



Identity Source: pxGrid Cloud Identity (ISE 3.4 and Later)

The following topics discuss how to configure and use the pxGrid Cloud Identity Source with Cisco ISE version 3.4 and later.

- [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 5](#)
- [Create an app instance, on page 8](#)
- [Create the identity source, on page 9](#)
- [Activate the app instance, on page 10](#)
- [Activate the pxGrid Cloud identity source, on page 13](#)
- [Test the pxGrid Cloud identity source, on page 15](#)
- [Troubleshoot the pxGrid Cloud identity source, on page 20](#)
- [Create dynamic attributes filters, on page 21](#)
- [Create access control rules or DNS rules using dynamic attributes filters, on page 22](#)
- [Deactivate and delete the pxGrid Cloud identity source, on page 24](#)

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 Cisco ISE in Cloud-Delivered Firewall Management Center access control rules. Also, the identity source uses constantly changing dynamic objects from Cisco ISE in access control policies in the Cloud-Delivered 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 Security Cloud Control, you must [Create a Cisco Account](#).

- [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

Related Topics

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

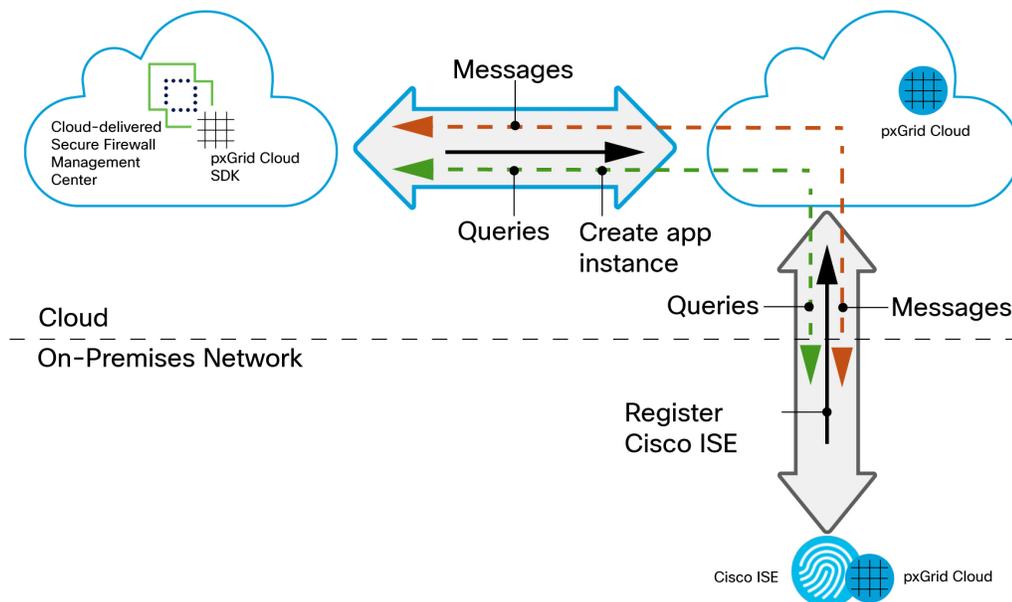
Limitations of the pxGrid Cloud identity source

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`.

How the pxGrid Cloud identity source works

The following figure shows how the identity source works.



Your Cloud-Delivered Firewall Management Center uses the pxGrid Cloud SDK to programmatically retrieve user information from an on-premises Cisco ISE server so these users can be used in identity policies on the Cloud-Delivered 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 Cloud-Delivered Firewall Management Center to authenticate the two with each other.
4. After completing all the preceding tasks, the Cloud-Delivered 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 Cloud-Delivered 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 \(Cisco ISE 3.4 or later\)](#), on page 3

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

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 \(Cisco ISE 3.4 or later\)](#), on page 3

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

[Enable the pxGrid Cloud service in Cisco ISE](#), on page 5

[Create an app instance](#), on page 8

[Create the identity source](#)

[Activate the app instance](#)

[Activate the pxGrid Cloud identity source](#)

How to configure a pxGrid Cloud identity source (Cisco ISE 3.4 or later)

