Instalar archivo de metadatos en ADFS

Contenido

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.

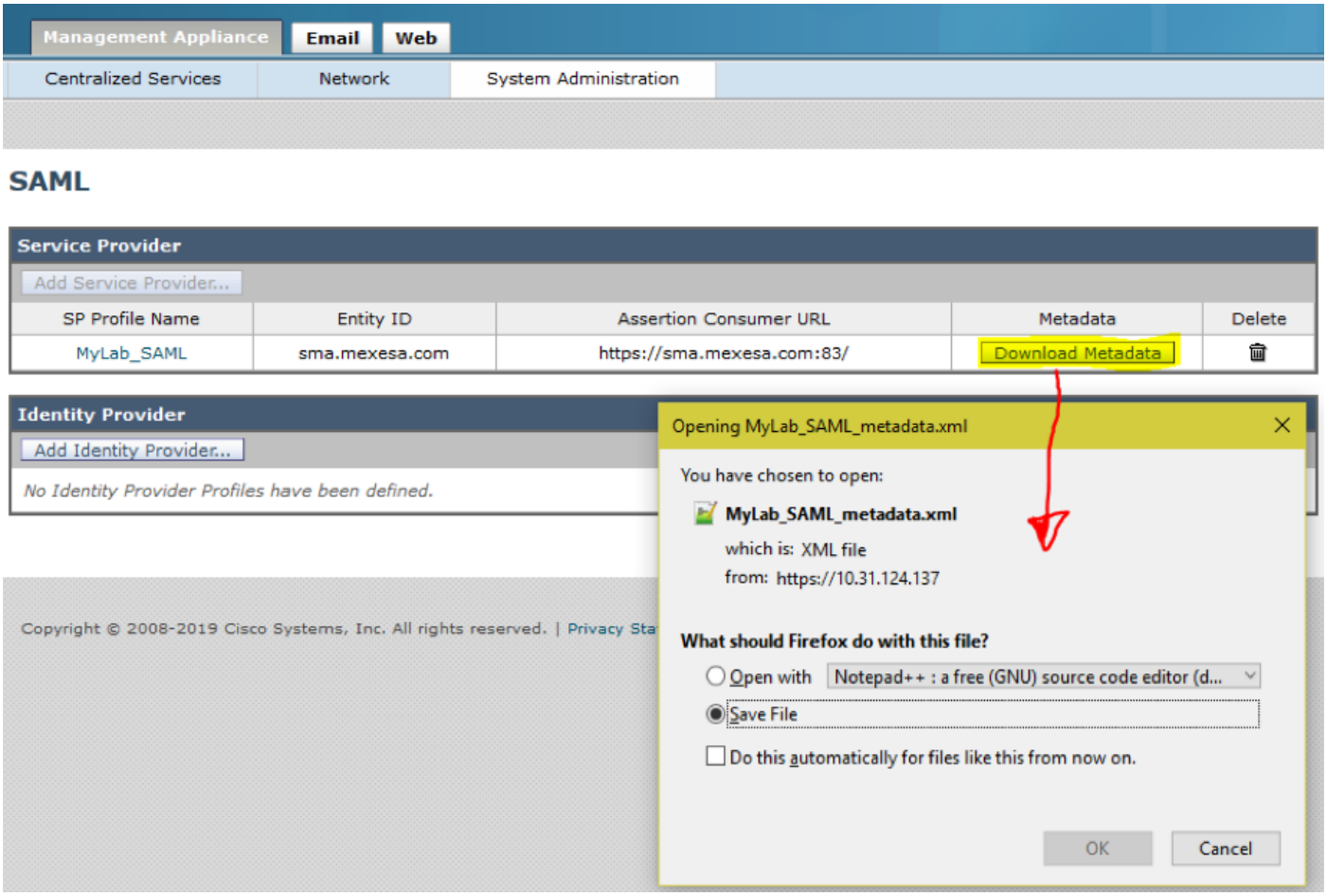
Antecedentes

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) 2.0Ping Identity Federate 7.2Dispositivo 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.



