# Configuración de SAML SSO en Cisco Unified Communications Manager con ADFS 3.0

## Contenido

# Introducción

Este documento describe los pasos para configurar el inicio de sesión único con el servicio de federación de Active Directory (ADFS 3.0) con el uso de Windows 2012 R2 en los productos Cisco Unified Communication Manager (CUCM), Cisco Unity Connection (CUC) y Expressway. Los pasos para configurar Kerberos también se incluyen en este documento.

# Prerequisites

## Requirements

Cisco recomienda que conozca los productos Single Sign-On (SSO) y Windows.

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CUCM 11.5
- CUC 11.5
- Expressway 12
- Servidor Windows 2012 R2 con estas funciones:
  - Servicios de certificados de Active Directory
  - Servicios de federación de Active Directory

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Comprobación previa de la configuración

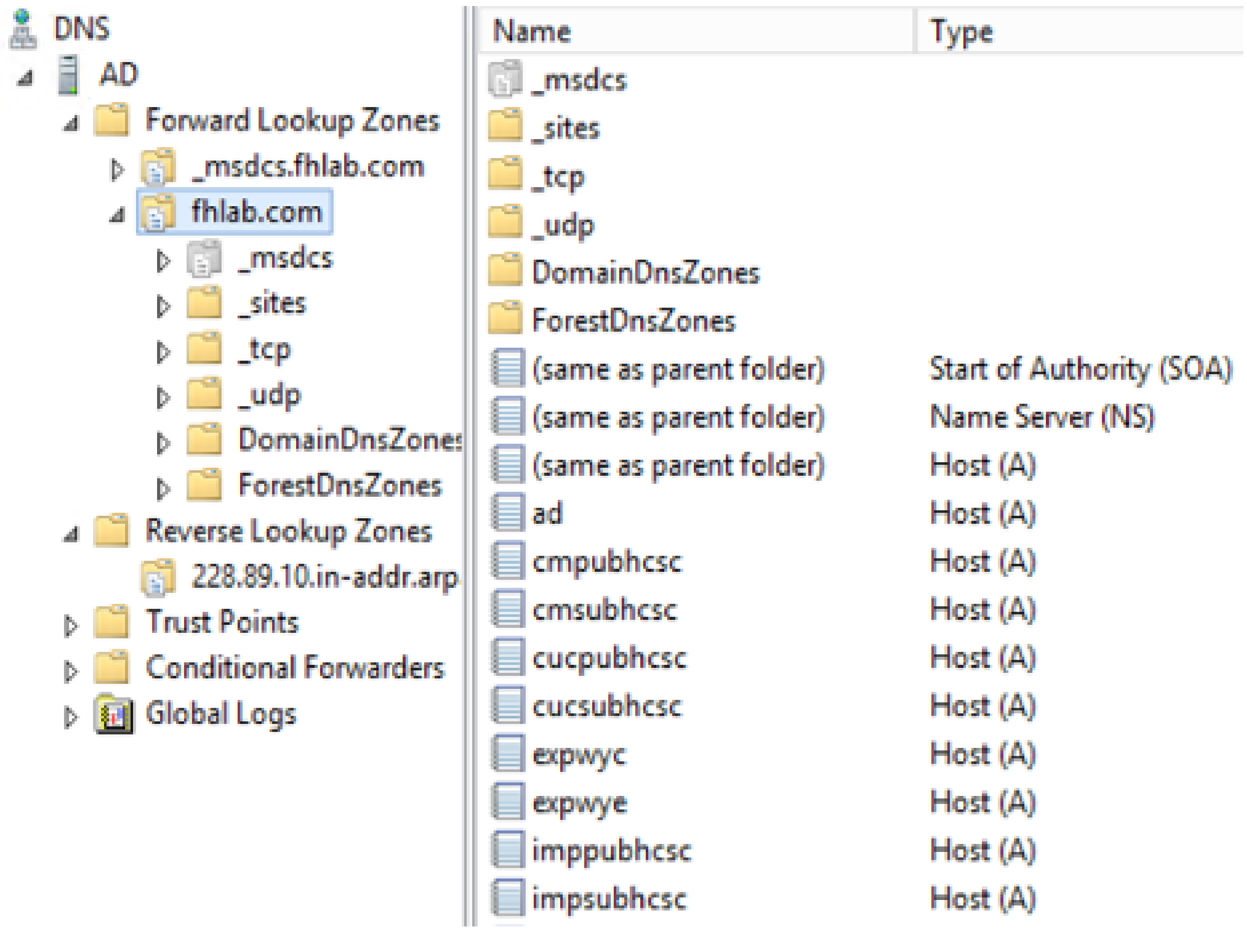
Antes de instalar ADFS3, estas funciones de servidor ya deben existir en el entorno:

·Domain Controller y DNS

·Todos los servidores deben agregarse como registros A junto con su registro de puntero (un tipo de registro DNS que resuelve una dirección IP en un dominio o nombre de host)

## A Records

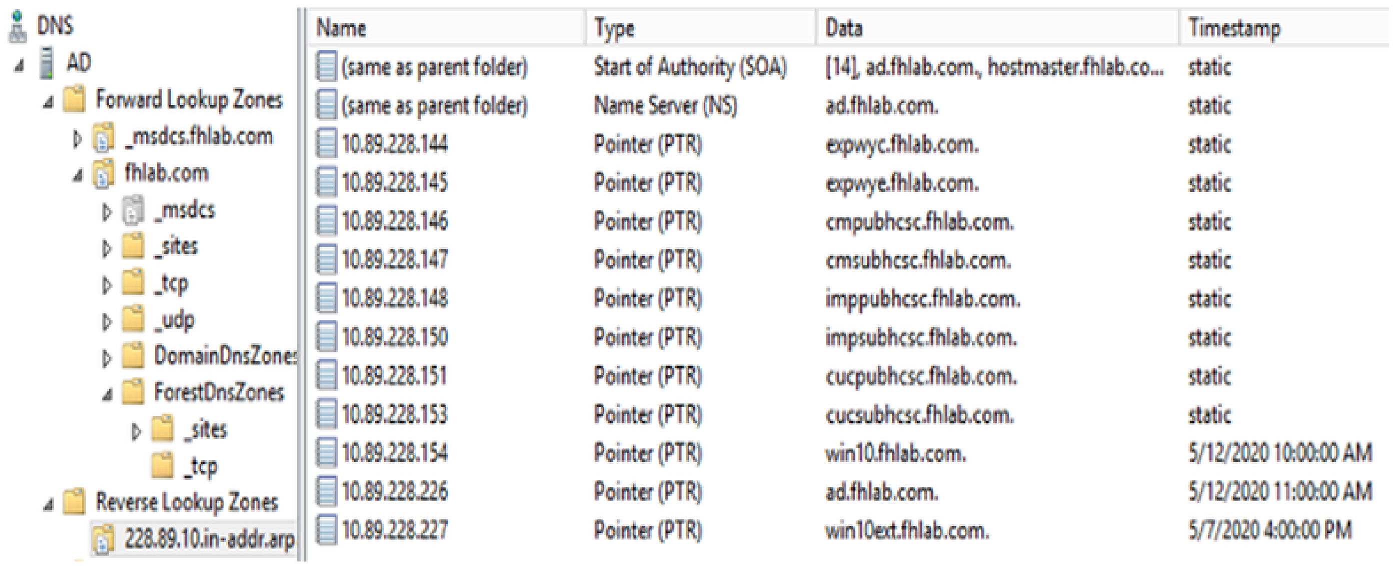
En fhlab.com. se han agregado los hosts cmpubhcsc, cmsubhcsc, cucpubhcsc, cucsubhcsc, expwyc, expwye, impubhcsc e imsubhcsc.



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

| 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) |

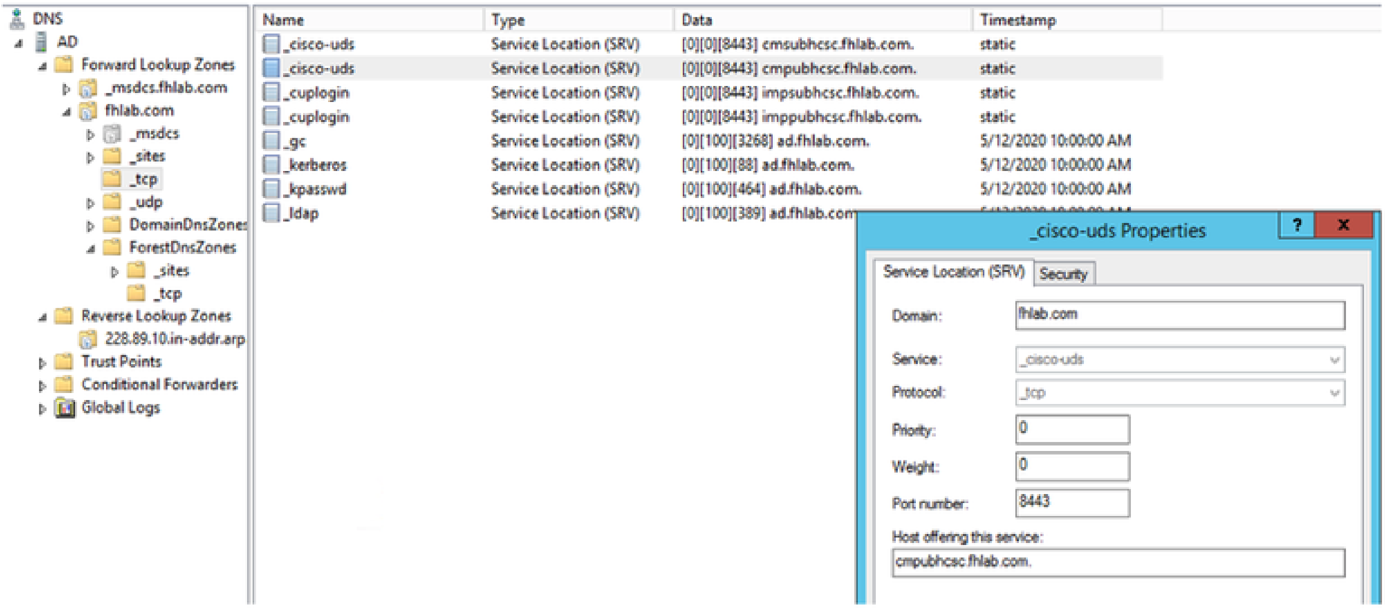
Registros de puntero (PTR)



- 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

| 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 |

Se necesitan registros SRV para Jabber Discovery Services



| 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

Domain: fhlab.com

Service: _cisco-uds

Protocol: _tcp

Priority: 0

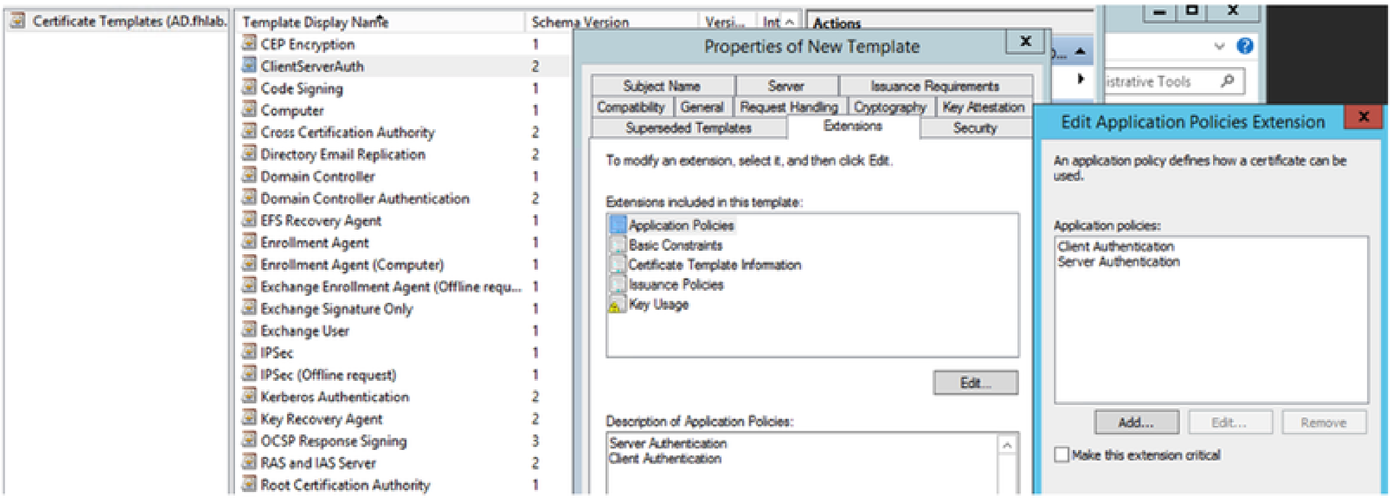
Weight: 0

Port number: 8443

Host offering this service: cmpubhcsc.fhlab.com.

- CA raíz (suponiendo que los certificados sean Enterprise CA-signed)

Es necesario crear una plantilla de certificado basada en la plantilla de certificado de servidor Web, la primera se duplica, se cambia el nombre y, en la ficha Extensiones, se modifican las políticas de aplicación agregando una política de aplicación de autenticación de cliente. Esta plantilla es necesaria para firmar todos los certificados internos (CUCM, CUC, IMP y núcleo de Expressway) en un entorno LAB, la CA interna también puede firmar las solicitudes de firma de certificados (CSR) de Expressway E.



| 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

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

Description of Application Policies:

Server Authentication
Client Authentication

Edit Application Policies Extension

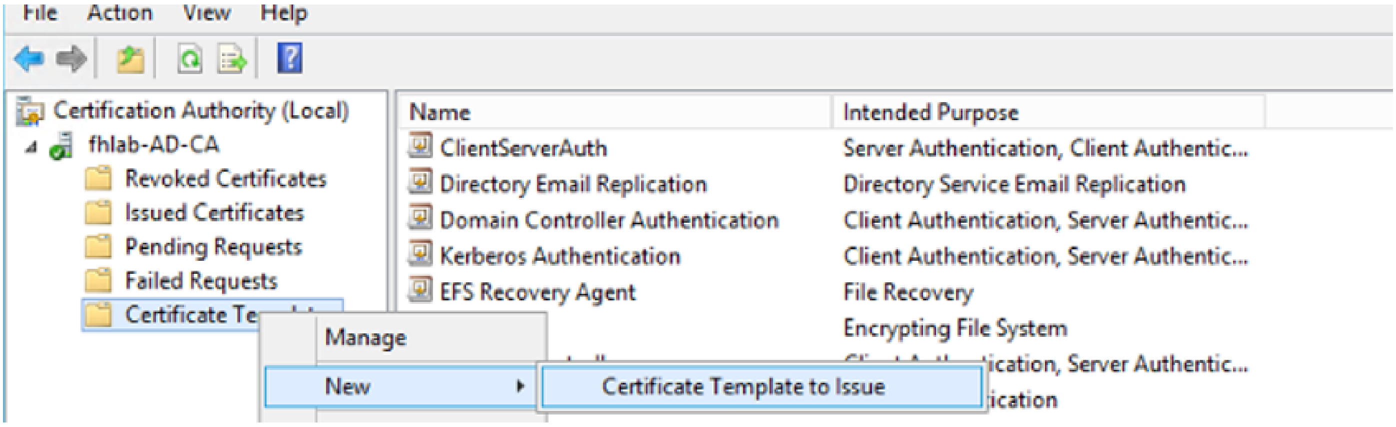
An application policy defines how a certificate can be used.

Application policies:

Client Authentication
Server Authentication

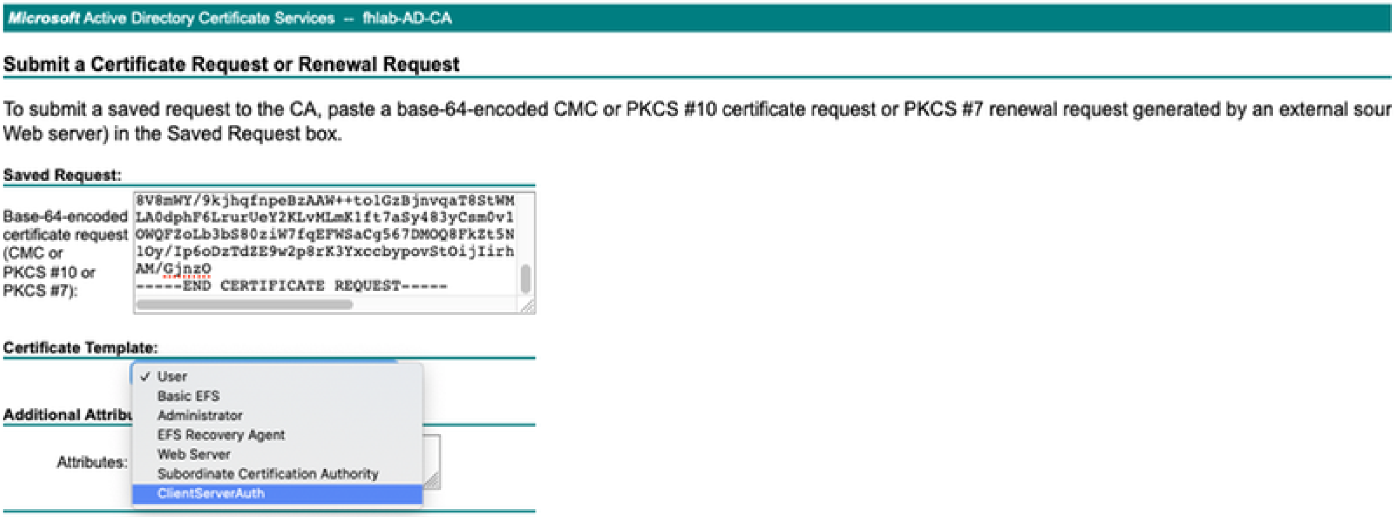
□ Make this extension critical

La plantilla creada debe emitirse para poder firmar CSR.



| 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 |
|  | ication, Server Authentic... |
|  | ication |

En la Web de certificados de CA, seleccione la plantilla que se ha creado anteriormente.


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.

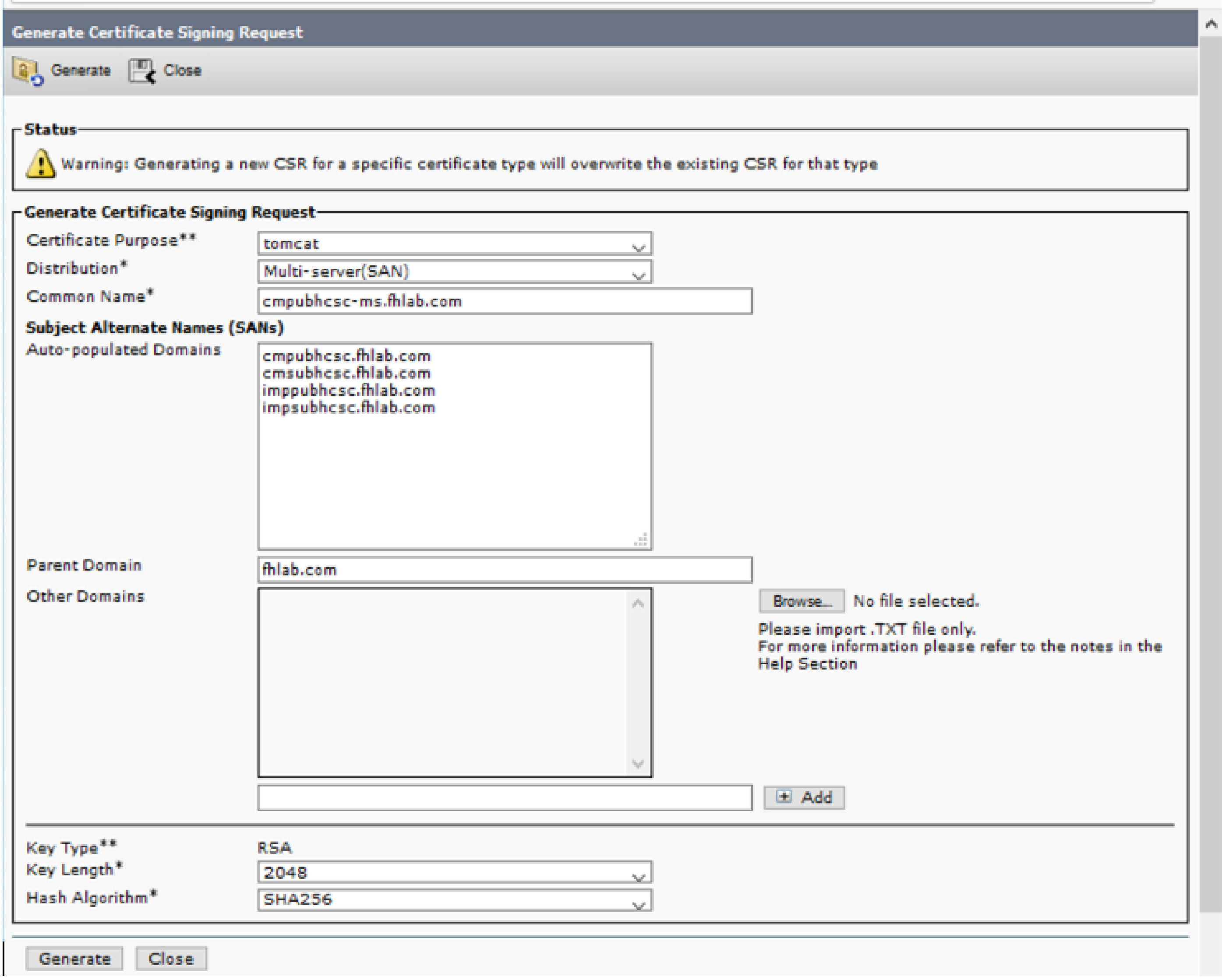
Saved Request:

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:

CUCM, IMP y CUC Multi-Server CSR deben ser generados y firmados por la CA. El propósito del certificado debe ser tomcat.



**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

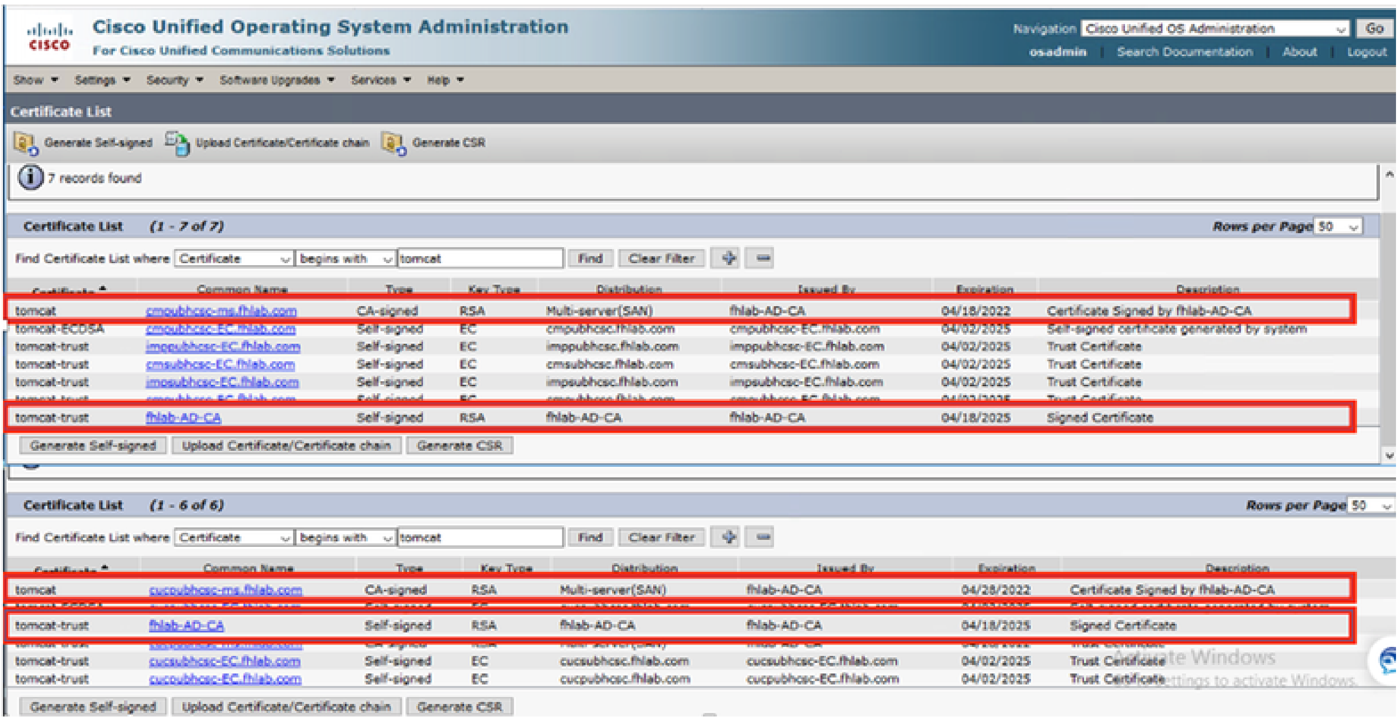
Other Domains

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 |

El certificado raíz de la CA debe cargarse en Tomcat Trust y el certificado firmado en tomcat.


cisco
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 Find Clear Filter

| 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 | cmpubhcsc-EC.fhlab.com | Self-signed | EC | cmpubhcsc.fhlab.com | cmpubhcsc-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 Find Clear Filter

| 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-ECDSA | [illegible] | [illegible] | EC | [illegible] | [illegible] | [illegible] | [illegible] |
| tomcat-trust | fhlab-AD-CA | Self-signed | RSA | fhlab-AD-CA | fhlab-AD-CA | 04/18/2025 | Signed Certificate |
| tomcat-trust | [illegible] | CA-signed | RSA | Multi-server(SAN) | fhlab-AD-CA | [illegible] | Trust 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.

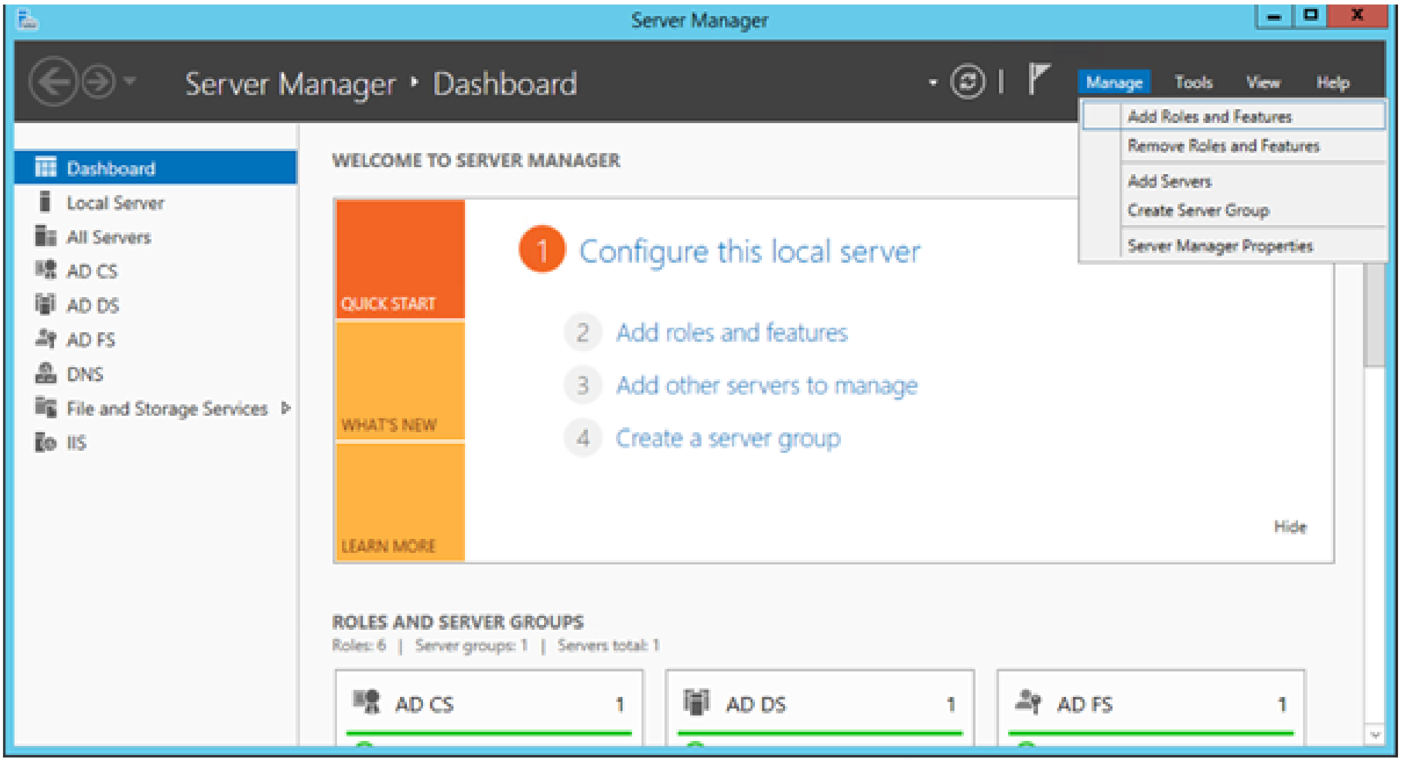
- IIS

Si no es así, esta sección atravesará la instalación de estas funciones. De lo contrario, omita esta sección y continúe directamente con la descarga de ADFS3 de Microsoft.

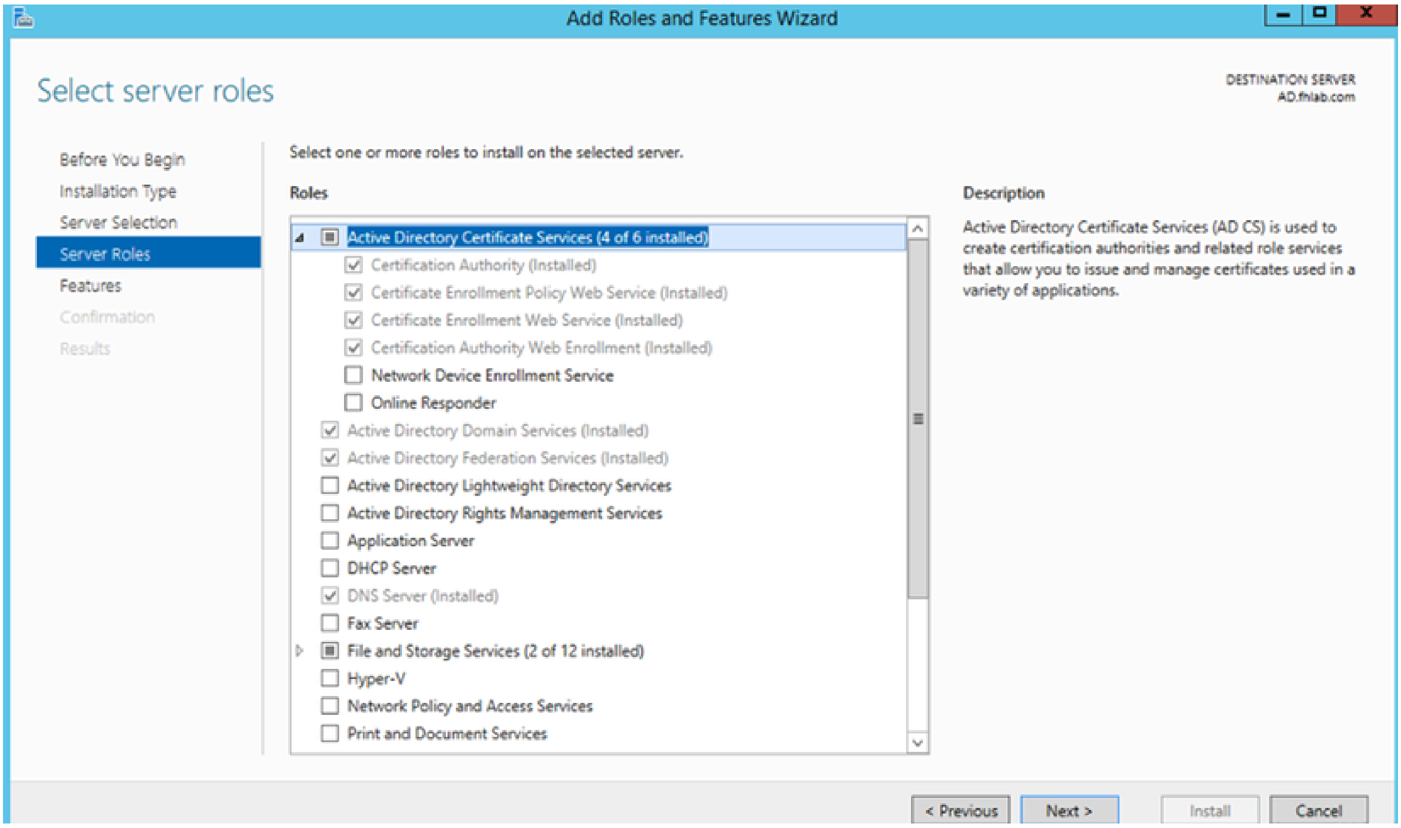
Después de instalar Windows 2012 R2 con DNS, promueva el servidor a un controlador de dominio.

La siguiente tarea será instalar Microsoft Certificate Services.

Navegue hasta Administrador de servidores y agregue una nueva función:



Seleccione la función **Servicios de certificados de Active Directory**.



