Cisco Secure Access-integratie met ISE voor Security Group-tag via Pargrid Cloud

Inhoud

Inleiding

In dit document wordt beschreven hoe u het delen van context tussen Cisco Secure Access en Cisco Identity Services Engine kunt inschakelen

Vereisten

Cisco raadt u aan deze onderwerpen te kennen:

- Cisco Secure Access—een cloud-gebaseerde security service edge (SSE) oplossing die zero-trust netwerktoegang biedt zodat gebruikers eenvoudig verbinding kunnen maken met het internet en privétoepassingen vanaf elk apparaat.
- Cisco Identity Service Engine (ISE) versie 3.4 Patch 5.
- Cisco Security Cloud Control—Een uniforme beheeroplossing voor uw Security Cloud-producten en -identiteit. Security Cloud Control is inbegrepen bij Secure Access.

Achtergrond

Deze integratie maakt de geautomatiseerde creatie van betrouwbare tunnels van Catalyst SD-WAN-vestigingen naar Cisco Secure Access mogelijk, waardoor de naadloze uitwisseling van VPN-ID / naam en SGT-context wordt vergemakkelijkt.

Cisco Identity Services Engine (ISE) blijft de centrale autoriteit voor SGT-configuratie en -beheer. Alle updates die in ISE worden uitgevoerd, worden automatisch gesynchroniseerd met Cisco Secure Access. Als een SGT wordt verwijderd, blijven de bestaande regels die ernaar verwijzen actief om ervoor te zorgen dat de matching van verkeer doorgaat zoals verwacht.

We bieden momenteel beperkte beschikbaarheid voor SGT-toewijzingen, waardoor de ondersteuning wordt uitgebreid met SGT-bestemmingsobjecten binnen uw beveiligingsregels. Bovendien komt er binnenkort ondersteuning voor het bouwen van SASE-tunnels die SGT van Meraki en Cisco Secure Firewall vervoeren

Use case:

SGT-naamruimte gebaseerd beleid:

Als beveiligingsbeheerder wil Kit aaneengesloten micro-segmentatie afdwingen met behulp van SGT van onprem ISE voor SSE Private en Internet Bound Traffic.Ability om SGT te importeren om beleid toe te passen.

Gebruikte componenten

De informatie in dit document is gebaseerd op:

- Identity Service Engine (ISE) versie 3.4 Patch 5
- beveiligde toegang
- Cisco Security Cloud

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuratie van contextdeling - Overzicht

- ISE verbinden met CIsco Security Cloud
- Cisco Secure Access verbinden met ISE

Configureren

In deze handleiding wordt de algemene configuratie opgesplitst in de volgende hoofdstappen:

1. Cisco ISE verbinden met Cisco Security Cloud
2. Cisco Secure-toegang verbinden met Cisco ISE
3. Tags voor beveiligingsgroepen in Cisco Secure Access

Voordat u begint

- Zorg ervoor dat u de Advantage-licentie hebt geïnstalleerd en geactiveerd in uw Cisco ISE-implementatie.
- De DNA Cloud-agent maakt een uitgaande HTTPS-verbinding met Cisco DNA Cloud. Daarom moet u de proxy-instellingen van Cisco ISE configureren als het netwerk een proxy gebruikt om het internet te bereiken. Als u proxyinstellingen wilt configureren in Cisco ISE, gaat u naar **Administration** > **System** > **Settings** > **Proxy**
- Zorg ervoor dat poort 443 is geopend voor uitgaande verbinding van Cisco ISE naar Cisco pxGrid Cloud portal. Als firewall- of proxy-instellingen zijn geconfigureerd, controleert u of deze URL's niet worden geblokkeerd:

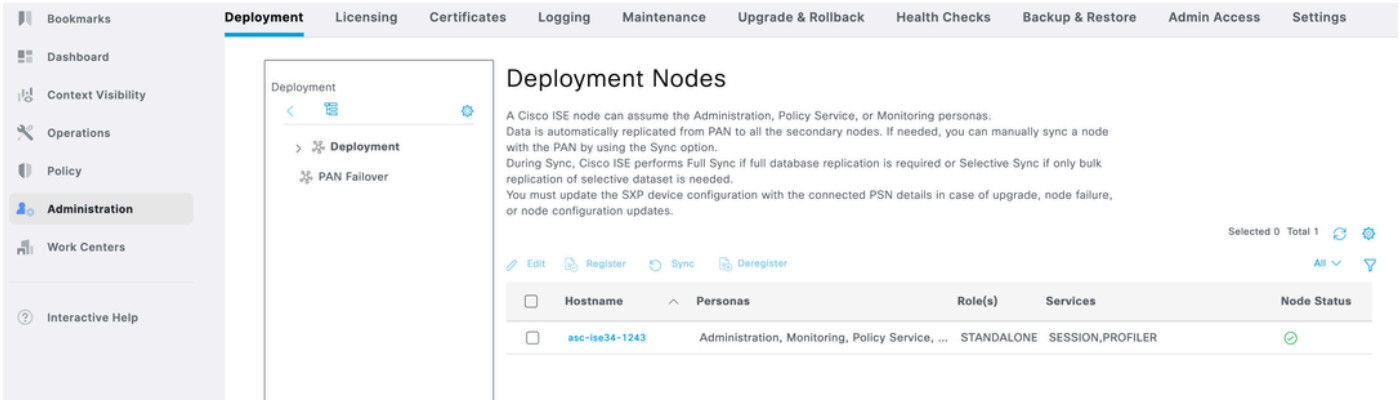
https://dna.cisco.com

https://security.cisco.com/

Stap 1: PxGrid Cloud inschakelen op ISE

1 Navigeer naar ISE GUI.

2 Klik op Beheer - Implementatie.

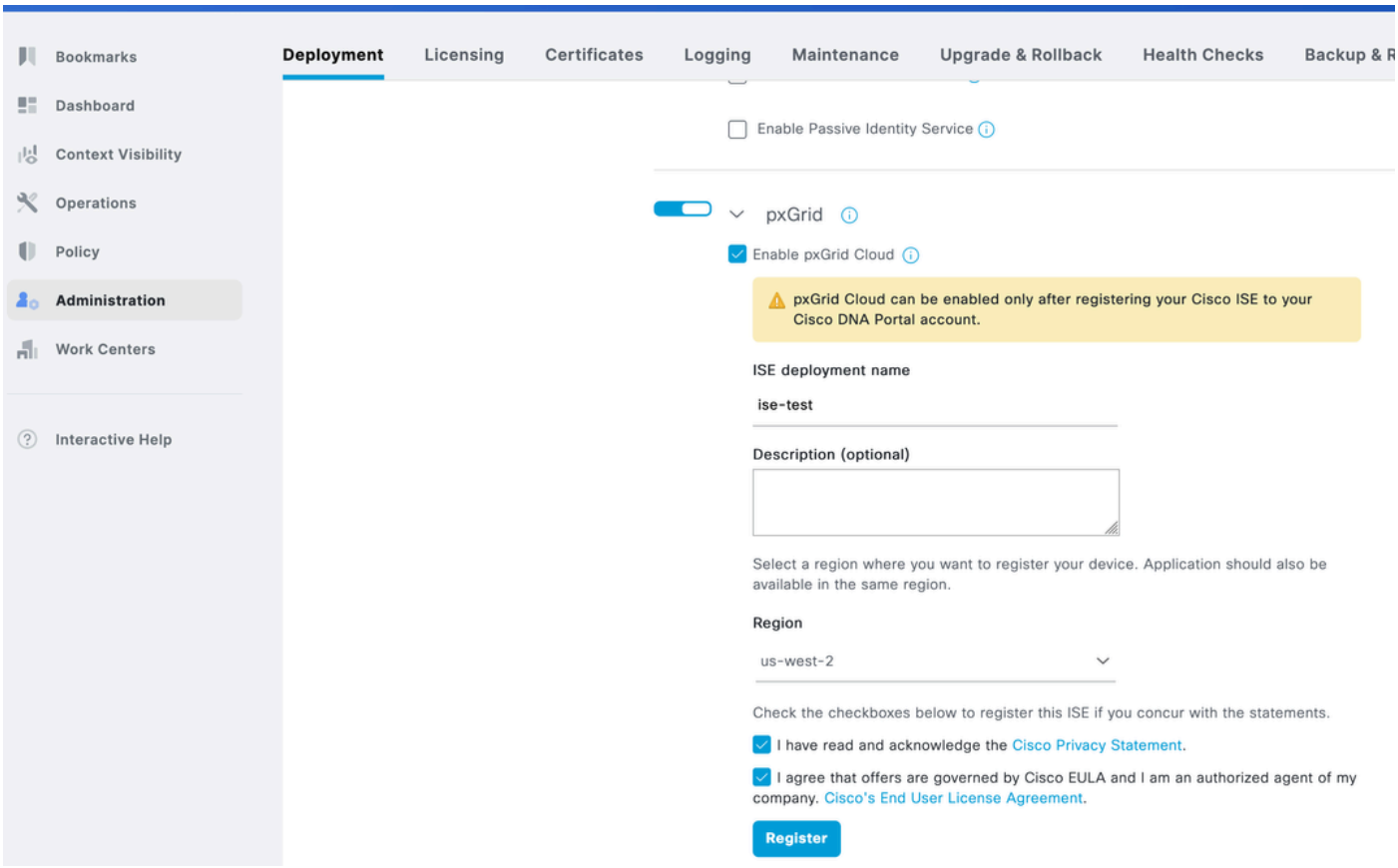


3 Klik op de Node en scroll naar beneden.

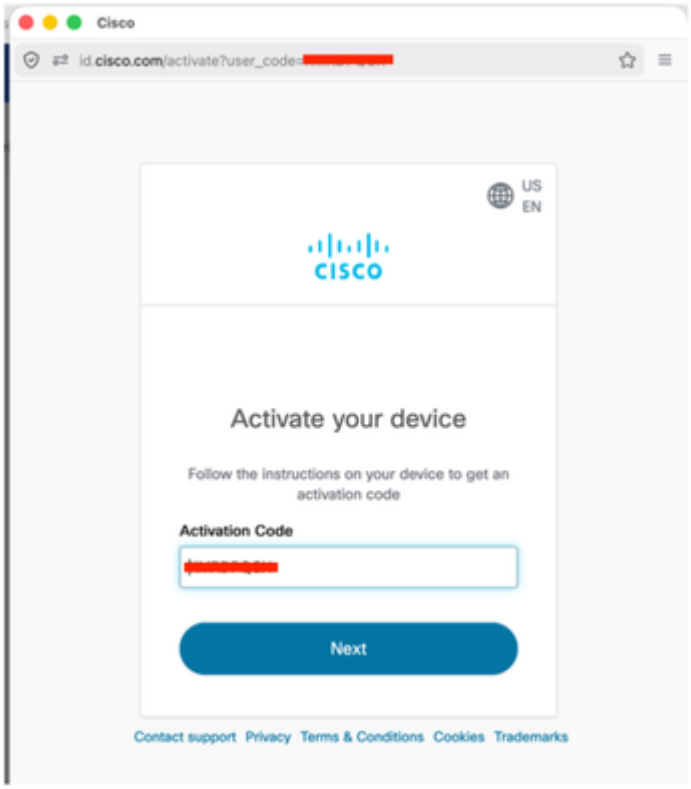
ISE-implementatienaam invoeren

Selecteer de regio als US West 2, de enige regio die op dit moment wordt ondersteund.

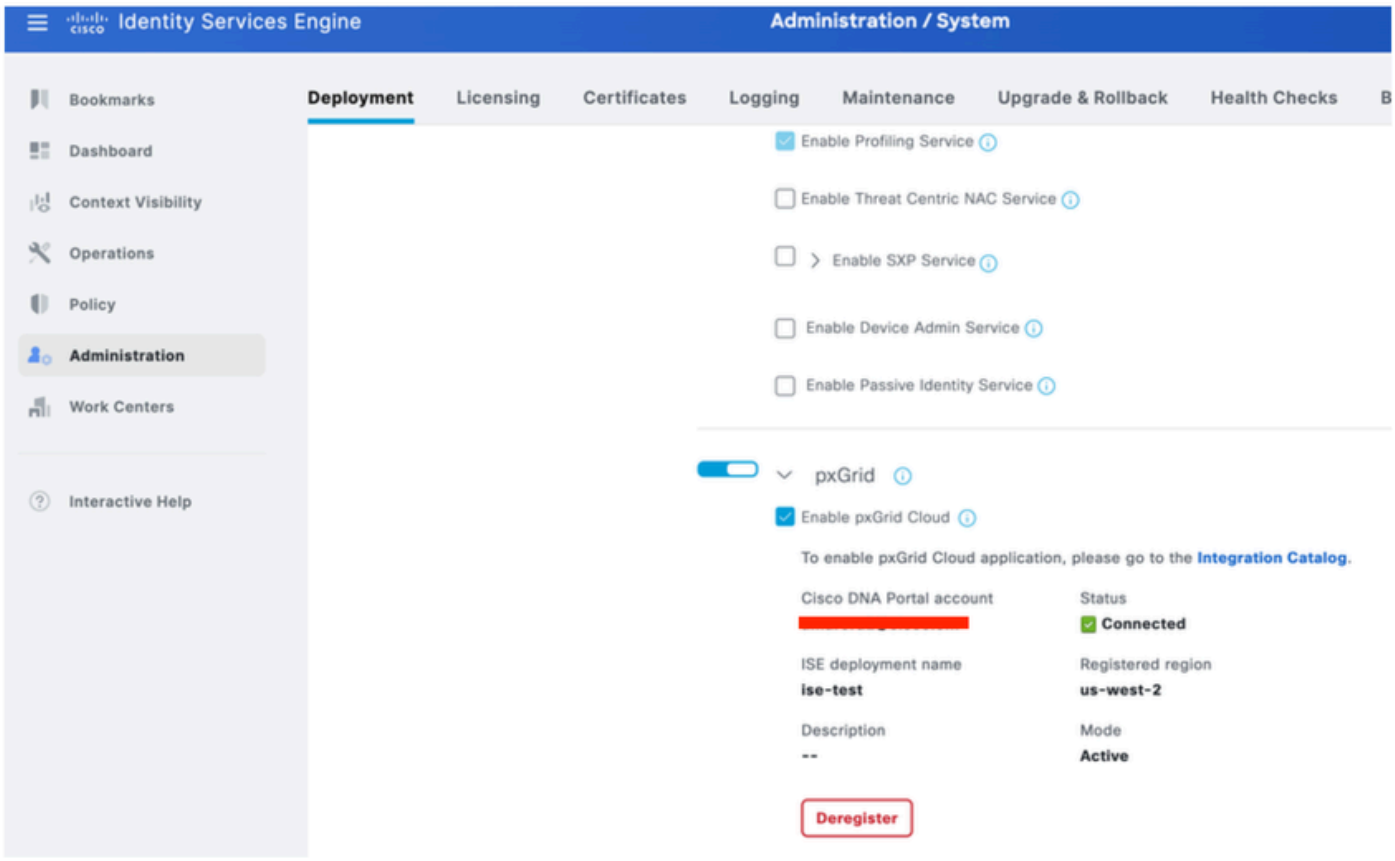
Schakel beide selectievakjes in en klik op Inschrijven.



4 Er verschijnt een pop-up met automatisch ingevulde activeringscode.Klik op Volgende,



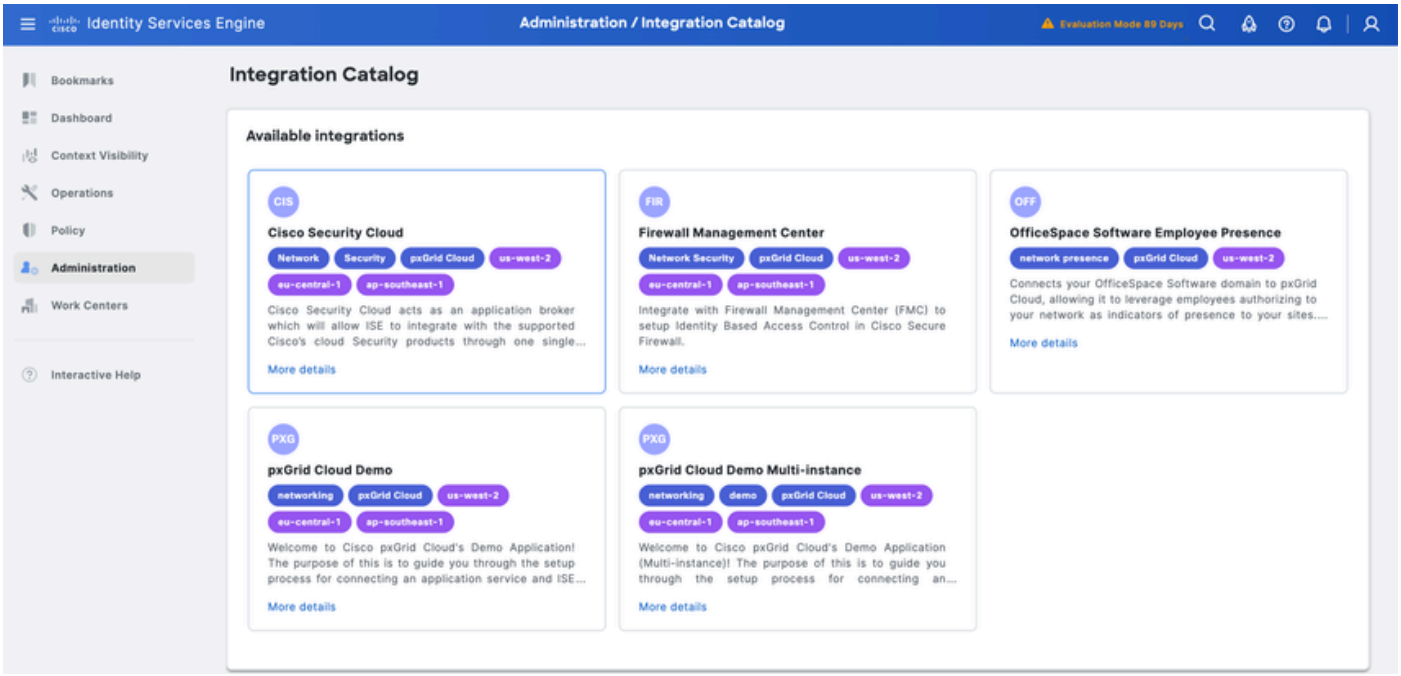
5 ISE toont aangesloten op Pargrid Cloud.



