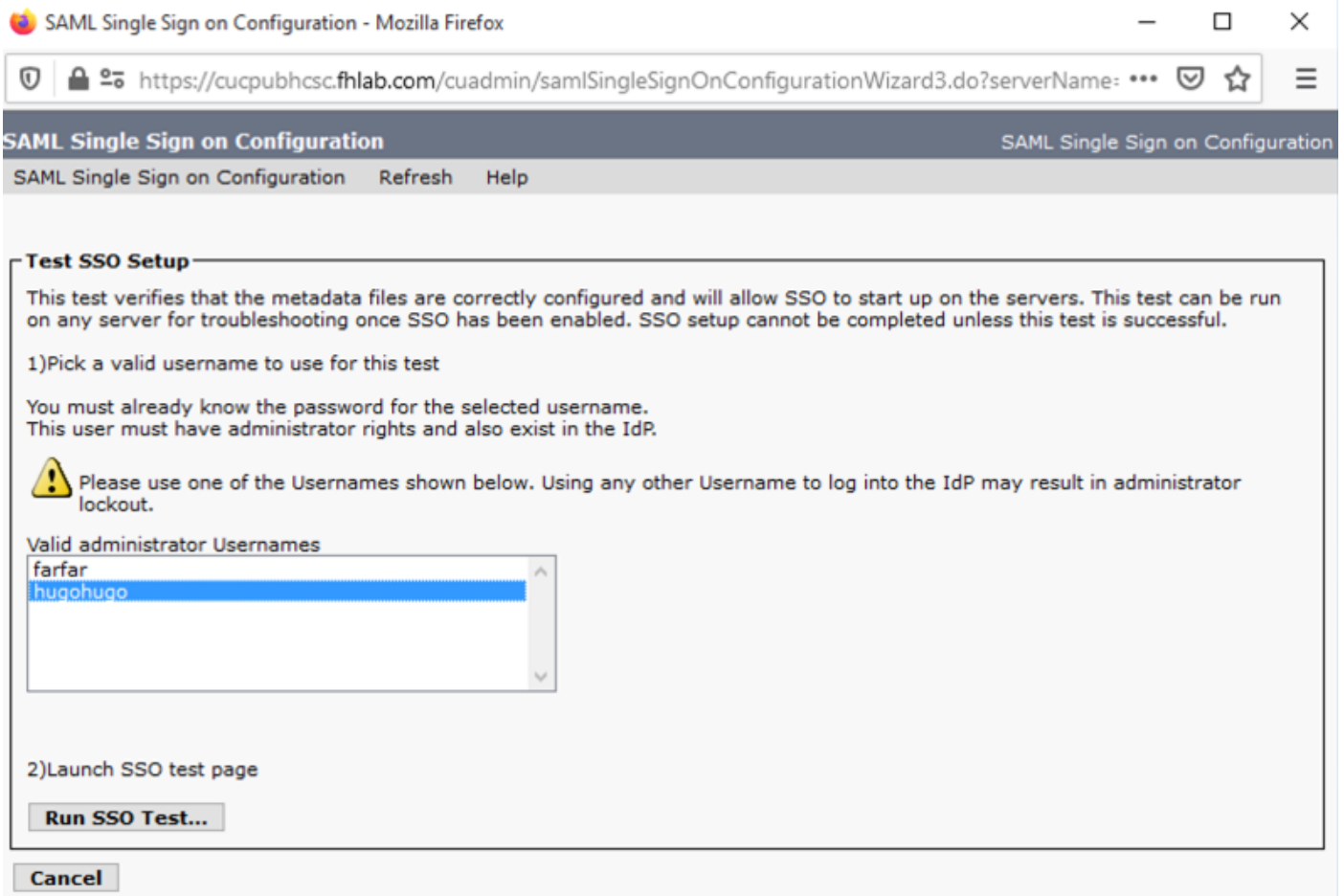


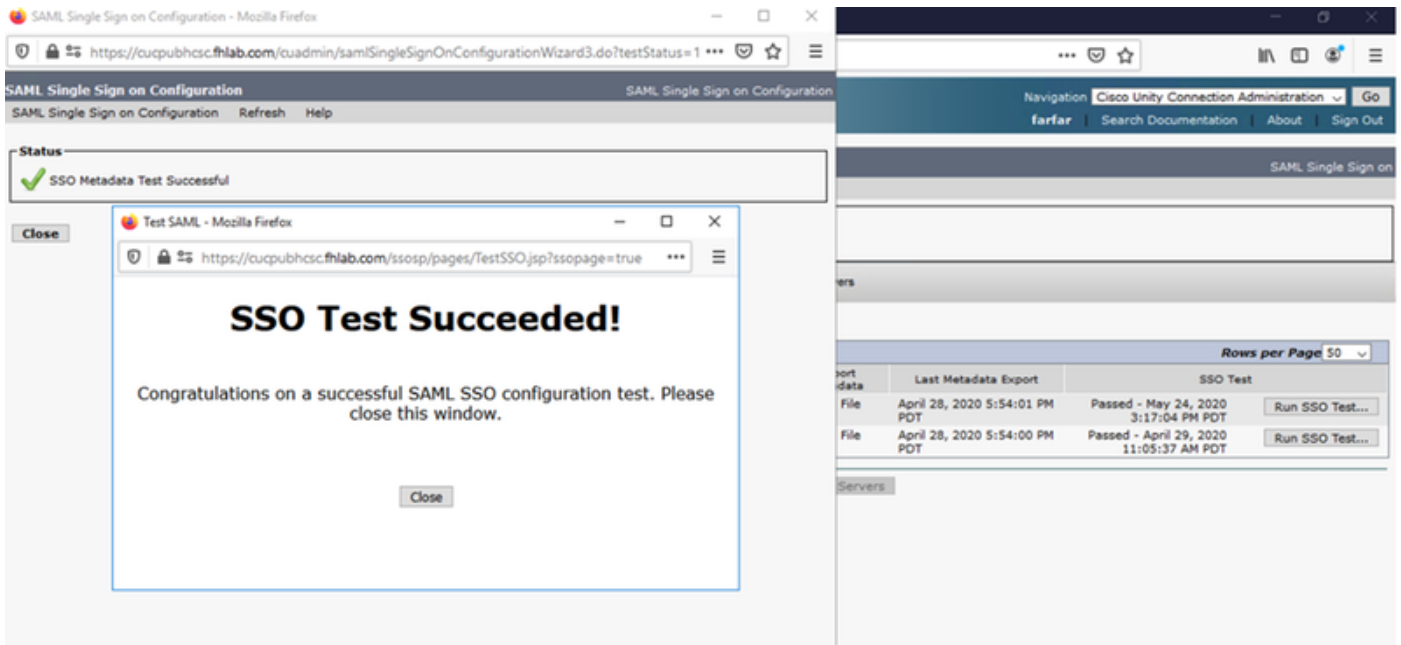
CUC Metadata

You should have by now downloaded CUC metadata, created the RelyingPartyTrust for CUC and uploaded CUC metadata and created the rules I AD FS on ADFS 3.0



Go to SAML Single Sign-On and Enable SAML SSO.





Configure SSO on Expressway

Import Metadata to Expressway C

Open a browser to <https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml> and SAVE the metadata to a local folder

Upload to **Configuration > Unified Communications > IDP**.

