Configuración sola Muestra-en usar CUCM y AD FS 2.0 (r2 2008 del Servidor Windows)

Contenido

Introducción

Este documento describe cómo configurar solo Muestra-en usar la comunicación unificada Cisco maneja (CUCM) y el servicio de la federación del Active Directory (AD FS) 2.0 (el r2 2008 del Servidor Windows).

Contribuido por Scott Kiewert, ingeniero de Cisco TAC.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco unificó al administrador de la comunicación
- Conocimiento de Basick de ADFS 2.0

Para habilitar el SSO en su ambiente de laboratorio, usted necesita esta configuración

- Servidor Windows con AD FS 2.0 instalado
- CUCM con el LDAP sincronizan configurado.
- **Un usuario final** con el papel de **superusuarios estándar de CCM** seleccionado.

Componentes Utilizados

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

- Servidor Windows con AD FS 2.0
- CUCM

Información interna de Cisco

Descargue y instale AD FS 2.0 en su Servidor Windows

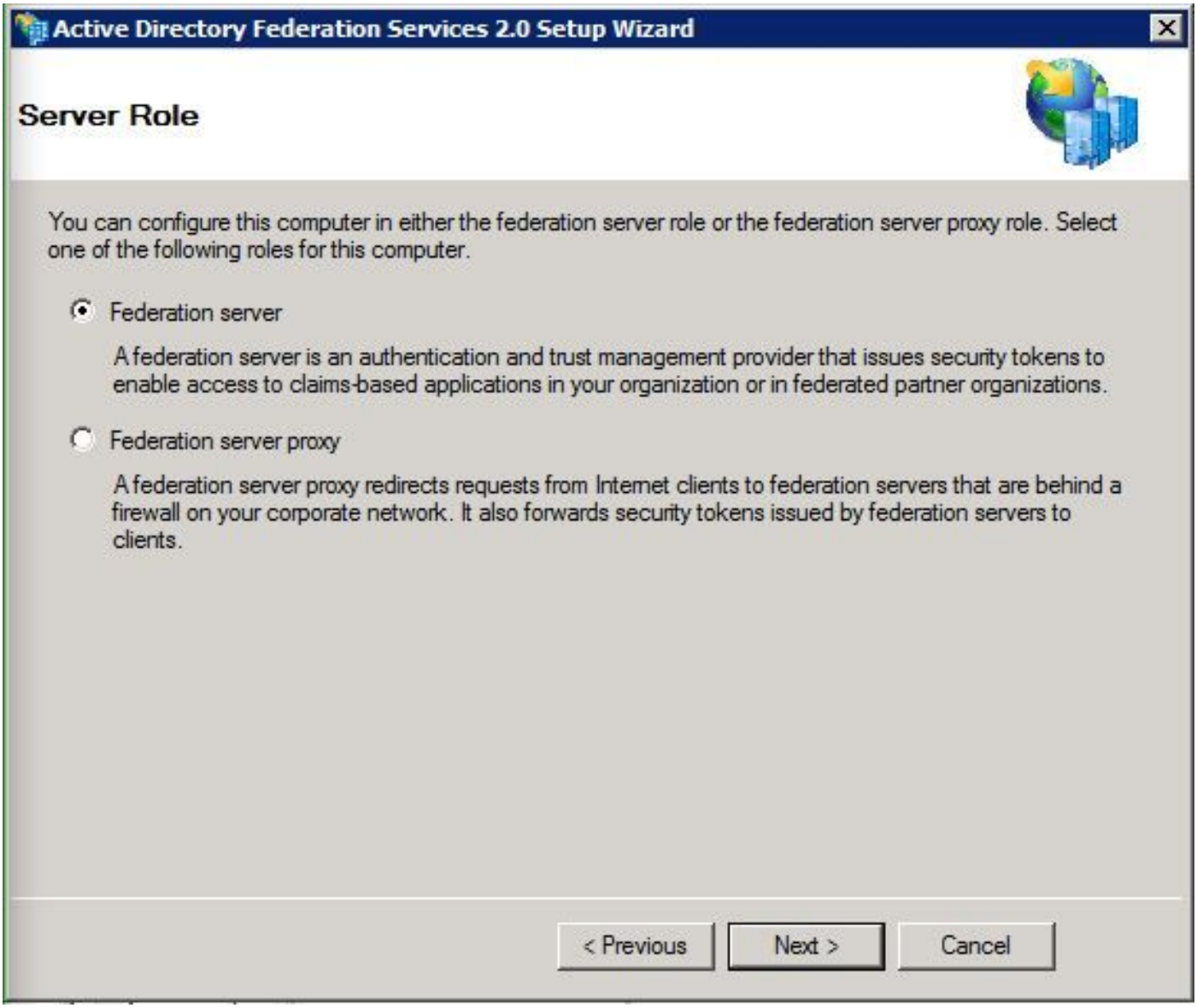
Paso 1. Navegue a https://www.microsoft.com/en-us/download/details.aspx?id=10909 y el tecleo continúa.

Paso 2. En la ventana emergente, aseegurese le seleccionar la descarga apropiada basada en su Servidor Windows.

Paso 3. Mueva el archivo descargado a su Servidor Windows.

Paso 4. Proceda con la instalación:

Paso 5. Cuando se le pregunte, **servidor** selecto de la **federación**:



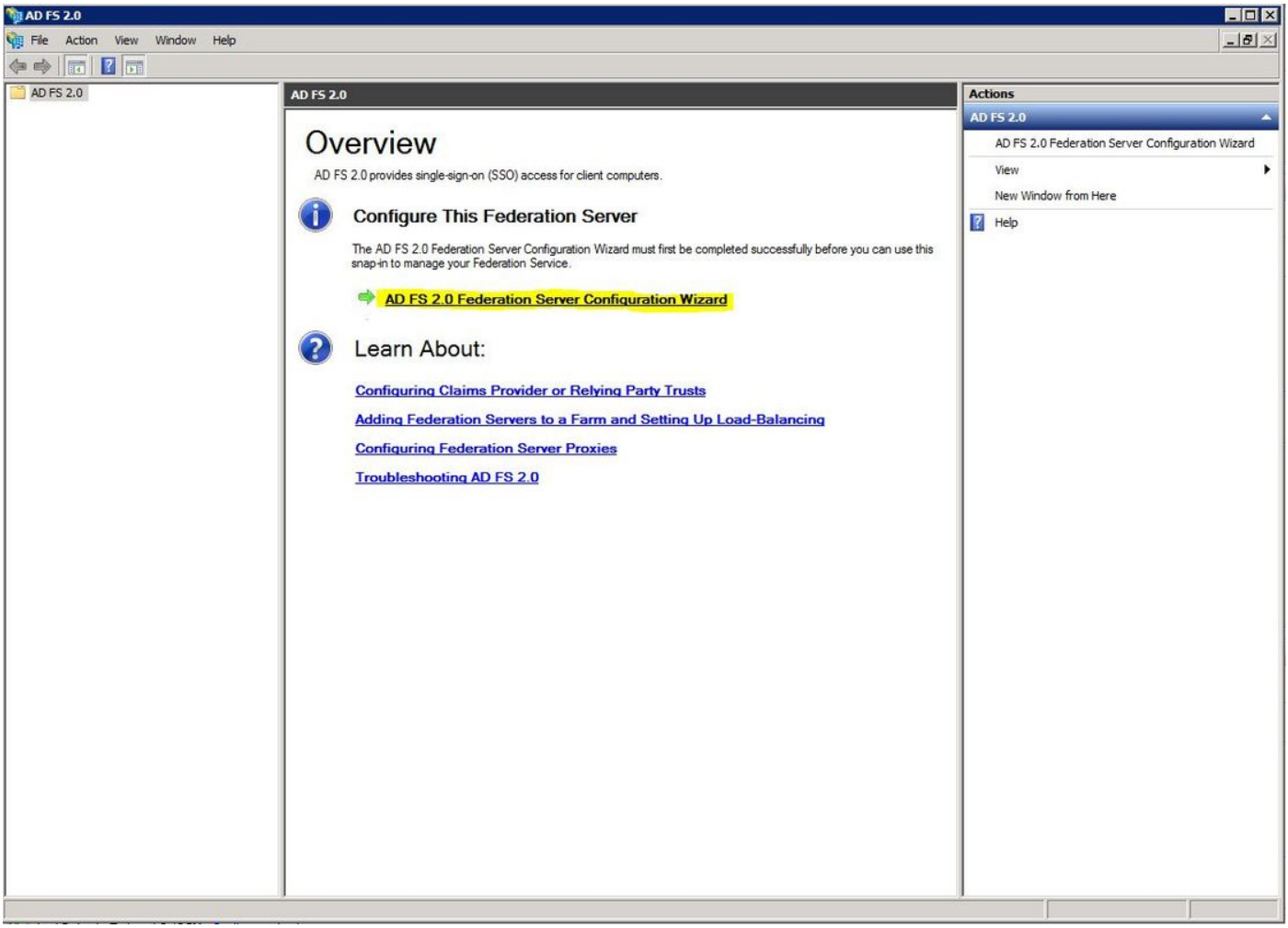
Paso 6. Algunas dependencias pueden ser instaladas automáticamente y le indican al clic en Finalizar.