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

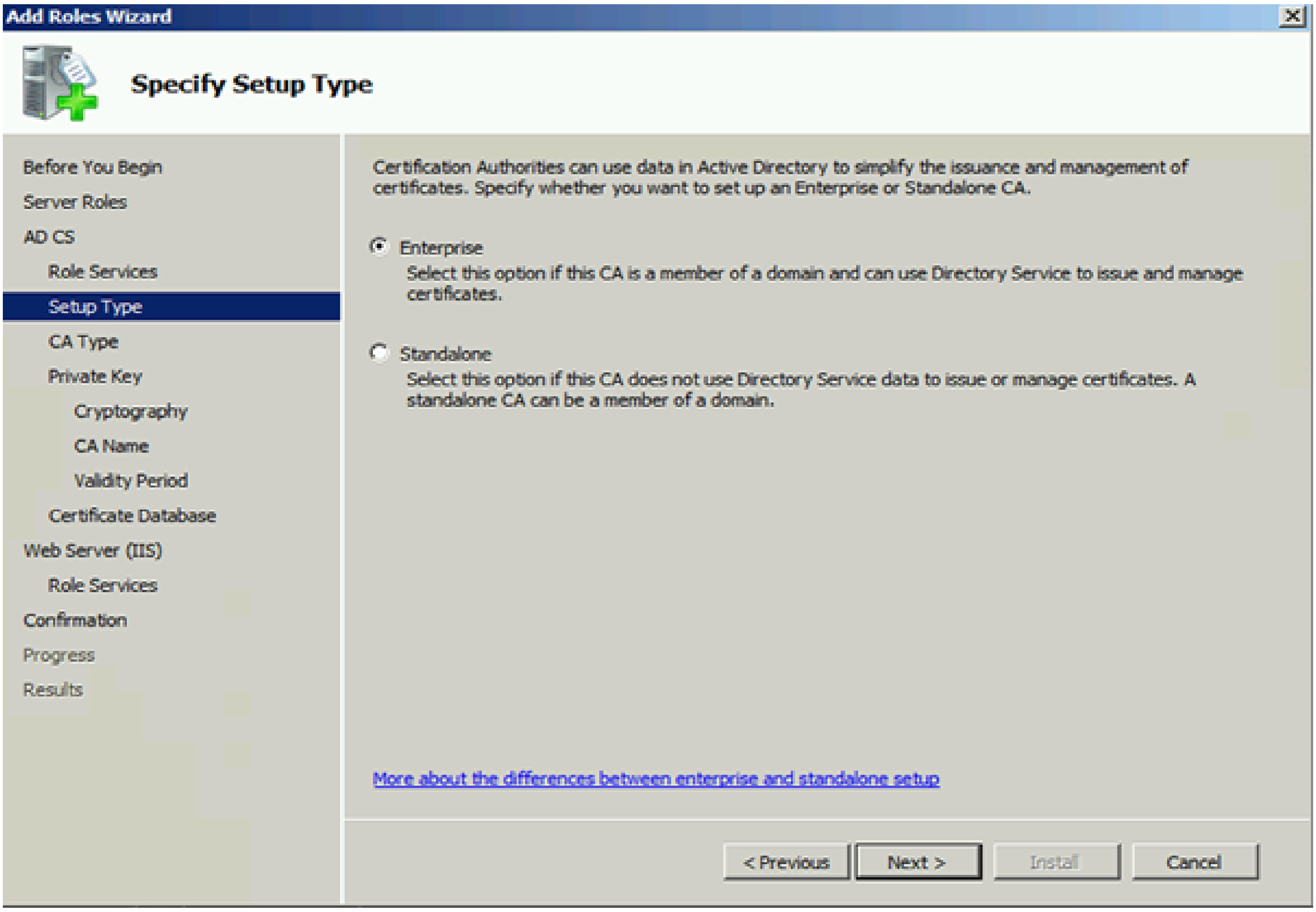
Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

E implemente estos servicios - Certificate Authority Certificate Enrollment Policy Web Service primero. Después de instalar esas dos funciones, configúrelas e instale **Servicio Web de**

**Inscripción de Certificados** y **Inscripción Web de Autoridad de Certificados**. Configurarlos.

También se agregarán servicios de rol y funciones adicionales requeridos, como IIS, cuando se instale la Autoridad de certificación.

En función de la implementación, puede seleccionar Empresa o Independiente.



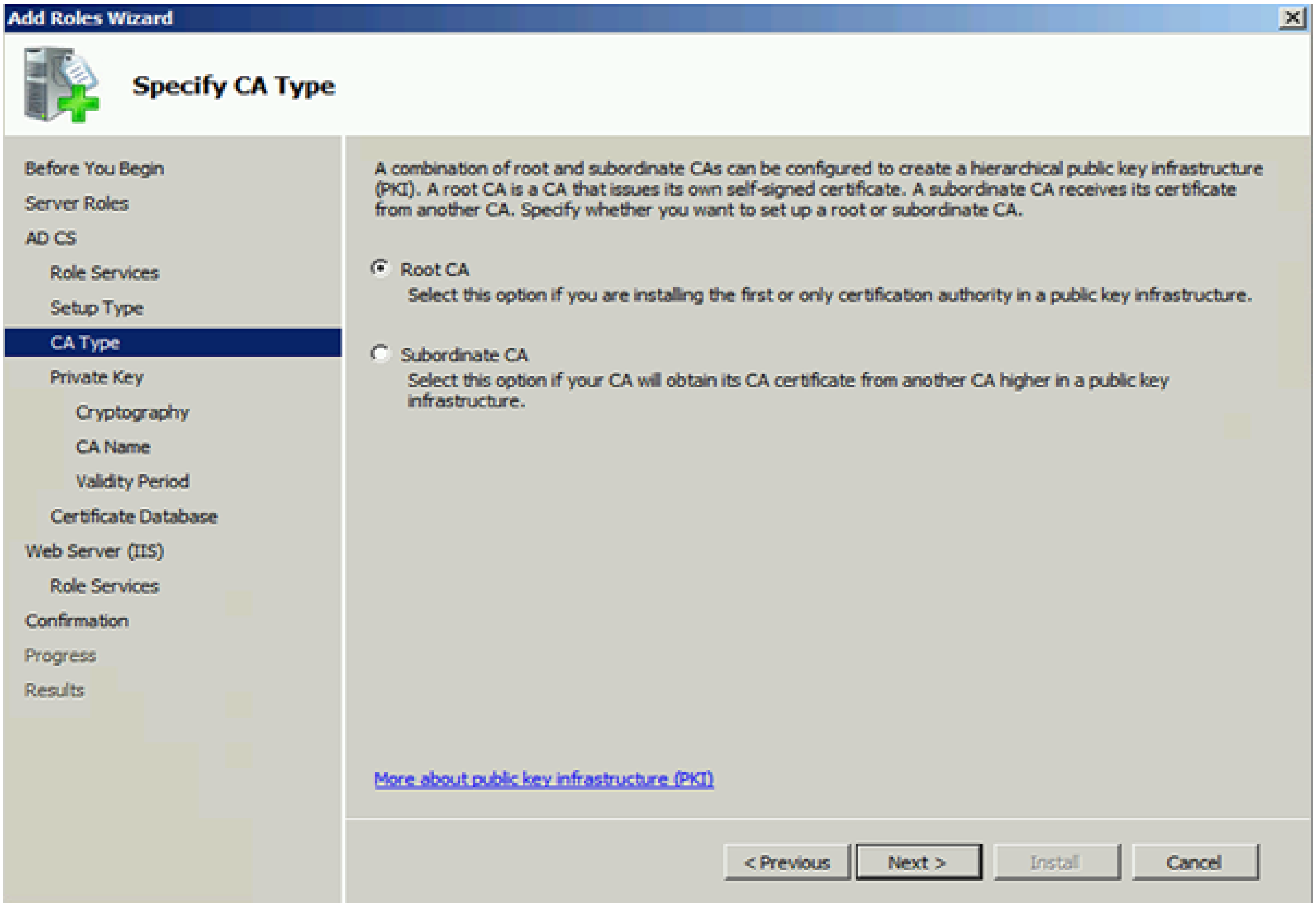
Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

● 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

Para el tipo de CA, puede seleccionar CA raíz o CA subordinada. Si no hay otra CA en ejecución en la organización, seleccione **CA raíz**.



### Specify CA Type

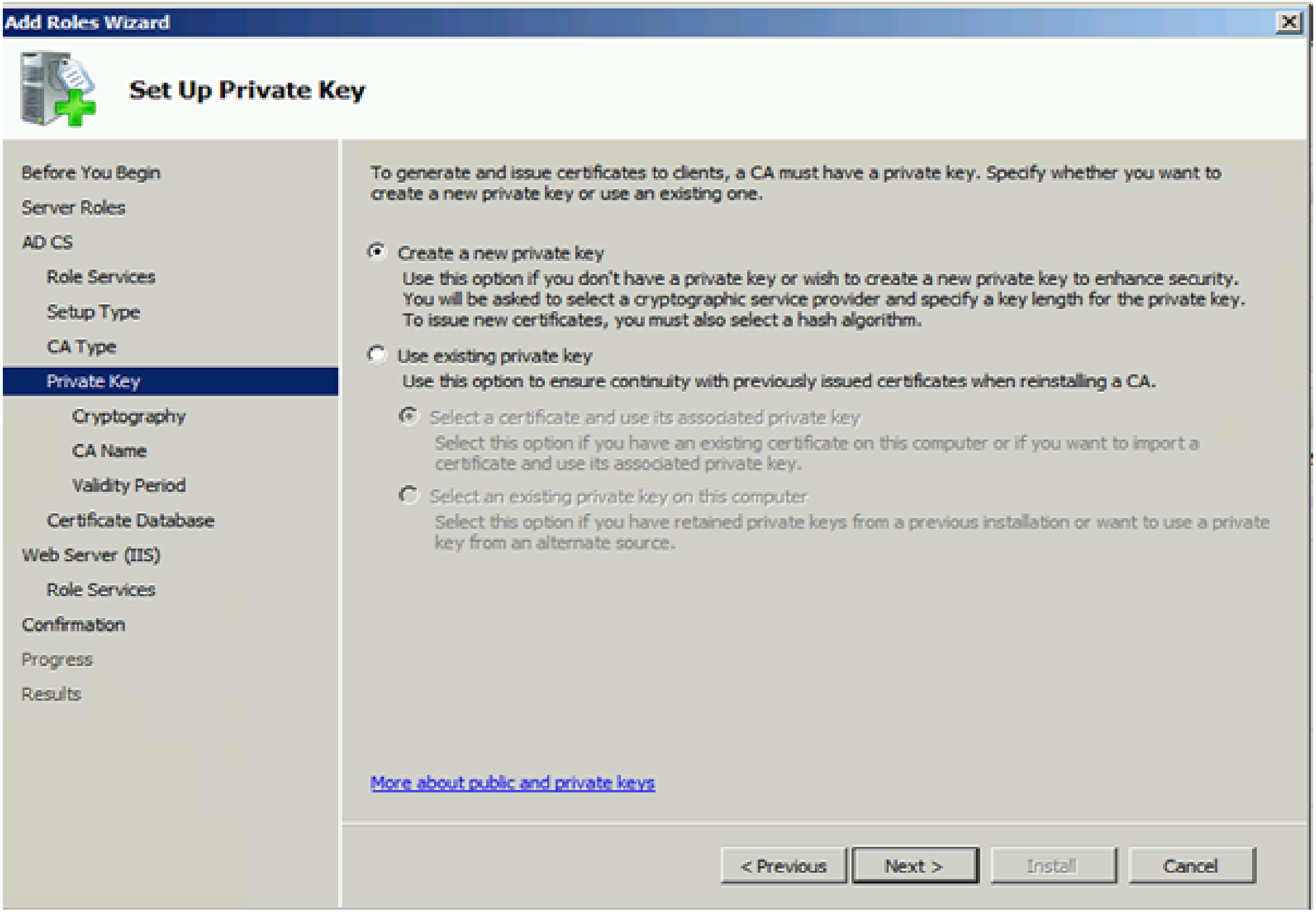
A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

● 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)

El siguiente paso es crear una clave privada para su CA.



### 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.

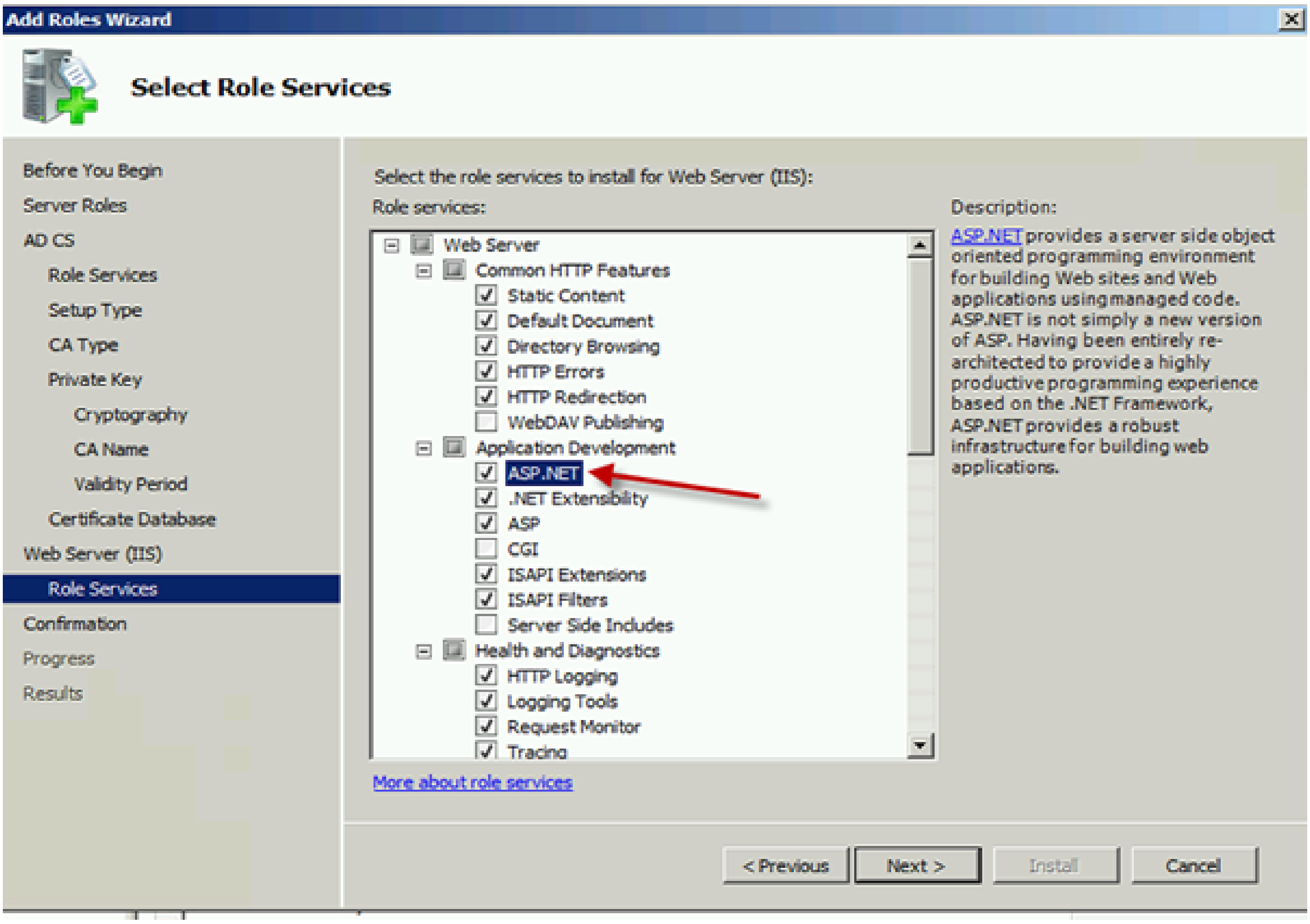
● Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ 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

Este paso sólo es necesario si instala el ADFS3 en un Windows Server 2012 independiente.

Después de configurar la CA, es necesario configurar los servicios de función para IIS. Esto es necesario para la inscripción Web en la CA. Para la mayoría de las implementaciones de ADFS, una función adicional en IIS, haga clic en **ASP.NET** en Desarrollo de aplicaciones.



Select Role Services

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

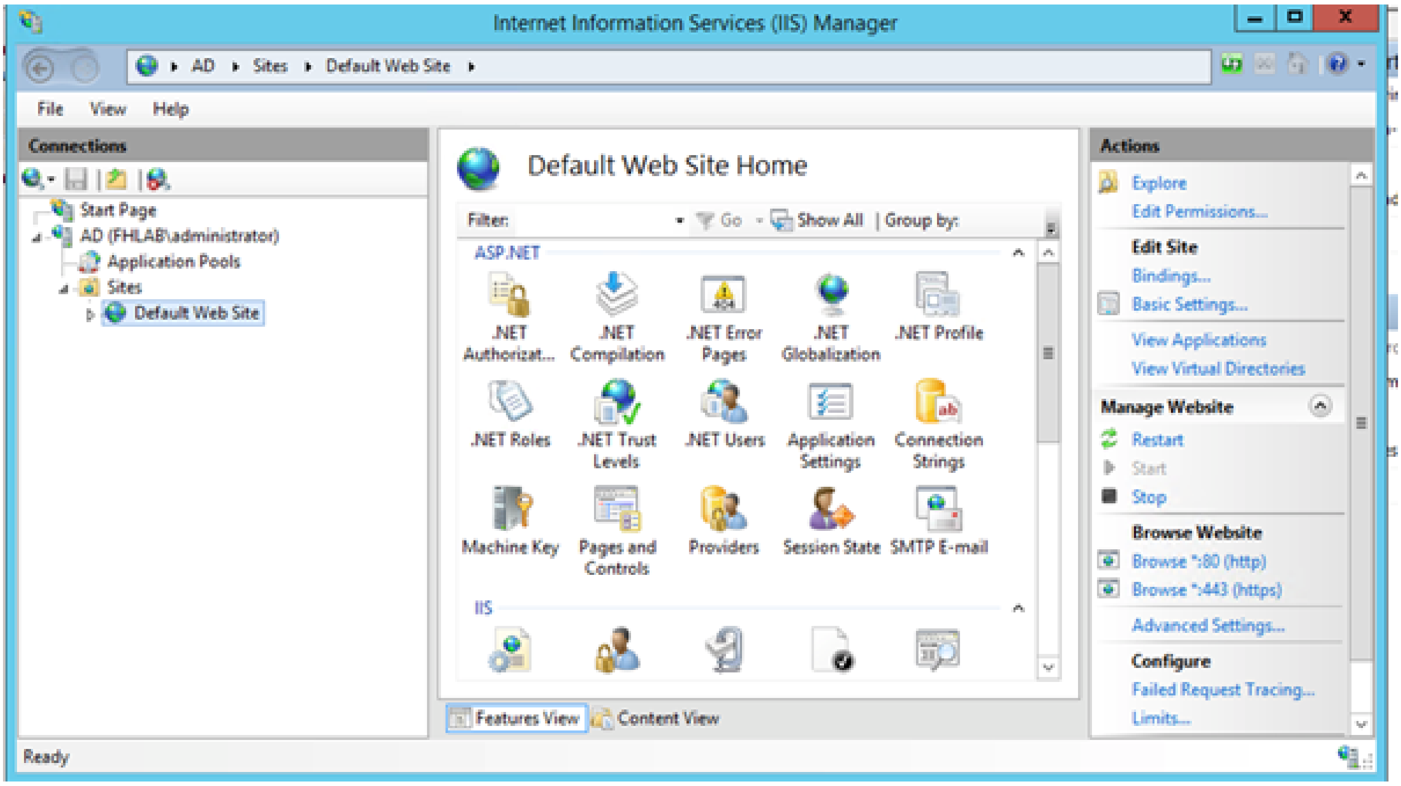
Role services:

- 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

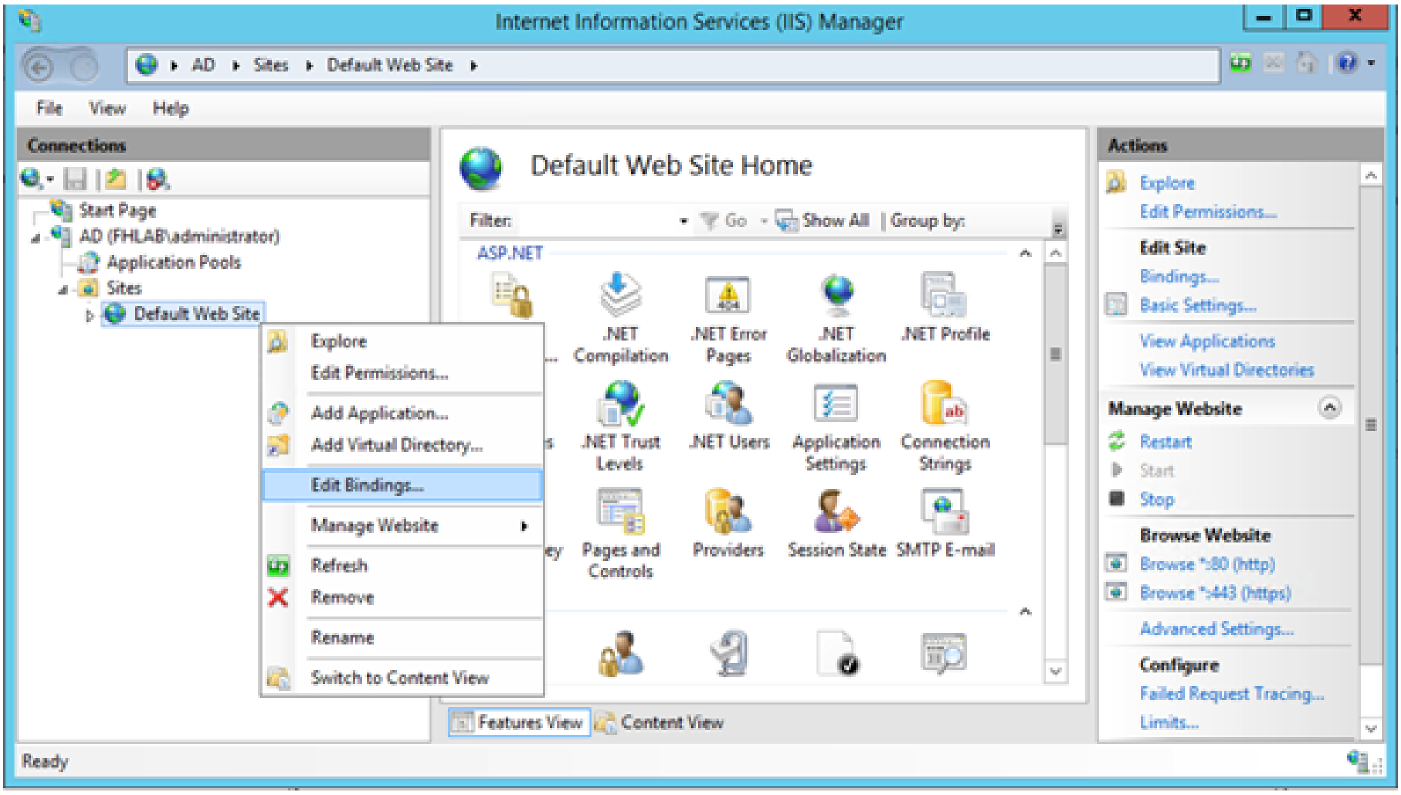
Description:

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.

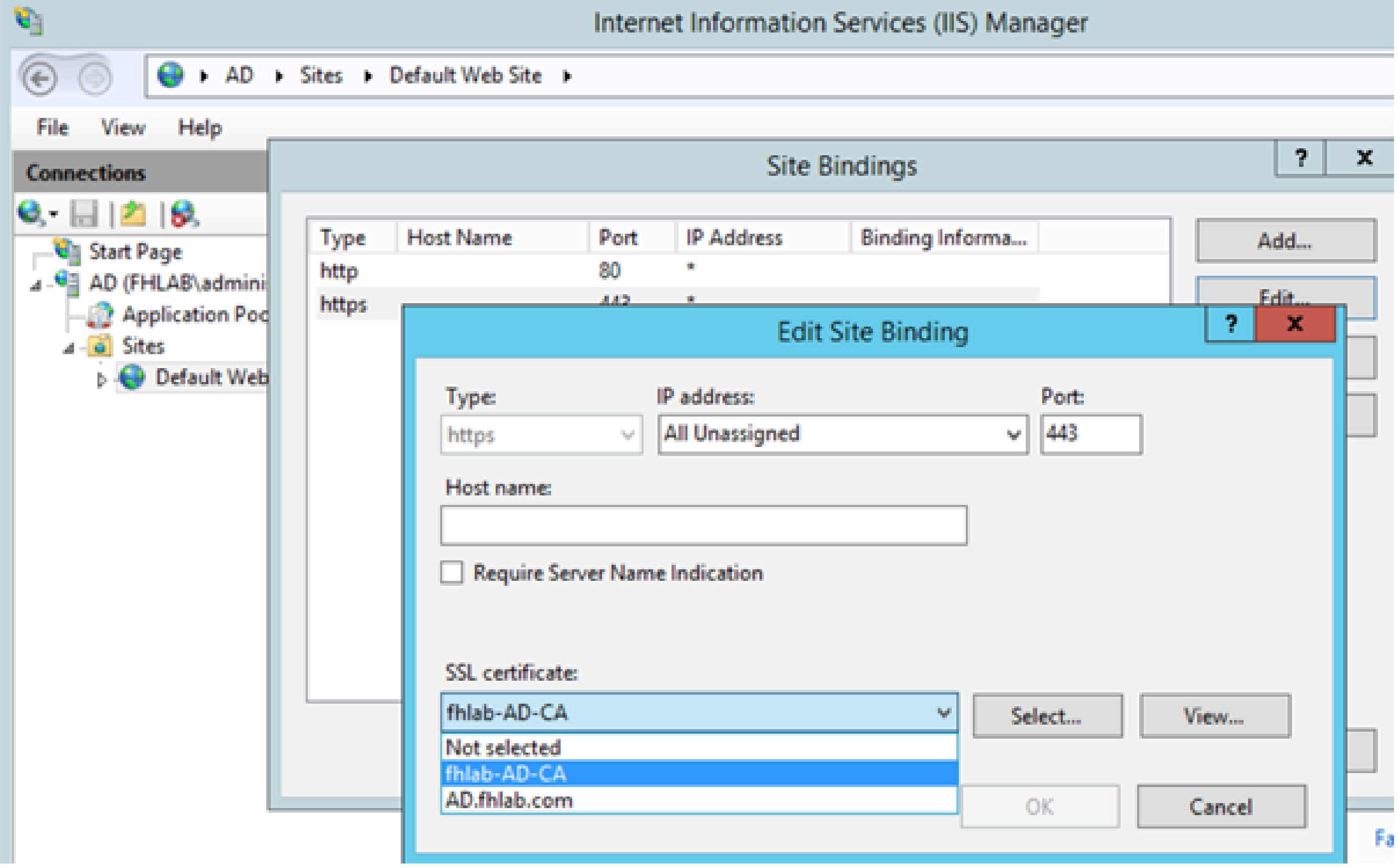
En Administrador de servidores, haga clic en **Servidor Web > IIS** y, a continuación, haga clic con el botón secundario en **Sitio Web predeterminado**. El enlace debe cambiarse para permitir también HTTPS además de HTTP. Esto se hace para admitir HTTPS.



Seleccione **Editar enlaces**.



Agregue un nuevo enlace de sitio y seleccione **HTTPS** como tipo. Para el certificado SSL, elija el certificado de servidor que debe tener el mismo FQDN que su servidor AD.

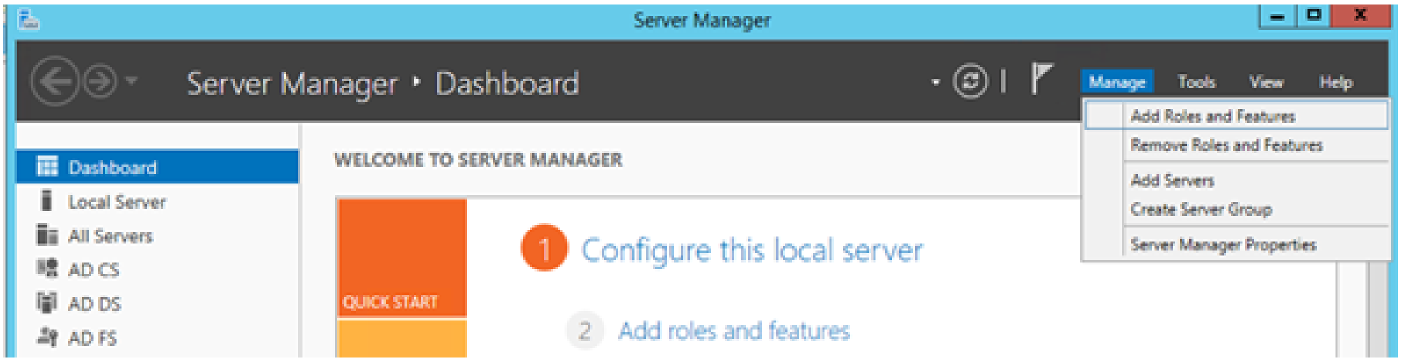


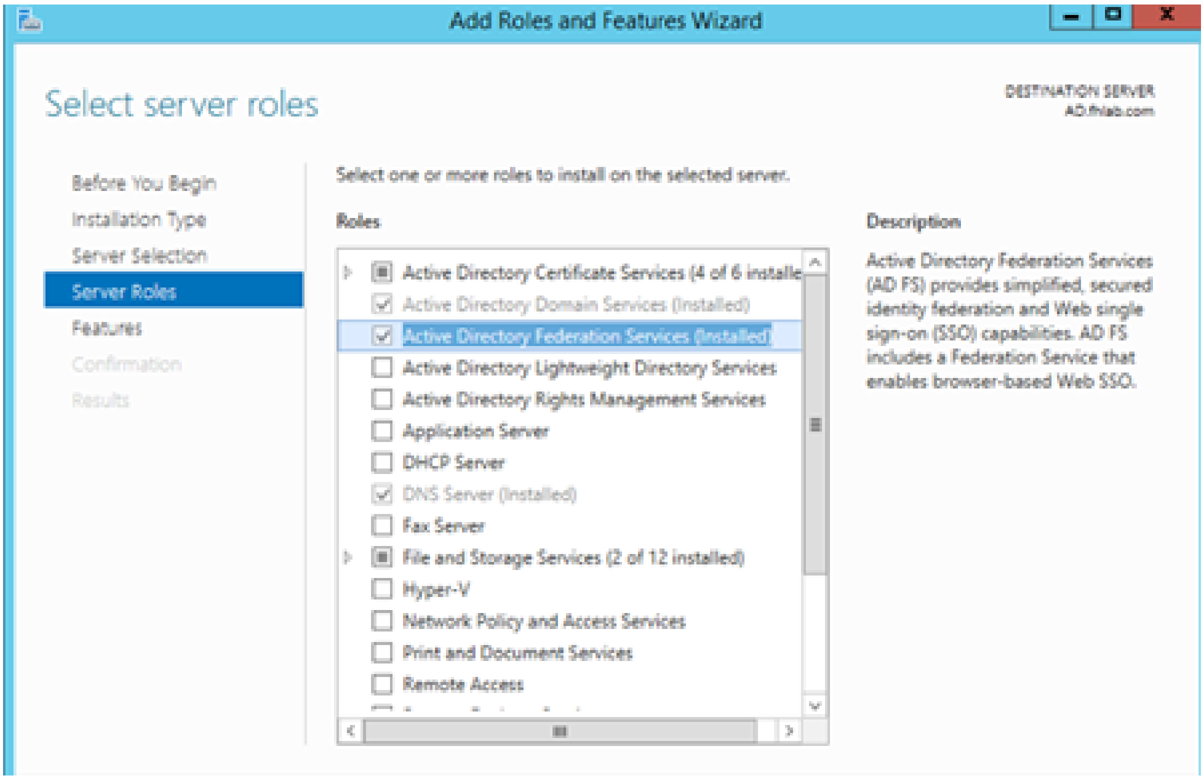
| Type | Host Name | Port | IP Address | Binding Informa... |
|---|---|---|---|---|
| http | | 80 | * | |
| https | | 443 | * | |

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

Todos los roles previos se instalan en el entorno, por lo que ahora puede continuar con la instalación de ADFS3 Active Directory Federation Services (en Windows Server 2012).

Para la función de servidor, navegue hasta **Administrador de servidores > Administrar > Agregar funciones y características de servidor** y luego seleccione **Servicios de federación de directorios activos** si instala el IDP dentro de la red del cliente, en la LAN privada.





Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
AD.fhlab.com

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

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

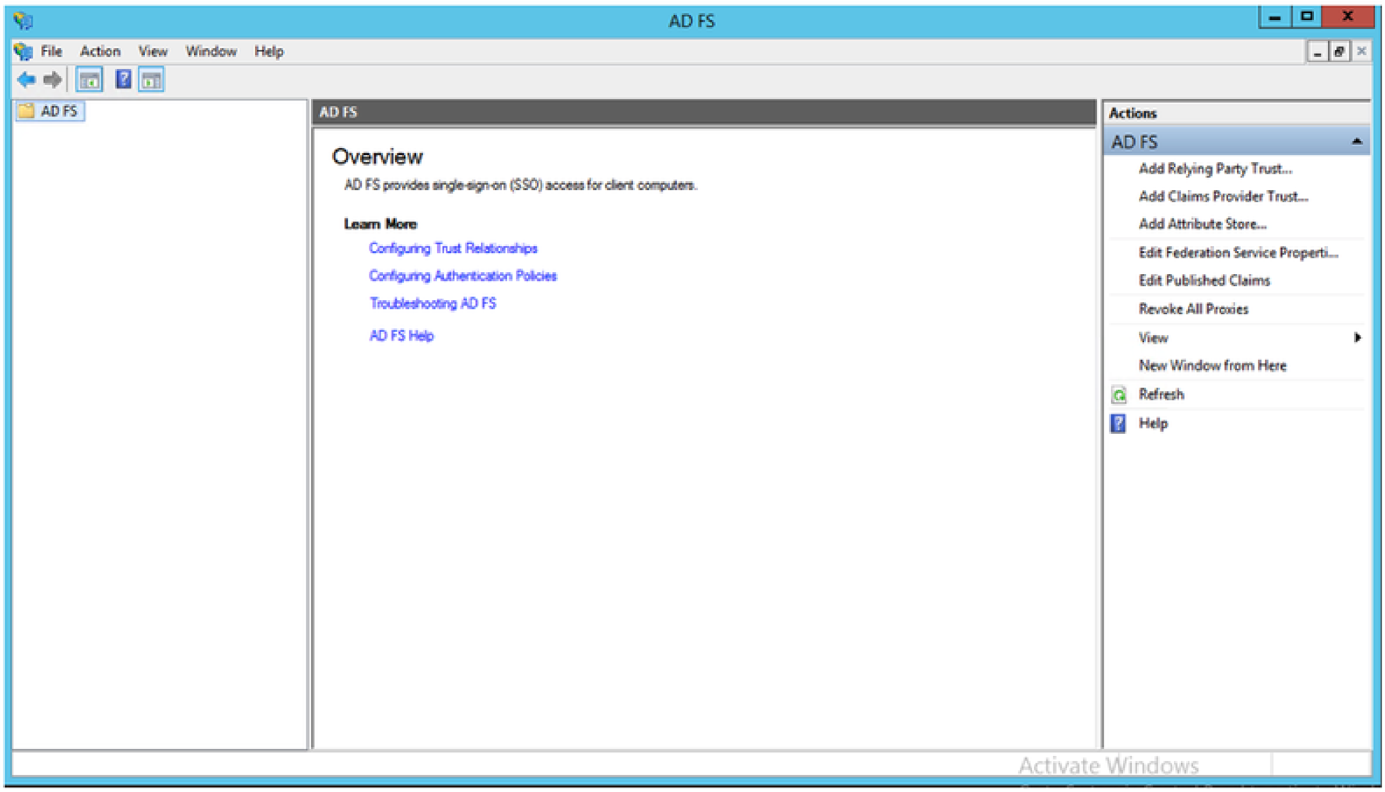
Roles

- ▣ 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.

