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す。

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

ッ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。

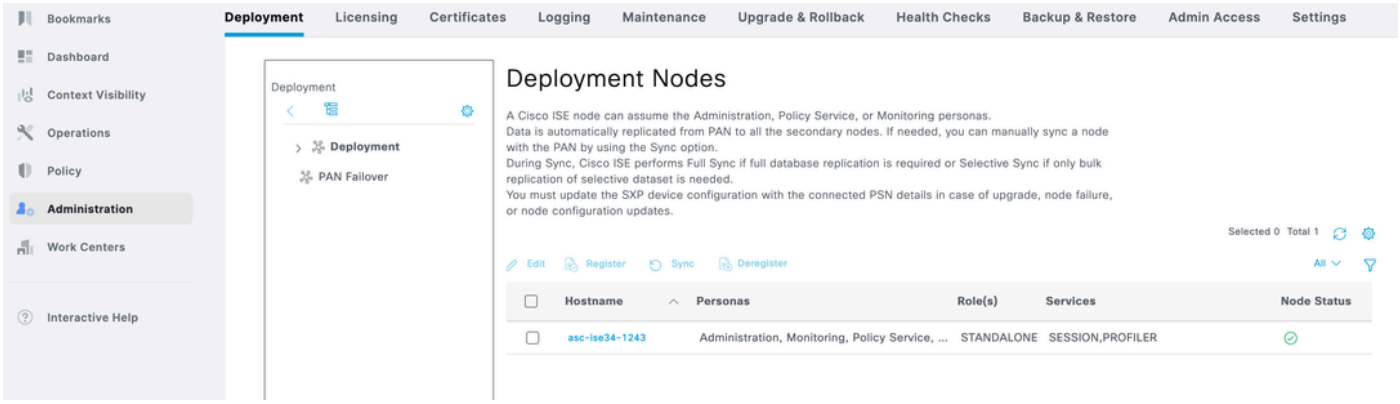
https://dna.cisco.com

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。

