Identificação de grupo do Cisco Secure Access Integration com ISE para segurança na nuvem Pxgrid

Contents

Introdução

Este documento descreve como habilitar o compartilhamento de contexto entre o Cisco Secure Access e o Cisco Identity Services Engine

Requisitos

A Cisco recomenda que você conheça estes tópicos:

- Cisco Secure Access—Uma solução de borda de serviço de segurança (SSE - Security Service Edge) baseada em nuvem que fornece acesso de rede de confiança zero para permitir que os usuários se conectem facilmente à Internet e a aplicativos privados de qualquer dispositivo.
- Cisco Identity Service Engine (ISE) Versão 3.4 Patch 5.
- Cisco Security Cloud Control—Uma solução de gerenciamento unificado para seus produtos e identidade Security Cloud. O Security Cloud Control está incluído no Secure Access.

Background

Essa integração permite a criação automatizada de túneis confiáveis de filiais Catalyst SD-WAN para o Cisco Secure Access, facilitando a troca transparente de ID/nome de VPN e contexto SGT.

O Cisco Identity Services Engine (ISE) continua sendo a autoridade central para configuração e gerenciamento de SGT. Todas as atualizações executadas no ISE são sincronizadas automaticamente com o Cisco Secure Access. Se um SGT for excluído, as regras existentes que fazem referência a ele permanecerão ativas para garantir que a correspondência de tráfego continue como esperado.

No momento, estamos oferecendo disponibilidade limitada para mapeamentos de SGT, que

estende o suporte para incluir objetos de destino de SGT em suas regras de segurança. Além disso, o suporte para a construção de túneis SASE que transportam SGT da Meraki e Cisco Secure Firewall será disponibilizado em breve

Caso de uso:

Política baseada em espaço de nome SGT:

Como administrador de segurança, o Kit deseja aplicar a microssegmentação contígua usando SGT do ISE local para o tráfego SSE privado e vinculado à Internet.Capacidade de importar SGT para aplicar políticas.

Componentes Utilizados

As informações neste documento são baseadas em:

- Identity Service Engine (ISE) versão 3.4 Patch 5
- Acesso seguro
- Nuvem de segurança da Cisco

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Visão geral da configuração de compartilhamento de contexto

- Conectar o ISE à nuvem de segurança da Cisco
- Conecte o Cisco Secure Access ao ISE

Configurar

Este guia divide a configuração geral nas seguintes etapas principais:

1. Conecte o Cisco ISE ao Cisco Security Cloud
2. Conecte o acesso seguro da Cisco ao Cisco ISE
3. Tags de grupos de segurança no Cisco Secure Access

Antes de Começar

- Verifique se você instalou e ativou a licença Advantage na implantação do Cisco ISE.
- O agente do DNA Cloud cria uma conexão HTTPS de saída com o Cisco DNA Cloud. Portanto, você deve definir as configurações de proxy do Cisco ISE se a rede usar um proxy para acessar a Internet. Para definir as configurações de proxy no Cisco ISE, navegue até **Administration** > **System** > **Settings** > **Proxy**
- Verifique se a porta 443 está aberta para conexão de saída do Cisco ISE para o portal Cisco pxGrid Cloud. Se as configurações de firewall ou proxy estiverem definidas, verifique se estes URLs não estão bloqueados:

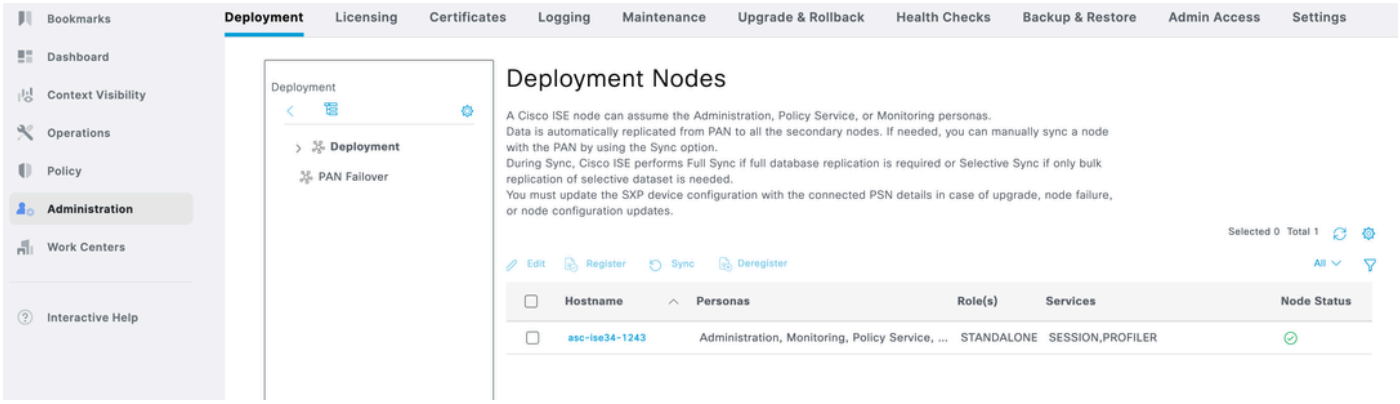
https://dna.cisco.com

https://security.cisco.com/

Etapa 1: Habilitar a nuvem Pxgrid no ISE

1 Navegue até a GUI do ISE.

2 Clique em Administration - Deployment (Administração - Implantação).

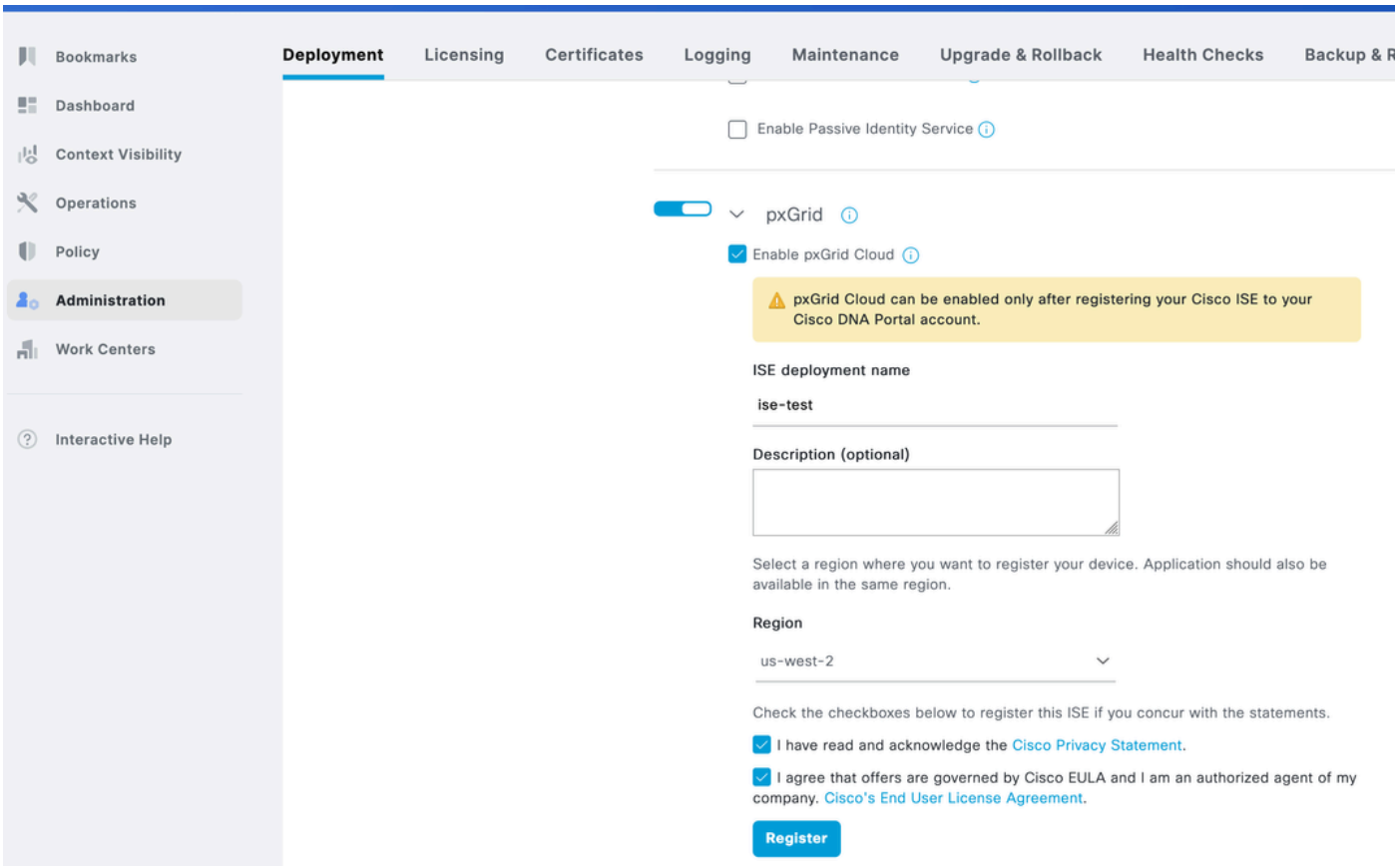


3 Clique no nó e role para baixo até a parte inferior.

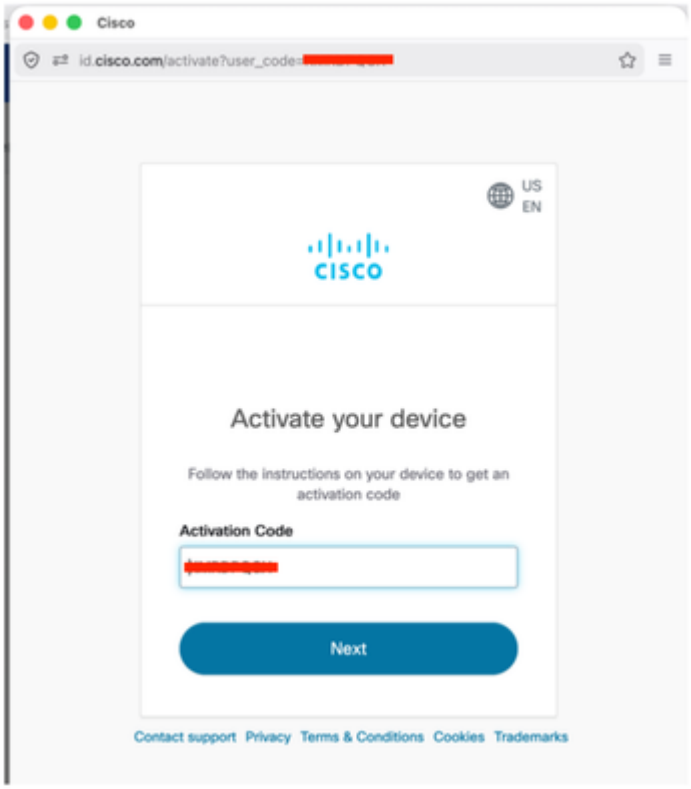
Inserir nome da implantação do ISE

Selecione a região como US West 2, que é a única região suportada até agora.

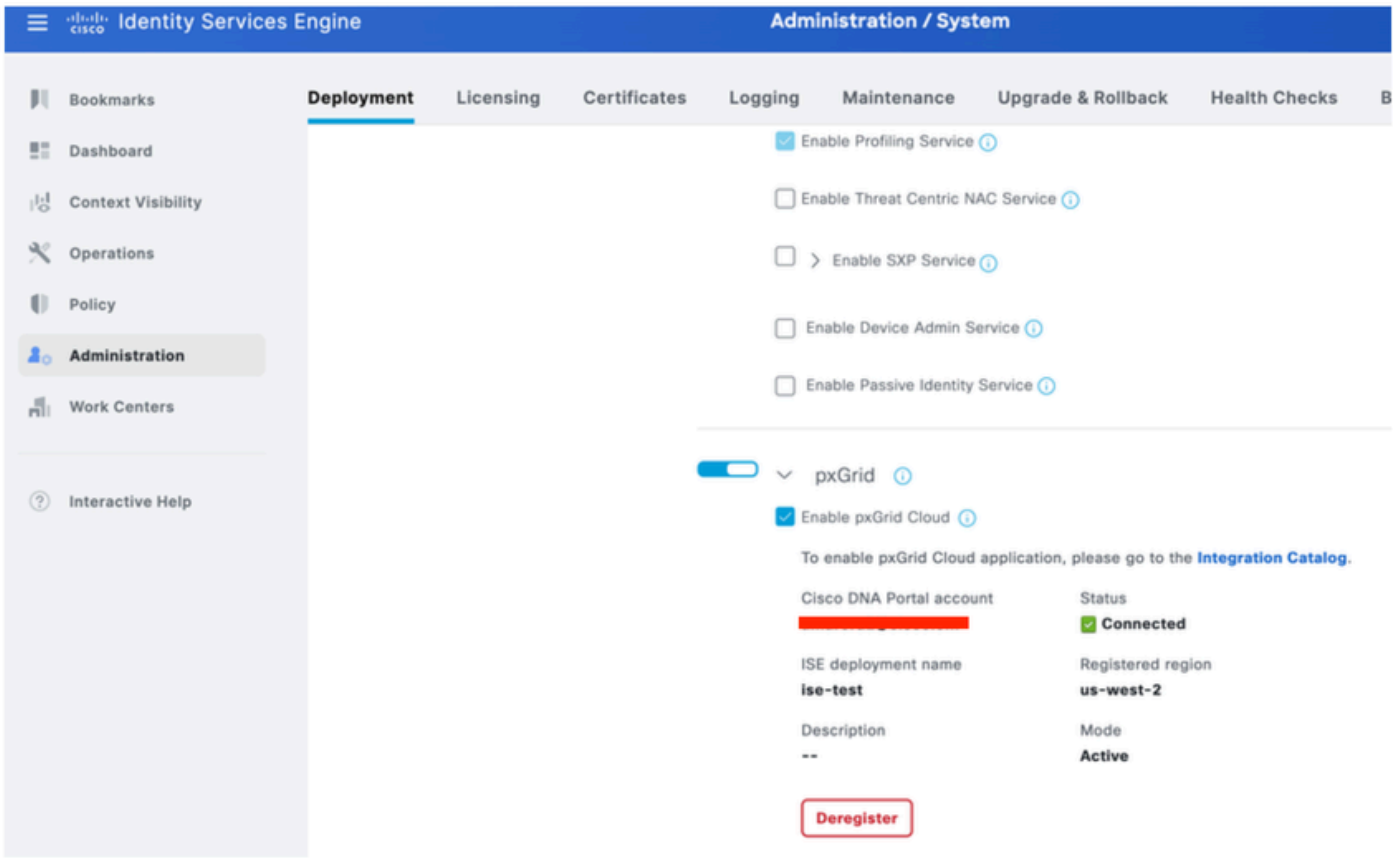
Marque ambas as caixas de seleção e clique em Registrar.



4 Você verá uma janela pop-up com o código de ativação preenchido automaticamente.Clique em Avançar,



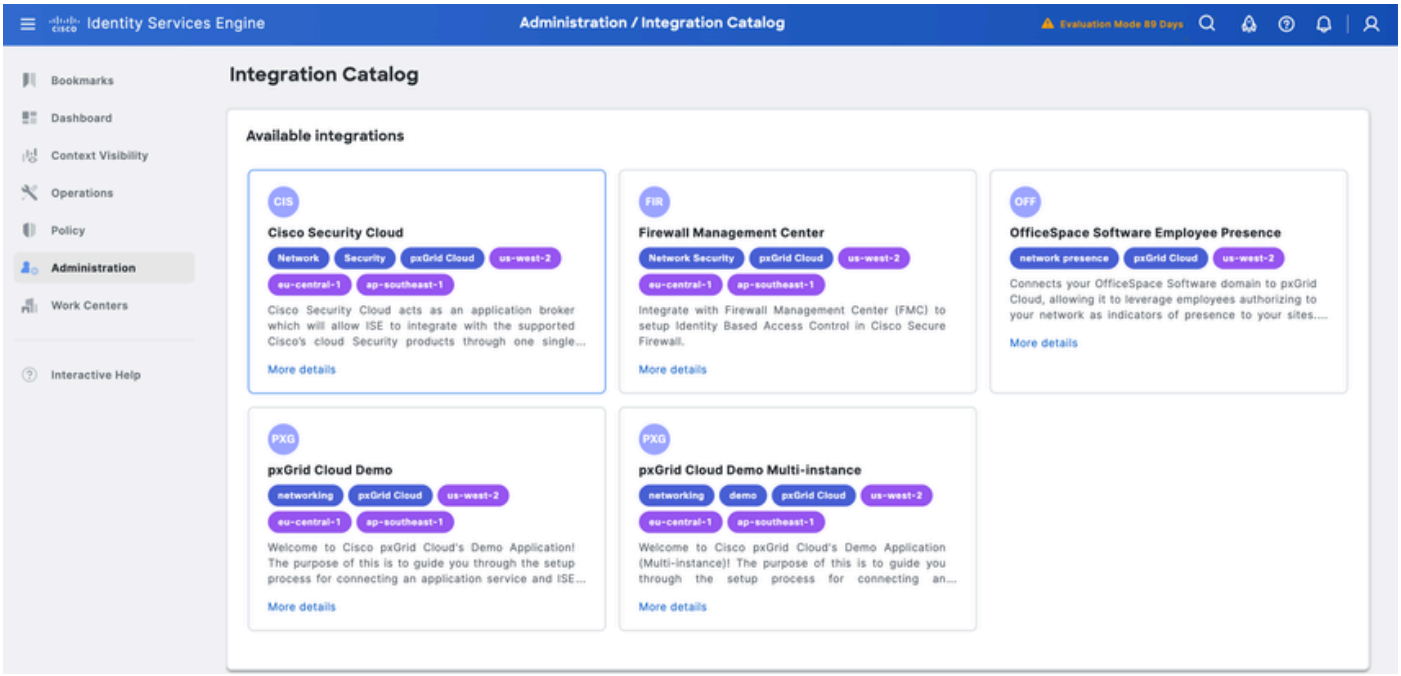
5 O ISE aparecerá conectado à nuvem Pxgrid.