Una vez finalizada la instalación, puede abrirla desde la barra de tareas o desde el menú de inicio.



AD FS

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

Actions

AD FS

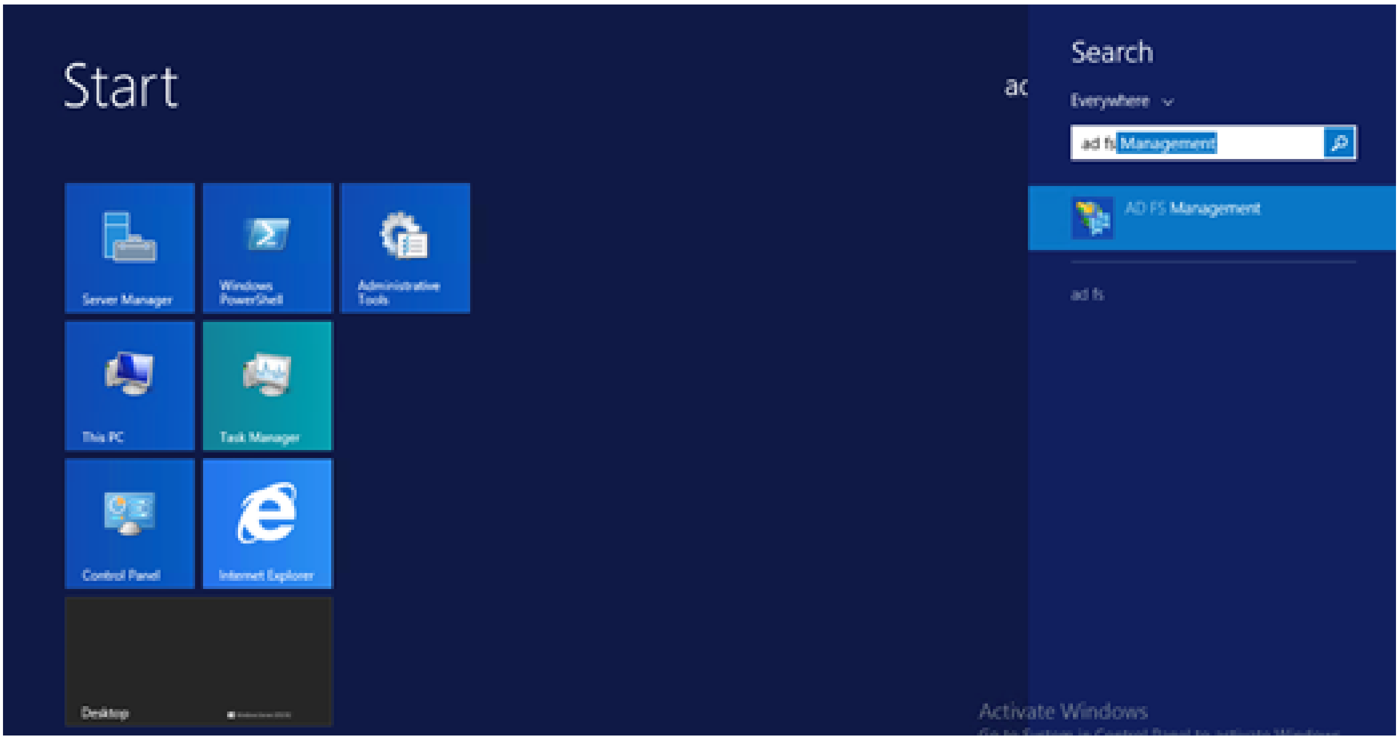
- Add Relying Party Trust...
- Add Claims Provider Trust...
- Add Attribute Store...
- Edit Federation Service Properti...
- Edit Published Claims
- Revoke All Proxies
- View
- New Window from Here
- Refresh
- Help

Activate Windows

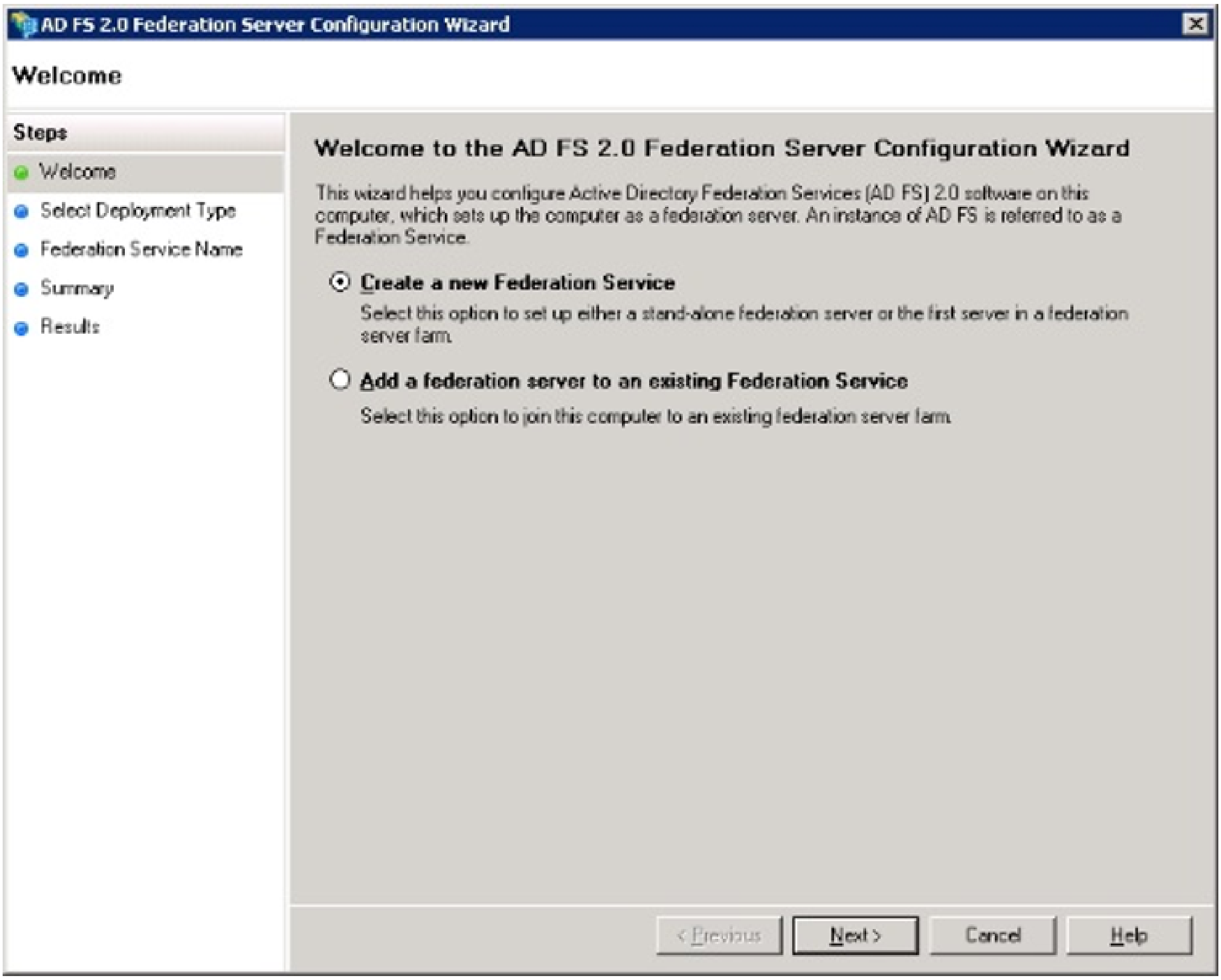
# Configuración inicial de ADFS3

Esta sección atravesará la instalación de un nuevo servidor de federación independiente, pero también se puede utilizar para instalarlo en un controlador de dominio

Seleccione **Windows** y escriba **AD FS Management** para iniciar la consola de administración de ADFS como se muestra en la imagen.



Seleccione la opción **Asistente de configuración del servidor de federación AD FS 3.0** para iniciar la configuración del servidor ADFS. Estas capturas de pantalla representan los mismos pasos en AD FS 3.


AD FS 2.0 Federation Server Configuration Wizard

Welcome

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

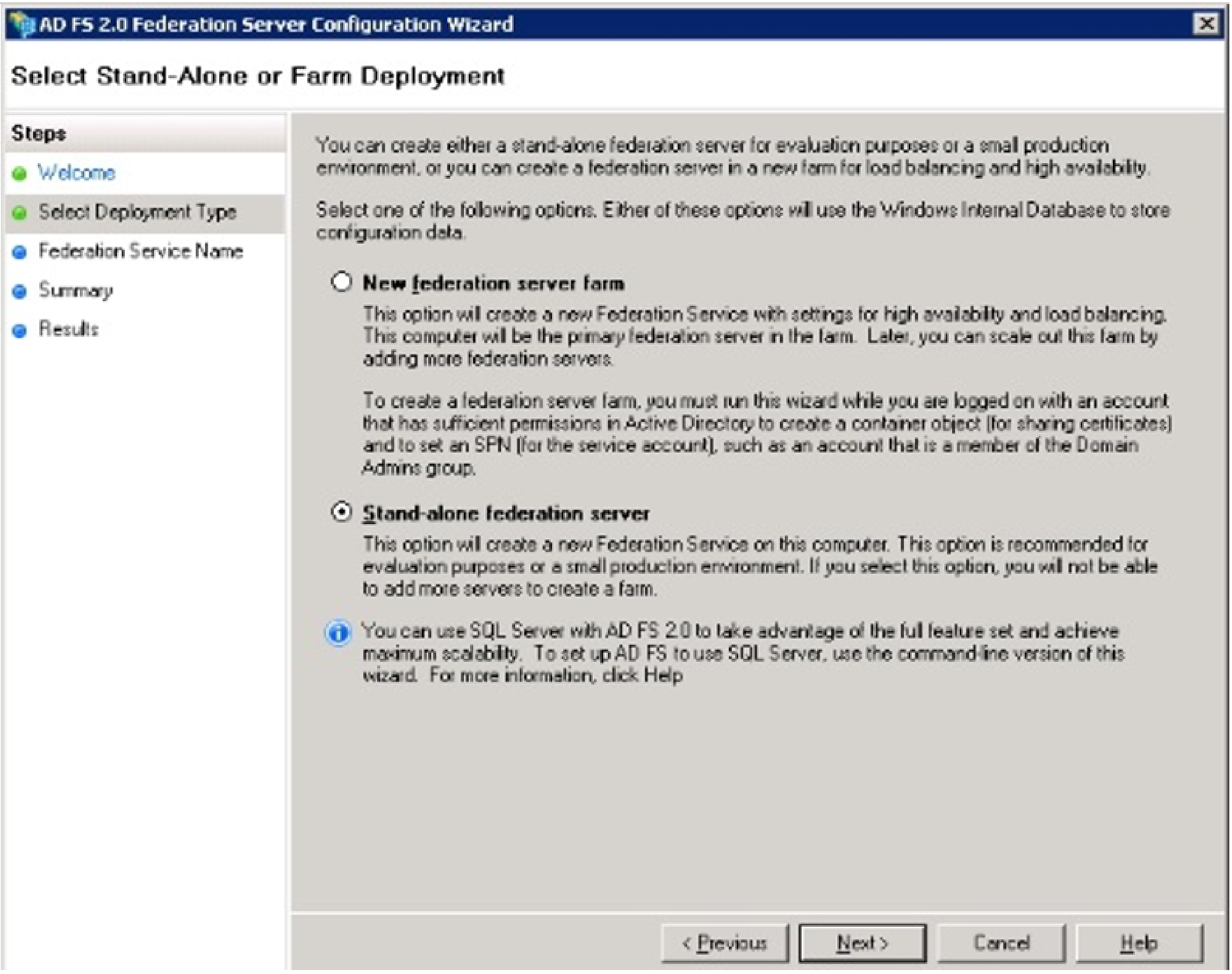
Welcome to the AD FS 2.0 Federation Server Configuration Wizard

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.

Seleccione Create a new **Federation Service** y haga clic en **Next**.



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.

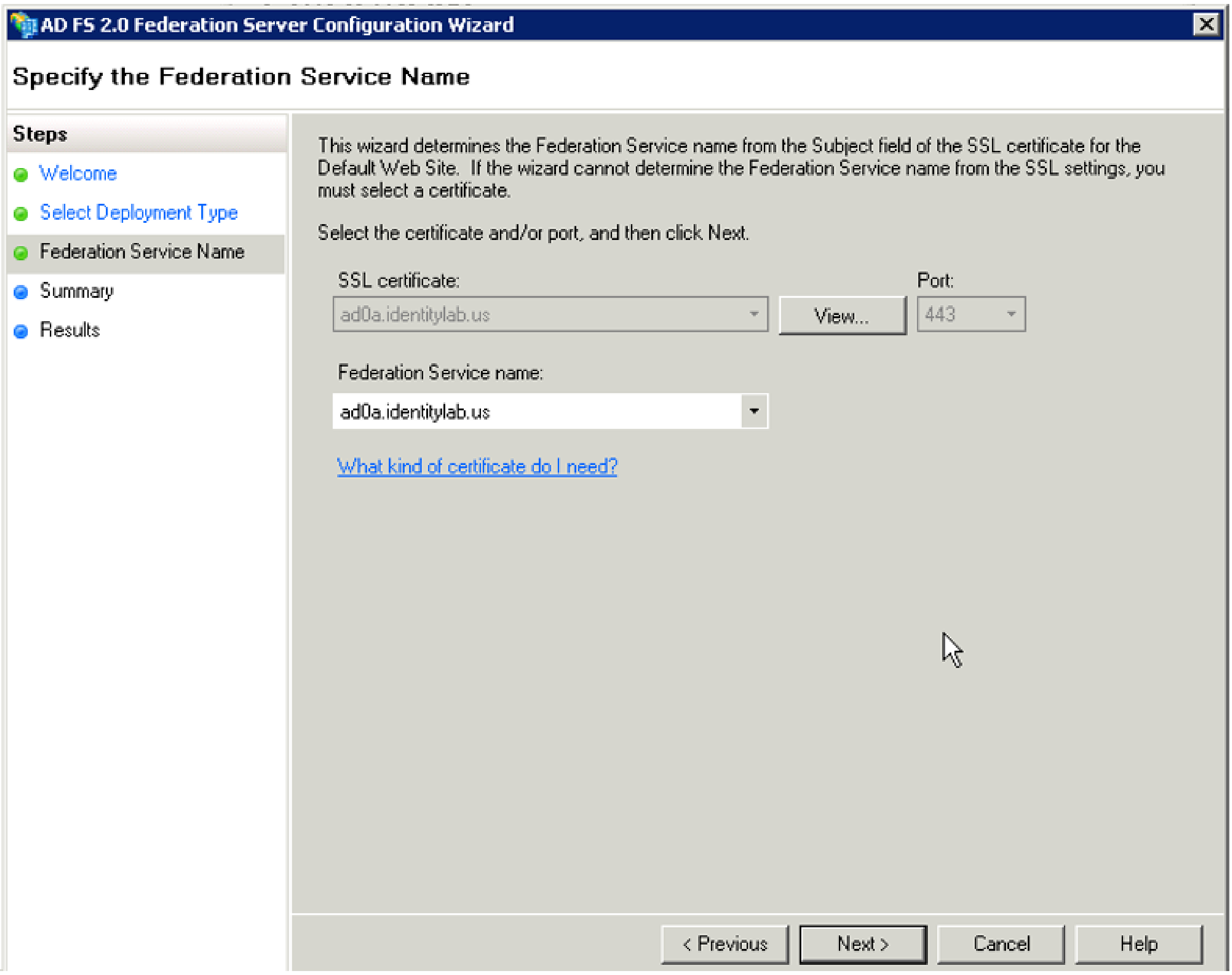
To create a federation server farm, you must run this wizard while you are logged on with an account that has sufficient permissions in Active Directory to create a container object (for sharing certificates) and to set an SPN (for the service account), such as an account that is a member of the Domain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

Seleccione Servidor de federación independiente y haga clic en **Siguiente** como se muestra en la imagen.



AD FS 2.0 Federation Server Configuration Wizard

Specify the Federation Service Name

Steps

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

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.

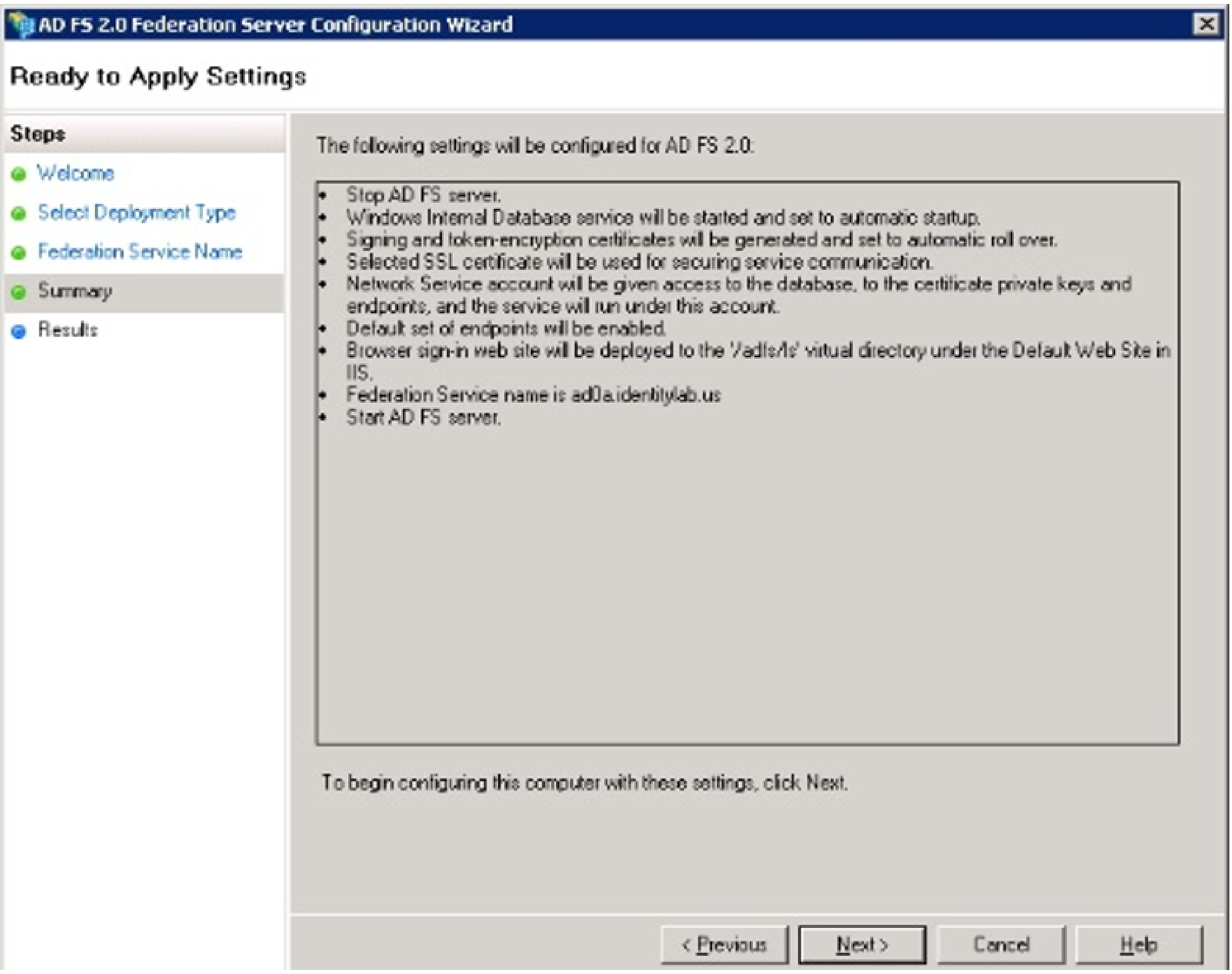
Select the certificate and/or port, and then click Next.

SSL certificate: ad0a.identitylab.us

Port: 443

Federation Service name: ad0a.identitylab.us

En el certificado SSL, seleccione el certificado autofirmado de la lista. El nombre del servicio de federación se rellenará automáticamente. Haga clic en Next (Siguiente).

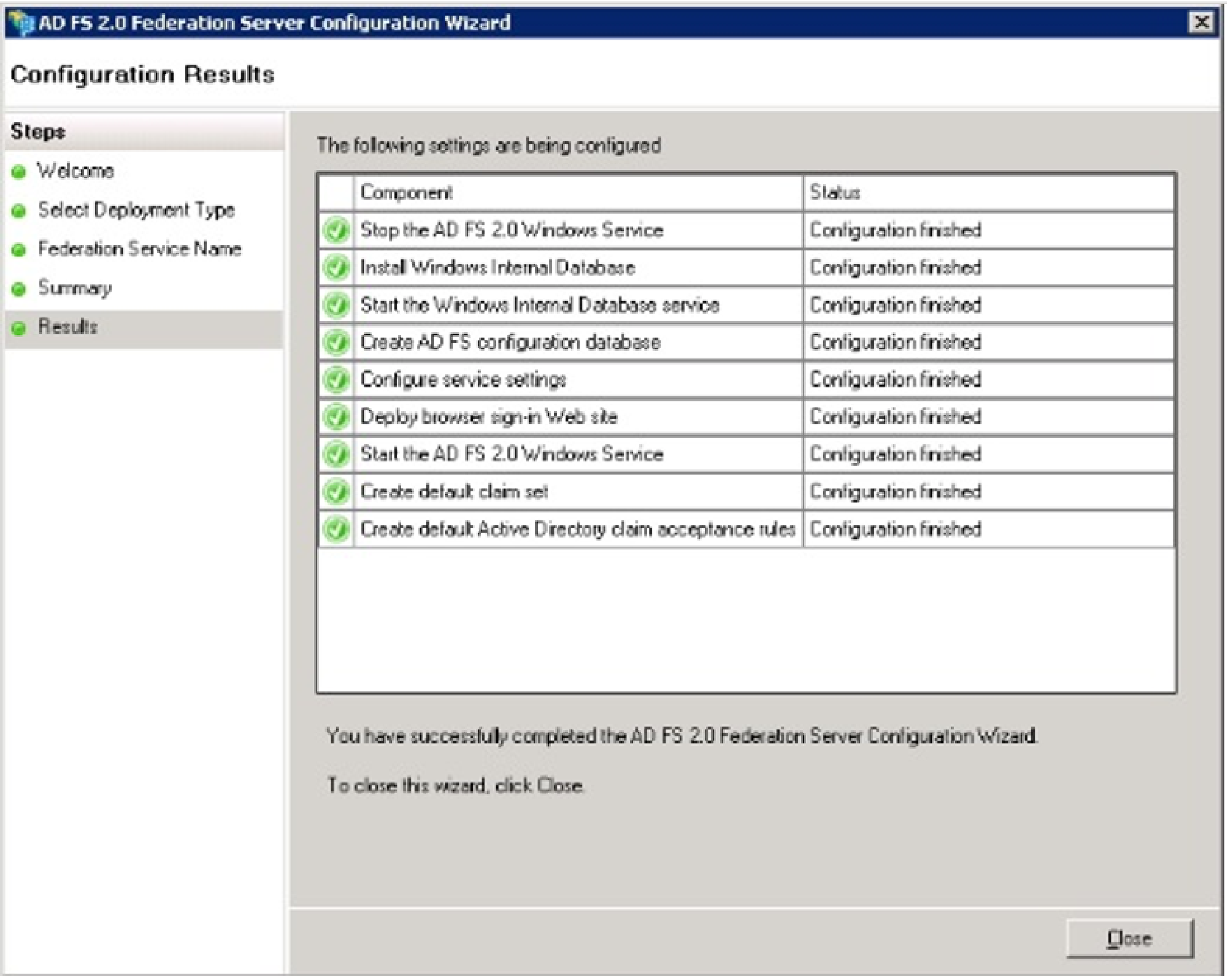


The following settings will be configured for AD FS 2.0:

- 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.

Revise la configuración y haga clic en **Siguiente** para aplicar la configuración.



AD FS 2.0 Federation Server Configuration Wizard

Configuration Results

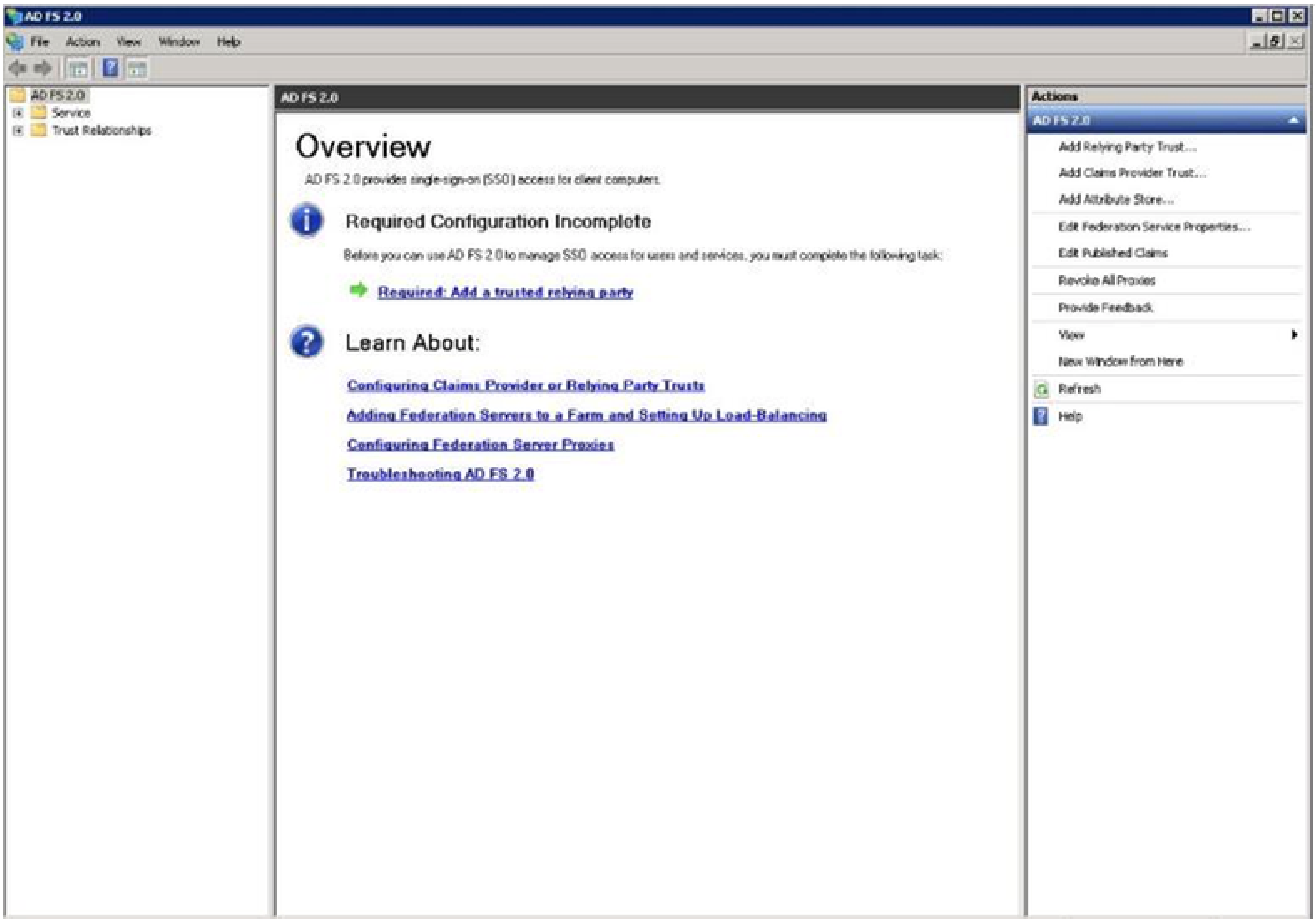
The following settings are being configured

| | 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.

Confirme que todos los componentes se han completado correctamente y haga clic en **Cerrar** para finalizar el asistente y volver a la consola de administración principal. Esto puede tardar unos minutos.



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

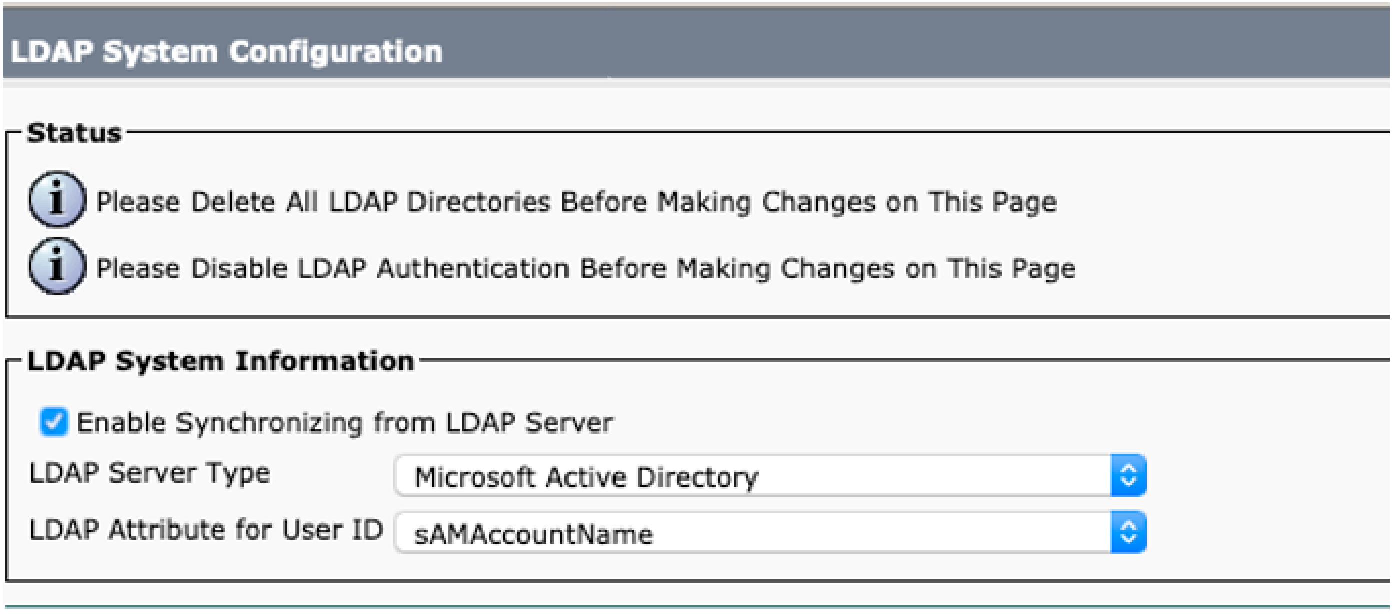
Troubleshooting AD FS 2.0

Ahora, ADFS está habilitado y configurado como proveedor de identidad (IdP). A continuación, debe agregar CUCM como partner de confianza. Antes de poder hacer esto, primero debe realizar alguna configuración en CUCM Administration.

# Configuración de SSO en CUCM con ADFS

## Configuración LDAP

El clúster debe estar integrado LDAP con Active Directory y la autenticación LDAP debe configurarse antes de continuar. Navegue hasta **la pestaña Sistema > Sistema LDAP** como se muestra en la imagen.



LDAP System Configuration

Status

Please Delete All LDAP Directories Before Making Changes on This Page

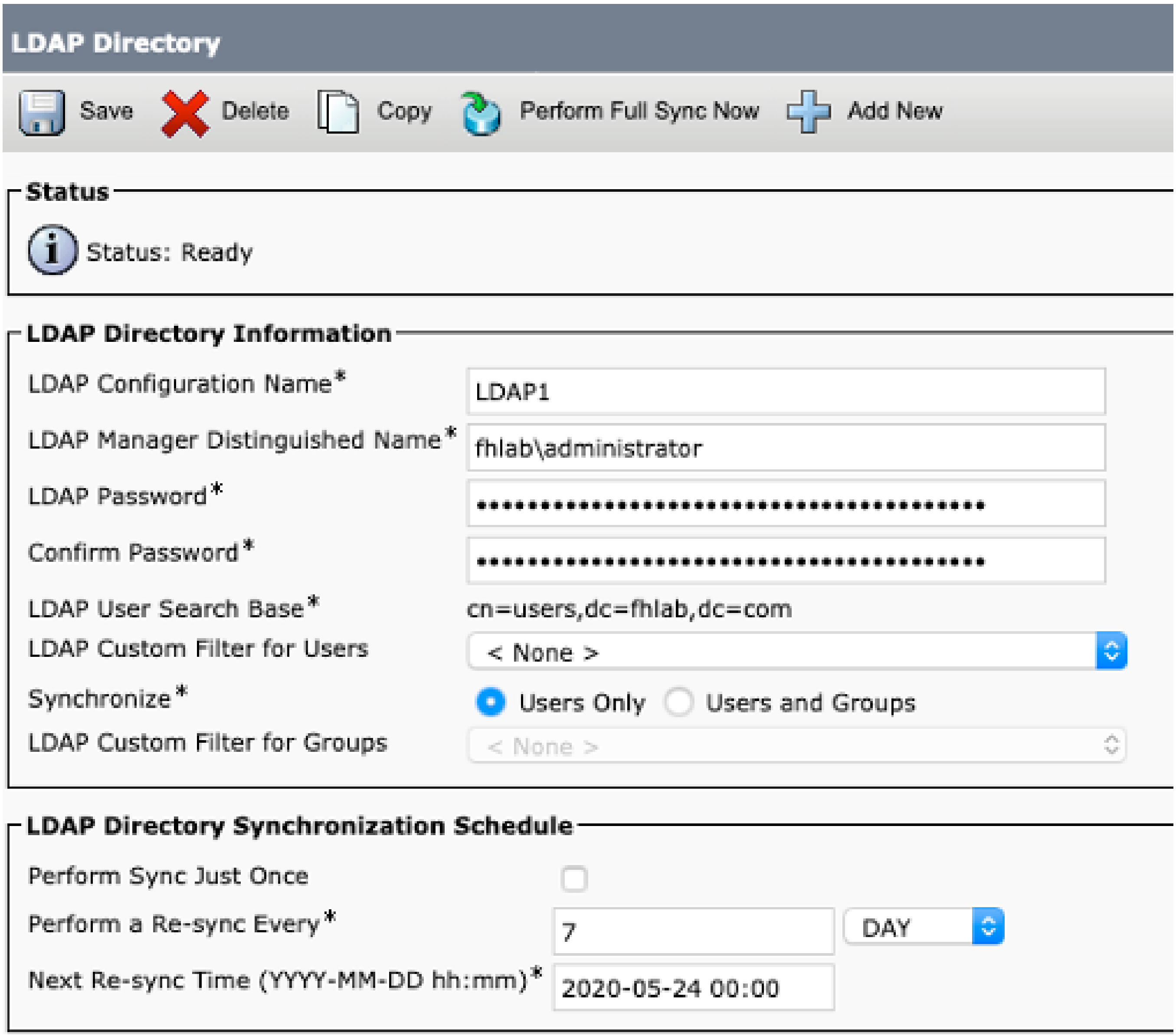
Please Disable LDAP Authentication Before Making Changes on This Page

LDAP System Information

☑ Enable Synchronizing from LDAP Server

|  |  |
|---|---|
| LDAP Server Type | Microsoft Active Directory |
| LDAP Attribute for User ID | sAMAccountName |

A continuación, navegue hasta **ficha Sistema > Directorio LDAP**.