Ahora que usted tiene AD FS 2.0 instalado en su servidor, usted necesita agregar una cierta configuración.

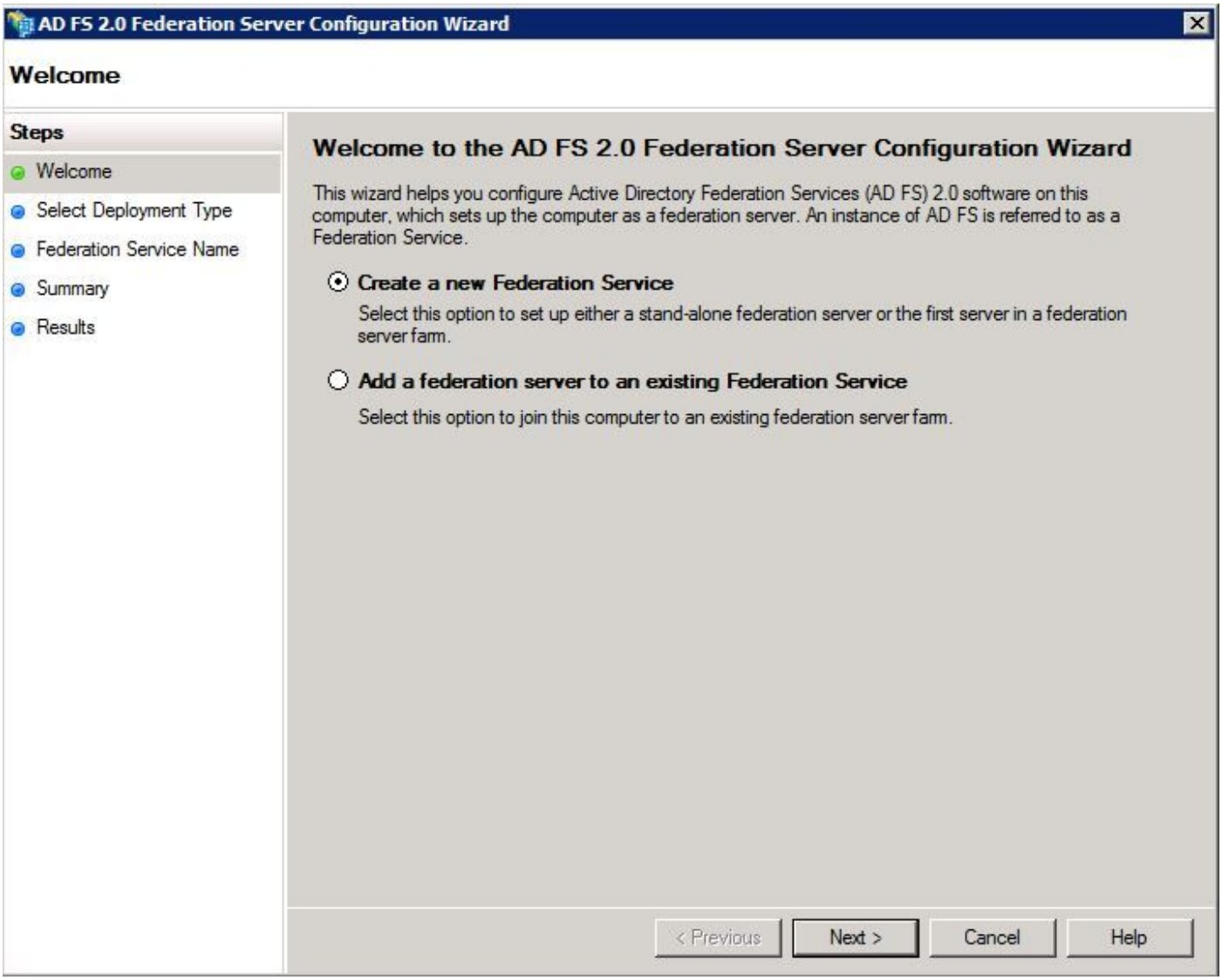
Configuración AD FS 2.0 en su Servidor Windows

Paso 1. La ventana AD FS 2.0 debe haberse abierto después de que el instalar, sin embargo, usted puede encontrarlo haciendo clic el **comienzo** y buscando para la Administración AD FS 2.0.

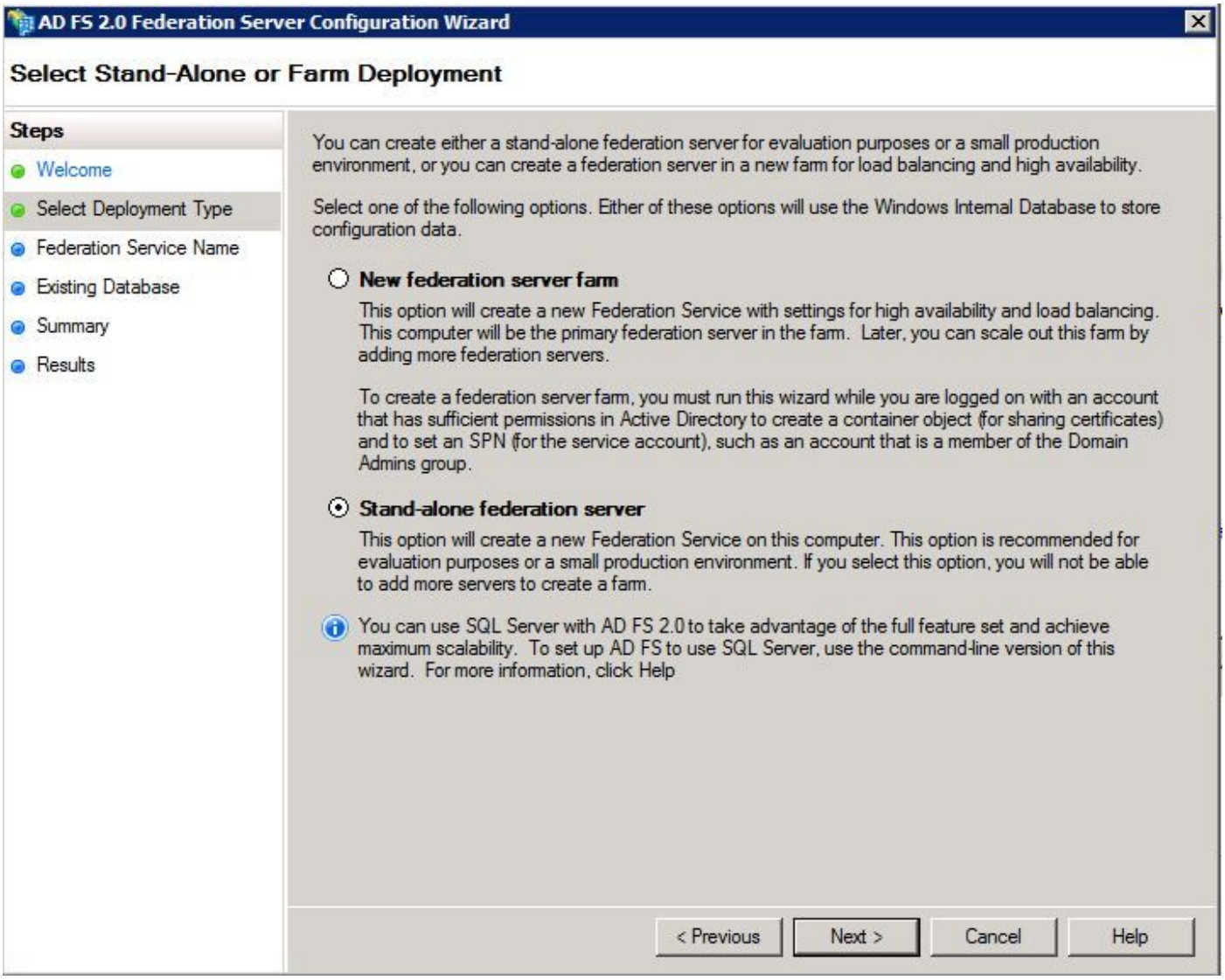
Paso 2. Una vez que usted tiene la ventana AD FS abierta, seleccione al **Asisitente de la Configuración del servidor de la federación AD FS 2.0.**



