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：

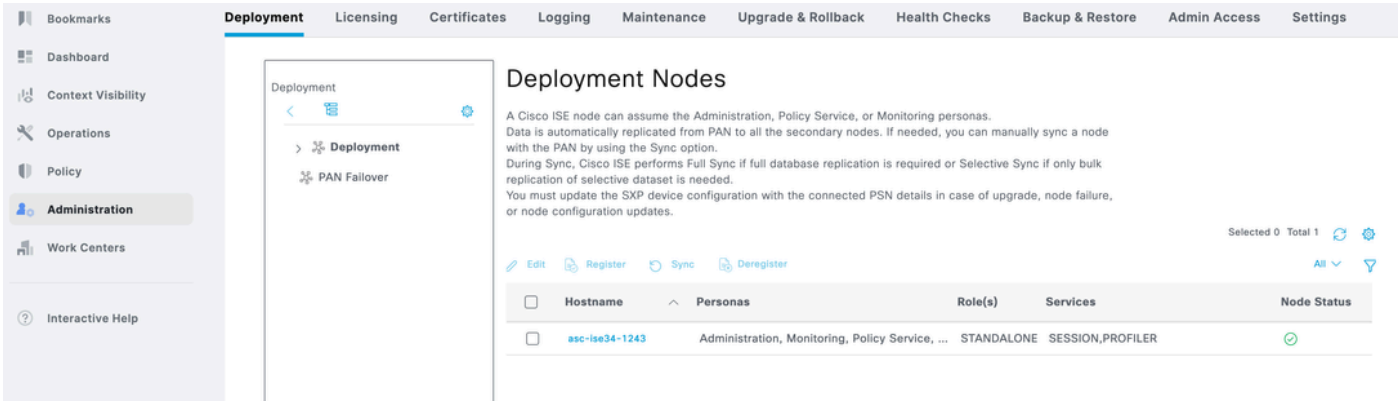
https://dna.cisco.com

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。

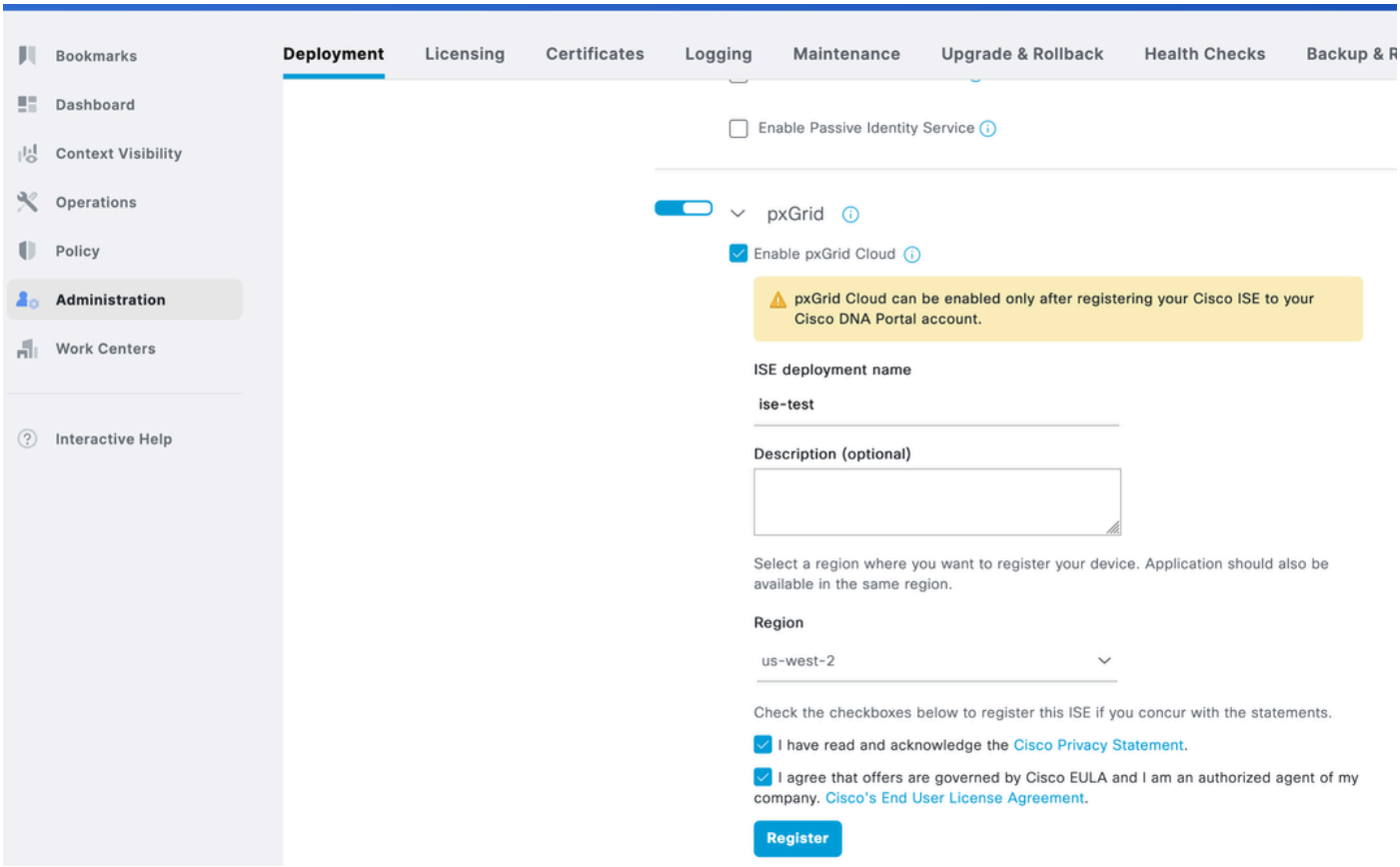


3单击节点并向下滚动到底部。

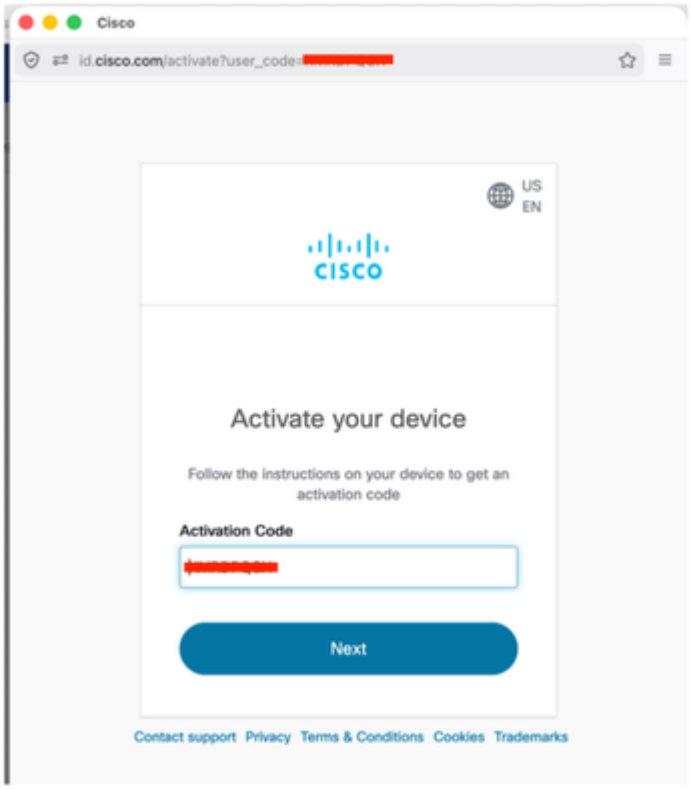
输入ISE部署名称

选择Region as US West 2，这是目前唯一支持的区域。

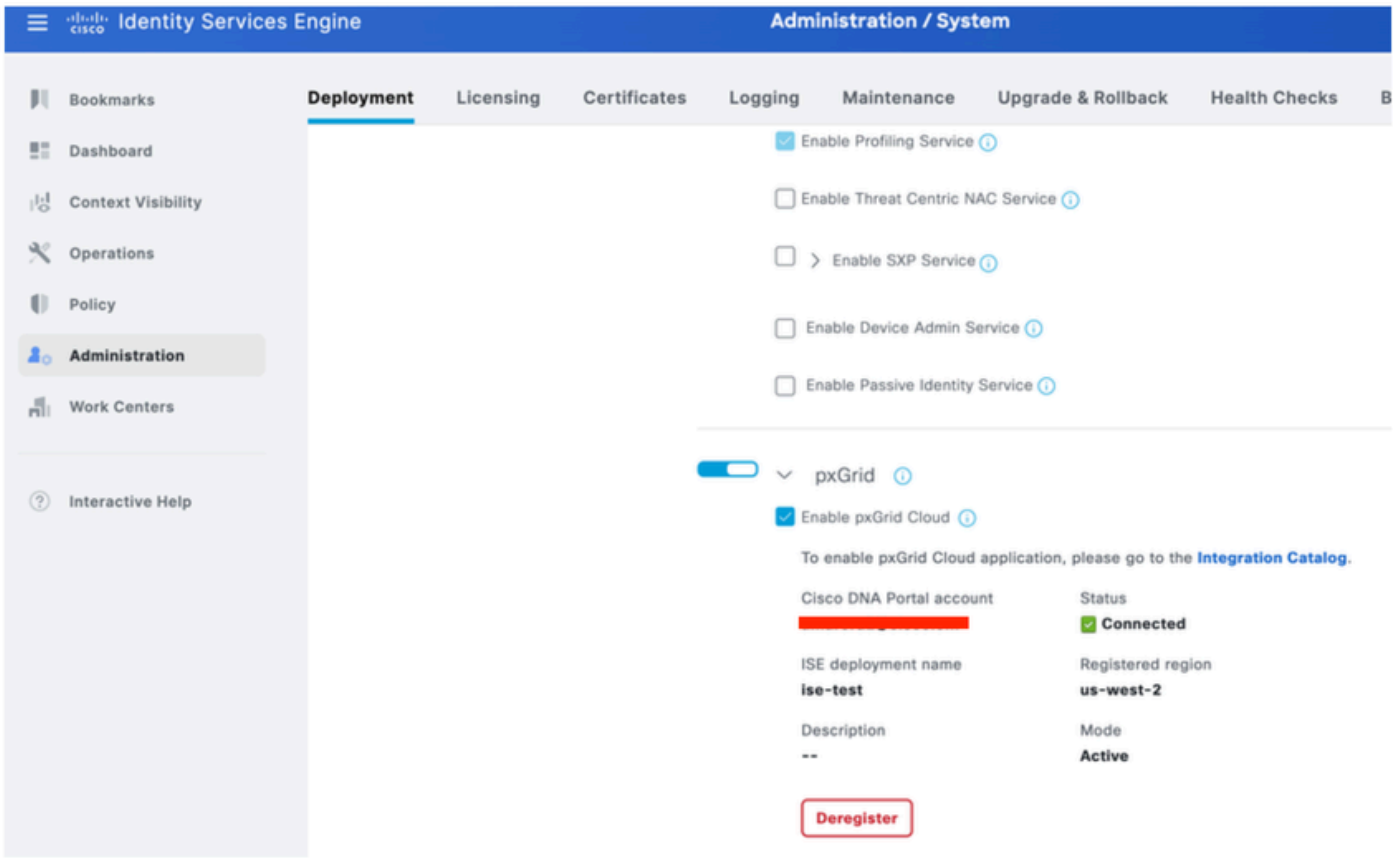
