Configuración de una Conexión/Acuerdo IDP de SAML por Clúster con AD FS versión 2.0

Contenido

Introducción

Este documento describe cómo configurar la conexión/acuerdo por clúster del proveedor de identidad (IdP) del Lenguaje de marcado de aserción de seguridad única (SAML) con el Servicio de federación de directorios activos (AD FS).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Communications Manager (CUCM) 11.5 o posterior
- Cisco Unified Communications Manager IM and Presence versión 11.5 o posterior
- Servicio de federación de Active Directory versión 2.0

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Servicio de federación de Active Directory versión 2.0 como IdP
- Cisco Unified Communications Manager versión 11.5
- Cisco IM and Presence Server versión 11.5

Antecedentes

Para SAML SSO, debe ser un círculo de confianza entre el proveedor de servicios (SP) y el IdP. Esta confianza se crea como parte de Habilitación de SSO, cuando se intercambia confianza (metadatos). Descargue los metadatos de CUCM y los carga en IdP, descargue los metadatos de IdP y cárguelos en CUCM.

Antes de CUCM 11.5, el nodo de origen genera el archivo de metadatos, y también recopila los archivos de metadatos de otros nodos del clúster. Agrega todos los archivos de metadatos a un único archivo zip y luego se presenta al administrador. El administrador debe descomprimir este archivo y aprovisionar cada archivo en el IdP. Por ejemplo, 8 archivos de metadatos para un clúster de 8 nodos.

La única función SAML IdP de conexión/acuerdo por clúster se introduce a partir de 11.5. Como parte de esta función, CUCM genera un único archivo de metadatos del proveedor de servicios para todos los nodos CUCM e IMP del clúster. El nuevo formato de nombre para el archivo de metadatos es **<hostname>-single-agreement.xml**

Básicamente, un nodo crea los metadatos y los envía a otros nodos SP del clúster. Esto facilita el aprovisionamiento, el mantenimiento y la gestión. Por ejemplo, 1 archivos de metadatos para un clúster de 8 nodos.

El archivo de metadatos de todo el clúster utiliza el certificado de tomcat de servidor múltiple que garantiza que el par de claves se utiliza es el mismo para todos los nodos del clúster. El archivo de metadatos también tiene una lista de URL del Servicio de consumidor de afirmación (ACS) para cada nodo del clúster.

CUCM y Cisco IM and Presence versión 11.5 Admite los modos SSO, en todo el **clúster** (un archivo de metadatos por clúster) y por nodo (modelo existente).

Este documento describe cómo configurar el modo de clúster de SAML SSO con AD FS 2.0.

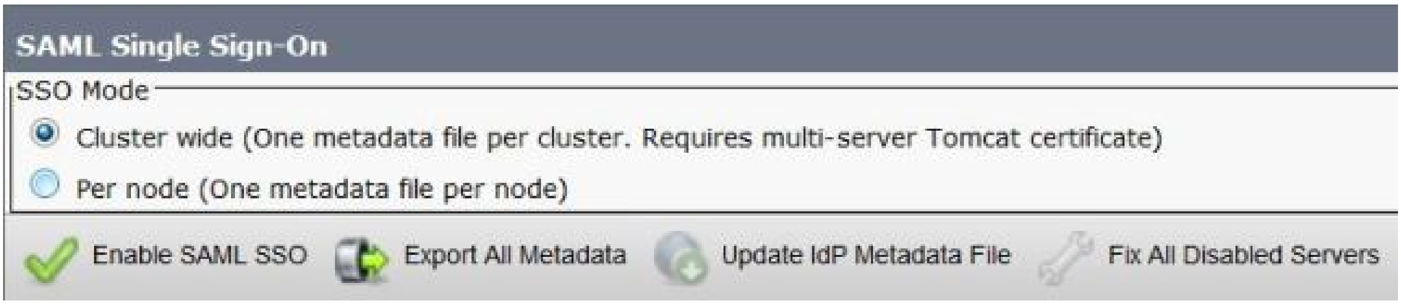
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Paso 1. Exportar metadatos SP de CUCM

Abra un navegador web, inicie sesión en CUCM como administrador y navegue **a System >SAML Single Sign On.**

De forma predeterminada, se selecciona el botón de opción **Clúster Wide**. Haga clic en **Exportar todos los metadatos.** El archivo de datos de metadatos presentado al administrador con el nombre **<hostname>-single-agreement.xml**



SAML Single Sign-On

SSO Mode

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

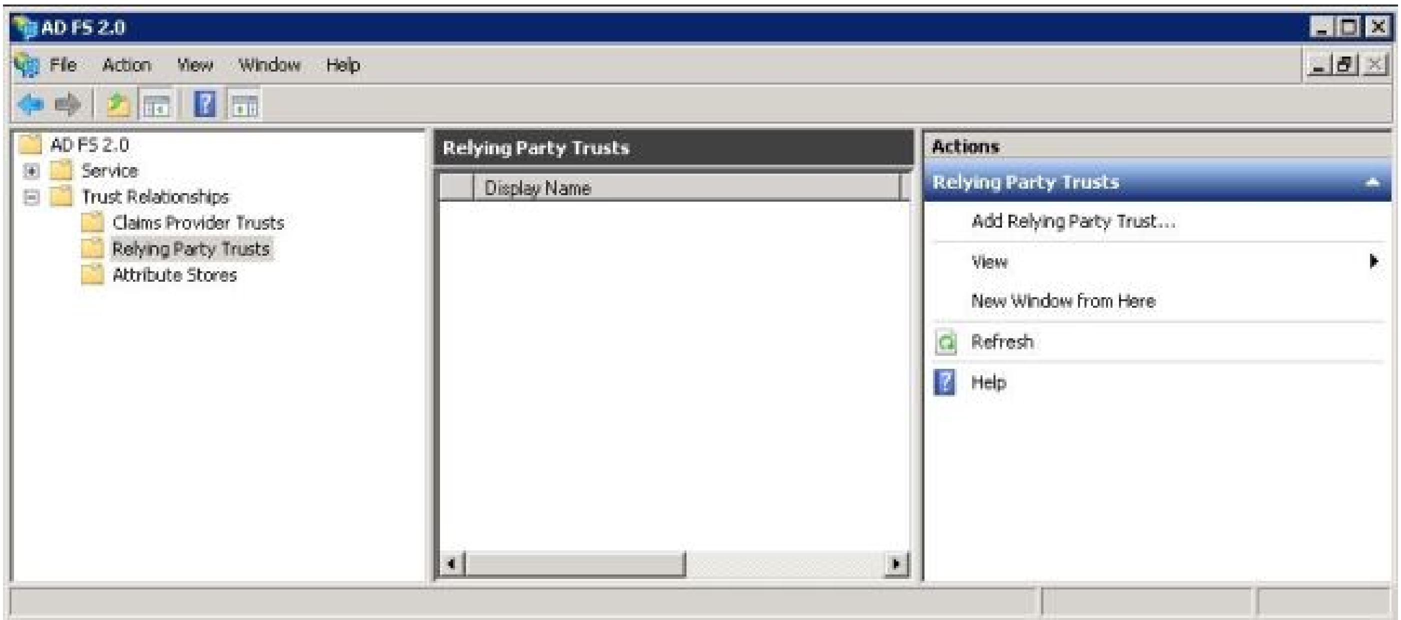
○ Per node (One metadata file per node)

Paso 2. Descargar metadatos IDP de AD FS

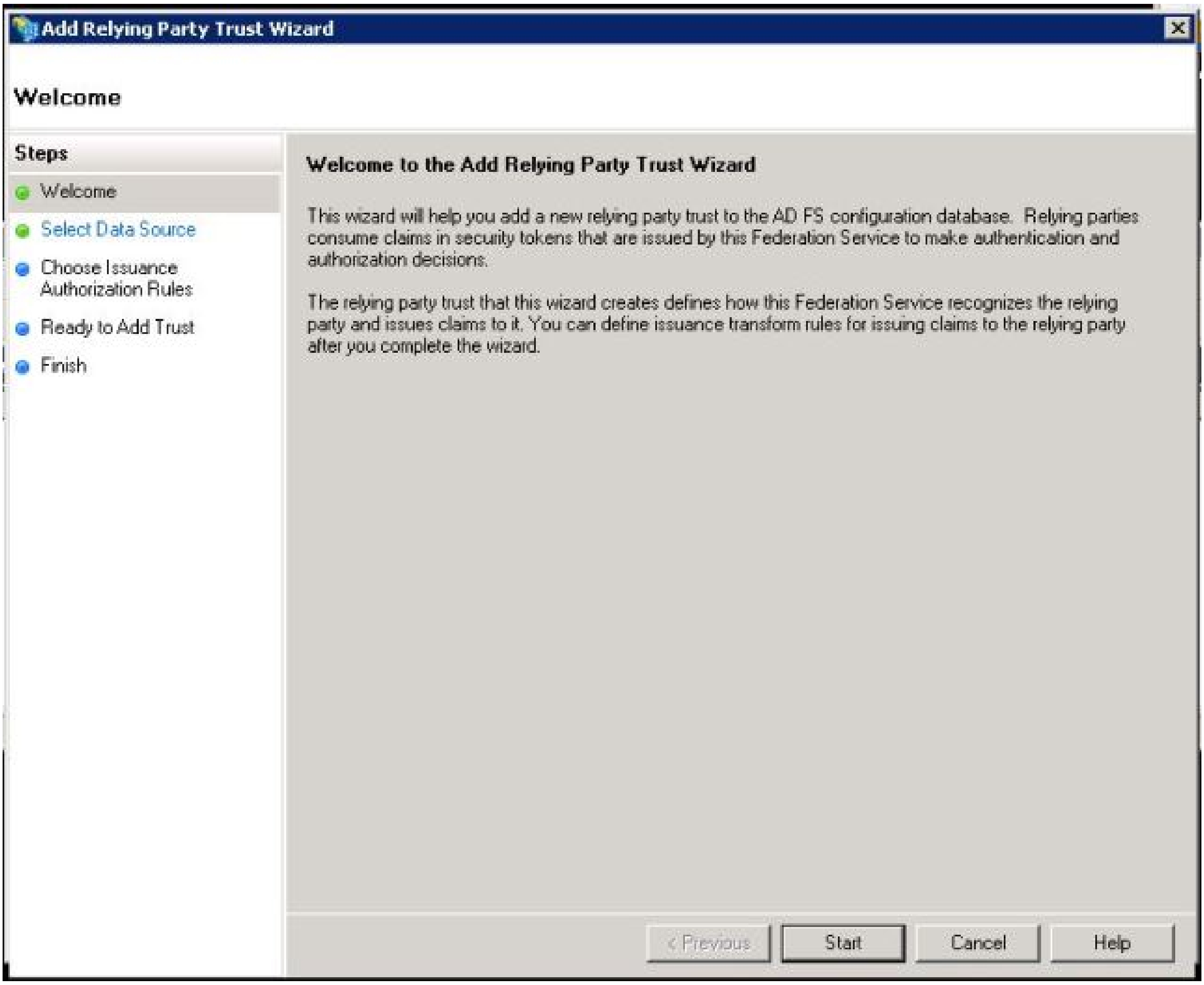
Para descargar los metadatos de IdP, consulte el enlace https:// <FQDN de ADFS>/federationmetadata/2007-06/federationmetadata.xml

Paso 3. IdP de aprovisionamiento

Como se muestra en la imagen, navegue hasta **AD FS 2.0 Management/Trust Relation Ships/ Confiying Party trust**. Haga clic en **Agregar confianza de persona de confianza**.



El Asistente para agregar confianza de terceros se abre como se muestra en la imagen y ahora haga clic en **Inicio**.

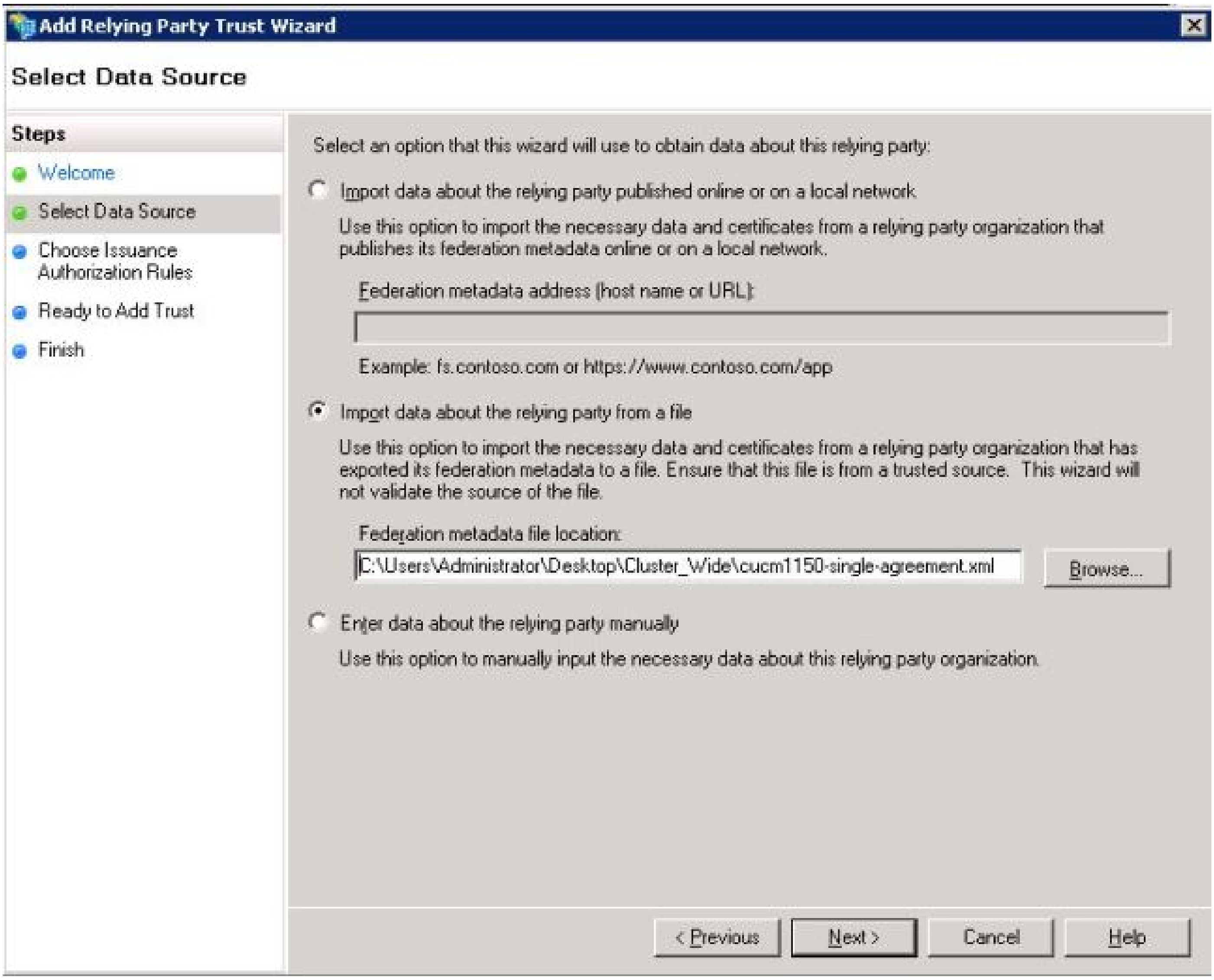


Welcome to the Add Relying Party Trust Wizard

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

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

Haga clic en los datos de importación de una persona que confía en un archivo. Examine los metadatos SP descargados de la página de configuración SSO de CUCM SAML. A continuación, haga clic en **Next**, como se muestra en la imagen:



Add Relying Party Trust Wizard

Select Data Source

Steps
Welcome
Select Data Source
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.

