Configurer SAML SSO sur Cisco Unified Communications Manager avec ADFS 3.0

Contenu

Introduction

Ce document décrit les étapes à suivre pour configurer l'authentification unique avec Active Directory Federation Service (ADFS 3.0) avec l'utilisation de Windows 2012 R2 sur Cisco Unified Communication Manage (CUCM), Cisco Unity Connection (CUC) et les produits Expressway. Les étapes de configuration de Kerberos sont également incluses dans ce document.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître les produits SSO (Single Sign-On) et Windows.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CUCM 11,5
- CUC 11,5
- Expressway 12
- Windows 2012 R2 Server avec les rôles suivants :
  - Services de certificats Active Directory
  - Services de fédération 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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Vérification préalable de la configuration

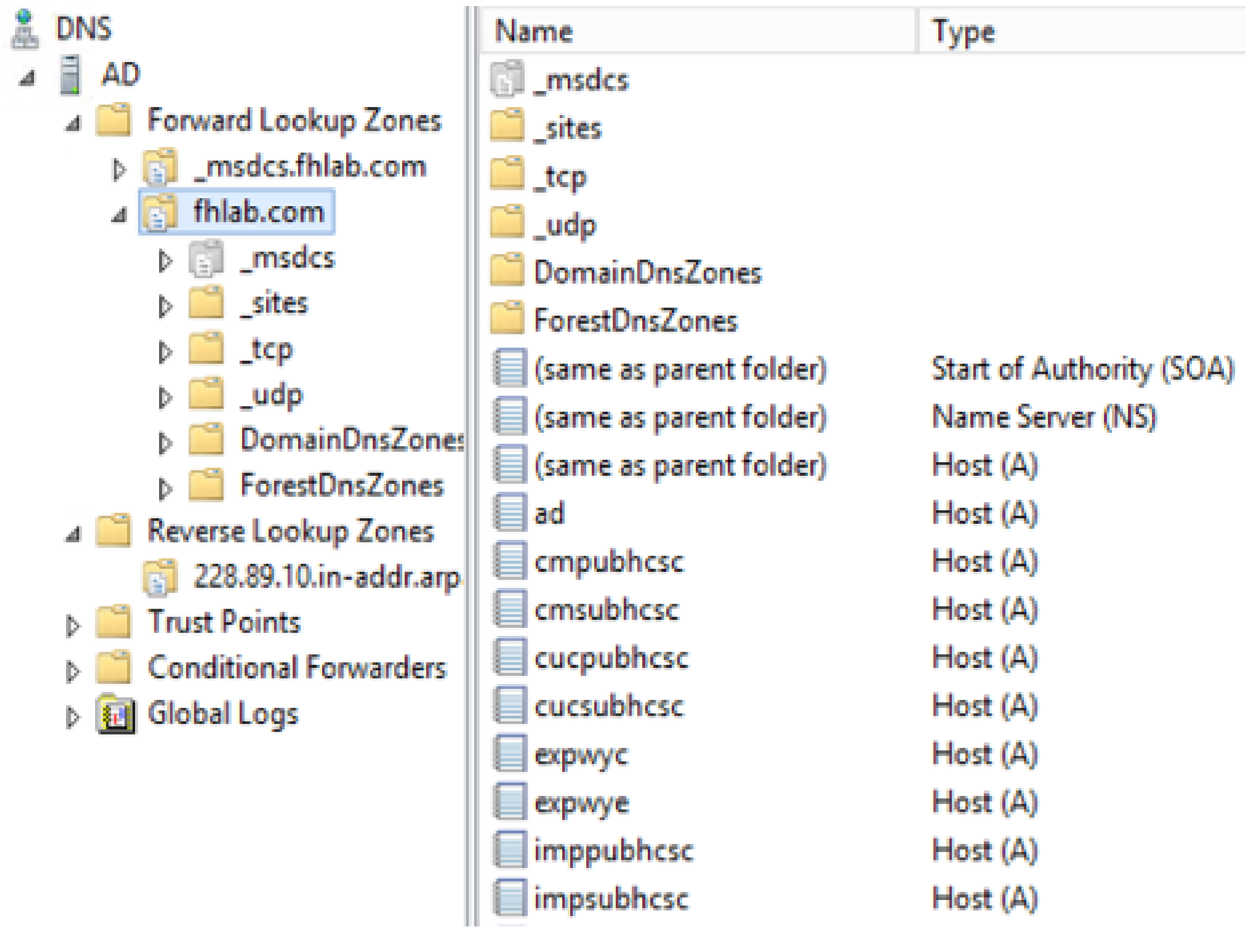
Avant d'installer ADFS3, ces rôles de serveur doivent déjà exister dans l'environnement :

Contrôleur de domaine · et DNS

·Tous les serveurs doivent être ajoutés en tant qu'enregistrements A avec leur enregistrement Pointer (type d'enregistrement DNS qui résout une adresse IP en un domaine ou un nom d'hôte)

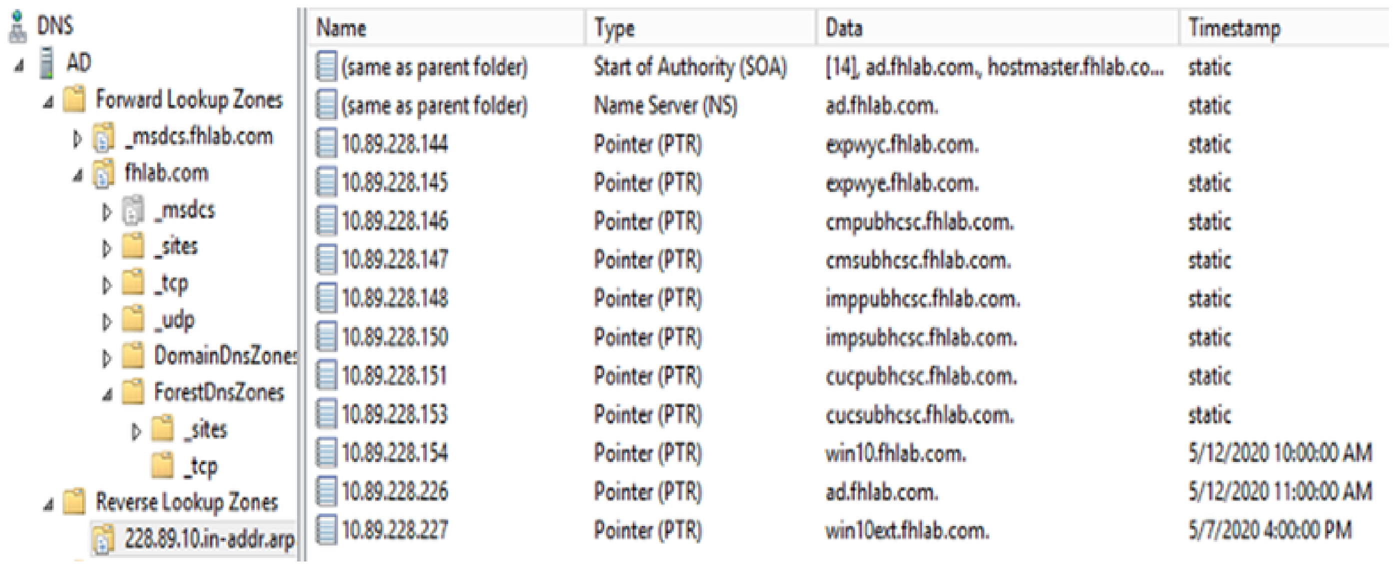
Enregistrements A

Dans fhlab.com. hosts cmpubhcsc, cmsubhcsc, cucpubhcsc, cucsubhcsc, expwyc, expwye, impubhcsc et imsubhcsc ont été ajoutés.



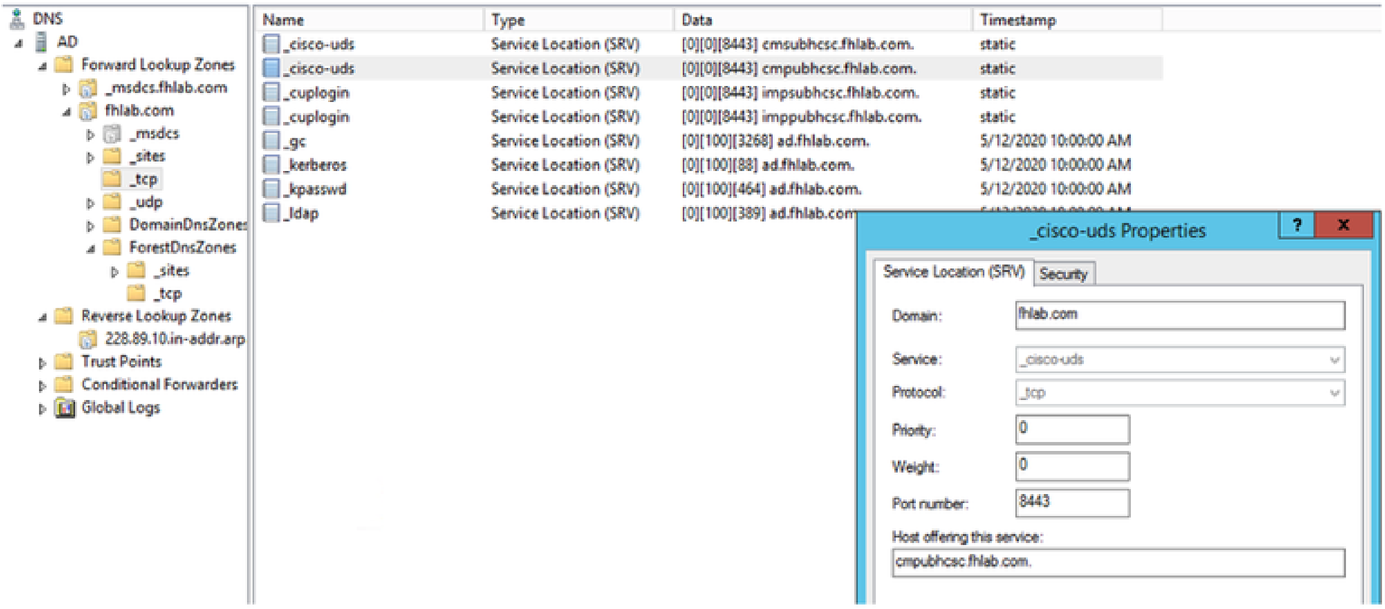
Name	Type
_msdcs	
_sites	
_tcp	
_udp	
DomainDnsZones	
ForestDnsZones	
(same as parent folder)	Start of Authority (SOA)
(same as parent folder)	Name Server (NS)
(same as parent folder)	Host (A)
ad	Host (A)
cmpubhcsc	Host (A)
cmsubhcsc	Host (A)
cucpubhcsc	Host (A)
cucsubhcsc	Host (A)
expwyc	Host (A)
expwye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

Enregistrements de pointeur (PTR)



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

Les enregistrements SRV doivent être en place pour 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

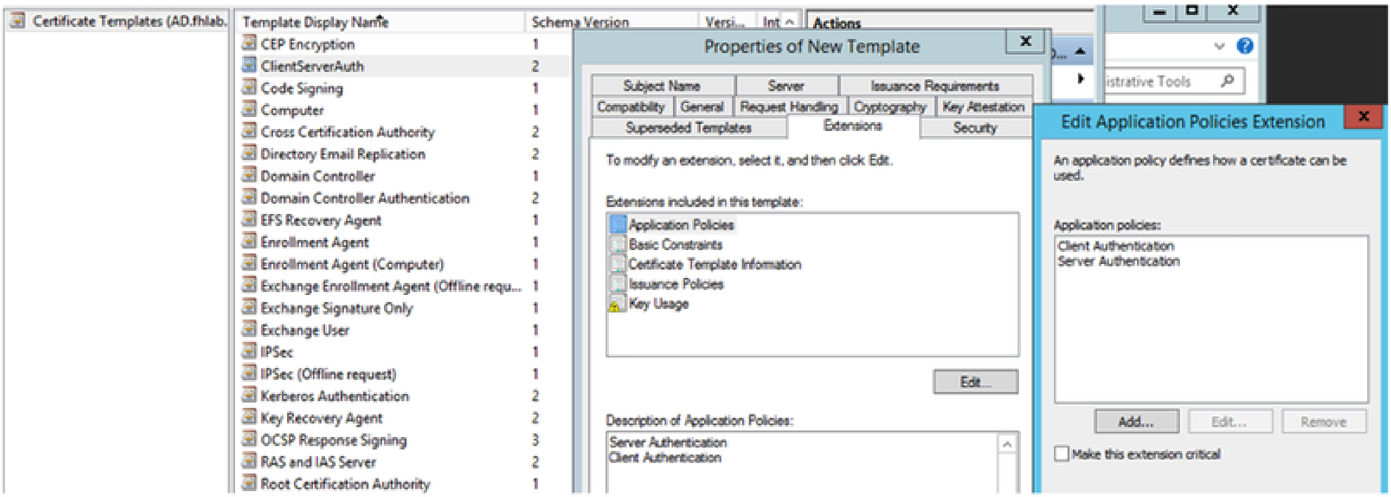
Weight: 0

Port number: 8443

Host offering this service: cmpubhcsc.fhlab.com.

- Autorité de certification racine (en supposant que les certificats seront signés par l'Autorité de certification d'entreprise)

Un modèle de certificat doit être créé en fonction du modèle de certificat du serveur Web, le premier est dupliqué, renommé et sous l'onglet Extensions, les stratégies d'application sont modifiées en ajoutant une stratégie d'application d'authentification du client. Ce modèle est nécessaire pour signer tous les certificats internes (CUCM, CUC, IMP et Expressway Core) dans un environnement LAB, l’autorité de certification interne peut également signer les demandes de signature de certificat (CSR) 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

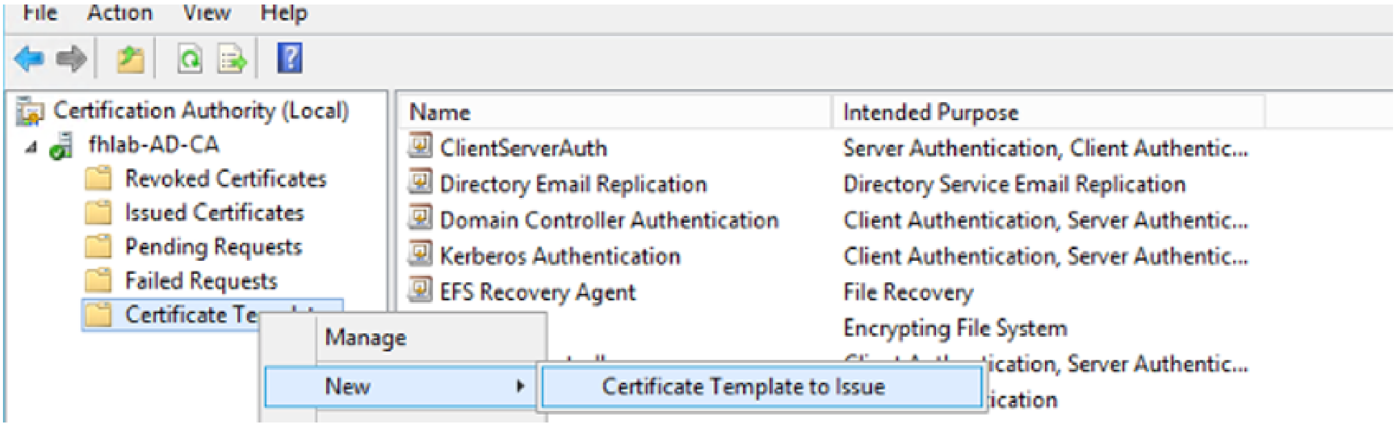
An application policy defines how a certificate can be used.

Application policies:

Client Authentication
Server Authentication

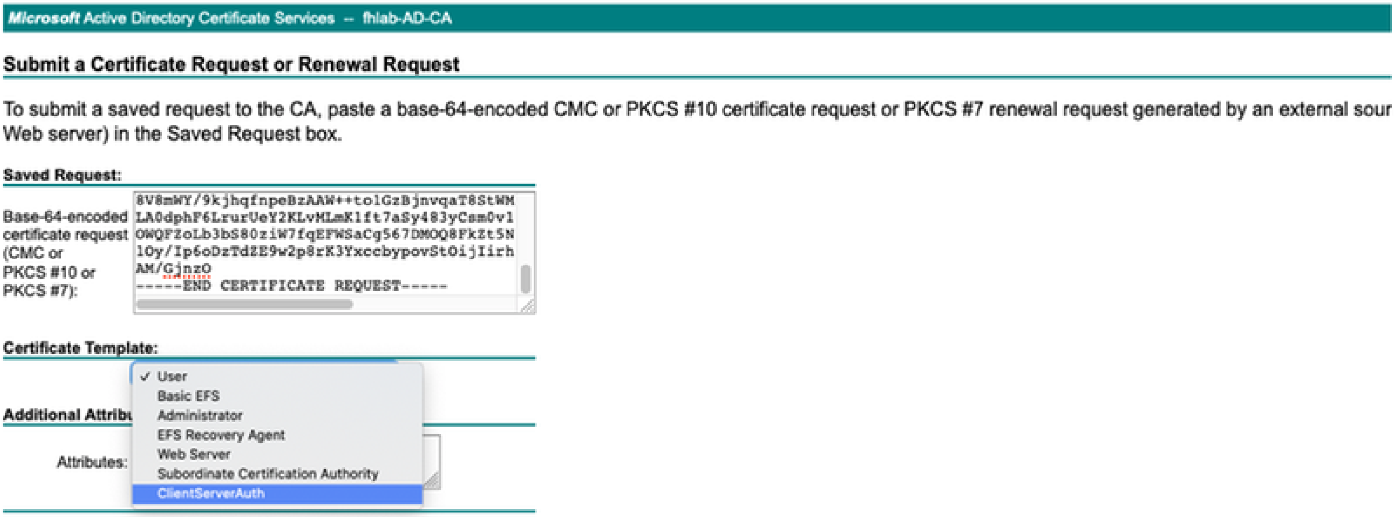
□ Make this extension critical

Le modèle créé doit être émis pour pouvoir signer 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

Sur le site Web des certificats de l'Autorité de certification, sélectionnez le modèle créé précédemment.


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):