LDAP Directory

Status

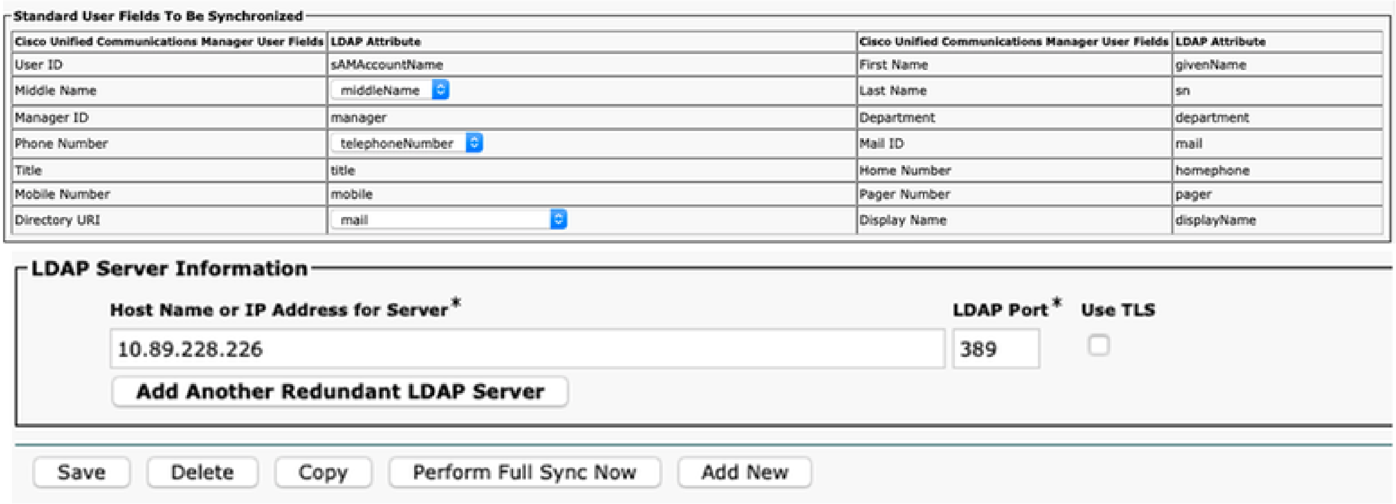
Status: Ready

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 |



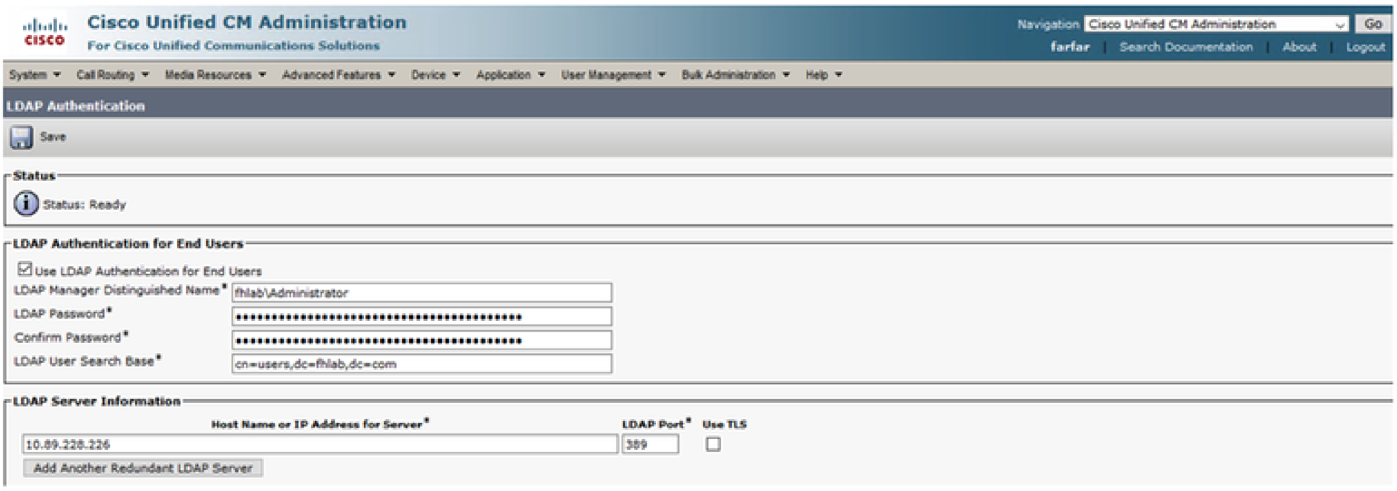
Standard User Fields To Be Synchronized

| 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 | □ |

Una vez que los usuarios de Active Directory se han sincronizado con CUCM, se debe configurar la autenticación LDAP.



Status

Status: Ready

LDAP Authentication for End Users

☑ Use LDAP Authentication for End Users

LDAP Manager Distinguished Name* fhlab\Administrator

LDAP Password* ••••••••••••••••••••••••••••••••••••••••••

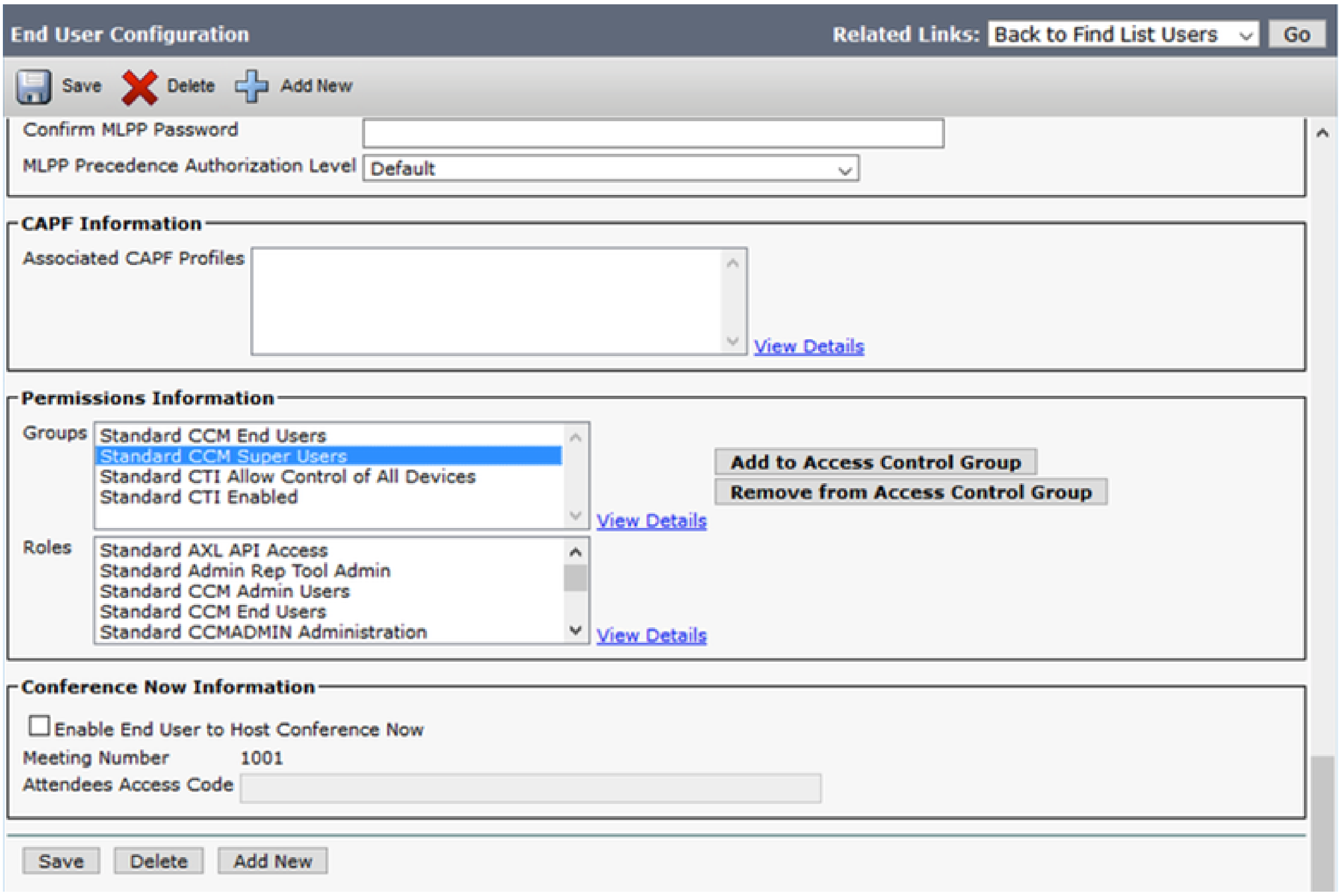
Confirm Password* ••••••••••••••••••••••••••••••••••••••••••

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 | □ |

Un usuario final de CUCM debe tener determinados grupos de control de acceso asignados a su perfil de usuario final. El ACG es superusuarios de CCM estándar. El usuario se utilizará para probar SSO cuando el entorno esté listo.


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

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

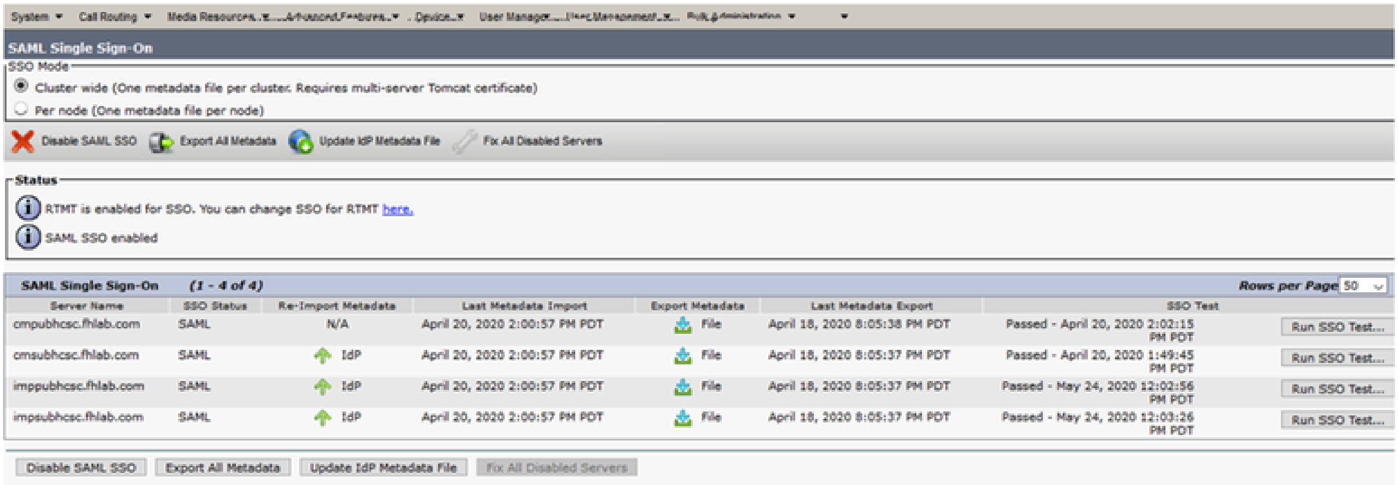
Meeting Number: 1001

Attendees Access Code

## Metadatos de CUCM

En esta sección se muestra el proceso del editor de CUCM.

La primera tarea es obtener los metadatos de CUCM, para lo cual debe buscar la URL; **https://<CUCM Pub FQDN>:8443/ssosp/ws/config/metadatos/sp** o se puede descargar desde la **ficha System > SAML Single Sign-on**. Esto se puede hacer por nodo o por clúster. Es preferible hacer esto en todo el clúster.



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

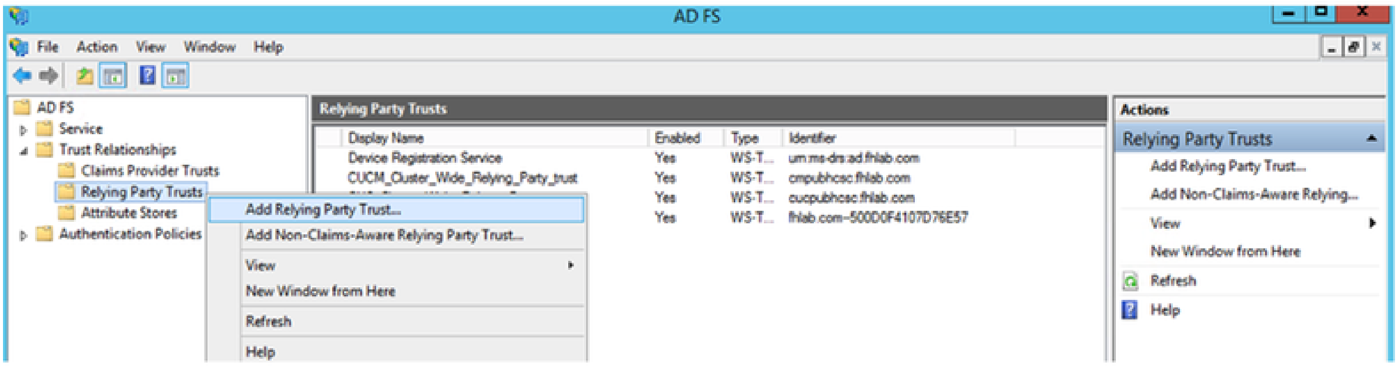
**SAML Single Sign-On** *(1 - 4 of 4)* — *Rows per Page* 50

| 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... |

Guarde los datos localmente con un nombre significativo como sp_cucm0a.xml, lo necesitará después.

## Configuración de la persona que confía en ADFS

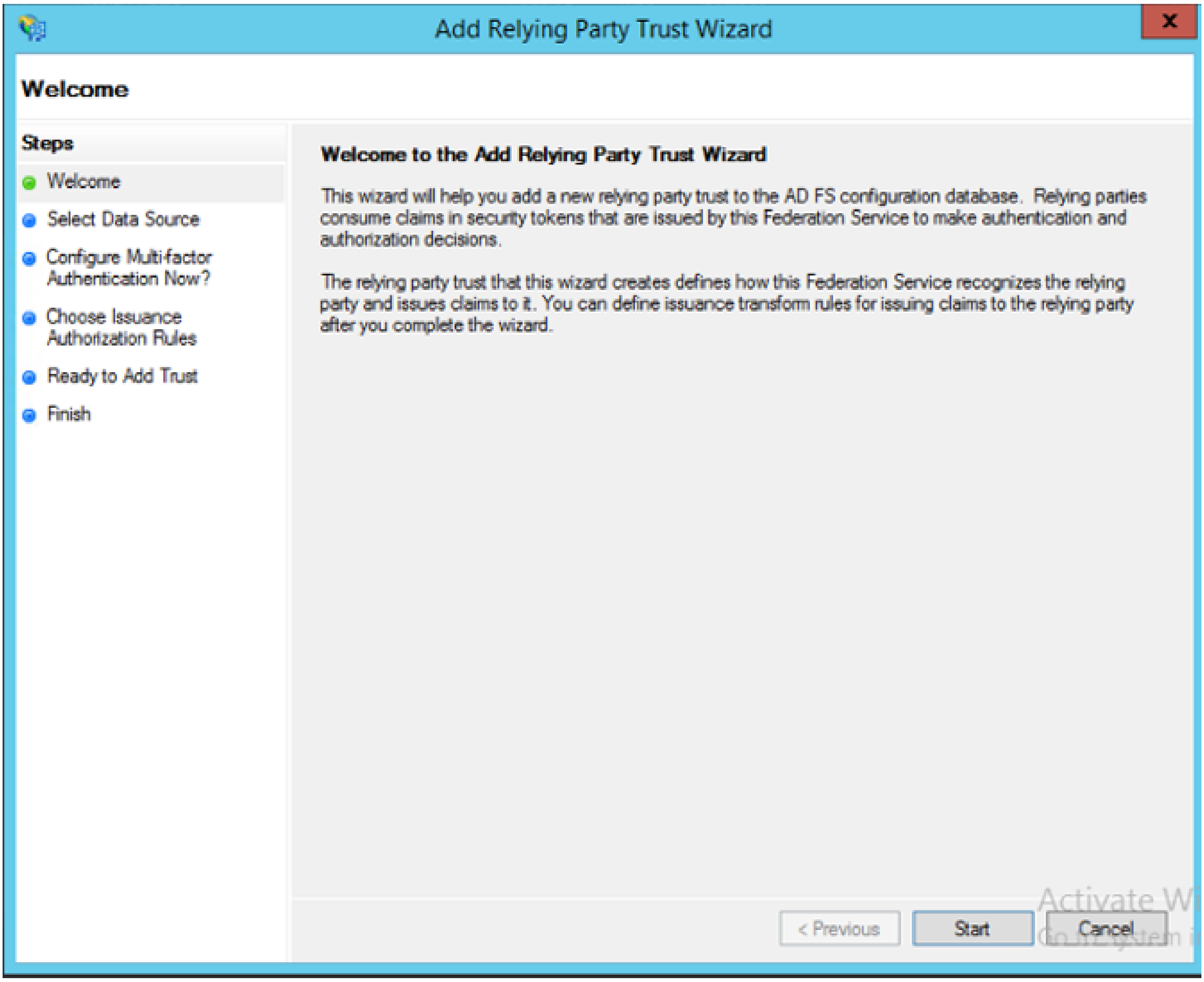
Vuelva a la consola de administración de AD FS 3.0.



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 |
|  | Yes | WS-T... | cucpubhcsc.fhlab.com |
|  | Yes | WS-T... | fhlab.com-500D0F4107D76E57 |

Haga clic en el **Asistente para agregar confianza de terceros**.


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

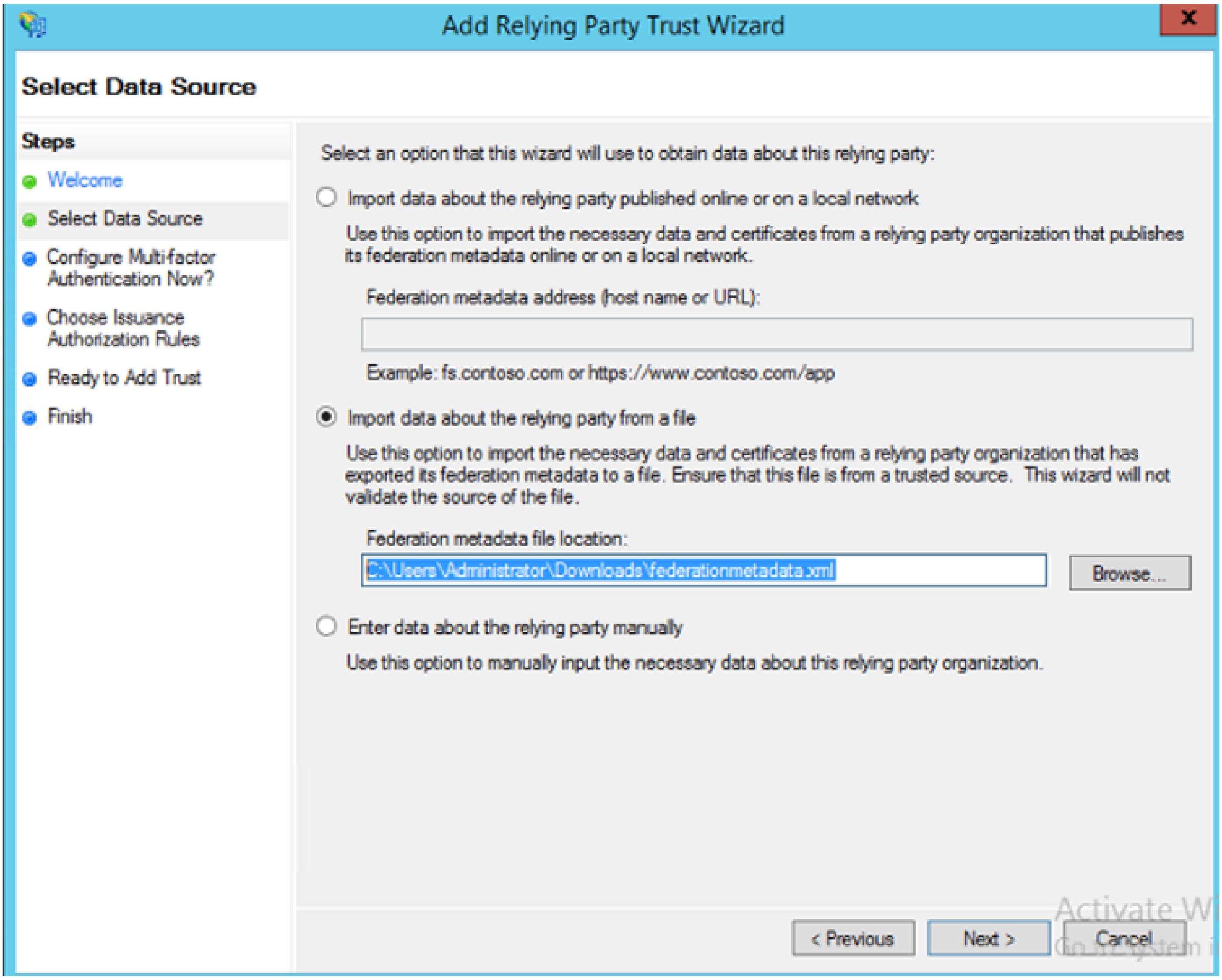
Welcome to the Add Relying Party Trust Wizard

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.

Haga clic en **Inicio** para continuar.

Seleccione el archivo XML de metadatos **federationmedatada.xml** que guardó anteriormente y haga clic en **Siguiente**.



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.

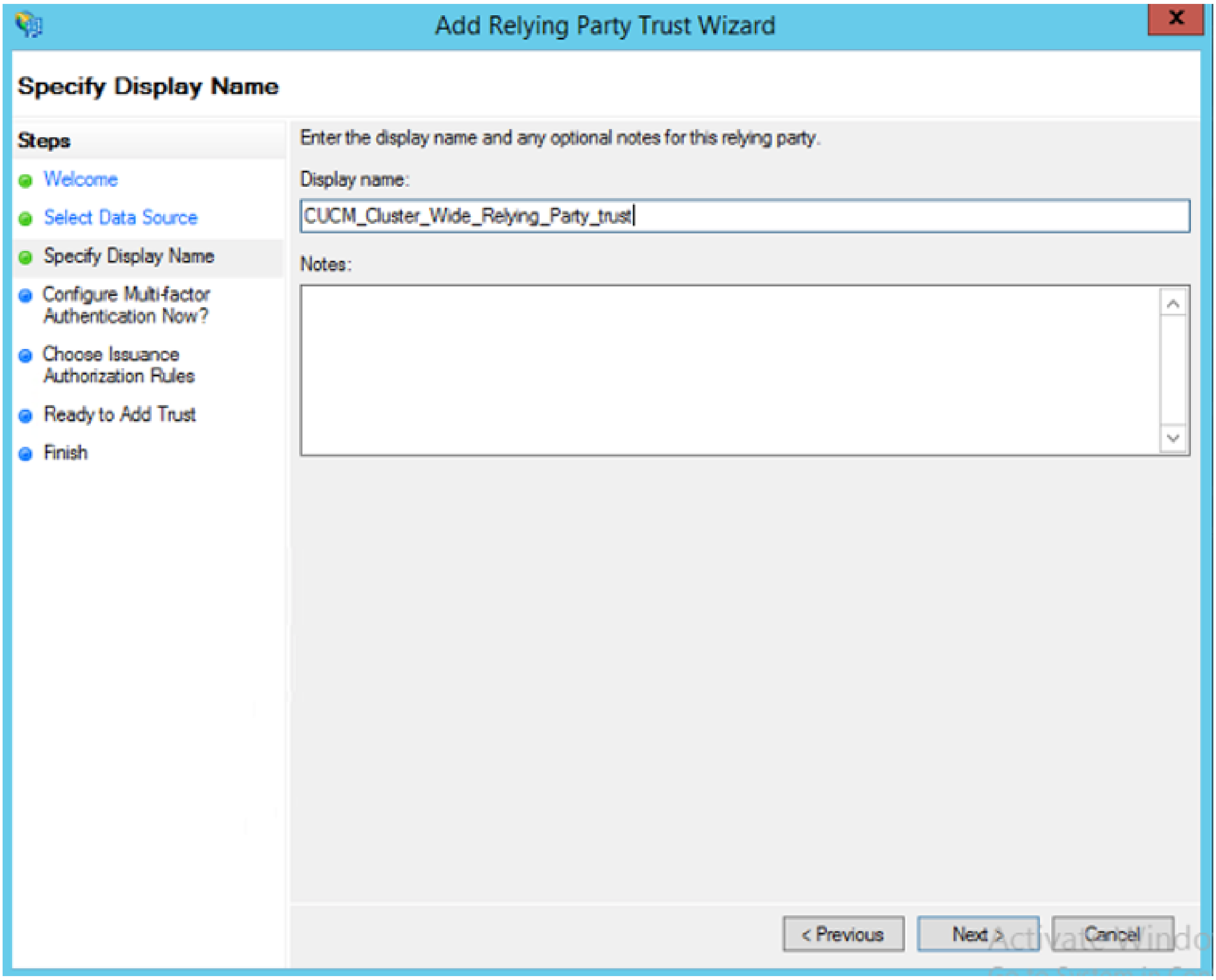
Federation metadata file location:

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.

Utilice **CUCM_Cluster_Wide_Relying_Party_trust** como nombre para mostrar y haga clic en **Siguiente**.



Add Relying Party Trust Wizard

Specify Display Name

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

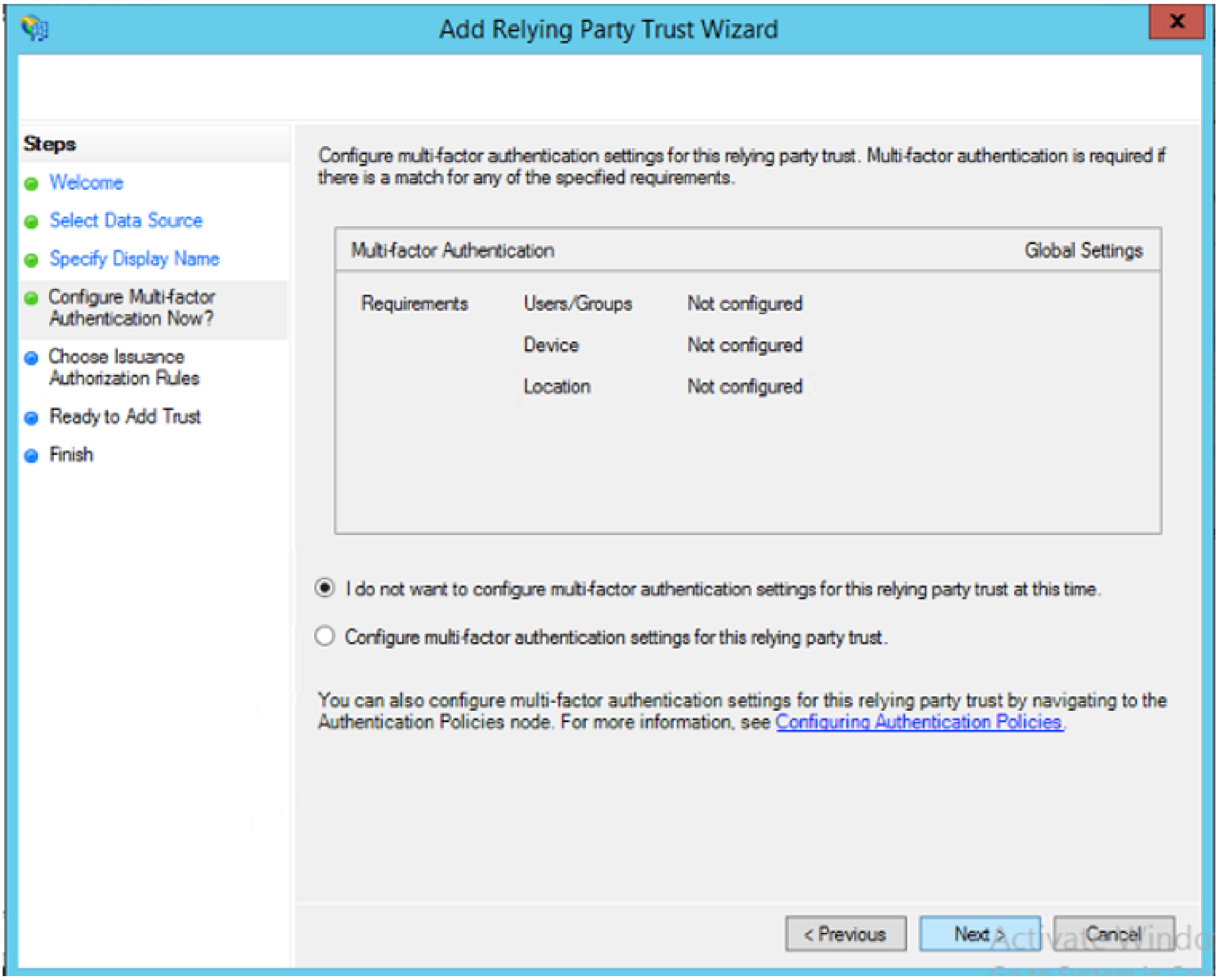
Enter the display name and any optional notes for this relying party.

Display name:

CUCM_Cluster_Wide_Relying_Party_trust

Notes:

Seleccione la primera opción y haga clic en **Siguiente**.



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.

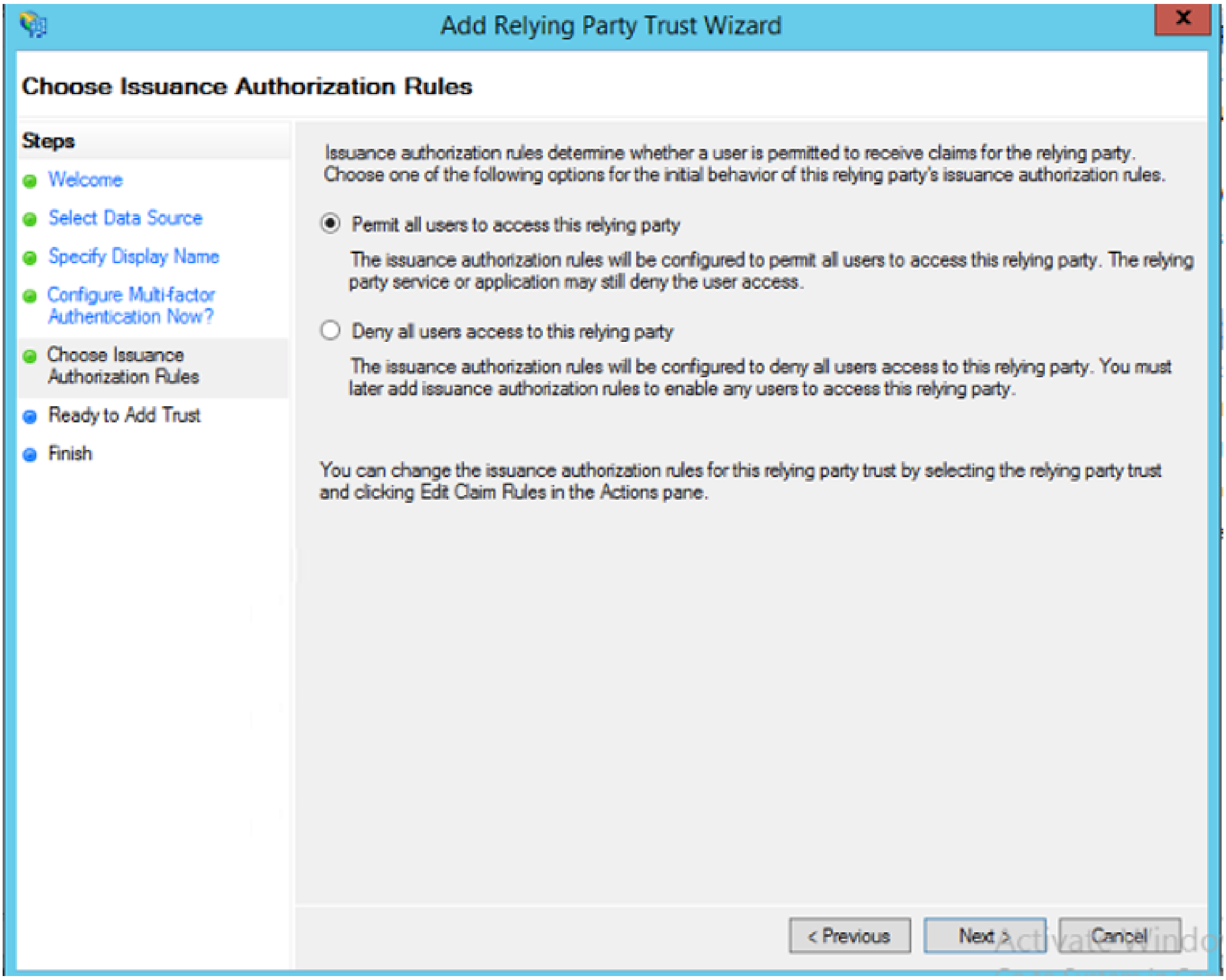
| Multi-factor Authentication | | Global Settings |
|---|---|---|
| Requirements | Users/Groups | Not configured |
| | Device | Not configured |
| | Location | Not configured |

● 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.

