Integrate Cloud-delivered Firewall Management Center with ISE Via pxGrid Cloud

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Cisco pxGrid Cloud Terminology

Background Information

Configure

- Network Diagram
- Configurations
  - Import the Cisco pxGrid Cloud server certificate in ISE
- Flow Diagram
  - Registration of ISE with Catalyst Cloud Portal
  - Activate the cdFMC Application on ISE using Integration Catalog
  - Create pxGrid Application (cdFMC) Instance

Verify

Troubleshoot

- ISE Enrollment/Registeration and App. activation Flow

Limitations

References

Introduction

This document describes the procedure to integrate Cisco ISE with cloud-delivered Firewall Management Center (cdFMC) via pxGrid Cloud.

Prerequisites

- A working knowledge of Cisco Identity Service Engine (ISE)
- An account in Cisco Catalyst Cloud Portal
- An account on Cisco Security Cloud Control Portal

Requirements

- Install and activate the Advantage license tier in your Cisco ISE deployment.
- The pxGrid Cloud agent creates an outbound HTTPS connection to Cisco pxGrid Cloud. Therefore, configure Cisco ISE proxy settings if network uses a proxy to reach the internet. To configure proxy settings in Cisco ISE, choose **Administration > System > Settings > Proxy**.
- The Cisco ISE Trusted Certificates Store must include the root CA certificate required to validate the server certificate presented by Cisco pxGrid Cloud. Ensure that the Trust for Authentication of Cisco

Services option is enabled for this root CA certificate. To enable Trust for Authentication of Cisco Services, choose **Administration > System > Certificates**.

- Ensure that port 443 is open for outbound connection from Cisco ISE to Cisco pxGrid Cloud Portal. If firewall or proxy settings are configured, ensure that these URLs are not blocked.

https://dna.cisco.com

https://dnaservices.cisco.com

https://ciscodnacloud.com

Components Used

ISE software version: 3.4 Patch 1, 4 nodes deployment (PAN, SAN and 2 PSN with pxGrid service enabled)

cdFMC version: 20241127

Cisco Firepower Threat Defense (FTD) for VMware version: 7.2.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Cisco pxGrid Cloud Terminology

Here are some of the common terms that are used in the Cisco pxGrid Cloud solution and their meaning in the Cisco pxGrid Cloud environment:

- **Offer:** A set of capabilities packaged together and offered as a solution
- **Subscription:** An instance of an offer being consumed by a tenant is a subscription
- **App:** You can create and register applications for your product based on your requirements.

Background Information

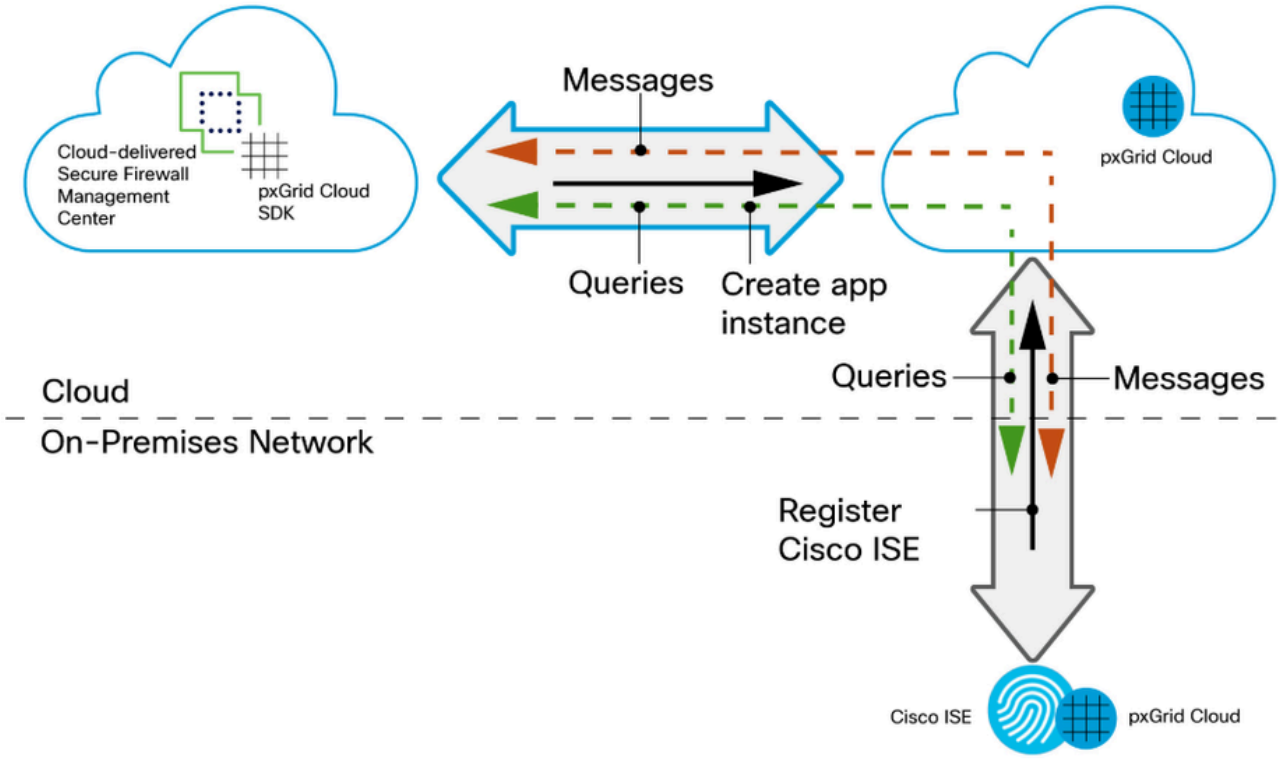
Cisco ISE provides context sharing between multiple security vendors; however, the current architecture does not allow communication between the on-prem ISE and cloud-based solutions through the network perimeter without some sort of bypass/putting holes in the firewall.

Cisco ISE's pxCloud is a cloud-based solution that solves this problem and enables context sharing between on-prem and the cloud without additional installation, overhead, and compromising the security of your network. It is secure and customizable, enabling you to share only the data that you want to share and consume only the contextual data that is relevant for your application.

Cisco ISE release 3.1 patch 3 and later support pxGrid Cloud. Cisco and its partners can develop pxGrid Cloud-based applications and register them with the pxGrid Cloud offer. It relies on cisco DNA-Cloud Portal to onboard and register applications without depending on other on-premise infrastructure. These applications use the External RESTful Services (ERS), Open APIs and pxGrid (APIs and websocket) to exchange information with Cisco ISE to use subscription and user data from ISE in cdFMC.

Configure

Network Diagram



cdFMC and ISE Integration via pxGrid Cloud

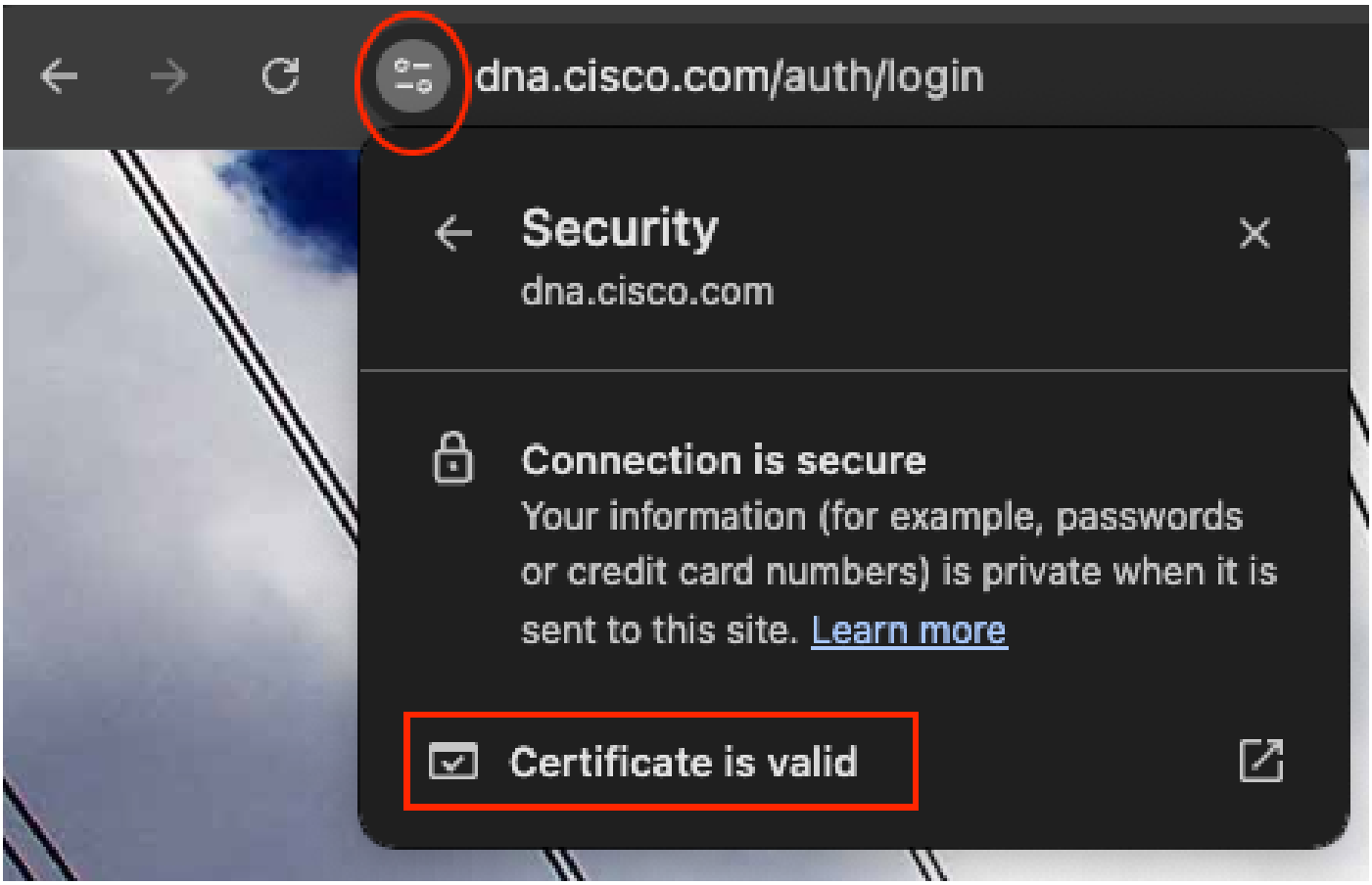
Configurations

Four main steps involved are:

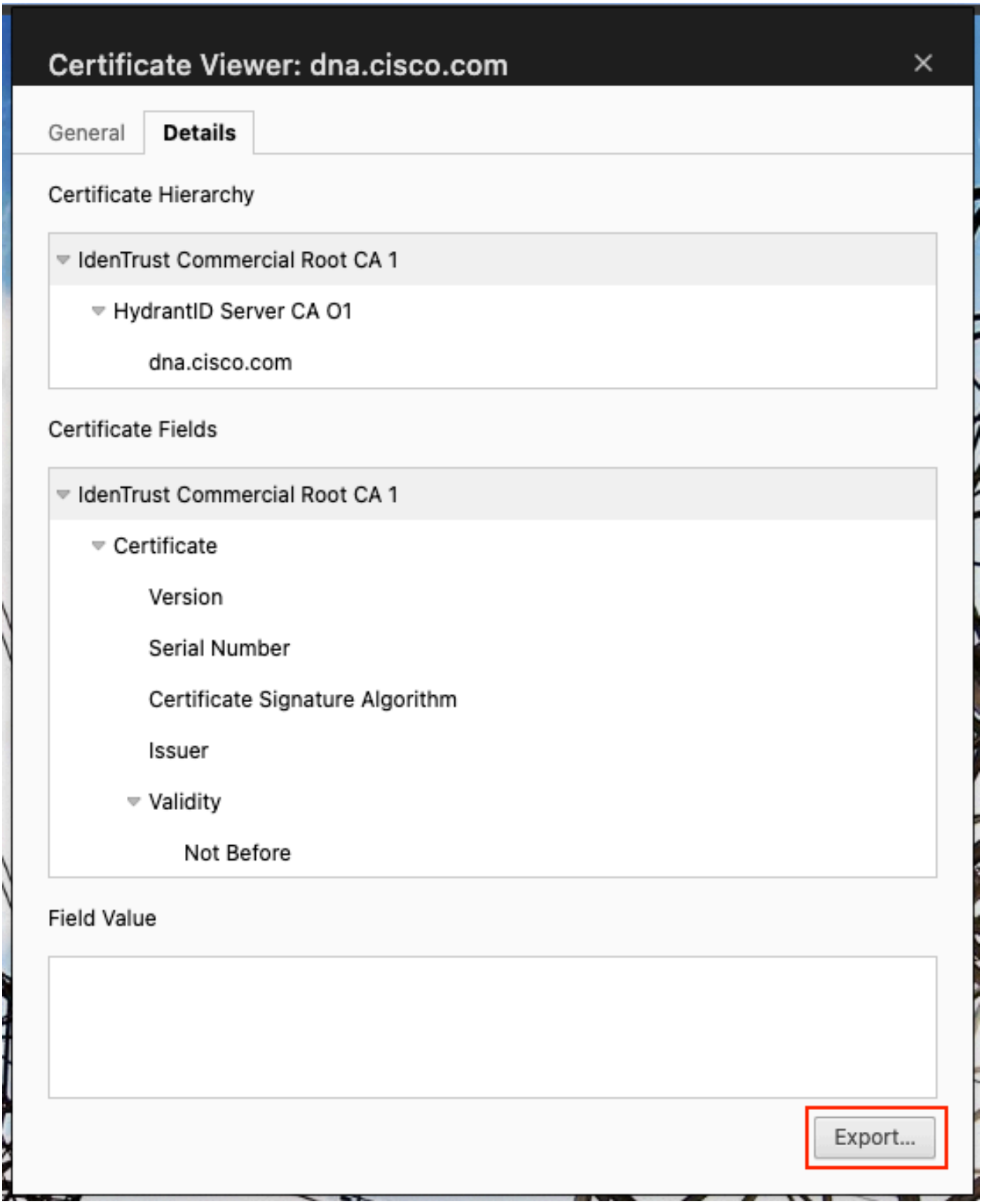
- Import the Cisco pxGrid Cloud server certificate in ISE.
- Register ISE with Catalyst Cloud Portal.
- Activate the cdFMC Application on ISE using Integration Catalog
- Create pxGrid Application (cdFMC) Instance

Import the Cisco pxGrid Cloud server certificate in ISE

ISE must establish trust with the Cisco pxGrid Cloud. Even though the cloud website is authenticated with a publicly signed certificate, ISE does not maintain a complete list of trusted root CAs. Therefore administrator must establish a trust relationship. Export the pxGrid Cloud Root and Intermediate certificates by browsing to Catalyst Cloud Portal . Most browsers allow this. Here are the steps to get certificate from Chrome Browser.



