

Integrazione di Firewall Management Center distribuito tramite cloud con ISE tramite pxGrid Cloud

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Terminologia Cisco pxGrid Cloud](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Importa il certificato del server Cisco pxGrid Cloud in ISE](#)

[Diagramma di flusso](#)

[Registrazione di ISE con Catalyst Cloud Portal](#)

[Attivare l'applicazione cdFMC su ISE utilizzando Integration Catalog](#)

[Crea istanza applicazione pxGrid \(cdFMC\)](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Iscrizione/registrazione ad ISE e applicazione. Flusso di attivazione](#)

[Limitazioni](#)

[Riferimenti](#)

Introduzione

Questo documento descrive la procedura per integrare Cisco ISE con Firewall Management Center (cdFMC) distribuito su cloud tramite pxGrid Cloud.

Prerequisiti

- Conoscenza pratica di Cisco Identity Service Engine (ISE)
- Un account nel portale Cisco Catalyst Cloud
- Un account sul portale Cisco Security Cloud Control

Requisiti

- Installare e attivare il livello di licenza Advantage nell'implementazione di Cisco ISE.
- L'agente pxGrid Cloud crea una connessione HTTPS in uscita a Cisco pxGrid Cloud.

Pertanto, configurare le impostazioni del proxy Cisco ISE se la rete utilizza un proxy per raggiungere Internet. Per configurare le impostazioni proxy in Cisco ISE, scegliere Amministrazione > Sistema > Impostazioni > Proxy.

- L'archivio dei certificati attendibili di Cisco ISE deve includere il certificato CA radice necessario per convalidare il certificato del server presentato da Cisco pxGrid Cloud. Verificare che l'opzione Trust for Authentication of Cisco Services sia abilitata per questo certificato CA radice. Per abilitare l'attendibilità per l'autenticazione dei servizi Cisco, scegliere Amministrazione > Sistema > Certificati.
- Verificare che la porta 443 sia aperta per la connessione in uscita da Cisco ISE al Cisco pxGrid Cloud Portal. Se sono configurate le impostazioni del firewall o del proxy, verificare che gli URL non siano bloccati.

<https://dna.cisco.com>

<https://dnaservices.cisco.com>

<https://ciscodnacloud.com>

Componenti usati

Versione del software ISE: 3.4 Distribuzione di patch 1, 4 nodi (PAN, SAN e 2 PSN con il servizio pxGrid abilitato)

versione cdFMC: 20241127

Cisco Firepower Threat Defense (FTD) per VMware versione: 7.2.5

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.

Terminologia Cisco pxGrid Cloud

Di seguito sono riportati alcuni dei termini comuni utilizzati nella soluzione Cisco pxGrid Cloud e il relativo significato nell'ambiente Cisco pxGrid Cloud:

- Offerta: Un insieme di funzionalità combinate e offerte come soluzione
- Sottoscrizione: Un'istanza di un'offerta utilizzata da un tenant è una sottoscrizione
- App: È possibile creare e registrare applicazioni per il prodotto in base alle proprie esigenze.

Premesse

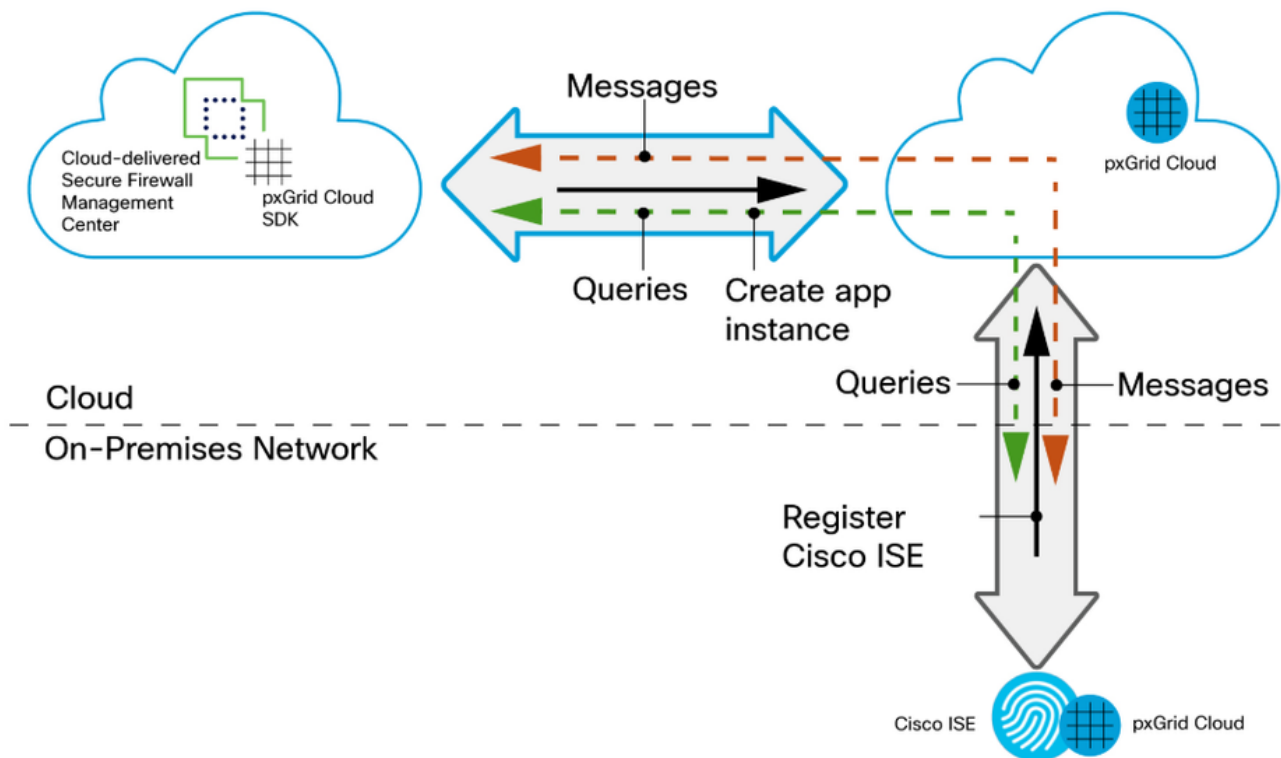
Cisco ISE offre la condivisione del contesto tra più fornitori di servizi di sicurezza; tuttavia, l'architettura corrente non consente la comunicazione tra l'ISE locale e le soluzioni basate sul cloud attraverso il perimetro della rete senza alcun tipo di bypass o buchi nel firewall.

Cisco ISE pxCloud è una soluzione basata su cloud che risolve questo problema e consente la condivisione del contesto tra cloud e locale senza ulteriori installazioni, sovraccarichi e compromettendo la sicurezza della rete. È sicuro e personalizzabile, consentendo di condividere solo i dati che si desidera condividere e utilizzare solo i dati contestuali rilevanti per l'applicazione.

Cisco ISE release 3.1 patch 3 e successive supportano pxGrid Cloud. Cisco e i suoi partner possono sviluppare applicazioni basate su pxGrid Cloud e registrarle con l'offerta pxGrid Cloud. Si basa sul portale cisco DNA-Cloud per integrare e registrare applicazioni senza dipendere da altre infrastrutture locali. Queste applicazioni utilizzano i servizi esterni RESTful (ERS), le API aperte e pxGrid (API e websocket) per scambiare informazioni con Cisco ISE e utilizzare i dati utente e di abbonamento da ISE in cdFMC.