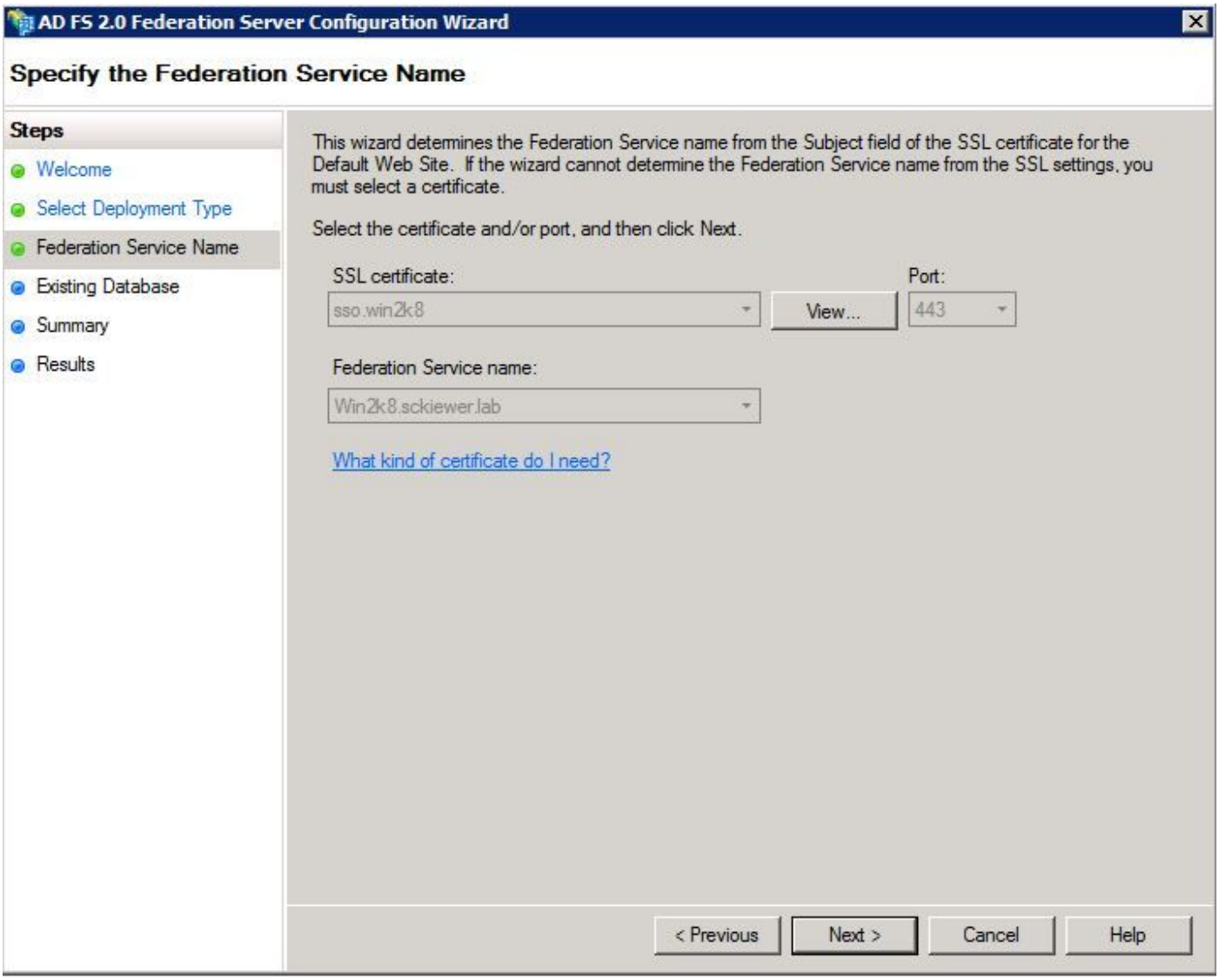
Paso 3. Después, el tecleo **crea un nuevo servicio de la federación.**



Paso 4. Para un ambiente de laboratorio, el **servidor independiente de la federación** es suficiente.



Paso 5. Después, le piden seleccionar un certificado que las aplicaciones del servidor. Esto si el auto puebla mientras el servidor tenga un certificado ya.



Paso 6. Si usted tiene una base de datos existente AD FS en el servidor, usted necesita quitarlo para continuar.

Paso 7. Finalmente, usted es en una pantalla sumaria donde usted puede apenas hacer clic **después**.

Importe los meta datos de Idp a CUCM/a la descarga los meta datos CUCM

Paso 1. Descargue los meta datos de su servidor AD FS navegando al URL siguiente: https://hostname/federationmetadata/2007-06/federationmetadata.xml

Paso 2. Navegue a **Cisco unificó la administración** > el **sistema CM** > **SAML escogen Muestra-en**

Paso 3. **Permiso SAML SSO del** tecleo

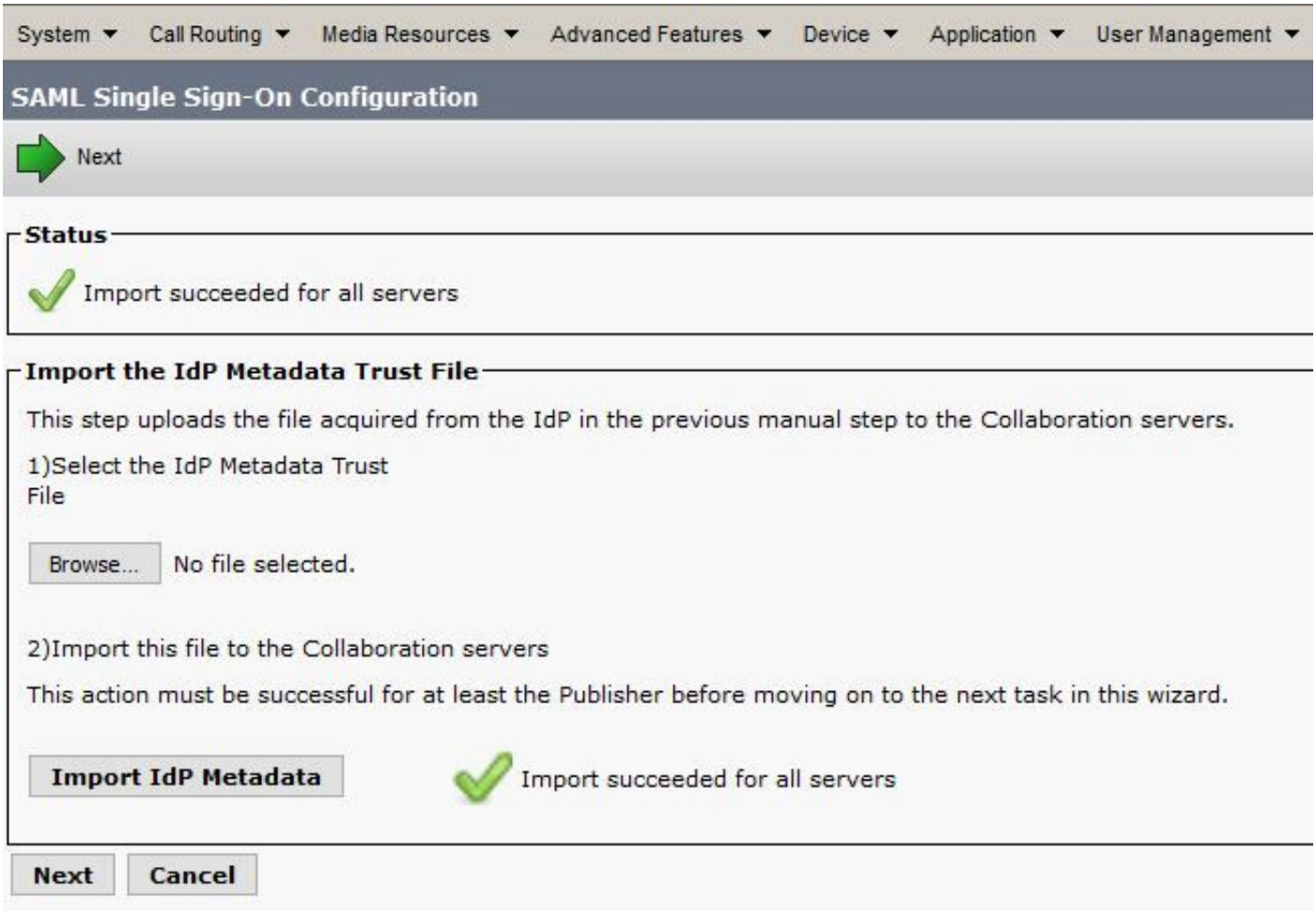
Paso 4. Usted puede recibir una advertencia sobre las conexiones del servidor Web que necesitan ser reajustado, golpe **continúa** simplemente

