

Instalar archivo de metadatos en ADFS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo instalar el archivo de metadatos en Microsoft Active Directory Federation Services (ADFS).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- ADFS
- Integración del lenguaje de marcado de aserción de seguridad (SAML) con el dispositivo de administración de seguridad

Componentes Utilizados

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

- SMA 11.x.x
- SMA 12.x.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Antes de instalar el archivo de metadatos en el ADFS, asegúrese de que se cumplen estos requisitos:

- SAML habilitado en SMA
- Compruebe si el dispositivo de administración de seguridad de contenido de Cisco admite el proveedor de identidad utilizado por su organización. Estos son los proveedores de identidad admitidos: Servicios de federación de Microsoft Active Directory (ADFS) 2.0 Ping Identity Federate 7.2 Dispositivo de seguridad Cisco Web Security Appliance 9.1
- Obtenga los siguientes certificados necesarios para proteger la comunicación entre el dispositivo y el proveedor de identidad: Si desea que su dispositivo firme solicitudes de autenticación SAML o si desea que su proveedor de identidad cifre las aserciones SAML, obtenga un certificado autofirmado o un certificado de una autoridad de certificación (CA) de confianza y la clave privada asociada. Si desea que el proveedor de identidad firme afirmaciones SAML, obtenga el certificado del proveedor de identidad. Su dispositivo utiliza este certificado para verificar las afirmaciones de SAML firmadas

Configurar

Paso 1. Navegue hasta su SMA y seleccione **Administración del sistema > SAML > Descargar metadatos**, como se muestra en la imagen.

The screenshot shows the SMA web interface. At the top, there are tabs for 'Management Appliance', 'Email', and 'Web'. Below that, there are tabs for 'Centralized Services', 'Network', and 'System Administration'. The 'SAML' section is active. Under 'Service Provider', there is a table with the following data:

SP Profile Name	Entity ID	Assertion Consumer URL	Metadata	Delete
MyLab_SAML	sma.mexesa.com	https://sma.mexesa.com:83/	Download Metadata	

Below the table, there is an 'Identity Provider' section with the text 'No Identity Provider Profiles have been defined.' A red arrow points from the 'Download Metadata' button in the table to a Firefox dialog box that has opened. The dialog box title is 'Opening MyLab_SAML_metadata.xml'. It contains the following text:

You have chosen to open:

MyLab_SAML_metadata.xml
which is: XML file
from: https://10.31.124.137

What should Firefox do with this file?

Open with Notepad++ : a free (GNU) source code editor (d...)

Save File

Do this automatically for files like this from now on.

Buttons: OK, Cancel

Paso 2. El perfil del proveedor de identidad se rellena automáticamente cuando el cliente carga su archivo de metadatos ADFS. Microsoft tiene una URL predeterminada: **https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml**.

