

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 privétoeepassingen 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 onpremise 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:

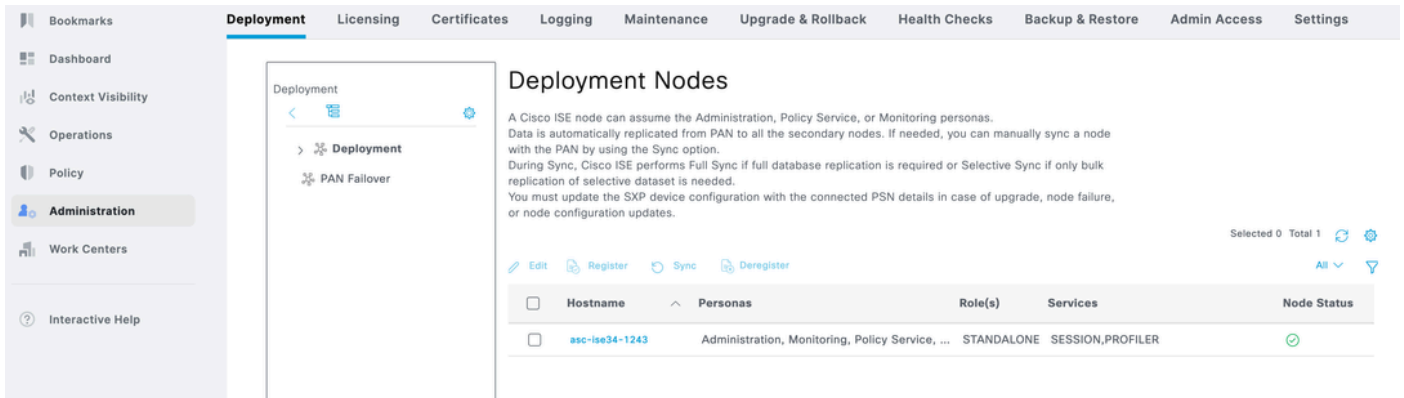
<https://dna.cisco.com>

<https://security.cisco.com/>

Stap 1: PxGrid Cloud inschakelen op ISE

1 Navigeer naar ISE GUI.

2 Klik op Beheer - Implementatie.

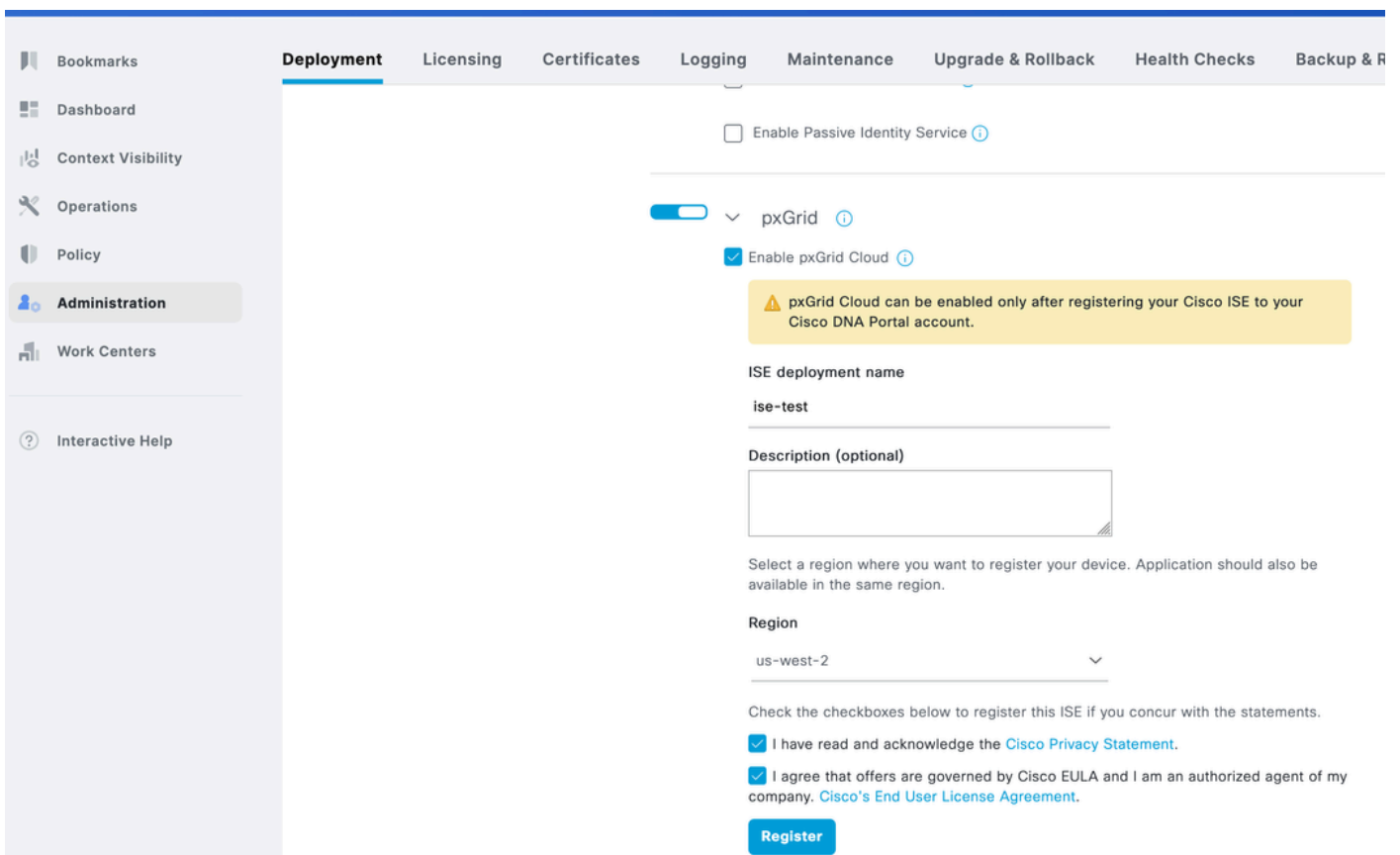


3 Klik op de Node en scroll naar beneden.

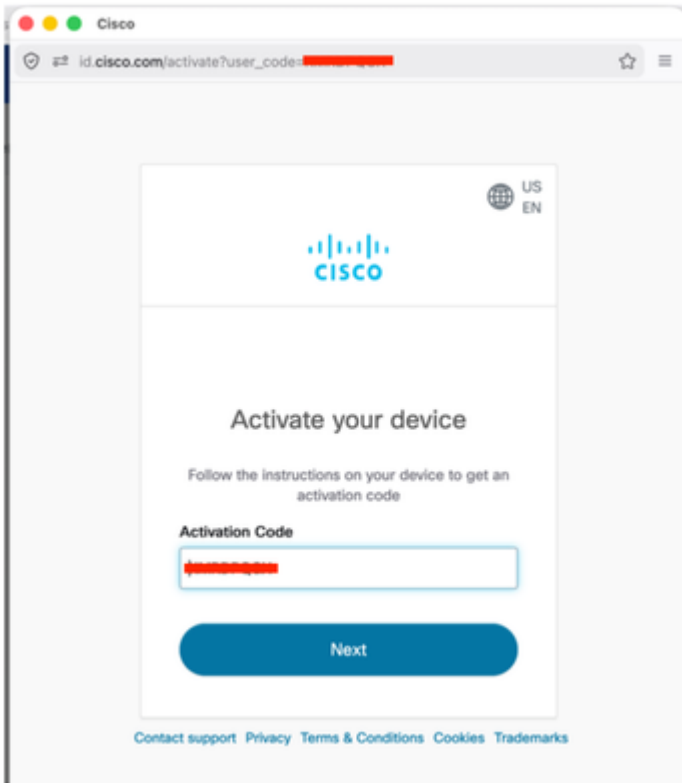
ISE-implementatienaam invoeren

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.

Administration / System

Deployment | Licensing | Certificates | Logging | Maintenance | Upgrade & Rollback | Health Checks

- Enable Profiling Service ⓘ
- Enable Threat Centric NAC Service ⓘ
- > Enable SXP Service ⓘ
- Enable Device Admin Service ⓘ
- Enable Passive Identity Service ⓘ

pxGrid ⓘ

- Enable pxGrid Cloud ⓘ

To enable pxGrid Cloud application, please go to the [Integration Catalog](#).

