

Intégration de Cisco Secure Access avec ISE pour le marquage de groupe de sécurité sur le cloud Pxgrid

Table des matières

Introduction

Ce document décrit comment activer le partage de contexte entre Cisco Secure Access et Cisco Identity Services Engine

Exigences

Cisco vous recommande de connaître les sujets suivants :

- Cisco Secure Access : solution de périphérie de services de sécurité (SSE) basée sur le cloud qui fournit un accès réseau sans confiance pour permettre aux utilisateurs de se connecter facilement à Internet et à des applications privées depuis n'importe quel périphérique.
- Cisco Identity Service Engine (ISE) version 3.4, correctif 5.
- Cisco Security Cloud Control : une solution de gestion unifiée pour vos produits et votre identité Security Cloud. Le contrôle du cloud de sécurité est inclus dans Secure Access.

Fond

Cette intégration permet la création automatisée de tunnels fiables entre les filiales SD-WAN de Catalyst et Cisco Secure Access, facilitant ainsi l'échange transparent d'ID/nom VPN et de contexte SGT.

Cisco Identity Services Engine (ISE) reste l'autorité centrale pour la configuration et la gestion des balises de groupe de sécurité. Toutes les mises à jour effectuées dans ISE sont automatiquement synchronisées avec Cisco Secure Access. Si une SGT est supprimée, les règles existantes qui la référencent restent actives pour s'assurer que la correspondance du trafic se poursuit comme prévu.

Nous offrons actuellement une disponibilité limitée pour les mappages SGT, ce qui étend la prise en charge pour inclure les objets de destination SGT dans vos règles de sécurité. En outre, la prise en charge de la construction de tunnels SASE transportant les balises SGT de Meraki et de Cisco Secure Firewall est prévue prochainement

Scénario:

Politique basée sur l'espace de noms SGT :

En tant qu'administrateur de sécurité, Kit souhaite appliquer une microsegmentation contiguë à l'aide de SGT provenant d'ISE sur site pour le trafic privé SSE et le trafic lié à Internet. Possibilité d'importer des SGT pour appliquer des politiques.



Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Identity Service Engine (ISE) version 3.4, correctif 5
- Accès sécurisé
- Cloud de sécurité Cisco

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Présentation de la configuration du partage de contexte

- Connectez ISE à Cisco Security Cloud
- Connexion de Cisco Secure Access à ISE

Configurer

Ce guide répartit la configuration globale en plusieurs étapes principales :

1. Connectez Cisco ISE à Cisco Security Cloud
2. Connexion de Cisco Accès sécurisé à Cisco ISE
3. Balises de groupe de sécurité dans Cisco Secure Access

Avant de commencer

- Vérifiez que vous avez installé et activé la licence Advantage dans votre déploiement Cisco ISE.
- L'agent DNA Cloud crée une connexion HTTPS sortante vers Cisco DNA Cloud. Par conséquent, vous devez configurer les paramètres du proxy Cisco ISE si votre réseau utilise un proxy pour accéder à Internet. Pour configurer les paramètres de proxy dans Cisco ISE, accédez à **Administration > System > Settings > Proxy**
- Assurez-vous que le port 443 est ouvert pour la connexion sortante de Cisco ISE vers le portail Cisco pxGrid Cloud. Si des paramètres de pare-feu ou de proxy sont configurés, assurez-vous que les URL suivantes ne sont pas bloquées :

