Revised: March 27, 2024

Cisco pxGrid Cloud Solution Guide

Cisco pxGrid Cloud Overview

Cisco pxGrid Cloud is a new Cisco cloud offer that enables you to share contextual information between Cisco Identity Services Engine (Cisco ISE) and cloud-based solutions without compromising the security of your network. It provides a unified framework that enables seamless data integration between Cisco ISE and cloud-based solutions. It is secure and customizable, enabling you to share only the data that you want to share and consume only the contextual data that is relevant for your application.

Cisco ISE 3.1 patch 3 and later releases support Cisco pxGrid Cloud. Cisco and its partners and customers can develop pxGrid Cloud-based applications and register them with the pxGrid Cloud offer. These applications can use the External RESTful Services (ERS), pxGrid, and Open APIs to exchange information with Cisco ISE.

Cisco pxGrid Cloud offers the following benefits:

- Plug-and-play deployment without requiring infrastructure changes to your network.

- Cisco ISE as a single source of truth for endpoint identity by delivering consistent context exchange with on-premise and cloud partners.

- Enrichment of Software as a Service-based (SaaS-based) security analysis with real-time endpoint context from Cisco ISE.

- Threat containment by isolating endpoints from the network through actions initiated from the security SaaS solutions.

Cisco pxGrid Cloud Terminology

The following are some of the common terms that are used in the Cisco pxGrid Cloud solution and their meaning in the Cisco pxGrid Cloud environment:

- Offer: A set of capabilities packaged together and offered as a solution.

- Subscription: An instance of an offer being consumed by a tenant is a subscription.

- App: You can create and register applications for your product based on your requirements. For example, you can create an app that can retrieve the session and endpoint data from Cisco ISE.

  Applications with a cloud offering can be onboarded to Cisco pxGrid Cloud. After an application is onboarded, you can share data between your Cisco ISE deployment and the application.

Cisco pxGrid Cloud and Cisco ISE Integration Workflow

Cisco ISE customers with Advantage license can register their Cisco ISE deployment with Cisco pxGrid Cloud and use the applications listed in the offer.

To access the Cisco DNA - Cloud portal, go to https://dna.cisco.com.

To access the Cisco pxGrid Cloud portal, go to https://pxgridcloud.cisco.com.

Cisco pxGrid Cloud and Cisco ISE integration workflow includes the following steps:

To share data between your Cisco ISE deployment and a cloud application, you must do the following:

1. Onboard an app in the Cisco pxGrid Cloud portal. For information on how to onboard an app in the Cisco pxGrid Cloud portal, see the Cisco pxGrid Cloud Onboarding Guide.

Enable pxGrid Cloud Service in Cisco ISE

Before you begin

- Ensure that you install and activate the Advantage license 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.

- Ensure that port 443 is open for outbound connection from Cisco ISE to Cisco pxGrid Cloud portal. If firewall or proxy settings are configured, ensure that the following URLs are not blocked:

    - https://dna.cisco.com

    - https://pxgridcloud.cisco.com

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.

Create an Account in the Cisco DNA - Cloud Portal

Step 1 Go to https://dna.cisco.com.

If you already have a Cisco account, skip to Step 4.

Step 2 If you do not have a Cisco account, click **Create a New Account**.

Step 3 Enter the required details in the **Create Account** window and click **Register**.

A verification email is sent to the email account that you entered in the **Create Account** window. To finish signing in, check your verification mail.

Step 4 Log in to the Cisco DNA - Cloud portal with your Cisco account.

Step 5 Enter a name for your account and click **Continue**.

Step 6 Confirm your account profile details and click **Create Account**.

The Cisco DNA - Cloud portal home page is displayed.

Note If you have multiple Cisco DNA - Cloud accounts, a pop-up window listing all your associated accounts is displayed. Choose an account and click **Continue** to launch the home page.

Subscribe to an Offer

Step 1 In the Cisco DNA - Cloud portal home page, click **Subscribe to Offer**.

Step 2 In the **Set Up Your Subscription** slide-in pane, from the **Offer** drop-down list, choose **pxGrid Cloud**.

Step 3 From the **Region** drop-down list, choose **US Region**.

Note This release of Cisco pxGrid Cloud supports only the U.S. region.

Step 4 Check the General Terms check box and click **Subscribe Offer**.

