

Integration von Cloud-basiertem Firewall Management Center mit ISE via pxGrid Cloud

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Cisco pxGrid Cloud-Terminologie](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Cisco pxGrid Cloud-Serverzertifikat in ISE importieren](#)

[Flussdiagramm](#)

[Registrierung der ISE beim Catalyst Cloud Portal](#)

[Aktivieren der cdFMC-Anwendung auf der ISE mithilfe des Integrationskatalogs](#)

[pxGrid-Anwendungsinstanz \(cdFMC\) erstellen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[ISE-Registrierung und -Anwendung Aktivierungsablauf](#)

[Einschränkungen](#)

[Referenzen](#)

Einleitung

In diesem Dokument wird das Verfahren zur Integration der Cisco ISE in das Cloud-basierte Firewall Management Center (cdFMC) über pxGrid Cloud beschrieben.

Voraussetzungen

- Umfassende Kenntnisse der Cisco Identity Service Engine (ISE)
- Ein Konto im Cisco Catalyst Cloud Portal
- Ein Konto im Cisco Security Cloud Control Portal

Anforderungen

- Installieren und aktivieren Sie die Advantage-Lizenzstufe in Ihrer Cisco ISE-Bereitstellung.
- Der pxGrid Cloud-Agent erstellt eine ausgehende HTTPS-Verbindung mit der Cisco pxGrid Cloud. Konfigurieren Sie daher die Cisco ISE-Proxyeinstellungen, wenn das Netzwerk einen Proxy verwendet, um das Internet zu erreichen. Um die Proxyeinstellungen in der Cisco ISE

zu konfigurieren, wählen Sie Administration > System > Settings > Proxy aus.

- Der vertrauenswürdige Zertifikatsspeicher der Cisco ISE muss das Zertifikat der Stammzertifizierungsstelle enthalten, das zur Validierung des von Cisco pxGrid Cloud bereitgestellten Serverzertifikats erforderlich ist. Stellen Sie sicher, dass die Option Trust for Authentication of Cisco Services für dieses Stammzertifikat der Zertifizierungsstelle aktiviert ist. Um die Vertrauenswürdigkeit für die Authentifizierung von Cisco Services zu aktivieren, wählen Sie Administration > System > Certificates (Verwaltung > System > Zertifikate).
- 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 diese URLs nicht blockiert werden.

<https://dna.cisco.com>

<https://dnaservices.cisco.com>

<https://ciscodnacloud.com>

Verwendete Komponenten

ISE-Softwareversion: 3.4 Patch 1, Bereitstellung von 4 Knoten (PAN, SAN und 2 PSN mit aktiviertem pxGrid-Service)

cdFMC-Version: 20241127

Version von Cisco Firepower Threat Defense (FTD) für VMware: 7.2.5

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.

Cisco pxGrid Cloud-Terminologie

Im Folgenden sind einige der gebräuchlichen Begriffe aufgeführt, die in der Cisco pxGrid Cloud-Lösung verwendet werden, und ihre Bedeutung in der Cisco pxGrid Cloud-Umgebung:

- Angebot: Eine Reihe von Funktionen in einem Paket als Lösung angeboten
- Abonnement: Ein Beispiel für ein Angebot, das von einem Tenant genutzt wird, ist ein Abonnement
- Anwendung: Je nach Ihren Anforderungen können Sie Anwendungen für Ihr Produkt erstellen und registrieren.

Hintergrundinformationen

Die Cisco ISE ermöglicht die gemeinsame Nutzung des Kontexts durch mehrere Anbieter von Sicherheitslösungen. Die aktuelle Architektur lässt jedoch keine Kommunikation zwischen der standortbasierten ISE und Cloud-basierten Lösungen über den Netzwerkperimeter zu, ohne dass

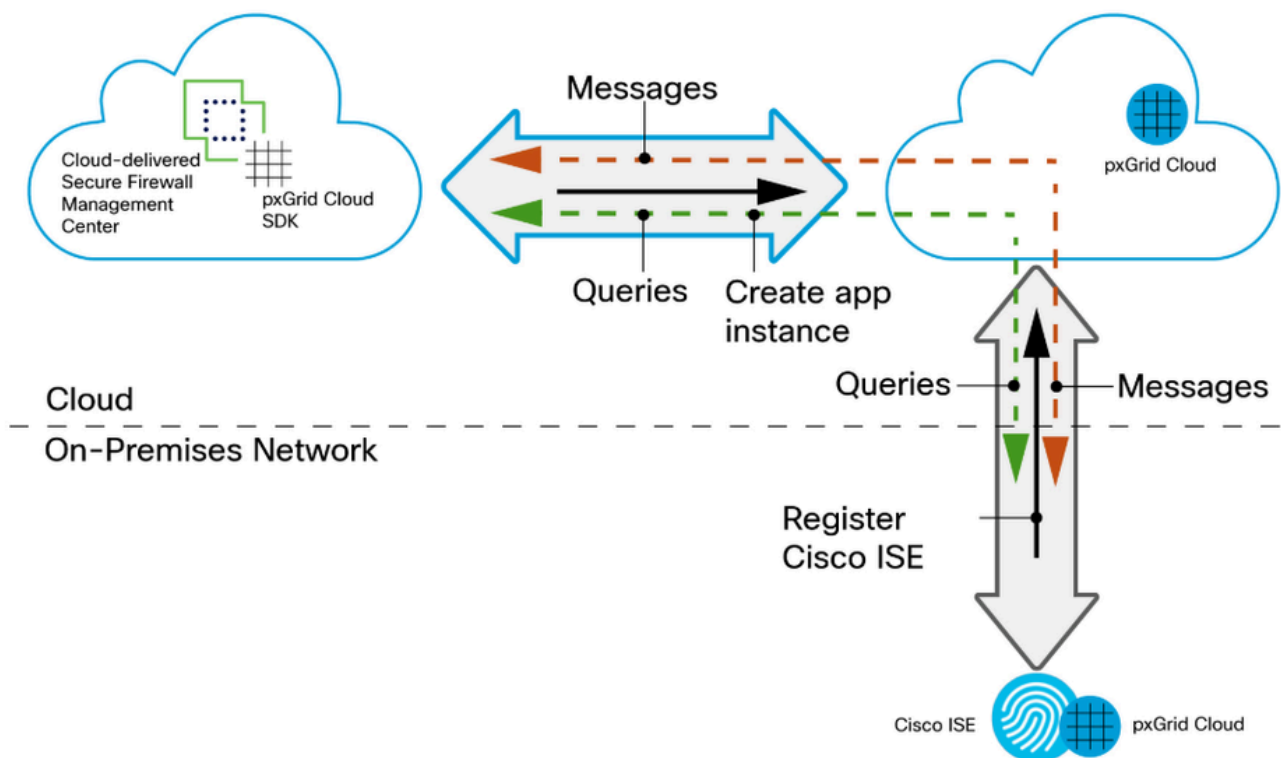
dabei irgendeine Art von Bypass implementiert wird oder Löcher in die Firewall gesteckt werden.

Die Cisco ISE pxCloud ist eine Cloud-basierte Lösung, die dieses Problem löst und eine gemeinsame Nutzung von Kontext am Standort und in der Cloud ohne zusätzliche Installation, zusätzlichen Aufwand und Beeinträchtigung der Netzwerksicherheit ermöglicht. Sie ist sicher und anpassbar, sodass Sie nur die Daten freigeben können, die Sie freigeben möchten, und nur die für Ihre Anwendung relevanten Kontextdaten nutzen können.

Cisco ISE Release 3.1 Patch 3 und höher unterstützen pxGrid Cloud. Cisco und seine Partner können pxGrid Cloud-basierte Anwendungen entwickeln und im pxGrid Cloud-Angebot registrieren. Das Cisco DNA-Cloud-Portal integriert und registriert Anwendungen, ohne auf andere Infrastrukturen vor Ort angewiesen zu sein. Diese Anwendungen nutzen die externen RESTful Services (ERS), offene APIs und pxGrid (APIs und Websocket), um Informationen mit der Cisco ISE auszutauschen und Abonnement- und Benutzerdaten von ISE in cdFMC zu verwenden.

Konfigurieren

Netzwerkdiagramm



Integration von cdFMC und ISE über pxGrid Cloud

Konfigurationen

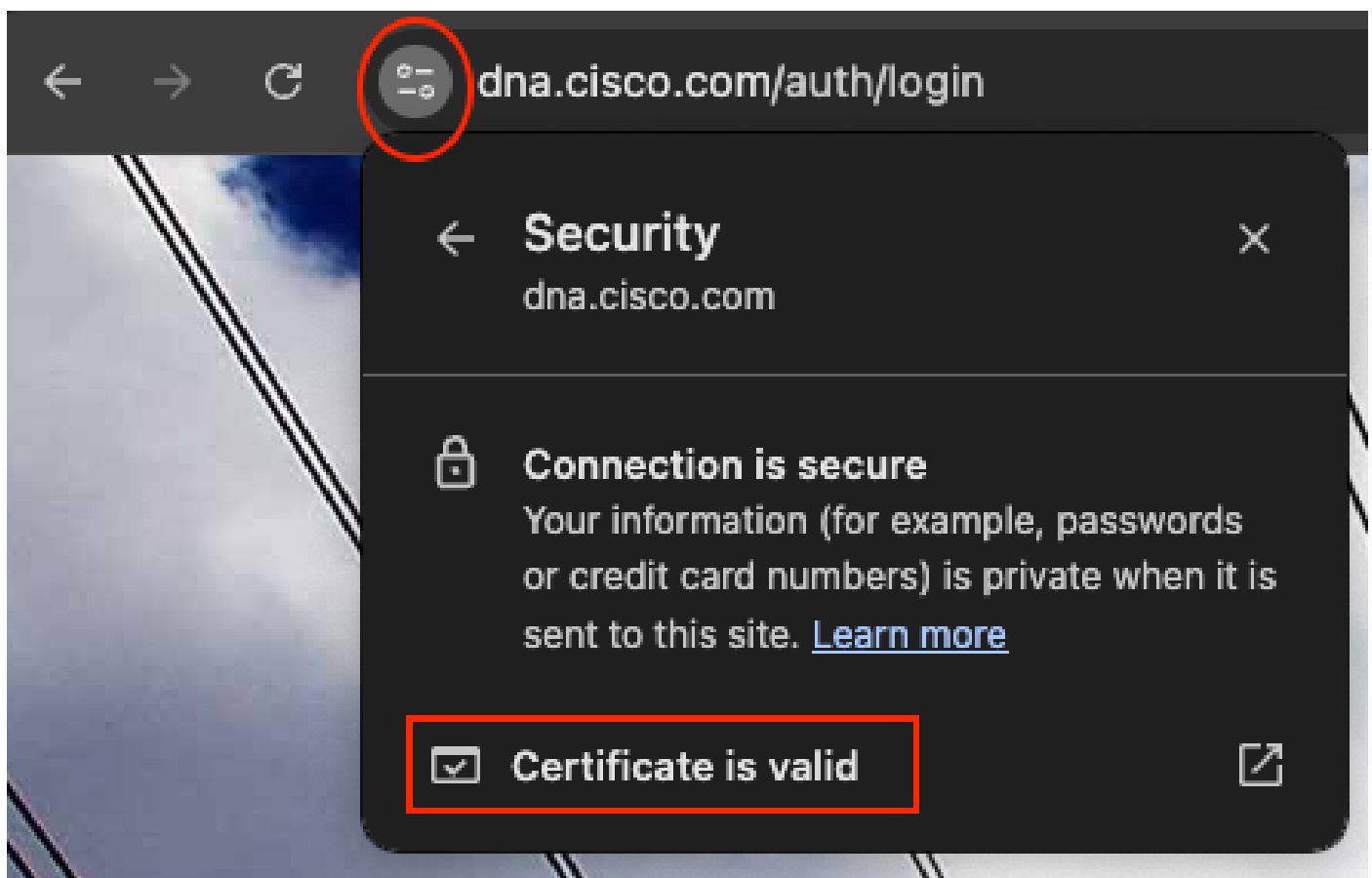
Vier Hauptschritte sind dabei zu nennen:

- Importieren Sie das Cisco pxGrid Cloud-Serverzertifikat in die ISE.
- Registrieren der ISE beim Catalyst Cloud Portal

