

Instalar arquivo de metadados no ADFS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como instalar o arquivo de metadados no Microsoft Active Directory Federation Services (ADFS).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ADFS
- Integração do Security Assertion Markup Language (SAML) com o Security Management Appliance

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Antes de instalar o arquivo de metadados no ADFS, certifique-se de que estes requisitos sejam atendidos:

- SAML habilitado no SMA

- Verifique se o provedor de identidade usado pela sua organização é compatível com o Cisco Content Security Management Appliance. Estes são os provedores de identidade suportados: Serviços de Federação do Microsoft Active Directory (ADFS) 2.0 Ping Identity Ping Federate 7.2 Cisco Web Security Appliance 9.1
- Obtenha os certificados necessários para proteger a comunicação entre seu dispositivo e o provedor de identidade: Se quiser que o aplicativo assine solicitações de autenticação SAML ou se quiser que o provedor de identidade criptografe asserções SAML, obtenha um certificado autoassinado ou um certificado de uma autoridade de certificação (CA) confiável e a chave privada associada. Se desejar que o provedor de identidade assine asserções SAML, obtenha o certificado do provedor de identidade. Seu aplicativo usa esse certificado para verificar as asserções SAML assinadas

Configurar

Etapa 1. Navegue até o SMA e selecione **Administração do sistema > SAML > Fazer download de metadados**, como mostrado na imagem.

The screenshot shows the Cisco 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 'System Administration' tab is selected, and 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	

The 'Download Metadata' button in the table is highlighted in yellow. A red arrow points from this button 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.

At the bottom of the dialog box are 'OK' and 'Cancel' buttons.

Etapa 2. O perfil do provedor de identidade é preenchido automaticamente quando o cliente carrega seu arquivo de metadados ADFS. A Microsoft tem um URL padrão: <https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml>.

