Installer le fichier de métadonnées sur ADFS

Contenu

Introduction

Ce document décrit comment installer le fichier de métadonnées sur les services ADFS (Microsoft Active Directory Federation Services).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ADFS
- Intégration du langage SAML (Security Assertion Markup Language) à l'appliance de gestion de la sécurité

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

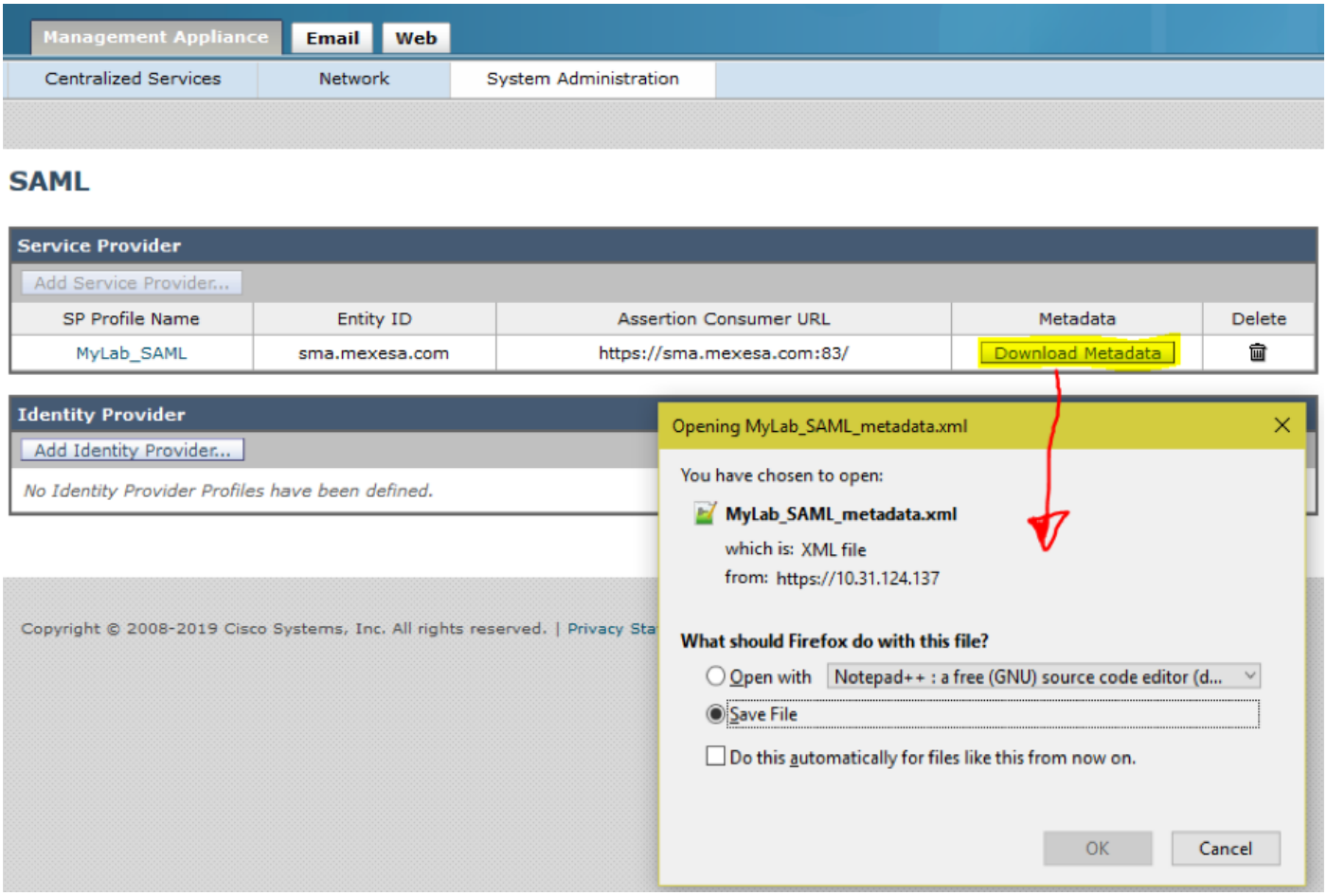
Informations générales

Avant d'installer le fichier de métadonnées dans ADFS, assurez-vous que ces exigences sont respectées :