Configurazione

Esempio di rete



Integrazione di cdFMC e ISE tramite pxGrid Cloud

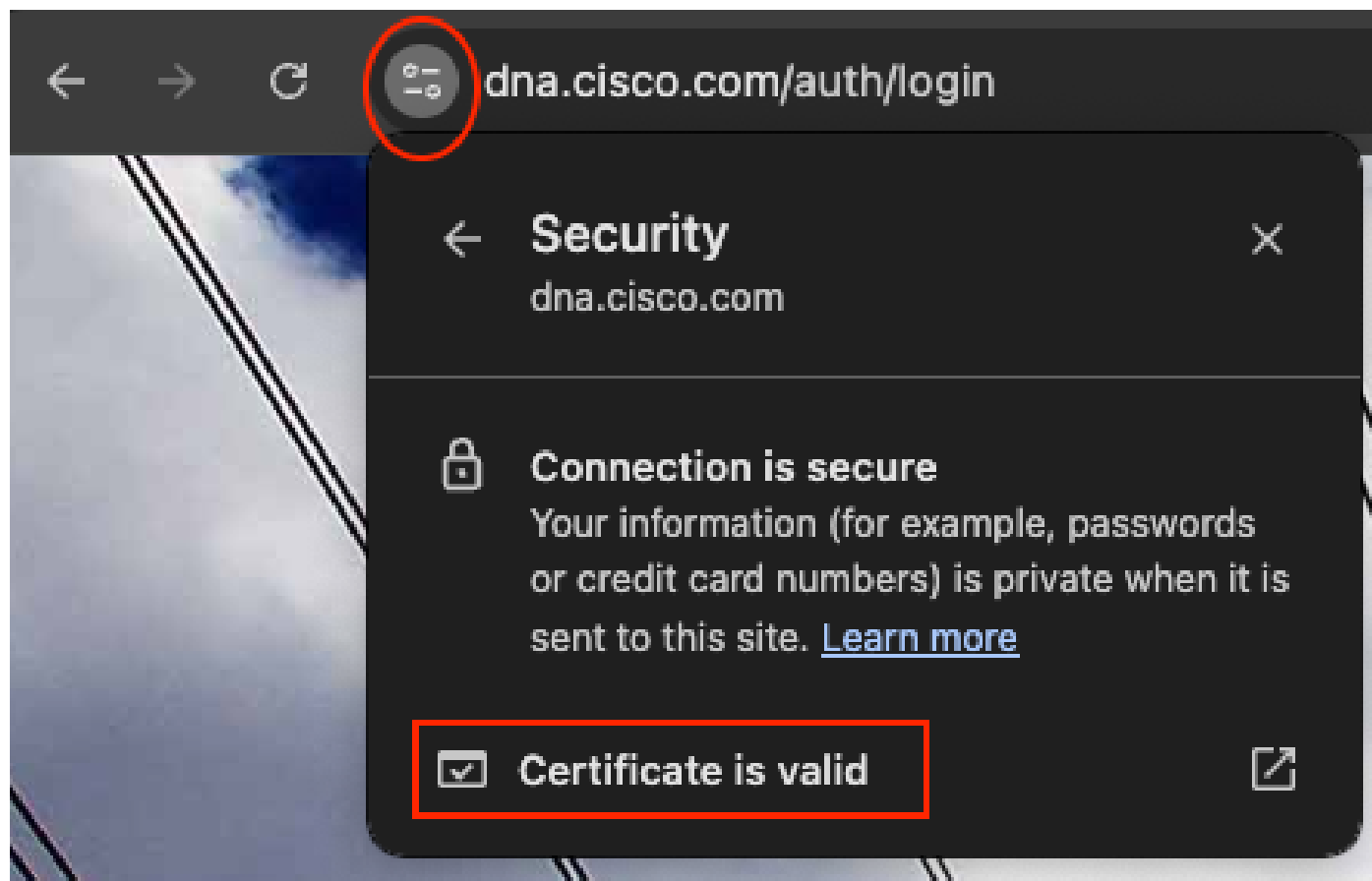
Configurazioni

Le quattro principali azioni da intraprendere sono:

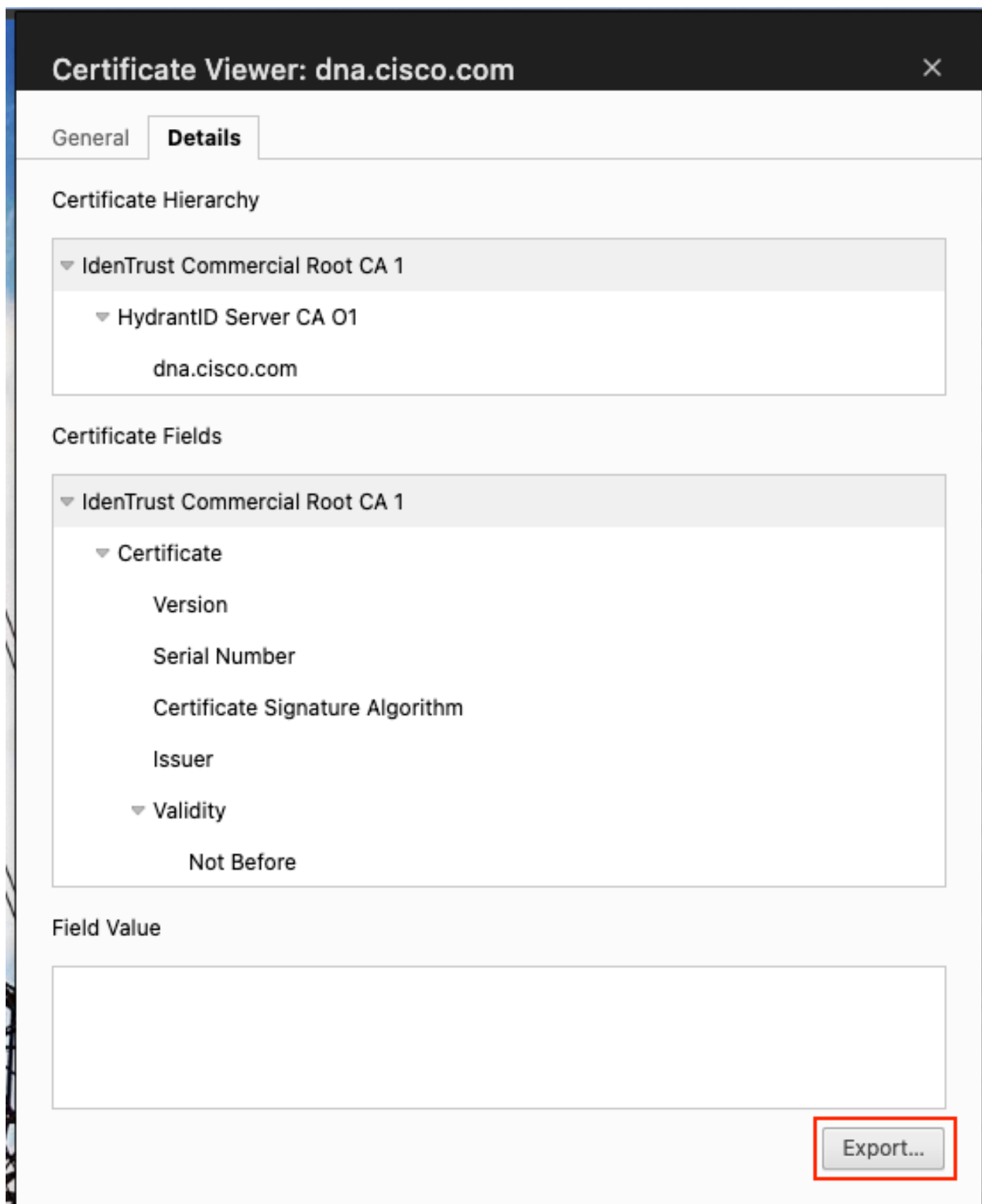
- Importare il certificato del server Cisco pxGrid Cloud in ISE.
- Registra ISE con Catalyst Cloud Portal.
- Attivare l'applicazione cdFMC su ISE utilizzando Integration Catalog
- Crea istanza applicazione pxGrid (cdFMC)

Importa il certificato del server Cisco pxGrid Cloud in ISE

ISE deve stabilire una relazione di fiducia con Cisco pxGrid Cloud. Anche se il sito Web del cloud è autenticato con un certificato firmato pubblicamente, ISE non mantiene un elenco completo di CA radice attendibili. Pertanto, l'amministratore deve stabilire una relazione di trust. Esportare i certificati radice e intermedi del cloud pxGrid selezionando [Catalyst Cloud Portal](#). La maggior parte dei browser lo consente. Ecco i passaggi per ottenere il certificato da Chrome Browser.



Visualizzazione delle informazioni sul sito



Esporta catena di certificati

Importare i certificati nell'archivio "Trusted Certificates" di ISE se la catena di certificati non è presente (ISE dispone già di IdemTrust Commercial Root CA 1).

Verificare che l'opzione "Trust for Authentication of Cisco Services" sia abilitata per questo

certificato CA radice. Per abilitare l'attendibilità per l'autenticazione dei servizi Cisco, scegliere Amministrazione > Sistema > Certificati.

