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:

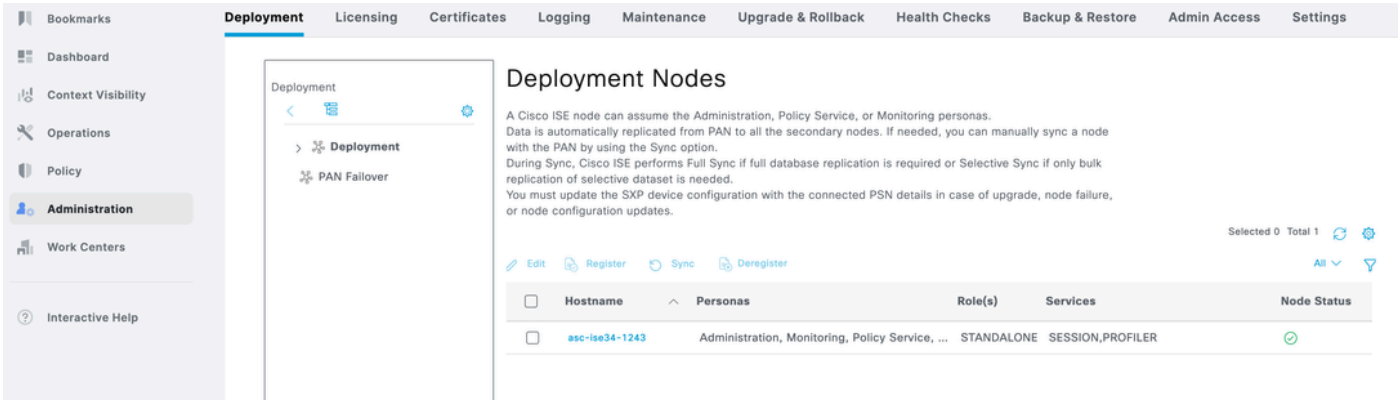
https://dna.cisco.com

https://security.cisco.com/

Fase 1. Abilitare Pxgrid Cloud su ISE

1 Passare alla GUI di ISE.

2 Fare clic su Amministrazione - Distribuzione.

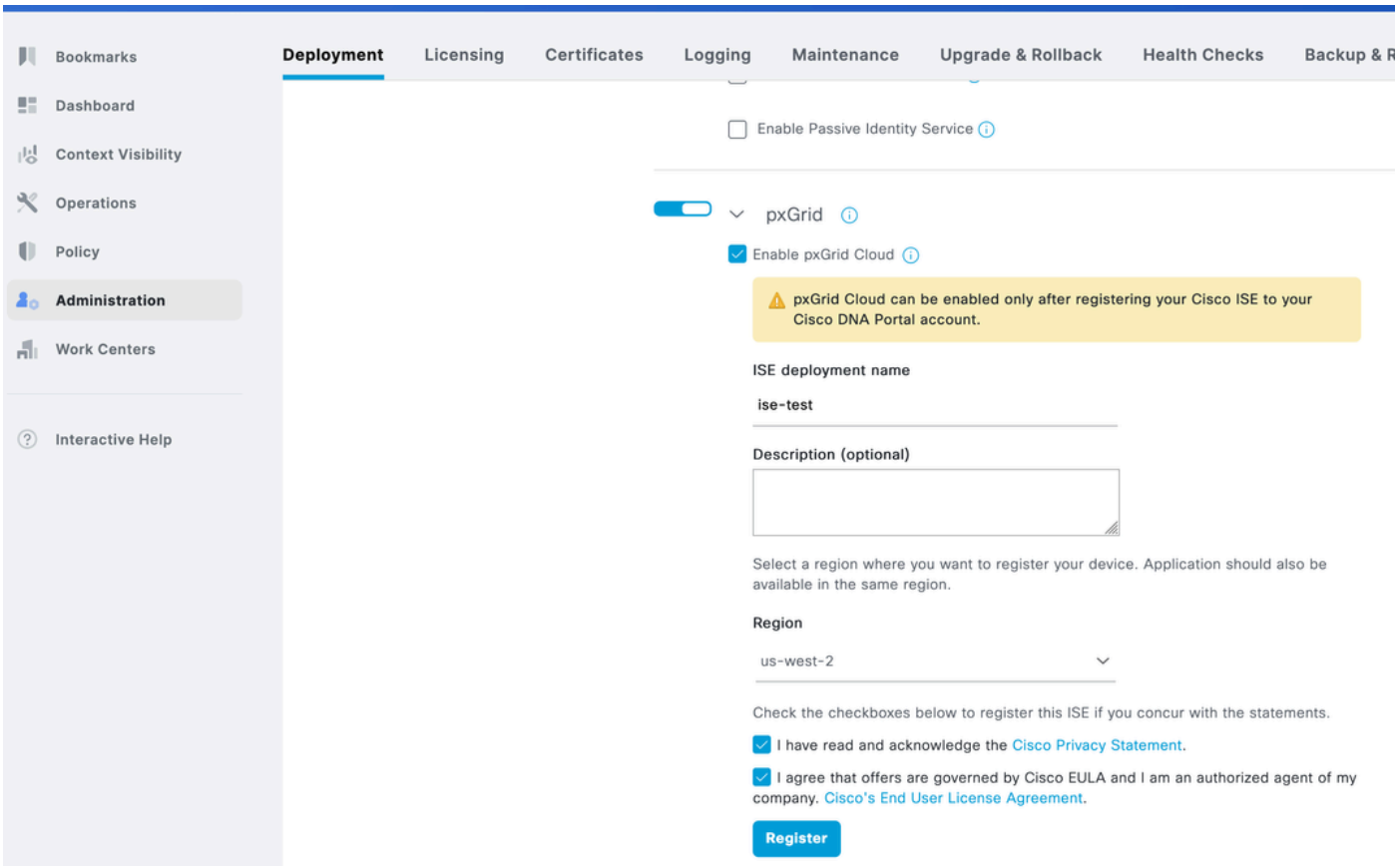


3 Fare clic sul Nodo e scorrere verso il basso.

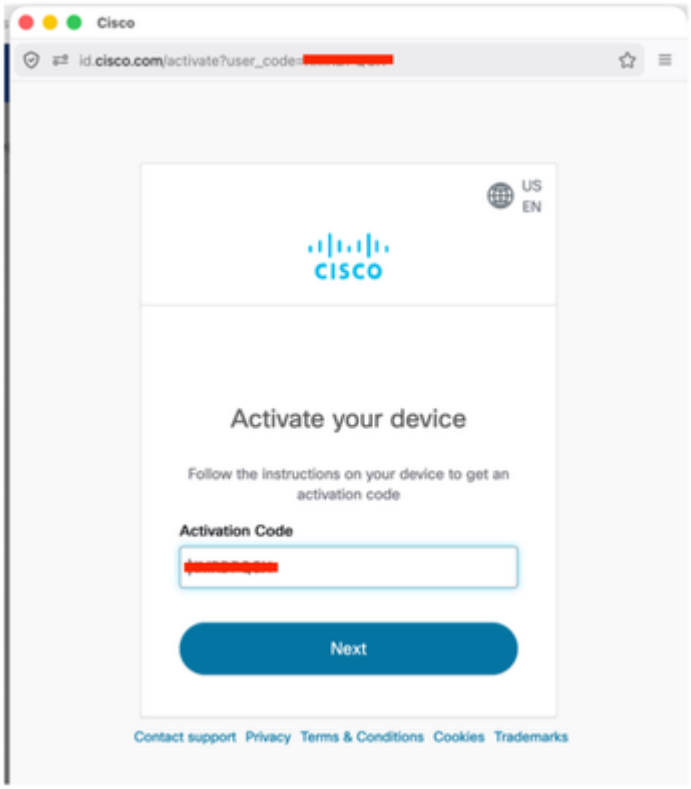
Immettere il nome dell'implementazione ISE