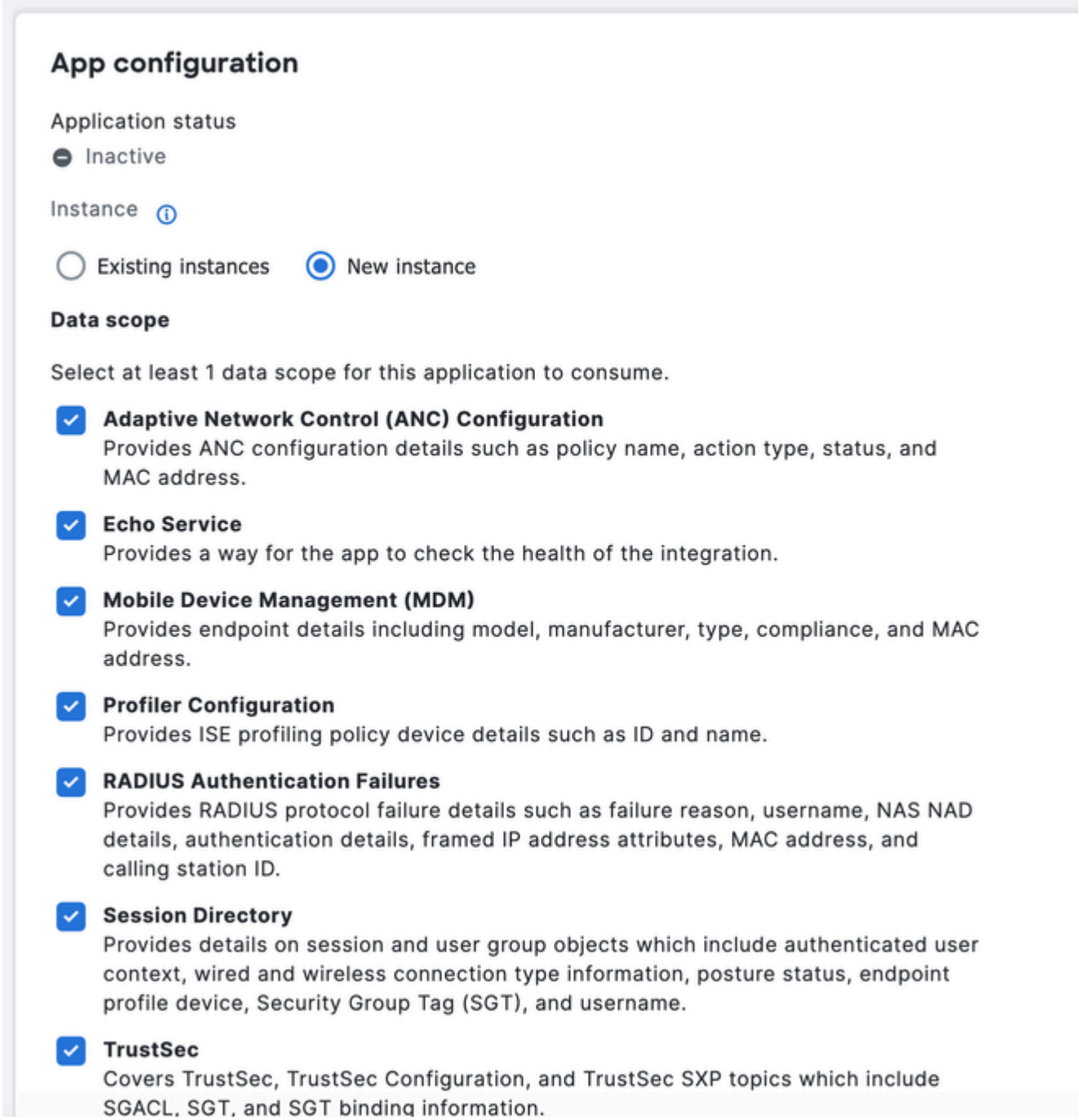
6 Clique no link Catálogo de integração na Etapa 5.

Em Available Integrations - Clique em Cisco Security Cloud

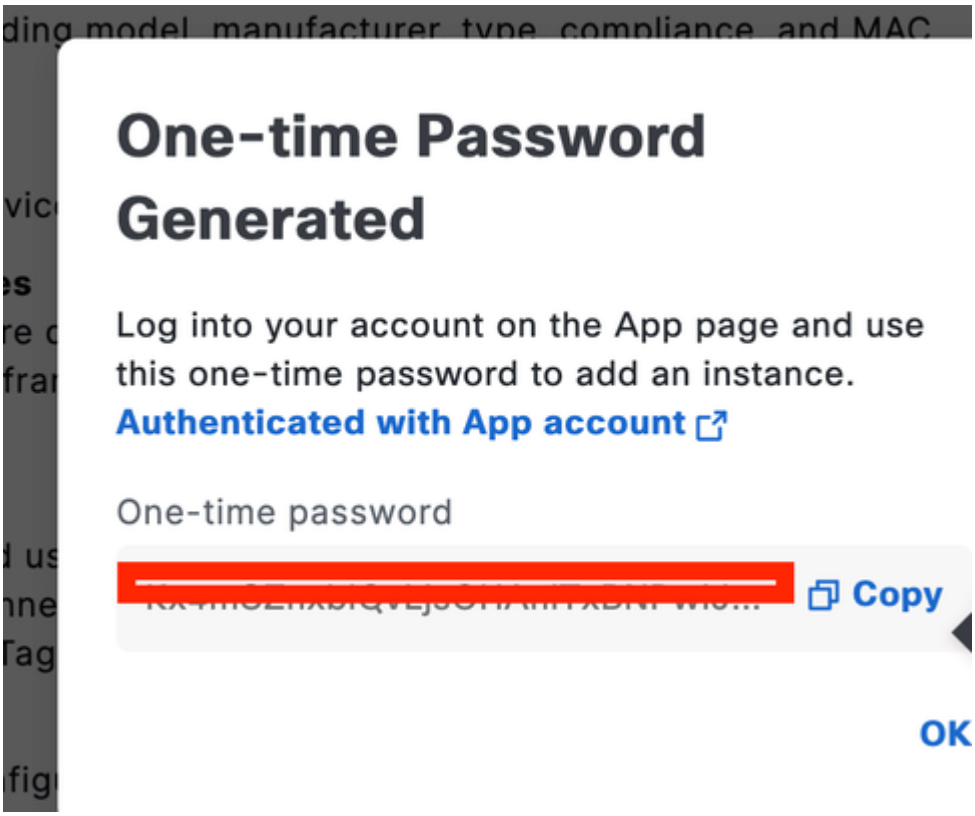
.



