

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:

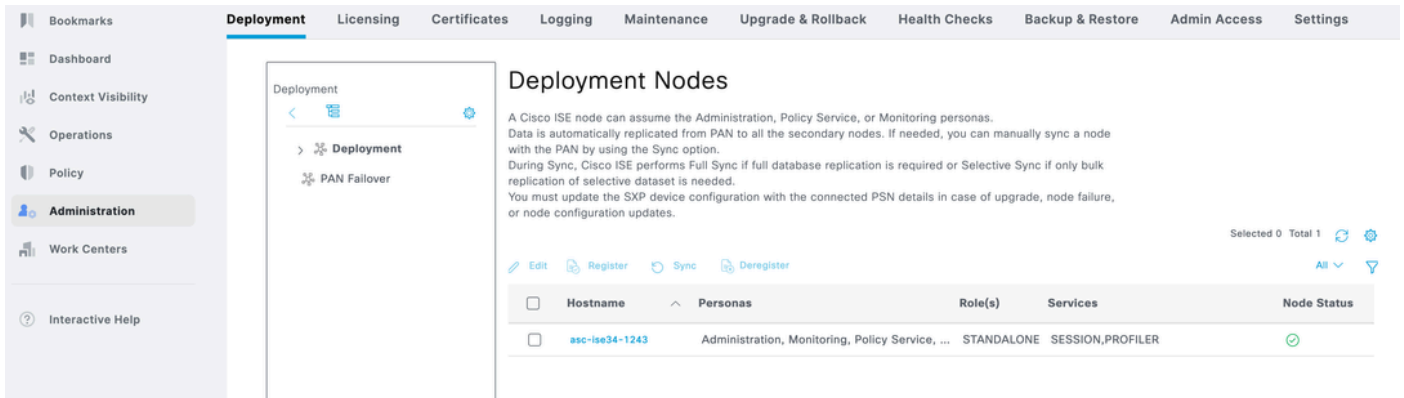
<https://dna.cisco.com>

<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).

