Integración de Cisco Secure Access con ISE para Security Group Tag en Pxgrid Cloud

Contenido

Introducción

Este documento describe cómo habilitar el uso compartido de contexto entre Cisco Secure Access y Cisco Identity Services Engine

Requirements

Cisco recomienda que conozca estos temas:

- Cisco Secure Access: una solución de extremo de servicios de seguridad (SSE) basada en la nube que proporciona acceso a la red sin confianza para permitir a los usuarios conectarse fácilmente a Internet y a las aplicaciones privadas desde cualquier dispositivo.
- Parche 5 de Cisco Identity Service Engine (ISE) versión 3.4.
- Cisco Security Cloud Control: una solución de gestión unificada para sus productos e identidad de la nube de seguridad. El control de seguridad en la nube se incluye con el acceso seguro.

Background

Esta integración permite la creación automatizada de túneles fiables desde sucursales Catalyst SD-WAN hasta Cisco Secure Access, lo que facilita el intercambio fluido de ID/nombre VPN y contexto SGT.

Cisco Identity Services Engine (ISE) sigue siendo la autoridad central para la configuración y gestión de SGT. Cualquier actualización realizada en ISE se sincroniza automáticamente con Cisco Secure Access. Si se elimina una SGT, las reglas existentes que hacen referencia a ella permanecen activas para garantizar que la coincidencia del tráfico continúa según lo esperado.

Actualmente ofrecemos una disponibilidad limitada para las asignaciones de SGT, lo que amplía la compatibilidad para incluir los objetos de destino de SGT en sus reglas de seguridad. Además, próximamente se ofrecerá asistencia para crear túneles SASE que transporten SGT de Meraki y

Cisco Secure Firewall

caso de uso:

Política basada en el espacio de nombres de SGT:

Como administrador de seguridad, Kit desea aplicar una microsegmentación contigua mediante SGT desde ISE en las instalaciones para el tráfico privado de SSE, así como tráfico enlazado a Internet. Capacidad para importar SGT para aplicar políticas.

Componentes Utilizados

La información de este documento se basa en:

- Parche 5 de Identity Service Engine (ISE) versión 3.4
- Acceso seguro
- Cisco Security Cloud

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Descripción general de la configuración de contexto compartido

- Conexión de ISE a Cisco Security Cloud
- Conexión de Cisco Secure Access a ISE

Configurar

Esta guía desglosa la configuración general en los siguientes pasos principales:

1. Conexión de Cisco ISE a Cisco Security Cloud
2. Conecte Cisco Secure access a Cisco ISE
3. Security Group Tags en Cisco Secure Access

Antes de comenzar

- Asegúrese de que ha instalado y activado la licencia Advantage en su implementación de Cisco ISE.
- El agente DNA Cloud crea una conexión HTTPS saliente con Cisco DNA Cloud. Por lo tanto, debe configurar los parámetros de proxy de Cisco ISE si la red utiliza un proxy para conectarse a Internet. Para configurar los parámetros de proxy en Cisco ISE, vaya a **Administration** > **System** > **Settings** > **Proxy**
- Asegúrese de que el puerto 443 esté abierto para la conexión saliente de Cisco ISE al portal Cisco pxGrid Cloud. Si se configuran los parámetros de firewall o proxy, asegúrese de que estas URL no están bloqueadas:

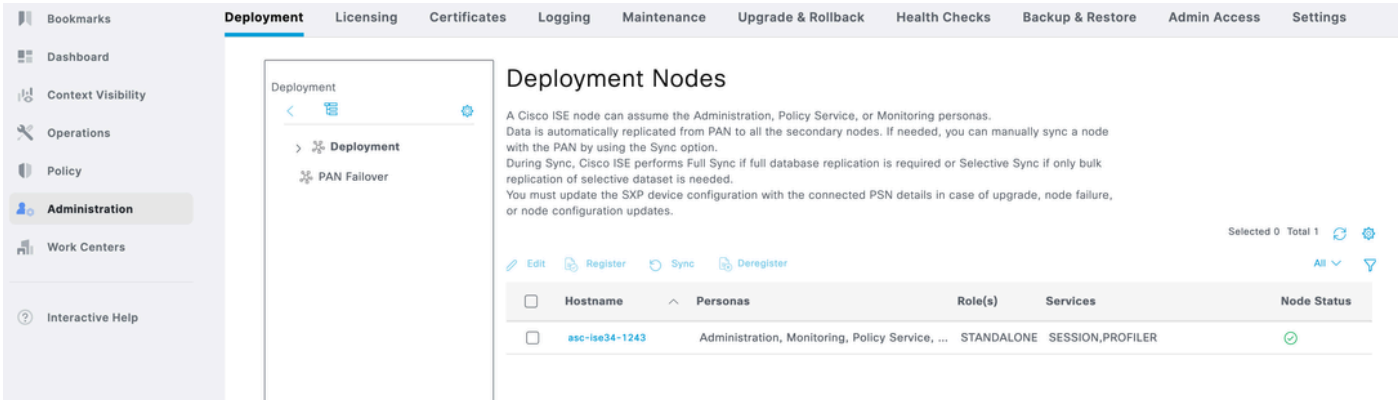
https://dna.cisco.com

https://security.cisco.com/

Paso 1:Habilitar Pxgrid Cloud en ISE

1 Vaya a la GUI de ISE.

2 Haga clic en Administration - Deployment (Administración - Implementación).

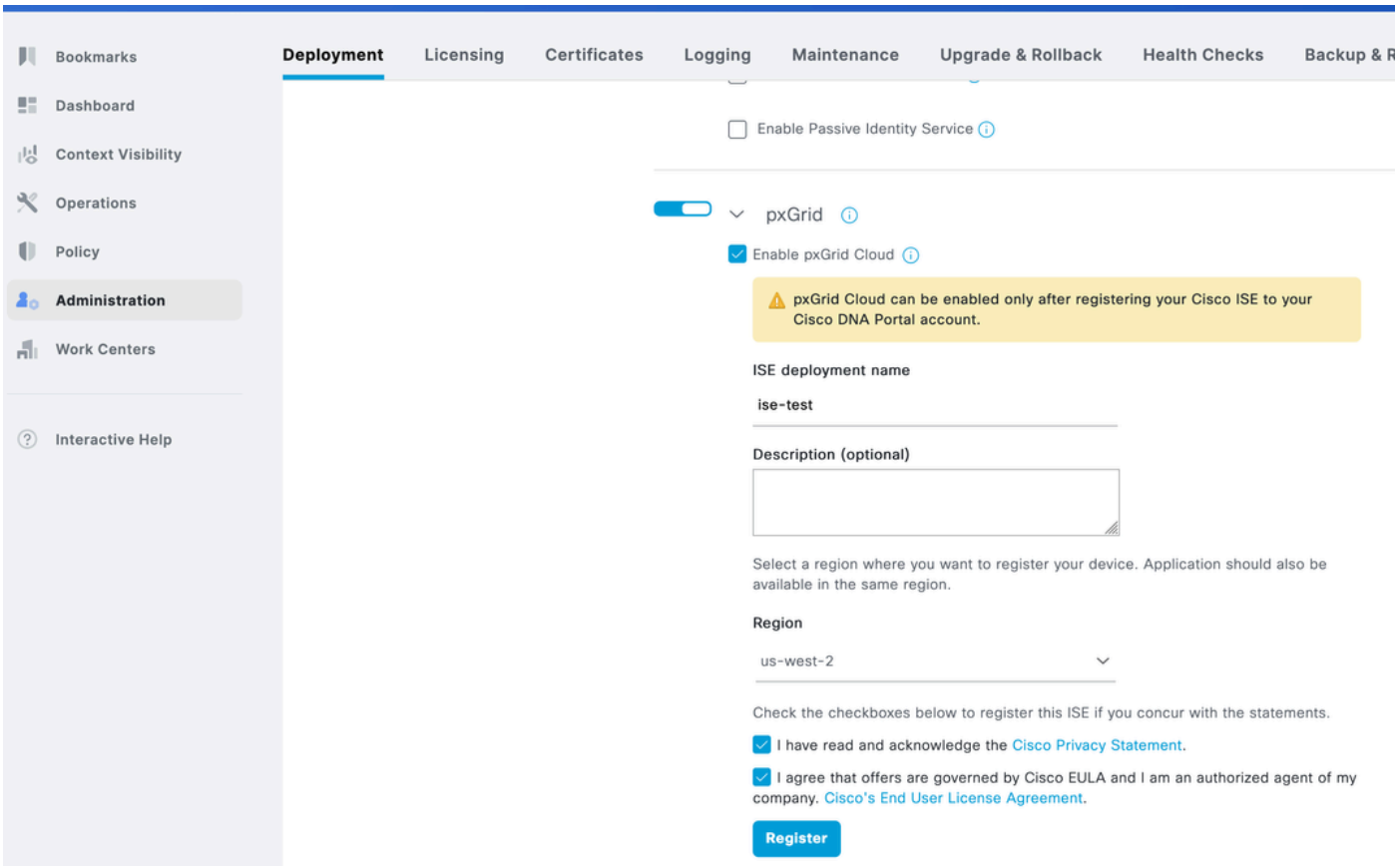


3 Haga clic en el nodo y desplácese hacia abajo.

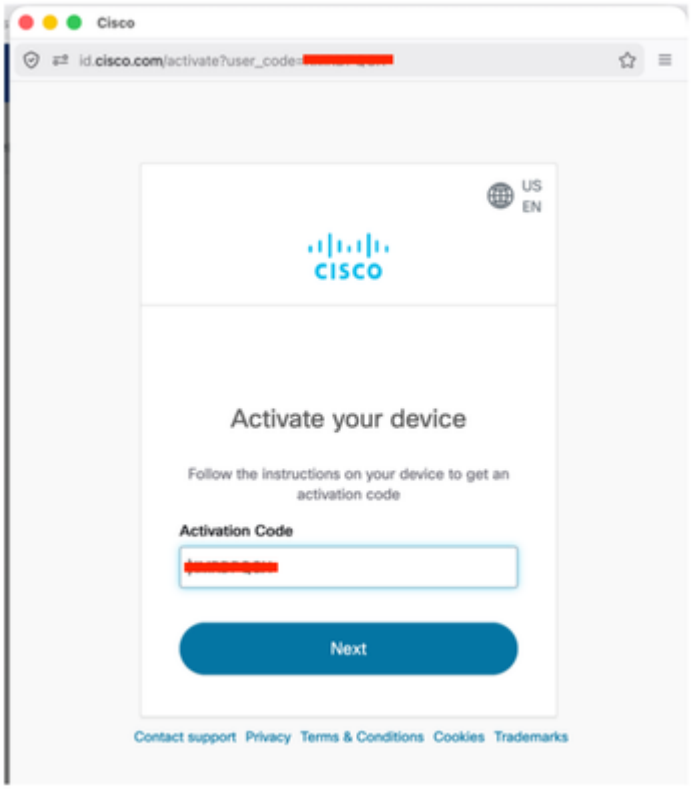
Introducir nombre de implementación de ISE

Seleccione la región como Oeste de EE.UU. 2, que es la única región admitida hasta el momento.

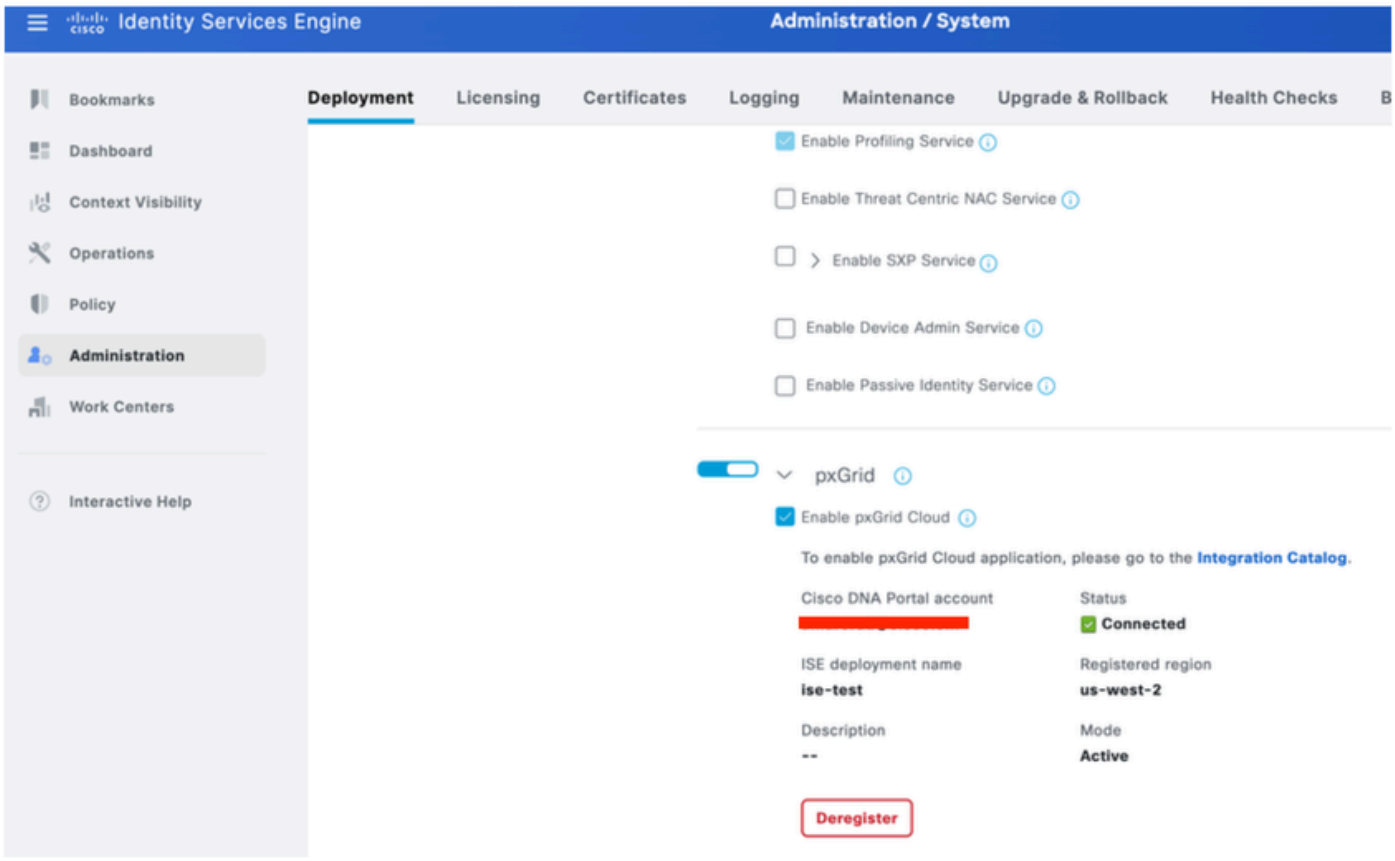
Marque ambas casillas de verificación y haga clic en Registrar.



4 Verá un elemento emergente con el código de activación rellenado automáticamente.Haga clic en Next (Siguiente),



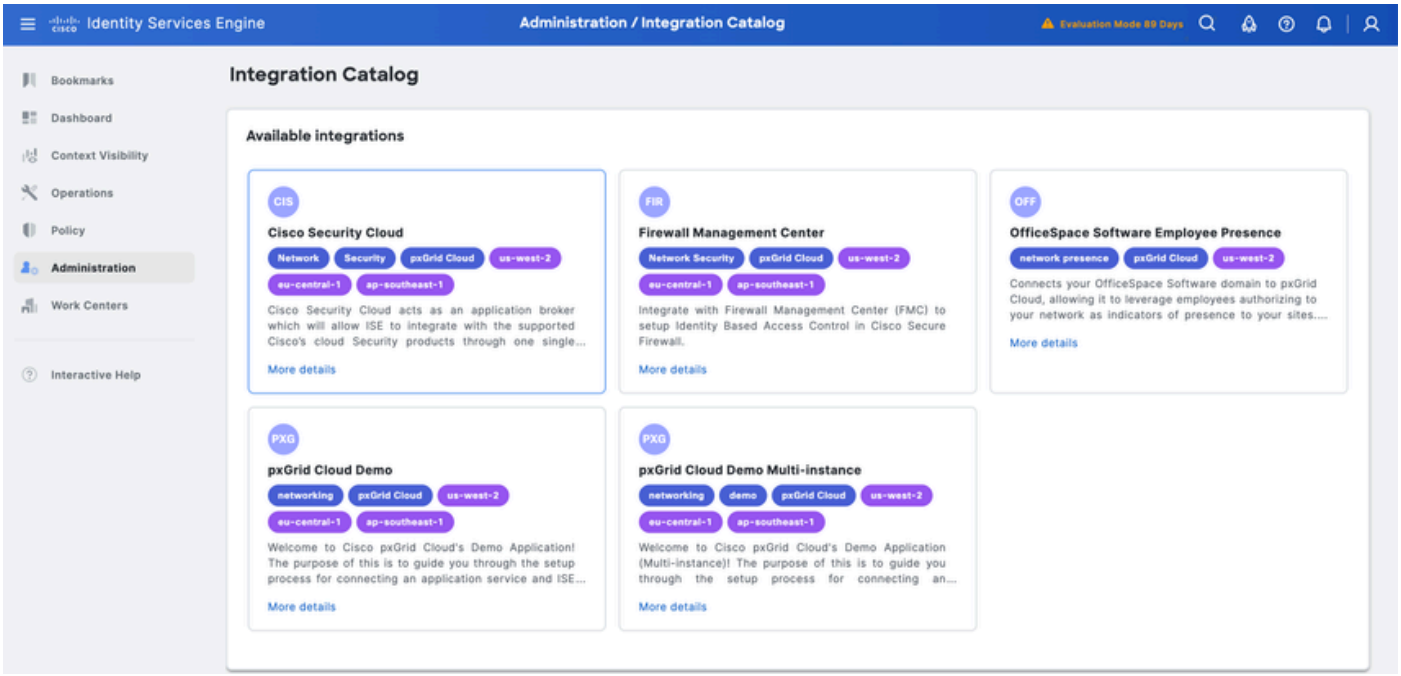
5 ISE mostrará Connected to Pxgrid Cloud.