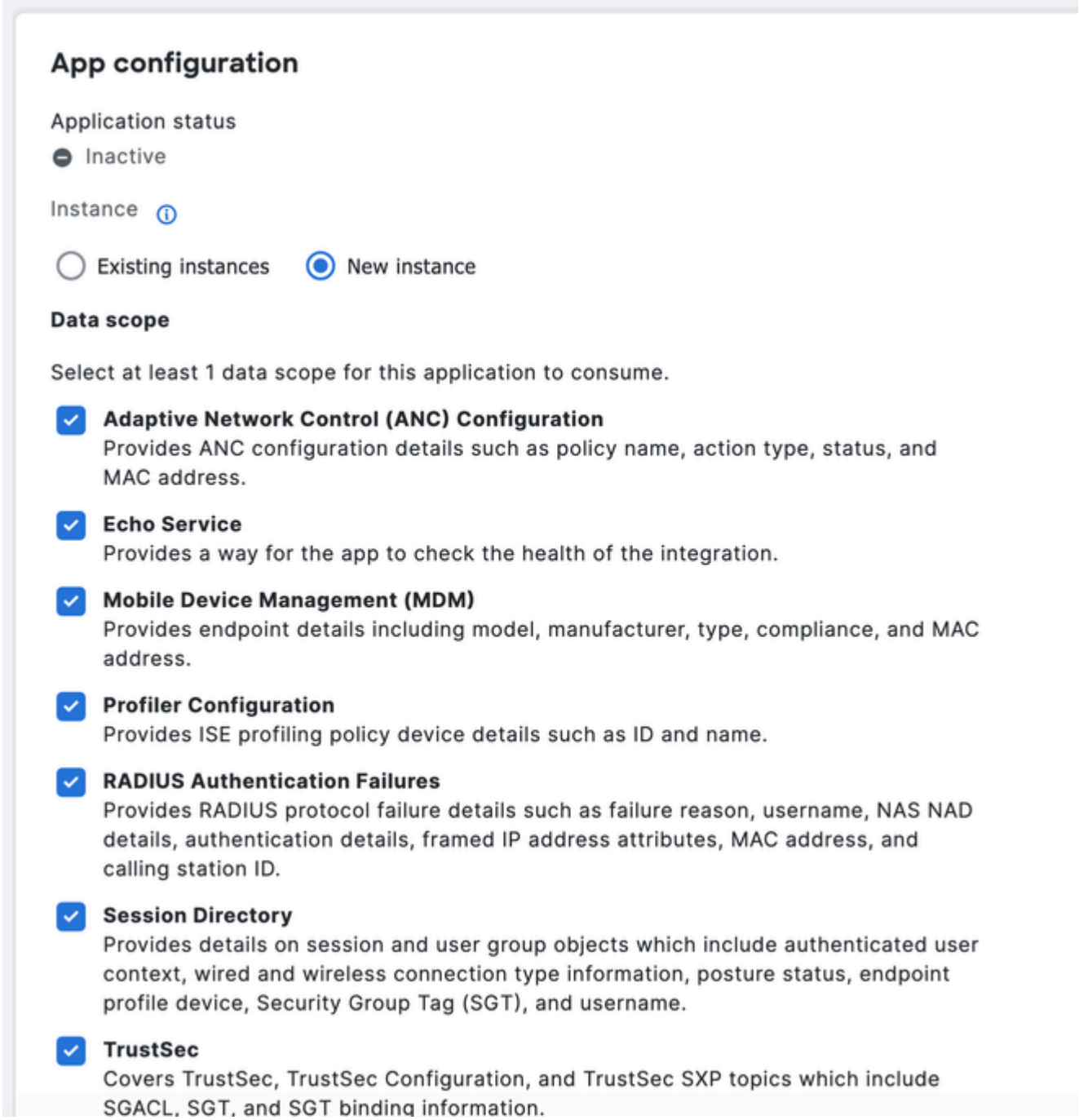
6 Klik op de link Integratiecatalogus van stap 5.

Klik onder Beschikbare integraties op Cisco Security Cloud

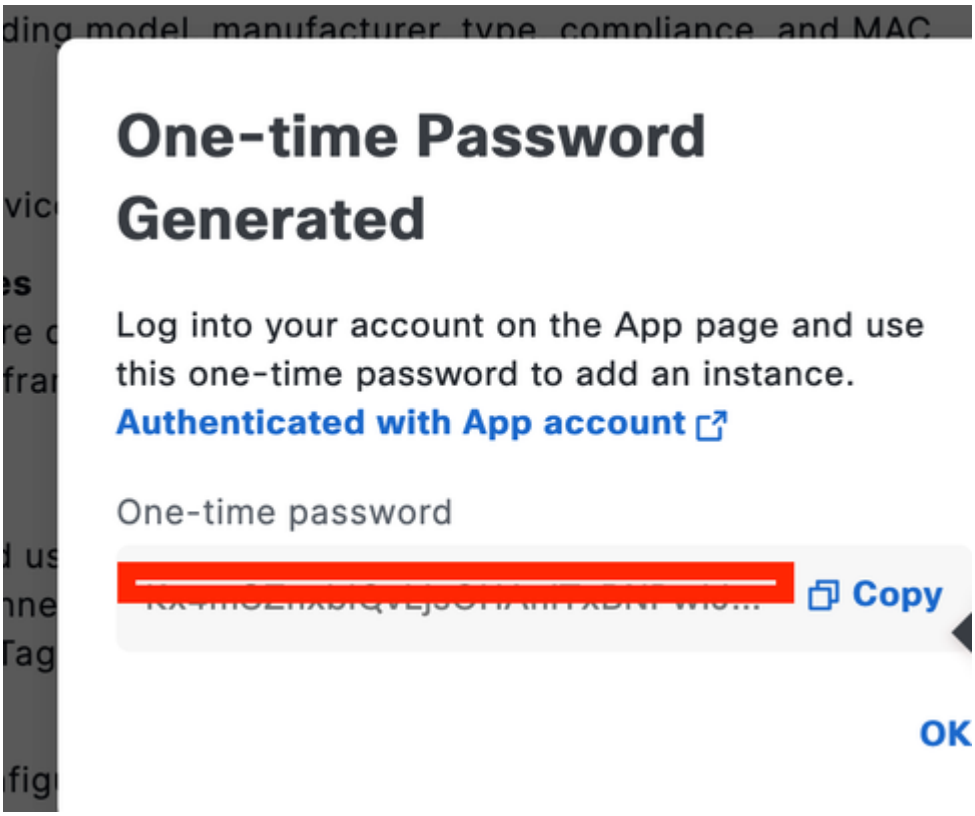
.



