# Problemen oplossen met synchronisatie van gebruikersidentiteit en groepsidentiteit in Cisco Secure Access met diff IDP

## Inhoud

## uitgifte

In dit document wordt beschreven hoe u de synchronisatie van gebruikers- en groepsidentiteiten in Cisco Secure Access kunt oplossen met verschillende Identity Providers (IdP's), zoals Okta, Microsoft Entra ID en IBM Cloud.

## milieu

- Cisco Secure Access — integratie van SCIM-provisioning
- Geldt voor SCIM 2.0 IdP-connector (Okta, Azure AD)

## resolutie

### Overzicht

Cisco Secure Access ondersteunt de provisioning van gebruikers- en groepsidentiteiten rechtstreeks vanuit Okta en Microsoft Entra ID (voorheen Azure AD) met behulp van de SCIM 2.0-standaard, waardoor de noodzaak om een on-premises Active Directory (AD) Connector te implementeren voor identiteitsbronnen die alleen in de cloud worden gebruikt, wordt weggenomen. Dit artikel consolideert de aannames over de architectuur, de gebruikelijke storingsmodi en de richtlijnen voor probleemoplossing die veldtechnici en beheerders het vaakst

tegenkomen wanneer ze deze integratie implementeren of onderhouden.

Dit document is onderverdeeld in vier delen:

- Configuratie — waar te gaan voor officiële setup-instructies
- Architectuuraannames die, indien geschonden, stille of moeilijk te diagnosticeren storingen veroorzaken
- Providerspecifieke problemen (Okta versus Entra ID)
- Algemene SCIM-protocolproblemen die van toepassing zijn ongeacht IdP

## Configuratie

Dit artikel richt zich op het oplossen van problemen, niet op de eerste installatie. Gebruik de officiële Cisco TechNotes in dit document voor stapsgewijze configuratie:

- Als u Cisco Secure Access wilt configureren met Microsoft Entra ID (Azure AD), raadpleegt u deze link: Gebruikers en groepen voorzien van beveiligde toegang via Entra ID
- Om Cisco Secure Access met Okta te configureren, raadpleegt u deze link: Gebruikers en groepen toegang bieden tot Secure Access via OKTA

Beide documenten hebben betrekking op het genereren van het SCIM-token en de provisioning-URL in Secure Access, het configureren van de bijbehorende toepassing in de IdP en het uitvoeren van de initiële provisioningsynchronisatie.

## Primer voor architectuur

Voordat u problemen oplost, moet u controleren of de implementatie overeenkomt met deze kernaannames. De meeste synchronisatiefouten komen terug op een van deze veronderstellingen.

Eén identiteitsbron tegelijk

Gelijktijdige provisioning van dezelfde gebruikers of groepen vanuit een on-premises AD Connector en een cloud-IdP (Okta of Entra ID) wordt niet ondersteund en leidt tot inconsistente handhaving van het beleid. Als u migreert van de AD Connector naar een cloud-IdP:

- Stop de on-premises AD Connector-service.
- Bevestig dat er geen resterende synchronisatietaken worden uitgevoerd voordat u cloud IdP-provisioning inschakelt.

Virtuele apparaten zijn een uitzondering

Entra ID of Okta kunnen geen identiteitsintegratie bieden voor virtuele apparaten (VA's), omdat de IdP geen zicht heeft op privé-IP-naar-gebruikerstoewijzingen, die VA's vereisen. VA-implementaties hebben nog steeds de on-premises AD Connector nodig, ongeacht wat voor andere componenten wordt gebruikt.

Toewijzen versus duwen

- Actie: gebruikers of groepen toewijzen aan de toepassing
    - Wat het feitelijk doet: Bepalingen voor de gebruikers van die groep om Secure Access
- Actie: Pushing a group (Okta)
    - Wat het eigenlijk doet: Bepalingen waartegen de groep zelf bezwaar maakt (voor beleidsgerichtheid). Het synchroniseert geen enkele gebruiker.

