

# Configuration d'une connexion/d'un contrat SAML par cluster avec AD FS version 2.0

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Étape 1. Exporter les métadonnées SP de CUCM](#)

[Étape 2. Télécharger les métadonnées PCI à partir d'AD FS](#)

[Étape 3. IdP de provisionnement](#)

[Étape 4. Activer SAML SSO](#)

[Vérification](#)

[Dépannage](#)

## Introduction

Ce document décrit comment configurer la connexion/l'accord de fournisseur d'identité (IdP) SAML (Single Security Assertion Markup Language) par cluster avec Active Directory Federation Service (AD FS).

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Communications Manager (CUCM) 11.5 ou version ultérieure
- Cisco Unified Communications Manager IM and Presence version 11.5 ou ultérieure
- Service de fédération Active Directory version 2.0

### Components Used

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

- Service de fédération Active Directory version 2.0 en tant qu'IDP
- Cisco Unified Communications Manager version 11.5
- Cisco IM and Presence Server version 11.5

## Informations générales

Pour SAML SSO, doit être un cercle de confiance entre le fournisseur de services (SP) et l'IDP. Cette approbation est créée dans le cadre de SSO Enablement, lorsque la confiance (métadonnées) est échangée. Téléchargez les métadonnées à partir de CUCM et téléchargez-les sur IdP, téléchargez les métadonnées à partir de IdP et téléchargez-les sur CUCM.

Avant CUCM 11.5, le noeud d'origine génère le fichier de métadonnées et collecte également les fichiers de métadonnées d'autres noeuds du cluster. Il ajoute tous les fichiers de métadonnées à un seul fichier zip puis les présente à l'administrateur. L'administrateur doit décompresser ce fichier et approvisionner chaque fichier sur l'IDP. Par exemple, 8 fichiers de métadonnées pour un cluster à 8 noeuds.

Une seule connexion/accord SAML IdP par fonction de cluster est introduite à partir de la version 11.5. Dans le cadre de cette fonctionnalité, CUCM génère un fichier de métadonnées unique pour le fournisseur de services pour tous les noeuds CUCM et IMP du cluster. Le nouveau format de nom du fichier de métadonnées est **<hostname>-single-agreement.xml**

En gros, un noeud crée les métadonnées et les transmet aux autres noeuds SP du cluster. Cela facilite le provisionnement, la maintenance et la gestion. Par exemple, 1 fichier de métadonnées pour un cluster à 8 noeuds.

Le fichier de métadonnées à l'échelle du cluster utilise un certificat multiserveur tomcat qui garantit que la paire de clés est utilisée de la même manière pour tous les noeuds du cluster. Le fichier de métadonnées contient également une liste d'URL ACS (Assertion Consumer Service) pour chaque noeud du cluster.

CUCM et Cisco IM and Presence version 11.5 prennent en charge les modes SSO, **à l'échelle du cluster** (un fichier de métadonnées par cluster) et par noeud (modèle existant).

Ce document décrit comment configurer le mode à l'échelle du cluster de SAML SSO avec AD FS 2.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configuration

### Étape 1. Exporter les métadonnées SP de CUCM

Ouvrez un navigateur Web, connectez-vous à CUCM en tant qu'administrateur et naviguez **vers System >Single Sign On SAML**.

Par défaut, le bouton radio **Cluster Wide** est sélectionné. Cliquez sur **Exporter toutes les métadonnées**. Fichier de données de métadonnées présenté à l'administrateur sous le nom **<hostname>-single-agreement.xml**

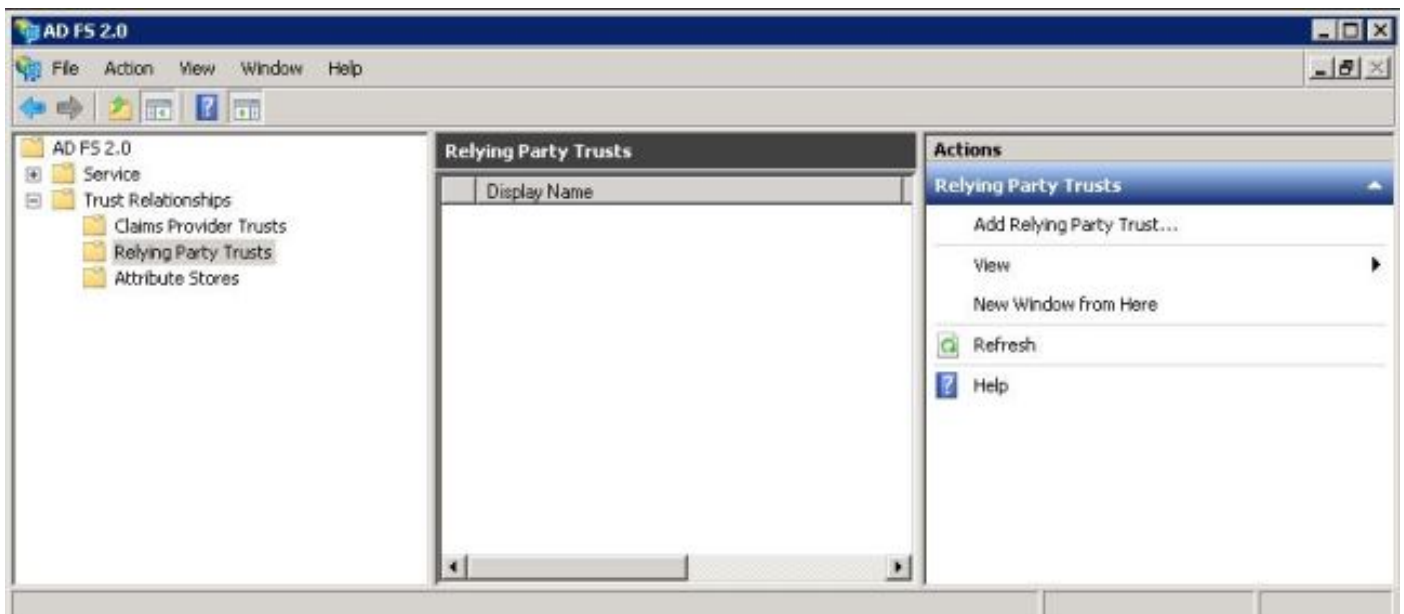


## Étape 2. Télécharger les métadonnées PCI à partir d'AD FS

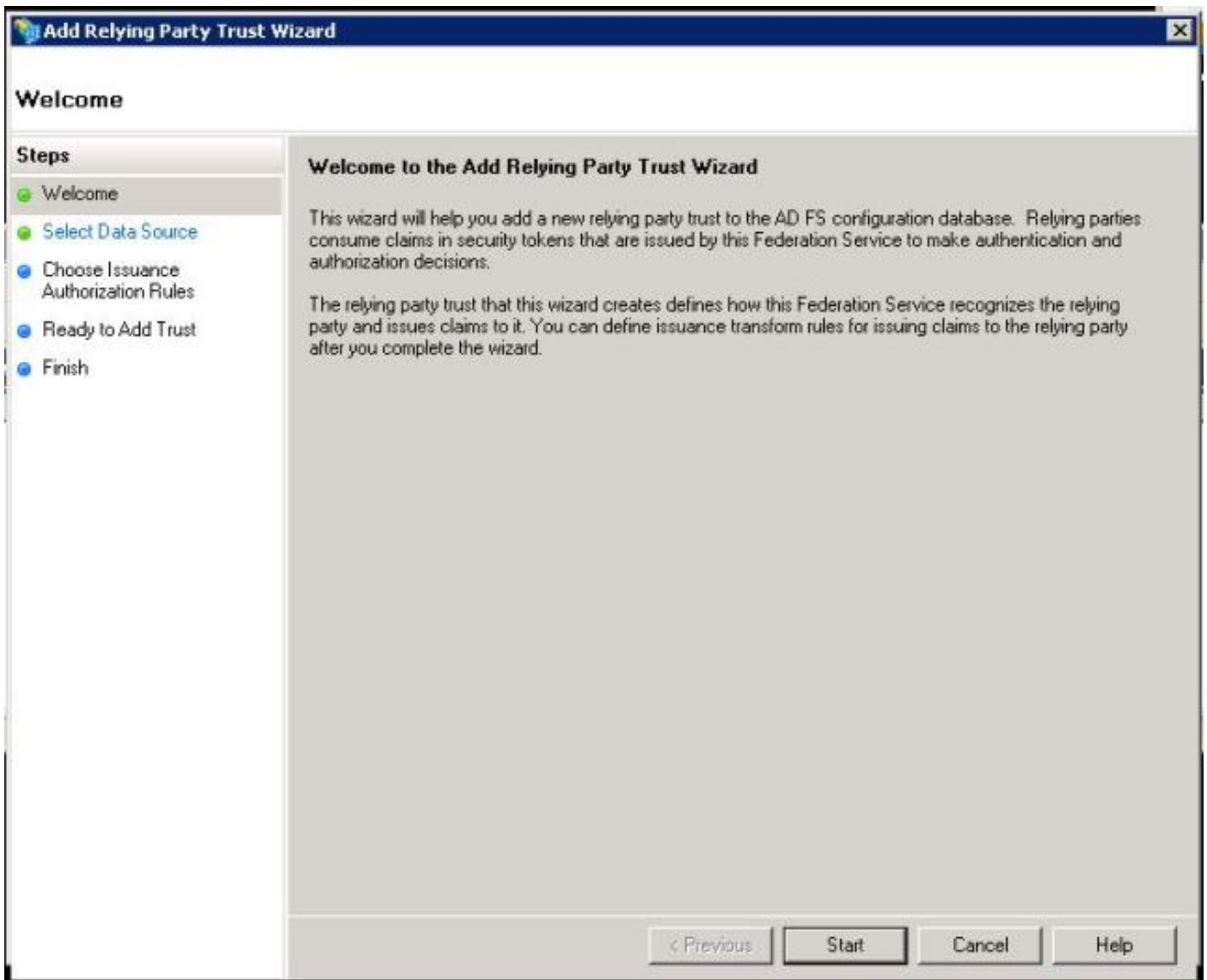
Pour télécharger les métadonnées IdP, consultez le lien [https:// <FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml](https://<FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml)

