

Cisco Secure Access Integration with ISE for Security Group Tag over Pxgrid Cloud

Contents

Introduction

This document describes how to enable context sharing between Cisco Secure Access and Cisco Identity Services Engine

Requirements

Cisco recommends that you know these topics:

- Cisco Secure Access—A cloud-based security service edge (SSE) solution that provides zero-trust network access to allow users to easily connect to the internet and private applications from any device.
- Cisco Identity Service Engine (ISE) Version 3.4 Patch 5.
- Cisco Security Cloud Control—A unified management solution for your Security Cloud products and identity. Security Cloud Control is included with Secure Access.

Background

This integration enables the automated creation of reliable tunnels from Catalyst SD-WAN branches to Cisco Secure Access, facilitating the seamless exchange of VPN-ID/name and SGT context.

Cisco Identity Services Engine (ISE) remains the central authority for SGT configuration and management. Any updates performed in ISE are automatically synchronized with Cisco Secure Access. If an SGT is deleted, existing rules that reference it remain active to ensure that traffic matching continues as expected.

We are currently offering limited availability for SGT mappings, which extends support to include SGT destination objects within your security rules. Additionally, support for building SASE tunnels that carry SGT from Meraki and Cisco Secure Firewall is coming soon

Use Case:

SGT Name Space Based Policy:

As a Security Admin, Kit wants to enforce contiguous micro segmentation using SGT from onprem ISE for SSE Private as well as Internet Bound traffic. Ability to import SGT to apply policies.



Components Used

The information in this document is based on:

- Identity Service Engine (ISE) Version 3.4 Patch 5
- Secure Access
- Cisco Security Cloud

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Context Sharing Configuration Overview

- Connect ISE to Cisco Security Cloud
- Connect Cisco Secure Access to ISE

Configure

This guide breaks up the overall configuration into the these main steps:

1. Connect Cisco ISE to Cisco Security Cloud
2. Connect Cisco Secure access to Cisco ISE
3. Security Group Tags in Cisco Secure Access

Before you begin

- Ensure that you have installed and activated the Advantage license in your Cisco ISE deployment.
- The DNA Cloud agent creates an outbound HTTPS connection to Cisco DNA Cloud. Therefore, you must configure Cisco ISE proxy settings if the your network uses a proxy to reach the internet. To configure proxy settings in Cisco ISE, navigate to **Administration > System > Settings > Proxy**
- Ensure that port 443 is open for outbound connection from Cisco ISE to Cisco pxGrid Cloud portal. If firewall or proxy settings are configured, ensure that the these URLs are not blocked:

