

# Tag Cisco Secure Access Integration con ISE per il gruppo di sicurezza su Pxgrid Cloud

## Sommario

---

---

## Introduzione

Questo documento descrive come abilitare la condivisione del contesto tra Cisco Secure Access e Cisco Identity Services Engine

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Access: una soluzione SSE (Security Service Edge) basata su cloud che fornisce accesso di rete senza attendibilità per consentire agli utenti di connettersi facilmente a Internet e alle applicazioni private da qualsiasi dispositivo.
- Cisco Identity Service Engine (ISE) versione 3.4, patch 5.
- Cisco Security Cloud Control: una soluzione di gestione unificata per l'identità e i prodotti Security Cloud. Security Cloud Control è incluso con Secure Access.

## Introduzione

Questa integrazione consente la creazione automatizzata di tunnel affidabili dalle filiali Catalyst SD-WAN a Cisco Secure Access, semplificando lo scambio continuo di VPN-ID/nome e contesto SGT.

Cisco Identity Services Engine (ISE) rimane l'autorità centrale per la configurazione e la gestione del SGT. Tutti gli aggiornamenti eseguiti ad ISE vengono sincronizzati automaticamente con Cisco Secure Access. Se si elimina un SGT, le regole esistenti che fanno riferimento a tale SGT rimangono attive per garantire che la corrispondenza del traffico continui come previsto.

Attualmente offriamo una disponibilità limitata per le mappature SGT, che estende il supporto agli oggetti di destinazione SGT all'interno delle regole di sicurezza. Inoltre, presto sarà disponibile il supporto per la creazione di tunnel SASE che trasportano SGT da Meraki e Cisco Secure Firewall

## Scenario d'uso:

Criterio basato sullo spazio dei nomi SGT:

In qualità di amministratore della sicurezza, il kit intende applicare la micro segmentazione contigua utilizzando il protocollo SGT di ISE per il traffico SSE privato e Internet. Capacità di importare il protocollo SGT per applicare le policy.



## Componenti usati

Le informazioni fornite in questo documento si basano su:

- Patch 5 per Identity Service Engine (ISE) versione 3.4
- Accesso sicuro
- Cisco Security Cloud

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Panoramica della configurazione di Condivisione contesto

- Collega ISE a Cisco Security Cloud
- Connessione di Cisco Secure Access ad ISE

## Configurazione

La presente guida suddivide la configurazione generale nei seguenti passaggi principali:

1. Collega Cisco ISE a Cisco Security Cloud
2. Connetti Cisco Secure access a Cisco ISE
3. Tag gruppo di sicurezza in Cisco Secure Access

## Operazioni preliminari

- Verificare di aver installato e attivato la licenza Advantage nell'implementazione di Cisco ISE.
- L'agente DNA Cloud crea una connessione HTTPS in uscita a Cisco DNA Cloud. Pertanto, è necessario configurare le impostazioni proxy di Cisco ISE se la rete utilizza un proxy per raggiungere Internet. Per configurare le impostazioni proxy in Cisco ISE, passare a **Administration > System > Settings > Proxy**
- Verificare che la porta 443 sia aperta per la connessione in uscita dal portale Cisco ISE a Cisco pxGrid Cloud. Se sono configurate le impostazioni del firewall o del proxy, verificare che questi URL non siano bloccati:

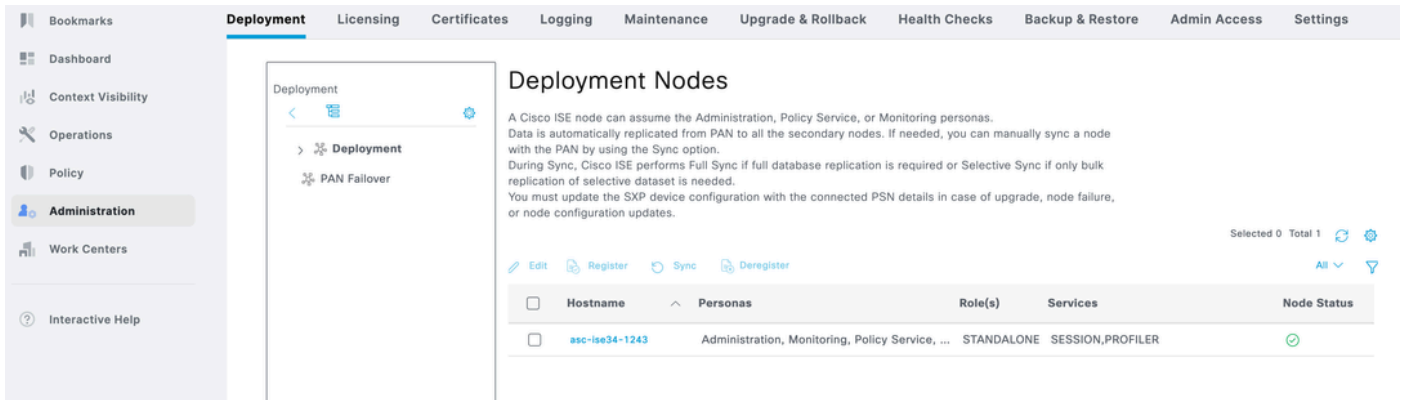
<https://dna.cisco.com>

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

## Fase 1. Abilitare Pxgrid Cloud su ISE

1 Passare alla GUI di ISE.

2 Fare clic su Amministrazione - Distribuzione.

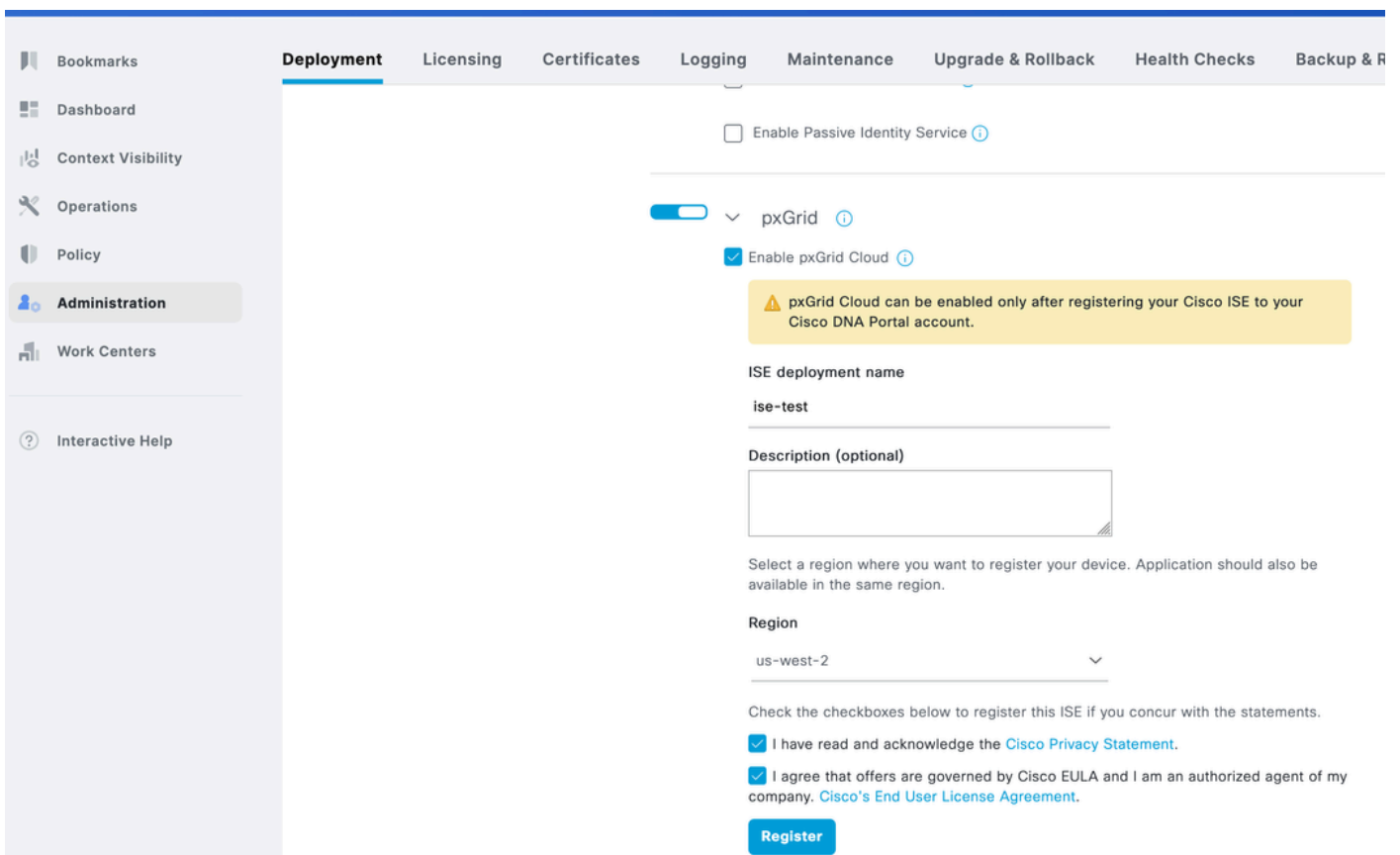


3 Fare clic sul Nodo e scorrere verso il basso.

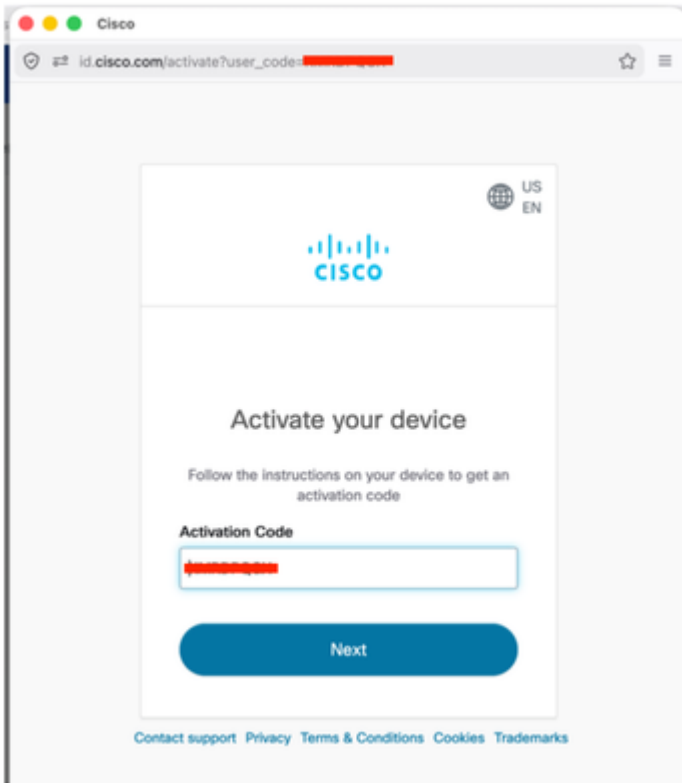
Immettere il nome dell'implementazione ISE

Selezionare l'area come US West 2 che è l'unica regione supportata al momento.