- SAML activé dans SMA
- Vérifiez si le fournisseur d'identité utilisé par votre entreprise est pris en charge par Cisco Content Security Management Appliance. Voici les fournisseurs d'identité pris en charge : Microsoft Active Directory Federation Services (ADFS) 2.0Ping Identity PingFederate 7.2Appareil de sécurité Web Cisco 9.1
- Obtenez les certificats requis pour sécuriser la communication entre votre appareil et le fournisseur d'identité :Si vous souhaitez que votre appliance signe des demandes d'authentification SAML ou que votre fournisseur d'identité chiffre les assertions SAML, obtenez un certificat auto-signé ou un certificat d'une autorité de certification (CA) de confiance et de la clé privée associée.Si vous voulez que le fournisseur d'identité signe des assertions SAML, obtenez le certificat du fournisseur d'identité. Votre appliance utilise ce certificat pour vérifier les assertions SAML signées

Configuration

Étape 1. Accédez à votre SMA et sélectionnez **Administration du système > SAML > Télécharger les métadonnées**, comme indiqué dans l'image.



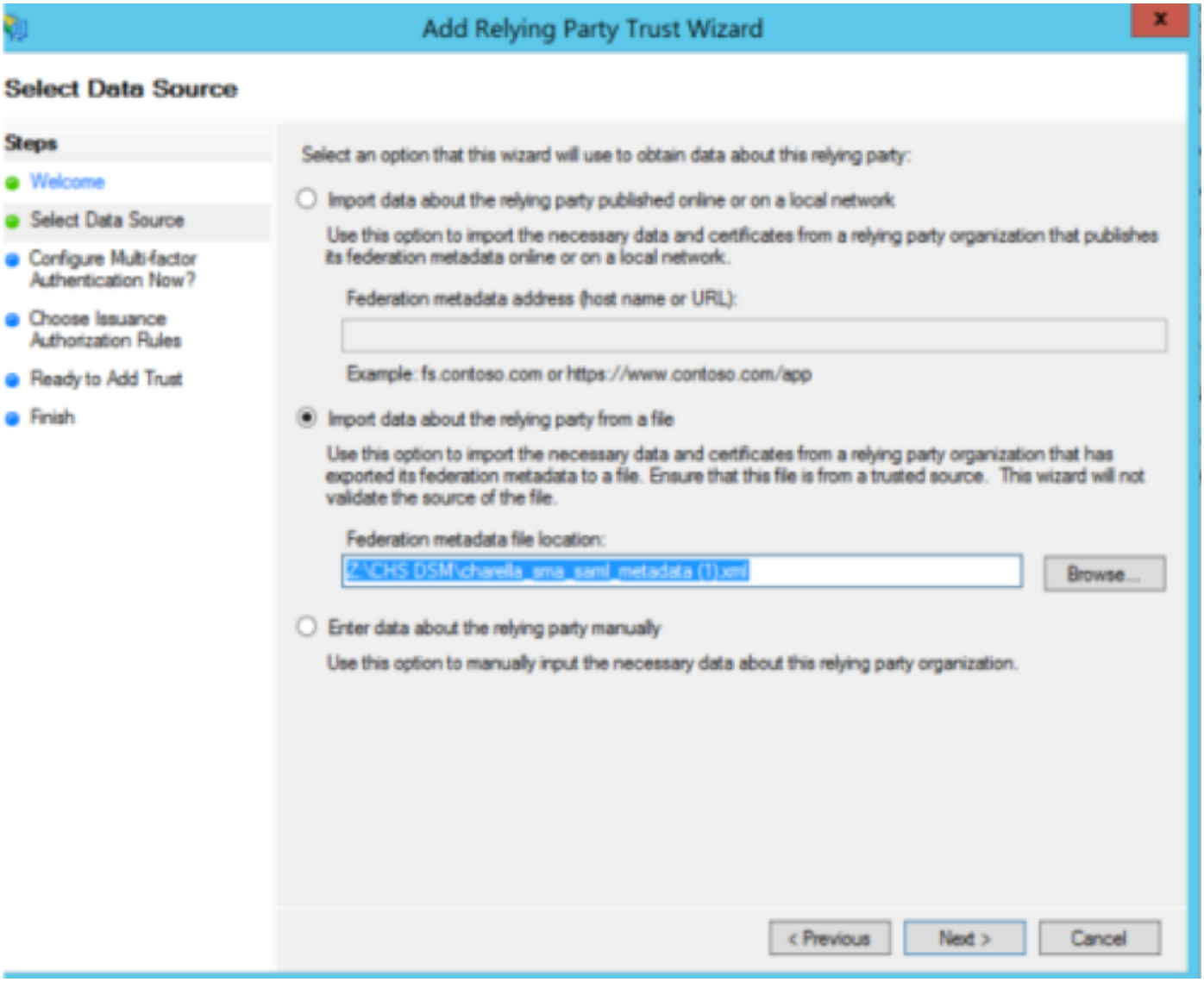
Étape 2. Le profil du fournisseur d'identité se remplit automatiquement lorsque le client télécharge son fichier de métadonnées ADFS. Microsoft a une URL par défaut : **https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml.**

