## Table of Contents

1.  Configuring the PXG ................................................................. 7
   1.1 Configuring Ethernet Access ............................................ 7

2.  Configuring Device Communications ....................................... 9
   2.1 Port Settings ................................................................. 9
   2.2 Network 1 (Ethernet) .................................................... 10
   2.3 Adding Devices ............................................................ 10
   2.4 Initial Setup ................................................................. 10
   2.4.1 Example 1: Adding an IQ 250 Meter ......................... 10

3.  Configuring Device Channels .................................................. 12
   3.1 Disabling a Device ....................................................... 12
   3.2 Managing Device Channels .......................................... 13

4.  Setting Preferences ............................................................... 14
   4.1 Time ............................................................................. 14
   4.2 Locale ......................................................................... 14

5.  Network Access Settings ....................................................... 16
   5.1 Access Control ............................................................ 16

6.  Modbus TCP Server .............................................................. 19
   6.1 Modbus TCP Server Setup ............................................ 19
   6.2 Viewing and Modifying the Modbus Map ...................... 20
   6.3 Pass Through ............................................................... 21
   6.3.1 Modbus ..................................................................... 21

7.  BACnet IP Server ................................................................. 22
   7.1 Setting up a BACnet/IP Server ....................................... 22
   7.1.1 Base ID for Auto-Assign .......................................... 22
   7.1.2 Auto-Assign Gateway ID ......................................... 22
   7.1.3 Auto-Assign Device IDs .......................................... 22
   7.1.4 BACnet Broadcast Management Device .................. 22
   7.2 Mapping ...................................................................... 23

8.  SNMP Server ...................................................................... 25
8.1 SNMP Server Setup .................................................................................................................. 25
8.1.1 Enabling SNMP v1 and v3 Support ....................................................................................... 25
8.1.2 Detailed SNMP v3 Configuration ......................................................................................... 25
8.1.2.1 Configuring the Read-Only User ....................................................................................... 26
8.1.2.2 Configuring the Read-Write User ..................................................................................... 26
8.1.3 Detailed SNMP v1 Configuration ......................................................................................... 26
8.1.3.1 Configuring the Read-Only Community String ................................................................. 27
8.1.3.2 Configuring the Read-Write Community String ............................................................... 27
8.1.4 Gateway-provided SNMP MIB Support ............................................................................... 27
8.1.4.1 Eaton OIDs ..................................................................................................................... 28
8.1.4.2 Eaton Power Device MIB ............................................................................................... 28
8.1.4.3 Eaton Power Meter MIB .................................................................................................. 29
8.1.4.4 Eaton Alarms+Traps MIB ............................................................................................... 29
8.1.4.5 Entity and Entity State MIB Support ................................................................................. 29
8.1.5 Configuring v1 Trap Support ............................................................................................... 29
8.1.5.1 v1 Trap Recipient Community String .............................................................................. 30
8.1.6 Configuring v3 Trap Support ............................................................................................... 31
8.1.6.1 v3 Auth Fail Trap ............................................................................................................. 31
8.1.7 Adding or Removing v1 and v3 Trap Recipients ................................................................. 31
9 Notifications .............................................................................................................................. 32
9.1 Setting up the Email Server .................................................................................................... 32
9.2 Adding Recipients .................................................................................................................. 33
9.3 System Use Notification ......................................................................................................... 34
10 Users and Access Control ......................................................................................................... 35
10.1 Building Roles ....................................................................................................................... 36
10.2 Creating Users ...................................................................................................................... 37
10.3 Deleting Admin and User ..................................................................................................... 37
10.4 Accessing Logs ..................................................................................................................... 38
10.5 Roles and Permissions Cookbook ....................................................................................... 38
10.6 Security Audit ....................................................................................................................... 38
10.7 Security Admin ..................................................................................................................... 38
10.8 Engineer ................................................................................................................................. 39
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.4</td>
<td>Waveform Files</td>
<td>61</td>
</tr>
<tr>
<td>18.5</td>
<td>Manual Waveform Capture</td>
<td>62</td>
</tr>
<tr>
<td>18.6</td>
<td>Signing up for Waveform Email Notifications</td>
<td>62</td>
</tr>
<tr>
<td>18.7</td>
<td>Waveform Link in Email Notifications</td>
<td>64</td>
</tr>
<tr>
<td>19</td>
<td>One-lines Tab</td>
<td>67</td>
</tr>
<tr>
<td>19.1</td>
<td>Device Tree</td>
<td>67</td>
</tr>
<tr>
<td>19.2</td>
<td>Graphic View</td>
<td>67</td>
</tr>
<tr>
<td>19.3</td>
<td>Link Objects</td>
<td>67</td>
</tr>
<tr>
<td>19.4</td>
<td>One-line Diagrams</td>
<td>67</td>
</tr>
<tr>
<td>20</td>
<td>Reset PXG</td>
<td>71</td>
</tr>
<tr>
<td>21</td>
<td>Certificate Management</td>
<td>73</td>
</tr>
<tr>
<td>21.1</td>
<td>Certificate Generation</td>
<td>73</td>
</tr>
<tr>
<td>21.2</td>
<td>Certificate Upload</td>
<td>73</td>
</tr>
<tr>
<td>21.3</td>
<td>Operations Supported by the Certificate Manager UI</td>
<td>74</td>
</tr>
<tr>
<td>21.3.1</td>
<td>Listing of Server Certificates</td>
<td>74</td>
</tr>
<tr>
<td>21.3.2</td>
<td>Viewing Details of Certificates</td>
<td>74</td>
</tr>
<tr>
<td>21.3.3</td>
<td>Export Server Certificate</td>
<td>75</td>
</tr>
<tr>
<td>21.3.4</td>
<td>Generate New Self-Signed Certificates</td>
<td>75</td>
</tr>
<tr>
<td>21.3.5</td>
<td>Generate Certificate Signing Request and Certificate Import</td>
<td>76</td>
</tr>
<tr>
<td>21.3.6</td>
<td>Revoke Certificate</td>
<td>77</td>
</tr>
<tr>
<td>22</td>
<td>Cloud Connection Setup</td>
<td>78</td>
</tr>
<tr>
<td>23</td>
<td>Cybersecurity Hardening the PXG</td>
<td>81</td>
</tr>
<tr>
<td>23.1</td>
<td>References</td>
<td>99</td>
</tr>
<tr>
<td>24</td>
<td>Cellular Settings and Wifi Configuration</td>
<td>100</td>
</tr>
<tr>
<td>24.1</td>
<td>Cellular Settings</td>
<td>100</td>
</tr>
<tr>
<td>24.2</td>
<td>Wi-Fi Configuration</td>
<td>100</td>
</tr>
<tr>
<td>25</td>
<td>Firmware Update</td>
<td>102</td>
</tr>
</tbody>
</table>
The Power Xpert Gateway 950-4G is an Internet-of-Things (IoT) device. It is mounted at the edge of a network, enabling you to collect, secure, analyze, and act on data from multiple devices and sensors. It enables you to connect with devices used in transportation, building automation, manufacturing, and other applications. With its low-power architecture, the PXG950-4G is capable of supporting industrial automation workloads while remaining fanless. This allows it to satisfy both environmental and reliability requirements. This guide will show you how to configure the PXG 950 from its web interface and how to work with the Network, One-lines, and Alarms tabs etc.
1 Configuring the PXG

The PXG950 is shipped from the factory with a default password. This assists commissioning agents in the original commissioning of the PXG950. Once original commissioning is complete and the PXG950 is put into operational use, it is important that the password be changed to a non-trivial password. Refer to your organizations Cyber Security practices to determine the minimum recommended complexity of the password.

To connect to the PXG950 web interface:

1. You can power on PXG950 using either 24V DC power supply (DC-IN) or with Power over Ethernet (PoE).
2. Default configuration of the PXG950 is DHCP, Wired Connection.
3. Use Advanced IP scanner utility to find dynamic (DHCP) IP address using Ethernet MAC 1 address available on PXG950 gateway hardware.
4. Use this IP address to access PXG950 web UI.
5. You’ll be prompted to enter a user ID and password. The default is "admin" for both.
6. After login you can change network setting to static IP or configure the PXG950 for Wireless connectivity.

1.1 Configuring Ethernet Access

Once Ethernet access is configured, the PXG web interface is available via an Ethernet LAN connection. Currently, the PXG supports only IPv4 addressing. You can specify the IP address for the gateway in one of two ways:

- Static IP, where you specify a static IP address in the PXG setup screens. This is the recommended approach. If you choose this approach note the IP address on the label, publish it to the users, and make certain it’s reserved in your network.
- DHCP, where the gateway is automatically assigned an IP address by the DHCP server or router. Eaton recommends that you don’t use this approach.

**Static IP address setting using USB**

The PXG950 IP address can also be configured using a USB drive formatted with a single FAT32 partition. In the top level directory of the USB drive place a file named “01-network-manager-all.yaml” and reboot the PXG950 with the USB drive connected.

Sample contents of the file are shown below.

```yaml
network:
  version: 2
  renderer: NetworkManager
  etheports:
    eth0:
      dhcp4: no
      addresses: [10.235.1.96/24]
      gateway4: 10.235.0.1
      nameservers:
        addresses: [151.110.232.49, 151.110.232.100]
```

This would set the device IP address: 10.235.1.96, netmask: 255.255.254.0, gateway: 10.235.0.1 and nameservers: 151.110.232.49, 151.110.232.100. Once the PXG950 is reconfigured upon boot up, the file on USB drive “01-network-manager-all.yaml” is renamed to “01-network-manager-all.yaml.bak”. It can be reused for performing forced settings by renaming the file back to “01-network-manager-all.yaml”.

**Wireless Network Settings**
PXG950 Can be configured to communicate over wireless network check section "Cellular Settings and Wifi Configuration" for more details.

After you've completed configuring an IP address (either through DHCP Reservations or as a static IP) set the port visibility options.

The Network tab displays devices attached to the various ports; however, you can use the Port Visibility check boxes to limit what’s shown on the tab to only the ports that you select.

NOTE: By default HTTPS is Enabled and HTTP is disabled per cyber security guidelines. The gateway's web interface uses TCP ports 80 and 7011 for its routine HTTP communications. For HTTPS access, ports 443 and 7012 are used. If you experience difficulty with your browser only showing the gateway's UI header and nothing else, your IT department may be blocking ports 7011 and 7012 internally.
2 Configuring Device Communications

2.1 Port Settings

You can configure the PXG’s Modbus ports and Ethernet Ports on the Network tab. Choose edit to change any of the port configurations. You can access the port settings by choosing the appropriate gear icon. Before connecting the PXG to a twisted pair Modbus cable, make sure that you observe the proper polarity when wiring the cable to one of the three-pin Phoenix connectors provided. The PXG RS-485 ports connection is as below:

<table>
<thead>
<tr>
<th>Pin</th>
<th>Signal</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data -</td>
<td>(-) TX/RX Data</td>
</tr>
<tr>
<td>2</td>
<td>Data +</td>
<td>(+) TX/RX Data</td>
</tr>
<tr>
<td>3</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>4</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>5</td>
<td>GND</td>
<td>Ground</td>
</tr>
<tr>
<td>6</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>7</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>8</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>9</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>10</td>
<td>GND</td>
<td>Ground</td>
</tr>
</tbody>
</table>

Note: If needed, add an external 120-ohm resistor.

