

# Cisco安全訪問與ISE整合，用於通過Pxgrid雲的安全組標籤

## 目錄

---

---

## 簡介

本文檔介紹如何在思科安全訪問和思科身份服務引擎之間啟用情景共用

## 需求

思科建議您瞭解以下主題：

- 思科安全訪問 — 基於雲的安全服務邊緣(SSE)解決方案，提供零信任網路訪問，允許使用者從任何裝置輕鬆連線到網際網路和專用應用。
- 思科身分識別服務引擎(ISE)版本3.4補丁5.
- 思科安全雲控制 — 適用於您的安全雲產品和身份的統一管理解決方案。安全訪問包含安全雲控制。

## 背景

通過這種整合，可以自動建立從Catalyst SD-WAN分支機構到Cisco Secure Access的可靠隧道，從而便於無縫交換VPN-ID/名稱和SGT上下文。

思科身份服務引擎(ISE)仍是SGT配置和管理的主要機構。在ISE中執行的任何更新都會自動與思科安全訪問同步。如果SGT被刪除，引用它的現有規則將保持活動狀態，以確保流量匹配按預期繼續。

我們目前為SGT對映提供有限的可用性，擴展了支援以將SGT目標對象包括在您的安全規則中。此外，即將提供支援來構建從Meraki和思科安全防火牆傳輸SGT的SASE隧道

## 使用案例:

基於名稱空間的SGT策略：

作為安全管理人員，Kit希望使用來自本地ISE的SGT對SSE私有和網際網路繫結的流量實施連續微分段。能夠匯入SGT以應用策略。



## 採用元件

本檔案中的資訊是根據：

- 身分識別服務引擎(ISE)版本3.4補丁5
- 安全訪問
- 思科安全雲端

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 情景共用配置概述

- 將ISE連線到Cisco安全雲
- 將思科安全訪問連線到ISE

## 設定

本指南將整體配置分為以下主要步驟：

1. 將Cisco ISE連線到Cisco Security Cloud
2. 連線思科安全訪問思科ISE
3. Cisco Secure Access中的安全組標籤

## 開始之前

- 確保您已在思科ISE部署中安裝和啟用優勢許可證。
- DNA雲代理建立到思科DNA雲的出站HTTPS連線。因此，如果您的網路使用代理訪問網際網路，您必須配置思科ISE代理設定。要在Cisco ISE中配置代理設定，請導航至 **Administration > System > Settings > Proxy**
- 確保為從思科ISE到思科pxGrid雲門戶的出站連線開啟埠443。如果配置了防火牆或代理設定，請確保這些URL未被阻止：

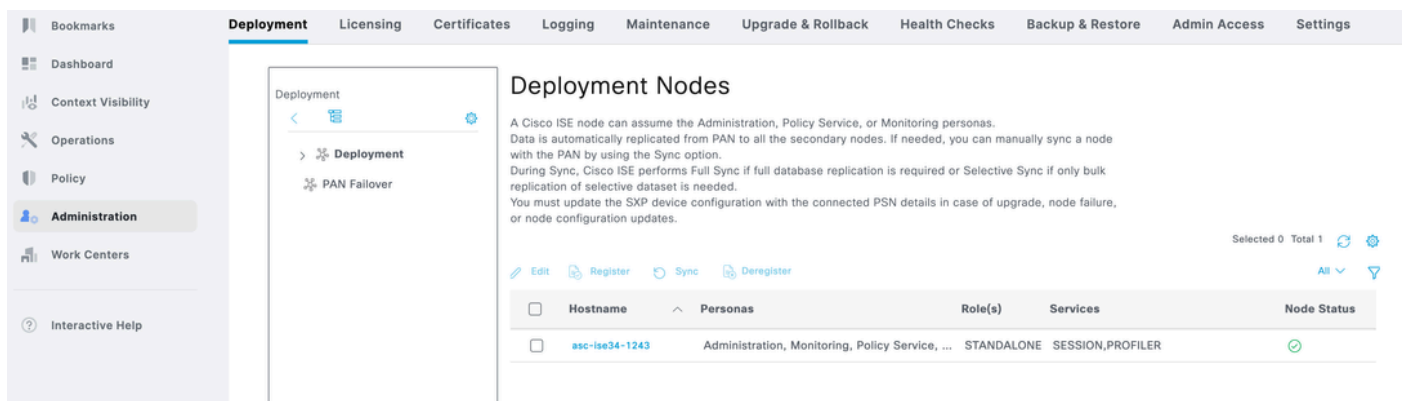
<https://dna.cisco.com>

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

## 第1步：在ISE上啟用Pxgrid雲

1導航到ISE GUI。

2按一下「管理」 — 「部署」。



The screenshot shows the Cisco ISE GUI interface. The top navigation bar includes tabs for Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade & Rollback, Health Checks, Backup & Restore, Admin Access, and Settings. The left sidebar contains a navigation menu with options like Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (highlighted), Work Centers, and Interactive Help. The main content area is titled 'Deployment Nodes' and contains a table with columns for Hostname, Personas, Role(s), Services, and Node Status. A single node is listed with the hostname 'isc-ise34-1243' and a green status icon.

