Cisco pxGrid

Cisco pxGrid Node

You can use Cisco pxGrid to share the context-sensitive information from Cisco ISE session directory with other network systems such as Cisco ISE ecosystem, partner systems, and other Cisco platforms. The pxGrid framework can also be used to exchange policy and configuration data between nodes, such as sharing tags and policy objects between Cisco ISE and third-party vendors, and for other information exchanges. Cisco pxGrid also allows third-party systems to invoke adaptive network control actions (ANC) to quarantine users or devices or both in response to a network or security event. Cisco TrustSec information, such as tag definition, value, and description can be passed from Cisco ISE through the Cisco TrustSec topic to other networks. The endpoint profiles with Fully Qualified Names (FQNs) can be passed from Cisco ISE to other networks through an endpoint profile meta topic. Cisco pxGrid also supports bulk download of tags and endpoint profiles.

You can publish and subscribe to SXP bindings (IP-SGT mappings) through Cisco pxGrid. For more information about SXP bindings, see e .

In a high-availability configuration, Cisco pxGrid servers replicate information between the nodes through the PAN. When the PAN goes down, the Cisco pxGrid server stops handling the client registration and subscription. You need to manually promote the PAN for the Cisco pxGrid server to become active. You can check the **Cisco pxGrid services** window (**Administration** > **pxGrid Services**) to verify whether a Cisco pxGrid node is currently in active or standby state.

On the active Cisco node that has the pxGrid persona, these processes are displayed as **Running**. On the standby Cisco pxGrid node, they are displayed as **Standby**. If the active pxGrid node goes down, the standby pxGrid node detects this, and starts the four pxGrid processes. Within a few minutes, these processes show as **Running**, and the standby node becomes the active node. You can verify whether the Cisco pxGrid service is in standby on that node by running the CLI command **show logging application pxgrid/pxgrid.state**.

For Extensible Messaging and Presence Protocol clients, Cisco pxGrid nodes work in active-standby high availability mode which means that the Cisco pxGrid Service is in **Running** state on the active node and in **Disabled** state on the standby node.

Note In a High Availability Cisco ISE deployment, the pxGrid persona nodes that work in an active-standby setup show that the pxGrid Service is in **running** state on the active node and in **standby** state on the standby node.

To verify the status of pxGrid services on a Cisco ISE node, use the following CLI command:

```
show logging application pxgrid/pxgrid.state
```

After the automatic failover to the secondary Cisco pxGrid node is initiated, if the original primary Cisco pxGrid node is brought back into the network, the original primary Cisco pxGrid node continues to have the secondary role and is not promoted back to the primary role unless the current primary node goes down.

Note At times, the original primary Cisco pxGrid node might be automatically promoted back to the primary role.

In a high-availability deployment, when the primary Cisco pxGrid node goes down, it might take around three to five minutes to switchover to the secondary Cisco pxGrid node. We recommend that the client waits for the switchover to complete, before clearing the cache data just in case the primary Cisco pxGrid node fails.

The following logs are available for the Cisco pxGrid node:

- pxgrid.log: Provides state change notifications.
- pxgrid-cm.log: Displays updates on publisher or subscriber or both and data exchange activity between the client and the server.
- pxgrid-controller.log: Displays the details of client capabilities, groups, and client authorization.
- pxgrid-jabberd.log: Displays all the logs related to system state and authentication.
- pxgrid-pubsub.log: Displays all the information related to publisher and subscriber events.

Note

- If Cisco pxGrid service is disabled on a node, port 5222 is down, but port 8910 (used by web clients) is functional and continues to respond to the requests.

Note You can enable Cisco pxGrid with Base license, but you must have a Plus license to enable the Cisco pxGrid persona. In addition, certain extended Cisco pxGrid services may be available in your Base installation if you have recently installed an upgrade license for .

Note

- Cisco pxGrid should be defined in order to work with the Passive ID Work Center. For more information, see PassiveID Work Center

Cisco pxGrid Client and Capability Management

Clients connecting to Cisco ISE must register and receive account approval before using Cisco pxGrid services. Cisco pxGrid clients use the Cisco pxGrid client library available in the Cisco pxGrid SDK to become the clients. Cisco ISE supports both auto and manual approvals. A client can log in to Cisco pxGrid using a unique name and certificate-based mutual authentication. Similar to the AAA setting on a switch, clients can connect to either a configured Cisco pxGrid server hostname or an IP address.

Cisco pxGrid capabilities are information topics or channels on Cisco pxGrid for clients to publish and subscribe. In Cisco ISE, only capabilities such as Identity, Adaptive Network Control (ANC) , and Security Group Access (SGA) are supported. When a client creates a new capability, it appears in the **View by Capabilities** window. The navigation path for this window is **Administration** > **pxGrid Services** > **View by Capabilities**. You can enable or disable capabilities individually. Capability information is available from the publisher through publish, directed query, or bulk download query.