Cisco DNA Portal account	Status
[Redacted]	<input checked="" type="checkbox"/> Connected
ISE deployment name	Registered region
ise-test	us-west-2
Description	Mode
--	Active

[Deregister](#)

6 Klik op de link Integratiecatalogus van stap 5.

Klik onder Beschikbare integraties op Cisco Security Cloud

The screenshot displays the 'Integration Catalog' page in the Cisco Identity Services Engine (ISE) Administration console. The page title is 'Administration / Integration Catalog'. The left sidebar shows navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Help. The main content area is titled 'Integration Catalog' and features a section for 'Available integrations'. Five integration cards are visible:

- CIS (Cisco Security Cloud):** Includes tags for Network, Security, pxGrid Cloud, us-west-2, eu-central-1, and ap-southeast-1. Description: Cisco Security Cloud acts as an application broker which will allow ISE to integrate with the supported Cisco's cloud Security products through one single... More details
- FIR (Firewall Management Center):** Includes tags for Network, Security, pxGrid Cloud, us-west-2, eu-central-1, and ap-southeast-1. Description: Integrate with Firewall Management Center (FMC) to setup Identity Based Access Control in Cisco Secure Firewall. More details
- OFF (OfficeSpace Software Employee Presence):** Includes tags for network presence, pxGrid Cloud, and us-west-2. Description: Connects your OfficeSpace Software domain to pxGrid Cloud, allowing it to leverage employees authorizing to your network as indicators of presence to your sites... More details
- PXG (pxGrid Cloud Demo):** Includes tags for networking, pxGrid Cloud, us-west-2, eu-central-1, and ap-southeast-1. Description: Welcome to Cisco pxGrid Cloud's Demo Application! The purpose of this is to guide you through the setup process for connecting an application service and ISE... More details
- PXG (pxGrid Cloud Demo Multi-instance):** Includes tags for networking, demo, pxGrid Cloud, us-west-2, eu-central-1, and ap-southeast-1. Description: Welcome to Cisco pxGrid Cloud's Demo Application (Multi-instance)! The purpose of this is to guide you through the setup process for connecting an... More details

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

App configuration

Application status

Inactive

Instance (i)

Existing instances New instance

Data scope

Select at least 1 data scope for this application to consume.

- Adaptive Network Control (ANC) Configuration**
Provides ANC configuration details such as policy name, action type, status, and MAC address.
- Echo Service**
Provides a way for the app to check the health of the integration.
- Mobile Device Management (MDM)**
Provides endpoint details including model, manufacturer, type, compliance, and MAC address.
- Profiler Configuration**
Provides ISE profiling policy device details such as ID and name.
- RADIUS Authentication Failures**
Provides RADIUS protocol failure details such as failure reason, username, NAS NAD details, authentication details, framed IP address attributes, MAC address, and calling station ID.
- Session Directory**
Provides details on session and user group objects which include authenticated user context, wired and wireless connection type information, posture status, endpoint profile device, Security Group Tag (SGT), and username.
- TrustSec**
Covers TrustSec, TrustSec Configuration, and TrustSec SXP topics which include SGACL, SGT, and SGT binding information.

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


ding model manufacturer type compliance and MAC

One-time Password Generated

Log into your account on the App page and use this one-time password to add an instance.

[Authenticated with App account](#) 