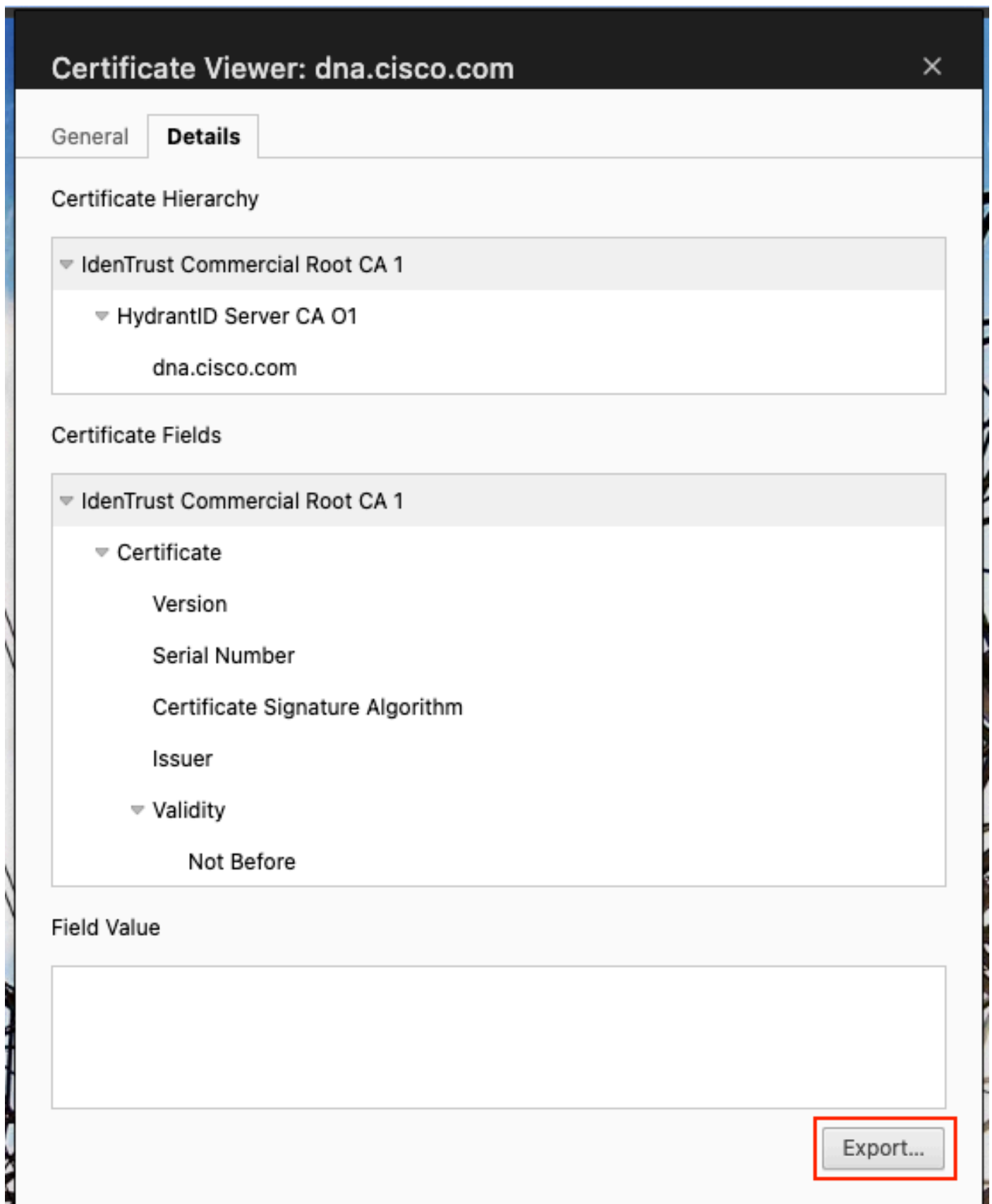
- Aktivieren der cdFMC-Anwendung auf der ISE mithilfe des Integrationskatalogs
- pxGrid-Anwendungsinstanz (cdFMC) erstellen

Cisco pxGrid Cloud-Serverzertifikat in ISE importieren

Die ISE muss eine Vertrauensstellung zur Cisco pxGrid Cloud herstellen. Obwohl die Cloud-Website mit einem öffentlich signierten Zertifikat authentifiziert ist, verfügt die ISE nicht über eine vollständige Liste vertrauenswürdiger Stammzertifizierungsstellen. Daher muss der Administrator eine Vertrauensstellung herstellen. Exportieren Sie die pxGrid Cloud Root and Intermediate-Zertifikate, indem Sie zum [Catalyst Cloud Portal](#) navigieren. Die meisten Browser erlauben dies. Hier sind die Schritte, um ein Zertifikat von Chrome Browser zu erhalten.



Standortinformationen anzeigen



Exportieren der Zertifikatskette

Importieren Sie die Zertifikate in den ISE-Speicher "Trusted Certificates", wenn die Zertifikatskette fehlt (ISE verfügt bereits über IdemTrust Commercial Root CA 1).

Stellen Sie sicher, dass die Option "Trust for Authentication of Cisco Services" (Für die

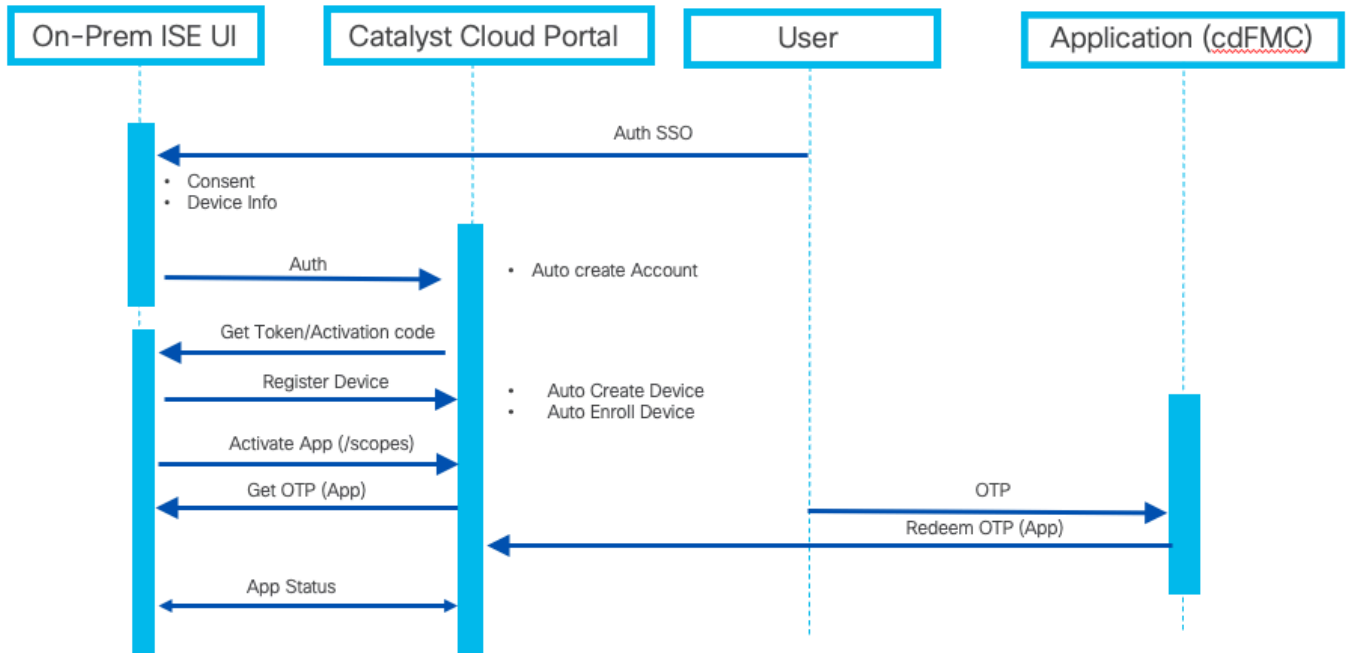
Authentifizierung von Cisco Services vertrauen) für dieses Stammzertifikat der Zertifizierungsstelle aktiviert ist. Um die Vertrauenswürdigkeit für die Authentifizierung von Cisco Services zu aktivieren, wählen Sie Administration > System > Certificates (Verwaltung > System > Zertifikate).

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade & Rollback	Health Checks
Certificate Management System Certificates Admin Certificate Node Restart Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Settings Certificate Authority			Issuer * Friendly Name IdenTrust Commercial Root CA 1 Status Enabled Description IdenTrust Commercial Root CA 1 Subject CN=IdenTrust Commercial Root CA 1,O=IdenTrust,C=US Issuer CN=IdenTrust Commercial Root CA 1,O=IdenTrust,C=US Valid From Thu, 16 Jan 2014 18:12:23 UTC Valid To (Expiration) Mon, 16 Jan 2034 18:12:23 UTC Serial Number 0A 01 42 80 00 00 01 45 23 C8 44 B5 00 00 00 02 Signature Algorithm SHA256withRSA Key Length 4096 Usage Trusted For: ☐ Trust for authentication within ISE ☐ Trust for client authentication and Syslog ☐ Trust for certificate based admin authentication ☒ Trust for authentication of Cisco Services ☐ Trust for Native IPSec certificate based authentication			

Unterstützung der Vertrauensstellung für die Authentifizierung von Cisco Services

Flussdiagramm

App Activation Workflow



App-Aktivierungs-Workflow

In dieser Konfiguration verwendete ISE-Bereitstellung

Deployment Nodes

A Cisco ISE node can assume the Administration, Policy Service, or Monitoring personas. Data is automatically replicated from PAN to all the secondary nodes. If needed, you can manually sync a node with the PAN by using the Sync option. During Sync, Cisco ISE performs Full Sync if full database replication is required or Selective Sync if only bulk replication of selective dataset is needed. You must update the SXP device configuration with the connected PSN details in case of upgrade, node failure, or node configuration updates.

Selected 0 Total 4

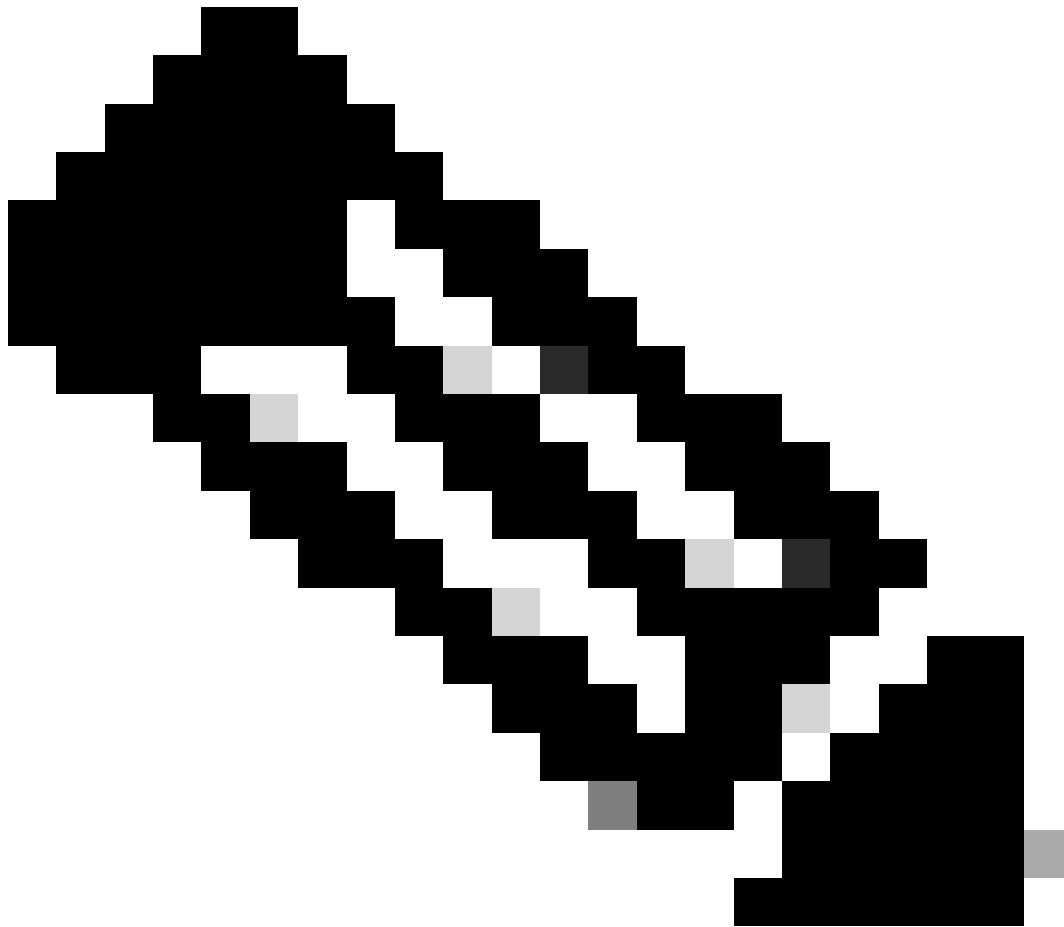
Edit Register Sync Deregister All

☐	Hostname	Personas	Role(s)	Services	Node Status
☐	ise341-PAN	Administration, Monitoring	PRI(A), PRI(M)	NONE	
☐	ise341-SAN	Administration, Monitoring	SEC(A), SEC(M)	NONE	
☐	ise341-psn1	Policy Service, pxGrid		SESSION,PROFILER	
☐	ise341-psn2	Policy Service, pxGrid		SESSION,PROFILER	

Registrierung der ISE beim Catalyst Cloud Portal

Aktivieren Sie den pxGrid Cloud-Service in der Cisco ISE, und registrieren Sie Ihr Gerät.

1. Wählen Sie in der Cisco ISE-GUI Administration > System > Deployment aus.
2. Klicken Sie auf den Knoten, auf dem Sie den pxGrid Cloud-Service aktivieren möchten (in diesem Fall den ersten PSN-Knoten).
3. Aktivieren Sie auf der Registerkarte Allgemeine Einstellungen den Dienst pxGrid.
4. Aktivieren Sie das Kontrollkästchen pxGrid Cloud.



Anmerkung: Der pxGrid Cloud-Service kann nur auf zwei Knoten aktiviert werden, um eine hohe Verfügbarkeit zu ermöglichen. Sie können die pxGrid Cloud-Option nur aktivieren, wenn der pxGrid-Dienst auf diesem Knoten aktiviert ist.

5. Geben Sie im Feld ISE-Bereitstellungsname einen sinnvollen Namen ein. Dieser Name wird im Catalyst Cloud Portal angezeigt und kann verwendet werden, um zu unterscheiden, ob mehrere ISE-Bereitstellungen bei der Cloud registriert sind. Sie können Ihre registrierte Cisco ISE-Bereitstellung im Cisco Catalyst Cloud Portal anhand des ISE-Bereitstellungsnamens überprüfen.

(Optional) Geben Sie im Feld Description (optional) eine Beschreibung für Ihre Cisco ISE-Bereitstellung ein.

6. Wählen Sie in der Dropdown-Liste "Region" eine Region aus, um Ihr Cisco ISE-Gerät zu registrieren. Cisco pxGrid Cloud wird nun neben den USA auch in Europa, im Asien-Pazifik-Raum und in Japan unterstützt. Beachten Sie, dass die Anwendung, die Sie mit pxGrid Cloud verwenden möchten, auch in der gleichen Region verfügbar sein muss.

7. Klicken Sie auf Registrieren.

Bookmarks Deployment Licensing Certificates Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help

☐ Enable Passive Identity Service

☒ pxGrid ☐ Enable pxGrid Cloud

pxGrid Cloud can be enabled only after registering your Cisco ISE to your Cisco DNA Portal account.

ISE deployment name
ISE341-PSN1

Description (optional)
Primary pxGrid node

Select a region where you want to register your device. Application should also be available in the same region.

