



Identity Source: pxGrid Cloud Identity (ISE 3.3 and Earlier)

The following topics discuss how to configure and use the pxGrid Cloud Identity Source with Cisco ISE version 3.3 and earlier.

- [About the pxGrid Cloud identity source, on page 1](#)
- [How to configure a pxGrid Cloud identity source, on page 3](#)
- [Enable the pxGrid Cloud service in Cisco ISE, on page 6](#)
- [Register Cisco ISE with the Catalyst Cloud Portal, on page 7](#)
- [Register the pxGrid Cloud connection with Cisco ISE, on page 9](#)
- [Create a pxGrid Cloud identity source, on page 10](#)
- [Create dynamic attributes filters, on page 23](#)
- [Create access control rules or DNS rules using dynamic attributes filters, on page 25](#)
- [Troubleshoot the pxGrid Cloud identity source, on page 26](#)
- [Deactivate and delete the pxGrid Cloud identity source, on page 27](#)

About the pxGrid Cloud identity source

The Cisco Identity Services Engine (Cisco ISE) pxGrid Cloud identity source enables you to use subscription and user data from a server or cluster in Secure Firewall Management Center access control rules. Also, the identity source uses constantly changing dynamic objects from in access control policies in the Secure Firewall Management Center.

The pxGrid Cloud identity source also uses:

- The Cisco Platform Exchange Grid (pxGrid), which enables multivendor, cross-platform network system collaboration in things like security monitoring and detection systems, network policy platforms, asset and configuration management, identity, and access management. pxGrid Cloud is the cloud-based interface to Cisco ISE.

More information about pxGrid can be found in resources such as [What is PxGrid?](#) on devnet.

- The Cisco Digital Network Architecture (Cisco DNA) delivers automation, security, predictive monitoring, and a policy-driven approach. It provides end-to-end network visibility and uses network insights to optimize network performance and deliver the best user and application experience.

To use the pxGrid Cloud identity source with the Secure Firewall Management Center, you must [Create a Cisco Account](#).

Limitations of the pxGrid Cloud identity source

- [What is pxGrid? on devnet](#)
- [Cisco Platform Exchange Grid Cloud on devnet](#)

Prerequisites

- *ISE-PIC is not supported*
- Cisco ISE 3.1 patch 3 and all later patches and versions

For information about Cisco ISE versions and query sizes, see [Query limitation](#) in the pxGrid Cloud SDK on GitHub.

Related Topics

- [How to configure a pxGrid Cloud identity source \(Cisco ISE 3.4 or later\)](#)
- [How to configure a pxGrid Cloud identity source \(Cisco ISE 3.3 or earlier\), on page 3](#)

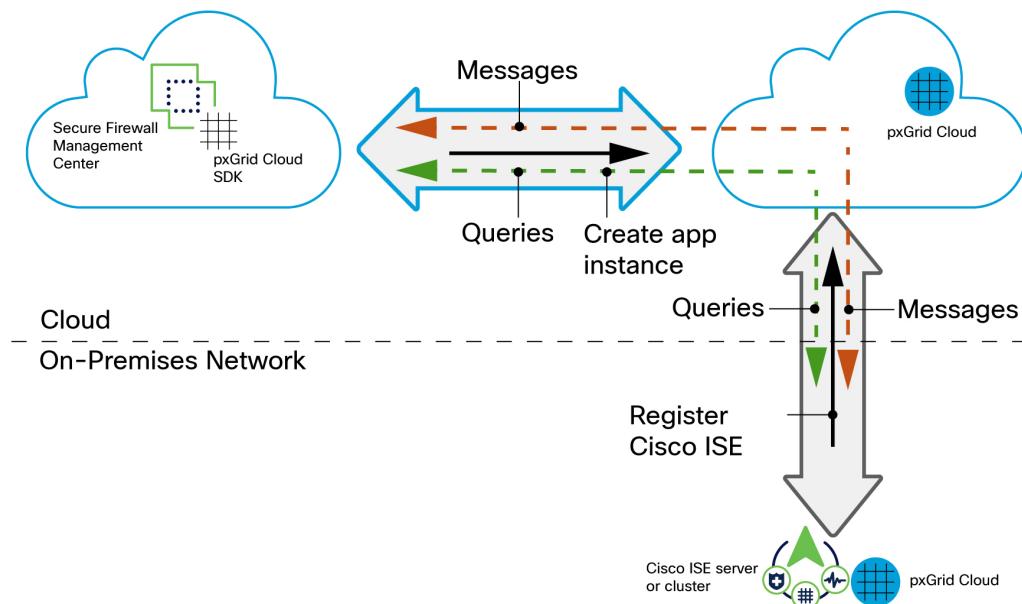
Limitations of the pxGrid Cloud identity source

Before you set up the pxGrid Cloud identity source, note the following:

- pxGrid Cloud supports these regions: `us-west-2`, `eu-central-1`, and `ap-southeast-1`.
- For information about Cisco ISE versions and query sizes, see [Query limitation](#) in the pxGrid Cloud SDK on GitHub.

How the pxGrid Cloud identity source works

The following figure shows how the identity source works.



Your Secure Firewall Management Center uses the pxGrid Cloud SDK to programmatically retrieve user information from an on-premises Cisco ISE server or cluster so these users can be used in identity policies on the Secure Firewall Management Center.

To authorize and authenticate this data exchange, you must:

1. In Cisco ISE, enable the use of pxGrid Cloud.
2. Register Cisco ISE as a product in pxGrid Cloud, which authenticates Cisco ISE and pxGrid Cloud and enables them to communicate with each other.

The authentication process requires you to paste a one-time password (OTP) from pxGrid Cloud into Cisco ISE.

3. In pxGrid Cloud, create an "app instance" that generates an OTP for you to use in the Secure Firewall Management Center to authenticate the two with each other.
4. After completing all the preceding tasks, the Secure Firewall Management Center (which includes the pxGrid Cloud SDK) can query Cisco ISE using pxGrid Cloud and retrieve sessions containing user information, SGT, endpoint profile, and other details.
5. Many types of dynamic objects can be filtered and sent to the Secure Firewall Management Center as dynamic objects to be used in access control rules. These include: SGT, endpoint profile, posture status, and machine authentication.

We retrieve user information from Cisco ISE and group information from either Microsoft Active Directory or Azure Active Directory.

Related Topics

[How to configure a pxGrid Cloud identity source \(Cisco ISE 3.4 or later\)](#)

[How to configure a pxGrid Cloud identity source \(Cisco ISE 3.3 or earlier\), on page 3](#)

How to configure a pxGrid Cloud identity source

These topics summarize how to configure a pxGrid Cloud identity source either for ISE 3.3 and earlier or for ISE 3.4 and later. The steps are different so make sure you follow them exactly.

Related Topics

[How to configure a pxGrid Cloud identity source \(Cisco ISE 3.4 or later\)](#)

[How to configure a pxGrid Cloud identity source \(Cisco ISE 3.3 or earlier\), on page 3](#)

[Enable the pxGrid Cloud service in Cisco ISE](#)

[Create an app instance](#)

[Create the identity source, on page 12](#)

[Activate the app instance, on page 13](#)

[Activate the pxGrid Cloud identity source, on page 16](#)

How to configure a pxGrid Cloud identity source (Cisco ISE 3.3 or earlier)

