通过pxGrid云将云交付的防火墙管理中心与ISE集成

目录

简介

本文档介绍通过pxGrid云将Cisco ISE与云交付的防火墙管理中心(cdFMC)集成的过程。

先决条件

- 思科身份服务引擎(ISE)的工作知识
- Cisco Catalyst云门户中的帐户
- 思科安全云控制门户上的帐户

要求

- 在思科ISE部署中安装和激活优势许可证层。
- pxGrid云代理创建到思科pxGrid云的出站HTTPS连接。因此，如果网络使用代理访问互联网，请配置Cisco ISE代理设置。要在Cisco ISE中配置代理设置，请选择Administration > System > Settings > Proxy。

- 思科ISE受信任证书库必须包括验证思科pxGrid云提供的服务器证书所需的根CA证书。确保为此根CA证书启用Trust for Authentication of Cisco Services选项。要启用Trust for Authentication of Cisco Services，请选择Administration > System > Certificates。
- 确保端口443为从Cisco ISE到Cisco pxGrid云门户的出站连接打开。如果配置了防火墙或代理设置，请确保这些URL未被阻止。

https://dna.cisco.com

https://dnaservices.cisco.com

https://ciscodnacloud.com

使用的组件

ISE软件版本：3.4补丁1,4节点部署（启用pxGrid服务的PAN、SAN和2 PSN）

cdFMC版本：20241127

适用于VMware版本的Cisco Firepower威胁防御(FTD):7.2.5

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

思科pxGrid云术语

下面是Cisco pxGrid云解决方案中使用的一些常用术语及其在Cisco pxGrid云环境中的含义：

- 产品：将一组功能打包在一起并作为解决方案提供
- 订用：租户使用的优惠的实例是订用
- 应用：您可以根据自己的要求为产品创建和注册应用程序。

背景信息

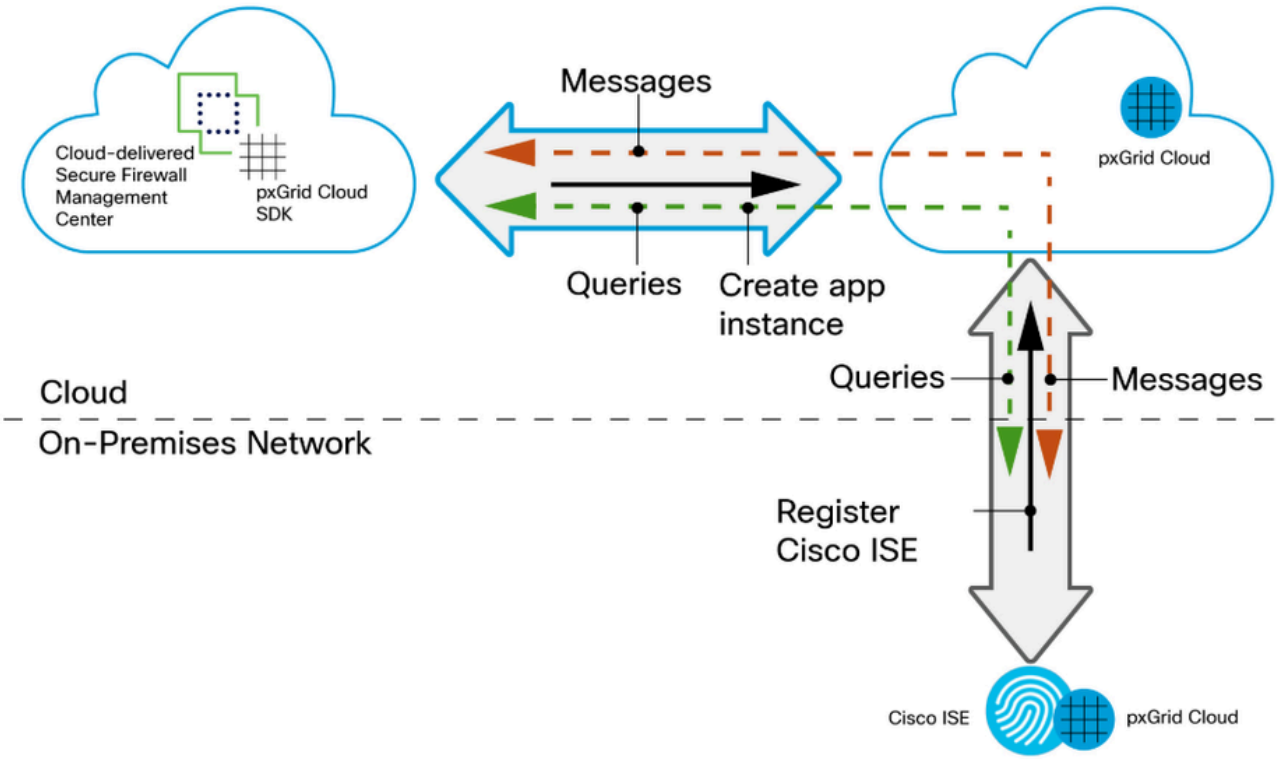
Cisco ISE在多个安全供应商之间提供情景共享；但是，当前架构不允许内部ISE和基于云的解决方案通过网络边界进行通信，而不在防火墙中造成某种旁路/放置漏洞。

思科ISE的pxCloud是基于云的解决方案，可解决此问题，并在本地和云之间实现情景共享，无需额外的安装、开销和影响网络安全性。它安全且可自定义，使您可以仅共享想要共享的数据，并仅使用与您的应用程序相关的情景数据。

思科ISE版本3.1补丁3及更高版本支持pxGrid云。思科及其合作伙伴可以开发基于pxGrid云的应用，并使用pxGrid云产品注册这些应用。思科依靠cisco DNA-Cloud Portal来加入和注册应用，无需依赖其他内部基础设施。这些应用使用外部RESTful服务(ERS)、开放式API和pxGrid（API和Websocket）与思科ISE交换信息，以使用cdFMC中ISE的订阅和用户数据。

配置

网络图



通过pxGrid云实现cdFMC和ISE集成

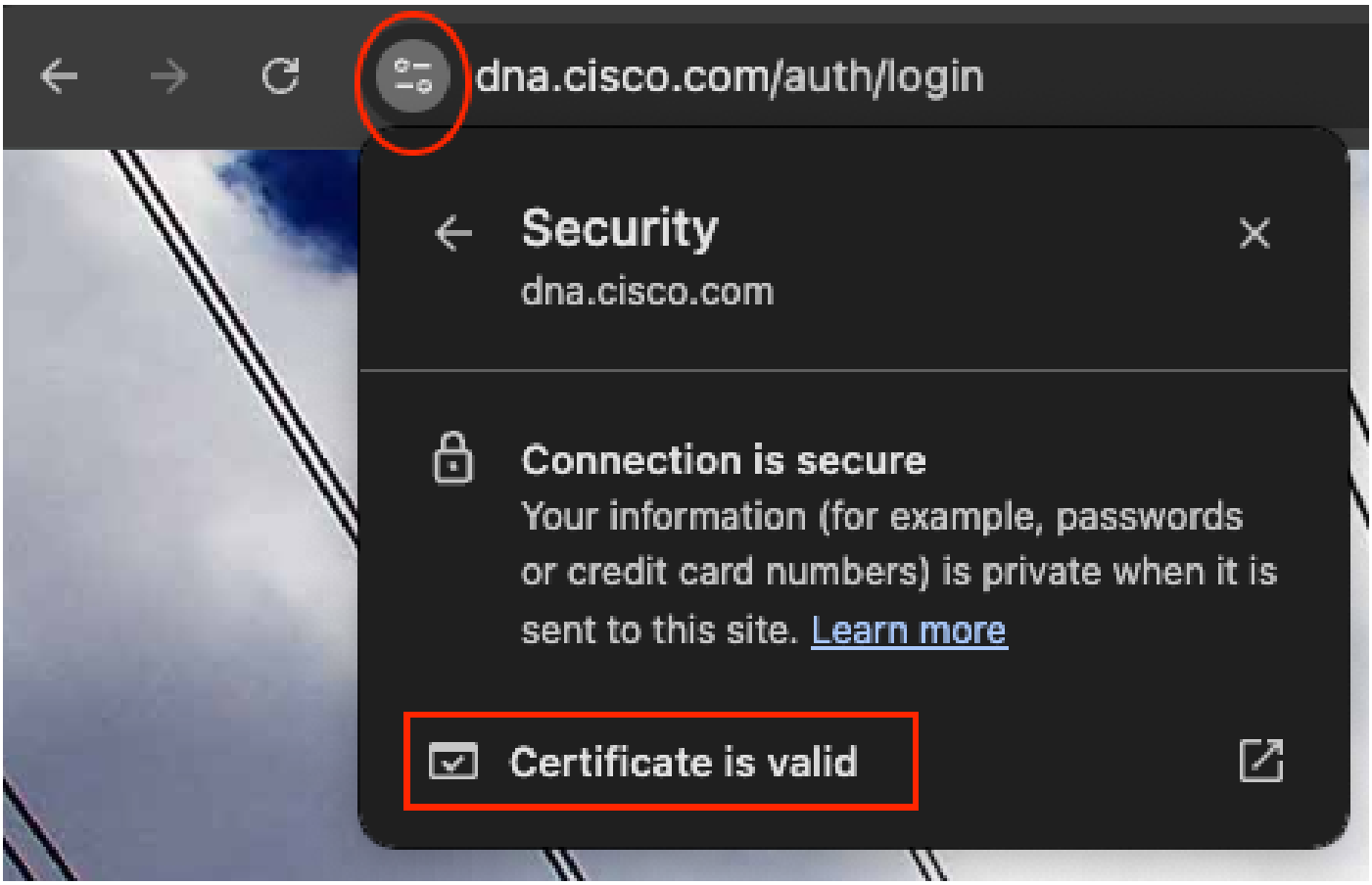
配置

涉及四个主要步骤：

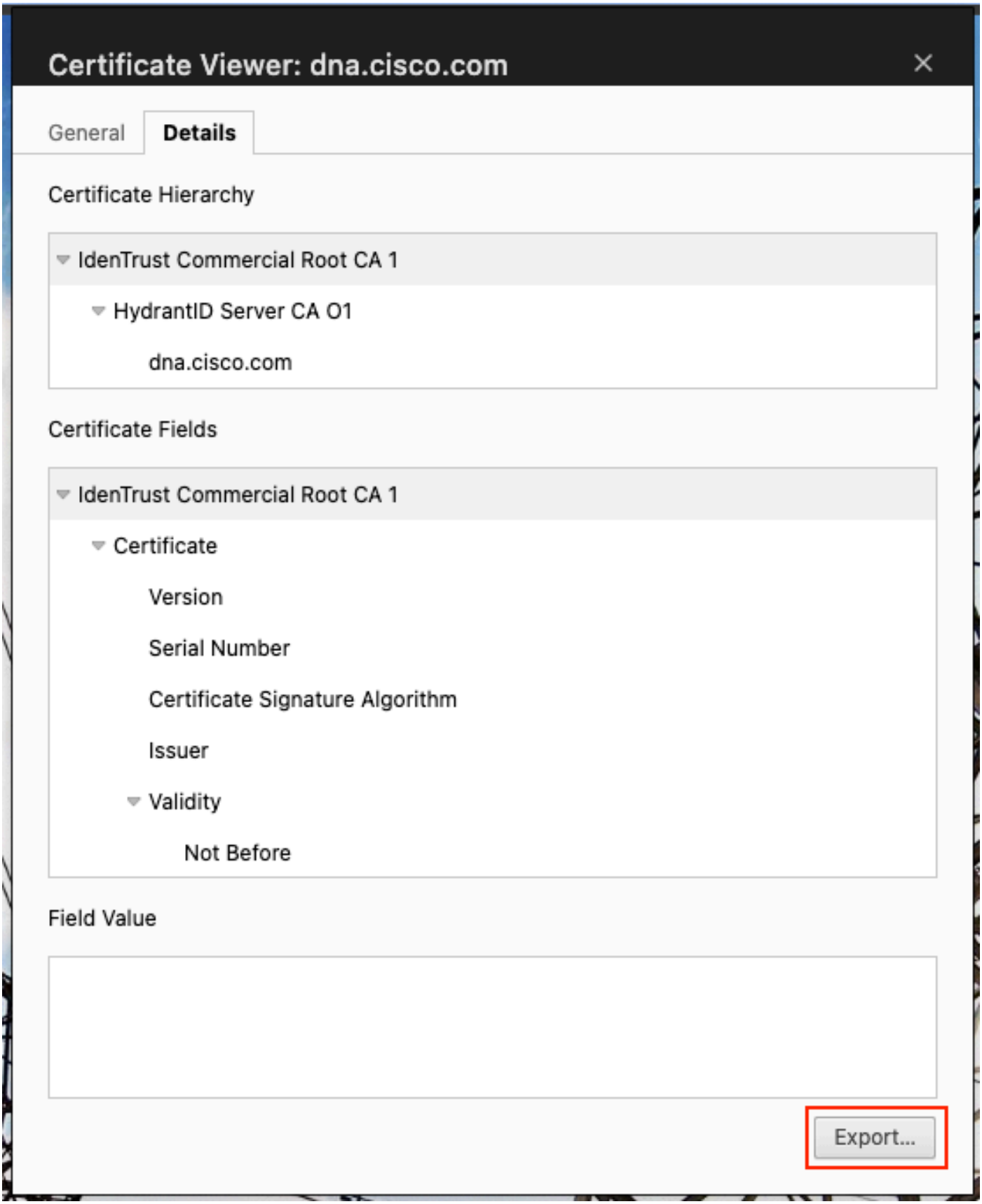
- 导入ISE中的思科pxGrid云服务器证书。
- 向Catalyst云门户注册ISE。
- 使用集成目录在ISE上激活cdFMC应用
- 创建pxGrid应用程序(cdFMC)实例

在ISE中导入思科pxGrid云服务器证书

ISE必须与Cisco pxGrid云建立信任。即使云网站使用公开签名的证书进行身份验证，ISE也不会维护受信任的根CA的完整列表。因此管理员必须建立信任关系。通过浏览到Catalyst Cloud Portal（仅限注册用户）导出pxGrid云根证书和中间证书。大多数浏览器都允许此操作。以下是从Chrome浏览器获取证书的步骤。


dna.cisco.com/auth/login
Security
dna.cisco.com
Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more
Certificate is valid