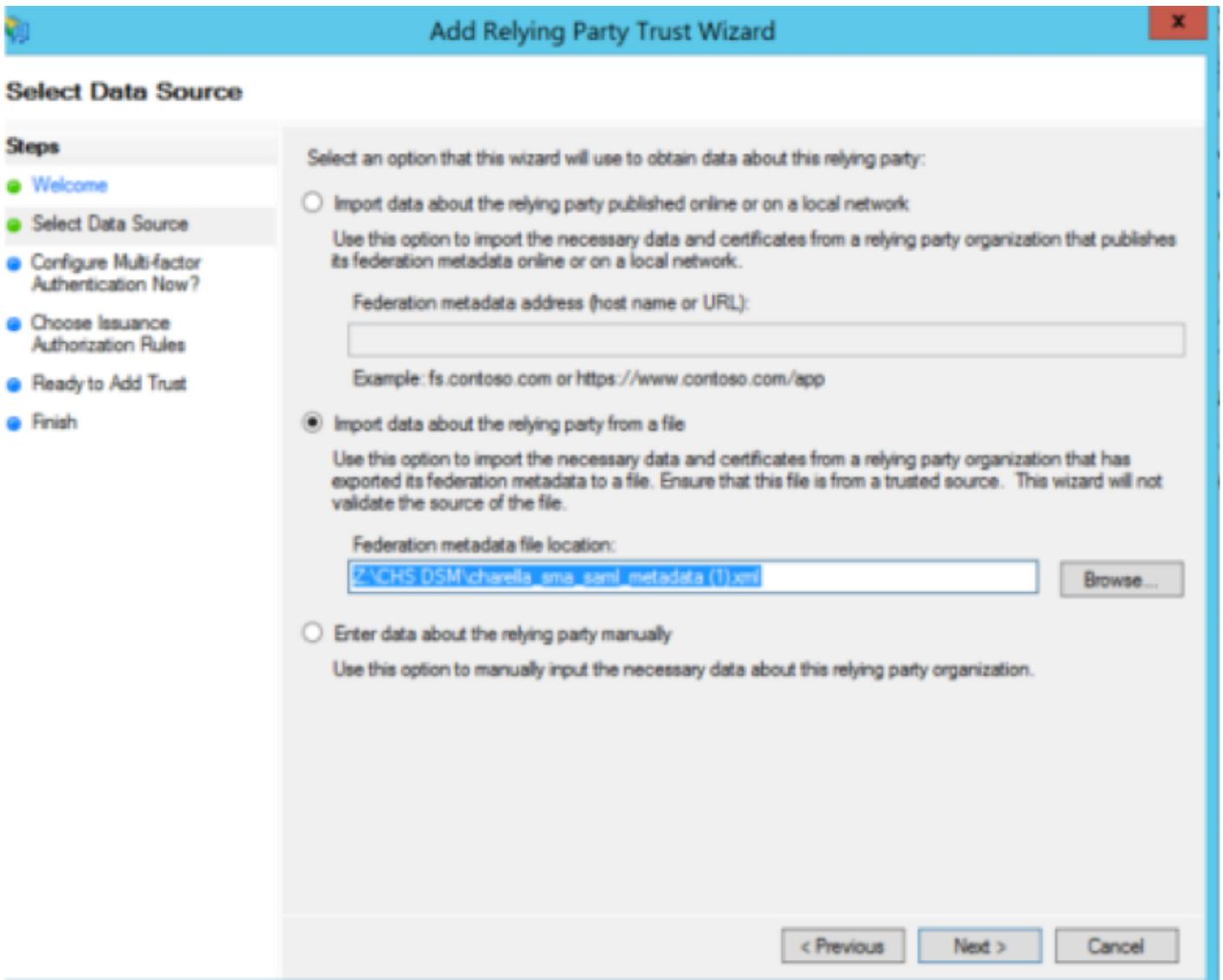
Paso 3. Una vez configurados ambos perfiles, se deben editar los metadatos del perfil SP, según el error [CSCvh30183](#). El archivo de metadatos aparece como se muestra en la imagen.

```

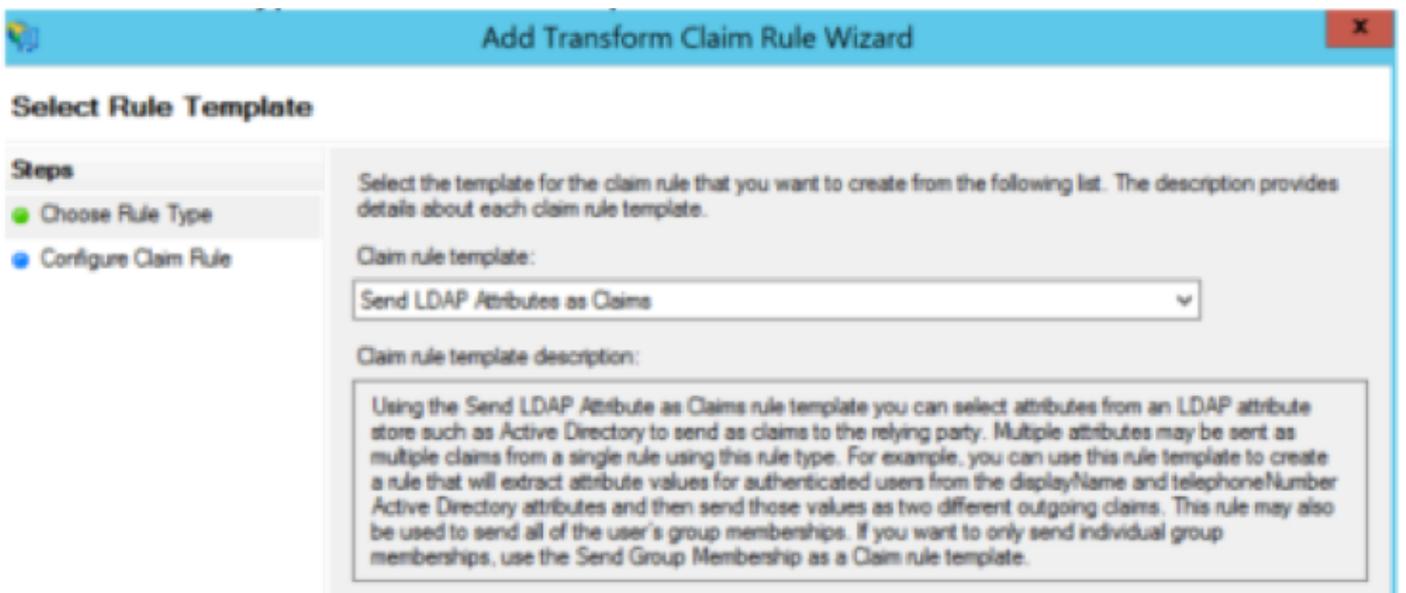
1  <?xml version="1.0"?>
2  <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
3      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
4      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
5      entityID="sma.mexesa.com">
6      <SPSSODescriptor
7          AuthnRequestsSigned="false" WantAssertionsSigned="true"
8          protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
9          <KeyDescriptor use="signing">
10             <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
11                 <ds:X509Data>
12                     <ds:X509Certificate>Bag Attributes
13                         localKeyID: D5 4F B4 DA BC 91 71 5C 53 94 4A 78 E0 4A C3 EF C4 BD 4C 8D
14                         friendlyName: sma.mexesa.com
15                         subject=/C=MX/CN=sma.mexesa.com/L=CDMX/O=Tizoncito Inc/ST=CDMX/OU=IT Security
16                         issuer=/C=MX/CN=sma.mexesa.com/L=CDMX/O=Tizoncito Inc/ST=CDMX/OU=IT Security
17                         -----BEGIN CERTIFICATE-----
18                         MIIDZTCCAk2gAwIBAwIJA0jXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHlxZAJBgNV
19                         BAYTAK1YMRcwFQYDVQQDDA5zbWEubWV4ZXXNhLmNvbTENCAsGA1UEBwwEQ0RNWDEW
20                         MBQGA1UECgwNVG16b25jaXRvIEluYzENMAAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