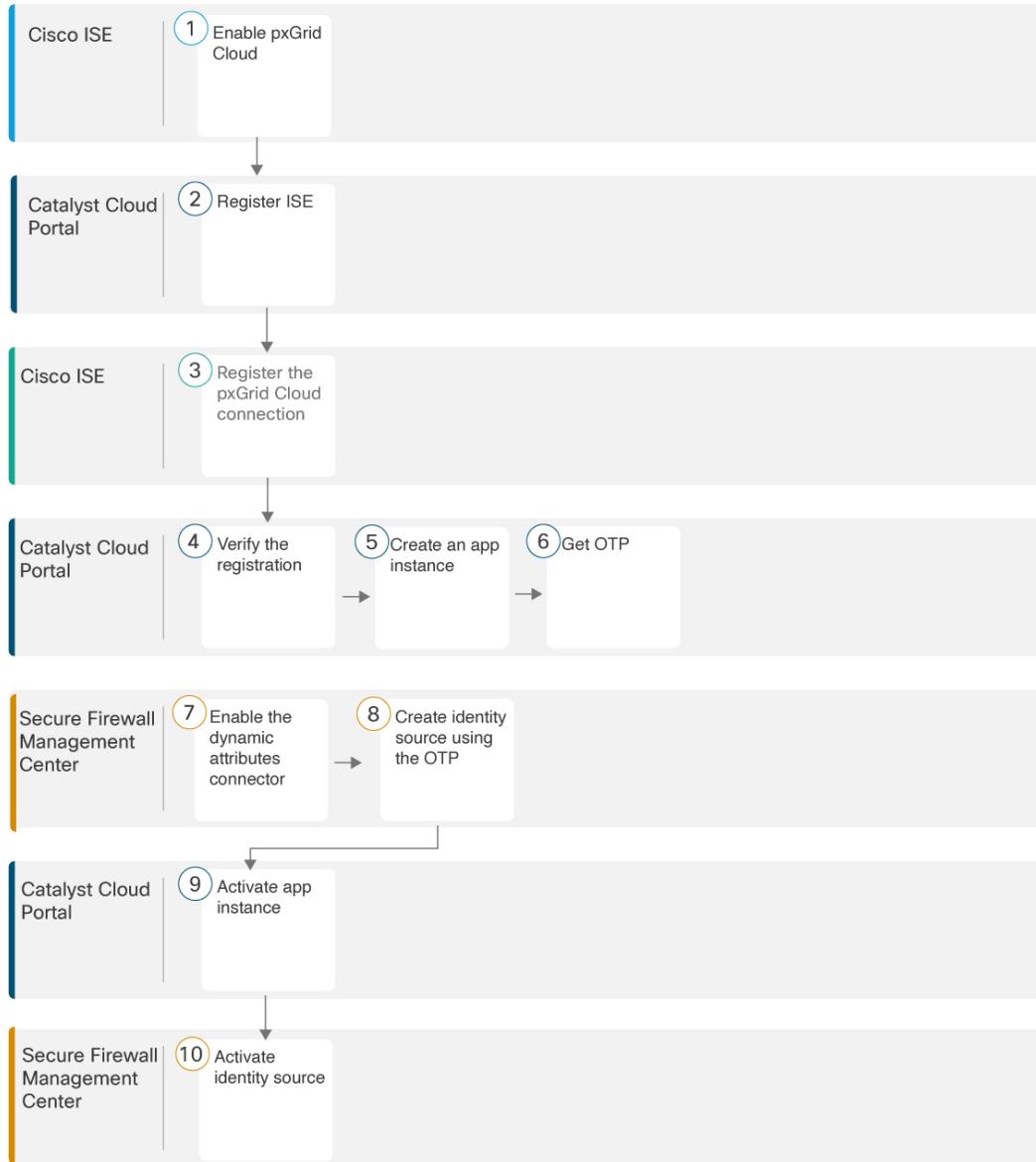
Before you begin, create a [Cisco Account](#).

How to configure a pxGrid Cloud identity source (Cisco ISE 3.3 or earlier)



Important This topic applies to Cisco ISE version 3.3 or earlier. If you are using a later version, see [How to configure a pxGrid Cloud identity source \(Cisco ISE 3.4 or later\)](#) instead.

The following figure shows the steps to configure a pxGrid Cloud identity source using Cisco ISE, the Catalyst Cloud Portal, and Secure Firewall Management Center.



- 1 [Enable the pxGrid Cloud service in Cisco ISE, on page 6](#)
- 2 [Register Cisco ISE with the Catalyst Cloud Portal, on page 7](#)
- 3 [Register Cisco ISE with the Catalyst Cloud Portal, on page 7](#)
- 4 [Create an app instance, on page 11](#)
- 5 [Enable the dynamic attributes connector](#)

- 6 [Create an app instance, on page 11](#)
- 7 [Activate the app instance, on page 13](#)
- 8 [Activate the pxGrid Cloud identity source, on page 16](#)

Table 1: Configure a pxGrid Cloud identity source

1	Cisco ISE	Enable the pxGrid Cloud in Cisco ISE. pxGrid Cloud enables you to subscribe to offers and to register apps (in this case, the Secure Firewall Management Center) for secure data exchange in a cloud environment. For more information, see Enable the pxGrid Cloud service in Cisco ISE, on page 6 .
2	Catalyst Cloud Portal	Register Cisco ISE in the Catalyst Cloud Portal and authenticate communication between Cisco ISE and the Catalyst Cloud Portal. For more information, see Register Cisco ISE with the Catalyst Cloud Portal, on page 7 .
3 4	Cisco ISE, Catalyst Cloud Portal	Register the pxGrid Cloud with Cisco ISE and verify the registration. For more information, see Register the pxGrid Cloud connection with Cisco ISE, on page 9 .
5 6	Catalyst Cloud Portal, Secure Firewall Management Center	Create an application instance in the Catalyst Cloud Portal and get the one-time password (OTP). The application instance enables the Secure Firewall Management Center to authenticate with Cisco ISE using the pxGrid Cloud service. The OTP, required for the next step, expires in 60 minutes.
7	Secure Firewall Management Center	Enable the dynamic attributes connector if you haven't done so already. The dynamic attributes connector is required to use the pxGrid Cloud identity source. For more information, see Enable the dynamic attributes connector .
8	Secure Firewall Management Center	Create the pxGrid Cloud identity source using the OTP you got in the previous step. Linking the app enables the Secure Firewall Management Center to authenticate with Cisco ISE and the Catalyst Cloud Portal so it can receive user data from Cisco ISE. For more information, see Create the identity source, on page 12 .
9	Catalyst Cloud Portal	Activate the app instance. For more information, see Activate the app instance, on page 13 .
10	Secure Firewall Management Center	Activate the pxGrid Cloud identity source. For more information, see Activate the pxGrid Cloud identity source, on page 16

After you have completed all the preceding tasks, you can:

- Test the pxGrid Cloud identity source to make sure it's working properly.
For more information, see [Test the pxGrid Cloud identity source, on page 18](#).
- Create dynamic attributes filters, which define what dynamic objects are sent to the Secure Firewall Management Center.

For more information, see [Create dynamic attributes filters, on page 23](#).

- After you configure the pxGrid Cloud identity source, you can use any of the following in access control rules:
 - Dynamic objects
 - Microsoft AD user and groups
 - Azure AD users and groups

Related Topics

[Enable the pxGrid Cloud service in Cisco ISE, on page 6](#)

Enable the pxGrid Cloud service in Cisco ISE

Before you begin

- Ensure that you 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, you must configure Cisco ISE proxy settings if the customer network uses a proxy to reach the internet. To configure proxy settings in Cisco ISE, click the **Menu** icon (≡) and 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 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**, navigate to **Administration > System > Certificates**.

Procedure

Step 1 In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration > System > Deployment**.

Step 2 Click the node on which you want to enable the pxGrid Cloud service.

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

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

The pxGrid Cloud service can be enabled on two nodes to enable high availability.

Note

You can enable the **pxGrid Cloud** option only when the **pxGrid** service is enabled on that node.

Register Cisco ISE with the Catalyst Cloud Portal

This task discusses how to register Cisco ISE as an app in the Catalyst Cloud Portal and to authenticate communication between the Catalyst Cloud Portal and Cisco ISE.

Also refer to [Register Cisco ISE](#) in the *pxGrid Cloud Solution Guide*.

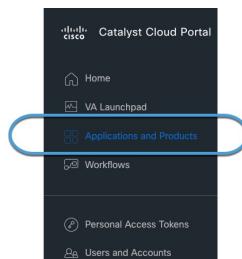
Procedure

Step 1 Log in to the [Cisco Cloud Catalyst Portal](#).

Step 2 If prompted, choose an account to use.

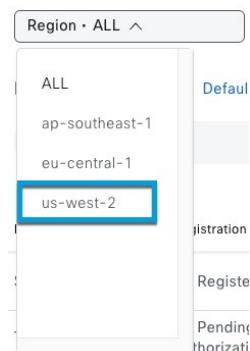
Step 3 Click **Register**.

