Externe SAML SSO-verificatie configureren met AD FS voor ESA en SMA

Inhoud

Inleiding

In dit document wordt beschreven hoe u Active Directory Federation Services configureert als SAML-identiteitsprovider voor externe verificatie op Cisco ESA en SMA.

Voorwaarden

Dit document biedt een weergave van de toepassing van derden die technici anders niet kunnen zien.

- Configuratiestappen voor externe verificatie van Security Assertion Markup Language (SAML) met Active Directory Federation Services (AD FS) 2012 en 2016 voor de nieuwste versies van Cisco Email Security Appliance (ESA) en Security Management Appliance (SMA).
- Basisstappen in het laboratorium die geen gespecialiseerde implementatiespecifieke configuraties bevatten.
- Een werkend voorbeeld uit een labo-omgeving die kan verschillen van een productie-implementatie.

⚠ Let op: vul de configuratie van de serviceprovider (SP) in vóór deze procedure. Zie.

Vereisten

- Microsoft Active Directory Federation Services (AD FS) 2012 of 2016
- Cisco Email Security Appliance (ESA) en Security Management Appliance (SMA) laatste versie.

Gebruikte componenten

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 live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

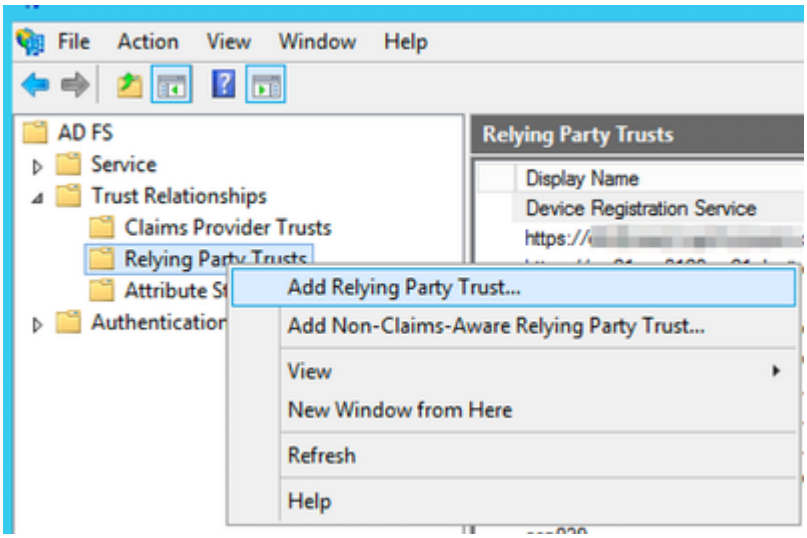
Stappen voor ADFS IDP-configuratie voor SAML

Het vertrouwen van de vertrouwende partij configureren

Gebruik een van de twee opties om het vertrouwen van de afhankelijke partij in AD FS te creëren.

Methode A: De vertrouwensrelatie van de afhankelijke partij maken door SP-metagegevens te importeren

1. Open de AD FS-beheerconsole vanuit Administratieve hulpmiddelen.
2. Vouw in de AD FS-beheerconsole Vertrouwde relaties uit, klik met de rechtermuisknop op Vertrouwen van vertrouwende partijen en selecteer vervolgens Vertrouwen van vertrouwende partijen toevoegen.



