Power Xpert Gateway 900

PXG 900 User's Guide

EATON

Powering Business Worldwide

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITY

The information, recommendations, descriptions and safety notations in this document are based on Eaton Corporation's ("Eaton") experience and judgment and may not cover all contingencies. If further information is required, an Eaton sales office should be consulted. Sale of the product shown in this literature is subject to the terms and conditions outlined in appropriate Eaton selling policies or other contractual agreement between Eaton and the purchaser.

THERE ARE NO UNDERSTANDINGS, AGREEMENTS, WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE OR MERCHANTABILITY, OTHER THAN THOSE SPECIFICALLY SET OUT IN ANY EXISTING CONTRACT BETWEEN THE PARTIES. ANY SUCH CONTRACT STATES THE ENTIRE OBLIGATION OF EATON. THE CONTENTS OF THIS DOCUMENT SHALL NOT BECOME PART OF OR MODIFY ANY CONTRACT BETWEEN THE PARTIES.

In no event will Eaton be responsible to the purchaser or user in contract, in tort (including negligence), strict liability or other-wise for any special, indirect, incidental or consequential damage or loss whatsoever, including but not limited to damage or loss of use of equipment, plant or power system, cost of capital, loss of power, additional expenses in the use of existing power facilities, or claims against the purchaser or user by its customers resulting from the use of the information, recommendations and descriptions contained herein. The information contained in this manual is subject to change without notice.

Table of Contents

1 Connecting the PXG to a PC 8

1.1 Connecting With a USB Cable 8

1.2 Connecting via an Ethernet Cable 12

2 Configuring the PXG 13

2.1 Configuring Ethernet Access 13

2.1.1 Setting Port Visibility 15

3 Configuring Device Communications 17

3.1 Modbus Serial Ports 17

3.2 INCOM Port 17

3.3 Network 2 (Ethernet) 17

3.4 Network 1 (Ethernet) 17

3.5 Adding Devices 18

3.6 Initial Setup 18

3.6.1 Example 1: Adding An IQ 250 Meter 18

3.6.2 Example 2: Adding a Digitrip 1150 Breaker 19

3.6.3 Example 3: Adding a BIM II Display Device 22

3.7 Special Considerations for the AEM II 24

4 Configuring Device Channels 25

4.1 Disabling a Device 25

4.2 Managing Device Channels 26

5 Setting Preferences 27

5.1 Time 27

5.2 Locale 27

6 Network Access Settings 29

6.1 Access Control 29

7 Modbus TCP Server 32

7.1 Modbus TCP Server Setup 32

7.2 Viewing and Modifying the Modbus Map 33

7.3 Pass Through 35

7.3.1 Modbus ... 35
7.4 EMINT (INCOM only) ... 35
7.5 Setup ... 35
8 BACnet IP Server ... 37
8.1 Setting up a BACnet/IP Server ... 37
8.1.1 Base ID for Auto-Assign ... 37
8.1.2 Auto-Assign Gateway ID ... 37
8.1.3 Auto-Assign Device IDs ... 37
8.1.4 BACnet Broadcast Management Device ... 37
8.2 Mapping ... 38
9 SNMP Server ... 40
9.1 SNMP Server Setup ... 40
9.1.1 Enabling SNMP v1 and v3 Support ... 40
9.1.2 Detailed SNMP v3 Configuration ... 40
9.1.2.1 Configuring the Read-Only User ... 41
9.1.2.2 Configuring the Read-Write User ... 41
9.1.3 Detailed SNMP v1 Configuration ... 41
9.1.3.1 Configuring the Read-Only Community String ... 42
9.1.3.2 Configuring the Read-Write Community String ... 42
9.1.4 Gateway-provided SNMP MIB Support ... 42
9.1.4.1 Eaton OIDs ... 43
9.1.4.2 Eaton Power Device MIB ... 43
9.1.4.3 Eaton Power Meter MIB ... 44
9.1.4.4 Eaton Alarms+Traps MIB ... 44
9.1.4.5 Entity and Entity State MIB Support ... 44
9.1.5 Configuring v1 Trap Support ... 44
9.1.5.1 v1 Trap Recipient Community String ... 45
9.1.5.2 Enable Auth Fail ... 45
9.1.6 Configuring v3 Trap Support ... 46
9.1.6.1 v3 Auth Fail Trap ... 46
9.1.7 Adding or Removing v1 and v3 Trap Recipients ... 46
10 Notifications ... 47
10.1 Setting up the Email Server ... 47

10.2 Adding Recipients 48
10.3 System Use Notification 49
11 Users and Access Control 50
11.1 Building Roles 51
11.2 Creating Users 52
11.3 Deleting Admin and User 52
11.4 Accessing Logs 53
11.5 Roles and Permissions Cookbook 53
11.6 Security Audit 53
11.7 Security Admin 53
11.8 Engineer 54
11.9 Service Engineer 54
11.10 IoT Agent 54
11.11 Password Policy 54
11.12 User Password Management 55
11.12.1 Password Expiration Changes 56
12 Advanced Administration 57
12.1 Choose an Action Functions 57
12.1.1 Audit Logs 58
13 Setting Alarms 60
13.1 Creating an Alarm Configuration 60
13.2 Alarm Levels 62
13.3 Setting Alarm Level for Multi-State Channels 63
14 One-lines 65
14.1 Creating One-Lines 65
14.2 Adding Devices to One-Lines 65
14.3 One-line Diagrams 65
14.3.1 Number of Sources 67
14.3.2 Tie Breaker Symbol 67
14.4 Using Auto-Draw 68
14.5 Working with Symbols and Graphics 68

15 Connecting to the Web Interface........ 69
16 Network Tab........ 70
16.1 Choose an Action........ 71
16.2 Device Details........ 72
17 Alarms Tab........ 74
18 Trend Viewer........ 75
19 Waveforms........ 76
19.1 Waveforms Captured by Devices........ 76
19.2 Enabling Waveform Capture in the PXG........ 76
19.3 Captured Waveforms List........ 76
19.4 Waveform Files........ 77
19.5 Manual Waveform Capture........ 77
19.6 Signing up for Waveform Email Notifications........ 77
19.7 Waveform Link in Email Notifications........ 79
20 One-lines Tab........ 82
20.1 Device Tree........ 82
20.2 Graphic View........ 82
20.3 Link Objects........ 82
20.4 One-line Diagrams........ 82
21 Cybersecurity Hardening the PXG........ 86
21.1 Enabling User Management of Root Certificates........ 86
21.1.1 Downloading the Certificate File from the Gateway........ 87
21.1.2 Installing the Certificate........ 87
21.2 Ports in Use........ 90
21.3 Browser Specific Notes........ 92
21.4 Settings........ 92
21.4.1 Network Access Tab - Controlling Access to Various Protocol Servers........ 92
21.4.1.1 BACnet/IP........ 92
21.4.1.2 Modbus TCP Server Configuration........ 92
21.4.1.3 SNMP........ 92
21.5 Notifications Tab, Email Server........ 92

21.6 Passwords 92
21.7 Last Login Notification and History 93
21.8 Browser Session Time-Out 94
21.9 Restricting Concurrent Logins 95
21.10 Auto Re-login 96
22 Reset PXG 97
23 Certificate Management 98
23.1 Certificate Generation 98
23.2 Certificate Upload 98
23.3 Operations Supported by the Certificate Manager UI 99
23.3.1 Listing of Server Certificates 99
23.3.2 Viewing Details of Certificates 99
23.3.3 Export Server Certificate 100
23.3.4 Generate New Self-Signed Certificates 100
23.3.5 Generate Certificate Signing Request and Certificate Import 101
23.3.6 Revoke Certificate 102
24 Cloud Connection Setup 103
24.1 IoT Data Integrity: 106

The Power Xpert Gateway(PXG) is a powerful tool for monitoring electrical systems. It can also serve as a data aggregation point if used with Eaton's Power Xpert Insight or third party software. This guide will show you how to configure the PXG from its web interface and how to work with the Network, One-lines, and Alarms tabs.

You can configure and interact with the PXG through its web interface. This is best viewed in either Google Chrome (current version) or Microsoft Internet Explorer 10 or 11. The screen resolution should be at least 1280 x 1024 pixels.

> *Note: You may experience display problems at zoom levels other than 100%*

1 Connecting the PXG to a PC

The first step in commissioning is to connect a PC to the PXG so that you can access the PXG web interface. The preferred method is to initially connect to the PXG via a USB cable. Some computers running Windows 8 and later include a driver for such connections. If your machine is running a prior version of Windows or if it asks for a driver, the section on connecting via the USB port provides instructions for downloading the driver from Eaton. If you can't connect through the USB port, you can use a CAT5 Ethernet cable to connect your PC to the PXG. This method relies on Zeroconf and establishing communication is more difficult and less reliable. Also, to initially connect through the Ethernet port you must be directly connected via a cable. You can't connect this way via a LAN until you configure the Ethernet settings.

1.1 **Connecting With a USB Cable**

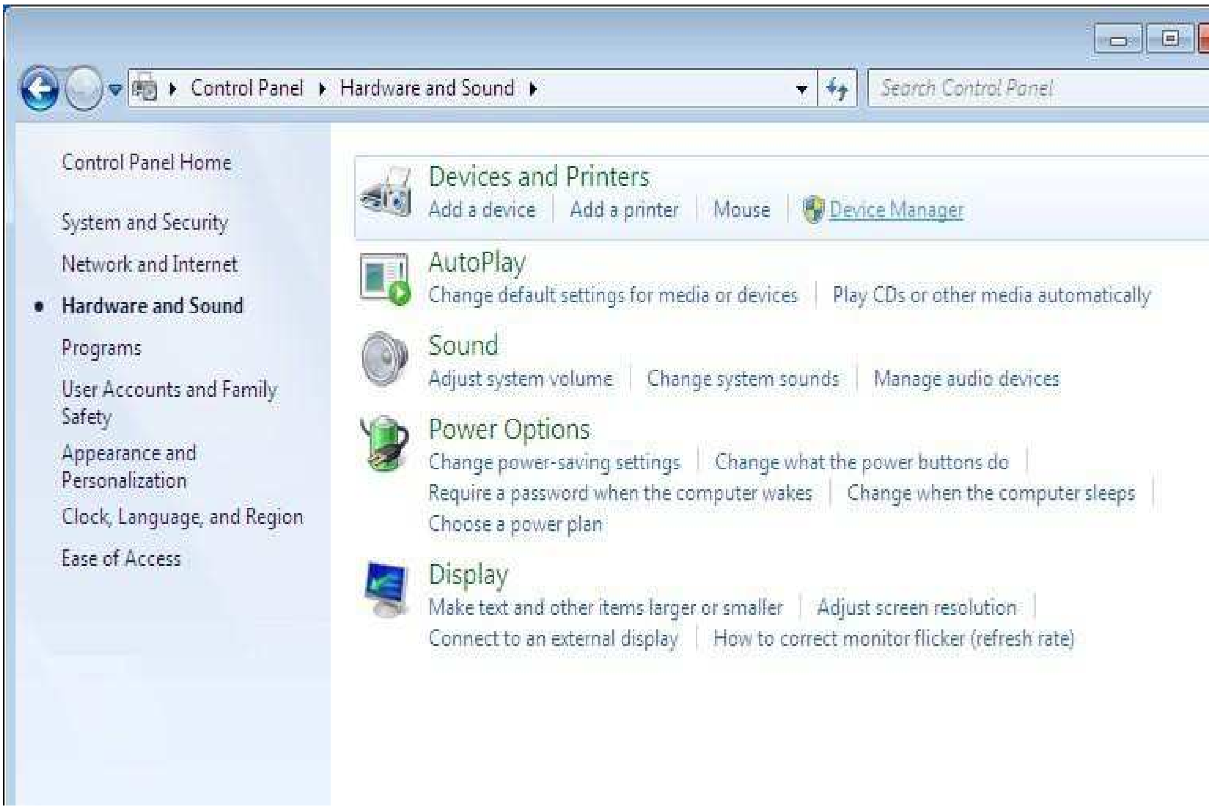
You can initially connect the PXG to a PC via the USB A to USB mini-B cable shipped with the gateway. Before your PC can connect to the gateway, you may first need to install the USB driver from Eaton. You'll need administrative privilege on the PC in order to install the driver. Also, the USB cable must be connected. You can access the driver at http://eaton.com/PXG.

1. Navigate to the eaton.com/PXG[1] site.
2. Choose Documentation tab.
3. Choose Software Downloads.
4. Choose the PX USB Configuration file.

After you've downloaded the powerxpert.inf file, use the following steps to activate the USB driver.

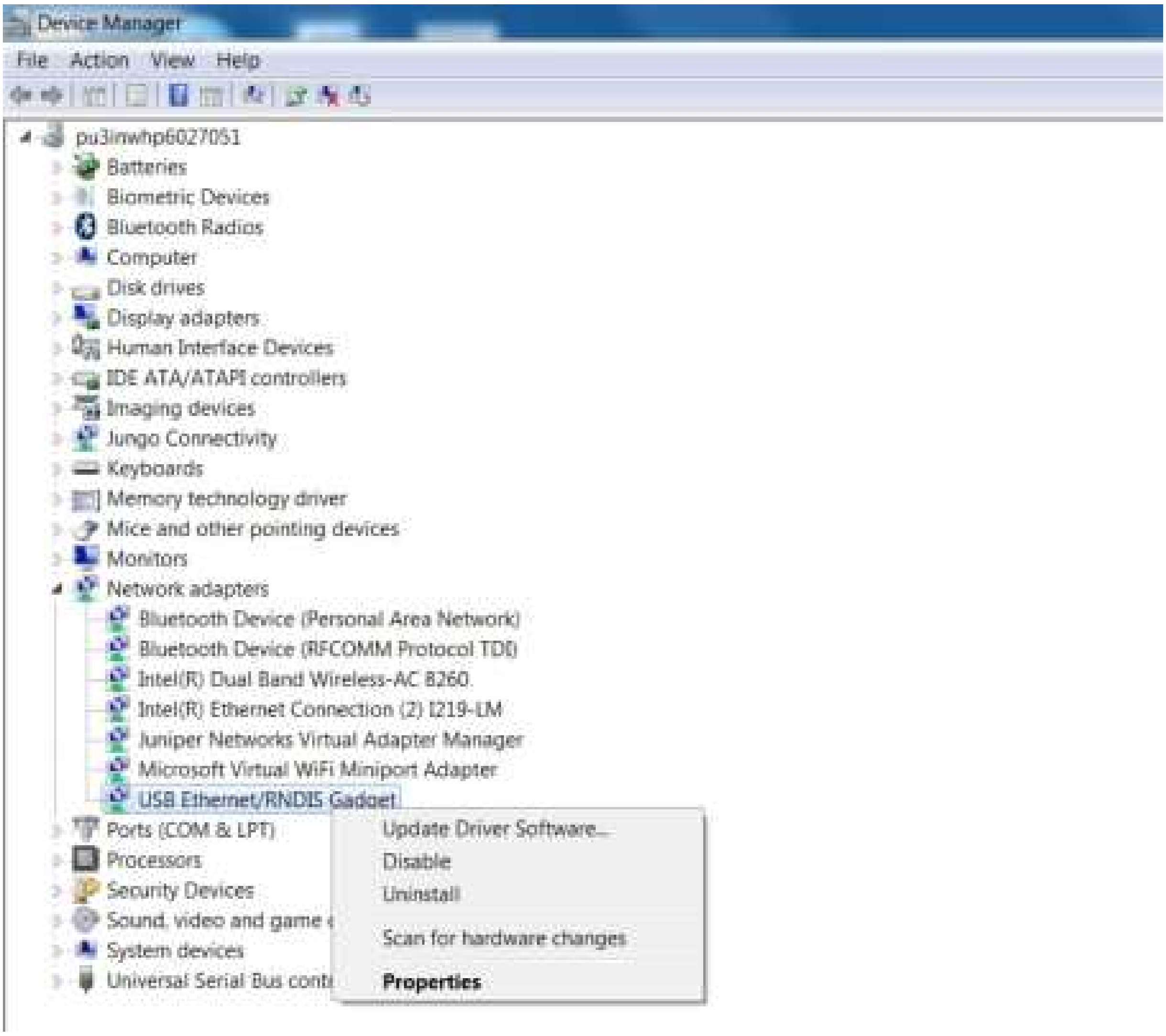
1. Make sure that the USB is connected between the PC and gateway. The cable must be connected to update the driver.
2. Open the Control Panel and select Hardware and Sound > Devices and Printers.

[1] http://eaton.com/PXG


Control Panel ▸ Hardware and Sound ▸
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts and Family Safety
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Devices and Printers
Add a device | Add a printer | Mouse | Device Manager
AutoPlay
Change default settings for media or devices | Play CDs or other media automatically
Sound
Adjust system volume | Change system sounds | Manage audio devices
Power Options
Change power-saving settings | Change what the power buttons do | Require a password when the computer wakes | Change when the computer sleeps | Choose a power plan
Display
Make text and other items larger or smaller | Adjust screen resolution | Connect to an external display | How to correct monitor flicker (refresh rate)

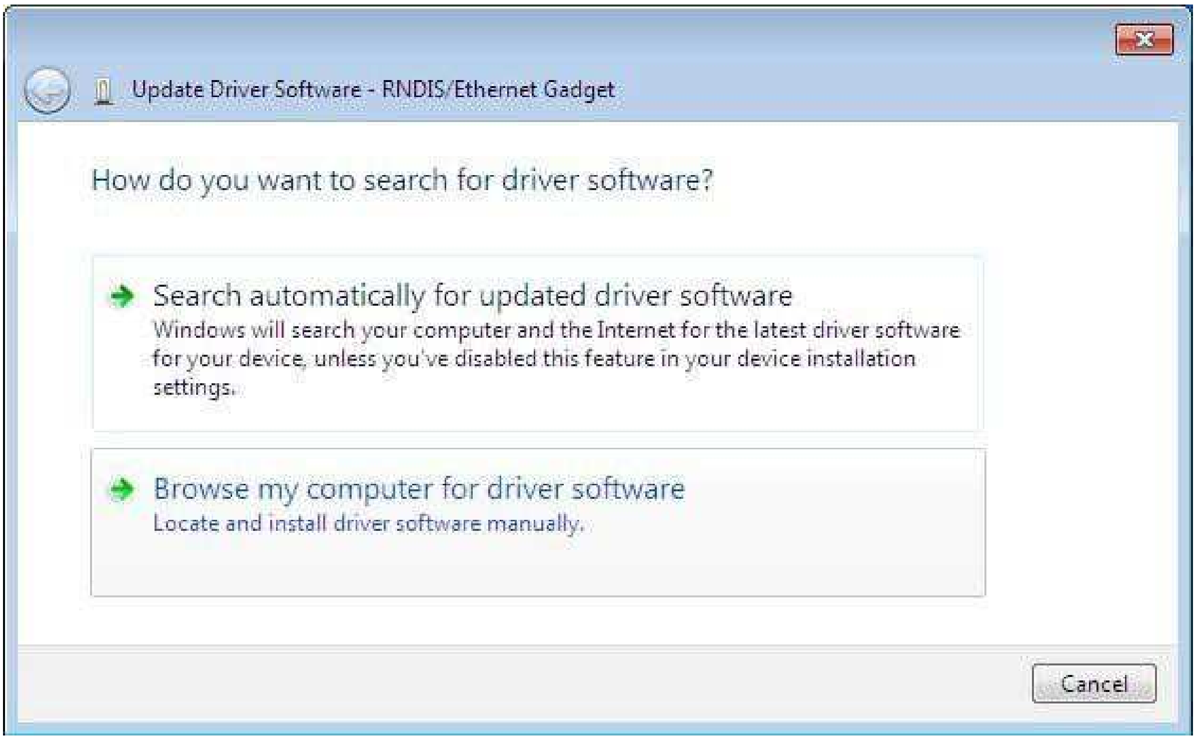
1 Hardware and Sound - Device Manager

3. Select Device Manager to open the Device Manager window.
4. Expand Other devices and select RNDIS/Ethernet Gadget.
5. Right-click and select Update Driver Software.


Device Manager
File Action View Help
pu3inwhp6027051
Batteries
Biometric Devices
Bluetooth Radios
Computer
Disk drives
Display adapters
Human Interface Devices
IDE ATA/ATAPI controllers
Imaging devices
Jungo Connectivity
Keyboards
Memory technology driver
Mice and other pointing devices
Monitors
Network adapters
Bluetooth Device (Personal Area Network)
Bluetooth Device (RFCOMM Protocol TDI)
Intel(R) Dual Band Wireless-AC 8260
Intel(R) Ethernet Connection (2) I219-LM
Juniper Networks Virtual Adapter Manager
Microsoft Virtual WiFi Miniport Adapter
USB Ethernet/RNDIS Gadget
Ports (COM & LPT)
Processors
Security Devices
Sound, video and game c
System devices
Universal Serial Bus contr
Update Driver Software...
Disable
Uninstall
Scan for hardware changes
Properties

2 Update Driver Software

6. Select Browse my computer for driver software.



Update Driver Software - RNDIS/Ethernet Gadget

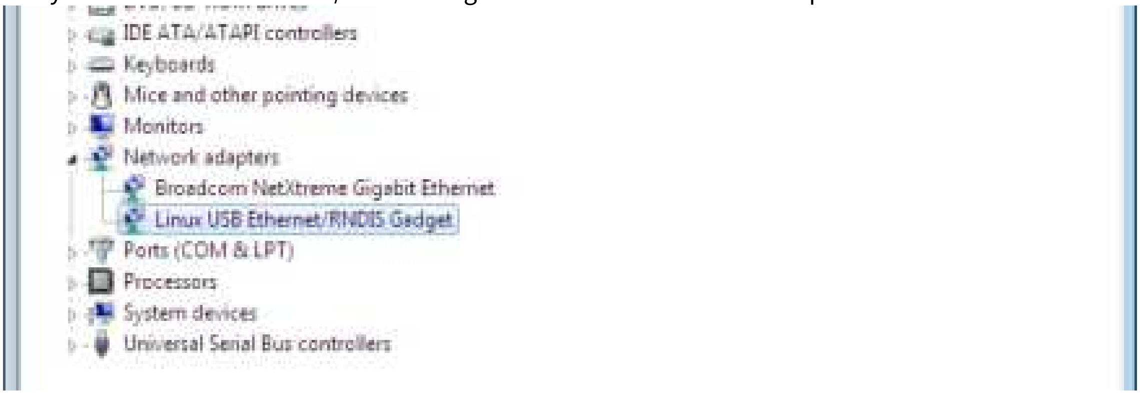
How do you want to search for driver software?

Search automatically for updated driver software
Windows will search your computer and the Internet for the latest driver software for your device, unless you've disabled this feature in your device installation settings.

Browse my computer for driver software
Locate and install driver software manually.

3 Browse for Driver

7. Choose Browse. The Locate File window opens.
8. .Locate and select the folder containing the powerxpert.inf file.
9. Choose Open. The folder displays in the Search for driver software in this location box.
10. Choose Next.
11. If the message "Windows can't verify the publisher of this driver software" displays, select Install this driver software anyway.
12. To verify that the device is installed:
    - Go to Control Panel > Hardware and Sound > Devices and Printers > Device Manager.
    - Expand Network adapters.
    - Verify that Linux USB Ethernet/RNDIS Gadget is listed under Network adapters.

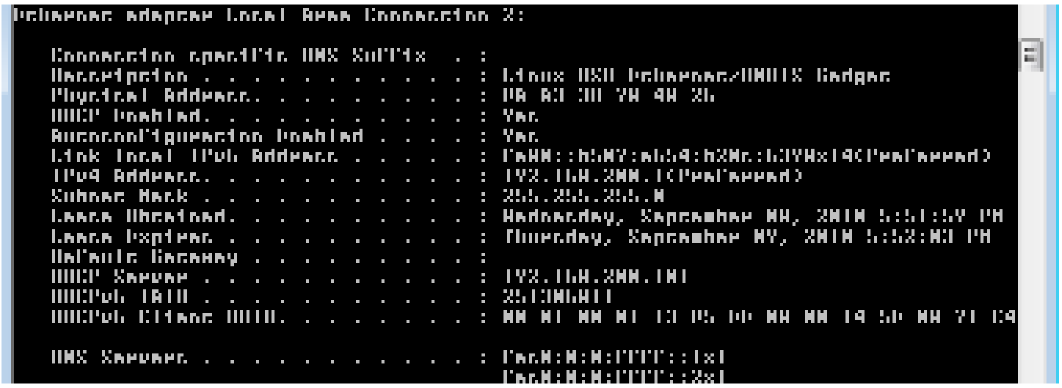


IDE ATA/ATAPI controllers
Keyboards
Mice and other pointing devices
Monitors
Network adapters
Broadcom NetXtreme Gigabit Ethernet
Linux USB Ethernet/RNDIS Gadget
Ports (COM & LPT)
Processors
System devices
Universal Serial Bus controllers

4 Linux USB Ethernet/RNDIS Gadget

13. From the Start menu, go to All Programs > Accessories > Command Prompt to open a Command Prompt window.
14. Enter ipconfig /all.

15. Verify that the assigned IPv4 address assigned to your PC is in the 192.168.200.x range (where "x" is typically "1").



```
Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Linux USB Ethernet/RNDIS Gadget
   Physical Address. . . . . . . . . : [illegible]
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::[illegible]%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.200.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, September [illegible] PM
   Lease Expires . . . . . . . . . . : Thursday, September [illegible] PM
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 192.168.200.101
   DHCPv6 IAID . . . . . . . . . . . : [illegible]
   DHCPv6 Client DUID. . . . . . . . : [illegible]

   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
```

5 Verifying the IP Address

1.2 Connecting via an Ethernet Cable

If you can't connect via a USB cable, you can use this method. It requires the following:

- A PC that is completely disconnected from all networks, including wireless. To ensure this, you may wish to turn off your wireless network adapter.
- A CAT5 Ethernet cable to connect to a single, unconfigured gateway.

To connect:

1. Plug the Ethernet cable into both the PC and the Network 1 Ethernet port on the PXG.
2. Wait at least 30 seconds for the PC and gateway to negotiate a connection.
3. Point your PC browser to http://169.254.1.1[2].

[2] http://169.254.1.1/

2 Configuring the PXG

The PXG900 is shipped from the factory with a default password. This assists commissioning agents in the original commissioning of the PXG900. Once original commissioning is complete and the PXG900 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 PXG web interface:

1. Navigate a browser to the following address: http://192.168.200.101[3] (USB) or http://169.254.1.1[4] (CAT5). Note that HTTPS does not work when connected by USB.
2. You'll be prompted to enter a user ID and password. The default is "admin" for both.

2.1 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. Software-controlled bridging is used to allow other Ethernet devices to access the gateway's LAN connection when the devices are plugged into Network 2. When power is applied to the PXG, the bridged LAN connection is not immediately available to the devices connected to Network 2.

If you do choose to use DHCP, you should use DHCP Reservations on your LAN so that the PXG is always assigned the same IP address. If you don't, neither the PXG users nor any management software connected to the PXG will be able to "find it" after a power interruption or reboot if the DHCP server provides a different address.
To edit the Ethernet settings:

On the Network tab, click the Edit button.

Choose the gear icon at the right of the Eaton Power Xpert Gateway bar.

Configuration is done in the sidebar.

To specify a static IP address:

Enter the IP Address for the PXG.

Enter the IP address information for your network, including the Subnet Mask, Gateway, and one or more DNS servers. Separate the DNS server addresses with a comma.

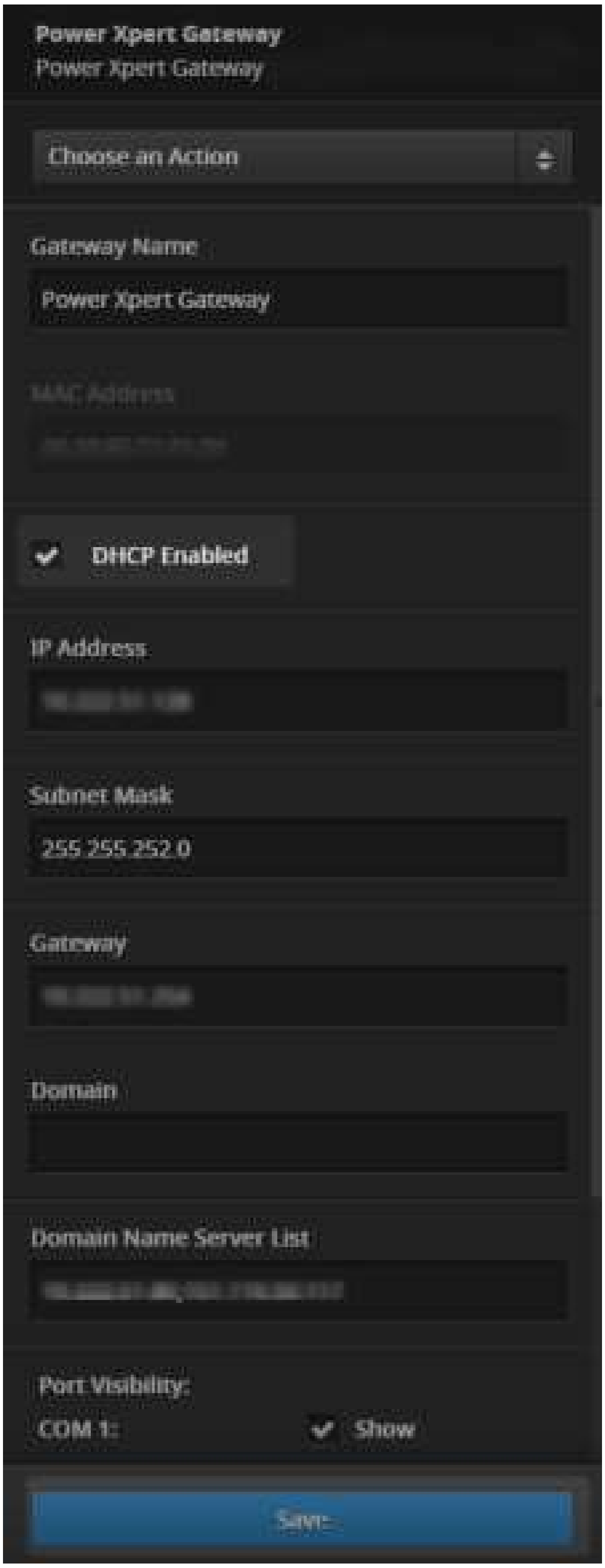
Choose Save.

To use DHCP to assign an IP address:

Select DHCP Enabled.

Choose Save.

[3] http://192.168.200.101/
[4] http://169.254.1.1/



Power Xpert Gateway
Power Xpert Gateway

Choose an Action

Gateway Name: Power Xpert Gateway

MAC Address: [redacted]

☑ DHCP Enabled

IP Address: [redacted]

Subnet Mask: 255.255.252.0

Gateway: [redacted]

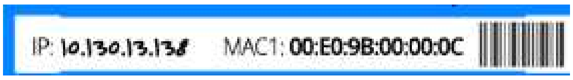
Domain:

Domain Name Server List: [redacted]

Port Visibility:
COM 1: ☑ Show

Click Edit again to exit edit mode.