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

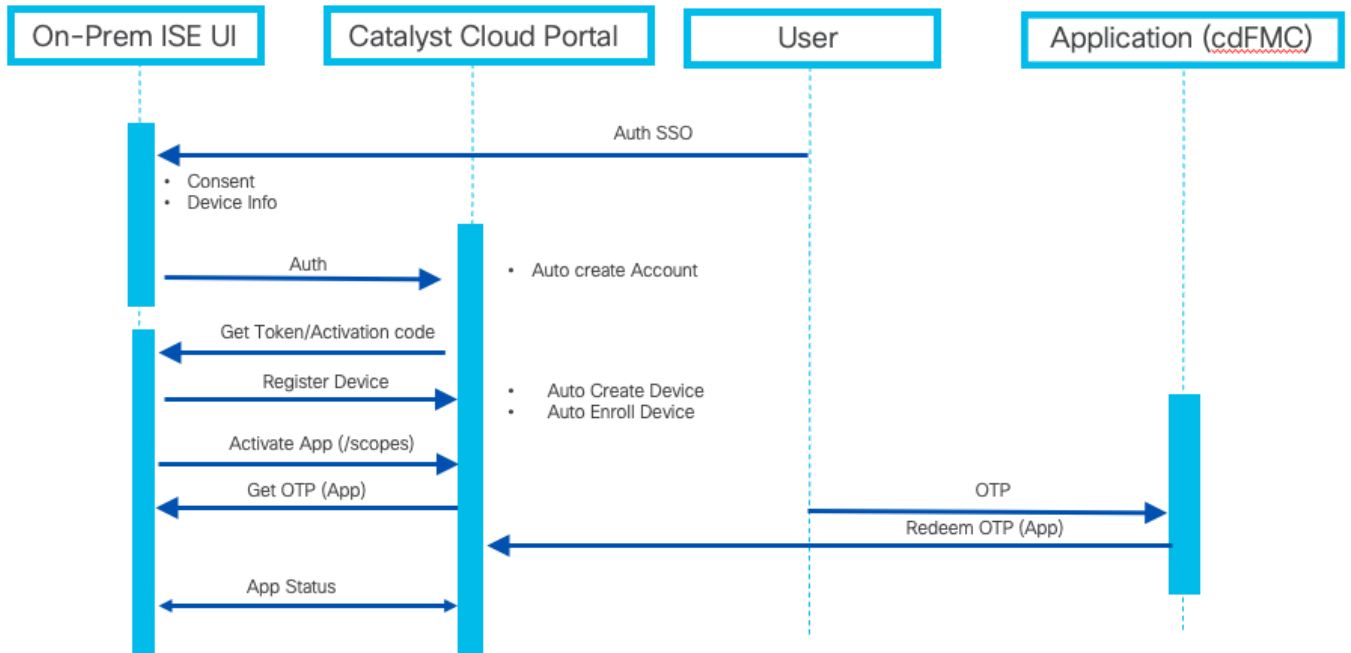
☒ Trust for authentication of Cisco Services

☐ Trust for Native IPSec certificate based authentication

Abilita attendibilità per l'autenticazione dei servizi Cisco

Diagramma di flusso

App Activation Workflow



Flusso di lavoro di attivazione app

Installazione ISE utilizzata in questa installazione

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	 

Registrazione di ISE con Catalyst Cloud Portal

Abilitare il servizio pxGrid Cloud in Cisco ISE e registrare il dispositivo.

1. Nell'interfaccia utente di Cisco ISE, scegliere Amministrazione > Sistema > Distribuzione.
2. Fare clic sul nodo in cui si desidera abilitare il servizio cloud pxGrid (in questo caso il primo nodo PSN).
3. Nella scheda Impostazioni generali, abilitare il servizio pxGrid.
4. Selezionare la casella di controllo pxGrid Cloud.



Nota: Il servizio pxGrid Cloud può essere abilitato solo su due nodi per abilitare l'alta disponibilità. È possibile abilitare l'opzione pxGrid Cloud solo quando il servizio pxGrid è abilitato su quel nodo.

5. Nel campo ISE deployment name (Nome distribuzione ISE), immettere un nome significativo. Questo nome viene mostrato nel portale Catalyst Cloud e può essere usato per distinguere se più distribuzioni ISE sono registrate con il cloud. È possibile verificare l'implementazione Cisco ISE registrata sul portale Cisco Catalyst Cloud usando il nome dell'implementazione ISE.

(Facoltativo) Nel campo Description (Descrizione) (facoltativo), immettere una descrizione per l'implementazione di Cisco ISE.

6. Nell'elenco a discesa Region (Area), scegliere un'area per registrare il dispositivo Cisco ISE. Cisco pxGrid Cloud è ora supportato in Europa, Asia, Pacifico e Giappone, oltre che negli Stati Uniti. Si noti che l'applicazione che si desidera utilizzare con pxGrid Cloud deve essere disponibile anche nella stessa area.

7. Fare clic su Registra.

The screenshot shows the Cisco ISE Administration interface. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (highlighted), Work Centers, and Interactive Help. The top navigation bar includes: Deployment (active), Licensing, Certificates, Logging, Maintenance, Upgrade & Rollback, Health Checks, Backup & Restore, Admin Access, and Settings.

Under the **Deployment** tab, the **pxGrid** section is expanded, showing a toggle switch for **pxGrid** (turned on) and a checkbox for **Enable pxGrid Cloud** (checked). A yellow warning message states: "pxGrid Cloud can be enabled only after registering your Cisco ISE to your Cisco DNA Portal account."

The registration form includes the following fields and options:

- ISE deployment name:** ISE341-PSN1
- Description (optional):** Primary pxGrid node
- Region:** us-west-2
- Checkboxes:**
 - ☒ 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](#).
- Buttons:** Register, Reset, Save

Registra ISE PSN con pxGrid Cloud

8. Nella pagina popup Attiva il dispositivo, il codice di attivazione del dispositivo viene compilato automaticamente. Fare clic su Next (Avanti).



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](#)



Nota: Quando si abilita la persona "pxGrid Cloud" sul secondo nodo, ISE non necessita di tutti questi dettagli, in quanto la registrazione di ISE con pxGrid Cloud è a livello di implementazione.

9. Accedere all'account [Cisco Catalyst Cloud Portal](#) usando le credenziali di accesso. Se non si dispone delle credenziali di accesso, creare un nuovo account per completare la registrazione del dispositivo. Per ulteriori informazioni, vedere [Creare un account sul portale del cloud Cisco Catalyst](#)

Il dispositivo Cisco ISE è attivato e registrato.



Nota: L'elenco delle applicazioni dipende dall'account. Alcune applicazioni potrebbero essere esposte solo ad account specifici.

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

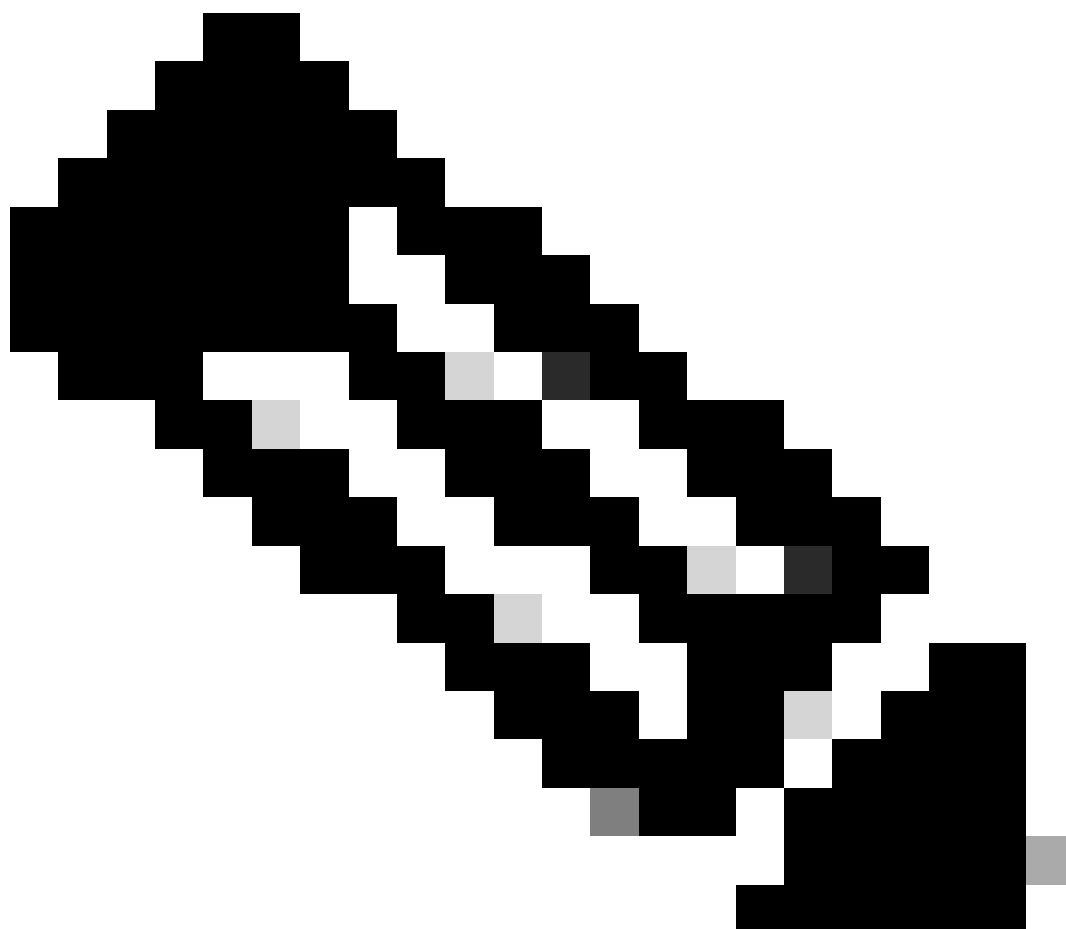
us-west-2 eu-central-1

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. Nella sezione Configurazione app, Seleziona nuova istanza e scegli gli ambiti dati per la configurazione della tua app. Scegliere almeno un ambito dati per continuare.



