Configuración de la autenticación externa SSO de SAML con AD FS para ESA y SMA

Contenido

Introducción

Este documento describe cómo configurar los Servicios de federación de Active Directory como proveedor de identidad SAML para la autenticación externa en Cisco ESA y SMA.

Prerequisites

Este documento proporciona una vista de la aplicación de terceros que los ingenieros no pueden ver de otra manera.

- Pasos de configuración para la autenticación externa de Lenguaje de marcado de aserción de seguridad (SAML) con las últimas versiones de los Servicios de federación de Active Directory (AD FS) 2012 y 2016 para Cisco Email Security Appliance (ESA) y Security Management Appliance (SMA).
- Pasos básicos basados en laboratorio que no incluyen configuraciones específicas de implementación especializadas.
- Un ejemplo de funcionamiento de un entorno de laboratorio que puede diferir de una implementación de producción.

⚠ Precaución: Complete la configuración del proveedor de servicios (SP) antes de este procedimiento. Consulte .

Requirements

- Microsoft Active Directory Federation Services (AD FS) 2012 o 2016
- Cisco Email Security Appliance (ESA) y Security Management Appliance (SMA) versión más reciente.

Componentes Utilizados

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.

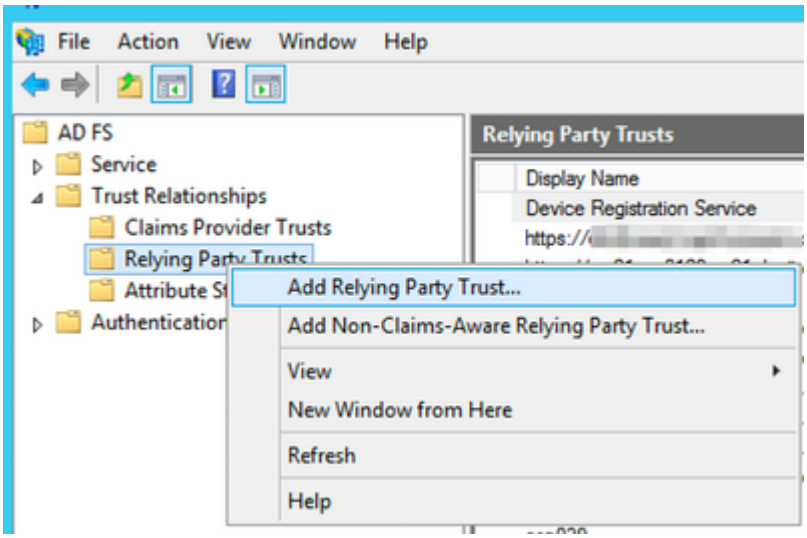
Pasos para la Configuración de ADFS IDP para SAML

Configuración de la confianza del usuario de confianza

Use una de las dos opciones para crear la confianza de usuario de confianza en AD FS.

Método A: Creación de la confianza del usuario de confianza mediante la importación de metadatos SP

1. Abra la consola AD FS Management desde Administrative Tools.
2. En la consola de administración de AD FS, expanda Relaciones de confianza, haga clic con el botón secundario en Confianzas de usuario de confianza y, a continuación, seleccione Agregar confianza de usuario de confianza.



