Instalar arquivo de metadados no ADFS

Contents

Introduction

Este documento descreve como instalar o arquivo de metadados no Microsoft Ative Diretory 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

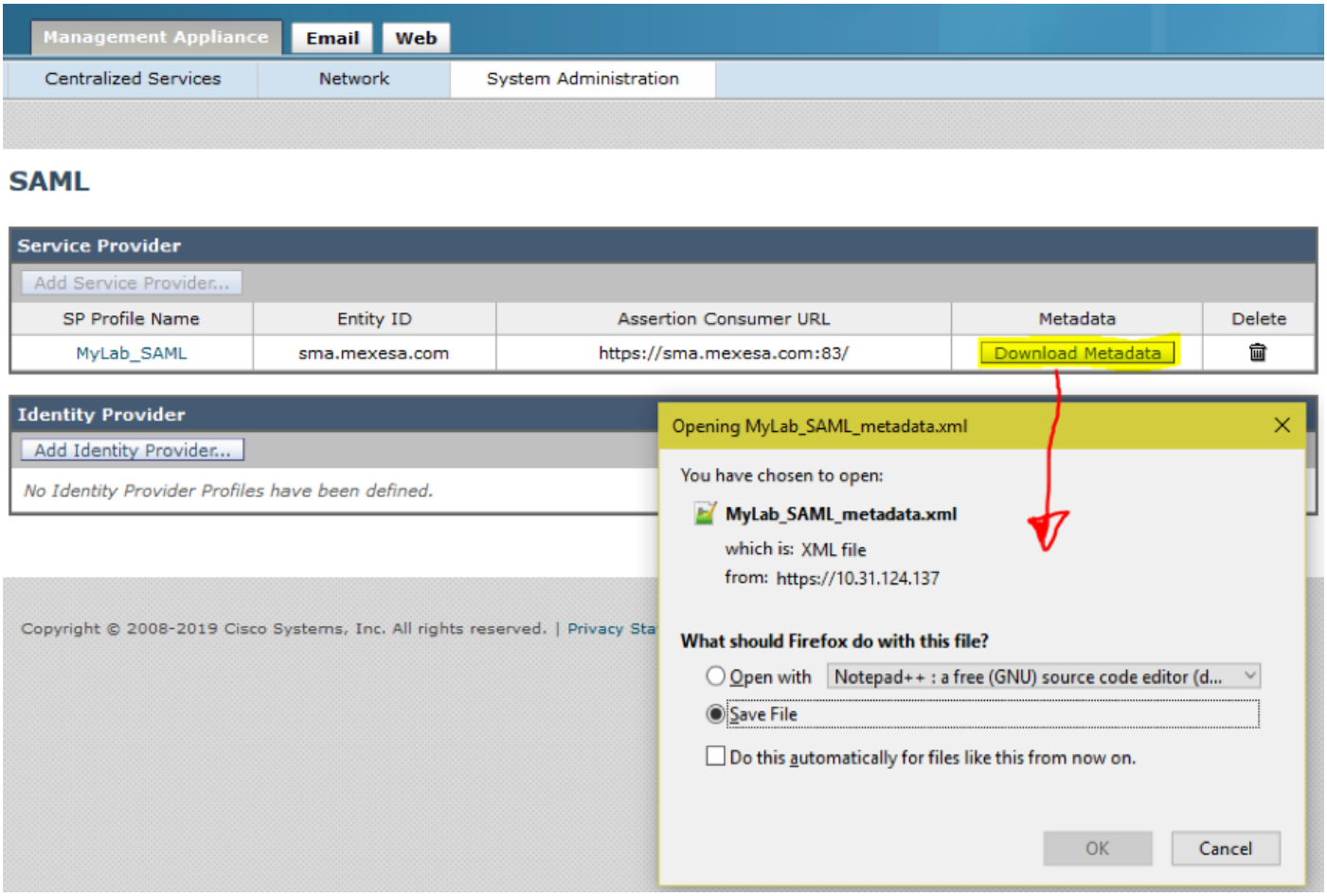
Antes de instalar o arquivo de metadados no ADFS, certifique-se de que estes requisitos sejam atendidos:

- 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 Ative Diretory (ADFS) 2.0Ping Identity Ping Federate 7.2Cisco 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.