Export Metadata From Expressway C

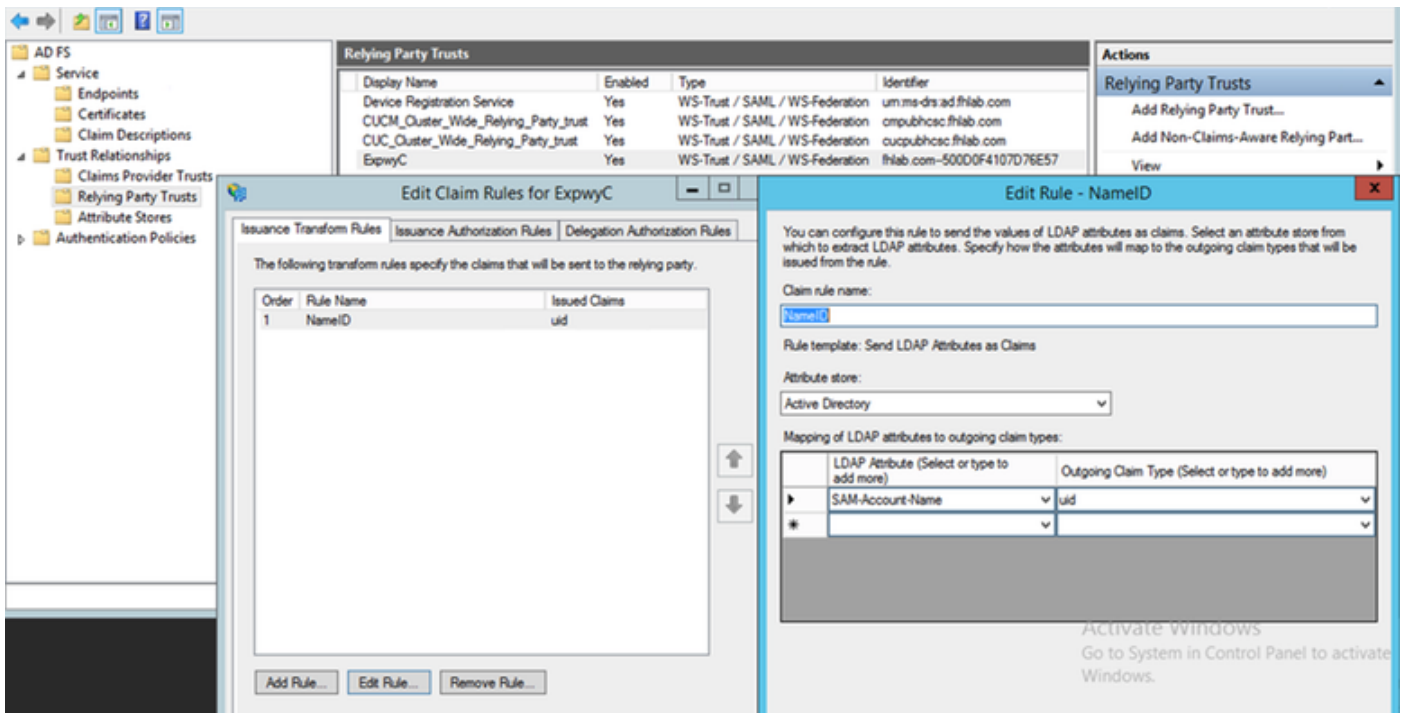
Go to configuration -> Unified Communications -> IDP -> Export SAML Data

Cluster mode uses a self-signed certificate (with long lifetime) that is included in the SAML metadata and used for signing SAML requests

- On cluster-wide mode, to download the single cluster-wide metadata file, click Download
- On per-peer mode, to download the metadata file for an individual peer, click Download next to the peer. To export all in a .zip file, click Download All.

Add a Relying Party Trust for Cisco Expressway-E

First, create Relying Party Trusts for the Expressway-Es and then Add a claim rule to send identity as UID attribute.

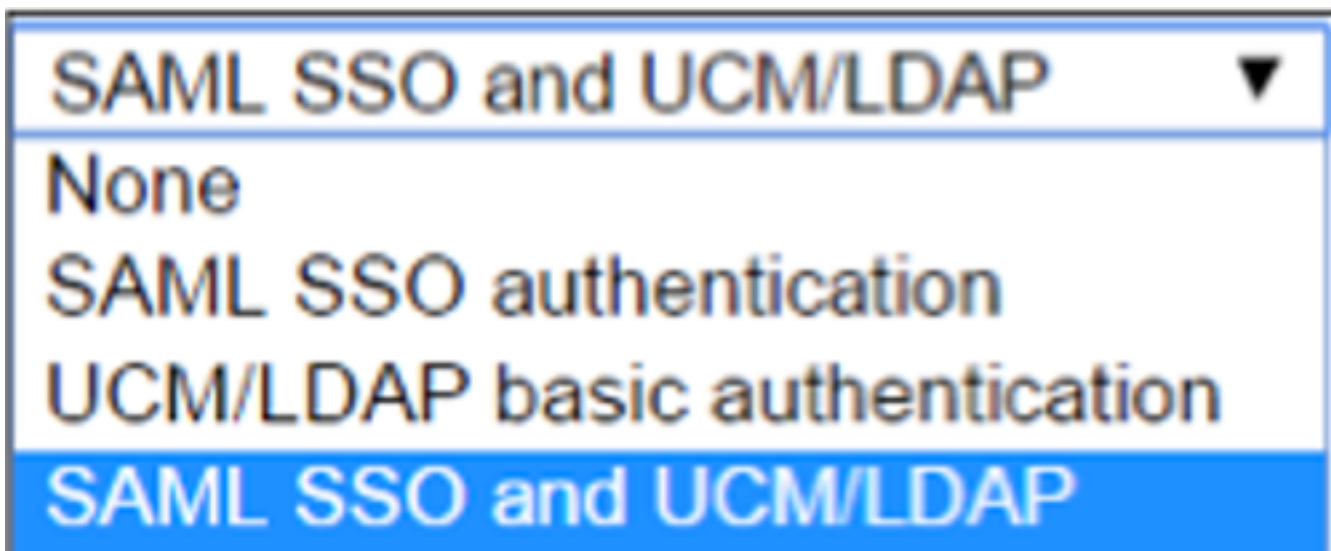


OAuth with Refresh Login

In Cisco CUCM Enterprise Parameters, Verify OAuth with Refresh login flow parameter is enabled. Go to **Cisco Unified CM Administration > Enterprise Parameters > SSO and OAuth Configuration**.