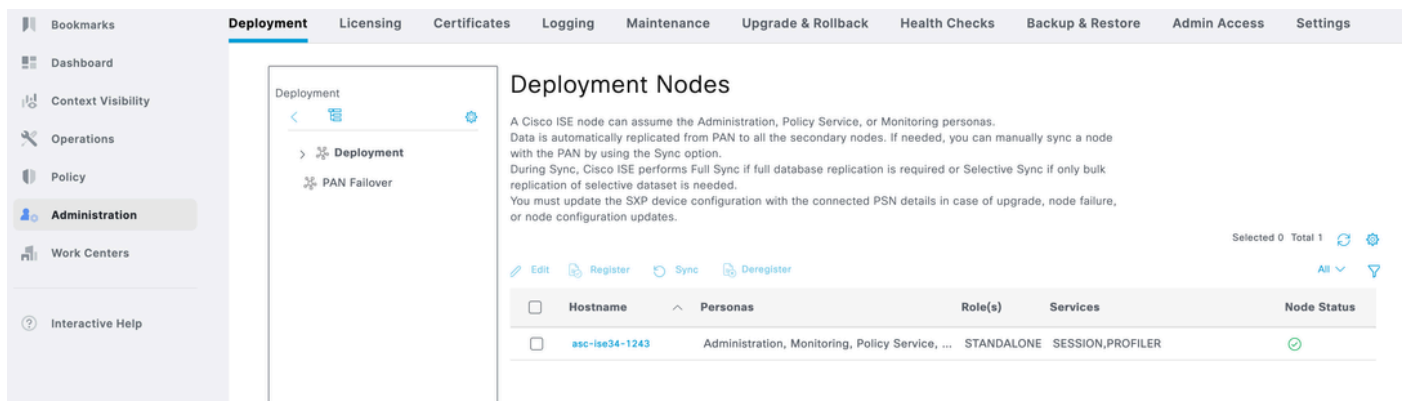
<https://dna.cisco.com>

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

Step1:Enable Pxgrid Cloud on ISE

1 Navigate to ISE GUI.

2 Click on Administration - Deployment.



3 Click on the Node and scroll down to the bottom.

Enter ISE Deployment Name

Select the Region as US West 2 which is the only region supported as of now.

Check both checkboxes and click Register.

The screenshot shows the Cisco ISE Administration interface. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (highlighted), Work Centers, and Interactive Help. The top navigation bar includes Deployment (highlighted), Licensing, Certificates, Logging, Maintenance, Upgrade & Rollback, Health Checks, and Backup & R. The main content area is titled 'pxGrid' and features a toggle switch that is turned on. Below the toggle, there is a checkbox for 'Enable pxGrid Cloud' which is checked. A yellow warning box states: 'pxGrid Cloud can be enabled only after registering your Cisco ISE to your Cisco DNA Portal account.' The 'ISE deployment name' field is filled with 'ise-test'. The 'Description (optional)' field is empty. The 'Region' dropdown menu is set to 'us-west-2'. Below these fields, there are two checked checkboxes: 'I have read and acknowledge the Cisco Privacy Statement.' and 'I agree that offers are governed by Cisco EULA and I am an authorized agent of my company. Cisco's End User License Agreement.' A blue 'Register' button is located at the bottom of the form.

4 You will see a Pop up with Auto filled Activation Code. Click Next,

The screenshot shows a browser window with the URL 'id.cisco.com/activate?user_code=...'. The page features the Cisco logo and a globe icon with 'US' and 'EN' labels. The main heading is 'Activate your device'. Below this, it says 'Follow the instructions on your device to get an activation code'. There is a text input field labeled 'Activation Code' containing a redacted code. A blue 'Next' button is positioned below the input field. At the bottom of the page, there are links for 'Contact support', 'Privacy', 'Terms & Conditions', 'Cookies', and 'Trademarks'.

5 ISE will show connected to Pxgrid Cloud.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System 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 'Administration / System' and has tabs for Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade & Rollback, and Health Checks. Under the 'Deployment' tab, there are several service enablement options:

- Enable Profiling Service ⓘ
- Enable Threat Centric NAC Service ⓘ
- > Enable SXP Service ⓘ
- Enable Device Admin Service ⓘ
- Enable Passive Identity Service ⓘ

Below these options, there is a section for 'pxGrid' with a toggle switch that is turned on. Underneath, 'Enable pxGrid Cloud' is checked. A message states: 'To enable pxGrid Cloud application, please go to the [Integration Catalog](#).'

| | |
|--------------------------|--|
| Cisco DNA Portal account | Status |
| [REDACTED] | <input checked="" type="checkbox"/> Connected |
| ISE deployment name | Registered region |
| ise-test | us-west-2 |
| Description | Mode |
| -- | Active |

A 'Deregister' button is located at the bottom of the pxGrid section.

6 Click Integration Catalog link from Step 5.

Under Available Integrations - Click Cisco Security Cloud

Identity Services Engine Administration / Integration Catalog Evaluation Mode 89 Days

Integration Catalog

Available integrations

- CIS Cisco Security Cloud**
Network Security pxGrid Cloud us-west-2
eu-central-1 ap-southeast-1
Cisco Security Cloud acts as an application broker which will allow ISE to integrate with the supported Cisco's cloud Security products through one single...
[More details](#)
- 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 presence to your sites...
[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 application service and ISE...
[More details](#)
- PXG pxGrid Cloud Demo Multi-instance**
networking demo pxGrid Cloud us-west-2
eu-central-1 ap-southeast-1
Welcome to Cisco pxGrid Cloud's Demo Application (Multi-instance)! The purpose of this is to guide you through the setup process for connecting an...
[More details](#)

7 Under App Configuration Click New Instance and click Activate

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.