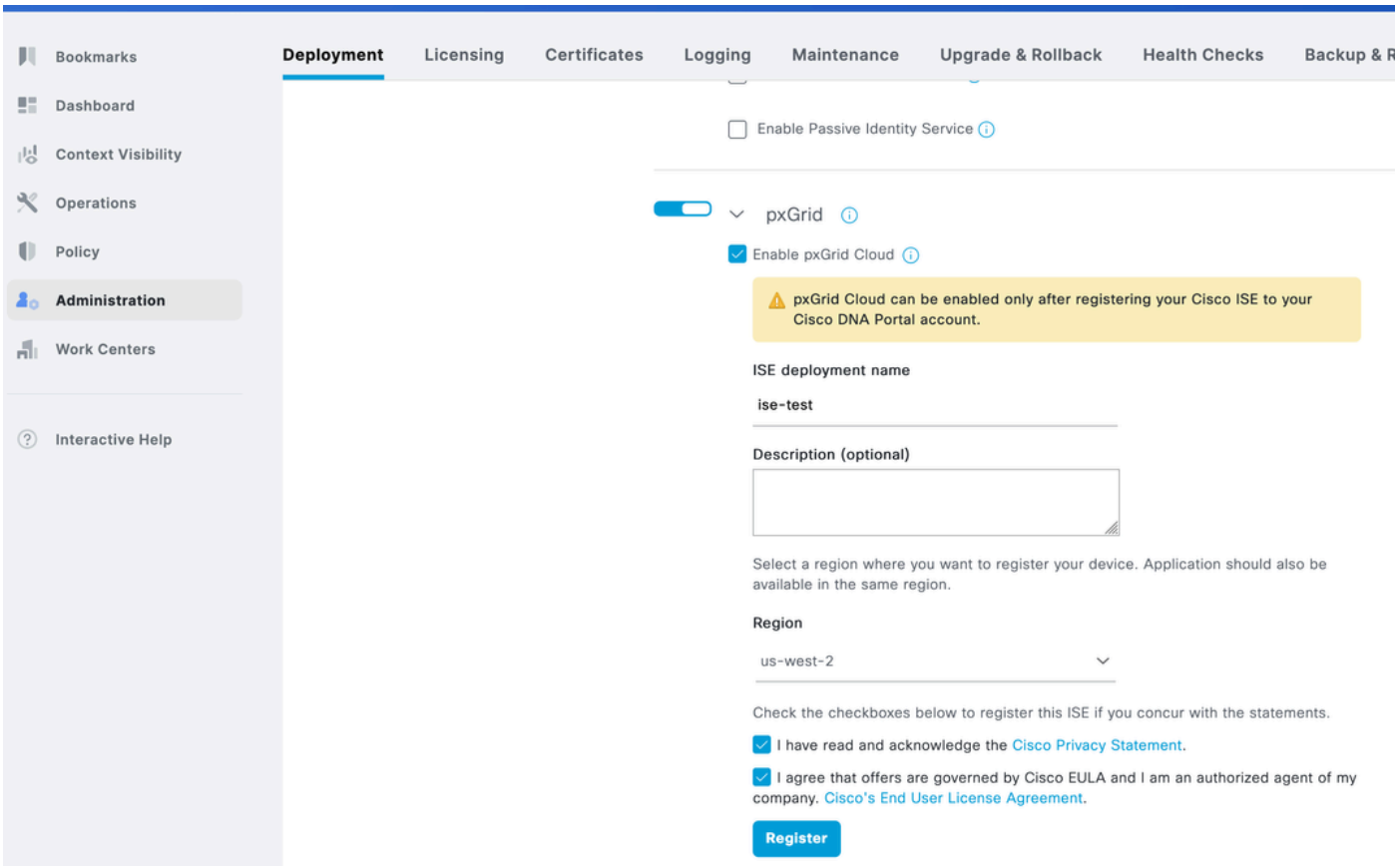


3ノードをクリックし、一番下までスクロールします。

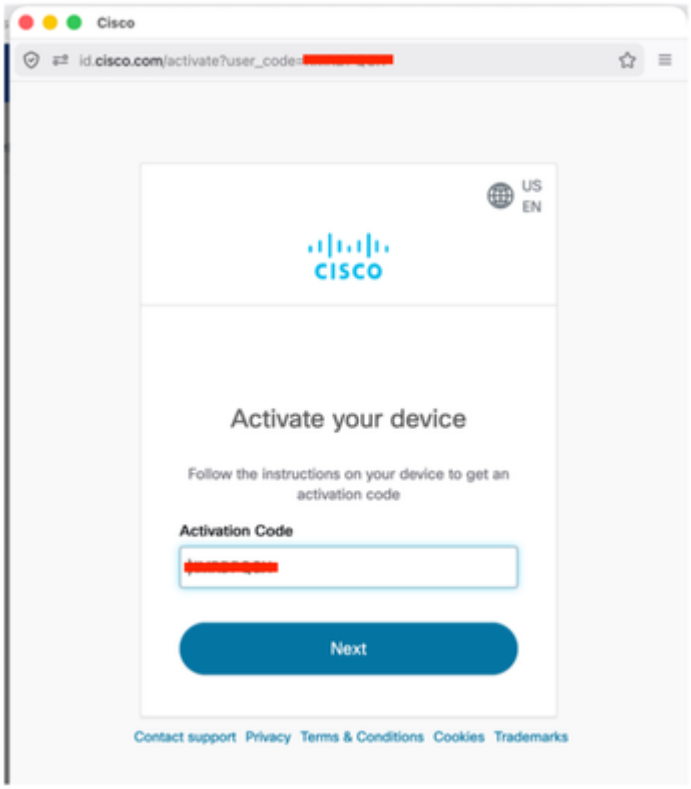
ISE導入名の入力

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。

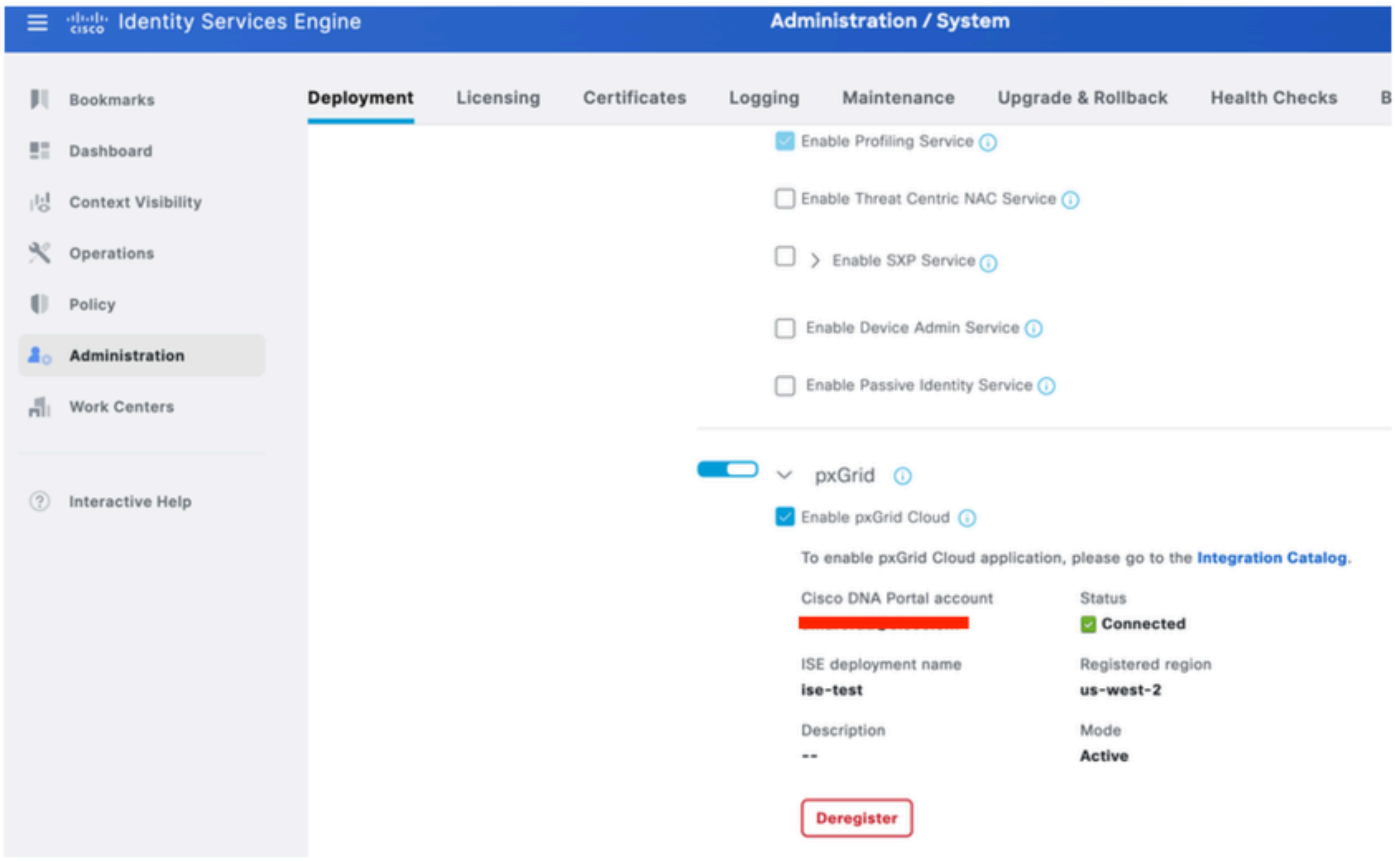
両方のチェックボックスをオンにして、[登録]をクリックします。



