

Ejemplo de Configuración de AD FS Versión 2.0 para SSO de SAML

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Descargar metadatos del proveedor de identidad \(IdP\) de AD FS versión 2.0](#)

[Descargar metadatos de Collaboration Server \(SP\)](#)

[CUCM IM and Presence Service](#)

[Unity Connection](#)

[Aprovisionamiento de Cisco Prime Collaboration](#)

[Agregar CUCM como confianza de usuario de confianza](#)

[Adición de CUCM IM y Presence como confianza de usuario de confianza](#)

[AddUCXN como confianza de usuario de confianza](#)

[Adición de Cisco Prime Collaboration Provisioning como elemento de confianza del usuario de confianza](#)

[Verificación](#)

[Troubleshoot](#)


Introducción

Este documento describe cómo configurar el servicio de federación de Active Directory (AD FS) versión 2.0 para habilitar el inicio de sesión único (SSO) del lenguaje de marcado de aserción de seguridad (SAML) para productos de Cisco Collaboration como Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (UCXN), CUCM IM and Presence y Cisco Prime Collaboration.

Prerequisites

Requirements

AD FS versión 2.0 debe estar instalado y probado.

 Precaución: esta guía de instalación se basa en una configuración de laboratorio y se supone que la versión 2.0 de AD FS se utiliza solo para SSO SAML con productos de Cisco Collaboration. En caso de que otras aplicaciones vitales para la empresa lo utilicen, la personalización necesaria debe realizarse según la documentación oficial de Microsoft.

Componentes Utilizados

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

- AD FS versión 2.0
- Microsoft Internet Explorer 10
- CUCM versión 10.5
- Cisco IM and Presence Server versión 10.5
- UCXN versión 10.5
- Cisco Prime Collaboration Provisioning 10.5

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Configurar

Descargar metadatos del proveedor de identidad (IdP) de AD FS versión 2.0

Para descargar metadatos IdP, ejecute este enlace en su navegador: <https://<FQDN of ADFS>/FederationMetadata/2007-06/FederationMetadata.xml>.

Descargar metadatos de Collaboration Server (SP)

CUCM IM and Presence Service

Abra un navegador web, inicie sesión en CUCM como administrador y navegue hasta Sistema > Inicio de sesión único SAML.

Unity Connection

Abra un navegador web, inicie sesión en UCXN como administrador y navegue hasta Configuración del sistema > Inicio de sesión único SAML.

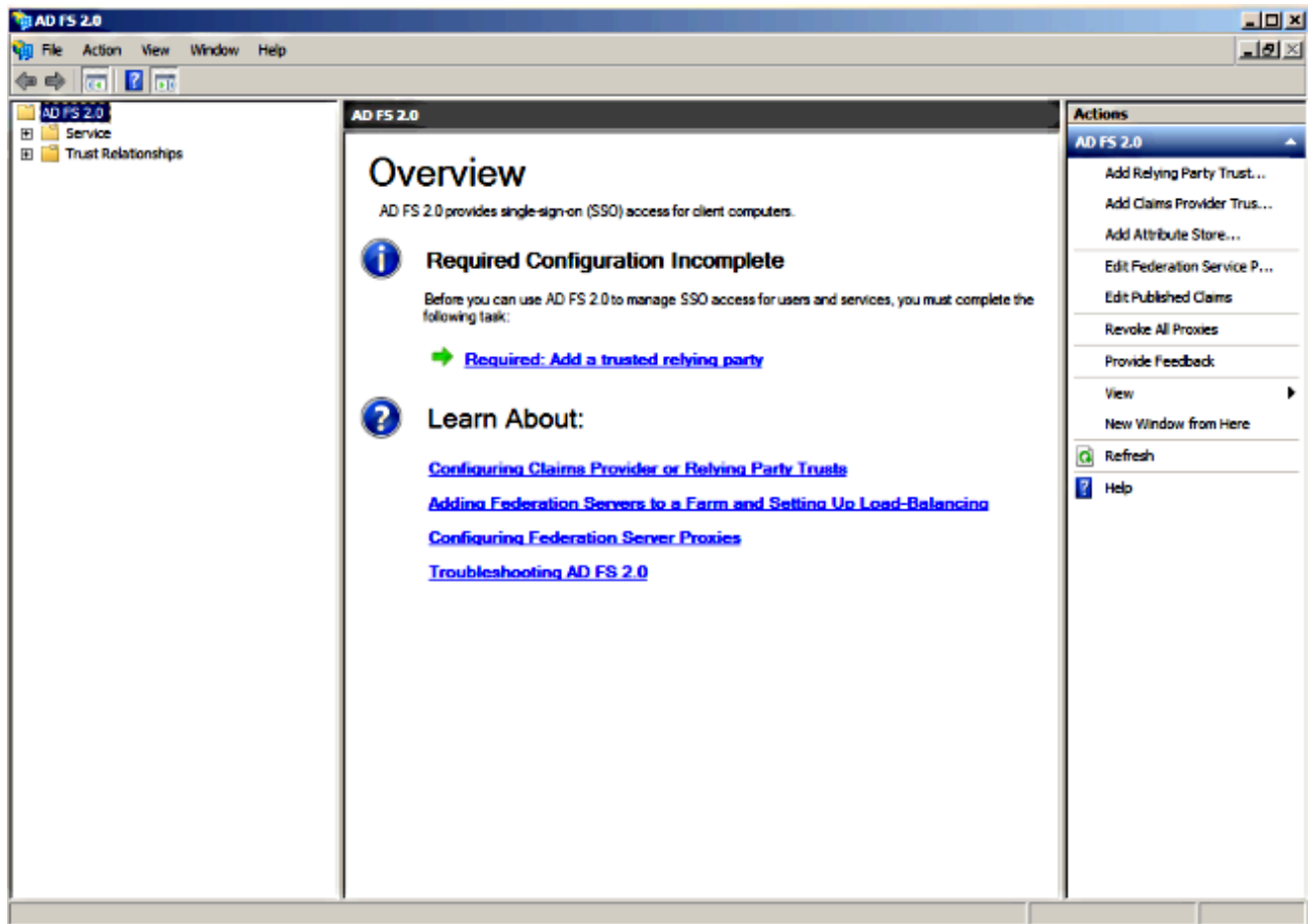
Aprovisionamiento de Cisco Prime Collaboration

Abra un navegador web, inicie sesión en Prime Collaboration Assurance como globaladmin y vaya a Administration > System Setup > Single Sign On.