Region
us-west-2

Check the checkboxes below to register this ISE if you concur with the statements.

☒ I have read and acknowledge the [Cisco Privacy Statement](#).

☒ I agree that offers are governed by Cisco EULA and I am an authorized agent of my company, [Cisco's End User License Agreement](#).

Register

Reset Save

Registrieren von ISE PSN bei pxGrid Cloud

8. Auf der Popup-Seite Gerät aktivieren wird der Aktivierungscode für das Gerät automatisch ausgefüllt. Klicken Sie auf Next (Weiter).



US
EN



Activate your device

Follow the instructions on your device to get an
activation code

Activation Code

XXXX-XXXX

Next

[Contact support](#) [Privacy](#) [Terms & Conditions](#) [Cookies](#) [Trademarks](#)

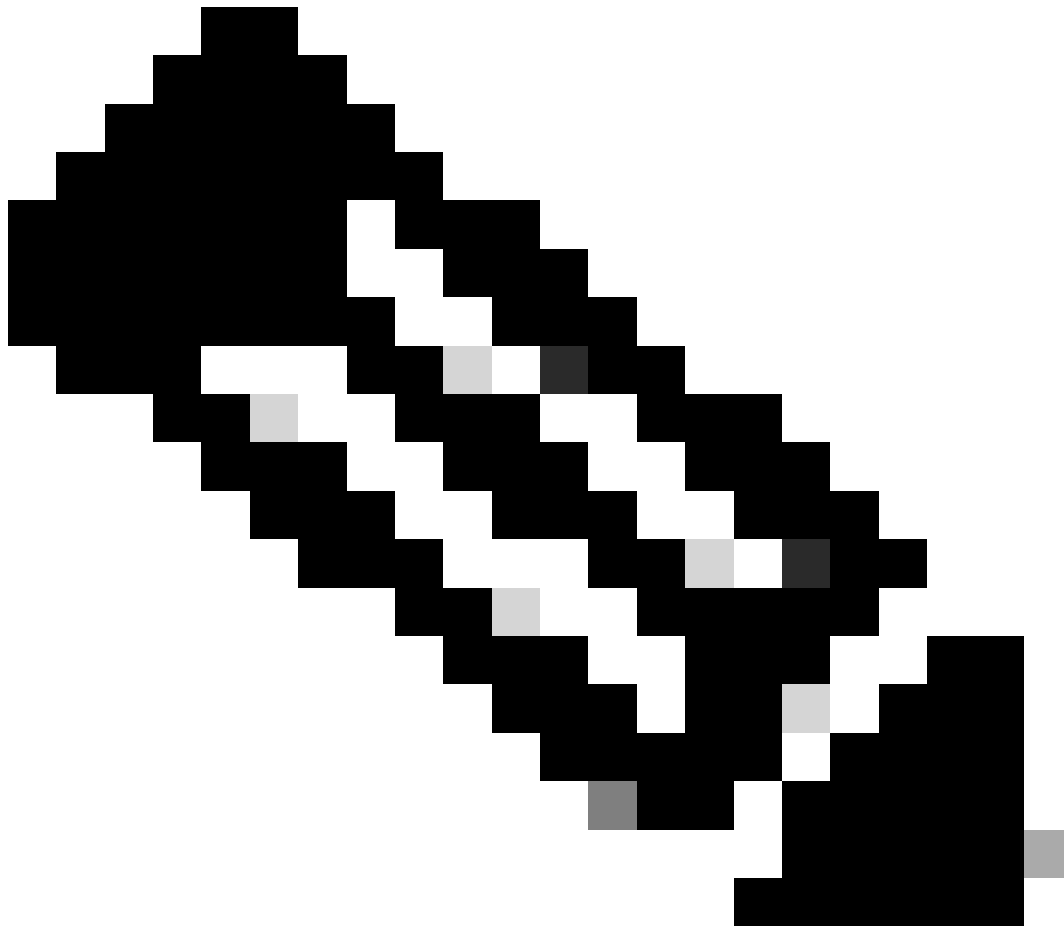


Device activated

 poongarg@cisco.com

Follow the instructions on your device for next
steps

[Contact support](#) [Privacy](#) [Terms & Conditions](#) [Cookies](#) [Trademarks](#)

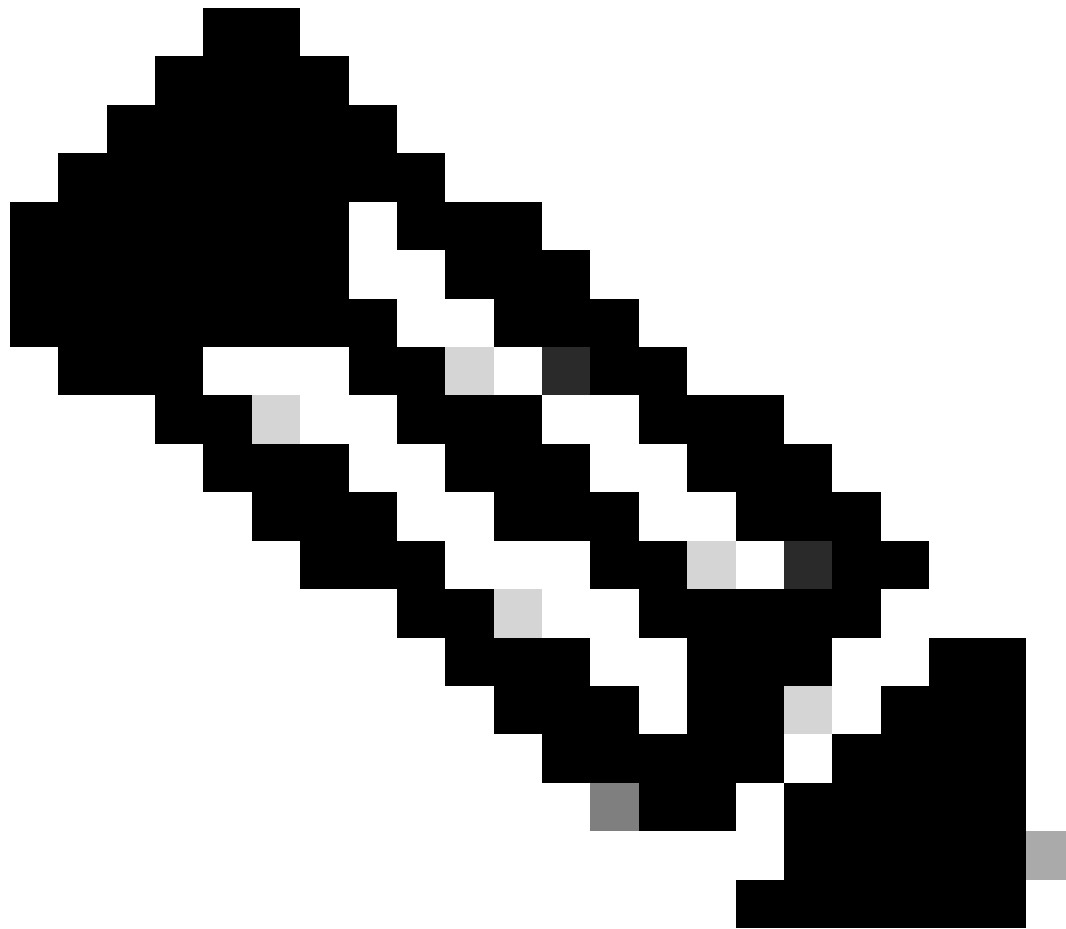


Anmerkung: Wenn Sie "pxGrid Cloud"-Personal auf dem zweiten Knoten aktivieren, benötigt die ISE nicht alle diese Details, da sich die Registrierung der ISE bei pxGrid Cloud auf Bereitstellungsebene befindet.

9. Melden Sie sich mit Ihren Anmeldeinformationen beim [Cisco Catalyst Cloud Portal](#)-Konto an. Wenn Sie keine Anmeldeinformationen haben, erstellen Sie ein neues Konto, um die Geräteregistrierung abzuschließen. Weitere Informationen finden Sie unter [Erstellen eines Kontos im Cisco Catalyst Cloud Portal](#).

Ihr Cisco ISE-Gerät ist aktiviert und registriert.

2. Wählen Sie unter Verfügbare Integrationen die Anwendung Firewall Management Center.



Anmerkung: Die Liste der Anwendungen hängt vom Konto ab. Einige Anwendungen können nur bestimmten Konten zugeordnet werden.

Identity Services Engine

Administration / Integration Catalog

Integration Catalog

Available integrations



Cisco Security Cloud

Network Security pxGrid Cloud

us-west-2

Cisco Security Cloud acts as an application broker which will allow ISE to integrate with the supported Cisco's cloud Security...

[More details](#)



Firewall Management Center

Network Security pxGrid Cloud

us-west-2

Integrate with Firewall Management Center (FMC) to setup Identity Based Access Control in Cisco Secure Firewall.

[More details](#)



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...

[More details](#)



pxGrid Cloud Demo Multi-instance

networking demo pxGrid Cloud

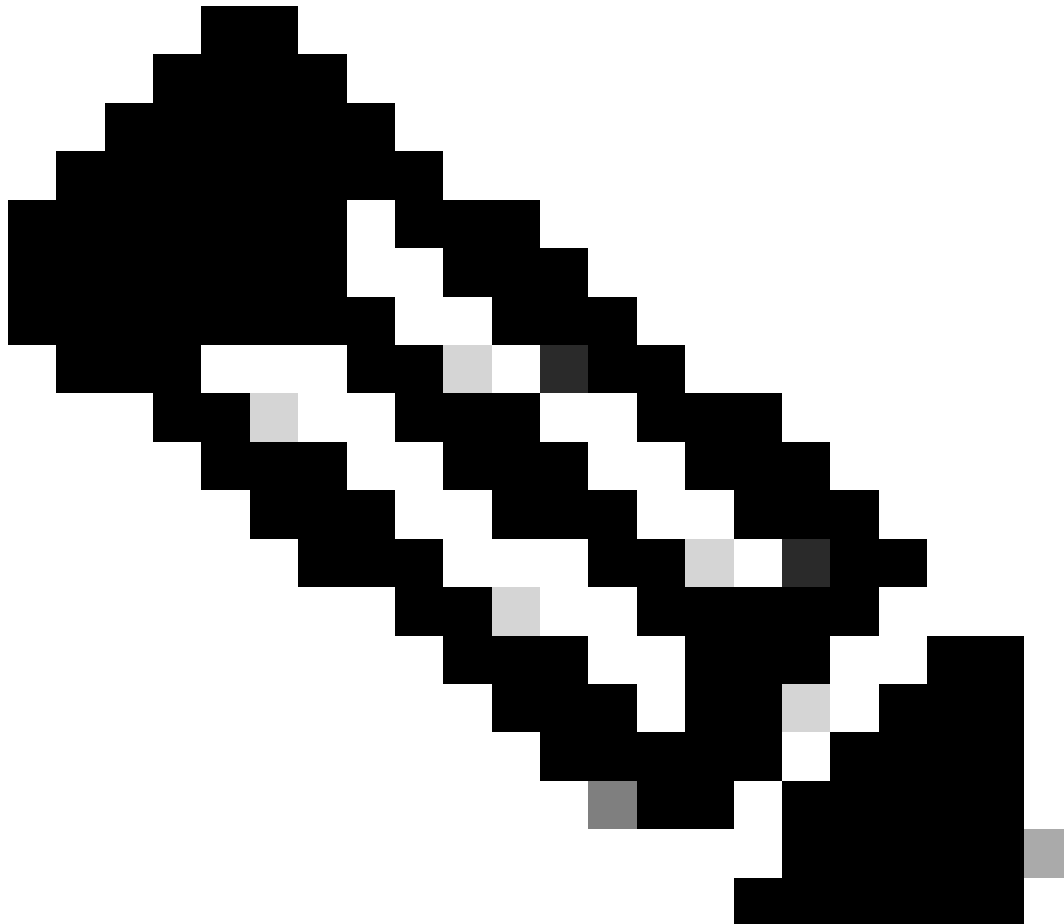
us-west-2 eu-central-1

ap-southeast-1

Welcome to Cisco pxGrid Cloud's Demo Application (Multi-instance)! The purpose of this is to guide you through the setup...

[More details](#)

3. Wählen Sie im Abschnitt App-Konfiguration die Option Neue Instanz auswählen und wählen Sie die Datenbereiche für die App-Konfiguration aus. Wählen Sie zum Fortfahren mindestens einen Datenbereich aus.



Anmerkung: Wenn Sie einen Datenbereich auswählen, wird dieser unter den pxGrid-Cloud-Richtlinieneinstellungen auf Systemebene aktiviert.

4. Klicken Sie auf Aktivieren, um die App zu aktivieren.

Identity Services Engine Administration / Integration Catalog

Integration Catalog

Firewall Management Center

Network Security pxGrid Cloud us-west-2

[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 cisco	Status Registered
Device name ISE341-PSN1	Registered region us-west-2
Description Primary pxGrid node	

App configuration

Application status
Inactive

Instance ⓘ

☐ 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.
- ☒ Profiler Configuration
Provides ISE profiling policy device details such as ID and name.
- ☒ 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.

• If you are associating multiple ISE clusters, please ensure that your SGT IDs and names are homogenized.
• When you select a data scope, it will also enable the same under system level pxGrid Cloud Policy settings.

Activate

FMC-Anwendungskonfiguration auf der ISE

5. Kopieren Sie aus dem Popup-Fenster "One-Time Password (OTP)" das OTP, um es bei der Erstellung der pxGrid-Anwendungsinstanz für cdFMC einzulösen.

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

1cOzAGz9sMayHJzy4ejSsbpq8Hc...

 **Copy**

OK

OTP für CdFMC-Anwendung

6. Konfigurieren Sie die pxGrid-Cloud-Richtlinie, indem Sie zu Administration > pxGrid Services > Client Management > pxGrid Cloud Policy navigieren. Wählen Sie die pxGrid-Services aus, die Sie mit den SaaS-Anwendungen gemeinsam nutzen möchten, und aktivieren Sie die externen RESTful Services (ERS)-APIs und OpenAPIs, nur Lesezugriff auf Cisco pxGrid Cloud Anwendungen.