7 Em Configuração do aplicativo, clique em Nova instância e em Ativar

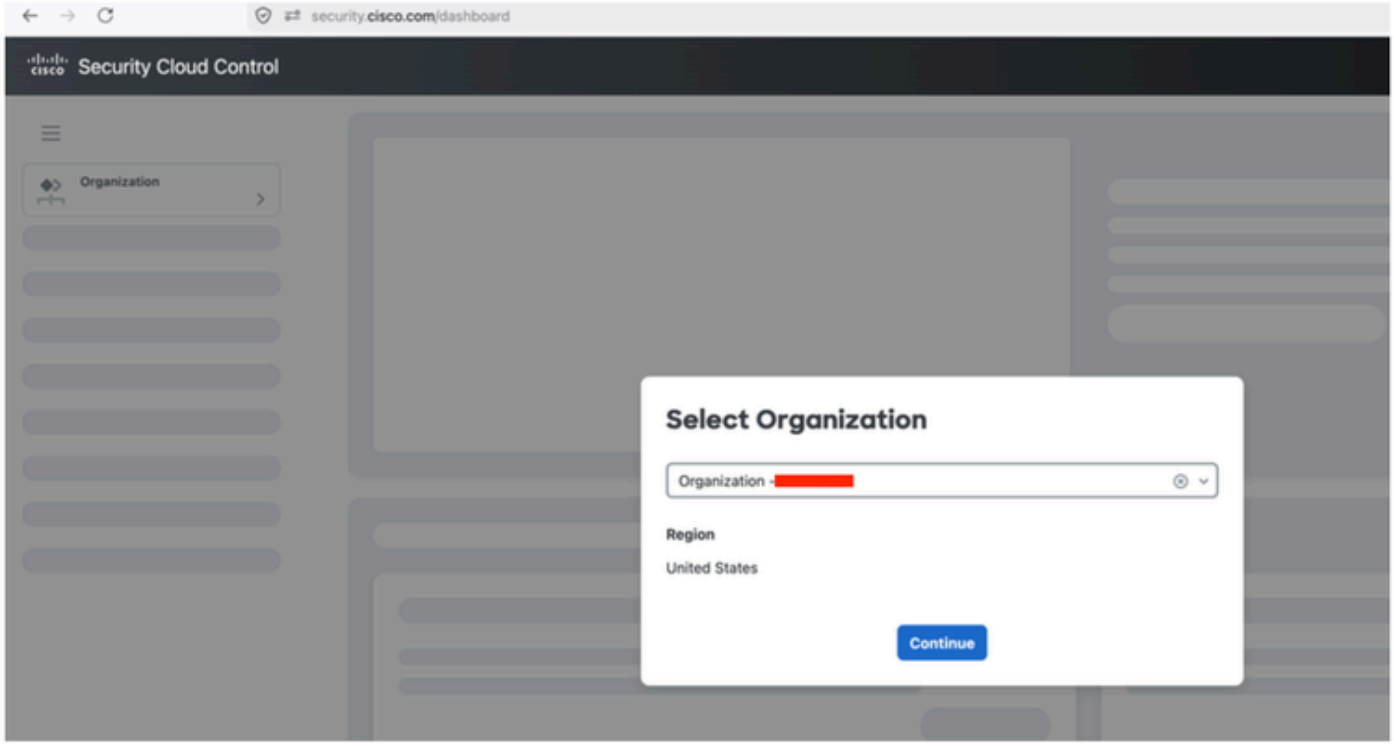


Copie a senha ocasional como ela será usada no Cisco Secure Access.

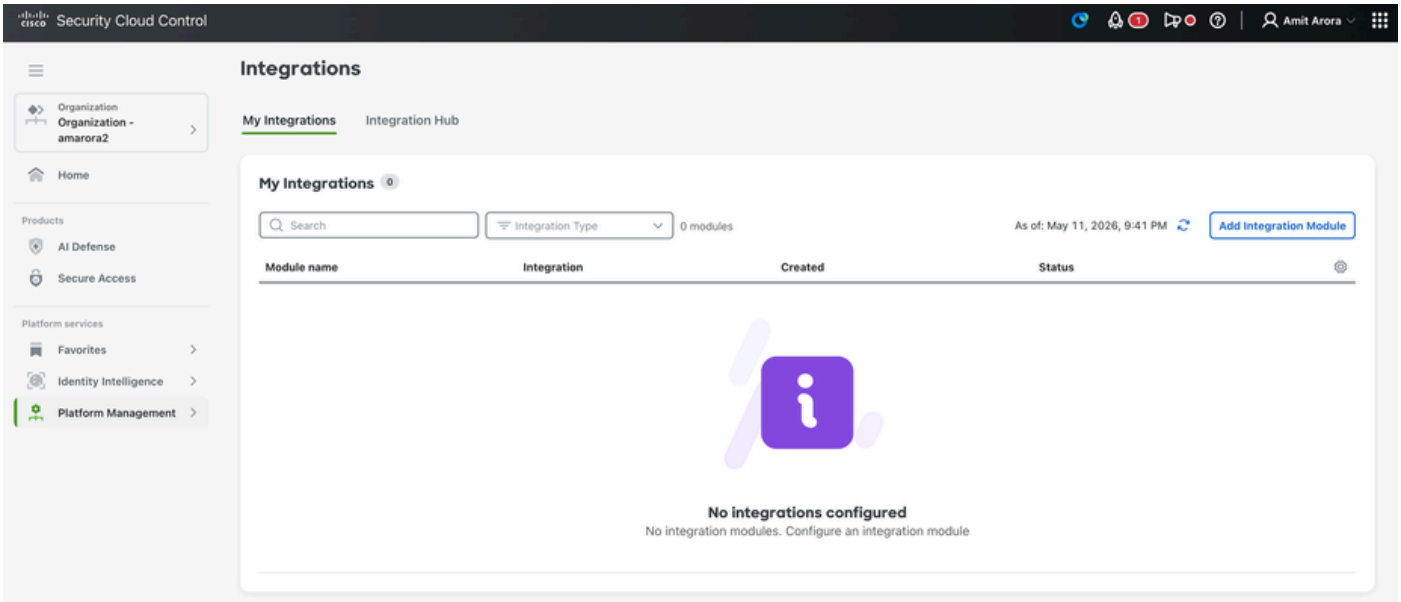


Etapa 2: Integrar o Cisco Secure Access ao ISE

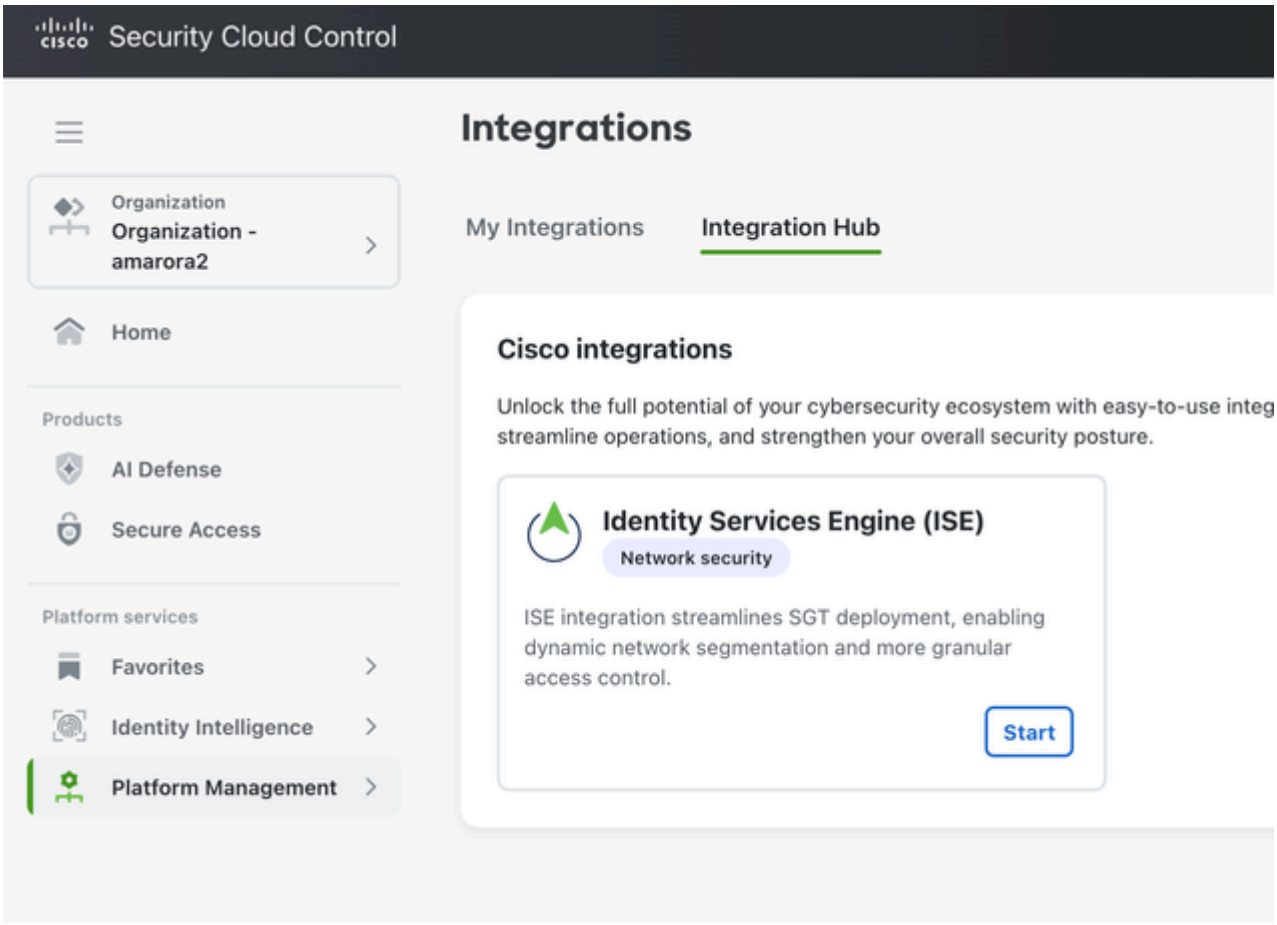
1. Faça login em security.cisco.com.
2. Selecione o Cisco Secure Access ORG



