

Cisco Secure Access-Integration mit ISE für Security Group Tag über PXGrid Cloud

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die gemeinsame Nutzung des Kontexts zwischen Cisco Secure Access und der Cisco Identity Services Engine aktivieren.

Anforderungen

Cisco empfiehlt, dass Sie folgende Themen kennen:

- Cisco Secure Access: Eine Cloud-basierte Security Service Edge (SSE)-Lösung, die einen nicht vertrauenswürdigen Netzwerkzugriff ermöglicht, sodass Benutzer von jedem Gerät aus auf das Internet und private Anwendungen zugreifen können.
- Cisco Identity Service Engine (ISE) Version 3.4 Patch 5.
- Cisco Security Cloud Control: Eine einheitliche Management-Lösung für Ihre Security Cloud-Produkte und -Identität. Security Cloud Control ist im Lieferumfang von Secure Access enthalten.

Hintergrund

Diese Integration ermöglicht die automatisierte Erstellung zuverlässiger Tunnel von Catalyst SD-WAN-Zweigstellen zu Cisco Secure Access, wodurch der nahtlose Austausch von VPN-ID/Name und SGT-Kontext vereinfacht wird.

Die Cisco Identity Services Engine (ISE) bleibt die zentrale Behörde für die Konfiguration und Verwaltung des SGT. Alle in der ISE durchgeführten Updates werden automatisch mit Cisco Secure Access synchronisiert. Wenn ein SGT gelöscht wird, bleiben die bestehenden Regeln, die auf das SGT verweisen, aktiv, um sicherzustellen, dass der Datenverkehrsabgleich wie erwartet fortgesetzt wird.

Wir bieten derzeit eine eingeschränkte Verfügbarkeit für SGT-Zuordnungen an. Dadurch wird die Unterstützung erweitert, sodass SGT-Zielobjekte in Ihre Sicherheitsregeln aufgenommen werden

können. Darüber hinaus wird in Kürze Unterstützung für den Aufbau von SASE-Tunneln mit SGT von Meraki und der Cisco Secure Firewall verfügbar sein.

Anwendungsfall:

SGT-Namensraum-basierte Richtlinie:

Als Sicherheitsadministrator möchte das Kit eine fortlaufende Mikrosegmentierung mithilfe des SGT von der Onprem ISE für privaten und Internet-basierten Datenverkehr durchsetzen. Die Möglichkeit zum Importieren von SGT zum Anwenden von Richtlinien.



Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

- Identity Service Engine (ISE) Version 3.4 Patch 5
- Sicherer Zugriff
- Cisco Security-Cloud

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurationsübersicht für die Kontextfreigabe

- Verbinden der ISE mit der Cisco Security Cloud
- Cisco Secure Access mit der ISE verbinden

Konfigurieren

In diesem Leitfaden wird die allgemeine Konfiguration in die folgenden Hauptschritte unterteilt:

1. Verbinden der Cisco ISE mit der Cisco Security Cloud
2. Sicherer Zugriff von Cisco auf die Cisco ISE
3. Sicherheitsgruppen-Tags in Cisco Secure Access

Vorbereitungen

- Stellen Sie sicher, dass Sie die Advantage-Lizenz in Ihrer Cisco ISE-Bereitstellung installiert und aktiviert haben.
- Der DNA Cloud-Agent stellt eine ausgehende HTTPS-Verbindung zur Cisco DNA Cloud her. Daher müssen Sie die Cisco ISE-Proxyeinstellungen konfigurieren, wenn Ihr Netzwerk einen Proxy verwendet, um das Internet zu erreichen. Um die Proxyeinstellungen in der Cisco ISE zu konfigurieren, navigieren Sie zu **Administration > System > Settings > Proxy**
- Stellen Sie sicher, dass Port 443 für ausgehende Verbindungen von der Cisco ISE zum Cisco pxGrid Cloud-Portal geöffnet ist. Wenn Firewall- oder Proxy-Einstellungen konfiguriert sind, stellen Sie sicher, dass die folgenden URLs nicht blockiert werden:

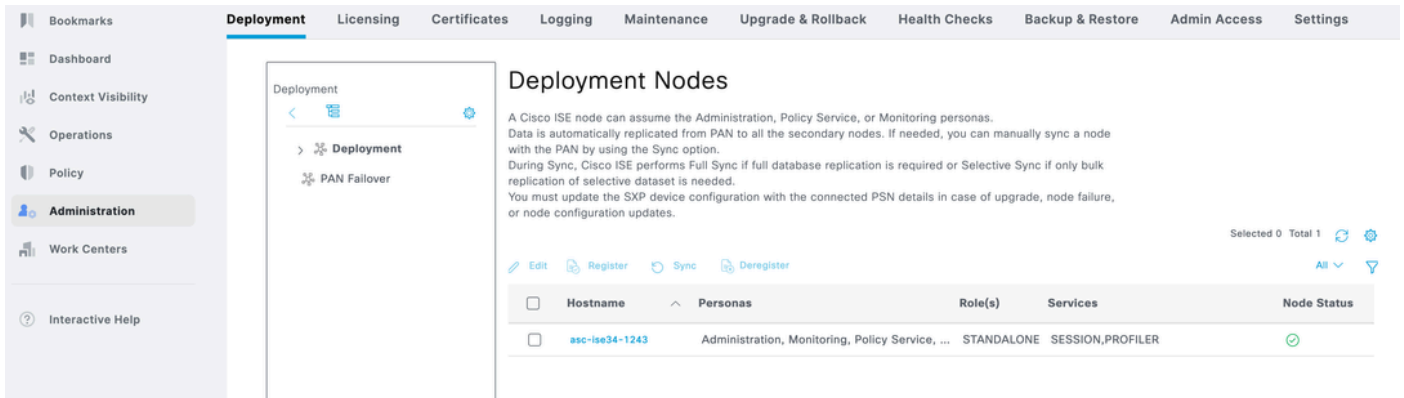
<https://dna.cisco.com>

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

Schritt 1: Aktivieren von Pxgrid Cloud auf der ISE

1 Navigieren Sie zur ISE-GUI.

2 Klicken Sie auf Administration - Deployment.

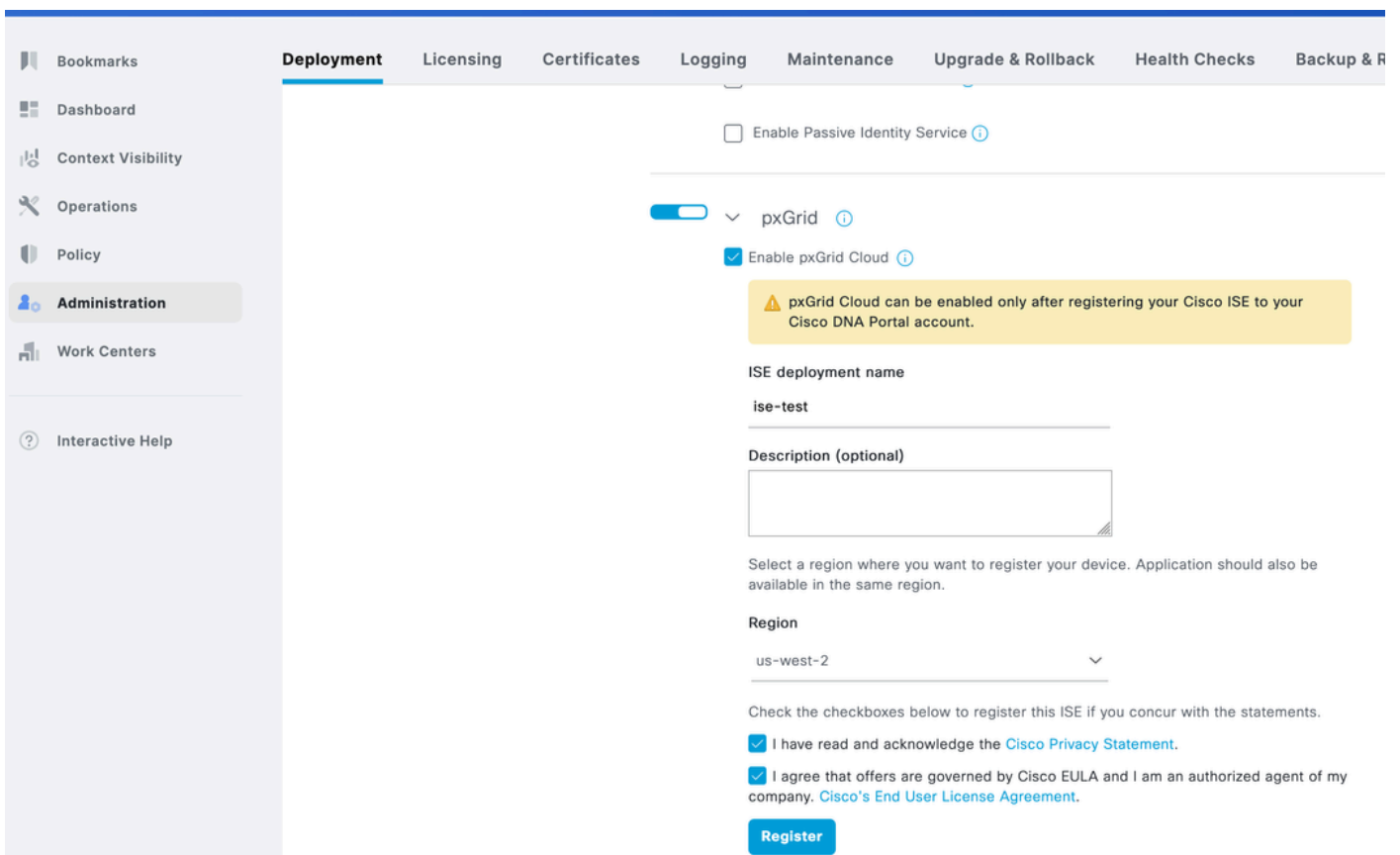