---

Opmerking: duw niet op een groep die ook is toegewezen aan de toepassing voor gebruikersprovisioning. Dit kan een dubbele of tegenstrijdige groepstoestand maken.

---

Groep- en gebruikerslimieten

Er is geen harde limiet voor het aantal gebruikers dat wordt aangeboden via IdP.

Groepen worden afgetopt. Historisch gezien was dit 200 groepen per organisatie van ofwel Okta of Entra ID; sommige huidige documentatie toont een hoger plafond (tot 1.000) voor Okta

specifiek. Behandel het exacte aantal als omgevingsafhankelijk en bevestig dit met het Cisco Technical Assistance Center (TAC) of de huidige Cisco-documentatie. Groepen buiten de limiet worden stilletjes niet voorzien en er wordt geen fout opgedoken.

Als je een bredere dekking nodig hebt, gebruik dan een dynamische "Alle gebruikers" (Entra ID) of "Iedereen" (Okta) groep in plaats van een poging om elke groep individueel te pushen.

SCIM-tokenlevenscyclus

In Cisco Secure Access worden tokens gegenereerd wanneer u Verbinden > Gebruikers, groepen en eindpuntapparaten > Configuratiebeheer > Directory integreren kiest. Het teken wordt slechts één keer getoond bij de schepping.

Wanneer u het token opnieuw genereert, wordt de provisioning aan de IdP-kant onmiddellijk onderbroken totdat het nieuwe token wordt ingevoerd in de provisioningconfiguratie van Microsoft Entra ID of Okta. Er is geen respijtperiode en de IdP-fout is vaak generiek (authenticatiefout) in plaats van een verlopen token-bericht.

Vernieuw het token periodiek voor veiligheidshygiëne en test de verbinding aan de IdP-kant onmiddellijk na rotatie.

## Okta-specifieke kwesties

- Symptoom: groepen worden niet weergegeven in Veilige toegang
    - Oorzaak hoofdzaak: het indrukken van een groep bepaalt alleen het groepsobject; het synchroniseert geen leden.
    - Resolutie: Zorg ervoor dat de relevante groepsleden afzonderlijk worden toegewezen aan de toepassing onder Opdrachten.
- Symptoom: gebruikers voorzien van voorzieningen, maar kenmerken ontbreken of zijn fout
    - Hoofdoorzaak: alleen beveiligde toegang komt op de weergavenaam en gebruikersnaam voor; de opgegeven en familienamen worden niet vermeld.
    - Resolutie: Bevestig dat de vereiste kenmerken expliciet zijn geselecteerd voor synchronisatie. Ga er niet van uit dat alle Okta-profielvelden zich voortplanten.

- Symptoom: stilzwijgend provisioning doet niets
    - Hoofdoorzaak: Gebruikers aanmaken, Gebruikersattributen bijwerken of Gebruikerskoppelingen uitschakelen is niet ingeschakeld.
    - Resolutie: Controleer of alle drie zijn gecontroleerd onder Provisioning > To App in de Okta-beheerdersconsole.
- Symptoom: objectGUID of aangepast kenmerk niet synchroniseren
    - Hoofdoorzaak: Attribuut wordt niet toegevoegd en toegewezen via Toewijzing gebruikersprofiel.
    - Resolutie: Voeg het objectGUID-kenmerk toe en maak de corresponderende profieltoewijzing als deze id vereist is.
- Symptoom: Synchronisatie gestopt na tokenrotatie
    - Hoofdoorzaak: SCIM of API-token geregenereerd in Secure Access, maar niet bijgewerkt in Okta.
    - Resolutie: Voer het nieuwe token in onder Provisioning > API-integratie configureren en voer opnieuw Test API Credentials uit.
- Symptoom: Kan niet bepalen waarom een specifieke gebruiker of groep heeft gefaald
    - Hoofdoorzaak: logboeken werden niet eerst gecontroleerd.
    - Resolutie: controleer Rapporten > Systeemlog in Okta, gefilterd in de Cisco User Management Connector-toepassing, voordat u escaleert.
- Symptoom: het aantal groepen overschrijdt de limiet, sommige ontbreken zonder fout
    - Hoofdoorzaak: organisatie heeft meer groepen bestreken dan Secure Access ondersteunt.
    - Resolutie: beperk het bereik tot alleen beleidsrelevante groepen of schakel Cisco TAC in voor ondersteuning van groepen op een hoger niveau.

