Installieren der Metadatendatei auf dem ADFS

Inhalt

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.

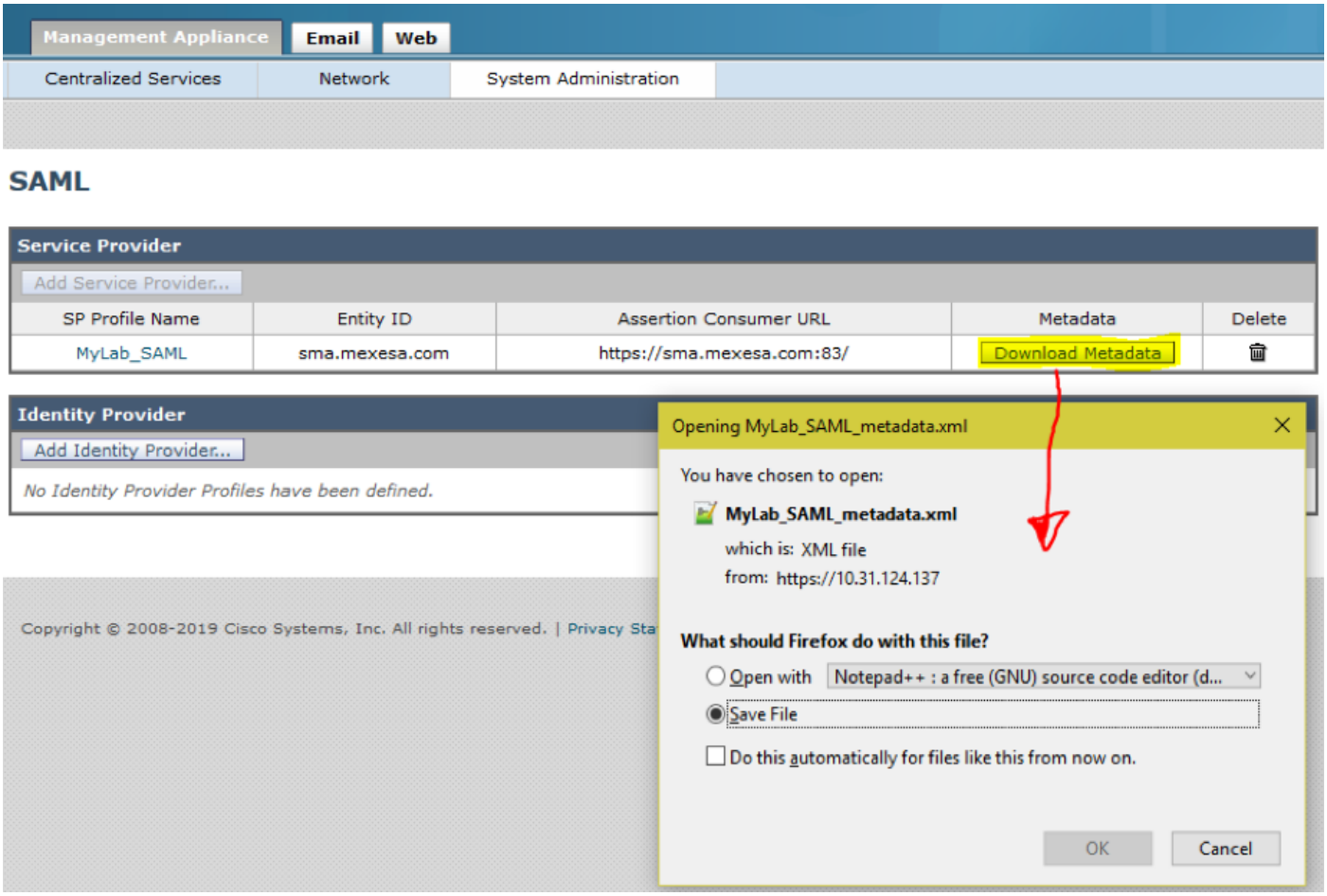
Hintergrundinformationen

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) 2.0Ping Identity Ping Federate 7.2Cisco 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.

