

# 思科安全访问与ISE集成，用于通过Pxgrid云进行安全组标记

## 目录

---

---

## 简介

本文档介绍如何在思科安全访问和思科身份服务引擎之间启用情景共享

## 要求

思科建议您了解以下主题：

- 思科安全访问 — 基于云的安全服务边缘(SSE)解决方案，提供零信任网络访问，允许用户从任何设备轻松连接到互联网和私有应用。
- 思科身份服务引擎(ISE)版本3.4补丁5.
- 思科安全云控制 — 适用于您的安全云产品和身份的统一管理解决方案。安全访问包含安全云控制。

## 背景

通过这种集成，可以自动创建从Catalyst SD-WAN分支机构到Cisco Secure Access的可靠隧道，从而便于无缝交换VPN-ID/名称和SGT情景。

思科身份服务引擎(ISE)仍然是SGT配置和管理的主要机构。在ISE中执行的所有更新都会自动与思科安全访问同步。如果SGT被删除，引用它的现有规则将保持活动状态，以确保流量匹配按预期继续执行。

目前，我们为SGT映射提供有限的可用性，扩展了支持以将SGT目标对象包含在您的安全规则中。此外，即将推出对构建从Meraki和思科安全防火墙传输SGT的SASE隧道的支持

## 使用案例:

基于SGT名称空间的策略：

作为安全管理员，Kit希望使用来自本地ISE的SGT对SSE专用和互联网绑定的流量执行连续微分段。能够导入SGT以应用策略。



## 使用的组件

本文档中的信息基于：

- 身份服务引擎(ISE)版本3.4补丁5
- 安全访问
- 思科安全云

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 情景共享配置概述

- 将ISE连接到思科安全云
- 将思科安全访问连接到ISE

## 配置

本指南将整体配置分为以下主要步骤：

1. 将Cisco ISE连接到Cisco Security Cloud
2. 将思科安全访问连接到Cisco ISE
3. 思科安全访问中的安全组标记

## 开始使用前

- 确保您已在思科ISE部署中安装和激活优势许可证。
- DNA云代理创建与思科DNA云的出站HTTPS连接。因此，如果您的网络使用代理访问互联网，您必须配置思科ISE代理设置。要在Cisco ISE中配置代理设置，请导航至 **Administration > System > Settings > Proxy**
- 确保端口443为从Cisco ISE到Cisco pxGrid云门户的出站连接打开。如果配置了防火墙或代理设置，请确保这些URL未被阻止：

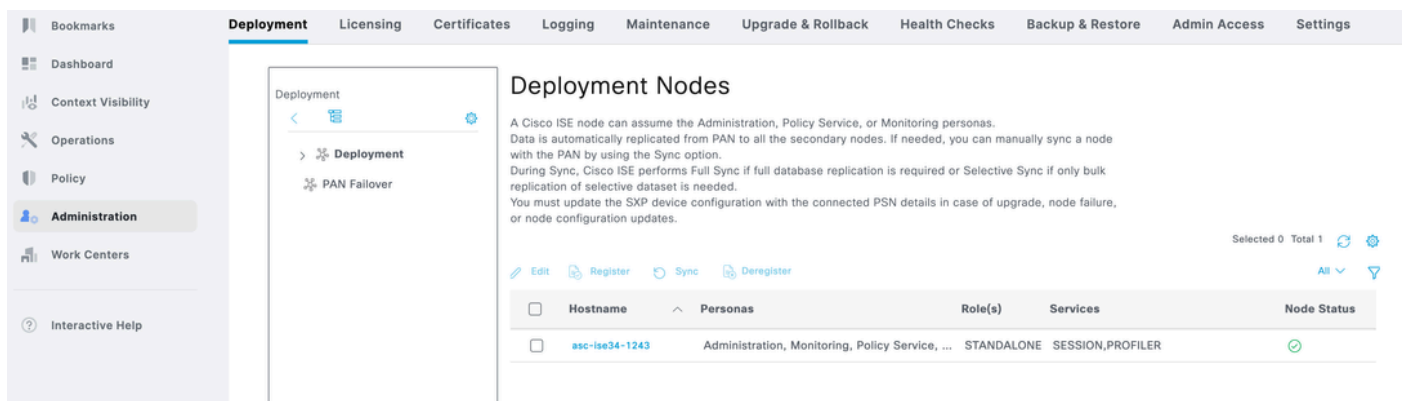
<https://dna.cisco.com>

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

## 第1步：在ISE上启用Pxgrid云

1导航到ISE GUI。

2点击Administration - Deployment。



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 shows a 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 the following data:

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

3单击节点并向下滚动到底部。

输入ISE部署名称

选择Region as US West 2，这是目前唯一支持的区域。

选中两个复选框并点击Register。

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Deployment Licensing Certificates Logging Maintenance Upgrade & Rollback Health Checks Backup & R

Enable Passive Identity Service ⓘ

pxGrid ⓘ

Enable pxGrid Cloud ⓘ

⚠ pxGrid Cloud can be enabled only after registering your Cisco ISE to your Cisco DNA Portal account.