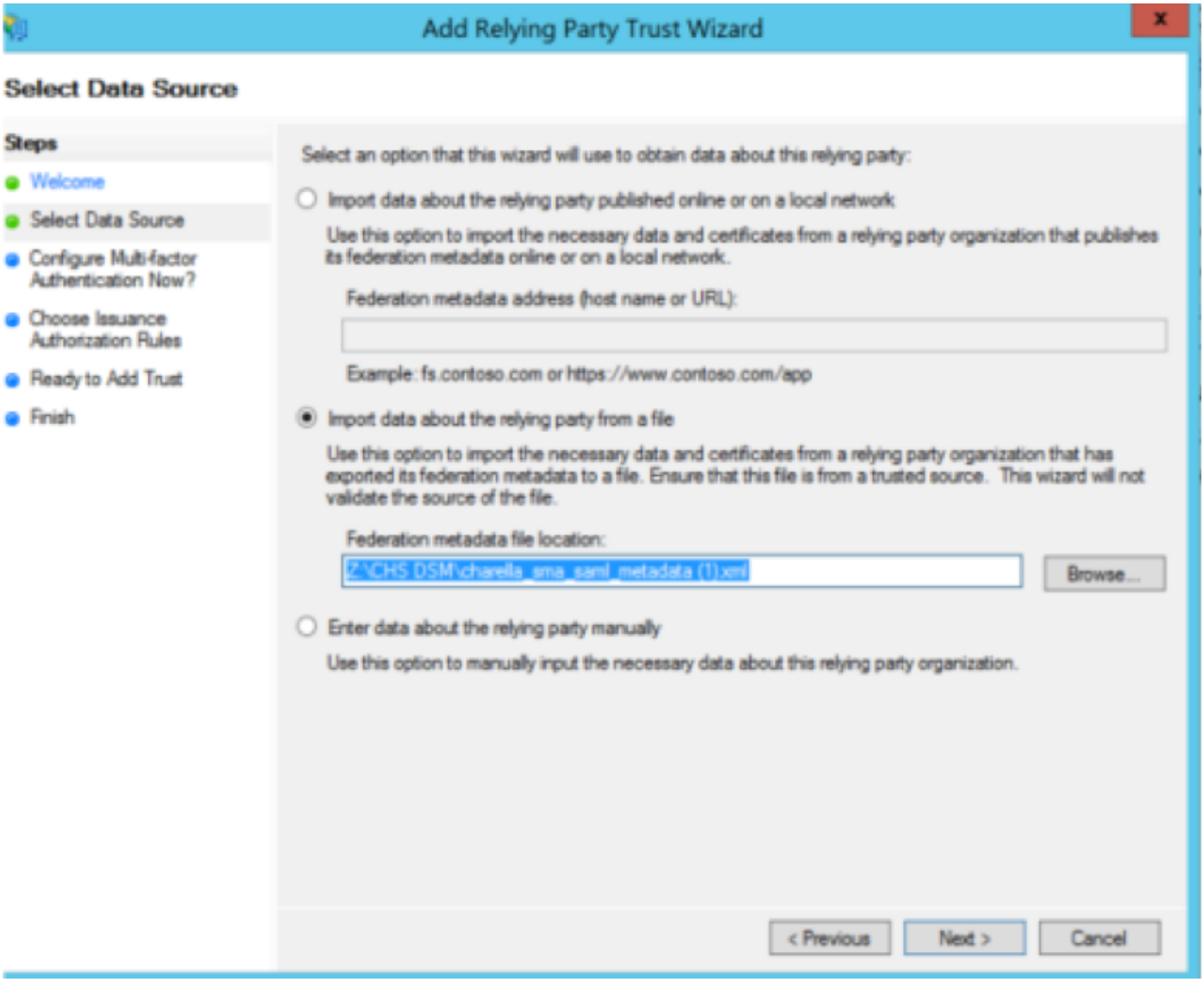
Paso 2. El perfil del proveedor de identidad se rellena automáticamente cuando el cliente carga su archivo de metadatos ADFS. Microsoft tiene una URL predeterminada: **https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml.**

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.

