inSIGHT™
Data Monitoring

Ethernet Gateway User's Manual

Version 1.1

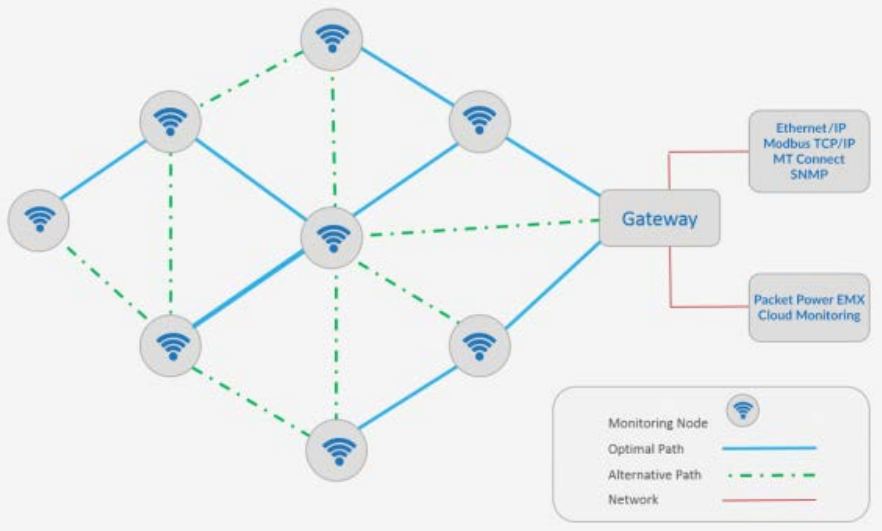
Wiring Device – Kellems
Hubbell Incorporated (Delaware)
Shelton, CT 06484
1-800-288-6000
www.hubbell-wiring.com

Contents

Ethernet Gateway Overview

The Ethernet Gateway is a key component of the Hubbell system architecture. It provides an interface between the wireless monitoring devices and the monitoring application. The Gateway automatically detects any new monitoring devices, seamlessly adding them to the network.

All Gateways need to be installed and configured to run on the local Ethernet network. If the monitoring application is gathering data using SNMP or Modbus protocols, some additional steps are needed that are specific to each of those protocols.



Gateway Models (US2 models also available)

Model Number	Description	Protocol	Monitoring units
HBLGW04000EUS1 HBLGW04000LUS1	Ethernet Gateway V4	EMX	100 30
HBLGW0400MEUS1 HBLGW0400MLUS1	Ethernet Gateway V4 Modbus	Modbus TCP/IP	100 30
HBLGW0400SEUS1 HBLGW0400SLUS1	Ethernet Gateway V4 SNMP	SNMP	100 30
HBLGW040MTEUS1 HBLGW040MTLUS1	Ethernet Gateway V4 MT Connect	MTConnect®	100 30
HBLGW0400EEUS1 HBLGW0400ELUS1	Ethernet Gateway V4 Ethernet/IP	EtherNet/IP™	100 30

Network Configuration

Installing the Ethernet Gateway

Each location in which Smart Power Cables are deployed must have one or more Hubbell Ethernet Gateways to gather data from the Smart Power Cables.

Refer to Hubbell's Ethernet Gateway User's Manual or Quick Start Guide for more information.

Configuring Network Settings

The Gateway requires an IP address prior to being network accessible unless it is being used in DHCP mode.

Before setting the IP address make sure that you have the following data provided to you by your IT administrator.

1) IP Address

2) Gateway

3) Netmask (subnet mask)

4) DNS

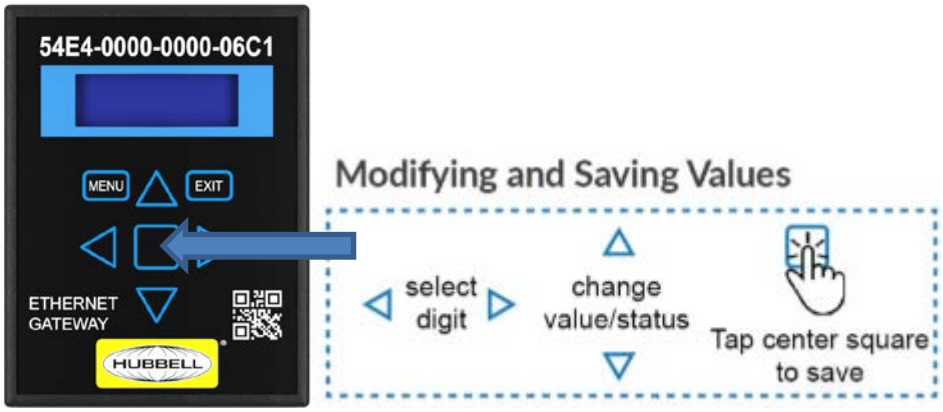
Using the touchpad to navigate

If the Gateway is new and does not have an IP address, you can enter the IP address directly onto the Gateway using the on board "touchpad" and display.

After the Gateway is energized and completes its boot sequence (approximately 30-60 seconds), the Network Status menu will appear.

This will reveal details about the Gateway's version, IP address (if previously programmed), MAC address, and Uptime (duration since last energization).

To navigate the menu, press the touchpad in a corresponding direction and "tap" to enter a selection.



Gateway LCD menu

The network status menu will display any configured network parameters.

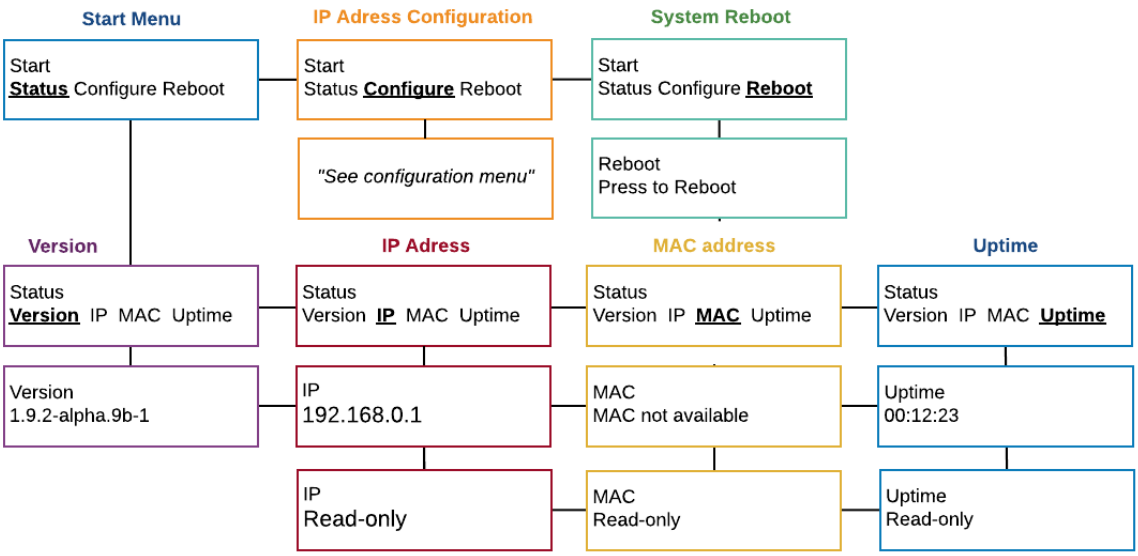
Version: Gateway's firmware version

IP Address: Programmed IP address

MAC Address: Applicable MAC address

System Reboot: Reboots the Gateway

Uptime: Total time since the Gateway was last energized



Turning DHCP on/off using the local LCD Menu

The Gateway is provided with DHCP "on" as a default.

DHCP addressing relies on the server to automatically assign the IP information eliminating the need to manually input the IP addressing.

To enable manual IP addressing, as required in most cases, it is necessary to turn DHCP off by following the menu instructions below.