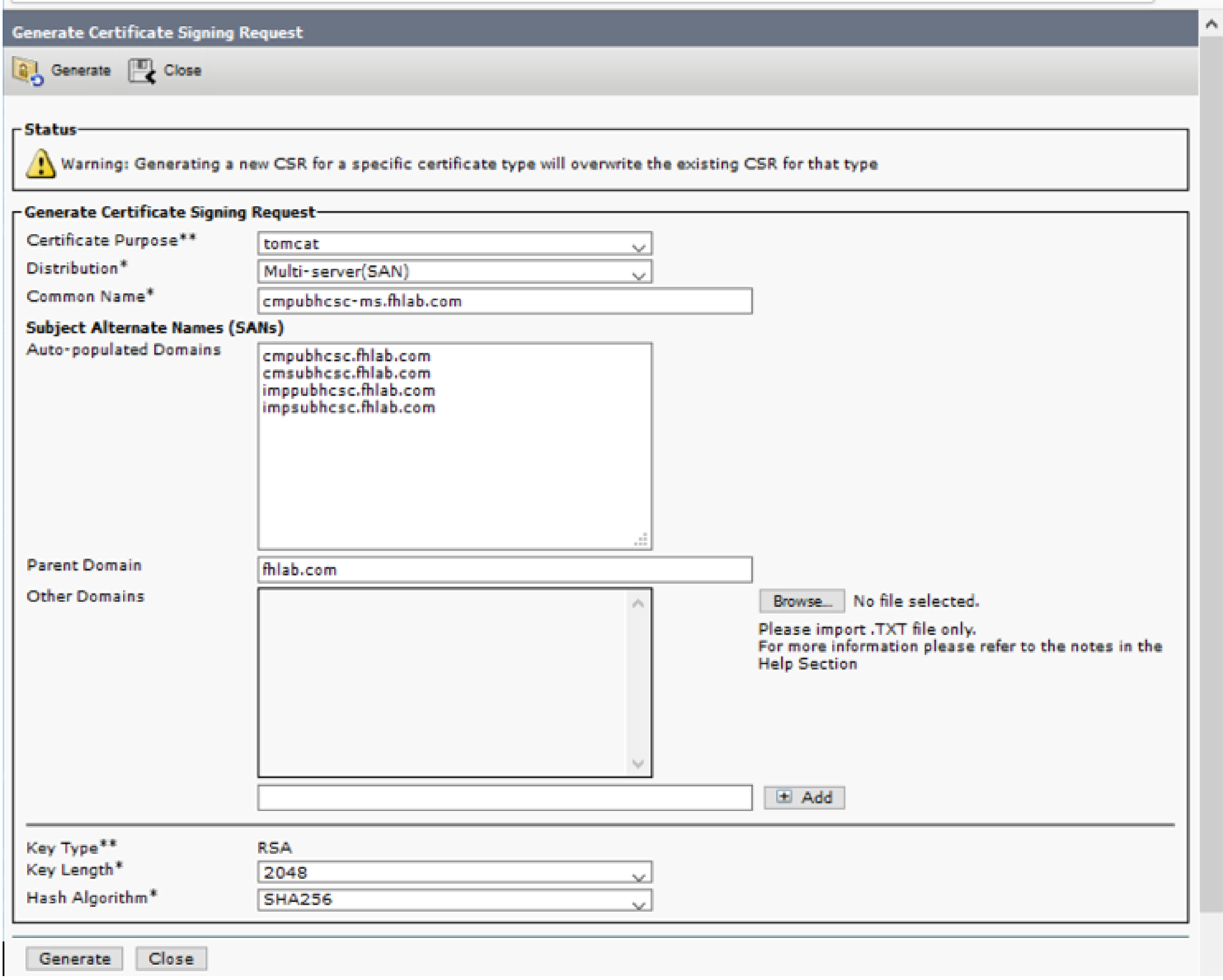
```
8V8mWY/9kjhqfnpeBzAAW++tolGzBjnvqaT8StWM
LA0dphF6LrurUeY2KLvMLmK1ft7aSy483yCsm0v1
OWQFZoLb3bS80ziW7fqEFWSaCg567DMOQ8FkZt5N
1Oy/Ip6oDzTdZE9w2p8rK3YxccbypovStOijIirh
AM/GjnzO
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Additional Attribu

Attributes:

CUCM, IMP et CUC Multi-Server CSR doivent être générés et signés par l'autorité de certification. L'objectif du certificat doit être défini.



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)

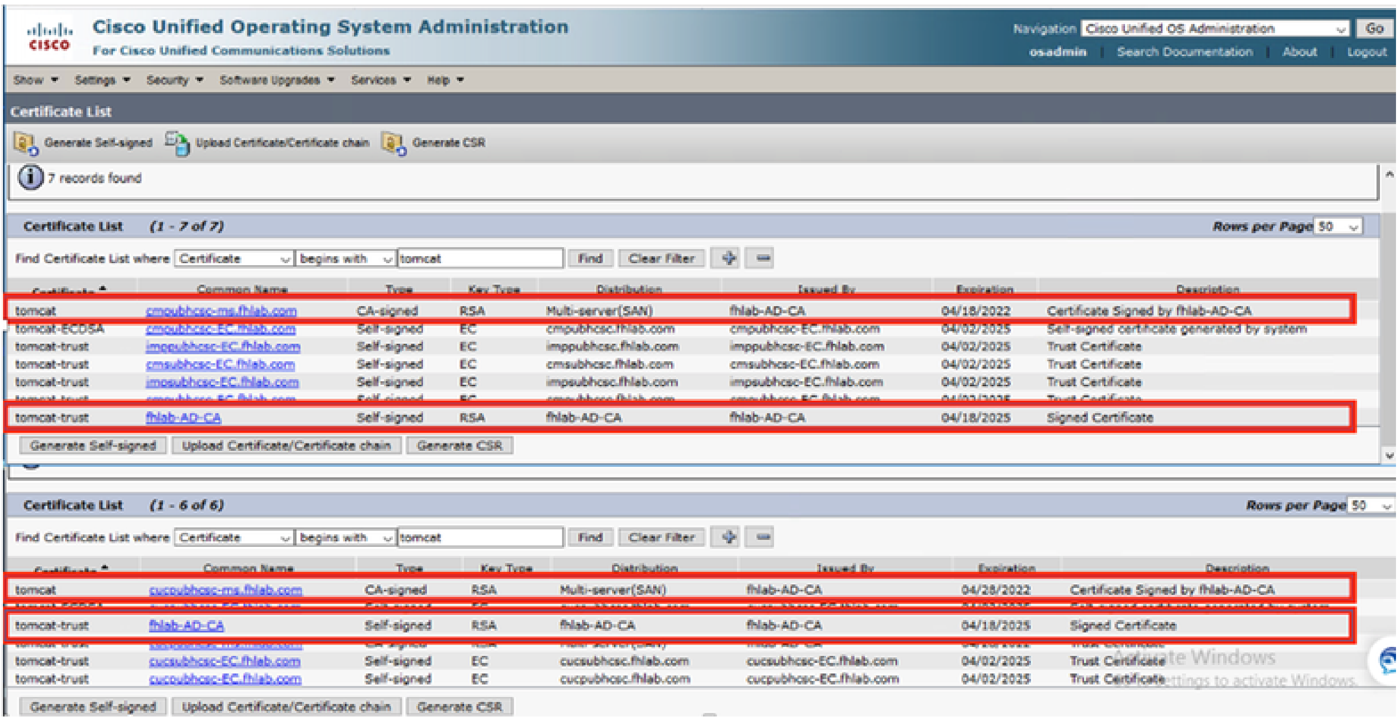
Auto-populated Domains	cmpubhcsc.fhlab.com cmsubhcsc.fhlab.com imppubhcsc.fhlab.com impsubhcsc.fhlab.com
Parent Domain	fhlab.com
Other Domains	

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

Le certificat racine CA doit être téléchargé vers Tomcat Trust et le certificat signé vers 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

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

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]	Self-signed	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

Activate Windows
Go to Settings to activate Windows.

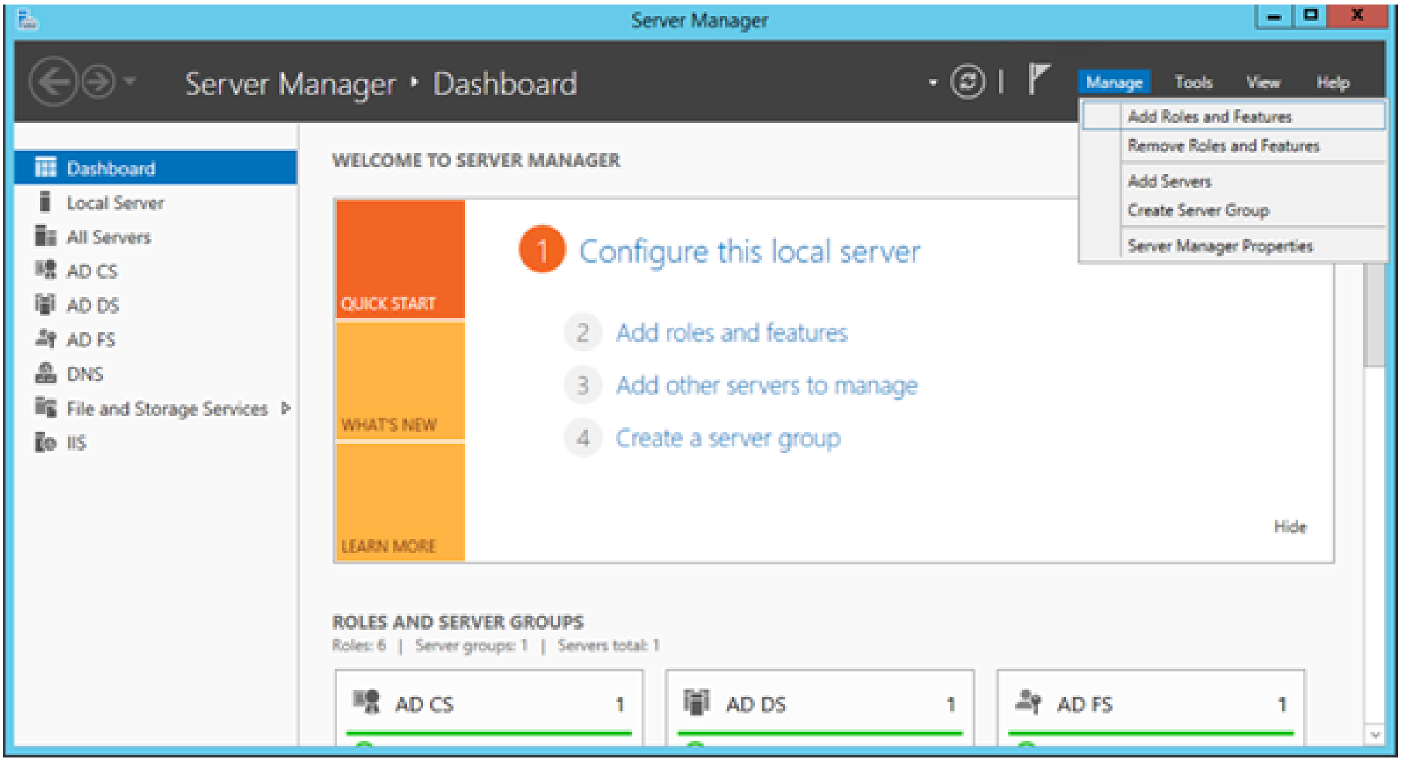
- IIS

Sinon, cette section va passer par l'installation de ces rôles. Sinon, ignorez cette section et accédez directement au téléchargement d'ADFS3 à partir de Microsoft.

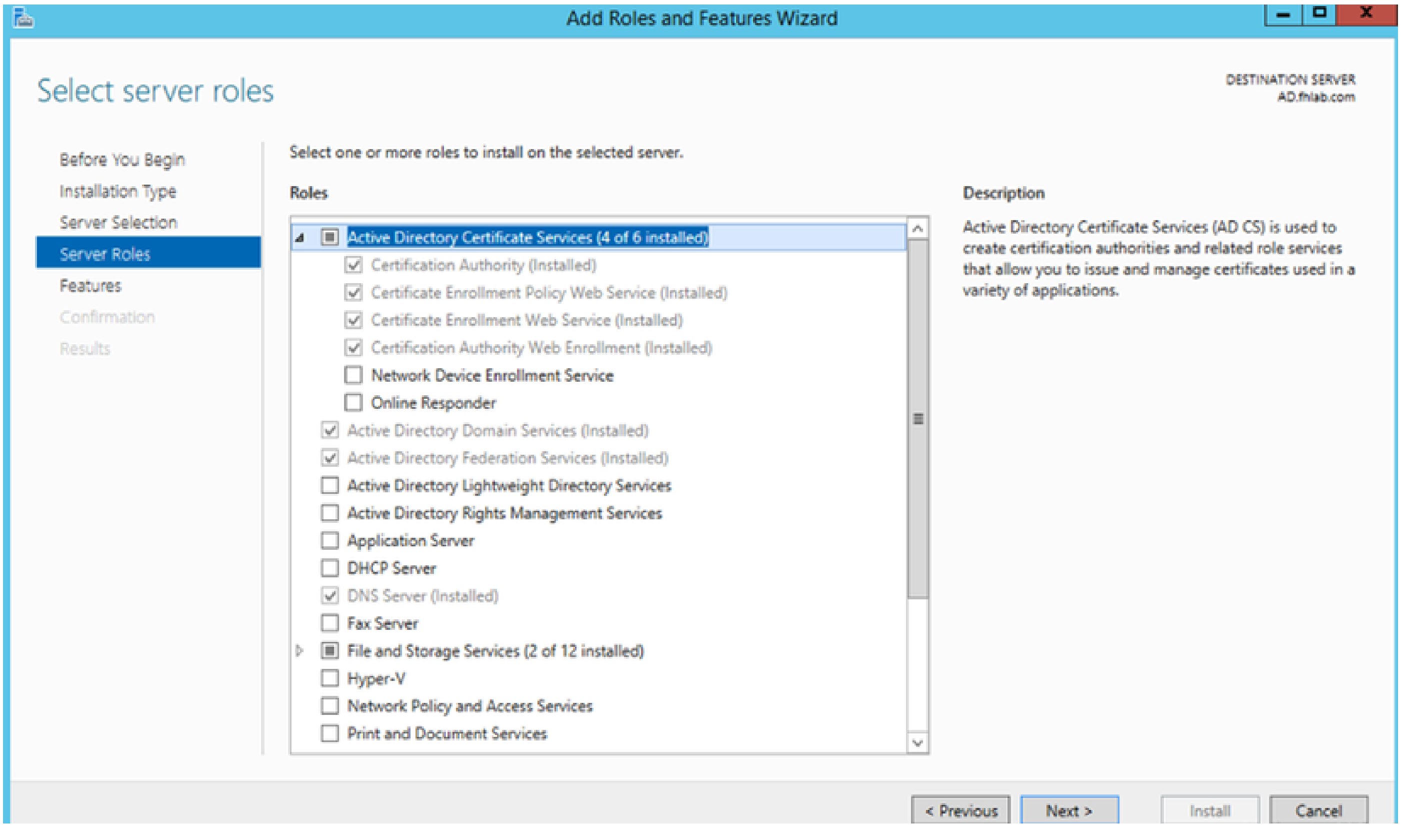
Après avoir installé Windows 2012 R2 avec DNS, faites passer le serveur à un contrôleur de domaine.

La tâche suivante consiste à installer les services de certificats Microsoft.

Accédez à Gestionnaire de serveur et ajoutez un nouveau rôle :



Sélectionnez le rôle **Services de certificats 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

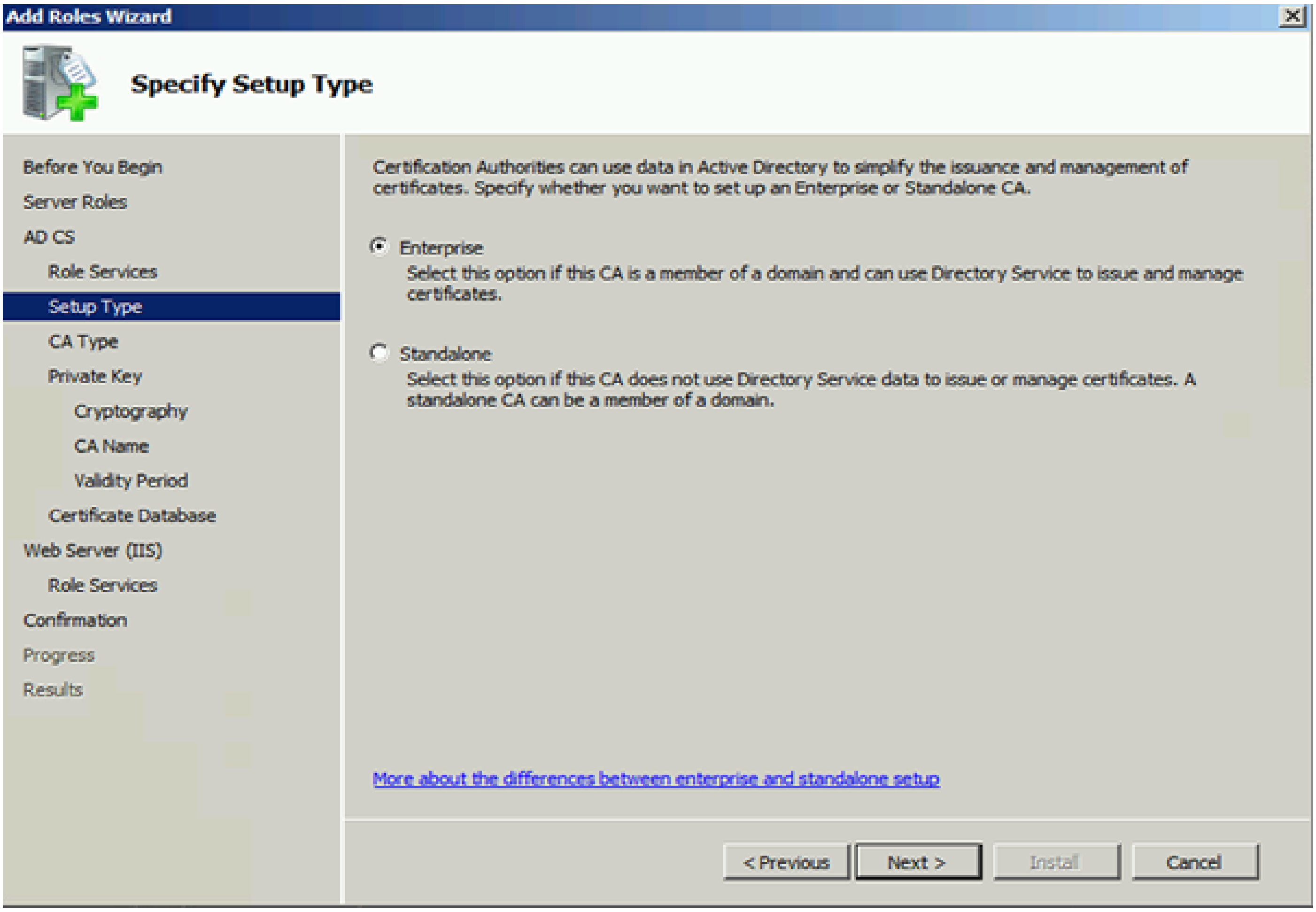
Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Déployez d'abord ces services - Service Web de stratégie d'inscription de certificat d'autorité de certification. Une fois ces deux rôles installés, configurez-les, puis installez **Certificate Enrollment**

Web Service et **Certificate Authority Web Enrollment**. Configurez-les.

Des fonctions et services de rôle supplémentaires requis, tels que IIS, seront également ajoutés lors de l'installation de l'autorité de certification.

Selon votre déploiement, vous pouvez sélectionner Entreprise ou Autonome.



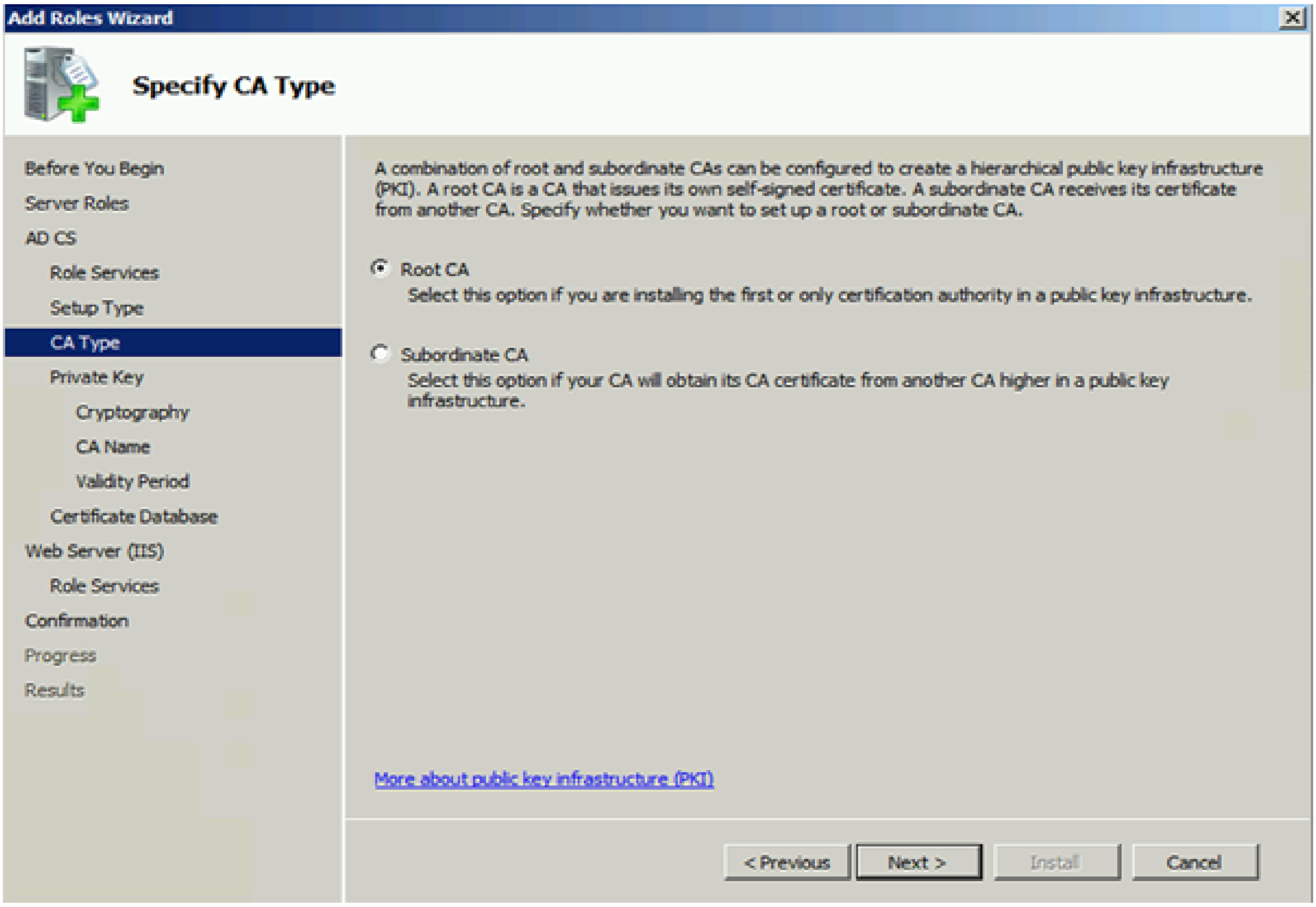
Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

● 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

Pour le type d'autorité de certification, vous pouvez sélectionner Autorité de certification racine ou Autorité de certification subordonnée. Si aucune autre autorité de certification n'est déjà en cours d'exécution dans l'organisation, sélectionnez **Autorité de certification racine**.



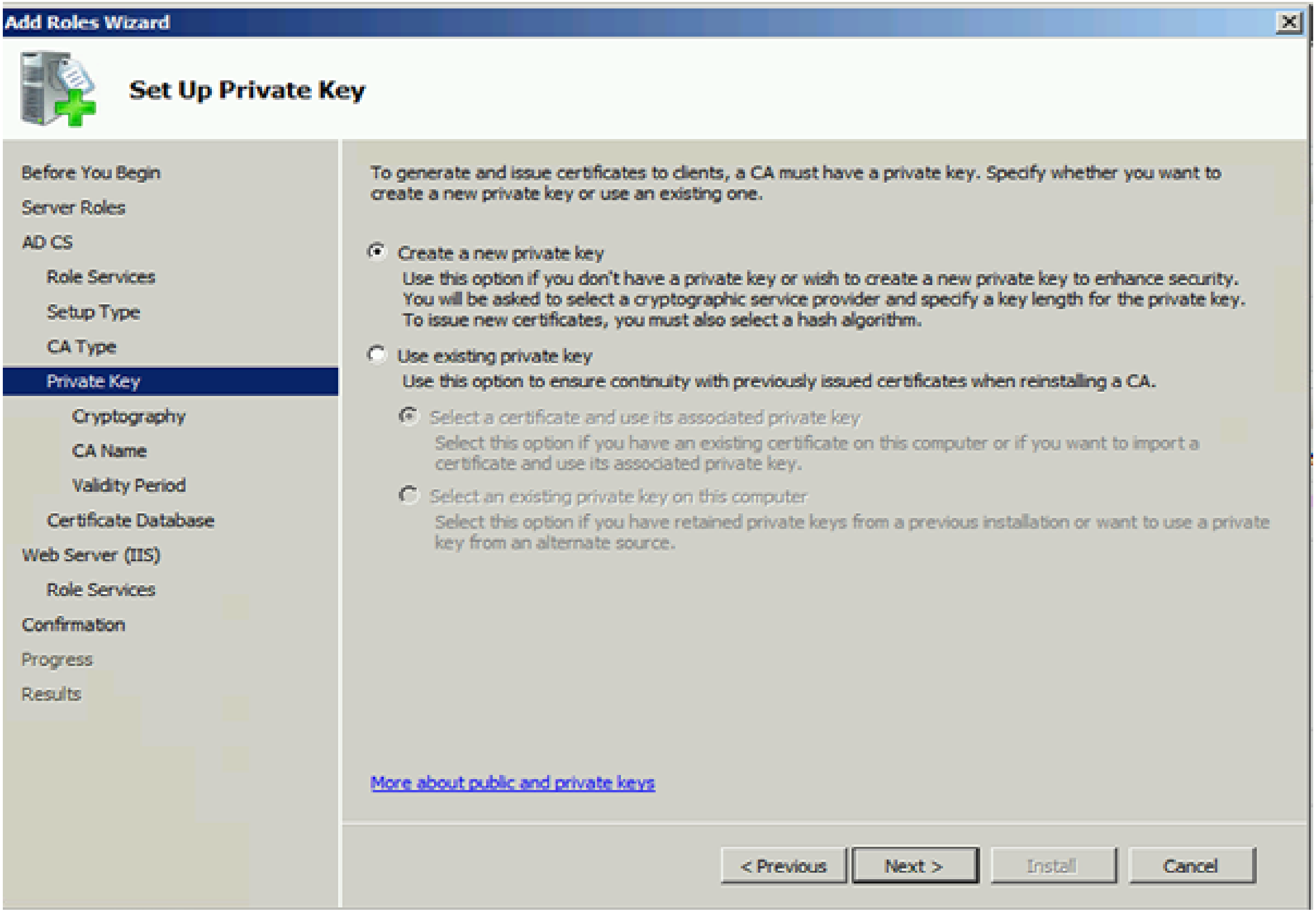
Specify CA Type

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.

L'étape suivante consiste à créer une clé privée pour votre 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.

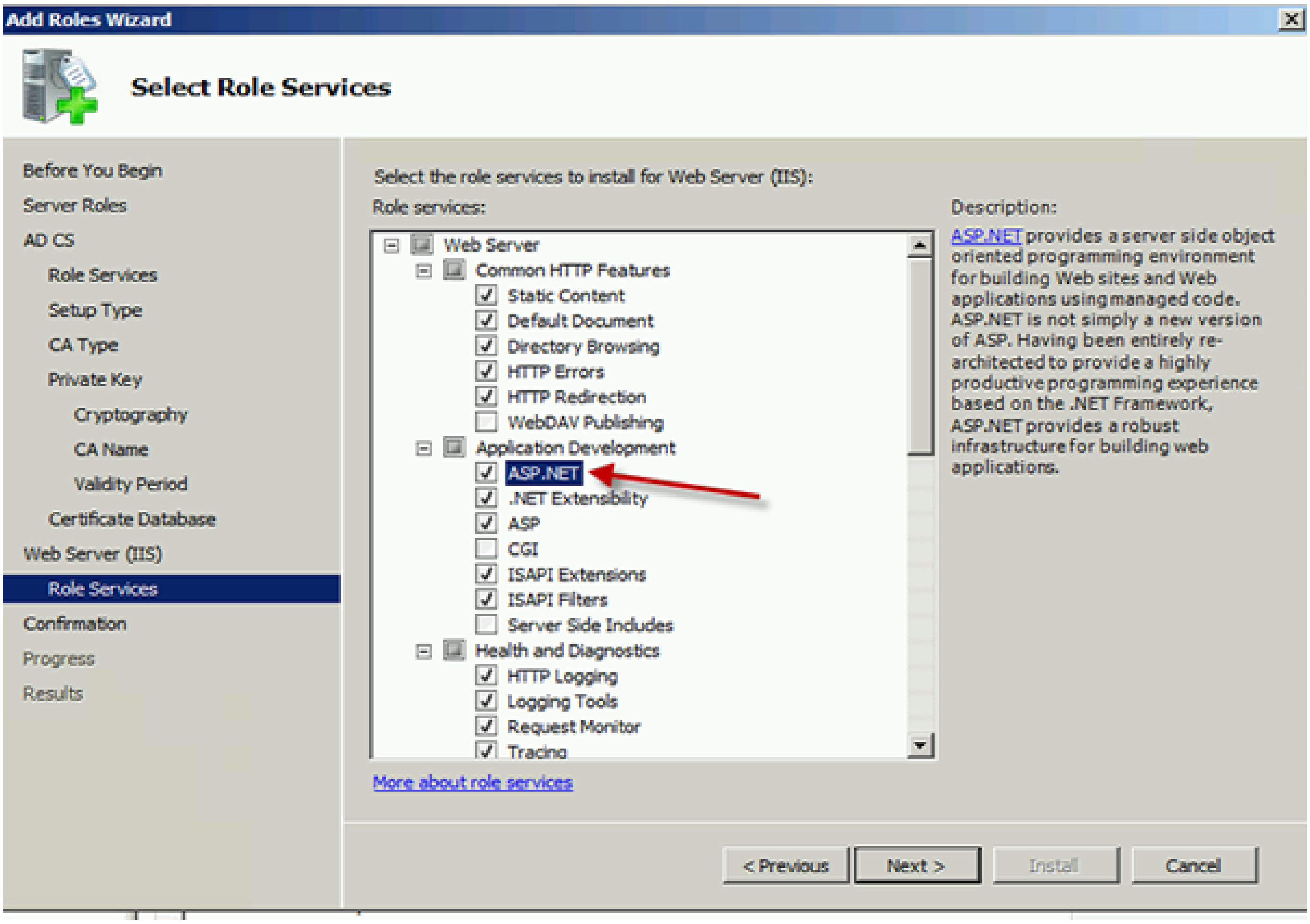
○ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

● 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.

Cette étape n'est nécessaire que si vous installez ADFS3 sur un Windows Server 2012 distinct.

Après avoir configuré l'autorité de certification, les services de rôle pour IIS doivent être configurés. Ceci est nécessaire pour l'inscription Web sur l'AC. Pour la plupart des déploiements ADFS, un rôle supplémentaire dans IIS, cliquez sur **ASP.NET** sous Développement d'applications est requis.



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

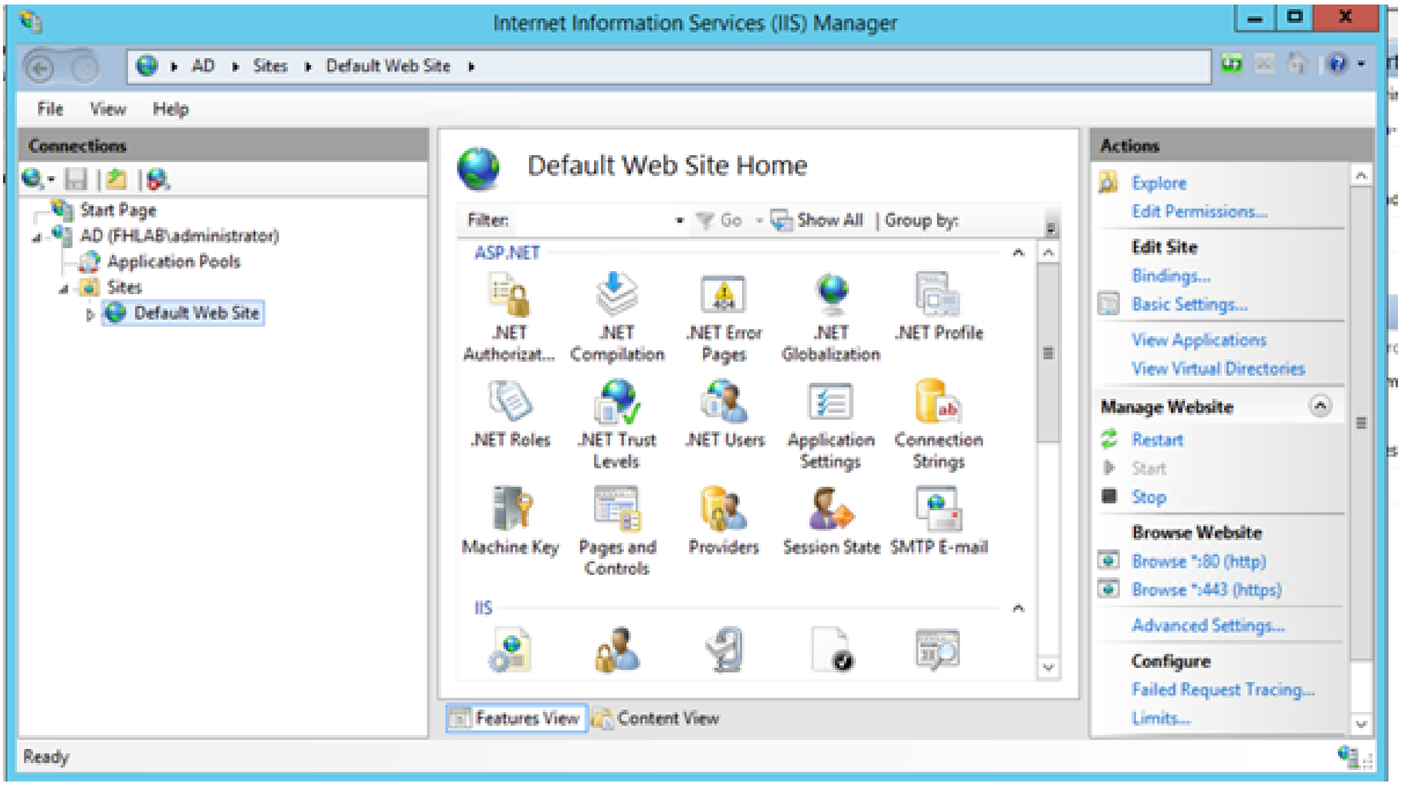
Role services:

- 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

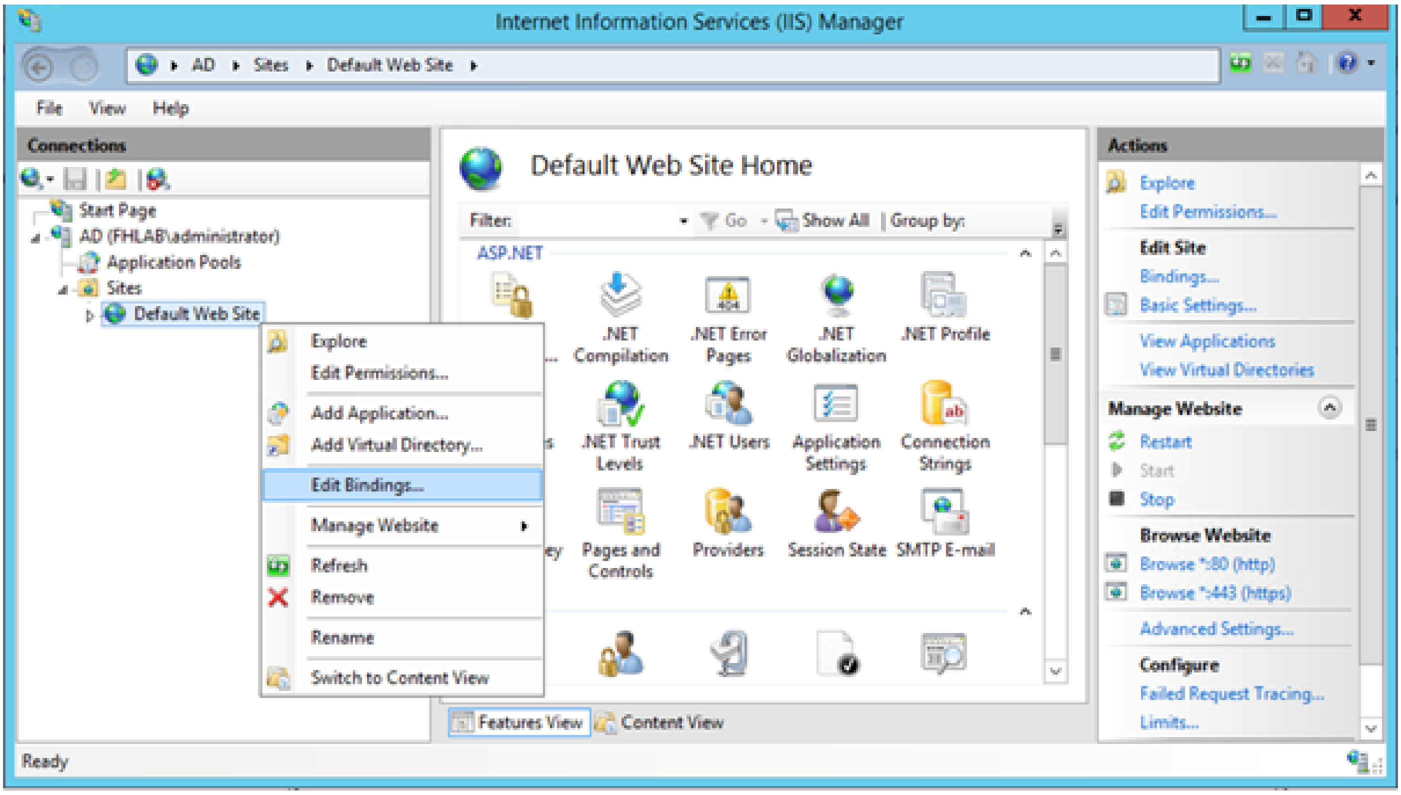
Description:

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.

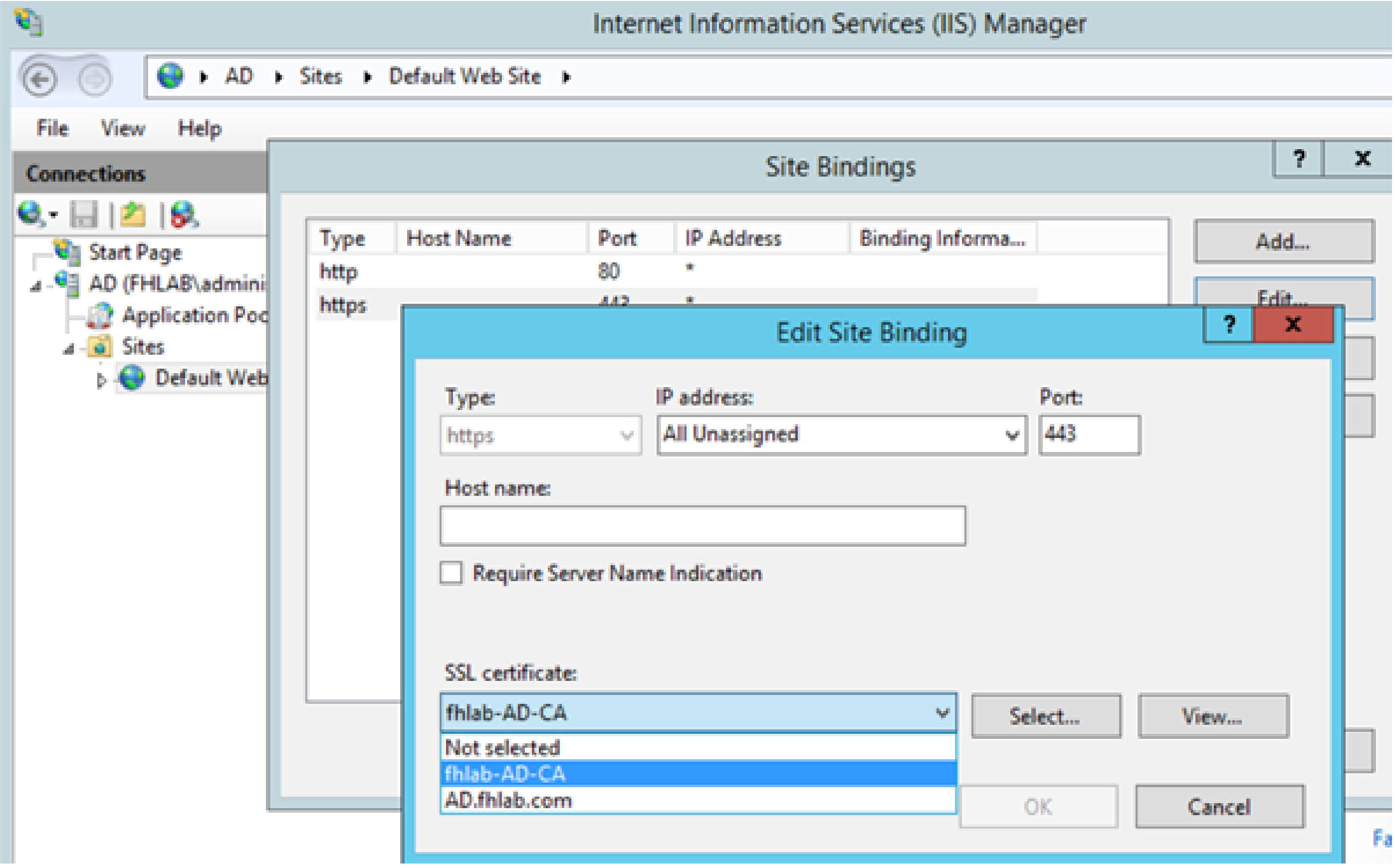
Dans le Gestionnaire de serveurs, cliquez sur **Serveur Web > IIS**, puis cliquez avec le bouton droit sur **Site Web par défaut**. La liaison doit être modifiée pour autoriser également HTTPS en plus du protocole HTTP. Ceci est fait pour prendre en charge HTTPS.



Sélectionnez **Modifier les liaisons**.



Ajoutez une nouvelle liaison de site et sélectionnez **HTTPS** comme type. Pour le certificat SSL, sélectionnez le certificat du serveur qui doit avoir le même nom de domaine complet que votre serveur AD.



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

Type: https

IP address: All Unassigned

Port: 443

Host name:

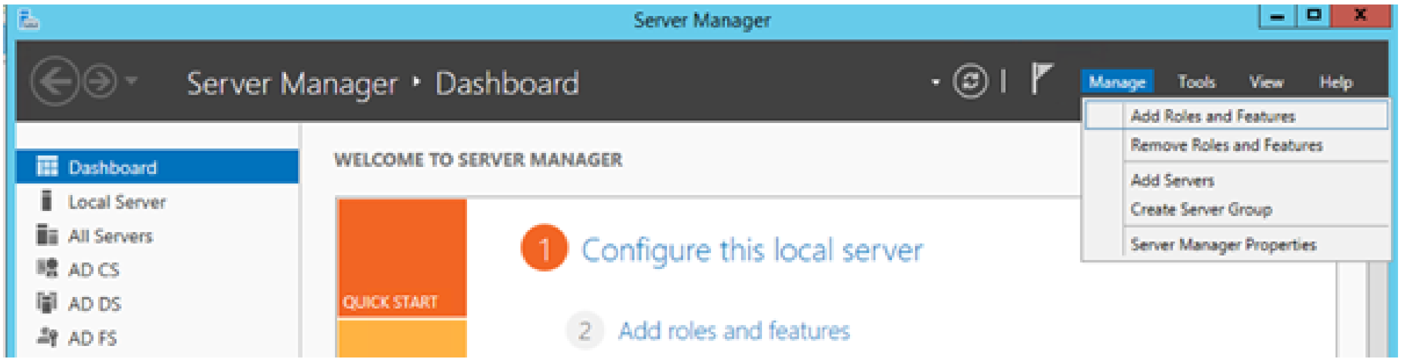
☐ Require Server Name Indication

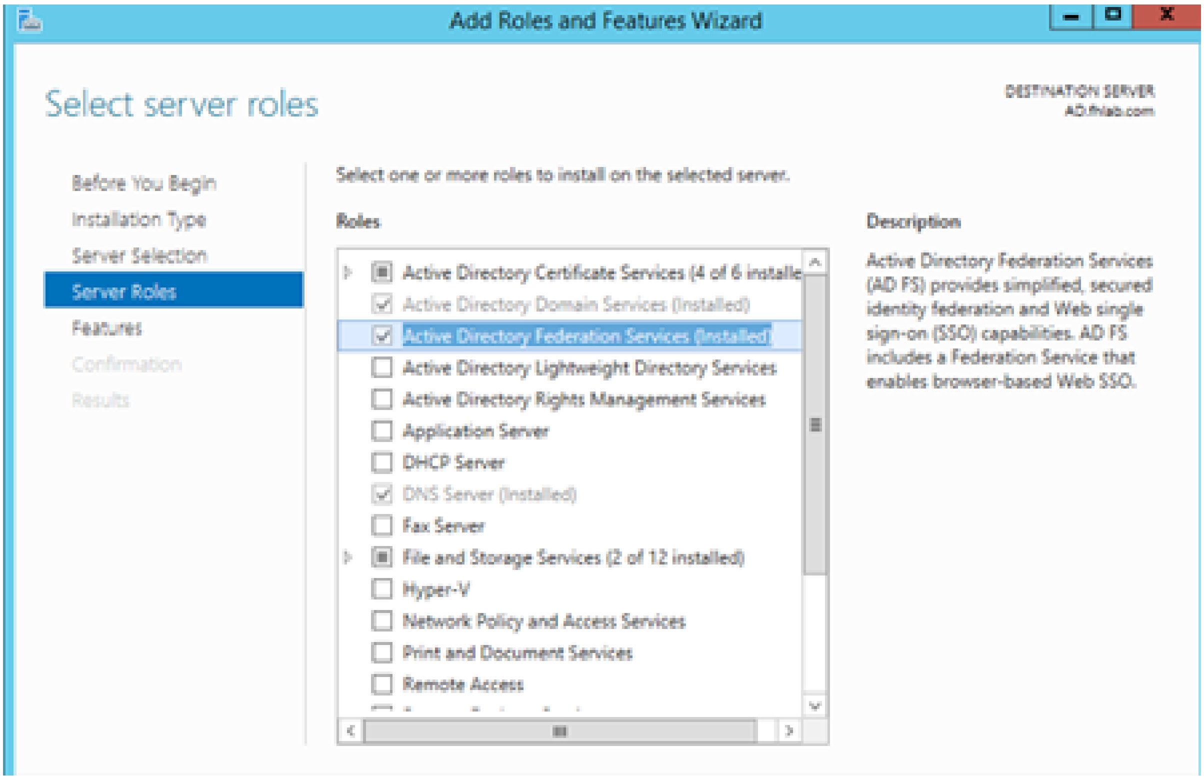
SSL certificate: fhlab-AD-CA

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

Tous les rôles requis sont installés dans l'environnement. Vous pouvez donc maintenant installer les services ADFS3 Active Directory Federation Services (sur Windows Server 2012).

Pour le rôle de serveur, accédez à **Gestionnaire de serveur > Gérer > Ajouter des rôles et des fonctionnalités de serveur**, puis sélectionnez **Services de fédération Active Directory** si vous installez le PCI à l'intérieur du réseau du client, sur le réseau local privé.





Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
AD.fhlab.com

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

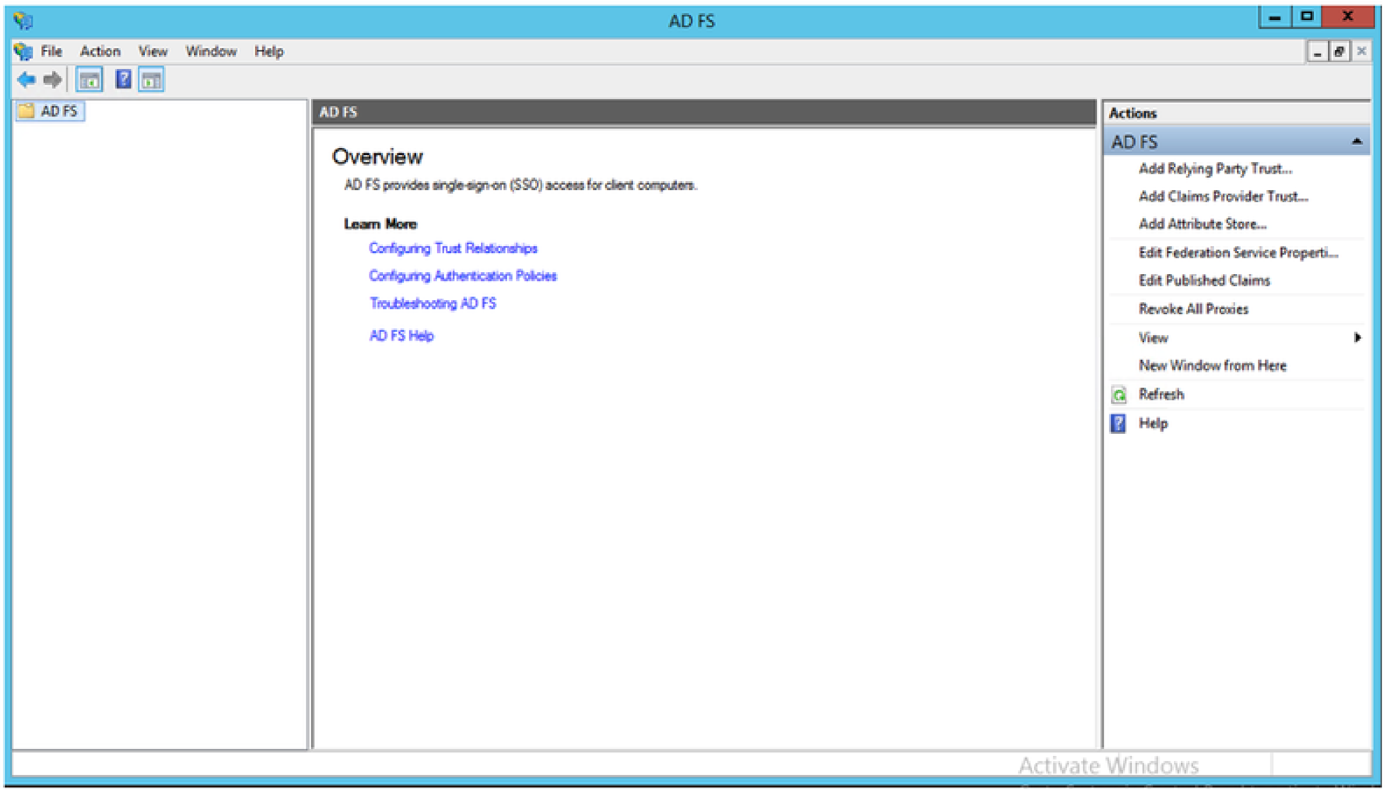
Roles

- ▣ 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.

Une fois l'installation terminée, vous pouvez l'ouvrir à partir de la barre des tâches ou du menu Démarrer.