选中两个复选框并点击Register。



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”，



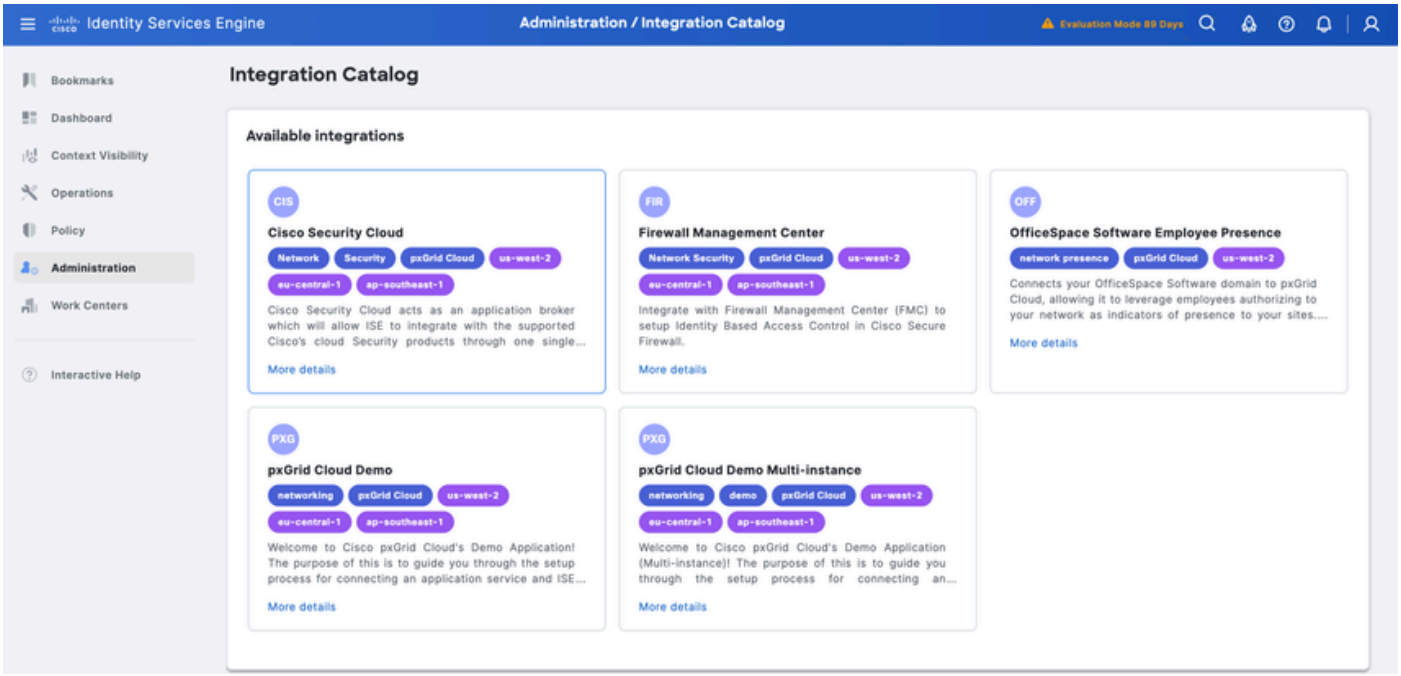
5个ISE将显示已连接到Pxgrid云。



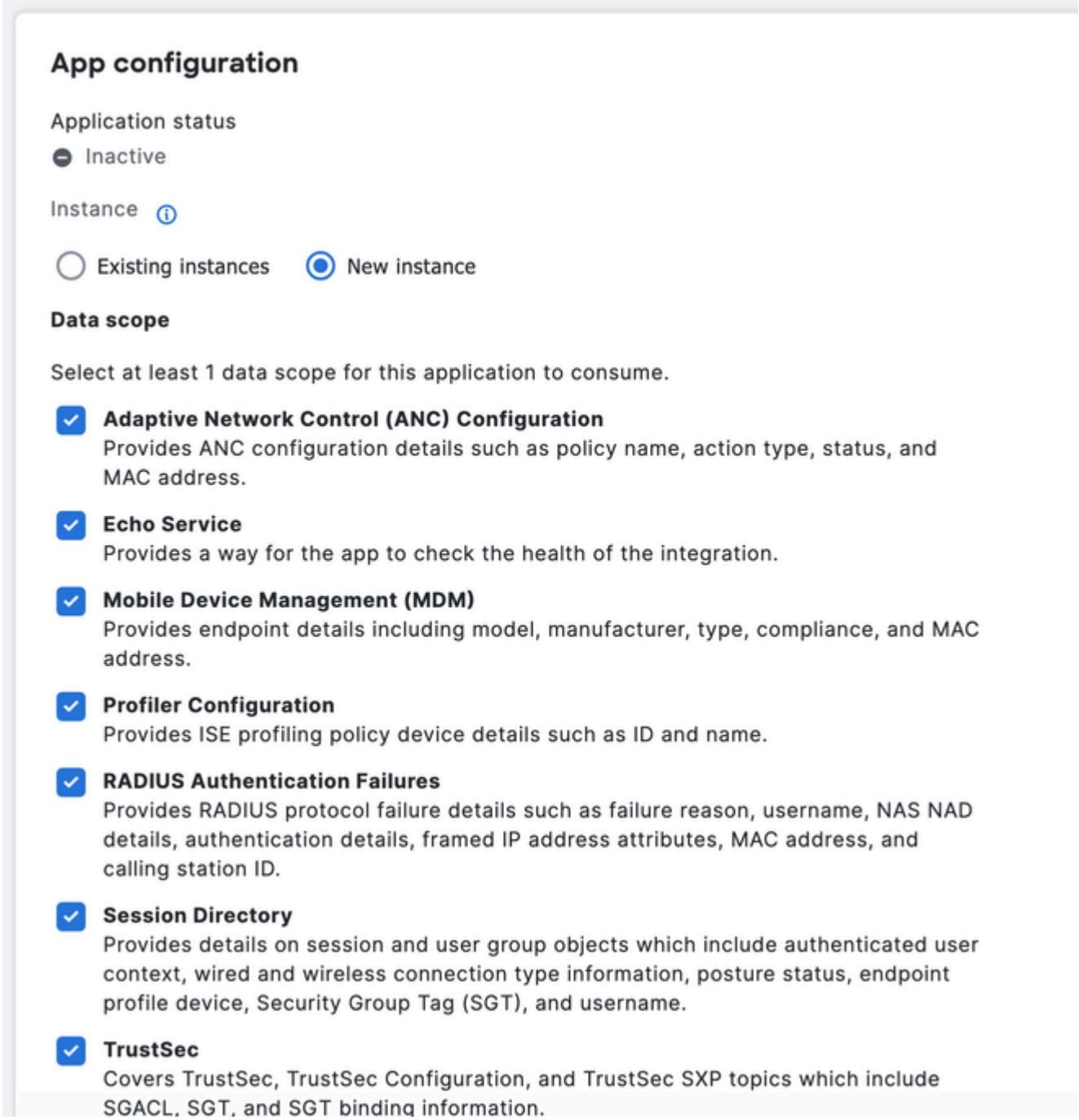
6单击第5步中的Integration Catalog（集成目录）链接。

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

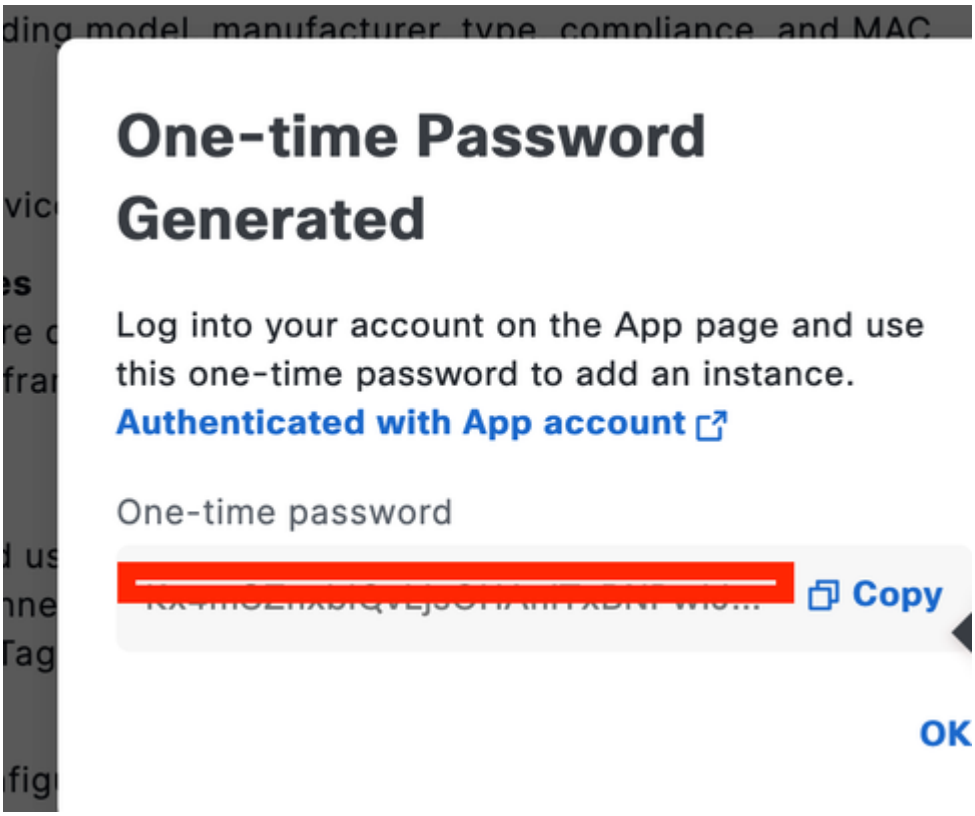
.



