

Cisco Secure AccessとISEの統合による Pxgridクラウド上のセキュリティグループタグ の実現

内容

はじめに

このドキュメントでは、Cisco Secure AccessとCisco Identity Services Engine(ISE)の間でコンテキスト共有を有効にする方法について説明します

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Access : クラウドベースのセキュリティサービスエッジ(SSE)ソリューション。信頼性のないネットワークアクセスを提供し、ユーザが任意のデバイスからインターネットやプライベートアプリケーションに簡単に接続できるようにします。
- Cisco Identity Service Engine(ISE)バージョン3.4パッチ5
- Cisco Security Cloud Control : セキュリティクラウド製品とアイデンティティのための統合管理ソリューションです。セキュリティクラウド制御は、セキュアアクセスに含まれていません。

背景

この統合により、Catalyst SD-WANブランチからCisco Secure Accessへの信頼できるトンネルを自動的に作成でき、VPN-ID/名前およびSGTコンテキストのシームレスな交換が容易になります

。

Cisco Identity Services Engine(ISE)は、引き続きSGTの設定と管理の中心的な権限です。ISEで実行されるすべてのアップデートは、Cisco Secure Accessと自動的に同期されます。SGTが削除されると、そのSGTを参照する既存のルールがアクティブのままになり、トラフィックの照合が期待どおりに続行されます。

現在、セキュリティルール内にSGT宛先オブジェクトを含めるようにサポートを拡張するSGTマ

ツピングの限定提供を提供しています。さらに、MerakiおよびCisco Secure FirewallからSGTを伝送するSASEトンネルの構築も間もなくサポートされる予定です

使用例：

SGT名前空間ベースのポリシー：

Kitは、セキュリティ管理者として、オンプレミスISEからのSGTを使用して、SSEプライベートおよびインターネットバウンドトラフィックに対して、連続するマイクロセグメンテーションを適用したいと考えています。ポリシーを適用するためにSGTをインポートする機能。



使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Identity Service Engine(ISE)バージョン3.4パッチ5
- セキュアなアクセス
- Cisco Security Cloud

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

コンテキスト共有の設定の概要

- ISEをシスコセキュリティクラウドに接続
- Cisco Secure AccessをISEに接続

設定

このガイドでは、全体的な設定を次の主要な手順に分けて説明します。

1. Cisco ISEをCisco Security Cloudに接続
2. Cisco SecureアクセスをCisco ISEに接続
3. Cisco Secure Accessのセキュリティグループタグ

はじめる前に

- Cisco ISE環境にAdvantageライセンスをインストールし、アクティブ化したことを確認します。
- DNA Cloudエージェントは、Cisco DNA CloudへのアウトバウンドHTTPS接続を作成します。したがって、ネットワークがインターネットに到達するためにプロキシを使用する場合、Cisco ISEプロキシを設定する必要があります。Cisco ISEでプロキシを設定するには、**Administration > System > Settings > Proxy**の順に選択します
- Cisco ISEからCisco pxGrid Cloudポータルへのアウトバウンド接続用にポート443が開いていることを確認します。ファイアウォールまたはプロキシの設定が構成されている場合は、次のURLがブロックされていないことを確認します。