Paso 5. Después, CUCM le da instrucciones para descargar el archivo de metadatos de su IdP. En este escenario, su servidor AD FS es el IdP, y descargamos los meta datos en el **paso 1** antedicho, así que el tecleo **después**.

Paso 6. Le piden importar el archivo.

Paso 7. El tecleo **hojea** > selecciona el .xml del **paso 1** > los **meta datos de IdP de la importación del** tecleo.

Paso 8. Usted debe recibir un mensaje que la importación era acertada:



Paso 9. Tecleo **después**

Paso 10. Ahora que usted tiene los meta datos de IdP importado en CUCM, usted necesita importar los meta datos CUCM en su IdP.

Paso 11 **Archivo de metadatos de la confianza de la descarga del** tecleo

Paso 12. Tecleo **después**

Paso 13. Mueva el archivo del .zip que fue descargado en el **paso 12 a** su Servidor Windows y extraiga el contenido a una carpeta.

Importe CUCM Metatdata al servidor AD FS 2.0 y cree las reglas de la demanda

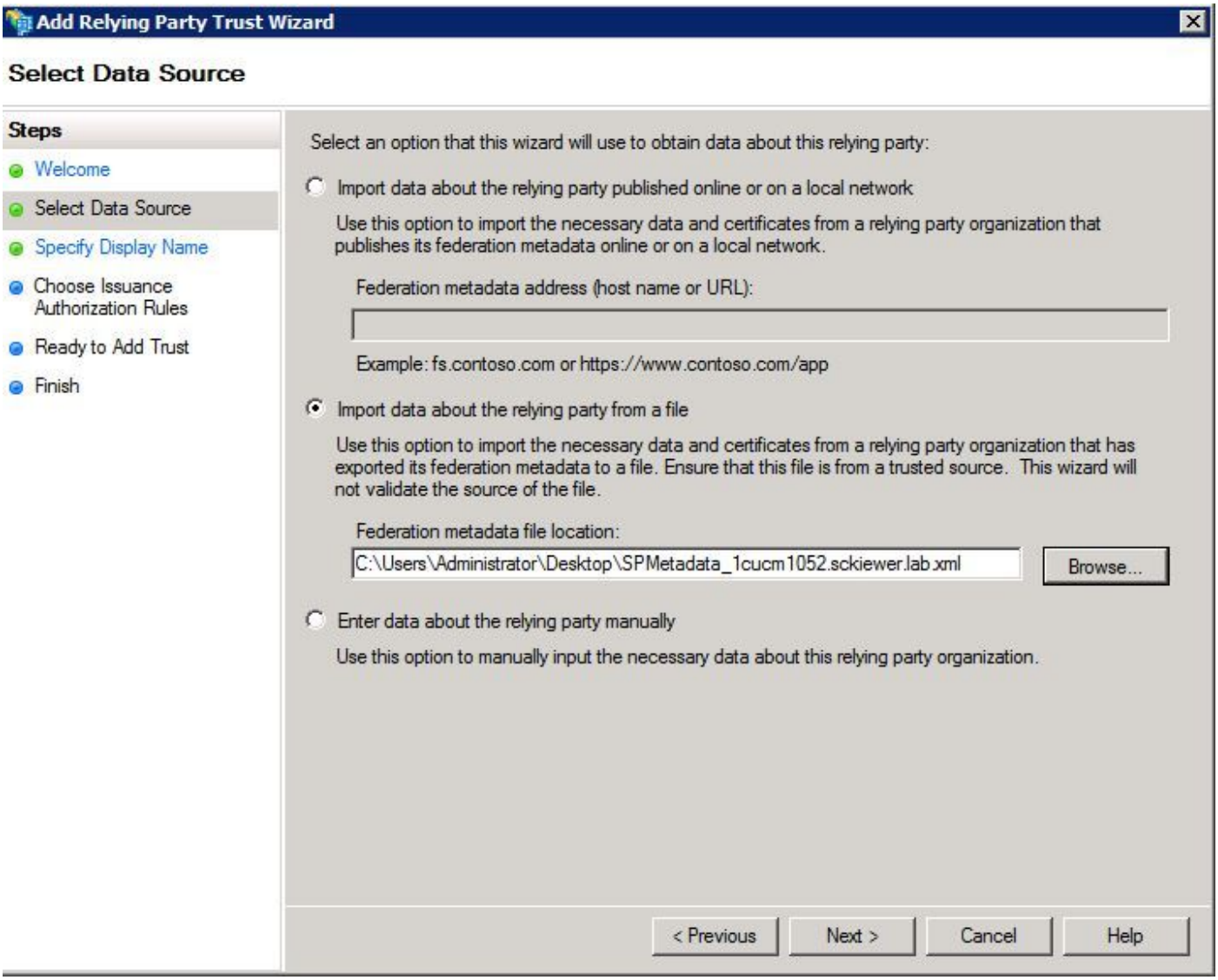
Paso 1. En este momento, vuelva a su servidor AD FS y abra la ventana de administración AD FS 2.0 haciendo clic el **comienzo** y buscando para la **Administración AD FS 2.0.**

Paso 2. Tecleo **requerido: Agregue un partido de confianza de confianza** (nota: si usted no ve esto, usted puede necesitar cerrar la ventana y abrirla de reserva. Esta opción no aparecerá si la ventana se ha dejado abierta puesto que el **Asisitente del servidor de la federación** completado).

Paso 3. Una vez que usted tiene el **Asisitente de confianza de la confianza del partido del agregar** abierto, haga clic el **comienzo**.

Paso 4. Aquí, usted necesita importar los archivos del .xml que usted extrajo en el **paso 13**, así que los **datos** selectos de la **importación sobre el partido de confianza de un archivo** y hojea a la carpeta que contiene los archivos, selecciona el .xml para su editor.

Nota: Siga los mismos pasos arriba para cualquier Collaboration Server unificado que usted quiera utilizar el SSO encendido.