ISE deployment name

ise-test

Description (optional)

Select a region where you want to register your device. Application should also be available in the same region.

Region

us-west-2

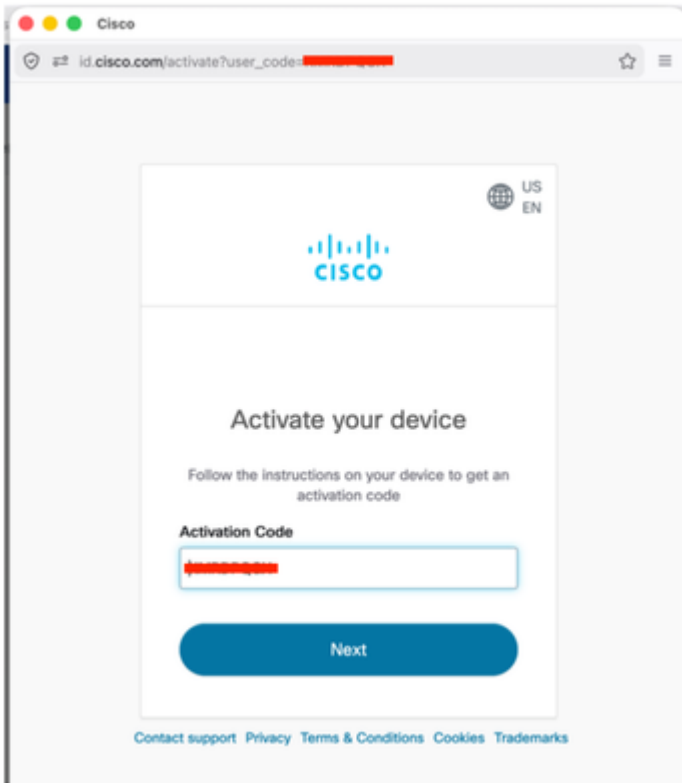
Check the checkboxes below to register this ISE if you concur with the statements.

I have read and acknowledge the [Cisco Privacy Statement](#).

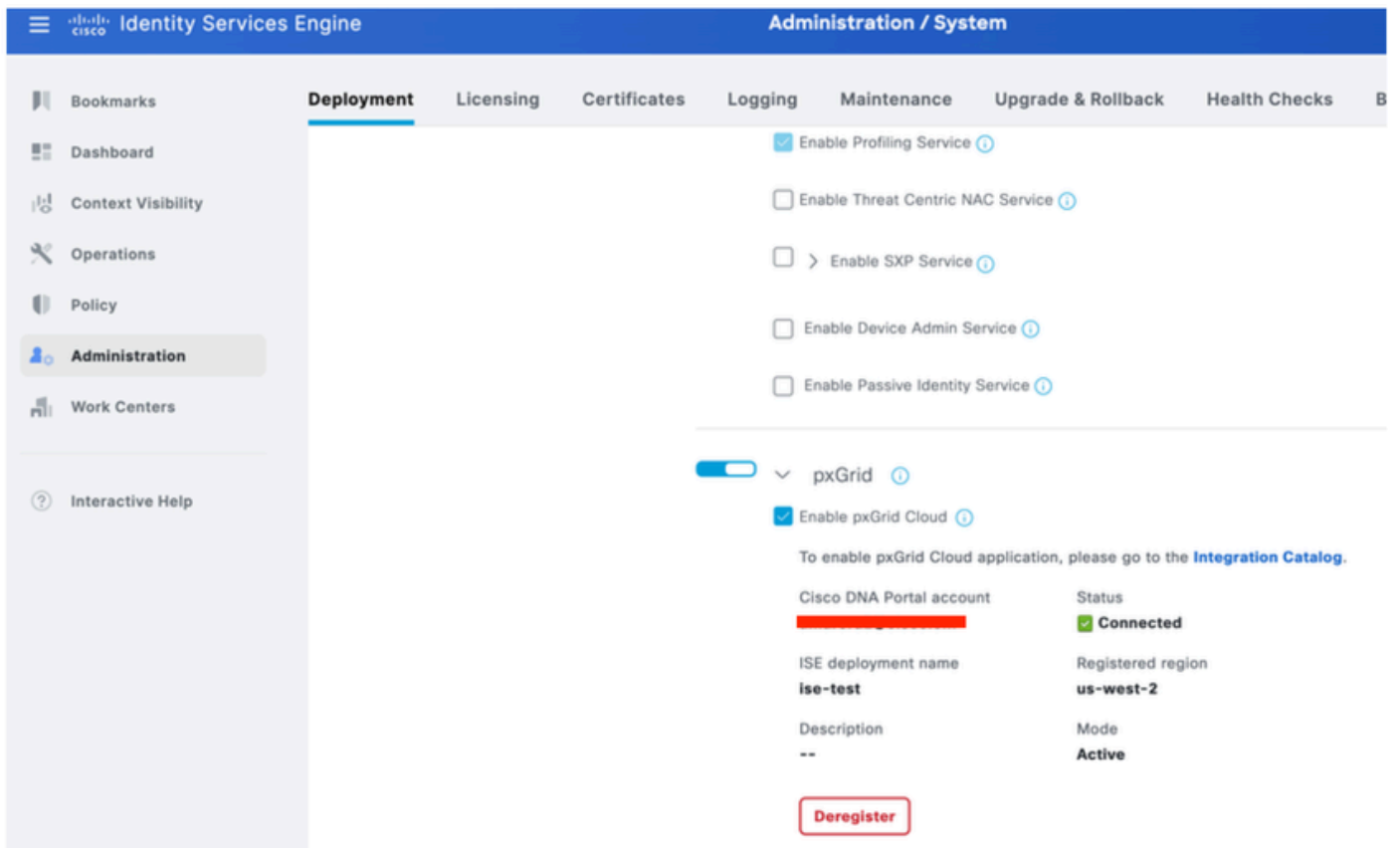
I agree that offers are governed by Cisco EULA and I am an authorized agent of my company. [Cisco's End User License Agreement](#).

