

Installieren der Metadatendatei auf dem ADFS

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument beschreibt, wie die Metadatendatei auf Microsoft Active Directory Federation Services (ADFS) installiert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- ADFS
- Integration von Security Assertion Markup Language (SAML) in Security Management Appliance

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Bevor die Metadatendatei im ADFS installiert wird, stellen Sie sicher, dass diese Anforderungen erfüllt sind:

- SAML aktiviert in SMA
- Überprüfen Sie, ob der von Ihrem Unternehmen verwendete Identitätsanbieter von der Cisco Content Security Management Appliance unterstützt wird. Dies sind die unterstützten Identitätsanbieter: Microsoft Active Directory Federation Services (ADFS) 2.0 Ping Identity Ping Federate 7.2 Cisco Web Security Appliance 9.1
- Rufen Sie die folgenden Zertifikate ab, die zum Sichern der Kommunikation zwischen Ihrer Appliance und dem Identitätsanbieter erforderlich sind: Wenn die Appliance SAML-Authentifizierungsanforderungen signieren soll oder wenn der Identitätsanbieter SAML-Assertionen verschlüsseln soll, erhalten Sie ein selbstsigniertes Zertifikat oder ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) und dem zugehörigen privaten Schlüssel. Wenn der Identitätsanbieter SAML-Assertionen signieren soll, rufen Sie das Zertifikat des Identitätsanbieters ab. Die Appliance überprüft mithilfe dieses Zertifikats die signierten SAML-Assertionen.

Konfigurieren

Schritt 1: Navigieren Sie zu Ihrem SMA, und wählen Sie **Systemverwaltung > SAML > Metadaten herunterladen aus**, wie im Bild gezeigt.

The screenshot shows the SMA web interface. At the top, there are tabs for 'Management Appliance', 'Email', and 'Web'. Below that, there are tabs for 'Centralized Services', 'Network', and 'System Administration'. The 'SAML' section is active, showing a 'Service Provider' table with one entry: 'MyLab_SAML' with Entity ID 'sma.mexesa.com' and Assertion Consumer URL 'https://sma.mexesa.com:83/'. The 'Metadata' column for this entry has a yellow 'Download Metadata' button. A red arrow points from this button to a Firefox dialog box that has opened, showing the file 'MyLab_SAML_metadata.xml' and the option 'Save File' selected.

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

Schritt 2: Das Identitätsanbieter-Profil wird automatisch ausgefüllt, wenn der Kunde seine ADFS-Metadatendatei hochlädt. Microsoft hat eine Standard-URL: **https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml**.