Paso 5. Tecleo **después**

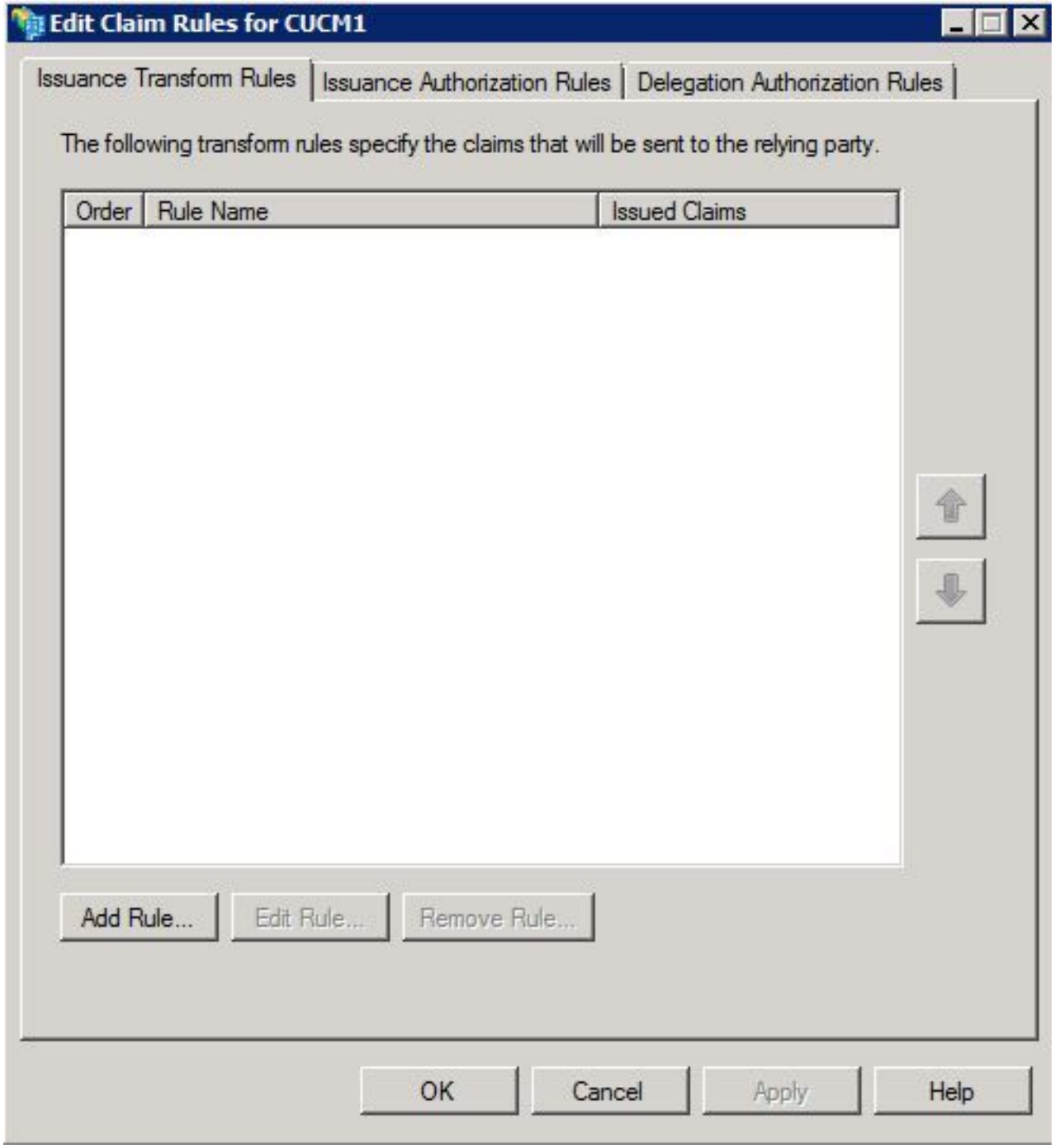
Paso 6. Edite el **nombre de la visualización** a sea cual sea usted entonces quisiera hacer clic **después.**

Paso 7. **Permiso** selecto **todos los usuarios de acceder este partido de confianza** y de hacer clic **después**

Paso 8. Tecleo **después** una vez más

Paso 9. En esta pantalla, aseegurese le tener **abierto el diálogo de las reglas de la demanda del editar para esta confianza de confianza del partido cuando el Asisitente se cierra** marcado, después hacen clic **cerca**

Paso 10. Usted debe ahora ser traído a una ventana que parezca esto:



Paso 11. En esta ventana, el tecleo **agrega la regla**.

Paso 12. Para la **plantilla de la regla de la demanda**, selecto **envíe los atributos LDAP como demandas** y haga clic **después.**

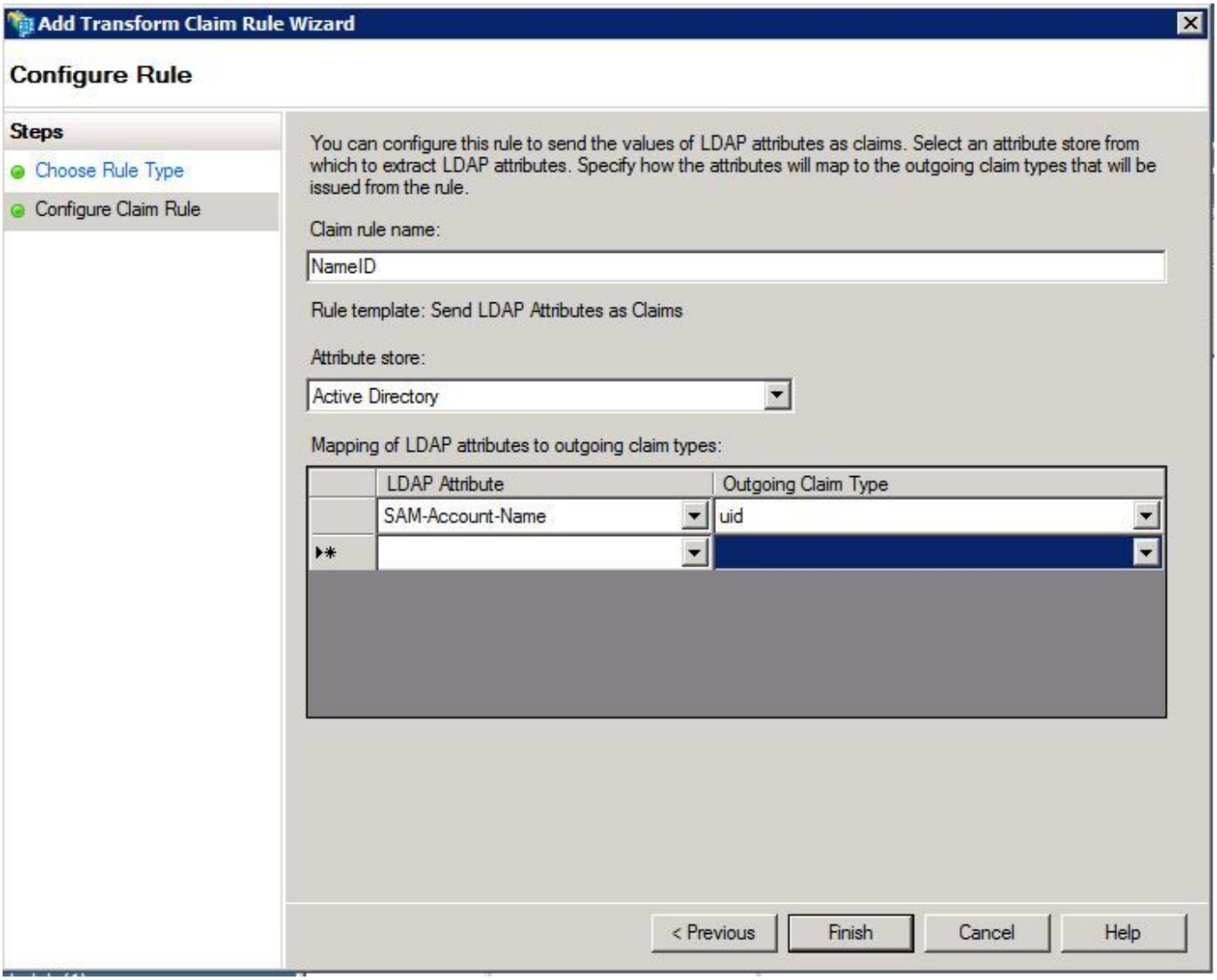
Paso 13. En la página siguiente, ingrese **NameID** para el **nombre de la regla de la demanda**

Paso 14. **Active Directory** selecto para el **almacén del atributo**

Paso 15. **SAM-Cuenta-nombre** selecto para el **atributo LDAP**

Paso 16. Ingrese el **uid** para el **tipo saliente de la demanda**

Nota: **el uid** no es una opción que autofill o aparecer en el menú desplegable



Paso 17. Clic en Finalizar

Paso 18. Usted debe ahora ver su regla, sin embargo, necesitaremos agregar otra regla así que el tecleo **agrega la regla** otra vez.

