Metagegevens-bestand op ADFS installeren

Inhoud

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.

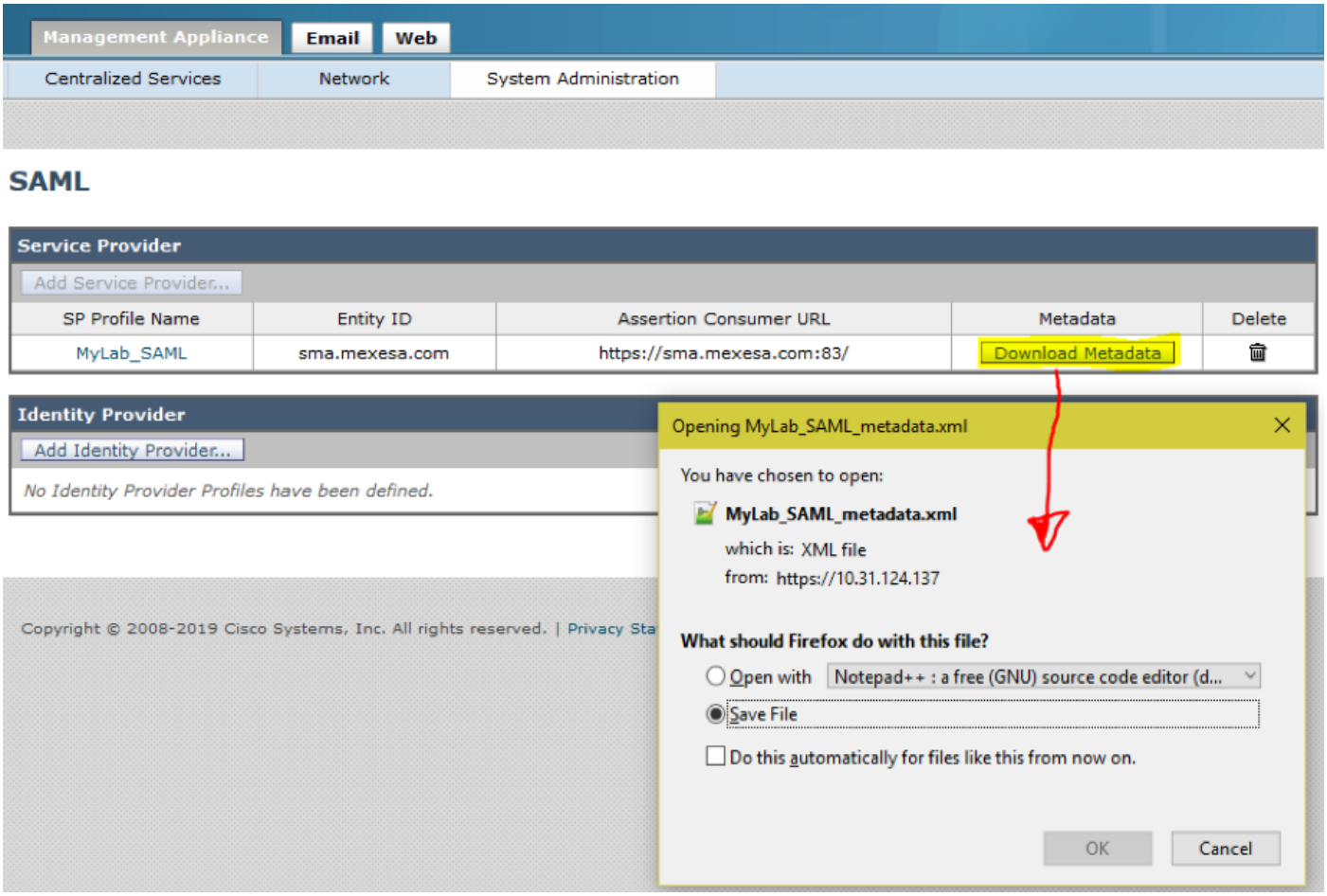
Achtergrondinformatie

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) 2.0Ping Identity PingFederate 7.2Cisco 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.