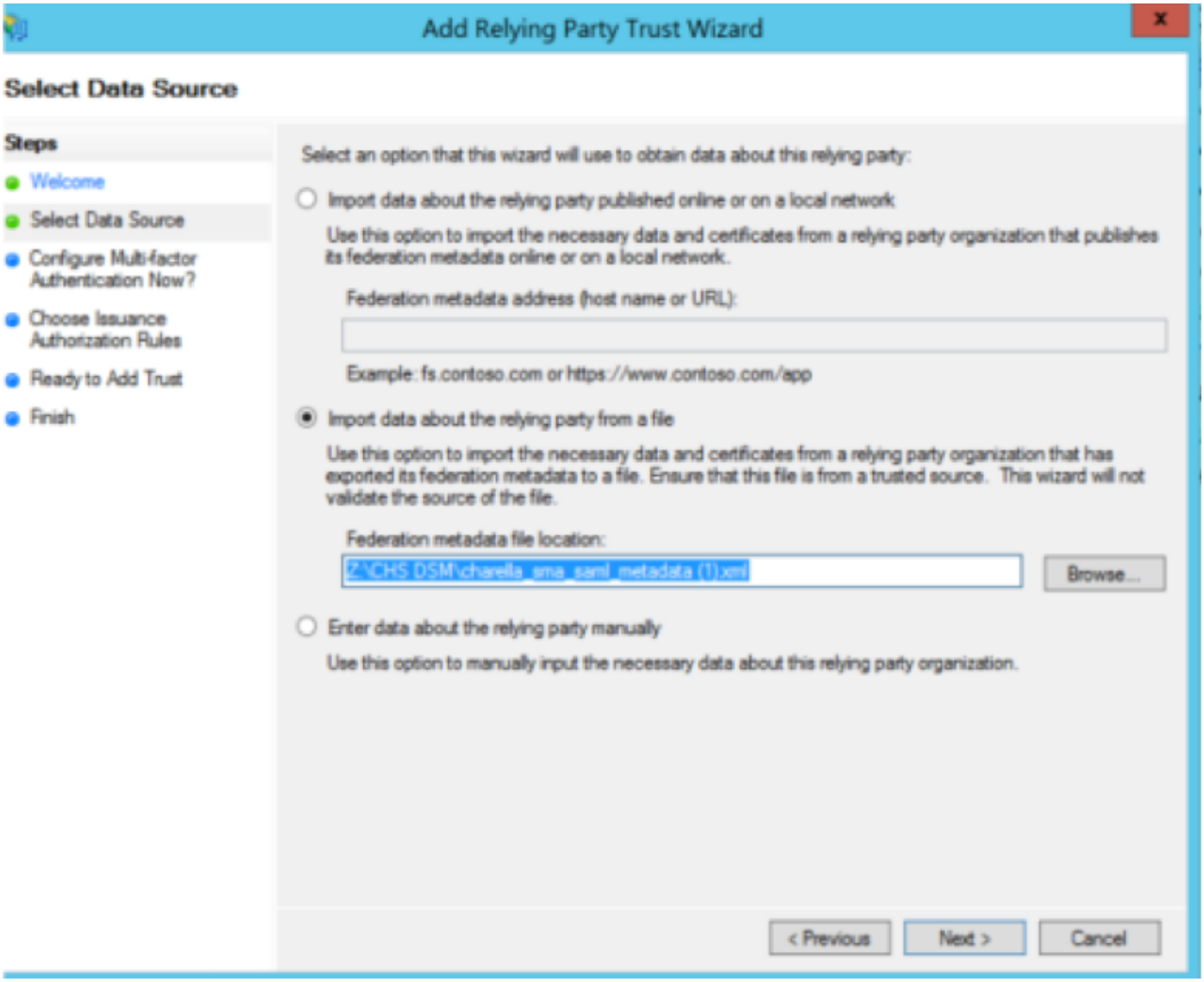


Schritt 2: Das Identitätsanbieter-Profil wird automatisch ausgefüllt, wenn der Kunde seine ADFS-Metadatendatei hochlädt. Microsoft hat eine Standard-URL: **https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml.**