Nota: Quando si seleziona un ambito dati, lo stesso viene abilitato anche nelle impostazioni dei criteri cloud pxGrid a livello di sistema.

4. Fare clic su Attiva per attivare l'app.

Identity Services Engine

Administration / Integration Catalog

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

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

Device name

ISE341-PSN1

Description

Primary pxGrid node

Status

Registered

Registered region

us-west-2

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

Configurazione dell'applicazione FMC su ISE

5. Dal popup One-Time Password (OTP), copiare OTP per riscattarlo su cdFMC durante la creazione dell'istanza dell'applicazione pxGrid

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 per applicazione cdFMC

6. Configurare il criterio cloud pxGrid passando a Amministrazione > pxgrid Services > Gestione client > criterio cloud pxGrid. Selezionare i servizi pxGrid che si desidera condividere con le applicazioni SaaS e abilitare le API ERS (External RESTful Services) e OpenAPI per l'accesso in sola lettura alle applicazioni cloud Cisco pxGrid.

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

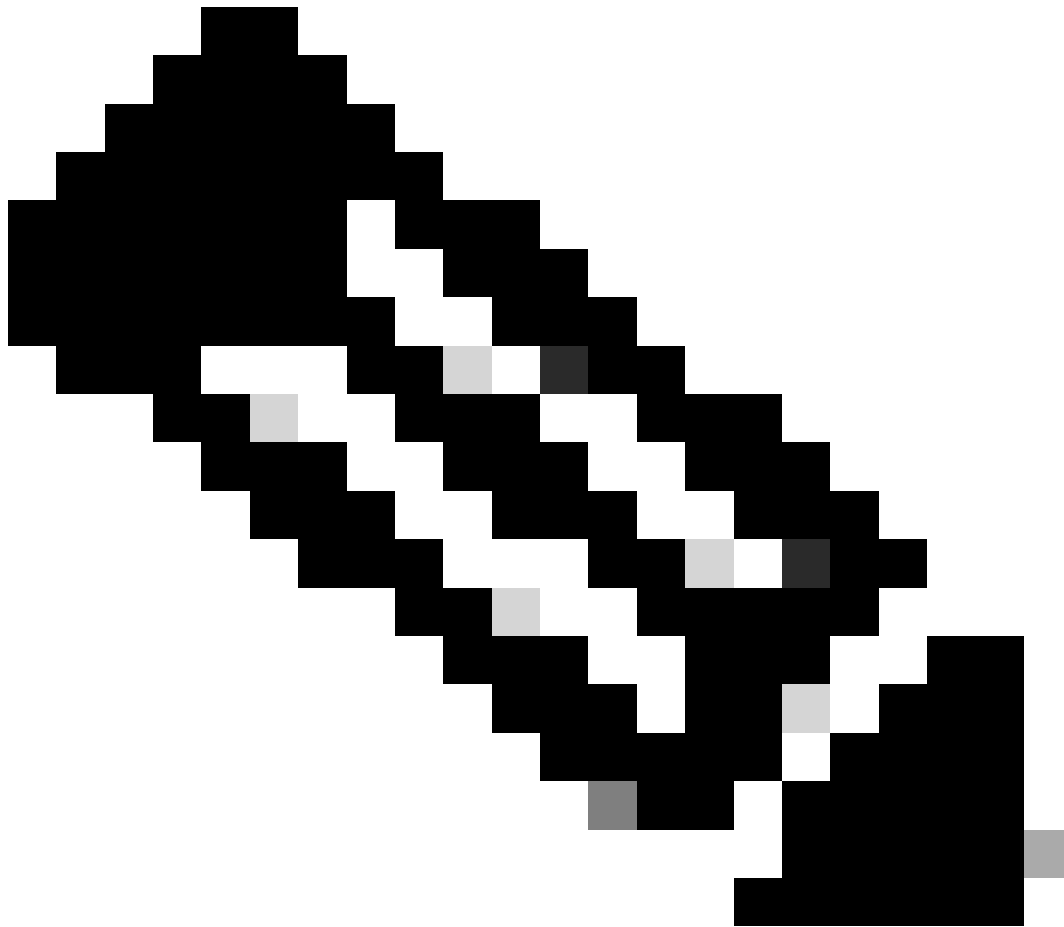
Read Only

Read/Write

Reset

Save

Configura criterio cloud pxGrid



Nota: Il servizio Echo viene utilizzato per eseguire i controlli di integrità per determinare la connettività pub-sub e API ad ISE.

Per impostazione predefinita, alle applicazioni Cisco pxGrid Cloud viene concesso l'accesso in sola lettura alle API (è possibile eseguire solo operazioni HTTP GET).
Abilitare l'opzione Read/Write nella finestra PxGrid Cloud Policy se si desidera consentire anche le operazioni POST, PUT ed DELETE.

Crea istanza applicazione pxGrid (cdFMC)

1. Accedere al portale SCC (Security Cloud Control) come utente con ruolo di amministratore privilegiato.



CONNECTING TO SECURITY CLOUD CONTROL (APJC)

Security Cloud Sign On

Email

Continue

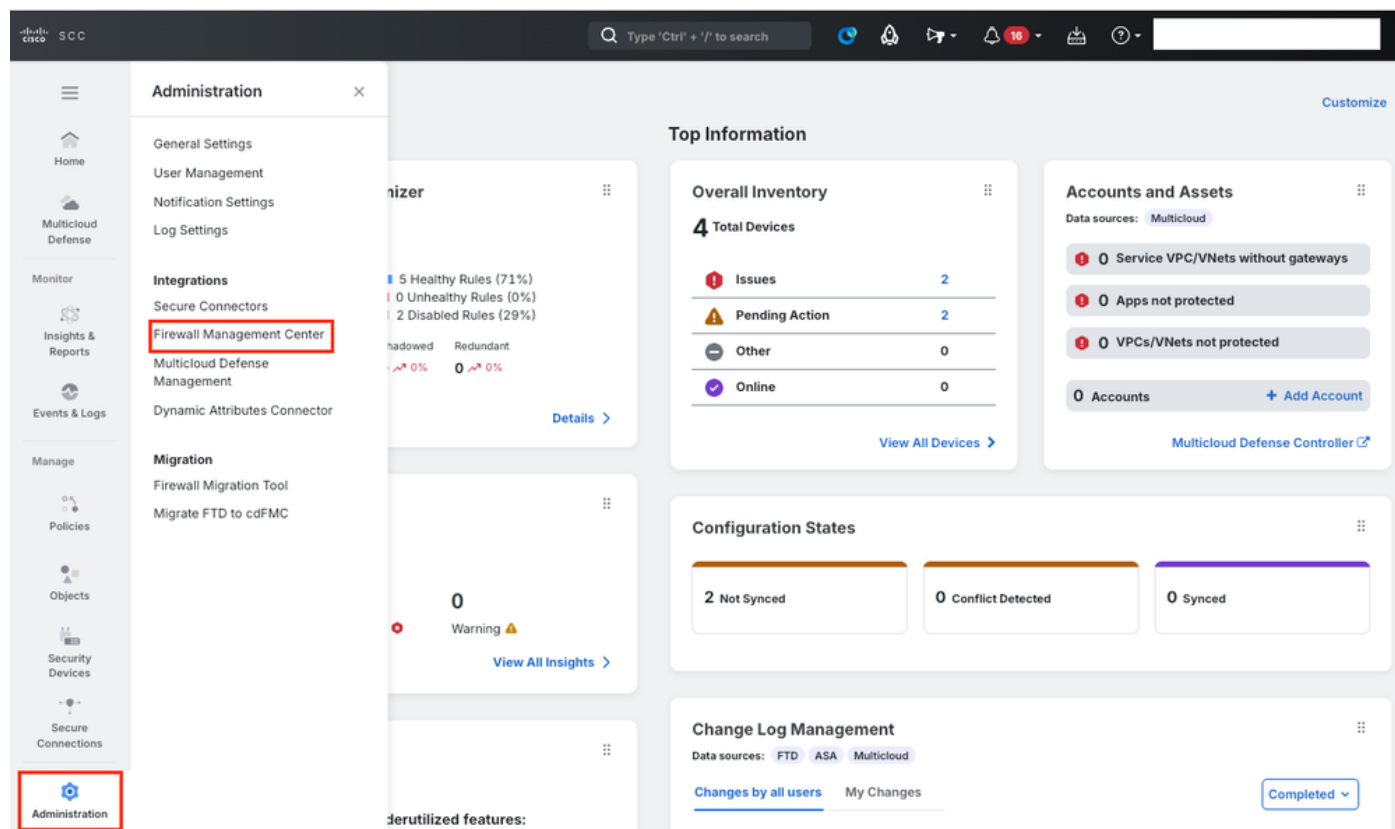
Don't have an account? [Sign up now](#)

