Configuración del inicio de sesión único con CUCM y AD FS 2.0

Contenido

Introducción

Este documento describe cómo configurar el inicio de sesión único (SSO) en Cisco Unified Communications Manager y el servicio de federación de Active Directory.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Communications Manager (CUCM)
- Conocimientos básicos del servicio de federación de Active Directory (AD FS)

Para habilitar SSO en su entorno de laboratorio, necesita esta configuración:

- Windows Server con AD FS instalado.
- CUCM con sincronización LDAP configurada.
- Usuario final con el rol Superusuarios de CCM estándar seleccionado.

Componentes Utilizados

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

- Windows Server con AD FS 2.0
- CUCM 10.5.2

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). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Se proporciona el procedimiento para AD FS 2.0 con Windows Server 2008 R2. Estos pasos también funcionan para AD FS 3.0 en Windows Server 2016.

Descargar e instalar AD FS 2.0 en Windows Server

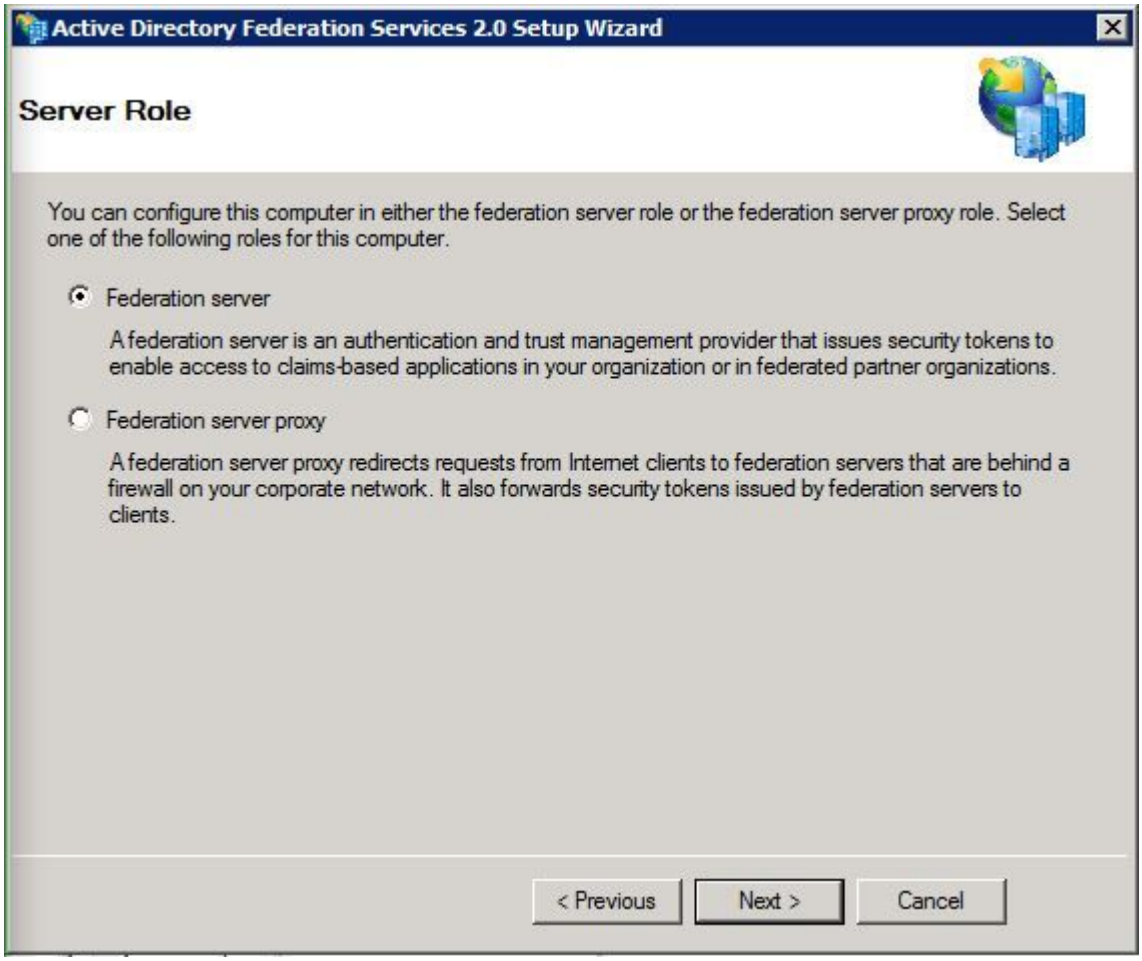
Paso 1. Vaya a Descargar AD FS 2.0.

Paso 2. Asegúrese de seleccionar la descarga adecuada en función de su servidor Windows.

Paso 3. **Mueva** el archivo descargado a su servidor Windows Server.

Paso 4. Continúe con la instalación:

Paso 5. Cuando se le solicite, elija **Servidor de federación**:



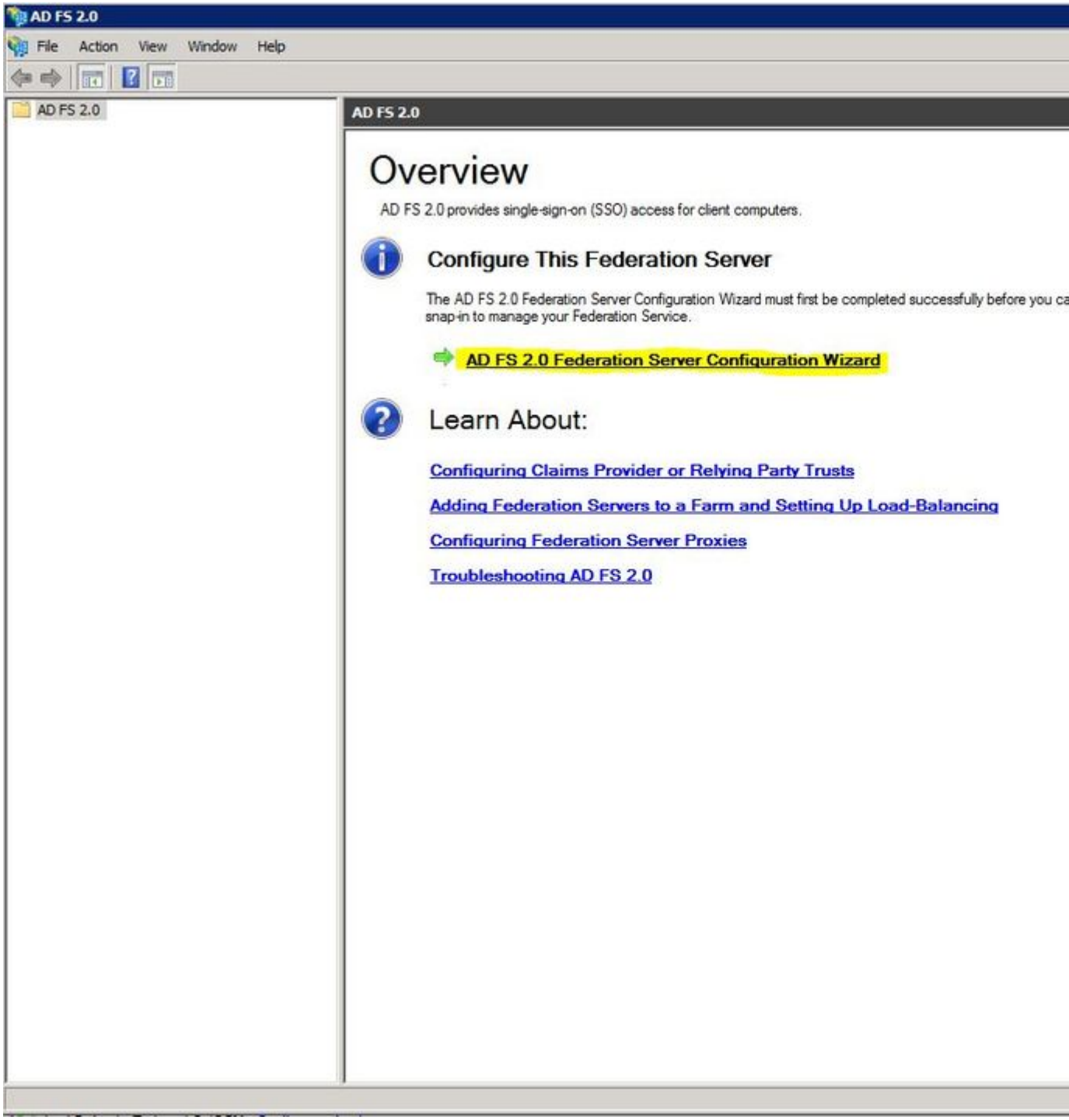
Paso 6. Algunas dependencias se instalan automáticamente; una vez hecho esto, haga clic en **Finish**.