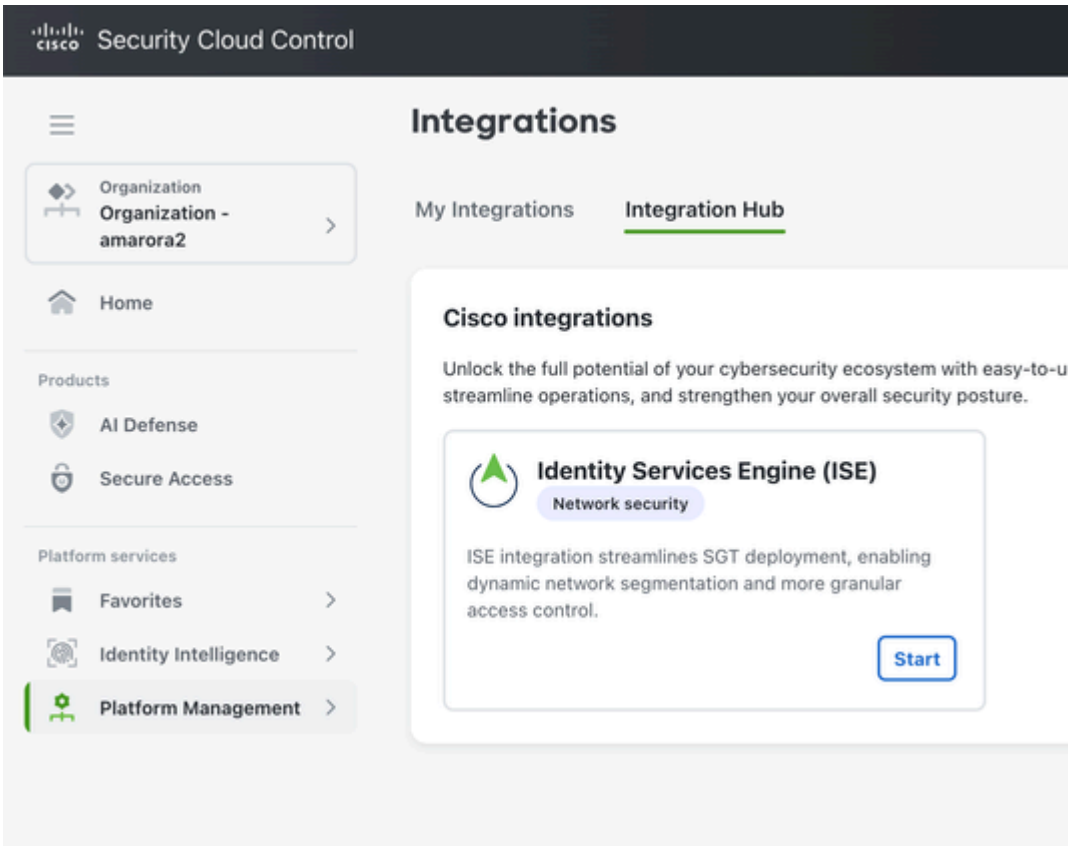
3 Clique em Gerenciamento de plataforma - Integrações de plataforma



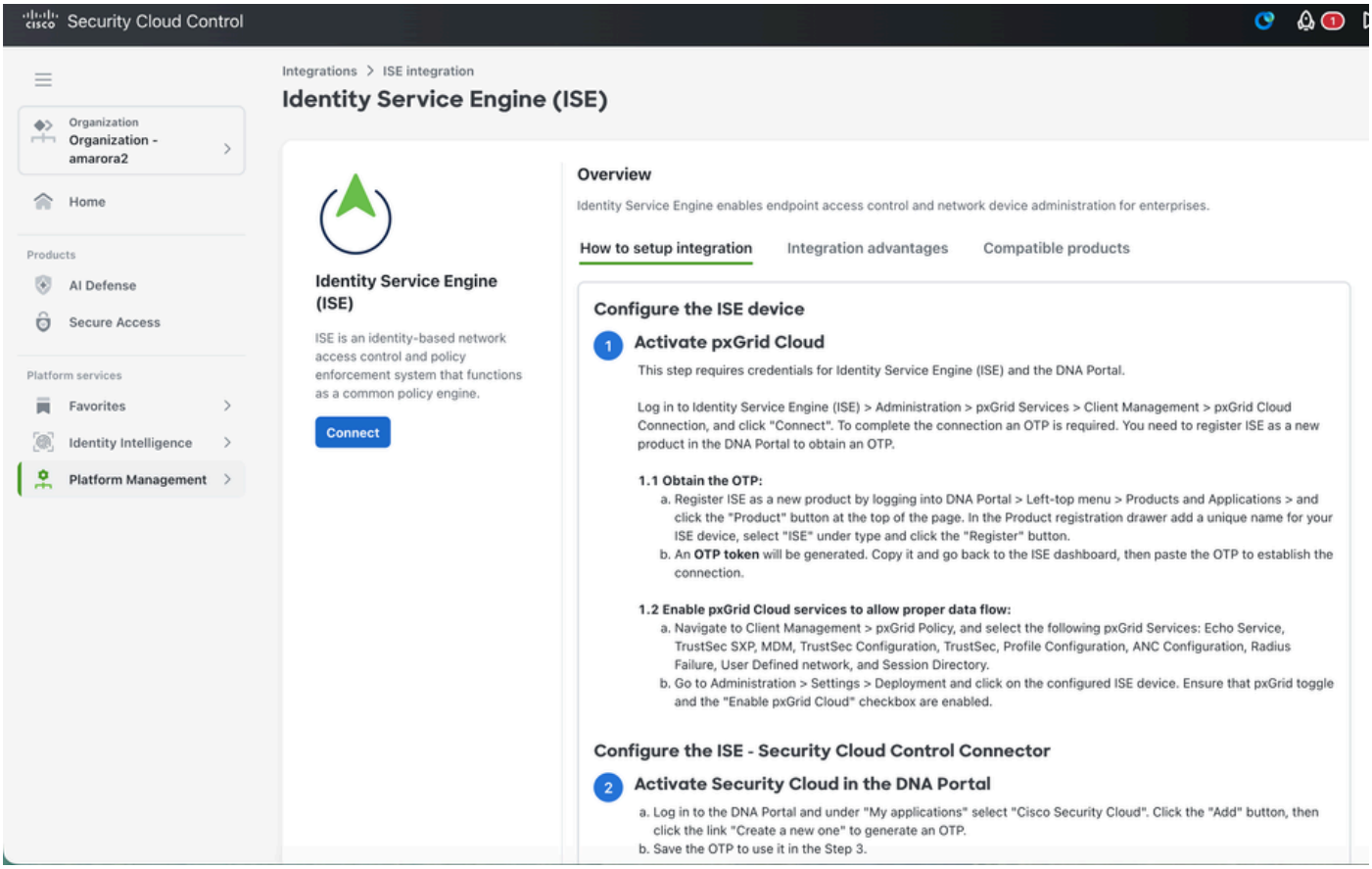
4 Clique em Adicionar módulo de integração