Identity Services Engine

Administration / pxGrid Services

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Summary

Client Management

Diagnostics

Settings

Clients

Policy

Groups

Certificates

pxGrid Cloud Policy

pxGrid Cloud Policy

You can create a general pxGrid Cloud policy for what is allowed or denied between your ISE deployment and the pxGrid Cloud service. The per partner authorization policy can be setup in the cloud portal.

pxGrid Services

You can use Cisco pxGrid to share the context-sensitive information from Cisco ISE session directory with other network systems such as ISE Eco system partner systems and other Cisco platforms. The pxGrid framework can also be used to exchange policy and configuration data between nodes like sharing tags and policy objects between Cisco ISE and third party vendors, and for other information exchanges.

Echo Service

TrustSec SXP

MDM

TrustSec configuration

TrustSec

Profiler configuration

Endpoint

ANC configuration

Radius Failure

User Defined Network

Session Directory

ERS APIs

Enable External RESTful Services (ERS) APIs Policy in pxGrid Cloud Policy.

Enabled

Read Only

Read/Write

Open APIs

Enable Open APIs for pxGrid Cloud.

Enabled

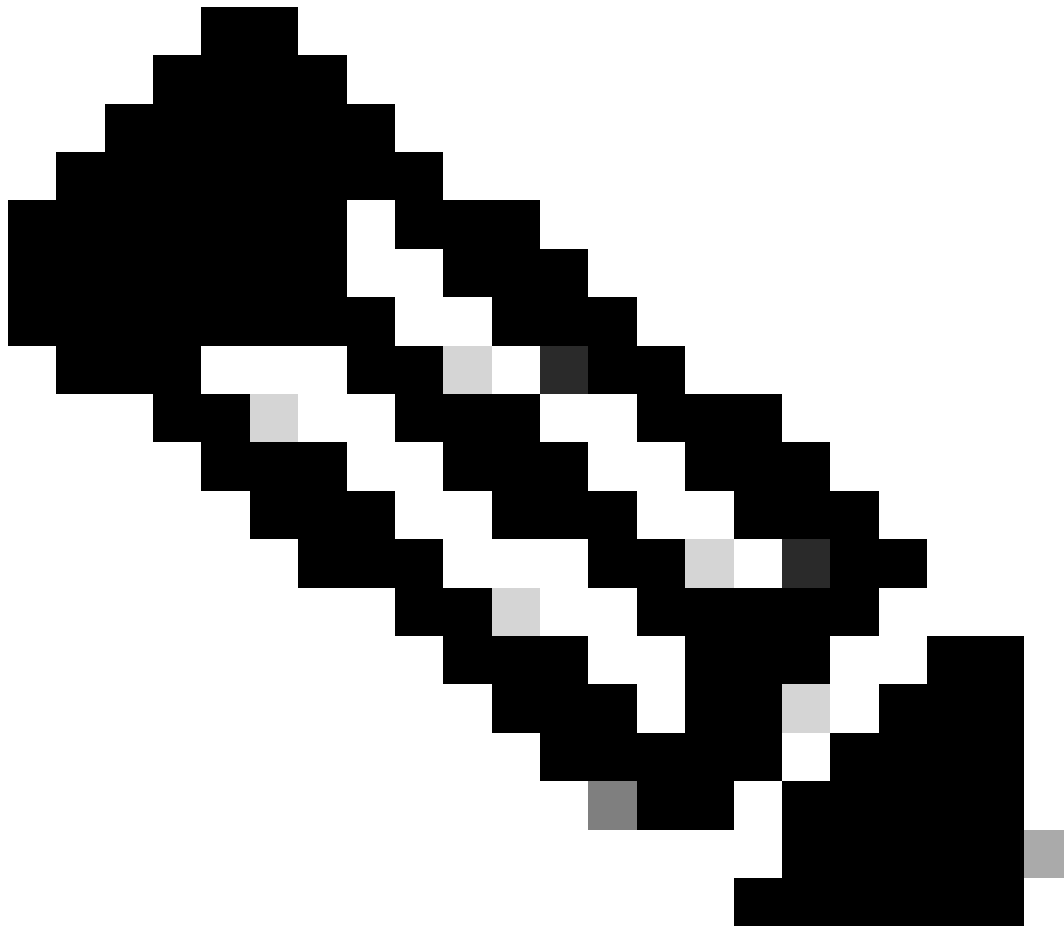
Read Only

Read/Write

Reset

Save

Konfigurieren der pxGrid-Cloud-Richtlinie



Anmerkung: Der Echo-Dienst dient zum Durchführen von Integritätsprüfungen, um sowohl die pub-sub- als auch die API-Verbindung mit der ISE zu ermitteln.

Standardmäßig erhalten die Cisco pxGrid Cloud-Anwendungen schreibgeschützten Zugriff auf die APIs (nur HTTP GET-Vorgänge können ausgeführt werden). Aktivieren Sie die Option Lesen/Schreiben im pxGrid Cloud Policy-Fenster, wenn Sie auch POST-, PUT- und DELETE-Vorgänge zulassen möchten.

pxGrid-Anwendungsinstanz (cdFMC) erstellen

1. Melden Sie sich beim Security Cloud Control (SCC)-Portal als Benutzer mit der Rolle "Super Admin" an.



CONNECTING TO SECURITY CLOUD CONTROL (APJC)

Security Cloud Sign On

Email

Continue

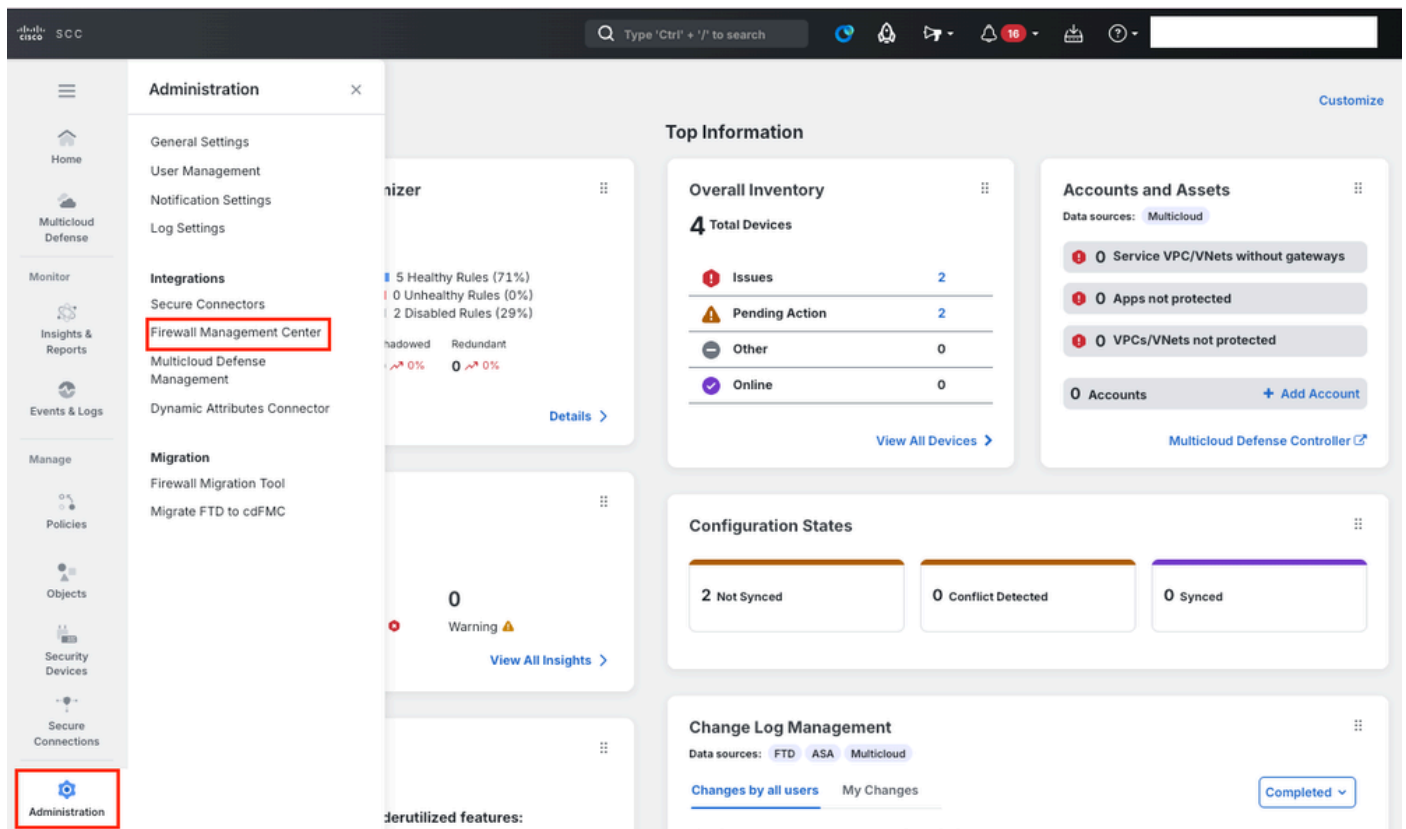
Don't have an account? [Sign up now](#)

Or

[Other login options](#)

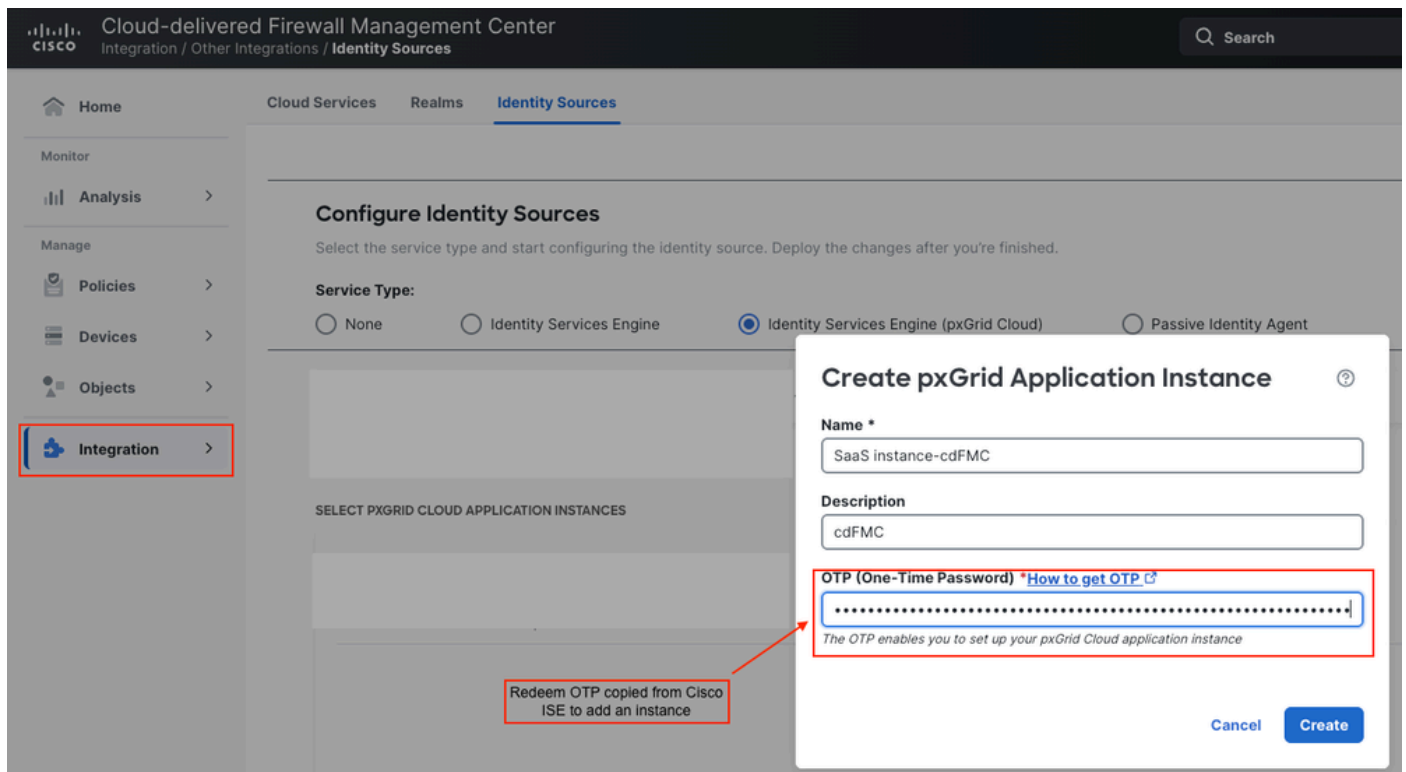
[System status](#) [Policy statement](#)

2. Klicken Sie im Menü Security Cloud Control auf Administration > Integrations > Firewall Management Center, wählen Sie Ihre cdFMC-Instanz aus, und wählen Sie im rechten Fensterbereich die Optionen System > Configuration aus.



