

Configuration de l'authentification unique avec CUCM et AD FS 2.0

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Téléchargez et installez AD FS 2.0 sur votre serveur Windows](#)

[Configurer AD FS 2.0 sur votre serveur Windows](#)

[Importer les métadonnées Idp dans CUCM / Télécharger les métadonnées CUCM](#)

[Importer les métadonnées CUCM sur le serveur AD FS 2.0 et créer des règles de revendication](#)

[Terminer l'activation SSO sur CUCM et exécuter le test SSO](#)

[Dépannage](#)

[Définir les journaux SSO à déboguer](#)

[Rechercher Le Nom Du Service De Fédération](#)

[Nom Du Service De Certificat Et De Fédération Sans Point](#)

[Le délai est désynchronisé entre les serveurs CUCM et IDP](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer l'authentification unique (SSO) sur Cisco Unified Communications Manager et le service de fédération Active Directory.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestionnaire de communications unifiées de Cisco (version CUCM)
- Connaissances de base du service de fédération Active Directory (AD FS)

Afin d'activer l'authentification unique dans votre environnement de travaux pratiques, vous avez besoin de cette configuration :

- Windows Server avec AD FS installé.
- CUCM avec synchronisation LDAP configurée.
- Utilisateur final avec le rôle de superutilisateur CCM standard sélectionné.

Composants utilisés

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

- Windows Server avec AD FS 2.0

- CUCM 10.5.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La procédure pour AD FS 2.0 avec Windows Server 2008 R2 est fournie. Ces étapes fonctionnent également pour AD FS 3.0 sur Windows Server 2016.

Téléchargez et installez AD FS 2.0 sur votre serveur Windows

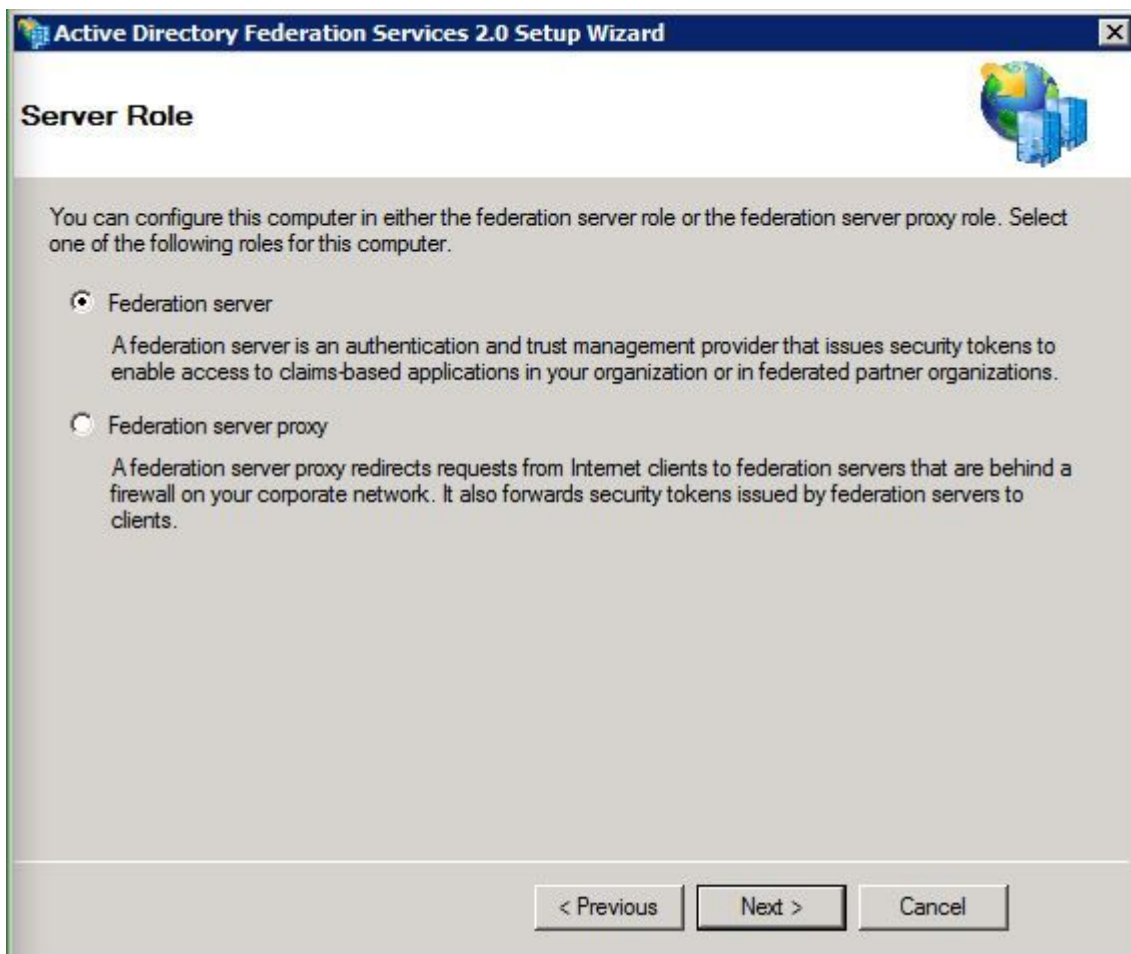
Étape 1. Accédez à [Télécharger AD FS 2.0](#).

Étape 2. Veillez à sélectionner le téléchargement approprié en fonction de votre serveur Windows.

Étape 3. **Déplacez** le fichier téléchargé vers votre serveur Windows.