The ports have the following device limits:

- COM1 port - 32 devices, supports Modbus RTU devices
- COM2 port - 32 devices, supports Modbus RTU devices
- Network 1 port - 50 (3-phase) metering points, supports Modbus TCP devices
2.2 Network 1 (Ethernet)

When Private Network is enabled, you can use Network 1 to connect to a network of devices using Modbus TCP. Choose the gear icon to access the network settings. The IP address should match that of the Modbus TCP subnet. You can add the network devices by clicking the 'Add Device' option under Network1 tab. Don't change the timeout setting unless this is absolutely necessary.

2.3 Adding Devices

After you've properly configured the serial ports and connected the gateway to your serial networks, you can begin adding any supported devices currently on that serial network. Adding devices, like port configuration, is done on the Network tab.

2.4 Initial Setup

The PXG helps you when adding devices, guiding you through the initial setup steps:

1. Goto Network Tab
2. Choose Edit.
3. Choose Add Device under the appropriate port.
4. In the sidebar, select the device type under Family.
5. Select the Model Series.
6. Select the device Model.
7. Enter a meaningful name for the device.
8. Enter the device address: 1-247 decimal for Modbus, 1-FFE hexadecimal for INCOM. If you enter an address that's already in use, the box outline will turn red and you won't be able to save the device configuration until you select a unique address.
9. If Enable Waveforms is available, decide whether you wish to have the PXG capture these.
10. Choose Save Device Configuration.

The following examples assume that the devices are on the appropriate networks and that the ports are properly configured.

2.4.1 Example 1: Adding An IQ 250 Meter

1. Connect the IQ 250 Meter to either COM1 or COM2.
2. Choose the Network tab.
3. Choose Edit.
4. Choose Add Device under the appropriate COM port column.
5. Select Meters under Family.
6. Select IQ 200 Series under Model Series.
7. Select IQ250 under Model.
8. Enter a name, such as "IQ250_1" under Name.
9. Set the Serial Address (1-247 decimal) to match the address you set on the meter.
10. Choose Save Device Configuration.
11. Choose Edit.
1 Adding an IQ 250
3 Configuring Device Channels

You can configure installed devices in the following ways:

- Disable the device itself.
- For Eaton Modbus supported devices, enable/disable individual device channels and channel trending.

To make configuration easier, you can multi-select and edit multiple channels.

3.1 Disabling a Device

It is recommended that users disable communications to device temporarily during device configuration. This will stop routine polling of data from that device. This is the recommended procedure if you plan to take the device offline to use a proprietary configuration software to connect to the device through the PXG in pass-through. It is always recommended to stop the gateway from polling data, while using the device's configuration software.

1. Select the Network tab.
2. Click Edit.
3. Select one or more devices. (Hold down the Shift key to multi-select.)
4. In Choose an Action in the sidebar, select Disable Device.
5. Verify that you wish to disable the device.

*Once disabled, just follow this procedure again but select Enable Device.*
3.2 Managing Device Channels

You can enable or disable individual channels for Modbus supported devices added to the PXG.

1. Select the Network tab.
2. Click Edit.
3. Select one or more devices. Hold down the Shift key to multi-select.
4. In Choose an Action in the sidebar, select Channel Mgmt. if you have multiple devices selected, you’ll see a heading in the pop-out something like the following figure.

If you select more than one device, the channel settings shown are for the first device selected only (this device is listed in the pop-up heading). When you save the configuration, those settings are applied to all of the selected devices.

5. Select the channels you wish to manage in the pop-out. You can expand channels to enable/disable minimum, maximum, average, and actual values. You can also select if trending should be active.

6. In the pop-out’s Choose an Action list, you can:
   - Enable or disable all channels for the selected devices.
   - Enable or disable trending for all channels for the selected devices.
   - Copy the current settings from another device to the selected devices.
   - Import or export a file that defines a device’s configuration. You can import the settings file for devices on this PXG or for the same device type on other PXGs.

7. Click Save and Exit.

   Saving a channel configuration file is a great way to back up your channel settings and to easily import them to other devices.

Note:

If using the IQ Eaton Meter Configuration Software (via Modbus pass-through) to modify the IQ250/260 option card configuration:

1) If the IQ250/260 was not added to the gateway before option card configuration occurs, a Gateway reboot is not required.

2) If the IQ250/260 was already added to the Gateway, and then the option card configuration occurs, a Gateway reboot is required.
4 Setting Preferences

Under Settings, you can configure:

- Date and Time
- Localization

Settings is in the upper right of the screen.

3 Click Settings

4.1 Time

If time stamp accuracy on data is important to you, NTP syncronization is the best option. However, you'll either need access to the Internet or you'll need to install an NTP server on your network. The PXG will periodically check the time and correct itself. Under Manually Set Time and Date, choose Set Time and Date to either set the clock to match your PC or set the time and date yourself.

Note: Make sure you set the time zone under Locale as well.

4 Date and Time Settings Showing Manual Selected

4.2 Locale

The PXG was set to United States format for date and to US Eastern Time (UTC-05:00) by default. Set the time zone and date format. As of this time, English is the only available choice. Changing the time zone will not change the time setting.
### Locale Settings

<table>
<thead>
<tr>
<th>Locale</th>
<th>English</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Format</td>
<td>mm/dd/yyyy</td>
</tr>
<tr>
<td>Time Zone</td>
<td>[GMT -05.00] Eastern Time (US &amp; Canada)</td>
</tr>
</tbody>
</table>
5 Network Access Settings

5.1 Access Control

As per factory default settings, ethernet communications defaults to the HTTPS: 443 port, HTTP and Modbus TCP: 80 and 502 ports respectively will remain disabled. You can enable HTTP by accessing PXG through HTTPS access.

You can enable, disable and change these ports. Enable HTTP, you will be warned for unsecure communication.
Warning after HTTP setting is Enabled

If you disable both HTTP and HTTPS, you will be warned before doing so as you could be locked out via ethernet. If you disabled both HTTP and HTTPS, you can not access the web UI and need to perform the Reset from USB to enable HTTPS port and get back the access for UI. Refer to 'Reset PXG' section for more details.
Warning after both HTTP and HTTPS settings are Disabled

You can also set each port so that it can only be used to access the PXG through trusted host names or IP addresses. While using trusted hosts increases security, you must be careful. You can set the gateway to use trusted hosts for HTTP and HTTPS access, and if your PC isn’t at an address on the list you could be “locked out” via Ethernet. You can not access the web UI and need to perform the Reset from USB to enable HTTPS port and get back the access for UI. Refer to ‘Reset PXG’ section for more details.

Note: You must enable Trusted Only for at least one Access Control type in order to save machine names or IP addresses you enter in the sidebar.

To add a trusted host:

1. Choose one of the Trusted Only boxes. This must be selected to save your trusted hosts.
2. Choose Add Trusted Host/IP Address.
3. Enter the name or address and port number in the sidebar.
4. Choose Save Trusted Host/IP.
6 Modbus TCP Server

The PXG can also function as a Modbus TCP server, providing channel data as Modbus registers from both Modbus devices. The device addresses and Modbus maps for these devices can be downloaded directly from the PXG.

6.1 Modbus TCP Server Setup

Server setup is in Settings, on the Network Access tab. Choose Edit to access the configuration settings. You enable the server under the Access Control group (Modbus TCP must be enabled to see Modbus TCP Server Configuration). You can also change the TCP port. To enhance security, enable Trusted Hosts and then add the IP address of each Modbus client using Add Trusted Host/IP Address. Under Modbus TCP Server Configuration, you can set up the way the server responds to client requests. For example you can allow the server to respond to write commands, where appropriate, or not to allow them.
7 Modbus TCP Server Setup

6.2 Viewing and Modifying the Modbus Map

Under Modbus TCP Server Configuration, the View Map button produces a window that lists the various devices attached to the PXG with their Modbus TCP ID. You can sort this list by device name, the native serial address set on the device, or the TCP ID. You can download the contents of the list as a CSV file by choosing Export. Note that you’ll also see INCOM devices in the list. The PXG maps data from all scanned devices, regardless of native protocol, to self-created Modbus TCP registers. The PXG maps data from all scanned devices, regardless of native protocol, to self-created Modbus TCP registers.

In Edit Mode, you can set the Modbus TCP ID for each device. You can also select the Modbus map type for all devices at once, or for each device individually. The possible map types are:

- Legacy PXG-E matches the maps from previous versions of the gateway firmware.
- Fixed reflects the native device map, which may have gaps in the register numbering.
- Efficient provides a register mapping that is optimized to have no gaps. The maximum data value size is 64 bits (4 registers).
- Efficient (32 bit Max size) provides a register mapping that is optimized to have no gaps. The maximum data value size is 32 bits (2 registers).
The download link beside each device provides the Modbus register map for channels in the device configuration file. Before downloading the map, decide if you want a zero based register map and then select the check box. The map contains all of the information you should need, including:

- The register offset.
- The number of registers for the channel.
- The register type.
- Possible values when there is a limited set (such as for boolean and some integer values).
- Whether you can write to the register.
- Provides recommended Modbus Function code for register
- The units for the data.
- Whether the channel data is trendable.

To help you reconcile the register map with the device channels shown in the PXG, the CSV file also contains:

- The device channel name
- The PXG category, such as Power, Current, or Demand.

### 6.3 Pass Through

#### 6.3.1 Modbus

On the Network Access tab, you can enable pass through mode for Modbus RTU ports COM1 and COM2. Doing so allows you to access the full, native Modbus map for the device. These maps are not provided through the PXG, you’ll need to access them from the device documentation.

Note that each Modbus pass through has its own port address. Thus, you can access the full register map for a connected device by simply referencing this port in your TCP connection. When using pass through mode, you must use the actual Modbus Serial Address for the device. This is also listed on the Device Mapping page and in the device list available through the Export button.
7 BACnet IP Server

7.1 Setting up a BACnet/IP Server

Note: Edit must be active to make these changes. The Base ID setting won’t be reflected in the Device Mapping until you save and exit edit mode.

If you enable BACnet/IP, you can present the connected devices as virtual devices on a BACnet/IP virtual network.

Routed Network Number
You must provide the Routed Network Number that will be assigned to the virtual network. Possible values are 1 through 65534. Ask someone in your facility maintenance group that is responsible for maintaining the BACnet network infrastructure for guidance in selecting a Routed Network Number. The Routed Network Number must be unique from all other BACnet network numbers within the BACnet global network.

Caution: If you choose a Routed Network Number that is already in use, communications problems will result.

7.1.1 Base ID for Auto-Assign
This is the base ID value used by auto-assign (if enabled) to assign the gateway and virtual device instance numbers.

7.1.2 Auto-Assign Gateway ID
If enabled, the ID for the gateway is automatically assigned. If you set a Base ID, the gateway will be the base value plus one. If disabled, you can manually set the ID by clicking View Map.

7.1.3 Auto-Assign Device IDs
The various virtual device IDs will be assigned based on the Base ID (if specified) and incrementing from the ID assigned to the gateway. If disabled, you can manually set the IDs by clicking View Map.

7.1.4 BACnet Broadcast Management Device
If you’re using a BACnet Broadcast Management Device (BBMD) to connect your meter to another subnet in your BACnet/IP network, you must also define the BBMD IP address (IPV4 only) to register with the BBMD on the remote subnet. You can also set the BBMD Time to Live value in seconds.
8 BACnet/IP Settings

7.2 Mapping

You can view and download the mapping information for your virtual network and virtual devices by clicking View Map (the download arrow is available only in non-edit mode). If you are manually setting IDs, you can do that in the Device Mapping dialog box. You can also download an EPICS .tpi file for each virtual device.

