Cisco pxGrid

Cisco pxGrid and ISE

✎

Note From Cisco ISE Release 3.1, all pxGrid connections must be based on pxGrid 2.0. pxGrid 1.0-based (XMPP-based) integrations will cease to work on Cisco ISE from Release 3.1 onwards.

pxGrid Version 2.0, which is based on WebSockets, was introduced in Cisco ISE Release 2.4. We recommend that you plan and upgrade your other systems to pxGrid 2.0-compliant versions in order to prevent potential disruptions, if any, to integrations.

Cisco Platform Exchange Grid (pxGrid) is an open and scalable Security Product Integration Framework that allows for bi-directional any-to-any partner platform integrations.

pxGrid 2.0 uses REST and WebSocket interfaces. A client uses REST for control messages, queries and application data, and WebSockets for pushing events. For more information about pxGrid 2.0, see Welcome to Learning Cisco Platform Exchange Grid (pxGrid).

For information about Cisco pxGrid Direct, see Cisco pxGrid Direct.

pxGrid can:

- Share context-sensitive information from the Cisco ISE session directory with other network systems, such as Cisco ISE ecosystem partner systems and other Cisco platforms.

- Enable third-party systems to invoke adaptive network control actions to quarantine users and devices in response to a network or security event. TrustSec information, such as tag definition, value, and description, pass from Cisco ISE via a TrustSec topic to other networks.

- Send endpoint profiles with Fully Qualified Names (FQNs) from Cisco ISE to other networks through an endpoint profile meta topic.

- Bulk download of tags and endpoint profiles.

- Publish and subscribe to SXP bindings (IP-SGT mappings) through pxGrid. For more information about SXP bindings, see the *Security Group Tag Exchange Protocol* section in the Segmentation chapter of the Cisco ISE Administrators Guide.

- Cisco pxGrid Context-in enables ecosystem partners to publish topic information into Cisco ISE. This enables Cisco ISE to take action based on the identified asset in the ecosystem. For more information about Cisco pxGrid Context-in, see pxGrid Context-In.

pxGrid Overview

pxGrid has the following components:

- Controller: Handles Discovery, Authentication, and Authorization.

- Provider: Returns query results or publishes.

- Pubsub: Provides pxGrid services to providers and consumers.

- Subscriber: Once authorized, subscribers get the contextual information and alerts from topics that they subscribe to.

pxGrid provides the following functions:

- Discovery: Discovers service properties based on service name. The flow starts when a provider asks to "Register Service" with the pxGrid Controller. After registration, the consumer uses "Lookup Service" to discover the locations of the providers.

- Authentication: The pxGrid Controller authenticates the pxGrid client for access to services. Credentials are either username and password, or certificates (preferred).

- Authorization: When pxGrid gets an operation request, it consults with pxGrid Controller to authorize the request. pxGrid assigns the client to a pre-defined group.

High Availability for pxGrid 2.0

pxGrid 2.0 nodes operate in an Active/Active configuration. For high availability, there should be at least two pxGrid nodes in the deployment. Large deployments can have up to four nodes for increased scale and redundancy. We recommend that you configure IP addresses for all nodes, so that if one node goes down, that node's clients connect to working node. When the PAN goes down, pxGrid server stops handling the activations. Manually promote the PAN to activate the pxGrid server. For more information about pxGrid deployments, see **ISE Performance & Scale**.

All pxGrid service provider clients periodically reregister themselves with the pxGrid controller within a span of 7.5 minutes. If the client does not reregister, the PAN node assumes it's inactive, and deletes that client. If the PAN node goes down for more than 7.5 minutes, when it comes back up, it deletes all the clients with timestamp values older than 7.5 minutes. All those clients must then register again with the pxGrid controller.

pxGrid 2.0 clients use WebSocket and REST-based APIs for pub/sub and query. These APIs are served by the ISE application server on port 8910. The pxGrid processes shown by `show logging application pxgrid` don't apply to pxGrid 2.0.

Note All the references to pxGrid 1.0 processes in the GUI and the CLI have been removed.

Loss Detection

In Cisco ISE 3.0, we added sequence IDs to pxGrid topics. If there is a break in transmission, the subscriber can recognize that by checking the gap in sequence of IDs. The subscriber notices the change in topic sequence

ID, and asks for data based on the date of last sequence number. If the Publisher goes down, when it comes back up, topic sequence starts at 0. When the Subscriber sees sequence 0, they must clear the cache and start bulk download. If subscriber goes down, the publisher keeps assigning sequential IDs. When the subscriber reconnects, and sees a gap in sequence IDs, the subscriber asks for data from time of the last sequence number. Loss detection works with Session Directory, and TrustSec Configuration. With Session Directory, when the client detects a loss, they must clear the cache and start bulk download.

