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 :

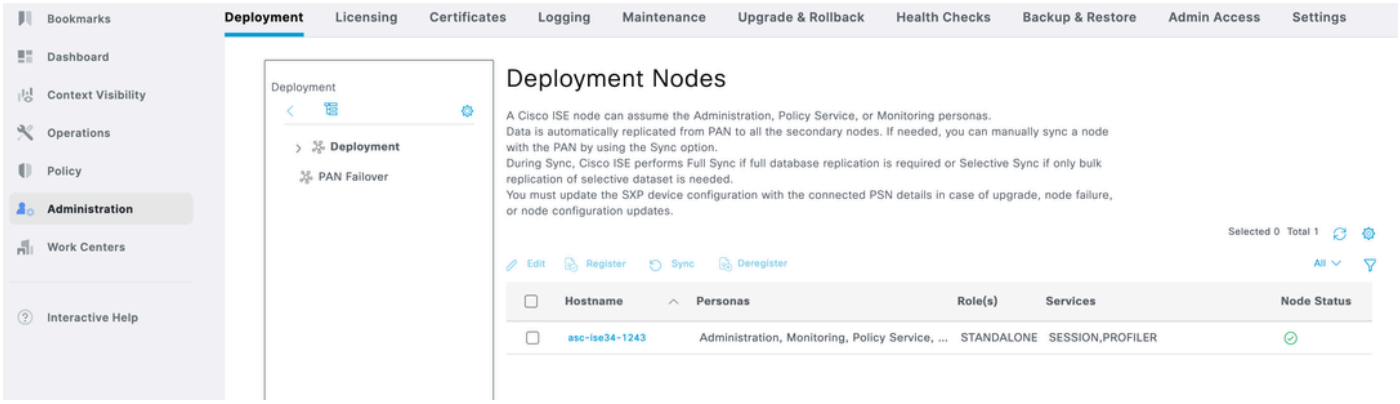
https://dna.cisco.com

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.