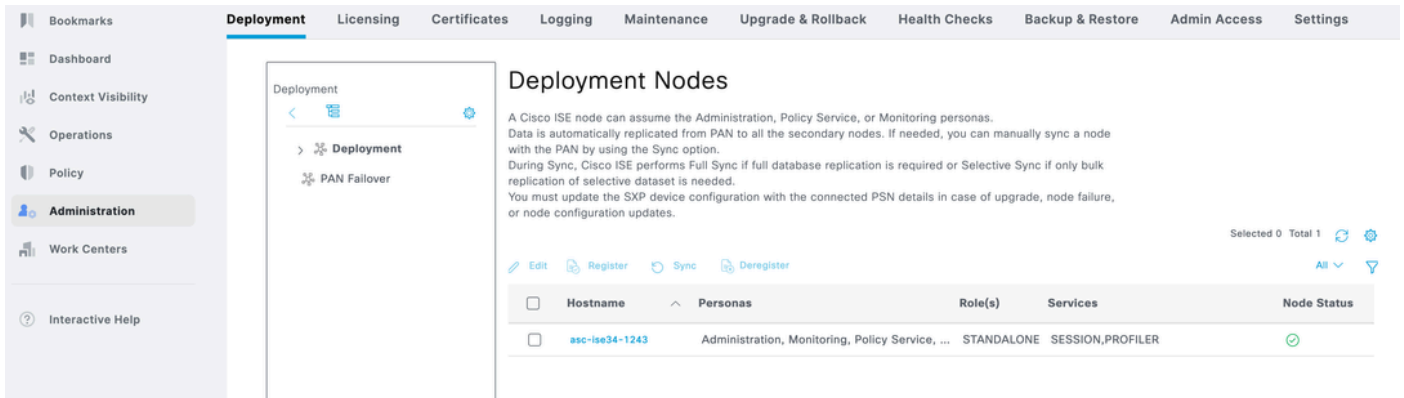
<https://dna.cisco.com>

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

手順1: ISEでPxgridクラウドを有効にします。

1 ISE GUIに移動します。

2 Administration - Deploymentをクリックします。

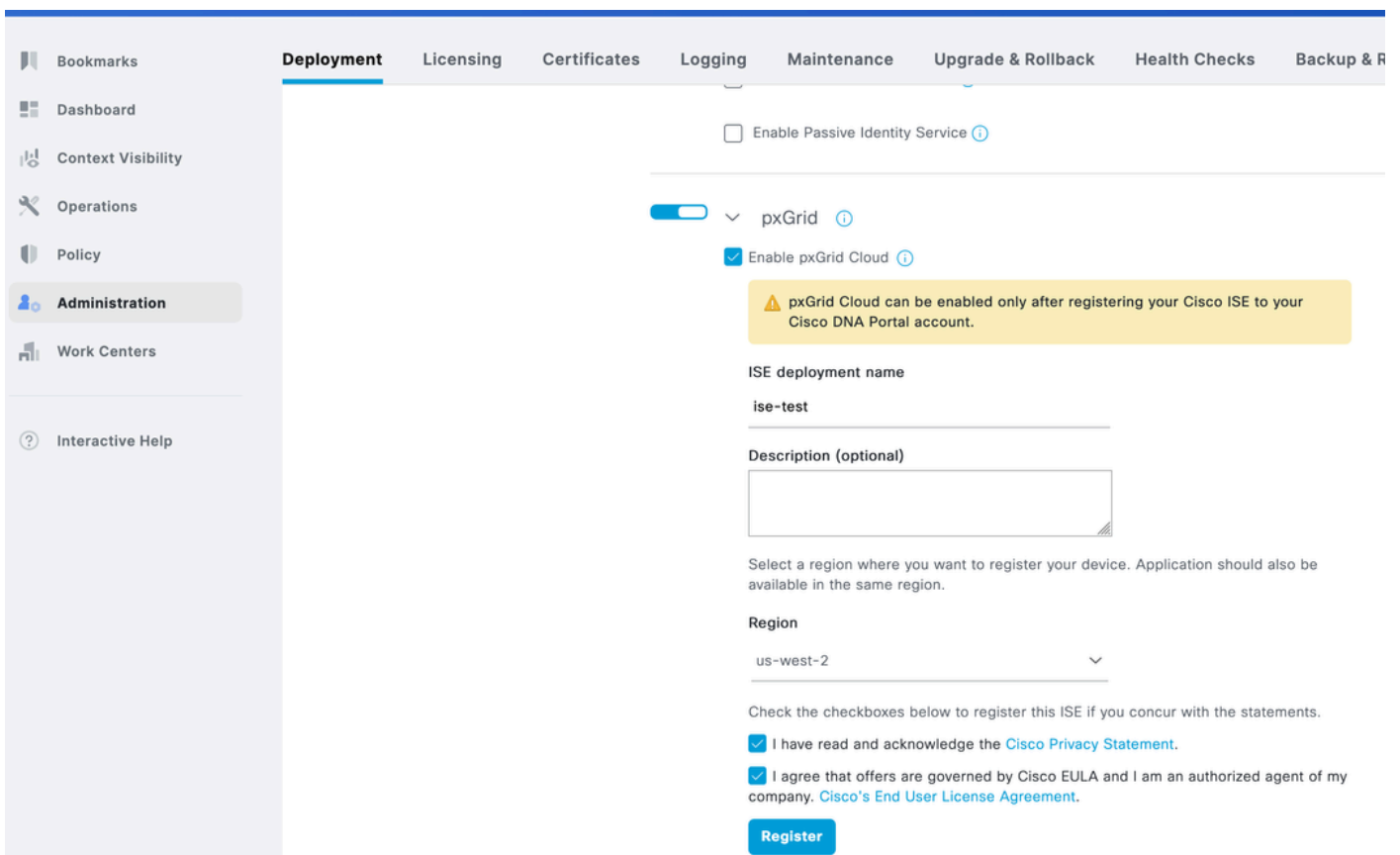


3ノードをクリックし、一番下までスクロールします。