| SSO and OAuth Configuration | | |
|---|--------------------------------|--------------------------------|
| OAuth Token Expiry Timer (minutes) * | 60 | 60 |
| OAuth Refresh Token Expiry Timer (days) * | 60 | 60 |
| Redirect URIs for Third Party SSO Client | | |
| SSO Login Behavior for iOS * | Use embedded browser (WebView) | Use embedded browser (WebView) |
| OAuth with Refresh Login Flow * | Enabled | Disabled |
| Use SSO for RTMT * | True | True |

Authentication Path



- If the authentication path is set to "SAML SSO authentication" only Jabber clients using an

SSO enabled Unified CM cluster would be able to use MRA on this Expressway. This is an SSO only configuration.

- Expressway MRA support for all IP phones, all TelePresence endpoints, and any Jabber clients homed to a Unified CM cluster not configured for SSO will require the authentication path to include UCM/LDAP authentication.
- If one or more of the Unified CM clusters supports Jabber SSO, select the “SAML SSO and UCM/LDAP” to allow for both SSO and basic authentication.

SSO Architecture

SAML is an XML-based open-standard data format that enables administrators to access a defined set of Cisco collaboration applications seamlessly after signing into one of those applications. SAML SSO uses the SAML 2.0 protocol to offer cross-domain and cross-product single sign-on for Cisco collaboration solutions.