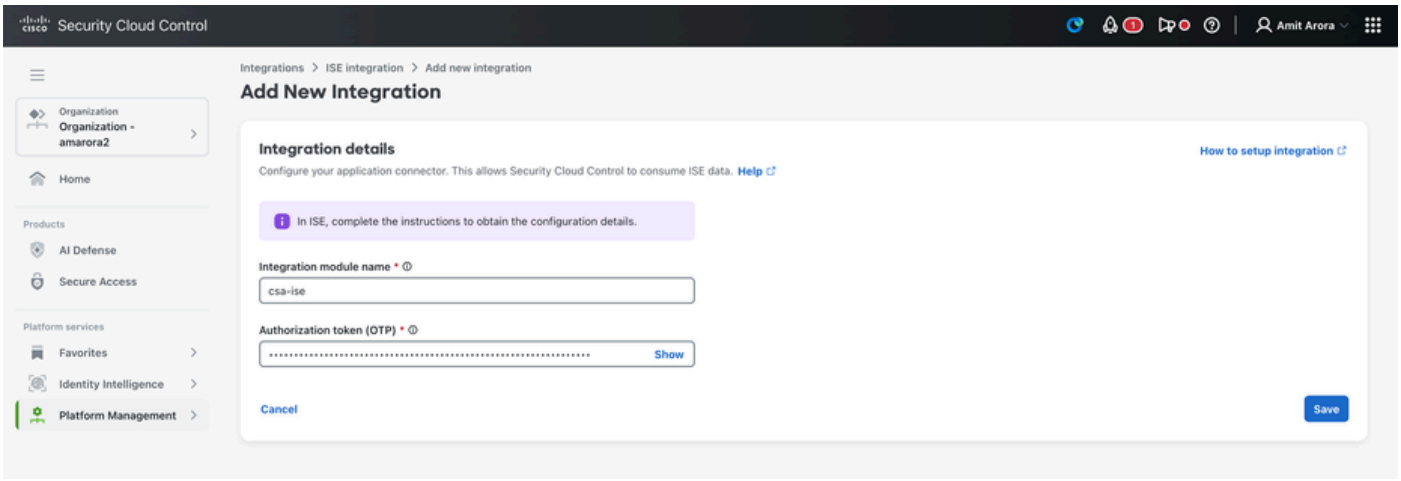
5 Clique em Iniciar



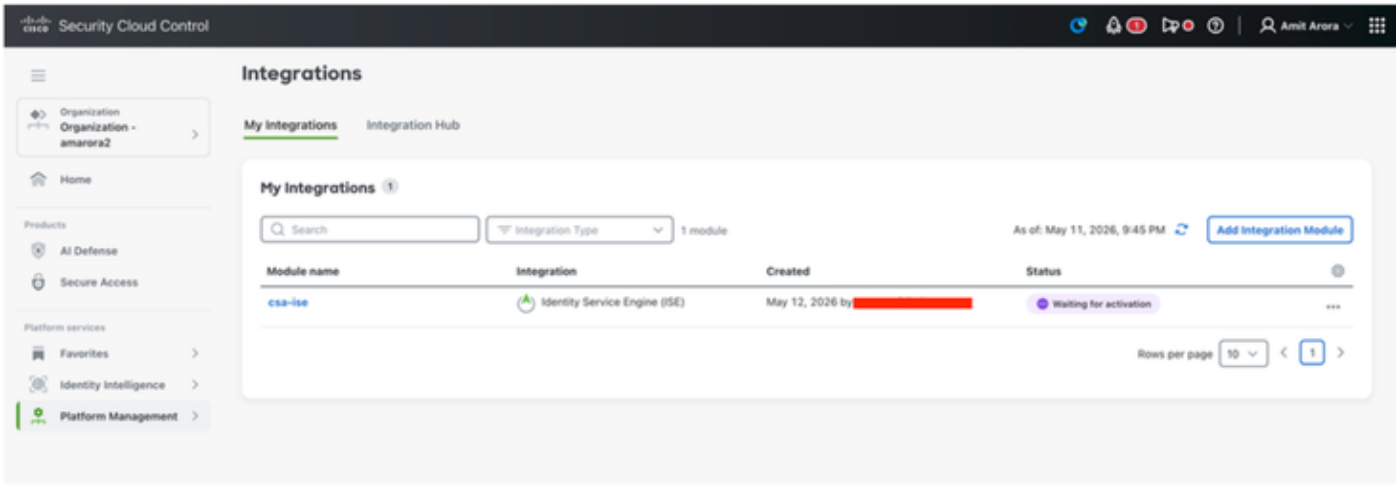
6 Clique em Connect



7. Insira o nome do módulo de integração e o OTP do Cisco ISE e clique em Salvar



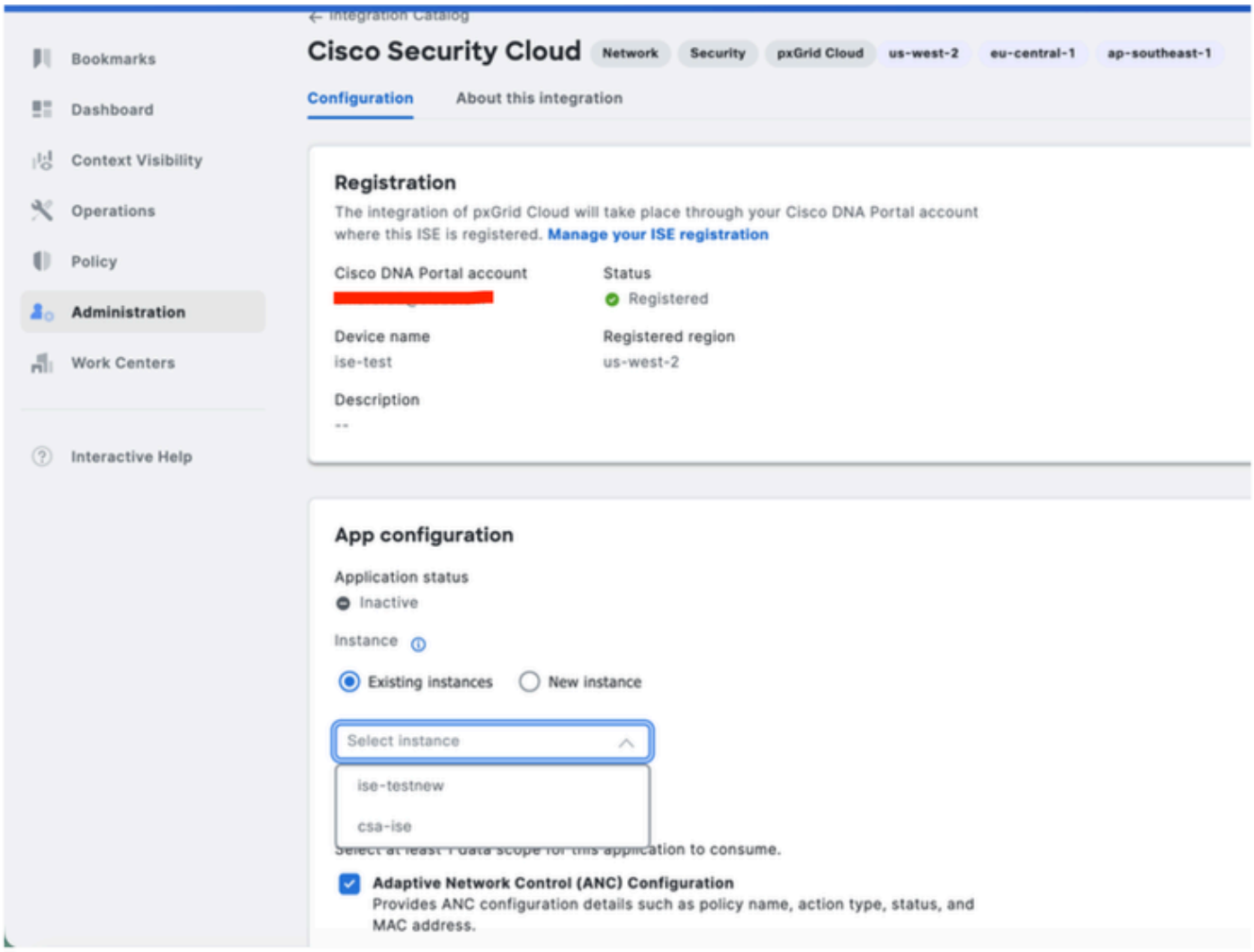
8 Depois de clicar em Save (Salvar), veremos Waiting for Ativation Status (Aguardando status de ativação).



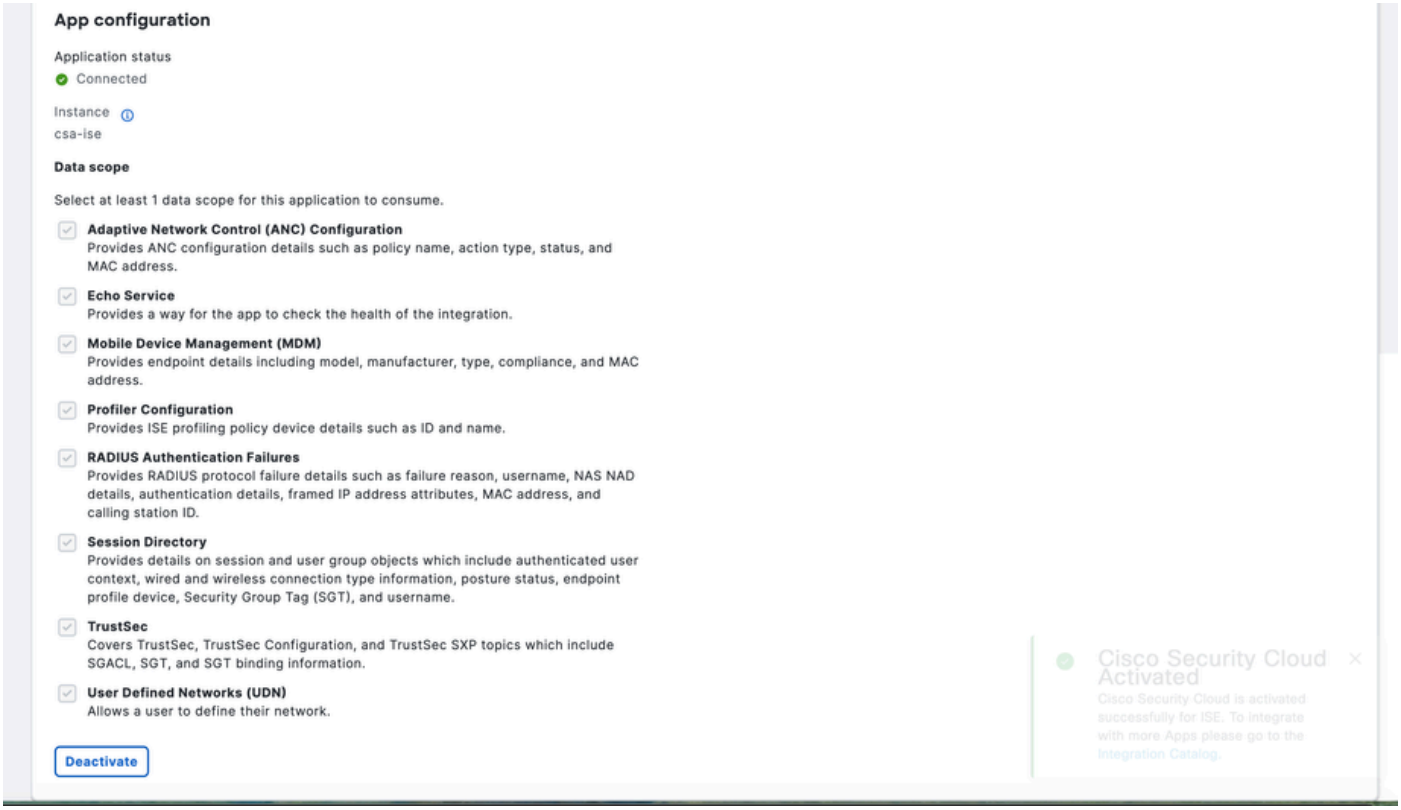
9 Faça login no ISE e navegue até Administração - Implantação. Clique no nó com pxgrid personna - clique em Nuvem de integração em Conexão Pxgrid.