Step 4 In the Catalyst Cloud Portal, click **☰ > Applications and Products** as the following figure shows:



Step 5 At the top of the page, click **Products**.

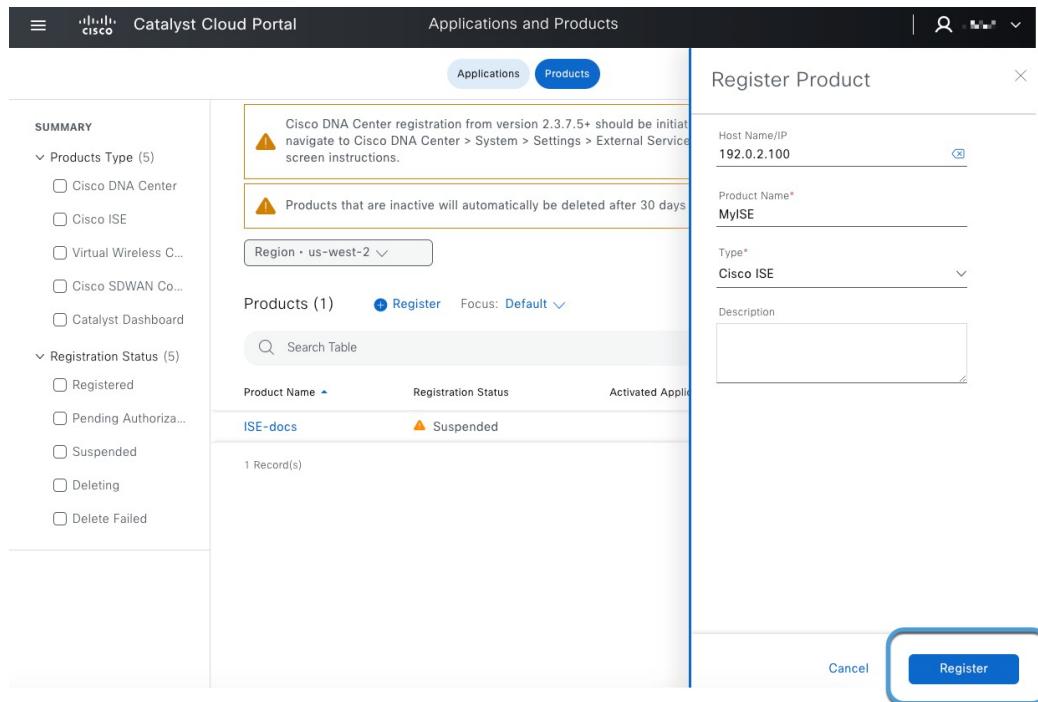
Step 6 From the **Region** list, click **us-west-2**, **eu-central-1**, or **ap-southeast-1**.



Step 7 Click **Register**.

The following figure shows a sample registration page.

Register Cisco ISE with the Catalyst Cloud Portal



Step 8

Enter the following information.

- **Host Name/IP:** (Optional.) Enter the ISE server's fully qualified domain name or IP address. If you enter an IP address, omit the scheme (for example, **https://**) and the port, if any.
- **Product Name:** Enter a unique name to identify this server.
- **Type:** From the list, click **Cisco ISE**.
- **Description:** Enter an optional description.

Step 9

Click **Register**.

Step 10

Generate a one-time password (OTP) in any of the following ways:

- If you've previously registered ISE apps and see yours listed, click **Generate OTP** in the **Actions** column; you'll need it in the next part of this procedure.
- If you're registering your app now, the OTP is displayed. Click  to copy it to the clipboard; you'll need it in the next part of this procedure.

What to do next

See [Register the pxGrid Cloud connection with Cisco ISE, on page 9](#).

Register the pxGrid Cloud connection with Cisco ISE

This task discusses how to register the pxGrid Cloud connection with Cisco ISE, which enables pxGrid Cloud to send user data to the pxGrid Cloud identity source in Security Cloud Control.

Before you begin

Complete the tasks discussed in [Register Cisco ISE with the Catalyst Cloud Portal, on page 7](#).

Procedure

Step 1 Log in to Cisco ISE as an administrator.

Step 2 Click  > **Administration** > **pxGrid Services** > **Client Management** > **pxGrid Cloud Connection**.

Step 3 Make sure all services are enabled with read/write privileges.

The following figure shows an example.

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.

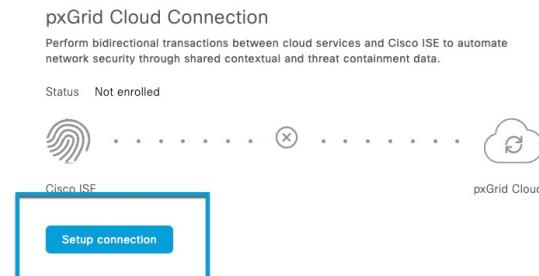
pxGrid Services

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.



Step 4 In the left navigation bar, click **pxGrid Cloud Connection**.

Step 5 Click **Setup Connection** as the following figure shows.

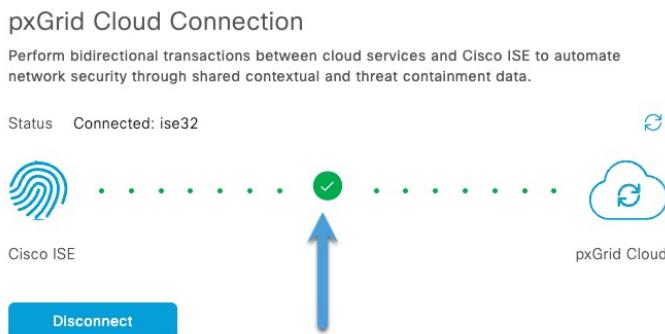


Step 6 Paste the OTP value in the provided field.

Create a pxGrid Cloud identity source

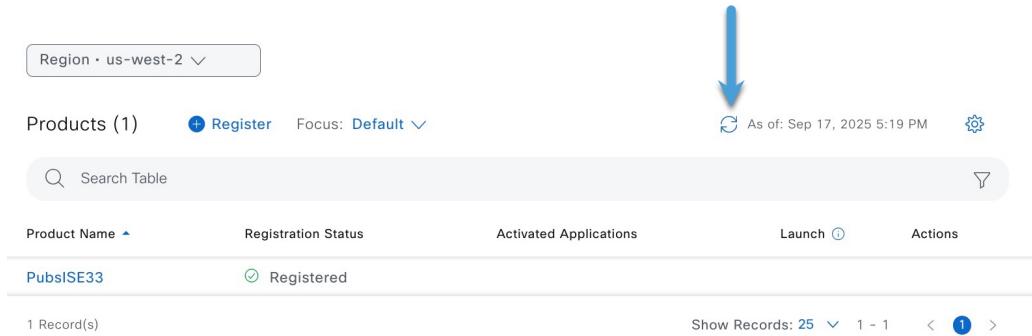
Step 7 Click Connect.

A green check mark like the following confirms that connection was successful.



Step 8 Confirm the setup has been successful so far:

- Log in to the Catalyst Cloud Portal.
- Click the **Products** tab.
- Click **Refresh** as the following figure shows.



- Verify that **Registered** is displayed as the status of your product.

What to do next

Continue with [Create the identity source, on page 12](#).

Create a pxGrid Cloud identity source

The following tasks discuss how to create a pxGrid Cloud identity source using Cisco ISE, the Catalyst Cloud Portal, and Security Cloud Control. You must complete all tasks in the order shown; in some cases, there is a time limit due to the expiration of a required One-Time Password (OTP).

Related Topics

- [Create an app instance, on page 11](#)
- [Create the identity source, on page 12](#)
- [Activate the app instance, on page 13](#)

Activate the pxGrid Cloud identity source, on page 16
 Test the pxGrid Cloud identity source, on page 18

Create an app instance

This task is one of several tasks you must perform to create a pxGrid Cloud identity source to send user session data to the Secure Firewall Management Center.