On-Premise Login Flow

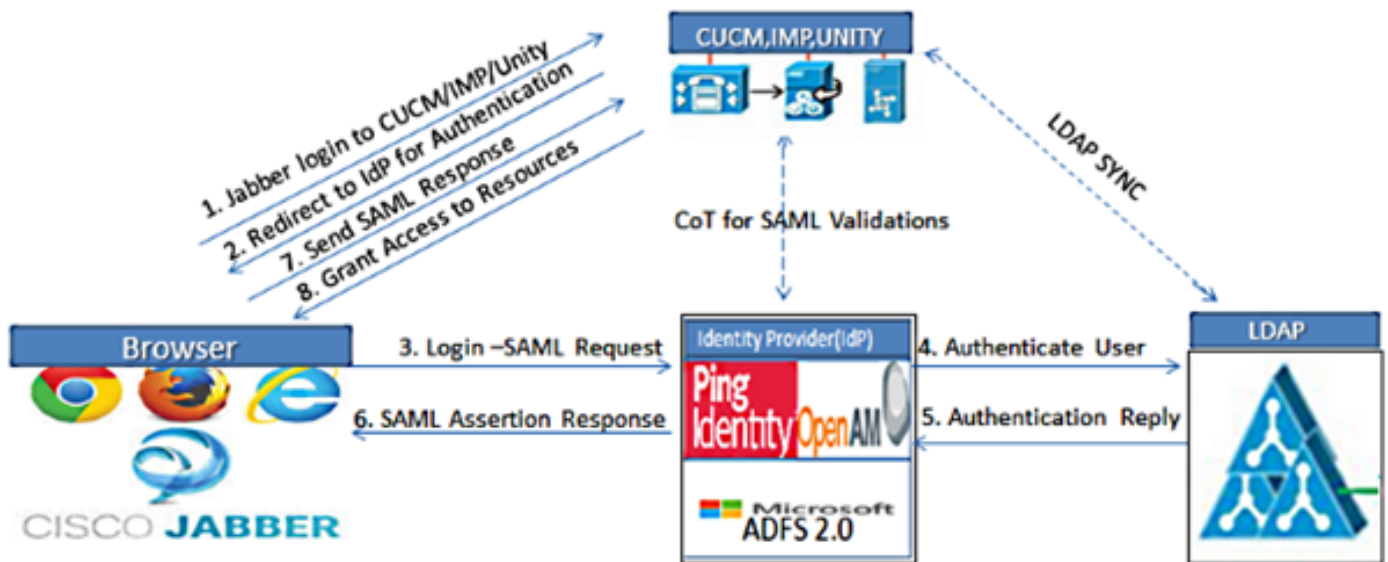
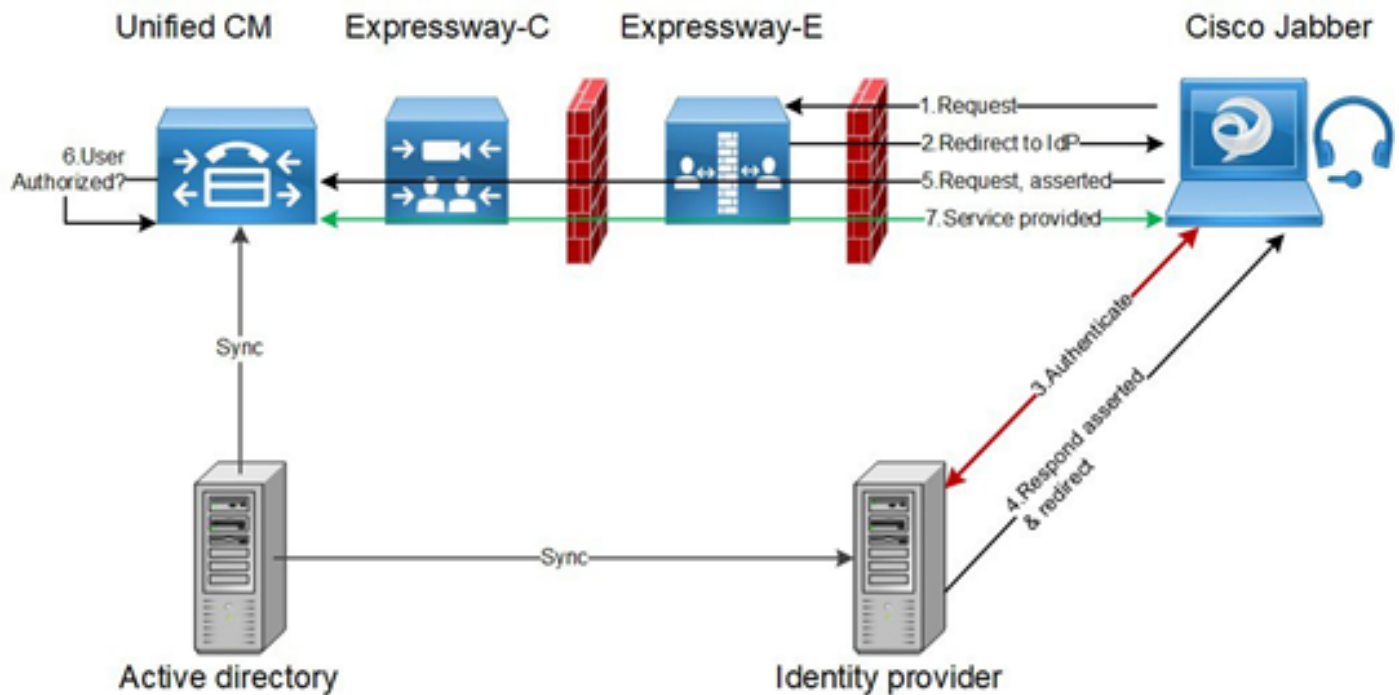


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

MRA Login Flow



OAuth

OAuth is a standard which supports authorization. A user must be authenticated before they can be authorized. The authorization code grant flow provides a method for a client to obtain access and refresh tokens to access a resource (Unified CM, IM&P, Unity and Expressway services). This flow is also based on redirection and thus requires the client to be able to interact with an HTTP user-agent (web browser) controlled by the user. The client will make an initial request to the authorization server using HTTPS. The OAuth server redirects the user to an authentication service. This may be running on Unified CM or an external IdP if SAML SSO is enabled. Depending on the authentication method being used, a web page view may be presented to the end user to authenticate themselves. (Kerberos authentication is an example that would not display a web page.) Unlike the implicit grant flow, a successful authentication code grant flow will result in the OAuth servers issuing an "Authorization Code" to the web browser. This is a one-use, short-lived unique code that is then passed back from the web browser to the client. The client provides this "Authorization Code" to the authorization server together with a pre-shared secret and receives in exchange an "Access Token" and a "Refresh Token". The client secret used in this step enables the authorization service to limit the use to only registered and authenticated clients. The tokens are used for the following purposes:

Access/Refresh Token

Access Token: This token is issued by the authorization server. The client presents the token to a resource server when it needs to access protected resources on that server. The resource server is able to validate the token and trusts connections using the token. (Cisco access tokens default to a lifetime of 60 minutes)

Refresh Token: This token again is issued by the authorization server. The client presents this token to the authorization server together with the client secret when the access token has expired or is due to expire. If the refresh token is still valid then the authorization server will issue a new access token without requiring another authentication. (Cisco refresh tokens default to a lifetime of 60 days). If the refresh token has expired, then a new full OAuth authorization code grant flow has to be initiated to obtain new tokens.