The offers that you have subscribed to are displayed in the Cisco DNA - Cloud portal home page.

If you want to delete an offer, select the offer and click **Delete**.

Note • Deleting a subscription removes the access of the accounts that are logged in to that offer. Hence, the logged-in users will no longer be able to register a device or perform any operation related to that offer.

• Deleting a subscription also impacts the products that are registered for that region.

Register Cisco ISE

Before you begin

You must subscribe to an offer before registering Cisco ISE.

Step 1 Go to https://pxgridcloud.cisco.com.

Step 2 In the Cisco pxGrid Cloud portal home page, click **Register Cisco ISE**.

Step 3 In the **Register Cisco ISE** slide-in pane, enter the Cisco ISE server name and description.

An OTP is generated. This OTP is valid for 30 minutes. For more information, see Cisco pxGrid Cloud and Cisco ISE Integration, on page 6.

Enter the OTP in the **Setup Connection** window in Cisco ISE (under **Administration > pxGrid Services > Client Management > pxGrid Cloud Connection**).

Note   The pxGrid Cloud service must be enabled on one or two pxGrid nodes in the Cisco ISE deployment. For information on how to enable the pxGrid Cloud service, see Enable pxGrid Cloud Service in Cisco ISE, on page 2.

The status of the Cisco ISE instance is displayed as **Registered** in the **On-Prem Connections** window after successful registration.

App Registration Workflow

You can create and register applications (referred to as *apps* in Cisco pxGrid Cloud portal) to your product based on your requirements. For example, you can create an app that can retrieve the session and endpoint data from Cisco ISE.

These applications can use the ERS, pxGrid, and Open APIs to exchange information with Cisco ISE. For information about the supported APIs, see the Cisco pxGrid Cloud API Reference Guide.

To share data between your Cisco ISE deployment and a cloud application, you must do the following:

1. Onboard an app in the Cisco pxGrid Cloud portal. For information on how to onboard an app in the Cisco pxGrid Cloud portal, see the Cisco pxGrid Cloud Onboarding Guide.

2. Connect to an App, on page 4

3. Activate an App, on page 5

Connect to an App

Step 1 In the Cisco pxGrid Cloud portal home page, click the **Menu** icon (☰) and choose **App Store**.

Step 2 In the **App Store** window, choose the required app and click **Connect to App**.

An OTP is generated. This OTP is valid for 60 minutes.

Step 3 Navigate to the application URL and paste the OTP in the **Enter Token** field. For example, if you are connecting the DNA Spaces application, the OTP is used in DNA Spaces.

After successful authentication, the app is listed in the **My Apps** window.

Activate an App

Before you begin

You must register Cisco ISE and connect your app before activating the app.

Step 1	In the Cisco pxGrid Cloud portal home page, click the **Menu** icon (≡) and choose **App Store**.
Step 2	Click **My Apps**.
Step 3	In the **My Apps** window, choose the app and click **Activate product**.
	The **Activate App for Products** window is displayed.
	Note *Product* refers to your registered Cisco ISE server.
Step 4	Click **Let's Do it**.
Step 5	In the **Select an App** window, choose the app from the **App Name** drop-down list.
	The compatible products and supported region details are displayed below the app.
Step 6	Click **Next**.
Step 7	In the **Select Product** window, from the **Product Type** drop-down list, choose **Cisco ISE**.
Step 8	From the **Product** drop-down list, choose the Cisco ISE server.
Step 9	In the **Configure App for Product** window, set the configuration for Cisco ISE. The following scopes are available:

- **Profiler**: Cisco ISE Profiler configuration
- **RADIUS**: RADIUS authentication failures
- **Session**: Cisco ISE session directory
- **TrustSec**: Cisco ISE TrustSec related topics
- **User Defined Network**: Cisco User Defined Network related topics
- **ANC**: Adaptive Network Control configuration
- **MDM**: Mobile Device Management related topics
- **Echo**: Echo service topics used for testing

For more information about scopes, see the Cisco pxGrid Cloud API Reference Guide.

Step 10	In the **Summary** window, review your settings and click **Activate App for Products**.
	The app activation status is displayed as **Activated** in the **Product Activation** window.
Step 11	Refresh the **ISE Enrollment** window in the app.
Step 12	Select the activated Cisco ISE instance and click **Connect**.
Step 13	Click **Accept**.
	The Cisco pxGrid Cloud setup is now complete.