## Étape 3. IdP de provisionnement

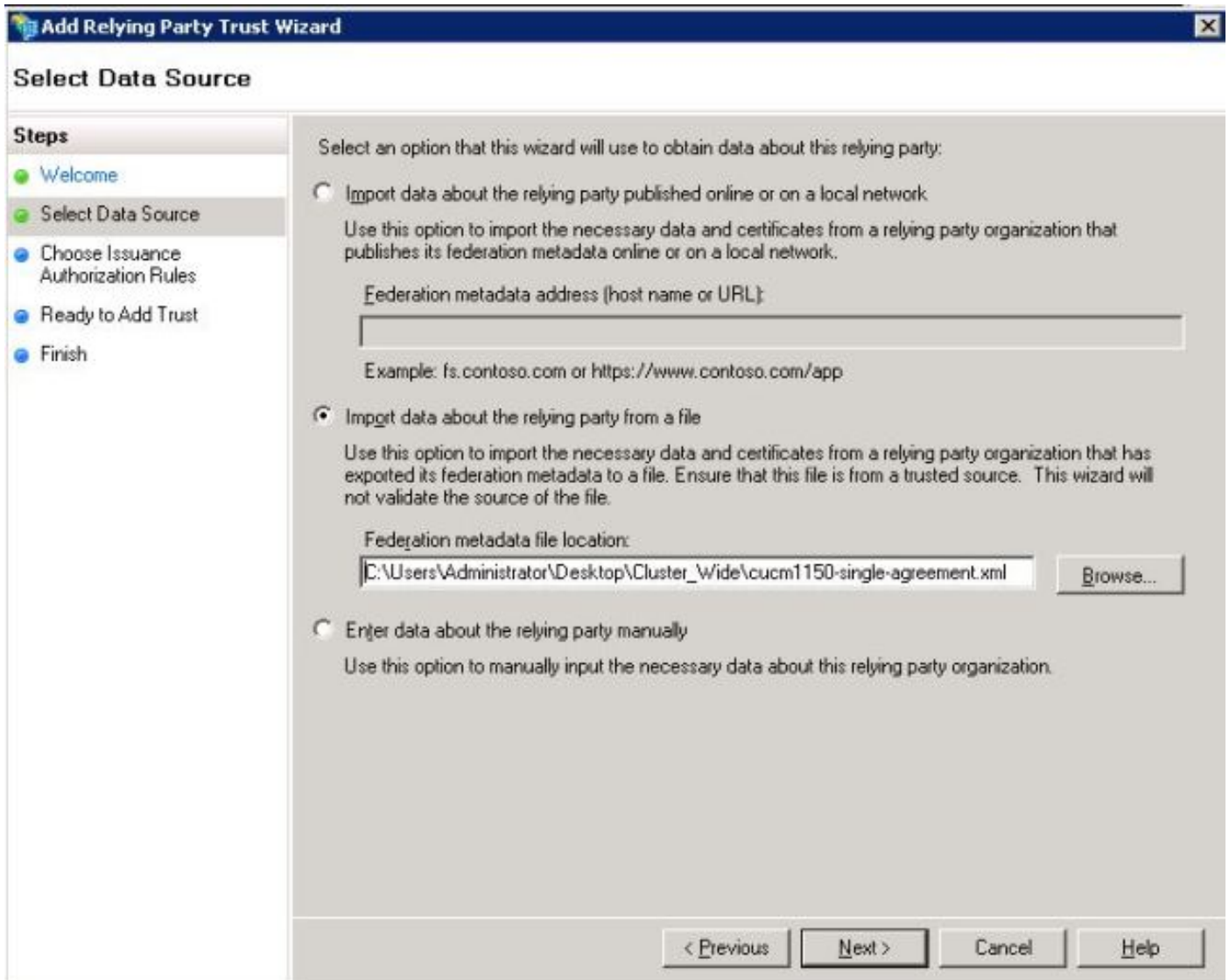
Comme l'illustre l'image, accédez à **Gestion/Approbation des expéditions/Approbation de la partie de confiance AD FS 2.0**. Cliquez sur **Ajouter une approbation de partie de confiance**.



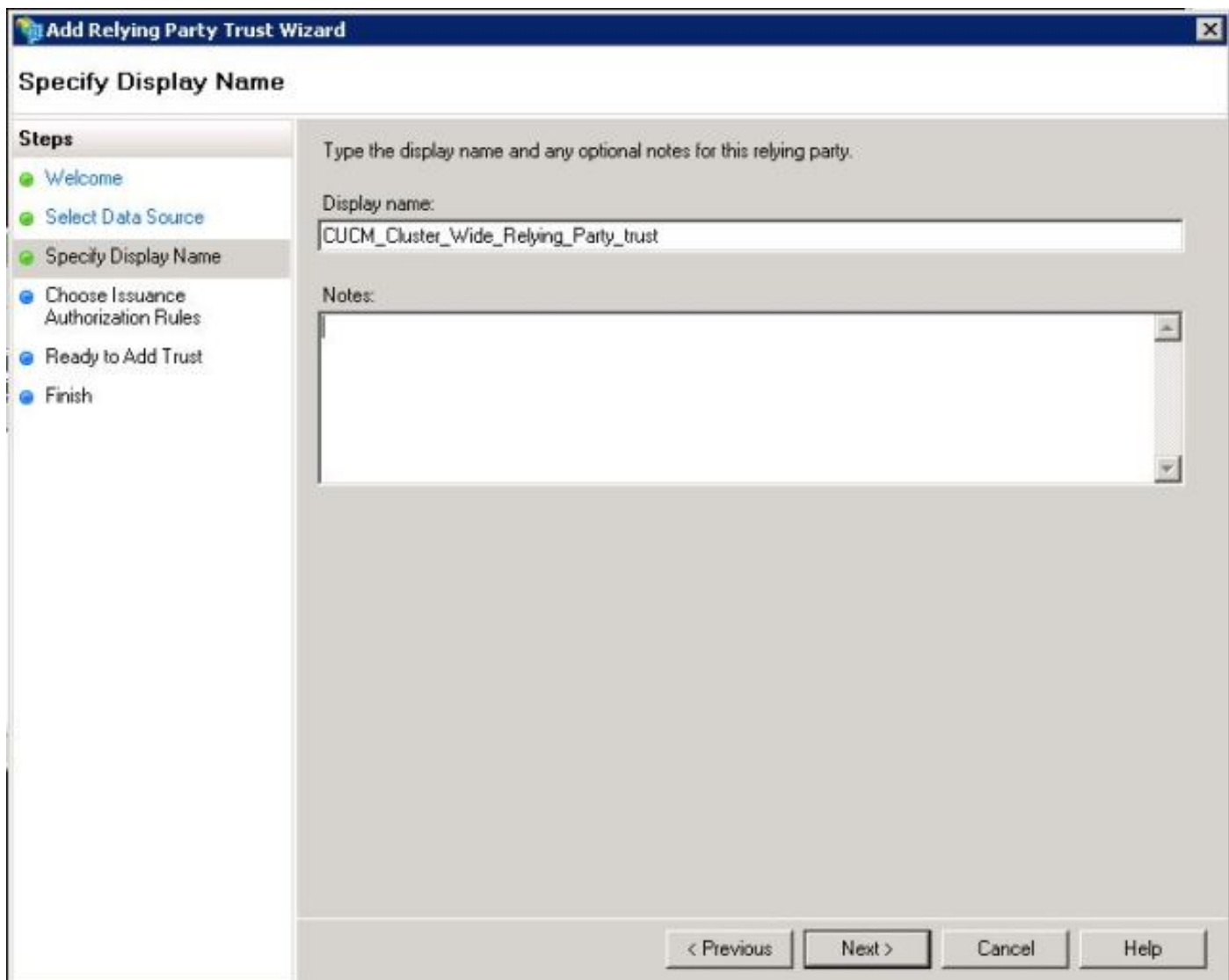
L'Assistant Ajout d'approbation de partie de confiance s'ouvre comme indiqué dans l'image, cliquez maintenant sur **Démarrer**.



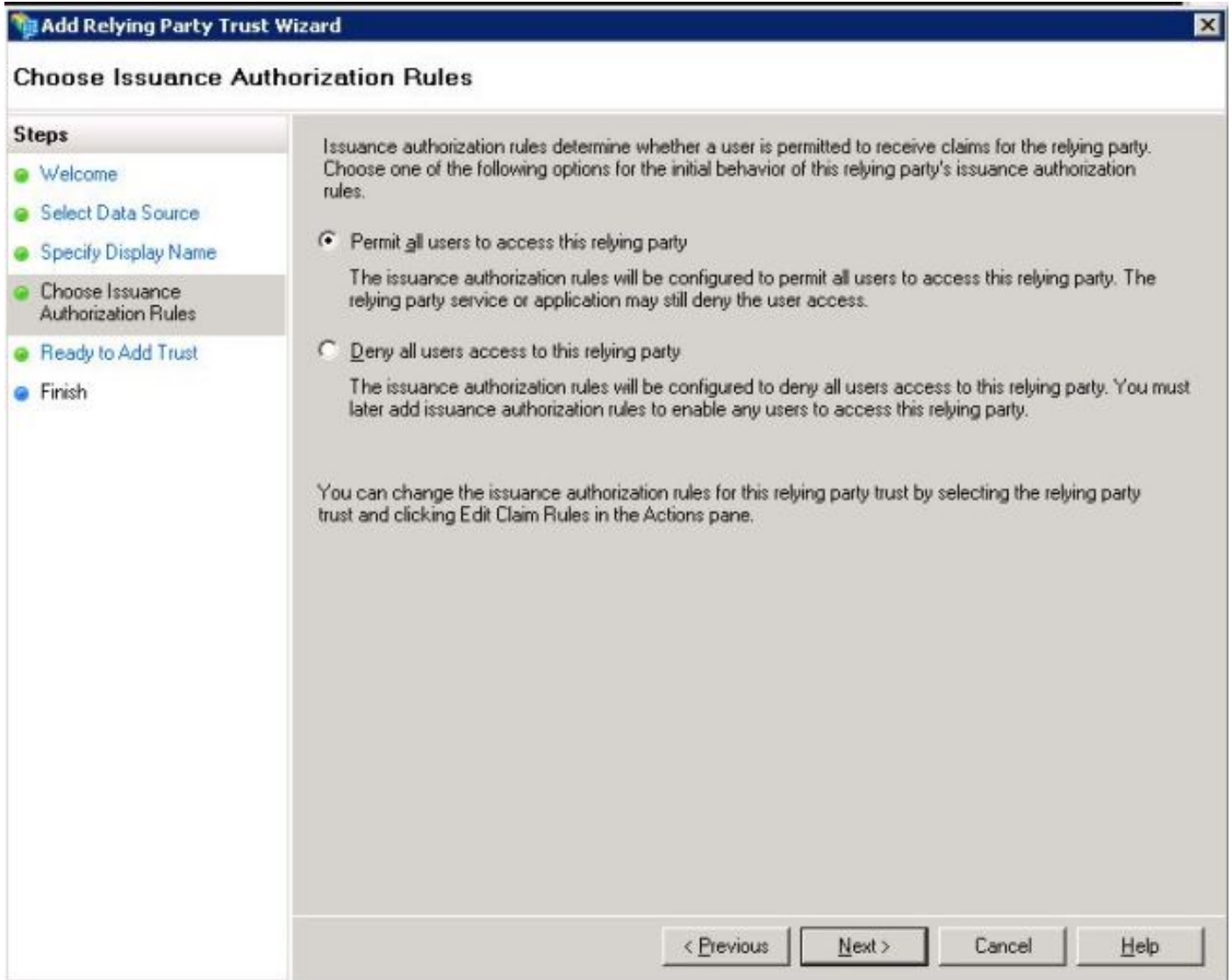
Cliquez sur les données d'importation relatives à la partie de confiance à partir d'un fichier. Parcourez les métadonnées SP téléchargées à partir de la page de configuration de CUCM SAML SSO. Cliquez ensuite sur **Suivant**, comme illustré dans l'image :