Agregar confianza de usuario de confianza

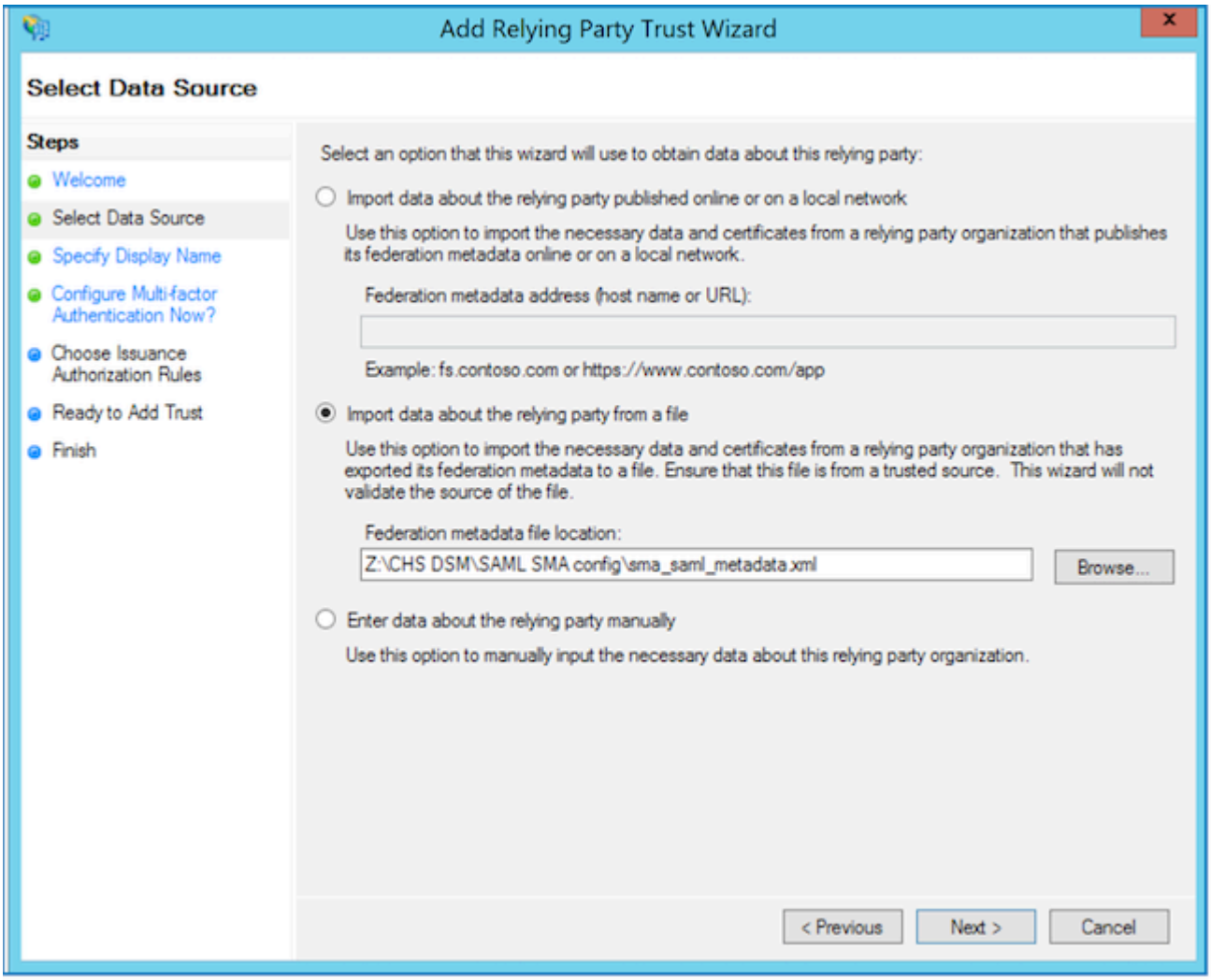
Consejo: Confianzas de Microsoft de confianza

Siga uno de estos procedimientos:

- Opción A: Importar datos sobre el usuario de confianza desde un archivo. Cargue el archivo metadata.xml de ESA o SMA service provider (SP).
- Opción B: Introduzca manualmente los datos sobre la persona que confía. Esta opción le guía por la configuración manual.

Opción A: Importar datos sobre el usuario de confianza desde un archivo. Cargue el archivo metadata.xml del ESA o del proveedor de servicios SMA (SP).

1. Seleccione la opción para importar datos sobre el usuario de confianza desde un archivo y, a continuación, seleccione Siguiente.