7 Klik onder App Configuration op New Instance en klik op Activate

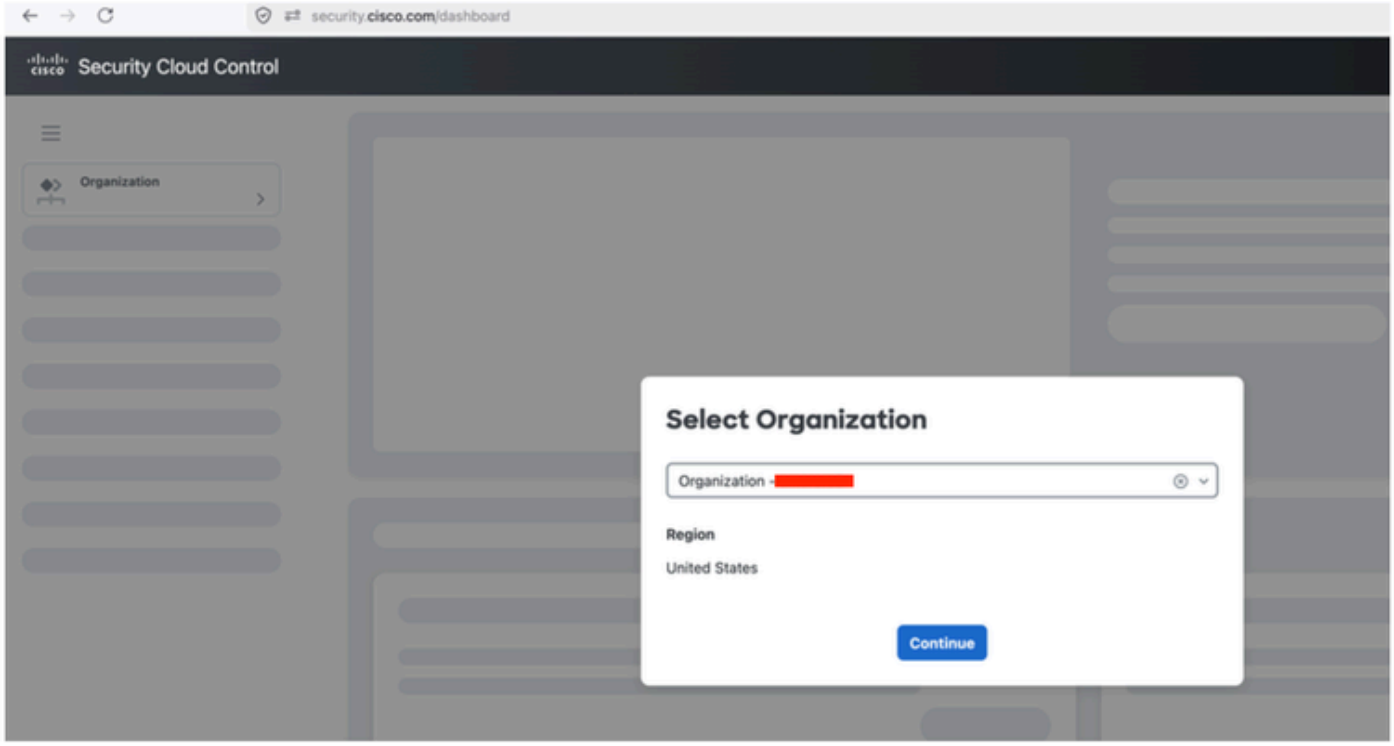


Kopieer het eenmalige wachtwoord zoals het wordt gebruikt in Cisco Secure Access.

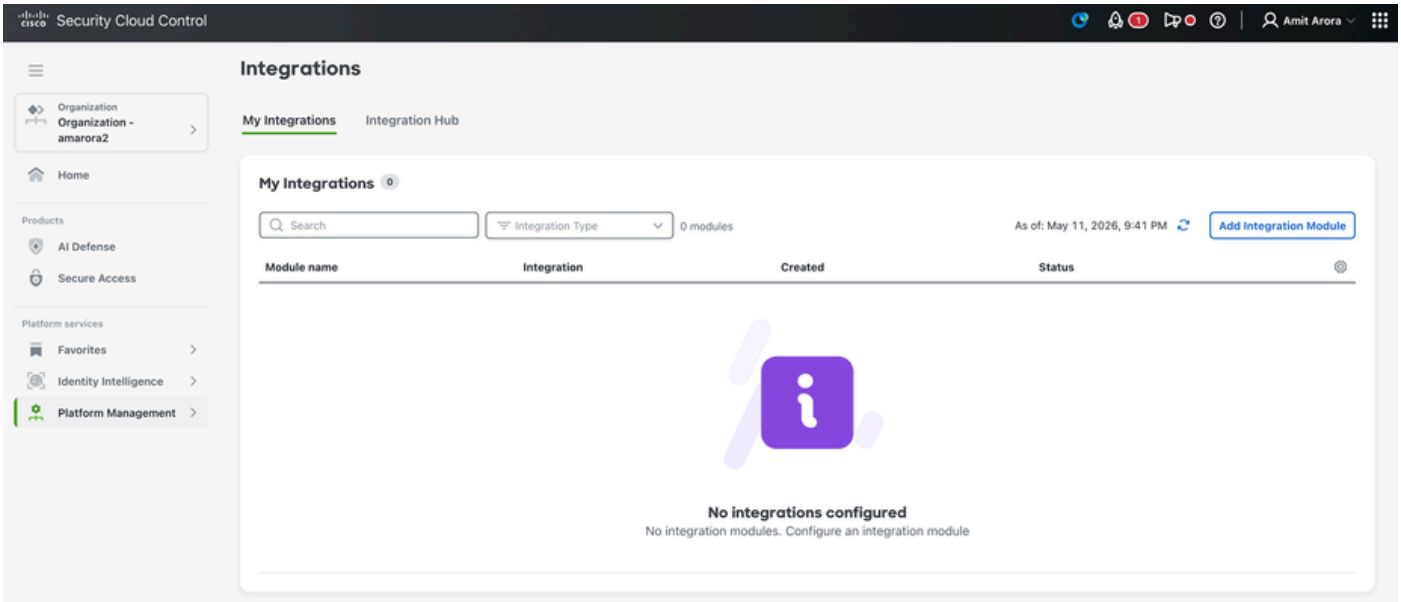


Stap 2: Cisco Secure Access integreren met ISE

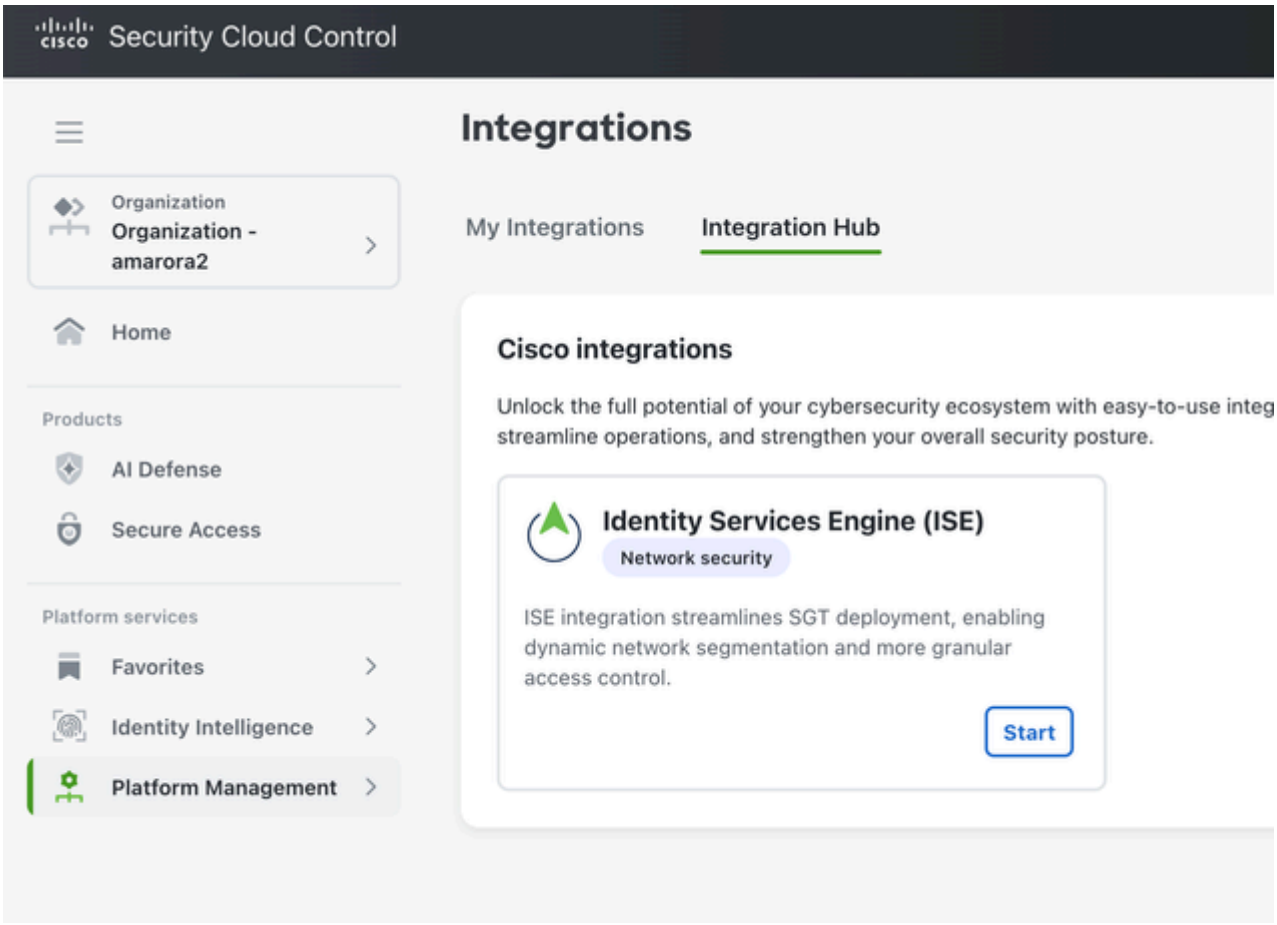
1. Log in op security.cisco.com.
2. Selecteer de Cisco Secure Access ORG