Vertrouwen van vertrouwende partij toevoegen

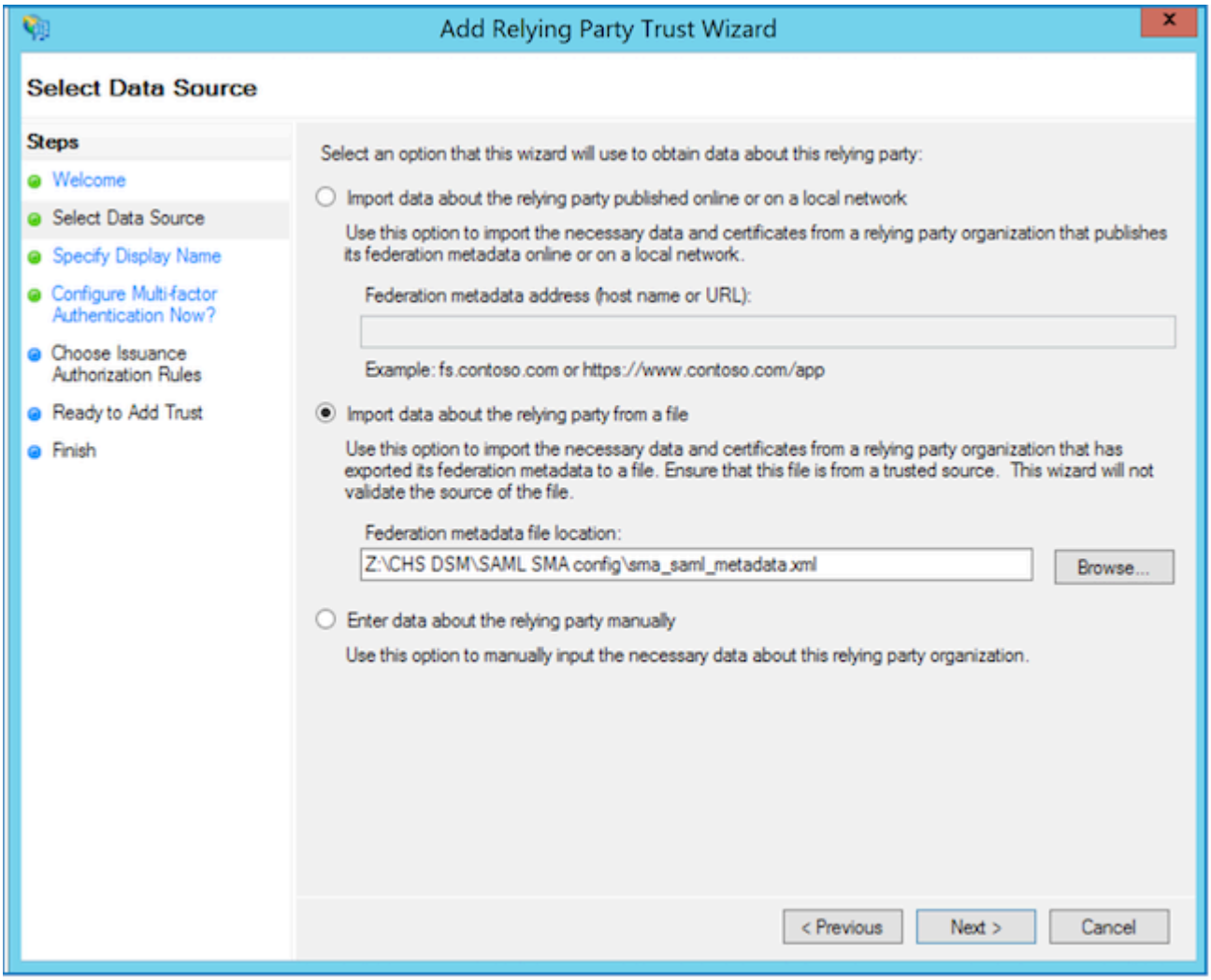
Tip: Microsoft vertrouwt op derden

Ga verder met een van de twee opties:

- Optie A: Gegevens over de vertrouwende partij importeren uit een bestand. Upload het bestand metadata.xml van de ESA- of SMA-serviceprovider (SP).
- Optie B: Voer handmatig gegevens in over de vertrouwende partij. Deze optie leidt u door de handmatige configuratie.

Optie A: Gegevens over de vertrouwende partij importeren uit een bestand. Upload het bestand ESA of SMA service provider (SP) metadata.xml.