查看站点信息

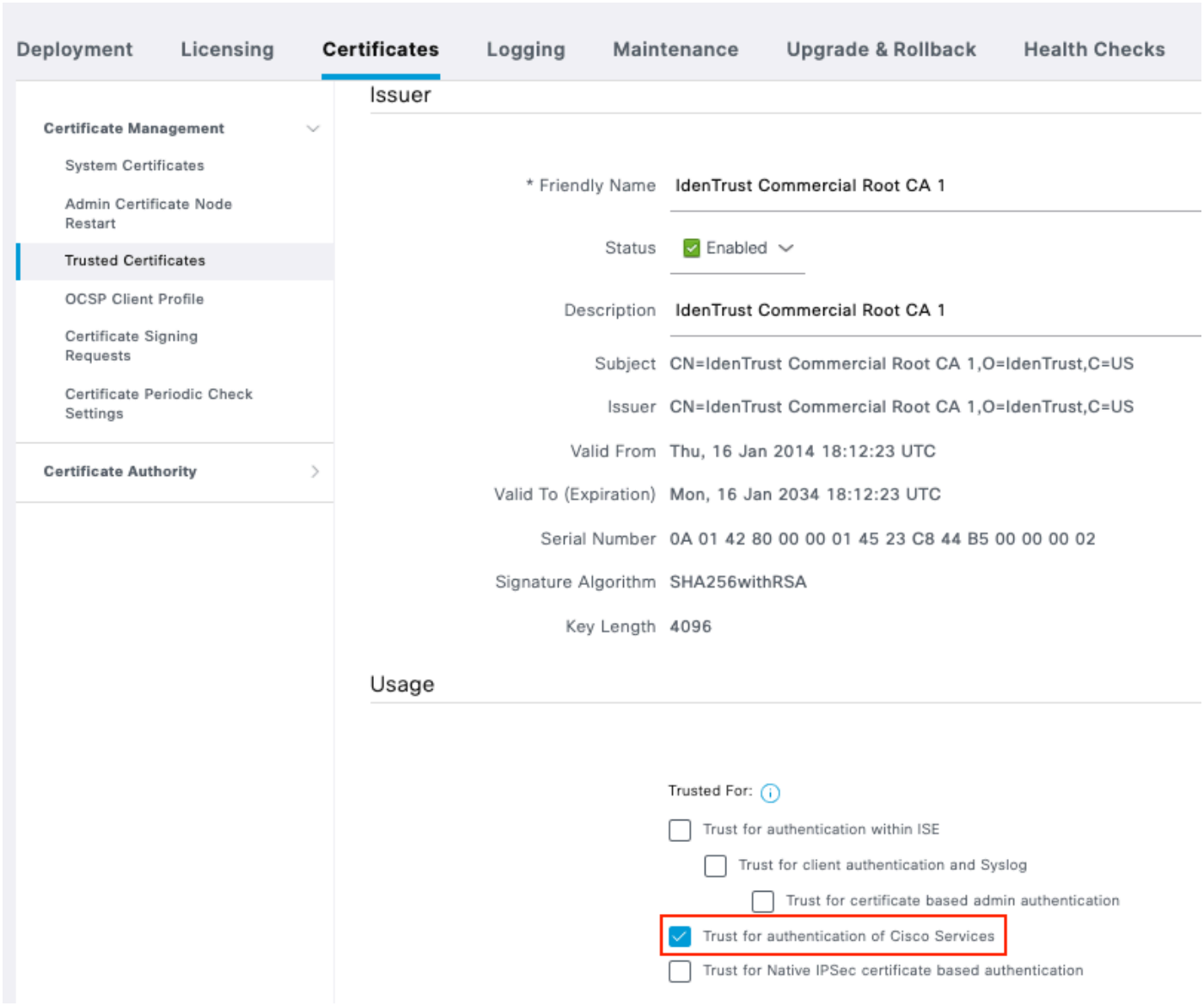


导出证书链

如果证书链缺失（ISE已具有IdenTrust Commercial Root CA 1），请将证书导入ISE中的“Trusted Certificates”存储区。

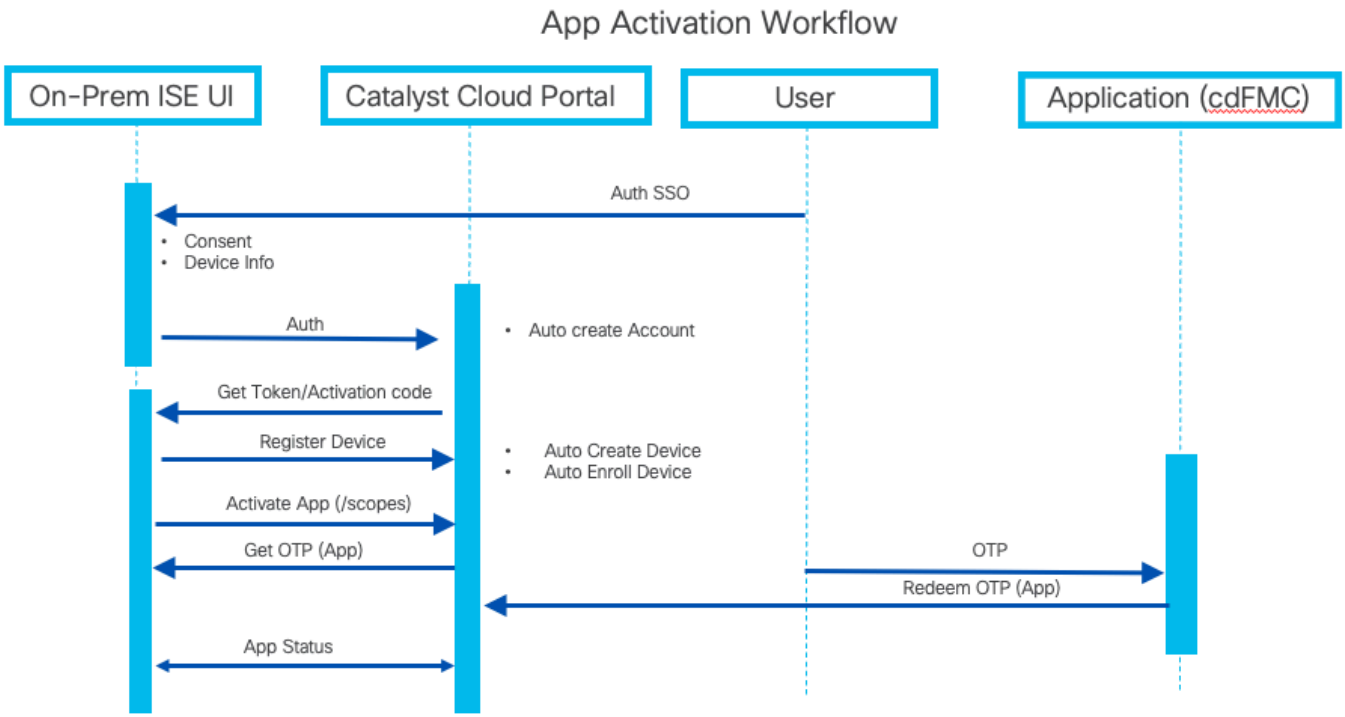
确保为此根CA证书启用“Trust for Authentication of Cisco Services”选项。要启用Trust for

Authentication of Cisco Services，请选择Administration > System > Certificates。



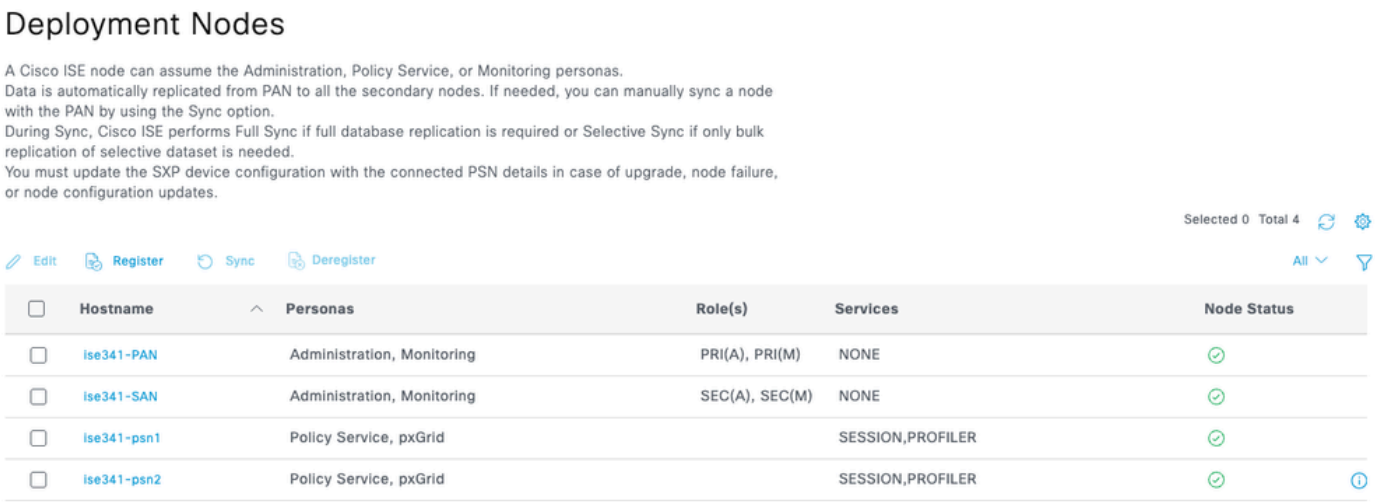
为思科服务的身份验证启用信任

流程图



应用激活工作流程

在此设置中使用的ISE部署



使用Catalyst云门户注册ISE

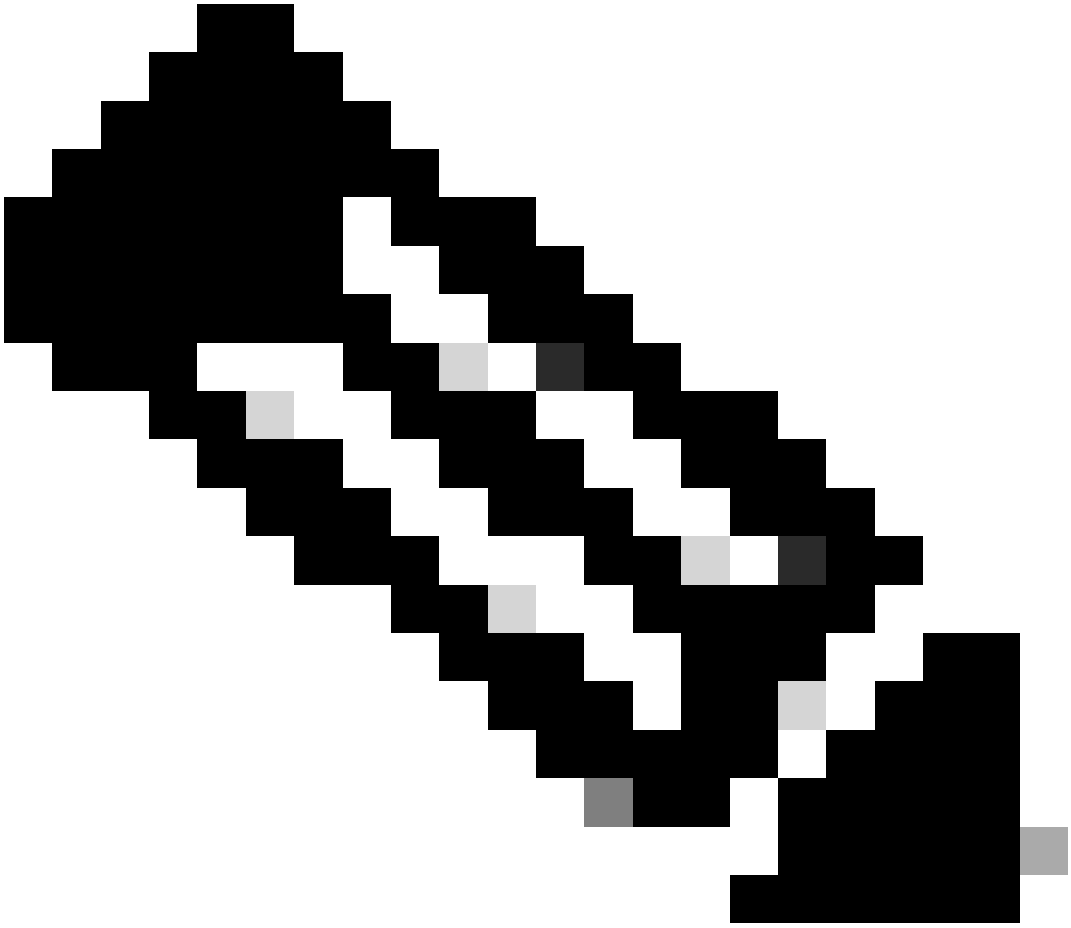
在思科ISE中启用pxGrid云服务并注册您的设备。

1.在Cisco ISE GUI中，选择Administration > System > Deployment。

2.点击要在其上启用pxGrid云服务的节点（在本例中是第一个PSN节点）。

3.在General Settings选项卡中，启用pxGrid服务。

4.选中pxGrid Cloud复选框。



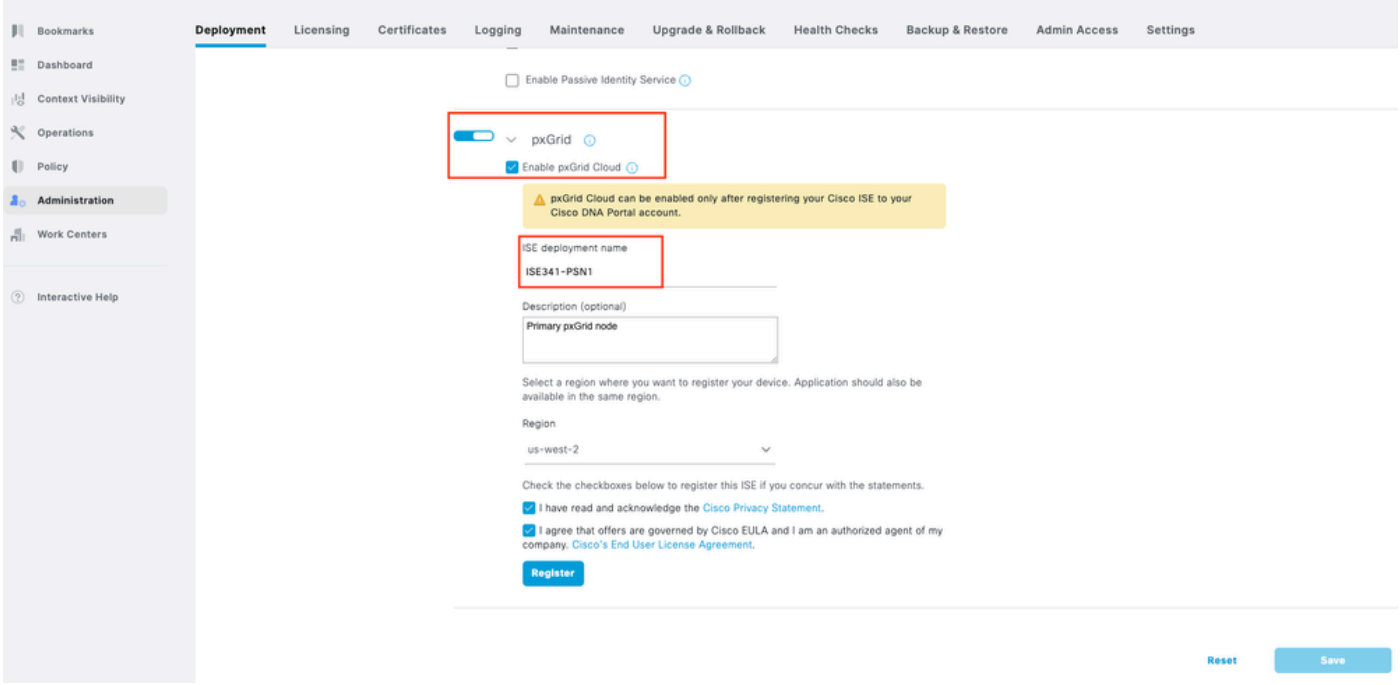
注意：pxGrid云服务只能在两个节点上启用，以实现高可用性。仅当在该节点上启用pxGrid服务时，才能启用pxGrid云选项。