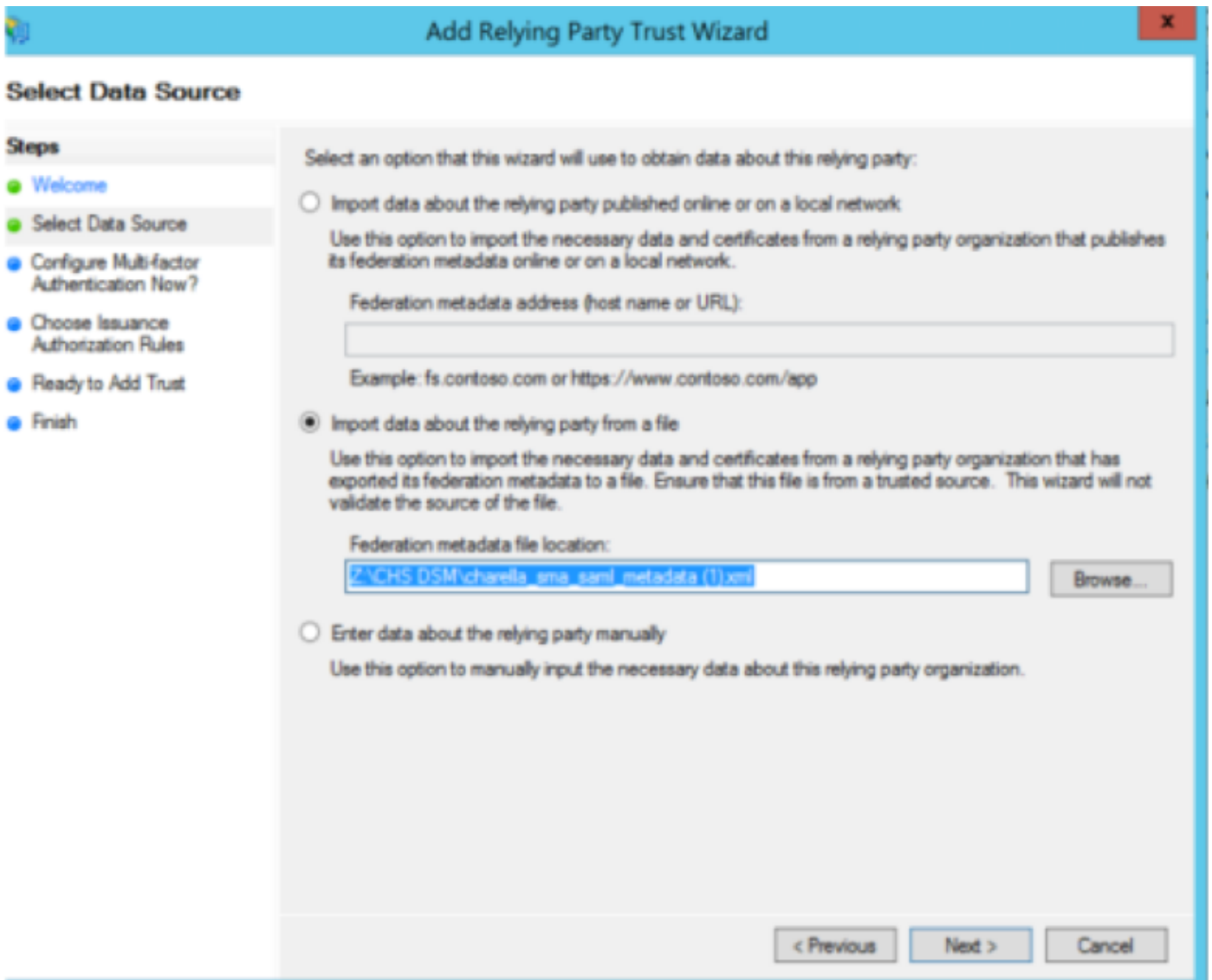
Schritt 3: Nach dem Einrichten beider Profile muss die SP Profile Metadata entsprechend dem Fehler [CSCvh30183](#) bearbeitet werden. Metadatendatei sieht wie im Bild gezeigt aus.

```

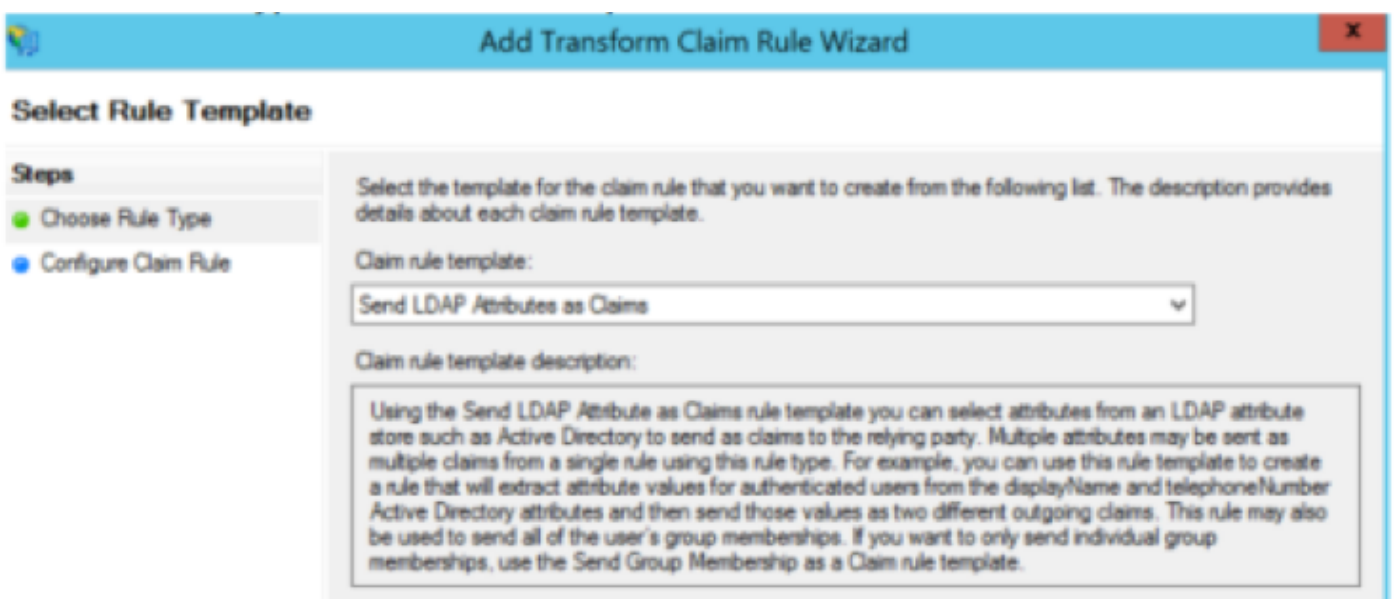
1  <?xml version="1.0"?>
2  <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
3      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
4      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
5      entityID="sma.mexesa.com">
6      <SPSSODescriptor
7          AuthnRequestsSigned="false" WantAssertionsSigned="true"
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                         BAYTAK1YMRcwFQYDVQQDDA5zbWEubWV4ZXXNhLmNvbTENCMAsgAlUEBwwEQ0RNWDEW
20                         MBQGA1UECgwNVG16b25jaXRvIEluYzENMAsgAlUECAwEQ0RNWDEUMBIGAlUECwwL
21                         SVQGU2VjdXJpdHkwHhcNMjkwNjA1MjEwNTUxWWhcNMjAwNjEwNTUxWjByMQsw
22                         CQYDVQQGEwJNWDEwXG16b25jaXRvIEluYzENMAsgAlUEAwOc21hLm1leGVzYS5jb20xDTALBgNVBACMBENE
23                         TVGxVjAUBG9wVBAoMDVRpem9uY210byBJbmMxDTALBgNVBAGMBENETVgxFDASBgNV
24                         BAsMC0lUIFNlY3VyaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
25                         g7kzRmL114q9TlklcTJzo8cmscu5nRXFWlohFPcJgn/oHXEUKvUnWe+9cTJQ41X4
26                         ojbGCP75UjD8GdPczkuBxqAZgkrfgNLR8mopsxTFVWb5x68tVsTBGFNyw8Wtd+Io
27                         MVowJ9h9Kju7kSXuYHU1BYoxfPOLyzHHcbAVYKuPM4Fi7y4jwj6rn04jtvPZp7B
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/72FVRAsGT3x1mBYqu/HTyOBZongM+isJHBhRZxSOMBL+45jFY
36                         PO1jBG5MZuWE
37                         -----END CERTIFICATE-----
38                     </ds:X509Certificate>
39                 </ds:X509Data>