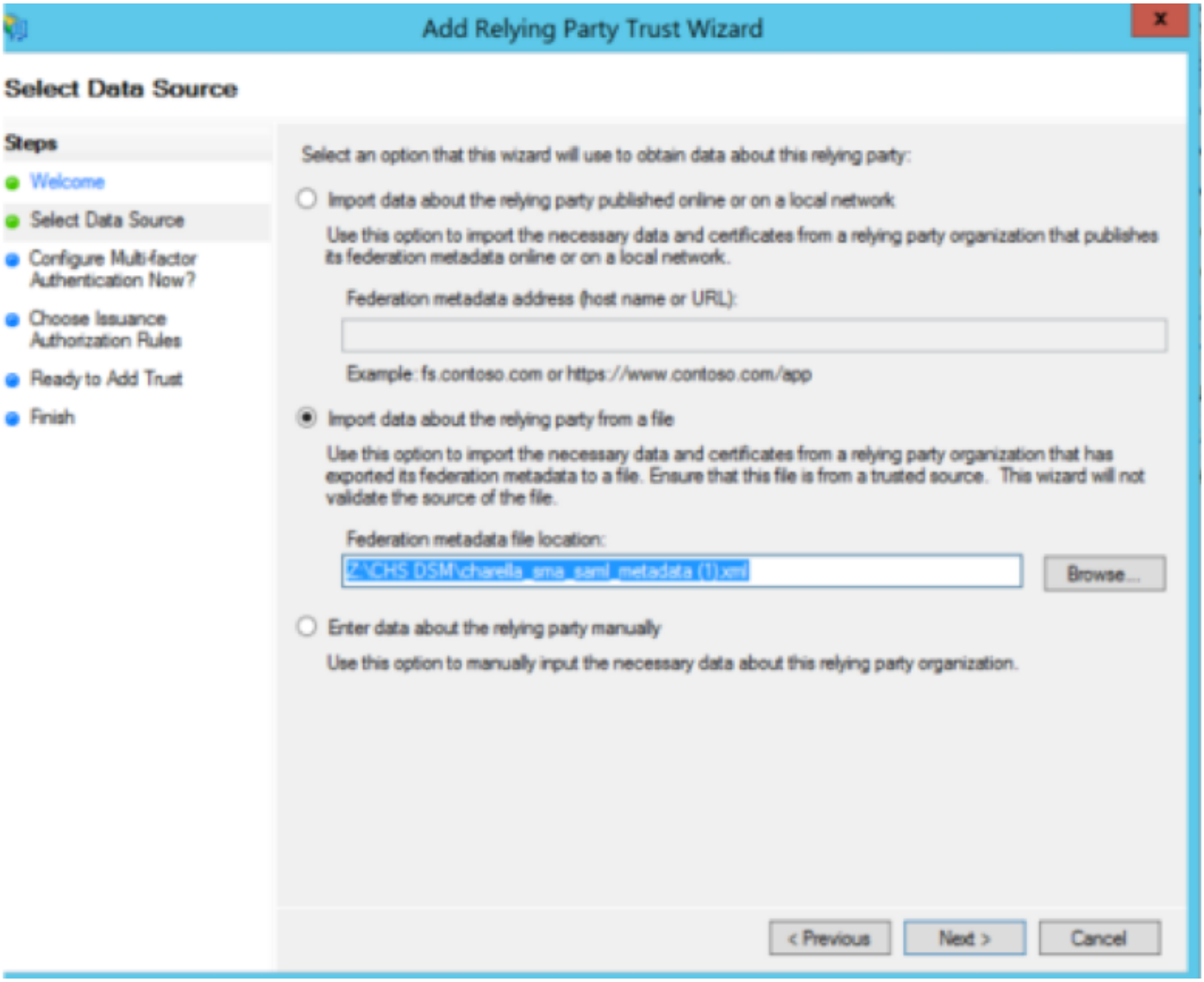


Stap 2. Het profiel van de Identity Provider wordt automatisch ingevuld wanneer de klant zijn ADFS-metagegevensbestand uploadt. Microsoft heeft een standaard-URL: **https://<ADFS-host>/FederationMetadata/2007-06/FederationMetadata.xml.**