Étape 4. Procédez à l'installation :

Étape 5. Lorsque vous y êtes invité, sélectionnez **Federation Server**:



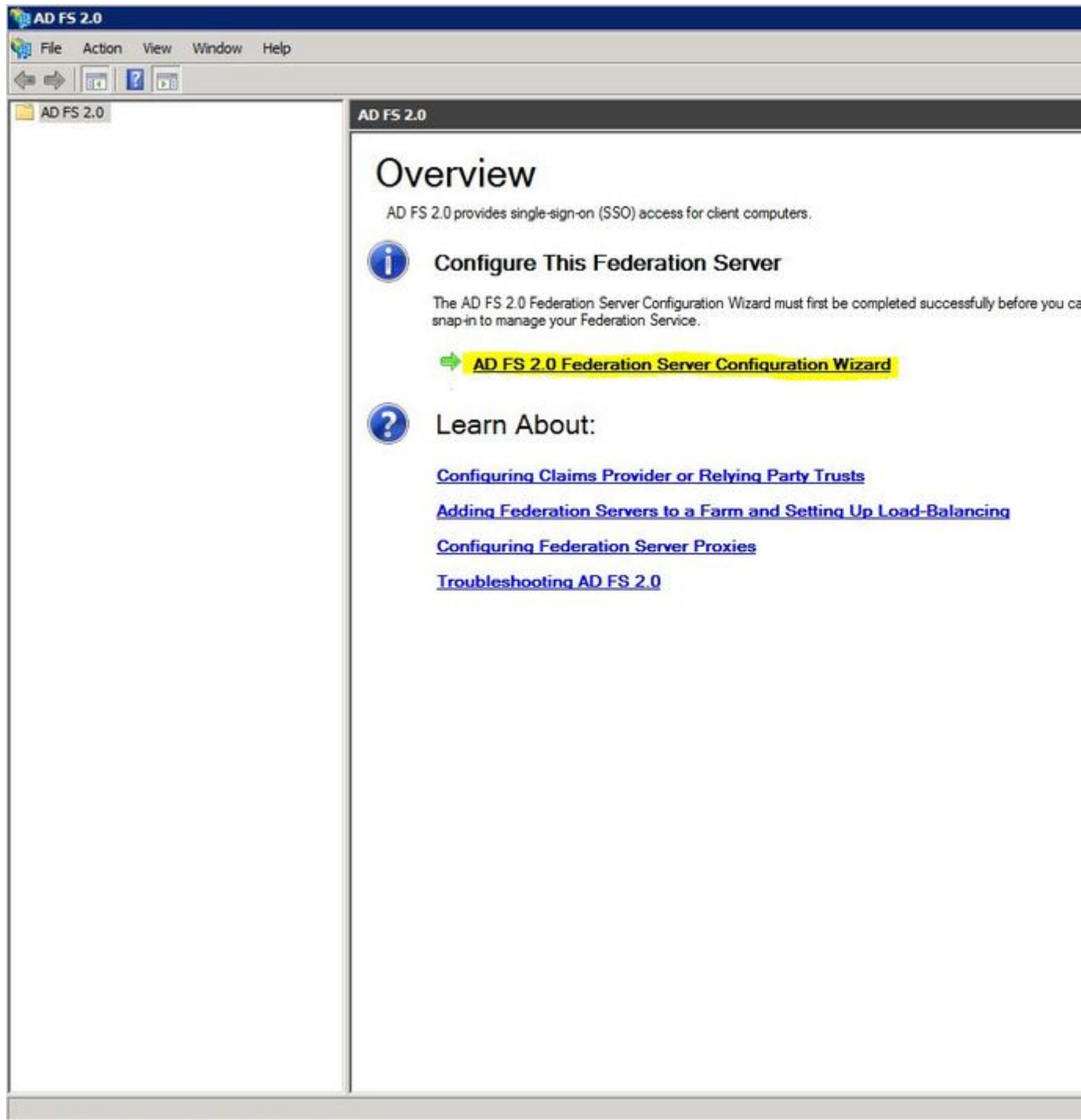
Étape 6. Certaines dépendances sont automatiquement installées. Une fois cela fait, cliquez sur **Terminer**.

Maintenant qu'AD FS 2.0 est installé sur votre serveur, vous devez ajouter une configuration.

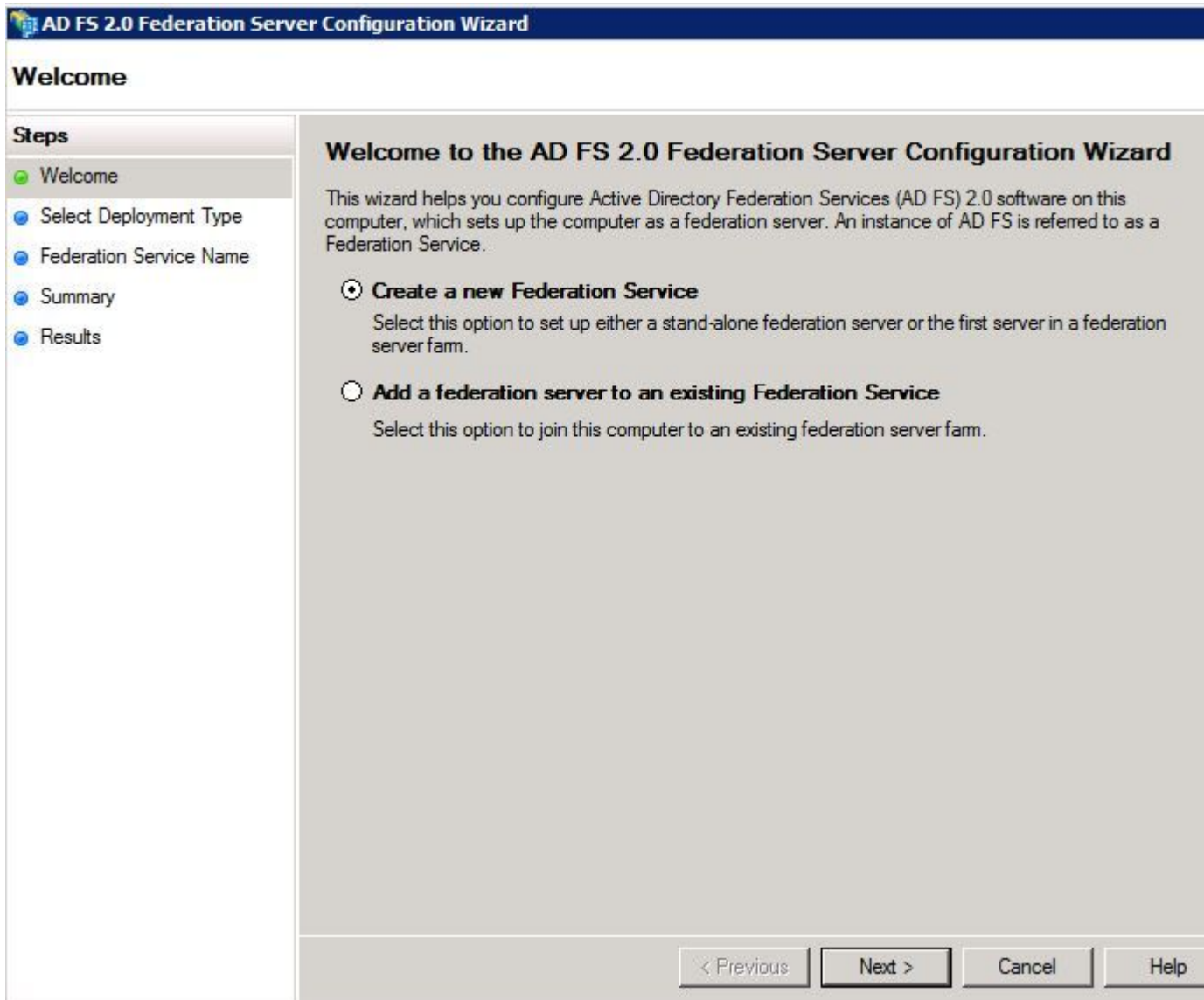
Configurer AD FS 2.0 sur votre serveur Windows