```

Schritt 4: Entfernen Sie die hervorgehobenen Informationen, am Ende muss die Metadaten-datei wie im Bild gezeigt sein.



Schritt 6: Nachdem Sie die Metadatei erfolgreich importiert haben, konfigurieren Sie die Anspruchsregeln für die neu erstellte Vertrauenswürdigkeit der Partei. Wählen Sie **Anspruchsregelvorlage > LDAP-Attribute senden aus**, wie im Bild gezeigt.



Schritt 7: Nennen Sie den Namen der Anspruchsregel, und wählen Sie **Attributspeicher > Active Directory** aus.

Schritt 8: Zuordnen von LDAP-Attributen, wie im Bild gezeigt.

- LDAP-Attribut > E-Mail-Adressen
- Ausgehender Anspruchstyp > E-Mail-Adresse

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: charella_sma

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

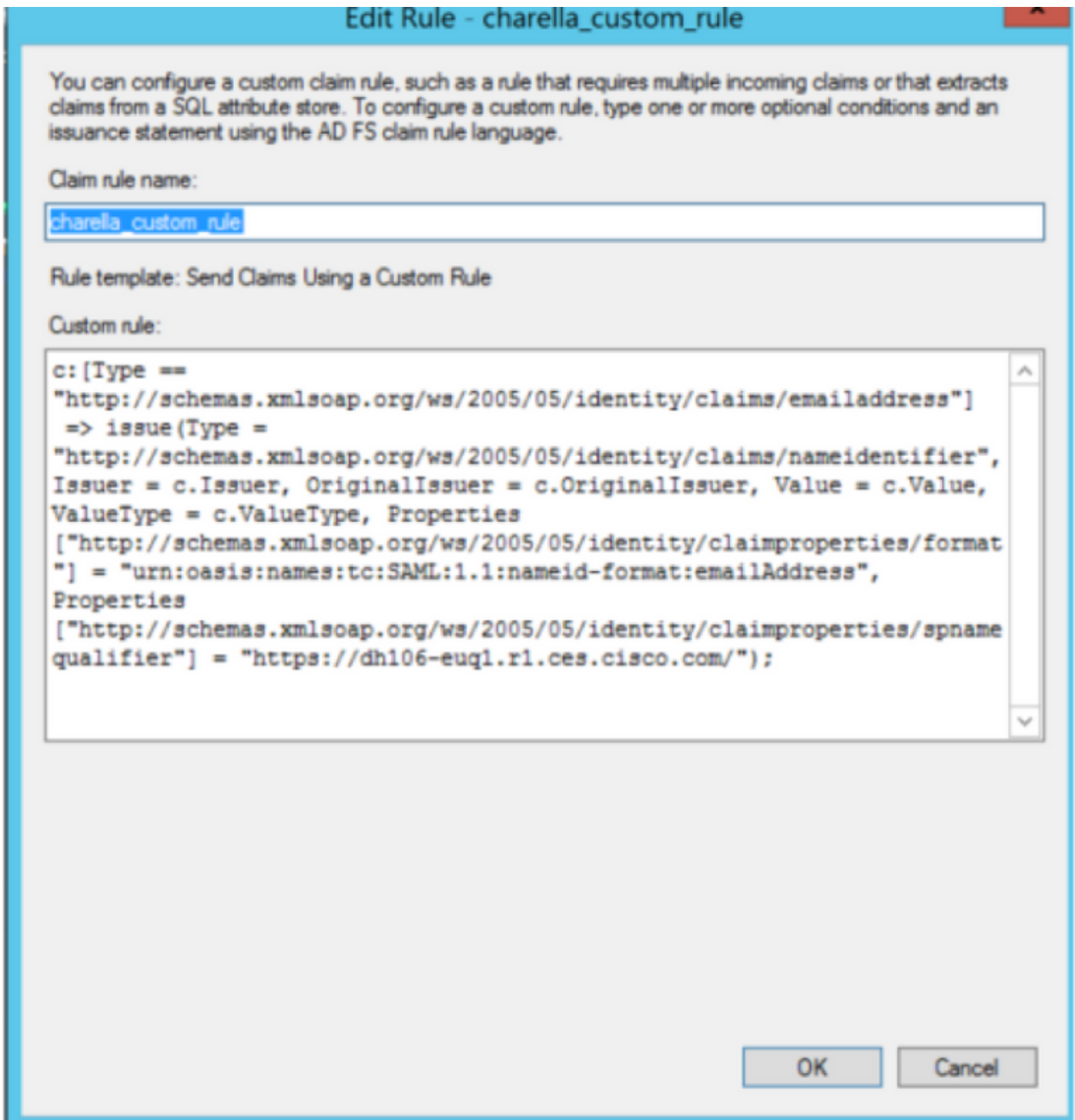
| | LDAP Attribute (Select or type to add more) | Outgoing Claim Type (Select or type to add more) |
|---|---|--|
| ▶ | E-Mail-Addresses | E-Mail Address |
| * | | |