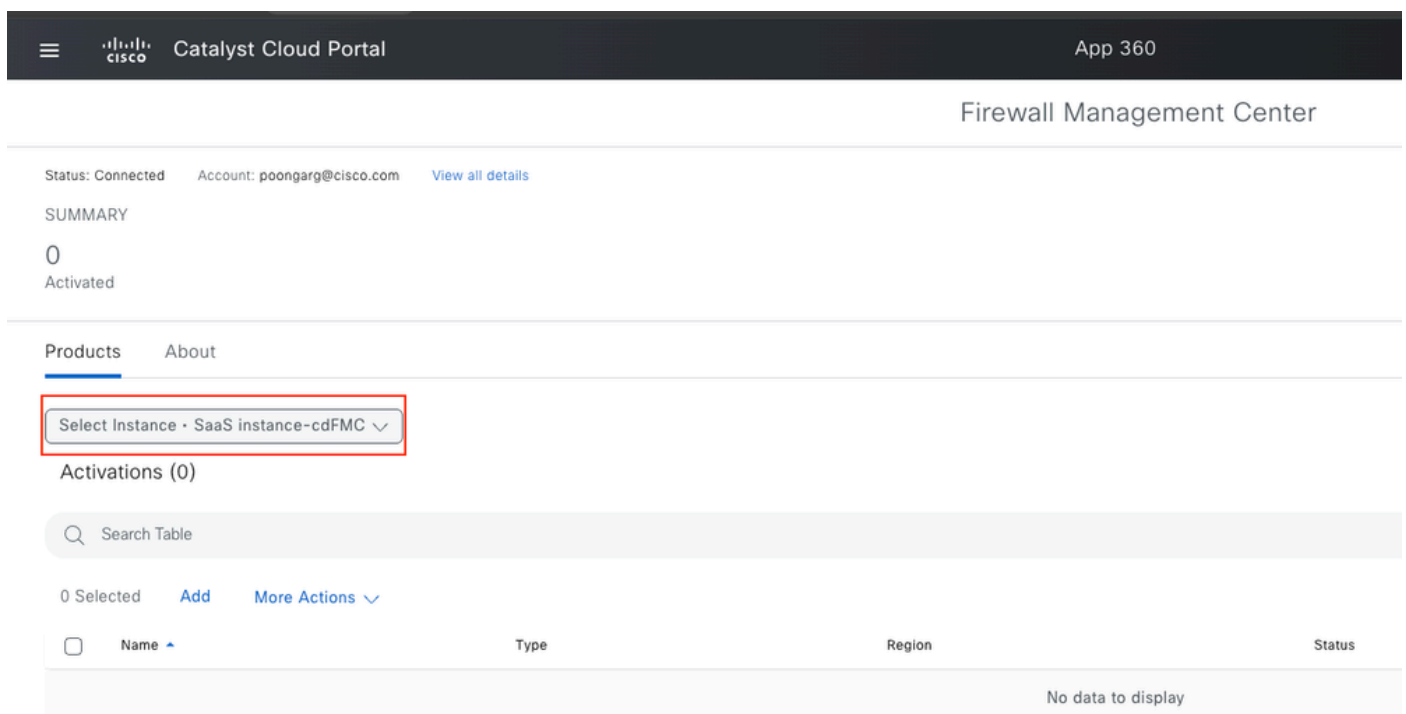
Navigieren zum Firewall Management Center

3. Wählen Sie auf der Konfigurationsseite Integration > Weitere Integrationen > Identitätsquellen > Wählen Sie den Servicetyp Identity Services Engine (pxGrid Cloud). Klicken Sie auf Create pxGrid Application Instance (PxGrid-Anwendungsinstanz erstellen), und lösen Sie das kopierte OTP von der Cisco ISE ein, um eine Instanz hinzuzufügen.



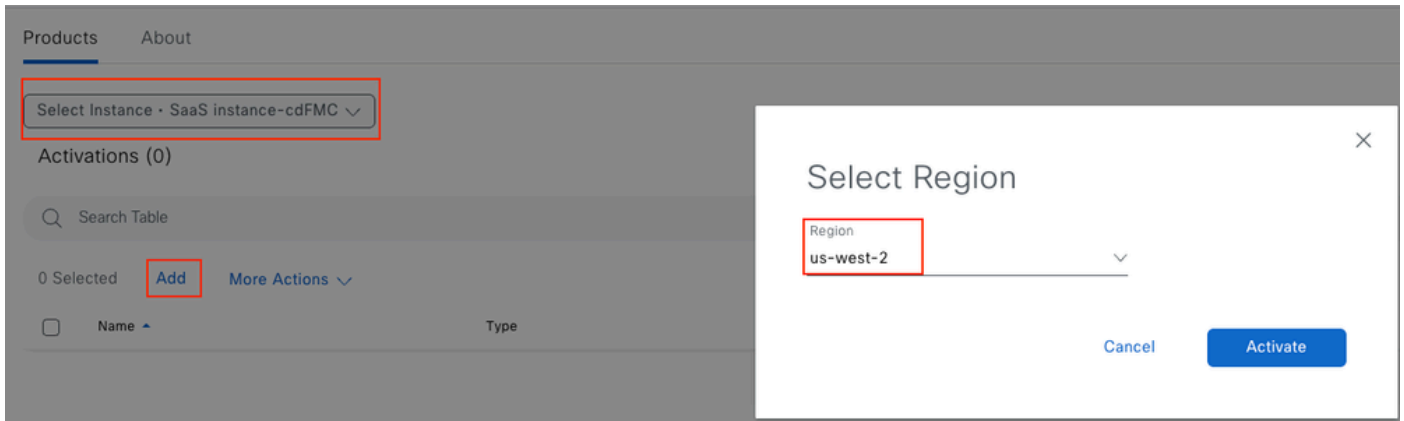
cdFMC-Anwendungsinstanz erstellen

4. Überprüfen Sie dies auf dem Cisco Catalyst Cloud Portal unter Applications and Products > Firewall Management Center > Manage > Products > Select Instance (Anwendungen und Produkte > Firewall-Verwaltungszentrum > Verwalten > Produkte > Select Instance).



Überprüfen Sie das cdFMC auf dem Catalyst Cloud Portal.

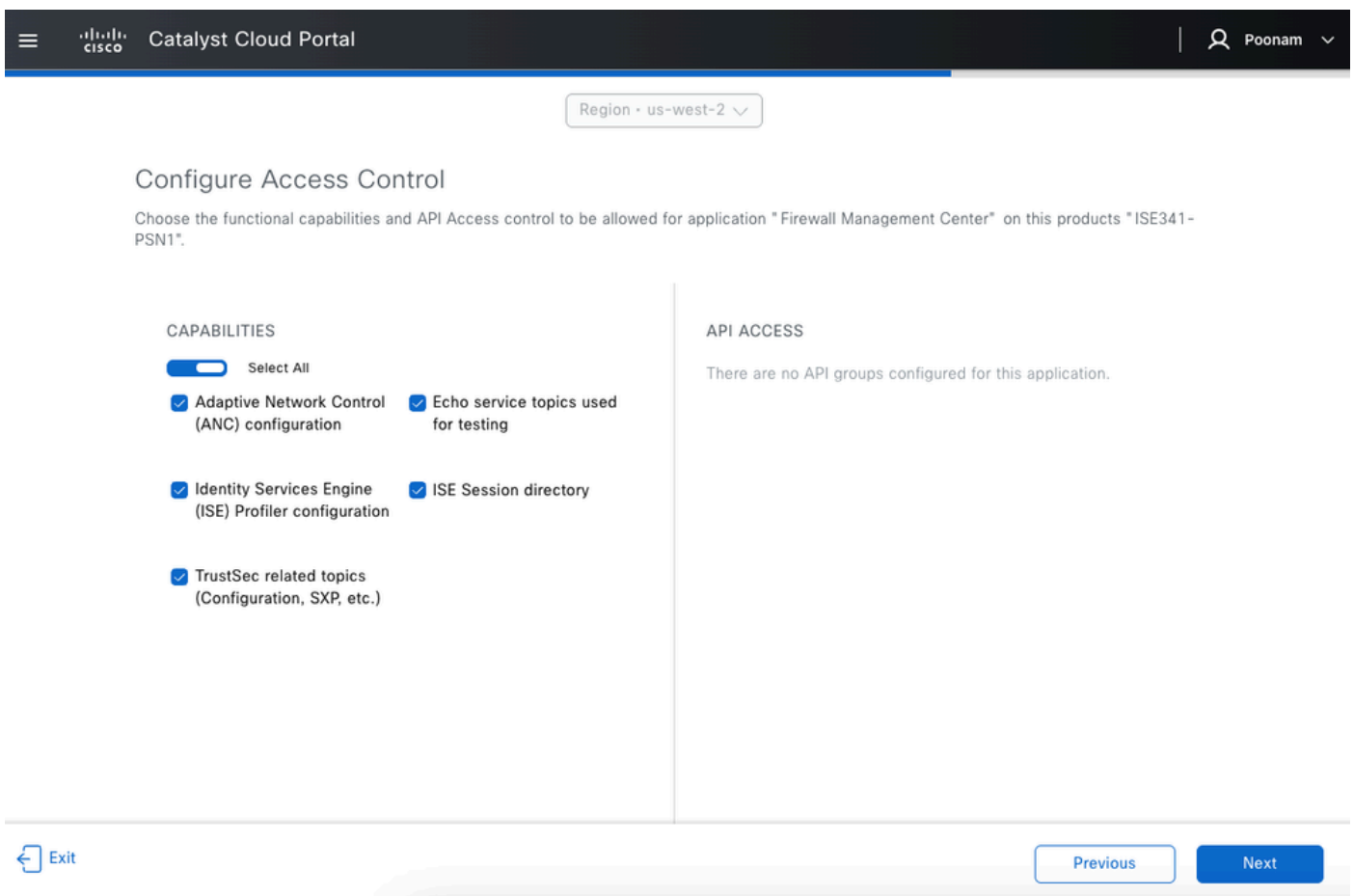
5. Wählen Sie die neu erstellte cdFMC-Anwendung und klicken Sie auf Hinzufügen. Wählen Sie Region aus, und klicken Sie auf Aktivieren.



Region auswählen

5. Wählen Sie Ihre Anwendungsinstanz aus, und klicken Sie auf Weiter. Wählen Sie Ihr Produkt (ISE pxGrid-Knoten), klicken Sie auf Weiter.

6. Konfigurieren der Zugriffskontrolle: Wählen Sie die für cdFMC zulässigen Funktionsfunktionen für das ausgewählte ISE-Produkt aus. Klicken Sie auf Next (Weiter). Eine Konfigurationsübersicht wird angezeigt. Überprüfen Sie die Einstellungen, und klicken Sie auf Aktivieren.



Konfigurieren Sie die Zugriffskontrolle für Ihr cdFMC.

Done! Your Product is connected to Firewall Management Center

It could take up to 5-10 minutes to activate this application on your products.

 Your Product is connected to Firewall Management Center 

Verbindung der Produkt-ISE mit cfFMC

8. Überprüfen Sie dies auf dem Cisco Catalyst Cloud Portal unter Applications and Products > Firewall Management Center > Manage > Products > Select Instance (Anwendungen und Produkte > Firewall-Verwaltungscenter > Verwalten > Produkte > Select Instance).

Catalyst Cloud Portal

Applications and Products / App 360

Person

Firewall Management Center

Status: Connected Account: [View all details](#)

SUMMARY

1 Activated

Products About

Select Instance - SaaS Instance-cdFMC

Activations (1)

0 Selected Add More Actions

☐	Name	Type	Region	Status	Actions
☐	ISE341-PSN1	Cisco ISE	us-west-2	Activated	

As of: Mar 17, 2025 6:24 PM

Überprüft, ob App aktiviert ist.

Überprüfung

1. Navigieren Sie im Catalyst Cloud Portal zu Anwendungen und Produkte. Wählen Sie Ihren ISE-Produktnamen aus, und überprüfen Sie die Produktdetails. Überprüfen Sie, ob cdFMC unter "Activated Application" (Aktivierte Anwendung) angezeigt wird.

Product Details



Product Name	ISE341-PSN1
Description	Primary pxGrid node
Product Type	Cisco ISE
Region	us-west-2
Last Heartbeat Status	✓ March 17th, 2025 - 6:28:08 PM
Registration Status	✓ Registered

Activated Applications

Search Table

Applications Id	Applications Name	Applications Activation Status
fmcmi-o1lsbr5b9	Firewall Management Center	✓ Activated

1 Record(s) Show Records: 25 1 - 1 < 1 >

Überprüfen Sie das Catalyst Cloud Control-Portal.

2. Testen Sie unter Security Cloud Control die konfigurierte cdFMC-Anwendungsinstanz. Der Test zeigt "Success"

SaaS instance-cdFMC	cdFMC	✓ Success Test again
Tenant ID: cisco		
Activated ISE: ISE341-PSN1		

Überprüfung im Security Cloud Control-Portal

3. Melden Sie sich beim Knoten Active pxGrid an, und überprüfen Sie, ob Hermes (pxGrid Cloud Agent) mit dem Befehl show application status ise ausgeführt wird. Dieser Agent befindet sich auf dem Knoten Standby pxGrid im deaktivierten Status.