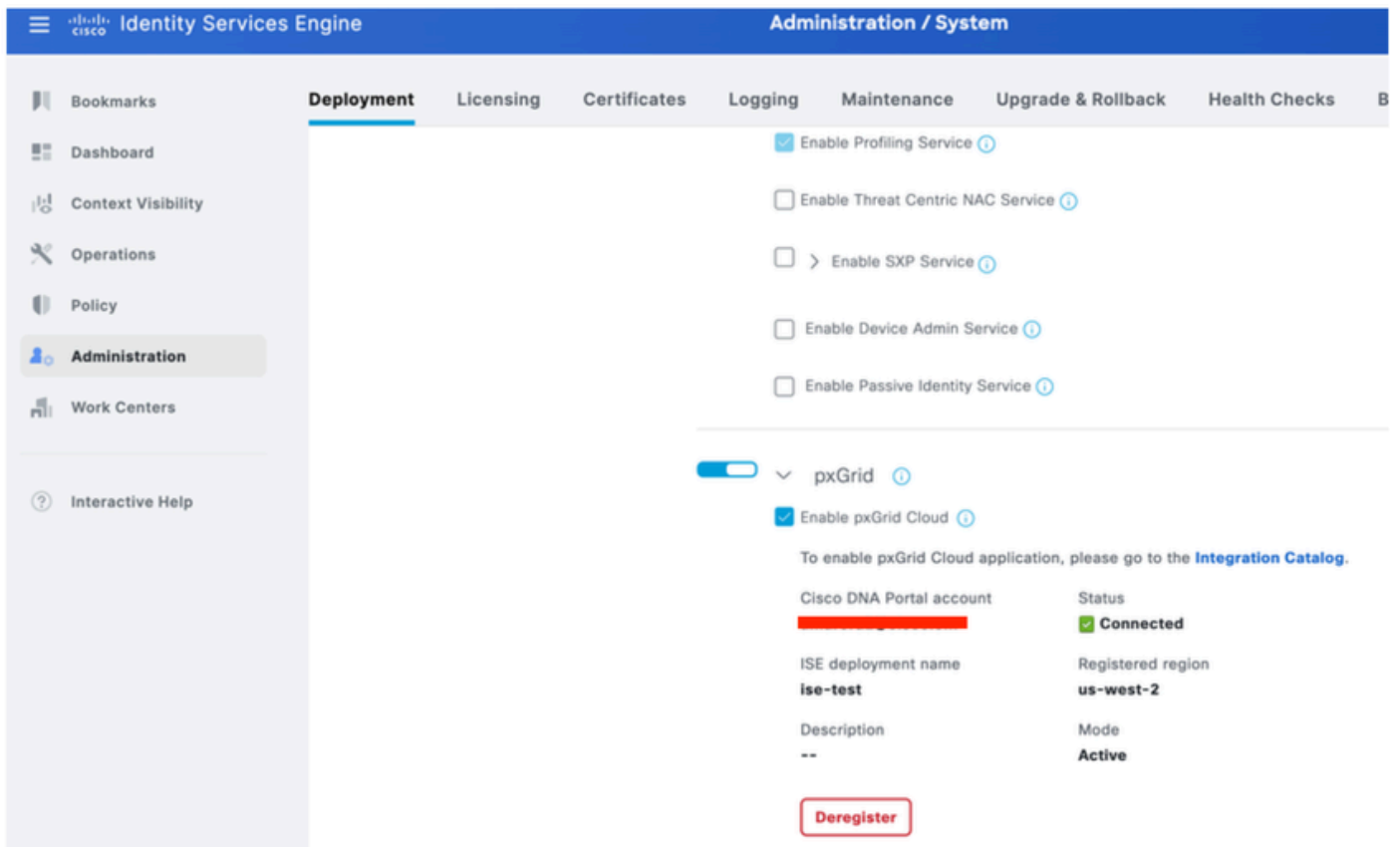
Selezionare entrambe le caselle e fare clic su Registra.



4 Viene visualizzata una schermata di popup con il codice di attivazione a riempimento automatico. Fare clic su Next (Avanti),

