تثبيت ملف البيانات الأولية على ADFS

المحتويات

المقدمة

يوضح هذا المستند كيفية تثبيت ملف بيانات التعريف على خدمات إتحاد Microsoft Active Directory (ADFS).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- نظام الملفات الموزعة
- تكامل لغة تمييز تأكيد الأمان (SAML) مع جهاز إدارة الأمان

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

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

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

قبل أن يتم تثبيت ملف البيانات الأولية في ADFS، تأكد من أن تلك المتطلبات يتم تلبيتها:

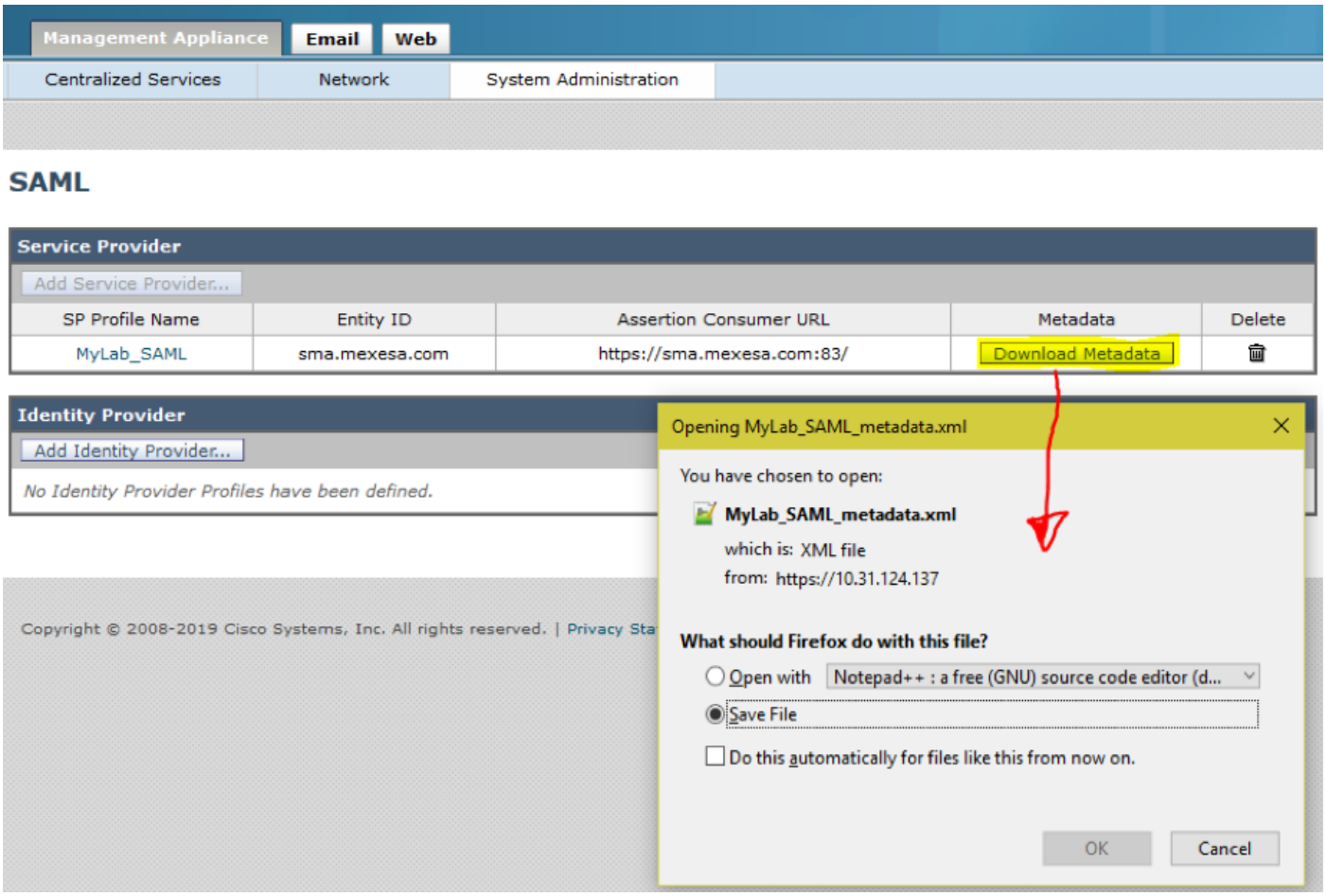
- تمكين SAML في SMA
- تحقق ما إذا كان موفر الهوية الذي تستخدمه مؤسستك مدعوما بواسطة جهاز إدارة أمان

