Secure Access AD Connectors migreren van legacy-verificatie naar API-verificatie

Inhoud

uitgifte

Organisaties die Cisco Secure Access met Active Directory (AD)-connectors gebruiken, ontvangen meldingen die aangeven dat API-verificatie wordt aanbevolen voor Active Directory en Virtual Appliances, waarbij de bestaande verificatie op 29 mei 2026 afloopt. Gebruikers hebben configuratiehulp nodig om vóór de vervaldatum van de oude verificatie naar API-verificatie te migreren en willen de mogelijke impact op de synchronisatie van AD en virtuele apparaten tijdens het migratieproces begrijpen. De belangrijkste zorg is of het implementeren van deze wijziging tijdens werkuren storingen in AD- en VA-synchronisatiebewerkingen kan veroorzaken die van invloed kunnen zijn op identiteit- en beleidsafhankelijke bewerkingen.

milieu

- Cisco Secure Access (voorheen Cisco Umbrella)
- Active Directory-connectors geïmplementeerd
- Legacy-verificatiemethode die momenteel wordt gebruikt
- API-authenticatiemigratie vereist vóór 29 mei 2026
- AD-only-omgeving (in sommige gevallen zonder virtuele apparaten)

resolutie

De migratie van legacy-verificatie naar API-verificatie omvat het genereren van API-sleutels in het Secure Access-portaal en het correct configureren ervan. Het proces vereist het maken van zowel Admin API-sleutels als Client API-sleutels voor de AD Connectors en Virtual Appliances.

Stap 1: API-sleutel voor beheerders genereren

Navigeer naar Beheer > API-sleutels in het beveiligde toegangsportaal en genereer een nieuwe Beheer-API-sleutel en Beheersleutel Geheim. Sla deze referenties veilig op, omdat ze nodig zijn om het Client API-sleutelpaar te genereren.

Stap 2: Client API Key Pair genereren

Navigeer naar Gebruikers en groepen > Configuratiebeheer > Geavanceerde instellingen en zoek de sectie API-verificatie. Voer de in stap 1 gegenereerde Admin API Key en Admin Key Secret in en klik vervolgens op Generate Client API Key Pair. Dit produceert de Client API Key en Client Secret die wordt gebruikt door de AD Connectors en Virtual Appliances.

Stap 3: API-verificatie configureren in geavanceerde instellingen

Kopieer de gegenereerde Client API Key en Client Secret in de sectie API Authentication Advanced Settings van het Secure Access-portaal. Sla deze referenties veilig op, omdat ze vereist zijn voor alle configuraties van AD Connector en Virtual Appliance.

Stap 4: AD-connectors en virtuele apparaten bijwerken

Pas de nieuw gegenereerde Client API Key en Client Secret toe op alle geïmplementeerde AD-connectors en virtuele apparaten. Dit zorgt ervoor dat ze correct kunnen verifiëren voor registratie en gezondheidscontroles met behulp van de nieuwe API-verificatiemethode.

Migratie-impact en best practices

Het genereren van API-sleutels in het Secure Access-portaal is doorgaans niet storend. Operationele impact treedt echter op tijdens het clientmoment wanneer AD Connectors en Virtual Appliances worden bijgewerkt om de nieuwe Client API Key en Secret te gebruiken.

Verwachte impact tijdens de cutover:

- Er kunnen tijdelijke synchronisatie- en healthcheck-fouten optreden voor componenten die nog steeds gebruikmaken van legacy-verificatie.
- AD/VA-synchronisatievertraging of -storing tijdens het overgangsvenster.
- Beleidsbeslissingen die gebaseerd zijn op nieuwe identiteits-/groepsgegevens kunnen worden beïnvloed als synchronisatie mislukt.

Aanbevolen uitvoeringsaanpak:

- Voer indien mogelijk migratie uit tijdens kantooruren of onderhoudsvensters.
- Gebruik voor de implementatie van werkuren een beheerste aanpak voor het bijwerken van werkuren.
- Werk één connector/VA tegelijk bij en controleer de gezonde status voordat u verdergaat.
- Vermijd het gelijktijdig bijwerken van alle nodes.
- Zorg voor voldoende redundantie met meerdere connectors/VA's voor rollende updates.

Compatibiliteit en eisen:

- API-verificatie werkt met AD-only implementaties en vereist geen virtuele apparaten.
- Zowel legacy- als API-authenticatiemethoden blijven actief tijdens de migratieperiode.
- AD Connectors moet kunnen synchroniseren met Umbrella via api.opendns.com en overstappen naar api.umbrella.com.

Oorzaak

Cisco Secure Access gaat over van legacy-authenticatiemethoden naar API-authenticatie als het standaard authenticatiemechanisme. De legacy authenticatiemethode heeft een geplande afschrijvingsdatum van 29 mei 2026. API-verificatie wordt uiteindelijk de enige ondersteunde verificatiemethode en organisaties moeten migreren voordat de oude methode verloopt om serviceonderbrekingen en mogelijke AD/VA-synchronisatiefouten te voorkomen die volledige herinstallatie vereisen om te herstellen.

Gerelateerde inhoud

- Cisco Secure Access API-verificatiedocumentatie
- Cisco Secure Access Advanced Configuration
- Cisco Secure Access Configuration Management
- 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.