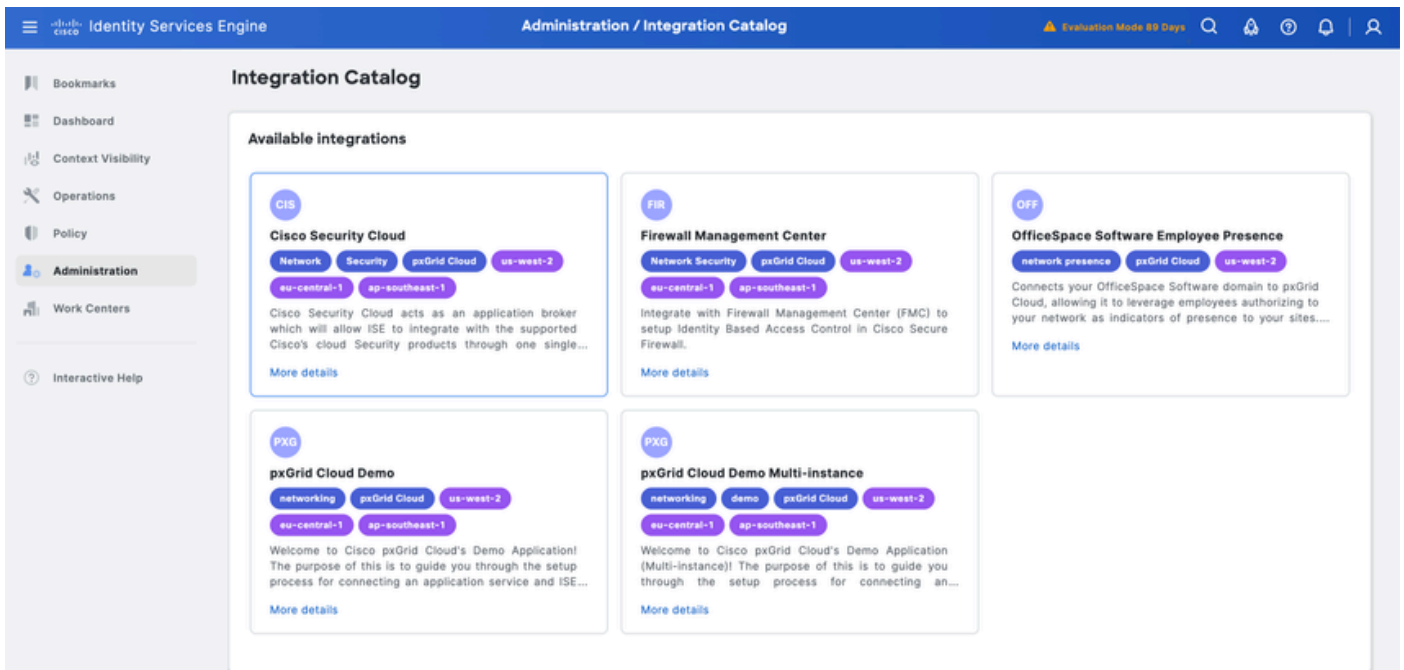


5 ISE mostrerà connected to Pxgrid Cloud.



6 Fare clic sul collegamento Integration Catalog dal passo 5.

In Integrazioni disponibili fare clic su Cisco Security Cloud



7 In Configurazione applicazione fare clic su Nuova istanza e quindi su Attiva

## 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.

Copiare la password monouso come verrà utilizzata in 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](#) 