OAuth Authorization Code Grant Flow is better

In the implicit grant flow, the access token is passed to the Jabber client via a HTTP user agent (browser). In the authorization code grant flow, the access token is exchanged directly between the authorization server and the Jabber client. The token is requested from the authorization server using a time-limited unique authorization code. This direct exchange of the access token is more secure and reduces risk exposure.

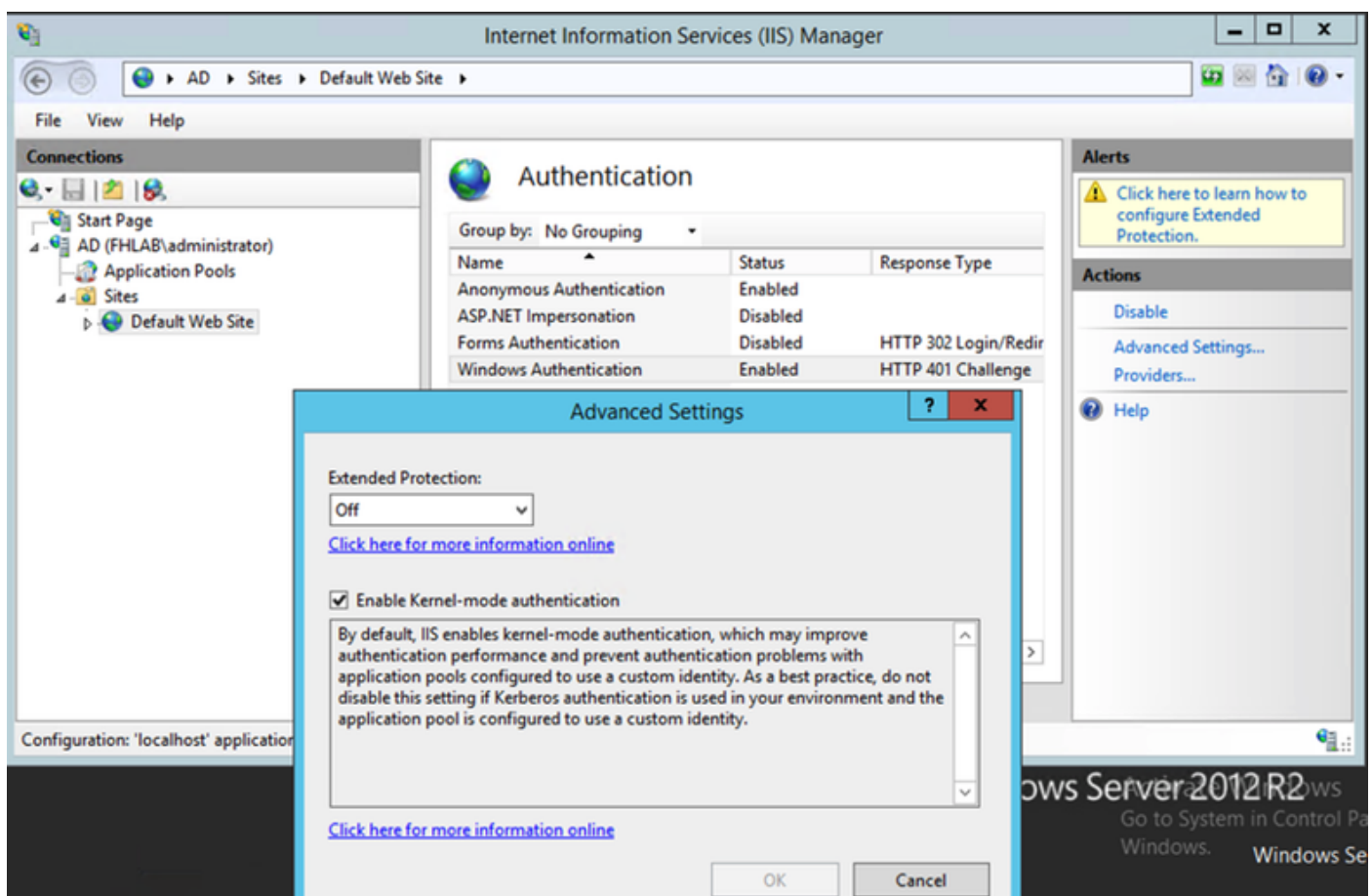
The OAuth authorization code grant flow supports the use of refresh tokens. This delivers a better experience to the end user since they don't need to re-authenticate as frequently (by default 60 days)

Configure Kerberos

Select Windows Authentication

Internet Information Services (IIS) Manager > Sites > Default Web Site > Authentication > Windows Authentication > Advance Settings.