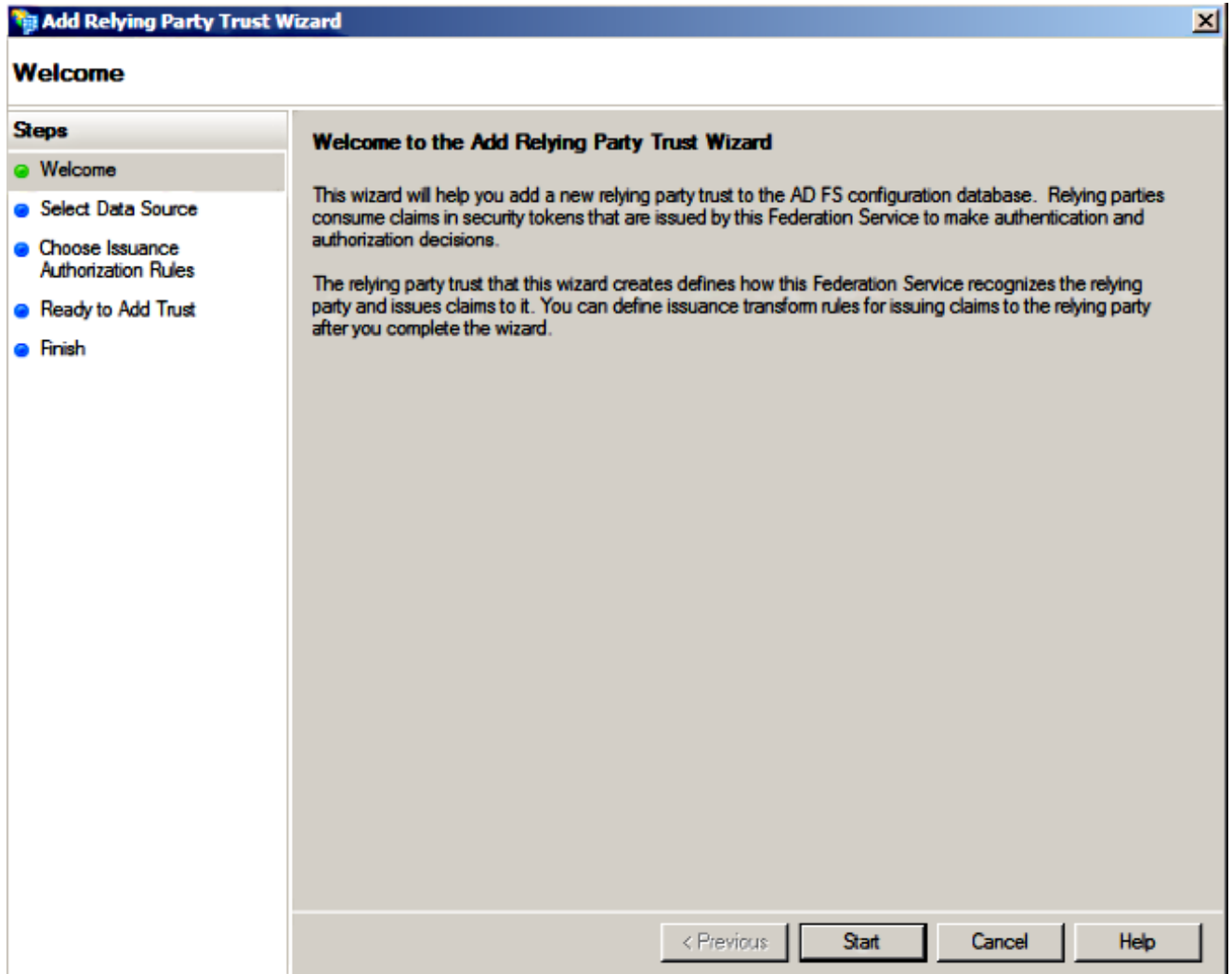
Agregar CUCM como confianza de usuario de confianza

1. Inicie sesión en el servidor de AD FS e inicie la versión 2.0 de AD FS desde el menú Programas de Microsoft Windows.

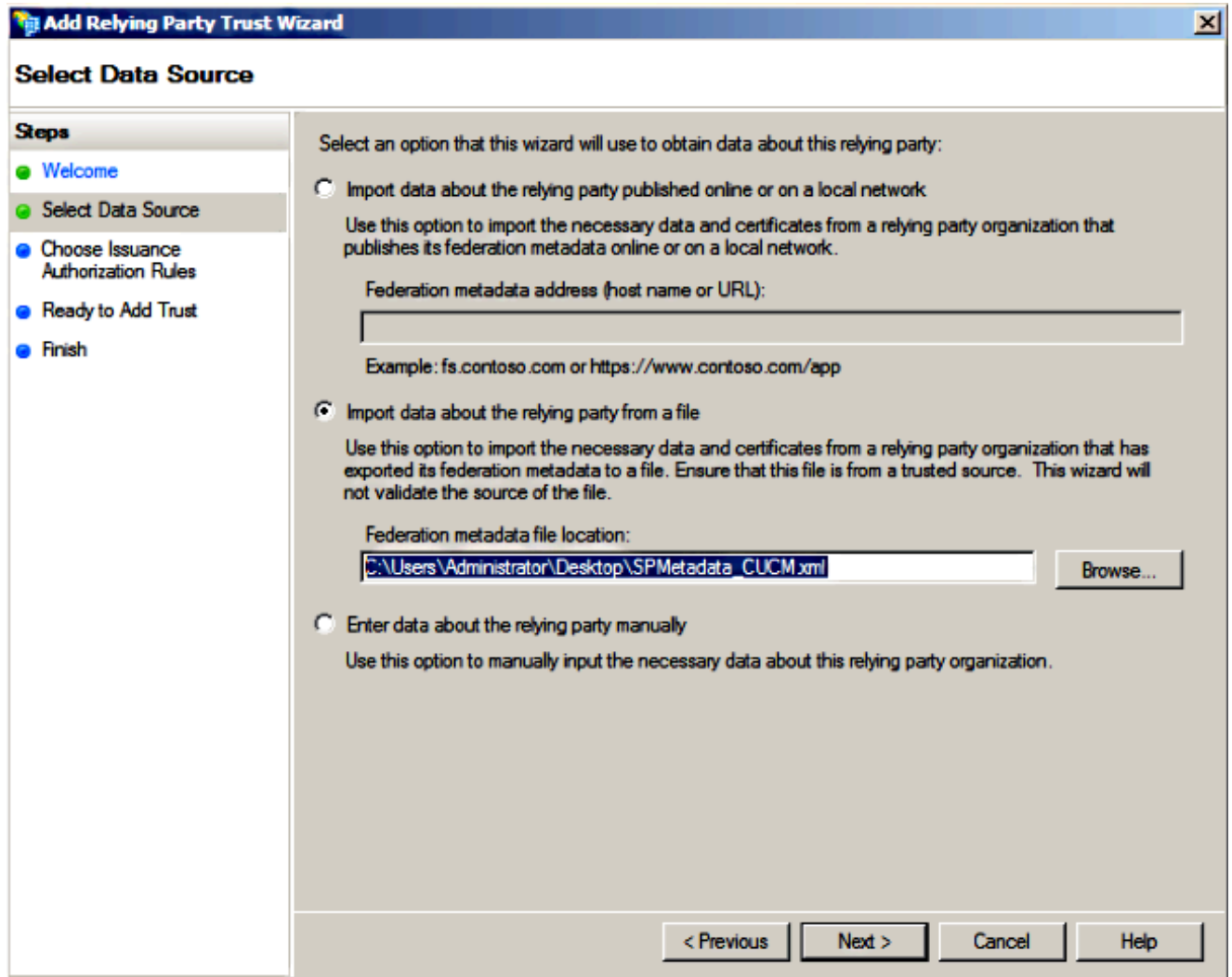
2. Seleccione Agregar confianza de usuario de confianza.



