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

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.

The pxGrid cloud identity source enables the use of constantly changing dynamic objects from ISE to be used for user control 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:

  - Cisco Platform Exchange Grid (pxGrid) on cisco.com

  - 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 DNA Portal account.

  - Cisco Platform Exchange Grid (pxGrid) on cisco.com
  - 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

What to do next

See How the pxGrid Cloud Identity Source Identity Source Works, on page 2

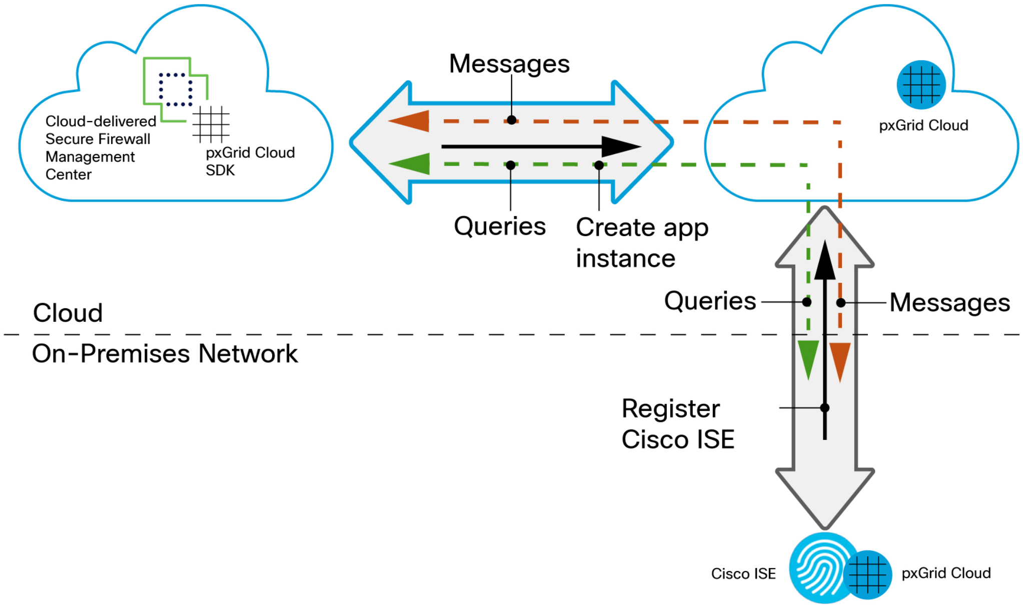
Limitations of the pxGrid Cloud Identity Source

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

- pxGrid Cloud supports only the `us-west-2` region
- You cannot use the following in access control rules: SGT, endpoint, and location IP.

How the pxGrid Cloud Identity Source 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.