Register

4您将看到一个包含自动填充激活代码的弹出窗口。单击“下一步”，

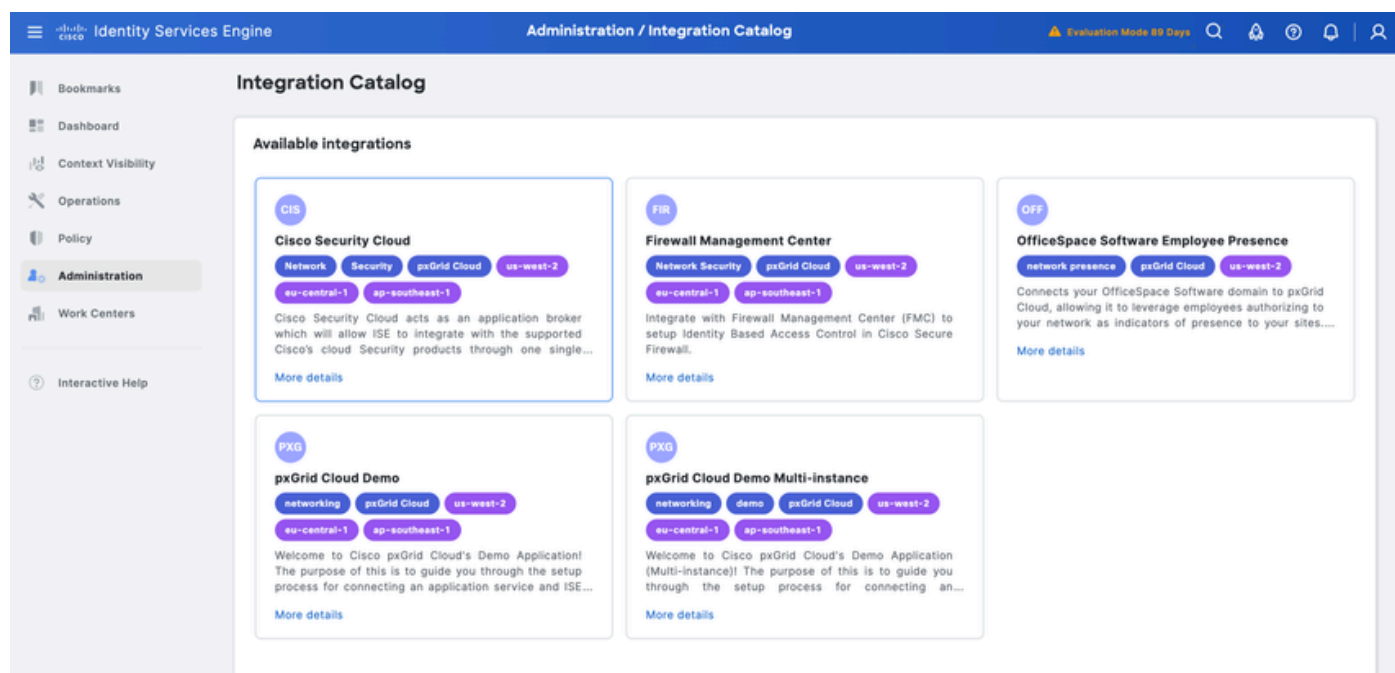


5个ISE将显示已连接到Pxgrid云。



6单击第5步中的Integration Catalog ( 集成目录 ) 链接。

在“可用集成”(Available Integrations)下 — 点击思科安全云(Cisco Security Cloud)



7在App Configuration下，点击New Instance，然后点击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.

