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：

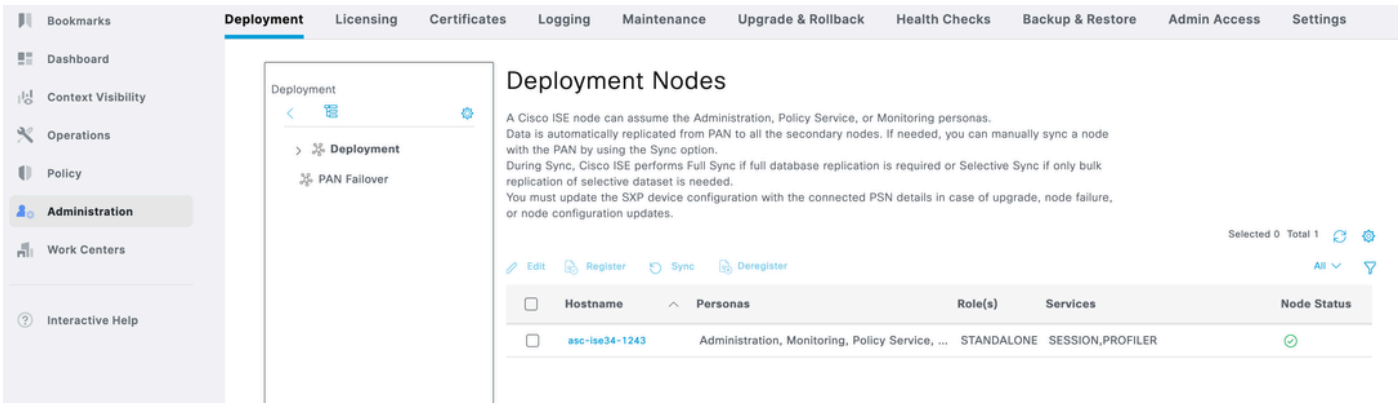
https://dna.cisco.com

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」。

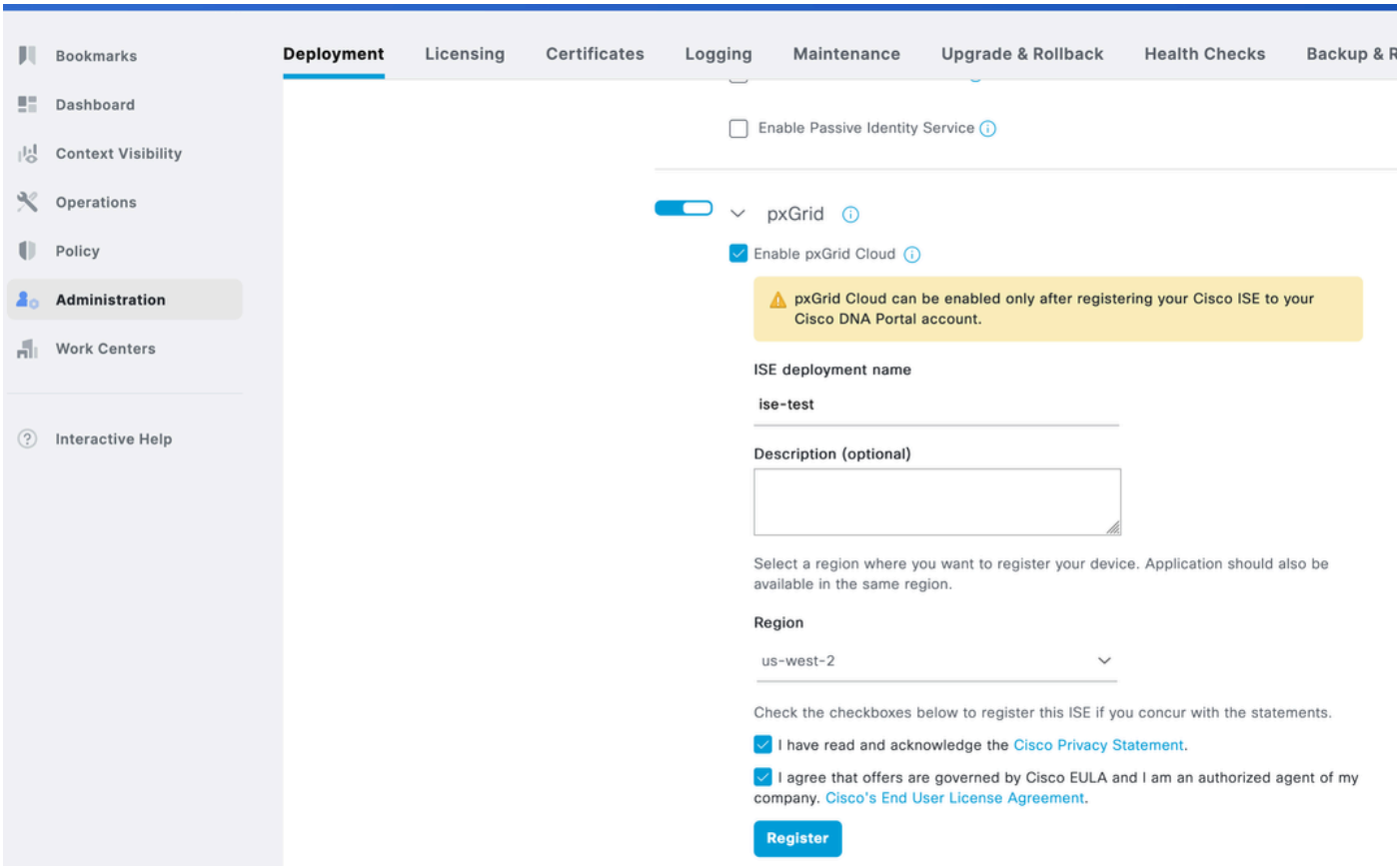


3按一下節點並向下滾動到底部。