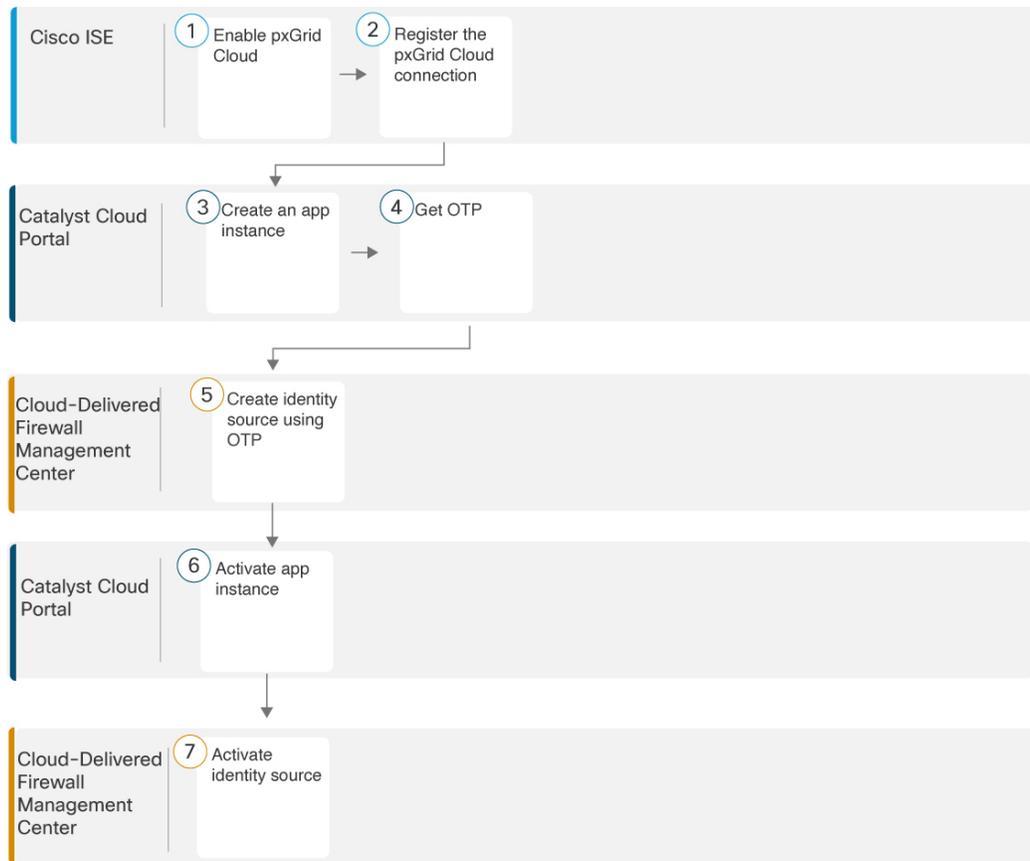
Before you begin, create a [Cisco Account](#).



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

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

How to configure a pxGrid Cloud identity source (Cisco ISE 3.4 or later)



- 1 Enable the pxGrid Cloud service in Cisco ISE, on page 5
- 2 Register the pxGrid Cloud connection with Cisco ISE
- 3 Create an app instance, on page 8
- 4 Create an app instance, on page 8
- 5 Create a pxGrid Cloud identity source
- 6 Activate the app instance
- 7 Activate the pxGrid Cloud identity source

Table 1: Configure a pxGrid Cloud identity source

1, 2	Cisco ISE	<p>Enable pxGrid Cloud in Cisco ISE.</p> <p>pxGrid Cloud enables you to subscribe to offers and to register apps (in this case, the Cloud-Delivered Firewall Management Center) for secure data exchange in a cloud environment.</p> <p>For more information, see Enable the pxGrid Cloud service in Cisco ISE, on page 5.</p>
3, 4	Catalyst Cloud Portal	<p>Create an app instance and get the one-time password (OTP) required to create the pxGrid Cloud identity source.</p> <p>For more information, see Create an app instance, on page 8.</p>

5	Cloud-Delivered Firewall Management Center	<p>Create the pxGrid Cloud identity source.</p> <p>The identity source enables the Cloud-Delivered Firewall Management Center to authenticate with Cisco ISE and the Catalyst Cloud Portal so it can receive user data from Cisco ISE.</p> <p>For more information, see Create the identity source.</p>
6	Catalyst Cloud Portal	<p>Activate the app instance.</p> <p>For more information, see Activate the app instance.</p>
7	Cloud-Delivered Firewall Management Center	<p>Activate the pxGrid Cloud identity source.</p> <p>For more information, see Activate the pxGrid Cloud identity source.</p>

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](#).
- Create dynamic attributes filters, which define what dynamic objects are sent to the Cloud-Delivered Firewall Management Center.
For more information, see [Create dynamic attributes filters](#).
- 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](#)

Enable the pxGrid Cloud service in Cisco ISE

This task explains how to enable pxGrid Cloud in Cisco ISE.

Before you begin

- 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 Cisco pxGrid Cloud. Verify 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** Log in as an administrator to Cisco ISE.
If your Cisco ISE server is part of a cluster, log in to the Primary Administration Node (PAN).
- Step 2** Click the **Menu** icon () , then click **Administration > Deployment**.
- Step 3** Under Deployment Nodes, click the name of the deployment node.
- Step 4** On the next page, scroll down to locate the **pxGrid** node.
- Step 5** Select the **Enable pxGrid Cloud** check box.
- Step 6** Enter the following information:

Option	Description
ISE Deployment Name	Enter a unique name to identify your ISE deployment.
Description (Optional)	Enter an optional description.
Region	Click the region you're in (us-west-2 , eu-central-1 , or ap-southeast-1). This is the only valid region at this time.
License agreements	You are required to select both check boxes to continue.