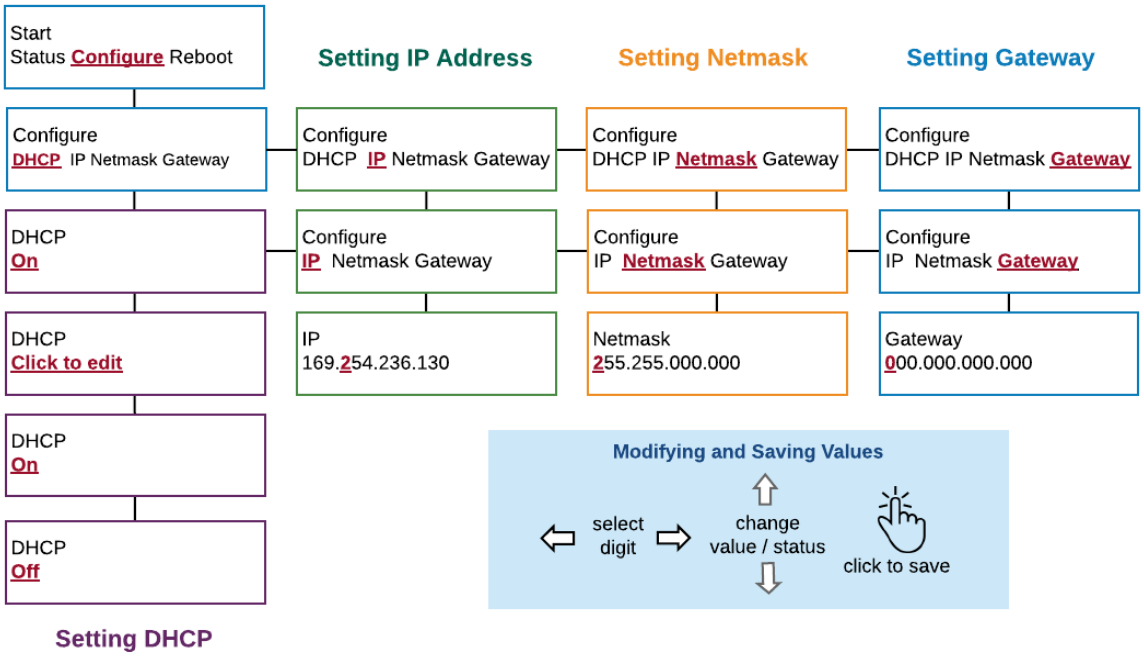
When DHCP is turned off, the configuration menu will reveal options for inputting IP address information.

Entering IP address data using the local LCD Menu

With DHCP turned off the *Configure* menu will reveal options for setting the IP address, Netmask and Gateway.

All of these parameters need to be filled in before the Gateway can be operational.

If you do not have this information it can be provided to you by your network administrator.

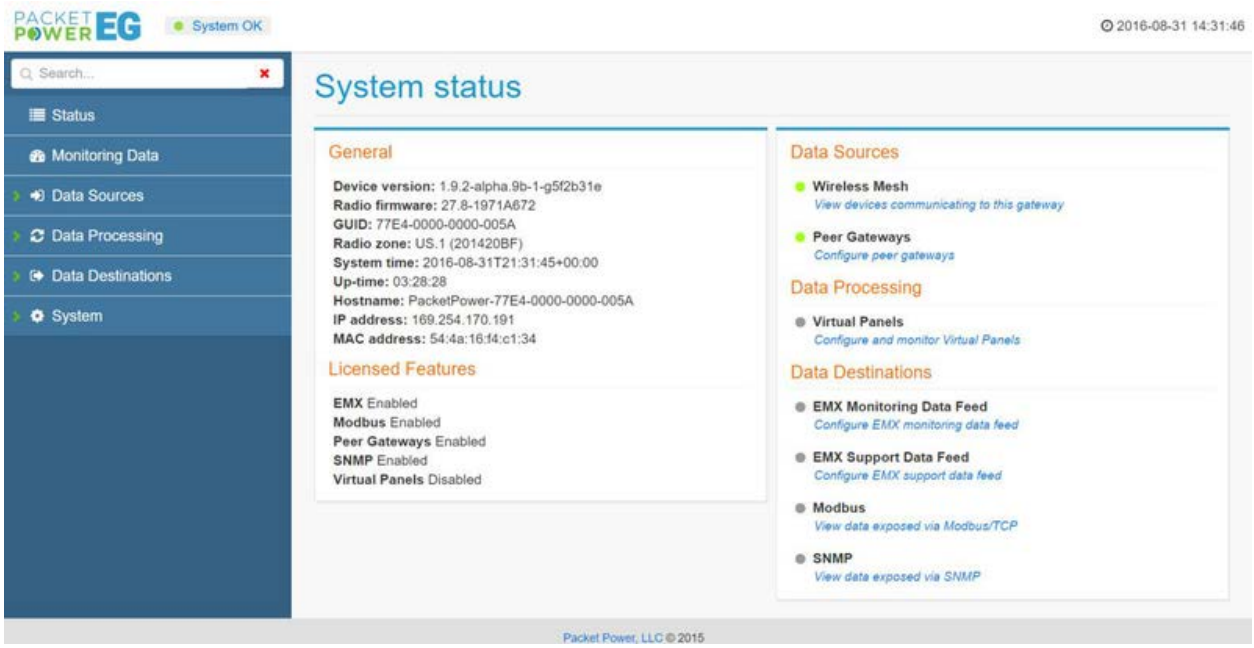


Configuring using the Gateway Web Console

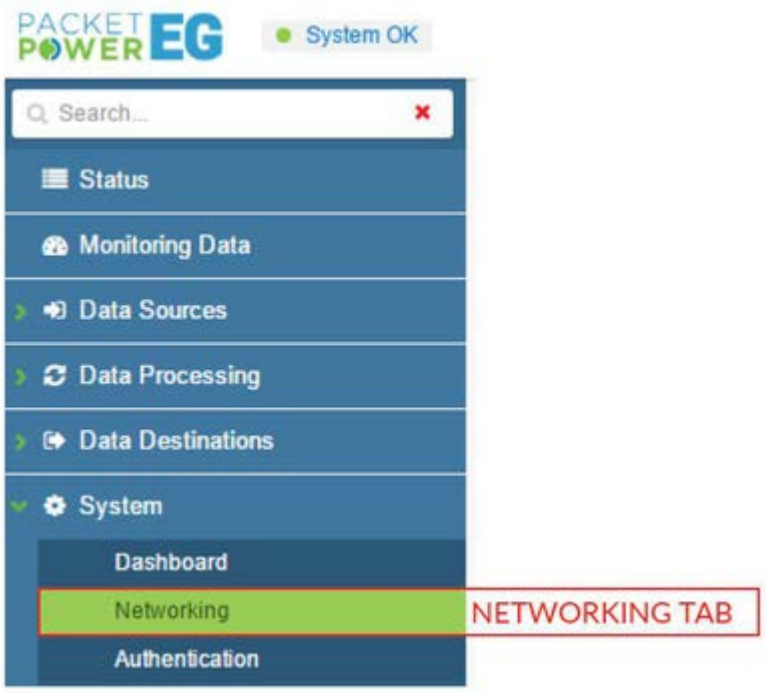
Once an IP address is assigned to the Gateway either manually or via DHCP, you can access the Gateway console using a standard web browser and entering the IP address of the Gateway.

This requires that the Gateway be connected via Ethernet network router or switch. Under some circumstances the Gateway can be accessed and configured directly from a PC but many enterprise systems prevent external IP addressing functions on a PC.

The Gateway console is described in greater detail online at: https://dox.packetpower.com/ Ethernet---Gateway---Version---4---Web---Console.html???
The Gateway Console status screen will appear as shown below.



To access the network settings, click the "**System"** tab on the left.



In the **System** tab sub menu, click the **"Networking"** tab.