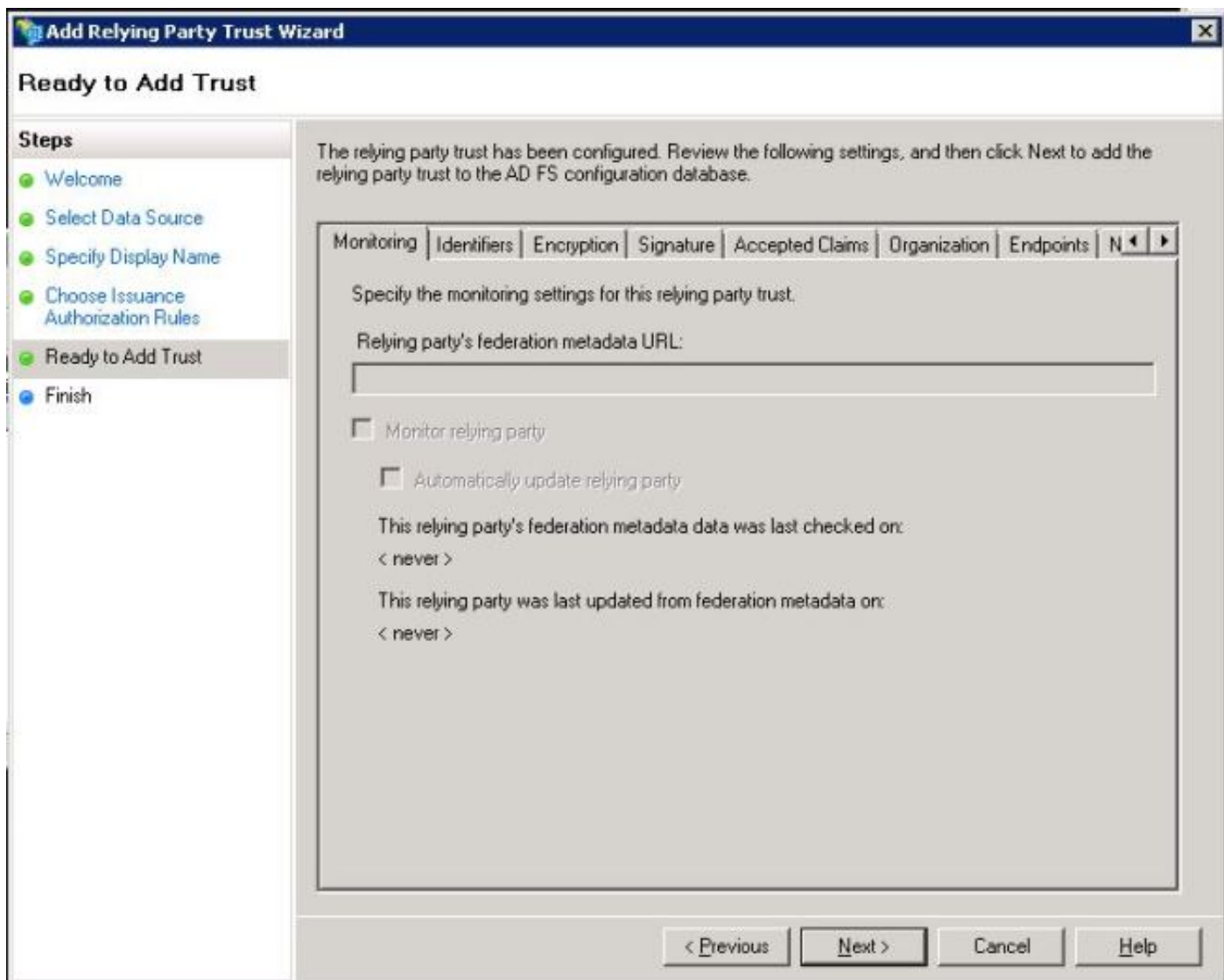
Tapez le nom d'affichage et toutes les notes facultatives pour la partie de confiance. Cliquez sur **Suivant.**, comme illustré dans l'image :



Sélectionnez **Autoriser tous les utilisateurs à accéder à cette partie de confiance** pour autoriser tous les utilisateurs à accéder à cette partie de confiance, puis cliquez sur **Suivant**, comme illustré dans l'image :

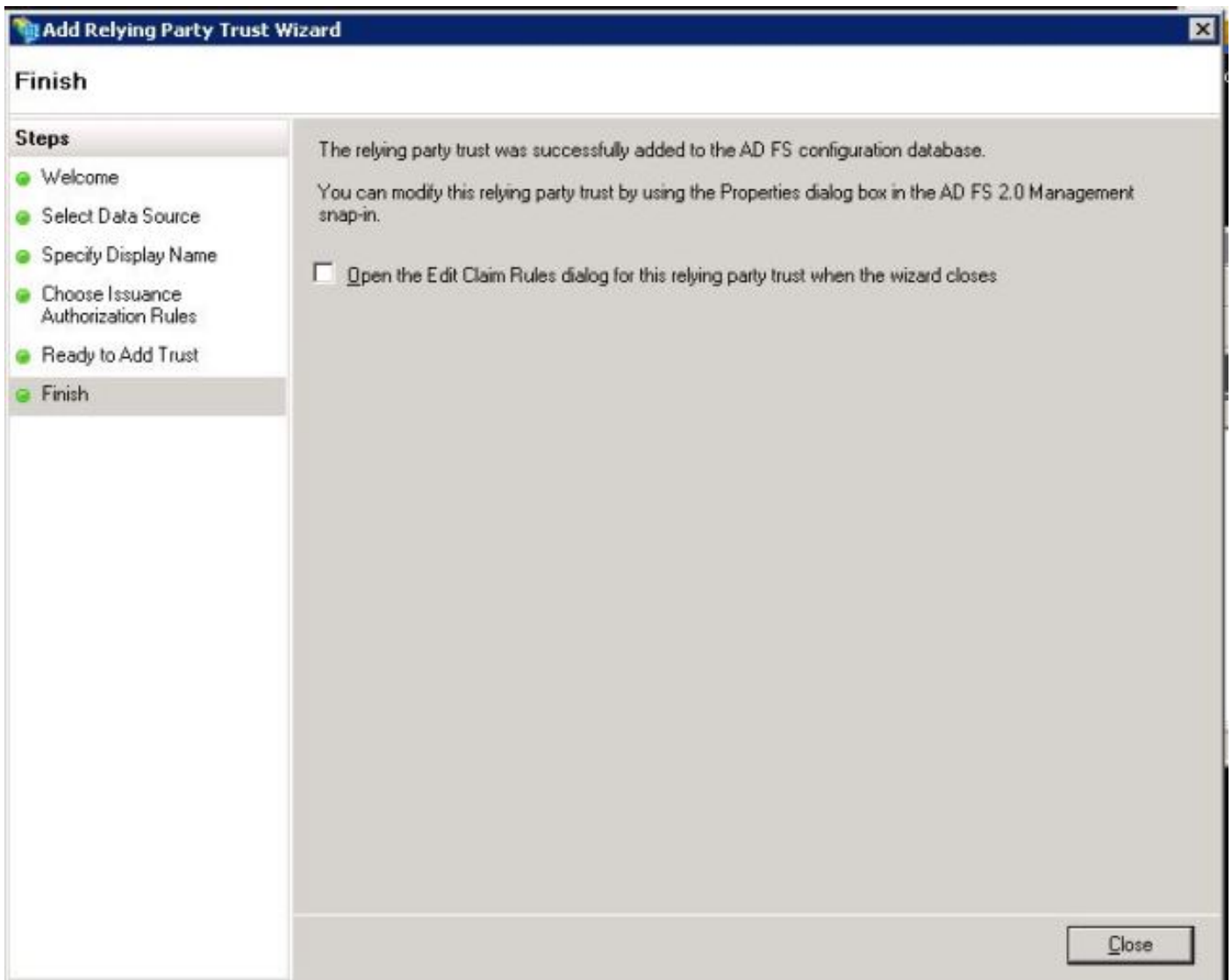


Sous la page **Prêt à ajouter une approbation**, vous pouvez consulter les paramètres de l'approbation de partie de confiance, qui a été configurée. Cliquez maintenant sur **Suivant**, comme illustré dans l'image :