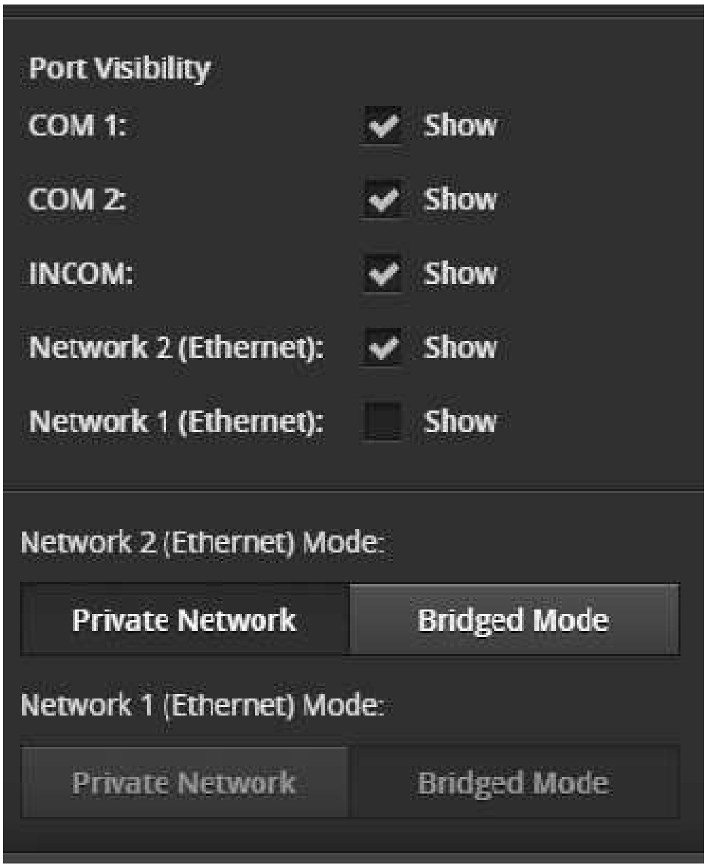
After you've completed configuring an IP address (either through DHCP Reservations or as a static IP), write this on the label
under the connectors.



IP: 10.130.13.138 MAC1: 00:E0:9B:00:00:0C

2.1.1 Setting Port Visibility

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. This only applies to the Network tab and all devices will still be visible on the other tabs.



Port Visibility

COM 1: ☑ Show

COM 2: ☑ Show

INCOM: ☑ Show

Network 2 (Ethernet): ☑ Show

Network 1 (Ethernet): ☐ Show

Network 2 (Ethernet) Mode:

Private Network | Bridged Mode

Network 1 (Ethernet) Mode:

Private Network | Bridged Mode

Connecting a PXG to the Ethernet LAN

The PXG has two 10/100/1000 Base T, RJ-45 connectors labeled Network 1 and Network 2.

Rules for connecting a PXG to the Ethernet LAN:

If the PXG is connected directly to the local area network, use Network 1.

If you want to connect the PXG to a Modbus TCP device, select the 'Network1(Ethernet)' setting. Save the changes and exit Edit mode.Network1 port will be available on user interface to connect with Modbus TCP devices. Modbus TCP devices IP address should be in same subnet of PXG IP address. 'Network 1(Ethernet) Mode: ' setting value will be 'Bridged Mode' and will not be editable by user.

You can hide Network1 port by deselecting the 'Network1(Ethernet)' . If any Modbus TCP device is connected to Network1, you need to remove the Network1 device first and then deselect the Network1 port from user interface.

If you are going to connect the PXG to a Modbus TCP private network, this can be connected to Network 2. If you're not connecting to a Modbus TCP network, but instead wish to connect to a second PXG gateway or other Ethernet devices to the gateway, connect it to Network 2. For more about using the Network 2 port, see "Bridged or Private Networks". The total length of any Ethernet cable run must not exceed 295.3 ft (90 m).

If the gateway loses power any devices connected to Network 2 to bridge to the local area network will lose network communication.

Bridged or Private Networks

In Bridged Mode, the PXG can be accessed via its IP address through both Ethernet ports (Network 1 and Network 2). This means that you can attach an upstream device to Network 2 instead of having to use an Ethernet switch. If Private Network is selected, Network 2 provides a private subnet to which you can connect Modbus TCP devices. Each of these must have an IP address that's part of the private subnet. You can set the IP address of the Net 2 port on this subnet during port configuration.

NOTE: 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.

3 Configuring Device Communications

You can configure the PXG's Modbus serial ports, Modbus TPC/IP port, and INCOM port 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 either a twisted pair Modbus or a twisted pair INCOM 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 are clearly marked for the A+, B- and CMN (common) connections.The PXG900 modeling tool can provide estimated communication performance estimates for the individual communication ports. The ports have the following device limits:

- INCOM port – 100 devices
- COM1 port – 32 devices, supports Modbus RTU devices
- COM2 port – 32 devices, supports Modbus RTU devices
- Network 2 - 50 devices, supports Modbus TCP devices when Private Network is enabled
- Network1 -10 devices, supports Modbus TCP devices, it will always be in Bridged mode

3.1 Modbus Serial Ports

You can set Modbus Ports 1 and 2 individually through their respective gear icons. Set the serial port parameters for your Modbus RTU network. You should only change the timeout settings if absolutely necessary.
To attach a Modbus RTU network to the PXG:

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

1. Attach one of the three-pin Phoenix connectors shipped with the PXG to the Modbus twisted pair cable.
2. Connect the Modbus cable to the COM1 or COM2 port of the PXG.

3.2 INCOM Port

Choose the gear icon to access the INCOM port serial settings. For more information on wiring an INCOM network, see the *Eaton Electrical Field Devices Communication Wiring Specification* (TD 17513)[5].

> *A 100-Ohm terminating resistor isn't required at the PXG.*

To attach a network of INCOM devices to the PXG:

1. Attach one of the three-pin Phoenix connectors shipped with the PXG to the INCOM twisted pair cable.
2. Insert the connector into the INCOM port on the PXG.

3.3 Network 2 (Ethernet)

When Private Network is enabled, you can use Network 2 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. Don't change the timeout setting unless this is absolutely necessary.

3.4 Network 1 (Ethernet)

In Network tab sidebar, when 'Network 1(Ethernet)' setting is checked, Modbus TCP device can be added which should be in same subnet of PXG IP address. 'Network1(Ethernet) mode' will always be set to 'Bridged mode'. You cannot edit this setting. You can hide Network1 port if not needed by deselecting the 'Network1(Ethernet)' setting in sidebar of Network tab. If a Modbus TCP device is connected to Network1 already, you need to remove this

[5] http://www.eaton.com/ecm/groups/public/@pub/@electrical/documents/content/td17513_appnote.pdf

Network1 device and then deselect the 'Network 1(Ethernet)' port in sidebar of Netwrok tab. Save the changed setting and Exit edit mode.

Note: Recommend upto 5 PXMP Modbus TCP devices on Network 1 port for optimal performance.

3.5 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.

3.6 Initial Setup

The PXG helps you when adding devices, guiding you through the initial setup steps:To add either a Modbus RTU or INCOM device:

1.Choose Edit.

2. Choose Add Device under the appropriate port.

3. In the sidebar, select the device type under Family.

4. Select the Model Series.

5. Select the device Model.

6. Enter a meaningful name for the device.

7. 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.

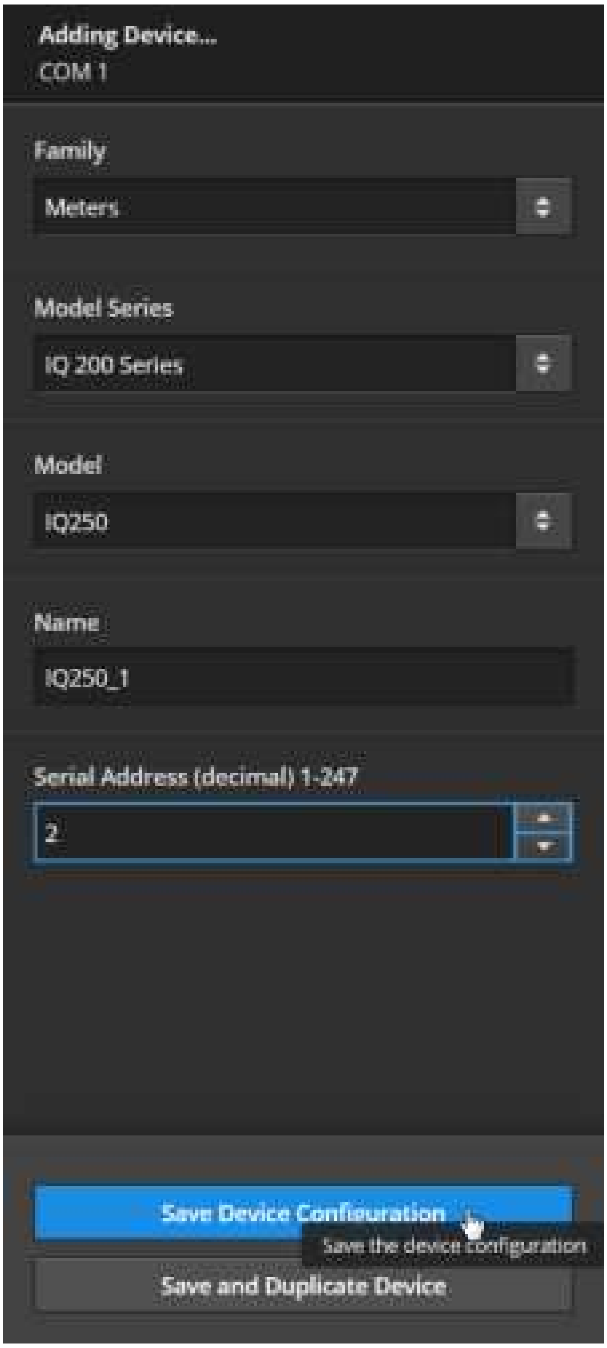
8. If Enable Waveforms is available, decide whether you wish to have the PXG capture these.

9. Choose Save Device Configuration.

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

3.6.1 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.



Adding Device...
COM 1

Family
Meters

Model Series
IQ 200 Series

Model
IQ250

Name
IQ250_1

Serial Address (decimal) 1-247
2

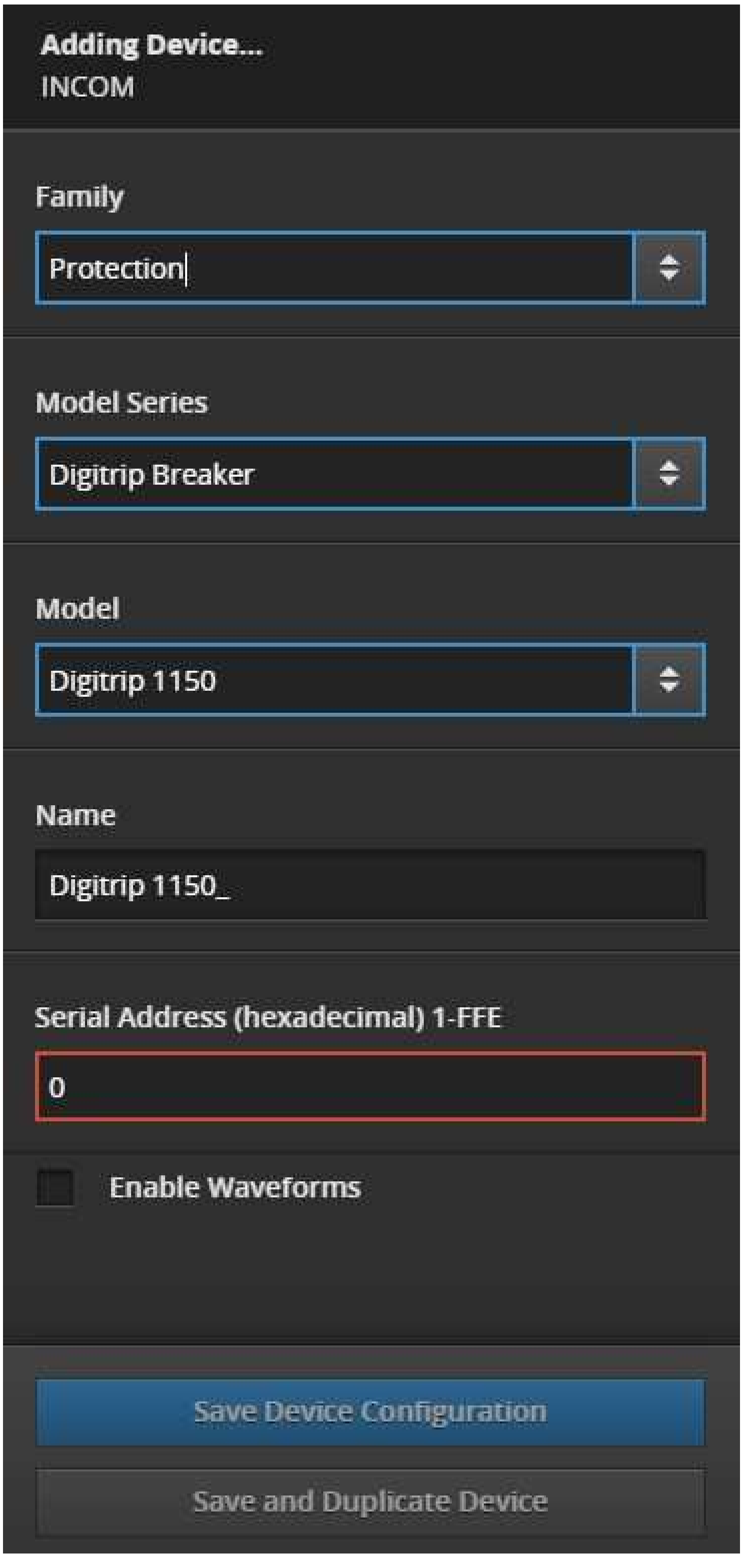
Save Device Configuration
Save the device configuration
Save and Duplicate Device

6 Adding an IQ 250

3.6.2 Example 2: Adding a Digitrip 1150 Breaker

1. Choose the Network tab.
2. Choose Edit.
3. Choose Add Device under INCOM.
4. Select Protection under Family.
5. Select Digitrip Breaker under Model Series
6. Select Digitrip 1150 under Model.

7. Enter a name, such as "Digitrip 1150_1" under Name.
8. Set the Serial Address (1-FFE hexadecimal) to match the address you set on the Digitrip.
9. Choose Enable Waveforms if you wish to view these in the PXG.
10. Choose Save Device Configuration.
11. Choose Edit.



Adding Device...
INCOM

Family: Protection

Model Series: Digitrip Breaker

Model: Digitrip 1150

Name: Digitrip 1150_

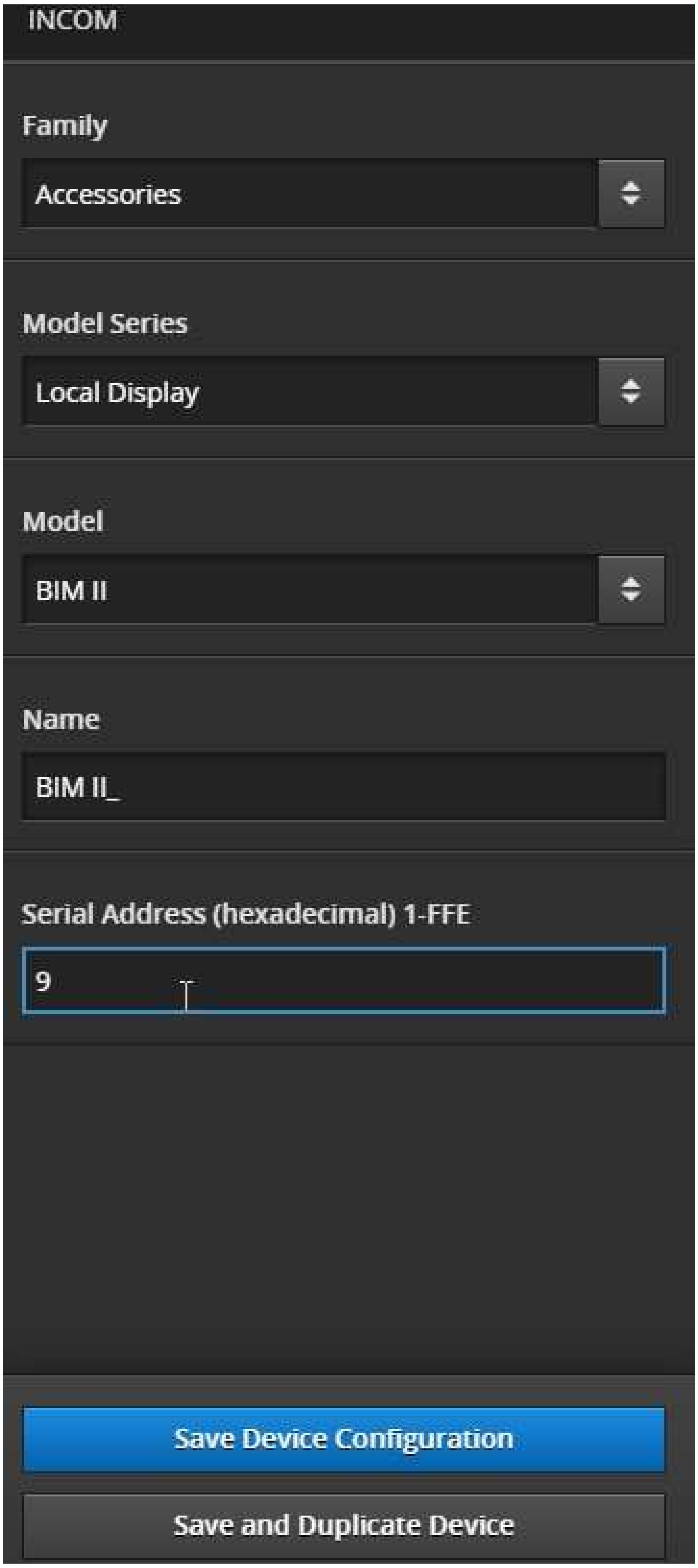
Serial Address (hexadecimal) 1-FFE: 0

□ Enable Waveforms

7 Adding a Digitrip 1150

3.6.3 Example 3: Adding a BIM II Display Device

1. Choose the Network tab.
2. Choose Edit.
3. Choose Add Device under INCOM.
4. Select Accessories under Family.
5. Select Local Display under Model Series
6. Select BIM II under Model.
7. Enter a name, such as "BIM II_1" under Name.
8. Set the Serial Address (1-FFE hexadecimal) to match the address you set on the BIM II.
9. Choose Save Device Configuration.
10. Choose Edit.



INCOM

Family: Accessories

Model Series: Local Display

Model: BIM II

Name: BIM II_

Serial Address (hexadecimal) 1-FFE: 9

8 Adding a BIM II

3.7 Special Considerations for the AEM II

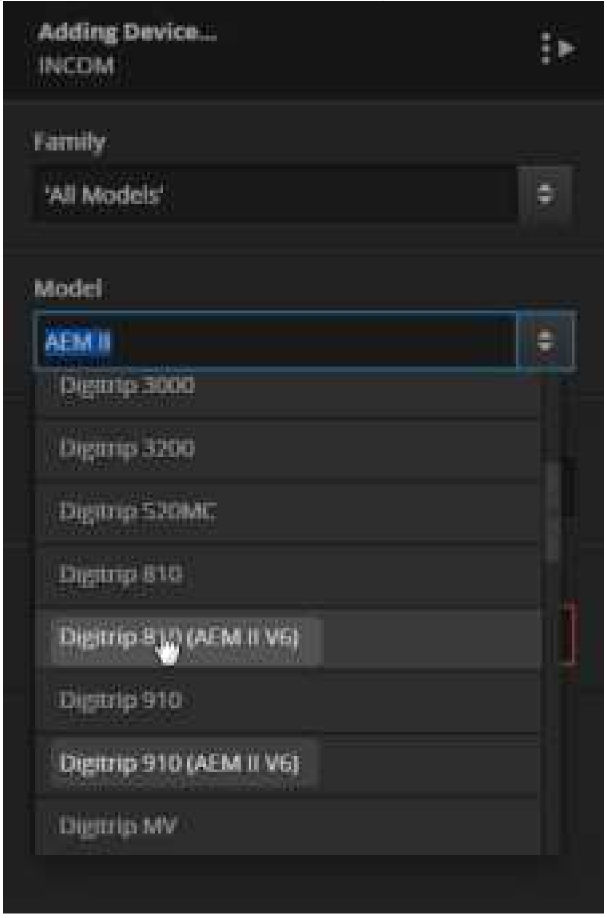
The gateway supports the AEM II with firmware at level 6 or greater. If your AEM II has a sub-network with devices attached, you can add these devices *after* you've added the AEM II to the gateway. Once you have added an AEM II to the gateway, it is important to determine the version of the AEM II:

1. Go to the Network tab.
2. Click Edit.
3. Select the gear icon for Power Expert Gateway
4. Under Choose an action, select System Inventory.

The System Inventory shows the Firmware version for the AEM II device. The AEM II version must be 6 or higher.

For an AEM II Version 7 or higher only the following devices may be added to the sub-network: Digitrip T800, Digitrip 810 and Digitrip 910. For an AEM II version 6, only the following devices may be added to the sub-network: Digitrip T800, Digitrip 810 (AEM II V6) and Digitrip 910 (AEM II V6). If an incompatible device type is added to an AEM II sub-network, the gateway will fail to properly communicate with the device and provide erroneous data.

> *Note: You can use these special version devices only as part of a AEM II sub-network and they will appear as child devices of the AEM II. If you install these special devices without having them on an AEM II sub-network, they either won't communicate at all or will provide erroneous information.*



Adding Device...
INCOM

Family: 'All Models'

Model: AEM II

9 Special versions of devices for use as part of an AEM II sub-network.

4 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.

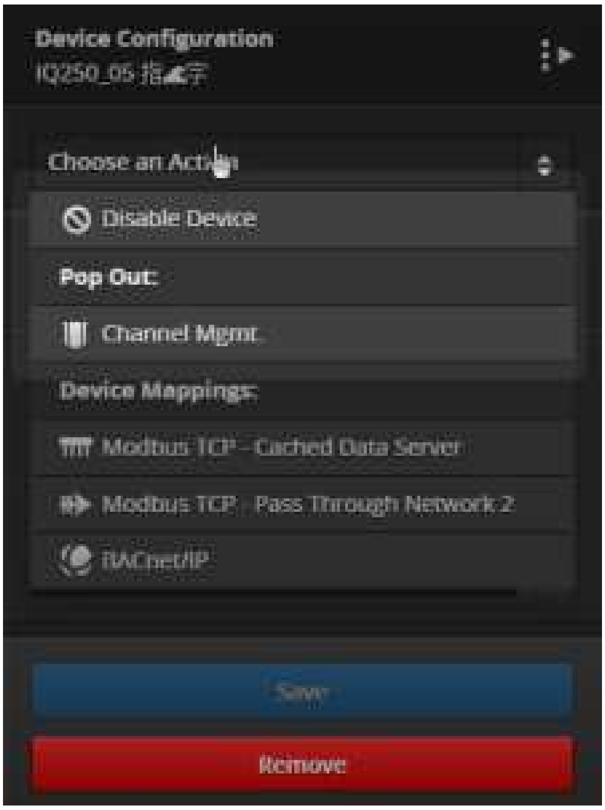
To make configuration easier, you can multi-select and edit multiple channels.

4.1 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.*

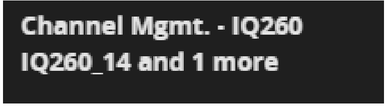


10 Device Configuration Commands in the Choose an Action Menu

4.2 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.

   Channel Mgmt. - IQ260
   IQ260_14 and 1 more

   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.

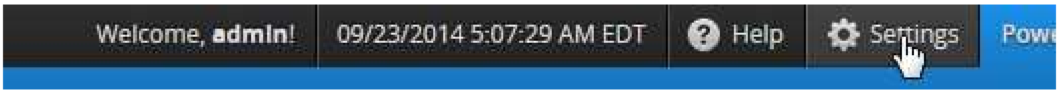
2) If the IQ250/260 was already added to the Gateway, and then the option card configuration occurs, a Gateway reboot is required.

5 Setting Preferences

Under Settings, you can configure:

- Date and Time
- Localization

Settings is in the upper right of the screen.

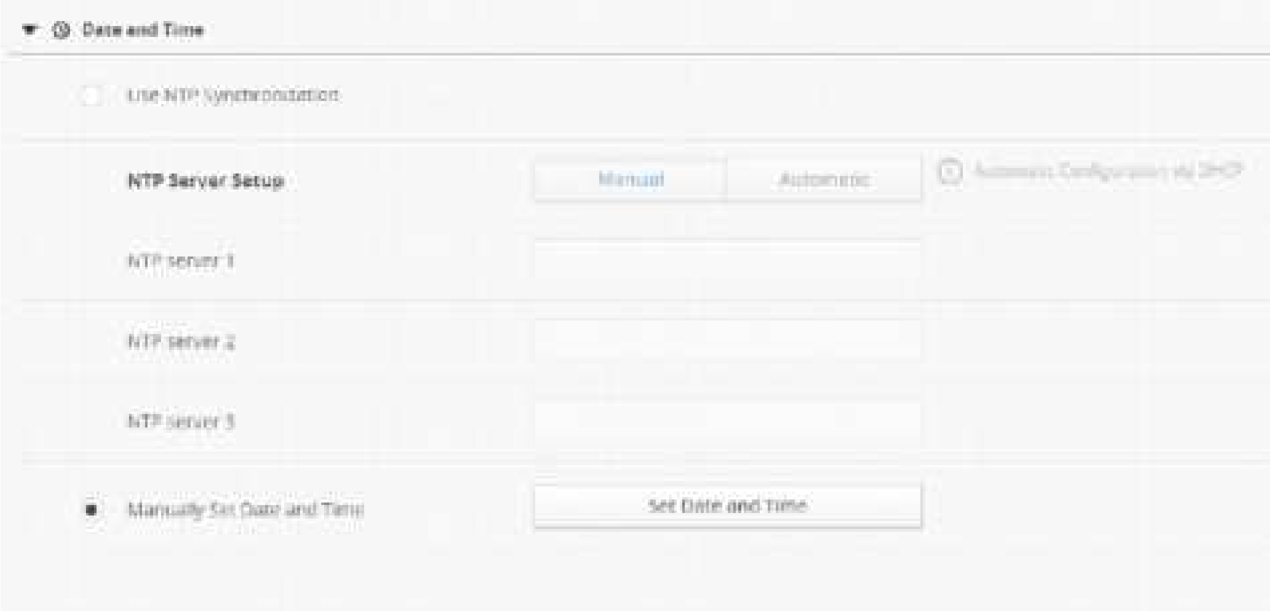


11 Click Settings

5.1 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.*



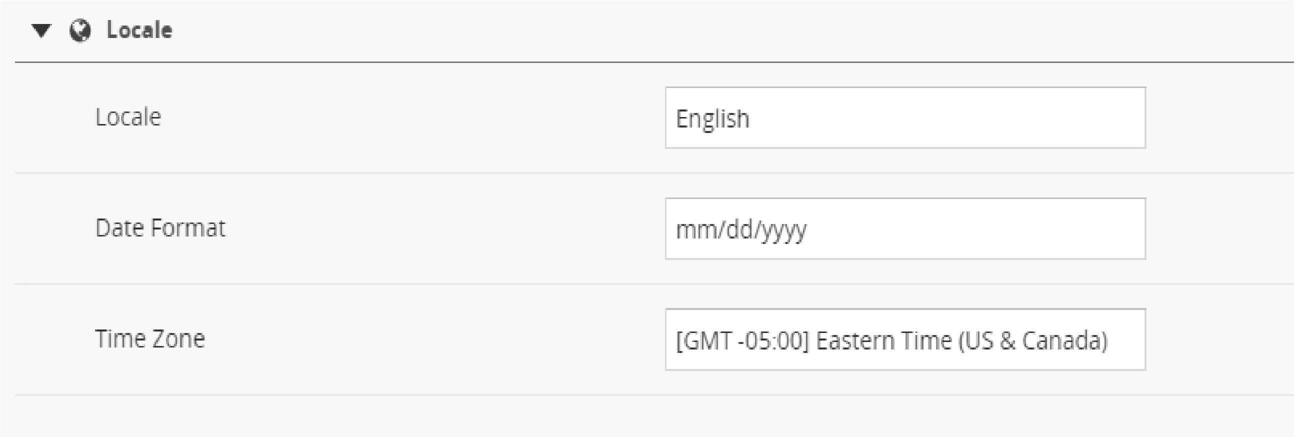
○ Use NTP Synchronization

● Manually Set Date and Time

12 Date and Time Settings Showing Manual Selected

5.2 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

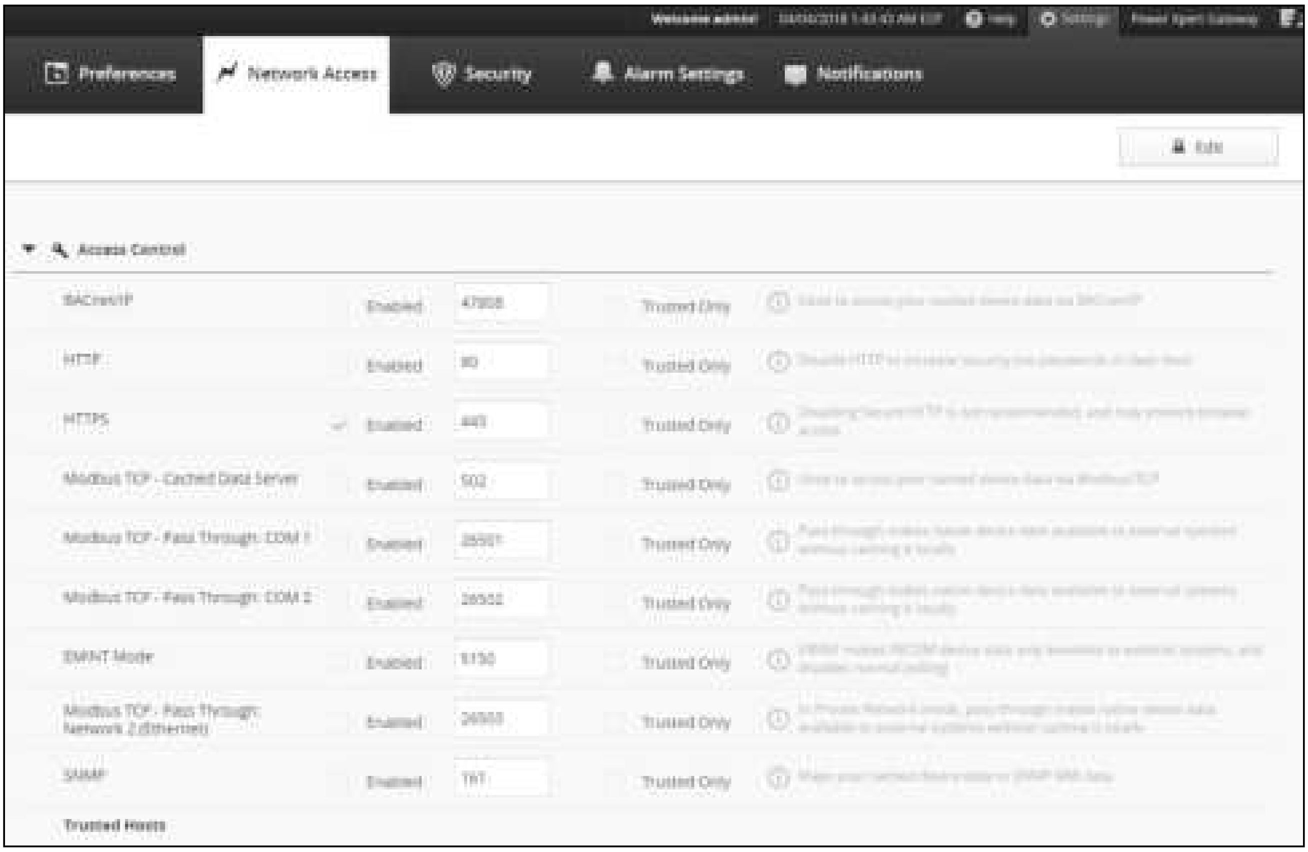
Locale	English
Date Format	mm/dd/yyyy
Time Zone	[GMT -05:00] Eastern Time (US & Canada)

13 Locale Settings

6 Network Access Settings

6.1 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.