1. Selecteer de optie om gegevens over de vertrouwende partij uit een bestand te importeren en selecteer Volgende.



Het ESA/SMA-metagegevensbestand importeren

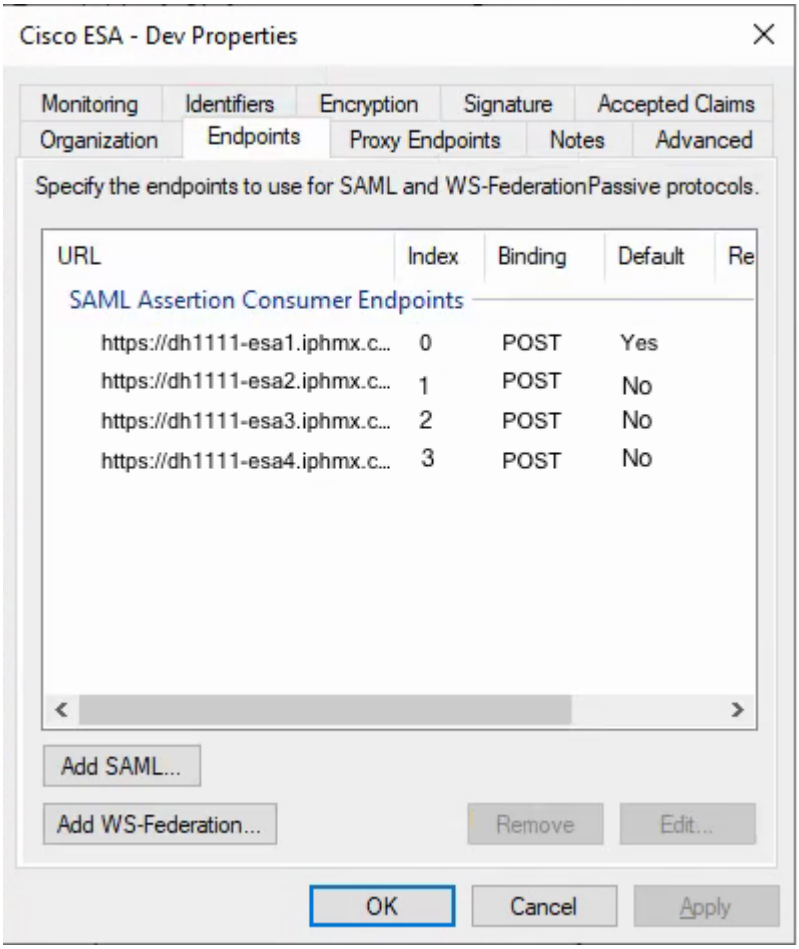
- Geef een naam voor de weergave op om het vertrouwen van deze vertrouwenspersoon te identificeren en selecteer vervolgens tweemaal Volgende.
- Selecteer voor autorisatieregels voor uitgifte de optie Alle gebruikers toestaan en selecteer Volgende.
- Accepteer op de pagina Ready to Add Trust de standaard instellingen en selecteer vervolgens Next.
- Selecteer Voltooien. Hiermee wordt het dialoogvenster Claimregels bewerken geopend voor het vertrouwen van de vertrouwende partij, dat wordt behandeld in Transformatieregels voor uitgifte - Claims.

Vertrouwenseigenschappen van vertrouwende partijen - Eindpunten

Voer deze stap alleen uit als er meerdere ESA's aanwezig zijn in een cluster.

1. Open Trusteigenschappen van vertrouwende partij > Eindpunten.
2. Voeg elk ESA-bereikbaar URL-adres toe en selecteer vervolgens OK.
3. De indexwaarden tellen vanaf 0, dat wil zeggen 0, 1, 2 en 3.

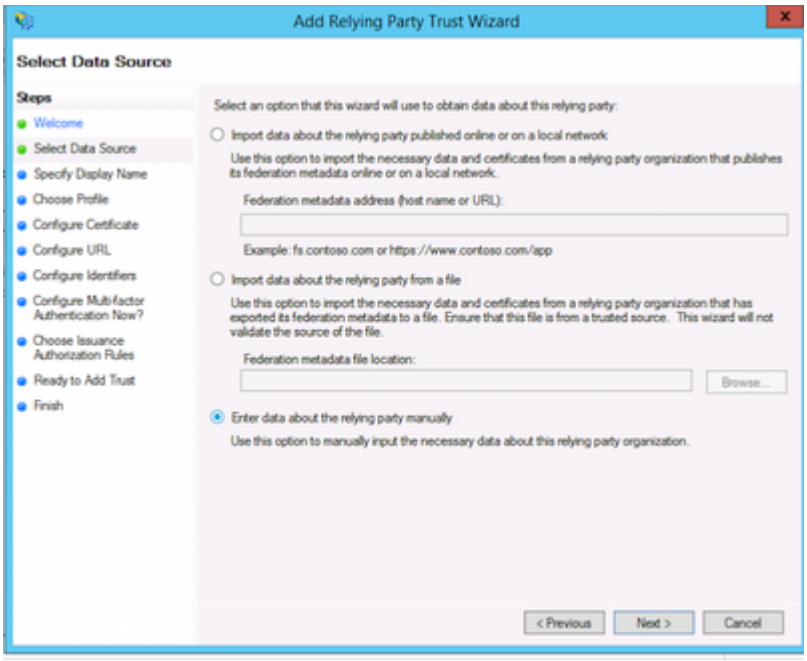
4. Stel slechts één item in op Standaard = Ja.
5. Stel de resterende items in op Standaard = Nee.