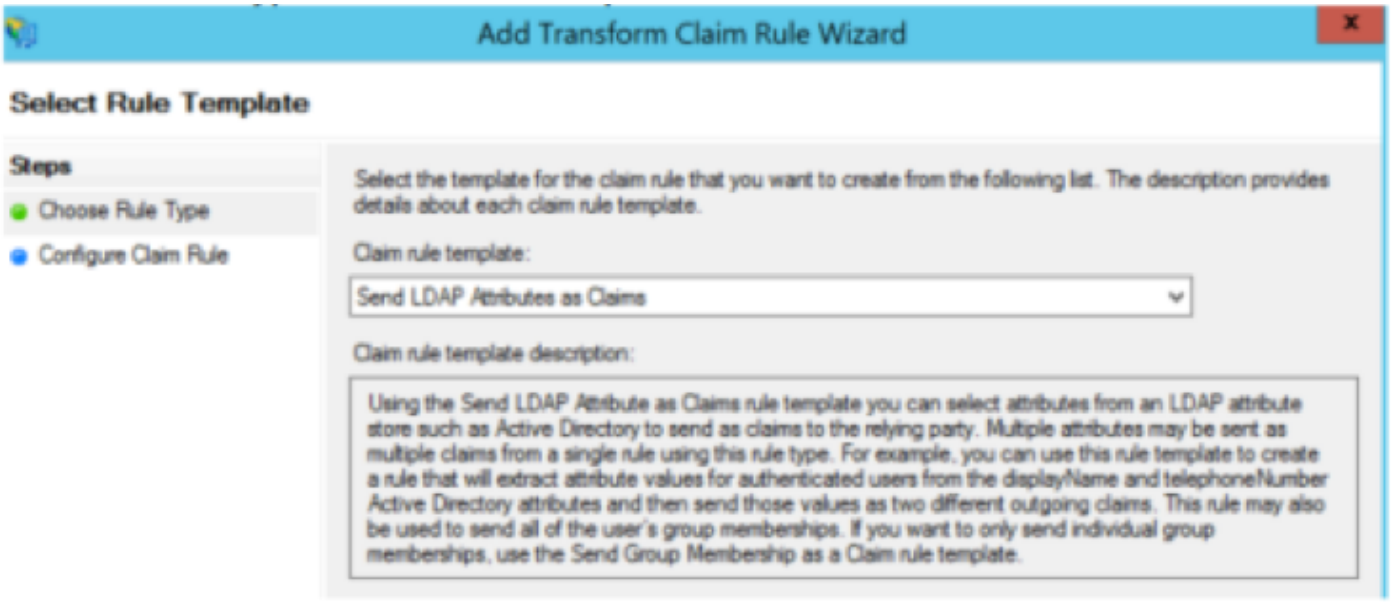
Schritt 3: Nach dem Einrichten beider Profile muss die SP Profile Metadata entsprechend dem Fehler CSCvh30183 bearbeitet werden.. Metadatendatei sieht wie im Bild gezeigt aus.

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

Schritt 5: Navigieren Sie zu Ihrem ADFS, und importieren Sie die bearbeitete Metadatendatei in **ADFS Tools > AD FS Management > Add Relying Party Trust**, wie im Bild gezeigt.