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	265600
Database Server	running	168 PROCESSES
Application Server	running	4158798
Profiler Database	running	272701
ISE Elasticsearch	running	4124473
AD Connector	running	285681
M&T Session Database	running	4122983
M&T Log Processor	running	4125430
Certificate Authority Service	running	4101637
EST Service	running	47678
SXP Engine Service	disabled	
TC-NAC Service	disabled	
PassiveID WMI Service	disabled	
PassiveID Syslog Service	disabled	
PassiveID API Service	disabled	
PassiveID Agent Service	disabled	
PassiveID Endpoint Service	disabled	
PassiveID SPAN Service	disabled	
DHCP Server (dhcpd)	disabled	
DNS Server (named)	disabled	
ISE Messaging Service	running	4107029
ISE API Gateway Database Service	running	4126393
ISE API Gateway Service	running	4140593
ISE pxGrid Direct Service	running	244678
ISE pxGrid Direct Pusher	running	245743
Segmentation Policy Service	disabled	
REST Auth Service	running	23551
SSE Connector	disabled	
Hermes (pxGrid Cloud Agent)	running	250688
MFA (Duo Sync Service)	disabled	
McTrust (Meraki Sync Service)	disabled	
aciconn (ACI Connection Service)	disabled	
Workload Connector Service	disabled	
ISE Prometheus Service	running	240758
ISE Prometheus Exporter	running	250921
ISE Grafana Service	running	4143487
ISE MNT LogAnalytics Elasticsearch	disabled	
ISE Logstash Service	disabled	
ISE Kibana Service	disabled	
ISE Native IPSec Service	running	4144654
MFC Profiler	running	27017
ISE Prometheus Alertmanager Service	running	4153383
Protocols Engine	running	236265

Status von Hermes (pxGrid Cloud Agent) überprüfen

Überprüfen Sie pxcloud.log auf beiden pxGrid-Knoten, um den Aktiv- und Standby-Status zu bestätigen:

On Active pxGrid node (pxcloud.log)

<#root>

```
2025-03-17 14:35:25,530 DEBUG [pxCloud-hermesCheck-2768][[]] cpm.pxcloud.ha.statemachine.StateMachine -::::- RUNNING (HERMES_OK) -----
2025-03-17 14:35:27,438 DEBUG [pxCloud-heartbeat-2769][[]] cpm.pxcloud.ha.statemachine.HeartBeat -::::- url -
```

<https://ise341-psn2.poongarg.local:8910/pxgrid/pxcloud/statusLookup>

```
2025-03-17 14:35:27,445 DEBUG [pxCloud-heartbeat-2769][[]] cpm.pxcloud.ha.statemachine.HeartBeat -::::-
```

role=STANDBY,

```
state=MONITORING, pxGridConnectionStatus=NOT_CONNECTED, cloudConnectionStatus=NOT_CONNECTED, reason=]
```

```
2025-03-17 14:35:27,445 DEBUG [pxCloud-heartbeat-2769][[]] cpm.pxcloud.ha.statemachine.HeartBeat -::::-
```

```
2025-03-17 14:35:27,445 DEBUG [pxCloud-heartbeat-2769][[]] cpm.pxcloud.ha.statemachine.StateMachine -::
```

RUNNING

(PEER_MONITORING)

```
2025-03-17 14:35:35,548 DEBUG [pxCloud-hermesCheck-2768][[]] cpm.pxcloud.ha.statemachine.HermesCheck -
```

```
2025-03-17 14:35:35,572 DEBUG [pxCloud-hermesCheck-2768][[]] cpm.pxcloud.ha.statemachine.HermesCheck -
```

```
2025-03-17 14:35:35,572 DEBUG [pxCloud-hermesCheck-2768][[]] cpm.pxcloud.ha.statemachine.HermesCheck -
```

On Standby pxGrid node (pxcloud.log)

<#root>

```
2025-03-17 14:34:14,145 DEBUG [pxCloud-heartbeat-6441][[]] cpm.pxcloud.ha.statemachine.HeartBeat -::::- url -
```

<https://ise341-psn1.poongarg.local:8910/pxgrid/pxcloud/statusLookup>

```
2025-03-17 14:34:14,153 DEBUG [pxCloud-heartbeat-6441][[]] cpm.pxcloud.ha.statemachine.HeartBeat -::::-
```

peer - StatusResponse [role=ACTIVE

```
, state=RUNNING, pxGridConnectionStatus=CONNECTED, cloudConnectionStatus=CONNECTED, reason=]
```

```
2025-03-17 14:34:14,154 DEBUG [pxCloud-heartbeat-6441][[]] cpm.pxcloud.ha.statemachine.HeartBeat -::::-
```

```
2025-03-17 14:34:14,154 DEBUG [pxCloud-heartbeat-6441][[]] cpm.pxcloud.ha.statemachine.StateMachine -::
```

MONITORING

(PEER_RUNNING)

Überprüfen Sie außerdem den Port 8913, der nur auf dem ACTIVE pxGrid-Knoten geöffnet wird:

<#root>

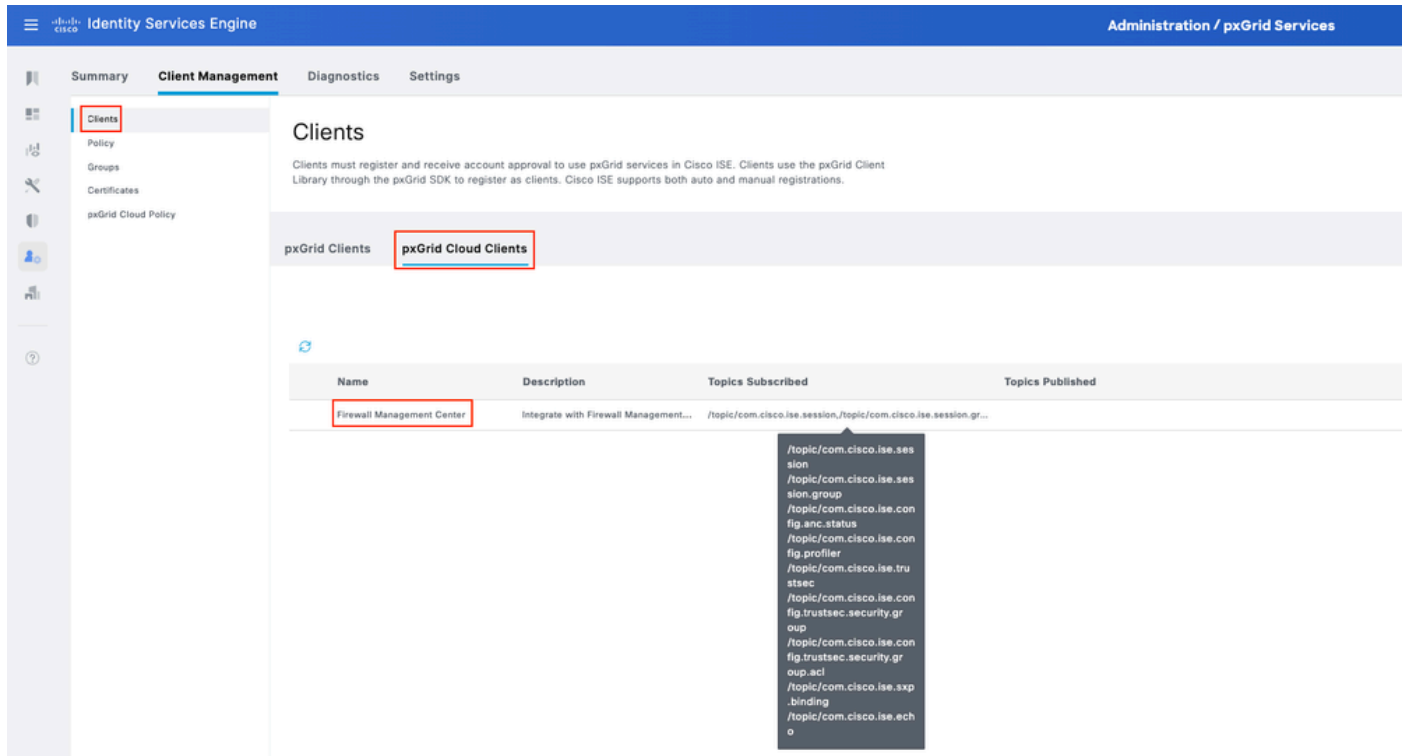
```
ise341-psn1/admin#show ports | include 8913
```

```
tcp:
```

127.0.0.1:8913

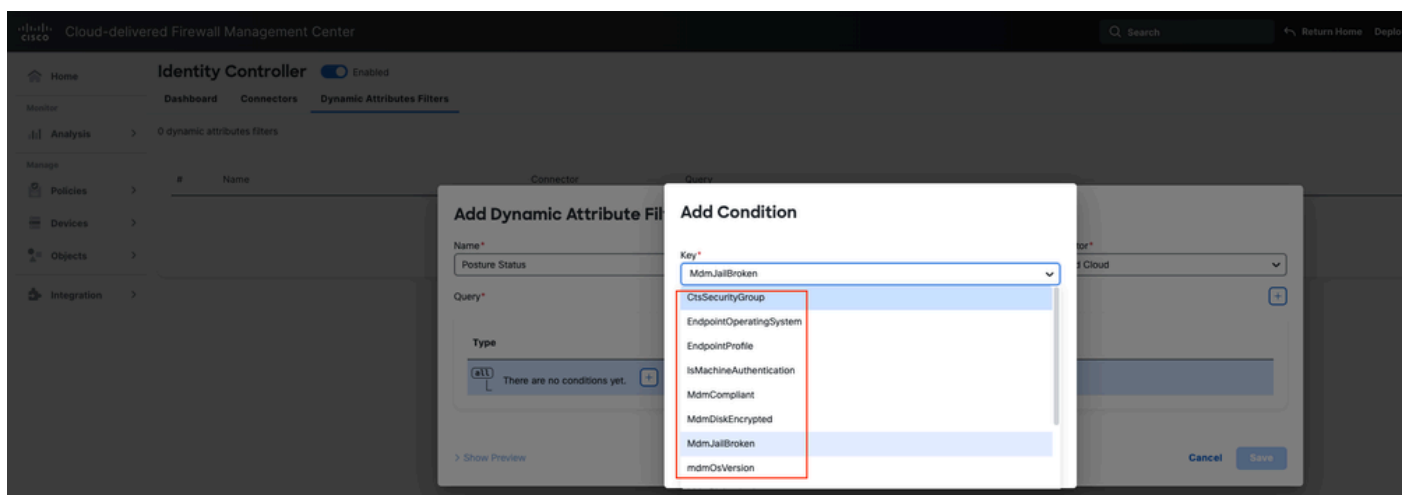
ise341-psn1/admin#

4. Überprüfen Sie den pxGrid-Cloud-Client, indem Sie zu Administration > pxGrid Services > Client Management > Clients > pxGrid Cloud Clients navigieren. Überprüfen Sie auch die abonnierten Themen.



pxGrid Cloud-Client auf der ISE

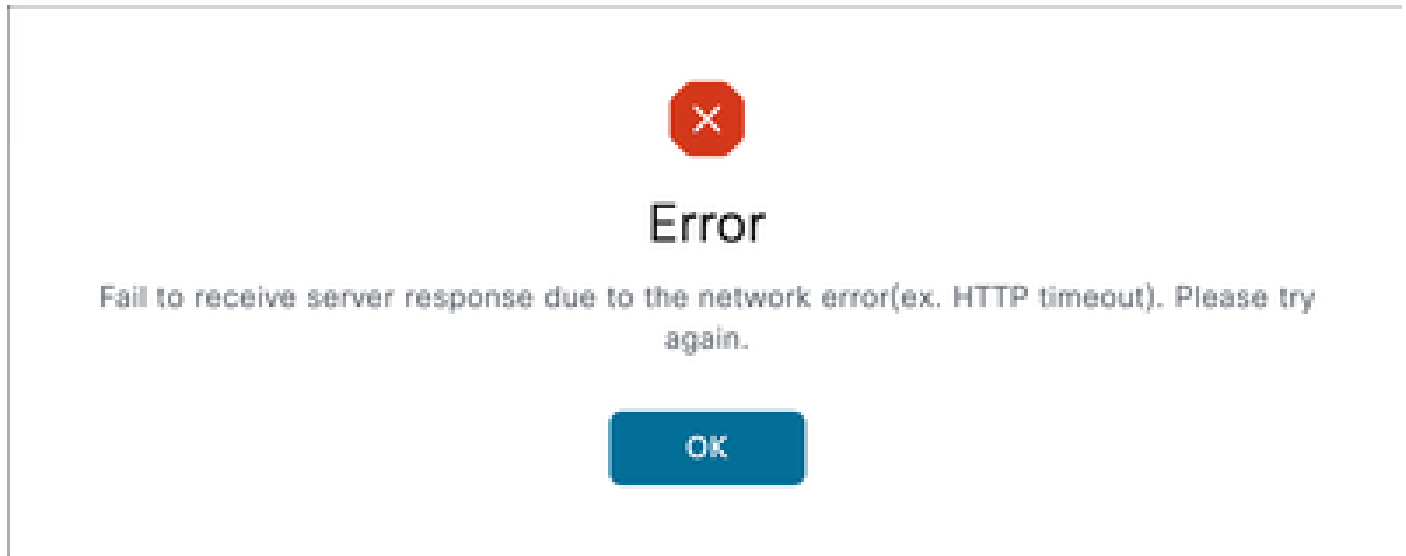
5. Stellen Sie sicher, dass die abonnierten Themen von cdFMC abgerufen werden. Klicken Sie im Security Cloud Control-Portal auf Policies > Threat Defense > Integration > Other Integrations > Identity Sources. Klicken Sie auf Identity Services Engine (pxGrid Cloud). Klicken Sie auf Configure Filters. Klicken Sie auf der Seite auf die Registerkarte Filter für dynamische Attribute. Erstellen Sie einen Filter für dynamische Attribute.



Attribute von ISE abgerufen

Fehlerbehebung

1. Fehler bei der ISE-Registrierung:



Fehlende Proxykonfiguration

Überprüfen Sie die Internetverbindung und mögliche Proxy-Fehlkonfigurationen.

2. Der pxGrid-Status zeigt nach der Aktivierung des pxGrid Cloud-Service und der Konfiguration der Name- und Regionsparameter Not connected auf der ISE Edit-Knotenseite an.