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

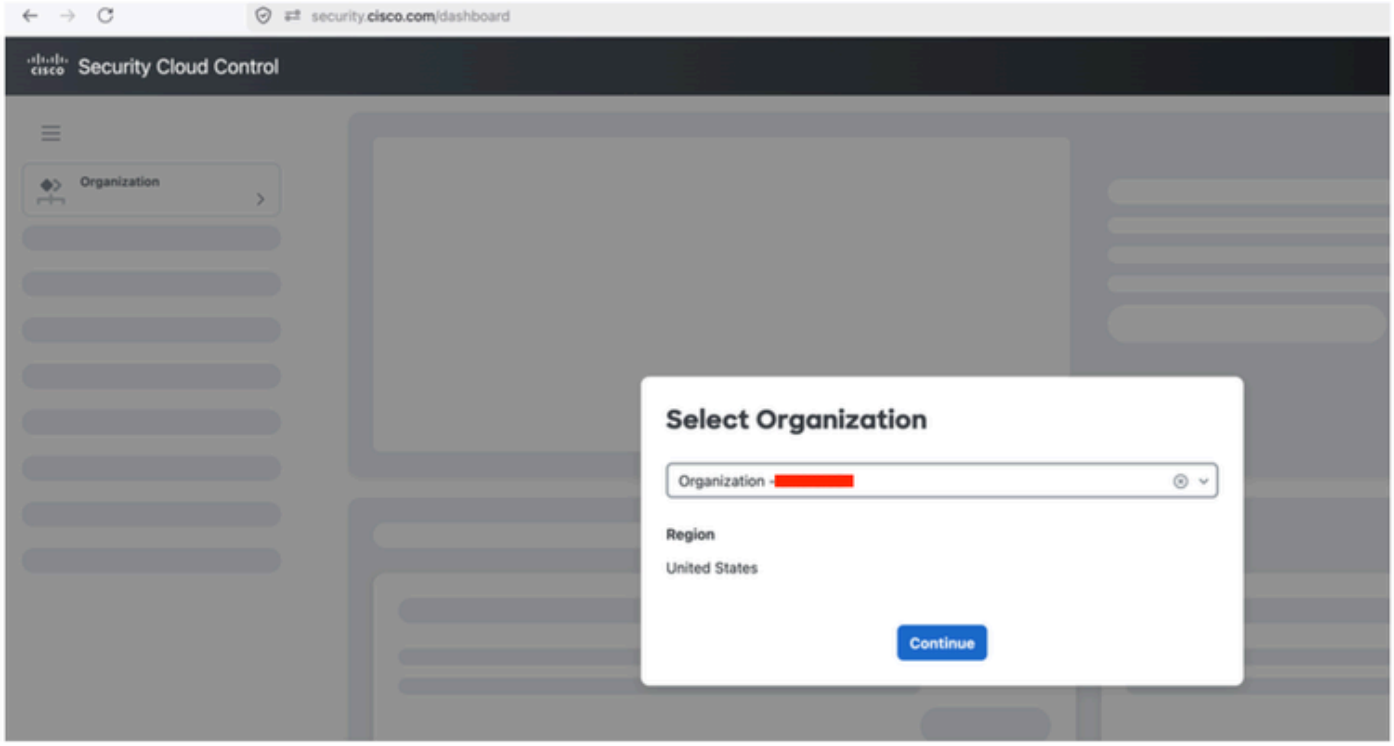


复制用于Cisco Secure Access的一次性密码。

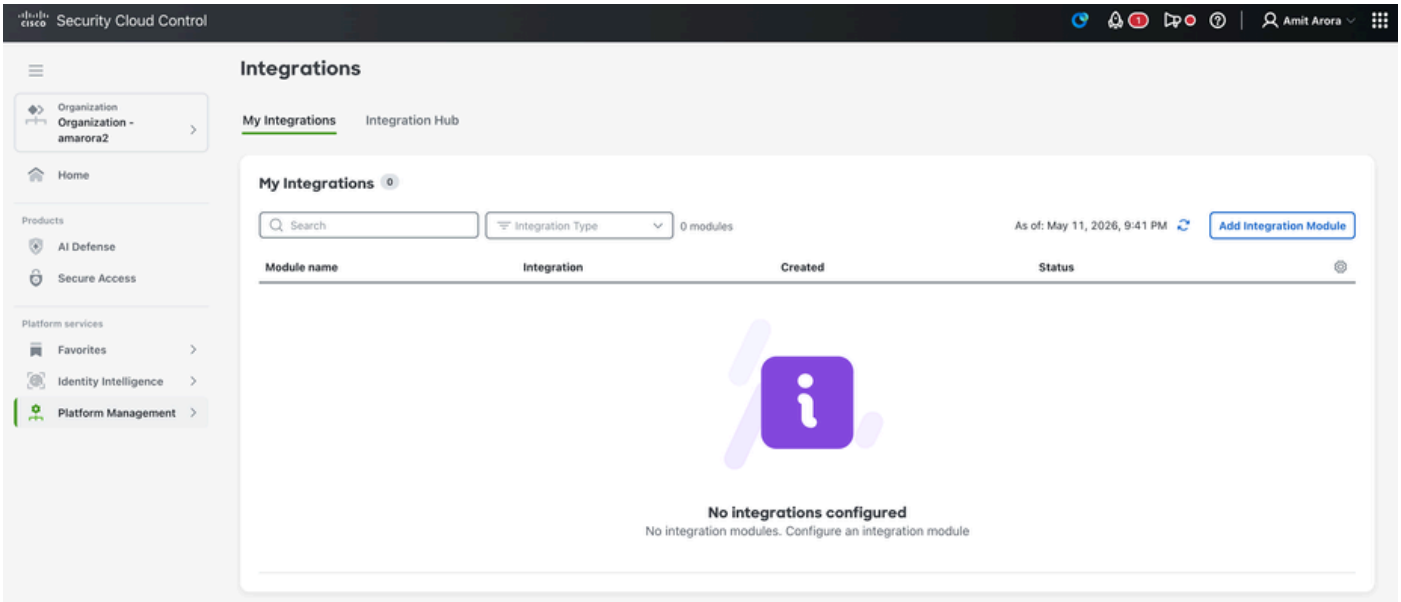