3 Klicken Sie auf den Knoten und scrollen Sie nach unten.

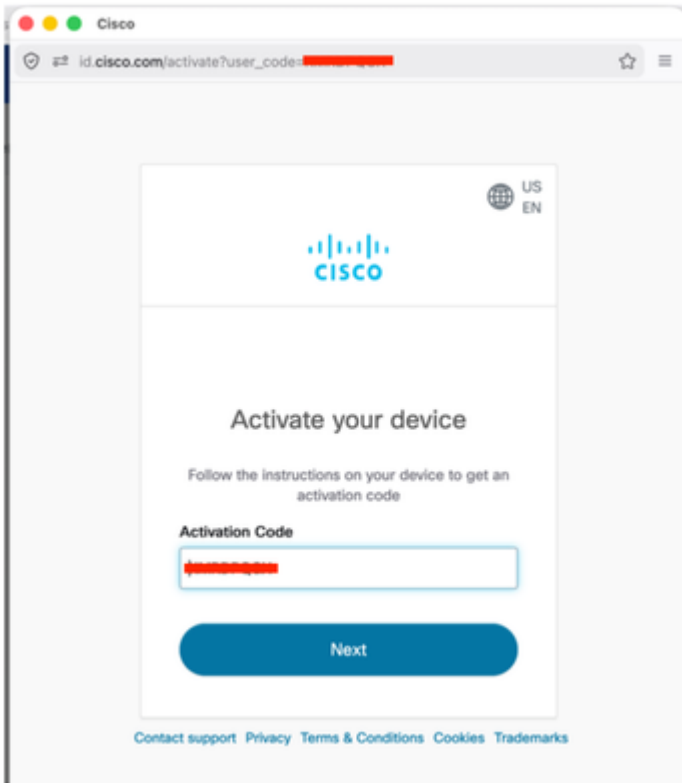
ISE-Bereitstellungsname eingeben

Wählen Sie die Region als US West 2 aus. Dies ist die einzige derzeit unterstützte Region.

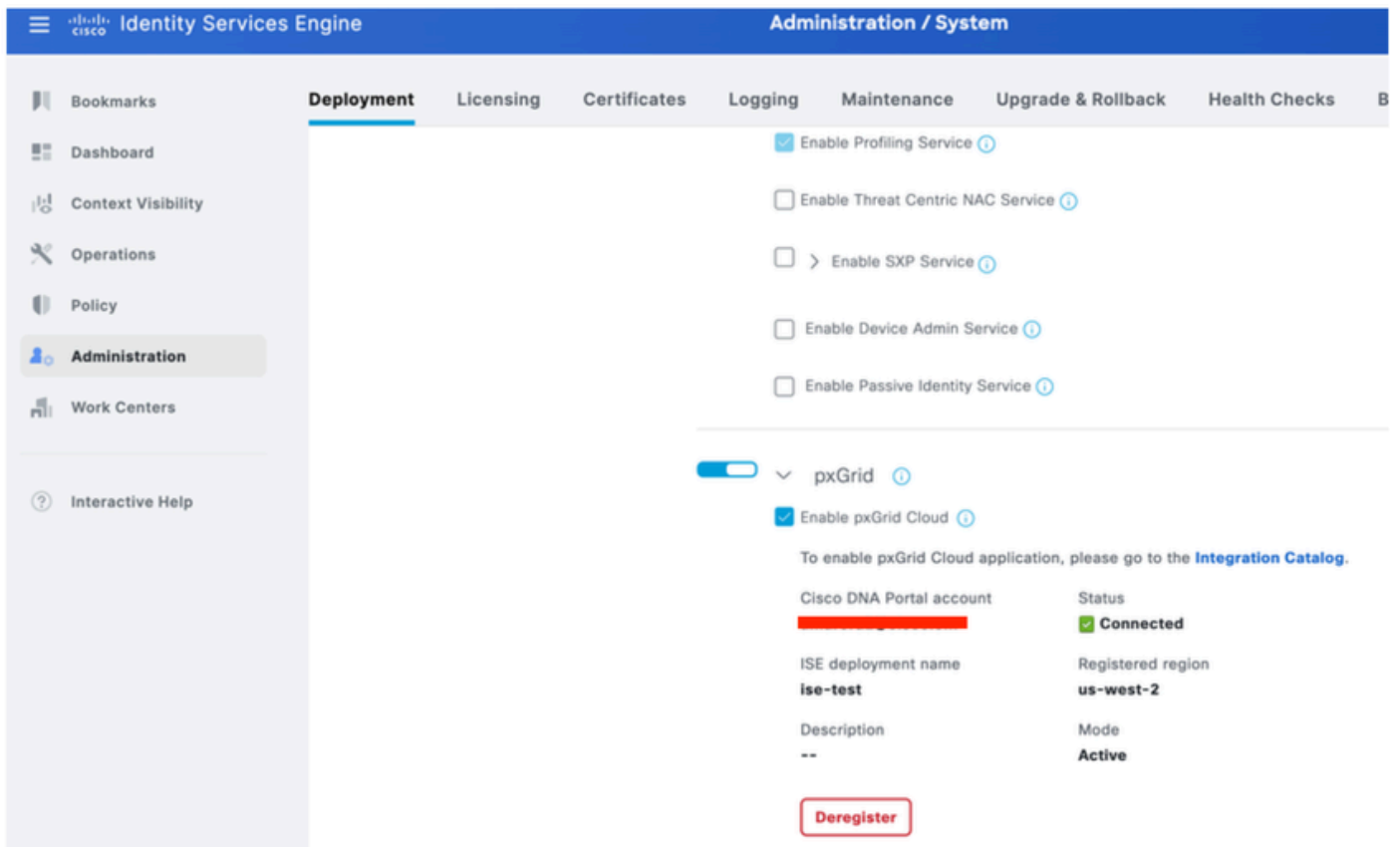
Aktivieren Sie beide Kontrollkästchen, und klicken Sie auf Registrieren.