< Previous Finish Cancel

Schritt 9: Erstellen Sie eine neue benutzerdefinierte Anspruchsregel mit diesen Informationen, wie im Bild gezeigt.

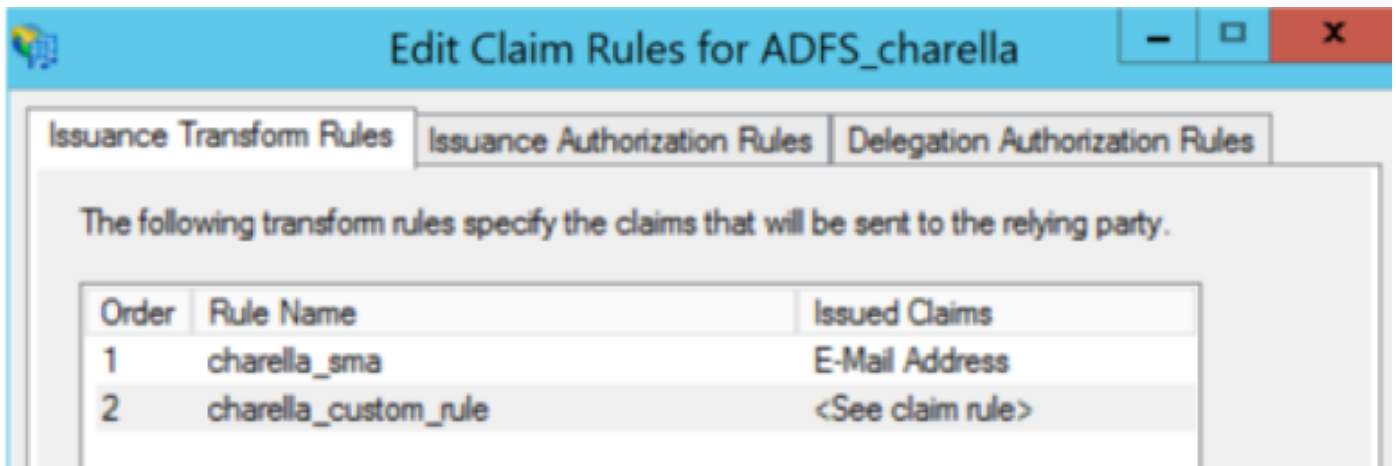
Dies ist die benutzerdefinierte Regel, die der benutzerdefinierten Anspruchsregel hinzugefügt werden muss:

```
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");
```



- Ändern Sie die hervorgehobene URL mit dem SMA-Hostnamen und -Port (wenn Sie sich in einer CES-Umgebung befinden, ist kein Port erforderlich, aber er muss auf euq1 verweisen.<allocation>.iphmx.com.

Schritt 10: Stellen Sie sicher, dass die Reihenfolge der Anspruchsregel folgendermaßen lautet: Die LDAP-Anspruchsregel wird zuerst und die benutzerdefinierte Anspruchsregel die zweite ausgeführt, wie im Bild gezeigt.



Schritt 11: Melden Sie sich beim EUQ an, muss dieser zum ADFS-Host umgeleitet werden.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [CSCvh30183](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)