步骤2:将思科安全访问与ISE集成

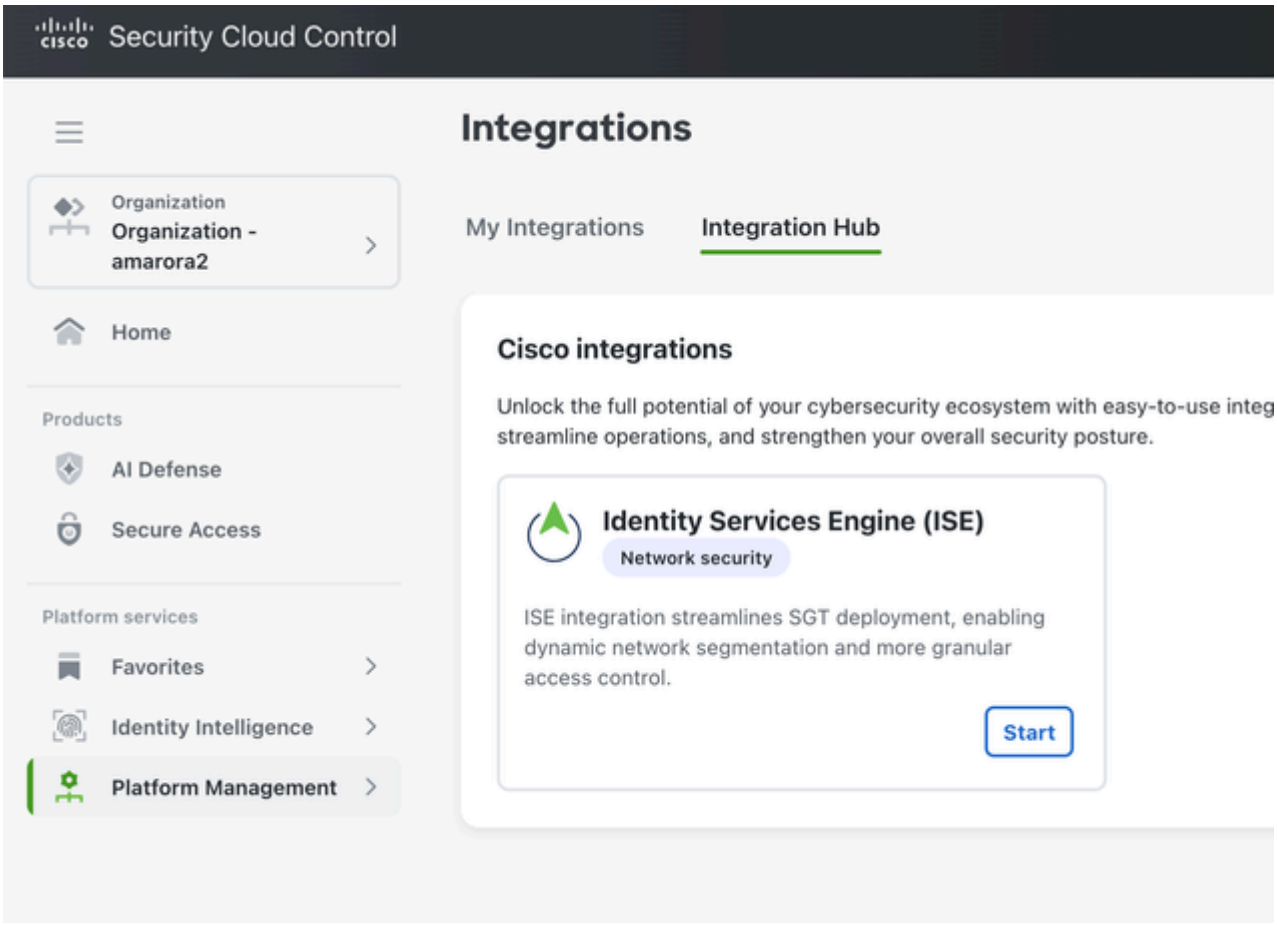
1. 登录security.cisco.com。
2. 选择思科安全访问组织



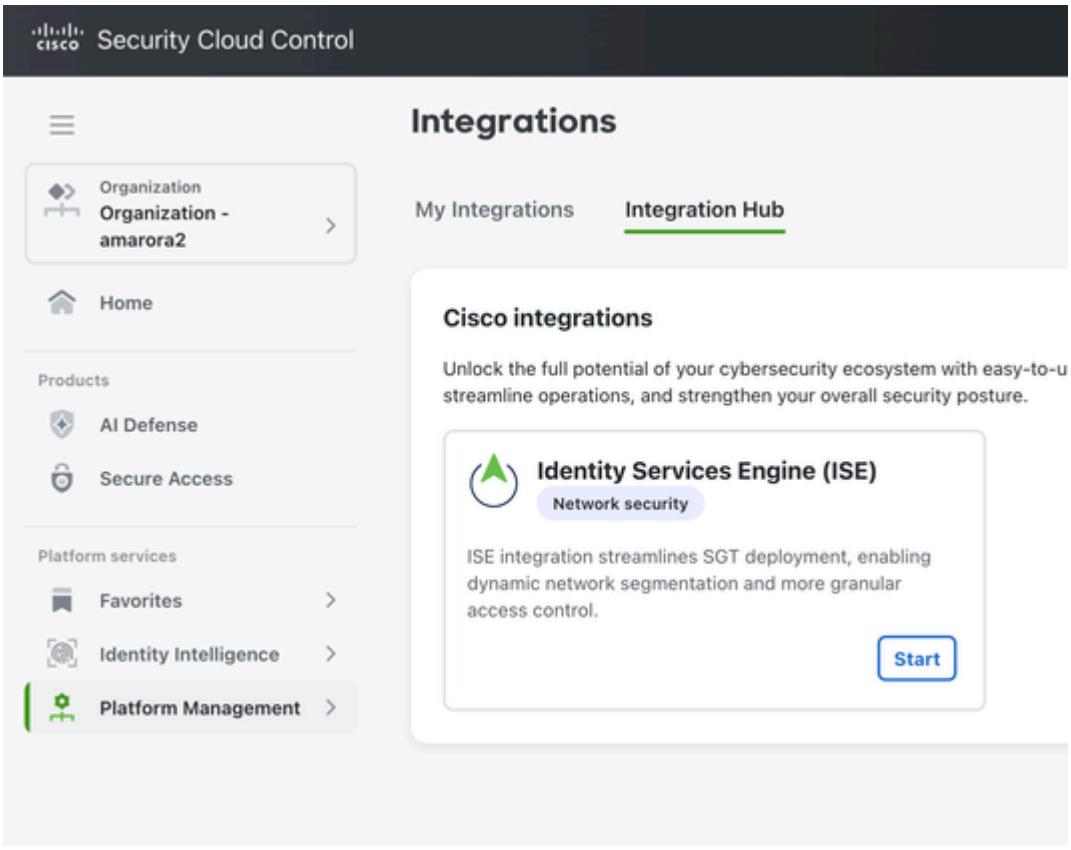
3点击“平台管理” — “平台集成”