Copy the One-time Password as it will be used on 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 

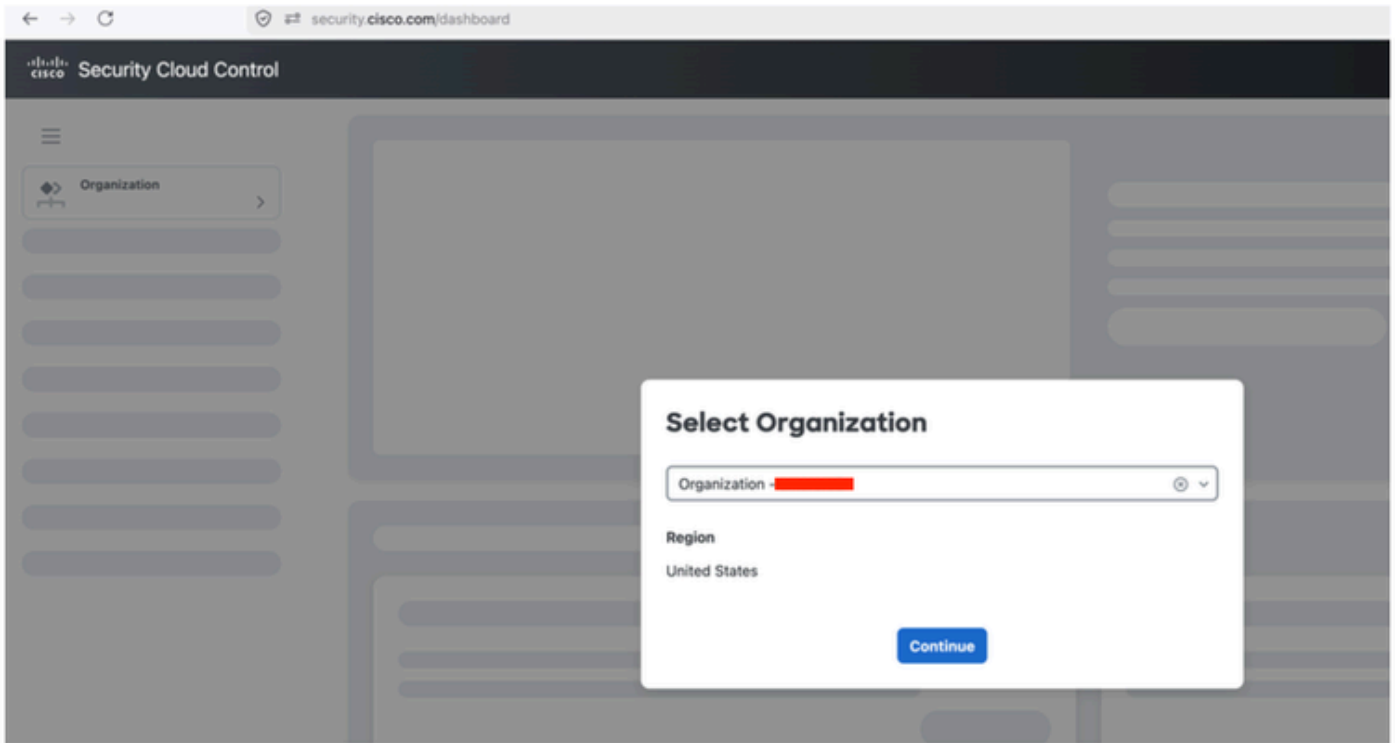
One-time password

  **Copy**

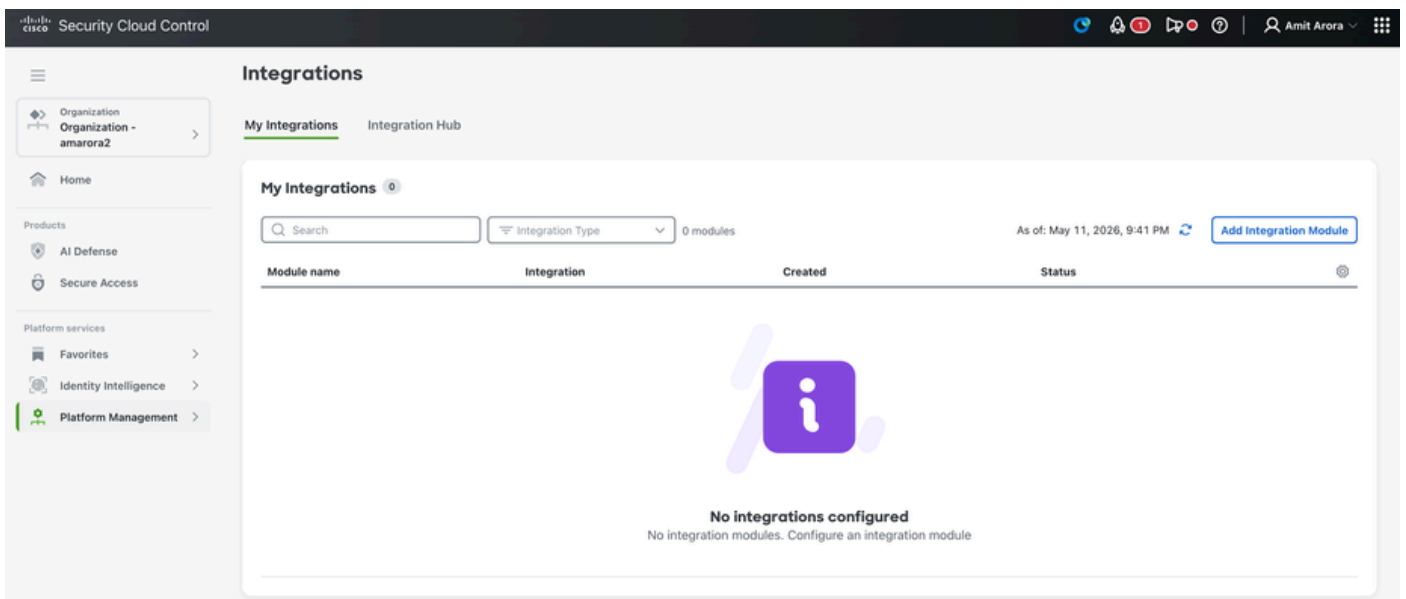
OK