Importar el archivo de metadatos ESA/SMA

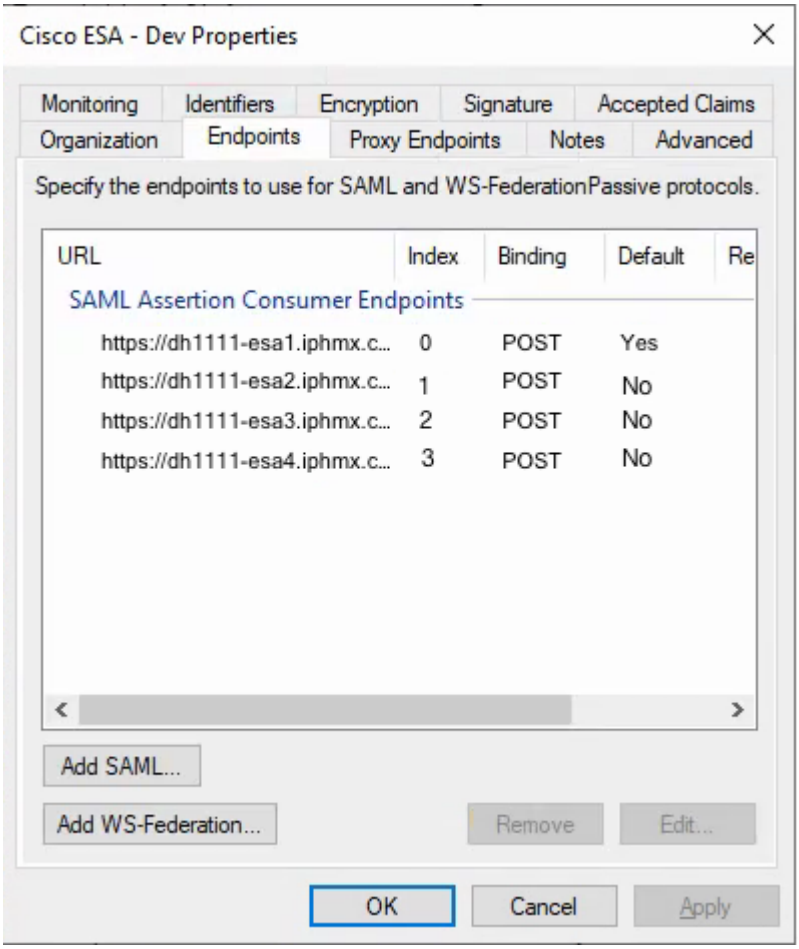
- Especifique un nombre para mostrar para identificar esta confianza de usuario de confianza y, a continuación, seleccione Siguiente dos veces.
- Para las reglas de autorización de emisión, seleccione Permitir a todos los usuarios y, a continuación, seleccione Siguiente.
- En la página Ready to Add Trust, acepte la configuración predeterminada y, a continuación, seleccione Next.
- Seleccione Finish. Se abre el cuadro de diálogo Editar reglas de reclamación para la relación de confianza de la parte que confía, que se trata en Reglas de transformación de emisión - Reclamaciones.

Propiedades de confianza de usuario de confianza: terminales

Realice este paso sólo si hay varios ESA presentes en un clúster.

1. Abra Propiedades de confianza del usuario de confianza > Terminales.
2. Agregue cada dirección URL accesible de ESA y, a continuación, seleccione Aceptar.
3. Los valores de índice cuentan entre 0, es decir, 0, 1, 2 y 3.

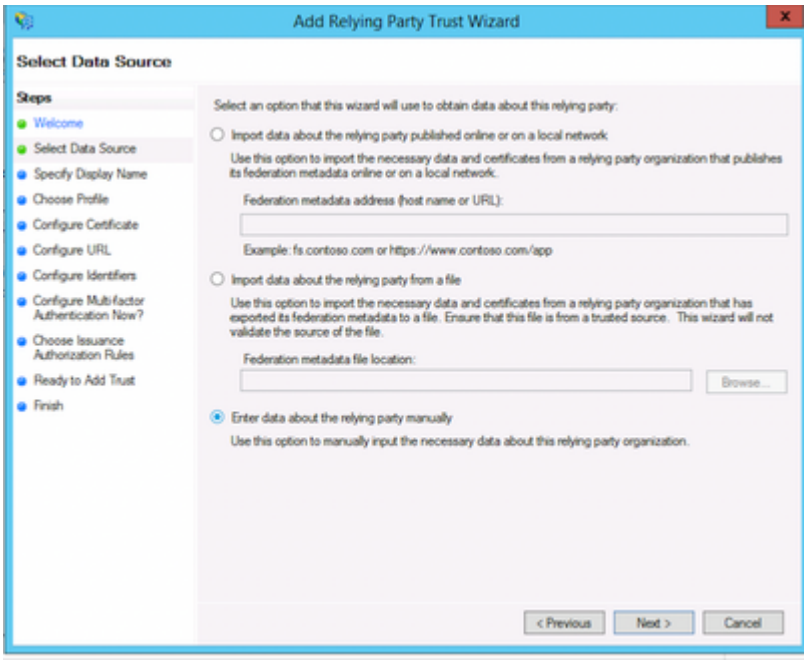
4. Establezca sólo una entrada en Predeterminado = Sí.
5. Establezca las entradas restantes en Default = No.