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

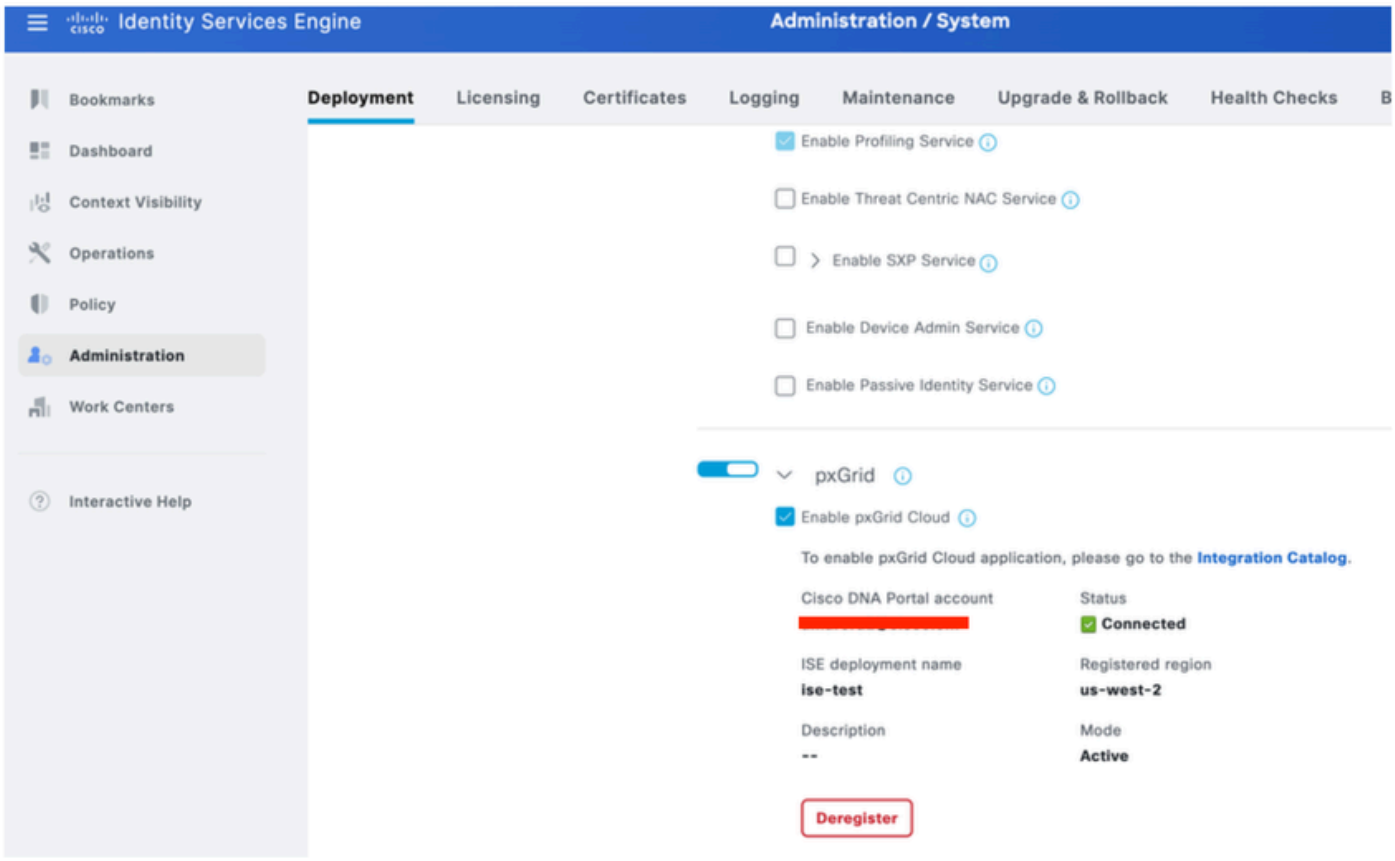
Selezionare entrambe le caselle e fare clic su Registra.



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



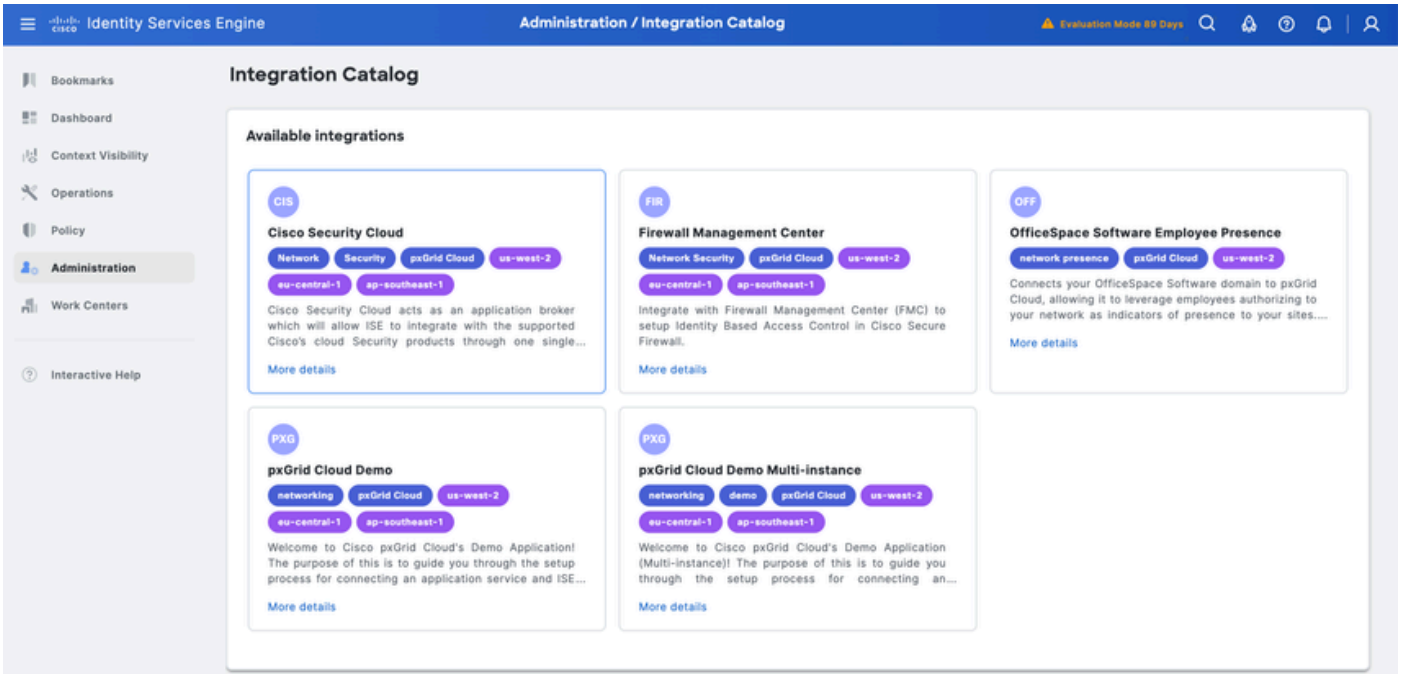
5 ISE mostrerà connected to Pxgrid Cloud.