Étape 3. Une fois les deux profils configurés, les métadonnées de profil SP doivent être modifiées, conformément au bogue CSCvh30183.. Le fichier de métadonnées apparaît comme illustré dans l'image.

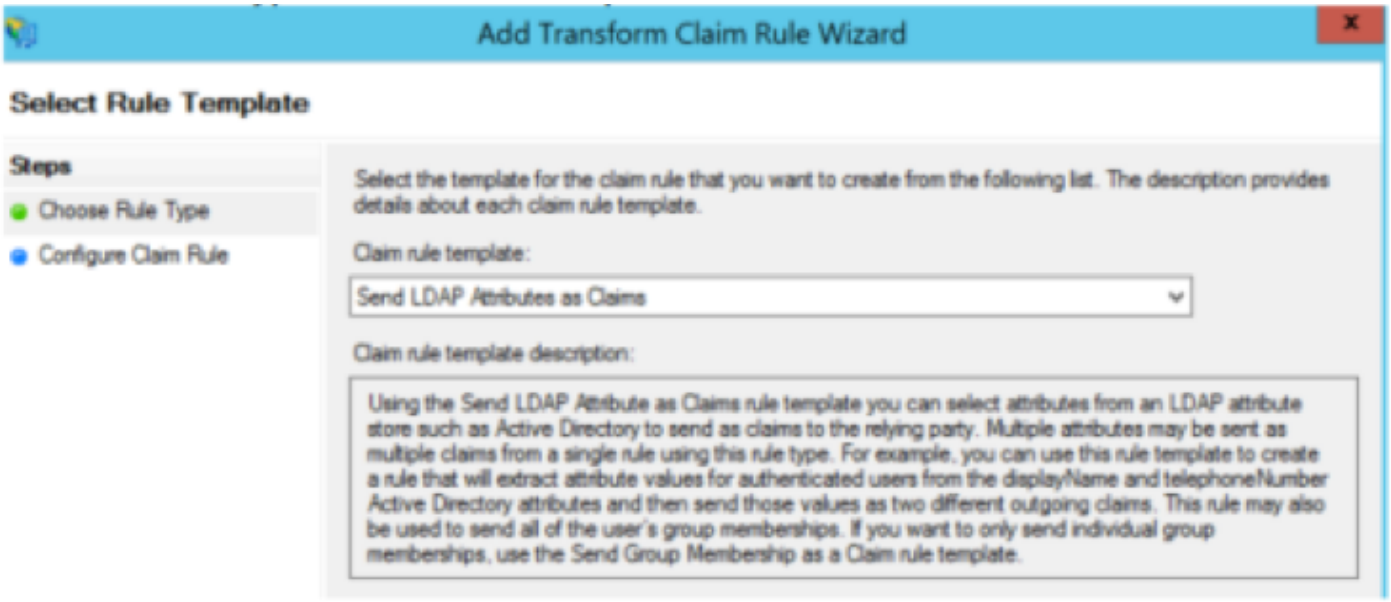
Étape 4. Supprimez les informations en surbrillance, à la fin du fichier de métadonnées doit être comme indiqué dans l'image.

```
<?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
```

