

# Installer le fichier de métadonnées sur ADFS

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

## 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) 2.0 Ping Identity PingFederate 7.2 Appareil 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.

The screenshot shows the Cisco SMA web interface. At the top, there are tabs for 'Management Appliance', 'Email', and 'Web'. Below these are navigation tabs for 'Centralized Services', 'Network', and 'System Administration'. The 'SAML' section is active, showing 'Service Provider' and 'Identity Provider' configuration areas. In the 'Service Provider' table, the 'Download Metadata' button for the 'MyLab\_SAML' profile is highlighted in yellow. A red arrow points from this button to a Firefox file dialog box. The dialog box shows the file 'MyLab\_SAML\_metadata.xml' which is an XML file from 'https://10.31.124.137'. The 'Save File' option is selected under the heading 'What should Firefox do with this file?'. There are 'OK' and 'Cancel' buttons at the bottom of the dialog.

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](https://cisco.com/warpcard/CSCvh30183). Le fichier de métadonnées apparaît comme illustré dans l'image.

```

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                         BAYTAK1YMRcwFQYDVQQDDA5zbWEubWV4ZXXNhLmNvbTENCAsGA1UEBwwEQ0RNWDEW
20                         MBQGA1UECgwNVG16b25jaXRvIEluYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
21                         SVQGU2VjdXJpdHkwHhcNMjkwNjA0MjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
22                         CQYDVQQGEwJNWDEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
23                         TVGxZjAUBG9wMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
24                         BAsMC0lUIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
25                         g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFPcJgn/oHXEUKvUnWe+9cTJQ41X4
26                         ojbGCP75UjD8GdPczkuBxqAZgkrfNLR8mopsxTFVWb5x68tVsTBGFNyw8Wtd+Io
27                         MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rn04jtvPZj7B
28                         cpWjawLlxAfUHVyvrC661Tblo0exG+hZ+AlS3B01+61mTNjF3IcGcGS/TE0chETx
29                         glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+LkF8As8B1Pm6YHi
30                         L6K8W4vOEj1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB3vxNL7jb
31                         emMTKSRP4hycUld69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFii2oOJ6yGEOdWD
32                         6+Bvj6wSBp7UoLyBdCxglyi+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>

```

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



### Add Relying Party Trust Wizard

#### Select Data Source

**Steps**

- Welcome
- Select Data Source
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

< Previous    Next >    Cancel

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.