## Microsoft Entra ID Specifieke problemen

- Symptoom: Dynamisch groepslidmaatschap wordt niet weergegeven in Secure Access
    - Hoofdoorzaak: de regel voor de dynamische groep is verkeerd geconfigureerd of de groep bevindt zich niet in het voorziene bereik.
    - Resolutie: Valideer de regel voor dynamisch lidmaatschap rechtstreeks in Entra ID

voordat u een fout in de synchronisatie van Secure Access aanneemt.

- Symptoom: SAML SSO zal naar verwachting SWG-identiteit aansturen
    - Hoofdoorzaak: AnyConnect Secure Web Gateway (SWG) ondersteunt geen SAML-verificatie tegen Entra ID; het gebruikt hetzelfde passieve verificatiemechanisme als on-premises AD.
    - Resolutie: ontwerp niet rond een SAML-gestuurde SWG-identiteit voor Entra ID; gebruik passieve verificatie zoals gedocumenteerd.
- Symptoom: gebruiker toont onjuist gedeactiveerd
    - Hoofdoorzaak: Entra-ID verzonden actief: false omdat de gebruiker buiten een toegewezen groepsbereik viel, of omdat een actieve attribuuttoewijzing verkeerd is geconfigureerd.
    - Resolutie: Controleer of de gebruiker is verwijderd uit een groep met een bereik; controleer de actieve toewijzing (moet gewoonlijk worden beoordeeld als Not([isSoftDeleted])).
- Symptoom: toepassing in quarantaine geplaatst, alle provisioning gestopt
    - Hoofdoorzaak: doeltoepassing gaf herhaalde niet-SCIM-conforme reacties terug.
    - Resolutie: Controleer de provisioningstatus van de Enterprise Application voor een quarantainevlag voordat u uitgaat van individuele gebruikersfouten.
- Symptoom: initiële provisioningcyclus mislukt volledig
    - Hoofdoorzaak: tijdelijke synchronisatiefout bij de eerste run.
    - Resolutie: Klik op Provisioning opnieuw opstarten vanaf de overzichtspagina om Entra ID te dwingen de initiële synchronisatie opnieuw te proberen.
- Symptoom: Dubbele gebruikers worden onverwacht samengevoegd
    - Oorzaak: twee bronidentiteiten delen dezelfde e-mail of gebruikersnaam (UPN).
    - Resolutie: zorg ervoor dat e-mail en UPN uniek zijn in de brondirectory; controleer of het e-mailattribuut afkomstig is van een geverifieerd domein.
- Symptoom: Attribuut stopt met bijwerken na wijziging schema
    - Hoofdoorzaak: Attribuuttype gewijzigd aan de doelzijde (bijvoorbeeld string naar boolean), maar de Entra ID mapping is niet bijgewerkt.
    - Resolutie: Corrigeer het type handmatig in Geavanceerde instellingen onder Toewijzing van kenmerken.
- Symptoom: referentiemanager vult nooit

- Hoofdoorzaak: een gebruiker bevond zich in het bereik voordat zijn manager was; provisioning wordt niet automatisch opnieuw gevuld.
- Resolutie: herstart de provisioning om een volledige herevaluatie van alle gebruikers binnen het bereik af te dwingen.