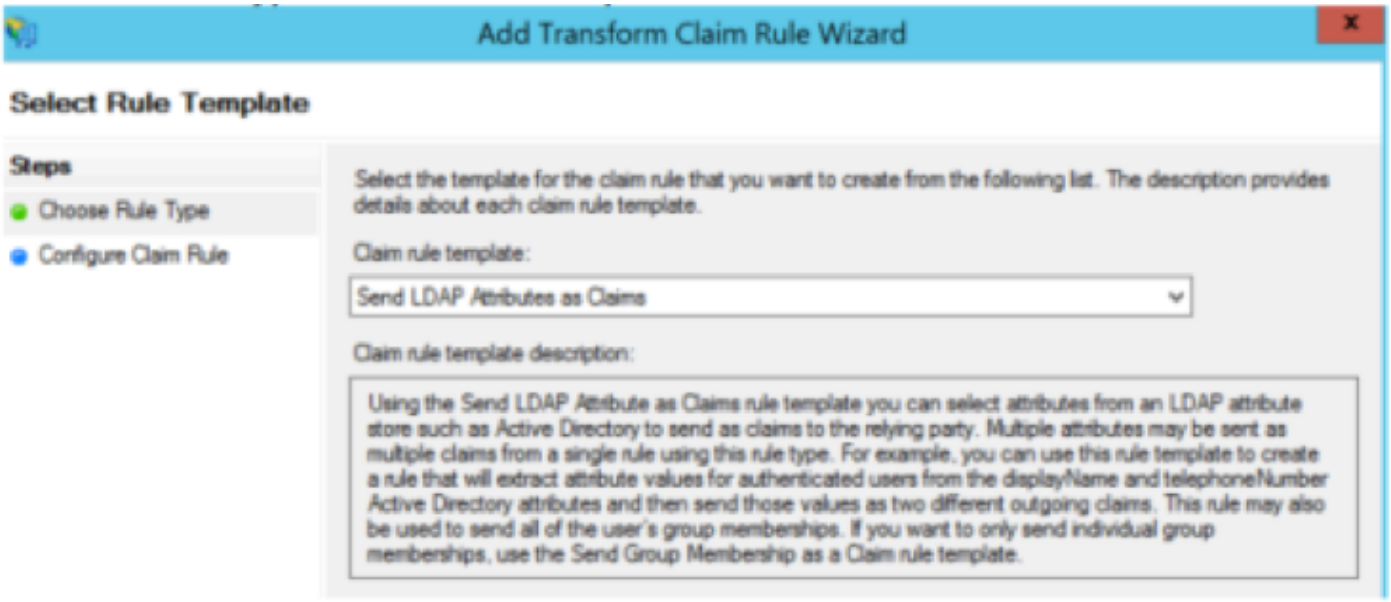
Paso 4. Quite la información resaltada, al final el archivo de metadatos debe ser como se muestra en la imagen.

```
<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
      entityID="sma.mexesa.com">
  <SPSSODescriptor
      AuthnRequestsSigned="false"  WantAssertionsSigned="true"
      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
MIIDZTCCAk2gAwIBAwIJAOjXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1UEBwwEQ0RNWDEW
MBQGA1UECgwNVGl6b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWhcNMjAwNjA0MjEwNTUxWjByMQsw
CQYDVQQGEwJNWDEXMBUGA1UEAwwOc21hLm1leGVzYS5jb20xDTALBgNVBAcMBENE
TVgxFjAUBgNVBAoMDVRpem9uY2l0byBJbmMxDTALBgNVBAgMBENETVgxFDASBgNV
BAsMC0lUIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFPcJgn/oHXEUKvUnWe+9cTJQ41X4
ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNyv8Wtd+Io
MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rnO4jtvpZPj7B
cpWjawLlxAfUHVyvrc661Tblo0exG+hZ+AlS3B0l+6lmTNjF3IcGcGS/TE0chETx
glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+LkF8As8B1Pm6YHi
L6K8W4vOEj1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBy3vxNL7jb
emMTKSRP4hycU1d69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFii2oOJ6yGEOdWD
6+Bvj6wSBp7UoLyBdCxglyi+vK4Y/R2+iCv13pyaXkbf0QSJvYpzOg7xSjkxZm79
+ZIjQkekyCAM5N0Of1ZRrJ9oGD5qoYlZjhuD7NHmRBj7LKHRKsFVqpKet/tTXCH7
7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVPxxKacjAVj/Zc1XnPBGSMxeo277ECJq
ix5aXRSxOMRRtD/72FVRAsgT3x1mBYqu/HTyOBZonGM+isJHBhRZxSOMBL+45jFY
PO1jBG5MZuWE
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <KeyDescriptor use="encryption">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
MIIDZTCCAk2gAwIBAwIJAOjXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1UEBwwEQ0RNWDEW
MBQGA1UECgwNVGl6b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWhcNMjAwNjA0MjEwNTUxWjByMQsw
```