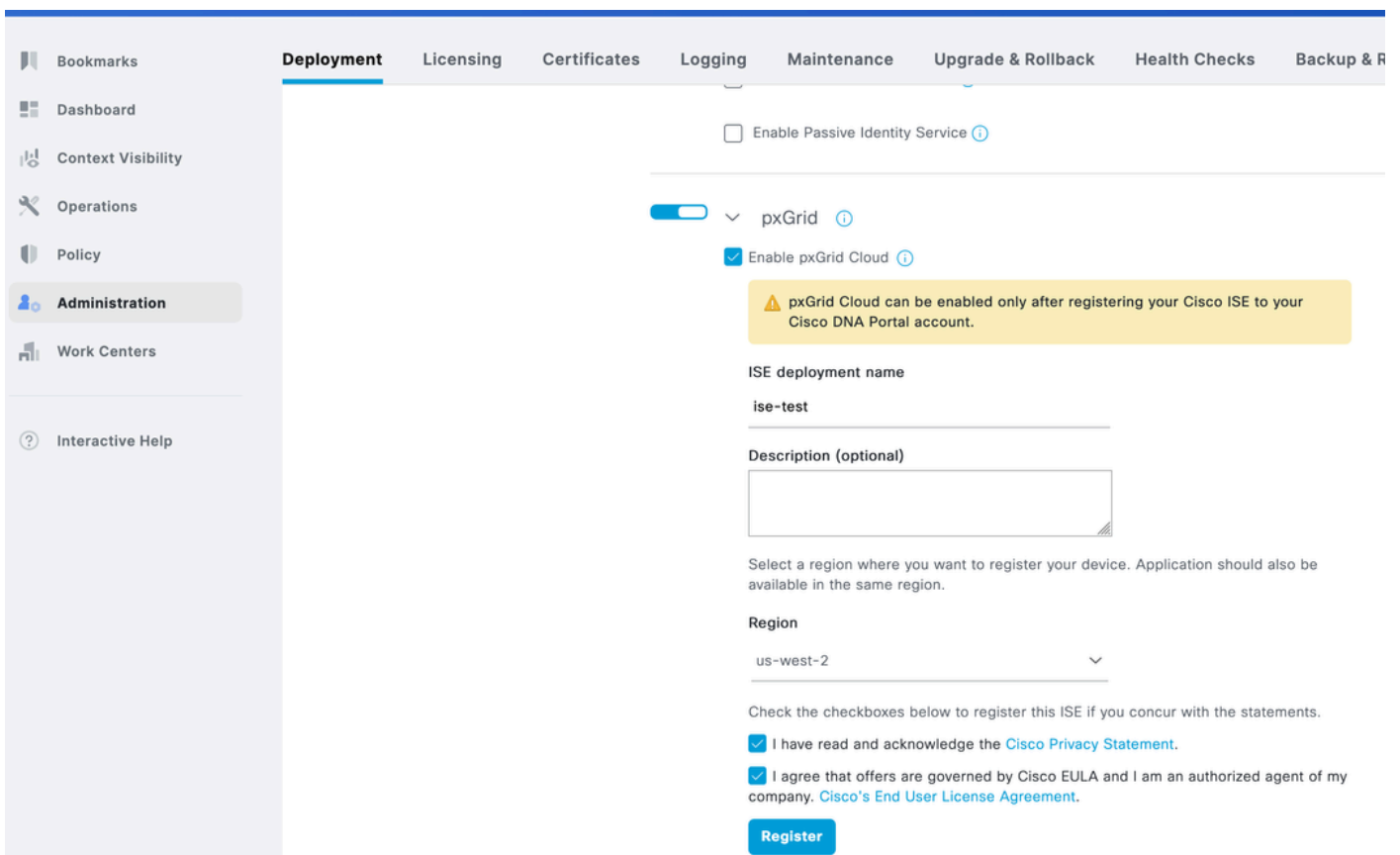


3 Haga clic en el nodo y desplácese hacia abajo.

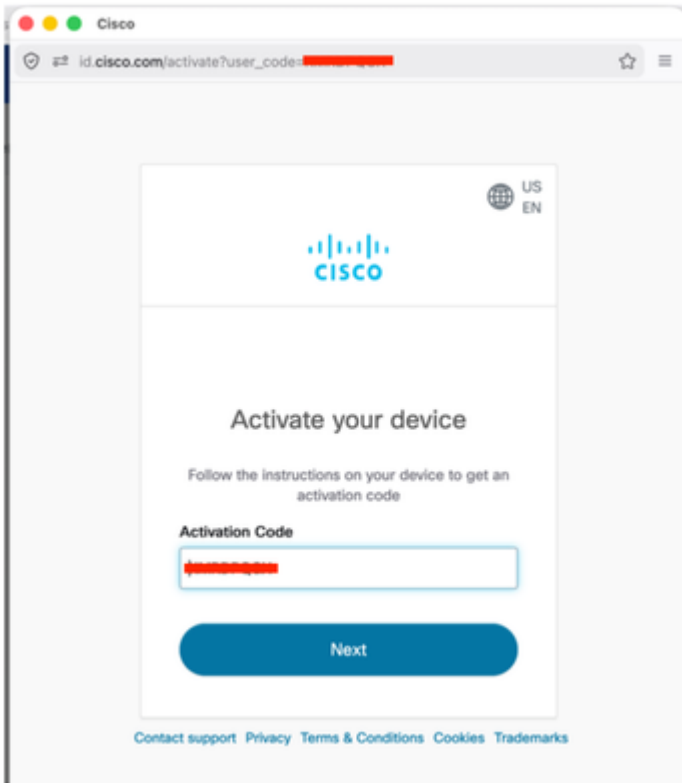
Introducir nombre de implementación de ISE