## IBM Security Specifieke problemen controleren

- Symptoom: Gebruikersvoorziening maar groepen verschijnen nooit in Secure Access
  - Hoofdoorzaak: Controleer of de aangepaste SCIM-connector alleen gebruikersbewerkingen uitgeeft; er worden nooit POST /Groups-oproepen verzonden (capaciteitstekort voor accountprovisioning, geen toewijzingsfout).
  - Resolutie: Leg een connectorspoor vast en bevestig of er groepen/aanroepen plaatsvinden; als dat niet het geval is, verschaf groepen via de Cisco AD Connector, CSV-import of een gepland script tegen het Secure Access SCIM-eindpunt.
- Symptoom: update van groepslidmaatschap mislukt met 400 of 404
  - Hoofdoorzaak: [].value-referenties Verifieer interne gebruikersnamen in plaats van de SCIM-ID Secure Access die bij het maken van de gebruiker wordt geretourneerd.
  - Resolutie: Corrigeer de toewijzende leden om de Secure Access SCIM ID te gebruiken en voer opnieuw een volledige synchronisatie uit.
- Symptomen: Groepen verschijnen maar zijn leeg
  - Hoofdoorzaak: groep gepusht voordat de gebruikers van het lid bestonden in Secure Access; lidmaatschap PATCH verwezen naar onbekende gebruikers.
  - Resolutie: Voer opnieuw een volledige synchronisatie uit nu er gebruikers bestaan; zorg ervoor dat synchronisatievolgorde gebruikers vóór groepen maakt.
- Symptoom: SAML-aanmeldingslussen of herhaalde omleidingen
  - Hoofdoorzaak: Controleer of het IdP-eindpunt is geproxied of gedecodeerd door de SWG, die de verificatiestroom doorbreekt.
  - Resolutie: omzeilen de Verify IdP URL van SAML of decryptie (externe domeinlijst of selectieve decryptie).
- Symptoom: Gebruiker verifieert via SAML, maar er komen geen gebruikersgebaseerde beleidsovereenkomsten overeen
  - Hoofdoorzaak: SAML NameID komt niet overeen met de voorziene user authName.

    - Resolutie: Lijn de indeling NameID > in de toepassing Verify SAML uit met de toewijzing van het attribuut authName (meestal e-mail of UPN); test opnieuw.

- Symptomen: Provisioning stopt na weken of maanden van stabiliteit

    - Hoofdoorzaak: SCIM-token is geroteerd of verlopen in Secure Access, maar niet bijgewerkt in de Verify-connector.

    - Resolutie: Vernieuw het token in Secure Access en werk het bij in de aangepaste toepassing verifiëren; kalender de cadans voor het vernieuwen.

- Symptoom: gebruikers dupliceren die bij hersynchronisatie zijn gemaakt

    - Hoofdoorzaak: externeId toegewezen aan een veranderbaar of niet-uniek kenmerk (bijvoorbeeld, weergavenaam, veranderbaar e-mailadres).

    - Resolutie: externeId toewijzen aan een onveranderlijke id (gebruikersnaam of objectGUID verifiëren); duplicaten opschonen en opnieuw synchroniseren.

- Symptoom: gedeactiveerd Gebruikers verifiëren actief te blijven in beveiligde toegang

    - Hoofdoorzaak: Actie opschorten die niet is toegewezen aan actief: false, of de bewerking deactiveren die is uitgeschakeld in de connector.

    - Resolutie: schakel de uitschakelbewerking in en de kaart wordt onderbroken om actief:false te activeren; controleer met een testgebruiker.

- Symptoom: wijzigingen in kenmerken in Verifiëren worden niet doorgegeven

    - Hoofdoorzaak: gebruiker of attribuut buiten het bereik van het provisioningbeleid of bijwerkingsbewerking uitgeschakeld.

    - Resolutie: controleer het beleid of de rechten voor provisioning van toepassingen; schakel updates in; activeer een handmatige synchronisatie.

- Symptoom: Secure Access weigert aanvragen met schema of 501-stijl fouten

    - Hoofdoorzaak: payload die niet voldoet aan SCIM (ontbrekende array met schema's, verkeerde URN, niet-ondersteunde bewerking).