Ahora que AD FS 2.0 está instalado en el servidor, debe agregar alguna configuración.

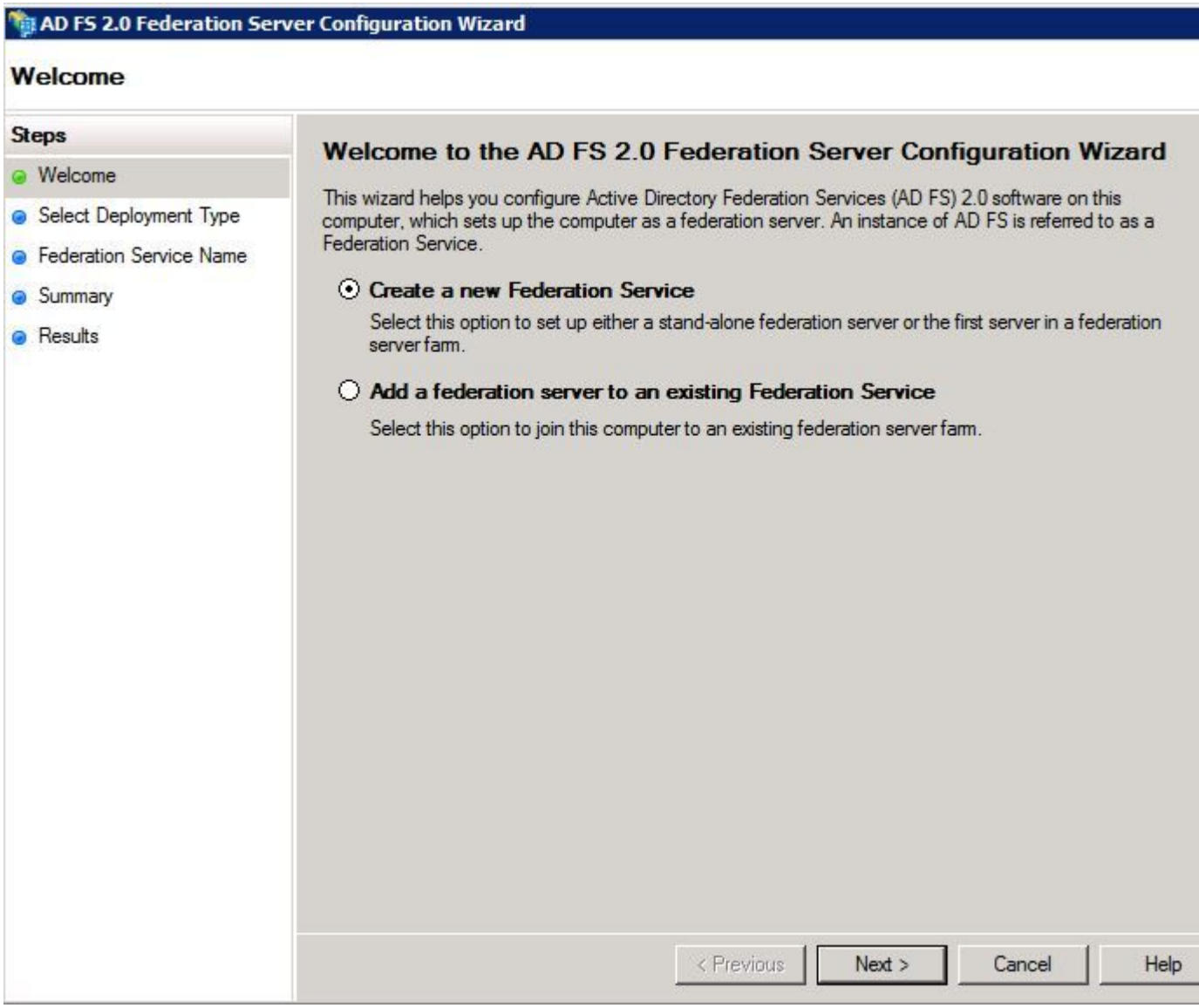
Configurar AD FS 2.0 en Windows Server

Paso 1. Si la ventana de AD FS 2.0 no se abrió automáticamente después de la instalación, puede hacer clic en **Inicio** y buscar Administración de AD FS 2.0 para abrirla manualmente.

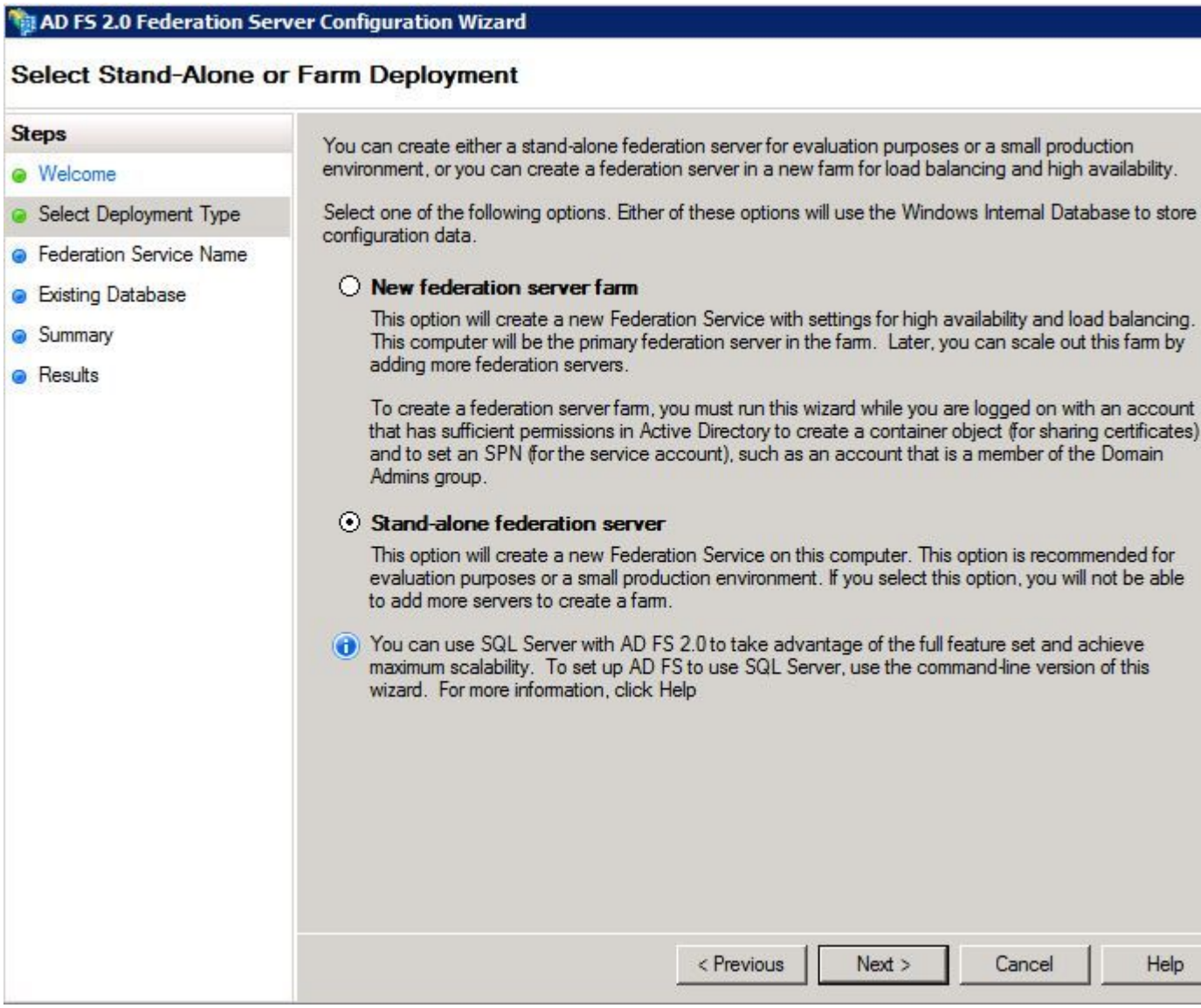
Paso 2. Elija **Asistente para la configuración del servidor de federación de AD FS 2.0**.