Vertrouwenseigenschappen van vertrouwende partijen - Eindpunten

Optie B: Voer handmatig gegevens in over de vertrouwende partij. Deze optie leidt u door de handmatige configuratie.

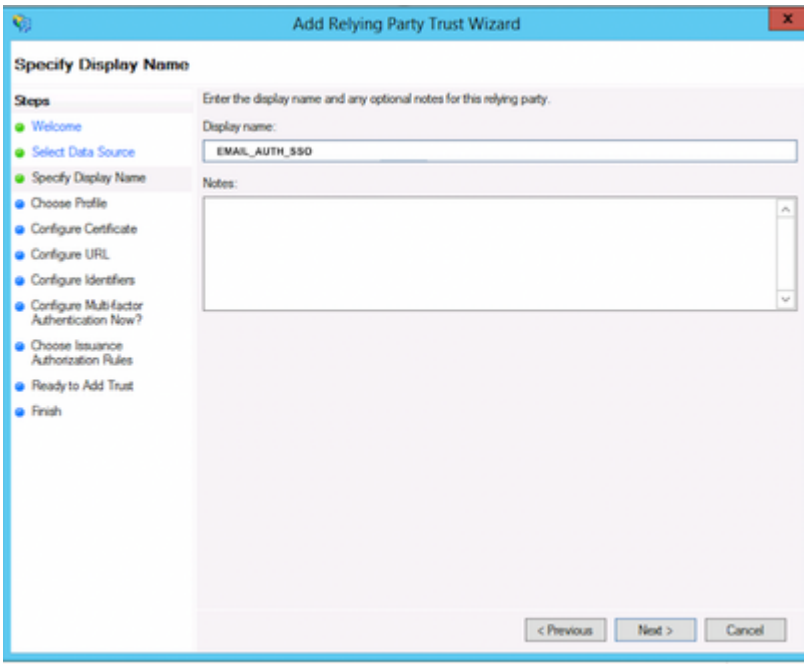
1. Selecteer Gegevens over de vertrouwende partij handmatig invoeren.



Betrouwbare partij handmatig toevoegen

Tip: Display Name is de naam die u kiest om de vertrouwenspersoon voor ESA of SMA SAML te identificeren.

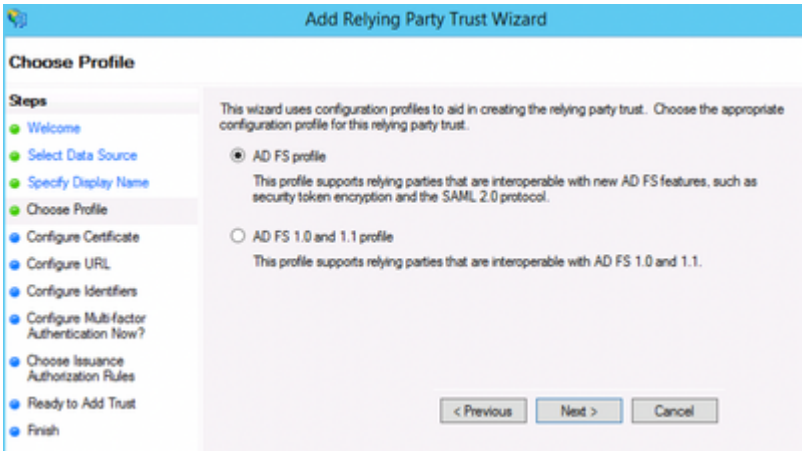
1. Voer een weergavenaam in voor de serviceprovider, bijvoorbeeld ESA_SP.