- Step 7** Click **Register**.
Example:

pxGrid ⓘ

Enable pxGrid Cloud ⓘ

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

ISE deployment name

PubsTest

Description (optional)

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

Region

us-west-2

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

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

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

Register

- Step 8** When prompted with an activation code for the Catalyst Cloud Portal, click **Next**.
- Step 9** When prompted, log in to the Catalyst Cloud Portal.
- Step 10** At the Select an Account dialog box, click the name of an account with which to register Cisco ISE.
- Step 11** Click **Register ISE**.

What to do next

See [Verify Cisco ISE registration in the Catalyst Cloud Portal, on page 7](#).

Verify Cisco ISE registration in the Catalyst Cloud Portal

This task explains how to verify that Cisco ISE is registered with the Catalyst Cloud Portal.

Before you begin

Complete the tasks discussed in [Enable the pxGrid Cloud service in Cisco ISE, on page 5](#).

Procedure

- Step 1** Log in to the [Cisco Catalyst Cloud Portal](#).
- Step 2** If prompted, select the account.
- Step 3** In the left navigation, click  > **Applications and Products**.
- Step 4** At the top of the page, click **Products**.
- Step 5** Click the name of the Cisco ISE deployment you created previously.
- Step 6** Make sure that **Registered** is displayed for its status.

Example:

Product Details

Product Name	PubsTest
Description	
Product Type	Cisco ISE
Region	us-west-2
Last Heartbeat Status	 September 15th, 2025 - 2:30:28 PM
Registration Status	 Registered

What to do next

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 Cloud-Delivered Firewall Management Center.

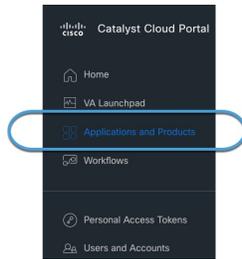
There is a one-hour time limit on the one-time password (OTP) required to complete this procedure successfully. You do not need to log in to Cisco ISE.

Before you begin

[Verify Cisco ISE registration in the Catalyst Cloud Portal, on page 7.](#)

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**.

Step 4 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**.

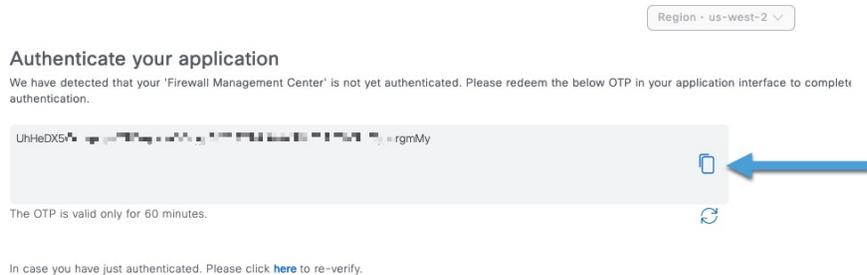
The following figure shows an example.

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:



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

Step 10 Continue with [Create the identity source](#).

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 Cloud-Delivered Firewall Management Center.

Before you begin

Complete the task discussed in [Create an app instance](#).

Procedure

- Step 1** Log in to Security Cloud Control as a user with the Super Admin role.
- Step 2** Click **Policies > Threat Defense > Integration > Other 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.

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

Activate the app instance

This task discusses how to create a pxGrid Cloud identity source to send user session data to the Cloud-Delivered 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.

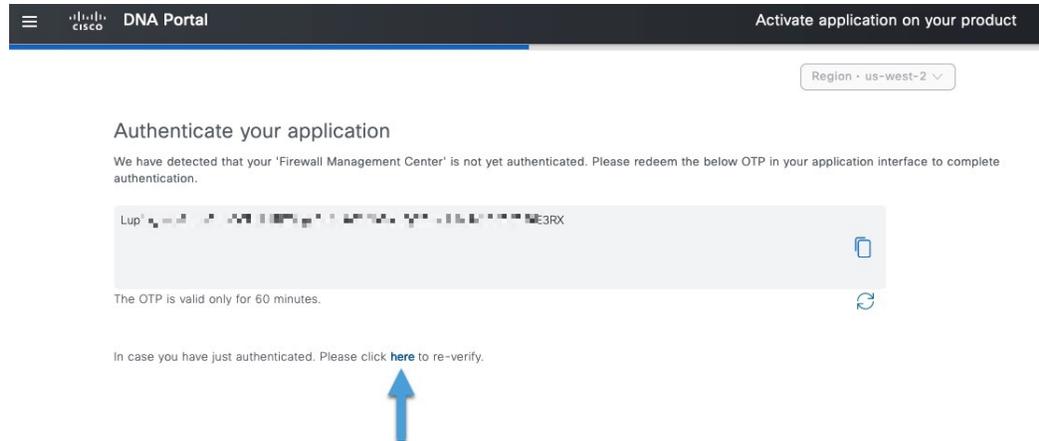
Before you begin

Complete the task discussed in [Create the identity source](#).