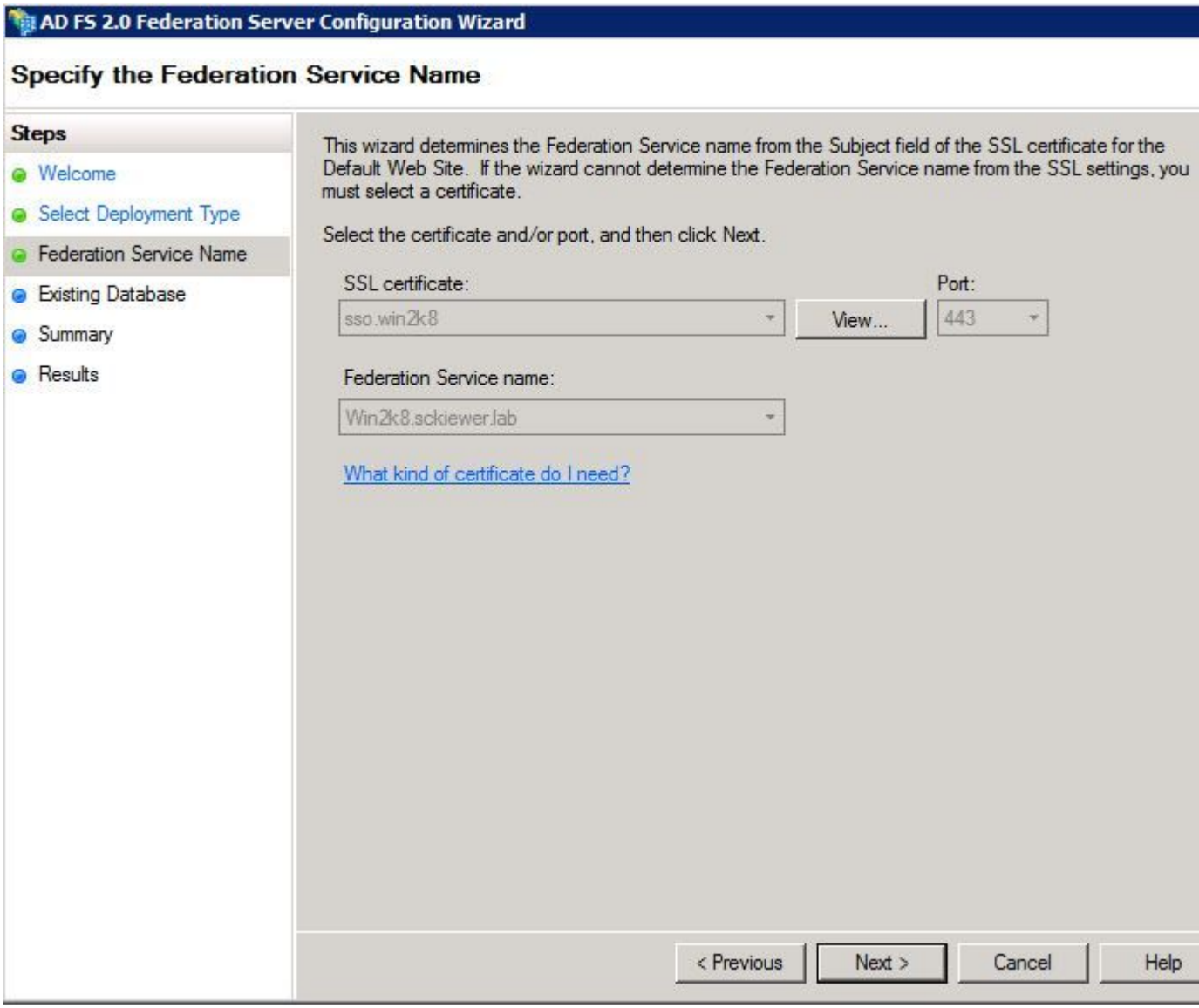
Paso 3. A continuación, haga clic en **Crear un nuevo Servicio de federación**.



Paso 4. Para la mayoría de los entornos, el **servidor de federación independiente** es suficiente.



Paso 5. A continuación, se le solicita que elija un certificado. Este campo se rellena automáticamente siempre que el servidor tenga un certificado.



Paso 6. Si ya tiene una base de datos de AD FS en el servidor, debe quitarla para continuar.

Paso 7. Por último, aparecerá una pantalla de resumen en la que puede hacer clic en **Next** (**Siguiente)**.

Importar los metadatos Idp a CUCM / Descargar los metadatos de CUCM

Paso 1. Actualice la dirección URL con el nombre de host o FQDN del servidor de Windows y descargue los metadatos del servidor de AD FS: https://hostname/federationmetadata/2007-06/federationmetadata.xml

Paso 2. Vaya a **Administración de Cisco Unified CM** > **Sistema** > **Inicio de sesión único SAML**.

Paso 3. Haga clic en **Enable SAML SSO**.