Click Edit to change the name of virtual device (Object Name) and, if you’re manually setting IDs, to set the ID numbers. You can sort devices by any of the column types. To download an EPICS file for a device, click the download arrow at the right of the device row.
8 SNMP Server

8.1 SNMP Server Setup

Enabling SNMP under Access Control will reveal functionality that allows IT-centric network management software (NMS) to obtain supported Management Information Base (MIB) data directly from the gateway.

12 SNMP Server Enabled

- Port 161 is the standard port used by NMS client software to listen for SNMP responses. Although you may edit this port number, it’s not recommended.
- Access to the SNMP Server may also be restricted to Trusted hosts only, if you choose, for a higher level of network security.
- Once SNMP functionality has been enabled in the Access Control section of the Network Access page, there are a few more configuration items necessary to take full advantage of the SNMP v1 and v3 functionality provided by the gateway.

8.1.1 Enabling SNMP v1 and v3 Support

SNMP v1 and v3 are independently configurable in the gateway, allowing you the choice of configuring and running support for either version, or both, depending on your NMS requirements. SNMP v1 support is notably insecure, since it only restricts use through configured Community Strings. It is recommended that you only use SNMP v3, unless you have a legacy application that still requires the use of v1, e.g. for v1 traps. Once you enable the overall SNMP support from the Access Control section, continue by specifically enabling and configuring v1 and v3 as noted below.

8.1.2 Detailed SNMP v3 Configuration

Enable SNMP v3 support and then continue by configuring the necessary Read-Only and Read-Write User.
### 8.1.2.1 Configuring the Read-Only User

The configured Read-Only User is restricted to only being able to request data from the gateway. Enter a Username for the the Read-Only User, along with a corresponding Passphrase. The Username may be from 1 to 32 characters in length, and may consist of ASCII printable characters 32-127 inclusive. The required Passphrase must be 8 or more characters and is also restricted to ASCII printable characters. For added protection, you may also choose to select the use of the AES128 block cypher for encryption associated with the Privacy feature.

### 8.1.2.2 Configuring the Read-Write User

The configured Read-Write User is allowed to request data from the gateway, as well as to write to data to supported MIB objects. Enter a Username for the the Read-Write User, along with a corresponding Passphrase. The Username may be from 1 to 32 characters in length, and may consist of ASCII printable characters 32-127 inclusive. The required Passphrase must be 8 or more characters and is also restricted to ASCII printable characters. For added protection, you may also choose to select the use of the AES128 block cypher for encryption associated with the Privacy feature.

### Important

Whenever you make a change to the Username for the Read-Only or Read-Write user, you must also reenter an appropriate Passphrase.

### 8.1.3 Detailed SNMP v1 Configuration

Enable SNMP v1 support and then continue by configuring the necessary Community Strings for Read-Only and Read-Write access.

---

#### Note

When SNMP v3 is enabled, the gateway automatically uses SHA authentication.
8.1.3.1 Configuring the Read-Only Community String

Proper configuration of the gateway and NMS requires that there be a community string match before the requested MIB data is returned from the gateway. By default, the commonly used string `public` is provided. However, good security practice recommends changing this string to something specific to your installation and also configuring your NMS with the same.

8.1.3.2 Configuring the Read-Write Community String

Similar to the Read-Only string, the gateway provides the commonly used string `private` for read-write access. Please take this opportunity to change the Read-Write Community string to something more secure for your installation.

8.1.4 Gateway-provided SNMP MIB Support

<table>
<thead>
<tr>
<th>MIBS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>View MIBS</td>
</tr>
</tbody>
</table>

15 Viewing the list of supported MIB files

Clicking on the View MIBS button provides access to downloadable copies of the SNMP Management Information Base (MIB) files supported in the gateway. More specific information is provided below.
8.1.4.1 Eaton OIDs
These objects document all the object identifier assignments for Eaton products. Downloaded Filename: EATON-OIDS.txt

8.1.4.2 Eaton Power Device MIB
This is Eaton's own MIB that includes common measures that most Eaton power-related devices can support. The MIB covers three areas, including:
- Voltage, Current, Frequency, and %Load measures
- Digital (binary) Inputs and Outputs
- Generic (non-specific) sensor readings
Downloaded Filename: EATON-PCD-MIB.txt
8.1.4.3 Eaton Power Meter MIB

This is Eaton's own MIB that includes common measures for power metering devices. The Power Meter MIB covers five areas:

- Power Quality group: PQ Index, % THD for Current and Volts
- ITIC Sags and Surges
- Real-time Measures: Voltage, Currents, and Power measures.
- Min/Avg/Max group for Voltage, Currents, Frequency, and PF
- Energy Measures group: Watt-, VAR-, and VA-hours
- Power Demand group: KW, KVA, and KVAR over the meter's Demand period

Downloaded Filename: EATON-PWR-MTR-MIB.txt

8.1.4.4 Eaton Alarms+Traps MIB

This is Eaton's own gateway-focused MIB with Objects providing a table of active alarms and a count of alarms currently active. The notification traps provided are triggered by the gateway's publishing of an alarm or event.

Downloaded Filename: EATON-PXG-MIB.txt

8.1.4.5 Entity and Entity State MIB Support

The objects in these MIB files provide information standard in the industry:

- The RFC 4133 Entity MIB provides standard objects for identifying and describing the physical devices attached to the gateway. Downloaded Filename: ENTITY-MIB.txt
- The RFC 4268 Entity State MIB provides available status measures for each device, including notifications and traps. Downloaded Filename: ENTITY-STATE-MIB.txt
- The RFC 4268 Entity State MIB Part 2 provides possible state values for the Entity State MIB.

Downloaded Filename: ENTITY-STATE-TC-MIB.txt

In addition, the gateway also supports RFC 1213 MIB-II, providing system and interface-related information.

8.1.5 Configuring v1 Trap Support
### Trap-related configuration

#### 8.1.5.1 v1 Trap Recipient Community String

This string defines a community string that will be associated with the traps generated by the gateway. It can be useful in separating or filtering the traps received by the NMS. If you changed it from the commonly used string: public make sure that you properly configure your NMS to actually see traps tagged with the alternate community string.

#### 8.1.5.2 Enable Auth Fail

If the gateway receives SNMP requests from any SNMP client using community strings that don’t match the configured strings in the gateway, it can send v1 traps that notify the NMS of the attempted communications. Enable Auth Fail notifications here if you wish to receive these traps.

<table>
<thead>
<tr>
<th>Trap Recipient Community String</th>
<th>public</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community string to be sent with trap messages. Defaults to public. Can be used on the receiving end to filter trap messages.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enable Auth Fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables the sending of authFail traps when an SNMP request is received with invalid credentials.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trap Recipients</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234 Hostname/IP Address</td>
</tr>
<tr>
<td>1234123 Hostname/IP Address</td>
</tr>
</tbody>
</table>
8.1.6 Configuring v3 Trap Support

8.1.6.1 v3 Auth Fail Trap

If the gateway receives SNMP requests from any SNMP client using passphrase strings that don't match the configured passphrase in the gateway, it can send v3 Auth Fail traps that notify the NMS of the attempted communications.

8.1.7 Adding or Removing v1 and v3 Trap Recipients

While in the Edit mode, you can enter IP addresses or qualified host names of computers designated to receive SNMP v3 traps from the PXG. Select Add Host/IP Address and entering the information in the field provided to the right. You can also remove Trap recipients. To do so, from Edit mode, select the recipient's IP address from the list and then select Remove.

Alternate Trap Sending Port

The PXG assumes the use of TCP port 162 for sending v1 and v3 traps to the recipient. If a different port number is necessary, you may append the alternate number to the trap receiver's Host/IP Address by adding a : and the port number after the recipient's IP address. For example, if you want to use port 163 instead, you would add the port to the recipient as: 10.222.51.122:163
9 Notifications

Notifications provide email alerts for alarms and related activities, such as acknowledging an alarm, or when an alarm is cleared. Emails can include attached event, trend, and/or data logs.

You set up notifications through Settings, on the Notifications tab. Choose Edit to modify the settings.

9.1 Setting up the Email Server

The PXG can send emails for alarm related events. You can set up your email notifications on the Notifications tab under Settings. Choose edit to access the setup fields. Setup requires that you define:

- The address of the email server.
- The username and password (if required) for the email account used by the PXG. It’s best if you use a username with a password that doesn’t change. If the password for that user changes, you’ll need to reset it here. Otherwise, Notifications will no longer work.
- The port. You append this to the IP address/machine name by first entering a colon. For example: 10.20.30.1:587. By default, port 25 is assumed (which is typical for unsecured connections, although it could be 587). If you are using SSL, the port is typically either 465 or 587. Always check with your IT group for the proper port number to use.
- The address from which the PXG sends its emails.
- Whether SSL/TLS is required.
9.2 Adding Recipients

19 Adding a New Email Recipient

1. In Edit mode, choose Add New Recipient.
2. In the sidebar enter the recipient’s email address.
3. HTML provides nicely formatted emails, but only works if your email system allows it (most do). Plain text provides emails in ASCII text.
4. Attachments defines what log information is included with the emails. Logs are sent as email attachments and are in CSV or plain text format.
5. For the alarm emails (only the Active alarm emails), the Alarm Log is attached if selected. It will contain the alarm data for the last 60 minutes. The other attachments are not applicable for the alarm emails.
6. The daily summary email includes all the selected attachments. If selected, the Alarm and Trend logs will contain data from midnight to the previous midnight. The other (audit) logs will contain the full log contents, not just data from the 24 hours, unless the content is extensive then it will be truncated to only contain the more recent data. The full content of the alarm and trend logs, including the older records, can be retrieved via export functions from the PXG’s web interface.
7. Use Real-Time Notifications to set what events trigger an email. Emails can be sent when an alarm is active, an alarm is acknowledged, or the alarm condition clears. You can receive emails for normal alarms, priority alarms, or both.

8. Selected Devices chooses the devices that will trigger notifications. You can choose All Devices or create a list of Selected Devices. You can add individual devices by selecting them in the sidebar and then selecting their channels. If another notification is similar, use Duplicate Notification and then modify the copy. If you don't choose Save Notification, a reminder will pop up when you switch to something else.

9. Notification Recipients lists all of the currently configured notifications.

Note: to send recipients email notifications when waveforms become available, select the Waveform Available channel (in the Operations category) for the device providing the waveform, as shown in the following figure.

![Selecting the Waveform Available channel.](image)

9.3 System Use Notification

Use the System Use notification to display a system use warning whenever a user first accesses the PXG web interface. This message appears before logging in and the user must acknowledge it. Companies can use the warning to let the user know who is legally allowed to log into this system and state what are the legitimate uses of this particular PXG device at this facility.
10 Users and Access Control

Note: For information about the Session Timeout, Max Concurrent Logins and Auto Re-login on the Security tab see Cybersecurity Hardening the PXG.

Controlling access to the PXG is a vital component in any effort to secure it. Many regulatory agencies and standards organizations now recommend or require Role-Based Access Control (RBAC) as part of any access control effort. To support this, the PXG has a robust set of tools that can be used to create the set of users and role-based permissions you need to comply with security policies in effect at a site. Before jumping into user and role setup, review all policies to ensure a good understanding of the access control requirements for the site.

By default, the PXG comes with two users:

- **Admin**: has access to all functions and can edit anything (admin role). Default password for the admin account is admin.
- **User**: can view any information on the tabs, but can’t access Settings or edit anything. Default password for user is user.

Before doing anything else, change the default account names and logins. Not only are these default users not compliant with RBAC, keeping them is a security vulnerability. It is a best practice to replace these accounts with RBAC compliant ones to meet the needs of your security policy.

