Install Metadata File on the ADFS

Contents

Introduction

This document describes how to install metadata file on the Microsoft Active Directory Federation Services (ADFS).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ADFS
- Security Assertion Markup Language (SAML) integration with Security Management Appliance

Components Used

The information in this document is based on these software and hardware versions:

- 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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Before the Metadata file is installed in the ADFS, ensure that these requirements are addressed:

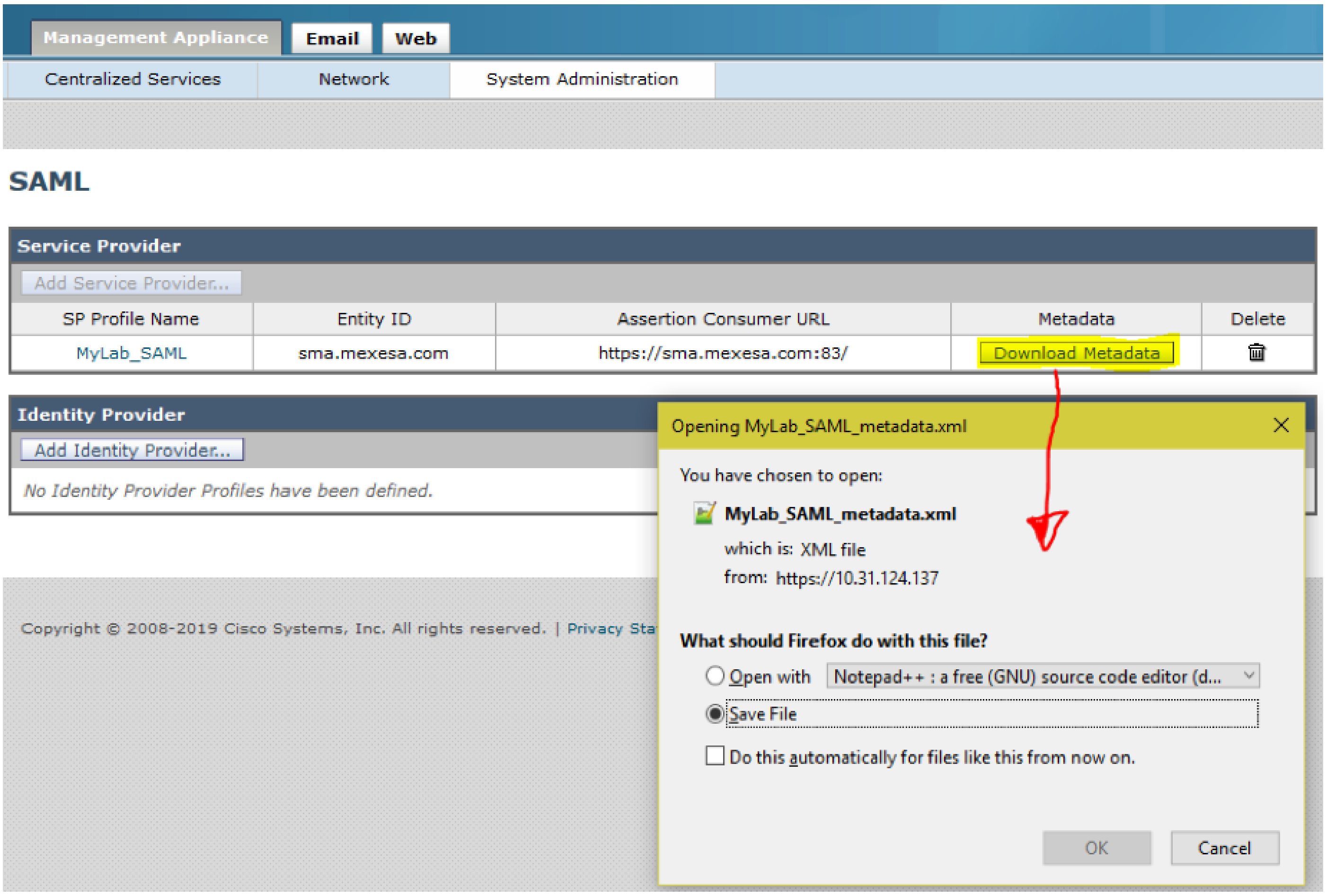
- SAML enabled in the SMA
- Verify whether the identity provider used by your organization is supported by Cisco Content