5.在ISE部署名称字段中，输入有意义的名称。此名称显示在Catalyst云门户中，可用于区分是否向云注册了多个ISE部署。您可以使用ISE部署名称验证在Cisco Catalyst云门户上注册的思科ISE部署。

（可选）在Description（可选）字段中，输入您的Cisco ISE部署的说明。

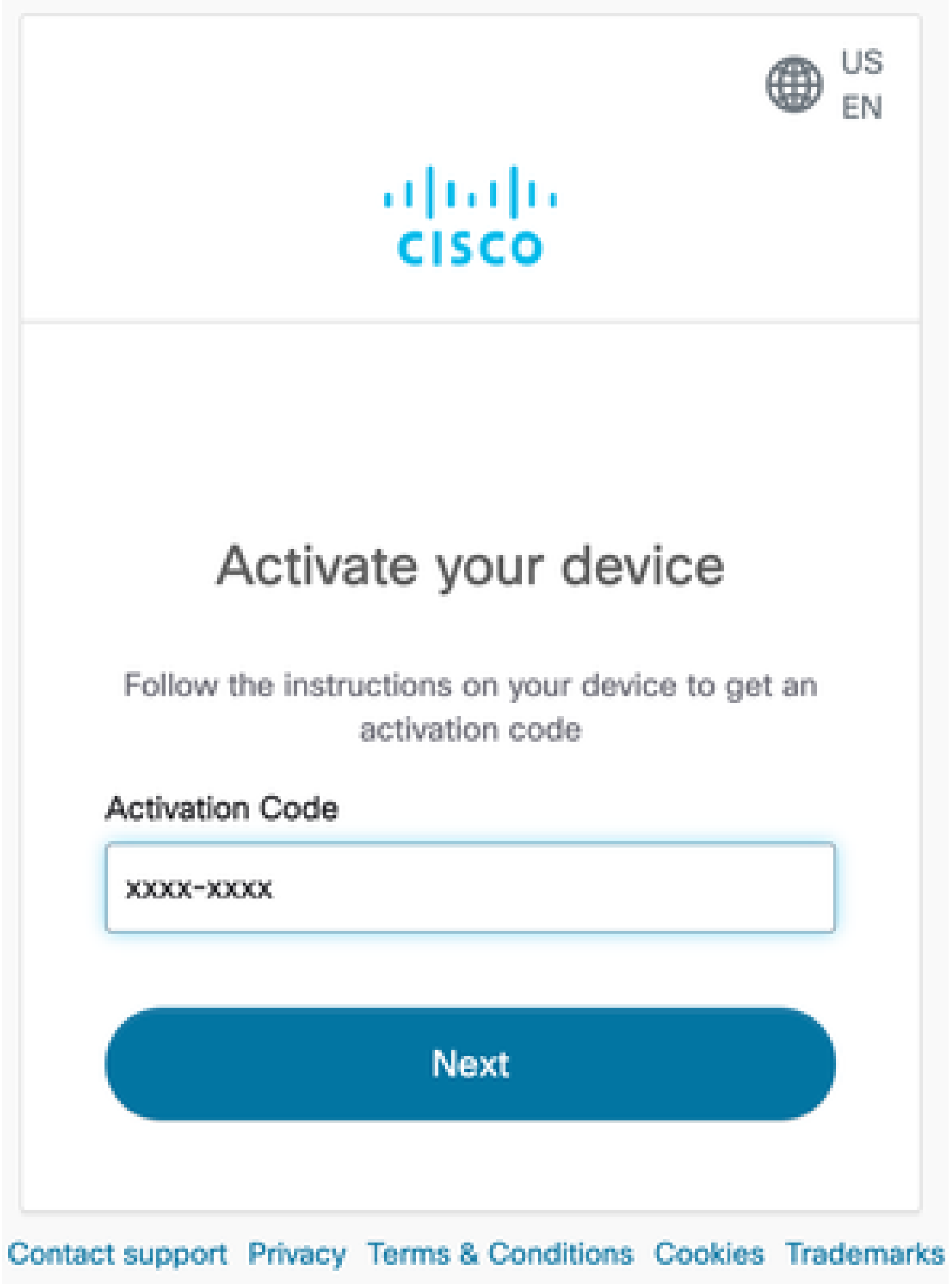
6.在Region下拉列表中，选择注册思科ISE设备的区域。除了美国，欧洲、亚太和日本也支持Cisco pxGrid云。请注意，要与pxGrid云一起使用的应用必须也位于同一区域。

7.单击Register。

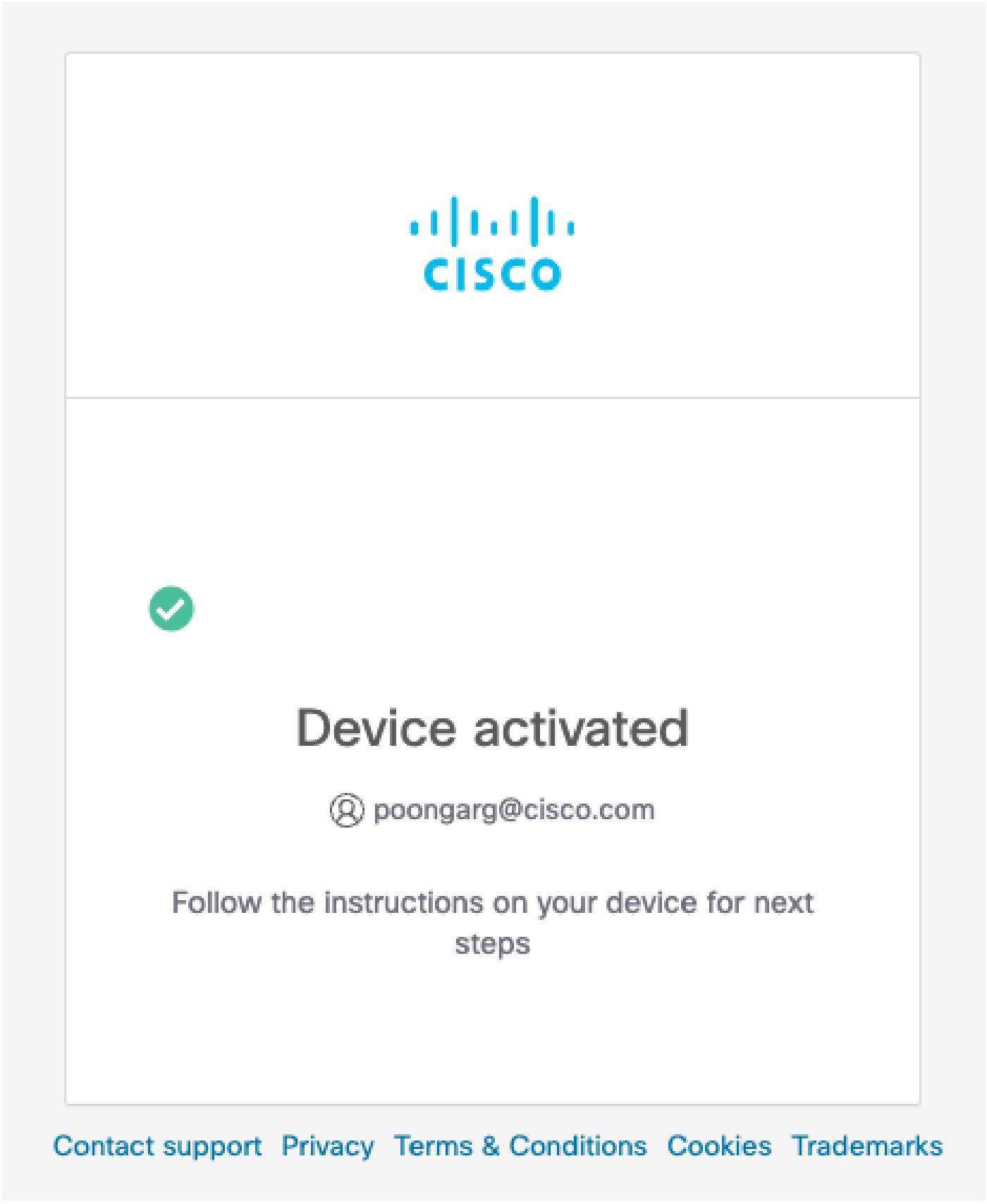


向pxGrid云注册ISE PSN

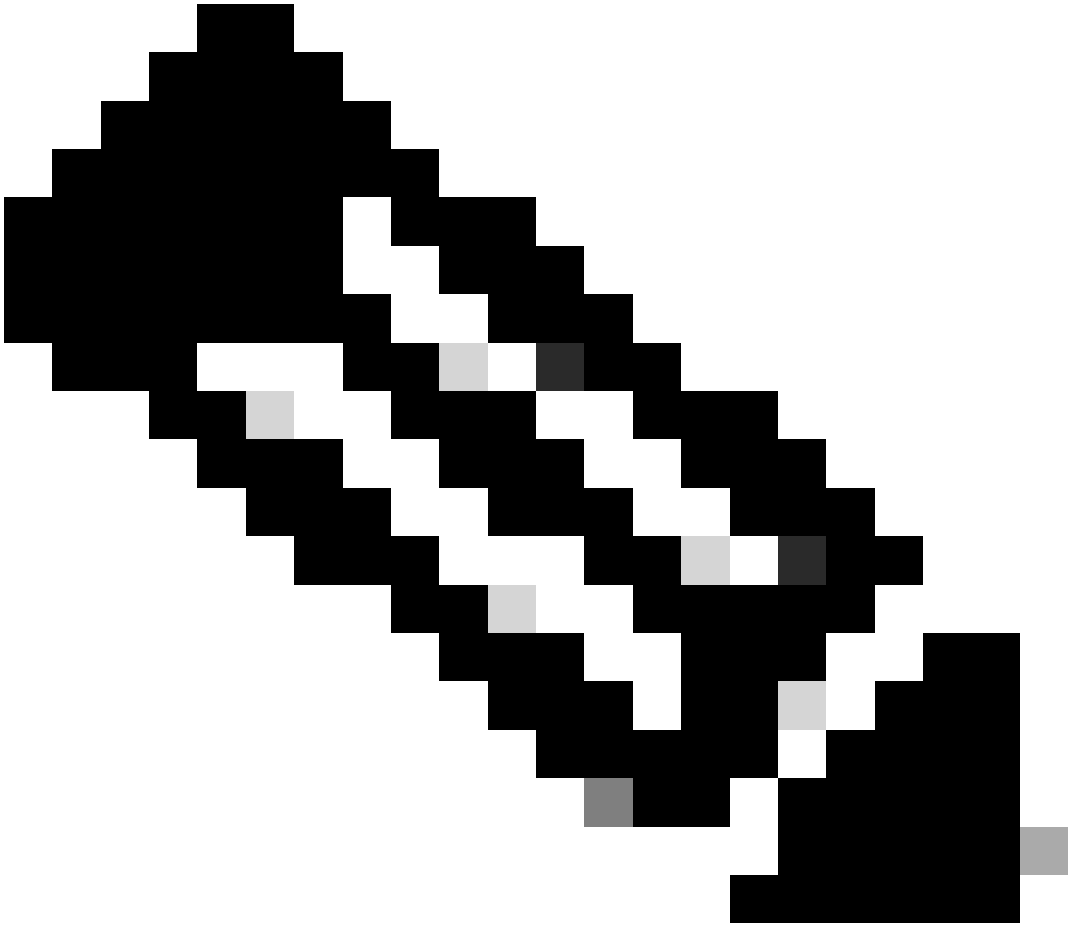
8.在激活设备弹出页中，将自动填写设备的激活代码。单击 Next。


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

激活设备


Device activated
poongarg@cisco.com
Follow the instructions on your device for next steps
Contact support
Privacy
Terms & Conditions
Cookies
Trademarks