There is a one-hour time limit on the one-time password (OTP) required to complete this procedure successfully. You do not need to log in to Cisco ISE.

Before you begin

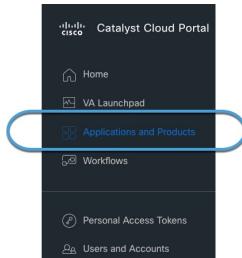
Complete all of the following tasks first:

- Enable the pxGrid Cloud service in Cisco ISE, on page 6
- Register Cisco ISE with the Catalyst Cloud Portal, on page 7
- Register the pxGrid Cloud connection with Cisco ISE, on page 9

Procedure

Step 1 Log in to the [Cisco Catalyst Cloud Portal](#).

Step 2 In the Catalyst Cloud Portal, click  **Applications and Products** as the following figure shows:



Step 3 At the top of the page, click **Applications**.

From the **Regions** list, click **us-west-2**, **eu-central-1**, or **ap-southeast-1**.

Step 5 Click **Manage** (or **Activate**) next to **Firepower Management Center**.

Step 6 Click **Add**.

Step 7 Click **Create a New One**.

The following figure shows an example.

Choose Application Instance

Select which Application Instance you would like to connect your product to. Not seeing the Instance that you want? [Create a New One](#)



Step 8 Click the copy button next to the displayed OTP as the following figure shows:

Create the identity source

Region - us-west-2 ✓

Authenticate your application

We have detected that your 'Firewall Management Center' is not yet authenticated. Please redeem the below OTP in your application interface to complete authentication.

UhHeDX5...  

The OTP is valid only for 60 minutes.

In case you have just authenticated. Please click [here](#) to re-verify.

Step 9 Copy the OTP to a text file; it expires in 60 minutes.

Step 10 Continue with [Create the identity source, on page 12](#).

Create the identity source

This task is one of several required to create a pxGrid Cloud identity source to send user session data to the Secure Firewall Management Center.

Before you begin

Complete the task discussed in [Create an app instance, on page 11](#).

Procedure

Step 1 Log in to the Secure Firewall Management Center

Step 2 Click **Integrations > Identity > Identity Sources**

Step 3 Click **Identity Services Engine (pxGrid Cloud)**.

Step 4 Click **Create pxGrid Application Instance**.

The following figure shows an example.

Create pxGrid App Instance

Name *

Description

OTP (One-Time Password) * [How to get OTP](#)

OTP Enables you to set up your pxGrid Tenant

Step 5 Enter the following information.

Value	Description
Name	Enter a name to uniquely identify this connector.
Description	Optional description.
OTP (One-Time Password)	Enter the OTP.

Step 6Click **Create**.**Step 7**At the top of the page, click **Save**.**Step 8**Continue with [Activate the app instance, on page 13](#).

Activate the app instance

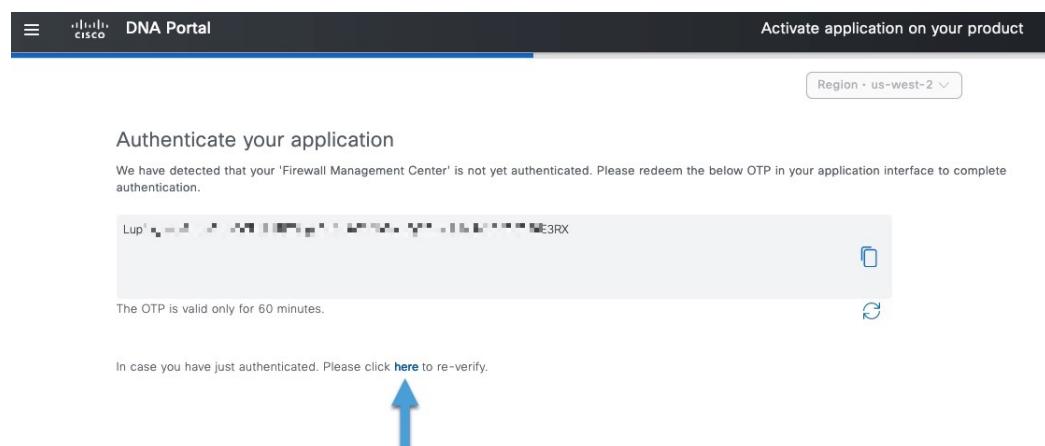
This task discusses how to create a pxGrid Cloud identity source to send user session data to the Secure Firewall Management Center.

There is a one-hour time limit on the one-time password (OTP) required to complete this procedure successfully. You do not need to log in to Cisco ISE.

Before you begin

Complete the task discussed in [Create the identity source, on page 12](#).

Procedure

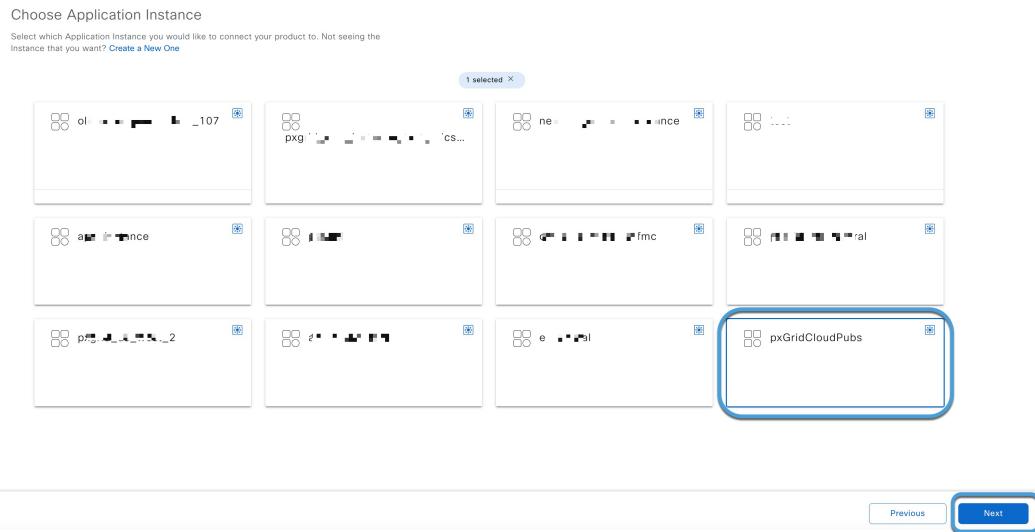
Step 1Log in to the [Cisco Catalyst Cloud Portal](#).**Step 2**Reverify the app by clicking the word **here** as the following figure shows.**Step 3**

Click the name of the application instance you just created in Secure Firewall Management Center.

Step 4Click **Next**.

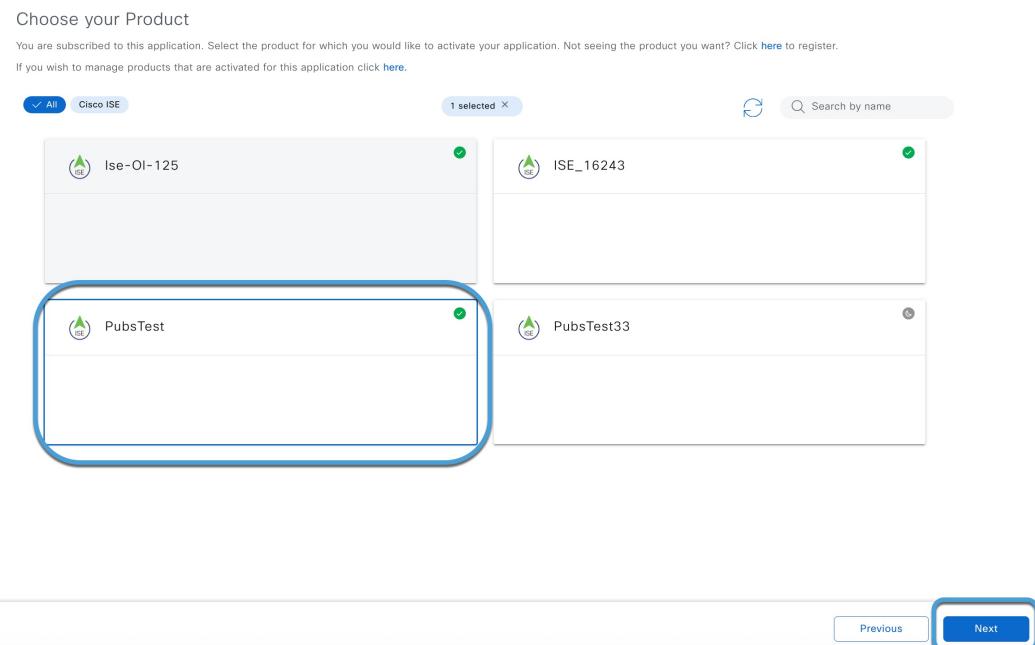
Example:

Activate the app instance



Step 5 On the Choose Product page, click the name of the Cisco ISE product and click **Next**.