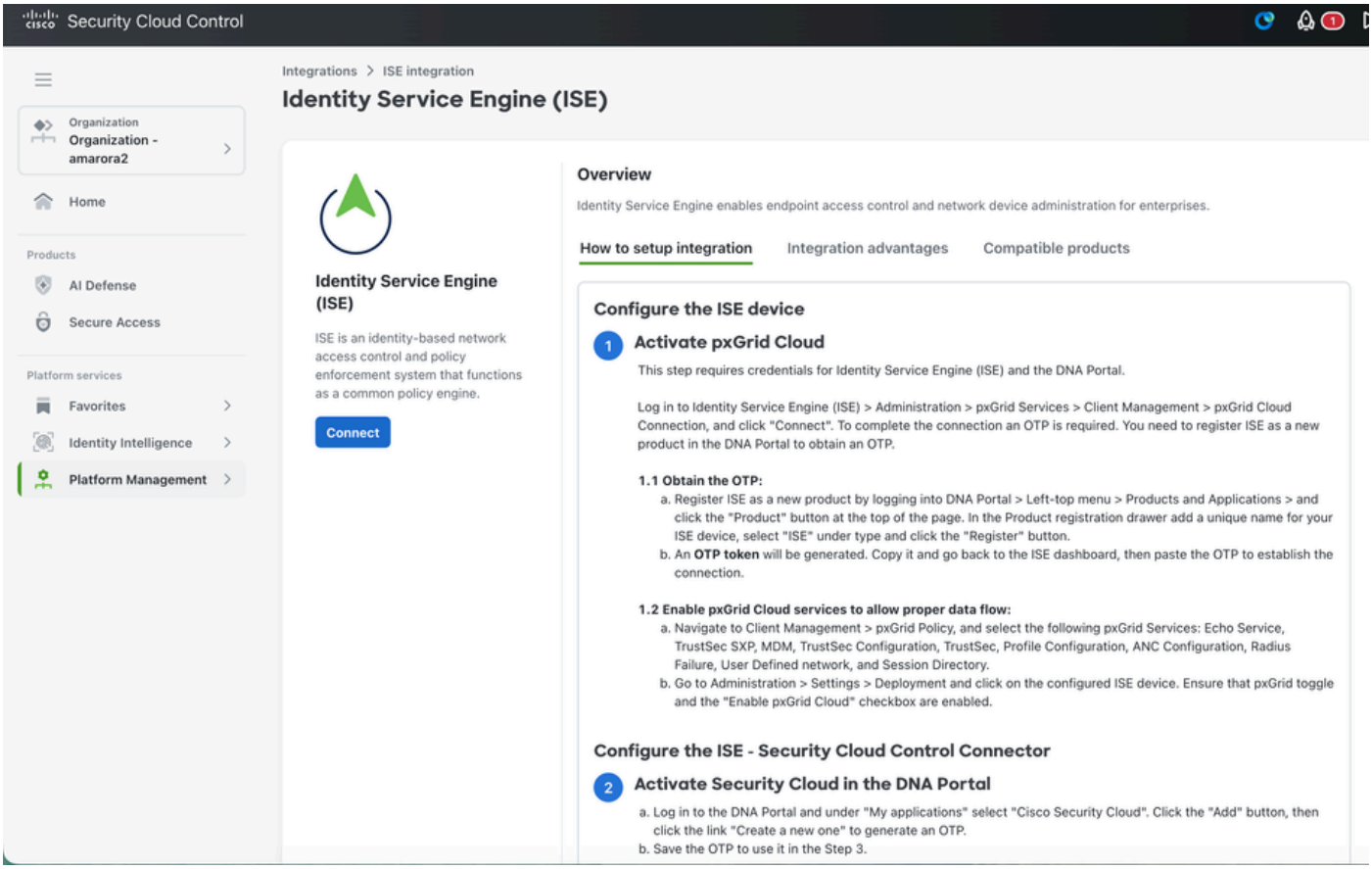
4点击Add Integration Module



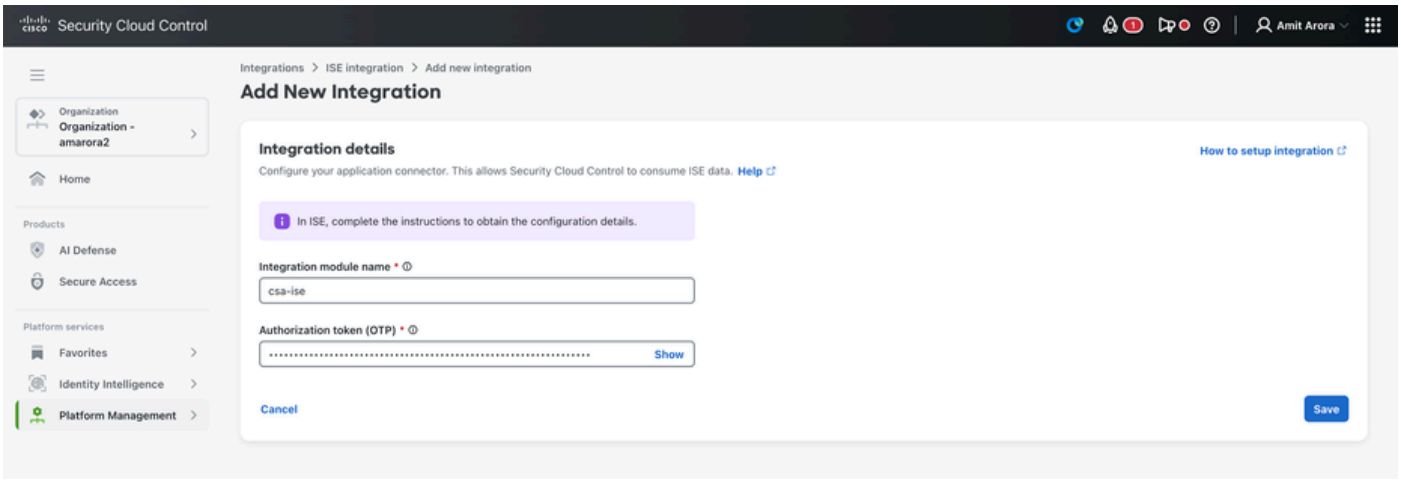
5单击“Start（开始）”


