

在ADFS上安装元数据文件

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何在Microsoft Active Directory联合身份验证服务(ADFS)上安装元数据文件。

先决条件

要求

Cisco 建议您了解以下主题：

- ADFS
- 安全断言标记语言(SAML)与安全管理设备集成

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

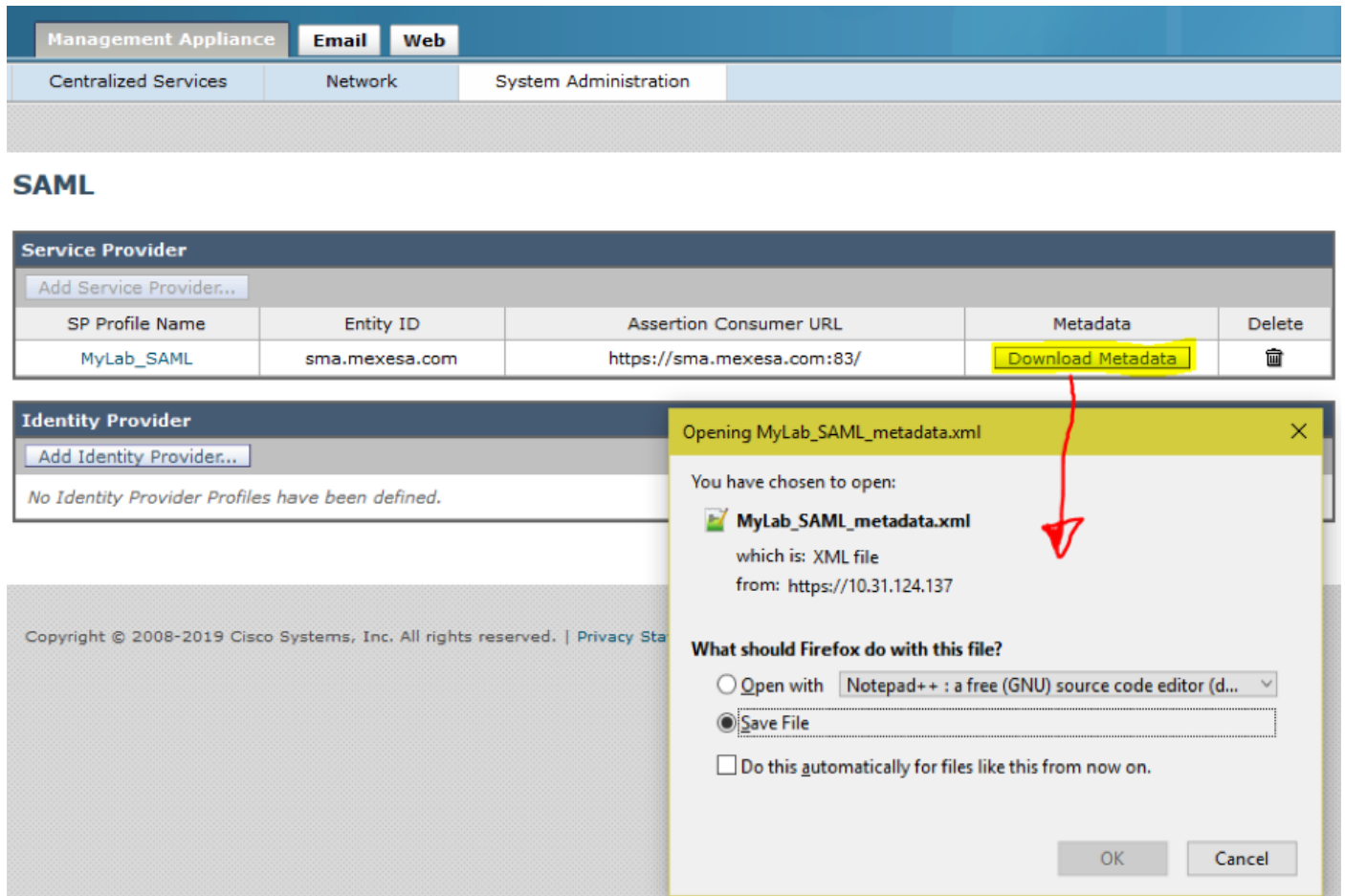
在ADFS中安装元数据文件之前，请确保满足以下要求：

- 在SMA中启用SAML
- 验证思科内容安全管理设备是否支持贵组织使用的身份提供程序。以下是受支持的身份提供程序：Microsoft Active Directory联合身份验证服务(ADFS)2.0Ping身份PingFederate 7.2思科网络安全设备9.1
- 获取保护设备与身份提供程序之间的通信所需的以下证书：如果希望设备签署SAML身份验证

请求，或者希望身份提供程序加密SAML断言，请从受信任证书颁发机构(CA)和关联的私钥获取自签名证书或证书。如果希望身份提供程序对SAML断言进行签名，请获取身份提供程序的证书。设备使用此证书验证签名的SAML断言

配置

步骤1.导航到SMA，然后选择**System Administration > SAML > Download Metadata**，如图所示。



The screenshot shows the SMA interface with the following components:

- Navigation Bar:** Management Appliance, Email, Web, Centralized Services, Network, System Administration.
- SAML Section:** Service Provider, Identity Provider.
- Service Provider Table:**

SP Profile Name	Entity ID	Assertion Consumer URL	Metadata	Delete
MyLab_SAML	sma.mexesa.com	https://sma.mexesa.com:83/	Download Metadata	
- Identity Provider Section:** No Identity Provider Profiles have been defined.
- Dialog Box:** Opening MyLab_SAML_metadata.xml. 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. OK Cancel

步骤2.当客户上传其ADFS元数据文件时，身份提供程序配置文件会自动填写。Microsoft有默认URL:<https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml>。