Überprüfen Sie hermes.log auf dem Knoten, auf dem Sie den pxGrid Cloud-Dienst aktivieren:

<#root>

ise341-psn1/admin#

show logging application hermes/hermes.log | begin 8913

2025-03-17T09:19:35.277Z | INFO | hermes/httpserver.go:57 |

Starting REST server on :8913

2025-03-17T09:19:35.285Z | INFO | hermes/httpserver.go:78 | REST server is up and running

2025-03-17T09:19:35.307Z | ERROR | hermes/pxgrid.go:194 | Failed to establish pxGrid WebSocket connection

"https://ise341-psn1.poongarg.local:8910/pxgrid/control/ServiceLookup": SSL errors: SSL routines:tls_pro

2025-03-17T09:19:35.307Z | ERROR | hermes/main.go:166 | Failed to open pxGrid WebSocket connection: Fai

2025-03-17T09:19:35.307Z | INFO | hermes/config.go:279 | Stopping monitoring of configuration file: /op

2025-03-17T09:19:35.307Z | INFO | hermes/connectionstatus.go:81 | Resetting connection status to DISCON

2025-03-17T09:19:35.308Z | ERROR | hermes/main.go:402 | Error running Hermes: Failed to establish pxGrid

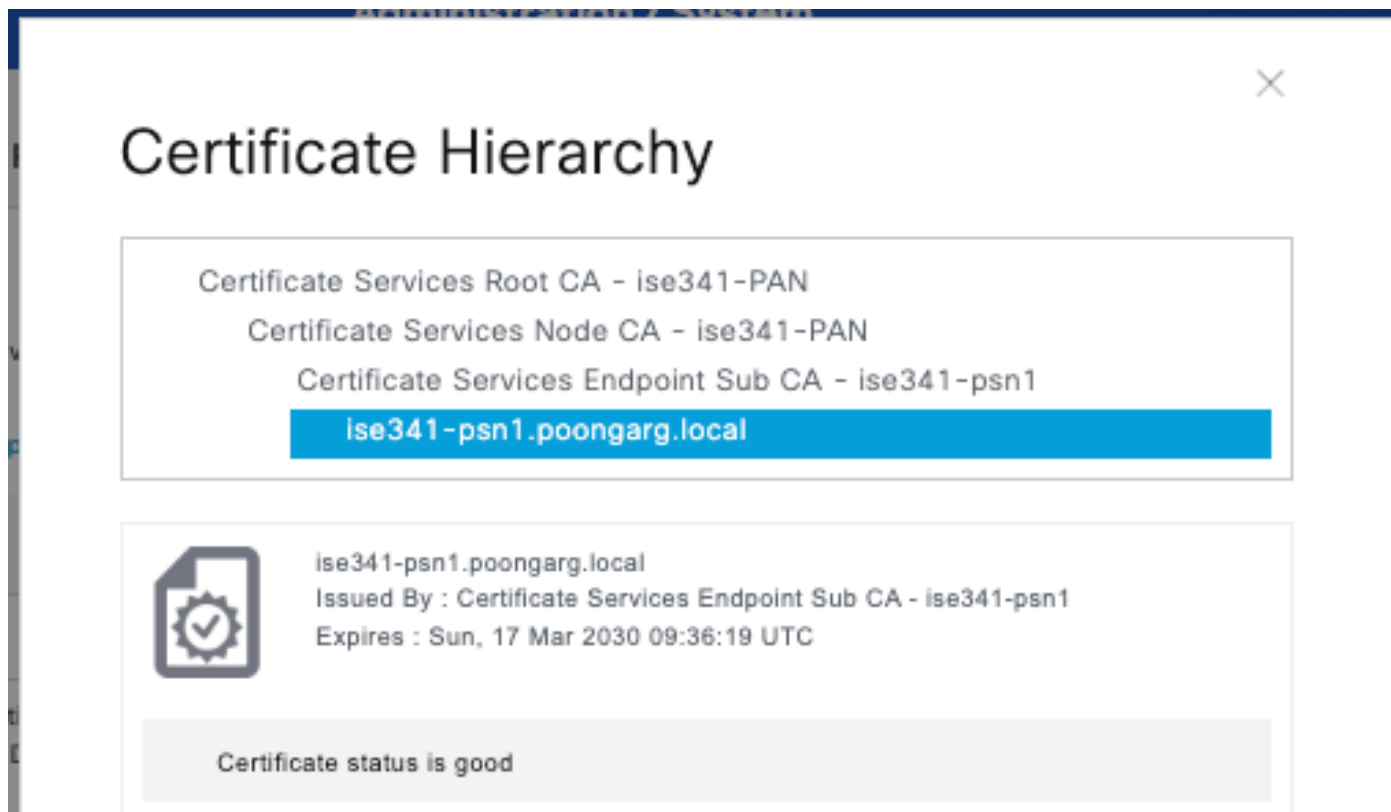
2025-03-17T09:19:35.308Z | INFO | hermes/httpserver.go:90 |

Stopping REST server on :8913

Hermes Rest Server lauscht auf Port 8913. Die Protokolle zeigen deutlich, dass der Hermes REST-Server versucht, eine pxGrid WebSocket-Verbindung herzustellen, jedoch aufgrund eines

Fehlers bei der Zertifikatsüberprüfung nicht.

Lösung: Überprüfen Sie, ob das pxGrid-Zertifikat gültig ist und die Zertifikatskette nicht unterbrochen ist. Zeigen Sie das Zertifikat an, und überprüfen Sie, ob der Zertifikatsstatus gültig ist. In diesem Fall war der ISE-Hostname im pxGrid-Zertifikat, das für diesen Knoten ausgestellt wurde, falsch.



Gültiges pxGrid-Zertifikat

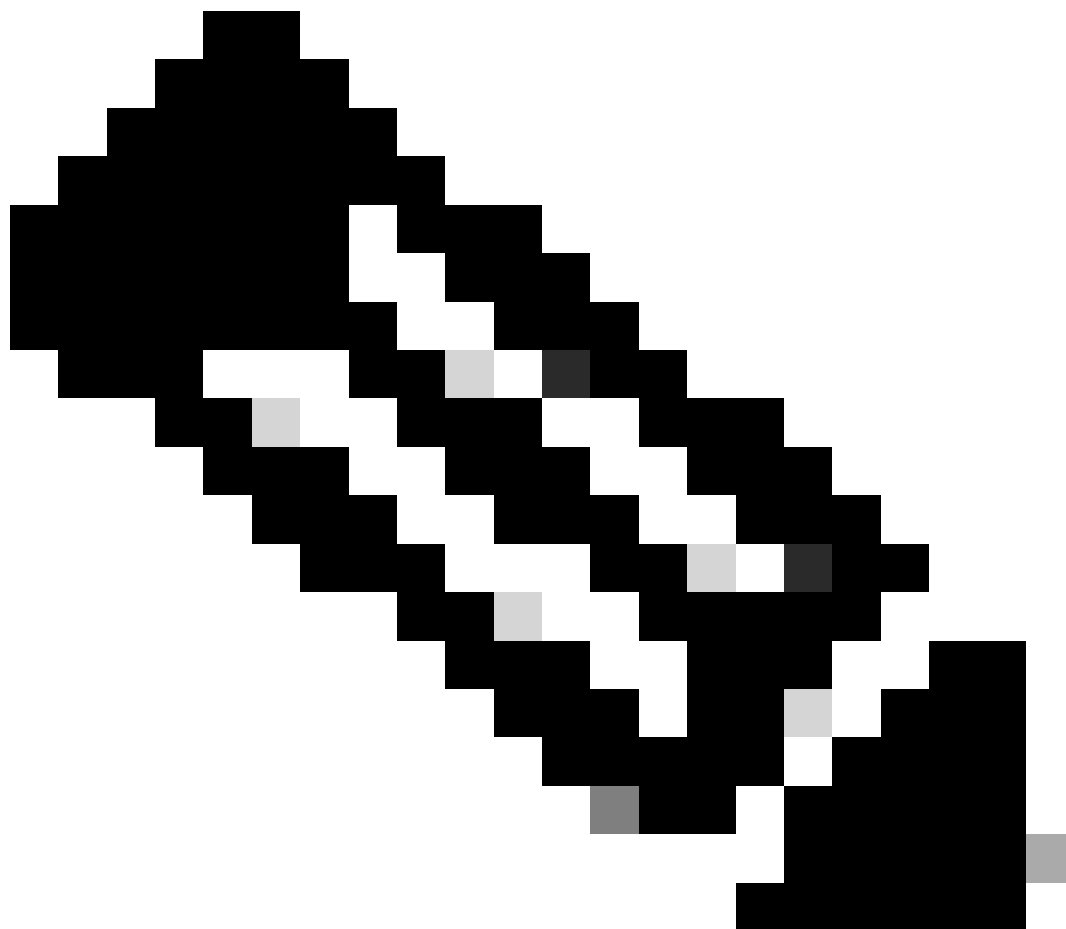
3. Fehler bei der Aktivierung der cdFMC-Anwendung auf dem Catalyst Cloud Portal.

Lösung: Stellen Sie sicher, dass auf der ISE unter der pxGrid-Cloud-Richtlinie die externen RESTful Services (ERS)-APIs und die OpenAPIs den schreibgeschützten Zugriff aktivieren.

Protokolle in Bezug auf pxGrid Cloud-Funktion:

Debug-Komponente	Protokolldateiname	Beschreibung
pxGrid-Cloud	pxcloud.log, hermes.log	pxcloud.log: Es protokolliert Konfigurationsänderungen des pxGrid-Cloud-Service, den Verbindungsstatus des pxGrid-Cloud-Service und den Hochverfügbarkeitsstatus.
pxGrid Cloud OpenAPI	pxcloud.log, hermes.log	hermes.log: protokolliert pxGrid Thema Abonnement-Status, ERS Rest Anfragen aus pxGrid

		Cloud, Konfigurationsänderungen auf ISE.
Telemetrie	z.B. Protokoll	Das Protokoll wird generiert, wenn der Benutzer den Integrationskatalog verwendet. Es enthält erste Protokolle mit Token, die für die Verbindung mit pxGrid Cloud verwendet werden.



Anmerkung: Unabhängig davon, auf welchem Knoten Sie die pxGrid Cloud-Person aktivieren, müssen Sie die Protokolle auf dem aktiven PAN-Knoten überprüfen. Nach der Registrierung des Geräts befinden sich die Hermes-Protokolle auf dem Knoten, auf dem es aktiviert ist.

Hermes.log unterstützt nur die Protokollstufen Debug, Info, Warn und Error. Wenn Sie also Trace auswählen, wird die Protokollstufe für hermes.log auf Debug festgelegt. Wenn Sie Fatal auswählen, wird die Protokollstufe für hermes.log auf Error (Fehler) festgelegt.

ISE-Registrierung und -Anwendung Aktivierungsablauf

Vor der Registrierung des Geräts verwendet die ISE einen Geräte-Token, um eine Liste der Regionen und Anwendungen aus der Cloud abzurufen. Dieses Token wird von der Telemetrikomponente der ISE bereitgestellt. Überprüfen Sie sch.log auf PAN-Knoten:

```
2025-03-17 09:10:23,361 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.DNATelemetryClient
2025-03-17 09:10:23,361 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.DNATelemetryClient
2025-03-17 09:10:23,463 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.TetheringStateManager
2025-03-17 09:10:23,467 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.TetheringStateManager
2025-03-17 09:10:23,480 INFO [openapi-http-pool7][[]] cisco.dna.tethering.client.TetheringClient -:::::
2025-03-17 09:10:23,480 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.DNATelemetryClient
2025-03-17 09:10:23,483 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.DNATetheringClient
2025-03-17 09:10:24,492 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.TetheringStateManager
2025-03-17 09:10:24,497 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.TetheringStateManager
2025-03-17 09:10:24,529 INFO [openapi-http-pool7][[]] cpm.infrastructure.telemetry.api.TelemetryConfigManager
```

pxcloud.log (PAN-Knoten), sobald Sie pxGrid Cloud-Service aktivieren, wird Hermes(pxGrid Cloud-Agent) aktiviert und ISE ruft die Regionsinformationen ab und erhält ein Token über die Telemetrikomponente.

```
2025-03-17 08:47:00,300 INFO [main][[]] cisco.cpm.pxcloud.api.PxCloudInitializer -:::::- Initializing pxcloud
2025-03-17 08:47:00,312 INFO [main][[]] cisco.cpm.pxcloud.pxgrid.PxCloudProviderRegistration -:::::- Registering
2025-03-17 08:47:00,314 INFO [main][[]] cisco.cpm.pxcloud.hermes.ProxyConfigNotificationHandler -:::::- Registering
2025-03-17 08:47:00,376 INFO [main][[]] cisco.cpm.pxcloud.hermes.HermesConfigManager -:::::- Registering
2025-03-17 08:47:00,376 INFO [main][[]] cisco.cpm.pxcloud.hermes.HermesConfigManager -:::::- Registering
2025-03-17 08:50:18,842 INFO [main][[]] cisco.cpm.pxcloud.hermes.HermesConfigManager -:::::- Updating Hermes
2025-03-17 08:52:46,834 INFO [pool-24-thread-1][[]] cpm.pxcloud.service.ui.IntegrationCatalogScheduler
2025-03-17 08:55:46,877 INFO [pool-24-thread-1][[]] cpm.pxcloud.service.ui.IntegrationCatalogScheduler
2025-03-17 08:58:46,781 INFO [pool-24-thread-1][[]] cpm.pxcloud.service.ui.IntegrationCatalogScheduler
2025-03-17 09:01:46,781 INFO [pool-24-thread-1][[]] cpm.pxcloud.service.ui.IntegrationCatalogScheduler
2025-03-17 09:03:37,136 INFO [pool-225-thread-1][[]] cpm.pxcloud.service.ui.IntegrationCatalogScheduler
2025-03-17 09:04:46,781 INFO [pool-24-thread-1][[]] cpm.pxcloud.service.ui.IntegrationCatalogScheduler
2025-03-17 09:06:37,136 INFO [pool-225-thread-1][[]] cpm.pxcloud.service.ui.IntegrationCatalogScheduler
2025-03-17 09:07:46,781 INFO [pool-24-thread-1][[]] cpm.pxcloud.service.ui.IntegrationCatalogScheduler
2025-03-17 09:09:11,901 DEBUG [hermes-change-monitor-0][[]] cisco.cpm.pxcloud.hermes.PxCloudNodeChangeListener
2025-03-17 09:09:37,136 INFO [pool-225-thread-1][[]] cpm.pxcloud.service.ui.IntegrationCatalogScheduler
2025-03-17 09:09:37,139 DEBUG [pool-225-thread-1][[]] cpm.pxcloud.service.ui.IntegrationCatalogScheduler
2025-03-17 09:10:22,475 TRACE [openapi-http-pool4][[]] cpm.iseopenapi.pxcloud.impl.PxGridApiDelegateImpl
2025-03-17 09:10:22,485 INFO [openapi-http-pool4][[]] cpm.pxcloud.service.ui.IseEnrollment -:::::- Fetching
2025-03-17 09:10:22,739 TRACE [openapi-http-pool7][[]] cpm.iseopenapi.pxcloud.impl.PxGridApiDelegateImpl
2025-03-17 09:10:22,750 INFO [openapi-http-pool7][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -:::::-
2025-03-17 09:10:22,754 DEBUG [openapi-http-pool7][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -:::::-
2025-03-17 09:10:24,529 DEBUG [openapi-http-pool7][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -:::::-
2025-03-17 09:10:24,537 INFO [openapi-http-pool7][[]] cisco.cpm.pxcloud.utils.PxCloudHttpClient -:::::-
```



```
2025-03-17 09:10:26,938 DEBUG [openapi-http-pool7][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -
2025-03-17 09:10:26,946 DEBUG [openapi-http-pool7][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -
id: ap-southeast-1
name: ap-southeast-1
fqdn: neoffers-sg.cisco.com
}, class Region {
id: eu-central-1
name: eu-central-1
fqdn: neoffers-de.cisco.com
}, class Region {
id: us-west-2
name: us-west-2
fqdn: neoffers.cisco.com
}}
2025-03-17 09:10:26,968 DEBUG [openapi-http-pool7][[]] cpm.pxcloud.api.impl.PxcloudApplicationCatalogImp
2025-03-17 09:10:27,051 INFO [openapi-http-pool7][[]] cpm.pxcloud.api.impl.PxcloudApplicationCatalogImp
2025-03-17 09:10:27,055 DEBUG [openapi-http-pool7][[]] cisco.cpm.pxcloud.utils.PxCloudUtils -::::- An
2025-03-17 09:10:27,533 DEBUG [openapi-http-pool7][[]] cpm.pxcloud.api.impl.PxcloudApplicationCatalogImp
2025-03-17 09:10:27,533 DEBUG [openapi-http-pool7][[]] cpm.pxcloud.api.impl.PxcloudApplicationCatalogImp
2025-03-17 09:10:27,533 DEBUG [openapi-http-pool7][[]] cpm.pxcloud.api.impl.PxcloudApplicationCatalogImp
2025-03-17 09:10:27,533 DEBUG [openapi-http-pool7][[]] cisco.cpm.pxcloud.utils.PxCloudHttpClient -::::-
!
2025-03-17 09:10:37,338 INFO [openapi-http-pool7][[]] cpm.pxcloud.api.impl.PxcloudApplicationCatalogImp
```