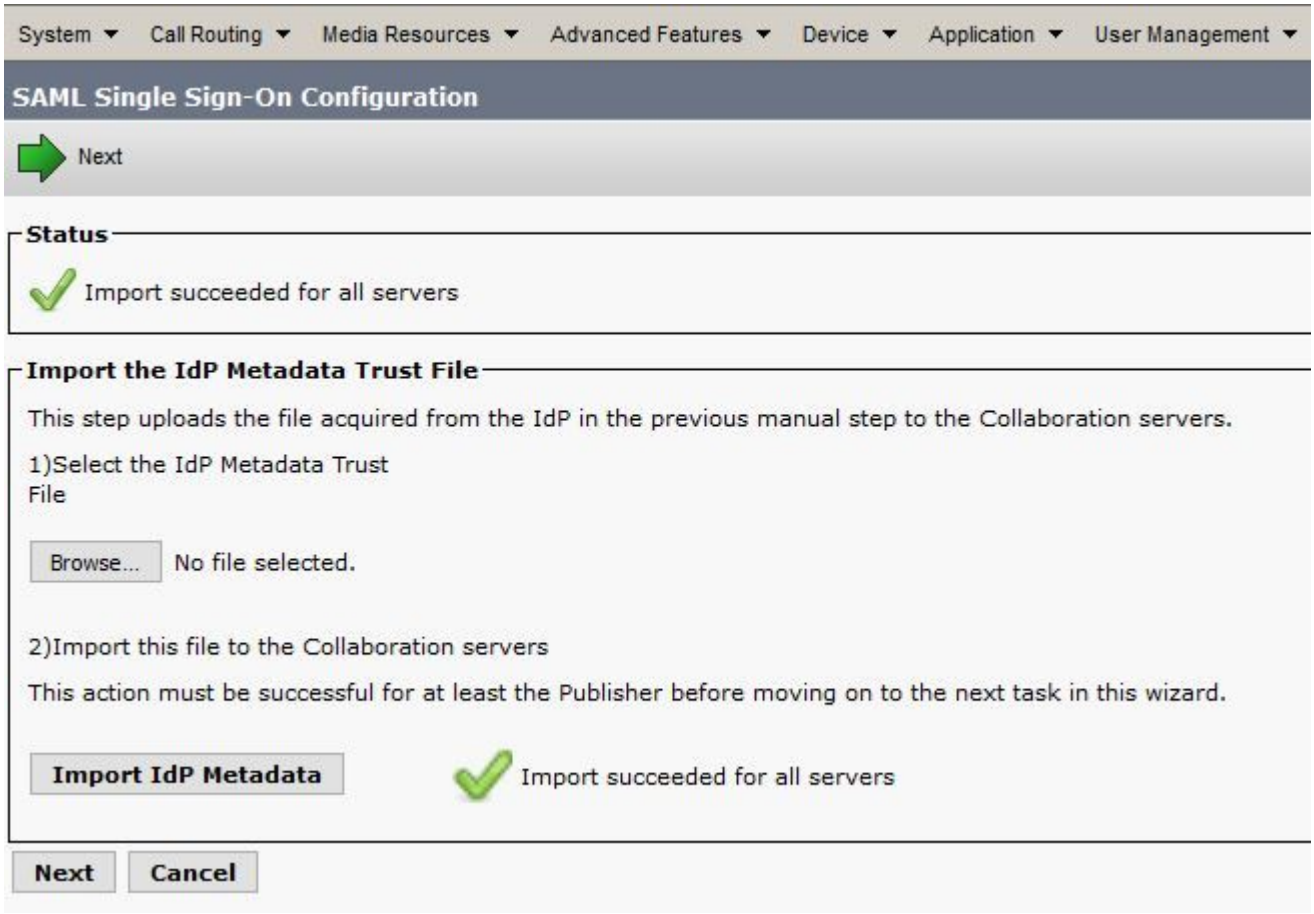
Paso 4. Si recibe una alerta acerca de Conexiones de servidor Web, haga clic en **Continuar**.

Paso 5. A continuación, CUCM le indica que descargue el archivo de metadatos de su IdP. En esta situación, el servidor de AD FS es el IdP y descargó los metadatos en el paso 1, así que haga clic en

Siguiente.

Paso 6. Haga clic en **Browse** > **Select the .xml from Step 1** > Click **Import IdP Metadata**.

Paso 7. Un mensaje indica que la importación se realizó correctamente:



Paso 8. Haga clic en Next (Siguiente).

Paso 9. Ahora que tiene los metadatos IdP importados en CUCM, necesita importar los metadatos de CUCM en su IdP.

Paso 10. Haga clic en **Descargar archivo de metadatos de confianza**.

Paso 11. Haga clic en Next (Siguiente).

Paso 12. Mueva el archivo .zip a su servidor de Windows y extraiga el contenido a una carpeta.

Importar metadatos de CUCM al servidor de AD FS 2.0 y crear reglas de reclamación

Paso 1. Haga clic en **Inicio** y busque **Administración de AD FS 2.0**.

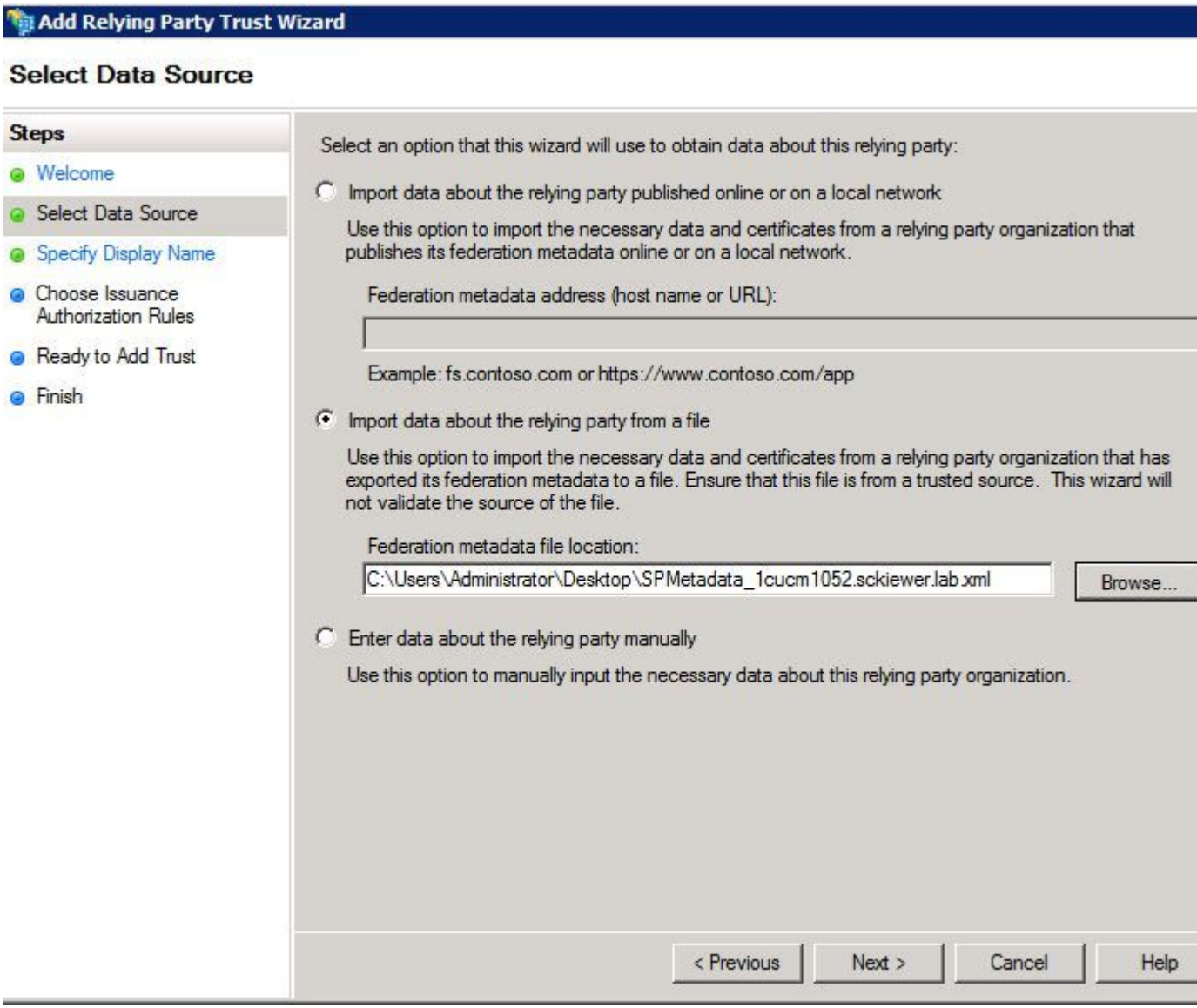
Paso 2. Haga clic en **Requerido: Agregar un usuario de confianza**.

Nota: Si no ve esta opción, debe cerrar la ventana y abrirla de nuevo.

Paso 3. Una vez que haya abierto el **Asistente para agregar usuario de confianza**, haga clic en **Inicio**.