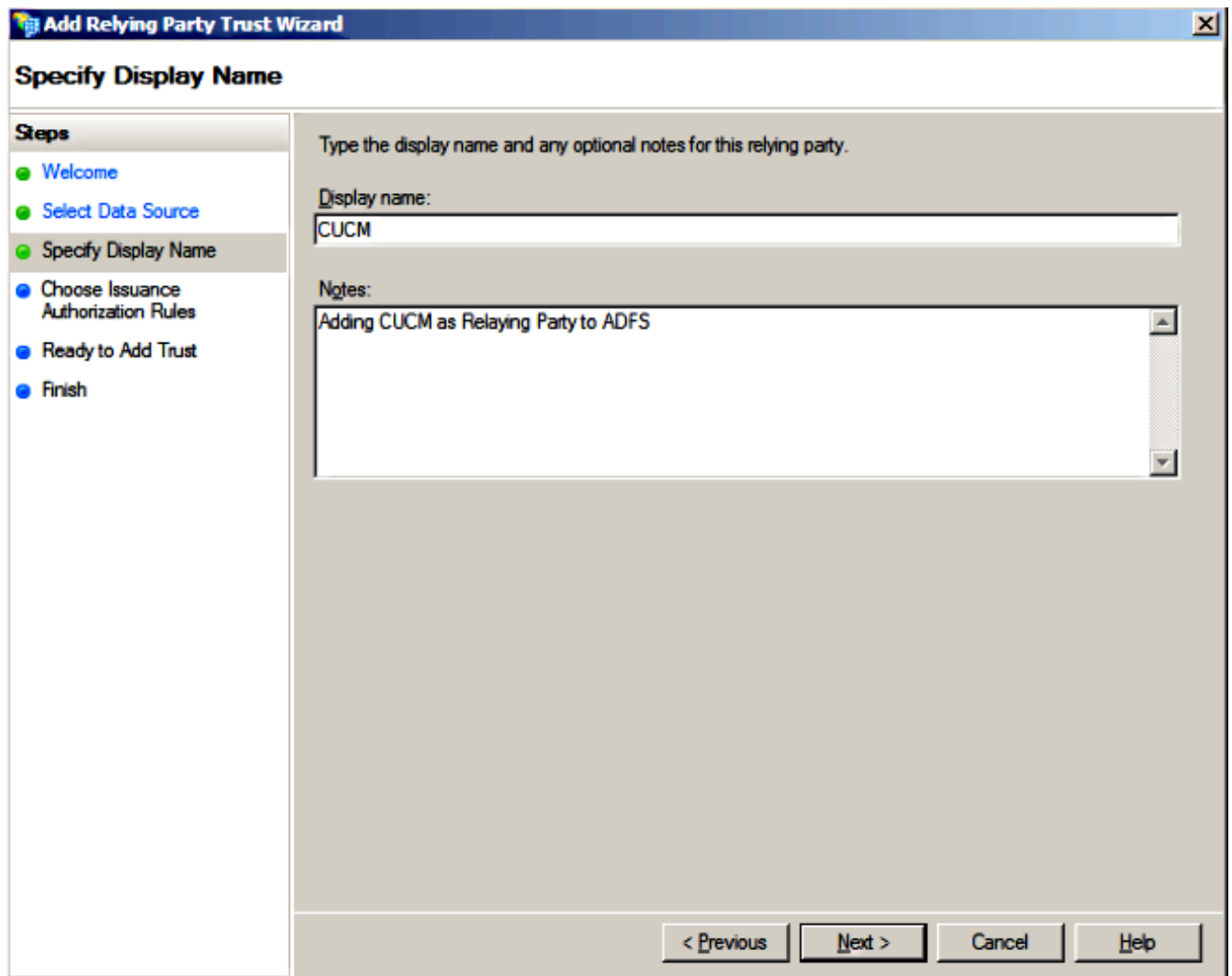
3. Haga clic en Start (Inicio).



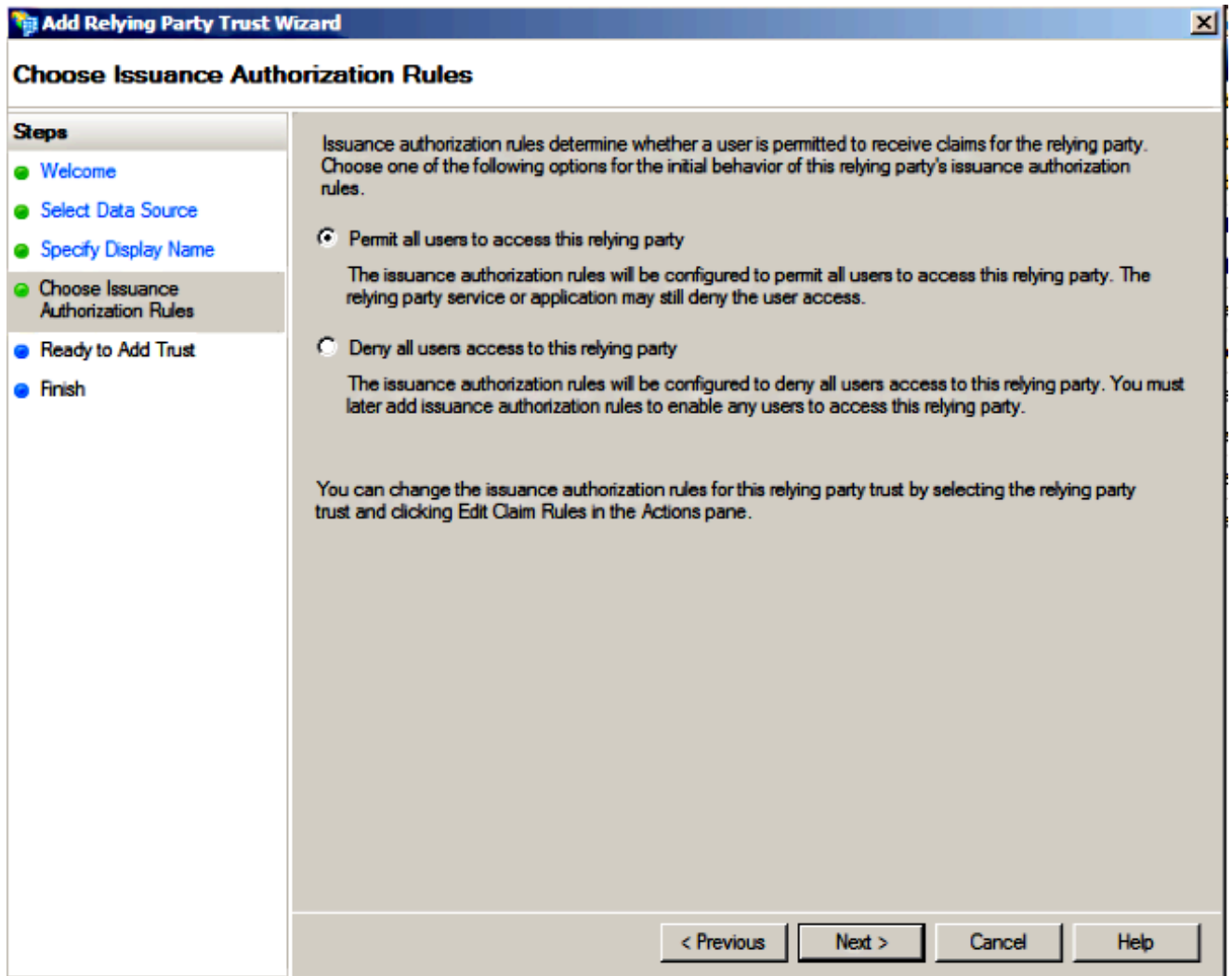
4. Seleccione la opción Importar datos sobre el usuario de confianza desde un archivo, elija el archivo de metadatos SPMetadata_CUCM.xml que descargó de CUCM anteriormente y haga clic en Siguiente.