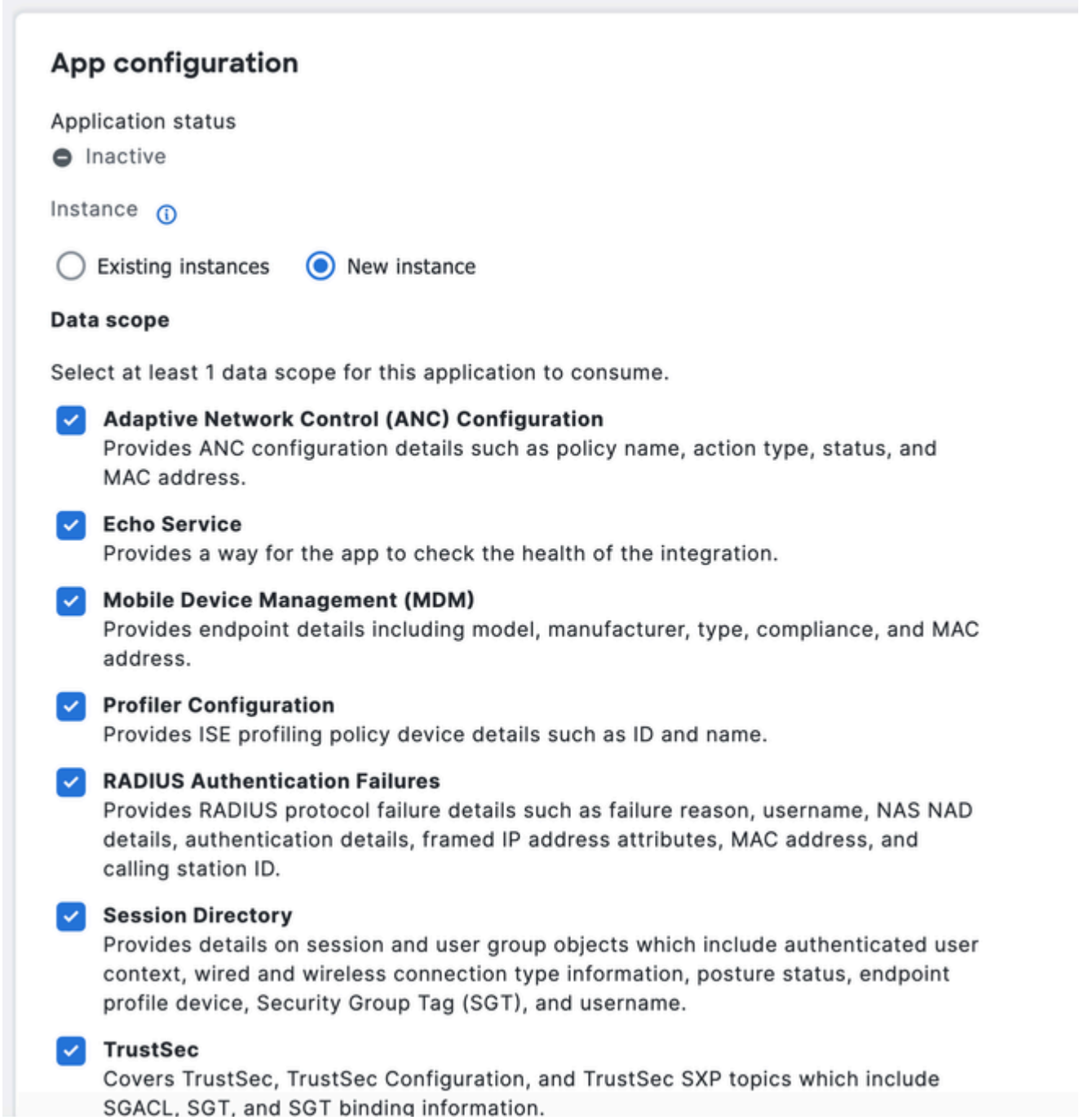
6 Haga clic en el enlace Integration Catalog (Catálogo de integración) del paso 5.

En Integraciones disponibles, haga clic en Cisco Security Cloud

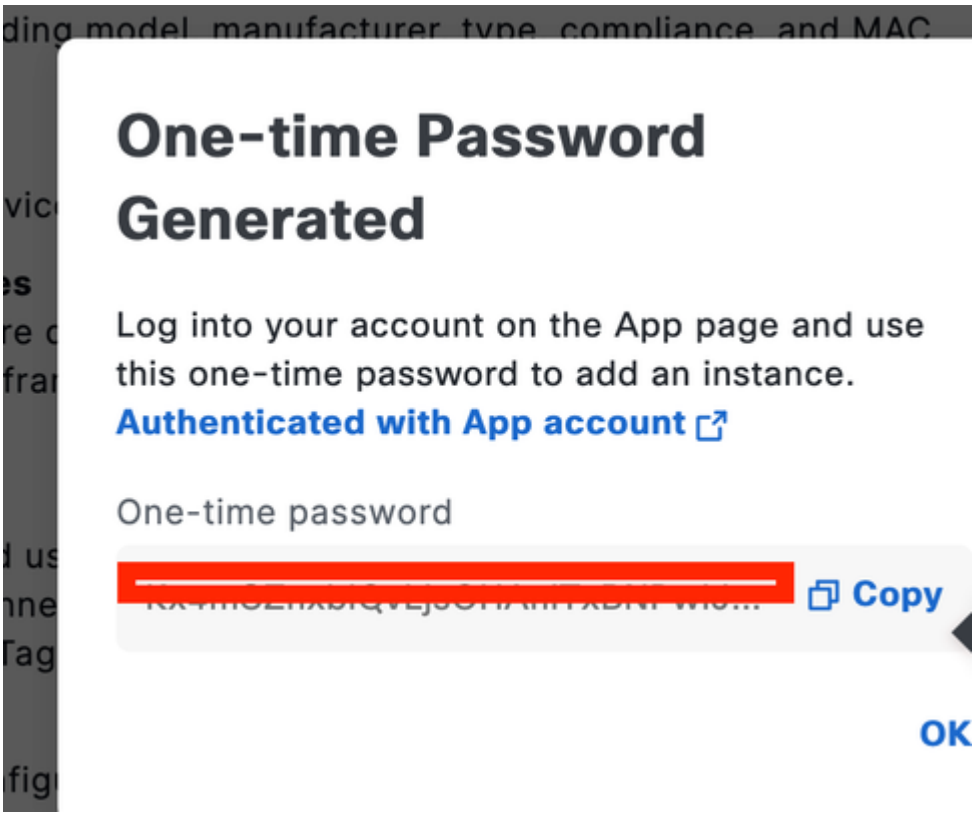
.



