Cisco ISE 2.4 Admin Guide: PxGrid

PxGrid

pxGrid Node

You can use Cisco pxGrid to share the context-sensitive information from Cisco ISE session directory with other network systems such as ISE Eco system partner systems and other Cisco platforms. The pxGrid framework can also be used to exchange policy and configuration data between nodes like sharing tags and policy objects between Cisco ISE and third party vendors, and for other information exchanges. pxGrid also allows 3rd party systems to invoke adaptive network control actions (EPS) to quarantine users/devices in response to a network or security event. The TrustSec information like tag definition, value, and description can be passed from Cisco ISE via TrustSec topic to other networks. The endpoint profiles with Fully Qualified Names (FQNs) can be passed from Cisco ISE to other networks through a 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 pxGrid. For more information about SXP bindings, see the Security Group Tag Exchange Protocol section in .

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

For XMPP (Extensible Messaging and Presence Protocol) clients, pxGrid nodes work in Active/Standby high availability mode which means that the pxGrid Service is in "running" state on the active node and in "disabled" state on the standby node.

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

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

In a high availability deployment, when the primary pxGrid node goes down, it might take around 3 to 5 minutes to switchover to the secondary pxGrid node. It is recommended that the client waits for the switchover to complete, before clearing the cache data in case of primary pxGrid node failure.

The following logs are available for pxGrid node:

- pxgrid.log—State change notifications.
- pxgrid-cm.log—Updates on publisher/subscriber and data exchange activity between client and server.
- pxgrid-controller.log—Displays the details of client capabilities, groups, and client authorization.
- pxgrid-jabberd.log—All logs related to system state and authentication.

- pxgrid-pubsub.log—Information related to publisher and subscriber events.

Note If pxGrid service is disabled on a node, port 5222 will be down, but port 8910 (used by Web Clients) will be functional and will continue to respond to the requests.

Note You can enable 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 for .

Note pxGrid should be defined in order to work with the Passive ID Work Center. For more information, see the PassiveID Work Center section in *Cisco ISE Admin Guide: Asset Visibility* .

pxGrid Client and Capability Management

Clients connecting to Cisco ISE must register and recieve account approved before using pxGrid services. pxGrid clients use the pxGrid Client Library available from Cisco through the pxGrid SDK to become the clients.Cisco ISE supports both auto and manual approvals. A client can log in to 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 pxGrid server hostname or an IP Address.

pxGrid "Capabilities" are information topics or channels on pxGrid for clients to publish and subscribe. In Cisco ISE, only capabilities such as Identity, adaptive network control, and SGA are supported. When a client creates a new capability, it appears in. **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.

Note Users that are assigned to EPS user group can perform actions in Session group, because pxGrid Session group is part of EPS group. If a user is assigned to EPS group, the user will be able to subscribe to Session group on pxGrid client.

Related Topics

Generate pxGrid Certificate, on page 4

Enable pxGrid Clients

Before you begin

- Enable the pxGrid persona on at least one node to view the requests from the Cisco pxGrid clients.
- Enable Passive Identity Services. Choose **Administration** > **Deployment**, checkmark the desired node, click **Edit** and from the settings screen, checkmark **Enable Passive Identity Service**.

Procedure

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.

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.

Procedure

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 pxGrid Node

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

Before you begin

- You can enable pxGrid with Base license, but you must have a Plus license to enable pxGrid persona.
- Cisco pxGrid services running on a Cisco ISE SNS 3415/3495 Appliance or in VMWare.
- All nodes are configured to use the CA certificate for pxGrid usage. If default certificate is used for pxGrid before upgrade, it will be replaced by the internal CA certificate after upgrade.
- If you are using a distributed deployment or upgrading from Cisco ISE 1.2, then you need to enable the pxGrid Usage option for the certificates. To enable the pxGrid Usage option, go to **Administration** > **Certificates** > **System Certificates**. Choose the certificate being used in the deployment and click **Edit**. Check the pxGrid: use certificate for the pxGrid Controller checkbox.

Procedure

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

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

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

Step 4 Click **Save**.

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 pxGrid Settings

Before you begin

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

Procedure

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

Step 2 Select the following options based on your requirements:

- Automatically Approve New Accounts—Check this check box to automatically approve the connection requests from new pxGrid clients.
- Allow Password Based Account Creation—Check this check box to enable username/password based authentication for pxGrid clients. If this option is enabled, the pxGrid clients cannot be automatically approved.

  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.

Step 3 Click **Save**.

You can use the **Test** option on the pxGrid Settings page to run a health check on the pxGrid node. You can view the details in the pxgrid/pxgrid-test.log file.

Generate pxGrid Certificate

Before you begin

- To perform the following task, you must be a Super Admin or System Admin.
- pxGrid certificate must be generated from the Primary PAN.
- If the pxGrid certificate uses the subject alternative name (SAN) extension, be sure to include the FQDN of the subject identity as a DNS name entry.

Procedure

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

Step 2 Select one of the following options from the **I want to** drop-down list:

- 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.

You can download the certificate template from the Certificate Template link and edit the template based on your requirements.

Step 3 (Required if you choose to Generate a single certificate (without a certificate signing request) option) Enter the FQDN of the pxGrid client.

Step 4 (optional) You can enter a description for this certificate.

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

- IP address—Enter the IP address of the pxGrid client to be associated with the certificate.
- FQDN—Enter the fully qualified domain name of the pxGrid client.

Note This field is not displayed if you have selected the Generate Bulk Certificate option.

Step 6 Select one of the following options from the **Certificate Download Format** drop-down list:

- 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 certificate 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 a certificate password.

Step 8 Click **Create**.

The certificate that you created is visible in ISE under **Administration** > **System** > **Certificates** > **Certificate Authority** > **Issued Certificates**, and downloaded to your browser's downloads directory.

Control Permissions for pxGrid Clients

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

You can create different types of groups and map the services provided to the pxGrid clients to these groups. Use the **Manage Groups** option in the **Permissions** window to add new groups. You can view the predefined

authorization rules that use predefined groups (such as EPS and ANC) in the Permissions window. Note that you can update only the **Operations** field for the predefined rules.

To create an authorization rule for pxGrid clients:

Procedure

Step 1 From the **Administration** tab, choose **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>**

  Note 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 manually added groups (using the **Manage Groups** option in the **Permissions** window) are listed in this drop-down list.

Cisco pxGrid Live Logs

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

Navigate to **Administration** > **pxGrid Services** > **Live Log** to view the list of events. You can also clear the logs and resynchronize or refresh the list.