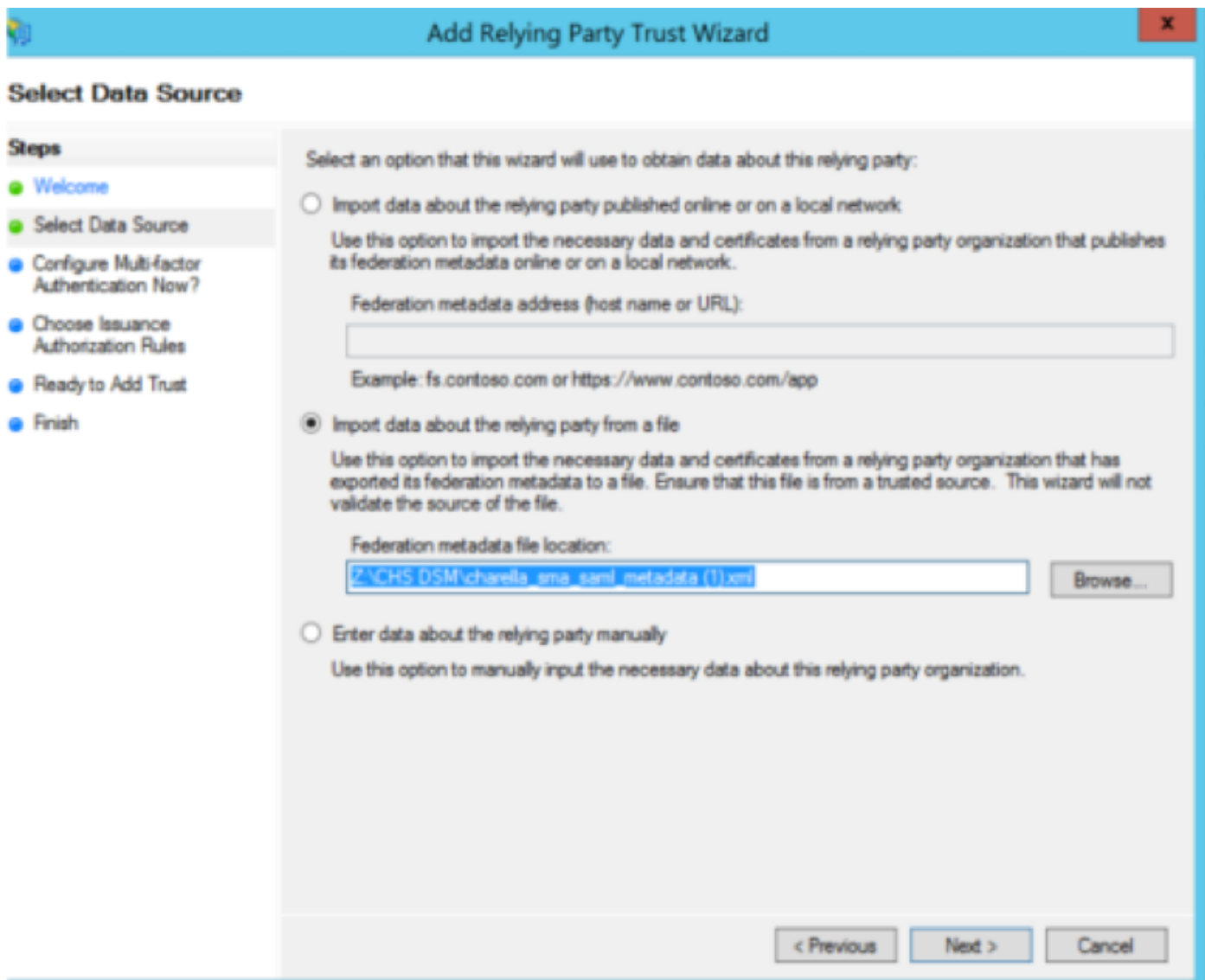
Etapa 3. Quando ambos os perfis estiverem configurados, os metadados do perfil SP devem ser editados, conforme o bug [CSCvh30183](https://bugzilla.mozilla.org/show_bug.cgi?id=CSCvh30183). O arquivo de metadados é exibido como mostrado na imagem.

```

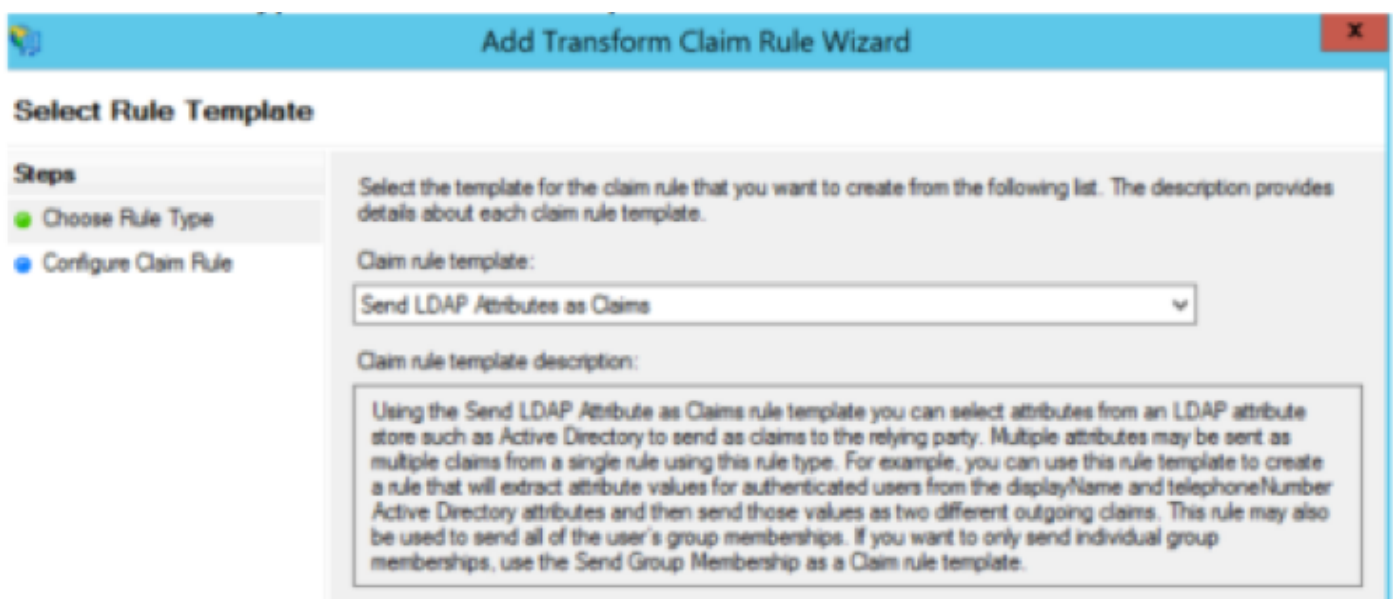
1  <?xml version="1.0"?>
2  <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
3      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
4      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
5      entityID="sma.mexesa.com">
6      <SPSSODescriptor
7          AuthnRequestsSigned="false" WantAssertionsSigned="true"
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                         MBQGA1UECgwNVG16b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
21                         SVQGU2VjdXJpdHkwHhcNMjkwNjA1MjEwNTUxWWhcNMjAwNjEwNTUxWjByMQsw
22                         CQYDVQQGEwJNWDEwXG16b25jaXRvIEluYzENMAsGA1UEAwwOcm1leGVzYS5jb20xDTALBgNVBACMBENE
23                         TVGxVjAUBGNVBAoMDVRpem9uY210byBJbmMxDTALBgNVBAGMBENETVgxFDASBgNV
24                         BAsMC0lUIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
25                         g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFPcJgn/oHXEUkVUnWe+9cTJQ41X4
26                         ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNyv8Wtd+Io
27                         MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rnO4jtvPZp7B
28                         cpWjawLlxAfUHVyvrC661Tblo0exG+hZ+AlS3B01+61mTNjF3IcGcGS/TE0chETx
29                         glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+LkF8As8B1Pm6YHi
30                         L6K8W4vOEj1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB3vxNL7jb
31                         emMTKSRP4hycUld69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFii2oOJ6yGEOdWD
32                         6+Bvj6wSBp7UoLyBdCxglyi+vK4Y/R2+iCv13pyaXkbf0QsJvYpzOg7xSjKxZm79
33                         +ZiJQkekyCAM5N0of1ZRrJ9oGD5qoYlZjhuD7NHmRbj7LKHrKsFVqpKet/tTXCH7
34                         7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVPxxKacjAVj/ZclXnPBGSMxexo277ECJq
35                         ix5aXRSxOMRRtD/72FVRAsGT3x1mBYqu/HTyOBZongM+isJHBhRZxSOMBL+45jFY
36                         PO1jBG5MZuWE
37                         -----END CERTIFICATE-----
38                 </ds:X509Certificate>
39             </ds:X509Data>