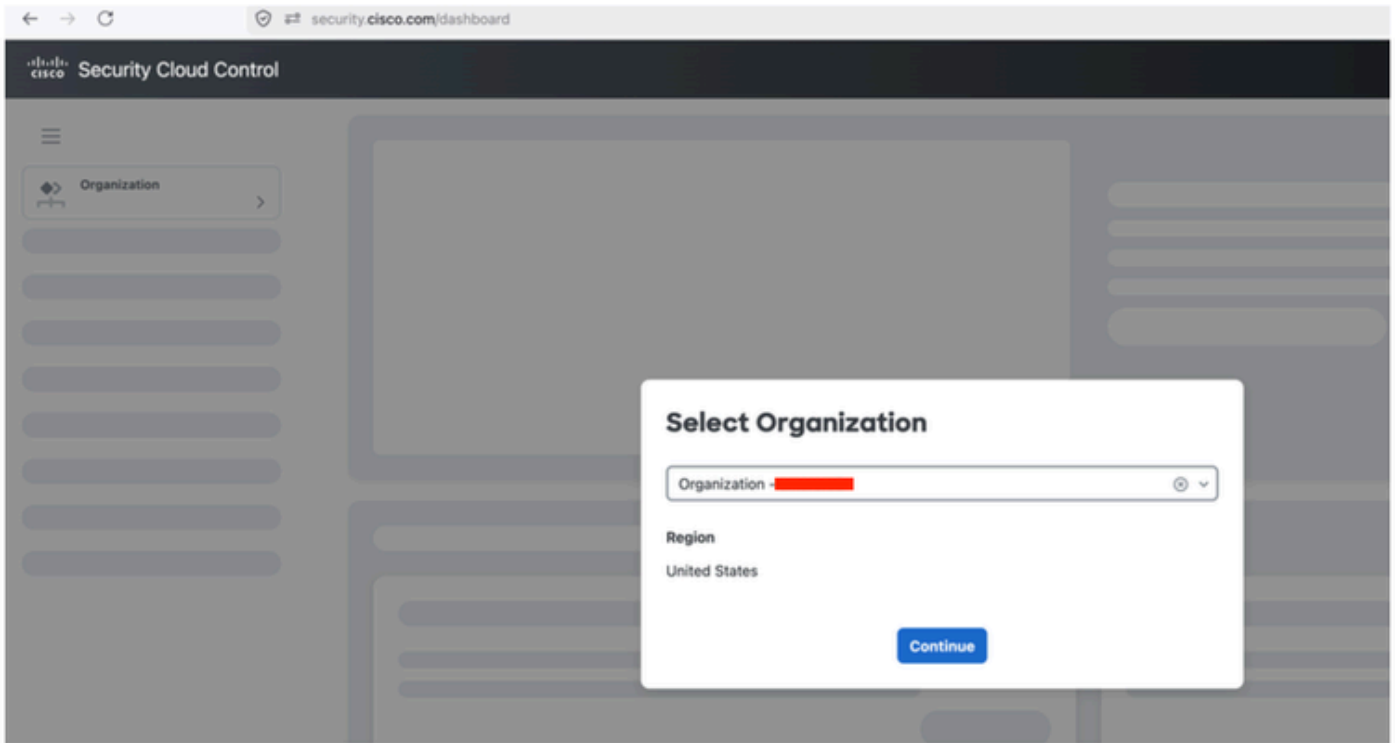
One-time password

  **Copy**

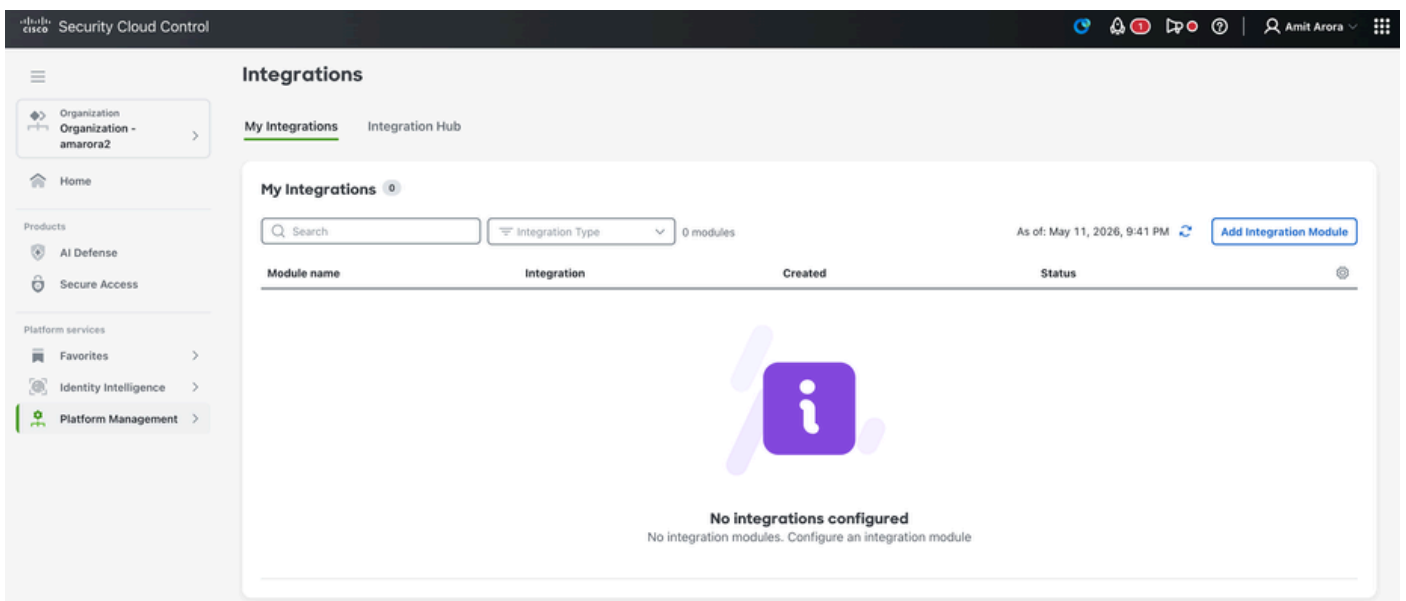
**OK**

### Fase 2: Integrazione di Cisco Secure Access con ISE

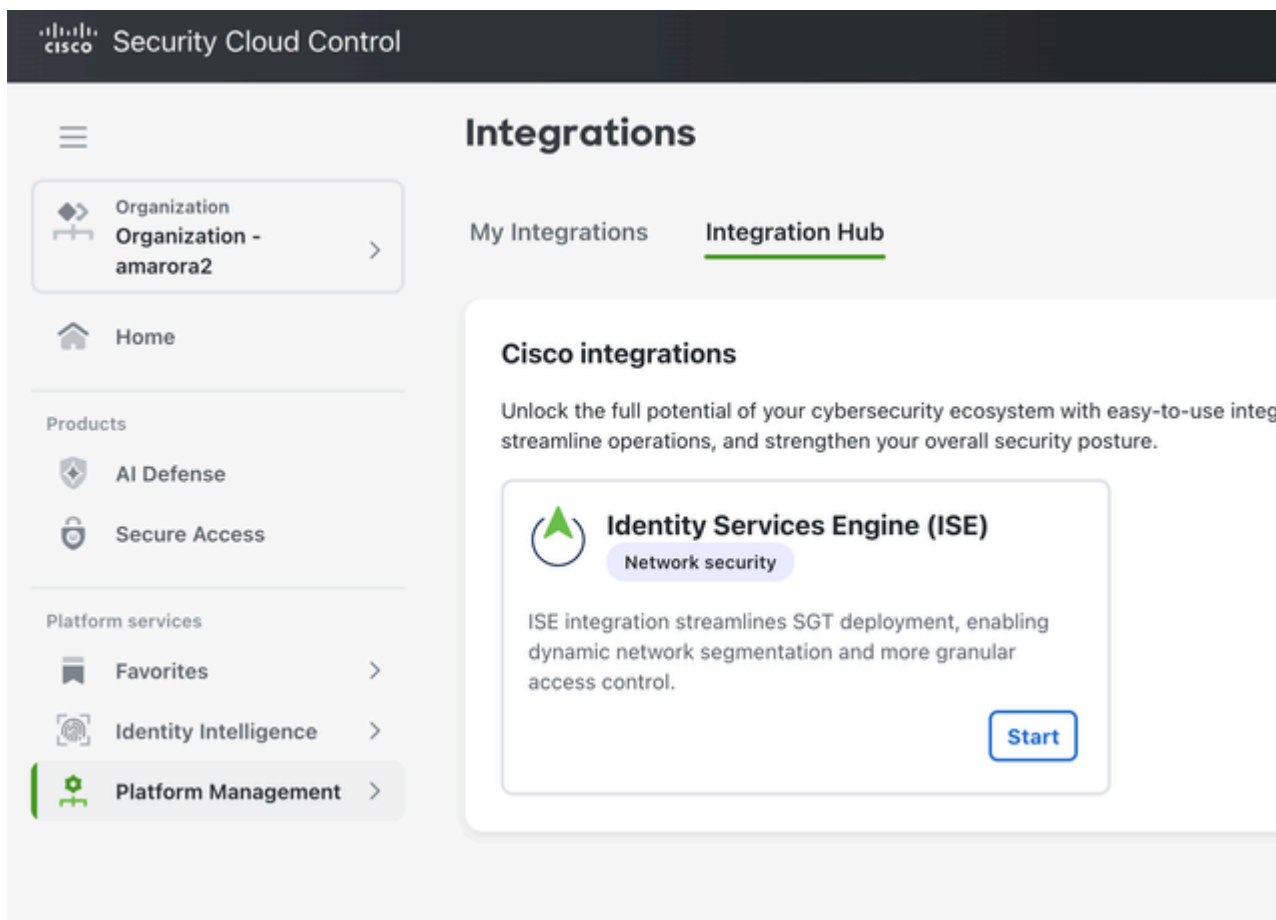
1. Accedere a security.cisco.com.
2. Selezionare Cisco Secure Access ORG



