使用ADFS 3.0在Cisco Unified Communications Manager上配置SAML SSO

目录

简介

本文档介绍在思科统一通信管理(CUCM)、思科统一连接(CUC)、Expressway产品上使用Windows 2012 R2配置使用Active Directory联合身份验证服务(ADFS 3.0)的单点登录的步骤。配置Kerberos的步骤也包含在本文档中。

先决条件

要求

思科建议您了解单点登录(SSO)和Windows产品。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CUCM 11.5
- CUC 11.5
- Expressway 12
- Windows 2012 R2 Server具有以下角色：
  - Active Directory证书服务
  - Active Directory联合身份验证服务

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。

配置预检查

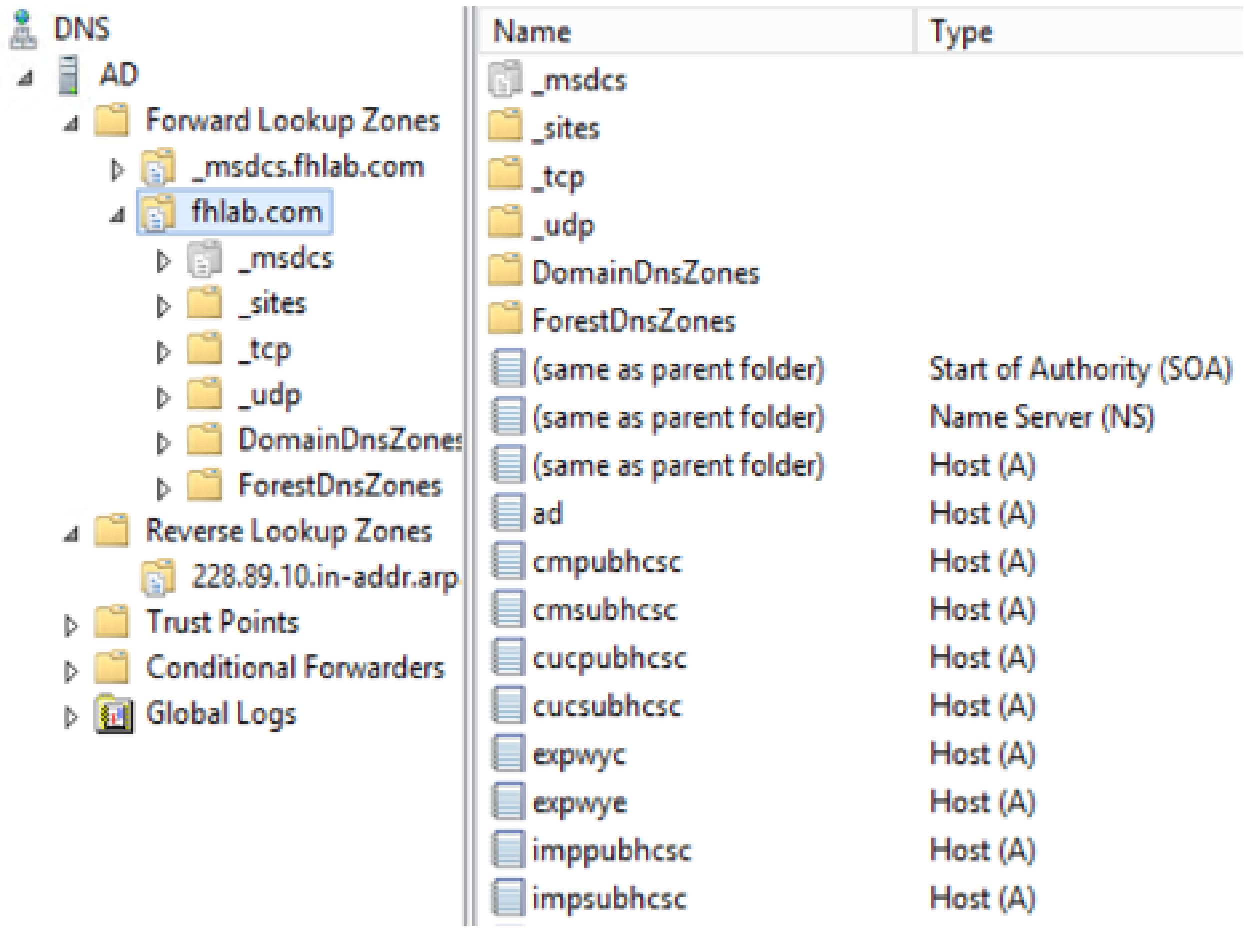
在安装ADFS3之前，环境中需要已存在以下服务器角色：

·域控制器和DNS

·所有服务器都必须作为记录和指针记录一起添加（一种将IP地址解析为域或主机名的DNS记录）

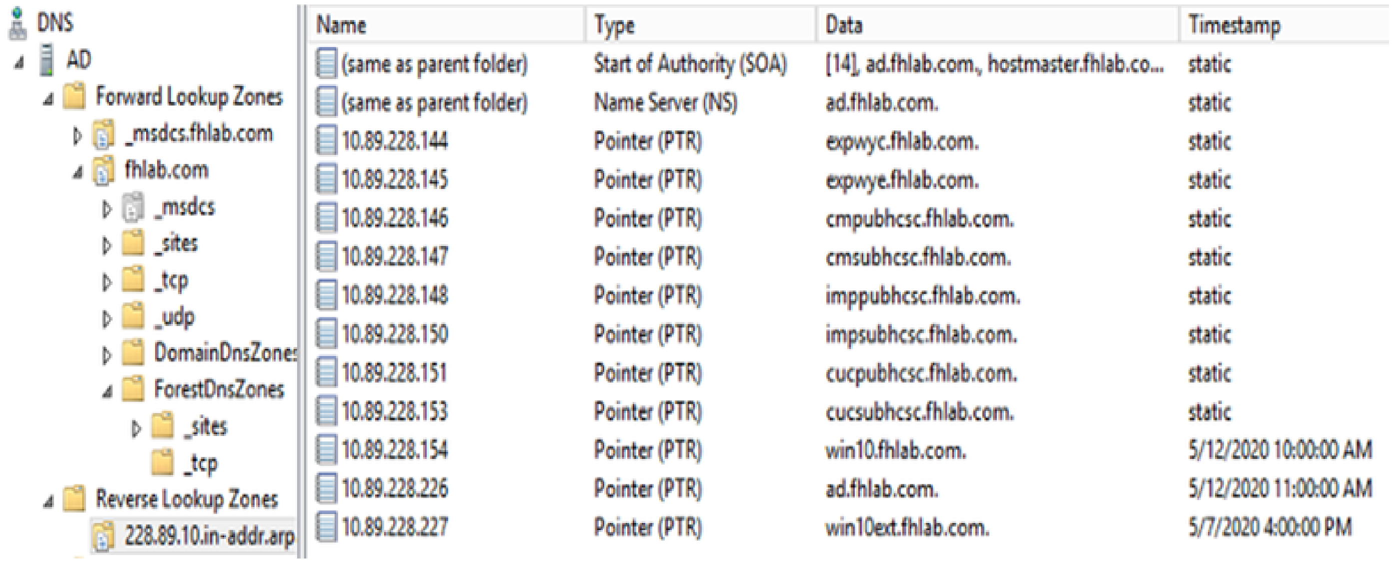
A记录

在fhlab.com中。hosts cmpubhcsc、cmsubhcsc、cucpubhcsc、cucsubhcsc、exwyc、expwye、impubhcsc和imsubhcsc已添加。



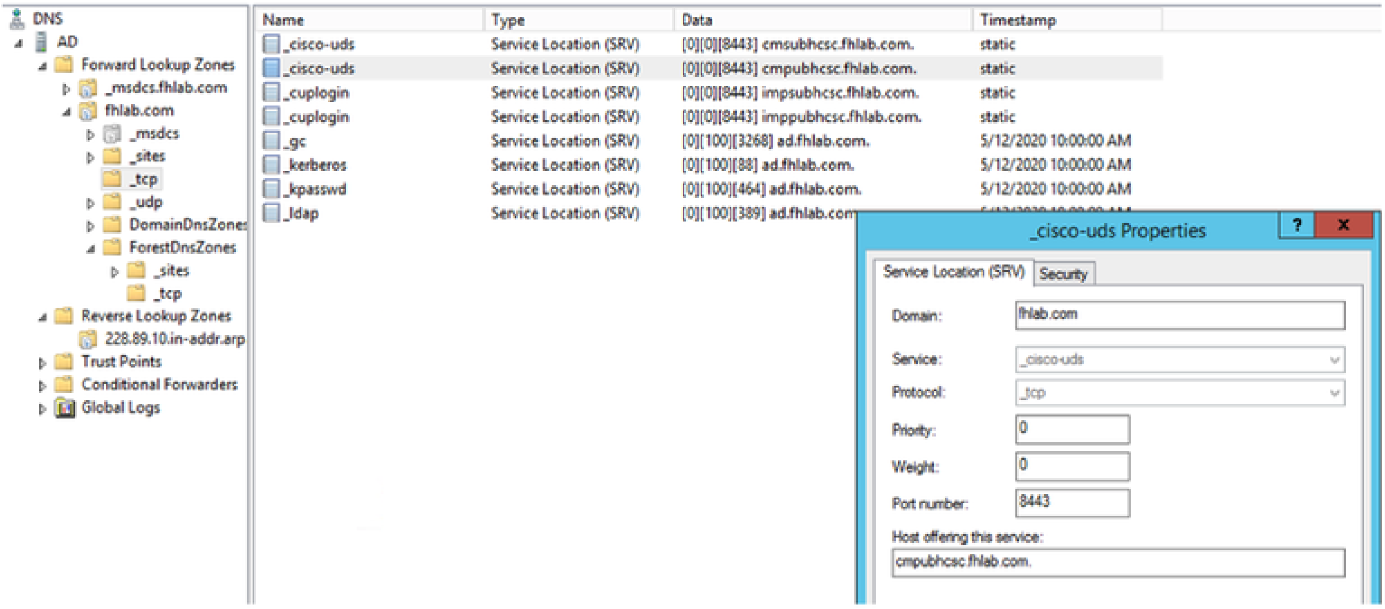
Name	Type
_msdcs	
_sites	
_tcp	
_udp	
DomainDnsZones	
ForestDnsZones	
(same as parent folder)	Start of Authority (SOA)
(same as parent folder)	Name Server (NS)
(same as parent folder)	Host (A)
ad	Host (A)
cmpubhcsc	Host (A)
cmsubhcsc	Host (A)
cucpubhcsc	Host (A)
cucsubhcsc	Host (A)
expwyc	Host (A)
expwye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

指针(PTR)记录



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

Jabber发现服务需要有SRV记录



DNS
- AD
  - Forward Lookup Zones
    - _msdcs.fhlab.com
    - fhlab.com
      - _msdcs
      - _sites
      - _tcp
      - _udp
      - DomainDnsZones
      - ForestDnsZones
        - _sites
        - _tcp
  - Reverse Lookup Zones
    - 228.89.10.in-addr.arp
  - Trust Points
  - Conditional Forwarders
  - Global Logs

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	

_cisco-uds Properties

Service Location (SRV) | Security

Domain: fhlab.com

Service: _cisco-uds

Protocol: _tcp

Priority: 0

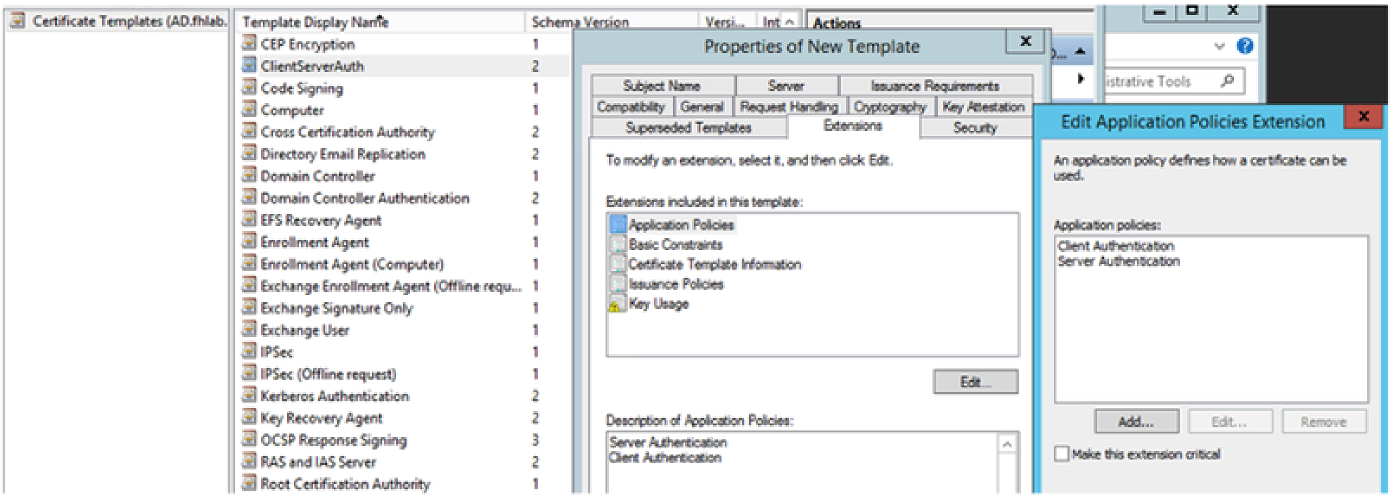
Weight: 0

Port number: 8443

Host offering this service: cmpubhcsc.fhlab.com.

- 根CA（假设证书将由企业CA签名）

需要根据Web服务器证书模板创建证书模板，前者是重复的、重命名的，在“扩展”(Extensions)选项卡上，“应用策略”(Application Policies)被修改，添加客户端身份验证应用策略(Client Authentication Application Policy)。在实验室环境中，内部CA还可以签署Expressway E证书签名请求(CSR)，在签署所有内部证书（CUCM、CUC、IMP和Expressway核心）时，需要使用此模板。



Certificate Templates (AD.fhlab.

Template Display Name	Schema Version
CEP Encryption	1
ClientServerAuth	2
Code Signing	1
Computer	1
Cross Certification Authority	2
Directory Email Replication	2
Domain Controller	1
Domain Controller Authentication	2
EFS Recovery Agent	1
Enrollment Agent	1
Enrollment Agent (Computer)	1
Exchange Enrollment Agent (Offline requ...	1
Exchange Signature Only	1
Exchange User	1
IPSec	1
IPSec (Offline request)	1
Kerberos Authentication	2
Key Recovery Agent	2
OCSP Response Signing	3
RAS and IAS Server	2
Root Certification Authority	1

Properties of New Template

Subject Name | Server | Issuance Requirements | Compatibility | General | Request Handling | Cryptography | Key Attestation | Superseded Templates | Extensions | Security

To modify an extension, select it, and then click Edit.

Extensions included in this template:
- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Edit...

Description of Application Policies:
Server Authentication
Client Authentication

Edit Application Policies Extension

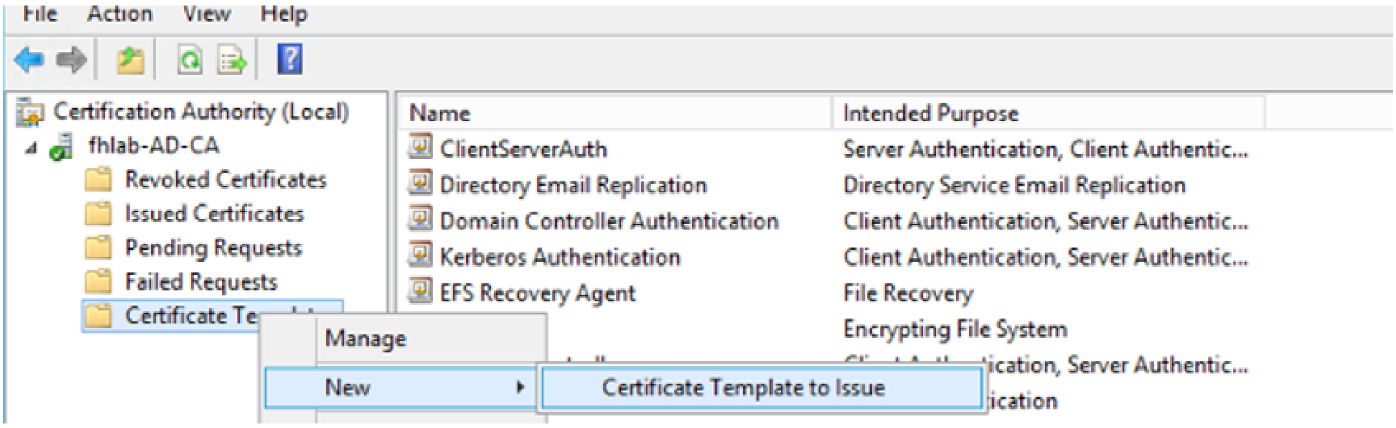
An application policy defines how a certificate can be used.

Application policies:
Client Authentication
Server Authentication

Add... | Edit... | Remove

□ Make this extension critical

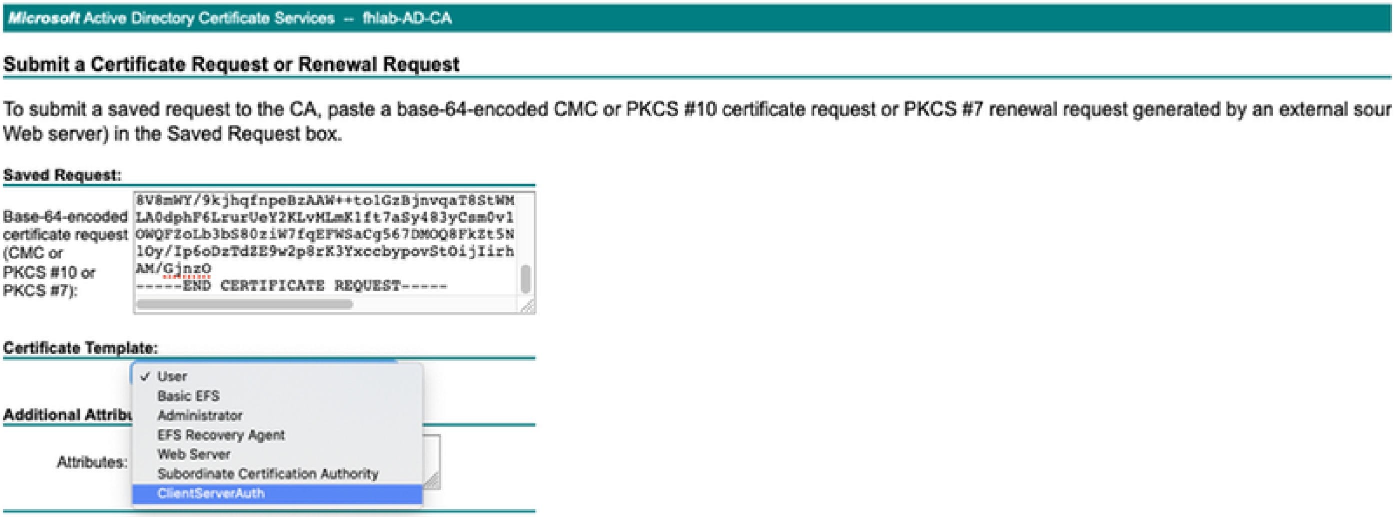
创建的模板需要发布才能签署CSR。



Certification Authority (Local)
- fhlab-AD-CA
  - Revoked Certificates
  - Issued Certificates
  - Pending Requests
  - Failed Requests
  - Certificate Te...

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...
	...ication

在CA证书Web上，选择之前创建的模板。



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 sour
Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