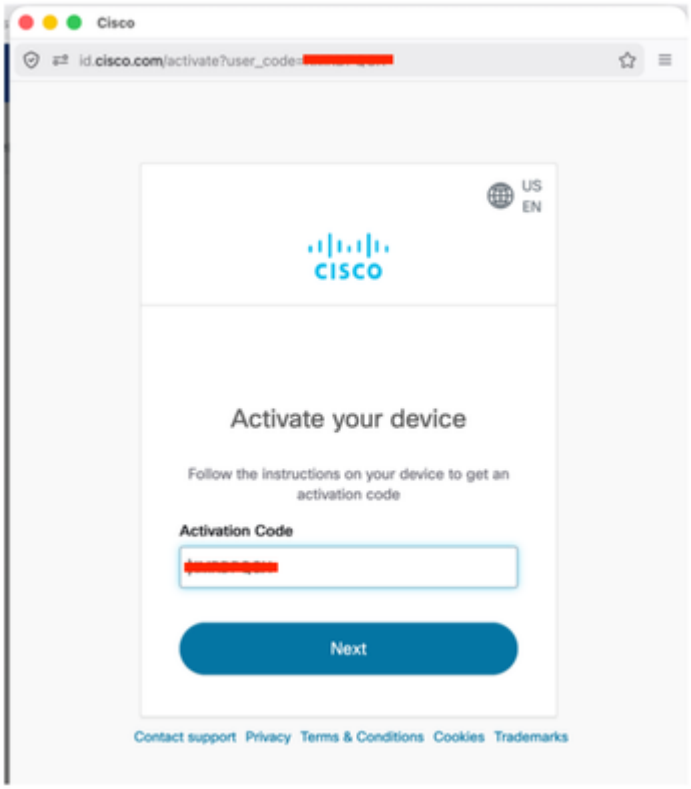
輸入ISE部署名稱

選擇Region（區域）為US West 2，這是目前唯一支援的區域。

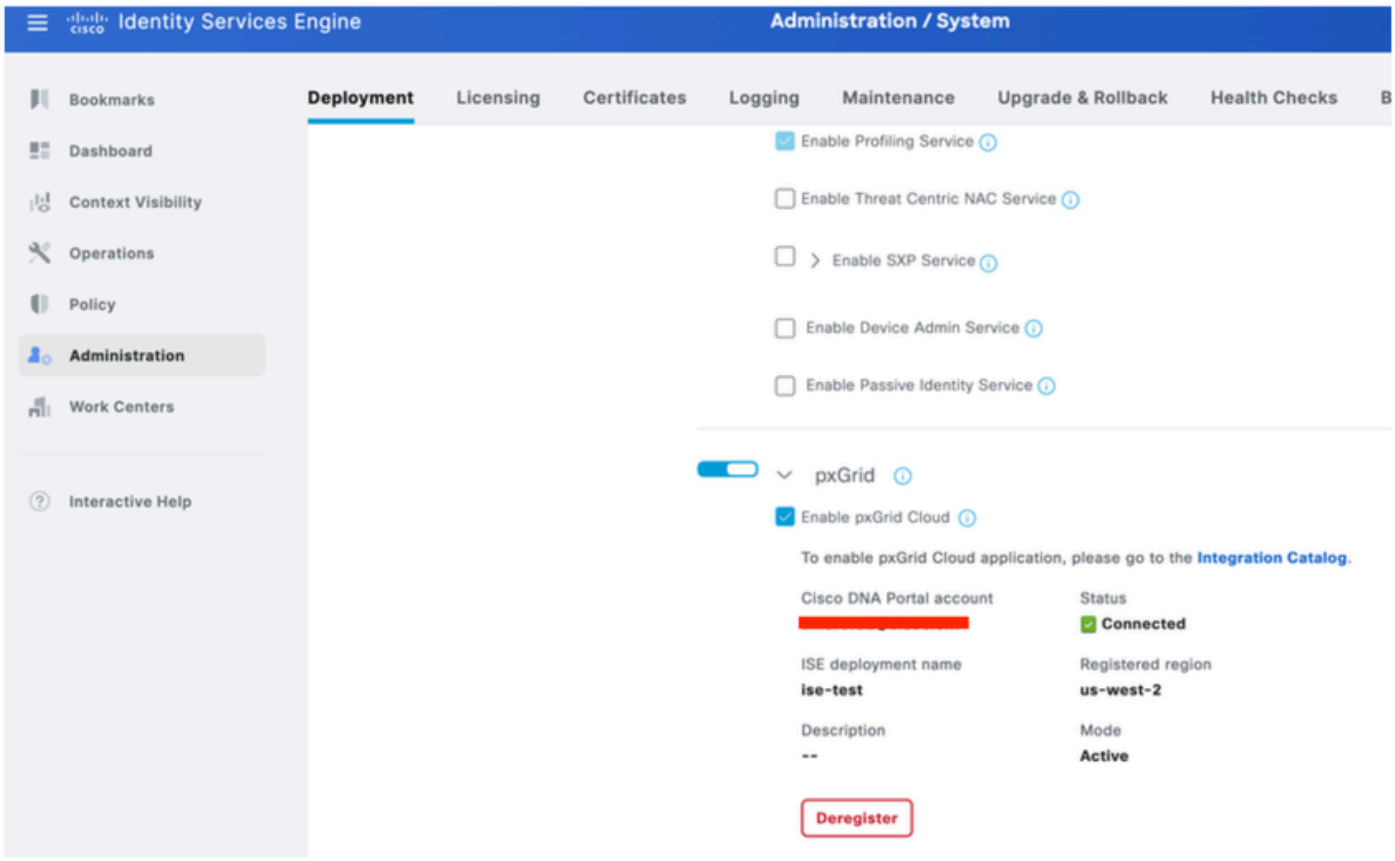
選中兩個覈取方塊並點選註冊(Register)。



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」，