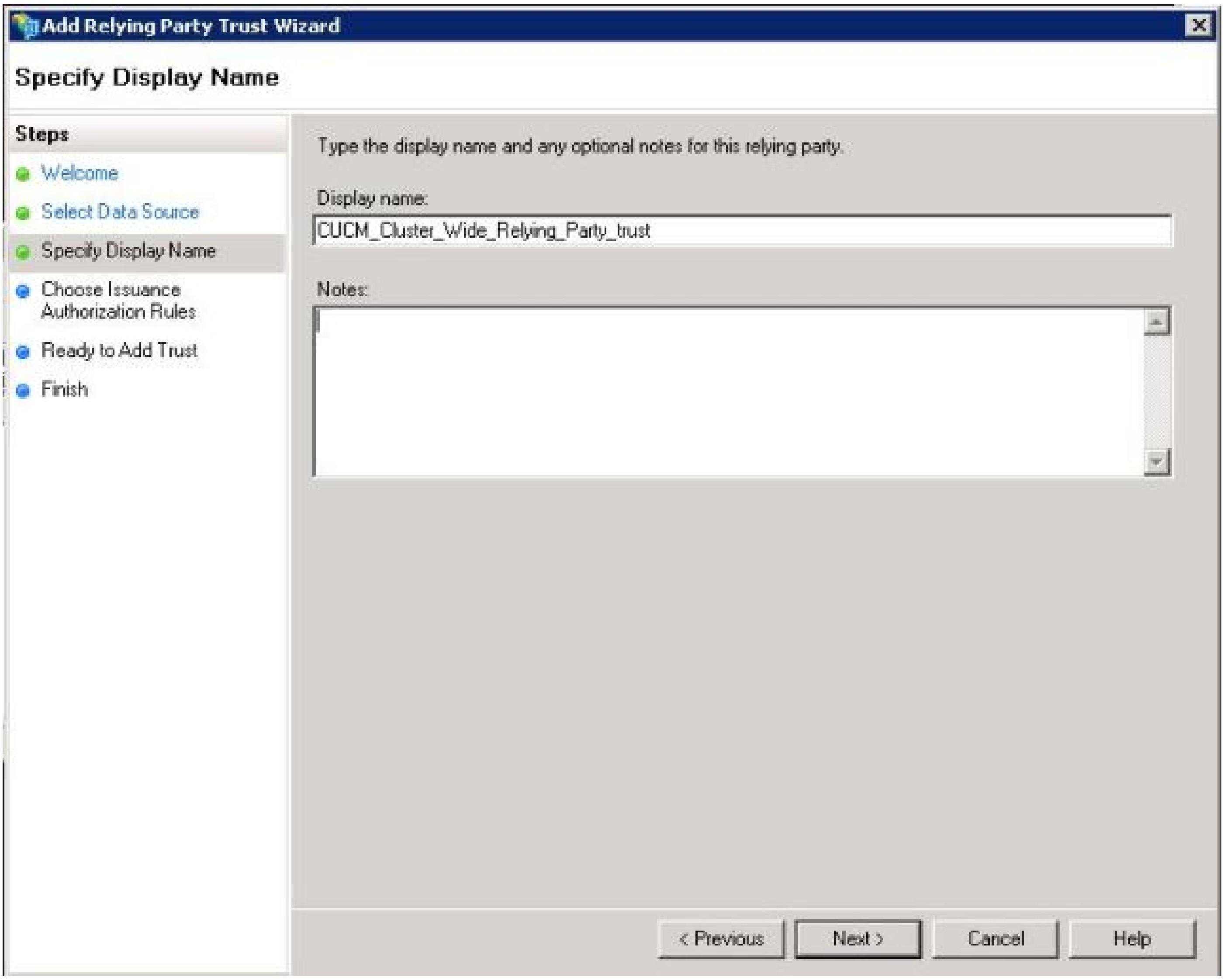
Federation metadata file location:

C:\Users\Administrator\Desktop\Cluster_Wide\cucm1150-single-agreement.xml

○ Enter data about the relying party manually

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

Escriba el nombre mostrado y las notas opcionales para la persona que confía. Haga clic en **Next.**, como se muestra en la imagen:

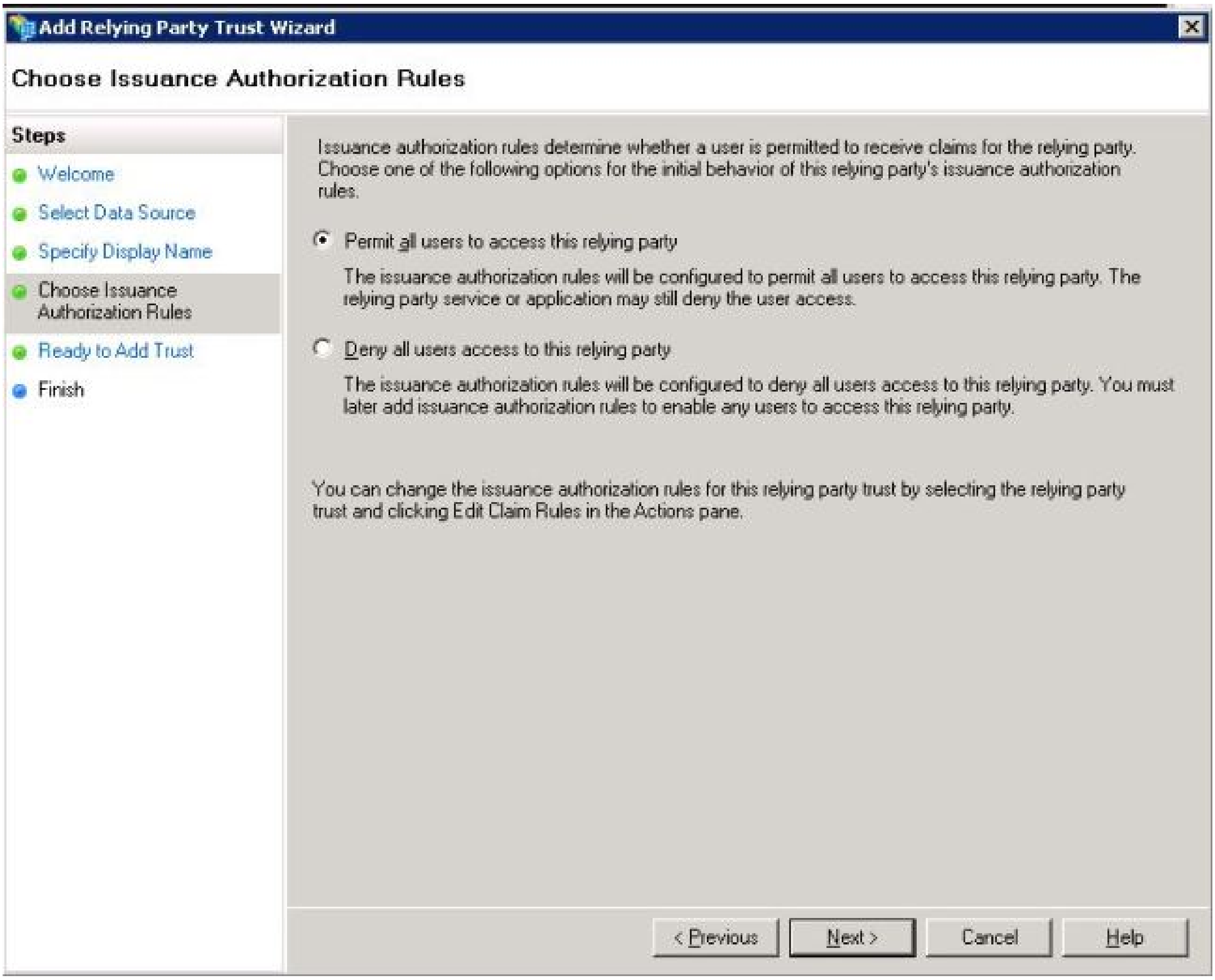


Type the display name and any optional notes for this relying party.

Display name: CUCM_Cluster_Wide_Relying_Party_trust

Notes:

Seleccione **Permitir que todos los usuarios accedan a esta persona de confianza** para permitir que todos los usuarios accedan a esta persona de confianza y, a continuación, haga clic en **Siguiente**, como se muestra en la imagen:



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

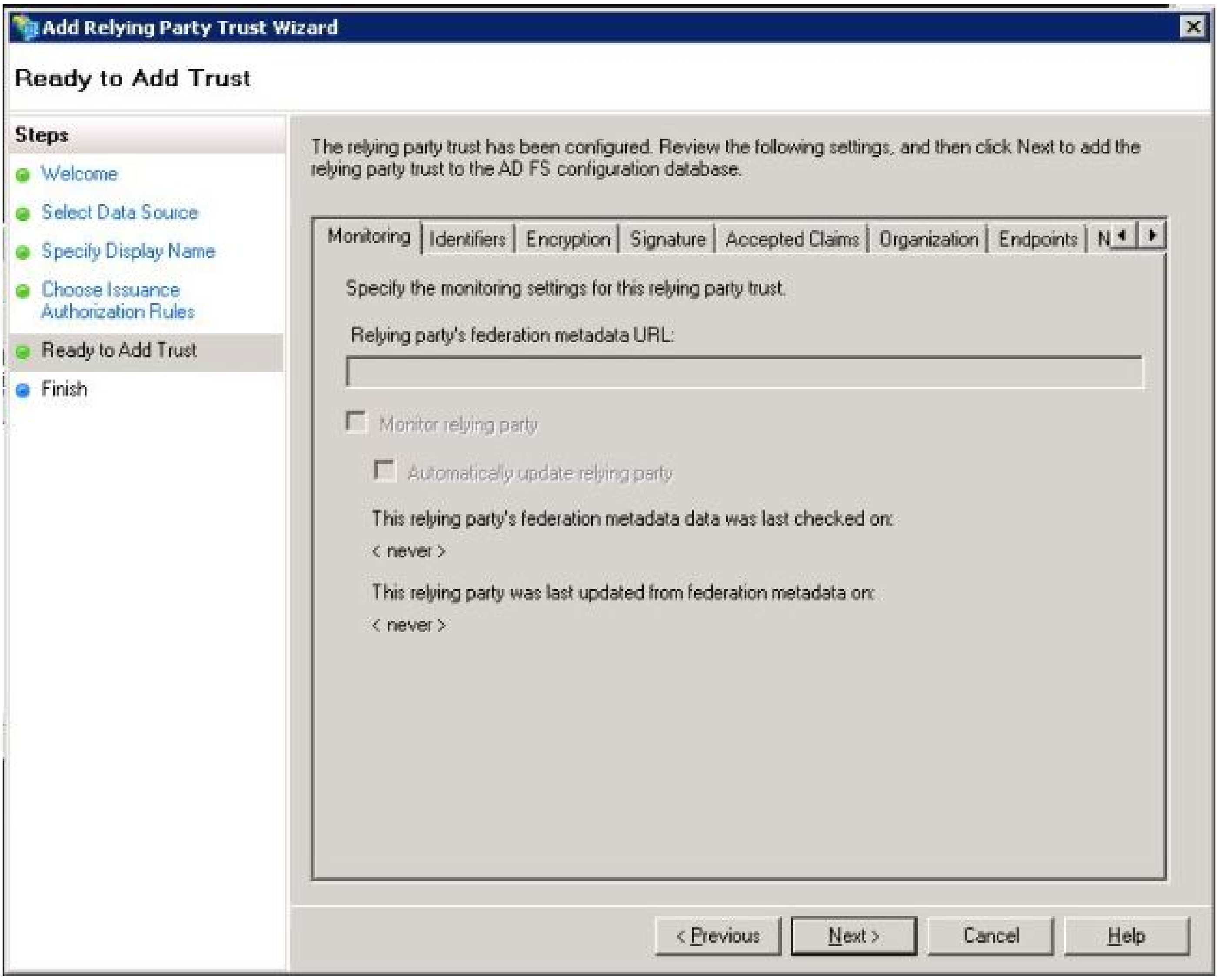
The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ 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.