Step2: Integrate Cisco Secure Access with ISE

1. Login to security.cisco.com.
2. Select the Cisco Secure Access ORG



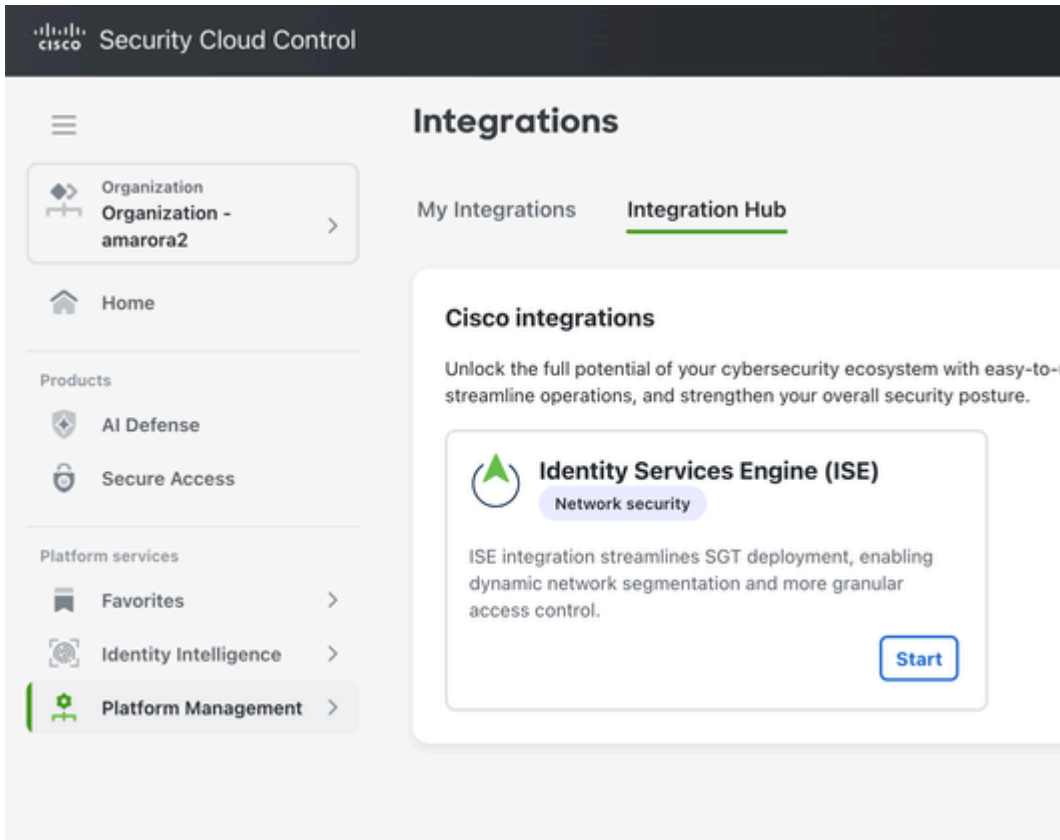
3 Click on Platform Management - Platform Integrations