AD FS

Overview

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

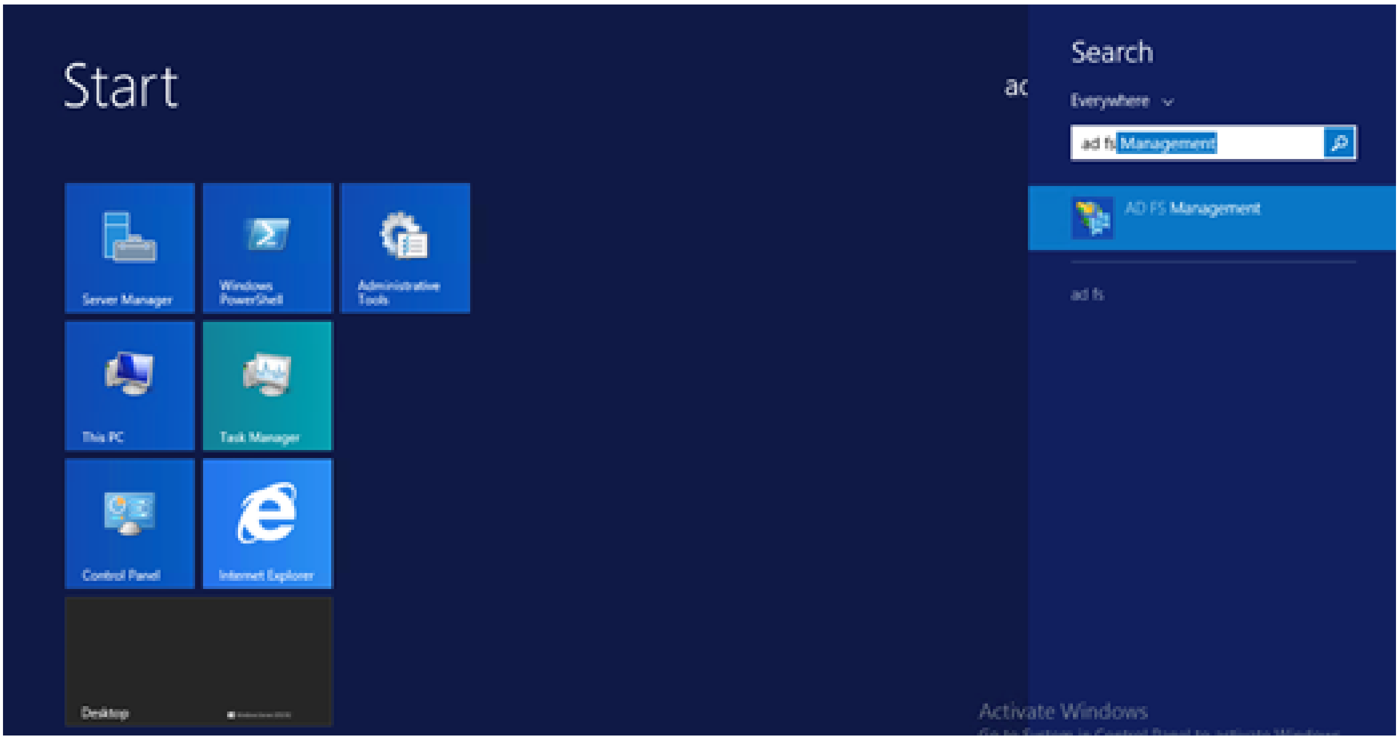
Learn More

- Configuring Trust Relationships
- Configuring Authentication Policies
- Troubleshooting AD FS
- AD FS Help

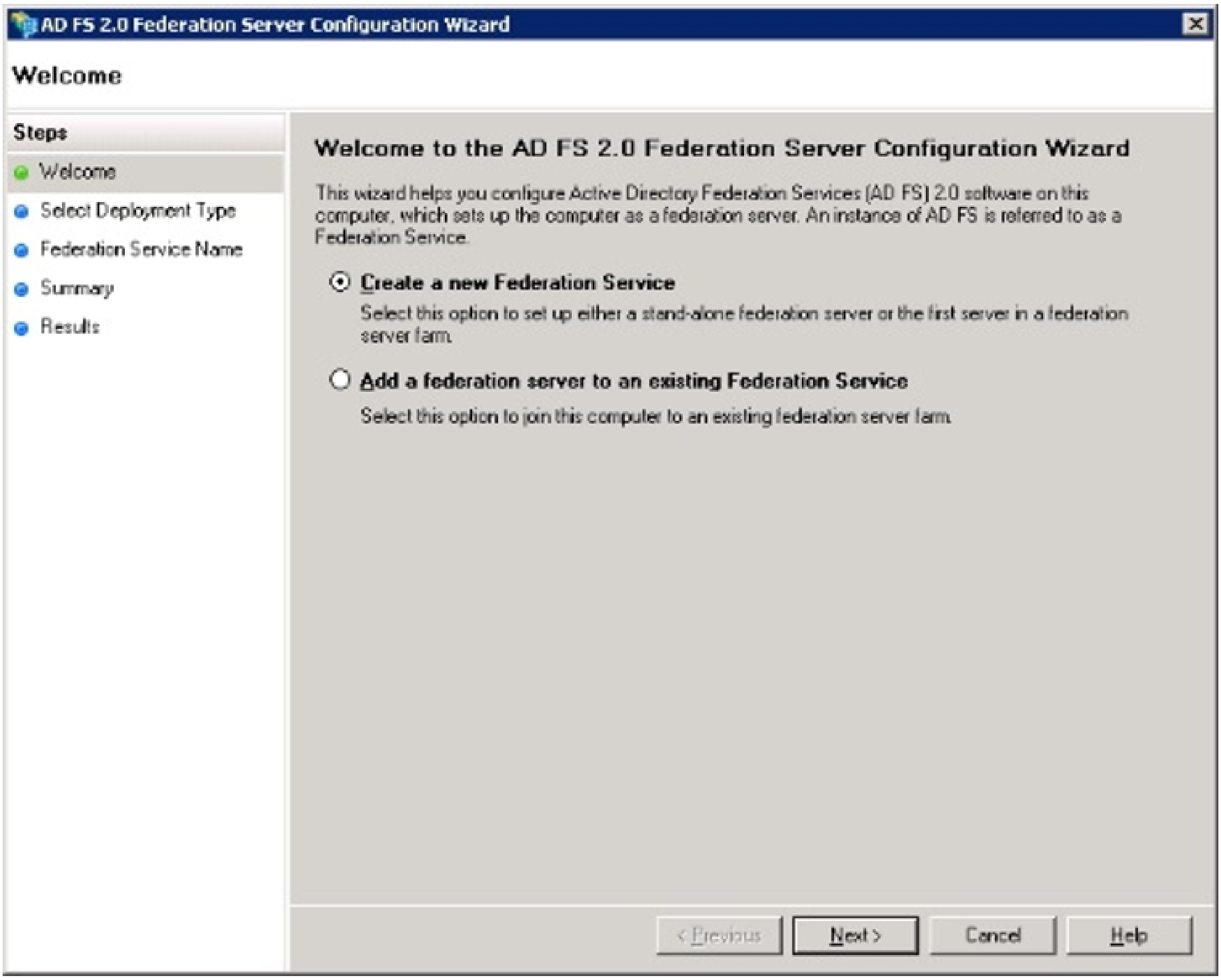
Configuration initiale ADFS3

Cette section va passer par l'installation d'un nouveau serveur de fédération autonome, mais elle peut également être utilisée pour l'installer sur un contrôleur de domaine

Sélectionnez **Windows** et tapez **AD FS Management** afin de lancer la console de gestion ADFS comme indiqué dans l'image.



Sélectionnez l'option **Assistant Configuration du serveur de fédération AD FS 3.0** afin de démarrer la configuration de votre serveur ADFS. Ces captures d'écran représentent les mêmes étapes dans 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.

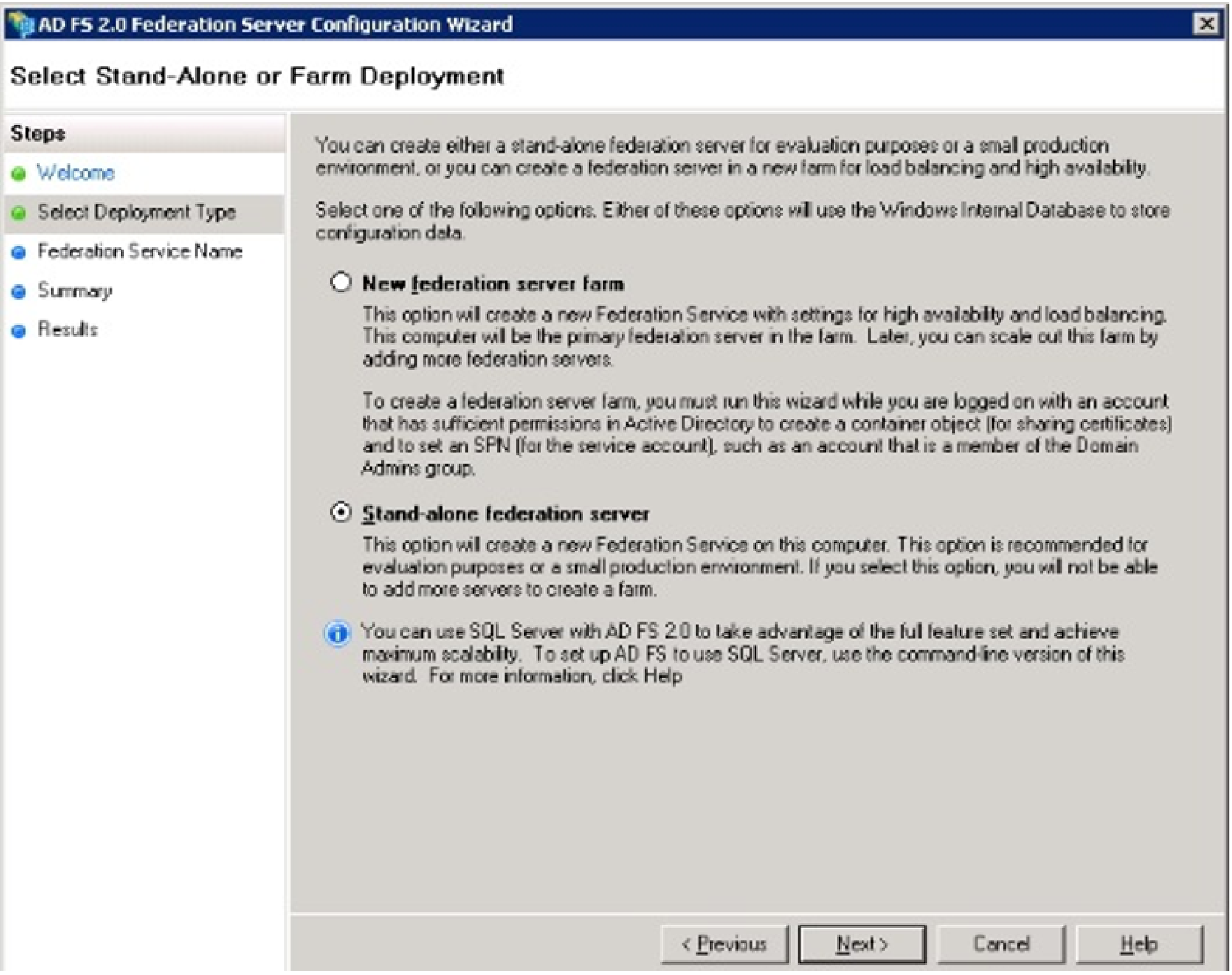
● Create a new Federation Service

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.

Sélectionnez Créer un nouveau **service de fédération** et cliquez sur **Suivant.**



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.

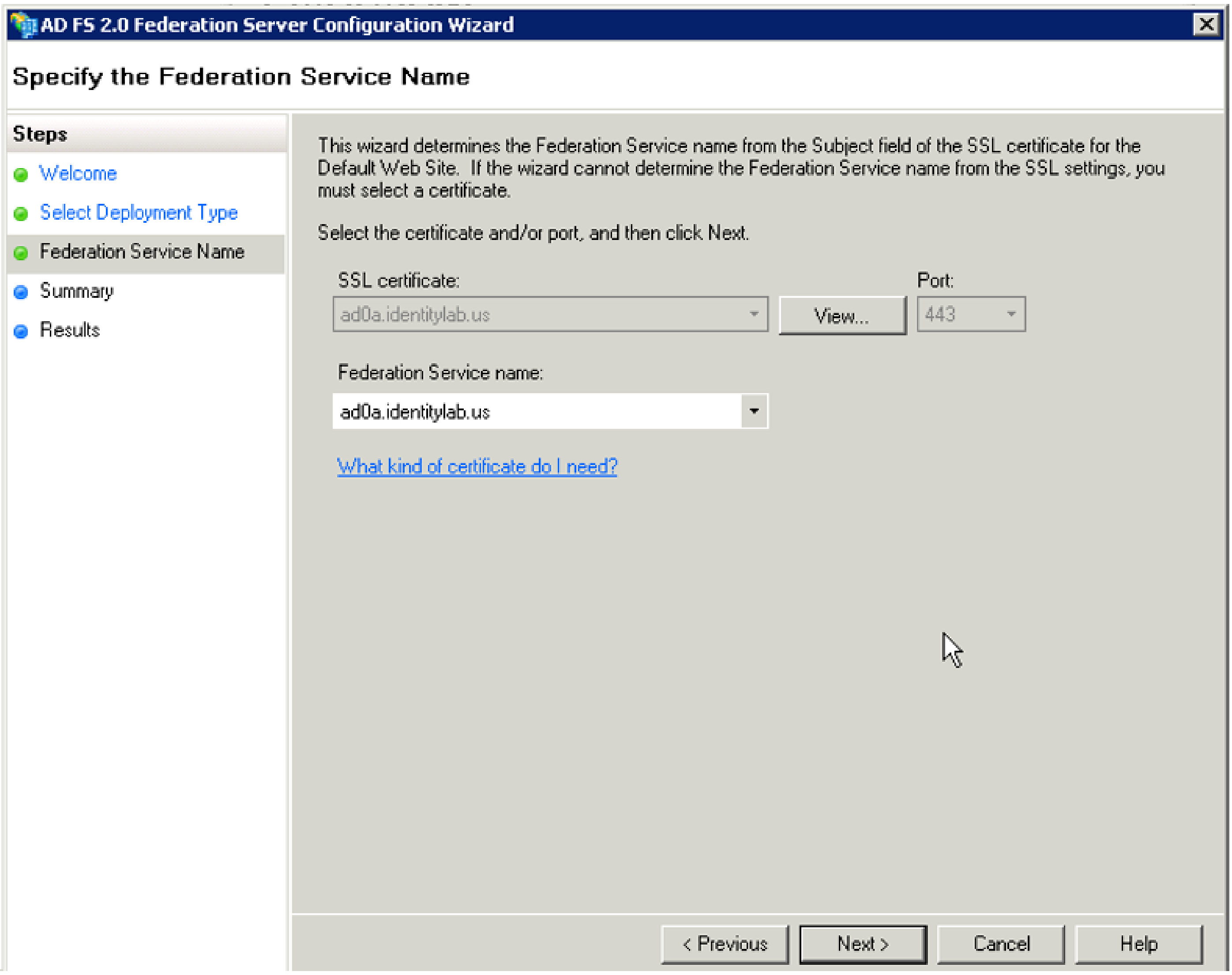
To create a federation server farm, you must run this wizard while you are logged on with an account that has sufficient permissions in Active Directory to create a container object (for sharing certificates) and to set an SPN (for the service account), such as an account that is a member of the Domain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

Sélectionnez Serveur de fédération autonome et cliquez sur **Suivant** comme indiqué dans l'image.



AD FS 2.0 Federation Server Configuration Wizard

Specify the Federation Service Name

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

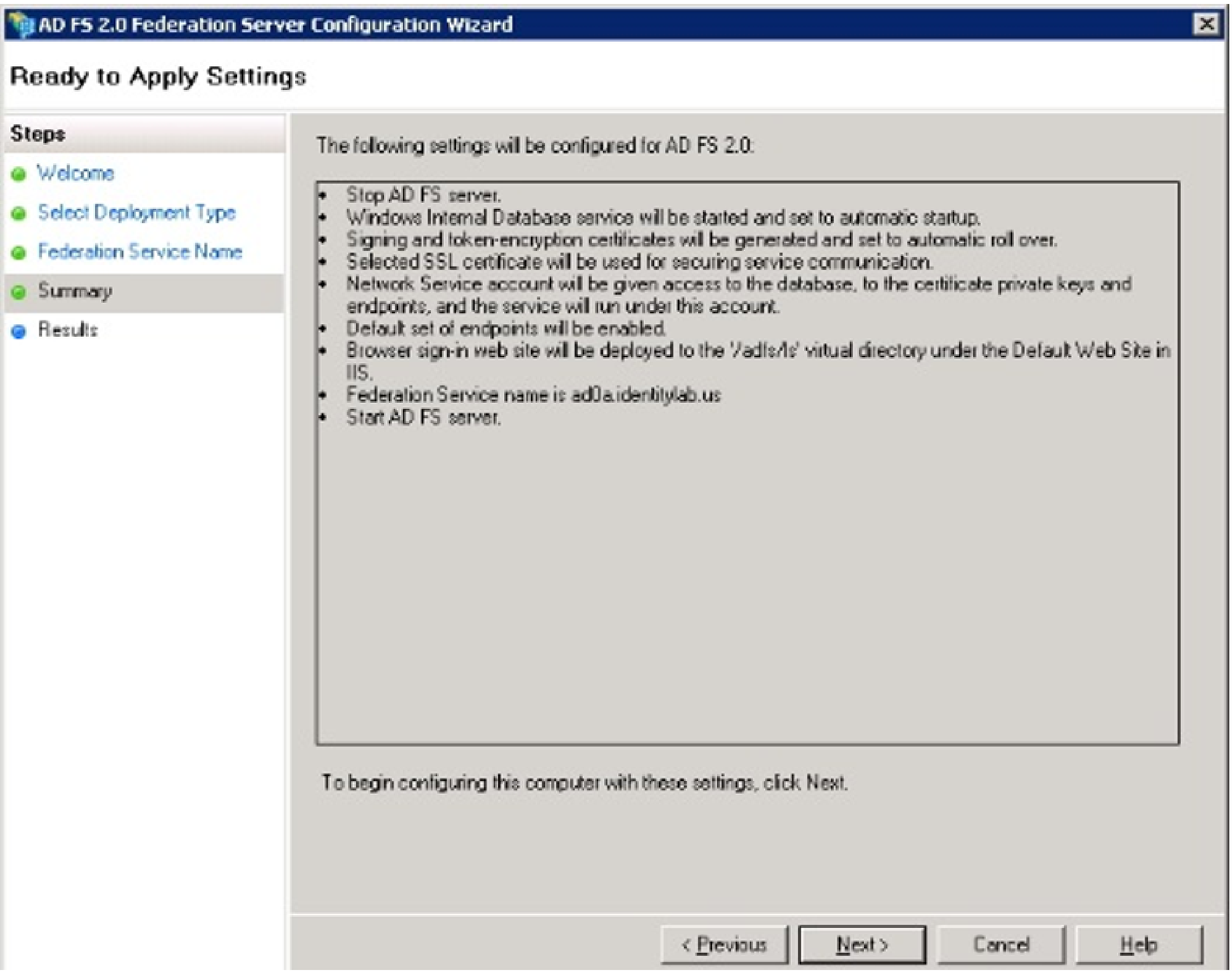
Select the certificate and/or port, and then click Next.

SSL certificate: ad0a.identitylab.us

Port: 443

Federation Service name: ad0a.identitylab.us

Sous Certificat SSL, sélectionnez le certificat auto-signé dans la liste. Le nom du service de fédération est renseigné automatiquement. Cliquez sur **Next** (Suivant).

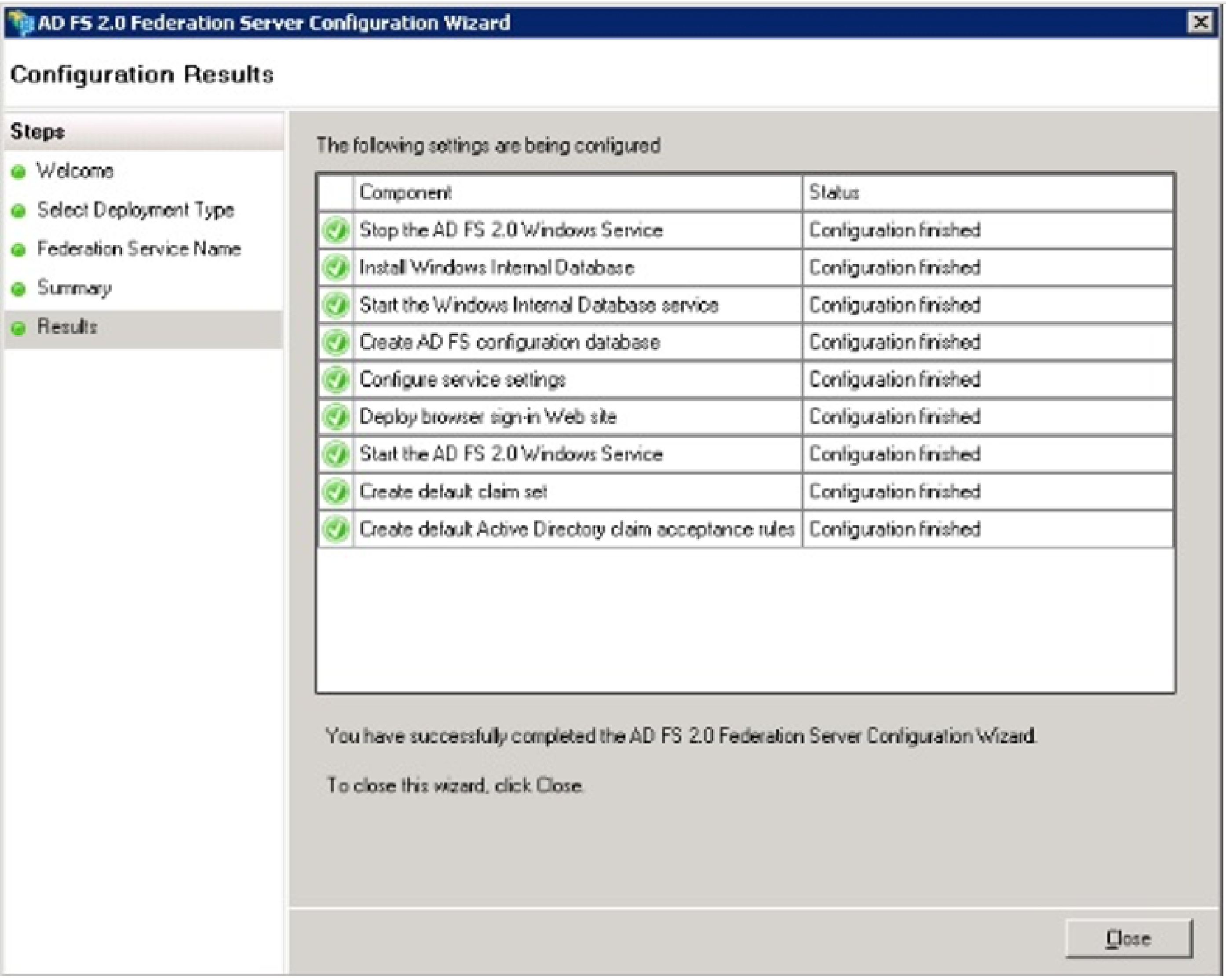


The following settings will be configured for AD FS 2.0:

- 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.

Vérifiez les paramètres et cliquez sur **Suivant** pour les appliquer.



AD FS 2.0 Federation Server Configuration Wizard

Configuration Results

Steps

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

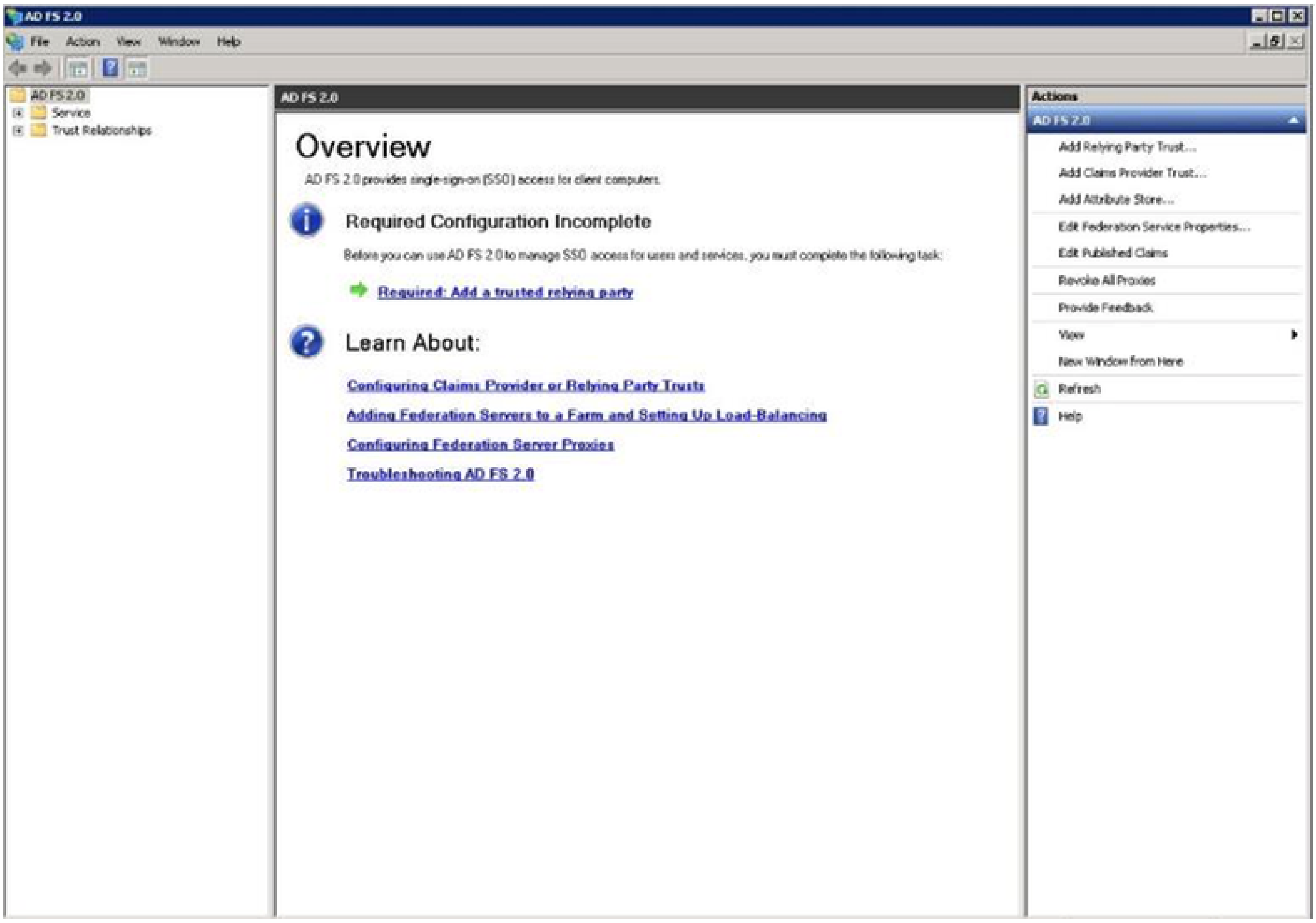
The following settings are being configured

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

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

To close this wizard, click Close.

Confirmez que tous les composants ont été terminés et cliquez sur **Fermer** pour terminer l'Assistant et revenir à la console de gestion principale. Cela pourrait prendre quelques minutes.



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

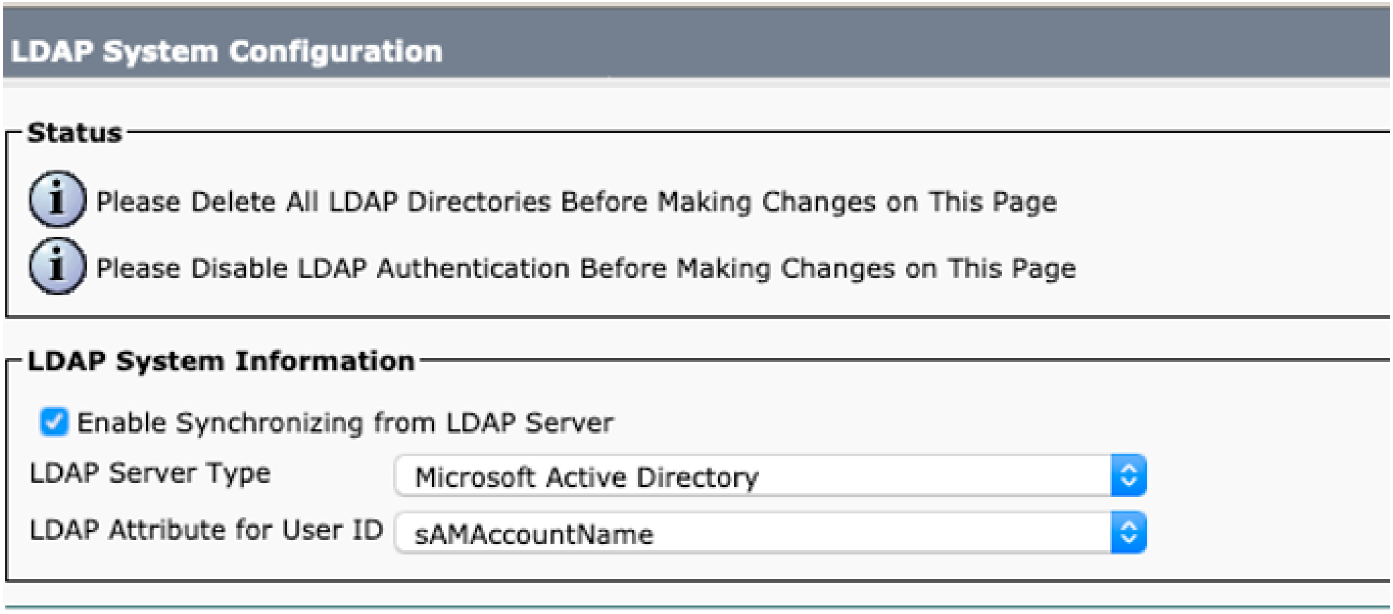
Troubleshooting AD FS 2.0

ADFS est désormais activé et configuré en tant que fournisseur d'identité (IdP). Ensuite, vous devez ajouter CUCM en tant que partenaire de confiance. Avant de pouvoir faire cela, vous devez d'abord effectuer une configuration dans l'administration CUCM.

Configurer SSO sur CUCM avec ADFS

Configuration LDAP

Le cluster doit être intégré à LDAP avec Active Directory et l'authentification LDAP doit être configurée avant d'aller plus loin. Accédez à **l'onglet Système > Système LDAP** comme indiqué dans l'image.



LDAP System Configuration

Status

Please Delete All LDAP Directories Before Making Changes on This Page

Please Disable LDAP Authentication Before Making Changes on This Page

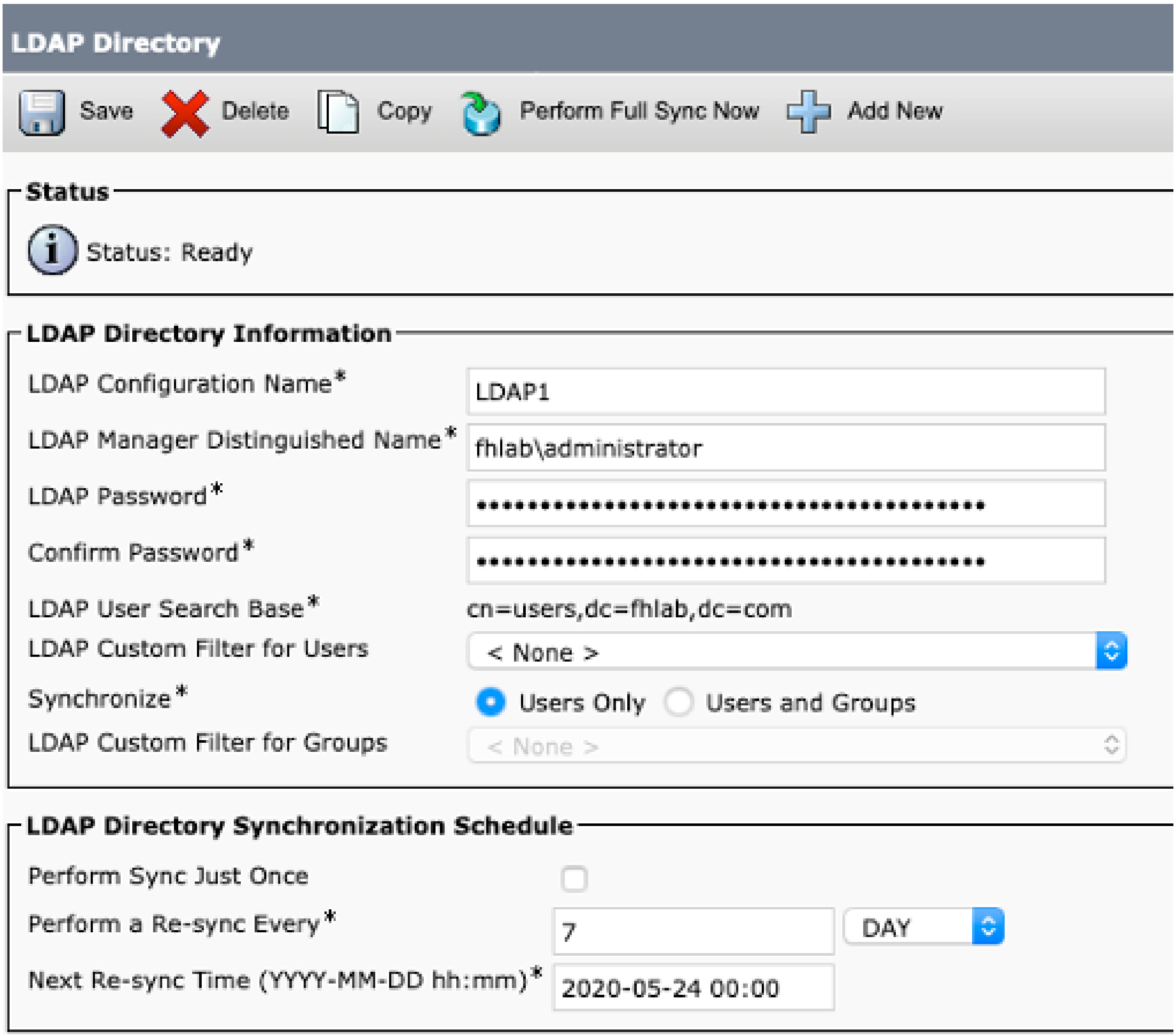
LDAP System Information

☑ Enable Synchronizing from LDAP Server

LDAP Server Type: Microsoft Active Directory

LDAP Attribute for User ID: sAMAccountName

Ensuite, accédez à l'**onglet Système > Répertoire LDAP**.



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

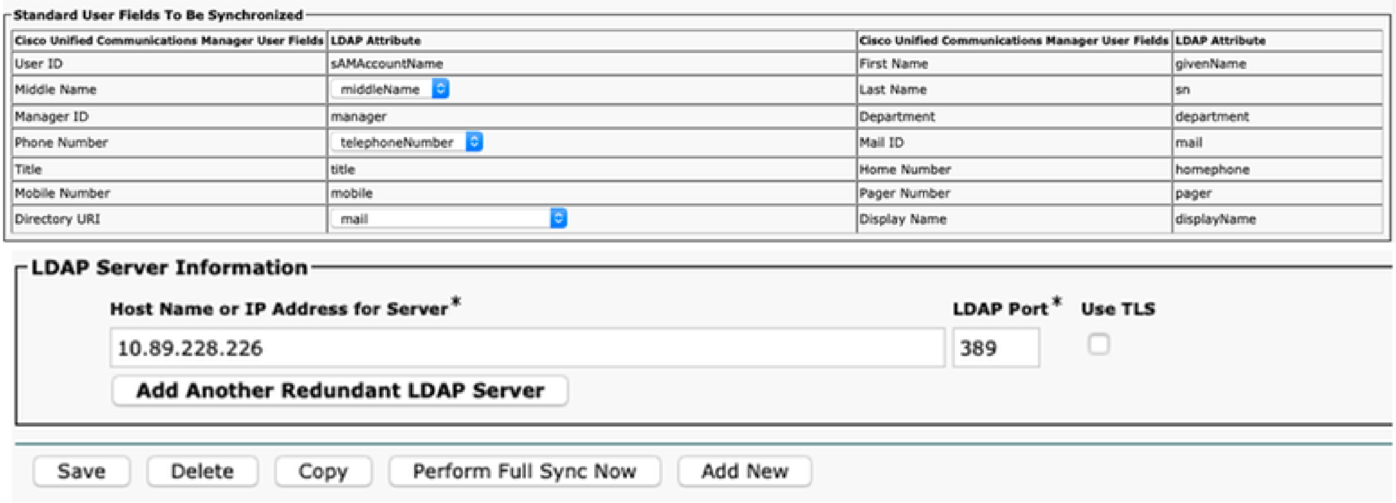
LDAP Custom Filter for Groups: < None >

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



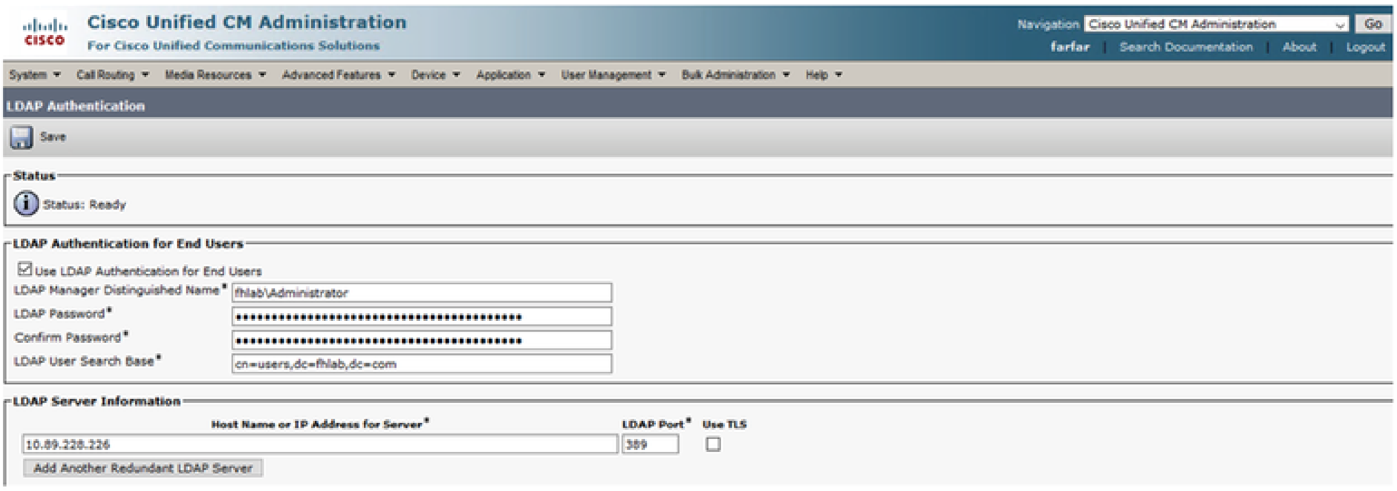
Standard User Fields To Be Synchronized

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	□

Une fois que les utilisateurs Active Directory ont été synchronisés avec CUCM, l'authentification LDAP doit être configurée.



Status

Status: Ready

LDAP Authentication for End Users

☑ Use LDAP Authentication for End Users

LDAP Manager Distinguished Name* fhlab\Administrator

LDAP Password* ••

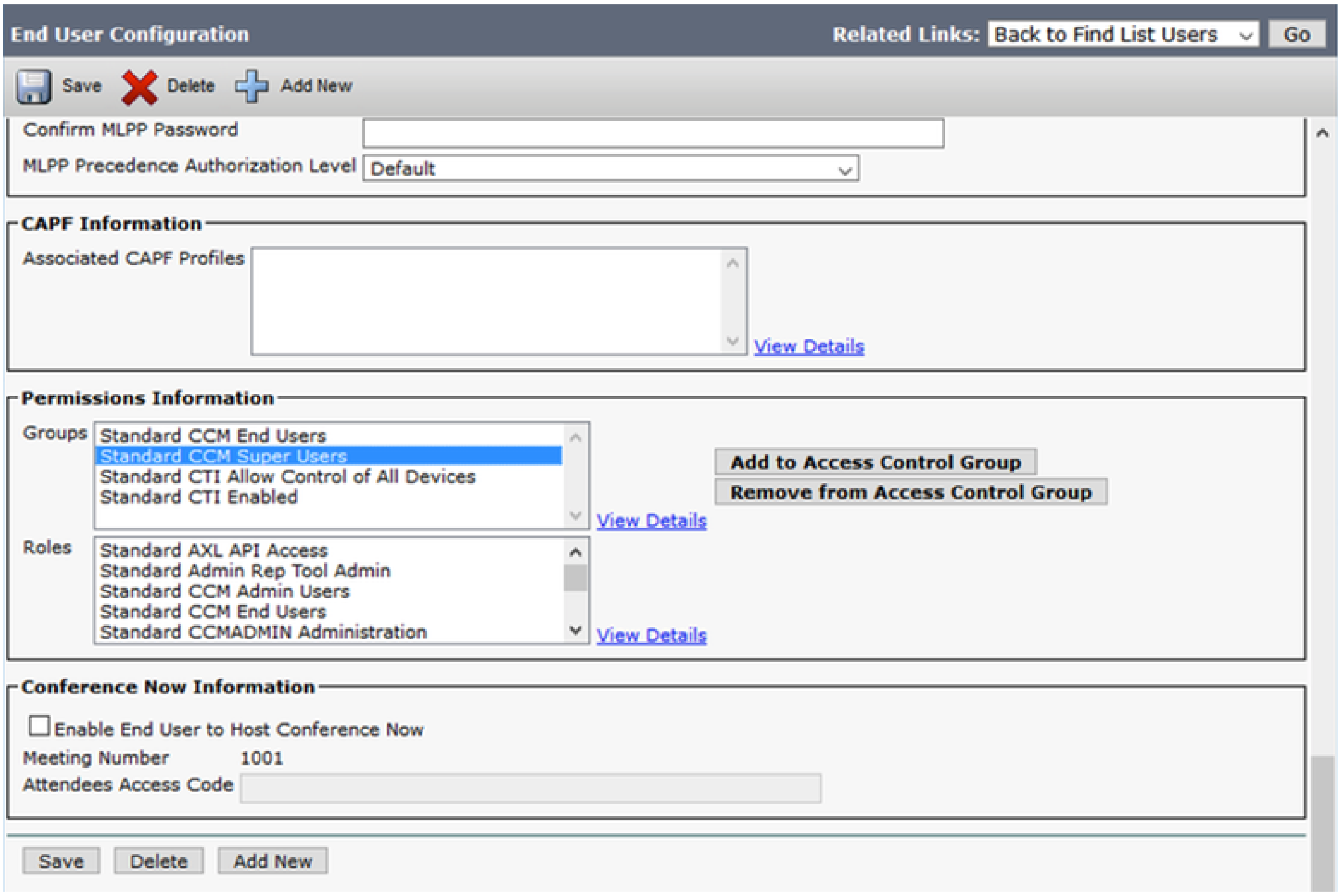
Confirm Password* ••

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 utilisateur final de CUCM doit avoir certains groupes de contrôle d'accès affectés à son profil d'utilisateur final. L'ACG est un super utilisateur CCM standard. L'utilisateur sera utilisé pour tester SSO lorsque l'environnement est prêt.


End User Configuration
Related Links: Back to Find List Users
Go
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

View Details
Add to Access Control Group
Remove from Access Control Group

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

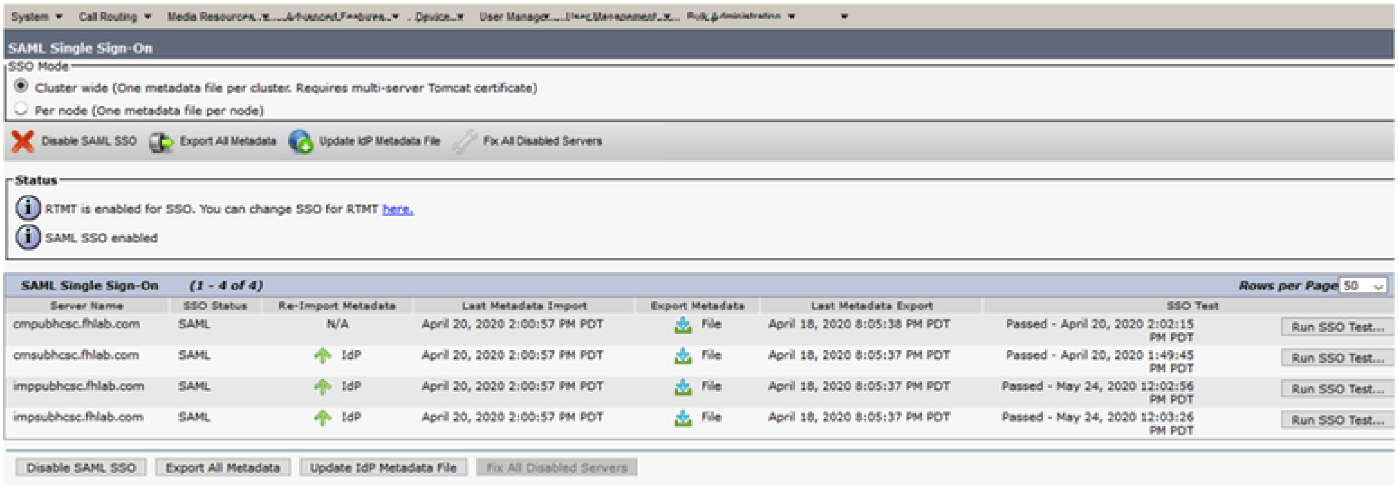
Meeting Number: 1001

Attendees Access Code

Métadonnées CUCM

Cette section affiche le processus du serveur de publication CUCM.