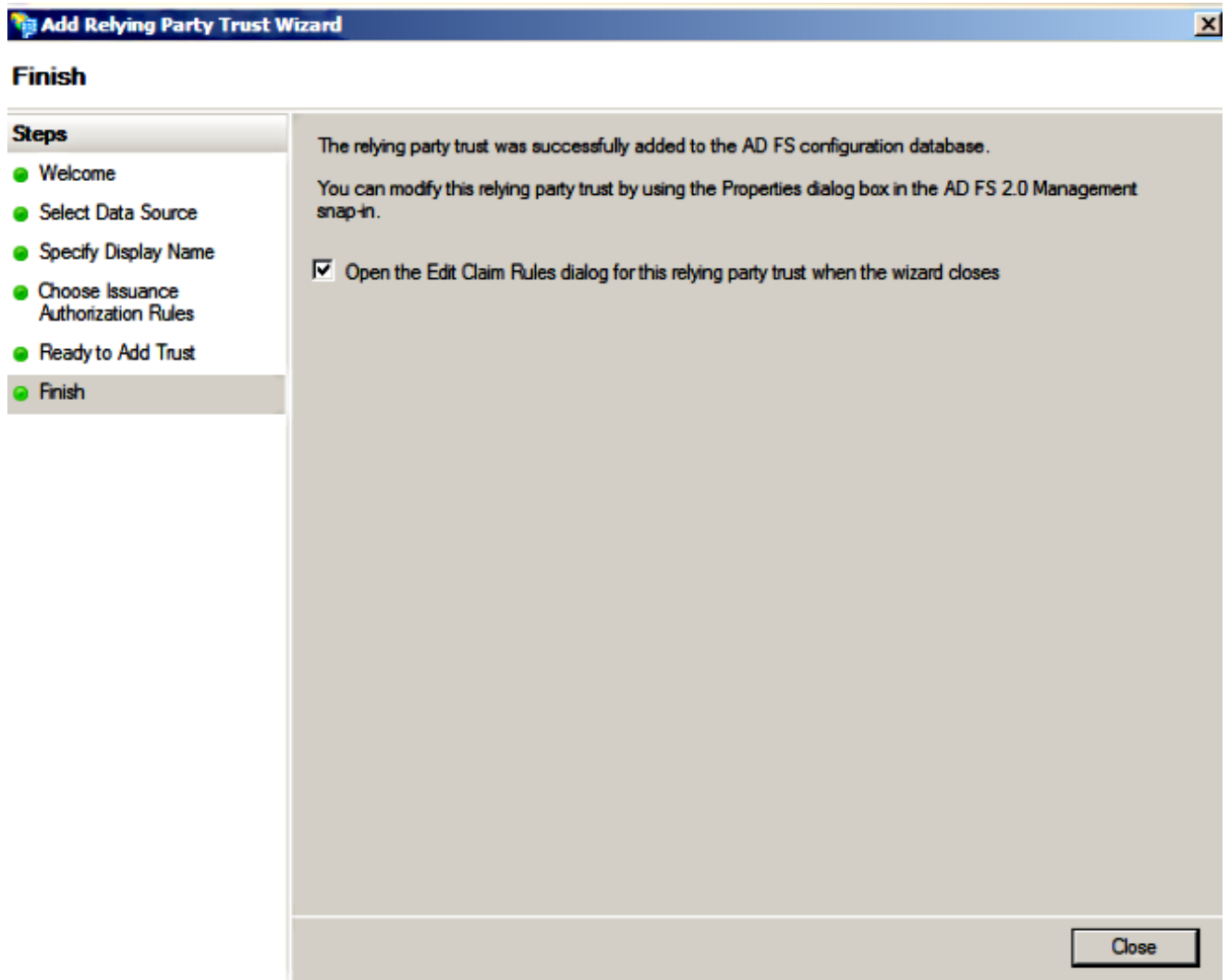
5. Ingrese Display name y haga clic en Next.