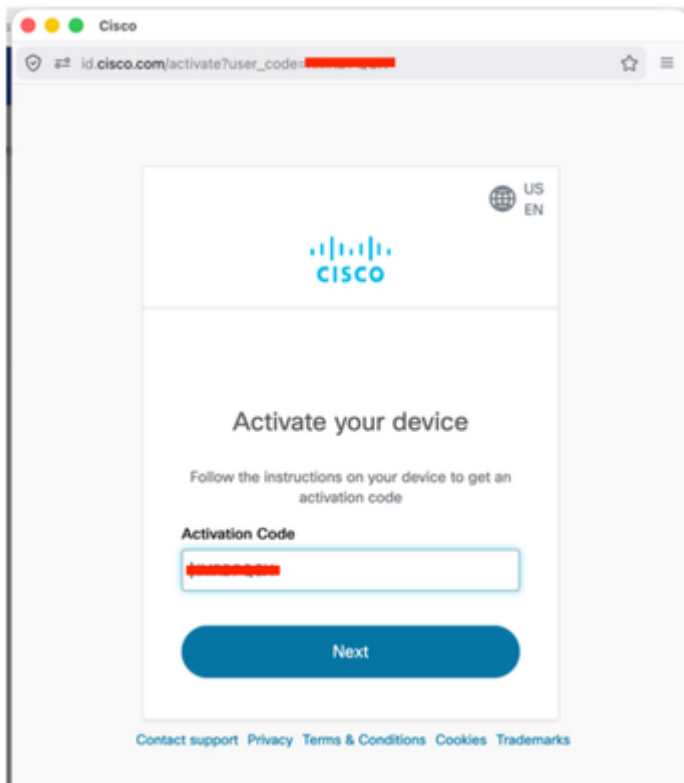
ISE導入名の入力

現在サポートされている唯一のリージョンであるUS West 2としてリージョンを選択します。

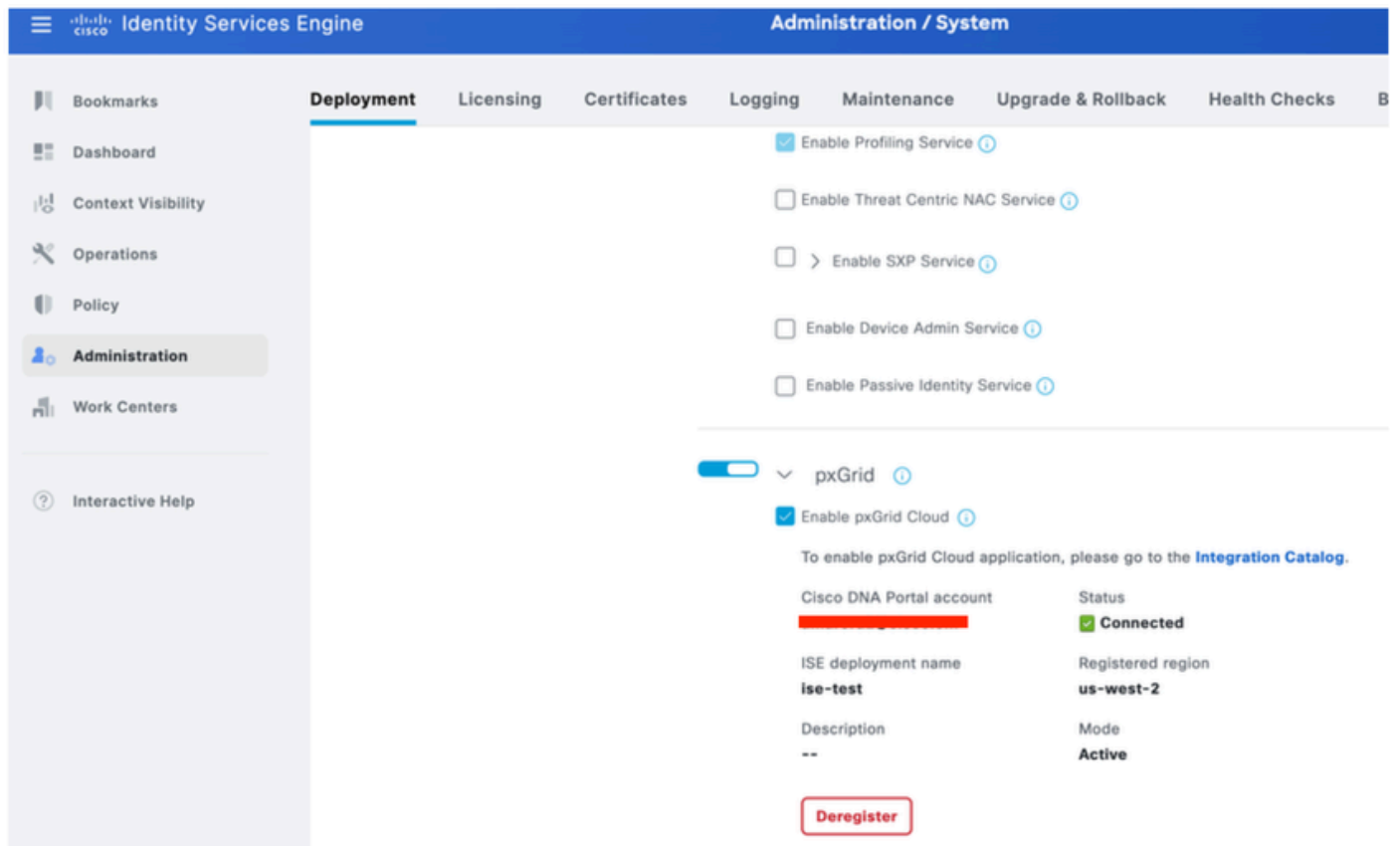
両方のチェックボックスをオンにして、[登録]をクリックします。



4自動入力のアクティベーションコードを示すポップアップが表示されます。[次へ]をクリックします。

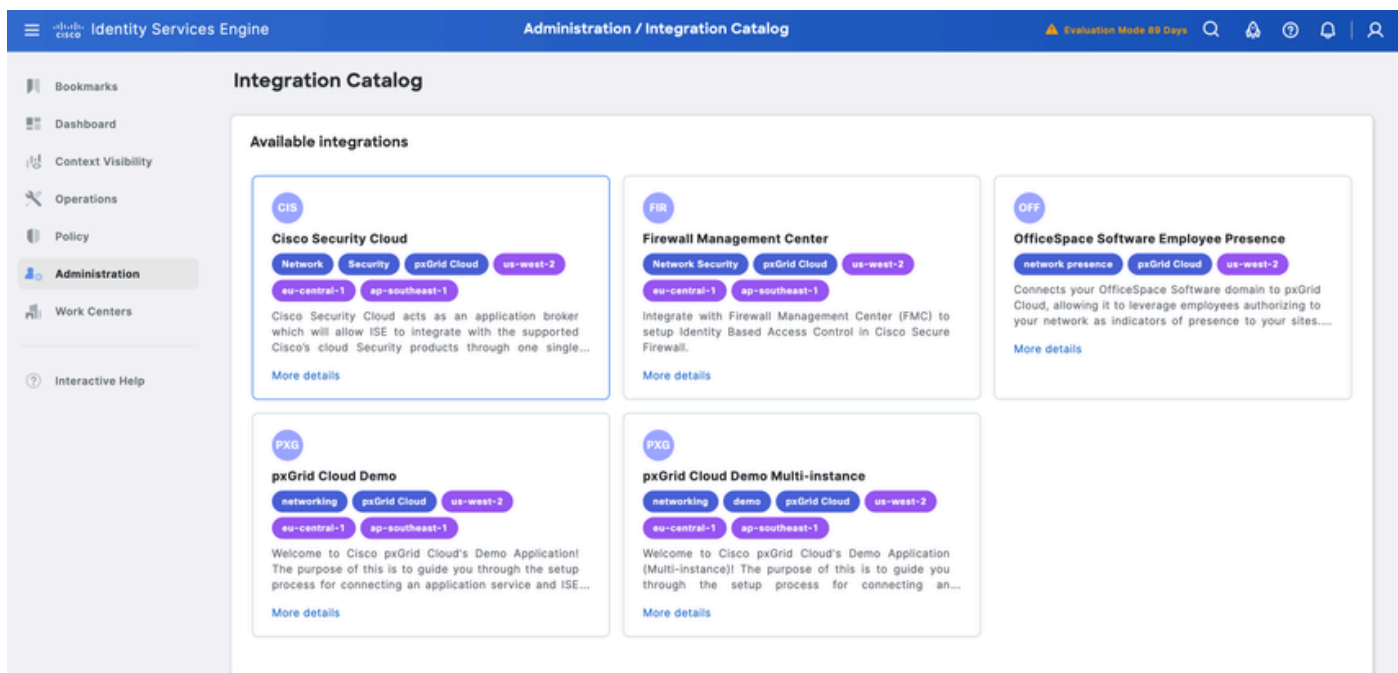


5 ISEがPxgridクラウドに接続していると表示されます。



6手順5の「統合カタログ」リンクをクリックします。

Available Integrationsの下にあるCisco Security Cloudをクリックします。



7 App ConfigurationでNew Instanceをクリックし、Activateをクリックします。

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.

Cisco Secure Accessで使用するワンタイムパスワードをコピーします。

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](#) 

