Configuración de Umbrella con ADFS versión 3.0 mediante SAML

Contenido

Introducción

Este documento describe cómo configurar SAML entre Cisco Umbrella y los Servicios de federación de Active Directory (ADFS) versión 3.0.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella.

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.

Overview

En este artículo se explica cómo configurar SAML entre Cisco Umbrella y los Servicios de federación de Active Directory (ADFS) versión 3.0. La configuración de SAML con ADFS difiere de otras integraciones SAML de Umbrella, ya que no es un proceso de un clic o dos en el asistente, sino que requiere cambios en ADFS para funcionar correctamente.

En este artículo se detallan las modificaciones que debe realizar para que SAML y ADFS funcionen conjuntamente. Los pasos principales consisten en deshabilitar primero el cifrado entre su entorno ADFS y Cisco Umbrella y, a continuación, agregar algunas reglas de notificación personalizadas de transformación de emisión a la configuración de la persona que transmite Umbrella.

Realice estos pasos sólo con un ADFS existente que funcione configurado. Cisco Umbrella Support no puede proporcionar asistencia ni asistencia para configurar ADFS en un entorno concreto.

En este momento, estas instrucciones solo admiten ADFS versión 3.0 (Windows Server 2012 R2). Es posible que las versiones anteriores (2.0 o 2.1) o posteriores (4.0) de ADFS puedan funcionar con la integración de Umbrella SAML, pero esto no se ha probado ni probado. Si tiene una versión diferente de ADFS y está interesado en trabajar con nuestros equipos de soporte y productos para la integración, póngase en contacto con el equipo de soporte de Cisco Umbrella.

Puede encontrar los prerrequisitos para la configuración inicial de SAML en la documentación de Umbrella: Integraciones de identidad: Prerrequisitos. Una vez completados estos pasos, puede seguir utilizando las instrucciones específicas de ADFS de este artículo para completar la configuración.

En los pasos de la documentación de Umbrella se menciona que debe cargar los metadatos de SAML (ADFS) en Umbrella. Puede acceder a los metadatos si se desplaza hasta esta dirección URL y carga el archivo XML.

```
https://{your-ADFS-domain-name}/federationmetadata/2007-06/federationmetadata.xml
```

Desactivar cifrado

1. Abra Administración de AD FS. Expanda Relaciones de confianza y seleccione Confianzas de usuario de confianza.

2. Haga clic con el botón derecho del ratón en el usuario de confianza de Umbrella (o en el nombre que le haya dado) y seleccione Propiedades.

