

Metagegevens-bestand op ADFS installeren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u metagegevensbestand in de Microsoft Active Directory Federation Services (ADFS) kunt installeren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ADFS
- Security Association Markup Language (SAML) integratie met Security Management-applicatie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Zorg ervoor dat, voordat het metagegevensbestand in de ADFS is geïnstalleerd, aan deze eisen wordt voldaan:

- SAML ingeschakeld in SMA
- Controleer of de identiteit die door uw organisatie wordt gebruikt, wordt ondersteund door Cisco Content Security Management-applicatie. Dit zijn de ondersteunde identiteitsaanbieders: Microsoft Active Directory Federation Services (ADFS) 2.0 Ping Identity PingFederate 7.2 Cisco web security applicatie 9.1
- Verkrijg deze certificaten die nodig zijn om de communicatie tussen uw apparaat en de identiteitsprovider te beveiligen: Als u wilt dat uw apparaat een SAML-verificatieaanvraag indient of als u wilt dat uw identiteitsbewijs SAML-beweringen versleutelt, dient u een zelfgetekend certificaat of een certificaat te verkrijgen van een vertrouwde certificeringsinstantie (CA) en de bijbehorende privésleutel. Indien u wilt dat de identiteitsverschaffer SAML-beweringen tekent, dient u het certificaat van de identiteitskaart te verkrijgen. Uw apparaat gebruikt dit certificaat om de ondertekende SAML-beweringen te controleren

Configureren

Stap 1. Navigeer naar uw SMA en selecteer **Systeembeheer > SAML > Downloadmetagegevens**, zoals in de afbeelding getoond.

The screenshot shows the SMA interface with the following elements:

- Navigation tabs: Management Appliance, Email, Web.
- Sub-navigation: Centralized Services, Network, System Administration.
- SAML** section header.
- 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."
- A Firefox dialog box titled "Opening MyLab_SAML_metadata.xml" is open, showing:
 - You have chosen to open: **MyLab_SAML_metadata.xml** (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.
 - Buttons: OK, Cancel

Stap 2. Het profiel van de Identity Provider wordt automatisch ingevuld wanneer de klant zijn ADFS-metagegevensbestand uploadt. Microsoft heeft een standaard-URL: **https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml**.

Stap 3. Zodra beide profielen zijn ingesteld, moet de metagegevens van het SP-profiel worden bewerkt, zoals per bug [CSCvh30183](#). Metagegevens-bestand ziet eruit zoals in de afbeelding.

```

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                         ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNyw8Wtd+Io
27                         MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rnO4jtvPZPj7B
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/ZclXnPBGSMxex0277ECJq
35                         ix5aXRSxOMRRtD/72FVRAsGT3x1mBYqu/HTyOBZongM+isJHBhRZxSOMBL+45jFY
36                         PO1jBG5MZuWE
37                         -----END CERTIFICATE-----
38                 </ds:X509Certificate>
39             </ds:X509Data>

```

Stap 4. Verwijder de gemarkeerde informatie aan het einde van het metagegevensbestand zoals in de afbeelding.

```

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 MIIDZTCCAk2gAwIBAwIJA0jXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHlxIzY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
14 BAYTAK1YMRcwFQYDVQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1UEBwwEQ0RNWDEW
15 MBQGA1UECgwNVG16b25jaXRvIELuYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
16 SVQGU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWWhcNMjAwNjA0MjEwNTUxWjByMQsw
17 CQYDVQQGEwJNwDEWEXMBUGA1UEAwwOc21hLm1leGVzYS5jb20xDTALBgNVBAAcMBENE
18 TVGxYjAUBGhNVA0MDVRpem9uY210byBjBmMxDALBgNVBAGMBENETVGxYjAUBGhNVA0
19 BAsMC01UIFN1Y3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
20 g7kzRmL114q9T1klctJzo8cmscu5nRXFWlohFPcJgn/oHXEUKvUnWe+9cTJQ41X4
21 ojbGCP75UjD8GdPczkuBxqAZgkrfGNLR8mopsxTFVWb5x68tVsTBGFNyw8Wtd+Io
22 MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rn04jtvzpZj7B
23 cpWjawLlxAFUHVYvrc661Tblo0exG+hZ+AlS3B0l+6lmTNjF3IcGcGS/TE0chETx
24 glScUk0iMipnPEtAZey/ebyh18EpH/WViNwZkMUjINvmIFq3+LkF8As8B1Pm6YHi
25 L6K8W4voEj1njtmnC/EQIQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB3vxnL7jb
26 emMTKSRP4hycUld69z2xGQC5e2EeyhnRgHUz7F/TEv0NkORotFii2oOJ6yGEOdWD
27 6+Bvj6wSBp7UoLyBdCxglyi+vK4Y/R2+iCv13pyaXkbF0QsJvYpzOg7xSjKXzm79
28 +ZIjQkekyCAM5N0of1ZRrJ9oGD5qoY1Zjhud7NHmRbj7LKHRKsFVqpKet/tTXCH7
29 7EuB+ogT7pvrTDJ/QoIKcvYkbXuZ30JNVPxxKacjAVj/Zc1XnFBGSMxexo277ECJq
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 MIIDZTCCAk2gAwIBAwIJA0jXJ35sNw2bMA0GCSqGSIb3DQEBCwUAMHlxIzY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
41 BAYTAK1YMRcwFQYDVQDDA5zbWEubWV4ZXNhLmNvbTENMAsGA1UEBwwEQ0RNWDEW
42 MBQGA1UECgwNVG16b25jaXRvIELuYzENMAsGA1UECAwEQ0RNWDEUMBIGA1UECwwL
43 SVQGU2VjdXJpdHkwHhcNMTkwNjA1MjEwNTUxWWhcNMjAwNjA0MjEwNTUxWjByMQsw