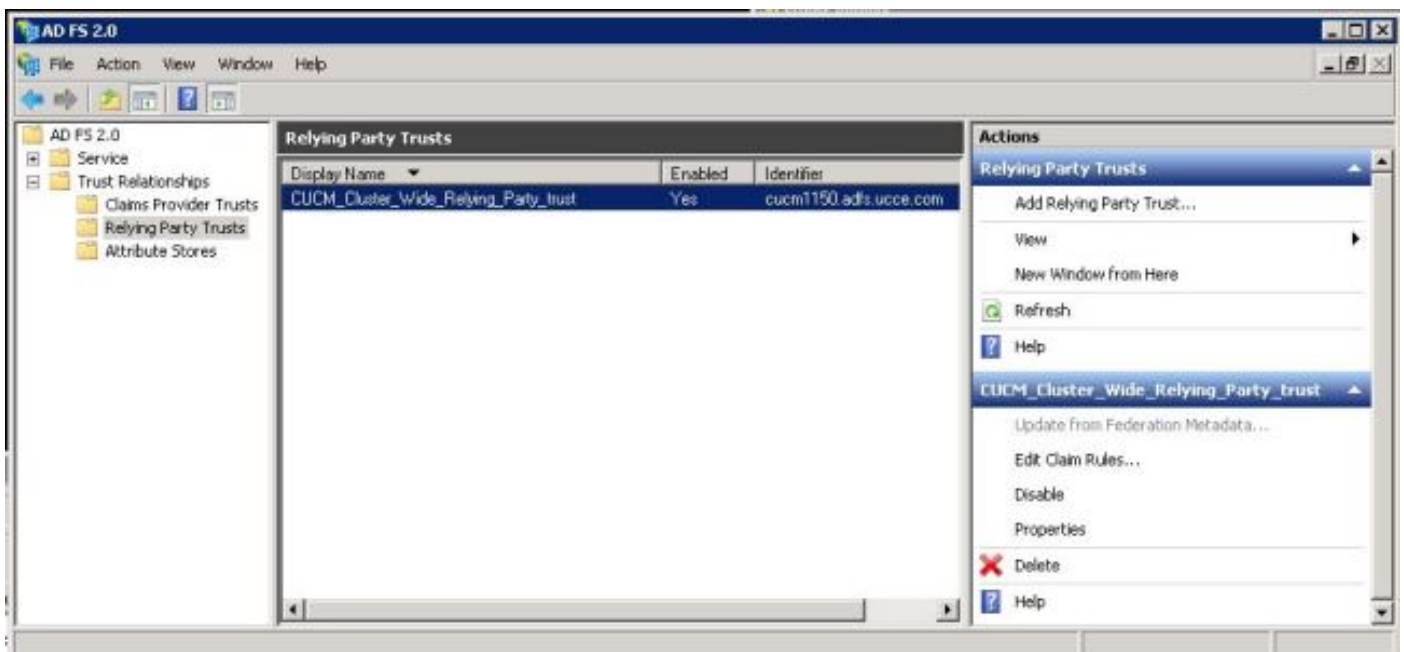


La page Finish confirme que l'approbation de partie de confiance a été ajoutée avec succès à la base de données de configuration AD FS. Décochez la case et cliquez sur **Fermer**, comme illustré dans l'image :

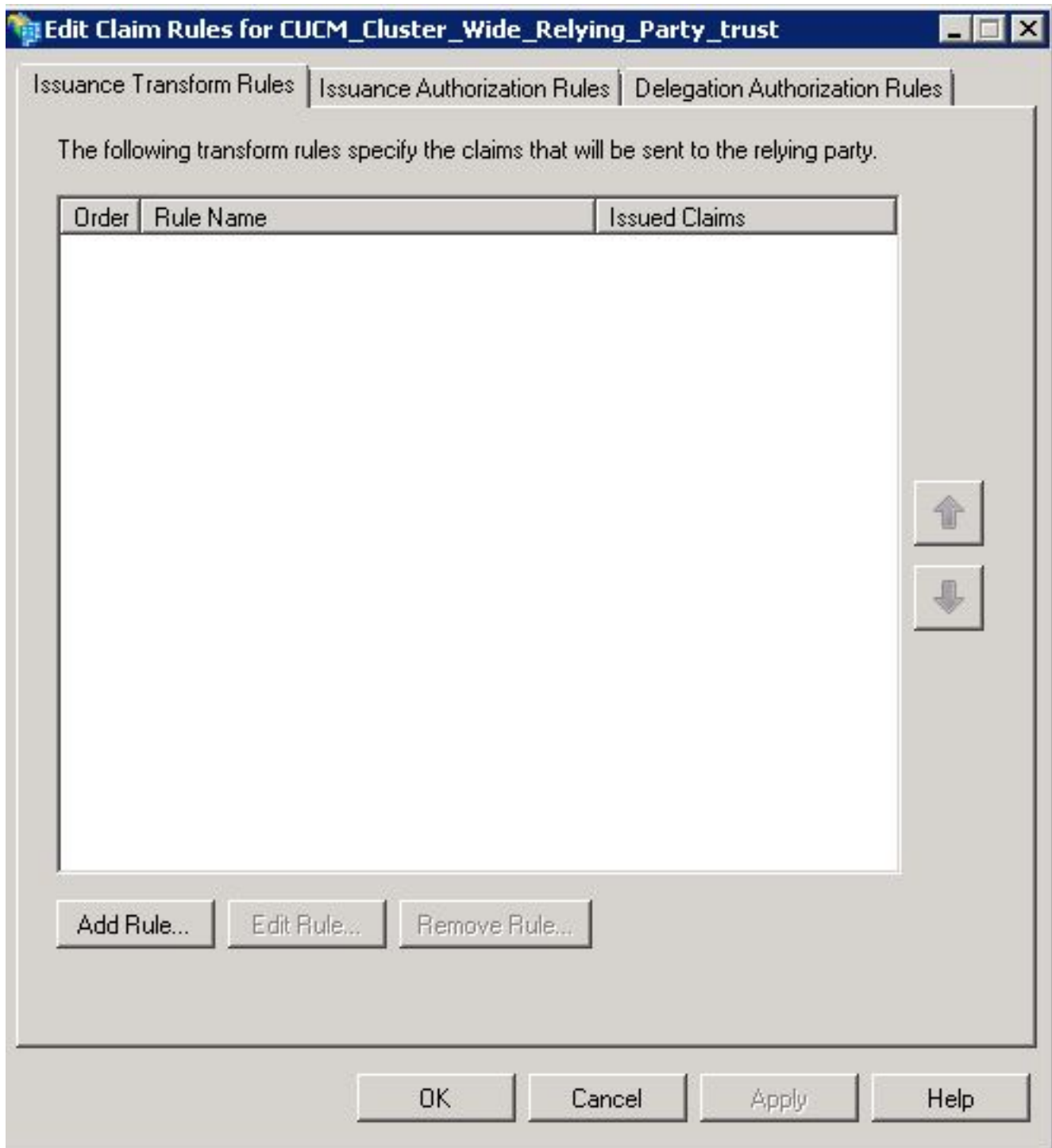




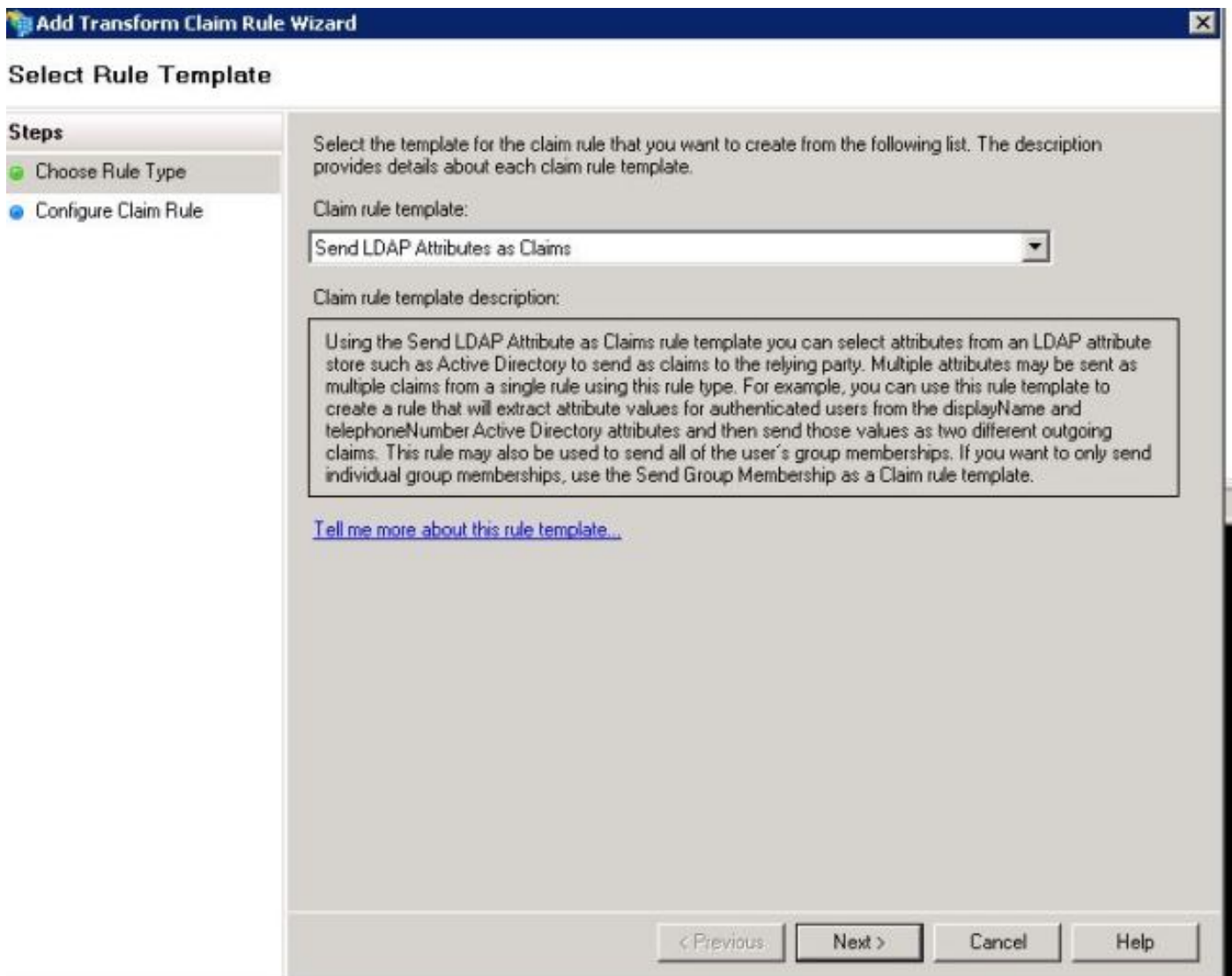
Cliquez avec le bouton droit de la souris sur les **approbations de la partie de confiance** et cliquez sur **Modifier les règles de demande**, comme illustré dans l'image :