Note: Should the need arise, you can always use the reset button on the PXG itself to reset the user set to the defaults. You’ll lose all of the users and roles you’ve created, but you’ll regain the two default users along with their login names and passwords.

### Security Tab

![Security Tab Image]

1 https://confluence-prod.tcc.etn.com/display/UD/CybersecurityHardeningthePXG+vPSI14
2 http://cipt0534.nam.ci.root:8090/display/UD/CybersecurityHardeningthePXG+vpsi9a
10.1 Building Roles

You should define roles that fit your organization’s security policy. Permissions can be appropriately assigned to each type of role. Users should be assigned roles, such as Engineer or Operator, based on their responsibilities. Each user can have only one role.
Roles are typically named for the job function they represent. The default set of roles includes job functions such as Operator and Service Engineer. You can create your own roles or redefine the defaults to fit your own security policy.
To create a role:

1. On the **Security** tab in **Settings**, click **Edit**.
2. Click **Edit**.
3. Click **Add Role**.
4. Enter the **Role Name** in the sidebar. This should describe the job function so that everyone in your organization knows what tasks this role is required to do.
5. Select the various permissions the role requires. Permissions are detailed in the following table.
6. Click **Save**.

### Permission Details

<table>
<thead>
<tr>
<th>Permission Details</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View devices and channels</td>
<td>View devices and information from their channels. Every user gets this by default.</td>
</tr>
<tr>
<td>Acknowledge alarms</td>
<td>Click the Acknowledge button and enter a note about the alarm; e.g., what caused the alarm and what action was taken.</td>
</tr>
<tr>
<td>Configure device channels</td>
<td>Enable trending for channels (where trending is available), set alarm triggers, and enable or disable individual channels.</td>
</tr>
<tr>
<td>View settings</td>
<td>View, but not change, PXG settings. This is automatically selected if you select Change settings.</td>
</tr>
<tr>
<td>Change settings</td>
<td>Change PXG settings in the various Settings tabs.</td>
</tr>
<tr>
<td>Install</td>
<td>Install devices in the PXG and update the PXG firmware.</td>
</tr>
<tr>
<td>Configuration file save/restore</td>
<td>Save all configuration information to a file and set all PXG configuration parameters from a configuration file.</td>
</tr>
<tr>
<td>User Role</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Troubleshoot</td>
<td>Remotely reboot the PXG. A role with this permission may be required by Eaton personnel to service/troubleshoot the gateway.</td>
</tr>
<tr>
<td>Minimal control</td>
<td>Issue device commands that don’t have control capabilities. The following figure shows the set of device commands available for the Eaton EDR 5000 with both this permission and with the addition of the Operational control permission.</td>
</tr>
<tr>
<td>Operational control</td>
<td>Issue device commands, such as opening or closing breakers or resetting breaker trips. Also associated with configuring DIM KYZ settings.</td>
</tr>
<tr>
<td>View users</td>
<td>View users and their assigned roles. This includes anything that lists users, such as the Audit logs. Also, view the individual permissions assigned to a role.</td>
</tr>
<tr>
<td>Manage users</td>
<td>Create or delete users, as well as assign a role to each user. Also, create and delete roles and assign permissions to roles. View users is automatically selected if you select Manage users, as you must be able to view the users to manage them.</td>
</tr>
</tbody>
</table>

### 10.2 Creating Users

2. Click Add User
3. Fill in the fields on the sidebar. Note that you can assign only one role to each user.
4. Click Save.

### 10.3 Deleting Admin and User

After you’ve set up the various roles and users, log in as a user with a role that contains Manage users. You can now delete both the user and admin users and the admin role. Users can only be deleted if they are not currently logged in.

**To delete a user:**

2. Click the user that you wish to delete.
3. In the sidebar, click Remove.
4. Click Save.

You can delete a Role if it is not assigned to any users. If you get an error a message when you attempt to delete it, check if any users are assigned to that role and then reassign them.

**To delete a role:**

2. Click the user that you wish to delete.
3. With the User or Role selected, click **Remove** to delete it. If the Remove button isn’t active, the role is in use or the user is logged in.

4. Click **Save**.

### 10.4 Accessing Logs

You can restrict or provide access to the various Audit Logs using permissions. The following table lists each of the Audit Logs and the permissions required to access them. Any of the listed permissions will allow the user to download that Audit Log file.

<table>
<thead>
<tr>
<th>Audit Log Name</th>
<th>Any of These Permissions Allow Log Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy</td>
<td>View users</td>
</tr>
<tr>
<td>User</td>
<td>View users</td>
</tr>
<tr>
<td>Device</td>
<td>View users, Install, Configure Device Channels, Troubleshoot</td>
</tr>
<tr>
<td>Configuration</td>
<td>View users, Install, Configure Device Channels</td>
</tr>
<tr>
<td>Session</td>
<td>View users</td>
</tr>
<tr>
<td>Command</td>
<td>View users</td>
</tr>
<tr>
<td>Update</td>
<td>View users, Install, Troubleshoot, Configuration file save/restore</td>
</tr>
</tbody>
</table>

### 10.5 Roles and Permissions Cookbook

The following are examples of how to combine permissions to create roles that make sense in your organization. The examples explain four of the default roles in the PXG. These default roles may not be a good fit for your security policies; however, discussing what they allow and how the permissions work can help you in picking the right permissions when you create your own roles.

### 10.6 Security Audit

This role must be able to view the various audit logs for the system as well as verify the set of users and their roles. In addition, this role must allow the user to verify the settings in the PXG. However, unlike a true administrator, users with this role only view this information; they cannot edit any settings. You can grant these capabilities through the View users permission. View users allows the user to view the **Security** tab under **Settings**. It also lets them see all of the logs listed under the **Audit Logs** command on the **Choose an Action** list in the **Network** tab. This command is available when the gear icon for Power Xpert Gateway is clicked.

### 10.7 Security Admin

This role must be able to create/delete users and roles, as well as change user passwords or other settings. Its permissions (and capabilities) are similar to the Security audit, but with the added capabilities for user administration. So, in addition, the following permission has been added:
Manage users: This lets the user not only view the current users and roles (View users is selected automatically when this is selected), but create, edit, and delete them as well.

10.8 Engineer

An engineer must be able to control everything related to the various devices that are connected to the PXG. However, an engineer doesn't need to access any of the security or maintenance features of the PXG. Therefore, that role has the following permissions that are related to working with devices.

Change settings: This setting permits the user to view Settings (which is automatically selected when Change settings is selected). It also unlocks the various fields in the sidebar within the Network tab.

Install: This lets the user add and edit devices.

Configure device channels: As the name implies, this permission allows the user to edit the list of device channels. It also allows the user to remove a device and configure the Modbus and INCOM ports.

Acknowledge alarms: The user can click the Acknowledge button and enter notes about the alarm.

Minimal and Operational control: The user can issue all available device commands through the Choose an action menu.

10.9 Service Engineer

In addition to what an Engineer can do, the Service Engineer must be able to troubleshoot and remotely reboot the PXG. This user must also be able to save and restore a configuration file. So, added to the permissions granted an Engineer, the Service Engineer also has Troubleshoot (remote rebooting) and Configuration file save/restore permissions. Eaton field service and customer support personnel may require a user with this role to help troubleshoot a PXG.

10.10 IoT Agent

An IoT agent role has the following permissions that are related to working with devices.

Change settings: This setting permits the user to view Settings (which is automatically selected when Change settings is selected). It also unlocks the various fields in the sidebar within the Network tab.

Install: This lets the user add and edit devices.

Minimal and Operational control: The user can issue all available device commands through the Choose an action menu.

10.11 Password Policy

The security provided by restricting access to authorized users is only as strong as uniqueness of the user passwords. The Password Policy settings provide a mechanism for security administrators make it more difficult for unauthorized users to guess the passwords of their users. It also provides a mechanism to control how often users must change their passwords. This single password policy applies to all users in the system.

To change the password policy:

2. Expand the Password Policy section.
3. Change any of the settings.
4. Click **Save**.

After changes are made, any attempts to make password changes (e.g., from the Security tab or Change Password dialog) will be restricted by the new policy settings. Existing passwords will continue to work even if they don’t meet any new content and length requirements, but all accounts will be immediately affected by the password history, age and grace period settings. New password requirements may be enforced to via **User Password Management** settings. Users will be prompted to change their password at their next login. New password policy settings are also available for users are Max Failed attempts, Failed Login Attempt Window and Failed Login Wait.

Note: PXG firmware now supports minimum password length of 6. Previously, the minimum length was 4. Existing (shorter) passwords are still valid, but any changes require a new minimum length of 6.

22 Password Policy

10.12 User Password Management

The security administrator may use the **User Password Management** settings to view and modify password expirations and lockouts for each user individually. The per user management provides a way to extend the global **Password Policy** choices; the administrator can override the **Password Expires** time or choose a **Expiration Date** instead. By setting a fixed expiration date, the administrator is saying the user’s account will be locked at the start of the fixed date versus just requiring a password change as is the case when the **Password Expires** field is set to a number of days.

This sidebar also provides the ability to immediately lock (or unlock) a user account and the ability to force a user to change the password on next login (vs. waiting for the password to expire).

To change a user’s password settings:

2. Expand the **User Password Management** section.
3. Click the user that you wish to modify.
4. Change any of the settings in the sidebar.
5. Click **Save**.

Note, when a user’s account has become locked due to password expiration, the account must both be unlocked and the password must be changed so that it doesn’t immediately get locked again. It’s also typical to set the "**Require Password Change**" flag so the user can replace the password with one of their own.

### 10.12.1 Password Expiration Changes

If the password expiration is changed from "never" to some finite time on an existing product, existing users who haven’t changed their passwords in a long time may get locked out immediately at that time. That can be a problem, especially if this change happened automatically as part of a firmware upgrade. (The same problem can happen if you change password expiration in the UI). So to mitigate this, the following actions cause a user’s expiration date to be re-evaluated:

1. Changing user’s password.
2. Editing user’s properties.
3. Editing global password policy (whether expiration time or something else like "require special characters") re-evaluates all users.

---

**Image Description**

The image shows a screenshot of a user password management interface with various settings and options related to password expiration and management. The interface includes fields for setting password requirements, expiration dates, and user-specific password changes. It also provides an overview of current user password settings and expiration dates.

---

23 User Password Management
11 Advanced Administration

Several advanced administration actions are available on the Network Tab. You can access these actions by clicking the row with your gateway's name (or additionally, by clicking the gear icon for the gateway while in Edit mode). The Choose an Action menu is in the sidebar. Depending on your user permissions and whether or not edit mode is active, you may see any of the following actions.

11.1 Choose an Action Functions

- **Advanced Network Settings**: This is a link to the Network Access tab under Settings.

- **Configuration File Save/Restore**: You should always save a configuration file to your PC after setting up the PXG. You can also reload configurations with this function. If you’re replacing an original PXG-A or PXG-E model gateway, this feature may also be used to restore a saved configuration from the older gateway.

- **Firmware Update**: Check the [eaton.com/PXG](http://eaton.com/PXG) web site for firmware upgrades. You can download the new firmware file from there and use this function to upload it to the gateway. When you upload new firmware, the gateway will reboot after updating itself.

---

3 [http://eaton.com/PXG](http://eaton.com/PXG)
Reboot Gateway: This provides a handy way to reboot a PXG without accessing the box directly. You’ll lose web contact during the rebooting process.

System Inventory: Provides an inventory of all of the devices attached to the gateway, including information such as connection port, status, and firmware level.