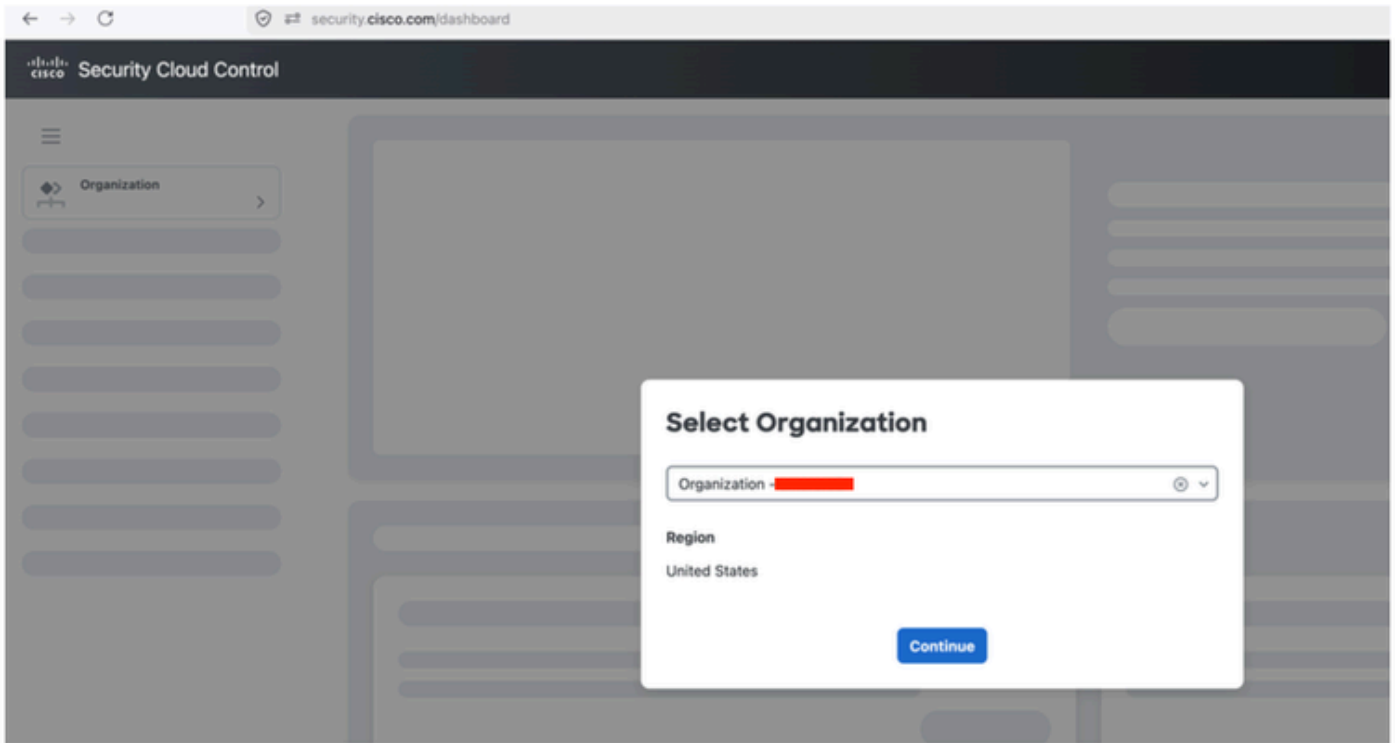
One-time password

  **Copy**

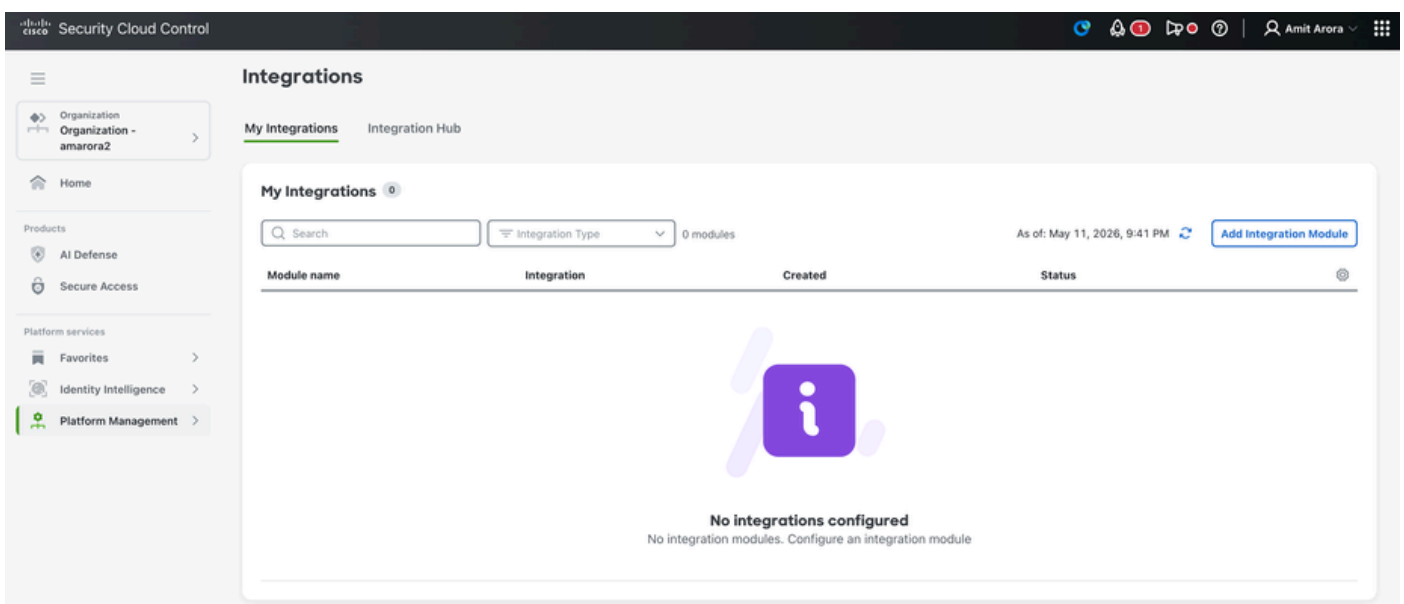
OK

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

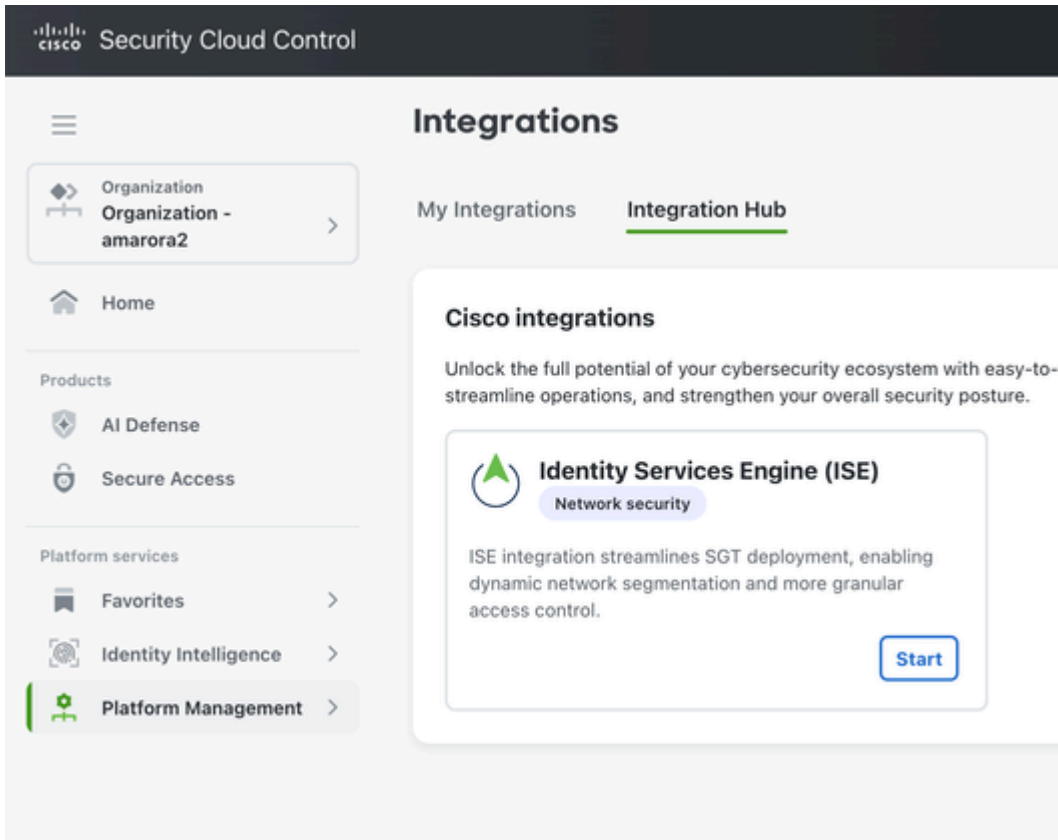


4 Klik op Integratiemodule toevoegen

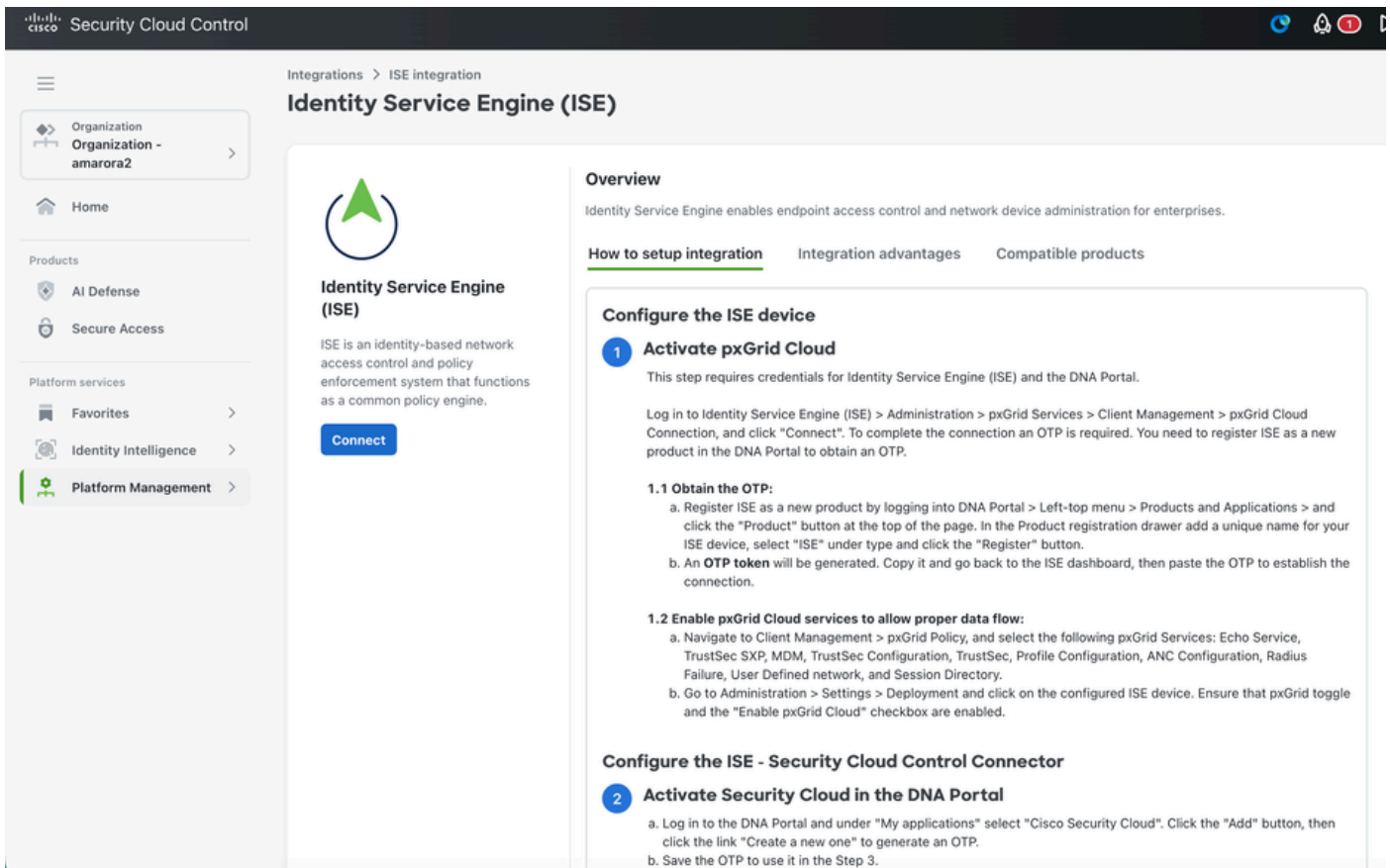


The screenshot shows the Cisco Security Cloud Control interface. The top navigation bar includes the Cisco logo and the text "Security Cloud Control". On the left, a sidebar menu contains a hamburger icon, a navigation item for "Organization - amarora2", a "Home" button, and sections for "Products" (AI Defense, Secure Access) and "Platform services" (Favorites, Identity Intelligence, Platform Management). The main content area is titled "Integrations" and has two tabs: "My Integrations" and "Integration Hub". Under "Integration Hub", there is a section for "Cisco integrations" with a descriptive paragraph. Below this, a card for "Identity Services Engine (ISE)" is displayed, featuring a green triangle icon, the category "Network security", a descriptive paragraph about SGT deployment, and a blue "Start" button.