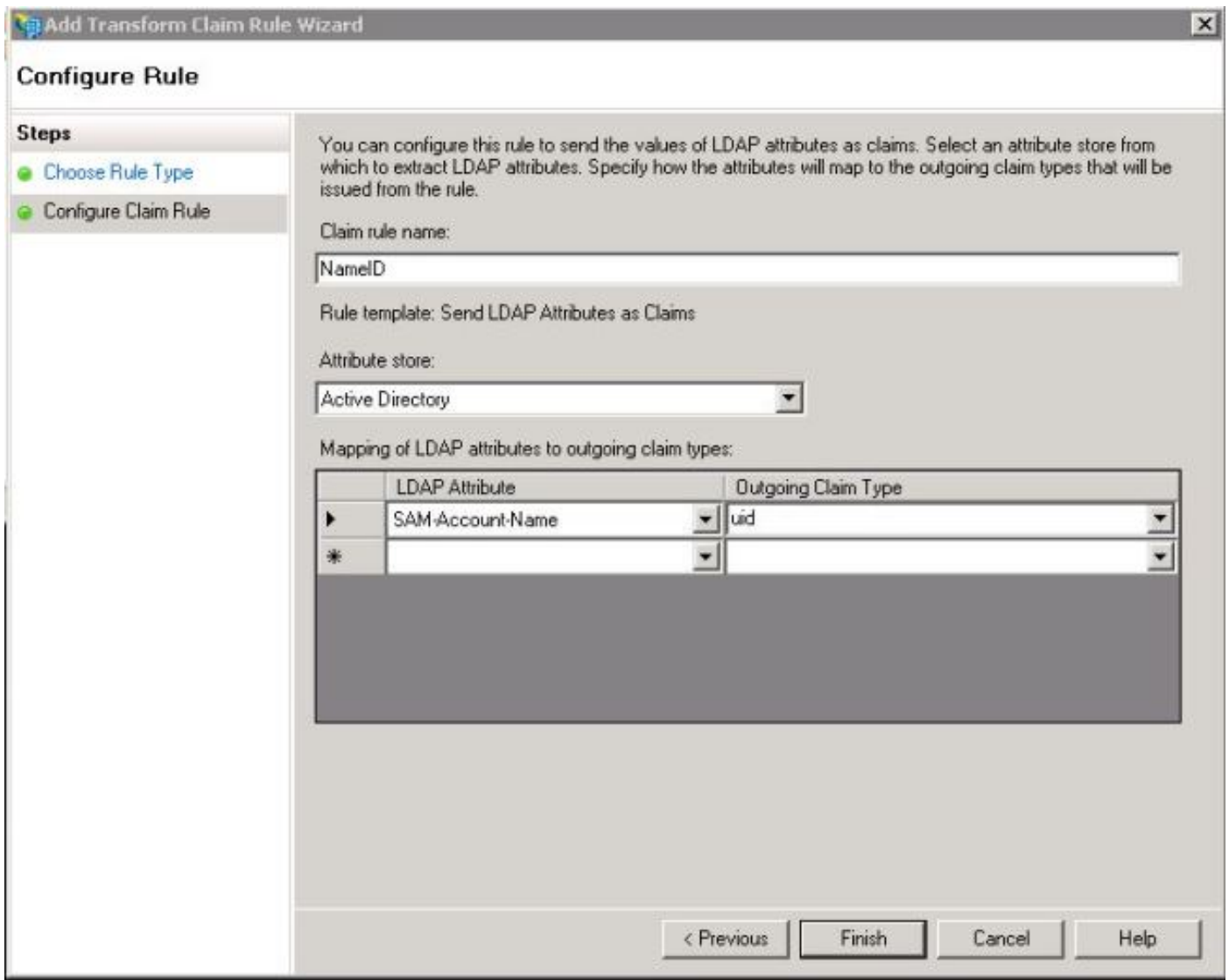
Cliquez maintenant sur **Ajouter une règle**, comme l'illustre l'image :



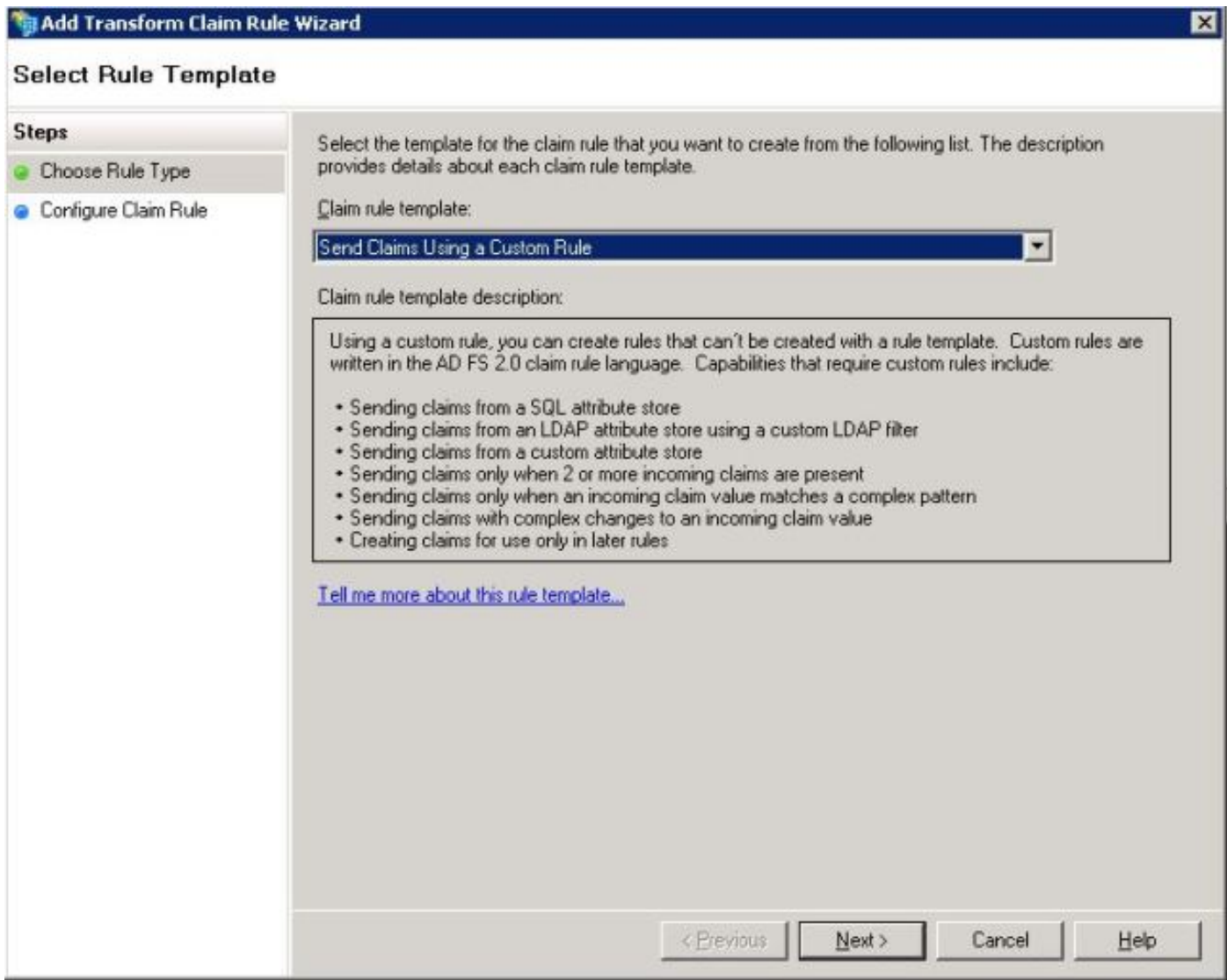
Lorsque la règle **Ajouter une revendication de transformation** s'ouvre, cliquez sur **Suivant** avec le modèle de règle de revendication par défaut **Envoyer les attributs LDAP en tant que revendications**, comme illustré dans l'image :



Cliquez sur **Configurer la règle de revendication** comme indiqué dans cette image. L'attribut LDAP doit correspondre à l'attribut LDAP dans la configuration de l'annuaire LDAP dans CUCM. Gérer le type de revendication sortante comme **uid**. Cliquez sur **Terminer**, comme l'illustre l'image :



Ajoutez la règle personnalisée pour la partie de confiance. Cliquez sur **Ajouter une règle**. Sélectionnez **Envoyer des revendications à l'aide d'une règle personnalisée** puis cliquez sur **Suivant**, comme illustré dans l'image :