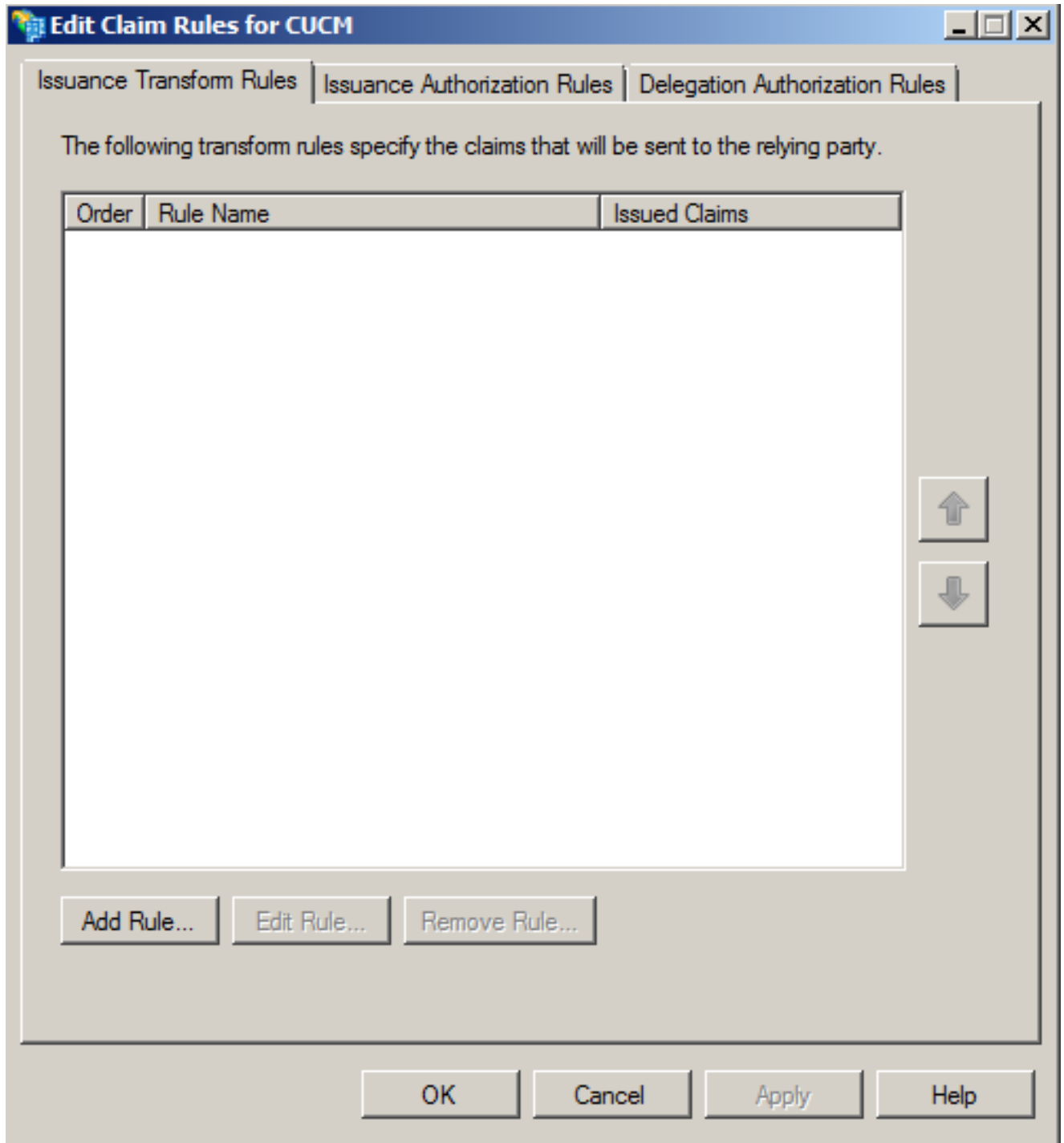
6. Elija Permitir a todos los usuarios acceder a este usuario de confianza y haga clic en Siguiente.



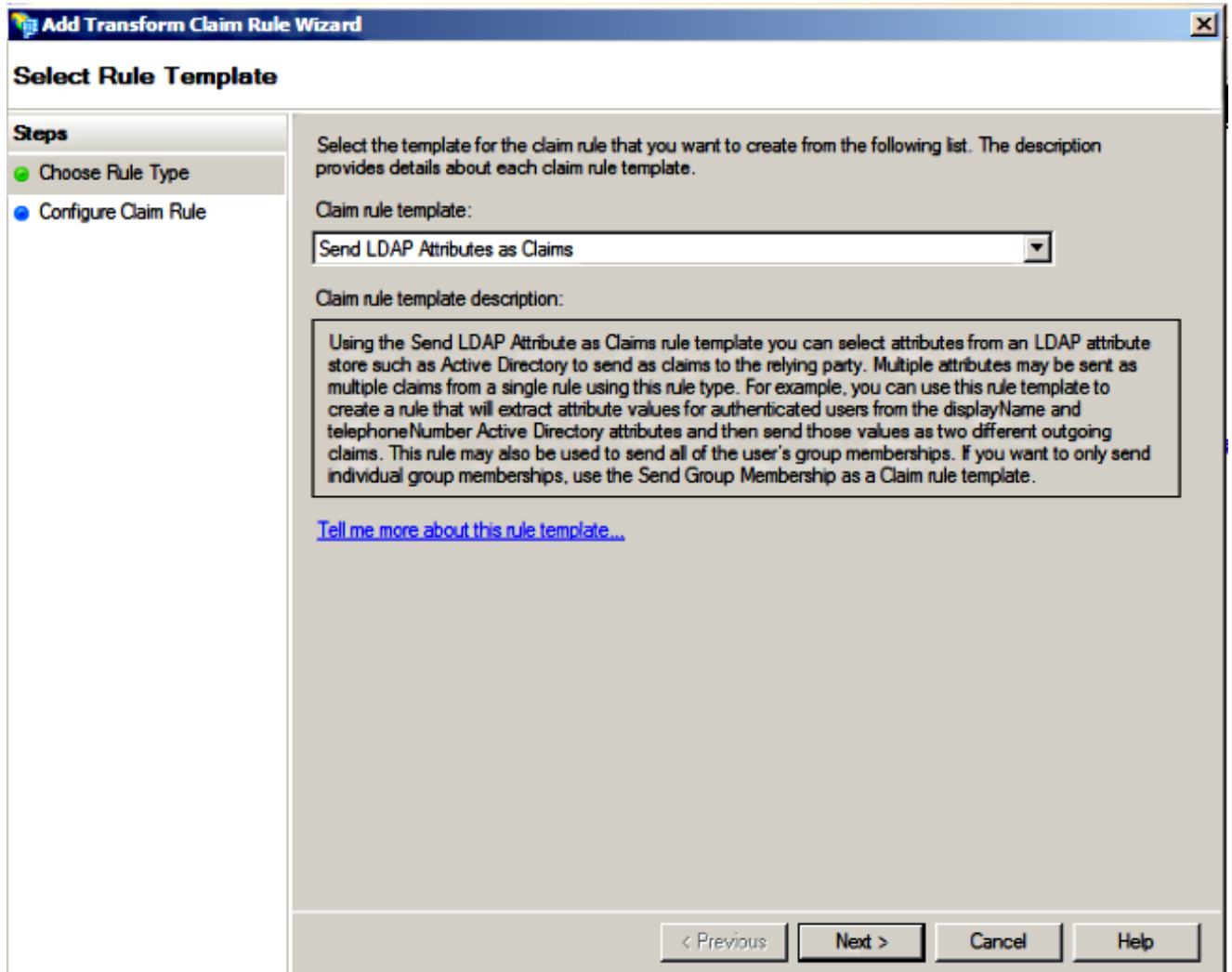
7. Seleccione Abrir el cuadro de diálogo Editar reglas de reclamación para la confianza del usuario de confianza cuando se cierre el asistente y haga clic en Cerrar.



8. Haga clic en Agregar regla.



9. Haga clic en Siguiete con la plantilla de regla de reclamación predeterminada establecida para Enviar atributos LDAP como reclamaciones.



10. En Configurar regla, ingrese el nombre de la regla de reclamación, seleccione Active Directory como el almacén de atributos, configure Atributo LDAP y el Tipo de reclamación saliente como se muestra en esta imagen, y haga clic en Finalizar.



Nota:

- El atributo del protocolo ligero de acceso a directorios (LDAP) debe coincidir con el atributo de sincronización de directorios en CUCM.
- "uid" debe estar en minúsculas.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim 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:
Name ID

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
*		

< Previous Finish Cancel Help

11. Haga clic en Agregar regla, seleccione Enviar reclamaciones usando una regla personalizada como plantilla de regla de reclamación y haga clic en Siguiente.