4 Ein Popup mit automatisch ausgefülltem Aktivierungscode wird angezeigt. Klicken Sie auf "Weiter",

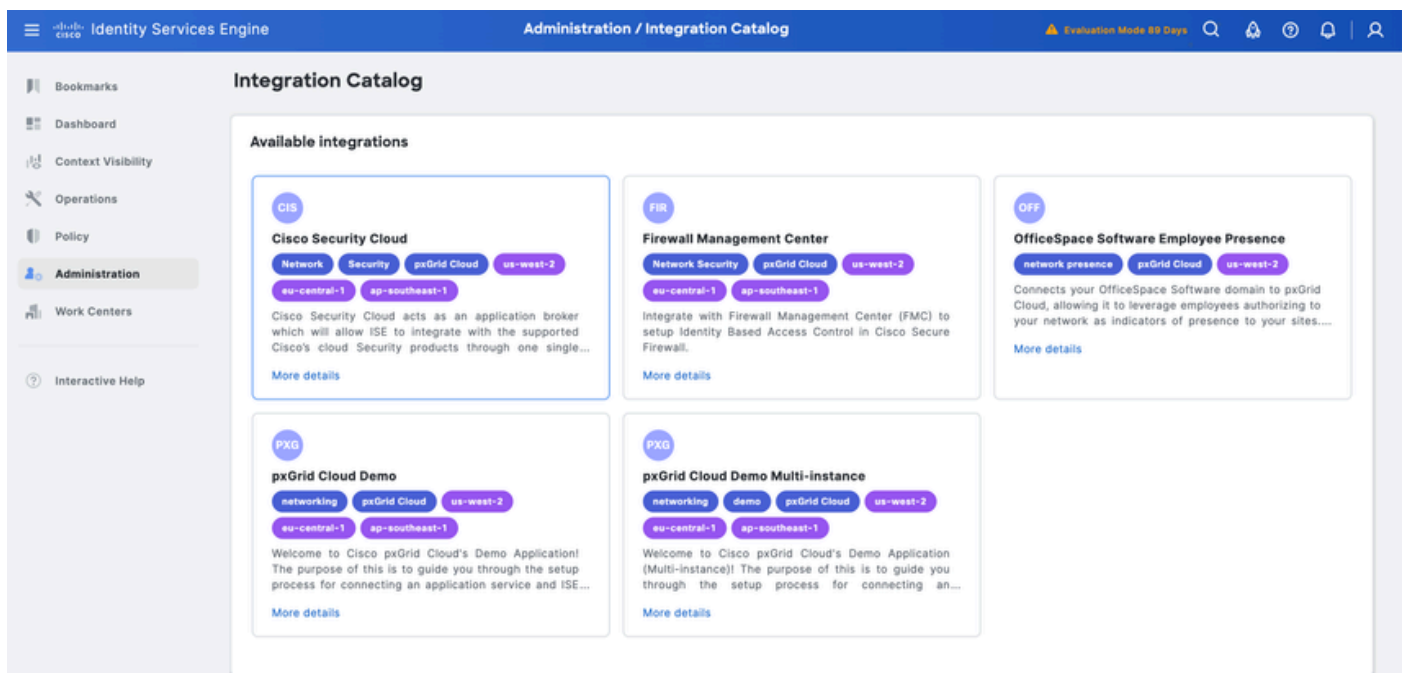


5 Die ISE zeigt die Verbindung zur Pxgrid Cloud an.



6 Klicken Sie in Schritt 5 auf den Link Integrationskatalog.

Klicken Sie unter Verfügbare Integrationen auf Cisco Security Cloud.



7 Klicken Sie unter App-Konfiguration auf Neue Instanz und dann auf Aktivieren.

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.

Kopieren Sie das einmalige Kennwort so, wie es in Cisco Secure Access verwendet wird.