Étape 1. Si la fenêtre AD FS 2.0 ne s'est pas ouverte automatiquement après l'installation, vous pouvez cliquer sur **Démarrer** et rechercher Gestion AD FS 2.0 pour l'ouvrir manuellement.

Étape 2. Sélectionnez **Assistant Configuration du serveur de fédération AD FS 2.0**.



Étape 3. Cliquez ensuite sur **Create a new Federation Service**.



Étape 4. Pour la plupart des environnements, un **serveur de fédération autonome** est suffisant.

Select Stand-Alone or Farm Deployment

Steps

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

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.

i 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

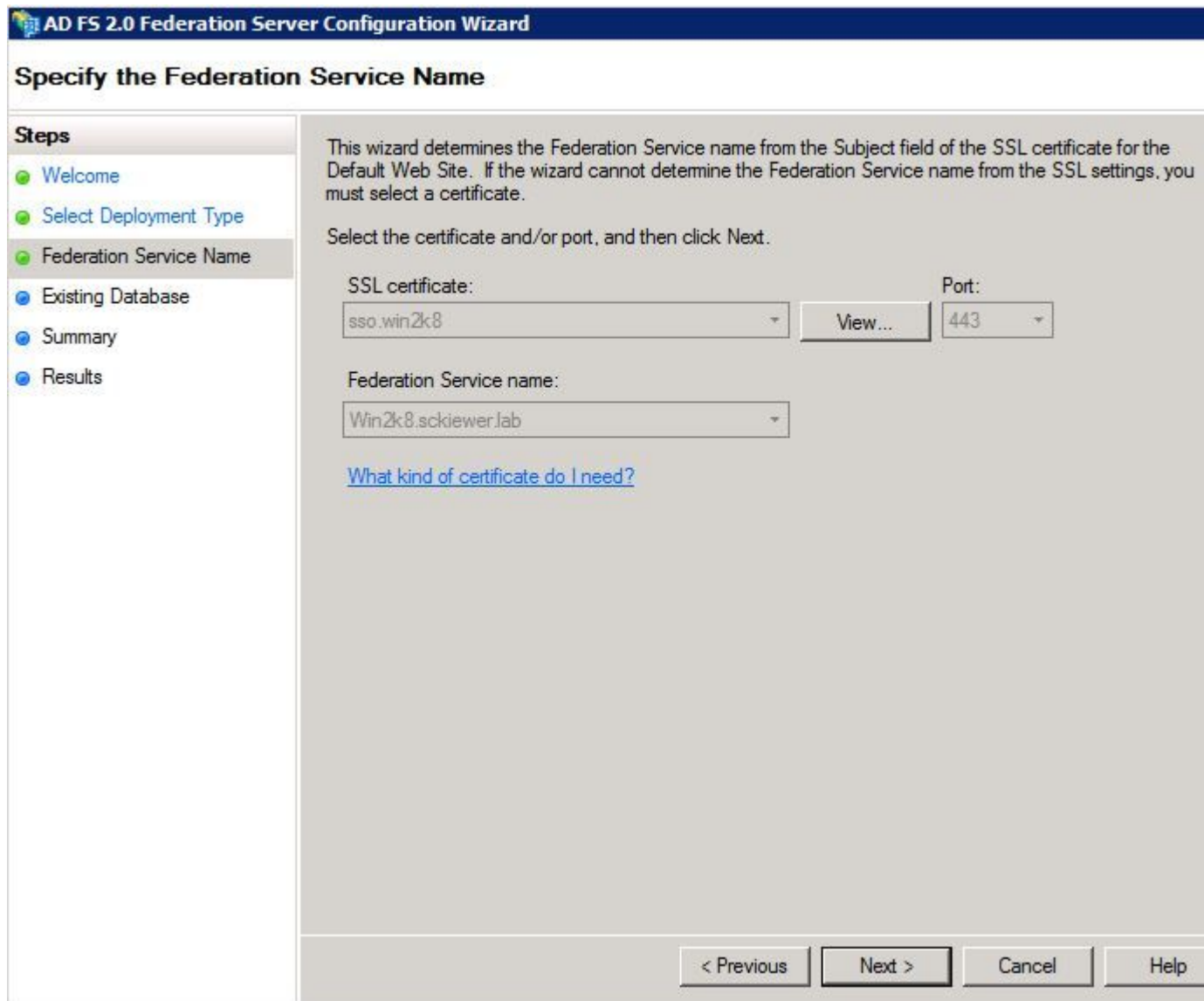
< Previous

Next >

Cancel

Help

Étape 5. Vous êtes ensuite invité à choisir un certificat. Ce champ est renseigné automatiquement tant que le serveur dispose d'un certificat.



Étape 6. Si vous disposez déjà d'une base de données AD FS sur le serveur, vous devez la supprimer pour continuer.

Étape 7. Enfin, vous êtes sur un écran récapitulatif dans lequel vous pouvez cliquer sur **Next**.

Importer les métadonnées Idp dans CUCM / Télécharger les métadonnées CUCM

Étape 1. Mettez à jour l'URL avec le nom d'hôte/nom de domaine complet de votre serveur Windows et téléchargez les métadonnées à partir de votre serveur AD FS - <https://hostname/federationmetadata/2007-06/federationmetadata.xml>

Étape 2. Accédez à **Cisco Unified CM Administration > System > SAML Single Sign-On**.