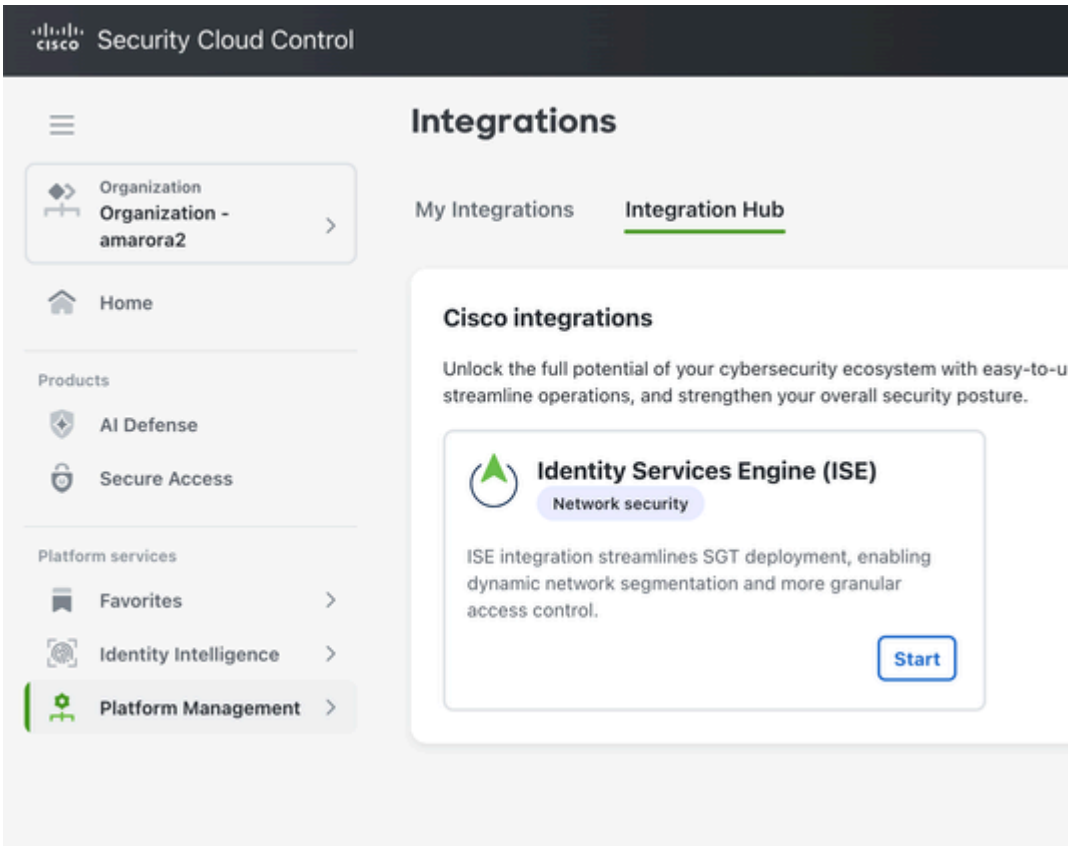
3 Klik op Platform Management - Platform Integraties