Paso 4. Aquí debe importar los archivos XML extraídos en el paso 12. Seleccione **Importar datos sobre el usuario de confianza desde un archivo** y busque los archivos de carpeta y elija el XML para el editor.

Nota: Utilice los pasos anteriores para cualquier servidor de Unified Collaboration en el que desee utilizar SSO.



Paso 5. Haga clic en Next (Siguiente).

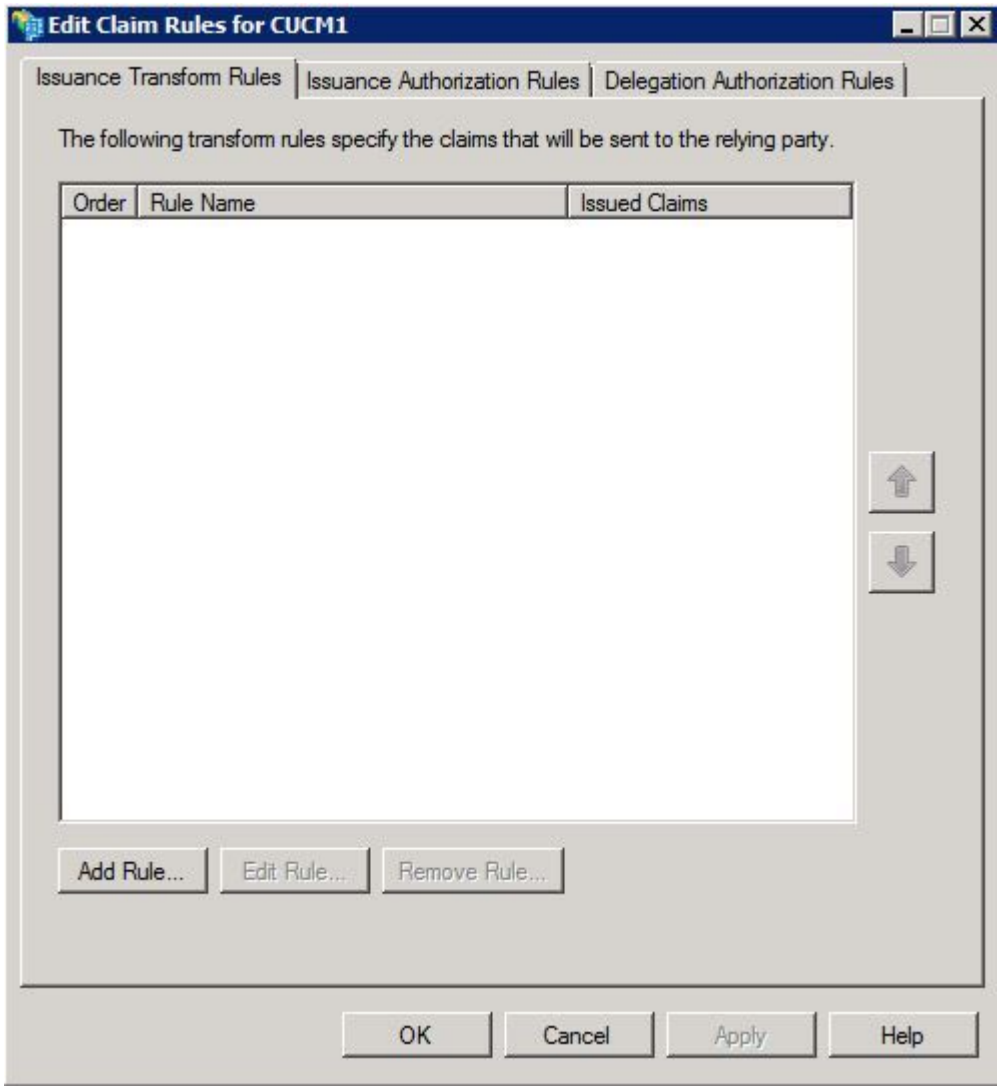
Paso 6. Edite **Display Name** y haga clic en **Next**.

Paso 7. Elija **Permitir a todos los usuarios acceder a este usuario de confianza** y haga clic en **Siguiente**.

Paso 8. Haga clic en **Next** nuevamente.

Paso 9. En esta pantalla, asegúrese de que la casilla de verificación **Abrir el cuadro de diálogo Editar reglas de reclamación para esta confianza de usuario de confianza cuando se cierre el asistente está** activada y, a continuación, haga clic en **Cerrar**.

Paso 10. Se abre la ventana Editar reglas de reclamación:



Paso 11. En esta ventana, haga clic en **Add** Rule.

Paso 12. Para la **plantilla de regla de reclamación**, elija **Enviar atributos LDAP como reclamaciones** y haga clic en **Siguiente**.

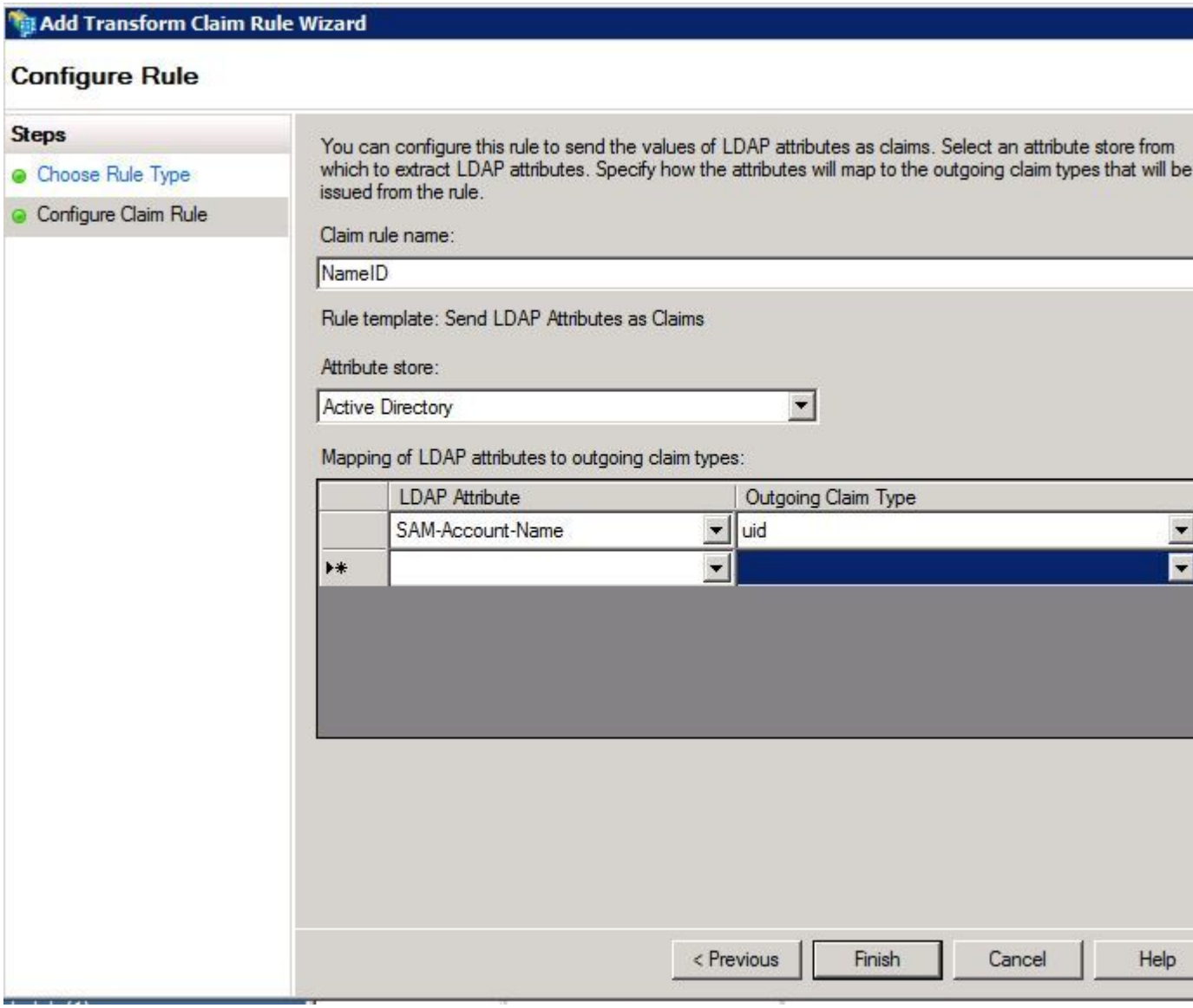
Paso 13. En la página siguiente, introduzca **NameID** para el **nombre de la regla de reclamación**.