Seleccione **Permitir que todos los usuarios accedan a esta persona de confianza** y haga clic en **Siguiente** como se muestra en la imagen.



Add Relying Party Trust Wizard

Choose Issuance Authorization Rules

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

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

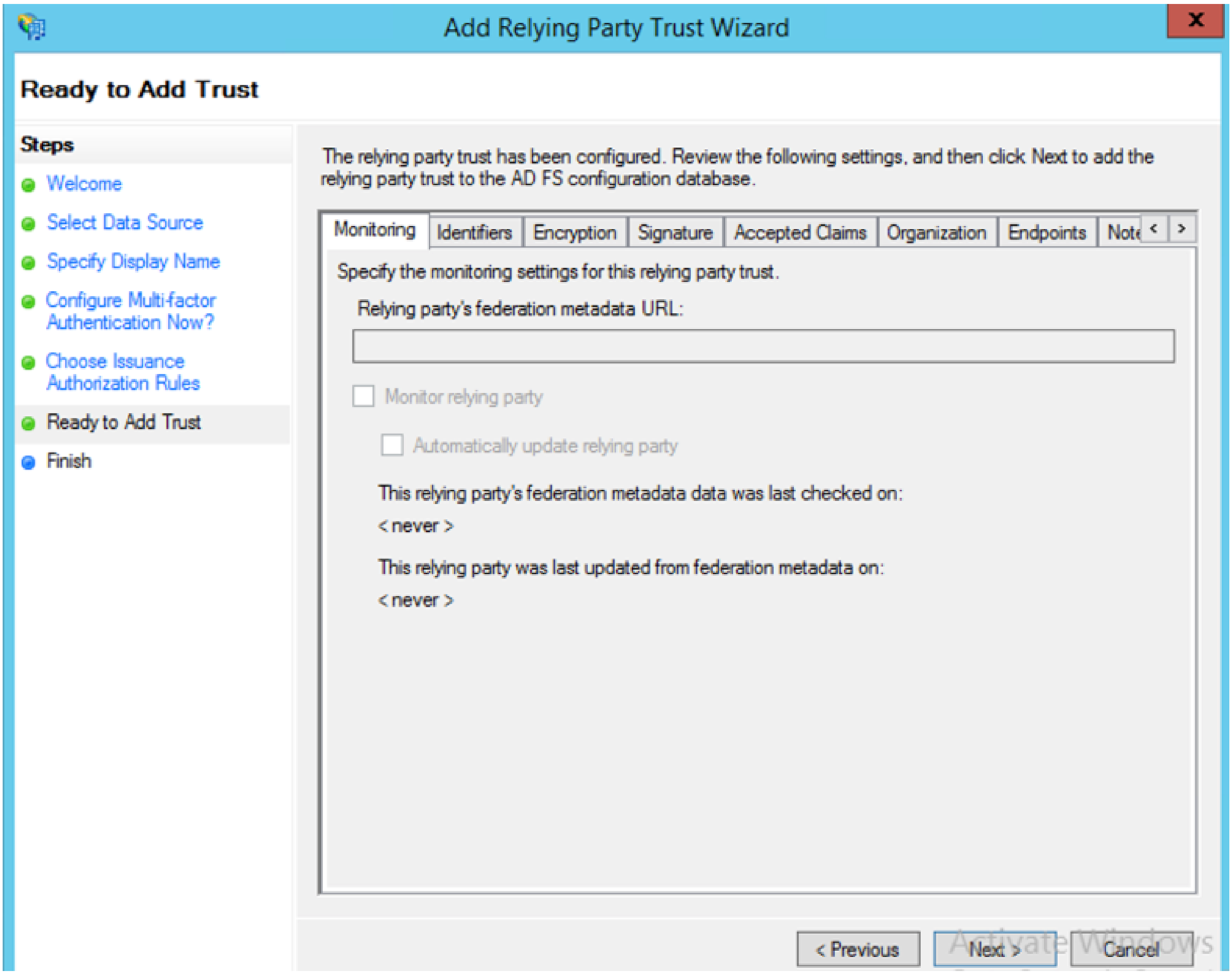
The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ 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.

Revise la configuración y haga clic en **Next** como se muestra en la imagen.



Ready to Add Trust

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

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

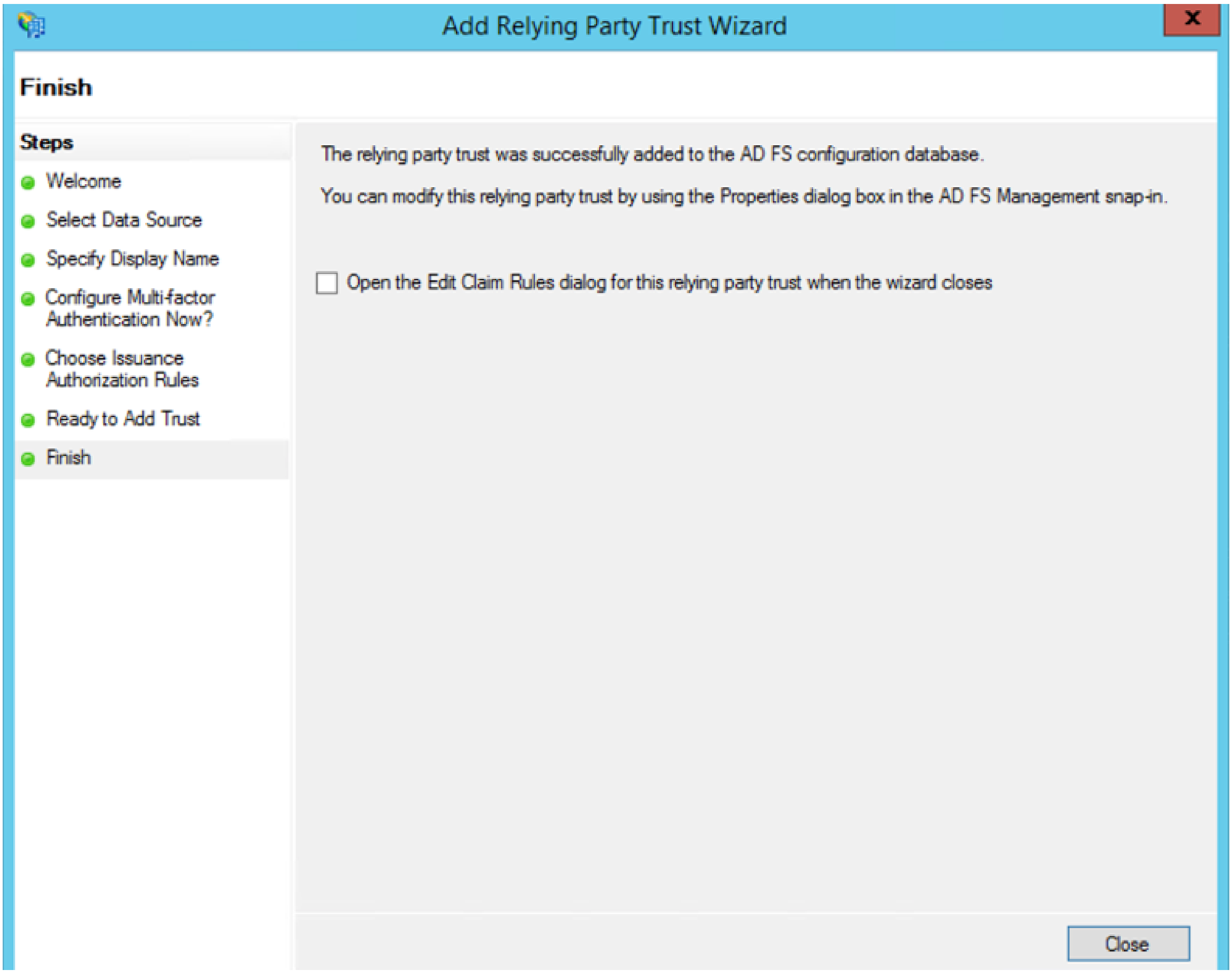
This relying party's federation metadata data was last checked on:

< never >

This relying party was last updated from federation metadata on:

< never >

Desactive la casilla y haga clic en **Cerrar**.

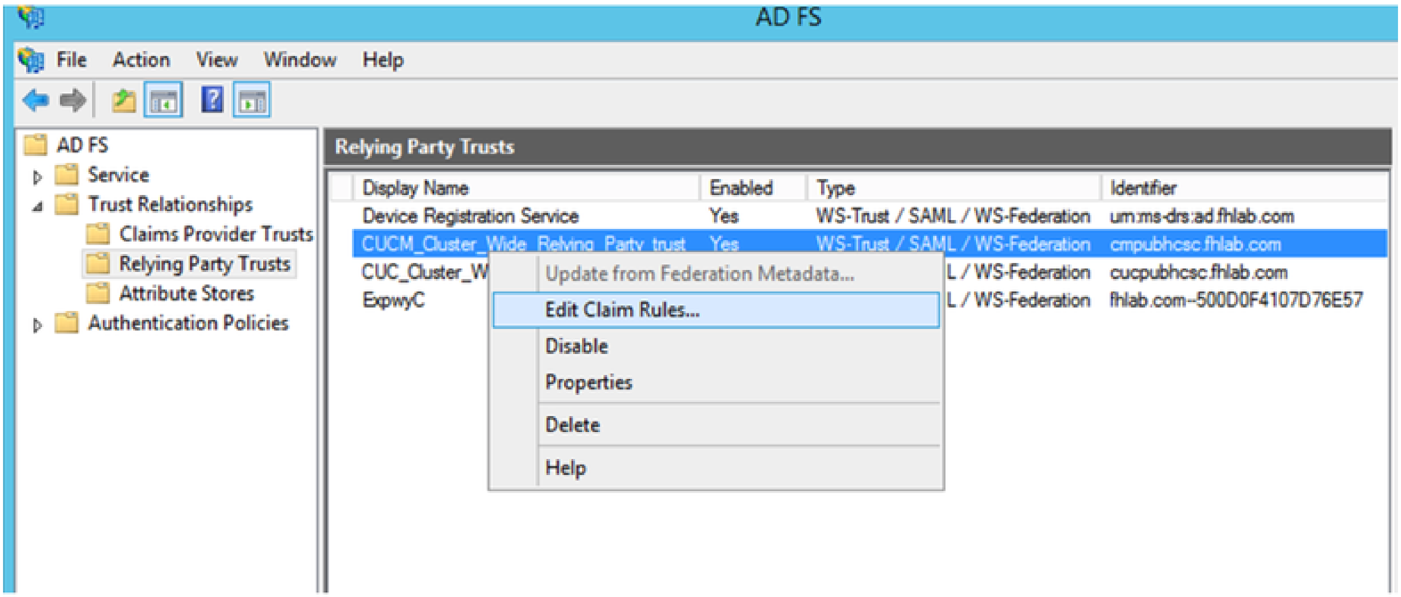

Add Relying Party Trust Wizard
Finish
Steps
Welcome
Select Data Source
Specify Display Name
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Close

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.

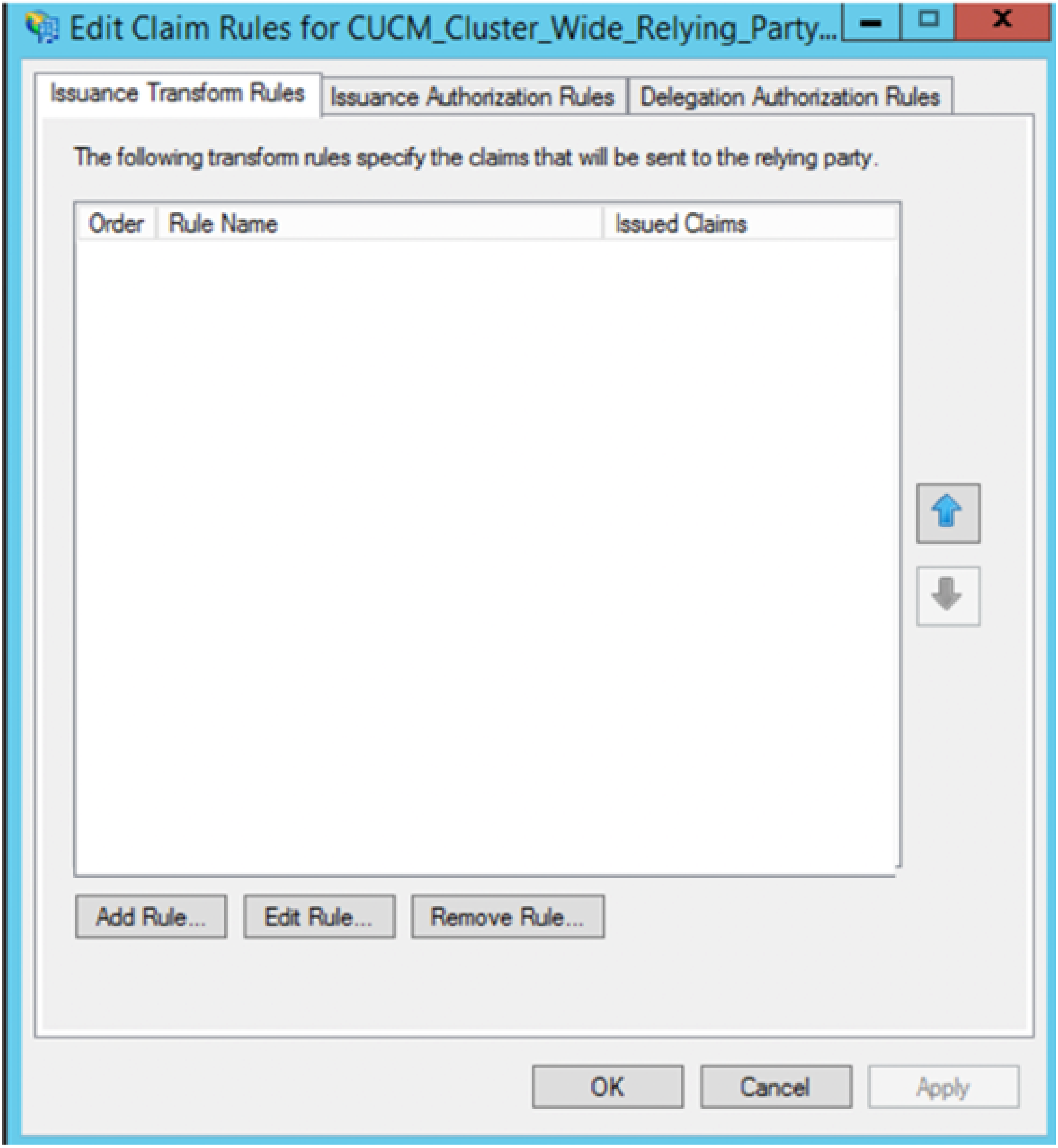
□ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes

Con el botón secundario del ratón, seleccione la configuración **Confianza en el usuario que** acaba de crear y **Editar reglas de reclamación**, como se muestra en la imagen.



| 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 |

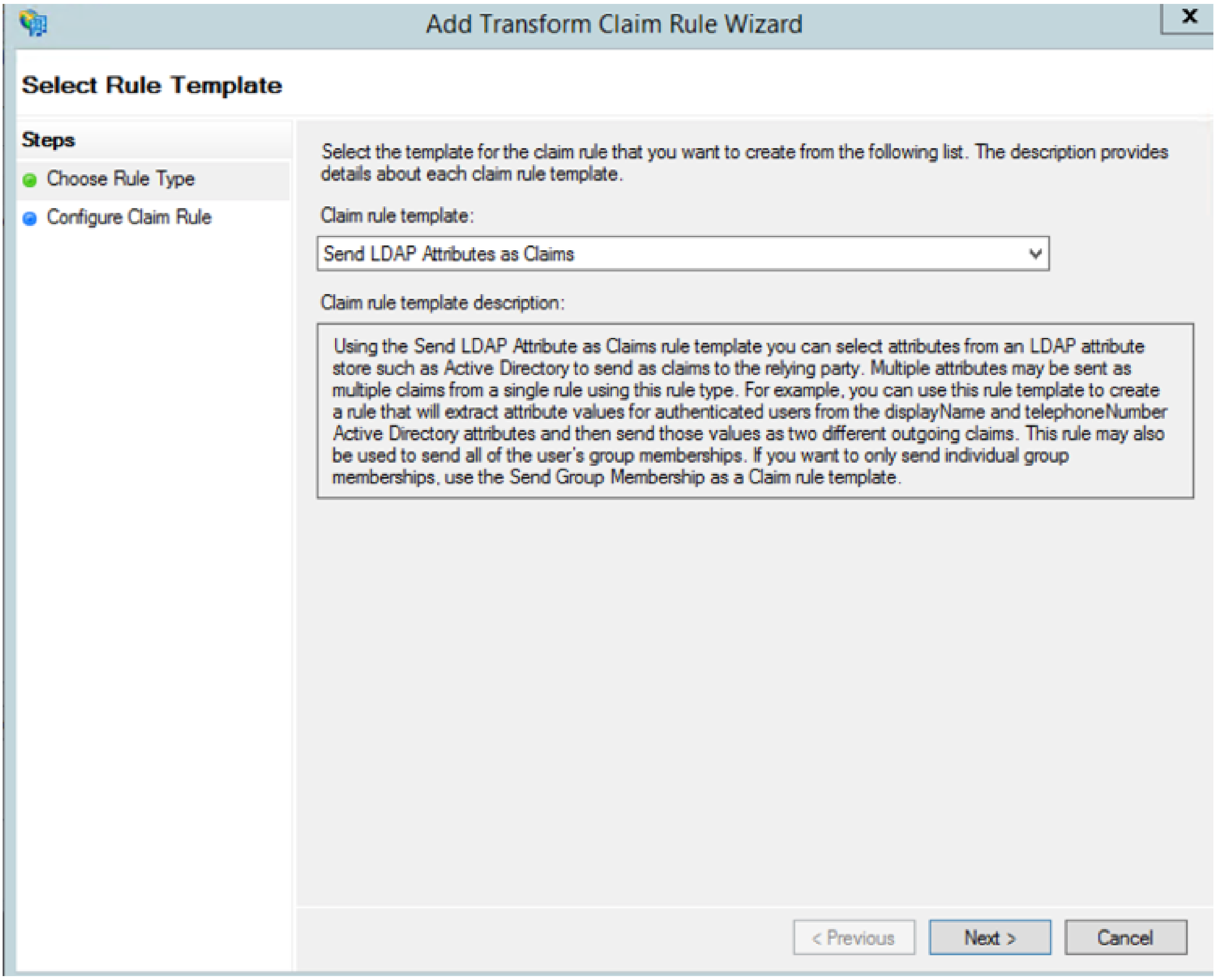
Haga clic en **Agregar regla** como se muestra en la imagen.



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

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

Seleccione **Enviar atributos LDAP como justificantes** y haga clic en **Siguiente**.



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.

Configure estos parámetros:

Nombre de regla de reclamación: ID de nombre

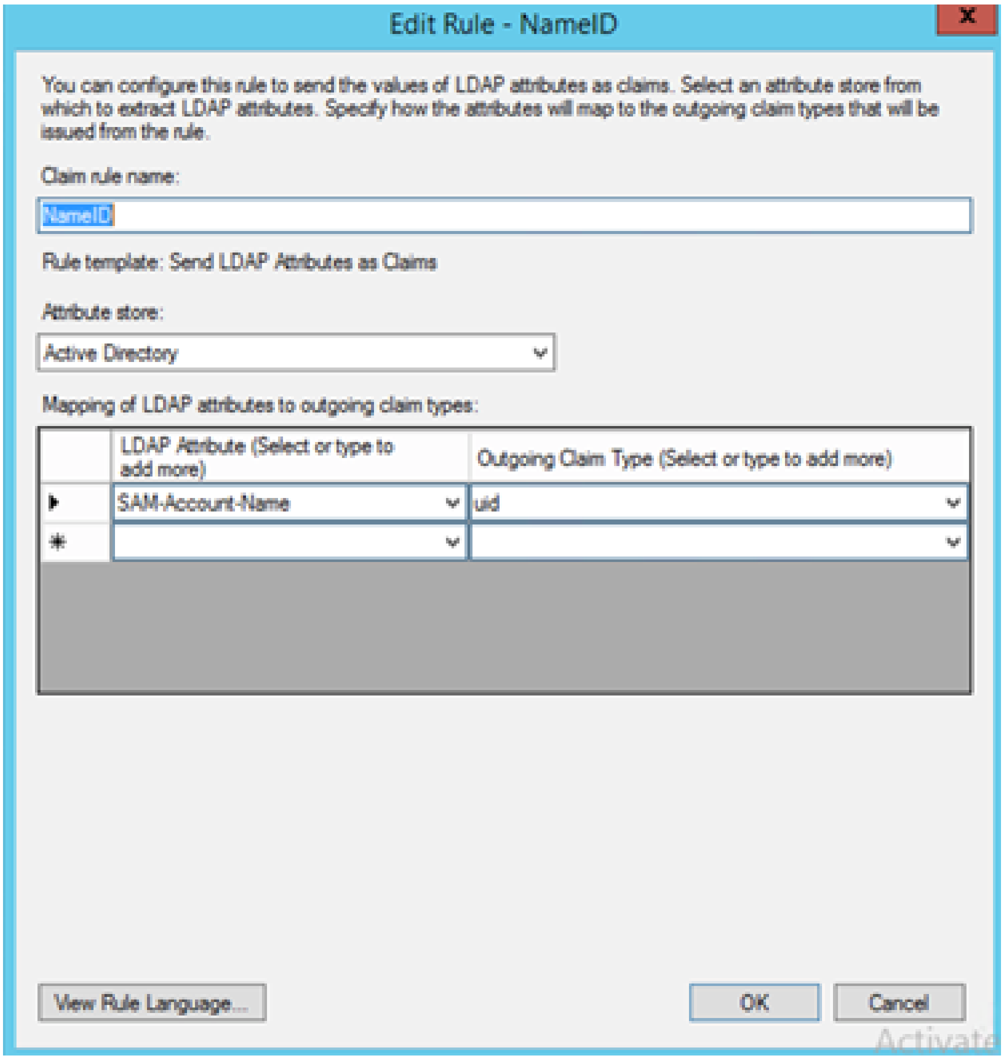
Almacén de atributos: Active Directory (doble clic en la flecha del menú desplegable)

Atributo LDAP: SAM-Account-Name

Tipo de reclamación saliente: uid

Haga clic en **FINISH/OK** para continuar.

Tenga en cuenta que uid no se encuentra en minúsculas y no existe ya en el menú desplegable. Escriba.



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

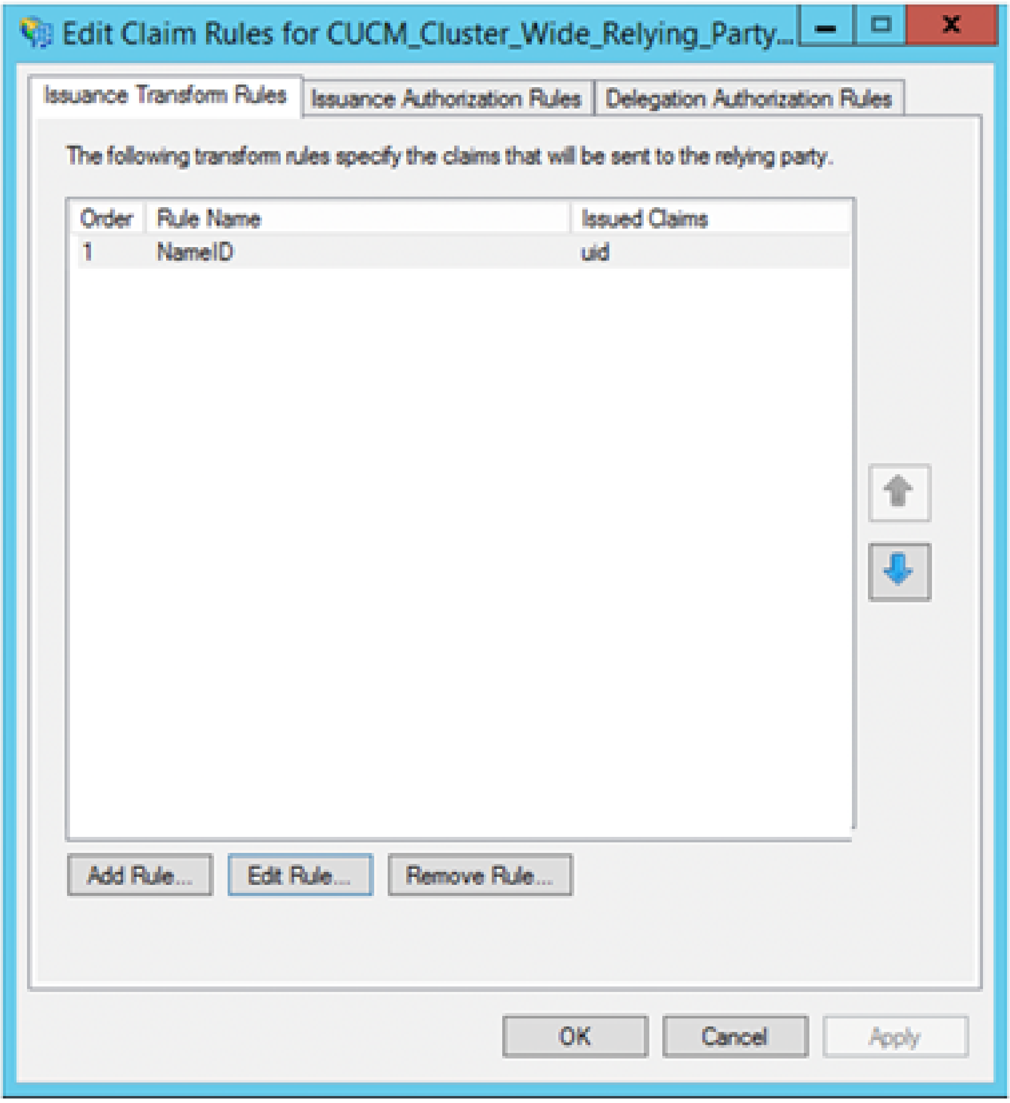
Attribute store:

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 |
| * | | |

Haga clic en **Agregar regla** de nuevo para agregar otra regla.

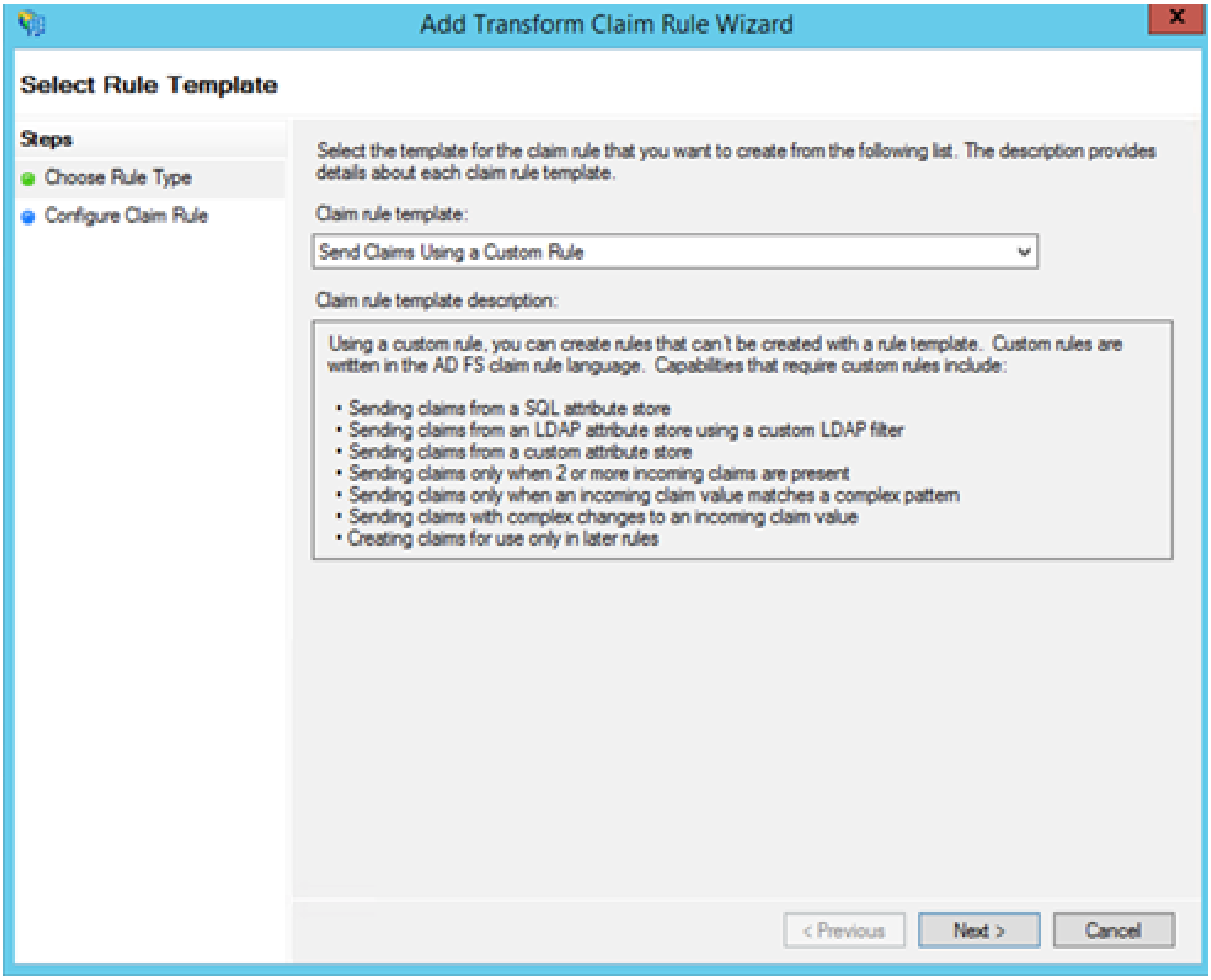

Edit Claim Rules for CUCM_Cluster_Wide_Relying_Party...
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules

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

| Order | Rule Name | Issued Claims |
|---|---|---|
| 1 | NameID | uid |

Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

Seleccione **Enviar justificantes de venta mediante una regla personalizada** y haga clic en **Siguiente**.



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

Cree una regla personalizada llamada Clúster_Side_Claim_Rule.

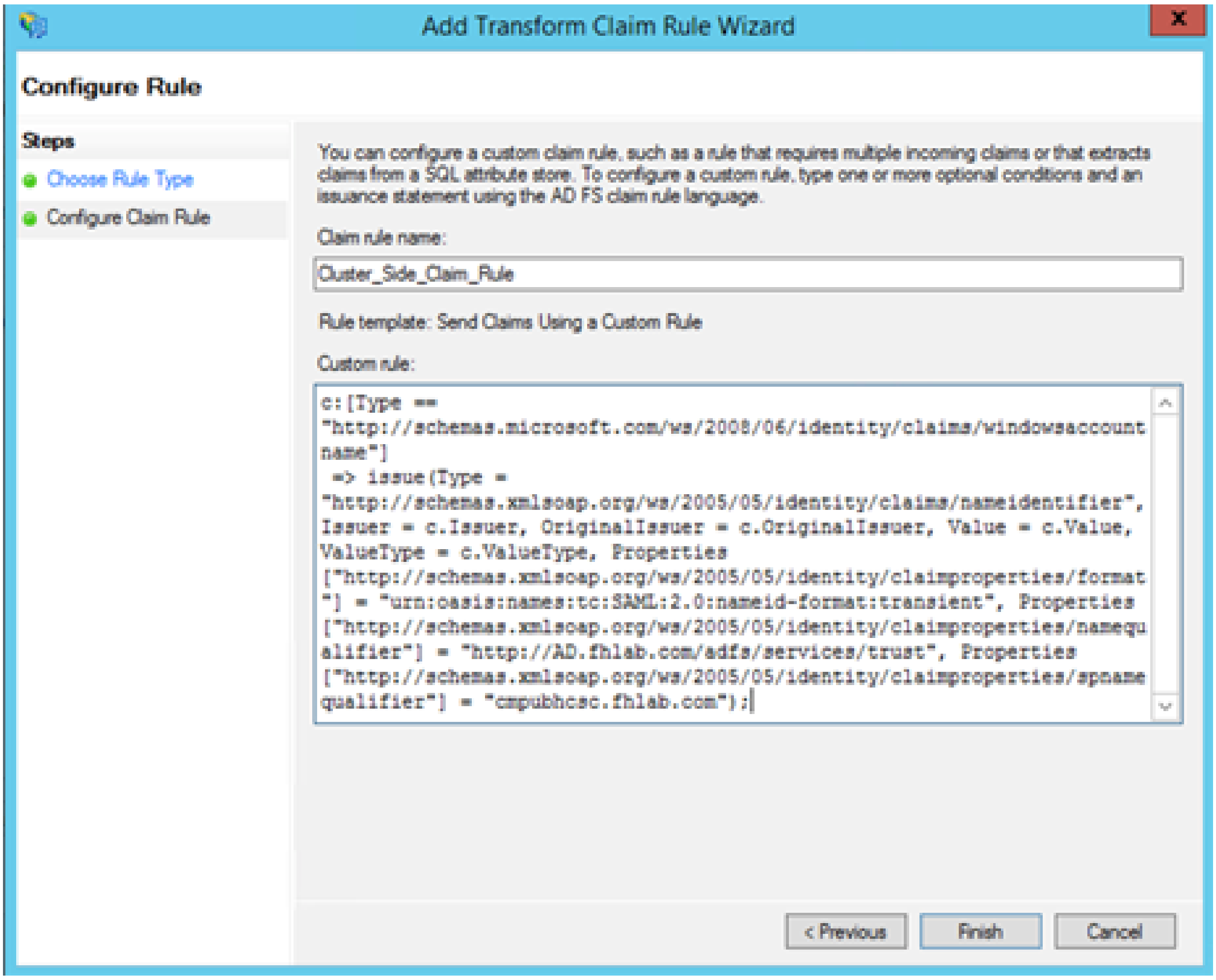
Copie y pegue este texto en la ventana de reglas directamente desde aquí. A veces, los presupuestos se cambian si se editan en un editor de texto y eso hará que la regla falle cuando se prueba SSO:

```
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");
```

Haga clic en **Finalizar** para continuar.