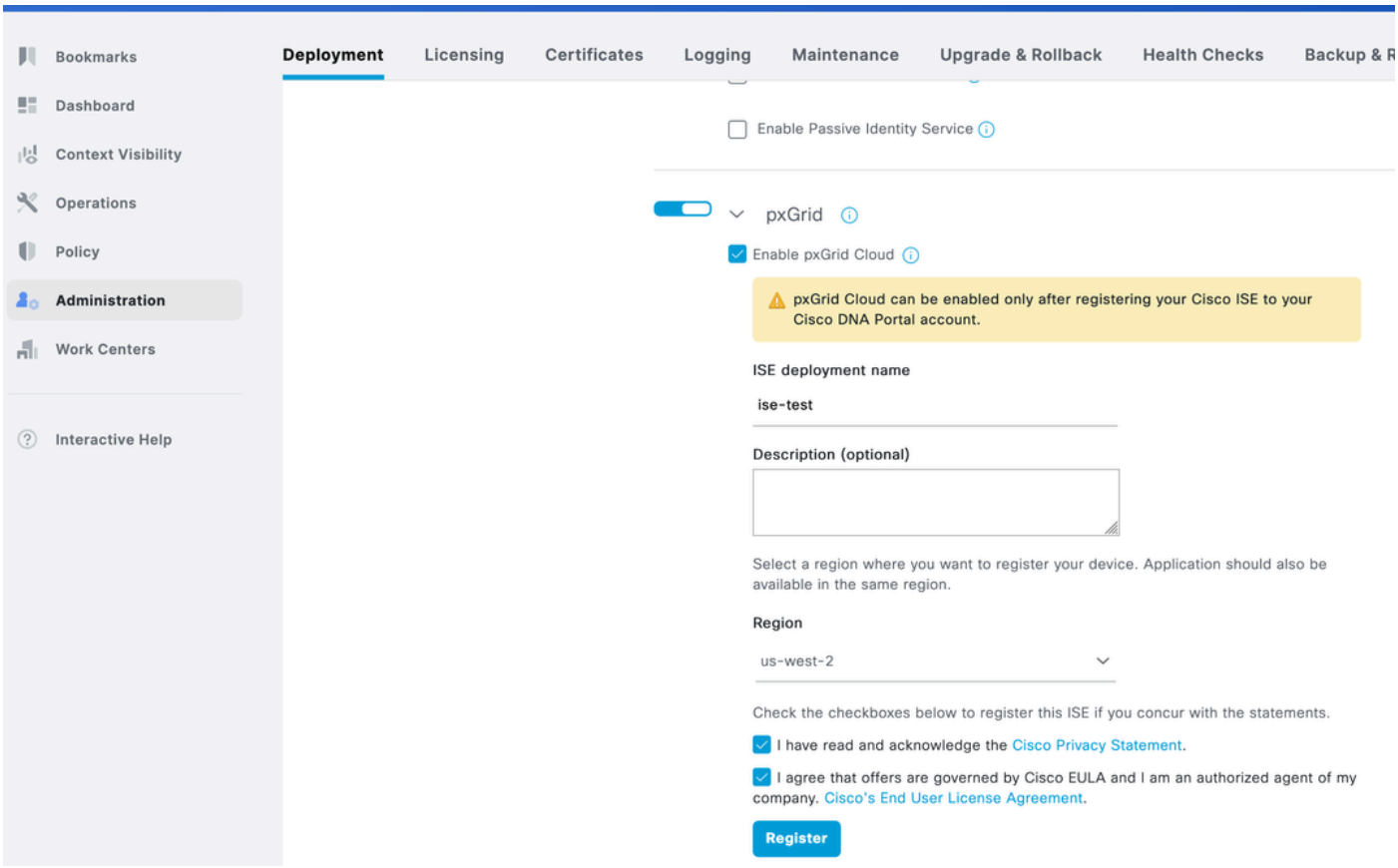


3 Cliquez sur le noeud et faites défiler la page vers le bas.

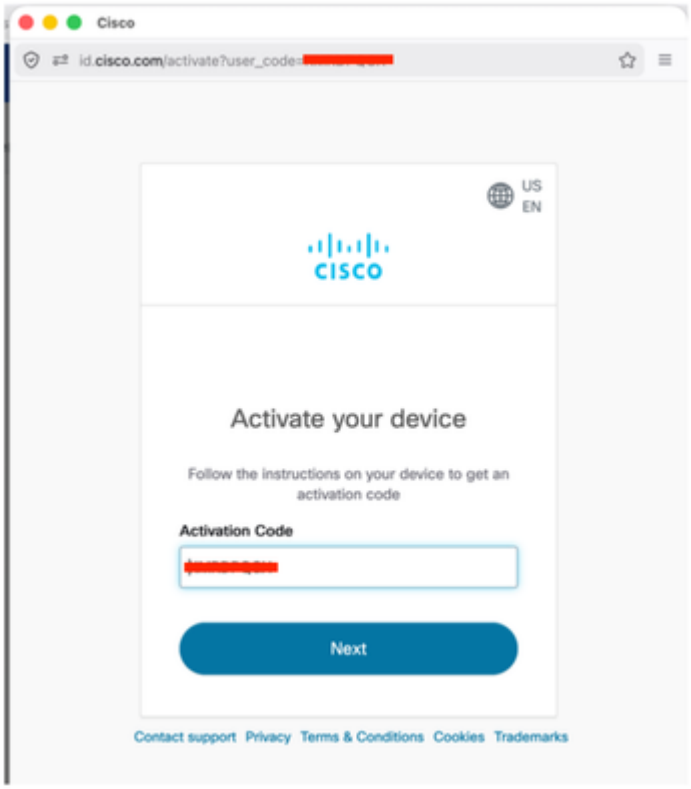
Saisissez le nom du déploiement ISE

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

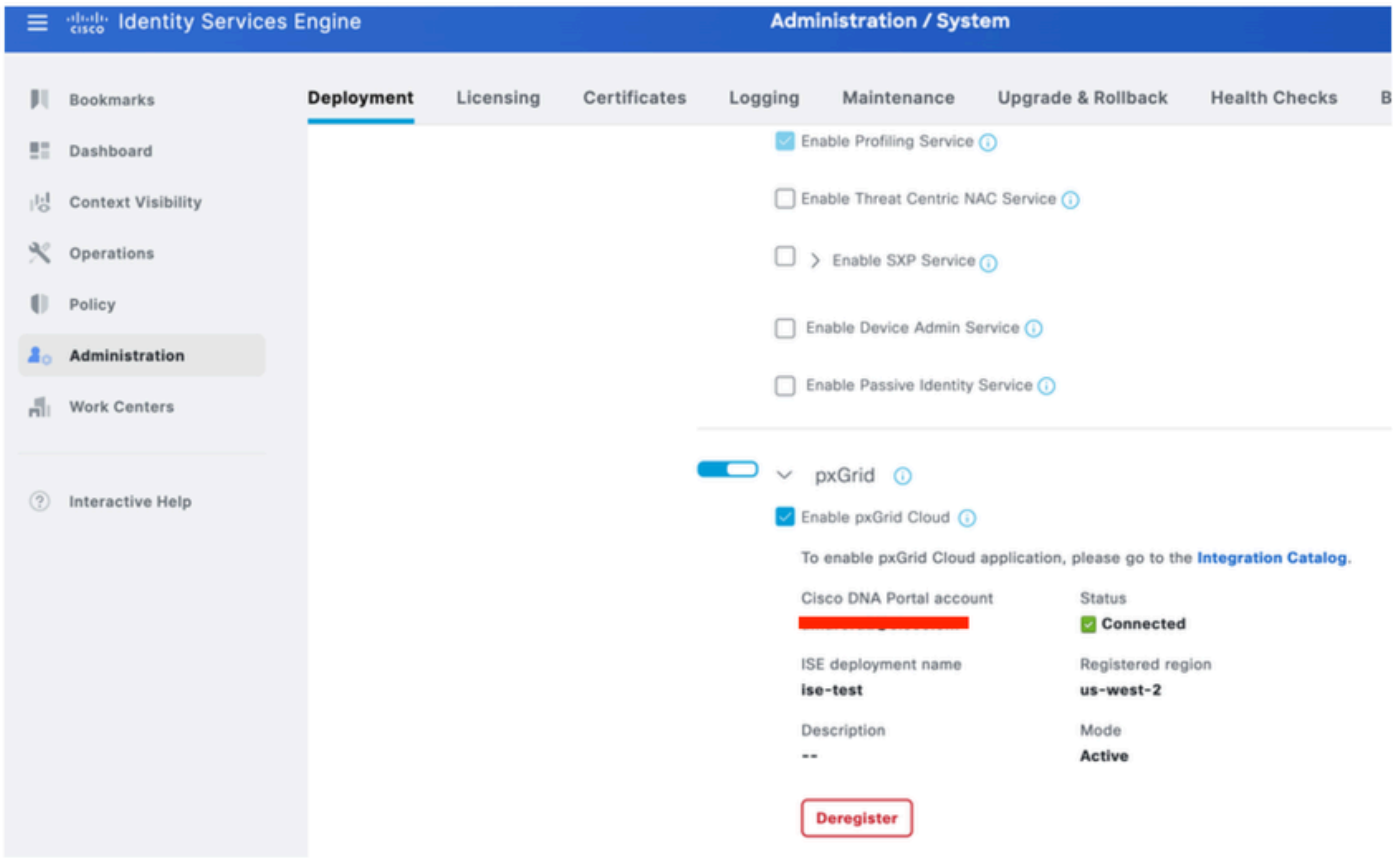
Cochez les deux cases et cliquez sur Register.



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



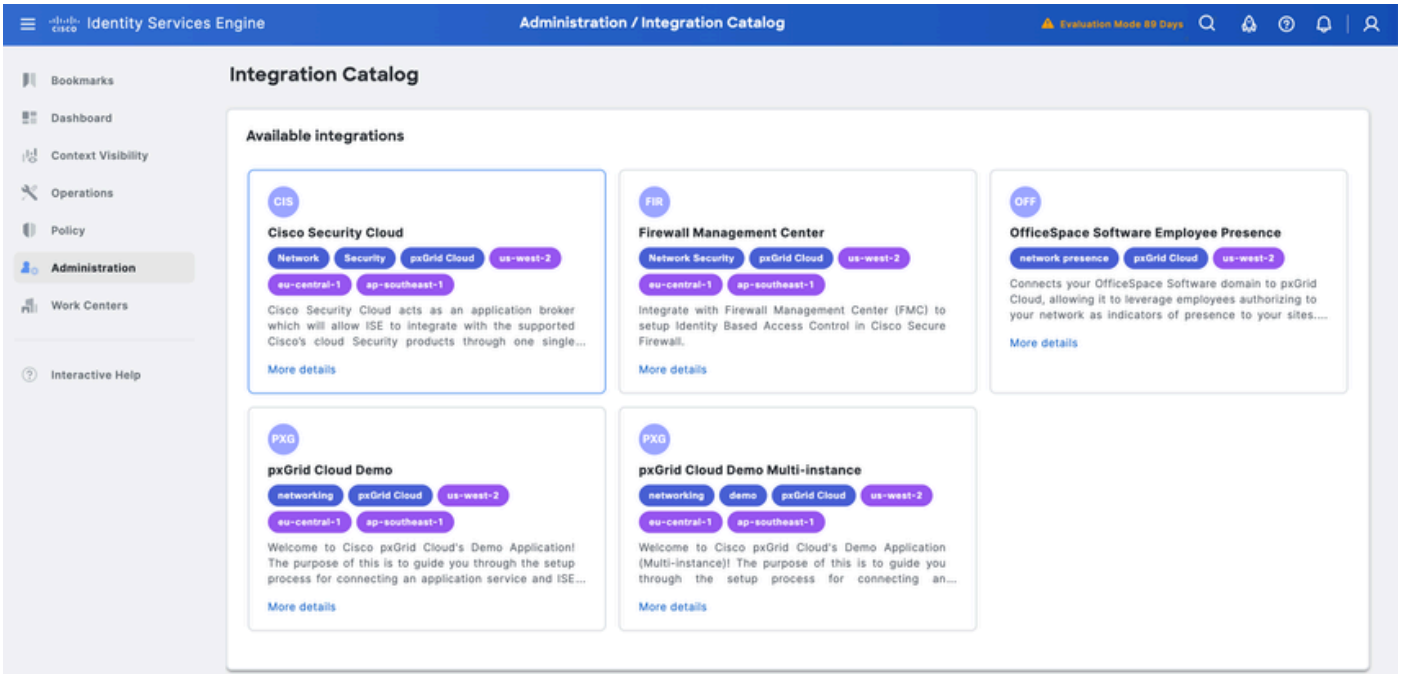
5 ISE indique connecté au cloud Pxgrid.