    - Resolutie: reproduceren met de curl-test bij baseline; de payload of mapping corrigeren; escaleren naar IBM als de connector het misvormde verzoek uitzendt.

- Symptoom: SWG-identiteit ontbreekt voor roamende gebruikers ondanks SAML-werking

- Hoofdoorzaak: verwacht dat SAML de identiteit van een implementatiemodus aanstuurt die passieve of agentgebaseerde identiteit gebruikt.

- Resolutie: Bevestig de methode voor het verkrijgen van de identiteit voor elke implementatiemodus aan de hand van documentatie voor beveiligde toegang; ontwerp

SAML niet als enige identiteitsbron.

### Algemene SCIM-problemen

Deze zijn niet Cisco-specifiek, maar worden consistent weergegeven in Secure Access-implementaties omdat het onderliggende transport standaard SCIM 2.0 is:

- Quarantainetoestanden maskeren individuele fouten: Als de synchronisatie volledig lijkt te zijn gestopt in plaats van per gebruiker te mislukken, controleert u op een quarantaine- of opschortingsstatus op toepassingsniveau voordat u individuele attribuutproblemen onderzoekt.
- 409 Conflict over deactivering: Een gemeenschappelijk patroon waarbij de IdP probeert een gebruiker te deactiveren en het doel een conflict veroorzaakt. Dit is meestal een probleem met actieve attribuuttoewijzing of een probleem met een groepsbereik, geen echte systeemfout.
- Lege of verwijderde velden verspreiden zich niet altijd: sommige SCIM-serverimplementaties behouden de laatste niet-nulwaarde; wanneer u een veld in de IdP wist, kan het vereisen dat u eerst een plaatsaanduidingswaarde doordrukt.
- Wijzigingen in URL of configuratie maken authenticatie in stilte ongeldig: elke wijziging in de SCIM-eindpunt-URL vereist meestal dat u het token aan toonder opnieuw verstrekt. Fouten duiken op als ongeldige URL, zelfs als het echte probleem een verouderd token is.
- Geen native webhook of gebeurtenisstroom: Automatisering die realtime pushmeldingen over gebruikers- of beleidswijzigingen verwacht, moet de rapportage-API pollen of integreren via Cisco XDR in plaats daarvan. Secure Access zendt geen uitgaande provisioning-webhooks uit.

Escaleer naar Cisco TAC met provisioninglogs van de IdP-kant als de vorige stappen het probleem niet oplossen. Backend provisioning logs aan de Secure Access kant vereisen over het algemeen TAC toegang tot pull.

## Oorzaak

De integratie van SCIM-provisioning is er niet in geslaagd een of meer records te pushen vanwege een verlopen token aan toonder, een mismatch in attribuuttoewijzing, ontbrekende doelgroep of onvoldoende provisioningbereik.

# Gerelateerde inhoud

- Cisco: gebruikers en groepen toegang bieden via Entra ID
- Cisco: gebruikers en groepen toegang bieden via OKTA
- Microsoft Learn: Bekende problemen met naleving van het SCIM 2.0-protocol – Microsoft Entra ID
- Microsoft Learn: Problemen oplossen met Microsoft Entra ID SCIM API-fouten
- SAML SSO configureren in de identiteitsprovider: https://www.ibm.com/docs/en/security-verify?topic=sign-configuring-saml-single-in-identity-provider
- Provisioning voor aangepaste (SCIM) toepassingen: https://www.ibm.com/docs/en/security-verify?topic=endpoints-configuring-provisioning-custom-applications
- Overzicht provisioning en governance (generieke SCIM-connector): https://docs.verify.ibm.com/verify/docs/use-cases-provisioning-and-governance
- On-premises provisioning bridge (AD/LDAP-bronnen): https://docs.verify.ibm.com/verify/docs/on-premises-provisioning

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.