Procedure

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

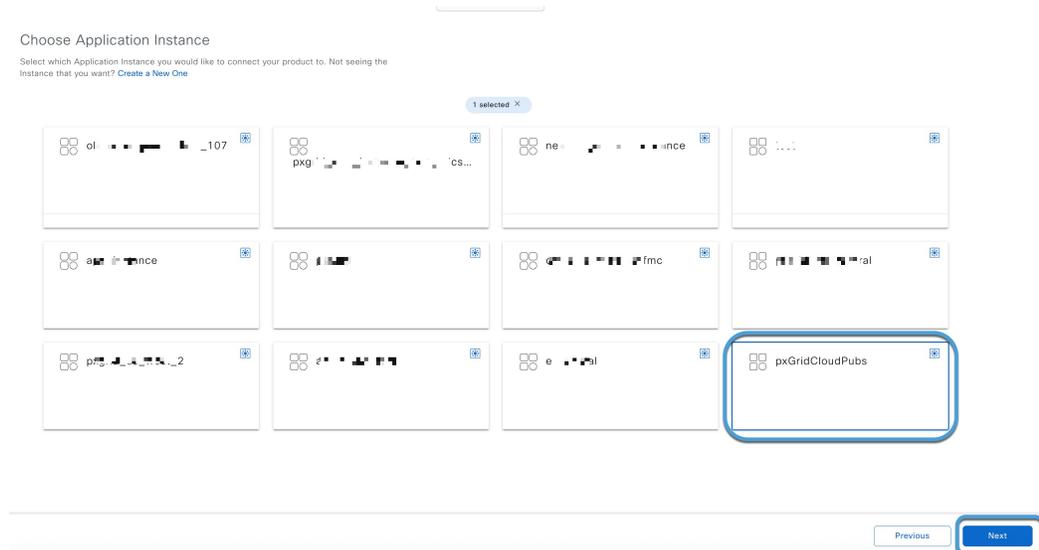
Step 2 Reverify the app by clicking the word **here** as the following figure shows.



Step 3 Click the name of the application instance you just created in Cloud-Delivered Firewall Management Center.

Step 4 Click **Next**.

Example:



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

Example:

Activate the app instance

Choose your Product

You are subscribed to this application. Select the product for which you would like to activate your application. Not seeing the product you want? Click [here](#) to register.
If you wish to manage products that are activated for this application click [here](#).

The screenshot shows a product selection interface. At the top, there's a filter for 'Cisco ISE' and a search bar. Below, four product cards are displayed: 'Ise-OI-125', 'ISE_16243', 'PubsTest', and 'PubsTest33'. The 'PubsTest' card is highlighted with a blue border. At the bottom right, there are 'Previous' and 'Next' buttons, with the 'Next' button also highlighted with a blue border.

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".

CAPABILITIES

Select All

- Adaptive Network Control (ANC) configuration
- Echo service topics used for testing
- Identity Services Engine (ISE) Profiler configuration
- ISE Session directory
- TrustSec related topics (Configuration, SXP, etc.)

API ACCESS

There are no API groups configured for this application.

Step 7

Click **Next**.

- Step 8** Review the displayed information for accuracy. Make sure all scopes are selected.
- 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](#).

Activate the pxGrid Cloud identity source

This task explains how to activate the pxGrid Cloud identity source in the Security Cloud Control.

Before you begin

Complete the tasks discussed in [Activate the app instance](#).



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

Procedure

- Step 1** Log in to Security Cloud Control as a user with the Super Admin role.
- Step 2** Click **Policies > Threat Defense > Integration > Other 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:

Make the pxGrid Cloud application instance active? ⓘ

You are selecting **PubsFMCInstance** pxGrid Cloud application instance as Active.