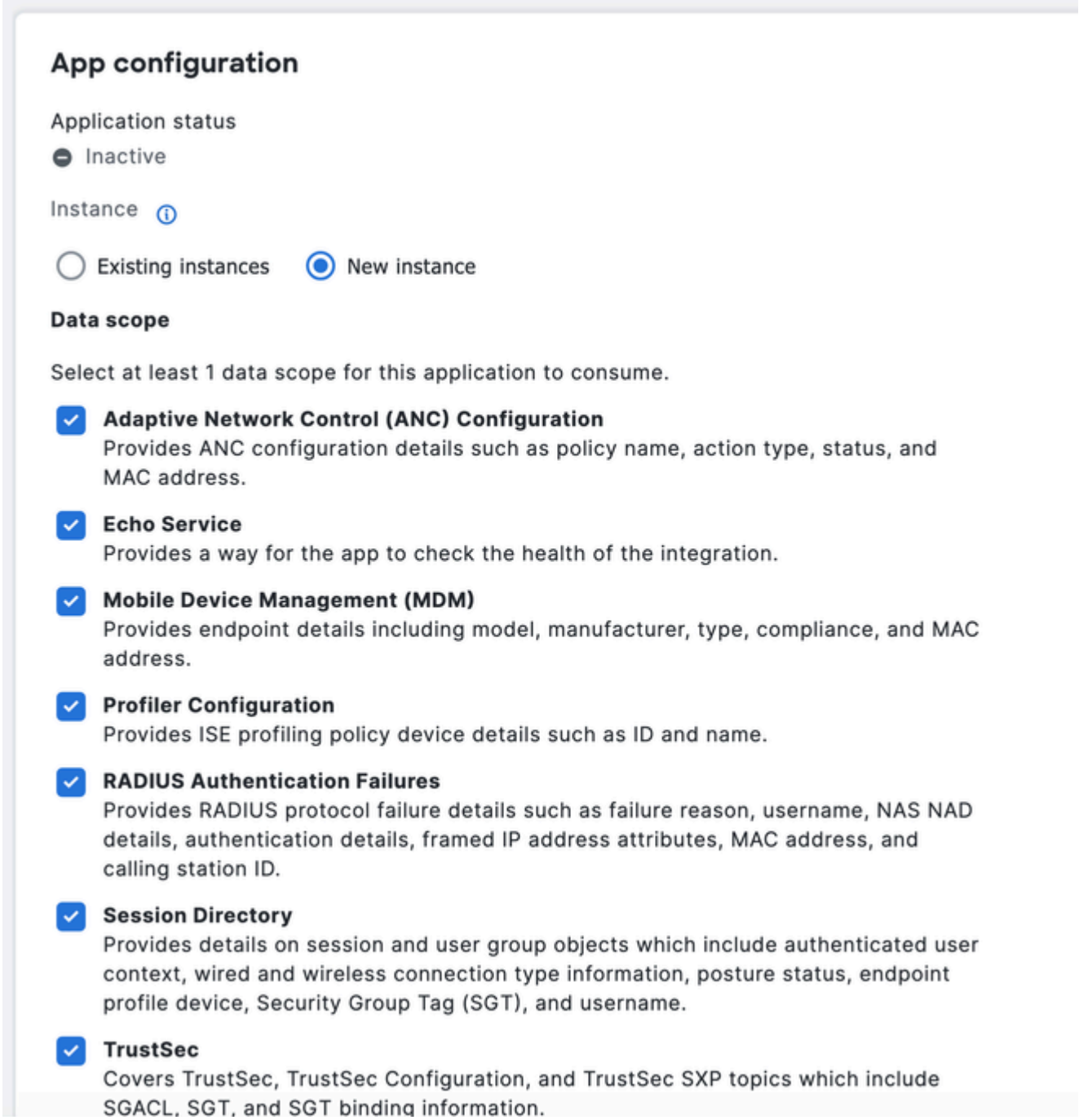
6 Cliquez sur le lien Catalogue d'intégration à l'étape 5.

Sous Available Integrations - Cliquez sur Cisco Security Cloud

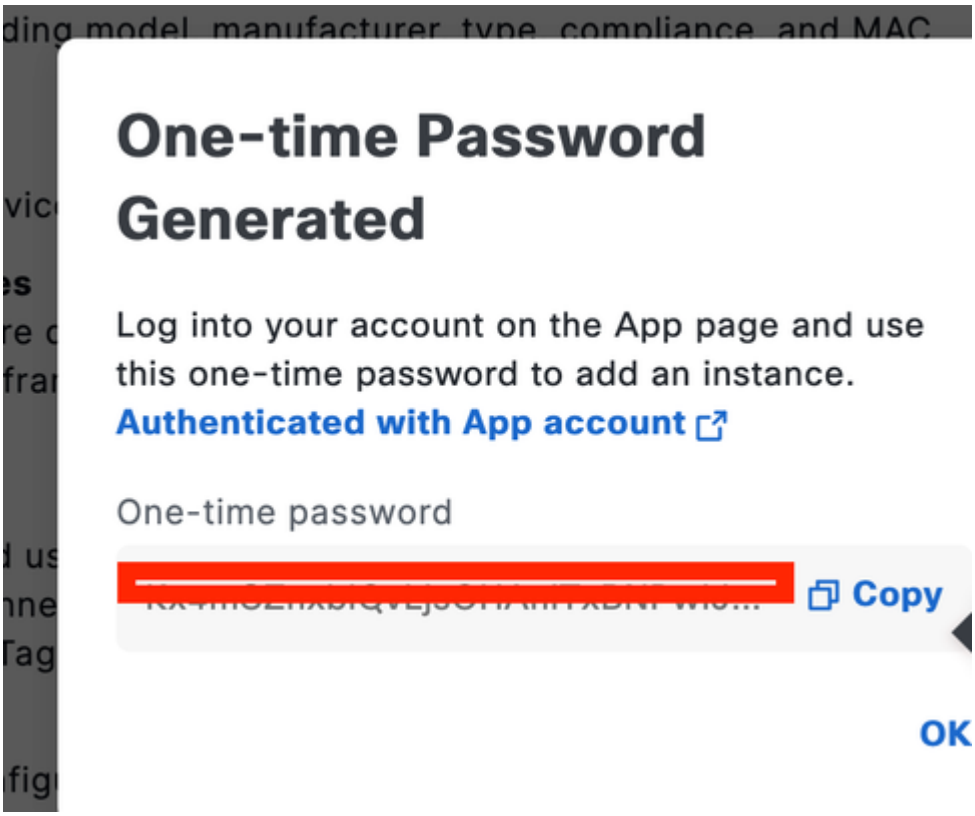
.



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

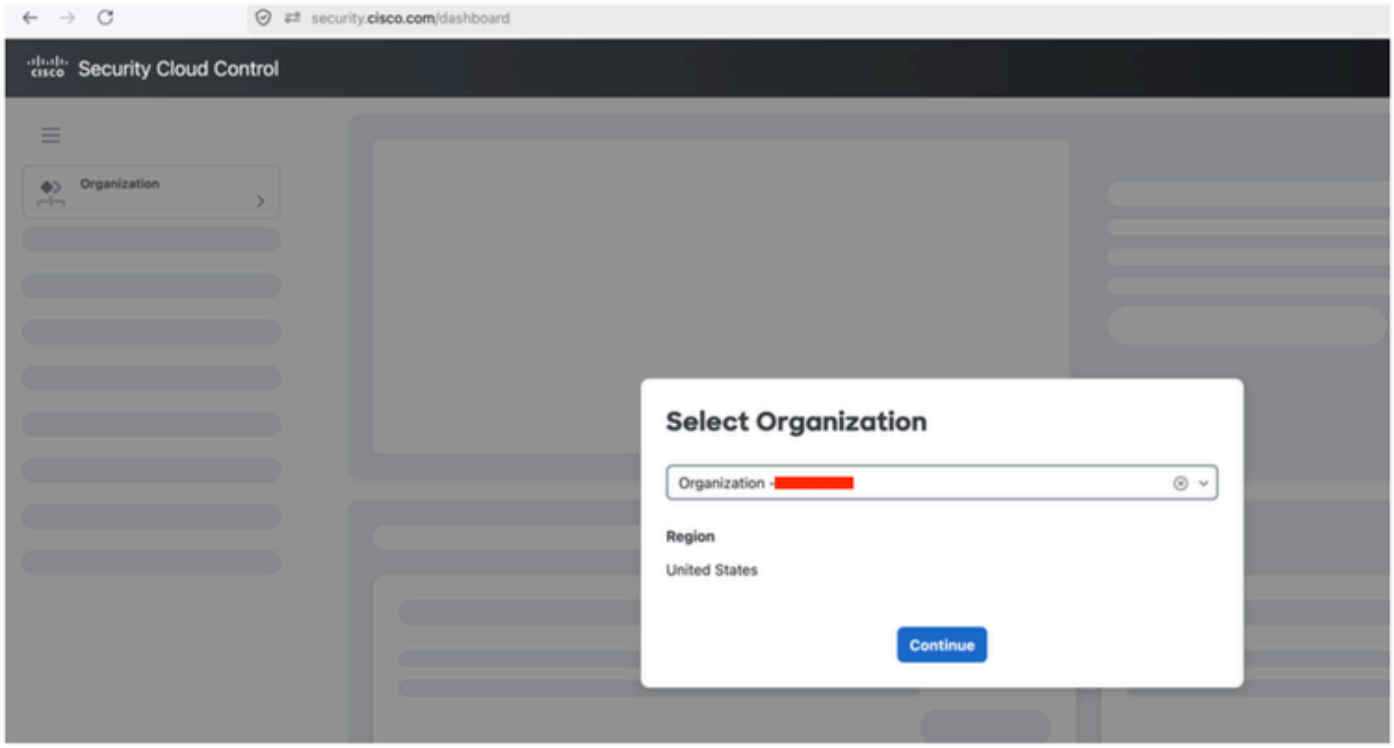


Copiez le mot de passe unique tel qu'il sera utilisé sur Cisco Secure Access.