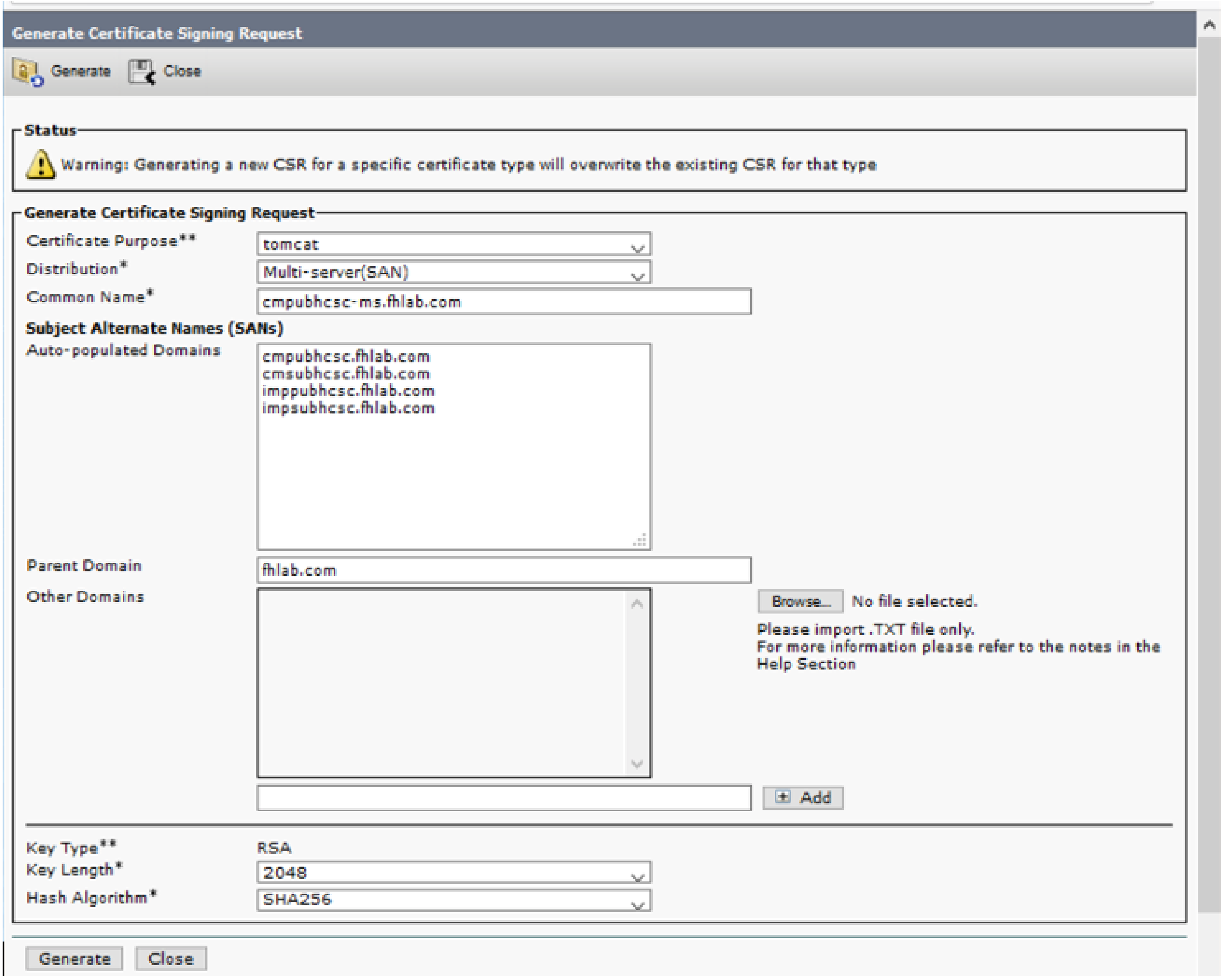
```
8V8mWY/9kjhqfnpeBzAAW++tolGzBjnvqaT8StWM
LA0dphF6LrurUeY2KLvMLmK1ft7aSy483yCsm0v1
OWQFZoLb3bS80ziW7fqEFWSaCg567DMOQ8FkZt5N
1Oy/Ip6oDzTdZE9w2p8rK3YxccbypovStOijIirh
AM/GjnzO
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Additional Attribu

Attributes:

CUCM、IMP和CUC多服务器CSR必须由CA生成和签名。证书用途必须是tomcat。



Generate Certificate Signing Request

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)

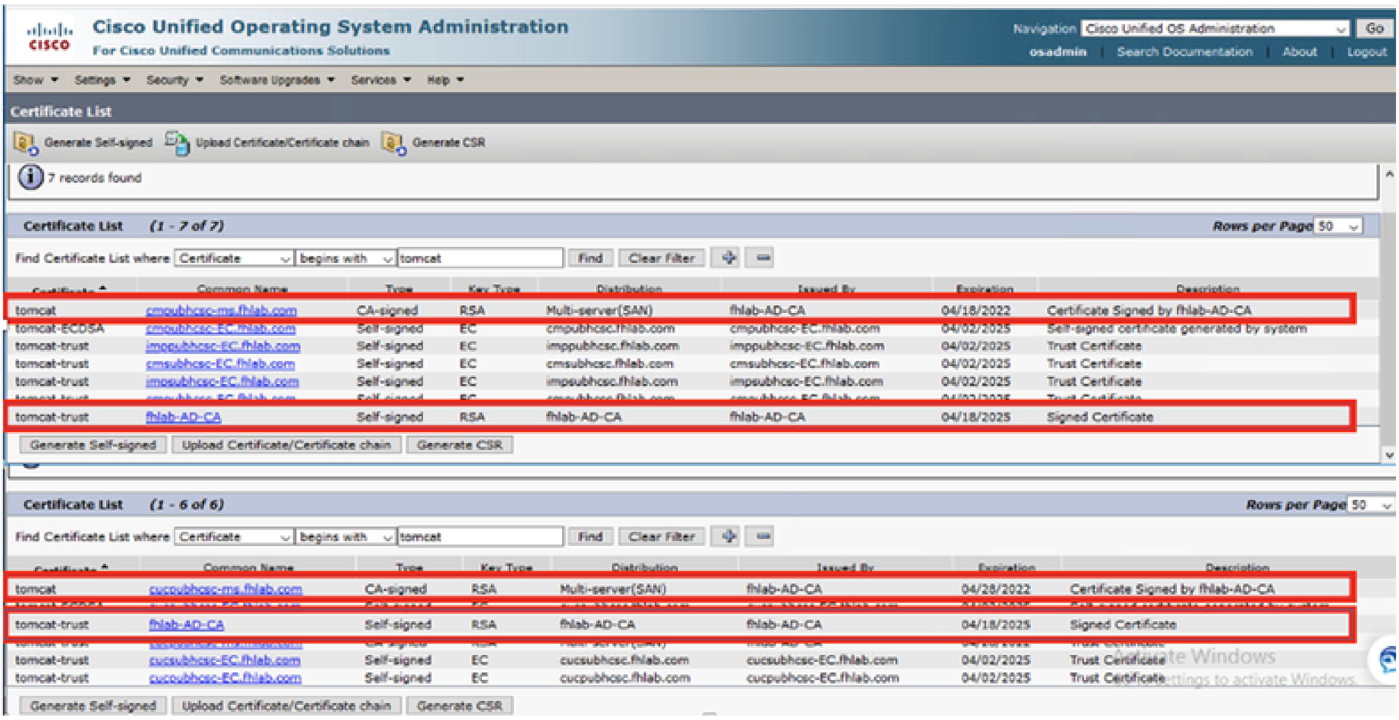
Auto-populated Domains	cmpubhcsc.fhlab.com cmsubhcsc.fhlab.com imppubhcsc.fhlab.com impsubhcsc.fhlab.com
Parent Domain	fhlab.com
Other Domains	

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

CA根证书必须上传到Tomcat Trust，签名证书必须上传到Tomcat。



Cisco Unified Operating System Administration

For Cisco Unified Communications Solutions

Navigation: Cisco Unified OS Administration | Go

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

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

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

Find Certificate List where Certificate begins with tomcat

Certificate ▲	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat	cucpubhcsc-ms.fhlab.com	CA-signed	RSA	Multi-server(SAN)	fhlab-AD-CA	04/28/2022	Certificate Signed by fhlab-AD-CA
tomcat-trust	fhlab-AD-CA	Self-signed	RSA	fhlab-AD-CA	fhlab-AD-CA	04/18/2025	Signed Certificate
tomcat-trust	cucsubhcsc-EC.fhlab.com	Self-signed	EC	cucsubhcsc.fhlab.com	cucsubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate
tomcat-trust	cucpubhcsc-EC.fhlab.com	Self-signed	EC	cucpubhcsc.fhlab.com	cucpubhcsc-EC.fhlab.com	04/02/2025	Trust Certificate

Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR
Activate Windows
Go to Settings to activate Windows.

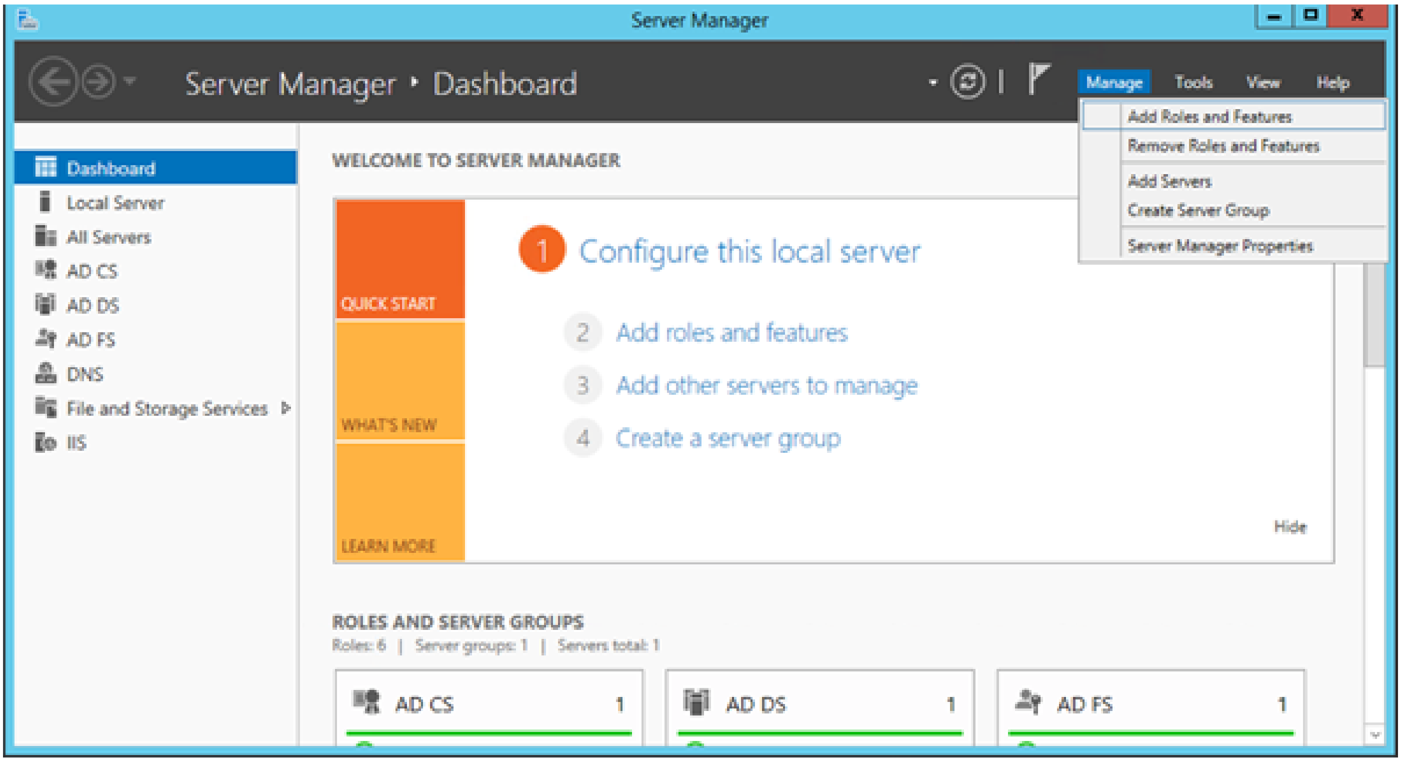
- IIS

否则，本节将介绍这些角色的安装过程。否则，请跳过此部分，直接从Microsoft下载ADFS3。

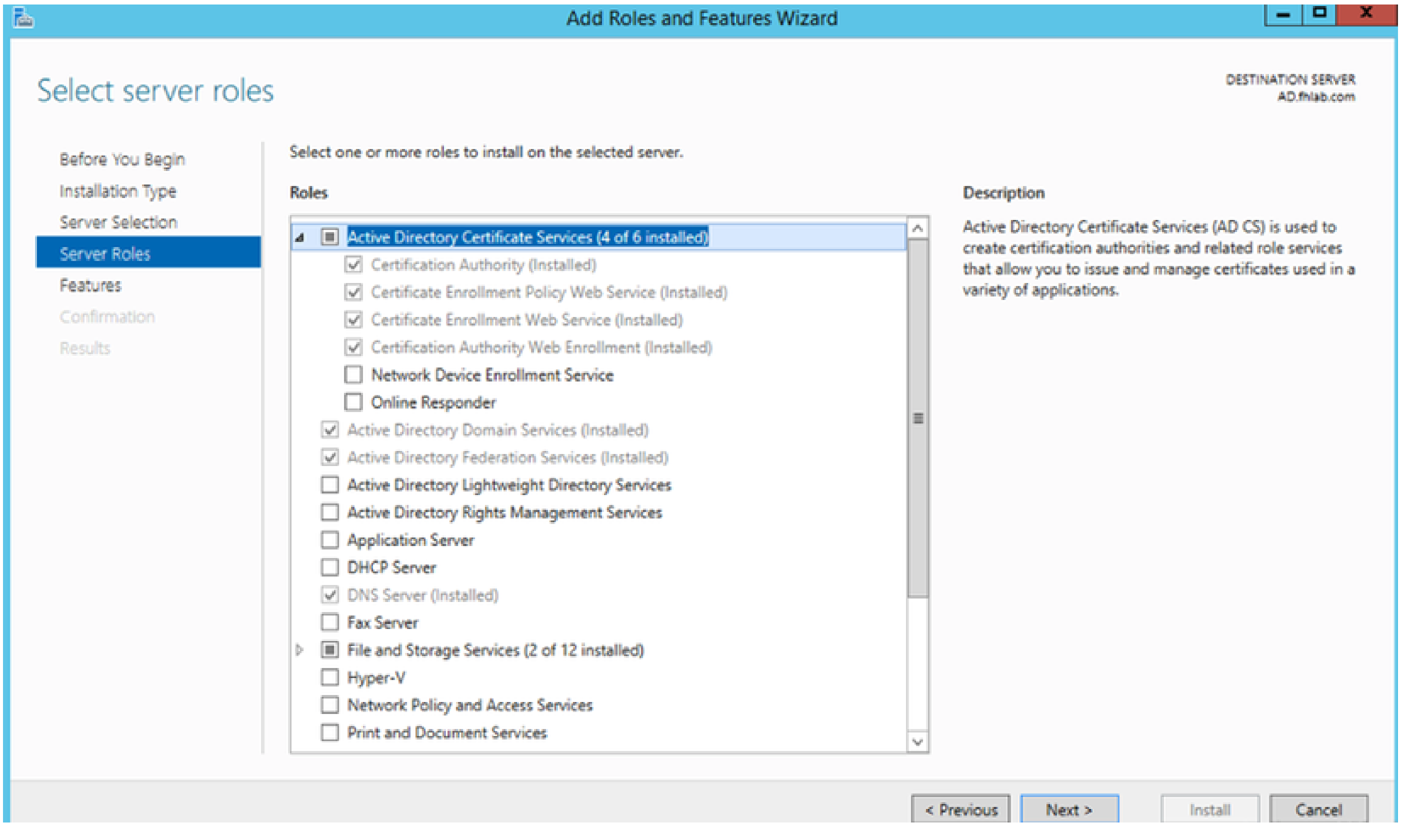
安装带DNS的Windows 2012 R2后，将服务器升级到域控制器。

下一个任务是安装Microsoft证书服务。

导航至服务器管理器并添加新角色：



选择**Active Directory证书服务**角色。



Select server roles

DESTINATION SERVER
AD.fhlab.com

Select one or more roles to install on the selected server.

Roles

- ▣ Active Directory Certificate Services (4 of 6 installed)
  - ☑ Certification Authority (Installed)
  - ☑ Certificate Enrollment Policy Web Service (Installed)
  - ☑ Certificate Enrollment Web Service (Installed)
  - ☑ Certification Authority Web Enrollment (Installed)
  - □ Network Device Enrollment Service
  - □ Online Responder
- ☑ Active Directory Domain Services (Installed)
- ☑ Active Directory Federation Services (Installed)
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- ▣ File and Storage Services (2 of 12 installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services

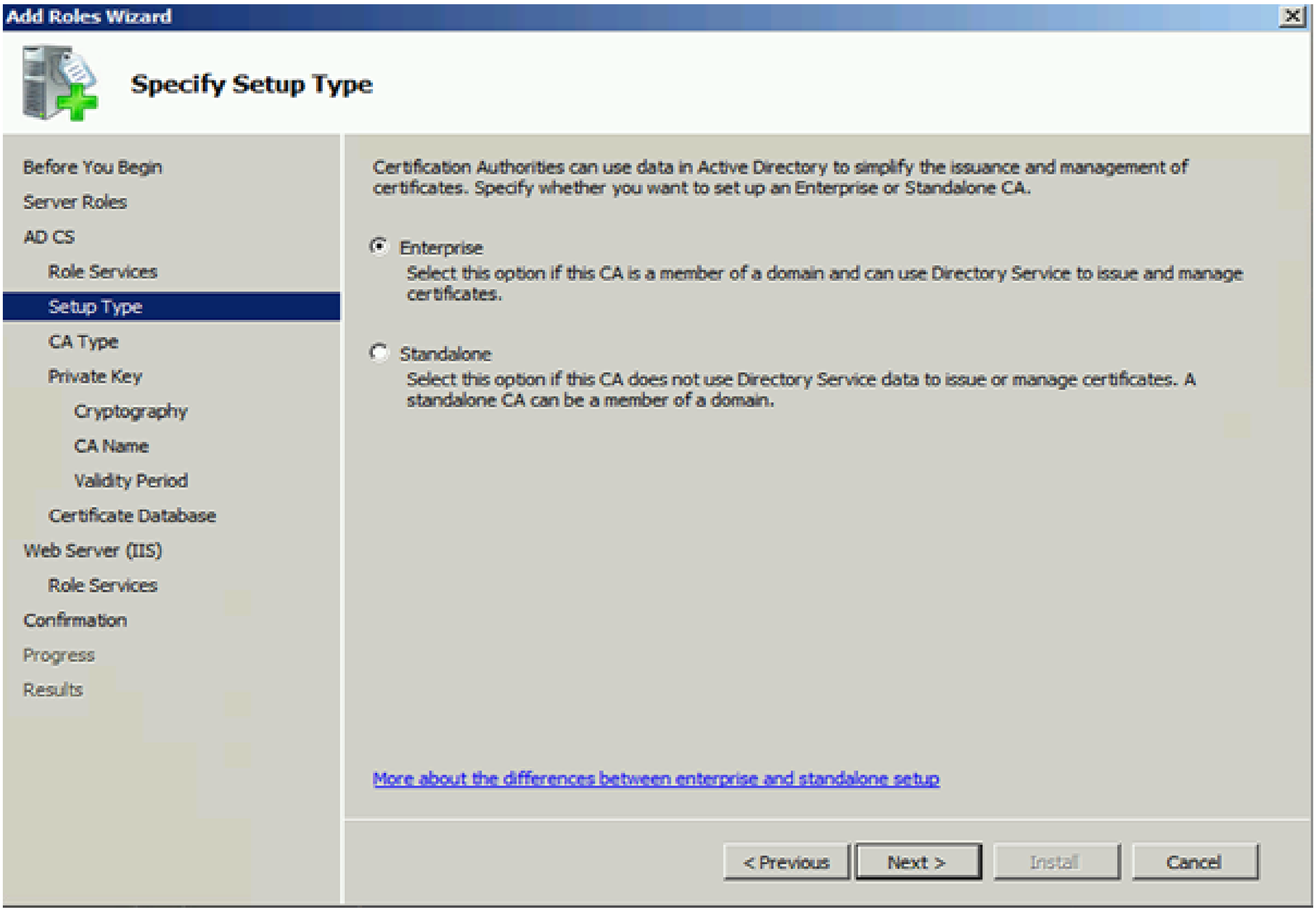
Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

并首先部署这些服务 — 证书颁发机构证书注册策略Web服务。安装这两个角色后，配置它们，然后安**装证书注册Web**服务**和证书颁发机构Web注册**。配置它们。

安装证书颁发机构后，还将添加IIS等其他角色服务和功能。

根据部署，您可以选择企业或独立。



Specify Setup Type

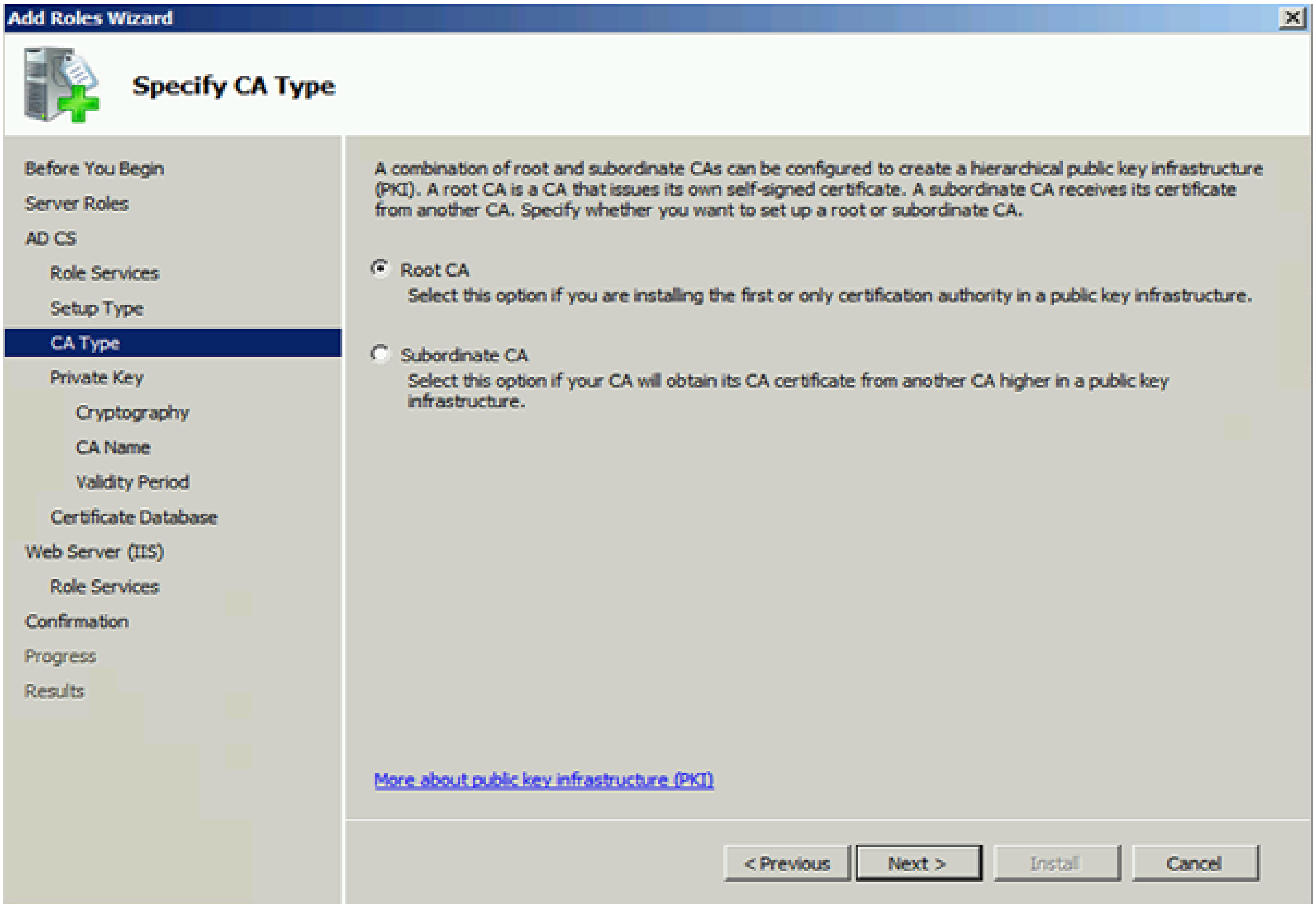
Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

● 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

对于CA类型，可以选择根CA或从属CA。如果组织中没有其他CA正在运行，请选择**根CA**。



Specify CA Type

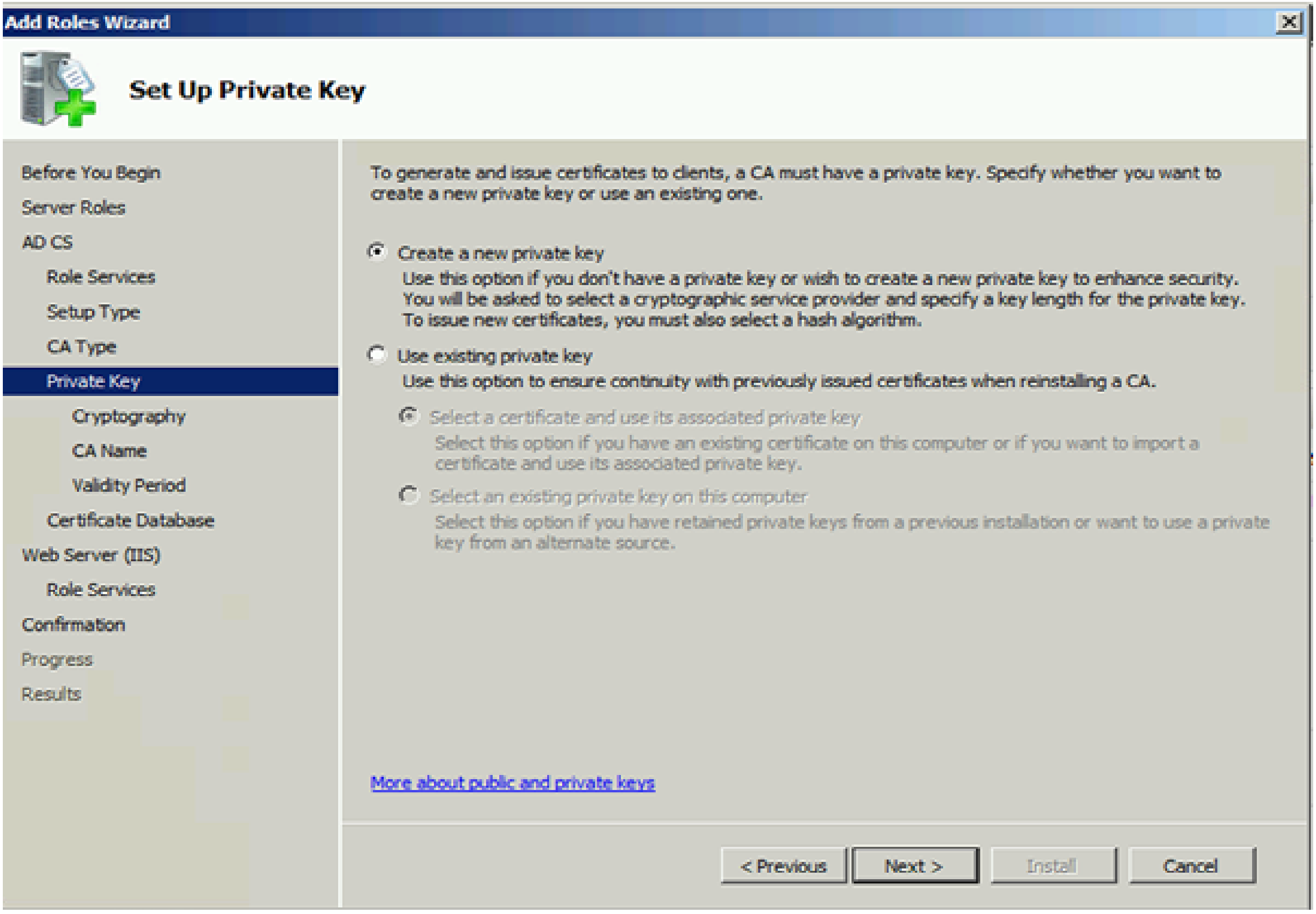
A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

● Root CA
Select this option if you are installing the first or only certification authority in a public key infrastructure.

○ Subordinate CA
Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.

More about public key infrastructure (PKI)

下一步是为CA创建私钥。



Set Up Private Key

To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.

● Create a new private key

Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.

○ Use existing private key

Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

● Select a certificate and use its associated private key

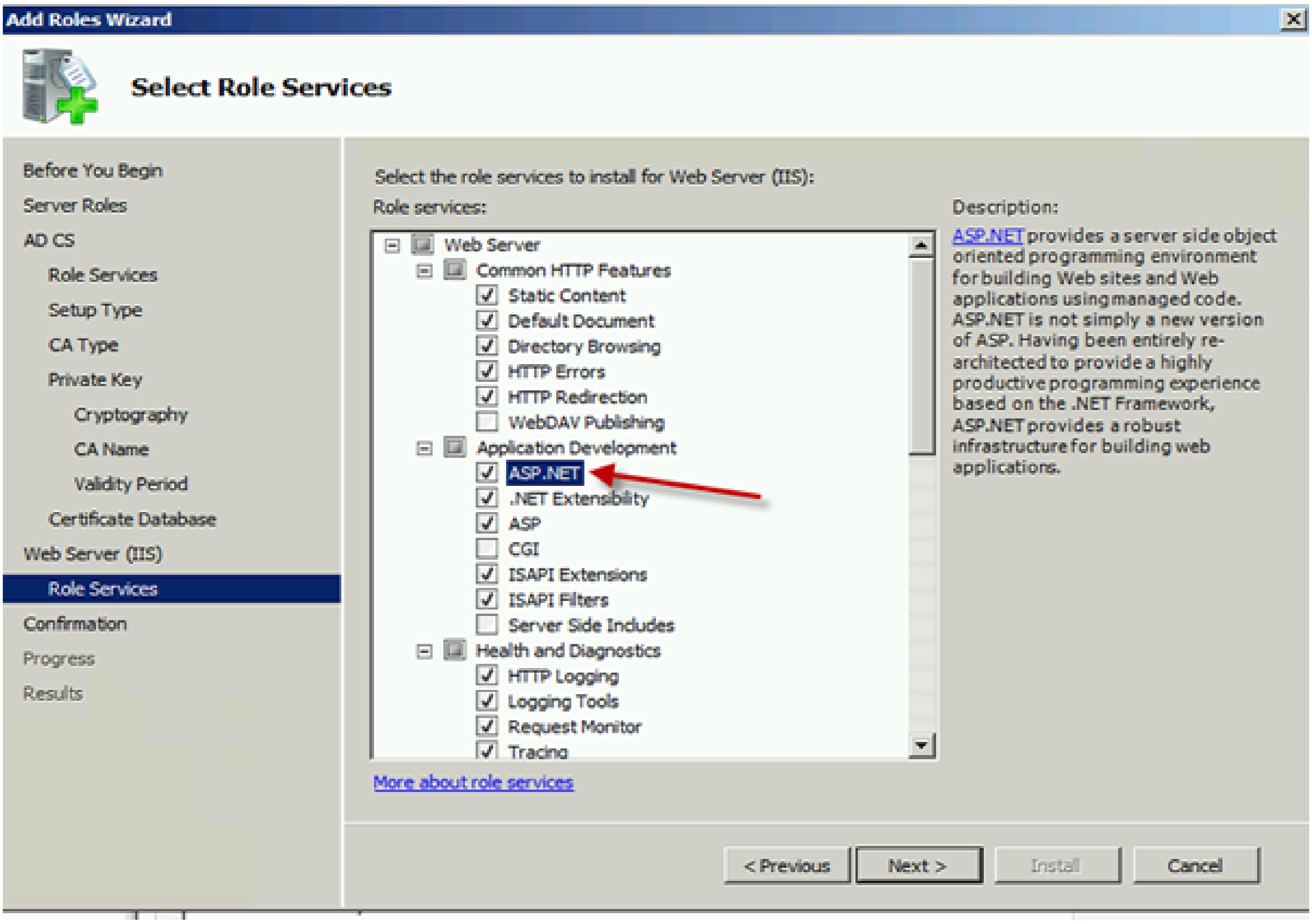
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer

Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

More about public and private keys

只有在单独的Windows Server 2012上安装ADFS3时，才需要执行此步骤。配置CA后，需要配置IIS的角色服务。在CA上进行Web注册时，这是必需的。对于大多数ADFS部署（即IIS中的额外角色），需要单击“应**用程序开**发”下的“ASP.NET”。



Add Roles Wizard

Select Role Services

Select the role services to install for Web Server (IIS):

Role services:

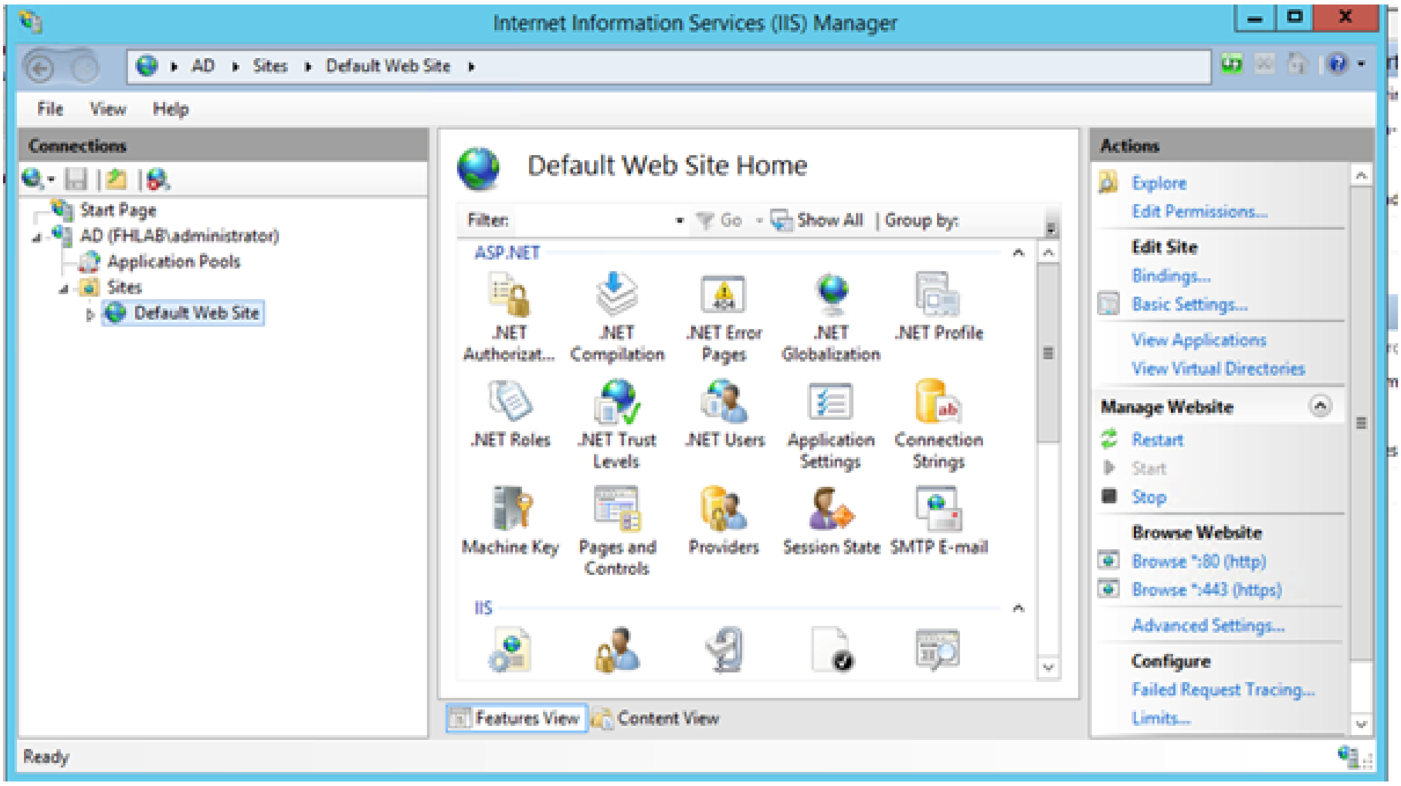
- Web Server
  - Common HTTP Features
    - ☑ Static Content
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ HTTP Redirection
    - □ WebDAV Publishing
  - Application Development
    - ☑ ASP.NET
    - ☑ .NET Extensibility
    - ☑ ASP
    - □ CGI
    - ☑ ISAPI Extensions
    - ☑ ISAPI Filters
    - □ Server Side Includes
  - Health and Diagnostics
    - ☑ HTTP Logging
    - ☑ Logging Tools
    - ☑ Request Monitor
    - ☑ Tracing

Description:

ASP.NET provides a server side object oriented programming environment for building Web sites and Web applications using managed code. ASP.NET is not simply a new version of ASP. Having been entirely re-architected to provide a highly productive programming experience based on the .NET Framework, ASP.NET provides a robust infrastructure for building web applications.

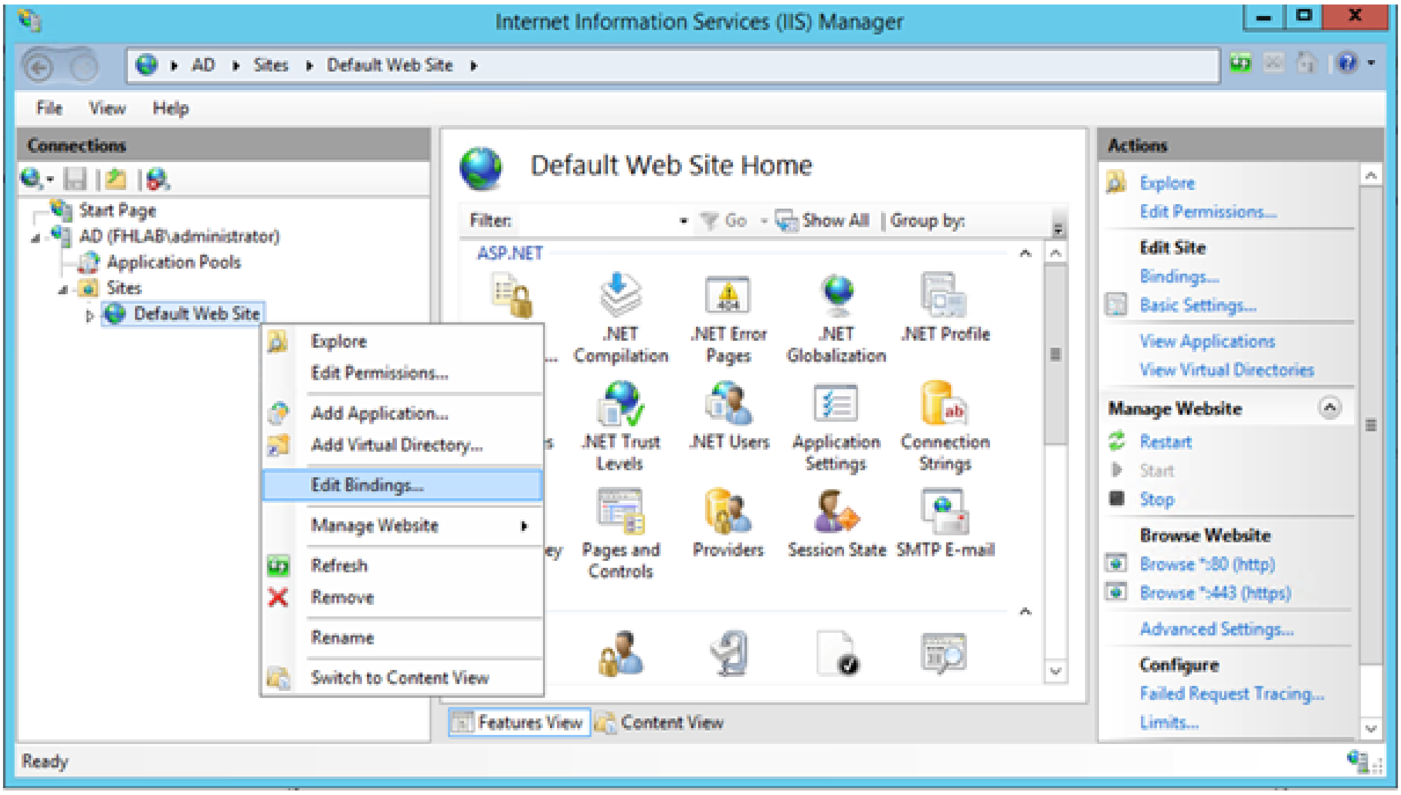
More about role services

在“服务器管理器”中，单**击“Web服务器”>“IIS”**，然后右键单击“默认**网站”**。绑定需要更改，以便除HTTP外还允许HTTPS。这是为了支持HTTPS。

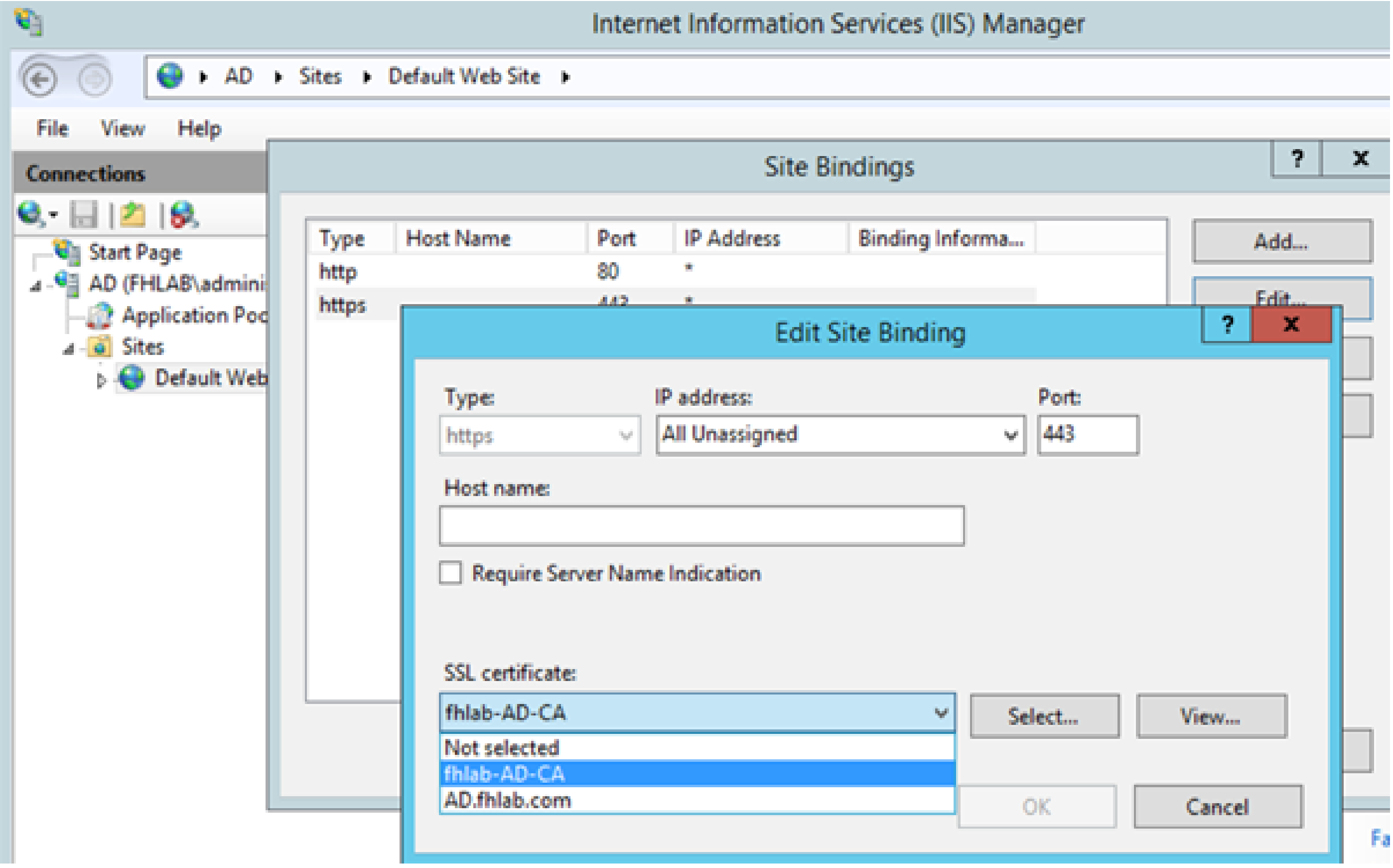


Internet Information Services (IIS) Manager

选择“编**辑绑定**”。



添加新的“站点绑定”并**选择**HTTPS作为类型。对于SSL证书，选择应具有与AD服务器相同的FQDN的服务器证书。



Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	*	

Type: https

IP address: All Unassigned

Port: 443

Host name:

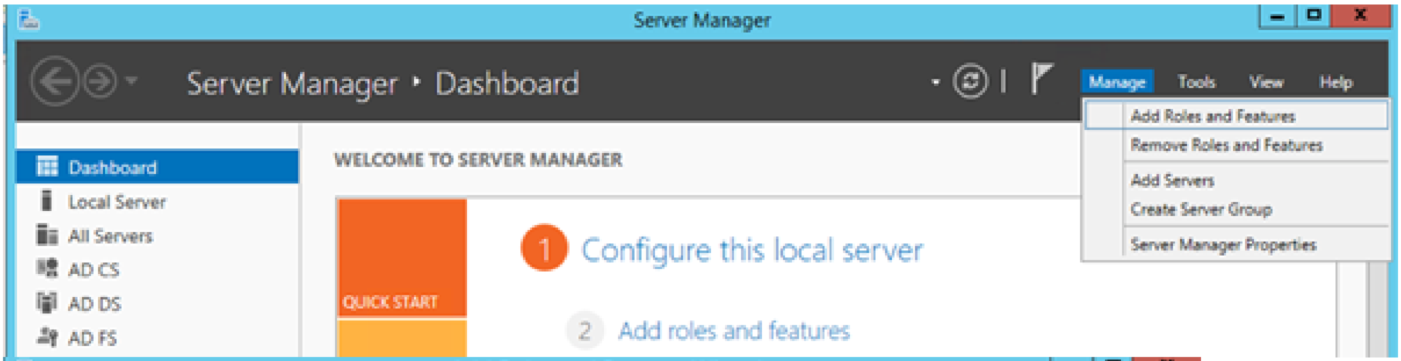
□ Require Server Name Indication

SSL certificate: fhlab-AD-CA

Not selected
fhlab-AD-CA
AD.fhlab.com

所有必备角色都安装在环境中，因此现在您可以继续安装ADFS3 Active Directory联合身份验证服务（在Windows Server 2012上）。

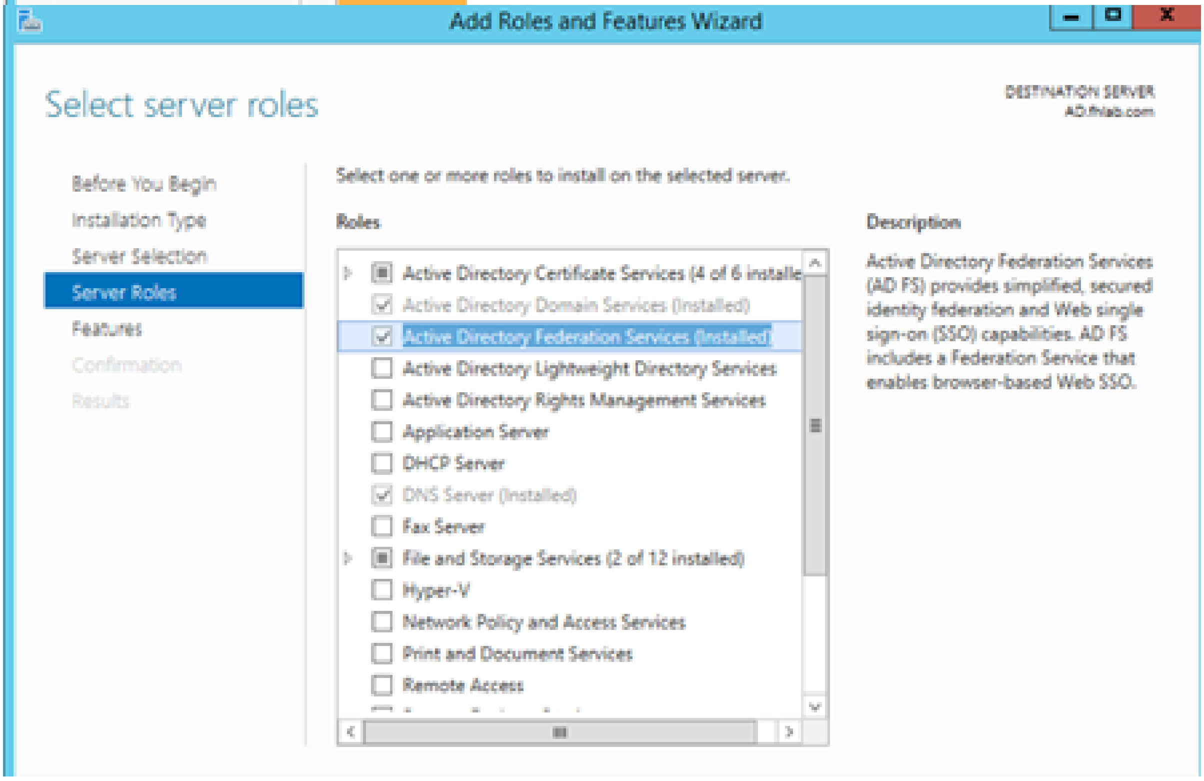
对于“服务器角色”，导航至**“服务器管理器”>“管理”>“添加服务器角色和功能”**，然后选择**Active Directory联合身份验证服务**（如果您在客户网络内部的专用LAN上安装IDP）。



WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features



Select server roles

DESTINATION SERVER
AD.fhlab.com

Select one or more roles to install on the selected server.

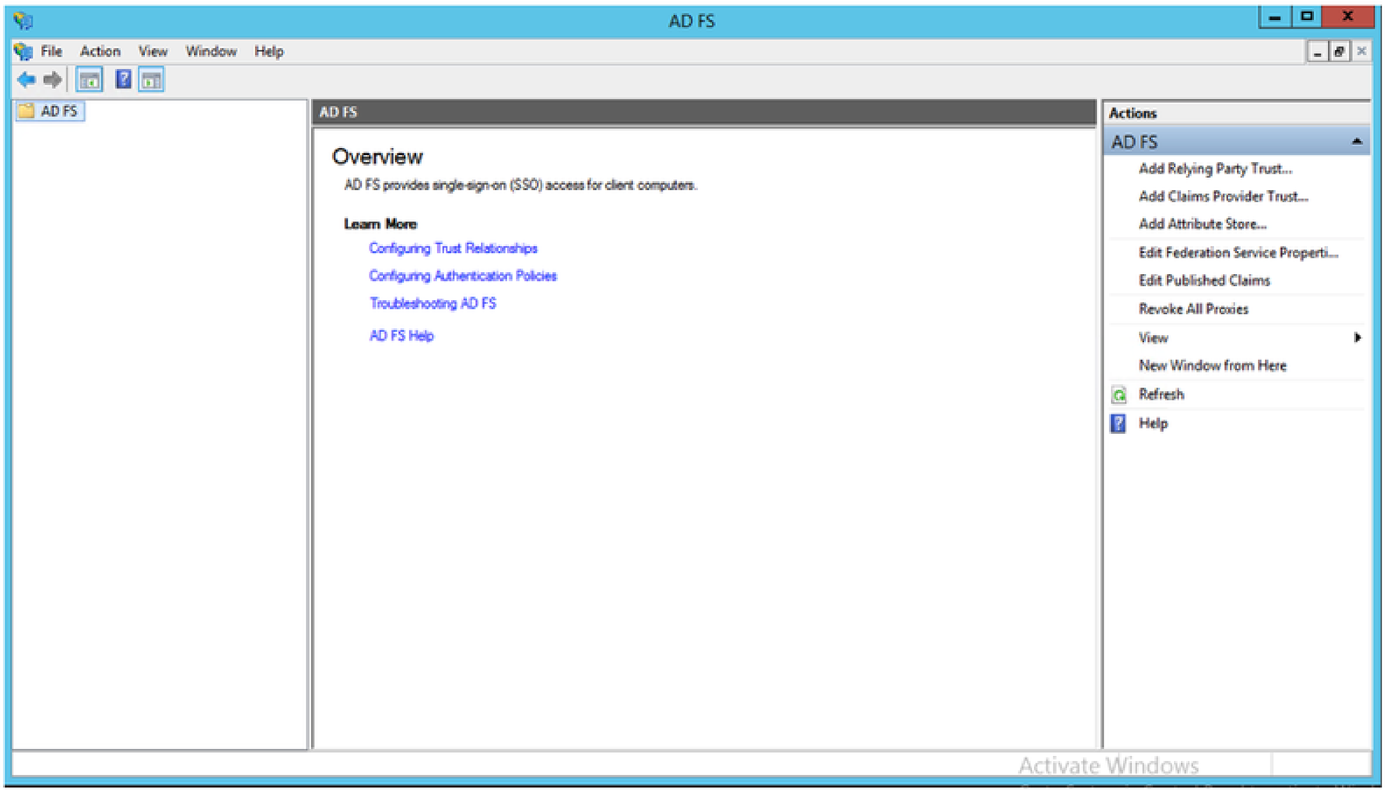
Roles

- ▣ Active Directory Certificate Services (4 of 6 installe
- ☑ Active Directory Domain Services (Installed)
- ☑ Active Directory Federation Services (Installed)
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- ▣ File and Storage Services (2 of 12 installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access

Description

Active Directory Federation Services (AD FS) provides simplified, secured identity federation and Web single sign-on (SSO) capabilities. AD FS includes a Federation Service that enables browser-based Web SSO.

安装完成后，您可以从任务栏或开始菜单打开它。



Overview

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

Learn More

Configuring Trust Relationships

Configuring Authentication Policies

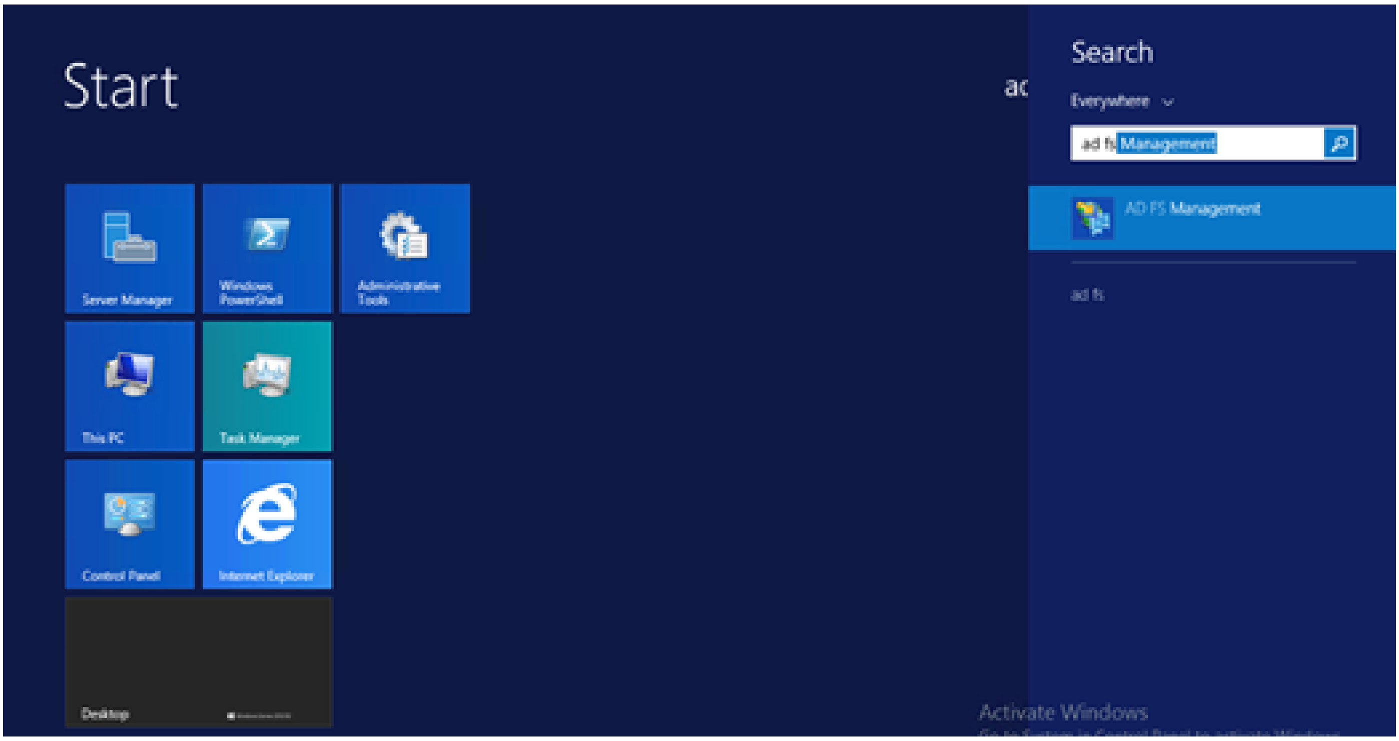
Troubleshooting AD FS

AD FS Help

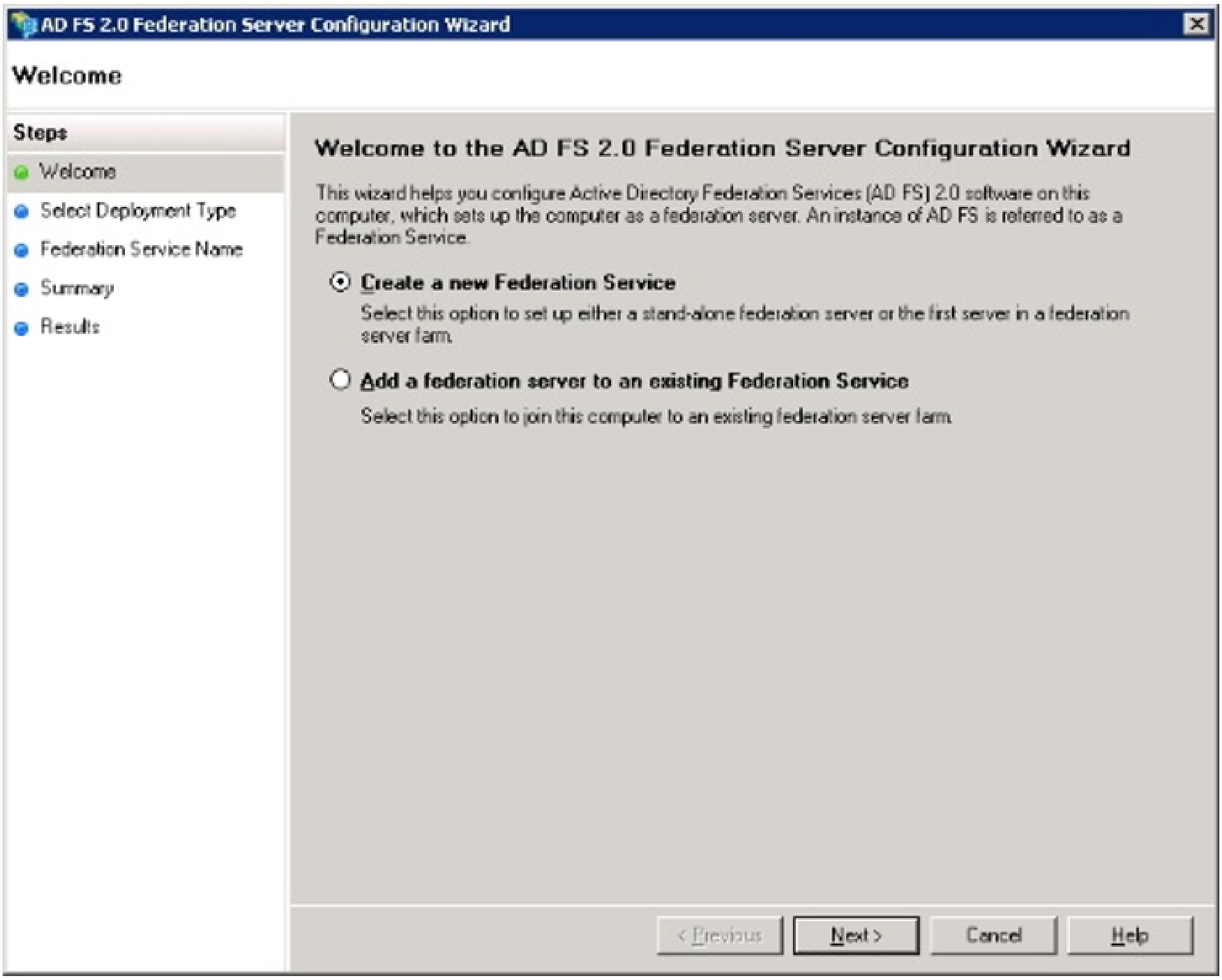
ADFS3初始配置

本节将介绍新的独立联合服务器的安装过程，但也可用于在域控制器上安装该服务器

选择**Windows**并键入**AD FS Management**以启动ADFS管理控制台，如图所示。



选择**AD FS 3.0联合服务器配置向**导选项以启动ADFS服务器配置。这些屏幕截图代表AD FS 3中的相同步骤。



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.

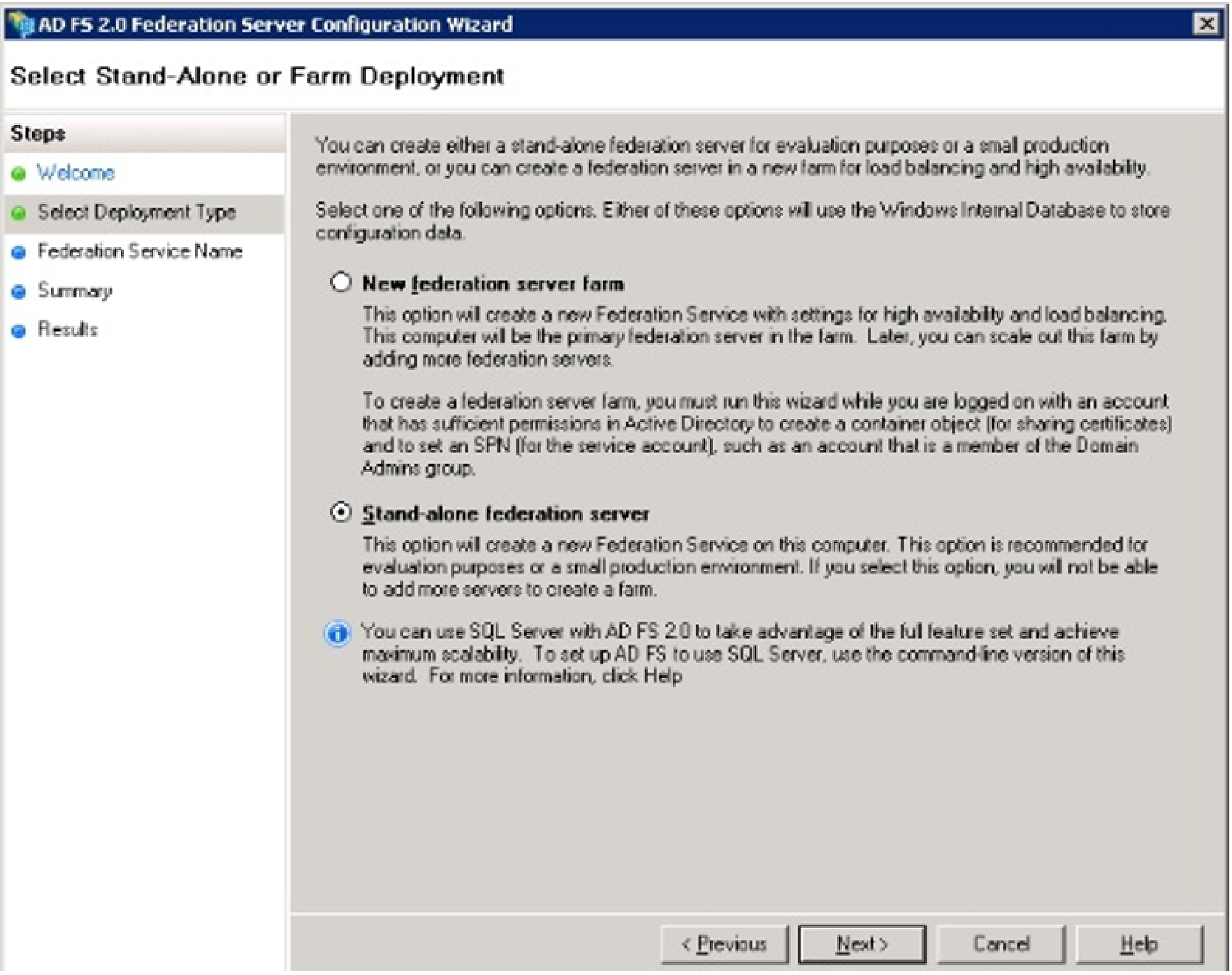
● Create a new Federation Service

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.

选择“创建新联合**身份验证服**务”并单**击“下一**步”。



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.

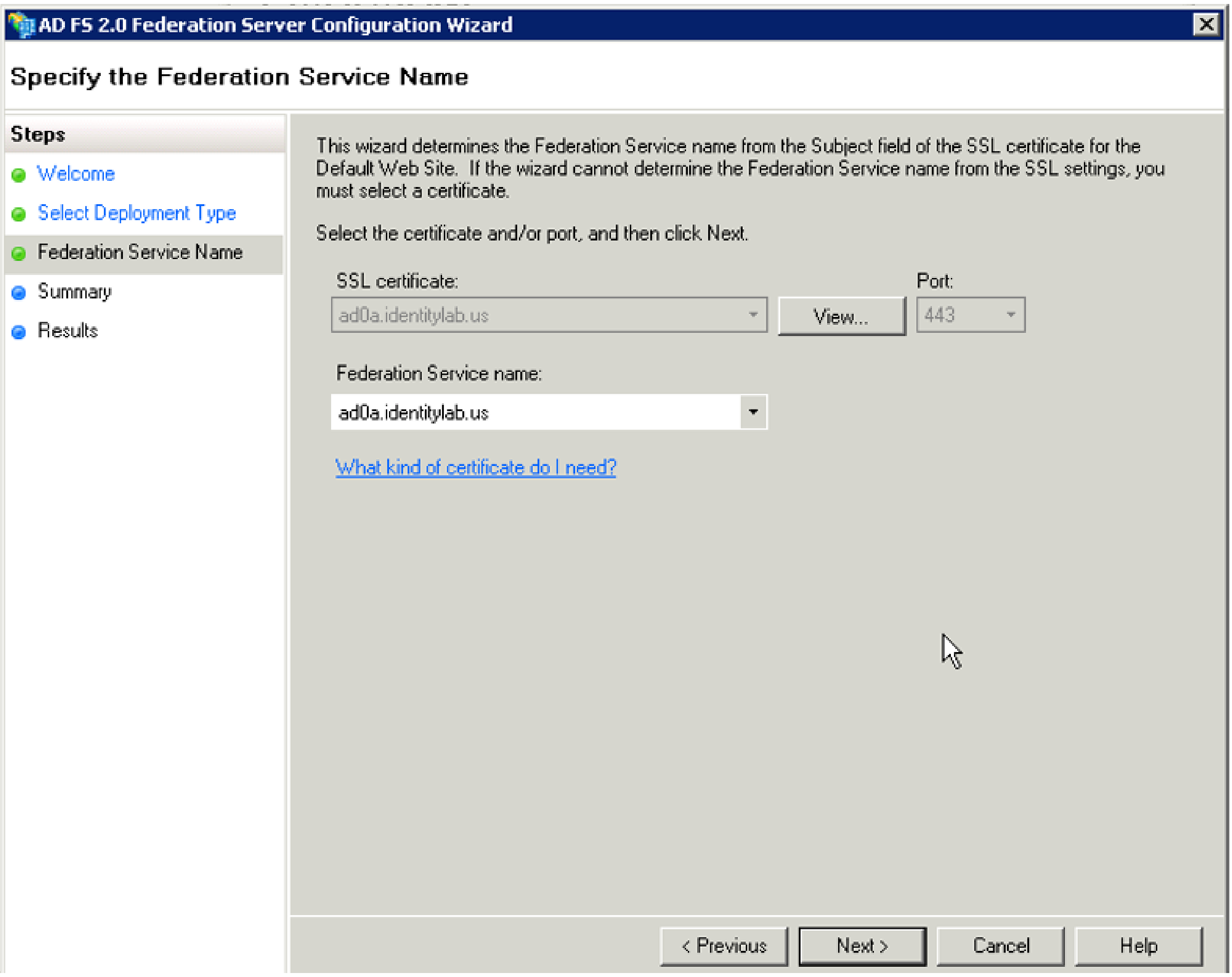
To create a federation server farm, you must run this wizard while you are logged on with an account that has sufficient permissions in Active Directory to create a container object (for sharing certificates) and to set an SPN (for the service account), such as an account that is a member of the Domain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

选择Stand-alone Federation Server，然后单击**Next(下一步)**，如图所示。



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.

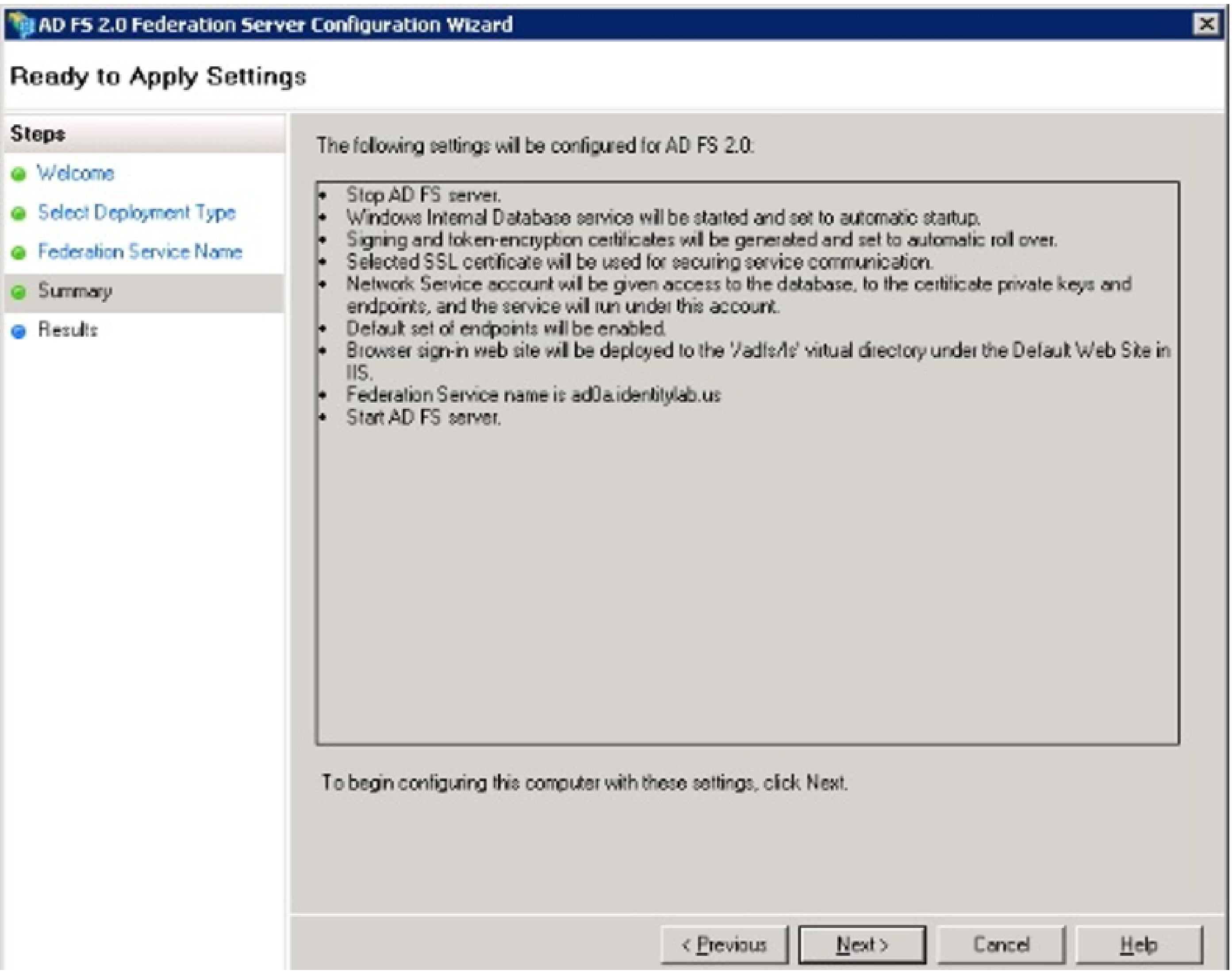
Select the certificate and/or port, and then click Next.

SSL certificate: ad0a.identitylab.us

Port: 443

Federation Service name: ad0a.identitylab.us

在SSL证书下，从列表中选择自签名证书。联合身份验证服务名称将自动填充。单击 **Next**。



AD FS 2.0 Federation Server Configuration Wizard

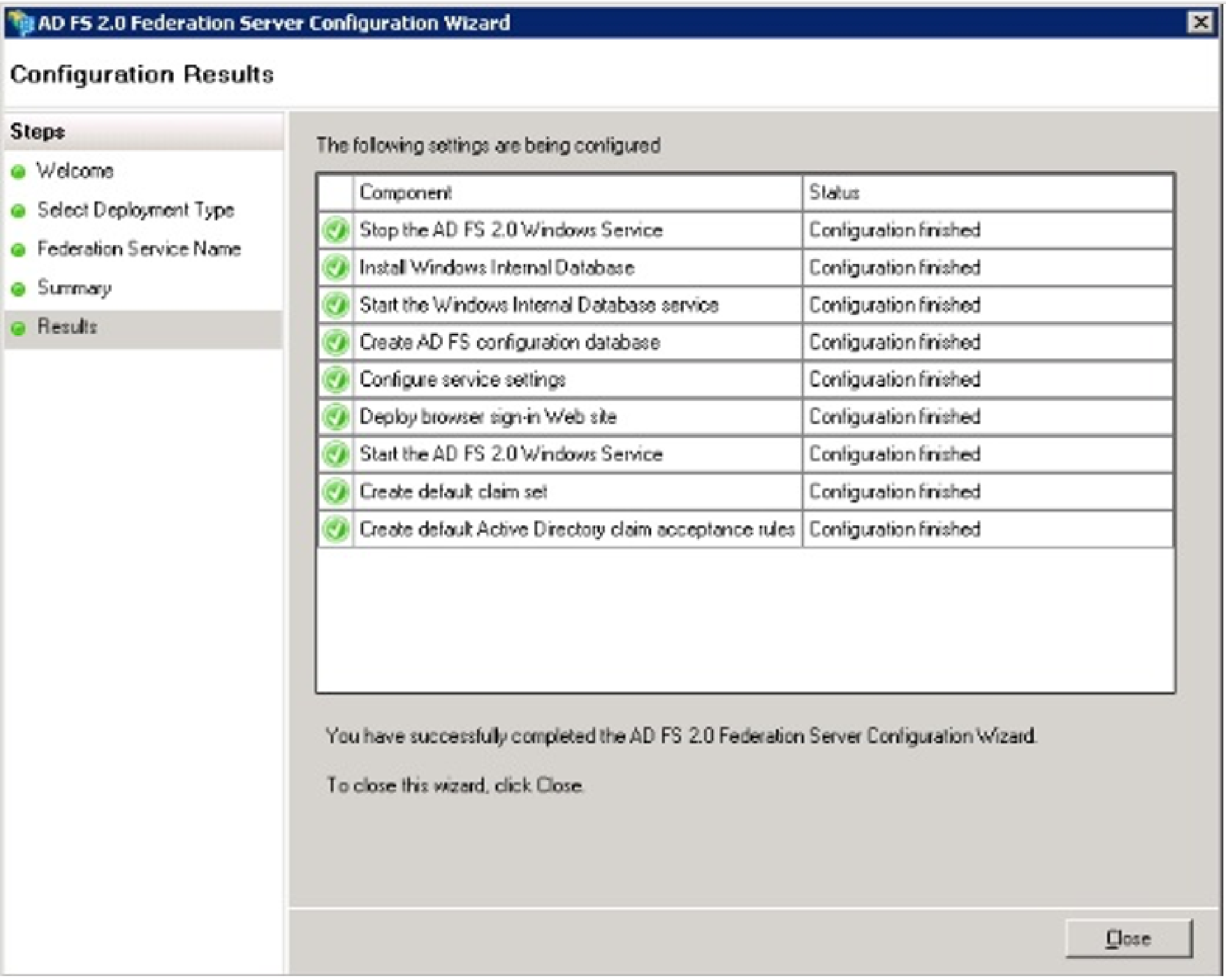
Ready to Apply Settings

The following settings will be configured for AD FS 2.0:

- Stop AD FS server.
- Windows Internal Database service will be started and set to automatic startup.
- Signing and token-encryption certificates will be generated and set to automatic roll over.
- Selected SSL certificate will be used for securing service communication.
- Network Service account will be given access to the database, to the certificate private keys and endpoints, and the service will run under this account.