المحتوى من Cisco. هؤلاء هم مزود الهوية المدعومون: خدمات إتحاد Microsoft Active Directory (ADFS) 2.0Ping Identity Federate 7.2جهاز أمان الويب 9.1 من Cisco

- احصل على هذه الشهادات المطلوبة لتأمين الاتصال بين الجهاز ومورد الهوية:إذا كنت تريد من الجهاز الخاص بك توقيع طلبات مصادقة SAML أو إذا كنت تريد من مورد الهوية تشفير تأكيدات SAML، احصل على شهادة موقعة ذاتيا أو شهادة من مرجع مصدق موثوق به (CA) والمفتاح الخاص المرتبط.إذا كنت تريد أن يوقع مورد الهوية على تأكيدات SAML، احصل على شهادة مورد الهوية. يستخدم الجهاز الخاص بك هذه الشهادة للتحقق من تأكيدات SAML الموقعة

التكوين

الخطوة 1. انتقل إلى SMA وحدد **إدارة النظام > SAML > تنزيل البيانات الأولية**، كما هو موضح في الصورة.



الخطوة 2. يتم علم ملف تعريف مورد الهوية تلقائيا عندما يقوم العميل بتحميل ملف بيانات تعريف ADFS الخاص به. يوجد لدى Microsoft عنوان URL افتراضي: **https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml**.

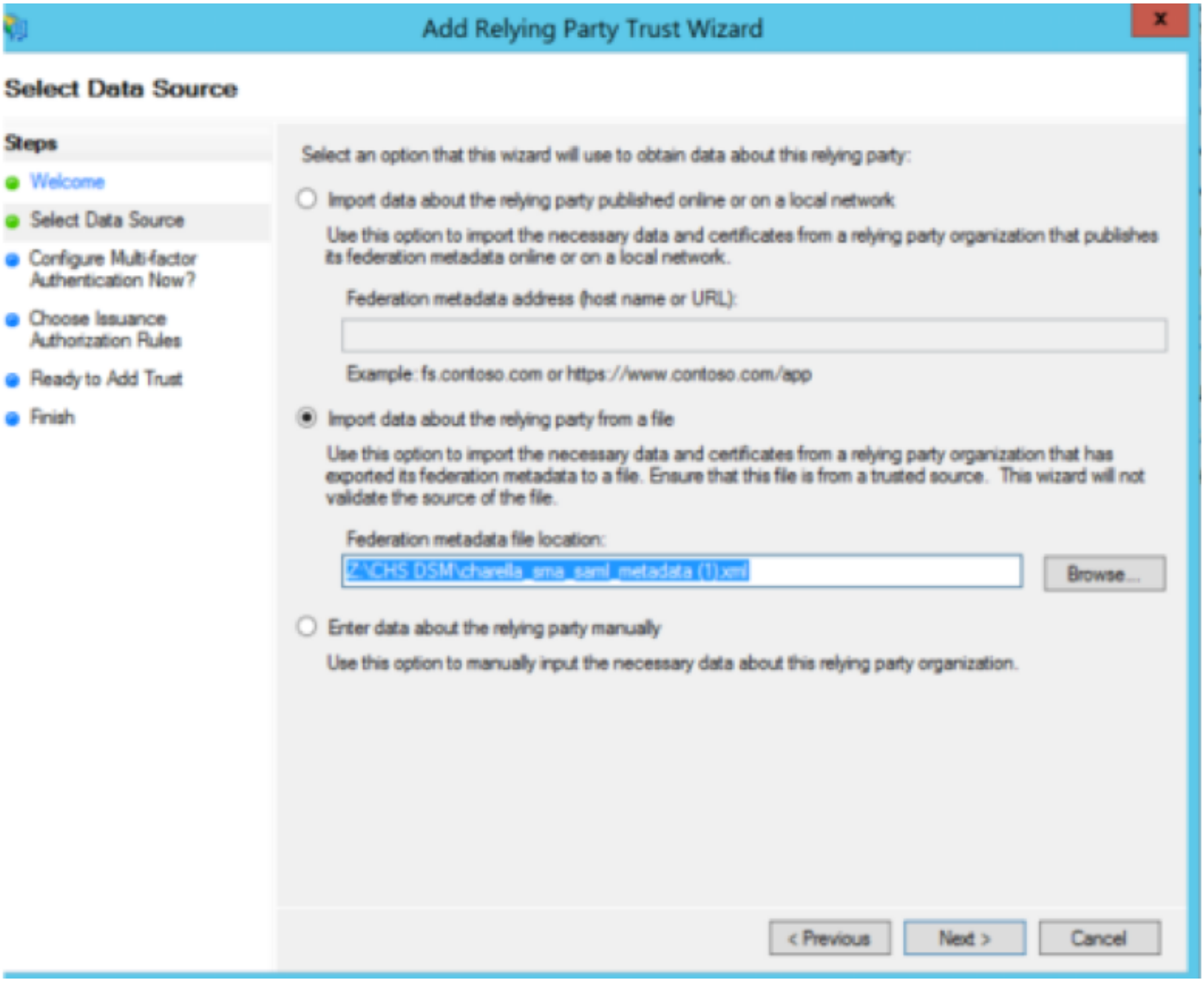
الخطوة 3. ما إن يتم إعداد كل من ملفات التعريف، يجب تحرير بيانات تعريف ملف تعريف SP، حسب الخطأ CSCvh30183.. يظهر ملف البيانات الأولية كما هو موضح في الصورة.

```
<?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>Bag Attributes
    localKeyID: D5 4F B4 DA BC 91 71 5C 53 94 4A 78 E0 4A C3 EF C4 BD 4C 8D
    friendlyName: sma.mexesa.com
subject=/C=MX/CN=sma.mexesa.com/L=CDMX/O=Tizoncito Inc/ST=CDMX/OU=IT Security
issuer=/C=MX/CN=sma.mexesa.com/L=CDMX/O=Tizoncito Inc/ST=CDMX/OU=IT Security
-----BEGIN CERTIFICATE-----
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
-----END CERTIFICATE-----
          </ds:X509Certificate>
        </ds:X509Data>
```