Een naam maken voor het profiel van de serviceprovider

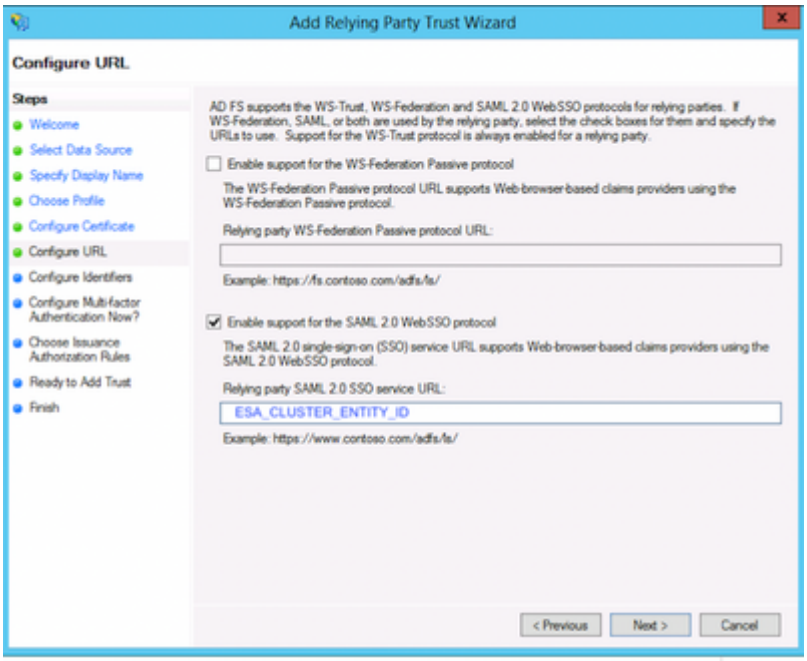
Tip: De rol van claimregels en uitgiftetransformatieregels

1. Kies de profieloptie AD FS-profiel.



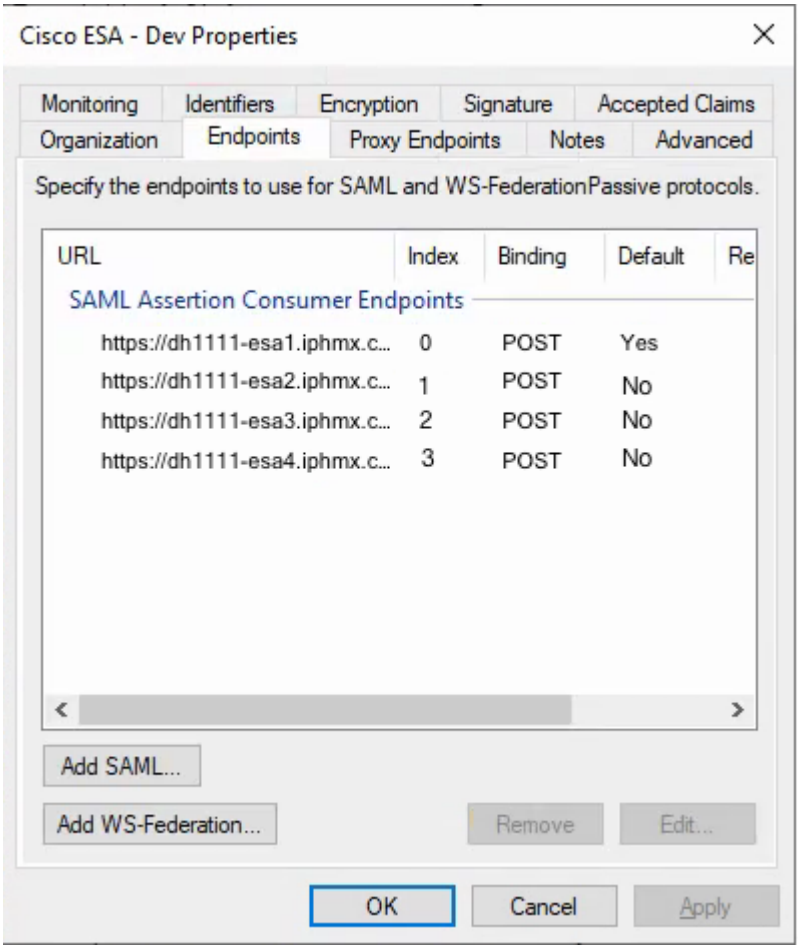
AD FS Profile Option om SAML 2.0 te gebruiken

1. Laad het openbare certificaat vanuit de configuratie van de ESA-serviceprovider (SP).
2. Kies Ondersteuning inschakelen voor de SAML 2.0 single-sign-on (SSO).
3. Voer de SAML 2.0 SSO-service-URL van de vertrouwende partij in met de waarde voor de Entiteit-ID van het SP-profiel.



Regels voor machtigingen voor afgifte - alle gebruikers toestaan

1. Kies Alle gebruikers toegang verlenen tot deze vertrouwende partij voor de regels voor de autorisatie van de uitgifte.