复制用于Cisco Secure Access的一次性密码。

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](#) 

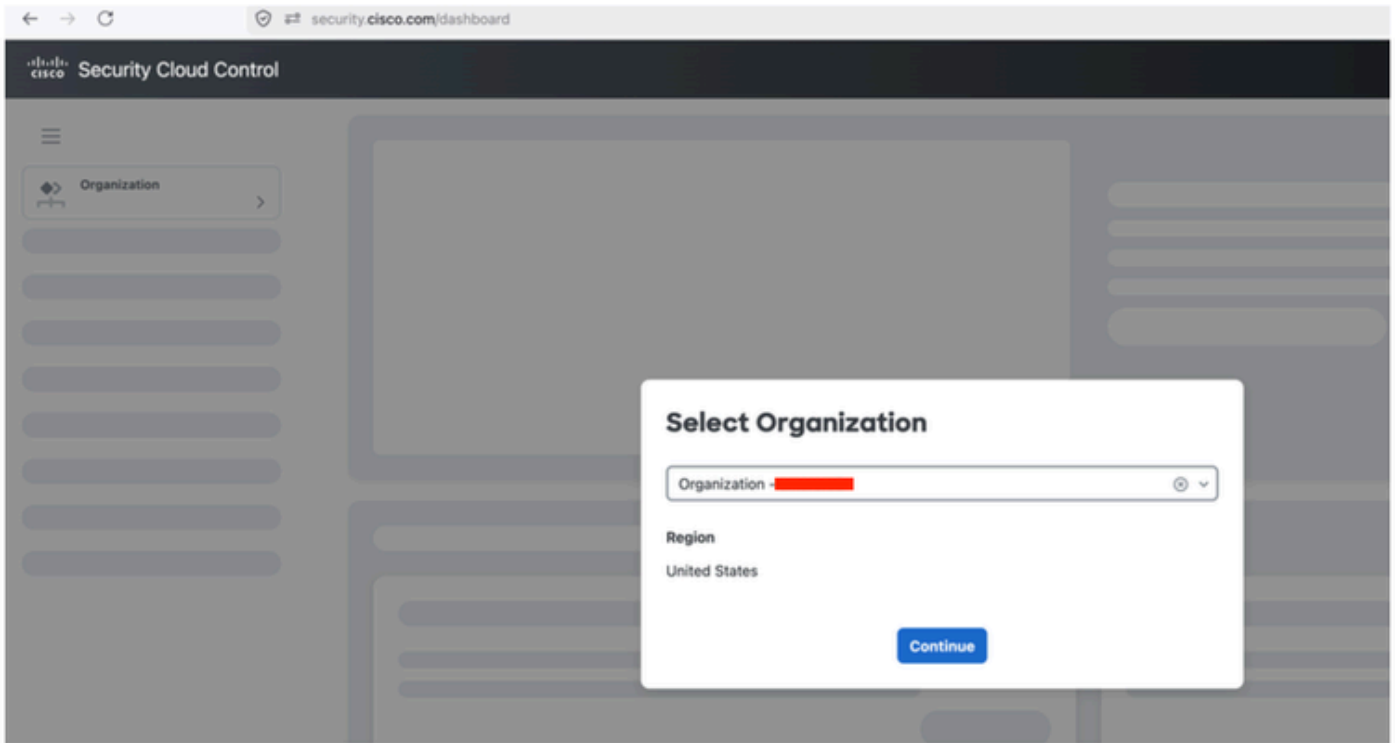
One-time password