Hostname	Personas	Role(s)	Services	Node Status
isc-ise34-1243	Administration, Monitoring, Policy Service, ...	STANDALONE	SESSION,PROFILER	🟢

3按一下節點並向下滾動到底部。

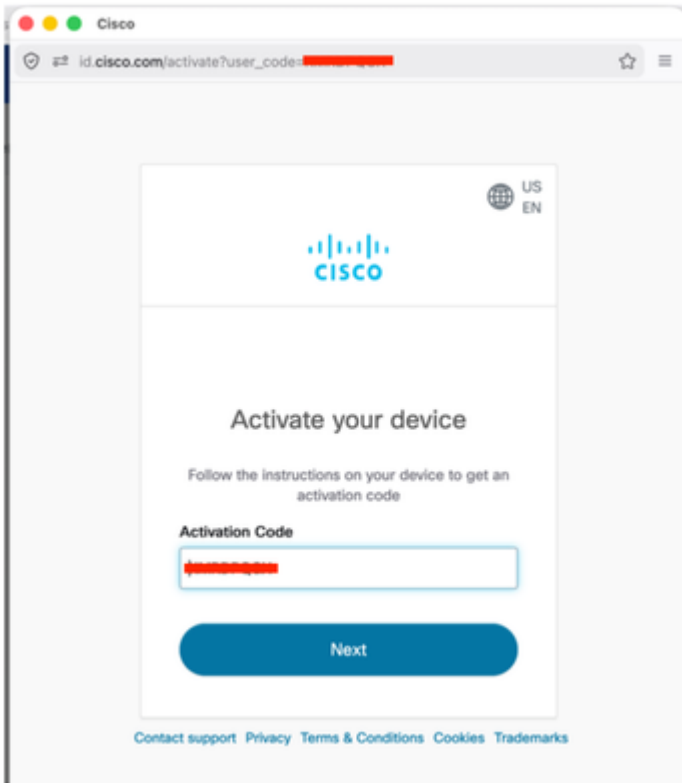
輸入ISE部署名稱

選擇Region ( 區域 ) 為US West 2 , 這是目前唯一支援的區域。

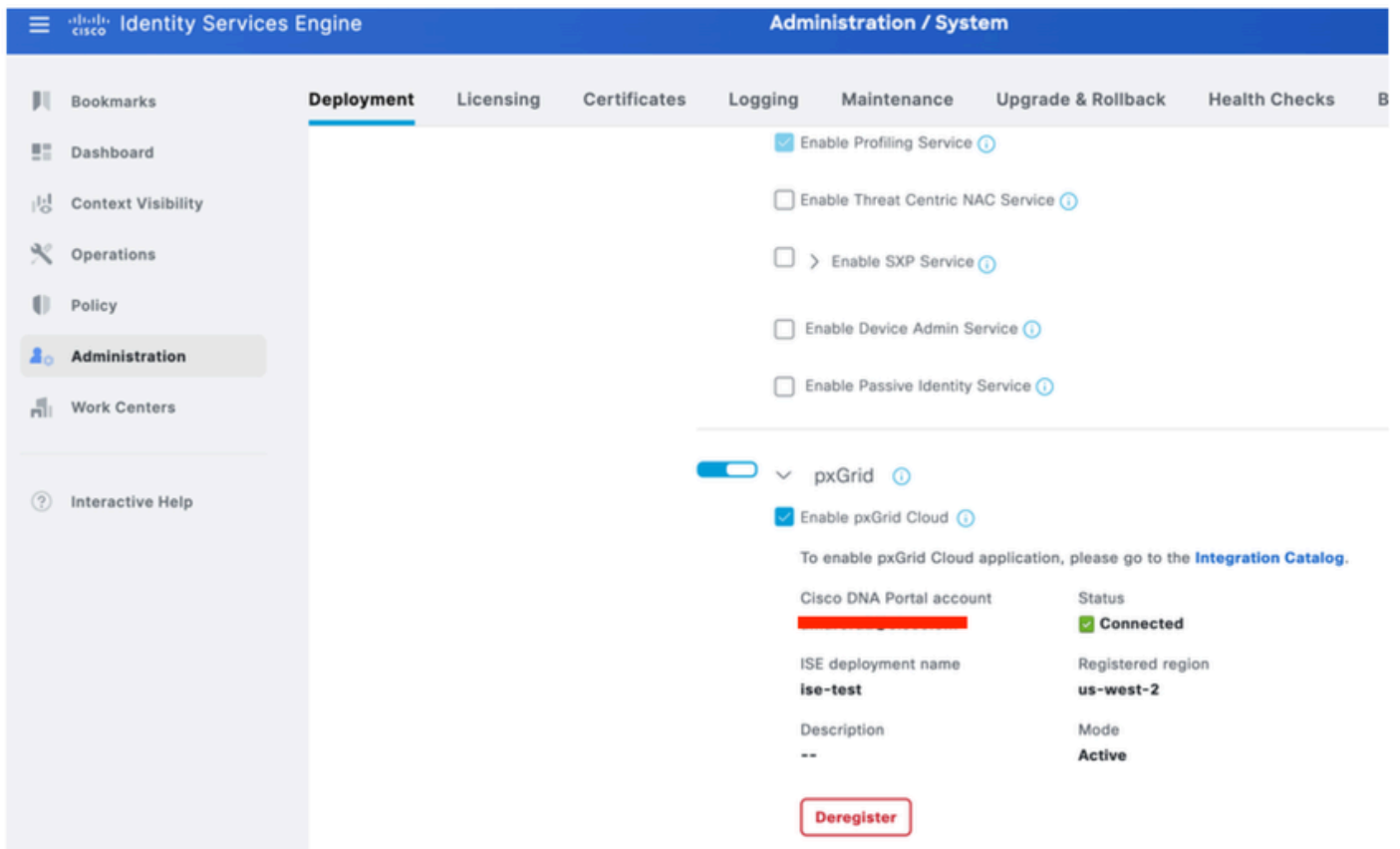
選中兩個竅取方塊並點選註冊(Register)。

The screenshot shows the Cisco ISE Administration console interface. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (highlighted), Work Centers, and Interactive Help. The main content area is under the 'Deployment' tab, with sub-tabs for Licensing, Certificates, Logging, Maintenance, Upgrade & Rollback, Health Checks, and Backup & R. The 'pxGrid' section is active, showing a toggle switch turned on. Below it, the 'Enable pxGrid Cloud' checkbox is checked. A yellow warning box with a triangle icon states: 'pxGrid Cloud can be enabled only after registering your Cisco ISE to your Cisco DNA Portal