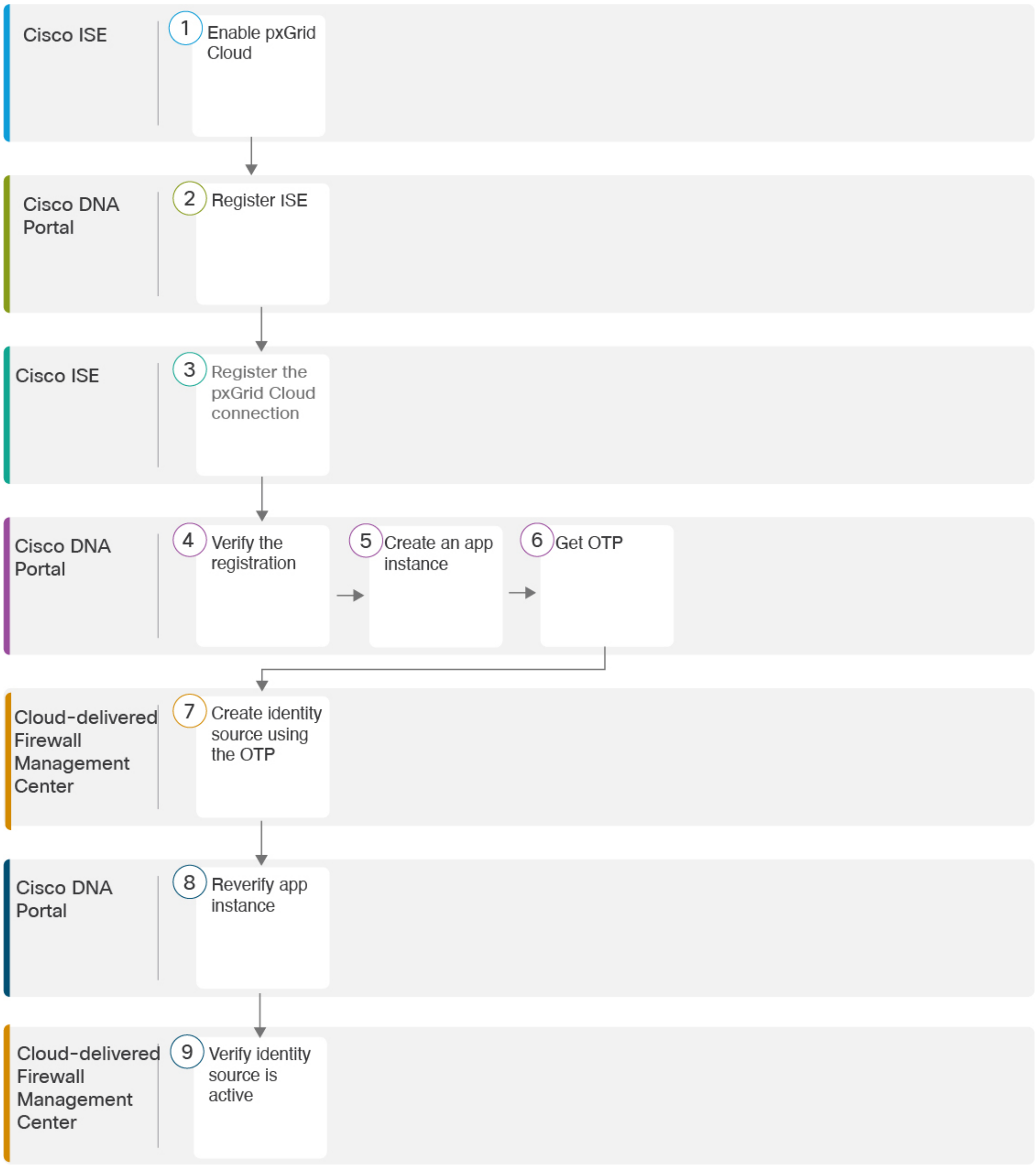
   The authentication process requires you to paste a one-time password (OTP) from pxGrid Cloud into Cisco ISE.
3. In pxGrid Cloud, create an "app instance" that generates an OTP for you to use in the cloud-delivered Firewall Management Center to authenticate the two with each other.
4. After completing all the preceding tasks, the cloud-delivered Firewall Management Center (which includes the pxGrid Cloud SDK) can query 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 DNA Portal account.

The following figure shows the steps to configure a pxGrid cloud identity source using Cisco ISE, the Cisco DNA Portal, and cloud-delivered Firewall Management Center.


Cisco ISE
1 Enable pxGrid Cloud
Cisco DNA Portal
2 Register ISE
Cisco ISE
3 Register the pxGrid Cloud connection
Cisco DNA Portal
4 Verify the registration
5 Create an app instance
6 Get OTP
Cloud-delivered Firewall Management Center
7 Create identity source using the OTP
Cisco DNA Portal
8 Reverify app instance
Cloud-delivered Firewall Management Center
9 Verify identity source is active

