

SAML-verificatie configureren voor SWG met ADFS en UPN

Inhoud

[Inleiding](#)

[Vereiste voor SAML-verificatie](#)

[Configuratiestappen in ADFS](#)

[UPN versus e-mailadres](#)

Inleiding

In dit document wordt beschreven hoe u SAML-verificatie configureert voor Secure Web Gateway (SWG) met Active Directory Federated Services (ADFS).

Vereiste voor SAML-verificatie

Umbrella SAML-verificatie vereist dat het SAML-antwoord de PrincipalName van de eindgebruiker (bijvoorbeeld [user@domain.local](#)) bevat als de claim Name ID. Deze verplichting geldt voor alle aanbieders van identiteitsbewijzen. Sommige, zoals ADFS, vereisen handmatige configuratie om dit kenmerk op te nemen.

Configuratiestappen in ADFS

1. Selecteer in ADFS de optie Relying Party Trusts gemaakt voor Umbrella onder ADFS > Relying Party Trusts.
2. Klik op Uitgiftebeleid voor claims bewerken.
3. Voeg een nieuwe regel toe met behulp van de claim templateLDAP Attribuut verzenden als claims.
4. Configureer de regel om het LDAP-attribut userPrincipalName toe te wijzen aan de uitgaande SAML-claim type Name ID.

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:

UPN to Name ID

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)
▶	User-Principal-Name	Name ID
*		

View Rule Language...

OK

Cancel

Screenshot_2021-10-20_at_12.33.50.png

5. Sla de configuratie op.

UPN versus e-mailadres

Het UPN van een gebruiker (bijvoorbeeld [user@domain.local](#)) komt vaak overeen met het e-mailadres van de gebruiker. In sommige omgevingen verschilt het e-mailadres (bijvoorbeeld [user@externaldomain.tld](#)) van het UPN.

- Umbrella vereist dat de Identity Provider de Name IDclaim met de UPN-waarde verzendt.

- Dit moet overeenkomen met de gebruikersnaam die is opgegeven in Implementaties > Gebruikers en groepen in paraplu.
- Overkoepelende hulpprogramma's voor gebruikersprovisioning (zoals de AD-connector) identificeren gebruikers aan de hand van hun UPN.

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.