7 En Configuración de la aplicación, haga clic en Nueva instancia y en Activar

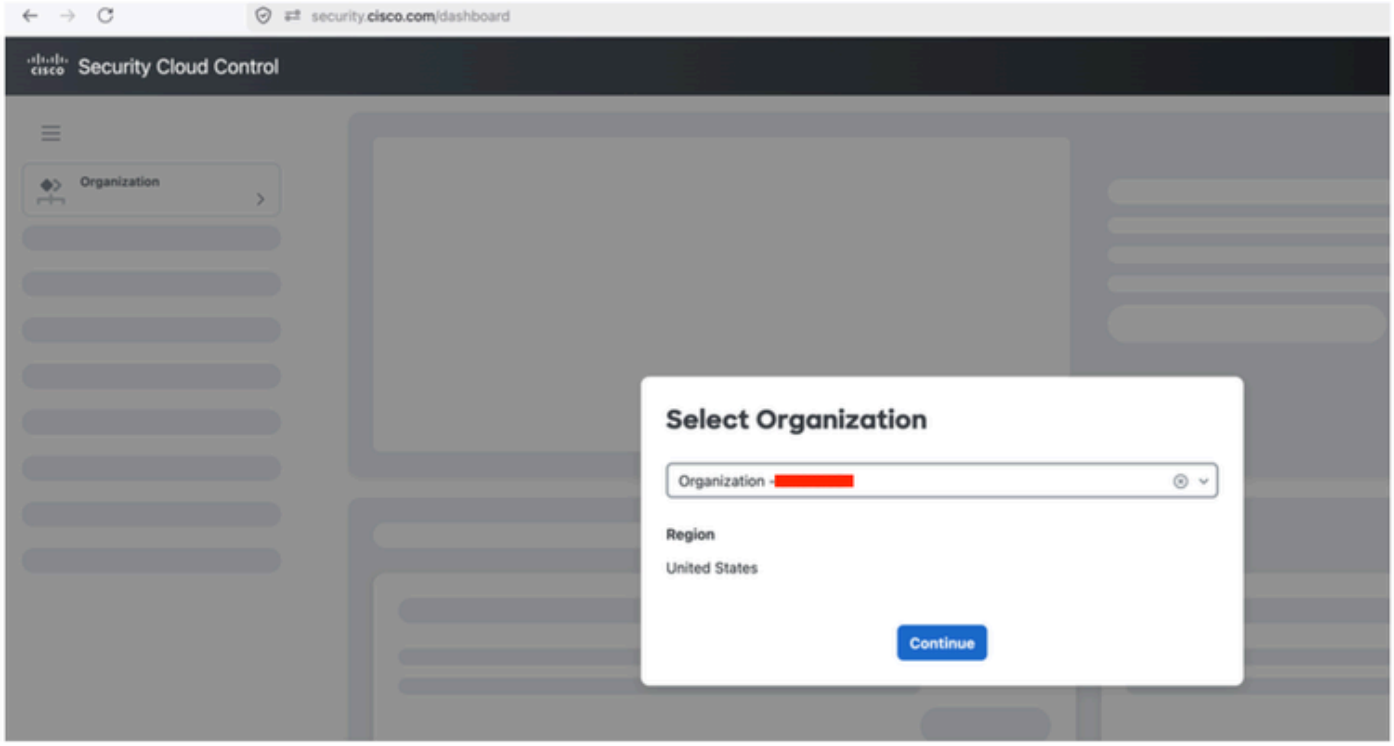


Copie la contraseña de un solo uso, ya que se utilizará en Cisco Secure Access.

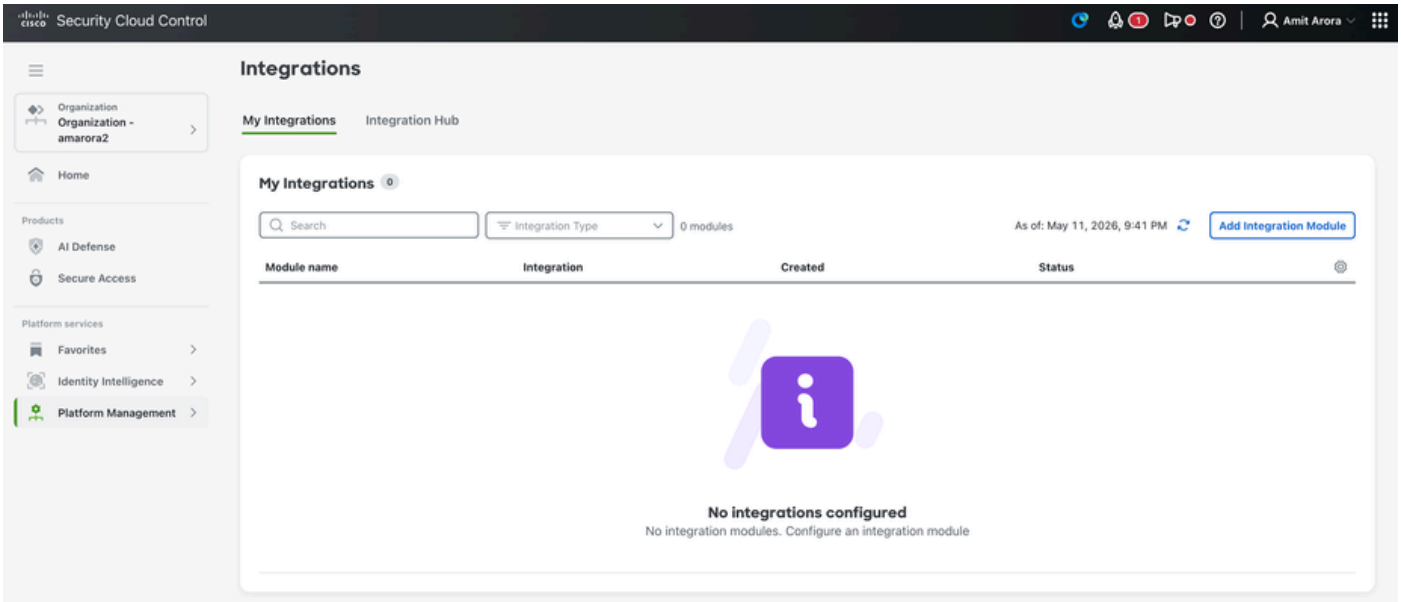


Paso 2: Integre Cisco Secure Access con ISE

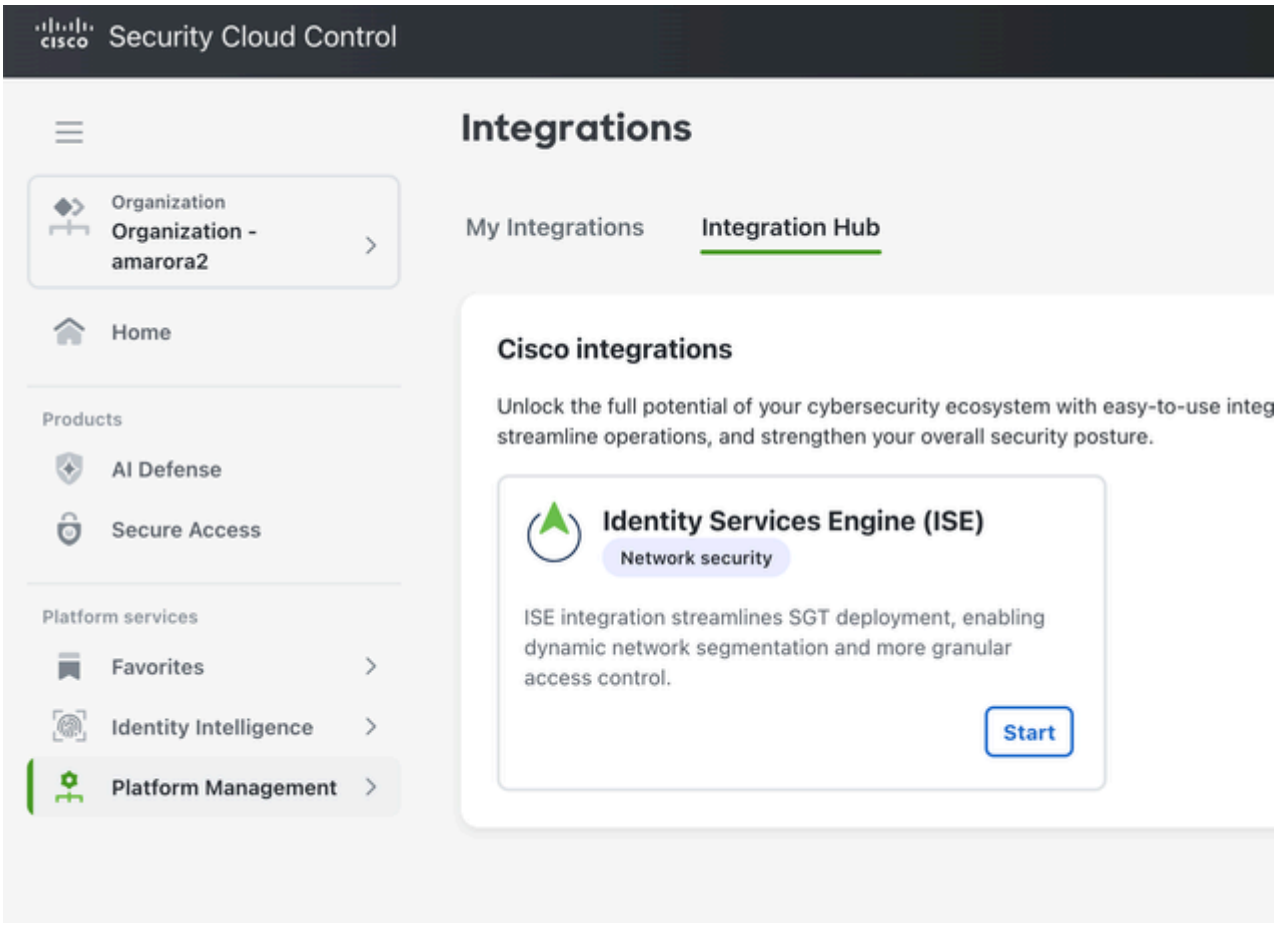
1. Inicie sesión en security.cisco.com.
2. Seleccione la organización Cisco Secure Access