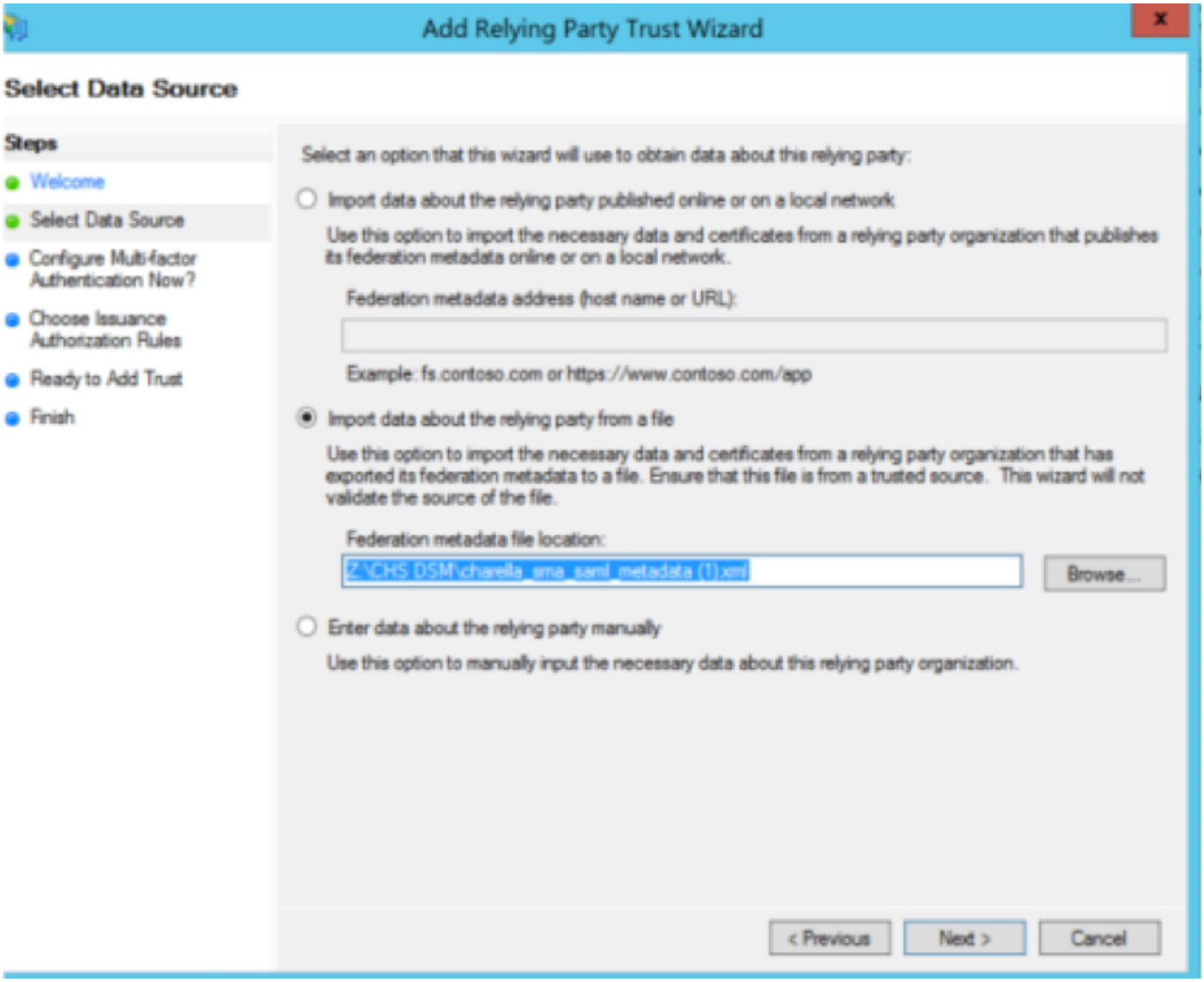
Etapa 2. O perfil do provedor de identidade é preenchido automaticamente quando o cliente carrega seu arquivo de metadados ADFS. A Microsoft tem um URL padrão: **https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml.**

Etapa 3. Quando ambos os perfis estiverem configurados, os metadados do perfil SP devem ser editados, conforme o bug CSCvh30183.. O arquivo de metadados é exibido como mostrado na imagem.