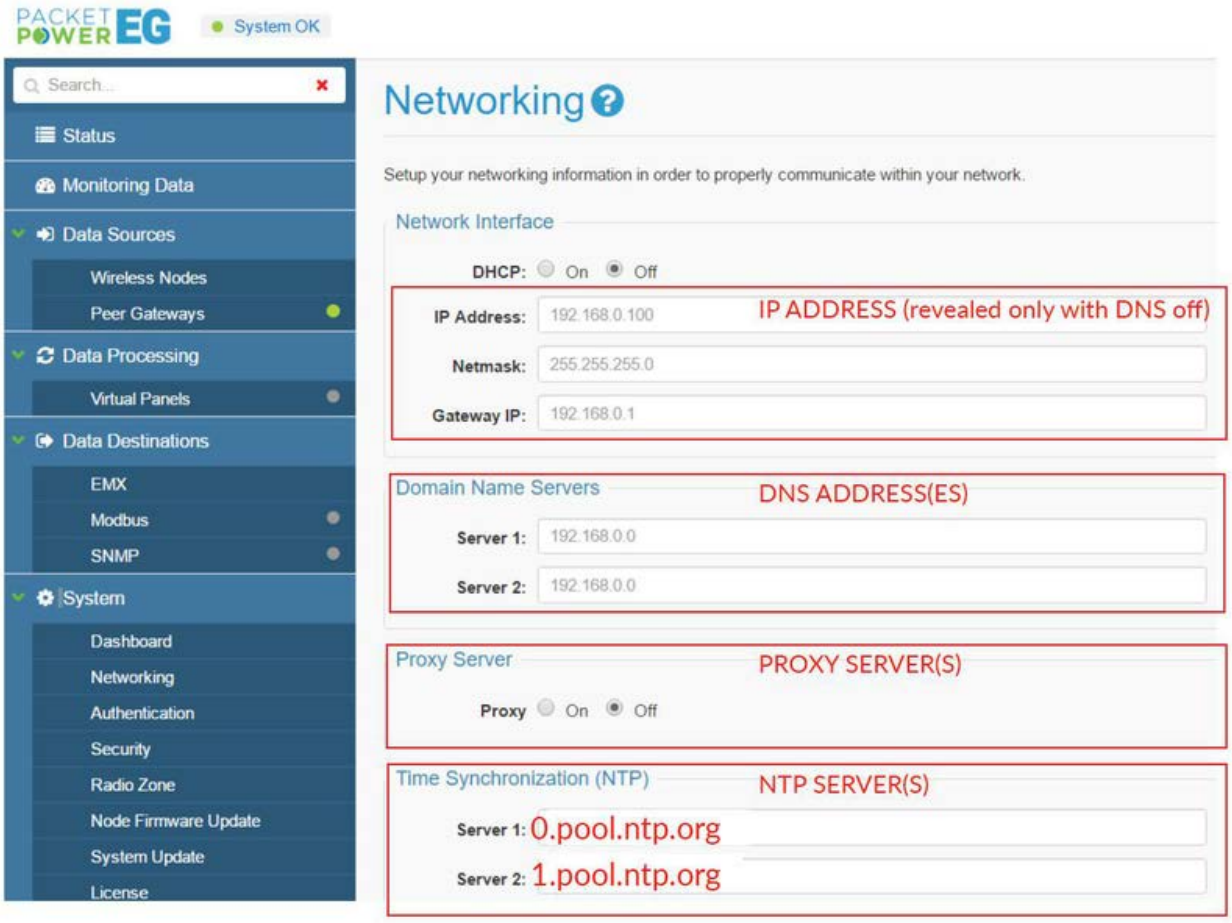
If DHCP is "on" you will not be able to access any network setting until it is switched off under the **Network Interface** section.

When DHCP is turned off the network settings will be revealed in the **Network Interface** section. It is now possible to modify the IP address, Netmask, Gateway addresses.

If using DNS (Domain Name Servers), input the server address under the **Domain Name Server** section.

In order for the Gateway to have a proper time reference, a NTP server address is needed in the Time Synchronization Section.

The default time servers are 0.pool.ntp.org and 1.pool.ntp.org. Once a time server is entered confirm the time at the top right of console. For more information on available NTP servers see the NTP server section. The time will be expressed in the top right corner of the Console screen.



Configuring Data Destinations

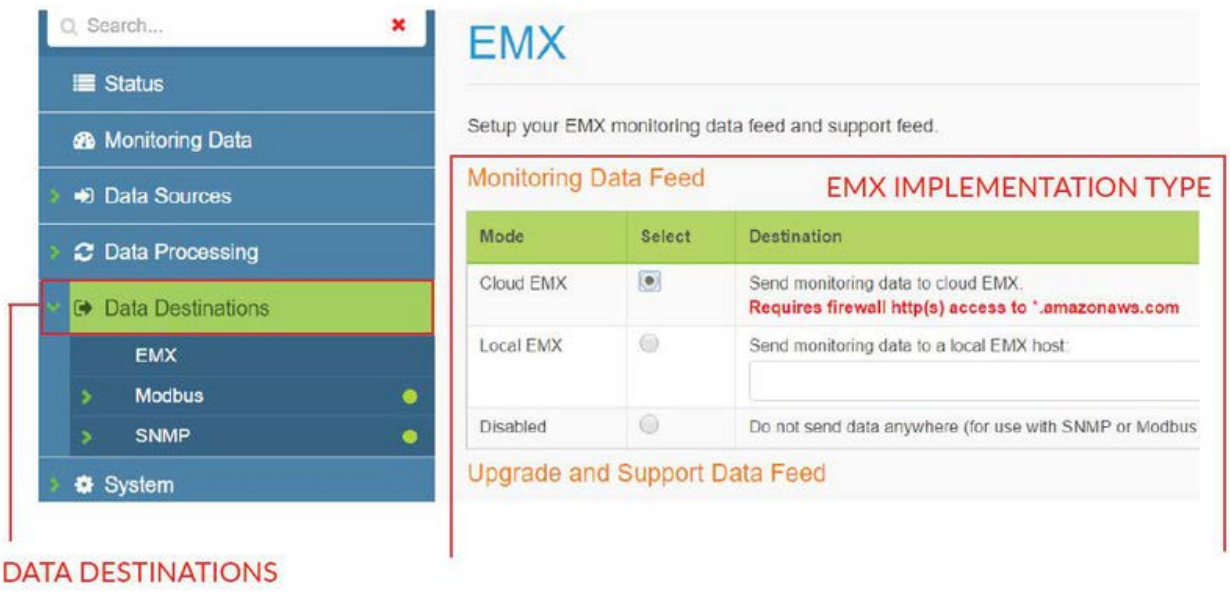
Data Destinations configures how the Gateway delivers data. The Gateway can make monitoring data accessible via three formats:

1. EMX Monitoring Portal – Note: data can be provided simultaneously to the EMX Portal while serving Modbus TCP/IP or SNMP data.
2. Modbus TCP/IP
3. SNMP (versions 1,2 and 3)

Configure the data destinations following these steps:

1. Click on the "Data Destinations" tab on the left menu.

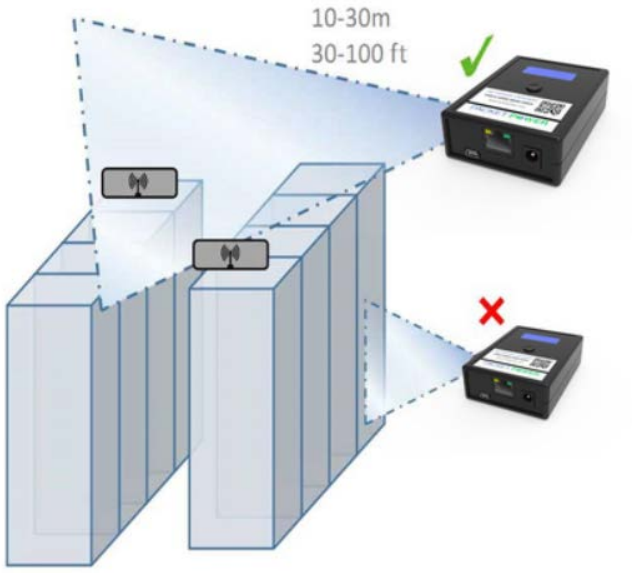
2. Select how you want to receive your data: EMX, Modbus or SNMP. Note that EMX feeds can be delivered simultaneously with Modbus and SNMP feeds.
3. For SNMP and Modbus implementation refer to the SNMP or Modbus support pages
4. Select the desired EMX implementation type (cloud is default) for both "Monitoring Data Feed" and "Upgrade and Support Data Feed" sections.
5. Ensure that the Gateway's IP address has outbound access to port 80 (HTTP) or 443 (HTPPS) for *.amazonaws.com when using cloud EMX.
6. Confirm that cloud and support data feeds are enabled with the network manager (cloud EMX implementations only).
7. For local EMX implementation, enter the IP address of the server.
8. Before you can access your data via EMX make sure your Hubbell representative has set up an EMX account. See the EMX support section for additional details.