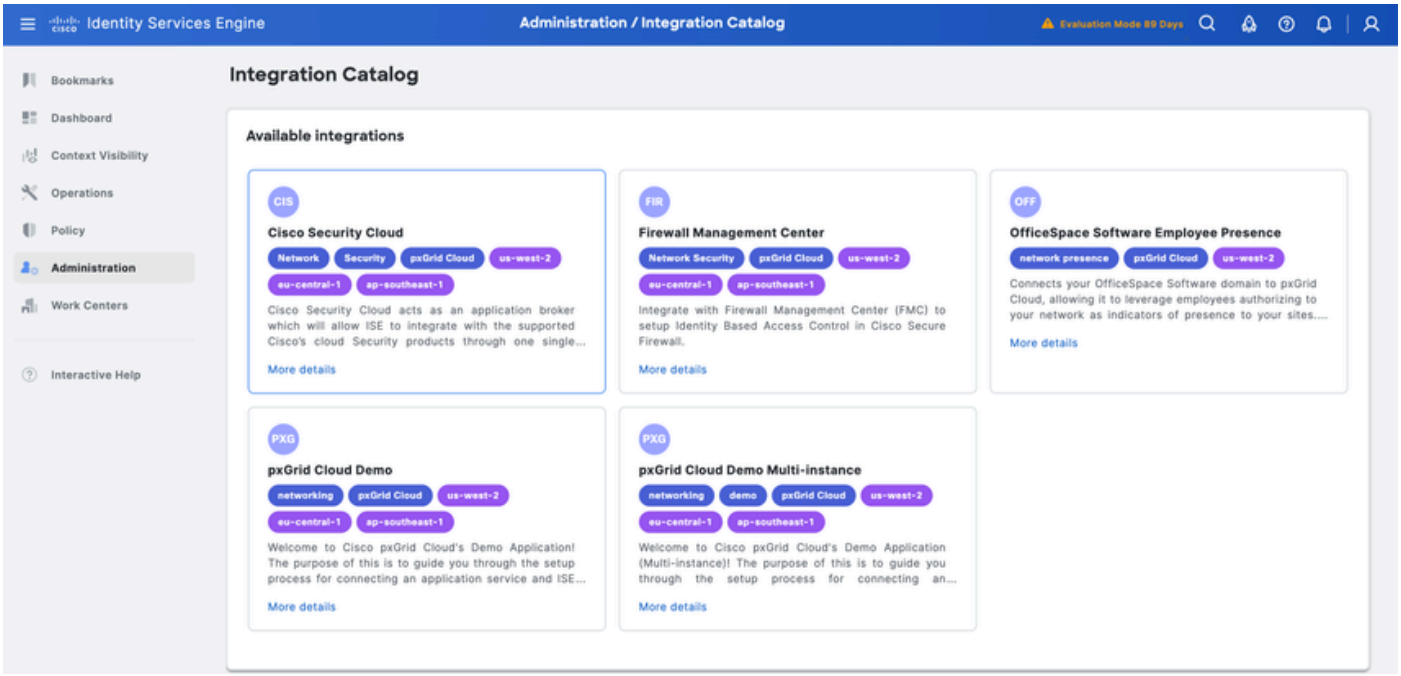
5個ISE將顯示已連線到Pxgrid雲。



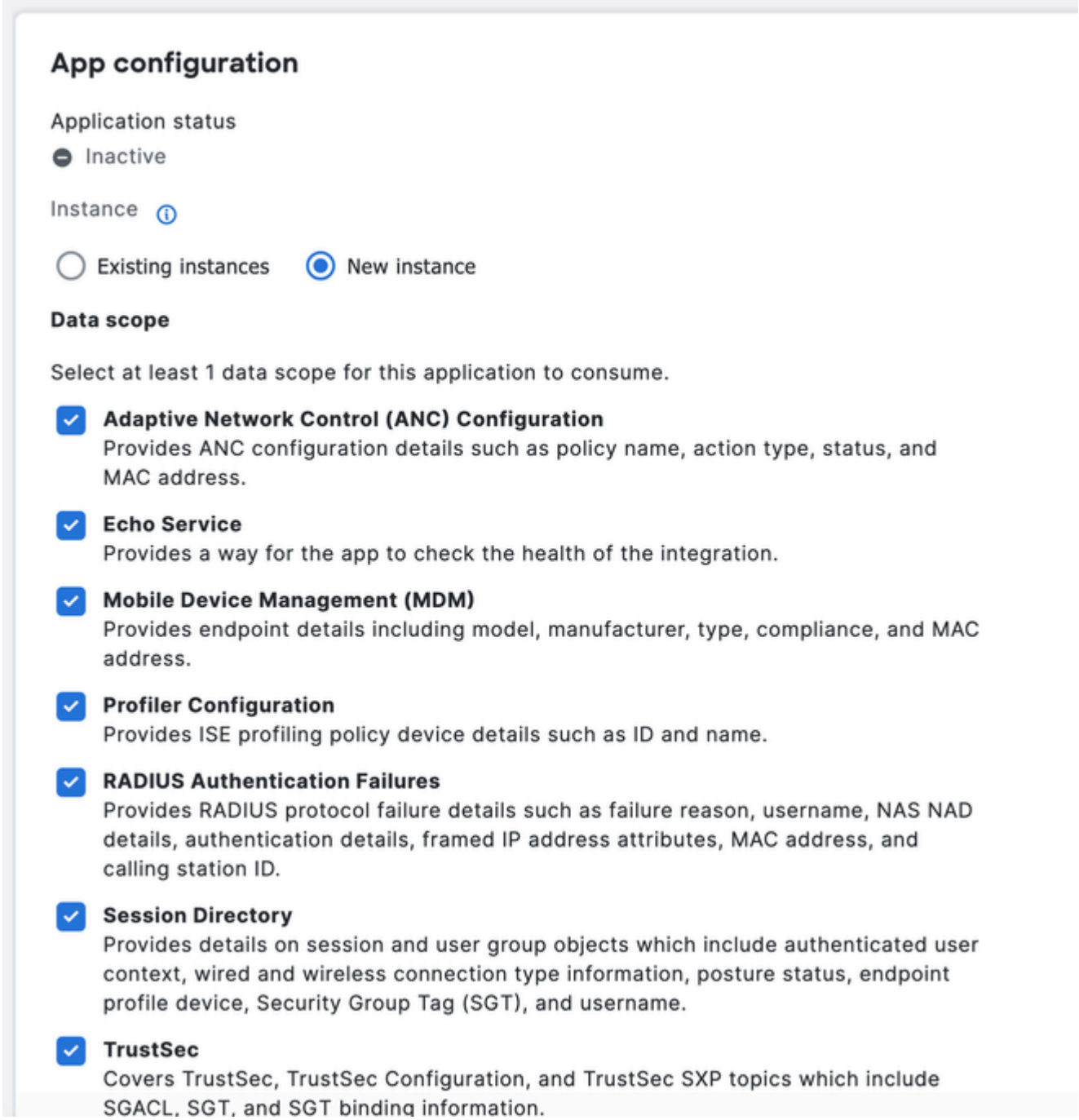
6按一下步驟5中的「Integration Catalog（整合目錄）」連結。

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

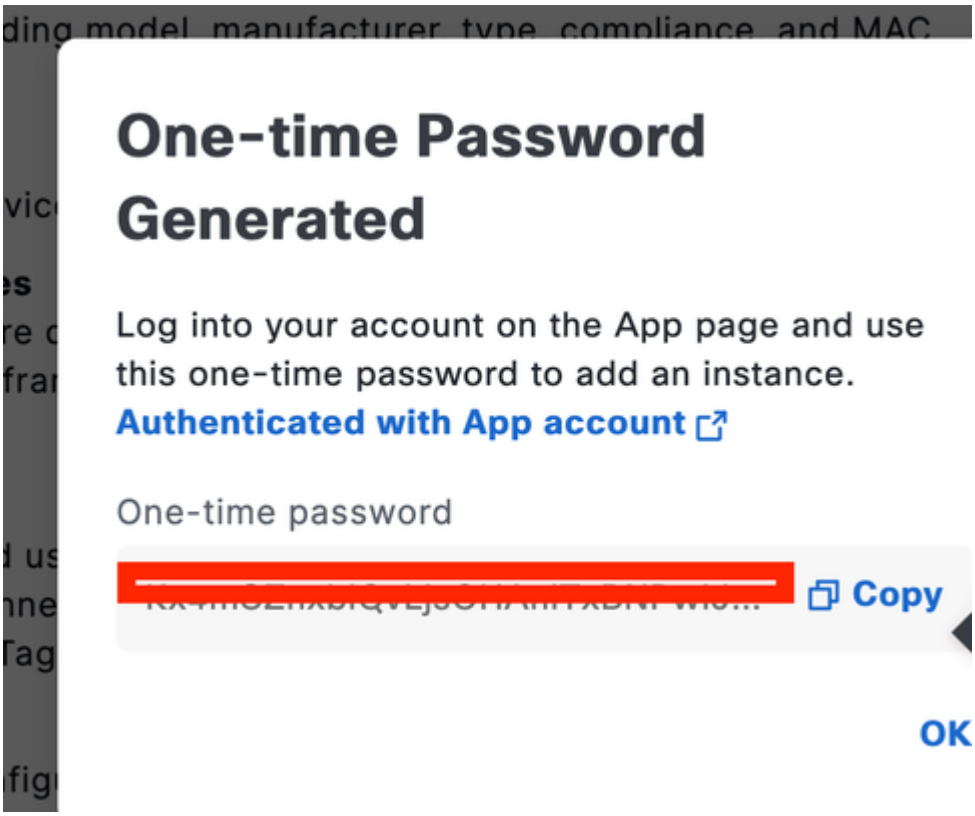
.