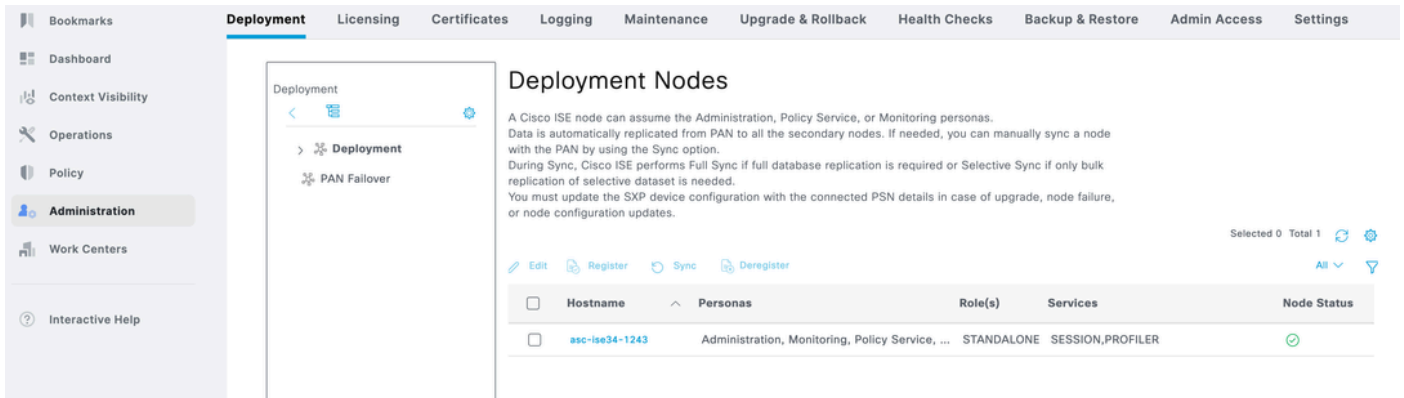
<https://dna.cisco.com>

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

Étape 1 :Activez le cloud Pxgrid sur ISE

1 Accédez à l'interface utilisateur graphique ISE.

2 Cliquez sur Administration - Deployment.

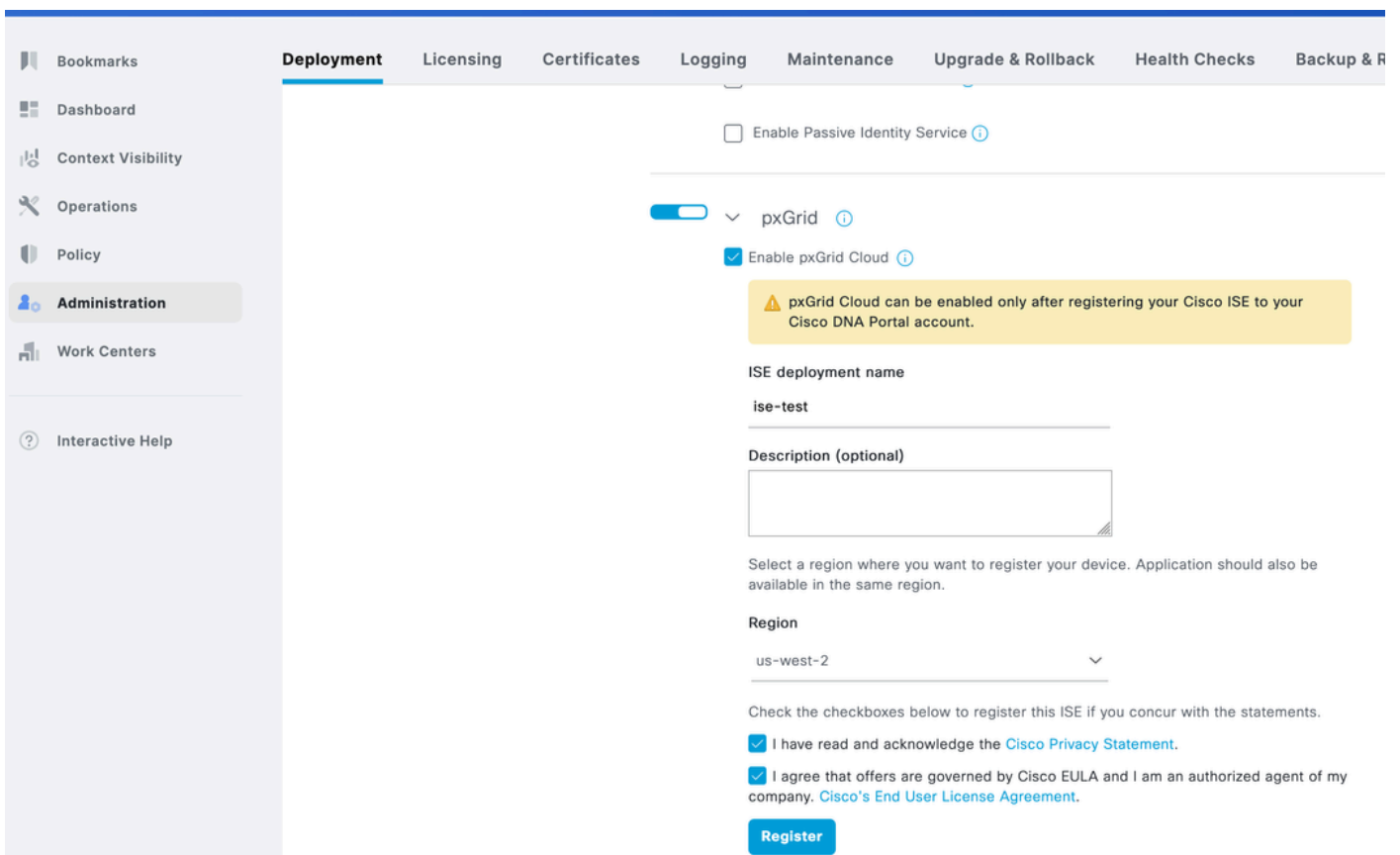


3 Cliquez sur le noeud et faites défiler la page vers le bas.

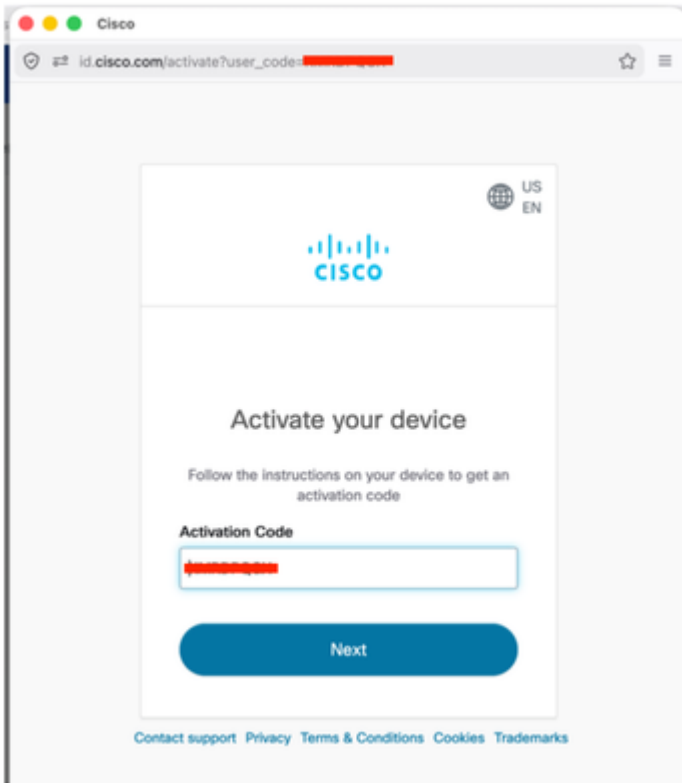
Saisissez le nom du déploiement ISE

Sélectionnez la région US West 2 qui est la seule région prise en charge à ce jour.

Cochez les deux cases et cliquez sur Register.



4 Une fenêtre contextuelle contenant le code d'activation rempli automatiquement s'affiche. Cliquez sur Next (Suivant),



5 ISE indique connecté au cloud Pxgrid.

Identity Services Engine 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
	<input checked="" type="checkbox"/> Connected
ISE deployment name	Registered region
ise-test	us-west-2
Description	Mode
--	Active

[Deregister](#)

6 Cliquez sur le lien Catalogue d'intégration à l'étape 5.

Sous Available Integrations - Cliquez sur Cisco Security Cloud

The screenshot shows the 'Integration Catalog' page in the Cisco Identity Services Engine Administration console. The page title is 'Administration / Integration Catalog'. The left sidebar contains 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 displayed:

- 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 link is present.
- 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 link is present.
- 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 link is present.
- 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 link is present.
- 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 link is present.

7 Sous App Configuration, cliquez sur New Instance, puis sur 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.

Copiez le mot de passe unique tel qu'il sera utilisé sur 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](#) ↗