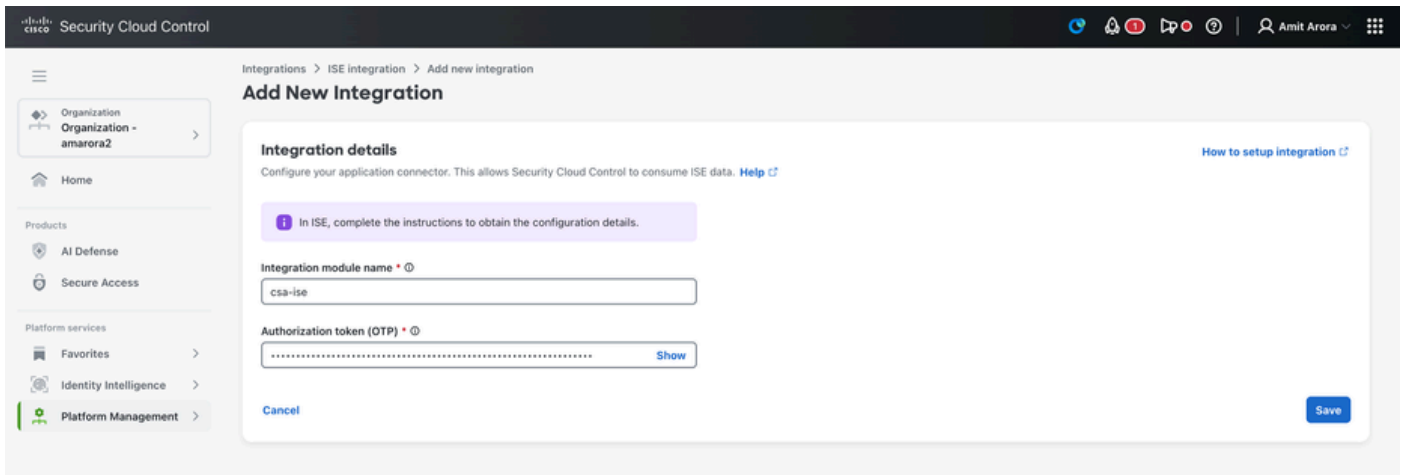
5 Klik op Start



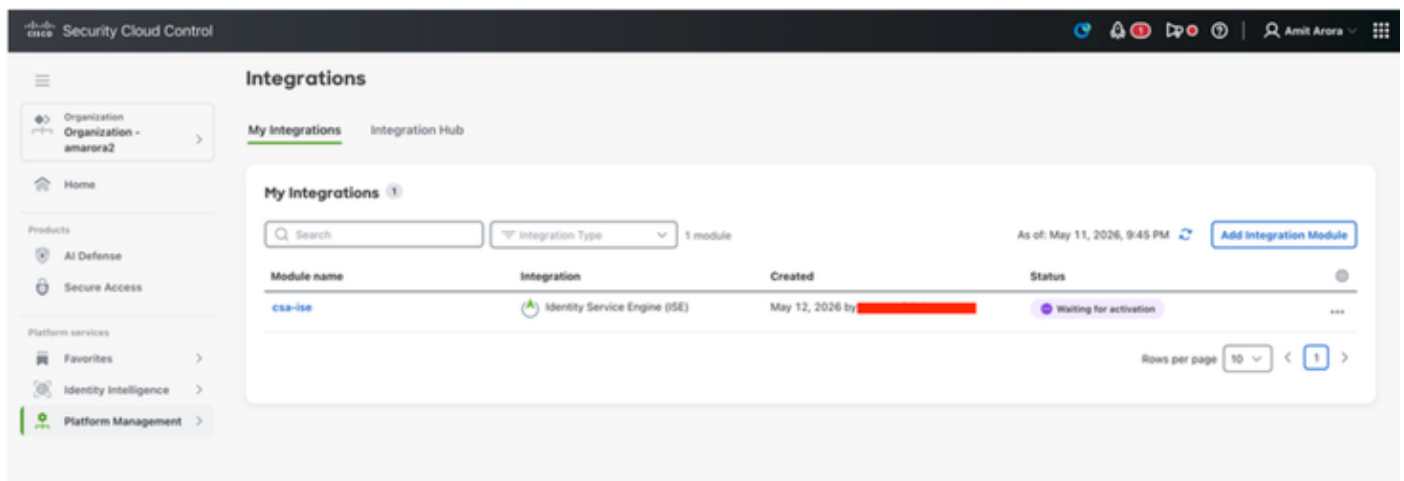
6 Klik op Verbinden



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 persona - 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