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

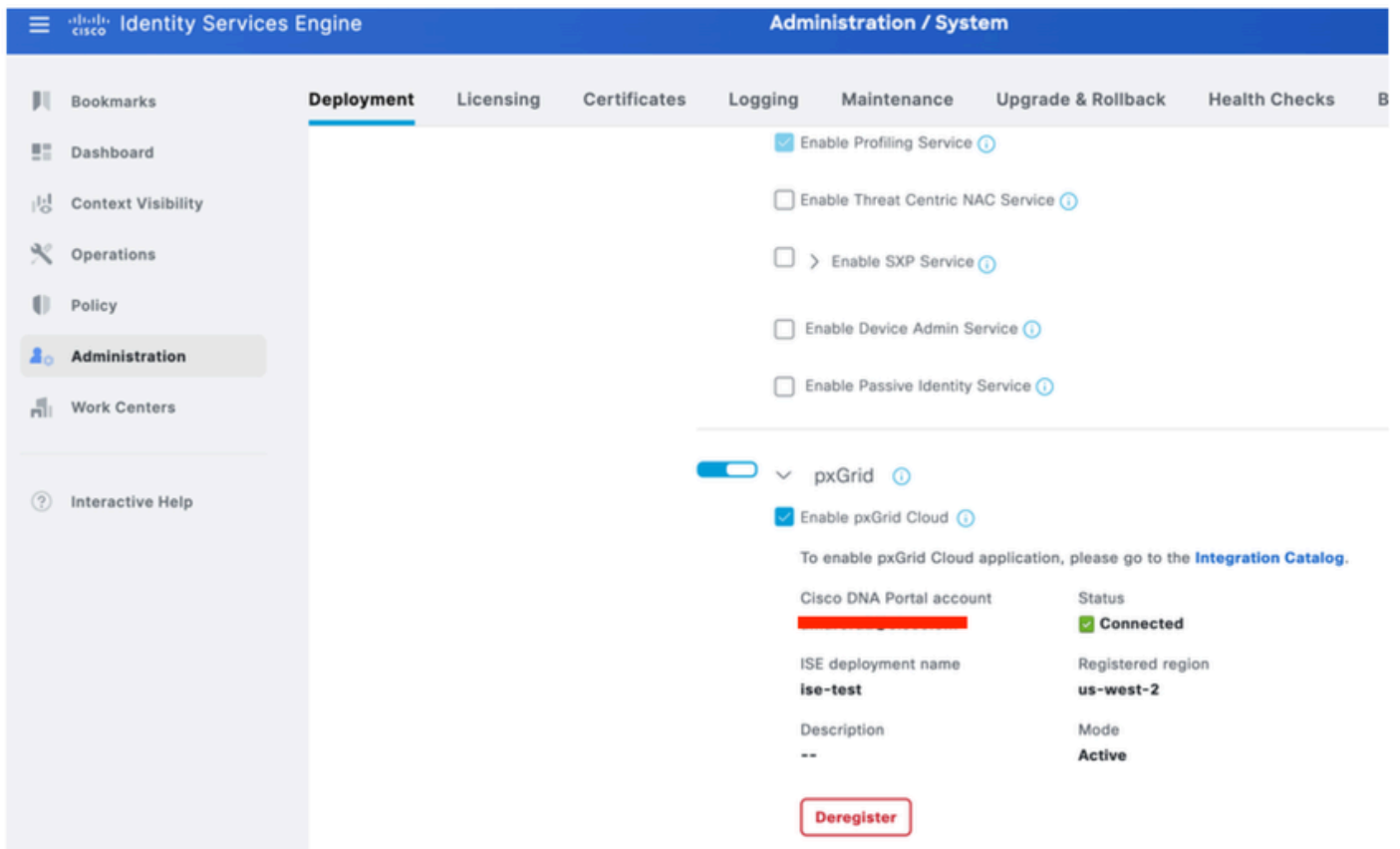
Marque ambas casillas de verificación y haga clic en Registrar.