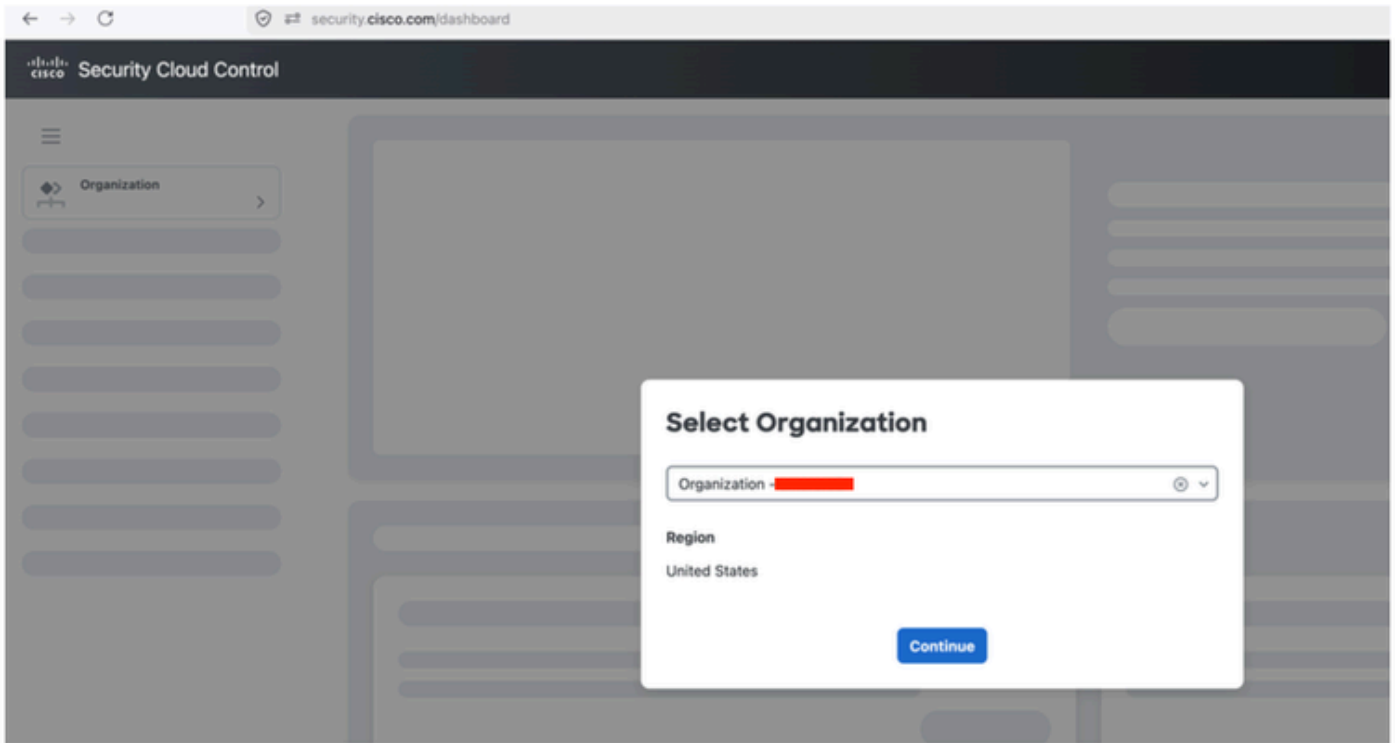
One-time password

[Redacted] [Copy](#)

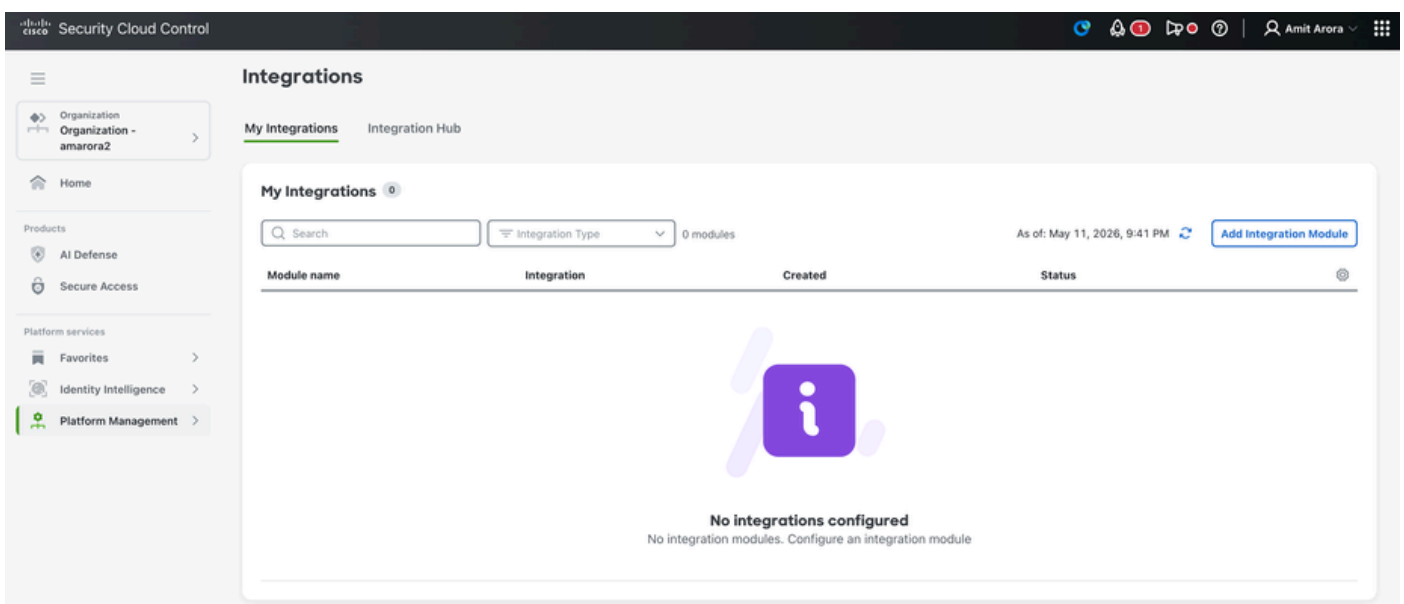
[OK](#)

Étape2: Intégrer Cisco Secure Access à ISE

1. Connectez-vous à security.cisco.com.
2. Sélectionnez l'ORG Cisco Secure Access



3 Cliquez sur Platform Management - Platform Integrations



4 Cliquez sur Add Integration Module

The screenshot displays 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, an "Organization" section with "Organization - amarora2", a "Home" button, a "Products" section with "AI Defense" and "Secure Access", and a "Platform services" section with "Favorites", "Identity Intelligence", and "Platform Management". The main content area is titled "Integrations" and has two tabs: "My Integrations" and "Integration Hub". Under "Integration Hub", there is a "Cisco integrations" section with a descriptive paragraph. Below this is a card for "Identity Services Engine (ISE)" with a "Network security" tag, a description of its benefits, and a "Start" button.