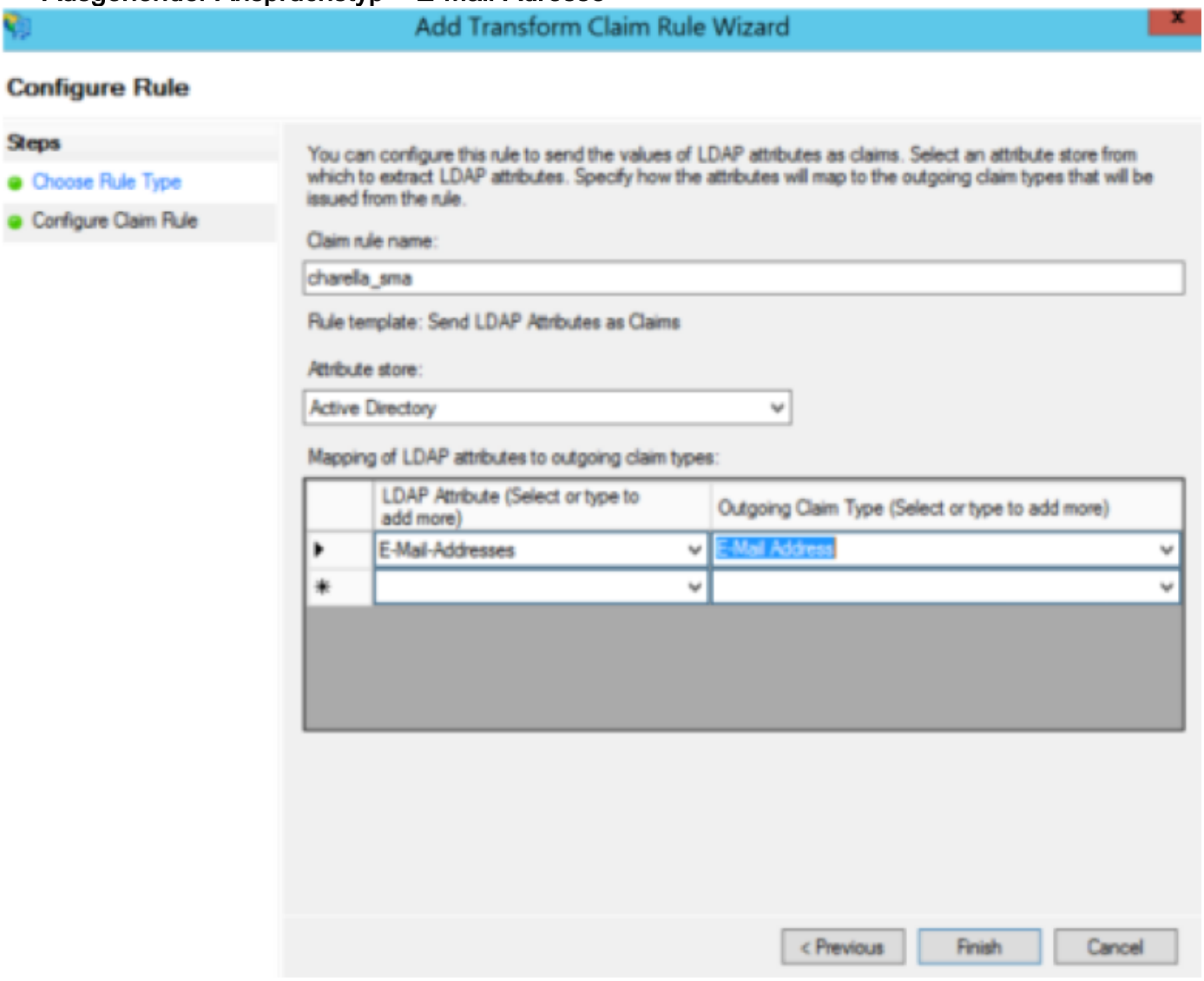
Schritt 6: Nachdem Sie die Metadatendatei erfolgreich importiert haben, konfigurieren Sie die Anspruchsregeln für die neu erstellte Vertrauenswürdigkeit der Partei. Wählen Sie **Anspruchsregelvorlage > LDAP-Attribute senden aus**, wie im Bild gezeigt.



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.