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

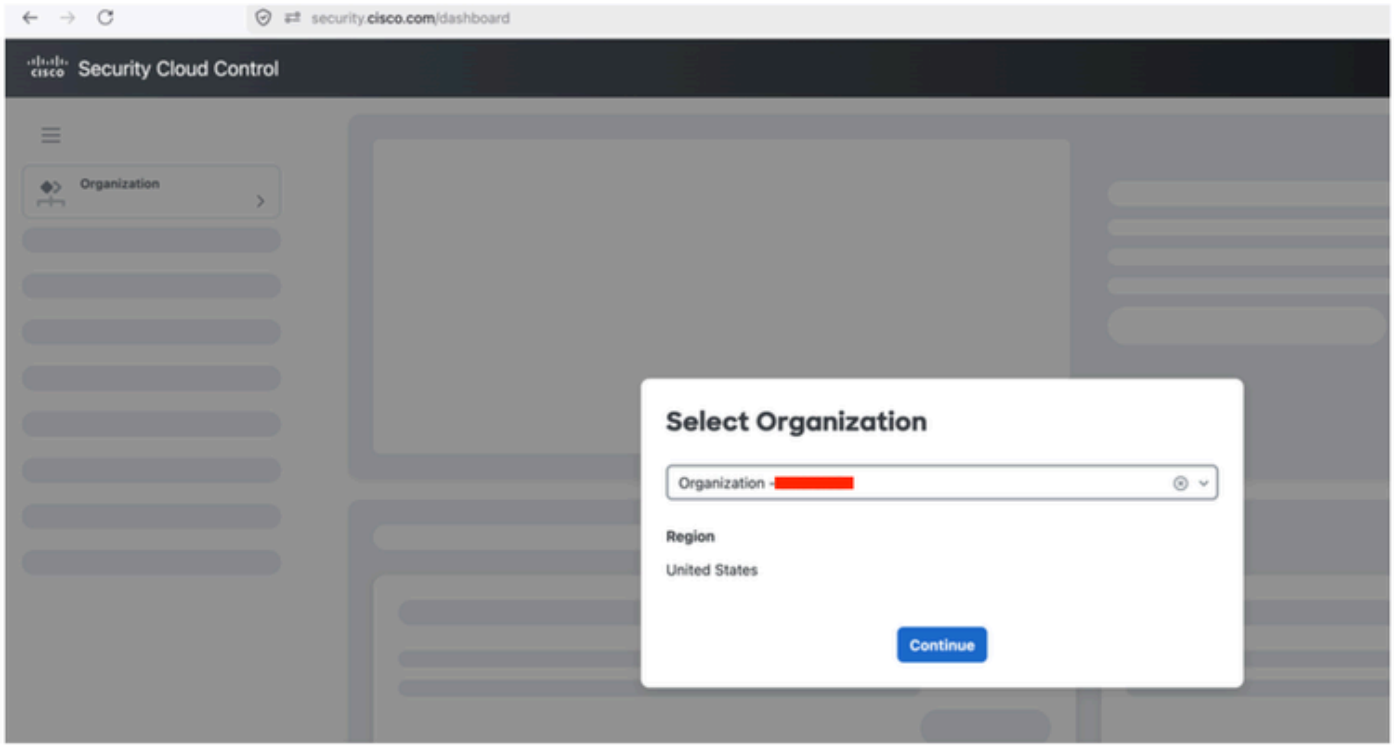


複製用於Cisco Secure Access的一次性密碼。

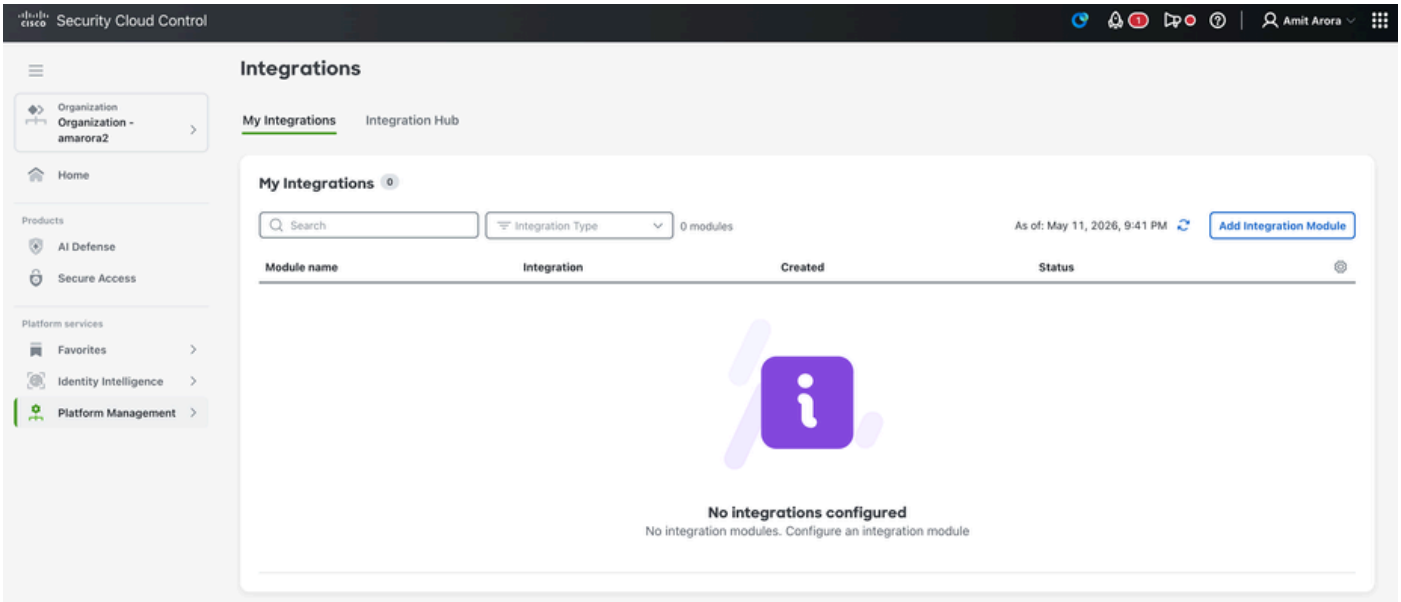


第2步：將思科安全訪問與ISE整合

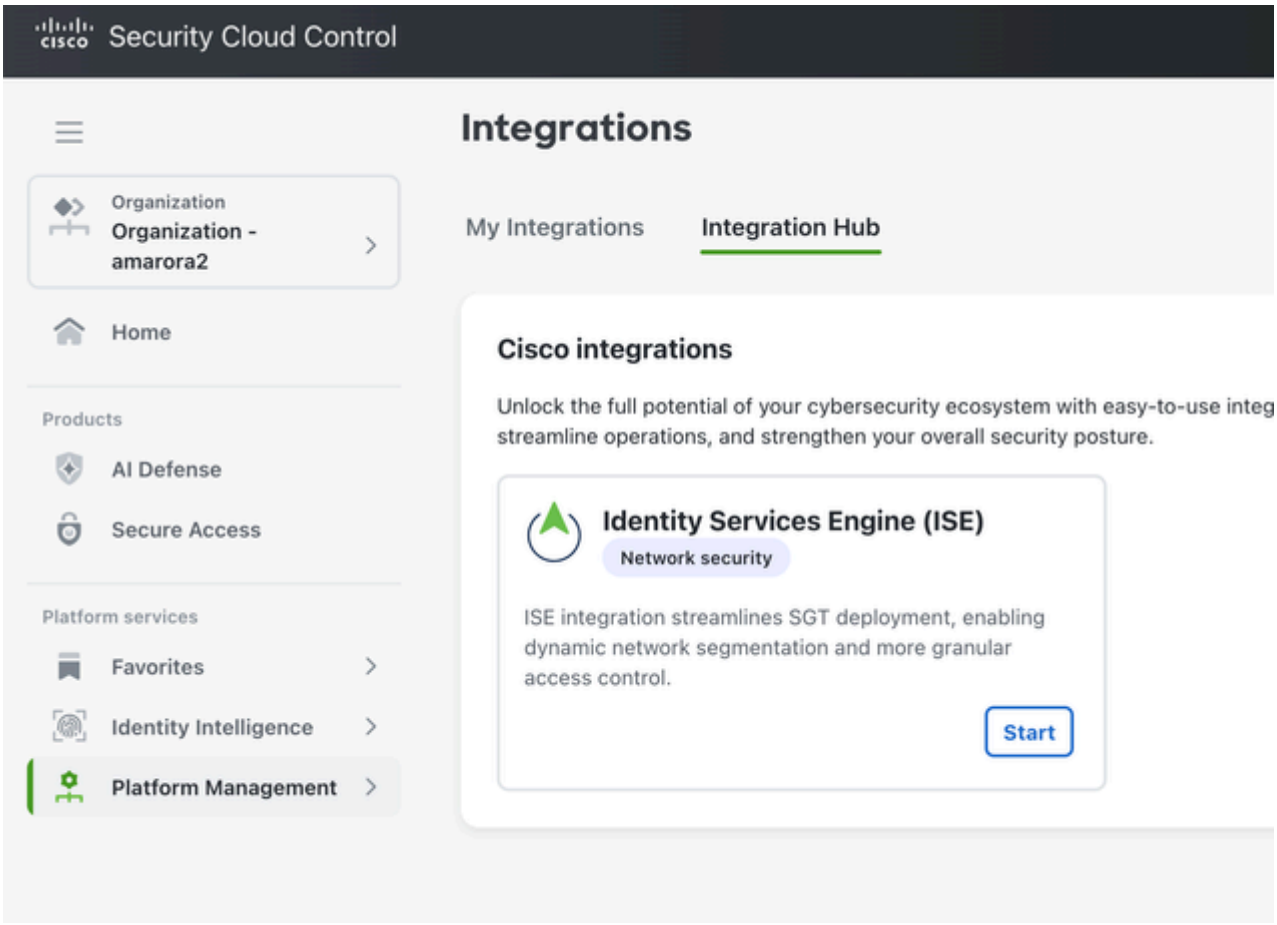
1. 登入security.cisco.com。
2. 選擇Cisco Secure Access ORG