When a web client publisher uses REST APIs or WebSocket protocols, the topics added in the web client publisher are not immediately listed in the **Administration** > **pxGrid Services** > **Web Clients** tab in Cisco ISE. Such a web client topic appears in the **Web Clients** tab only after its first instance of publishing.

Note Users that are assigned to Endpoint Protection service (EPS) user group can perform actions in session group, because Cisco pxGrid session group is part of EPS group. If a user is assigned to EPS group, the user will be able to subscribe to the session group on the Cisco pxGrid client.

Related Topics

Generate Cisco pxGrid Certificate

Enable pxGrid Service

Before you begin

- Enable the pxGrid persona on at least one node to view the requests from the Cisco pxGrid clients.

Step 1 Choose **Administration** > **pxGrid Services**.

Step 2 Check the checkbox next to the client and click **Approve**.

Step 3 Click **Refresh** to view the latest status.

Step 4 Select the capability you want to enable and click **Enable**.

Step 5 Click **Refresh** to view the latest status.

Enable pxGrid Capabilities

Before you begin

- Enable the pxGrid persona on at least one node to view the requests from the Cisco pxGrid clients.
- Enable a pxGrid client.

Step 1 Choose **Administration** > **pxGrid Services**.

Step 2 Click **View by Capabilities** at the top-right.

Step 3 Select the capability you want to enable and click **Enable**.

Step 4 Click **Refresh** to view the latest status.

Deploy Cisco pxGrid Node

You can enable Cisco pxGrid persona both on a standalone node and distributed deployment node.

Before you begin

- You can enable the pxGrid with Base license, but you must have a Plus license to enable pxGrid persona. In addition, certain extended pxGrid services may be available in your Base installation if you have recently installed an upgrade license .
- All nodes use the CA certificate for Cisco pxGrid service usage. If you used the default certificate for Cisco pxGrid service before the upgrade, the upgrade replaces that certificate with the internal CA certificate.
- You must have port 8910 open for Websockets (pxGrid 2.0), and port 5222 open for XMPP (pxGrid V1.0). If the Cisco pxGrid service is disabled on a node, port 5222 goes down, but port 8910 remains functional, and continues to respond to the requests.

Step 1 Choose **Administration** > **System** > **Deployment**.

Step 2 In the **Deployment Nodes** window, check the check box next to the node for which you want to enable the Cisco pxGrid services, and click **Edit**.

Step 3 Click the **General Settings** tab and check the **pxGrid** check box.

Step 4 Click **Save**.

Note When you upgrade from the previous version, the **Save** option might be disabled. This happens when the browser cache refers to the old files from the previous version of Cisco ISE. Clear the browser cache to enable the **Save** option.

Configure Cisco pxGrid Settings

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration** > **pxGrid Services** > **Settings**.

Step 2 Check one of the following check boxes based on your requirements:

- **Automatically approve new certificate-based accounts**: Check this check box to automatically approve the connection requests from new Cisco pxGrid clients.
- **Allow password-based account creation**: Check this check box to enable username or password-based authentication for Cisco pxGrid clients. When this option is enabled, Cisco pxGrid clients cannot be automatically approved.

Step 3 Click **Save**.

Use the **Test** option in the Cisco pxGrid **Settings** window to run a health check on the Cisco pxGrid node. View the details in the pxgrid or pxgrid-test.log file.

https://<*ISE-Admin-Node*>:9060/ers/sdk

Generate Cisco pxGrid Certificate

Before you begin

- You must not use the same certificate for Cisco ISE pxGrid server and pxGrid clients. You must use client certificates for the pxGrid clients. To generate client certificates, choose **Administration > System > Certificates**.
- Some versions of Cisco ISE have a certificate for Cisco pxGrid that uses NetscapeCertType. We recommend that you generate a new certificate.
- To perform the following task, you must be a Super Admin or System Admin.
- A Cisco pxGrid certificate must be generated from the primary PAN.
- If the Cisco pxGrid certificate uses the subject alternative name (SAN) extension, be sure to include the FQDN of the subject identity as a DNS name entry.
- Create a certificate template with digital signature usage and use that to generate a new Cisco pxGrid certificate.

Step 1 Choose **Administration** > **pxGrid Services** > **Certificates**.

Step 2 From the **I want to** drop-down list, choose one of the following options:

- **Generate a single certificate (without a certificate signing request)**: You must enter the Common Name (CN) if you select this option.
- **Generate a single certificate (with a certificate signing request)**: You must enter the Certificate Signing Request details if you select this option.
- **Generate bulk certificates**: You can upload a CSV file that contains the required details.
- **Download Root Certificate Chain**: You can download the root certificates and add them to the trusted certificate store. You must specify the host name and the certificate download format.

Step 3 (Optional) Enter a description for this certificate.