Étape 5. Accédez à votre ADFS et importez le fichier de métadonnées modifié dans **Outils ADFS > Gestion AD FS > Ajouter une approbation de partie de confiance**, comme illustré dans l'image.



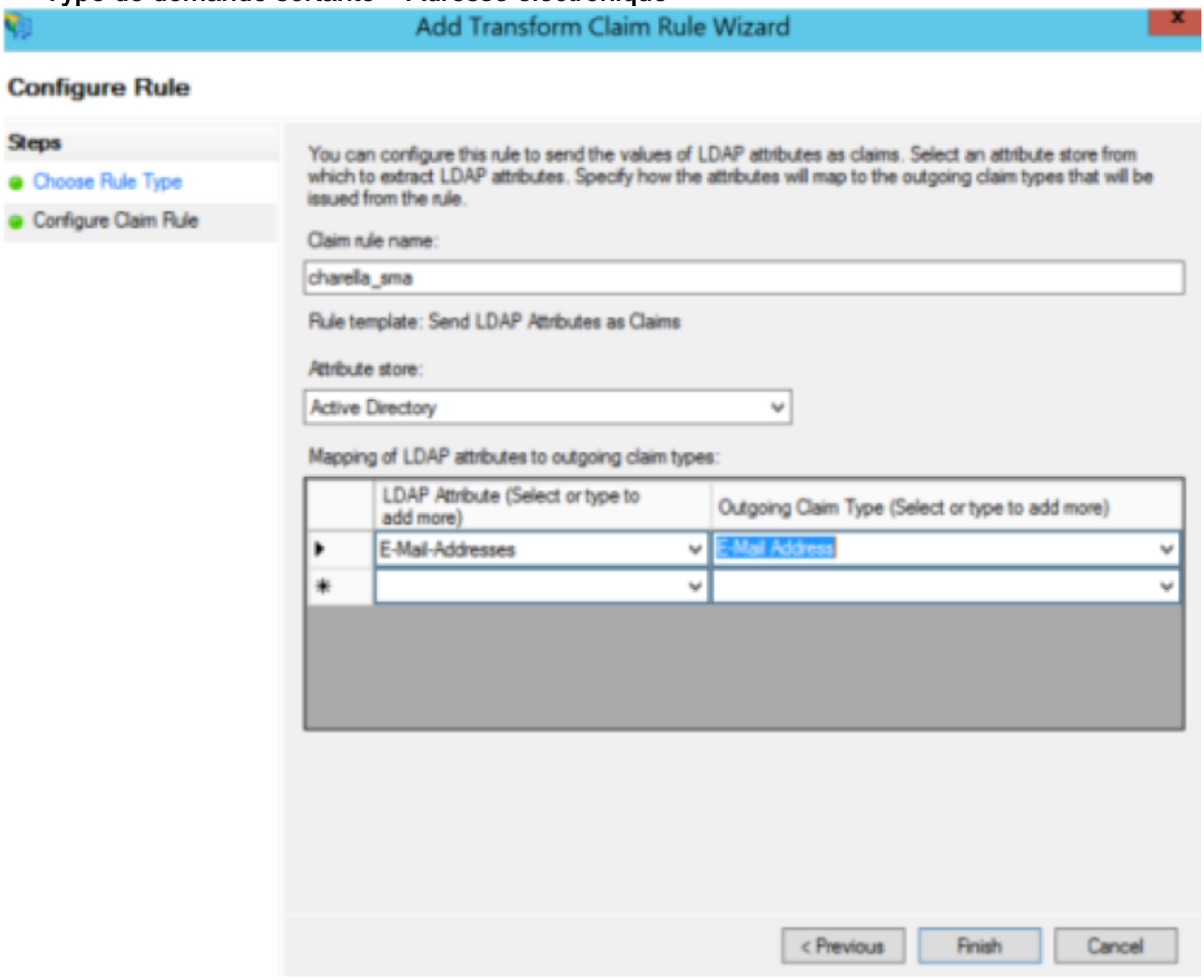
Étape 6. Après avoir importé le fichier de métadonnées, configurez les règles de revendication pour l'approbation de partie de confiance nouvellement créée, sélectionnez le **modèle de règle de revendication > Envoyer les attributs LDAP**, comme indiqué dans l'image.