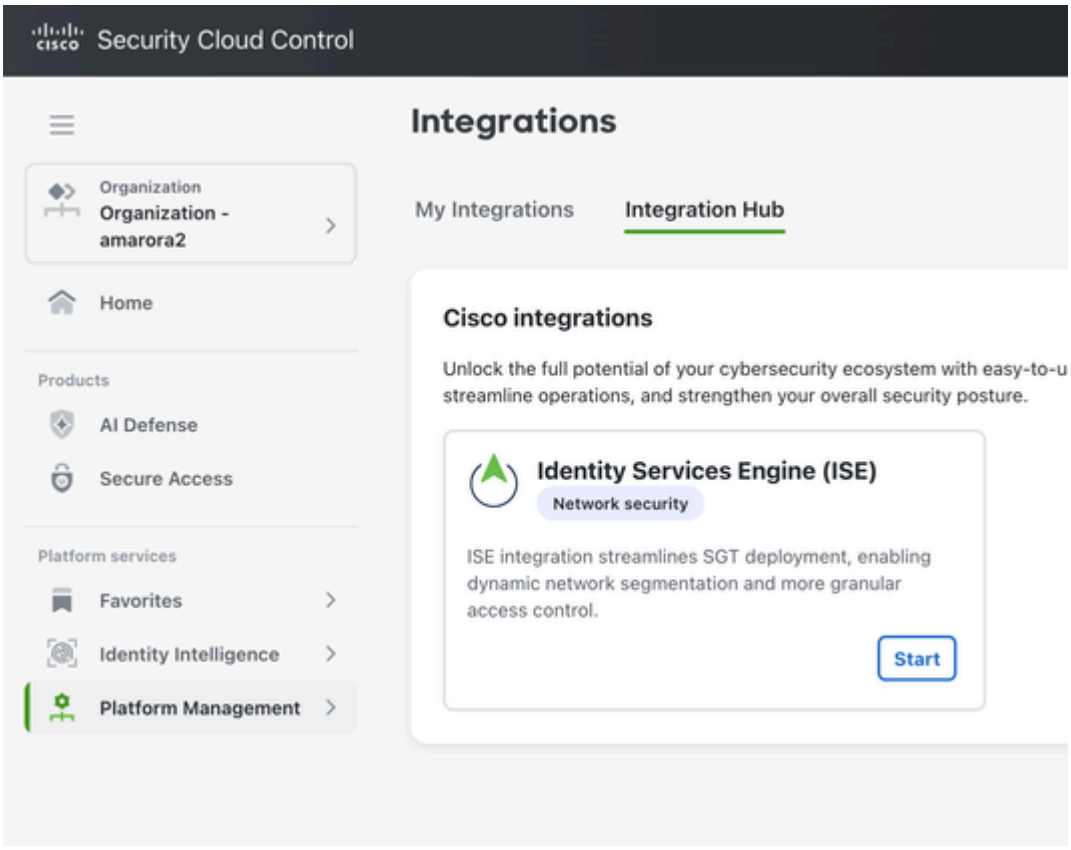
3點選「平台管理」—「平台整合」



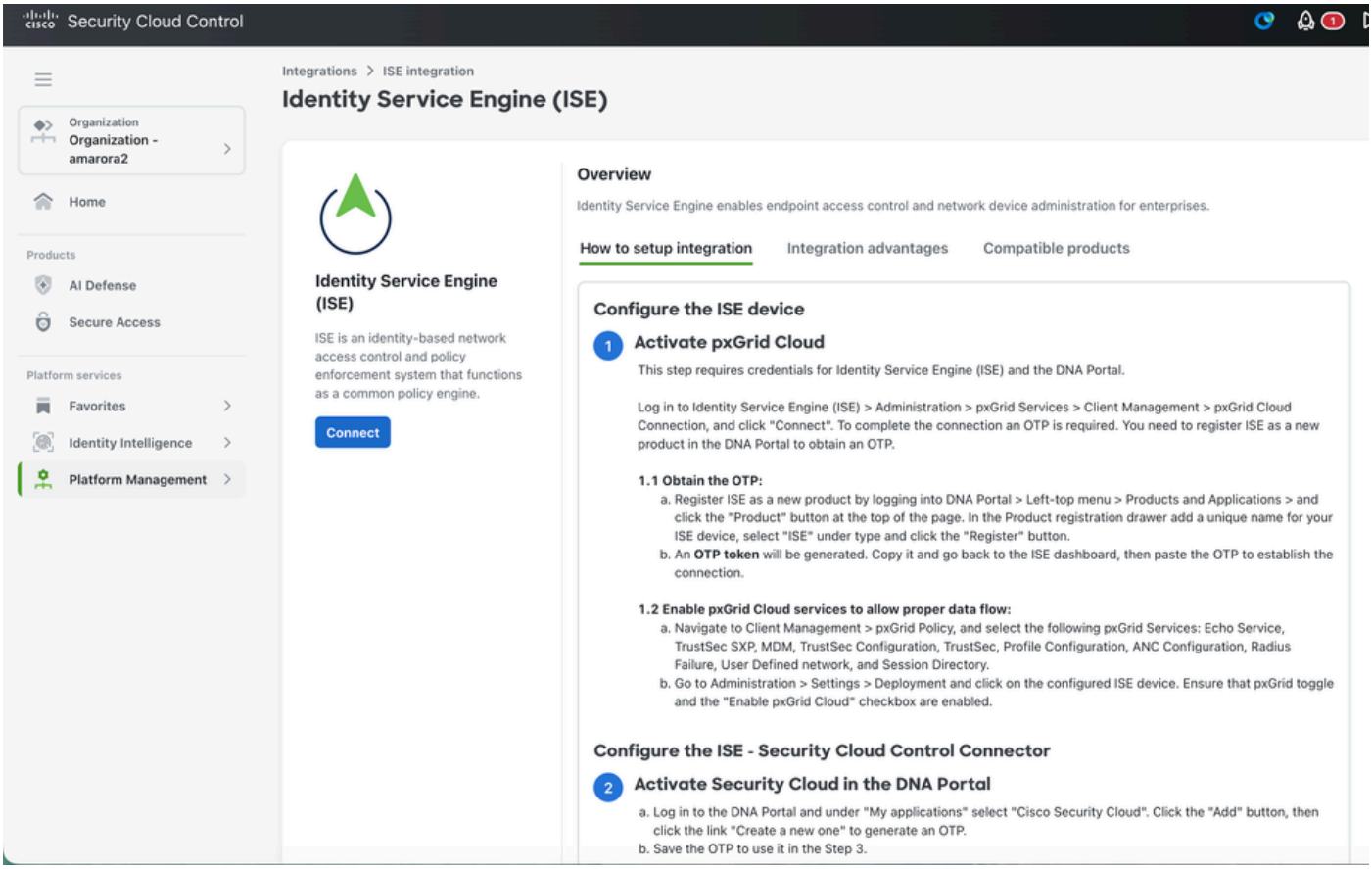
4點選Add Integration Module



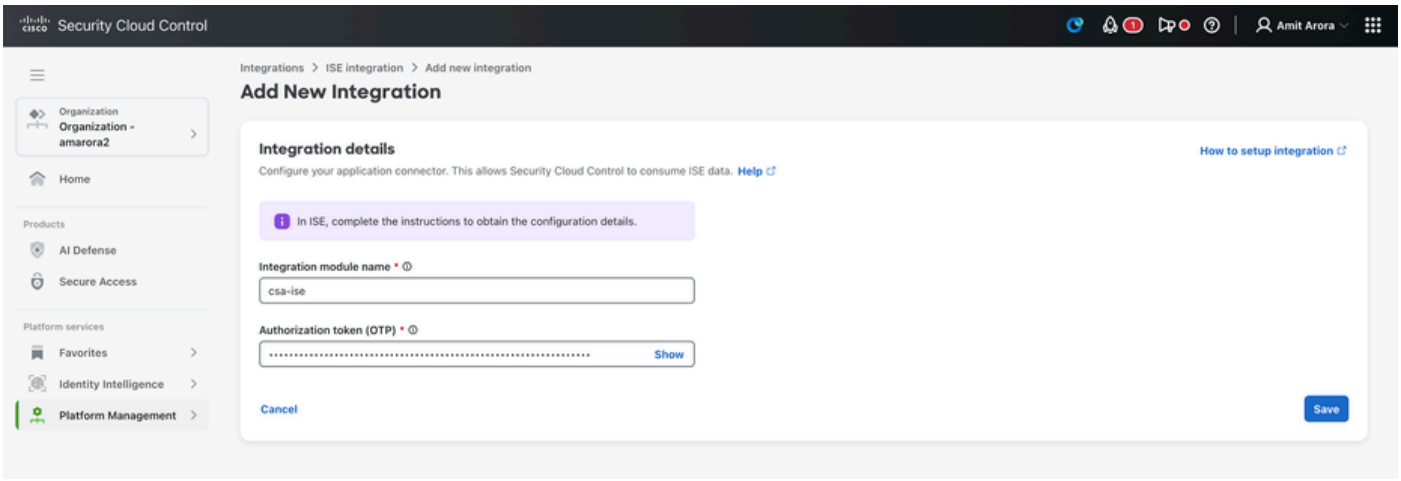
5按一下「Start（開始）」


Security Cloud Control
Integrations
Organization
Organization - amarora2
Home
Products
AI Defense
Secure Access
Platform services
Favorites
Identity Intelligence
Platform Management
My Integrations
Integration Hub
Cisco integrations
Unlock the full potential of your cybersecurity ecosystem with easy-to-u
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