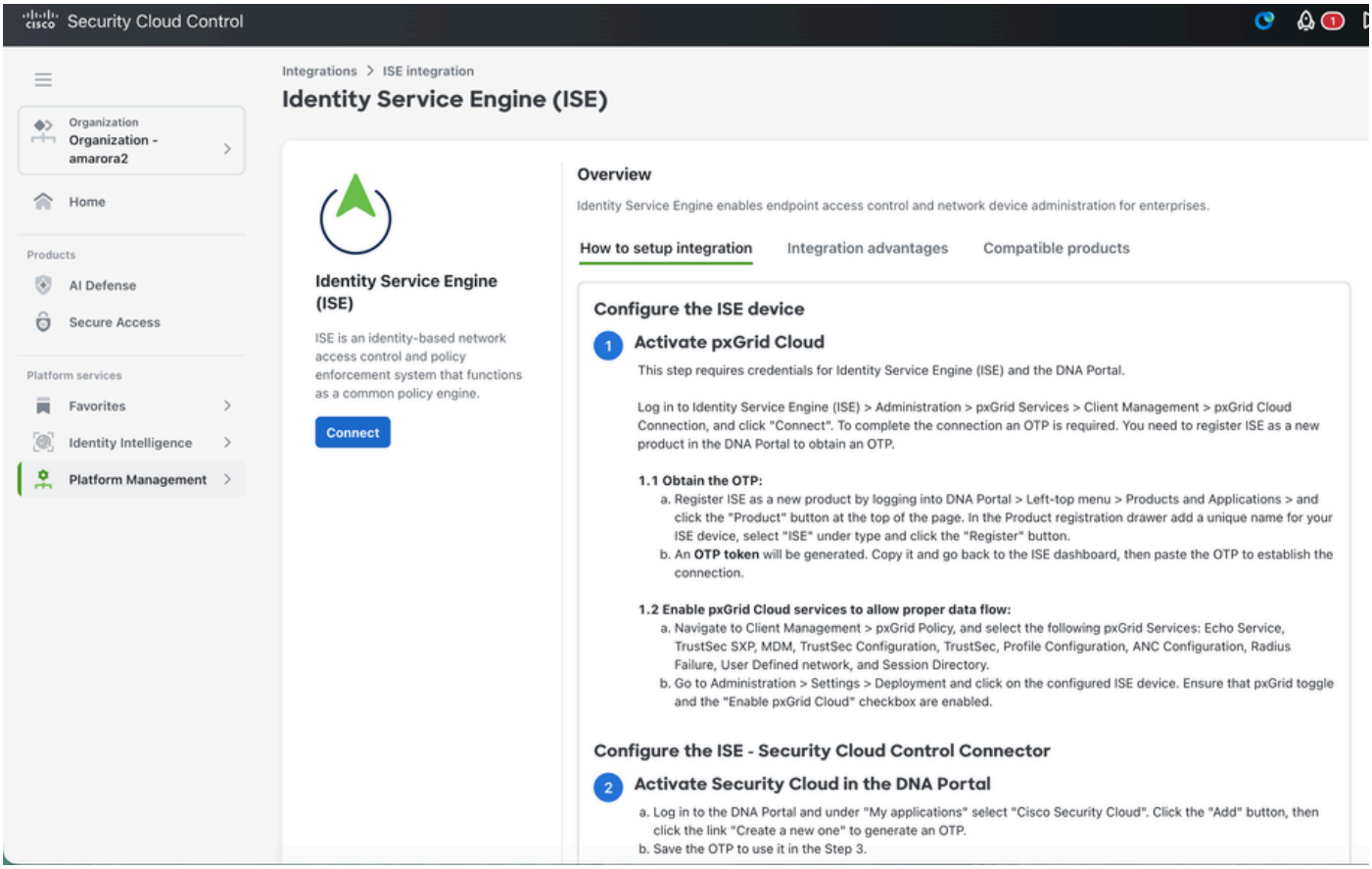
4 Klik op Integratiemodule toevoegen



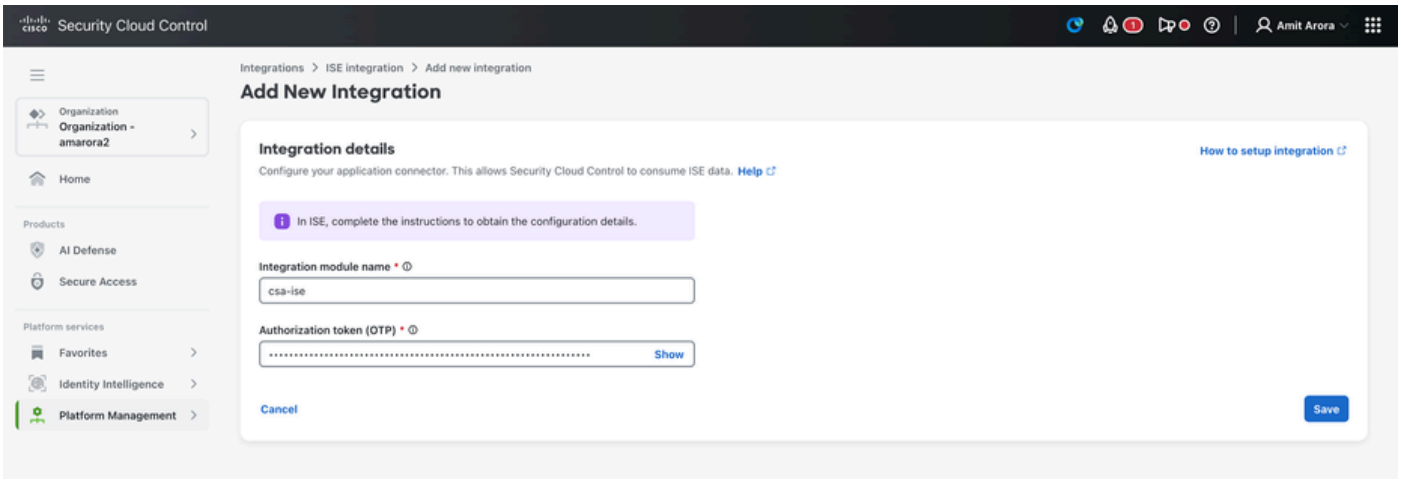
5 Klik op Start



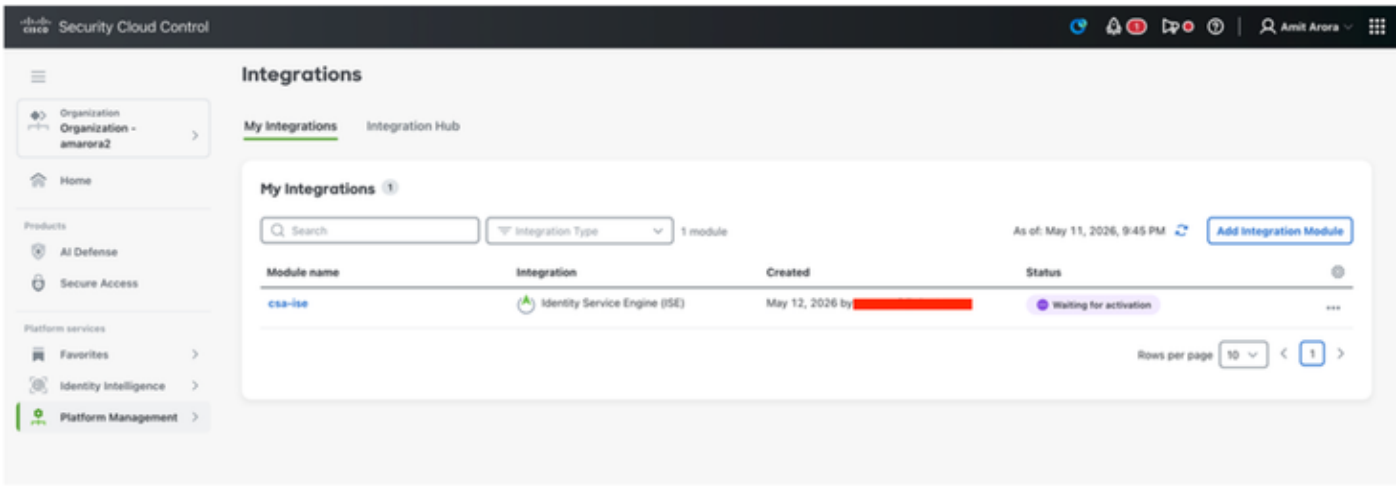
6 Klik op Verbinden



7. Voer de naam van de integratiemodule en de OTP van Cisco ISE in en klik op Opslaan

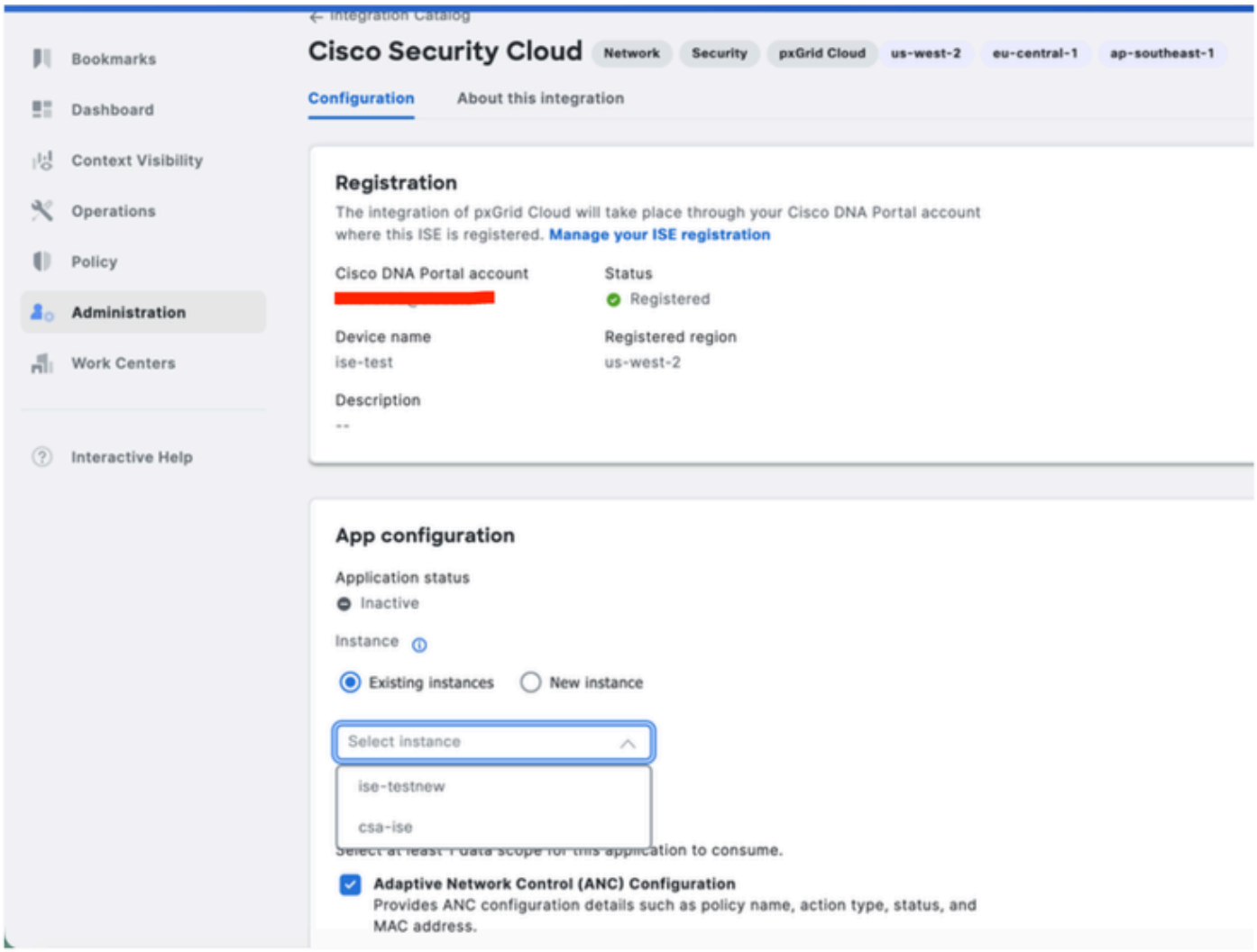


8 Zodra u op Opslaan klikt, wordt de status Wachten op activering weergegeven.

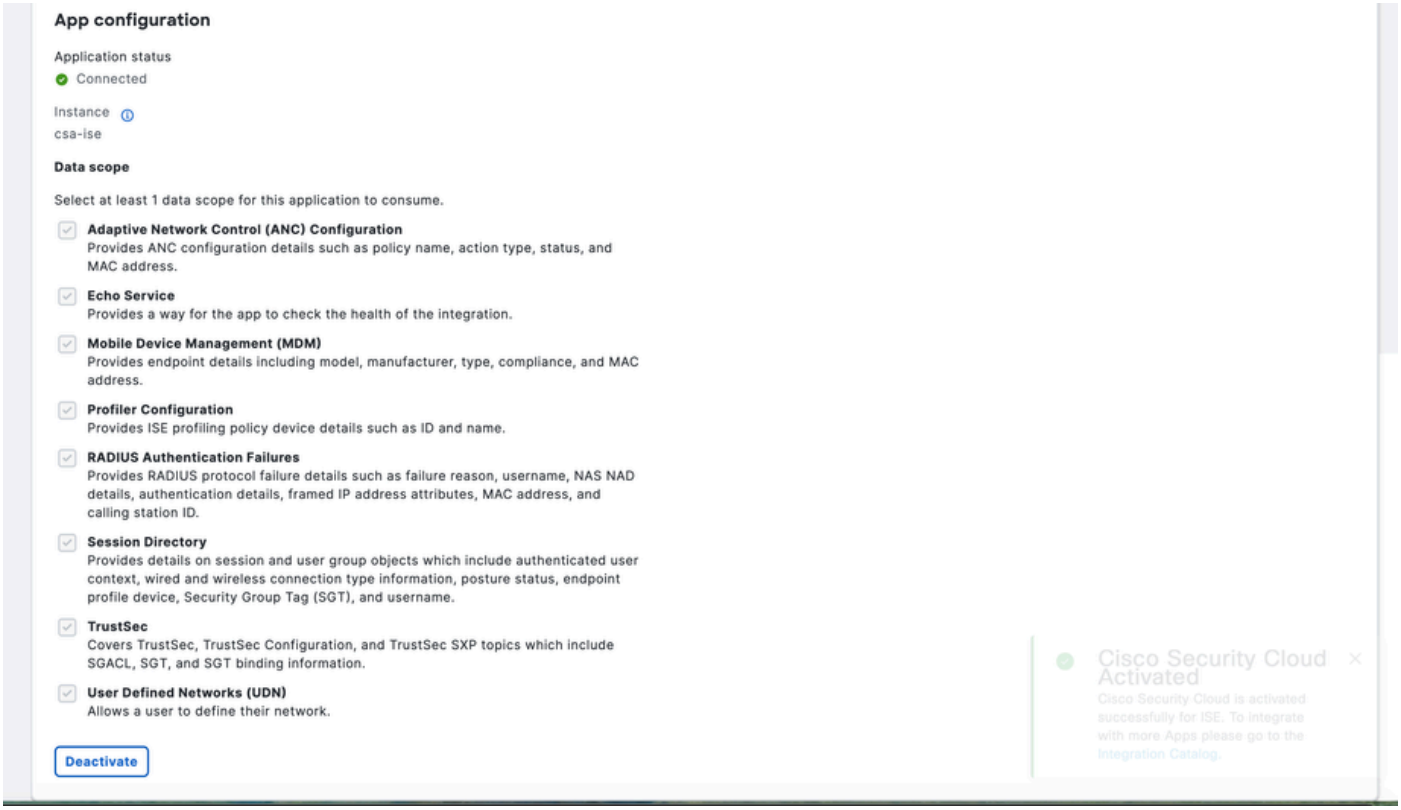