Paso 5. Navegue hasta su ADFS e importe el archivo de metadatos editado en **ADFS Tools > AD FS Management > Add Reliying Party Trust**, como se muestra en la imagen.



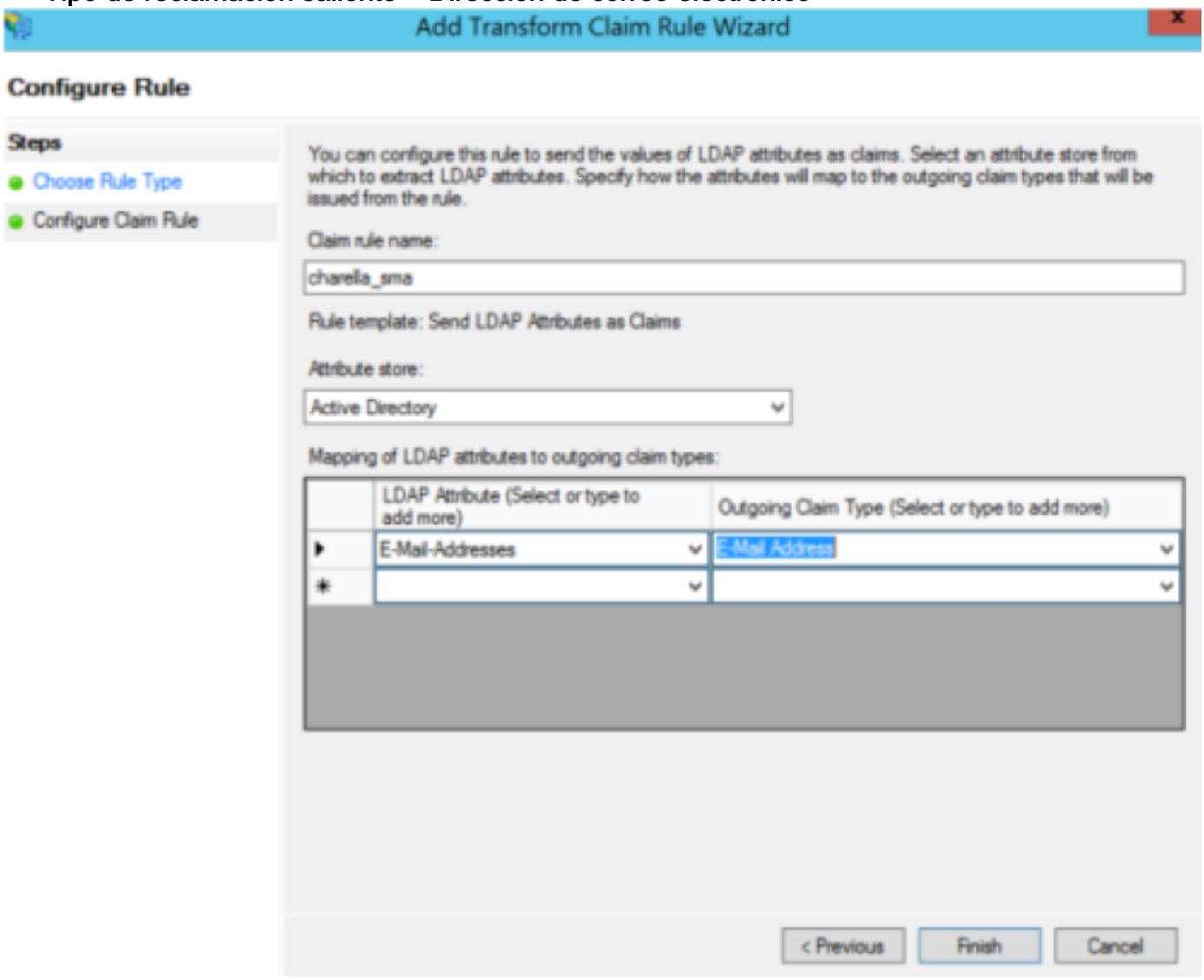
Paso 6. Después de importar correctamente el archivo de metadatos, configure las reglas de reclamación para la confianza de la parte que confía recientemente, seleccione la **plantilla de regla reclamación > Enviar atributos LDAP**, como se muestra en la imagen.