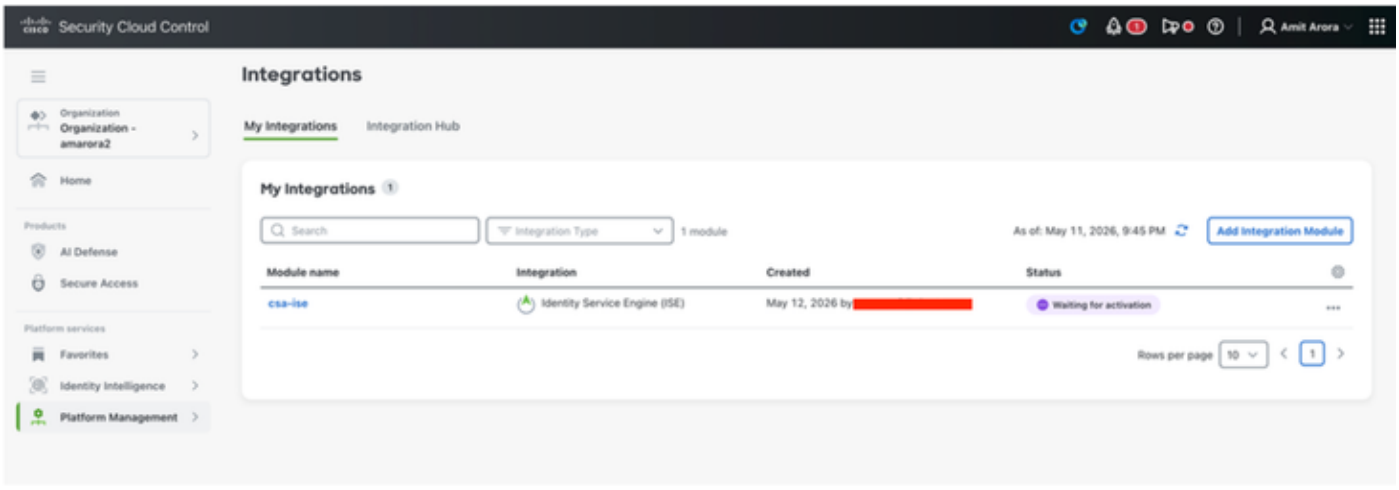
6按一下「連線」


Security Cloud Control
Integrations > ISE integration
Identity Service Engine (ISE)
Organization
Organization - amarora2
Home
Products
AI Defense
Secure Access
Platform services
Favorites
Identity Intelligence
Platform Management
Identity Service Engine (ISE)
ISE is an identity-based network access control and policy enforcement system that functions as a common policy engine.
Connect
Overview
Identity Service Engine enables endpoint access control and network device administration for enterprises.
How to setup integration
Integration advantages
Compatible products
Configure the ISE device
1 Activate pxGrid Cloud
This step requires credentials for Identity Service Engine (ISE) and the DNA Portal.
Log in to Identity Service Engine (ISE) > Administration > pxGrid Services > Client Management > pxGrid Cloud Connection, and click "Connect". To complete the connection an OTP is required. You need to register ISE as a new product in the DNA Portal to obtain an OTP.
1.1 Obtain the OTP:
a. Register ISE as a new product by logging into DNA Portal > Left-top menu > Products and Applications > and click the "Product" button at the top of the page. In the Product registration drawer add a unique name for your ISE device, select "ISE" under type and click the "Register" button.
b. An OTP token will be generated. Copy it and go back to the ISE dashboard, then paste the OTP to establish the connection.
1.2 Enable pxGrid Cloud services to allow proper data flow:
a. Navigate to Client Management > pxGrid Policy, and select the following pxGrid Services: Echo Service, TrustSec SXP, MDM, TrustSec Configuration, TrustSec, Profile Configuration, ANC Configuration, Radius Failure, User Defined network, and Session Directory.
b. Go to Administration > Settings > Deployment and click on the configured ISE device. Ensure that pxGrid toggle and the "Enable pxGrid Cloud" checkbox are enabled.
Configure the ISE - Security Cloud Control Connector
2 Activate Security Cloud in the DNA Portal
a. Log in to the DNA Portal and under "My applications" select "Cisco Security Cloud". Click the "Add" button, then click the link "Create a new one" to generate an OTP.
b. Save the OTP to use it in the Step 3.

