Paraplu configureren met ADFS versie 3.0 met SAML

Inhoud

Inleiding

In dit document wordt beschreven hoe u SAML kunt configureren tussen Cisco Umbrella en Active Directory Federation Services (ADFS) versie 3.0.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

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.

Overzicht

In dit artikel wordt uitgelegd hoe u SAML kunt configureren tussen Cisco Umbrella en Active Directory Federation Services (ADFS) versie 3.0. Het configureren van SAML met ADFS verschilt van de andere SAML-integraties van Umbrella, omdat het geen één- of tweeklikproces in de wizard is, maar wijzigingen in ADFS vereist om correct te werken.

Dit artikel bevat gedetailleerde wijzigingen die u moet aanbrengen om SAML en ADFS samen te laten werken. De primaire stappen zijn om eerst de codering tussen uw ADFS-omgeving en Cisco Umbrella uit te schakelen en vervolgens enkele aangepaste claimregels voor uitgiftetransformatie toe te voegen aan de instelling van de umbrella-relaying-partij.

Voer deze stappen alleen uit met een bestaande, werkende ADFS-configuratie. Cisco Umbrella Support kan geen hulp of ondersteuning bieden bij het configureren van ADFS in een bepaalde omgeving.

Alleen ADFS versie 3.0 wordt op dit moment ondersteund (Windows Server 2012 R2) volgens deze instructies. Het is mogelijk dat eerdere (2.0 of 2.1) of latere (4.0) versies van ADFS kunnen werken met de Umbrella SAML-integratie, maar dit is niet getest of bewezen. Als u een andere versie van ADFS hebt en geïnteresseerd bent in samenwerking met onze Support- en Productteams om te integreren, neem dan contact op met Cisco Umbrella Support.

U kunt de vereisten voor de eerste SAML-configuratie vinden in de overkoepelende documentatie: Identiteits-integraties: vereisten. Nadat u deze stappen hebt voltooid, kunt u doorgaan met het gebruik van de ADFS-specifieke instructies in dit artikel om de configuratie te voltooien.

De stappen in de Umbrella documentatie vermelden dat u uw SAML (ADFS) metadata moet uploaden naar Umbrella. U kunt toegang krijgen tot uw metagegevens door naar deze URL te navigeren en vervolgens het XML-bestand te uploaden.

```
https://{your-ADFS-domain-name}/federationmetadata/2007-06/federationmetadata.xml
```

Codering uitschakelen

1. AD FS-beheer openen. Breid vertrouwensrelaties uit en selecteer Vertrouwende partijen.

2. Klik met de rechtermuisknop op de vertrouwende partij voor de paraplu (of hoe u deze ook hebt genoemd) en selecteer Eigenschappen.