Propiedades de confianza de usuario de confianza: terminales

Opción B: Introduzca manualmente los datos sobre la persona que confía. Esta opción le guía por la configuración manual.

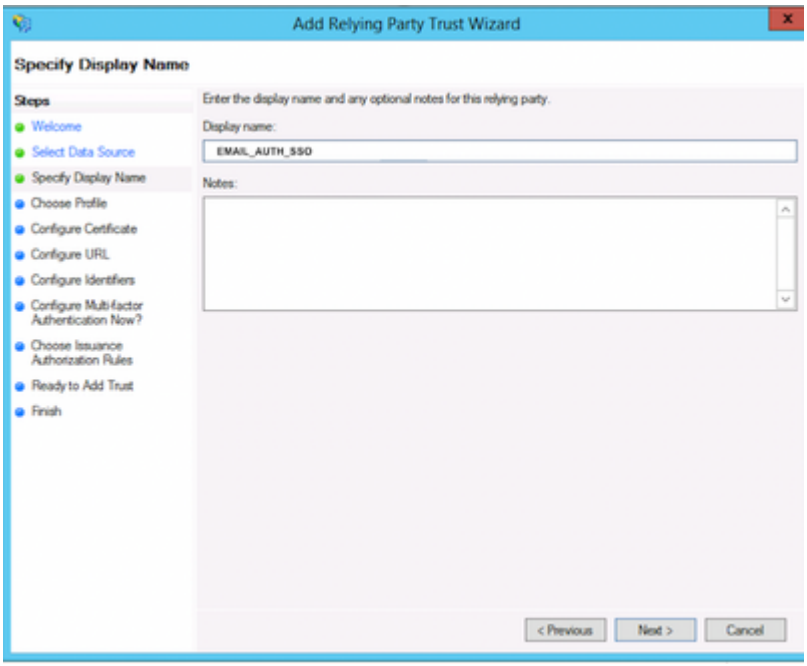
1. Seleccione Introducir datos sobre el usuario de confianza manualmente.



Agregar usuario de confianza manualmente

Consejo: Nombre para mostrar es el nombre que elige para identificar la confianza de la persona que confía para ESA o SMA SAML.

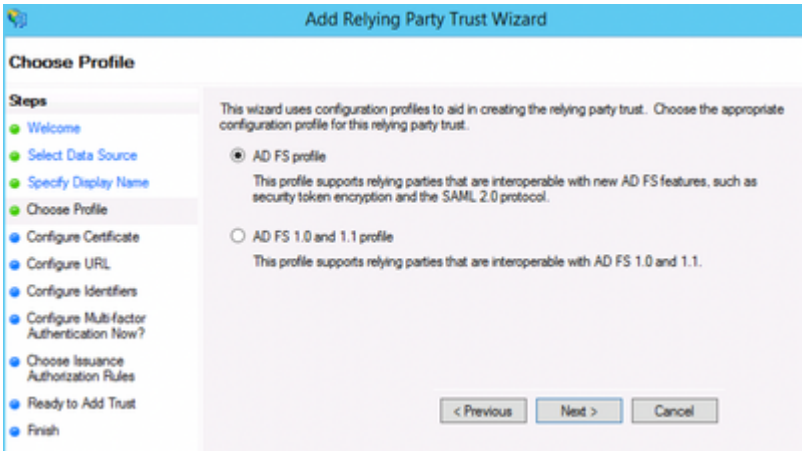
1. Introduzca un nombre para mostrar para el proveedor de servicios, por ejemplo, ESA_SP.