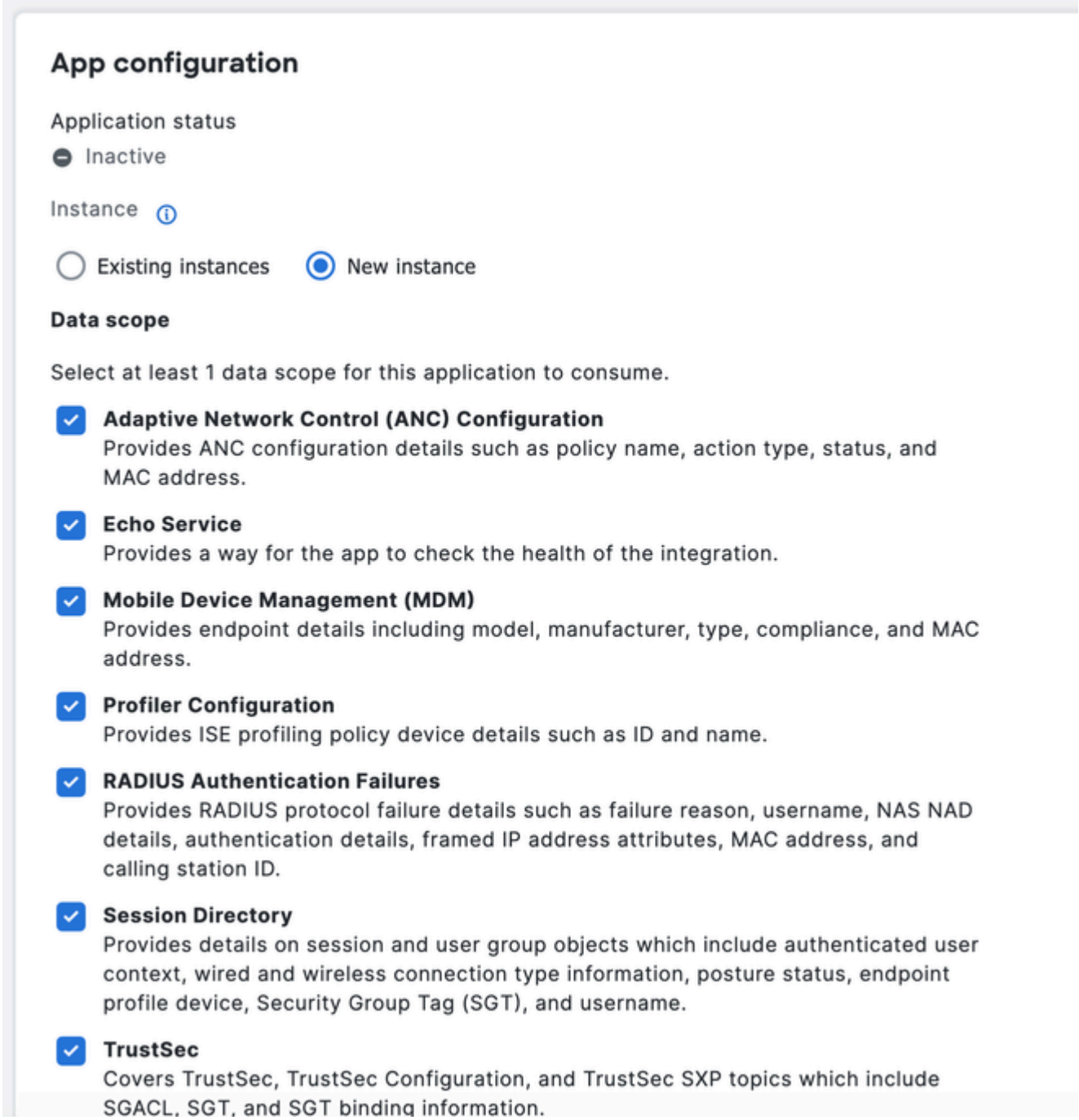
6 Fare clic sul collegamento Integration Catalog dal passo 5.

In Integrazioni disponibili fare clic su Cisco Security Cloud

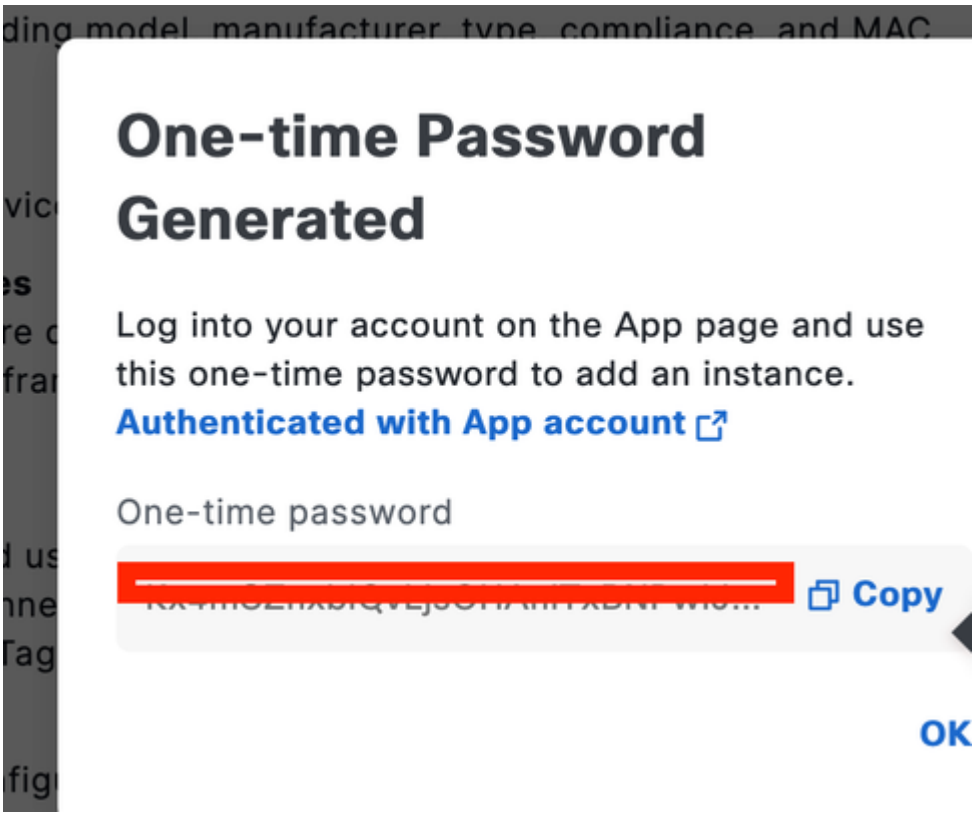
.



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

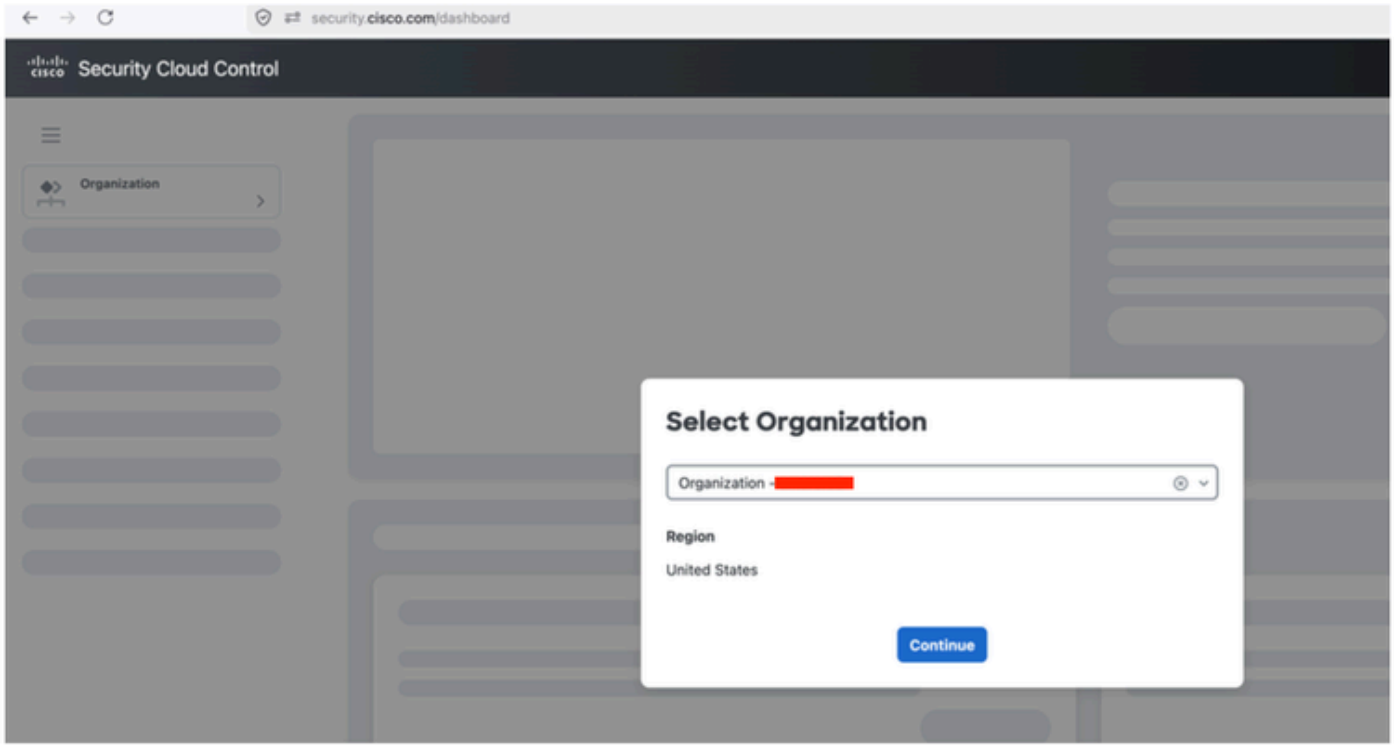


Copiare la password monouso come verrà utilizzata in Cisco Secure Access.