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

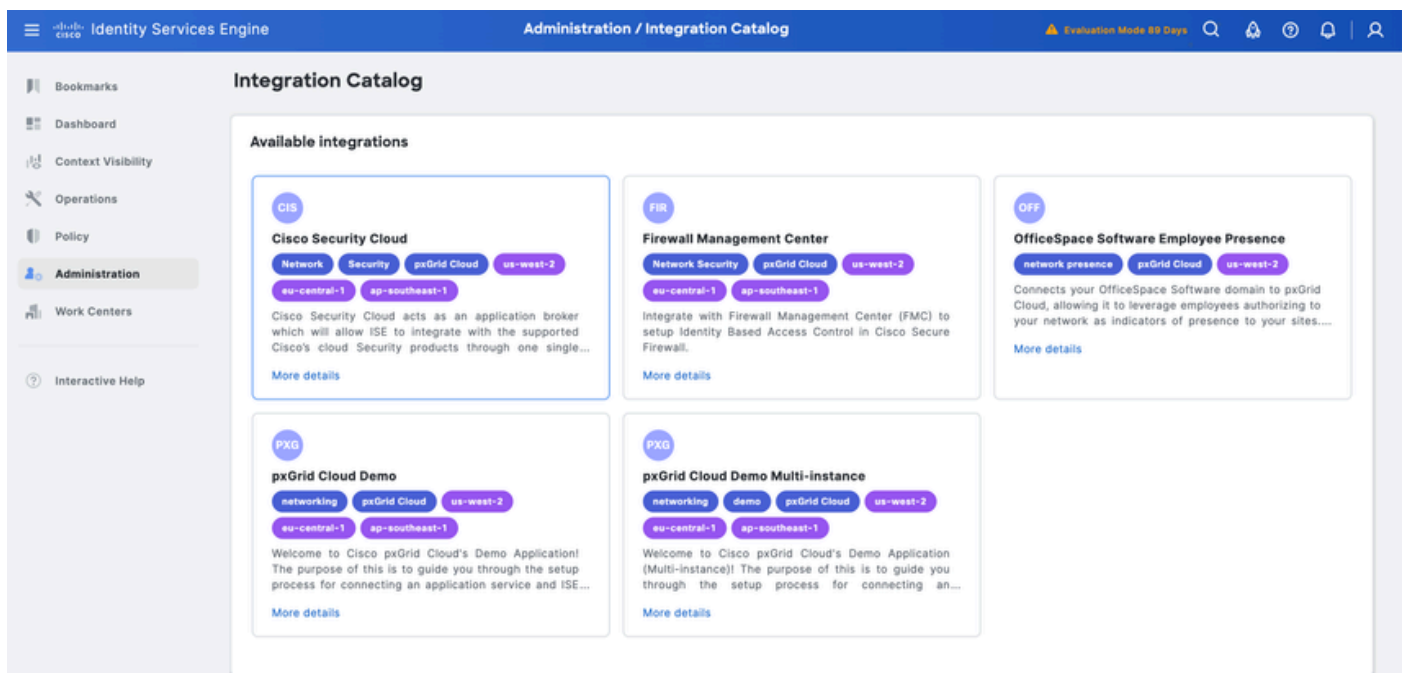


5 ISE mostrará Connected to Pxgrid Cloud.



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

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.

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

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](#) 