3 Fare clic su Platform Management - Platform Integration (Gestione piattaforma - Integrazioni della piattaforma)

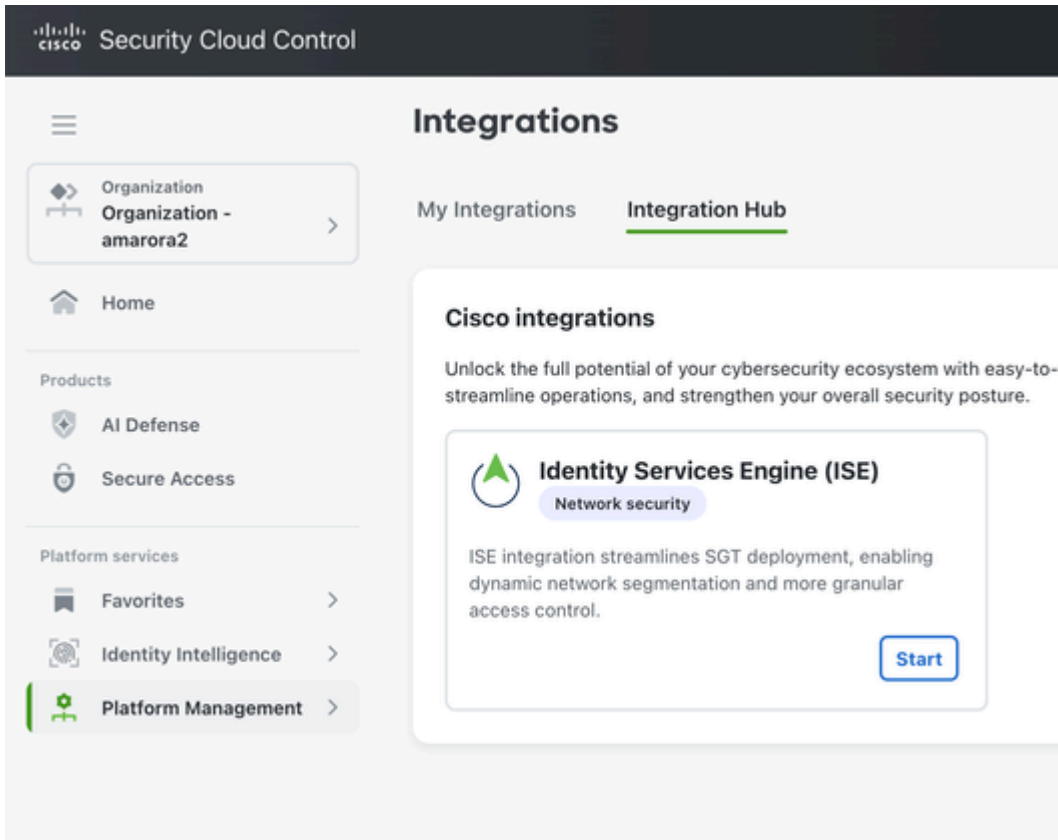


#### 4 Fare clic su Add Integration Module

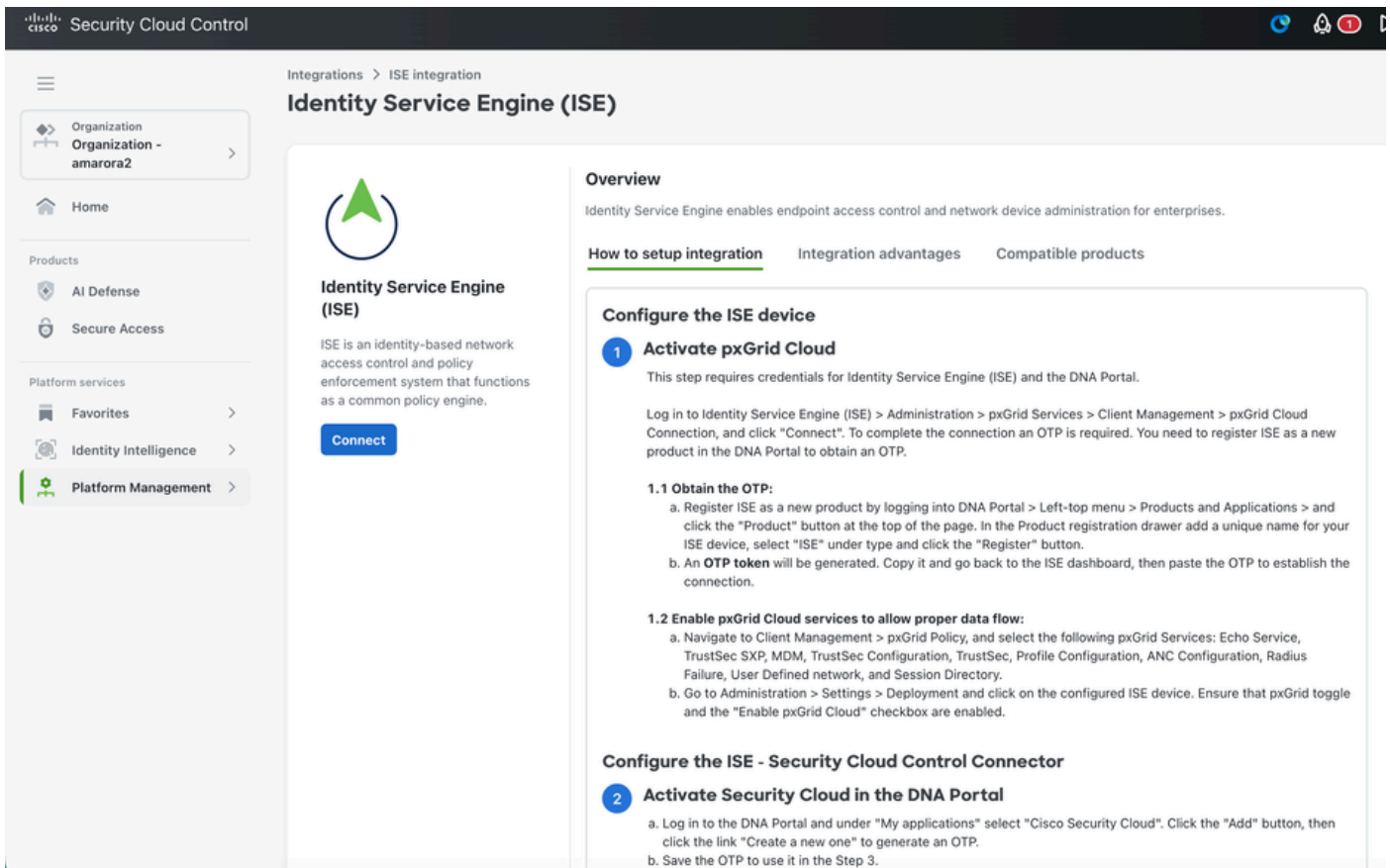


The screenshot shows the Cisco Security Cloud Control interface. The top navigation bar includes the Cisco logo and the text "Security Cloud Control". On the left, a sidebar menu contains a hamburger icon, a button for "Organization - amarora2", a "Home" button, and sections for "Products" (AI Defense, Secure Access) and "Platform services" (Favorites, Identity Intelligence, Platform Management). The main content area is titled "Integrations" and has two tabs: "My Integrations" and "Integration Hub" (which is selected). Below the tabs, a section titled "Cisco integrations" contains a descriptive paragraph and a card for "Identity Services Engine (ISE)". The ISE card includes a green triangle icon, the text "Identity Services Engine (ISE)", a "Network security" tag, a descriptive paragraph about SGT deployment, and a blue "Start" button.

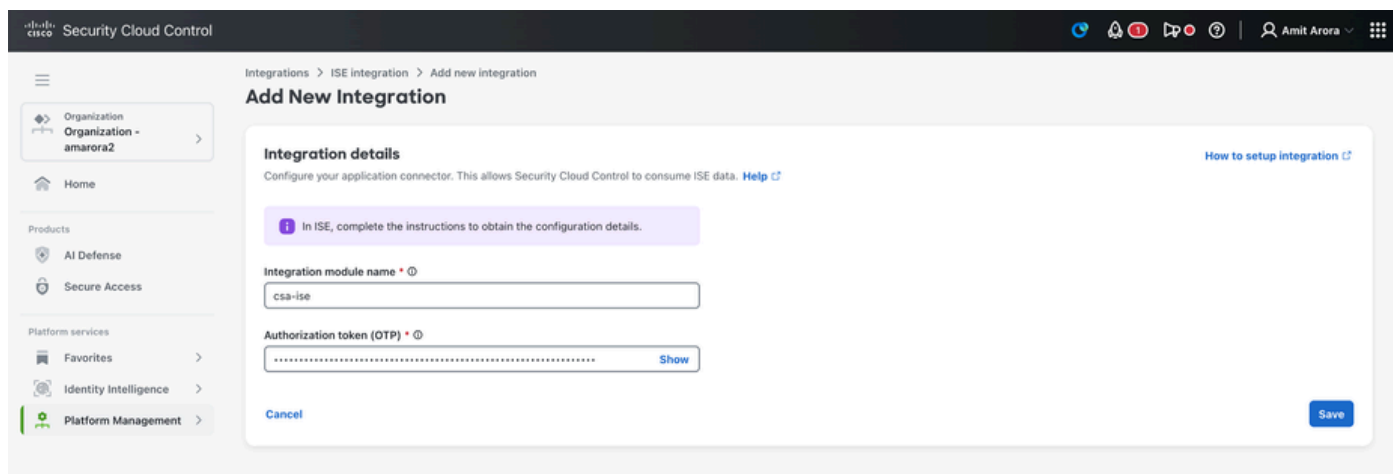
#### 5 Fare clic su Start



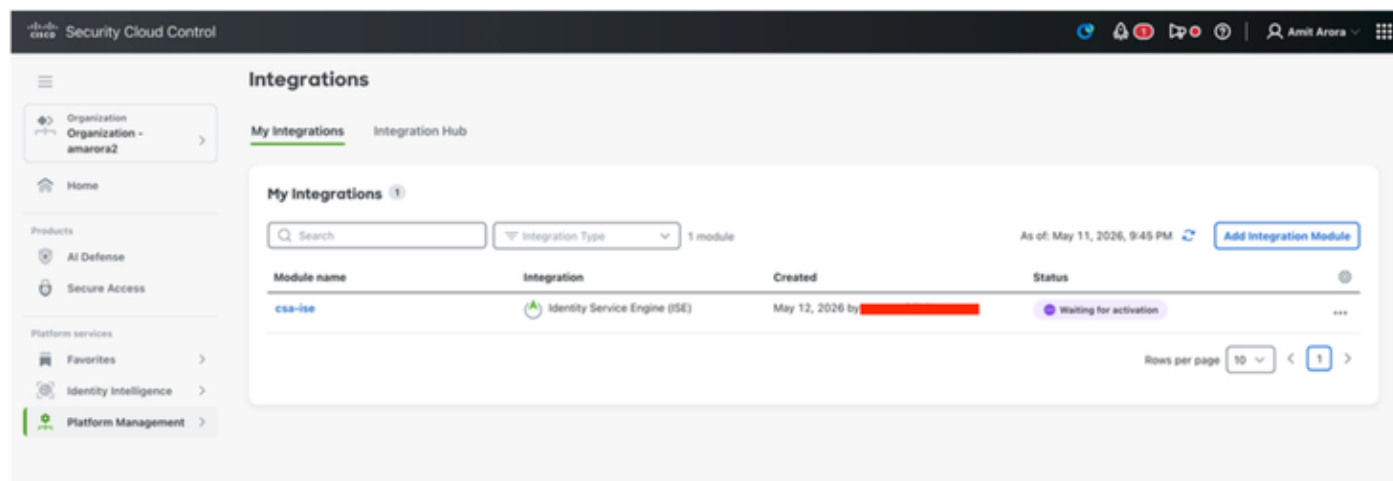
## 6 Fare clic su Connect



7. Inserire il nome del modulo di integrazione e OTP da Cisco ISE e fare clic su Salva



8. Facendo clic su Save (Salva), viene visualizzato Waiting for Activation Status (In attesa dello stato di attivazione).