Cree un nombre para el perfil de proveedor de servicios

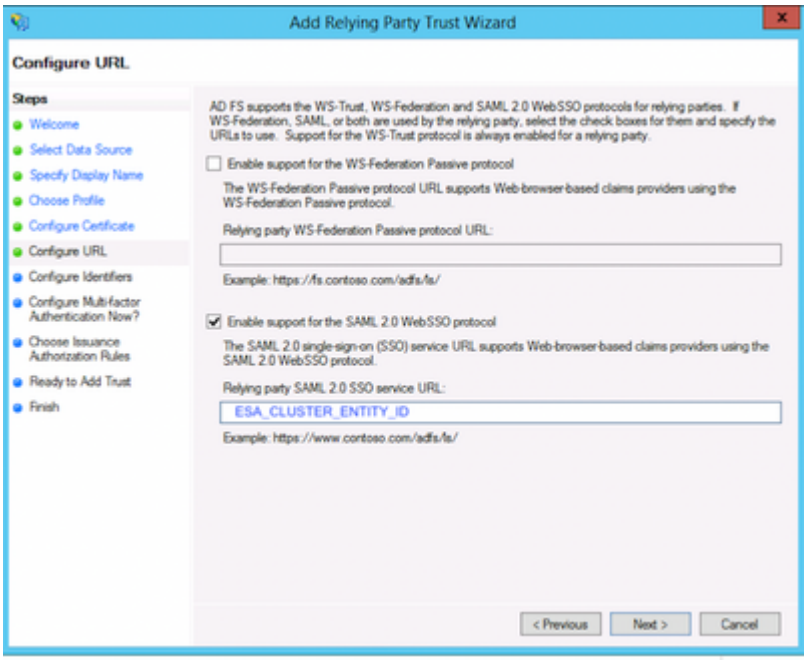
Consejo: La función de las reglas de reclamación y las reglas de transformación de emisión

1. Elija la opción de perfil Perfil de AD FS.



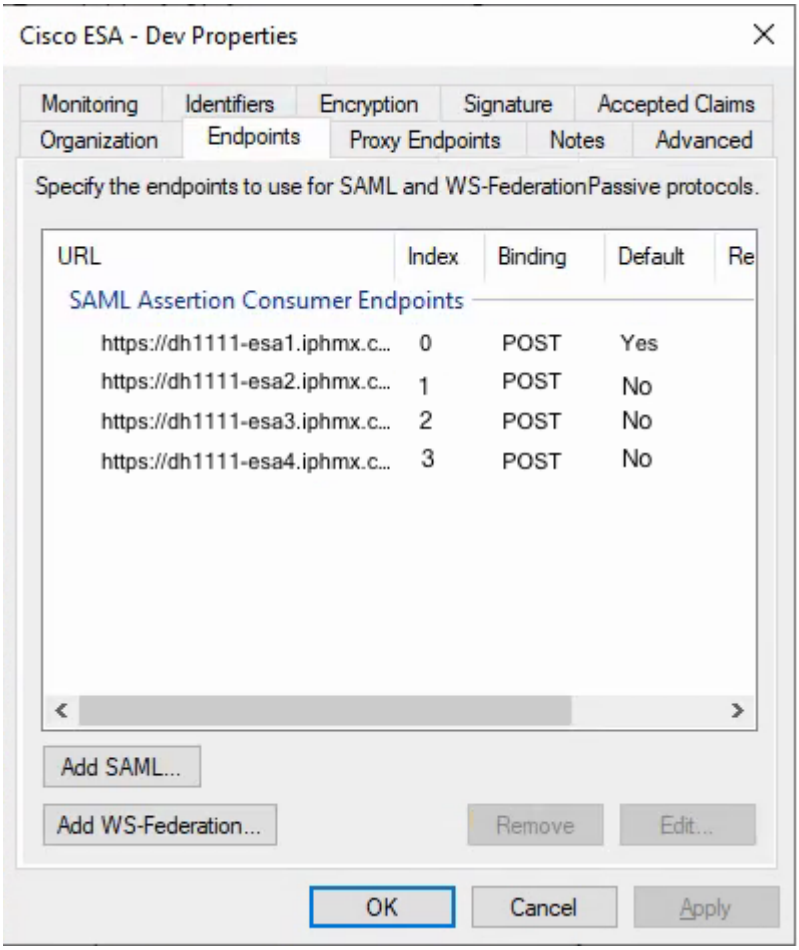
Opción de perfil de AD FS para utilizar SAML 2.0

1. Cargue el certificado público de la configuración del proveedor de servicios (SP) ESA.
2. Para Configurar URL, elija Habilitar soporte para el inicio de sesión único (SSO) de SAML 2.0.
3. Ingrese la URL del servicio SSO SAML 2.0 del usuario de confianza con el valor de ID de entidad de perfil SP.