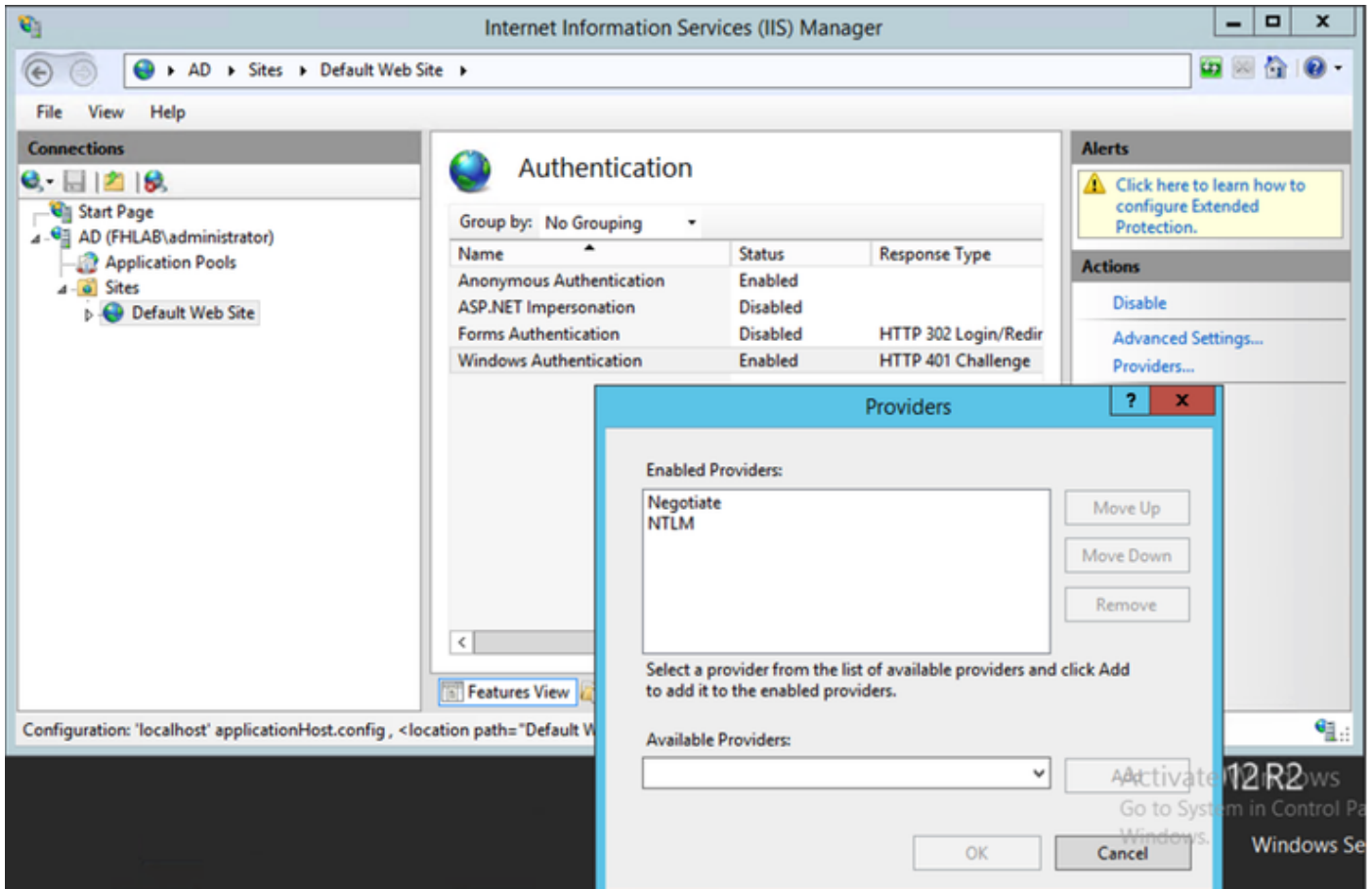
1. Uncheck Enable Kernel-mode authentication.
2. Ensure Extended Protection is Off.