account.' The 'ISE deployment name' field contains 'ise-test'. The 'Description (optional)' field is empty. Below this, a note says: 'Select a region where you want to register your device. Application should also be available in the same region.' The 'Region' dropdown menu is set to 'us-west-2'. At the bottom, there are two checked checkboxes: 'I have read and acknowledge the Cisco Privacy Statement.' and 'I agree that offers are governed by Cisco EULA and I am an authorized agent of my company. Cisco's End User License Agreement.' A blue 'Register' button is located at the bottom right of the form.

4 您將看到一個包含自動填充啟用代碼的彈出視窗。按一下「下一步」 ,

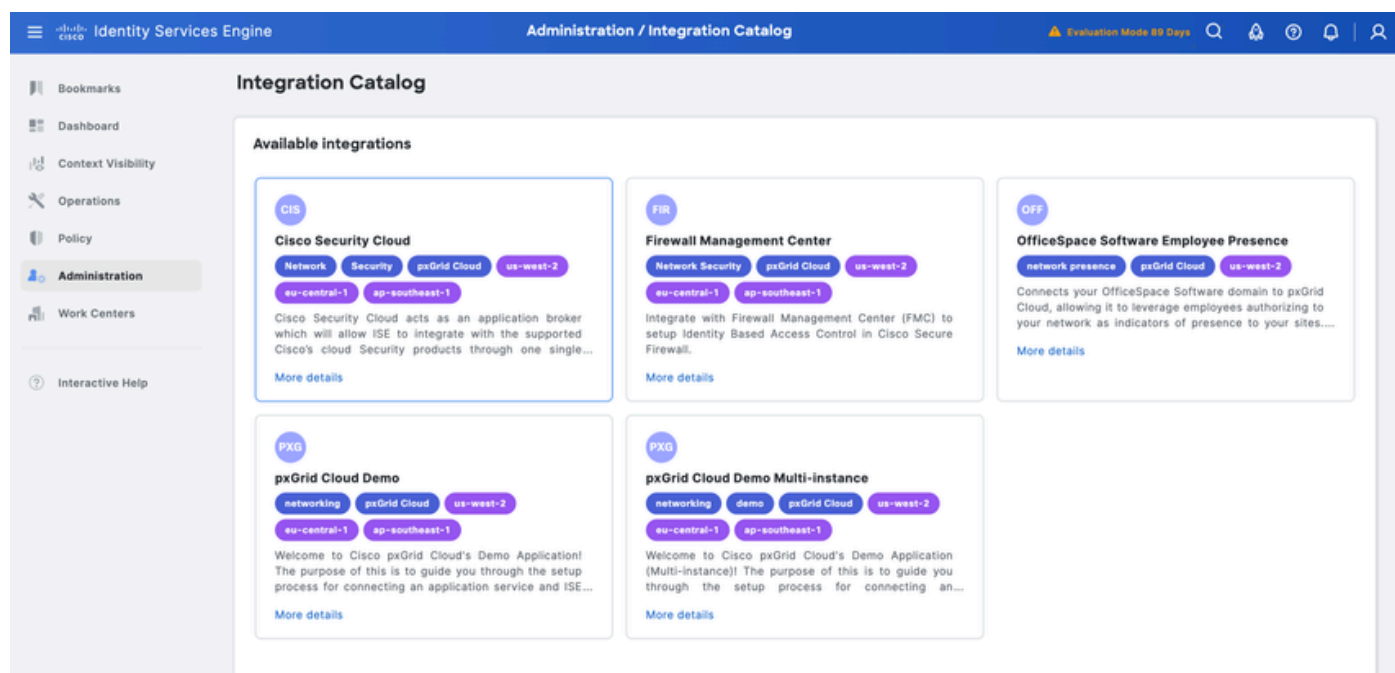


5個ISE將顯示已連線到Pxgrid雲。



6按一下步驟5中的「Integration Catalog ( 整合目錄 )」連結。

在「Available Integrations ( 可用整合 )」下，按一下「Cisco Security Cloud ( 思科安全雲 )」



7在App Configuration下，按一下New Instance，然後按一下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.