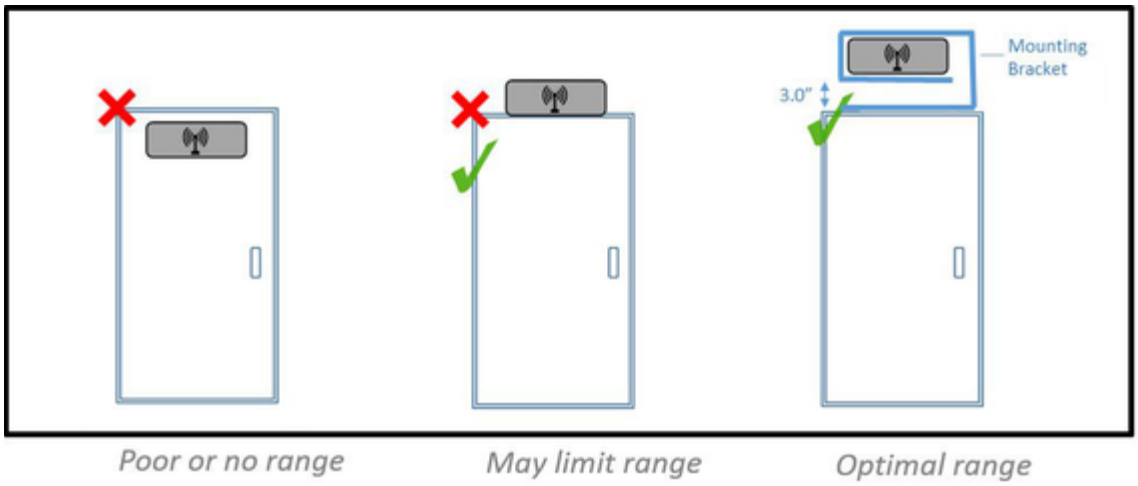
Physical Installation

Placement Guidelines

- The Gateway must be placed in a location likely to have good radio communication with monitoring nodes.
- Gateways should be located 10-30 meters from one or more monitoring nodes (ideally line of site)
- Place Gateways away from large metallic surfaces (use the mounting bracket for optimal placement)
- Never place a Gateway inside of a fully enclosed metal structure (exterior of the rack is better)
- Always try and locate the Gateway at the highest point that allows an unobstructed (line of sight) path to monitoring nodes
- Redundant Gateways are advised for any critical environment
- One Gateway can support up to 150 Hubbell monitoring devices; additional Gateways will improve polling speeds
- If you are placing multiple Gateways for better coverage or redundancy, try to space them approximately evenly throughout the facility as they will automatically balance network traffic
- In raised floor environments with monitoring nodes below the raised floor, Gateways may have to be placed below the floor or near floor air vents

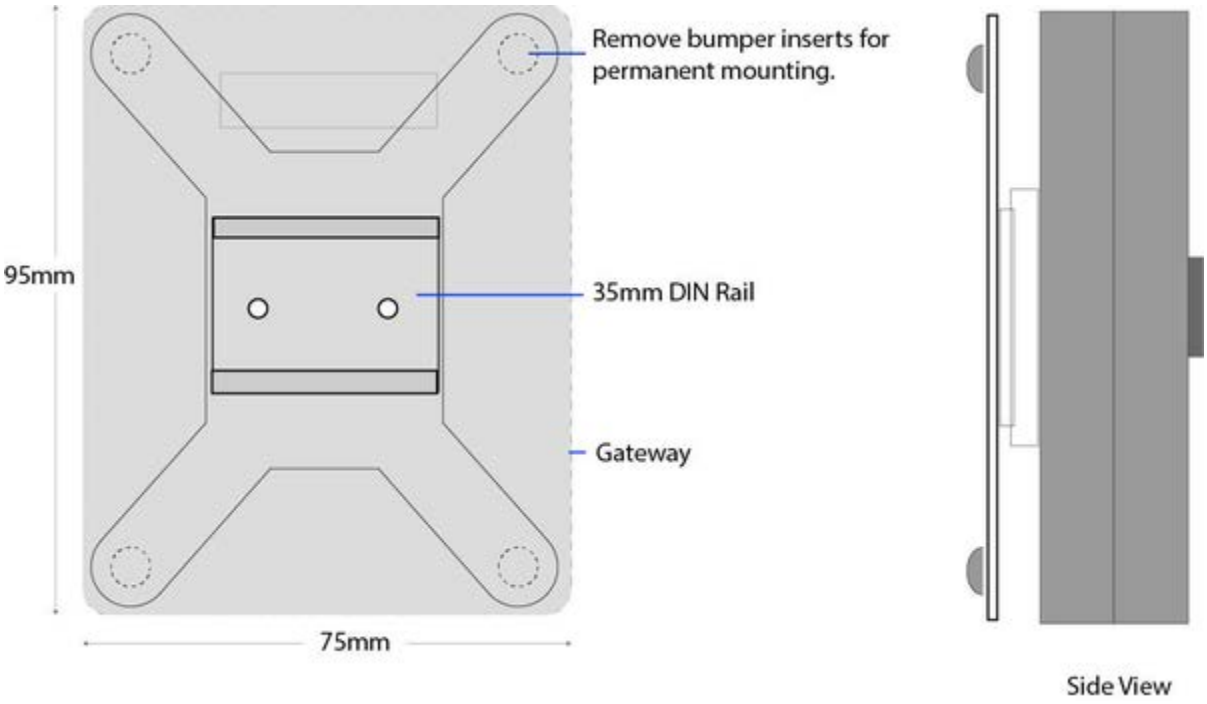


Always place Gateways as high as possible within line of site to monitoring nodes.



Never place Gateways inside metallic cabinets.

Mounting Bracket

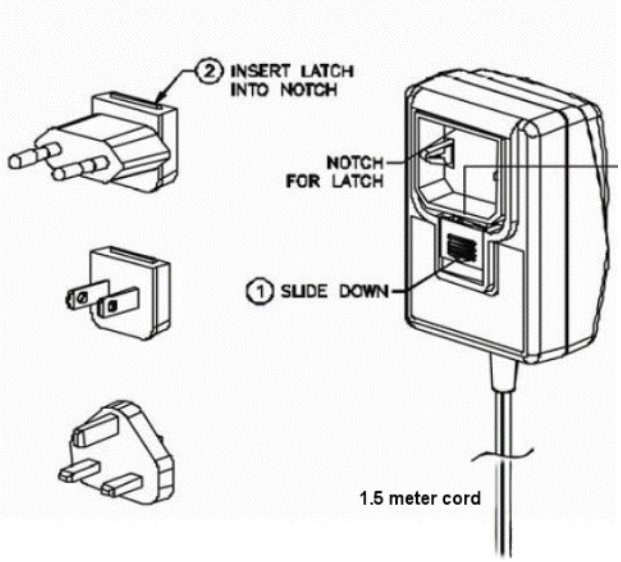


- The Gateway attaches to the mounting bracket using the DIN rail clip which snaps onto the receiver clip on the back of the Gateway
- The rubber bumpers on the back of the Gateway mount can be removed to expose 0.20" holes which can be used for permanent mounting with mechanical fasteners
- Adhesive tabs allow the Gateway to be wall mounted or surface mounted away from metallic surfaces like server cabinets
- Orientation of the Gateway is not critical