Cisco pxGrid Cloud and Cisco ISE Integration

To allow connectivity between a Cisco ISE deployment and Cisco pxGrid Cloud, the **pxGrid Cloud** option must be enabled on one or two pxGrid nodes in the Cisco ISE deployment. If you have configured high availability for pxGrid nodes, one of the nodes acts as the Active node and the other one will be the Standby node. The Standby node takes over when the Active node goes down.

Only the Active node establishes connection to Cisco pxGrid Cloud and handles the traffic between the Cisco ISE deployment and Cisco pxGrid Cloud. No other Cisco ISE node interacts with Cisco pxGrid Cloud.

The pxGrid Cloud agent resides in Cisco ISE and serves as the bridge between Cisco ISE and Cisco pxGrid Cloud. A pxGrid Cloud application can subscribe to a pxGrid topic. The pxGrid Cloud agent in Cisco ISE learns about this subscription from Cisco pxGrid Cloud and establishes the actual subscription to the pxGrid service in Cisco ISE. When the agent receives a notification on the pxGrid topic, it forwards the notification to Cisco pxGrid Cloud over a logical channel dedicated to the pxGrid service. The pxGrid Cloud application can invoke ERS, pxGrid, and Open APIs in the Cisco ISE deployment. The pxGrid Cloud agent proxies a REST request from Cisco pxGrid Cloud to Cisco ISE, and returns the response back to Cisco pxGrid Cloud.

Cisco ISE customers who have a pxGrid Cloud subscription can register their Cisco ISE deployment with Cisco pxGrid Cloud and use the applications listed in the offer. To do this, they must:

1. Acquire and activate the pxGrid Cloud subscription.

2. Enable the pxGrid Cloud service on one or two pxGrid nodes in the Cisco ISE deployment.

3. Register the Cisco ISE deployment with Cisco pxGrid Cloud (associating it with the subscription) and receive an authentication token.

4. Enter the authentication token in the **Setup Connection** window in Cisco ISE (under **Administration > pxGrid Services > Client Management > pxGrid Cloud Connection**).

   This activates the pxGrid Cloud agent on the Active pxGrid node and establish a connection between the Cisco ISE deployment and Cisco pxGrid Cloud.

5. Select a pxGrid Cloud application from the offer and associate it with the subscription. The application will then have access to the Cisco ISE deployment.

Connect Cisco ISE to Cisco pxGrid Cloud

After the pxGrid Cloud service is enabled, you must connect the Cisco ISE deployment to Cisco pxGrid Cloud. You must register your Cisco ISE deployment in Cisco pxGrid Cloud and generate an authentication token.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration > pxGrid Services > Client Management > pxGrid Cloud Connection**.

Step 2 Click **Setup Connection**.

Step 3 Enter the OTP in the **Setup Connection** window, and then click **Connect**.

For information on how to obtain the OTP, see Register Cisco ISE, on page 3.

The connection setup includes the following steps:

   a. **Enrollment**: A request is sent to Cisco pxGrid Cloud to enroll the Cisco ISE deployment using the authentication token. When this step is successfully completed, the pxGrid Cloud agent is started on the Active node in the Cisco ISE deployment.

b. pxGrid Connection: The pxGrid Cloud agent establishes a persistent connection to the pxGrid component running locally on the same Cisco ISE node. All pxGrid notifications from Cisco ISE are sent to the pxGrid Cloud agent using this connection.

c. Cloud Connection: The pxGrid Cloud agent establishes a persistent connection to Cisco pxGrid Cloud and sets up the logical channels. These logical channels are used to receive the ERS and pxGrid requests from Cisco pxGrid Cloud, and to send the pxGrid notifications to Cisco pxGrid Cloud.

You can view the connection setup progress in the **pxGrid Cloud Connection** window. After all these steps are completed, the status is displayed as **Connected** and the name of the active pxGrid node is displayed.

To terminate the pxGrid Cloud connection, click **Disconnect** in the **pxGrid Cloud Connection** window. This disconnects the Cisco ISE deployment from Cisco pxGrid Cloud and terminates the pxGrid Cloud agent on the Active node.

