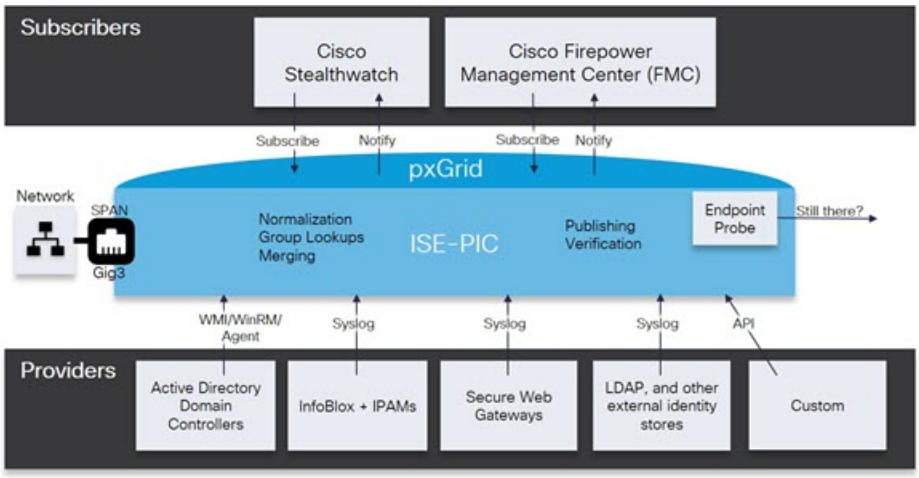
Subscribers

ISE-PIC uses Cisco pxGrid services to deliver authenticated user identities that are collected from various providers and stored by the Cisco ISE-PIC session directory, to other network systems such as Cisco Stealthwatch or Cisco Firepower Management Center (FMC).

In the following figure, the pxGrid node collects user identities from external providers. Those identities are parsed, mapped and formatted. pxGrid takes those formatted user identities and sends them to ISE-PIC subscribers.

Figure 1: ISE-PIC Flow



Subscribers connected to Cisco ISE-PIC must register to use the pxGrid services. A subscriber can log in to pxGrid using a unique name and certificate-based mutual authentication. Once they have sent a valid certificate, Cisco pxGrid subscribers are automatically approved by ISE-PIC.

Subscribers can connect to either a configured pxGrid server hostname or an IP Address. We recommend that you use hostname to avoid unnecessary errors, particularly to ensure the DNS queries work properly. Capabilities are information topics or channels that are created on pxGrid for subscribers to publish and subscribe. In Cisco ISE-PIC, only SessionDirectory and IdentityGroup are supported. You can view capability information that is available from the publisher through publish, directed query, or bulk download query, by navigating to **Subscribers** in the **Capabilities** tab.

To enable subscribers to receive information from ISE-PIC, you must:

1. Optionally, generate a certificate from the subscriber's side.

2. Generate pxGrid Certificates for Subscribers, on page 2 from ISE-PIC.
3. Enable Subscribers, on page 3. Either perform this step, or automatically enable approvals, in order to allow subscribers to receive user identities from ISE-PIC. See Configure Subscriber Settings, on page 4.

Generate pxGrid Certificates for Subscribers

Before you begin

At installation, ISE-PIC automatically generates self-signed certificates for the pxGrid services that are digitally signed by the primary ISE-PIC node. Thereafter, you can generate certificates for pxGrid subscribers in order to guarantee mutual trust between pxGrid and the subscribers, thereby ultimately enabling user identities to be passed from ISE-PIC to the subscribers.

Step 1 Choose **Subscribers** and go to the **Certificates** tab.

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. In the Common Name field, enter the pxGrid FQDN which includes pxGrid as the prefix. For example, www.pxgrid-ise.ise.net. Or, alternatively, use wildcards. For example, *.ise.net
- **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**: Download the ISE public root certificates in order to add them to the pxGrid client's trusted certificate store. The ISE pxGrid node only trusts the newly signed pxGrid client certificate and vice-versa, eliminating the need for outside certificate authorities.

Step 3 (optional) You can enter a description for this certificate.

Step 4 View or edit the pxGrid Certificate template on which this certificate is based. Certificate templates contain properties that are common to all certificates issued by the Certificate Authority (CA) based on that template. The certificate template defines the Subject, Subject Alternative Name (SAN), key type, key size, SCEP RA profile that must be used, validity period of the certificate, and the extended key usage (EKU) that specifies whether the certificate has to be used for client or server authentication or both. The internal Cisco ISE CA (ISE CA) uses a certificate template to issue certificates based on that template. For pxGrid, only the pxGrid certificate template can be used when working with Passive Identity services and only the Subject information can be edited for this template. To edit this template, choose **Certificates** > **Certificate TemplatesAdministration** > **Certificates** > **Certificate Authority** > **Certificate Templates**.

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

- **FQDN**: Enter the fully qualified domain name of the ISE node. For example www.isepic.ise.net. Or, alternatively, use wildcards for the FQDN. For example, *.ise.net

An additional line can be added for FQDN in which the pxGrid FQDN can also be entered. This should be identical to the FQDN you used in the Common Name field.

- **IP address**: Enter the IP address of the ISE node to be associated with the certificate. This information must be entered if the subscriber uses IP addresses instead of an FQDN.

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**.

Enable Subscribers

You must perform this task, or alternatively automatically enable approvals, in order to allow subscribers to receive user identities from Cisco ISEISE-PIC. See Configure Subscriber Settings, on page 4.

Step 1 Choose **Subscribers** and ensure you are viewing the **Clients** tab.

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

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

View Subscriber Events from Live Logs

The Live Logs page displays all the Subscriber events. Event information includes the subscriber and capability names along with the event type and timestamp.

Navigate to **Subscribers** and select the **Live Log** tab to view the list of events. You can also clear the logs and resynchronize or refresh the list.

Configure Subscriber Settings

Step 1 Choose **Subscribers** and go to the **Settings** tab.

Step 2 Select the following options based on your requirements:

- **Automatically Approve New Accounts**: Check this checkbox to automatically approve the connection requests from new pxGrid clients.
- **Allow Password Based Account Creation**: Check this checkbox 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**.