Der Aktivierungslink wird empfangen, die automatische Registrierung und Registrierung erfolgen.

```
2025-03-17 09:16:42,536 TRACE [openapi-http-pool2][[]] cpm.iseopenapi.pxcloud.impl.PxGridApiDelegateImp
2025-03-17 09:16:42,537 DEBUG [openapi-http-pool2][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -
2025-03-17 09:16:42,569 DEBUG [openapi-http-pool2][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -
2025-03-17 09:16:42,569 DEBUG [openapi-http-pool2][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -
!
2025-03-17 09:16:44,729 DEBUG [openapi-http-pool2][[]] cisco.cpm.pxcloud.api.PxCloudPropertiesNotificat
2025-03-17 09:16:44,735 DEBUG [openapi-http-pool2][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -
2025-03-17 09:16:45,310 TRACE [openapi-http-pool3][[]] cpm.iseopenapi.pxcloud.impl.PxGridApiDelegateImp
2025-03-17 09:16:45,345 INFO [openapi-http-pool3][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -
!
2025-03-17 09:16:45,538 INFO [openapi-http-pool3][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -
2025-03-17 09:16:45,589 DEBUG [openapi-http-pool3][[]] cisco.cpm.pxcloud.utils.PxCloudHttpClient -::::-
2025-03-17 09:16:46,805 INFO [pool-24-thread-1][[]] cpm.pxcloud.service.ui.IntegrationCatalogScheduler
2025-03-17 09:16:46,816 DEBUG [pool-24-thread-1][[]] cpm.pxcloud.service.ui.IntegrationCatalogScheduler
2025-03-17 09:16:47,631 DEBUG [openapi-http-pool3][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -
!
2025-03-17 09:19:14,196 INFO [openapi-http-pool9][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -
2025-03-17 09:19:14,196 INFO [openapi-http-pool9][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -
2025-03-17 09:19:14,199 DEBUG [openapi-http-pool9][[]] cisco.cpm.pxcloud.utils.PxCloudHttpClient -::::-
2025-03-17 09:19:16,956 DEBUG [openapi-http-pool9][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -
2025-03-17 09:19:16,964 DEBUG [openapi-http-pool9][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -
2025-03-17 09:19:16,964 INFO [openapi-http-pool9][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -
2025-03-17 09:19:16,964 INFO [openapi-http-pool9][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -
2025-03-17 09:19:17,284 INFO [openapi-http-pool9][[]] cpm.pxcloud.service.ui.IseEnrollment -::::- ISE
2025-03-17 09:19:17,284 DEBUG [openapi-http-pool9][[]] cpm.pxcloud.service.ui.IseEnrollment -::::- ISE
2025-03-17 09:19:17,306 DEBUG [openapi-http-pool9][[]] cisco.cpm.pxcloud.api.PxCloudPropertiesNotificat
2025-03-17 09:19:17,325 DEBUG [openapi-http-pool9][[]] cisco.cpm.pxcloud.api.PxCloudPropertiesNotificat
2025-03-17 09:19:17,342 DEBUG [openapi-http-pool9][[]] cisco.cpm.pxcloud.api.PxCloudPropertiesNotificat
2025-03-17 09:19:17,369 DEBUG [openapi-http-pool9][[]] cisco.cpm.pxcloud.api.PxCloudPropertiesNotificat
2025-03-17 09:19:17,394 DEBUG [openapi-http-pool9][[]] cisco.cpm.pxcloud.api.PxCloudPropertiesNotificat
2025-03-17 09:19:17,418 DEBUG [openapi-http-pool9][[]] cisco.cpm.pxcloud.api.PxCloudPropertiesNotificat
```

```

2025-03-17 09:19:17,438 DEBUG [openapi-http-pool9][[]] cisco.cpm.pxcloud.api.PxCloudPropertiesNotificat
2025-03-17 09:19:17,463 DEBUG [openapi-http-pool9][[]] cisco.cpm.pxcloud.api.PxCloudPropertiesNotificat
2025-03-17 09:19:17,485 DEBUG [openapi-http-pool9][[]] cisco.cpm.pxcloud.api.PxCloudPropertiesNotificat
2025-03-17 09:19:17,489 INFO [openapi-http-pool9][[]] cpm.pxcloud.service.ui.IseEnrollment -:::::- ISE
2025-03-17 09:19:17,495 INFO [openapi-http-pool9][[]] cpm.pxcloud.service.ui.IseEnrollment -:::::- ISE
2025-03-17 09:19:17,500 INFO [openapi-http-pool9][[]] cpm.pxcloud.service.ui.IseEnrollment -:::::- Init
2025-03-17 09:19:17,500 INFO [openapi-http-pool9][[]] cpm.pxcloud.api.impl.DeviceRegistrationApiImpl -:
2025-03-17 09:19:17,554 INFO [openapi-http-pool9][[]] cpm.iseopenapi.pxcloud.util.PxGridCloudUtil -::::
2025-03-17 09:19:17,554 DEBUG [openapi-http-pool9][[]] cpm.iseopenapi.pxcloud.util.PxGridCloudUtil -::::
2025-03-17 09:19:18,501 INFO [pxcloud-configuration-1243][[]] cpm.pxcloud.service.ui.CloudConfiguration
2025-03-17 09:19:18,505 DEBUG [pxcloud-configuration-1243][[]] cpm.pxcloud.service.ui.CloudConfiguration

```

pxGrid-Knoten übernehmen AKTIVE Rolle, aber hier beobachteten wir pxGridConnectionStatus als NOT_CONNECTED, die behoben wurde, nachdem das richtige pxGrid-Zertifikat (mit vollständiger Wurzel-CA-Kette) auf diesem pxGrid-Knoten hinzugefügt wurde.

```

2025-03-17 09:20:12,301 TRACE [openapi-http-pool8][[]] cpm.iseopenapi.pxcloud.impl.PxGridApiDelegateImp
2025-03-17 09:20:12,301 INFO [openapi-http-pool8][[]] cpm.pxcloud.service.ui.IseEnrollment -:::::- Fetc
2025-03-17 09:20:12,310 INFO [Thread-150][[]] cpm.pxcloud.service.ui.IseEnrollment -:::::- Get pxCloud
2025-03-17 09:20:12,311 INFO [Thread-150][[]] cpm.pxcloud.service.ui.IseEnrollment -:::::- pxCloud stat
2025-03-17 09:20:12,427 INFO [Thread-150][[]] cpm.pxcloud.service.ui.IseEnrollment -:::::- Received res

```

Überprüfen Sie jetzt Hermes.log auf dem ACTIVE pxGrid-Knoten auf pubsub-Ereignisse:

```

2025-03-17T09:37:43.906Z | INFO | hermes/config.go:332 | configMgr created successfully: configMgr[path
2025-03-17T09:37:43.907Z | INFO | hermes/config.go:117 | Parsing configuration file: /opt/hermes/config
2025-03-17T09:37:43.907Z | INFO | hermes/config.go:338 | Config file /opt/hermes/config.yaml parsed suc
2025-03-17T09:37:43.907Z | INFO | hermes/main.go:126 | Configuration loaded successfully
2025-03-17T09:37:43.908Z | INFO | trust/trust.go:28 | Custom trust bundle has been set/updated
2025-03-17T09:37:43.908Z | INFO | hermes/pxgrid.go:187 | Creating pxGrid WebSocket connection
2025-03-17T09:37:43.908Z | INFO | hermes/httpserver.go:57 | Starting REST server on :8913
2025-03-17T09:37:43.921Z | INFO | hermes/httpserver.go:78 | REST server is up and running
2025-03-17T09:37:43.983Z | INFO | pxgrid/websocket.go:93 | Got WS URL: wss://ise341-psn1.poongarg.local
2025-03-17T09:37:44.066Z | INFO | pxgrid/websocket.go:107 | Connection to wss://ise341-psn1.poongarg.lo
2025-03-17T09:37:44.066Z | INFO | hermes/connectionstatus.go:44 | Setting pxGrid connection status to C

```

Die Root-CA-Kette des Catalyst Cloud Portal wird verifiziert.

```

2025-03-17T09:37:44.731Z | INFO | hermes/pxgrid.go:267 | Cloud credentials are obtained from ISE
2025-03-17T09:37:45.034Z | INFO | hermes/pxgrid.go:376 | DeviceID: 67d7e91688c5fd08d0860039, TenantID:
2025-03-17T09:37:45.743Z | INFO | rest/ocsp.go:207 | Making OCSP request at http://commercial.ocsp.iden
2025-03-17T09:37:45.743Z | INFO | rest/ocsp.go:207 | Making OCSP request at http://commercial.ocsp.iden
2025-03-17T09:37:46.273Z | INFO | rest/ocsp.go:254 | OCSP Validation passed for CN=HydrantID Server CA
2025-03-17T09:37:46.279Z | INFO | rest/ocsp.go:254 | OCSP Validation passed for CN=dnaservices.cisco.co
2025-03-17T09:37:47.054Z | INFO | rest/ocsp.go:207 | Making OCSP request at http://commercial.ocsp.iden
2025-03-17T09:37:47.432Z | INFO | hermes/config.go:262 | File /opt/hermes/config.yaml modified. Event:
2025-03-17T09:37:47.533Z | INFO | hermes/config.go:117 | Parsing configuration file: /opt/hermes/config
2025-03-17T09:37:47.533Z | INFO | hermes/config.go:305 | New configuration loaded

```

2025-03-17T09:37:47.533Z | INFO | hermes/config.go:314 | Restarting Hermes due to configuration change

Die Abonnementanforderung für bestimmte Themen wurde einmal erstellt. Die FMC-Anwendung ist unter Integration Catalog konfiguriert:

```
2025-03-17T12:54:09.975Z | INFO | pxgrid/subscriber.go:40 | Request to create new subscriber: service=c
2025-03-17T12:54:09.975Z | INFO | pxgrid/subscriber.go:55 | Subscriber[service: com.cisco.ise.session,
2025-03-17T12:54:10.263Z | INFO | device-manager@v1.1.12/control.go:240 | Completed activate sync ID [s
2025-03-17T12:54:10.263Z | INFO | device-manager@v1.1.12/control.go:227 | Processing activate sync ID [
2025-03-17T12:54:10.263Z | INFO | hermes/pxgrid.go:117 | Request to add new pxGrid subscriber [com.cisco
2025-03-17T12:54:10.263Z | INFO | pxgrid/subscriber.go:28 | Request to create new subscriber: com.cisco
2025-03-17T12:54:10.270Z | INFO | pxgrid/subscriber.go:40 | Request to create new subscriber: service=c
2025-03-17T12:54:10.270Z | INFO | pxgrid/subscriber.go:55 | Subscriber[service: com.cisco.ise.config.pr
2025-03-17T12:54:10.559Z | INFO | device-manager@v1.1.12/control.go:240 | Completed activate sync ID [p
2025-03-17T12:54:10.559Z | INFO | device-manager@v1.1.12/control.go:227 | Processing activate sync ID [
2025-03-17T12:54:10.559Z | INFO | hermes/pxgrid.go:117 | Request to add new pxGrid subscriber [com.cisco
2025-03-17T12:54:10.559Z | INFO | pxgrid/subscriber.go:28 | Request to create new subscriber: com.cisco
!
2025-03-17T16:17:30.050Z | INFO | api-proxy@v1.0.10/broker.go:114 | API-Proxy: Broker Agent start consu
2025-03-17T16:17:30.050Z | INFO | hermes/apiproxy.go:43 | API Proxy connection established
2025-03-17T16:17:30.050Z | INFO | hermes/connectionstatus.go:62 | Setting cloud connection status to CO
2025-03-17T16:17:30.057Z | INFO | hermes/dxhub.go:94 | Policies are obtained from ISE : &{Pxgrid:{Conte
```

Einschränkungen

1. Der Benutzer kann pxGrid Cloud-Persona nicht auf mehr als 2 Knoten aktivieren.
2. Die Deregistrierung vom Catalyst Cloud Portal zu cdFMC wird unterstützt, aber nicht umgekehrt.

Referenzen

[Benutzerkontrolle mit der pxGrid Cloud-Identitätsquelle](#)

[Cisco pxGrid-Cloud](#)

[Cisco pxGrid Cloud-Lösungsleitfaden](#)

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.