En la página **Ready to Add Trust** (Listo para agregar confianza)**,** puede revisar la configuración de la confianza de la persona que confía, que se ha configurado. Ahora haga clic en **Next**, como se muestra en la imagen:



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:

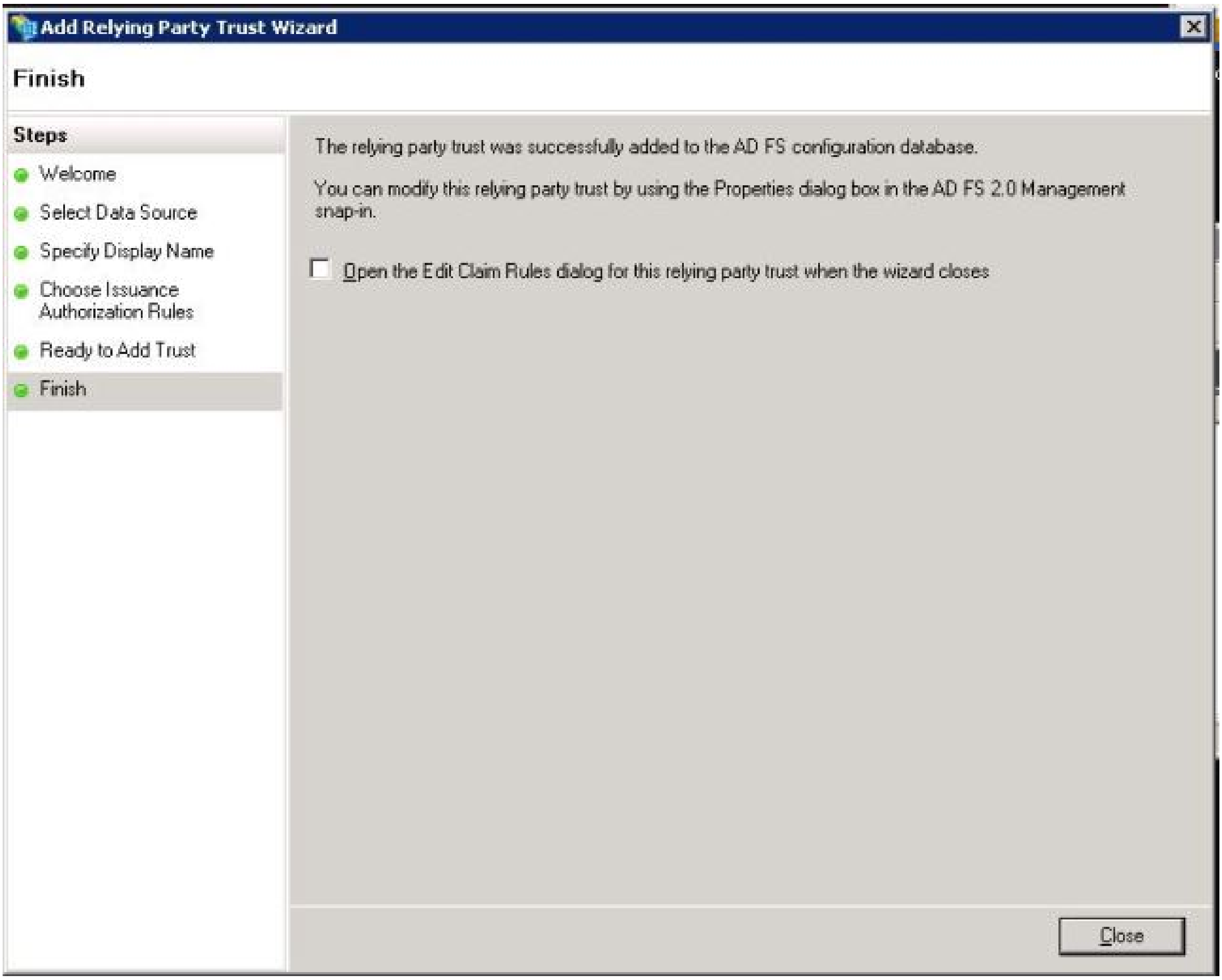
□ Monitor relying party

□ 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 >

La página final confirma que la confianza de la parte que confía se ha agregado correctamente a la base de datos de configuración de AD FS. Desactive la casilla y haga clic en **Cerrar**, como se muestra en la imagen:



Add Relying Party Trust Wizard

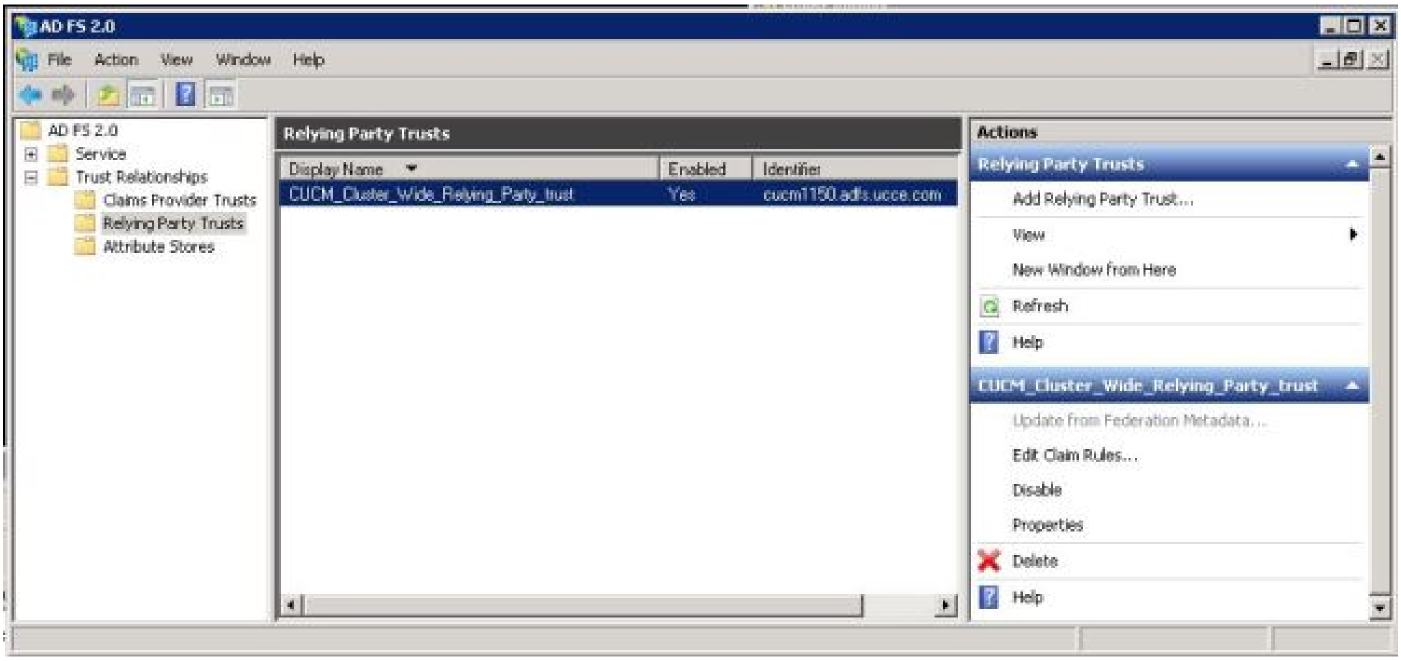
Finish

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 2.0 Management snap-in.

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

Haga clic con el botón derecho del ratón en **Confiar en los Fideicomisos** y haga clic en **Editar Reglas de Reclamación**, como se muestra en la imagen:

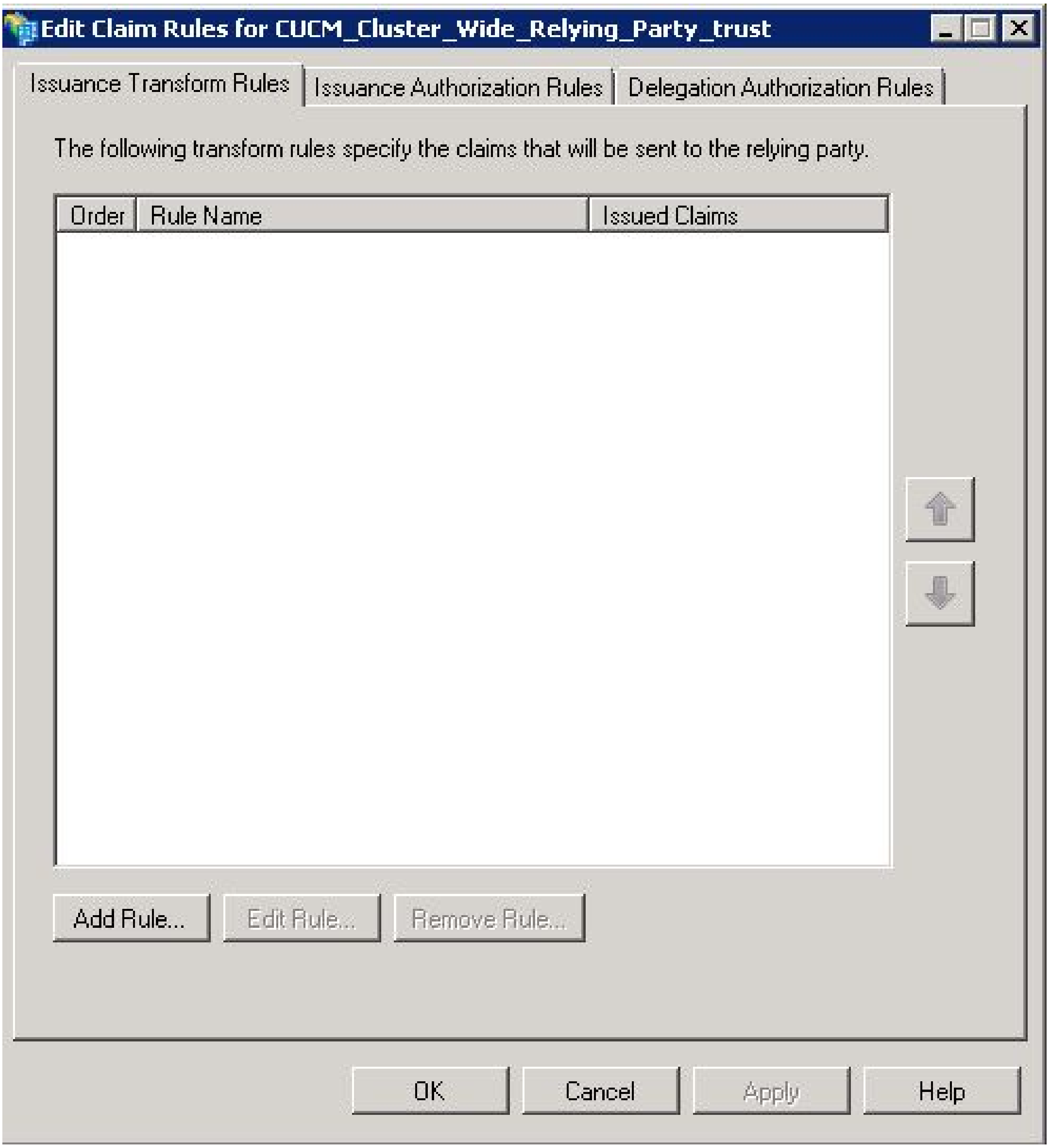


AD FS 2.0

Relying Party Trusts

Display Name	Enabled	Identifier
CUCM_Cluster_Wide_Relying_Party_trust	Yes	cucm1150.adfs.ucce.com

Ahora haga clic en **Agregar regla.**, como se muestra en la imagen:

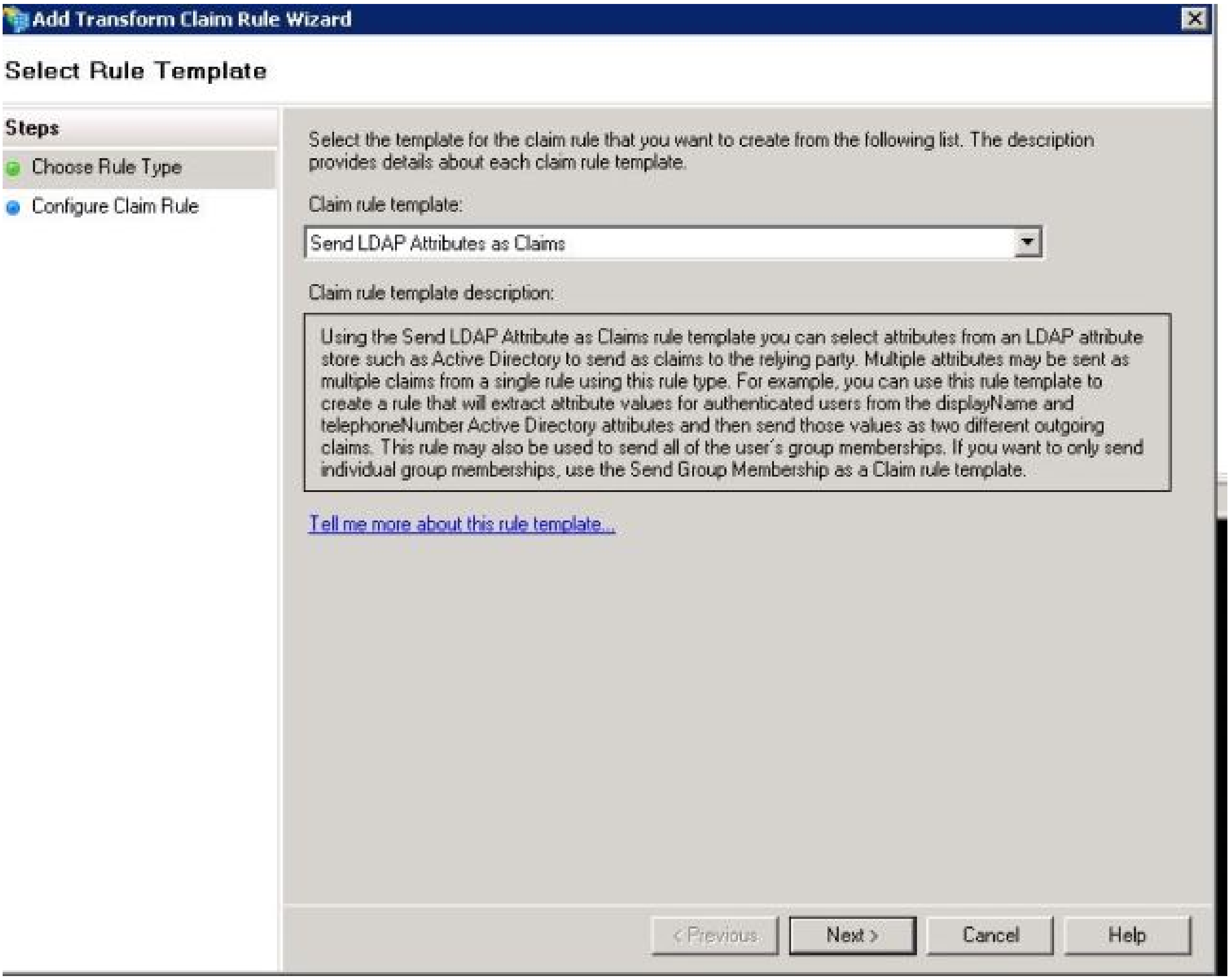


Edit Claim Rules for CUCM_Cluster_Wide_Relying_Party_trust

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

Order	Rule Name	Issued Claims

Cuando se abra **Add Transform Claim Rule**, haga clic en **Next** con la plantilla de regla de reclamación predeterminada **Send LDAP Attributes as Clas**, como se muestra en la imagen:



Select Rule Template

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

Claim rule template:

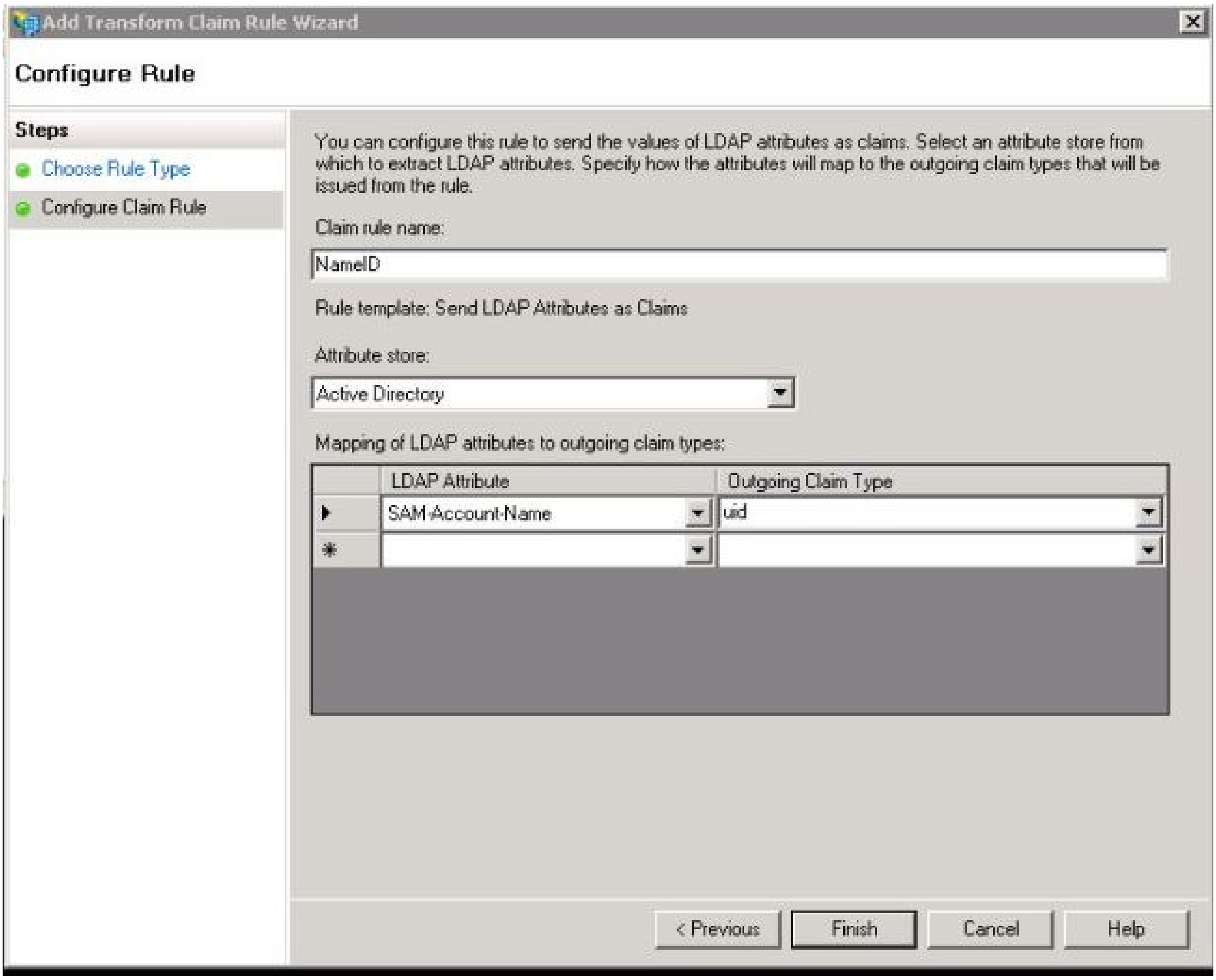
Send LDAP Attributes as Claims

Claim rule template description:

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

Tell me more about this rule template...

Haga clic en **Configurar regla de reclamación** como se muestra en esta imagen. El atributo LDAP debe coincidir con el atributo LDAP en la configuración del directorio LDAP en CUCM. Administrar el tipo de reclamación saliente como **uid**. Haga clic en **Finalizar**, como se muestra en la imagen:



Add Transform Claim Rule Wizard

Configure Rule

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

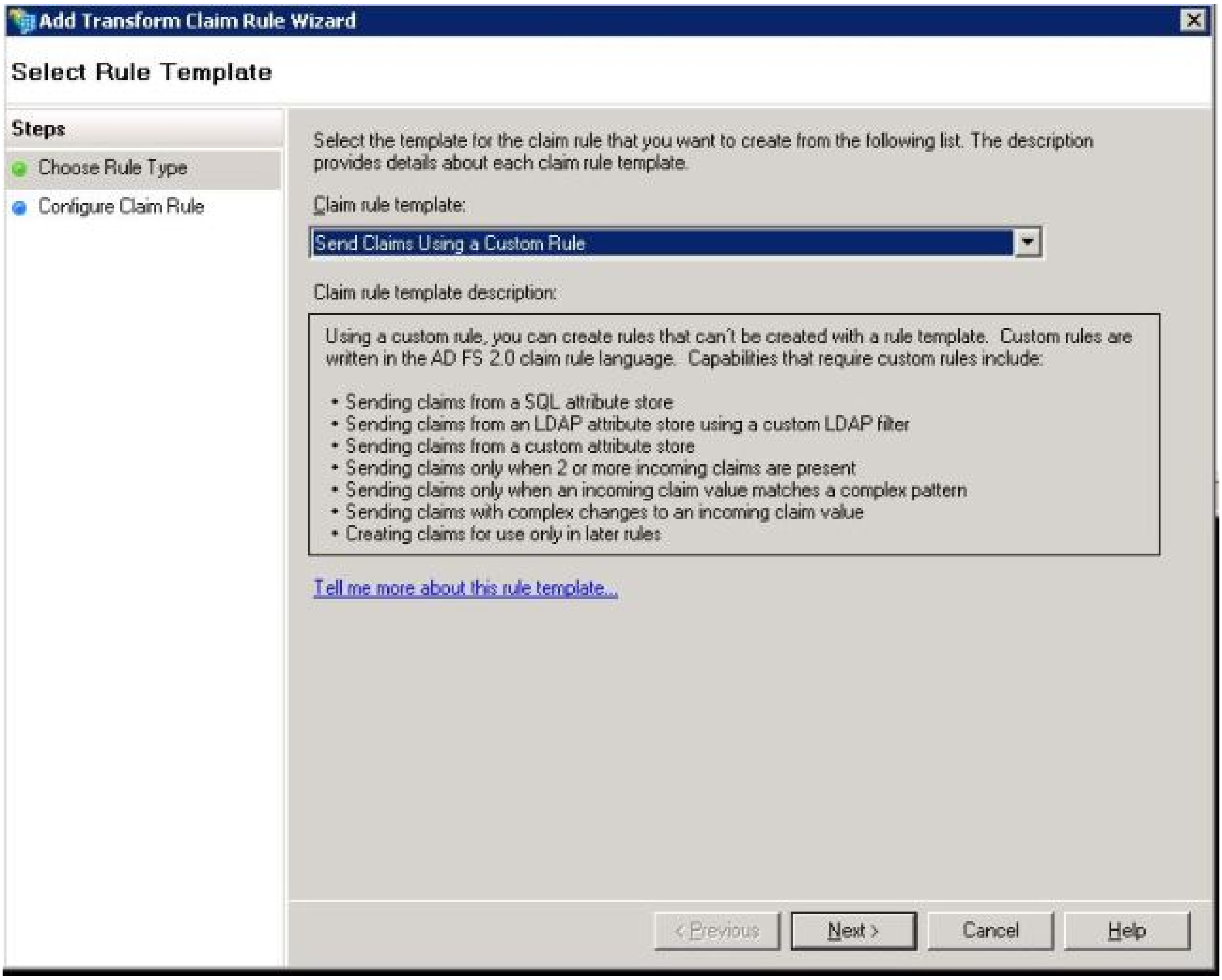
Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
▶	SAM-Account-Name	uid
✱		

Agregue la regla personalizada para la persona de confianza. Haga clic en **Agregar regla**. Seleccione **Enviar justificantes de venta utilizando una regla personalizada** y, a continuación, haga clic en **Siguiente,** como se muestra en la imagen:



Add Transform Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule

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 2.0 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

Tell me more about this rule template...

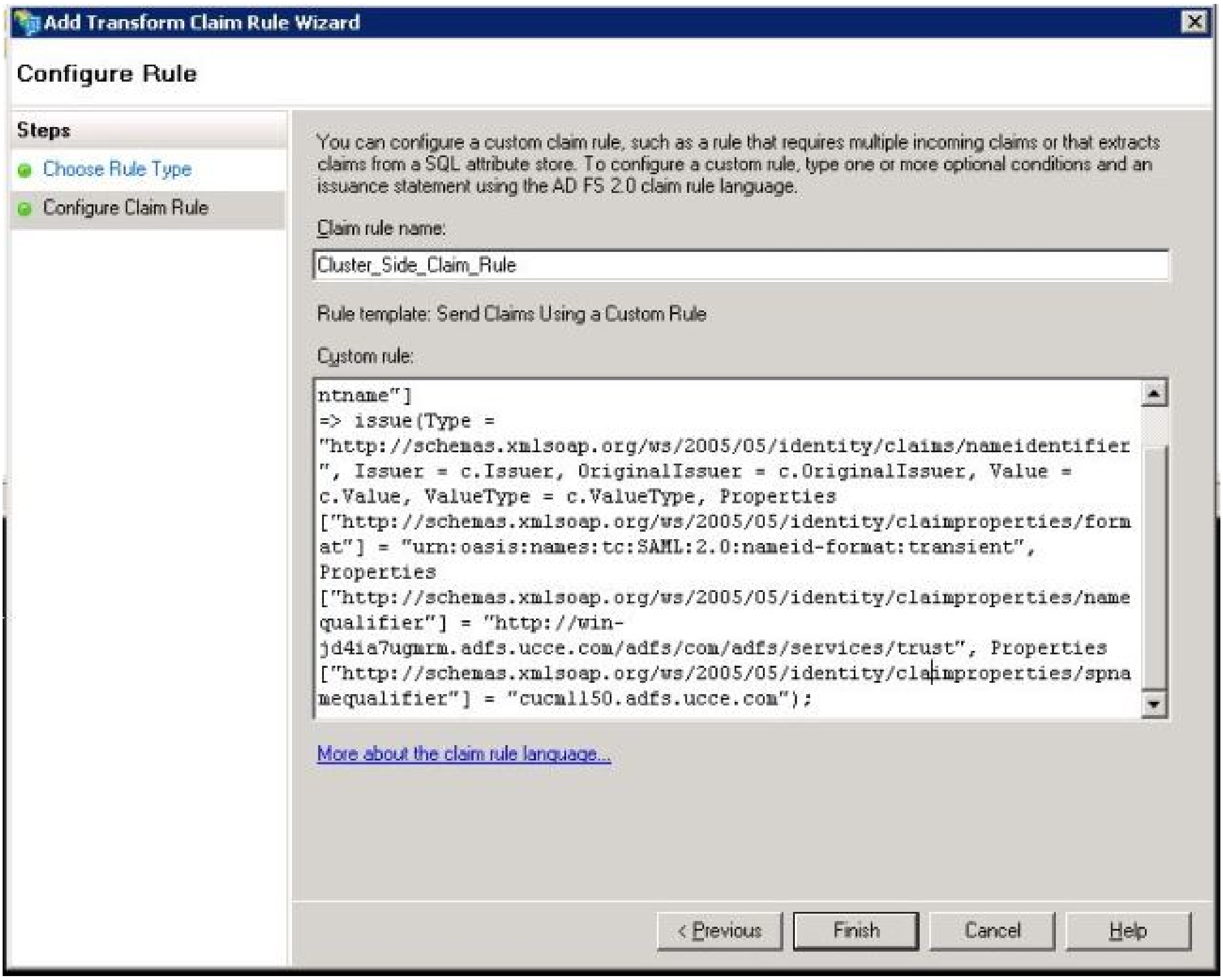
En la regla Configurar reclamación, escriba un Nombre de regla de reclamación y, a continuación, copie la regla de reclamación dada y pasada en el campo Regla personalizada del asistente modificando el calificador de nombre y nombre de archivo en la regla de reclamación. Haga clic en **Finalizar**., como se muestra en la imagen:

Regla de reclamación:

```
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.
```



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.

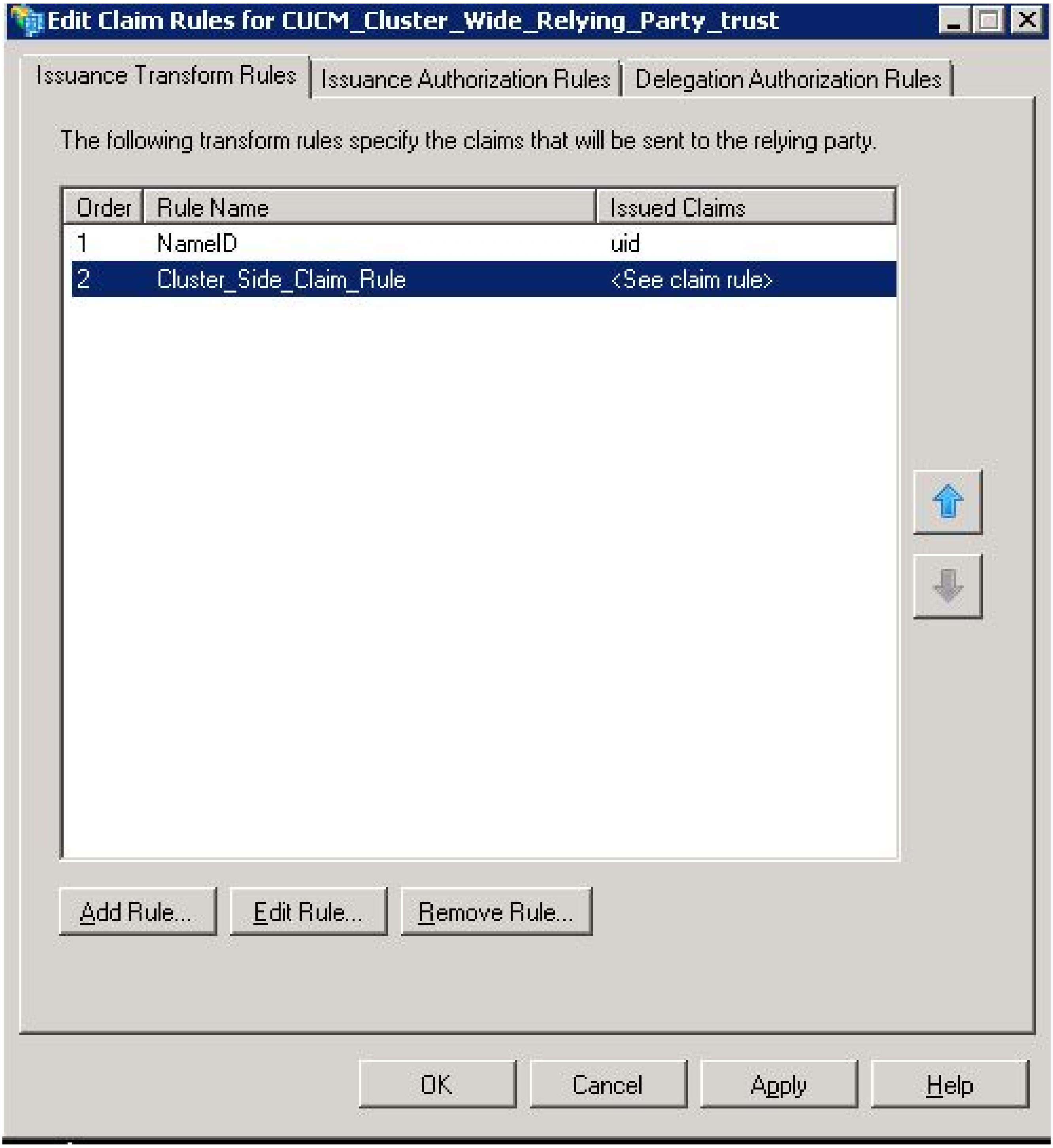
Claim rule name: Cluster_Side_Claim_Rule