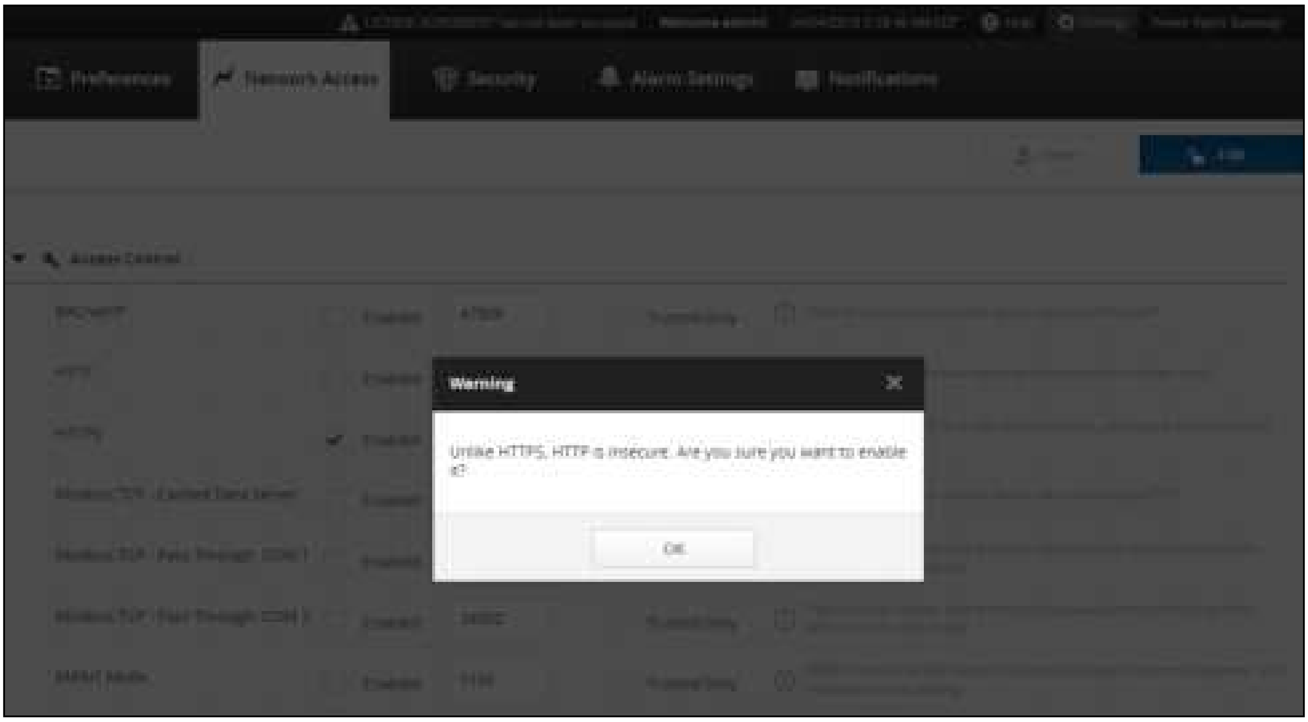
Access Control

BACnet/IP		Enabled	47808	Trusted Only	[illegible]
HTTP		Enabled	80	Trusted Only	Disable HTTP to increase security (no passwords in clear text)
HTTPS	✓	Enabled	443	Trusted Only	Disabling Secure HTTP is not recommended, and may prevent browser access
Modbus TCP - Cached Data Server		Enabled	502	Trusted Only	[illegible]
Modbus TCP - Pass Through: COM 1		Enabled	26501	Trusted Only	[illegible]
Modbus TCP - Pass Through: COM 2		Enabled	26502	Trusted Only	[illegible]
EMINT Mode		Enabled	5150	Trusted Only	[illegible]
Modbus TCP - Pass Through: Network 2 (Ethernet)		Enabled	26503	Trusted Only	[illegible]
SNMP		Enabled	161	Trusted Only	[illegible]

Trusted Hosts

Disabled HTTP and Enabled HTTPS after firmware update

You can enable, disable and change these ports. Enable HTTP, you will be warned for unsecure communication.



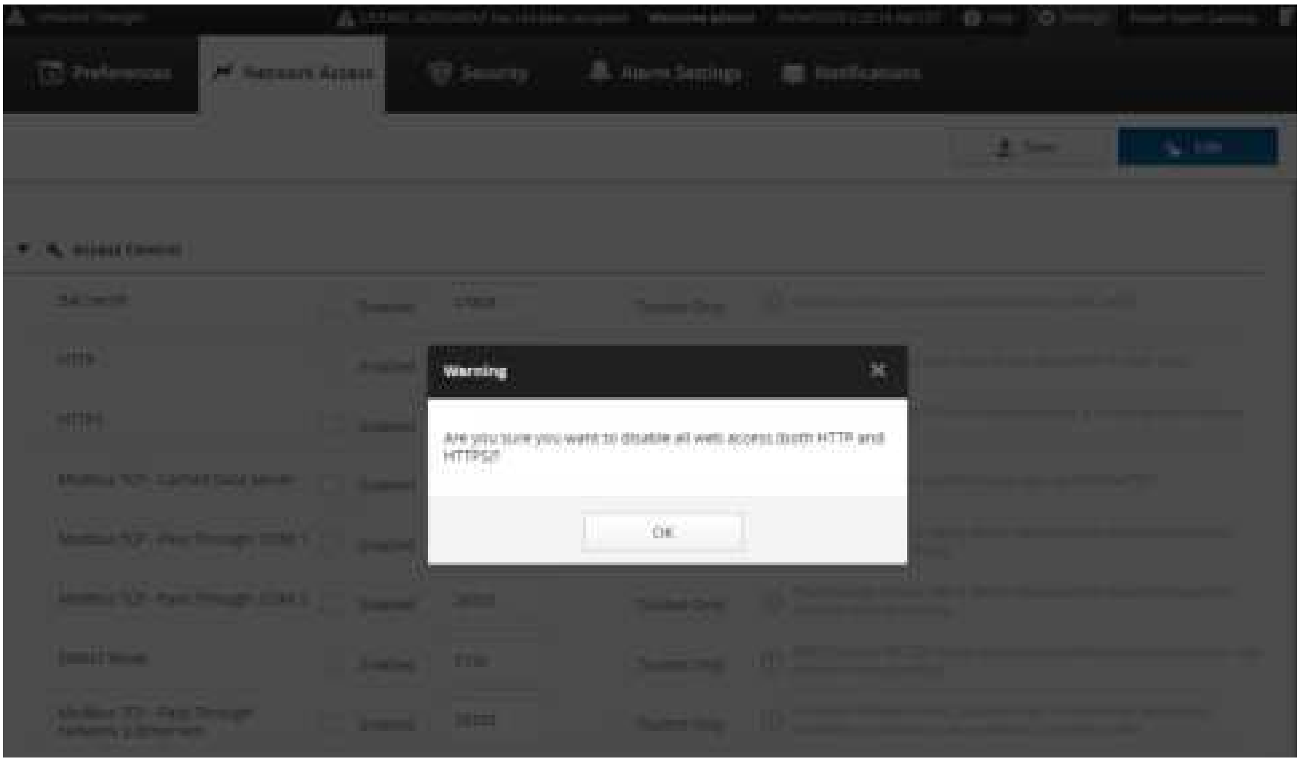
Warning

Unlike HTTPS, HTTP is insecure. Are you sure you want to enable it?

OK

Warning after HTTP setting is Enabled

You can disable both HTTP and HTTPS, you will warned before doing so as you could be locked out via ethernet.If you disabled both HTTP and HTTPS, you can still connect via the USB port.



Warning

Are you sure you want to disable all web access (both HTTP and HTTPS)?

OK

Warning after both HTTP and HTTPS settings are Disabled

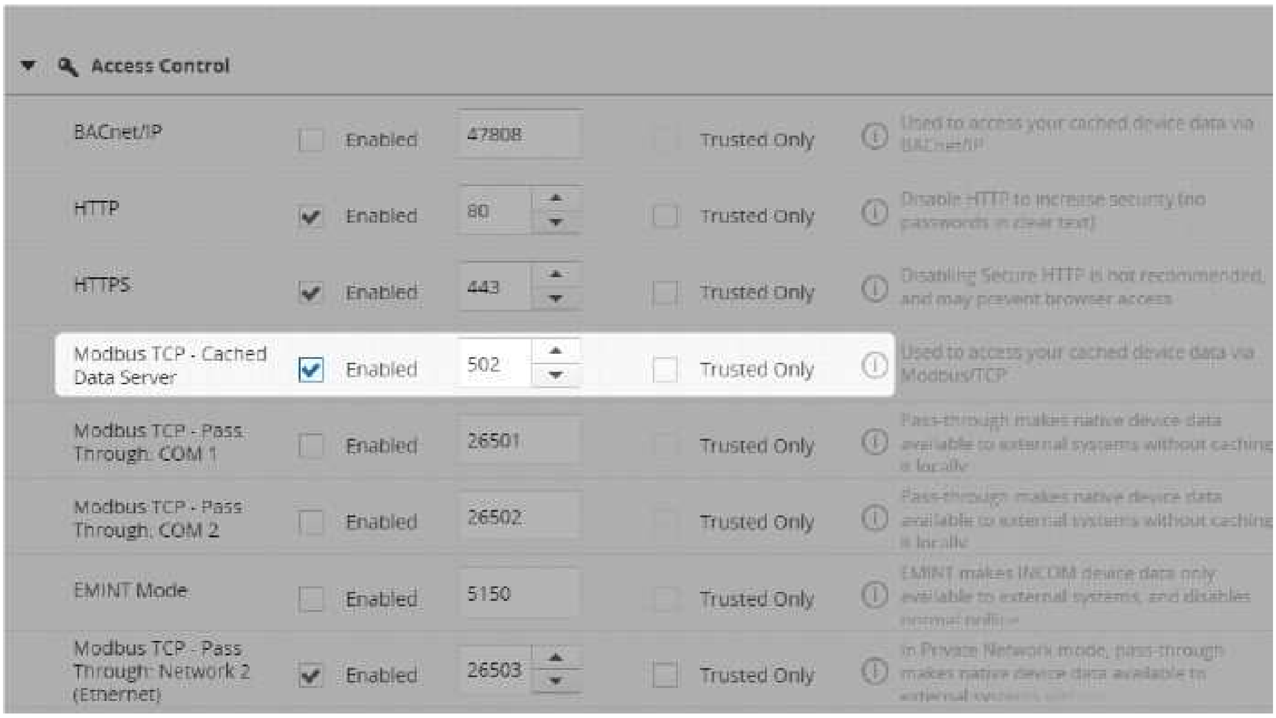
You can also set each port so that it can only be used to access the PXG through trusted host names or IP addresses. While using trusted hosts increases security, you must *be careful*. You can set the gateway to use trusted hosts for HTTP and HTTPS access, and if your PC isn't at an address on the list you could be "locked out" via Ethernet.To correct this situation, you can still connect via the USB port.

> *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.

7 Modbus TCP Server



▾ Access Control

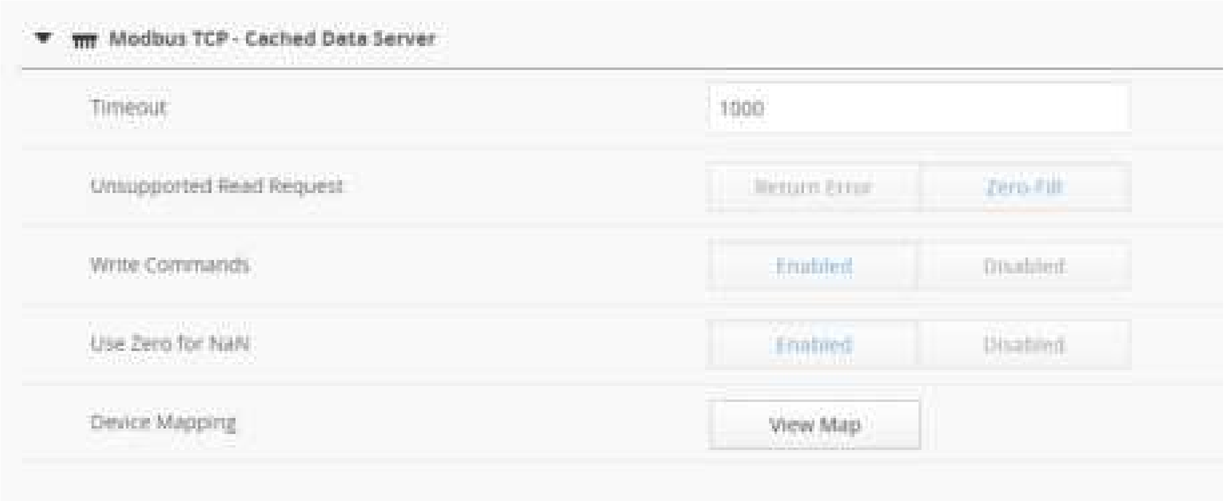
BACnet/IP	□ Enabled	47808	□ Trusted Only	Used to access your cached device data via BACnet/IP
HTTP	☑ Enabled	80	□ Trusted Only	Disable HTTP to increase security (no passwords in clear text)
HTTPS	☑ Enabled	443	□ Trusted Only	Disabling Secure HTTP is not recommended, and may prevent browser access
Modbus TCP - Cached Data Server	☑ Enabled	502	□ Trusted Only	Used to access your cached device data via Modbus/TCP
Modbus TCP - Pass Through: COM 1	□ Enabled	26501	□ Trusted Only	Pass-through makes native device data available to external systems without caching it locally
Modbus TCP - Pass Through: COM 2	□ Enabled	26502	□ Trusted Only	Pass-through makes native device data available to external systems without caching it locally
EMINT Mode	□ Enabled	5150	□ Trusted Only	EMINT makes INCOM device data only available to external systems, and disables normal polling
Modbus TCP - Pass Through: Network 2 (Ethernet)	☑ Enabled	26503	□ Trusted Only	In Private Network mode, pass-through makes native device data available to external systems

14 Modbus TCP Server Enabled

The PXG can also function as a Modbus TCP server, providing channel data as Modbus registers from both Modbus and INCOM devices. The device addresses and Modbus maps for these devices can be downloaded directly from the PXG.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.Normally, the PXG provides only channel data supported by its internal device definition: the EDS file. However, the PXG also has a Modbus "pass through" mode, allowing a Modbus client to connect directly with the device and use the device's native Modbus register set. You can set pass through for COM1, COM2, and Network 2 (Ethernet). 'Pass through' mode is not supported for Network1 Modbus TCP devices.Normally, the PXG provides only channel data supported by its internal device definition: the EDS file. However, the PXG also has a Modbus "pass through" mode, allowing a Modbus client to connect directly with the device and use the device's native Modbus register set. You can set pass through for COM1 and COM2 ports.

7.1 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.



Modbus TCP - Cached Data Server

Timeout: 1000

Unsupported Read Request: Return Error [✓ Zero Fill]

Write Commands: [✓ Enabled] Disabled

Use Zero for NaN: [✓ Enabled] Disabled

Device Mapping: View Map

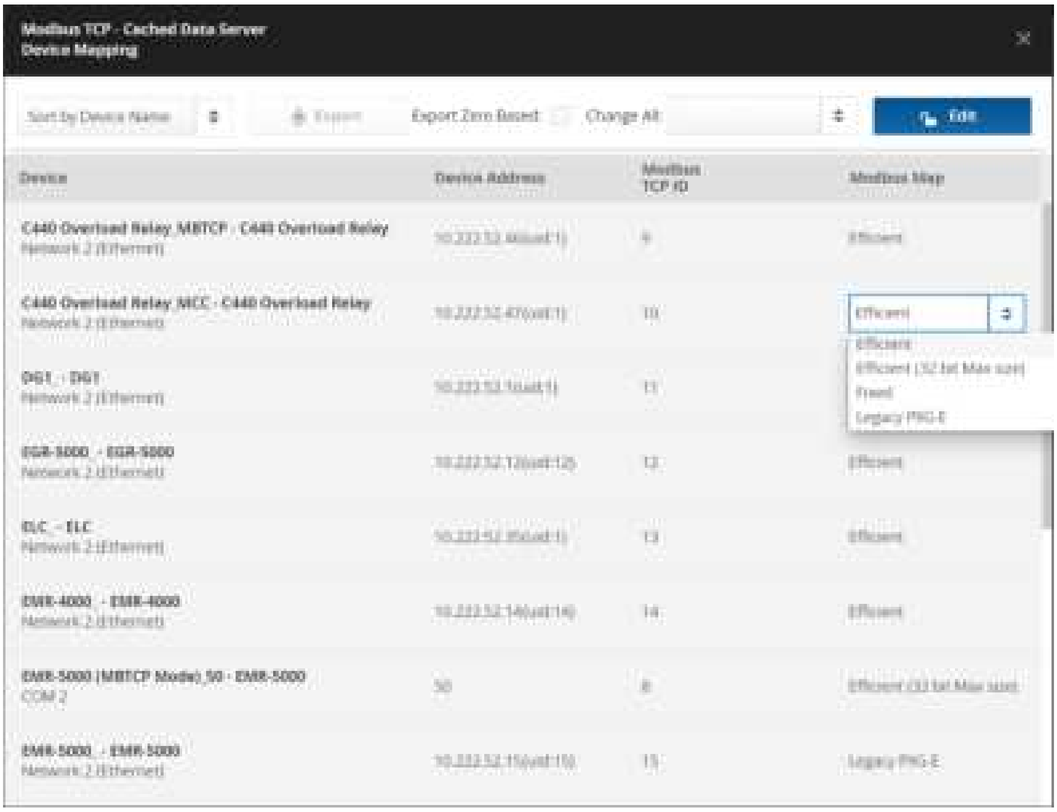
15 Modbus TCP Server Setup

7.2 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.

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).



Modbus TCP - Cached Data Server
Device Mapping

Device	Device Address	Modbus TCP ID	Modbus Map
C440 Overload Relay_MBTCP - C440 Overload Relay Network 2 (Ethernet)	10.222.52.46(uid:1)	9	Efficient
C440 Overload Relay_MCC - C440 Overload Relay Network 2 (Ethernet)	10.222.52.47(uid:1)	10	Efficient
DG1_ - DG1 Network 2 (Ethernet)	10.222.52.1(uid:1)	11	
EGR-5000_ - EGR-5000 Network 2 (Ethernet)	10.222.52.12(uid:12)	12	Efficient
ELC_ - ELC Network 2 (Ethernet)	10.222.52.85(uid:1)	13	Efficient
EMR-4000_ - EMR-4000 Network 2 (Ethernet)	10.222.52.14(uid:14)	14	Efficient
EMR-5000 (MBTCP Mode)_50 - EMR-5000 COM 2	50	8	Efficient (32 bit Max size)
EMR-5000_ - EMR-5000 Network 2 (Ethernet)	10.222.52.15(uid:15)	15	Legacy PXG-E

16 Selecting the Modbus map type

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:

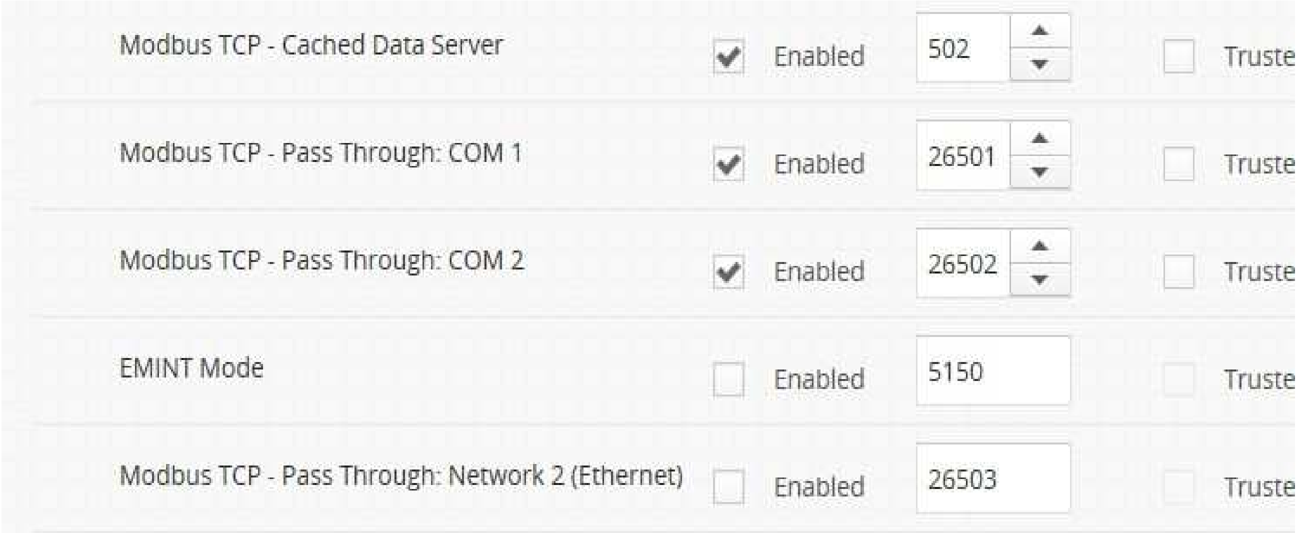
- The device channel name
- The PXG category, such as Power, Current, or Demand.

7.3 Pass Through

7.3.1 Modbus

On the Network Access tab, you can enable pass through mode for either Modbus RTU port as well as Network 2 (Ethernet). 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.



Modbus TCP - Cached Data Server	☑ Enabled	502	□ Truste
Modbus TCP - Pass Through: COM 1	☑ Enabled	26501	□ Truste
Modbus TCP - Pass Through: COM 2	☑ Enabled	26502	□ Truste
EMINT Mode	□ Enabled	5150	□ Truste
Modbus TCP - Pass Through: Network 2 (Ethernet)	□ Enabled	26503	□ Truste

7.4 EMINT (INCOM only)

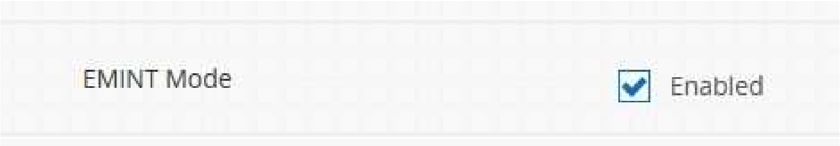
In some cases, you may need to use Eaton's legacy software to configure set points on INCOM devices. The PXG makes this easier by providing a way to connect legacy software directly to the gateway via a UDP connection, allowing that software to then connect to all of the "downstream" INCOM devices.

7.5 Setup

You enable this mode through Settings, on the Network Access tab. You can change the port as well.

An important point: INCOM networks can only have one master, and when EMINT mode is active the externally connected software takes over that role. So, as long as EMINT mode is active, all INCOM devices are essentially disconnected from monitoring by the PXG. The INCOM channel values won't be displayed and alarms for INCOM devices can't be issued. For this reason, while EMINT mode is active INCOM devices will be shown as not communicating in the PXG interface. Unless there's a valid reason to leave the external software connected to the INCOM network, you should disable EMINT mode as soon as you've finished configuring INCOM set points.

> ***Important***: *If you have a legacy Eaton PowerNet system, or some other reason to keep EMINT Mode active, you should enable Trusted Hosts to ensure that only one INCOM master will be on the network.*



EMINT Mode ☑ Enabled

8 BACnet IP Server

8.1 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.*

8.1.1 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.

8.1.2 Auto-Assign Gateway ID

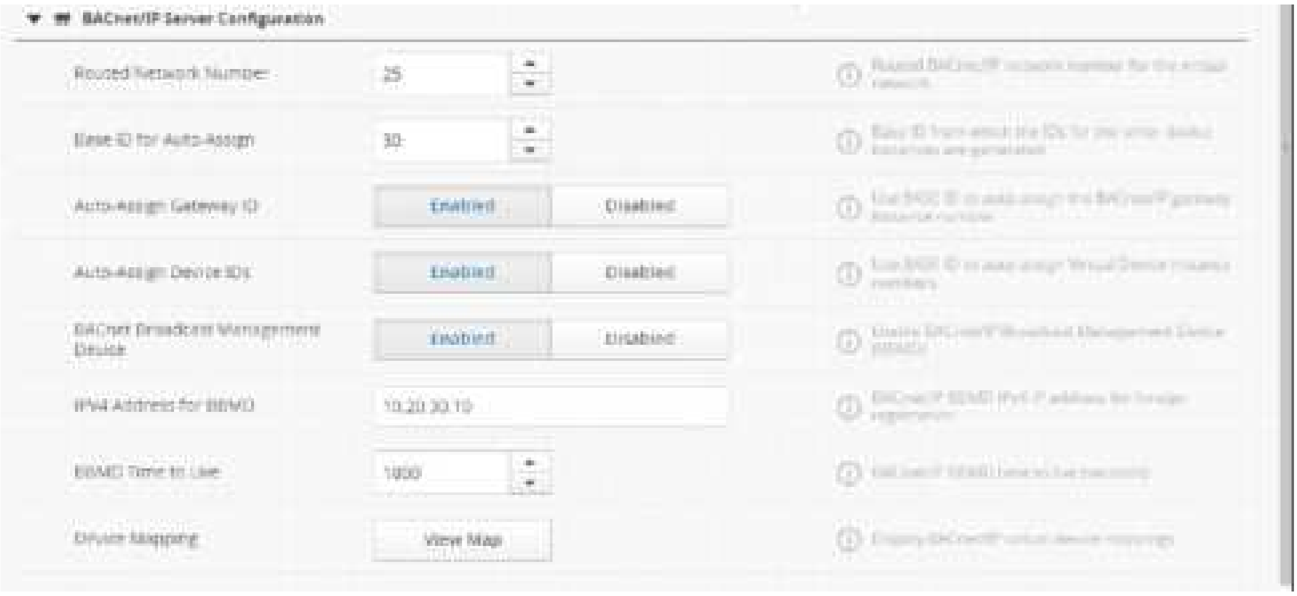
If enabled, the ID for the gateway is automatically assigned. If you set a Base ID, the gateway will be the base value plus one. If disabled, you can manually set the ID by clicking View Map.

8.1.3 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.

8.1.4 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.



BACnet/IP Server Configuration

Routed Network Number: 25 — Routed BACnet/IP network number for the virtual network

Base ID for Auto-Assign: 30 — Base ID from which the IDs for the virtual device instances are generated

Auto-Assign Gateway ID: Enabled / Disabled — Use PXG ID to auto-assign the BACnet/IP gateway instance number

Auto-Assign Device IDs: Enabled / Disabled — Use PXG ID to auto-assign Virtual Device instance numbers

BACnet Broadcast Management Device: Enabled / Disabled — Enable BACnet/IP Broadcast Management Device (BBMD)

IPv4 Address for BBMD: 10.20.30.10 — BACnet/IP BBMD IPv4 IP address for foreign registration

BBMD Time to Live: 1800 — BACnet/IP BBMD time to live (seconds)

Device Mapping: View Map — Display BACnet/IP virtual device mappings

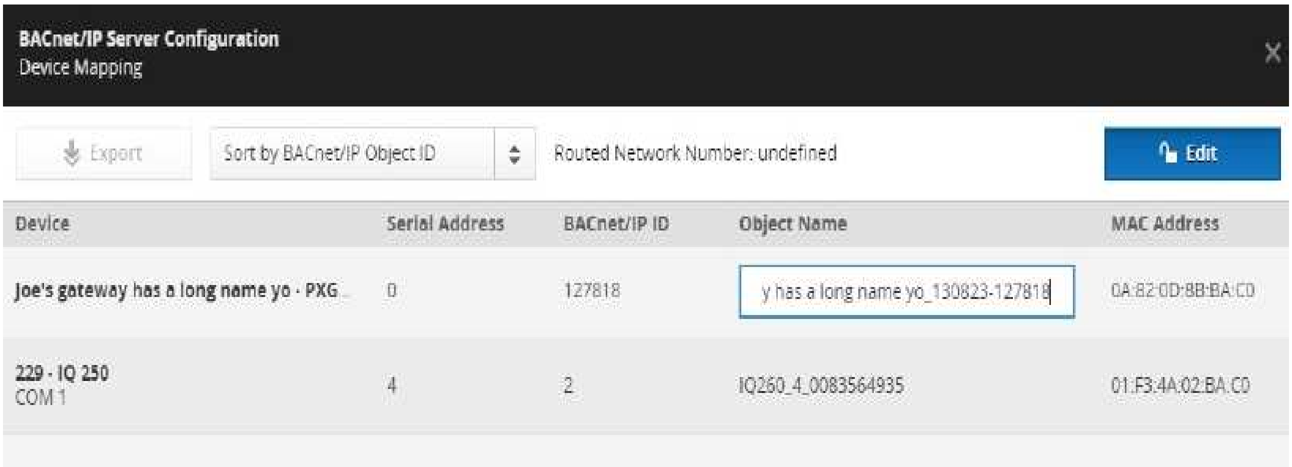
17 BACnet/IP Settings

18

8.2 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.



BACnet/IP Server Configuration

Device Mapping

Routed Network Number: undefined

Device	Serial Address	BACnet/IP ID	Object Name	MAC Address
Joe's gateway has a long name yo - PXG...	0	127818	y has a long name yo_130823-127818	0A:82:0D:8B:BA:C0
229 - IQ 250 COM 1	4	2	IQ260_4_0083564935	01:F3:4A:02:BA:C0

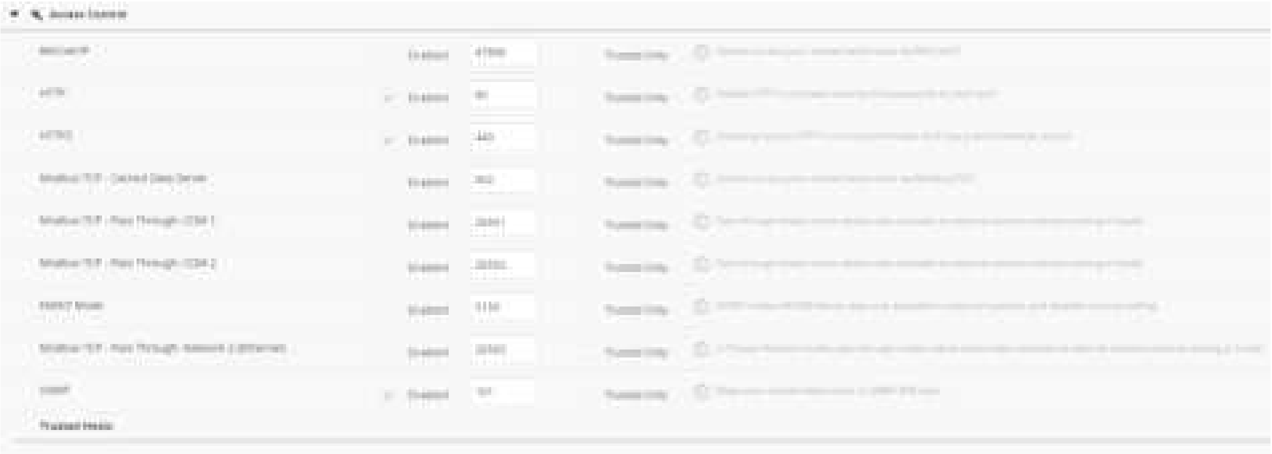
19 View Map Dialog Box

20

9 SNMP Server

9.1 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.



21 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.

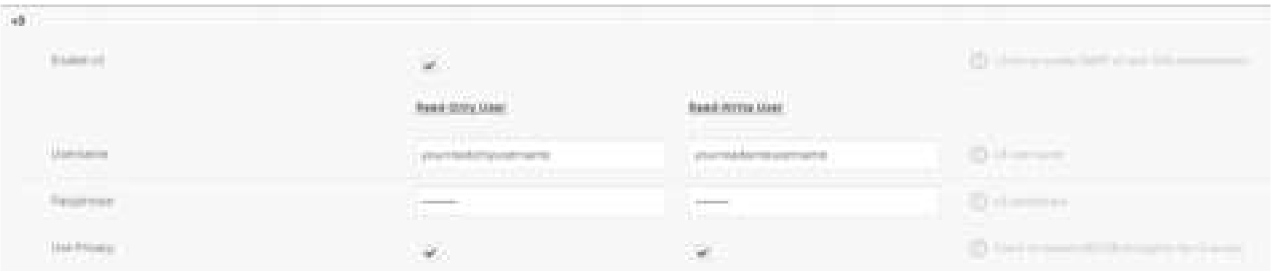
9.1.1 Enabling SNMP v1 and v3 Support

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 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.

9.1.2 Detailed SNMP v3 Configuration

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

> **Note**
> When SNMP v3 is enabled, the gateway automatically uses SHA authentication.



v3

	Read-Only User	Read-Write User
Enable v3	✓	
Username	[illegible]	[illegible]
Passphrase	------	------
Use Privacy	✓	✓

22 SNMP v3 Configuration

9.1.2.1 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.