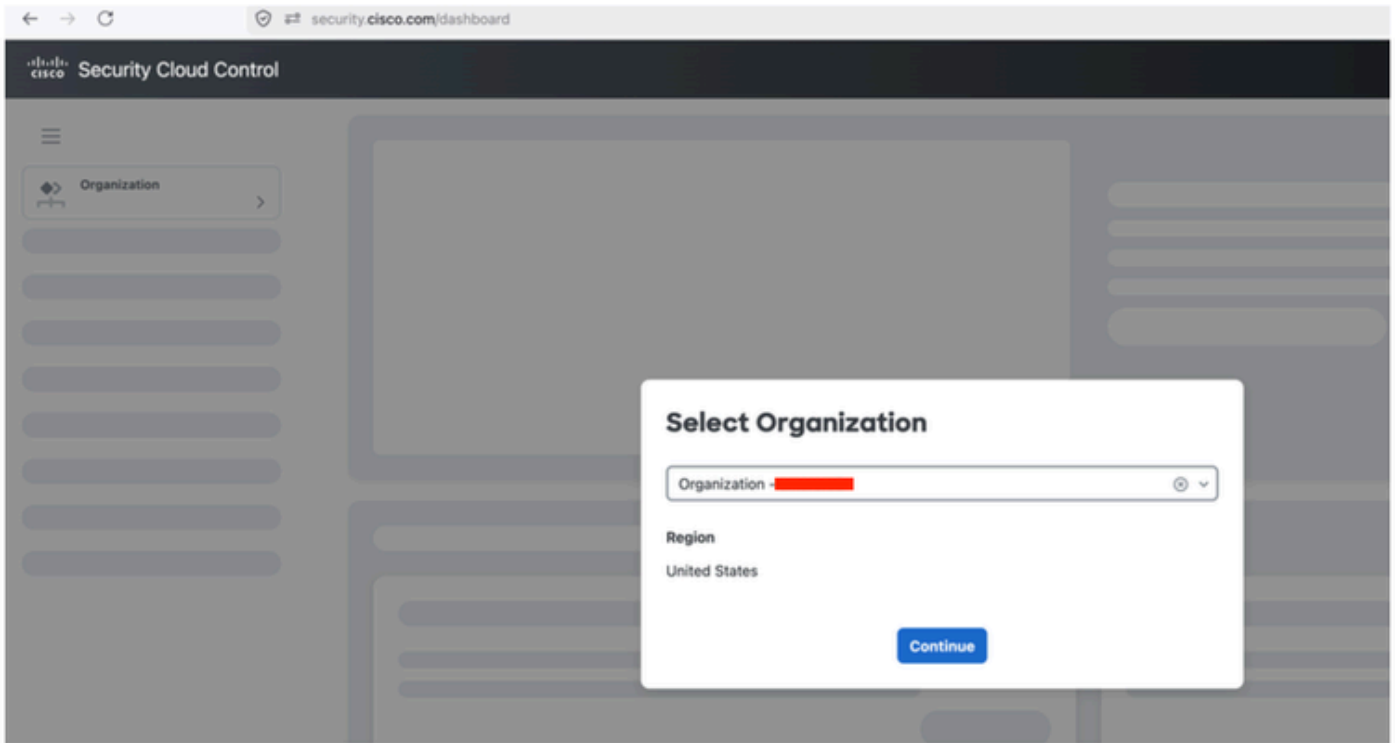
One-time password

  **Copy**

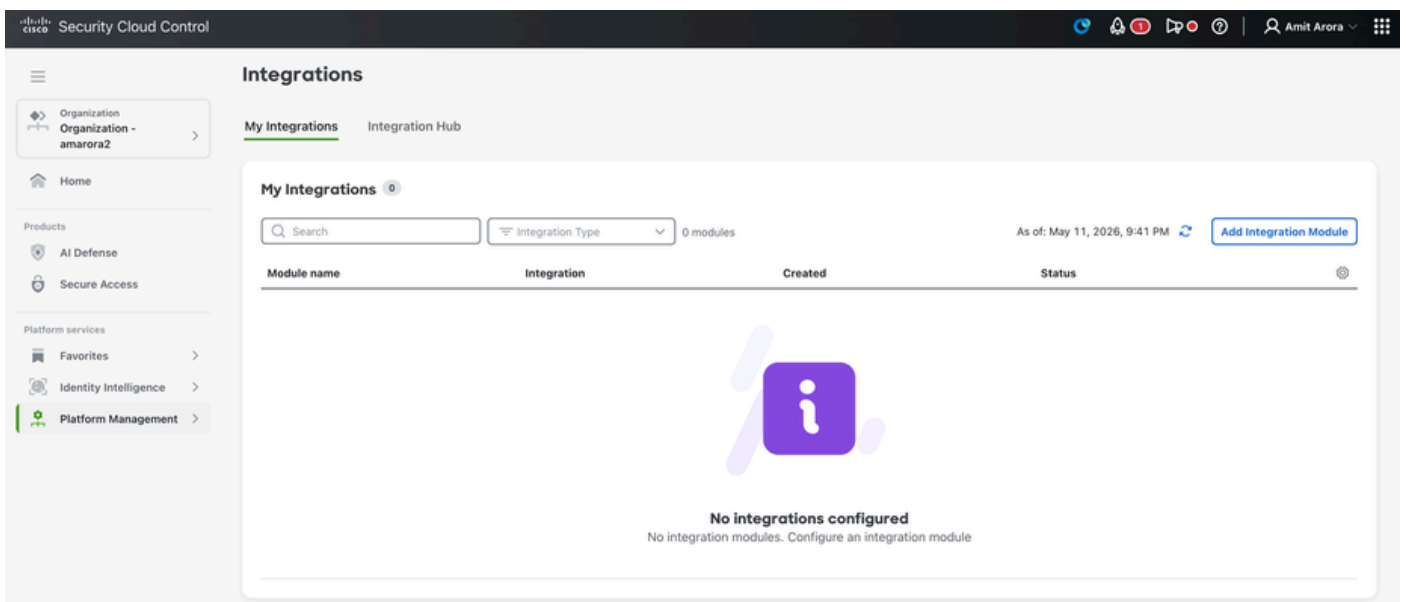
OK

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

Security Cloud Control

Integrations

My Integrations Integration Hub

Cisco integrations

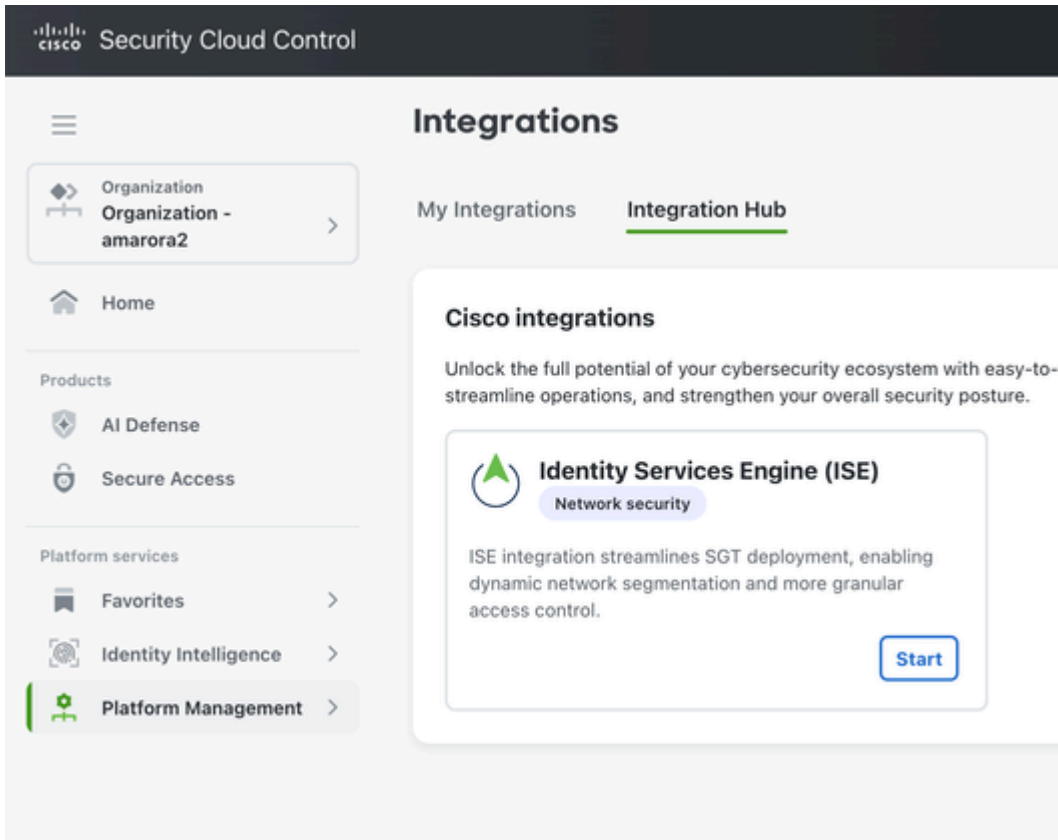
Unlock the full potential of your cybersecurity ecosystem with easy-to-use integ streamline operations, and strengthen your overall security posture.