Reglas de autorización de emisión: -Permitir a todos los usuarios

1. Para las reglas de autorización de emisión, elija Permitir a todos los usuarios acceder a esta persona de confianza.



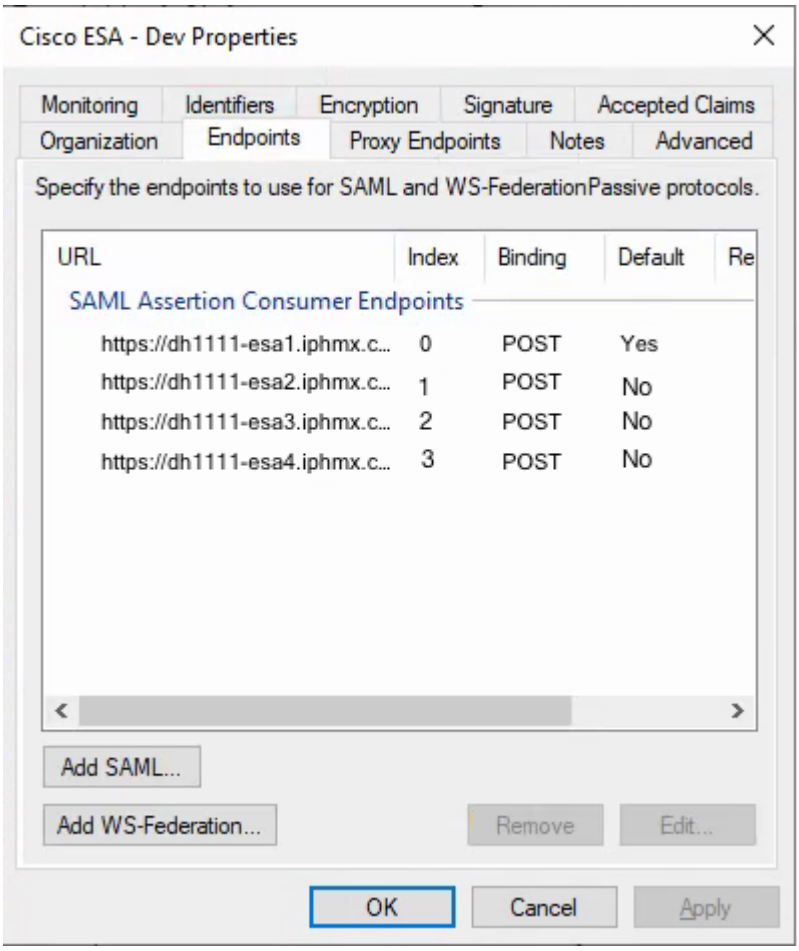
Elegir reglas de autorización de emisión

1. Seleccione Siguiente para ir a la página Finalizar.

Configuración de terminales de confianza de usuario de confianza (solo clústeres)

Realice este paso sólo si hay varios ESA presentes en un clúster.

1. Abra Propiedades de confianza del usuario de confianza > Terminales.
2. Agregue cada dirección URL accesible de ESA y haga clic en Aceptar.
3. Establezca los valores de endpoint index comenzando por 0 (por ejemplo, 0, 1, 2, 3).
4. Establezca sólo un punto final en Predeterminado = Sí. Establezca los extremos restantes en Default = No

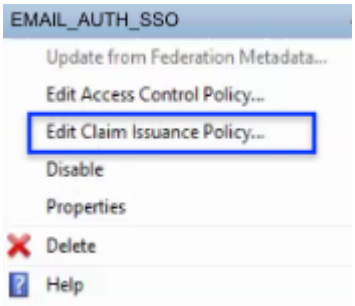


Reglas de autorización de emisión: permitir a todos los usuarios

- El paso Finalizar inicia el cuadro de diálogo Editar reglas de reclamación para la relación de confianza de la parte que confía, que se trata en Reglas de transformación de emisión.