Paso 14. Elija **Active Directory** para el **almacén de atributos**.

Paso 15. Elija **SAM-Account-Name** para el **atributo LDAP**.

Paso 16. Introduzca **uid** para el **tipo de reclamación saliente**.

Nota: uid no es una opción de la lista desplegable; debe introducirse manualmente.



Paso 17. Haga clic en Finish (Finalizar).

Paso 18. La primera regla ha finalizado. Haga clic en **Agregar regla** nuevamente.

Paso 19. Seleccione **Enviar justificantes de venta mediante una regla personalizada**.

Paso 20. Introduzca un **nombre de regla de reclamación**.

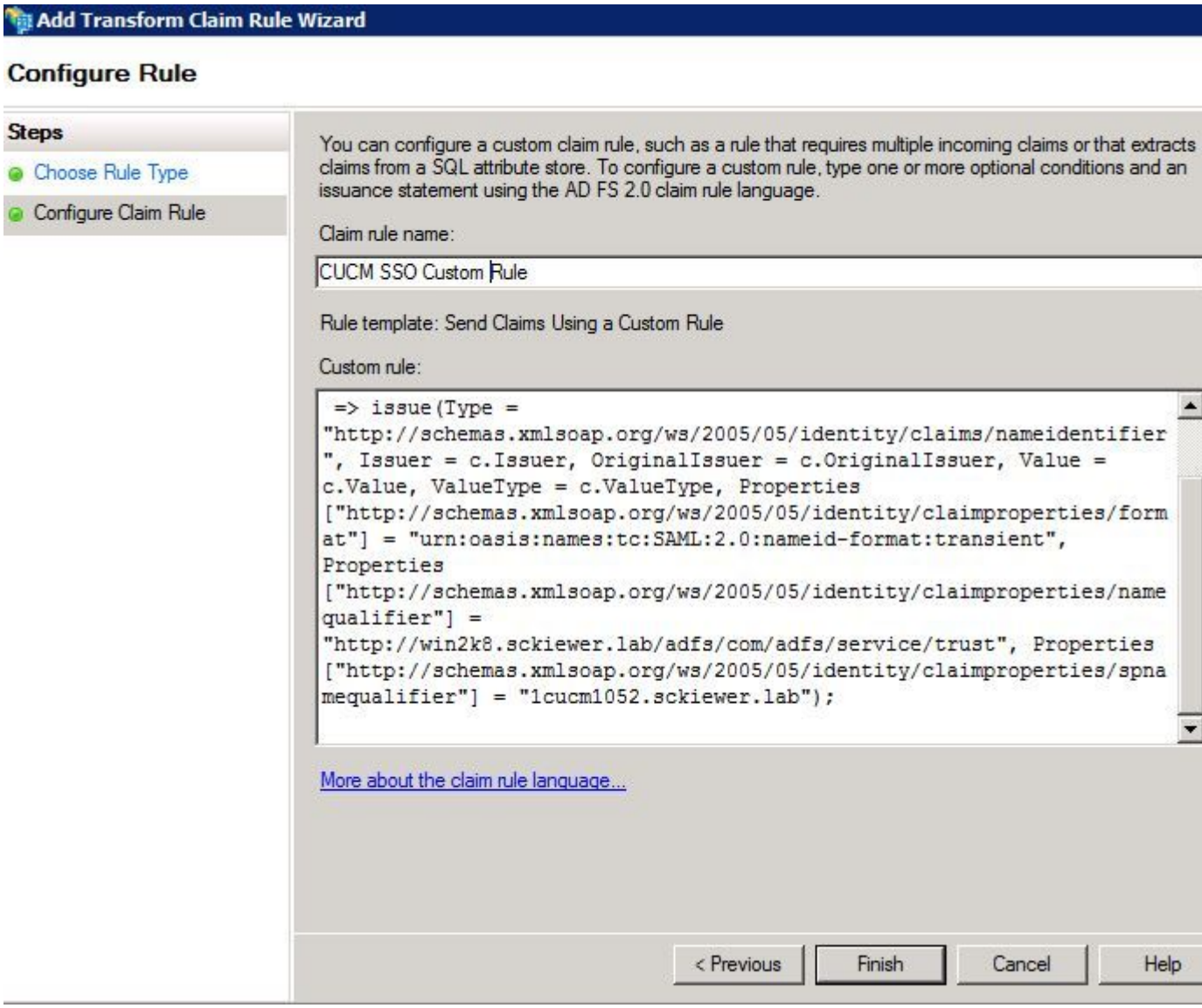
Paso 21. En el campo **Regla personalizada**, pegue este texto:

```
c:[Tipo == "http://schemas.microsoft.com/ws/2008/06/identity/reclamaciones/nombredecuenta de Windows"]
=> issue(Tipo = "http://schemas.xmlsoap.org/ws/2005/05/identity/clobjetivos/identificador de nombre", Emisor = c.Emisor, EmisorOriginal = c.EmisorOriginal, Valor = c.Valor, TipoDeValor = c.TipoDeValor,Propiedades["http://schemas.xmlsoap.org/ws/2005/05/identity/Claimproperties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",Propiedades["http://schemas.xmlsoap.org/ws/2005/05/identity/Claimproperties/namequalifier"] = "http://ADFS_FEDERATION_SERVICE_NAME/com/adfs/service/trust", Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/Claimproperties/spnamequalifier"] = "CUCM_ENTITY_ID");
```

Paso 22. Asegúrese de cambiar AD_FS_SERVICE_NAME y CUCM_ENTITY_ID por los valores

adecuados.

Nota: si no está seguro del nombre de servicio de AD FS, puede seguir los pasos para encontrarlo. La ID de entidad de CUCM se puede extraer de la primera línea del archivo de metadatos de CUCM. Hay un entityID en la primera línea del archivo que tiene este aspecto, entityID=1cucm1052.sckiewer.lab,. Debe introducir el valor subrayado en la sección correspondiente de la regla de reclamación.



Paso 23. Haga clic en Finish (Finalizar).