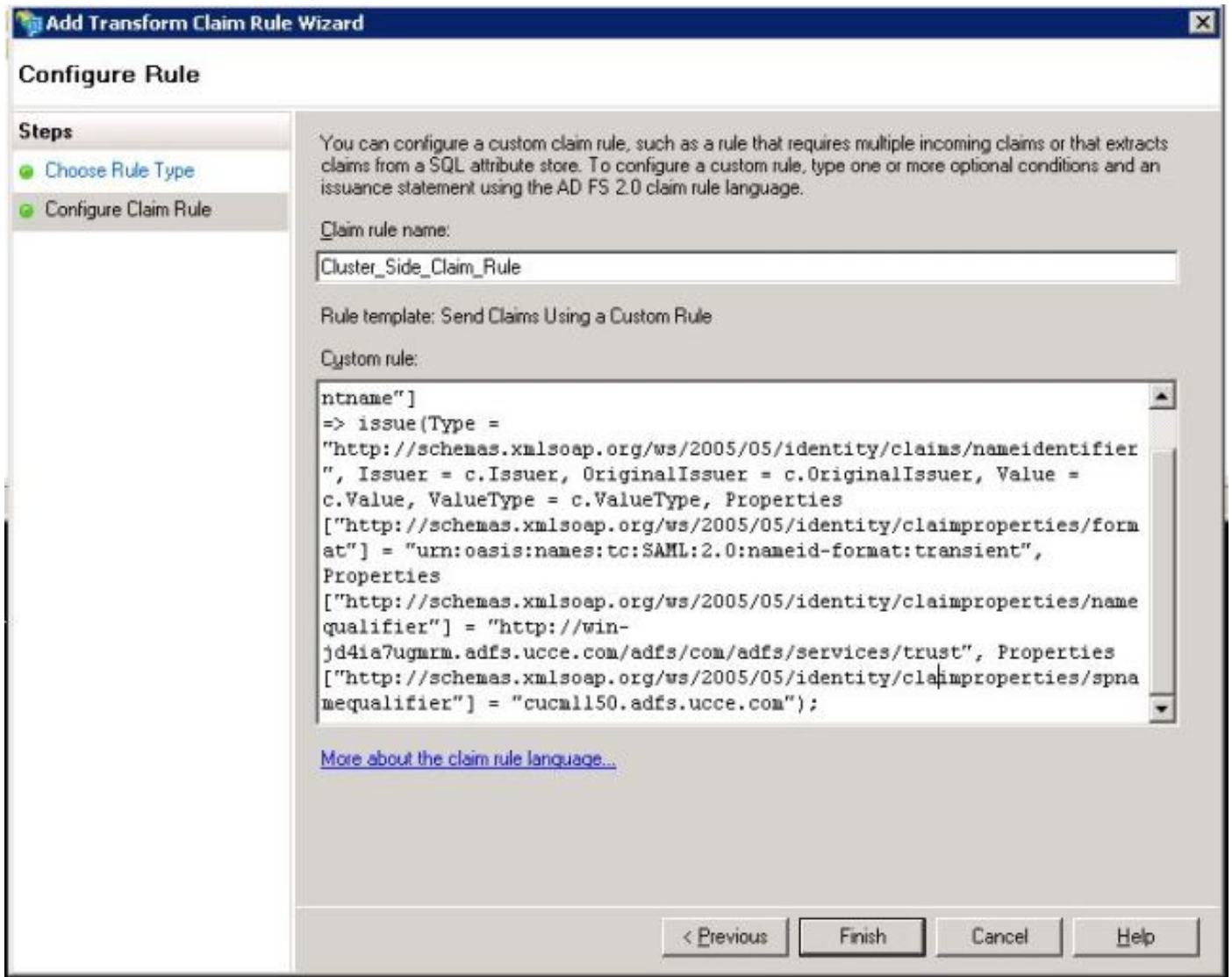


Dans Configurer la règle de revendication, tapez un nom de règle de revendication, puis Copiez la règle de revendication donnée et passée dans le champ Règle personnalisée de l'Assistant modifiant l'égaliseur de noms et le qualificateur de nom dans la règle de revendication. Cliquez sur **Terminer.**, comme l'illustre l'image :

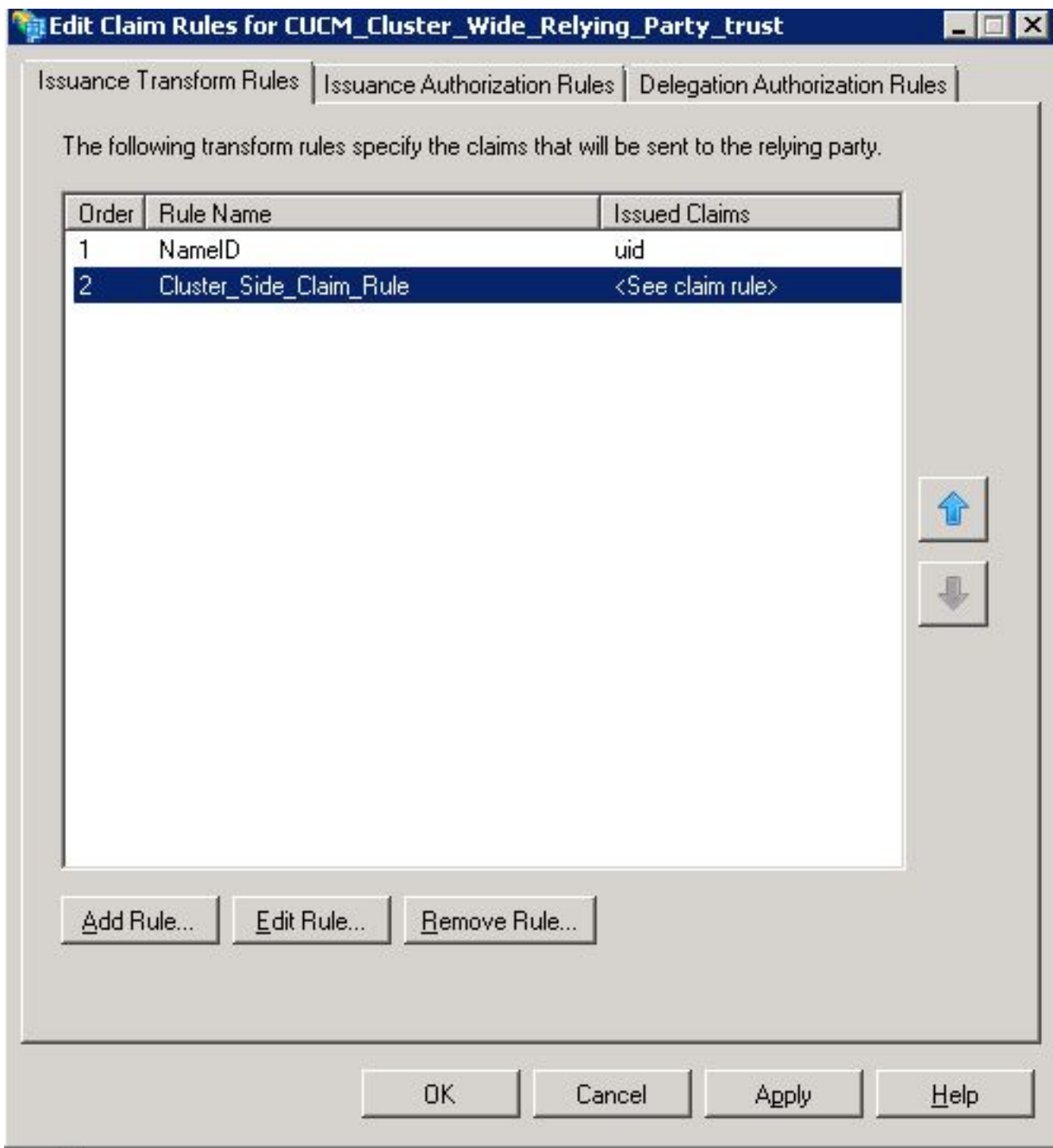
### Règle de revendication :

```
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://<FQDN of ADFS>/adfs/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"<Entity ID in the SP Metadata>");
```

Entity ID = Open the SP metadata and check the Entity ID. Basically, its the CUCM Publisher's FQDN.



Comme le montre l'image, cliquez sur **Apply**, puis sur **OK**.



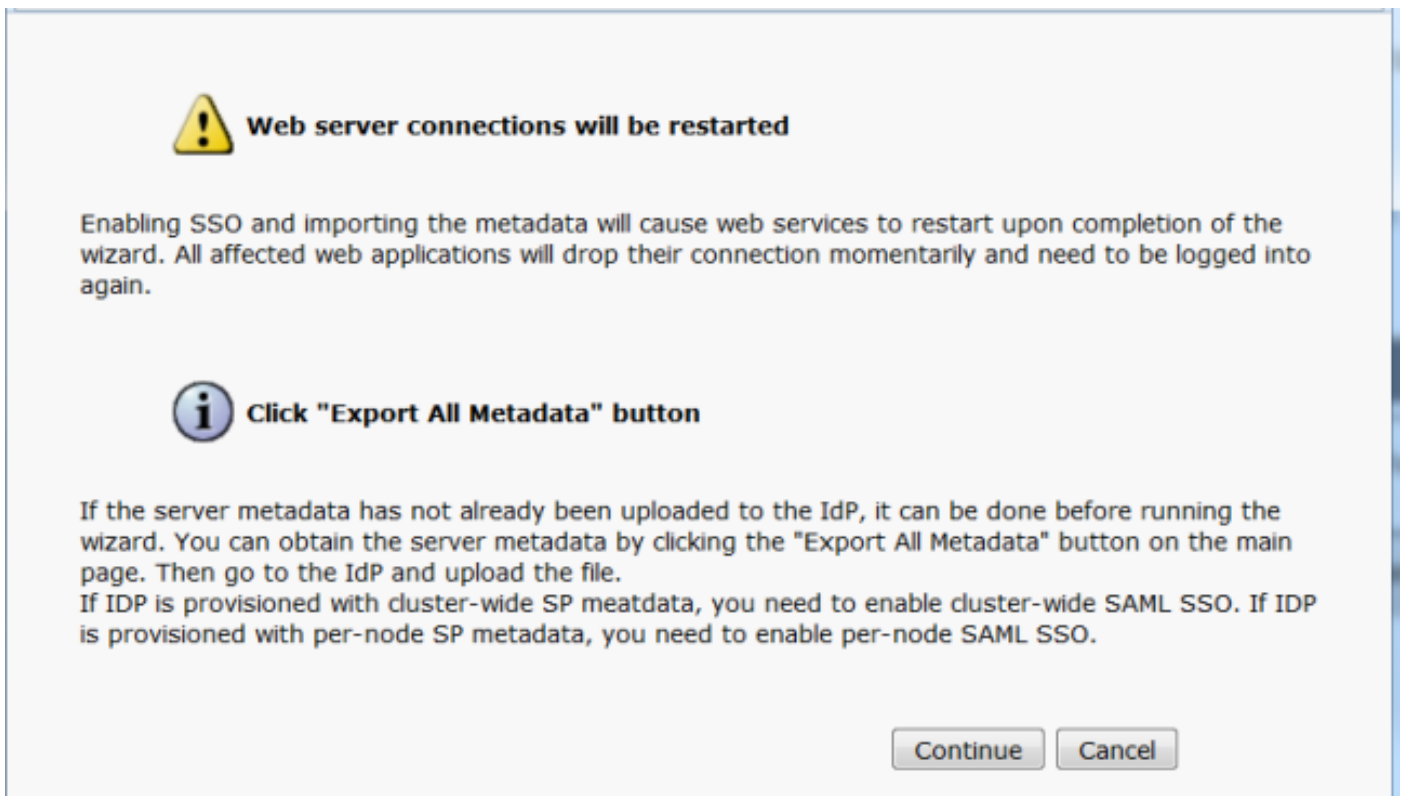
#### Étape 4. Activer SAML SSO

Ouvrez un navigateur Web, connectez-vous à CUCM en tant qu'administrateur et naviguez vers **System >Single Sign On SAML**.