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

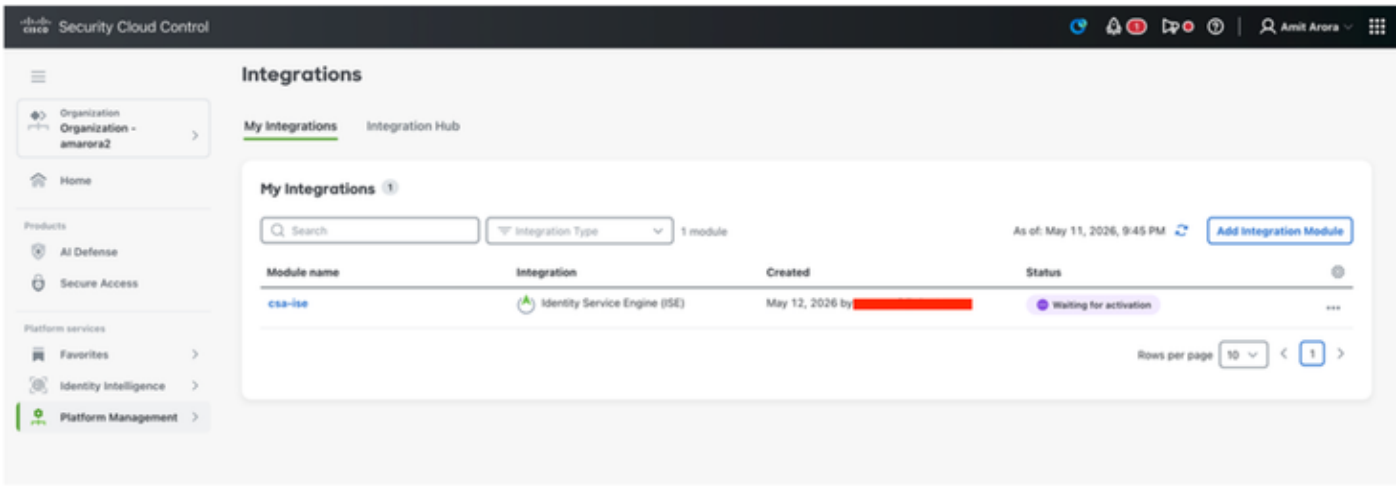
6点击Connect


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.从Cisco ISE输入集成模块名称和OTP，然后点击Save