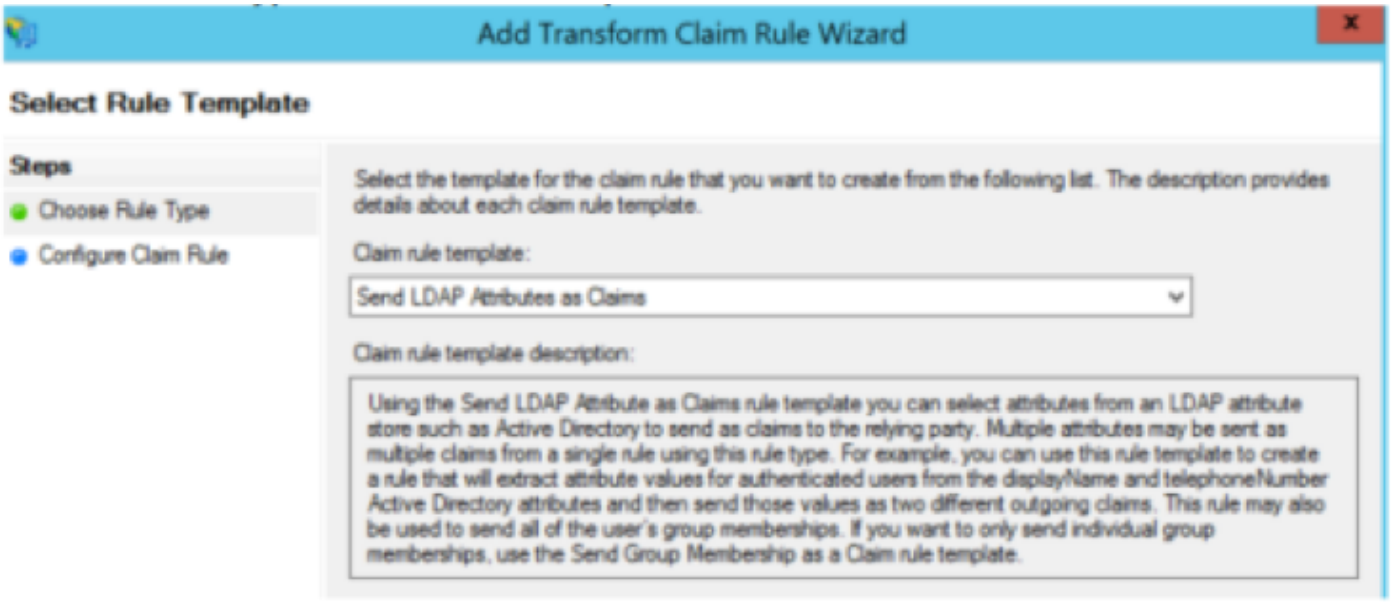
Etapa 4. Remova as informações realçadas, no final, o arquivo Metadados deve estar conforme mostrado na imagem.

```
<?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
```

Etapa 5. Navegue até seu ADFS e importe o arquivo de metadados editados nas **Ferramentas ADFS > Gerenciamento do AD FS > Adicionar Confiança de terceira parte confiável**, como mostrado na imagem.



