



User Control with the pxGrid Cloud Identity Source

The following topics discuss how to configure and use the pxGrid Cloud Identity Source.

- [About the pxGrid Cloud Identity Source, on page 1](#)
- [How to Configure a pxGrid Cloud Identity Source, on page 3](#)
- [Enable pxGrid Cloud Service in Cisco ISE, on page 6](#)
- [Register Cisco ISE with the Catalyst Cloud Portal, on page 6](#)
- [Register the pxGrid Cloud Connection with Cisco ISE, on page 9](#)
- [Create and Subscribe to the Firewall Management Center Application, on page 10](#)
- [Create a pxGrid Cloud Identity Source, on page 11](#)
- [Configure the pxGrid Cloud Identity Source, on page 15](#)
- [About the Cisco Identity Controller Dashboard, on page 16](#)
- [Create Dynamic Attributes Filters Using the Cisco Identity Controller, on page 17](#)
- [Create Access Control Rules Using Dynamic Attributes Filters, on page 19](#)
- [History for the pxGrid Cloud Identity Source, on page 21](#)

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 Cisco 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

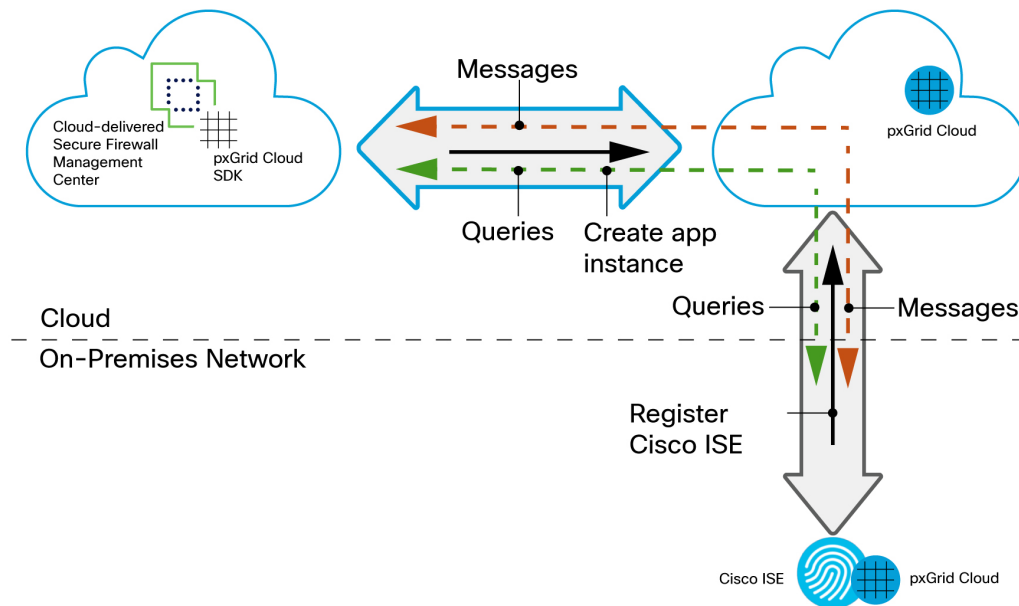
Limitations of the pxGrid Cloud Identity Source

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

- pxGrid Cloud supports only the `us-west-2` region.

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.

