

# 在ADFS上安裝後設資料檔案

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

本文檔介紹如何在Microsoft Active Directory聯合身份驗證服務(ADFS)上安裝後設資料檔案。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- ADFS
- 與安全管理裝置整合的安全斷言標籤語言(SAML)

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

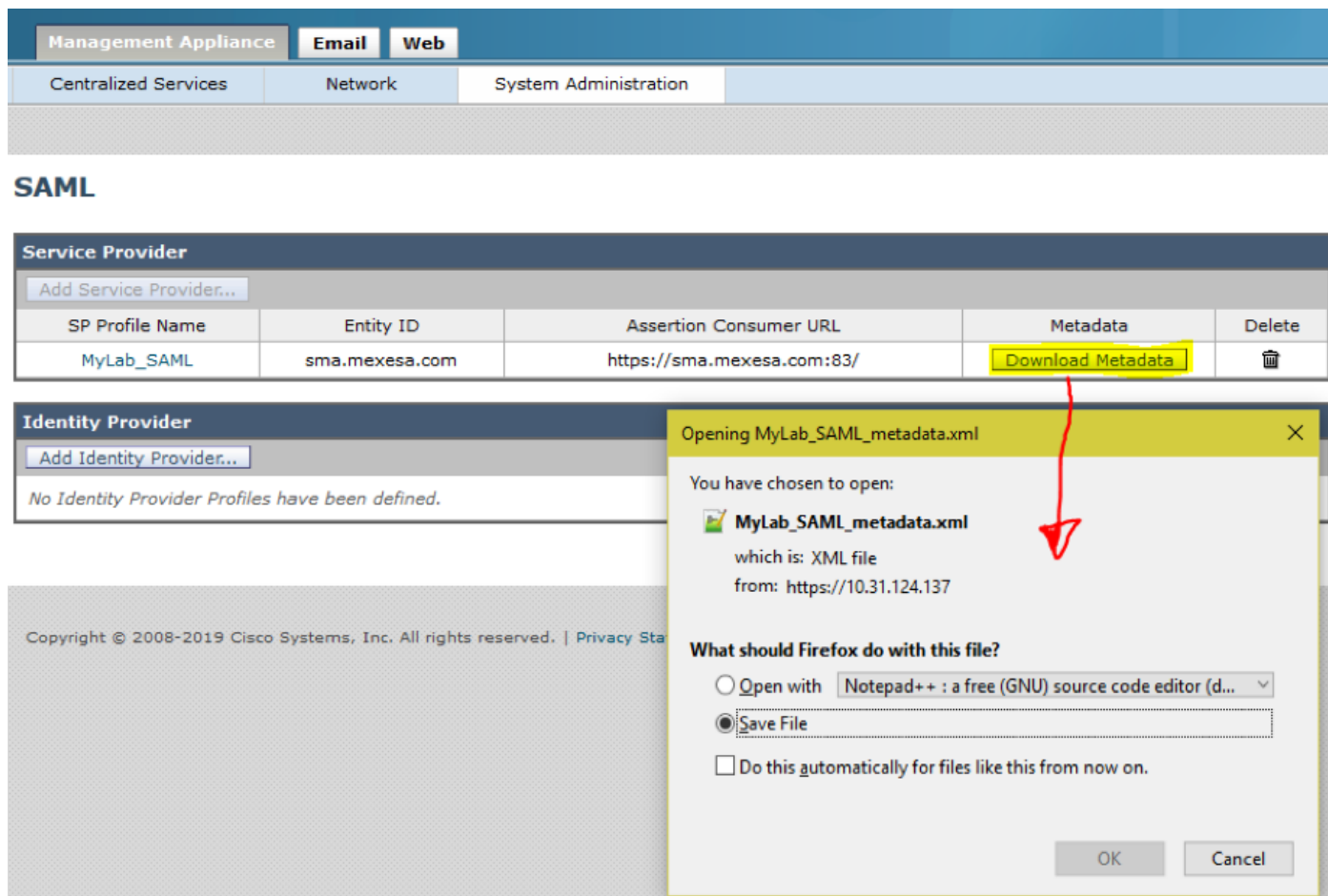
在ADFS中安裝後設資料檔案之前，請確保滿足以下要求：

- 在SMA中啟用SAML
- 驗證您的組織使用的身份提供程式是否受思科內容安全管理裝置支援。以下是受支援的身份提供程式：Microsoft Active Directory聯合身份驗證服務(ADFS)2.0Ping身份Ping聯盟版本7.2思科網路安全裝置9.1
- 獲取保護您的裝置和身份提供商之間的通訊所需的證書：如果您希望裝置對SAML身份驗證請