Or

[Other login options](#)

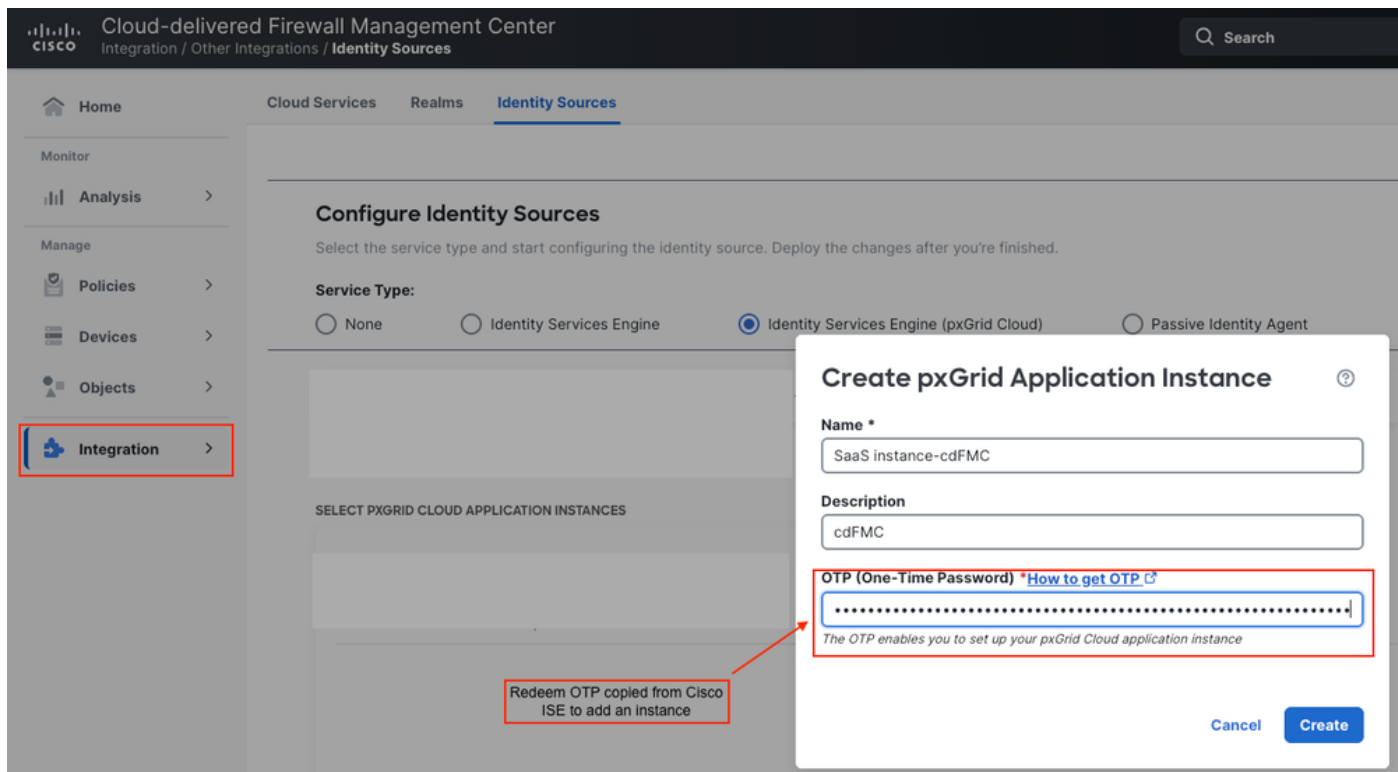
[System status](#) [Policy statement](#)

2. Dal menu Security Cloud Control, fare clic su Amministrazione > Integrazioni > Centro gestione firewall e selezionare l'istanza di cdFMC. Nel riquadro di destra, selezionare Sistema > Configurazione.



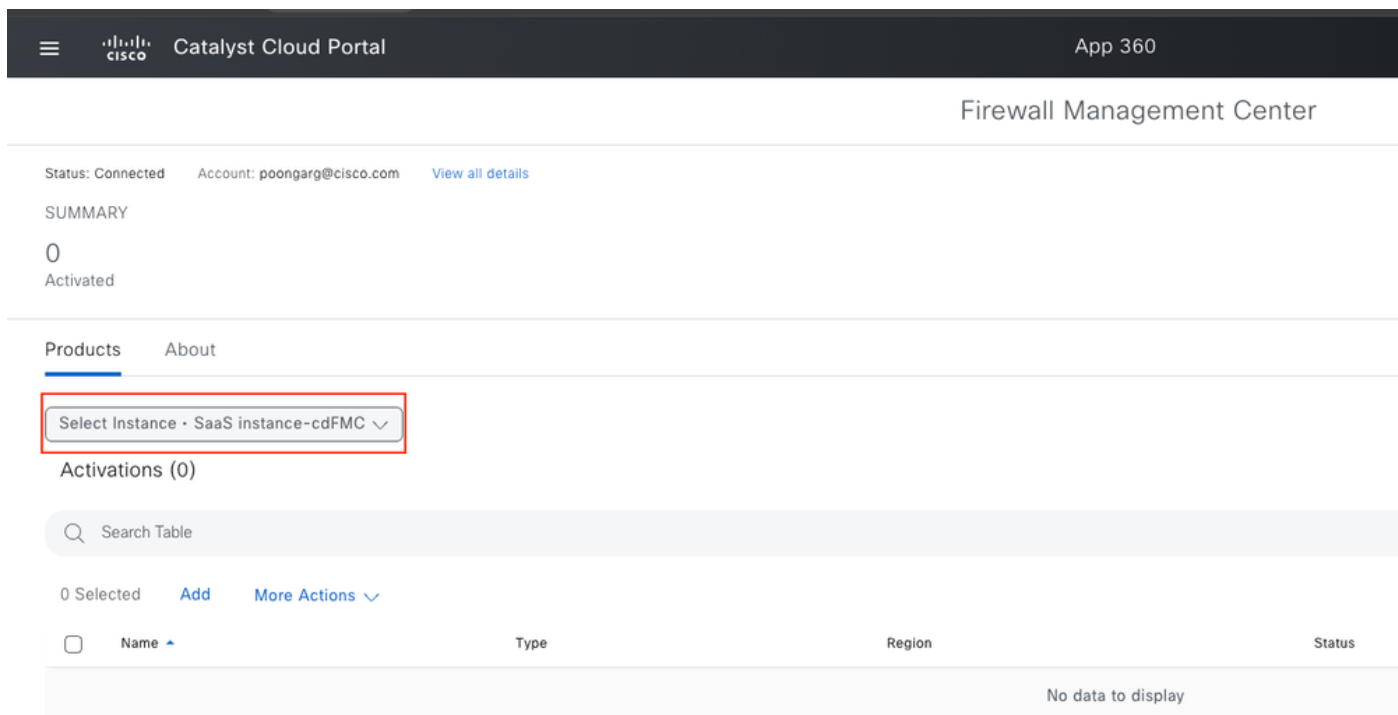
Spostamento in Centro gestione firewall

3. Nella pagina Configurazione, selezionare Integrazione > Altre integrazioni > Origini identità > Scegli tipo di servizio Identity Services Engine (pxGrid Cloud). Fare clic su Create pxGrid Application Instance (Crea istanza applicazione pxGrid) e riscattare l'OTP copiato da Cisco ISE per aggiungere un'istanza.