- Default set of endpoints will be enabled.
- Browser sign-in web site will be deployed to the '/adfs/ls' virtual directory under the Default Web Site in IIS.
- Federation Service name is ad0a.identitylab.us
- Start AD FS server.

To begin configuring this computer with these settings, click Next.

查看设置并单击“下**一步”**以应用设置。



AD FS 2.0 Federation Server Configuration Wizard

Configuration Results

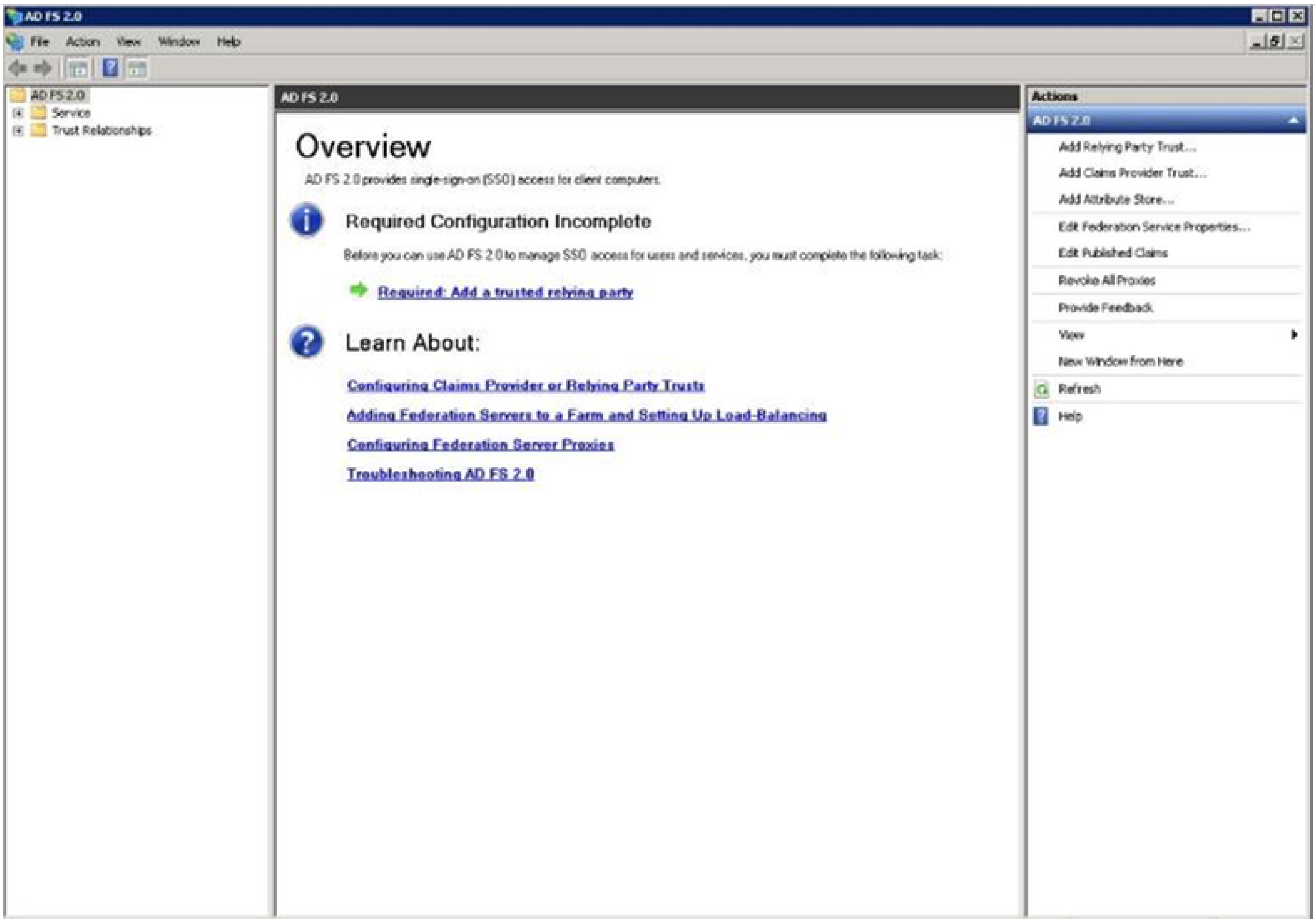
The following settings are being configured

	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.

确认所有组件都已成功完成，然后单击**关闭**以结束向导并返回主管理控制台。这可能需要几分钟。



Overview

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

Required Configuration Incomplete

Before you can use AD FS 2.0 to manage SSO access for users and services, you must complete the following task:

Required: Add a trusted relying party

Learn About:

Configuring Claims Provider or Relying Party Trusts

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

Configuring Federation Server Proxies

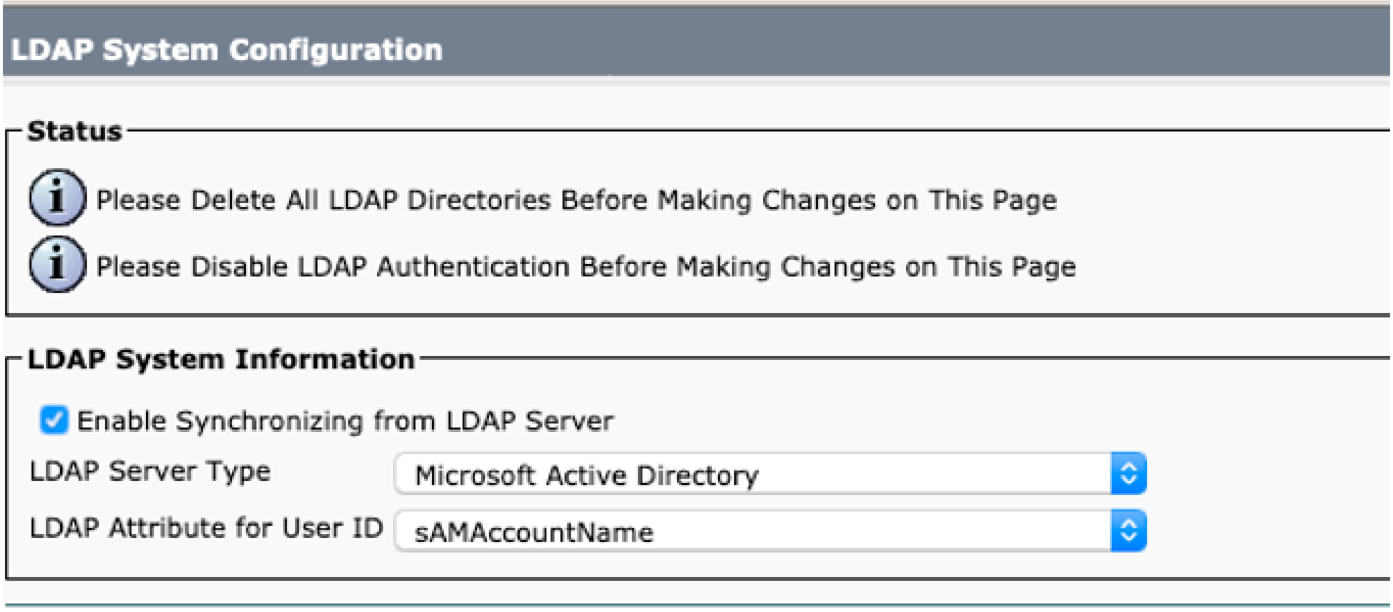
Troubleshooting AD FS 2.0

ADFS现在已有效启用并配置为身份提供程序(IdP)。 接下来，您需要将CUCM添加为可信赖的合作伙伴。在执行此操作之前，您需要先在CUCM管理中执行一些配置。

使用ADFS在CUCM上配置SSO

LDAP配置

群集需要与Active Directory进行LDAP集成，并且在进一步配置之前，需要配置LDAP身份验证。导航至**系统选项卡> LDAP**系统，如图所示。



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

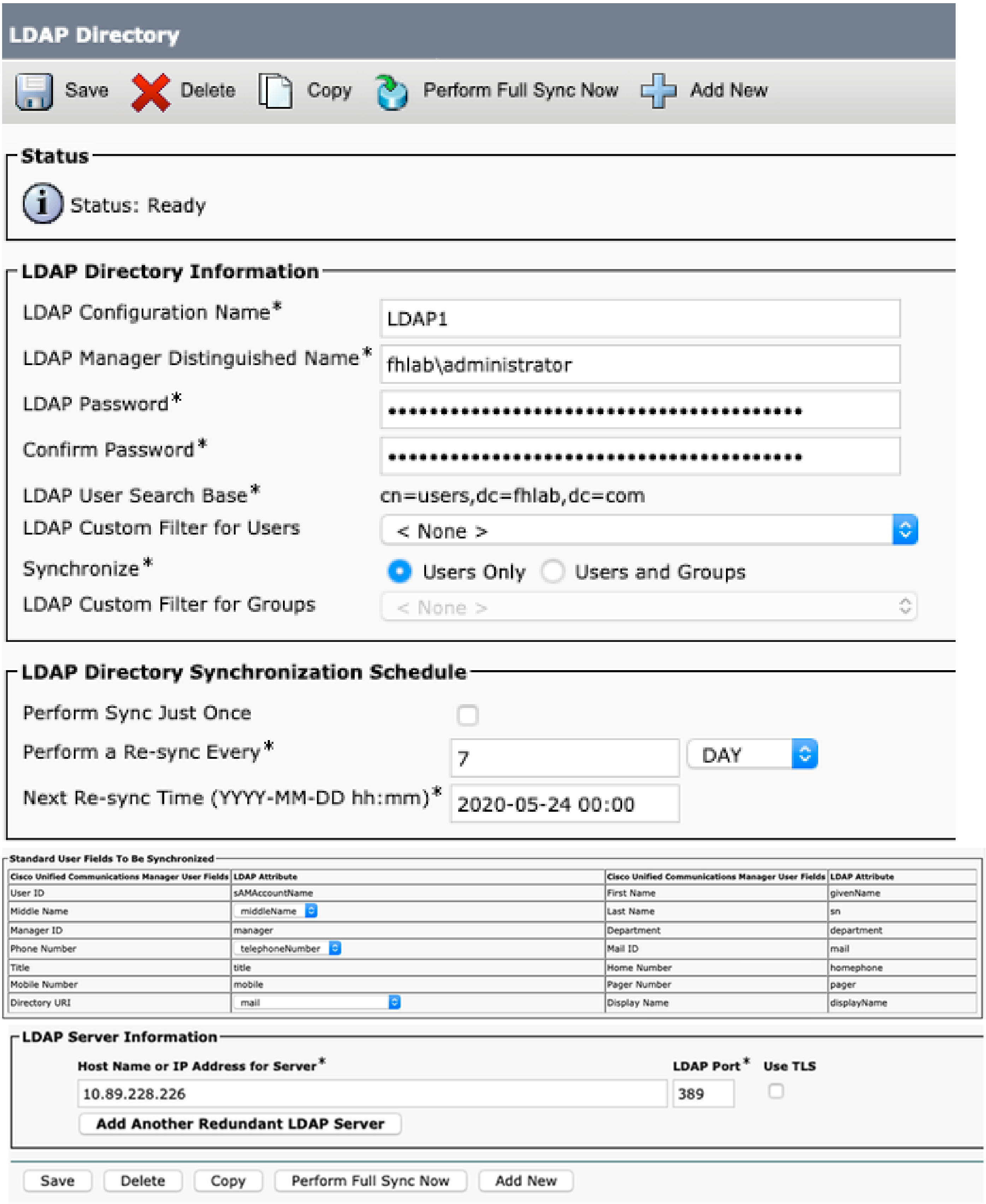
LDAP System Information

☑ Enable Synchronizing from LDAP Server

LDAP Server Type: Microsoft Active Directory

LDAP Attribute for User ID: sAMAccountName

然后，导航至“系统”**选项卡>“LDAP目录**”。



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

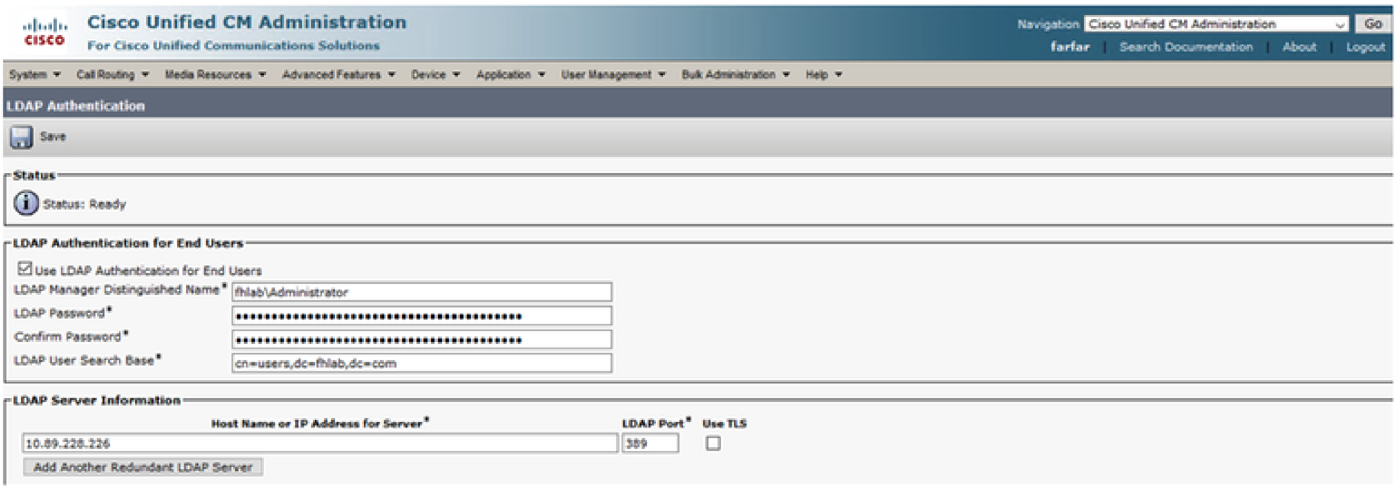
Standard User Fields To Be Synchronized

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
10.89.228.226	389	□

在Active Directory用户与CUCM同步后，需要配置LDAP身份验证。


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
Go
farfar | Search Documentation | About | Logout
System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾
Save
Add Another Redundant LDAP Server

LDAP Authentication

Status

Status: Ready

LDAP Authentication for End Users

☑ Use LDAP Authentication for End Users

LDAP Manager Distinguished Name* fhlab\Administrator

LDAP Password* ••

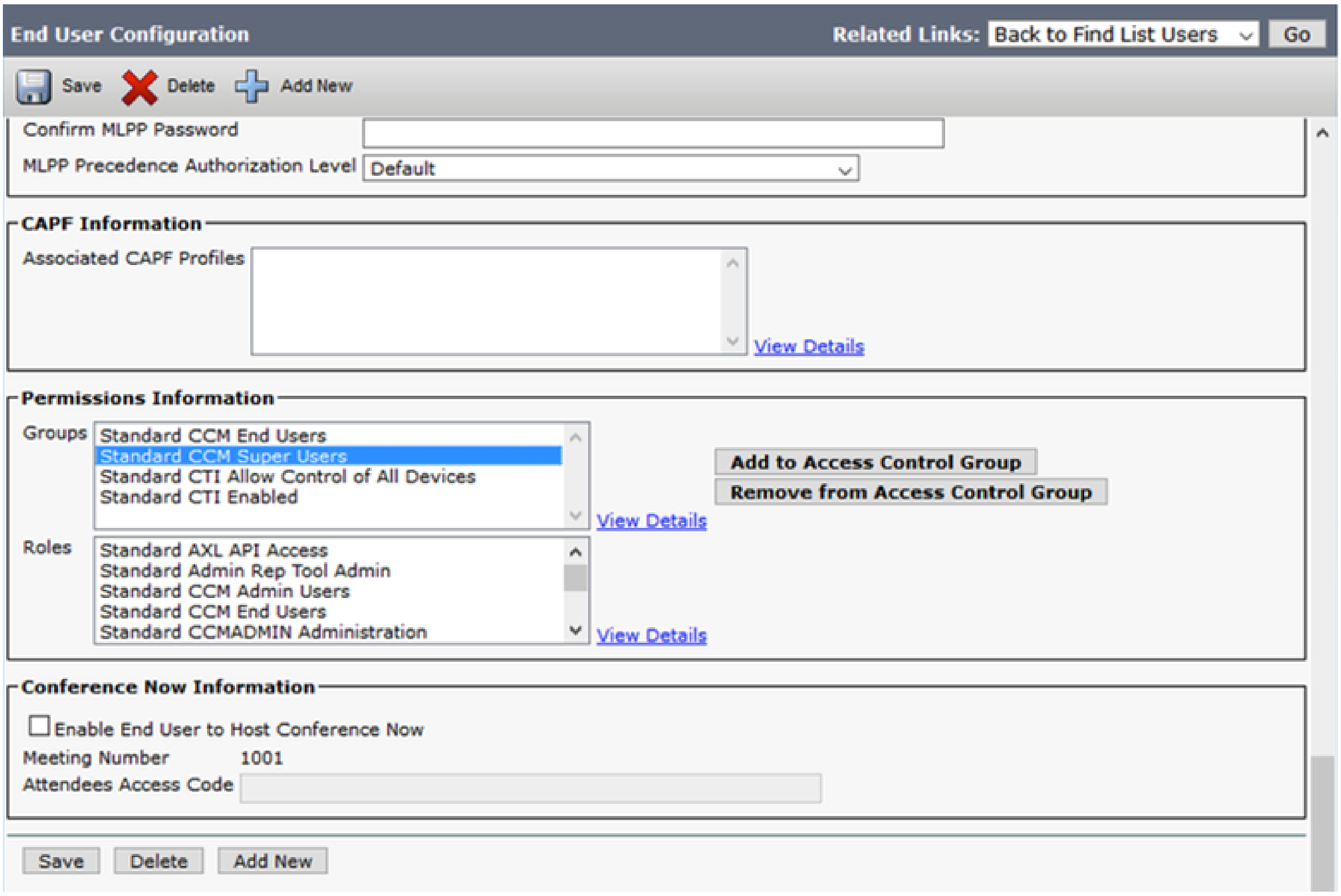
Confirm Password* ••

LDAP User Search Base* cn=users,dc=fhlab,dc=com

LDAP Server Information

Host Name or IP Address for Server*	LDAP Port*	Use TLS
10.89.228.226	389	□

CUCM中的最终用户需要将特定访问控制组分配给其最终用户配置文件。ACG是标准CCM超级用户。当环境就绪时，用户将用于测试SSO。


Related Links: Back to Find List Users
Go
Save
Delete
Add New
View Details
View Details
View Details
Add to Access Control Group
Remove from Access Control Group
Save
Delete
Add New

End User Configuration

Confirm MLPP Password

MLPP Precedence Authorization Level Default

CAPF Information

Associated CAPF Profiles

Permissions Information

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

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

Conference Now Information

□ Enable End User to Host Conference Now

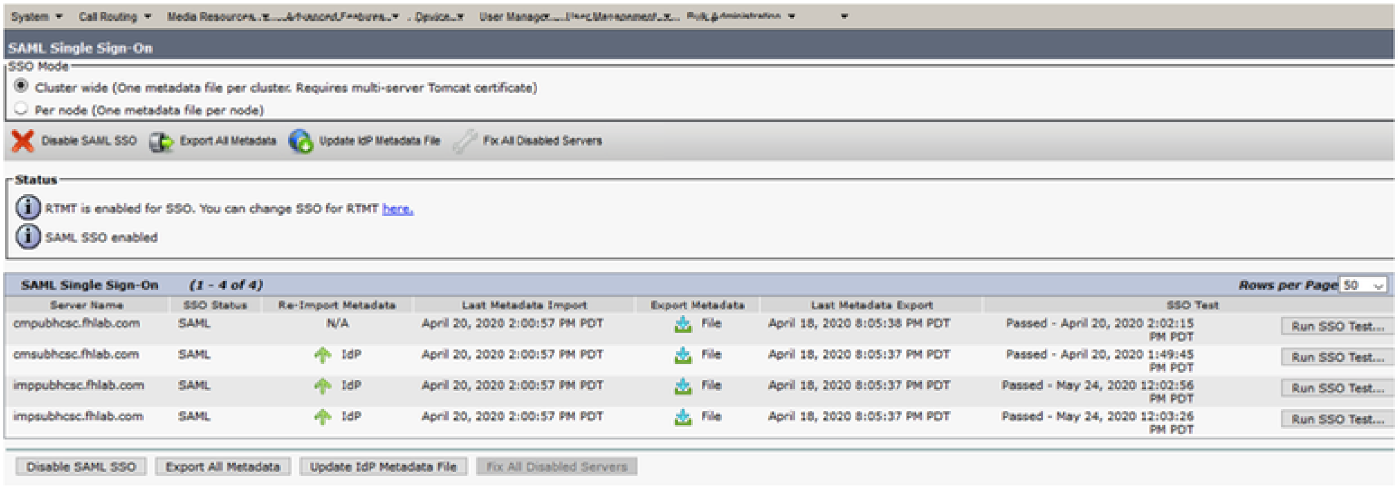
Meeting Number 1001

Attendees Access Code

CUCM元数据

本节将显示CUCM发布者的流程。

第一项任务是获取CUCM元数据，您需要浏览到URL;**https://<CUCM Pub FQDN>:8443/ssosp/ws/config/metadata/sp**，或者可以从**System选项卡> SAML Single Sign-on下载**。这可以按节点或集群范围完成。首选执行此集群范围。



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

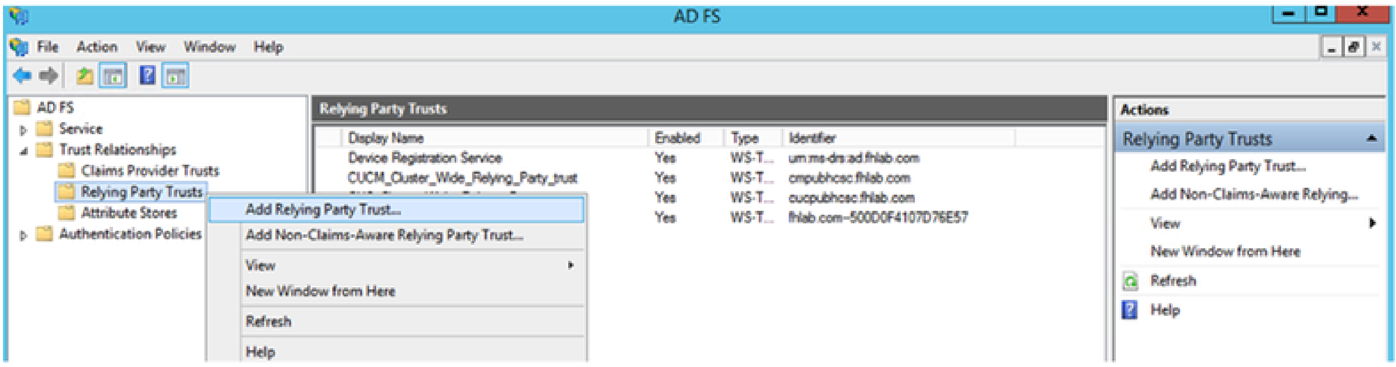
SAML Single Sign-On (1 - 4 of 4) Rows per Page 50

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	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	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	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	Run SSO Test...

使用有意义的名称（如sp_cucm0a.xml）将数据保存到本地，之后您将需要它。

配置ADFS信赖方

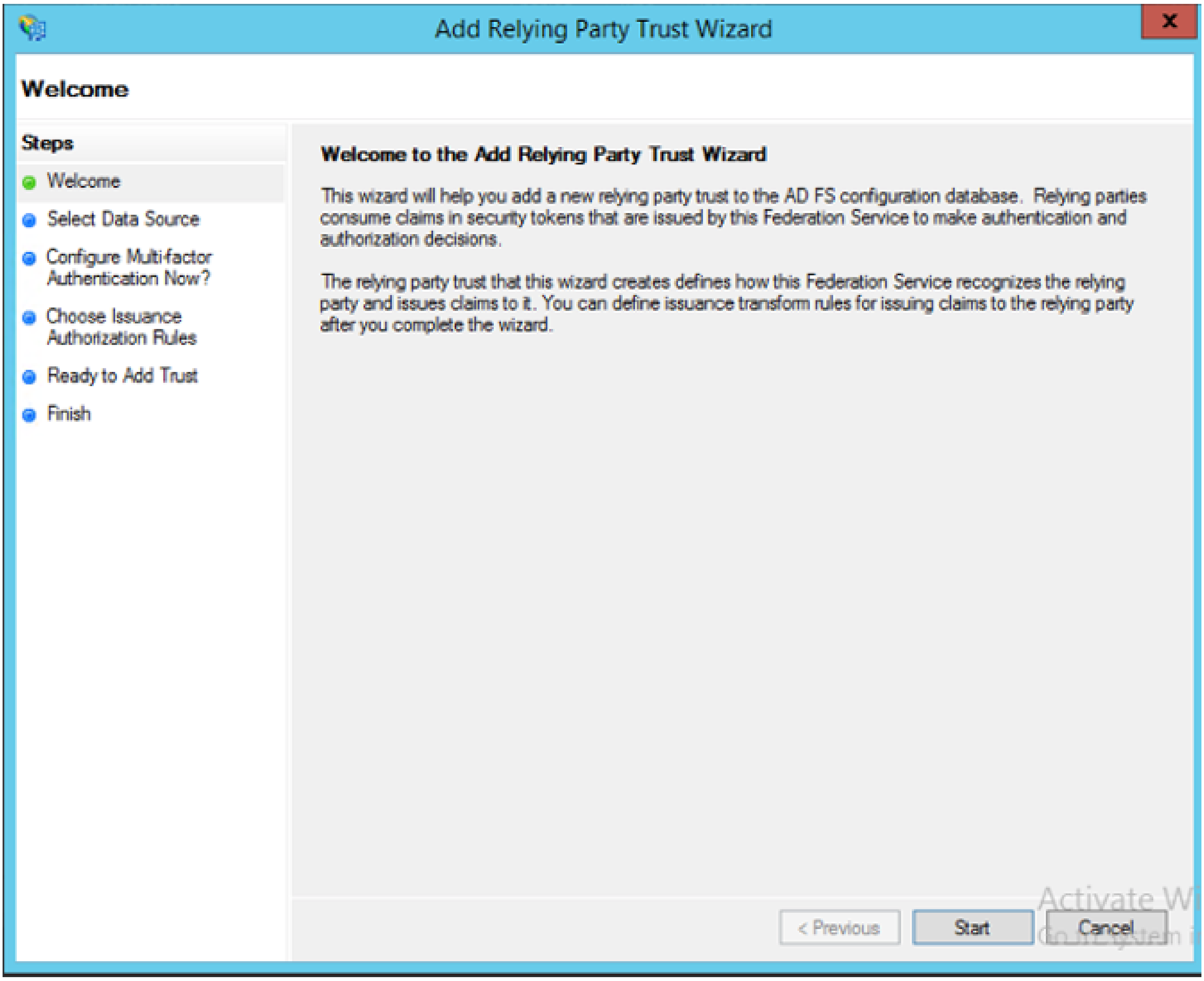
反向到AD FS 3.0管理控制台。



Relying Party Trusts

Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-T...	urn:ms-drs:ad.fhlab.com
CUCM_Cluster_Wide_Relying_Party_trust	Yes	WS-T...	cmpubhcsc.fhlab.com
[illegible]	Yes	WS-T...	cucpubhcsc.fhlab.com
	Yes	WS-T...	fhlab.com-500D0F4107D76E57

单击“添加信赖方信任向导”。



Welcome

Welcome to the Add Relying Party Trust Wizard

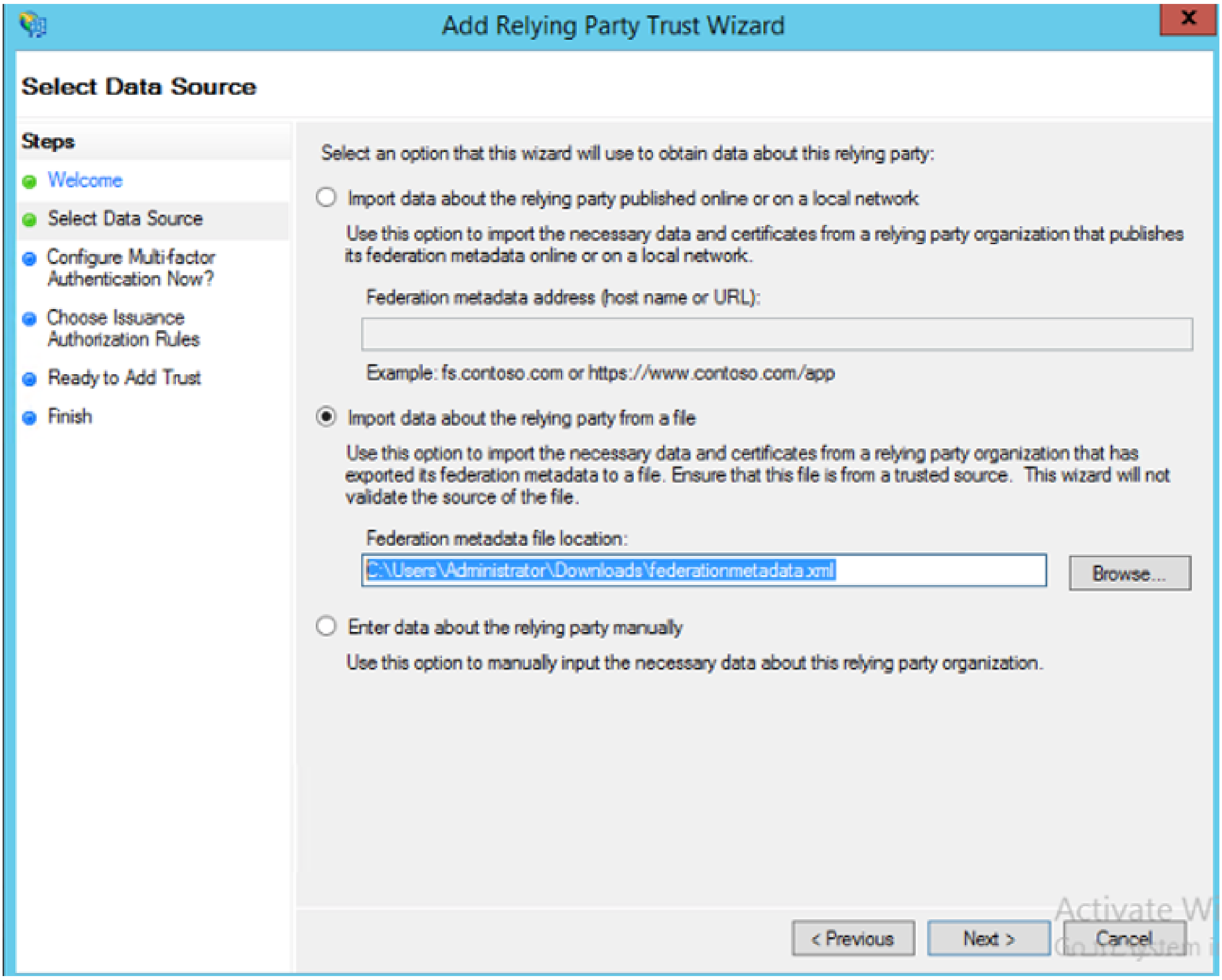
This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.

Add Relying Party Trust Wizard
Steps
Welcome
Select Data Source
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
< Previous
Start
Cancel
Activate Wi

单击**Start(开**始)继续。

选择您**之前保存的**federationmedata.xml元数据XML文件，然后单击**下一步**。



Add Relying Party Trust Wizard

Select Data Source

Steps
Welcome
Select Data Source
Configure Multi-factor Authentication Now?
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.

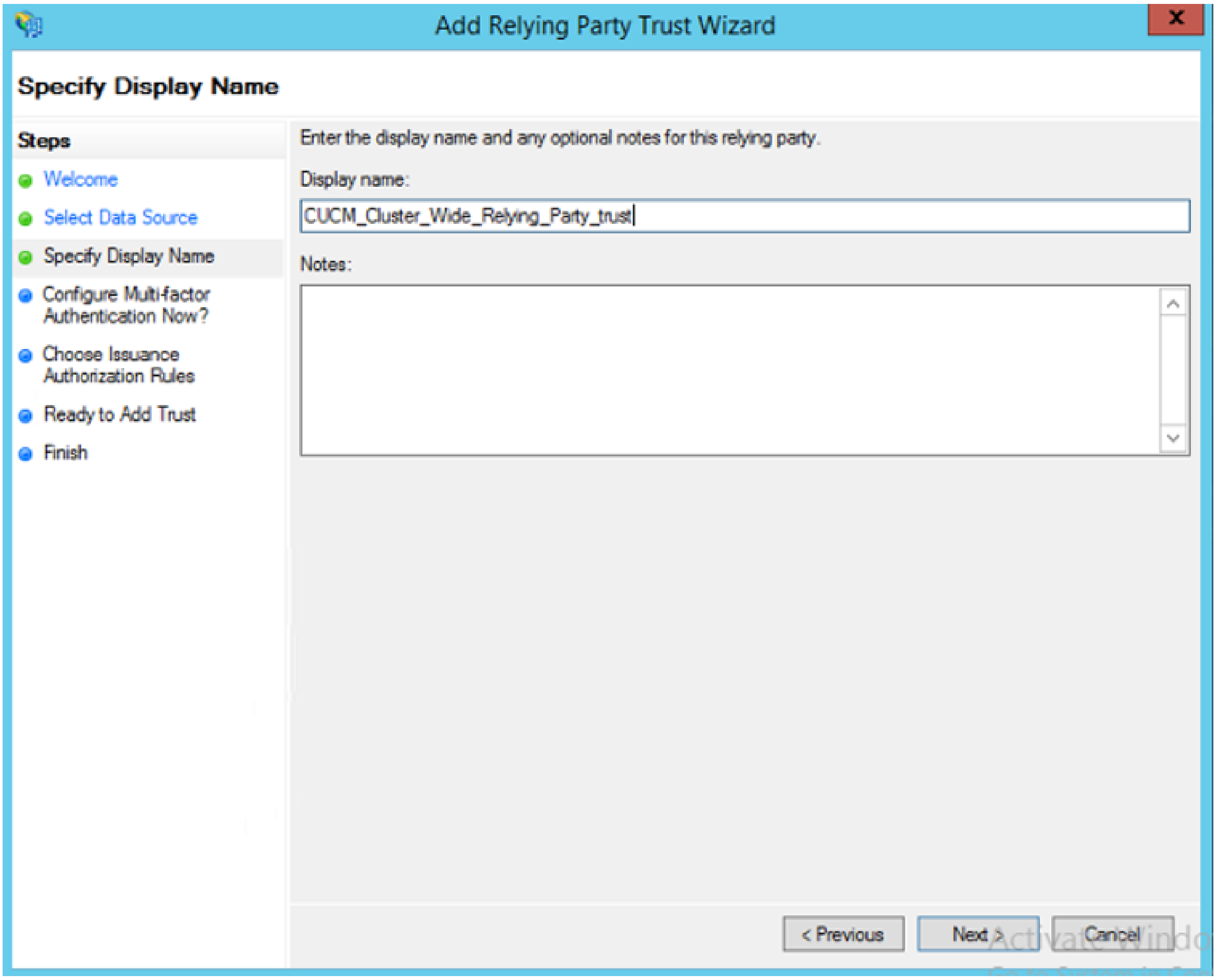
Federation metadata file location:

C:\Users\Administrator\Downloads\federationmetadata.xml

○ Enter data about the relying party manually

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

使用CUCM_Cluster_Wide_Releing_Party_trust作为显示名称，然后单击Next。



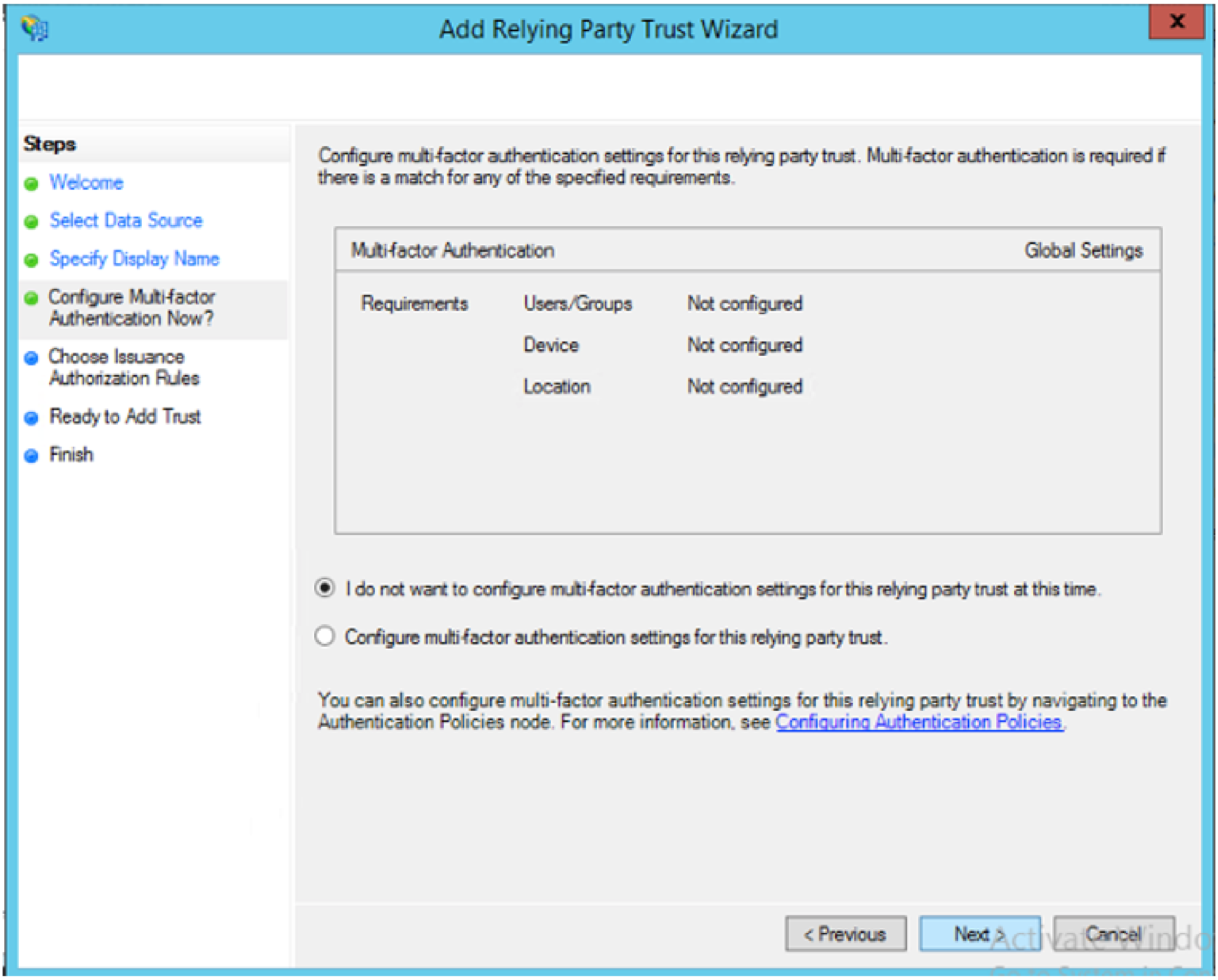
Enter the display name and any optional notes for this relying party.

Display name:

CUCM_Cluster_Wide_Relying_Party_trust

Notes:

选择第一个选项，然后单击“下**一步”**。



Add Relying Party Trust Wizard
Steps
Welcome
Select Data Source
Specify Display Name
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
< Previous
Next >
Cancel

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

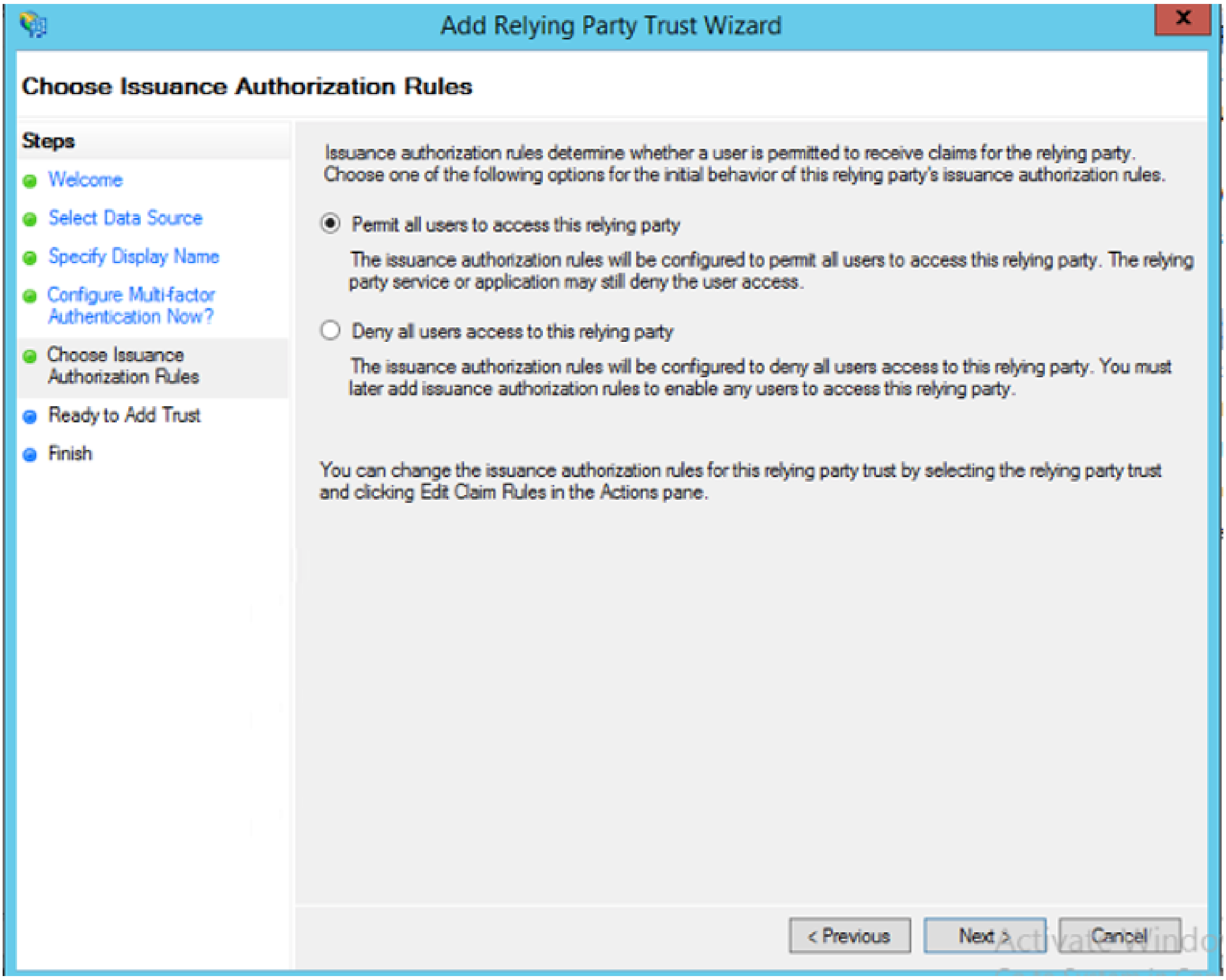
Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

● I do not want to configure multi-factor authentication settings for this relying party trust at this time.

○ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see Configuring Authentication Policies.

选择**允许所有用户访问此信赖方**，然后单击**下一步**，如图所示。



Choose Issuance Authorization Rules

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

● Permit all users to access this relying party

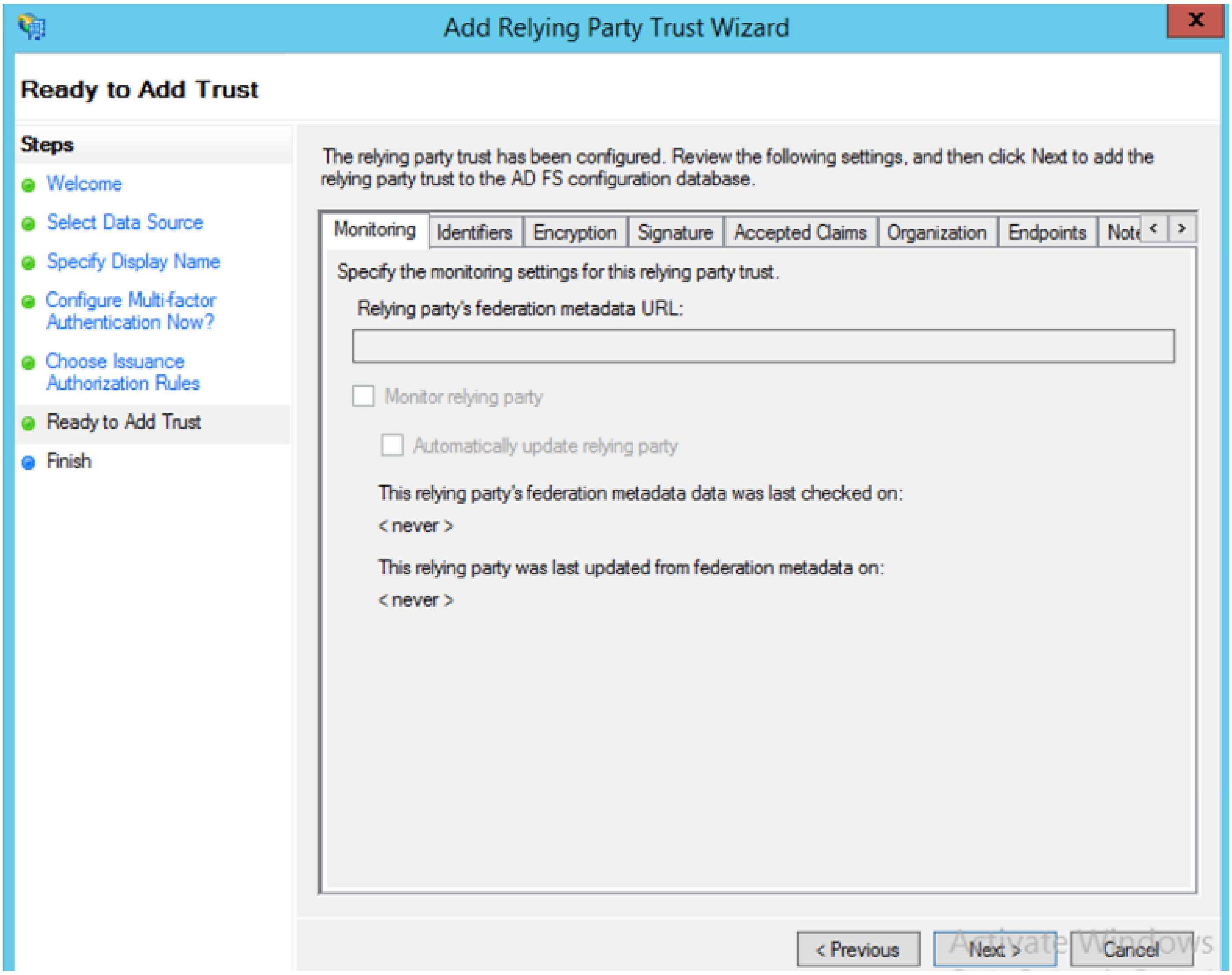
The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

查看配置并单击**Next**(如图所示)。



The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

□ Monitor relying party

□ Automatically update relying party

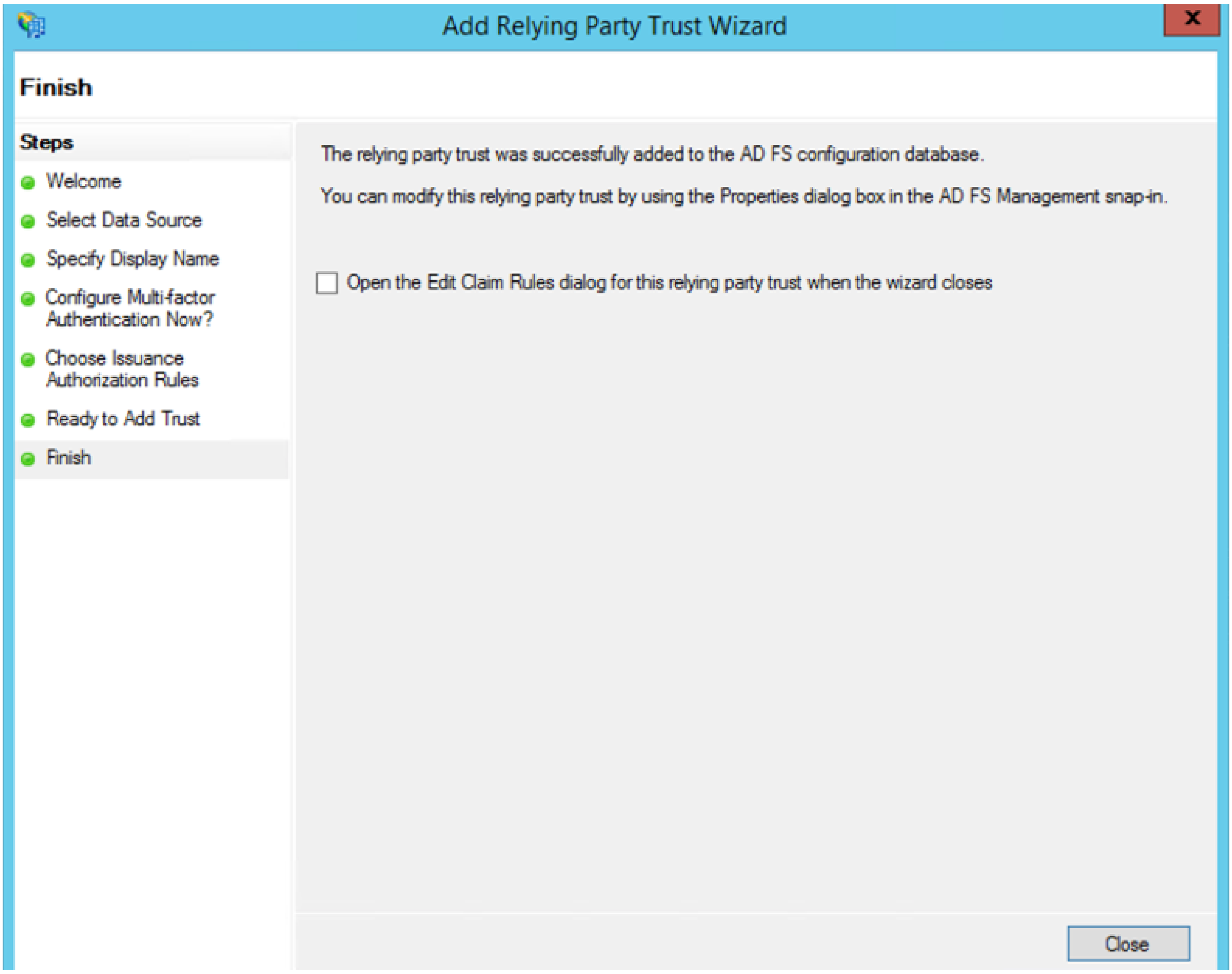
This relying party's federation metadata data was last checked on:

< never >

This relying party was last updated from federation metadata on:

< never >

取消选中此框，然后单击“**关闭**”。

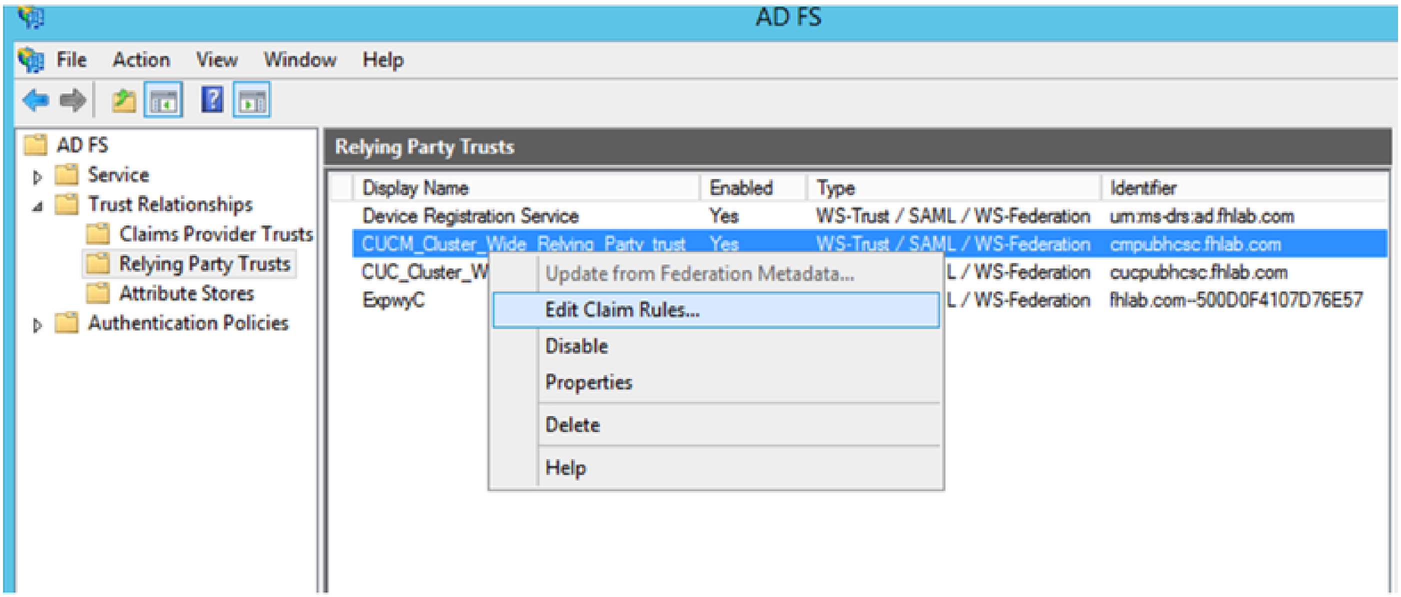

Add Relying Party Trust Wizard
Finish
Steps
Welcome
Select Data Source
Specify Display Name
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Close

The relying party trust was successfully added to the AD FS configuration database.

You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.

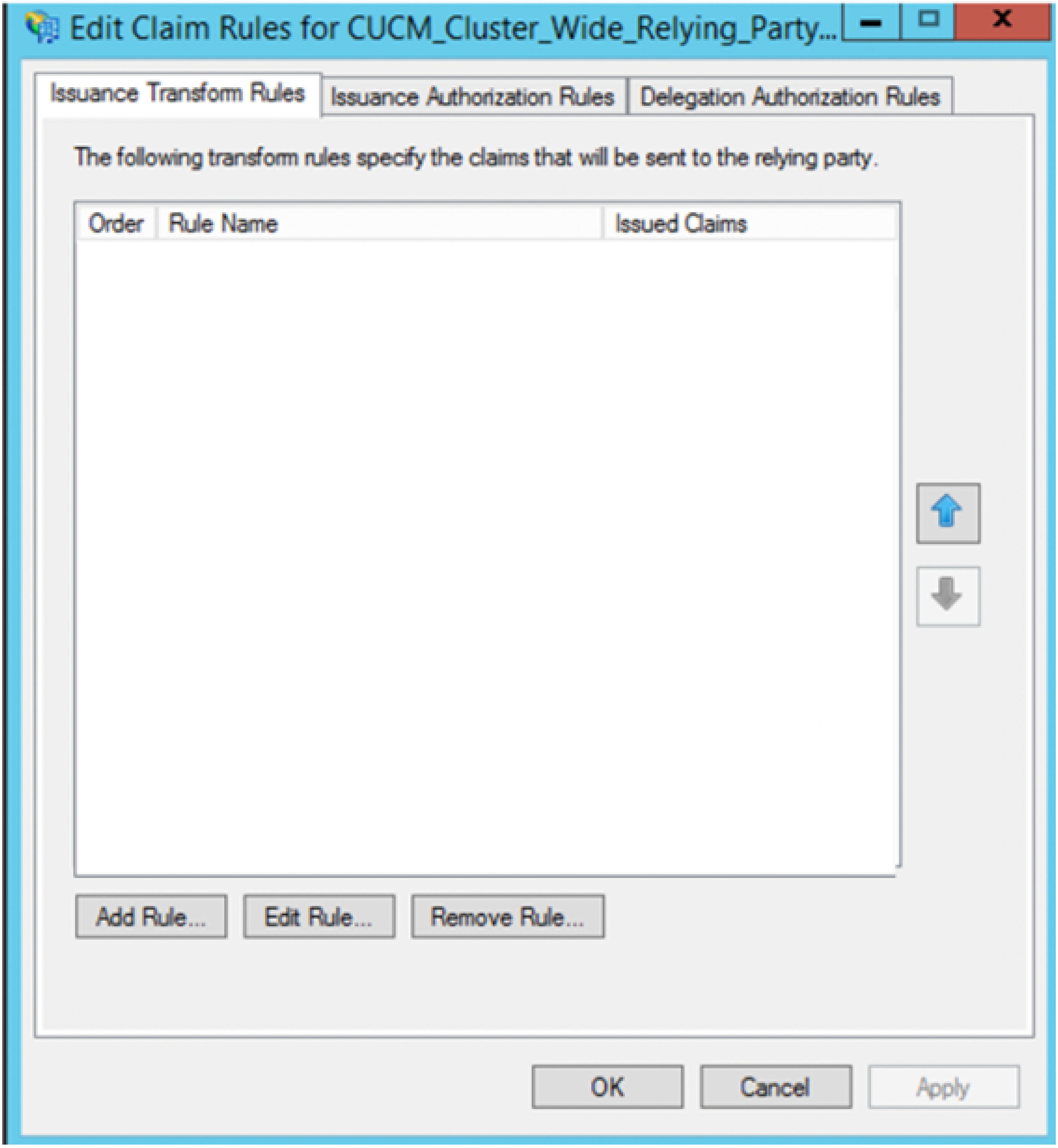
□ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes

使用鼠标辅助按钮选择您刚**创建的信**赖方信任和**编辑领款**申请规则配置，如图所示。



Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-Trust / SAML / WS-Federation	urn:ms-drs:ad.fhlab.com
CUCM_Cluster_Wide_Relying_Party_trust	Yes	WS-Trust / SAML / WS-Federation	cmpubhcsc.fhlab.com
CUC_Cluster_W		L / WS-Federation	cucpubhcsc.fhlab.com
ExpwyC		L / WS-Federation	fhlab.com-500D0F4107D76E57

单击**Add Rule(添**加规则)，如图所示。



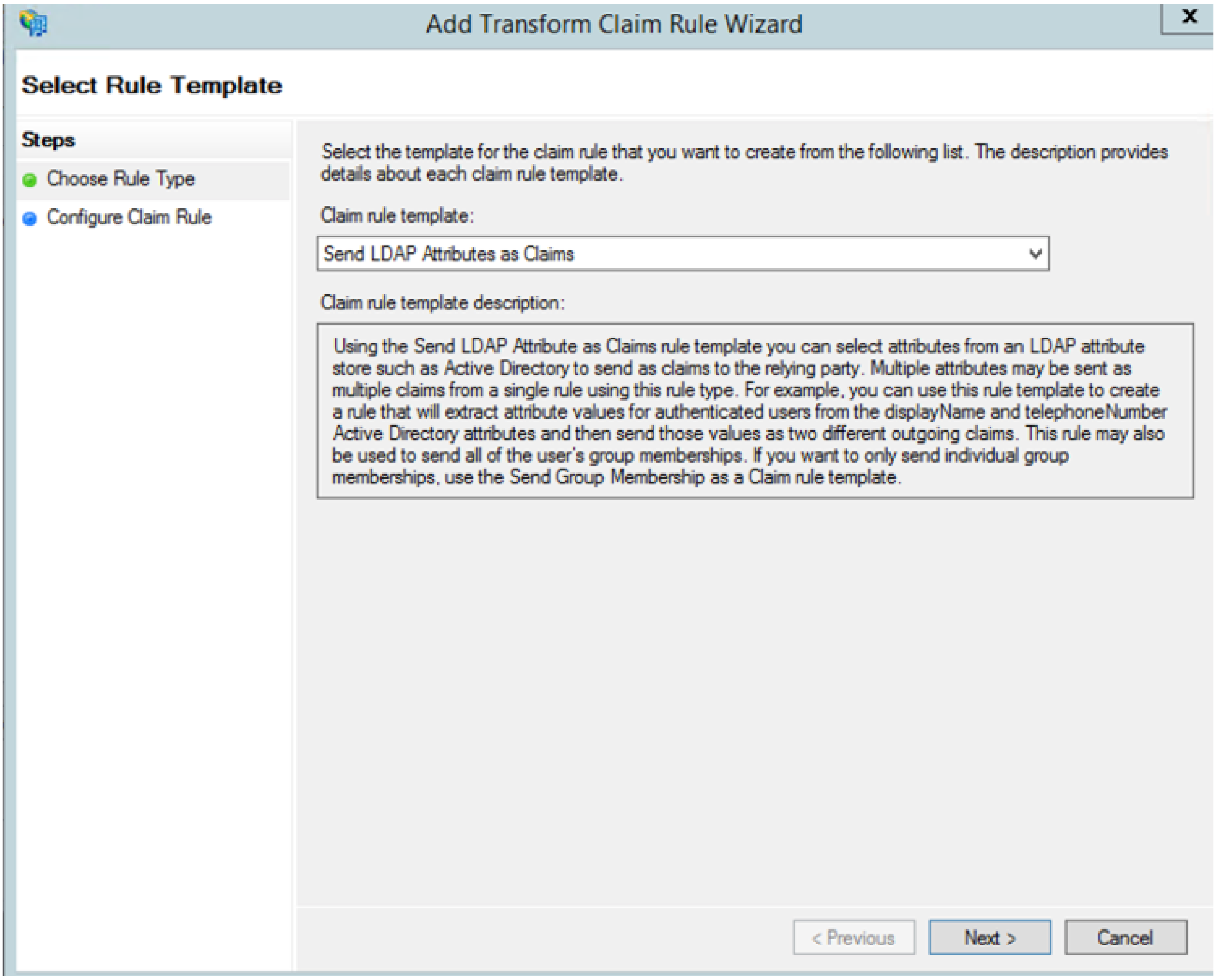
Edit Claim Rules for CUCM_Cluster_Wide_Relying_Party...
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules

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

选择“**将LDAP属性作为声明发送**”，然后**单击“下一步**”。



Select Rule Template

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

配置以下参数：

领款申请规则名称：名称ID

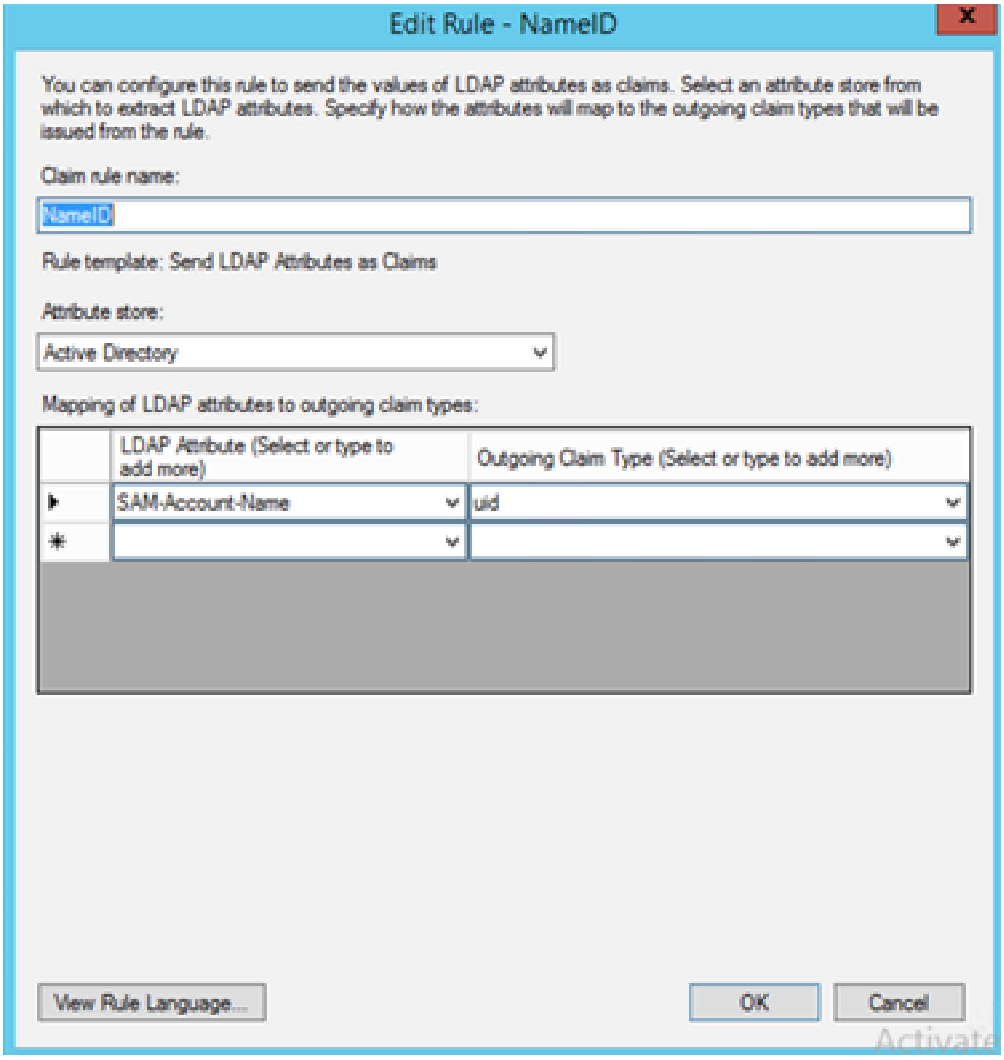
属性存储：Active Directory（双击下拉菜单箭头）

LDAP属性：SAM帐户名称

传出领款申请类型：uid

单击**完成/确**定继续。

请注意，uid不是小写的，并且下拉菜单中不存在。键入。



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

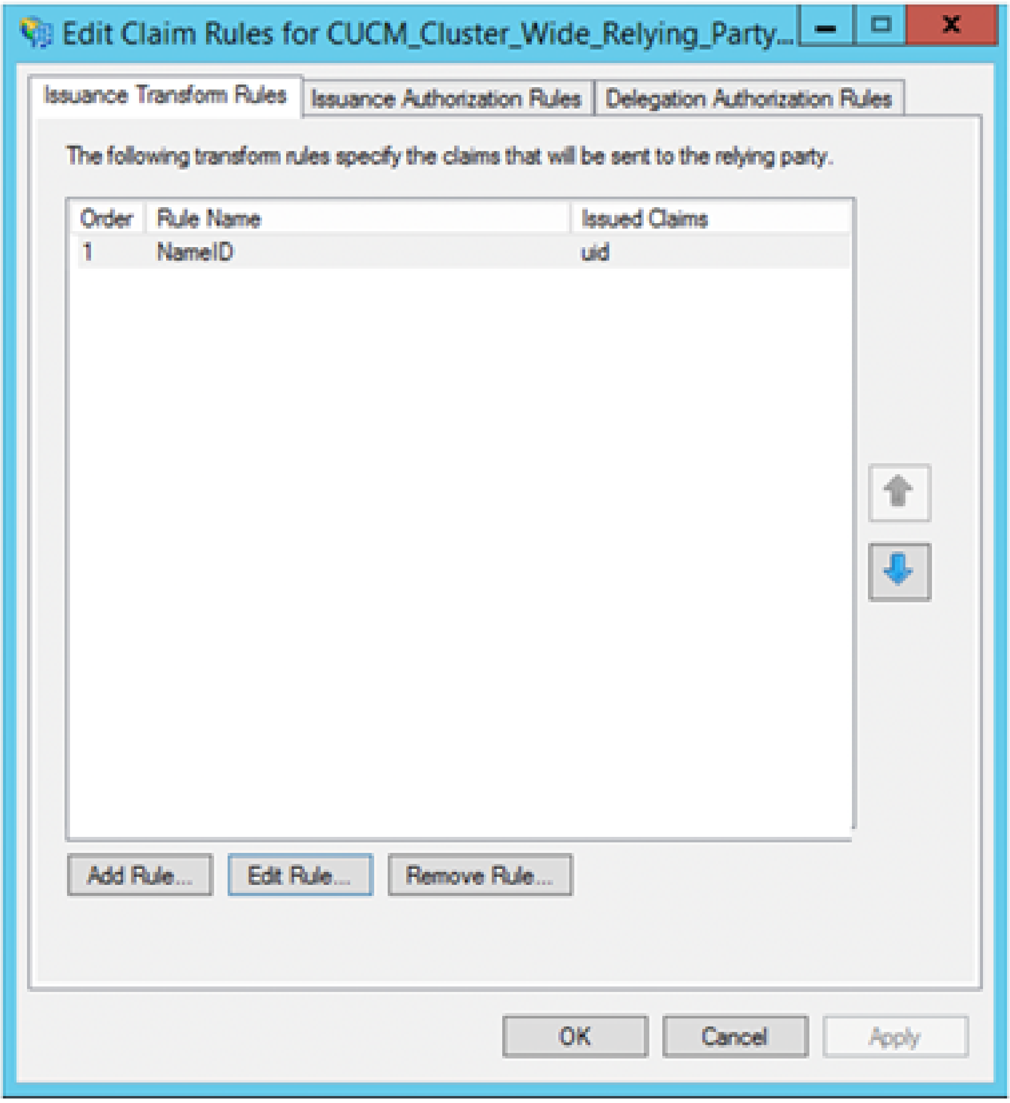
Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

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

再次**单击Add Rule（添加规则）**以添加另一个规则。

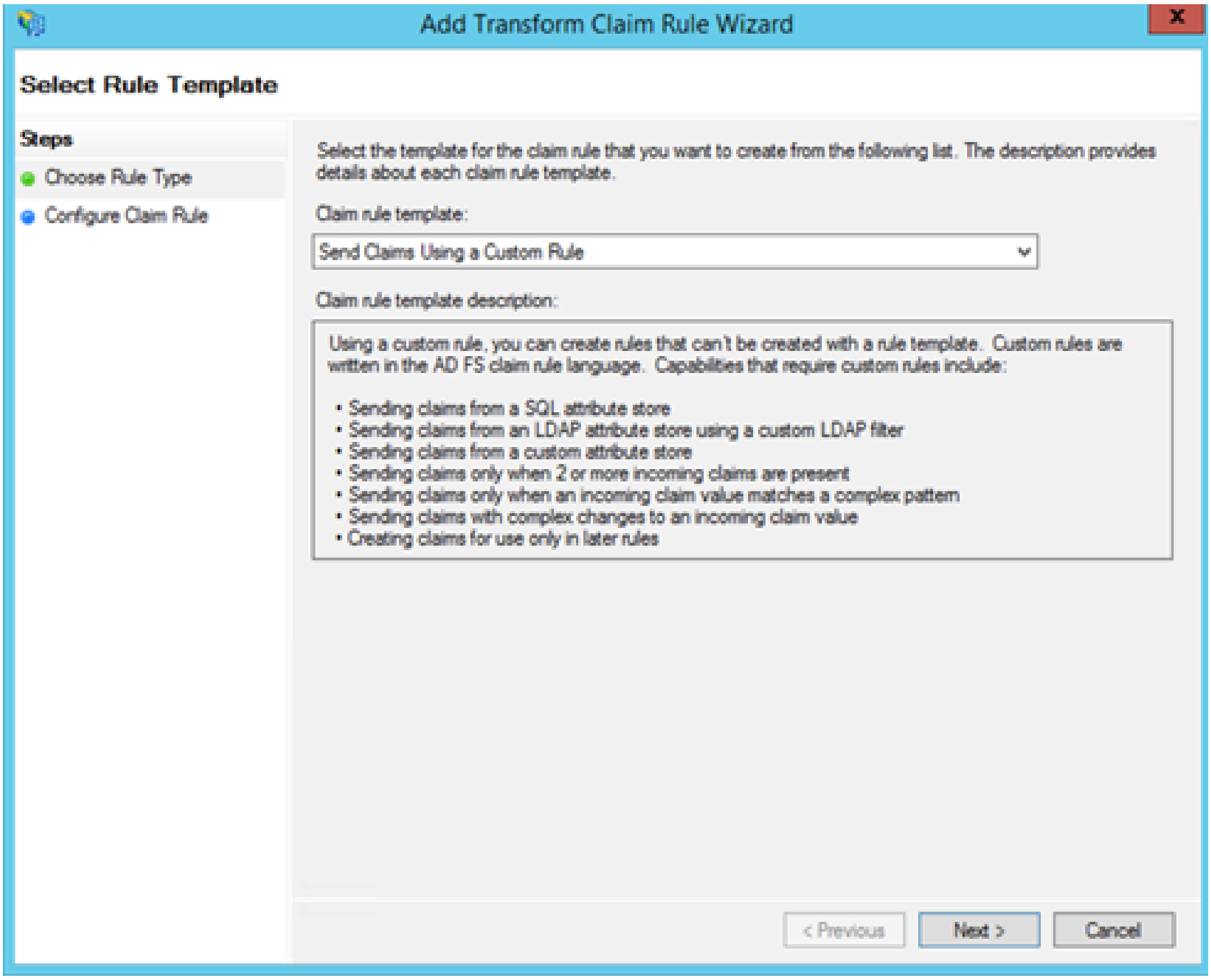


Edit Claim Rules for CUCM_Cluster_Wide_Relying_Party...

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

Order	Rule Name	Issued Claims
1	NameID	uid

选择“**使用自定义规则发送声明”**，然后单**击“下一步**”。



Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send Claims Using a Custom Rule

Claim rule template description:

Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include:

- Sending claims from a SQL attribute store
- Sending claims from an LDAP attribute store using a custom LDAP filter
- Sending claims from a custom attribute store
- Sending claims only when 2 or more incoming claims are present
- Sending claims only when an incoming claim value matches a complex pattern
- Sending claims with complex changes to an incoming claim value
- Creating claims for use only in later rules

创建名为Cluster_Side_Claim_Rule的自定义规则。

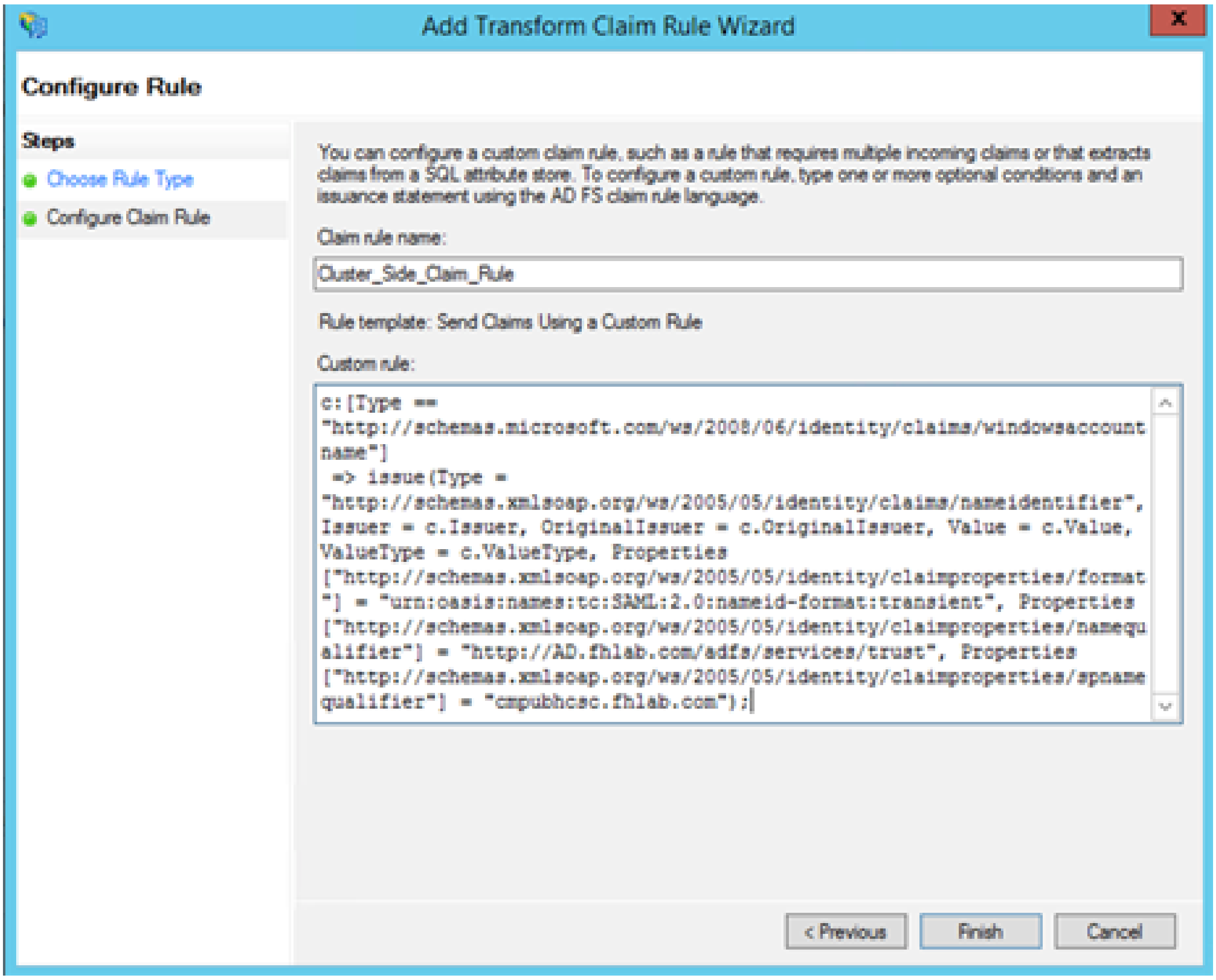
将此文本直接从此处复制并粘贴到规则窗口中。有时，如果在文本编辑器上编辑引号，则会更改引号，这会使规则在测试SSO时失败：