If you have an existing application that doesn't use sequence IDs, you don't have to use them. But using them provides benefits of loss detection and recovery from loss.

Session Directory sessions are batched and published by MnT asynchronously for every notify interval to `/topic/com.cisco.ise.session`.

Changes to TrustSec Security Groups are published to `/topic/com.cisco.ise.config.trustsec.security.group`.

Loss Detection is only supported for pxGrid 2.0, and is on by default.

To see code examples of using Loss Detection, see https://github.com/cisco-pxgrid/pxgrid-rest-ws/tree/master/java/src/main/java/com/cisco/pxgrid/samples/ise.

Monitoring and Debugging

The following logs are available for pxGrid:

• pxgrid-server.log: pxGrid 2.0 activities and errors

The **Log** page displays all the pxGrid 2.0 management events. Event info includes the client and capability names along with the event type and timestamp. Choose **Administration > pxGrid Services > Diagnostics > Log** to view the list of events. You can also clear the logs and resynchronize or refresh the list.

pxGrid Failover and Recovery

The time taken for pxGrid recovery in different failover scenarios in a multi-pxGrid node deployment with atleast one primary and secondary pxGrid node each, varies depending on the node that goes down or comes back up and certain other variables, some of which are described in detail below.

Following are four different pxGrid failover and recovery scenarios and the workflows triggered internally in each of these cases:

• **Primary pxGrid node goes down**

Secondary pxGrid node MnT continues to be the sessions data publisher. If the Firewall Management Center (FMC) is connected to the primary node, after a few unsuccessful retry attempts, it connects and subscribes to the secondary node. Since there has been a disruption, FMC will do a bulk download.

If the FMC is already subscribed to the secondary pxGrid node, the recovery will be even smoother. Since there is no disruption, the FMC does not need to do a bulk download. Hence, the recovery is much faster. In this scenario, the recovery time can be as less as 2 minutes.

• **Primary pxGrid node comes back up**

The FMC is still connected to the secondary pxGrid node and disruption will be less as the secondary node continues to publish sessions data. Bulk download is unncessary in this case, hence recovery is fast as in the case of the previous scenario.

The FMC will be able to re-establish connection with pxGrid and connect to the primary pxGrid node only after all the fanouts are re-established and database sync is complete.

- **Secondary pxGrid node goes down**

  If the FMC is connected to the primary node pxGrid, it will continue to be connected there. But there will be a disruption because the secondary MnT node would have been the publisher of session topic data so far. Primary MnT node takes some time to realize that the secondary MnT node is down and when it realizes, it starts to publish session topic data from the primary node.

  If the FMC is connected to pxGrid on the secondary node, it retries connection, and on failure, connects to the primary PxGrid node for subscription. This happens in parallel to the previous step. On a successful reconnection with the secondary pxGrid node, FMC does a bulk download.

- **Secondary pxGrid node comes back up**

  This is the scenario in which recovery takes the longest time. If there were any pxGrid related database changes during the time that the secondary node had been down, there is a possibility that pxGrid will not be functional until the database sync operation completes. The time taken for database sync depends on the size of configuration database.

  The secondary pxGrid node goes back to being the sessions data publisher.

  A refresh deployment notification is sent to all modules and when pxgrid module receives this, it re-establishes all the fanouts that are used for internal distribution of data. Until this is completed, pxGrid will not be completely functional.

  If the FMC has to reconnect, after the reconnection succeeds, FMC will do a bulk download.

pxGrid Summary Page

The pxGrid Summary page displays statistics of the current pxGrid 2.0 environment.

- Current Connections: Lists the connections to the controller

- Control Messages: Authentication, Authorization, and service Discovery

- REST APIs: Number of clients who connected using WebSockets or XMPP

- Pubsub Throughput: Amount of data published to clients

- Clients: Clients connected by REST or WebSocket

- Errors: Number of transmission errors, which caused client to ask for data transfer restart

pxGrid Client Management

Clients must register and receive account approval to use pxGrid services in Cisco ISE. Clients use the pxGrid Client library through the pxGrid SDK to register. Cisco ISE supports both auto and manual registrations.

- **Clients**: Choose **Administration > pxGrid Services > Client Management > Clients** to view this window. Lists external client accounts for pxGrid 2.0.