Cancel **Make active**

Activate the pxGrid Cloud identity source

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:

The screenshot shows the configuration page for an identity source. At the top, the status is "Active". Under "Settings: Subscribe To:", the checkboxes for "Session Directory Topic", "SXP Topic", and "ISE Network Filter" are all checked. The "ISE Network Filter" field contains the example value "ex. 10.89.31.0/24". Below this, there is a table of "Application Instances". The table has columns for "Selected", "Name", "Activated ISE", "Description", and "Actions". One instance is listed: "PubsFMCInstance" with "Tenant ID: SteveJPubs". The "Activated ISE" column is expanded to show a tree view for "PubsTest (Primary)". Under "Scopes", there are tabs for "Any", "Echo", "Profiler", "Session", and "Trustsec". Under "Topics", there are three items: "SecurityGroup" (Total no. of events: 17), "EndpointProfile" (Total no. of events: 872), and "SessionDirectory" (Total no. of events: 1). "SxpBinding" is listed with 0 events. An "Actions" column contains a "Test" button.

Example *error* result:

The screenshot shows the "Configure Identity Sources" page. The "Service Type" is set to "Identity Services Engine (pxGrid Cloud)". A message states: "ISE_208 is/are unhealthy". Below this, the status is "Error". Under "Settings: Subscribe To:", "Session Directory Topic" is checked, while "SXP Topic" and "ISE Network Filter" are unchecked. The "ISE Network Filter" field contains "ex. 10.89.31.0/24". The "Application Instances" table shows one instance: "App" with "Tenant ID: Dynamic Firewall". The "Activated ISE" column is expanded to show a tree view for "ISE065_P1 (Primary)". Under "Scopes", there are tabs for "Any", "Echo", "Profiler", "Session", and "Trustsec". Under "Topics", there is one item: "SessionDirectory" (Total no. of events: 0). An "Echo" topic is listed with an error message: "API failed with the error - 'Post 'https://neoflows.cisco.com/api/v1/sub/v2/api/proxy/request/68cbee918a884fd4f6c0b81f/directquery': context deadline exceeded'". An "Actions" column contains a "Test" button.

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

- 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](#).

Test the pxGrid Cloud identity source

This topic discusses diagnostics you can perform using the Security Cloud Control 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 Security Cloud Control as a user with the Super Admin role.
2. Click **Policies > Threat Defense > Integration > Other Integrations > Identity > Identity Sources**
3. Click **Identity Services Engine (pxGrid Cloud)**.

Sample configuration status

The following figure shows an example configuration.

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

1 Status: ● Active

Settings: Subscribe To: Session Directory Topic SXP Topic ISE Network Filter

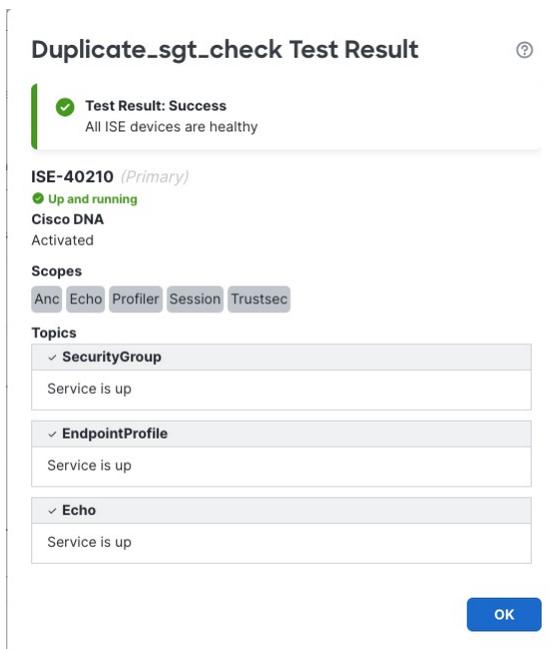
Application Instances How it works Configure Filters + Create pxGrid Application Instance

Selected	Name	Activated ISE	Description	Actions
<input type="radio"/>	App_instance1 Tenant ID: Dynamic Firewall	<input type="radio"/> Ise202		4 Test <input type="checkbox"/>
<input checked="" type="radio"/>	pxgrid_multi_ise_testing Tenant ID: <input type="text" value="..."/>	<input checked="" type="radio"/> ISE-235 (Configured)		Test <input type="checkbox"/>
<input type="radio"/>	test-empty-app-instance Tenant ID: <input type="text" value="..."/>	<input type="radio"/> Ise-234-1		Test <input type="checkbox"/>

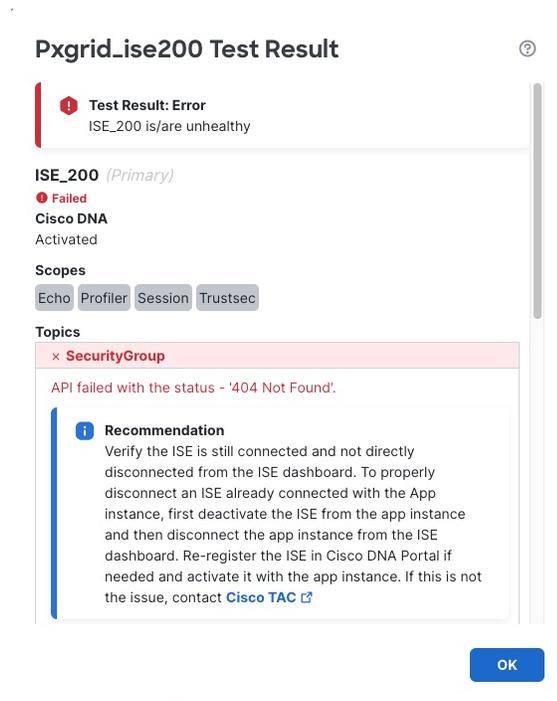
The following table has more information about the numbered areas in the figure.