Power

The Ethernet Gateway uses a standard 5V DC power supply with a 5.5 x 2.1 x 11mm positive-on-center power jack. The following power supply options are available from Hubbell:

- Universal 100-240V wall-plug power adapters with a full set of international plugs, including C13 connectors for data center installations
- Power-over-Ethernet (PoE) adapters using a PoE splitter that plugs into the DC jack (cannot be powered by PoE in the Ethernet jack)
- USB power adapter cable for powering from any USB port (power-only, no data connection is made)



If powering using PoE (Power-over-Ethernet)

- A PoE splitter is required as the Gateway will not accept a PoE source directly into its Ethernet port
- Be sure that the PoE injector source is 5V DC, not 12, 24 or 48V DC and capable of at least 4W of power
- Splitters with voltage regulators that will drop the voltage to 5V DC are available

Gateway Web Console

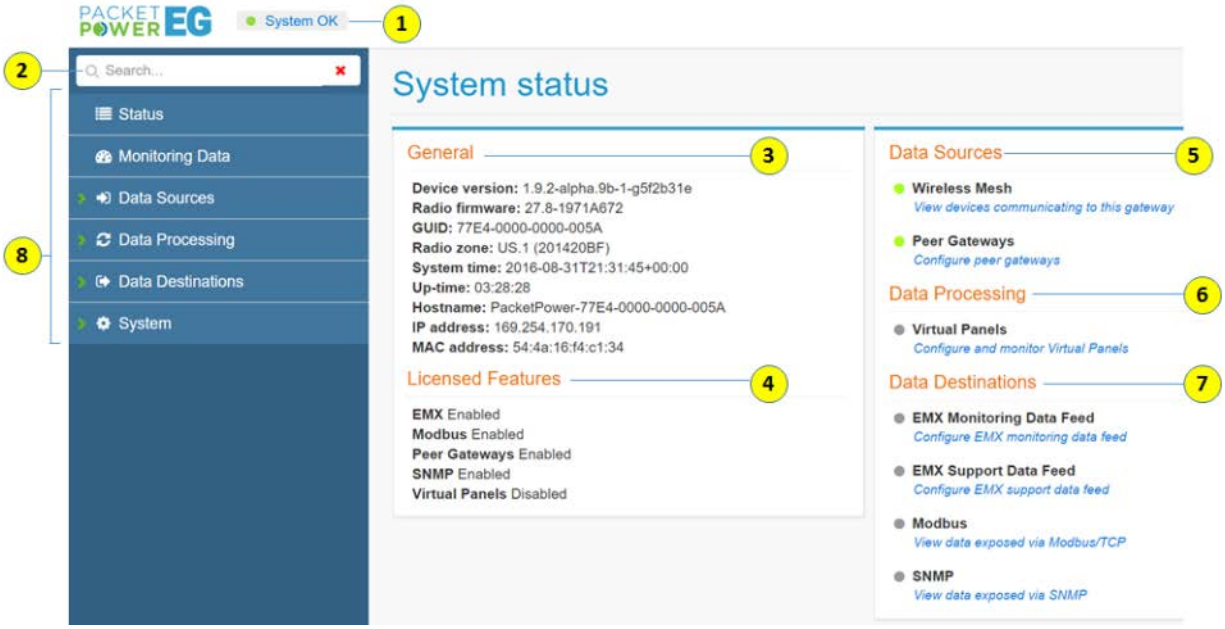
The Console is accessed by entering the IP address of the Gateway into a standard web browser.

Web Console contents

Status - provides a general overview of all critical Gateway functions as well as links to key sections required for configuration
Monitoring Data - shows which monitoring units are communicating with a gateway and provides access to real-time readings
Data Sources - indicate from where the Gateway is acquiring its data
Data Processing - provides the ability to manipulate data, including the Panel Editor for defining branch circuit panel maps
Data Destinations - configures the Gateway for data access via Modbus TCP/IP, SNMP and the EMX Portal
System - manage system settings such as IP addresses and firmware versions

Status

The Status page provides a general overview of all critical Gateway functions as well as links to key sections required for configuration.



(1) System Status Indicator: Indicates if Gateway is properly communicating with nodes and the network.

Green:	System OK
Yellow:	System problems
Red:	System not operational

(2) Search: Allows searching for any Gateway related item. For example, you can input the last four digits of a Node ID and relevant nodes will appear.

(3) General: Provides all data relating to the Gateway communications settings.

(4) Licensed Features: Indicates which features are licensed for use with this Gateway.

(5) Data Sources: Indicates from where the Gateway is acquiring data. This can be via wireless monitoring nodes or through other Peer Gateways.

(6) Data Processing: This function is used for virtual circuit mapping. It allows users to assign breaker types and locations when using multi-circuit monitoring features such as Branch Circuit Monitoring.

(7) Data Destinations: Configures data for export from the Gateway to Modbus TCP/IP, SNMP and the EMX Portal (cloud or local implementations).

(8) Menu: Provides access to various Gateway settings and tools.

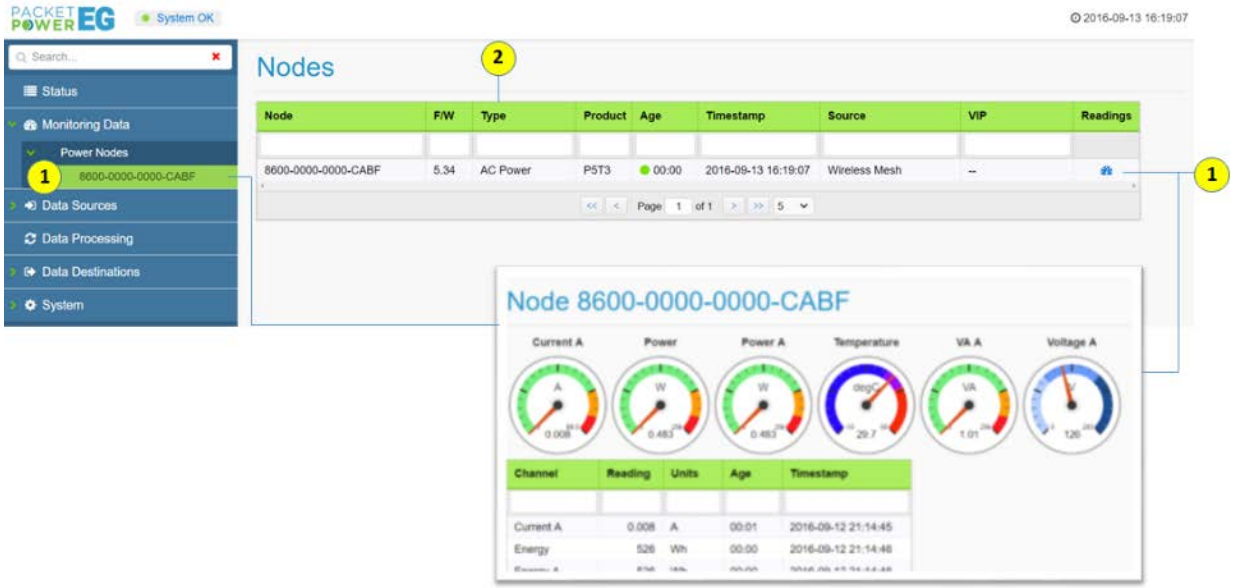
Monitoring Data

The Monitoring Data tab exposes all the nodes (monitors) associated with the Gateway. The sub menu will show associated nodes by type (power or environmental) along with their GUID.

(1) Clicking on a specific node ID will expose the "readings" for that node. Likewise the readings for a specific node can also be exposed by clicking on the "readings" icon.