3. Seleccione la pestaña Encryption.

4. Seleccione Eliminar para eliminar el certificado para el cifrado.

5. Seleccione OK para cerrar la pantalla.

Adición de nuevas reglas de reclamación de transformación de emisión

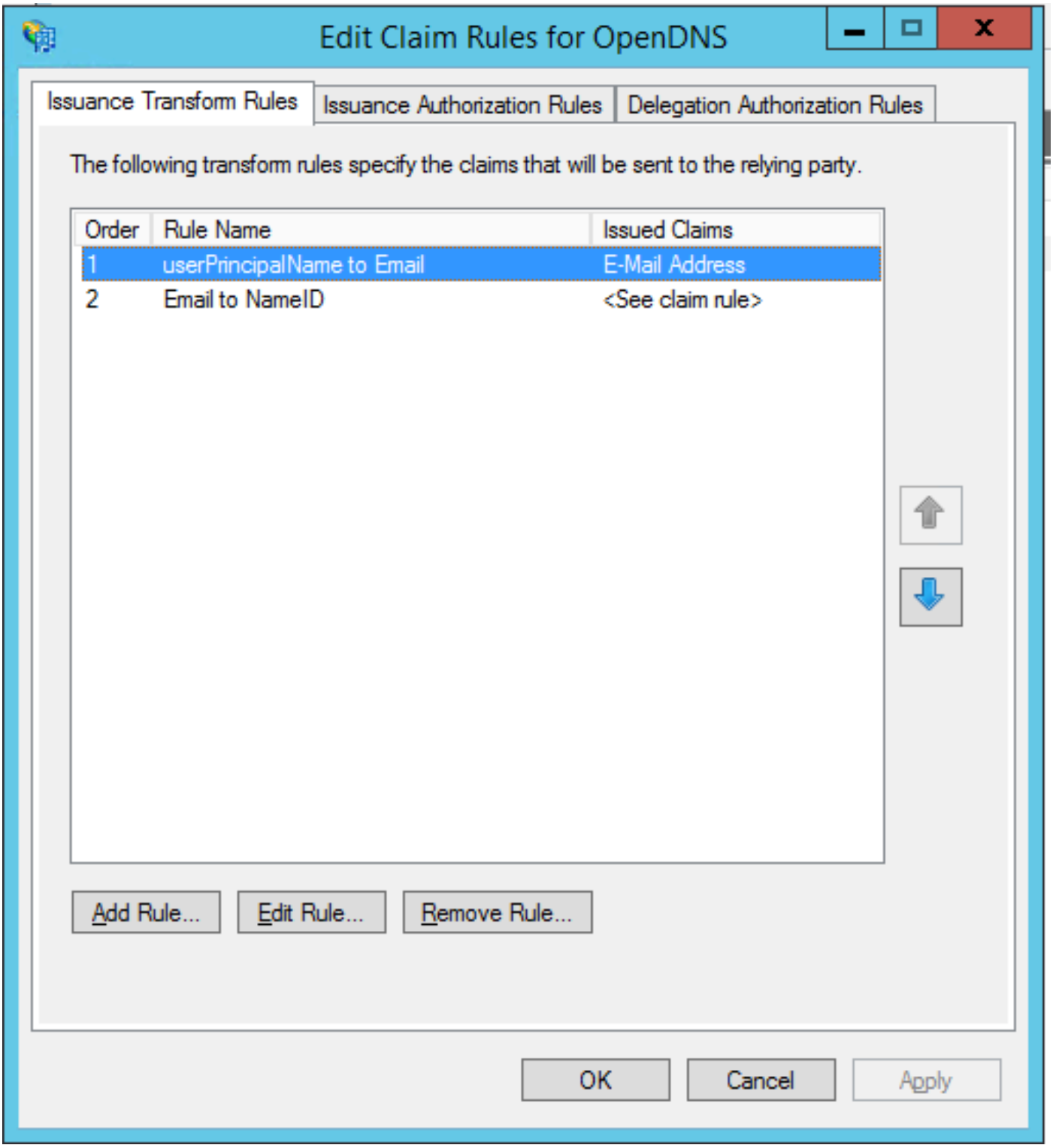
1. Abra Administración de AD FS. Expanda Relaciones de confianza y seleccione Retransmisión de confianza de partes.

2. Haga clic con el botón derecho del ratón en la persona que retransmite Umbrella (o en el nombre que le haya asignado) y seleccione Editar reglas de reclamación.