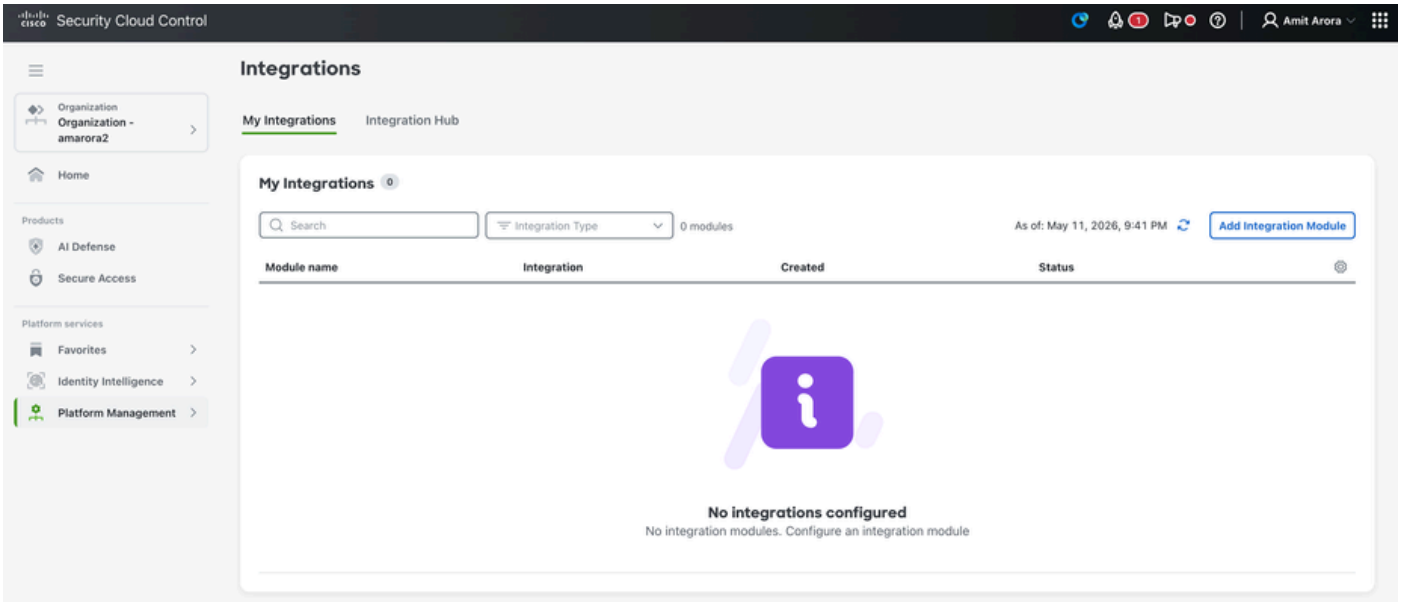


Étape2: Intégrer Cisco Secure Access à ISE

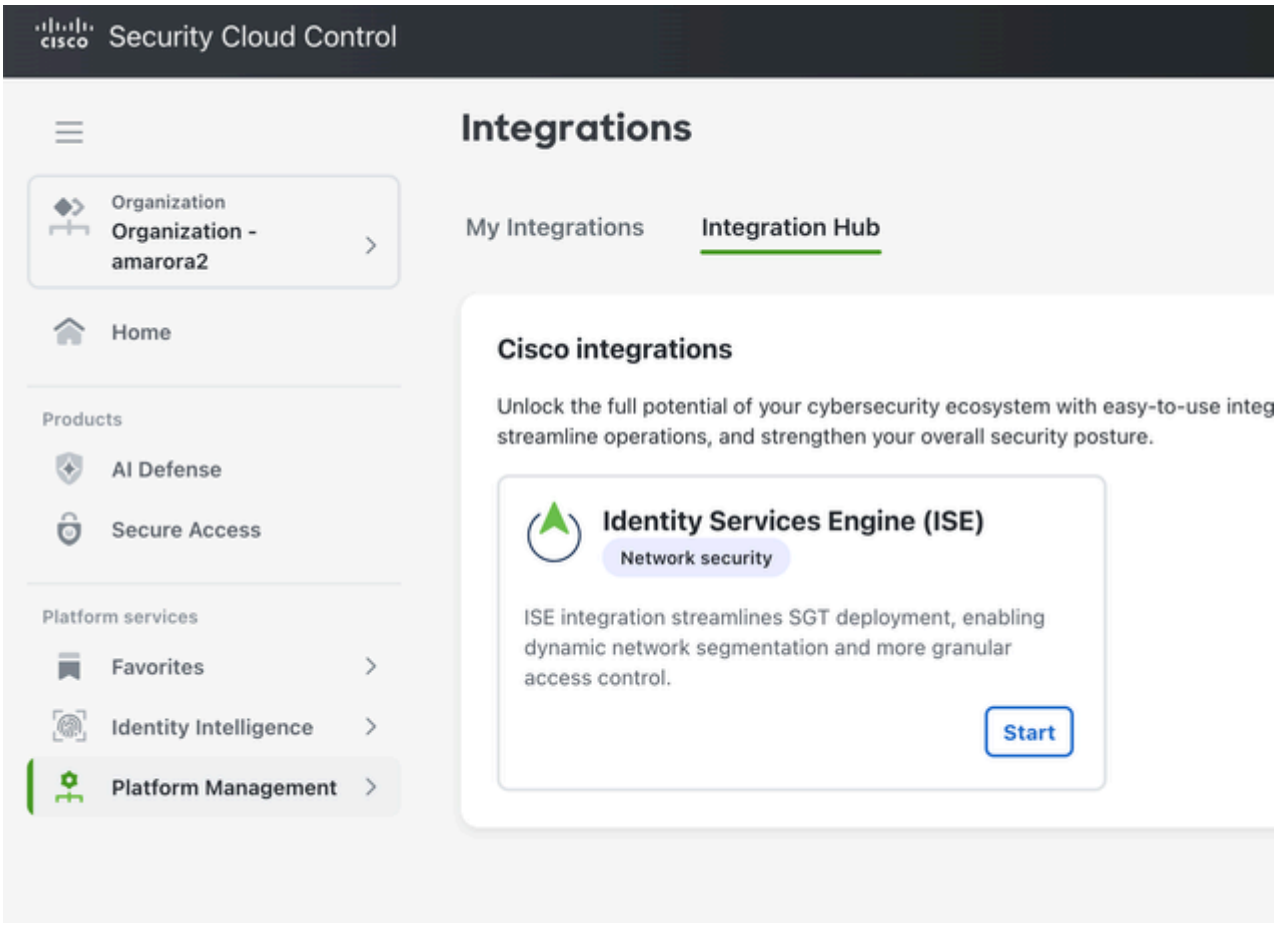
1. Connectez-vous à security.cisco.com.
2. Sélectionnez l'ORG Cisco Secure Access



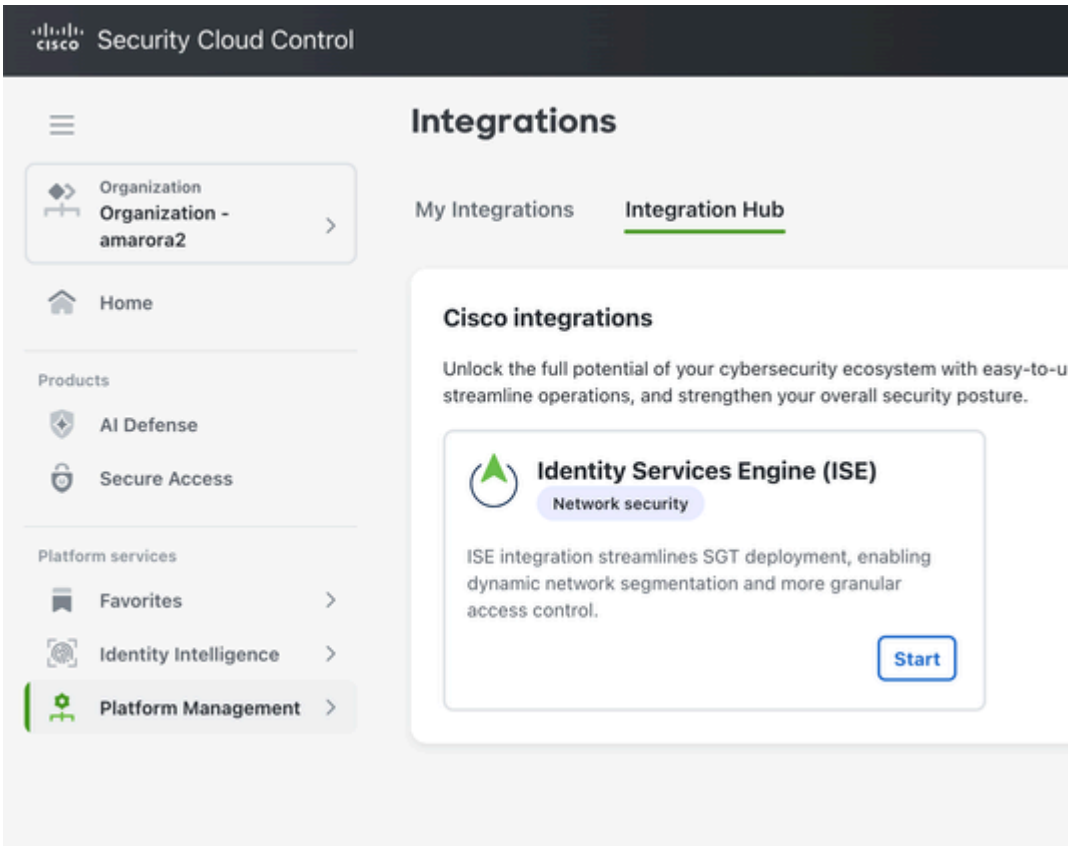
3 Cliquez sur Platform Management - Platform Integrations