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。



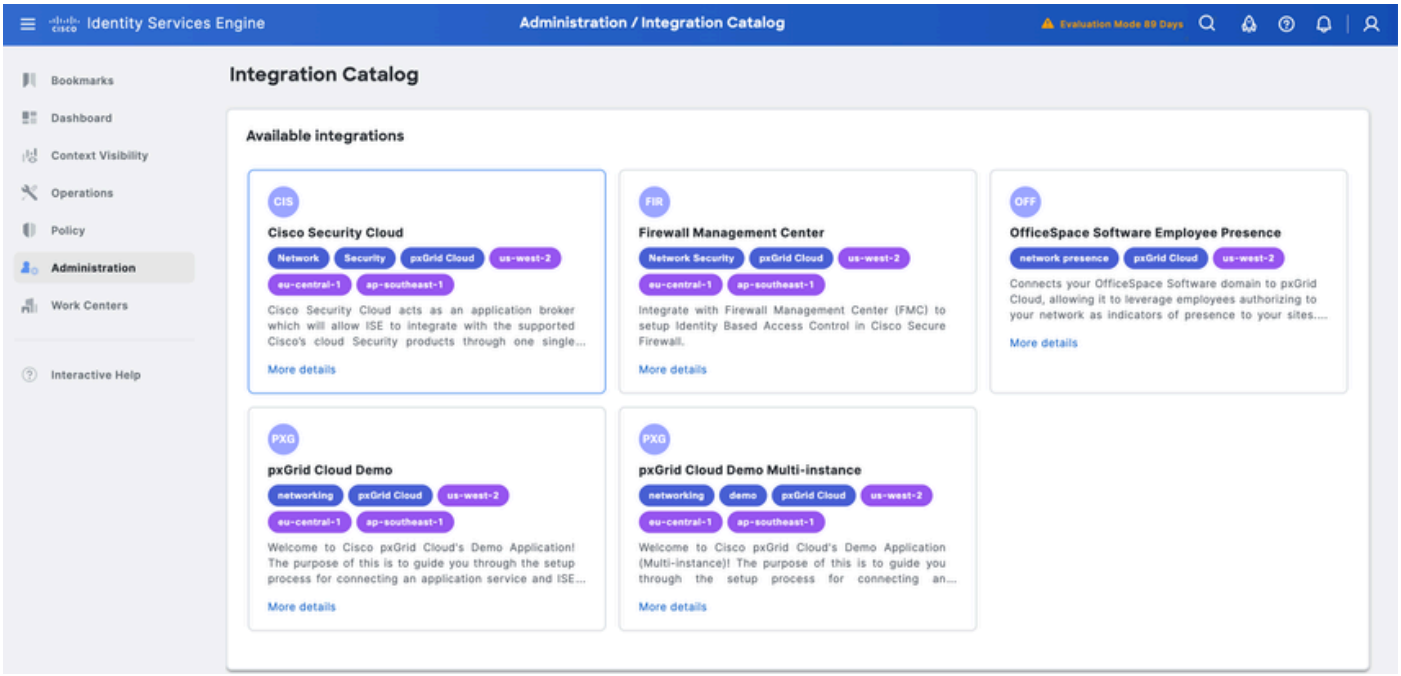
5 ISEがPxgridクラウドに接続していると表示されます。



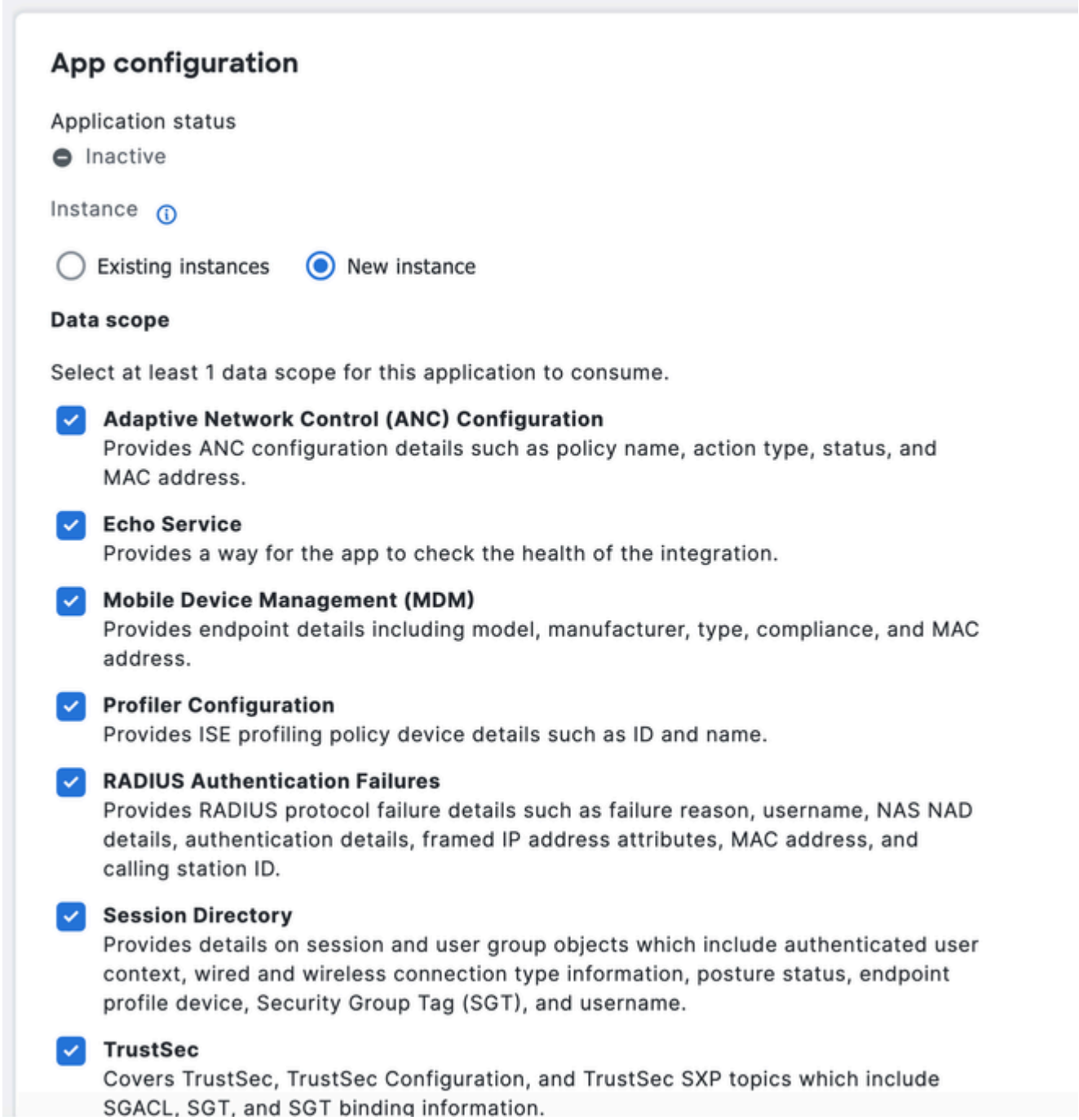
6手順5の「統合カタログ」リンクをクリックします。

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

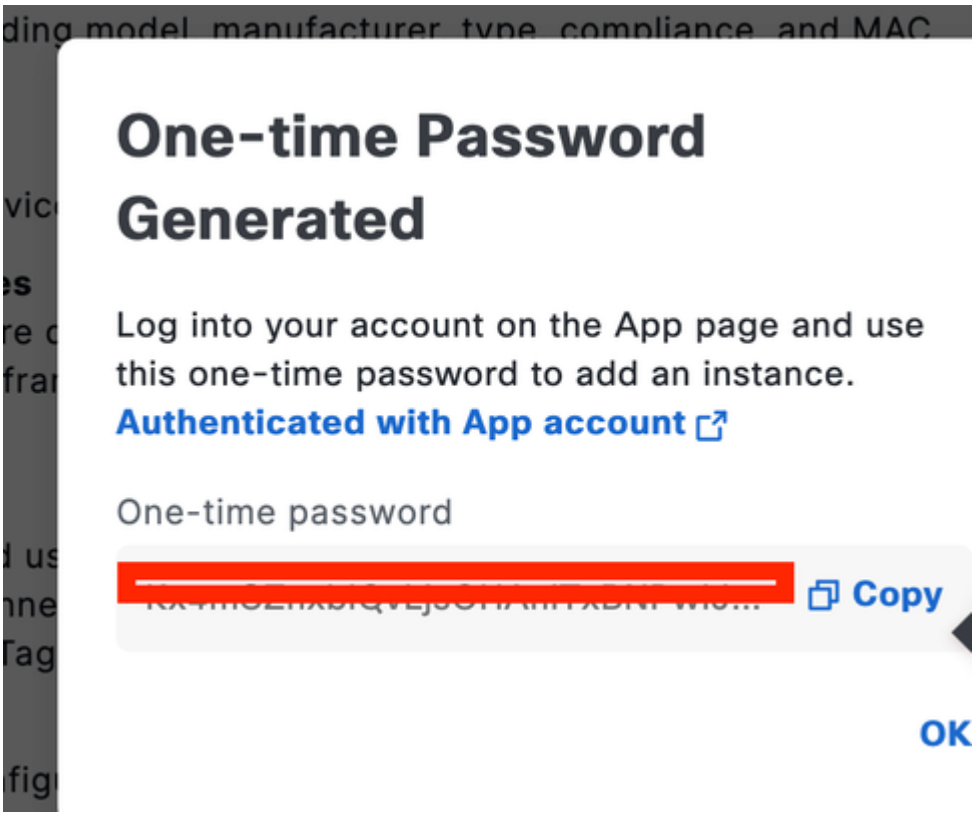
.