When the Cisco ISE deployment is connected to Cisco pxGrid Cloud, the pxGrid Cloud agent (called Hermes process) is listed in the output of the **show application status ise** CLI command.

Disable pxGrid Cloud Service on Cisco ISE

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

Step 2   Check the check box next to the pxGrid node and click **Edit**.

Step 3   Uncheck the **Enable pxGrid Cloud** check box.

This stops the pxGrid Cloud agent in the Cisco ISE deployment. You can re-enable the pxGrid Cloud service later when needed.

Configure a pxGrid Cloud Policy

By default, pxGrid Cloud applications are not permitted to access any pxGrid services or APIs in the Cisco ISE deployment. Access must be explicitly granted by configuring policies in Cisco ISE.

You can create a policy to specify what is allowed or denied between your Cisco ISE deployment and the pxGrid Cloud service. Authorization policies specific to each partner environment can be configured in the cloud portal. You will need the Cisco ISE Advantage license to configure a pxGrid Cloud policy.

Step 1   In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration > pxGrid Services > Client Management > pxGrid Cloud Policy**.

Step 2   In the **pxGrid Services** area, choose the required services from the list. You can enable one or more pxGrid services by clicking their names.

Step 3   In the **ERS APIs** area, enable the **ERS APIs** option to provide ERS API access to pxGrid Cloud applications.

The **ERS APIs** option is disabled here if the ERS service is disabled in Cisco ISE.

To enable this service in Cisco ISE, perform these steps:

a. In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration > System > Settings > API Settings > API Service Settings**.

b. Enable the **ERS (Read/Write)** option.

Step 4   In the **Open APIs** area, enable the **Open APIs** option to provide Open API access to pxGrid Cloud applications.

The **Open APIs** option is disabled here if the **Open API** option is disabled in Cisco ISE.

To enable this service in Cisco ISE, perform these steps:

a. In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration > System > Settings > API Settings > API Service Settings**.

b. Enable the **Open API (Read/Write)** option.

Note   By default, the pxGrid Cloud applications are granted Read Only access to the APIs (only HTTP GET operations can be performed). Enable the **Read/Write** option in the **pxGrid Cloud Policy** window if you want to allow POST, PUT, and DELETE operations as well.

Change Scopes for an App

You can change the scopes that are configured for an app based on your requirements. Ensure that the scopes that you configure for the app on the pxGrid Cloud portal matches the pxGrid Services that you choose in Cisco ISE.

Step 1   In the Cisco ISE GUI, click the **Menu** icon (≡) and choose **Administration > pxGrid Services > Client Management > pxGrid Cloud Policy**.

Step 2   In the **pxGrid Services** area, choose the required services from the list. You can enable one or more pxGrid services by clicking their names.

Step 3   In the Cisco pxGrid Cloud portal home page, click the **Menu** icon (≡) and choose **App Store**.

Step 4   Click **My Apps**.

Step 5   In the **Select an App** window, choose the app from the **App Name** drop-down list.

Step 6   In the **Select Product** window, from the **Product Type** drop-down list, choose **Cisco ISE**.

Step 7   From the **Product** drop-down list, choose the Cisco ISE server.

Step 8   In the **Configure App for Product** window, set the configuration for Cisco ISE. The following scopes are available:

- **Profiler**: Cisco ISE Profiler configuration

- **RADIUS**: RADIUS authentication failures

- **Session**: Cisco ISE session directory

- **TrustSec**: Cisco ISE TrustSec related topics

- **User Defined Network**: Cisco User Defined Network related topics

- **ANC**: Adaptive Network Control configuration

- **MDM**: Mobile Device Management related topics

• **Echo**: Echo service topics used for testing

For more information about scopes, see the Cisco pxGrid Cloud API Reference Guide.

Cisco pxGrid Cloud Clients

To view the pxGrid Cloud applications, choose **Administration > pxGrid Services > Client Management > Clients > pxGrid Cloud Clients**.

The pxGrid Cloud offer provides a collection of registered applications that pxGrid Cloud subscribers can select and use. For example, if a subscriber registers Cisco ISE deployment in Cisco pxGrid Cloud and uses two applications, those two applications are listed in the **pxGrid Cloud Clients** tab. Note that you can only view the pxGrid Cloud applications in this tab. You cannot make any changes from this tab.