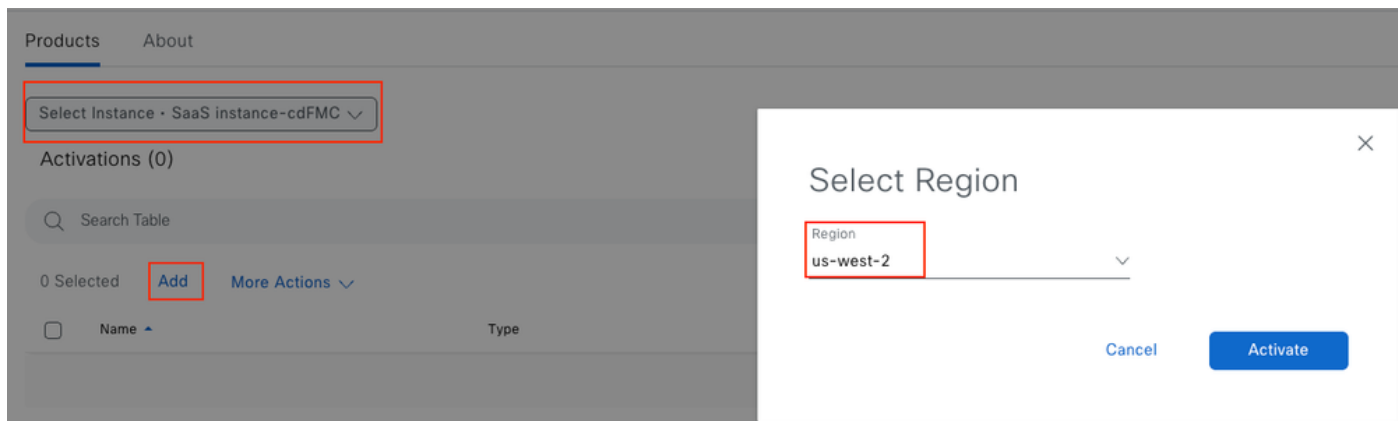
Crea istanza applicazione cdFMC

4. Verificarlo sul portale Cisco Catalyst Cloud all'indirizzo Applications and Products > Firewall Management Center > Manage > Products > Select Instance (Applicazioni e prodotti > Centro di gestione firewall > Gestisci > Prodotti > Seleziona istanza).



Verifica di cdFMC sul portale Catalyst Cloud

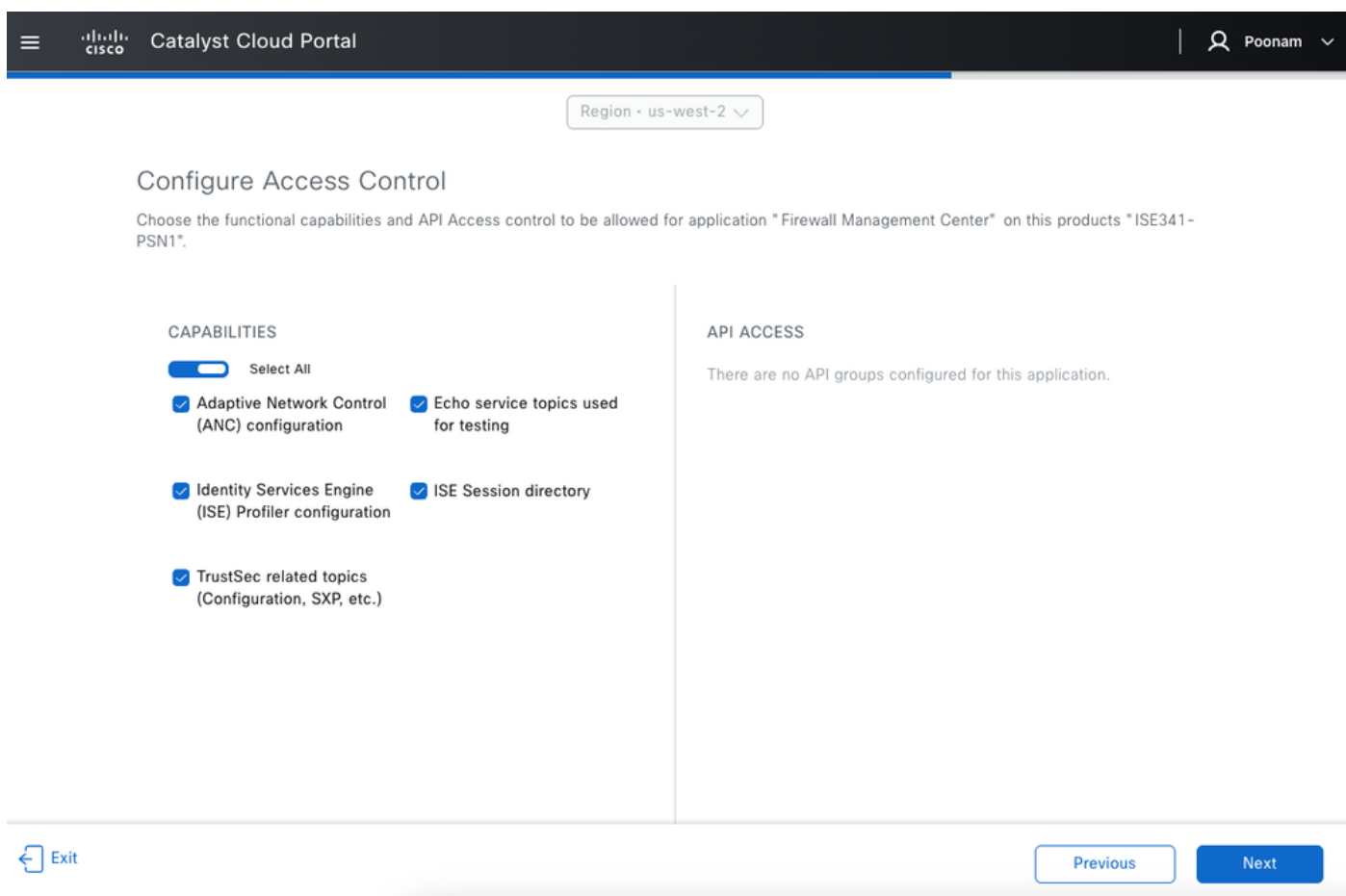
5. Selezionare l'applicazione cdFMC appena creata e fare clic su Aggiungi. Selezionate Regione (Region) e fate clic su Attiva (Activate).



Seleziona area

5. Scegliere l'istanza dell'applicazione e fare clic su Avanti. Selezionare il prodotto (ISE pxGrid node), quindi fare clic su Avanti.

6. Configurare il controllo dell'accesso: scegliere le funzionalità funzionali da consentire a cdFMC sul prodotto ISE scelto. Fare clic su Next (Avanti). Viene visualizzato il riepilogo della configurazione. Verificate e fate clic su Attiva (Activate).



Configurare il controllo di accesso per 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 

ISE prodotto collegato a cfFMC

8. Verificarlo sul portale Cisco Catalyst Cloud all'indirizzo Applications and Products > Firewall Management Center > Manage > Products > Select Instance (Applicazioni e prodotti > Centro di gestione firewall > Gestisci > Prodotti > Seleziona istanza).

Catalyst Cloud Portal

Applications and Products / App 360

Firewall Management Center

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

SUMMARY

1 Activated

Products About

Select Instance - SaaS Instance-cdFMC ▾

Activations (1)

Search Table

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 [Refresh](#)

Verifica che l'app sia attivata

Verifica

1. Sul portale Catalyst Cloud, passare a Applicazioni e prodotti. Selezionare il nome del prodotto ISE e controllare la sezione Product Details. Verificare che cdFMC sia visualizzato in Applicazione attivata.

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 >

Verifica sul portale Catalyst Cloud Control

2. In Security Cloud Control, verificare l'istanza dell'applicazione cdFMC configurata. Il test mostra "Success"

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

Verifica sul portale di controllo di Security Cloud

3. Accedere al nodo ActivePxGrid e verificare che Hermes (agente cloud pxGrid) sia in esecuzione utilizzando il comando `show application status ise`. Questo agente è in stato disabilitato sul nodo Standby pxGrid.

