

# ZTNA-inschrijvingsfouten voor gastgebruikers met persoonlijke Google-accounts in Cisco Secure Access

## Inhoud

---

---

## uitgeven

Tijdens de implementatie van Private Access met ZTNA (Zero Trust Network Access) mislukt de inschrijving van een gastgebruiker met een persoonlijk Google-account na succesvolle registratie in Entra ID en provisioning in Secure Access. De specifieke symptomen zijn onder meer:

- Client-based enrollment: Het inschrijvingsproces bereikt SSO-authenticatie, referenties worden verstrekt, maar ZTNA geeft een "I / O-fout" weer en het inschrijvingsproces raakt vast
- Clientloze toegang: Geeft de foutmelding "Cisco Secure Access Login failure" terug. Controleer IDP-configuratie" samen met een transactie-ID

Deze fouten voorkomen toegang tot privébronnen en hebben gevolgen voor het testen van de ZTNA-functionaliteit voor toegang in de stijl van een aannemer met behulp van niet-bedrijfsidentiteiten.

## milieu

- Cisco Secure Access met ZTNA-implementatie
- Microsoft Entra ID (voorheen Azure AD) als Identity Provider
- Persoonlijk Google-account (@gmail.com) geregistreerd als gastgebruiker in Entra ID
- Gastaccount beschikbaar gesteld en zichtbaar in Beveiligde toegang
- SAML-verificatie geconfigureerd tussen Entra ID en Cisco Secure Access

## resolutie

De inschrijvingsfout werd opgelost door de toewijzingsconfiguratie van het SAML-attribuut in Microsoft Entra ID aan te passen. De volgende stappen werden genomen om het probleem aan te pakken:

### Stap 1: DART-bundel en klantgedrag analyseren

Controleer de DART-bundel om te bevestigen dat de componenten Cisco Secure Client en ZTA normaal werken. Bij de analyse moet worden geverifieerd of de inschrijvingsstroom Cisco Secure Access heeft bereikt en of de fout optreedt tijdens de SAML-verificatie bij de Identity Provider.

### Stap 2: Entra ID-verificatielogs onderzoeken

Controleer de verificatielogboeken van de Entra ID om te bevestigen dat het verificatieproces succesvol is voltooid vanuit het perspectief van de Identity Provider. De logs moeten een succesvolle verificatie weergeven, maar Secure Access weigert de aanmelding vanwege een verkeerde attribuutovereenkomst.

### Stap 3: Probleem met toewijzen van SAML-kenmerken identificeren

Bepaal dat Entra ID de UPN (hoofdgebruikersnaam) uitgeeft als de SAML-claim, die niet overeenkomt met de persoonlijke Gmail-accountidentiteit die wordt verwacht door Secure Access. Het opgegeven IdP-kenmerk komt niet overeen met de verwachte gebruikersidentificatie.

### Stap 4: Toewijzing van SAML-kenmerken wijzigen

Wijzig de toewijzing van SAML-kenmerken in Microsoft Entra ID van UPN naar e-mailadres. Dit zorgt ervoor dat het e-mailadres claim overeenkomt met de persoonlijke Google-account identiteit.

### Stap 5: Controleer het succes van de inschrijving

Na het implementeren van de attribuut mapping wijziging, probeer het opnieuw ZTNA inschrijvingsproces. Cisco Secure Access ZTA moet nu het Gmail-adres herkennen en de inschrijving met succes voltooien.

## Oorzaak

De inschrijvingsfout is veroorzaakt door een mismatch tussen het SAML-kenmerk dat wordt bevestigd door Microsoft Entra ID en de verwachte gebruikersidentificatie in Cisco Secure Access. Entra ID is geconfigureerd om de UPN (User Principal Name) te verzenden als de SAML-claim, maar voor persoonlijke Google-accounts (@gmail.com) kwam dit UPN niet overeen met de daadwerkelijke identiteit van het e-mailadres. Cisco Secure Access zal naar verwachting het e-mailadres ontvangen als het identificatiekenmerk dat overeenkomt met de geleverde gastgebruikersaccount, wat resulteert in authenticatieafwijzing ondanks succesvolle IdP-verificatie.

## Verwante inhoud

- [Cisco Technical Support en downloads](#)

## 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.