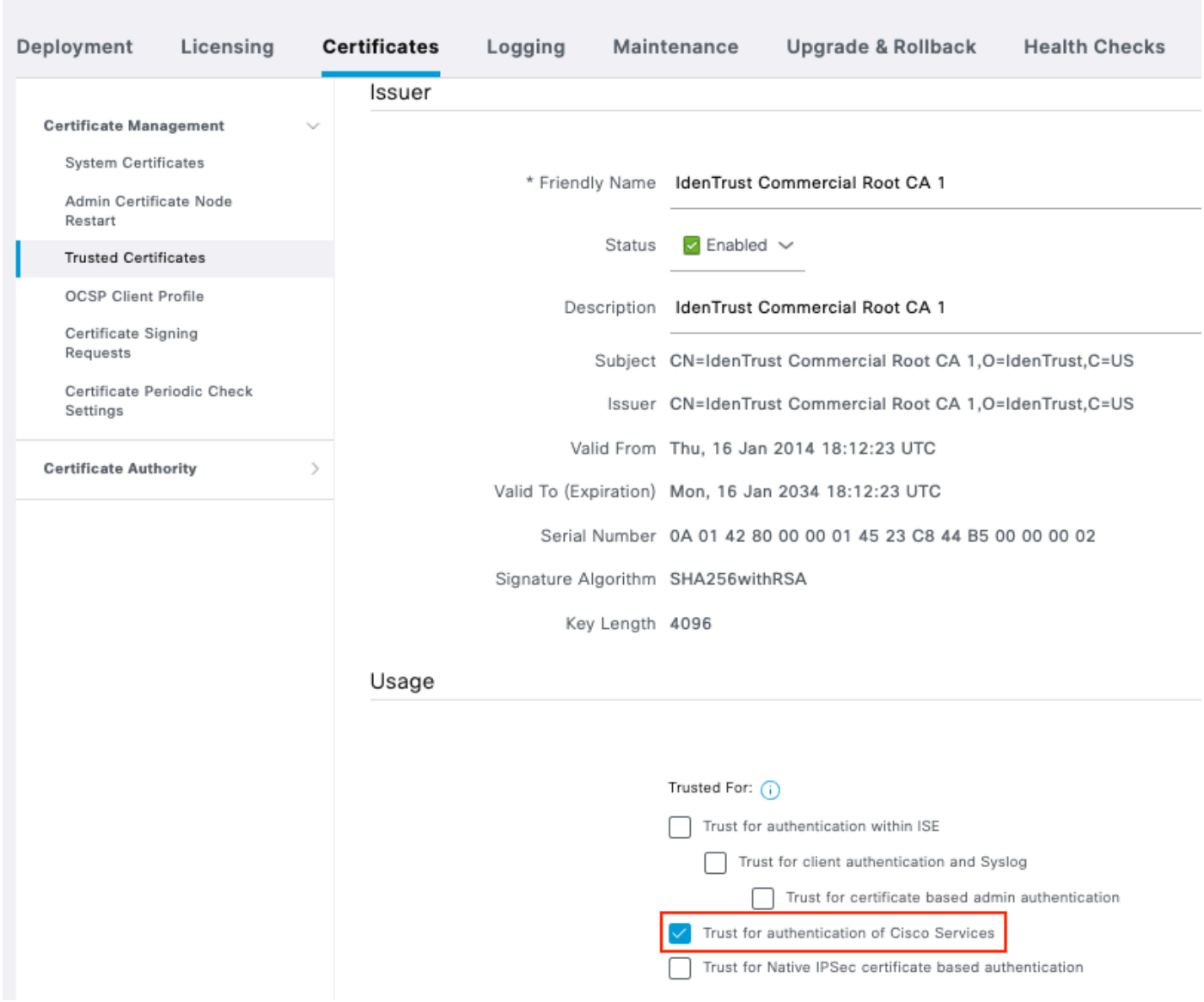
View the Site Information



Export the Certificate Chain

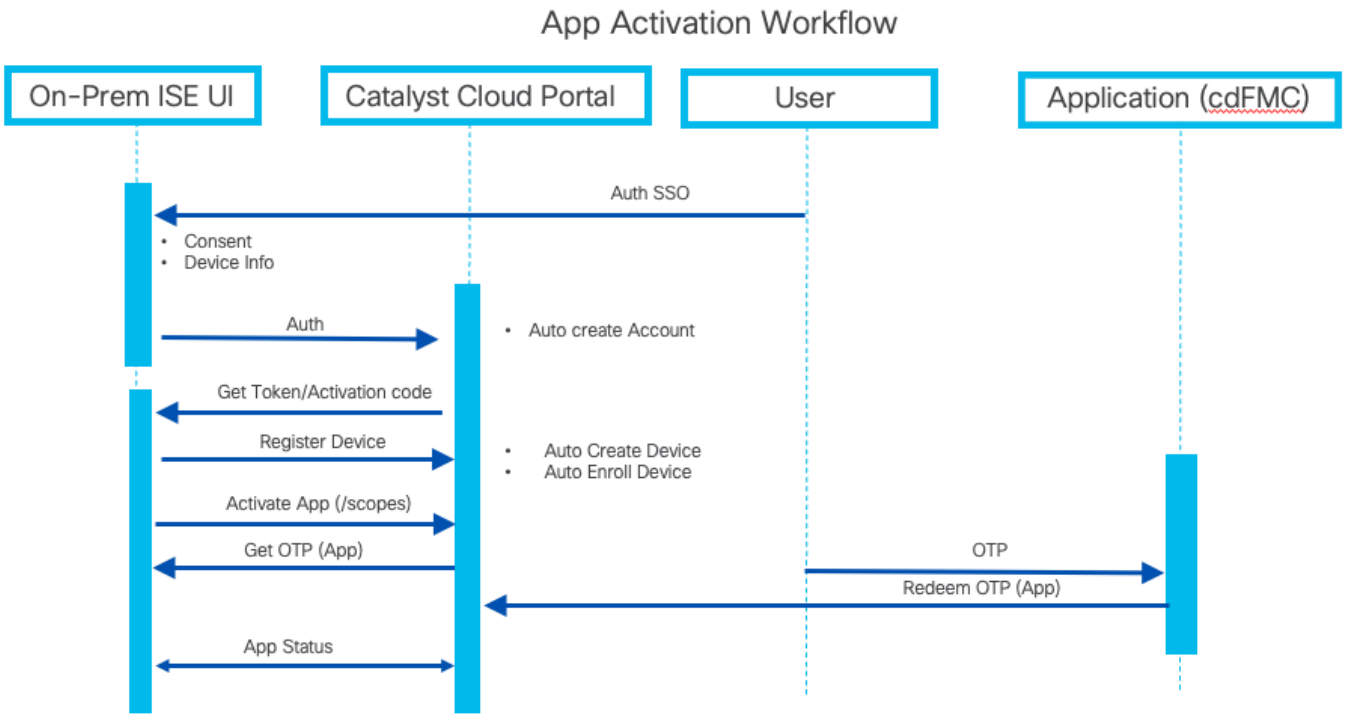
Import the certificates into "**Trusted Certificates**" store in ISE if the certificate chain is missing (ISE already have IdenTrust Commercial Root CA 1).

Ensure that the "**Trust for Authentication of Cisco Services**" option is enabled for this root CA certificate. To enable Trust for Authentication of Cisco Services, choose **Administration > System > Certificates**.



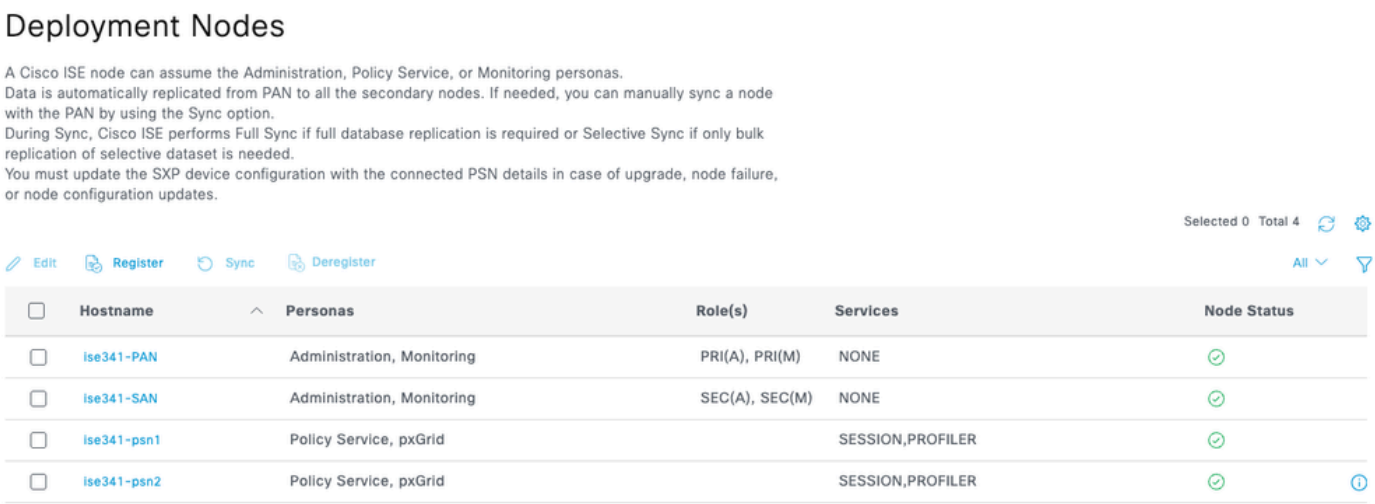
Enable Trust for authentication of Cisco Services

Flow Diagram



App Activation Workflow

ISE deployment used in this setup



Registration of ISE with Catalyst Cloud Portal

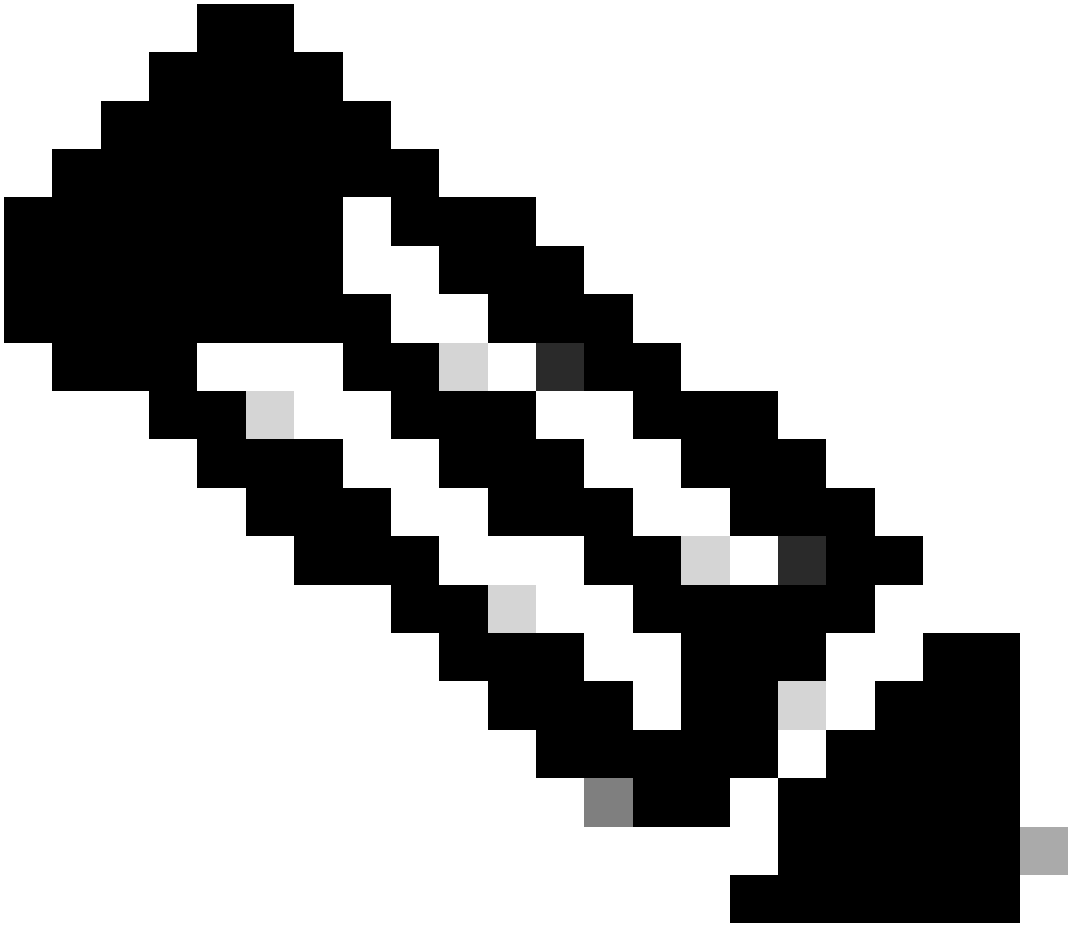
Enable pxGrid Cloud service in Cisco ISE and register your device.

1. In the Cisco ISE GUI, choose **Administration > System > Deployment**.

2. Click the node on which you want to enable the pxGrid Cloud service (in this case first PSN node).

3. In the **General Settings** tab, enable the **pxGrid service**.

4. Check the **pxGrid Cloud** check box.



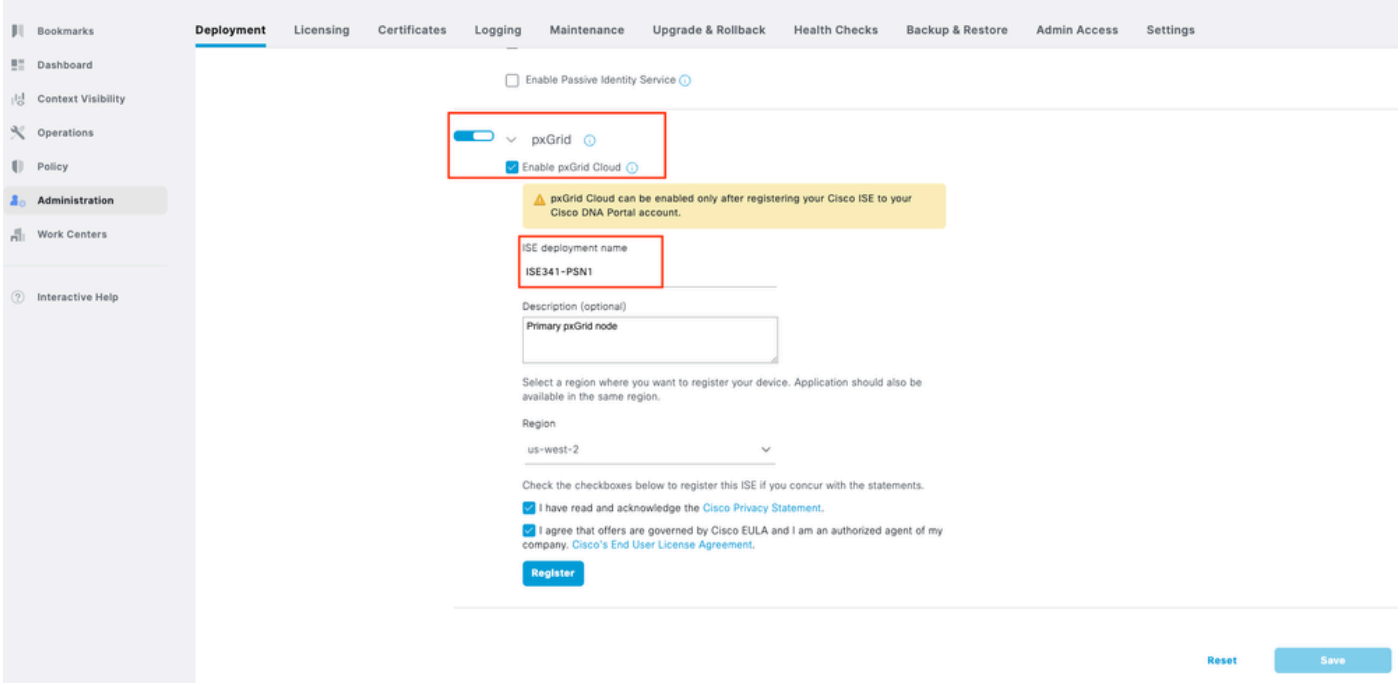
Note: The pxGrid Cloud service can be enabled only on two nodes to enable high availability. You can enable the pxGrid Cloud option only when the pxGrid service is enabled on that node.