7.輸入來自思科ISE的整合模組名稱和OTP，然後點選Save

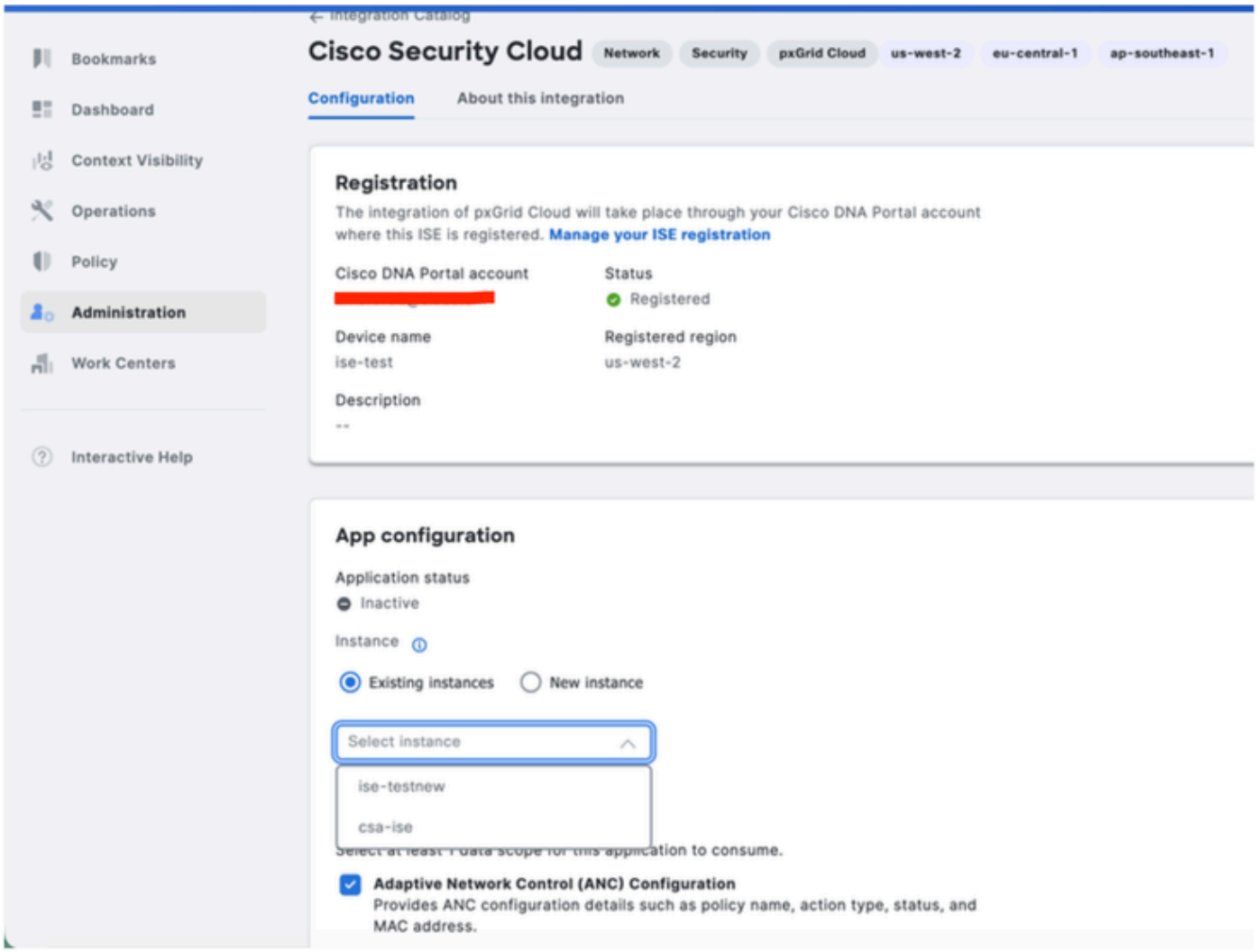


8按一下「儲存」後，我們將看到「等待啟用狀態」。

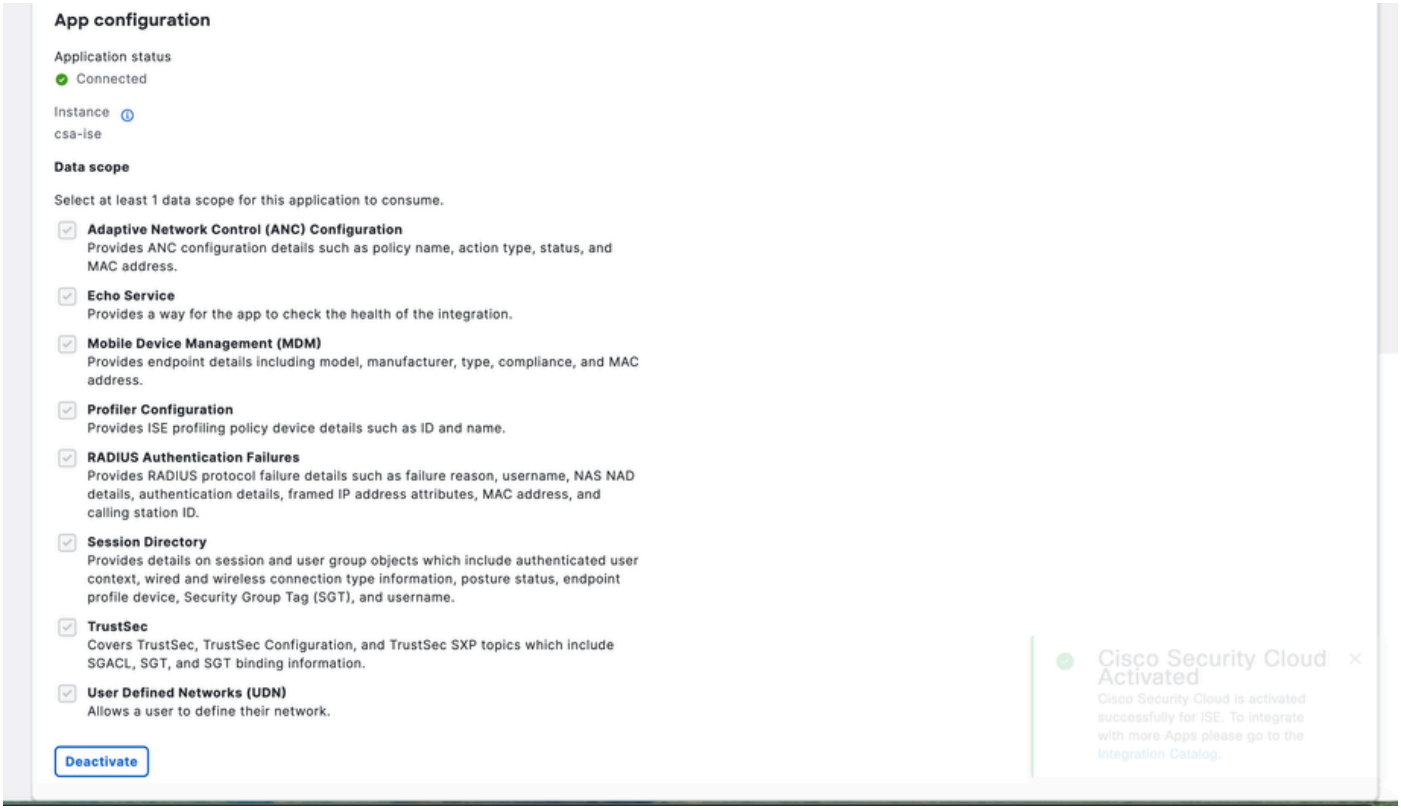


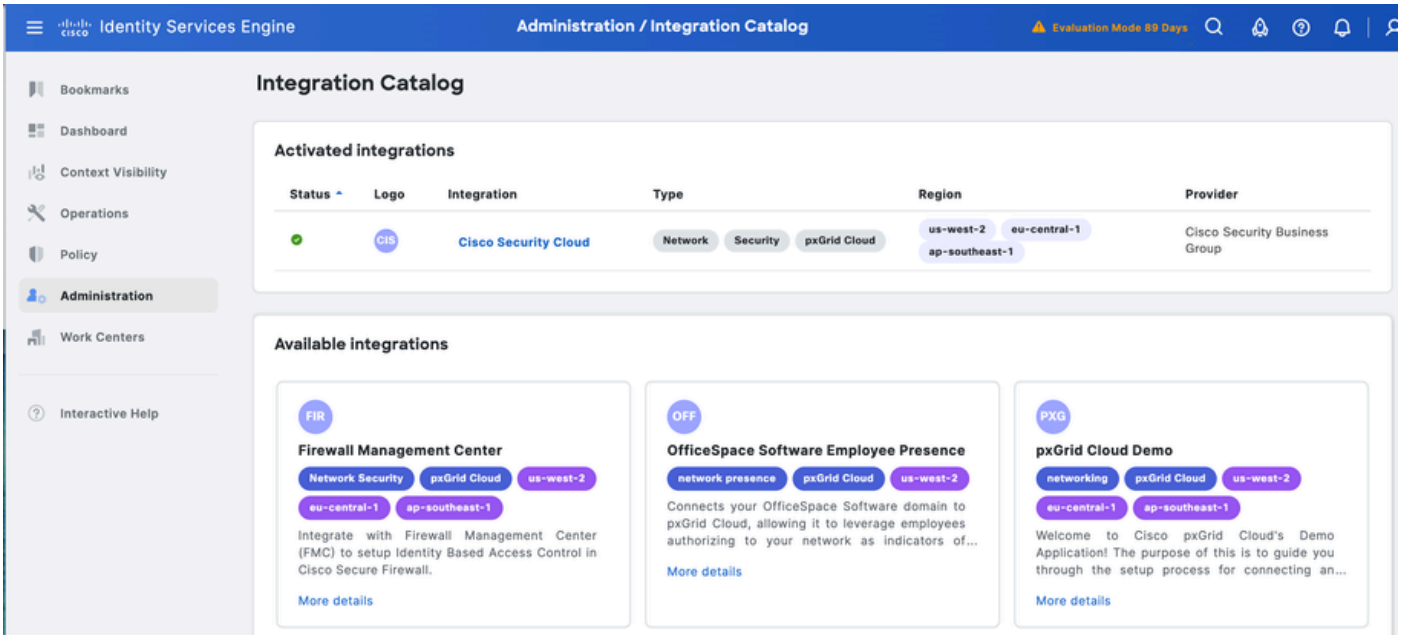
9登入到ISE並導航到Administration - Deployment。點選pxgrid角色的節點 — 點選Pxgrid Connection下的Integration cloud。