Paso 19. Selecto **envíe las demandas usando una regla de encargo**

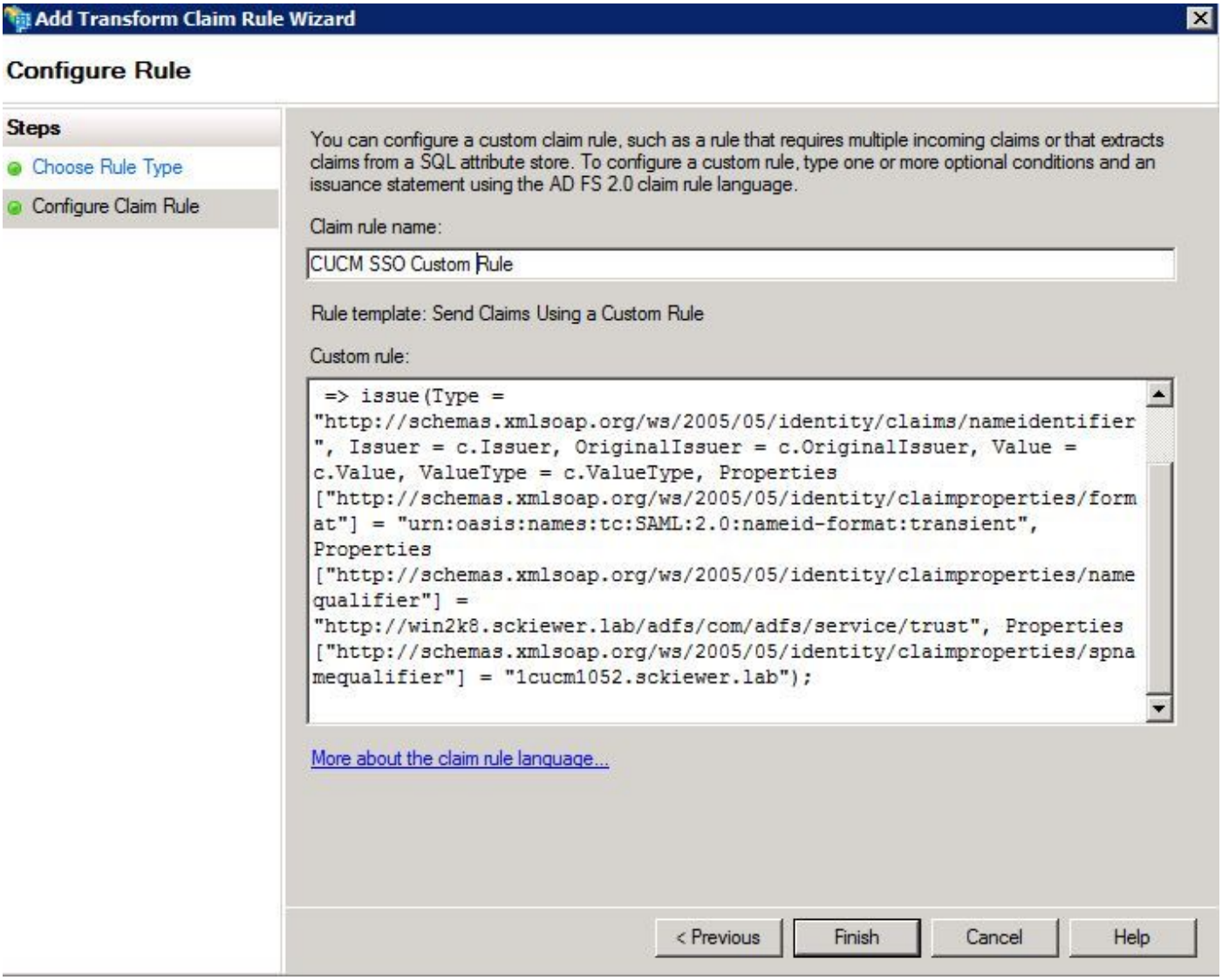
Paso 20. Ingrese un **nombre de la regla de la demanda** (éste puede ser cualquier cosa)

Paso 21. En el campo de la **regla de encargo**, pegue el texto siguiente:

```
c: [== "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] del tipo

 problema del => (tipo = el "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", emisor = c.Issuer, OriginalIssuer = c.OriginalIssuer, valor = c.Value, ValueType = c.ValueType, propiedades ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] el = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",

propiedades ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] = "http:// <AD_FS_SERVICE_NAME>

/adfs/com/adfs/service/trust", propiedades ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"<CUCM_FQDN>");
```

Paso 22. Aseegurese le modificar los dos bloques de texto en azul con los valores apropiados.

Nota: Si usted no está seguro sobre el **nombre del servicio AD FS**, vaya a los comentarios de este documento a aprender cómo idendtify el **nombre del servicio AD FS.**



Paso 23. Clic en Finalizar

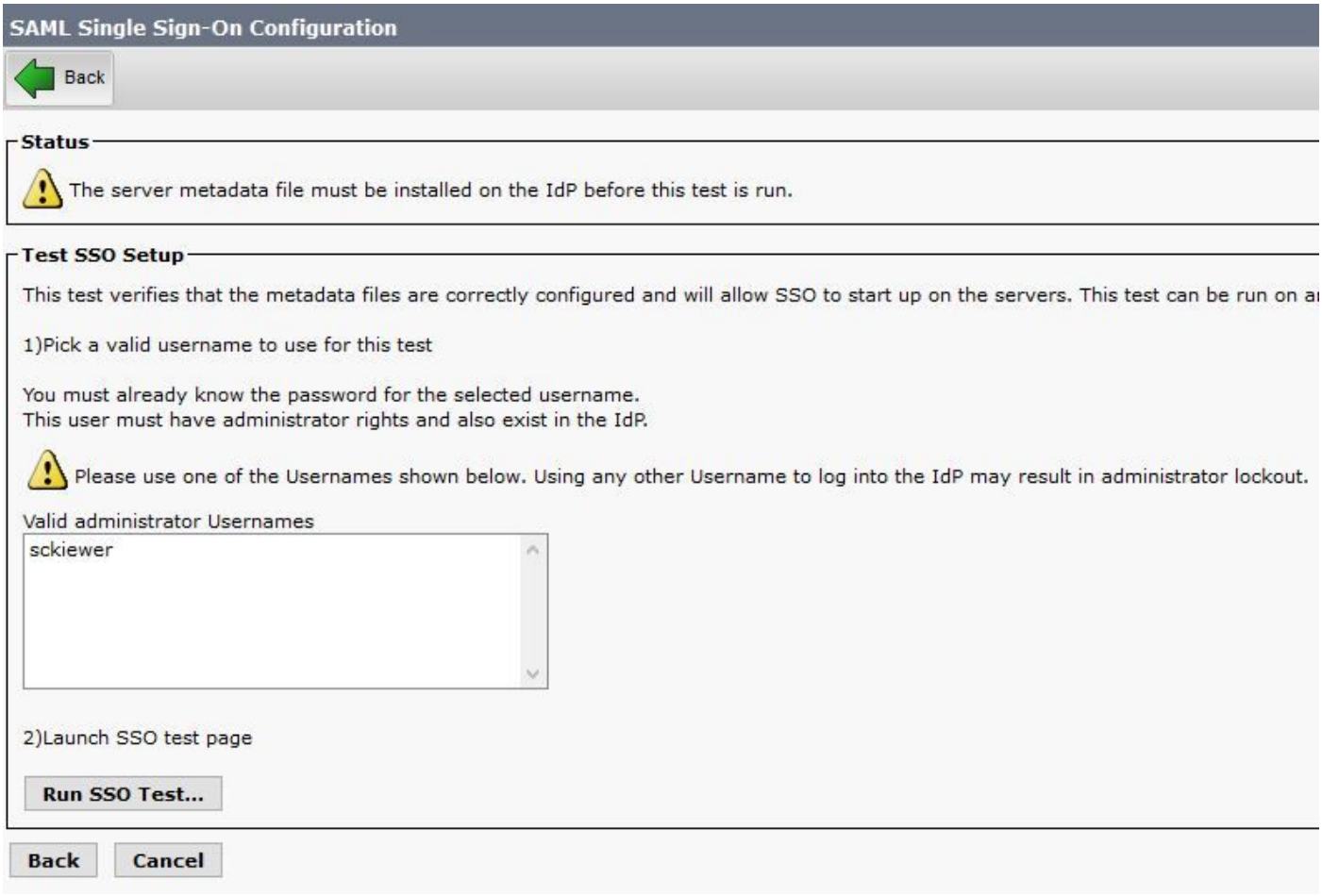
Paso 24. Haga clic en OK (Aceptar).