5. In the **ISE deployment name** field, enter a meaningful name. This name is shown in Catalyst Cloud Portal and can be used to distinguish if multiple ISE deployments are registered with cloud. You can verify your registered Cisco ISE deployment on the Cisco Catalyst Cloud Portal using the ISE deployment name.

(Optional) In the **Description** (optional) field, enter a description for your Cisco ISE deployment.

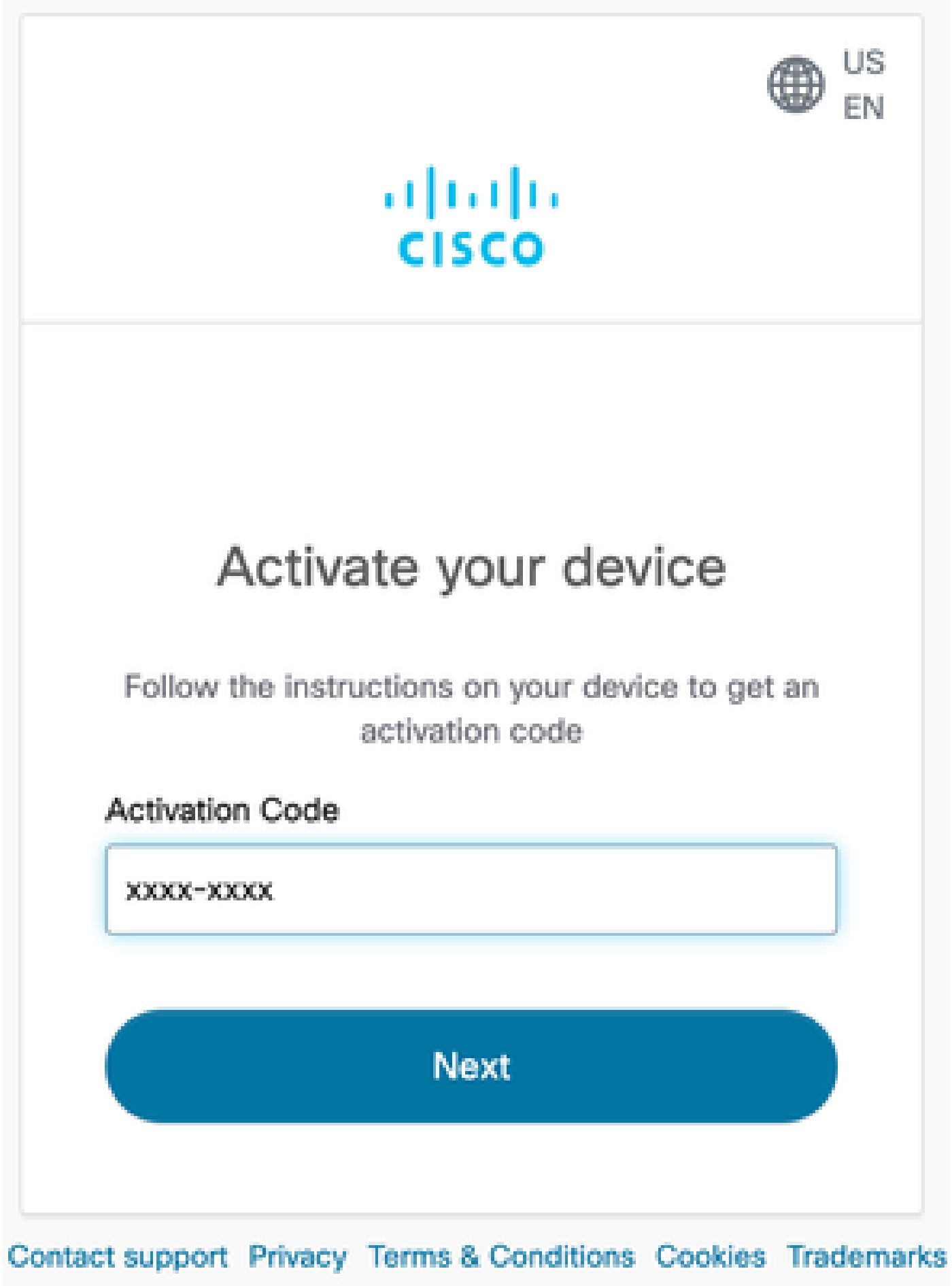
6. In the **Region** drop-down list, choose a region to register your Cisco ISE device. Cisco pxGrid Cloud is now supported in Europe, Asia Pacific and Japan in addition to the U.S.. Note that the application that you want to use with pxGrid Cloud must also be available in the same region.

7. Click **Register**.

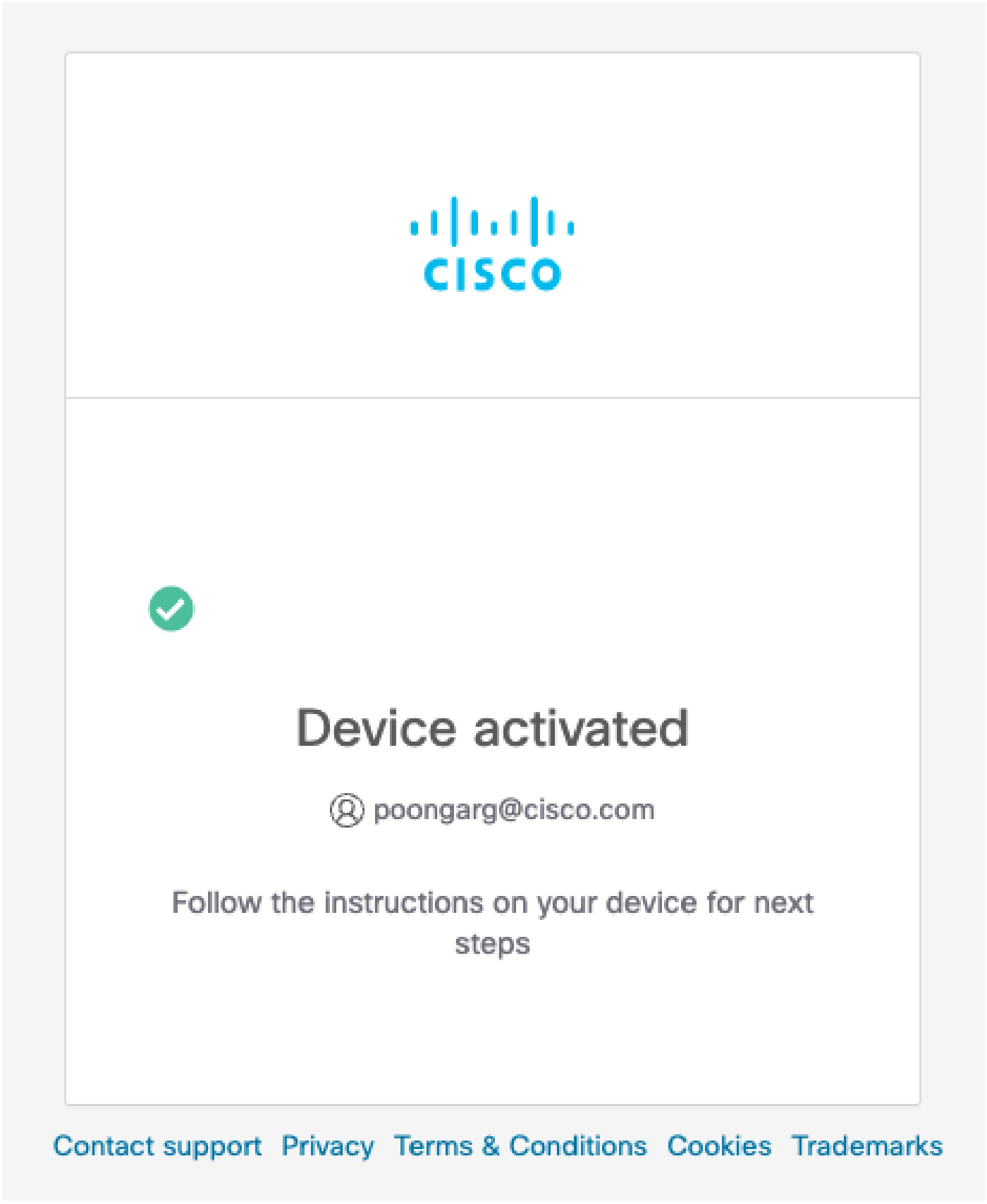


Register ISE PSN with pxGrid Cloud

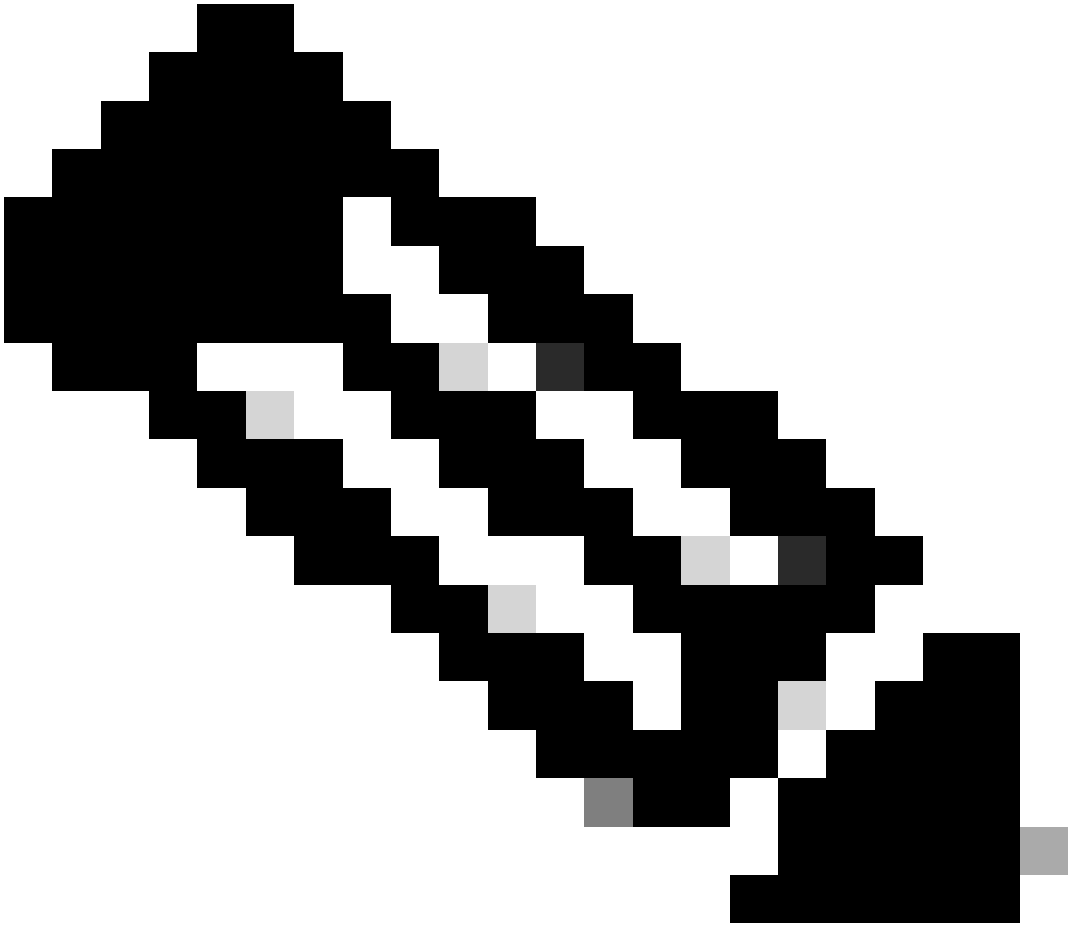
8. In the **Activate your device** pop-up page, the Activation Code for your device is automatically filled. Click **Next**.



Activate the device



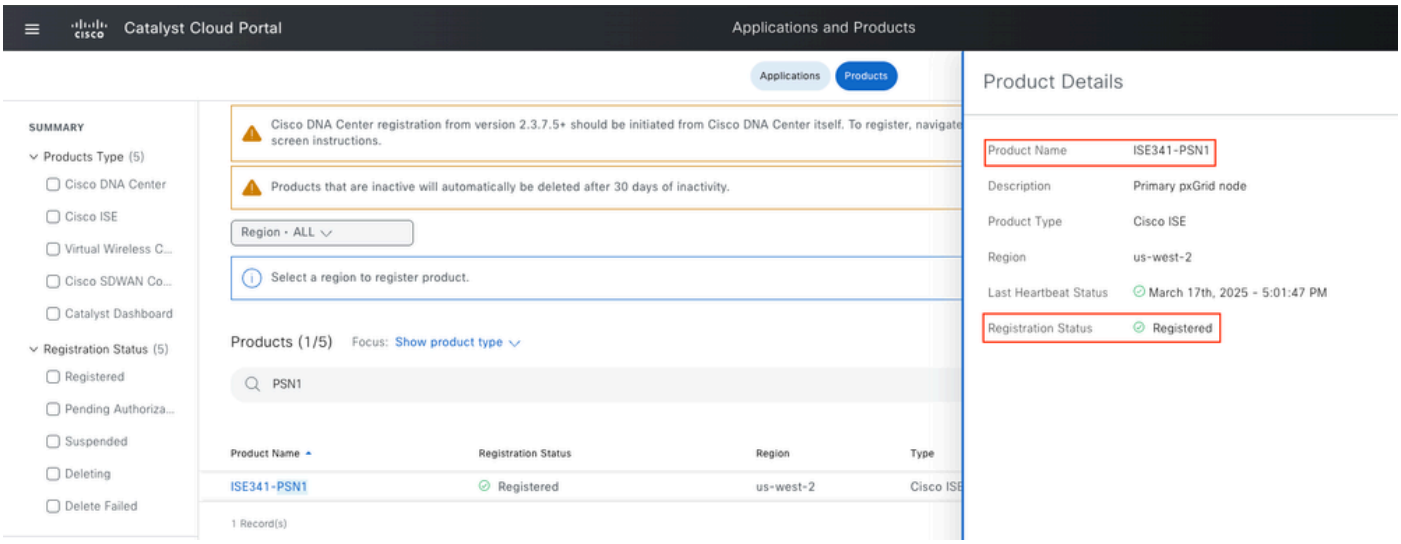
Device Activated



Note: When you enable "pxGrid Cloud" persona on second node, ISE do not need all these details as the registration of ISE with pxGrid Cloud is at deployment level.