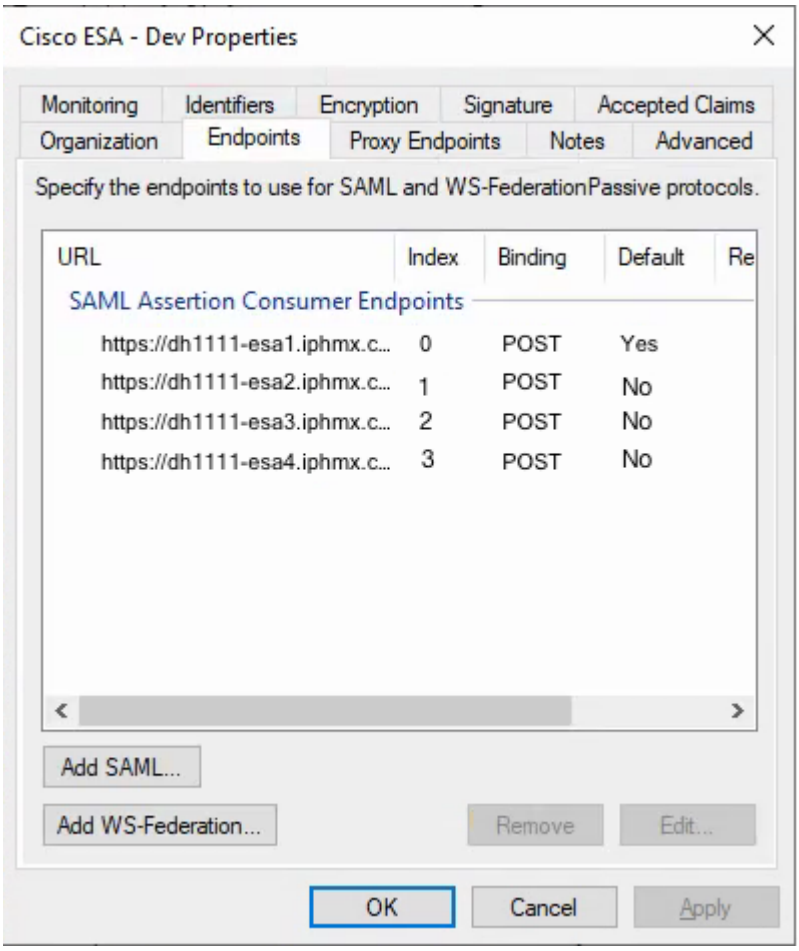
Kies regels voor autorisatie voor uitgifte

1. Selecteer Volgende om naar de pagina Voltooien te gaan.

Eindpunten voor vertrouwen van derden configureren (alleen clusters)

Voer deze stap alleen uit als er meerdere ESA's aanwezig zijn in een cluster.

1. Open Trusteigenschappen van vertrouwende partij > Eindpunten.
2. Voeg elk ESA-bereikbaar URL-adres toe en klik vervolgens op OK.
3. Stel waarden voor de eindpuntindex in vanaf 0 (bijvoorbeeld 0, 1, 2, 3).
4. Stel slechts één eindpunt in op Standaard = Ja. De resterende eindpunten instellen op Standaard = Nee

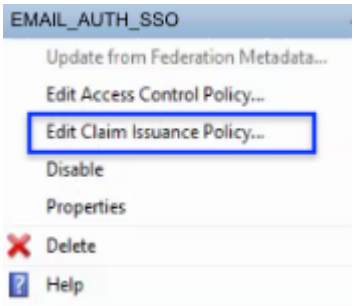


Regels voor machtigingen voor afgifte - alle gebruikers toestaan

- Met de stap Voltooien wordt het dialoogvenster Claimregels bewerken gestart voor het vertrouwen van de vertrouwenspersoon, dat wordt behandeld in Transformatieregels voor uitgifte.