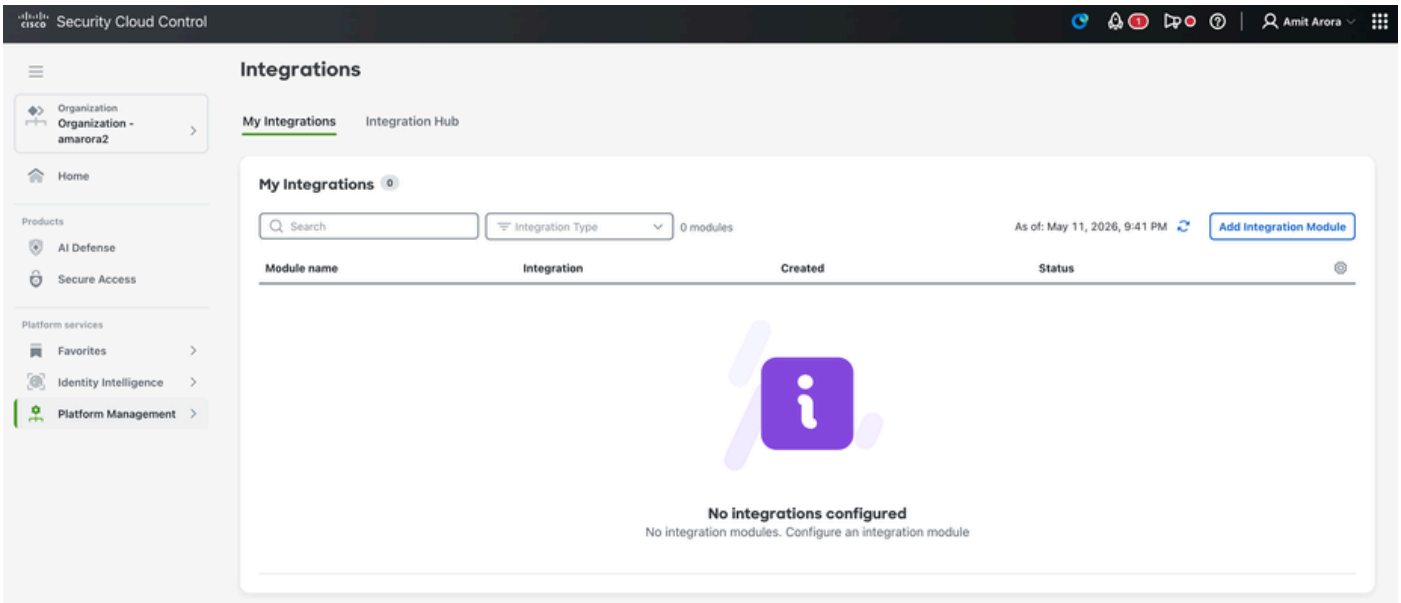


Fase 2: Integrazione di Cisco Secure Access con ISE

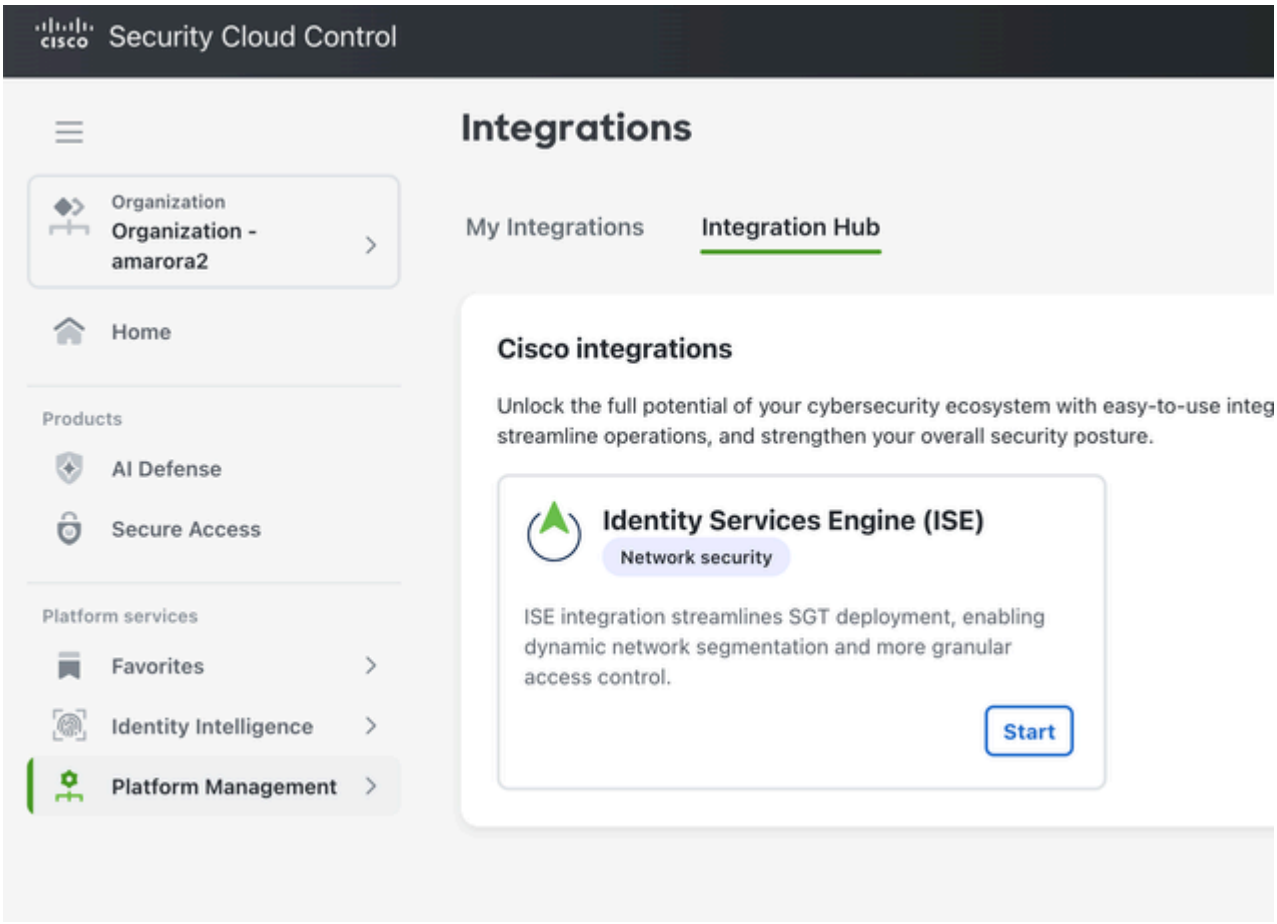
1. Accedere a security.cisco.com.
2. Selezionare Cisco Secure Access ORG



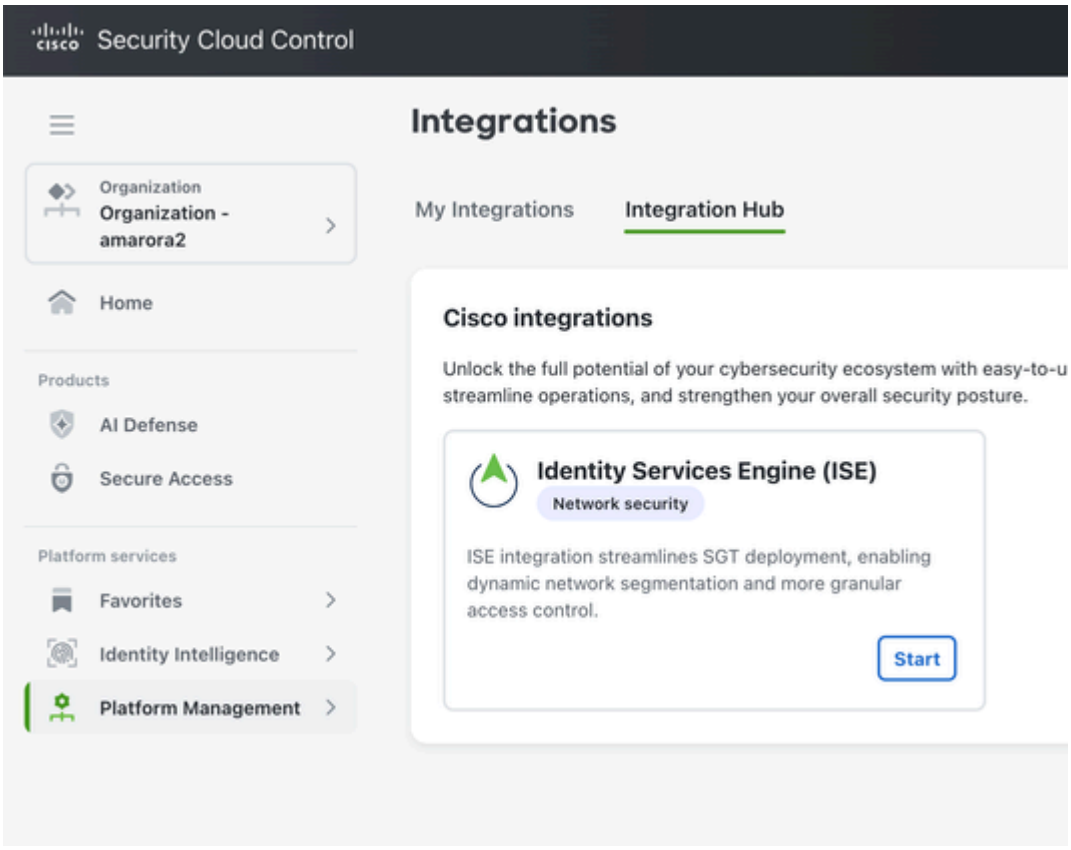
3 Fare clic su Platform Management - Platform Integration (Gestione piattaforma - Integrazioni della piattaforma)