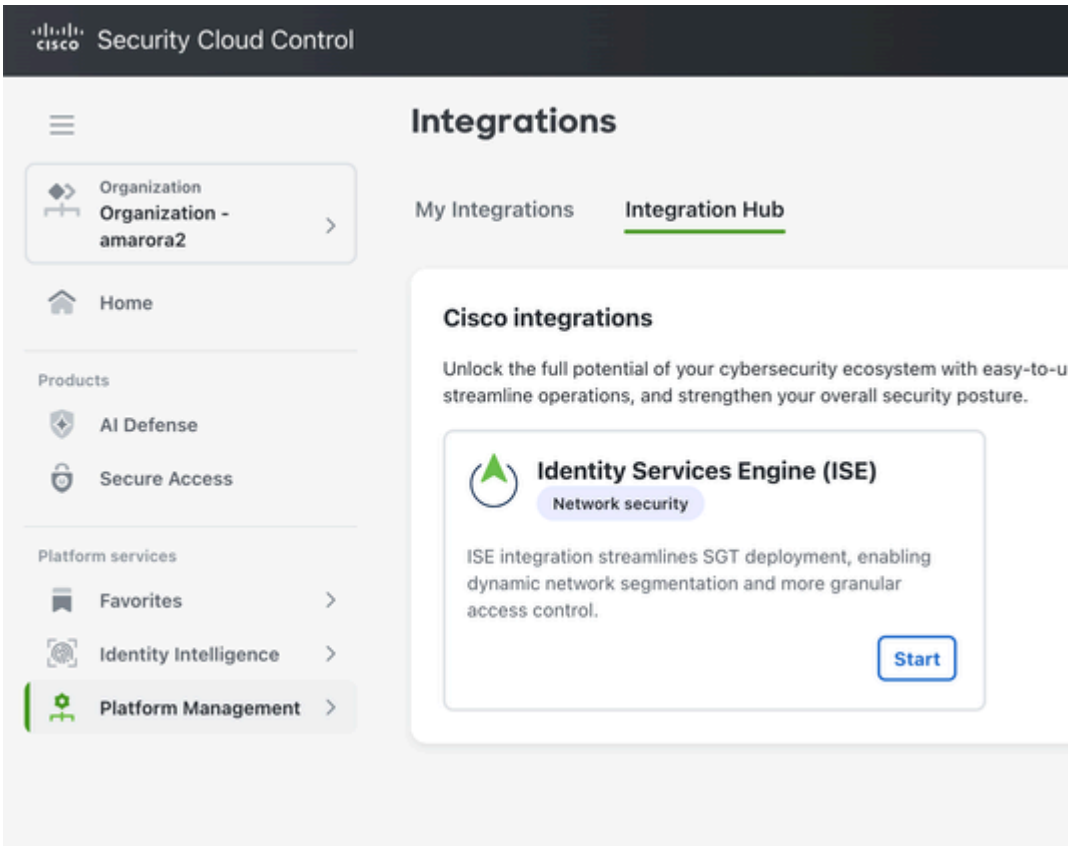
3 Haga clic en Platform Management - Platform Integrations



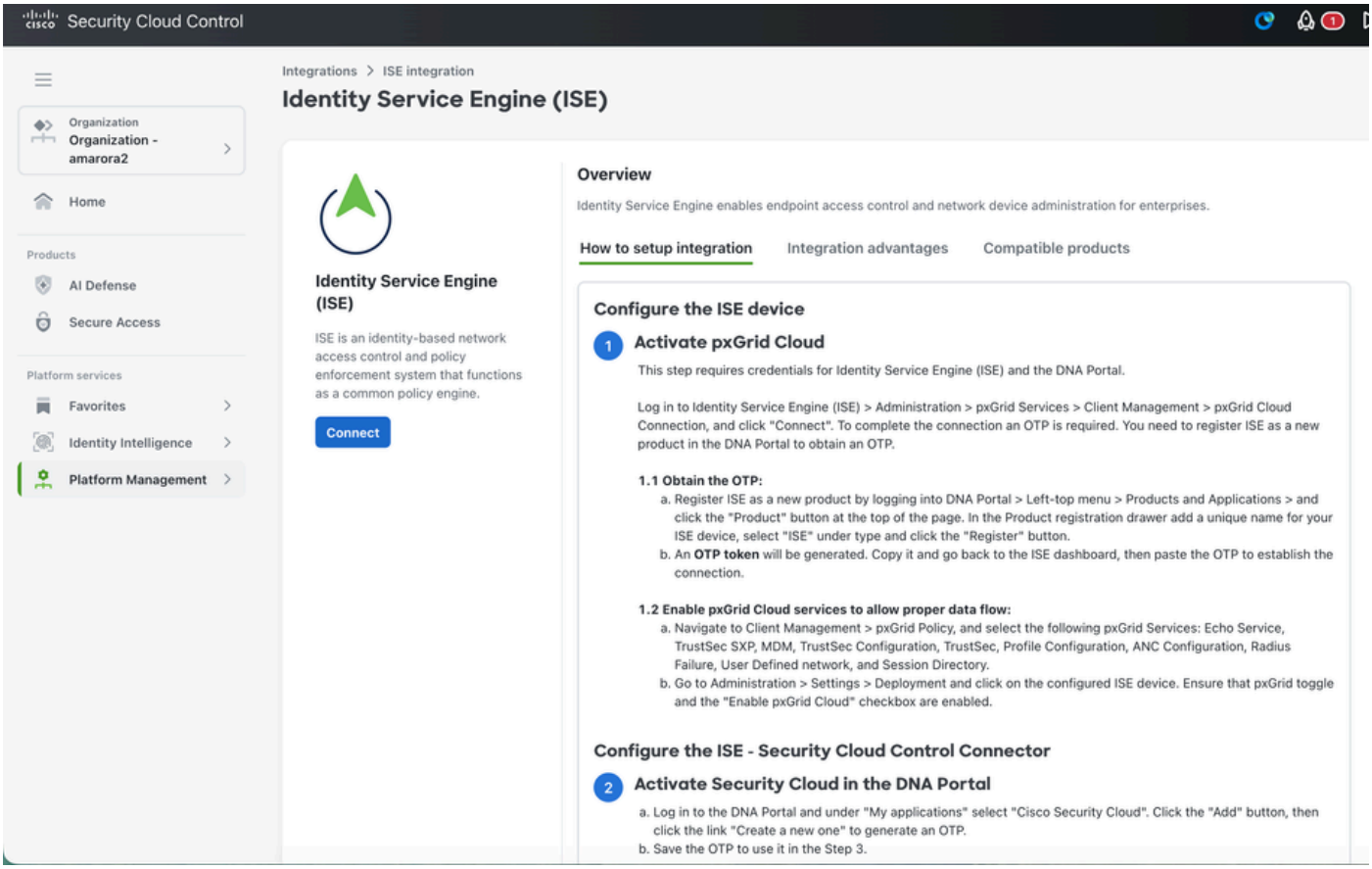
4 Haga clic en Agregar módulo de integración