Step 4 Click the **pxGrid_Certificate_Template** link to download and edit the certificate template based on your requirements.

Step 5 Enter the **Subject Alternative Name (SAN)**. You can add multiple SANs. The following options are available:

- **IP address**: Enter the IP address of the Cisco pxGrid client to be associated with the certificate.
- **FQDN**: Enter the FQDN of the pxGrid client.

Note This field is not displayed if you select the **Generate Bulk Certificate** option.

Step 6 From the **Certificate Download Format** drop-down list, choose one of the following options:

- **Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)**: The root certificate, the intermediate CA certificates, and the end entity certificate are represented in the PEM format. PEM-formatted certificates are BASE64-encoded ASCII files. Each certificate starts with the `"--------BEGIN CERTIFICATE-----"` tag and ends with the `"-------END CERTIFICATE----"` tag. The end entity's private key is stored using PKCS* PEM. It starts with the `"-----BEGIN ENCRYPTED PRIVATE KEY----"` tag and ends with the `"-----END ENCRYPTED PRIVATE KEY----"` tag.
- **PKCS12 format (including certificate chain; one file for both the certificate chain and key)**: A binary format to store the root CA certificate, the intermediate CA certificate, and the end entity's certificate and private key in one encrypted file.

Step 7 Enter the password for the certificate.

Step 8 Click **Create**.

You can view the certificate that you created in the **Issued Certificates** window. The navigation path for this window is **Administration** > **System** > **Certificates** > **Certificate Authority** > **Issued Certificates**.

You can view the certificate that you created in the **Issued Certificates** window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Certificate Authority** > **Issued Certificates**.

Note From Cisco ISE 2.4 patch 13 onwards, the certificate requirements have become stricter for the pxGrid service. If you are using the Cisco ISE default self-signed certificate as the pxGrid certificate, Cisco ISE might reject that certificate after applying Cisco ISE 2.4 patch 13 or later. This is because the earlier versions of that certificate have the **Netscape Cert Type** extension specified as **SSL Server**, which now fails (a client certificate is also required now).

Any client with a noncompliant certificate fails to integrate with Cisco ISE. Use a certificate issued by the internal CA, or generate a new certificate with proper usage extensions:

- The **Key Usage** extension in the certificate must contain the **Digital Signature** and **Key Encipherment** fields.
- The **Extended Key Usage** extension in the certificate must contain the **Client Authentication** and **Server Authentication** fields.
- The **Netscape Certificate Type** extension is not required. If you want to include that extension, add both **SSL Client** and **SSL Server** in the extension.
- If you are using a self-signed certificate, the **Basic Constraints CA** field must be set to **True**, and the **Key Usage** extension must contain the **Key Cert Sign** field.

Control Permissions for Cisco pxGrid Clients

You can create Cisco pxGrid authorization rules for controlling the permissions for the Cisco pxGrid clients. Use these rules to control the services that are provided to the Cisco pxGrid clients.

You can create different types of groups and map the services provided to the Cisco pxGrid clients to these groups. Use the **Manage Groups** option in the **Permissions** window to add new groups. You can view the example authorization rules in the **Client Management** > **Policies window.** Note that you can update only the **Operations** field for the predefined rules.

To create an authorization rule for pxGrid clients:

Step 1 Choose **Administration** > **pxGrid Services** > **Permissions**.

Step 2 From the **Service** drop-down list, choose one of the following options:

- **com.cisco.ise.pubsub**
- **com.cisco.ise.config.anc**
- **com.cisco.ise.config.profiler**
- **com.cisco.ise.config.trustsec**
- **com.cisco.ise.service**
- **com.cisco.ise.system**
- **com.cisco.ise.radius**
- **com.cisco.ise.sxp**
- **com.cisco.ise.trustsec**
- **com.cisco.ise.mdm**

Step 3 From the **Operation** drop-down list, choose one of the following options:

- **<ANY>**
- **publish**
- **publish /topic/com.cisco.ise.session**
- **publish /topic/com.cisco.ise.session.group**
- **publish /topic/com.cisco.ise.anc**
- **<CUSTOM>**: You can specify a custom operation if you select this option.

Step 4 From the **Groups** drop-down list, choose the groups that you want to map to this service.

ANC and manually added groups are listed in this drop-down list.

Note Only the clients that belong to the groups included in the policy can subscribe to the service specified in that policy. For example, if you define a pxGrid policy for com.cisco.ise.pubsub service and assign the ANC group to this policy, only the clients that belong to the ANC group can subscribe to the com.cisco.ise.pubsub service.

Cisco pxGrid Live Logs

The Live Logs window displays all the pxGrid management events. Event info includes the client and capability names along with the event type and timestamp.

The navigation path for this window is **Administration** > **pxGrid Services** > **Live Log**. You can also clear the logs and resynchronize or refresh the list.