Edit Claim Rules for CUCM

Issuance Transform Rules | Issuance Authorization Rules | Delegation Authorization Rules

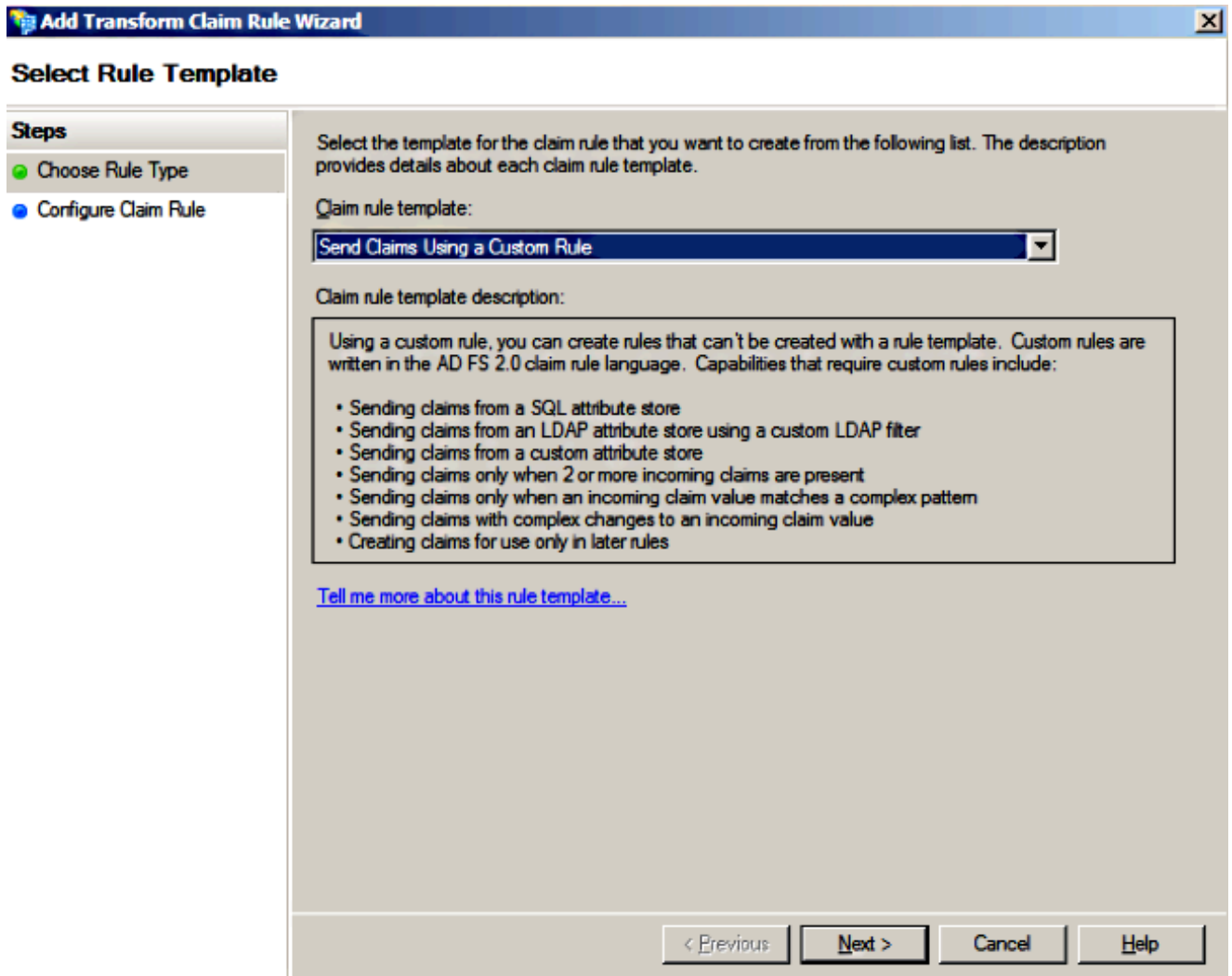
The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Name ID	uid



Add Rule... Edit Rule... Remove Rule...