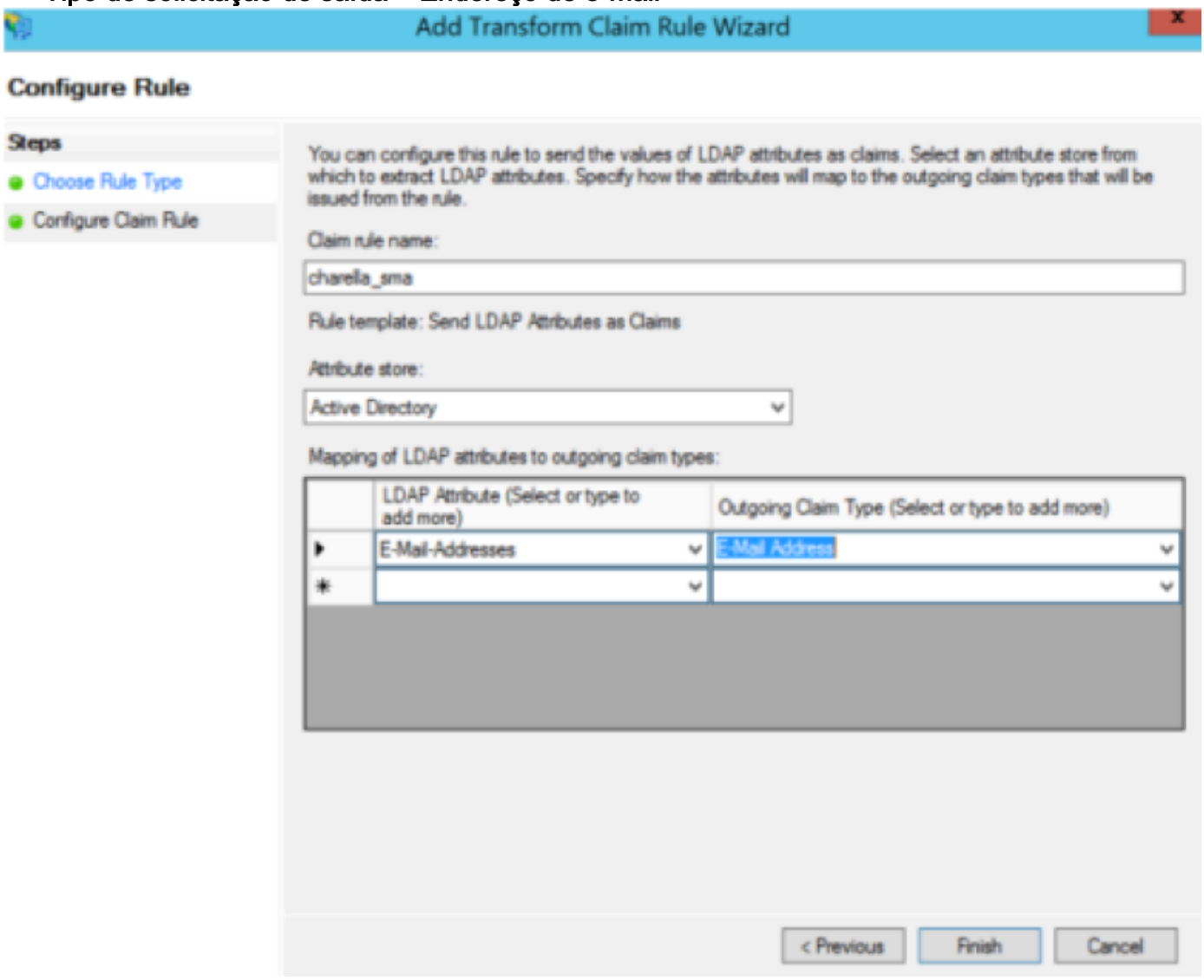
Etapa 6. Depois de importar com êxito o arquivo de metadados, configure as regras de reivindicação para a confiança de terceira parte confiável recém-criada, selecione **Claim rule template > Send LDAP Attributes**, como mostrado na imagem.