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

Verifica dello stato di Hermes (agente cloud pxGrid)

Controllare il file pxcloud.log su entrambi i nodi pxGrid per confermare lo stato Attivo e Standby:

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, ccloudConnectionStatus=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, ccloudConnectionStatus=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)

Verificare inoltre la porta 8913, che viene aperta solo sul nodo ACTIVE pxGrid:

<#root>

ise341-psn1/admin#show ports | include 8913

tcp:

127.0.0.1:8913

ise341-psn1/admin#

4. Verificare il client cloud pxGrid passando a Amministrazione > servizi pxGrid > Gestione client > Client > Client > client cloud pxGrid. Consultare anche gli argomenti sottoscritti.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The 'Clients' page is displayed, showing a list of pxGrid Cloud Clients. The 'Firewall Management Center' client is highlighted. A tooltip shows the topics subscribed to by this client.

Name	Description	Topics Subscribed	Topics Published
Firewall Management Center	Integrate with Firewall Management...	/topic/com.cisco.ise.session,/topic/com.cisco.ise.session.gr...	

pxGrid Cloud Client su ISE

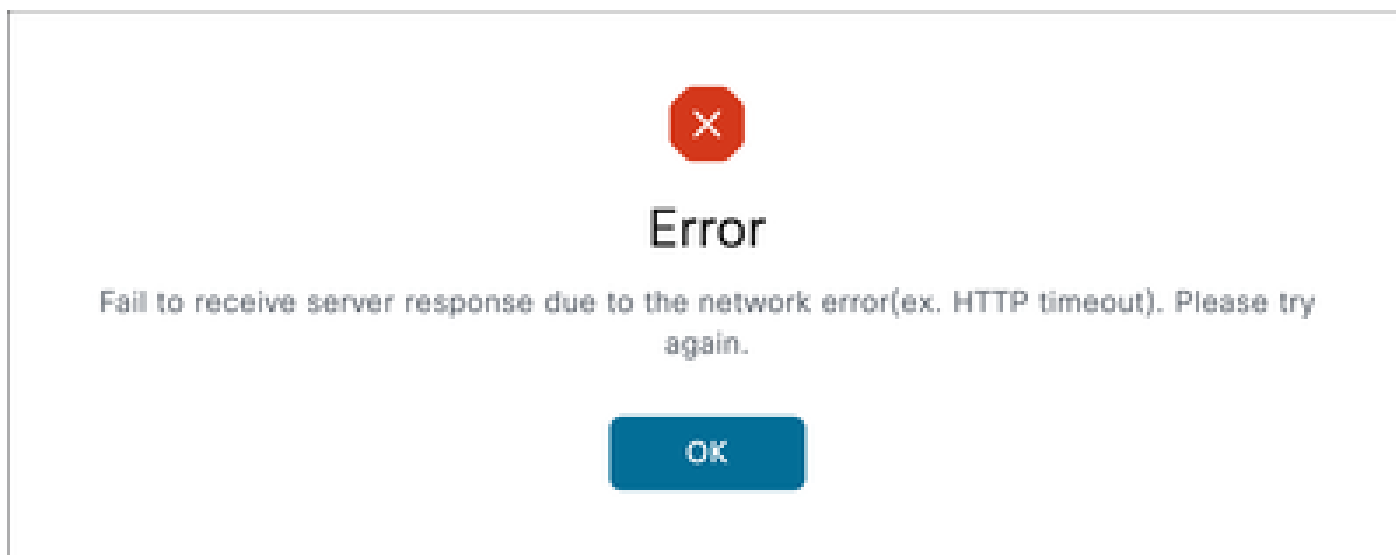
5. Verificare che gli argomenti sottoscritti siano recuperati da cdFMC. Nel portale di controllo di Security Cloud, fare clic su Criteri > Difesa delle minacce > Integrazione > Altre integrazioni > Origini identità. Fare clic su Identity Services Engine (pxGrid Cloud). Fare clic su Configura filtri. Nella pagina fare clic sulla scheda Filtro attributi dinamici. Creare un filtro attributi dinamici.

The screenshot shows the Cisco Cloud-delivered Firewall Management Center (cdFMC) console. The 'Add Dynamic Attribute Filter' dialog is open, and the 'Add Condition' sub-dialog is also open. The 'CtsSecurityGroup' condition is highlighted in the list of conditions.

Attributi recuperati da ISE

Risoluzione dei problemi

1. Errore durante la registrazione all'ISE:



Configurazione proxy mancante

Controllare la connettività Internet e possibili errori di configurazione del proxy.

2. Lo stato di pxGrid mostra Non connesso nella pagina Modifica nodo ISE dopo aver abilitato il servizio PxGrid Cloud e aver configurato i parametri name e region.

Controllare il file hermes.log sul nodo in cui si sta abilitando il servizio cloud pxGrid:

<#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
```

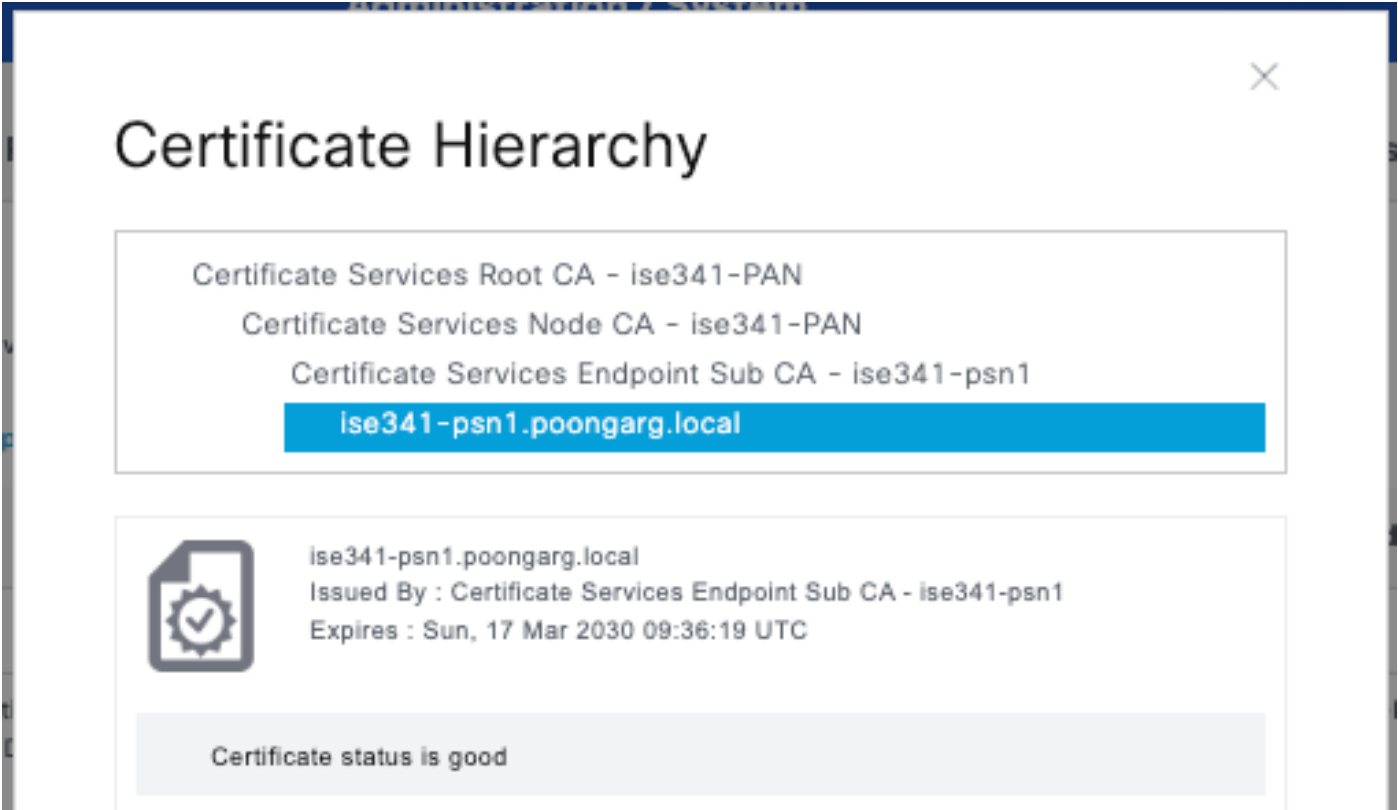
```
2025-03-17T09:19:35.308Z | ERROR | hermes/main.go:402 | Error running Hermes: Failed to establish pxGrid
```

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