求進行簽名，或者希望身份提供程式加密SAML宣告，請從受信任的證書頒發機構(CA)獲取自簽名證書或證書以及關聯的私鑰。如果您希望身份提供程式對SAML斷言進行簽名，請獲取身份提供程式的證書。您的裝置使用此證書來驗證簽名的SAML斷言

## 設定

步驟1.導航到SMA，然後選擇系統管理> SAML >下載後設資料，如下圖所示。



The screenshot shows the SMA web interface. At the top, there are tabs for 'Management Appliance', 'Email', and 'Web'. Below these are 'Centralized Services', 'Network', and 'System Administration'. The 'SAML' section is active. Under 'Service Provider', there is a table with one entry: 'MyLab\_SAML' with Entity ID 'sma.mexesa.com' and Assertion Consumer URL 'https://sma.mexesa.com:83/'. The 'Download Metadata' button is highlighted in yellow. A Firefox dialog box is open, showing the file 'MyLab\_SAML\_metadata.xml' which is an XML file from 'https://10.31.124.137'. The dialog asks 'What should Firefox do with this file?' and the 'Save File' option is selected. A red arrow points from the 'Download Metadata' button to the dialog box.

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

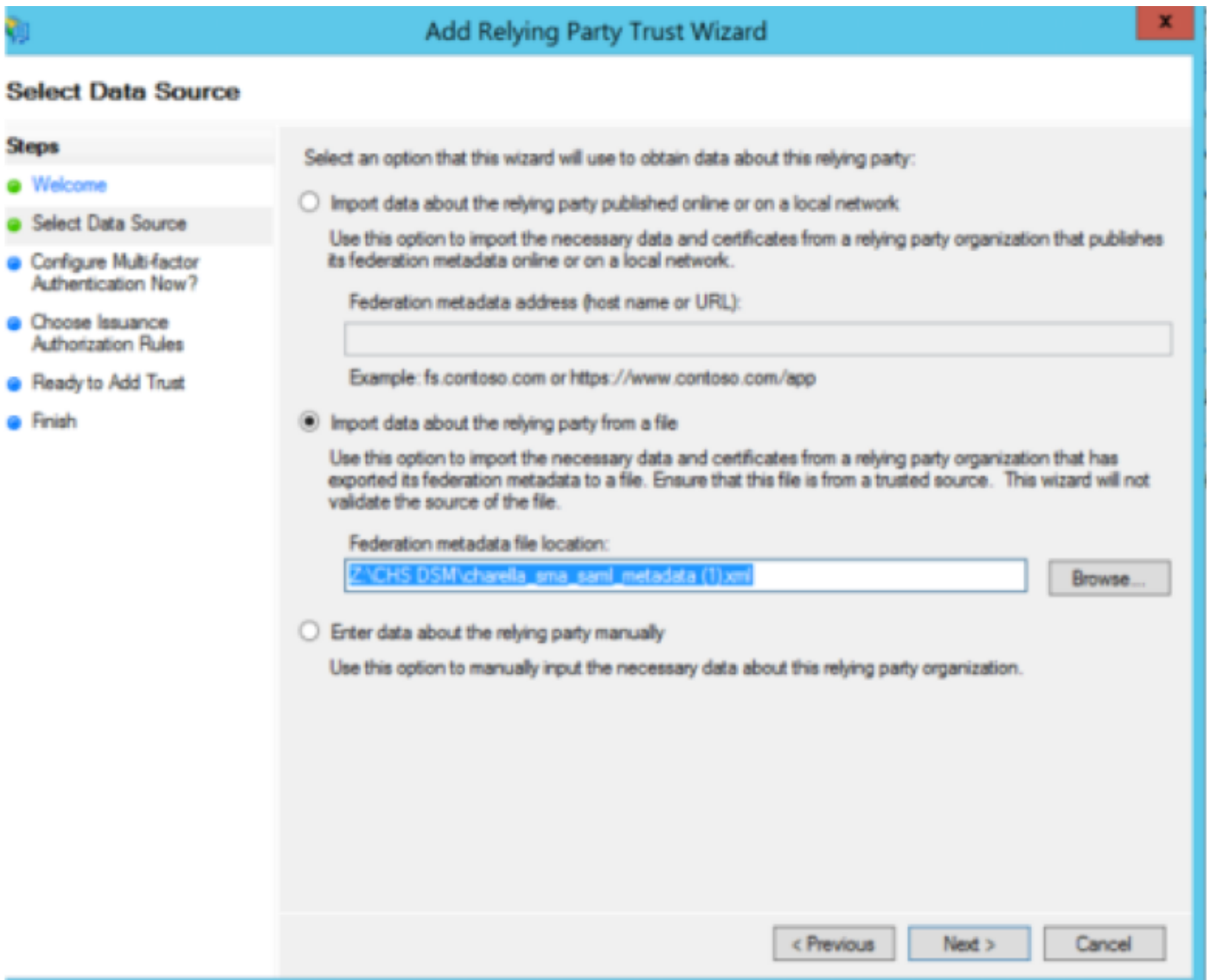
步驟2.客戶上傳其ADFS後設資料檔案時，身份提供程式配置檔案會自動填寫。Microsoft有一個預設URL:<https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml>。