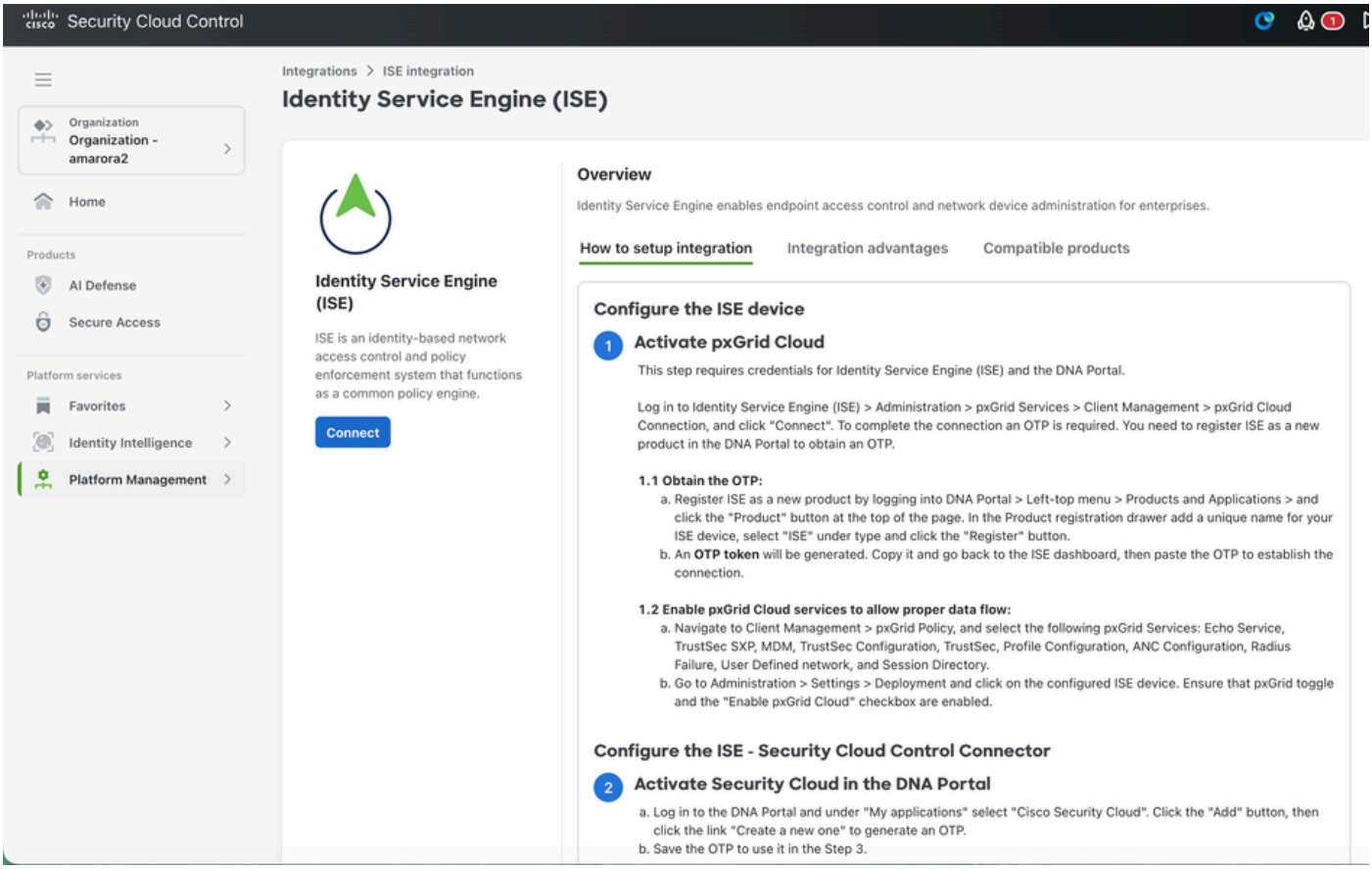
4 Fare clic su Add Integration Module



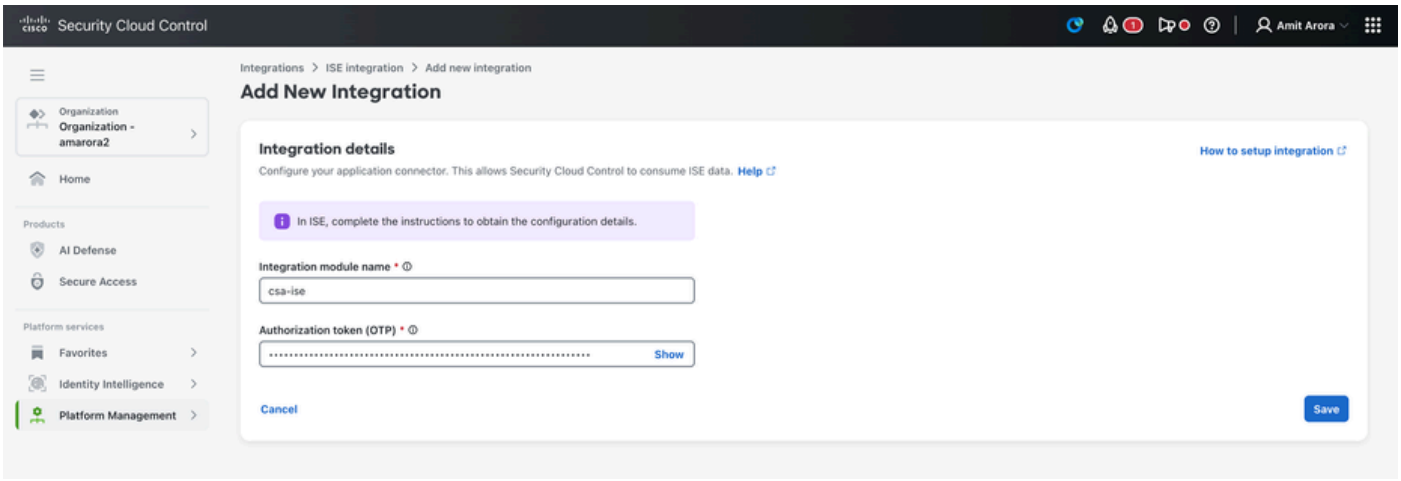
5 Fare clic su Start



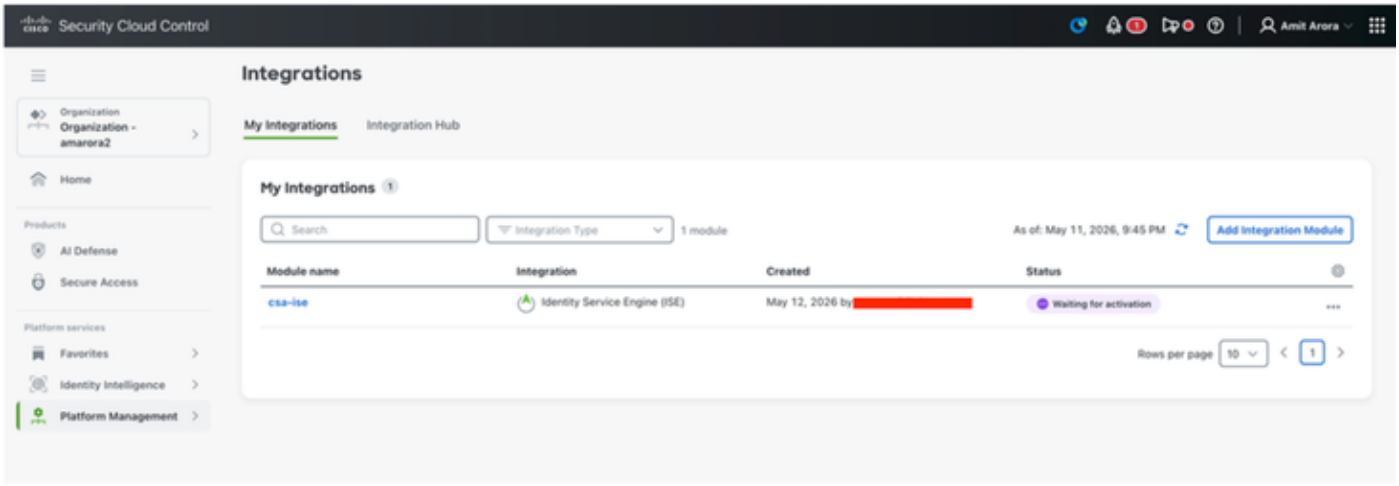
6 Fare clic su Connect



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



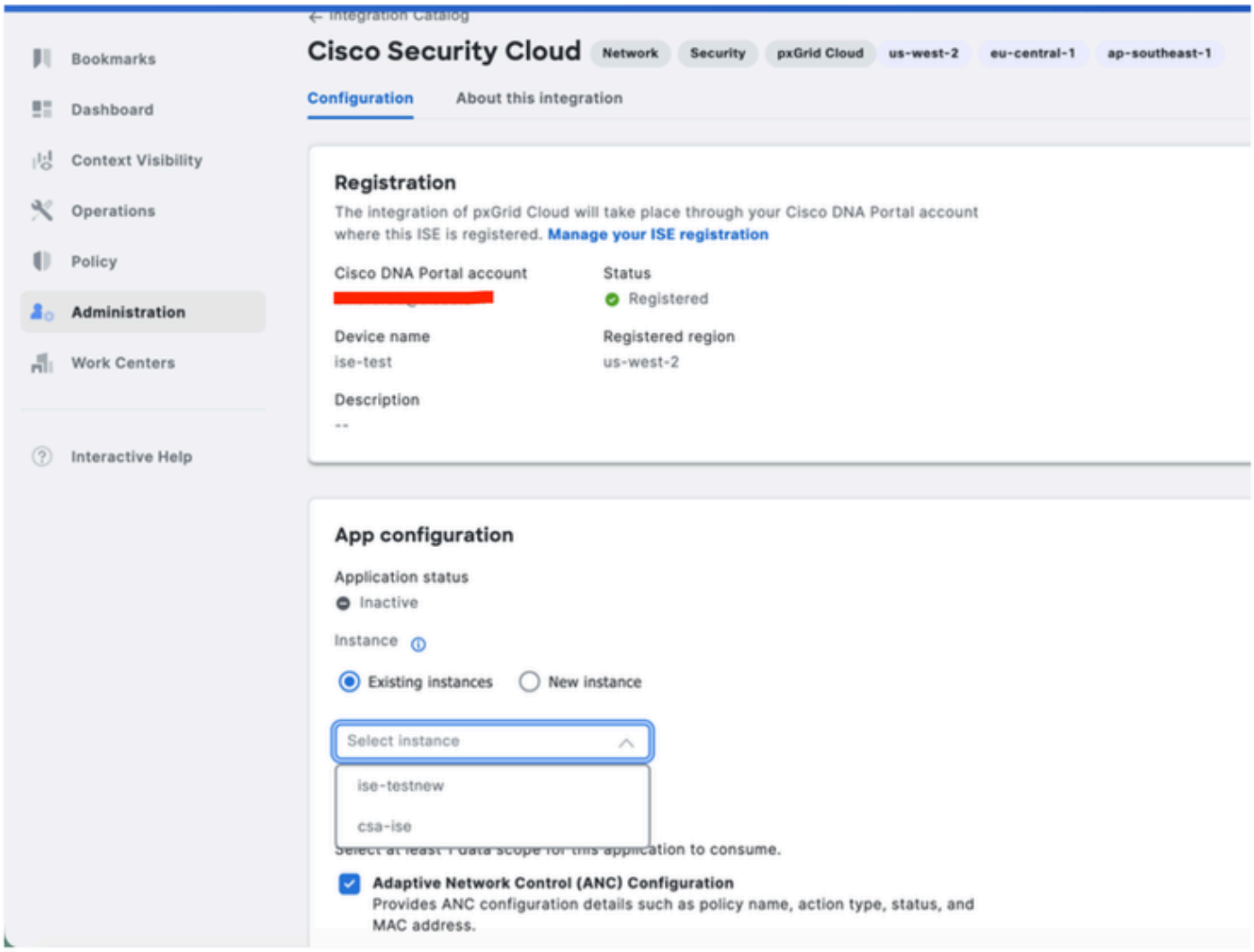