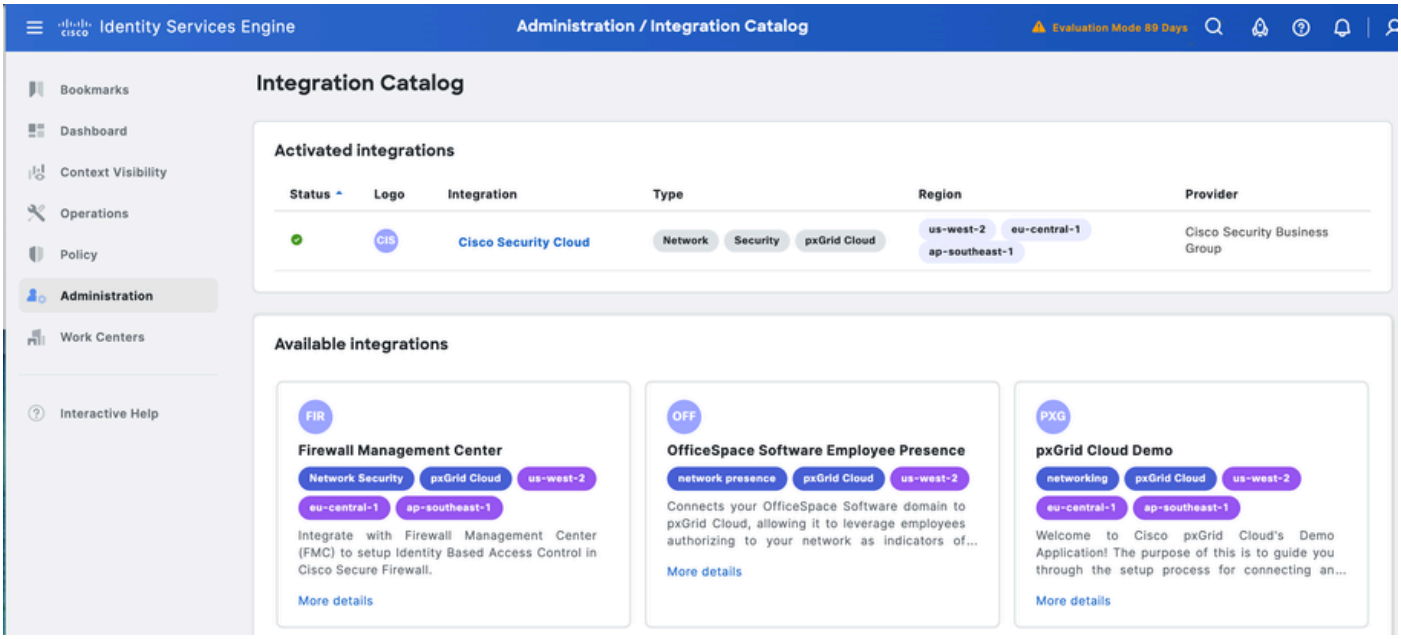
Em Configuração do aplicativo - selecione a instância do ISE criada no Security Cloud Control e

clique em Ativar



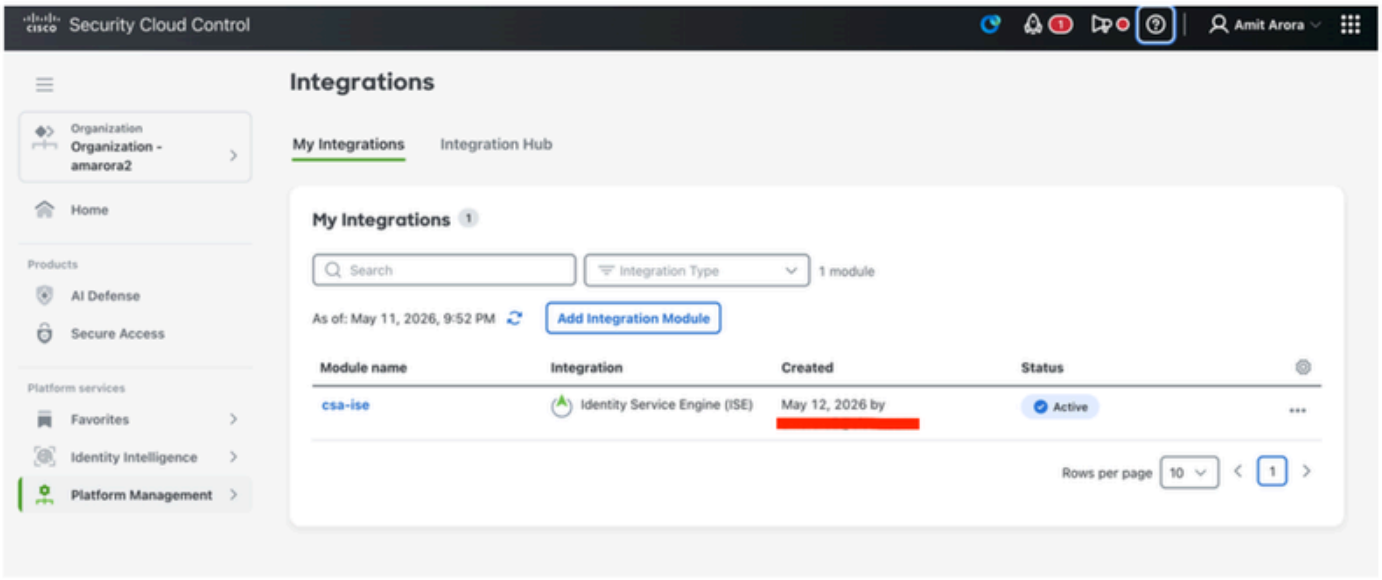
10 Application Status agora está conectado.