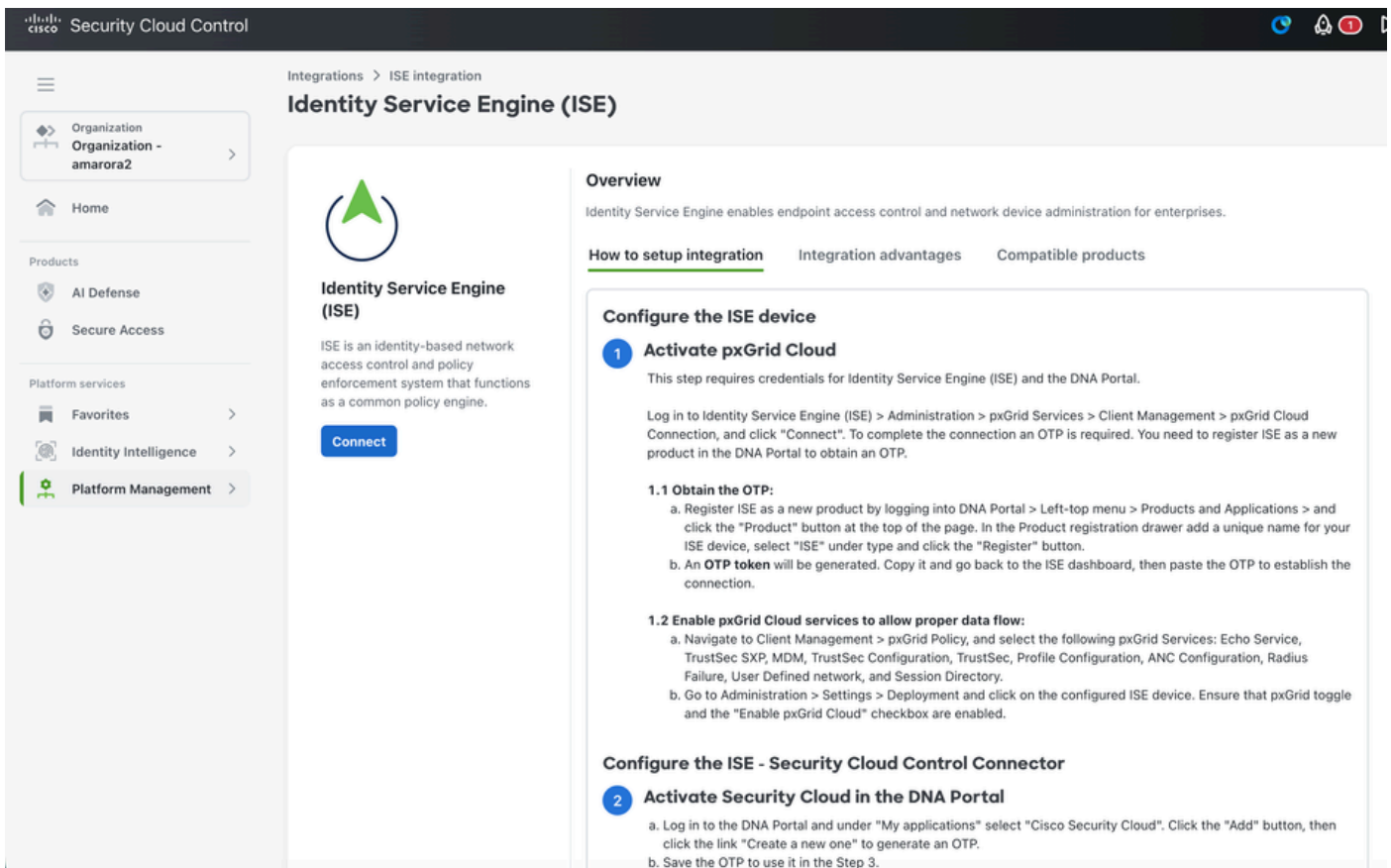
4 Click on Add Integration Module

The screenshot displays the Cisco Security Cloud Control interface. The top navigation bar includes the Cisco logo and the text "Security Cloud Control". On the left, a sidebar menu contains a hamburger icon, a navigation item for "Organization - amarora2", a "Home" button, and sections for "Products" (AI Defense, Secure Access) and "Platform services" (Favorites, Identity Intelligence, Platform Management). The main content area is titled "Integrations" and features two tabs: "My Integrations" and "Integration Hub" (which is underlined). Below the tabs, a section titled "Cisco integrations" provides a brief overview: "Unlock the full potential of your cybersecurity ecosystem with easy-to-use integ streamline operations, and strengthen your overall security posture." A prominent card for "Identity Services Engine (ISE)" is shown, categorized under "Network security". The card text states: "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 Click Start



6 Click Connect



7. Enter Integration module name and OTP from Cisco ISE and Click Save

Integrations > ISE integration > Add new integration

Add New Integration

Integration details [How to setup integration](#)

Configure your application connector. This allows Security Cloud Control to consume ISE data. [Help](#)

i In ISE, complete the instructions to obtain the configuration details.

Integration module name *

Authorization token (OTP) * [Show](#)

[Cancel](#) [Save](#)

8 Once click Save we will see Waiting for Activation Status.

Integrations

My Integrations Integration Hub

Search Integration Type 1 module As of: May 11, 2026, 9:45 PM [Add Integration Module](#)

| Module name | Integration | Created | Status |
|-------------------------|-------------------------------|-----------------|------------------------|
| csa-ise | Identity Service Engine (ISE) | May 12, 2026 by | Waiting for activation |

Rows per page: 10 < 1 >

9 Login to ISE and navigate to Administration - Deployment. Click on the node with pxgrid persona - click on Integration cloud under Pxgrid Connection.

Under App configuration - select the ISE instance created on Security Cloud Control and click Activate

← Integration Catalog

Cisco Security Cloud

Network Security pxGrid Cloud us-west-2 eu-central-1 ap-southeast-1

Configuration About this integration

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 ^

- 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 Application Status is now connected.

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.