La première tâche consiste à obtenir les métadonnées CUCM, pour lesquelles vous devez accéder à l'URL ; **https://<CUCM Pub FQDN> :8443/ssosp/ws/config/adata/sp** ou il peut être téléchargé à partir de l'**onglet Système > Authentification unique SAML**. Cela peut être fait par noeud ou à l'échelle du cluster. Préférable pour faire ce cluster Wide.



SAML Single Sign-On

SSO Mode

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

○ Per node (One metadata file per node)

Status

RTMT is enabled for SSO. You can change SSO for RTMT here.

SAML SSO enabled

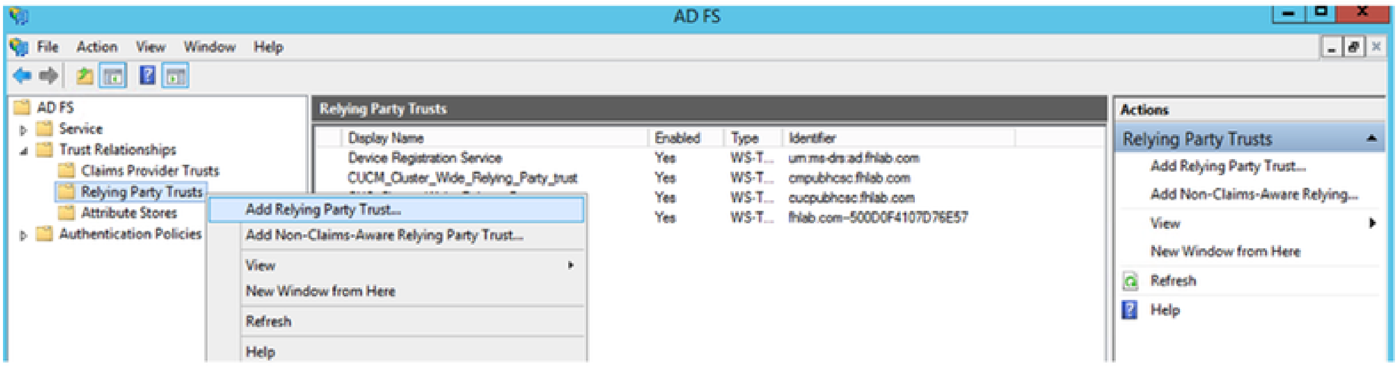
SAML Single Sign-On (1 - 4 of 4) — Rows per Page 50

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...

Enregistrez les données localement avec un nom significatif tel que sp_cucm0a.xml, vous en aurez besoin après.

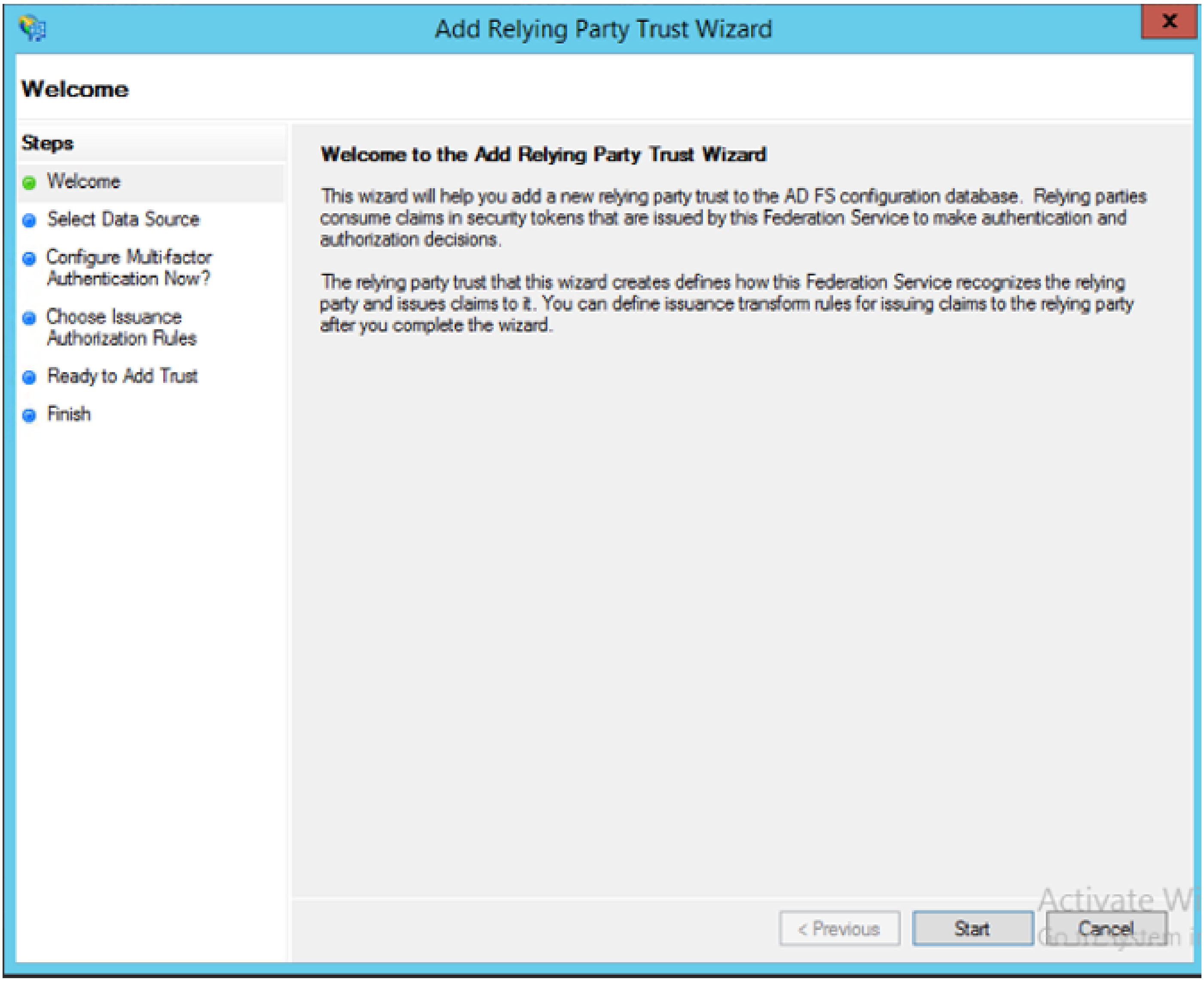
Configurer la partie de confiance ADFS

Revenir à la console de gestion AD FS 3.0.



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

Cliquez sur **Assistant Ajout d'approbation de partie de confiance**.


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

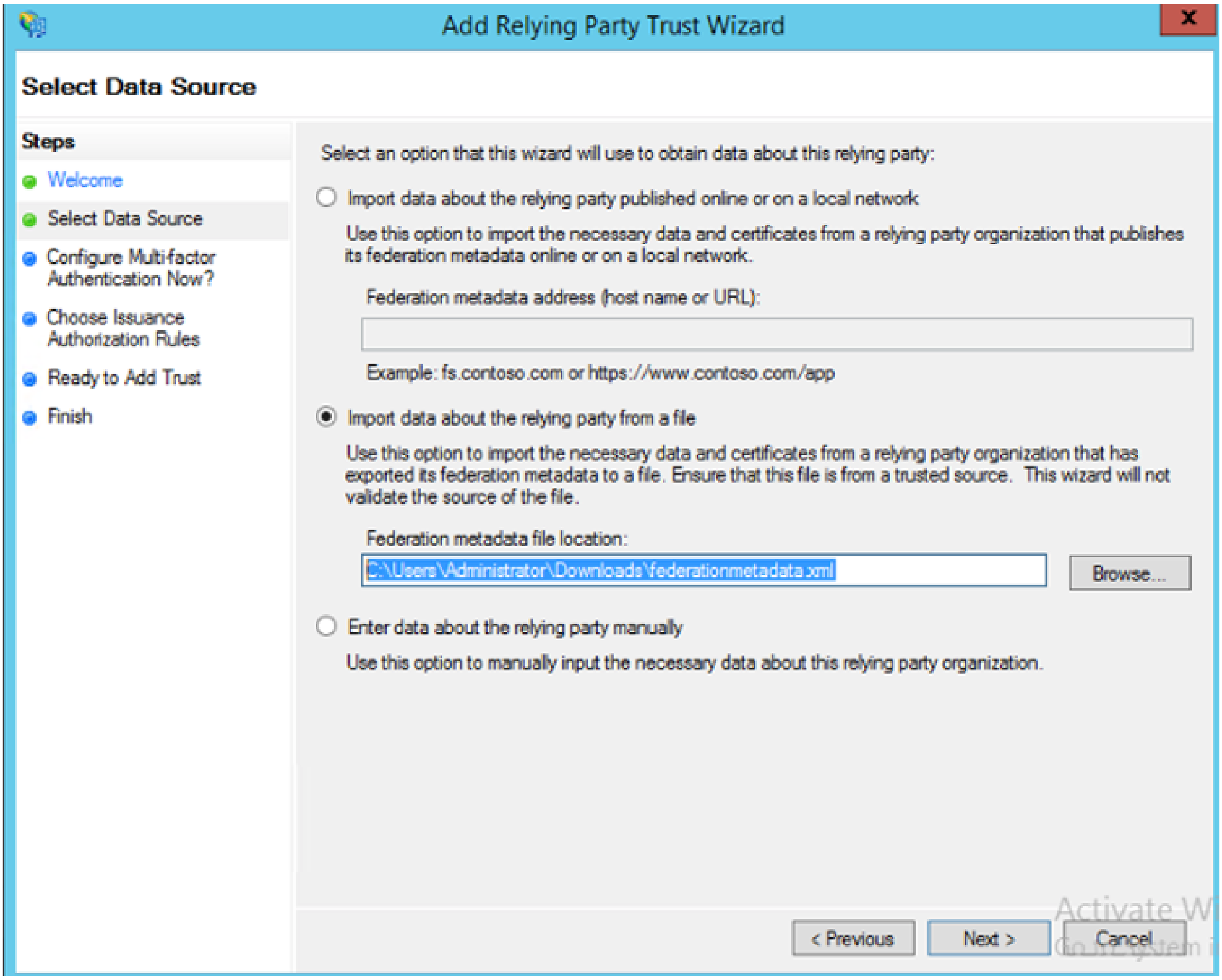
Welcome to the Add Relying Party Trust Wizard

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.

Cliquez sur **Démarrer** pour continuer.

Sélectionnez le fichier XML de métadonnées **federationmedatada.xml** que vous avez enregistré précédemment et cliquez sur **Suivant**.


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.

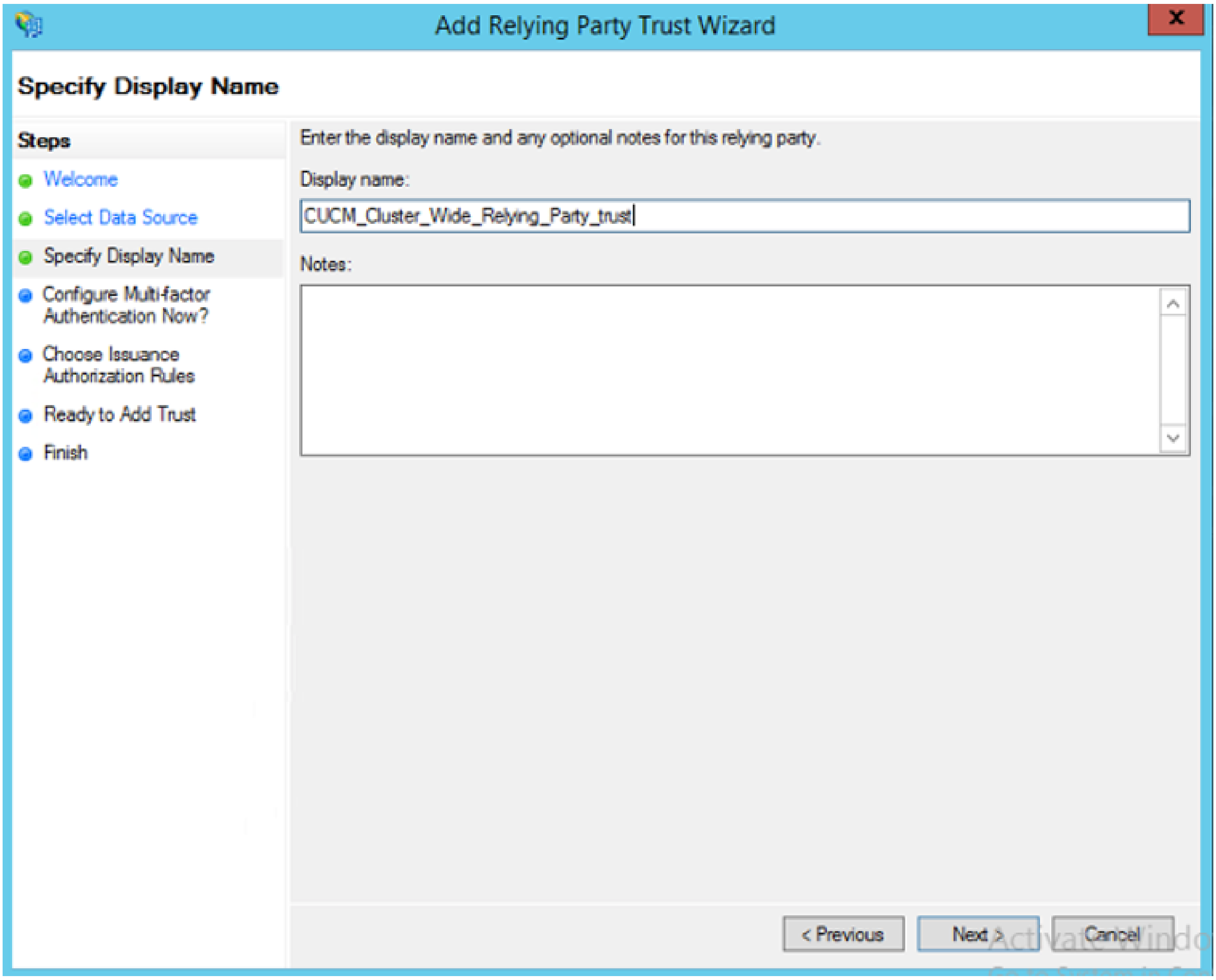
Federation metadata file location:

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.

Utilisez **CUCM_Cluster_Wide_Relying_Party_trust** comme nom d'affichage et cliquez sur **Suivant**.



Add Relying Party Trust Wizard

Specify Display Name

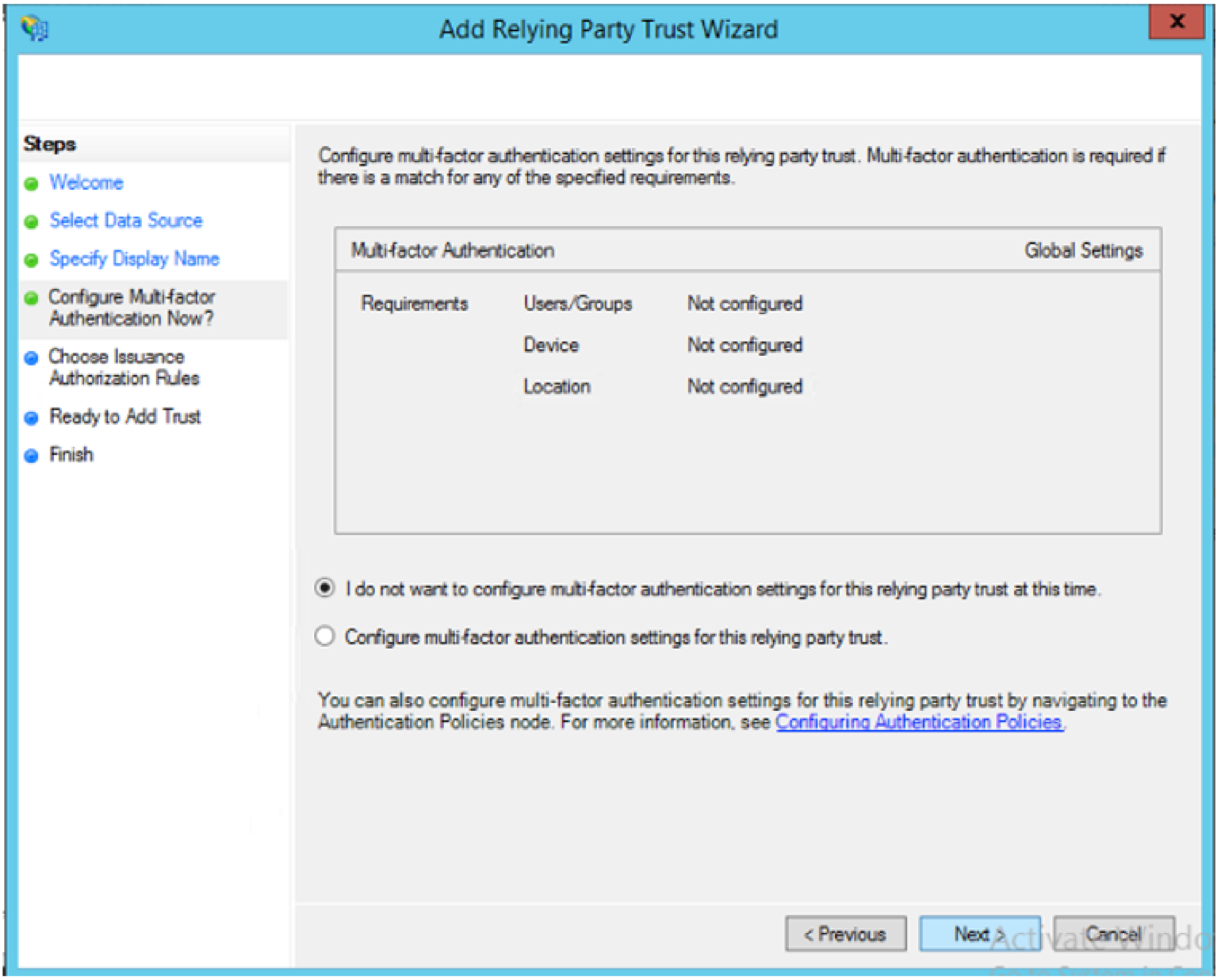
Enter the display name and any optional notes for this relying party.

Display name:

CUCM_Cluster_Wide_Relying_Party_trust

Notes:

Sélectionnez la première option et cliquez sur **Suivant**.


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

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.

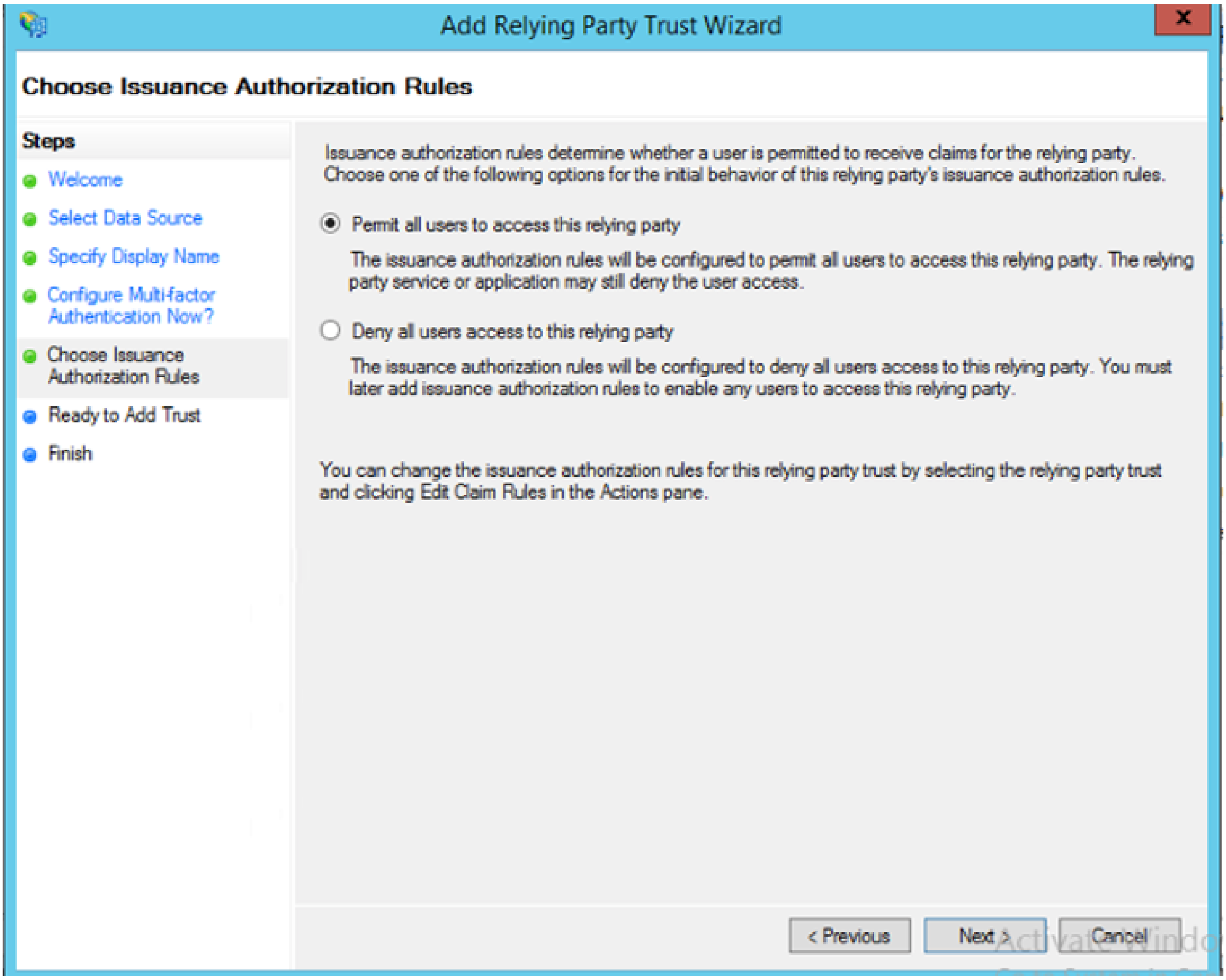
Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

● 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.

Sélectionnez **Autoriser tous les utilisateurs à accéder à cette partie de confiance** et cliquez sur **Suivant** comme indiqué dans l'image.



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

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

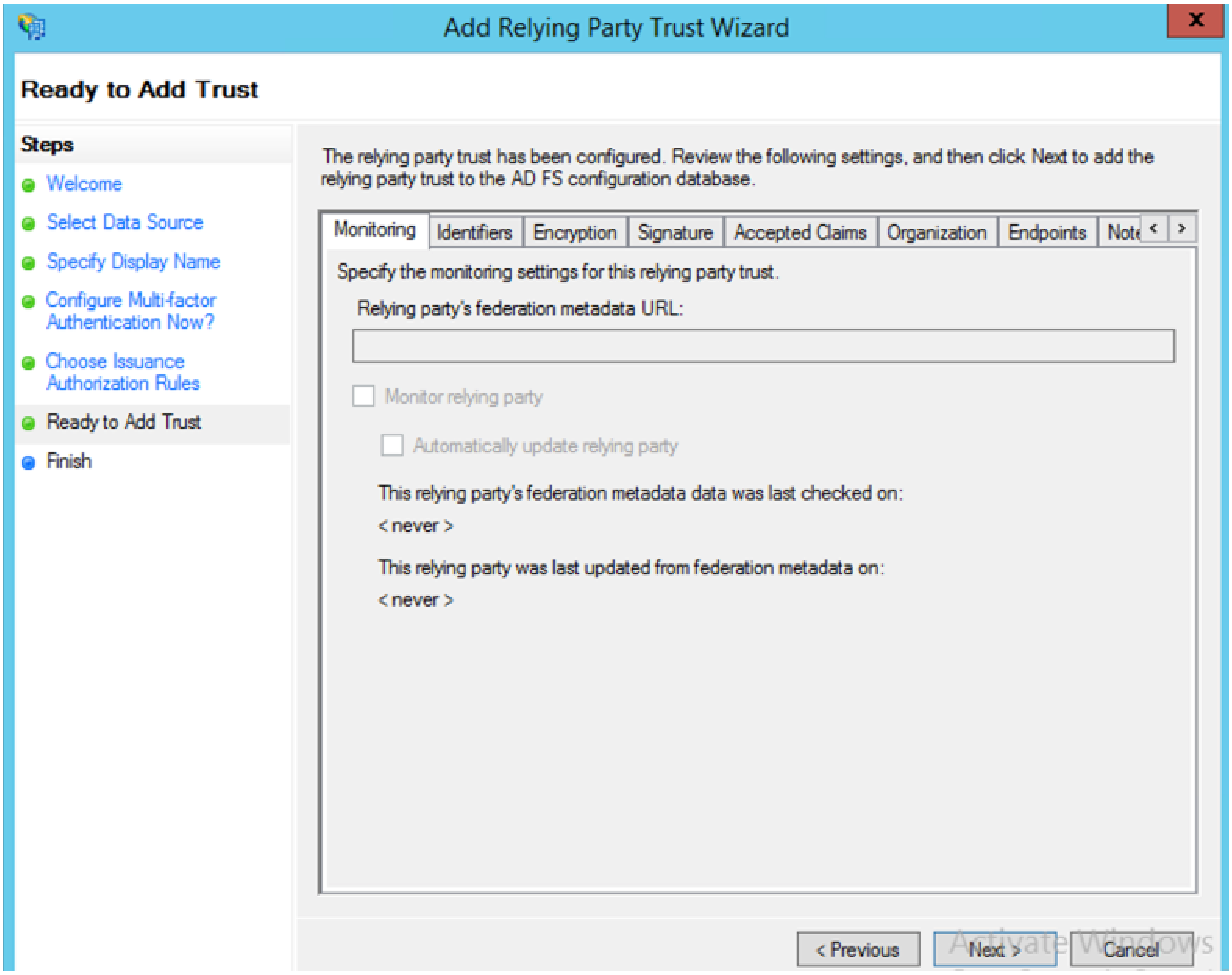
The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ 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.

Vérifiez la configuration et cliquez sur **Suivant** comme indiqué dans l'image.



Add Relying Party Trust Wizard

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

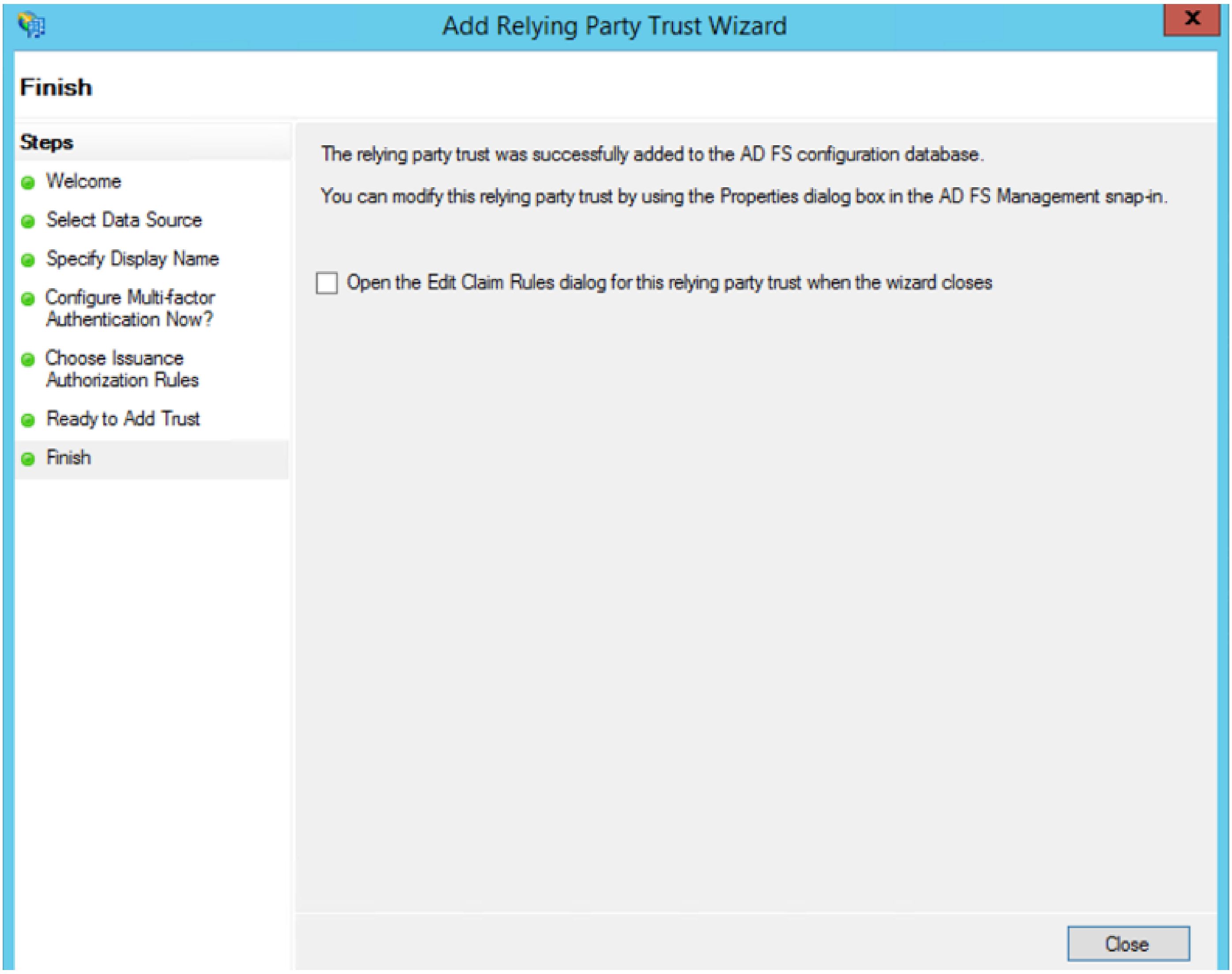
This relying party's federation metadata data was last checked on:

< never >

This relying party was last updated from federation metadata on:

< never >

Décochez la case et cliquez sur **Fermer**.

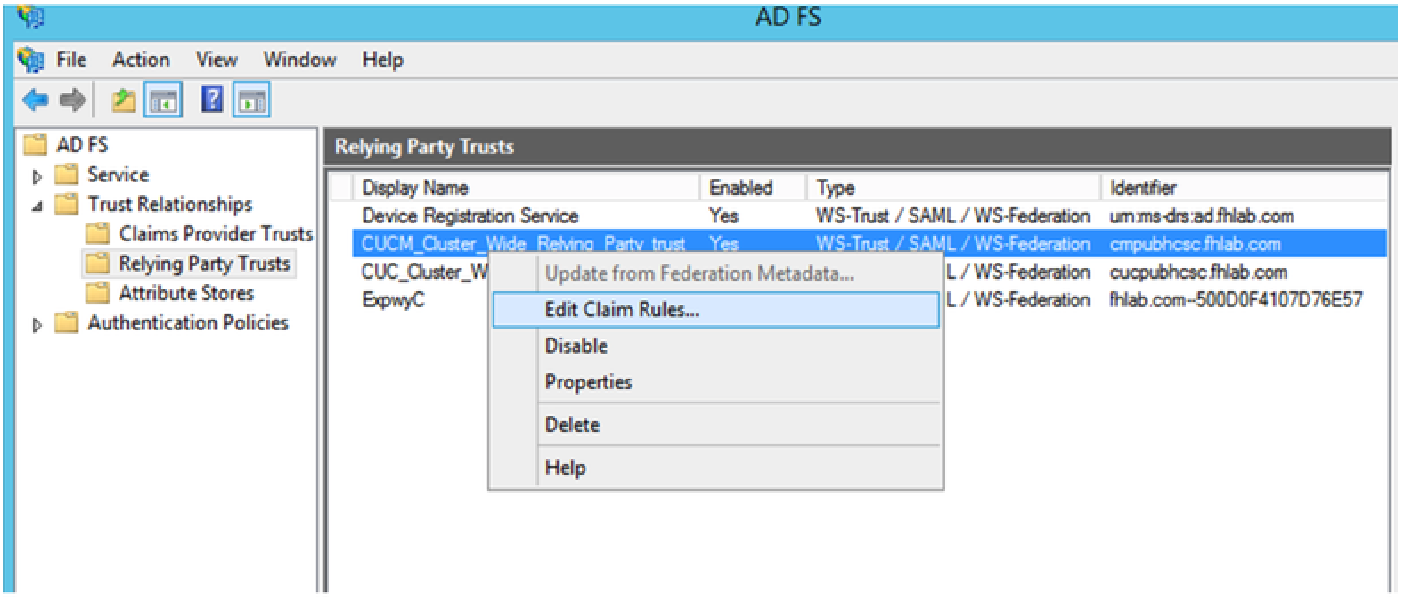

Add Relying Party Trust Wizard
Finish
Steps
Welcome
Select Data Source
Specify Display Name
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
Close

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.

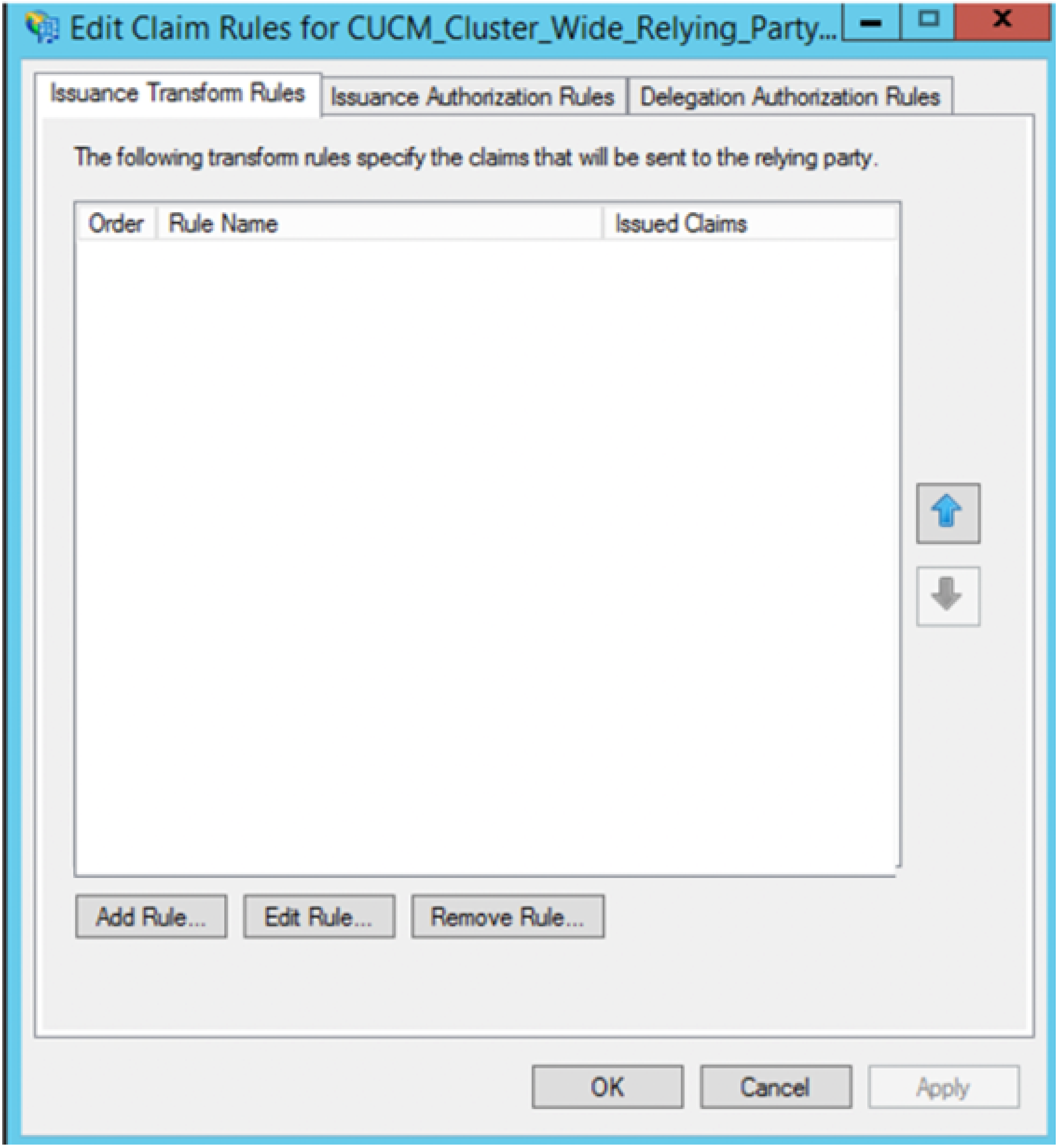
□ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes

Àl'aide du bouton secondaire de la souris, sélectionnez la configuration **Confiance de la partie de confiance** que vous venez de créer et **modifiez les règles de revendication** comme indiqué dans l'image.



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

Cliquez sur **Ajouter une règle** comme indiqué dans l'image.

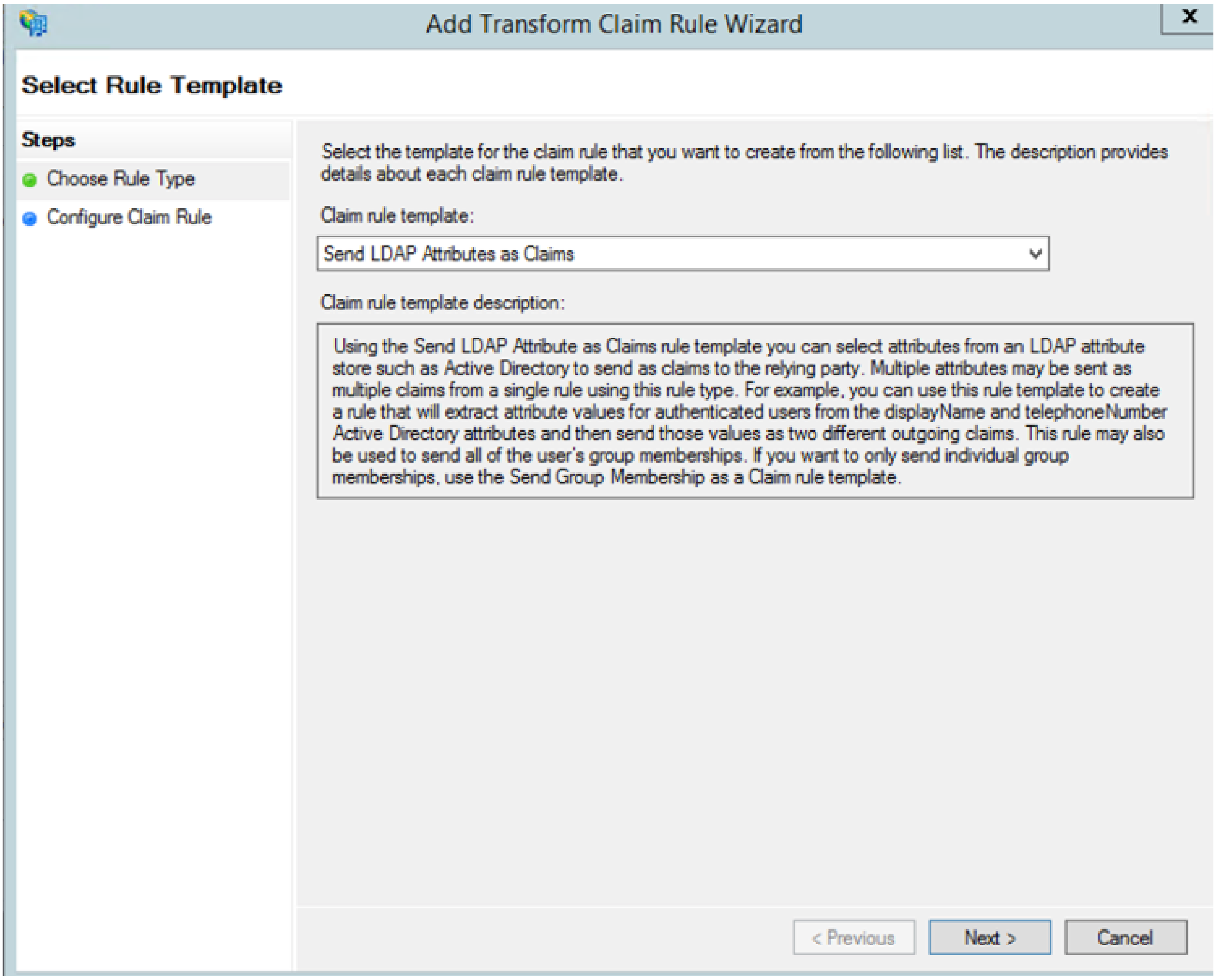


Edit Claim Rules for CUCM_Cluster_Wide_Relying_Party...

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

Order	Rule Name	Issued Claims

Sélectionnez **Envoyer les attributs LDAP en tant que revendications** et cliquez sur **Suivant**.



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.

Configurez ces paramètres :

Nom de la règle de demande : IDNom

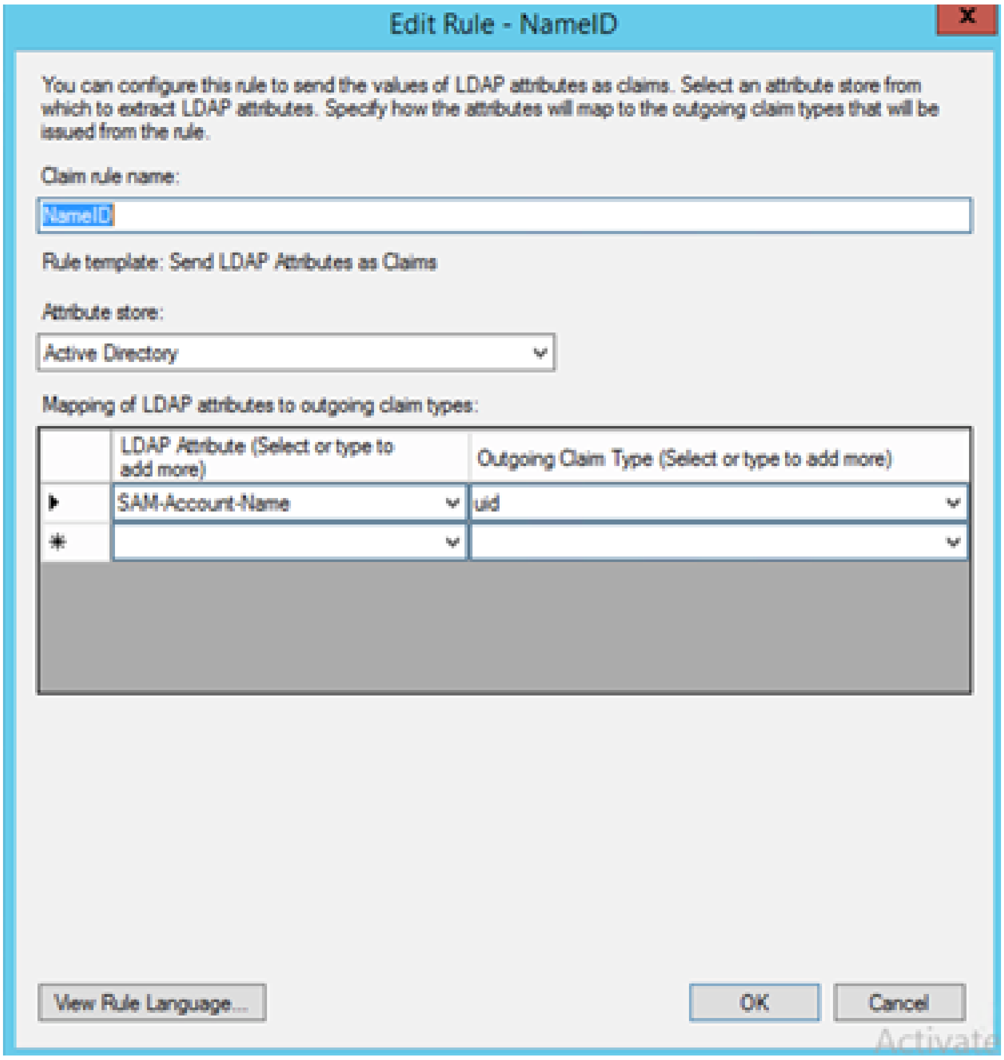
Magasin d'attributs : Active Directory (double-cliquez sur la flèche du menu déroulant)

Attribut LDAP : Nom du compte SAM

Type de demande sortante : uid

Cliquez sur **FINISH/OK** pour continuer.

Veuillez noter que uid n'est pas en minuscules et n'existe pas déjà dans le menu déroulant. Tapez-le.



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

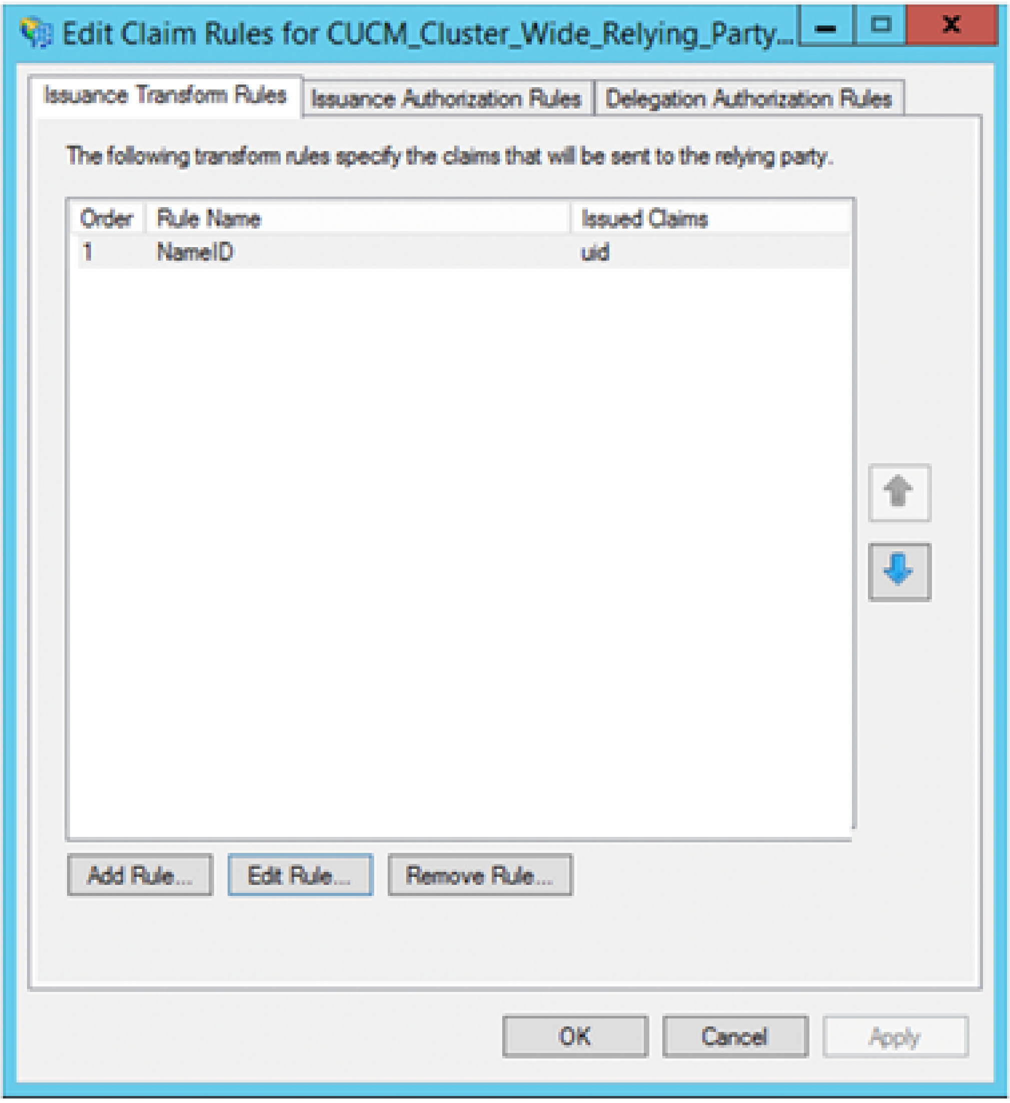
Attribute store:

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
*		

Cliquez à nouveau sur **Ajouter une règle** afin d'ajouter une autre règle.

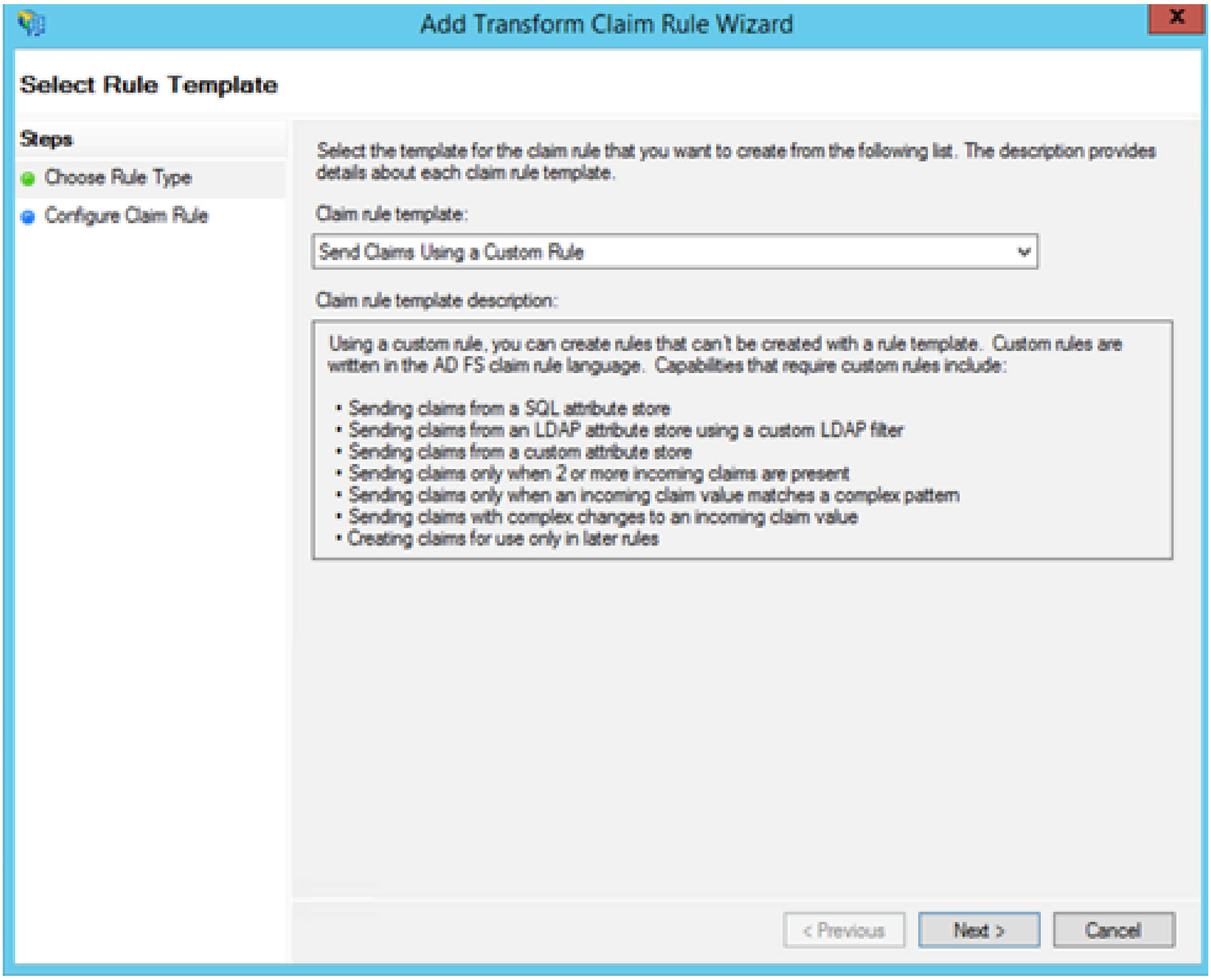

Edit Claim Rules for CUCM_Cluster_Wide_Relying_Party...
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules

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

Sélectionnez **Envoyer des revendications à l'aide d'une règle personnalisée** et cliquez sur **Suivant**.



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 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

Créez une règle personnalisée appelée Cluster_Side_Request_Rule.

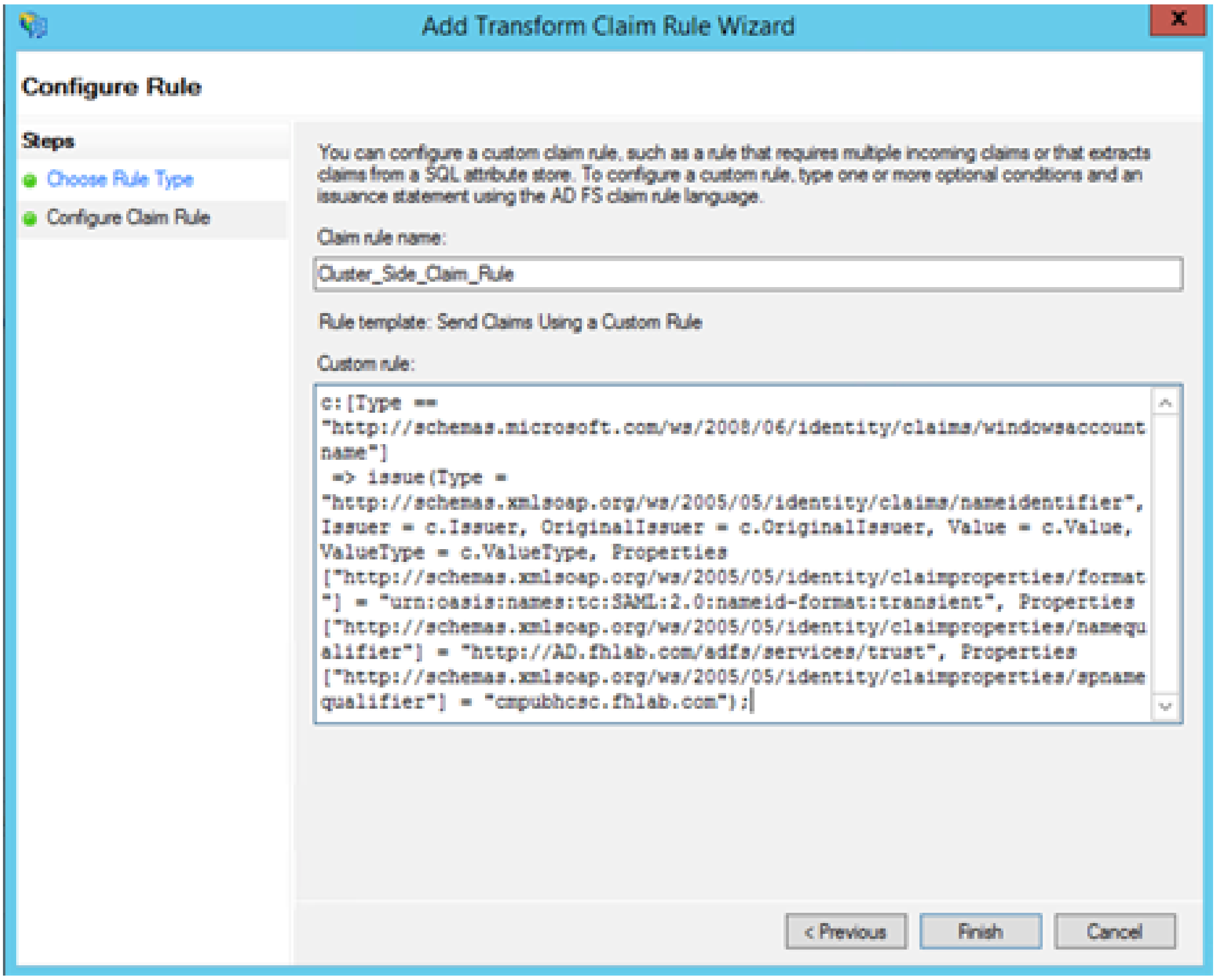
Copiez et collez ce texte dans la fenêtre de règle directement à partir d'ici. Parfois, les guillemets sont modifiés sur un éditeur de texte et la règle échouera lorsque vous testez SSO :