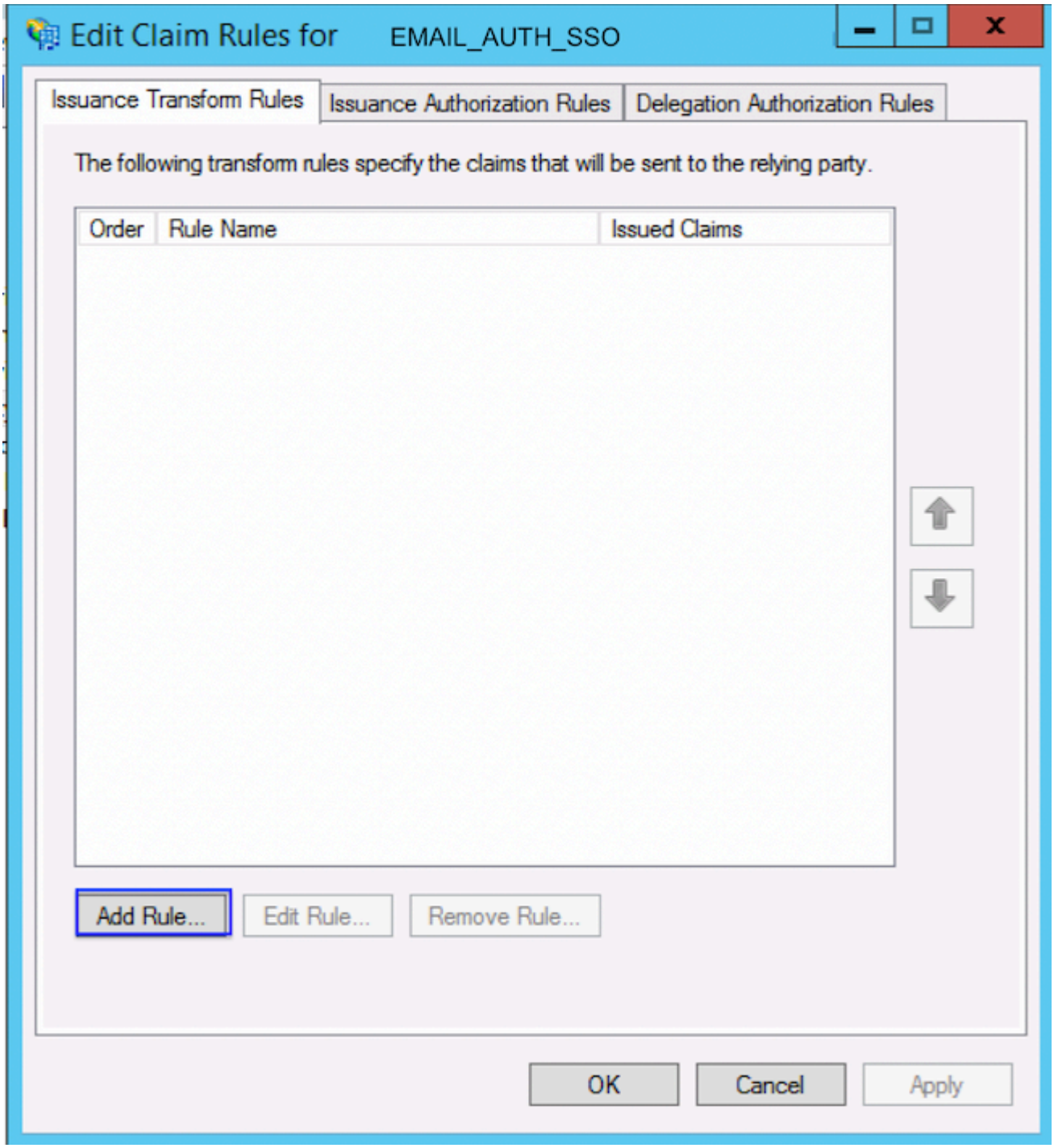
Reglas de transformación de emisión - Reclamaciones

- Seleccione Editar directiva de emisión de reclamaciones.



Editar directiva de emisión de reclamaciones

- Seleccione Agregar regla.