(2) Nodes table headings

Node:	Monitoring node 16 digit user ID (GUID)
F/W:	Firmware version of monitoring node
Type:	Monitor type (i.e. AC power monitor, environmental monitor)
Product:	Product model name
Age:	Duration online
Time stamp:	Time reported by node
Source:	Where the data is originating from (wireless mesh network, other Gateway or third party device)
VIP:	Virtual IP address (used in SNMP applications)
Readings:	Exposes readings from the device



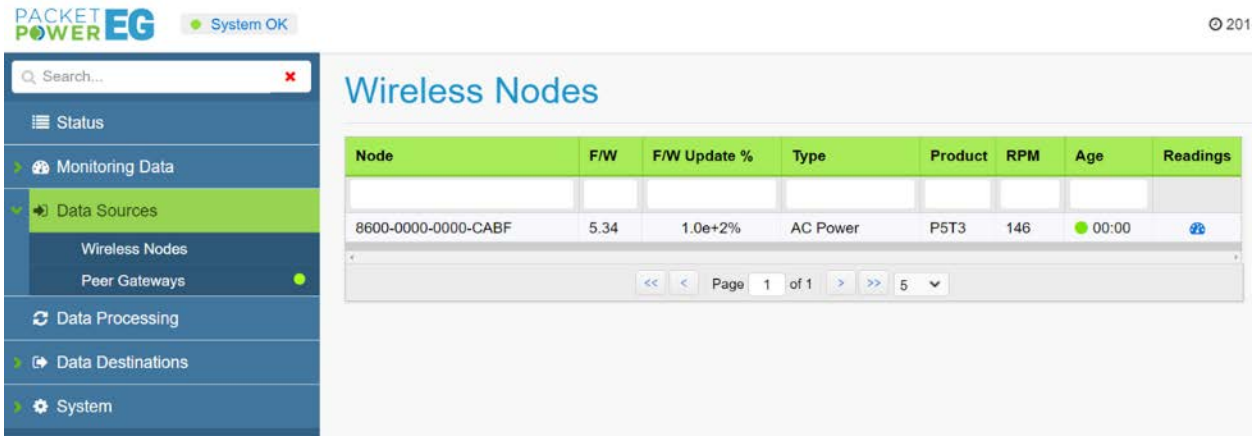
Data Sources

Data Sources indicate from where the Gateway is acquiring its data. This can originate from wireless nodes connected to the Gateway or from peered Gateways which are connected to the Gateway via the Ethernet network.

Wireless Nodes

The Wireless Nodes sub-menu will expose all of the monitoring nodes in radio contact with the Gateway. Nodes may be segregated by "type" in the sub menu i.e. "power" or "environmental monitors". To search for a specific node, input the node ID in part or full in the "Node" column. The data table for nodes is explained below:

Node: Monitoring node 16 digit user ID (GUID)
F/W: Firmware version of monitoring node
F/W Update %: Indicates the progress of a wireless firmware update of a monitoring node
Type: Monitor type (i.e. AC power monitor, environmental monitor)
Product: Product model name
RPM: Readings per minute or the frequency of data reports received from the node each minute. This will vary depending on the strength of the radio signal and ratio of node to Gateways
Age: Duration online
Readings: Exposes readings from the device



RPM (Readings per Minute) and Reporting Frequency: The reporting frequency of wireless nodes to the Gateway is a function of how many nodes share the Gateway and the strength of the radio connection(s) between the nodes and the Gateway. Nodes take readings up to hundreds of times per second depending on the model. This data will be stored and forwarded with each successful transmission. This means that even in the event of a lower RPM no data is compromised, but the data update rate will be slower.

If an improved RPM rate is required, you can add another Gateway to the network to load balance node traffic. This works best when there are high node counts. Alternatively, place the Gateway in a more central area with better radio visibility to all nodes or identify slow nodes and improve their radio visibility to another node or the Gateway.

Peer Gateways

Gateways can be peered (connected) with other Gateways over the network. This allows for retrieving data from multiple Gateways by polling a single Gateway. The peered Gateways do not have to be in similar locations as long as they are permitted to communicate with each other over the network.

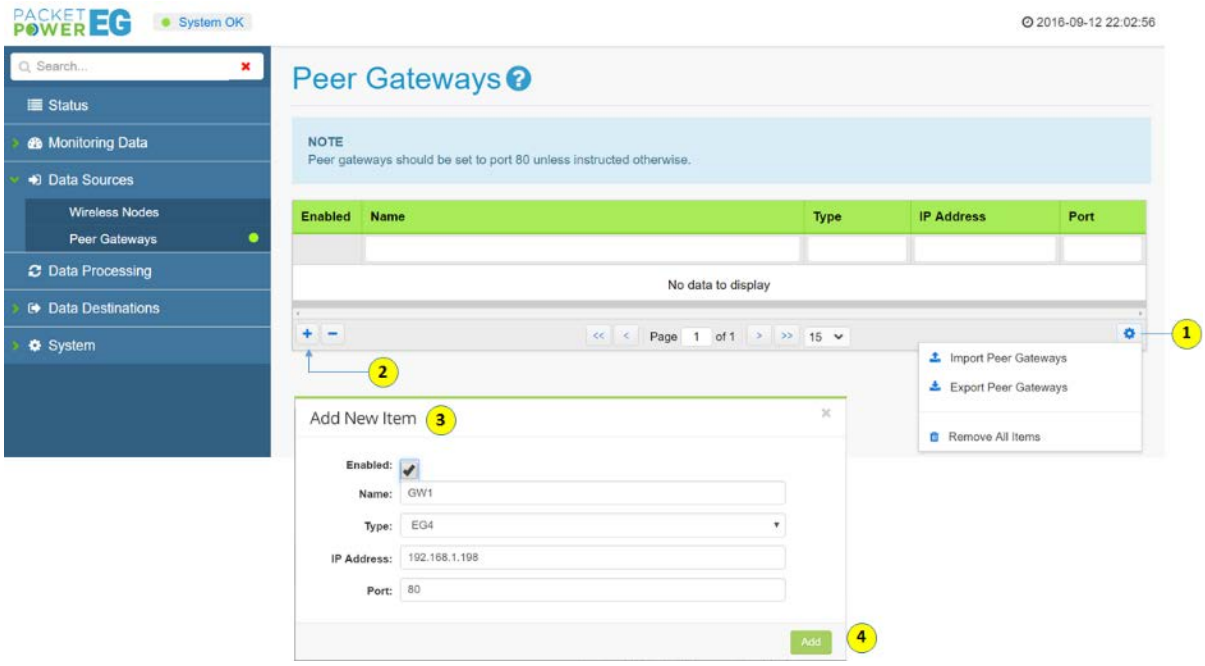
To enable Gateway peering on a specific Gateway:

1. Select the "Peer Gateways" tab under the "Data Sources" tab on the left menu
2. Click on the "+" icon (2) on the Peer Gateways chart
3. Complete the data on the "Add New Item" pop up menu (3) making sure the "Enabled" box is checked
   - **Name**: Friendly name description
   - **Type**: Gateway model (EG3 or EG4) of peer Gateway
   - **IP Address**: IP address of peered Gateway
   - **Port**: Network port; typically port 80
4. Click the green "Add" button to complete the process.

It will now be possible to extract data for the peered Gateway from this Gateway. Note that each Gateway must have peering data completed in order to receive data from other Gateways and act as "master".

Importing and Exporting Peer Gateway Data: For larger networks that contain a large volume of Gateways, peering data can be exported and saved as well as re-imported. This makes it easy to load peering data onto many Gateways without manual data entry.

To import or export peering data click on the utility icon (1) to expose the menu and follow the steps listed below. Note that data will be stored on a JSON file.



Data Destinations

The Gateway can make monitoring data accessible via five formats:

- EMX Monitoring portal
- Modbus TCP/IP
- SNMP (versions 1, 2 and 3)
- MTConnect
- EthernetIP

Note that data can be provided simultaneously to the EMX Portal while serving Modbus TCP/IP, SNMP, MTConnect or EthernetIP data.