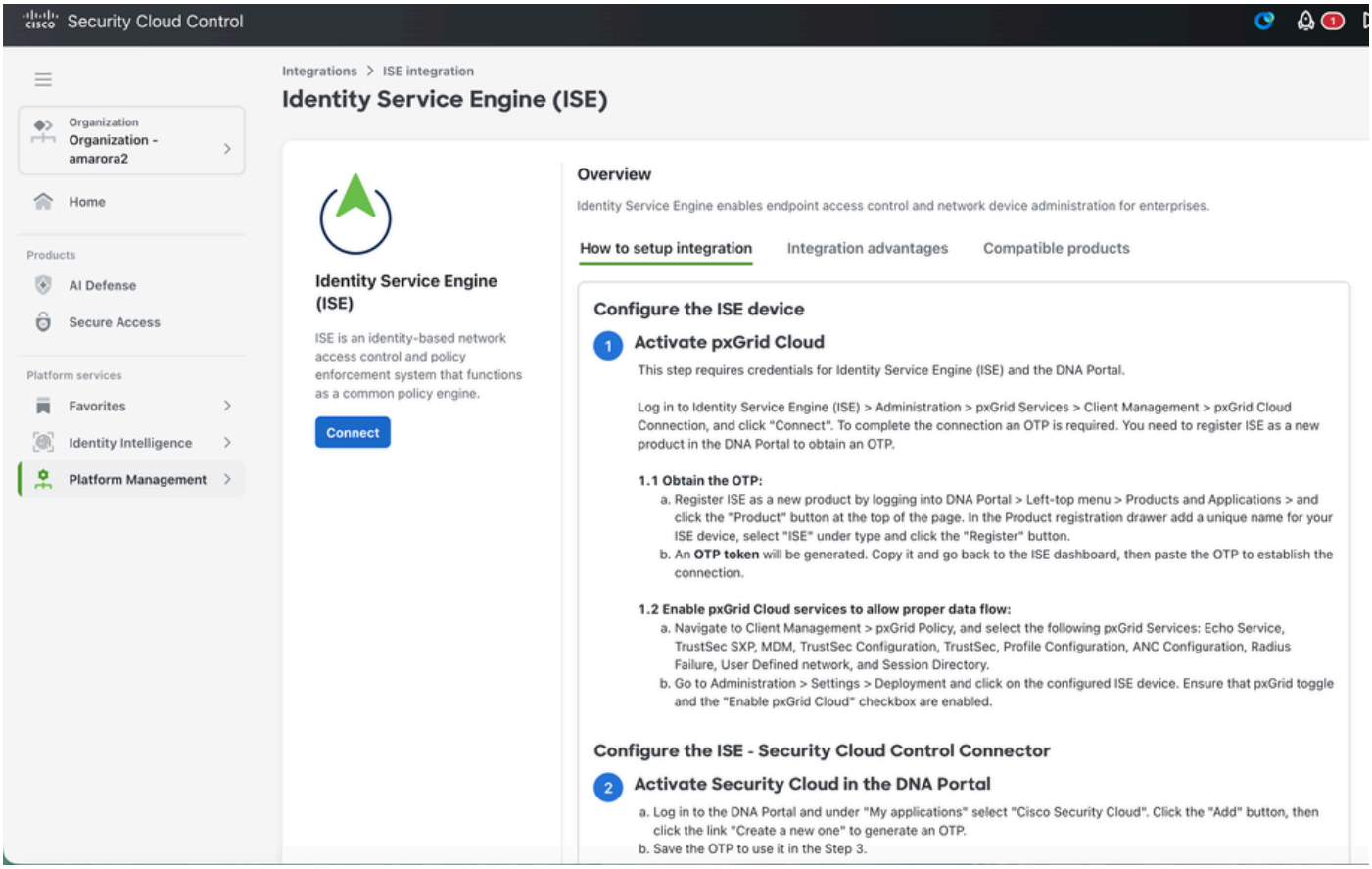
4 Cliquez sur Add Integration Module



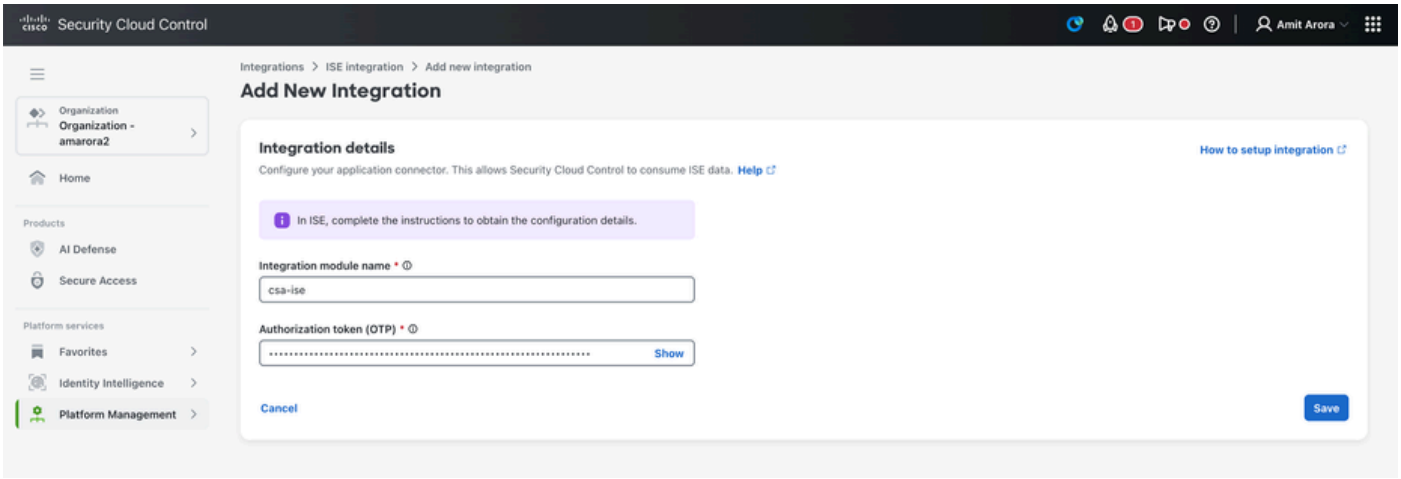
5 Cliquez sur Démarrer



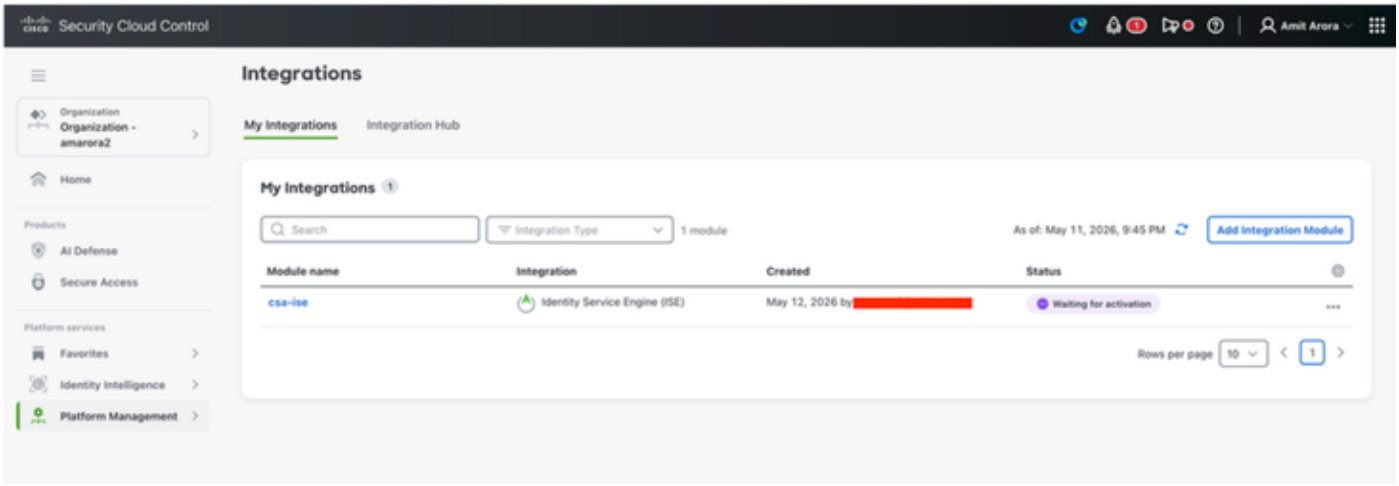
6 Cliquez sur Connect



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



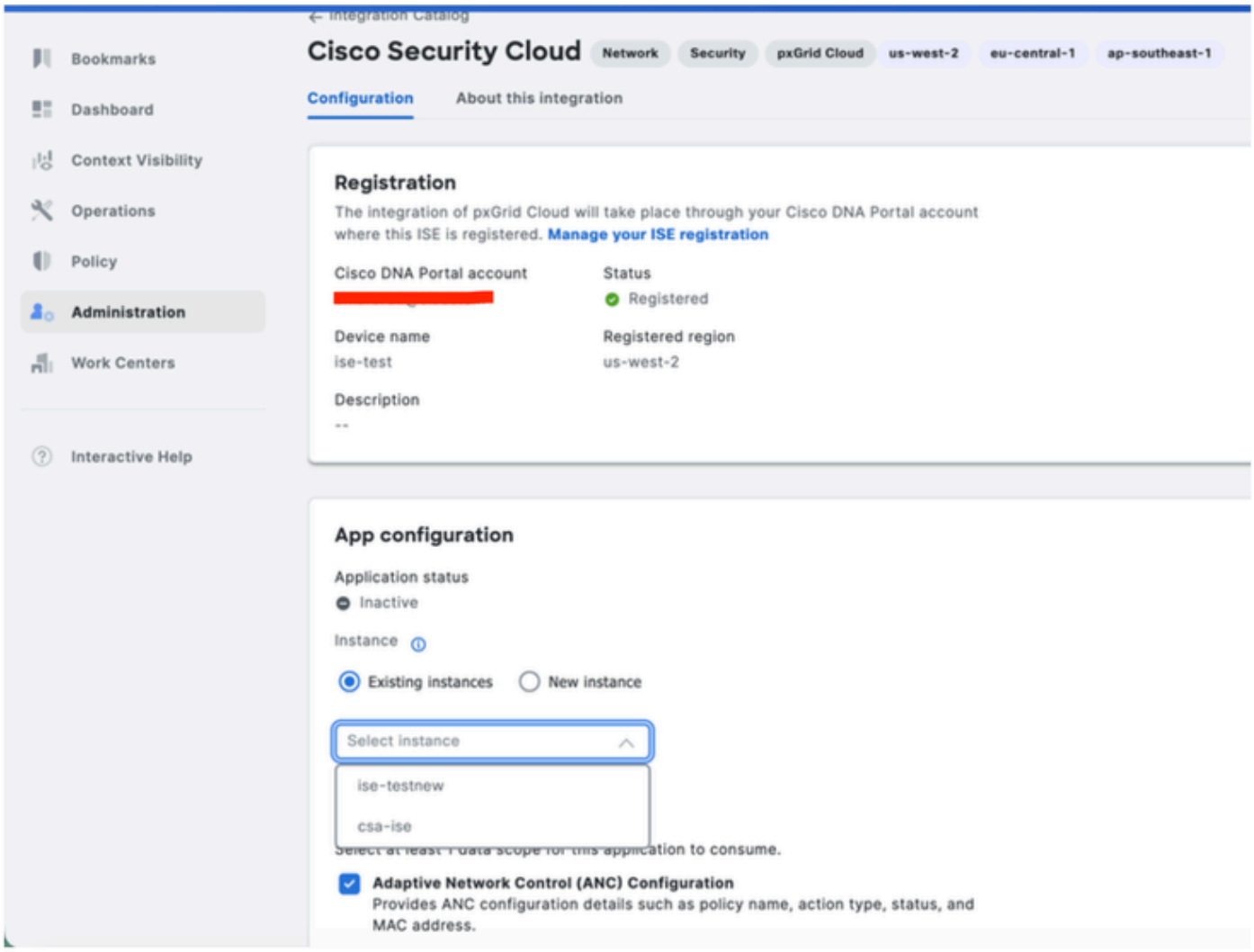