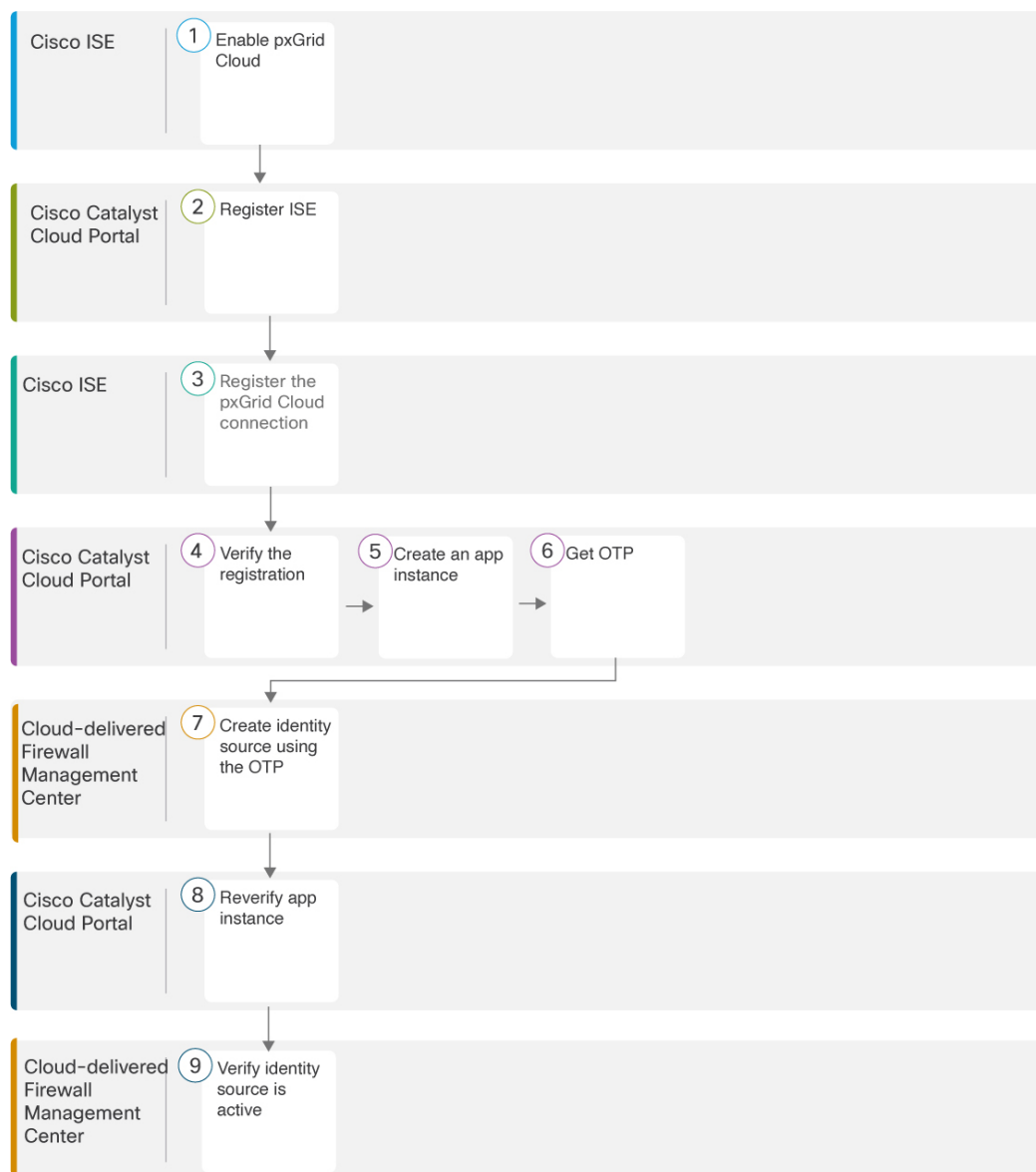
3. In pxGrid Cloud, create an "app instance" that generates an OTP for you to use in the Cloud-Delivered Firewall Management Center to authenticate the two with each other.
4. After completing all the preceding tasks, the Cloud-Delivered Firewall Management Center (which includes the pxGrid Cloud SDK) can query Cisco ISE using pxGrid Cloud and retrieve sessions containing user information.
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.

How to Configure a pxGrid Cloud Identity Source

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

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.



- 1 [Enable pxGrid Cloud Service in Cisco ISE, on page 6](#)
- 2 [Register Cisco ISE with the Catalyst Cloud Portal, on page 6](#)
- 3 [Register the pxGrid Cloud Connection with Cisco ISE, on page 9](#)
- 4 [Create and Subscribe to the Firewall Management Center Application, on page 10](#)
- 5 [Create the Identity Source, on page 12](#)
- 6 [Verify It's Working, on page 14](#)