9. Accedere ad ISE e selezionare Administration - Deployment. Fare clic sul nodo con pxgrid persona. Fare clic su Integration cloud in Pxgrid Connection.

In Configurazione app - selezionare l'istanza ISE creata in Security Cloud Control e fare clic su

The screenshot displays the Cisco Security Cloud interface. On the left is a navigation sidebar with options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (highlighted), Work Centers, and Interactive Help. The main header shows 'Integration Catalog' and 'Cisco Security Cloud' with tabs for Network, Security, pxGrid Cloud, us-west-2, eu-central-1, and ap-southeast-1. Below the header, there are two main sections:

- Registration:** This section explains that integration with pxGrid Cloud occurs through a Cisco DNA Portal account. It includes a link to 'Manage your ISE registration'. Below this, a table lists registration details:

Cisco DNA Portal account	Status
[Redacted]	Registered
Device name	Registered region
ise-test	us-west-2
Description	--
- App configuration:** This section shows the application status as 'Inactive'. It allows selecting an instance from a dropdown menu, with options for 'Existing instances' (selected) and 'New instance'. The dropdown menu is open, showing 'ise-testnew' and 'csa-ise'. Below the dropdown, there is a note: 'Select at least 1 data scope for this application to consume.' and a checked checkbox for 'Adaptive Network Control (ANC) Configuration', which provides details on policy name, action type, status, and MAC address.

10 Lo stato dell'applicazione è connesso.

## 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](#).

**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 Accesso al controllo di Security Cloud - security.cisco.com

In Gestione piattaforma - Integrazioni di piattaforma è possibile visualizzare lo stato di integrazione come Attivo

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 >

Verifica tag gruppo di sicurezza:

Accedere a Cisco Secure Access. Passare a Risorse - Tag gruppo di sicurezza.



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

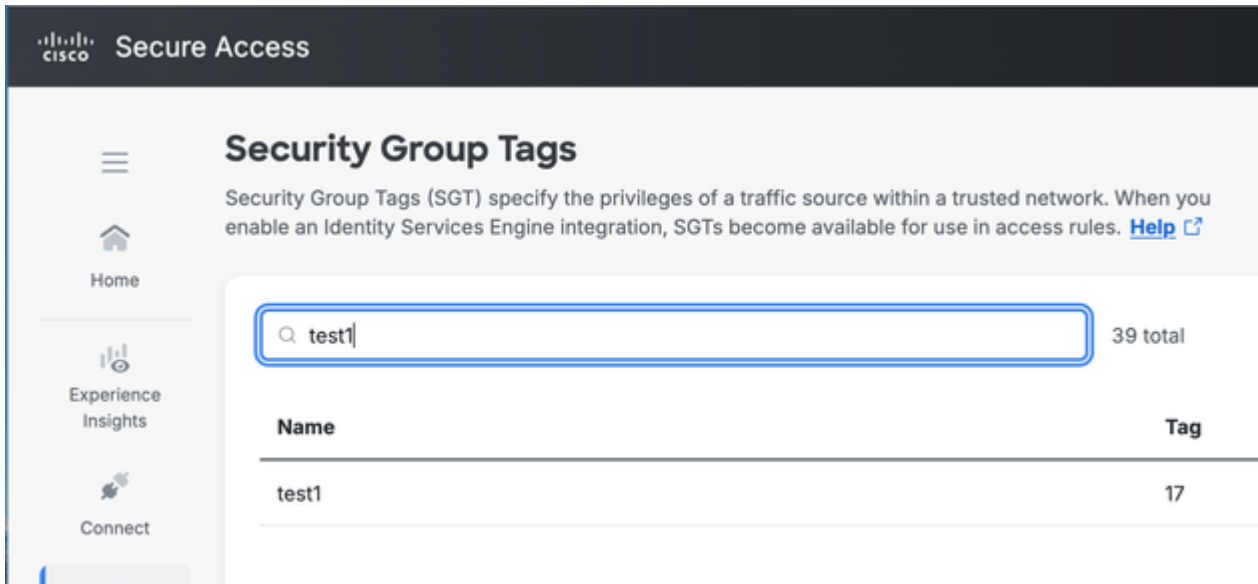
Application Portal

### Settings

AAA Servers

DNS Servers

Enablement Schedule



## Informazioni richieste per Cisco TAC

ISE:

[Come raccogliere ISE Support Bundle](#) con i seguenti componenti impostati su Debug Level sul nodo ISE con Pxgrid Persona:

pxgrid

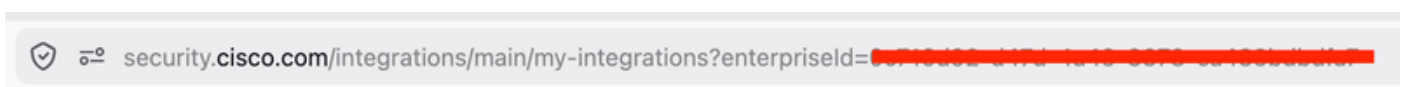
Infrastruttura

ERS

componente hermes a livello di debug.

SCC:

ID organizzazione: nell'URL di security.cisco.com



ID integrazione.

Avvia [acquisizione HAR](#)

Accedi a [Security.cisco.com](https://Security.cisco.com)

Passare a Gestione piattaforme - Integrazioni di piattaforme

Cercare le integrazioni? chiamata dell'API della pagina e nella scheda delle risposte è disponibile un ID di Integrations.

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

Below the table, a network inspector shows the response of an API call. The response is a JSON object containing an array of integration details. A red box highlights the following JSON structure:

```
{
  "integrationId": "2722c2c6-ee6-416f-9617-389993b0b7d",
  "integrationName": "csa-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"
}
```

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).