複製用於Cisco Secure Access的一次性密碼。


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](#) 

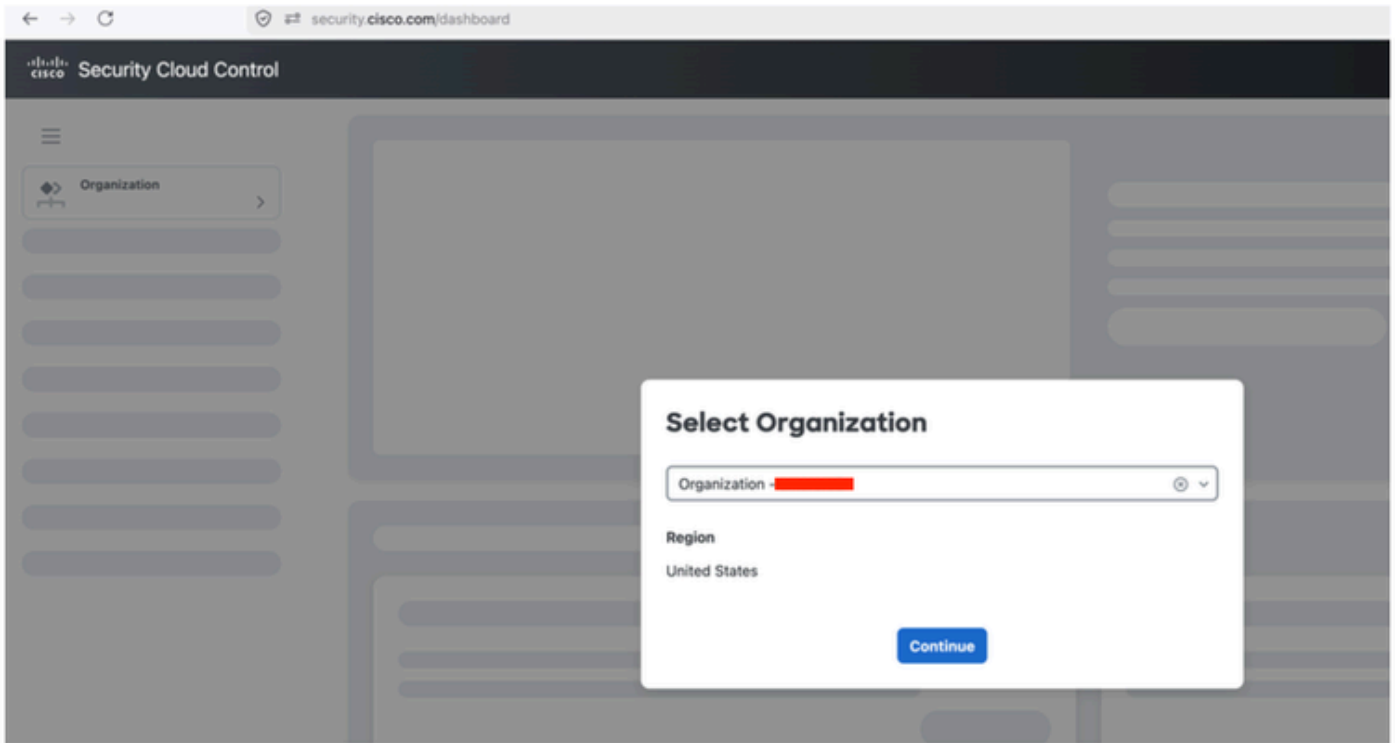
One-time password

  **Copy**

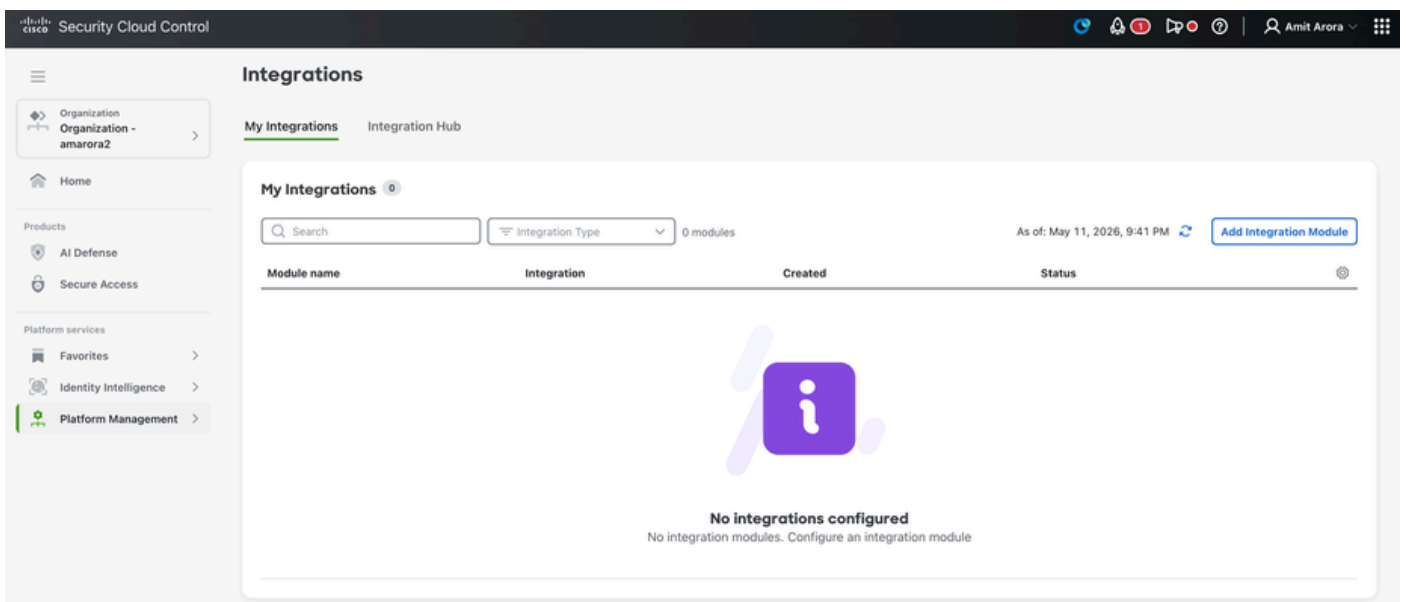
**OK**

### 第2步：將思科安全訪問與ISE整合

1. 登入security.cisco.com。
2. 選擇Cisco Secure Access ORG



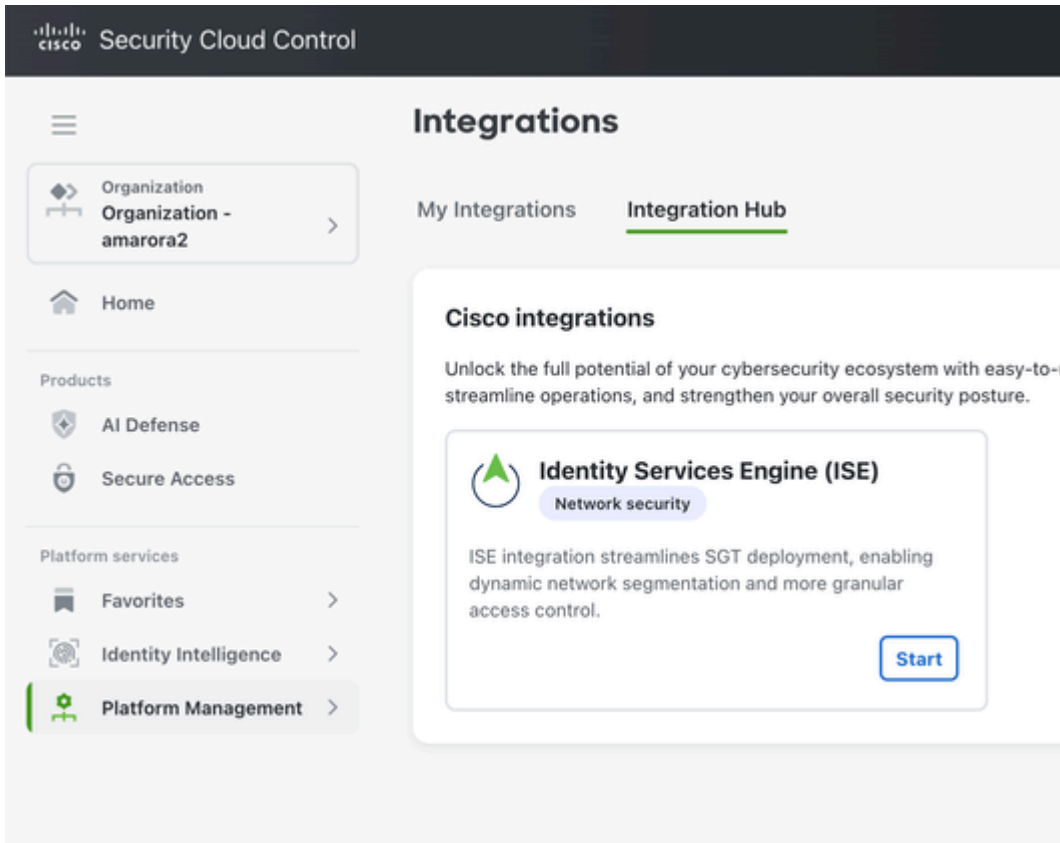
3點選「平台管理」 — 「平台整合」



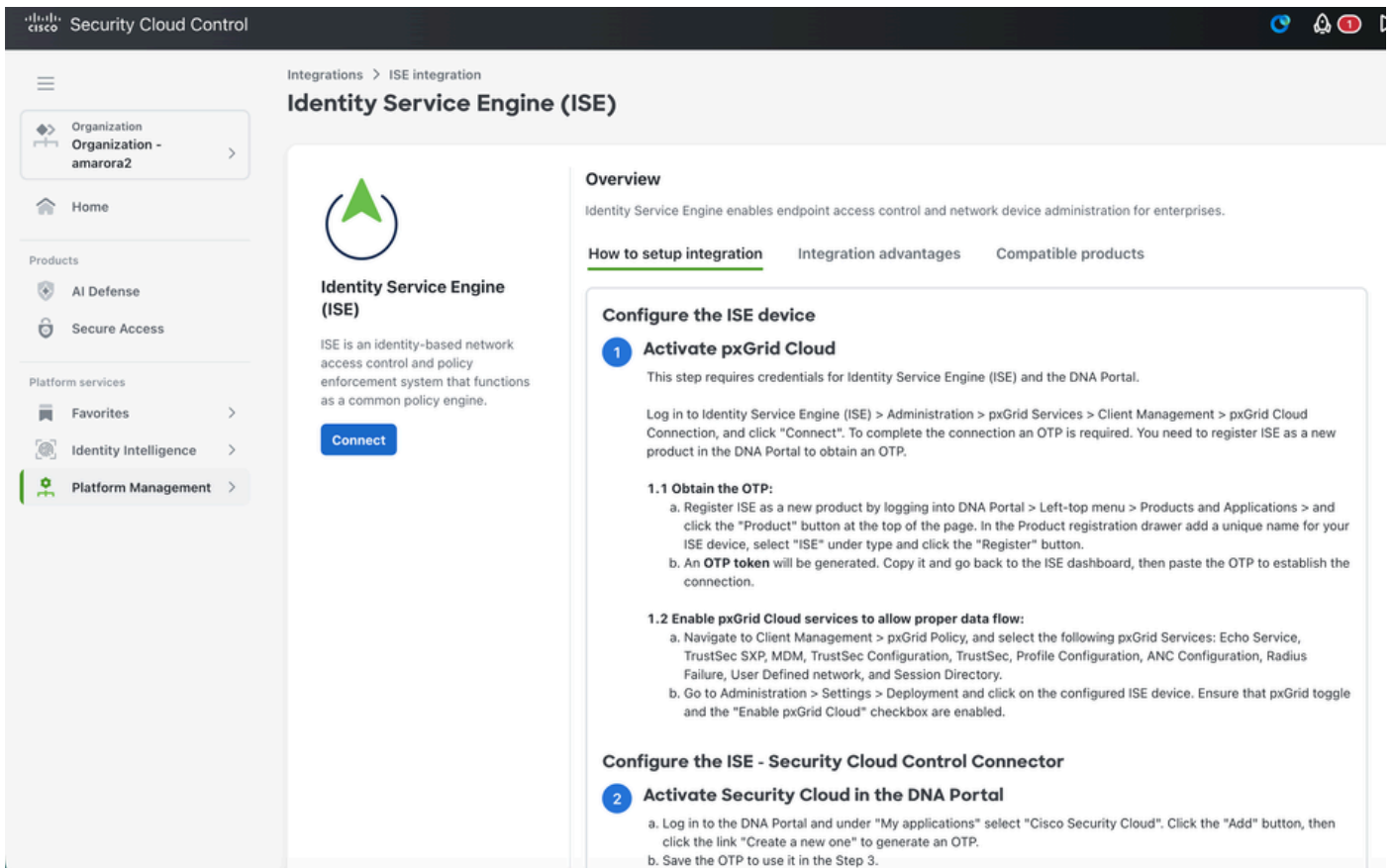
## 4 點選 Add Integration Module

The screenshot displays the Cisco Security Cloud Control interface. The top navigation bar includes the Cisco logo and the text 'Security Cloud Control'. A sidebar on the left contains a menu with the following items: 'Organization - amarora2', 'Home', 'Products' (AI Defense, Secure Access), and 'Platform services' (Favorites, Identity Intelligence, Platform Management). The main content area is titled 'Integrations' and features two tabs: 'My Integrations' and 'Integration Hub'. The 'Integration Hub' tab is active, showing a section for 'Cisco integrations' with the text: 'Unlock the full potential of your cybersecurity ecosystem with easy-to-use integ streamline operations, and strengthen your overall security posture.' Below this is a card for 'Identity Services Engine (ISE)' with a 'Network security' tag, a description: 'ISE integration streamlines SGT deployment, enabling dynamic network segmentation and more granular access control.', and a 'Start' button.