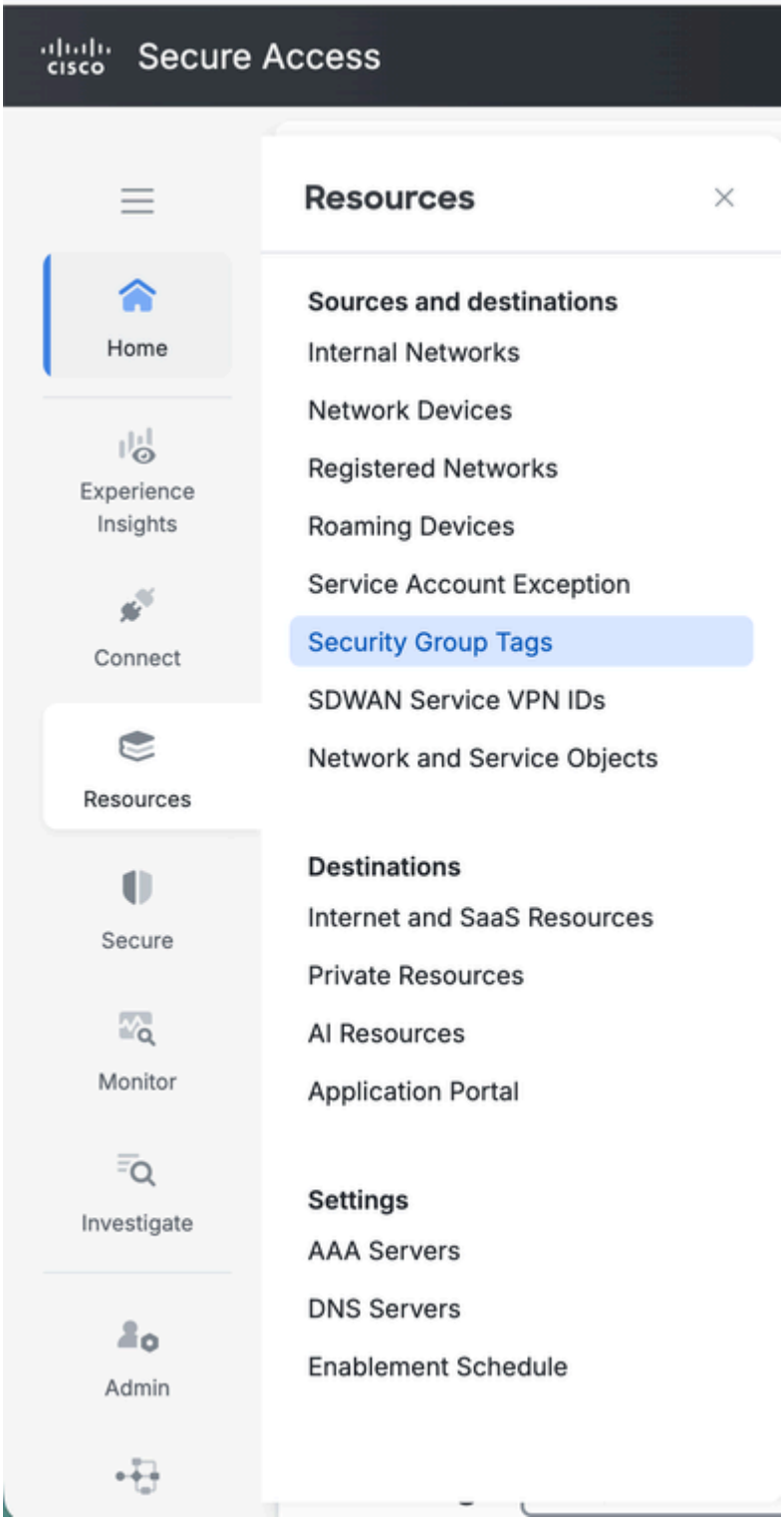
11 Login no controle de segurança em nuvem - security.cisco.com

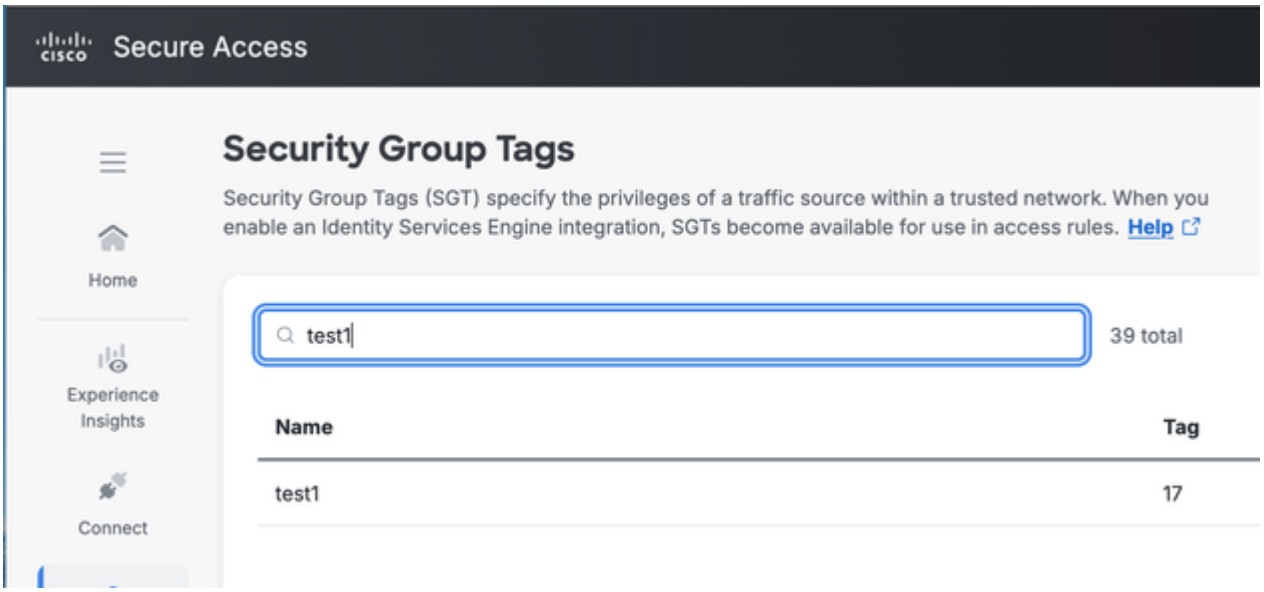
Em Gerenciamento de plataforma - Integrações de plataforma, podemos ver o Status de integração como Ativo



Verificar Marca do Grupo de Segurança:

Faça login no Cisco Secure Access. Navegue até Recursos - Tags de grupos de segurança.


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



Informações necessárias para o Cisco TAC

ISE:
Como coletar o pacote de suporte do ISE com os seguintes componentes definidos para o nível de depuração no nó do ISE com Pxgrid Personna :

pxgrid

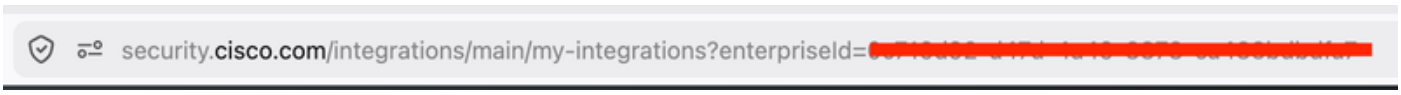
Infraestrutura

ERS

componente hermes no nível de depuração.

SCC:

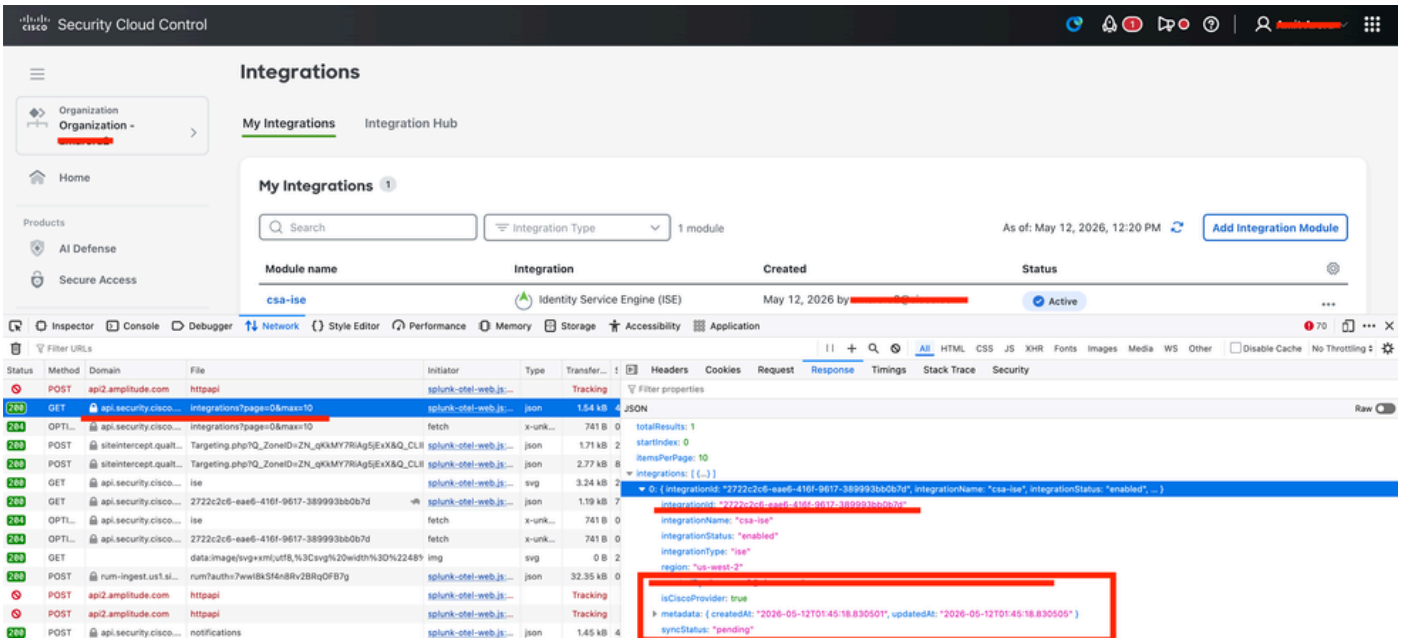
ID da empresa: no URL de security.cisco.com



ID de integração.
Iniciar captura HAR

Faça login em Security.cisco.com
Navegue até Gerenciamento de plataforma - Integrações de plataforma

Procure integrações?chamada de api de página e, na guia de resposta, você encontrará uma ID de integração.



Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.