Nota: Las reglas de la demanda son necesarias para cualquier Collaboration Server unificado que usted quiera utilizar el SSO encendido.

Acabe de habilitar el SSO en CUCM y funcione con la prueba SSO

Paso 1. Ahora que el servidor AD FS es de configuración completa, usted puede volver a CUCM.

Paso 2. Usted debe sentarse en una página que parezca esto:



Paso 3. Continúe y seleccione a su usuario final que haga el papel de **superusuarios estándar de CCM** seleccionar y haga clic **para funcionar con la prueba SSO…**

Paso 4. Una ventana emergente debe aparecer que puede tardar cerca de 30 segundos para cargar, pero usted debe ser presentado eventual con un desafío para iniciar sesión.

Paso 5. Ingrese la contraseña que usted configuró en el servidor LDAP para el usuario seleccionado y usted debe entonces ver:

Paso 6. **El cierre del** tecleo en la ventana emergente y entonces **acaba**.

El SSO ahora se configura en su laboratorio.

Resolución de problemas

Fije los registros SSO para hacer el debug de

Para fijar el SSO los registros para hacerle el debug de tienen que funcionar con este comando en el CLI del CUCM: **fije el debug del nivel del samltrace**

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

Encontrar el nombre del servicio de la federación

Usted puede confirmar el nombre del servicio de la federación haciendo clic el **comienzo** y buscando para y abriendo la **Administración AD FS 2.0**.

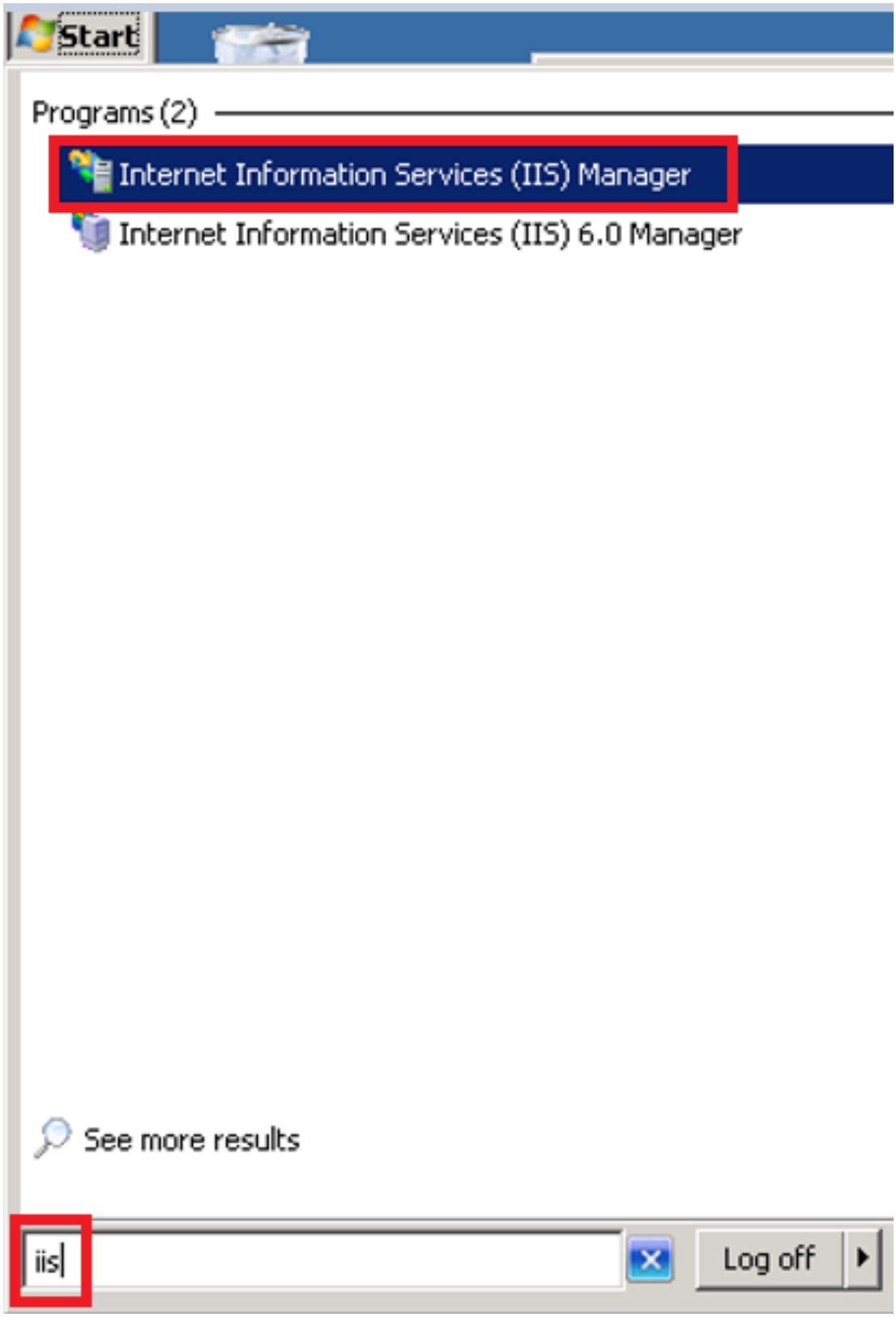
• Haga clic en editan las **propiedades del servicio de la federación…**
• Mientras que en la ficha general busque el **nombre del servicio de la federación**

Certificado Dotless cuando Specifing el nombre del servicio de la federación

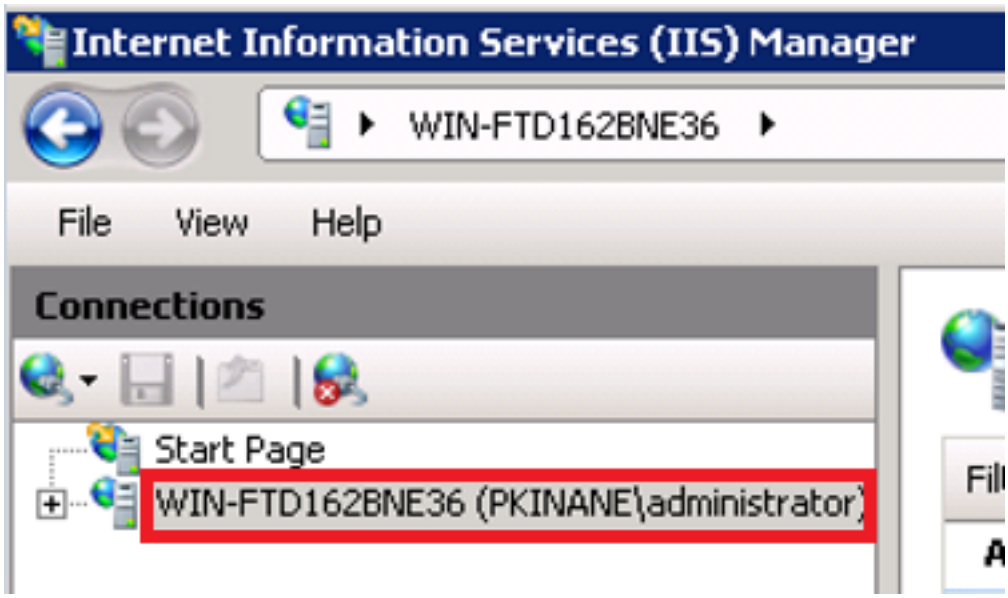
Si usted recibe el mensaje de error siguiente mientras que pasa a través del asistente de configuración AD FS, usted necesitará crear un nuevo certificado.