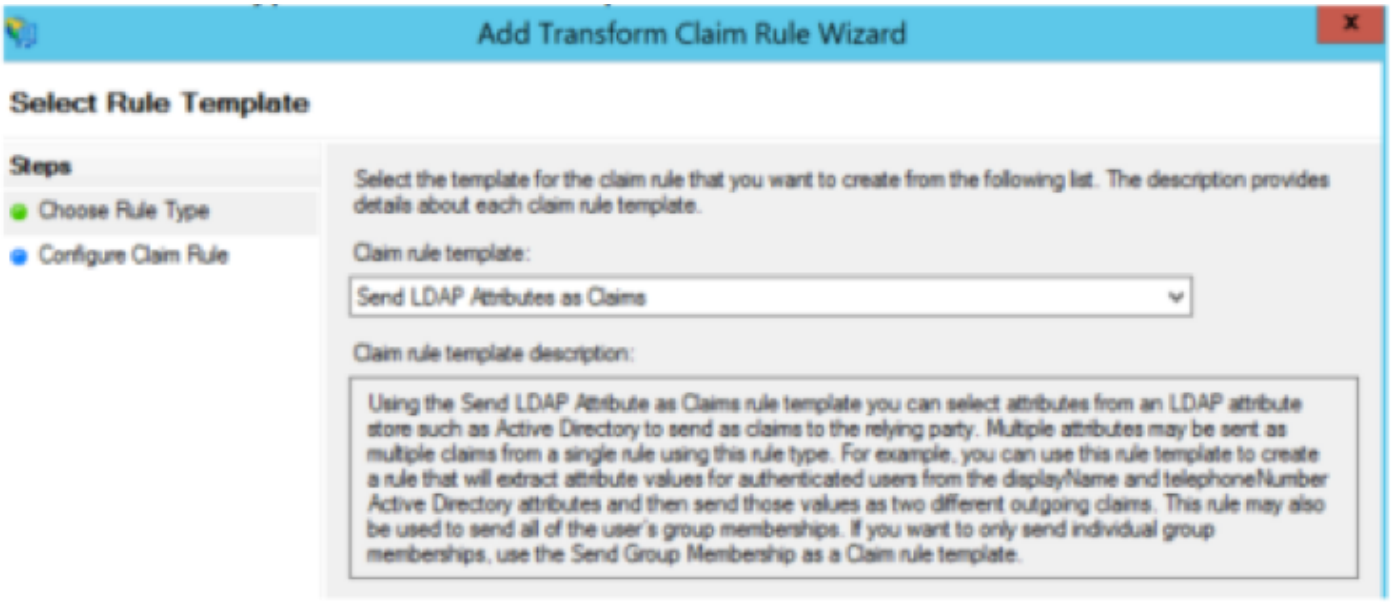
الخطوة 4. إزالة المعلومات المبرزة، في ملف نهاية البيانات الأولية يجب أن يكون كما هو موضح في الصورة.

```
<?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
```