步驟3.安裝兩個配置檔案後，必須根據錯誤CSCvh30183.編輯SP配置檔案後設資料。後設資料檔案如下圖所示。

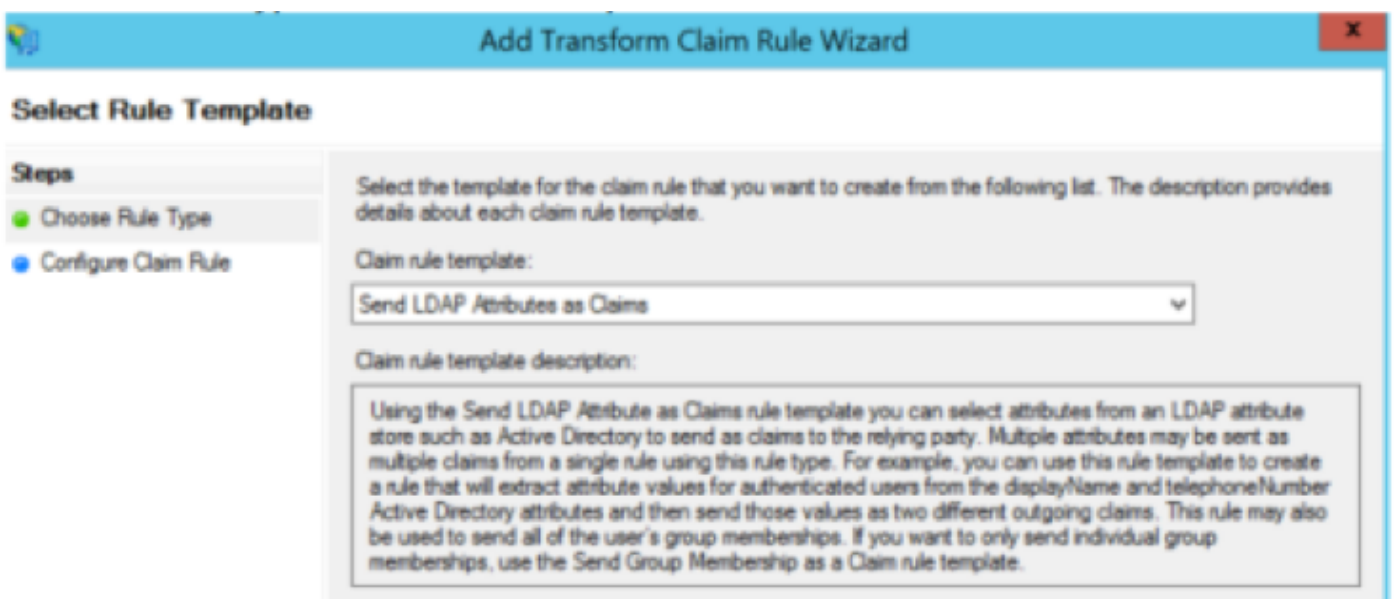


```
1 <?xml version="1.0"?>
2 <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
3   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
4   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
5   entityID="sma.mexesa.com">
6   <SPSSODescriptor
7     AuthnRequestsSigned="false" WantAssertionsSigned="true"
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 BAYTAK1YMRcwFQYDVQDDA5zbWEubWV4ZXXNhLmNvbTENMA5GA1UEBwwEQ0RNWDEW
15 MBQGA1UECgwNVG16b25jaXRvIEluYzENMA5GA1UECAwEQ0RNWDEUMBIGA1UECwwL
16 SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWWhcNMjAwNjA0MjEwNTUxWjByMQsw
17 CQYDVQGEwJNwDEWEXMBUGA1UEAwOc21hLm1leGVzYS5jb20xDALBgNVBAcMBENE
18 TVGxFjAUBGNVBAoMDVRpem9uY210byBjBmMxDTALBgNVBAGMBENETVGxFDASBgNV
19 BAsMC0lUIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
20 g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFPcJgn/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+iCv13pyaXkbF0QSJvYpzOg7xSjKxZm79
28 +ZIjQkekyCAM5N0of1ZRrJ9oGD5qoYlZjhUD7NHmRbj7LKHRSFVqPket/tTXCH7
29 7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVPxxKacjAVj/Zc1XnPBGSMxex0277ECJq
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 BAYTAK1YMRcwFQYDVQDDA5zbWEubWV4ZXXNhLmNvbTENMA5GA1UEBwwEQ0RNWDEW
42 MBQGA1UECgwNVG16b25jaXRvIEluYzENMA5GA1UECAwEQ0RNWDEUMBIGA1UECwwL
43 SVQgU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWWhcNMjAwNjA0MjEwNTUxWjByMQsw
```