步骤3.在设置两个配置文件后，必须编辑SP配置文件元数据，如Bug CSCvh30183所示。元数据文件如图所示。

```

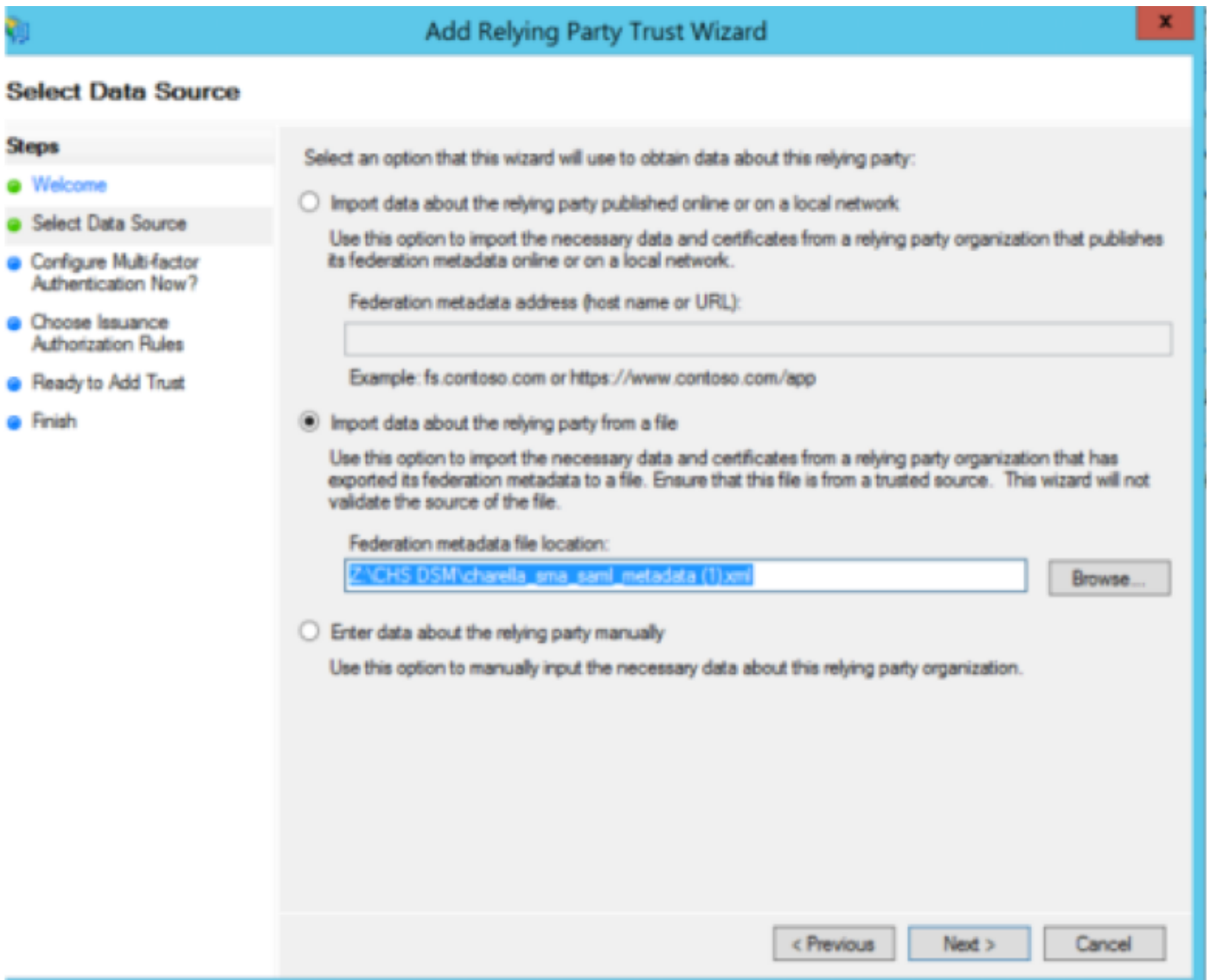
1  <?xml version="1.0"?>
2  <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
3      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
4      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
5      entityID="sma.mexesa.com">
6      <SPSSODescriptor
7          AuthnRequestsSigned="false" WantAssertionsSigned="true"
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                         BAYTAK1YMRcwFQYDVQQDDA5zbWEubWV4ZXXNhLmNvbTENCMAsgAlUEBwwEQ0RNWDEW
20                         MBQGA1UECgwNVG16b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
21                         SVQGU2VjdXJpdHkwHhcNMjkwNjA0MjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
22                         CQYDVQQGEwJNWDEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
23                         TVGxZjAUBGNVBAoMDVRpem9uY210byBJbmMxDTALBgNVBAGMBENETVgxZDASBgNV
24                         BAsMC0lUIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
25                         g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFPcJgn/oHXEUkVUnWe+9cTJQ41X4
26                         ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNyw8Wtd+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>