← Integration Catalog

Cisco Security Cloud

Network Security pxGrid Cloud us-west-2 eu-central-1 ap-southeast-1

Configuration About this integration

Registration

The integration of pxGrid Cloud will take place through your Cisco DNA Portal account where this ISE is registered. [Manage your ISE registration](#)

Cisco DNA Portal account	Status
[REDACTED]	Registered
Device name	Registered region
ise-test	us-west-2
Description	--

App configuration

Application status
 Inactive

Instance ⓘ

Existing instances New instance

Select instance ^

- ise-testnew
- csa-ise

Select at least 1 data scope for this application to consume.

Adaptive Network Control (ANC) Configuration
Provides ANC configuration details such as policy name, action type, status, and MAC address.

10 Toepassingsstatus is nu verbonden.

App configuration

Application status

Connected

Instance

csa-ise

Data scope

Select at least 1 data scope for this application to consume.

- Adaptive Network Control (ANC) Configuration**
Provides ANC configuration details such as policy name, action type, status, and MAC address.
- Echo Service**
Provides a way for the app to check the health of the integration.
- Mobile Device Management (MDM)**
Provides endpoint details including model, manufacturer, type, compliance, and MAC address.
- Profiler Configuration**
Provides ISE profiling policy device details such as ID and name.
- RADIUS Authentication Failures**
Provides RADIUS protocol failure details such as failure reason, username, NAS NAD details, authentication details, framed IP address attributes, MAC address, and calling station ID.
- Session Directory**
Provides details on session and user group objects which include authenticated user context, wired and wireless connection type information, posture status, endpoint profile device, Security Group Tag (SGT), and username.
- TrustSec**
Covers TrustSec, TrustSec Configuration, and TrustSec SXP topics which include SGACL, SGT, and SGT binding information.
- User Defined Networks (UDN)**
Allows a user to define their network.

Deactivate

Cisco Security Cloud x Activated
Cisco Security Cloud is activated successfully for ISE. To integrate with more Apps please go to the [Integration Catalog](#).

Integration Catalog

Activated integrations

Status	Logo	Integration	Type	Region	Provider
ON	CIS	Cisco Security Cloud	Network Security pxGrid Cloud	us-west-2 eu-central-1 ap-southeast-1	Cisco Security Business Group

Available integrations

- FIR Firewall Management Center**
Network Security pxGrid Cloud us-west-2 eu-central-1 ap-southeast-1
Integrate with Firewall Management Center (FMC) to setup Identity Based Access Control in Cisco Secure Firewall.
[More details](#)
- OFF OfficeSpace Software Employee Presence**
network presence pxGrid Cloud us-west-2
Connects your OfficeSpace Software domain to pxGrid Cloud, allowing it to leverage employees authorizing to your network as indicators of...
[More details](#)
- PXG pxGrid Cloud Demo**
networking pxGrid Cloud us-west-2 eu-central-1 ap-southeast-1
Welcome to Cisco pxGrid Cloud's Demo Application! The purpose of this is to guide you through the setup process for connecting an...
[More details](#)

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

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

Security Cloud Control

Organization - amarora2

Integrations

My Integrations Integration Hub

My Integrations 1

Search Integration Type 1 module

As of: May 11, 2026, 9:52 PM Add Integration Module

Module name	Integration	Created	Status
csa-ise	Identity Service Engine (ISE)	May 12, 2026 by	Active

Rows per page 10 < 1 >

Verifieer de tag van de beveiligingsgroep:

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



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

Secure Access

Security Group Tags

Security Group Tags (SGT) specify the privileges of a traffic source within a trusted network. When you enable an Identity Services Engine integration, SGTs become available for use in access rules. [Help](#)

test1 39 total

Name	Tag
test1	17

Vereiste informatie voor Cisco TAC

ISE:

[ISE-ondersteuningspakket verzamelen](#) met de volgende onderdelen die zijn ingesteld op foutopsporingsniveau op de ISE-node met Pargrid Persona:

paragrid

infrastructuur

ERS

Hermes-component op debugniveau.

SCC:

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

security.cisco.com/integrations/main/my-integrations?enterpriseld=

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.