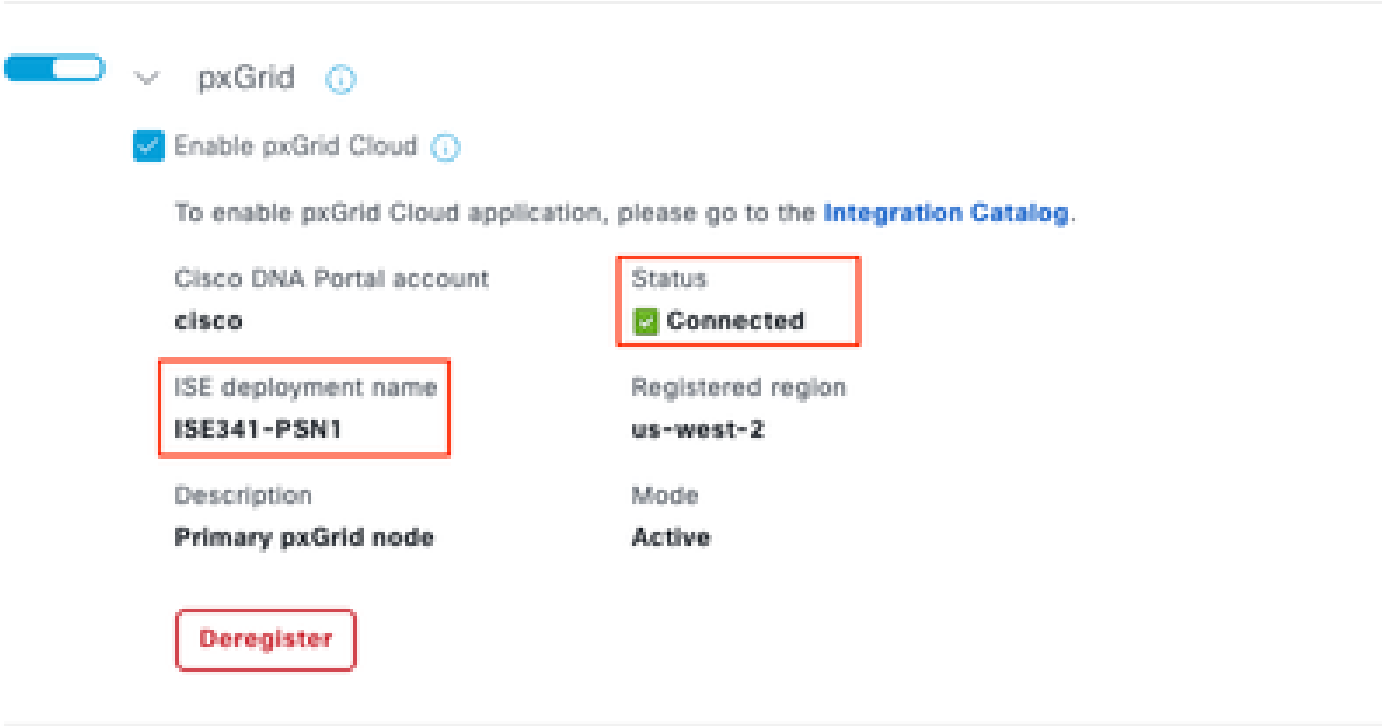
9. Log in to your Cisco Catalyst Cloud Portal account using your login credentials. If you do not have login credentials then create a new account to complete your device registration. For more information, see Create an account on Cisco Catalyst Cloud Portal

Your Cisco ISE device is activated and registered.



ISE node registered with Catalyst Cloud Portal

10. You can find details of your registered Cisco ISE in the pxGrid section (**Administration > System> Deployment > pxGrid**).



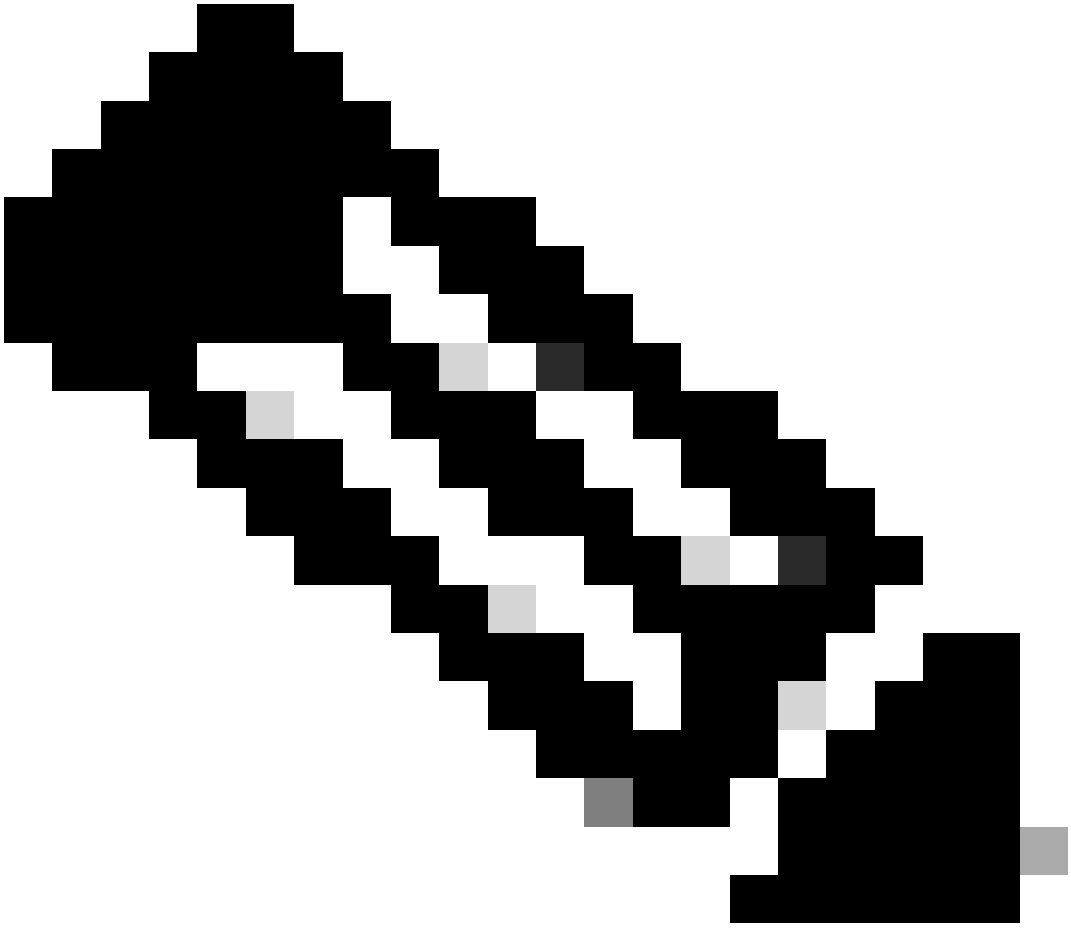
Verify ISE registered with pxGrid Cloud

You can click **Deregister** to deregister your Cisco ISE device. Deregistering Cisco ISE also automatically deactivates the connected applications.

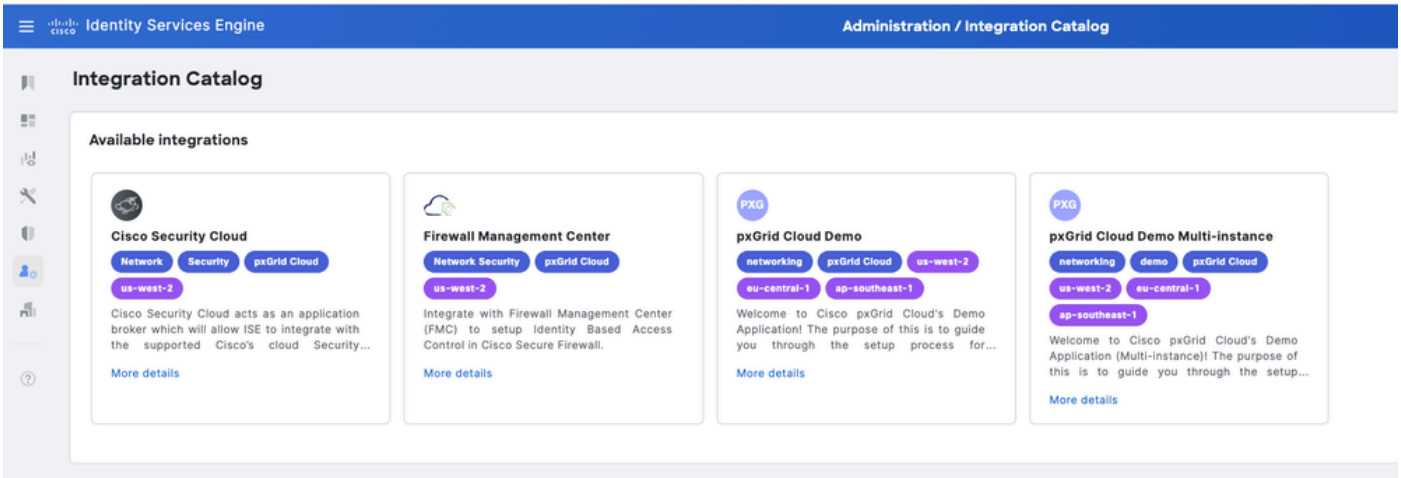
Activate the cdFMC Application on ISE using Integration Catalog

1. In the ISE GUI, choose **Administration > Integration Catalog**.

2. Under the **Available integrations**, select **Firewall Management center** application.



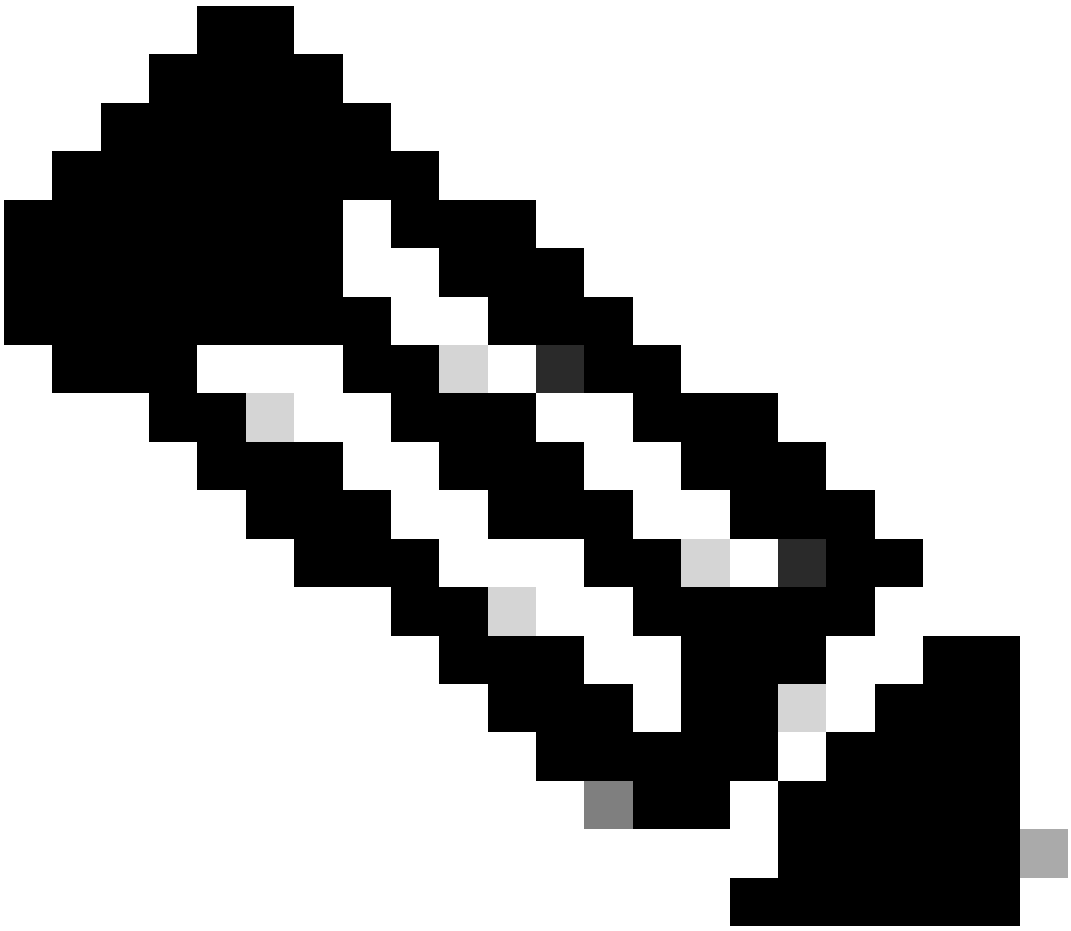
Note: The list of applications depend on the account. Some application could be exposed to only specific accounts.



Integration catalog

3. In the **App configuration** section, Select **New instance** and choose the **Data scopes** for your app

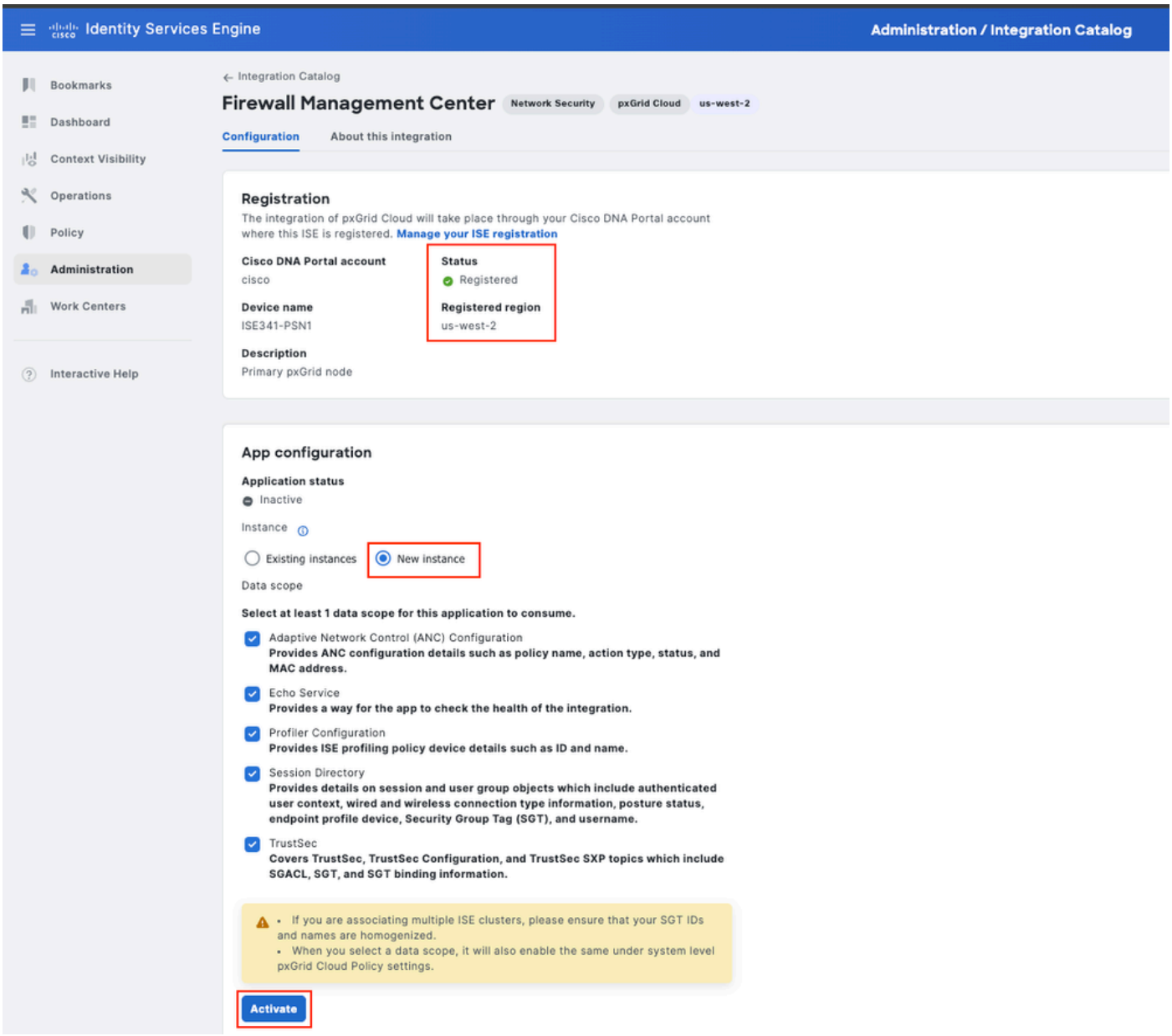
configuration. Choose at least one data scope to proceed.