8 Une fois que vous avez cliqué sur Save, le message Waiting for Activation Status s'affiche.



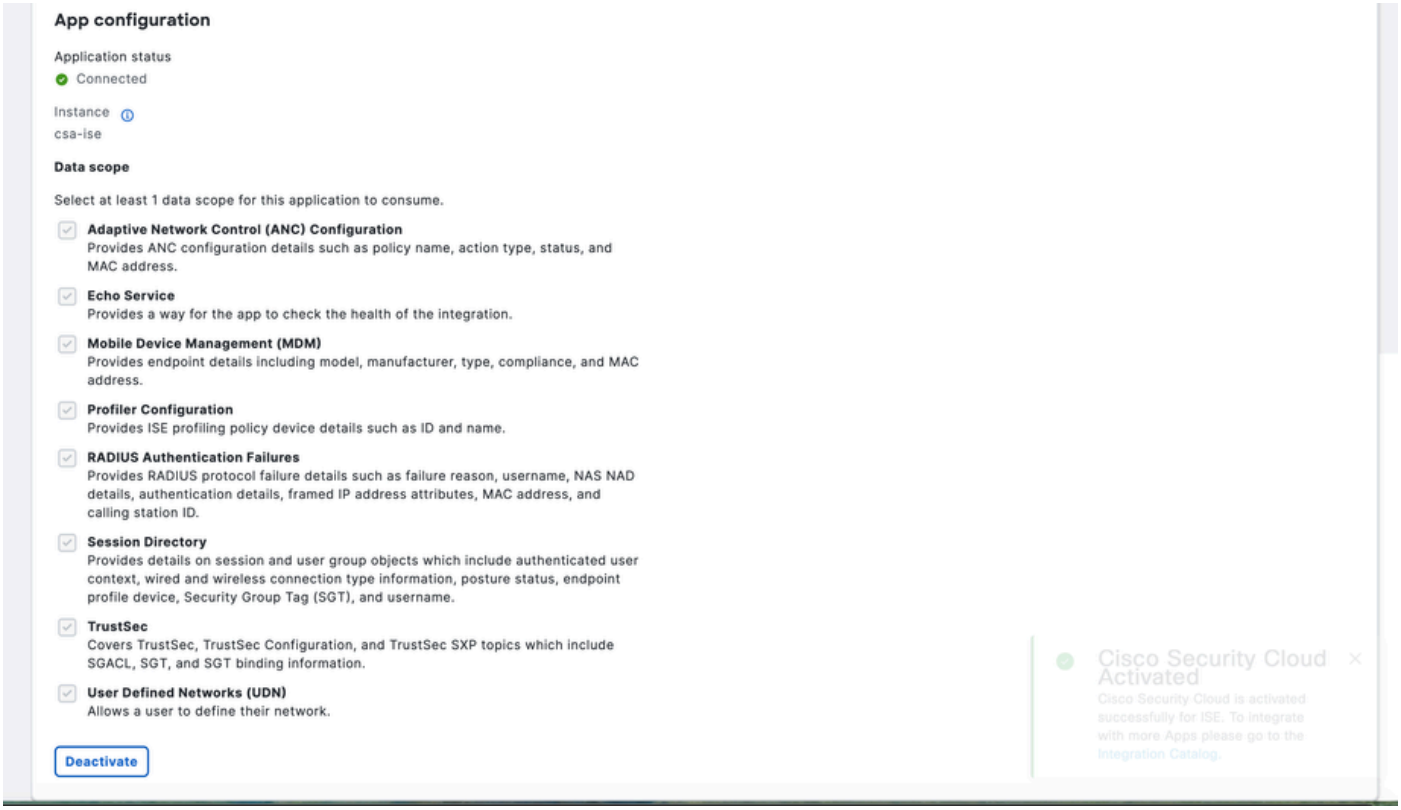
9 Connectez-vous à ISE et accédez à Administration - Deployment. Cliquez sur le noeud avec pxgrid persona - cliquez sur le nuage d'intégration sous Pxgrid Connection.