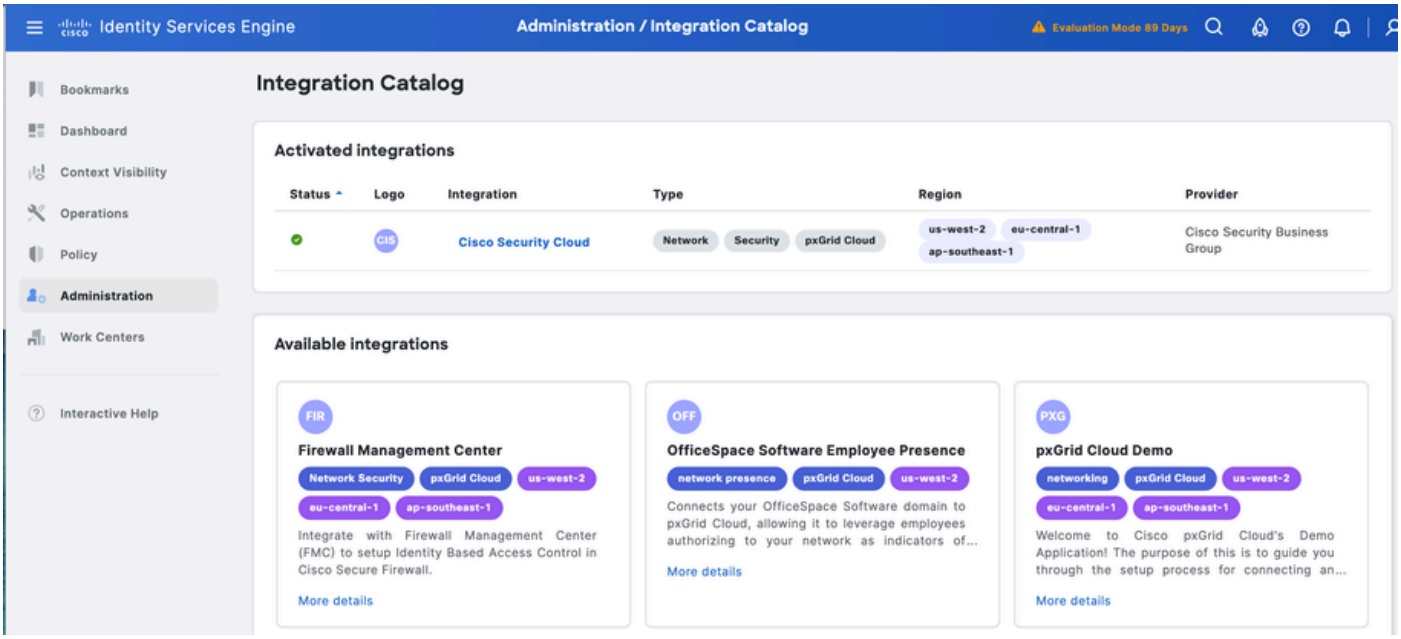
9 Meld u aan bij ISE en navigeer naar Beheer - Implementatie. Klik op de node met pxgrid personna - klik op Integratie cloud onder Pargrid Connection.

Selecteer onder App-configuratie de ISE-instantie die is gemaakt in Security Cloud Control en klik op Activeren



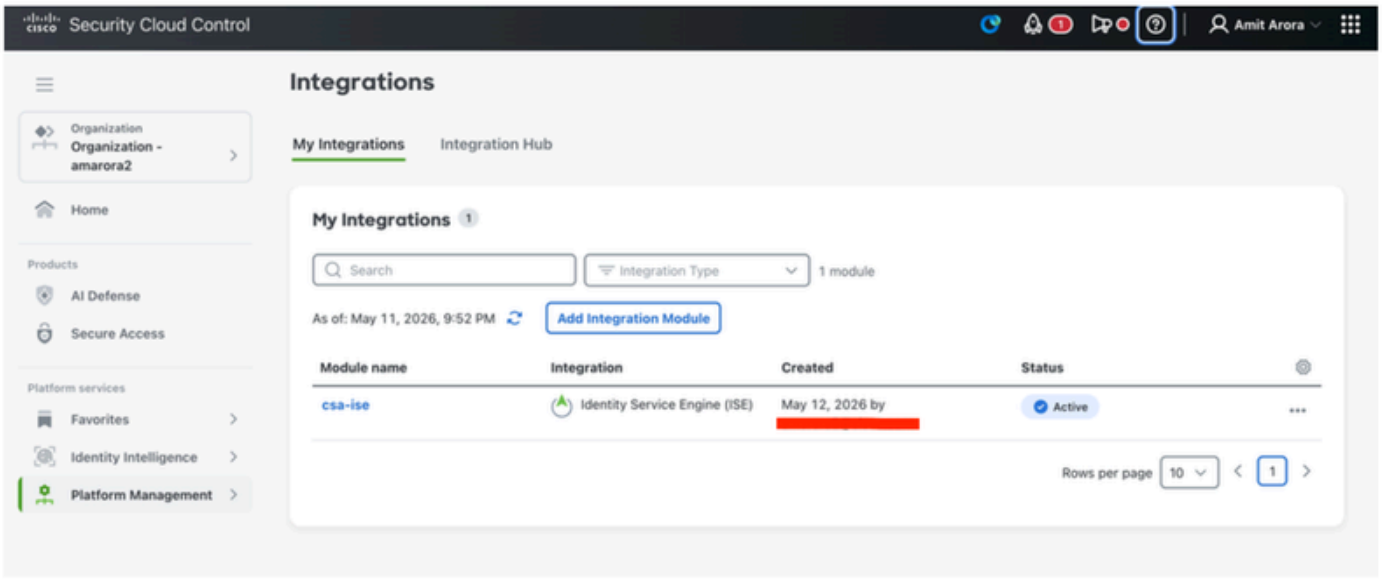
10 Toepassingsstatus is nu verbonden.





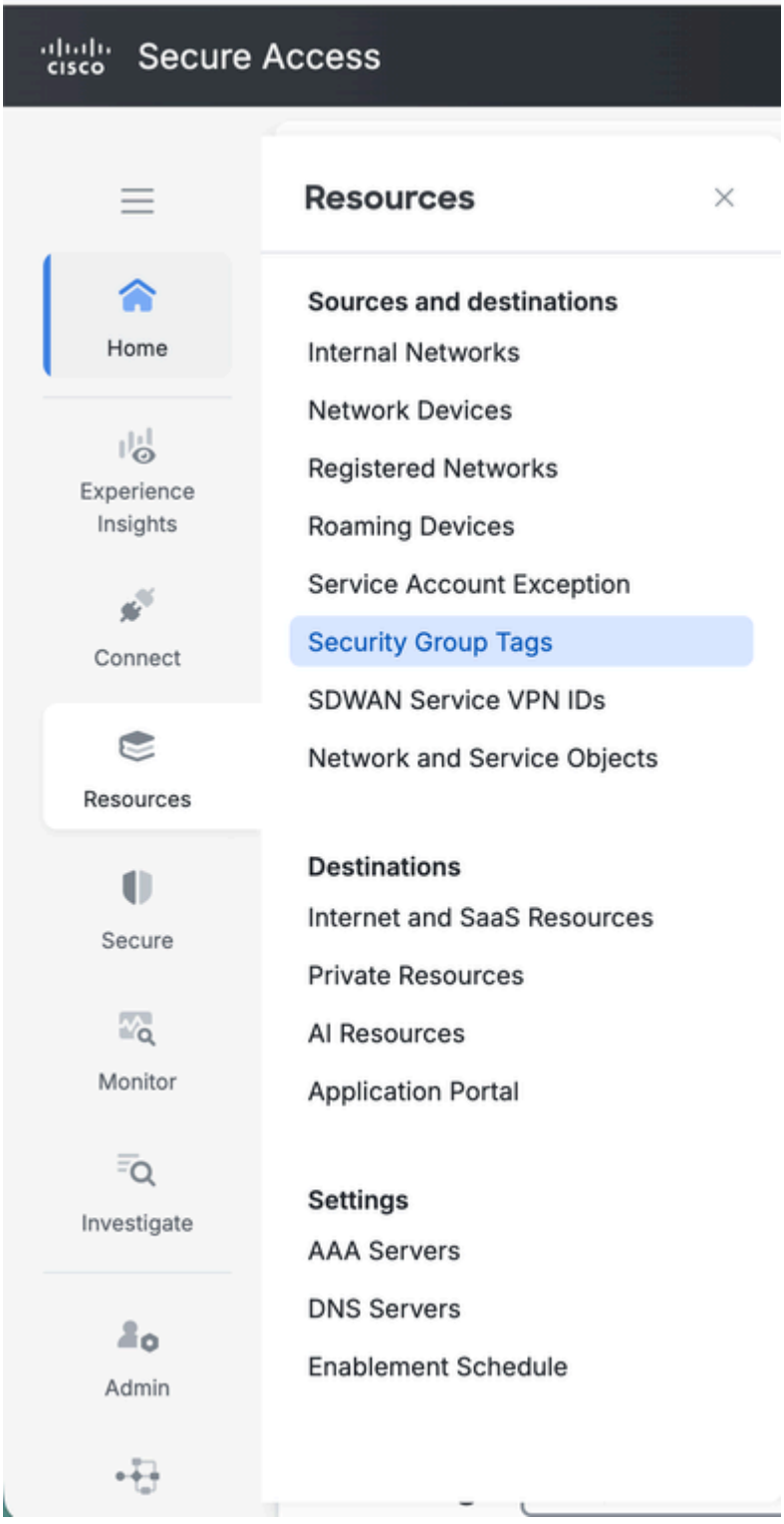
11 Aanmelden bij Security Cloud control - security.cisco.com