Security Management Appliance. These are the supported identity providers: Microsoft Active Directory Federation Services (ADFS) 2.0Ping Identity PingFederate 7.2Cisco Web Security Appliance 9.1

- Obtain these certificates that are required to secure the communication between your appliance and the identity provider:If you want your appliance to sign SAML authentication requests or if you want your identity provider to encrypt SAML assertions, obtain a self-signed certificate or a certificate from a trusted Certificate Authority (CA) and the associated private key.If you want the identity provider to sign SAML assertions, obtain the identity provider’s certificate. Your appliance uses this certificate to verify the signed SAML assertions

Configure

Step 1. Navigate to your SMA and select **System Administration > SAML > Download Metadata**, as shown in the image.



SAML

Service Provider

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

Identity Provider

No Identity Provider Profiles have been defined.

Copyright © 2008-2019 Cisco Systems, Inc. All rights reserved. | Privacy Sta

Opening MyLab_SAML_metadata.xml

You have chosen to open:

MyLab_SAML_metadata.xml

which is: XML file

from: https://10.31.124.137

What should Firefox do with this file?

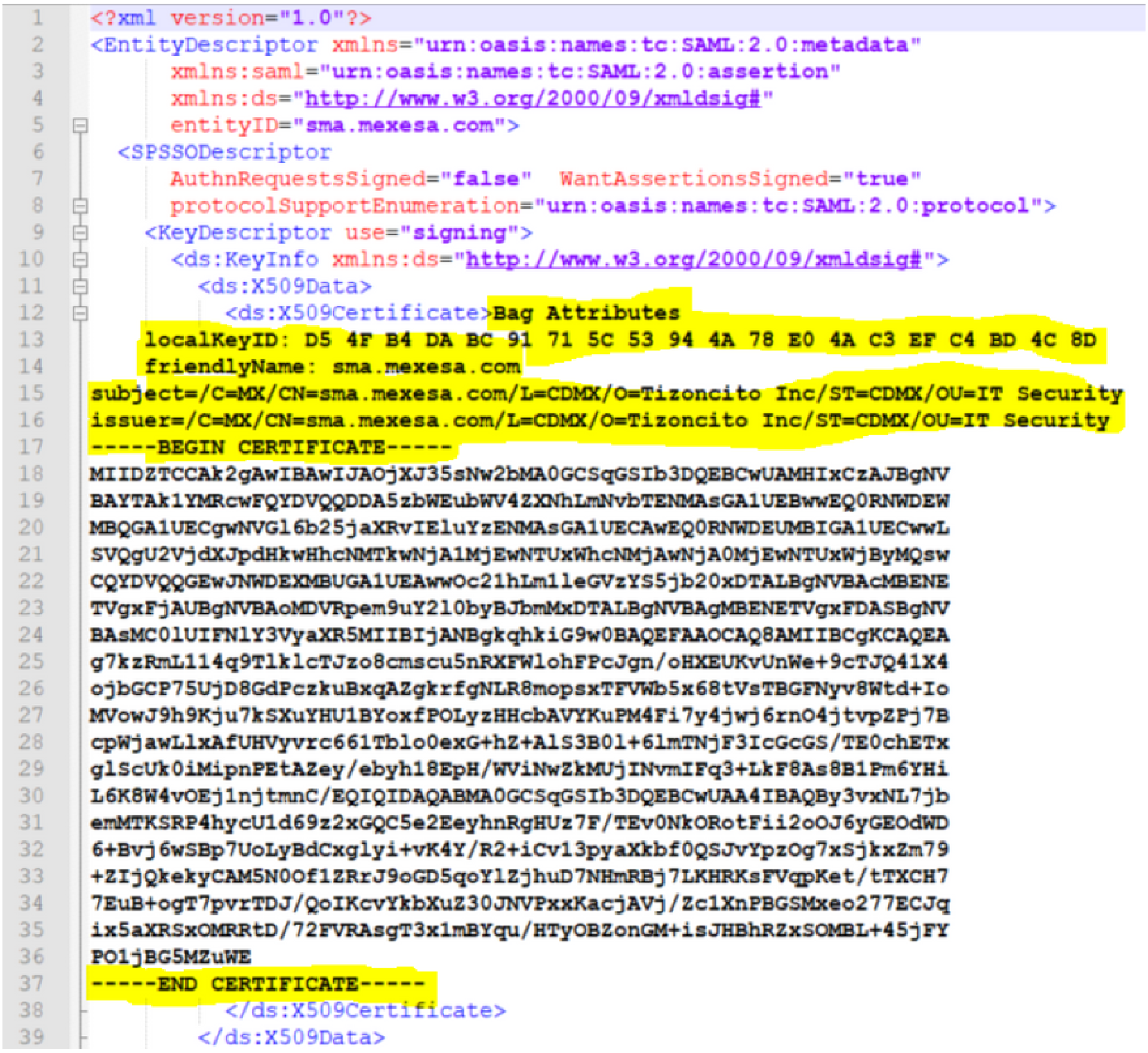
○ Open with Notepad++ : a free (GNU) source code editor (d...