Organization
Organization - amarora2

Home

Products

- AI Defense
- Secure Access

Platform services


- Favorites
- Identity Intelligence
- Platform Management

Integrations

My Integrations Integration Hub

Cisco integrations

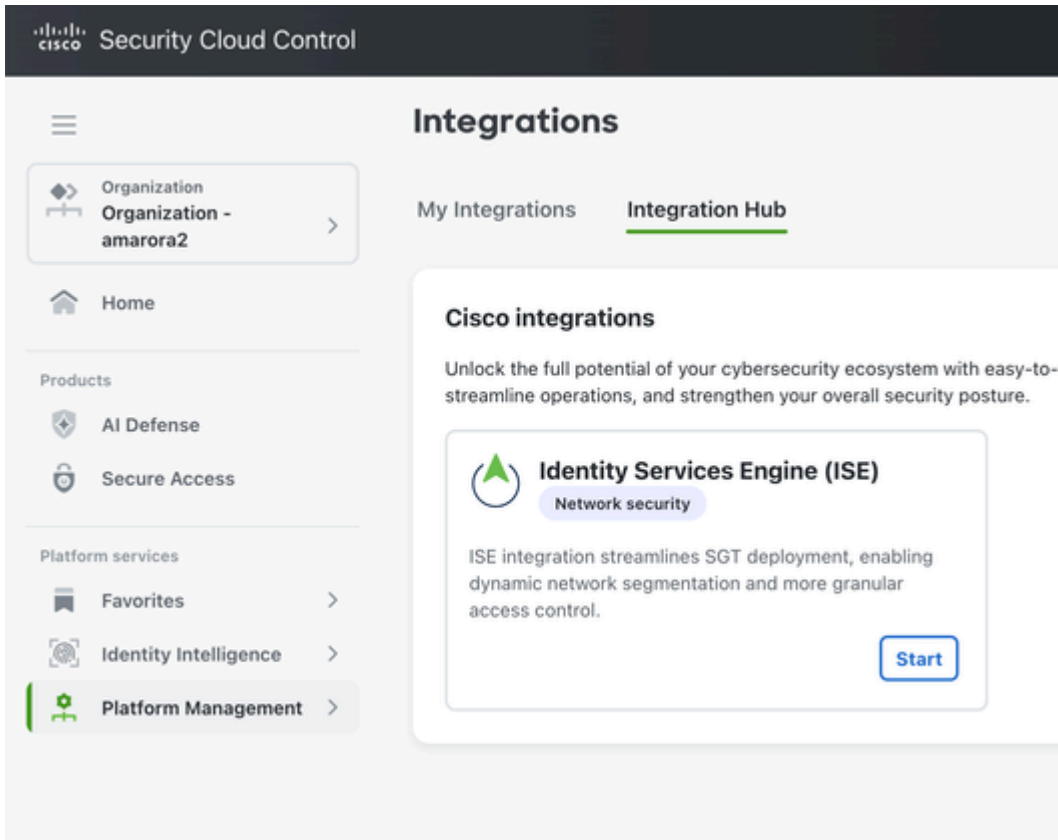
Unlock the full potential of your cybersecurity ecosystem with easy-to-use integ streamline operations, and strengthen your overall security posture.