```

Etapa 4. Remova as informações realçadas, no final, o arquivo Metadados deve estar conforme mostrado na imagem.



Etapa 6. Depois de importar com êxito o arquivo de metadados, configure as regras de reivindicação para a confiança de terceira parte confiável recém-criada, selecione **Claim rule template > Send LDAP Attributes**, como mostrado na imagem.



Passo 7. Nomeie o nome da regra de Reivindicação e selecione **Repositório de atributos > Ative Directory**.

Etapa 8. Mapear atributos LDAP, como mostrado na imagem.

- Atributo LDAP > Endereços de e-mail
- Tipo de solicitação de saída > Endereço de e-mail

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:

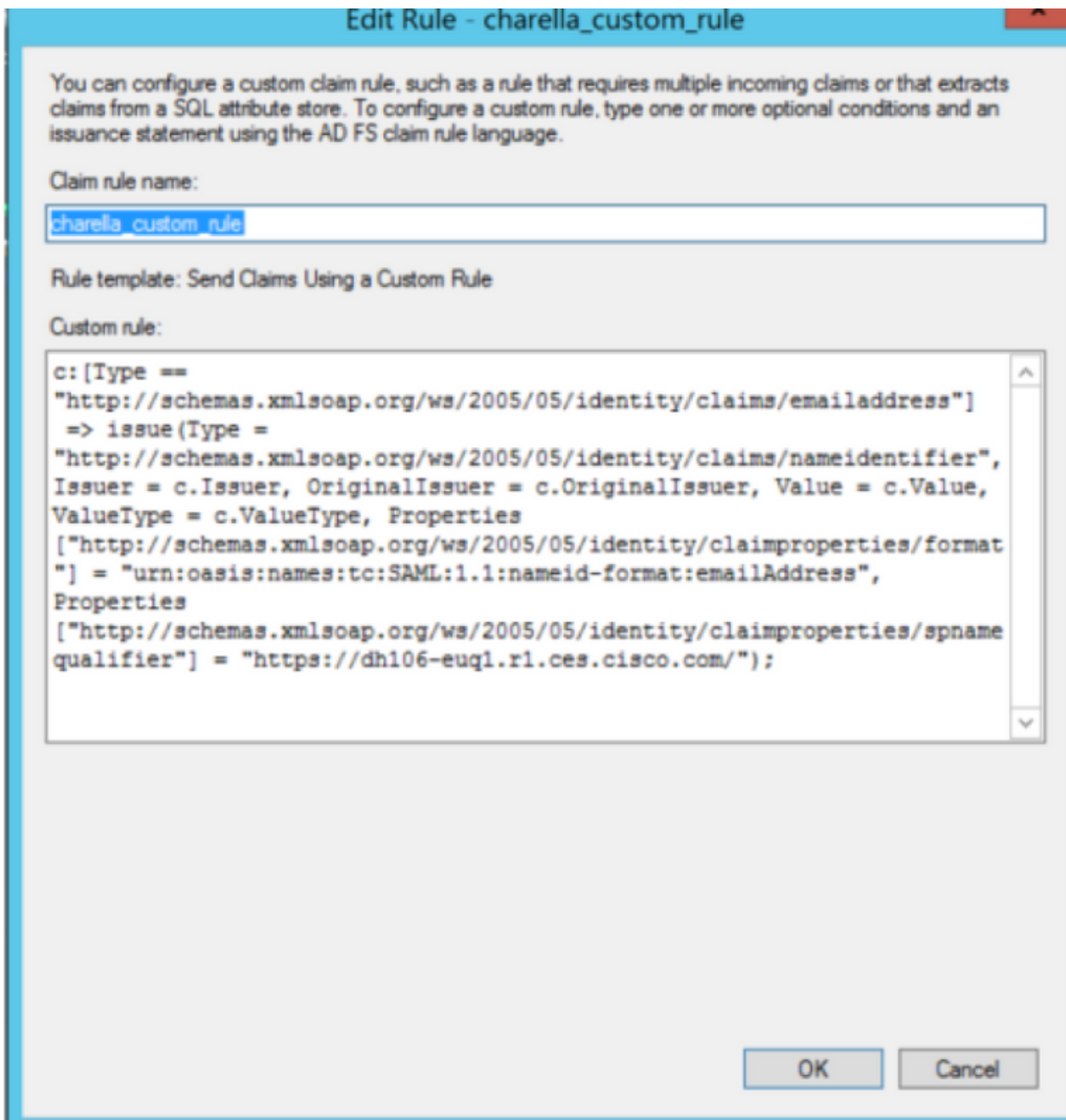
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	E-Mail Address
*		