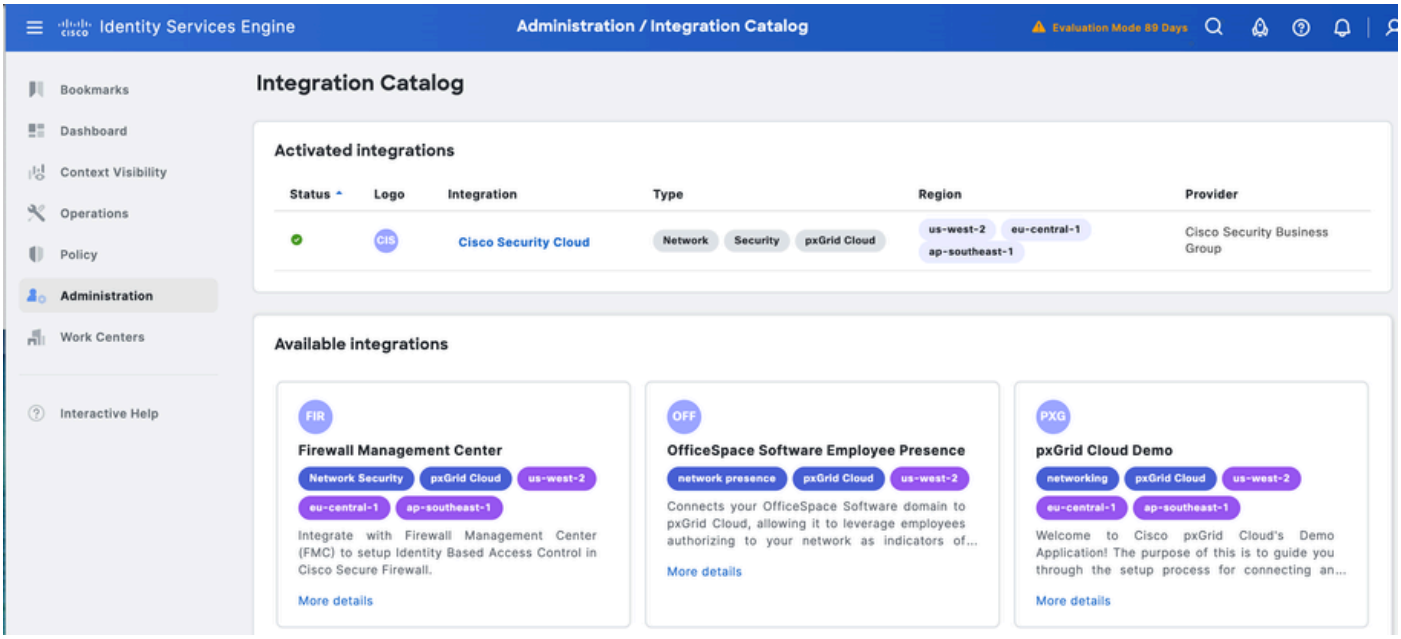
Sous App configuration - sélectionnez l'instance ISE créée dans Security Cloud Control et cliquez

sur Activate



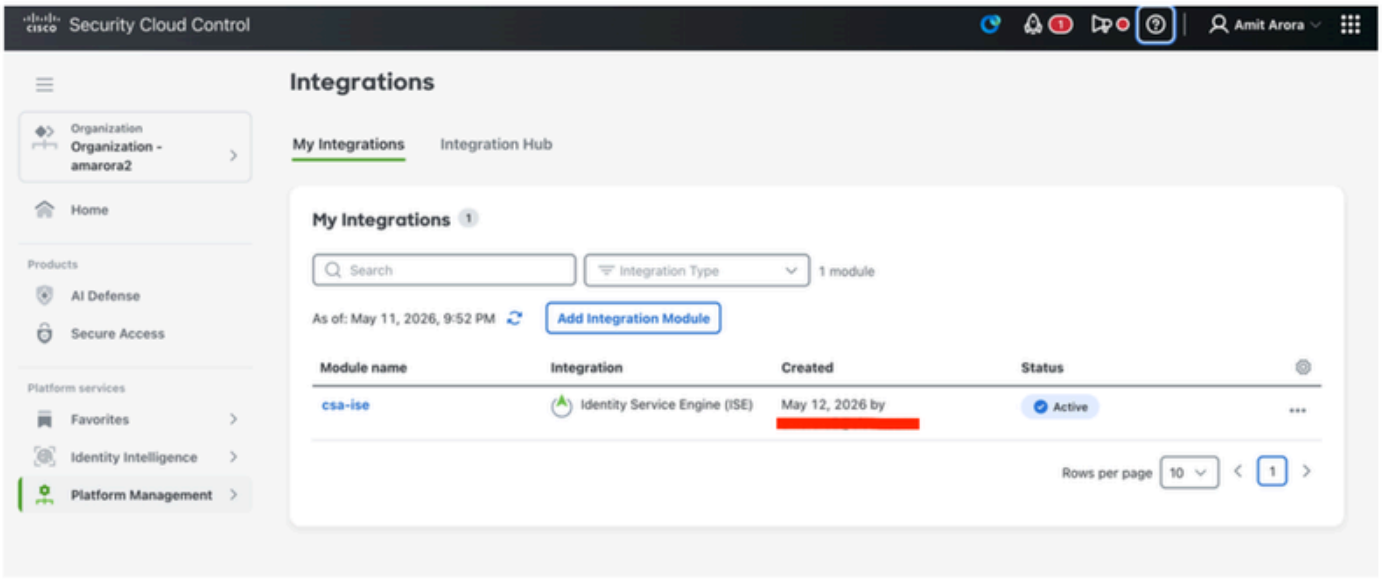
10 L'état de l'application est maintenant connecté.