 **Identity Services Engine (ISE)**
Network security

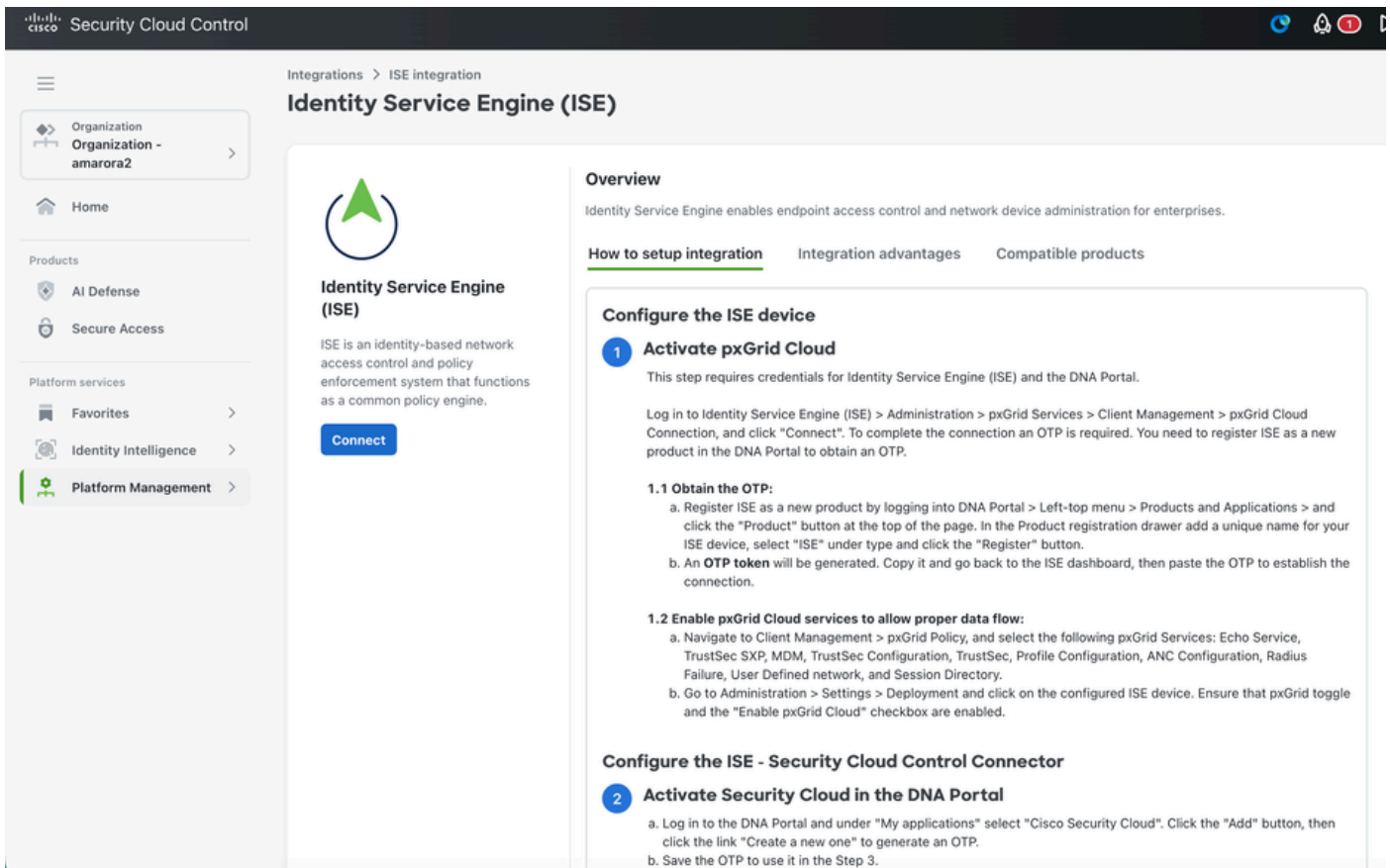
ISE integration streamlines SGT deployment, enabling dynamic network segmentation and more granular access control.

[Start](#)