1 Enable pxGrid Cloud Service in Cisco ISE, on page 6

2 Register Cisco ISE with the Cisco DNA Portal, on page 6

3 Register the pxGrid Cloud Connection with Cisco ISE, on page 8

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	Enable the pxGrid Cloud in Cisco ISE. 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. For more information, see Enable pxGrid Cloud Service in Cisco ISE, on page 6.
2	Cisco DNA Portal	Register Cisco ISE in the Cisco DNA portal and authenticate communication between Cisco ISE and the Cisco DNA Portal. For more information, see Register Cisco ISE with the Cisco DNA Portal, on page 6.
3, 4	Cisco ISE, Cisco DNA 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 8.
5, 6	Cisco DNA Portal, cloud-delivered Firewall Management Center	Create an application instance in the Cisco DNA Portal and get the one-time password (OTP). The application instance enables the cloud-delivered 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	Cloud-delivered Firewall Management Center	Create the pxGrid cloud identity source using the OTP you got in the previous step. Linking the app enables the cloud-delivered Firewall Management Center to authenticate with ISE and the Cisco DNA Portal so it can receive user data from Cisco ISE. For more information, see Create the Identity Source, on page 12.
8	Cisco DNA Portal	Reverify the application instance. Activate the App Instance, on page 13.
9	Cloud-delivered Firewall Management Center	Verify the identity source is active. Verify It's Working, on page 14.

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.

- 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

See 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 Cisco DNA Portal

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

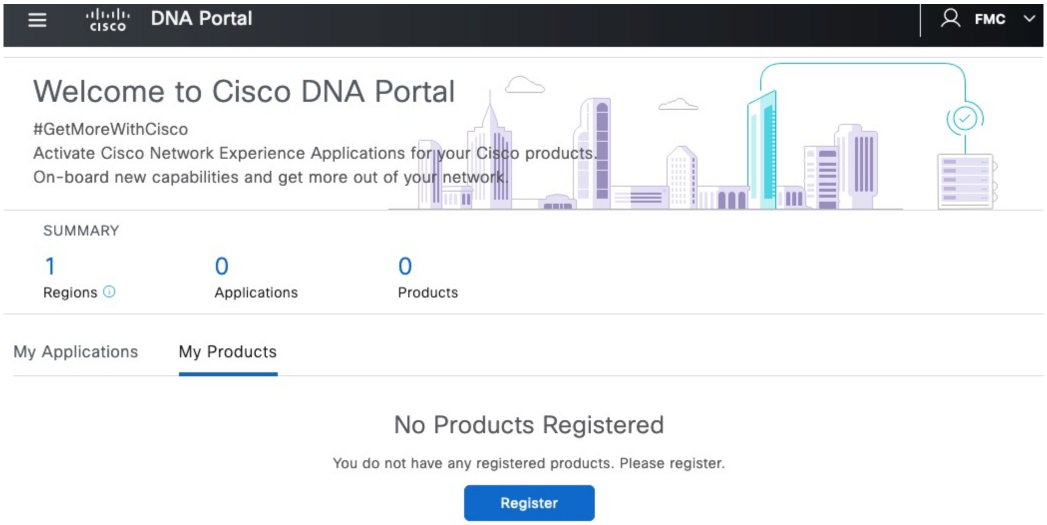
Procedure

Step 1 Log in to the Cisco DNA 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.


DNA Portal

FMC

Welcome to Cisco DNA Portal

#GetMoreWithCisco
Activate Cisco Network Experience Applications for your Cisco products.
On-board new capabilities and get more out of your network.

SUMMARY

1 Regions

0 Applications

0 Products

My Applications

My Products

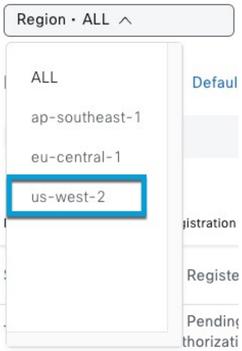
No Products Registered

You do not have any registered products. Please register.

Register

Step 4 Click **Register**.