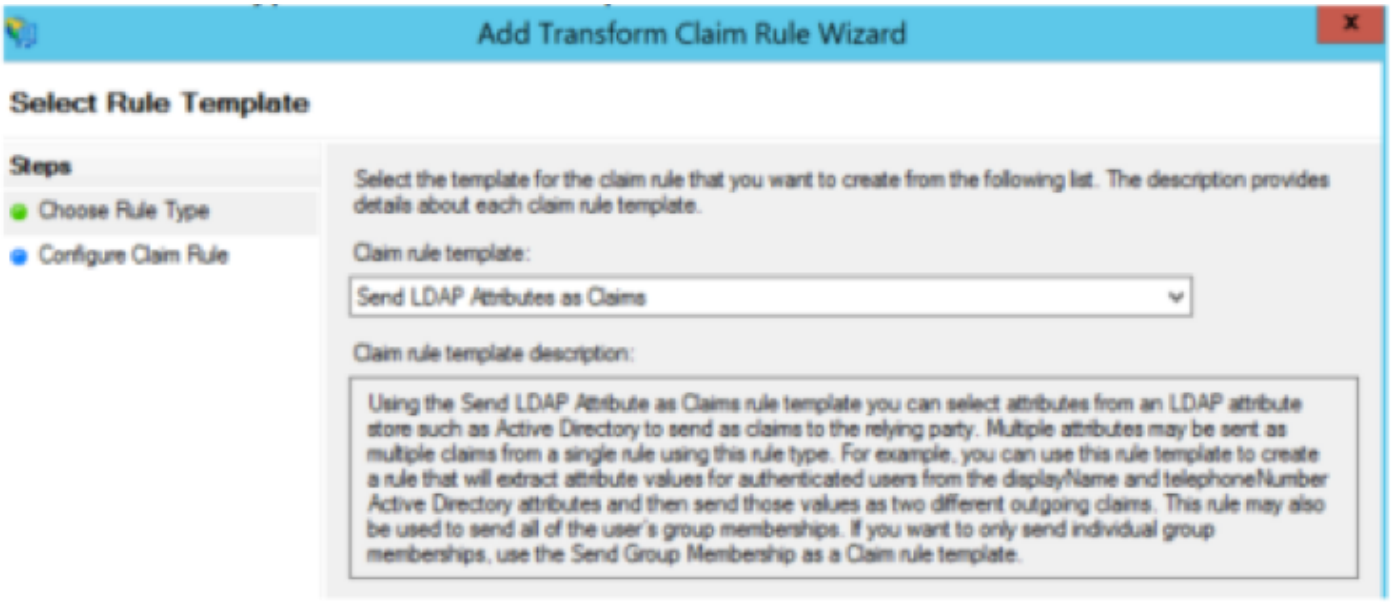
Stap 3. Zodra beide profielen zijn ingesteld, moet de metagegevens van het SP-profiel worden bewerkt, zoals per bug CSCvh30183.. Metagegevens-bestand ziet eruit zoals in de afbeelding.

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

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.