Note: When you select a data scope, it also enables the same under system level pxGrid Cloud Policy settings.

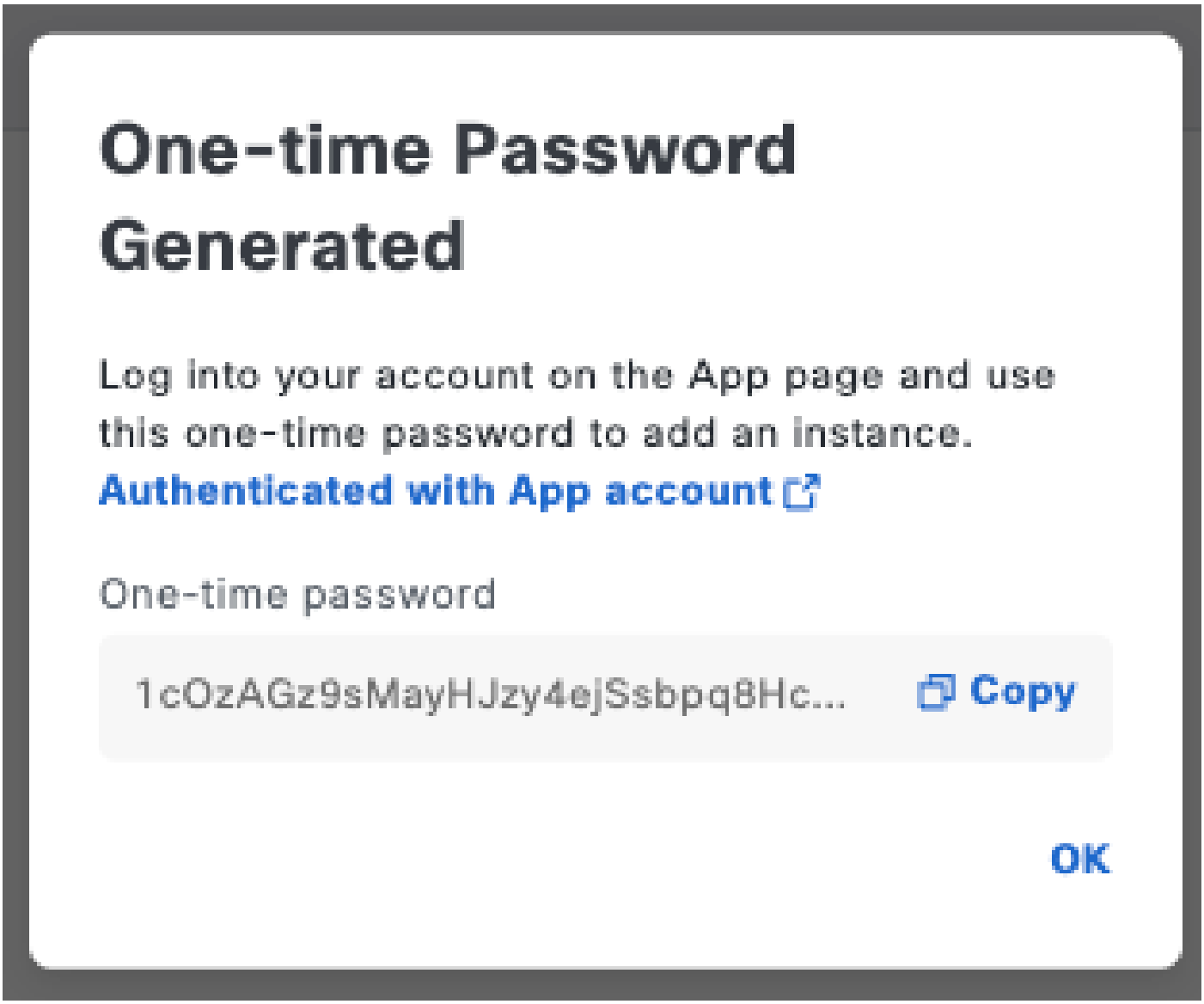
---

4. Click **Activate** to activate the app.



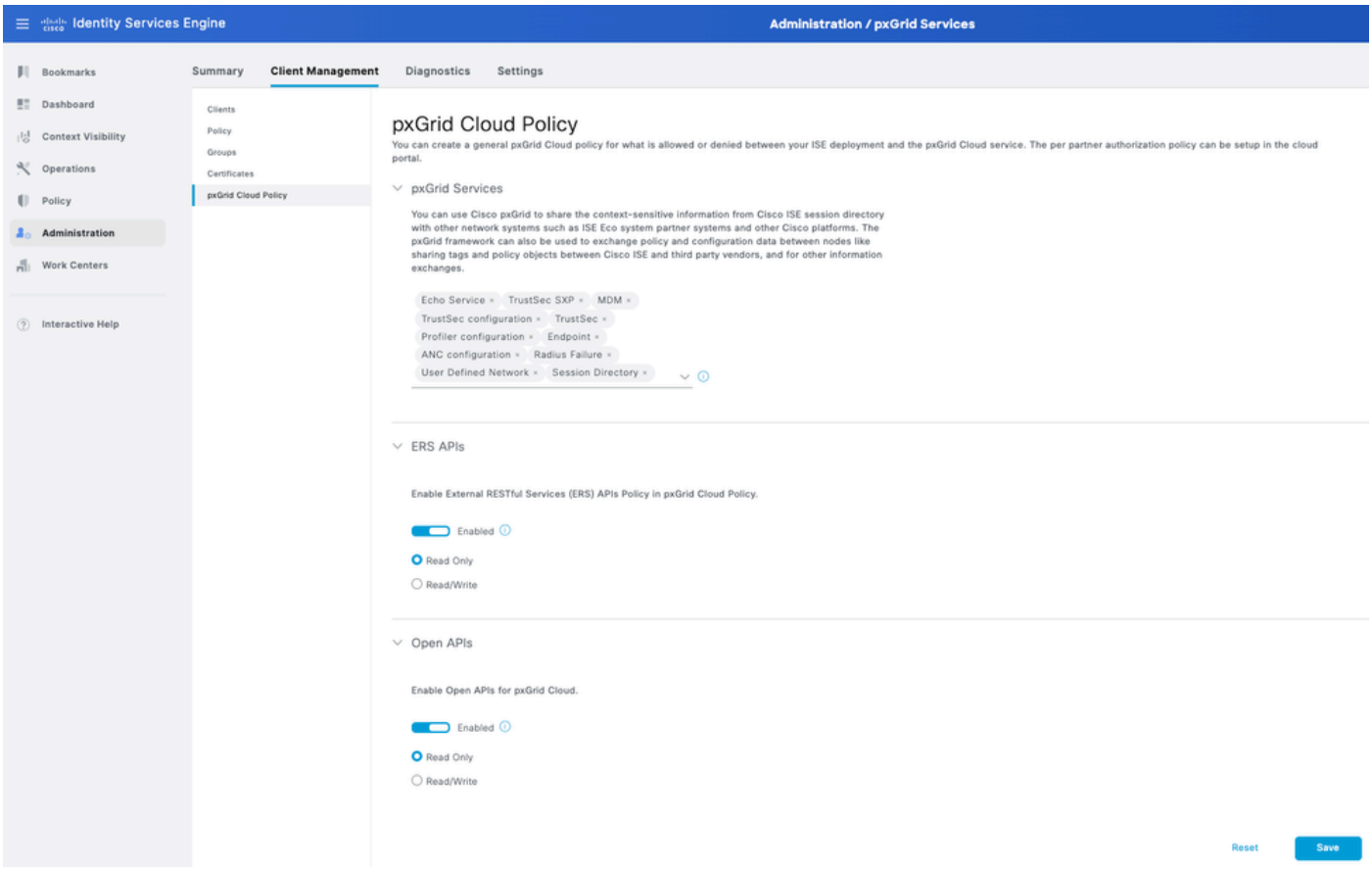
FMC Application Configuration on ISE

5. From the One-Time Password (OTP) pop-up, copy the OTP to redeem it on cdFMC while creating pxGrid Application instance

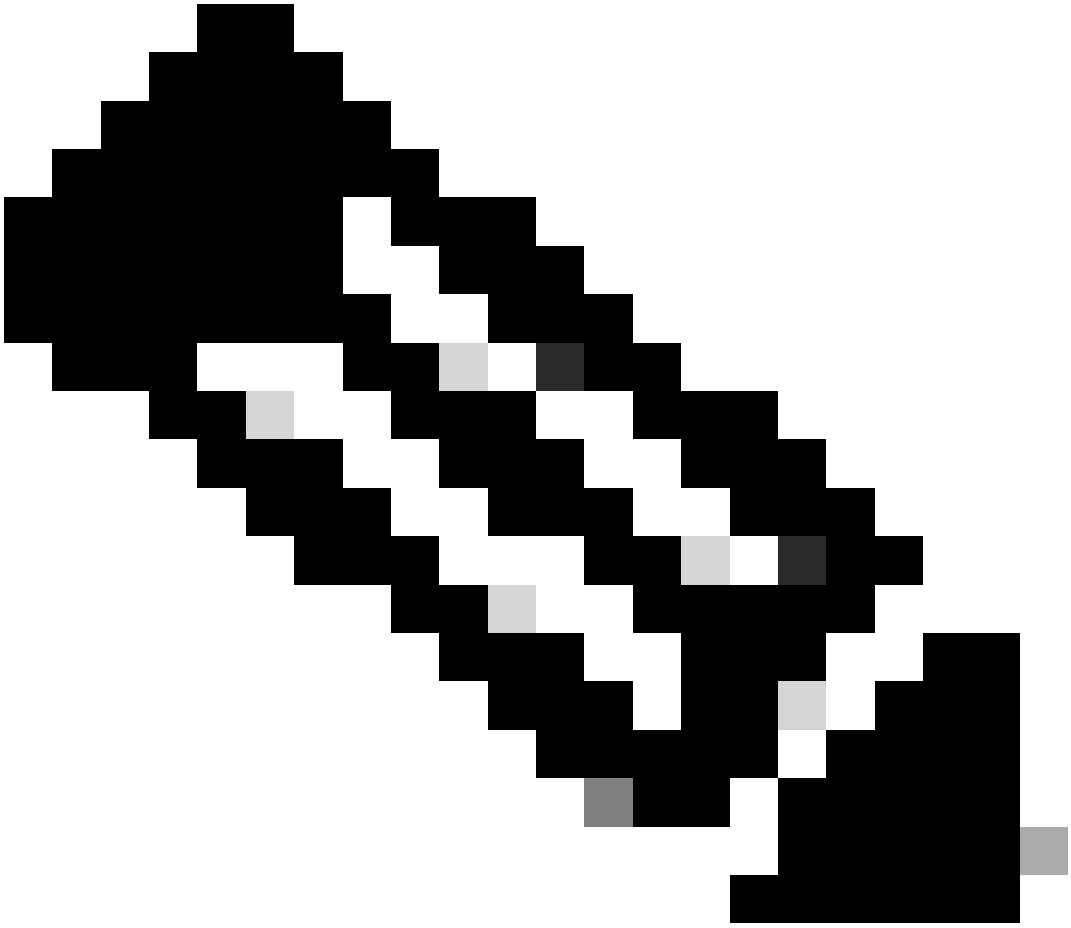


OTP for cdFMC Application

6. Configure pxGrid Cloud Policy by navigating to **Administration > pxgrid Services > Client Management > pxGrid Cloud Policy.** Select the pxGrid services, that you wish to share with the Saas Applications and enable **External RESTful Services (ERS) APIs** and **OpenAPIs** read only access to Cisco pxGrid Cloud applications.



Configure pxGrid Cloud Policy

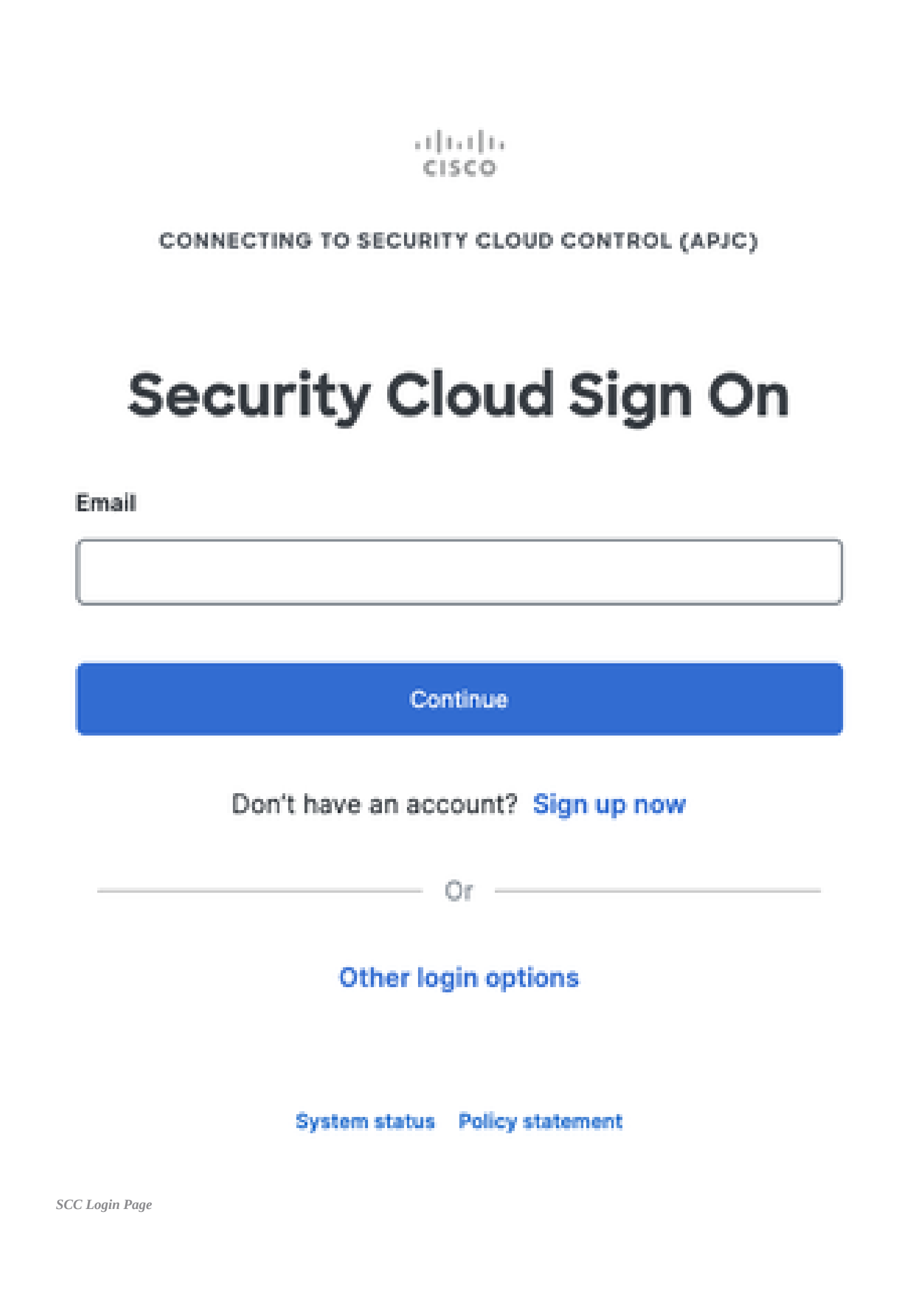


Note: Echo service is used to run health checks to determine both pub-sub and API connectivity to ISE.

By default, the Cisco pxGrid Cloud applications are granted Read Only access to the APIs (only HTTP GET operations can be performed). Enable the **Read/Write** option in the **pxGrid Cloud Policy** window if you want to allow POST, PUT, and DELETE operations as well.