“El certificado seleccionado no se puede utilizar para determinar el nombre del servicio de la federación porque el certificado seleccionado tiene un asunto (cortocircuito-Nombrado) dotless (por ejemplo, fabrikam). Seleccione otro certificado sin un asunto (cortocircuito-Nombrado) dotless (por ejemplo, fs.fabrikam.com), y después intente otra vez.”

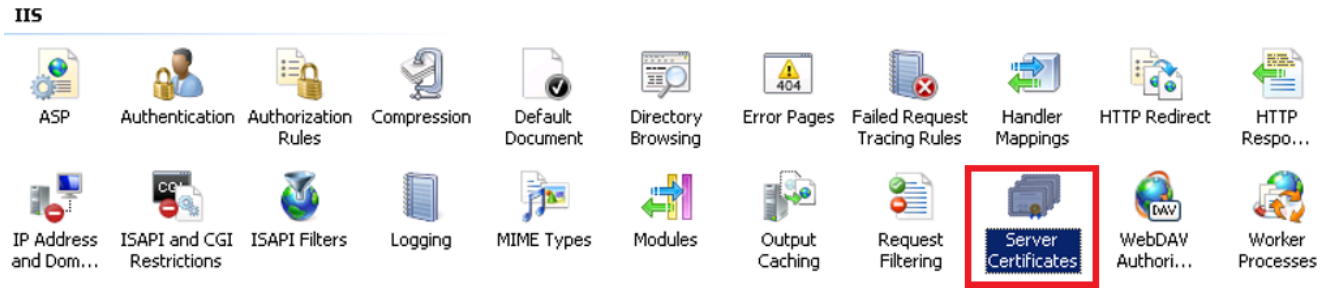
Haga clic el comienzo y la búsqueda para los iis después abre al administrador de los Servicios de Internet Information Server (IIS)



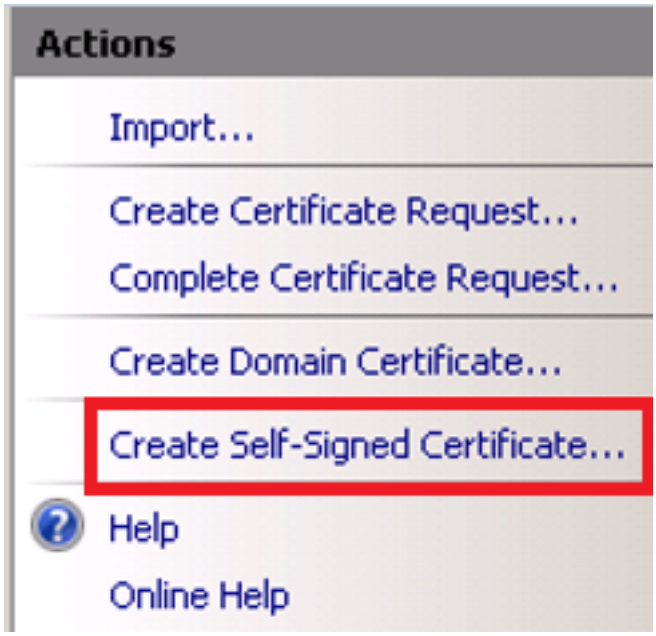
Haga clic en su nombre de servidor



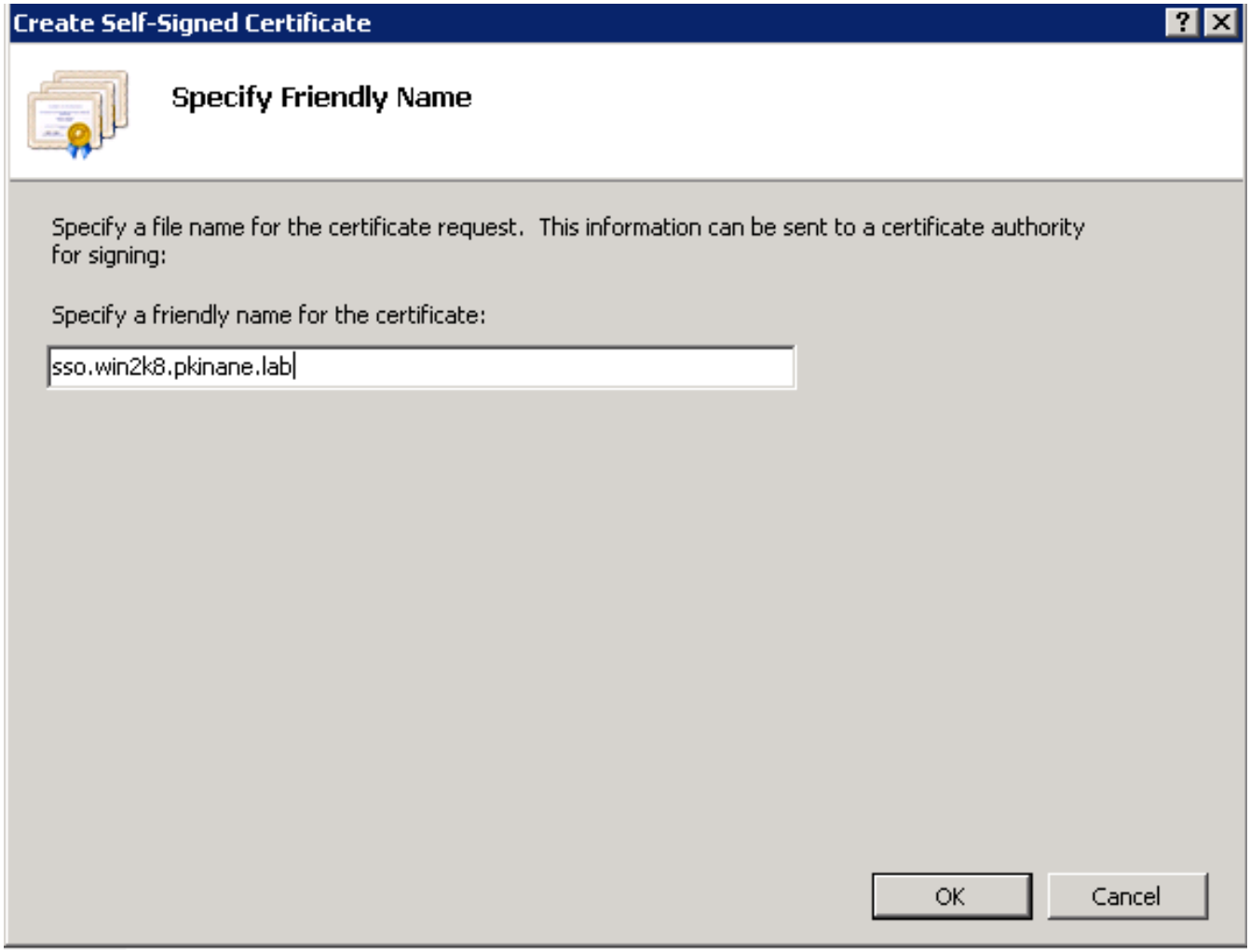
Haga clic en los certificados de servidor



Haga clic en crean el certificado autofirmado



Ingrese el nombre que usted quiere para el alias de su certificado



El tiempo está fuera de sincroniza entre los servidores CUCM e IDP

Si usted está recibiendo el error enumerado debajo al intentar funcionar con la prueba SSO de CUCM, usted puede necesitar configurar al Servidor Windows para utilizar a los mismos servidores NTP que el CUCM. El proceso para hacer esto se cubre en los comentarios de.

"Respuesta inválida de SAML. Esto puede ser causada cuando el tiempo está fuera de sincroniza entre el administrador de las Comunicaciones unificadas de Cisco y los servidores IDP. Verifique por favor la configuración del NTP en ambos servidores. Ejecute "el estatus NTP del utils" del CLI para marcar este estatus en el administrador de las Comunicaciones unificadas de Cisco."

Una vez que el Servidor Windows tiene los servidores NTP le especificaron deben conseguir los meta datos del Idp otra vez y cargarlos al CUCM. Después vaya directamente a la prueba SSO y vea si usted todavía consigue el mismo error.