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:

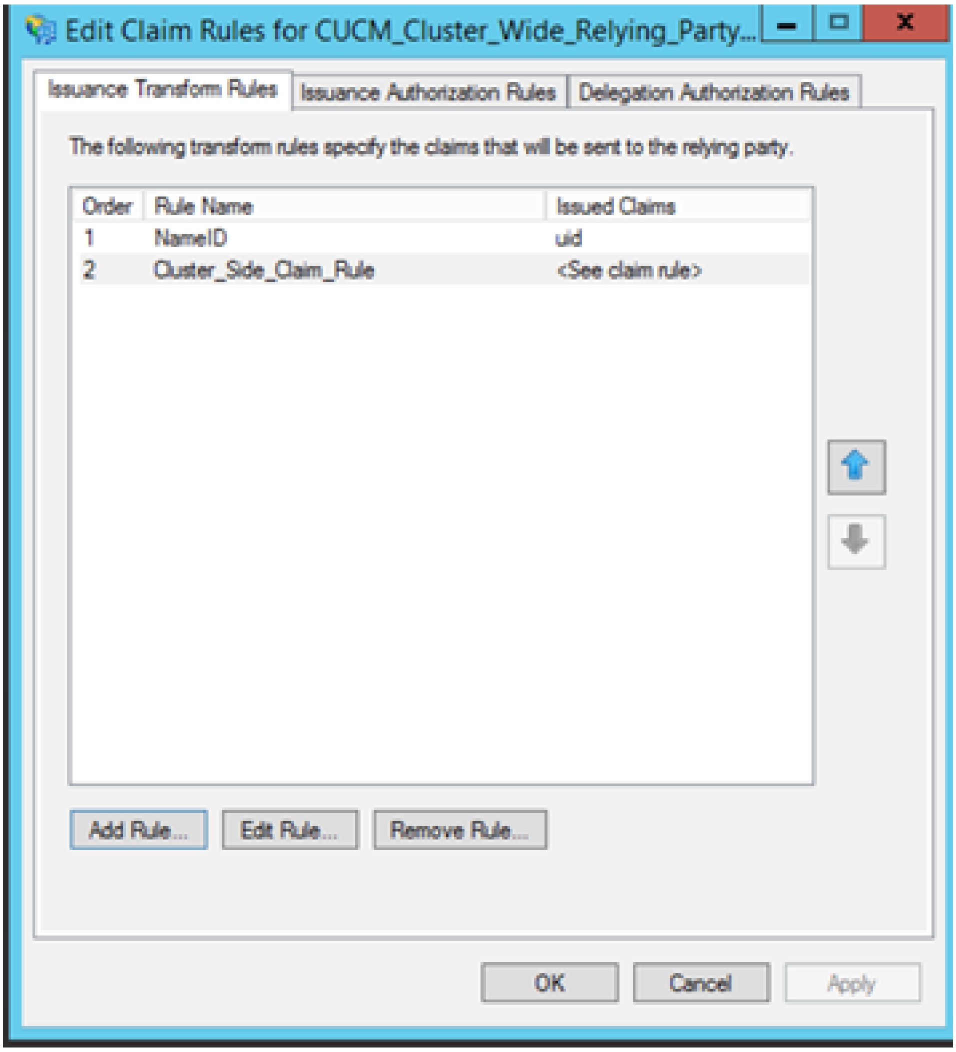
Cluster_Side_Claim_Rule

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");
```

Ahora debe tener dos reglas definidas en ADFS. Haga clic en **Aplicar** y **Aceptar** para cerrar la ventana de reglas.



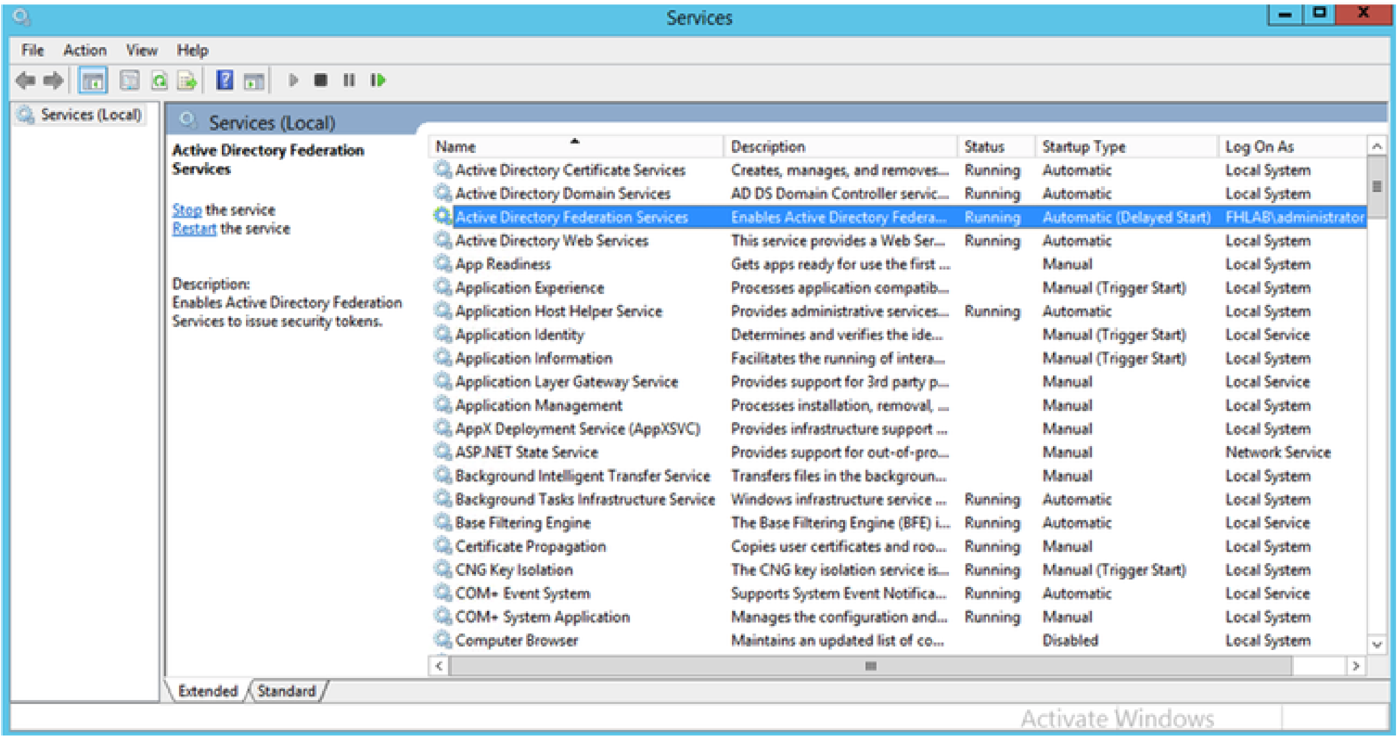
Edit Claim Rules for CUCM_Cluster_Wide_Relying_Party...
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules

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

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

Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

CUCM se ha agregado correctamente como parte de confianza a ADFS.



**Active Directory Federation Services**

Stop the service
Restart the service

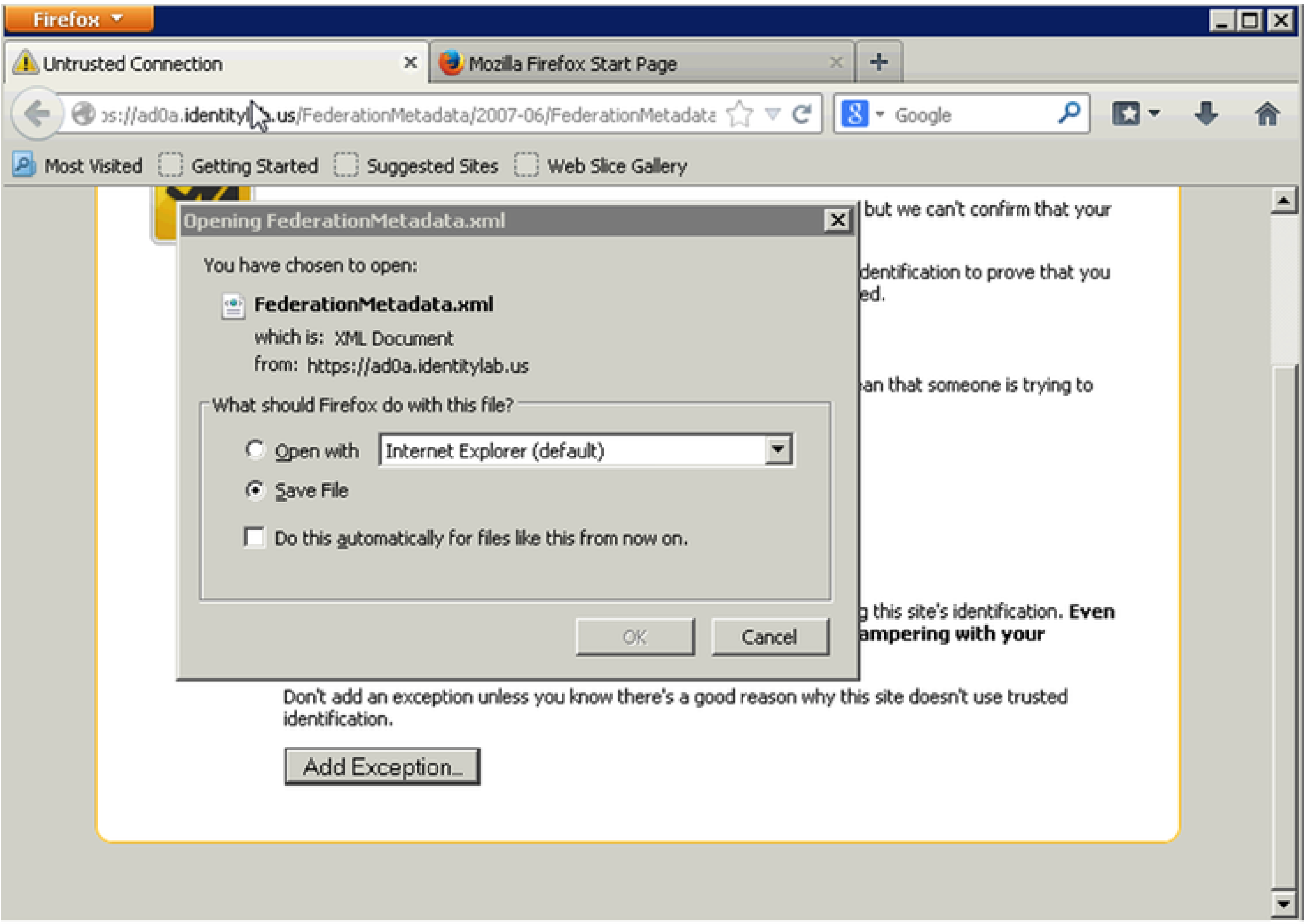
Description:
Enables Active Directory Federation Services to issue security tokens.

| 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 |

Antes de continuar, reinicie el servicio ADFS. Vaya a **Menú Inicio > Herramientas administrativas > Servicios**.

## Metadatos de IDP

Debe proporcionar a CUCM información sobre nuestro IdP. Esta información se intercambia mediante metadatos XML. Asegúrese de realizar este paso en el servidor donde está instalado ADFS.



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.

but we can't confirm that your

dentification to prove that you
ed.

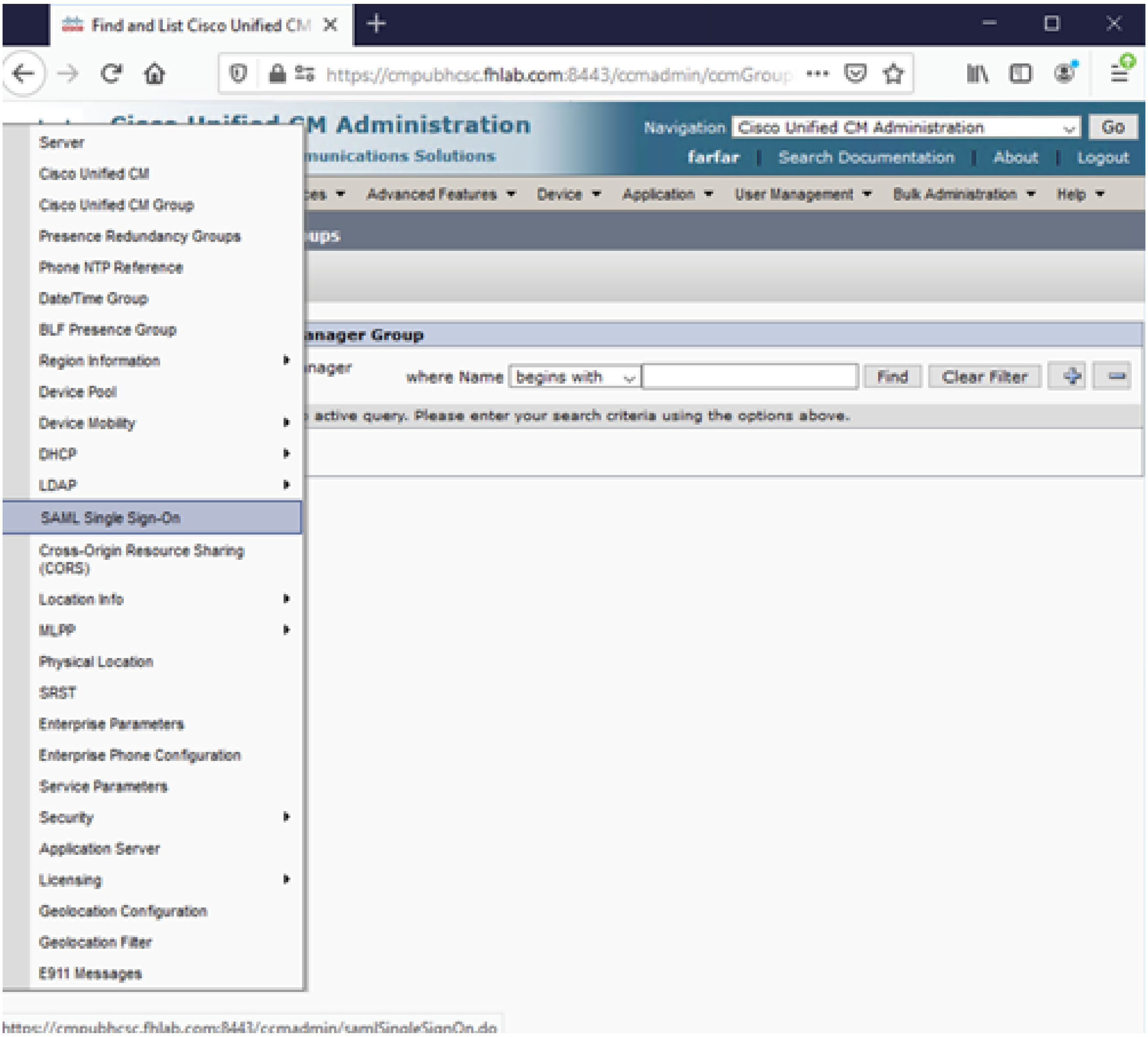
an that someone is trying to

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.

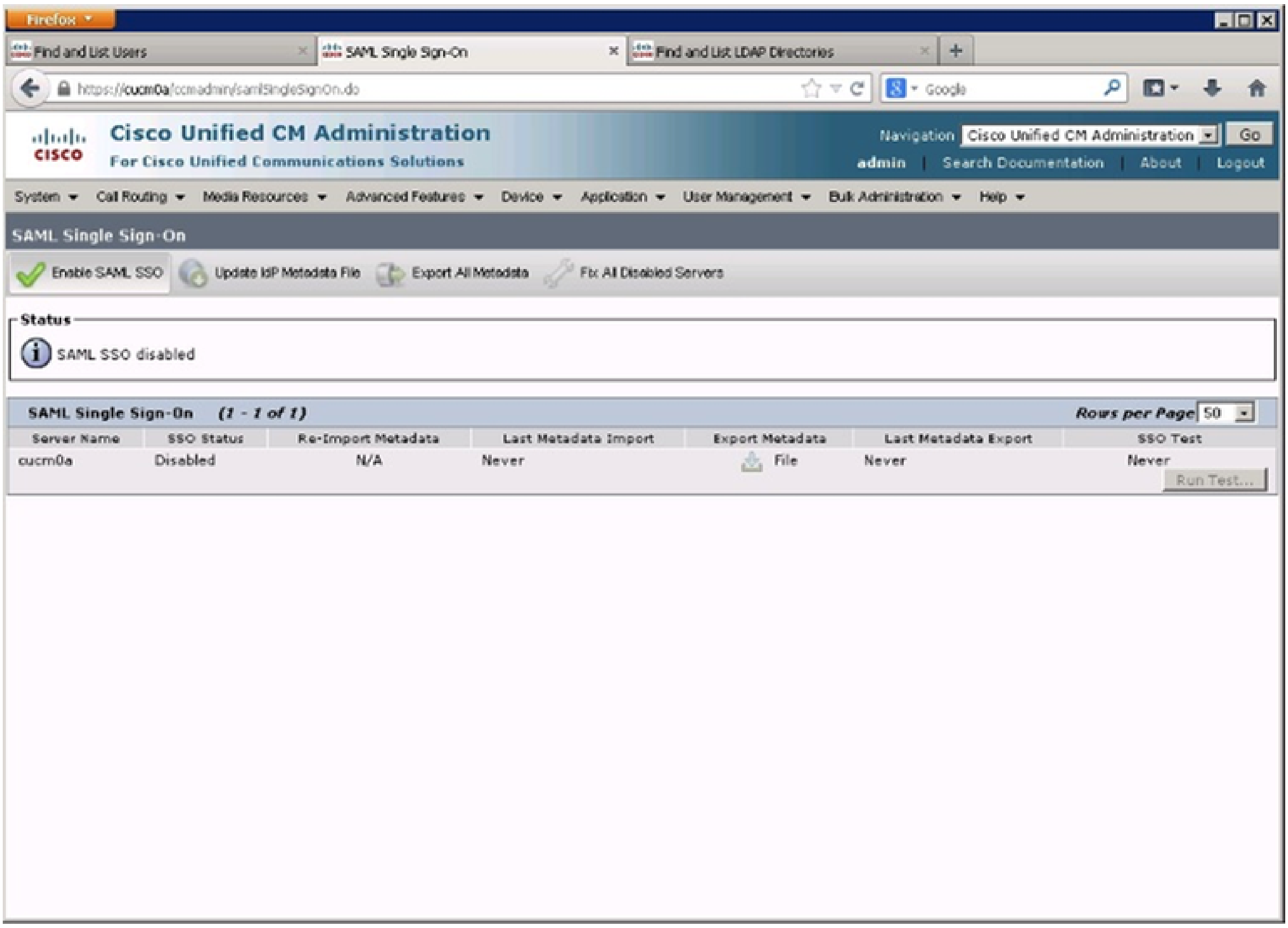
En primer lugar, debe conectarse a ADFS (IdP) mediante un navegador Firefox para descargar los metadatos XML. Abra un explorador en https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml y GUARDE los metadatos en una carpeta local.

Ahora, vaya a la configuración de CUCM al **menú** del sistema **> menú SAML Single Sign-On**.


Find and List Cisco Unified CM
https://cmpubhcsc.fhlab.com:8443/ccmadmin/ccmGroup
Cisco Unified CM Administration
munications Solutions
Navigation Cisco Unified CM Administration Go
farfar | Search Documentation | About | Logout
ces Advanced Features Device Application User Management Bulk Administration Help
ups
anager Group
nager where Name begins with Find Clear Filter
Server
Cisco Unified CM
Cisco Unified CM Group
Presence Redundancy Groups
Phone NTP Reference
Date/Time Group
BLF Presence Group
Region Information
Device Pool
Device Mobility
DHCP
LDAP
SAML Single Sign-On
Cross-Origin Resource Sharing (CORS)
Location Info
MLPP
Physical Location
SRST
Enterprise Parameters
Enterprise Phone Configuration
Service Parameters
Security
Application Server
Licensing
Geolocation Configuration
Geolocation Filter
E911 Messages
https://cmpubhcsc.fhlab.com:8443/ccmadmin/samlSingleSignOn.do

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

Vuelva a la administración de CUCM y seleccione **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
SAML Single Sign-On
Enable SAML SSO
Update IdP Metadata File
Export All Metadata
Fix All Disabled Servers

Status

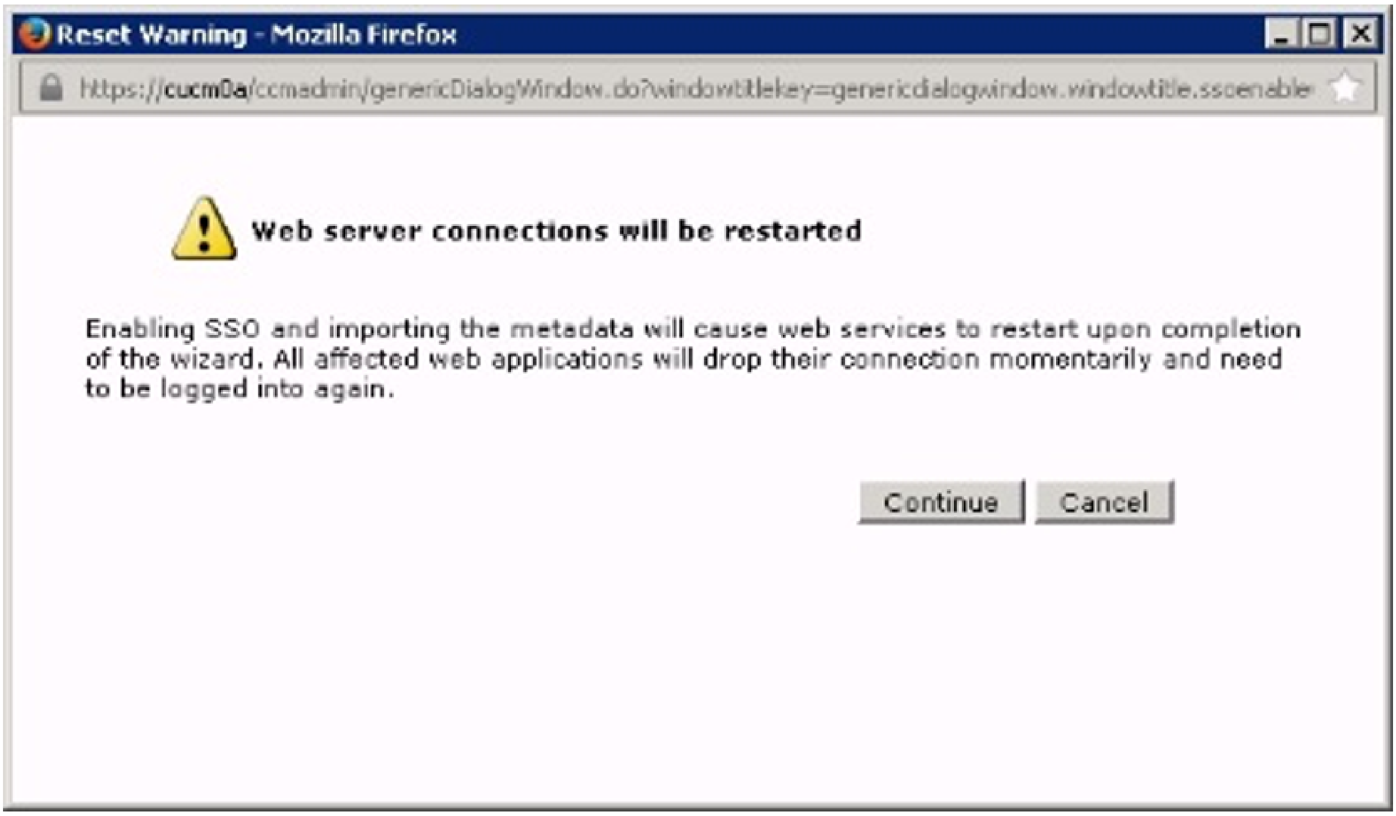
SAML SSO disabled

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<br>Run Test... |

Seleccione **Enable SAML SSO**.

Haga clic en **Continuar** para aceptar la advertencia.

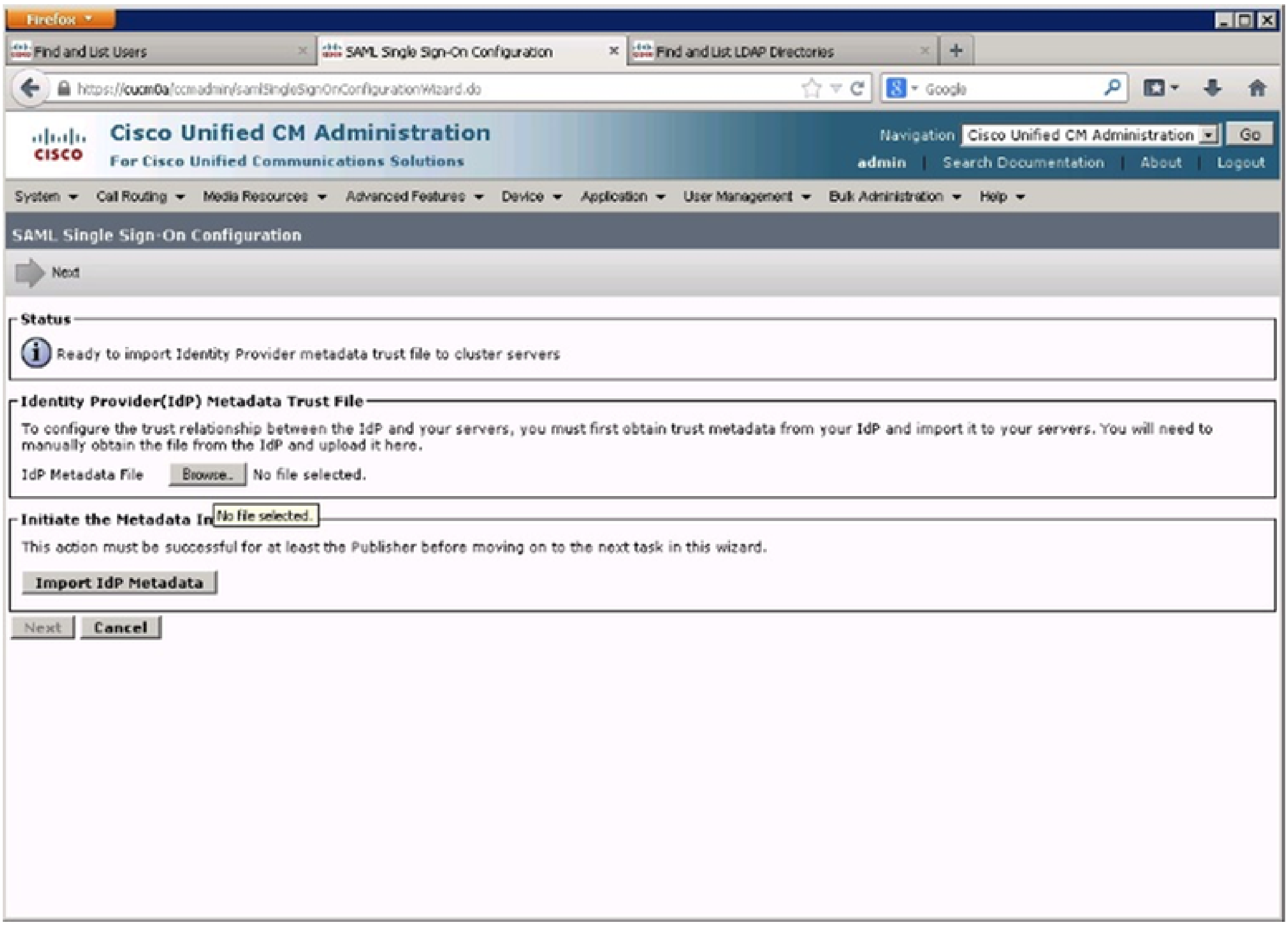

Reset Warning - Mozilla Firefox
https://cucm0a/ccmadmin/genericDialogWindow.do?windowtitlekey=genericdialogwindow.windowtitle.ssoenable
Continue
Cancel

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.

En la pantalla SSO y haga clic en **Browse.** para importar el archivo XML de metadatos

FederationMetadata.xml que guardó anteriormente, como se muestra en la imagen.


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
Next
Browse..
Import IdP Metadata
Next
Cancel

SAML Single Sign-On Configuration

Status

Ready to import Identity Provider metadata trust file to cluster servers

Identity Provider(IdP) Metadata Trust File

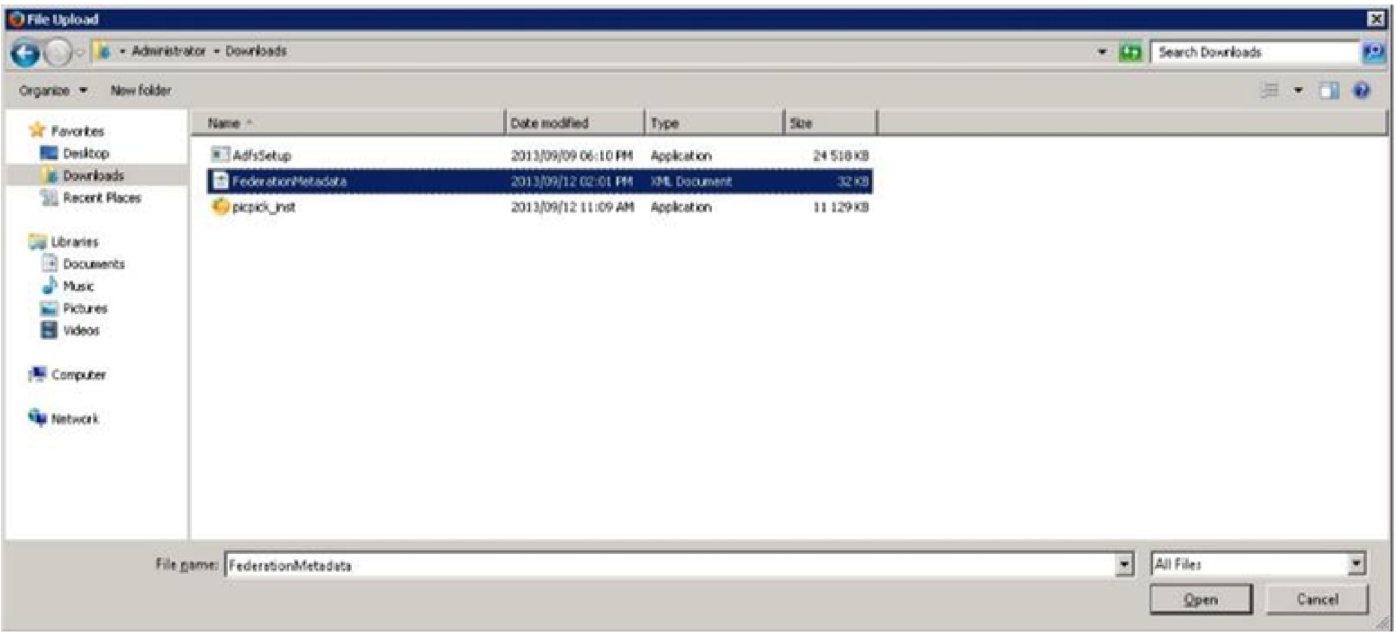
To configure the trust relationship between the IdP and your servers, you must first obtain trust metadata from your IdP and import it to your servers. You will need to manually obtain the file from the IdP and upload it here.

IdP Metadata File    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.

Seleccione el archivo XML y haga clic en **Abrir** para cargarlo en CUCM desde las Descargas bajo Favoritos.

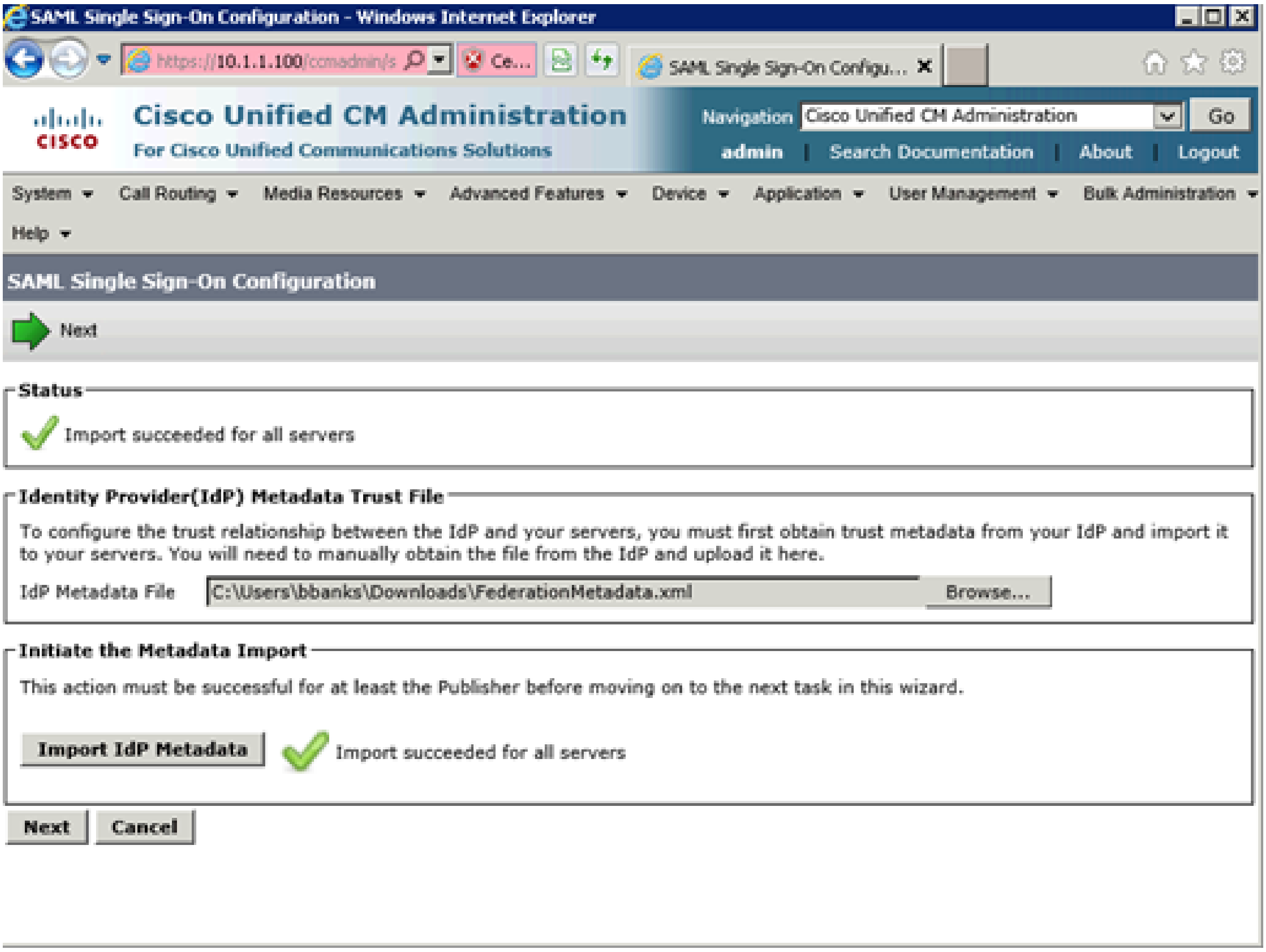


| Name | Date modified | Type | Size |
|---|---|---|---|
| AdfsSetup | 2013/09/09 06:10 PM | Application | 24 518 KB |
| FederationMetadata | 2013/09/12 02:01 PM | XML Document | 32 KB |