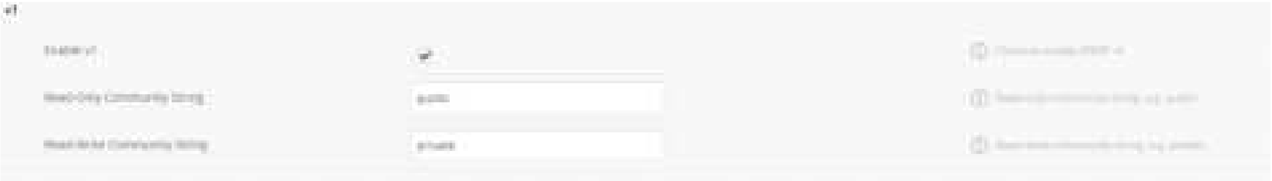
9.1.2.2 Configuring the Read-Write User

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.

9.1.3 Detailed SNMP v1 Configuration

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



v1

Enable v1	✓
Read-Only Community String	public
Read-Write Community String	private

23 SNMP v1 Configuration

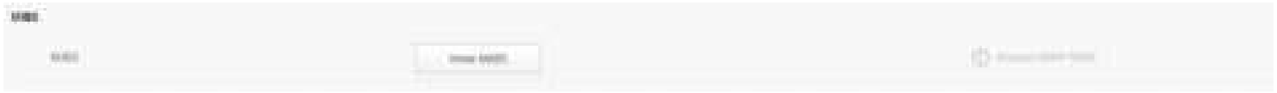
9.1.3.1 Configuring the Read-Only Community String

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.

9.1.3.2 Configuring the Read-Write Community String

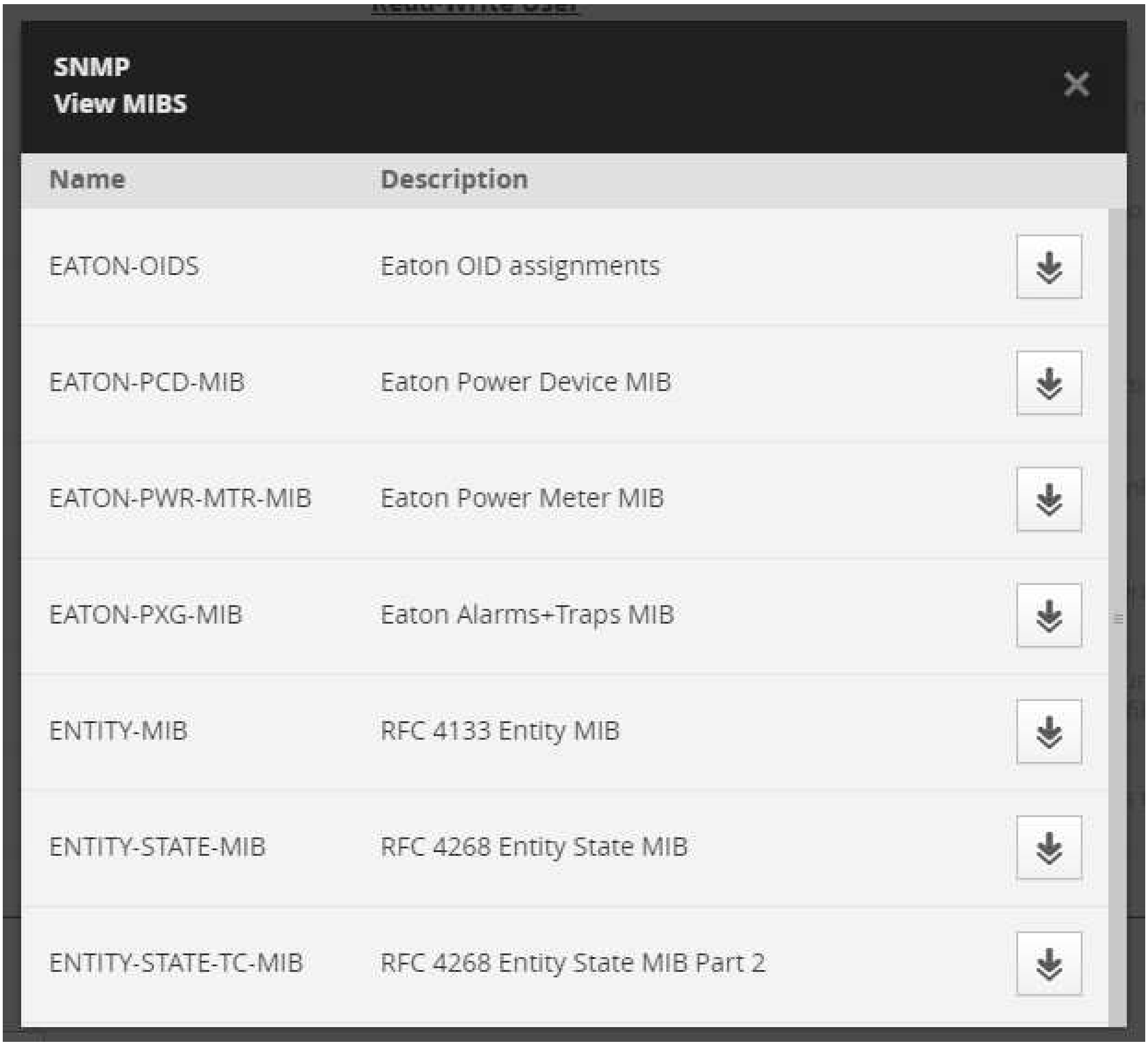
Similar to the Read-Only string, the gateway provides the commonly used string *private* for read-write access. Please take this opportunity to change the Read-Write Community string to something more secure for your installation.

9.1.4 Gateway-provided SNMP MIB Support



24 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.



SNMP
View MIBS

Name	Description
EATON-OIDS	Eaton OID assignments
EATON-PCD-MIB	Eaton Power Device MIB
EATON-PWR-MTR-MIB	Eaton Power Meter MIB
EATON-PXG-MIB	Eaton Alarms+Traps MIB
ENTITY-MIB	RFC 4133 Entity MIB
ENTITY-STATE-MIB	RFC 4268 Entity State MIB
ENTITY-STATE-TC-MIB	RFC 4268 Entity State MIB Part 2

25 Downloadable MIB Files

9.1.4.1 Eaton OIDs

These objects document all the object identifier assignments for Eaton products. Downloaded Filename: EATON-OIDS.txt

9.1.4.2 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

9.1.4.3 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

> ⓘ **Scaled Energy Values**
> Energy-related SNMP objects with units of Kilo or Mega may return values that require scaling adjustment in order to match the units listed in the Power Meter MIB. Examples of supported devices with scaled energy values include the PXM1000, PXBCM, PXMP, EM20-M, EM21-M, EM22-M, EM24-M, AC Pro II and Solar Inverter.

9.1.4.4 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

9.1.4.5 Entity and Entity State MIB Support

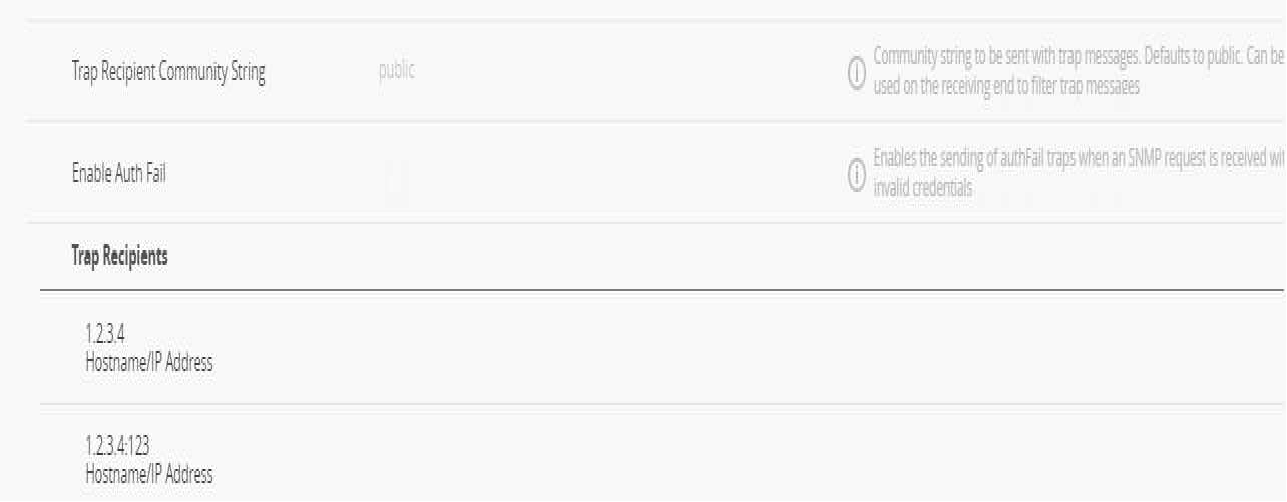
The objects in these MIB files provide information standard in the industry:

- 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.

9.1.5 Configuring v1 Trap Support



Trap Recipient Community String public Community string to be sent with trap messages. Defaults to public. Can be used on the receiving end to filter trap messages

Enable Auth Fail Enables the sending of authFail traps when an SNMP request is received wi invalid credentials

Trap Recipients

1.2.3.4
Hostname/IP Address

1.2.3.4:123
Hostname/IP Address

26 Trap-related configuration

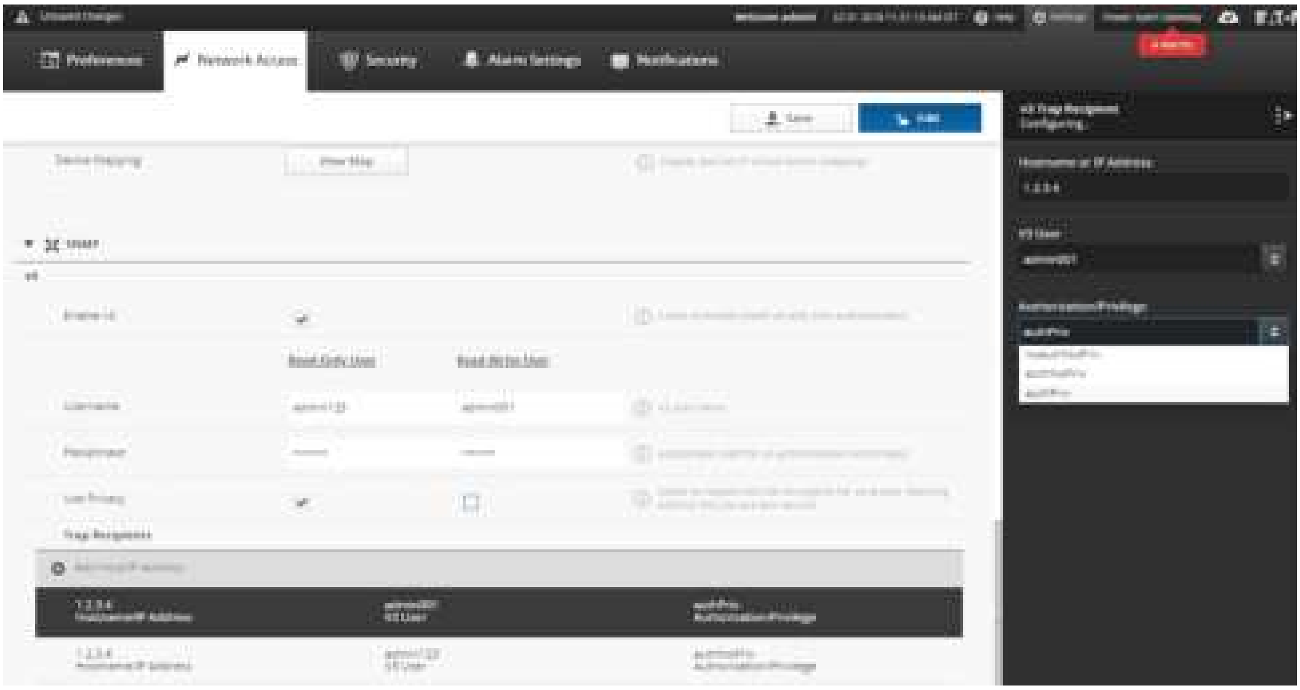
9.1.5.1 v1 Trap Recipient Community String

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.

9.1.5.2 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.

9.1.6 Configuring v3 Trap Support



9.1.6.1 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.

9.1.7 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

10 Notifications

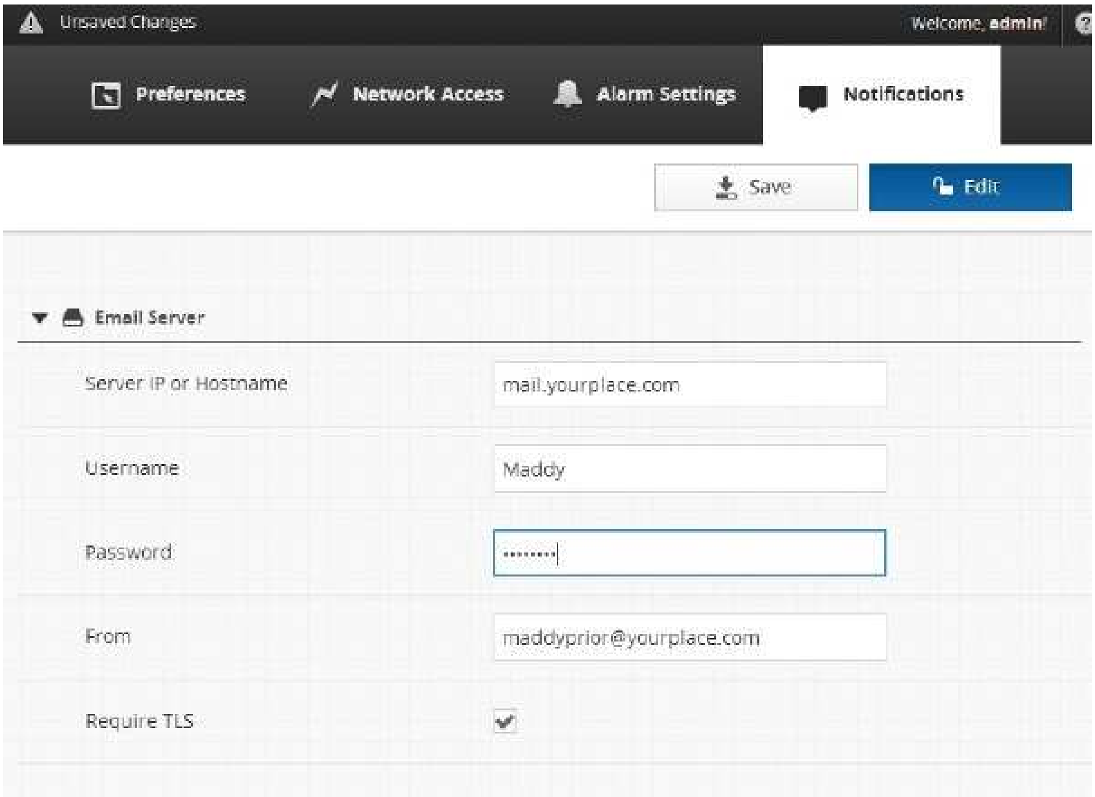
Notifications provide email alerts for alarms and related activities, such as acknowledging an alarm, or when an alarm is cleared. Emails can include attached event, trend, and/or data logs.

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

10.1 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:

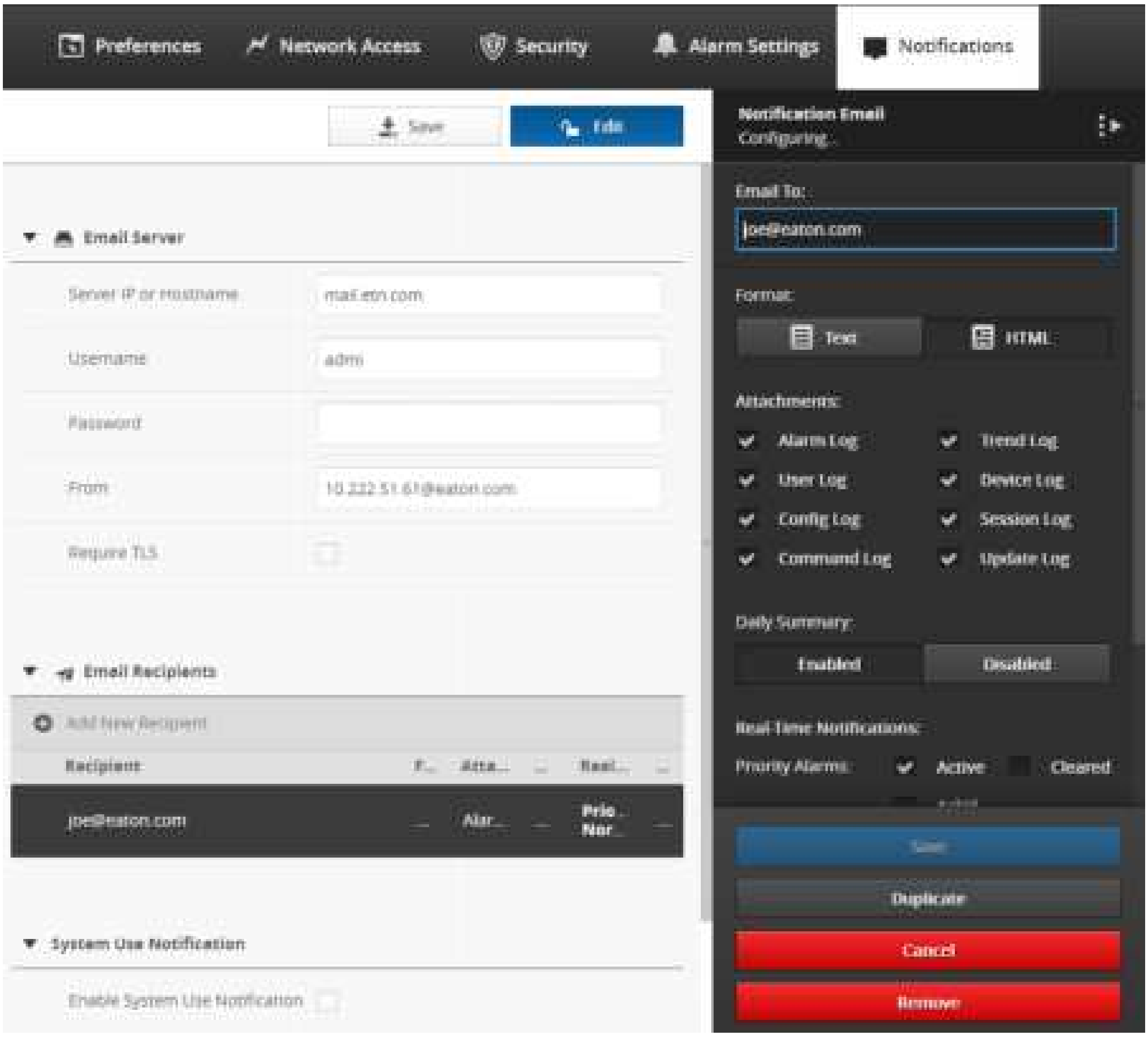
- The address of the email server.
- The username and password (if required) for the email account used by the PXG. It's best if you use a username with a password that doesn't change. If the password for that user changes, you'll need to reset it here. Otherwise, Notifications will no longer work.
- 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.



Server IP or Hostname	mail.yourplace.com
Username	Maddy
Password	••••••••
From	maddyprior@yourplace.com
Require TLS	✓

27 Mail Server Setup

10.2 Adding Recipients



Server IP or Hostname: mail.etn.com

Username: admin

Password:

From: 10.222.51.61@eaton.com

Require TLS □

joe@eaton.com ... Alar... ... Prio... Nor...

Enable System Use Notification □

Email To: joe@eaton.com

Format: Text | HTML

Attachments:
- ✓ Alarm Log
- ✓ User Log
- ✓ Config Log
- ✓ Command Log
- ✓ Trend Log
- ✓ Device Log
- ✓ Session Log
- ✓ Update Log

Daily Summary: Enabled | Disabled

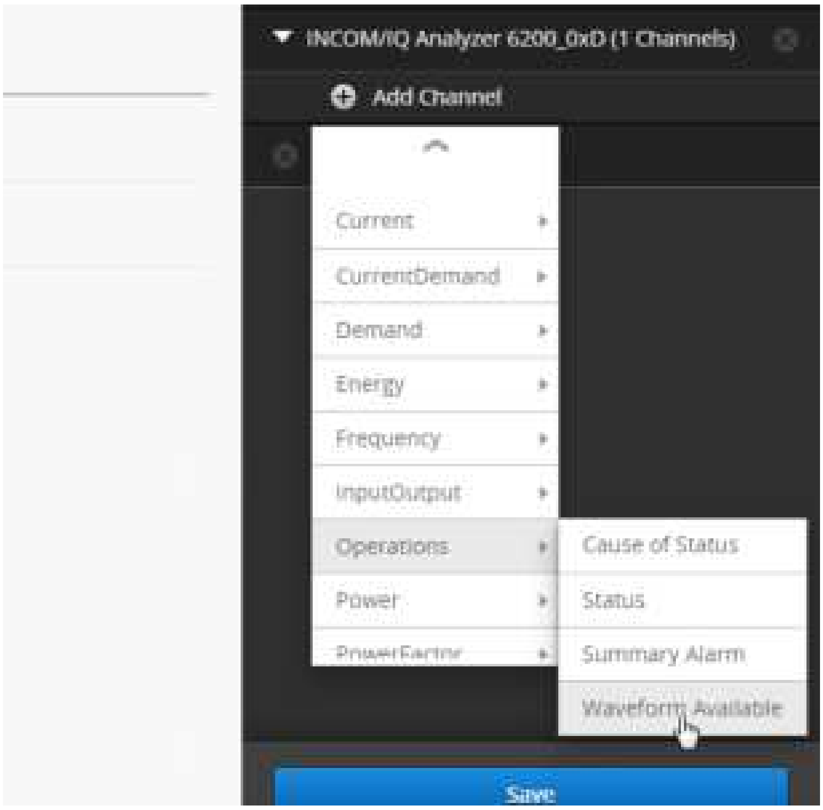
Priority Alarms: ✓ Active □ Cleared

28 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.



29 Selecting the Waveform Available channel.

10.3 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.

11 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(see page 86) .[6]

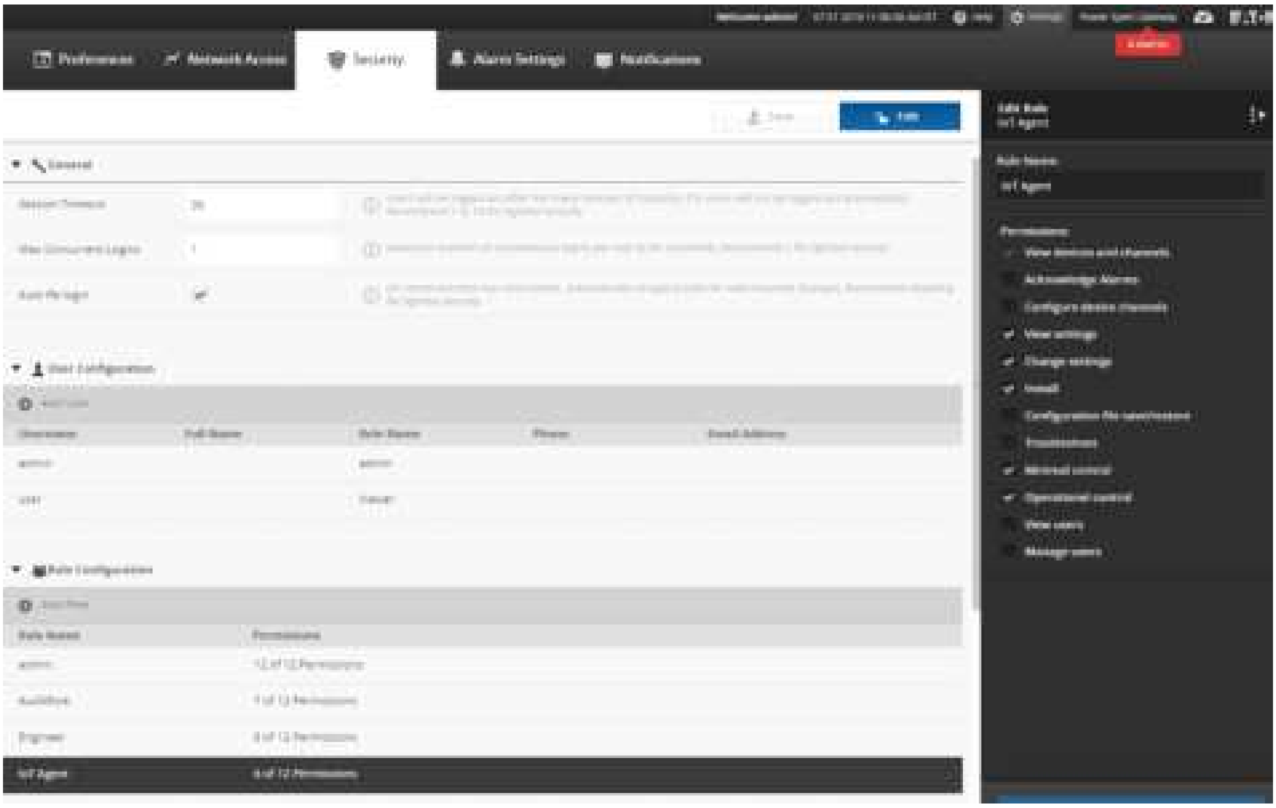
Controlling access to the PXG is a vital component in any effort to secure it. Many regulatory agencies and standards organizations now recommend or require Role-Based Access Control (RBAC) as part of any access control effort. To support this, the PXG has a robust set of tools that can be used to create 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 thesite.

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.*



Session Timeout 30

Max Concurrent Logins 1

Auto Re-login ✓

Username	Full Name	Role Name	Phone	Email Address
admin		admin		
user		Viewer		

Role Name	Permissions
admin	12 of 12 Permissions
AuditRole	1 of 12 Permissions
Engineer	8 of 12 Permissions
IoT Agent	6 of 12 Permissions

Edit Role
IoT Agent

Role Name
IoT Agent

Permissions
- View devices and channels
- Acknowledge Alarms
- Configure device channels
- ✓ View settings
- ✓ Change settings
- ✓ Install
- Configuration file save/restore
- Provisioning
- ✓ Minimal control
- ✓ Operational control
- View users
- Manage users

30 Security Tab

[6] http://cipt0534.nam.ci.root:8090/display/UD/.Cybersecurity+Hardening+the+PXG+vpsi9a

11.1 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	
View devices and channels	View devices and information from their channels. Every user gets this by default.
Acknowledge alarms	Click the Acknowledge button and enter a note about the alarm; e.g., what caused the alarm and what action was taken.
Configure device channels	Enable trending for channels (where trending is available), set alarm triggers, and enable or disable individual channels.
View settings	View, but not change, PXG settings. This is automatically selected if you select Change settings.
Change settings	Change PXG settings in the various Settings tabs.
Install	Install devices in the PXG and update the PXG firmware.
Configuration file save/restore	Save all configuration information to a file and set all PXG configuration parameters from a configuration file.

Troubleshoot	Remotely reboot the PXG. A role with this permission may be required by Eaton personnel to service/troubleshoot the gateway.
Minimal control	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.
Operational control	Issue device commands, such as opening or closing breakers or resetting breaker trips. Also associated with configuring DIM KYZ settings.
View users	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.
Manage users	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.

11.2 Creating Users

1. On the **Security** tab in **Settings**, click **Edit**.
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**.

11.3 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:

1. On the **Security** tab in **Settings**, click **Edit**.
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:

1. On the **Security** tab in **Settings,** click **Edit.**
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.**

11.4 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.

Audit Log Name	Any of These Permissions Allow Log Download
User	View users
Device	View users, Install, Configure Device Channels, Troubleshoot
Configuration	View users, Install, Configure Device Channels
Session	View users
Command	View users
Update	View users, Install. Troubleshoot, Configuration file save/restore

11.5 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.

11.6 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.

11.7 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.

11.8 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.

11.9 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.

11.10 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.

11.11 Password Policy

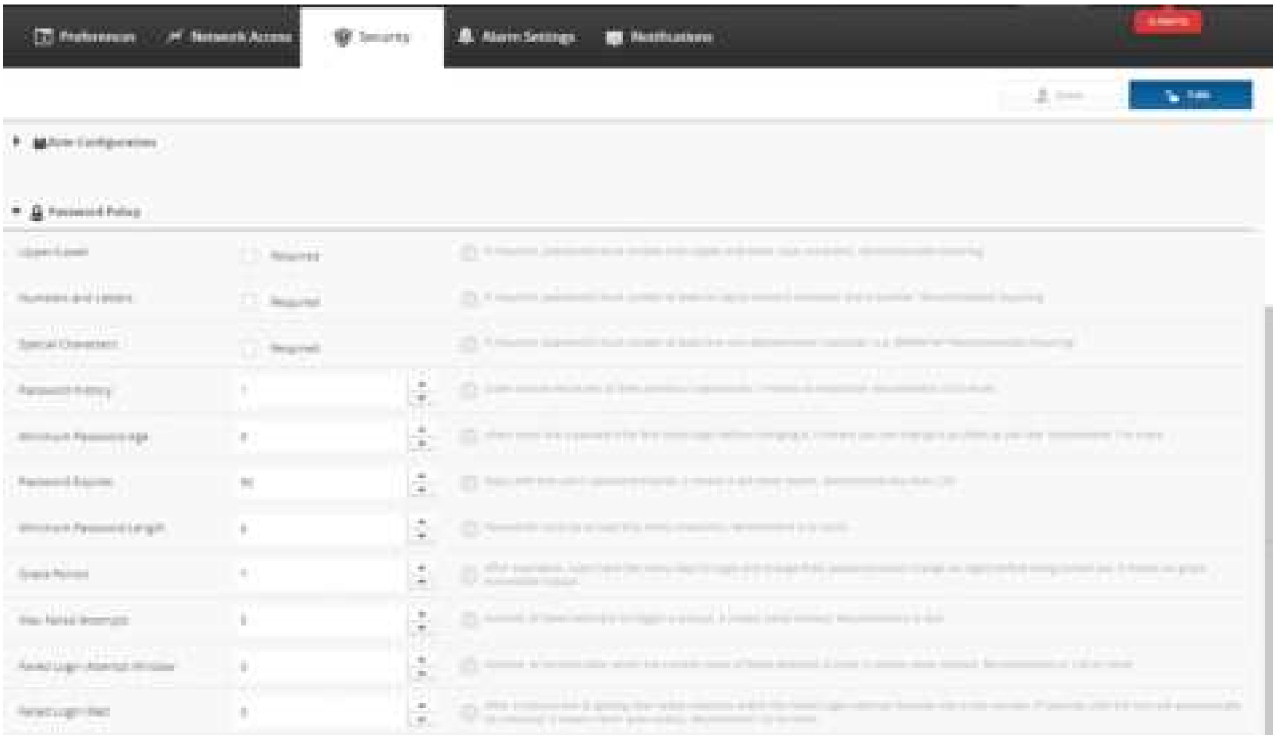
The security provided by restricting access to authorized users is only as strong as uniqueness of the user passwords. The Password Policy settings provide a mechanism for security administrators make it more difficult for unauthorized users to guess the passwords of their users. It also provides a mechanism 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:

1. On the **Security** tab in **Settings,** click **Edit.**
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 minimm length was 4. Existing (shorter) passwords are still valid, but any changes require a new minimum length of 6.