Identity Services Engine (ISE)
Network security

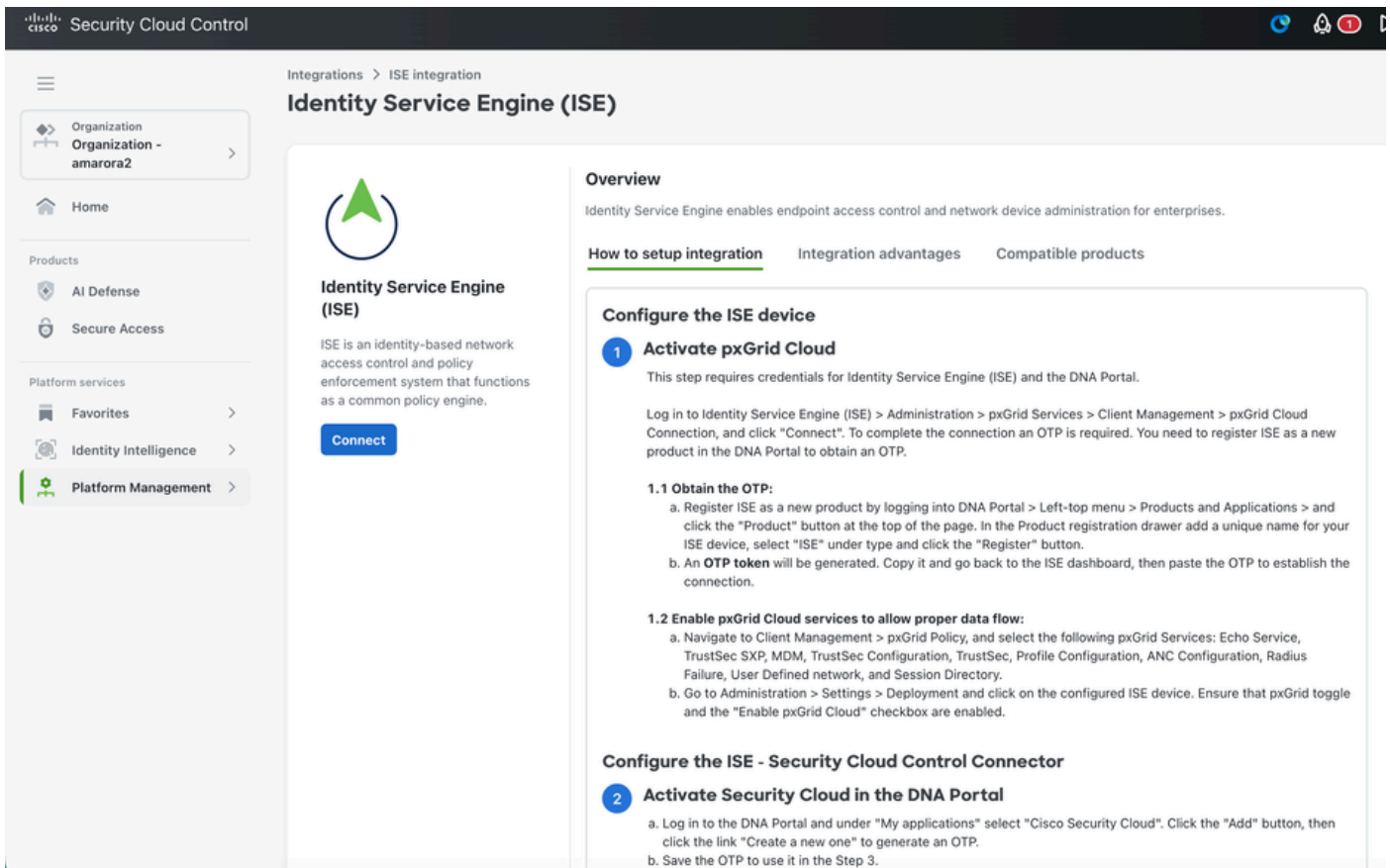
ISE integration streamlines SGT deployment, enabling dynamic network segmentation and more granular access control.