21                         SVQGU2VjdXJpdHkwHhcNMjkwNjA0MjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
22                         CQYDVQQGEwJNWDEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
23                         TVGxZjAUBGNVBAoMDVRpem9uY210byBJbmMxDTALBgNVBAGMBENETVgxZDASBgNV
24                         BAsMC0lUIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
25                         g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFPcJgn/oHXEUKvUnWe+9cTJQ41X4
26                         ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNyv8Wtd+Io
27                         MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rnO4jtvPZp7B
28                         cpWjawLlxAfUHVyvrc661Tblo0exG+hZ+AlS3B0l+6lmTNjF3IcGcGS/TE0chETx
29                         glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+LkF8As8B1Pm6YHi
30                         L6K8W4vOEj1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB3vxNL7jb
31                         emMTKSRP4hycUld69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFii2oOJ6yGEOdWD
32                         6+Bvj6wSBp7UoLyBdCcxglyi+vK4Y/R2+iCv13pyaXkbf0QsJvYpzOg7xSjKxZm79
33                         +ZiJQkekyCAM5N0of1ZRrJ9oGD5qoYlZjhud7NHmRbj7LKHrKsFVqpKet/tTXCH7
34                         7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVPxxKacjAVj/ZclXnPBGSMxexo277ECJq
35                         ix5aXRSxOMRRtD/72FVRAsGT3xlmBYqu/HTyOBZongM+isJHBhRZxSOMBL+45jFY
36                         PO1jBG5MZuWE
37                         -----END CERTIFICATE-----
38                 </ds:X509Certificate>
39             </ds:X509Data>