31 Password Policy

11.12 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:

1. On the **Security** tab in **Settings,** click **Edit.**
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.

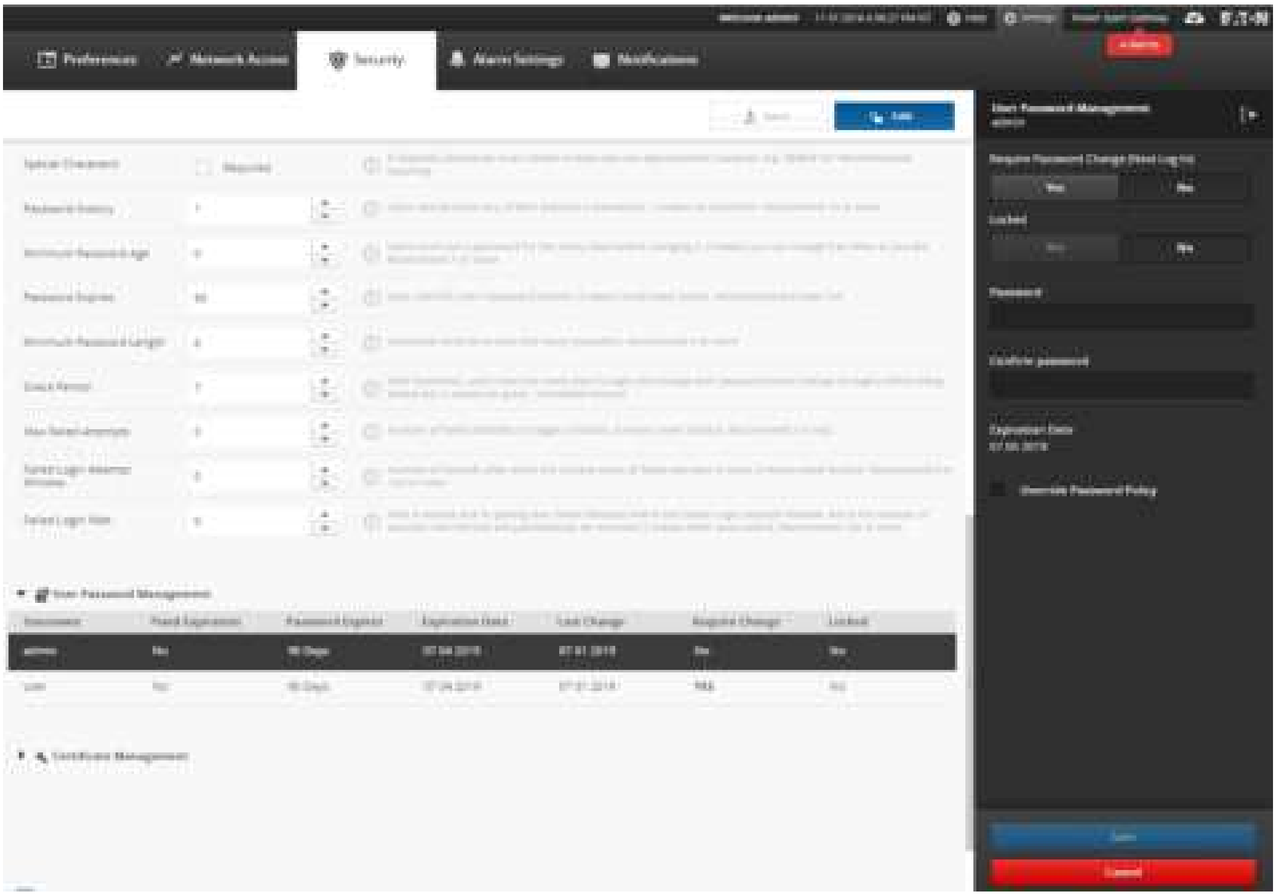
5. Click **Save.**

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 to so the user can replace the password with one of their own.

11.12.1 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:

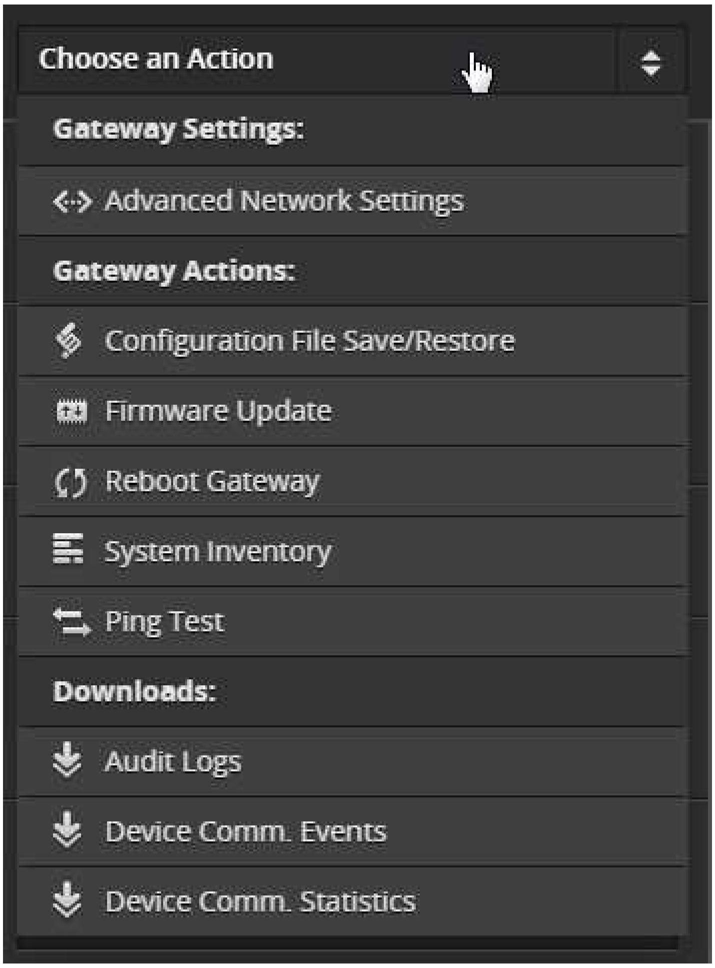
1. Changing user's password.
2. Editing user's properties.
3. Editing global password policy (whether expiration time or something else like "require special characters") re-evaluates all users.



32 User Password Management

12 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.



33 Choose an Action Menu

12.1 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[7] 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.

[7] 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.

12.1.1 **Audit Logs**

The following audit logs are available to users, depending on the permissions(see page 50) their account has been granted, and provide:

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

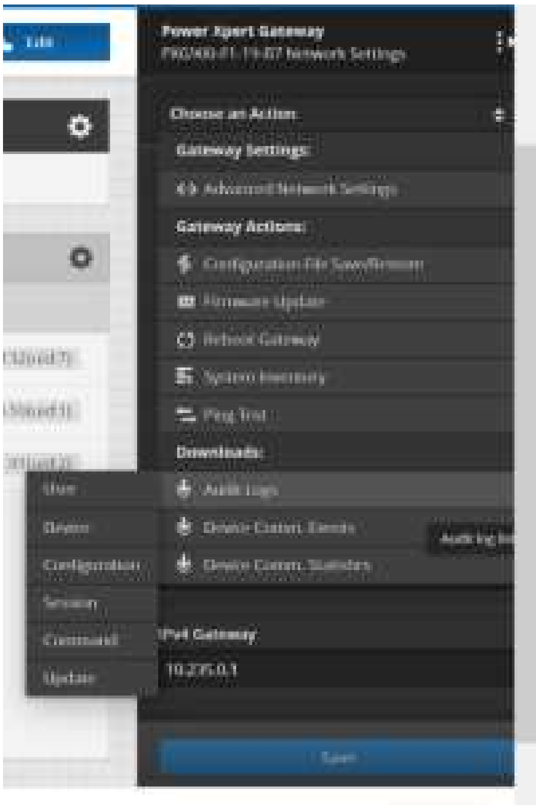
Device – Content related to the addition, removal, enabling, and disabling of connected devices.

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.



IPv4 Gateway

10.235.0.1

Audit Logs

13 Setting Alarms

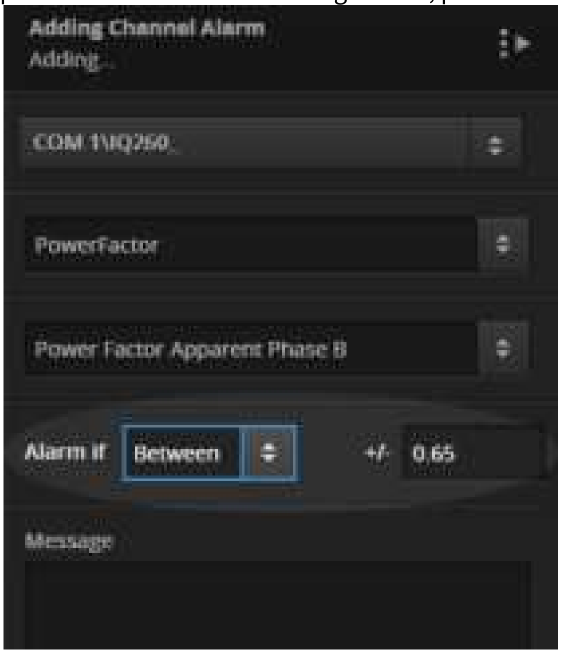
You can set custom alarms for any channel on any connected device directly in the PXG. Each alarm configuration references values on a single channel and specifies either:

- 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.

13.1 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.



Adding Channel Alarm
Adding...

COM 1\IQ260

PowerFactor

Power Factor Apparent Phase B

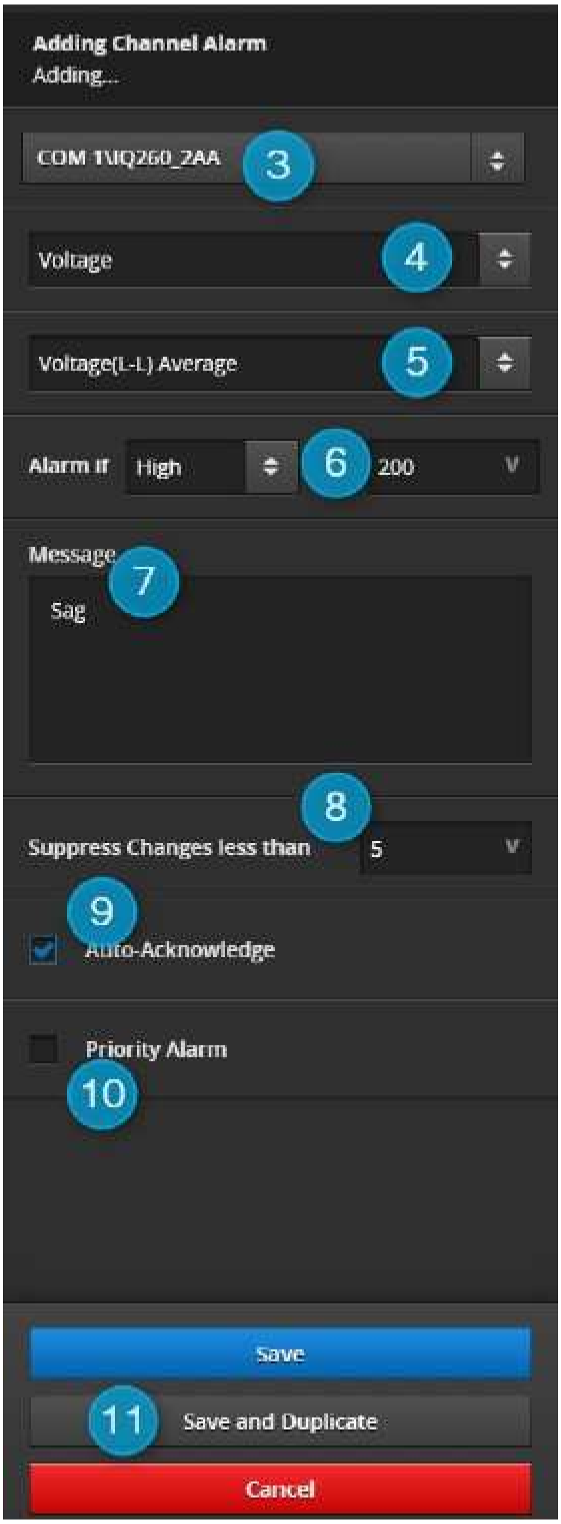
Alarm if Between +/- 0.65

Message

34 Power Factor Between Setting

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.



Adding Channel Alarm
Adding...

COM 1\IQ260_2AA

Voltage

Voltage(L-L) Average

Alarm if High 200 V

Message
Sag

Suppress Changes less than 5 V

☑ Auto-Acknowledge

□ Priority Alarm

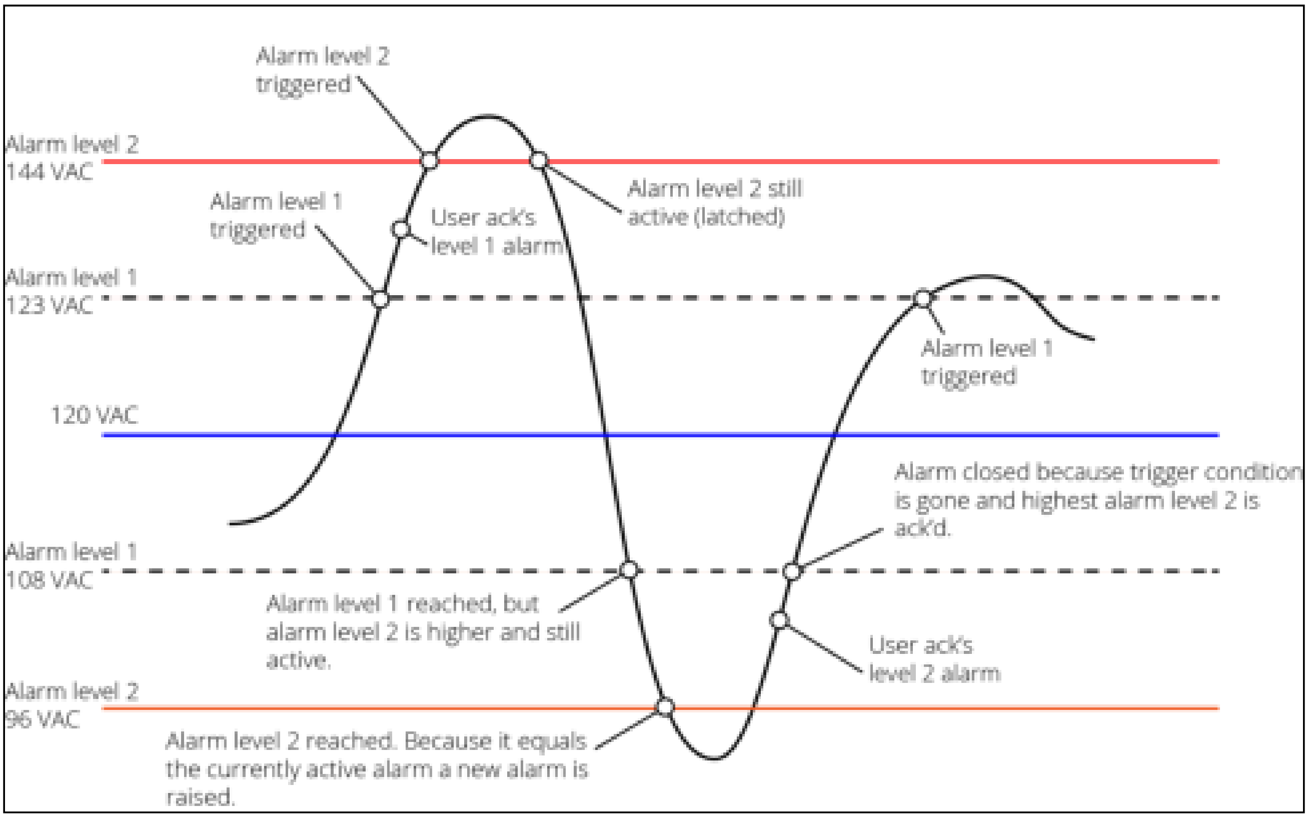
35 Creating an alarm configuration

13.2 Alarm Levels

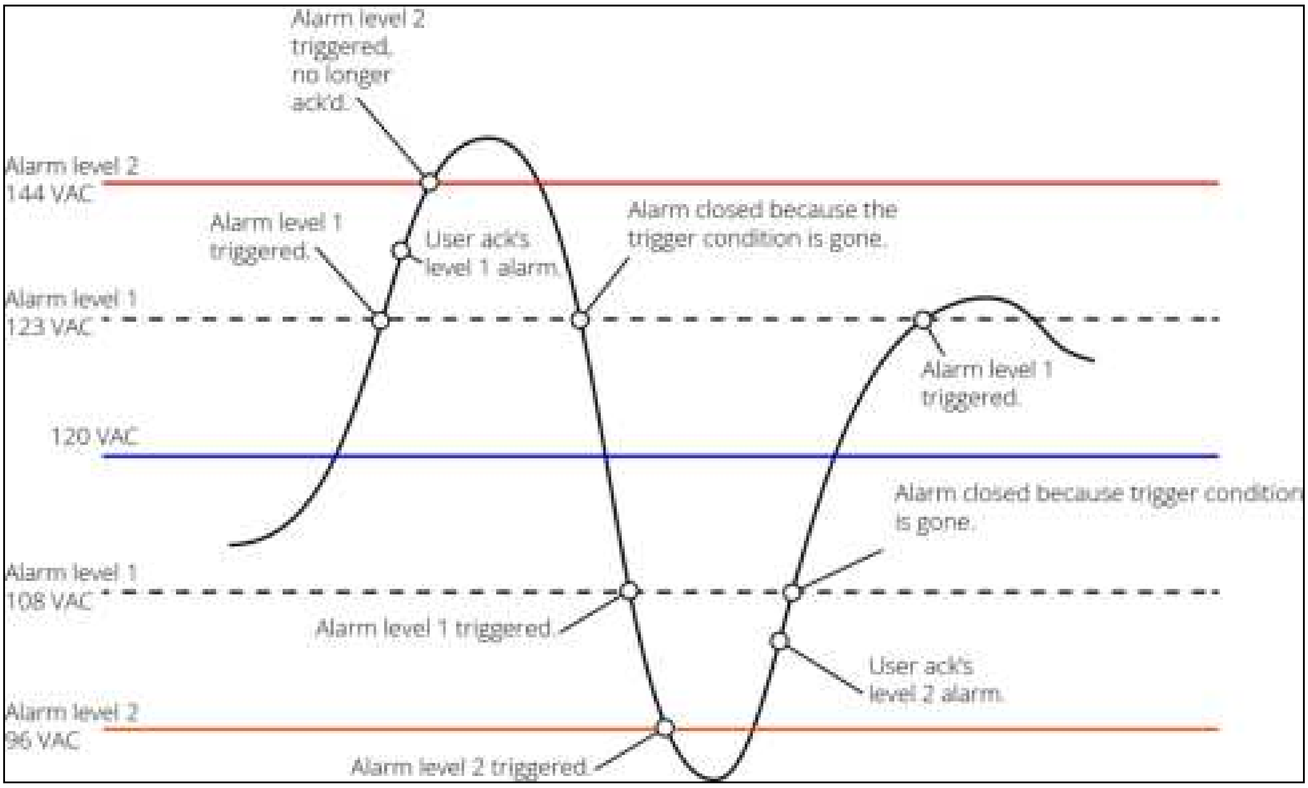
Every channel can have multiple alarm triggers (not just High and Low). Each time you define an additional High or Low alarm trigger point for a particular analog channel, it automatically becomes a new alarm level. The alarm level is assigned based on the comparative values of the trigger settings.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

Type	Value	Level
High	144 VAC	2
High	132 VAC	1
Low	108 VAC	1
Low	96 VAC	2

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.


Alarm level 2 triggered
Alarm level 2 144 VAC
Alarm level 1 triggered
User ack's level 1 alarm
Alarm level 2 still active (latched)
Alarm level 1 123 VAC
Alarm level 1 triggered
120 VAC
Alarm closed because trigger condition is gone and highest alarm level 2 is ack'd.
Alarm level 1 108 VAC
Alarm level 1 reached, but alarm level 2 is higher and still active.
User ack's level 2 alarm
Alarm level 2 96 VAC
Alarm level 2 reached. Because it equals the currently active alarm a new alarm is raised.

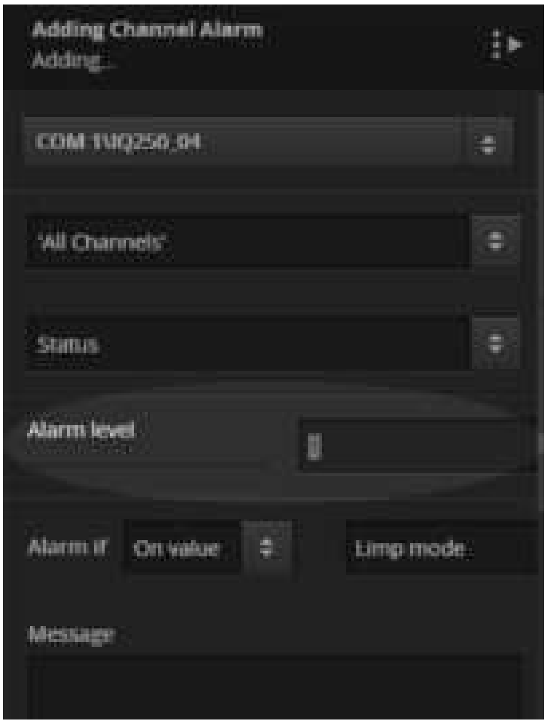
36 Latching Alarm Example


Alarm level 2 triggered, no longer ack'd.
Alarm level 2 144 VAC
Alarm level 1 triggered.
User ack's level 1 alarm.
Alarm closed because the trigger condition is gone.
Alarm level 1 123 VAC
Alarm level 1 triggered.
120 VAC
Alarm closed because trigger condition is gone.
Alarm level 1 108 VAC
Alarm level 1 triggered.
User ack's level 2 alarm.
Alarm level 2 96 VAC
Alarm level 2 triggered.

37 Non-Latching Alarm Example

13.3 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.



Adding Channel Alarm
Adding...

COM 1UQ250_04

'All Channels'

Status

Alarm level

Alarm if On value

Limp mode

Message

38 Alarm level field for multi-state channels

14 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.

14.1 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.

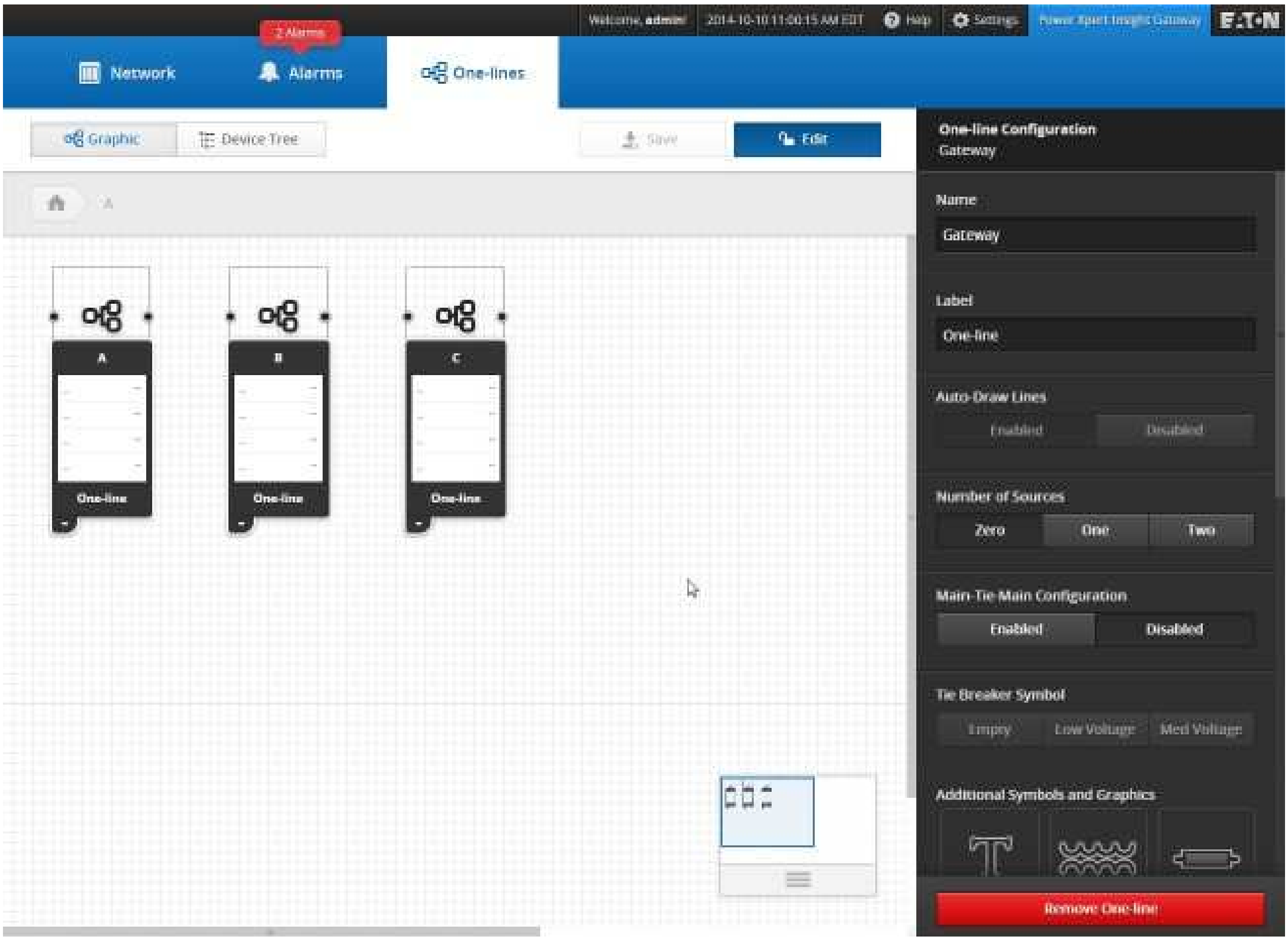
14.2 Adding Devices to One-Lines

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

14.3 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.



One-line Configuration
Gateway

Name
Gateway

Label
One-line

Auto-Draw Lines

Number of Sources

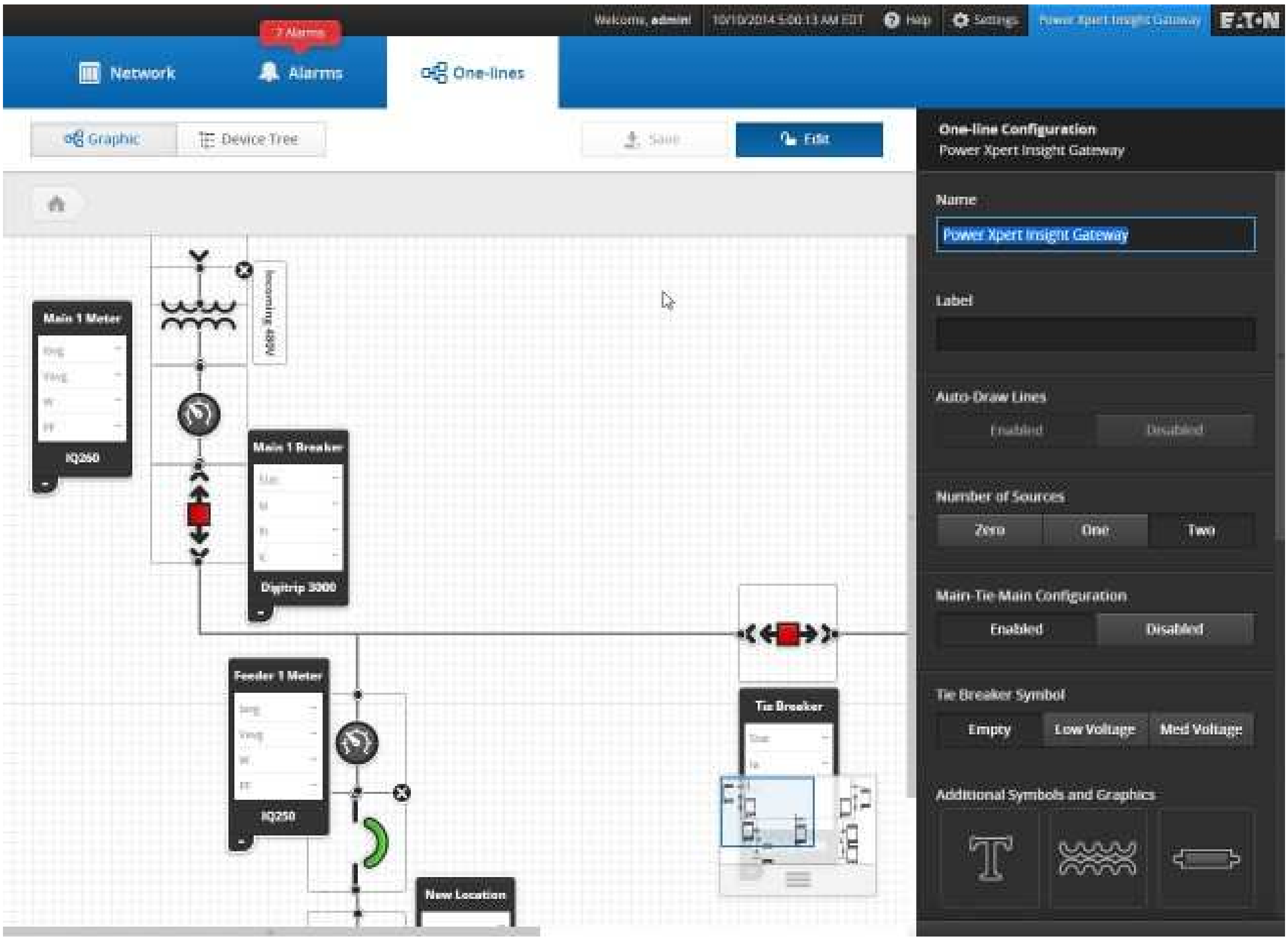
Main-Tie-Main Configuration

Tie Breaker Symbol

Additional Symbols and Graphics

39 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.



One-line Configuration
Power Xpert Insight Gateway

Name: Power Xpert Insight Gateway

Label:

Auto-Draw Lines: Enabled Disabled

Number of Sources: Zero One Two

Main-Tie-Main Configuration: Enabled Disabled

Tie Breaker Symbol: Empty Low Voltage Med Voltage

40 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:

14.3.1 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.

14.3.2 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.

14.4 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.

14.5 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/9cyfwvxo

15 Connecting to the Web Interface

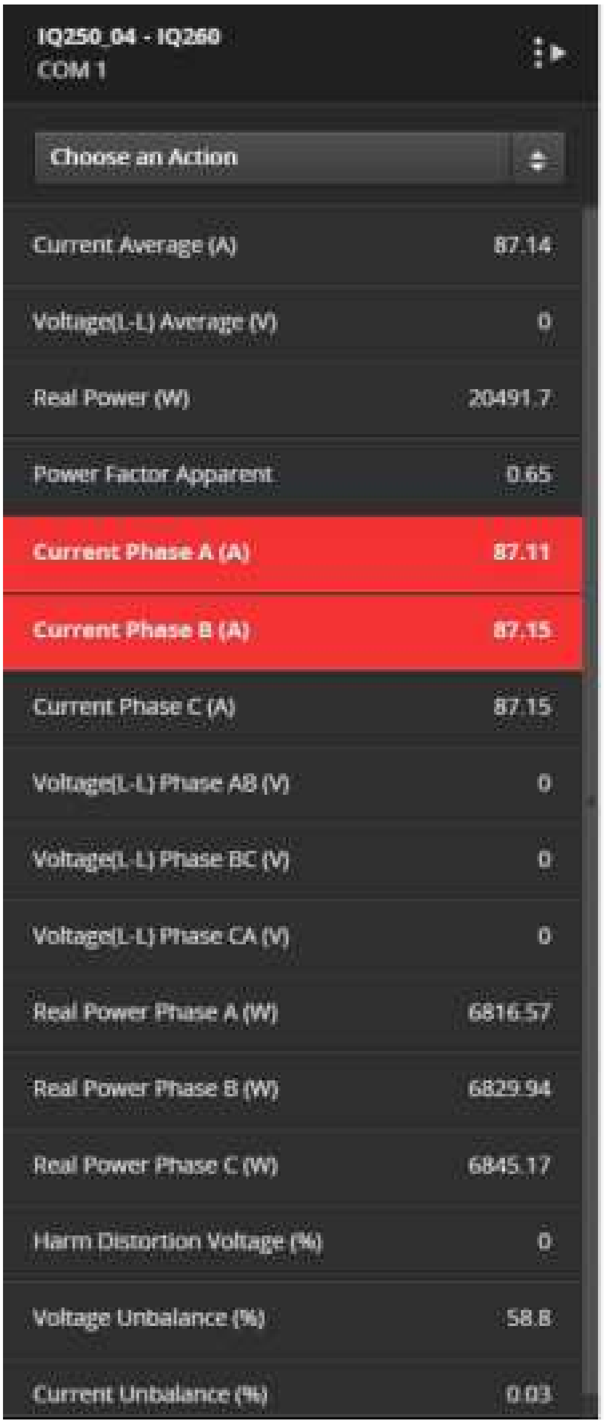
After the PXG is fully configured, users can interact with the web interface. This is best viewed in either Google Chrome (current version) or Microsoft Internet Explorer 11. Users should have a screen resolution of at least 1280 x 1024 pixels. The connection is https://*machine_name* where *machine_name* 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".