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）



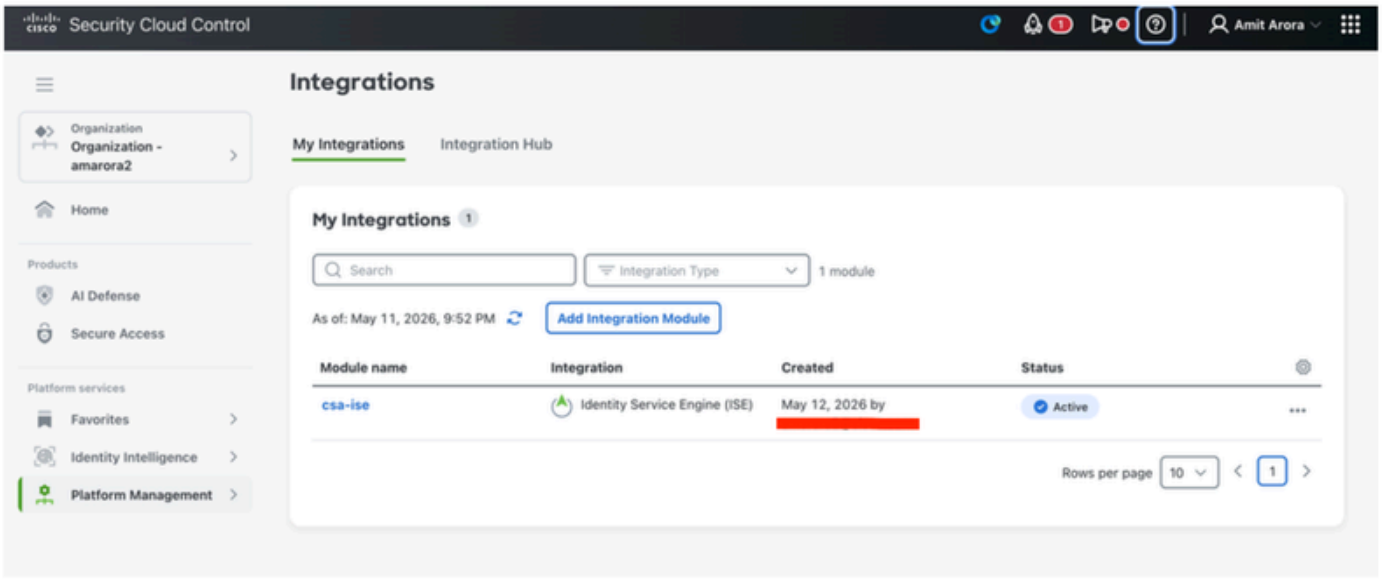
10應用狀態現在已連線。





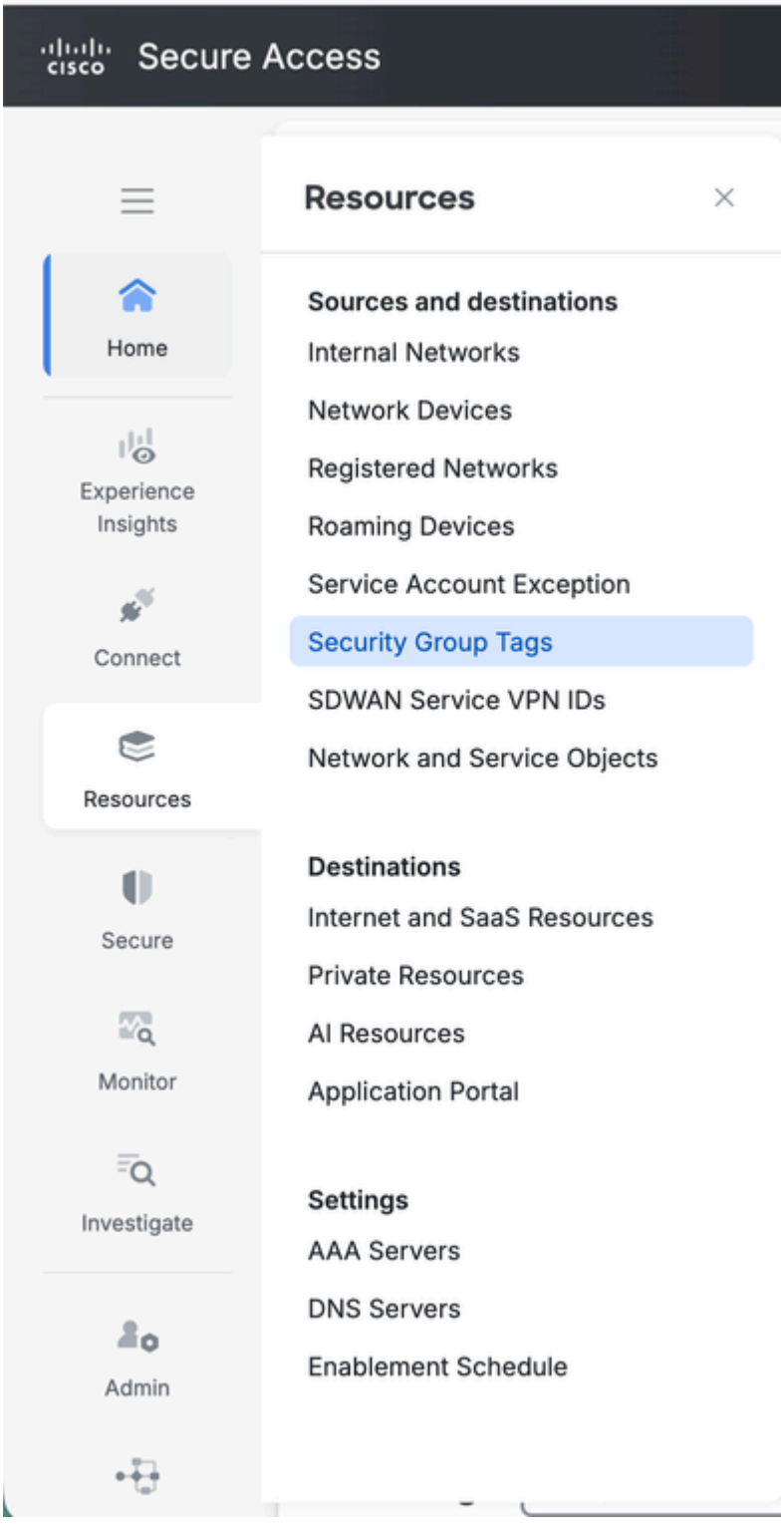
11登入到安全雲控制 — security.cisco.com

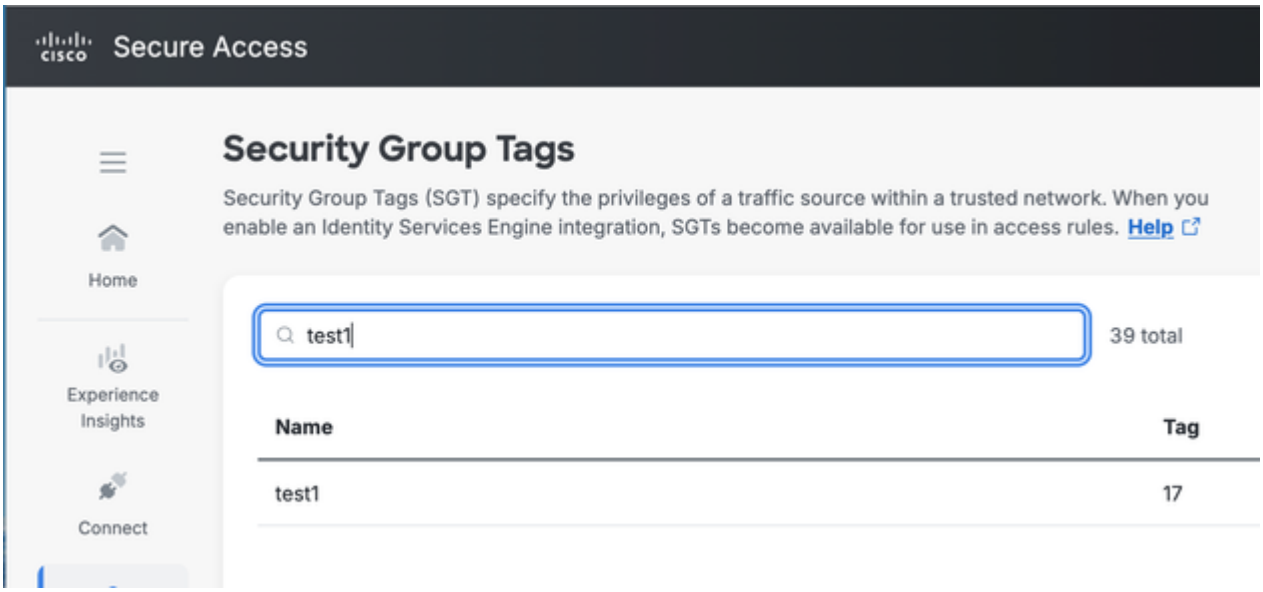
在Platform Management - Platform Integrations下，我們可以看到整合狀態為Active



驗證安全組標籤：

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


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



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

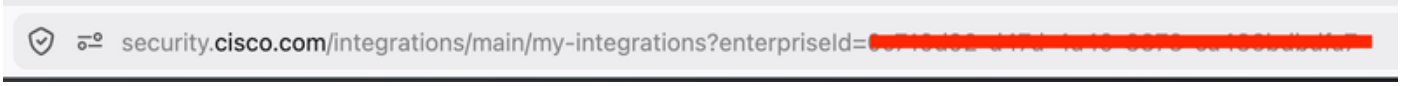
基礎設施

ERS

hermes元件處於調試級別。

SCC:

企業ID:在security.cisco.com的URL中

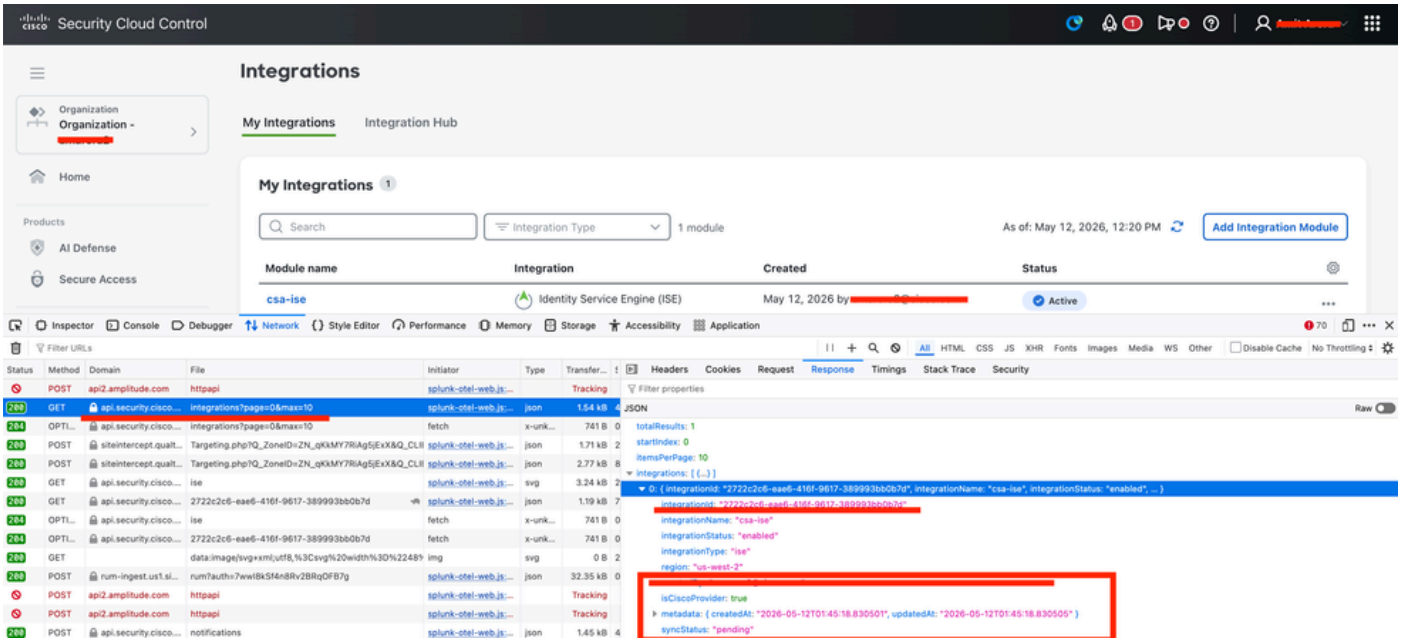


整合ID。

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。



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）。