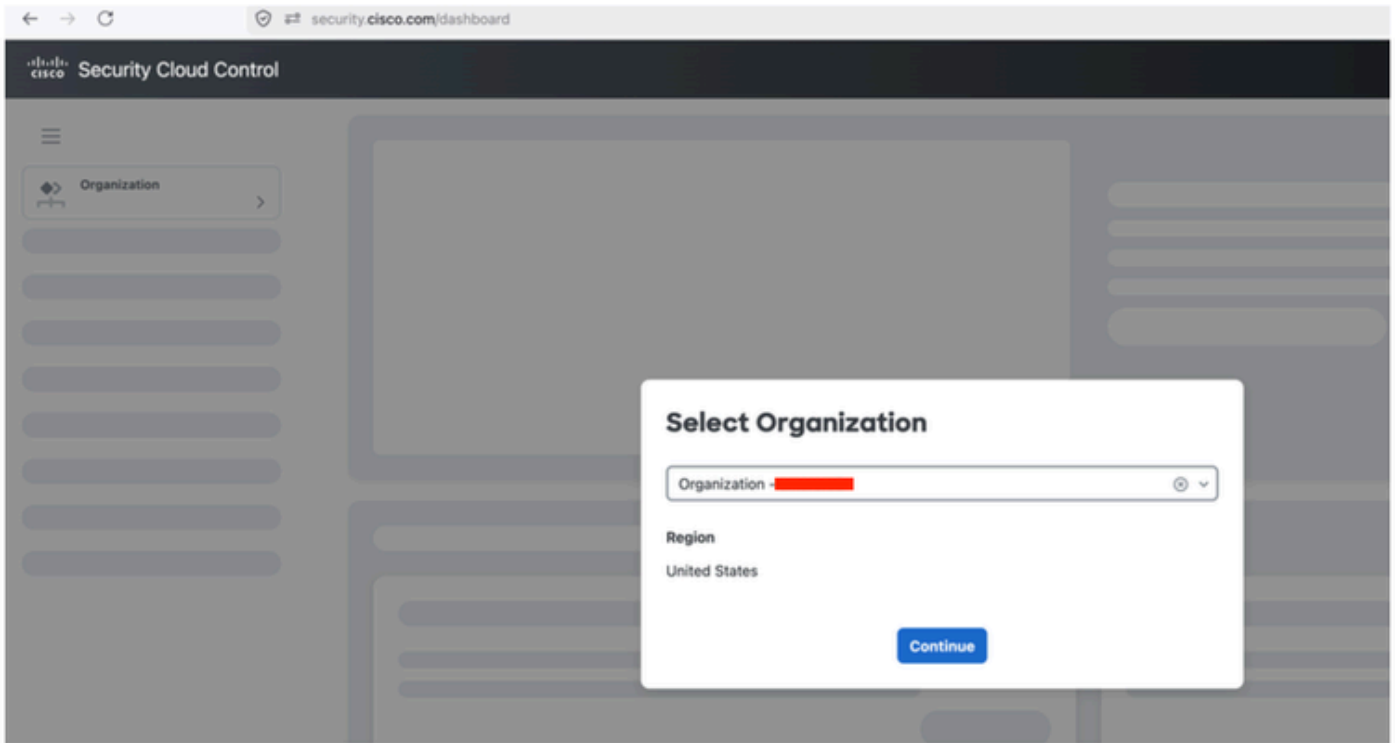
One-time password

  **Copy**

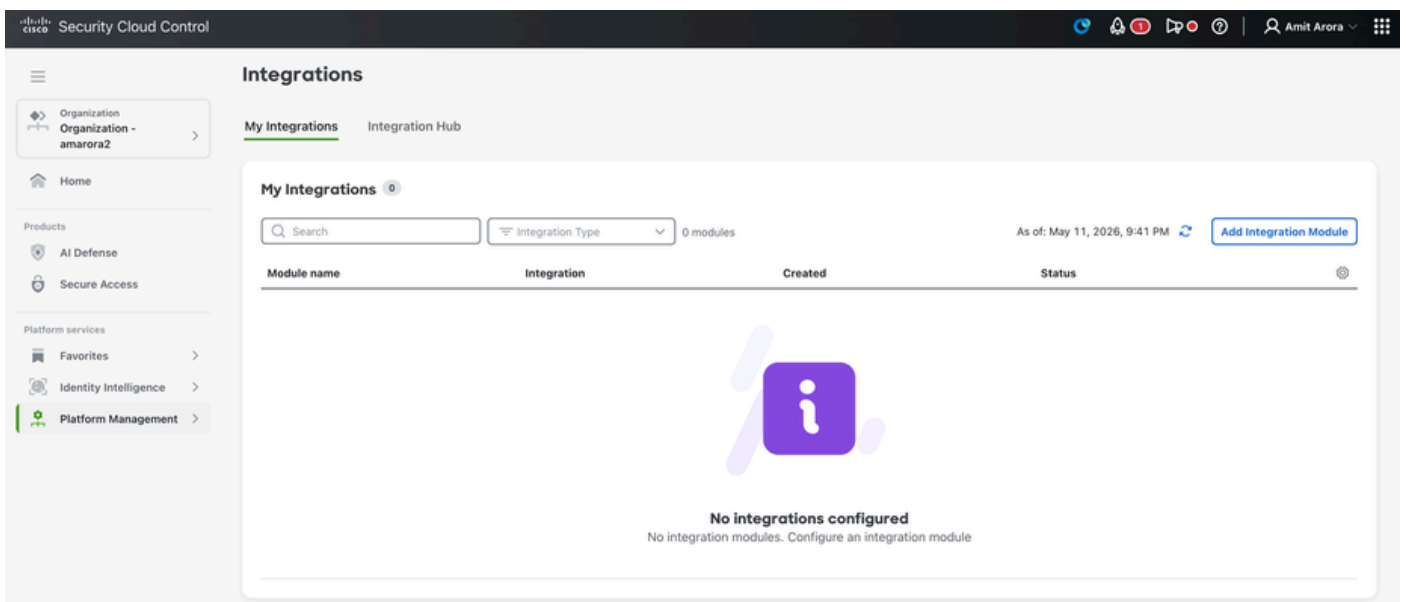
OK

ステップ2: Cisco Secure AccessとISEの統合

1. security.cisco.comにログインします。
2. Cisco Secure Access ORGを選択します。



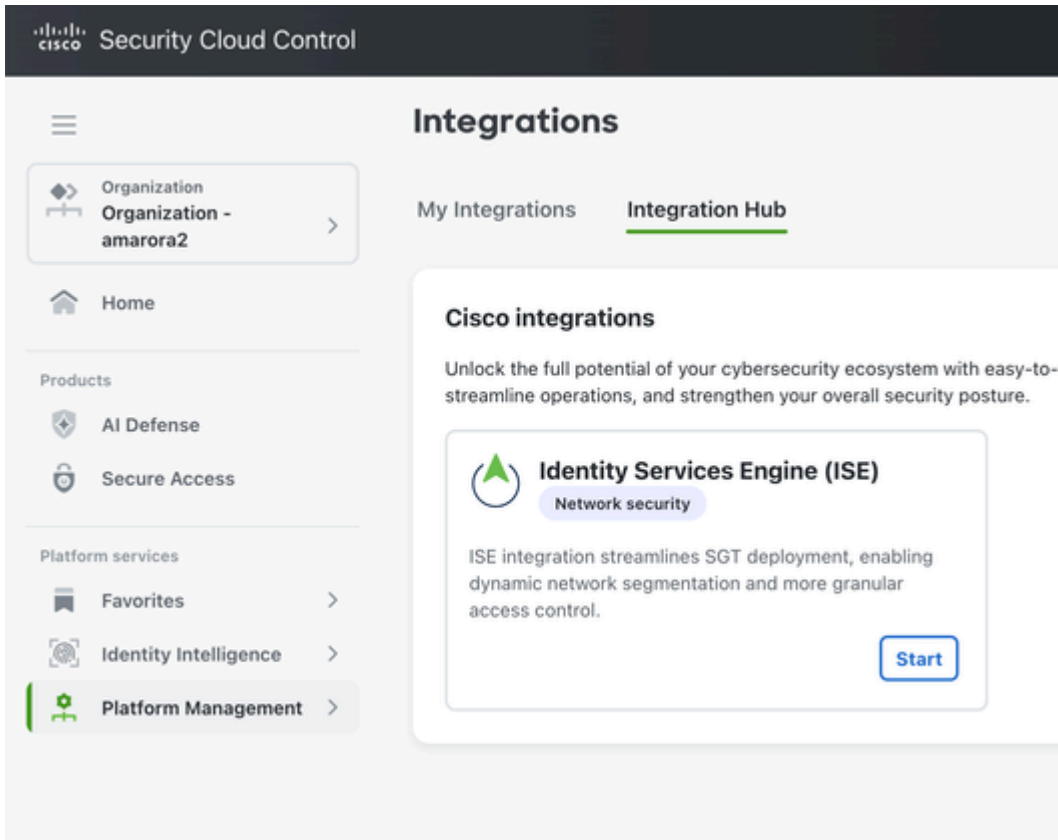
3プラットフォーム管理 – プラットフォーム統合をクリック



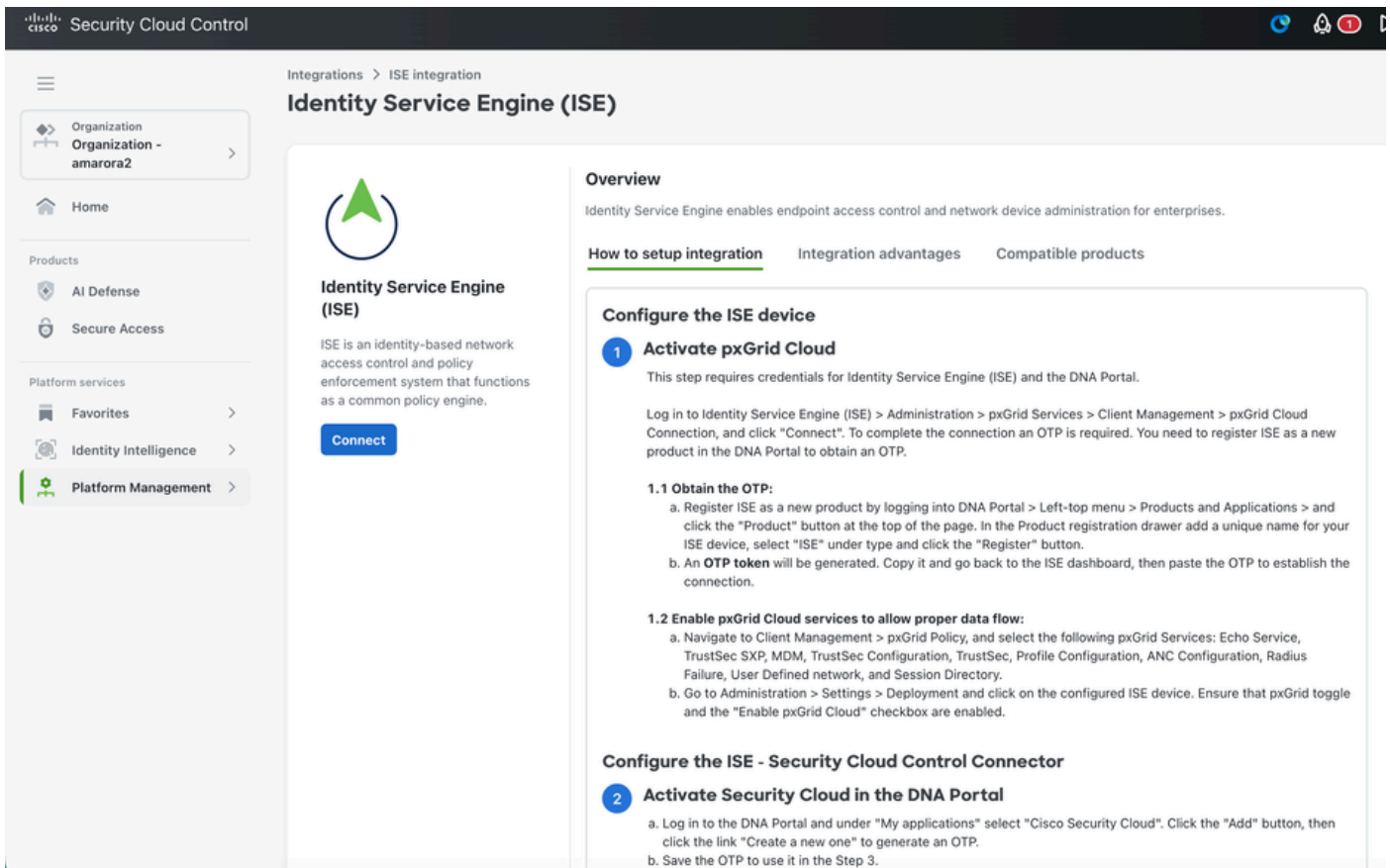
4 [Add Integration Module]をクリックします。

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' (with sub-items 'AI Defense' and 'Secure Access'), and 'Platform services' (with sub-items '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, there is a section titled '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.' A card for 'Identity Services Engine (ISE)' is displayed, featuring a green triangle icon, the text 'Identity Services Engine (ISE)', a 'Network security' tag, and a description: 'ISE integration streamlines SGT deployment, enabling dynamic network segmentation and more granular access control.' A blue 'Start' button is located at the bottom right of the ISE card.