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.

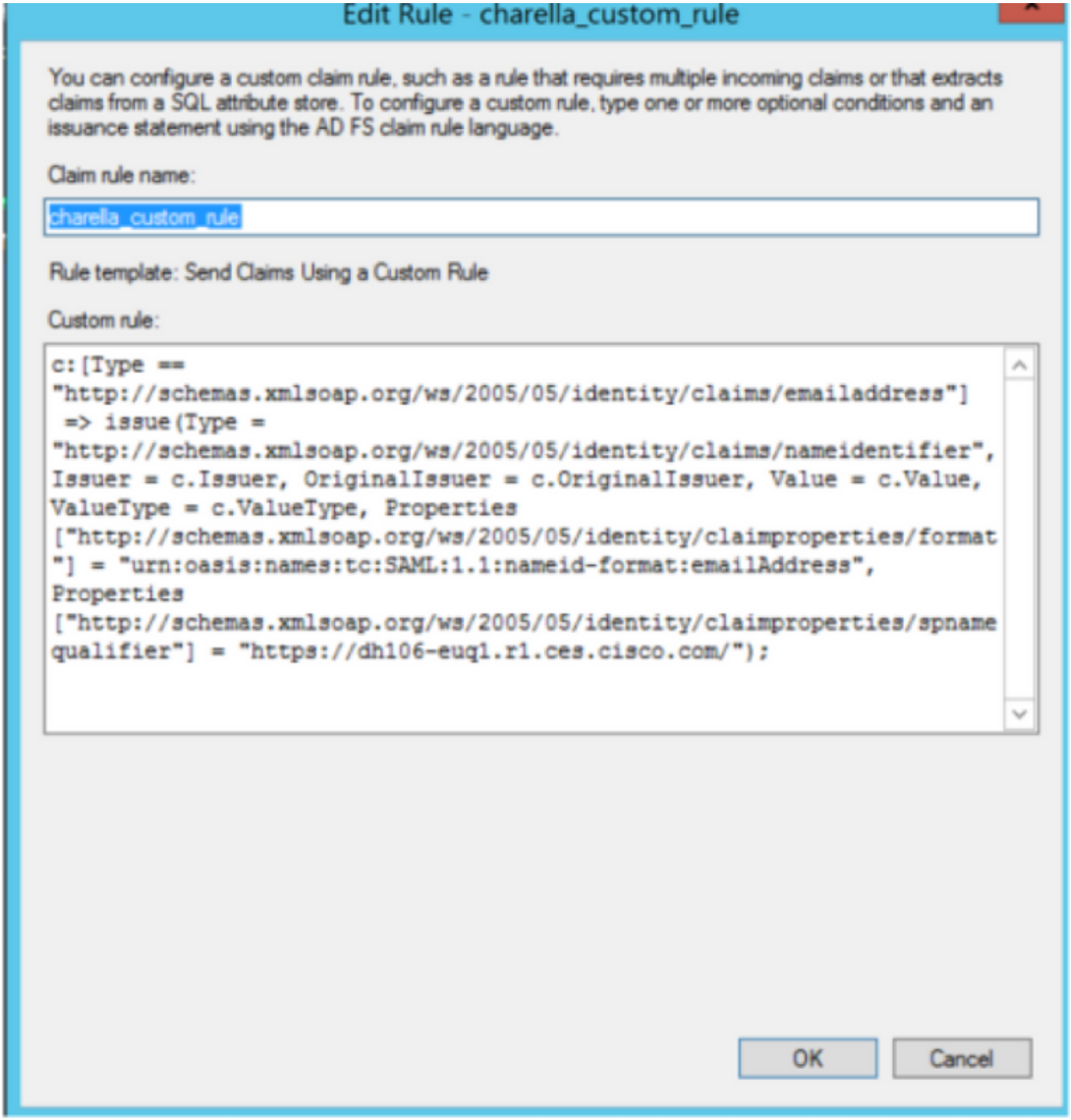
- **Atributo LDAP > Direcciones de correo electrónico**
- **Tipo de reclamación saliente > Dirección de correo electrónico**