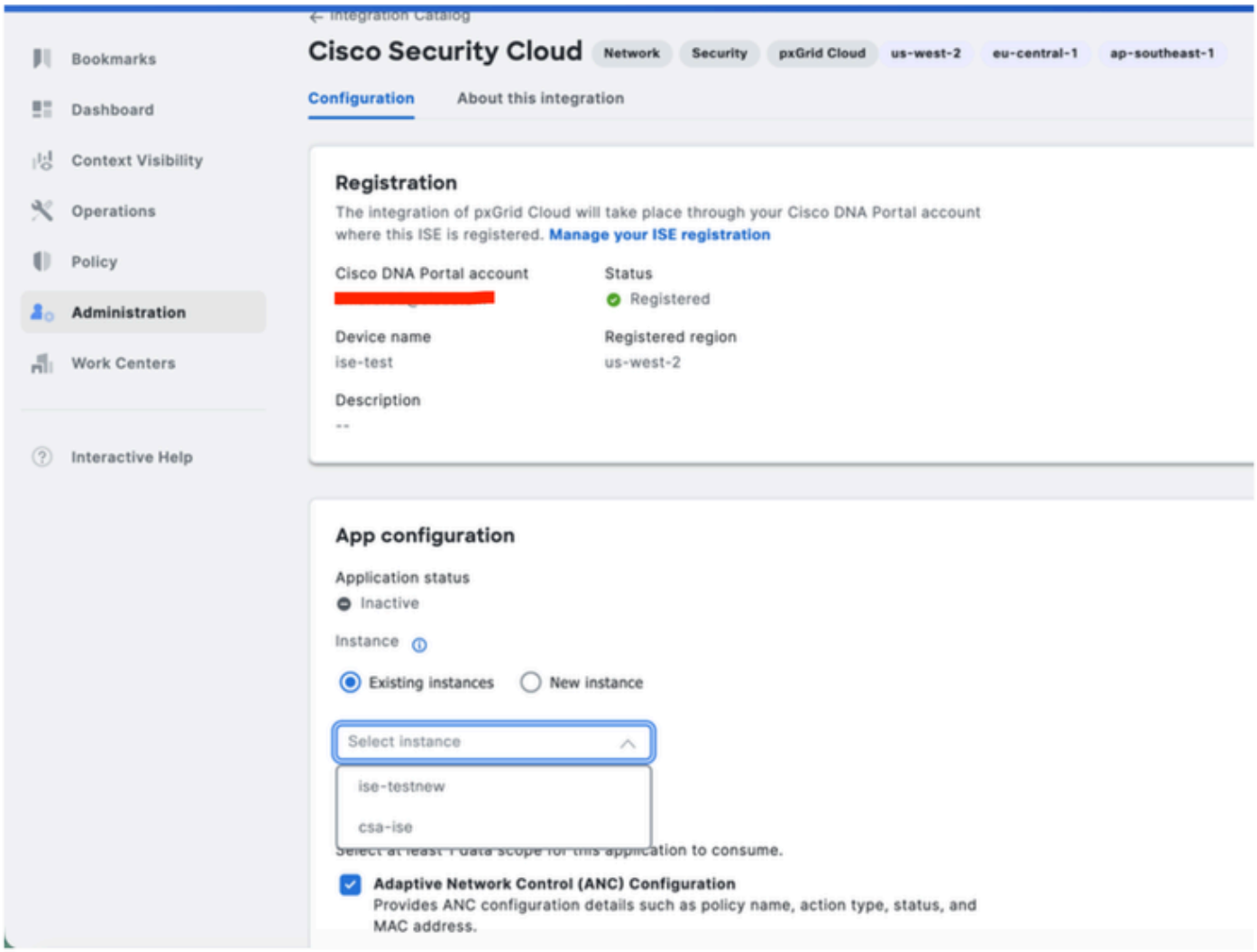


8点击Save后，我们将看到Waiting for Activation Status。

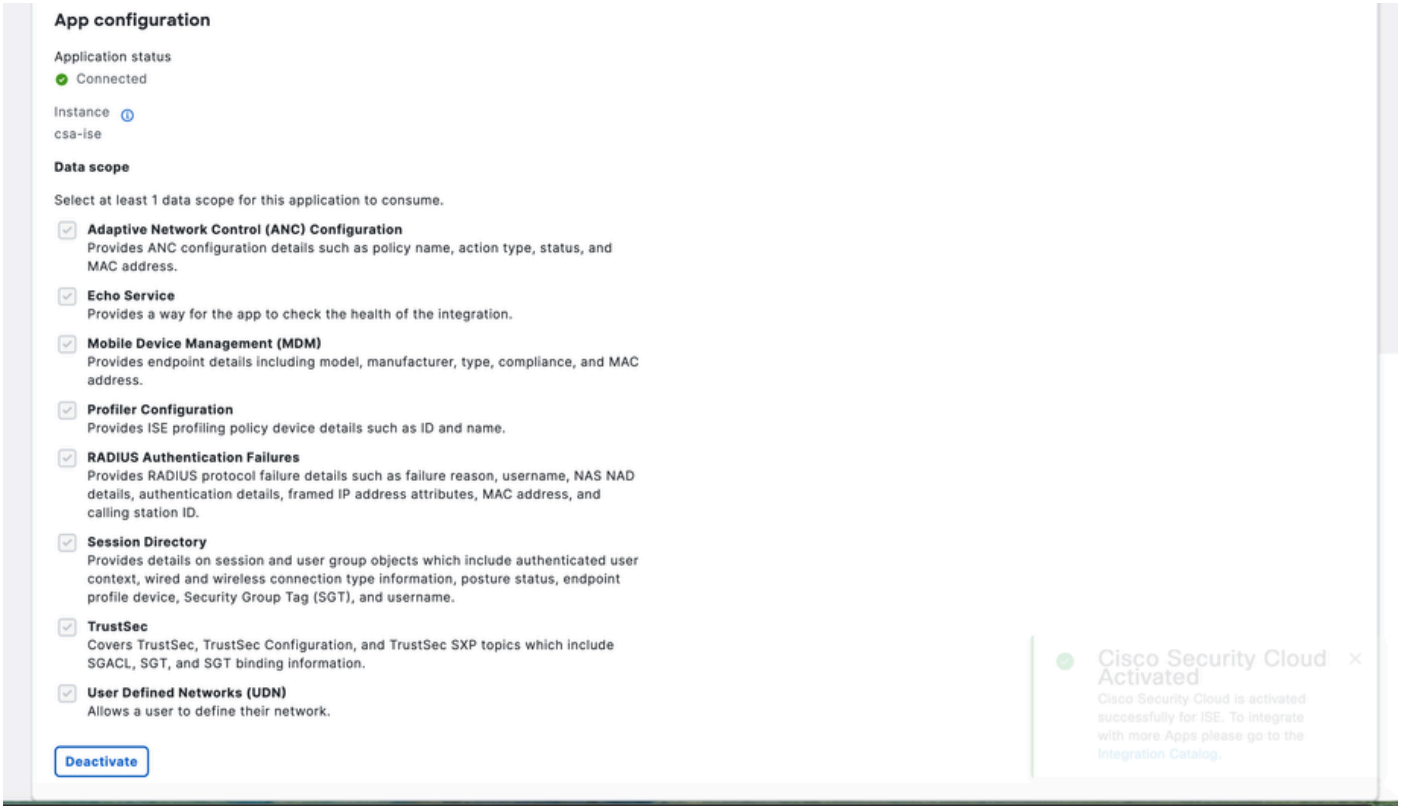


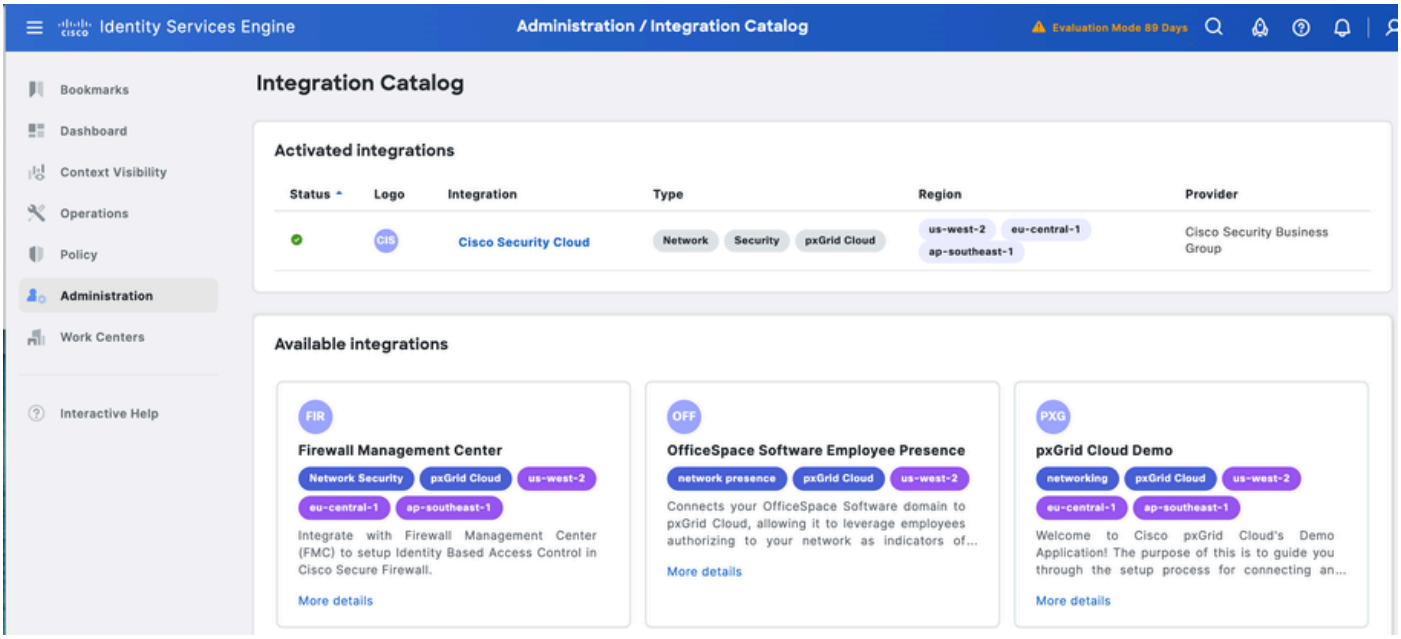
9登录到ISE并导航到Administration - Deployment。点击pxgrid角色的节点 — 点击Pxgrid Connection下的Integration cloud。

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
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
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
ise-test
Registered region
us-west-2
Description
--
App configuration
Application status
Inactive
Instance
Existing instances
New instance
Select instance
ise-testnew
csa-ise
to consume.
Adaptive Network Control (ANC) Configuration
Provides ANC configuration details such as policy name, action type, status, and MAC address.