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
ntname"]
=> 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/form
at"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/name
qualifier"] = "http://win-
jd4ia7ugmrm.adfs.ucce.com/adfs/com/adfs/services/trust", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spna
mequalifier"] = "cucm1150.adfs.ucce.com");
```

Como se muestra en la imagen, haga clic en **Aplicar** y luego **Aceptar**.


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

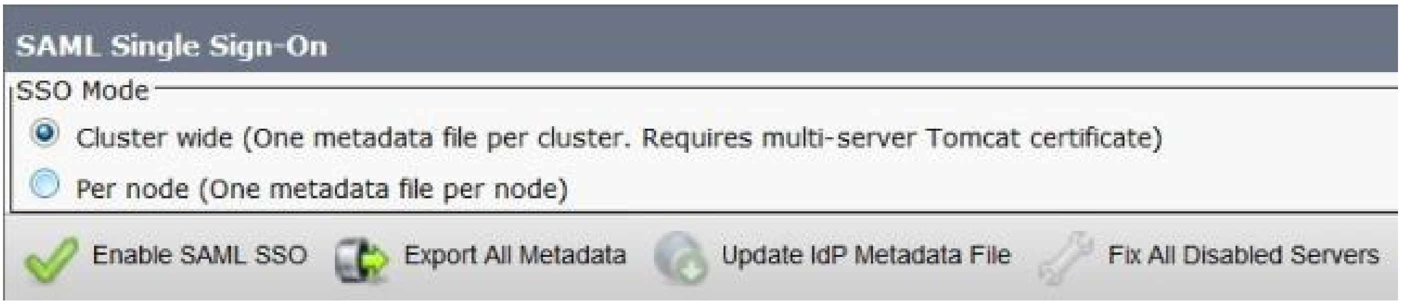
The following transform rules specify the claims that will be sent to the relying party.

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

Paso 4. Habilitar SAML SSO

Abra un navegador web, inicie sesión en CUCM como administrador y navegue **a System >SAML Single Sign On**.

De forma predeterminada, se selecciona el botón de opción **Clúster Wide**. Haga clic en **Enable Saml SSO**, como se muestra en la imagen:



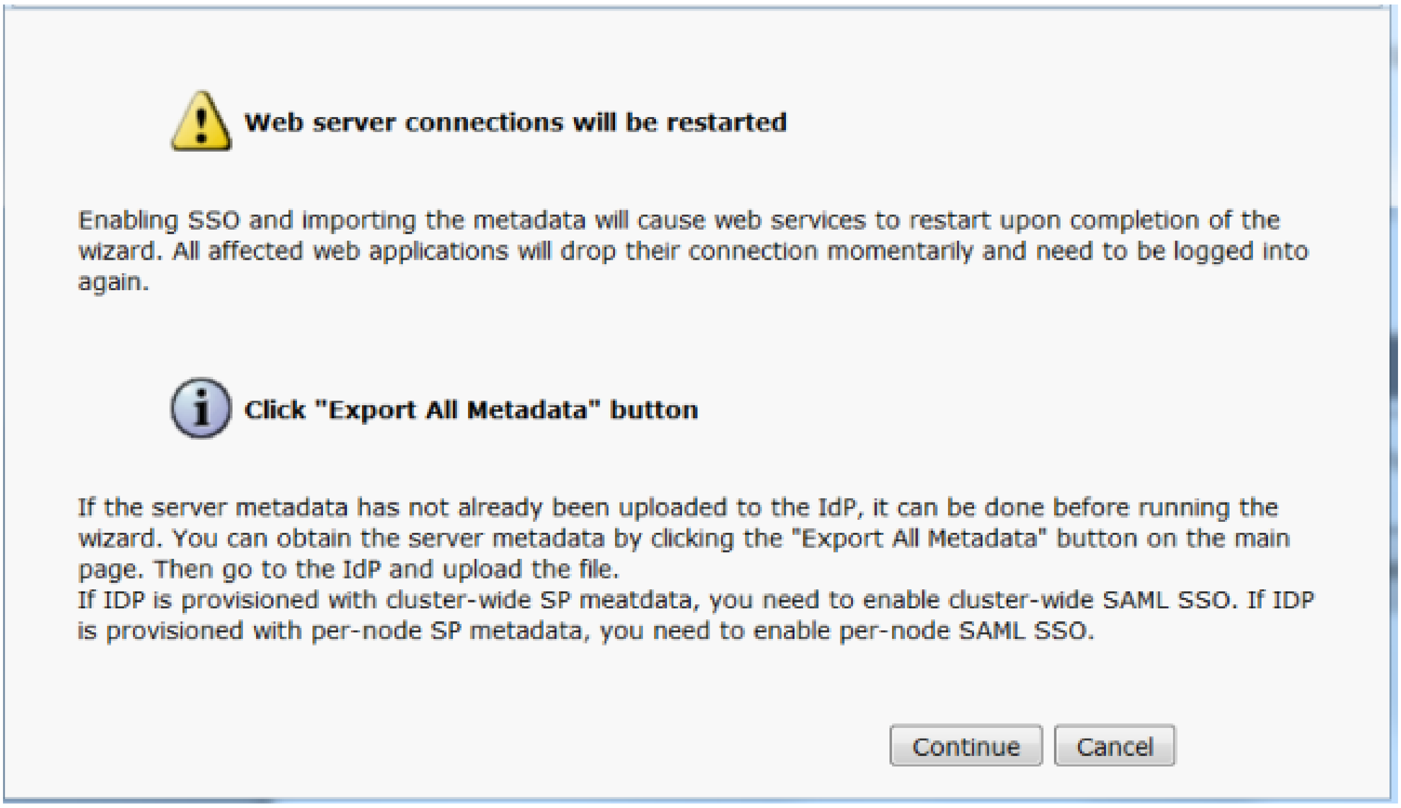
SAML Single Sign-On

SSO Mode

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

○ Per node (One metadata file per node)

Como se muestra en la imagen, la ventana emergente notifica la advertencia de reinicio del servidor web e información para elegir el SSO SAML de clúster o el SSO SAML de nodo por nodo según idp. Haga clic en **Continue** (Continuar).



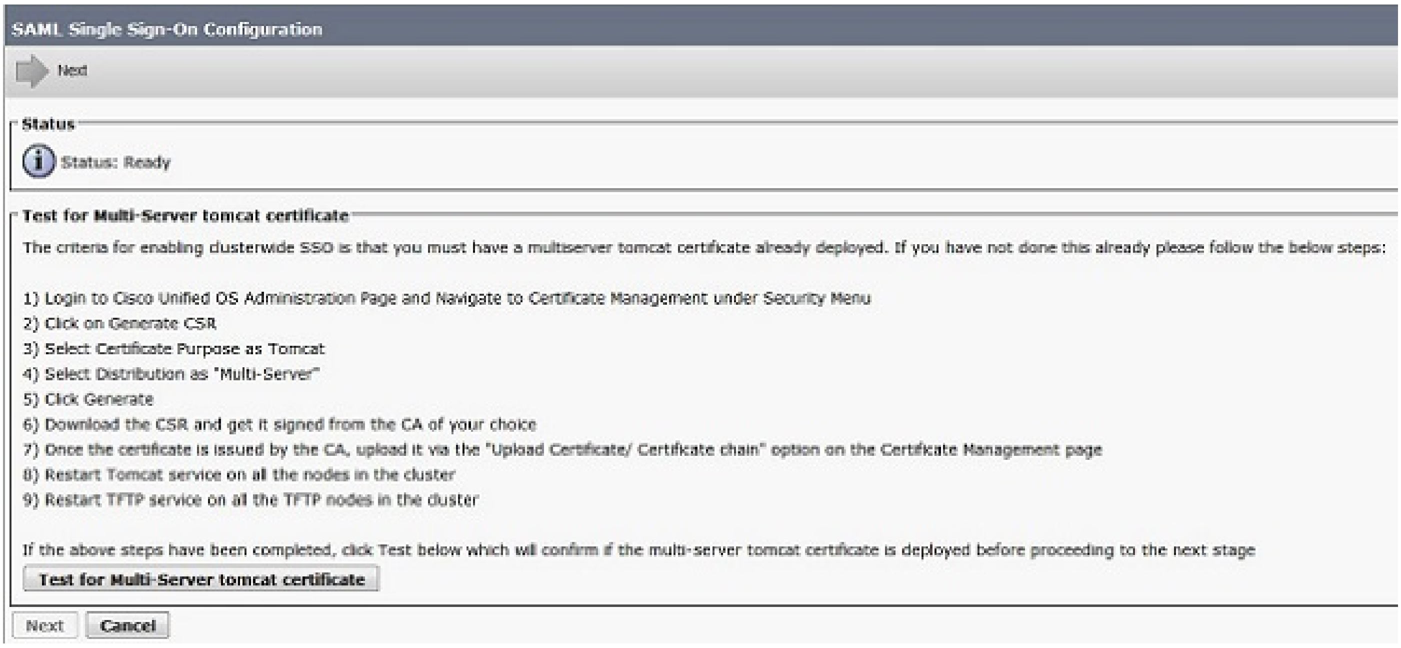
Web server connections will be restarted

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.

Click "Export All Metadata" button

If the server metadata has not already been uploaded to the IdP, it can be done before running the wizard. You can obtain the server metadata by clicking the "Export All Metadata" button on the main page. Then go to the IdP and upload the file.
If IDP is provisioned with cluster-wide SP meatdata, you need to enable cluster-wide SAML SSO. If IDP is provisioned with per-node SP metadata, you need to enable per-node SAML SSO.

El criterio para habilitar el SSO en todo el clúster es que debe tener un certificado de tomcat multiservidor ya implementado. Haga clic en **Test for Multi-Server tomcat Certificate**, como se muestra en la imagen:


SAML Single Sign-On Configuration
Next
Status

Status: Ready

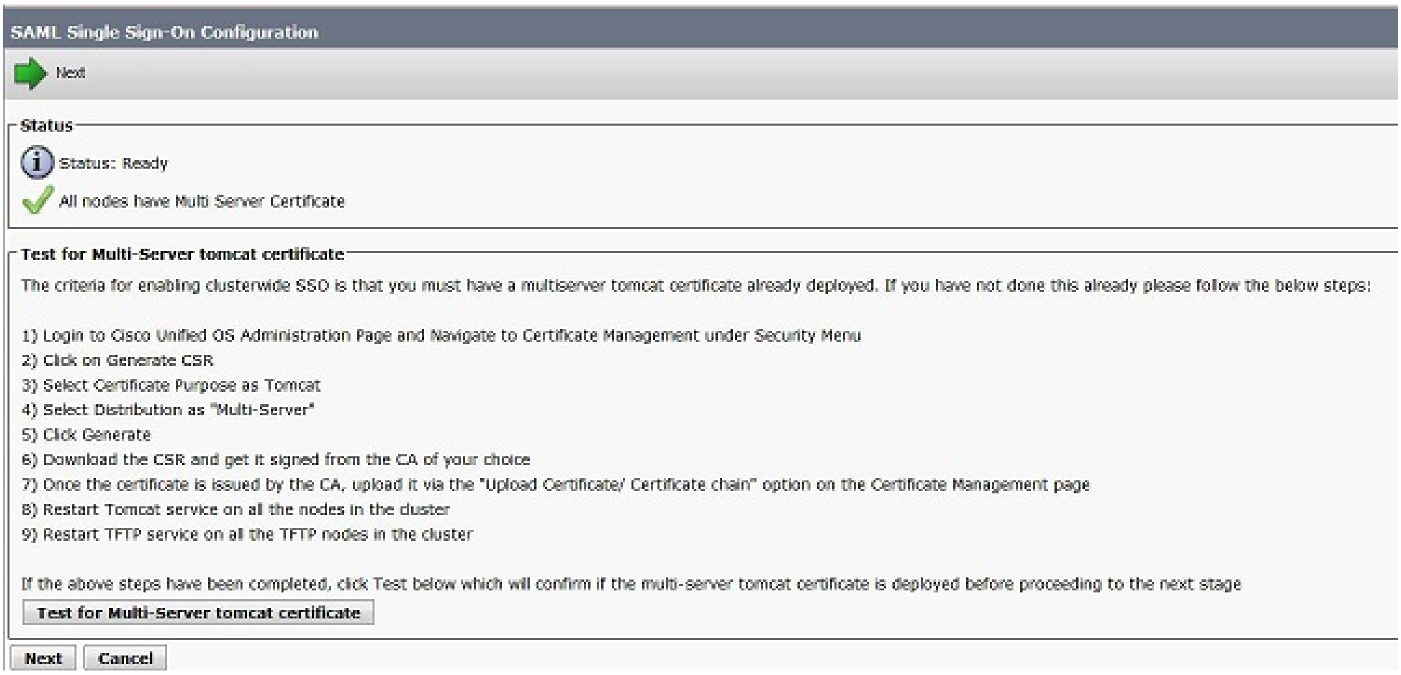
Test for Multi-Server tomcat certificate

The criteria for enabling clusterwide SSO is that you must have a multiserver tomcat certificate already deployed. If you have not done this already please follow the below steps:

1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
2) Click on Generate CSR
3) Select Certificate Purpose as Tomcat
4) Select Distribution as "Multi-Server"
5) Click Generate