```
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");
```

Cliquez sur **Terminer** pour continuer.



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:

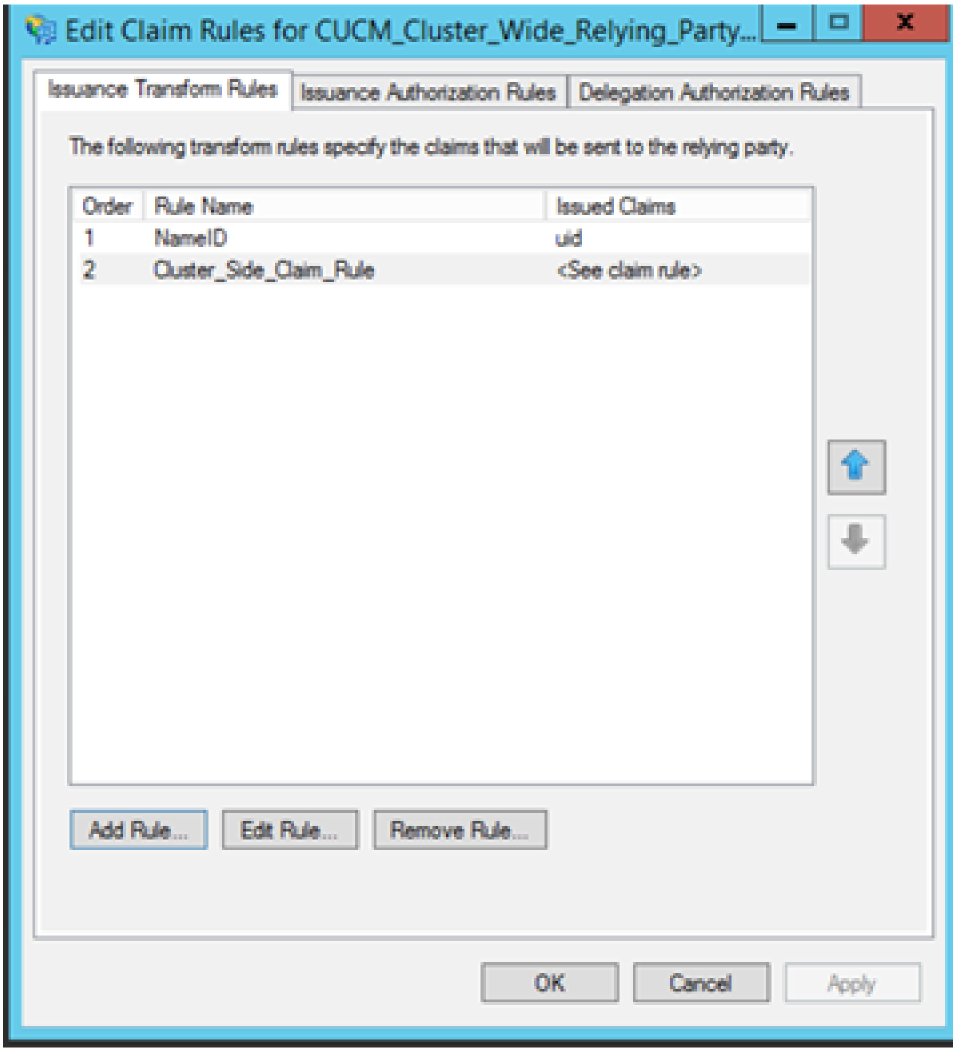
Cluster_Side_Claim_Rule

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");
```