8 Facendo clic su Save (Salva), viene visualizzato Waiting for Activation Status (In attesa dello stato di attivazione).



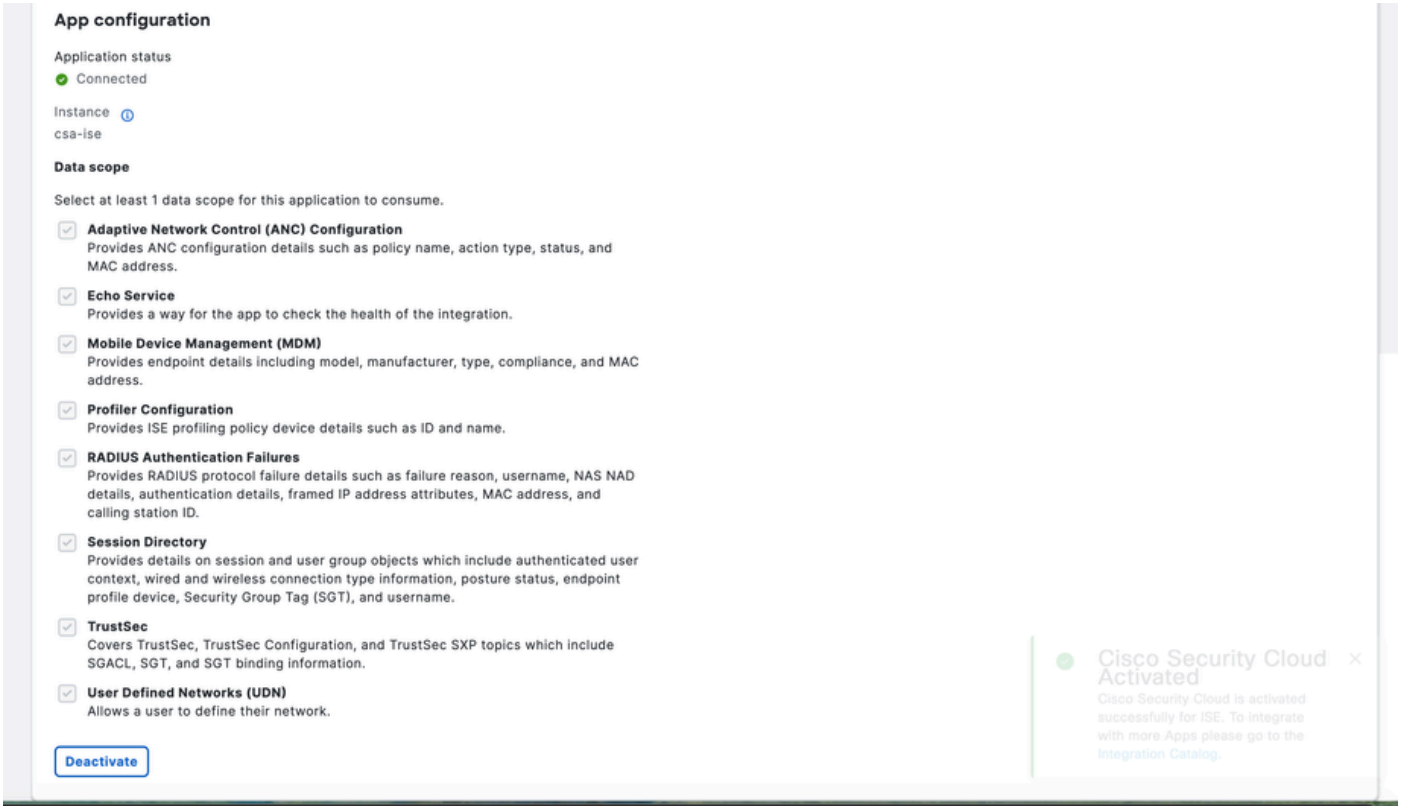
9 Accedere ad ISE e selezionare Administration - Deployment. Fare clic sul nodo con pxgrid personna. Fare clic su Integration cloud in Pxgrid Connection.