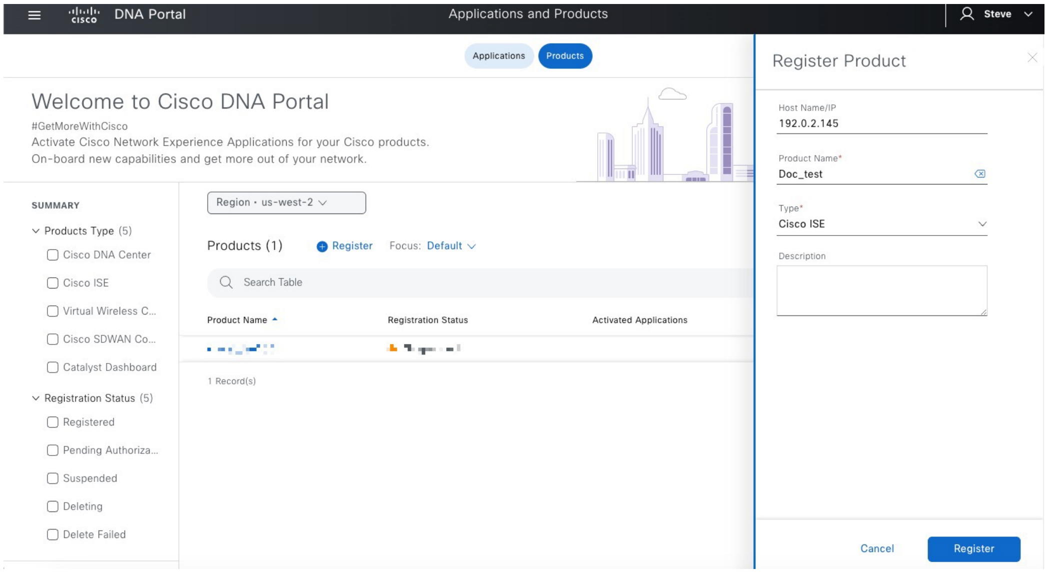
Step 5 From the **Region** list, click **us-west-2**, as the following figure shows.



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

Step 6 Click **Register**.

The following figure shows a sample registration page.



Host Name/IP: 192.0.2.145

Product Name*: Doc_test

Type*: Cisco ISE

Description:

Step 7 Enter the following information.

- **Host Name/IP**: (Optional.) Enter the ISE server's fully qualified host 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 Create and Subscribe to the Firewall Management Center Application, on page 10.

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 Enable pxGrid Cloud Service in Cisco ISE, on page 6.

Procedure

Step 1 Log in to Cisco ISE as an administrator.

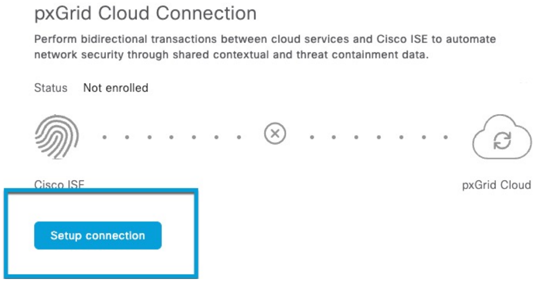
Step 2 Click ☰ > **Administration** > **pxGrid Services** > **Client Management**.

Step 3 Click the **pxGrid Cloud Policy** tab.

Step 4 Make sure all services are enabled with read/write privileges.

Step 5 In the left navigation bar, click **pxGrid Cloud Connection**.