16 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.



IQ250_04 - IQ260
COM 1

Current Average (A)	87.14
Voltage(L-L) Average (V)	0
Real Power (W)	20491.7
Power Factor Apparent	0.65
Current Phase A (A)	87.11
Current Phase B (A)	87.15
Current Phase C (A)	87.15
Voltage(L-L) Phase AB (V)	0
Voltage(L-L) Phase BC (V)	0
Voltage(L-L) Phase CA (V)	0
Real Power Phase A (W)	6816.57
Real Power Phase B (W)	6829.94
Real Power Phase C (W)	6845.17
Harm Distortion Voltage (%)	0
Voltage Unbalance (%)	58.8
Current Unbalance (%)	0.03

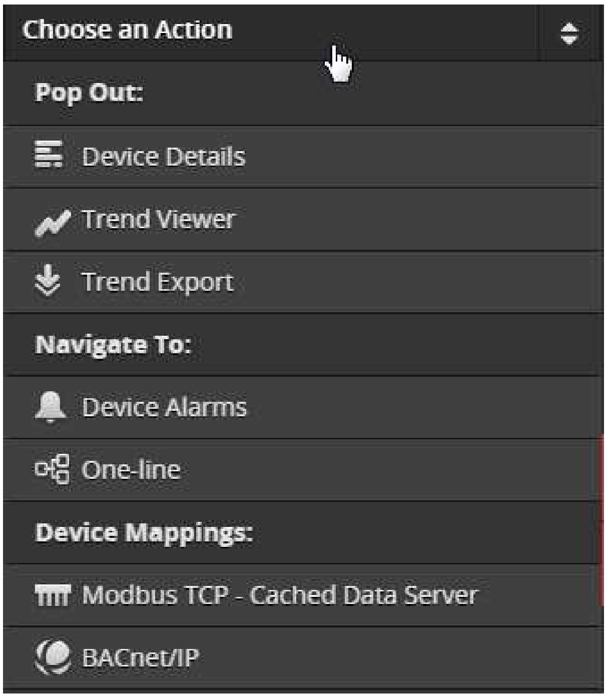
41 Sidebar, showing channels and values

16.1 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

- Device Alarms (navigate to Alarms tab)
- One-line (navigate to One-lines tab)
- Waveform (pop-out)
- Modbus TCP- Cached Data Server Mapping
- Network 2 Mapping (pass-through)
- BACnet/IP Mapping



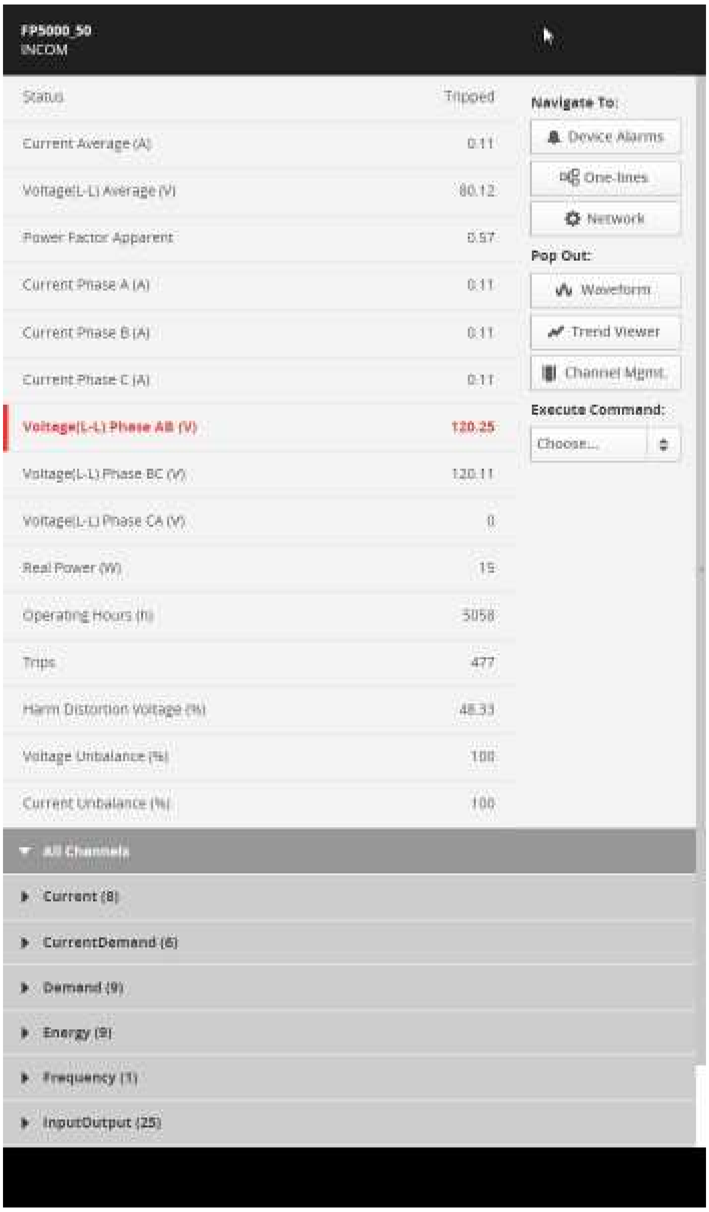
16.2 Device Details

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.

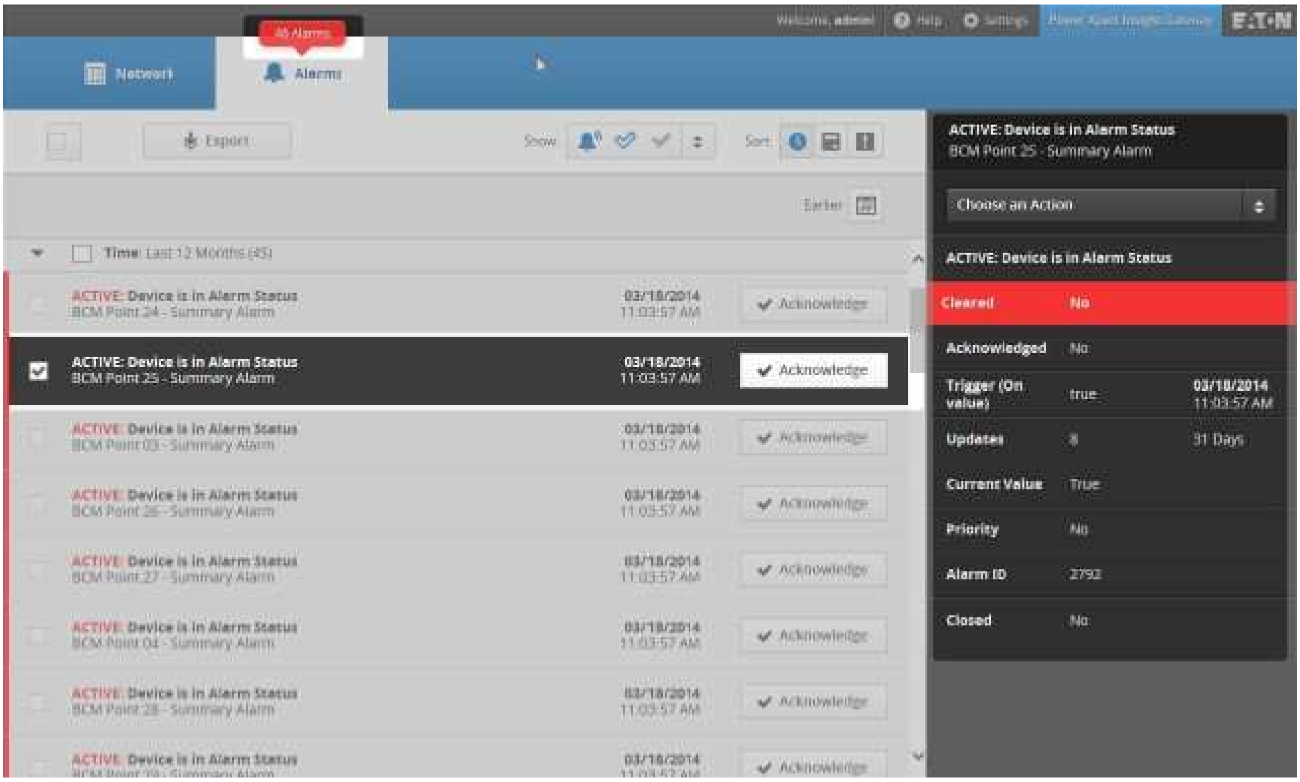


FP5000_50
INCOM

Status	Tripped
Current Average (A)	0.11
Voltage(L-L) Average (V)	80.12
Power Factor Apparent	0.57
Current Phase A (A)	0.11
Current Phase B (A)	0.11
Current Phase C (A)	0.11
Voltage(L-L) Phase AB (V)	120.25
Voltage(L-L) Phase BC (V)	120.11
Voltage(L-L) Phase CA (V)	0
Real Power (W)	15
Operating Hours (h)	3058
Trips	477
Harm Distortion Voltage (%)	48.33
Voltage Unbalance (%)	100
Current Unbalance (%)	100

42 Device Details

17 Alarms Tab



□ Time: Last 12 Months (45)

ACTIVE: Device is in Alarm Status
BCM Point 24 - Summary Alarm
03/18/2014
11:03:57 AM

☑ ACTIVE: Device is in Alarm Status
BCM Point 25 - Summary Alarm
03/18/2014
11:03:57 AM

ACTIVE: Device is in Alarm Status
BCM Point 03 - Summary Alarm
03/18/2014
11:03:57 AM

ACTIVE: Device is in Alarm Status
BCM Point 26 - Summary Alarm
03/18/2014
11:03:57 AM

ACTIVE: Device is in Alarm Status
BCM Point 27 - Summary Alarm
03/18/2014
11:03:57 AM

ACTIVE: Device is in Alarm Status
BCM Point 04 - Summary Alarm
03/18/2014
11:03:57 AM

ACTIVE: Device is in Alarm Status
BCM Point 28 - Summary Alarm
03/18/2014
11:03:57 AM

ACTIVE: Device is in Alarm Status
BCM Point 29 - Summary Alarm
03/18/2014
11:03:57 AM

ACTIVE: Device is in Alarm Status
BCM Point 25 - Summary Alarm

Choose an Action

ACTIVE: Device is in Alarm Status

Cleared	No	
Acknowledged	No	
Trigger (On value)	true	03/18/2014 11:03:57 AM
Updates	8	31 Days
Current Value	True	
Priority	No	
Alarm ID	2792	
Closed	No	

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.

18 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.

19 Waveforms

The PXG can download waveforms:

- From any attached INCOM device that's capable of capturing waveforms. The following Eaton devices are supported: FP-5000, FP-6000, IQ Analyzer Logger 6400/6600, MPCV Relay, Digitrip 1150.
- If Enable Waveforms in the device configuration for that device is selected.

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.

19.1 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.

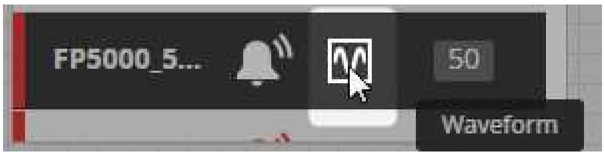
19.2 Enabling Waveform Capture in the PXG

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 INCOM device that supports waveforms.
3. Select Enable Waveforms in the sidebar.
4. Click Save Device Configuration.

19.3 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 INCOM device that has captured waveforms shows the following waveform icon. You can click the icon to launch the Waveforms list pop-out.



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.

19.4 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.

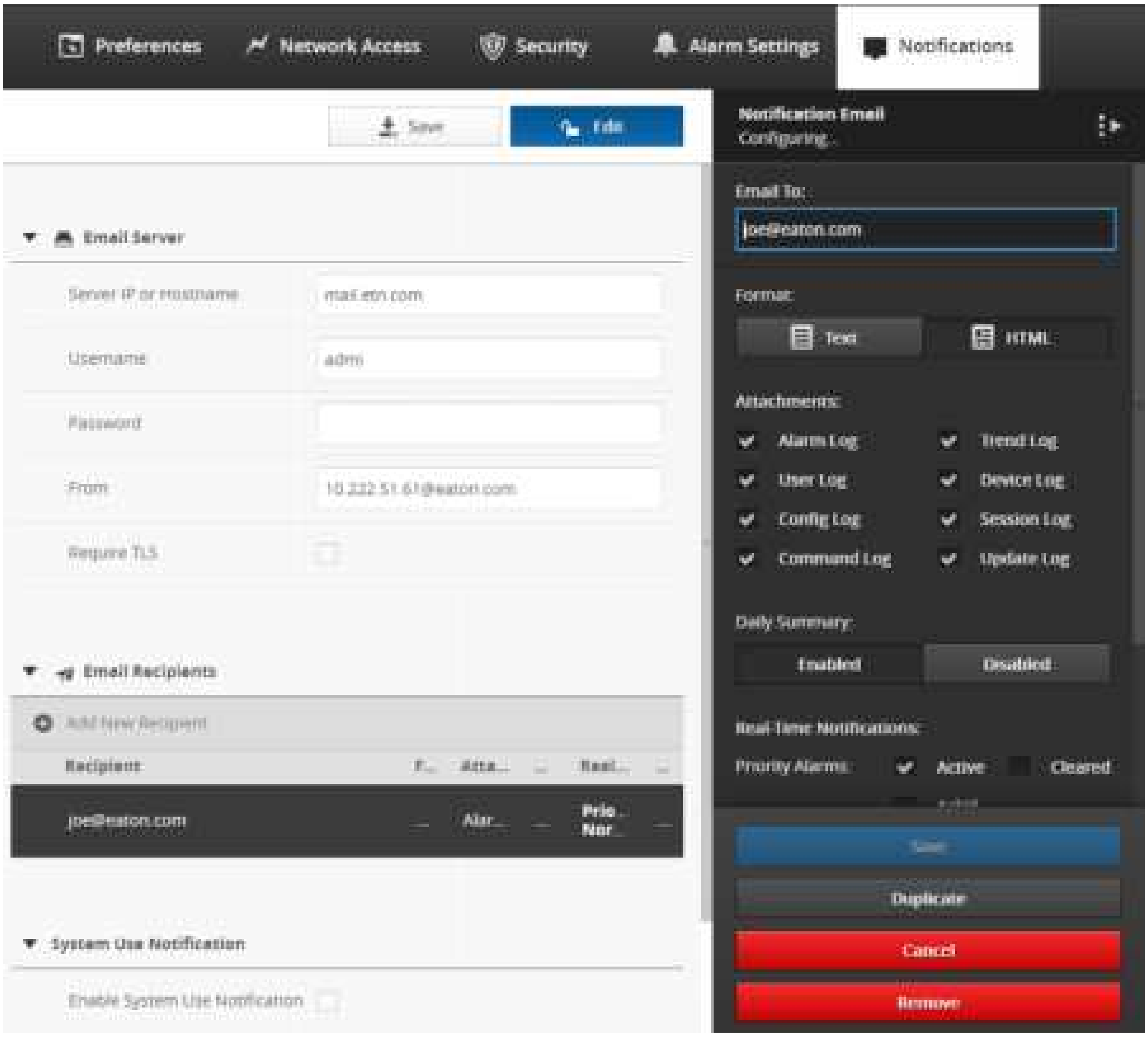
> ⓘ **Available Space**
> The PXG allocates 100MB of internal space for saving waveform files. This is enough storage for approximately 300 waveform files. Roll-off of older waveform files occurs automatically as the available waveform log space is filled.

19.5 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.

19.6 Signing up for Waveform Email Notifications

To receive emails notifying you of available waveforms:



Email Server

Server IP or Hostname: mail.etn.com

Username: admi

Password:

From: 10.222.51.61@eaton.com

Require TLS ☐

Email Recipients

Add New Recipient

Recipient	F...	Atta...	...	Real...	...
joe@eaton.com	...	Alar...	...	Prio... Nor...	...

System Use Notification

Enable System Use Notification ☐

Notification Email
Configuring...

Email To: joe@eaton.com

Format: Text | HTML

Attachments:
✓ Alarm Log ✓ Trend Log
✓ User Log ✓ Device Log
✓ Config Log ✓ Session Log
✓ Command Log ✓ Update Log

Daily Summary: Enabled | Disabled

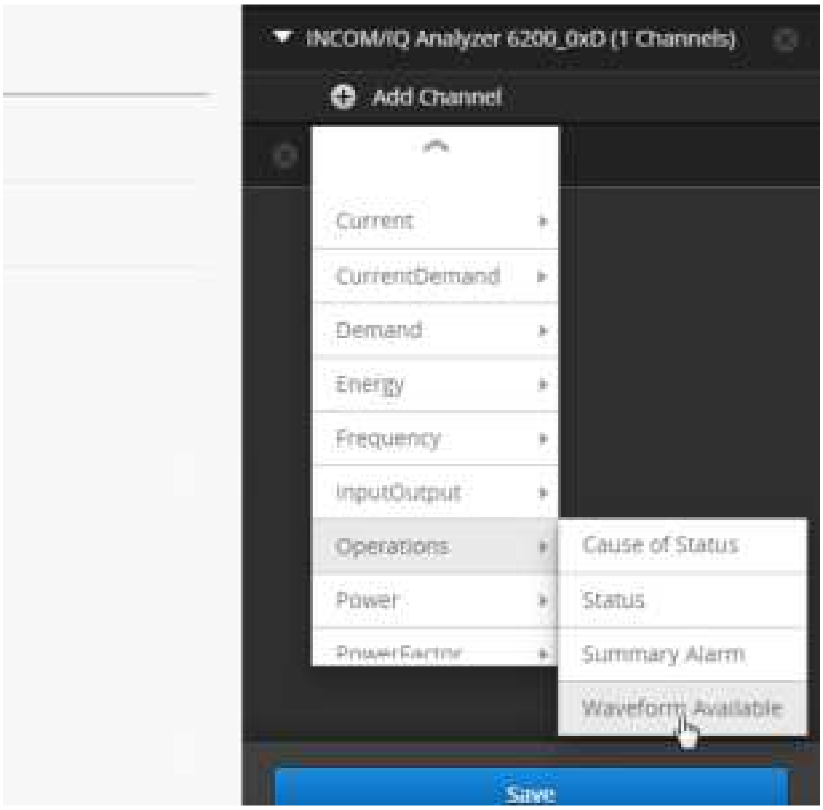
Real-Time Notifications:
Priority Alarms: ✓ Active ☐ Cleared

43 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.

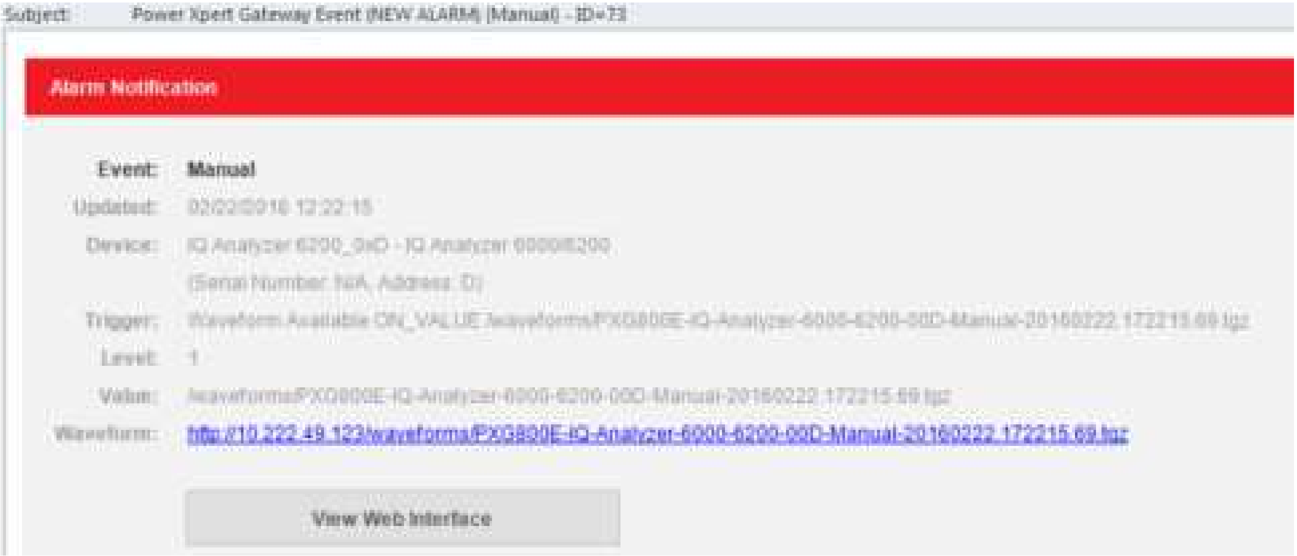
Note: to send recipients email notifications when waveforms become available, select the Waveform Available channel (in the Operations category) for the device providing the waveform, as shown in the following figure.



44 Selecting the Waveform Available channel.

19.7 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.



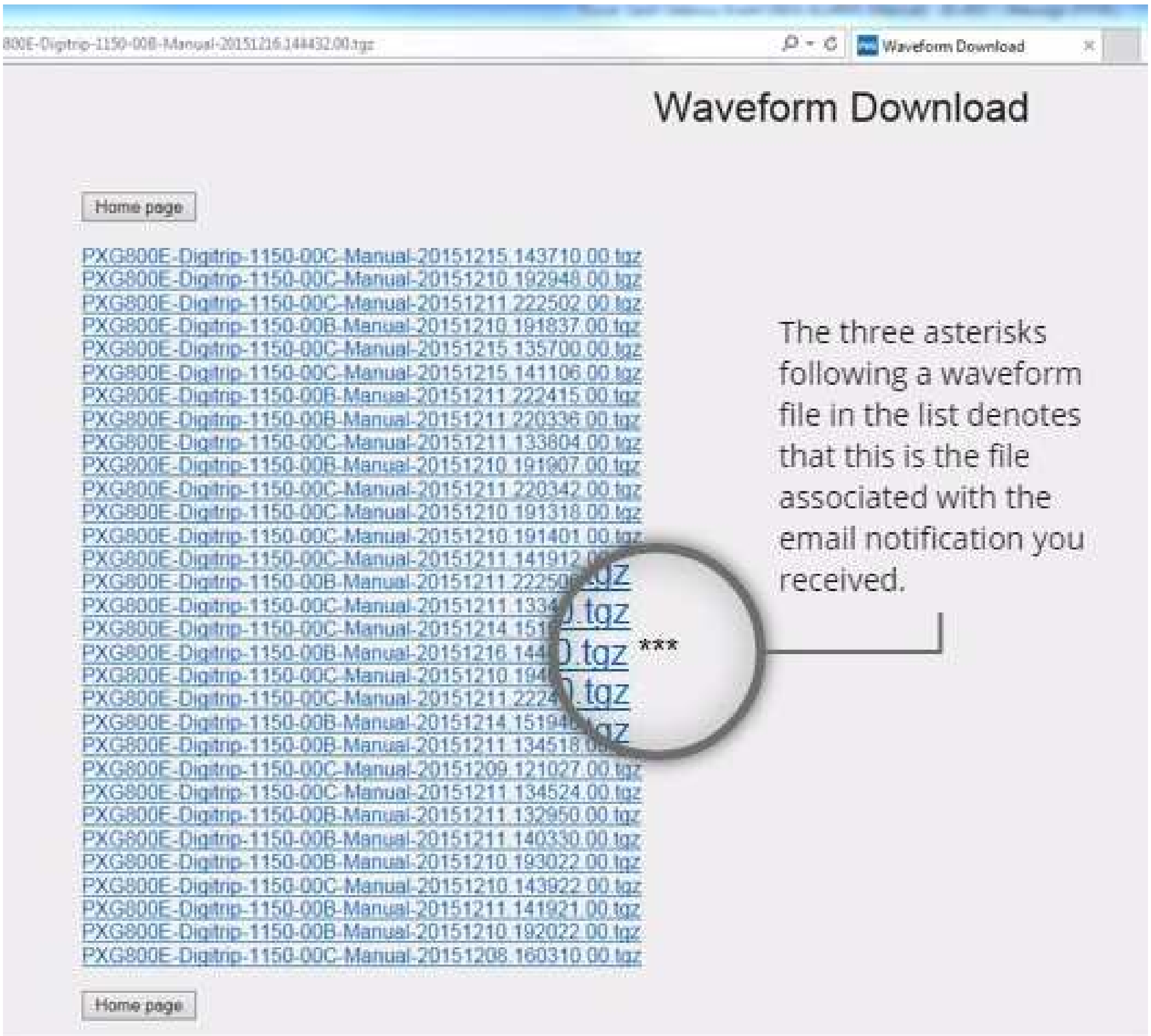
Subject: Power Xpert Gateway Event (NEW ALARM) [Manual] - ID=73

Alarm Notification

Event:	**Manual**
Updated:	02/22/2016 12:22:15
Device:	IQ Analyzer 6200_0xD - IQ Analyzer 6000/6200 (Serial Number: N/A, Address: D)
Trigger:	Waveform Available ON_VALUE /waveforms/PXG800E-IQ-Analyzer-6000-6200-00D-Manual-20160222.172215.69.tgz
Level:	1
Value:	/waveforms/PXG800E-IQ-Analyzer-6000-6200-00D-Manual-20160222.172215.69.tgz
Waveform:	http://10.222.49.123/waveforms/PXG800E-IQ-Analyzer-6000-6200-00D-Manual-20160222.172215.69.tgz

45 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.



Waveform Download

PXG800E-Digitrip-1150-00C-Manual-20151215.143710.00.tgz
PXG800E-Digitrip-1150-00C-Manual-20151210.192948.00.tgz
PXG800E-Digitrip-1150-00C-Manual-20151211.222502.00.tgz
PXG800E-Digitrip-1150-00B-Manual-20151210.191837.00.tgz
PXG800E-Digitrip-1150-00C-Manual-20151215.135700.00.tgz
PXG800E-Digitrip-1150-00C-Manual-20151215.141106.00.tgz
PXG800E-Digitrip-1150-00B-Manual-20151211.222415.00.tgz
PXG800E-Digitrip-1150-00B-Manual-20151211.220336.00.tgz
PXG800E-Digitrip-1150-00C-Manual-20151211.133804.00.tgz
PXG800E-Digitrip-1150-00B-Manual-20151210.191907.00.tgz
PXG800E-Digitrip-1150-00C-Manual-20151211.220342.00.tgz
PXG800E-Digitrip-1150-00C-Manual-20151210.191318.00.tgz
PXG800E-Digitrip-1150-00C-Manual-20151210.191401.00.tgz
PXG800E-Digitrip-1150-00C-Manual-20151211.141912.0
PXG800E-Digitrip-1150-00B-Manual-20151211.22250 gz
PXG800E-Digitrip-1150-00C-Manual-20151211.1334 .tgz
PXG800E-Digitrip-1150-00C-Manual-20151214.151 .tgz
PXG800E-Digitrip-1150-00B-Manual-20151216.144 .tgz ***
PXG800E-Digitrip-1150-00C-Manual-20151210.194 .tgz
PXG800E-Digitrip-1150-00C-Manual-20151211.2224 .tgz
PXG800E-Digitrip-1150-00B-Manual-20151214.15194 gz
PXG800E-Digitrip-1150-00B-Manual-20151211.134518
PXG800E-Digitrip-1150-00C-Manual-20151209.121027.00.tgz
PXG800E-Digitrip-1150-00C-Manual-20151211.134524.00.tgz
PXG800E-Digitrip-1150-00B-Manual-20151211.132950.00.tgz
PXG800E-Digitrip-1150-00B-Manual-20151211.140330.00.tgz
PXG800E-Digitrip-1150-00B-Manual-20151210.193022.00.tgz
PXG800E-Digitrip-1150-00C-Manual-20151210.143922.00.tgz
PXG800E-Digitrip-1150-00B-Manual-20151211.141921.00.tgz
PXG800E-Digitrip-1150-00B-Manual-20151210.192022.00.tgz
PXG800E-Digitrip-1150-00C-Manual-20151208.160310.00.tgz

The three asterisks following a waveform file in the list denotes that this is the file associated with the email notification you received.

46 List of Available Waveforms

20 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.

20.1 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".

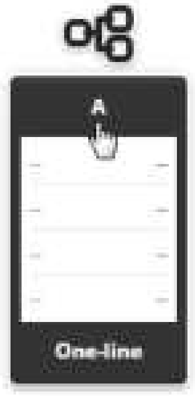
20.2 Graphic View

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.

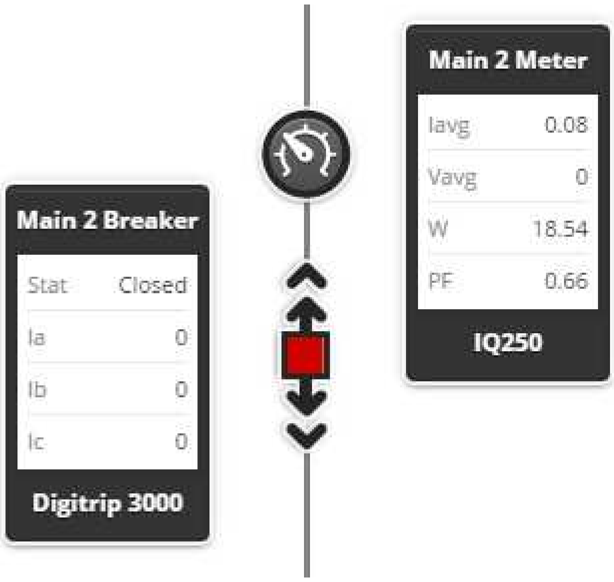
20.3 Link Objects

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.



20.4 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.