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

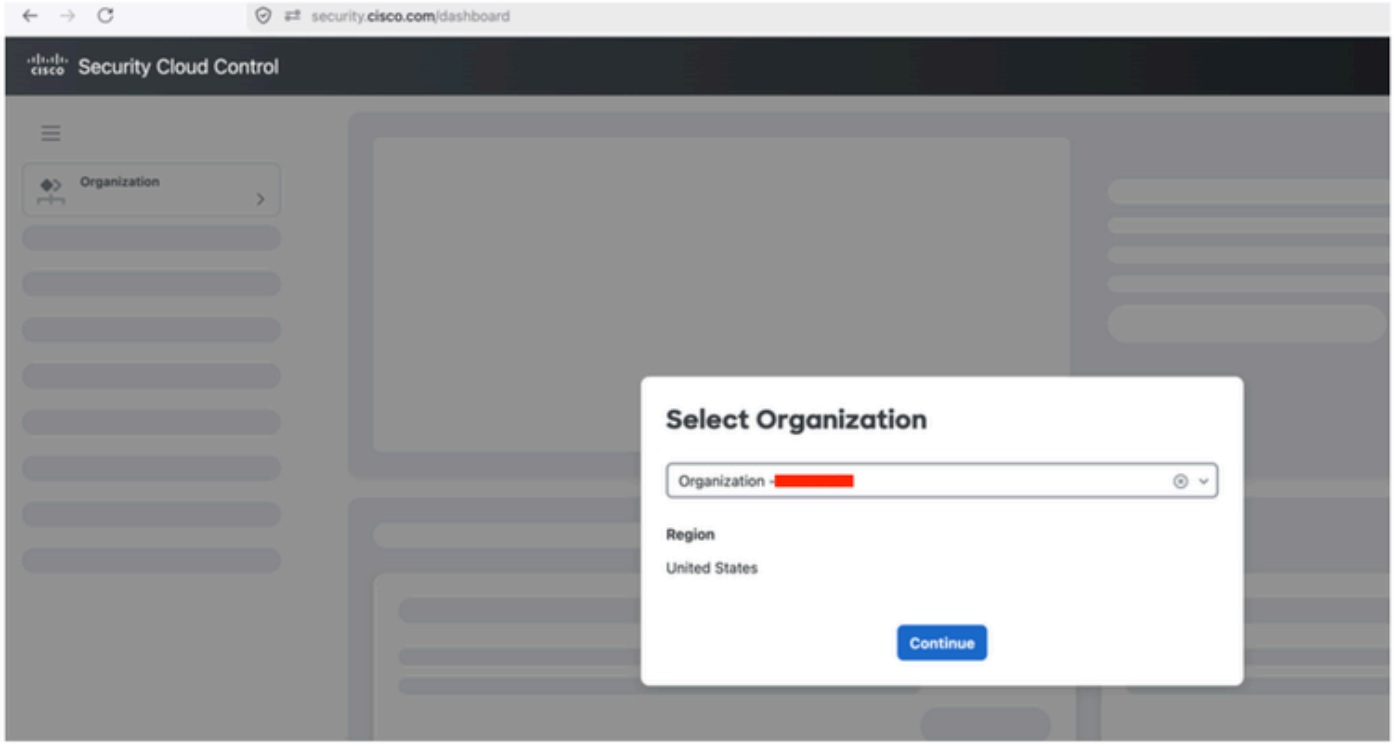


Cisco Secure Accessで使用するワンタイムパスワードをコピーします。

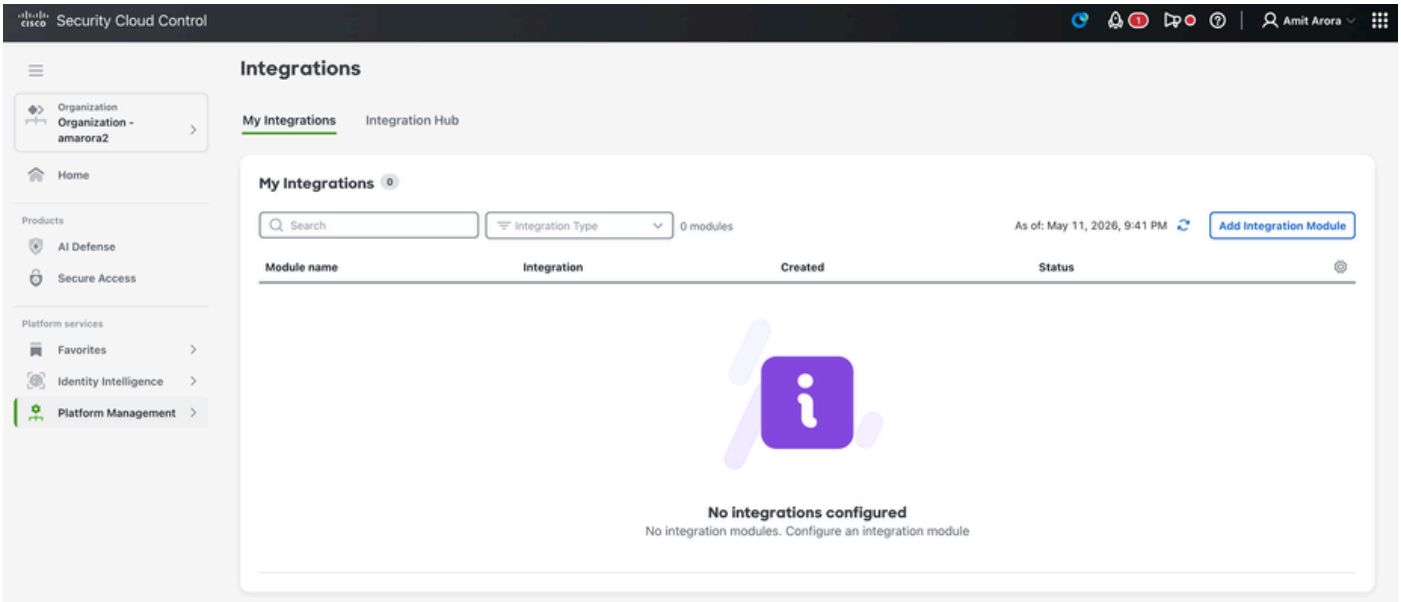


ステップ2:Cisco Secure AccessとISEの統合

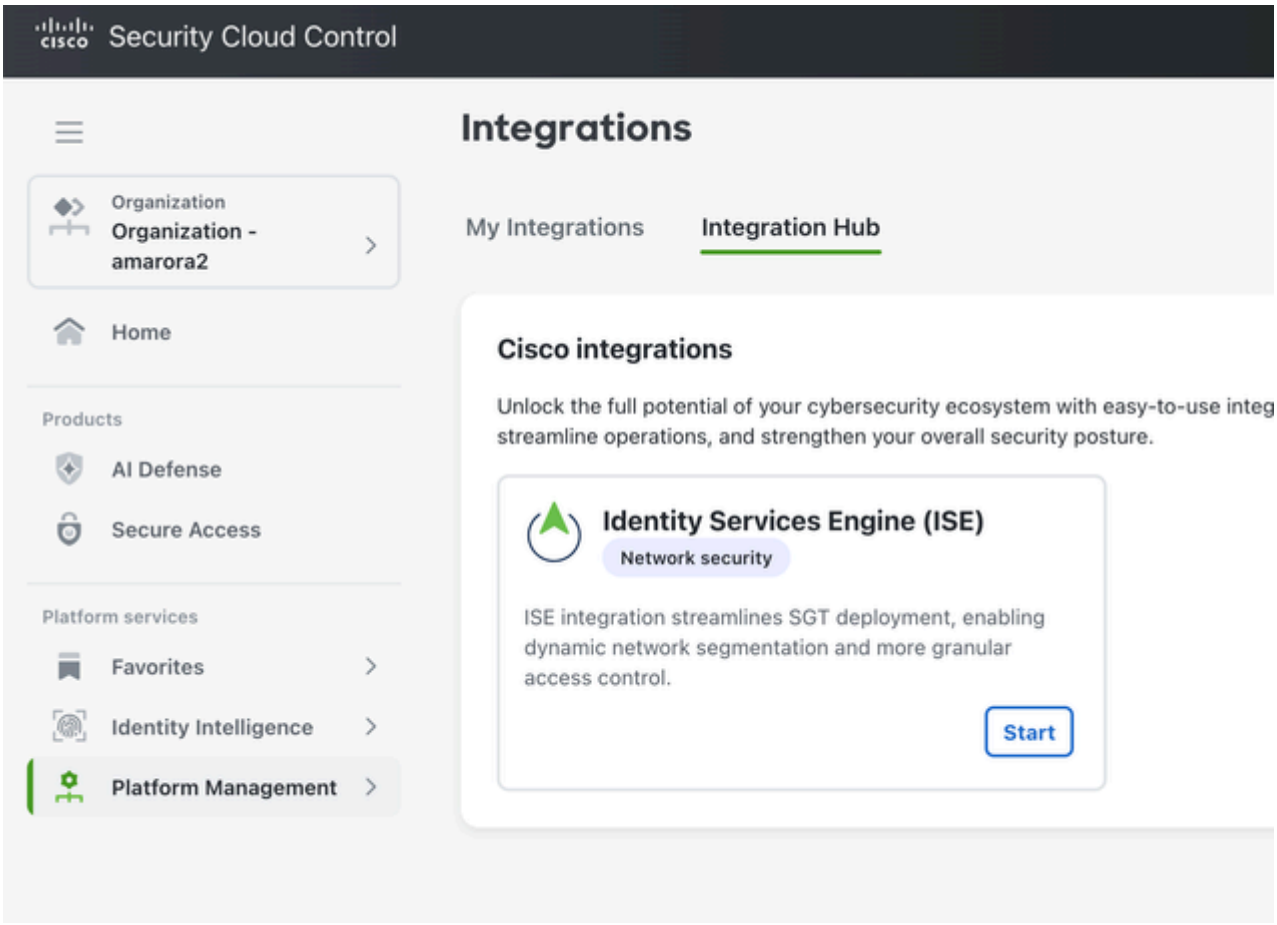
1. security.cisco.comにログインします。
2. Cisco Secure Access ORGを選択します。