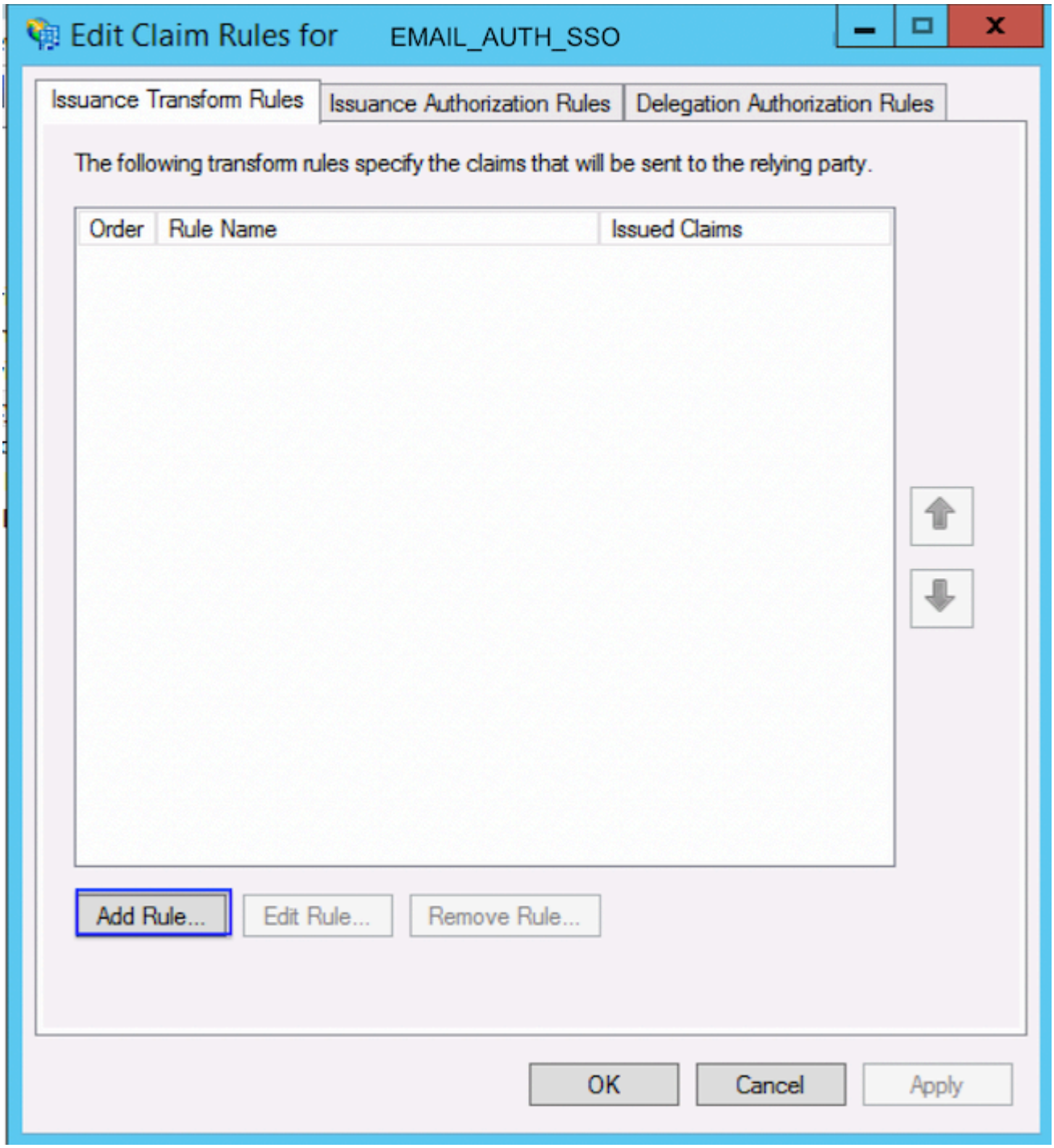
Transformatieregels voor uitgifte - Vorderingen

- Selecteer Uitgiftebeleid voor claims bewerken.



Uitgiftebeleid voor claims bewerken

- Selecteer Regel toevoegen.