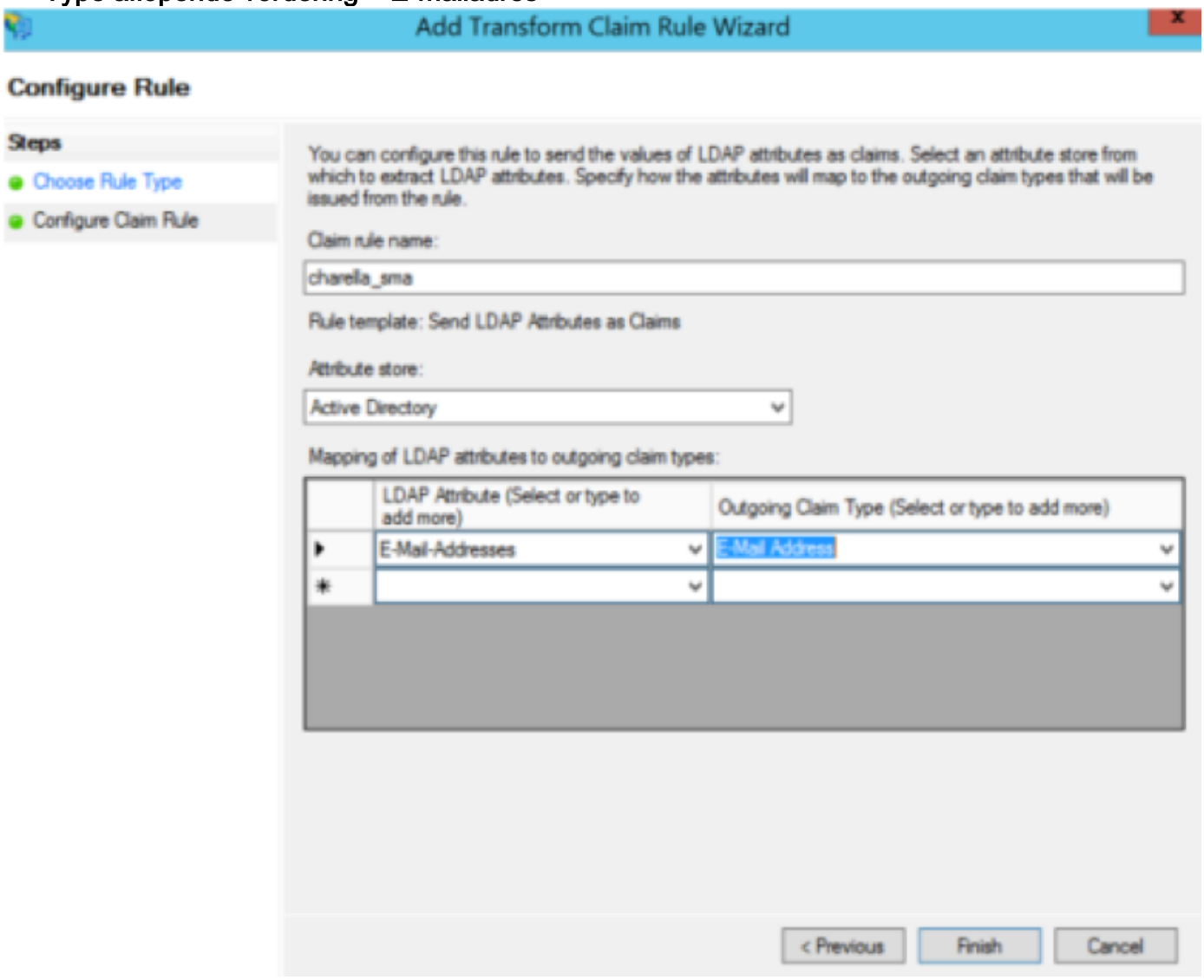
Stap 6. Nadat u met succes het metagegevensbestand hebt geïmporteerd, dient u de claimregels te configureren voor het nieuwe vertrouwen van de Relay Party, selecteert u de optie **Claim Rule sjabloon > Verzend LDAP-kenmerken**, zoals in de afbeelding weergegeven.



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.