3. Selecteer het tabblad Codering.

4. Selecteer Verwijderen om het certificaat voor versleuteling te verwijderen.

5. Selecteer OK om het scherm te sluiten.

Nieuwe claimregels voor uitgiftetransformatie toevoegen

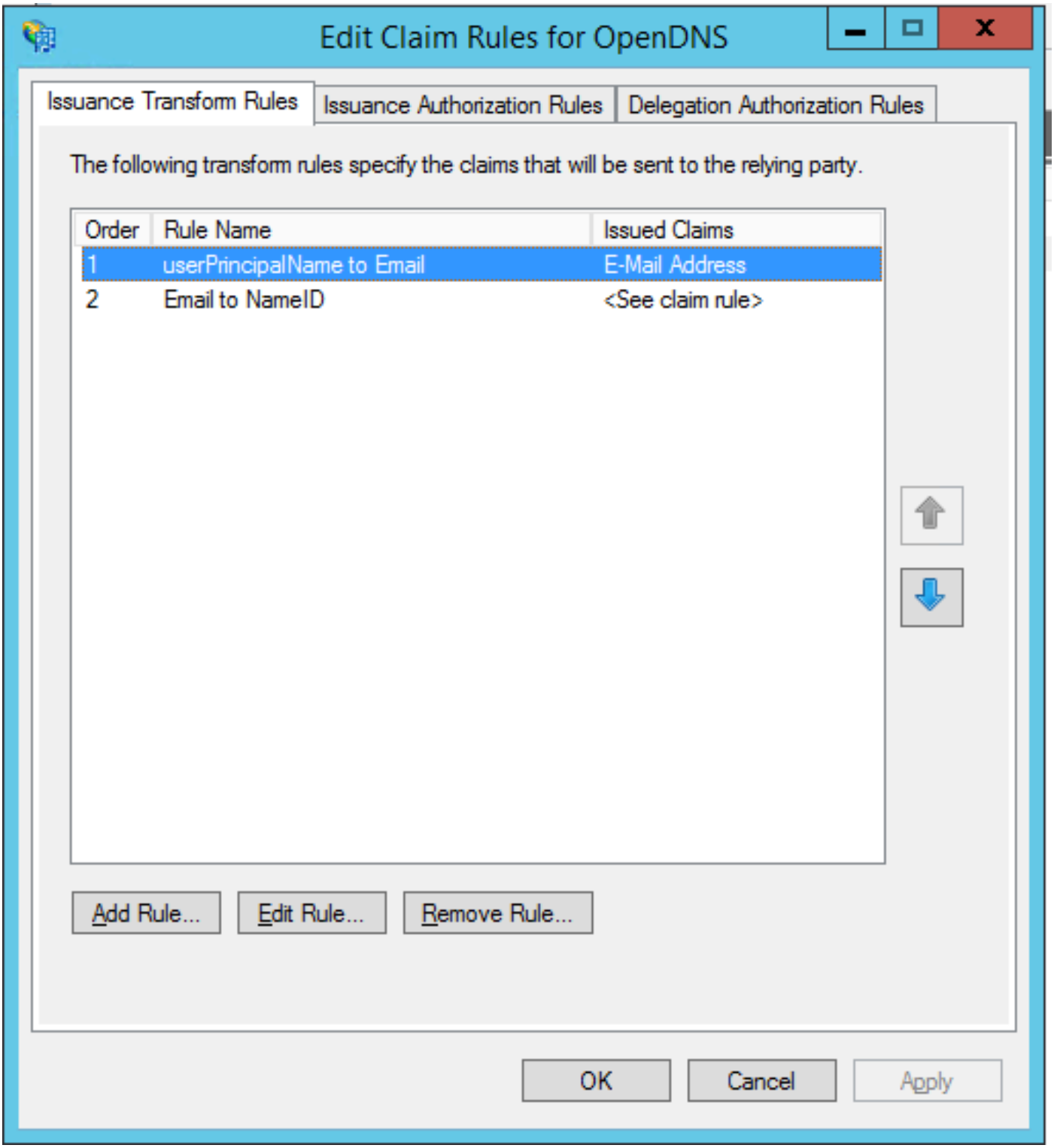
1. AD FS-beheer openen. Breid vertrouwensrelaties uit en selecteer Relaying Party Trusts.

2. Klik met de rechtermuisknop op de partij die de paraplu doorgeeft (of hoe u deze ook hebt genoemd) en selecteer Claimregels bewerken.