[Start](#)

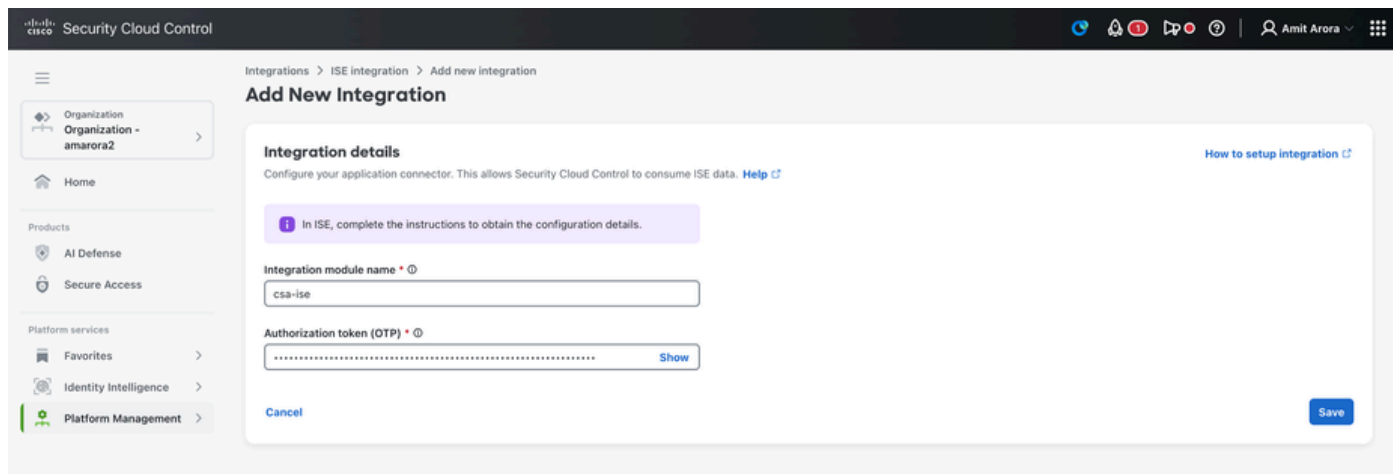
5 Haga clic en Inicio



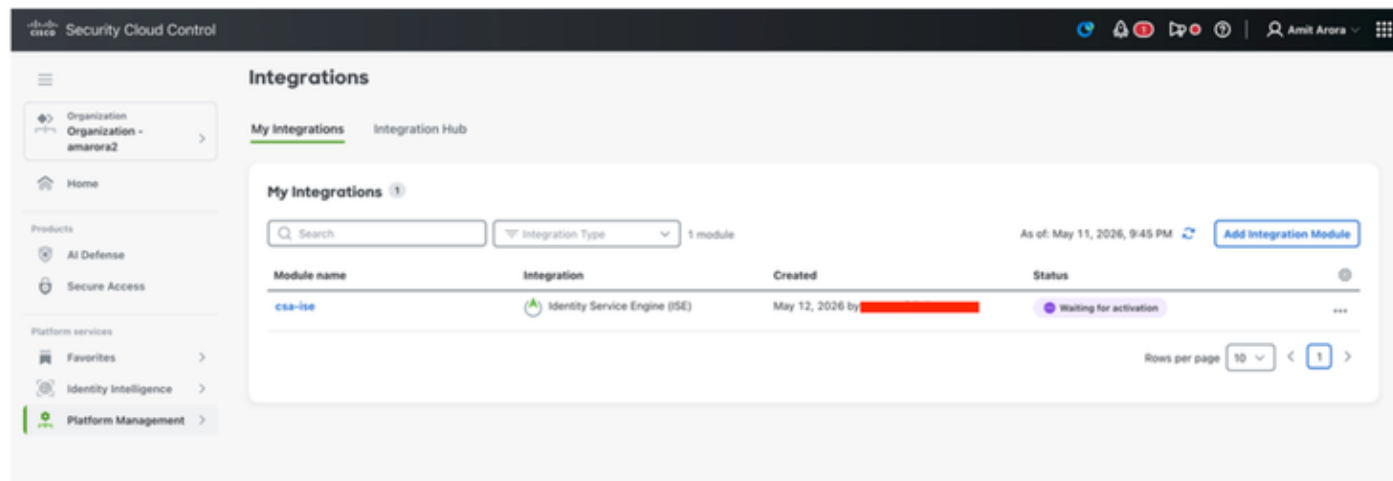
6 Haga clic en Conectar



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 persona - 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

The screenshot shows the Cisco Security Cloud configuration 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. The 'Configuration' tab is active, showing 'About this integration' information.