● Save File

□ Do this automatically for files like this from now on.

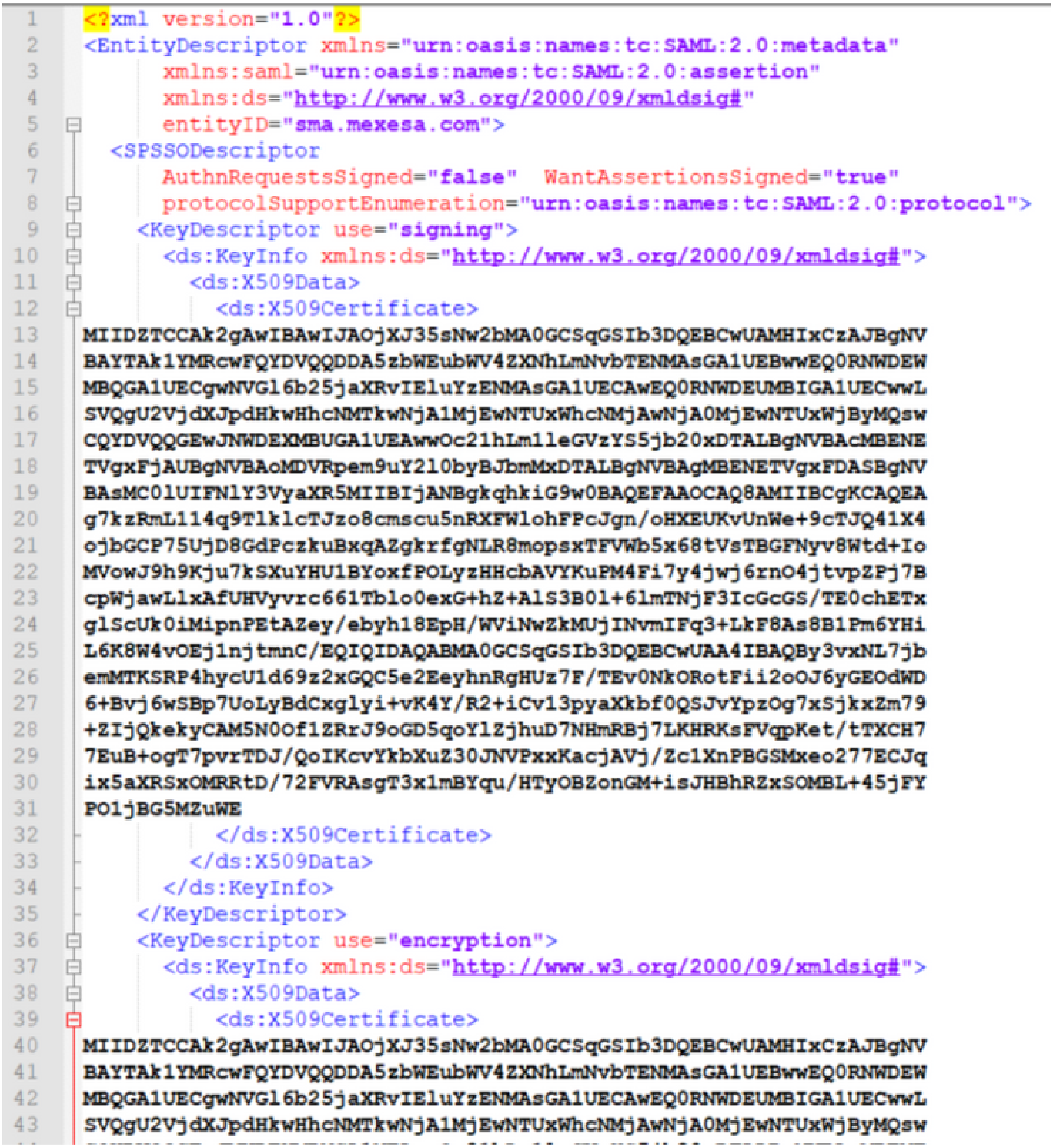
Step 2. The Identity Provider Profile fills out automatically when the Customer uploads his ADFS Metadata file. Microsoft has a default URL: **https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml.**