Étape 7. Nommez le nom de la règle de revendication, puis sélectionnez **Magasin d'attributs > Active Directory**.

Étape 8. Mapper les attributs LDAP, comme illustré dans l'image.

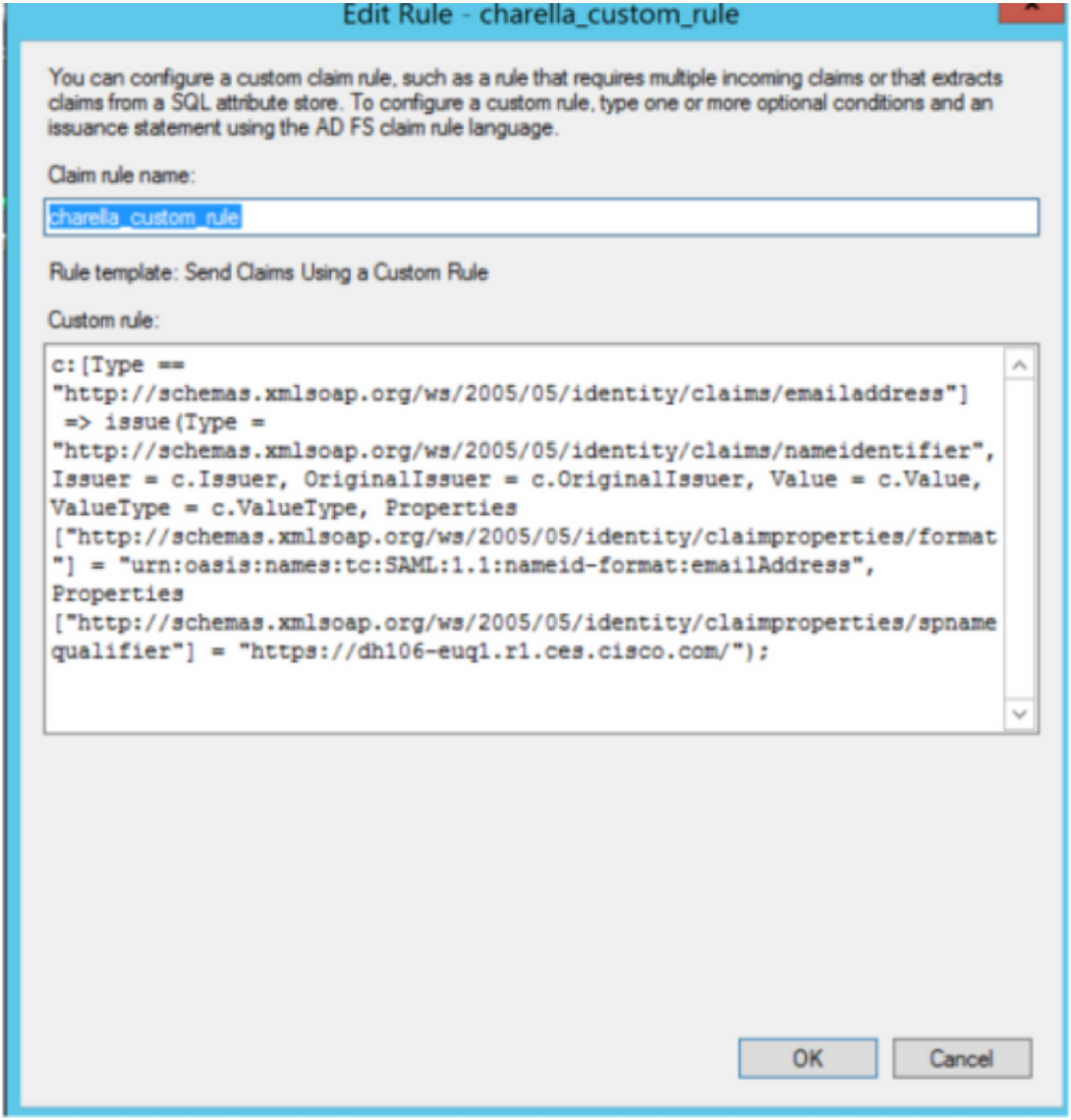
- **Attribut LDAP > Adresses de messagerie**
- **Type de demande sortante > Adresse électronique**