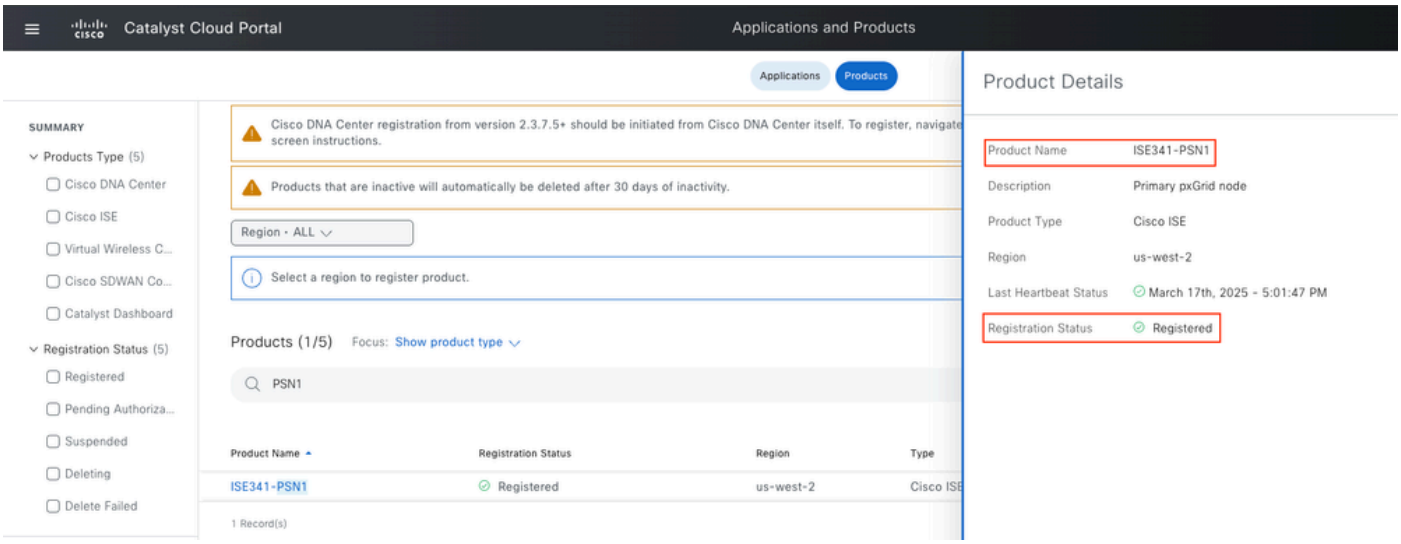
设备已激活



注意：当您在第二个节点上启用“pxGrid云”角色时，ISE不需要所有这些详细信息，因为ISE与pxGrid云的注册处于部署级别。

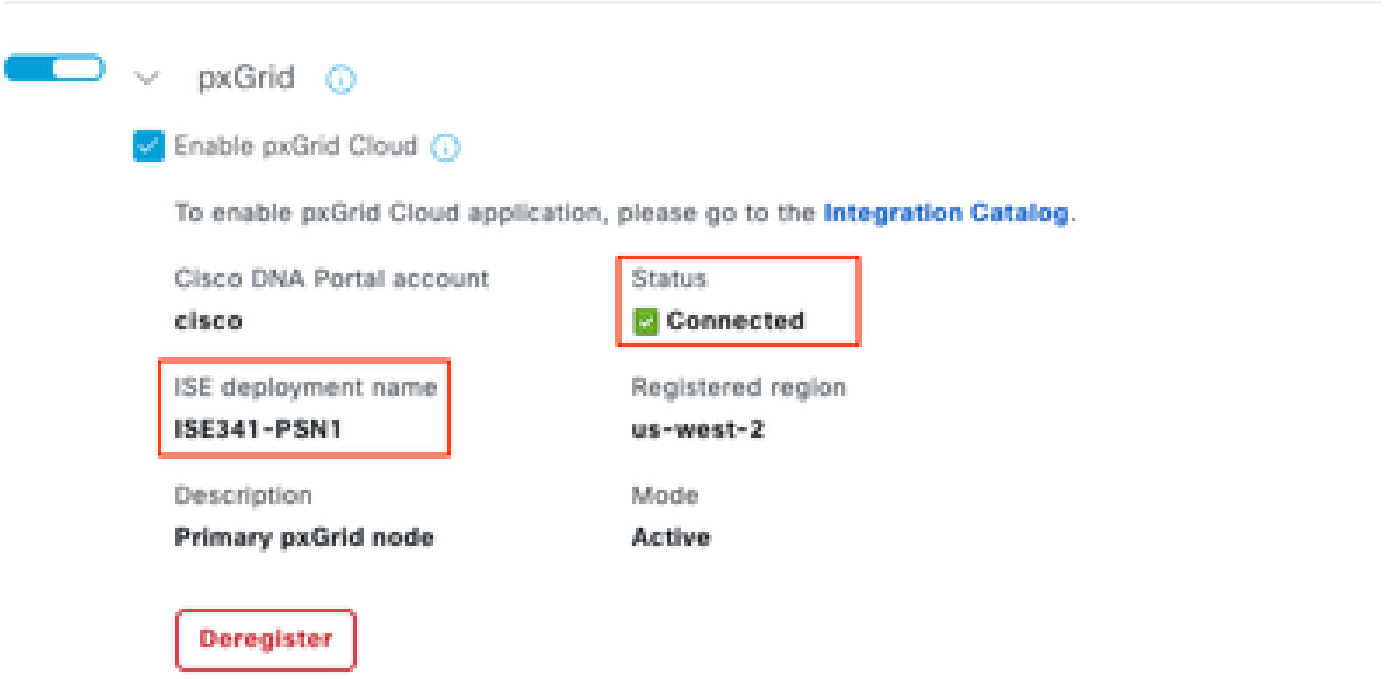
9.使用登录凭证登录Cisco Catalyst云门户帐户。如果您没有登录凭证，请创建新帐户以完成设备注册。有关详细信息，请参阅在Cisco Catalyst云门户上创建帐户

您的思科ISE设备已激活并注册。



向Catalyst云门户注册的ISE节点

10.您可以在pxGrid部分(Administration > System > Deployment > pxGrid)中找到已注册的思科ISE的详细信息。



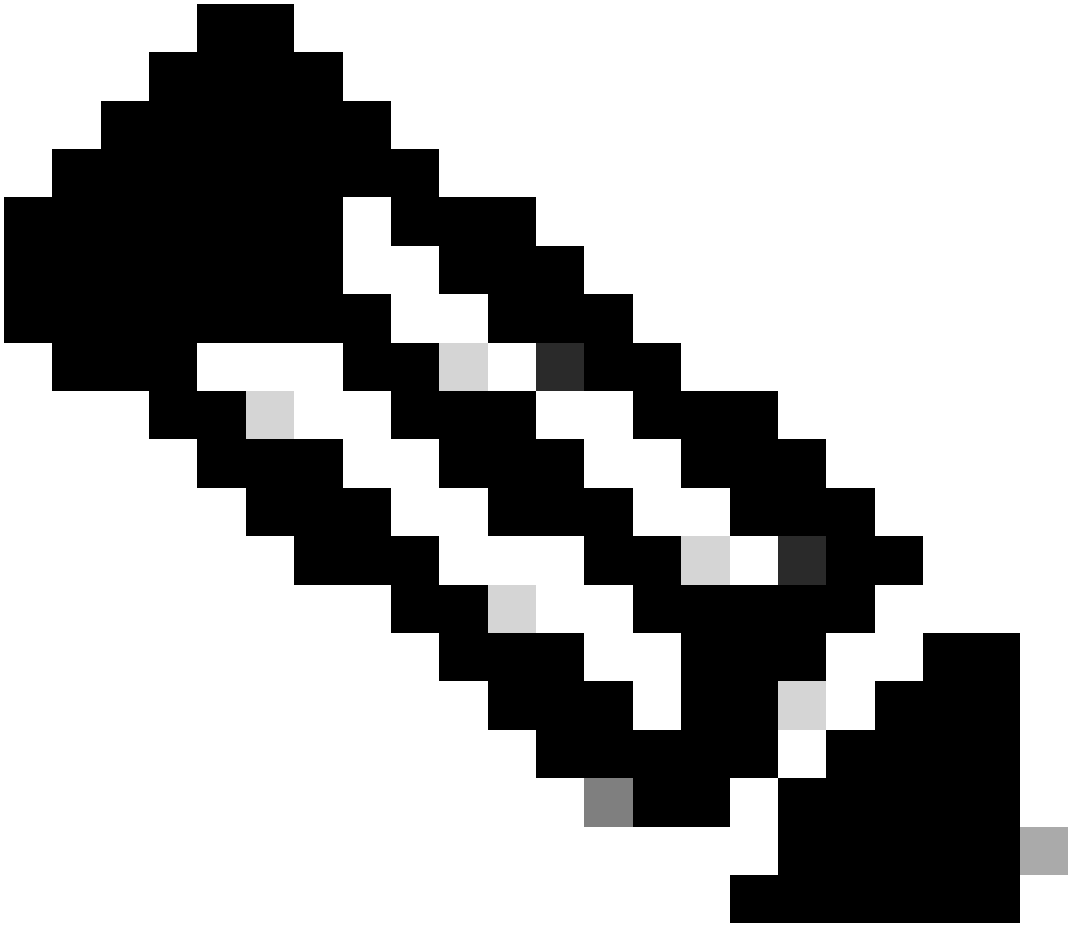
验证向pxGrid云注册的ISE

您可以点击Deregister取消注册您的Cisco ISE设备。注销思科ISE还会自动停用连接的应用。

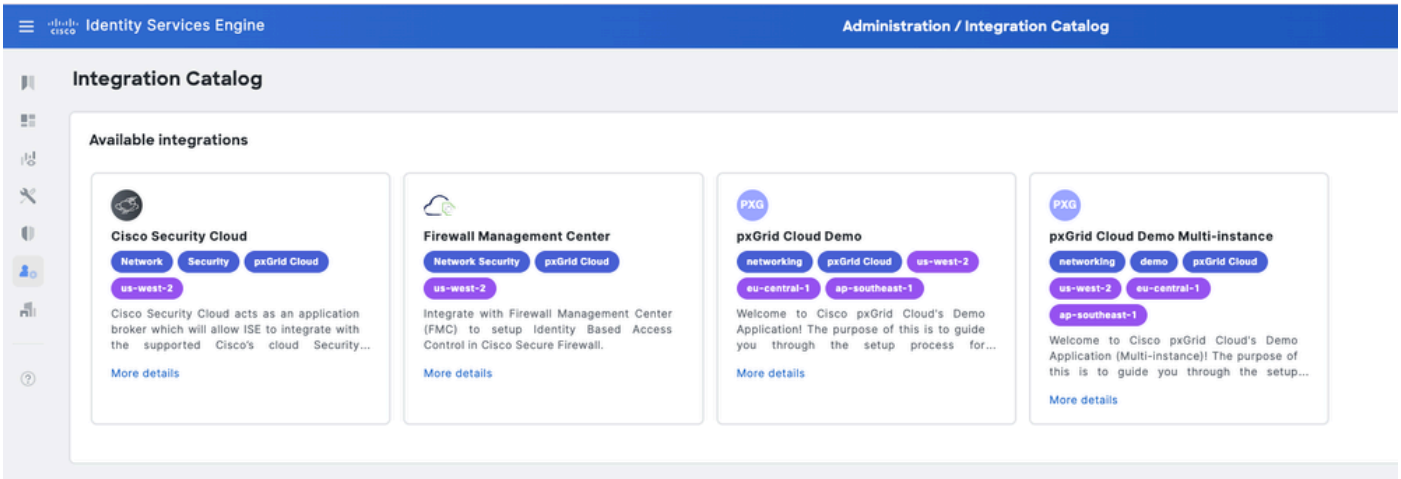
使用集成目录在ISE上激活cdFMC应用

1.在ISE GUI中，选择Administration > Integration Catalog。

2.在Available integrations下，选择Firewall Management center 应用程序。



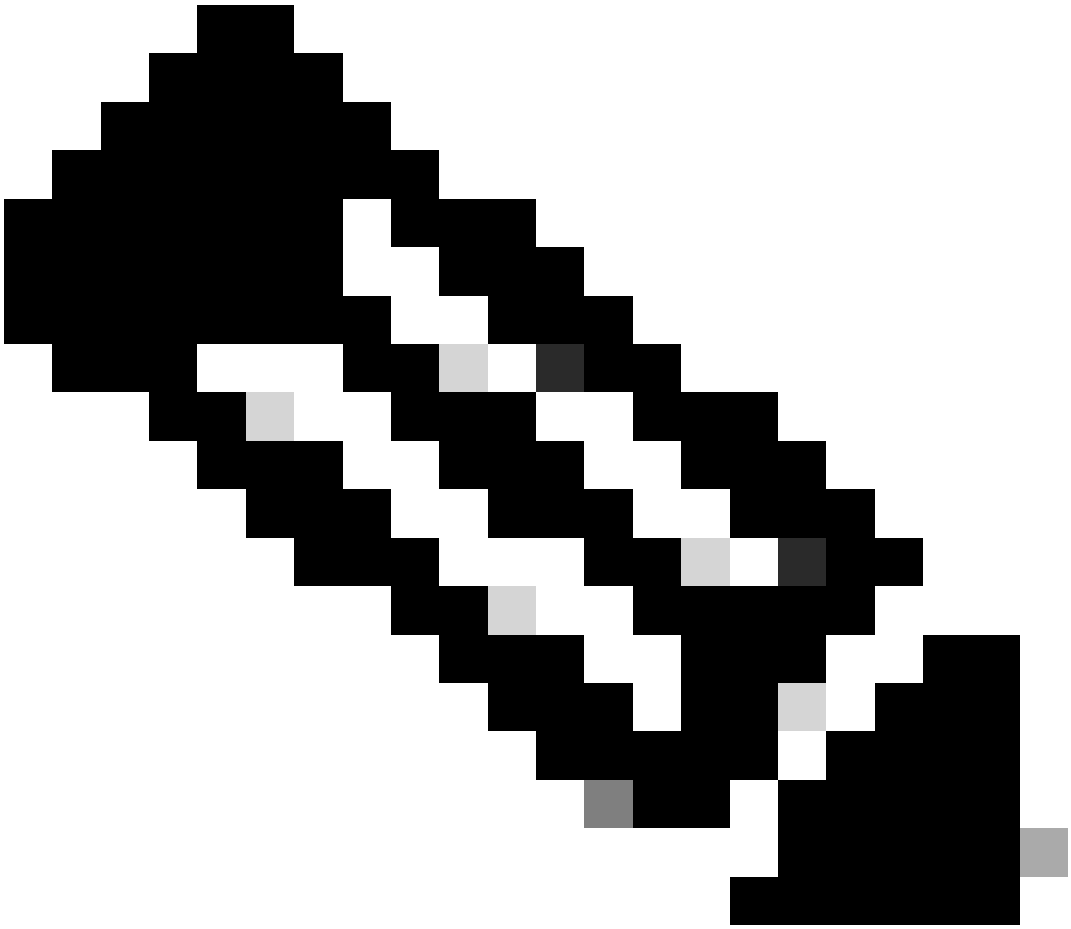
注意：应用程序列表取决于帐户。某些应用程序可能只暴露给特定帐户。



集成目录

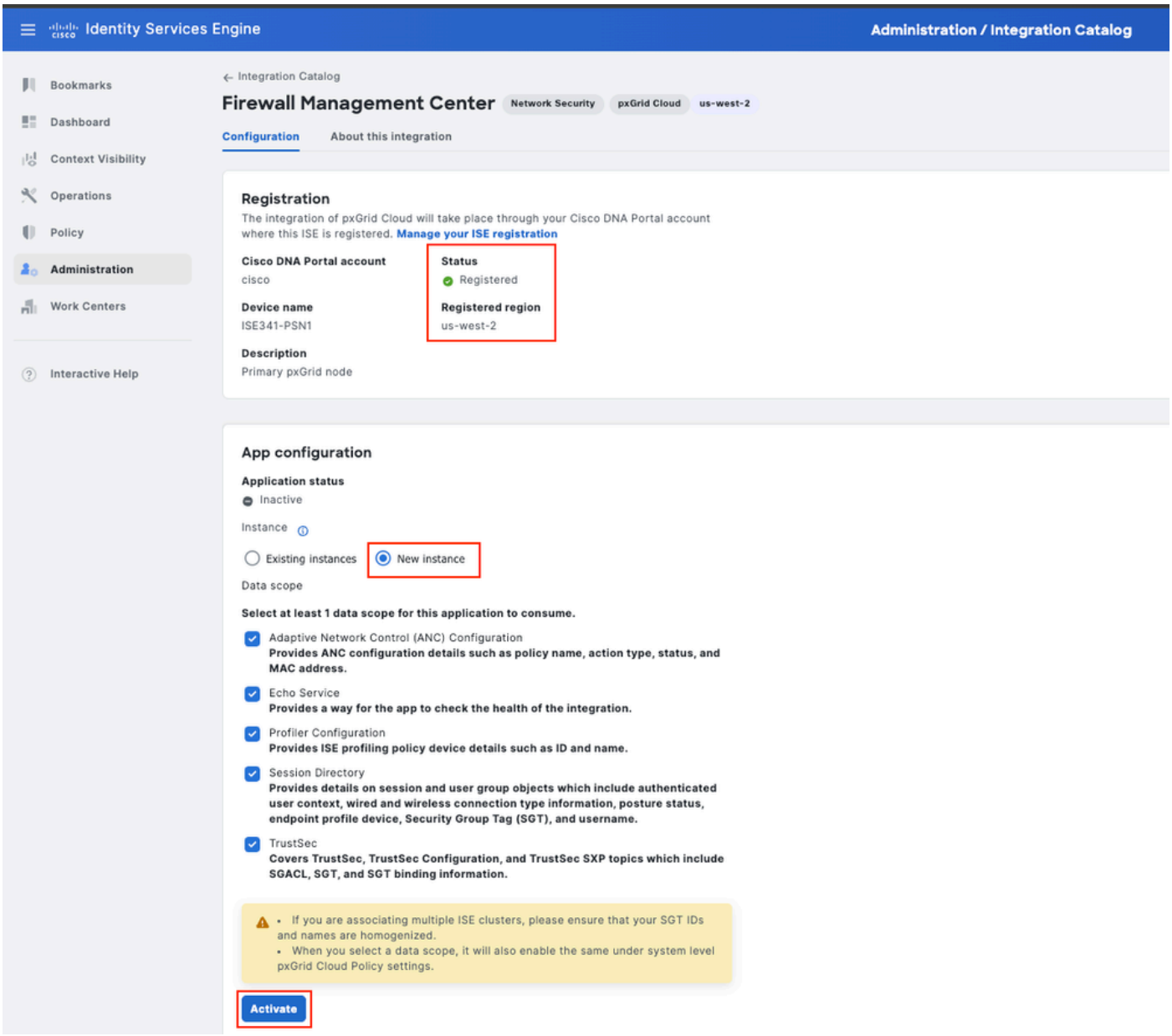
3.在App configuration部分中，选择New instance，然后选择Data scope作为您的应用配置。至少