Example:



Step 6 Select the check box next to each scope. The following figure shows an example.

Region • us-west-2 ✓

Configure Access Control

Choose the functional capabilities and API Access control to be allowed for application "Firewall Management Center" on this products "PubsTest".

The screenshot shows a configuration interface for an application. At the top, a region is selected as 'us-west-2'. The main section is titled 'Configure Access Control' with a sub-instruction: 'Choose the functional capabilities and API Access control to be allowed for application "Firewall Management Center" on this products "PubsTest".' On the left, under 'CAPABILITIES', there is a 'Select All' button followed by several checkboxes. The checked items are: 'Adaptive Network Control (ANC) configuration', 'Identity Services Engine (ISE) Profiler configuration', 'TrustSec related topics (Configuration, SXP, etc.)', and 'Echo service topics used for testing'. On the right, under 'API ACCESS', it is noted that 'There are no API groups configured for this application.'

CAPABILITIES		API ACCESS
<input type="button" value="Select All"/>		There are no API groups configured for this application.
<input checked="" type="checkbox"/> Adaptive Network Control (ANC) configuration	<input checked="" type="checkbox"/> Echo service topics used for testing	
<input checked="" type="checkbox"/> Identity Services Engine (ISE) Profiler configuration	<input checked="" type="checkbox"/> ISE Session directory	
<input checked="" type="checkbox"/> TrustSec related topics (Configuration, SXP, etc.)		

Step 7 Click **Next**.

Step 8 Review the displayed information for accuracy. Make sure all scopes are selected. The following figure shows an example.

Activate the pxGrid Cloud identity source

Region - us-west-2

Summary

Please review all settings that you have entered. Click corresponding Edit for the settings you like to change.

Selected Application [Edit](#)

Name	Firewall Management Center
Description	Firepower Management Center (FMC) is integrating with to provide User Identity based access policy.
Instance Name	SteveJNew

Selected Product [Edit](#)

Region	us-west-2
Name	SteveJISE2
Description	

Selected Scopes [Edit](#)

Adaptive Network Control (ANC) configuration
 Echo service topics used for testing
 ISE Session directory

TrustSec related topics (Configuration, SXP, etc.)

Step 9 Click **Activate**.

It can take several minutes for the app instance to be activated.

Step 10 Continue with [Activate the pxGrid Cloud identity source, on page 16](#).

Activate the pxGrid Cloud identity source

This task explains how to activate the pxGrid Cloud identity source in the Secure Firewall Management Center.

Before you begin

Complete the tasks discussed in [Activate the app instance, on page 13](#).



Note Only one pxGrid Cloud identity source can be active at a time.

Procedure

Step 1 Log in to the Secure Firewall Management Center

Step 2 Click **Integrations > Identity > Identity Sources**

Step 3 Click **Identity Services Engine (pxGrid Cloud)**.

Step 4 Click **Save** at the top of the page.

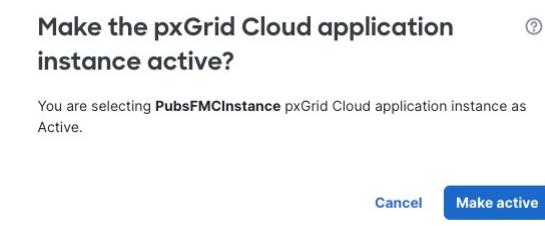
Step 5 If a green check mark is *not* displayed next to the name of the identity source, select it.

Example:

Selected	Name
<input checked="" type="checkbox"/>	pxGridISE33 Tenant ID: Cisco

Step 6 Click **Make Active**.

Example:



Step 7 (Optional.) Select the following options if desired:

- **Session Directory Topic:** Select the check box to receive ISE user session information from the Cisco ISE server.
- **SXP Topic:** Select the check box to receive updates to SGT-to-IP mappings when available from the ISE server. This option is required to use destination SGT tagging in access control rules.
- **ISE Network Filter:** Optional filter you can set to restrict the data that Cisco ISE reports. If you provide a network filter, Cisco ISE reports data from the networks in that filter.

You have the following options:

- Leave the field blank to specify **any**.
- Enter a single IPv4 address block using CIDR notation.
- Enter a list of IPv4 address blocks using CIDR notation, separated by commas.

Step 8 Under Activated ISE, expand the identity source.

Example *normal* result:

Test the pxGrid Cloud identity source

Status: Active

Settings: Subscribe To: Session Directory Topic SXP Topic | ISE Network Filter ex. 10.89.31.0/24

Application Instances

How it works Configure Filters

Selected	Name	Activated ISE	Description	Actions
	PubsFMCinstance	<ul style="list-style-type: none"> Scopes <ul style="list-style-type: none"> Anc Echo Profiler Session Trustsec Topics <ul style="list-style-type: none"> SecurityGroup EndpointProfile SessionDirectory SxpBinding 		<input type="button" value="Test"/>

Example *error* result:

Configure Identity Sources

Select the service type and start configuring the identity source. Deploy the changes after you're finished.

Service Type:

- None
- Identity Services Engine
- Identity Services Engine (pxGrid Cloud)
- Passive Identity Agent

Info You can configure Dynamic Firewall based on pxGrid Cloud. [Click here to learn more](#)

Error ISE_208 is/are unhealthy

Status: Error

Settings: Subscribe To: Session Directory Topic SXP Topic | ISE Network Filter ex. 10.89.31.0/24

Application Instances

How it works Configure Filters

Selected	Name	Activated ISE	Description	Actions
	ISE065_P1 (/Primary)	<ul style="list-style-type: none"> ISE065_P1 (/Primary) ISE_208 <ul style="list-style-type: none"> Cisco DNA Activated Scopes <ul style="list-style-type: none"> Anc Echo Profiler Session Trustsec Topics <ul style="list-style-type: none"> SessionDirectory Echo <ul style="list-style-type: none"> API failed with the error - Post "https://neoffers.cisco.com/api/dkhub/v2/api/proxy/request/68cbe918a884fd4f6c0b81f/direct/query": context deadline exceeded. 		<input type="button" value="Test"/>
	App	<ul style="list-style-type: none"> Tenant ID: Dynamic Firewall 		

In the event of an error, see [Test the pxGrid Cloud identity source, on page 18](#).

Step 9

Verify the status is Active and that all scopes and topics are displayed.

Step 10

Wait a few minutes for data to be downloaded.

What to do next

See [Test the pxGrid Cloud identity source, on page 18](#).

Test the pxGrid Cloud identity source

This topic discusses diagnostics you can perform using the Secure Firewall Management Center to determine if the identity source is working. Errors might include communication with Cisco ISE, or with the Cisco ISE configuration with Catalyst Cloud Portal.

View the current configuration

To get started:

1. Log in to the Secure Firewall Management Center.
2. Click **Integrations > Identity > Identity Sources**
3. Click **Identity Services Engine (pxGrid Cloud)**.

Sample configuration status

The following figure shows an example configuration.