6) Download the CSR and get it signed from the CA of your choice
7) Once the certificate is issued by the CA, upload it via the "Upload Certificate/ Certificate chain" option on the Certificate Management page
8) Restart Tomcat service on all the nodes in the cluster
9) Restart TFTP service on all the TFTP nodes in the cluster

If the above steps have been completed, click Test below which will confirm if the multi-server tomcat certificate is deployed before proceeding to the next stage

Una vez que se confirma, todos los nodos tienen certificado de servidor múltiple muestra un **certificado de todos los nodos tienen un certificado de servidor múltiple**, y luego haga clic en **Siguiente**, como se muestra en la imagen:


SAML Single Sign-On Configuration
Next
Status

Status: Ready

✓ All nodes have Multi Server Certificate

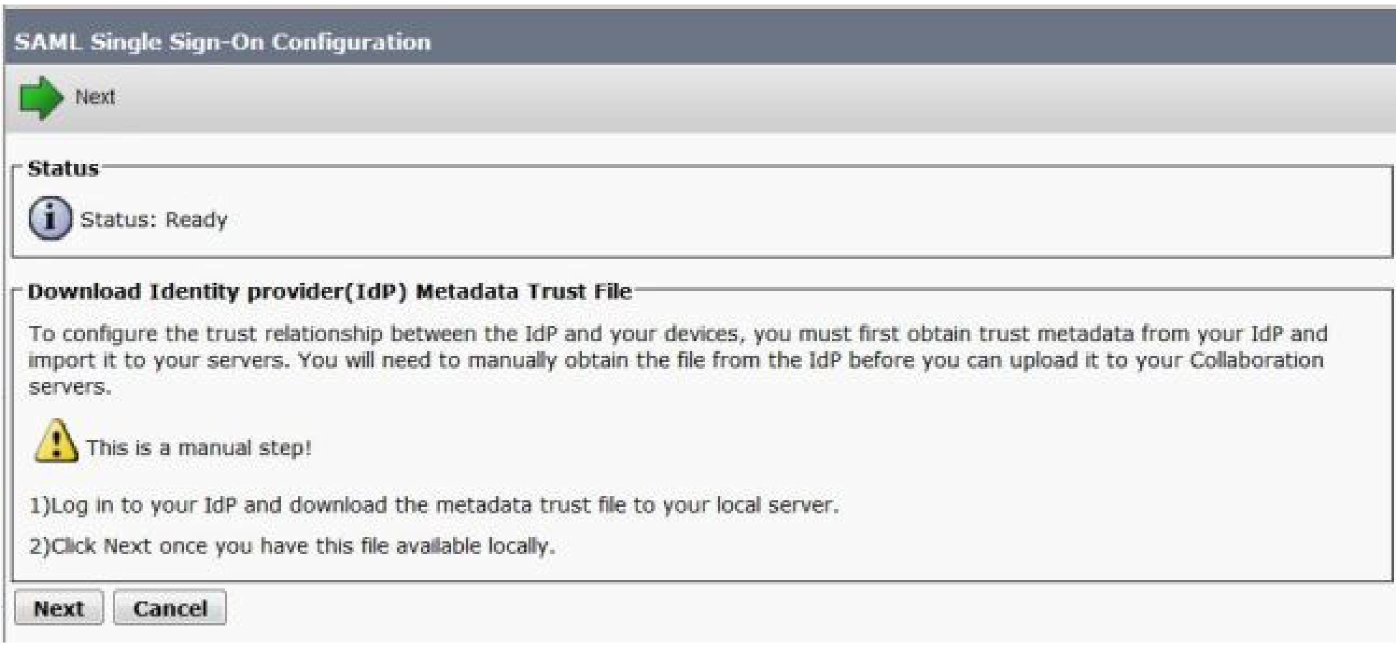
Test for Multi-Server tomcat certificate

The criteria for enabling clusterwide SSO is that you must have a multiserver tomcat certificate already deployed. If you have not done this already please follow the below steps:

1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
2) Click on Generate CSR
3) Select Certificate Purpose as Tomcat
4) Select Distribution as "Multi-Server"
5) Click Generate
6) Download the CSR and get it signed from the CA of your choice
7) Once the certificate is issued by the CA, upload it via the "Upload Certificate/ Certificate chain" option on the Certificate Management page
8) Restart Tomcat service on all the nodes in the cluster
9) Restart TFTP service on all the TFTP nodes in the cluster

If the above steps have been completed, click Test below which will confirm if the multi-server tomcat certificate is deployed before proceeding to the next stage

Como se muestra en la imagen, haga clic en **Next**.



SAML Single Sign-On Configuration

Status

Status: Ready

Download Identity provider(IdP) Metadata Trust File

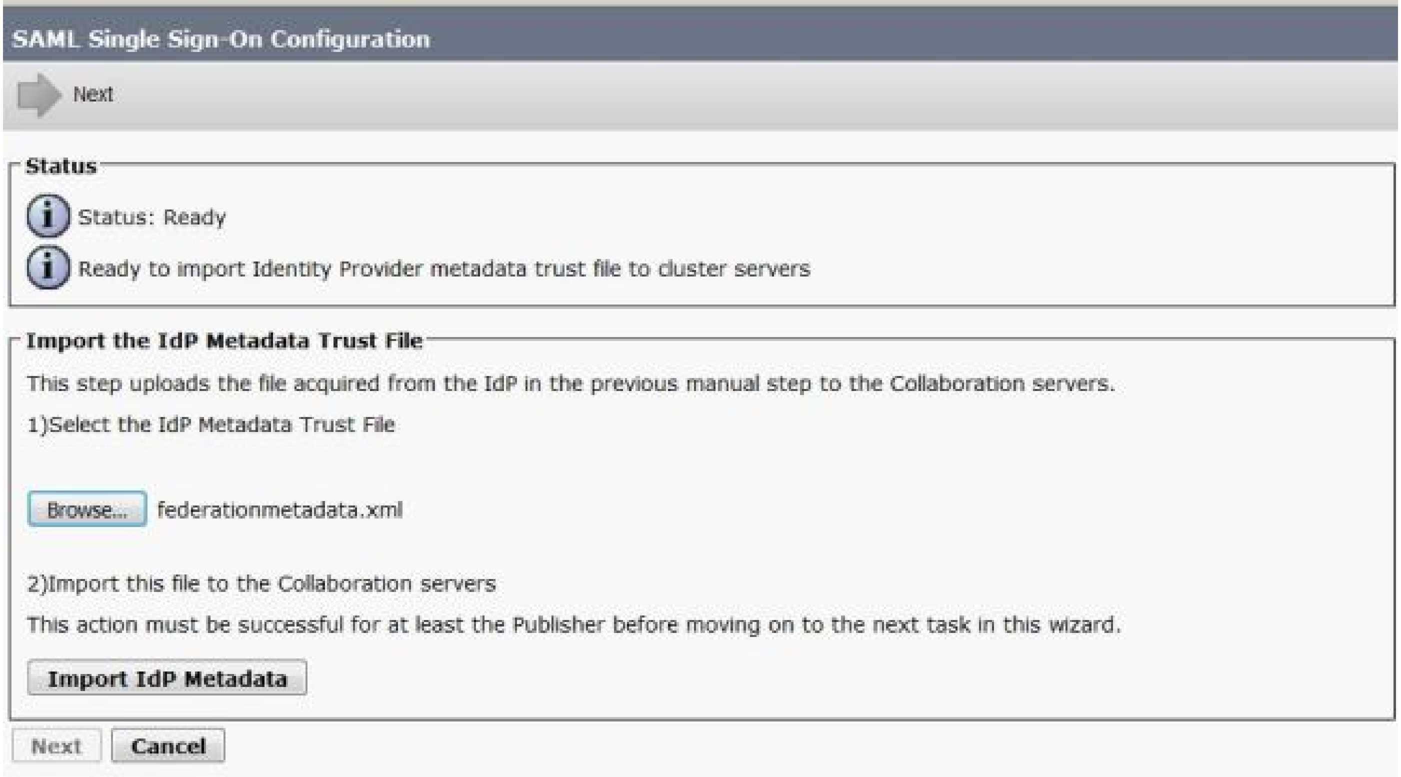
To configure the trust relationship between the IdP and your devices, you must first obtain trust metadata from your IdP and import it to your servers. You will need to manually obtain the file from the IdP before you can upload it to your Collaboration servers.

This is a manual step!

1)Log in to your IdP and download the metadata trust file to your local server.

2)Click Next once you have this file available locally.

Busque y seleccione los metadatos de IdP descargados. Haga clic en **Importar metadatos IdP**, como se muestra en la imagen:



SAML Single Sign-On Configuration

Status

Status: Ready

Ready to import Identity Provider metadata trust file to cluster 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.

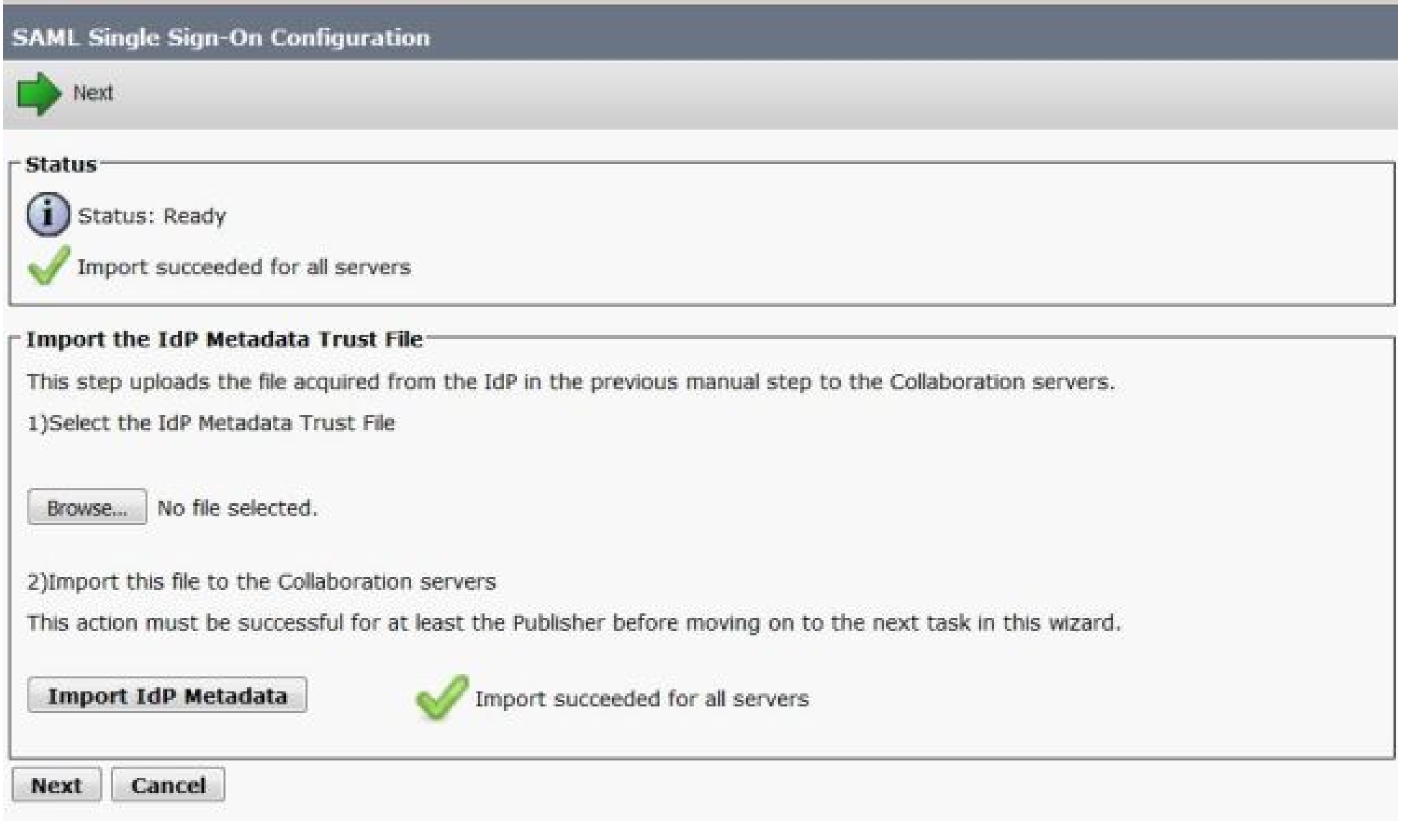