选择一个数据范围以继续。



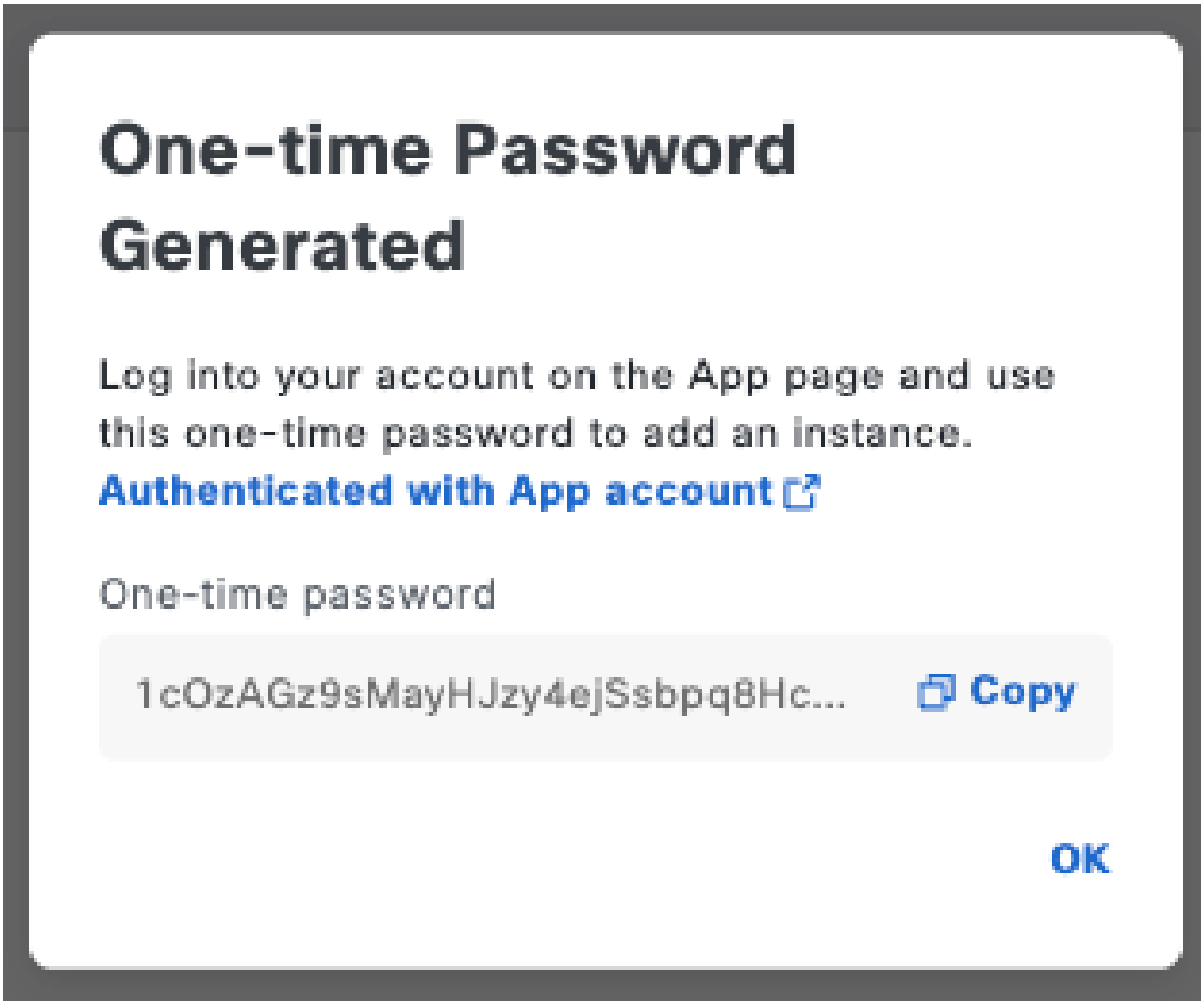
注意：选择数据范围时，它还在系统级别pxGrid云策略设置下启用该范围。

4.单击Activate激活应用。



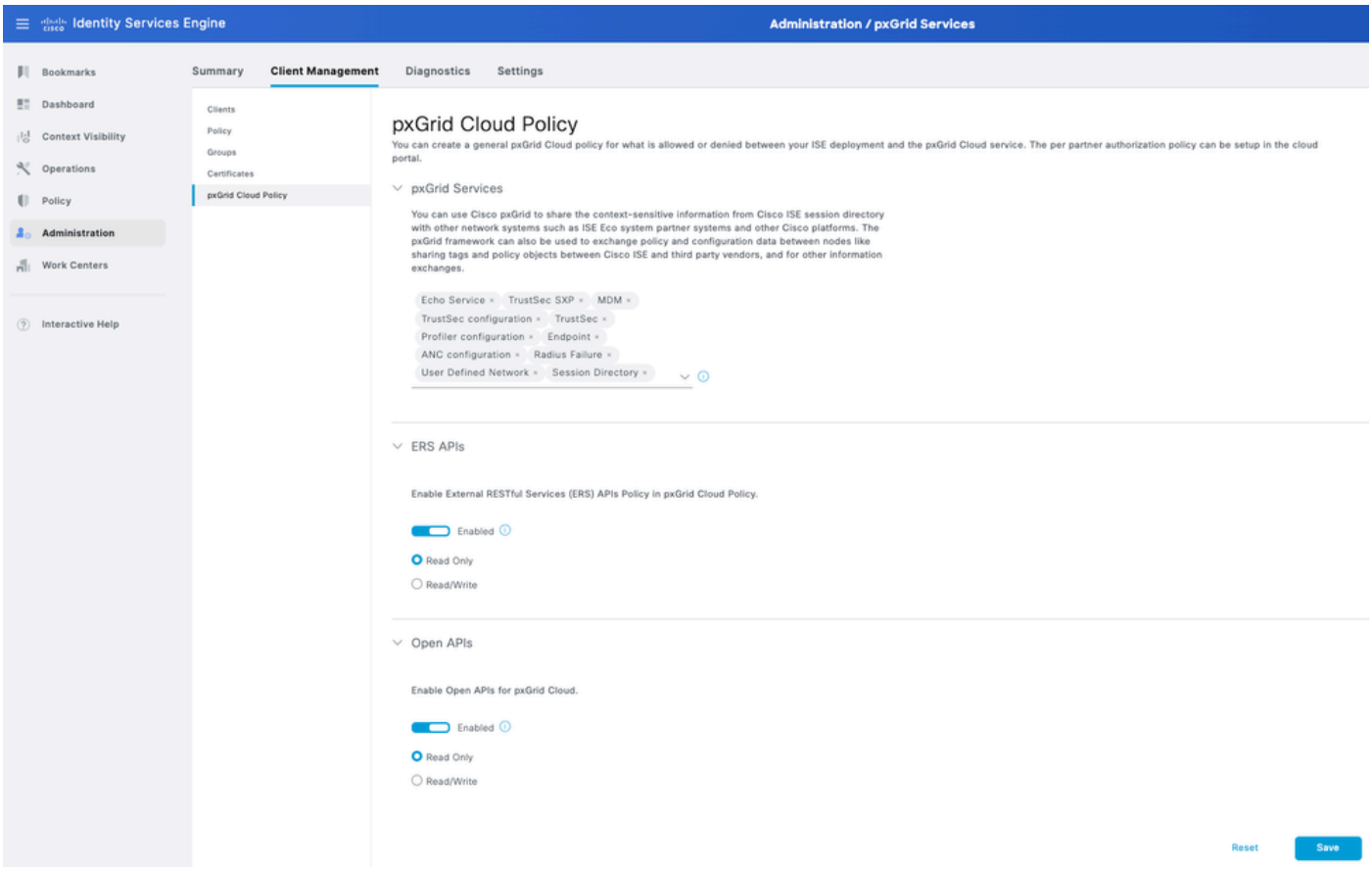
ISE上的FMC应用配置

5.从一次性密码(OTP)弹出窗口中，复制OTP以在创建pxGrid应用实例时将其兑换到cdFMC上

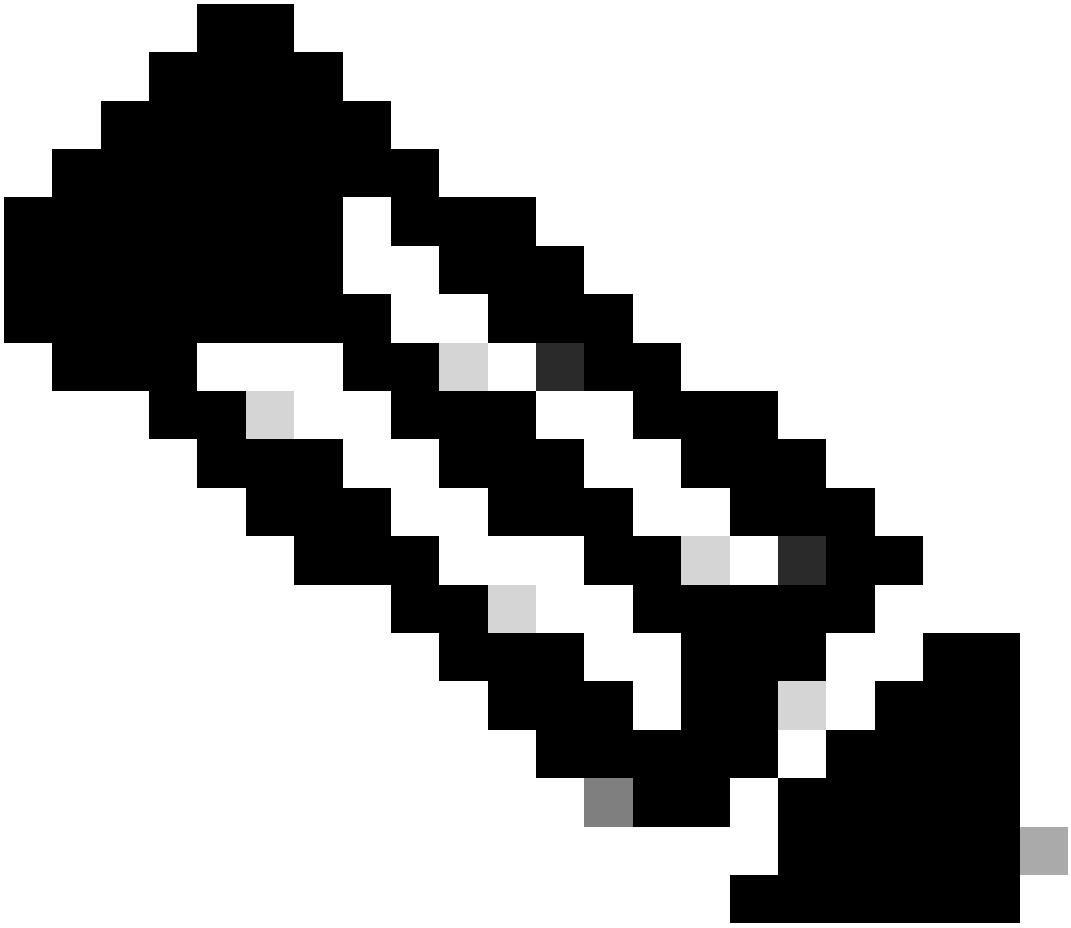


用于cdFMC应用的OTP

6.通过导航到管理> pxgrid服务>客户端管理> pxGrid云策略，配置pxGrid云策略。选择要与Saas应用共享的pxGrid服务，并启用外部RESTful服务(ERS)API和OpenAPI对Cisco pxGrid云应用的只读访问。



配置pxGrid云策略



注意：Echo服务用于运行运行状况检查以确定与ISE的pub-sub和API连接。

默认情况下，Cisco pxGrid云应用被授予对API的只读访问权限（只能执行HTTP GET操作）。 如果您还希望允许POST、PUT和DELETE操作，请在pxGrid Cloud Policy窗口中启用Read/Write选项。

创建pxGrid应用程序(cdFMC)实例

1.以具有超级管理员角色的用户身份登录安全云控制(SCC)门户。

CONNECTING TO SECURITY CLOUD CONTROL (APJC)