```
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");
```

单击Finish(完成)继续。



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 claim rule language.

Claim rule name:

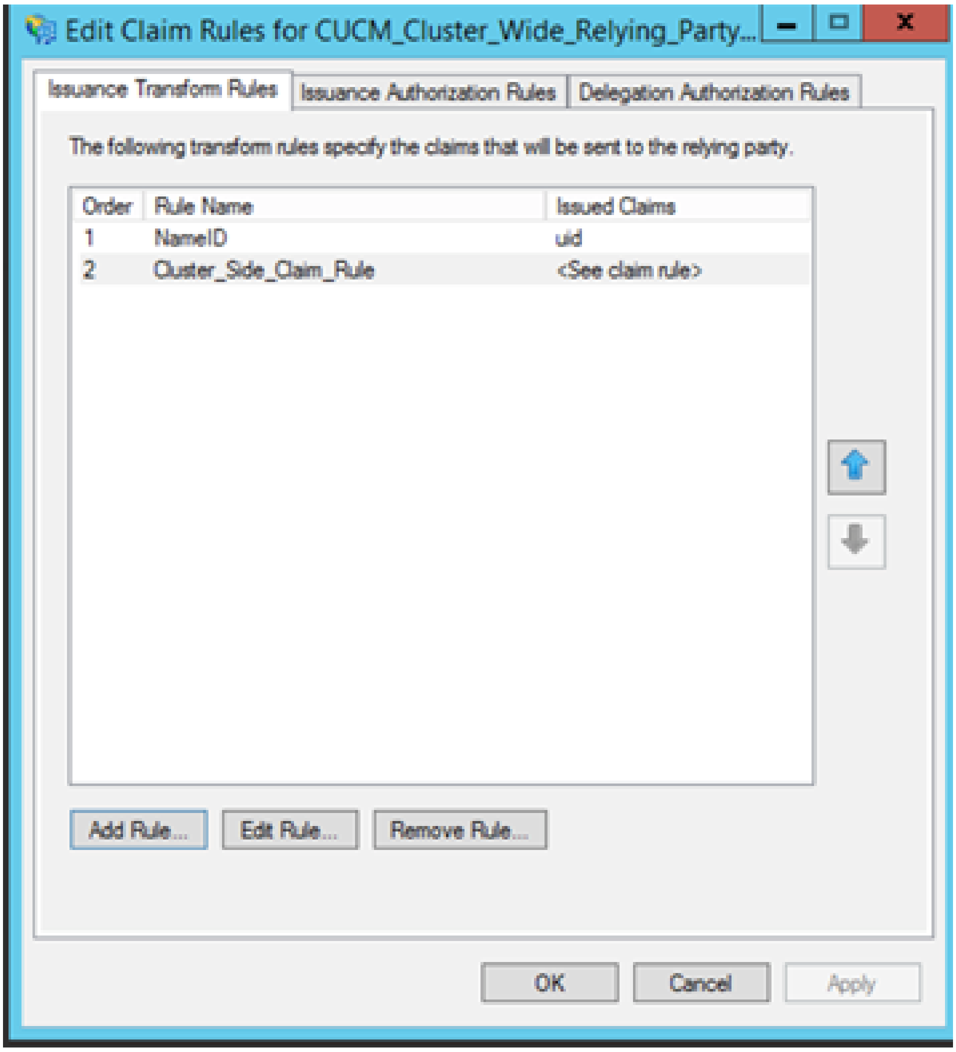
Cluster_Side_Claim_Rule

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount
name"]
 => 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/namequ
alifier"] = "http://AD.fhlab.com/adfs/services/trust", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spname
qualifier"] = "cmpubhcsc.fhlab.com");
```