ADFS Supports both Kerberos NTLM

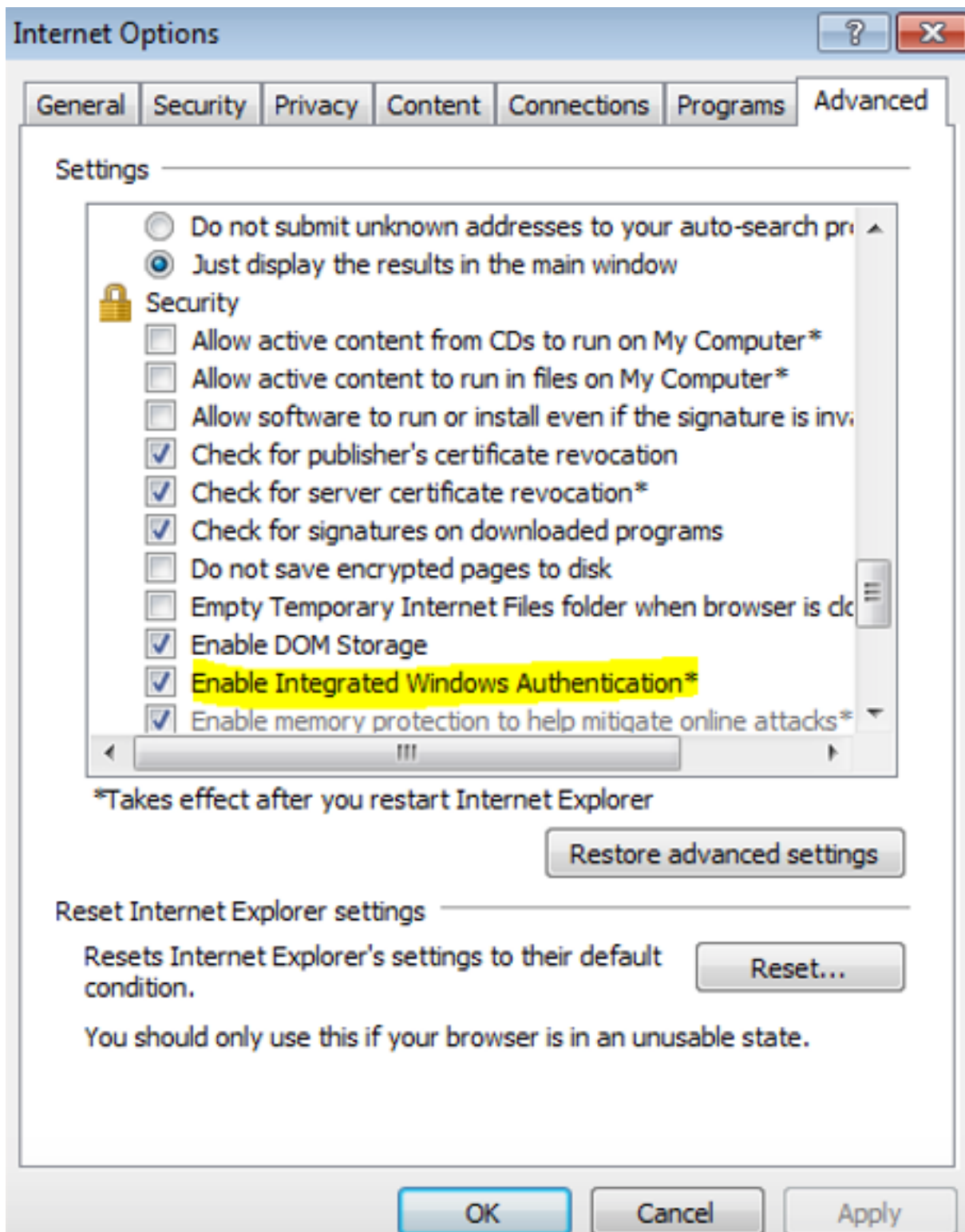
Ensure that AD FS Version 3.0 supports both the Kerberos protocol and the NT LAN Manager (NTLM) protocol because all Non-Windows clients cannot use Kerberos and rely on NTLM.

In the right-pane, select Providers and ensure Negotiate and NTLM are present under Enabled Providers:



Configure Microsoft Internet Explorer

Ensure that **Internet Explorer > Advanced > Enable Integrated Windows Authentication** is checked.



Add ADFS URL under Security > Intranet zones > Sites