3. Selecteer onder Transformatieregels voor uitgifte de optie Regel toevoegen.

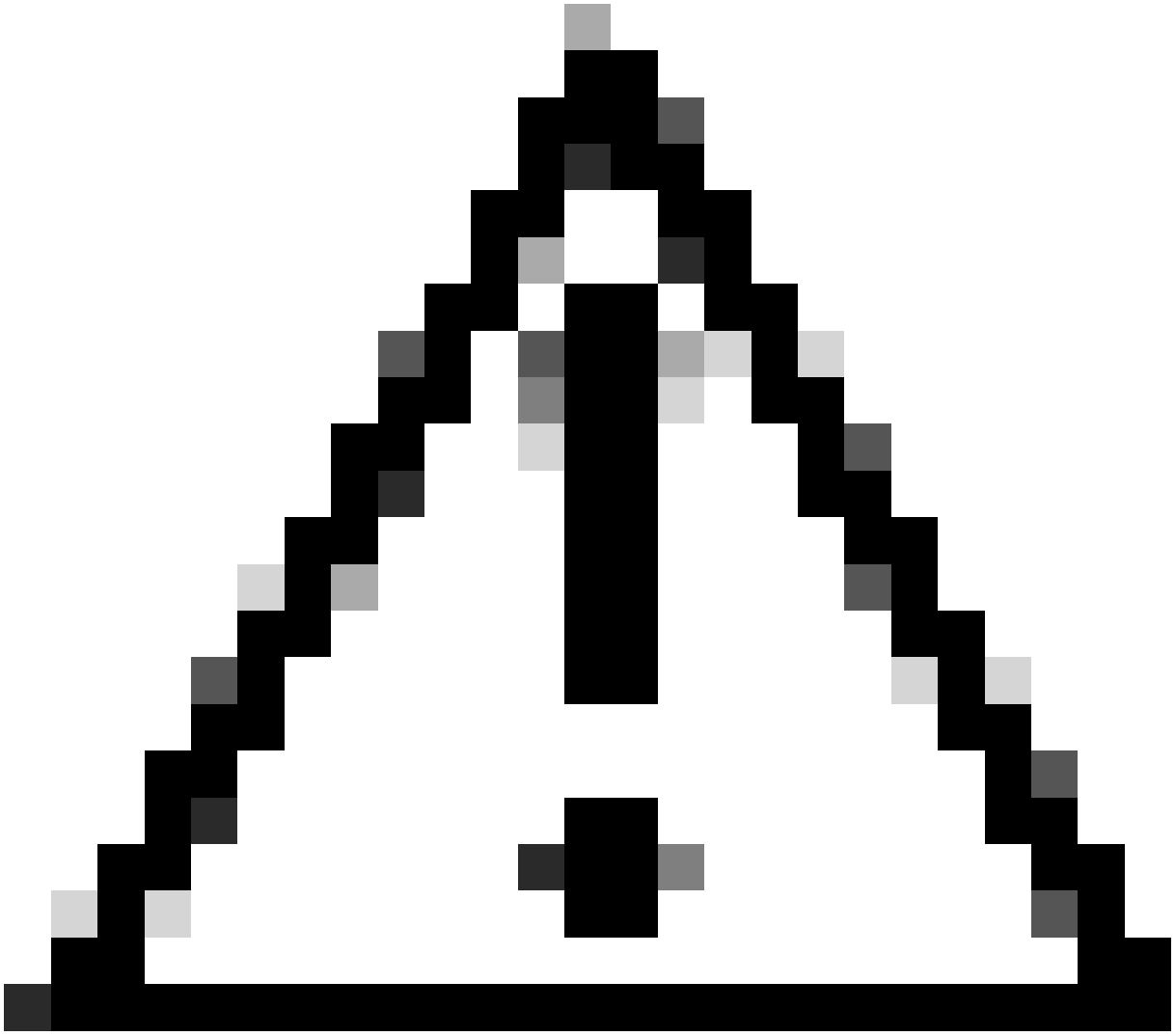
4. Selecteer Claims verzenden met behulp van een aangepaste regel.

Zie deze screenshot voor de lijst met regels die u kunt toevoegen.



Zodra u elk van deze regels toevoegt, kan de integratie beginnen te werken.

Regels transformeren



Let op: deze regels zijn getest en werken in de ADFS-laboratoriumomgeving van Umbrella en in een paar productieomgevingen van klanten. Pas ze aan uw omgeving aan.

---

userPrincipalName naar e-mailadres

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/em
```

E-mail naar NameID

```
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");
```

Bijlage: Inloggen met 'mail' Attribuut

Standaard verifieert ADFS gebruikers aan de hand van hun UPN (User Principal Name). Als het e-mailadres van uw gebruiker (naam van uw Umbrella-account) niet overeenkomt met hun UPN, zijn aanvullende stappen vereist. Zie dit artikel in de Knowledge Base: Hoe configureer ik AD FS in het Cisco Umbrella Dashboard om aanmeldingen met een e-mailadres toe te staan?

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.