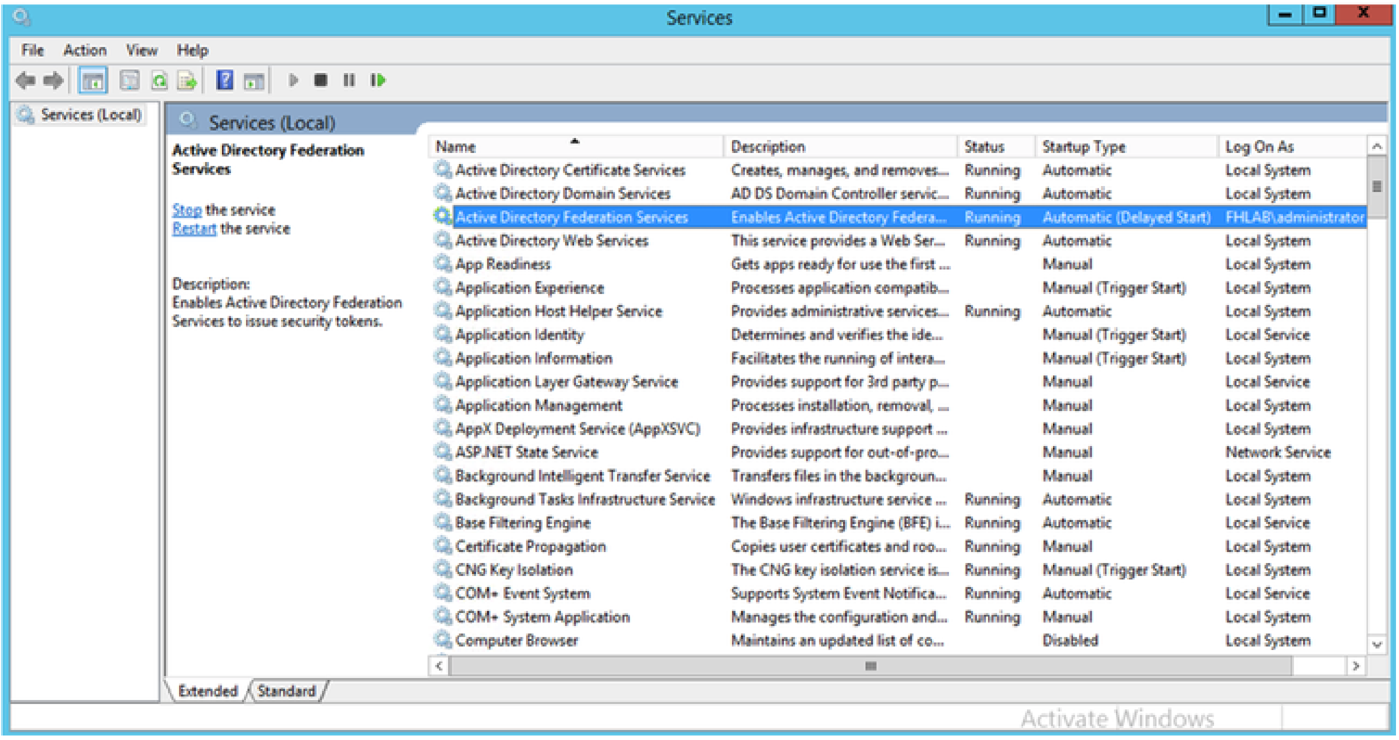
现在，您应在ADFS上定义两个规则。单击**Apply**和**OK**以关闭规则窗口。