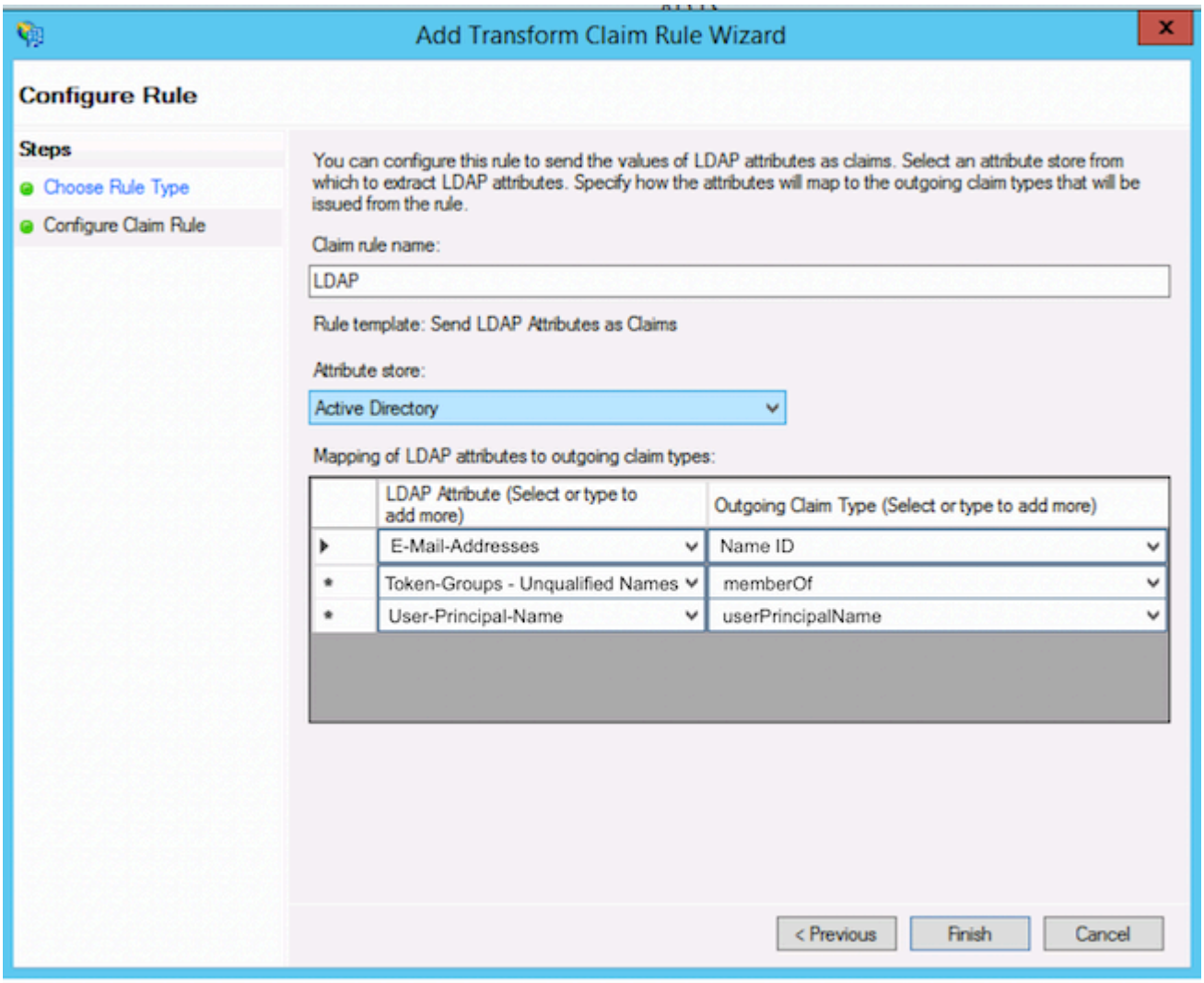


Agregar regla de transformación de emisión

Los valores que se muestran aquí son valores comunes que permiten que ESA rellene los nombres de grupo en la configuración de autenticación externa.

Consejo: Los valores de la asignación pueden variar en función de las preferencias del administrador.

Consejo: En el ejemplo que se muestra, ingrese los tipos de reclamación saliente memberOf y userPrincipalName manualmente. Seleccione Name ID en la lista desplegable.



Transformar regla de reclamación

- Seleccione Finish.

Descargue los metadatos IdP y cárguelos en ESA

Después de completar la configuración de la regla de notificación y confianza de usuario de confianza, exporte los metadatos del proveedor de identidad (IdP) y cárguelos en ESA.

⚠ Precaución: Al reiniciar el servicio AD FS se pueden interrumpir las sesiones de autenticación activas. Realice este paso durante una ventana de mantenimiento si es necesario.

- Reinicie el servicio AD FS si es necesario.
- Ejecute estos comandos:

```
net stop adfssrv
net start adfssrv
```

- Descargue el archivo de metadatos desde esta URL:

https://myserver.domain.com/FederationMetadata/2007-06/FederationMetadata.xml

- Finalice y vuelva al clúster ESA.

Verificación

1. En ESA o SMA, confirme que la importación de metadatos IdP se completa correctamente.
2. Pruebe un inicio de sesión administrativo mediante el inicio de sesión único (SSO) de SAML.
3. Compruebe que se reciben las notificaciones de grupo esperadas y que la asignación de funciones se completa según lo esperado en la configuración de autenticación externa.

Información Relacionada

-

- Dispositivo de seguridad Cisco Email Security Appliance: guías del usuario final
- Cisco Content Security Management Appliance: Guías para el usuario final

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).