Vous devez maintenant avoir deux règles définies sur ADFS. Cliquez sur **Appliquer** et **OK** pour fermer la fenêtre des règles.

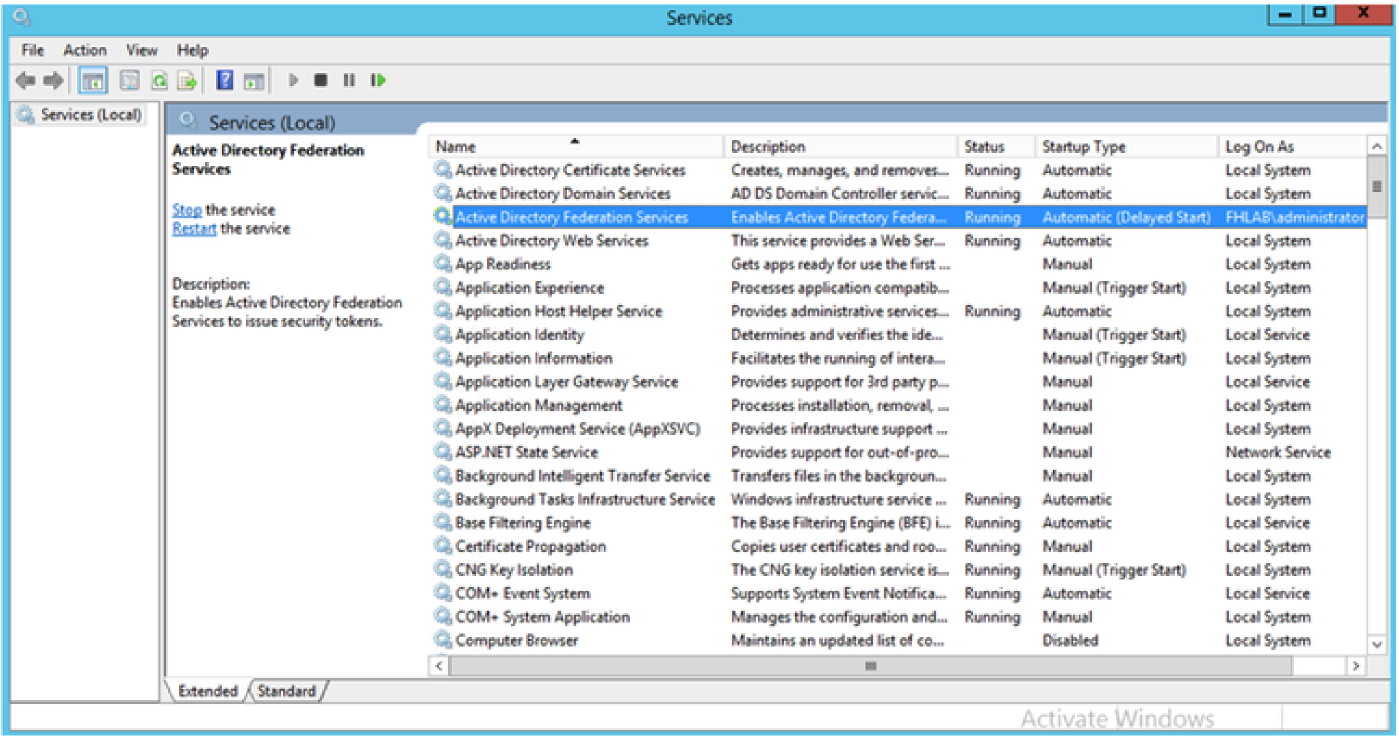


Edit Claim Rules for CUCM_Cluster_Wide_Relying_Party...
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

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 est maintenant ajouté en tant que partie de confiance à ADFS.



Active Directory Federation Services

Stop the service
Restart the service

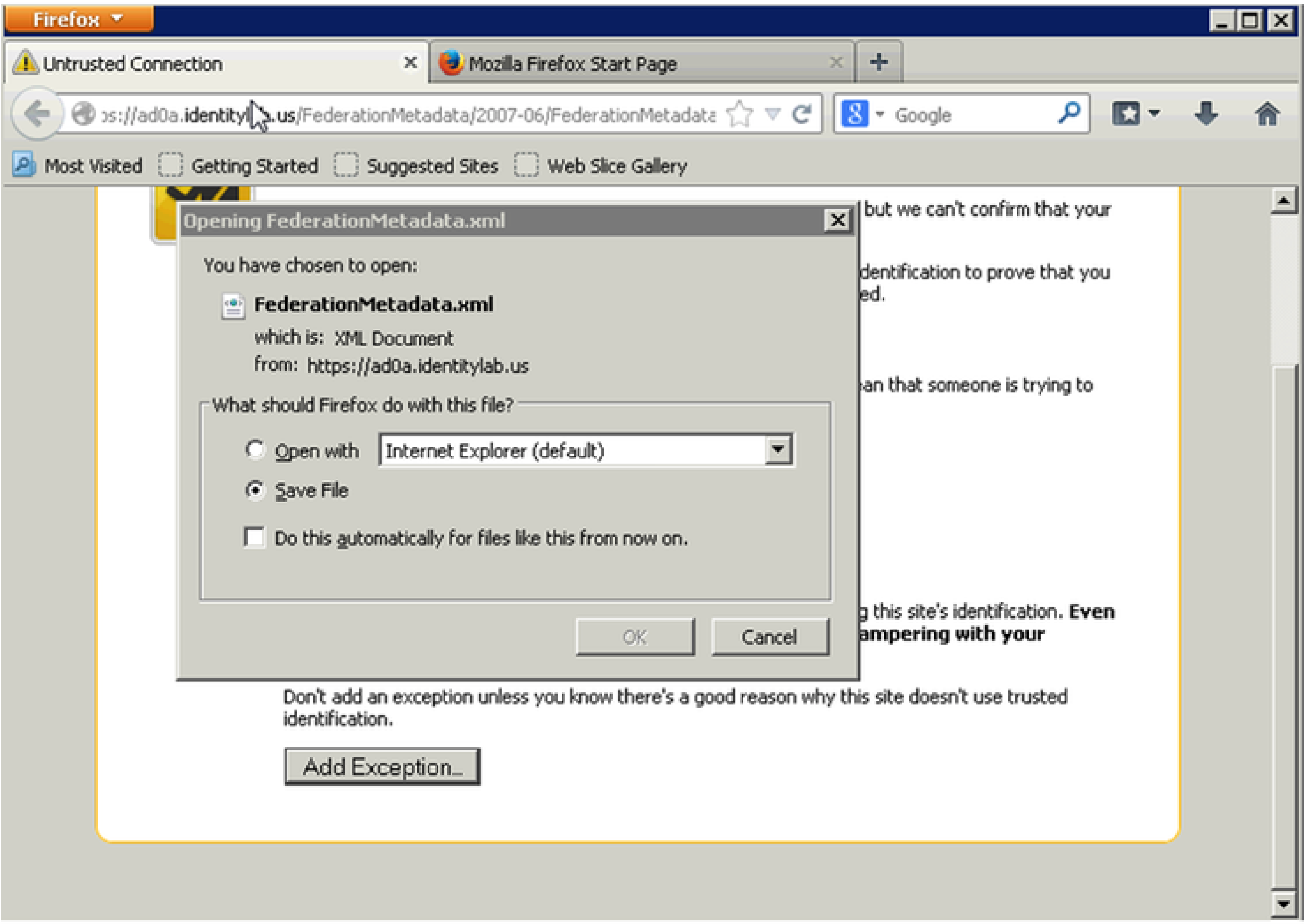
Description:
Enables Active Directory Federation Services to issue security tokens.

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

Avant de continuer, redémarrez le service ADFS. Accédez au **menu Démarrer > Outils d'administration > Services**.

Métadonnées PCI

Vous devez fournir à CUCM des informations sur notre IdP. Ces informations sont échangées à l'aide de métadonnées XML. Assurez-vous d'effectuer cette étape sur le serveur sur lequel ADFS est installé.



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

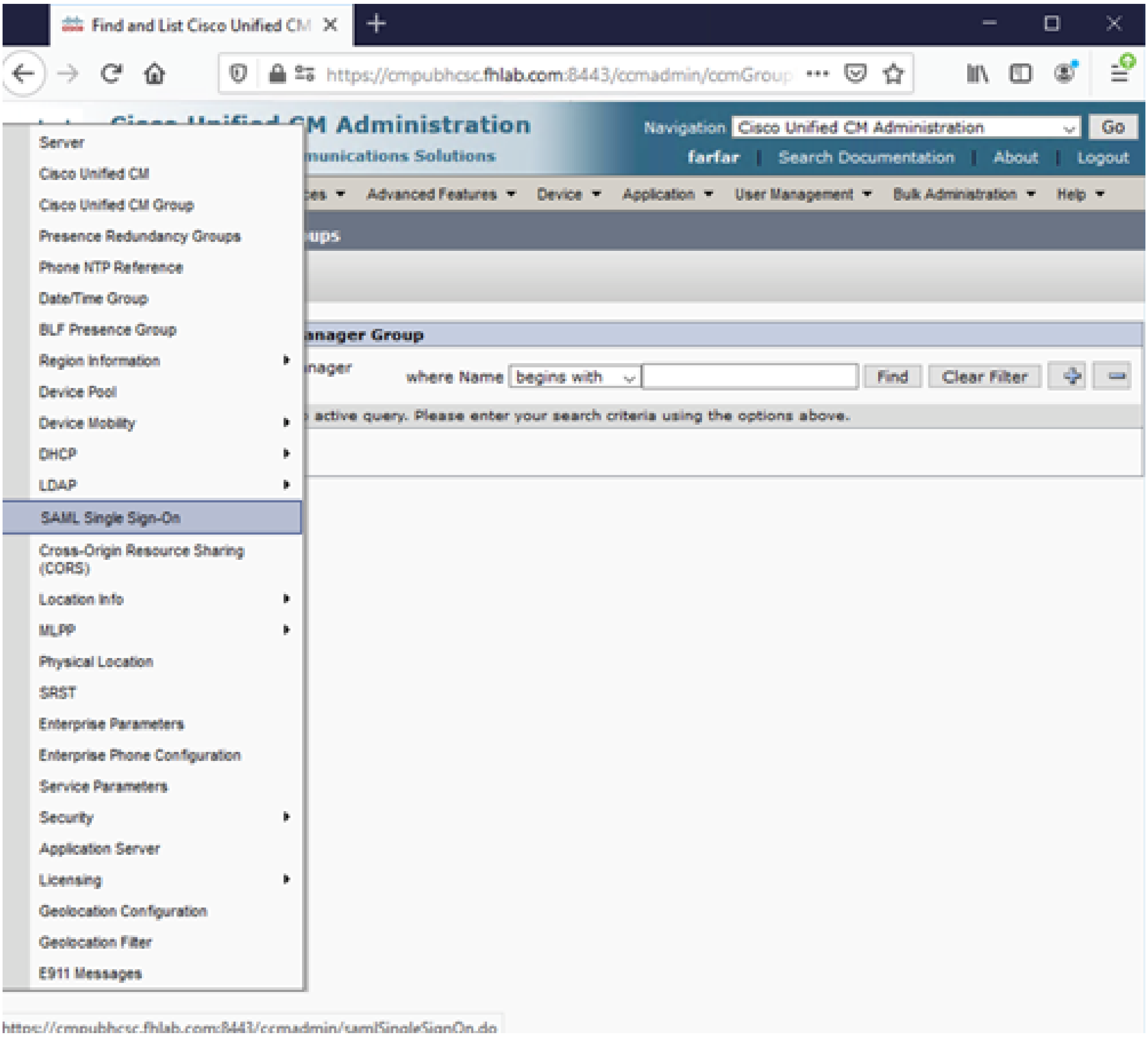
☐ Do this automatically for files like this from now on.

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.

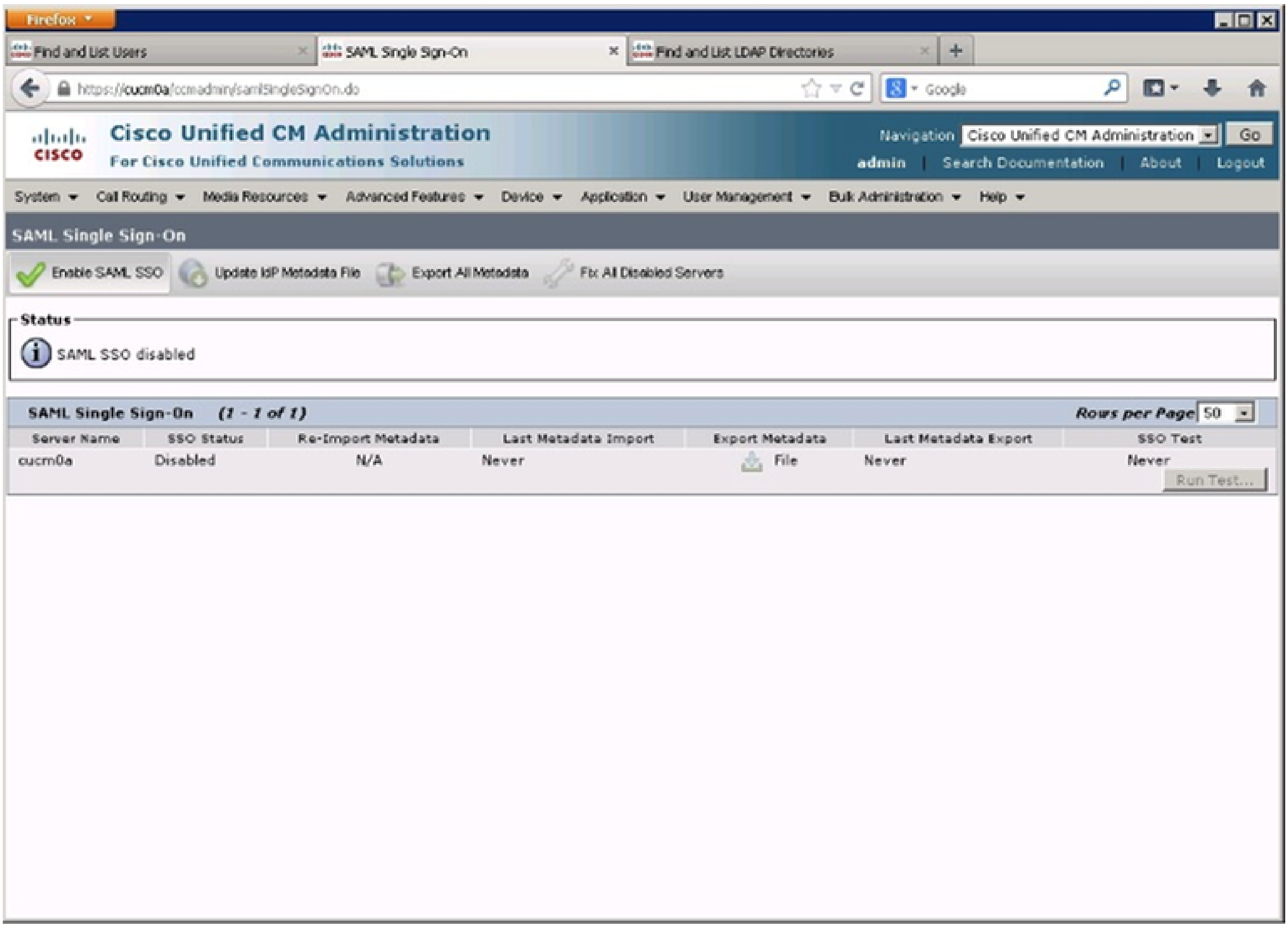
Tout d'abord, vous devez vous connecter à ADFS (IdP) à l'aide d'un navigateur Firefox pour télécharger les métadonnées XML. Ouvrez un navigateur sur https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml et ENREGISTREZ les métadonnées dans un dossier local.

Maintenant, accédez à la configuration CUCM jusqu'au **menu** système **> menu d'authentification unique SAML**.



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

Retournez à l'Administration CUCM et sélectionnez **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

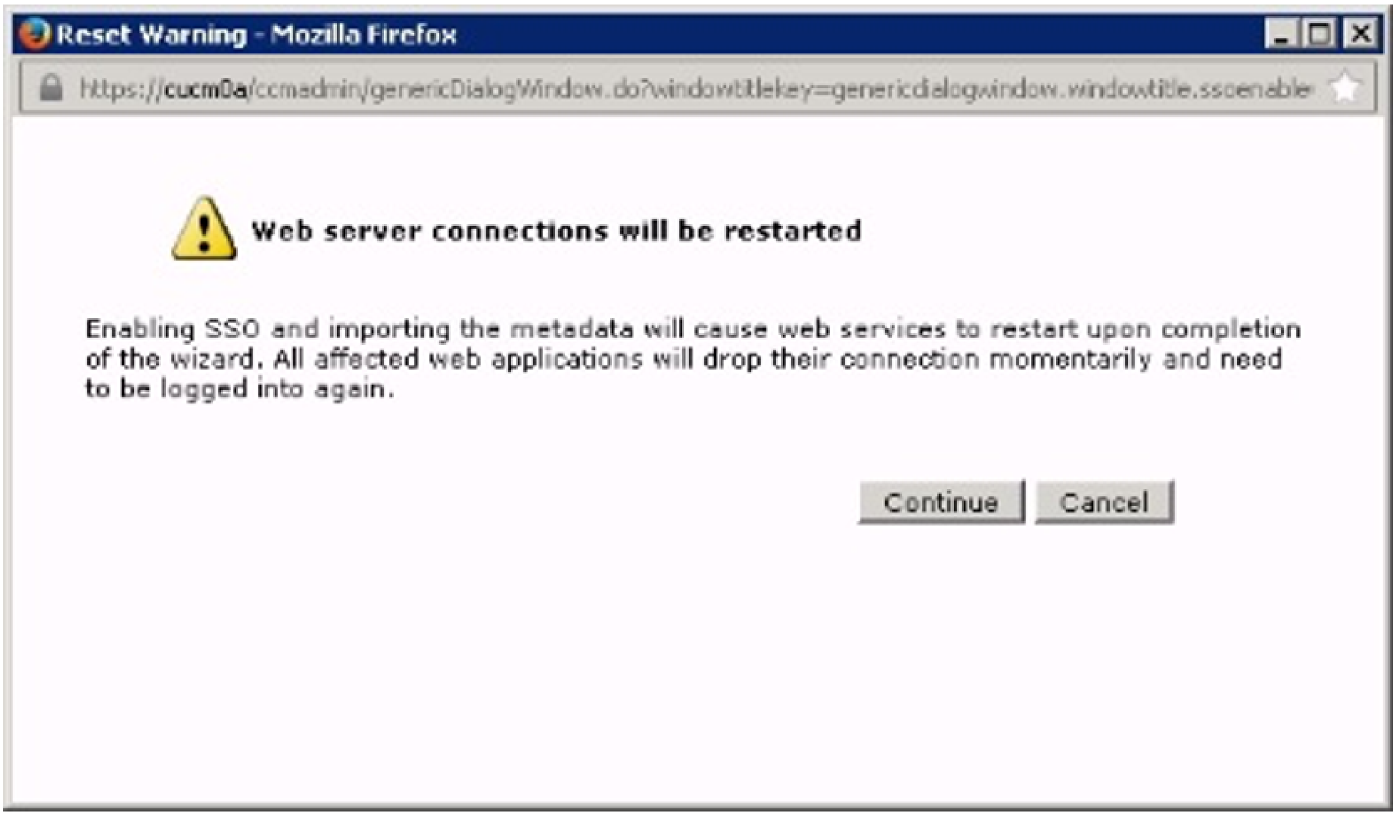
SAML SSO disabled

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 Run Test...

Sélectionnez **Activer SAML SSO**.

Cliquez sur **Continuer** pour accuser réception de l'avertissement.

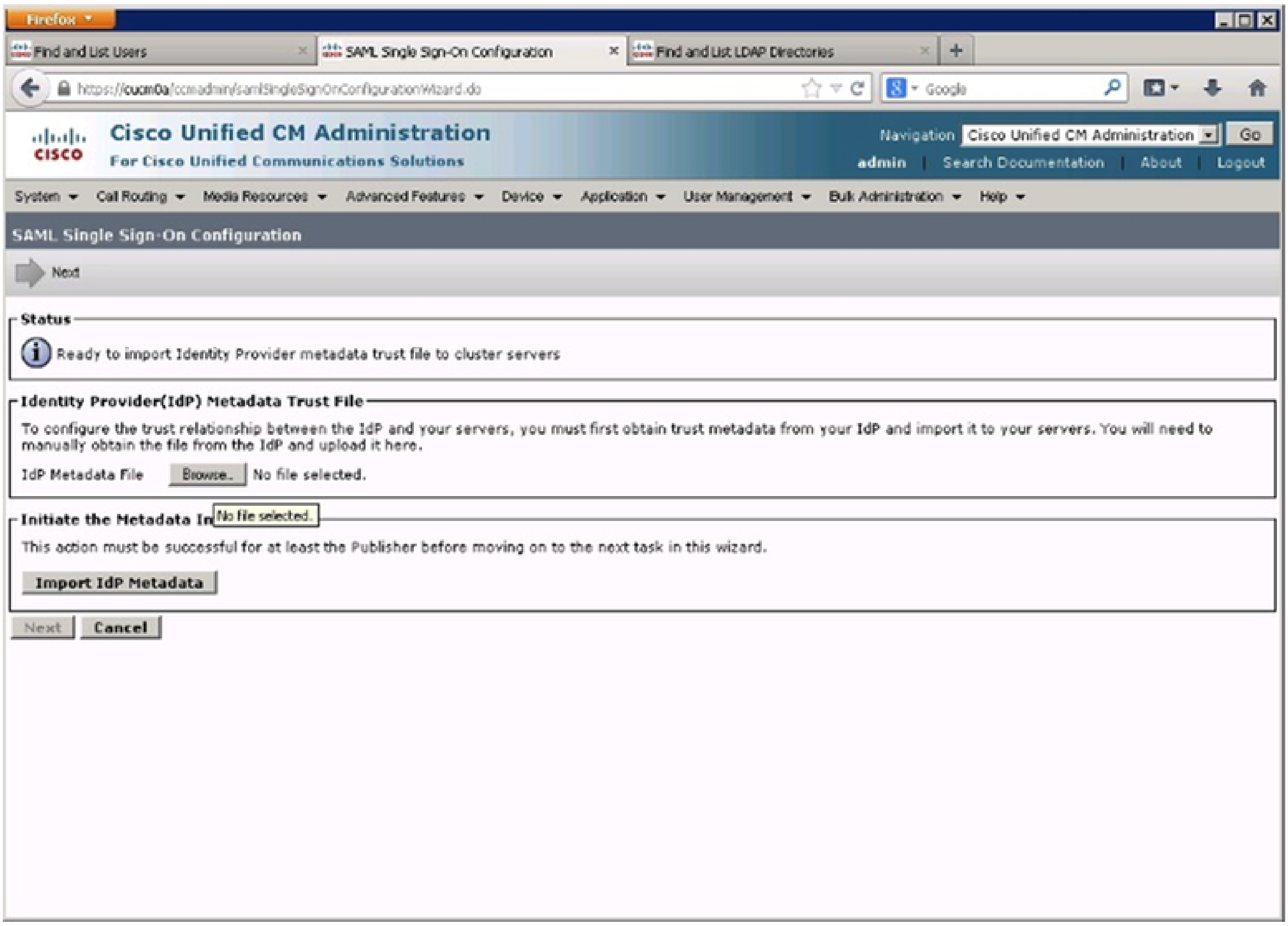

Reset Warning - Mozilla Firefox
https://cucm0a/ccmadmin/genericDialogWindow.do?windowtitlekey=genericdialogwindow.windowtitle.ssoenable
Continue
Cancel

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.

Sur l'écran SSO et cliquez sur **Parcourir.** afin d'importer le fichier XML de métadonnées

FederationMetadata.xml que vous avez enregistré précédemment, comme indiqué dans l'image.



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.

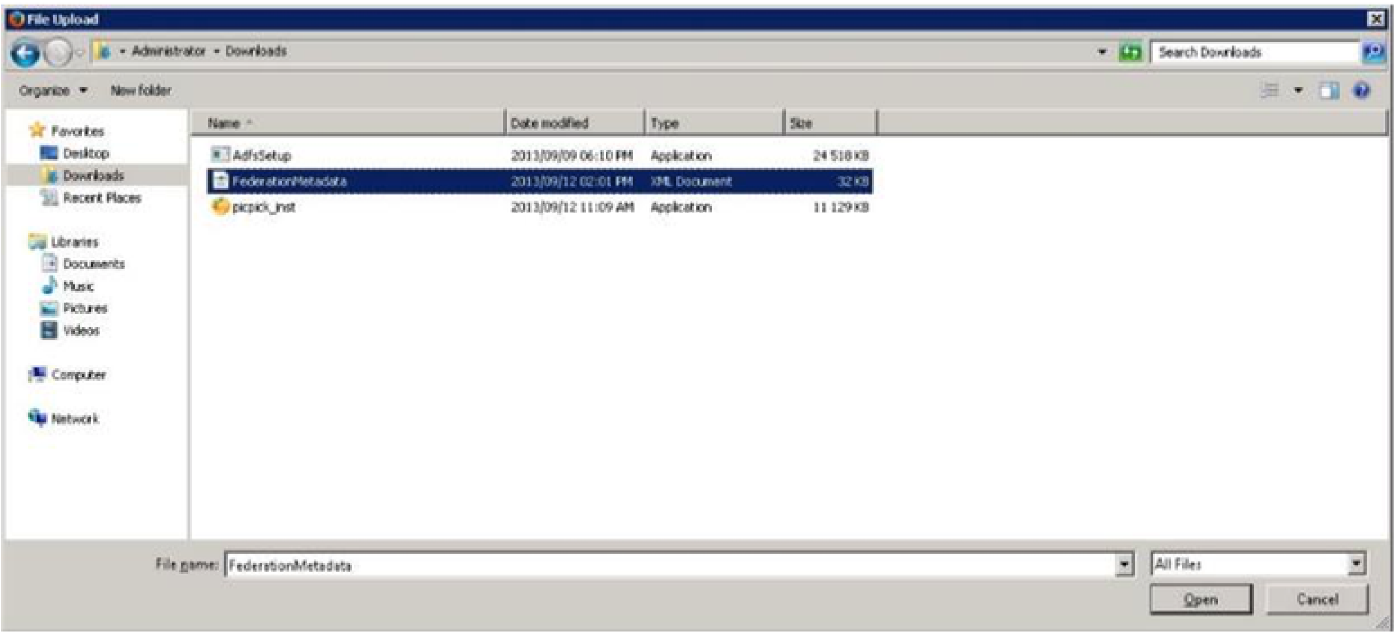
Initiate the Metadata In No file selected.

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

Sélectionnez le fichier XML et cliquez sur **Ouvrir** afin de le télécharger vers CUCM à partir des téléchargements sous Favoris.



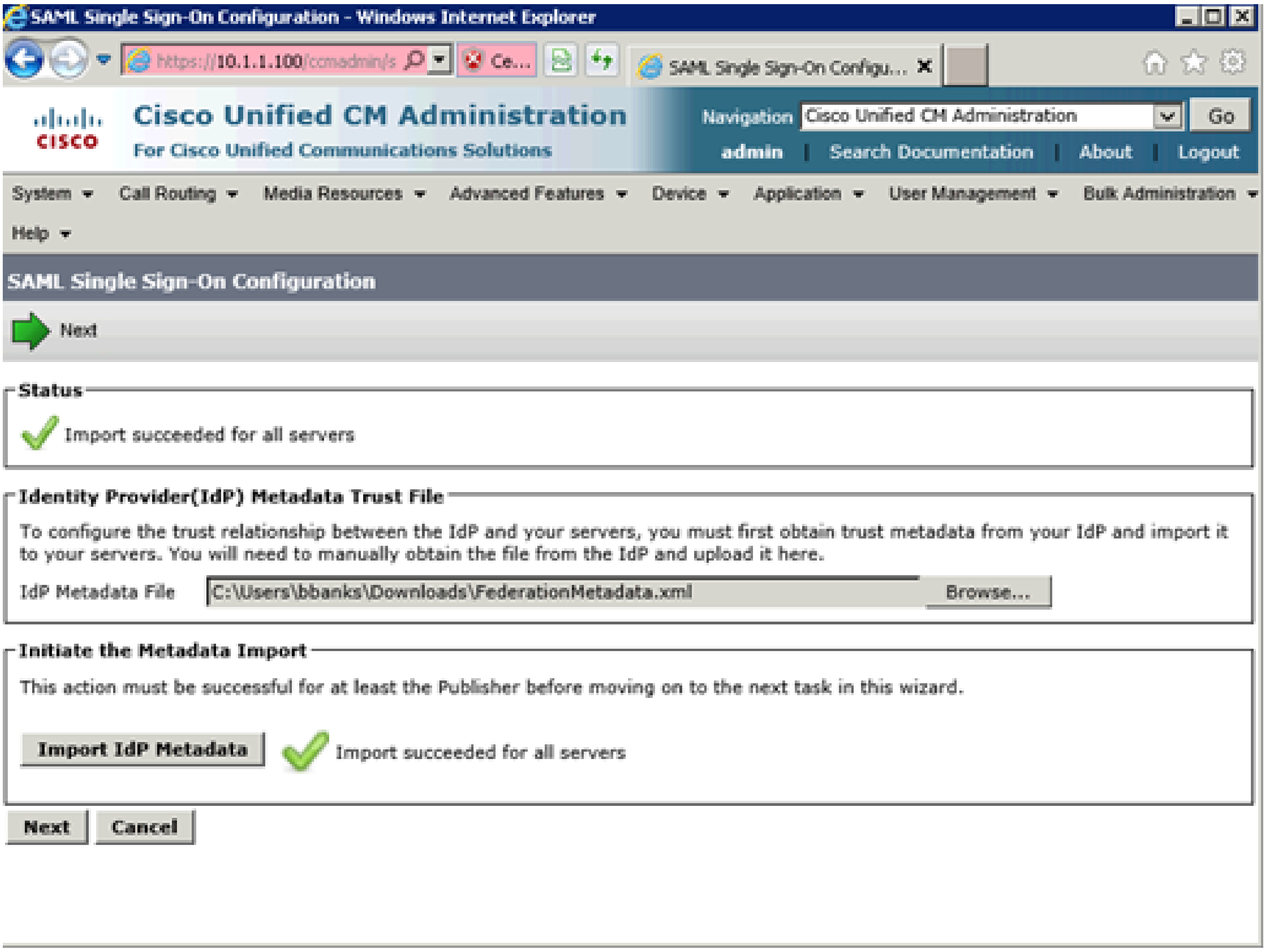
Name	Date modified	Type	Size
AdfsSetup	2013/09/09 06:10 PM	Application	24 518 KB
FederationMetadata	2013/09/12 02:01 PM	XML Document	32 KB
picpick_inst	2013/09/12 11:09 AM	Application	11 129 KB

File name: FederationMetadata

All Files

Open Cancel

Une fois téléchargé, cliquez sur Import IdP Metadata pour importer les informations IdP dans CUCM. Confirmez que l'importation a réussi et cliquez sur Suivant pour continuer.