```

Paso 4. Quite la información resaltada, al final el archivo de metadatos debe ser como se muestra en la imagen.



Paso 6. Después de importar correctamente el archivo de metadatos, configure las reglas de reclamación para la confianza de la parte que confía recientemente, seleccione la **plantilla de regla reclamación > Enviar atributos LDAP**, como se muestra en la imagen.



Paso 7. Asigne el nombre de la regla de reclamación y seleccione **Almacén de atributos > Active Directory**.

Paso 8. Asignar atributos LDAP, como se muestra en la imagen.

- Atributo LDAP > Direcciones de correo electrónico
- Tipo de reclamación saliente > Dirección de correo electrónico

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: charella_sma

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

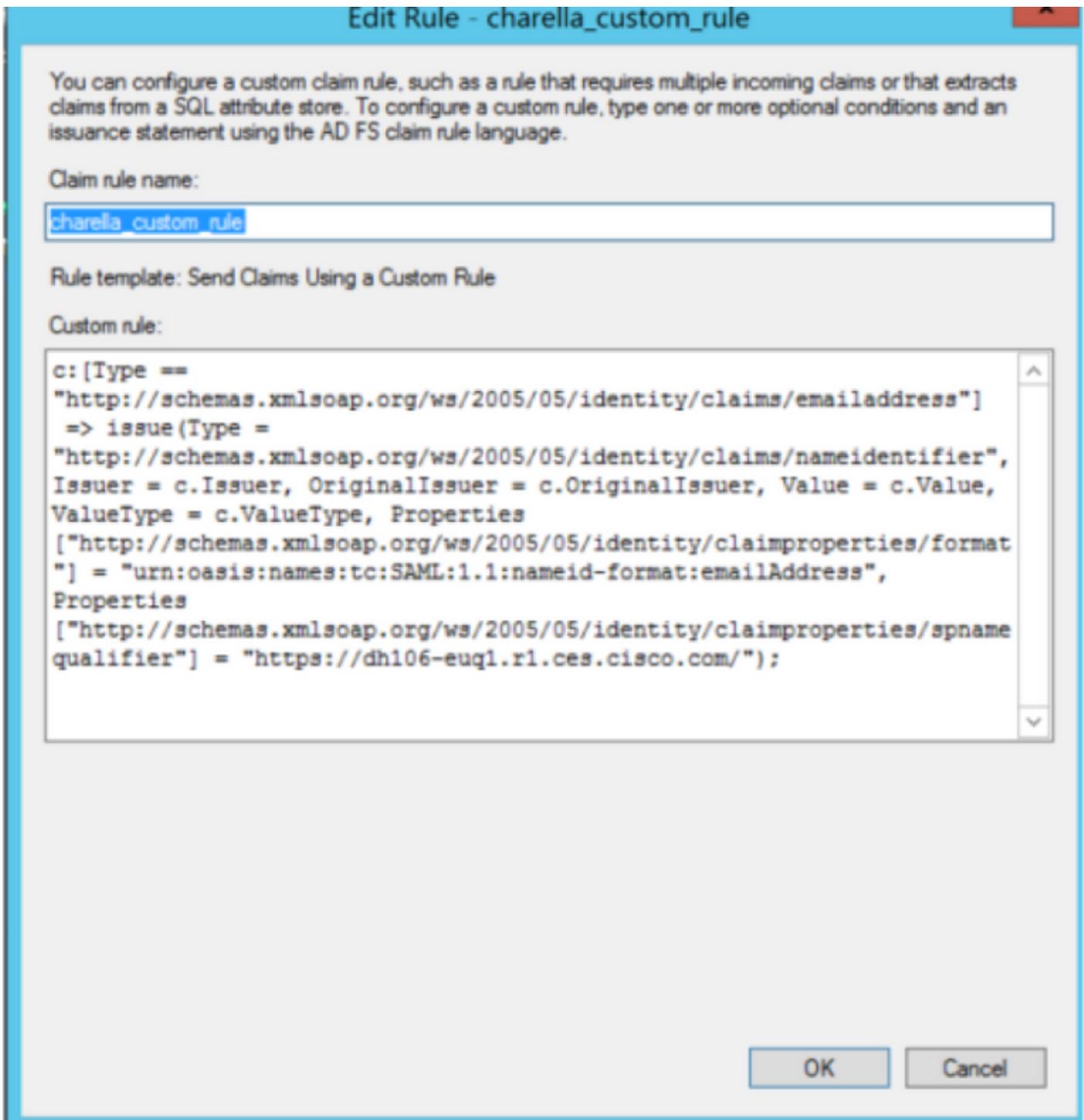
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	E-Mail Address
*		