Step 6 Click **Setup Connection** as the following figure shows.



pxGrid Cloud Connection

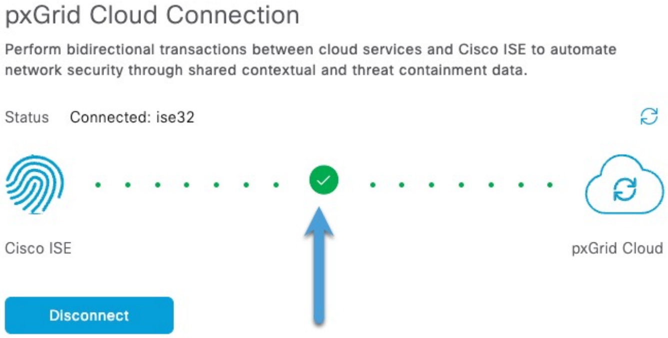
Perform bidirectional transactions between cloud services and Cisco ISE to automate network security through shared contextual and threat containment data.

Status Not enrolled

Step 7 Paste the OTP value in the provided field.

Step 8 Click **Connect**.

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



pxGrid Cloud Connection

Perform bidirectional transactions between cloud services and Cisco ISE to automate network security through shared contextual and threat containment data.

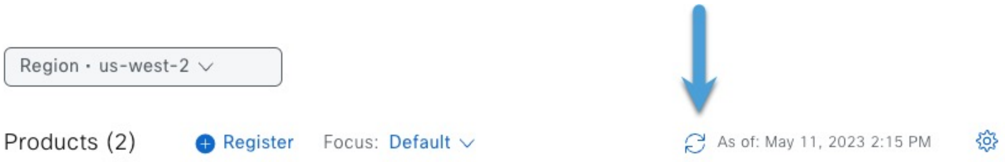
Status Connected: ise32

Step 9 Confirm the setup has been successful so far:

a) Log in to the Cisco DNA 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 an App Instance, on page 11.

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

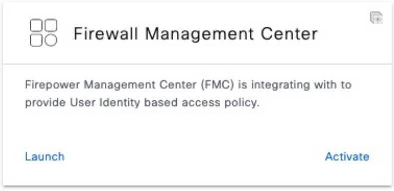
You must have already performed this task: Register Cisco ISE with the Cisco DNA Portal, on page 6.

Procedure

Step 1 Log in to the Cisco DNA Portal.

Step 2 Click **Applications**.

Step 3 Click **Firewall Management Center**, then click **Activate**.
The following figure shows an example.


Firewall Management Center

Firepower Management Center (FMC) is integrating with to provide User Identity based access policy.

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 an App Instance, 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 Cisco DNA 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 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

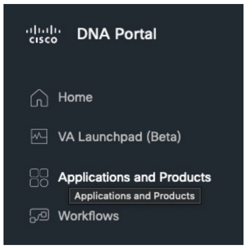
Complete all of the following tasks first:

- Enable pxGrid Cloud Service in Cisco ISE, on page 6
- Register Cisco ISE with the Cisco DNA Portal, on page 6
- Register the pxGrid Cloud Connection with Cisco ISE, on page 8
- Create and Subscribe to the Firewall Management Center Application, on page 10

Procedure

Step 1 Log in to the Cisco DNA portal.

Step 2 In the Cisco DNA Portal, go to **Applications and Products** as the following figure shows:

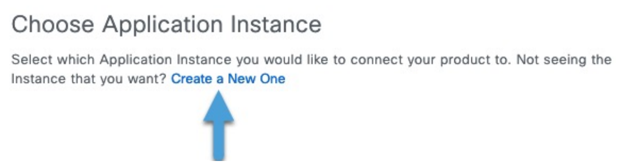


Step 3 Click **Manage** next to **Firepower Management Center**.

Step 4 Click **Add**.

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

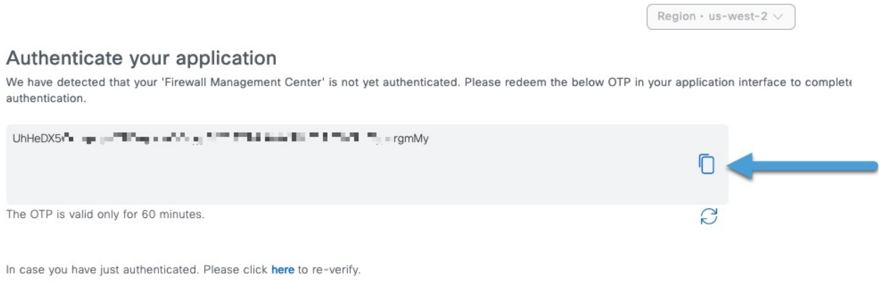
The following figure shows an example.