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
SAML Single Sign-On Configuration
Next

Status

✓ Import succeeded for all servers

Identity Provider(IdP) Metadata Trust File

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

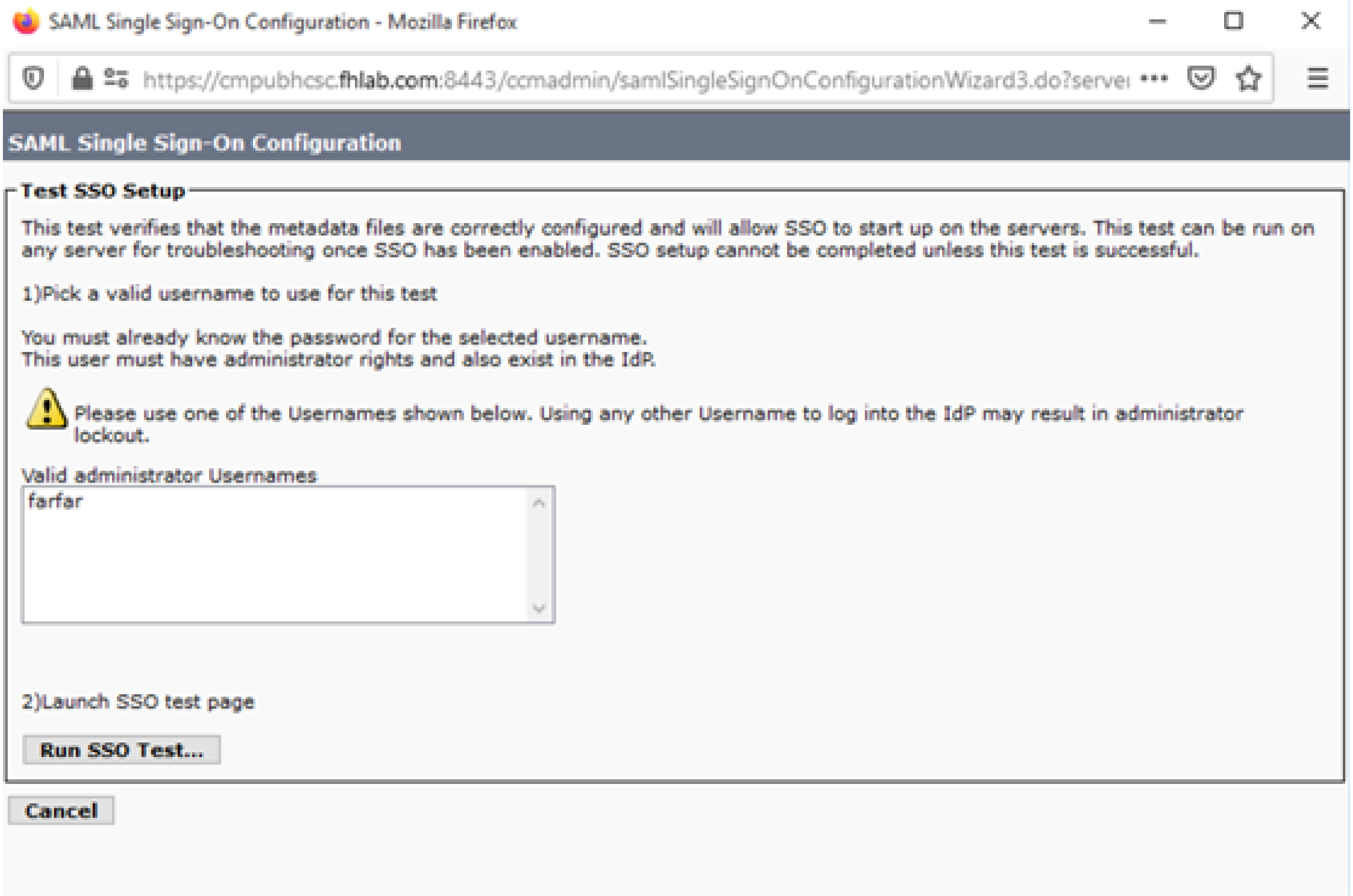
IdP Metadata File: C:\Users\bbanks\Downloads\FederationMetadata.xml

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

Sélectionnez l'utilisateur appartenant aux super utilisateurs CCM standard et cliquez sur EXÉCUTER LE TEST SSO.


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.

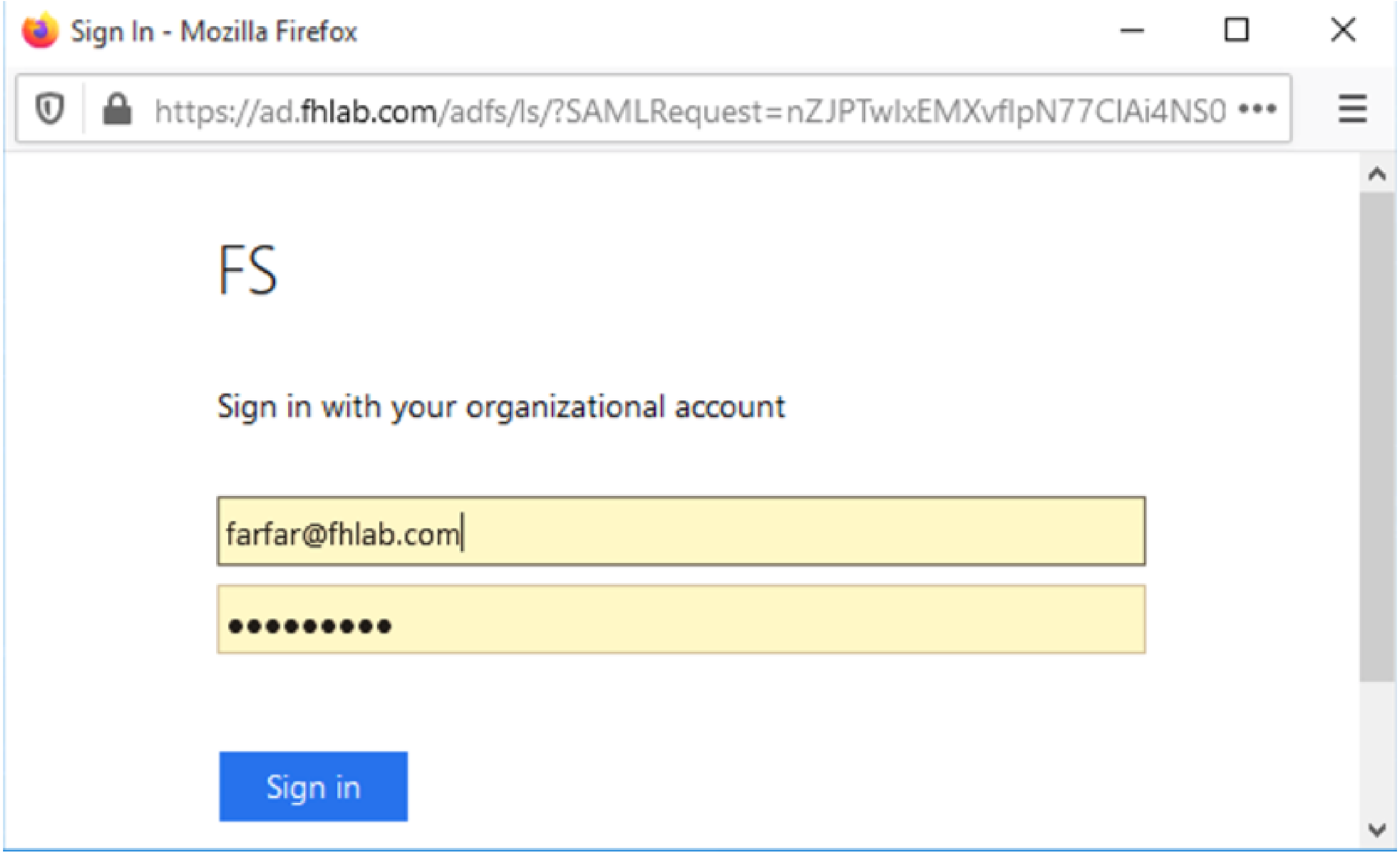
Valid administrator Usernames
farfar

2)Launch SSO test page

Run SSO Test...

Cancel

Lorsqu'une boîte de dialogue d'authentification utilisateur s'affiche, connectez-vous avec le nom d'utilisateur et le mot de passe appropriés.


Sign In - Mozilla Firefox
https://ad.fhlab.com/adfs/ls/?SAMLRequest=nZJPTwlxEMXvflpN77ClAi4NS0

FS

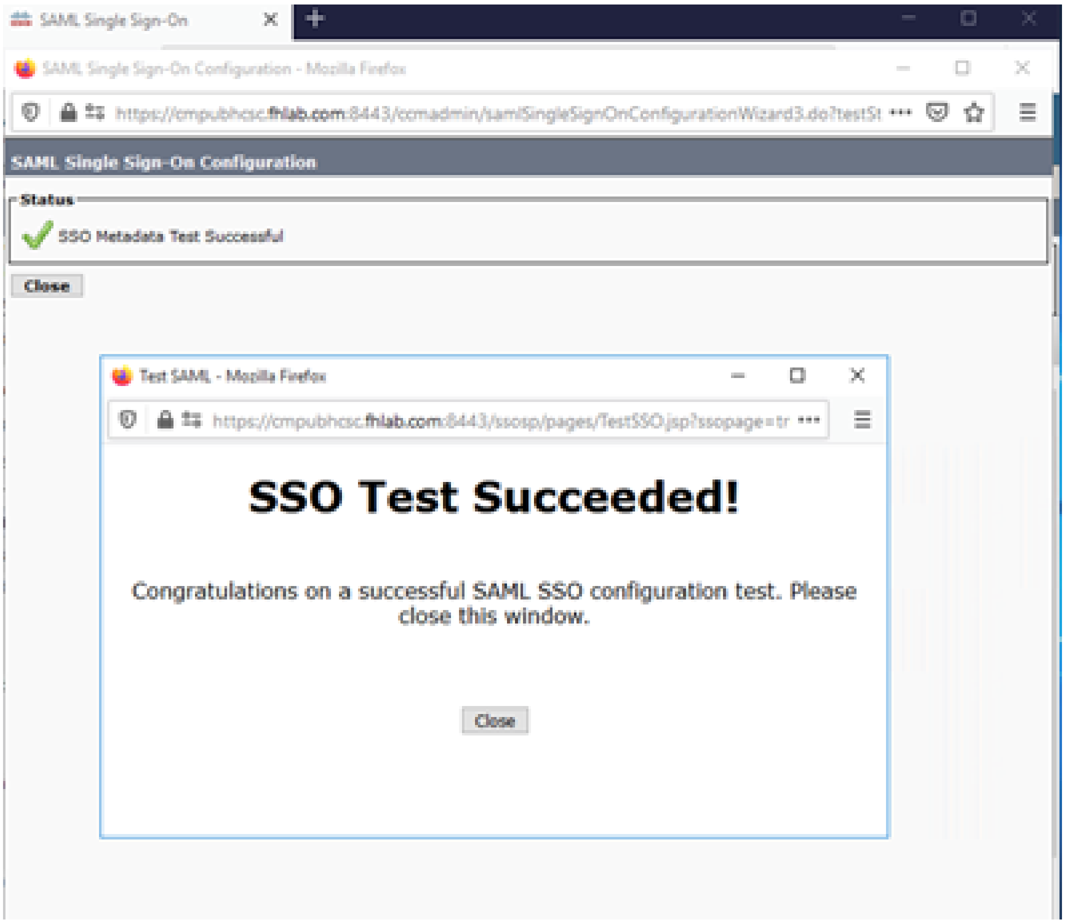
Sign in with your organizational account

farfar@fhlab.com

●●●●●●●●●●

Sign in

Si tout a été correctement configuré, vous devriez voir un message indiquant que le test SSO a réussi !


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

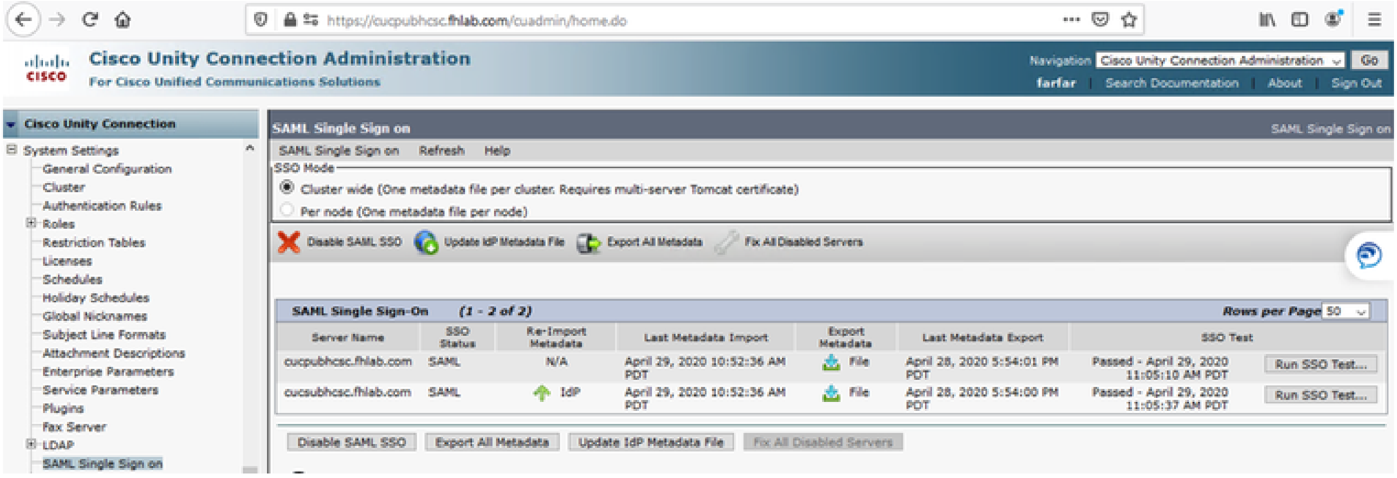
Cliquez sur FERMER et FINISH pour continuer.

Nous avons maintenant terminé les tâches de configuration de base pour activer SSO sur CUCM à l'aide d'ADFS.

Configurer SSO sur CUC

Le même processus peut être suivi pour activer SSO dans Unity Connection.

Intégration LDAP avec CUC.



SAML Single Sign on

SSO Mode

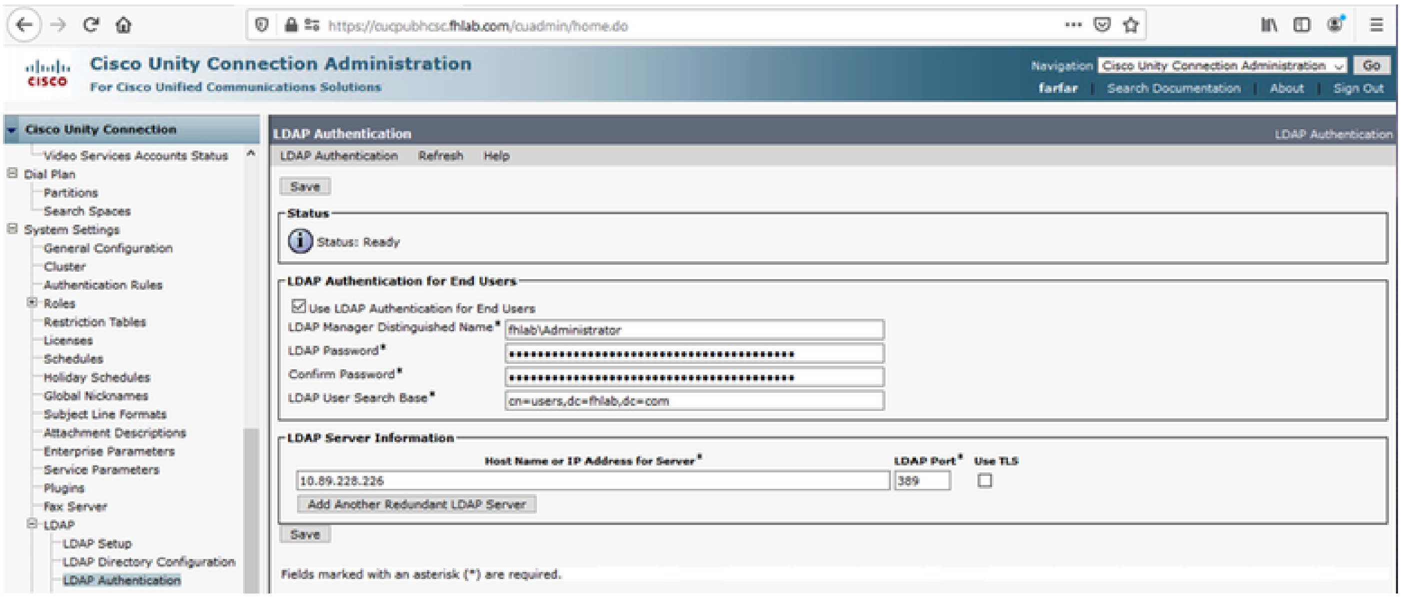
● Cluster wide (One metadata file per cluster. Requires multi-server Tomcat certificate)

○ Per node (One metadata file per node)

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

Configurez l'authentification LDAP.



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* ••

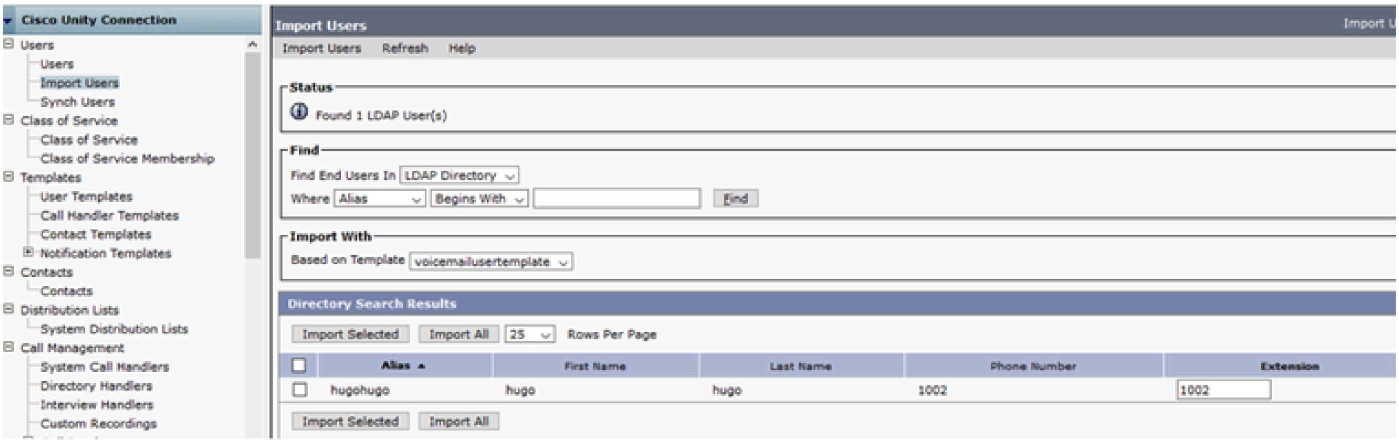
LDAP User Search Base* cn=users,dc=fhlab,dc=com

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.

Importez les utilisateurs LDAP auxquels la messagerie vocale sera affectée, ainsi que l'utilisateur qui servira à tester SSO.



Import Users

Status

Found 1 LDAP User(s)

Find

Find End Users In LDAP Directory

Where Alias Begins With

Import With

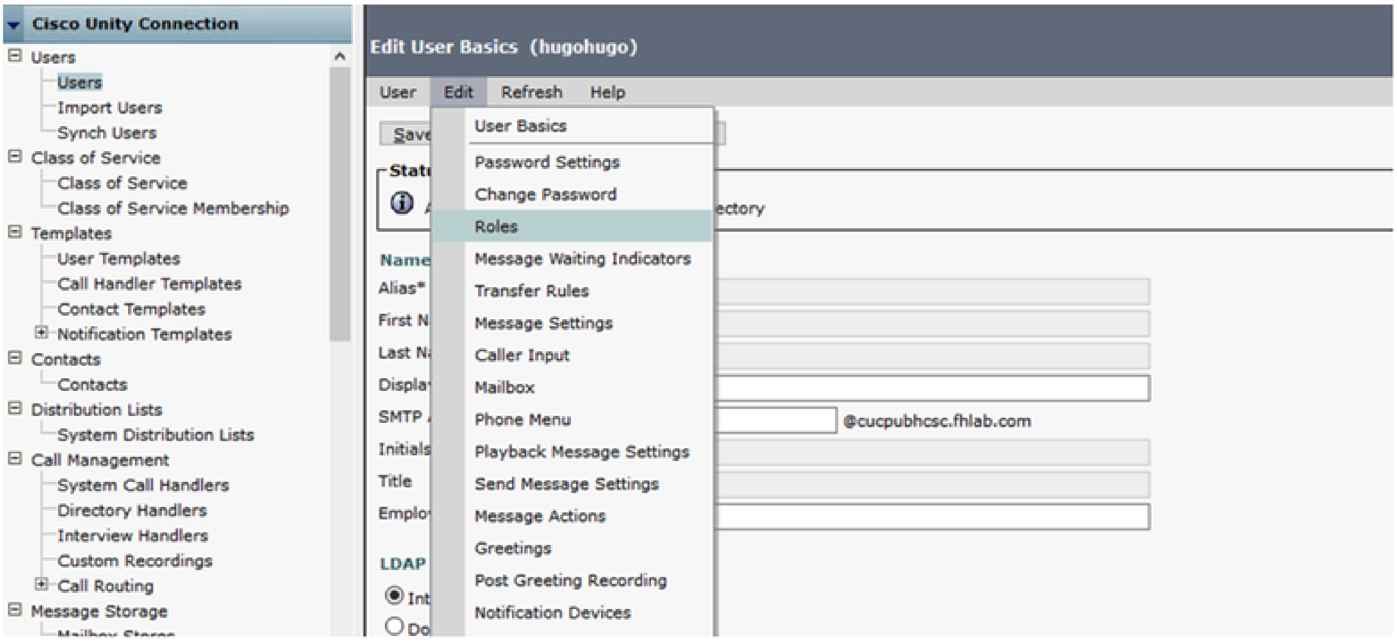
Based on Template voicemailusertemplate

Directory Search Results

25 Rows Per Page

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

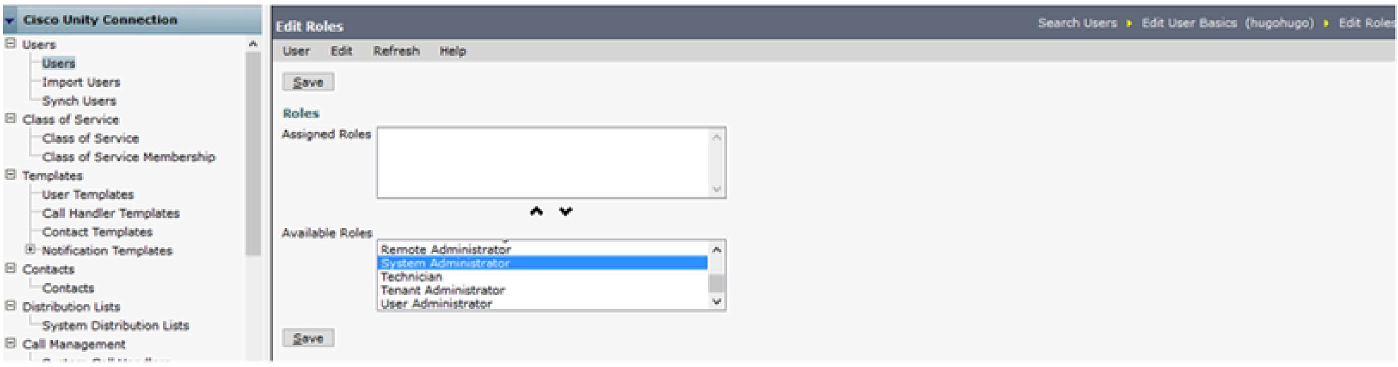
Accédez à **Utilisateurs > Modifier > Rôles** comme indiqué dans l'image.



Edit User Basics (hugohugo)

@cucpubhcsc.fhlab.com

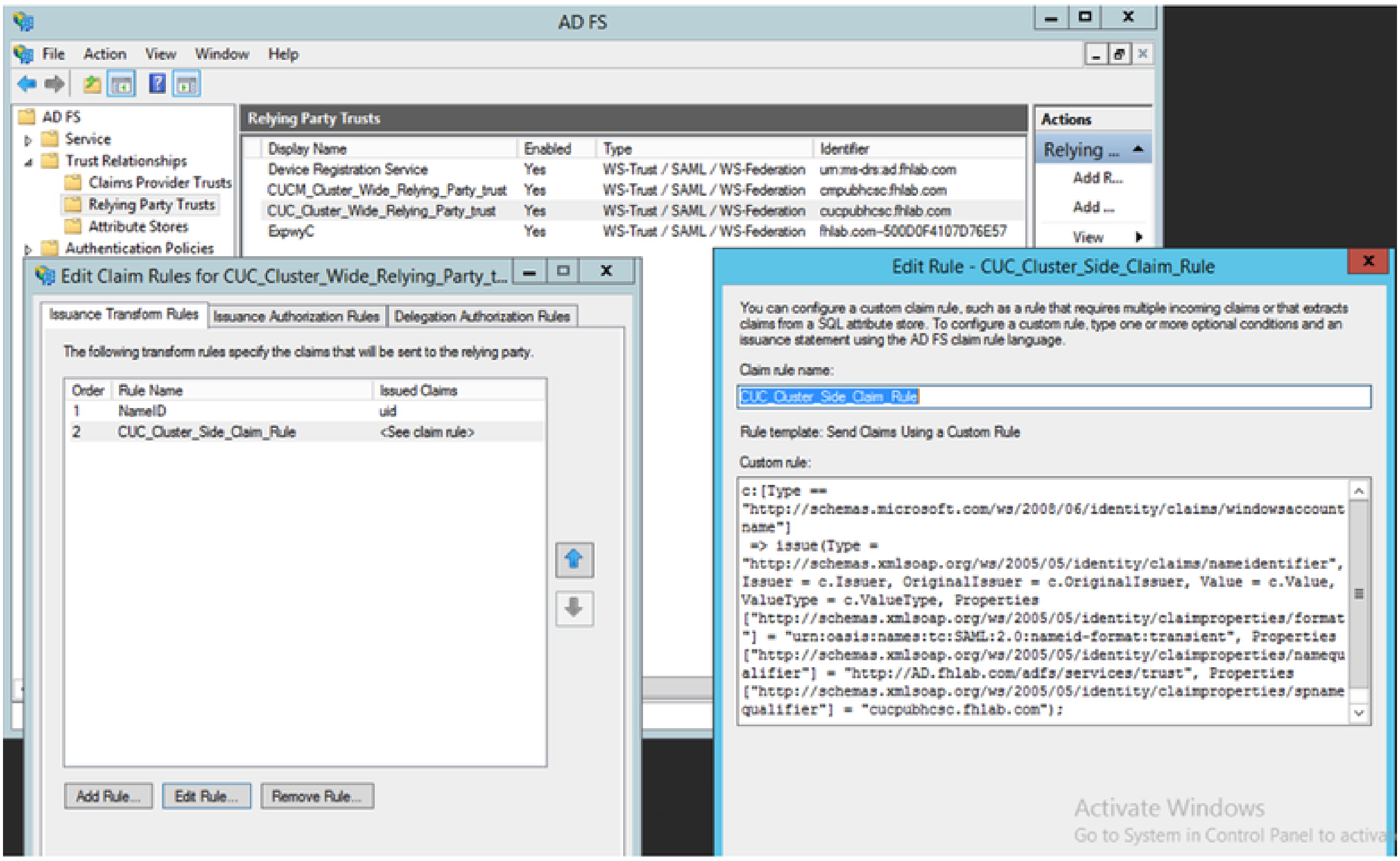
Attribuez à l'utilisateur de test le rôle Administrateur système.



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

Métadonnées CUC

Vous devez maintenant avoir téléchargé les métadonnées CUC, créé le RelyingPartyTrust pour CUC et téléchargé les métadonnées CUC et créé les règles I AD FS sur 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

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.

