

# Cloud-webbeveiliging: Configuratie van gebruiker/groepseigenschappen met PingFederate en ADFS terwijl u SAML gebruikt.

## Inhoud

[Inleiding](#)

[Vereisten](#)

[Configuratie](#)

[PingFed](#)

[ADFS](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde Cisco Support Community-discussies](#)

## Inleiding

Dit document beschrijft hoe u PingFederate en ADFS (Active Directory Federated Services) IDP-servers kunt configureren om gebruiker/groep-details te verzenden naar de Cloud Web Security Service om beleid met een filter in detail te kunnen filteren.

## Vereisten

Cisco raadt u aan een basisbegrip van het volgende te hebben.

- Administratieve inlognaam/toegang tot de PingFed/ADFS-server
- Kennis van het navigeren met de PingFed/ADFS-server
- Om te kunnen werken aan HTTPS-verkeer, moet voor al het verkeer een HTTPS-inspectie worden uitgevoerd

## Configuratie

Volg onderstaande stappen om gebruiker/groepskenmerken te configureren met PingFederate en ADFS.

### PingFed

Onder **Kenmerken > Bron: User lookup** tabblad:

- Contract van kenmerken **GEAUTHENTICEERDE\_GROEPEN**  
Bron:LDAP

Value: lid van

- Contract van kenmerken **SAML\_SUBJECT**

Bron: **LDAP**

Value: **AMAaccountNaam**

## **ADFS**

Onder **vertrouwensrelaties** > tabblad **Relying party trusts**:

- contract met LEAP-kenmerken: **SAM-accountnaam**  
Aflopende vordering Type LDAP: **Naam ID**
- contract met LEAP-kenmerken: **Token-groepen**  
Aflopende vordering Type LDAP: **Groep**

## **Verifiëren**

## **Problemen oplossen**

Er is geen sectie voor probleemoplossing voor dit document.