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:



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 complet authentication.

UhHeDX5[redacted]rgmMy

The OTP is valid only for 60 minutes.

In case you have just authenticated. Please click here to re-verify.

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

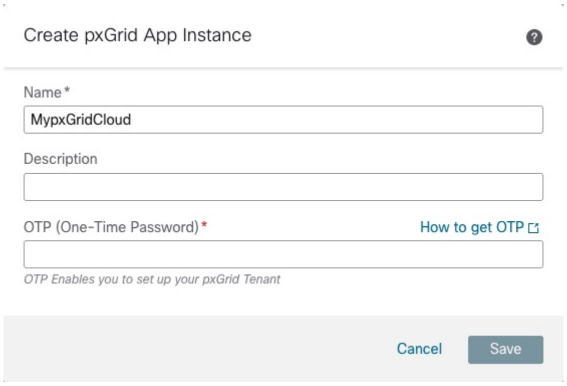
Step 1 Log in to Cisco Security Cloud Control as a user with the Super Admin role.

Step 2 Click **Tools & Settings** > **Firewall Management Center** > **Devices** > **Integrations** > **Other Integrations** > **Identity Sources**.

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

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

Step 5 The following figure shows an example.



Create pxGrid App Instance

Name *

MypxGridCloud

Description

OTP (One-Time Password) *

OTP Enables you to set up your pxGrid Tenant

Step 6 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 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.

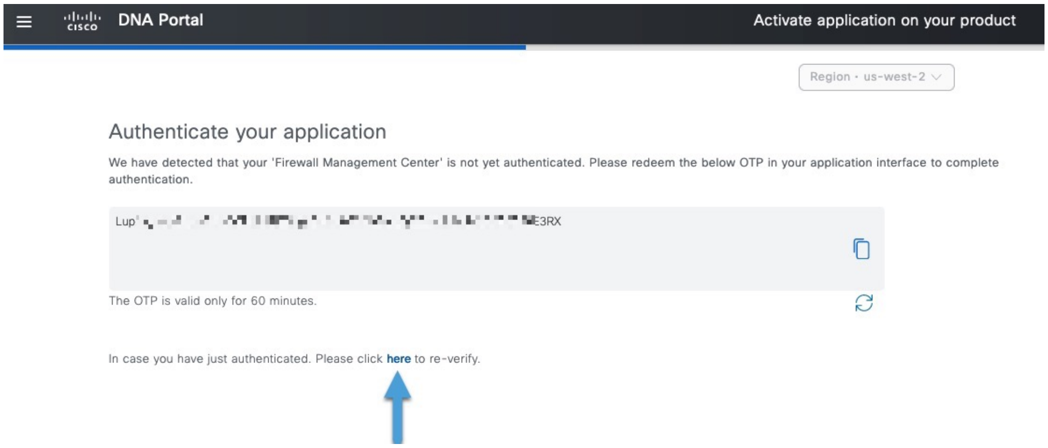
Before you begin

Complete the task discussed in Create the Identity Source, on page 12.

Procedure

Step 1 Log in to the Cisco DNA Portal.

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



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.

[redacted]

The OTP is valid only for 60 minutes.

In case you have just authenticated. Please click here to re-verify.