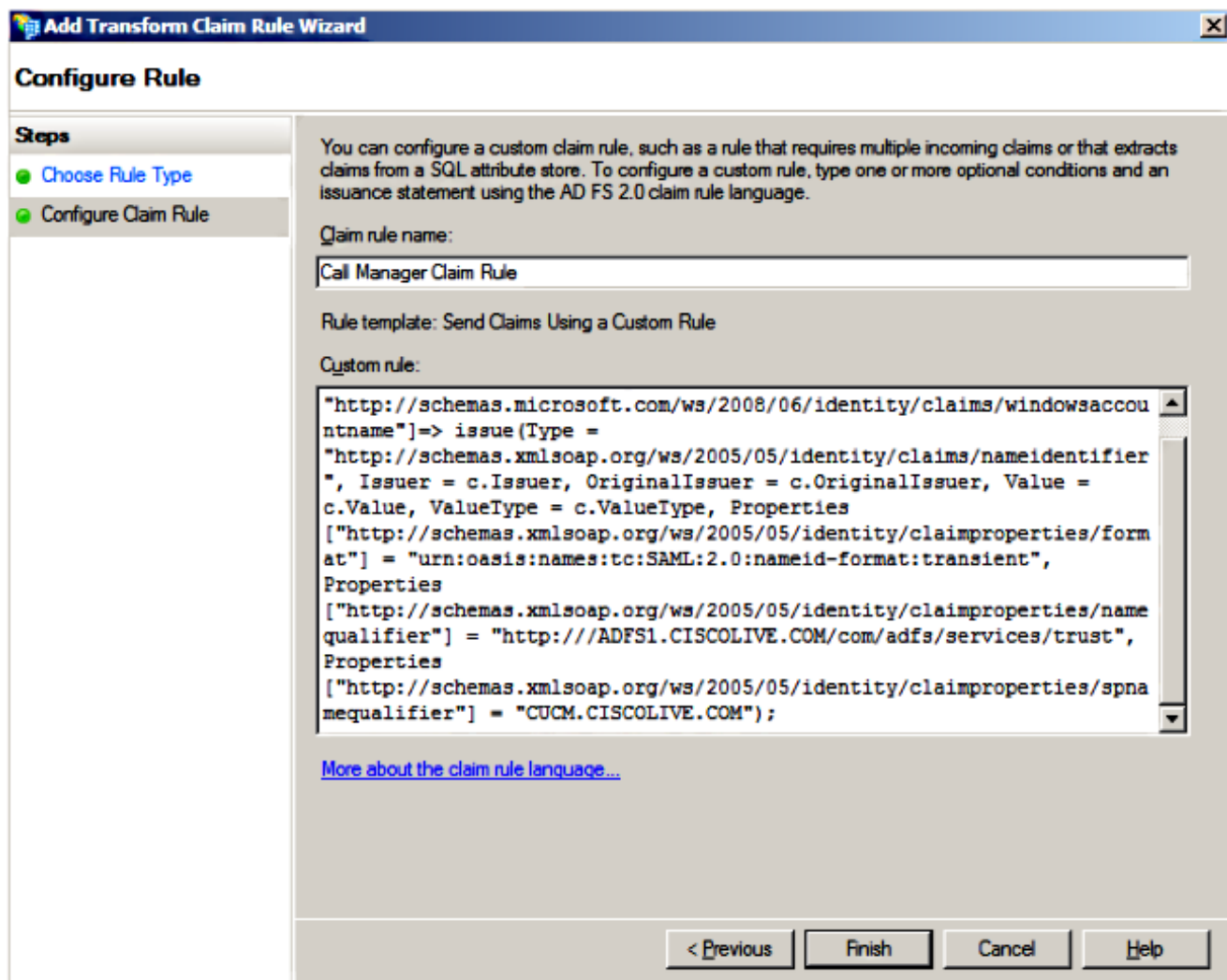
OK Cancel Apply Help



12. Introduzca un nombre para el nombre de la regla de reclamación y copie esta sintaxis en el espacio proporcionado en Regla personalizada:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=> issue(T
```

(NOTA: Si copia y pega el texto de estos ejemplos, tenga en cuenta que algún software de procesamiento de texto sustituirá las comillas ASCII (") por las versiones UNICODE ("). Las versiones UNICODE provocarán un error en la regla de notificación.)



Nota:

- El nombre de dominio completo (FQDN) de CUCM y ADFS se rellena automáticamente con el laboratorio CUCM y AD FS en este ejemplo y se debe modificar para que coincida con su entorno.
- El FQDN de CUCM/ADFS distingue entre mayúsculas y minúsculas y debe coincidir con los archivos de metadatos.

13. Haga clic en Finish (Finalizar).

14. Haga clic en Aplicar y luego en Aceptar.

15. Reinicie el servicio AD FS versión 2.0 desde Services.msc.

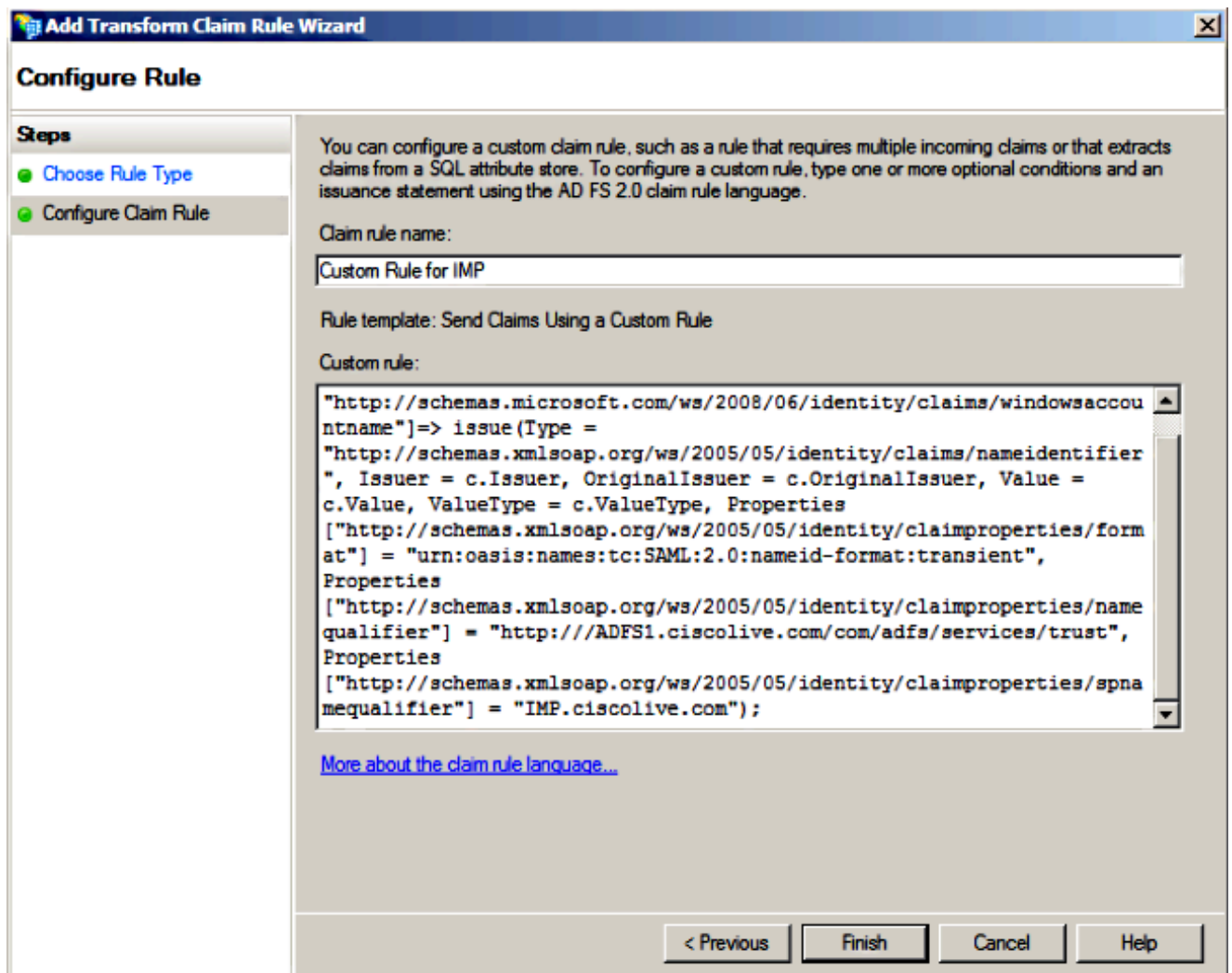
Adición de CUCM IM y Presence como confianza de usuario de confianza

1. Repita los pasos del 1 al 11 tal y como se describe en Agregar CUCM como confianza de

usuario de confianza y vaya al paso 2.

2. Introduzca un nombre para el nombre de la regla de reclamación y copie esta sintaxis en el espacio proporcionado en Regla personalizada:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=> issue(T
```



Observe que el FQDN de IM and Presence y AD FS se rellena automáticamente con el laboratorio de IM and Presence y AD FS en este ejemplo y se debe modificar para que coincida con su entorno.

3. Haga clic en Finish (Finalizar).

4. Haga clic en Aplicar y luego en Aceptar.

5. Reinicie el servicio AD FS versión 2.0 desde Services.msc.

Agregar UCXN como confianza de usuario de confianza

1. Repita los pasos del 1 al 12 tal y como se describe en Agregar CUCM como confianza de usuario de confianza y vaya al paso 2.