| picpick_inst | 2013/09/12 11:09 AM | Application | 11 129 KB |

File name: FederationMetadata

All Files

Una vez cargado, haga clic en Importar metadatos IdP para importar la información de IdP a CUCM. Confirme que la importación se ha realizado correctamente y haga clic en Next (Siguiente) para continuar.


SAML Single Sign-On Configuration - Windows Internet Explorer
https://10.1.1.100/ccmadmin/s
Ce...
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
Browse...
Import IdP Metadata
Next
Cancel

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.

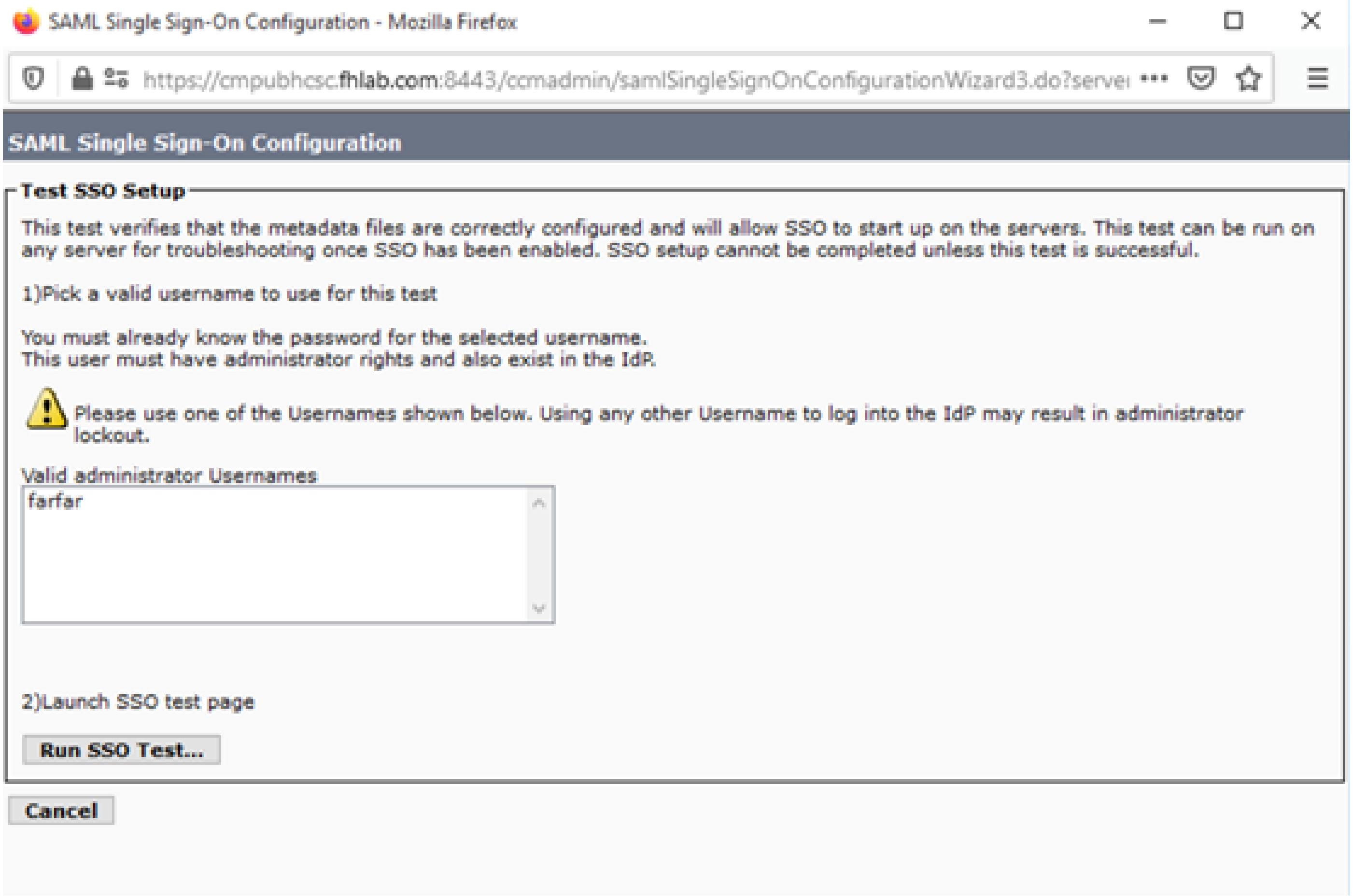
IdP Metadata File: C:\Users\bbanks\Downloads\FederationMetadata.xml

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

Seleccione el usuario que pertenece a los superusuarios de CCM estándar y haga clic en 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

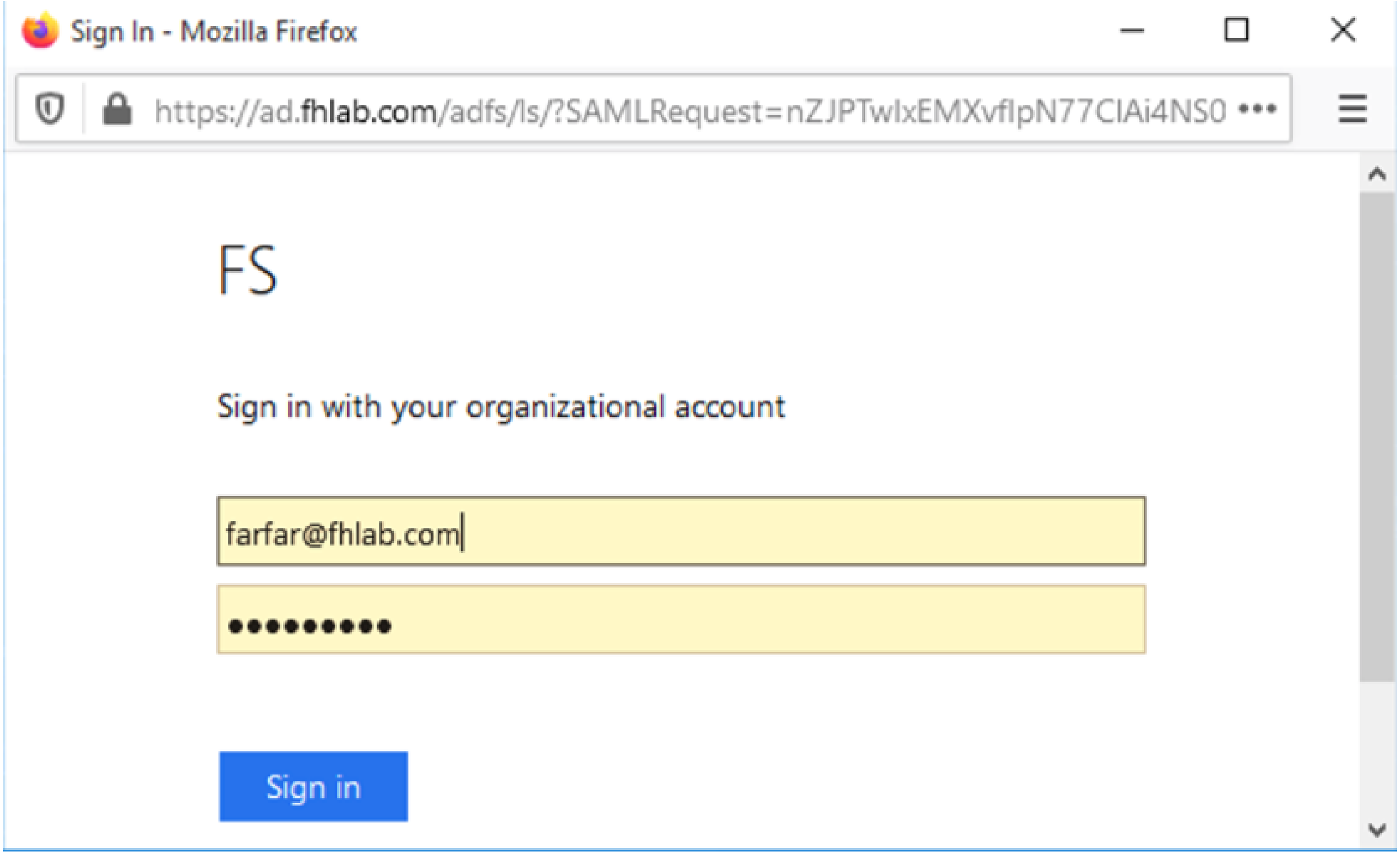
You must already know the password for the selected username.
This user must have administrator rights and also exist in the IdP.

⚠ 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

Cuando se presenta con un cuadro de diálogo de autenticación de usuario, inicie sesión con el nombre de usuario y la contraseña adecuados.

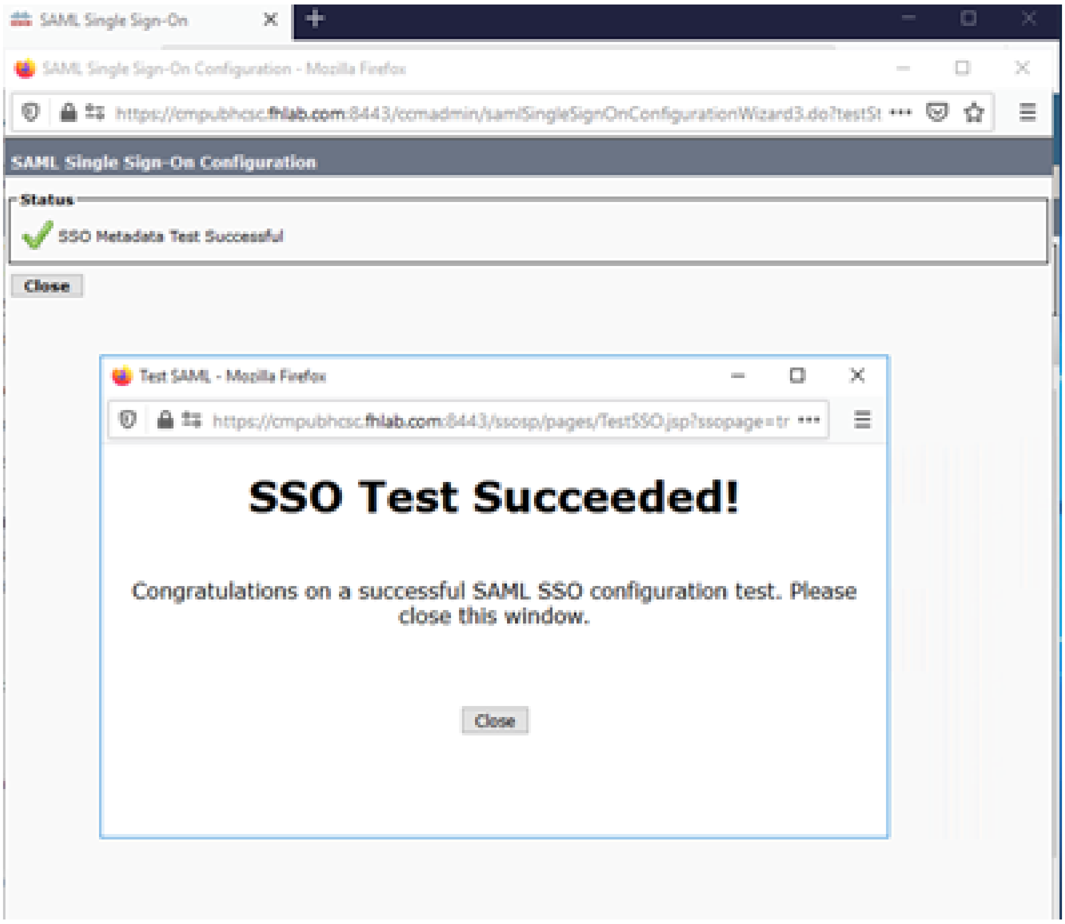

Sign In - Mozilla Firefox
https://ad.fhlab.com/adfs/ls/?SAMLRequest=nZJPTwlxEMXvflpN77CIAi4NS0
FS

Sign in with your organizational account

farfar@fhlab.com

●●●●●●●●●●

Si todo se ha configurado correctamente, debería ver un mensaje que dice SSO Test Succeeded (Prueba de SSO satisfactoria).


SAML Single Sign-On
SAML Single Sign-On Configuration - Mozilla Firefox
https://cmpubhcsc.fhlab.com:8443/ccmadmin/samlSingleSignOnConfigurationWizard3.do?testSt
Close
Test SAML - Mozilla Firefox
https://cmpubhcsc.fhlab.com:8443/ssosp/pages/TestSSO.jsp?ssopage=tr
Close

SAML Single Sign-On Configuration

Status

✓ SSO Metadata Test Successful

SSO Test Succeeded!

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

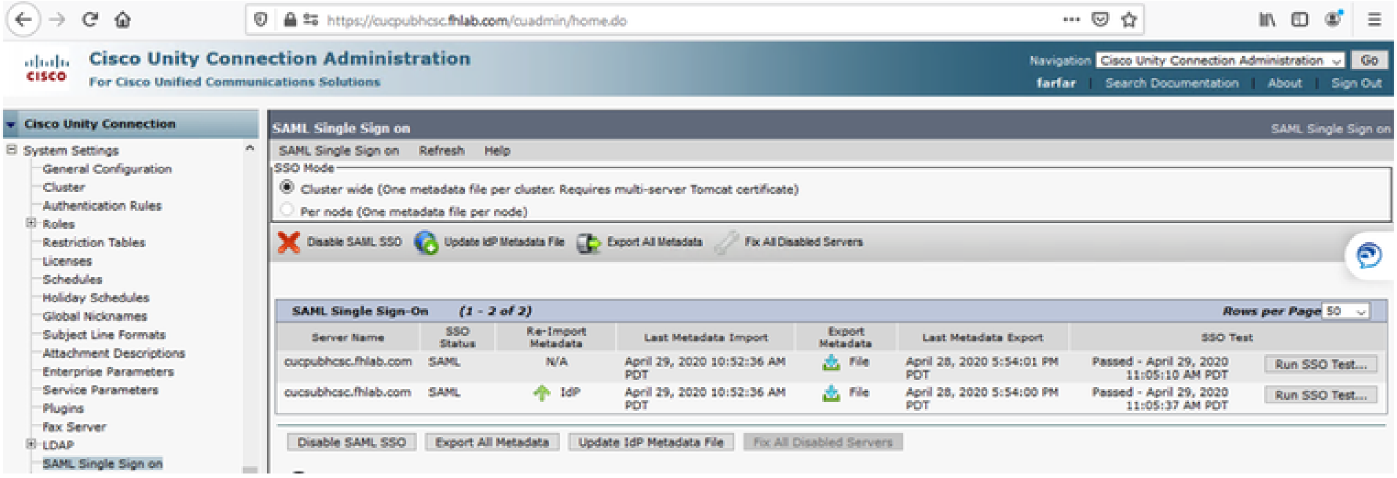
Haga clic en CERRAR y FINALIZAR para continuar.

Hemos completado con éxito las tareas de configuración básicas para habilitar SSO en CUCM mediante ADFS.

# Configuración de SSO en CUC

Se puede seguir el mismo proceso para habilitar SSO en Unity Connection.

Integración de LDAP con CUC.



SAML Single Sign on

SSO Mode

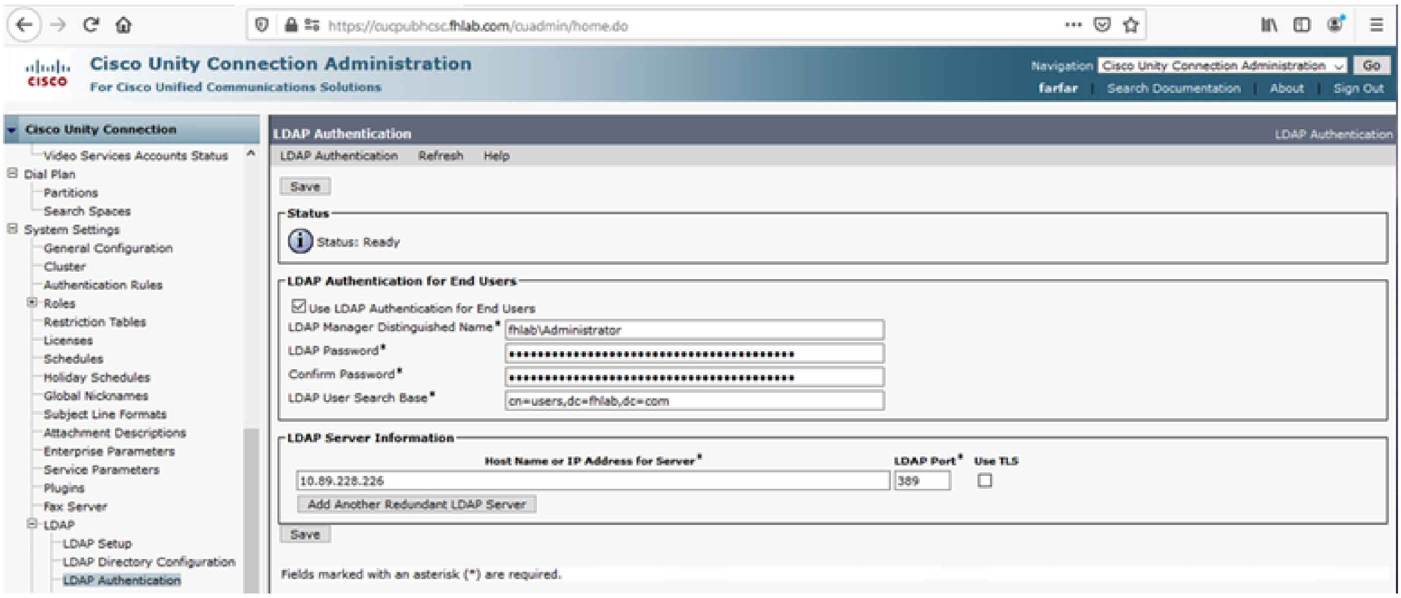
● Cluster wide (One metadata file per cluster. Requires multi-server Tomcat certificate)

○ Per node (One metadata file per node)

SAML Single Sign-On (1 - 2 of 2)

| 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 |
| 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 |

Configuración de la autenticación LDAP.



**Status**

Status: Ready

**LDAP Authentication for End Users**

☑ Use LDAP Authentication for End Users

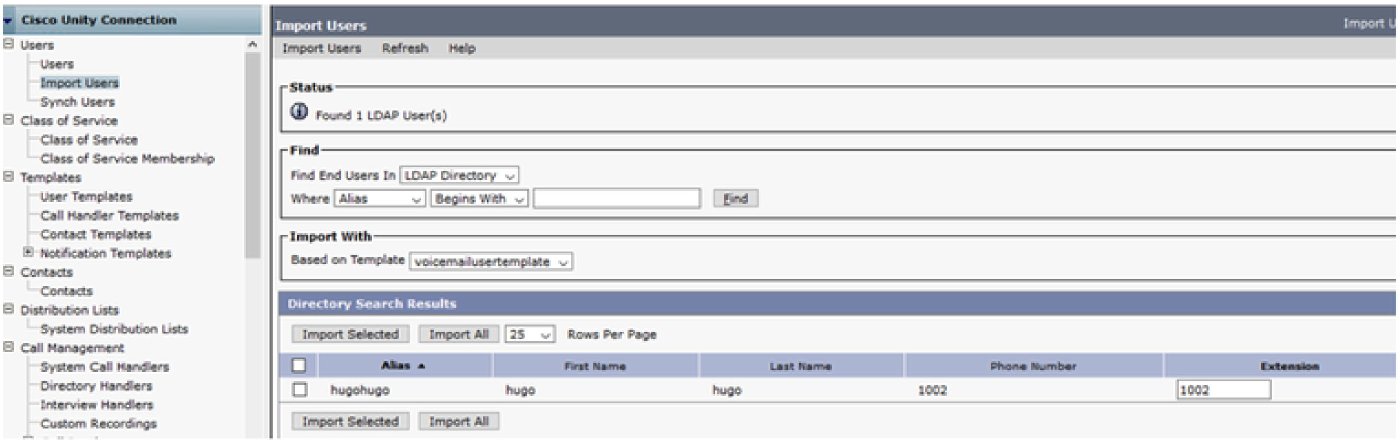
| | |
|---|---|
| LDAP Manager Distinguished Name* | fhlab\Administrator |
| LDAP Password* | •••••••••••••••••••••••••••••••••••••••••• |
| Confirm Password* | •••••••••••••••••••••••••••••••••••••••••• |
| LDAP User Search Base* | cn=users,dc=fhlab,dc=com |

**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.

Importe los Usuarios de LDAP que tendrán asignado el buzón de voz y también el usuario que servirá para probar SSO.



**Status**

Found 1 LDAP User(s)

**Find**

Find End Users In LDAP Directory

Where Alias Begins With Find

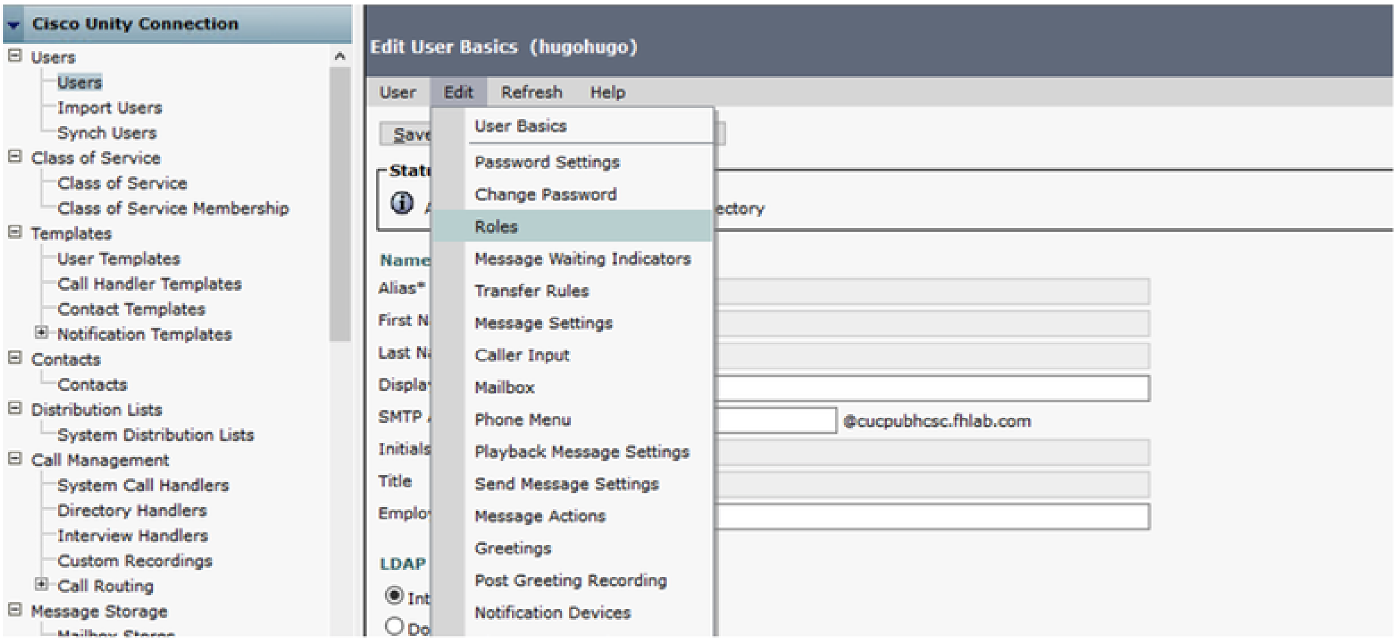
**Import With**

Based on Template voicemailusertemplate

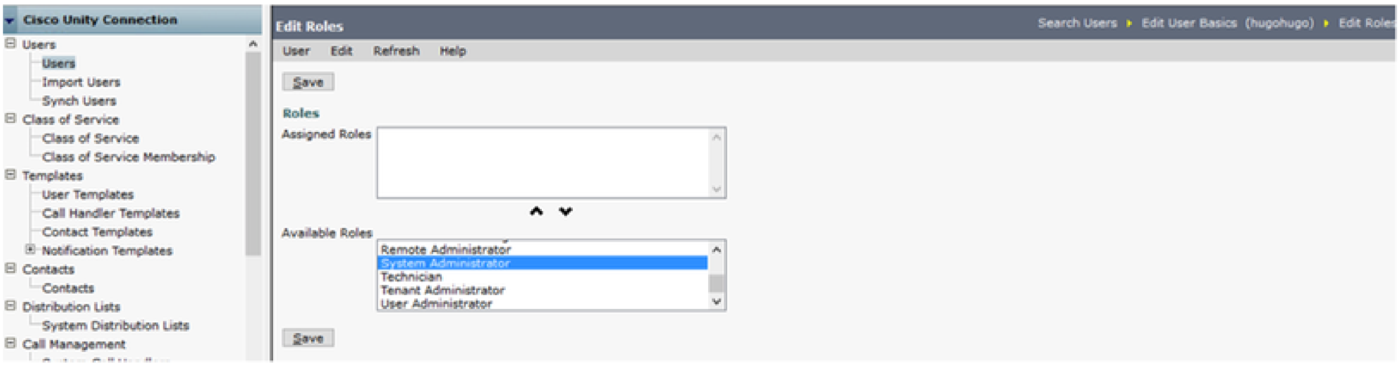
**Directory Search Results**

| □ | Alias ▲ | First Name | Last Name | Phone Number | Extension |
|---|---|---|---|---|---|
| □ | hugohugo | hugo | hugo | 1002 | 1002 |

Navegue hasta **Usuarios > Editar > Funciones** como se muestra en la imagen.



Asigne al usuario de prueba la función de administrador del sistema.



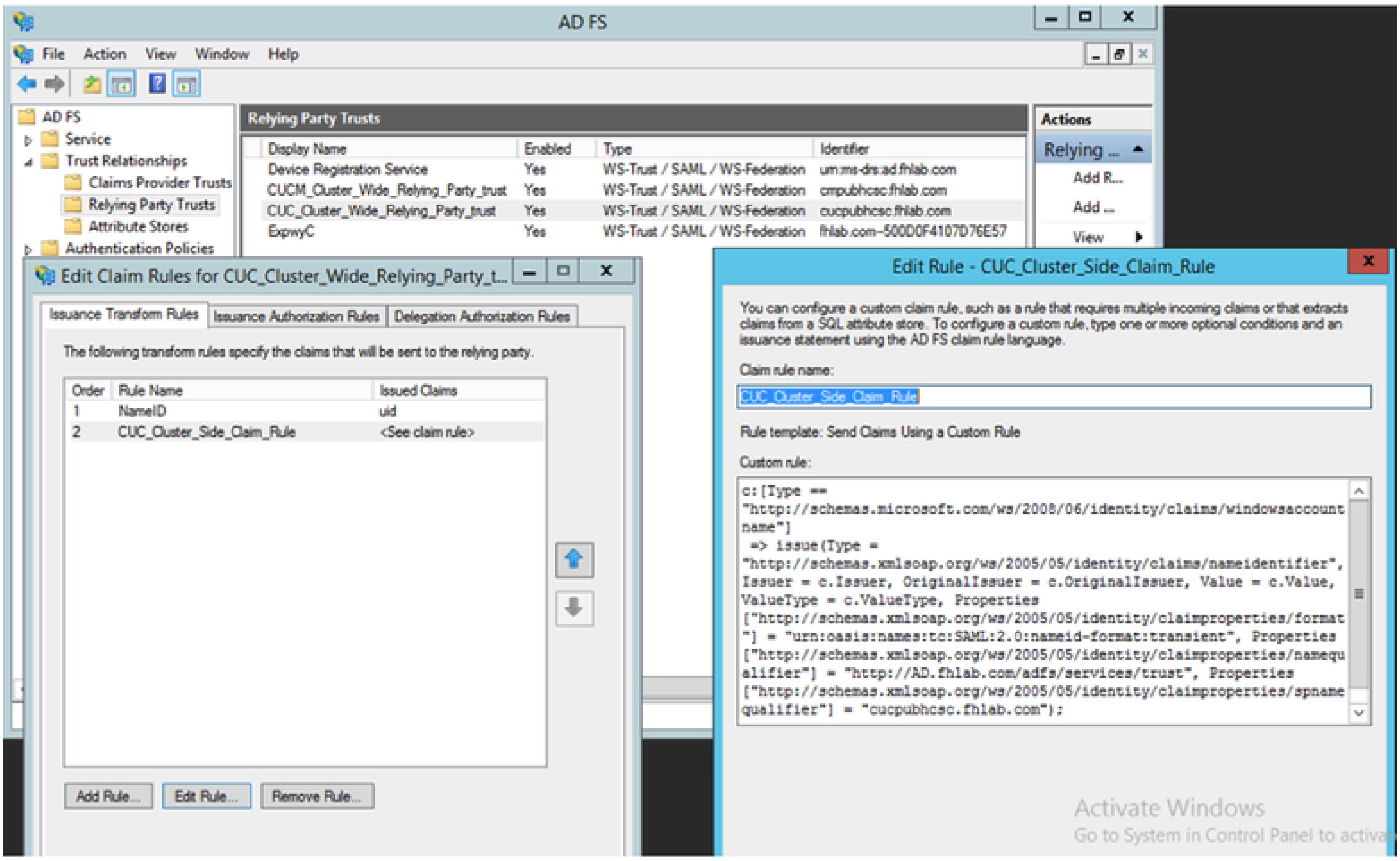
Roles

Assigned Roles:

Available Roles:
Remote Administrator
System Administrator
Technician
Tenant Administrator
User Administrator

## Metadatos CUC

Ya debería haber descargado los metadatos CUC, creado el FiyingPartyTrust para CUC y cargado los metadatos CUC y creado las reglas I AD FS en ADFS 3.0



| 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...
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 |
| 2 | CUC_Cluster_Side_Claim_Rule | <See 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.

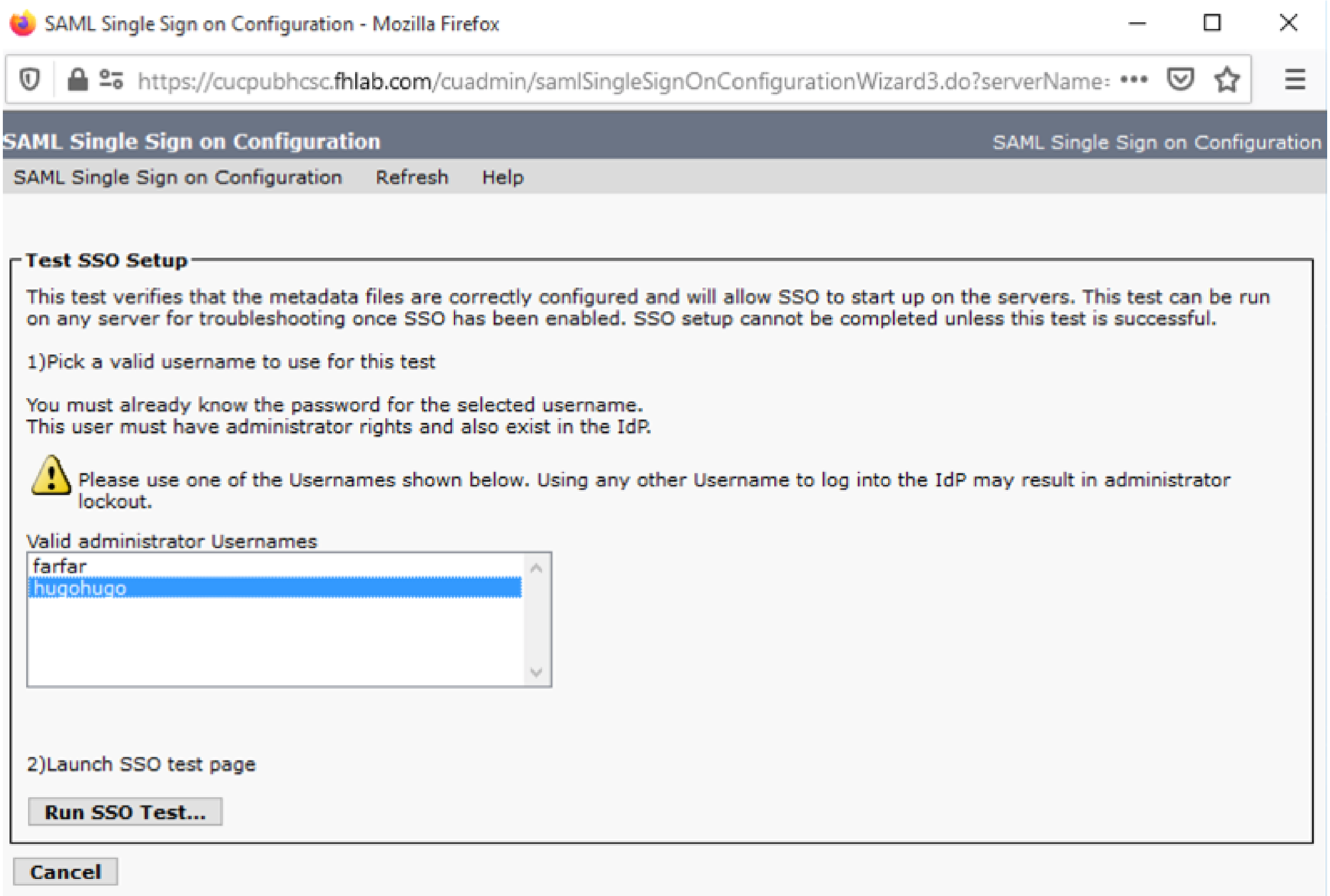
Claim rule name: CUC_Cluster_Side_Claim_Rule

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");
```

Vaya a Inicio de sesión único SAML y active SAML SSO.