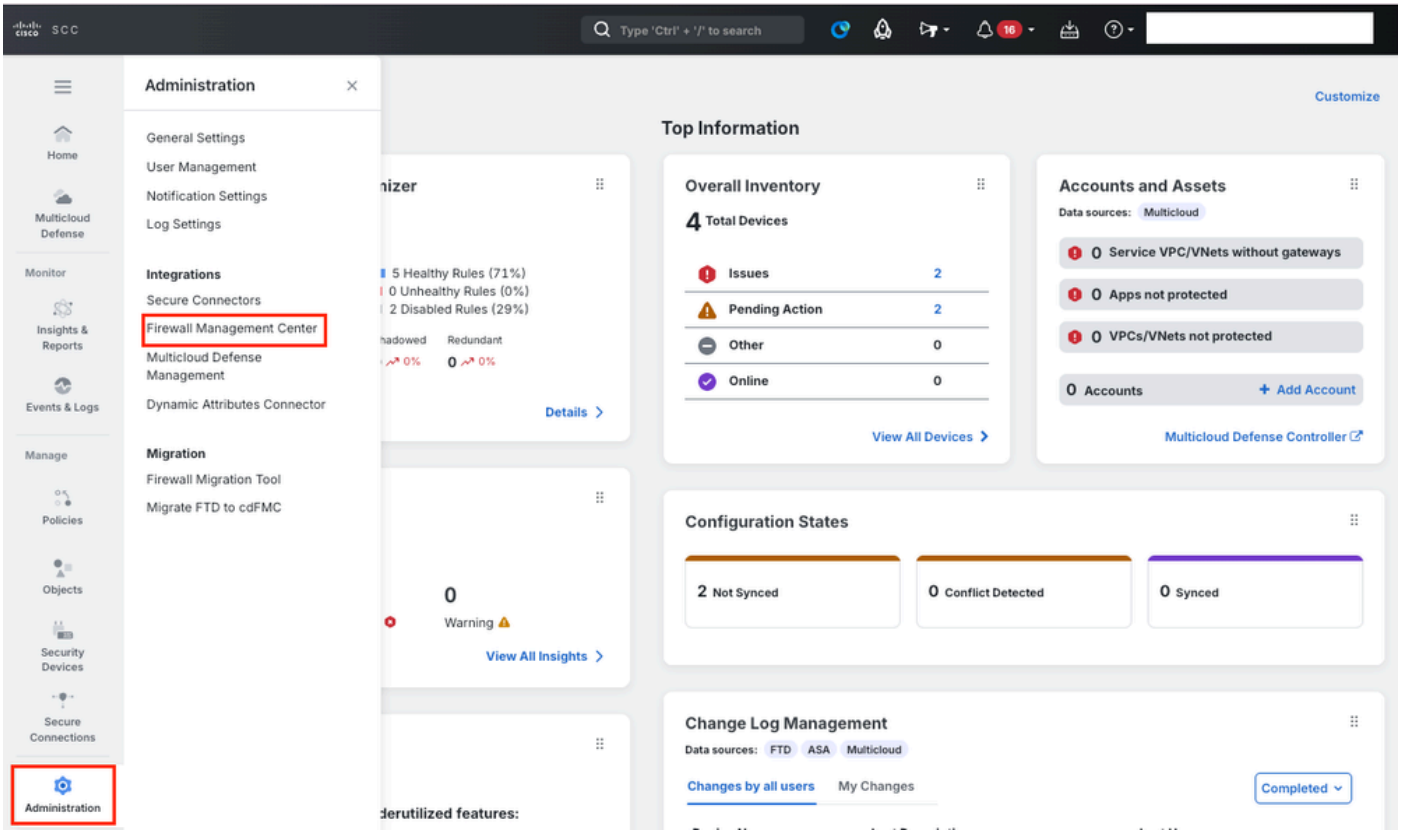
Create pxGrid Application (cdFMC) Instance

1. Login to Security Cloud Control (SCC) Portal as a user with the Super Admin role.



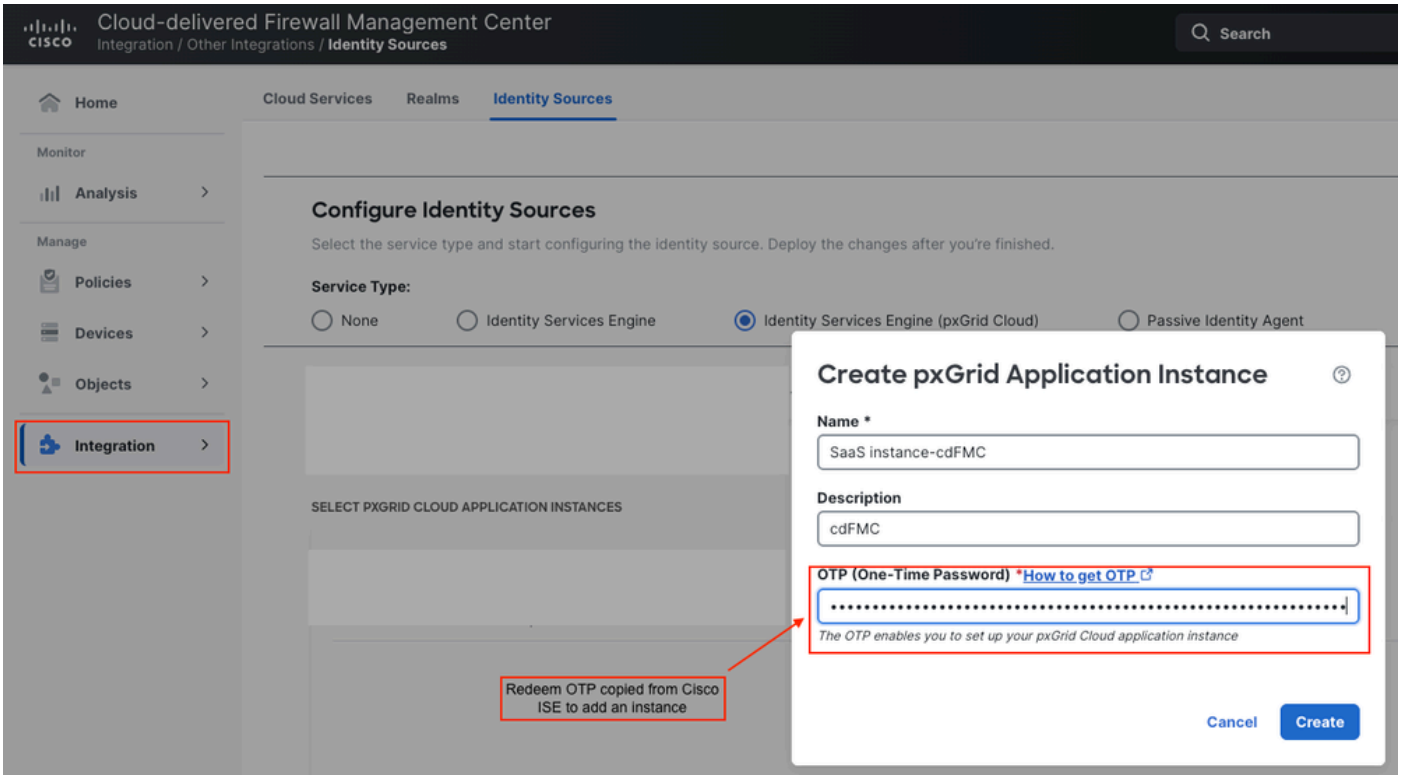
SCC Login Page

2. From the Security Cloud Control menu, click A**dministration > Integrations > Firewall Management Center** and select your cdFMC instance and on the right pane options, select **System > Configuration**.



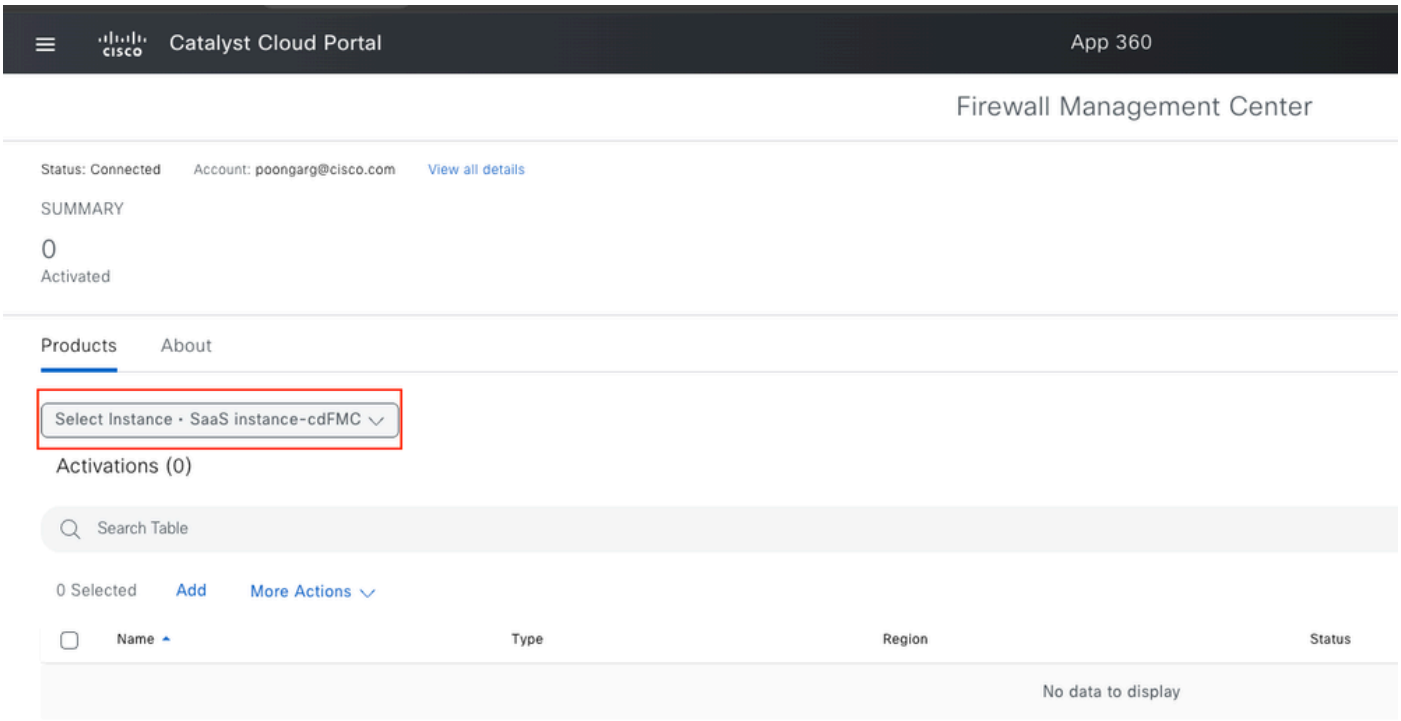
Navigating to Firewall Management Center

3. On the Configuration Page, select **Integration > Other Integrations > Identity Sources** > Choose **Service Type Identity Services Engine (pxGrid Cloud)**. Click on **Create pxGrid Application Instance** and redeem the OTP copied from Cisco ISE to add an instance.



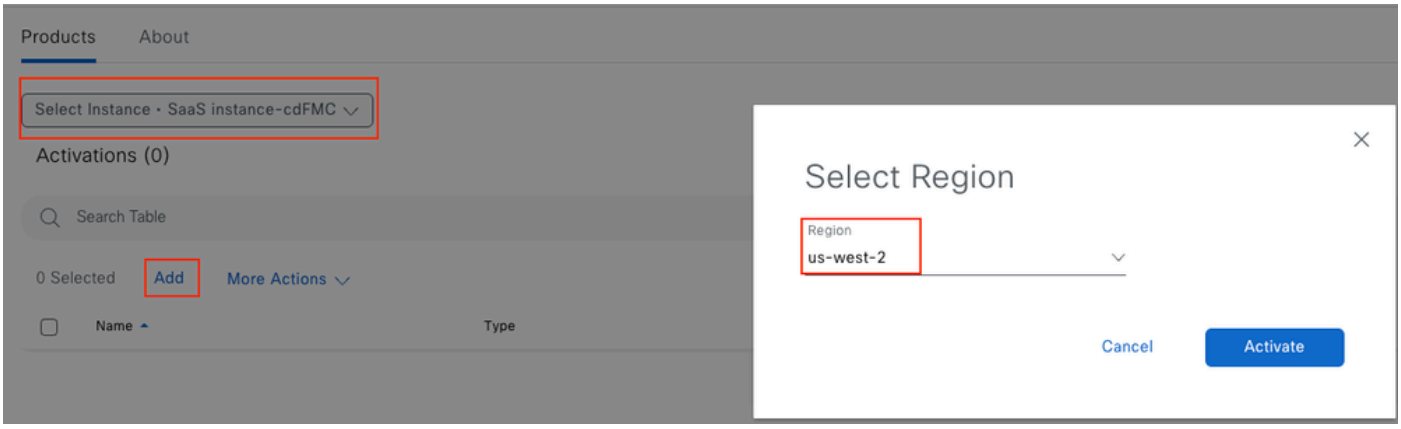
Create cdFMC Application Instance

4. Verify it on Cisco Catalyst Cloud Portal at **Applications and Products > Firewall Management Center > Manage > Products >** Select **Instance drop down menu**.



Verify the cdFMC on Catalyst Cloud Portal

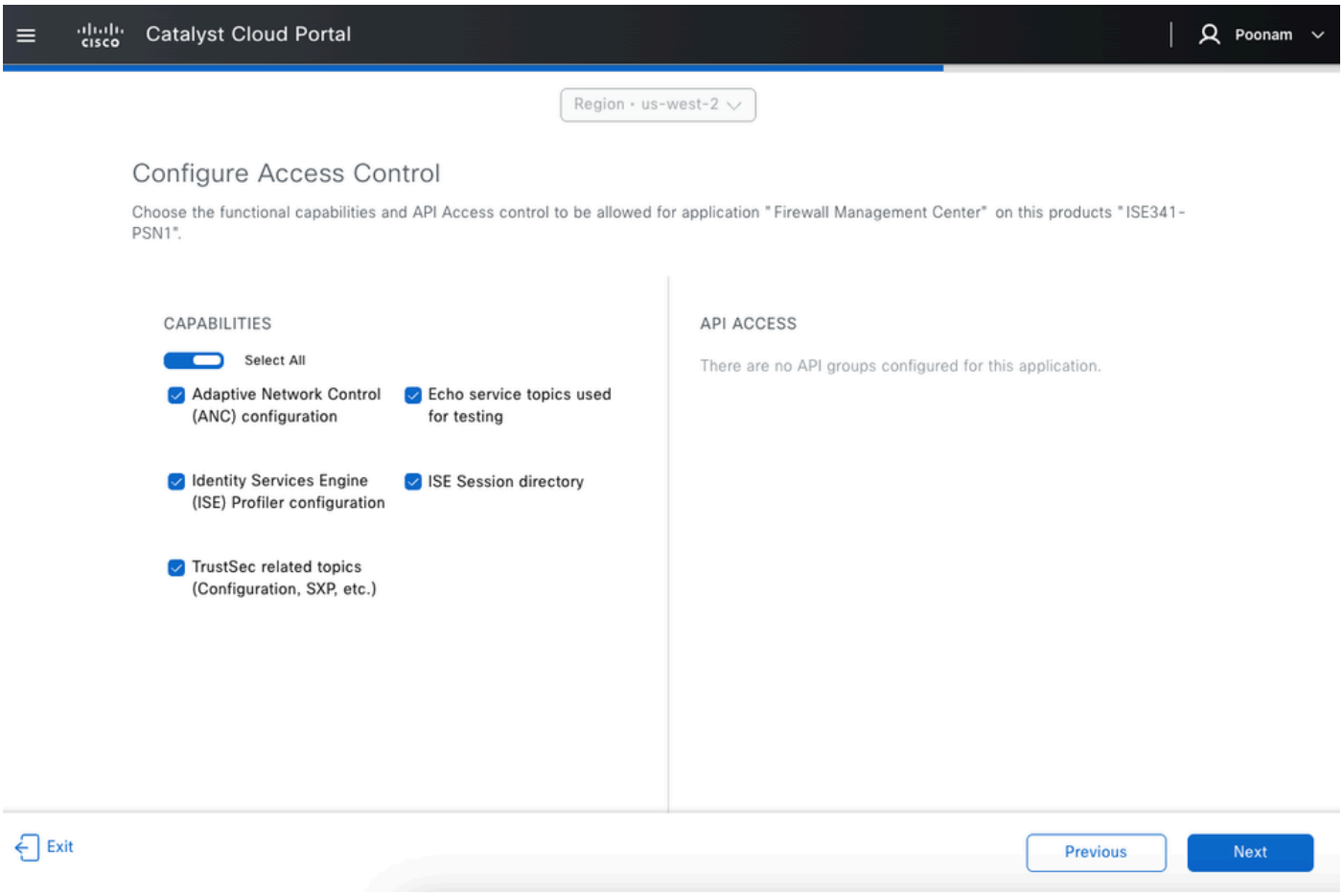
5. Select newly created cdFMC application and click **Add**. Select **Region** and click **Activate**.