```

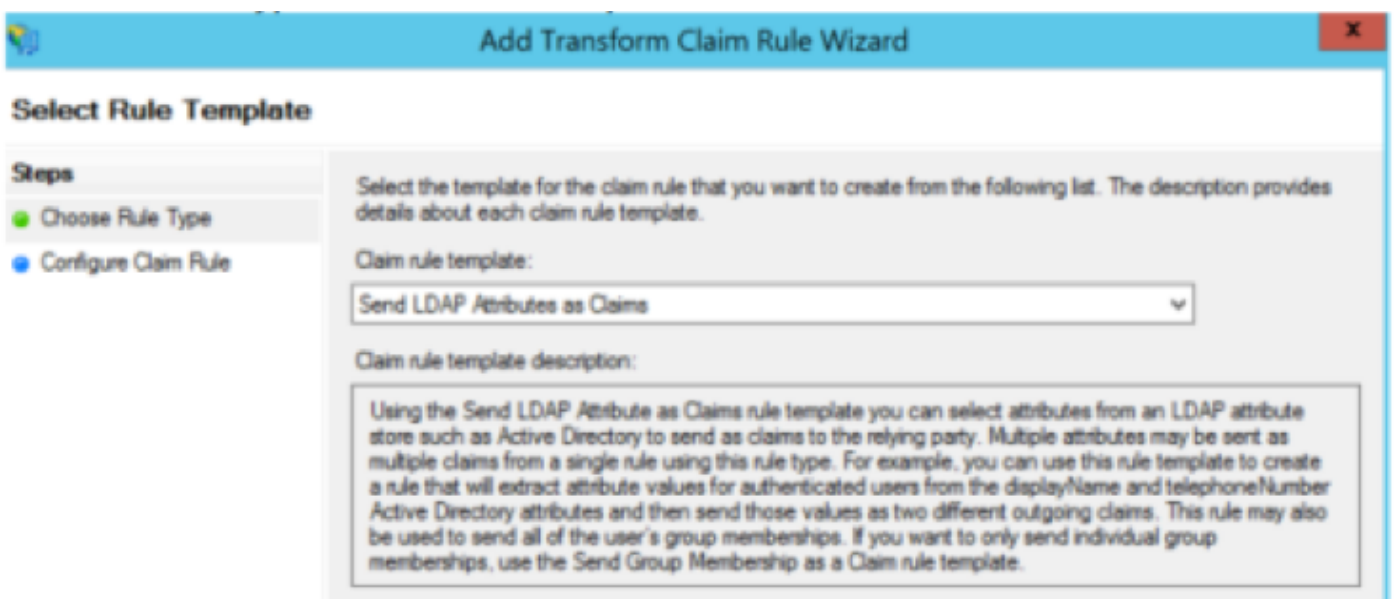
步骤4.删除突出显示的信息，元数据文件的结尾必须如图所示。

```
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>
13 MIIDZTCCAk2gAwIBAwIJA0jXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIXCzAJBgNV
14 BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZlZlLnVzTENMAAGAlUEBwwEQ0RNWDEW
15 MBQGA1UECgwNVG16b25jaXRvIEluYzENMAAGAlUECAwEQ0RNWDEUMBIGAlUECwwL
16 SVQGU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWWhcNMjAwNjA0MjEwNTUxWjByMQsw
17 CQYDVQQGEwJNWDEUMBUGAlUEAAwOc21hLm1leGVzYS5jb20xDTALBgNVBAAcMBENE
18 TVGxFjAUBGNVBAoMDVRpem9uY210byBjBmMxDTALBgNVBAGMBENETVGxvFDASBgNV
19 BAsMC01UIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
20 g7kzRmLl14q9TlklcTJzo8cmscu5nRXFWlohFpcJgn/oHXEUkVUnWe+9cTJQ41X4
21 ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNyv8Wtd+Io
22 MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rnO4jtvPZPj7B
23 cpWjawLlxAfUHVyvrc661Tblo0exG+hZ+AlS3B0l+6lmTNjF3IcGcGS/TE0chETx
24 glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+LkF8As8B1Pm6YHi
25 L6K8W4vOEj1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB3vxnL7jb
26 emMTKSRP4hycUld69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFii2oOJ6yGEOdWD
27 6+Bvj6wSBp7UoLyBdCxglyi+vK4Y/R2+iCv13pyaXkbf0QsJvYpzOg7xSjkkZm79
28 +ZIjQkekyCAM5N0of1ZRrJ9oGD5qoY1Zjhud7NHmRbj7LKHRSFVqpKet/tTXCH7
29 7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVpXXKacjAVj/ZclXnPBGSMxex277ECJq
30 ix5aXRSxOMRRtD/72FVRASgT3xlmBYqu/HTyOBZonGM+isJHBhRZxSOMBL+45jFY
31 PO1jBG5MZuWE
32        </ds:X509Certificate>
33      </ds:X509Data>
34    </ds:KeyInfo>
35  </KeyDescriptor>
36  <KeyDescriptor use="encryption">
37    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
38      <ds:X509Data>
39        <ds:X509Certificate>
40 MIIDZTCCAk2gAwIBAwIJA0jXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHIXCzAJBgNV
41 BAYTAk1YMRcwFQYDVQQDDA5zbWEubWV4ZlZlLnVzTENMAAGAlUEBwwEQ0RNWDEW
42 MBQGA1UECgwNVG16b25jaXRvIEluYzENMAAGAlUECAwEQ0RNWDEUMBIGAlUECwwL
43 SVQGU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWWhcNMjAwNjA0MjEwNTUxWjByMQsw
```