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.



The following figure shows an example error result.



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](#).

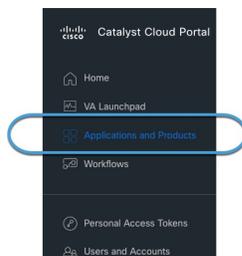
403 – Forbidden

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.

The screenshot shows the Catalyst Cloud Portal interface. The 'Products' tab is selected. On the left, there are filters for 'Products Type' and 'Registration Status'. The 'Registration Status' filter is set to 'Suspended'. The main content area shows a table with one product listed: 'ISE-docs' with a status of 'Suspended' (indicated by a red triangle icon). The 'Registration Status' column for this product is circled in blue. Above the table, there are warning messages and a search bar.

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](#).

404 – Not Found

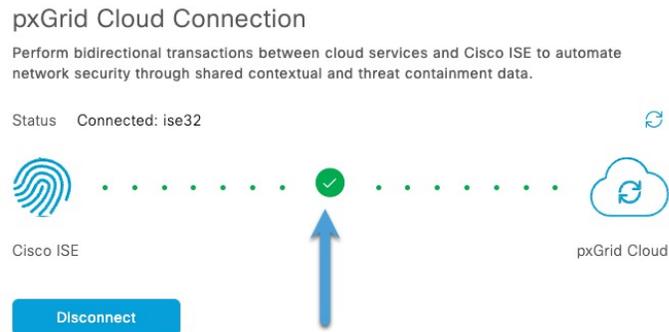
Verify the Cisco ISE server is not directly disconnected from the Cisco ISE dashboard. To properly disconnect Cisco ISE already connected with the app instance, first deactivate Cisco ISE from the app instance and then disconnect the app instance from the Cisco ISE dashboard.

408 – Request Timeout

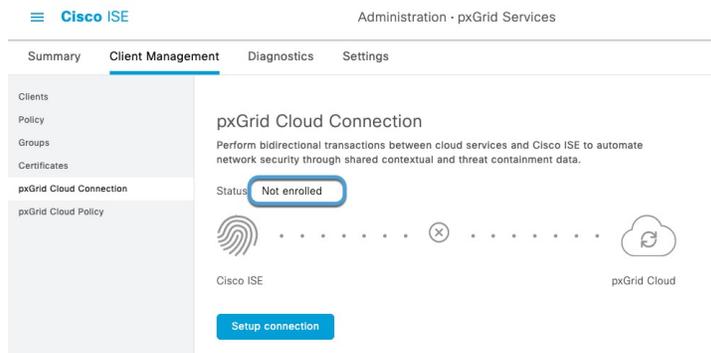
General connectivity

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.



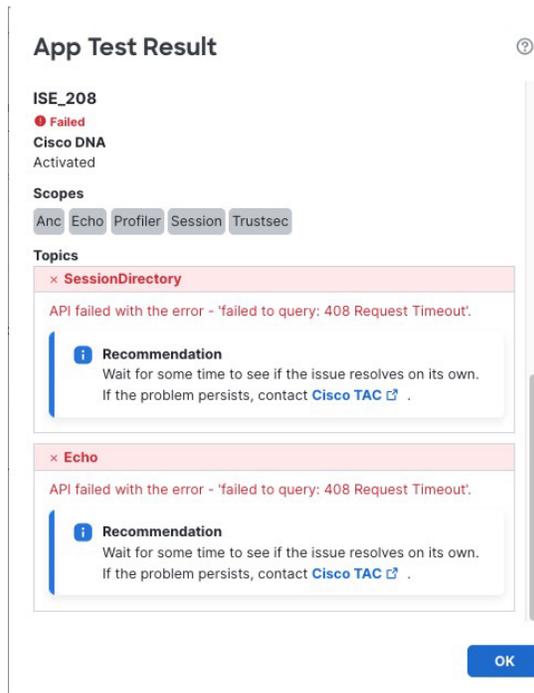
The following figure shows an example of a system that is not enrolled (meaning, not connected.)



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*.