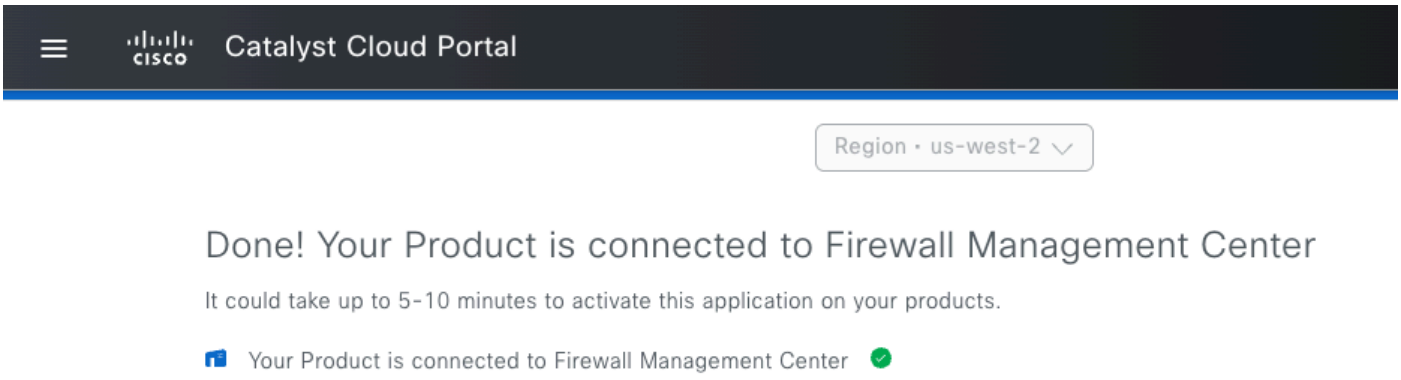
Select Region

5. Choose your application instance and click **Next**. Choose your Product (ISE pxGrid node), click **Next**.

6. **Configure Access Control:** Choose the functional capabilities to be allowed for cdFMC on your choosen ISE product. Click **Next**. Configuration summary is displayed. Verify and click **Activate**.

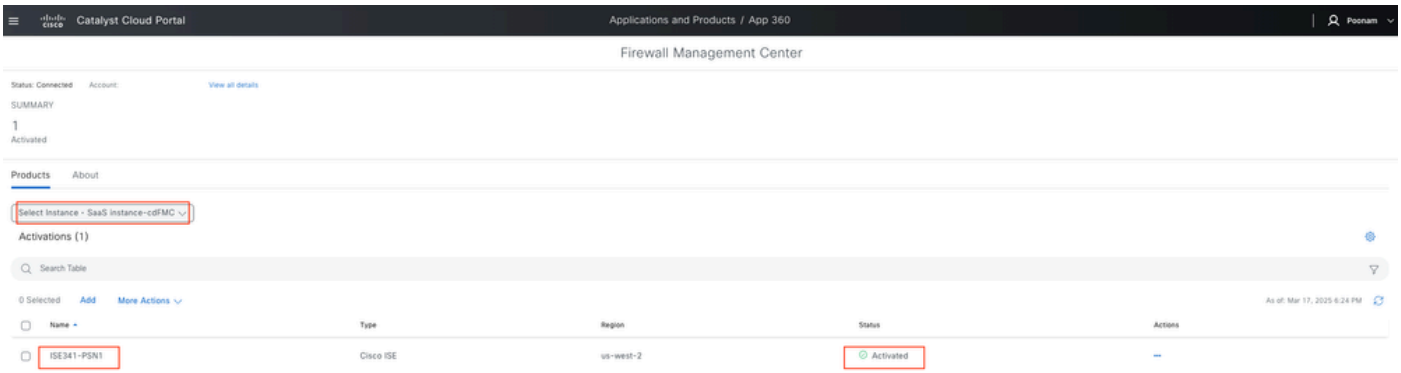


Configure Access Control for your cdFMC



Product ISE connected to cfFMC

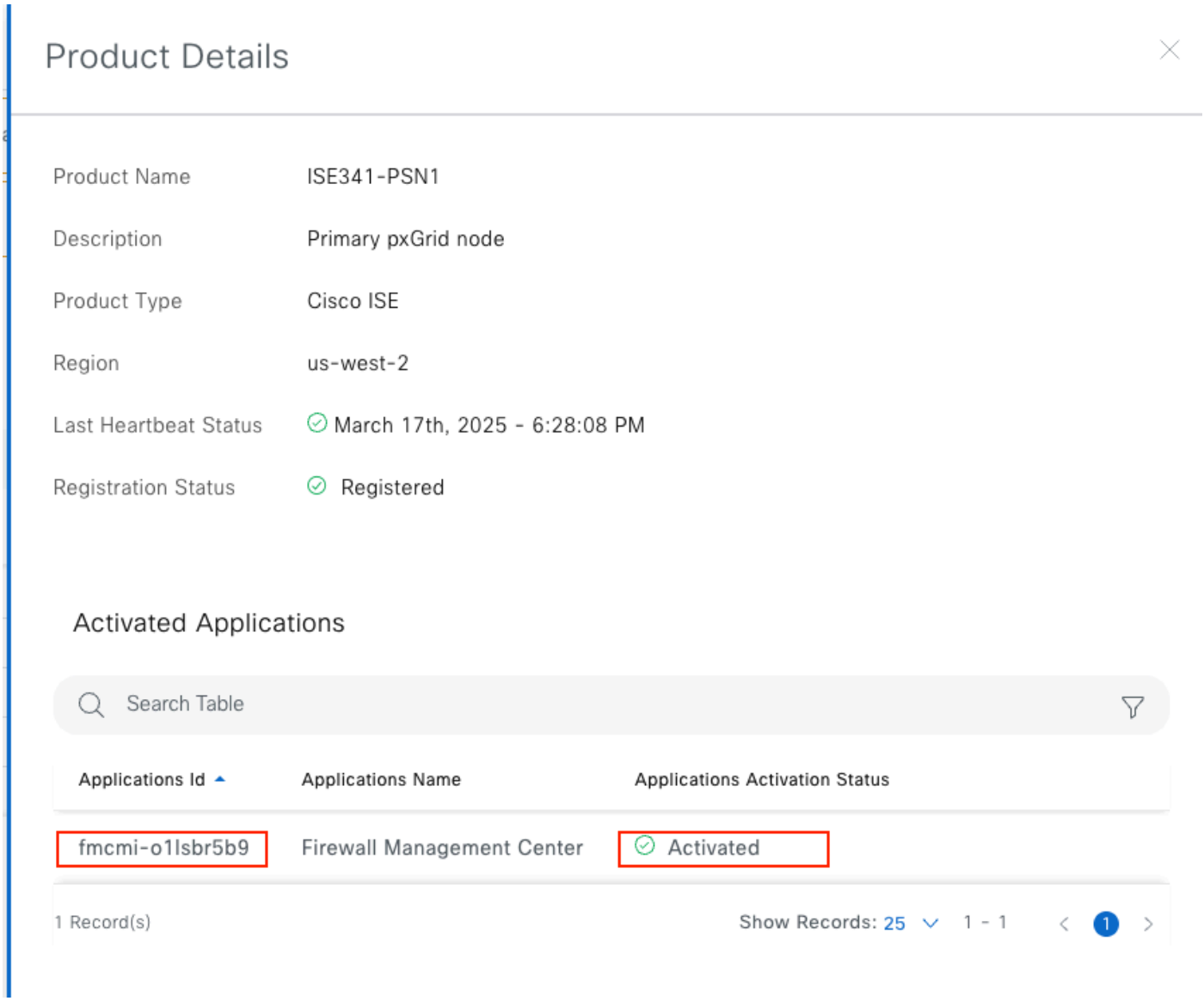
8. Verify it on Cisco Catalyst Cloud Portal at **Applications and Products > Firewall Management Center > Manage > Products >** Select **Instance drop down menu**.



Verify that App is activated

Verify

1. On the Catalyst Cloud Portal, Navigate to **Applications and Products**. Select your ISE product name and check the Product Details. Verify that cdFMC is seen under Activated Application.



Verify on Catalyst Cloud Control Portal

2. On Security Cloud Control, test the configured cdFMC application Instance. The test shows "Success"



Verify on Security Cloud Control Portal

3. Login to Active pxGrid node and verify that Hermes (pxGrid Cloud Agent) is in running state using the command **show application status ise**. This agent is in disabled status on Standby pxGrid node.

```
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
```

Verify Hermes (pxGrid Cloud Agent) status

Check the pxcloud.log on both pxGrid nodes to confirm the Active and Standby Status:

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)

Additionally check the port 8913, which gets opened only on the ACTIVE pxGrid node:

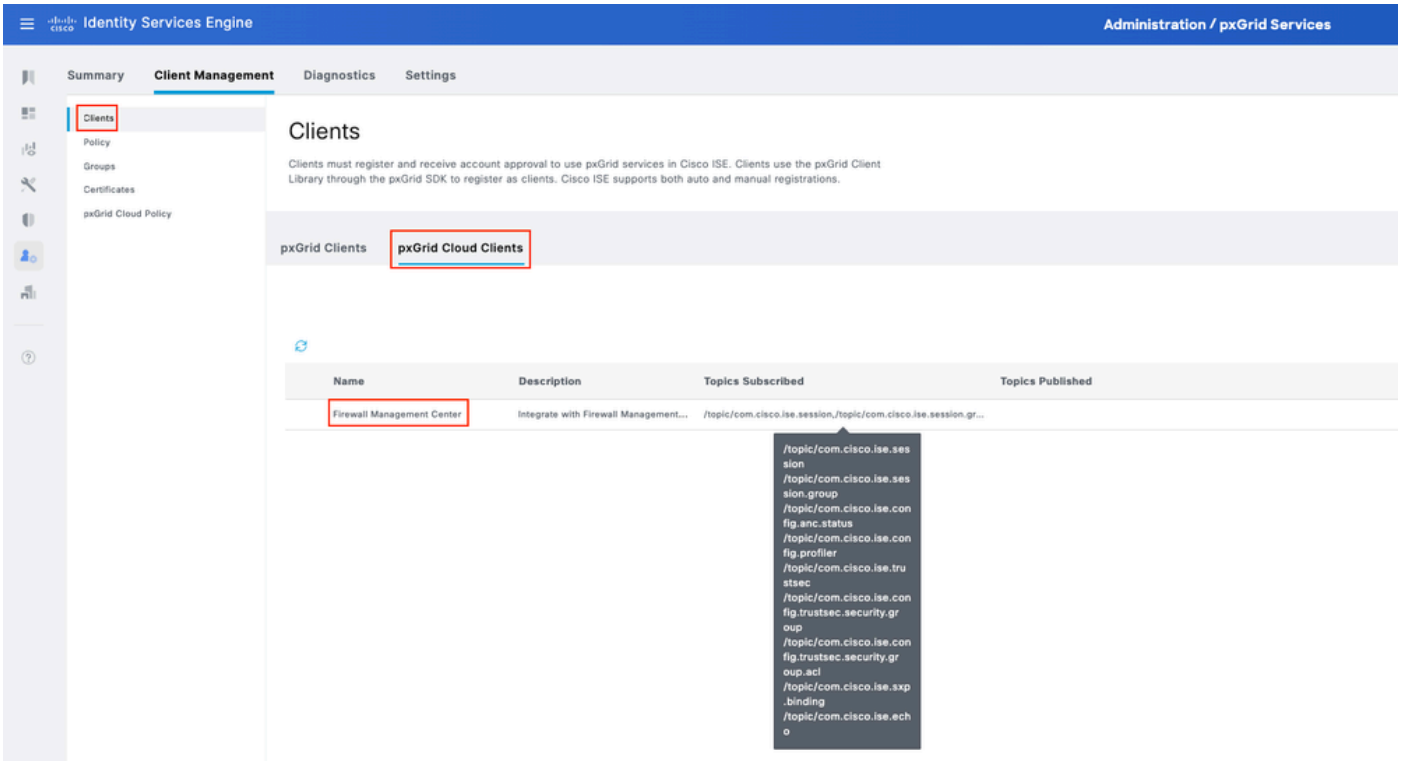
<#root>

ise341-psn1/admin#show ports | include 8913
tcp:

127.0.0.1:8913

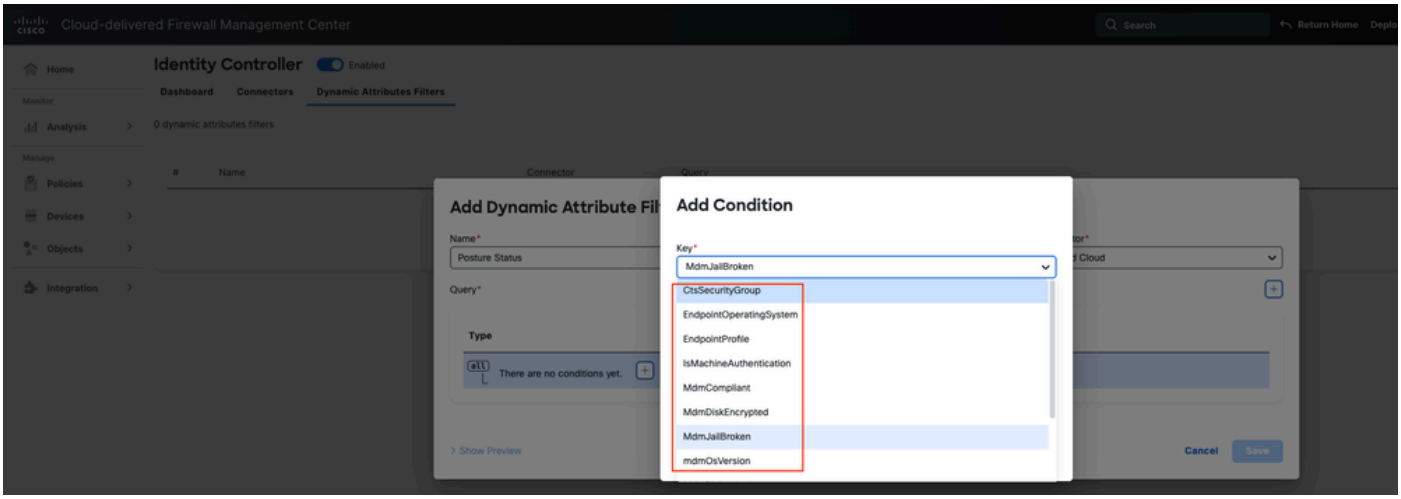
ise341-psn1/admin#

4. Verify pxGrid cloud client by navigating to **Administration > pxGrid Services > Client Management > Clients > pxGrid Cloud clients**. Also check the subscribed topics.