You can view the total number of pxGrid Cloud applications that are currently running on this deployment in the **Total Clients** pane in the **Summary** window (under **Administration > pxGrid Services > Summary**).

High Availability for pxGrid Nodes

The pxGrid Cloud service can be enabled on two nodes to enable high availability. When the Cisco ISE deployment is successfully connected to Cisco pxGrid Cloud, one of the nodes is selected as the Active node and the pxGrid Cloud agent is started on that node. If the Active node is down, or if the network connectivity to the Active node is lost, the Standby node is moved to the Active state. The pxGrid Cloud agent is started on that node and the connectivity to Cisco pxGrid Cloud is established again.

Note The failover process might take around 30 seconds.

Table 1: Events that Trigger High-Availability Response

Event	High-Availability Response
pxGrid Cloud service disabled on Active node	Standby node immediately becomes the Active node.
Active node restarted because of a crash or user-initiated sequence	Standby node becomes Active. When the restarted node comes up, this node becomes the Standby node and monitors the Active node.
Upgrade deployment (or standalone Cisco ISE node) with one pxGrid node	After the upgrade, the node functions as the Active node.
Upgrade deployment with Active and Standby nodes	When the Standby node is upgraded, it acts as Standby node post upgrade and continues to monitor the Active node. When the Active node is upgraded, the Standby node takes over as the Active node. When the upgraded node comes up, it becomes Standby and monitors the Active node.
Network issue occurs between the Active and Standby nodes	Both the nodes operate in Active mode. When this occurs, the names of both the nodes are displayed in the **pxGrid Cloud Connection** window. After the connectivity between the nodes is restored, one of the nodes is selected as the Active node and the other node acts as the Standby node.

Add a new pxGrid node with pxGrid Cloud service enabled to the deployment	The new node initially acts as the Active node. After the node is fully synchronized and able to communicate with its peer, one of the nodes is selected as the Active node.

The following configuration changes restart the pxGrid Cloud agent:

- Replacing the pxGrid system certificate

- Replacing the Admin system certificate

- Enabling or disabling the **Trust for authentication within ISE** or **Trust for authentication of Cisco Services** option for any trust certificate

- Changing Cisco ISE proxy settings

- Enabling or disabling the ERS service for Cisco pxGrid Cloud

- Enabling or disabling any pxGrid service in the **pxGrid Cloud Policy** window

Log Files Specific to pxGrid Cloud Service

You can check the following log files in the active pxGrid node if there is any issue related to pxGrid Cloud service:

Log File	Contents	Where to find
pxcloud.log	- pxGrid Cloud service configuration changes - pxGrid Cloud service connection status - High-availability status (selection of Active node, detection of failures, and so on)	Cisco ISE nodes where the pxGrid Cloud service is enabled
hermes.log	All activities logged by the pxGrid Cloud agent including: - Cisco ISE and Cisco pxGrid Cloud connection status - pxGrid topic subscription status - Handling pxGrid and ERS REST requests from Cisco pxGrid Cloud - Configuration changes made in Cisco ISE	Active pxGrid node **Note** If the Standby node was previously Active, hermes.log is retained in that node, but the log file is not updated after it moves to the Standby state.

These log files are included in the Cisco ISE support bundle when the **Include Debug Logs** option is enabled. To download these logs, choose **Operations > Troubleshoot > Download Logs > Debug Logs > Application Logs**.

Configure Debug Log Level for pxGrid Cloud Service

To configure the level of detail included in the pxcloud.log and hermes.log files:

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration**.

Step 2 Click the pxGrid node.

Step 3 Click **pxGrid Cloud**.

Step 4 Choose one of the following options from the **Log Level** drop-down list:

- **Trace**

- **Debug**

- **Info**

- **Warn**

- **Error**

- **Fatal**

The selected log level applies to both pxcloud.log and hermes.log files.

Note   Hermes.log supports only the **Debug**, **Info**, **Warn**, and **Error** log levels. Hence, if you choose **Trace**, the log level is set as **Debug** for hermes.log. If you choose **Fatal**, the log level is set as **Error** for hermes.log.

Support Information

For any issue with deploying or registering Cisco ISE with pxGrid Cloud, contact Cisco Technical Assistance Center.

For any issue with an application on pxGrid Cloud, contact Cisco Technical Assistance Center.