  **Copy**

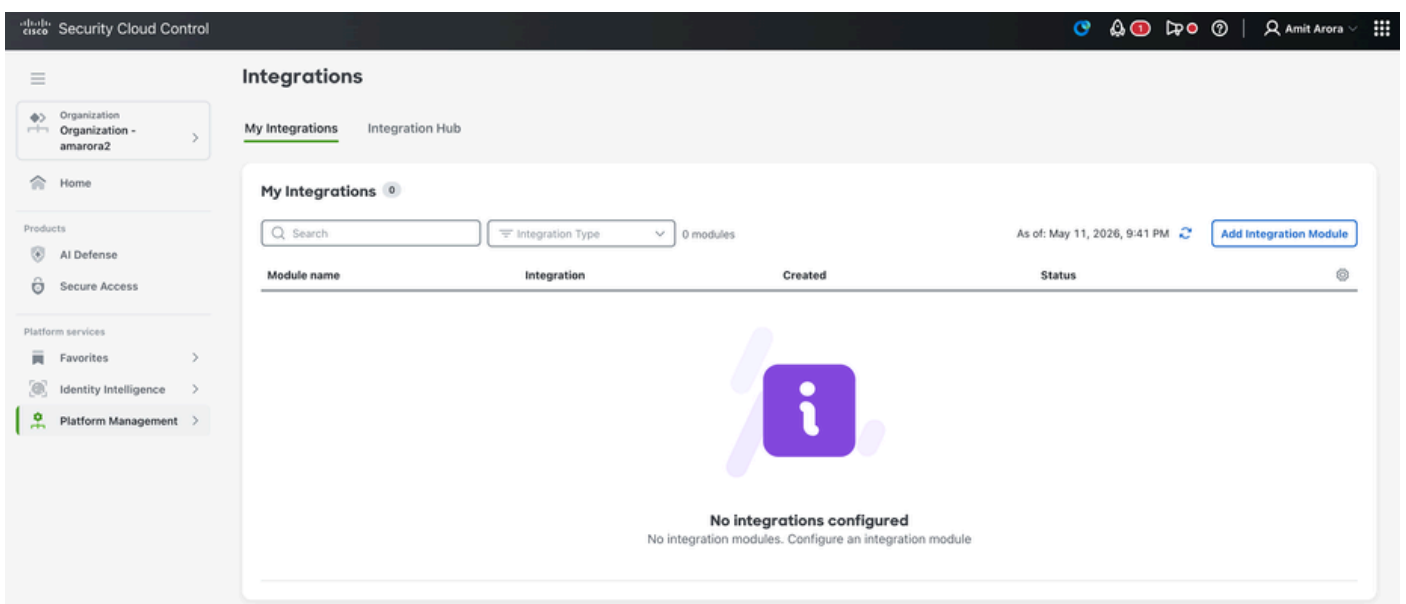
**OK**

### 步骤2:将思科安全访问与ISE集成

1. 登录security.cisco.com。
2. 选择思科安全访问组织



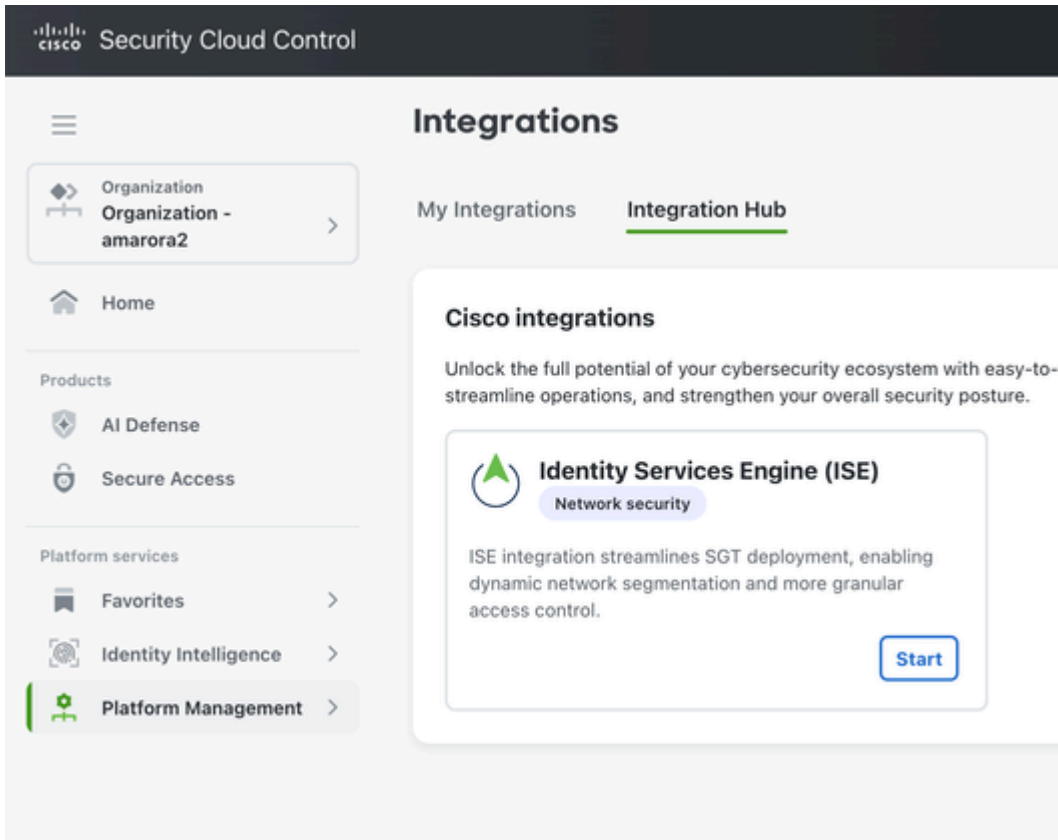
3. 点击“平台管理” — “平台集成”