### Add Transform Claim Rule Wizard

#### Select Rule Template

**Steps**

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

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

**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:

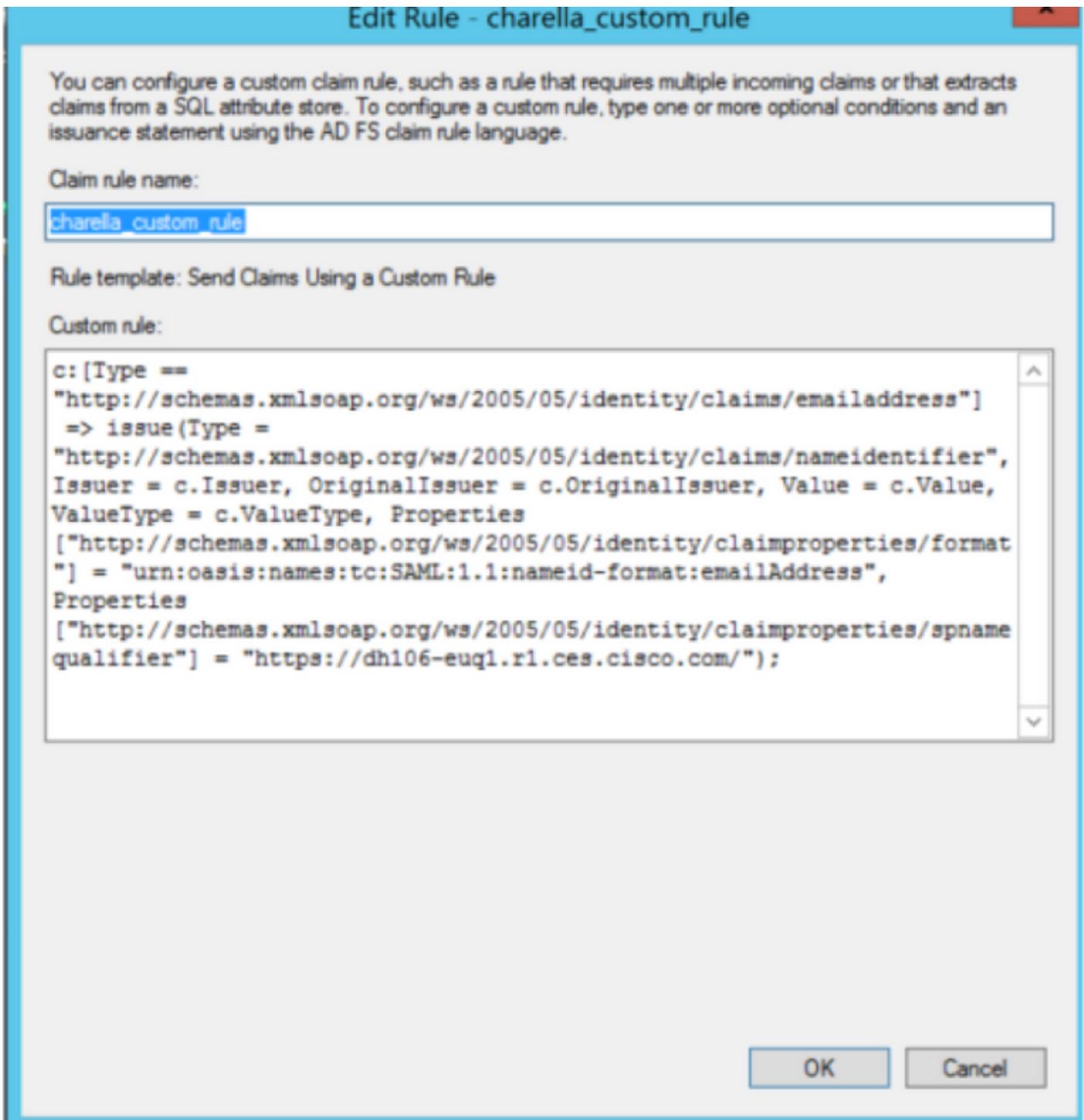
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	E-Mail Address
*		

< Previous   Finish   Cancel

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

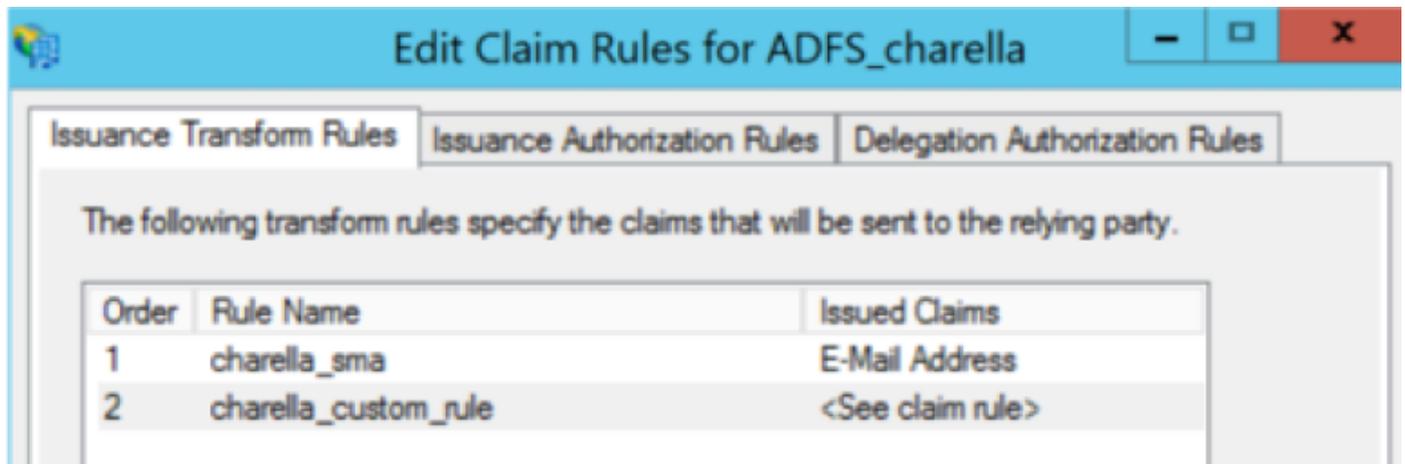
Il s'agit de la règle personnalisée qui doit être ajoutée à la règle de revendication personnalisée :

```
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](#)