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
[Redacted]	Registered
Device name	Registered region
ise-test	us-west-2
Description	--

App configuration

Application status
 Inactive

Instance ⓘ
 Existing instances New instance

Select instance [dropdown menu]
ise-testnew
csa-ise

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.

10 El estado de la aplicación está conectado.

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.

Identity Services Engine Administration / 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 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

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 >

Verificar etiqueta de grupo de seguridad:

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



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

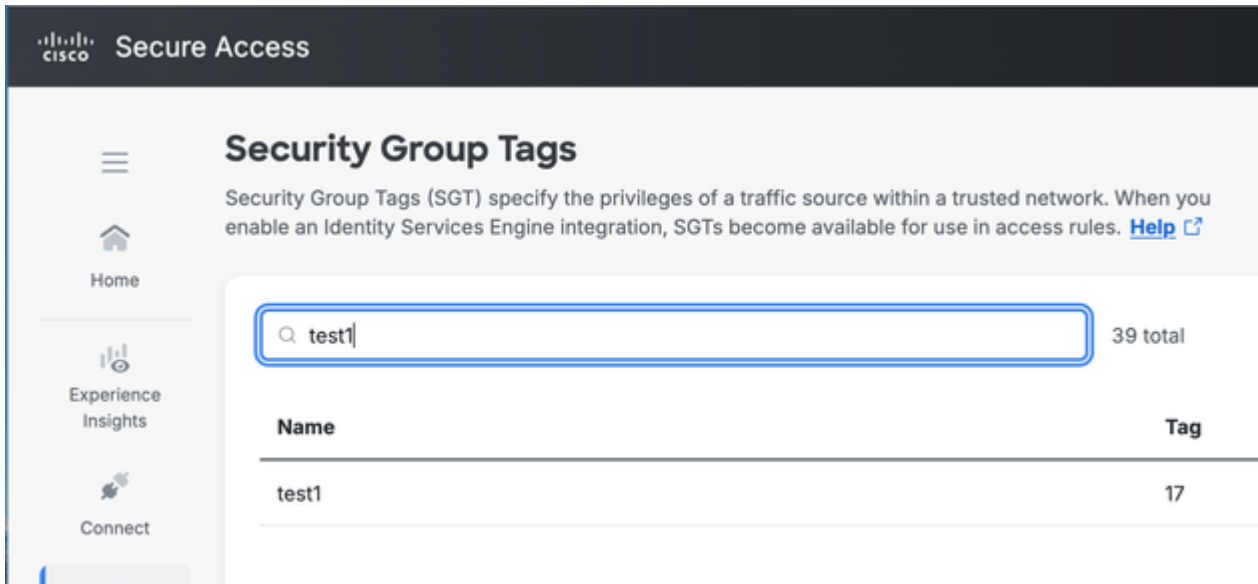
Application Portal

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

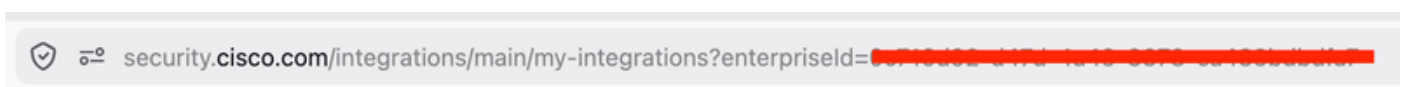
Infraestructura

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.

The screenshot shows the Cisco Security Cloud Control interface. The main content area is titled "Integrations" and displays a table of "My Integrations". The table has columns for "Module name", "Integration", "Created", and "Status". One integration is listed: "cisa-ise" (Identity Service Engine (ISE)), created on May 12, 2026, and is "Active".

Below the table, the "Response" tab is selected, showing the JSON response for the "cisa-ise" integration. The response is a JSON array with one object. The object contains the following fields:

- `integrationId`: "2722c2c6-ee6-416f-9617-389993b0b7d"
- `integrationName`: "cisa-ise"
- `integrationStatus`: "enabled"
- `region`: "us-west-2"
- `isCiscoProvider`: true
- `metadata`: {
 `createdAt`: "2026-05-12T01:45:18.830501"
 `updatedAt`: "2026-05-12T01:45:18.830505"
}
- `syncStatus`: "pending"

The `integrationId` field is highlighted with a red box in the original image.

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).