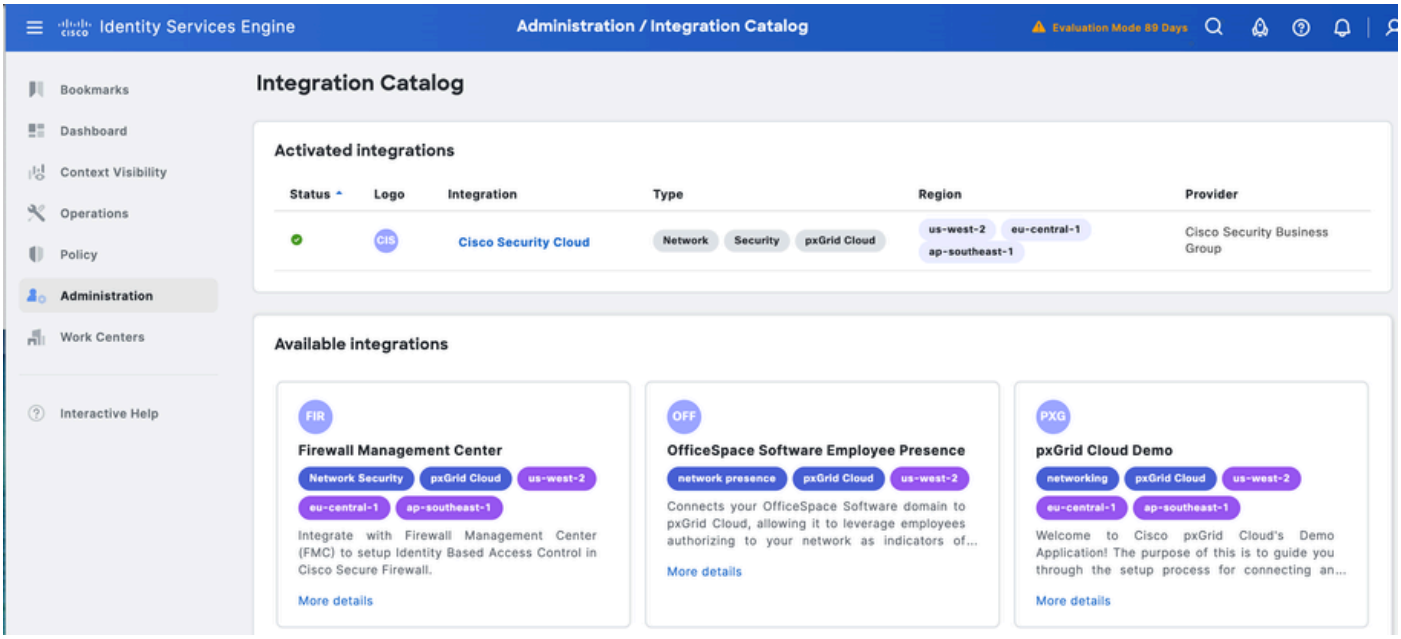
In Configurazione app - selezionare l'istanza ISE creata in Security Cloud Control e fare clic su

Attiva



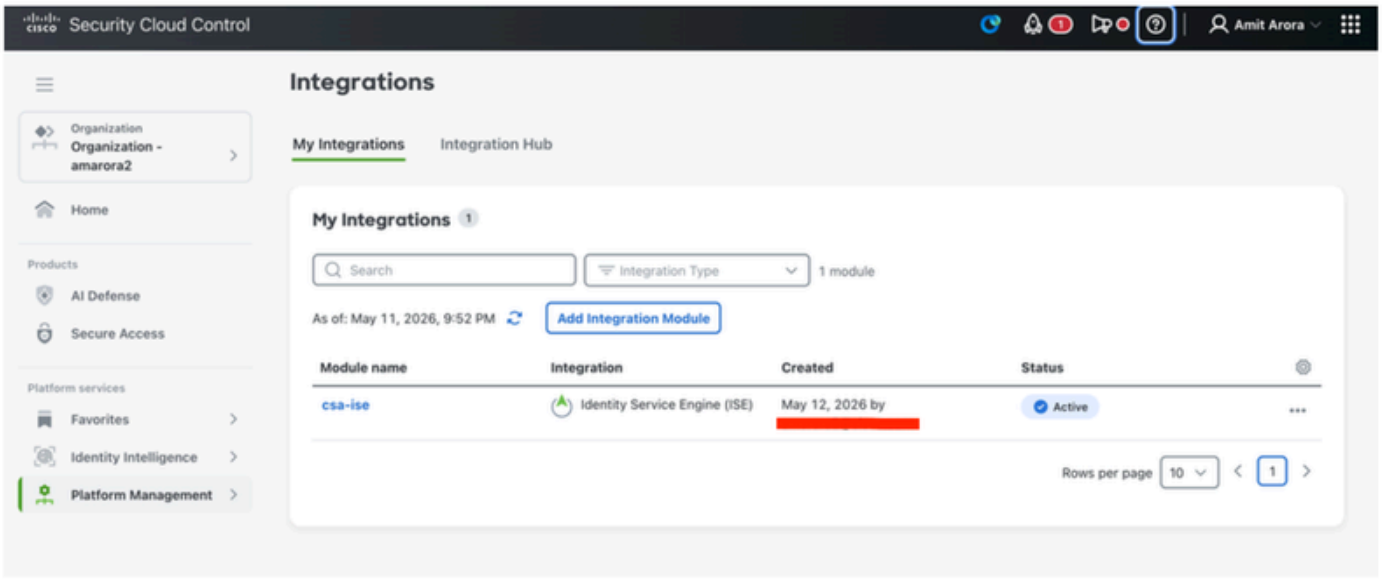
10 Lo stato dell'applicazione è connesso.