- **pxGrid Policy**: Choose **Administration > pxGrid Services > Client Management > pxGrid Policy** to view this window. Lists the available services that clients can subscribe to. You can edit a policy to change which groups can access to that policy. You can also create a new policy for a service that doesn't already have a policy.

- **Groups**: Choose **Administration > pxGrid Services > Client Management > Groups** to view this window. ANC is a predefined group. You can add more groups, and use them to limit access to services.

  A pxGrid client can register itself with the pxGrid controller by sending the username via REST API. The pxGrid controller generates a password for the pxGrid client during client registration. The administrator can approve or deny the connection request.

- **Certificates**: Choose **Administration > pxGrid Services > Client Management > Certificates** to view this window. You can generate a new certificate to use the Cisco ISE internal Certificate Authority.

  For information about creating certificates for pxGrid, see:

  - Deploying Certificates with Cisco pxGrid - Using Self-Signed Certificates Updates to Cisco ISE 2.0/2.1/2.2

  - Deploying Certificates with Cisco pxGrid - Using External CA with updates to Cisco ISE 2.0/2.1/2.2

Control pxGrid Policies

You can create pxGrid authorization policies to control access to the services that pxGrid clients can access. These policies control which services are available to the pxGrid clients.

You can create different types of groups and map the available services to the pxGrid clients to these groups. Use the **Manage Groups** option in the **Client Management > Groups** window to add new groups. You can view the example authorization rules in the **Client Management** > **Policies** window.

To create an authorization policies for pxGrid clients:

Step 1   Choose **Administration > pxGrid Services > Client Management > Policy**, and then click **Add**.

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

- com.cisco.ise.radius

- come.cisco.ise.sxp

- com.cisco.ise.trustsec

- com.cisco.ise.session

- com.cisco.ise.system

- com.cisco.ise.mdm

- com.cisco.ise.config.trustsec

- com.cisco.ise.config.profiler

- com.cisco.ise.pxgrid.admin

- com.cisco.ise.config.deployment.node

- com.cisco.ise.endpoint

- com.cisco.ise.config.anc

- com.cisco.ise.dnac

- com.cisco.ise.config.upn

- com.cisco.ise.pubsub

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.

Predefined groups (such as EPS and ANC) and groups that you manually added are listed in this drop-down list.

Note   Only the clients that are part of the groups included in the policy can subscribe to the service specified in that policy.

Step 5   Click **Submit**.

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   In the Cisco ISE GUI, click the **Menu** icon (☰) and 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.

pxGrid Diagnostics

- **Websocket**: The **Administration > pxGrid Services > Diagnostics > Websocket** window lists pxGrid 2.0 clients (external and internal). It also lists the available pxGrid 2.0 topics, and the clients that publish or subscribe to each one.

- **Logs**: The **Administration > pxGrid Services > Diagnostics > Live Logs** window lists management events.

• **Tests**: Choose **Administration > pxGrid Services > Diagnostics > Tests > Health Monitoring test** and click **Start Test** to verify whether a client can access the Session Directory service. When the test is complete, you can view the log of the test activities.

pxGrid Settings

Choose one of the following options in the **Administration > pxGrid Services > Settings** window:

• **Automatically approve new certificate-based accounts**: This option is disabled by default. It gives you control over connections to the pxGrid server. Enable this option only when you trust all clients in your environment.

• **Allow password based account creation**: Check this check box to enable username/password based authentication for pxGrid clients. If you enable this option, the pxGrid clients are not automatically approved.

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.

Note   If FIPS mode is enabled, the pxGrid certificate template's RSA private key size must be 2048 bits or greater. Else an error is displayed when you try to generate a pxGrid certificate. To change the private key size of the certificate template, see Change pxGrid Certificate Template Key Size, on page 9.

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

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.

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. 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.

Known Limitations in pxGrid Certificate Generation

pxGrid certificate generation in Cisco ISE follows the tabulated logic explained below:

Serial number	System Certificate (EAP)	Issuer Certificate	pxGrid Format	Support
1	Multiple Common Name	Single Common Name	PKCS8 , PKCS12	Yes, supported
2	Multiple Common Name	Multiple Common Name	PKCS12	Yes, supported
3	Multiple Common Name	Multiple Common Name	PKCS8	Not supported

Change pxGrid Certificate Template Key Size

The following task helps you to change the key size of the pxGrid certificate template.

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

Step 2 Check the check box next to the template **pxGrid_Certificate_Template**.

Step 3 Click **Edit**.

Step 4 From the **Key Size** drop-down list, choose **2048**.

Step 5 Click **Save**.