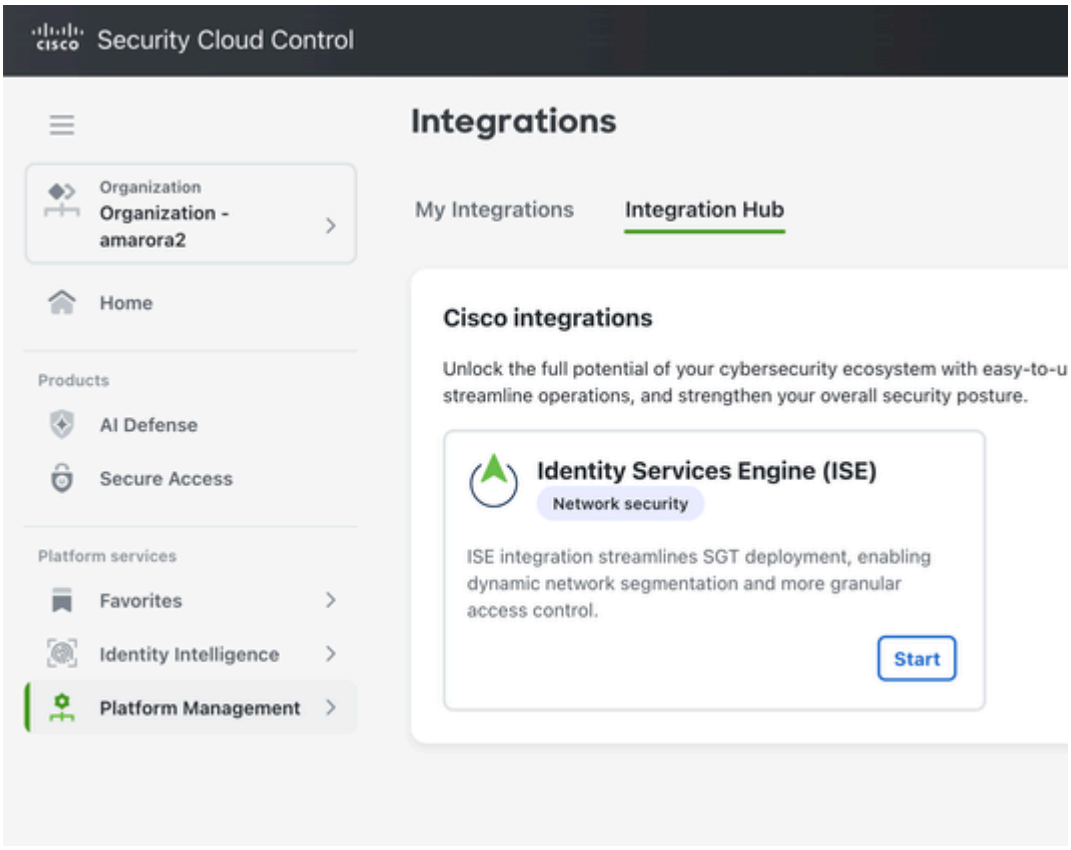
3プラットフォーム管理 – プラットフォーム統合をクリック



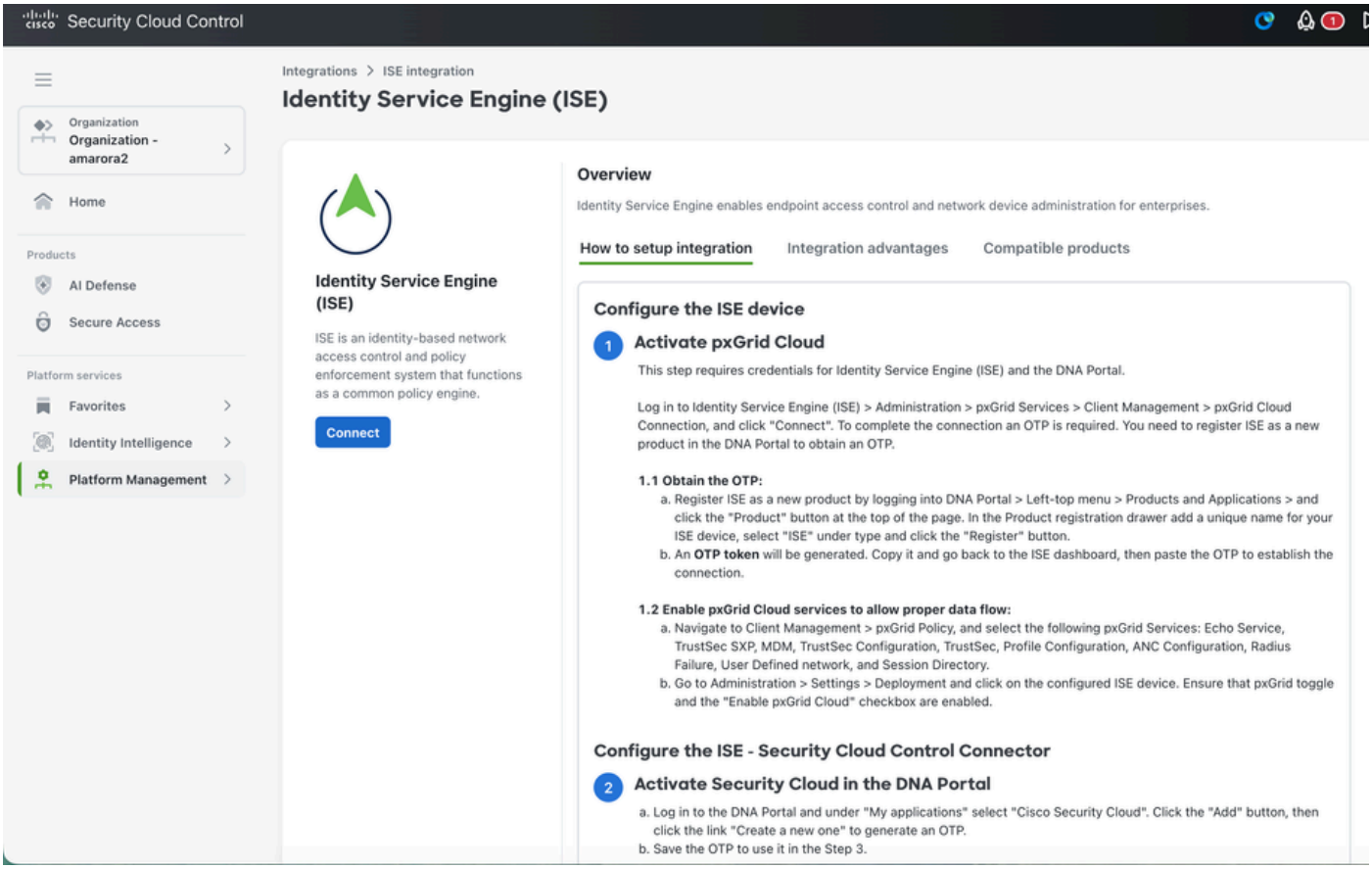
4 [Add Integration Module]をクリックします。



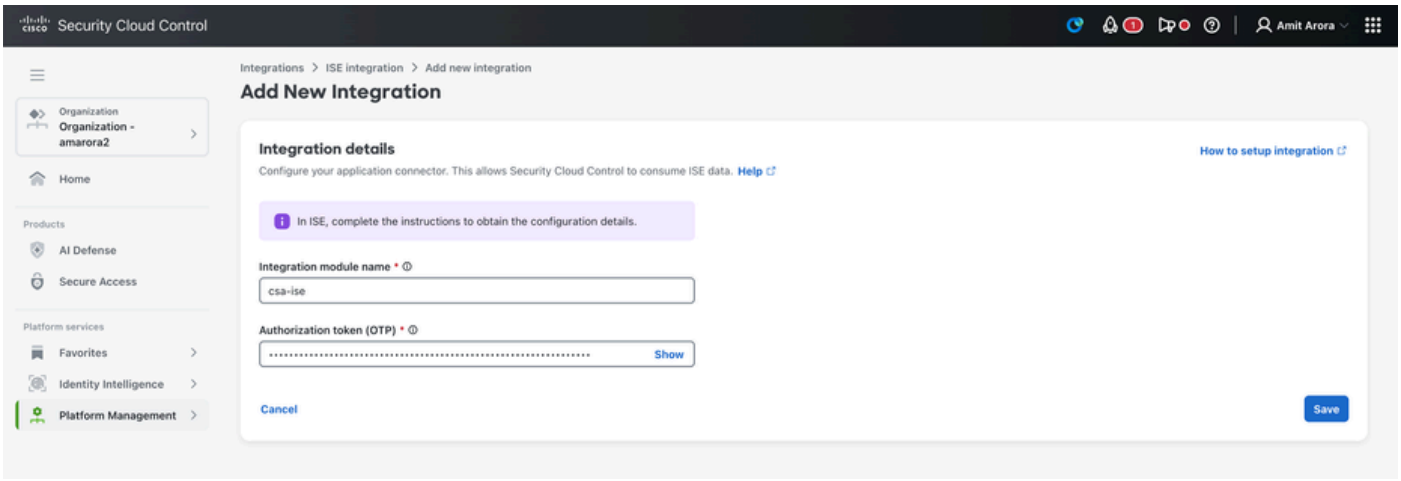
5 [開始]をクリックします。



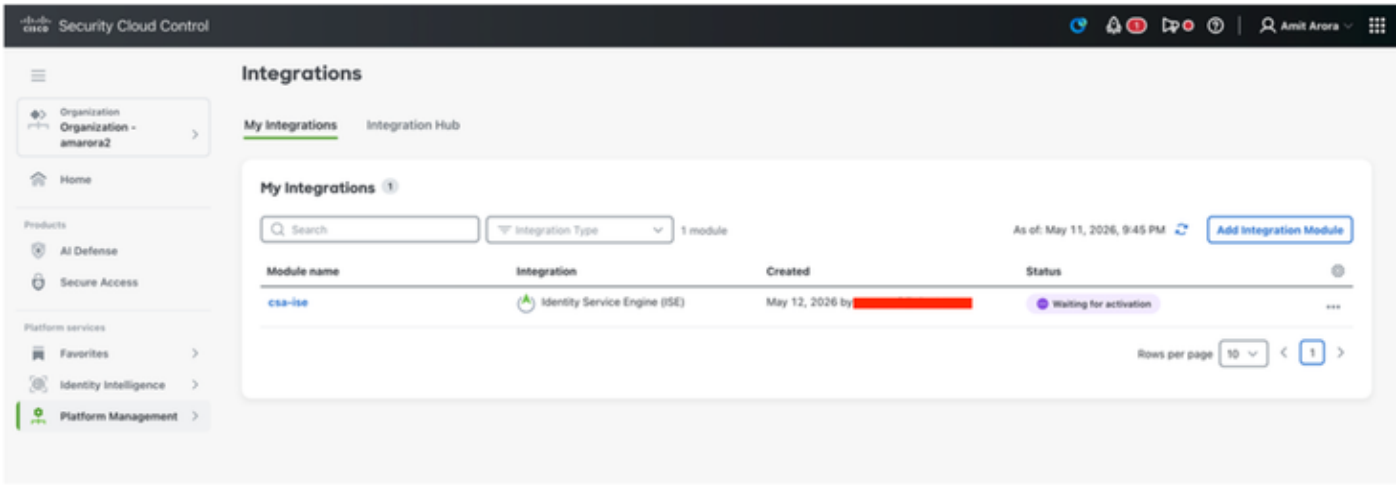
6 [接続]をクリックします。