Table 1: Configure a pxGrid cloud identity source

1	Cisco ISE	<p>Enable the 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 pxGrid Cloud Service in Cisco ISE, on page 6.</p>
2	Catalyst Cloud Portal	<p>Register Cisco ISE in the Catalyst Cloud Portal and authenticate communication between Cisco ISE and the Catalyst Cloud Portal.</p> <p>For more information, see Register Cisco ISE with the Catalyst Cloud Portal, on page 6.</p>
3 4	Cisco ISE, Cisco DNA Portal	<p>Register the pxGrid Cloud with Cisco ISE and verify the registration.</p> <p>For more information, see Register the pxGrid Cloud Connection with Cisco ISE, on page 9.</p>
5 6	Catalyst Cloud Portal, Cloud-Delivered Firewall Management Center	<p>Create an application instance in the Catalyst Cloud Portal and get the one-time password (OTP).</p> <p>The application instance enables the Cloud-Delivered Firewall Management Center to authenticate with Cisco ISE using the pxGrid Cloud service.</p> <p>The OTP, required for the next step, expires in 60 minutes.</p>
7	Cloud-Delivered Firewall Management Center	<p>Create the pxGrid cloud identity source using the OTP you got in the previous step.</p> <p>Linking the app 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, on page 12.</p>
8	Catalyst Cloud Portal	<p>Reverify the application instance.</p> <p>Activate the App Instance, on page 13.</p>
9	Cloud-Delivered Firewall Management Center	<p>Verify the identity source is active.</p> <p>Verify It's Working, on page 14.</p>

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

- 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 Using the Cisco Identity Controller, on page 17](#).


- 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 pxGrid Cloud Service in Cisco ISE](#), on page 6

Enable 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 Cisco pxGrid Cloud. Ensure that the **Trust for Authentication of Cisco Services** option is enabled for this root CA certificate. To enable **Trust for Authentication of Cisco Services**, 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.

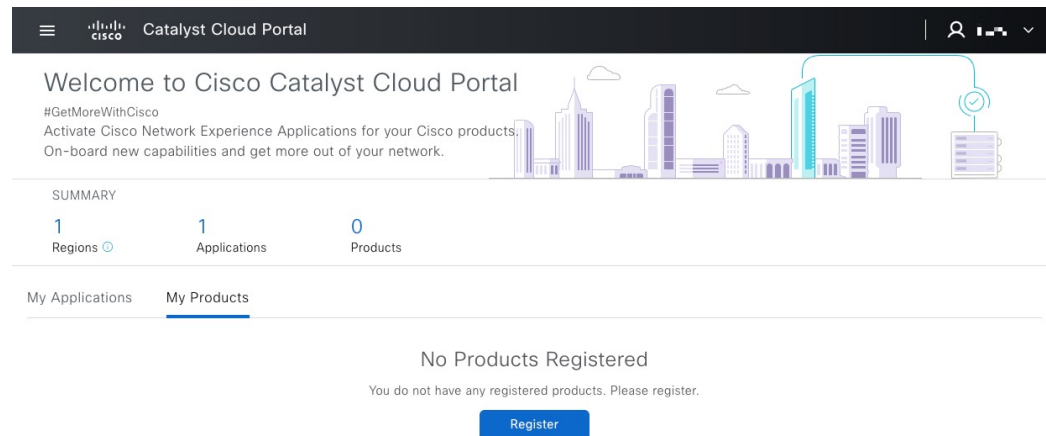
Also refer to [Register Cisco ISE](#) in the *pxGrid Cloud Solution Guide*.

Procedure

-
- Step 1** Log in to the [Cisco Cloud Catalyst Portal](#).
- Step 2** If prompted, choose an account to use.

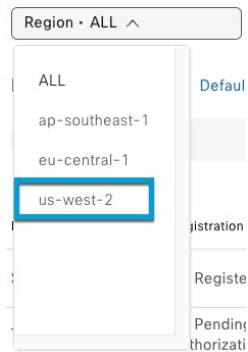
Step 3 On the Welcome page, click the **My Products** tab.

The following figure shows an example.



Step 4 Click **Register**.

Step 5 From the **Region** list, click **us-west-2**, as the following figure shows.



Note

us-west-2 is the only supported region at this time.

Step 6 Click **Register**.

The following figure shows a sample registration page.

Register Cisco ISE with the Catalyst Cloud Portal

Register Product

Host Name/IP
192.0.2.100

Product Name*
MyISE

Type*
Cisco ISE

Description

Cancel Register

Summary

Products Type (5)

- ☐ Cisco DNA Center
- ☐ Cisco ISE
- ☐ Virtual Wireless C...
- ☐ Cisco SDWAN Co...
- ☐ Catalyst Dashboard

Registration Status (5)

- ☐ Registered
- ☐ Pending Authoriza...
- ☐ Suspended
- ☐ Deleting
- ☐ Delete Failed

Region: us-west-2

Products (1) Register Focus: Default

Search Table


Product Name	Registration Status	Activated Appli
ISE-docs	Suspended	

1 Record(s)

Step 7 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 8 Click **Register**.**Step 9** 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