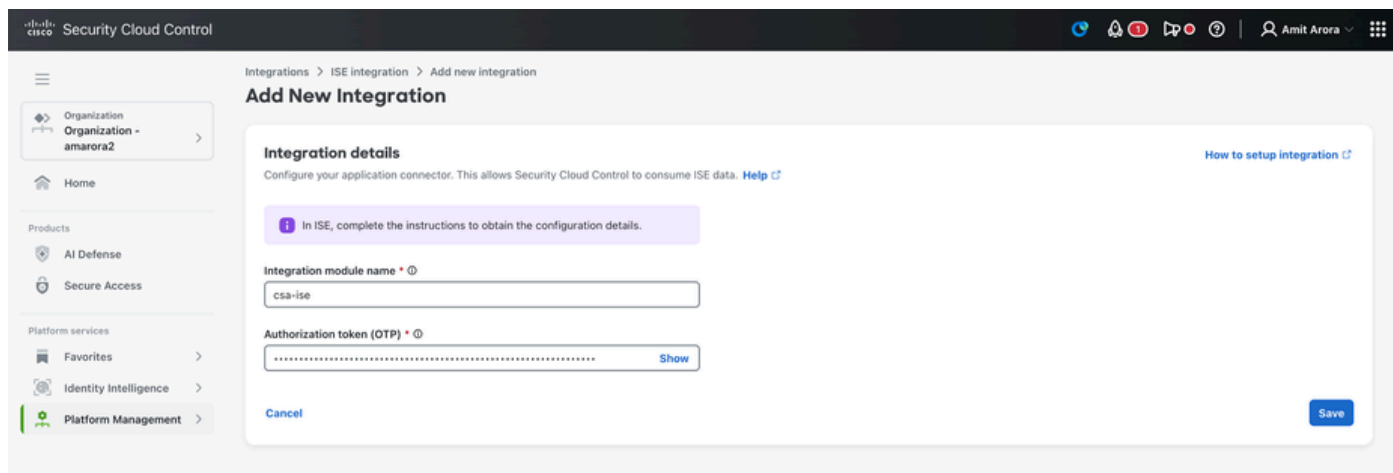
5 Cliquez sur Démarrer



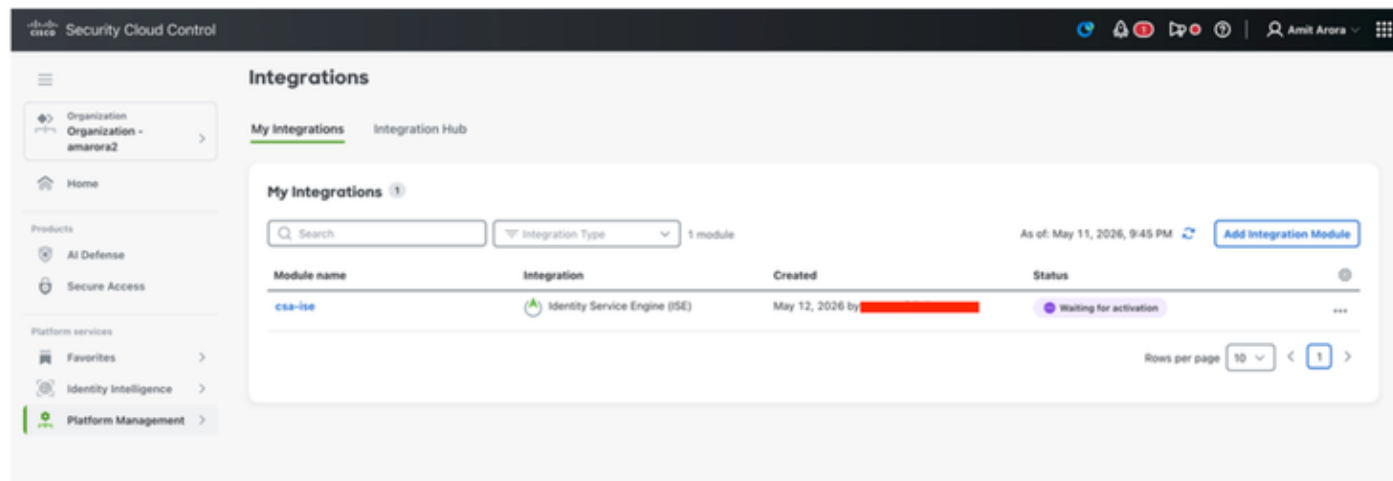
6 Cliquez sur Connect



7. Saisissez le nom du module d'intégration et le mot de passe à usage unique de Cisco ISE, puis cliquez sur Enregistrer



8 Une fois que vous avez cliqué sur Save, le message Waiting for Activation Status s'affiche.



9 Connectez-vous à ISE et accédez à Administration - Deployment. Cliquez sur le noeud avec pxgrid persona - cliquez sur le nuage d'intégration sous Pxgrid Connection.

Sous App configuration - sélectionnez l'instance ISE créée dans Security Cloud Control et cliquez

sur Activate

The screenshot displays the Cisco Security Cloud interface. On the left is a navigation sidebar with options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (highlighted), Work Centers, and Interactive Help. The main header shows 'Integration Catalog' and 'Cisco Security Cloud' with tabs for Network, Security, pxGrid Cloud, us-west-2, eu-central-1, and ap-southeast-1. Below the header, there are two main sections:

- Registration:** This section explains that integration with pxGrid Cloud occurs through a Cisco DNA Portal account. It includes a link to 'Manage your ISE registration'. Below this, a table lists registration details:

Cisco DNA Portal account	Status
[Redacted]	Registered
Device name	Registered region
ise-test	us-west-2
Description	--
- App configuration:** This section shows the application status as 'Inactive'. It allows selecting an instance from a dropdown menu, with options for 'Existing instances' (selected) and 'New instance'. The dropdown menu is open, showing 'ise-testnew' and 'csa-ise'. Below the dropdown, there is a note: 'Select at least 1 data scope for this application to consume.' and a checked checkbox for 'Adaptive Network Control (ANC) Configuration', which provides details on policy name, action type, status, and MAC address.

10 L'état de l'application est maintenant connecté.

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](#)
- PXC** **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 Connexion au contrôle du cloud de sécurité - security.cisco.com

Sous Platform Management - Platform Integrations, nous pouvons voir l'état de l'intégration comme Actif

Security Cloud Control

Organization - amarora2

Home

Products

- AI Defense
- Secure Access

Platform services

- Favorites
- Identity Intelligence
- Platform Management

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 >

Vérifier la balise du groupe de sécurité :

Connectez-vous à Cisco Secure Access. Accédez à Ressources - Balises du groupe de sécurité.