Par défaut, le bouton radio **Cluster Wide** est sélectionné. Cliquez sur **Enable Saml SSO**, comme illustré dans l'image :

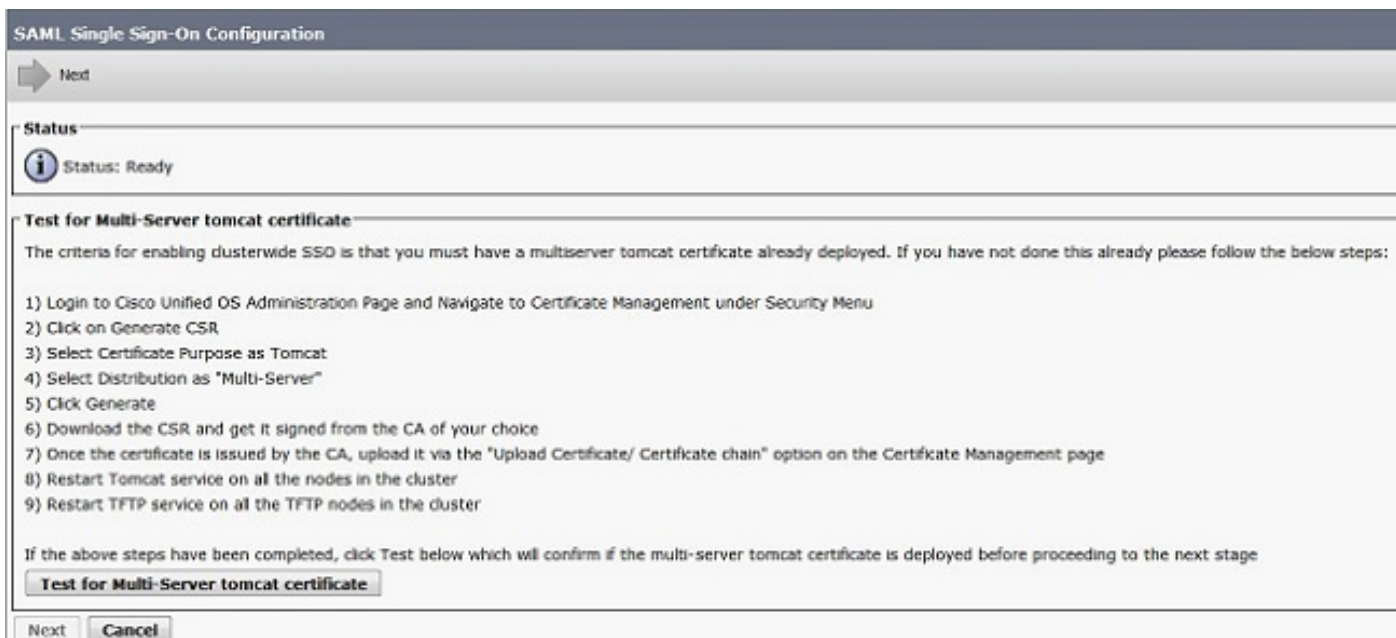


Comme l'illustre l'image, la fenêtre contextuelle avertit l'avertissement de redémarrage du serveur Web et les informations permettant de choisir l'SSO SAML ou SSO SAML par noeud à l'échelle du cluster, conformément à idp. Cliquez sur **Continue**.

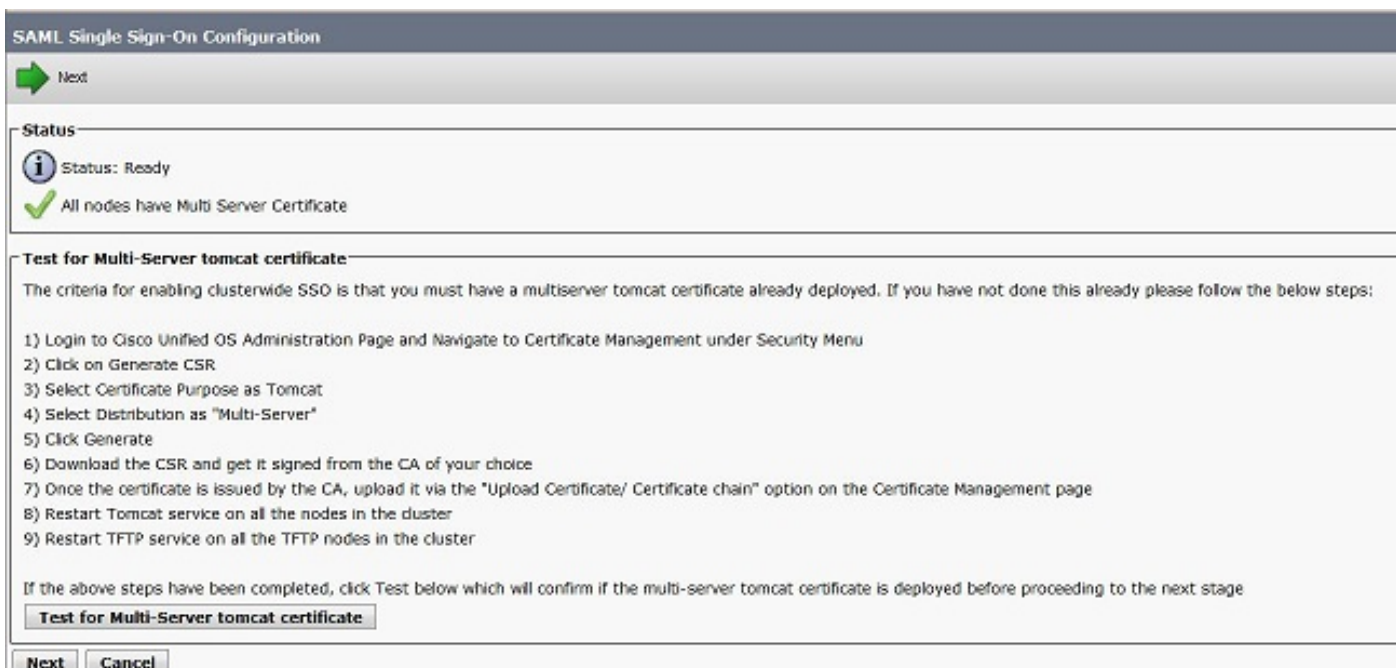


Le critère d'activation de l'authentification unique à l'échelle du cluster est que vous devez disposer d'un certificat tomcat multiserveur déjà déployé. Cliquez sur **Test for Multi-Server Tomcat Certificate**, comme illustré dans l'image :