3. En Reglas de transformación de emisión, seleccione Agregar regla.

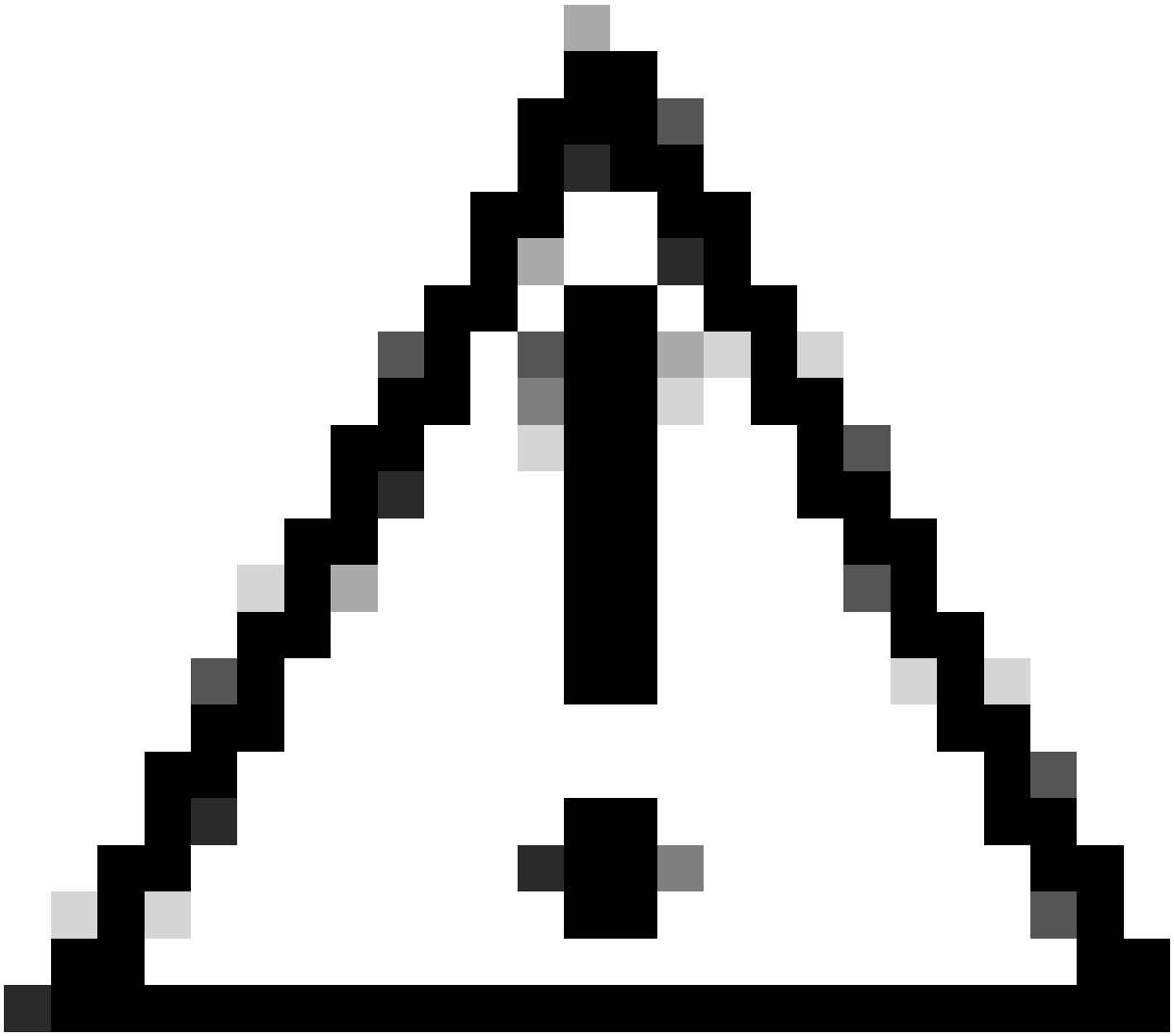
4. Seleccione Enviar justificantes de venta mediante una regla personalizada.

Consulte esta captura de pantalla para ver la lista de reglas que puede agregar.



Una vez agregadas estas reglas, la integración puede empezar a funcionar.

Reglas de transformación



Precaución: Estas reglas se probaron y funcionaron en el entorno de laboratorio ADFS de Umbrella, así como en algunos entornos de producción de clientes. Modifíquelos para que se adapten a su entorno.

userPrincipalName a dirección de correo electrónico

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/em
```

Correo electrónico a ID de nombre

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> 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:1.1:nameid-format:emailAddress");
```

Apéndice: Iniciar sesión con el atributo 'mail'

De forma predeterminada, ADFS autentica a los usuarios por su UPN (nombre principal de usuario). Si la dirección de correo electrónico del usuario (nombre de cuenta de Umbrella) no coincide con su UPN, se requieren pasos adicionales. Consulte este artículo de la base de conocimientos: ¿Cómo configuro AD FS en Cisco Umbrella Dashboard para permitir inicios de sesión con una dirección de correo electrónico?

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).