Étape 3. Cliquez sur **Enable SAML SSO**.

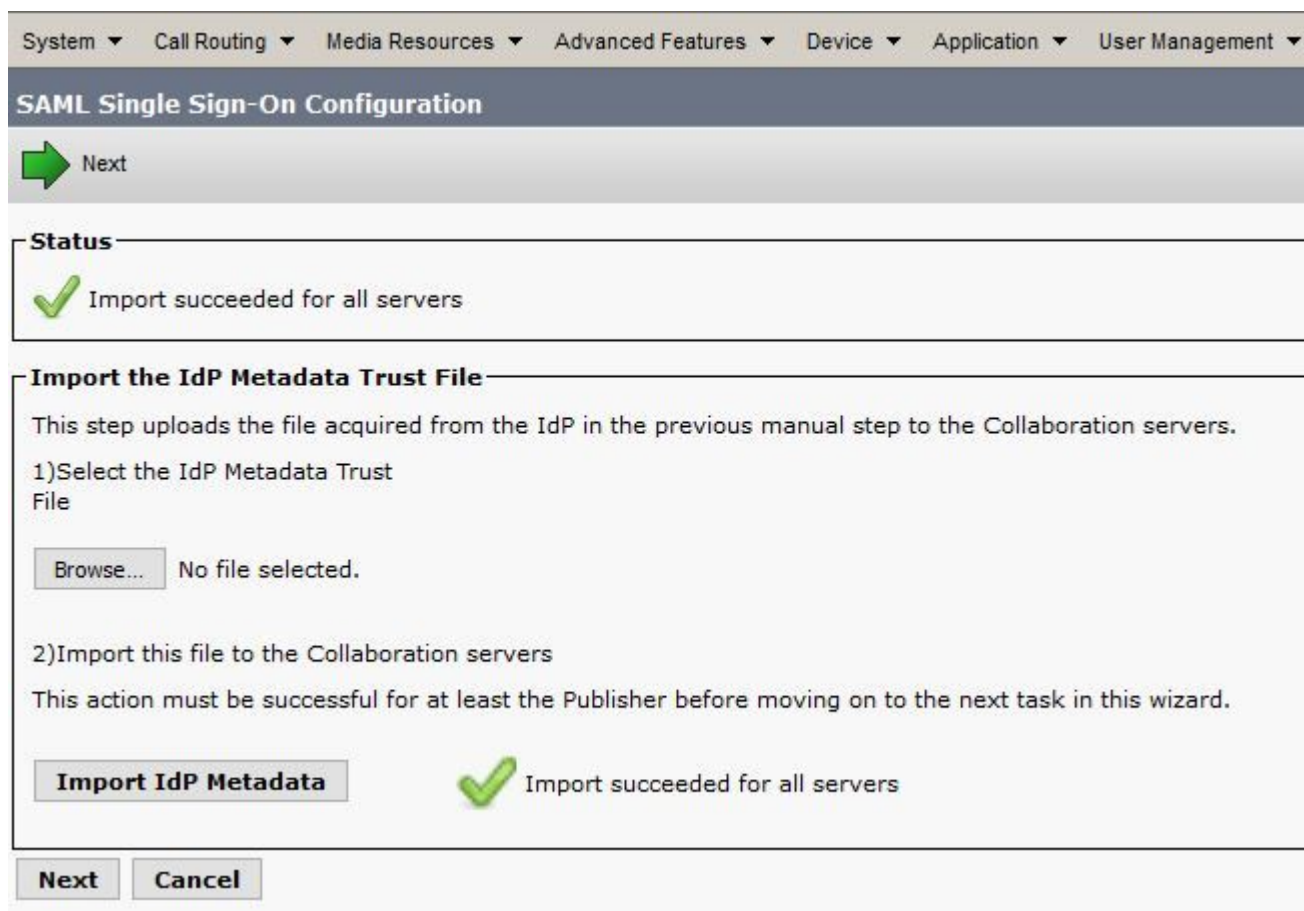
Étape 4. Si vous recevez une alerte à propos de Web Server Connections, cliquez sur **Continue**.

Étape 5. Ensuite, CUCM vous demande de télécharger le fichier de métadonnées à partir de votre

fournisseur d'identité. Dans ce scénario, votre serveur AD FS est le fournisseur d'identité et vous avez téléchargé les métadonnées à l'étape 1. Cliquez donc sur **Suivant**.

Étape 6. Cliquez sur **Browse > Select the .xml from Step 1 >** Cliquez sur **Import IdP Metadata**.

Étape 7. Un message indique que l'importation a réussi :



Étape 8. Cliquez sur Next (Suivant).

Étape 9. Maintenant que vous avez importé les métadonnées de l'IdP dans CUCM, vous devez importer les métadonnées de CUCM dans votre IdP.

Étape 10. Cliquez sur **Télécharger le fichier de métadonnées de confiance**.

Étape 11. Cliquez sur Next (Suivant).

Étape 12. Déplacez le fichier .zip vers votre serveur Windows et extrayez le contenu vers un dossier.

Importer les métadonnées CUCM sur le serveur AD FS 2.0 et créer des règles de revendication

Étape 1. Cliquez sur **Start** et recherchez **AD FS 2.0 Management**.

Étape 2. Cliquez sur **Obligatoire : Ajouter une partie de confiance approuvée**.

Remarque : si cette option n'apparaît pas, vous devez fermer la fenêtre et l'ouvrir de nouveau.

Étape 3. Une fois l'**Assistant Ajout d'approbation de partie de confiance** ouvert, cliquez sur **Démarrer**.

Étape 4. Ici, vous devez importer les fichiers XML que vous avez extraits à l'étape 12. Sélectionnez **Importer des données sur la partie de confiance à partir d'un fichier** et naviguez jusqu'aux fichiers de dossier et choisissez le fichier XML pour votre éditeur.