步骤5. 导航至ADFS，然后在ADFS Tools > AD FS Management > Add Relying Party Trust中导入编辑的元数据文件，如图所示。



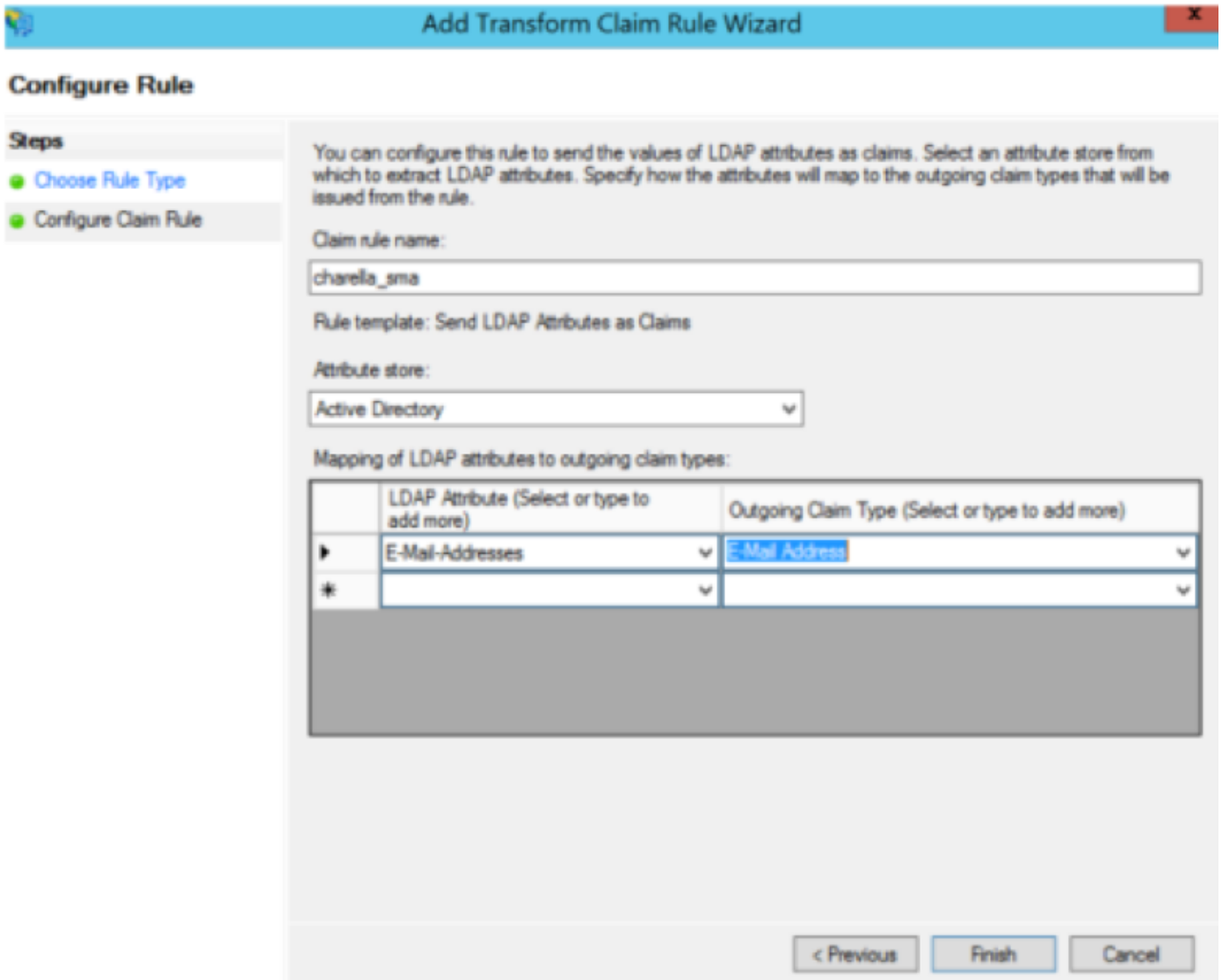
步骤6.成功导入元数据文件后，为新创建的信赖方信任配置声明规则，选择声明规则模板>发送LDAP属性，如图所示。