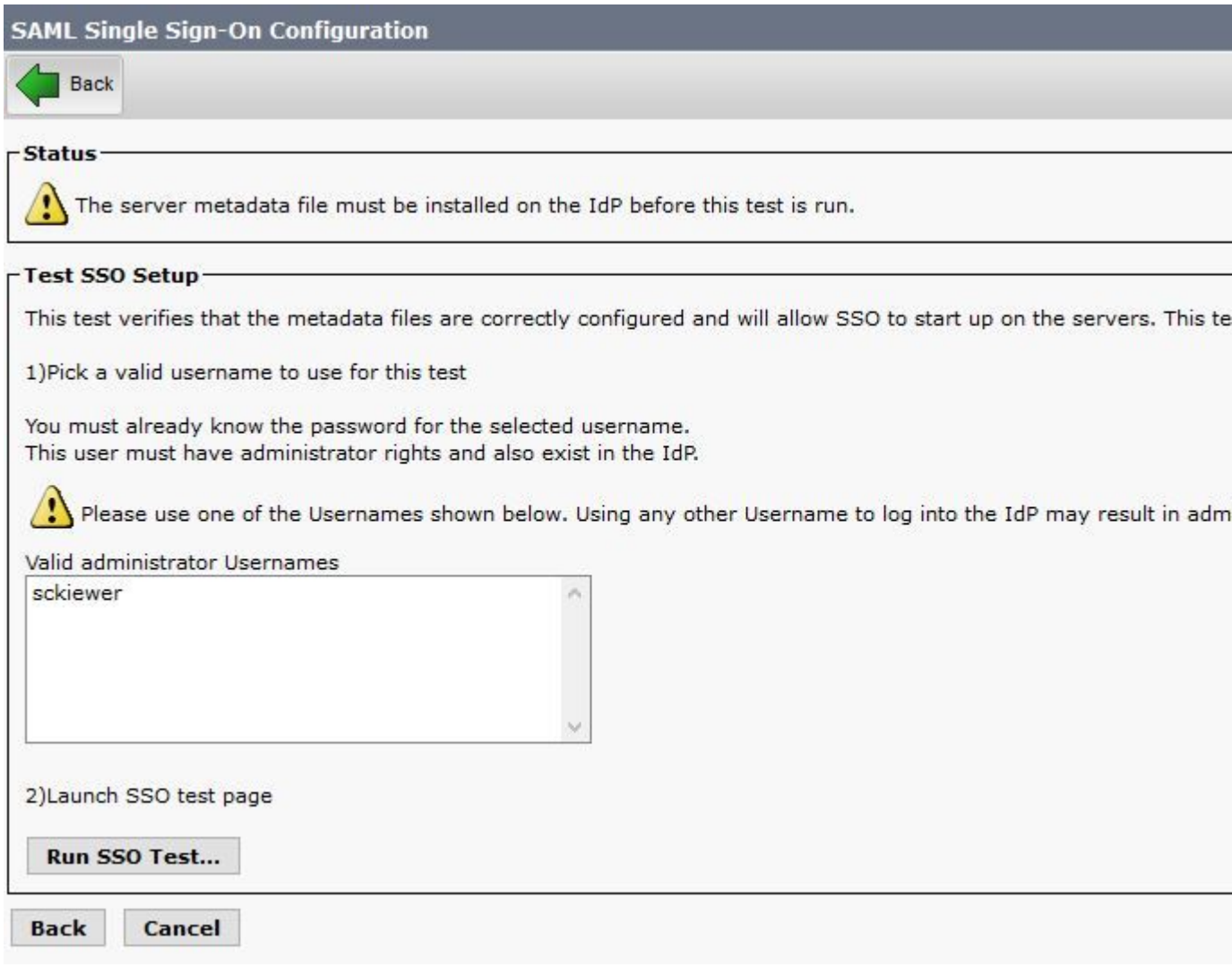
Paso 24. Click OK.

Nota: las reglas de reclamación son necesarias para cualquier servidor de Unified Collaboration en el que pretenda utilizar SSO.

Finalice la habilitación de SSO en CUCM y ejecute la prueba de SSO

Paso 1. Ahora que el servidor de AD FS está completamente configurado, puede volver a CUCM.

Paso 2. Lo dejó en la página de configuración final:



Paso 3. Seleccione el usuario final que tenga la función **Superusuarios de CCM estándar** seleccionada y haga clic en **Ejecutar prueba de SSO...**

Paso 4. Asegúrese de que el explorador permite las ventanas emergentes e introduzca sus credenciales en la solicitud.

Paso 5. Haga clic en **Cerrar** en la ventana emergente y, a continuación, en **Finalizar**.

Paso 6. Tras un breve reinicio de las aplicaciones web, se habilita SSO.

Troubleshoot

Establecer registros de SSO en Debug

Para configurar los registros de SSO para depurar, debe ejecutar este comando en la CLI de CUCM: **set samltrace level debug**

Los registros de SSO se pueden descargar desde RTMT. El nombre del conjunto de registros es **Cisco SSO**.

Buscar El Nombre Del Servicio De Federación

Para buscar el nombre del servicio de federación, haga clic en **Inicio** y busque **Administración de AD FS 2.0**.

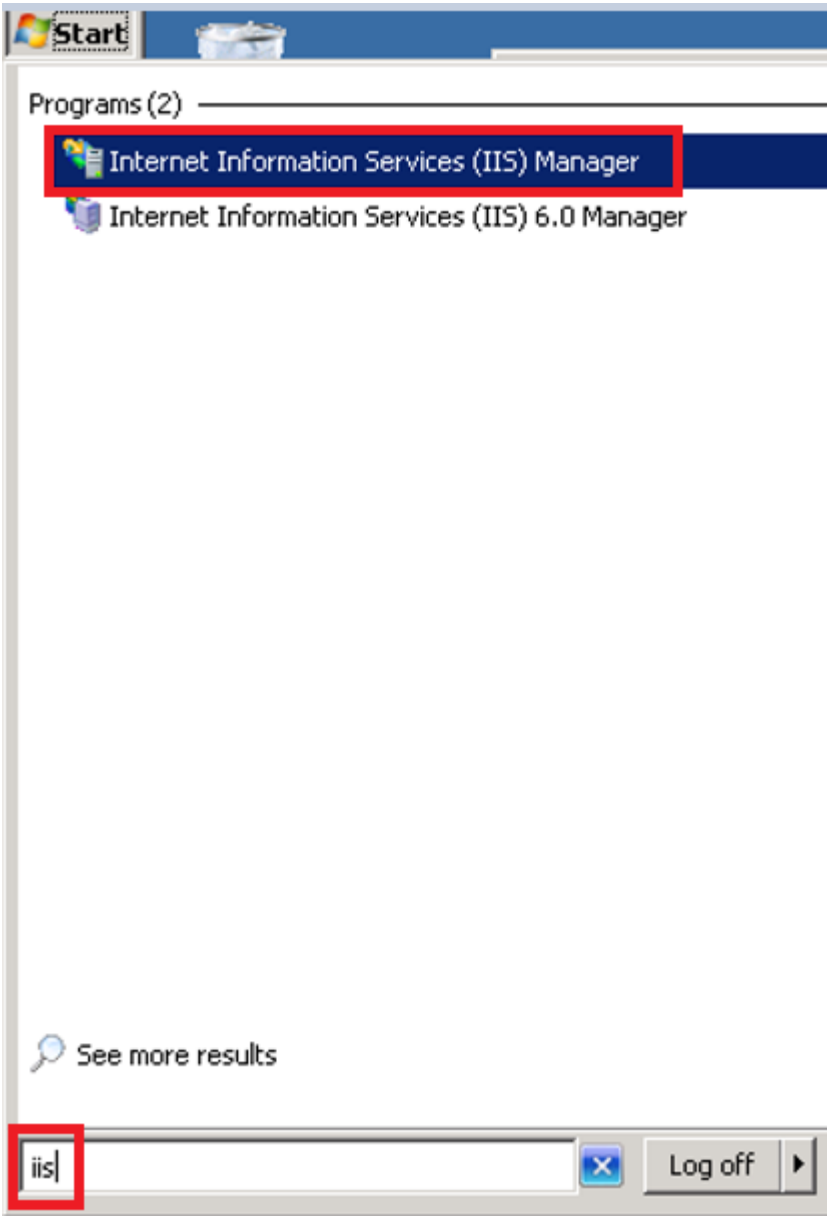
· Haga clic en Editar **propiedades del servicio de federación...**
· En la ficha General, busque el **nombre del Servicio de federación**

Certificado Sin Puntos Y Nombre Del Servicio De Federación

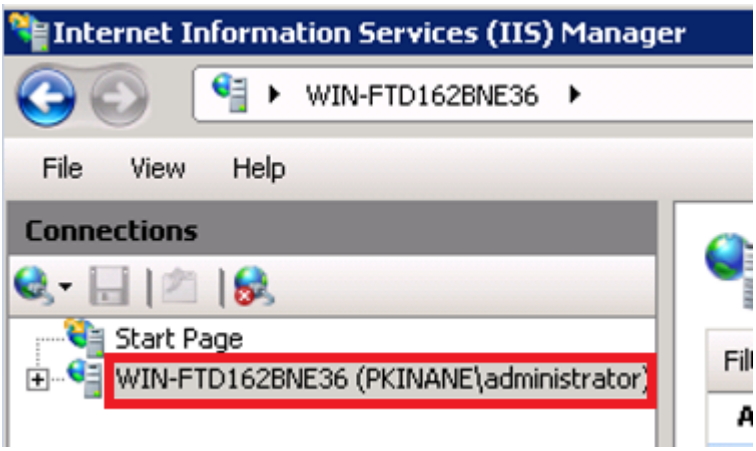
Si recibe este mensaje de error en el asistente para configuración de AD FS, debe crear un nuevo certificado.