| 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

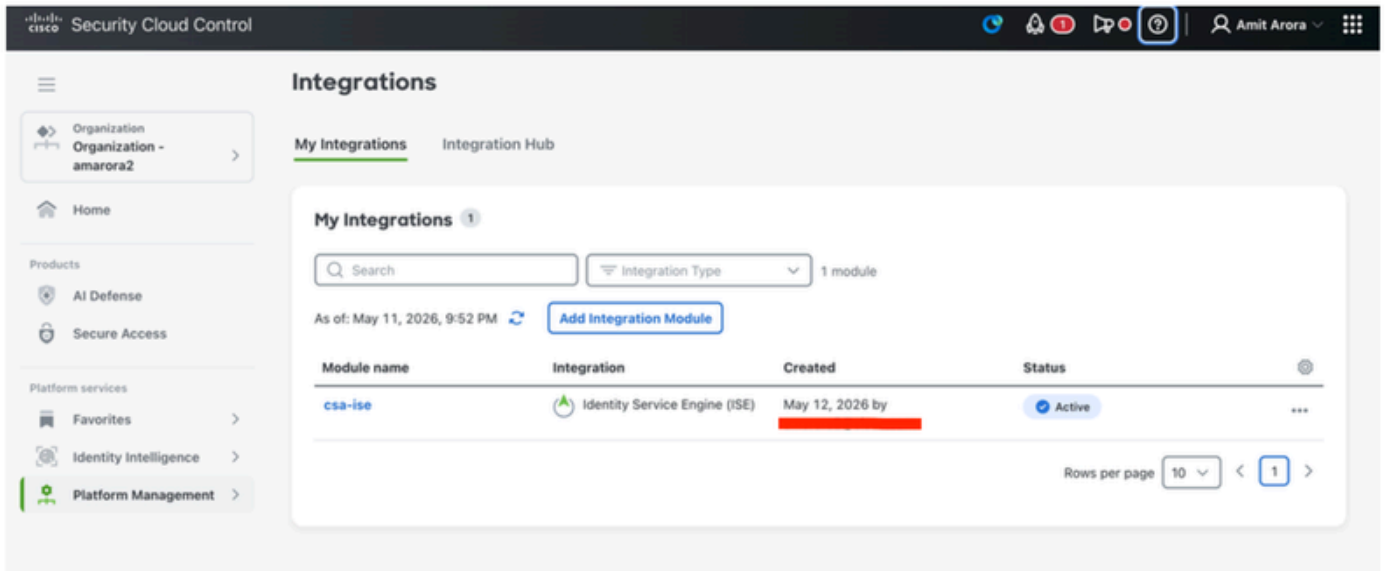
networking pxGrid Cloud us-west-2 eu-central-1 ap-southeast-1

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 Login to Security Cloud control - security.cisco.com

Under Platform Management - Platform Integrations We can see Integration Status as Active



The screenshot shows the Cisco Security Cloud Control interface. The top navigation bar includes the Cisco logo, the text "Security Cloud Control", and user information "Amit Arora". The main content area is titled "Integrations" and has two tabs: "My Integrations" (selected) and "Integration Hub". On the left, a sidebar menu lists "Organization - amarora2", "Home", "Products" (AI Defense, Secure Access), and "Platform services" (Favorites, Identity Intelligence, Platform Management). The "My Integrations" section features a search bar, a filter for "Integration Type", and a refresh button. Below this is a table with one entry:

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

At the bottom right of the table, there is a "Rows per page" dropdown set to 10 and a pagination control showing page 1 of 1.

Verify Security Group Tag:

Login to Cisco Secure Access. Navigate to Resources - Security Group Tags.



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

Login to Security.cisco.com
Navigate to Platform Management - Platform Integrations

Search for integrations?page=api call and in response tab you will find an Integrations ID.

The screenshot shows the Cisco Security Cloud Control interface. The main heading is "Integrations" with sub-sections "My Integrations" and "Integration Hub". A search bar and "Integration Type" dropdown are visible. A table lists integrations with columns for "Module name", "Integration", "Created", and "Status". One integration, "csc-ise", is highlighted as "Identity Service Engine (ISE)" and "Active".

Below the table, the "Inspector" console shows a series of API requests. The selected request is a GET call to `api2.amplitude.com/integrations?page=0&max=10`. The response is a JSON object containing an array of integration details:

```
{
  "integrations": [
    {
      "integrationId": "2722c2c6-ee46-416f-9617-389993bb0b7d",
      "integrationName": "csc-ise",
      "integrationStatus": "enabled",
      "integrationType": "ise",
      "region": "us-west-2",
      "isCiscoProvider": true,
      "metadata": {
        "createdAt": "2026-05-12T01:45:18.830501",
        "updatedAt": "2026-05-12T01:45:18.830505"
      },
      "syncStatus": "pending"
    }
  ]
}
```