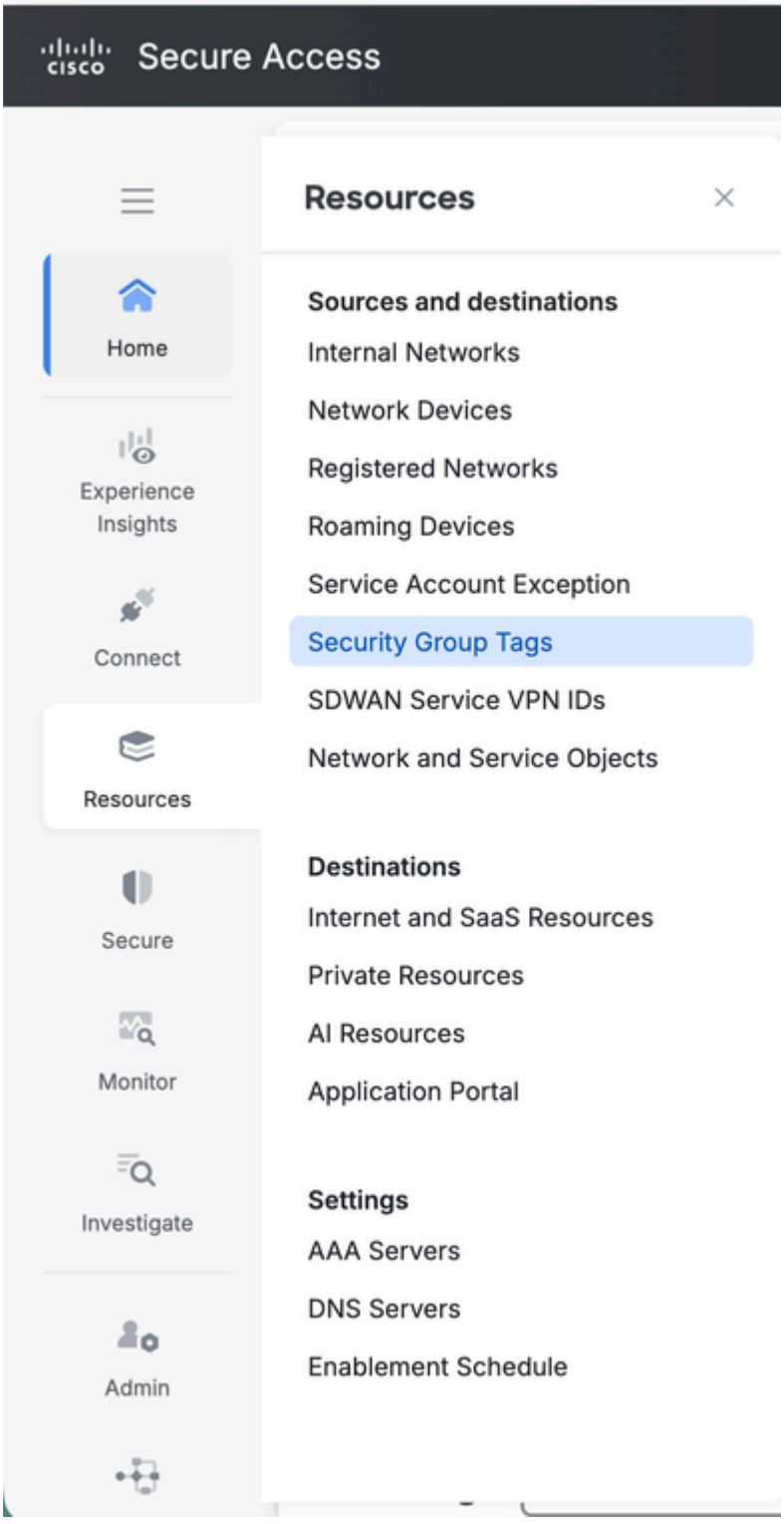
11 Accesso al controllo di Security Cloud - security.cisco.com

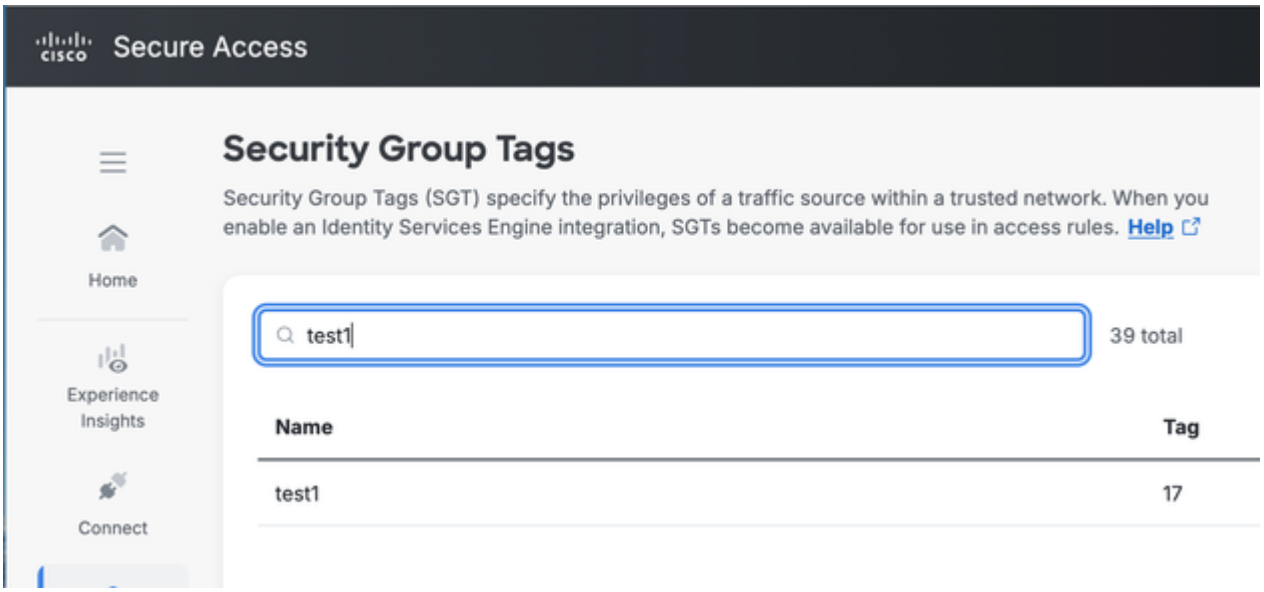
In Gestione piattaforma - Integrazioni di piattaforma è possibile visualizzare lo stato di integrazione come Attivo



Verifica tag gruppo di sicurezza:

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


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



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

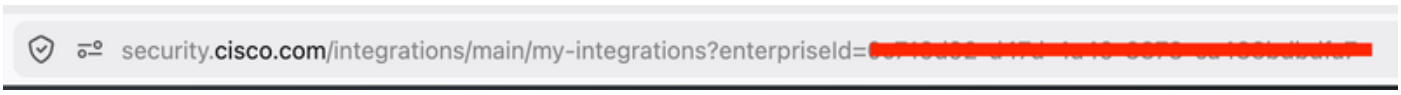
Infrastruttura

ERS

componente hermes a livello di debug.

SCC:

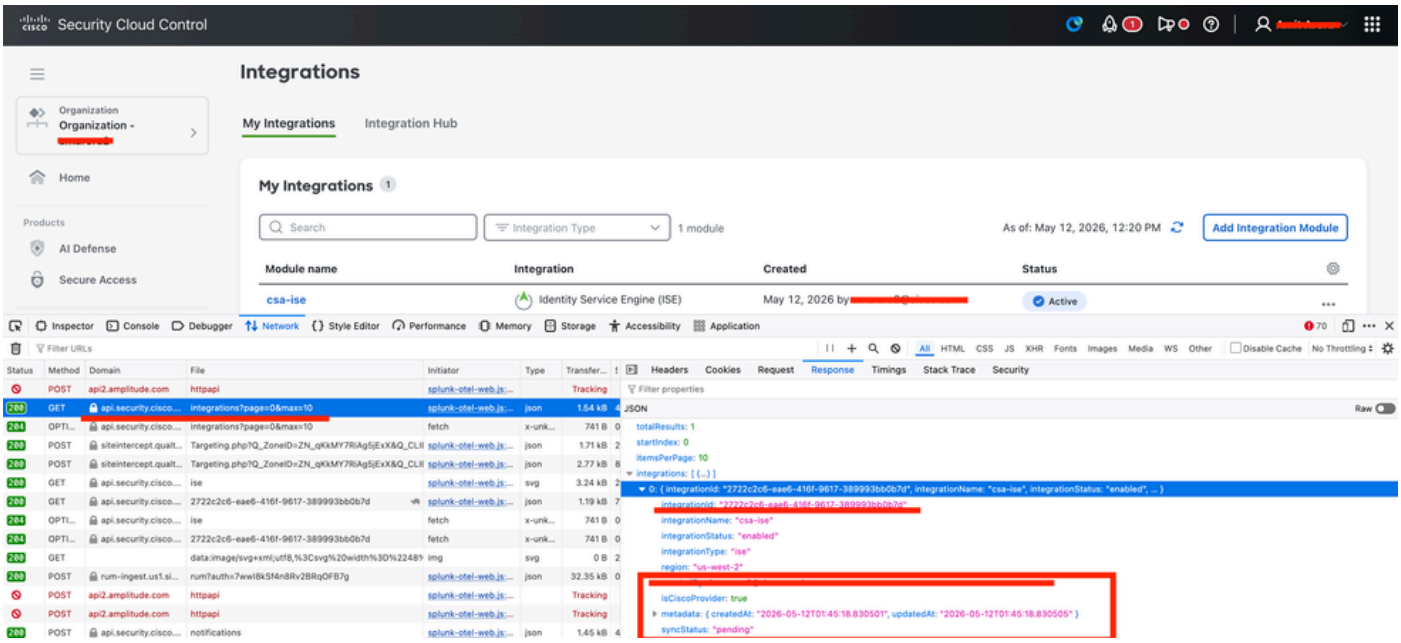
ID organizzazione: nell'URL di security.cisco.com



ID integrazione.
Avvia acquisizione HAR

Accedi a Security.cisco.com
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.



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).