Remarque : suivez les étapes précédentes pour tout serveur de collaboration unifiée sur lequel vous envisagez d'utiliser SSO.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard'. The main window has a 'Steps' pane on the left with the following items: 'Welcome', 'Select Data Source' (highlighted), 'Specify Display Name', 'Choose Issuance Authorization Rules', 'Ready to Add Trust', and 'Finish'. The main area is titled 'Select Data Source' and contains the following text: 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options: 1. 'Import data about the relying party published online or on a local network'. Description: '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.' Input field: 'Federation metadata address (host name or URL):' with an empty text box. Example: 'fs.contoso.com or https://www.contoso.com/app'. 2. 'Import data about the relying party from a file'. Description: '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.' Input field: 'Federation metadata file location:' with a text box containing 'C:\Users\Administrator\Desktop\SPMetadata_1cucm1052.sckiewer.lab.xml' and a 'Browse...' button. 3. 'Enter data about the relying party manually'. Description: 'Use this option to manually input the necessary data about this relying party organization.' At the bottom right, there are four buttons: '< Previous', 'Next >', 'Cancel', and 'Help'.

Étape 5. Cliquez sur Next (Suivant).

Étape 6. Modifiez le **nom d'affichage** et cliquez sur **Suivant**.

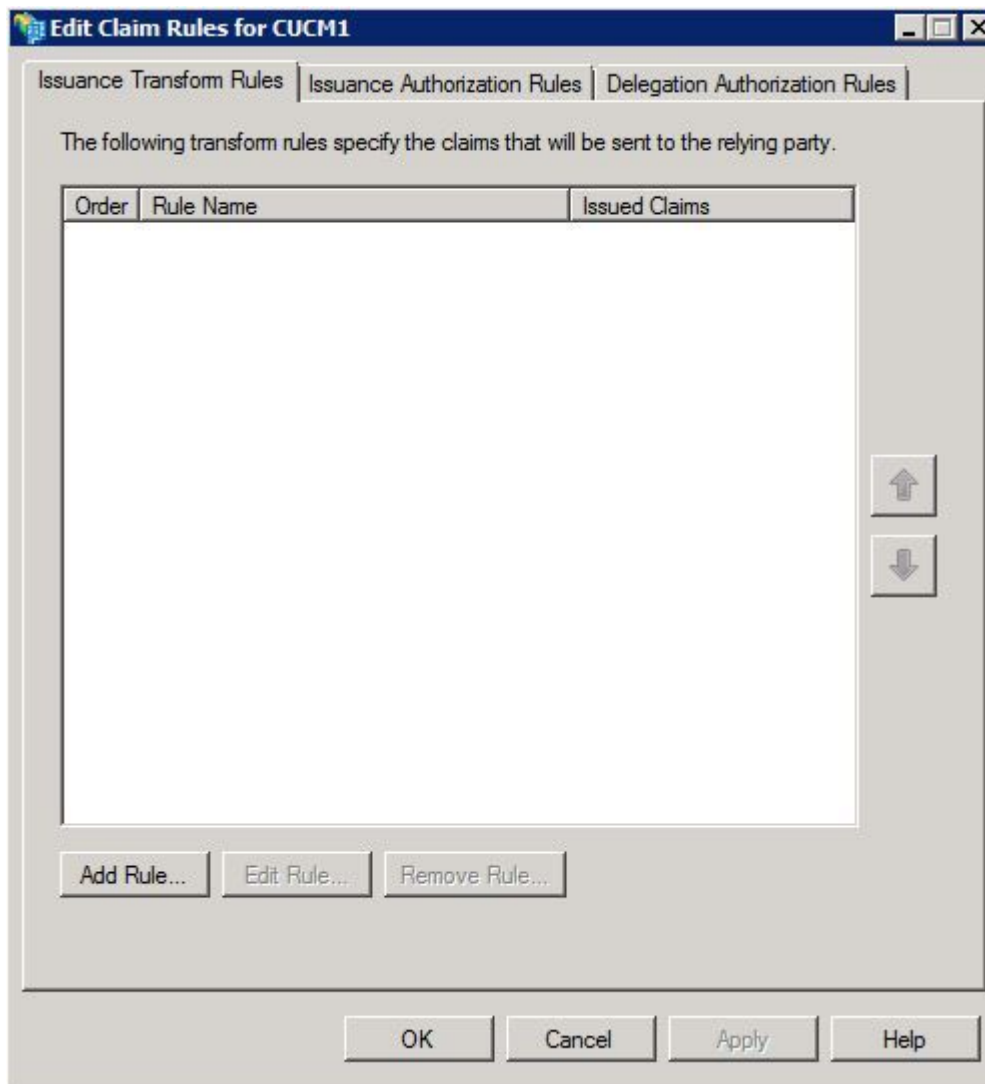
Étape 7. Sélectionnez **Autoriser tous les utilisateurs à accéder à cette partie de confiance** et cliquez sur **Suivant**.

Étape 8. Cliquez à nouveau sur **Next**.

Étape 9. Dans cet écran, assurez-vous que **la case Ouvrir la boîte de dialogue Modifier les règles de revendication pour cette approbation de partie de confiance est cochée lorsque l'Assistant se**

ferme, puis cliquez sur **Fermer**.

Étape 10. La fenêtre Modifier les règles de réclamation s'ouvre :



Étape 11. Dans cette fenêtre, cliquez sur **Add Rule**.

Étape 12. Pour le **modèle de règle de revendication**, choisissez **Envoyer les attributs LDAP en tant que revendications** et cliquez sur **Suivant**.