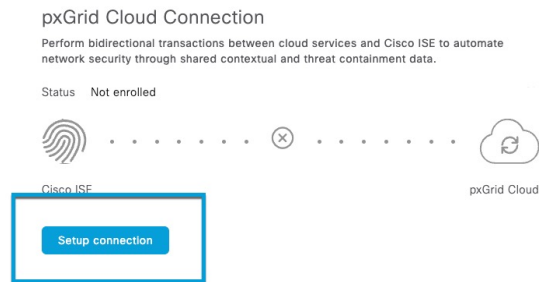
This task discusses how to register the pxGrid Cloud connection with Cisco ISE, which enables pxGrid Cloud to send user data to the pxGrid cloud identity source in Cisco Security Cloud Control.

Before you begin

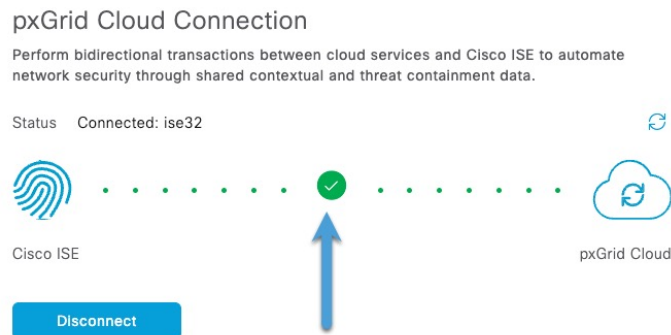
Complete the tasks discussed in [Register Cisco ISE with the Catalyst Cloud Portal](#), on page 6.

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.
- 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.
 - 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:
 - a) Log in to the Catalyst Cloud Portal.
 - b) Click the **Products** tab.

- c) Click **Refresh** as the following figure shows.



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

What to do next

Continue with [Create and Subscribe to the Firewall Management Center Application, on page 10](#).

Create and Subscribe to the Firewall Management Center Application

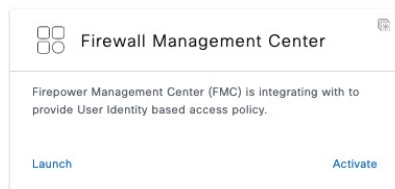
This topic discusses how to register Cisco ISE with the pxGrid cloud identity source and activate your Firewall Management Center application with the Cisco ISE product. You can subscribe to ISE's Session Directory subscriptions and enable the Cloud-Delivered Firewall Management Center to get user data for user control.

Before you begin

You must have already performed this task: [Register the pxGrid Cloud Connection with Cisco ISE, on page 9](#).

Procedure

- Step 1** Log in to the [Cisco Catalyst Cloud Portal](#).
- Step 2** Click **Applications**.
- Step 3** Click **Firewall Management Center**, then click **Activate** (or **Manage**).
The following figure shows an example.



- Step 4** Accept the agreement and click **Subscribe**.
After subscribing, you must copy the provided OTP to the clipboard and use it in 60 minutes or less to complete the next step in this process.

What to do next

[Create a pxGrid Cloud Identity Source, on page 11](#)

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 Cisco 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](#)

[Verify It's Working, on page 14](#)

Create an App Instance

This task is one of several tasks you have to 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

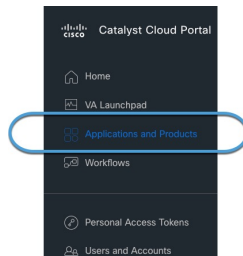
Complete all of the following tasks first:

- [Enable pxGrid Cloud Service in Cisco ISE, on page 6](#)
- [Register Cisco ISE with the Catalyst Cloud Portal, on page 6](#)
- [Register the pxGrid Cloud Connection with Cisco ISE, on page 9](#)
- [Create and Subscribe to the Firewall Management Center Application, on page 10](#)

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

Step 4 Click **Add**.

Step 5 Click **Create a New One**.