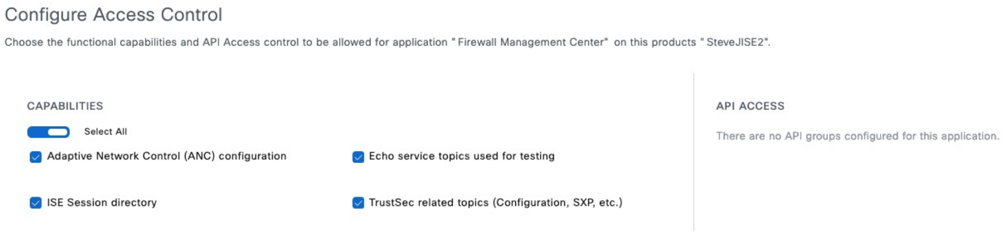
Step 3 Click the name of the application instance you just created in cloud-delivered Firewall Management Center.

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

☑ Echo service topics used for testing

☑ 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**.

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 Cisco DNA 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 Security Cloud Control.

Step 2 Wait a few minutes for the identity source to be activated then click **Refresh**.

Step 3 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.

Create Dynamic Attributes Filters for the pxGrid Cloud Identity Source

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

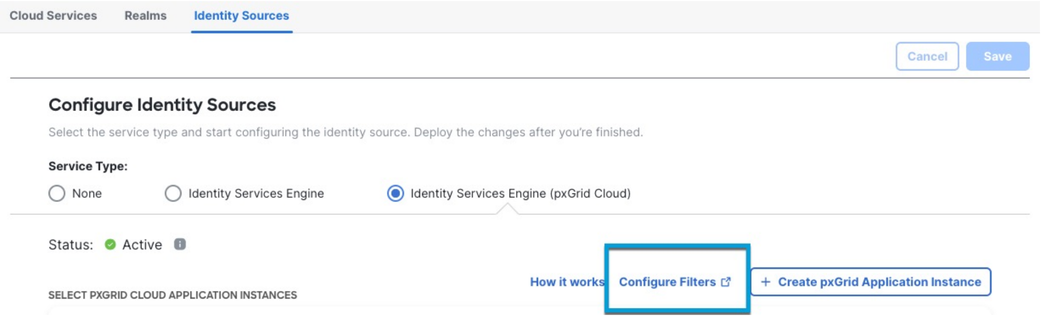
Step 1 Log in to Cisco Security Cloud Control.

Step 2 Click **Objects** > **Other FTD Objects**.

Step 3 Click **Integration** > **Other Integrations** > **Identity Sources**.

Step 4 Click **Identity Services Engine (pxGrid Cloud)**.

Step 5 Click **Configure Filters** as the following figure shows.



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

SELECT PXGRID CLOUD APPLICATION INSTANCES

Step 6 On the Dynamic Attributes Connector page, click the **Dynamic Attributes Filter** tab.

Step 7 Do any of the following:

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

Step 8 Enter the following information.

Item	Description
Name	Unique name to identify the dynamic filter (as a dynamic object) in access control policy and in the ((CDO)) Object Manager (**External Attributes** > **Dynamic Object**).
Connector	From the list, click **pxGrid Cloud**.
Query	• Add a new query: click Add icon (+⌄). • Edit or delete a query: Click **More** (⋮), then click **Edit** or **Delete** at the end of the row.

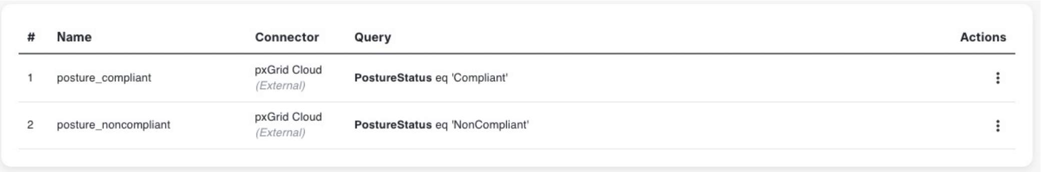
Step 9 To add or edit a query, enter the following information.

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: • **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 10 Click **Show Preview** to display a list of networks or IP addresses returned by your query.