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](#) ↗

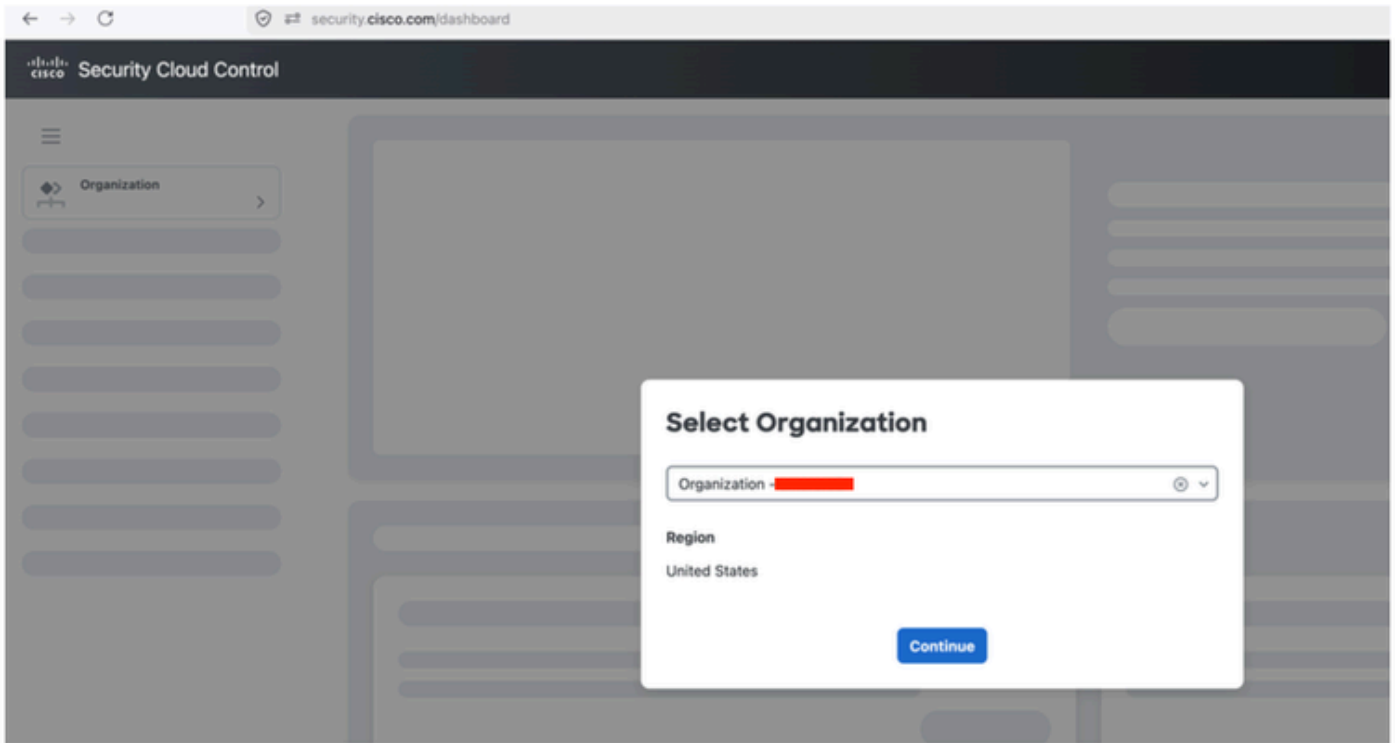
One-time password

[REDACTED] [Copy](#)

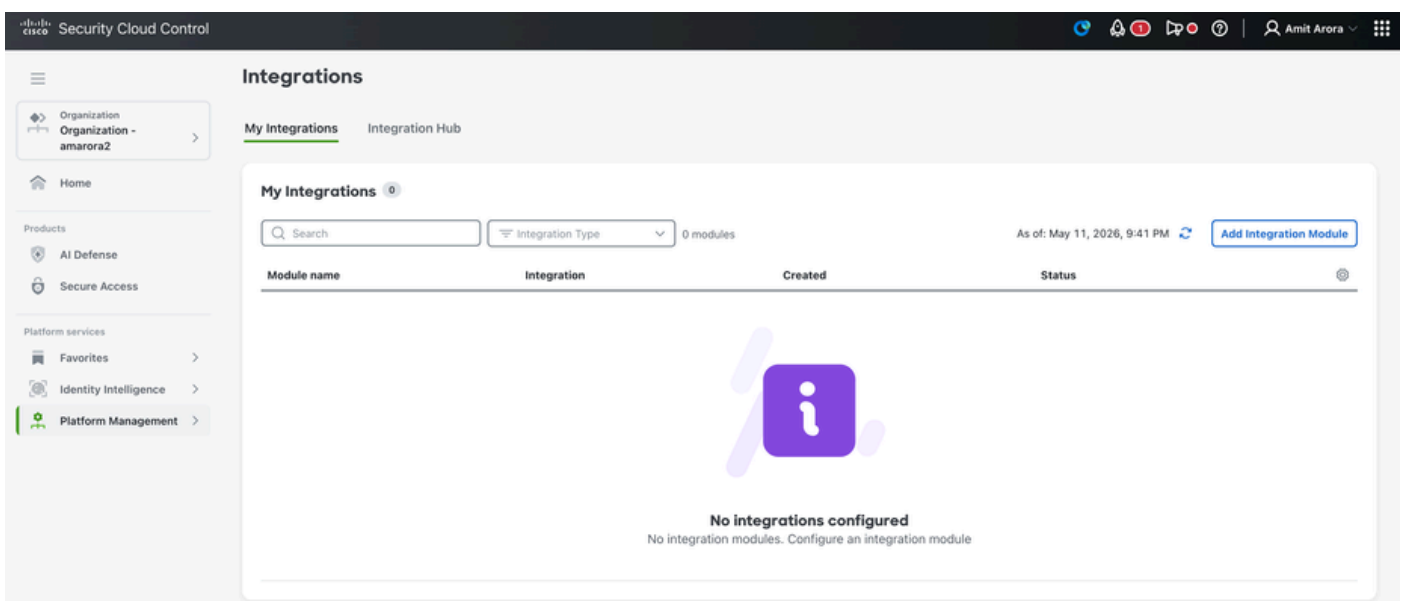
[OK](#)