pxGrid Cloud Client on ISE

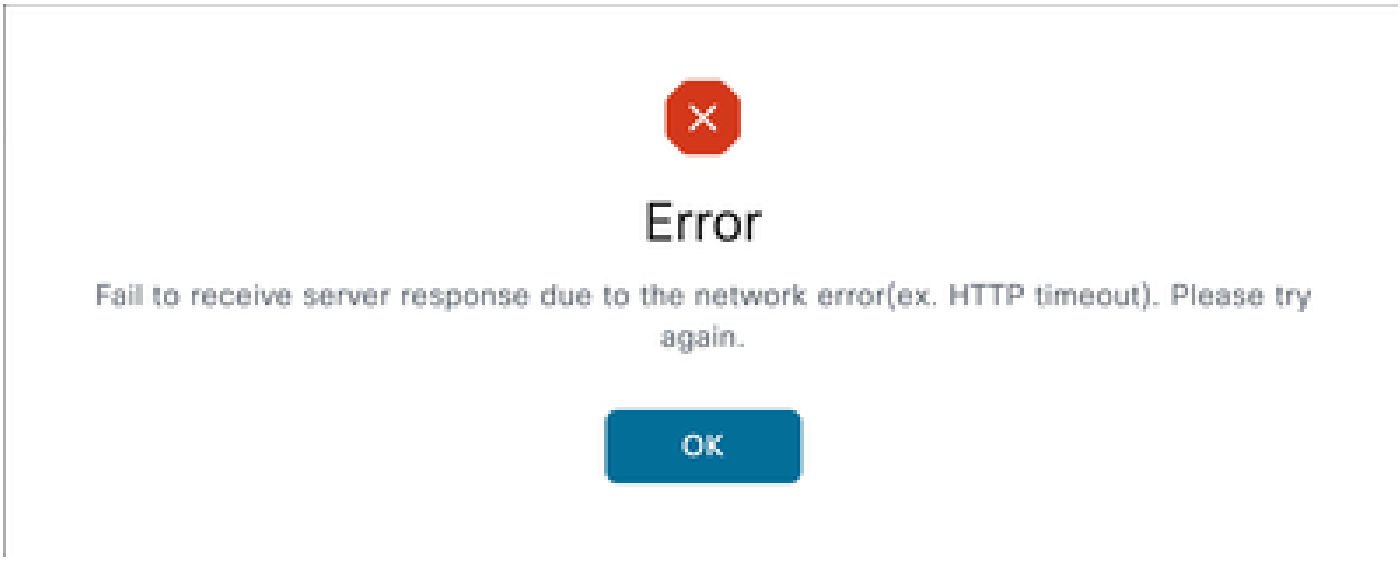
5. Verify the subscribed Topics are fetched on cdFMC. On Security Cloud Control portal, Click **Policies > Threat Defense > Integration > Other Integrations > Identity Sources**. Click **Identity Services Engine (pxGrid Cloud)**. Click **Configure Filters**. On the page, click the **Dynamic Attributes Filter** tab. Create a **Dynamic Attributes Filter**.



Fetched attributes from ISE

Troubleshoot

1. Failure during ISE registration:



Missing Proxy Configuration

Check the internet connectivity and possible proxy misconfiguration.

2. pxGrid status shows **Not connected** on ISE Edit node page after enabling pxGrid Cloud service and configuring the name and region parameters.

Check the **hermes.log** on the node where you are enabling the **pxGrid Cloud** service:

<#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 connecti

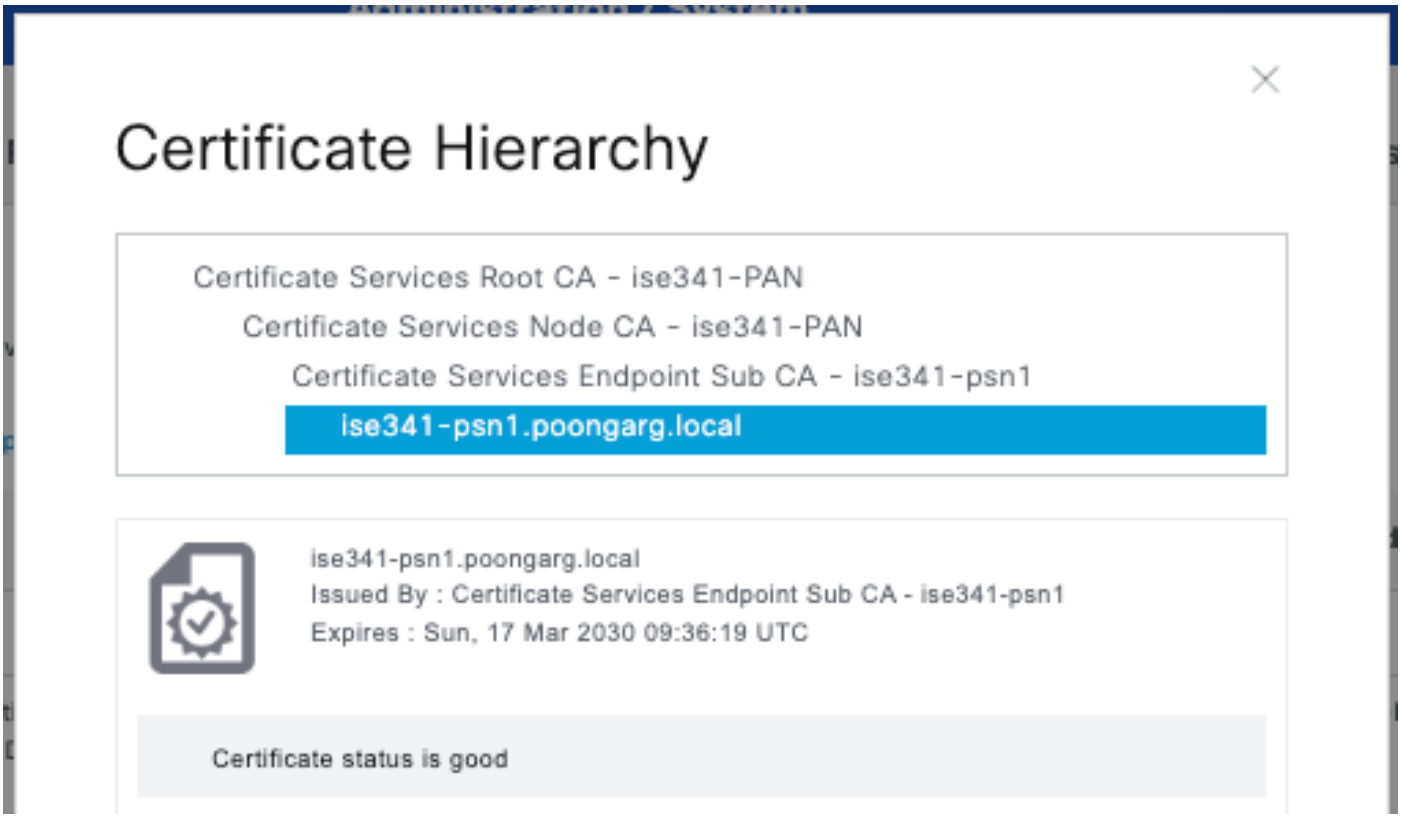
"https://ise341-psn1.poongarg.local:8910/pxgrid/control/ServiceLookup": SSL errors: SSL routines:tls_pro

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 DISCONN
2025-03-17T09:19:35.308Z | ERROR | hermes/main.go:402 | Error running Hermes: Failed to establish pxGri
2025-03-17T09:19:35.308Z | INFO | hermes/httpserver.go:90 |

Stopping REST server on :8913

Hermes Rest server listen on port 8913. Logs clearly shows that Hermes REST server is trying to start but failed to establish pxGrid WebSocket connection due to Certificate verification failure.

Solution: Verify that the pxGrid Certificate is valid and the certificate chain is not broken. View the certificate and verify **Certificate status is good**. In this case, the ISE host name was incorrect in the pxGrid certificate issued to this node.



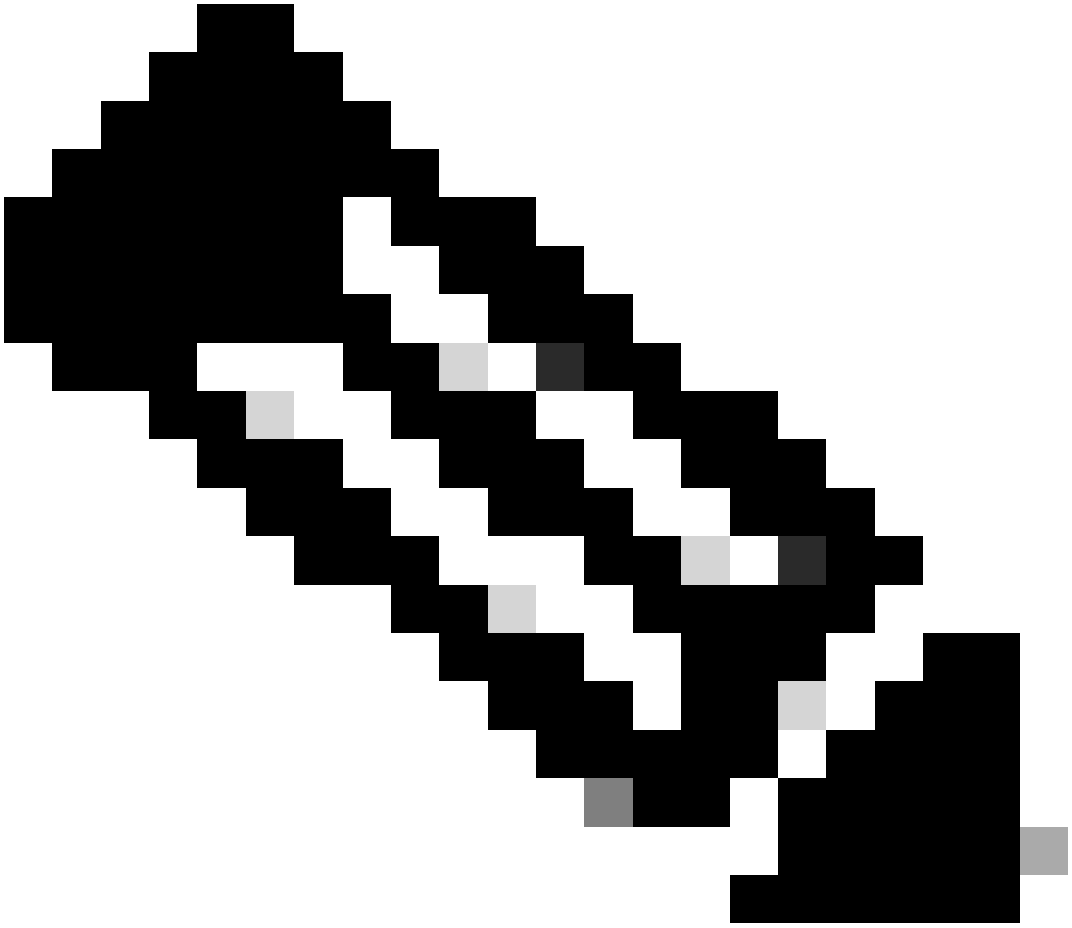
Valid pxGrid certificate

3. cdFMC application activation failed on Catalyst Cloud Portal.

Solution: Make sure that on ISE, under the pxGrid Cloud Policy, External RESTful Services (ERS) APIs and OpenAPIs read only access is enabled.

Logs related to pxGrid Cloud feature:

Debug Component	**Log File Name**	Description
pxGrid Cloud	pxcloud.log, hermes.log	pxcloud.log: It logs pxGrid cloud service config changes, pxGrid Cloud service connection status and High-availability status hermes.log: logs pxGrid topic subscription status, ERS Rest requests form pxGrid Cloud, Configuration changes on ISE.
pxGrid Cloud OpenAPI	pxcloud.log, hermes.log	
Telemetry	sch.log	log is generated when user uses Integration Catalog. It includes initial logs with token used to connect to pxGrid Cloud.



Note: Regardless of the node on which you are enabling the pxGrid Cloud persona, you need to check the logs on the **active PAN node**. Once device is registered, the Hermes logs is on the specific node where it is enabled.

Hermes.log supports only the **Debug**, **Info**, **Warn**, and **Error** log levels. Hence, if you choose **Trace**, the log level is set as **Debug** for hermes.log. If you choose **Fatal**, the log level is set as **Error** for hermes.log.

ISE Enrollment/Registeration and App. activation Flow

Before the device is registered, ISE uses a device token to fetch list of regions, list of apps from the cloud. This token is provide by the "telemetry" component of ISE. Check sch.log on PAN node:

```
2025-03-17 09:10:23,361 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.DNATelemetryClie
2025-03-17 09:10:23,361 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.DNATelemetryClie
2025-03-17 09:10:23,463 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.TetheringStateSt
2025-03-17 09:10:23,467 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.TetheringStateSt
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.DNATelemetryClie
```

```
2025-03-17 09:10:23,483 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.DNATetheringClie
2025-03-17 09:10:24,492 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.TetheringStateSt
2025-03-17 09:10:24,497 INFO [openapi-http-pool7][[]] infrastructure.telemetry.sch.api.TetheringStateSt
2025-03-17 09:10:24,529 INFO [openapi-http-pool7][[]] cpm.infrastructure.telemetry.api.TelemetryConfigH
```

pxcloud.log (PAN node), once you enable pxGrid Cloud service, Hermes(pxGrid Cloud agent) gets activated and ISE fetch the region information and received a token via telemetry component.

```
2025-03-17 08:47:00,300 INFO [main][[]] cisco.cpm.pxcloud.api.PxCloudInitializer -::::- Initializing p
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.PxcloudApplicationCatalogIm
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.PxcloudApplicationCatalogIm
2025-03-17 09:10:27,533 DEBUG [openapi-http-pool7][[]] cpm.pxcloud.api.impl.PxcloudApplicationCatalogIm
2025-03-17 09:10:27,533 DEBUG [openapi-http-pool7][[]] cpm.pxcloud.api.impl.PxcloudApplicationCatalogIm
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
```

Activation link is received and auto register and enrollment happens.

```
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.CloudConfiguratio
```

pxGrid node assume ACTIVE role, however, here we observed pxGridConnectionStatus as NOT_CONNECTED, which got fixed after adding the right pxGrid Certificate (with complete root CA chain) on this pxGrid node)

```
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
```

Now check Hermes.log on ACTIVE pxGrid node for pubsub events:

```
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
```

Root CA chain of Catalyst Cloud Portal is verified.

```
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
```

Specific Topics subscription request got created once, FMC application is configured under Integration Catalog:

```
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.cisc
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.cisc
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
```

Limitations

1. User cannot enable pxGrid Cloud persona on more than 2 nodes.

2. De-registration from Catalyst Cloud Portal to cdFMC is supported but not vice-versa.

References

User Control with the pxGrid Cloud Identity Source

Cisco pxGrid Cloud

Cisco pxGrid Cloud Solution Guide