El certificado seleccionado no se puede usar para determinar el nombre del Servicio de federación porque el certificado seleccionado tiene un nombre de sujeto sin puntos (nombre abreviado). Seleccione otro certificado sin un nombre de asunto sin puntos (nombre abreviado) e inténtelo de nuevo.

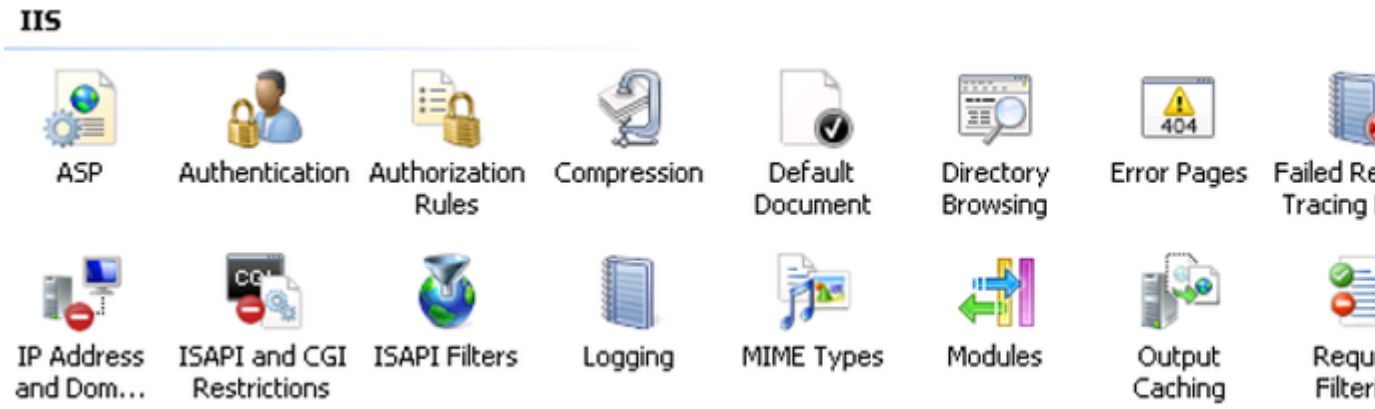
Paso 1. Haga clic en Inicio y busque iis y, a continuación, abra el Administrador de Internet Information Services (IIS)



Paso 2. Haga clic en el nombre del servidor.

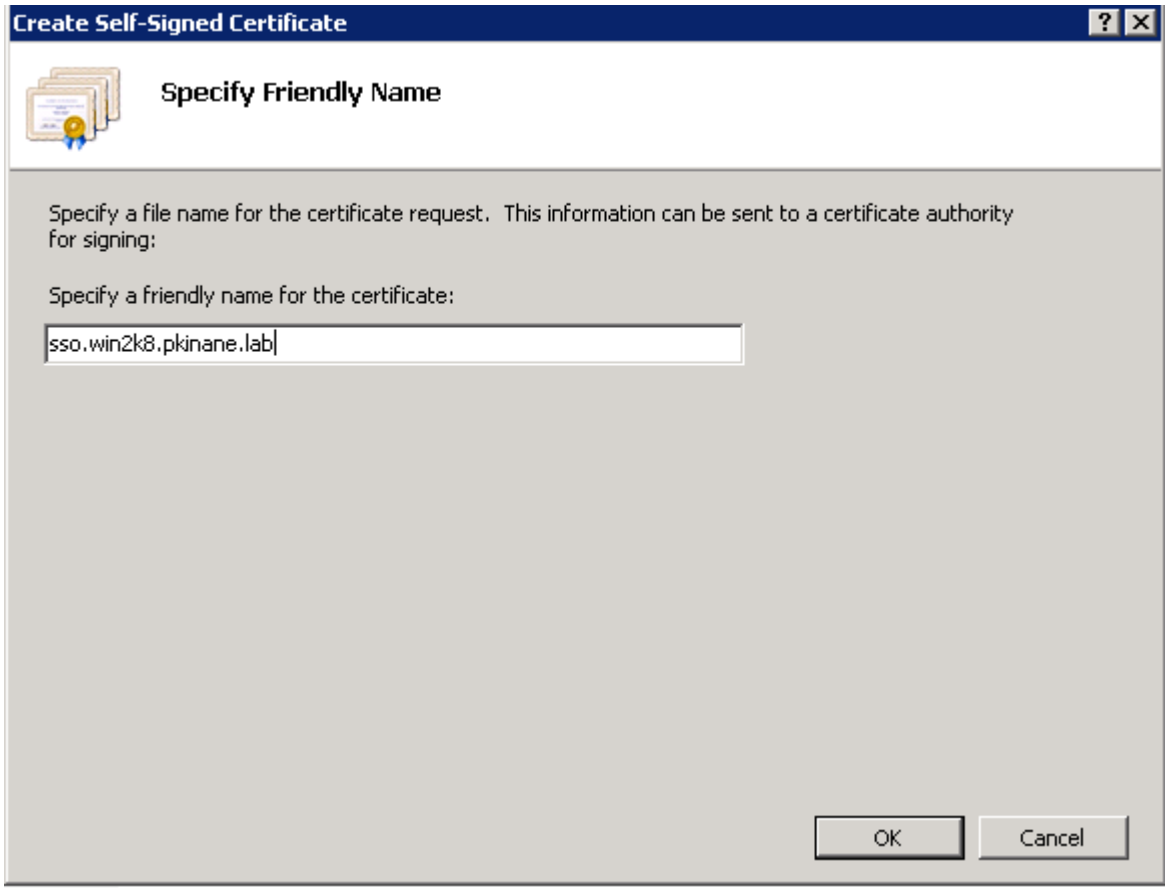


Paso 3. Haga clic en Certificados de servidor.



Paso 4. Haga clic en Crear certificado autofirmado.

Paso 5. Introduzca el nombre que desee para el alias del certificado.



Tiempo fuera de sincronización entre los servidores CUCM y IDP

Si recibe este error al ejecutar la prueba de SSO desde CUCM, debe configurar Windows Server para que utilice los mismos servidores NTP que CUCM.

Respuesta SAML no válida. Esto puede deberse a que el tiempo no está sincronizado entre Cisco Unified Communications Manager y los servidores IDP. Verifique la configuración de NTP en ambos servidores. Ejecute "utils ntp status" desde la CLI para comprobar este estado en Cisco Unified Communications Manager.

Una vez que Windows Server tiene los servidores NTP correctos especificados, debe realizar otra prueba de SSO y ver si el problema continúa. En algunos casos, es necesario sesgar el período de validez de la afirmación. Más detalles sobre ese proceso aquí.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems

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).