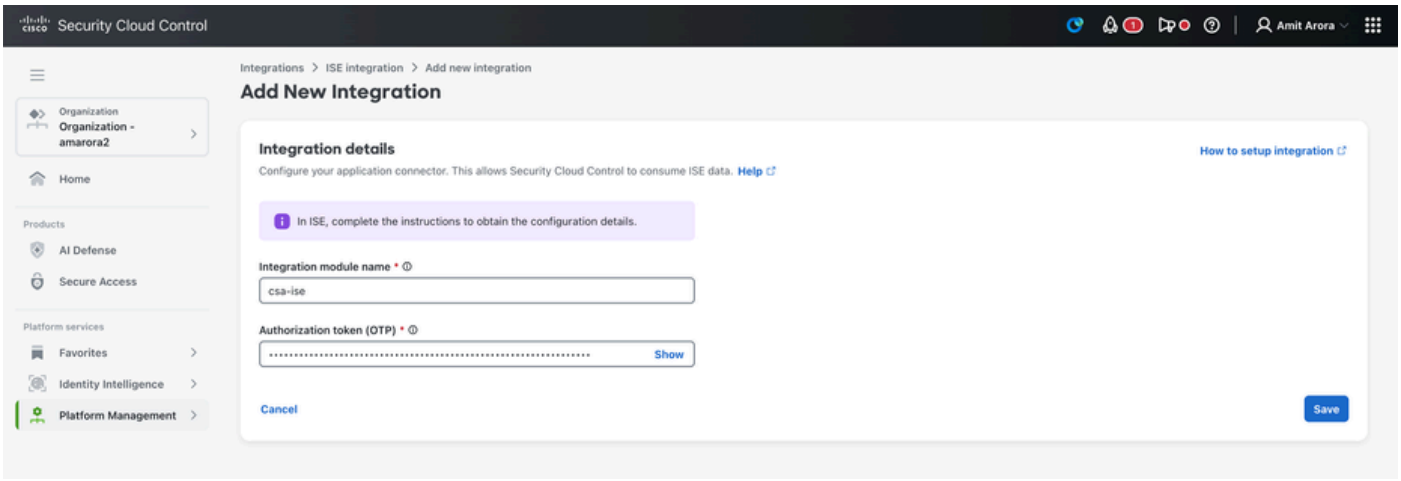
5 Haga clic en Inicio



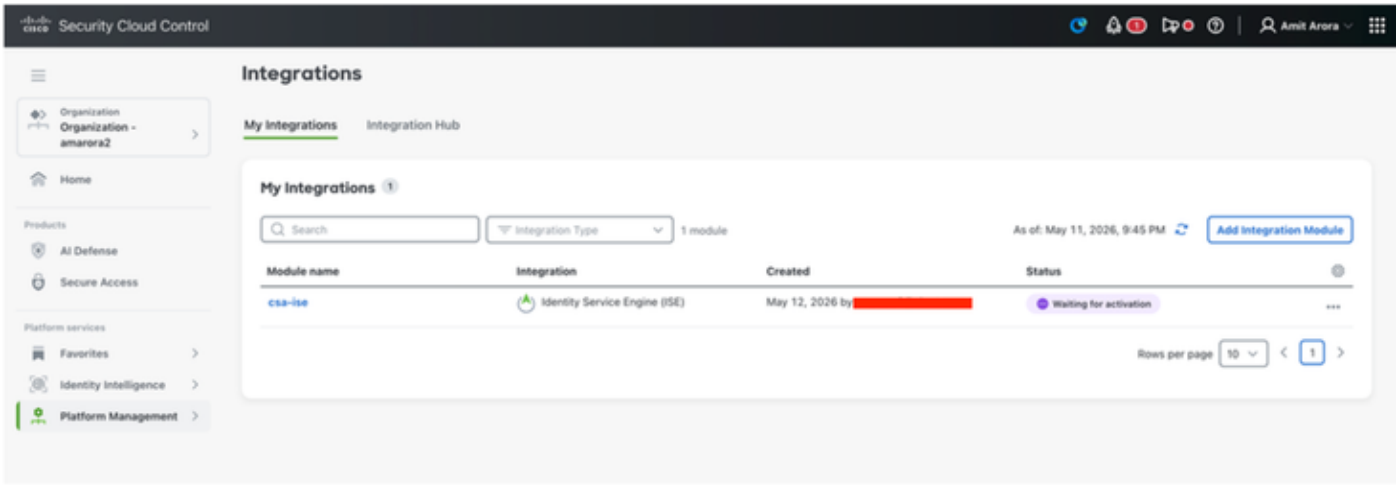
6 Haga clic en Conectar



7. Introduzca el nombre del módulo de integración y OTP desde Cisco ISE y haga clic en Guardar

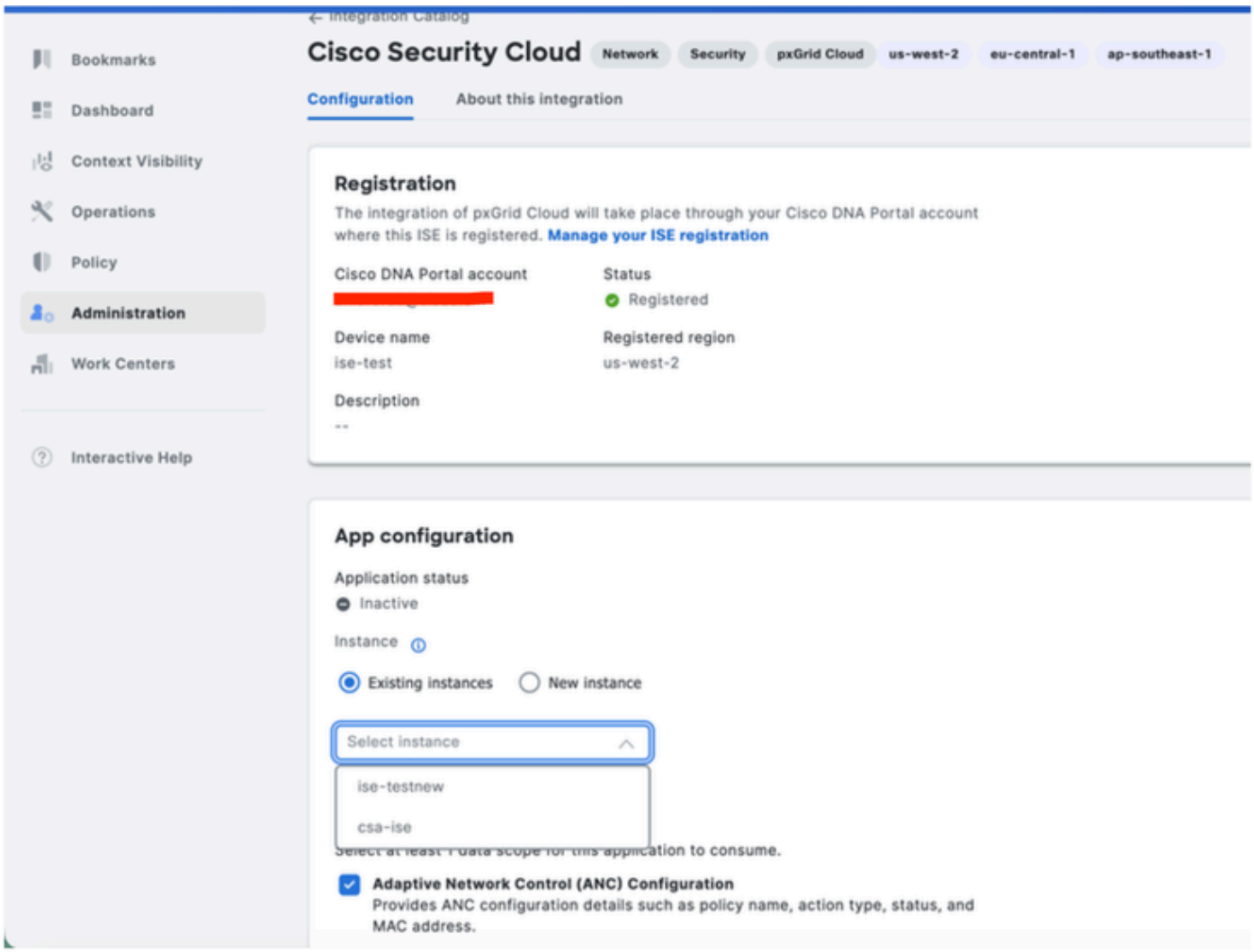


8 Una vez que haga clic en Save (Guardar), veremos Waiting for Activation Status (Esperando estado de activación).

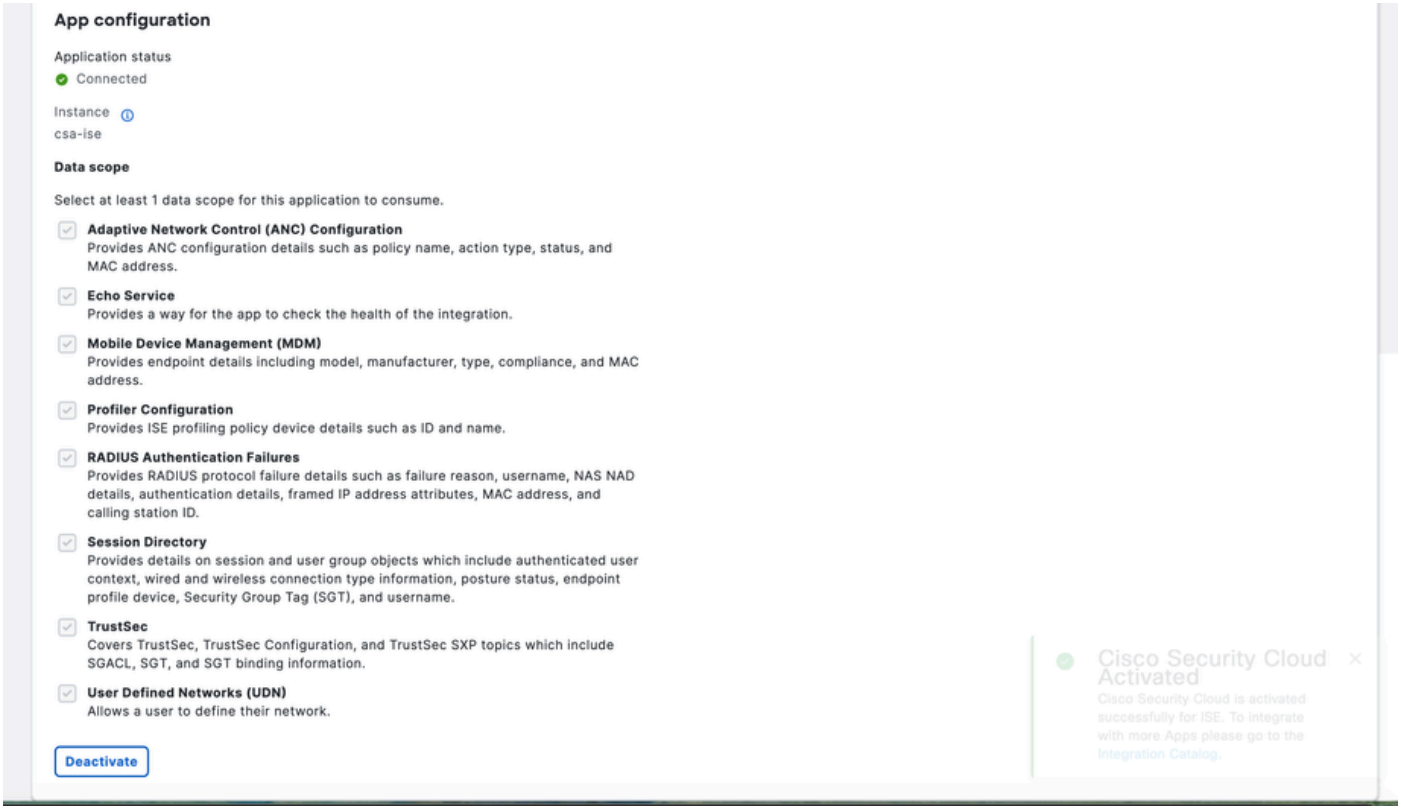