The screenshot shows the 'Configure Identity Sources' page for pxGrid Cloud. The page has a header with tabs: Cloud Services, Realms, **Identity Sources**, High Availability, eStreamer, Host Input Client, and Smart Software Manager On-Prem. Below the tabs is a sub-header 'Configure Identity Sources' with a note: 'Select the service type and start configuring the identity source. Deploy the changes after you're finished.' The 'Service Type' section shows 'Identity Services Engine (pxGrid Cloud)' selected. A note below says: 'You can configure Dynamic Firewall based on pxGrid Cloud. [Click here to learn more](#)'. The main area shows 'Application Instances' with three entries:

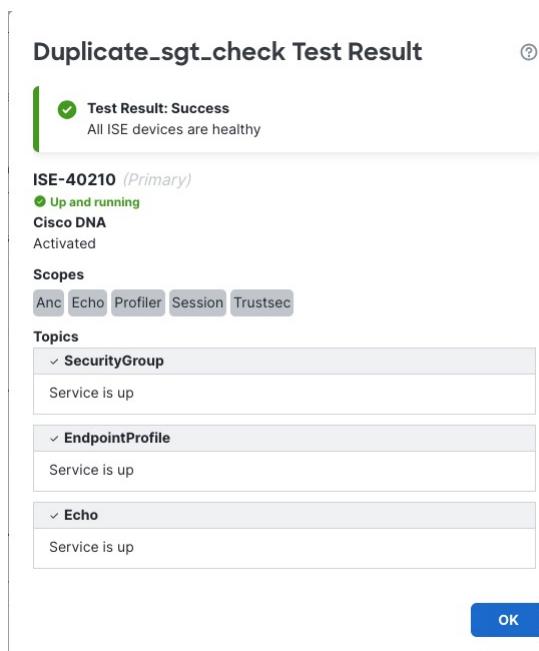
Selected	Name	Activated ISE	Description	Actions
<input type="radio"/>	App_instance1 Tenant ID: Dynamic Firewall	<input checked="" type="radio"/> ise202		4 Test Edit
<input checked="" type="radio"/>	pxgrid_multi_is_e_testing Tenant ID: ISE-235	> <input checked="" type="radio"/> ISE-235 (Configured)		Test Edit
<input type="radio"/>	test-empty-app-instance Tenant ID: ISE-234-1	<input checked="" type="radio"/> ise-234-1		Test Edit

The following table has more information about the numbered areas in the figure.

Number	Meaning
1	Overall status Any errors in the overall status of the Cisco ISE app instances are displayed. In that case, scroll to that instance and either expand the error message or click Test for more information.
2	Active A green check mark indicates the app is active.
3	Inactive A dimmed app instance is inactive. You can activate it by selecting the check box next to its name and then clicking Make active .
4	Test button Click Test to perform diagnostic tests that show more detailed status of the app instance. See the next section for more information.

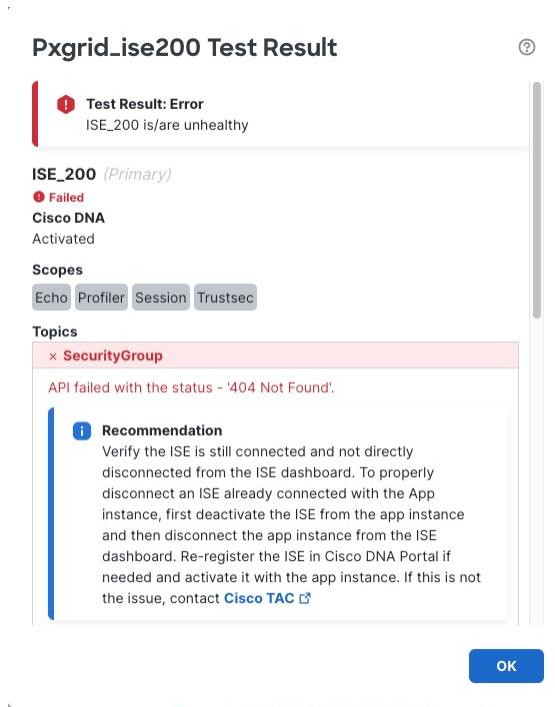
The following figure shows a sample success message.

Test the pxGrid Cloud identity source



The screenshot shows a test result dialog titled "Duplicate_sgt_check Test Result". The status is "Test Result: Success" with the message "All ISE devices are healthy". The "ISE-40210 (Primary)" device is listed as "Up and running" with "Cisco DNA" and "Activated" status. Under "Scopes", "Anc" is selected. Under "Topics", "SecurityGroup", "EndpointProfile", and "Echo" are listed, all showing "Service is up". A blue "OK" button is at the bottom right.

The following figure shows an example error result.



The screenshot shows a test result dialog titled "Pxgrid_ise200 Test Result". The status is "Test Result: Error" with the message "ISE_200 is/are unhealthy". The "ISE_200 (Primary)" device is listed as "Failed" with "Cisco DNA" and "Activated" status. Under "Scopes", "Echo" is selected. Under "Topics", "SecurityGroup" is highlighted in red with the error message "API failed with the status - '404 Not Found'". A "Recommendation" section suggests verifying the ISE connection and contacting Cisco TAC. A blue "OK" button is at the bottom right.

The following section provides a reference for the possible errors.

Error code reference

The following information is provided to help you diagnose and solve issues with Cisco ISE, pxGrid Cloud, and the Catalyst Cloud Portal. If these suggestions do not work, or if you have a different issue, contact [Cisco TAC](#).

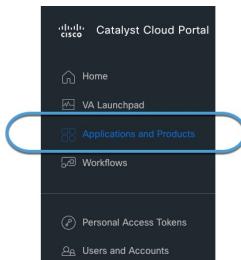
403 – Forbidden

Verify the Cisco ISE product is not in a **Pending** or **Suspended** state in the Catalyst Cloud Portal. If suspended, verify that Cisco ISE is registered as discussed in [Enable pxGrid Cloud service in Cisco ISE and register your device](#).

Additionally, verify pxGrid Cloud services are publicly available.

To verify whether or not your product is active:

1. Log in to the Catalyst Cloud Portal.
2. In the Catalyst Cloud Portal, go to  > **Applications and Products** as the following figure shows:



3. Click the **Products** tab.

The following figure shows an example of a suspended product.

Product Name	Registration Status	Region	Activated Applications	Launch	Actions
ISE-docs	 Suspended	us-west-2			...

4. To correct the issue, in the Actions column, click  and click **Generate OTP**.
5. Use the OTP as discussed in [Create the identity source, on page 12](#).

404 – Not Found

Verify the Cisco ISE server is not directly disconnected from the Cisco ISE dashboard. To properly disconnect Cisco ISE already connected with the app instance, first deactivate Cisco ISE from the app instance and then disconnect the app instance from the Cisco ISE dashboard.

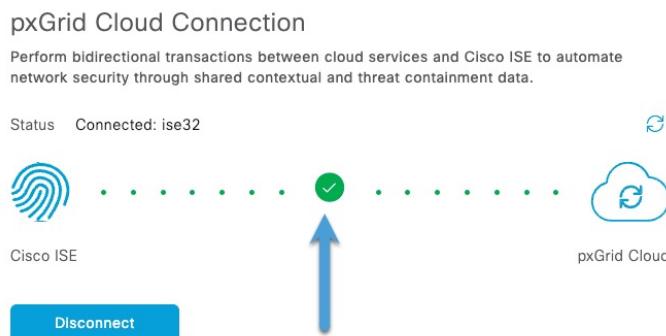
Test the pxGrid Cloud identity source

408 – Request Timeout

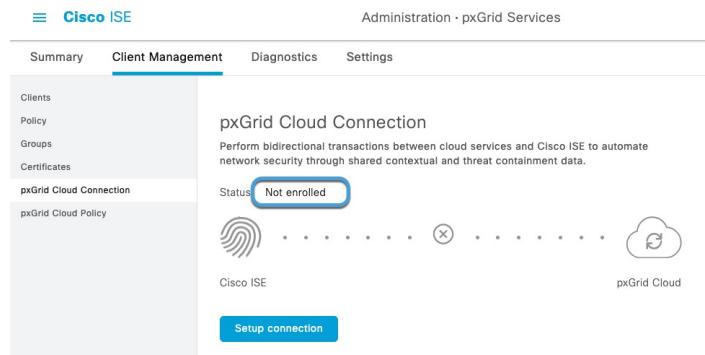
General connectivity

Check whether there are any general connectivity issues with Cisco ISE and verify pxGrid Cloud connectivity status is **Connected** in the ISE dashboard under [☰ > Administration > pxGrid Services > Client Management > pxGrid Cloud Connection](#).