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

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

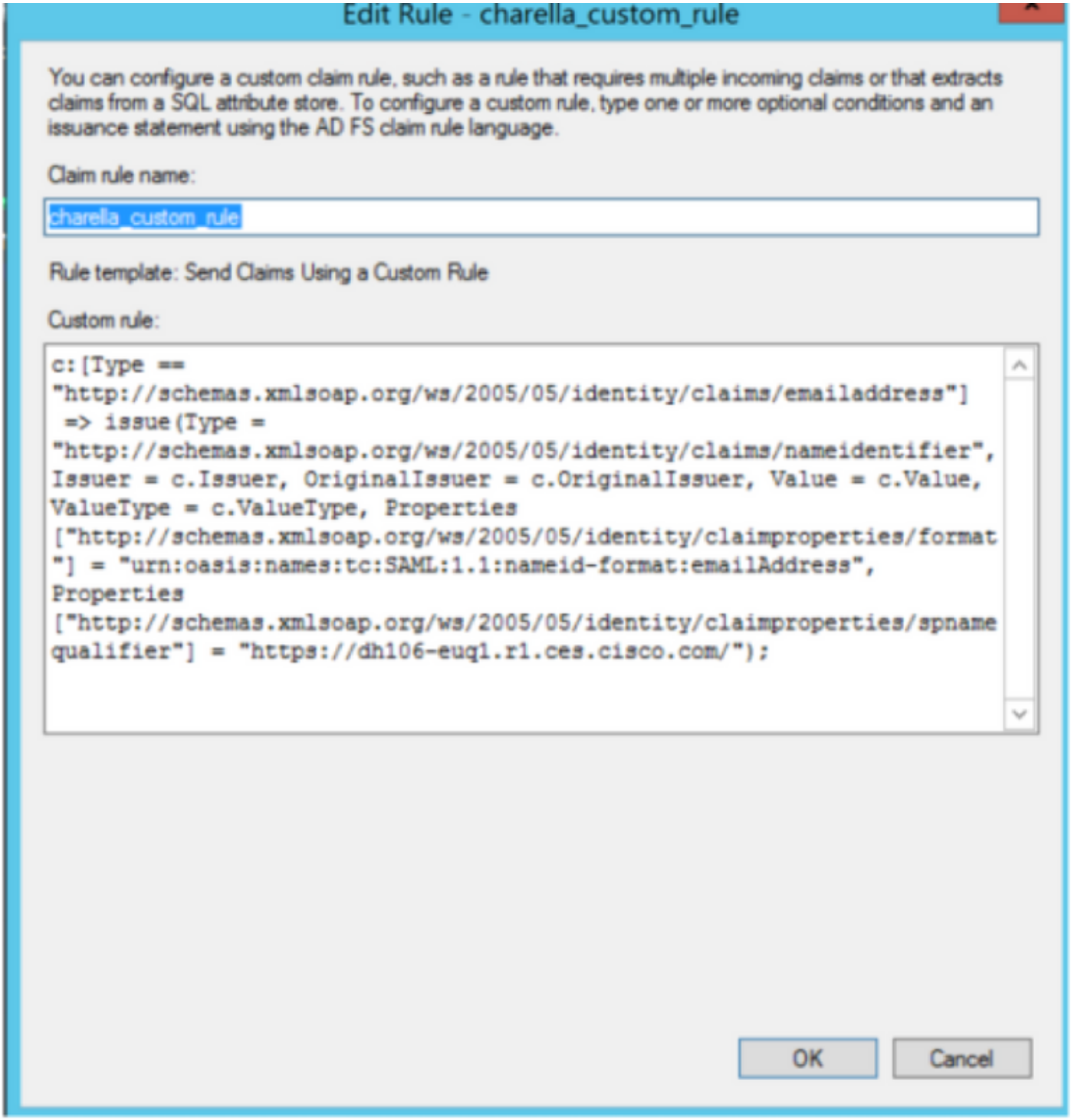
- **Atributo LDAP > Endereços de e-mail**
- **Tipo de solicitação de saída > Endereço de e-mail**



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

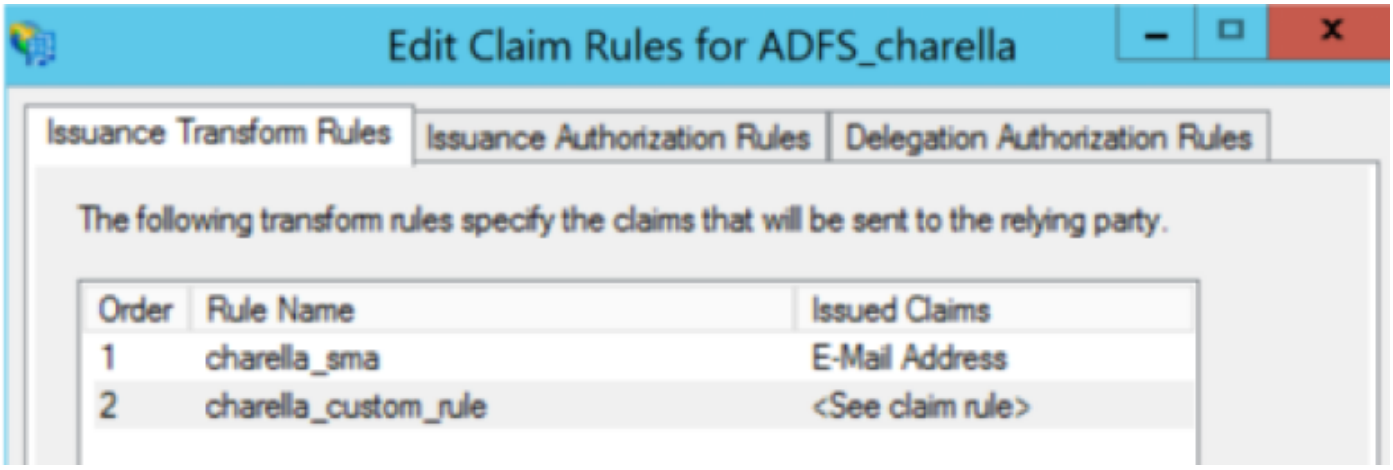
Esta é a regra personalizada que precisa ser adicionada à regra de Reivindicação personalizada:

```
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