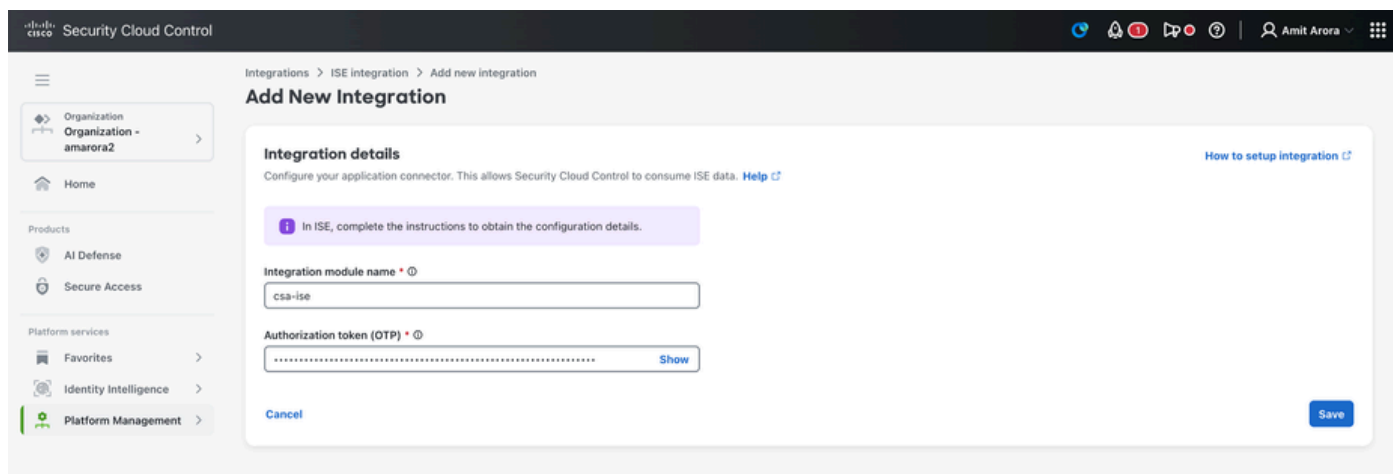
5 按一下「Start (開始)」



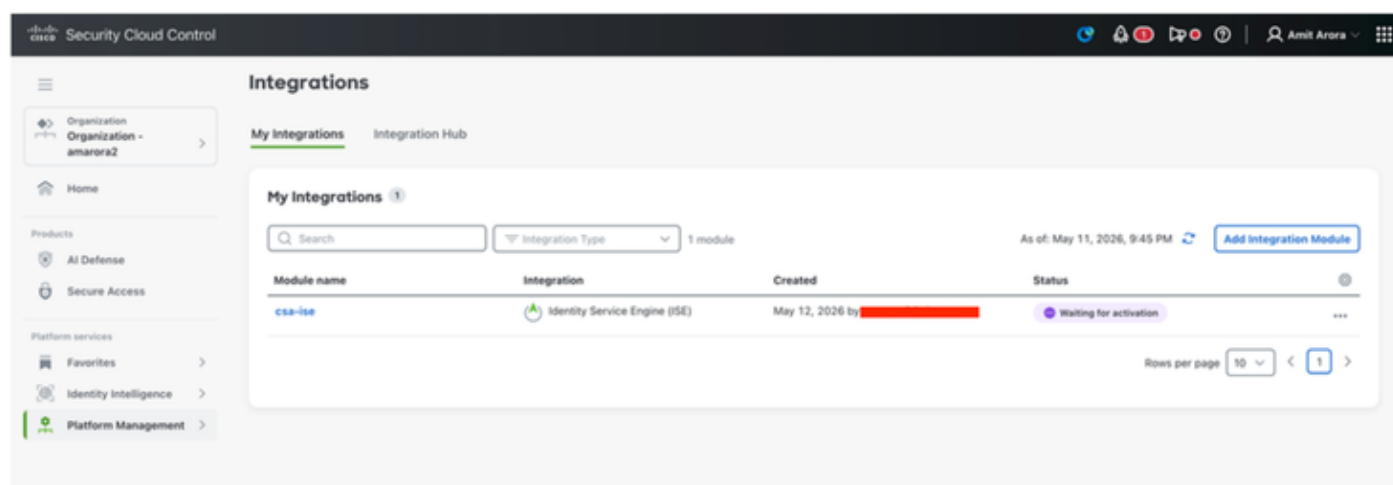
6按一下「連線」



7.輸入來自思科ISE的整合模組名稱和OTP，然後點選Save



8按一下「儲存」後，我們將看到「等待啟用狀態」。



9登入到ISE並導航到Administration - Deployment。點選pxgrid角色的節點 — 點選Pxgrid Connection下的Integration cloud。

在App configuration ( 應用配置 ) 下 — 選擇在Security Cloud Control ( 安全雲控制 ) 中建立的ISE例項，然後按一下Activate ( 啟用 )

← 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
██████████	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應用狀態現在已連線。

## 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**

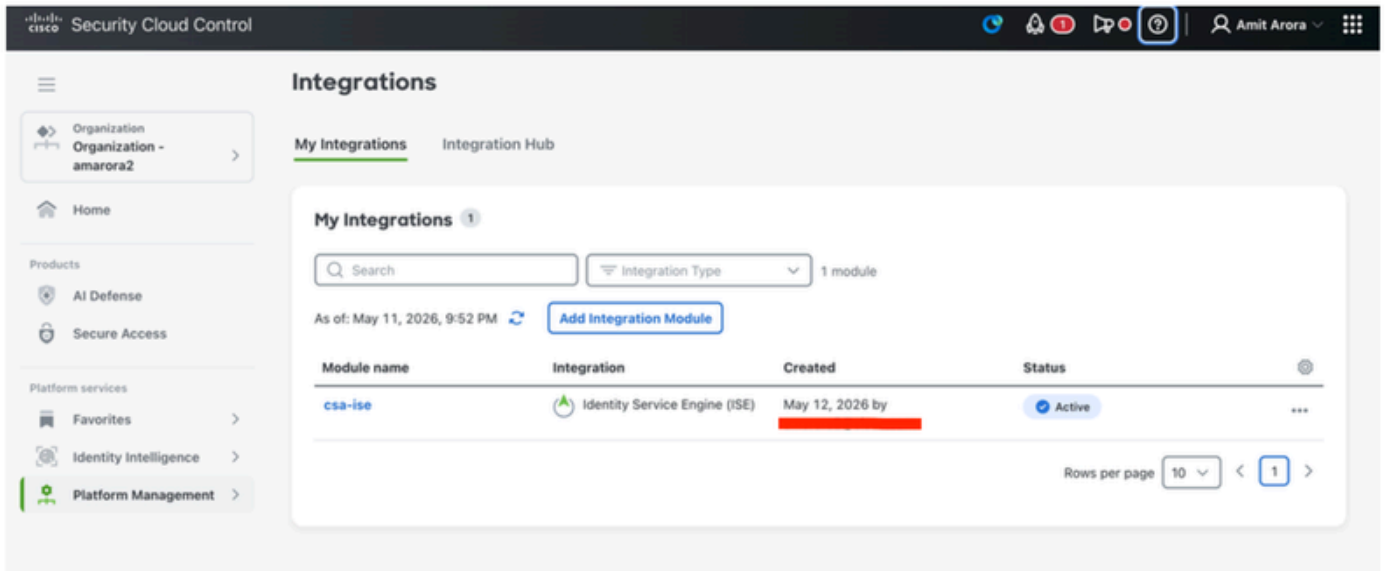
Status	Logo	Integration	Type	Region	Provider
ON	CIS	Cisco Security Cloud	Network Security pxGrid Cloud	us-west-2 eu-central-1 ap-southeast-1	Cisco Security Business Group