EMX Energy Portal

To enable data to flow to the EMX portal: Select the "Data Destinations" tab on the left menu and click on "EMX" in the sub menu.There are two versions of EMX, a cloud based version and in some instances EMX may be installed as a local application. Select the version of EMX to be implemented in the "Monitoring Data Feed" and "Upgrade and Support Data Feed" sections. Note that Cloud EMX is the default selection.

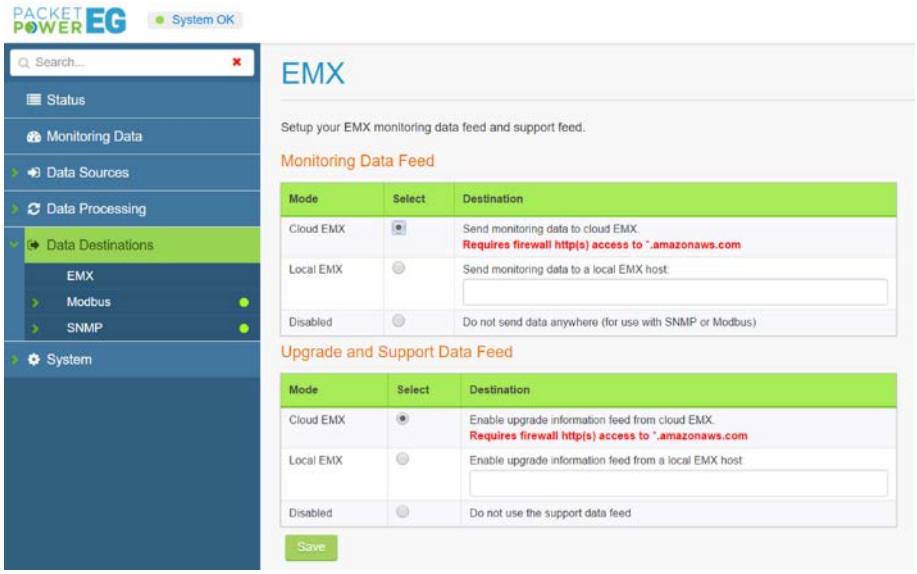
Cloud EMX

- Ensure that the Gateway's IP address has outbound access to port 80 (HTTP) or 443 (HTTPS) for *.amazonaws.com when using cloud EMX
- Confirm that cloud and support data feeds are enabled with the network manager (cloud EMX implementations only)

Local EMX

- Select "Local EMX" in the "Monitoring Data Feed" and "Upgrade and Support Data Feed" sections
- Enter the IP address of the local EMX server.

Note: Before you can access your data via EMX make sure your Hubbell representative has set up an EMX account.



Modbus

See Modbus TCP/IP Implementation section

SNMP

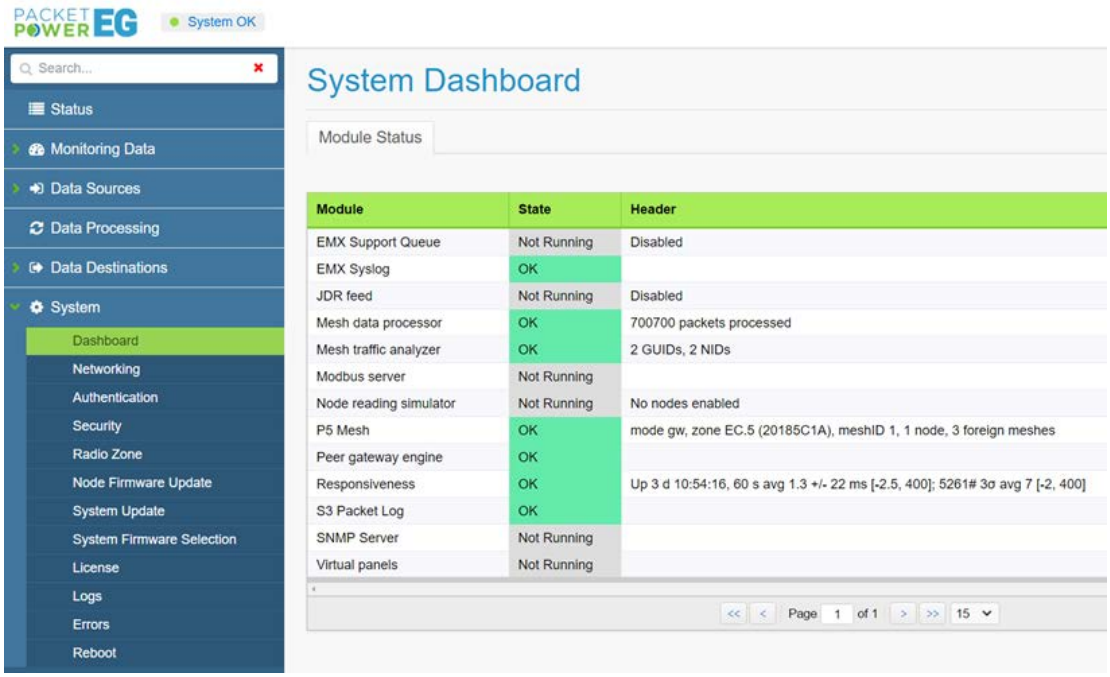
See SNMP Implementation section

System

The following resources are accessible under the "System" menu.

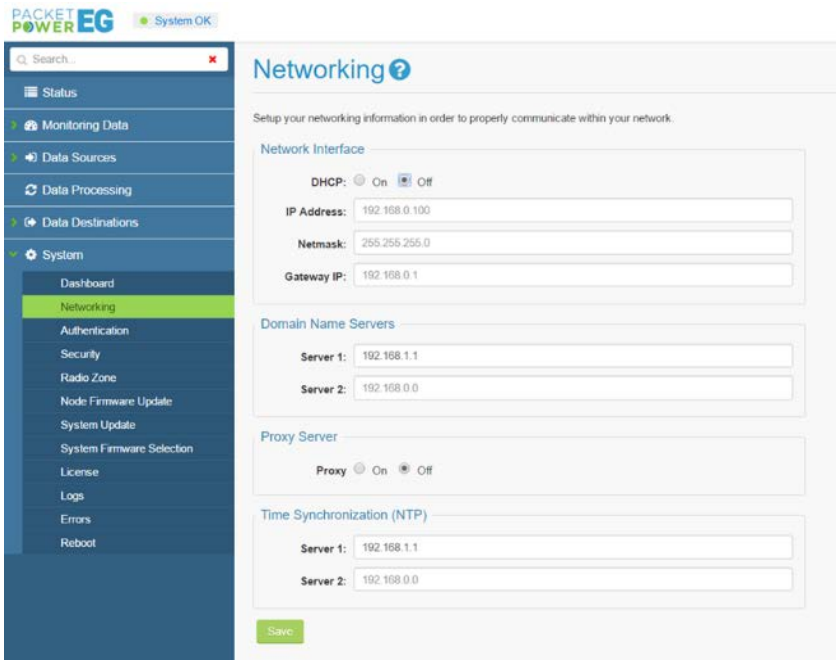
Dashboard

The Dashboard feature is a diagnostic tool for use by Hubbell and authorized partners. It may not be exposed on all Gateways.