Ping Test: Use this to verify that there is an Ethernet connection between the PXG and another device, NTP server, SMTP server, or Power Xpert Insight software.

Audit Logs: The following section lists the various available logs.

Download Comm. Events & Download Comm. Statistics: These download diagnostic information about PXG communications as CSV files.

### 11.1.1 Audit Logs

The following audit logs are available to users, depending on the permissions (see page 35) their account has been granted, and provide:

**Legacy** – Older style audit log format supported by previous versions of the gateway's firmware. Newly logged data will appear in the more specific log files.

**User** – Content related to changes made to users or roles, including password changes.

**Device** – Content related to the addition, removal, enabling, and disabling of connected devices.

**Configuration** – Content related to individual changes to system setup; e.g., device or channel settings, time zone, etc.

**Session** – Content related to logins/sessions, including login failures and invalid (possibly malicious) access attempts. This also includes valid and invalid non-HTTP protocol sessions, including Modbus/TCP and BACnet/IP.

**Command** – Content related to user actions, such as commands and gateway reboots.

**Update** – Content related to the application of firmware updates, configuration file uploads, and factory resets of the gateway.
25 Audit Logs
12 Setting Alarms

You can set custom alarms for any channel on any connected device directly in the PXG. Each alarm configuration references values on a single channel and specifies either:

- A High or Low alarm value for analog channels.
- A Between value for power factor channels (explained below).
- An On Value trigger that matches a state in a multi-state alarm.

If you wish to have both High and Low alarms set for a single channel, create an alarm configuration for each. You configure alarms through Settings, on the Alarm Settings tab.

12.1 Creating an Alarm Configuration

1. Click Edit.
2. Click Add Alarm Configuration. A sidebar appears with all of the alarm settings.
3. Select the device from the drop down list.
4. Select the channel type; i.e., Voltage, Current, Power Factor, etc.
5. Select the individual channel.
6. For analog channels other than power factor, choose whether it’s a High or Low alarm, then set the alarm trigger value. For Boolean channels, set whether to trigger an alarm on either True or False. Other discrete multi-state channels may have more than two options, e.g. the Status channel on many of the devices. See below for more about multi-state alarms and alarm levels.

   Power factor channels have a "Between" setting that applies to both positive and negative power factor. So, if you set power factor to 0.90, any value less than that will raise an alarm for both positive and negative power factor. Like other analog alarms, power factor alarms are automatically assigned a level.

7. Type a custom message that will appear with this alarm.
8. Set Suppress Changes less than to eliminate alarm "chatter" (rapid oscillation above and below the trigger point) by setting a dead band value.
9. Choose if the alarm should be acknowledged automatically if the value falls outside the trigger range.
10. Choose if the alarm will be a Priority Alarm. Priority alarms are shown with an exclamation point and you can filter on these in the Alarms tab.
11. Save the Alarm Configuration when you're done. If you're going to create a similar configuration, choose Save and Duplicate Alarm. You can then just edit the fields in the copy to create a new configuration.

27 Creating an alarm configuration
12.2 Alarm Levels

Every channel can have multiple alarm triggers (not just High and Low). Each time you define an additional High or Low alarm trigger point for a particular analog channel, it automatically becomes a new alarm level. The alarm level is assigned based on the comparative values of the trigger settings. For High alarms, greater values have higher levels. The opposite is true for Low alarms. The following table shows how this works:

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>144 VAC</td>
<td>2</td>
</tr>
<tr>
<td>High</td>
<td>132 VAC</td>
<td>1</td>
</tr>
<tr>
<td>Low</td>
<td>108 VAC</td>
<td>1</td>
</tr>
<tr>
<td>Low</td>
<td>96 VAC</td>
<td>2</td>
</tr>
</tbody>
</table>

The following figures show the alarm logic and how this is affected by alarm levels. Examples for both latching and non-latching alarms are given.
12.3 Setting Alarm Level for Multi-State Channels

Multi-state channels, such as Status, can't be automatically assigned a level. Instead, you must assign the levels yourself when configuring alarms for such channels. When configuring multi-state channels, the dialog box includes an Alarm level field for this purpose. For multi-state alarms there is no High or Low alarm, just a single set of alarm levels. Note that you cannot assign the same level to two alarms for the same multi-state channel.
30 Alarm level field for multi-state channels
13 One-lines

One-lines are the way to group electrical devices and creating One-lines is the first step to creating a graphical representation of your system on the One-lines tab.

13.1 Creating One-Lines

1. Click Edit on the One-lines tab in Device Tree view.
2. Click Add One-line, and a new One-line will appear with the name "New Location." You can update the name in the sidebar. You can arrange the device tree by dragging:
   • Between One-lines to change order.
   • Over a One-line to nest.
   • From the All Devices section into the One-lines.

13.2 Adding Devices to One-Lines

You add devices to the One-lines in the same way: drag a device over a One-line and drop it.

13.3 One-line Diagrams

There are two types of One-lines:
   • Location only One-lines, which simply contain link symbols to other, nested One-lines. Users click a link to navigate to its One-line.
31 Location only one-line

- Electrical One-lines, which you can draw quickly using the PXG's Auto-draw technology. Auto-draw is assisted drawing, where the PXG does much of the work in creating a One-line for you yet still provides you with control over the drawing.
### 32 Electrical One-line

The PXG helps you create diagrams on a One-line through a feature called "Auto-draw." Auto-draw dramatically reduces the time it takes to create an electrical One-line diagram. It not only sets up the starting point for your One-line diagram, it helps you connect devices in the diagram as you edit. How Auto-draw behaves is based on the following configuration settings:

#### 13.3.1 Number of Sources

If you don't want to automatically add a source, select Zero Sources. If you choose One source, Auto-Draw adds a source symbol in the upper left and connects all devices to this. Choose Two sources and a second source symbol appears in the upper right. Once sources are created, you can place them anywhere you like. Devices will automatically connect to the closest source. If you've chosen Zero Sources, you can still add lines and symbols to the page.

#### 13.3.2 Tie Breaker Symbol

You can add a tie breaker to your diagram if you have two power sources. This is automatically centered on a horizontal tie line in the upper half of your one-line diagram. Choosing Low or Med (Medium) Voltage changes the symbol appropriately. Choosing blank provides a place to drag an actual breaker device into that position. You can also drag any of the colored medium voltage breaker symbols there.
13.4 Using Auto-Draw

When you enable Auto-Draw for one or two sources, Auto-Draw automatically connects all devices on their closest source symbol. As you drag a device across the center of the screen, its connection line automatically snaps to the other side. Each device has two parts that you can position: the device box and the connection symbol. If you drag the device box, the symbol follows. However, if you drag the symbol, it moves independently from the device box.

If you double click a symbol, both it and the line connection points flip by 90 degrees. The exceptions are the vertical and horizontal line symbols (which do not flip) and the Lettered Circle symbols (the letter doesn't flip but the connection points do). When you click on a device in edit mode, the side bar changes to allow you to remove the device. To go back to the configuration for the current one-line, click on any blank spot in the diagram.

13.5 Working with Symbols and Graphics

- When you click one of the Additional Symbols in the sidebar, it appears in the upper left of the screen. From there, drag it to the appropriate location.
- Symbols and graphics flip just like the symbols on top of devices. Just double click them.
- You can delete a symbol by clicking the "X" in the upper right corner of its selection box.
- Click Save to save your changes so far without leaving edit mode. Click Edit to save and exit or cancel all changes and return to viewing mode.

You can view a video detailing how to use the one-line tools by clicking this link: http://bcove.me/9cyfwx0
14 Connecting to the Web Interface

After the PXG is fully configured, users can interact with the web interface. This is best viewed in either Google Chrome (current version) or Microsoft Internet Explorer 11. Users should have a screen resolution of at least 1280 x 1024 pixels. The connection is https://machine_name where machine_name is the machine name or IP address of the PXG. You can also use HTTP to connect, if that's enabled, although Eaton recommends that you only connect via HTTPS. For information about enabling HTTPs, see "Cybersecurity Hardening the PXG".
15 Network Tab

The Network tab shows all of the devices attached to the gateway. These are grouped under their communication port. Devices are color coded based on status:

- Red shows that there are alarms from one or more channels for that device.
- Orange means that the device is no longer communicating.
- Purple means that a device is disabled.
- Black means the device is communicating.

Click a device to see its top 16 channels in the sidebar. Any channels in alarm show as red here too.
33 Sidebar, showing channels and values

15.1 Choose an Action

The Choose an Action list can provide some of the following functions (what shows depends on the device).

- Device Details (pop-out)
- Trend Viewer (pop-out)
- Trend Export
15.2 Device Details

You can see more about a device through the Device Details. This is available under Choose an Action. The first section shows the top 16 channels. The last section shows All Channels from the device. Channels are organized into groups by electrical measurement category. You can also launch the Waveform export and capture dialog box as well as the Trend Viewer through Choose an Action.

Export Waveform saves a Comtrade file with waveform data from the chosen captured waveform(s) to your computer file system. Export Trends saves a .csv file with trend data from that device. For Export Trends you can either export data from the top 16 channels or all channels.

Each device has its own particular set of Commands. For example a device might have commands such as these:

- Reset Energy: resets the accumulated energy values to zero.
- Reset all Min/Max Values: resets these calculated values and begins calculating again from this point in time.
Network Tab

34 Device Details
The PXG shows alarms when devices indicate something is wrong. Devices with alarms are shown as red in the Network Tab. If there are any open alarms on the PXG, there will be an alarm callout at the top of the page indicating the number of open alarms (shown above). Priority alarms are shown with an exclamation mark in a red box.

The Alarms tab shows all alarms from the selected time range (the default is 48 hours) plus all open alarms. Initially, when you click the Alarms tab, all Unacknowledged alarms for connected devices and all Active alarms are shown. Users acknowledge alarms to indicate they've seen the problem. You can acknowledge alarms individually using the acknowledge button. Alarms are active when the condition that caused the alarm is still present. Even if an active alarm has been acknowledged, it still shows under Active alarms until the condition goes away.

While alarms are initially sorted by date, you can also sort them by device or priority. The current time range for alarms in the list is shown next to the calendar button. You can filter the list to show a specific date range. You can further filter the list to show active alarms, acknowledged alarms, or unacknowledged alarms. Any open alarms will always be shown, regardless of when they occurred.

The Export button on the Alarms tab downloads a CSV file containing an alarm log. You can limit the date range for the alarm or the number of alarms in the file. When an alarm is selected, you can use the Choose an Action button in the sidebar to export just the information about that alarm as a CSV file. Use Alarm Details to view a pop out with all information about the alarm, including its history.

You can acknowledge alarms in groups using the check boxes, then clicking Acknowledge at the top. The top check box will select all. Past alarms are always available for viewing by selecting to show all alarms and All Dates.
17 Trend Viewer

You can launch the Trend Viewer from the Choose an Action menu in the sidebar. Choose Add Device to include any installed device that has trend data. Choose Add Channel to select a channel from the device. Channels are arranged in categories. Clear a check box to remove a trend line for that channel.

To zoom, select the Zoom button then click-and-drag. Dragging left-or-right zooms along the horizontal axis, while dragging up-or-down zooms along the vertical axis. Click the Zoom Out button to return to the default view.

To pan, select the Pan button and then click the left or right arrows. There are a few other controls:

- Use the calendar control to select the date or time range.
- Place the cursor over any point on the graph to see its value and time stamp.
- Click the Export Chart button to save a .png file snapshot of the graph to your local file system.
18 Waveforms

Waveform support is also available from Eaton’s PXM2280 and PXM2290 power quality meters when connected to the PXG via Modbus RTU. Supplimental documentation for this application is available at https://eaton.com/pxg.