**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 登入到安全雲控制 — security.cisco.com

在Platform Management - Platform Integrations下，我們可以看到整合狀態為Active



The screenshot shows the Cisco Security Cloud Control interface. The top navigation bar includes the Cisco logo, the text "Security Cloud Control", and user information "Amit Arora". The main content area is titled "Integrations" and has two tabs: "My Integrations" (selected) and "Integration Hub". On the left, a sidebar menu lists "Organization - amarora2", "Home", "Products" (AI Defense, Secure Access), and "Platform services" (Favorites, Identity Intelligence, Platform Management). The "My Integrations" section features a search bar, a filter for "Integration Type" (1 module), and a refresh button. Below this is a table with the following data:

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

At the bottom right of the table, there is a "Rows per page" dropdown set to 10 and a pagination control showing page 1 of 1.

驗證安全組標籤：

登入到Cisco Secure Access。導航到Resources - Security Group Tags。



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

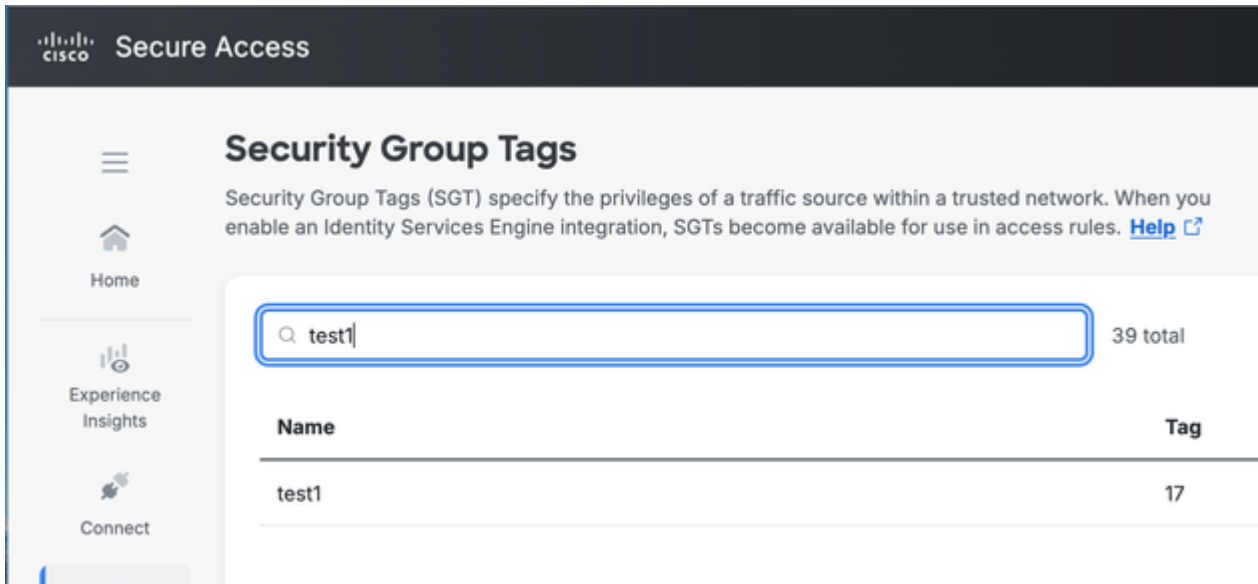
Application Portal

### Settings

AAA Servers

DNS Servers

Enablement Schedule



## Cisco TAC所需資訊

ISE :

[如何收集ISE支援捆綁](#)，使用以下元件設定為調試級別的ISE節點上的Pxgrid個人：

pxgrid

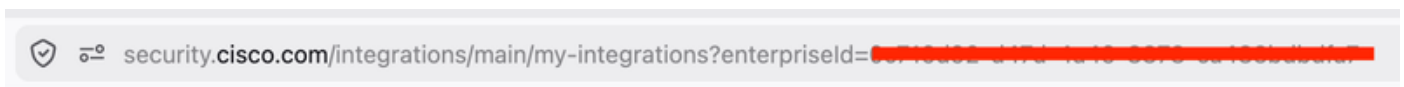
基礎設施

ERS

hermes元件處於調試級別。

SCC:

企業ID:在security.cisco.com的URL中



整合ID。

## 開始HAR捕獲

登入Security.cisco.com

導航到Platform Management - Platform Integrations

搜尋整合(Integrations)頁面api呼叫，並在響應頁籤中查詢整合ID。

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, "csc-ise", is listed with the description "Identity Service Engine (ISE)" and a status of "Active".

Below the table, the network inspector shows a series of API calls. The response for a GET call to the "integrations?page=0&max=10" endpoint is expanded, showing a JSON array of integration objects. One object is highlighted with a red box, containing the following details:

```
{
  "integrationId": "2722c2c6-aae6-416f-9617-389993bb0b7d",
  "integrationName": "csc-ise",
  "integrationStatus": "enabled",
  "region": "us-west-2",
  "isCiscoProvider": true,
  "metadata": {
    "createdAt": "2026-05-12T01:45:18.830501",
    "updatedAt": "2026-05-12T01:45:18.830501"
  },
  "syncStatus": "pending"
}
```

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。