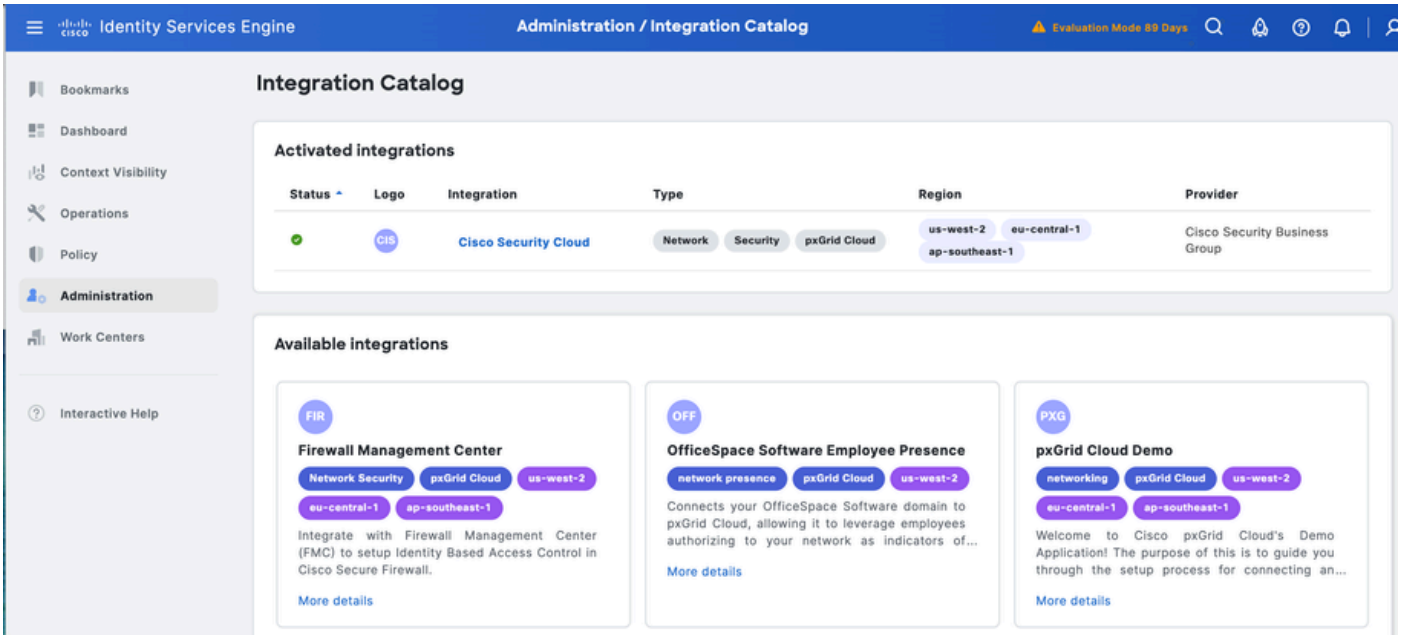
9 Inicie sesión en ISE y navegue hasta Administration (Administración) - Deployment (Implementación). Haga clic en el nodo con pxgrid personna - haga clic en Nube de integración en Conexión Pxgrid.

En Configuración de la aplicación, seleccione la instancia de ISE creada en Security Cloud Control y haga clic en Activar



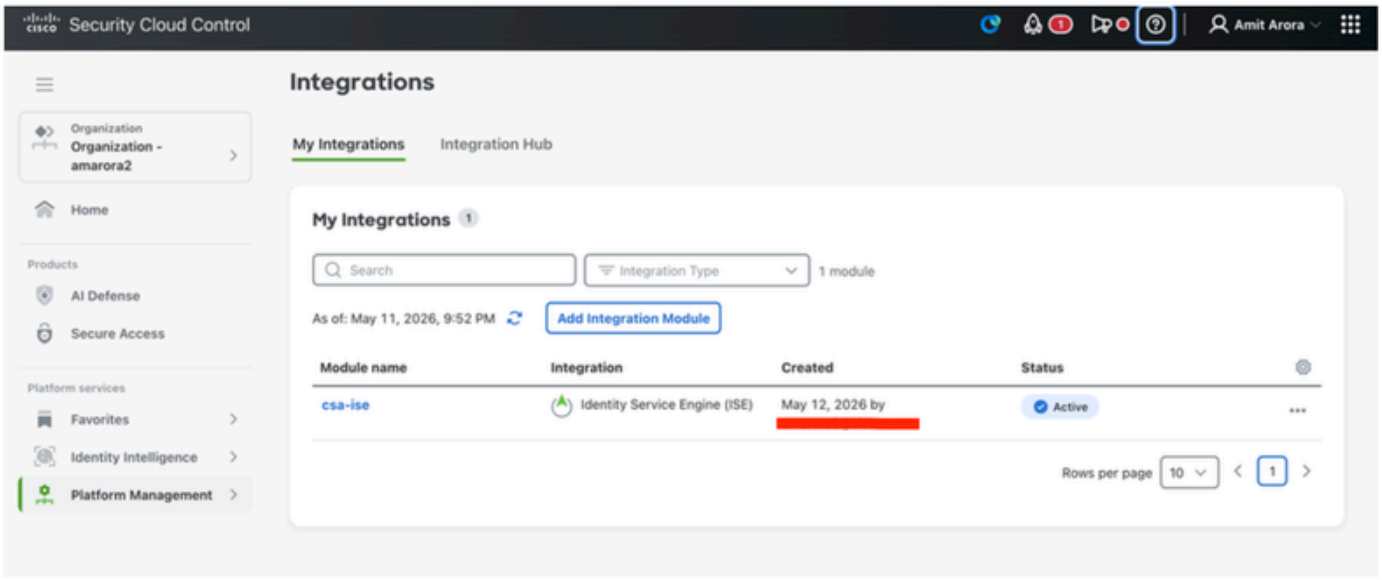
10 El estado de la aplicación está conectado.