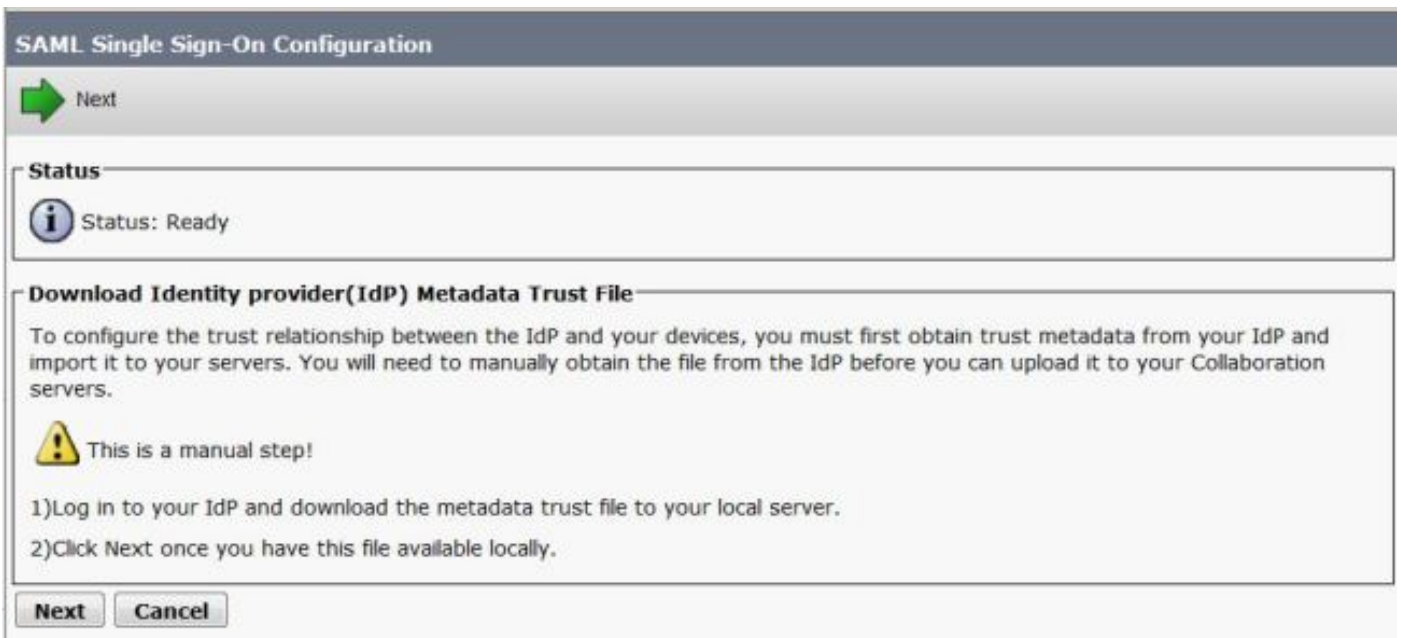




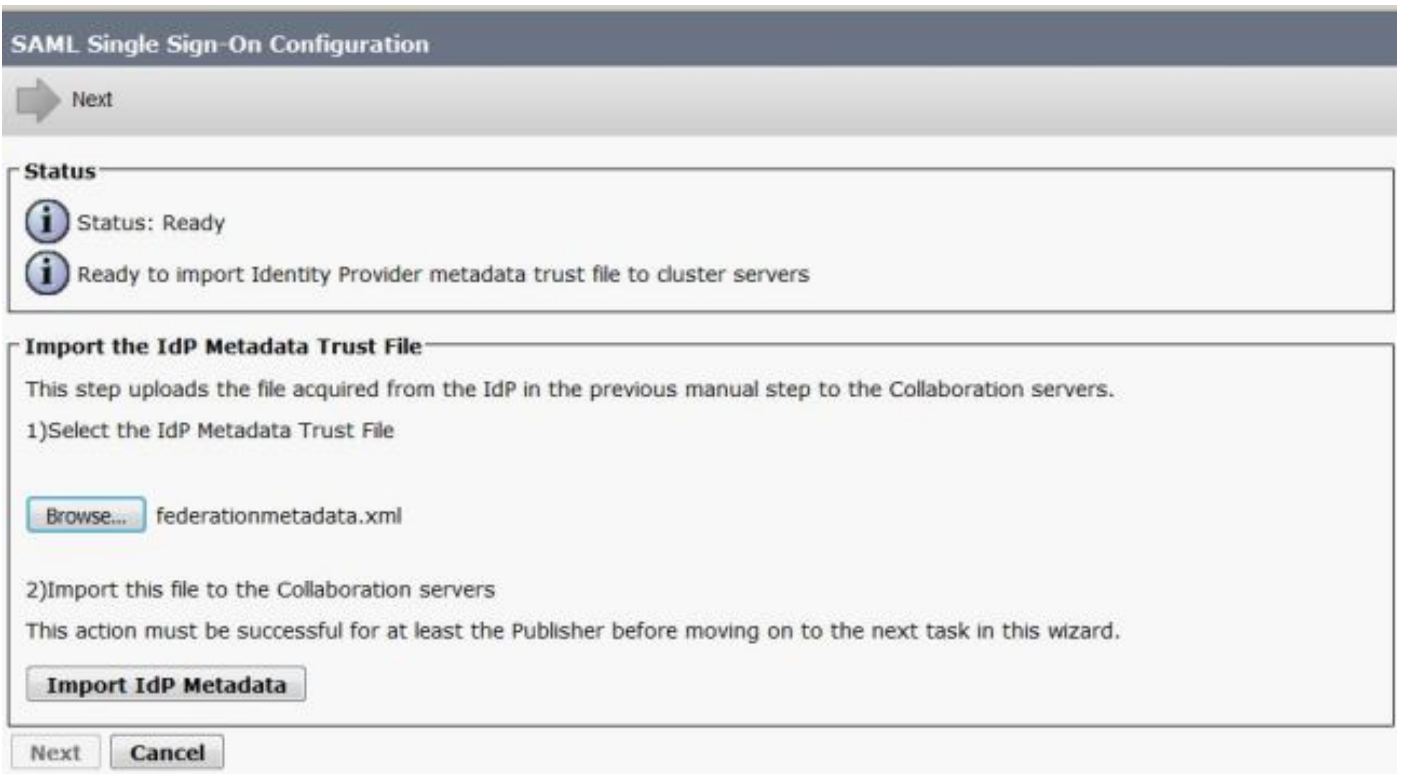
Une fois la confirmation obtenue, tous les noeuds ont un certificat multi-serveur affiche un **certificat multi-serveur pour tous les noeuds**, puis cliquez sur **Suivant**, comme illustré dans l'image :



Comme le montre l'image, cliquez sur **Suivant**.



Parcourez et sélectionnez les métadonnées IdP téléchargées. Cliquez sur **Importer les métadonnées IdP**, comme indiqué dans l'image :



La page confirme que l'importation a réussi pour tous les serveurs, puis cliquez sur **Suivant**, comme illustré dans l'image :

**SAML Single Sign-On Configuration**

Next

**Status**

- Status: Ready
- Import succeeded for all servers

**Import the IdP Metadata Trust File**

This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.

1) Select the IdP Metadata Trust File

Browse... No file selected.

2) Import this file to the Collaboration servers

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

Import IdP Metadata

Import succeeded for all servers

Next Cancel

Comme l'illustre l'image, cliquez sur **Suivant**, car les métadonnées SP ont déjà été exportées à partir de la page de configuration initiale SAML SSO.

**SAML Single Sign-On Configuration**

Back Next

**Status**

- Status: Ready
- If Admin has already uploaded the server metadata to IdP then skip the steps below and click Next. Otherwise follow the steps below to upload the server metadata to IdP
- IdP Metadata has been imported to servers in this cluster

**Download Server Metadata and install on the IdP**

Download the metadata trust file from Collaboration servers and manually install it on the IdP server to complete SSO setup.

1) Download the server metadata trust files to local storage

Download Trust Metadata File

⚠ This is a manual step!


2) Log in to your IdP and upload the server metadata trust file.

3) Click Next once you have installed the server metadata on the IdP.


Back Next Cancel

CUCM doit être synchronisé avec l'annuaire LDAP. L'Assistant affiche les utilisateurs administrateur valides configurés dans l'annuaire LDAP. Sélectionnez l'utilisateur et cliquez sur **Exécuter le test SSO**, comme illustré dans l'image :

### 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 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

samluser

2) Launch SSO test page

Comme l'illustre l'image, entrez l'ID utilisateur et le mot de passe respectifs une fois qu'il l'invite.

### Authentication Required

 Enter username and password for <https://win-jd4ia7ugmrm.adfs.ucce.com>

User Name:

Password:


La fenêtre contextuelle, comme le montre l'image, confirme que le test est réussi.

# 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

Comme l'illustre l'image, cliquez sur **Terminer** afin de terminer la configuration pour activer SSO.



System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administra

### SAML Single Sign-On Configuration

← Back → Finish

**Status**

✓ SSO Metadata Test Successful

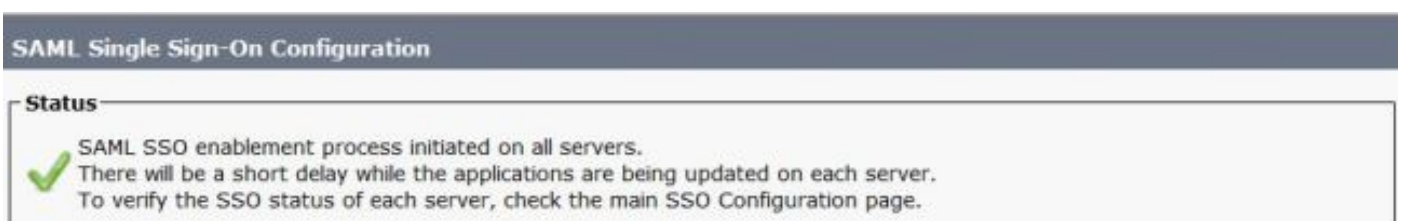
**Ready to Enable SSO**

Clicking "Finish" will complete enabling SSO on all the servers in this cluster. There will be a short delay while the applications are being updated.

To verify the SSO status of each server, check the main SSO Configuration page.  
Additional testing and manual uploads may be performed from the main page if necessary.

Back Finish Cancel

La page illustrée dans l'image confirme que le processus d'activation SAML SSO est lancé sur tous les serveurs.



### SAML Single Sign-On Configuration

**Status**

✓ SAML SSO enablement process initiated on all servers.  
There will be a short delay while the applications are being updated on each server.  
To verify the SSO status of each server, check the main SSO Configuration page.

Déconnectez-vous et reconnectez-vous à CUCM à l'aide des informations d'identification SAML SSO. Accédez à **System >SAML Single Sign On**. Cliquez sur **Exécuter le test SSO** pour les autres noeuds du cluster, comme illustré dans l'image :

**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)

Disable SAML SSO Export All Metadata Update IdP Metadata File Fix All Disabled Servers

**Status**

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

SAML SSO enabled

SAML Single Sign-On (1 - 3 of 3)							Rows per Page 50
Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test	
cucom1150.adfs.uccoe.com	SAML	N/A	June 21, 2016 9:28:39 PM IST	File	June 21, 2016 7:46:56 PM IST	Passed - June 21, 2016 9:29:14 PM IST	
cucom1150sub.adfs.uccoe.com	SAML	IdP	June 21, 2016 9:28:39 PM IST	File	June 21, 2016 7:46:56 PM IST	Never	
imp115.adfs.uccoe.com	SAML	IdP	June 21, 2016 9:28:39 PM IST	File	June 21, 2016 7:46:56 PM IST	Never	

## Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Confirmez que le test SSO a réussi pour les noeuds qui sont activés SSO SAML. Accédez à **System >SAML Single Sign On**. Les tests SSO réussis indiquent l'état Passé.

**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)

Disable SAML SSO Export All Metadata Update IdP Metadata File Fix All Disabled Servers

**Status**

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

SAML SSO enabled

SAML Single Sign-On (1 - 3 of 3)							Rows per Page 50
Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test	
cucom1150.adfs.uccoe.com	SAML	N/A	June 20, 2016 9:57:30 AM IST	File	June 20, 2016 10:06:27 PM IST	Passed - June 20, 2016 9:59:02 PM IST	
cucom1150sub.adfs.uccoe.com	SAML	IdP	June 20, 2016 10:15:46 PM IST	File	June 20, 2016 10:06:26 PM IST	Passed - June 20, 2016 10:11:39 PM IST	
imp115.adfs.uccoe.com	SAML	IdP	June 20, 2016 10:15:46 PM IST	File	June 20, 2016 10:06:26 PM IST	Passed - June 20, 2016 10:12:40 PM IST	

Disable SAML SSO Export All Metadata Update IdP Metadata File Fix All Disabled Servers

Une fois l'OSS SAML activé, les applications installées et les applications de plate-forme sont répertoriées pour la page de connexion CUCM, comme illustré dans cette image.

## Installed Applications

- Cisco Unified Communications Manager
  - Recovery URL to bypass Single Sign On (SSO)
- Cisco Unified Communications Self Care Portal
- Cisco Prime License Manager
- Cisco Unified Reporting
- Cisco Unified Serviceability

## Platform Applications

- Disaster Recovery System
- Cisco Unified Communications OS Administration

Une fois le SSO SAML activé, les applications installées et les applications de plate-forme sont répertoriées pour la page de connexion IM and Presence, comme illustré sur cette image :

## Installed Applications

- Cisco Unified Communications Manager IM and Presence
  - Recovery URL to bypass Single Sign On (SSO)
- Cisco Unified Reporting
- Cisco Unified Serviceability

## Platform Applications

- Disaster Recovery System
- Cisco Unified Communications OS Administration

# Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Afin de définir les journaux SSO sur debug, utilisez la commande **set samltrace level DEBUG**

Collectez les journaux SSO à l'aide de RTMT ou à partir de l'emplacement **active.log** **/tomcat/logs/ssosp/log4j/\*.log** à l'aide de l'interface de ligne de commande.

Exemple pour les journaux SSO montre les métadonnées générées et envoyées à d'autres noeuds

```
2016-05-28 14:59:34,026 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Call GET
API to generate Clusterwide SP Metadata in the Local node.
2016-05-28 14:59:47,184 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Call to
post the generated SP Metadata to other nodes
2016-05-28 14:59:47,185 INFO [http-bio-443-exec-297] cluster.SAMLSSOClusterManager -
Begin:postClusterWideSPMetadata
2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Nodes
[cucm1150, cucm1150sub.adfs.ucce.com]
2016-05-28 14:59:47,186 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post
ClusterWideSPMetadata to the cucm1150
2016-05-28 14:59:47,187 DEBUG [http-bio-443-exec-297] cluster.SAMLSSOClusterManager - Post
ClusterWideSPMetadata to the cucm1150sub.adfs.ucce.com
```