18.1 Waveforms Captured by Devices

Devices have their own waveform capture settings that control what triggers a waveform. You can’t set this from the PXG. Also, what information is captured varies on a device-by-device basis. As such, the first step in using waveforms within the PXG is to configure each of the devices through their own interfaces, then enable Waveform capture in the PXG.

18.2 Enabling Waveform Capture in the PXG

The Device Configuration sidebar has the Enable Waveform setting, and you can access this through the Network tab as follows:
1. Click Edit.
2. Select an COM device that supports waveforms.
3. Select Enable Waveforms in the sidebar.
4. Click Save Device Configuration.

18.3 Captured Waveforms List

The PXG maintains a list of all waveforms captured for each device, from which you can download any waveform as a set of Comtrade files. The easiest way to access the list is through the Network tab. Each COM device that has captured waveforms shows the following waveform icon. You can click the icon to launch the Waveforms list pop-out.

![Waveform Icon]

To help find the waveform you’re looking for you can sort the list by time captured or received, as well as by cause. If you’re looking for a specific file, you can also sort by filename. Select the checkbox for each waveform that you wish to download or select the master checkbox (beside the Export button) to select all of the waveforms.

When you click Export, you'll see a file Save As dialog box for each selected waveform so that you can rename each file or save them to various folders. If you have a large number of files selected, you may wish to download these a few at a time; otherwise, you’ll have to deal with an equally large number of Save As dialog boxes.

18.4 Waveform Files

The Waveform files themselves are packaged in a .tgz compressed tar archive file. Unpacking this in Windows requires special software such as 7-Zip. When you unpack the file, you may need to first decompress it and then unpack the resulting .tar file. Each waveform archive unpacks into a set of four files with the following extensions. .hdr, .cfg, .dat, and .inf. Your Comtrade viewer may not require all of these.
Available Space
The PXG allocates 100MB of internal space for saving waveform files. This is enough storage for approximately 300 waveform files. Roll-off of older waveform files occurs automatically as the available waveform log space is filled.

18.5 Manual Waveform Capture
If you wish, you can initiate a waveform capture from an enabled device. This is under the Command section of the Choose an Action menu within the sidebar. The sidebar is available on the Network or One-lines tab when the device is selected. You can also access the menu on the Device Details pop-out.

18.6 Signing up for Waveform Email Notifications
To receive emails notifying you of available waveforms:
35 Adding a New Email Recipient

1. In Edit mode, choose Add New Recipient.
2. In the sidebar enter the recipient’s email address.
3. HTML provides nicely formatted emails, but only works if your email system allows it (most do). Plain text provides emails in ASCII text.
4. Attachments defines what log information is included with the emails. Logs are sent as email attachments and are in CSV or plain text format.
5. For the alarm emails (only the Active alarm emails), the Alarm Log is attached if selected. It will contain the alarm data for the last 60 minutes. The other attachments are not applicable for the alarm emails.
6. The daily summary email includes all the selected attachments. If selected, the Alarm and Trend logs will contain data from midnight to the previous midnight. The other (audit) logs will contain the full log contents, not just data from the 24 hours, unless the content is extensive then it will be truncated to only contain the more recent data. The full content of the alarm and trend logs, including the older records, can be retrieved via export functions from the PXG’s web interface.
7. Use Real-Time Notifications to set what events trigger an email. Emails can be sent when an alarm is active, an alarm is acknowledged, or the alarm condition clears. You can receive emails for normal alarms, priority alarms, or both.
8. Selected Devices chooses the devices that will trigger notifications. You can choose All Devices or create a list of Selected Devices. You can add individual devices by selecting them in the sidebar and then selecting their channels. If another notification is similar, use Duplicate Notification and then modify the copy. If you don’t choose Save Notification, a reminder will pop up when you switch to something else.

9. Notification Recipients lists all of the currently configured notifications.

Note: to send recipients email notifications when waveforms become available, select the Waveform Available channel (in the Operations category) for the device providing the waveform, as shown in the following figure.

36 Selecting the Waveform Available channel.

18.7 Waveform Link in Email Notifications

When waveforms are manually or automatically generated, you should receive an email in your inbox similar to the following. Such email notifications contain a link to download an associated waveform file, if such a file is available. Clicking the link opens a log-in page for the gateway.
37 Typical Email Showing Waveform Link

After authenticating you'll see something like the following page, which you can use to download available waveform files. The Home page button will take you to the gateway interface.
The three asterisks following a waveform file in the list denotes that this is the file associated with the email notification you received.

38 List of Available Waveforms
19 One-lines Tab

The One-lines tab shows all of the devices in your facility, organized as either a Device Tree or in Graphic View.

19.1 Device Tree

Device Tree view is similar to viewing devices in the Network tab. The main difference is that in the Device Tree, devices are grouped and ordered the way you wish instead of by connection. Click an alarm icon to jump to the Alarms tab and view that particular alarm. Click the graph icon to launch the Trend Viewer and load that device. For detailed information about the Choose an Action list, see "Choose an Action and Device Details".

19.2 Graphic View

Graphic view shows your system as either:

- One or more link objects which lead to child One-lines.
- One or more electrical One-line diagrams. These can also contain links to child One-lines.

19.3 Link Objects

Link objects have a network symbol, as shown below. To navigate through link objects, just click them. As you navigate down through a branch of the tree, the "bread crumbs," indicate your current position. You can return to any level by clicking it in the bread crumbs.

19.4 One-line Diagrams

These diagrams show your electrical system as it is connected. Each device has both a symbol to show what type of device it is as well as a device box, which shows the top four channels. The following shows two devices, a meter and a breaker, in a One-line diagram. When you click a device, the device highlights and the side bar shows the top 16 channels and provides a series of commands, some of which are device specific, under the Choose an Action List.
Every device has the following commands:

**Device Details**: This produces a pop-out window that shows all of the channels available for that device, organized by channel type. It also includes navigational controls and (for convenience) the same set of controls in the device sidebar.

**Channel Management**: This shows which channels are currently active and which channels have trending enabled. If you are an Admin user, you can click Edit and enable or disable channels and trending.
Channel Management

Trend Viewer and Trend Export: This launches the Trend Viewer pop-out, preloading the selected device. For more information on the Trend Viewer, see "Trend Viewer". You can also export the trend information as a CSV file.

Commands: The various Commands listed are specific to that type of device. These are only available if you are logged in through the Admin account. The following example figure shows the set of commands for a Digitrip.
<table>
<thead>
<tr>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Close Request</td>
</tr>
<tr>
<td>Open Request</td>
</tr>
<tr>
<td>Reset Peak Demand Currents</td>
</tr>
<tr>
<td>Reset Trip</td>
</tr>
</tbody>
</table>
20 Reset PXG

You can select factory reset from user interface which will clear all Network settings, One-line and Users for a PXG.
You can re-connect to gateway with DHCP IP address after factory reset.

Factory Reset gateway setting command

PXG 950 can be reset to factory default via USB port. Follow the steps below to reset device via USB.

1. Open a new file in a text editor. Type the serial number of the device to reset for e.g. ‘2H2FM42’
2. Save this file to the USB drive with the name ‘loadfactorydefault’ (no extension).
3. Connect USB to device
4. Power Cycle the device
5. Remove USB when completed
6. All Device Settings are reset network configuration is set to ‘Wired DHCP’
7. Use Advanced Scanning tool or NMAP command to get the new IP of the device
8. Access the device with factory default credentials (Username - ‘admin’, Password - ‘admin’)
   • Note: Single partition FAT formatted SD card should be used
21 Certificate Management

21.1 Certificate Generation
Certificates play a crucial role in keeping communication secure. These certificates are sent out when communication starts. The other end will receive this certificate and will validate it. If the other end finds the certificate valid and trusted, that will allow for further communication. Otherwise, the device will reject the communication.

1. A certificate can be generated for one service (i.e. HTTPS service) by signing it from another service (i.e. PKI service).
2. User can generate self-signed signed certificate for a service (e.g. HTTPS).
3. User can Import, Export and Revoke certificates. They can also generate Certificate Signing Request (CSR) files, which can be CA signed and then re-imported into the Certificate Manager.

21.2 Certificate Upload
1. Users can get a CA-signed certificate from a third party and upload that for any service (e.g. HTTPS). These CA certificates can be used by the service to validate the issuer, and allow communications to begin.
2. Users can upload certificates of any trusted devices. Uploading a device’s certificate to the PXG classifies that device as a trusted client and authorizes communication.

Certificate Re-Generation
1. Any server certificates (e.g. HTTPS) generated by the Certificate Manager will automatically be regenerated upon expiration.
2. If a previously uploaded CA-signed certificate expires, the Certificate Manager provides the ability to generate a self-signed certificate for a service (e.g. HTTPS).
3. For a network change, the network dependent certificates (e.g. HTTPS service certificate) are created/reloaded.
4. With a system date/time change, the certificates will be revalidated. Expired certificates will be automatically regenerated.
5. If a certificate was signed by a CA service (e.g. PKI), then the certificate will be renewed automatically if its CA certificate (e.g. PKI) gets renewed.

Note: Currently HTTPS service is configured by default for generation of self-signed signed certificates. Users may enable the generation of self-signed certificates for services like Modbus, BACnet, Email and IoT Agent.

The Certificate Manager module is located at Settings → Security → Certificate Management.
21.3 Operations Supported by the Certificate Manager UI

21.3.1 Listing of Server Certificates

The first list of certificates in the Certificate Manager module is the Server Certificates.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used For</td>
<td>The PX Red Service that uses that certificate.</td>
</tr>
<tr>
<td>Issued By</td>
<td>PKI that issued the certificate.</td>
</tr>
<tr>
<td>Issued To</td>
<td>Protocol/Data Server that certificate was issued to.</td>
</tr>
<tr>
<td>Valid From</td>
<td>Date the certificate became valid. MM/DD/YYYY format.</td>
</tr>
<tr>
<td>Expiration</td>
<td>Date the certificate becomes invalid and expires. MM/DD/YYYY format.</td>
</tr>
<tr>
<td>Status</td>
<td>Valid state of the certificate.</td>
</tr>
</tbody>
</table>

21.3.2 Viewing Details of Certificates

To view the details of a certificate, click on the certificate of interest. A panel listing all of the certificate details will open on right side of the browser. All details can be viewed by using the scroll bar on the right side of the panel.
21.3.3 Export Server Certificate

To export a server certificate, click the certificate of interest. The Export button then becomes visible. When clicking the Export button, the certificate is downloaded as a CRT file using the string in the Used For field as the file name. In the example below, the Export button will download the certificate in a file called "https.crt".

21.3.4 Generate New Self-Signed Certificates

To generate a new self-signed certificate for a service, the Security page must be in Edit mode. A user may enter Edit mode by clicking the Edit button at the top right of the Security page. In the example below, the Generate New Self-signed Certificate button will generate a new self-signed certificate that replaces the existing one.
21.3.5 Generate Certificate Signing Request and Certificate Import

To generate a certificate signing request for a service, the Security page must be in Edit mode. A user may enter Edit mode by clicking the Edit button at the top right of the Security page. In the first example below, the Generate CSR button will generate a Certificate Signing Request (CSR) file that may be entered into a Certificate Authority to generate a CA-signed certificate. This certificate can then be imported using the Import button in the second example.
21.3.6 Revoke Certificate

To revoke a certificate for a service, the Security page must be in Edit mode. A user may enter Edit mode by clicking the Edit button at the top right of the Security page. In the example below, clicking the Revoke button will revoke the selected certificate.