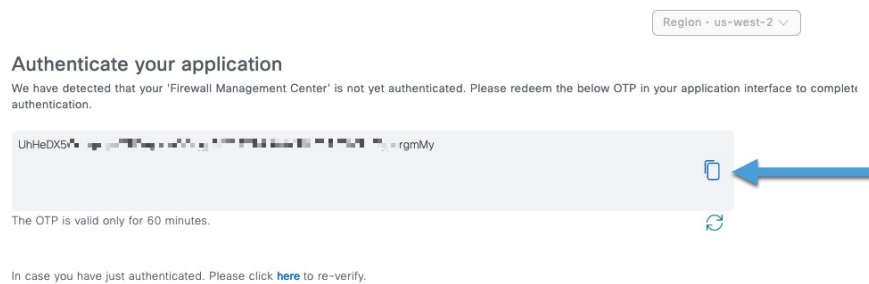
The following figure shows an example.

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



Step 7 Copy the OTP to a text file; it expires in 60 minutes.

Step 8 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 Cloud-Delivered Firewall Management Center.

Before you begin

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

Procedure

Step 1 Log in to Cisco Security Cloud Control as a user with the Super Admin role.

Step 2 Click **Policies > Threat Defense > Integration > Other Integrations > Identity Sources**

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

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

The following figure shows an example.

Create pxGrid App Instance

Name *

MypxGridCloud

Description

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

OTP Enables you to set up your pxGrid Tenant

Cancel Save

Step 5 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
OTP (One-Time Password)	Enter the OTP you obtained in the preceding steps.

Step 6 Click **Create**.

Step 7 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 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.

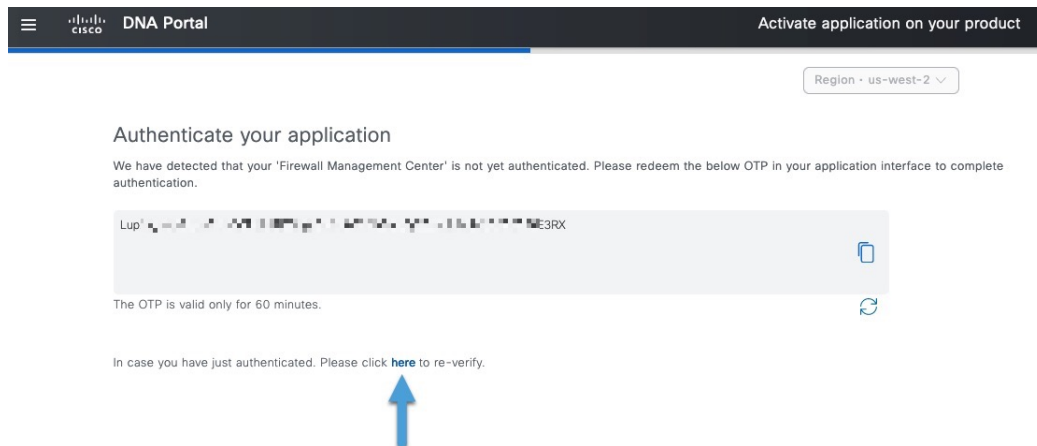
Before you begin

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

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**.
- Step 5** Click the name of the Cisco ISE product and click **Next**.
- Step 6** Select the check box next to each scope. The following figure shows an example.

Configure Access Control

Choose the functional capabilities and API Access control to be allowed for application "Firewall Management Center" on this products "SteveJISE2".

CAPABILITIES

☒ Select All

☒ Adaptive Network Control (ANC) configuration

☒ ISE Session directory

☒ Echo service topics used for testing

☒ 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**.
- Step 10** Continue with [Verify It's Working, on page 14](#).

Verify It's Working

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. To do that, you must log in to both Cloud-Delivered Firewall Management Center and the Catalyst Cloud Portal at the same time. You do not need to log in to Cisco ISE.

Before you begin

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

Procedure

-
- Step 1** Log in to Cisco Security Cloud Control as a user with the Super Admin role.
- Step 2** Click **Policies > Threat Defense > Integration > Other Integrations > Identity Sources**.
- Step 3** Click **Integration > Other Integrations > Identity Sources**.
- Step 4** Click **Identity Services Engine (pxGrid Cloud)**.
- Step 5** Wait a few minutes for the identity source to be activated then click **Refresh**.
- Step 6** After the identity source has been activated, click **Save**.
-

What to do next

Complete the following tasks:

- 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 Using the Cisco Identity Controller, on page 17](#).

Configure the pxGrid Cloud Identity Source

This topic discusses how to set configuration options for the pxGrid cloud identity source.