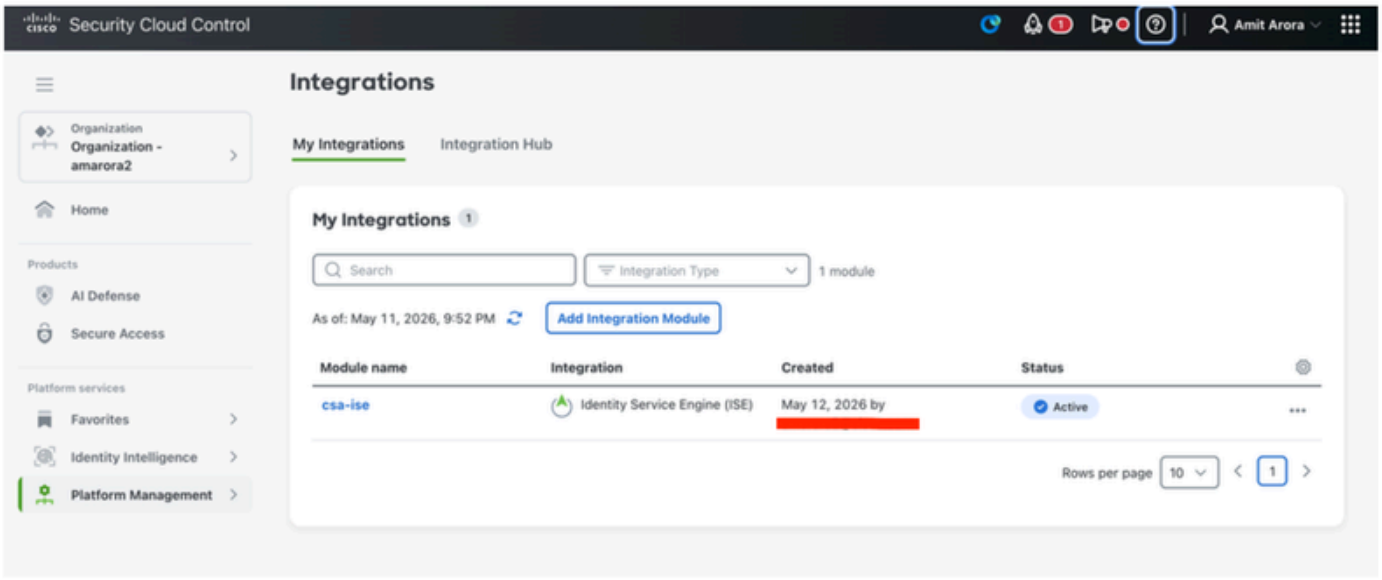
10应用状态现已连接。





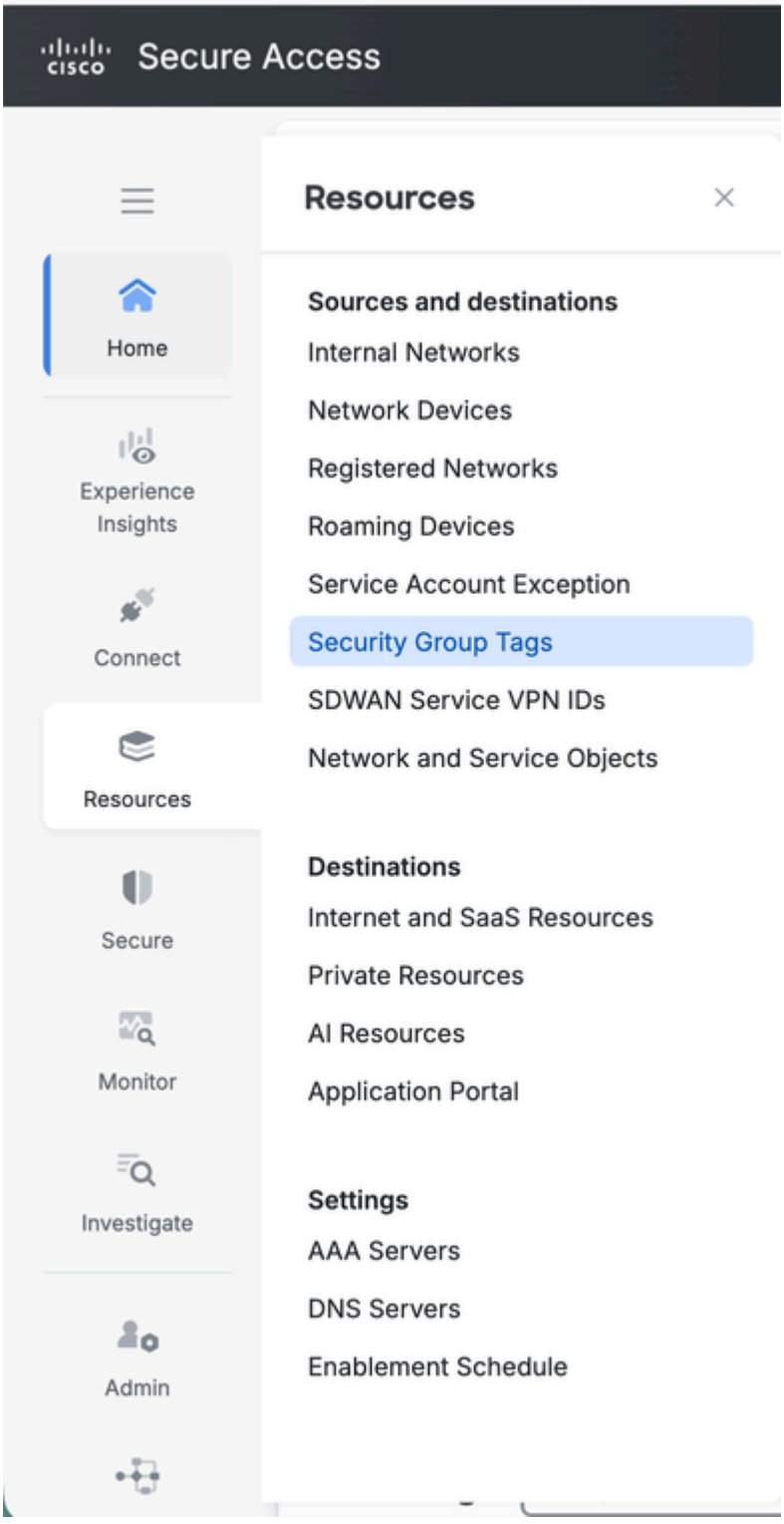
11登录安全云控制 — security.cisco.com

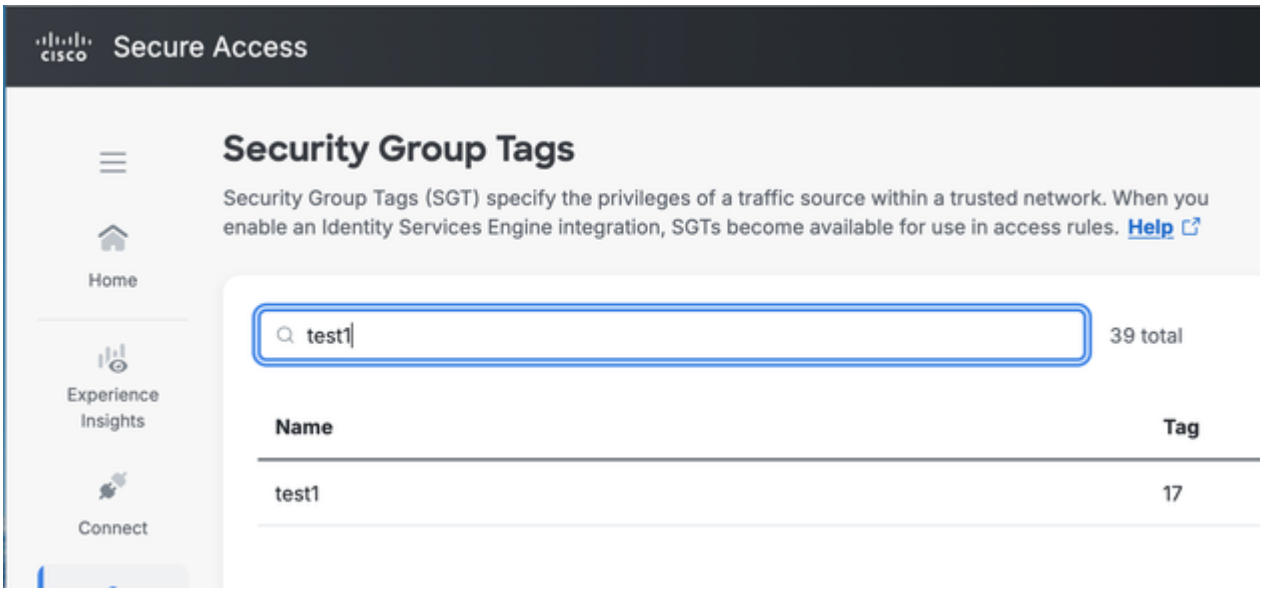
在“平台管理 — 平台集成”下，我们可以看到集成状态为“活动”



验证安全组标记：

登录到Cisco Secure Access。导航至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

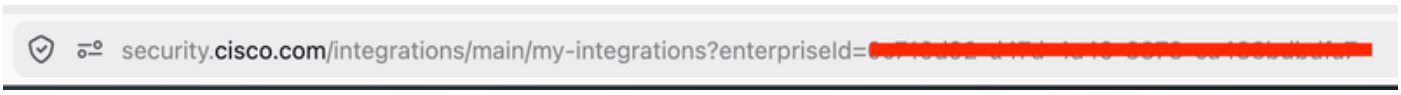
基础设施

ERS

hermes组件处于调试级别。

SCC:

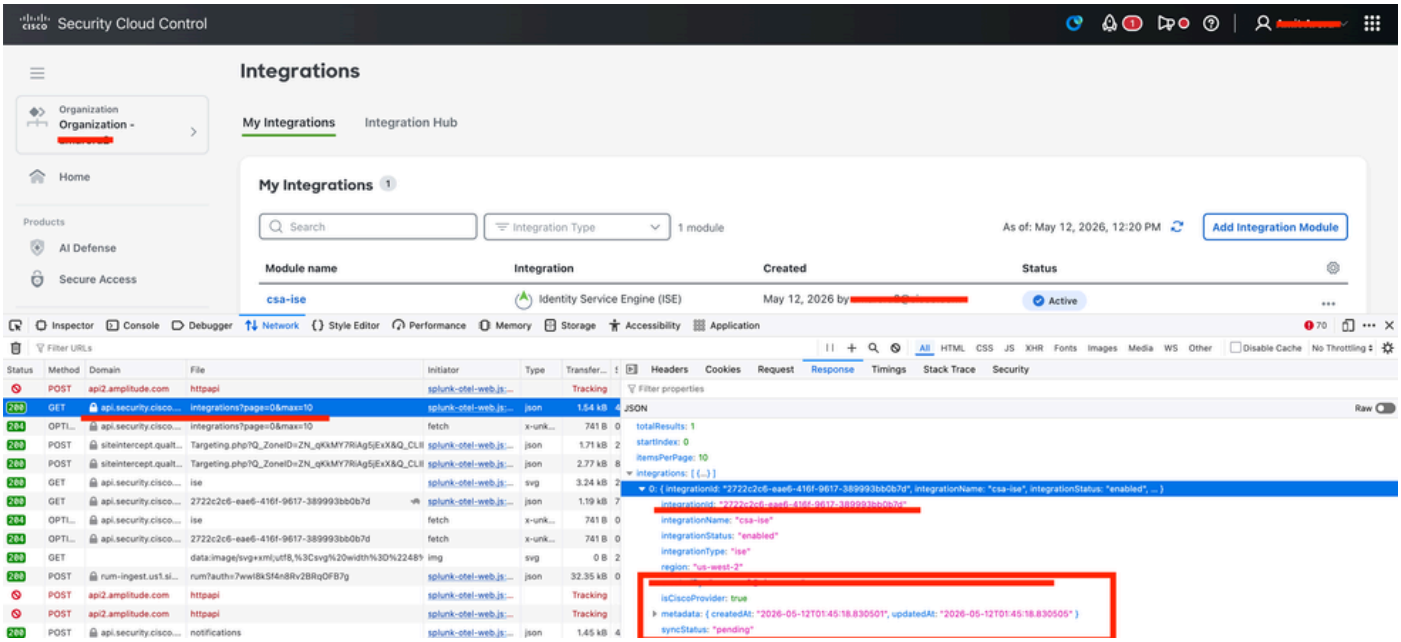
企业ID:在security.cisco.com的URL中



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。



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）。