1)Select the IdP Metadata Trust File

Browse... federationmetadata.xml

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.

La página confirma que la importación se ha realizado correctamente en todos los servidores y, a continuación, hace clic en **Siguiente**, como se muestra en la imagen:


SAML Single Sign-On Configuration

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

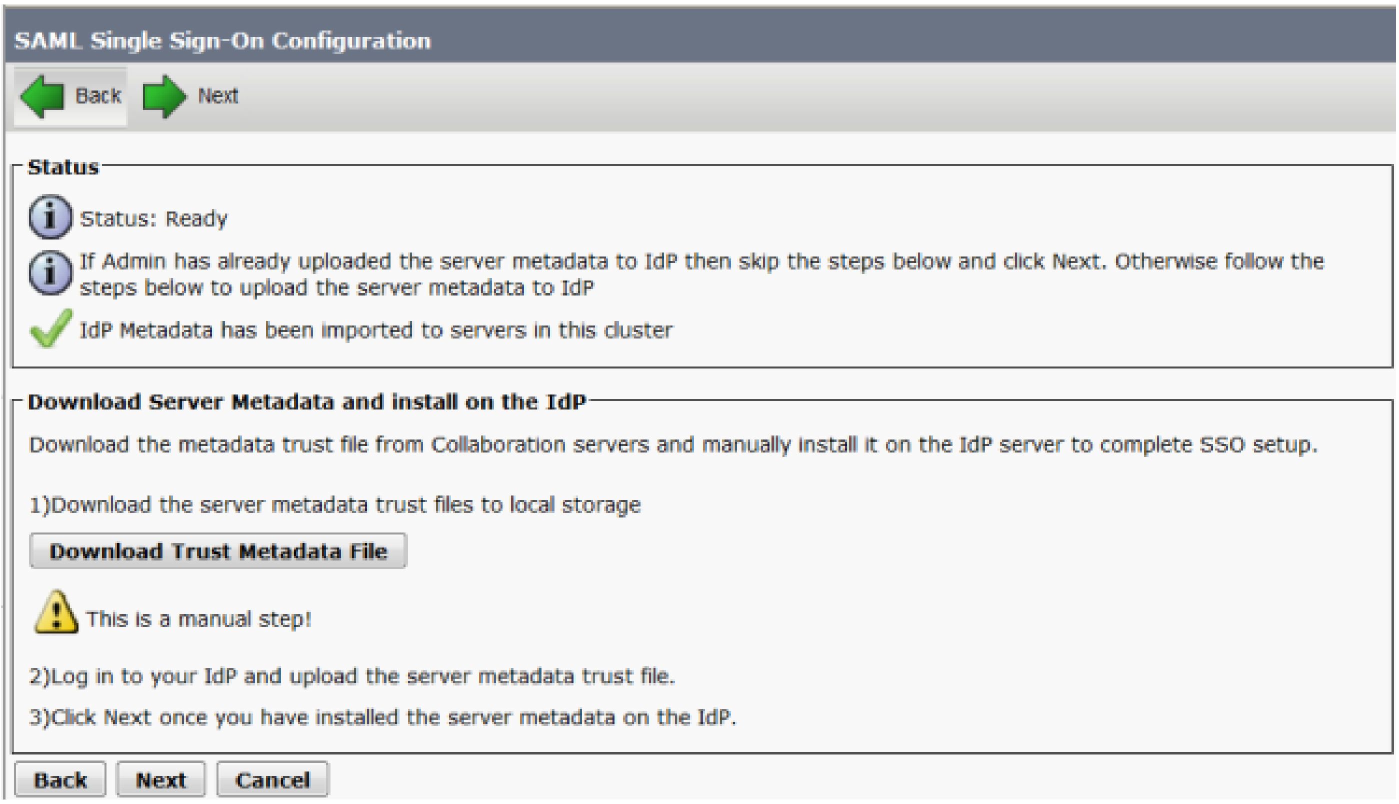
Browse... No file selected.

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

Como se muestra en la imagen, haga clic en **Next**, ya que ya exportó los metadatos SP de la página de configuración SSO de SAML inicial.


SAML Single Sign-On Configuration

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

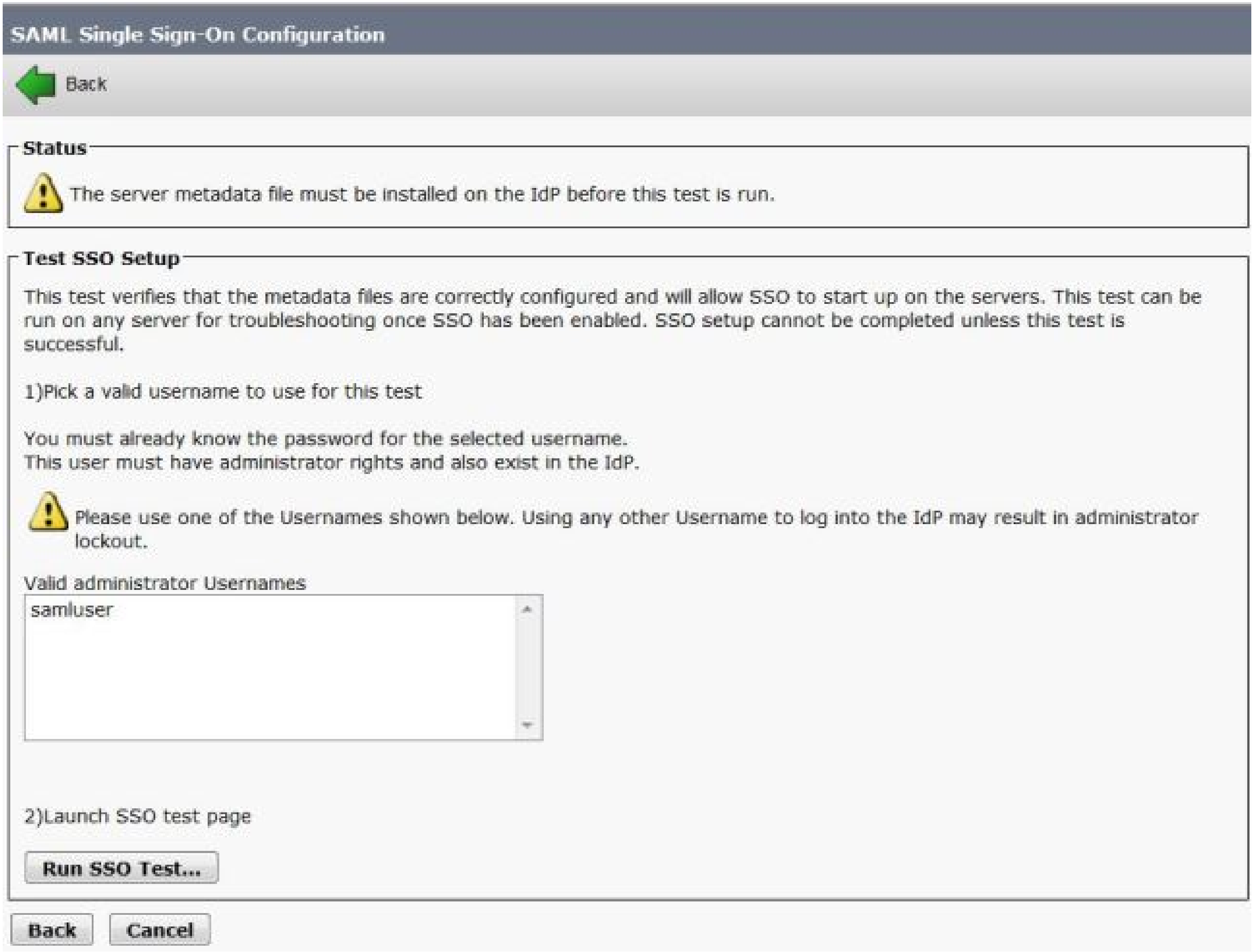
Download Trust Metadata File

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.

CUCM debe estar sincronizado con el directorio LDAP. El asistente muestra los usuarios de administrador válidos configurados en el directorio LDAP. Seleccione el usuario y haga clic en **Ejecutar prueba SSO**, como se muestra en la imagen:



SAML Single Sign-On Configuration

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

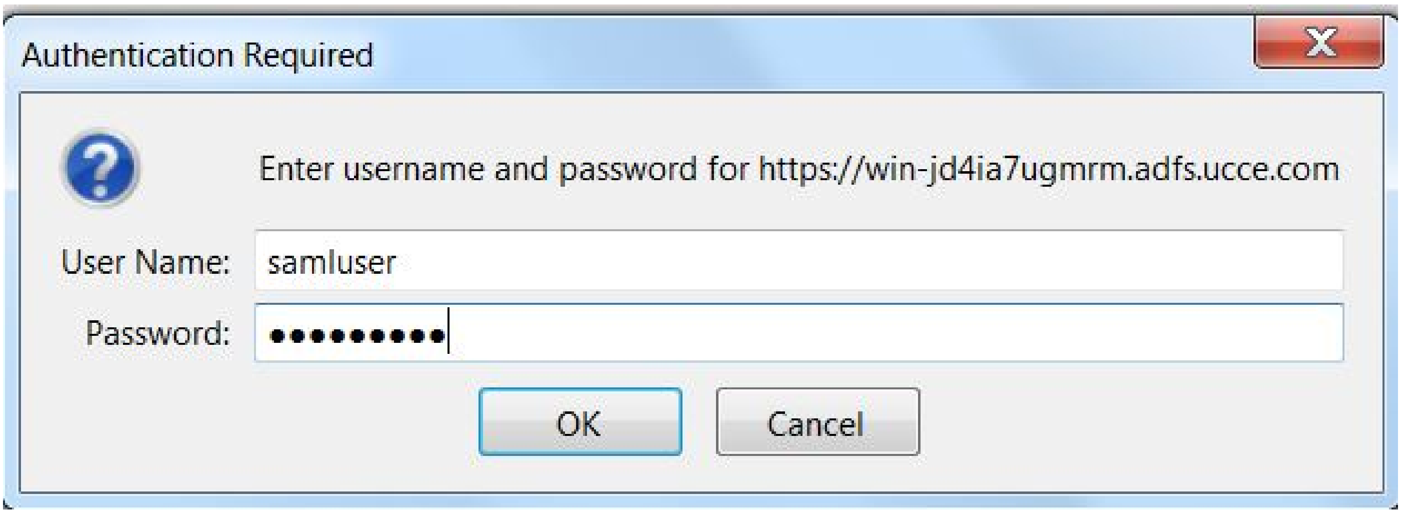
You must already know the password for the selected username.
This user must have administrator rights and also exist in the IdP.

⚠ 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

Como se muestra en la imagen, introduzca el ID de usuario y la contraseña correspondiente una vez que se lo solicite.



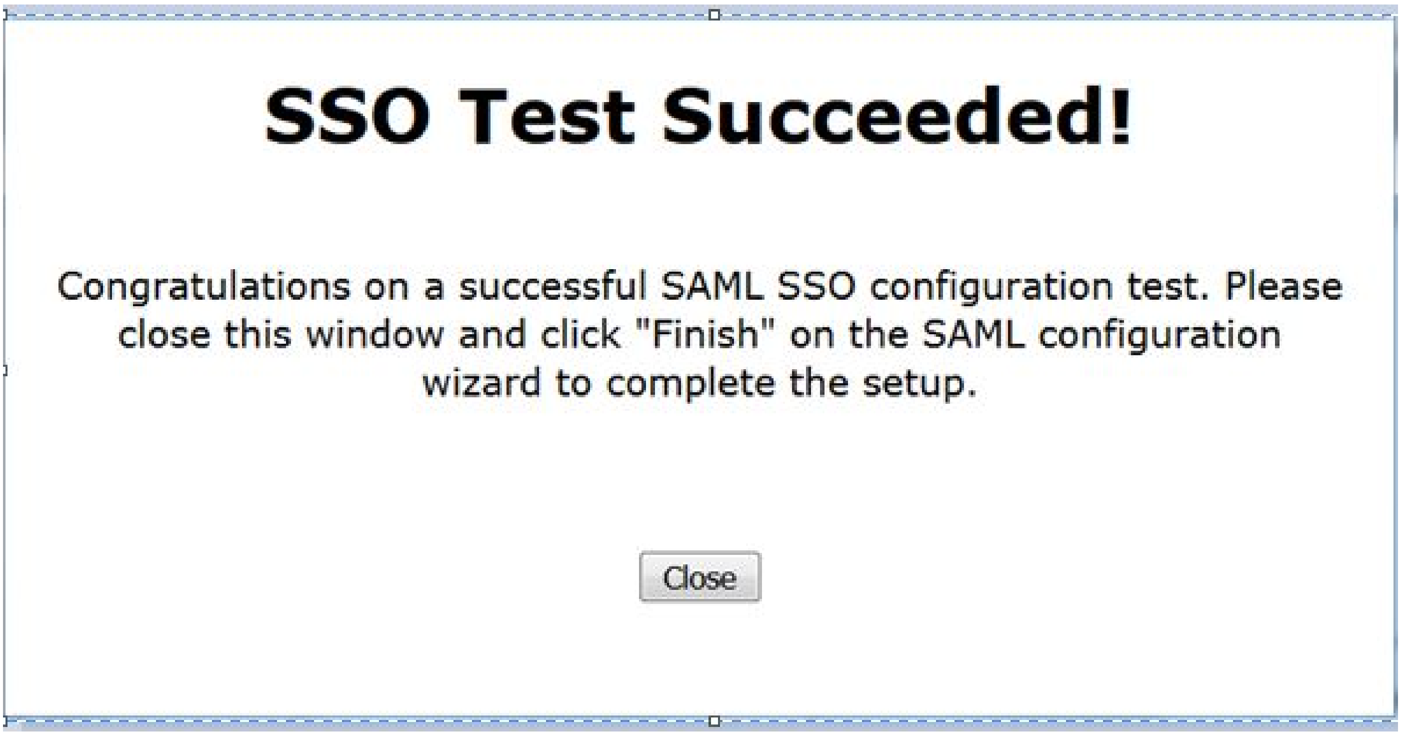
Authentication Required

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

User Name: samluser

Password: ●●●●●●●●●

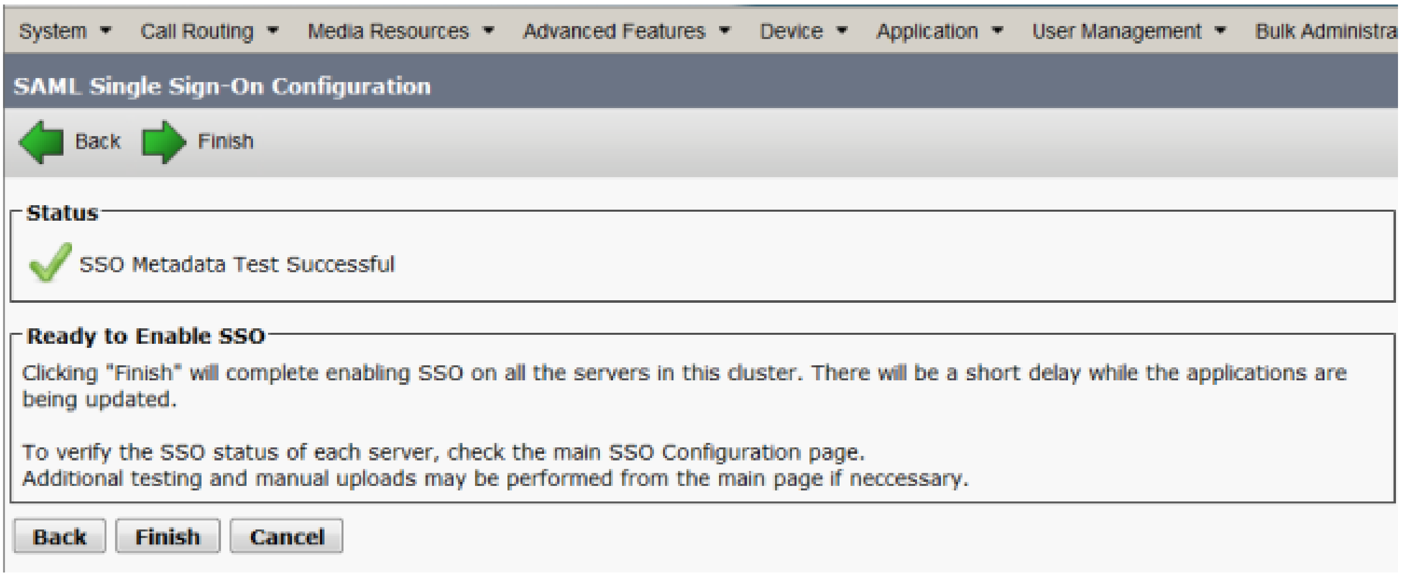
La ventana emergente, como se muestra en la imagen, confirma que la prueba se ha realizado correctamente.



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.

Como se muestra en la imagen, haga clic en **Finalizar** para completar la configuración para habilitar SSO.



SAML Single Sign-On Configuration

Status

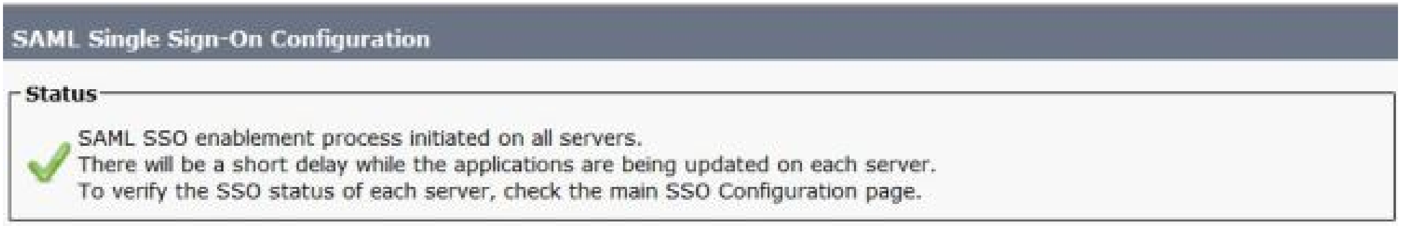
✓ SSO Metadata Test Successful

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 neccessary.

La página mostrada en la imagen confirma que el proceso de habilitación de SAML SSO se inicia en todos los servidores.

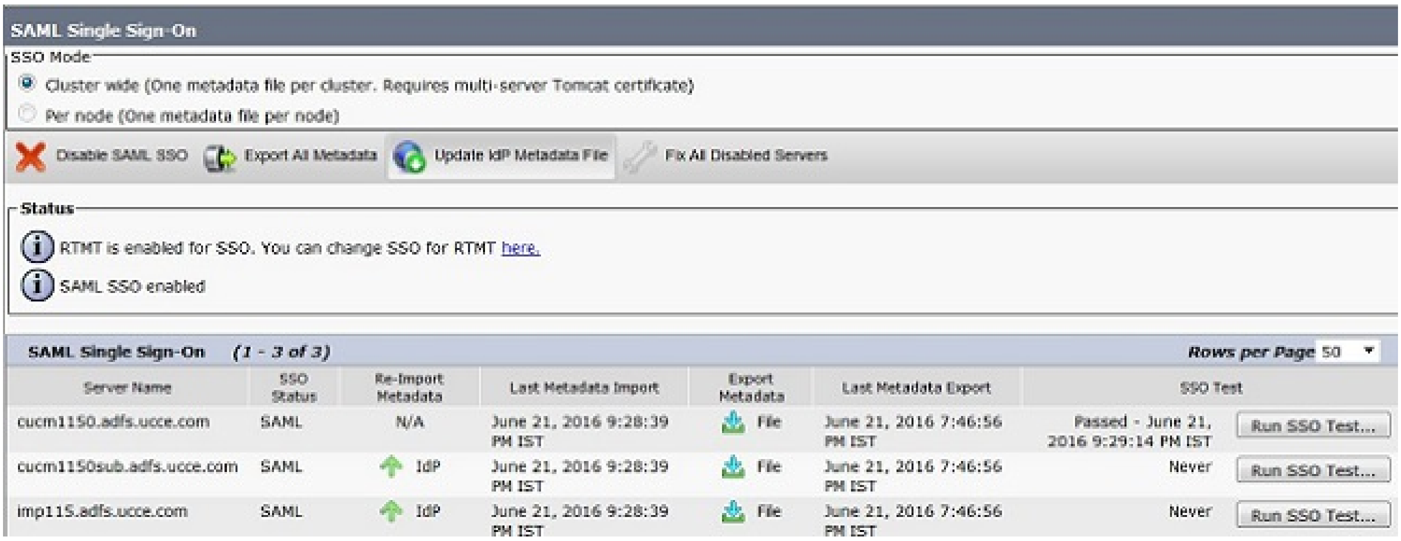


SAML Single Sign-On Configuration

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.

Cierre la sesión y vuelva a iniciarla en CUCM mediante las credenciales SAML SSO. Vaya a **System >SAML Single Sign On**. Haga clic en **Ejecutar prueba SSO** para otros nodos del clúster, como se muestra en la imagen:



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