Security Cloud Sign On

Email

Continue

Don't have an account? Sign up now

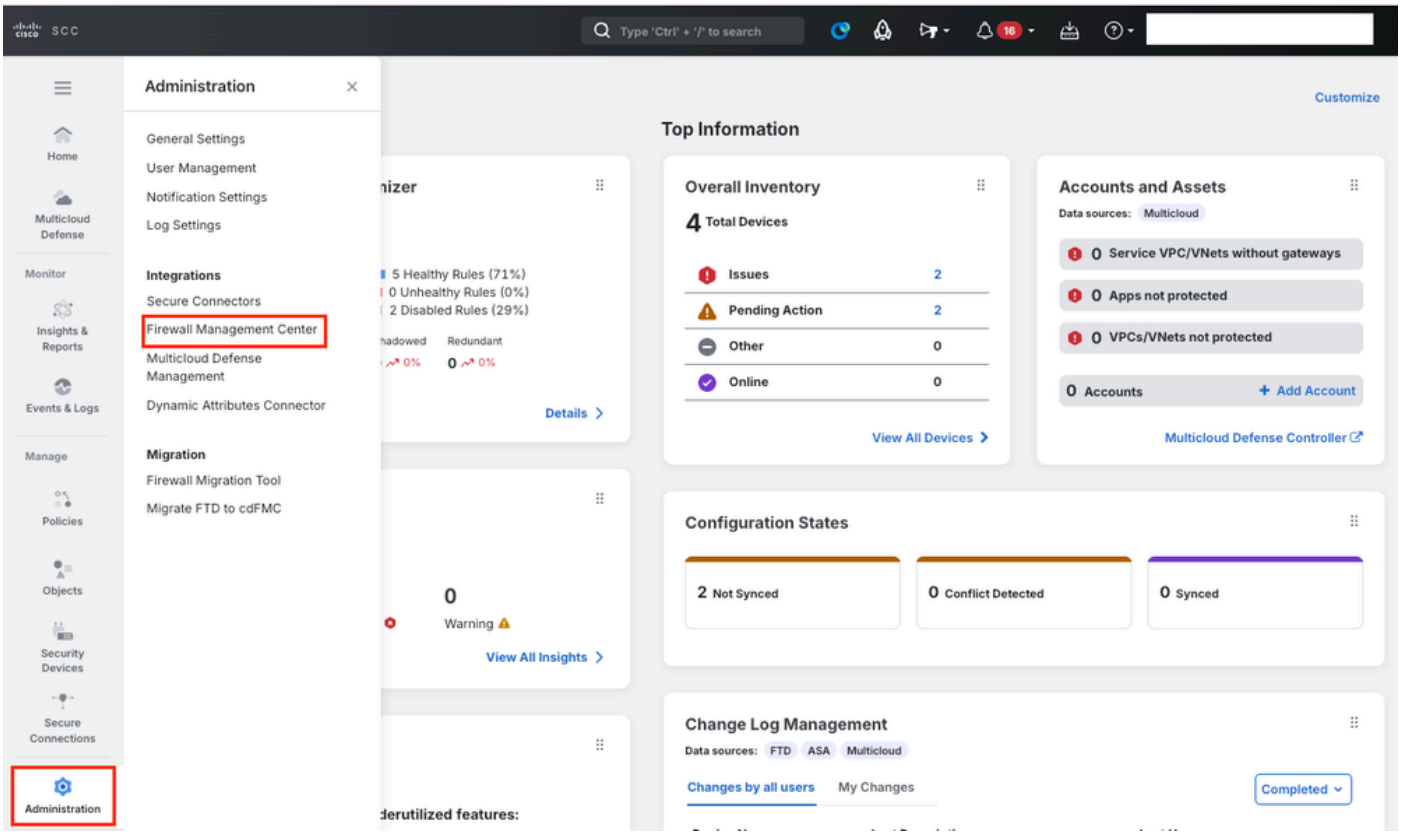
Or

Other login options

System status Policy statement

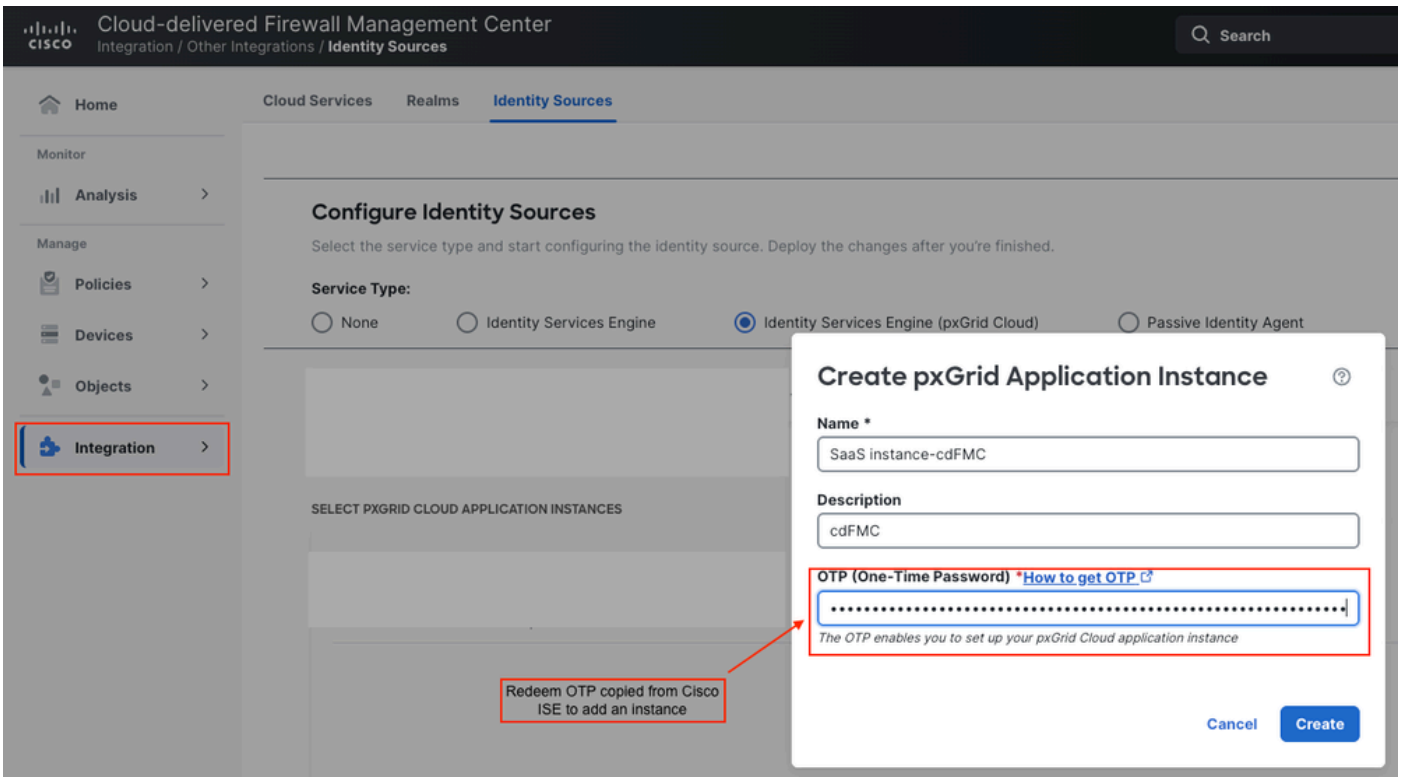
SCC登录页

2.从“安全云控制”菜单中，单击管理> 集成 > 防火墙管理中心，然后选择您的cdFMC实例，并在右侧窗格选项中选择System > Configuration。



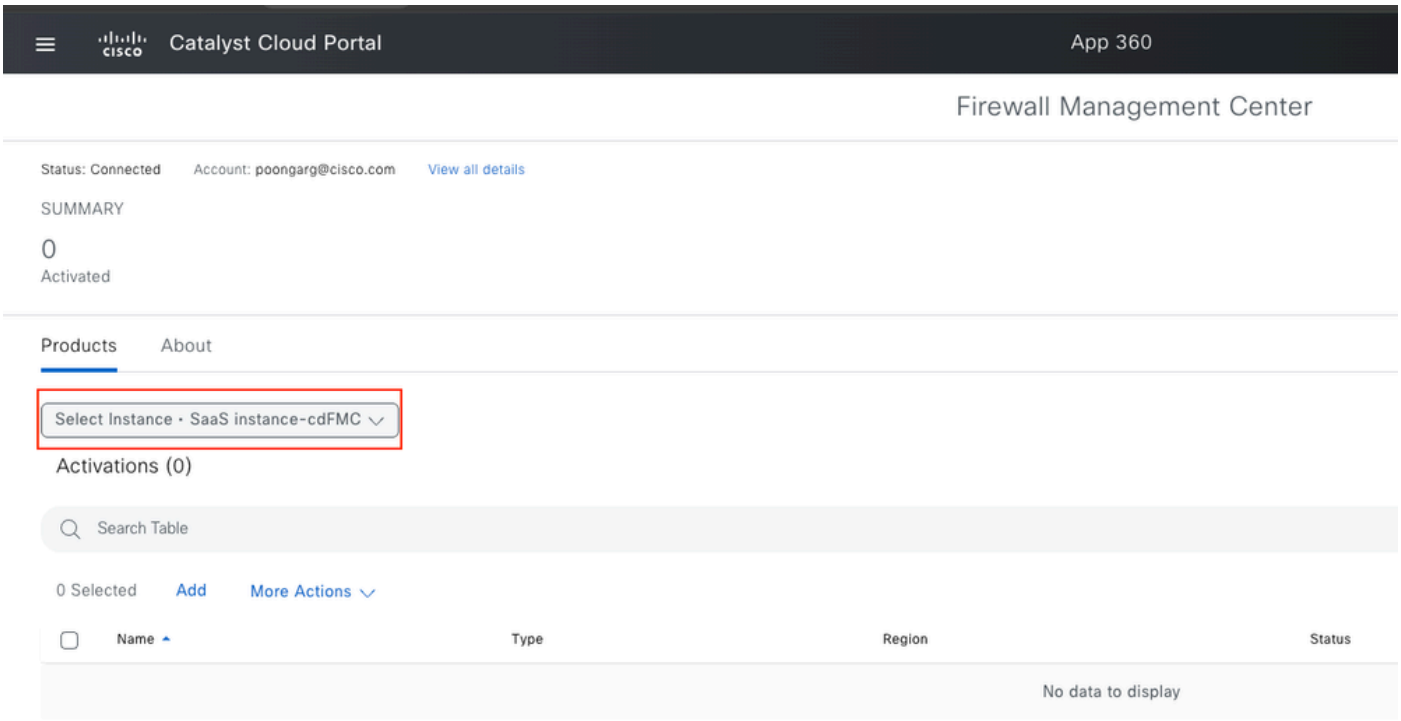
导航到防火墙管理中心

3.在“配置”页上，选择集成>其他集成>身份源>选择服务类型身份服务引擎（pxGrid云）。 点击创建pxGrid应用实例并兑换从思科ISE复制的OTP以添加实例。



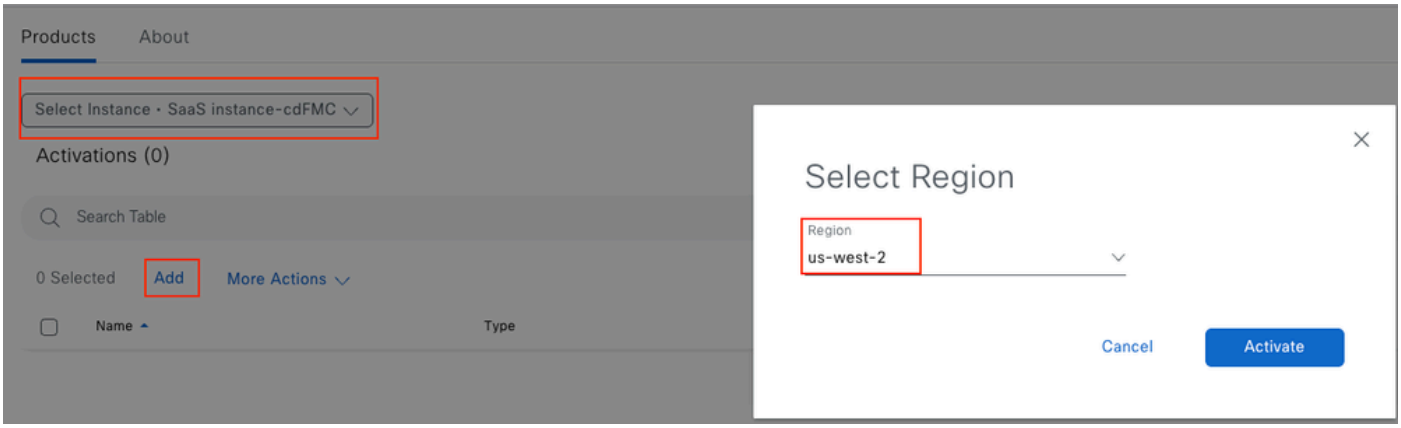
创建cdFMC应用实例

4.在Cisco Catalyst云门户上验证它，位于Applications and Products > Firewall Management Center > Manage > Products > Select Instance下拉菜单。



验证Catalyst云门户上的cdFMC

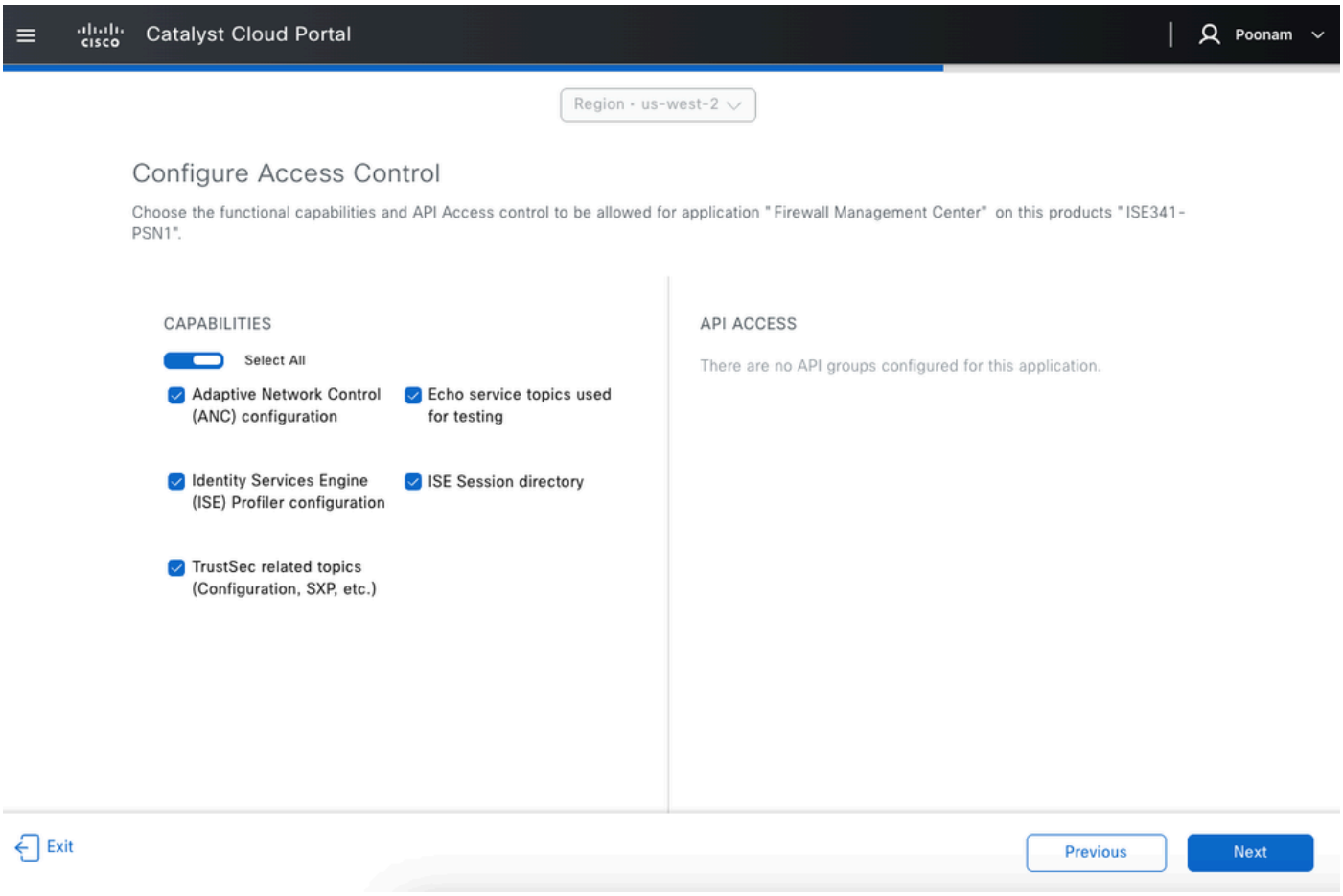
5.选择新创建的cdFMC应用程序，然后单击Add。选择Region，然后单击Activate。