```
Stopping REST server on :8913
```

Il server Hermes Rest è in ascolto sulla porta 8913. Registri indica chiaramente che il server REST Hermes sta tentando di avviarsi ma non è riuscito a stabilire la connessione WebSocket di pxGrid a causa di un errore di verifica del certificato.

Soluzione: Verificare che il certificato pxGrid sia valido e che la catena di certificati non sia interrotta. Visualizzare il certificato e verificare che lo stato del certificato sia corretto. In questo caso, il nome host ISE non era corretto nel certificato pxGrid emesso per questo nodo.



Certificato pxGrid valido

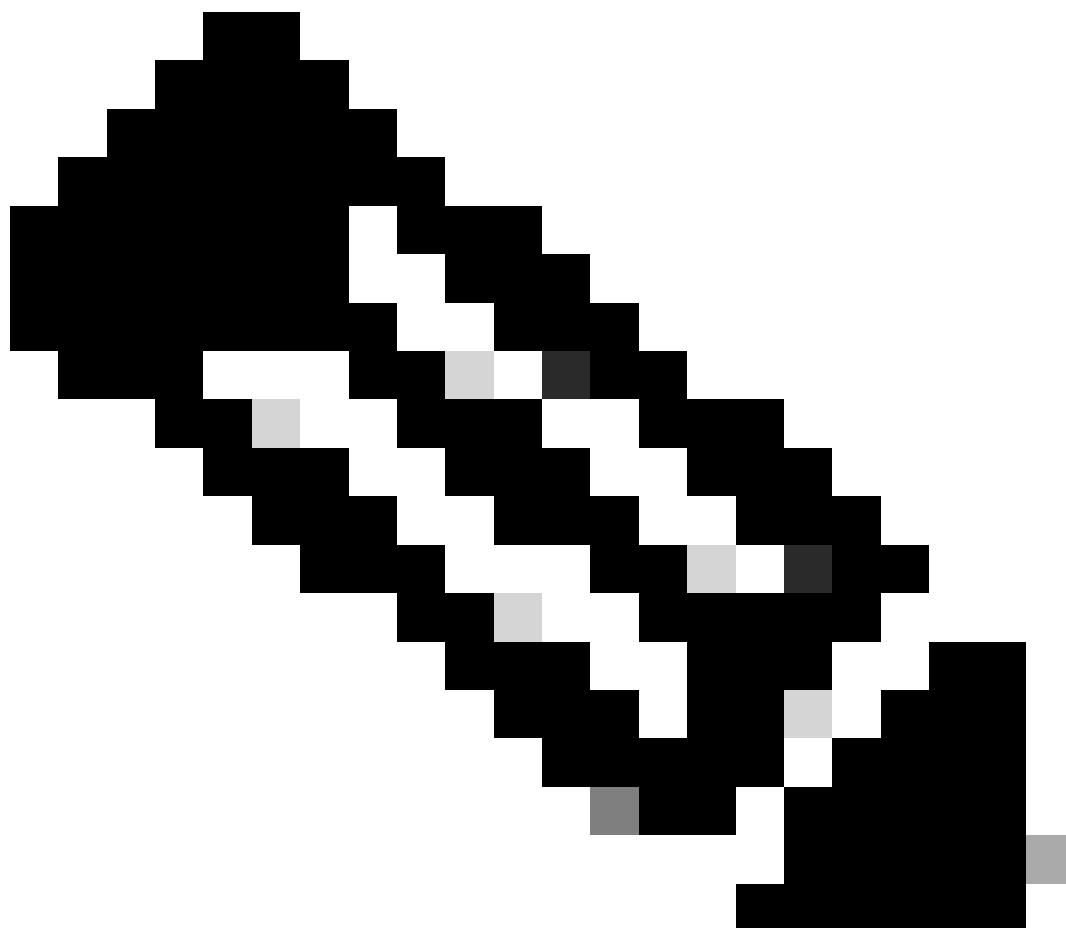
3. Attivazione dell'applicazione cdFMC non riuscita sul portale Catalyst Cloud.

Soluzione: Verificare che su ISE, nell'ambito della policy cloud pxGrid, le API ERS (External RESTful Services) e OpenAPIs abbiano accesso in sola lettura.

Registri relativi alla funzionalità pxGrid Cloud:

Debug componente	Nome file di log	Descrizione
pxGrid Cloud	pxcloud.log, hermes.log	pxcloud.log: Registra le modifiche alla configurazione del servizio cloud pxGrid, lo stato della connessione al servizio cloud pxGrid e lo stato di elevata disponibilità
pxGrid Cloud OpenAPI	pxcloud.log, hermes.log	hermes.log: registra lo stato dell'abbonamento all'argomento pxGrid, le richieste di riposo ERS da pxGrid Cloud, le modifiche alla configurazione su ISE.

Telemetria	sch.log	viene generato quando l'utente utilizza il catalogo di integrazione. Include i log iniziali con il token utilizzato per la connessione a pxGrid Cloud.
------------	---------	--



Nota: Indipendentemente dal nodo su cui si sta abilitando la persona pxGrid Cloud, è necessario controllare i log sul nodo PAN attivo. Una volta registrato il dispositivo, i registri Hermes si trovano sul nodo specifico in cui è attivato.

Hermes.log supporta solo i livelli di log Debug, Info, Warn e Error. Pertanto, se si sceglie Trace, il livello di log viene impostato su Debug per hermes.log. Se si sceglie Irreversibile, il livello di log viene impostato su Errore per hermes.log.

Iscrizione/registrazione ad ISE e applicazione. Flusso di attivazione

Prima che il dispositivo venga registrato, ISE utilizza un token del dispositivo per recuperare l'elenco di aree e l'elenco di app dal cloud. Questo token viene fornito dal componente "telemetria" di ISE. Controllare sch.log sul nodo PAN:

```
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.TetheringStateService
2025-03-17 09:10:23,467 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.TetheringStateService
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.TetheringStateService
2025-03-17 09:10:24,497 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.TetheringStateService
2025-03-17 09:10:24,529 INFO [openapi-http-pool7][[]] cpm.infrastructure.telemetry.api.TelemetryConfig
```

pxcloud.log (nodo PAN), una volta abilitato il servizio pxGrid Cloud, Hermes (agente pxGrid Cloud) viene attivato e ISE recupera le informazioni sulla regione e riceve un token tramite il componente di telemetria.

```
2025-03-17 08:47:00,300 INFO [main][[]] cisco.cpm.pxcloud.api.PxCloudInitializer -::::- Initializing px
2025-03-17 08:47:00,312 INFO [main][[]] cisco.cpm.pxcloud.pxgrid.PxCloudProviderRegistration -::::- Re
2025-03-17 08:47:00,314 INFO [main][[]] cisco.cpm.pxcloud.hermes.ProxyConfigNotificationHandler -::::-
2025-03-17 08:47:00,376 INFO [main][[]] cisco.cpm.pxcloud.hermes.HermesConfigManager -::::- Registerin
2025-03-17 08:47:00,376 INFO [main][[]] cisco.cpm.pxcloud.hermes.HermesConfigManager -::::- Registerin
2025-03-17 08:50:18,842 INFO [main][[]] cisco.cpm.pxcloud.hermes.HermesConfigManager -::::- Updating H
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.PxCloudNodeChangeH
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.IntegrationCatalogSchedule
2025-03-17 09:10:22,475 TRACE [openapi-http-pool4][[]] cpm.iseopenapi.pxcloud.impl.PxGridApiDelegateImp
2025-03-17 09:10:22,485 INFO [openapi-http-pool4][[]] cpm.pxcloud.service.ui.IseEnrollment -::::- Fetc
2025-03-17 09:10:22,739 TRACE [openapi-http-pool7][[]] cpm.iseopenapi.pxcloud.impl.PxGridApiDelegateImp
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 -::::- Ano
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
```

Viene ricevuto il collegamento per l'attivazione e viene eseguita la registrazione automatica.

```
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
```

Il nodo pxGrid assume il ruolo ACTIVE, tuttavia, in questo caso è stato osservato pxGridConnectionStatus come NOT_CONNECTED, che è stato corretto dopo l'aggiunta del certificato pxGrid corretto (con catena CA radice completa) in questo nodo pxGrid

```
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 -:::- Fetch
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
```

Ora controllare Hermes.log sul nodo Active pxGrid per eventi pubsub:

```
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
```

Catena CA radice del portale Catalyst Cloud verificata.

```
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: M
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
```

La richiesta di sottoscrizione ad argomenti specifici è stata creata una volta, l'applicazione FMC è configurata nel catalogo di integrazione:

```
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
```

Limitazioni

1. L'utente non può abilitare la persona pxGrid Cloud su più di 2 nodi.
2. È supportata la deregistrazione dal portale Catalyst Cloud a cdFMC, ma non viceversa.

Riferimenti

[Controllo utente con origine identità cloud pxGrid](#)

[Cisco PxGrid Cloud](#)

[Guida alla soluzione Cisco PxGrid Cloud](#)

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).