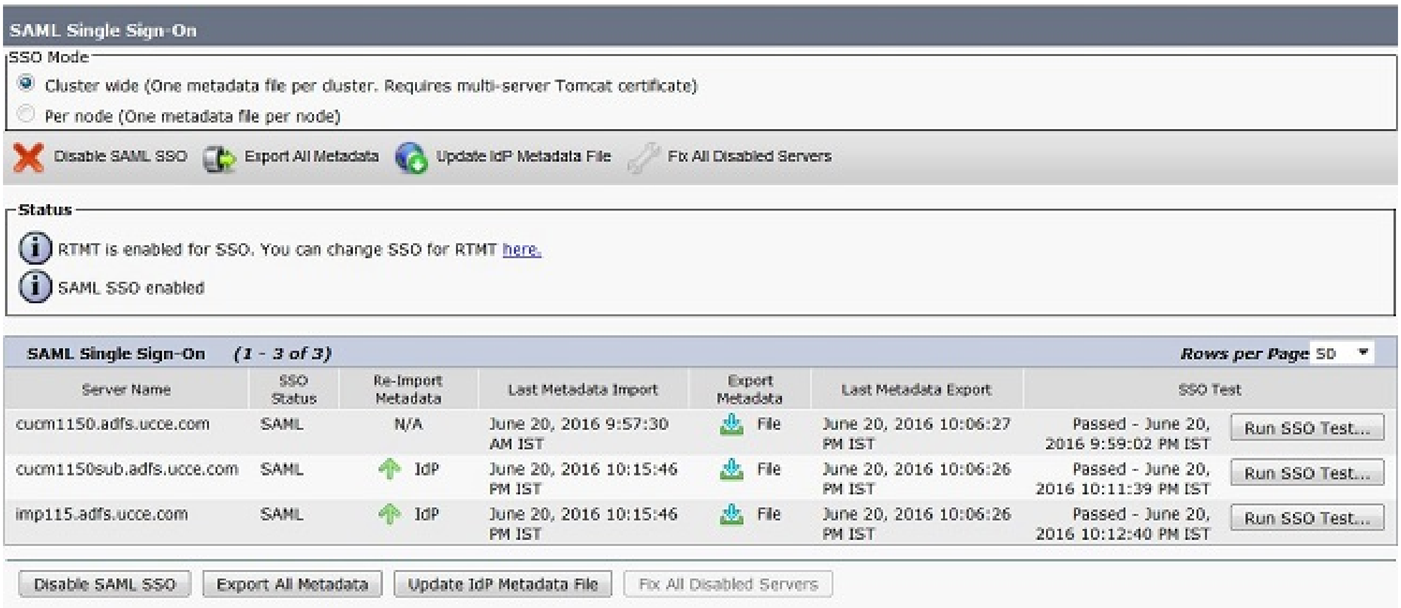
SAML Single Sign-On (1 - 3 of 3) Rows per Page 50

Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
cucm1150.adfs.ucce.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
cucm1150sub.adfs.ucce.com	SAML	IdP	June 21, 2016 9:28:39 PM IST	File	June 21, 2016 7:46:56 PM IST	Never
imp115.adfs.ucce.com	SAML	IdP	June 21, 2016 9:28:39 PM IST	File	June 21, 2016 7:46:56 PM IST	Never

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Confirme que la prueba SSO se realiza correctamente para los nodos que están habilitados para SAML SSO. Vaya a **System >SAML Single Sign On**. Las pruebas SSO exitosas muestran el estado Pasado.



SSO Mode

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

○ Per node (One metadata file per node)

Status

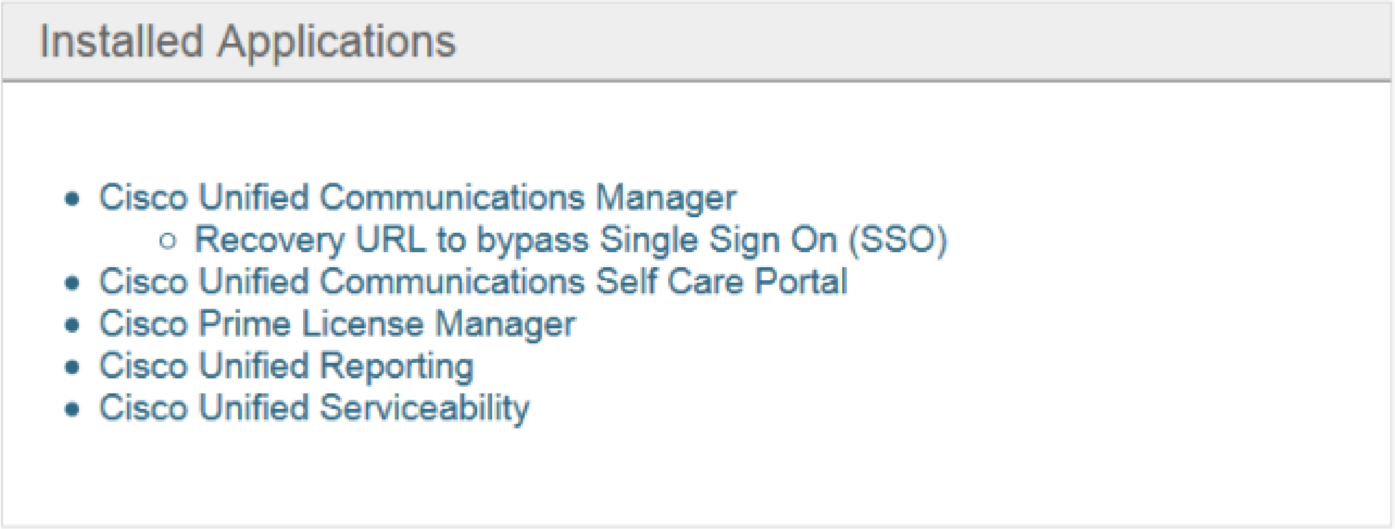
RTMT is enabled for SSO. You can change SSO for RTMT here.

SAML SSO enabled

SAML Single Sign-On (1 - 3 of 3) Rows per Page 50

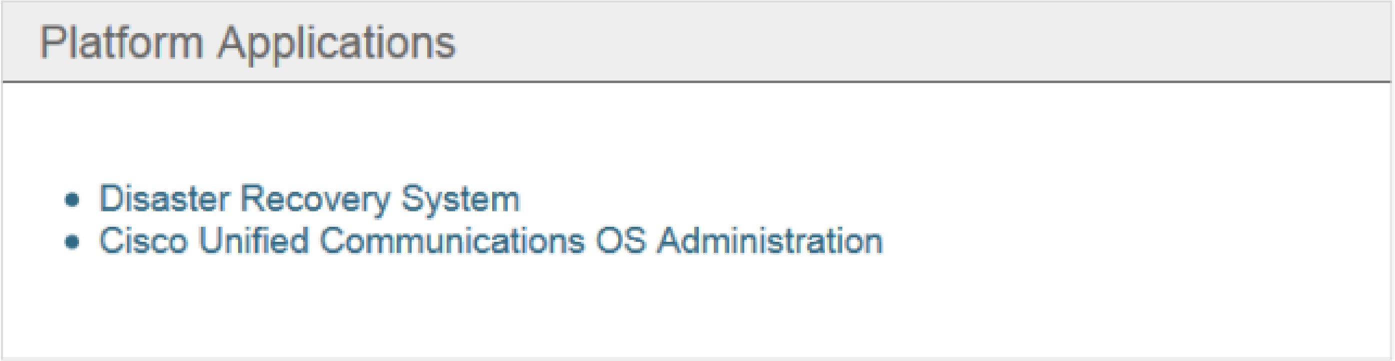
Server Name	SSO Status	Re-Import Metadata	Last Metadata Import	Export Metadata	Last Metadata Export	SSO Test
cucm1150.adfs.ucce.com	SAML	N/A	June 20, 2016 9:57:30 AM IST	File	June 20, 2016 10:06:27 PM IST	Passed - June 20, 2016 9:59:02 PM IST
cucm1150sub.adfs.ucce.com	SAML	IdP	June 20, 2016 10:15:46 PM IST	File	June 20, 2016 10:06:26 PM IST	Passed - June 20, 2016 10:11:39 PM IST
imp115.adfs.ucce.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

Una vez que se activa SAML SSO, se muestran las aplicaciones instaladas y las aplicaciones de plataforma para la página de inicio de sesión de CUCM, como se muestra en esta imagen.



Installed Applications

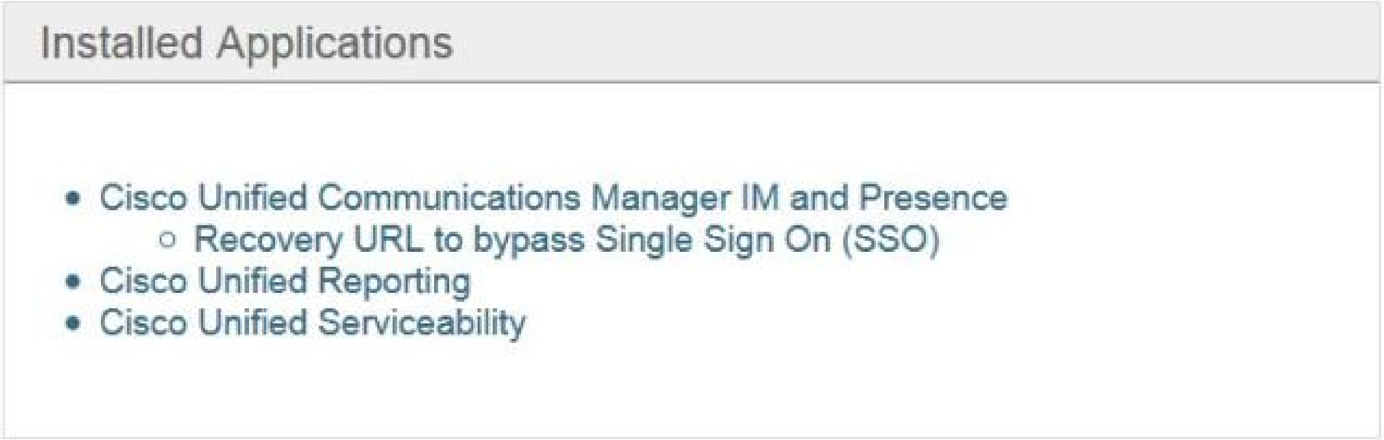
- Cisco Unified Communications Manager
  - Recovery URL to bypass Single Sign On (SSO)
- Cisco Unified Communications Self Care Portal
- Cisco Prime License Manager
- Cisco Unified Reporting
- Cisco Unified Serviceability



Platform Applications

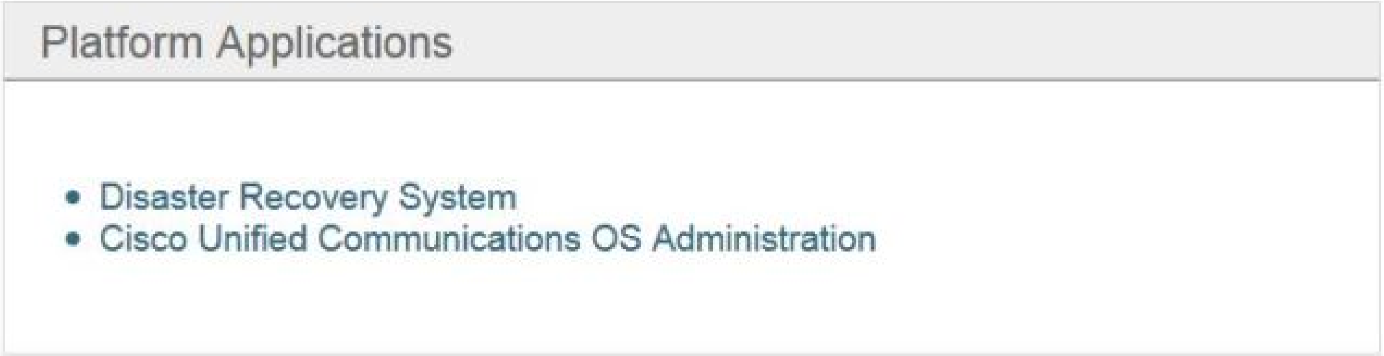
- Disaster Recovery System
- Cisco Unified Communications OS Administration

Una vez que se activa SAML SSO, se muestran las aplicaciones instaladas y las aplicaciones de plataforma para la página de inicio de sesión de IM and Presence, como se muestra en esta imagen:



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

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Para configurar los registros de SSO en debug, use el comando **set samltrace level DEBUG**

Recopile los registros de SSO usando RTMT o desde la ubicación **activa/tomcat/logs/ssosp/log4j/*.log** usando CLI.

Ejemplo de registros SSO muestra los metadatos generados y enviados a otros nodos

```
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
```