Procedure

-
- Step 1** Log in to Cisco Security Cloud Control as a user with the Super Admin role.
- Step 2** Click **Policies > Threat Defense > Integration > Other Integrations > Identity Sources**.
- Step 3** Click **Integration > Other Integrations > Identity Sources**.
- Step 4** Click **Identity Services Engine (pxGrid Cloud)**.
- Step 5** In the Settings section, set the following options:

ISE Network Filter

An optional filter you can set to restrict the data that ISE reports to the Cloud-Delivered Firewall Management Center. If you provide a network filter, ISE reports data from the networks within that filter. You can specify a filter in the following ways:

- 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.

Note

This version of the system does not support filtering using IPv6 addresses, regardless of your ISE version.

Subscribe to:

Session Directory Topic: Check this box to subscribe to user session information from the ISE server. Includes SGT and endpoint metadata.

SXP Topic: Check this box to subscribe to SXP mappings from the ISE server.

About the Cisco Identity Controller Dashboard

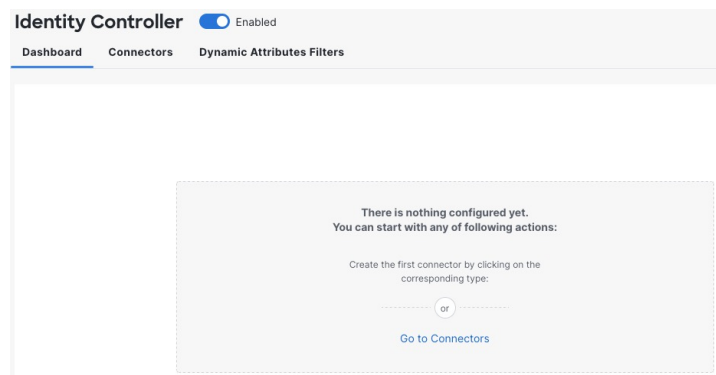
To access the Cisco Identity Controller Dashboard, log in to Cisco Security Cloud Control and click **Policies > Firewall Threat Defense > Integration > Other Integrations > Cisco Identity Controller**.

The Cisco Identity Controller Dashboard page displays the status of the pxGrid cloud identity source identity source and filters at a glance.

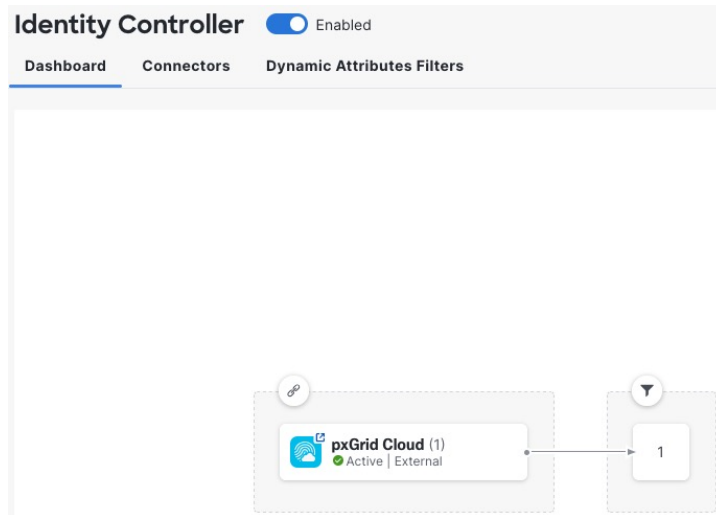
For more information about other types of dynamic attributes connectors (such as AWS and GitHub), see [About the Cisco Secure Dynamic Attributes Connector](#).


If needed, slide the control to **Enabled** and wait approximately 15 minutes for the Cisco Identity Controller to be enabled.

Following is an example of the Dashboard of an unconfigured system:



Following is an example of the Dashboard of a configured system:



Click  to view more information about all configured filters. You can also click the name of a filter to add, edit, or delete filters; or to view detailed information about them.

The dashboard enables you to configure dynamic attributes filters for either the pxGrid cloud identity source or the Cisco ISE identity source; you cannot create connectors here; instead, go to **Policies > Threat Defense > Integration > Other Integrations > Identity Sources**.

Where to Go Next

[Create Dynamic Attributes Filters Using the Cisco Identity Controller, on page 17.](#)

Create Dynamic Attributes Filters Using the Cisco Identity Controller

Dynamic attributes filters determine which dynamic objects are sent to the Cloud-Delivered Firewall Management Center for use in access control policies. We recommend setting up dynamic attributes filters for the pxGrid cloud identity source that specify clients that are in compliance with posture and for clients that are not in compliance with posture. You can create other dynamic attributes filter as you desire.