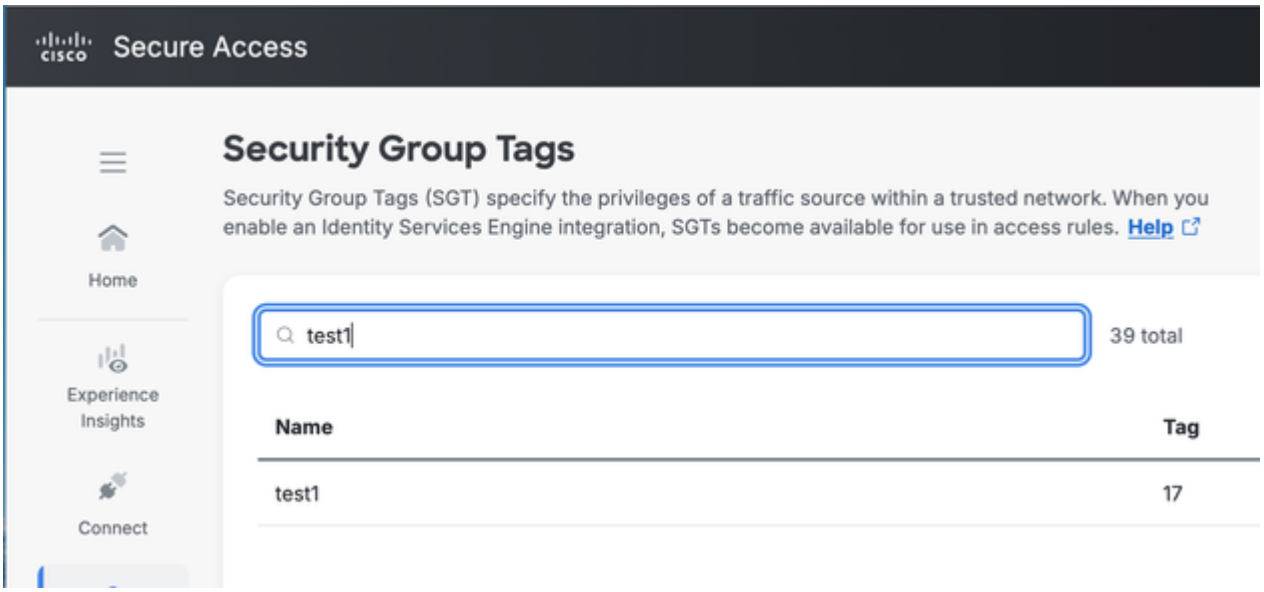
Onder Platform Management - Platform Integraties kunnen we de integratiestatus als actief zien



Verifieer de tag van de beveiligingsgroep:

Meld u aan bij Cisco Secure Access. Navigeer naar Bronnen - Tags beveiligingsgroep.


Secure Access
Home
Experience Insights
Connect
Resources
Secure
Monitor
Investigate
Admin
Resources
Sources and destinations
Internal Networks
Network Devices
Registered Networks
Roaming Devices
Service Account Exception
Security Group Tags
SDWAN Service VPN IDs
Network and Service Objects
Destinations
Internet and SaaS Resources
Private Resources
AI Resources
Application Portal
Settings
AAA Servers
DNS Servers
Enablement Schedule



Vereiste informatie voor Cisco TAC

ISE:
ISE-ondersteuningspakket verzamelen met de volgende onderdelen die zijn ingesteld op foutopsporingsniveau op de ISE-node met Pargrid Personna:

paragrid

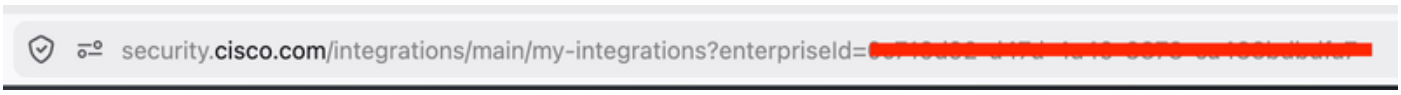
infrastructuur

ERS

Hermes-component op debugniveau.

SCC:

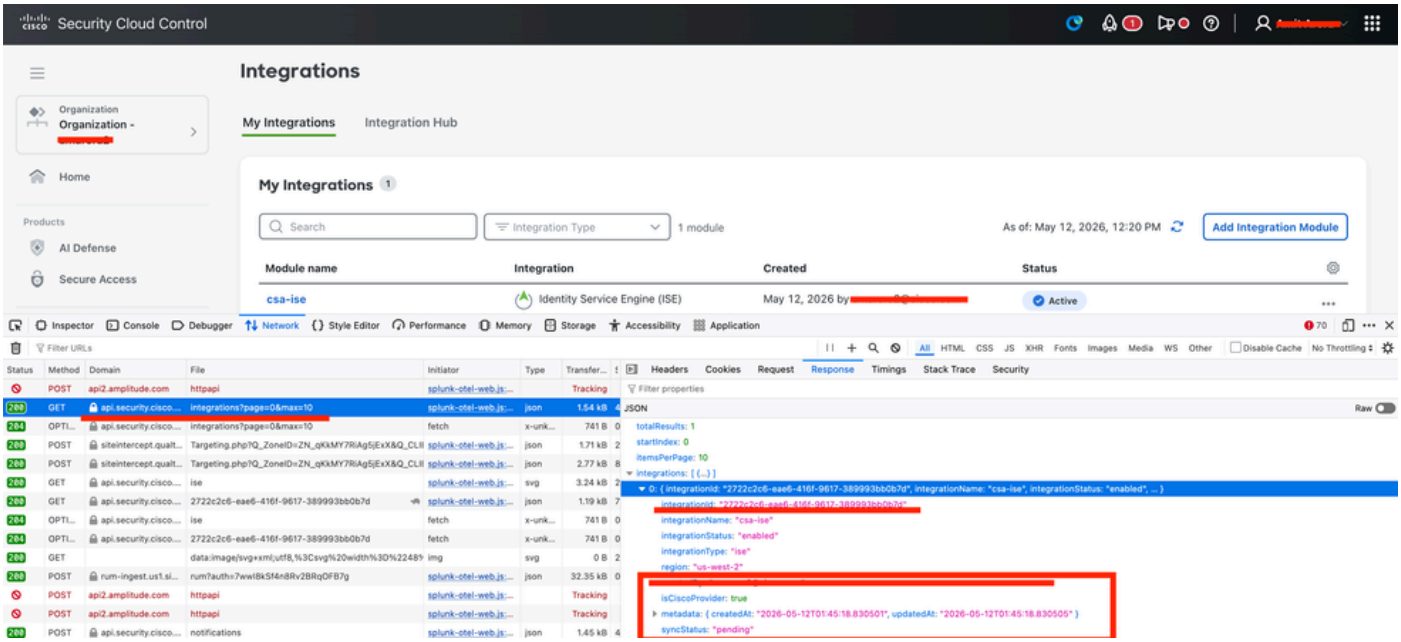
Enterprise ID: in de URL van security.cisco.com



Integratie-ID.
Start HAR Capture

Login op Security.cisco.com
Navigeer naar Platform Management - Platform Integraties

Zoeken naar integraties? pagina api oproep en in reactie tabblad vindt u een Integratie-ID.



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.