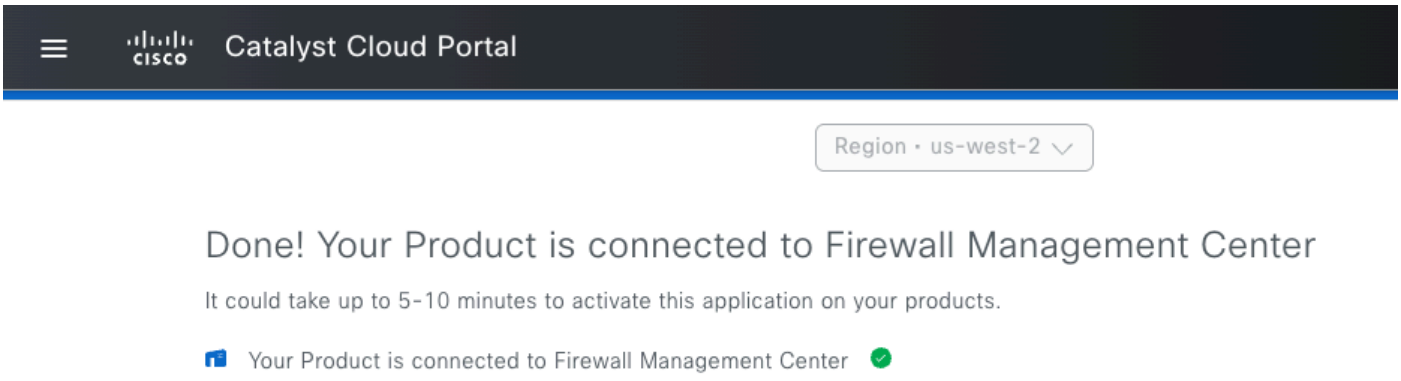
选择区域

5.选择您的应用实例，然后单击下一步。选择您的产品（ISE pxGrid节点），然后点击下一步。

6.配置访问控制：选择所选ISE产品上cdFMC允许的功能功能。单击 Next。系统将显示配置摘要。验证并单击Activate。

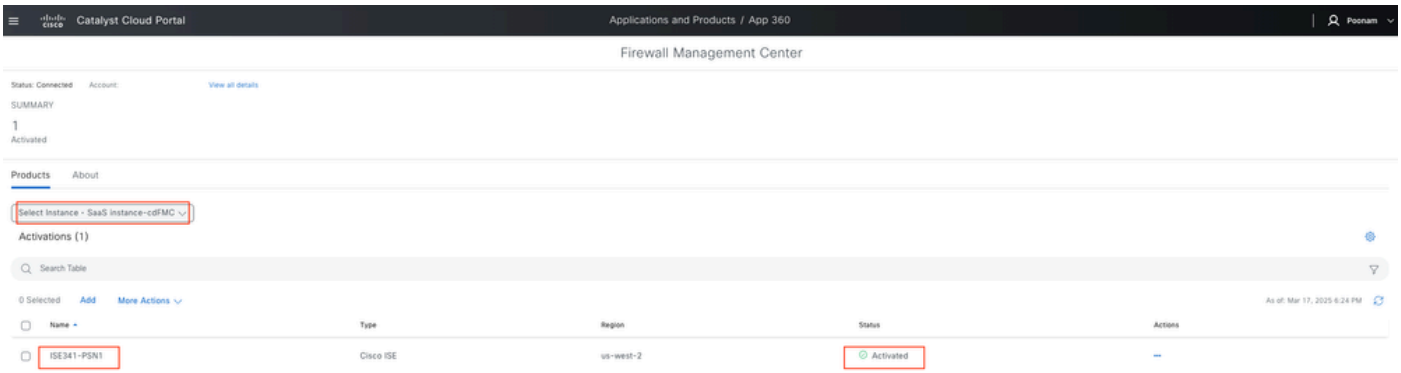


为cdFMC配置访问控制



产品ISE连接到cfFMC

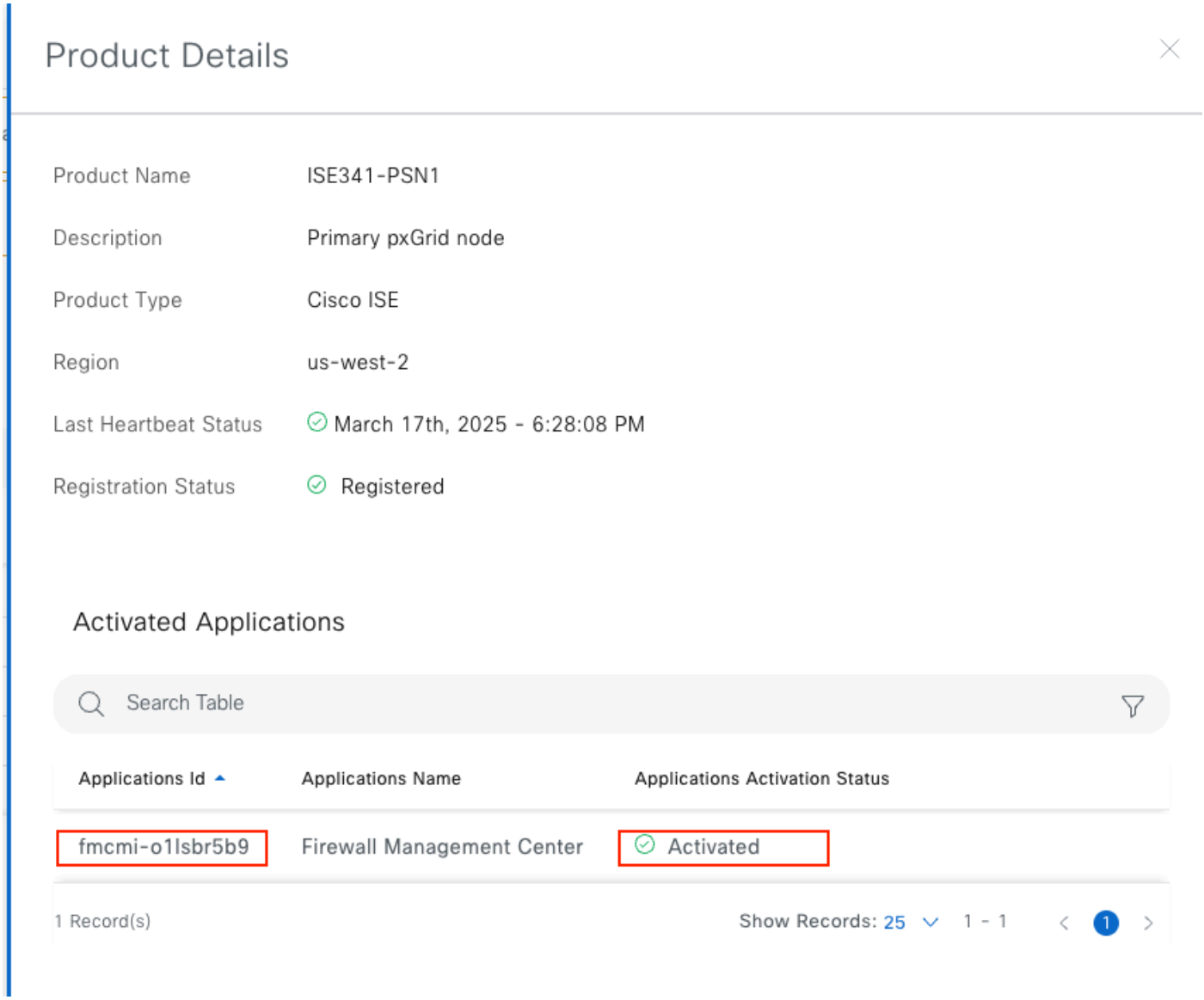
8.在Cisco Catalyst云门户上验证它，位于Applications and Products > Firewall Management Center > Manage > Products > Select Instance下拉菜单。



验证应用是否已激活

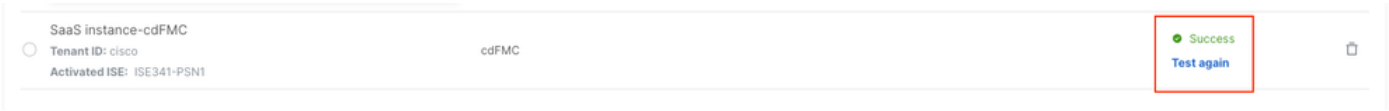
验证

1. 在Catalyst云门户上，导航至应用和产品。选择您的ISE产品名称并检查产品详细信息。验证在Activated Application（激活的应用）下是否看到cdFMC。



在Catalyst云控制门户上验证

2. 在安全云控制上，测试配置的cdFMC应用实例。测试显示“成功”



在安全云控制门户上验证

3.使用show application status ise命令登录到活动pxGrid节点并验证Hermes（pxGrid云代理）是否处于运行状态。此代理在备用pxGrid节点上处于禁用状态。

```
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
```

验证Hermes（pxGrid云代理）状态

检查两个pxGrid节点上的pxcloud.log以确认Active和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)

此外，检查仅在活动pxGrid节点上打开的端口8913:

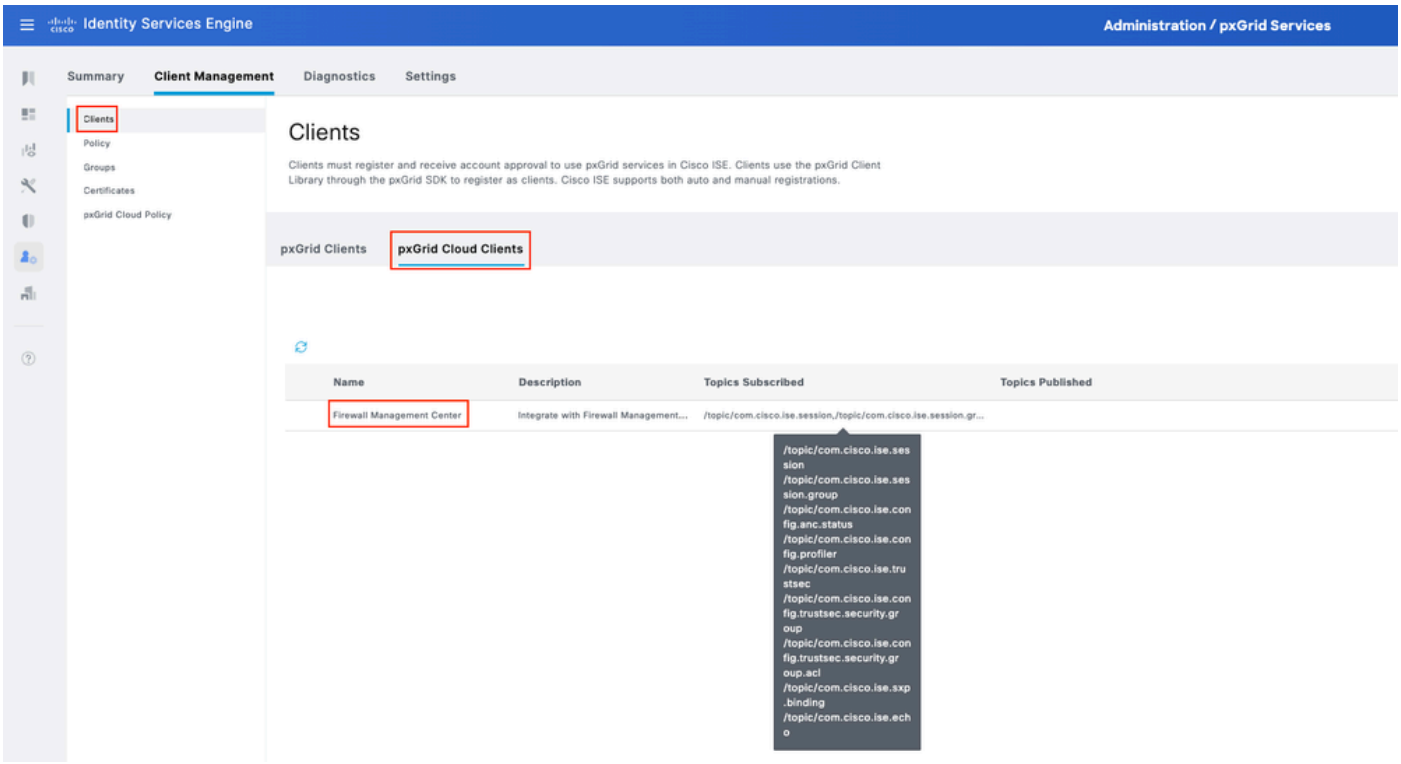
<#root>

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

127.0.0.1:8913

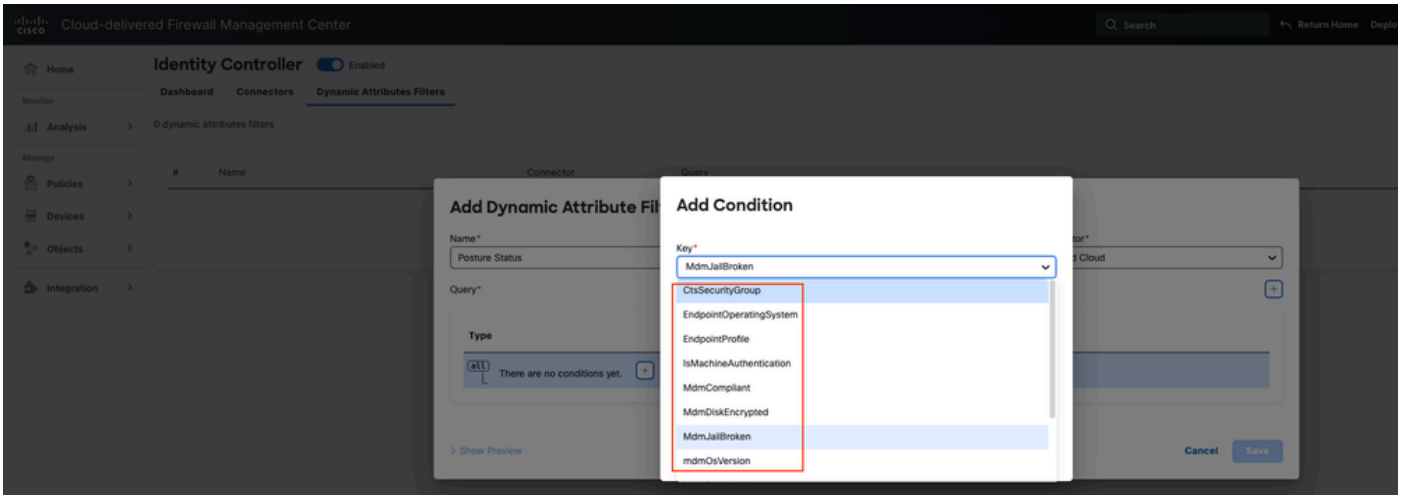
```
ise341-psn1/admin#
```

4.导航到管理> pxGrid服务>客户端管理>客户端> pxGrid云客户端，验证pxGrid云客户端。另请检查订阅的主题。



ise上的pxGrid云客户端

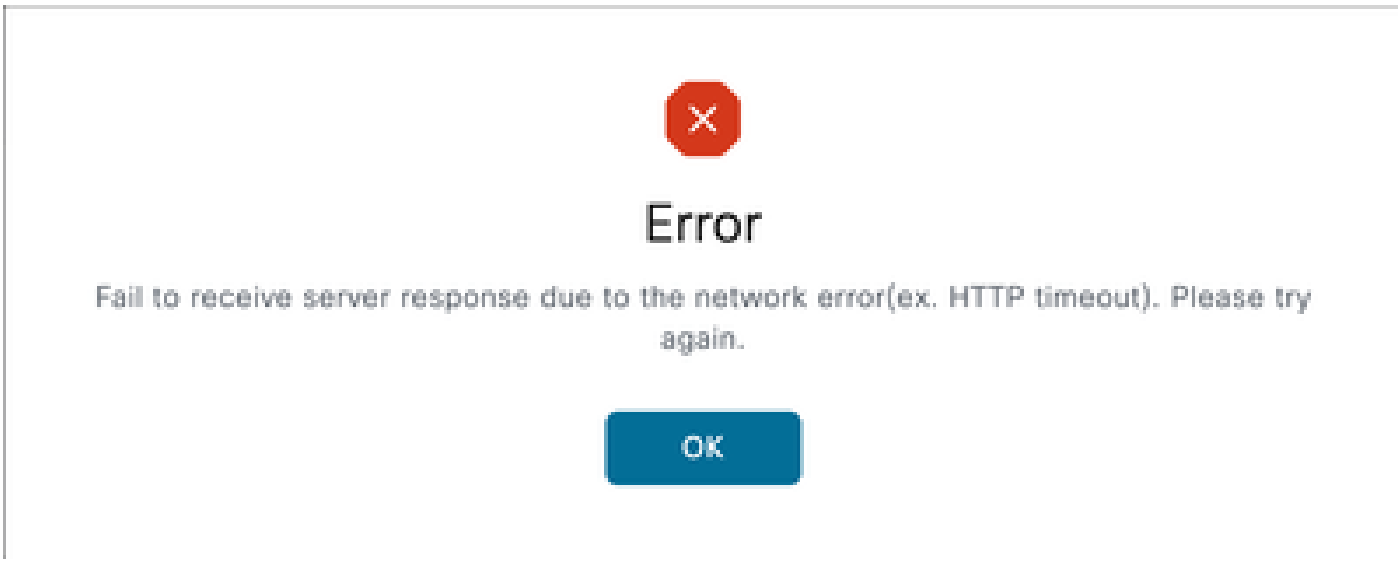
5.验证订阅的主题是否获取在cdFMC上。在安全云控制门户上，单击策略>威胁防御>集成>其他集成>身份源。单击身份服务引擎（pxGrid云）。单击配置过滤器。在该页上，单击动态属性过滤器选项卡。创建动态属性过滤器。



从ISE获取属性

故障排除

1.在ISE注册期间失败：



缺少代理配置

检查Internet连接和可能的代理配置错误。

2. 启用pxGrid云服务并配置名称和区域参数后，pxGrid状态在ISE编辑节点页面上显示Not connected。

在要启用pxGrid云服务的节点上检查hermes.log:

<#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**

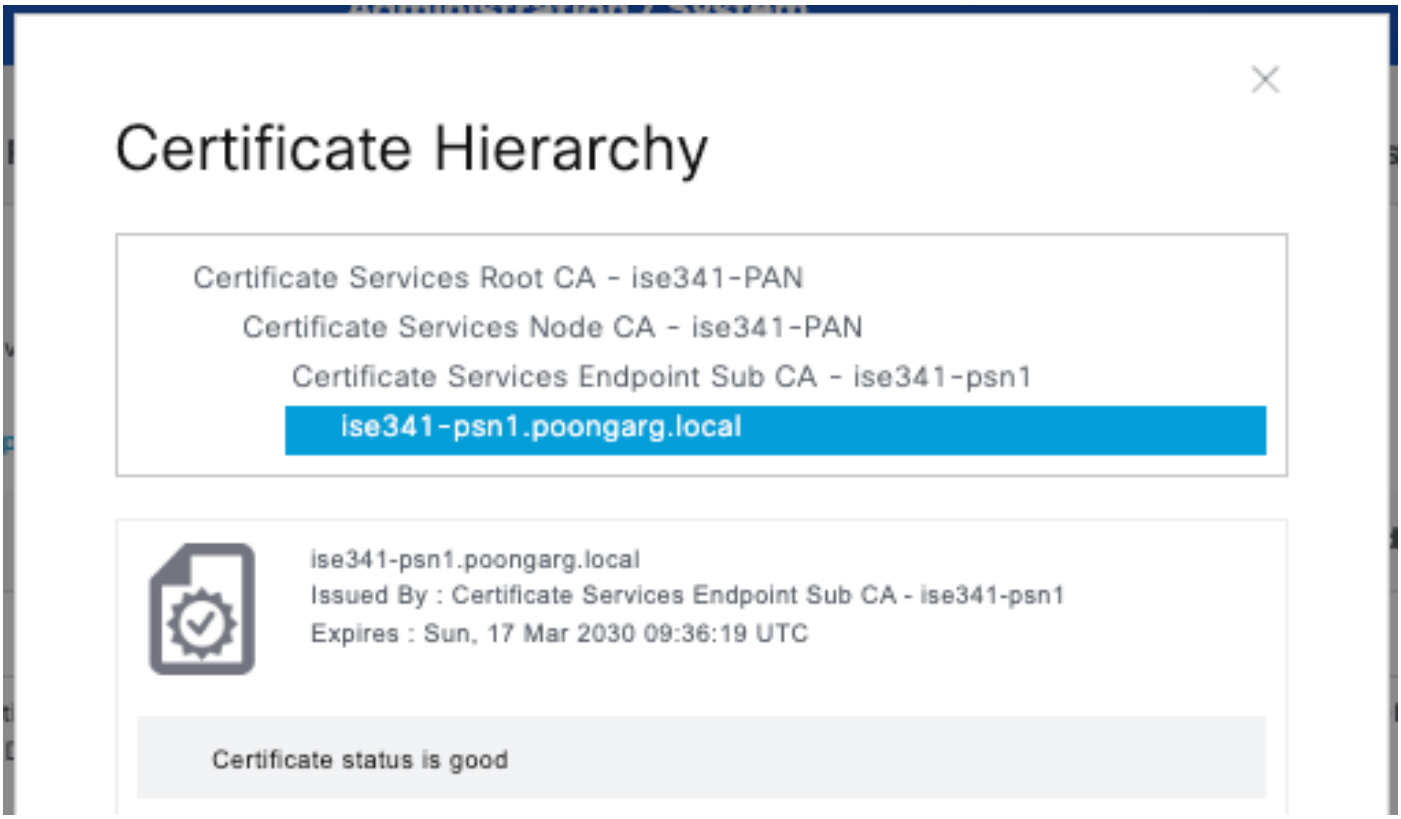
2025-03-17T09:19:35.307Z | ERROR | hermes/main.go:166 | Failed to open pxGrid WebSocket connection: Fai
2025-03-17T09:19:35.307Z | INFO | hermes/config.go:279 | Stopping monitoring of configuration file: /op
2025-03-17T09:19:35.307Z | INFO | hermes/connectionstatus.go:81 | Resetting connection status 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服务器侦听端口8913。日志清楚地显示Hermes REST服务器正在尝试启动，但由于证书验证失败，未能建立pxGrid WebSocket连接。

解决方案：验证pxGrid证书是否有效，证书链是否未中断。查看证书并验证证书状态是否正常。在

这种情况下，颁发给此节点的pxGrid证书中的ISE主机名不正确。



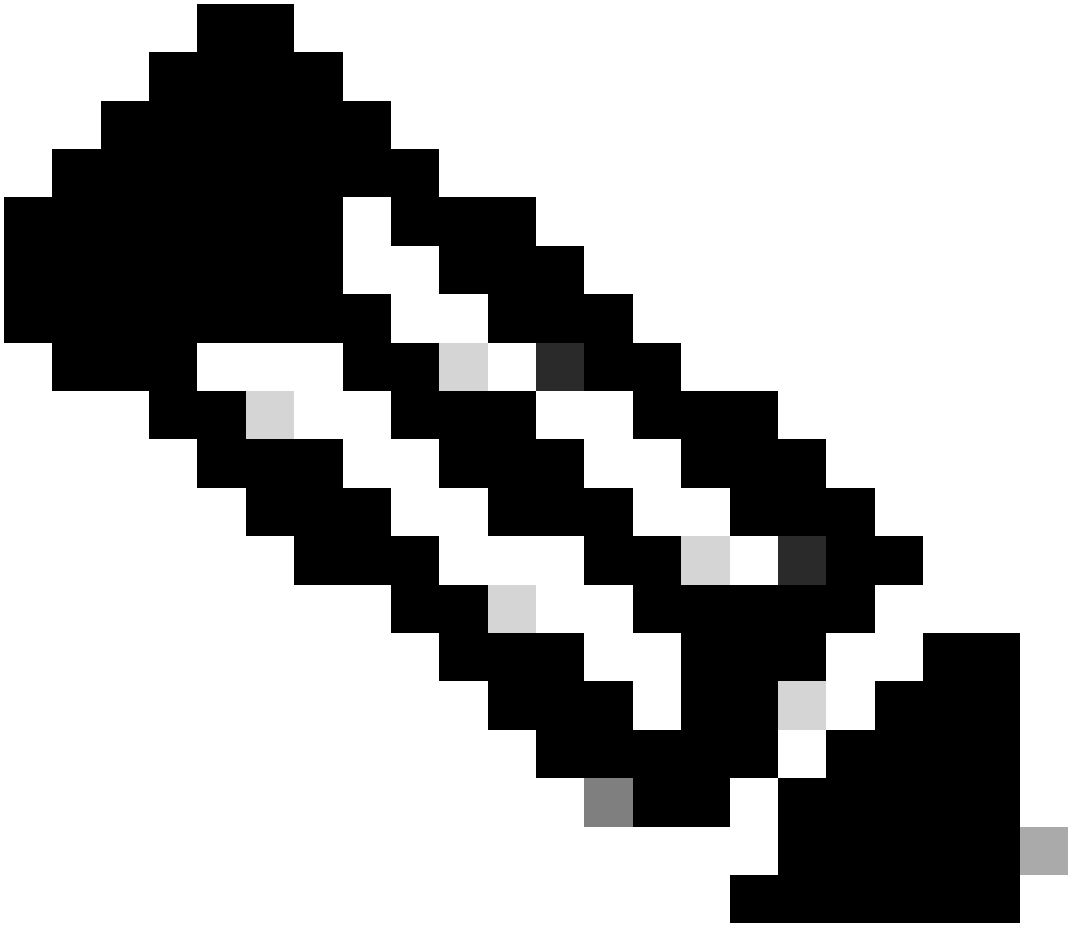
有效的pxGrid证书

3.cdFMC应用激活在Catalyst云门户上失败。

解决方案：确保在ISE上，在pxGrid云策略下，启用外部RESTful服务(ERS)API和OpenAPI只读访问。

与pxGrid云功能相关的日志：

调试组件	日志文件名称	描述
pxGrid云	pxcloud.log、hermes.log	pxcloud.log:它记录pxGrid云服务配置更改、pxGrid云服务连接状态和高可用性状态 hermes.log:记录pxGrid主题订阅状态、来自pxGrid云的ERS Rest请求、ISE上的配置更改。
pxGrid云OpenAPI	pxcloud.log、hermes.log	
遥测	sch.log	用户使用集成目录时生成日志。它包括初始日志，带有用于连接到pxGrid云的令牌。



注意：无论您在哪个节点上启用pxGrid云角色，您都需要检查活动PAN节点上的日志。设备注册后，Hermes日志位于启用该设备的特定节点上。

Hermes.log仅支持Debug、Info、Warn和Error日志级别。因此，如果选择Trace，日志级别将设置为Debug for hermes.log。如果选择Fatal，则hermes.log的日志级别设置为Error。

ISE注册/注册和应用激活流程

在注册设备之前，ISE使用设备令牌从云获取区域列表和应用列表。此令牌由ISE的“遥测”组件提供。检查PAN节点上的sch.log:

```
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节点），一旦启用pxGrid云服务，Hermes（pxGrid云代理）将激活，ISE获取区域信息并通过遥测组件接收令牌。

```
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
```

激活链接已收到，并且自动注册和注册。

```
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节点承担了ACTIVE角色，但是，此处我们将pxGridConnectionStatus观察为NOT_CONNECTED，在在此pxGrid节点上添加正确的pxGrid证书（具有完整的根CA链）后，此状态得到修复

```
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
```

现在检查ACTIVE pxGrid节点上的Hermes.log以查找pubsub事件：

```
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
```

已验证Catalyst云门户的根CA链。

```
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
```

特定主题订用请求创建一次，FMC应用在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
```

限制

1.用户无法在超过2个节点上启用pxGrid云角色。

2.支持从Catalyst云门户取消注册到cdFMC，但不支持反向。

参考

使用pxGrid云身份源的用户控制

思科pxGrid云

思科pxGrid云解决方案指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。