⚠️ When revoking a certificate, the service will no longer function in a secure manner (and likely not at all) until a new certificate is generated or imported. In the case of HTTPS, the certificate manager will automatically generate a new self-signed certificate so that the web browser can function once the self-signed certificate has been imported to the browser.
22 Cloud Connection Setup

To connect a PXG to the cloud, users must have access to an Eaton cloud application, such as PX-EVA.

Users need to login to https://px-eva.eaton.com with existing credentials for PX-EVA.

Within PX-EVA, users will need to click on the facility in the left-hand pane where the PXG is physically installed. Click on Devices tab at the top of the screen, and add a new device with + New Device. Select PXG as the model.

Log in to the PXG. Under Settings > Network Access > Connect to Eaton Hosted Service, make sure Allow Connection to Eaton Hosted Service is selected. Then copy the Device GUID and paste into the GUID field of the Add a New Device page in PX-EVA. Complete the rest of the page by naming the device, providing the device’s serial number and physical location.

Submit when complete.
PX-EVA will return a **Connection String** that the user should copy the Connection String manually *without any quotation marks*. Users should, then, paste this string into **Connection String to Access the IoT Hub Server** field in the PXG.
Users may also need to update the **Proxy settings** within the PXG.

**Connected to Server** will be displayed on mouse-over. (If the connection was unsuccessful, the icon will display an 'X' and provide an error message on mouse-over.)

Once connected, all of the PXG subdevices will be automatically created as devices in the same facility within PX-EVA.

Note: When Eaton Hosted Service is disabled by default when it is enabled for first time gateway reboot is required to get cloud connectivity. Reboot gateway when IOT is configured for first time.

**PXG - Network Access page**
23 Cybersecurity Hardening the PXG

The PXG 950 acquires and consolidates data from devices typically found in electrical assemblies and systems. Multiple devices can be connected to PXG via RS485 or Ethernet connectivity. PXG supports Wired and Wireless TCP/IP Communication. With a web browser, the user can view detailed interfaces such as networking, alarms, trends, configurable settings, voltages, and current. The device is capable of sending the data to cloud over Ethernet or Cellular Connectivity.

PXG 950 has been designed with cybersecurity as an important consideration. A number of features are offered in the product to address cybersecurity risks. These Cybersecurity Recommendations provide information to help users deploy and maintain the product in a manner that minimizes the cybersecurity risks. These Cybersecurity Recommendations are not intended to provide a comprehensive guide to cybersecurity, but rather to complement customers' existing cybersecurity programs.

Eaton is committed to minimizing the Cybersecurity risk in its products and deploying cybersecurity best practices with the latest cybersecurity technology in its products and solutions; making them more secure, reliable, and competitive for the customers.

Eaton Cybersecurity Best Practices whitepapers are available that can be referenced for general cybersecurity best practices and guidelines:

- **Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):** [http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf](http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf)

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| Asset Management    | Keeping track of software and hardware assets in your environment is a prerequisite for effectively managing cybersecurity. Eaton recommends that you maintain an asset inventory that uniquely identifies each important component. To facilitate this, PXG950 supports the following identifying information:  
  - Catalog Number  
  - Product Revision  
  - Serial Number  
  - Firmware Version  
  This information is available on the device Hardware. Information is also available on the web UI under section Help -> About. |
| Risk Assessment     | Eaton recommends conducting a risk assessment to identify and assess reasonably foreseeable internal and external risks to the confidentiality, availability and integrity of the system/device and its environment. This exercise should be conducted in accordance with applicable technical and regulatory frameworks such as IEC 62443 and NERC-CIP. The risk assessment should be repeated periodically. |

---

4 [http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf](http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf)
Physical Security

An attacker with unauthorized physical access can cause serious disruption to system/device functionality. Additionally, Industrial Control Protocols don’t offer cryptographic protections, making ICS and SCADA communications especially vulnerable to threats to their confidentiality. Physical security is an important layer of defense in such cases. PXG950 is designed to be deployed and operated in a physically secure location. Following are some best practices that Eaton recommends to physically secure your system/device:

- Secure the facility and equipment rooms or closets with access control mechanisms such as locks, entry card readers, guards, man traps, CCTV, etc. as appropriate.
- Restrict physical access to cabinets and/or enclosures containing PXG950 and the associated system. Monitor and log the access at all times.
- Physical access to the telecommunication lines and network cabling should be restricted to protect against attempts to intercept or sabotage communications. It's a best practice to use metal conduits for the network cabling running between equipment cabinets.
- PXG 950 supports the following physical access ports.
  - COM1 and COM2 RS-485 for Modbus RTU
  - LAN Ethernet RJ45 CAT5 10/100Base
  - USB
  - Micro SD Card Slot
  - SIM Slot for Cellular Connectivity

Access to these ports should be restricted

- Do not connect removable media (e.g., USB devices, SD cards, etc.) for any operation (e.g., firmware upgrade, configuration change, or boot application change) unless the origin of the media is known and trusted.
- Before connecting any portable device through USB or SD card slot, scan the device for malwares and virus.

Eaton Cybersecurity Best Practices whitepaper provides additional information about general physical security considerations. Note: The USB port on the device is reserved for use only by an expert user with a customized USB key for maintenance when the device is unable to boot or the PXG application is inaccessible.
| Account Management | Logical access to the system | device should be restricted to legitimate users, who should be assigned only the privileges necessary to complete their job roles/functions. Some of the following best practices may need to be implemented by incorporating them into the organization’s written policies:

- Ensure default credentials are changed upon first login. PXG950 should not be deployed in production environments with default credentials, as default credentials are publicly known.
- No account sharing. Each user should be provisioned a unique account instead of sharing accounts and passwords. Security monitoring/logging features in the product are designed based on each user having a unique account. Allowing users to share credentials weakens security.
- Restrict administrative privileges. Attackers seek to gain control of legitimate credentials, especially those for highly privileged accounts. Administrative privileges should be assigned only to accounts specifically designated for administrative duties and not for regular use.
- Leverage the roles/access privileges goto ‘Users and Access Control’ to get more details about account management. Provide tiered access to the users as per the business/operational need. Follow the principle of least privilege (allocate the minimum authority level and access to system resources required for the role).
- Perform periodic account maintenance (remove unused accounts).
- Ensure password length, complexity and expiration requirements are appropriately set, particularly for all administrative accounts (e.g., minimum 10 characters, mix of upper- and lower-case and special characters, and expire every 90 days, or otherwise in accordance with your organization’s policies).
- Enforce session time-out after a period of inactivity.

Global Password Policy settings are configurable in the PXG, allowing security administrators to define the complexity, length, reuse and expiration rules for passwords of all users of the gateway. Individually, User Password Management features allows security administrators to further define password rules on a per-user basis. Additionally, accounts can be locked and unlocked as necessary. Refer to ‘Users and Access Control’ to get more details about password policies and secured access.

| Time Synchronization | Many operations in power grids and IT networks heavily depend on precise timing information.

- Ensure the system clock is synchronized with an authoritative time source (using manual configuration, NTP, SNTP, or IEEE 1588).
- Look into ‘Setting Preferences’ section of the document for more details about time synchronization. |
Network Security

PXG950 supports network communication with other devices in the environment. This capability can present risks if it's not configured securely. Following are Eaton recommended best practices to help secure the network. Additional information about various network protection strategies is available in Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1].

- Eaton recommends segmentation of networks into logical enclaves, denying traffic between segments except that which is specifically allowed, and restricting communication to host-to-host paths (for example, using router ACLs and firewall rules). This helps to protect sensitive information and critical services and creates additional barriers in the event of a network perimeter breach. At a minimum, a utility Industrial Control Systems network should be segmented into a three-tiered architecture (as recommended by NIST SP 800-82[R3]) for better security control.
- Deploy adequate network protection devices like Firewalls, Intrusion Detection/Protection devices.

Communication Protection: PXG950 provides the option to encrypt its network communications. Please ensure that encryption options are enabled. You can secure the product's communication capabilities by taking the following steps:

For added security, you should always disable HTTP access and enable HTTPS access for the gateway. To use HTTPS to connect to the PXG, you'll need to:

- Set either the local machine policy to allow users to manage certificates or, if multiple people in your organization will access the PXG, set a group policy. You'll need assistance from your IT organization to set a group policy.
- Download the certificate file from the PXG.
- Install the certificate in the Trusted Root Certification Authorities store. This is not the default store that the certificate installation wizard will choose, which is why you need permission to manage certificates.

Both enabling user management for certificates and installing a certificate require administrative privileges for the PC. If you don't have such privileges, you'll need to contact your IT organization for assistance before proceeding.

Enabling User Management of Root Certificates

The process for either enabling this on a local machine or setting a group policy is outlined in the following Microsoft Technet Article:


Essentially, you’re going to enable the users to allow trusted root CAs to be used to validate certificates and to trust peer trust
certificates. You'll do this through MMC. If you're changing the local policy, you'll have policy settings for certificate stores set as is shown in the following figure.

**Downloading the Certificate File from the Gateway**

1. Point either Google Chrome or Microsoft Internet Explorer to the IP address of the gateway followed by /ca.html. For example: [http://192.168.1.1/ca.html](http://192.168.1.1/ca.html).
2. Click the Root CA Certificate link. The browser will download the certificate.

Note that the certificate uses SHA-256 as its cryptographic hash function to avoid incompatibility problems with various browsers.

**Installing the Certificate**

1. Double-click the certificate file. This will launch the certificate installation wizard.
2. Click Install certificate.
3. On the Welcome dialog box, click Next.
4. Select Place all certificates in the following store and then click Browse.
5. Select Trusted Root Certification Authorities from the list, then click OK.

6. On the Completing the Certificate Import Wizard dialog box, click Finish.
7. You should see an alert box stating that the import was successful. Click OK.

8. Close all running sessions of a browser and open a new session. You can now access the gateway using the HTTPS protocol (for example, https://192.168.1.1/).

For web-based communications with the gateway, TCP Port 443 (HTTPS) is enabled by default and TCP Port 80 (HTTP) is disabled by default. For special situations, you may elect to disable one or the other. However, disabling both prevents any web access to the gateway and is not recommended. You may also choose to change the assigned port number for either.

**Ports in Use:**
Eaton recommends opening only those ports that are required for operations and protect the network communication using network protection systems like firewalls and intrusion detection systems / intrusion prevention systems. Use the information below to configure your firewall rules to allow access needed for PXG950 to operate smoothly. The following ports and protocols are disabled by default. You must elect to enable them and may choose to change the assigned port number.

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Protocol/Use</th>
<th>TCP/UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>502</td>
<td>Modbus TCP</td>
<td>TCP</td>
</tr>
<tr>
<td>26501</td>
<td>Modbus (COM1 Pass-thru)</td>
<td>TCP</td>
</tr>
<tr>
<td>26502</td>
<td>Modbus (COM2 Pass-thru)</td>
<td>TCP</td>
</tr>
<tr>
<td>47808</td>
<td>BACnet/IP</td>
<td>UDP</td>
</tr>
<tr>
<td>161</td>
<td>SNMP</td>
<td>UDP</td>
</tr>
<tr>
<td>162</td>
<td>SNMP</td>
<td>UDP</td>
</tr>
</tbody>
</table>

The following ports are open and necessary for proper PXG operation:

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Protocol/Use</th>
<th>TCP/UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>7012</td>
<td>Eaton’s Mercury Websockets Secure via TLS</td>
<td>TCP</td>
</tr>
<tr>
<td>8443</td>
<td>Eaton’s Mercury Secure via TLS for communications with PXI Software</td>
<td>TCP</td>
</tr>
</tbody>
</table>

These ports cannot be disabled or their port numbers changed. The following ports are disabled when PXG configuration is restored to defaults. These ports are enabled when user enables HTTP from user interface.