SAML Single Sign on Configuration - Mozilla Firefox

https://cucpubhcsc.fhlab.com/cuadmin/samlSingleSignOnConfigurationWizard3.do?serverName:

**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

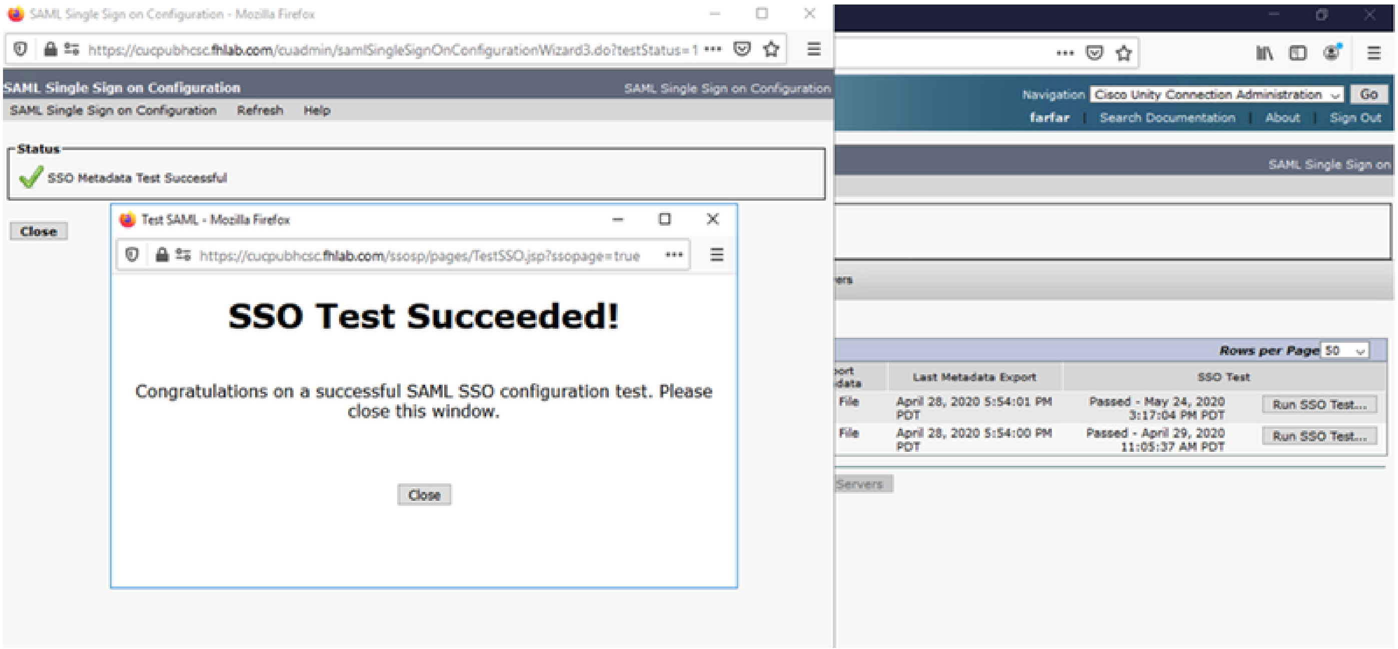
You must already know the password for the selected username.
This user must have administrator rights and also exist in the IdP.

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
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**

**Status**

✓ SSO Metadata Test Successful

Test SAML - Mozilla Firefox

https://cucpubhcsc.fhlab.com/ssosp/pages/TestSSO.jsp?ssopage=true

**SSO Test Succeeded!**

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

Navigation Cisco Unity Connection Administration

farfar | Search Documentation | About | Sign Out

Rows per Page 50

| ort<br>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... |

# Configuración de SSO en Expressway

## Importar metadatos a Expressway C

Abra un explorador en https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml y GUARDE los metadatos en una carpeta local

Cargar en **Configuración > Unified Communications > IDP**.

## Exportar metadatos de Expressway C

Vaya a la configuración -> Unified Communications -> IDP -> Exportar datos SAML

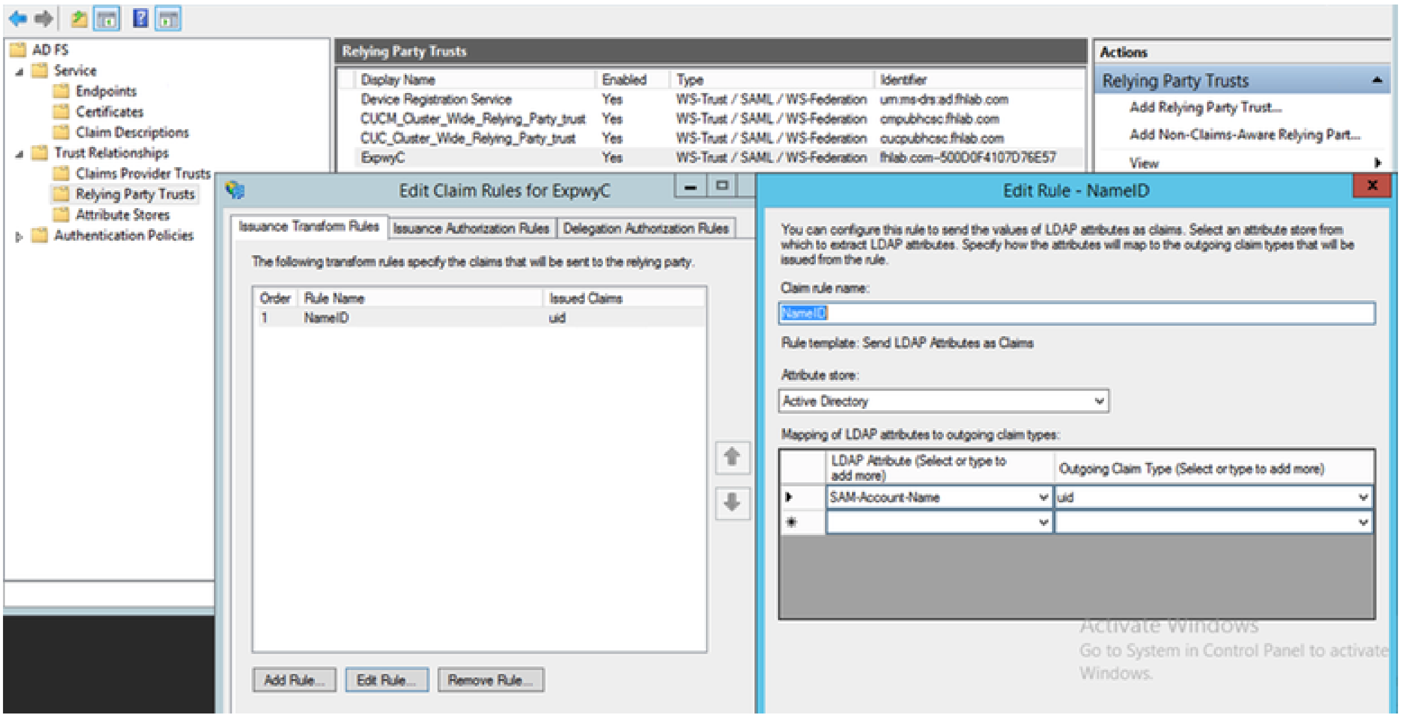
El modo de clúster utiliza un certificado autofirmado (con una duración prolongada) que se incluye en el SAML

metadatos y utilizados para firmar solicitudes SAML

- En el modo de todo el clúster, para descargar el único archivo de metadatos de todo el clúster, haga clic en Descargar
- En el modo por peer, para descargar el archivo de metadatos de un peer individual, haga clic en Descargar junto al par. Para exportar todo en un archivo .zip, haga clic en Descargar todo.

## Adición de confianza de una persona que confía en Cisco Expressway-E

En primer lugar, cree Confianzas de Parte Confiable para Expressway-Es y, a continuación, agregue una regla de reclamación para enviar la identidad como atributo UID.



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

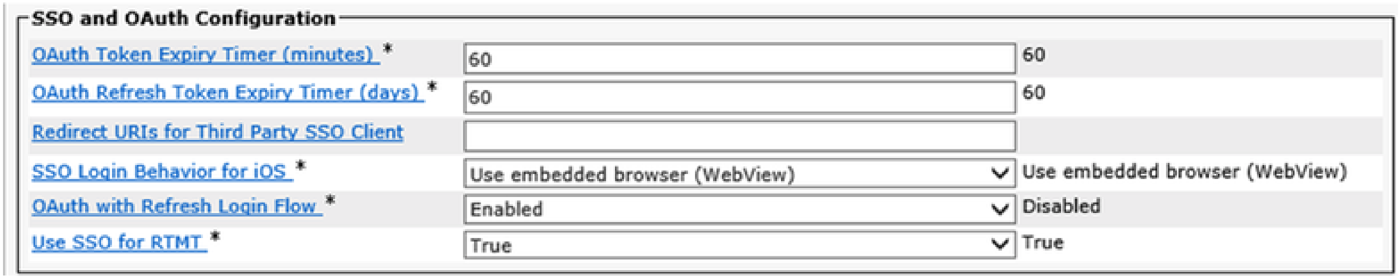
Mapping of LDAP attributes to outgoing claim types:

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

Activate Windows
Go to System in Control Panel to activate Windows.

## OAuth con actualización de inicio de sesión

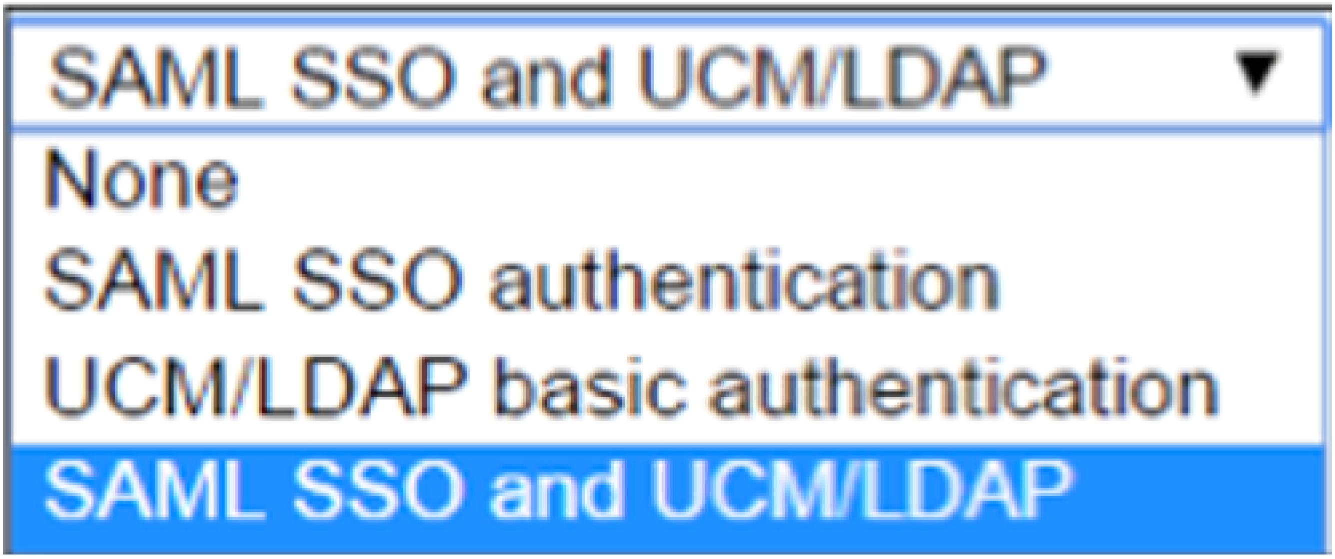
En Cisco CUCM Enterprise Parameters, se habilita el parámetro Verify OAuth with Refresh login flow . Vaya a **Administración de Cisco Unified CM > Parámetros empresariales > Configuración de SSO y OAuth**.



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 |

## Ruta de autenticación



- Si la ruta de autenticación se establece en "autenticación SAML SSO", sólo los clientes Jabber que utilicen un clúster de Unified CM habilitado para SSO podrán utilizar MRA en este Expressway. Esta es una configuración sólo de SSO.
- La compatibilidad con MRA de Expressway para todos los teléfonos IP, todos los terminales de TelePresence y cualquier cliente Jabber que se aloje en un clúster de Unified CM no configurado para SSO requerirá la ruta de autenticación para incluir la autenticación de UCM/LDAP.
- Si uno o más de los clústeres de Unified CM son compatibles con Jabber SSO, seleccione "SAML SSO y UCM/LDAP" para permitir la autenticación básica y SSO.

# Arquitectura SSO

SAML es un formato de datos abierto estándar basado en XML que permite a los administradores acceder a un conjunto definido de aplicaciones de colaboración de Cisco sin problemas después de iniciar sesión en una de esas aplicaciones. SAML SSO utiliza el protocolo SAML 2.0 para ofrecer un inicio de sesión único entre dominios y productos para las soluciones de colaboración de Cisco.

## Flujo de inicio de sesión en las instalaciones

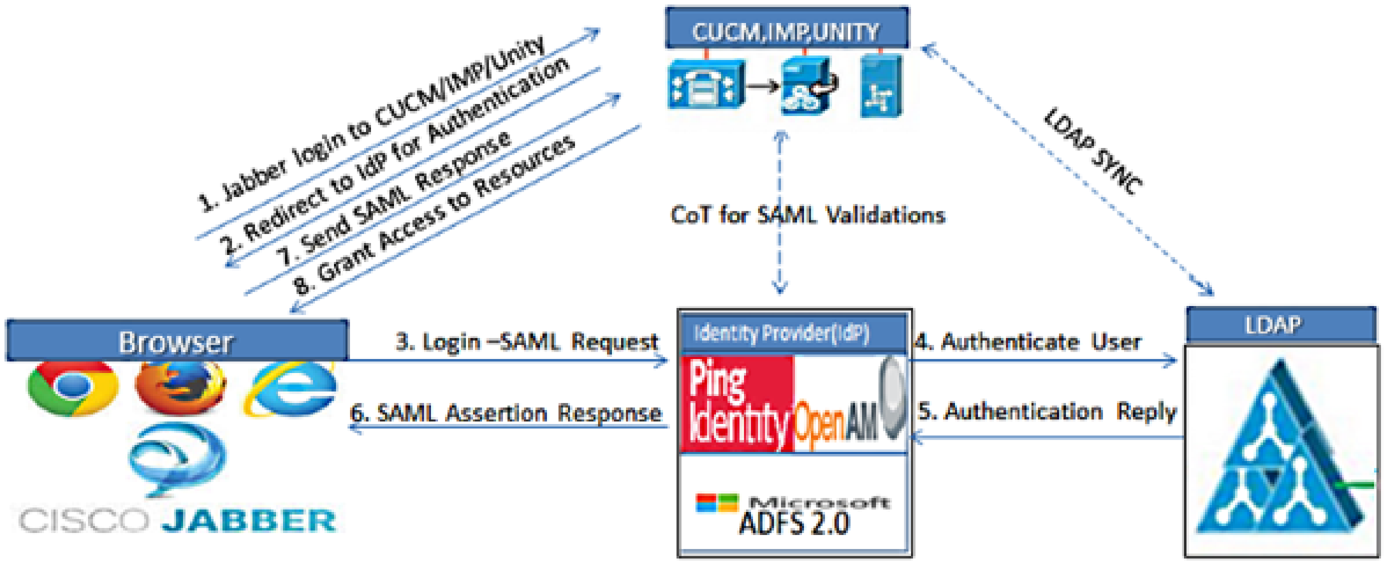
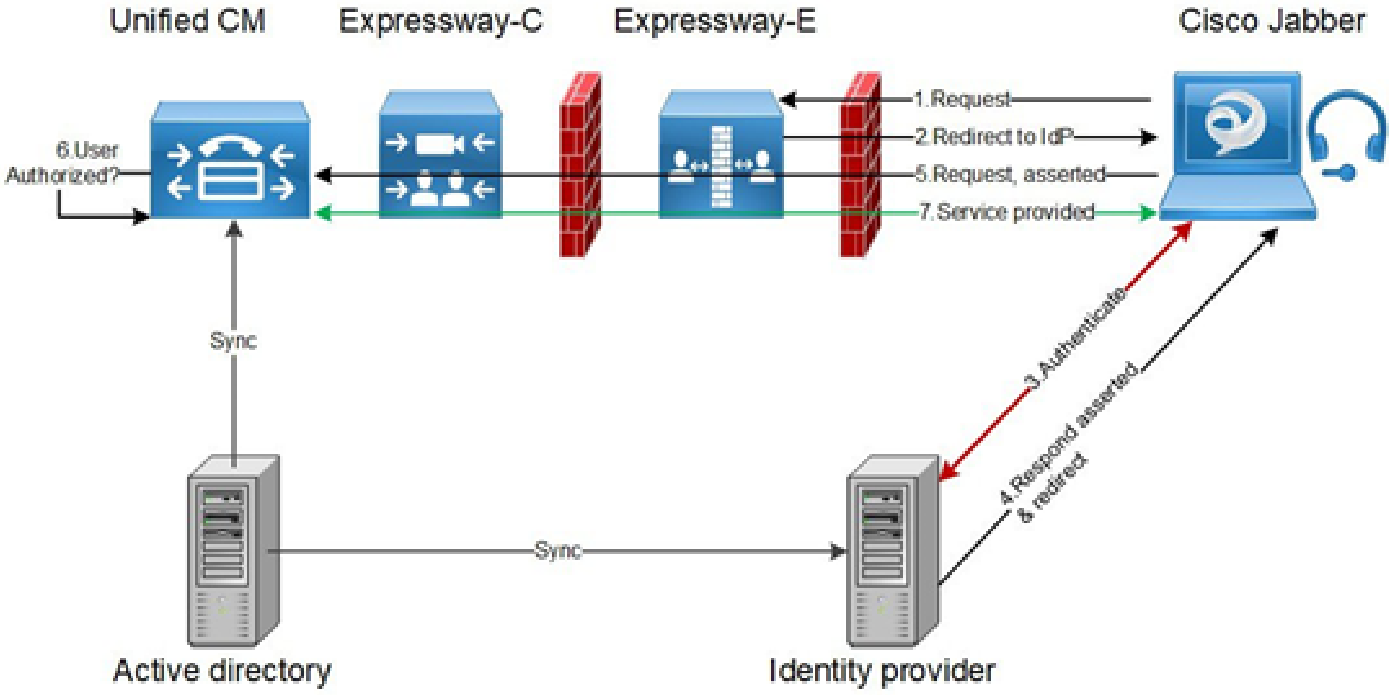


*Figure :SAML Single sign SSO Call Flow for Collaboration Servers*

## Flujo de inicio de sesión de MRA



## OAuth

OAuth es un estándar que admite la autorización. Se debe autenticar a un usuario antes de que pueda autorizarse. El flujo de concesión de código de autorización proporciona un método para que un cliente obtenga acceso y actualice tokens para acceder a un recurso (servicios de Unified CM, IM&P, Unity y Expressway). Este flujo también se basa en la redirección y, por lo tanto, requiere que el cliente pueda interactuar con un agente de usuario HTTP (navegador web) controlado por el usuario. El cliente realizará una solicitud inicial al servidor de autorización mediante HTTPS. El servidor OAuth redirige al usuario a un servicio de autenticación. Esto puede estar ejecutándose en Unified CM o en un IdP externo si SAML SSO está habilitado. Según el método de autenticación que se utilice, se puede presentar al usuario final una vista de página web para que se autentique. (La autenticación Kerberos es un ejemplo que no mostraría una página web.) A diferencia del flujo de concesión implícito, un flujo de concesión de código de autenticación exitoso resultará en que los servidores OAuth emitan un "Código de autorización" al navegador web. Se trata de un código único de un solo uso y de corta duración que se devuelve del navegador web al cliente. El cliente proporciona este "código de autorización" al servidor de autorización junto con un secreto previamente compartido y recibe a cambio un "token de acceso" y un "token de actualización". El secreto de cliente utilizado en este paso permite al servicio de autorización limitar el uso sólo a clientes registrados y autenticados. Los tokens se utilizan para los siguientes fines:

### Access/Refresh Token

Token de acceso: Este token lo emite el servidor de autorización. El cliente presenta el token a un servidor de recursos cuando necesita acceder a los recursos protegidos en ese servidor. El servidor de recursos puede validar el token y confía en las conexiones mediante el token. (El valor predeterminado de los tokens de acceso de Cisco es de 60 minutos de duración)

Actualizar token: El servidor de autorización vuelve a emitir este token. El cliente presenta este token al servidor de autorización junto con el secreto del cliente cuando el token de acceso ha caducado o va a caducar. Si el token de actualización sigue siendo válido, el servidor de autorización emitirá un nuevo token de acceso sin necesidad de otra autenticación. (Los tokens de actualización de Cisco tienen como valor predeterminado una duración de 60 días). Si el token de actualización ha caducado, se debe iniciar un nuevo flujo de concesión de código de autorización OAuth completo para obtener nuevos tokens.

### El flujo de concesión de código de autorización de OAuth es mejor

En el flujo de concesión implícito, el token de acceso se pasa al cliente Jabber a través de un agente de usuario HTTP (navegador). En el flujo de concesión de código de autorización, el token de acceso se intercambia directamente entre el servidor de autorización y el cliente Jabber. El token se solicita desde el servidor de autorización mediante un código de autorización único y limitado en tiempo. Este intercambio directo del token de acceso es más seguro y reduce la exposición al riesgo.

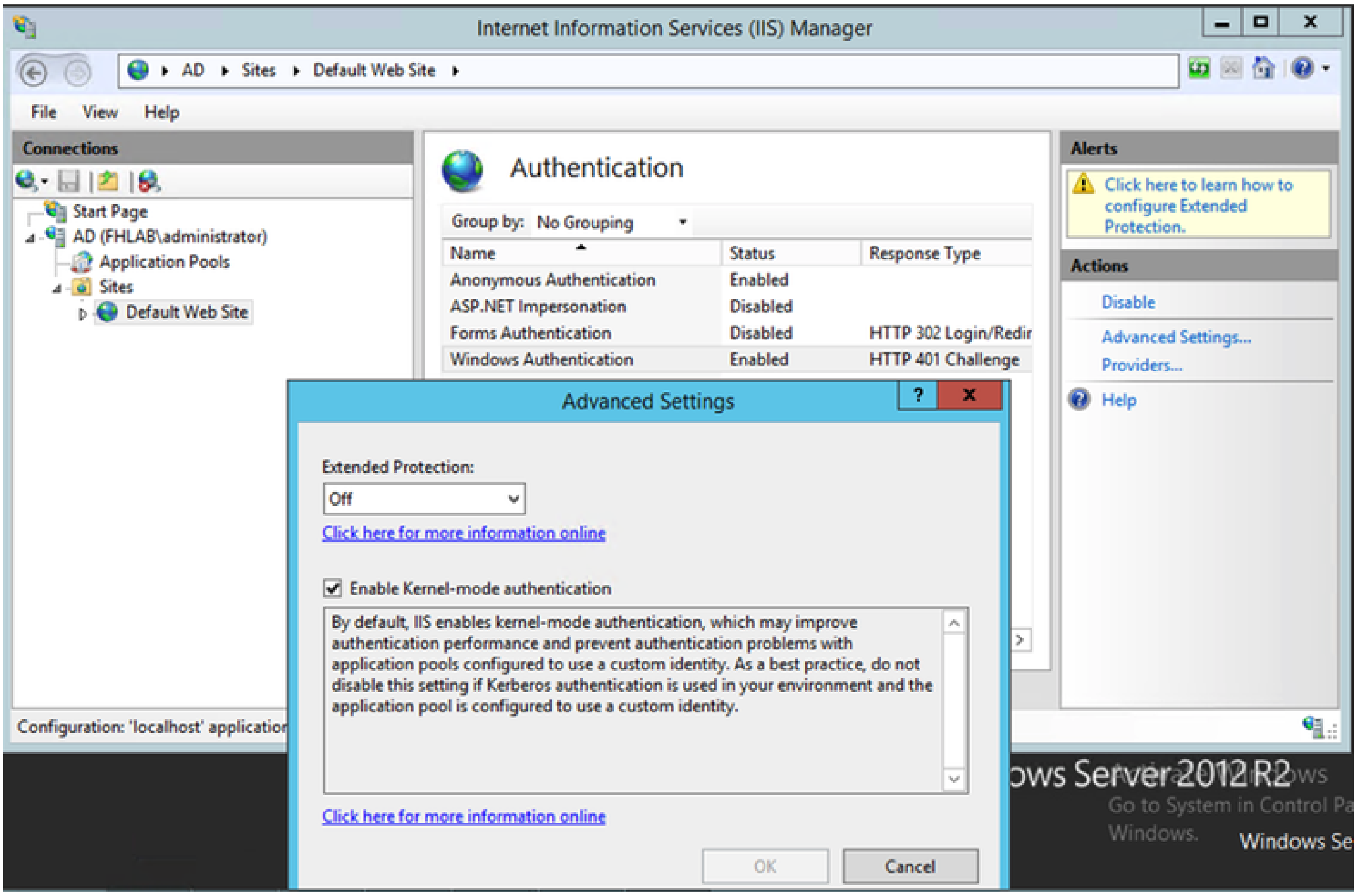
El flujo de concesión de código de autorización OAuth admite el uso de tokens de actualización. Esto ofrece una mejor experiencia al usuario final, ya que no necesita volver a autenticarse con la misma frecuencia (de forma predeterminada, 60 días)

# Configurar Kerberos

## Seleccionar autenticación de Windows

**Administrador de Internet Information Services (IIS) > Sitios > Sitio Web predeterminado > Autenticación > Autenticación de Windows > Configuración avanzada**.

1. Desmarque Enable Kernel-mode authentication .
2. Asegúrese de que la protección ampliada está desactivada.



| 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

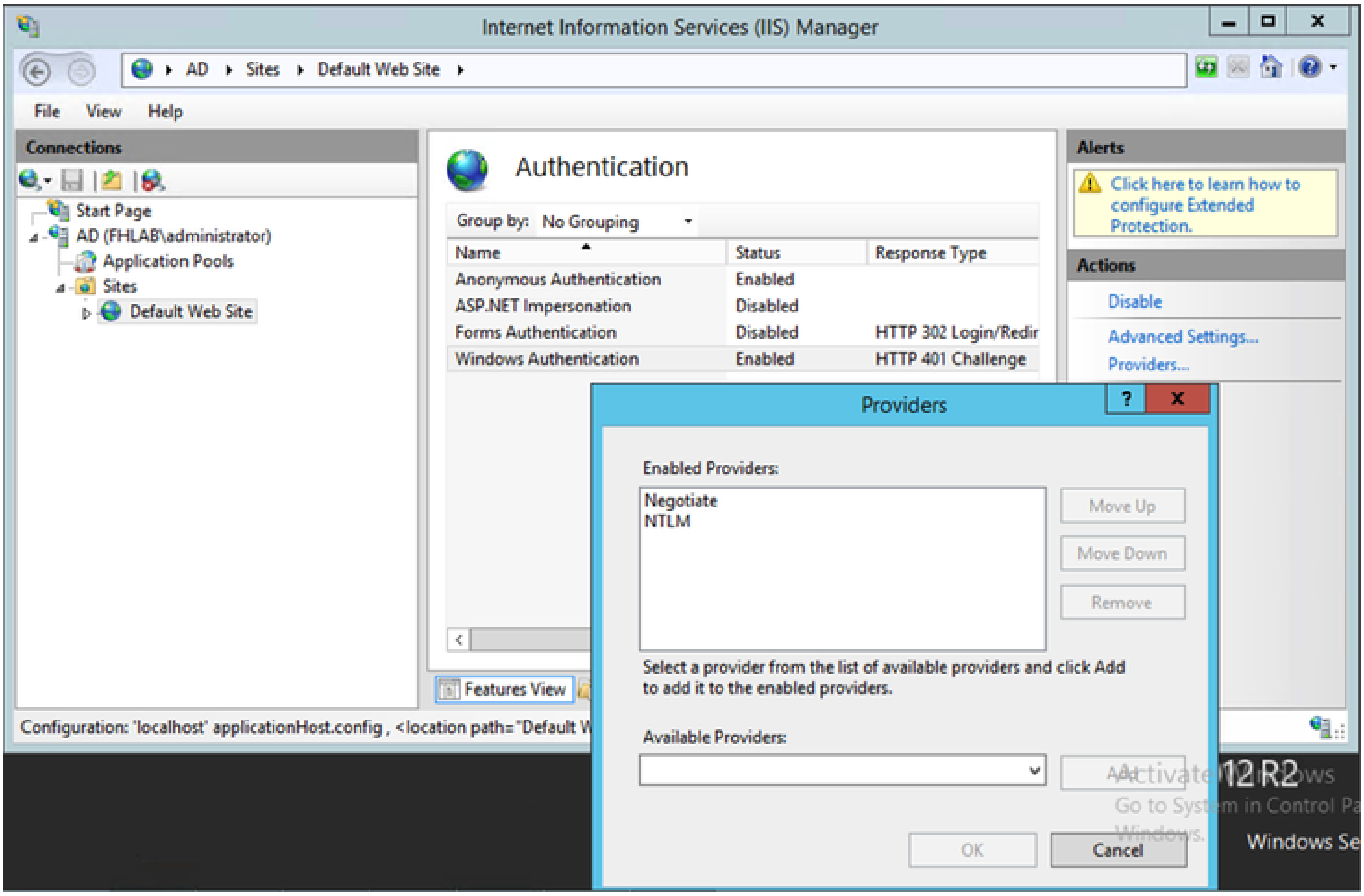
By default, IIS enables kernel-mode authentication, which may improve authentication performance and prevent authentication problems with application pools configured to use a custom identity. As a best practice, do not disable this setting if Kerberos authentication is used in your environment and the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

Click here for more information online

## ADFS admite Kerberos NTLM

Asegúrese de que AD FS versión 3.0 admita tanto el protocolo Kerberos como el protocolo NT LAN Manager (NTLM) porque todos los clientes que no son de Windows no pueden utilizar Kerberos y confían en NTLM.

En el panel derecho, seleccione Proveedores y asegúrese de que Negotiate y NTLM estén presentes en Proveedores habilitados:



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 |

Enabled Providers:

Negotiate
NTLM

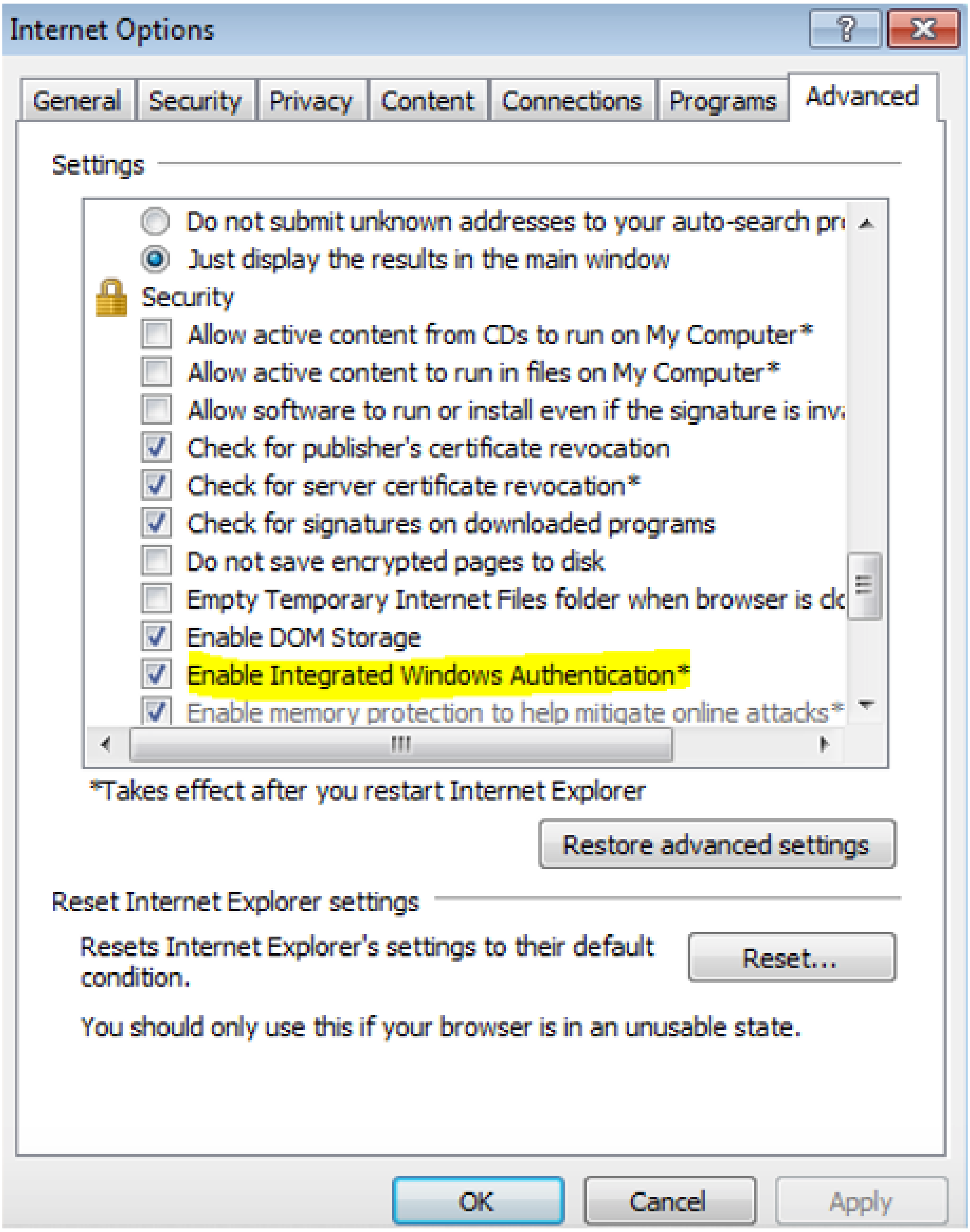
Select a provider from the list of available providers and click Add to add it to the enabled providers.

Available Providers:

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

## Configurar Microsoft Internet Explorer

Asegúrese de que **Internet Explorer > Advanced > Enable Integrated Windows Authentication** esté activado.



○ 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

Resets Internet Explorer's settings to their default condition.

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

Agregar URL de ADFS en Seguridad > Zonas de Intranet > Sitios