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

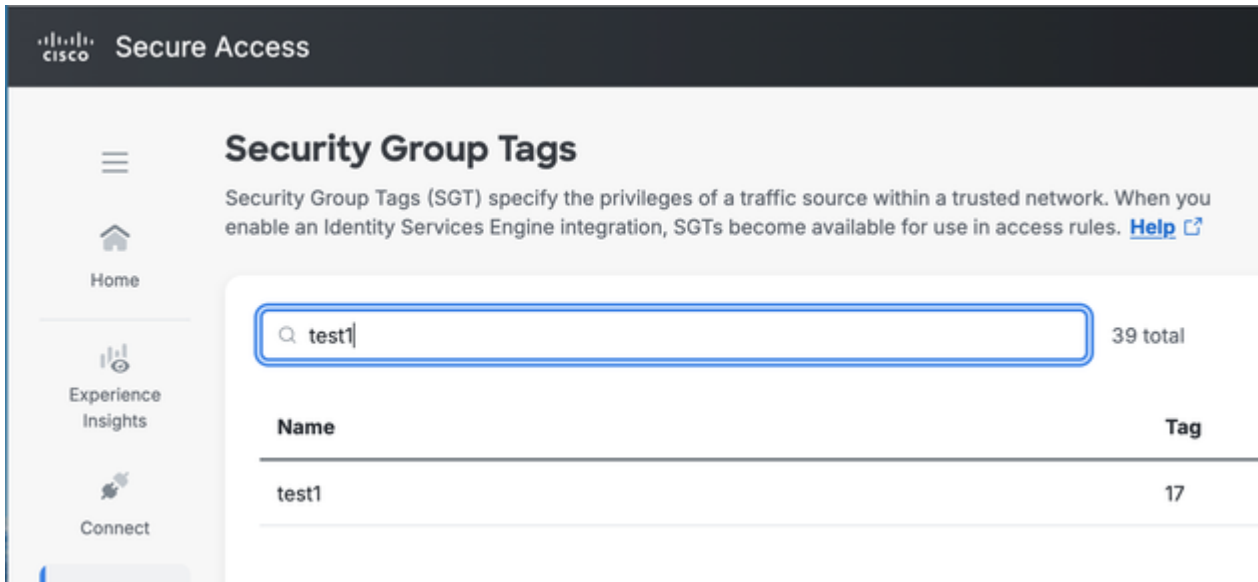
Application Portal

Settings

AAA Servers

DNS Servers

Enablement Schedule



Informations requises pour le centre d'assistance technique Cisco

ISE:

[Comment collecter le bundle d'assistance ISE](#) avec les composants suivants définis sur le niveau de débogage sur le noeud ISE avec Pxgrid Persona :

grille pxgrid

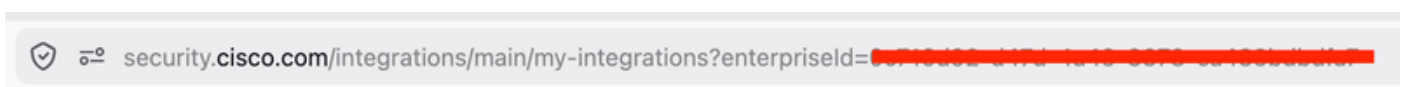
Infrastructure

ERS

composant hermes au niveau du débogage.

SCC :

ID d'entreprise : dans l'URL de security.cisco.com



ID d'intégration

Démarrer la [capture HAR](#)

Connectez-vous à Security.cisco.com
Accédez à Gestion des plates-formes - Intégrations des plates-formes

Recherchez l'appel de l'API de la page des intégrations et, dans l'onglet Réponse, vous trouverez un ID d'intégration.

The screenshot shows the Cisco Security Cloud Control interface. The main content area is titled "Integrations" and displays a table of "My Integrations". The table has columns for "Module name", "Integration", "Created", and "Status". One integration is listed: "csc-ise" (Identity Service Engine (ISE)), created on May 12, 2026, and is "Active".

Below the table, the network inspector shows a GET request to "api2.amplitude.com" with a response containing JSON data. The response data includes an integration ID: "2722c2c6-ee6e-416f-9617-389993b0b7d" and other details like "integrationName: 'csc-ise'", "integrationStatus: 'enabled'", and "syncStatus: 'pending'".

Module name	Integration	Created	Status
csc-ise	Identity Service Engine (ISE)	May 12, 2026 by [redacted]	Active

```
{
  "totalResults": 1,
  "startIndex": 0,
  "itemsPerPage": 10,
  "integrations": [
    {
      "integrationId": "2722c2c6-ee6e-416f-9617-389993b0b7d",
      "integrationName": "csc-ise",
      "integrationStatus": "enabled",
      "integrationType": "ise",
      "region": "us-west-2",
      "isCiscoProvider": true,
      "metadata": {
        "createdAt": "2026-05-12T01:45:18.830501",
        "updatedAt": "2026-05-12T01:45:18.830505"
      },
      "syncStatus": "pending"
    }
  ]
}
```

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.