```

Stap 5. Navigeer naar uw ADFS en voer het bewerkte metagegevensbestand in de ADFS-tools > AD FS-beheer > Add Relying Party Trust, zoals in de afbeelding getoond.

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

Stap 6. Nadat u met succes het metagegevensbestand hebt geïmporteerd, dient u de claimregels te configureren voor het nieuwe vertrouwen van de Relay Party, selecteert u de optie **Claim Rule sjabloon > Verzend LDAP-kenmerken**, zoals in de afbeelding weergegeven.

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.

Stap 7. Geef de naam van de Claim Rule aan, en selecteer **Bewaren van Kenmerken > Actieve Map**.

Stap 8. Kaart u LDAP-kenmerken, zoals in de afbeelding.

- LDAP-kenmerk > E-mailadressen
- Type aflopende vordering > E-mailadres

The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box, specifically the 'Configure Rule' step. The window title is 'Add Transform Claim Rule Wizard'. On the left, there is a 'Steps' pane with two items: 'Choose Rule Type' (highlighted in blue) and 'Configure Claim Rule' (highlighted in green). The main area contains the following information:

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)
▶	<input type="text" value="E-Mail-Addresses"/>	<input type="text" value="E-Mail Address"/>
*	<input type="text"/>	<input type="text"/>

At the bottom right, there are three buttons: '< Previous', 'Finish', and 'Cancel'.

Stap 9. Maak een nieuwe Aangepaste claim met deze informatie, zoals in de afbeelding.

Dit is de aangepaste regel die aan de regel Eigen claim moet worden toegevoegd:

```
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");
```

Edit Rule - charella_custom_rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:

charella_custom_rule

Rule template: Send Claims Using a Custom Rule

Custom rule:

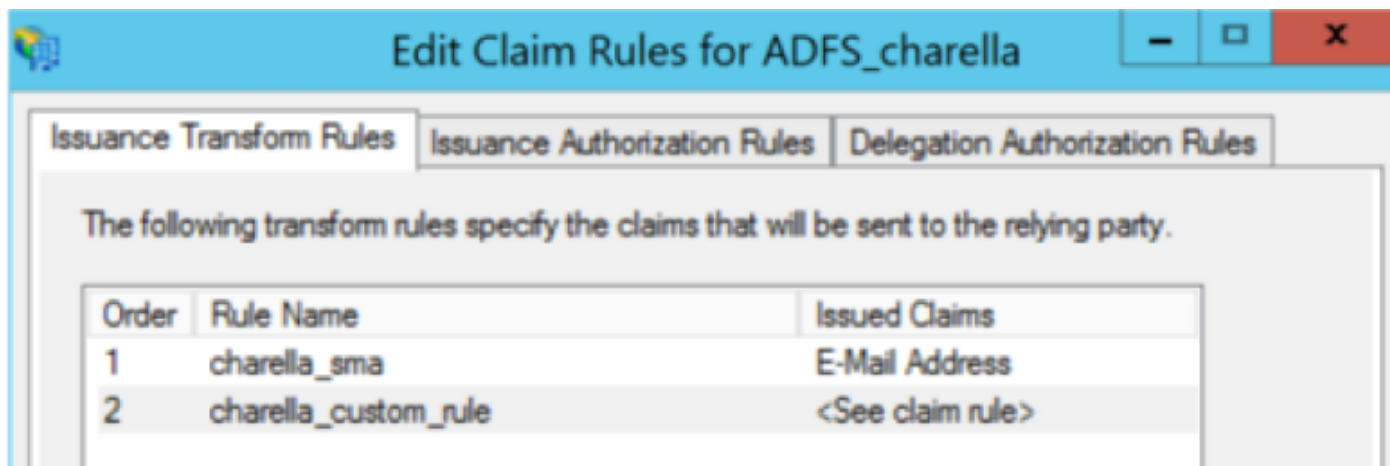
```
c:[Type ==
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue (Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value,
ValueType = c.ValueType, Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format
"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spname
qualifier"] = "https://dh106-euq1.rl.ces.cisco.com/");
```

OK

Cancel

- Wijzig de gemarkeerde URL met de SMA-hostname en poort (als u op een CES-omgeving bent, is er geen poort vereist, maar u moet deze naar euq1 wijzen.<toewijzing>.iphmx.com)

Stap 10. Zorg ervoor dat de order van de eisingsregel: LDAP claimregel eerst en Aangepaste claim tweede, zoals in de afbeelding wordt weergegeven.



Stap 11. Meld u aan bij het EUQ, dan moet u deze opnieuw naar de ADFS-host sturen.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- [CSCv30183](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)