< Previous Finish Cancel

Paso 9. Cree una nueva regla de reclamación personalizada con esta información, como se muestra en la imagen.

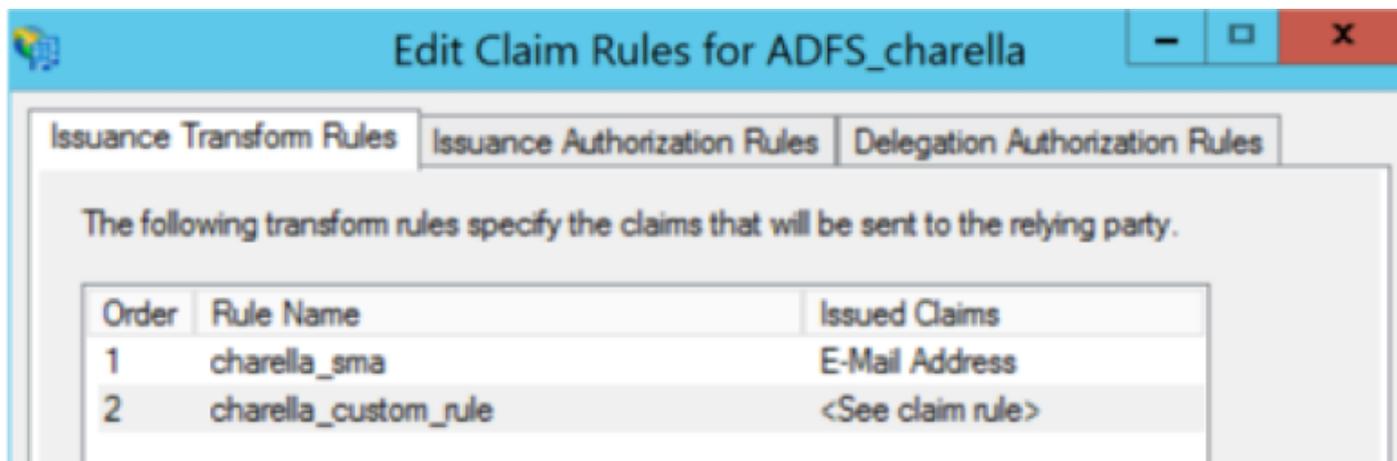
Ésta es la regla personalizada que debe agregarse a la regla de reclamación personalizada:

```
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",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier
"] = "https://<smahostname>:83");
```



- Modifique la dirección URL resaltada con el nombre de host y el puerto de SMA (si se encuentra en un entorno de CES, no se necesita un puerto pero debe apuntar a euq1.<location>.iphmx.com)

Paso 10. Asegúrese de que el orden de la regla de reclamación es: Regla de reclamación LDAP primero y regla de reclamación personalizada en segundo lugar, como se muestra en la imagen.



Paso 11. Inicie sesión en la EUQ, debe redirigir al host ADFS.

Verificación

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

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [CSCvh30183](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)