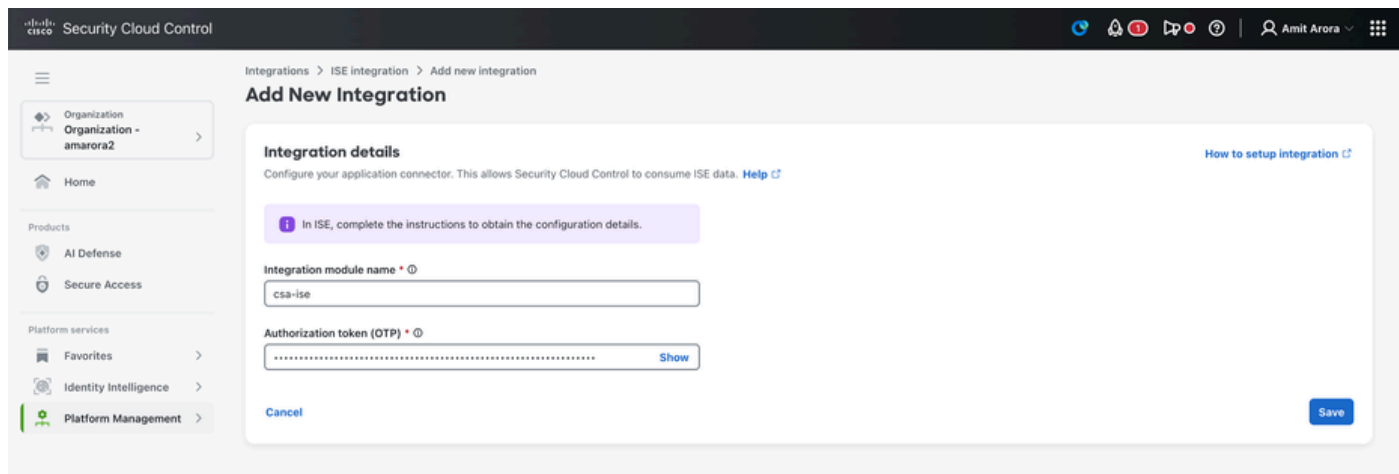
5 [開始]をクリックします。



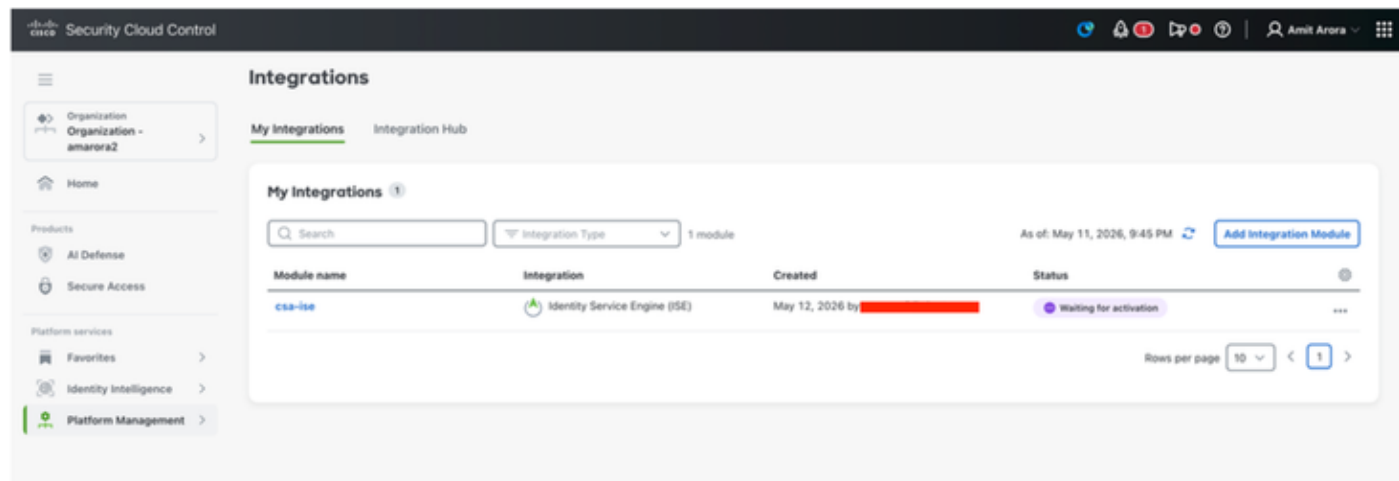
6 [接続]をクリックします。



7. Cisco ISEから統合モジュール名とOTPを入力し、Saveをクリックします。



8 [Save] (保存) をクリックすると、[Waiting for Activation Status] (ライセンス認証ステータスを待っています) が表示されます。



9 ISEにログインし、Administration - Deploymentの順に移動します。pxgridペルソナを持つノードをクリックします。Pxgrid接続の下の統合クラウドをクリックします。

App configurationの下で、Security Cloud Controlで作成したISEインスタンスを選択し、

Activateをクリックします。

The screenshot shows the Cisco Security Cloud 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 titled 'Cisco Security Cloud' and includes tabs for Network, Security, pxGrid Cloud, us-west-2, eu-central-1, and ap-southeast-1. Below these are 'Configuration' and 'About this integration' tabs. The 'Registration' section displays the following information:

Field	Value
Cisco DNA Portal account	[Redacted]
Status	Registered
Device name	ise-test
Registered region	us-west-2
Description	--

The 'App configuration' section shows the application status as 'Inactive'. Under 'Instance', the 'Existing instances' radio button is selected. A dropdown menu is open, showing 'ise-testnew' and 'csa-ise' as options. Below the dropdown, there is a note: 'Select at least 1 data scope for this application to consume.' The 'Adaptive Network Control (ANC) Configuration' checkbox is checked, with a sub-note: 'Provides ANC configuration details such as policy name, action type, status, and MAC address.'

10 Application Statusがconnectedになりました。

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 Security Cloud Controlへのログイン – security.cisco.com

「プラットフォーム管理 – プラットフォーム統合」で、「統合ステータス」が「アクティブ」と表示されます。

Organization - amarora2

Home

Products

- AI Defense
- Secure Access

Platform services

- Favorites
- Identity Intelligence
- Platform Management

Integrations