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。



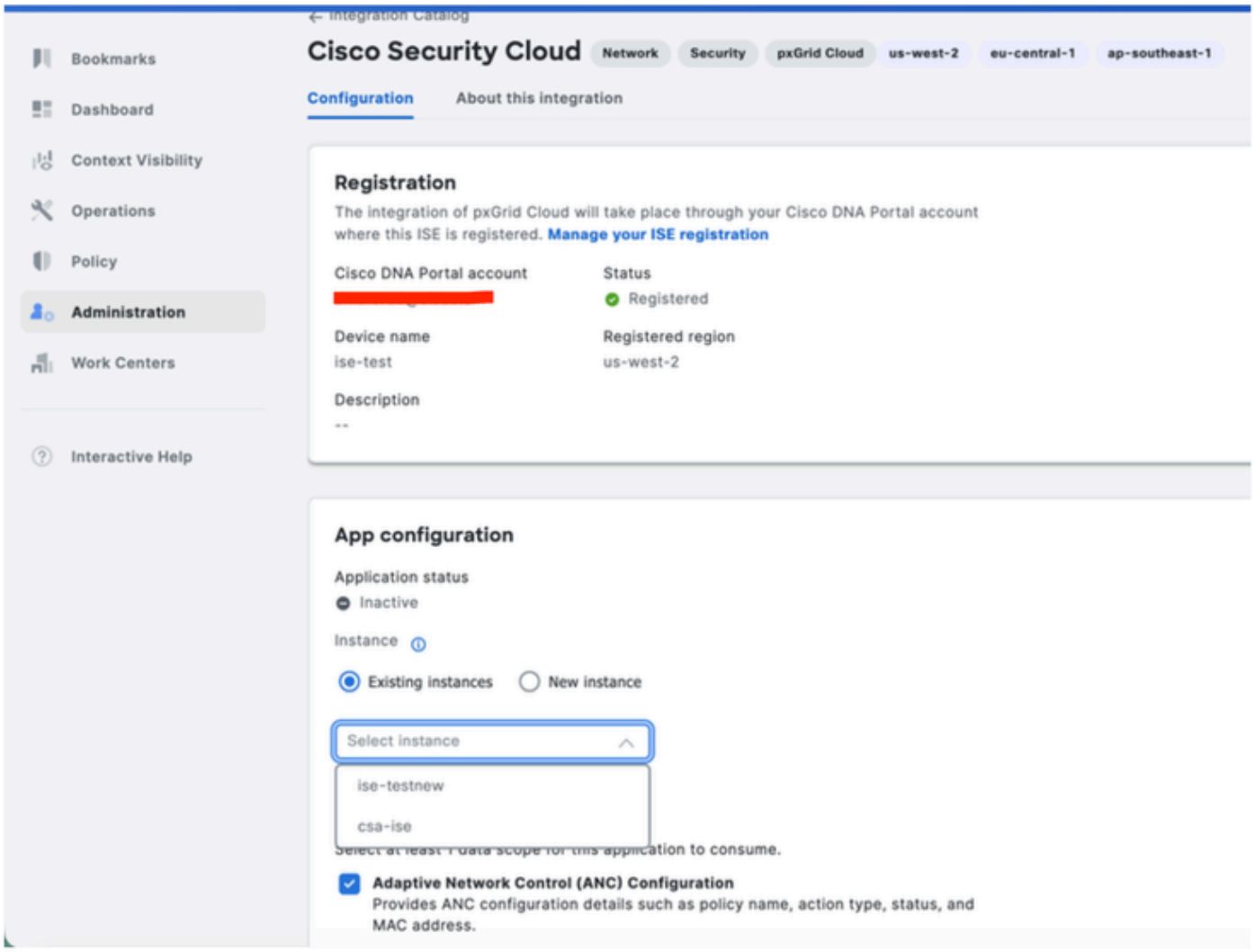
8 [Save]（保存）をクリックすると、 [Waiting for Activation Status]（ライセンス認証ステータスを待っています）が表示されます。



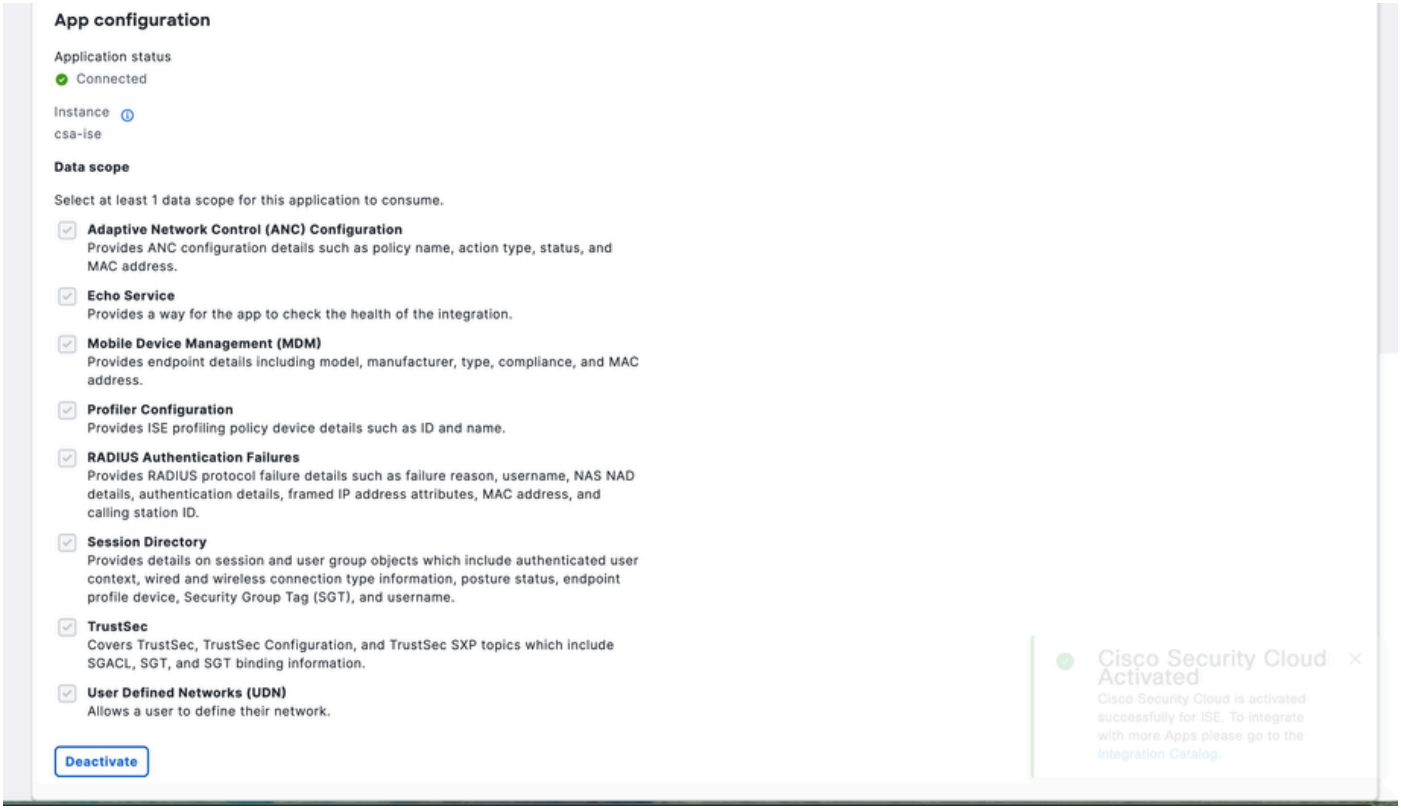
9 ISEにログインし、Administration - Deploymentの順に移動します。pxgridペルソナを持つノードをクリックします。Pxgrid接続の下の統合クラウドをクリックします。