Procedure

-
- Step 1** Log in to Cisco Security Cloud Control as a user with the Super Admin role.
 - Step 2** Click **Policies > Threat Defense > Integration > Other Integrations > Identity Sources**.
 - Step 3** Click **Identity Services Engine (pxGrid Cloud)**.
 - Step 4** Click **Configure Filters** as the following figure shows.

Cloud Services Realms **Identity Sources**

Cancel Save

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)

Status: ● Active ⓘ

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

SELECT PXGRID CLOUD APPLICATION INSTANCES

Step 5 On the Cisco Identity Controller page, click the **Dynamic Attributes Filter** tab.

Step 6 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 7 Enter the following information.

Item	Description
Name	Unique name to identify the dynamic filter (as a dynamic object) in access control policy and in Manage > Policies > Threat Defense > Objects > Object Manager > External Attributes > Dynamic Object .
Connector	From the list, click pxGrid Cloud .
Query	Click Add (+).

Step 8 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. A typical key for the pxGrid Cloud Identity Source is PostureStatus .
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 9 Click **Show Preview** to display a list of networks or IP addresses returned by your query.

Step 10 When you're finished, click **Save**.

The following figure shows two sample dynamic attributes filters: one for clients whose posture is compliant and the other for clients whose posture is non-compliant.

#	Name	Connector	Query	Actions
1	posture_compliant	pxGrid Cloud (External)	PostureStatus eq 'Compliant'	⋮
2	posture_noncompliant	pxGrid Cloud (External)	PostureStatus eq 'NonCompliant'	⋮

Step 11 (Optional.) Verify the dynamic object.

- Log in to Cisco Security Cloud Control as a user with the Super Admin role.
- Click **Manage > Policies > Threat Defense > Objects > Object Manager > External Attributes > Dynamic Object**.

What to do next

[Create Access Control Rules Using Dynamic Attributes Filters](#)

Create Access Control 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).

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, vCenter, Webex, and Zoom). These types of cloud objects provide their own IP addresses.

Procedure

- Step 1** Log in to Cisco Security Cloud Control as a user with the Super Admin role.
- Step 2** Click **Firewall**.
- Step 3** Click **Administration > Dynamic Attributes Connector > Connectors**.
- Step 4** Click **Manage > Policies > Firewall Threat Defense > Access Control heading > Access Control**.
- Step 5** Click **Edit** (✎) next to an access control policy.
- Step 6** Click **Add Rule**.
- Step 7** Click the **Dynamic Attributes** tab.

Step 8 In the Available Attributes section, from the list, click **Dynamic Objects**.
The following figure shows an example.

The screenshot shows the 'Add Rule' configuration window. At the top, there are fields for 'Name', 'Enabled' (checked), 'Insert into Mandatory' (dropdown), 'Action' (set to 'Allow'), and 'Time Range' (set to 'None'). Below these are tabs for 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Ports', 'URLs', 'Dynamic Attributes' (selected), 'Inspection', 'Logging', and 'Comments'. The 'Dynamic Attributes' section is divided into 'Available Attributes' and 'Selected Attributes'. Under 'Available Attributes', there is a search bar and a list with 'Dynamic Objects' and 'FinanceNetwork'. 'Dynamic Objects' is selected. To the right of the list are 'Add to Source' and 'Add to Destination' buttons. The 'Selected Source Attributes' and 'Selected Destination Attributes' boxes are empty. At the bottom right are 'Cancel' and 'Add' buttons.

The preceding example shows a dynamic object named `APIC Dynamic Attribute` that corresponds to the dynamic attribute filter created in the Cisco Secure Dynamic Attributes Connector.

Step 9 Add the desired object to source or destination attributes.

Step 10 Add other conditions to the rule if desired.

What to do next

See [Dynamic Attributes Rule Conditions](#).

History for the pxGrid Cloud Identity Source

Feature	Minimum Secure Firewall Threat Defense Version	Details
pxGrid Cloud Identity Source.	November 8, 2024	<p>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.</p> <p>New/updated screens: Integration > Other Integrations > Identity Sources > Identity Services Engine (pxGrid Cloud).</p> <p>See: User Control with the pxGrid Cloud Identity Source</p>