The following figure shows an example of a system that is connected.



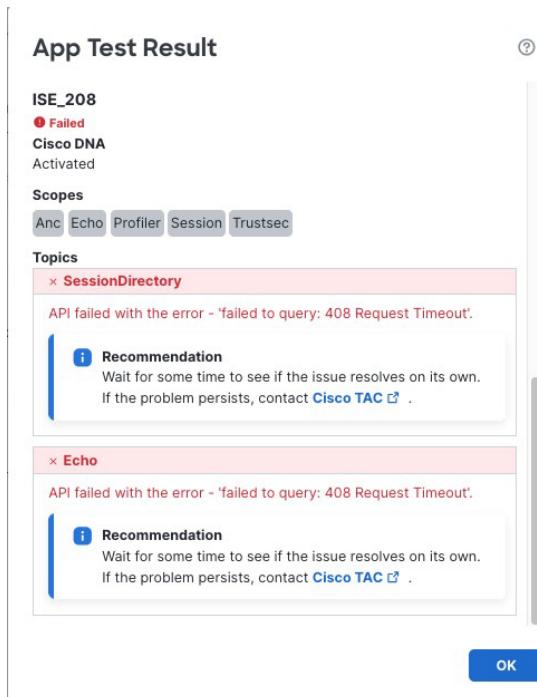
The following figure shows an example of a system that is not enrolled (meaning, not connected).



Verify the Cisco ISE server is not directly disconnected from the Cisco ISE dashboard. To properly disconnect Cisco ISE already connected with the app instance, first deactivate Cisco ISE from the app instance and then disconnect the app instance from the Cisco ISE dashboard.

Cluster member not reachable

If a member of the Cisco ISE cluster is not reachable, a page like the following is displayed:



To find what node is not reachable, log in to Cisco ISE primary administration node as an administrator and click the **Menu** icon (≡) and choose **Administration > System > Deployment**, then see [Node Status in a Cisco ISE Deployment](#).

413 – Content Too Large

We recommend you review the [pxGrid Cloud API limitations on GitHub](#). If needed, consider upgrading your Cisco ISE version to fully utilize pxGrid Cloud support.

500 – Internal Server Error

Check that the Cisco ISE server is operational and that pxGrid Cloud services are active (verify MNT, SXP, pxGrid nodes, and so on).

For more information, see Monitoring and debugging in the [Cisco pxGrid chapter](#) in the *Cisco Identity Services Engine Administrator Guide*.

Create dynamic attributes filters

Dynamic attributes filters that you define using the Dynamic Attributes Connector are exposed in the Secure Firewall Management Center as dynamic objects that can be used in access control policies. For example, restrict access to an AWS server for the Finance Department to only members of the Finance group defined in Microsoft Active Directory.



Note You cannot create dynamic attributes filters for Generic Text, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

Create dynamic attributes filters

For more information about access control or DNS rules, see [Create access control rules or DNS rules using dynamic attributes filters, on page 25](#).

Before you begin

[Create a connector](#)

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations > Dynamic Attributes Connector > Dynamic Attributes Filters**.

Step 3 Do any of the following:

- Add a new filter: click **Add** (+).
- Edit or delete a filter: Click **More** (⋮), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the following information.

Item	Description
Name	Unique name to identify the dynamic filter (as a dynamic object) in a policy and in the Secure Firewall Management Center Object Manager (External Attributes > Dynamic Object).
Connector	From the list, click the name of a connector to use.
Query	Click Add (+).

Step 5 To add or edit a query, enter the following information.

Item	Description
Key	Click a key from the list. Keys are fetched from the connector.
Operation	Click one of the following: <ul style="list-style-type: none"> • Equals to exactly match the key to the value. • Contains to match the key to the value if any part of the value matches.
Values	Click either Any or All and click one or more values from the list. Click Add another value to add values to your query.

Step 6 Click **Show Preview** to display a list of networks or IP addresses returned by your query.

Step 7 When you're finished, click **Save**.

Step 8 (Optional.) Verify the dynamic object in the Secure Firewall Management Center .

- Log in to the Secure Firewall Management Center as a user with the Network Admin role at minimum.
- Click **Objects > External Attributes > Dynamic Object**.

The dynamic attribute query you created should be displayed as a dynamic object.

Create access control rules or DNS rules using dynamic attributes filters

This topic discusses how to create access control rules using dynamic objects (these dynamic objects are named after the dynamic attributes filters you created previously).

To add dynamic attributes filters to DNS policies, see [Creating Basic DNS Policies](#).

To add dynamic attributes filters to DNS policies, see [Creating Basic DNS Policies](#).

Before you begin

Create dynamic attributes filters as discussed in [Create dynamic attributes filters, on page 23](#).



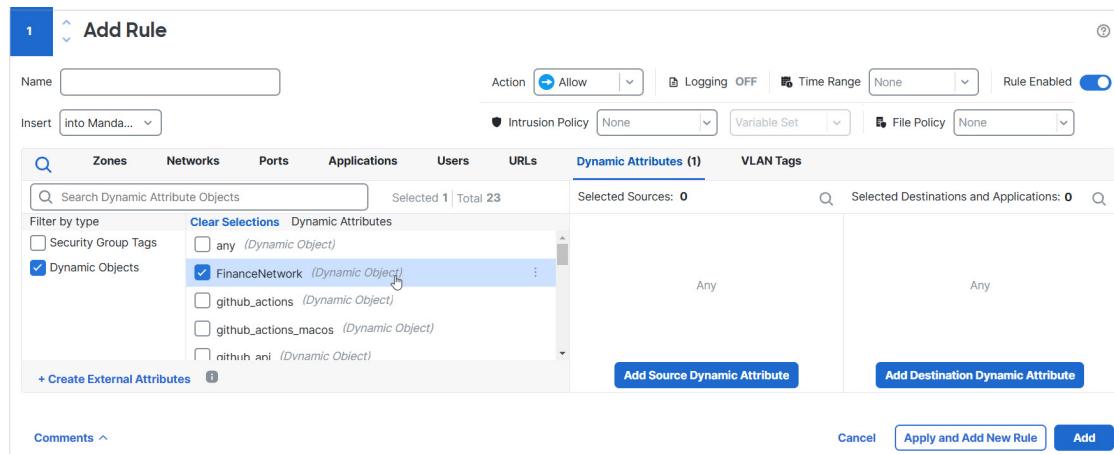
Note You cannot create dynamic attributes filters for Generic Text, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

Procedure

- Log in to the Secure Firewall Management Center
- Click **Policies > Security policies > Access Control**.
- Click **Edit** () next to an access control policy.
- Click **Add Rule**.
- Click the **Dynamic Attributes** tab.
- In the Available Attributes section, from the list, click **Dynamic Objects**.

The following figure shows an example.

Troubleshoot the pxGrid Cloud identity source



This example shows a dynamic object named `APIC Dynamic Attribute` that corresponds to the dynamic attribute filter created in the dynamic attributes connector.

Step 7 Add the desired object to source or destination attributes.

Step 8 Add other conditions to the rule if desired.

What to do next

See [Dynamic attributes rule conditions](#).

Troubleshoot the pxGrid Cloud identity source

These topics describe troubleshooting the pxGrid Cloud identity source.

Related Topics

[Primary device cannot be processed](#), on page 26

Primary device cannot be processed

Each Cisco ISE cluster must be associated with one and only one app instance, typically in a single dedicated tenant.

If you associate a Cisco ISE with more than one app instance, an error such as `Error occurred: primary device cannot be processed` or `ISE is unhealthy` is displayed for the identity source.

Example:

The solution is to deactivate the ISE properly from other app instances for that tenant, before using it in any other tenant or app instance

Procedure

Step 1 Log in to the [Cisco Catalyst Cloud Portal](#).

Step 2 At the top of the page, click **Applications**.

Step 3 Locate a Cisco ISE product that is activated and verify it is the one causing the issue.
Example:

Step 4 Wait for the product to be removed.