Main 2 Breaker

Stat	Closed
Ia	0
Ib	0
Ic	0

Digitrip 3000

Main 2 Meter

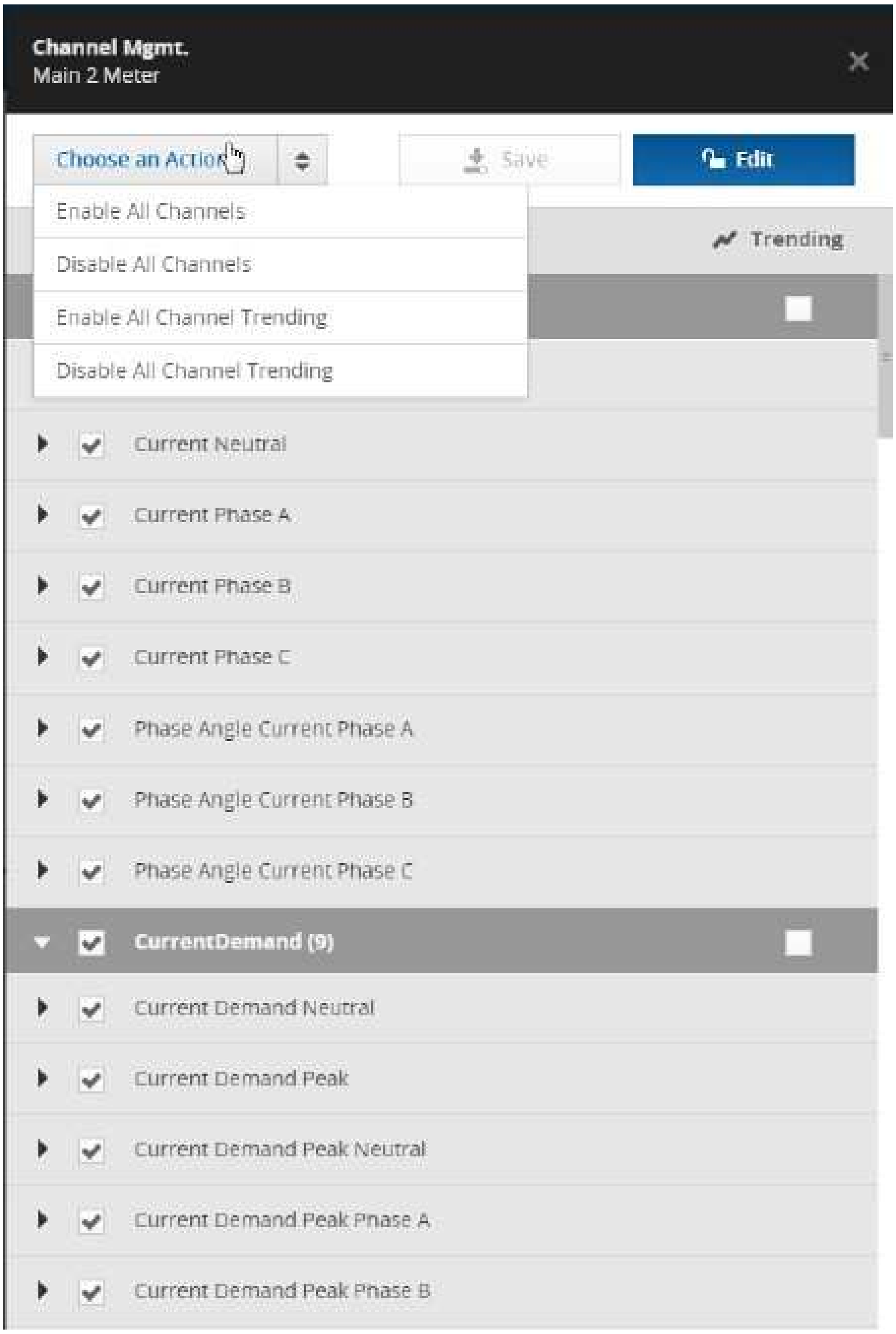
Iavg	0.08
Vavg	0
W	18.54
PF	0.66

IQ250

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.

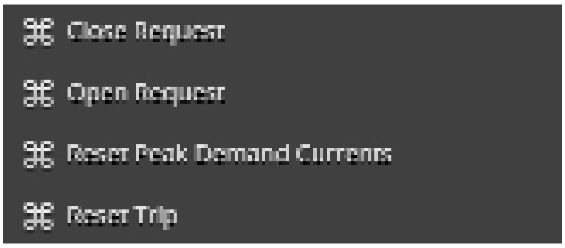


- ☑ Current Neutral
- ☑ Current Phase A
- ☑ Current Phase B
- ☑ Current Phase C
- ☑ Phase Angle Current Phase A
- ☑ Phase Angle Current Phase B
- ☑ Phase Angle Current Phase C
- ☑ CurrentDemand (9) □
- ☑ Current Demand Neutral
- ☑ Current Demand Peak
- ☑ Current Demand Peak Neutral
- ☑ Current Demand Peak Phase A
- ☑ Current Demand Peak Phase B

47 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.


⌘ Close Request
⌘ Open Request
⌘ Reset Peak Demand Currents
⌘ Reset Trip

21 Cybersecurity Hardening the PXG

Eaton recommends that all customers using the PXG900 check periodically for updated PXG900 firmware which is available on Eaton's Website at www.Eaton.com/monitor[8]. From this landing page, choose Networking hardware, then PowerXpert Gateway 900 to obtain the latest released firmware. As new PXG900 firmware is made available, Eaton recommends that PXG900's be upgraded to the latest available release of firmware to stay up to date with Cybersecurity vulnerability remediations.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:

1. 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.
2. Download the certificate file from the PXG.
3. 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.

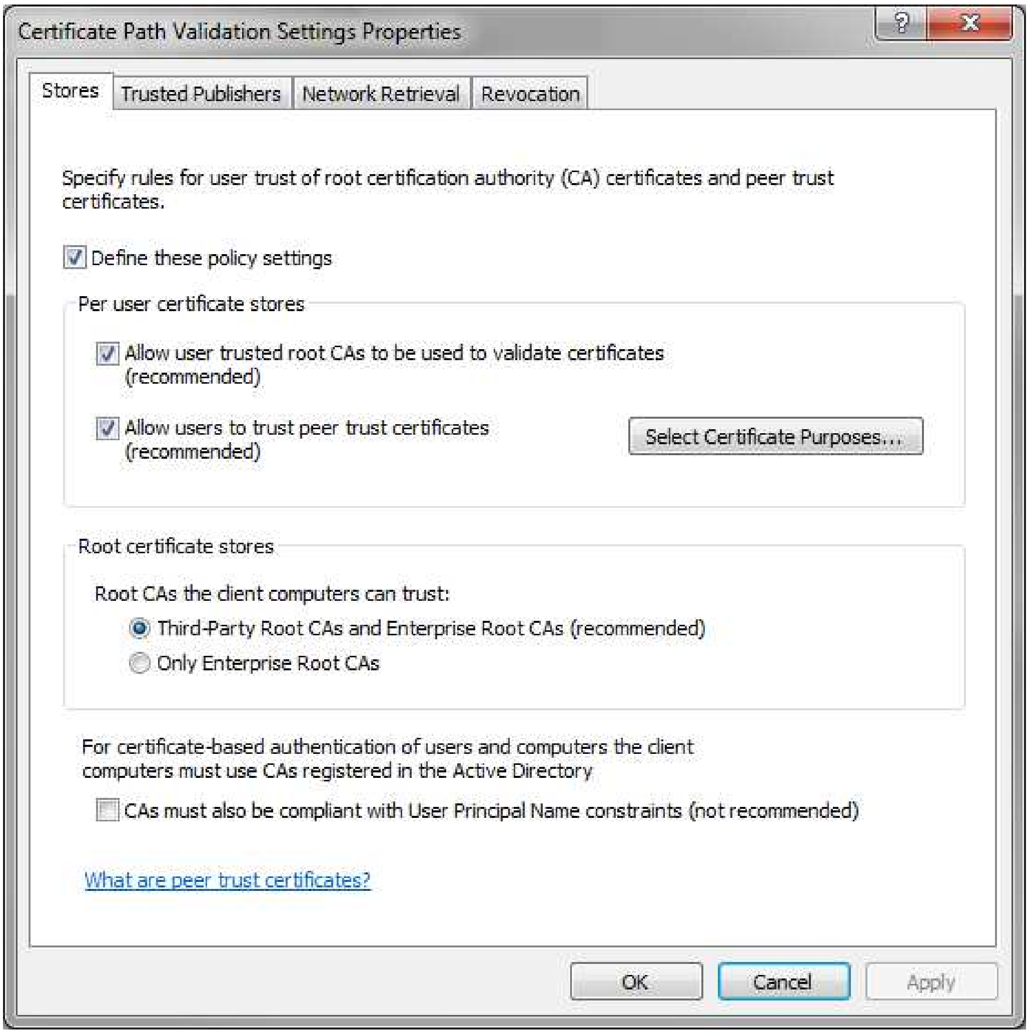
21.1 Enabling User Management of Root Certificates

The process for either enabling this on a local machine or setting a group policy is outlined in the following Microsoft Technet Article: https://technet.microsoft.com/en-us/library/Cc754841.aspx .
[9]

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.

[8] http://www.Eaton.com/monitor

[9] https://technet.microsoft.com/en-us/library/Cc754841.aspx


Certificate Path Validation Settings Properties
Stores
Trusted Publishers
Network Retrieval
Revocation

Specify rules for user trust of root certification authority (CA) certificates and peer trust certificates.

☑ Define these policy settings

Per user certificate stores

☑ Allow user trusted root CAs to be used to validate certificates (recommended)

☑ Allow users to trust peer trust certificates (recommended)

Select Certificate Purposes...

Root certificate stores

Root CAs the client computers can trust:

● Third-Party Root CAs and Enterprise Root CAs (recommended)

○ Only Enterprise Root CAs

For certificate-based authentication of users and computers the client computers must use CAs registered in the Active Directory

□ CAs must also be compliant with User Principal Name constraints (not recommended)

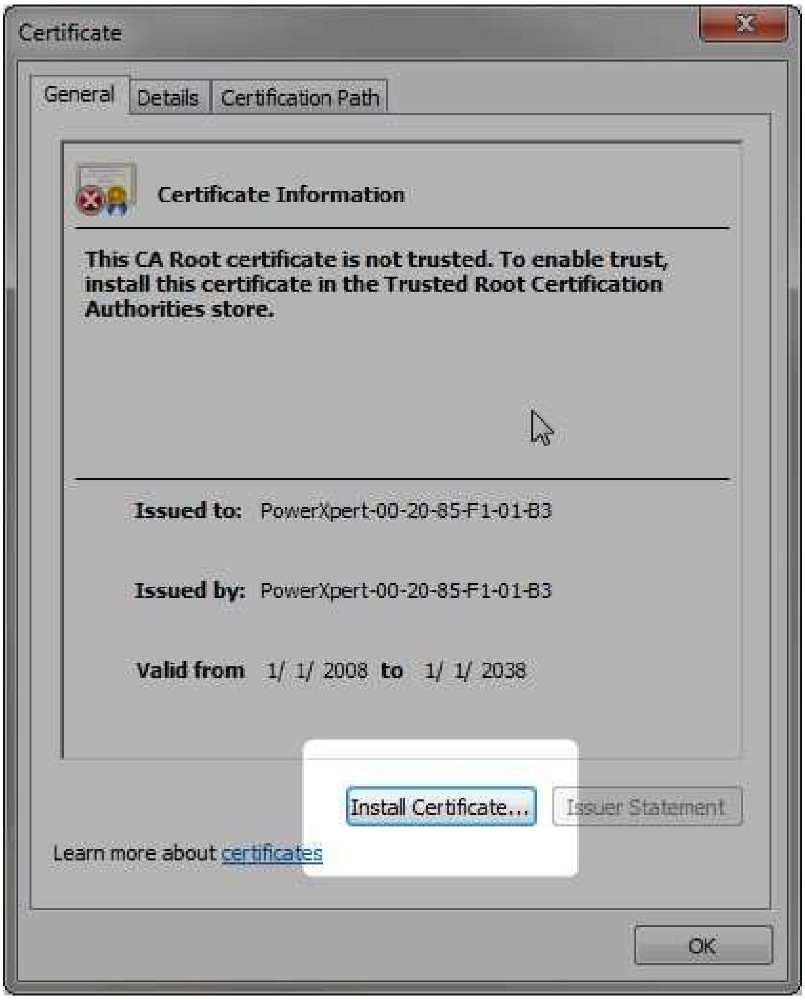
21.1.1 Downloading the Certificate File from the Gateway

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.
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.*

21.1.2 Installing the Certificate

1. Double-click the certificate file. This will launch the certificate installation wizard.
2. Click Install certificate.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

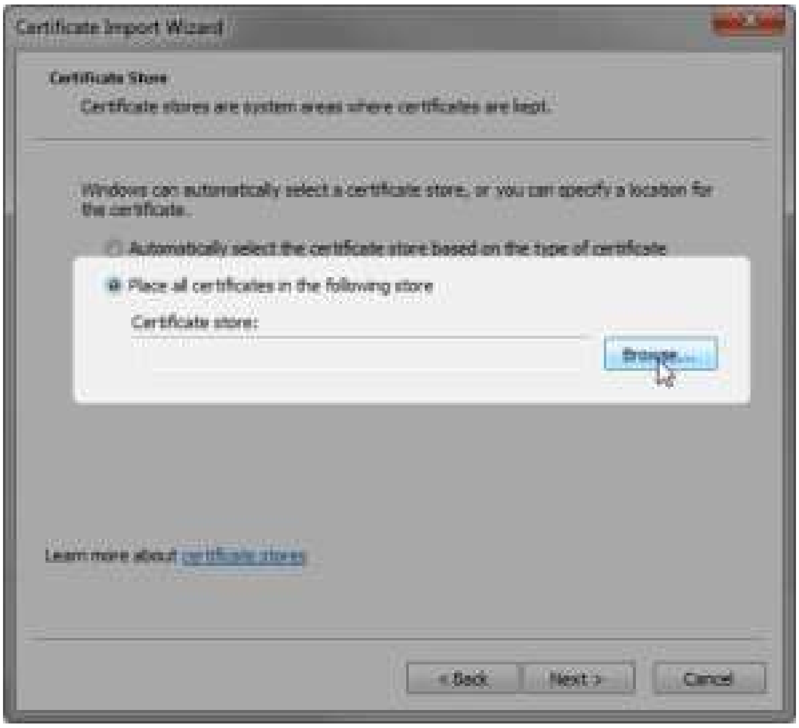
Issued to: PowerXpert-00-20-85-F1-01-B3

Issued by: PowerXpert-00-20-85-F1-01-B3

Valid from 1/ 1/ 2008 to 1/ 1/ 2038

Learn more about certificates

3. On the Welcome dialog box, click Next.
4. Select Place all certificates in the following store and then click Browse.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

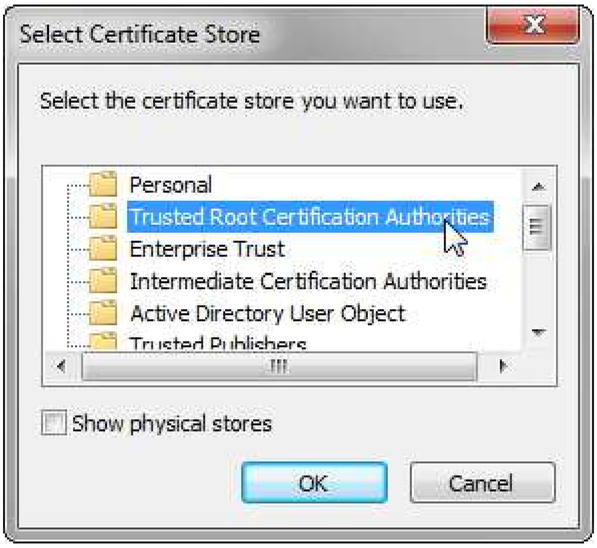
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Learn more about certificate stores

5. Select Trusted Root Certification Authorities from the list, then click OK.



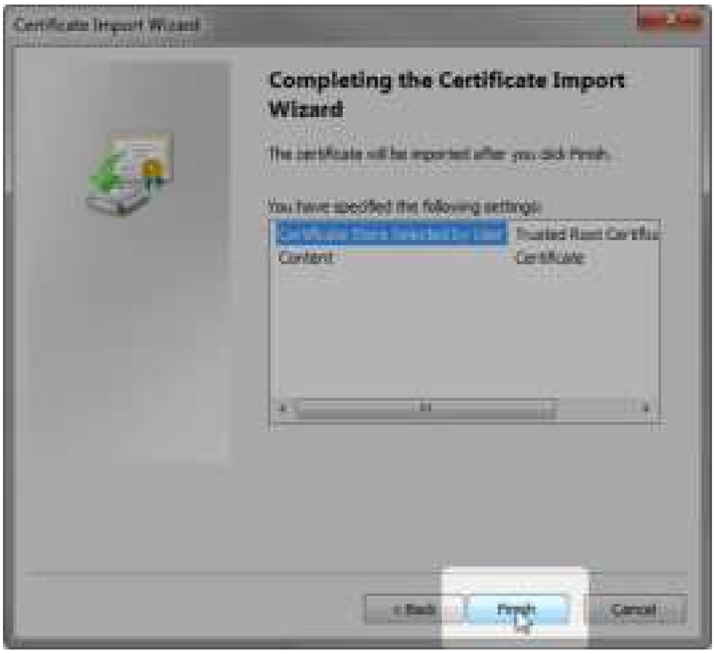
Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers

□ Show physical stores

6. On the Completing the Certificate Import Wizard dialog box, click Finish.



Completing the Certificate Import Wizard

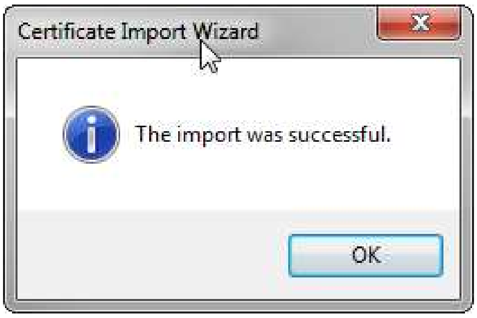
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User Trusted Root Certific

Content Certificate

7. You should see an alert box stating that the import was successful. Click OK.



The import was successful.

You can now access the gateway using the HTTPS protocol (for example, https://192.168.1.1/).

21.2 Ports in Use

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.

The following ports and protocols are disabled by default. You must elect to enable them and may choose to change the assigned port number.

Port Number	Protocol/Use	TCP/UDP
502	Modbus TCP	TCP

5150	EMINT Mode - INCOM	UDP
26501	Modbus (COM1 Pass-thru)	TCP
26502	Modbus (COM2 Pass-thru)	TCP
26503	Modbus (Ethernet Pass-thru)	TCP
47808	BACnet/IP	UDP
161	SNMP	UDP
162	SNMP	UDP

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

Port Number	**Protocol/Use**	**TCP/UDP**
7012	Eaton's Mercury Websockets – Secure via TLS	TCP
8443	Eaton's Mercury – Secure via TLS for communications with PXI Software	TCP

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.

Port Number	**Protocol/Use**	**TCP/UDP**
7011	Eaton's Mercury Websockets	TCP
8181	Eaton's Mercury for communications with PXI Software	TCP
80	Eaton's Mercury-Standard HTTP port	TCP

21.3 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.

21.4 Settings

21.4.1 Network Access Tab - Controlling Access to Various Protocol Servers

21.4.1.1 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.

21.4.1.2 Modbus TCP Server Configuration

Unless you have a specific need to enable Write Commands, make sure that this is Disabled.

21.4.1.3 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.

21.5 Notifications Tab, Email Server

You should, if possible, require TLS when communicating with an email server. Also, limit the recipient list to those who truly need this information.

21.6 Passwords

One of the first things that you should do is to change the passwords for both the Admin and User accounts. You can change these on the Network tab, under the settings for the PXG itself. When in edit mode, the Security tab under settings lets you change passwords, add and delete users, and assign roles.
When changing passwords, follow good security practices including, but not limited to:

- Passwords should be in excess of seven characters.
- Passwords should contain at least one capital letter, number, and special character.

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.

> ***Important**: It's always good security practice to only use admin level accounts when performing admin activities. By only using admin level accounts for such activity, you minimize the risk of an admin being logged in and leaving their computer unlocked.*

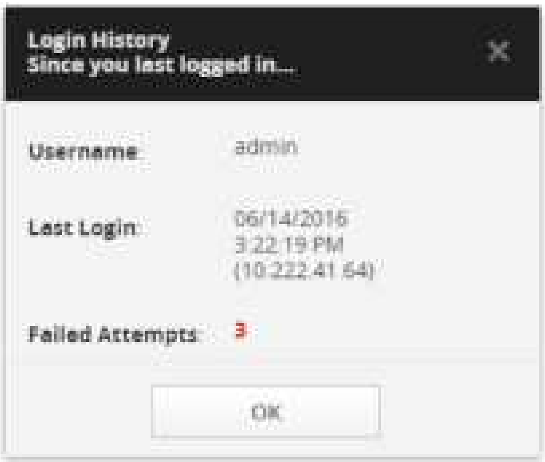
The Global Password Policy and User Password Management features are further documented in the Users and Access Control(see page 50) section.

You can verify who has accessed the PXG through the Choose an Action drop down list in the sidebar on the Network tab. Click Edit, select the Power Xpert Insight Gateway gear icon, and then select Audit Logs to download the appropriate logs. The Session log may be of particular interest as it lists login attempts and failures. For more information about the various logs, see Advanced Administration(see page 57).

Eaton recommends that all products should be installed on a secure network. For more information on how to secure this product in your environment please refer to the whitepaper "Cybersecurity considerations for electrical distribution systems" at http://www.eaton.com/Eaton/ProductsServices/Electrical/ThoughtLeadership/WhitePapers/index.htm.

21.7 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.



Login History
Since you last logged in...

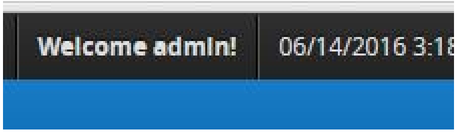
Username: admin

Last Login: 06/14/2016 3:22:19 PM (10.222.41.64)

Failed Attempts: 3

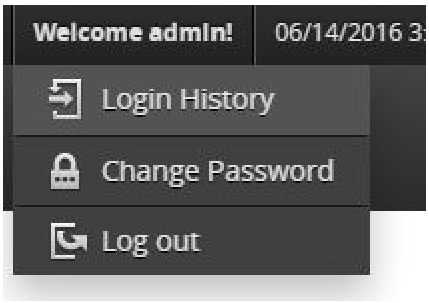
48 Failed Login Attempt Warning

Last Login History can be viewed at any time by clicking on the Welcome text found next to the displayed Date and Time.



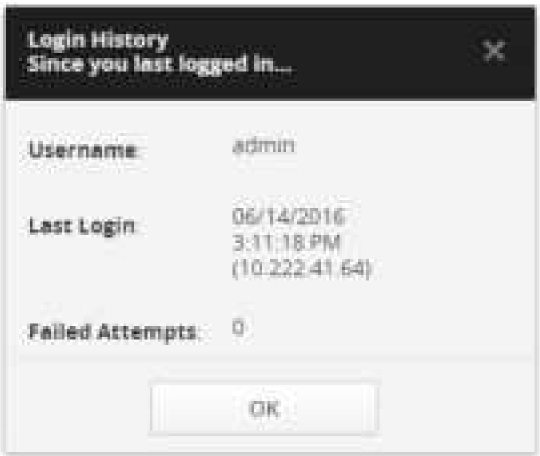
49 Login Menu

Doing so, produces the following menu.



50 Selecting the Last Login History

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



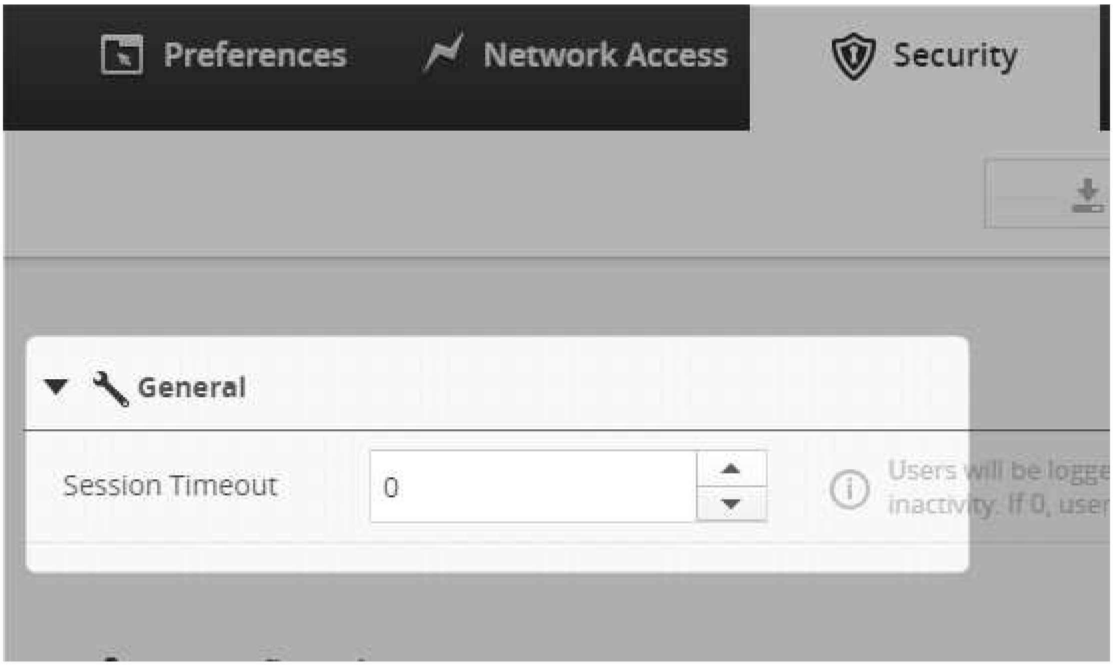
Login History
Since you last logged in...

Username	admin
Last Login	06/14/2016 3:11:18 PM (10.222.41.64)
Failed Attempts	0

51 Login History

21.8 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.

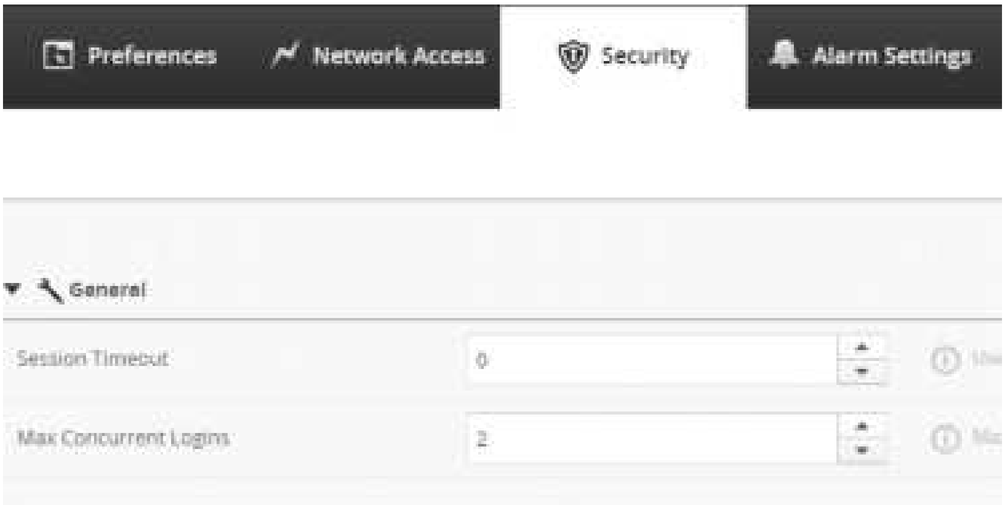


Session Timeout 0

52 Browser Time-Out Setting

21.9 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.

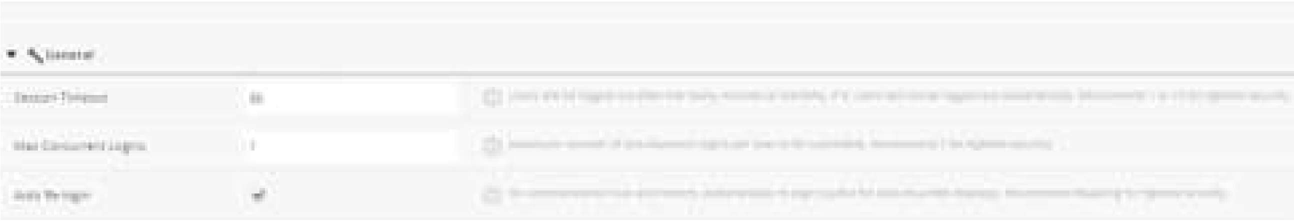


Session Timeout 0

Max Concurrent Logins 2

53 Maximum Concurrent Logins

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.



▼ General

Session Timeout	60	[illegible]
Max Concurrent Logins	1	[illegible]
Auto Re-login	✓	[illegible]

21.10 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.

22 Reset PXG

Reset Button

The recessed push-button switch located on the front of the PXG gateway provides three functions:

- A momentary button press (< 5 Seconds) will restart the gateway.
- Pressing and holding the button for more than 5 seconds, but less than 15 seconds, will reset the stored username and password settings to their defaults.
- Pressing and holding the button for 15 seconds or more will completely reset the gateway to factory defaults.

23 Certificate Management

23.1 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**.

23.2 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

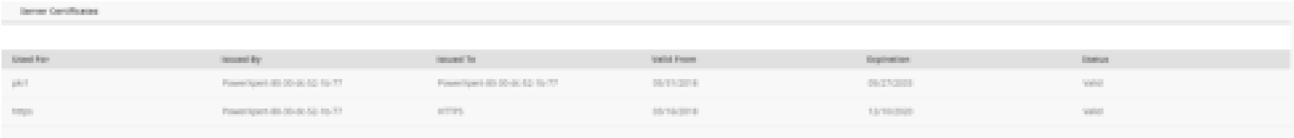
1. Any server certificates (e.g. HTTPS) generated by the **Certificate Manager** will automatically be regenerated upon expiration.
2. If a previously uploaded CA-signed certificate expires, the **Certificate Manager** provides provides the ability to generate a self-signed certificate for a service (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**.

23.3 Operations Supported by the Certificate Manager UI

23.3.1 Listing of Server Certificates

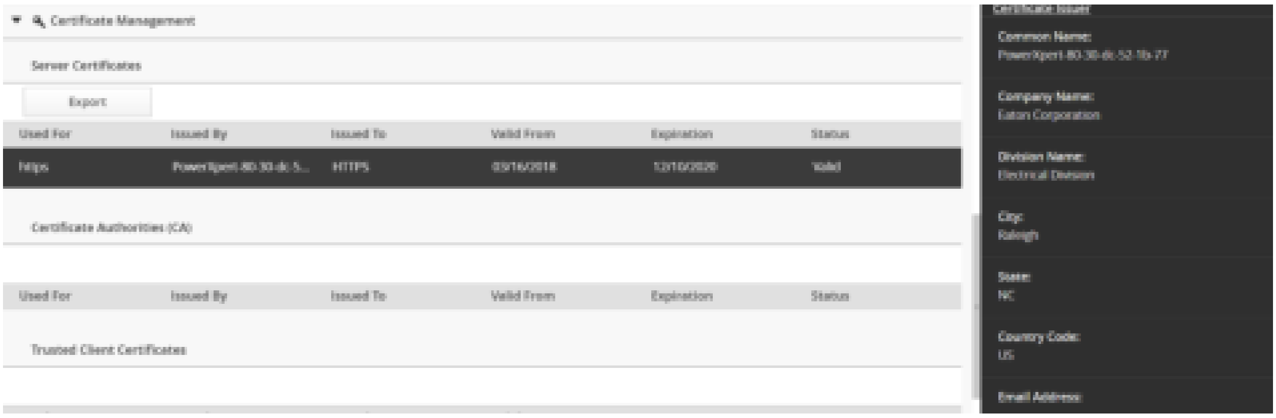


The first list of certificates in the **Certificate Manager** module is the **Server Certificates**.

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

23.3.2 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.



Certificate Management

Server Certificates

Export

Used For	Issued By	Issued To	Valid From	Expiration	Status
https	PowerXpert-80-30-dc-5...	HTTPS	03/16/2018	12/10/2020	Valid

Certificate Authorities (CA)

Used For	Issued By	Issued To	Valid From	Expiration	Status

Trusted Client Certificates

Certificate Issuer

Common Name:
PowerXpert-80-30-dc-52-1b-77

Company Name:
Eaton Corporation

Division Name:
Electrical Division

City:
Raleigh

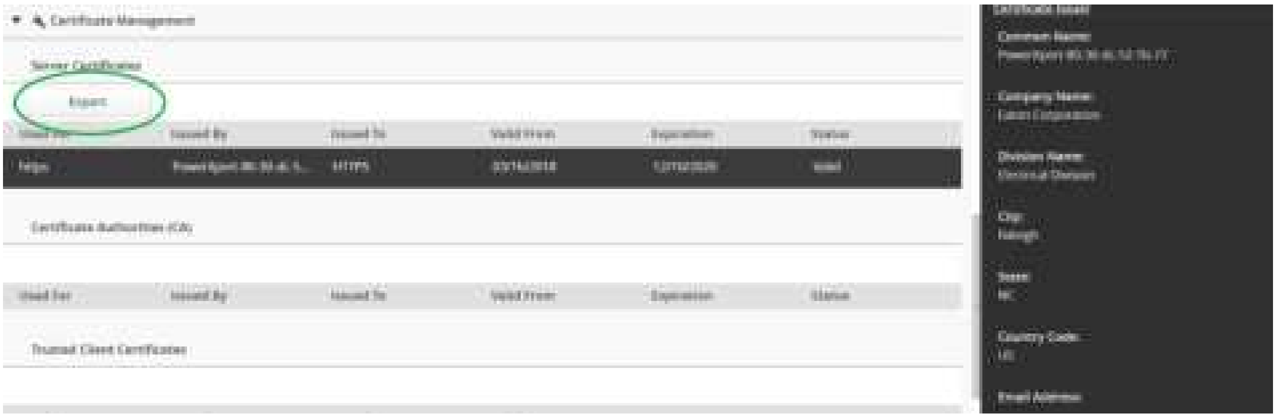
State:
NC

Country Code:
US

Email Address:

23.3.3 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".