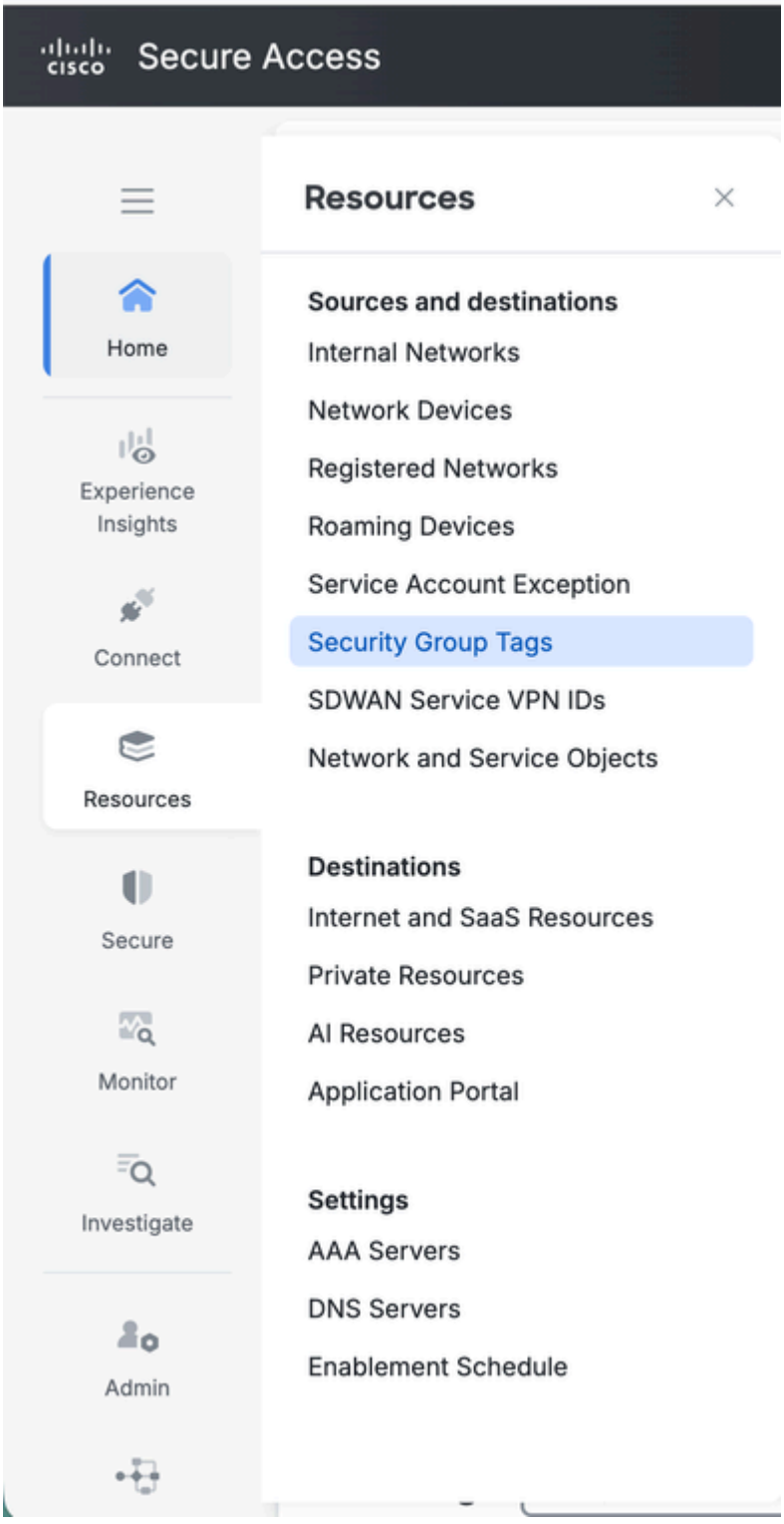
11 Inicie sesión en Security Cloud control: security.cisco.com

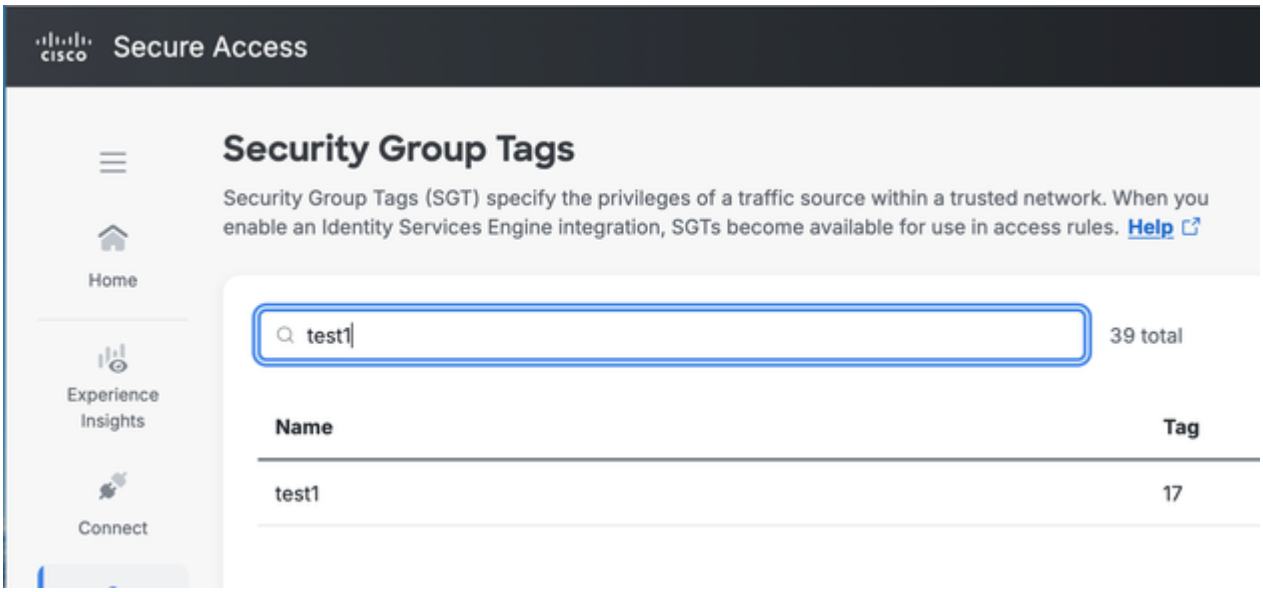
En Administración de la plataforma - Integraciones de la plataforma Podemos ver el estado de integración como Activo



Verificar etiqueta de grupo de seguridad:

Inicie sesión en Cisco Secure Access. Vaya a Recursos - Etiquetas de grupos de seguridad.


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



Información necesaria para Cisco TAC

ISE:
Cómo recopilar el paquete de soporte de ISE con los siguientes componentes configurados en Nivel de depuración en el nodo de ISE con Pxgrid Persona:

pxgrid

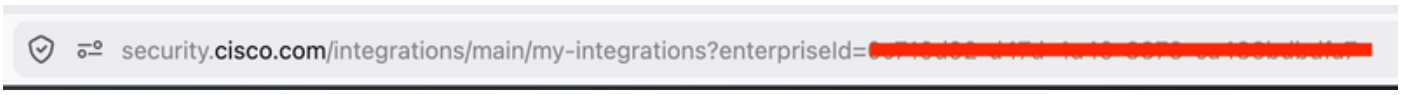
Infraestructura

ERS

componente hermes en el nivel de depuración.

SCC:

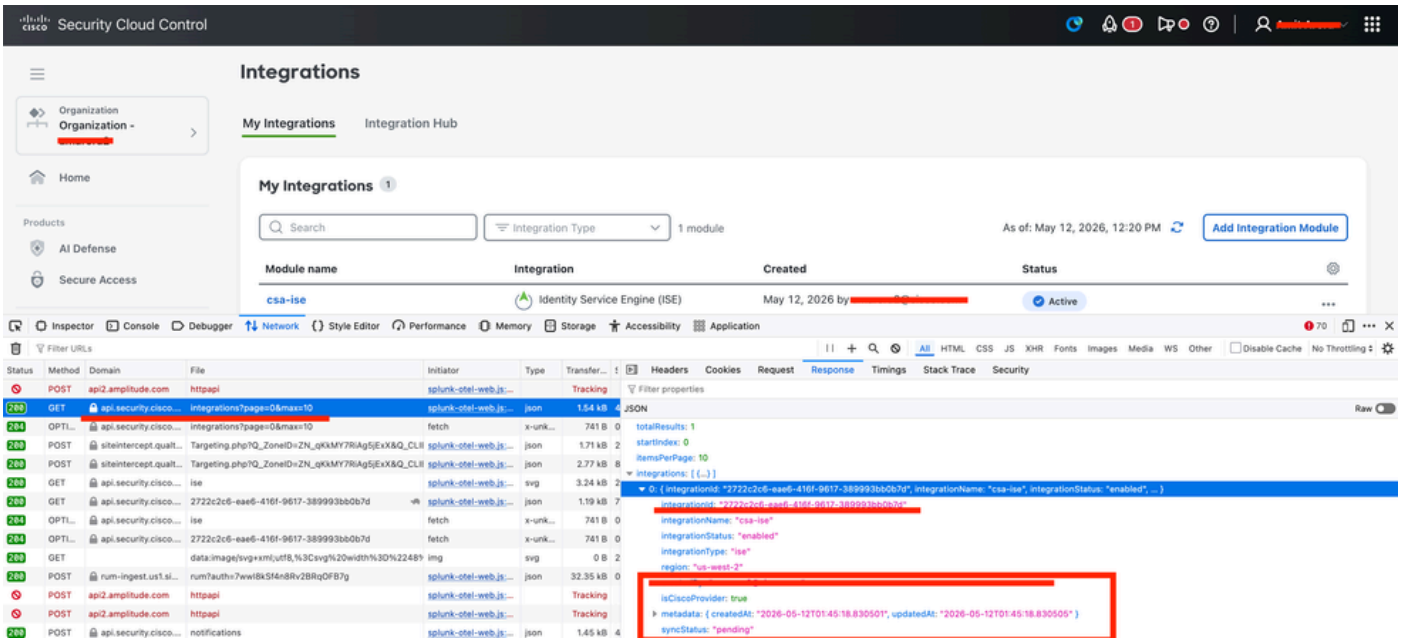
ID de empresa: en la URL de security.cisco.com



ID de integración.
Iniciar captura HAR

Inicie sesión en Security.cisco.com
Vaya a Platform Management - Platform Integrations

Busque la llamada a la API de la página de integraciones y, en la ficha de respuesta, encontrará una ID de integraciones.



Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).