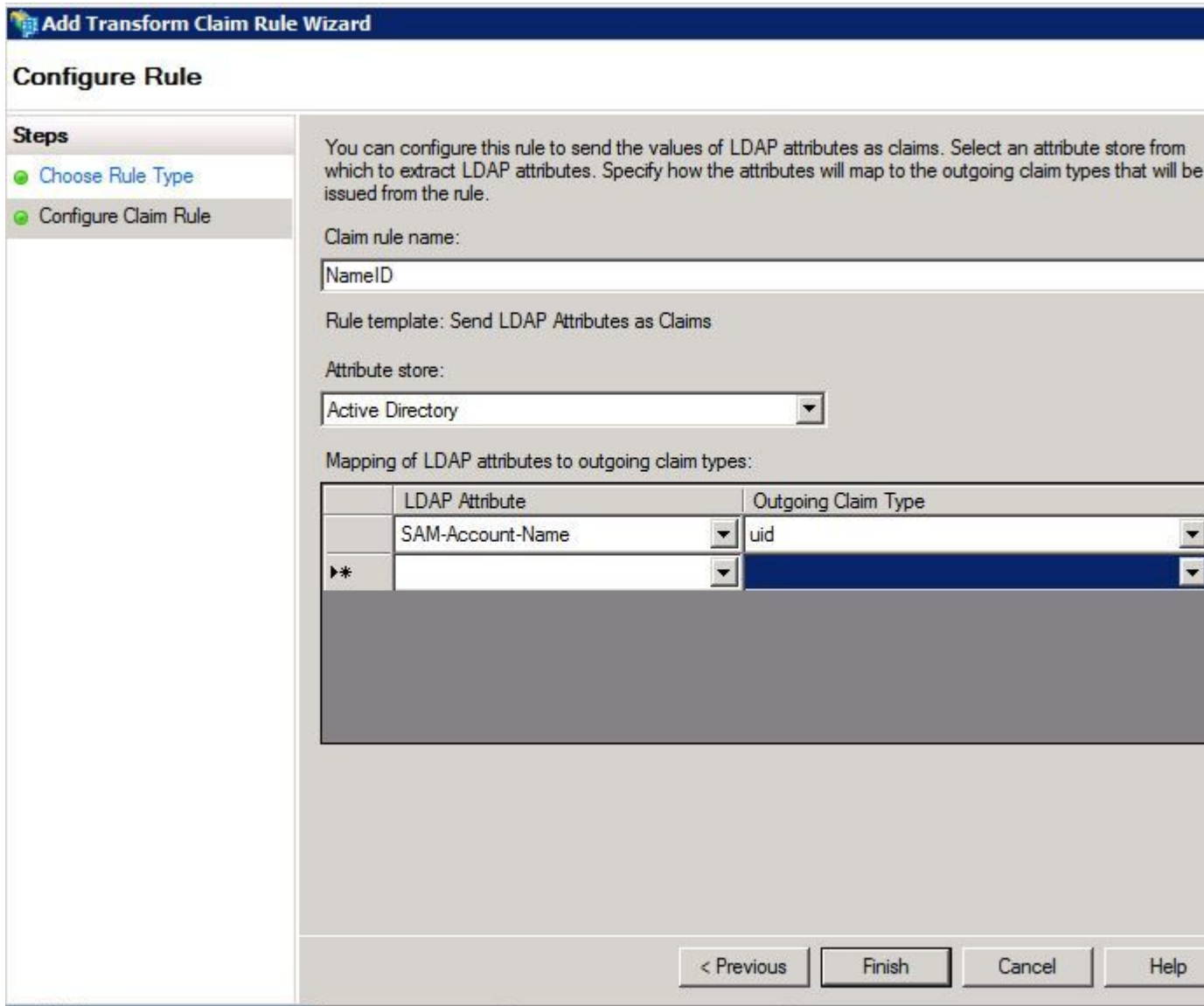
Étape 13. Sur la page suivante, entrez **NameID** comme **nom de règle de revendication**.

Étape 14. Sélectionnez **Active Directory** pour le **magasin d'attributs**.

Étape 15. Choisissez **SAM-Account-Name** pour l'**attribut LDAP**.

Étape 16. Entrez **uid** pour le **type de demande sortante**.

Remarque : l'uid n'est pas une option de la liste déroulante. Vous devez l'entrer manuellement.



Étape 17. Cliquez sur Finish (Terminer).

Étape 18. La première règle est maintenant terminée. Cliquez à nouveau sur **Ajouter une règle**.

Étape 19. Sélectionnez **Envoyer les revendications à l'aide d'une règle personnalisée**.

Étape 20. Entrez un **nom de règle de revendication**.

Étape 21. Dans le champ **Règle personnalisée**, collez ce texte :

```
c : [Tapez == "http://schemas.microsoft.com/ws/2008/06/identity/revendications/nomcompte windows"]
=> problème(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claim/nameidentfier", 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", Propriétés["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
"http://ADFS\_FEDERATION\_SERVICE\_NAME/com/adfs/service/trust",
Propriétés["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"CUCM_ENTITY_ID");
```

Étape 22. Veillez à remplacer AD_FS_SERVICE_NAME et CUCM_ENTITY_ID par les valeurs appropriées.

Remarque : si vous n'êtes pas sûr du nom du service AD FS, vous pouvez suivre les étapes pour le trouver. L'ID d'entité CUCM peut être extrait de la première ligne du fichier de métadonnées CUCM. La première ligne du fichier contient un entityID qui ressemble à ceci : entityID=1cucm1052.sckiewer.lab,. Vous devez saisir la valeur soulignée dans la section appropriée de la règle de demande.

The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box, specifically the 'Configure Rule' step. The 'Steps' pane on the left shows 'Configure Claim Rule' as the current step. The main area contains the following text:

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS 2.0 claim rule language.