Certificate Management

Server Certificates

Export

Used For	Issued By	Issued To	Valid From	Expiration	Status
https	PowerXpert-80-30-dc-5...	HTTPS	03/16/2018	12/10/2020	Valid

Certificate Authorities (CA)

Used For	Issued By	Issued To	Valid From	Expiration	Status

Trusted Client Certificates

Certificate Issuer

Common Name:
PowerXpert-80-30-dc-52-1b-77

Company Name:
Eaton Corporation

Division Name:
Electrical Division

City:
Raleigh

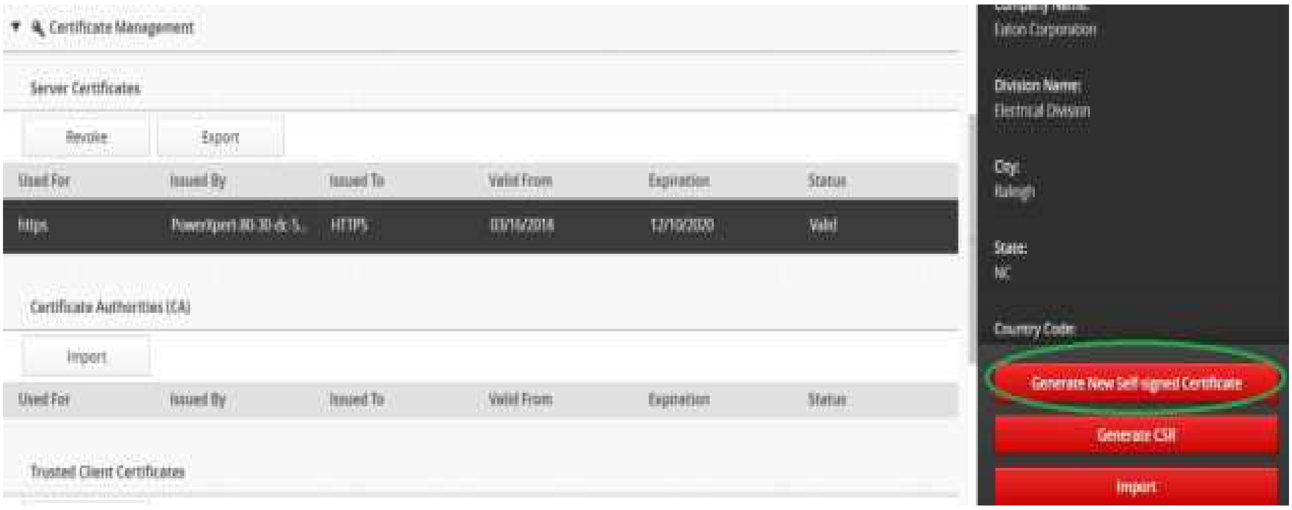
State:
NC

Country Code:
US

Email Address:

23.3.4 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.



Certificate Management

Server Certificates

Used For	Issued By	Issued To	Valid From	Expiration	Status
https	PowerXpert 80-30-dc-5...	HTTPS	03/16/2014	12/10/2020	Valid

Certificate Authorities (CA)

Used For	Issued By	Issued To	Valid From	Expiration	Status

Trusted Client Certificates

Company Name: Eaton Corporation

Division Name: Electrical Division

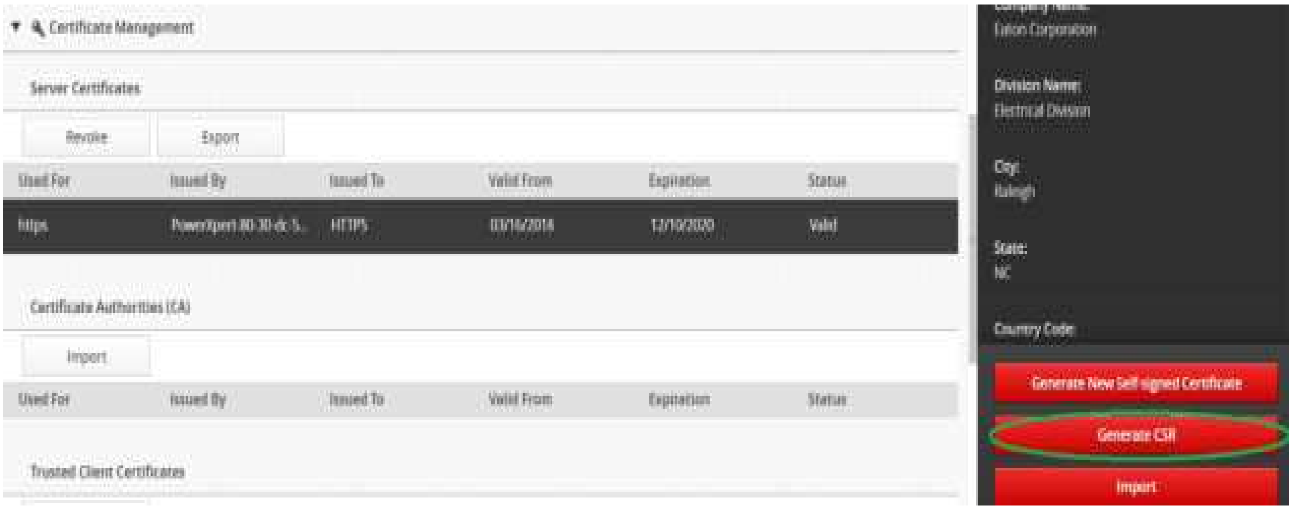
City: Raleigh

State: NC

Country Code:

23.3.5 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.



Certificate Management

Server Certificates

Used For	Issued By	Issued To	Valid From	Expiration	Status
https	PowerXpert 80-30-dc-5...	HTTPS	03/16/2014	12/10/2020	Valid

Certificate Authorities (CA)

Used For	Issued By	Issued To	Valid From	Expiration	Status

Trusted Client Certificates

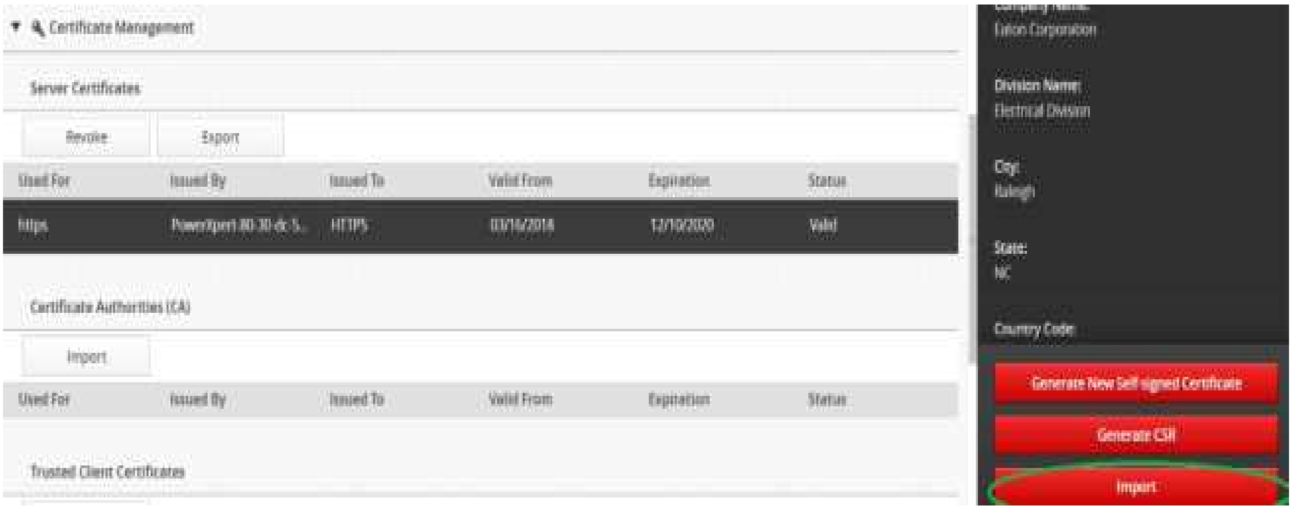
Company Name: Eaton Corporation

Division Name: Electrical Division

City: Raleigh

State: NC

Country Code:



Certificate Management

Server Certificates

Used For	Issued By	Issued To	Valid From	Expiration	Status
https	PowerXpert 80-30-dc-5...	HTTPS	03/16/2014	12/10/2020	Valid

Certificate Authorities (CA)

Used For	Issued By	Issued To	Valid From	Expiration	Status

Trusted Client Certificates

Company Name:
Eaton Corporation

Division Name:
Electrical Division

City:
Raleigh

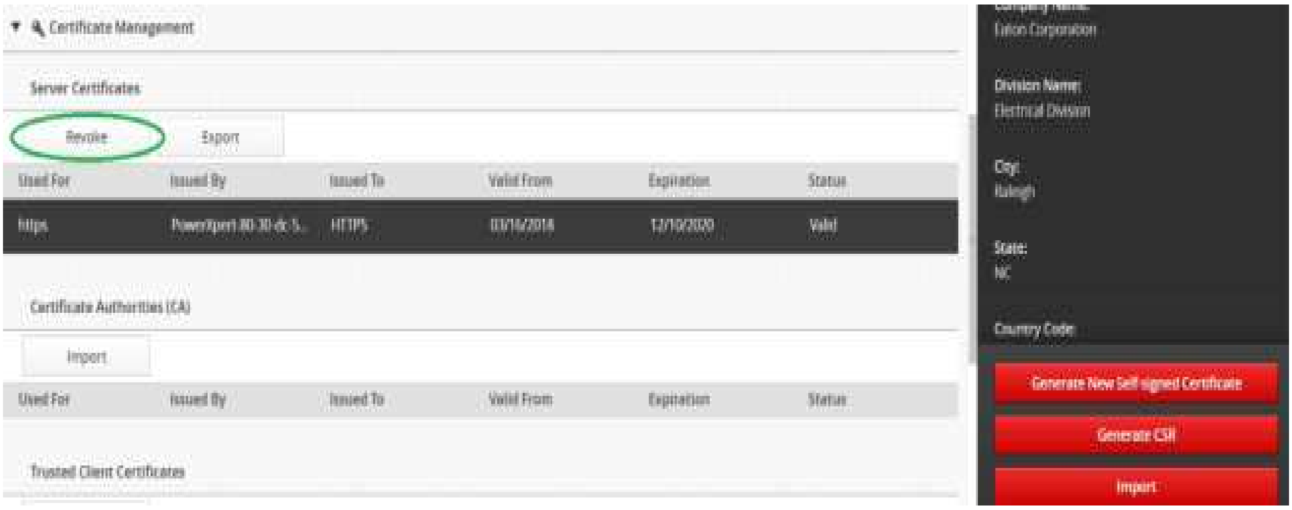
State:
NC

Country Code:

23.3.6 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.



Certificate Management

Server Certificates

Used For	Issued By	Issued To	Valid From	Expiration	Status
https	PowerXpert 80-30-dc-5...	HTTPS	03/16/2014	12/10/2020	Valid

Certificate Authorities (CA)

Used For	Issued By	Issued To	Valid From	Expiration	Status

Trusted Client Certificates

Company Name:
Eaton Corporation

Division Name:
Electrical Division

City:
Raleigh

State:
NC

Country Code:

24 Cloud Connection Setup

Eaton's PXG900 is capable of publishing device data to the cloud, and data can be visualized with the Eaton cloud application: 'Power Xpert Energy Visualization Application' (PX-EVA).

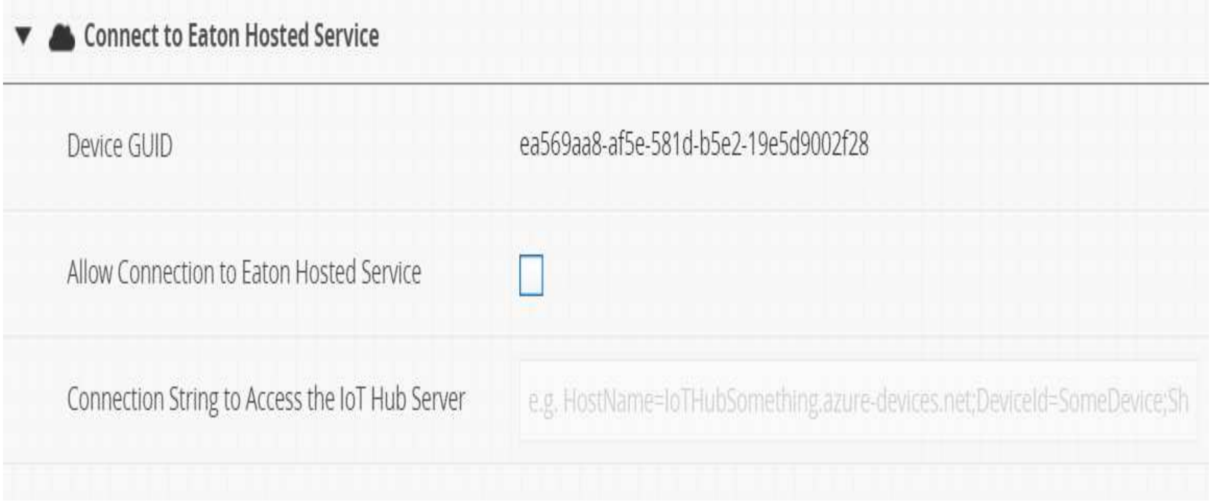
Please contact Eaton customer support to enable cloud connectivity for your device.

Email: MRSupport@eaton.com[10]

Contact number: 1-844-435-8982

With the help of Eaton's support team, follow steps below to enable cloud connectivity for your device.

1. The Eaton support team will need unique GUID and Serial Number for your device to enable cloud connectivity. On PXG900 Web UI, navigate to Settings > Network Access> Connect to Eaton Hosted Service and copy the Device GUID.



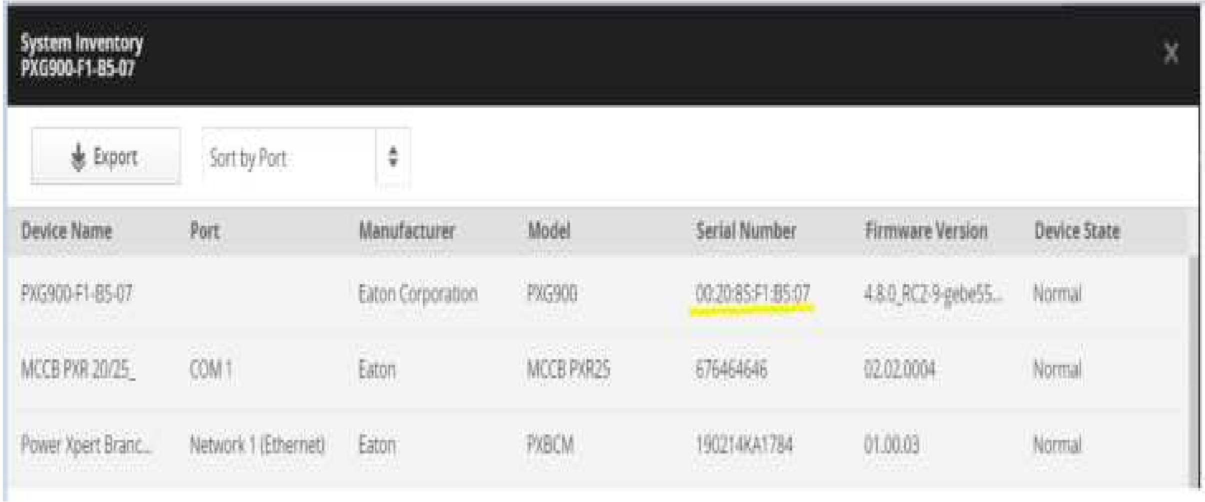
▼ Connect to Eaton Hosted Service

Device GUID ea569aa8-af5e-581d-b5e2-19e5d9002f28

Allow Connection to Eaton Hosted Service □

Connection String to Access the IoT Hub Server e.g. HostName=IoTHubSomething.azure-devices.net;DeviceId=SomeDevice;Sh

2. To get the serial number for the device, navigate to Network > PXG900 > Choose An Action > System Inventory and copy the serial number of PXG900 (shown below).



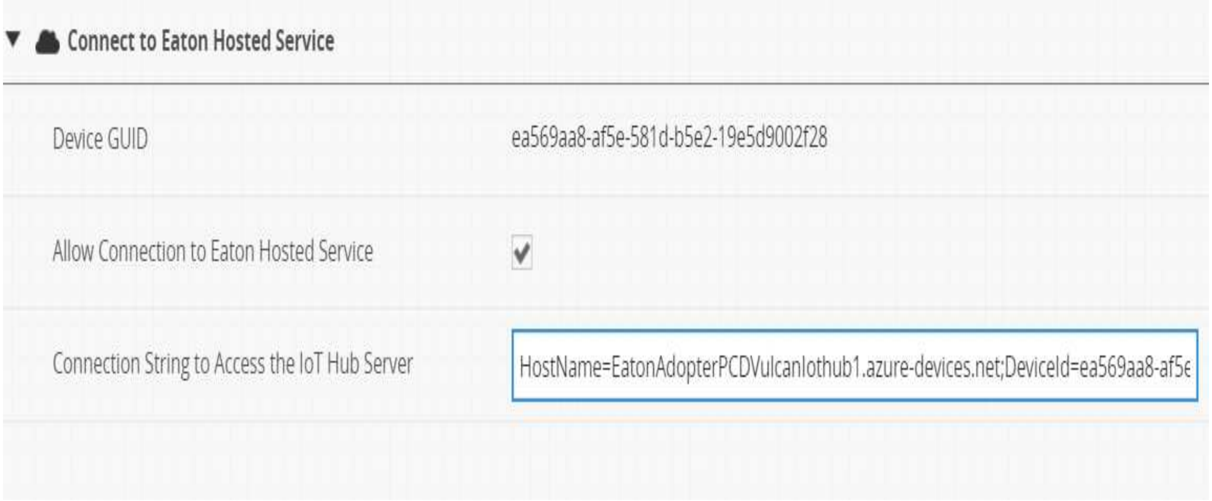
System Inventory
PXG900-F1-B5-07

Device Name	Port	Manufacturer	Model	Serial Number	Firmware Version	Device State
PXG900-F1-B5-07		Eaton Corporation	PXG900	00:20:85:F1:B5:07	4.8.0_RC2-9-gebe55...	Normal
MCCB PXR 20/25_	COM 1	Eaton	MCCB PXR25	676464646	02.02.0004	Normal
Power Xpert Branc...	Network 1 (Ethernet)	Eaton	PXBCM	190214KA1784	01.00.03	Normal

[10] mailto:MRSupport@eaton.com

3. Using GUID and Serial Number Eaton team will register your device on the cloud and will provide a connection string, which looks like this:
   HostName=EatonAdopterPCDVulcanIothub1.azure-devices.net[11];DeviceId=ea569aa8-af5e-581d-b5e2-19e5d9002f28;SharedAccessKey=GA6+YMl6ykBxaP5z4qJbz2Yn2UcCnlqE1BbDal3RO0s=

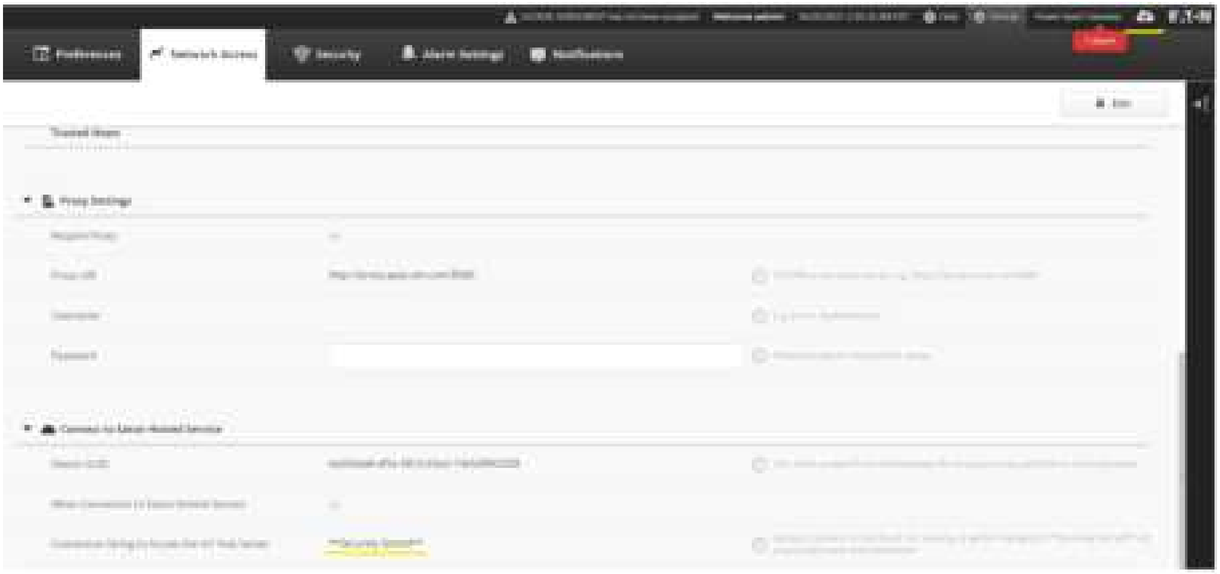
4. Navigate to Settings > Network Access > Connect to Eaton Hosted Service. Click the Edit button at the top right corner and set the checkbox for 'Allow Connection to Eaton Hosted Service'. Copy the connection string and save changes.



▼ Connect to Eaton Hosted Service

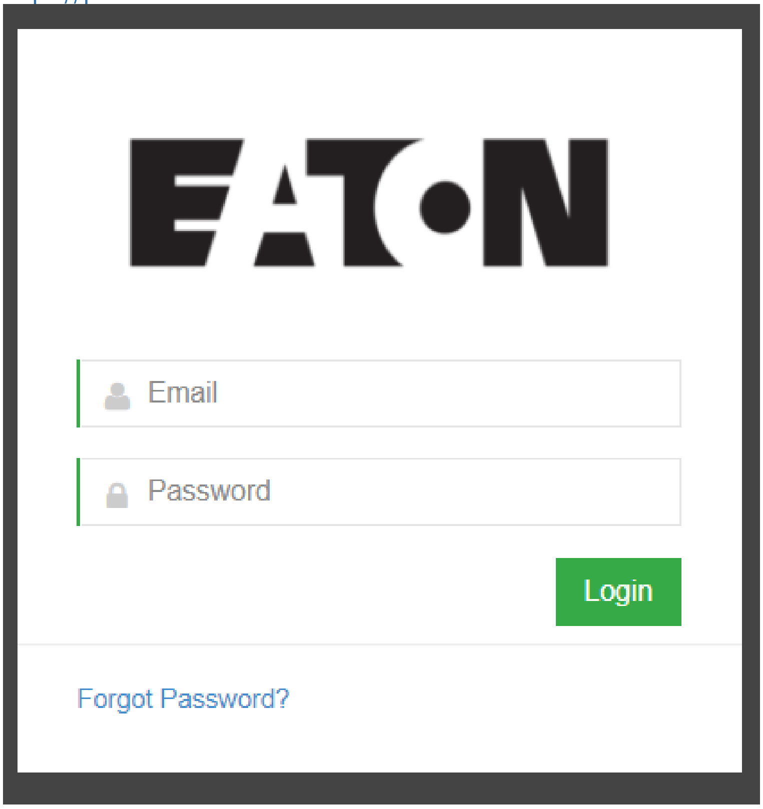
Device GUID	ea569aa8-af5e-581d-b5e2-19e5d9002f28
Allow Connection to Eaton Hosted Service	☑
Connection String to Access the IoT Hub Server	HostName=EatonAdopterPCDVulcanIothub1.azure-devices.net;DeviceId=ea569aa8-af5e

5. The device will try to establish a connection to the cloud. Cloud connectivity status is displayed at the top right corner. A check mark denotes a connection; an 'x' means that the PXG is disconnected.
   If the device is not able to establish connection in the first attempt, it will try to reconnect after every 1 minute.



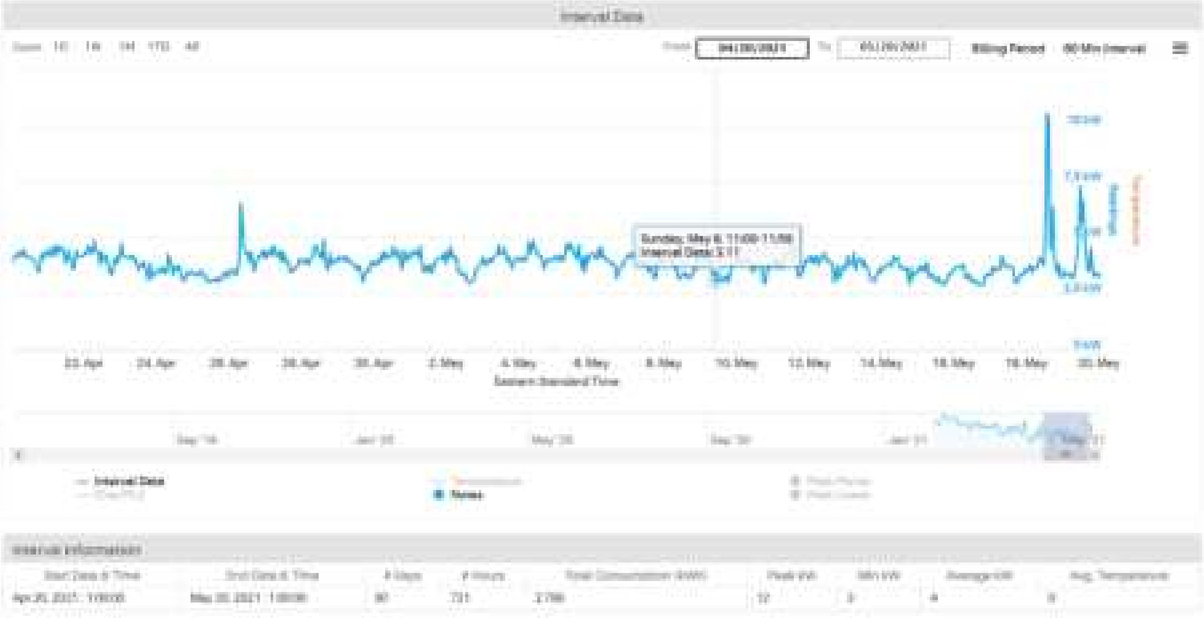
[11] http://eatonadopterpcdvulcaniothub1.azure-devices.net/

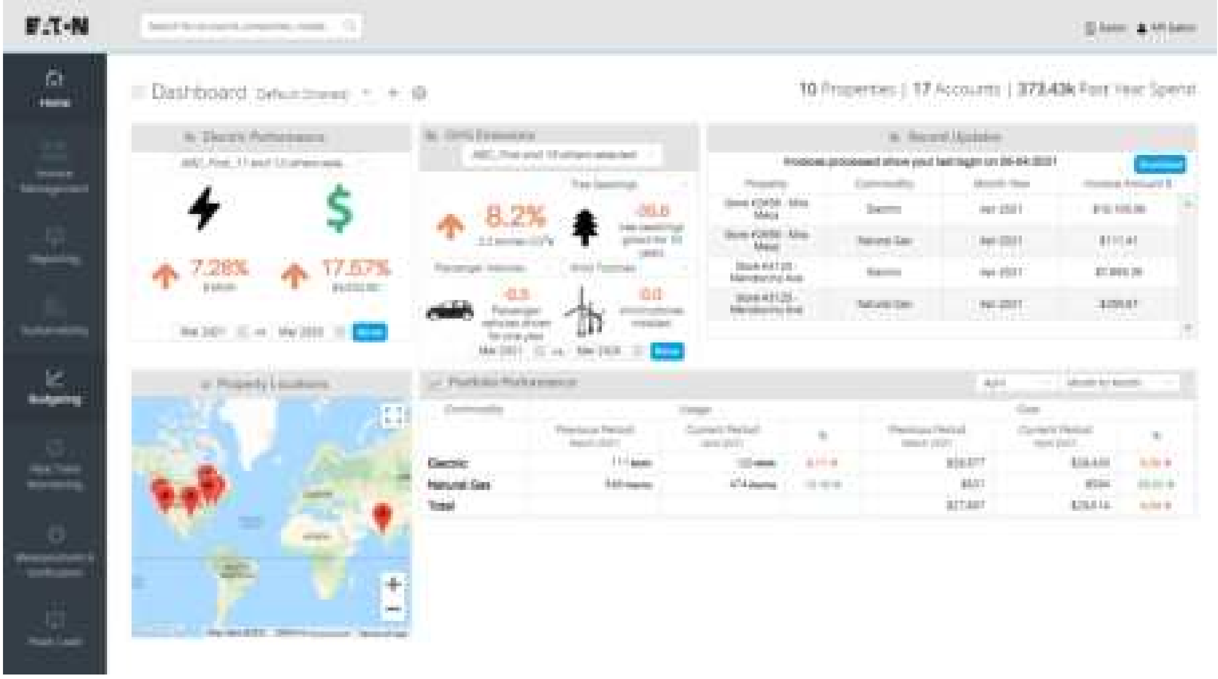
6. The Eaton support team will create an account for you to access Power Xpert Energy Visualization Application (PX-EVA). You can access the application at: https://px-eva.eaton.com[12]



[12] https://px-eva.eaton.com/

7. This how you can visualize your real-time device data and energy usage using PX-EVA.





Note : Before attempting a connection to a cloud application, make sure PXG is connected to the internet, Proxy and DNS must be correctly configured.

24.1 IoT Data Integrity:

PXG900 is capable of ensuring IoT data integrity by publishing data up to 24 hours after capture in case of loss of IOT connectivity due to network issues. If the device is unable to send messages to the configured IOT Hub due to a network outage, once the network issue is resolved and the device starts communicating, pending messages will be sent. If IOT connectivity is down for more than 24 hours, the latest 24 hours of data will be published.

Time to publish past data:

The time taken to publish the past data is dependent on the number of devices connected to the gateway and time for which the network was down. To avoid message congestion at the IOT hub, a 10 second delay is added for each message.
For example, with a trend interval of 5 minutes, 12 trend messages will sent every hour per device; with a 10 second delay while publishing the past data, it would take 120 seconds (2 minutes) per device, per hour. Refer to the example below to understand how to calculate the time required to publish past data.

Consider a gateway with 20 devices (including sub meters or virtual meters) connected to it, and it lost connectivity for 5 hours. Here is how to estimate the time required to publish the data after connection is re-established.
Number messages to be published for 5 hours = Number of devices * Number of hours of discontinuity * Number of messages per hour
=20*5*12
= 1200 messages to be published

Time taken to publish the data with 10sec delay within messages = 1200 *10 sec
= 12000 sec
= 3 hours and 20 minutes

If network connection is interrupted again during the backup process, it may take longer than was calculated. If there are multiple outages, the outage data will be published sequentially for each instance.

Session Log:
In the event of loss of connectivity with the IOT hub, re-connection and publishing of past data is recorded in the session log. Users can download session logs from the UI.
Network -> Power Xpert Gateway -> Choose an Action -> Audit Logs -> Session
Check entries for iot_agent in session log.

Powering Business Worldwide

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Printed in USA
Publication No. MN152006EN
June 2021