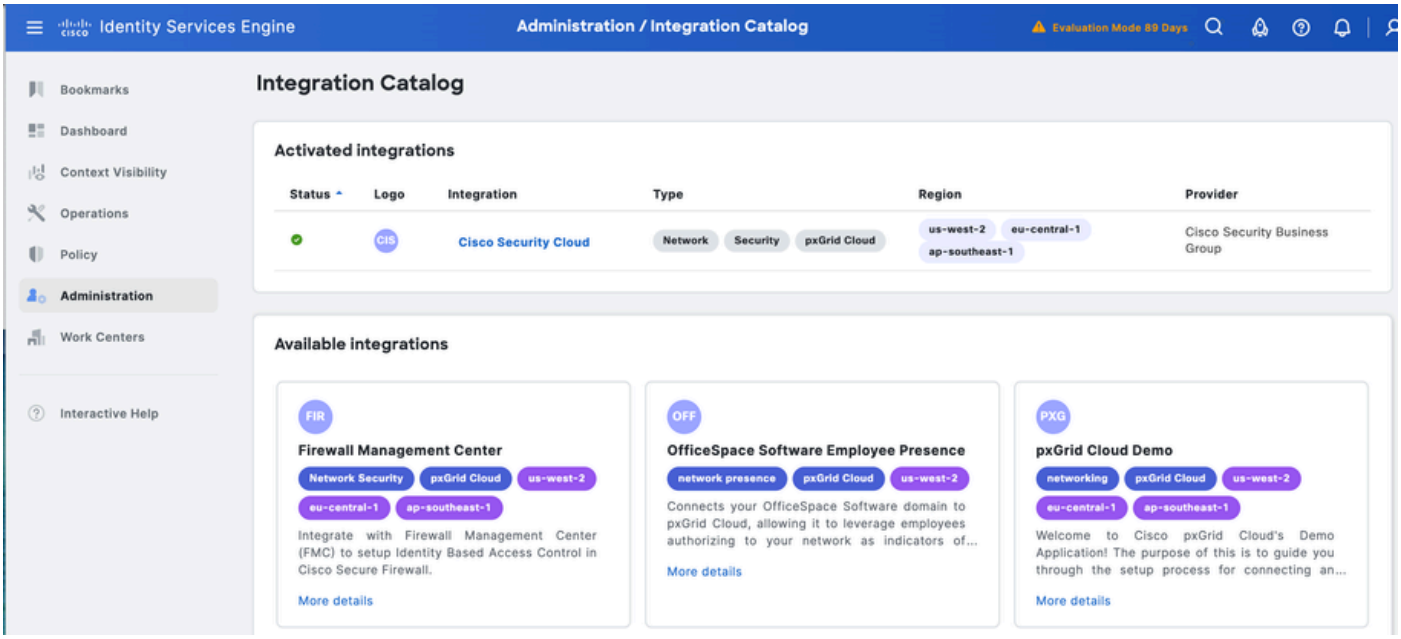
App configurationの下で、Security Cloud Controlで作成したISEインスタンスを選択し、