Schritt 2: Integration von Cisco Secure Access mit der ISE

1. Melden Sie sich unter security.cisco.com an.
2. Cisco Secure Access ORG auswählen



3 Klicken Sie auf Plattformmanagement - Plattformintegration.



4 Klicken Sie auf Integration hinzufügen

Security Cloud Control

Integrations

My Integrations Integration Hub

Cisco integrations

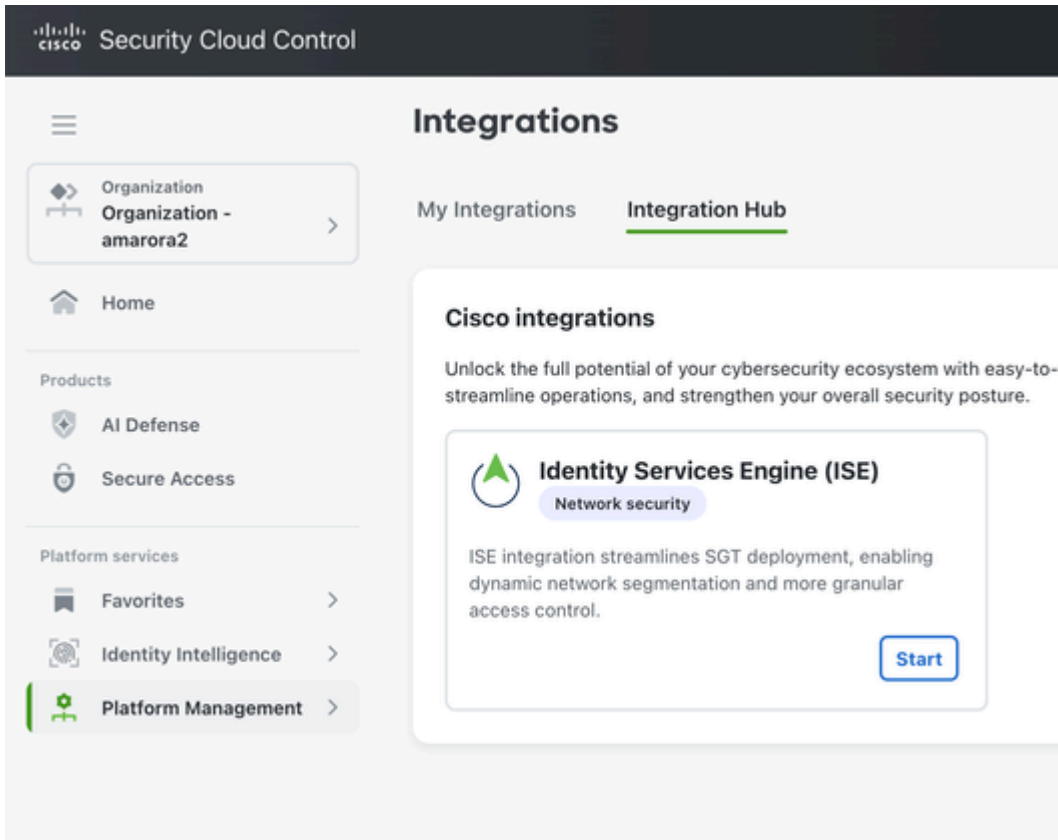
Unlock the full potential of your cybersecurity ecosystem with easy-to-use integ streamline operations, and strengthen your overall security posture.

Identity Services Engine (ISE)
Network security

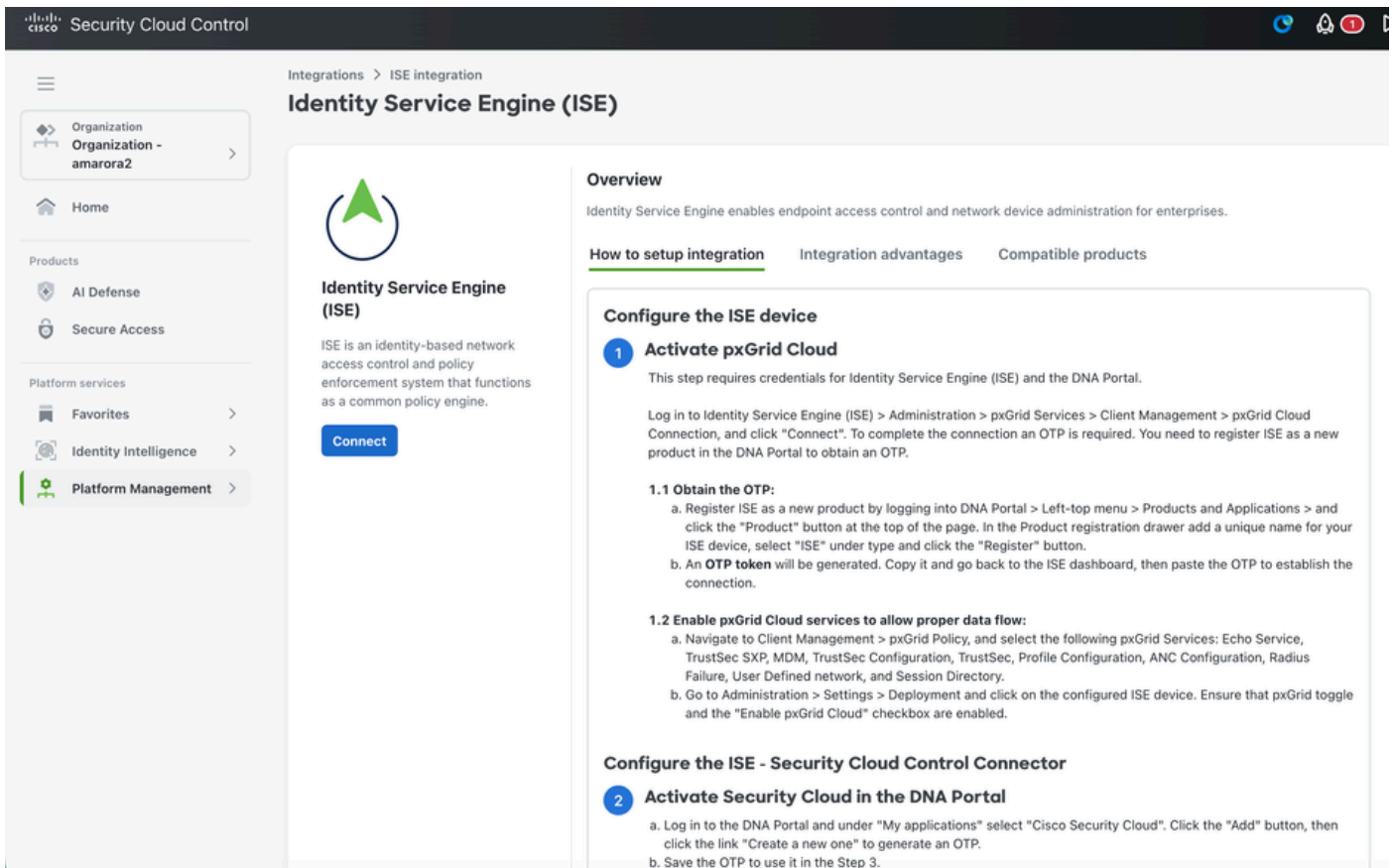
ISE integration streamlines SGT deployment, enabling dynamic network segmentation and more granular access control.