步骤7.命名领款申请规则名称，然后选择Attribute Store > Active Directory。

步骤8.映射LDAP属性，如图所示。

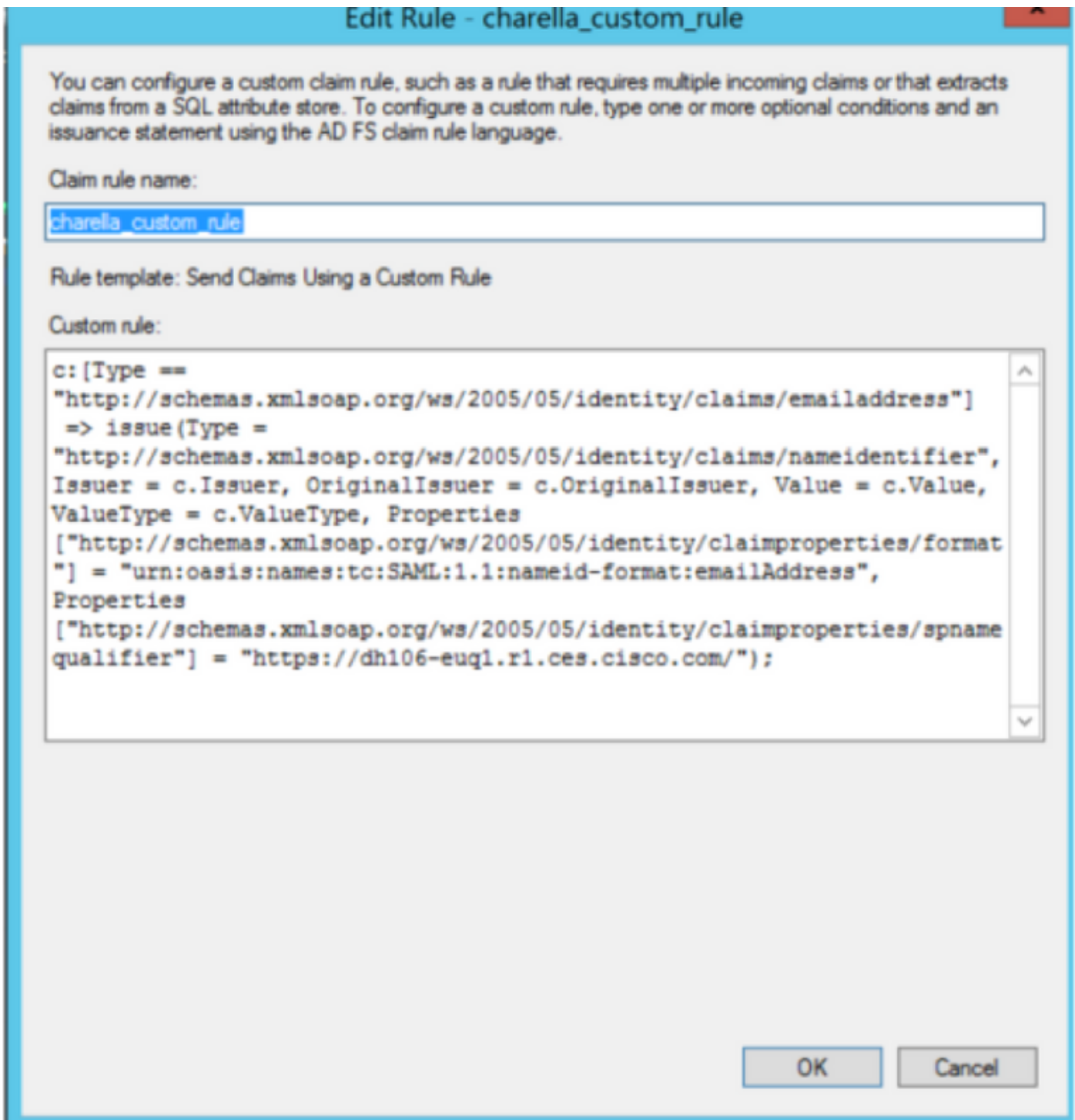
- LDAP属性>邮件地址
- 外发领款申请类型>邮件地址



步骤9.使用此信息创建新的自定义声明规则，如图所示。

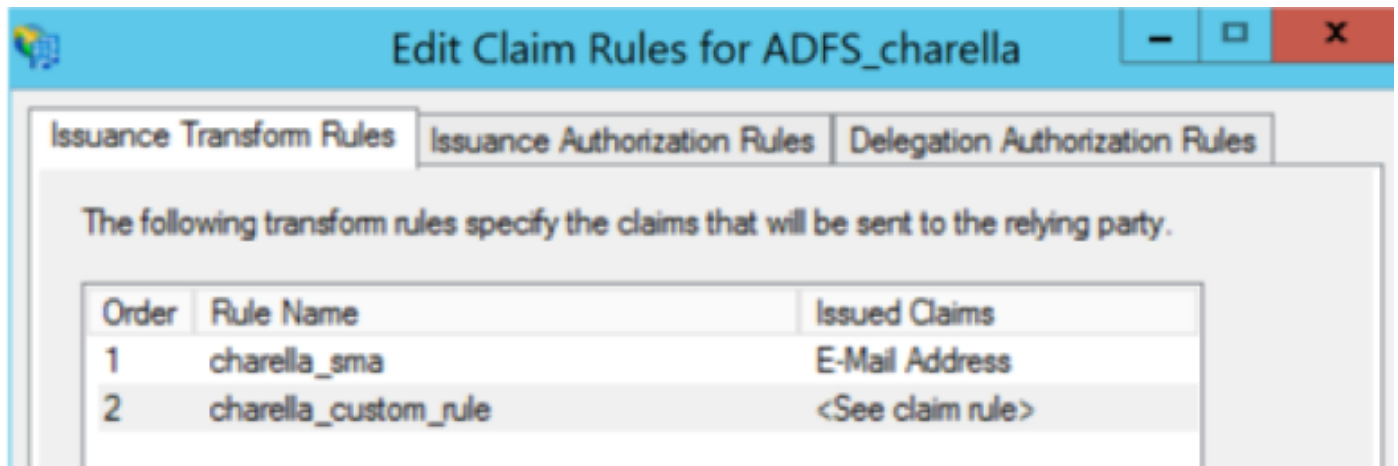
这是需要添加到自定义声明规则的自定义规则：

```
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");
```



- 使用SMA主机名和端口修改突出显示的URL (如果您在CES环境中, 则不需要端口, 但它必须指向euq1。 <allocation>.iphmx.com)

步骤10. 确保领款申请规则顺序为: 如图所示, LDAP声明规则优先, 自定义声明规则次之。



步骤11.登录EUQ，它必须重定向到ADFS主机。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- [CSCvh30183](#)
- [技术支持和文档 - Cisco Systems](#)