الخطوة 5. انتقل إلى ADFS الخاص بك وقم بإدراج ملف البيانات الأولية المحررة في **أدوات ADFS > إدارة AD FS > إضافة ثقة طرف الاعتماد**، كما هو موضح في الصورة.



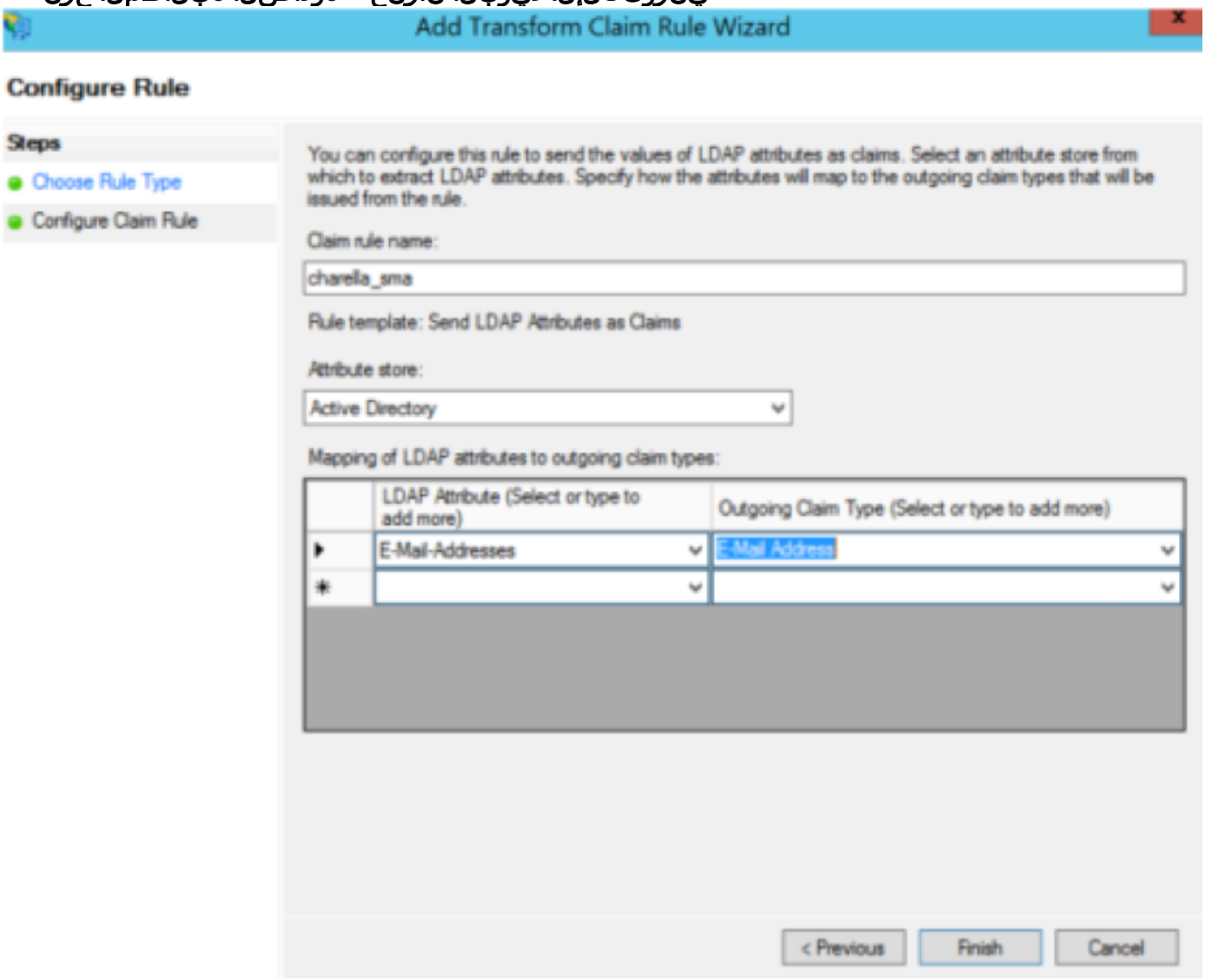
الخطوة 6. بعد قيامك باستيراد ملف بيانات التعريف بنجاح، قم بتكوين قواعد المطالبات الخاصة ب "ثقة الطرف المعول" التي تم إنشاؤها حديثا، حدد **قالب قاعدة المطالبة** >إرسال سمات LDAP، كما هو موضح في الصورة.