Edit Claim Rules for CUCM_Cluster_Wide_Relying_Party...
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

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

Order	Rule Name	Issued Claims
1	NameID	uid
2	Cluster_Side_Claim_Rule	<See claim rule>

CUCM现在已成功添加为ADFS的可信赖方。



Services (Local)

Active Directory Federation Services

Stop the service
Restart the service

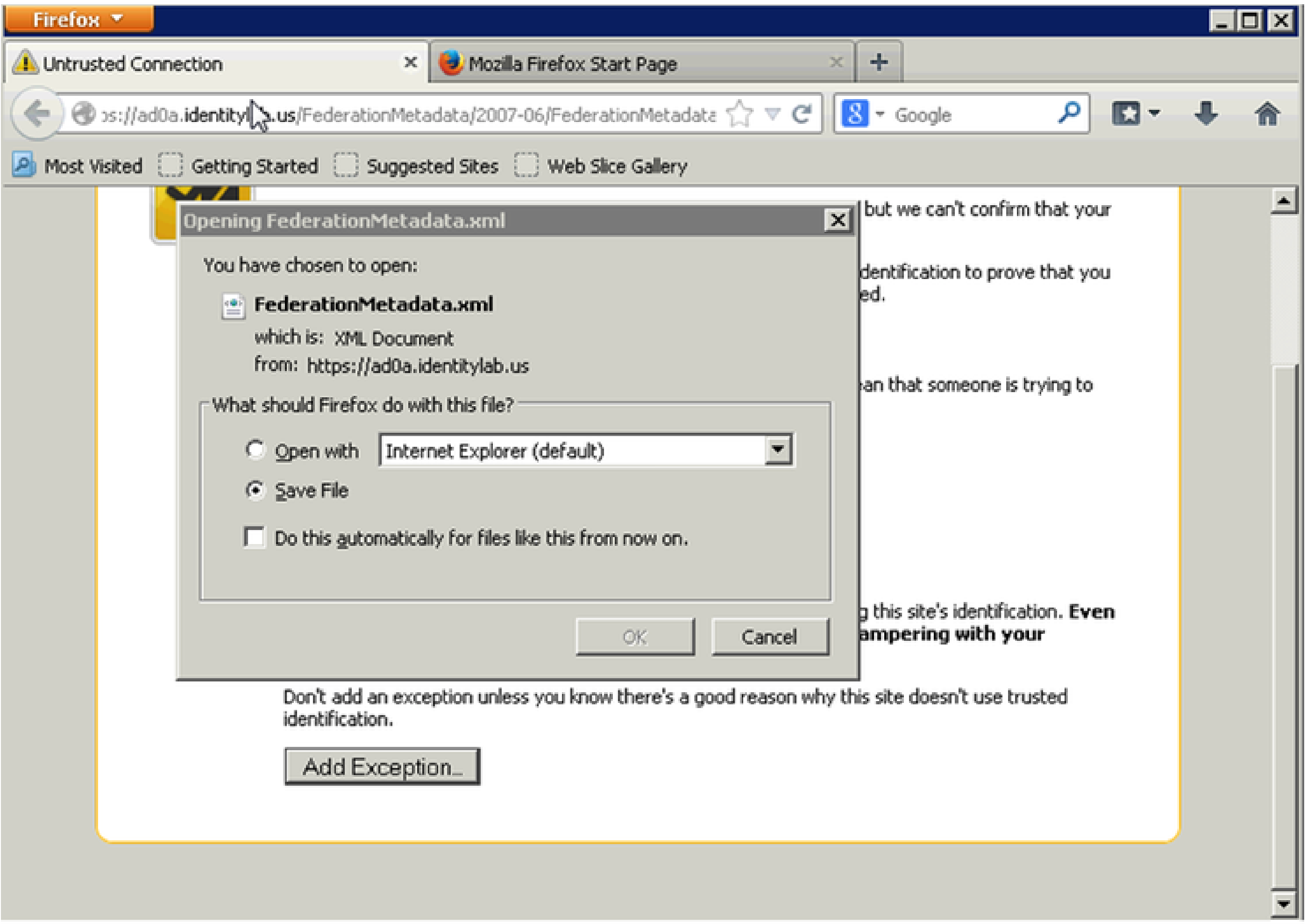
Description:
Enables Active Directory Federation Services to issue security tokens.

Name	Description	Status	Startup Type	Log On As
Active Directory Certificate Services	Creates, manages, and removes...	Running	Automatic	Local System
Active Directory Domain Services	AD DS Domain Controller servic...	Running	Automatic	Local System
Active Directory Federation Services	Enables Active Directory Federa...	Running	Automatic (Delayed Start)	FHLAB\administrator
Active Directory Web Services	This service provides a Web Ser...	Running	Automatic	Local System
App Readiness	Gets apps ready for use the first ...		Manual	Local System
Application Experience	Processes application compatib...		Manual (Trigger Start)	Local System
Application Host Helper Service	Provides administrative services...	Running	Automatic	Local System
Application Identity	Determines and verifies the ide...		Manual (Trigger Start)	Local Service
Application Information	Facilitates the running of intera...		Manual (Trigger Start)	Local System
Application Layer Gateway Service	Provides support for 3rd party p...		Manual	Local Service
Application Management	Processes installation, removal, ...		Manual	Local System
AppX Deployment Service (AppXSVC)	Provides infrastructure support ...		Manual	Local System
ASP.NET State Service	Provides support for out-of-pro...		Manual	Network Service
Background Intelligent Transfer Service	Transfers files in the backgroun...		Manual	Local System
Background Tasks Infrastructure Service	Windows infrastructure service ...	Running	Automatic	Local System
Base Filtering Engine	The Base Filtering Engine (BFE) i...	Running	Automatic	Local Service
Certificate Propagation	Copies user certificates and roo...	Running	Manual	Local System
CNG Key Isolation	The CNG key isolation service is...	Running	Manual (Trigger Start)	Local System
COM+ Event System	Supports System Event Notifica...	Running	Automatic	Local Service
COM+ System Application	Manages the configuration and...	Running	Manual	Local System
Computer Browser	Maintains an updated list of co...		Disabled	Local System

在继续之前，请重新启动ADFS服务。导航至“开**始”菜单>“管理工具”>“服务**”。

IDP元数据

您需要向CUCM提供有关我们IdP的信息。此信息使用XML元数据交换。确保在安装了ADFS的服务器上执行此步骤。


Firefox
Untrusted Connection
Mozilla Firefox Start Page
ps://ad0a.identitylab.us/FederationMetadata/2007-06/FederationMetadata
Google
Most Visited
Getting Started
Suggested Sites
Web Slice Gallery

Opening FederationMetadata.xml

You have chosen to open:

FederationMetadata.xml

which is: XML Document

from: https://ad0a.identitylab.us

What should Firefox do with this file?

○ Open with Internet Explorer (default)

● Save File

□ Do this automatically for files like this from now on.

OK Cancel

but we can't confirm that your

dentification to prove that you ed.

an that someone is trying to

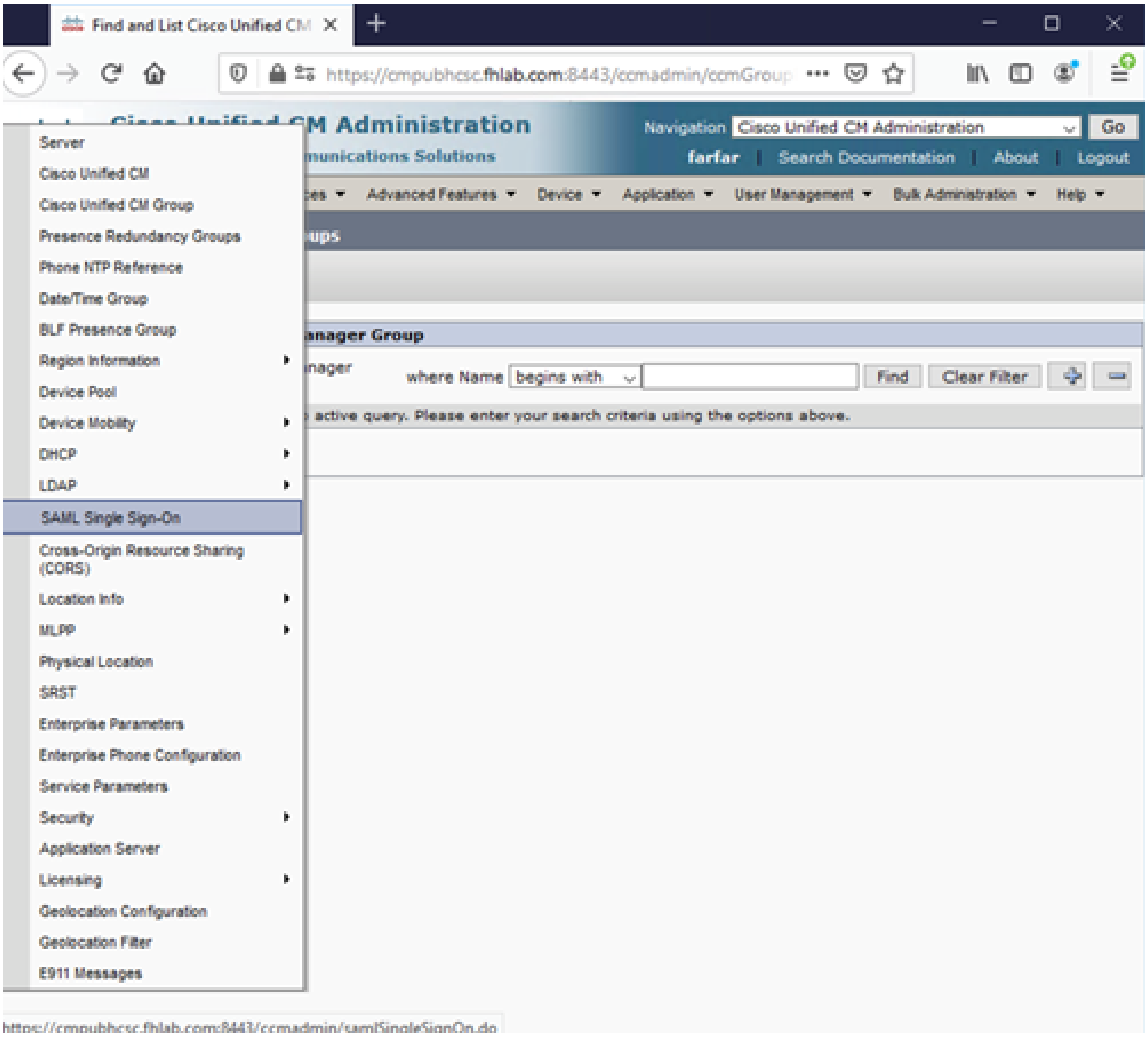
g this site's identification. **Even ampering with your**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Add Exception...

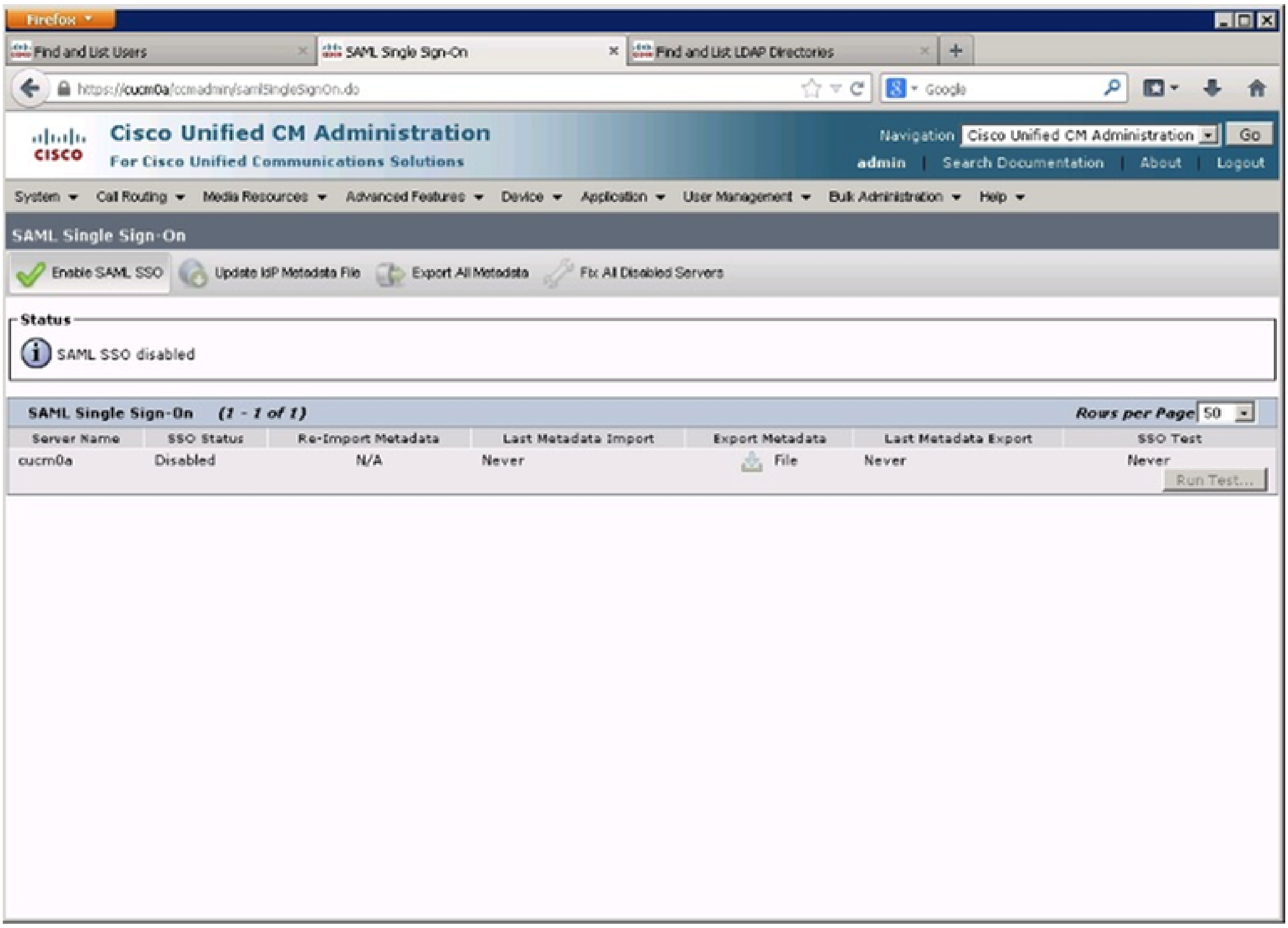
首先，您需要使用Firefox浏览器连接到ADFS(IdP)以下载XML元数据。打开浏览器到https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml并将元数据保存到本地文件夹。

现在，导航至CUCM配置到系统菜**单> SAML单点登录菜单**。



active query. Please enter your search criteria using the options above.

反向到CUCM Administration并选择**SYSTEM > SAML Single Sign-On**。


Firefox
Find and List Users
SAML Single Sign-On
Find and List LDAP Directories
https://cucm0a/ccmadmin/samlSingleSignOn.do
Google
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Enable SAML SSO
Update IdP Metadata File
Export All Metadata
Fix All Disabled Servers
Run Test...

SAML Single Sign-On

Status

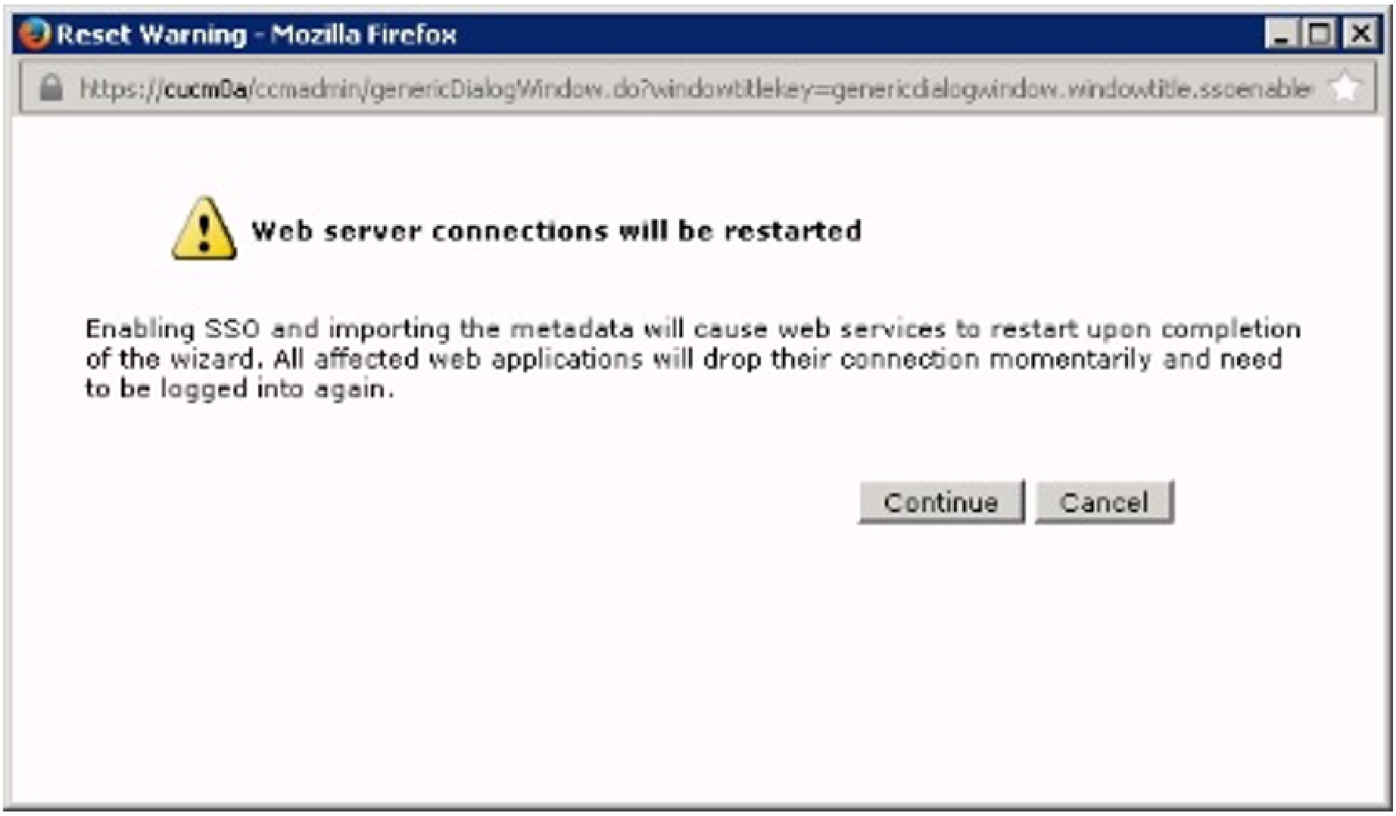
SAML SSO disabled

SAML Single Sign-On (1 - 1 of 1) Rows per Page 50

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
cucm0a	Disabled	N/A	Never	File	Never	Never

选择Enable SAML SSO。

单击Continue以确认警告。

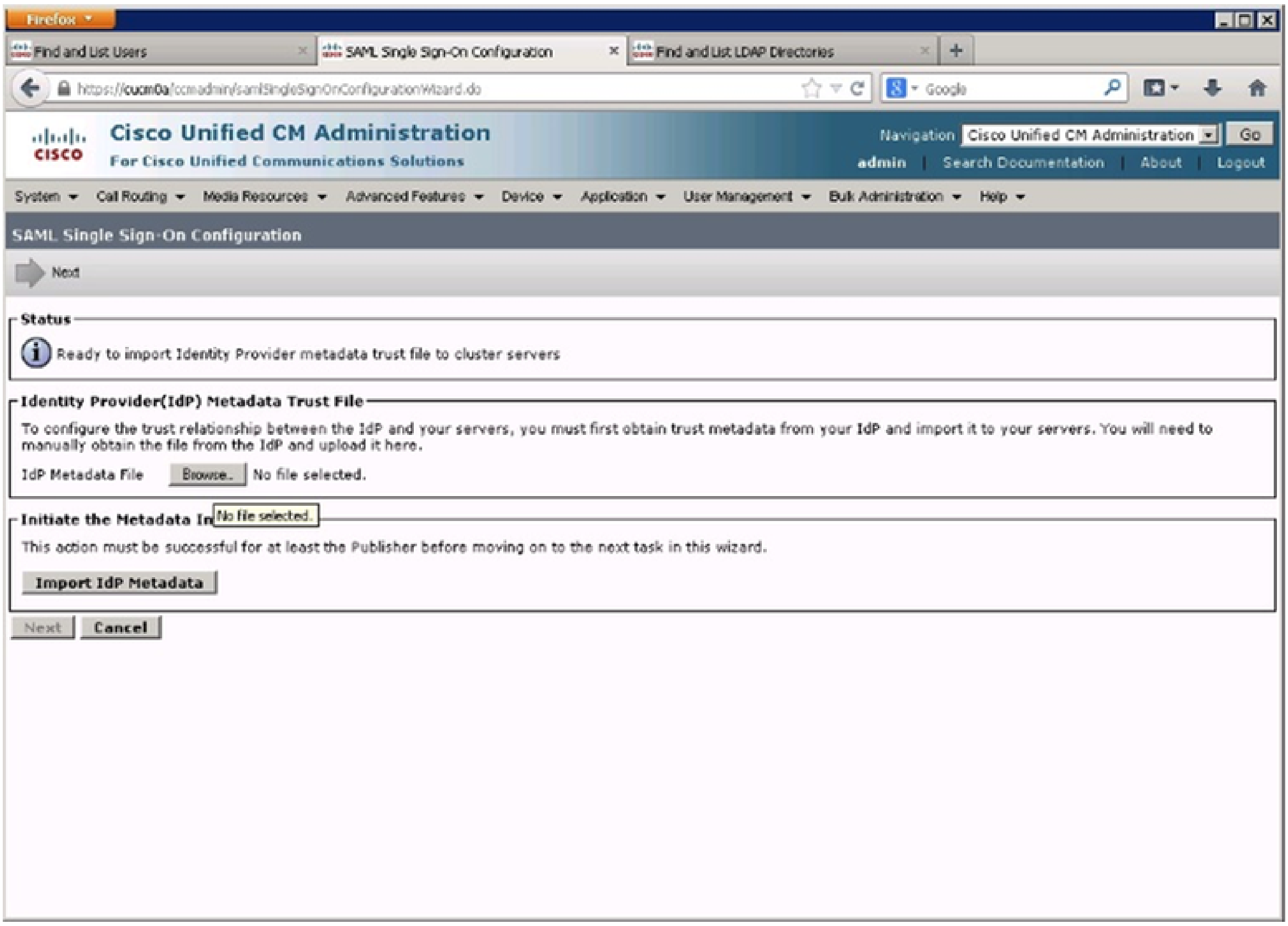

Reset Warning - Mozilla Firefox
https://cucm0a/ccmadmin/genericDialogWindow.do?windowtitlekey=genericdialogwindow.windowtitle.ssoenable
Continue
Cancel

Web server connections will be restarted

Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again.

在SSO屏幕上，单击“浏**览……**”以导入之前保存的FederationMetadata.xml元数据XML文件，如图

所示。


Firefox
Find and List Users
SAML Single Sign-On Configuration
Find and List LDAP Directories
https://cucm0a/ccmadmin/samlSingleSignOnConfigurationWizard.do
Google
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
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

Ready to import Identity Provider metadata trust file to cluster 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... No file selected.

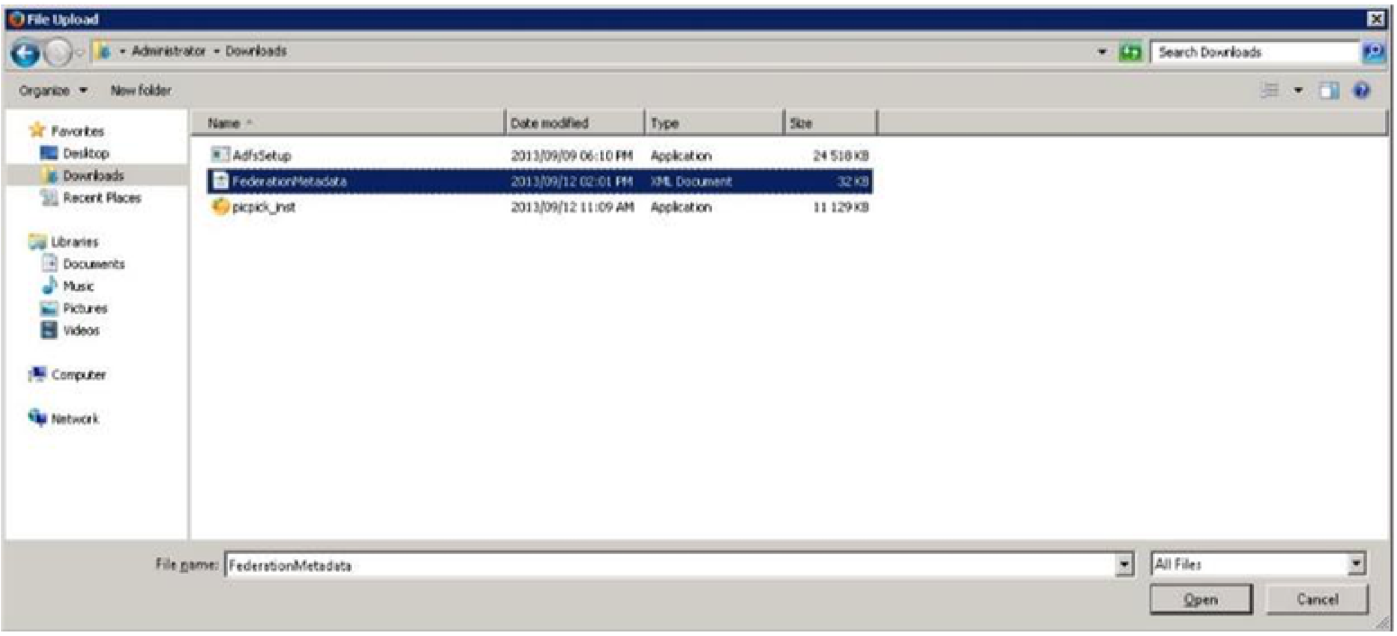
Initiate the Metadata In[No file selected.]

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

Import IdP Metadata

Next Cancel

选择XML文件，然后单击**打开**，以便从“收藏夹”下的“下载”中将其上传到CUCM。



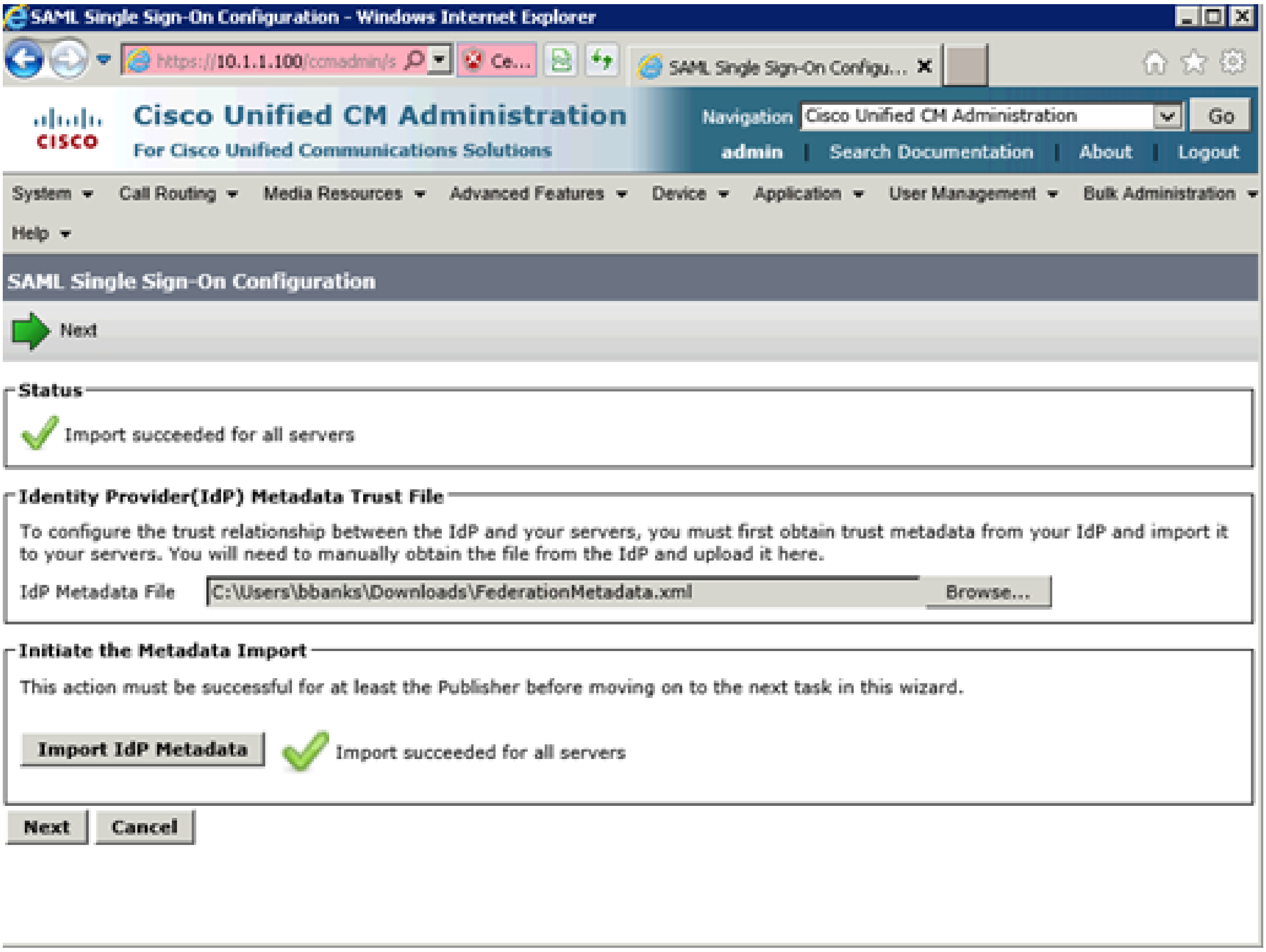
Name	Date modified	Type	Size
AdfsSetup	2013/09/09 06:10 PM	Application	24 518 KB
FederationMetadata	2013/09/12 02:01 PM	XML Document	32 KB
picpick_inst	2013/09/12 11:09 AM	Application	11 129 KB

File name: FederationMetadata

All Files

Open Cancel

上传后，点击Import IdP Metadata（导入IdP元数据），将IdP信息导入CUCM。确认导入成功，然后单击“下一步”继续。


SAML Single Sign-On Configuration - Windows Internet Explorer
https://10.1.1.100/ccmadmin/s
SAML Single Sign-On Configu...
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation
Cisco Unified CM Administration
Go
admin
Search Documentation
About
Logout
System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Bulk Administration
Help
Next

SAML Single Sign-On Configuration

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: C:\Users\bbanks\Downloads\FederationMetadata.xml Browse...