Step 5 Deactivate the app instance as described in [Deactivate the pxGrid Cloud app instance, on page 28](#).

Deactivate and delete the pxGrid Cloud identity source

These topics discuss how to optionally:

- Deactivate the FMC app instance in the Catalyst Cloud Portal.

You can perform this optional task to troubleshoot issues with the Cisco ISE integration.

Deactivate the pxGrid Cloud app instance

- Delete the pxGrid Cloud identity source from the Secure Firewall Management Center.
You should delete the identity source only if you're certain you don't want to use it again.

Related Topics

[Deactivate the pxGrid Cloud app instance](#), on page 28

[Delete the pxGrid Cloud identity source](#), on page 30

Deactivate the pxGrid Cloud app instance

(Optional.) This task explains how to deactivate a pxGrid Cloud app instance using the Catalyst Cloud Portal. You should do this only if your Cisco ISE or pxGrid Cloud stops working or you need to update it.

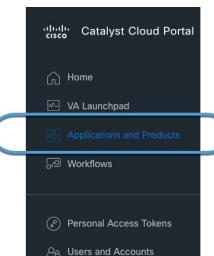
Before you begin

Make sure your current pxGrid Cloud identity source is active as discussed in [Activate the pxGrid Cloud identity source](#), on page 16.

Procedure

Step 1 Log in to the [Cisco Catalyst Cloud Portal](#).

Step 2 In the Catalyst Cloud Portal, click  > **Applications and Products** as the following figure shows:

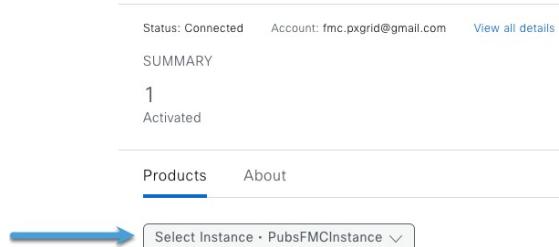


Step 3 Click **Applications**.

Step 4 Click **Manage** for Firewall Management Center.

Step 5 From the **Select Instance** list, click the name of the firewall application you created earlier.

Example:



Step 6 In the Actions column, click More icon () > **Deactivate**.

Step 7 Wait until the product is removed.

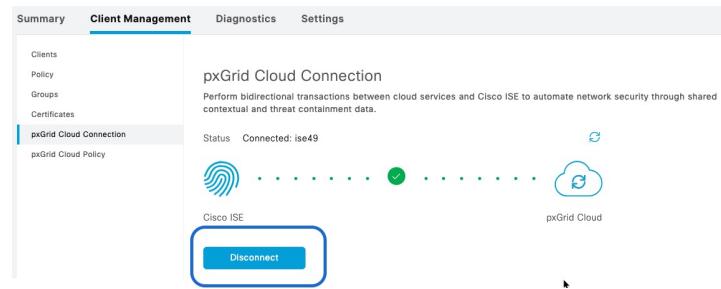
You can click **Refresh (C)** to see updated status if necessary.

Step 8

ISE 3.3 or earlier: Disconnect the app instance:

- Log in to Cisco ISE as an administrator.
- Click **Administration > pxGrid Services > Client Management > pxGrid cloud connection**.
- Click **Disconnect**.

Example:

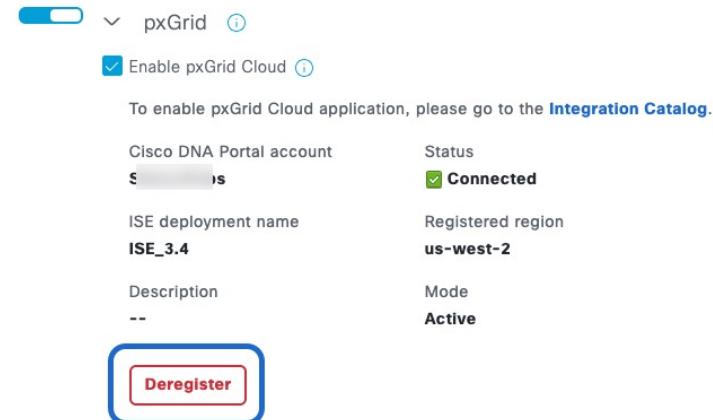


Step 9

ISE 3.4 or later: Deregister the app instance:

- Log in to Cisco ISE as an administrator.
- Click **Administration > System > Deployment**.
- Expand **Deployment**.
- Click the name of the ISE node.
- In the **General Settings** tab page, scroll to locate **pxGrid**.
- Click **Deregister**.

Example:



Step 10

To verify the app instance is deactivated in Secure Firewall Management Center:

- Log in to Secure Firewall Management Center.
- Click **Integrations > Identity > Identity Sources**.
- Click **Identity Services Engine (pxGrid Cloud)**.
- Verify that **Not Activated** is displayed in the Activated ISE column.

Example:

Delete the pxGrid Cloud identity source

Configure Identity Sources

Select the service type and start configuring the identity source. Deploy the changes after you're finished.

Service Type:

- None
- Identity Services Engine
- Identity Services Engine (pxGrid Cloud)
- Passive Identity Agent

Notes:

- Info:** You can configure Dynamic Firewall based on pxGrid Cloud. [Click here to learn more](#)
- Warning:** Register the ISE Product, activate it and try saving again

Status: Error

Settings: Subscribe To: Session Directory Topic SXP Topic | ISE Network Filter ex. 10.89.31.0/24

Application Instances

Selected	Name	Activated ISE	Description	Actions
<input checked="" type="checkbox"/>	PubsFMCInstance Tenant ID: SteveJPubs	Not Activated Info: Go to the Cisco DNA Portal to activate the application instance there.		Test Edit

[How it works](#) [Configure Filters](#) [+ Create pxGrid Application Instance](#)

What to do next

- To register Cisco ISE with pxGrid Cloud and activate the app instance, see:
 - ISE 3.3 and earlier: [Register Cisco ISE with the Catalyst Cloud Portal, on page 7](#).
 - ISE 3.4 and later: [Create an app instance](#).
- To completely remove the identity source, see [Delete the pxGrid Cloud identity source, on page 30](#).

Delete the pxGrid Cloud identity source

(Optional.) This task explains how to delete the pxGrid Cloud identity source from Secure Firewall Management Center, which is necessary if you do not want to use it again.

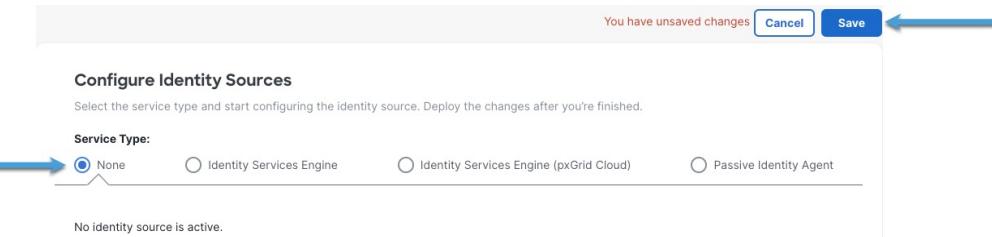
Before you begin

Deactivate the FMC app instance from the Catalyst Cloud Portal as discussed in [Deactivate the pxGrid Cloud app instance, on page 28](#).

Procedure

- Step 1** Log in to the Secure Firewall Management Center
- Step 2** Click **Integrations > Identity > Identity Sources**
- Step 3** Click **Identity Services Engine (pxGrid Cloud)**.
- Step 4** For Service Type, click **None**.

Example:



Step 5 Click **Save**.

Step 6 You are required to confirm your choice.

Step 7 Click **Identity Services Engine (pxGrid Cloud)**.

Step 8 Click **Delete** (☒).

Example:

Selected	Name	Activated ISE	Description	Actions
<input checked="" type="checkbox"/>	PubsFMCinstance Tenant ID: SteveJPubs	Not Activated Go to the Cisco DNA Portal to activate the application instance there.		Test ☒

Step 9 You are required to confirm the action.

■ Delete the pxGrid Cloud identity source