Step 3. Once both profiles are setup, the SP Profile Metadata must be edited, as per bug CSCvh30183.. Metadata file looks as shown in the image.



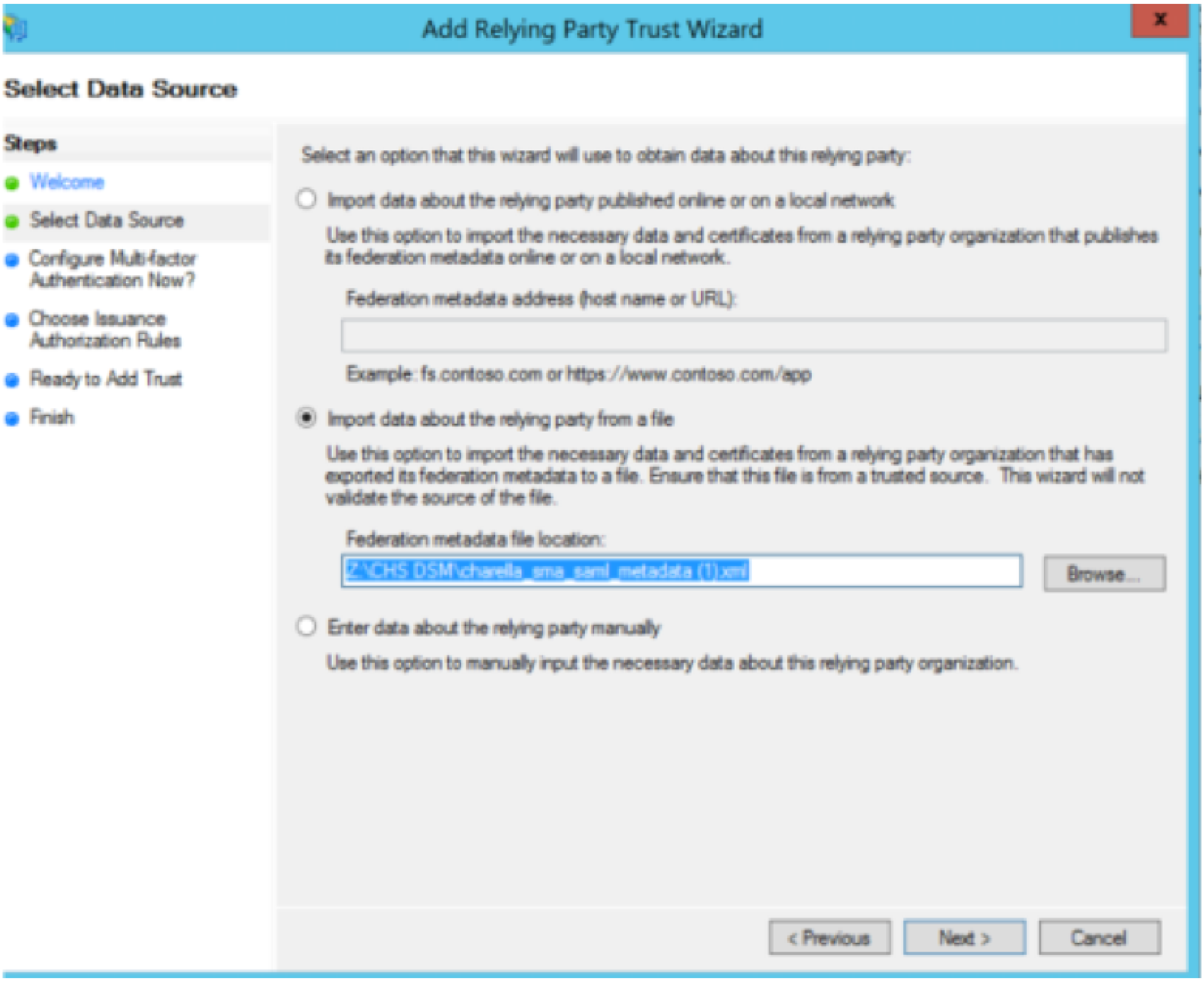
```
<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
      entityID="sma.mexesa.com">
  <SPSSODescriptor
      AuthnRequestsSigned="false"  WantAssertionsSigned="true"
      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>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>
```