الخطوة 7. قم بتسمية اسم قاعدة المطالبة، ثم حدد **مخزن السمات > Active Directory**.

الخطوة 8. تخطيط خصائص LDAP، كما هو موضح في الصورة.

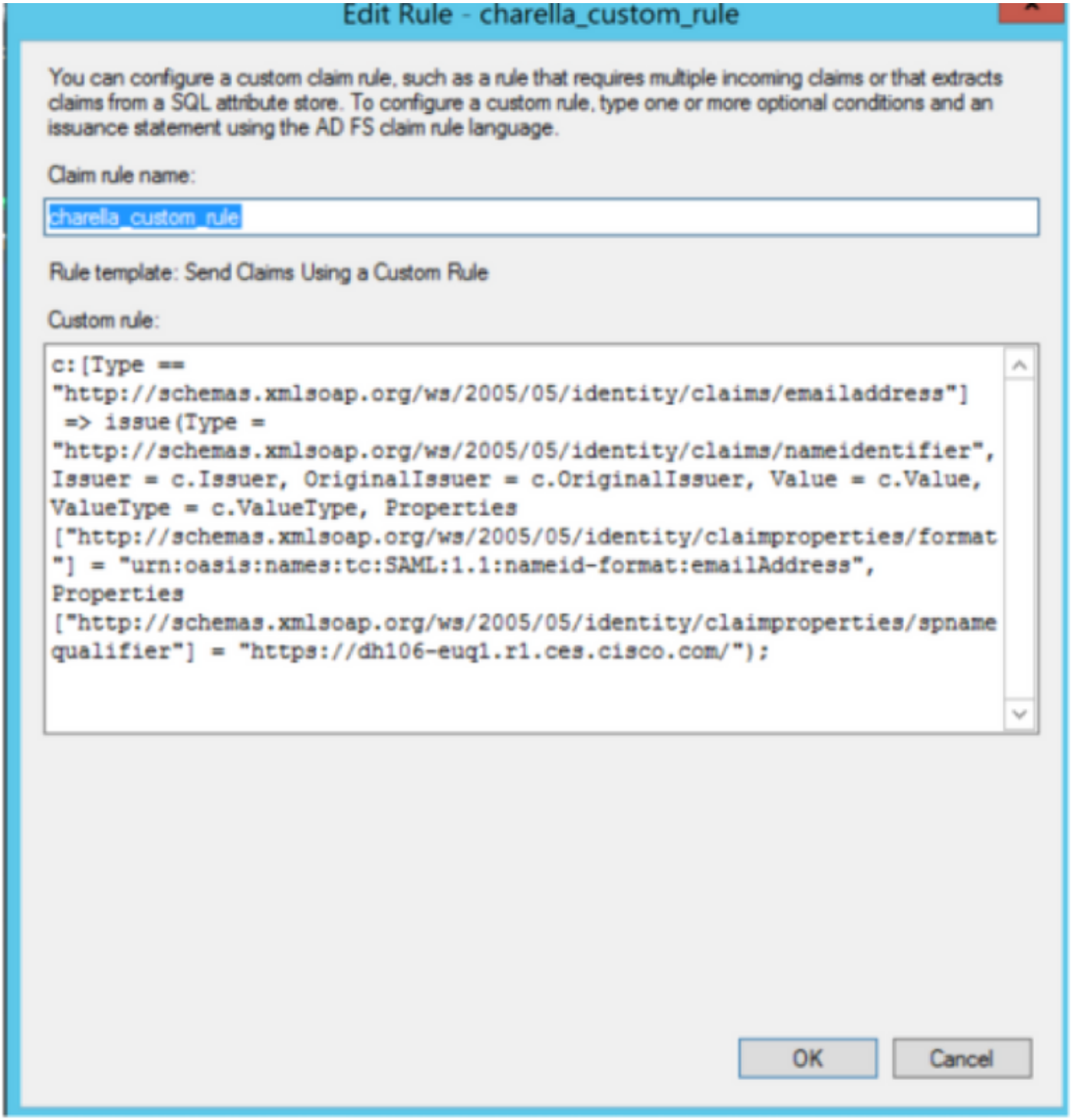
- سمة LDAP > عناوين البريد الإلكتروني
- نوع المطالبة الصادرة > عنوان البريد الإلكتروني