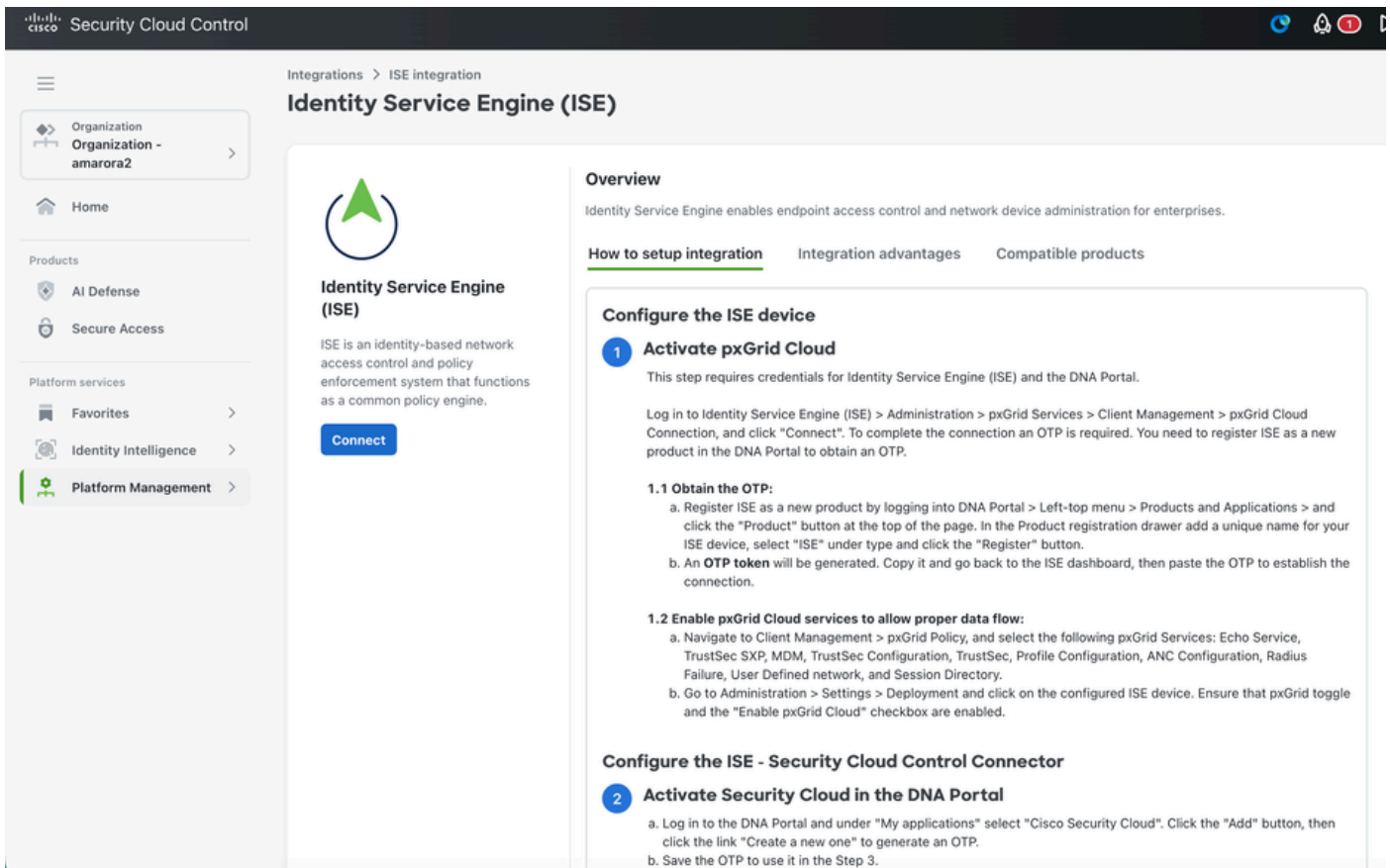
4 点击 Add Integration Module

The screenshot displays the Cisco Security Cloud Control interface. The top navigation bar includes the Cisco logo and the text "Security Cloud Control". A left-hand navigation menu contains a hamburger menu 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 features two tabs: "My Integrations" and "Integration Hub". The "Integration Hub" tab is active. Below the tabs, a "Cisco integrations" section provides a brief overview: "Unlock the full potential of your cybersecurity ecosystem with easy-to-use integ streamline operations, and strengthen your overall security posture." A prominent card for "Identity Services Engine (ISE)" is displayed, categorized under "Network security". The card includes a description: "ISE integration streamlines SGT deployment, enabling dynamic network segmentation and more granular access control." and a blue "Start" button.