Step 4. Remove the highlighted information, at the end Metadata file must be as shown in the image.



```xml
<?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
g7kzRmL114q9Tlk1cTJzo8cmscu5nRXFWlohFPcJgn/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
```

Step 5. Navigate to your ADFS and import the edited Metadata file in the **ADFS Tools > AD FS Management > Add Relying Party Trust**, as shown in the 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.

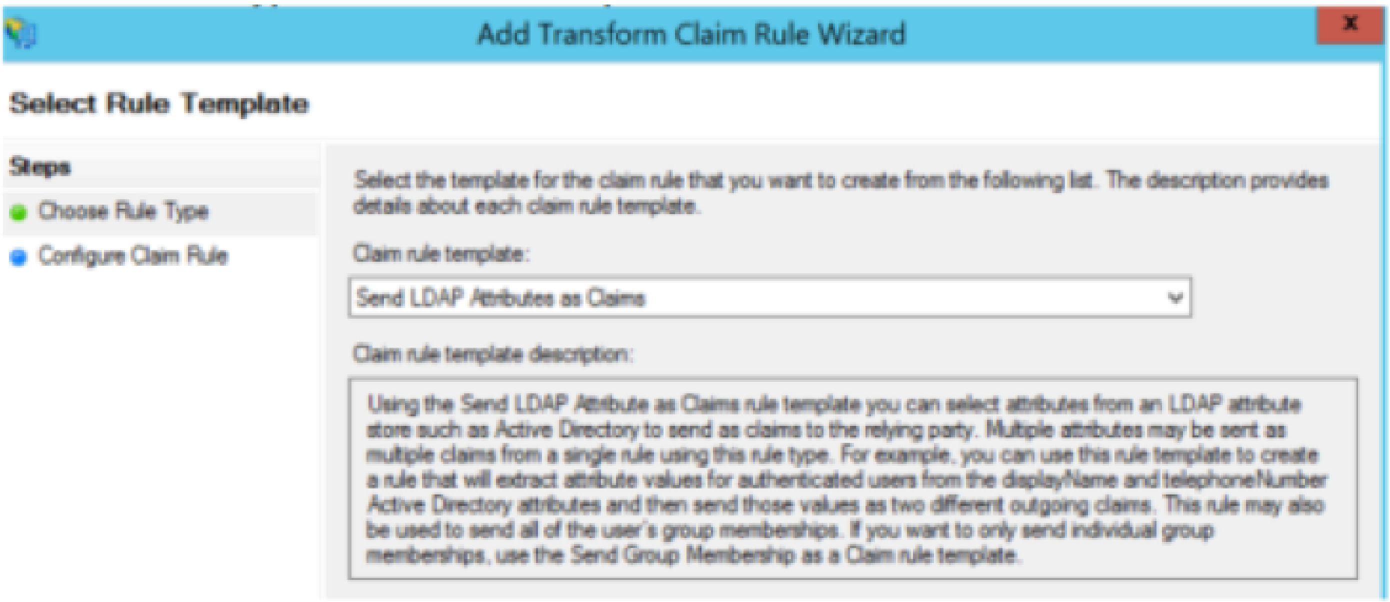
Federation metadata file location:

Z:\CHS DSM\charella_sma_saml_metadata (1).xml

○ Enter data about the relying party manually

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

Step 6. After you successfully import the Metadata File, configure the Claim Rules for the newly created Relying Party Trust, select **Claim rule template > Send LDAP Attributes**, as shown in the 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:

Send LDAP Attributes as Claims

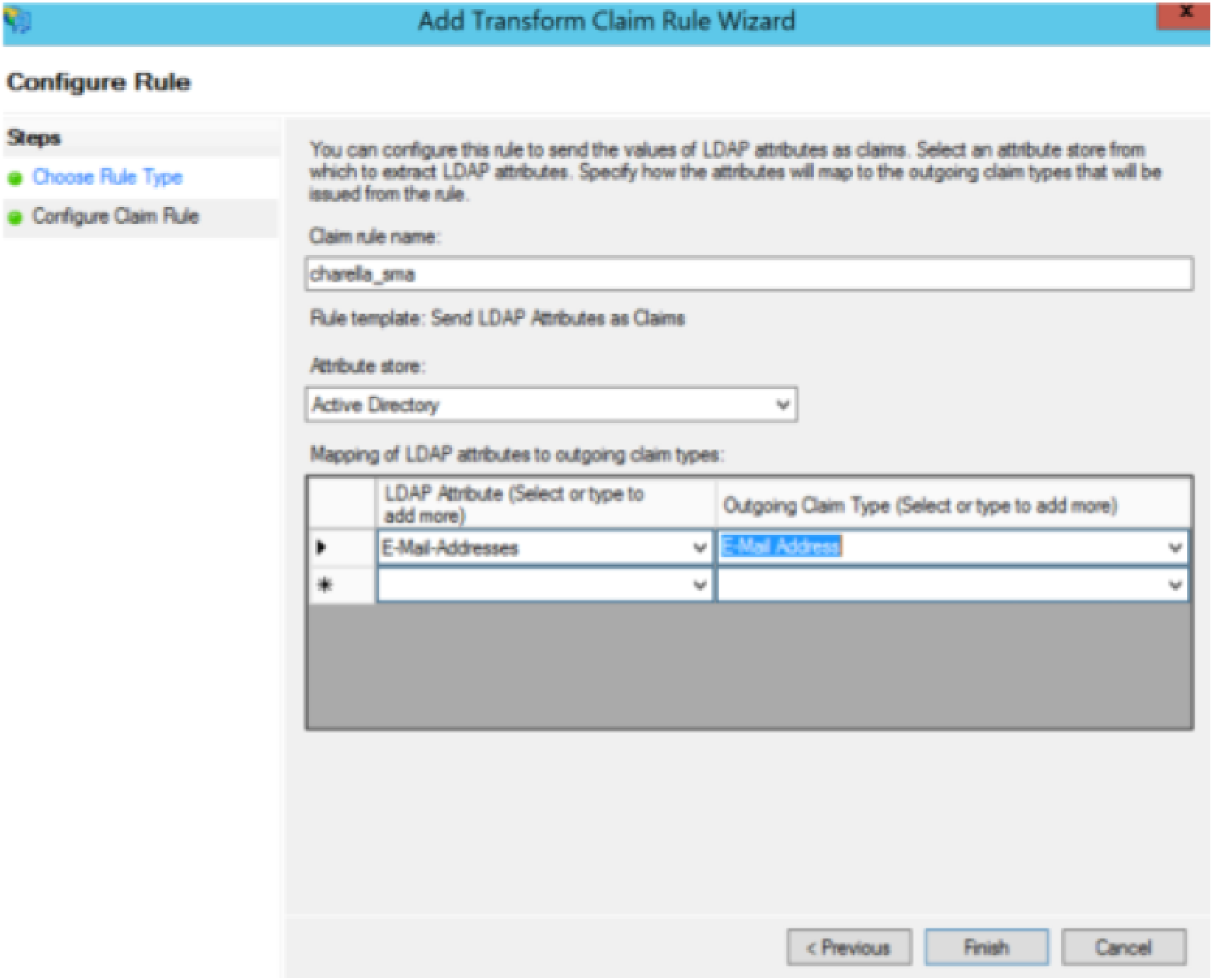
Claim rule template description:

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.

Step 7. Name the Claim rule name, and select **Attribute Store > Active Directory**.

Step 8. Map LDAP Attributes, as shown in the image.

- **LDAP Attribute > E-Mail-Addresses**
- **Outgoing Claim Type > E-Mail-Address**



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:

charella_sma

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

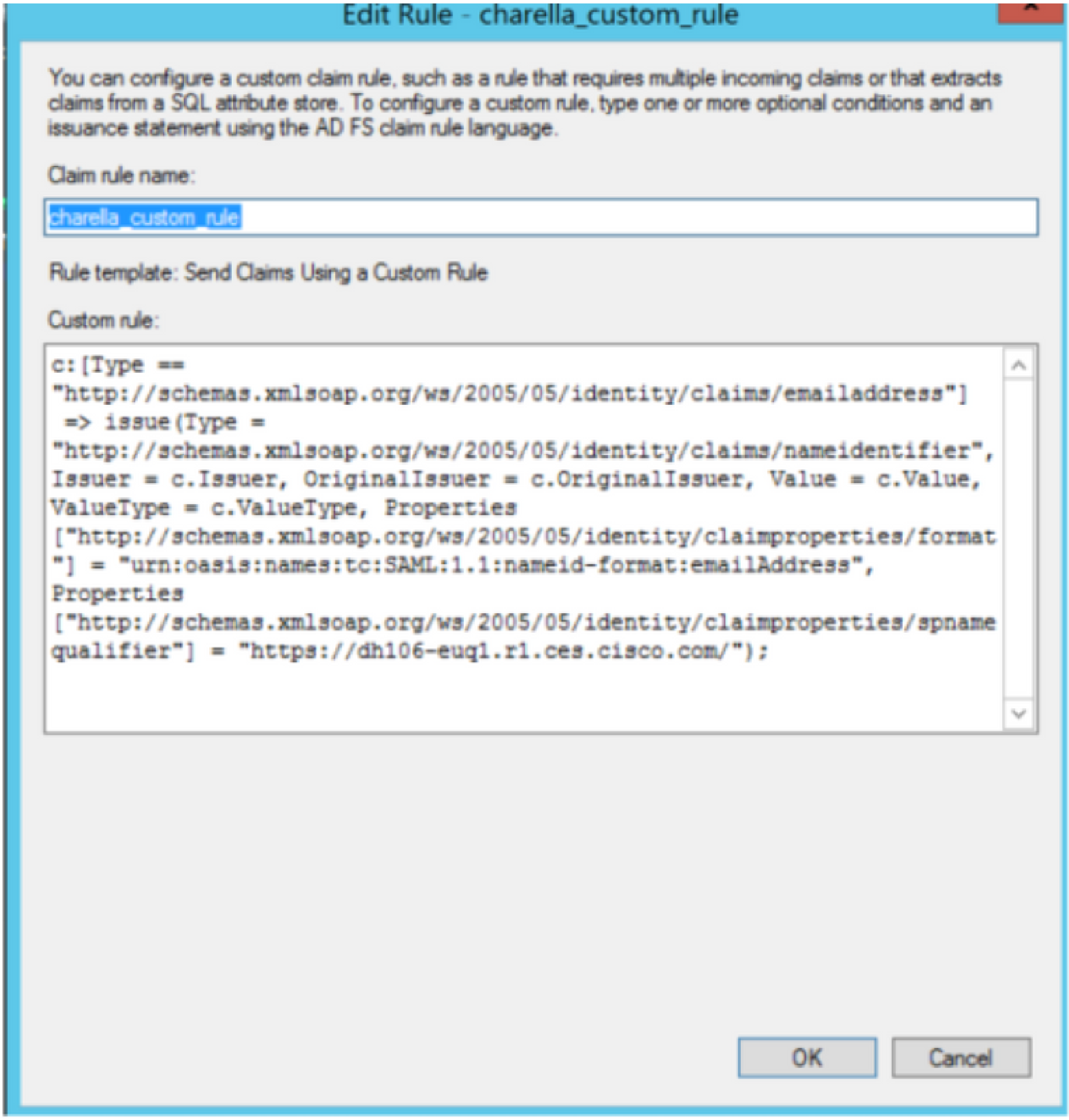
Mapping of LDAP attributes to outgoing claim types:

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

Step 9. Create a new Custom Claim rule with this information, as shown in the image.

This is the custom rule that needs to be added to the Custom Claim 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/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

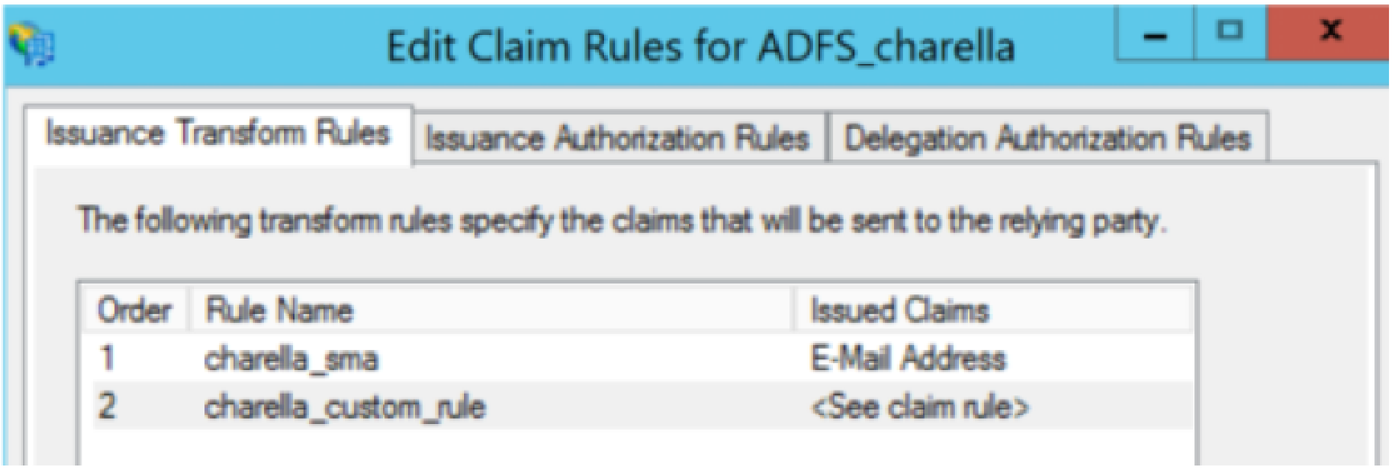
Rule template: Send Claims Using a Custom Rule

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.r1.ces.cisco.com/");
```

- Modify the highlighted URL with the SMA hostname and port (if you are on a CES environment, a port is not required but it must point to euq1.<allocation>.iphmx.com)

Step 10. Ensure that the Claim rule order is: LDAP claim rule first and Custom Claim rule second, as shown in the image.


Edit Claim Rules for ADFS_charella

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	charella_sma	E-Mail Address
2	charella_custom_rule	<See claim rule>

Step 11. Log in to the EUQ, it must redirect to the ADFS host.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **CSCvh30183**
- **Technical Support & Documentation - Cisco Systems**