Troubleshoot the pxGrid Cloud identity source

These topics describe troubleshooting the pxGrid Cloud identity source.

Related Topics

[Primary device cannot be processed](#)

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 screenshot shows the 'Configure Identity Sources' page in the Cisco ISE management console. The 'Service Type' is set to 'Identity Services Engine (pxGrid Cloud)'. A red error message is displayed: 'Error occurred: primary device cannot be processed'. Below the error, the status is 'Error'. The settings include 'Subscribe To' with 'Session Directory Topic' and 'SXP Topic' checked, and 'ISE Network Filter' set to 'ex. 10.89.31.0/24'. Under 'Application Instances', a table shows one instance with 'Selected' checked, 'Name' 'sl-pxgrid-2', and 'Activated ISE' checked.

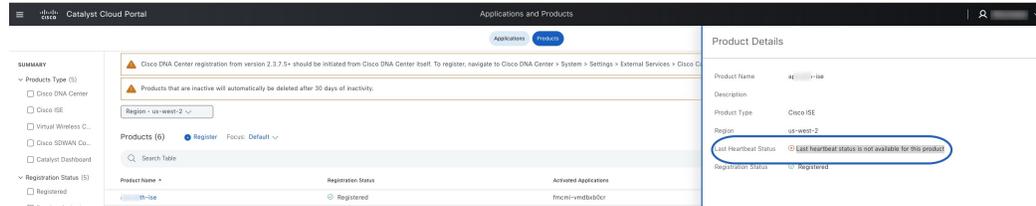
Selected	Name	Activated ISE
<input checked="" type="checkbox"/>	sl-pxgrid-2 Tenant ID: Jagan-US-QE	<input checked="" type="checkbox"/>

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](#).

Create dynamic attributes filters

Dynamic attributes filters that you define using the Dynamic Attributes Connector are exposed in the Security Cloud Control 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 AWS, Azure, Azure Service Tags, Cisco Multicloud Defense, Generic Text, GitHub, Google Cloud, and Outlook 365, pxGrid Cloud identity source, Tenable, vCenter, Webex, and Zoom). These types of cloud objects provide their own IP addresses.

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

Before you begin

[Create a connector](#)

Procedure

- Step 1** Log in to Security Cloud Control.
- Step 2** Click **Firewall**.
- Step 3** Click **Administration** > **Dynamic Attributes Connector** > **Dynamic Attributes Filters**.
- Step 4** 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 5 Enter the following information.

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

Step 6 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 7 Click **Show Preview** to display a list of networks or IP addresses returned by your query.

Step 8 When you're finished, click **Save**.

Step 9 (Optional.) Verify the dynamic object in the Security Cloud Control.

- Log in to the Security Cloud Control.
- Click **Policies > Firewall Threat Defense**.
- Click **Objects > Object Management > 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](#).



Note You cannot create dynamic attributes filters for AWS, Azure, Azure Service Tags, Cisco Multicloud Defense, Generic Text, GitHub, Google Cloud, and Outlook 365, pxGrid Cloud identity source, Tenable, vCenter, Webex, and Zoom). These types of cloud objects provide their own IP addresses.

Procedure

- Step 1** Log in to Security Cloud Control as a user with the Super Admin role.
- Step 2** Click **Firewall**.
- Step 3** Click **Policies > Firewall Threat Defense > Access Control heading > Access Control**.
- Step 4** Click **Edit** (✎) next to an access control policy.
- Step 5** Click **Add Rule**.
- Step 6** Click the **Dynamic Attributes** tab.
- Step 7** In the Available Attributes section, from the list, click **Dynamic Objects**.

The following figure shows an example.

The screenshot shows the 'Add Rule' configuration interface. At the top, there are fields for 'Name', 'Enabled' (checked), and 'Insert' (set to 'into Mandatory'). Below that, 'Action' is set to 'Allow' and 'Time Range' is 'None'. A navigation bar includes tabs for 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Ports', 'URLs', 'Dynamic Attributes' (selected), 'Inspection', 'Logging', and 'Comments'. The main area is divided into three sections: 'Available Attributes' with a search bar and a list containing 'Dynamic Objects' and 'FinanceNetwork'; 'Selected Source Attributes (0)' with a search bar and 'any' listed; and 'Selected Destination Attributes (0)' with a search bar and 'any' listed. 'Add to Source' and 'Add to Destination' buttons are positioned between the available and selected sections. At the bottom right, there are 'Cancel' and 'Add' buttons.

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

- Step 8** Add the desired object to source or destination attributes.

Step 9 Add other conditions to the rule if desired.

What to do next

See [Dynamic attributes rule conditions](#).

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.
- Delete the pxGrid Cloud identity source from the Security Cloud Control.
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](#)

[Delete the pxGrid Cloud identity source](#)

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.