Étape 9. Créez une nouvelle règle de revendication personnalisée avec ces informations, comme l'illustre l'image.

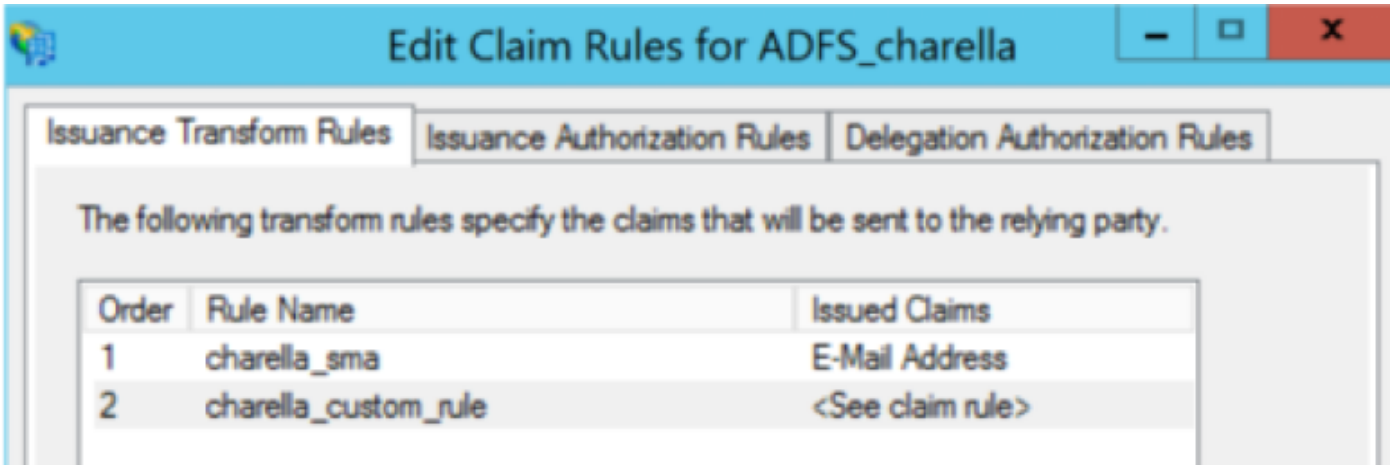
Il s'agit de la règle personnalisée qui doit être ajoutée à la règle de revendication personnalisée :

```
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");
```



- Modifiez l'URL mise en surbrillance avec le nom d'hôte et le port SMA (si vous êtes dans un environnement CES, un port n'est pas requis mais doit pointer sur euq1.<allocation>.iphmx.com)

Étape 10. Assurez-vous que l'ordre des règles de revendication est : Règle de revendication LDAP en premier et Règle de revendication personnalisée en second, comme illustré dans l'image.



Étape 11. Connectez-vous à EUQ, il doit rediriger vers l'hôte ADFS.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- CSCvh30183
- Support et documentation techniques - Cisco Systems