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Protocol/Use</th>
<th>TCP/UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>7011</td>
<td>Eaton’s Mercury Websockets</td>
<td>TCP</td>
</tr>
<tr>
<td>8181</td>
<td>Eaton’s Mercury for communications with PXI Software</td>
<td>TCP</td>
</tr>
</tbody>
</table>

The following ports are open and necessary for proper PXG operation:
**Browser Specific Notes**

- If you use HTTPS with Internet Explorer 10 you must enable TLS version 1.2 support in the browser. The PXG does not support SSL version 3.
- Restart your browser after loading the certificate to avoid any problems caused by the browser caching data.

**Network Access Tab - Controlling Access to Various Protocol Servers**

- BACnet/IP: Under BACnet/IP, you should only enable those services that you will be using. Leave everything else disabled. For those services that you do enable, make sure that you also enable Trusted Hosts for each and then maintain the minimum number of trusted hostnames/IP addresses that you need. Note that you must have Trusted Hosts enabled in order to save any trusted host machine names/IP addresses you’ve added.
- Modbus TCP Server Configuration: Unless you have a specific need to enable Write Commands, make sure that this is Disabled.
- SNMP: Unless you require SNMP features, it is recommended that you leave the overall support turned off by unchecking SNMP support in the Access Control section of the Network Access tab. If you require SNMP support, v1 and v3 features are independently configurable.
- Notifications Tab, Email Server: You should enable require TLS when communicating with an email server. Also, limit the recipient list to those who truly need this information.

**Note:** Many compliance frameworks and cybersecurity best practices require an audit of ports and services before and after applying updates and system changes. An end user should be able to refer to the ports and services documentation to determine the expected minimal set of ports and services on a device.
Remote Access

Remote access to devices/systems represents a provision of control to an external party. Strict management and validation of termination of such access is vital for maintaining control over the overall ICS security. Remote access to devices/systems creates another entry point into the network. Strict management and validation of termination of such access is vital for maintaining control over overall ICS security.

PXG950 has following features to ensure secured remote access.

**Browser Session Time-Out**

You can use the Session Timeout (on the Security tab under General Settings) to impose a time-out to automatically log out a browser session. This time-out applies to all user accounts. The Session Timeout value is the number of minutes during which no browser activity is detected. Once the specified number of minutes of account inactivity is reached, the current browser session will be logged out. A value of zero disables the time-out function.

![Session Timeout Setting](image)

**Restricting Concurrent Logins**

You can use Max Concurrent Logins (on the Security tab under General Settings) to limit on the number of login sessions that can share the same account. This limitation, once set, applies to all user accounts. A value of zero removes any restriction.
In this example, setting Max Concurrent Logins to 2 limits the number of users logging in using a shared account to just 2. Good security practice suggests setting this to the lowest practical non-zero number for your specific installation. As the gateway allows you to create additional users with specific roles and permissions, you may consider restricting concurrent logins to just one.

**Auto Re-login**

The PXG has an **Auto Re-login** feature. When enabled, it automatically logs in the user after a communication loss is restored. User can keep it disabled for tightest security.
Logging and Event Management

- Eaton recommends logging all relevant system and application events, including all administrative and maintenance activities.
- Logs should be protected from tampering and other risks to their integrity (for example, by restricting permissions to access and modify logs, transmitting logs to a security information and event management system, etc.).
- Ensure that logs are retained for a reasonable and appropriate length of time.
- Review the logs regularly. The frequency of review should be reasonable, taking into account the sensitivity and criticality of the system/device and any data it processes.
- PXG950 is capable of logging the events and activities on device, all the logging functionalities are enabled all time.
- Activities of Users, Connected Device, Configuration, Session, Commands and Update are logged.
- User can download logs from Web UI -> Network -> PXG950 -> Choose An Action -> Download section

Gateway keeps records of last login and failed login attempts as described below:

**Last Login Notification and History**

The gateway will warn you of previously failed login attempts. Any time there has been at least one failed login attempt, you'll be greeted with a warning message on your next successful login.

Last Login History can be viewed at any time by clicking on the Welcome text found next to the displayed Date and Time.
Doing so, produces the following menu.

Selecting Login History from the menu will provide the latest historical information associated with the username you're currently logged in as.
### Vulnerability Scanning

- It is possible to install and use third-party software with PXG950. Any known critical or high severity vulnerabilities on third party component/libraries used to run software / applications should be remediated before putting the device | system into production.

- Eaton recommends running a vulnerability scan to identify known vulnerabilities for software used with the product. For COTS components (e.g., applications running on Windows), vulnerabilities can be tracked on the National Vulnerability Database (NVD), available at [https://nvd.nist.gov/](https://nvd.nist.gov/).

- Keep software updated by monitoring security patches made available by COTS vendors and installing them as soon as possible.

Note: Many compliance frameworks and security best practices require a monthly vulnerability review. For many non-COTS products vulnerabilities will be communicated directly through the vendor site.

### Malware defenses

Eaton recommends its customers to deploy adequate Malware defenses to the platforms / products that are used to run Eaton applications / products. Eaton Cybersecurity Best Practices whitepaper provides additional information about general physical security considerations.
Secure Maintenance

Best Practices

Update device firmware prior to putting the device into production. Thereafter, apply firmware updates and software patches regularly. Eaton publishes patches and updates for its products to protect them against vulnerabilities that are discovered. Eaton encourages customers to maintain a consistent process to promptly monitor for and install new firmware updates.

- Device firmware can be upgraded from Web UI -> Network -> PXG950 -> Edit -> Firmware Update
- Conduct regular Cybersecurity risk analyses of the organization /system.

Advanced Troubleshooting Resources

The device includes a tools.html page reserved for use only by an expert user. This webpage allows an expert user with help from site administrator to troubleshoot the device functionality. This page allows user to perform following tasks.

- Email Debug Data
- Enable SSH
- Disable SSH
- Reboot
- Ping
- SMTP Test
- Upload Factory Configuration

Caution: The Enabling of SSH is provided for diagnostic purposes and should not be left enabled at any point in time. The USB port on the device is reserved for use only by an expert user with a customized USB key for maintenance when the device is unable to boot or the PXG application is inaccessible.

Please check Eaton’s cybersecurity website for information bulletins about available firmware and software updates. Eaton customer support: For support on any aspect of the product or installation process contact the Customer Integrity Team by MRSsupport@eaton.com or calling 1-844-435-8982.
| Business Continuity / Cybersecurity Disaster Recovery | Plan for Business Continuity / Cybersecurity Disaster Recovery  
Eaton recommends incorporating PXG950 into the organization’s business continuity and disaster recovery plans. Organizations should establish a Business Continuity Plan and a Disaster Recovery Plan and should periodically review and, where possible, exercise these plans. As part of the plan, important system/device data should be backed up and securely stored, including:  
- Updated firmware for PXG950. Make it a part of standard operating procedure to update the backup copy as soon as the latest firmware is updated.  
- The current configuration.  
- Documentation of the current permissions/access controls, if not backed up as part of the configuration.  

The following section describes the details of failures states and backup functions:  
- Keep backup of the latest f/w copy of PXG950. Make it a part of SOP to update the backup copy as soon as the latest f/w is updated.  
- Keep backup of the most current configuration. Goto Web UI -> Network -> PXG950 -> Edit->Configuration File Save/Restore -> Download link get the current device configuration.  
- During normal operation power led will continuous ON  
- In case of failure power led will become off, check the device input power and power up device again  

To load the new configuration device use web UI link Network -> PXG950 -> Edit->Configuration File Save/Restore  

| Sensitive Information Disclosure | Eaton recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by <Product Name> be adequately protected through the deployment of organizational security practices. Following information should be protected.  
- Device Configuration (Network settings/IP Address/IOT connection details etc)  
- User account details (No of users/Access Control/Password)  
- Audit Logs  


Decommissioning or Zerolisation

It is a best practice to purge the data before disposing any device containing data. Proper decommissioning is described in NIST SP800-88. Eaton recommends that products containing embedded flash memory be destroyed to ensure any secure data is unrecoverable.

*Embedded Flash Memory on Boards and Devices*

- This includes motherboards and peripheral cards such as network adapters or any other adapter containing non-volatile flash memory.
- **Clear**: Reset the device to factory default. Use the command from Web UI -> Network -> PXG950 -> Choose An Action -> Factory Reset Gateway.
- In case web UI is not accessible device can set to factory default with USB. Refer to ‘Reset PXG’ section of the document to get the details.
- **Purge**: If the flash memory can be easily identified and removed from the board, the flash memory may be Destroyed independently from the disposal of the board that contained the flash memory. Otherwise, the whole board should be Destroyed.
- **Destroy**: Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
23.1 References


24 Cellular Settings and Wifi Configuration

24.1 Cellular Settings

Celluar settings are available in Network Access tab. You can check ‘Enable Cellular connectivity’ checkbox and update the settings in Edit mode. Access Point Name (APN) setting is mandatory to enable cellular connectivity.

**Note:** APN name depends on the service provider and the purpose the sim was bought for. Hence the user should request APN info from their service provider.

'PIN' is required to unlock the SIM, if it is locked. Maximum three attempts are given to unlock SIM. In case wrong pin is entered for three times. SIM is set into PUK mode.

In PUK mode user can set a new PIN using PUK number.

Once the cellular settings are saved, it tooks few seconds to get the connectivity and display signal strength in top right corner. Cellular connectivity status can be read by hover your cursor over the signal strength symbol.

![Cellular Settings](image)

**Note:** Before enabling cellular connectivity SIM should be inserted into SIM Slot of the gateway. You must power down the gateway while inserting the SIM. In case SIM is locked and you dont have infromation about PIN or PUK, contact service provider to get the details.

24.2 Wi-Fi Configuration

Wi-Fi configuration is available on Network tab. In Edit mode, you can enable Wi-Fi button. Enter the ESSID, select the Encryption Mode and then enter the appropriate Passphrase for the access point you're connecting to. You can also view Signal Strength percentage for Wi-Fi connectivity.
Note: Wi-Fi is supported to work with 2.4 GHz routers. In case you face any issues with Wireless connectivity even after using correct SSID and password you might have to check the router settings or contact local IT for support. For more details about Wi-Fi and Cellular network specification refer to Technical Data Sheet (TD150032EN).
25 Firmware Update

PXG950 Firmware can be updated from Web UI. Follow the steps below to update the firmware.

1. Download the latest firmware file from Eaton site
2. Goto 'Network' Page
3. Select Gateway and open Edit Mode
4. From 'Choose an Action' menu select 'Firmware Update'

5. Browse and select firmware file

6. Click on Upload to start the upload process
7. Firmware upload takes 4-5 mins, it may take more time if network speed is low.
8. After successful upload PXG will reboot and communication to device will be lost
9. Wait for 2-3 mins to boot up the device

Cloud LED Status Indicator
Cloud LED blinks green while the firmware update is in progress. It is ON for 700ms and OFF for 300ms while it blinks.

Note: If PXG is running in DHCP mode device ip address may get change. If device is not accessible after firmware update use IP scanner tool and check IP address of the device. Upload process will fail if firmware file selected is invalid.