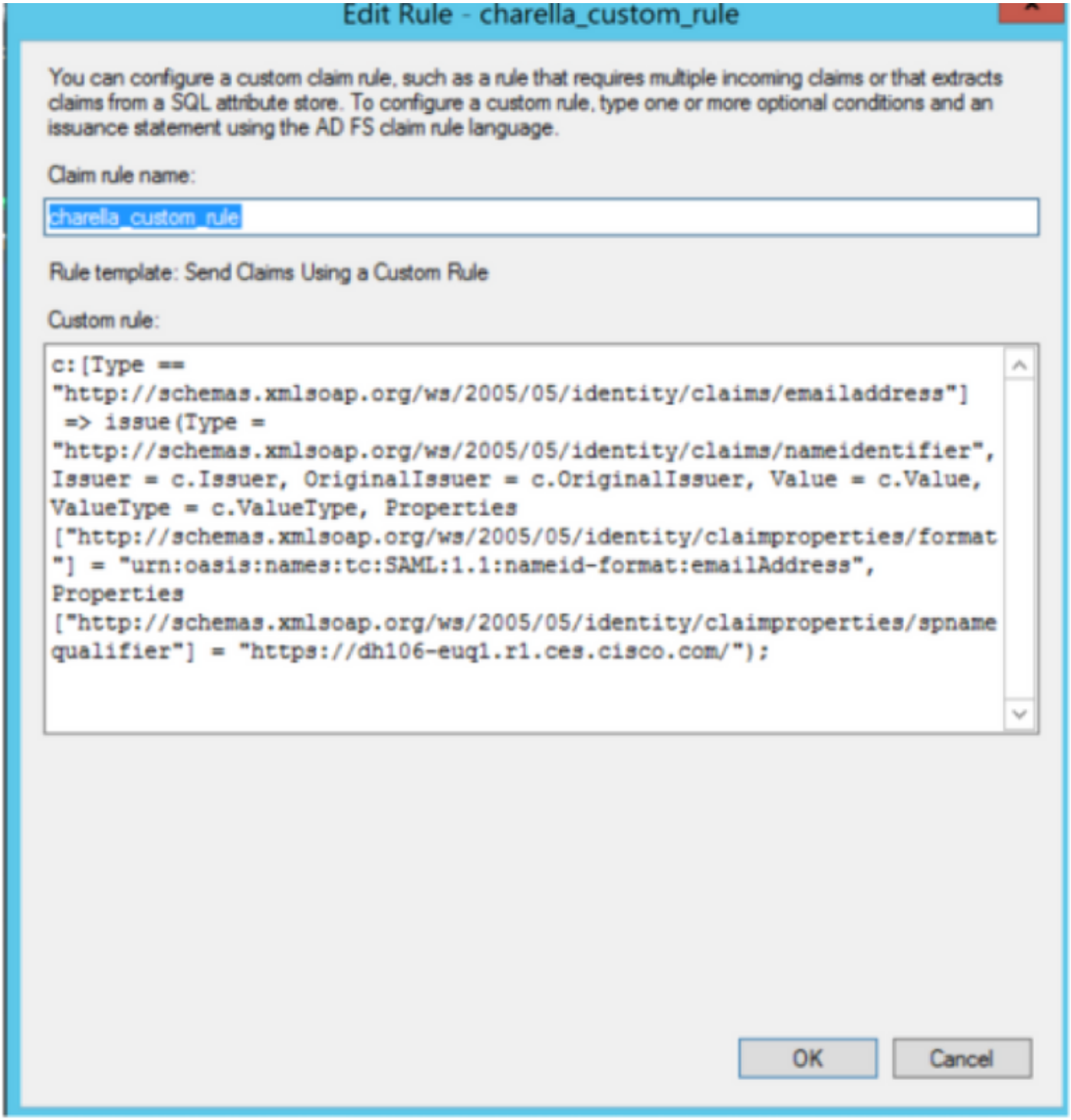
- **LDAP-kenmerk > E-mailadressen**
- **Type aflopende vordering > E-mailadres**



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

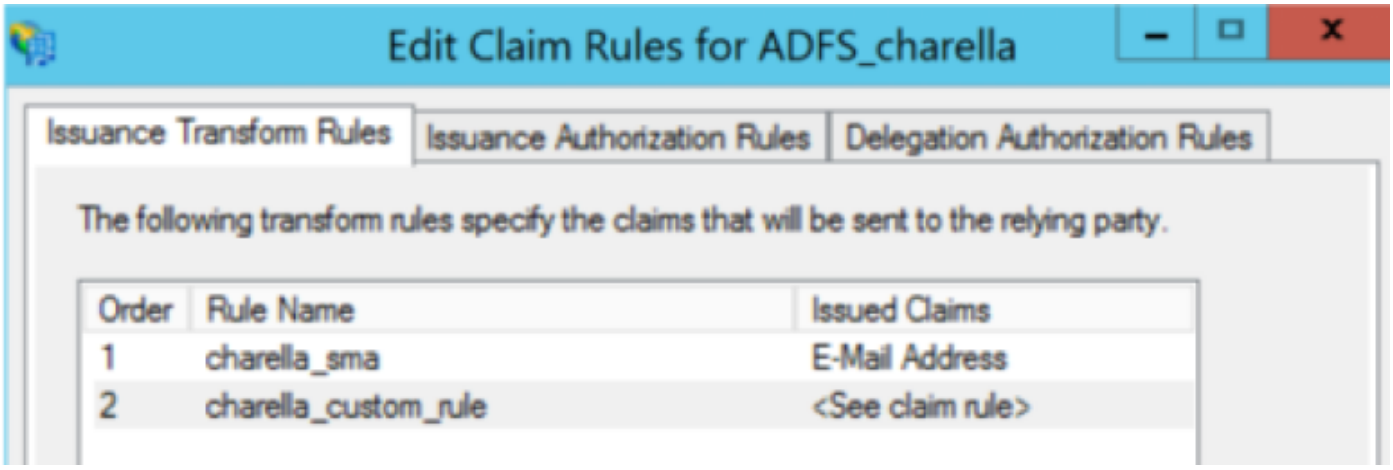
Dit is de aangepaste regel die aan de regel Eigen claim moet worden toegevoegd:

```
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");
```



- 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