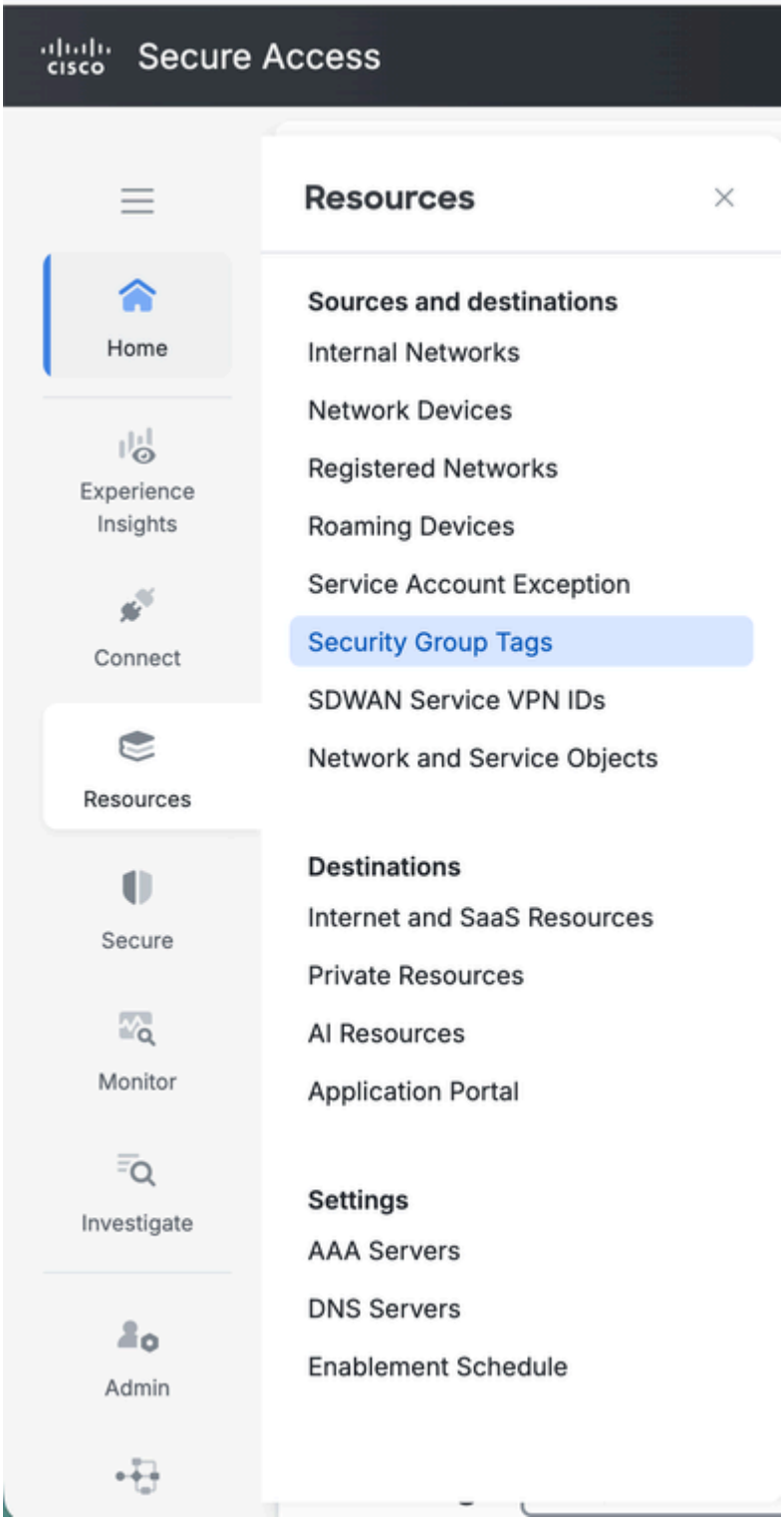
11 Connexion au contrôle du cloud de sécurité - security.cisco.com

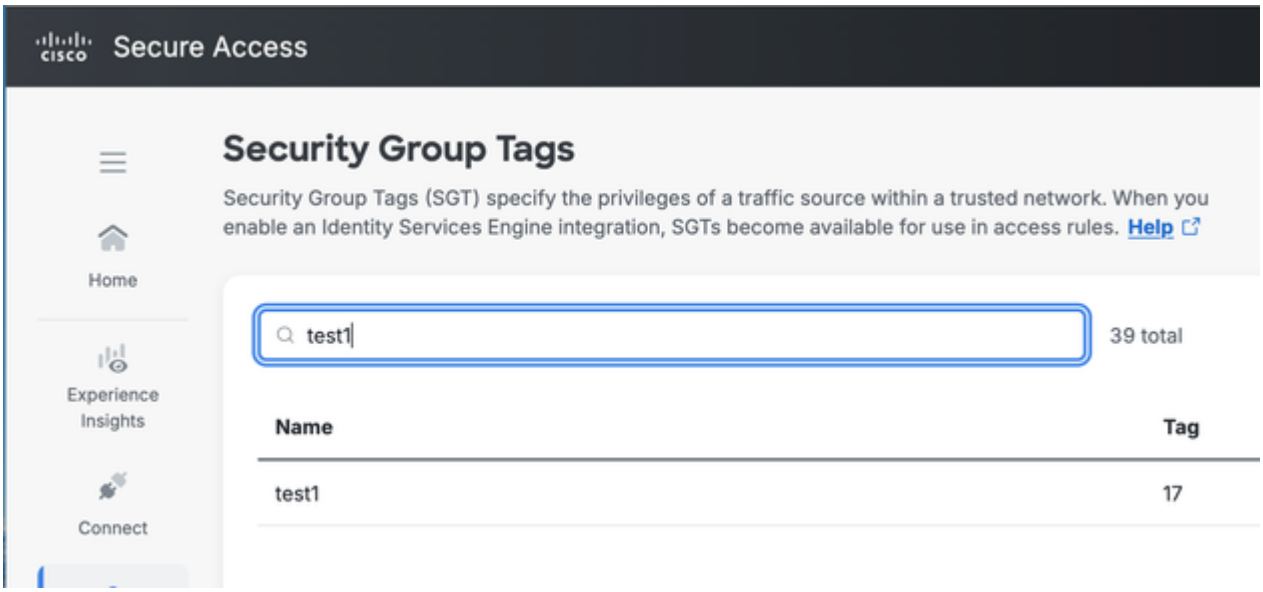
Sous Platform Management - Platform Integrations, nous pouvons voir l'état de l'intégration comme Actif



Vérifier la balise du groupe de sécurité :

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


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



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 Personna :

grille pxgrid

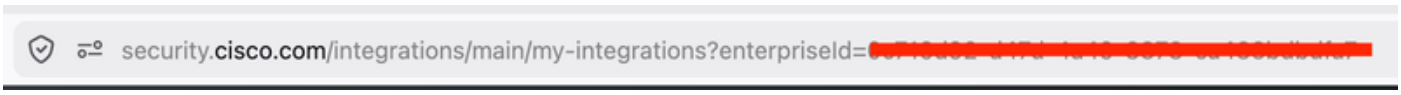
Infrastructure

ERS

composant hermes au niveau du débogage.

SCC :

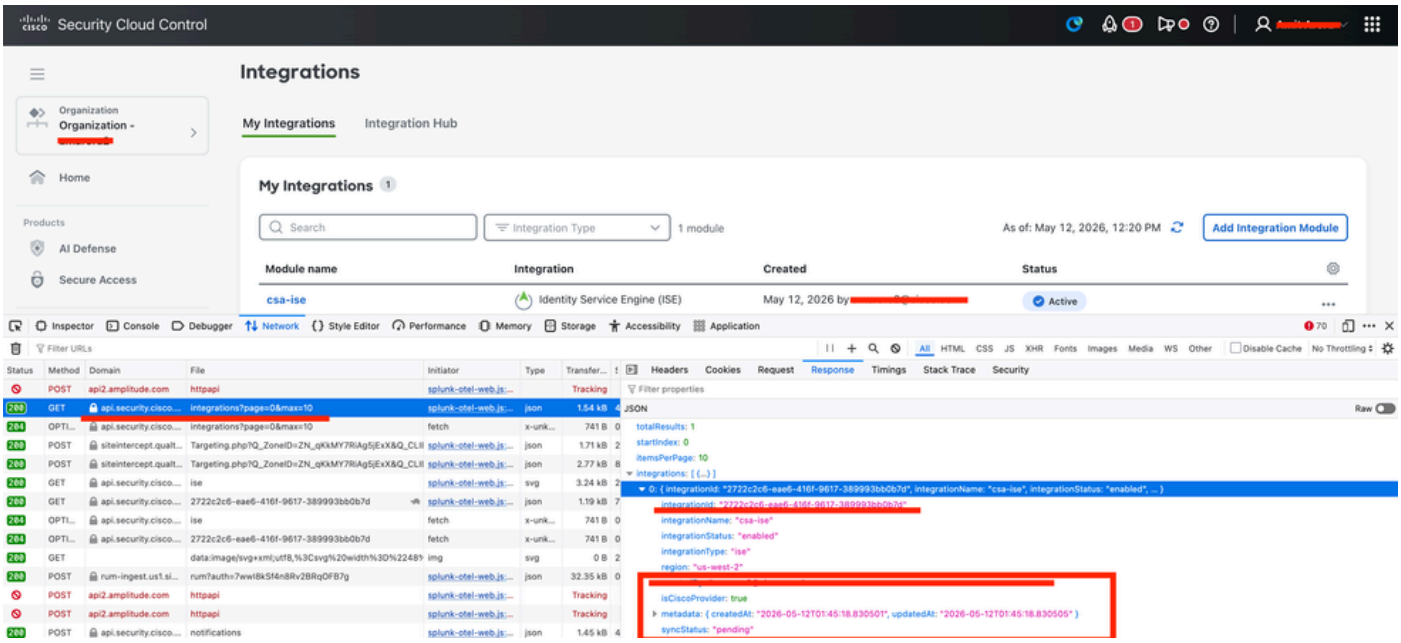
ID d'entreprise : dans l'URL de security.cisco.com



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.



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.