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

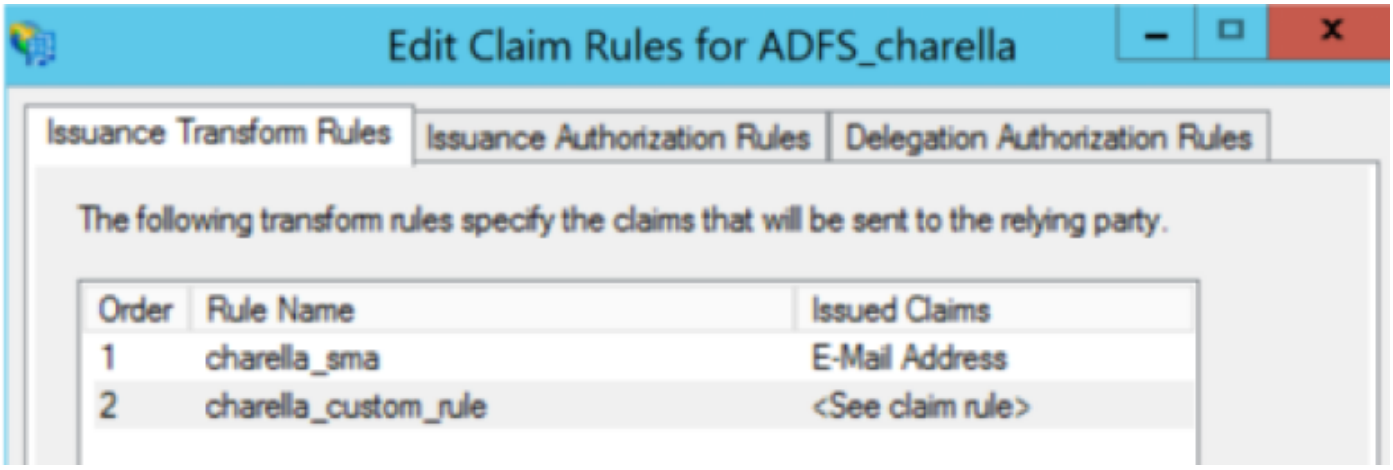
Ésta es la regla personalizada que debe agregarse a la regla de reclamación personalizada:

```
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