[Start](#)

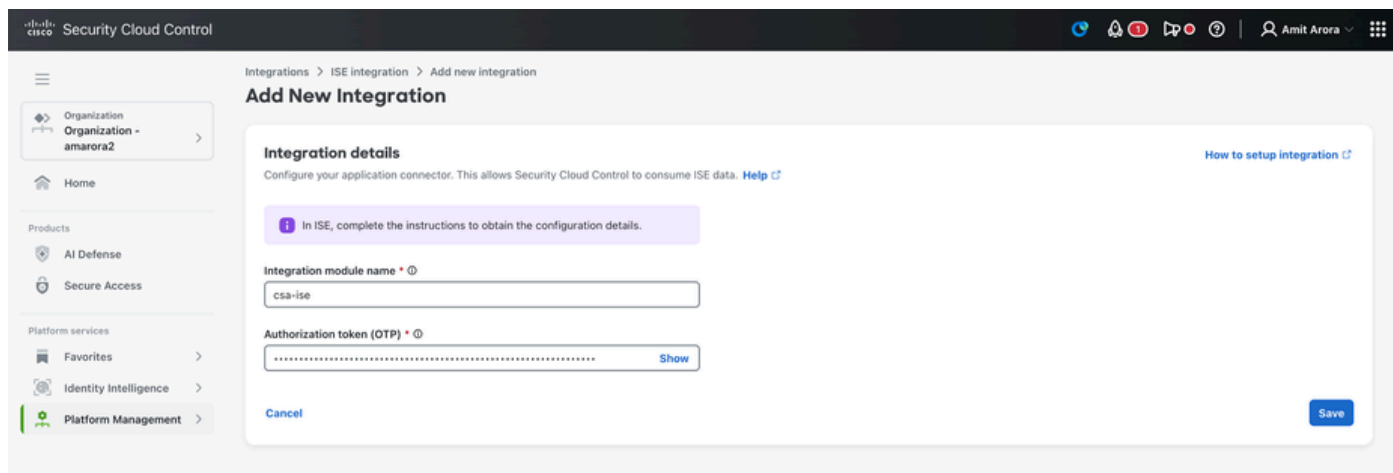
5 Klicken Sie auf Start



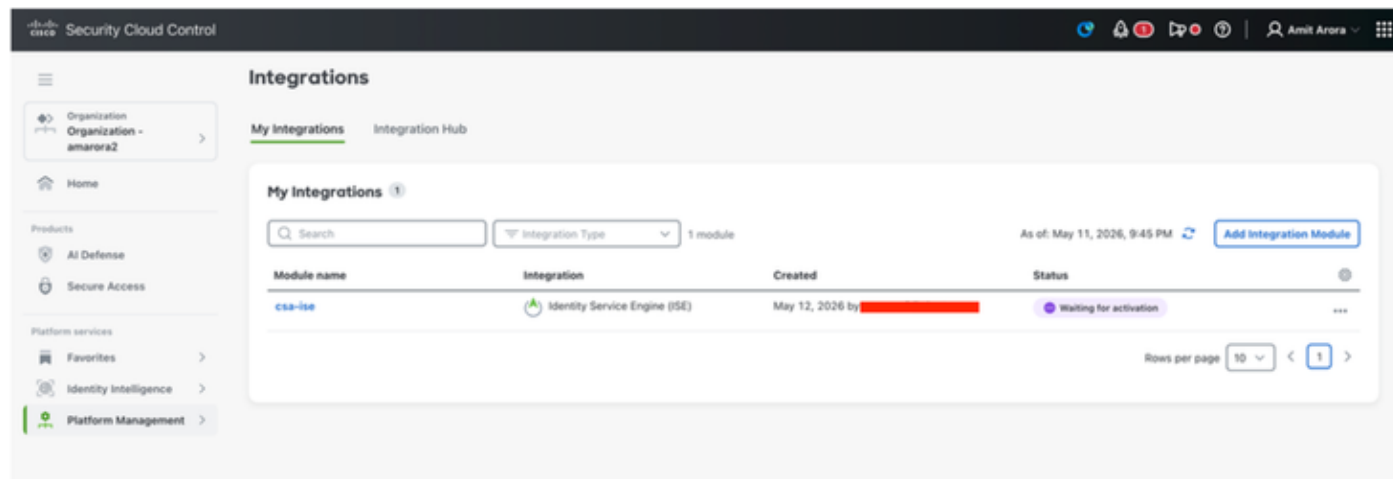
6 Klicken Sie auf Verbinden



7. Geben Sie den Namen des Integrationsmoduls und OTP von der Cisco ISE ein, und klicken Sie auf Speichern.



8 Sobald Sie auf Speichern geklickt haben, wird Wartet auf Aktivierungsstatus angezeigt.



9 Melden Sie sich bei der ISE an, und navigieren Sie zu Administration - Deployment. Klicken Sie auf den Knoten mit pxgrid persona - klicken Sie auf Integration Cloud unter Pxgrid Connection.