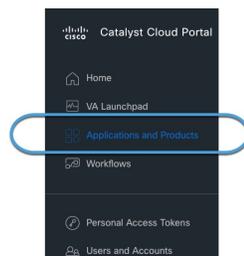
Before you begin

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

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:

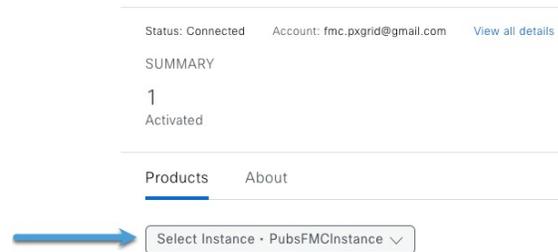


Step 3 Click **Applications**.

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**.

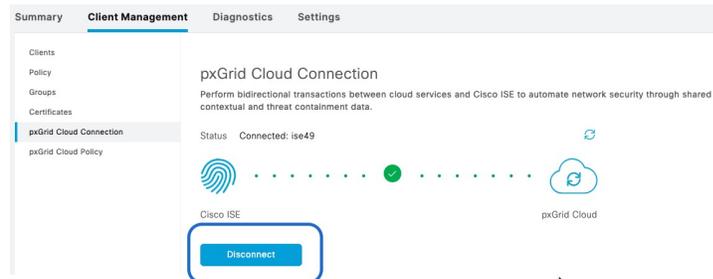
Step 7 Wait until the product is removed.

You can click **Refresh** (↻) 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:

Deactivate the pxGrid Cloud app instance

pxGrid ⓘ

Enable pxGrid Cloud ⓘ

To enable pxGrid Cloud application, please go to the [Integration Catalog](#).

Cisco DNA Portal account	Status
s...s	<input checked="" type="checkbox"/> Connected
ISE deployment name	Registered region
ISE_3.4	us-west-2
Description	Mode
--	Active

Deregister

Step 10 To verify the app instance is deactivated in Security Cloud Control:

- Log in to Security Cloud Control.
- Click **Policies > Threat Defense > Integration > Other Integrations > Identity > Identity Sources**
- Click **Identity Services Engine (pxGrid Cloud)**.
- Verify that **Not Activated** is displayed in the Activated ISE column.

Example:

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

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

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

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

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](#).
 - ISE 3.4 and later: [Create an app instance, on page 8](#).
- To completely remove the identity source, see [Delete the pxGrid Cloud identity source](#).

Delete the pxGrid Cloud identity source

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

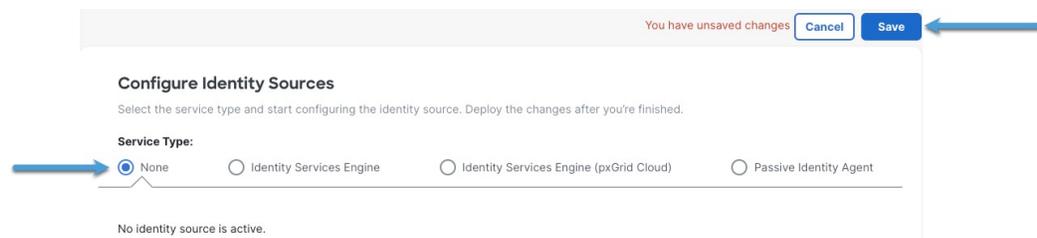
Before you begin

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

Procedure

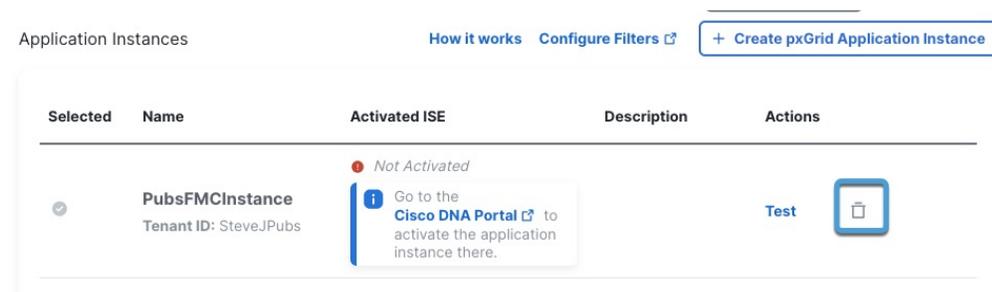
- Step 1** Log in to Security Cloud Control as a user with the Super Admin role.
- Step 2** Click **Policies > Threat Defense > Integration > Other Integrations > Identity > Identity Sources**
- Step 3** Click **Identity Services Engine (pxGrid Cloud)**.
- Step 4** For Service Type, click **None**.

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:



- Step 9** You are required to confirm the action.

Delete the pxGrid Cloud identity source