步驟5. 導航到ADFS，然後在ADFS Tools > AD FS Management > Add Relisting Party Trust中匯入編輯的後設資料檔案，如下圖所示。



步驟6.成功匯入後設資料檔案後，為新建立的信賴方信任配置宣告規則，選擇宣告規則模板>傳送LDAP屬性，如下圖所示。



步驟7.命名宣告規則名稱，然後選擇Attribute Store > Active Directory。

步驟8.對映LDAP屬性，如下圖所示。

- LDAP屬性>電子郵件地址
- 傳出宣告型別>電子郵件地址

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:

Rule template: Send LDAP Attributes as Claims

Attribute store:

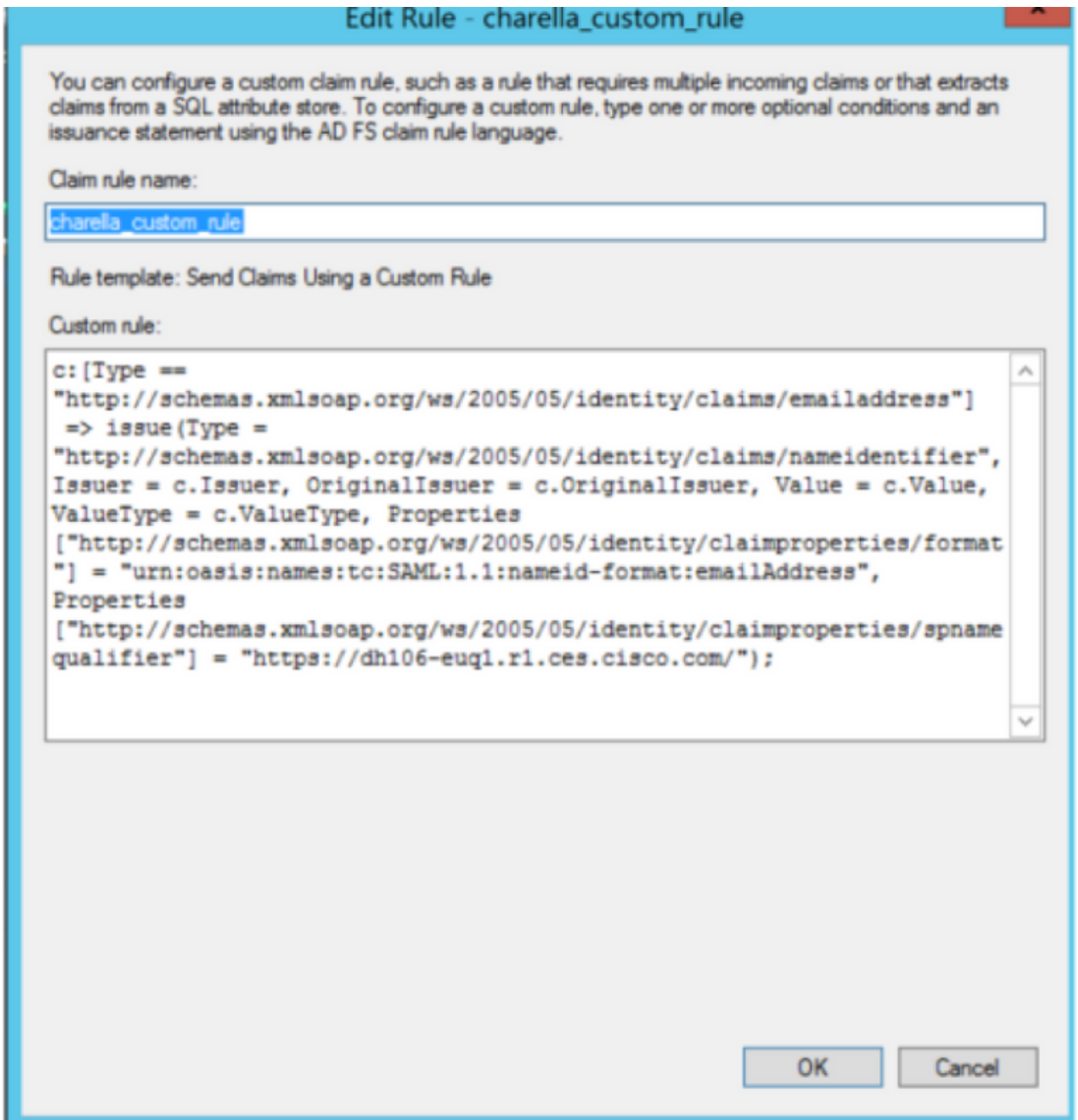
Mapping of LDAP attributes to outgoing claim types:

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

步驟9.使用此資訊建立新的自定義宣告規則，如下圖所示。

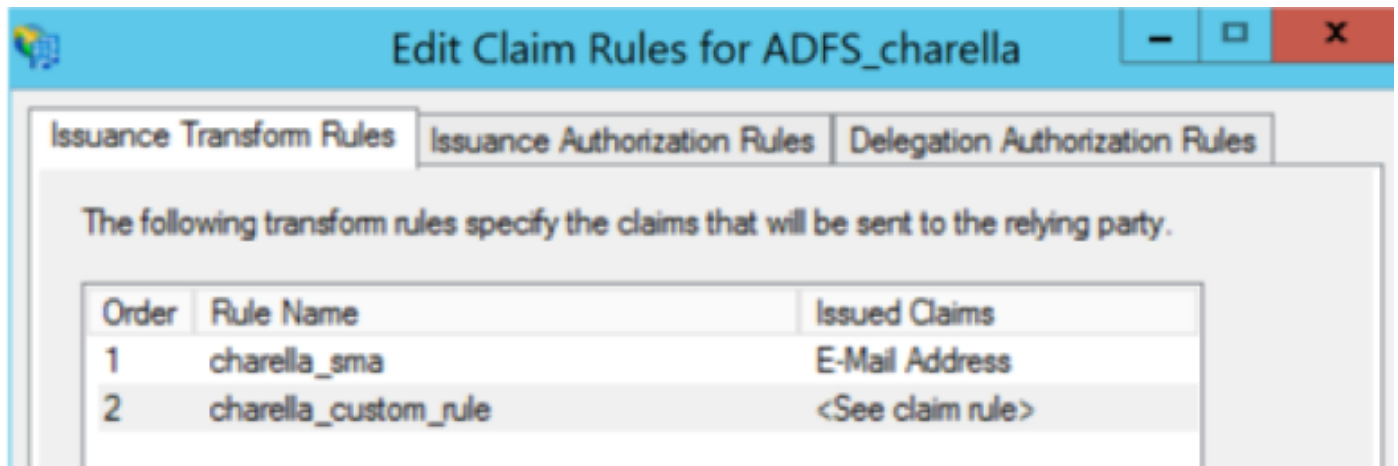
這是需要新增到自定義宣告規則的自定義規則：

```
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主機名和埠修改突出顯示的URL(如果您在CES環境中，則不需要埠，但埠必須指向 euq1。 <allocation>.iphmx.com)

步驟10.確保索賠規則順序為：LDAP宣告規則第一，自定義宣告規則第二，如下圖所示。



步驟11.登入到EUQ，必須重定向到ADFS主機。

## 驗證

目前沒有適用於此組態的驗證程序。

## 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

## 相關資訊

- [CSCvh30183](#)
- [技術支援與文件 - Cisco Systems](#)