My Integrations Integration Hub

My Integrations 1

Search Integration Type 1 module

As of: May 11, 2026, 9:52 PM Add Integration Module

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

Rows per page 10 < 1 >

セキュリティグループタグを確認します。

Cisco Secure AccessにログインするResources - Security Group Tagsの順に移動します。



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

Security Group Tags

Security Group Tags (SGT) specify the privileges of a traffic source within a trusted network. When you enable an Identity Services Engine integration, SGTs become available for use in access rules. [Help](#)

test1 39 total

Name	Tag
test1	17

Cisco TACに必要な情報

ISE :

[PXGRIDペルソナを使用してISEノードのデバッグレベルに設定された次のコンポーネントを含むISEサポートバンドルを収集する方法:](#)

pxgrid

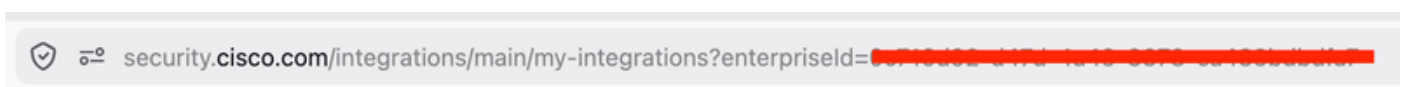
インフラストラクチャ

ERS

デバッグレベルのhermesコンポーネント。

SCC:

security.cisco.comのURLにあるエンタープライズID:



統合ID。

HARキャプチャの開始

Security.cisco.com にログインします。

「プラットフォーム管理 – プラットフォーム統合」に移動します。

統合の検索：ページapiの呼び出しで、応答タブに統合IDが表示されます。

The screenshot displays 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 a list of 'My Integrations'. One integration, 'csa-ise', is listed as 'Identity Service Engine (ISE)' and is in an 'Active' state, created on May 12, 2026.

Below the integrations list, a HAR capture is shown. The 'Response' tab is selected, displaying the JSON response for a GET request to the integrations API. The response includes the integration ID '2722c2c6-ee66-416f-9617-389993bb0b7d' and other details like 'integrationName: "csa-ise"' and 'integrationStatus: "enabled"'. A red box highlights the 'metadata' field, which contains 'createdAt: "2026-05-12T01:45:18.830501"' and 'updatedAt: "2026-05-12T01:45:18.830501"'. Another red box highlights the 'integrationId' field in the response body.

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。