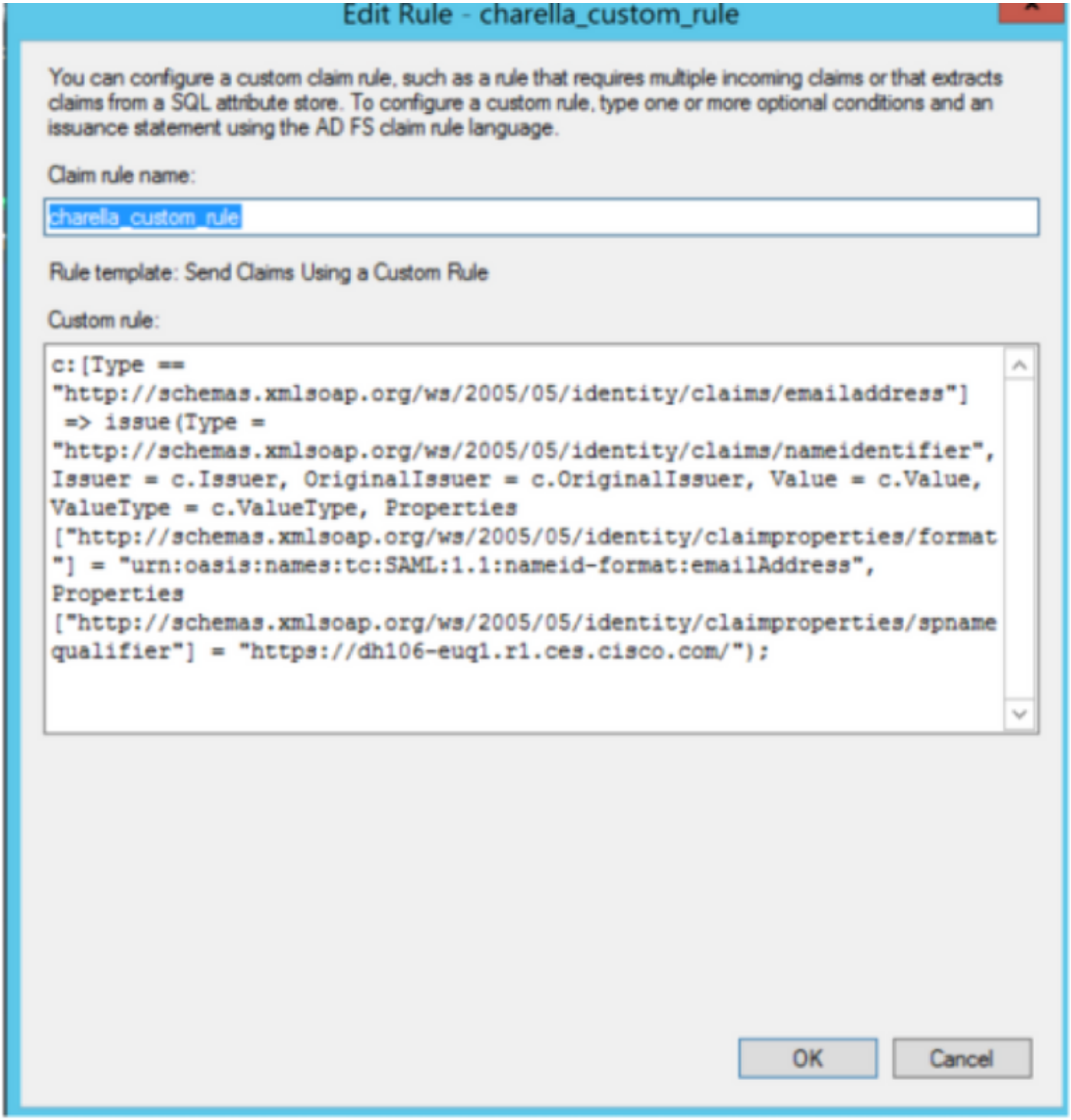
- **LDAP-Attribut > E-Mail-Adressen**
- **Ausgehender Anspruchstyp > E-Mail-Adresse**



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

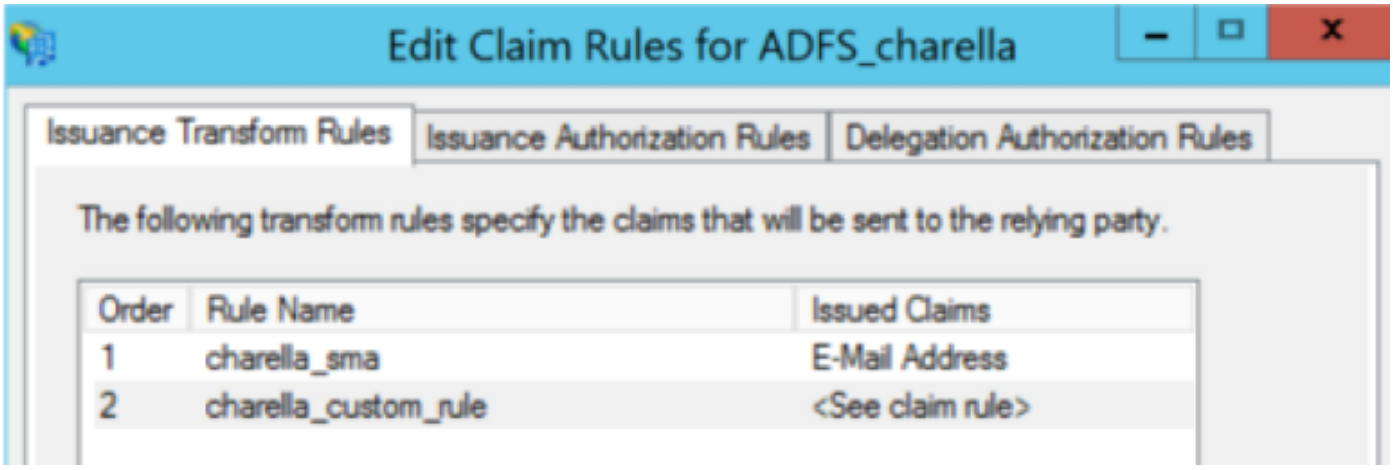
Dies ist die benutzerdefinierte Regel, die der benutzerdefinierten Anspruchsregel hinzugefügt werden muss:

```
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