Step 11 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 12 (Optional.) Verify the dynamic object in the Cisco Security Cloud Control.

a) Log in to Cisco Security Cloud Control.
b) Click **Policies** > **FTD Policies**.
c) Click **Objects** > **Object Management**.
d) In the left pane, click **External Attributes** > **Dynamic Object**.
The dynamic attribute query you created should be displayed as a 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 Security Cloud Control.

Step 2 Click **Policies** > **FTD Policies**.

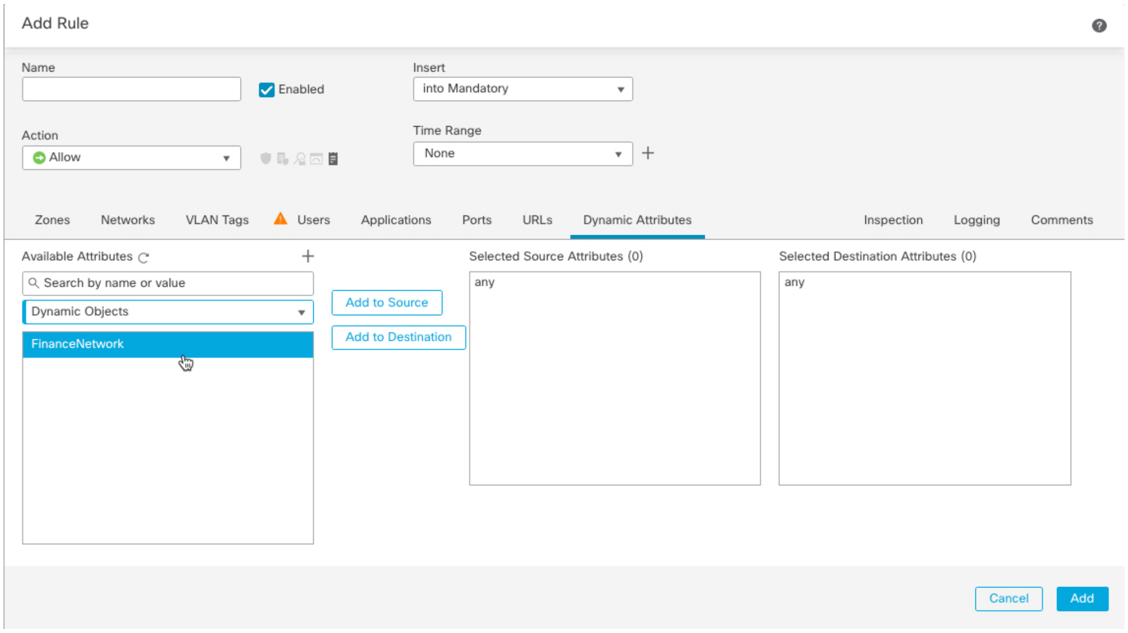
Step 3 Click **Edit** (✎) next to an access control policy.

Step 4 Click **Add Rule**.

Step 5 Click the **Dynamic Attributes** tab.

Step 6 In the Available Attributes section, from the list, click **Dynamic Objects**.

The following figure shows an example.



Add Rule

Name:

☑ Enabled

Insert: into Mandatory

Action: Allow

Time Range: None

Available Attributes: Dynamic Objects

FinanceNetwork

Selected Source Attributes (0): any

Selected Destination Attributes (0): any

The preceding example shows a dynamic object named `FinanceNetwork` that corresponds to the dynamic attribute filter created in the Cisco Secure 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

Dynamic Attributes Rule Conditions in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

History for the pxGrid Cloud Identity Source

Feature	Minimum Secure Firewall Threat Defense Version	Details
pxGrid Cloud Identity Source.	November 8, 2024	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. The pxGrid cloud identity source enables the use of constantly changing dynamic objects from ISE to be used for user control in access control policies in the cloud-delivered Firewall Management Center. New/updated screens: **Integration** > **Other Integrations** > **Identity Sources** > **Identity Services Engine (pxGrid Cloud)** See: User Control with the pxGrid Cloud Identity Source