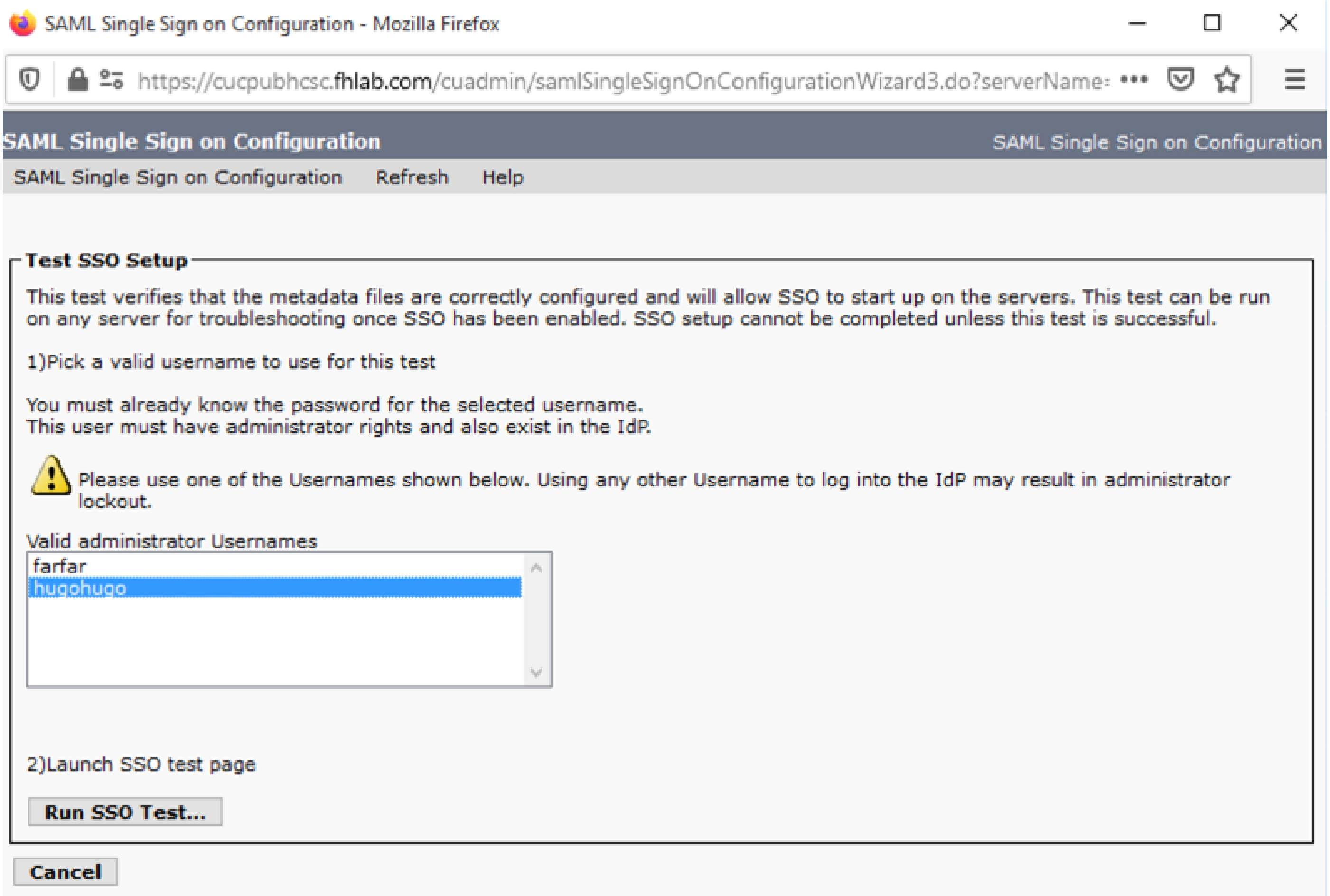
Claim rule name: CUC_Cluster_Side_Claim_Rule

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");
```

Accédez à Connexion unique SAML et activez 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.

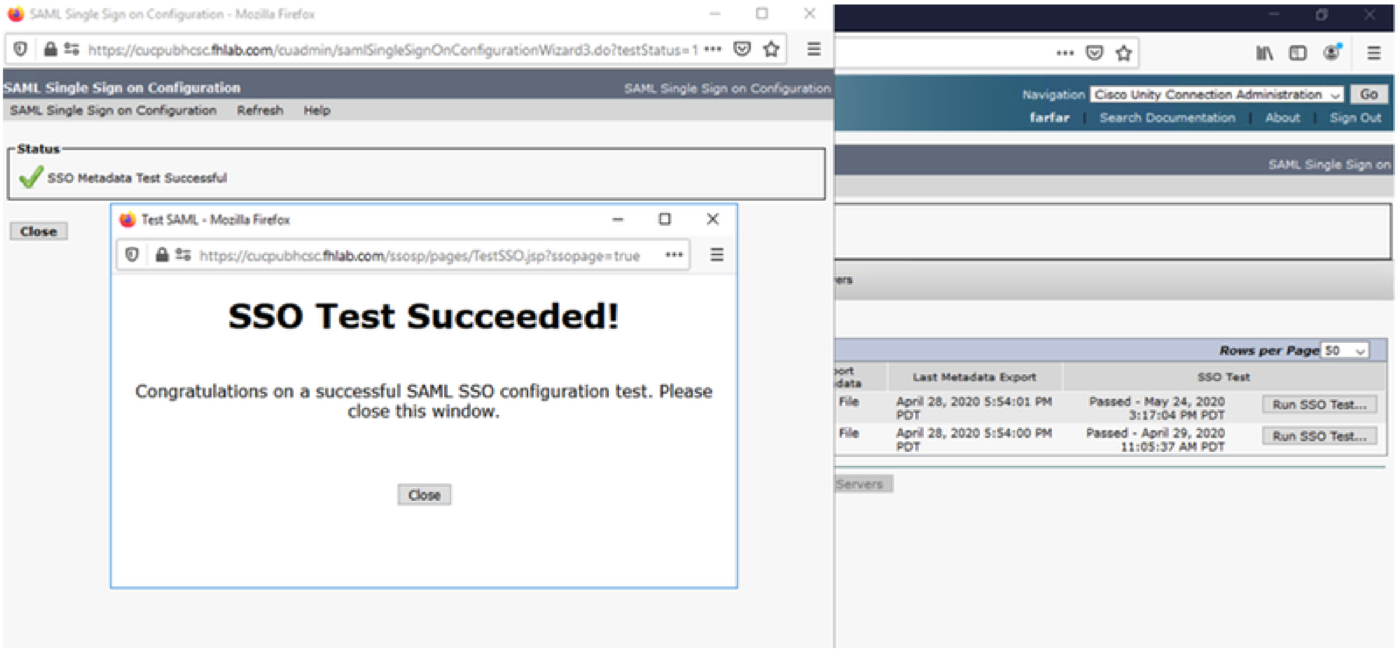
⚠ Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.

Valid administrator Usernames
farfar
hugohugo

2)Launch SSO test page

Run SSO Test...

Cancel



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
SAML Single Sign on Configuration
Refresh
Help

Status
✓ SSO Metadata Test Successful

Close
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.

Close
Navigation
Cisco Unity Connection Administration
Go
farfar
Search Documentation
About
Sign Out
SAML Single Sign on
ers
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...

Configuration de SSO sur Expressway

Importer des métadonnées sur Expressway C

Ouvrez un navigateur sur https://<ADFS FQDN>/FederationMetadata/2007-06/FederationMetadata.xml et ENREGISTREZ les métadonnées dans un dossier local

Télécharger vers **Configuration > Unified Communications > IDP**.

Exporter les métadonnées à partir d’Expressway C

Accéder à la configuration -> Communications unifiées -> PDI -> Exporter les données SAML

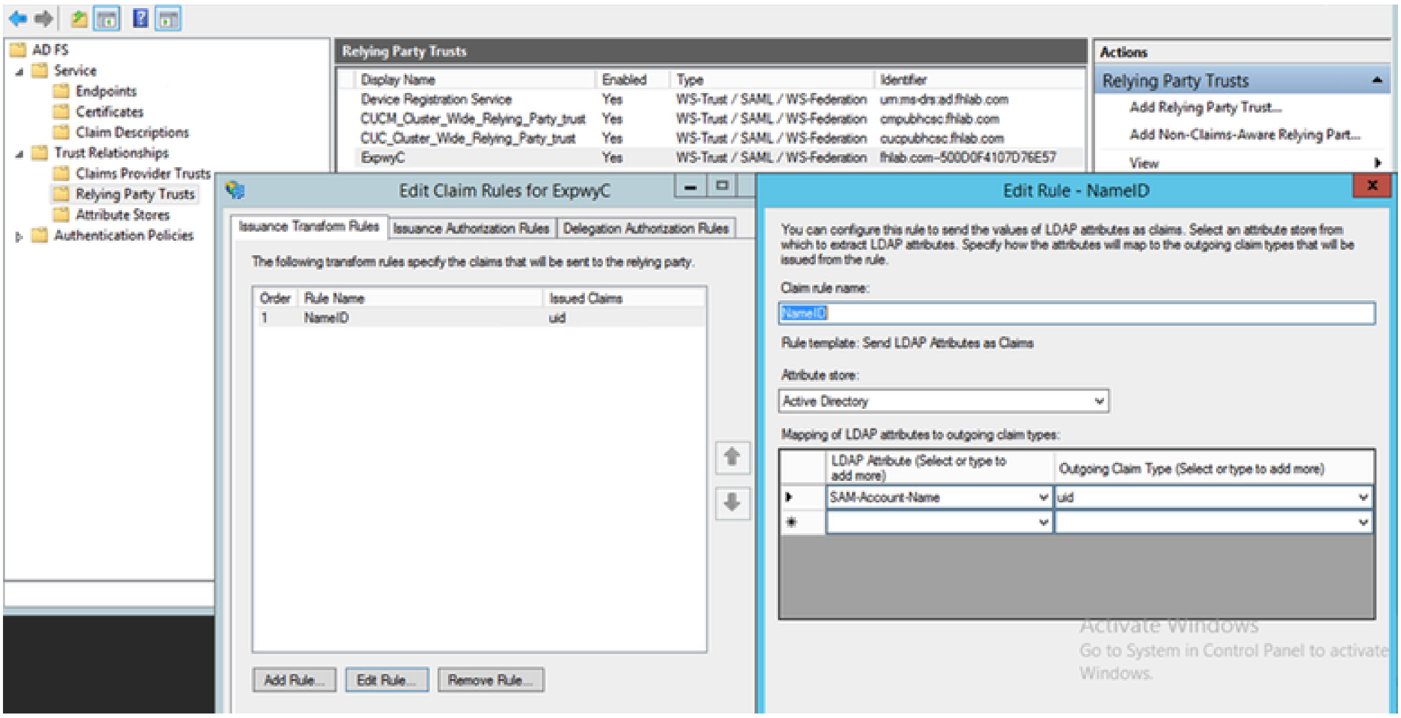
Le mode cluster utilise un certificat auto-signé (avec une longue durée de vie) inclus dans le SAML

Métadonnées et utilisées pour la signature de requêtes SAML

- En mode cluster, pour télécharger le fichier de métadonnées unique à l'échelle du cluster, cliquez sur Télécharger
- En mode par homologue, pour télécharger le fichier de métadonnées d'un homologue individuel, cliquez sur Télécharger en regard de l'homologue. Pour exporter tout dans un fichier .zip, cliquez sur Télécharger tout.

Ajouter une approbation de partie de confiance pour Cisco Expressway-E

Tout d’abord, créez des approbations de partie de confiance pour l’Expressway-Es, puis ajoutez une règle de revendication pour envoyer l’identité en tant qu’attribut 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

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

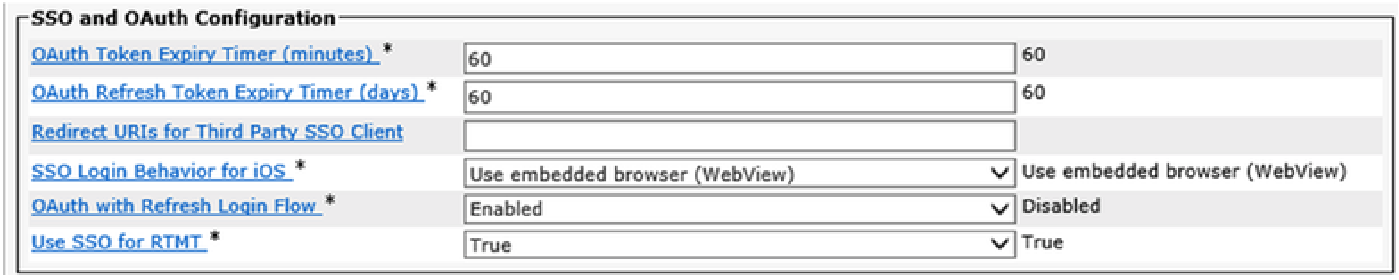
Attribute store: Active Directory

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 avec actualisation de la connexion

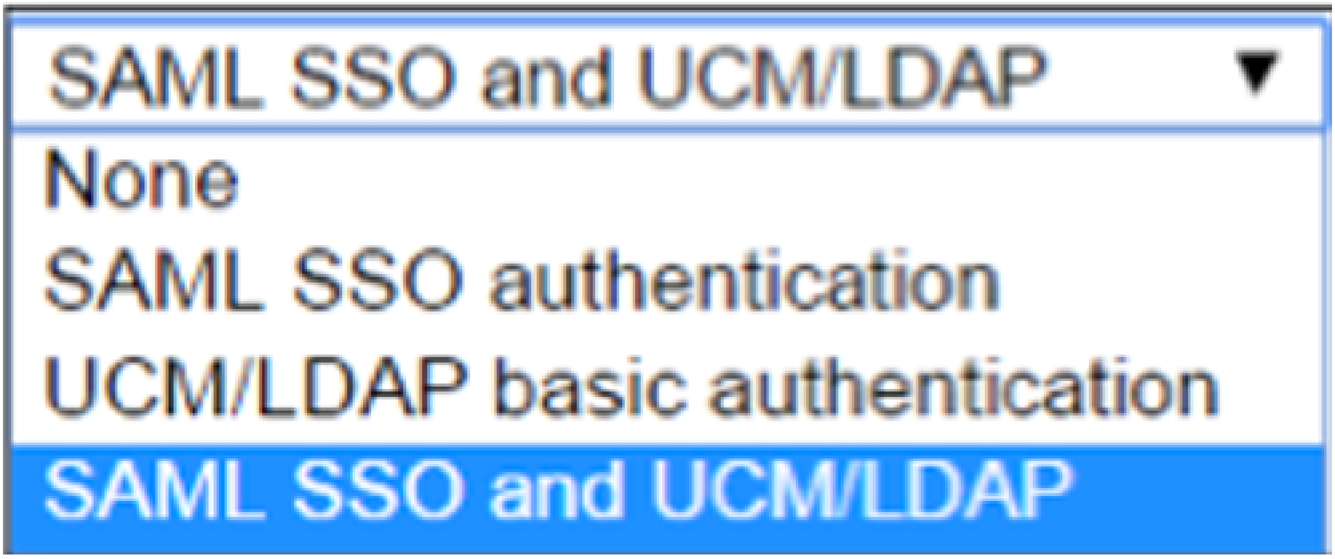
Dans les paramètres d'entreprise de Cisco CUCM, le paramètre de flux de connexion Verify OAuth with Refresh est activé. Accédez à **Cisco Unified CM Administration > Enterprise Parameters > SSO and OAuth Configuration**.



SSO and OAuth Configuration

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

Chemin d'authentification



SAML SSO and UCM/LDAP

- Si le chemin d’authentification est défini sur “ authentification SAML SSO ” seuls les clients Jabber utilisant une grappe Unified CM activée par SSO pourraient utiliser MRA sur cet Expressway. Il s'agit d'une configuration SSO uniquement.
- La prise en charge MRA d’Expressway pour tous les téléphones IP, tous les terminaux TelePresence et tous les clients Jabber hébergés dans un cluster Unified CM non configuré pour SSO nécessitera le chemin d’authentification pour inclure l’authentification UCM/LDAP.
- Si un ou plusieurs clusters Unified CM prennent en charge Jabber SSO, sélectionnez le ” SAML SSO et UCM/LDAP “ pour autoriser l'authentification de base et SSO.

Architecture SSO

SAML est un format de données XML standard ouvert qui permet aux administrateurs d'accéder de manière transparente à un ensemble défini d'applications de collaboration Cisco après s'être connectés à l'une de ces applications. SAML SSO utilise le protocole SAML 2.0 pour offrir une connexion unique interdomaine et interproduit pour les solutions de collaboration Cisco.

Flux de connexion sur site

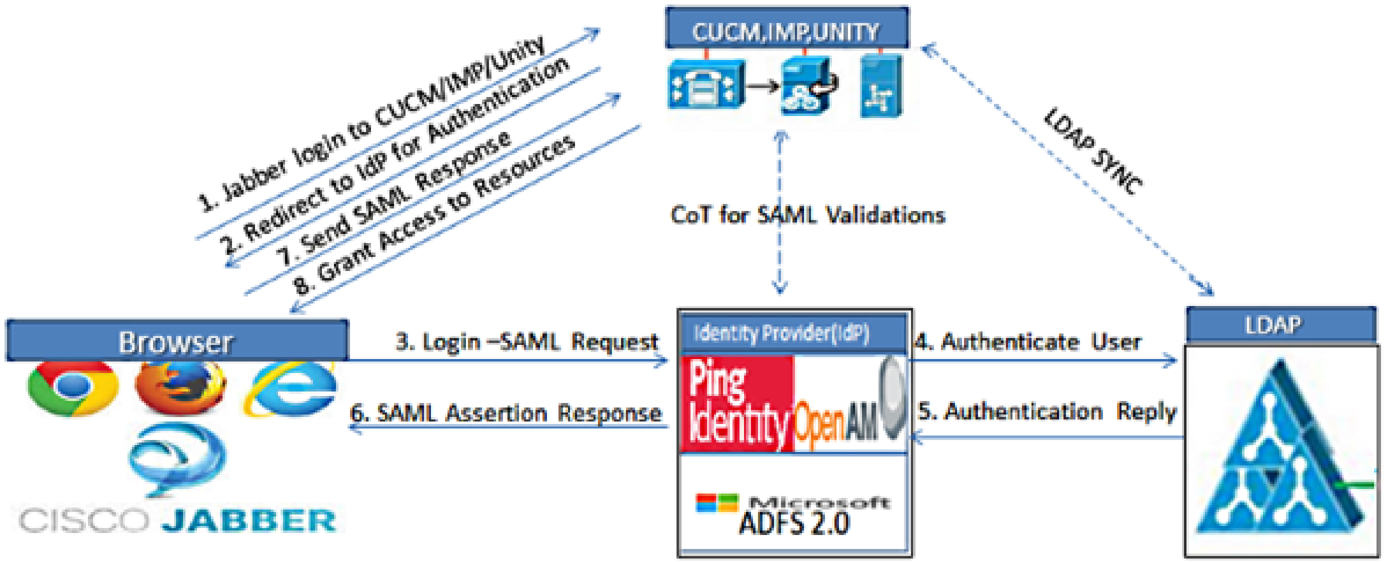
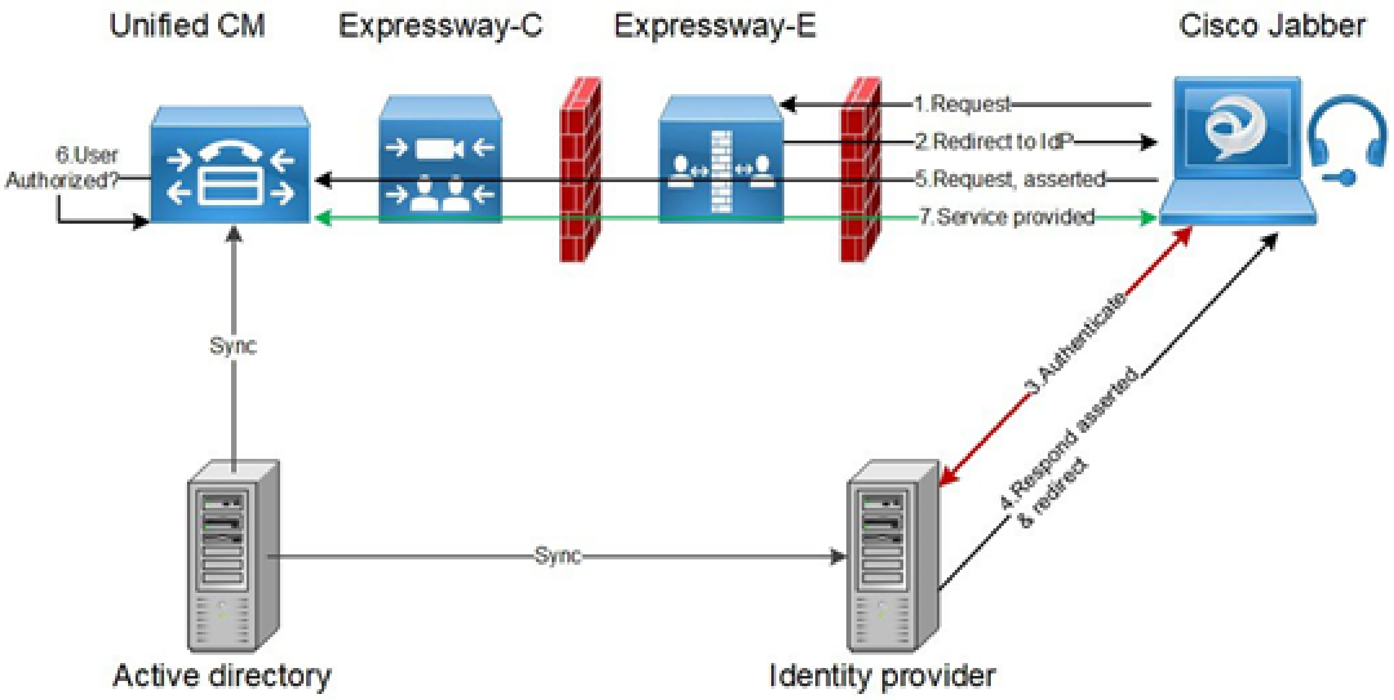


Figure :SAML Single sign SSO Call Flow for Collaboration Servers

Flux de connexion MRA



OAuth

OAuth est une norme qui prend en charge l'autorisation. Un utilisateur doit être authentifié avant d'être autorisé. Le flux d’octroi de code d’autorisation fournit une méthode permettant à un client d’obtenir des jetons d’accès et d’actualisation pour accéder à une ressource (services Unified CM, IM&P, Unity et Expressway). Ce flux est également basé sur la redirection et nécessite donc que le client puisse interagir avec un agent-utilisateur HTTP (navigateur web) contrôlé par l'utilisateur. Le client fera une demande initiale au serveur d'autorisation à l'aide de HTTPS. Le serveur OAuth redirige l'utilisateur vers un service d'authentification. Cela peut être exécuté sur Unified CM ou un IdP externe si SAML SSO est activé. Selon la méthode d'authentification utilisée, une page Web peut être présentée à l'utilisateur final pour s'authentifier. (L'authentification Kerberos est un exemple qui n'afficherait pas de page Web.) Contrairement au flux de subvention implicite, un flux de subvention de code d'authentification réussi entraînera l'émission par les serveurs OAuth d'un code d'autorisation “ ” au navigateur Web. Il s'agit d'un code unique à usage unique, de courte durée, qui est ensuite transféré du navigateur Web au client. Le client fournit ce code d'autorisation “ ” au serveur d'autorisation avec un secret pré-partagé et reçoit en échange un ” de jeton d'accès “ et un ” de jeton d'actualisation “. Le secret client utilisé dans cette étape permet au service d'autorisation de limiter l'utilisation aux clients enregistrés et authentifiés uniquement. Les jetons sont utilisés aux fins suivantes :

Jeton d'accès/d'actualisation

Jeton d'accès : Ce jeton est émis par le serveur d'autorisation. Le client présente le jeton à un serveur de ressources lorsqu'il a besoin d'accéder à des ressources protégées sur ce serveur. Le serveur de ressources peut valider le jeton et approuve les connexions à l'aide du jeton. (Les jetons d'accès Cisco ont une durée de vie de 60 minutes par défaut)

Actualiser le jeton : Ce jeton est à nouveau émis par le serveur d'autorisation. Le client présente ce jeton au serveur d'autorisation ainsi que le secret du client lorsque le jeton d'accès a expiré ou arrive à expiration. Si le jeton d'actualisation est toujours valide, le serveur d'autorisation émettra un nouveau jeton d'accès sans nécessiter une autre authentification. (Les jetons d'actualisation Cisco ont une durée de vie de 60 jours par défaut). Si le jeton d'actualisation a expiré, un nouveau flux complet d'octroi de code d'autorisation OAuth doit être lancé pour obtenir de nouveaux jetons.

Le flux de subvention du code d'autorisation OAuth est meilleur

Dans le flux de subvention implicite, le jeton d'accès est transmis au client Jabber via un agent utilisateur HTTP (navigateur). Dans le flux d'octroi de code d'autorisation, le jeton d'accès est échangé directement entre le serveur d'autorisation et le client Jabber. Le jeton est demandé au serveur d'autorisation à l'aide d'un code d'autorisation unique limité dans le temps. Cet échange direct du jeton d'accès est plus sûr et réduit l'exposition aux risques.

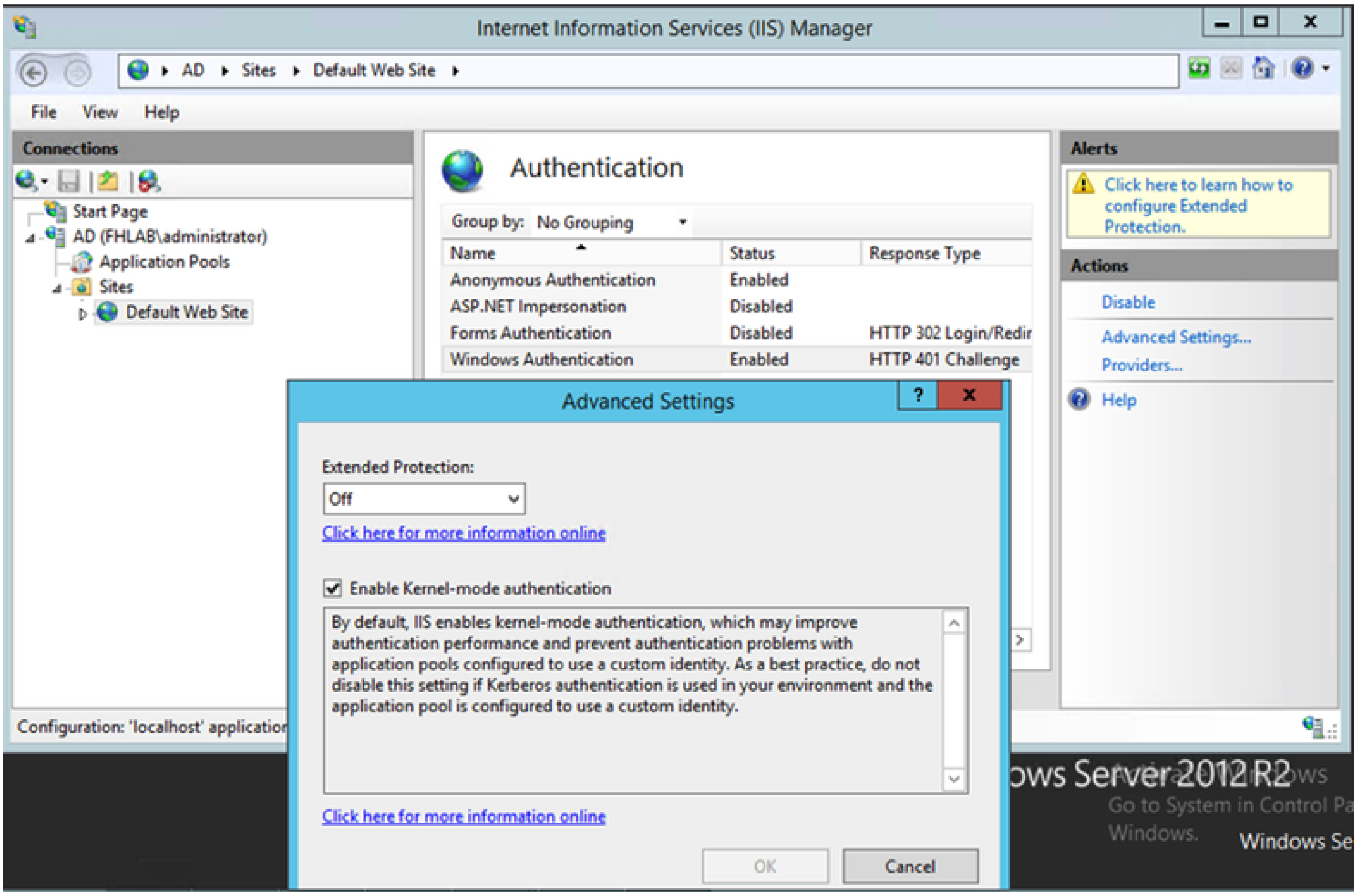
Le flux de subvention du code d'autorisation OAuth prend en charge l'utilisation de jetons d'actualisation. Cela offre une meilleure expérience à l'utilisateur final puisqu'il n'a pas besoin de se réauthentifier aussi fréquemment (par défaut, 60 jours)

Configurer Kerberos

Sélectionner l'authentification Windows

Gestionnaire des services Internet (IIS) > Sites > Site Web par défaut > Authentification > Authentification Windows > Paramètres avancés.

1. Décochez la case Activer l'authentification en mode noyau.
2. Assurez-vous que la protection étendue est désactivée.



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

Click here to learn how to configure Extended Protection.

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.

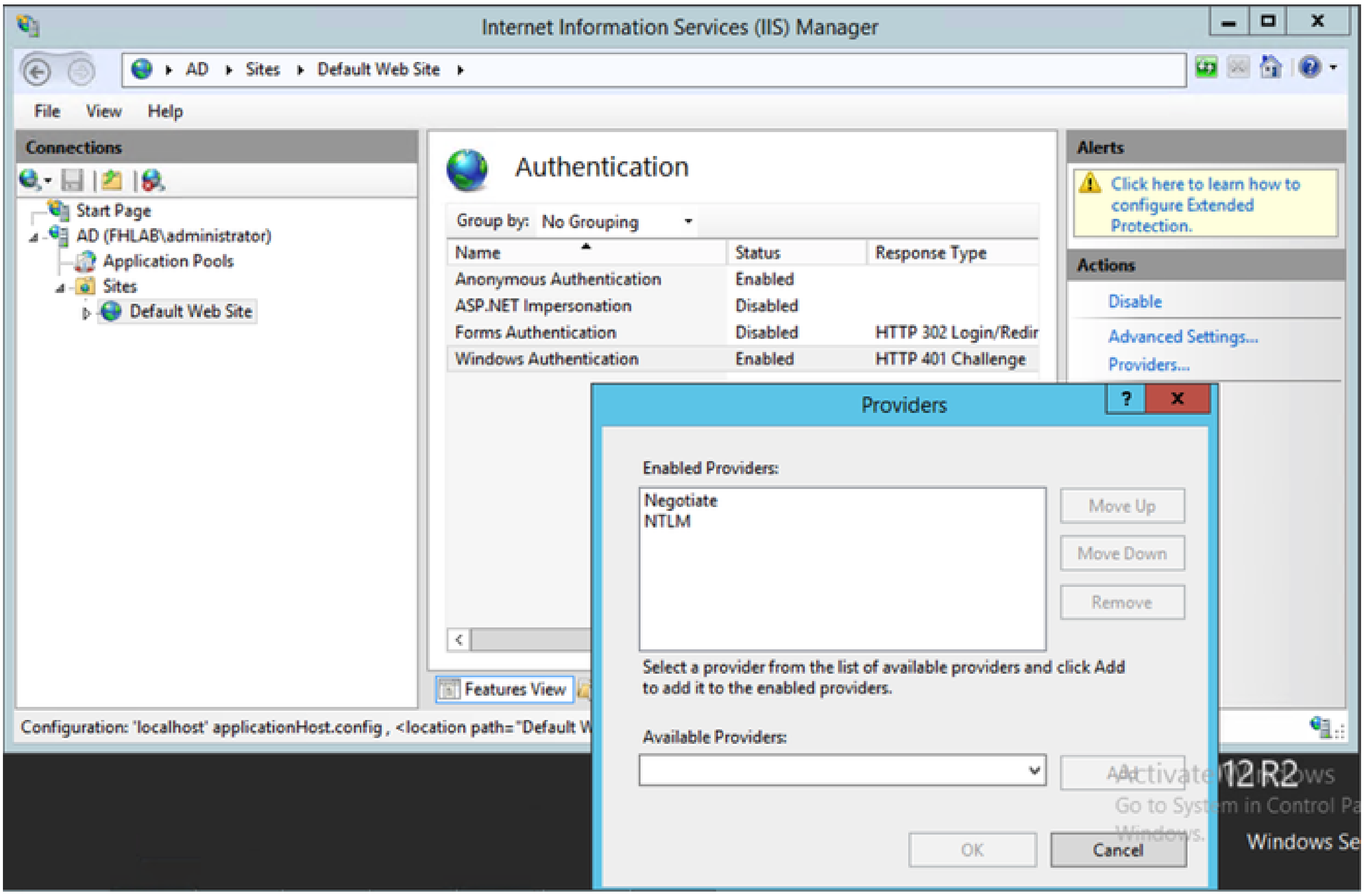
Click here for more information online

Configuration: 'localhost' application

ADFS prend en charge Kerberos NTLM

Assurez-vous qu'AD FS version 3.0 prend en charge le protocole Kerberos et le protocole NTLM (NT LAN Manager), car tous les clients non Windows ne peuvent pas utiliser Kerberos et utiliser NTLM.

Dans le volet de droite, sélectionnez Fournisseurs et assurez-vous que Negotiate et NTLM sont présents sous Fournisseurs activés :



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

Enabled Providers:

Negotiate
NTLM

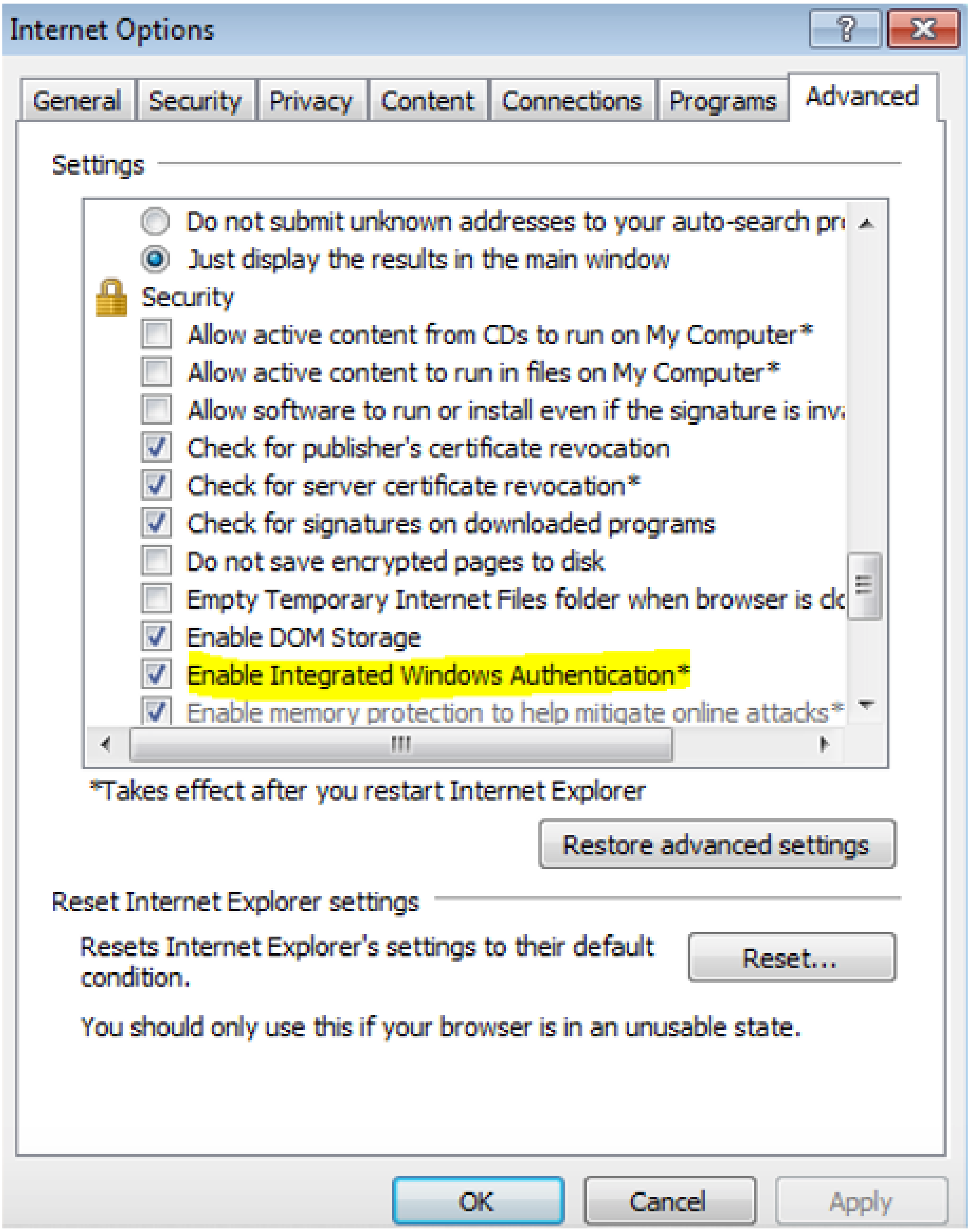
Select a provider from the list of available providers and click Add to add it to the enabled providers.

Available Providers:

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

Configurer Microsoft Internet Explorer

Assurez-vous que **Internet Explorer > Advanced > Enable Integrated Windows Authentication** est coché.



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.

Ajouter une URL ADFS sous Sécurité > Zones intranet > Sites