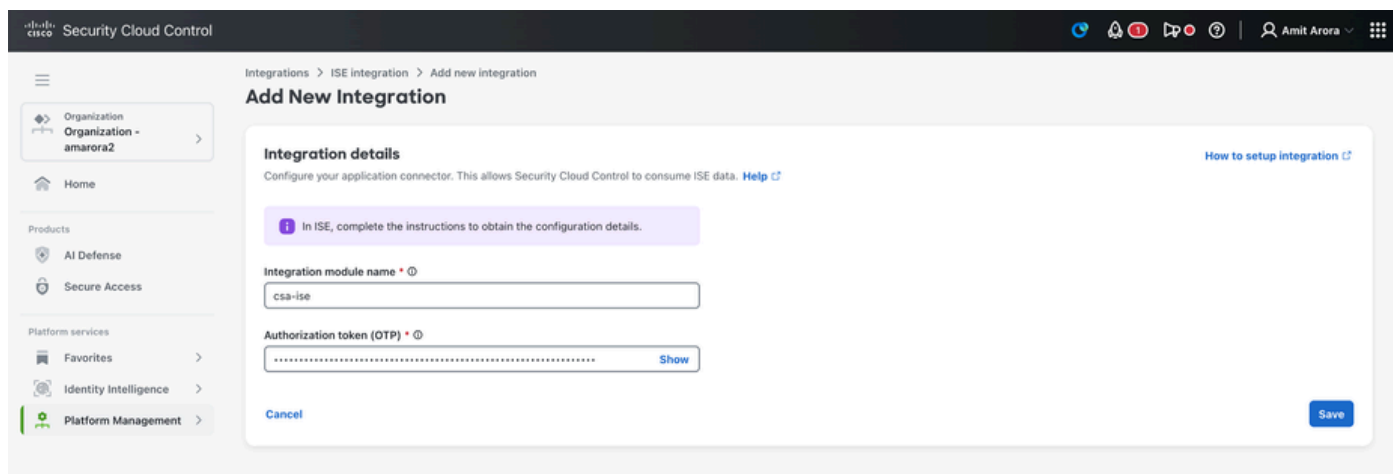
5 单击“Start ( 开始 )”



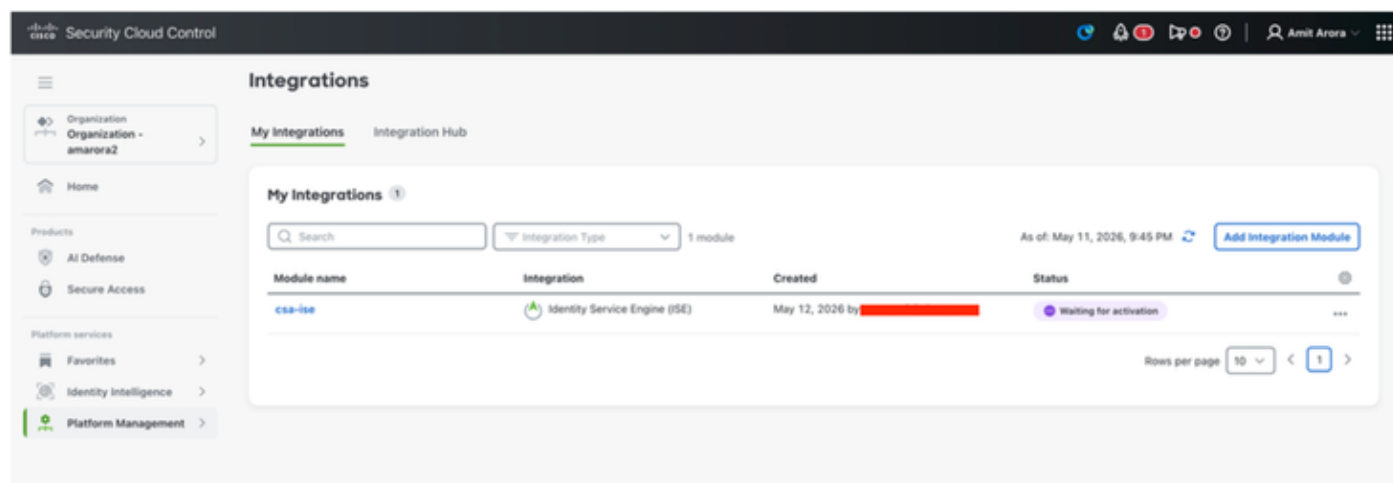
6. 点击Connect



7.从Cisco ISE输入集成模块名称和OTP，然后点击Save



8.点击Save后，我们将看到Waiting for Activation Status。



9.登录到ISE并导航到Administration - Deployment。点击pxgrid角色的节点 — 点击Pxgrid Connection下的Integration cloud。

在App configuration — 选择在Security Cloud Control上创建的ISE实例，然后点击Activate

← 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应用状态现已连接。

## 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 登录安全云控制 — security.cisco.com

在“平台管理 — 平台集成”下，我们可以看到集成状态为“活动”

The screenshot displays the Cisco Security Cloud Control interface. The top navigation bar shows the Cisco logo, the text "Security Cloud Control", and user information "Amit Arora". The main content area is titled "Integrations" and includes a sub-section "My Integrations" with a refresh icon and a timestamp "As of: May 11, 2026, 9:52 PM". A search bar and a filter for "Integration Type" are present, along with a button to "Add Integration Module". Below this is a table listing integration modules:

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

The table also includes a "Rows per page" selector set to 10 and a page indicator showing 1 of 1 pages.