Activateをクリックします。



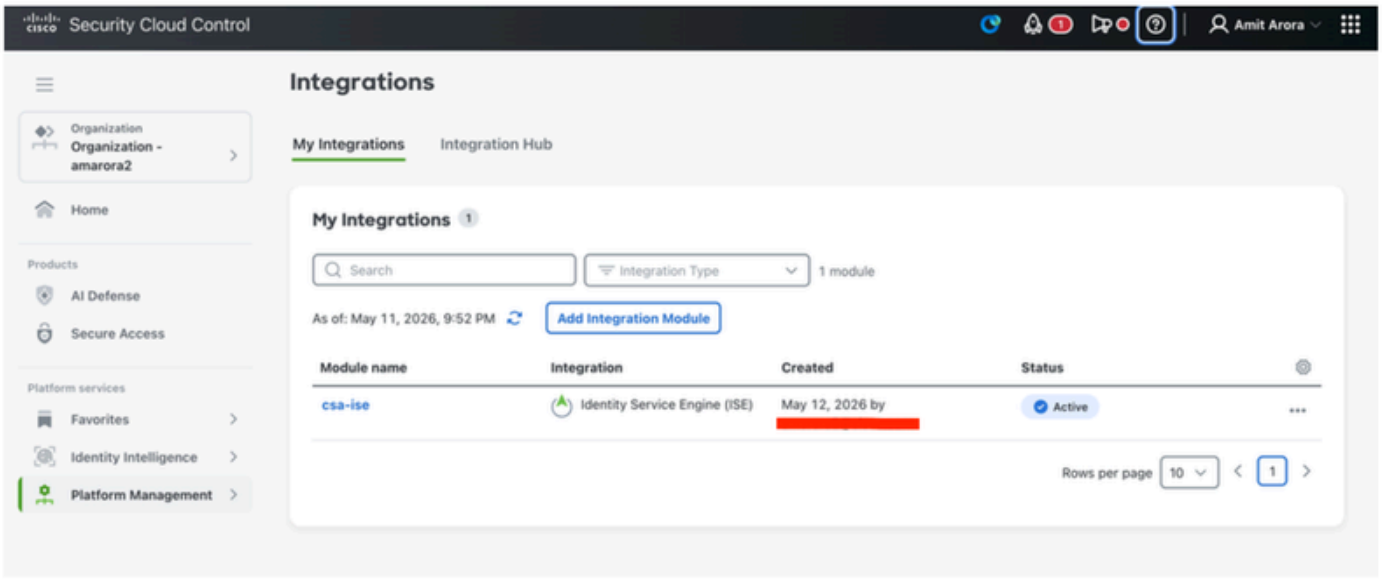
10 Application Statusがconnectedになりました。





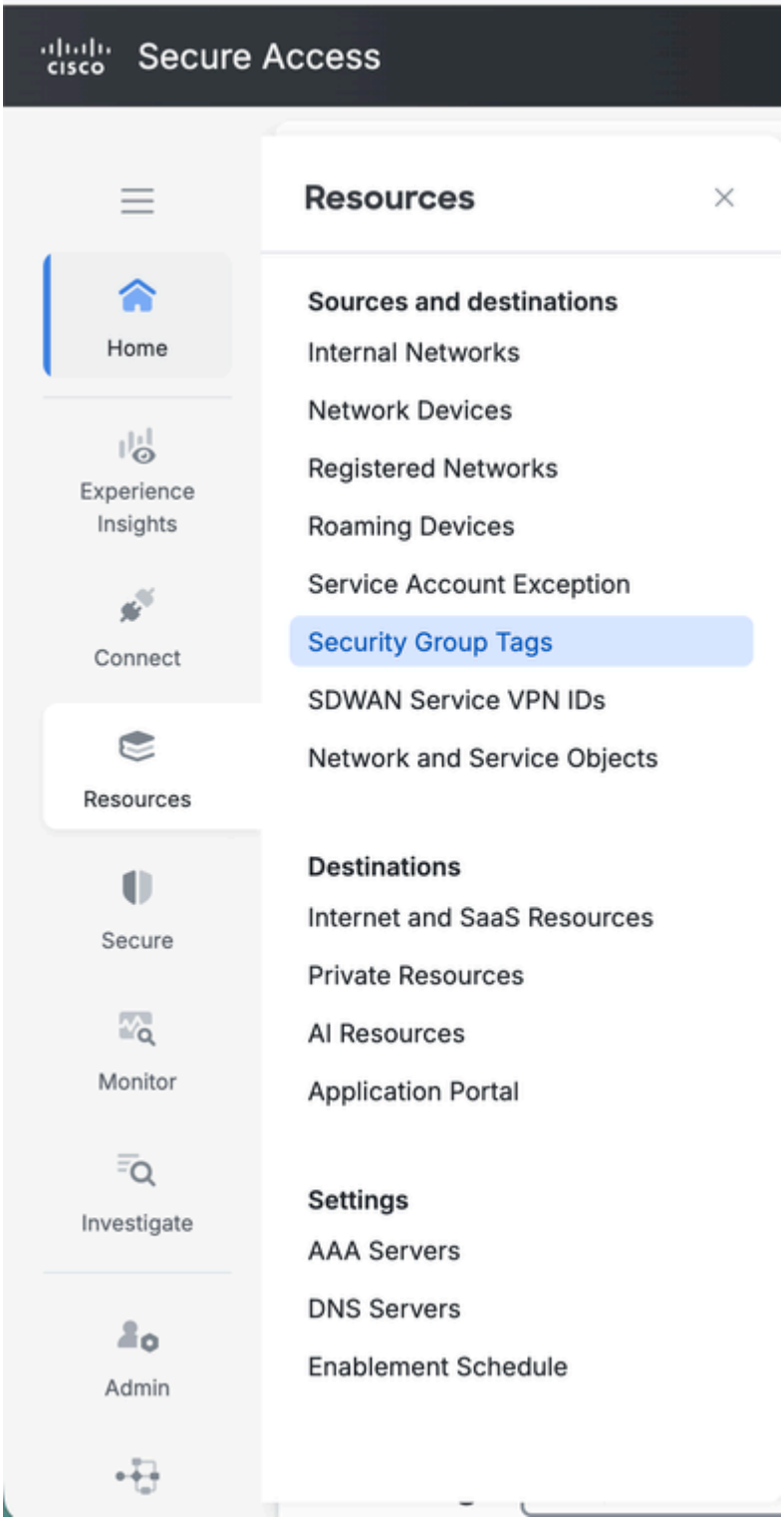
11 Security Cloud Controlへの口グイン – security.cisco.com

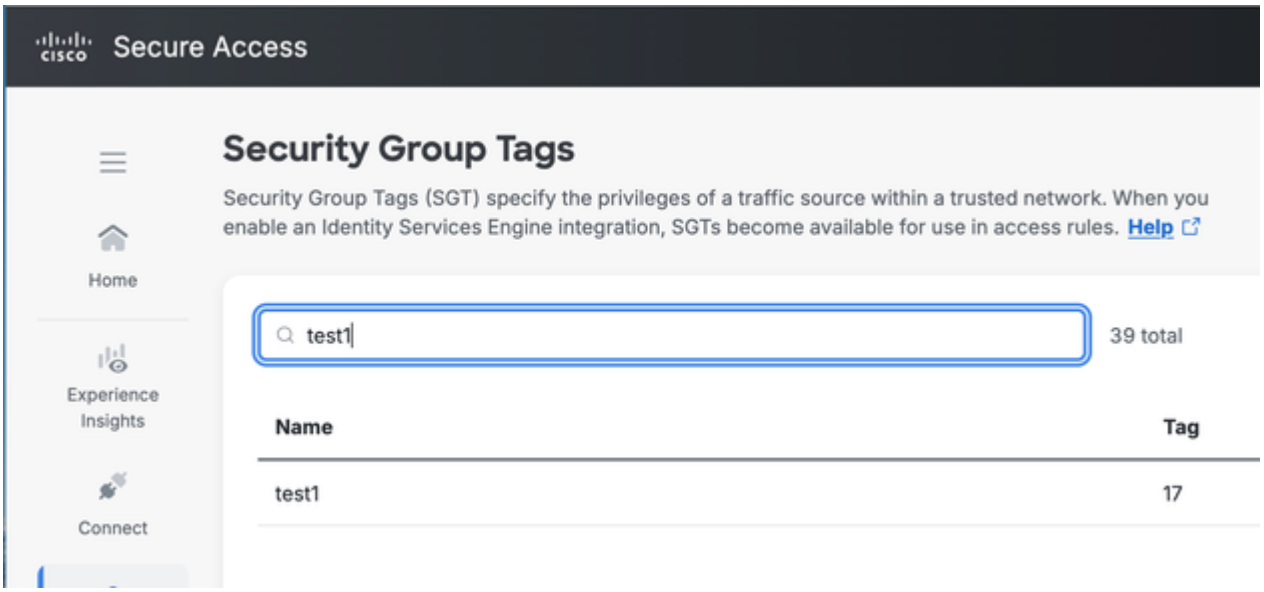
「プラットフォーム管理 – プラットフォーム統合」で、「統合ステータス」が「アクティブ」と表示されます。



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。


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

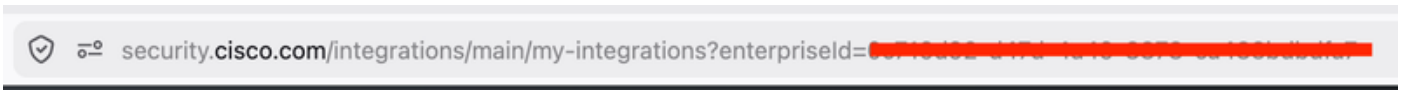
インフラストラクチャ

ERS

デバッグレベルのhermesコンポーネント。

SCC:

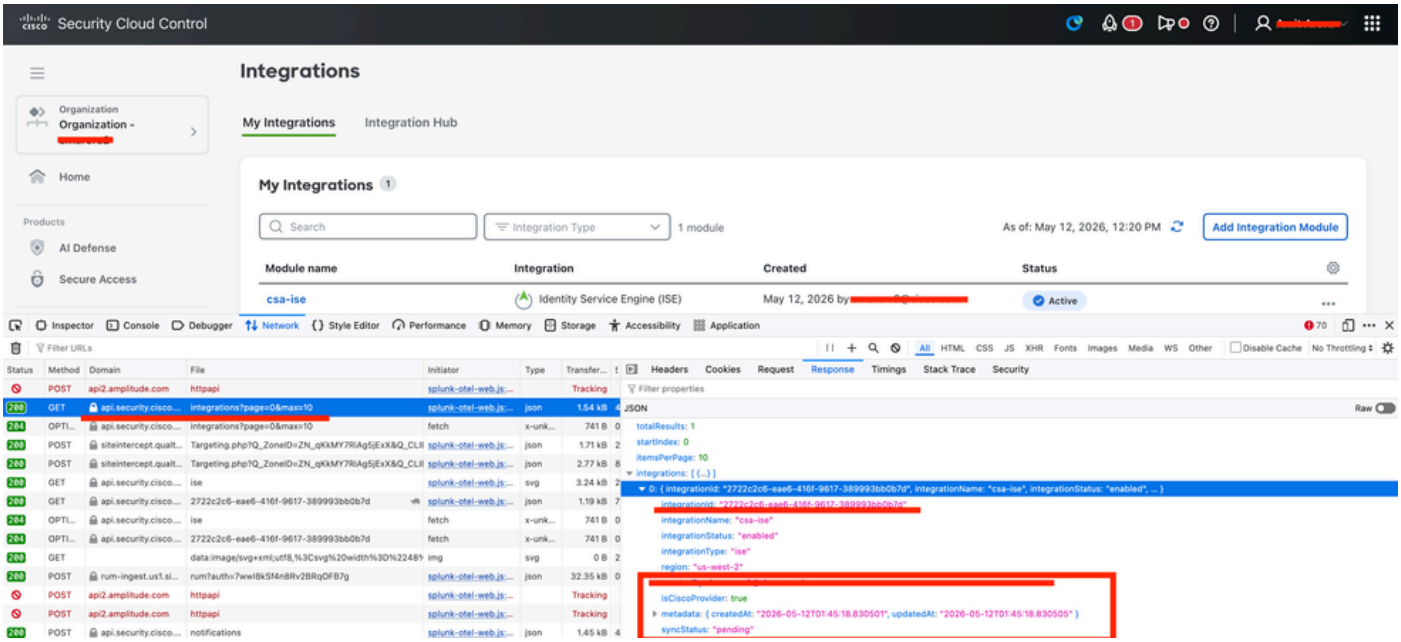
security.cisco.comのURLにあるエンタープライズID:



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。



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。