الخطوة 9. قم بإنشاء قاعدة مطالبة مخصصة جديدة باستخدام هذه المعلومات، كما هو موضح في الصورة.

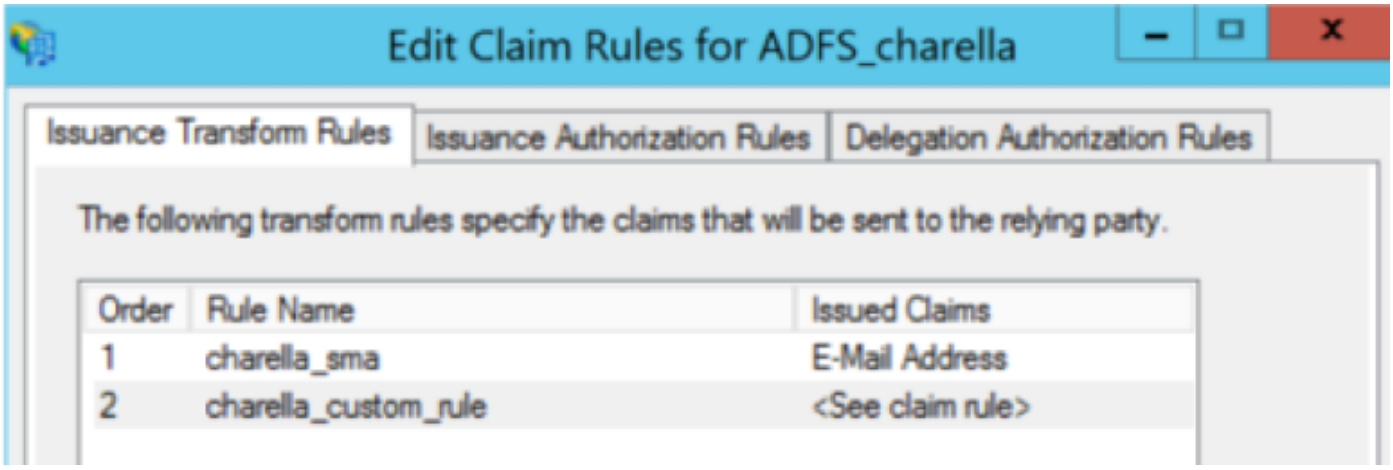
هذه هي القاعدة المخصصة التي يجب إضافتها إلى قاعدة المطالبة المخصصة:

```
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");
```



- قم بتعديل عنوان URL المميز باستخدام اسم مضيف ومنفذ SMA (إذا كنت على بيئة CES، فلن يكون المنفذ مطلوبا ولكنه يجب أن يشير إلى euq1.<distribution>.iphmx.com)

الخطوة 10. تأكد من أن ترتيب قاعدة المطالبة هو: قاعدة مطالبة LDAP أولا وقاعدة المطالبة المخصصة الثانية، كما هو موضح في الصورة.



الخطوة 11. قم بتسجيل الدخول إلى EUQ، ويجب أن يعيد التوجيه إلى مضيف ADFS.

التحقق من الصحة

ال يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

ال تتوفر حالياً معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- CSCvh30183
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).