验证安全组标记：

登录到Cisco Secure Access。导航至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

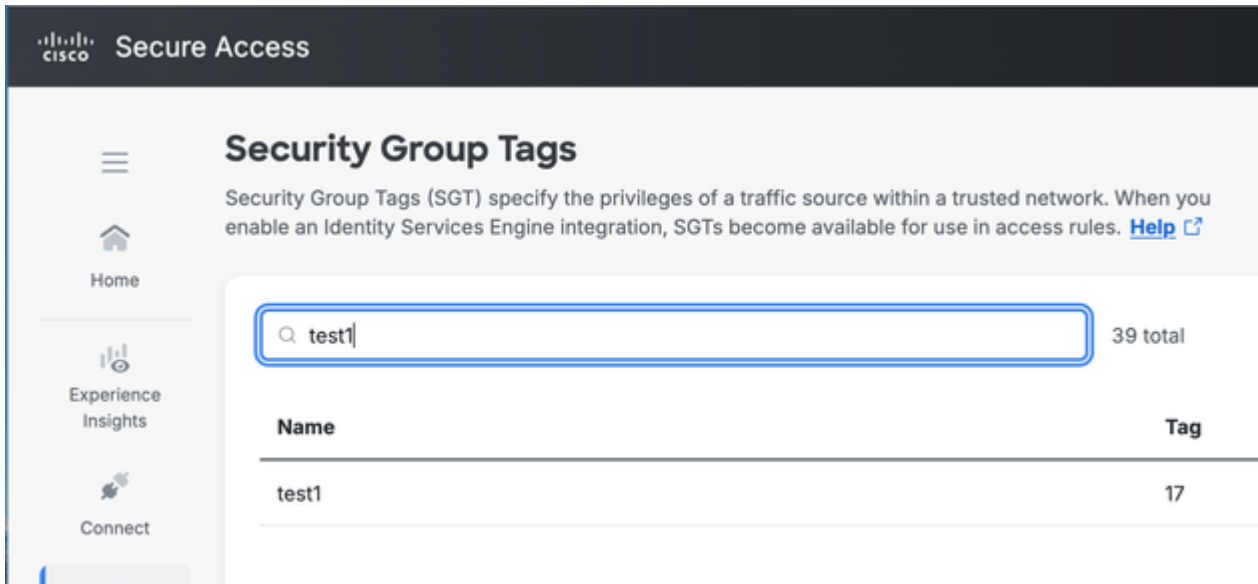
Application Portal

### Settings

AAA Servers

DNS Servers

Enablement Schedule



## Cisco TAC所需信息

ISE:

[如何收集具有以下组件](#)的ISE支持捆绑包，这些组件在具有Pxgrid角色的ISE节点上设置为调试级别：

pxgrid

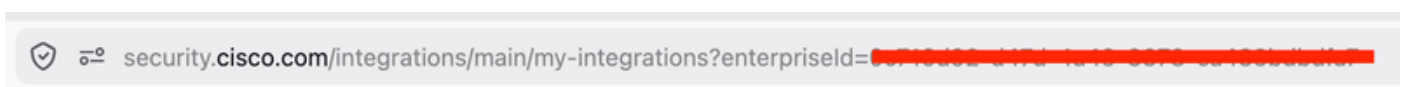
基础设施

ERS

hermes组件处于调试级别。

SCC:

企业ID:在security.cisco.com的URL中



集成ID。  
开始[HAR捕获](#)

登录Security.cisco.com  
导航至“平台管理” — “平台集成”

搜索集成？页面api调用，并在响应选项卡中找到集成ID。

The screenshot shows the Cisco Security Cloud Control interface. The top navigation bar includes the Cisco logo and "Security Cloud Control". The main content area is titled "Integrations" and shows "My Integrations" with a table listing integration details. The table has columns for "Module name", "Integration", "Created", and "Status". One integration is listed: "csa-ise" with the integration name "Identity Service Engine (ISE)", created on "May 12, 2026", and status "Active".

Below the integrations table, a HAR capture tool is open, showing a list of network requests. The "Response" tab is selected, displaying the JSON response for a GET request to "api.security.cisco.com/integrations?page=0&max=10". The response is a JSON object with the following structure:

```
{
  "integrations": [
    {
      "integrationId": "2722c2c6-ee6f-416f-9617-389993bb0b7d",
      "integrationName": "csa-ise",
      "integrationStatus": "enabled",
      "region": "us-west-2"
    }
  ]
}
```

The response is highlighted with a red box, and the "integrationId" and "integrationName" fields are also highlighted with a red box.

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。