Claim rule name: CUCM SSO Custom Rule

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
=> issue (Type =  
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",  
Properties  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =  
"http://win2k8.sckiewer.lab/adfs/com/adfs/service/trust", Properties  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "1cucm1052.sckiewer.lab");
```

[More about the claim rule language...](#)

At the bottom, there are buttons for '< Previous', 'Finish', 'Cancel', and 'Help'.

Étape 23. Cliquez sur Finish (Terminer).

Étape 24. Cliquez sur OK.


Remarque : des règles de demande sont nécessaires pour tout serveur de collaboration unifiée sur lequel vous avez l'intention d'utiliser SSO.

Terminer l'activation SSO sur CUCM et exécuter le test SSO


Étape 1. Maintenant que le serveur AD FS est entièrement configuré, vous pouvez revenir à CUCM.

Étape 2. Vous vous êtes arrêté sur la page de configuration finale :

SAML Single Sign-On Configuration

 Back

Status


 The server metadata file must be installed on the IdP before this test is run.

Test SSO Setup

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test

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 administrative access.

Valid administrator Usernames

sckiewer

2) Launch SSO test page

Étape 3. Sélectionnez l'utilisateur final pour lequel le rôle **Superutilisateurs CCM standard est** sélectionné et cliquez sur **Exécuter le test SSO...**

Étape 4. Assurez-vous que votre navigateur autorise les fenêtres publicitaires intempestives et entrez vos informations d'identification dans l'invite.

SSO Test Succeeded!

Congratulations on a successful SAML SSO configuration test. Please close this window and click "Finish" on the SAML configuration wizard to complete the setup.

Close

Étape 5. Cliquez sur **Close** dans la fenêtre contextuelle, puis sur **Finish**.

Étape 6. Après un bref redémarrage des applications Web, l'authentification unique est activée.

Dépannage

Définir les journaux SSO à déboguer

Pour définir les journaux SSO sur debug, vous devez exécuter cette commande dans la CLI de CUCM : **set samltrace level debug**

Les journaux SSO peuvent être téléchargés depuis RTMT. Le nom du jeu de journaux est **Cisco SSO**.