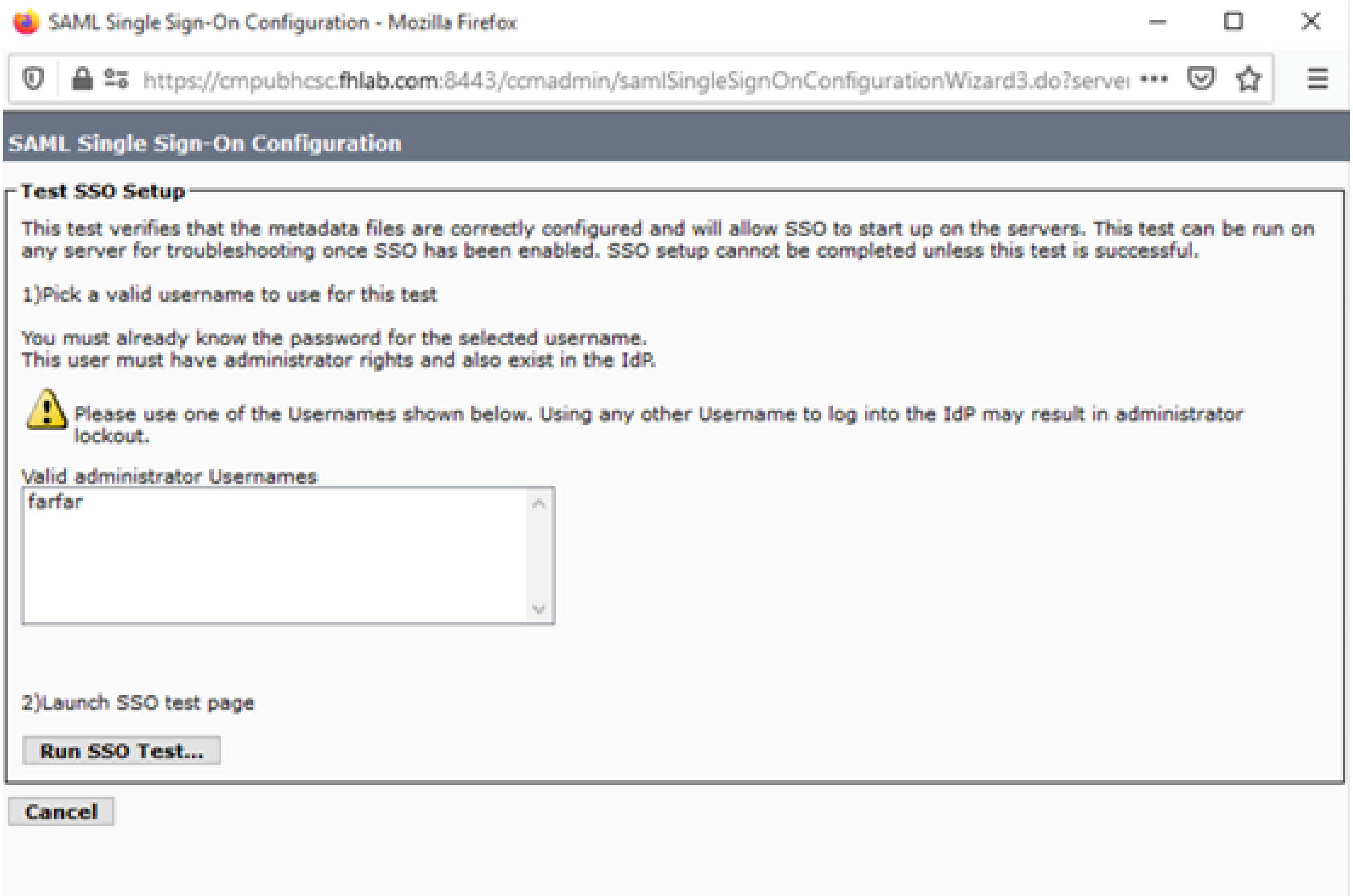
Initiate the Metadata Import

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

Import IdP Metadata ✓ Import succeeded for all servers

Next Cancel

选择属于标准CCM超级用户的用户，然后点击RUN SSO TEST。


SAML Single Sign-On Configuration - Mozilla Firefox
https://cmpubhcsc.fhlab.com:8443/ccmadmin/samlSingleSignOnConfigurationWizard3.do?server

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

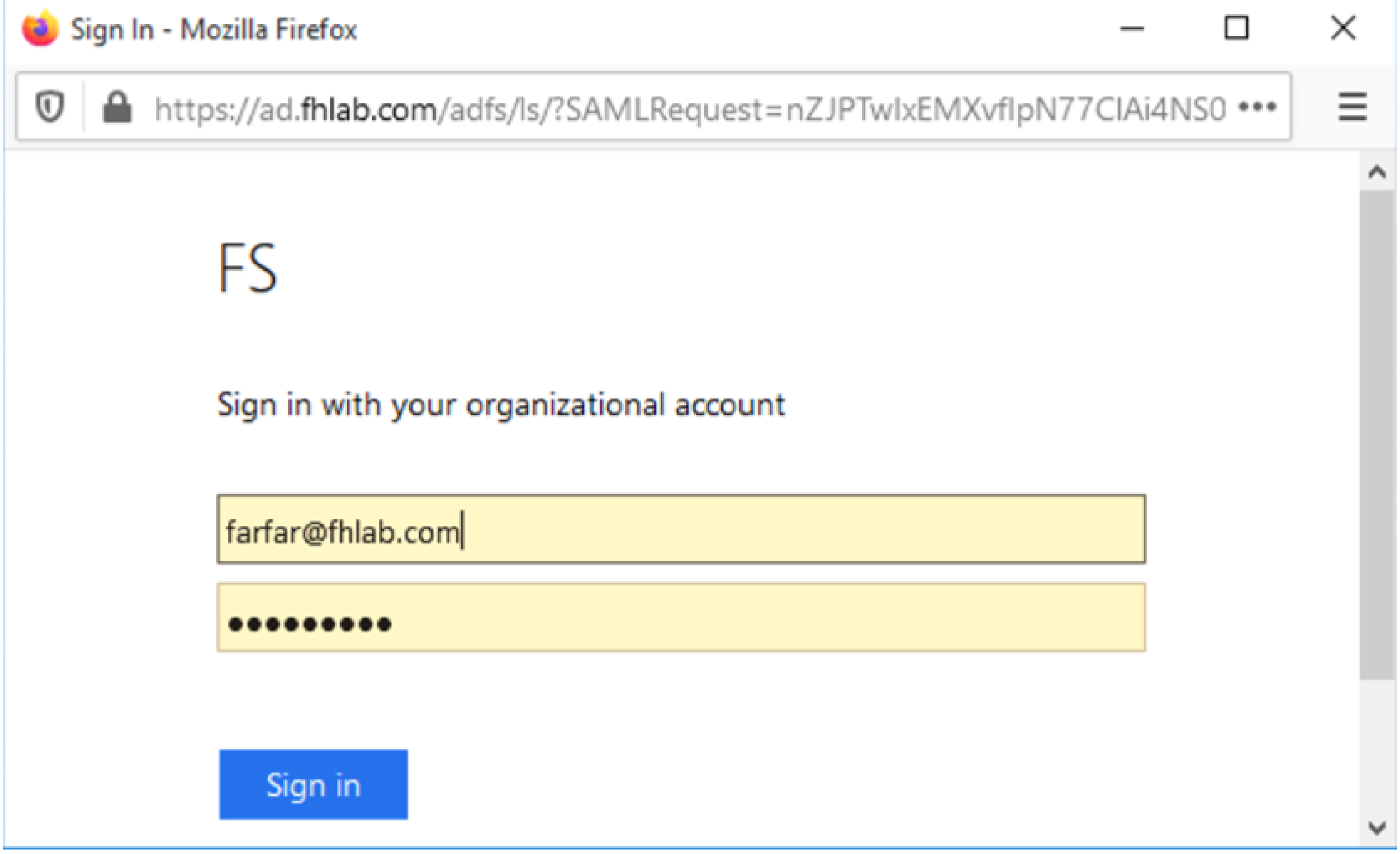
farfar

2)Launch SSO test page

Run SSO Test...

Cancel

当显示用户身份验证对话框时，使用适当的用户名和密码登录。


Sign In - Mozilla Firefox

https://ad.fhlab.com/adfs/ls/?SAMLRequest=nZJPTwlxEMXvflpN77ClAi4NS0

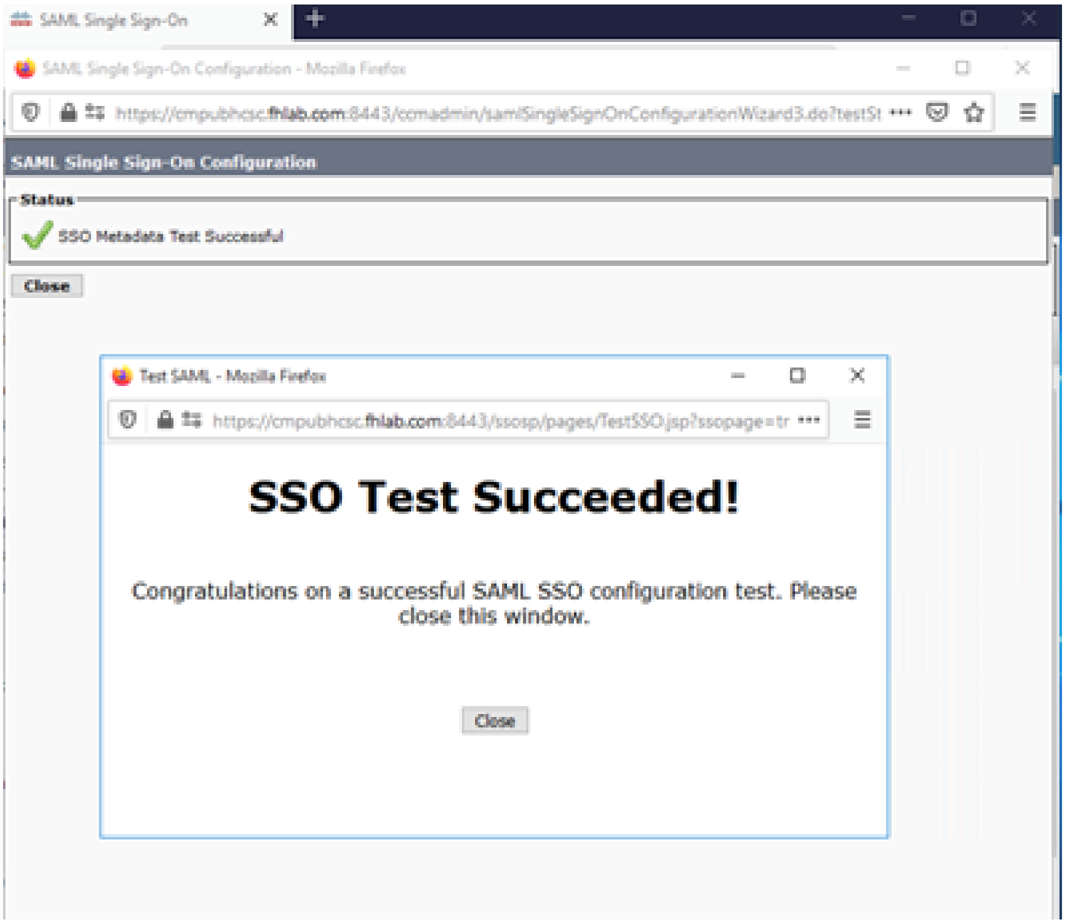
FS

Sign in with your organizational account

farfar@fhlab.com

••••••••••

如果所有配置都正确，您应看到一条消息，说SSO测试成功！


SAML Single Sign-On

SAML Single Sign-On Configuration - Mozilla Firefox

https://cmpubhcsc.fhlab.com:8443/ccmadmin/samlSingleSignOnConfigurationWizard3.do?testS!

SAML Single Sign-On Configuration

Status

✓ SSO Metadata Test Successful

Test SAML - Mozilla Firefox

https://cmpubhcsc.fhlab.com:8443/ssosp/pages/TestSSO.jsp?ssopage=tr

SSO Test Succeeded!

Congratulations on a successful SAML SSO configuration test. Please close this window.

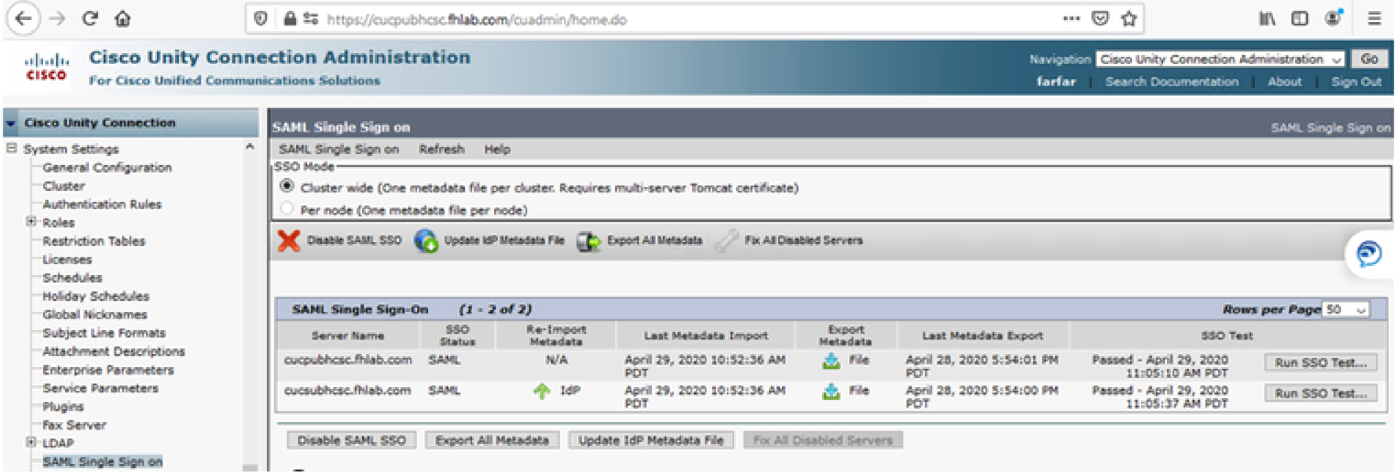
单击“关闭”和“完成”继续。

现在，我们已成功完成基本配置任务，以使用ADFS在CUCM上启用SSO。

在CUC上配置SSO

在Unity Connection中启用SSO时，可遵循相同的流程。

LDAP与CUC集成。



SAML Single Sign on

SSO Mode

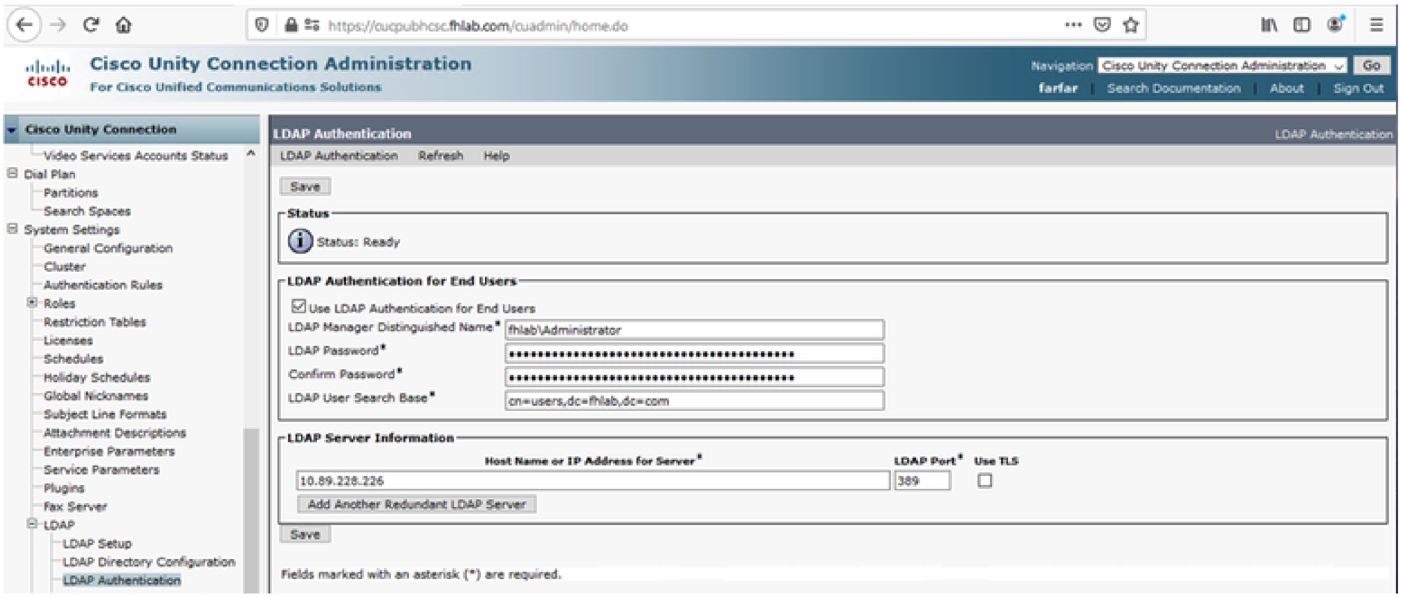
● Cluster wide (One metadata file per cluster. Requires multi-server Tomcat certificate)

○ Per node (One metadata file per node)

SAML Single Sign-On (1 - 2 of 2) Rows per Page 50

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test	
cucpubhcsc.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...
cucsubhcsc.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...

配置 LDAP 验证.



LDAP Authentication

Status

Status: Ready

LDAP Authentication for End Users

☑ Use LDAP Authentication for End Users

LDAP Manager Distinguished Name* fhlab\Administrator

LDAP Password* ••

Confirm Password* ••

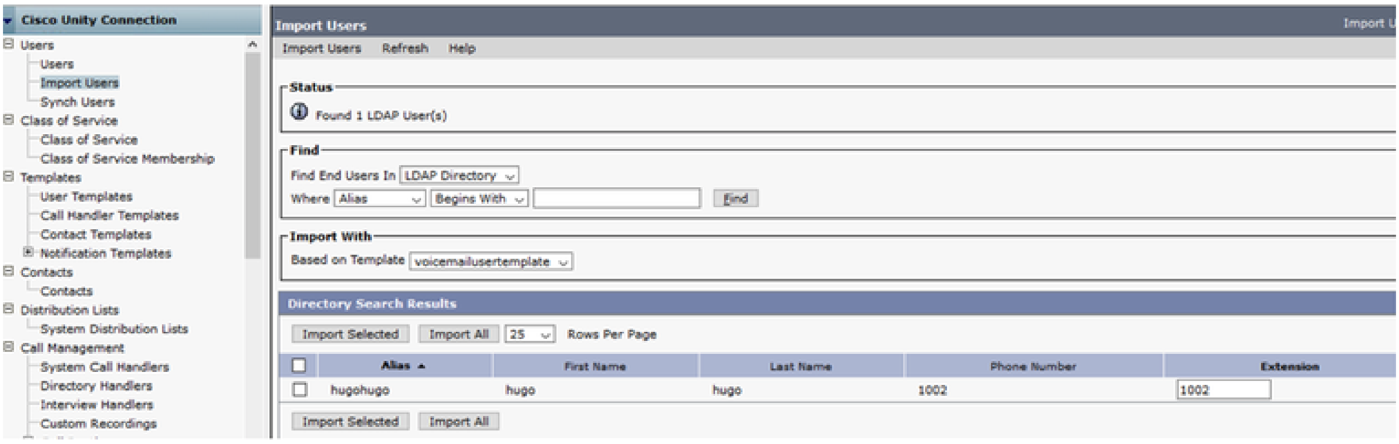
LDAP User Search Base* cn=users,dc=fhlab,dc=com

LDAP Server Information

Host Name or IP Address for Server*	LDAP Port*	Use TLS
10.89.228.226	389	□

Fields marked with an asterisk (*) are required.

从分配了语音邮件的LDAP导入用户，以及将用于测试SSO的用户。



Found 1 LDAP User(s)

Find End Users In: LDAP Directory

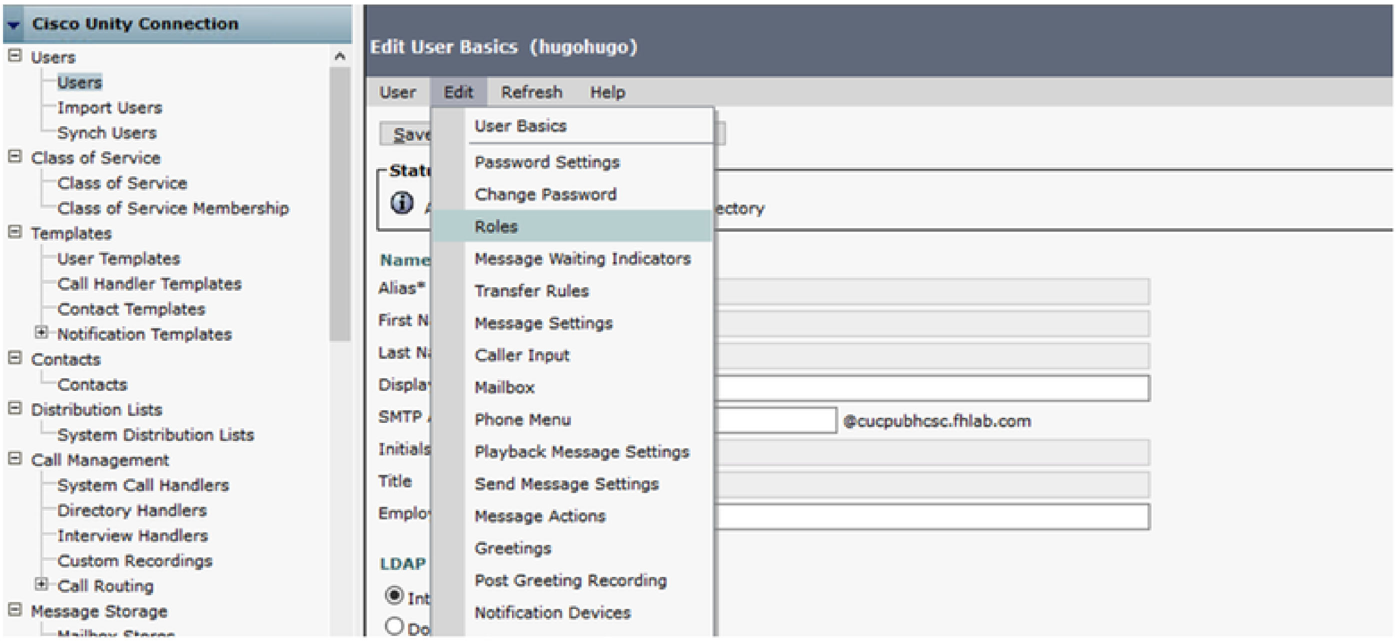
Where: Alias, Begins With

Based on Template: voicemailusertemplate

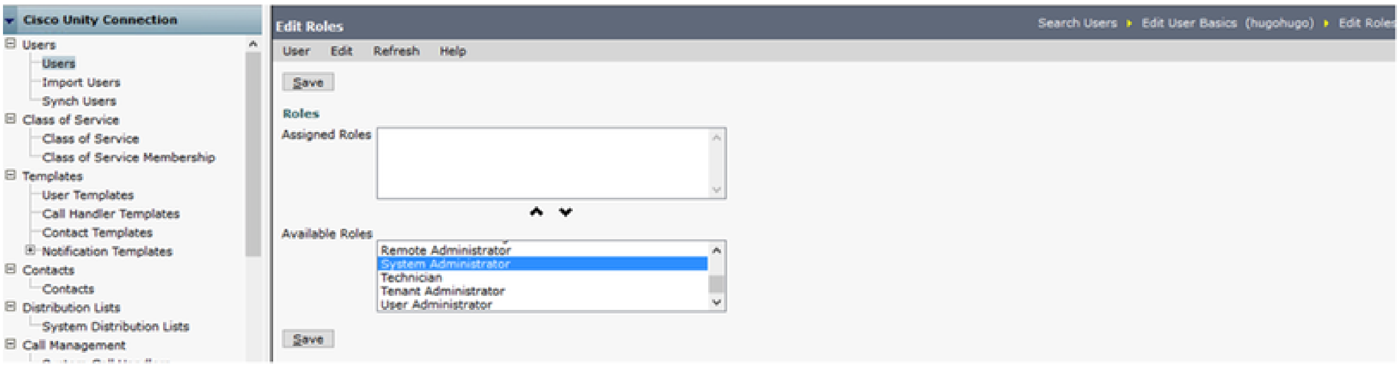
Rows Per Page: 25

☐	Alias ▲	First Name	Last Name	Phone Number	Extension
☐	hugohugo	hugo	hugo	1002	1002

导航到**用户>编辑>角**色，如图所示。

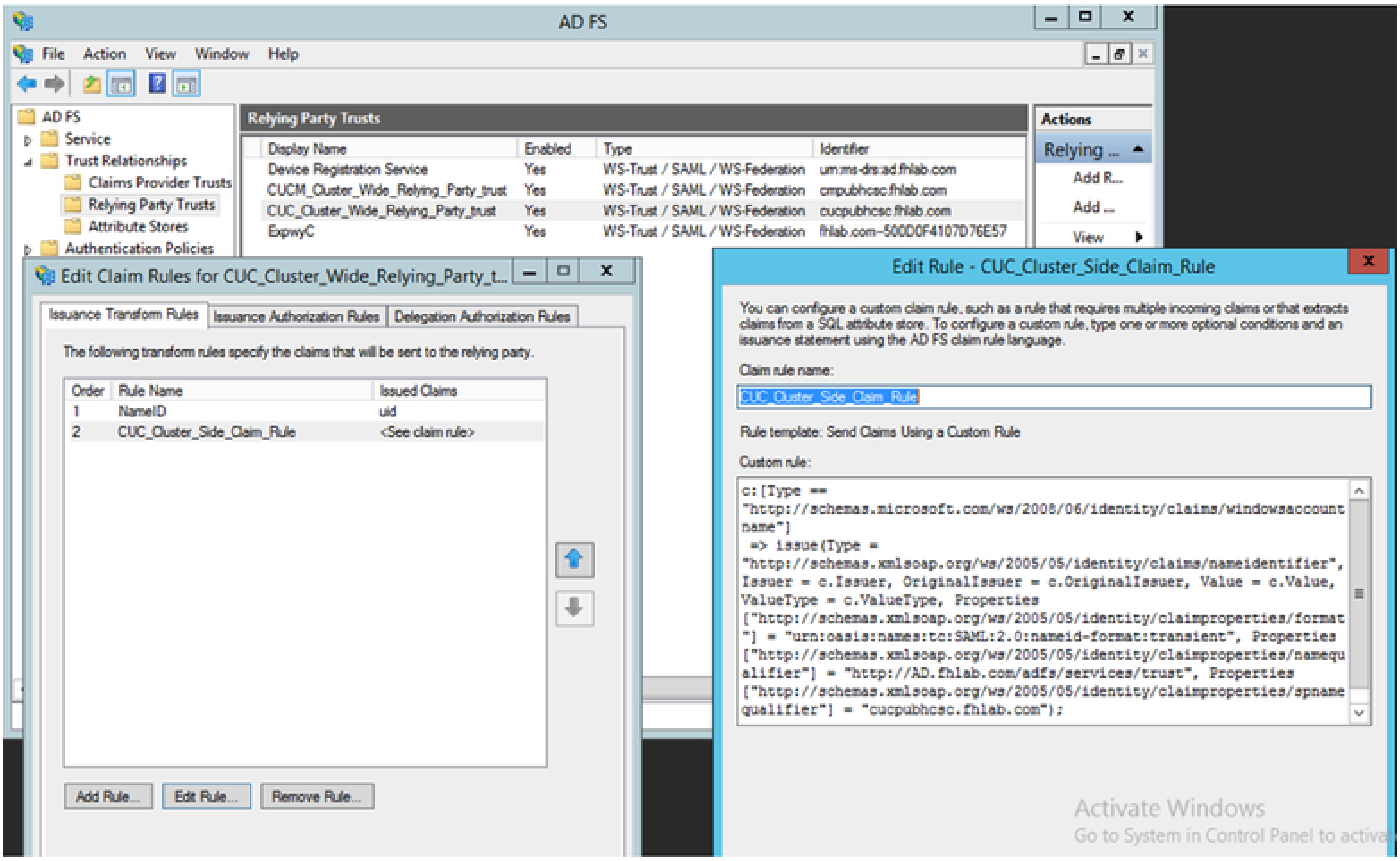


为测试用户分配系统管理员的角色。



CUC元数据

现在，您应该已经下载了CUC元数据，为CUC创建了RelingPartyTrust，并上传了CUC元数据，并在ADFS 3.0上创建了规则I AD FS



Relying Party Trusts

Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-Trust / SAML / WS-Federation	urn:ms-drs:ad.fhlab.com
CUCM_Cluster_Wide_Relying_Party_trust	Yes	WS-Trust / SAML / WS-Federation	cmpubhcsc.fhlab.com
CUC_Cluster_Wide_Relying_Party_trust	Yes	WS-Trust / SAML / WS-Federation	cucpubhcsc.fhlab.com
ExpwyC	Yes	WS-Trust / SAML / WS-Federation	fhlab.com-500D0F4107D76E57

Edit Claim Rules for CUC_Cluster_Wide_Relying_Party_t...

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

Order	Rule Name	Issued Claims
1	NameID	uid
2	CUC_Cluster_Side_Claim_Rule	<See claim rule>

Edit Rule - CUC_Cluster_Side_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 claim rule language.