< Previous Finish Cancel

Etapa 9. Crie uma nova regra de Reivindicação personalizada com essas informações, como mostrado na imagem.

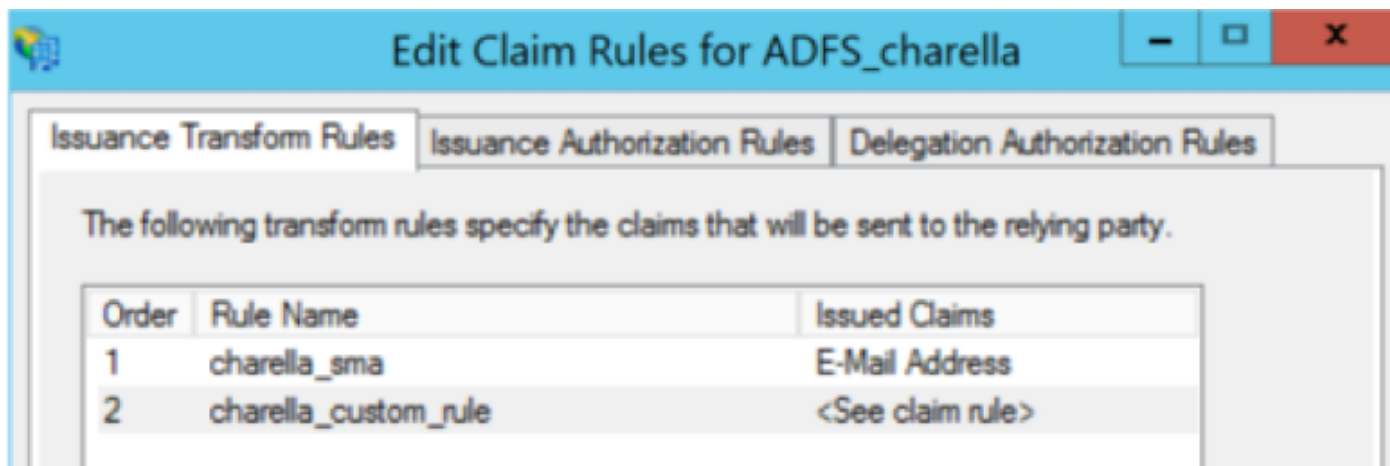
Esta é a regra personalizada que precisa ser adicionada à regra de Reivindicação personalizada:

```
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 a URL realçada com o nome de host e a porta SMA (se você estiver em um ambiente CES, uma porta não será necessária, mas deve apontar para euq1.<alocação>.iphmx.com)

Etapa 10. Certifique-se de que o pedido da regra de Reivindicação seja: A regra de afirmação LDAP primeiro e a regra de solicitação personalizada em segundo lugar, como mostrado na imagem.



Etapa 11. Faça login no EUQ e redirecione para o host ADFS.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- [CSCvh30183](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)