Rechercher Le Nom Du Service De Fédération

Pour trouver le nom du service de fédération, cliquez sur **Démarrer** et recherchez **Gestion AD FS 2.0**.

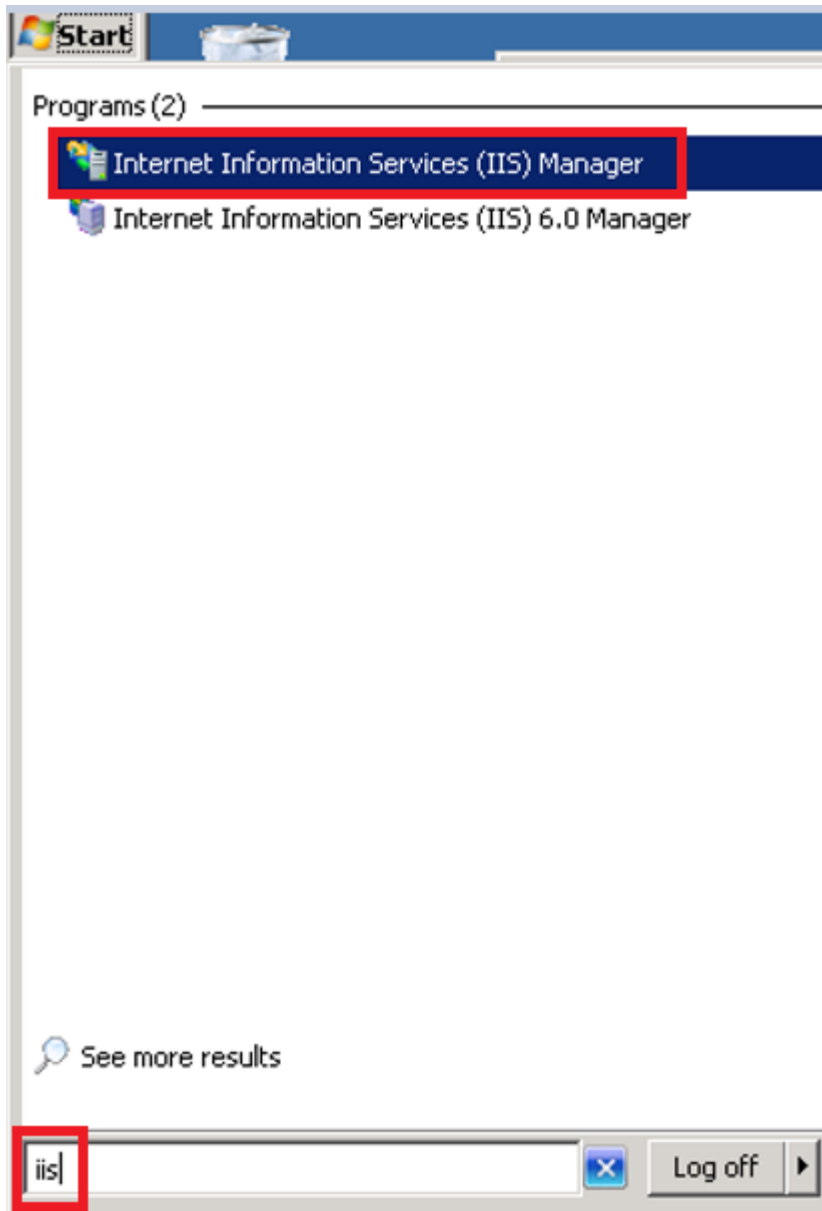
- Cliquez sur Edit **Federation Service Properties...**
- Dans l'onglet Général, recherchez le **nom du service de fédération**

Nom Du Service De Certificat Et De Fédération Sans Point

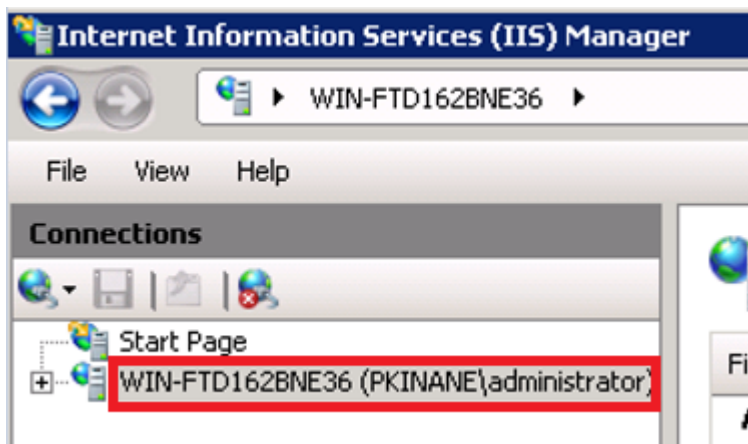
Si vous recevez ce message d'erreur dans l'assistant de configuration AD FS, vous devez créer un nouveau certificat.

Le certificat sélectionné ne peut pas être utilisé pour déterminer le nom du service de fédération, car le certificat sélectionné a un nom d'objet sans point (abrégé). Sélectionnez un autre certificat sans nom d'objet sans point (abrégé), puis réessayez.

Étape 1. Cliquez sur Démarrer et recherchez iis, puis ouvrez le Gestionnaire des services Internet (IIS)

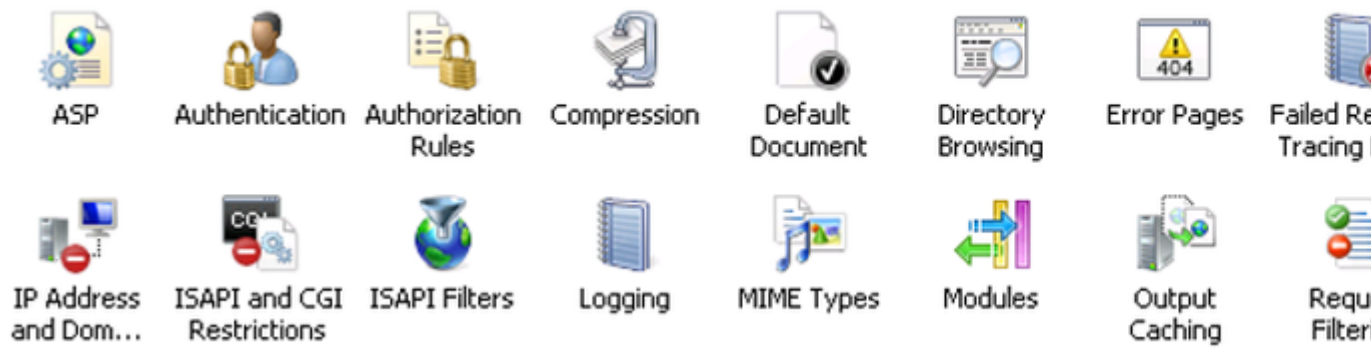


Étape 2. Cliquez sur le nom de votre serveur.

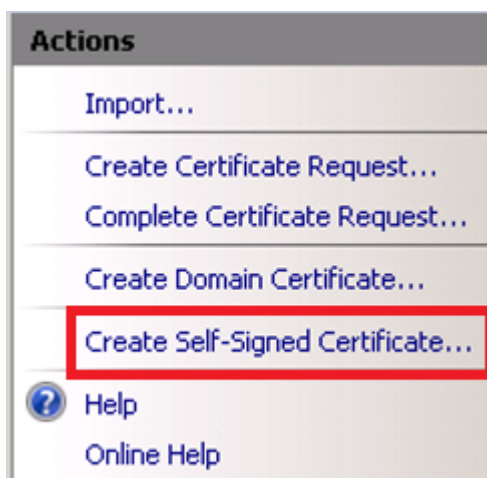


Étape 3. Cliquez sur Certificats du serveur.

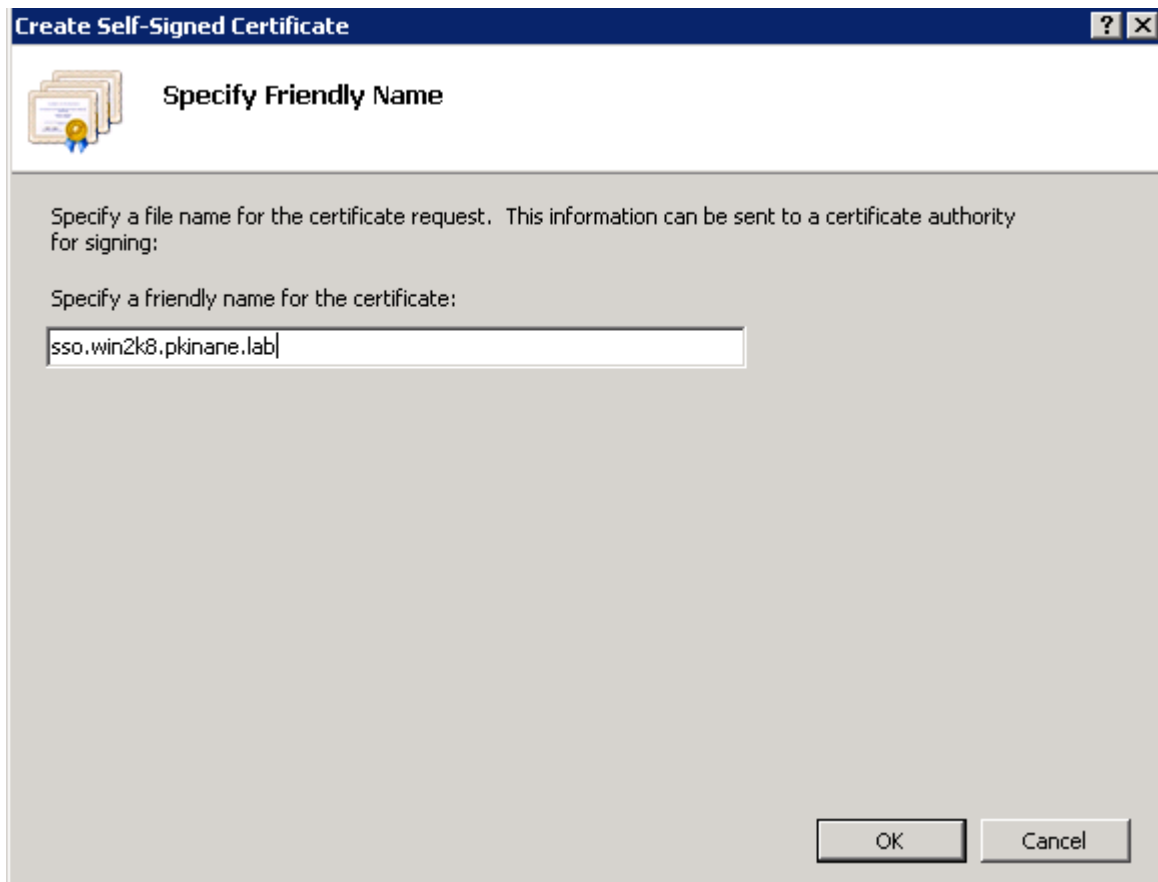
IIS



Étape 4. Cliquez sur Créer un certificat auto-signé.



Étape 5. Entrez le nom que vous souhaitez attribuer à l'alias de votre certificat.



Le délai est désynchronisé entre les serveurs CUCM et IDP

Si vous recevez cette erreur lorsque vous exécutez le test SSO à partir de CUCM, vous devez configurer Windows Server pour utiliser le ou les mêmes serveurs NTP que CUCM.

Réponse SAML non valide. Cela peut se produire lorsque le temps est désynchronisé entre Cisco Unified Communications Manager et les serveurs IDP. Vérifiez la configuration NTP sur les deux serveurs. Exécutez « `utils ntp status` » à partir de l'interface de ligne de commande pour vérifier cet état sur Cisco Unified Communications Manager.

Une fois que les serveurs NTP spécifiés pour Windows Server sont corrects, vous devez effectuer un autre test SSO et voir si le problème persiste. Dans certains cas, il est nécessaire de biaiser la période de validité de l'assertion. Plus de détails sur ce processus [ici](#).

Informations connexes

- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.