Claim rule name:

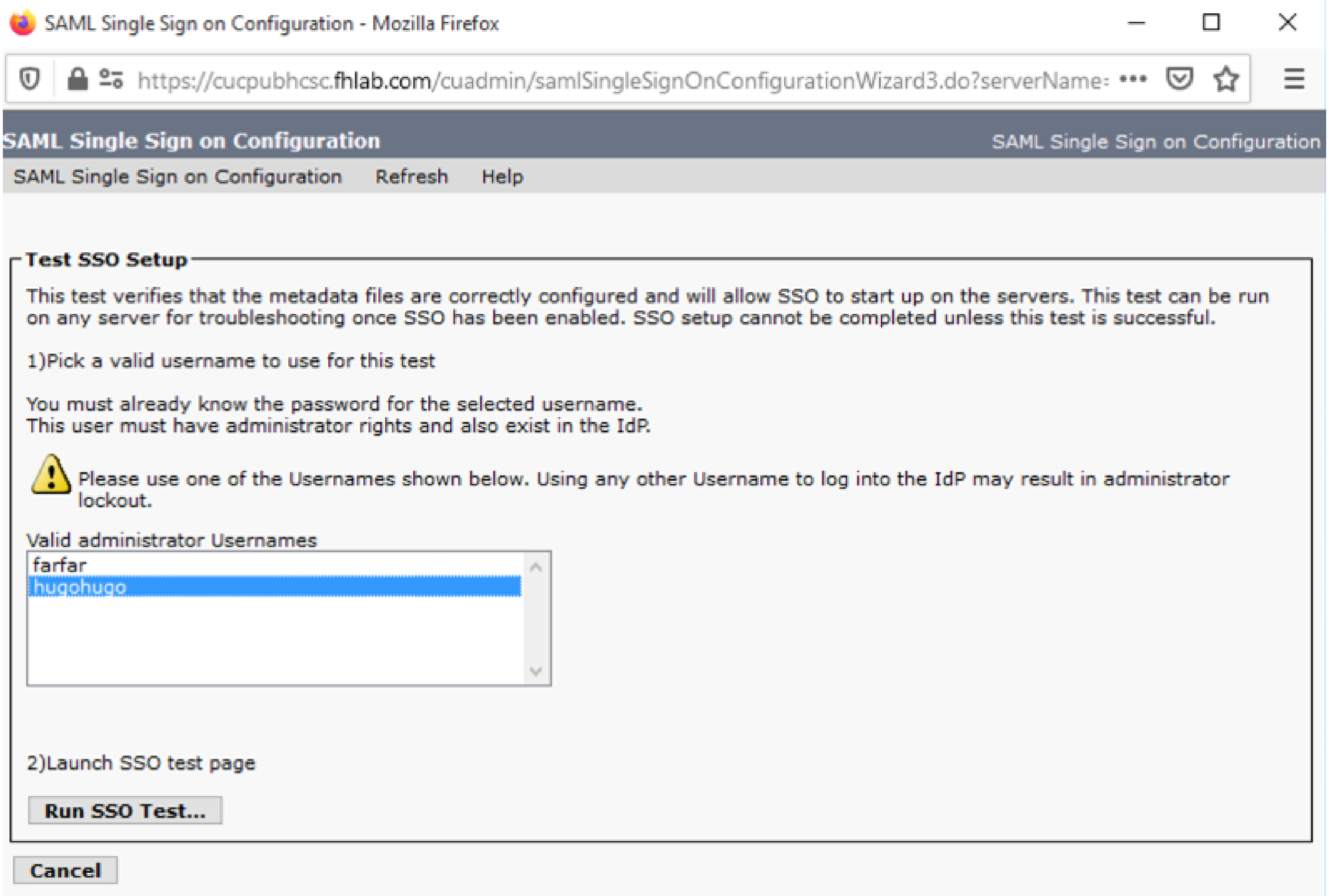
CUC_Cluster_Side_Claim_Rule

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount
name"]
 => 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/namequ
alifier"] = "http://AD.fhlab.com/adfs/services/trust", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spname
qualifier"] = "cucpubhcsc.fhlab.com");
```

转到SAML单点登录并启用SAML SSO。



SAML Single Sign on Configuration - Mozilla Firefox
https://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?serverName=
SAML Single Sign on Configuration
SAML Single Sign on Configuration
SAML Single Sign on Configuration Refresh Help

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

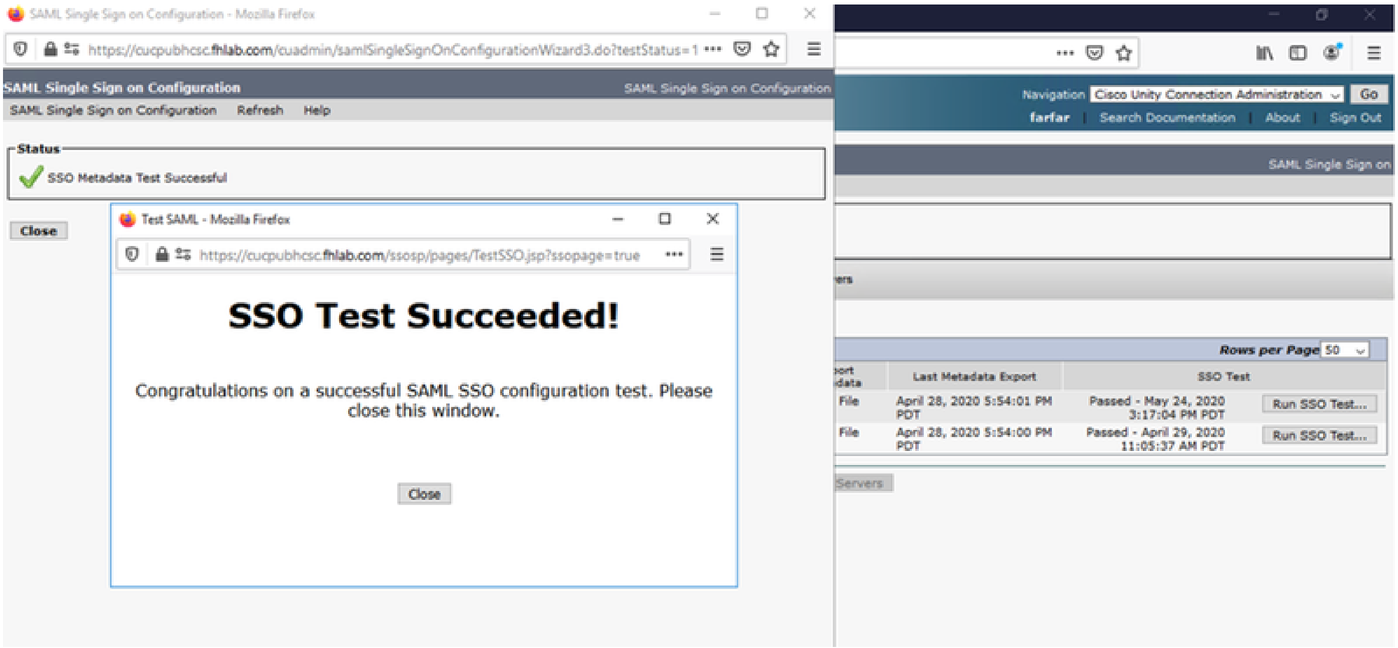
You must already know the password for the selected username.
This user must have administrator rights and also exist in the IdP.

⚠ 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

farfar
hugohugo

2)Launch SSO test page


SAML Single Sign on Configuration - Mozilla Firefox
https://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?testStatus=1
SAML Single Sign on Configuration
SAML Single Sign on Configuration
Refresh
Help
Close
Test SAML - Mozilla Firefox
https://cucpubhcsc.fhlab.com/ssosp/pages/TestSSO.jsp?ssopage=true
Close
Navigation
Cisco Unity Connection Administration
Go
farfar
Search Documentation
About
Sign Out
SAML Single Sign on
Servers

Status

SSO Metadata Test Successful

SSO Test Succeeded!

Congratulations on a successful SAML SSO configuration test. Please close this window.

Rows per Page 50

ort data	Last Metadata Export	SSO Test	
File	April 28, 2020 5:54:01 PM PDT	Passed - May 24, 2020 3:17:04 PM PDT	Run SSO Test...
File	April 28, 2020 5:54:00 PM PDT	Passed - April 29, 2020 11:05:37 AM PDT	Run SSO Test...

在Expressway上配置SSO

将元数据导入Expressway C

打开浏览器到https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml，并将元数据保存到本地文件夹

上传到**Configuration > Unified Communications > IDP**。

从Expressway C导出元数据

转至配置 — >统一通信 — > IDP ->导出SAML数据

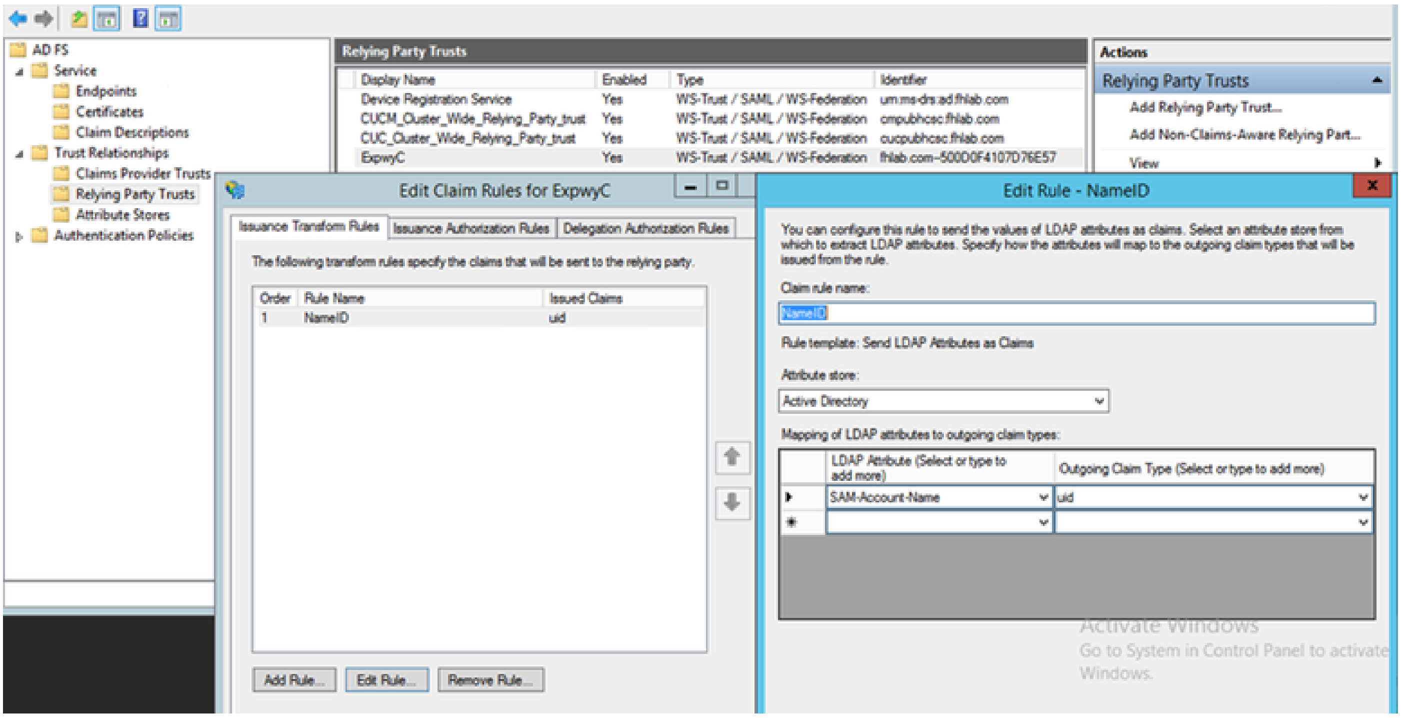
集群模式使用SAML中包含的自签名证书（具有长生命期）

元数据，用于对SAML请求签名

- 在集群范围模式下，要下载单个集群范围的元数据文件，请点击Download
- 在每对等模式下，要下载单个对等体的元数据文件，请点击对等体旁边的下载。要在.zip文件中导出所有内容，请点击Download All。

为Cisco Expressway-E添加信赖方信任

首先，为Expressway Es创建信赖方信任，然后添加声明规则以将身份作为UID属性发送。



Relying Party Trusts

Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-Trust / SAML / WS-Federation	urn:ms-drs:ad.fhlab.com
CUCM_Cluster_Wide_Relying_Party_trust	Yes	WS-Trust / SAML / WS-Federation	cmpubhcsc.fhlab.com
CUC_Cluster_Wide_Relying_Party_trust	Yes	WS-Trust / SAML / WS-Federation	cucpubhcsc.fhlab.com
ExpwyC	Yes	WS-Trust / SAML / WS-Federation	fhlab.com-500D0F4107D76E57

Edit Claim Rules for ExpwyC

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
1	NameID	uid

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:
NameID

Rule template: Send LDAP Attributes as Claims

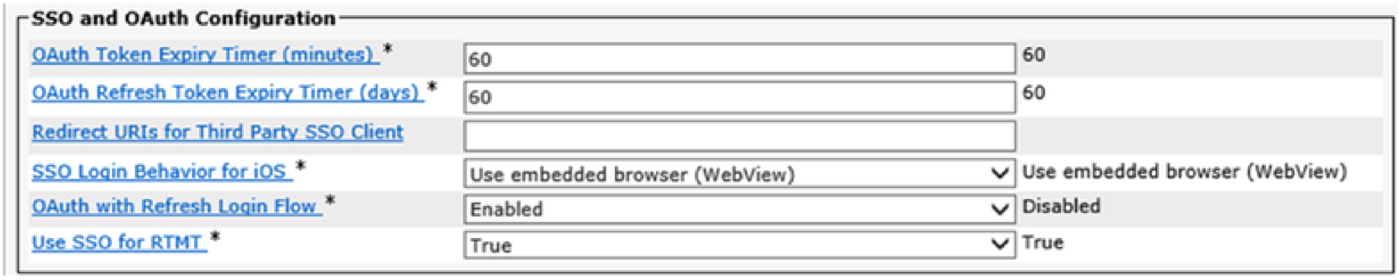
Attribute store:
Active Directory

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
*		

OAuth与刷新登录

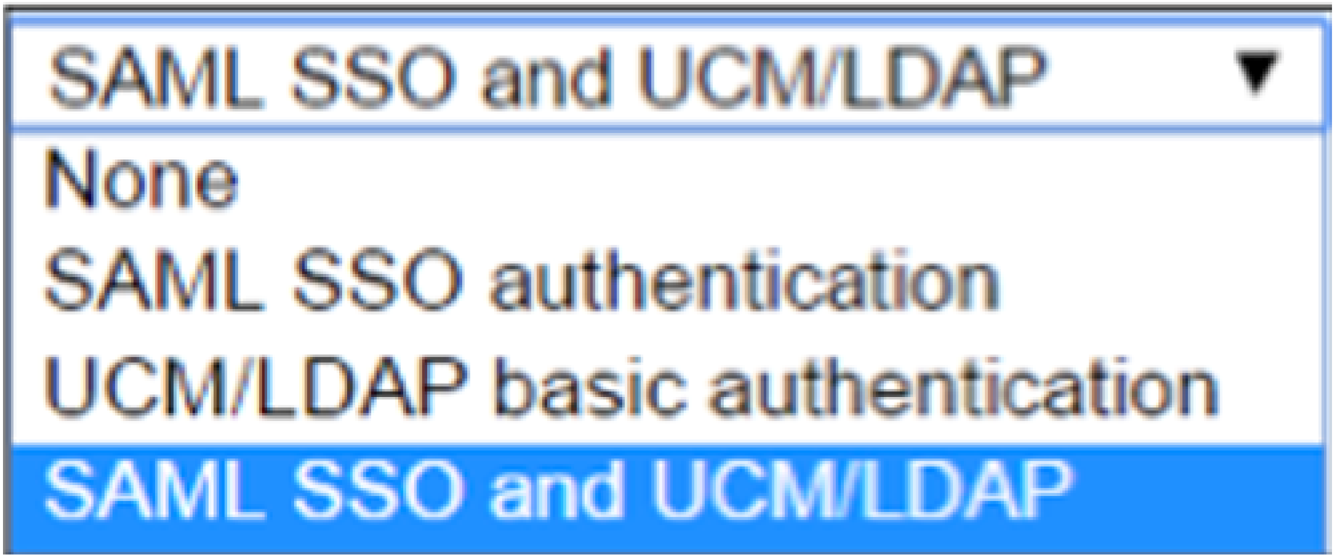
在Cisco CUCM企业参数中，启用了使用刷新登录流参数验证OAuth。转到**Cisco Unified CM管理 >企业参数> SSO和OAuth配置**。



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

身份验证路径



- 如果身份验证路径设置为“SAML SSO身份验证”，则只有使用启用SSO的Unified CM集群的Jabber客户端才能在此Expressway上使用MRA。这是仅SSO配置。

- 对所有IP电话、所有网真终端和驻留在未配置SSO的Unified CM集群上的任何Jabber客户端的Expressway MRA支持将需要身份验证路径以包括UCM/LDAP身份验证。
- 如果一个或多个Unified CM集群支持Jabber SSO，请选择“SAML SSO和UCM/LDAP”以允许SSO和基本身份验证。

SSO架构

SAML是基于XML的开放标准数据格式，使管理员能够在登录到其中一个应用后无缝访问一组定义的思科协作应用。SAML SSO使用SAML 2.0协议为思科协作解决方案提供跨域和跨产品单点登录。

本地登录流

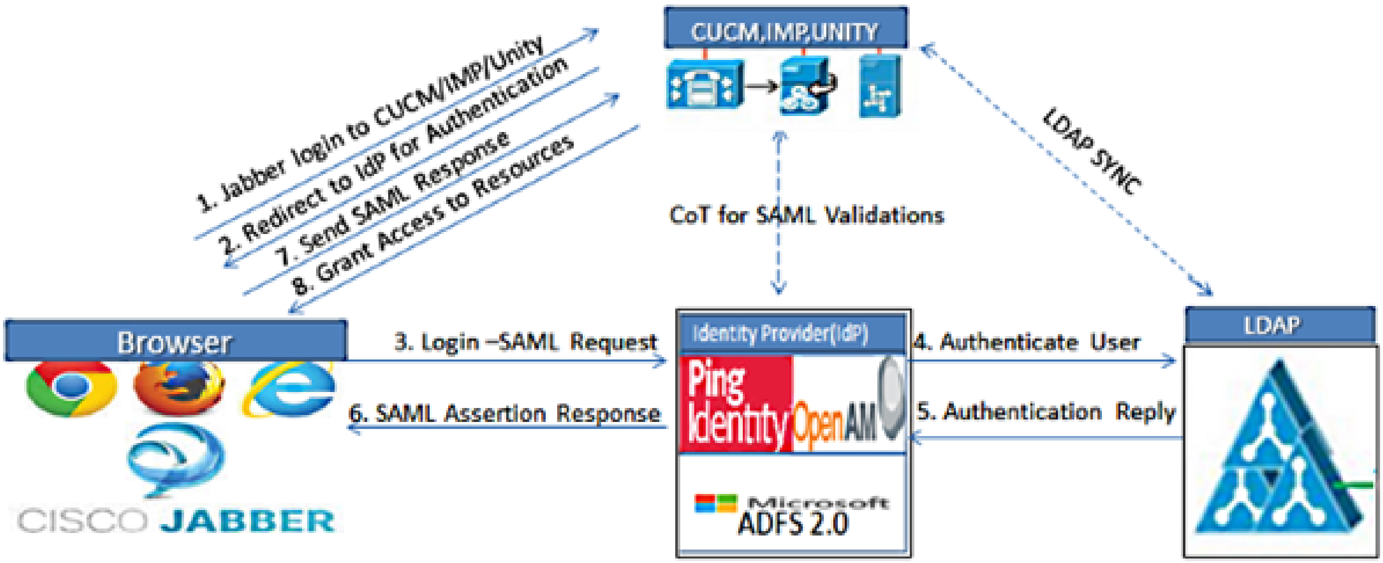
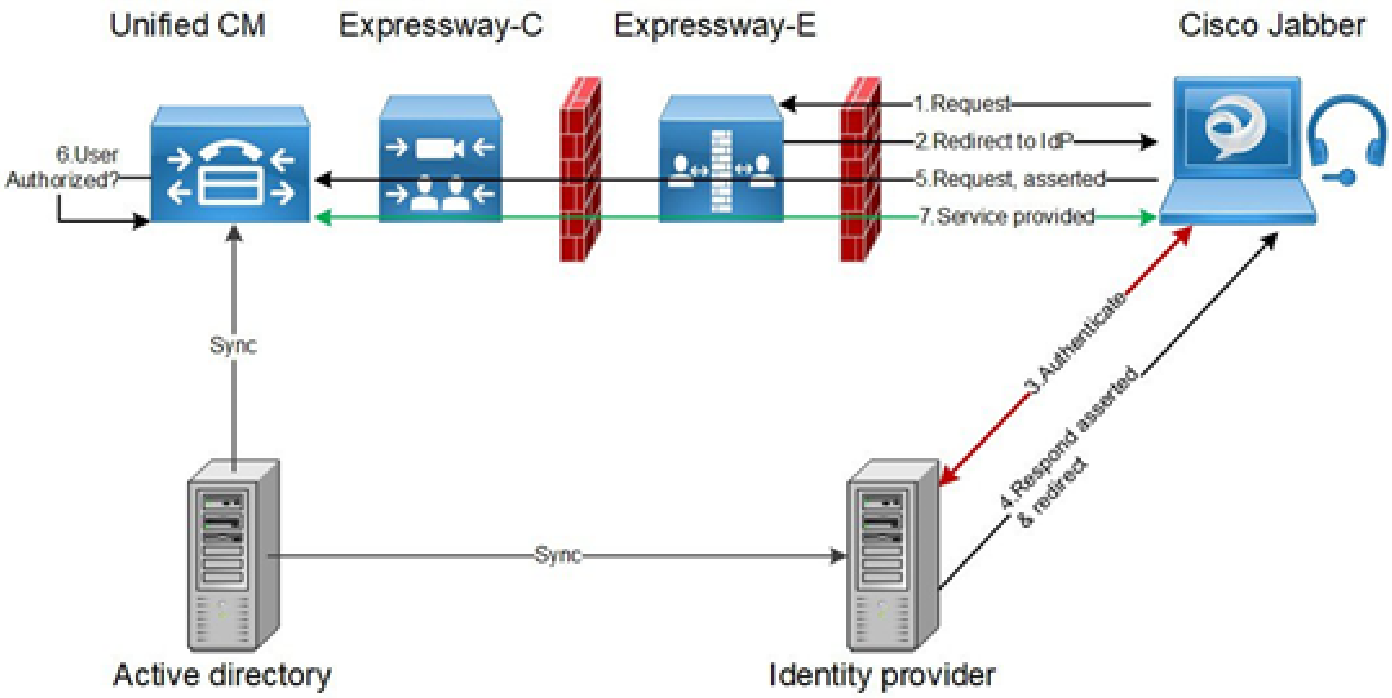


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

MRA登录流



OAuth

OAuth是支持授权的标准。用户必须经过身份验证才能获得授权。授权码授权流为客户端提供获取访问和刷新令牌以访问资源（Unified CM、IM&P、Unity和Expressway服务）的方法。 此流程也基于重定向，因此要求客户端能够与用户控制的HTTP用户代理（Web浏览器）交互。客户端将使用HTTPS向授权服务器发出初始请求。OAuth服务器将用户重定向到身份验证服务。如果启用了SAML SSO，则此操作可能在Unified CM或外部IdP上运行。根据所使用的验证方法，网页视图可呈现给最终用户以验证自己。（Kerberos身份验证是不显示网页的示例。）与隐式授权流不同，成功的身份验证代码授权流将导致OAuth服务器向Web浏览器发出“授权代码”。这是一次性、短暂的唯一代码，然后从Web浏览器传回客户端。客户端将此“授权代码”连同预共享密钥一起提供给授权服务器，并接收“访问令牌”和“刷新令牌”交换。此步骤中使用的客户端密钥使授权服务能够将使用限制为仅允许注册和经过身份验证的客户端使用。令牌用于以下目的：

访问/刷新令牌

访问令牌：此令牌由授权服务器颁发。当客户端需要访问该服务器上的受保护资源时，会将令牌呈现给资源服务器。资源服务器能够验证令牌并信任使用该令牌的连接。（思科访问令牌默认为60分钟的生命周期）

刷新令牌：授权服务器再次发出此令牌。当访问令牌过期或到期时，客户端将此令牌连同客户端密钥一起呈现给授权服务器。如果刷新令牌仍然有效，则授权服务器将发出新的访问令牌，而无需进行其他身份验证。（思科刷新令牌默认为60天。）如果刷新令牌已过期，则必须启动新的完整OAuth授权码授权流以获取新令牌。

OAuth授权代码授予流程更好

在隐式授权流中，访问令牌通过HTTP用户代理（浏览器）传递到Jabber客户端。 在授权代码授权流中，访问令牌直接在授权服务器和Jabber客户端之间交换。使用限时唯一授权码从授权服务器请求令牌。这种访问令牌的直接交换更安全，并降低了风险。

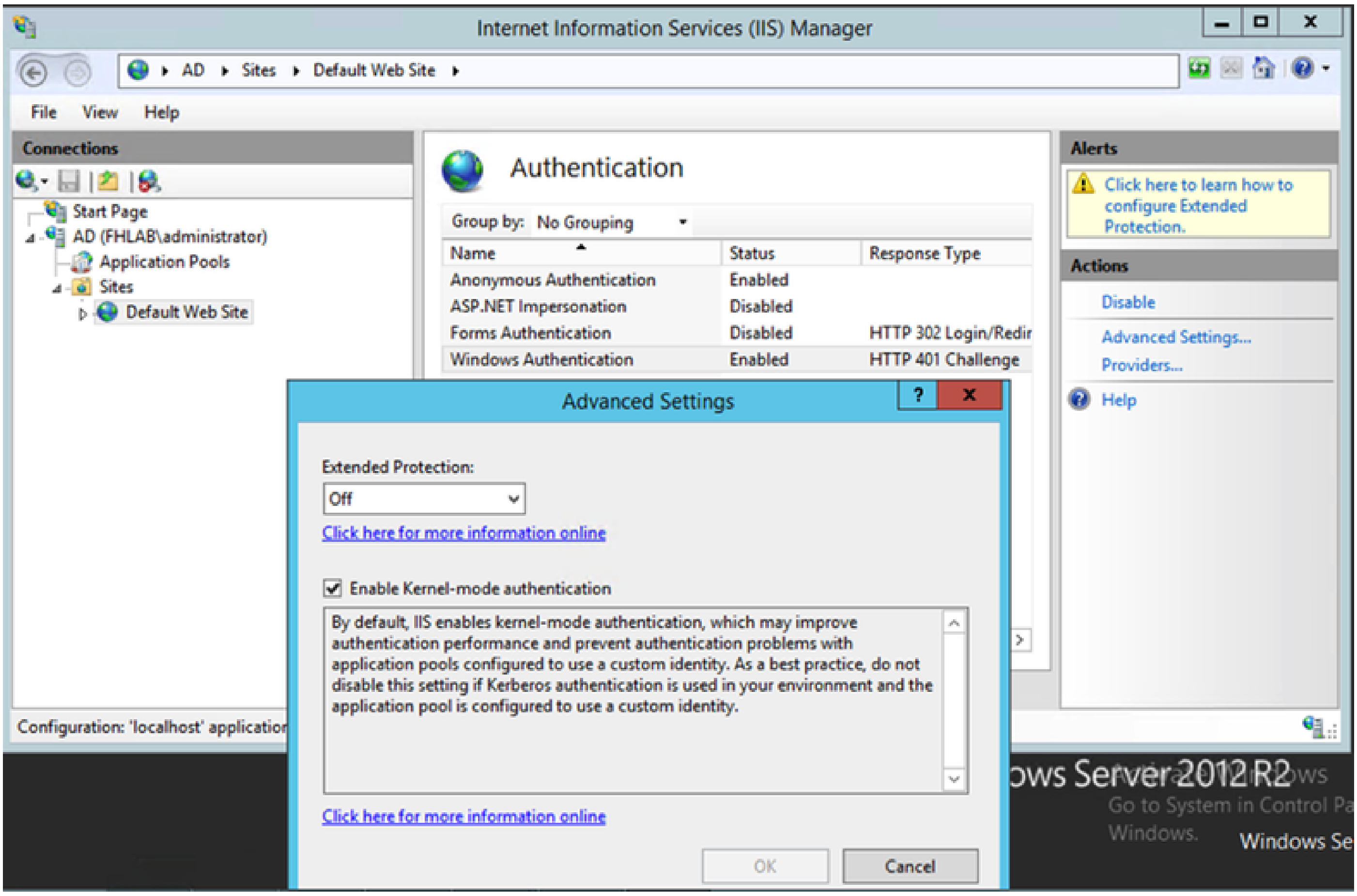
OAuth授权代码授予流支持使用刷新令牌。这为最终用户提供了更好的体验，因为他们不需要像以前那样频繁地重新进行身份验证（默认为60天）

配置Kerberos

选择Windows身份验证

Internet信息服务(IIS)管理器>站点>默认网站>身份验证> Windows身份验证>高级设置。

1. 取消选中Enable Kernel-mode authentication。
2. 确保“扩展保护”已关闭。



Internet Information Services (IIS) Manager
AD ▸ Sites ▸ Default Web Site ▸
File
View
Help
Connections
Start Page
AD (FHLAB\administrator)
Application Pools
Sites
Default Web Site
Configuration: 'localhost' application
Alerts
Click here to learn how to configure Extended Protection.
Actions
Disable
Advanced Settings...
Providers...
Help
ows Server 2012 R2
Go to System in Control Pa
Windows.
Windows Se
OK
Cancel

Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redir
Windows Authentication	Enabled	HTTP 401 Challenge

Advanced Settings

Extended Protection: Off

Click here for more information online

☑ Enable Kernel-mode authentication

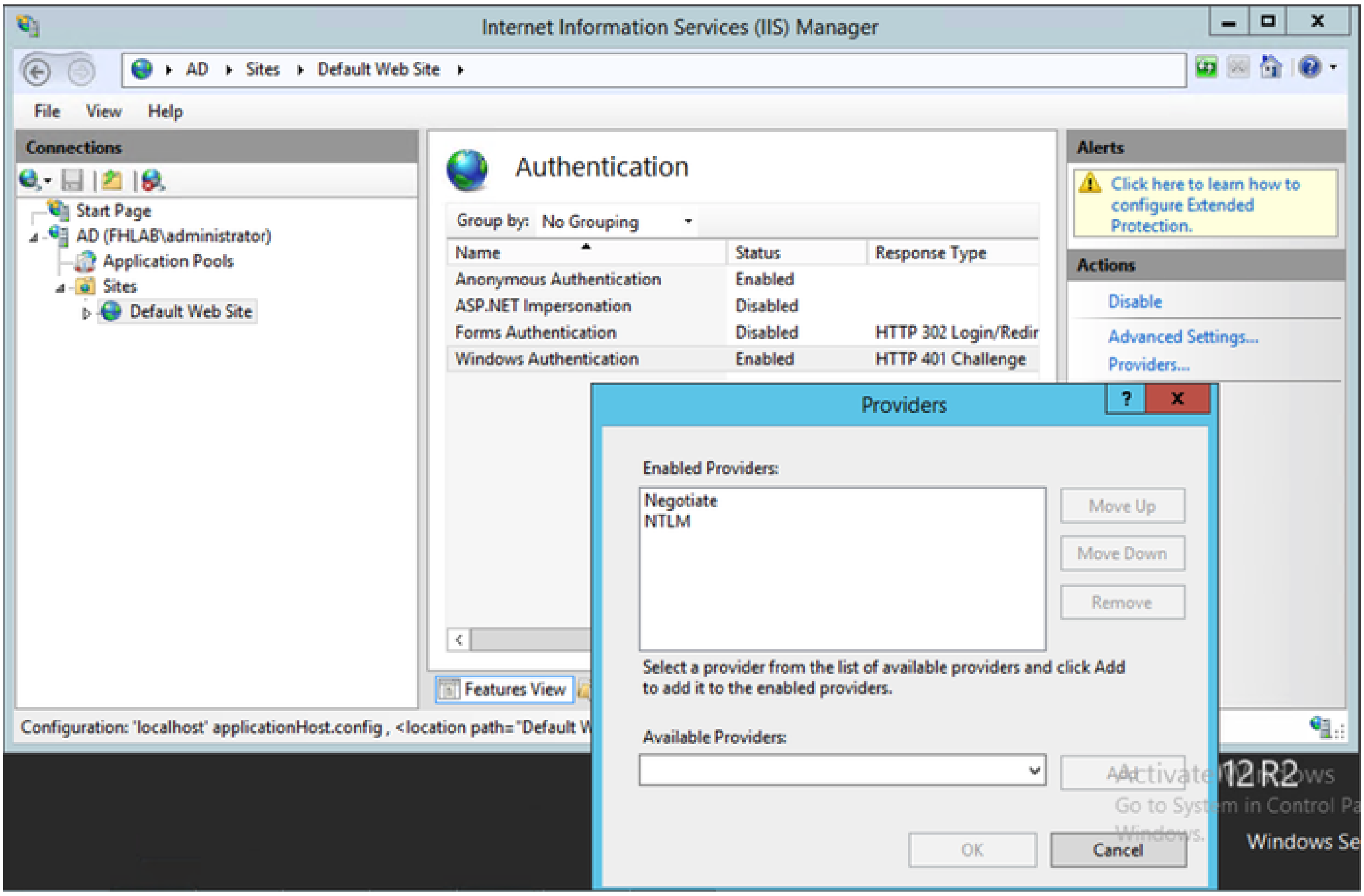
By default, IIS enables kernel-mode authentication, which may improve authentication performance and prevent authentication problems with application pools configured to use a custom identity. As a best practice, do not disable this setting if Kerberos authentication is used in your environment and the application pool is configured to use a custom identity.

Click here for more information online

ADFS支持两个Kerberos NTLM

确保AD FS版本3.0同时支持Kerberos协议和NT LAN Manager(NTLM)协议，因为所有非Windows客户端都无法使用Kerberos并依赖NTLM。

在右窗格中，选择提供程序，并确保协商和NTLM在已启用的提供程序下：



Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redir
Windows Authentication	Enabled	HTTP 401 Challenge

Enabled Providers:

Negotiate
NTLM

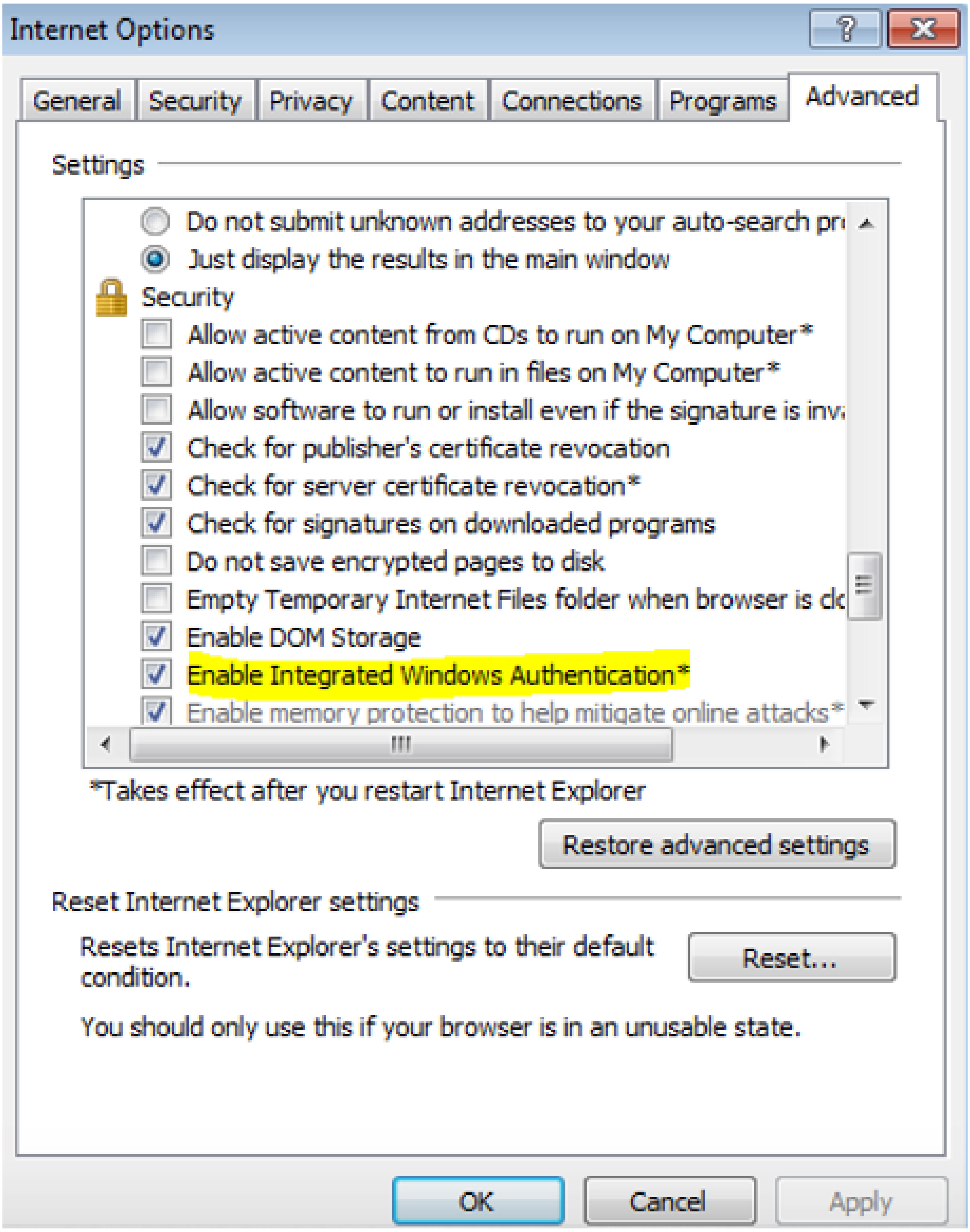
Select a provider from the list of available providers and click Add to add it to the enabled providers.

Available Providers:

Configuration: 'localhost' applicationHost.config , <location path="Default W

配置Microsoft Internet Explorer

确保选中Internet Explorer > Advanced > Enable Integrated Windows Authentication。



Settings

○ Do not submit unknown addresses to your auto-search pr

● Just display the results in the main window

Security

□ Allow active content from CDs to run on My Computer*

□ Allow active content to run in files on My Computer*

□ Allow software to run or install even if the signature is inv

☑ Check for publisher's certificate revocation

☑ Check for server certificate revocation*

☑ Check for signatures on downloaded programs

□ Do not save encrypted pages to disk

□ Empty Temporary Internet Files folder when browser is cl

☑ Enable DOM Storage

☑ Enable Integrated Windows Authentication*

☑ Enable memory protection to help mitigate online attacks*

*Takes effect after you restart Internet Explorer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

在“安全”>“内部网区域”>“站点”下添加ADFS URL