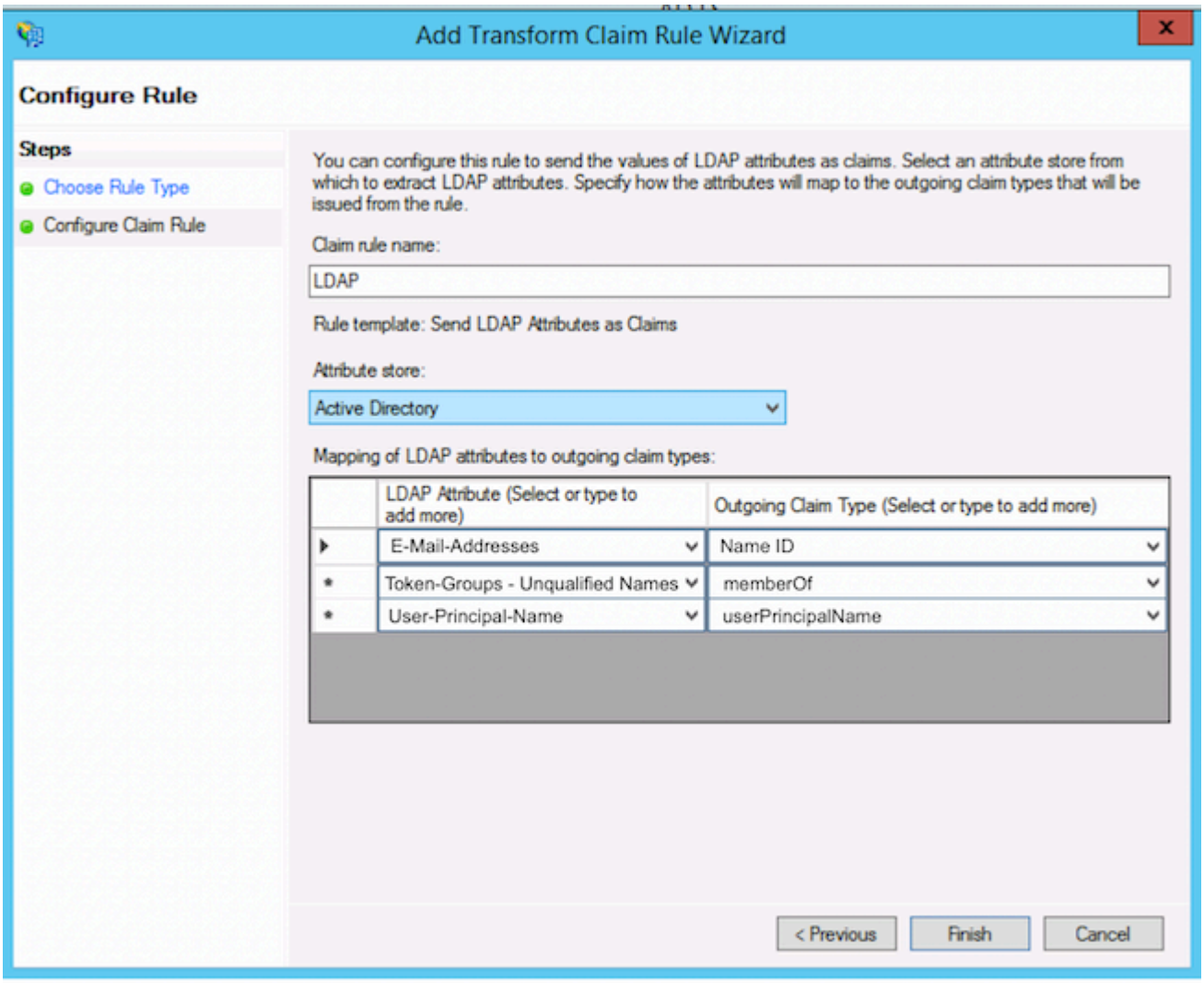


Transformatieregel voor uitgifte toevoegen

De waarden die hier worden weergegeven, zijn gemeenschappelijke waarden waarmee ESA groepsnamen kan invullen in de externe verificatie-instellingen.

Tip: De waarden in de toewijzing kunnen variëren op basis van de beheerdersvoorkeur.

Tip: Voer in het weergegeven voorbeeld de uitgaande claimtypen MemberOf en UserPrincipalName handmatig in. Selecteer Naam ID in de vervolgkeuzelijst.



Claimregel transformeren

- Selecteer Voltooien.

IdP-metagegevens downloaden en uploaden naar ESA

Nadat u de configuratie van de vertrouwens- en claimregel hebt voltooid, exporteert u de metagegevens van de identiteitsprovider (IdP) en uploadt u deze naar ESA.

⚠ Let op: als u de AD FS-service opnieuw opstart, kunnen actieve verificatiesessies worden onderbroken. Voer deze stap uit tijdens een onderhoudsvenster indien nodig.

- Start de AD FS-service indien nodig opnieuw.
- Voer de volgende opdrachten uit:

```
net stop adfssrv
net start adfssrv
```

- Download het metagegevensbestand vanaf deze URL:

https://myserver.domain.com/FederationMetadata/2007-06/FederationMetadata.xml

- Voltooi en keer terug naar het ESA-cluster.

Verifiëren

1. Bevestig in ESA of SMA dat het importeren van IdP-metagegevens met succes is voltooid.
2. Test een administratieve aanmelding met behulp van SAML single sign-on (SSO).
3. Controleer of de verwachte groepsclaims zijn ontvangen en of roltoewijzing wordt ingevuld zoals verwacht in de externe verificatieconfiguratie.

Gerelateerde informatie

-

- Cisco e-mail security applicatie – eindgebruikershandleiding
- Cisco Content Security Management Appliance - Handleidingen voor eindgebruikers

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.