Wählen Sie unter Anwendungskonfiguration die ISE-Instanz aus, die auf Security Cloud Control

erstellt wurde, und klicken Sie auf Aktivieren.

The screenshot displays the Cisco Security Cloud interface for configuring the pxGrid Cloud integration. 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'. Below these are 'Configuration' and 'About this integration' tabs.

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 Anwendungsstatus ist jetzt verbunden.

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
Connected	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 Anmeldung bei Security Cloud Control - security.cisco.com

Unter Plattformverwaltung - Plattformintegrationen wird der Integrationsstatus als aktiv angezeigt.

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 >

Sicherheitsgruppen-Tag überprüfen:

Melden Sie sich bei Cisco Secure Access an. Navigieren Sie zu Ressourcen - Sicherheitsgruppen-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

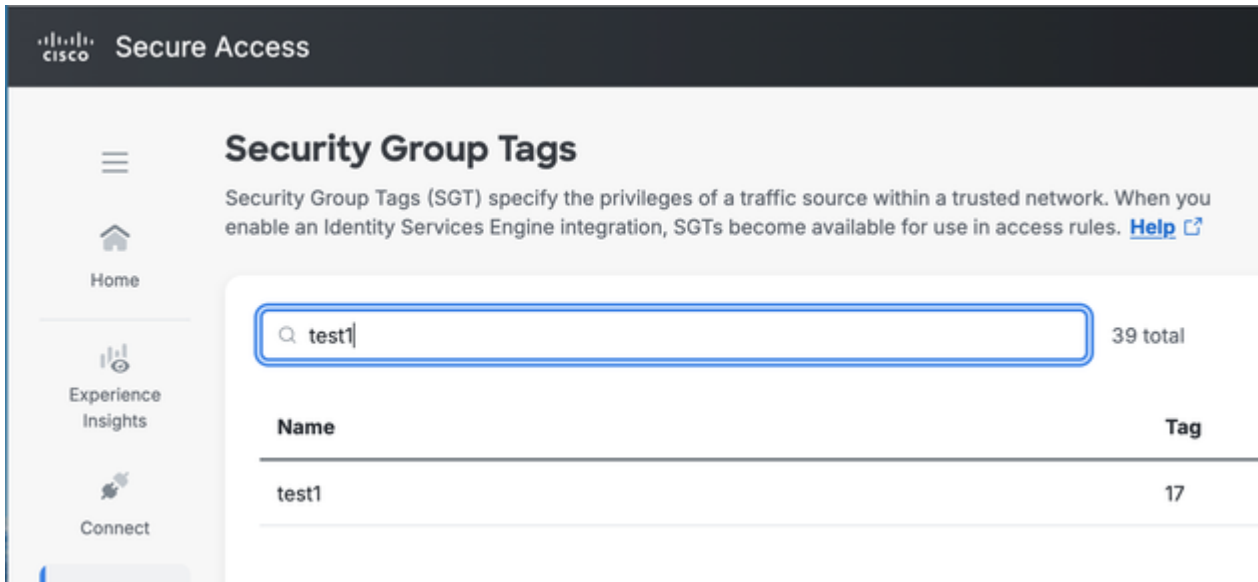
Application Portal

Settings

AAA Servers

DNS Servers

Enablement Schedule



Erforderliche Informationen für das Cisco TAC

ISE:

[So sammeln Sie das ISE-Supportpaket](#) mit den folgenden Komponenten, für die auf "Debug Level" (Debugstufe) auf dem ISE-Knoten mit Pxgrid Personan festgelegt wurde:

pxgrid

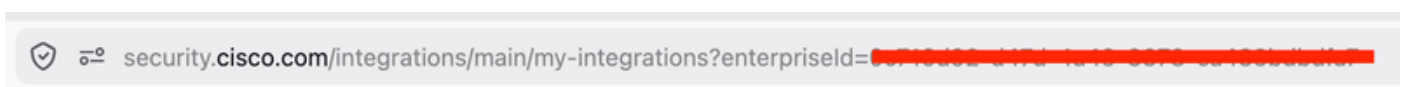
Infrastruktur

ERS

hermes-Komponente auf Debugebene.

SCC:

Unternehmens-ID: in the URL of security.cisco.com



Integrations-ID. [HAR-Erfassung](#) starten

Melden Sie sich unter Security.cisco.com an.
Navigieren Sie zu Plattformmanagement - Plattformintegration.

Suchen Sie nach Integrationen? Seite API-Anruf und in Antwort Registerkarte finden Sie eine Integrations-ID.

The screenshot displays the Cisco Security Cloud Control interface. The top navigation bar includes the Cisco logo and the text "Security Cloud Control". The main content area is titled "Integrations" and shows "My Integrations" with a search bar and a filter for "Integration Type" set to "1 module". A table lists the integrations:

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

Below the integrations list, the "Inspector" tab is active, showing a network request. The request details include:

- Method: GET
- Domain: api.security.cisco.com
- File: integrations?page=0&max=10
- Initiator: splunk-otel-web.js...
- Type: json
- Transfer: 1.54 kB
- Response: JSON

The response body is expanded to show the following JSON data:

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

The "metadata" field in the response is highlighted with a red box:

```
metadata: { createdAt: "2026-05-12T01:45:18.830501", updatedAt: "2026-05-12T01:45:18.830505" }
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.