2. Introduzca un nombre para el nombre de la regla de reclamación y copie esta sintaxis en el espacio proporcionado en Regla personalizada:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=> issue(T
```

The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box, specifically the 'Configure Rule' step. The window title is 'Add Transform Claim Rule Wizard'. The 'Steps' pane on the left shows 'Choose Rule Type' and 'Configure Claim Rule', with 'Configure Claim Rule' selected. 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:

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://ADFS1.ciscolive.com/com/adfs/services/trust",  
Properties  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "UCXN1.ciscolive.com");
```

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

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

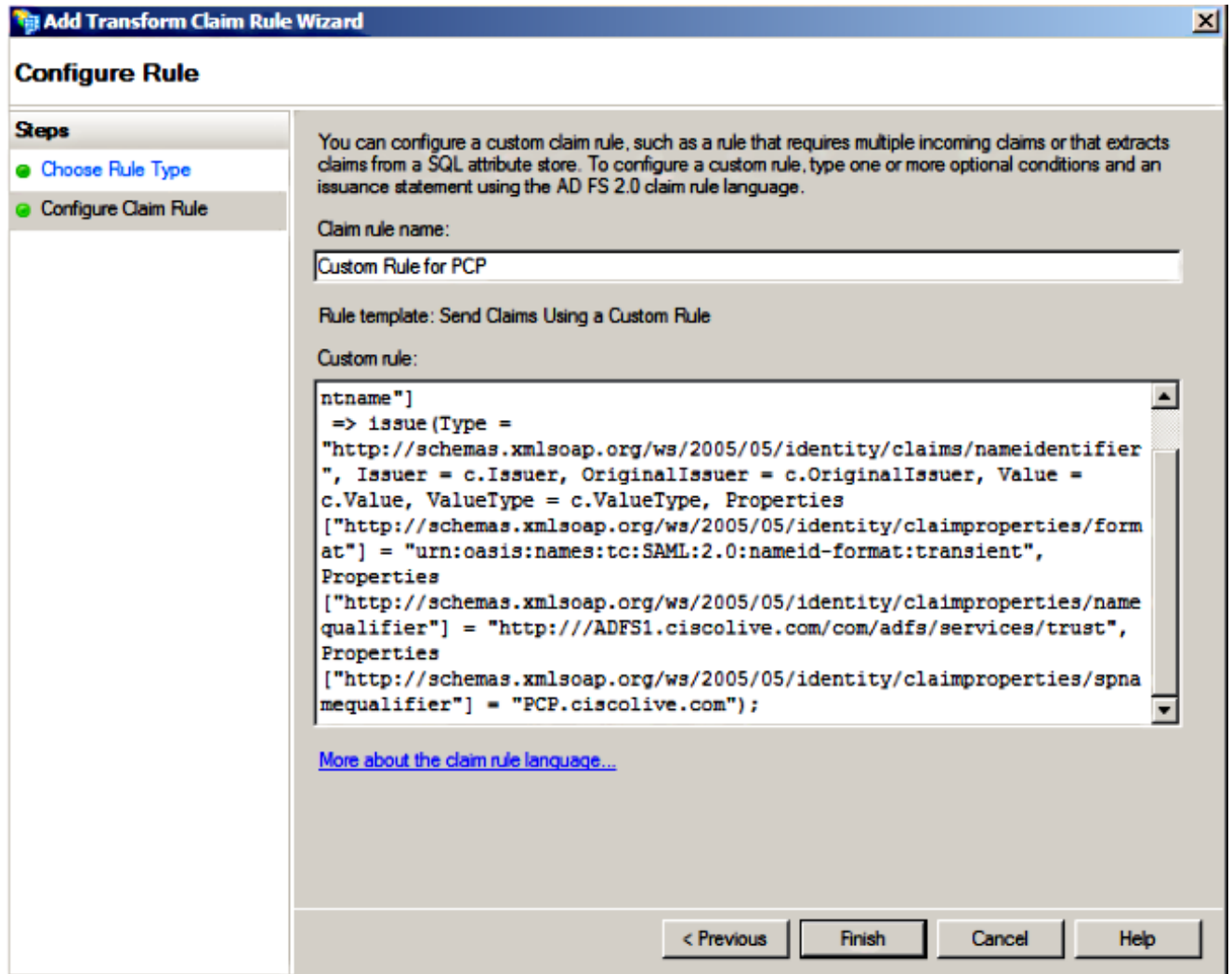
Observe que el FQDN de UCXN y AD FS se rellena automáticamente con el UCXN y ADFS de laboratorio en este ejemplo y se debe modificar para que coincida con su entorno.

3. Haga clic en Finish (Finalizar).
4. Haga clic en Aplicar y luego en Aceptar.
5. Reinicie el servicio AD FS versión 2.0 desde Services.msc.

Adición de Cisco Prime Collaboration Provisioning como elemento de confianza del usuario de confianza

1. Repita los pasos del 1 al 12 tal y como se describe en Agregar CUCM como confianza de usuario de confianza y vaya al paso 2.
2. Introduzca un nombre para el nombre de la regla de reclamación y copie esta sintaxis en el espacio proporcionado en Regla personalizada:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=> issue(T
```



Observe que el FQDN de Prime Provisioning y AD FS se rellena automáticamente con el aprovisionamiento de colaboración de Prime (PCP) y AD FS de este ejemplo y se debe modificar para que coincida con su entorno.

- Haga clic en Finish (Finalizar).
- Haga clic en Aplicar y luego en Aceptar.
- Reinicie el servicio AD FS versión 2.0 desde Services.msc.

Una vez configurada la versión 2.0 de AD FS, continúe para habilitar SSO de SAML en los productos de Cisco Collaboration.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

AD FS registra los datos de diagnóstico en el Registro de eventos del sistema. Desde el Administrador del servidor en el servidor AD FS, abra Diagnóstico -> Visor de eventos -> Aplicaciones y servicios -> AD FS 2.0 -> Administrador

Buscar errores registrados para actividad de AD FS

Server Manager (CUC-ADFS)

Admin Number of events: 211

Level	Date and Time	Source	Event ID	Task Category
Information	6/28/2016 11:18:12 AM	AD FS 2.0	337	None
Information	6/28/2016 11:18:12 AM	AD FS 2.0	336	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	390	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	386	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	399	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	157	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	156	None
Information	6/27/2016 11:18:02 PM	AD FS 2.0	337	None
Information	6/27/2016 11:18:02 PM	AD FS 2.0	336	None
Information	6/27/2016 8:12:59 PM	AD FS 2.0	388	None
Error	6/27/2016 8:12:11 PM	AD FS 2.0	364	None
Error	6/27/2016 8:12:11 PM	AD FS 2.0	321	None
Information	6/27/2016 8:12:10 PM	AD FS 2.0	251	None
Information	6/27/2016 8:11:59 PM	AD FS 2.0	100	None

Event 321, AD FS 2.0

General Details

The SAML authentication request had a NameID Policy that could not be satisfied.
Requestor: ciscouc-105-imps1.ciscouc.org
Name identifier format: urn:oasis:names:tc:SAML:2.0:nameid-format:transient

Log Name: AD FS 2.0/Admin
Source: AD FS 2.0 Logged: 6/27/2016 8:12:11 PM
Event ID: 321 Task Category: None

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).