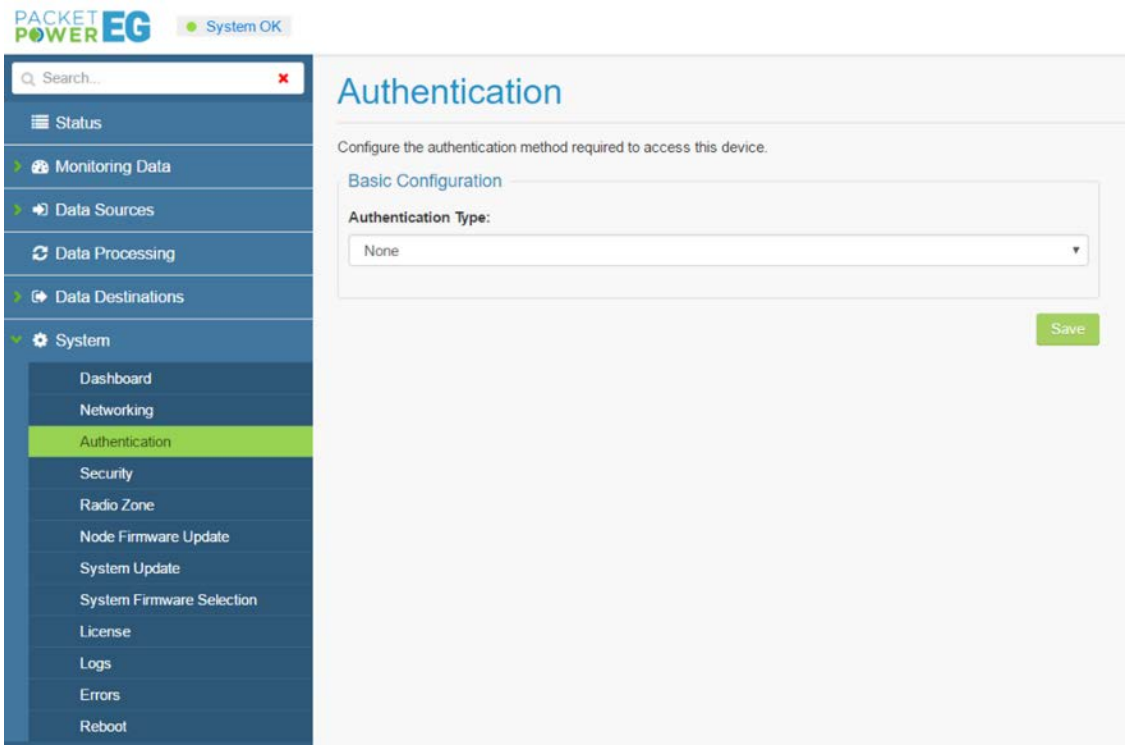
Networking

The Networking tab allows for the input of network settings. See the Network Configuration section for a detailed explanation.



Authentication

Configure your desired method of authenticating user access to the Gateway. Several options exist including "None".



Security

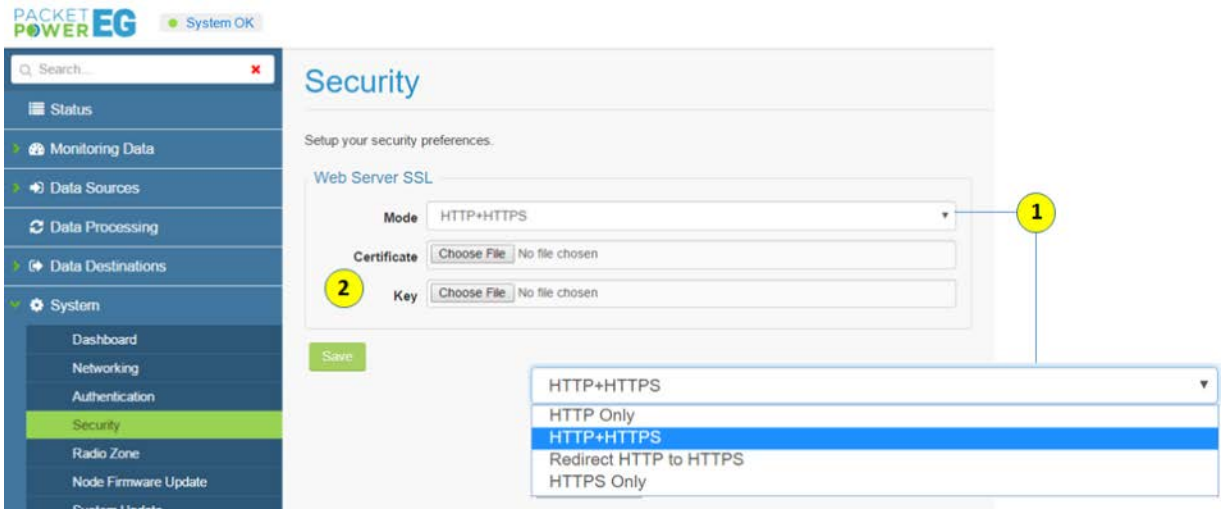
The Security tab provides access to additional network security features for the Gateway allowing for the use of HTTPS and SSL protocol with security certificates.

The default exchange protocol is HTTP Only. This can be upgraded to a SSL protocol using one of the three other optional settings by selecting from the "Mode" drop down menu (1)

- HTTP Only (no SSL)
- HTTP + HTTPS
- Redirect HTTP to HTTPS
- HTTPS Only

After selecting an enhanced SSL protocol it is necessary to enter the "Certificate" and "Key" files (2) for the related protocols.

Once the data has been entered click the "Save" button to implement.

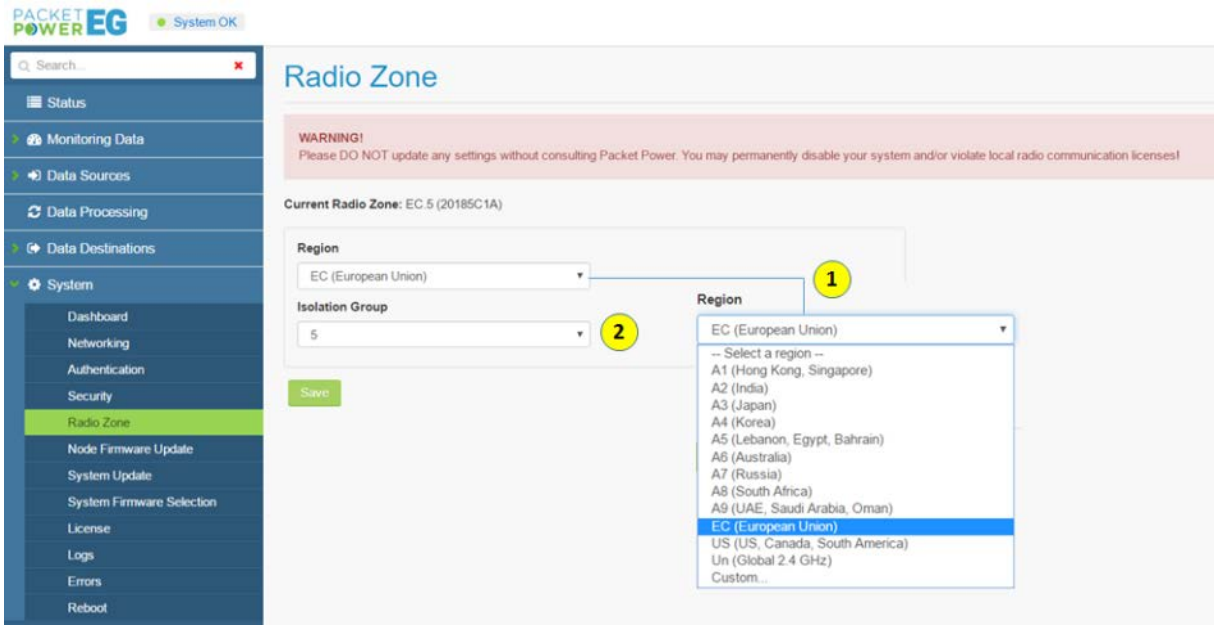


Additional security options are available. Consult Hubbell for details.

Radio Zone

WARNING: DO NOT update any Radio Zone settings without consulting Hubbell. You may permanently disable your system and/or violate local radio communication licenses!

Hubbell Gateways and monitors are capable of transmitting on both the 900 MHz and 2.4 GHz bands in the ISM spectrum along with segregated channels within these bandwidths. Depending on geographic region or country there are specific bandwidths required. This is defined by the "Region" (1) setting in the Radio Zone configuration.



Radio Isolation / Isolation Group

In many cases there is a requirement to "radio isolate" or segregate specific Gateways and monitors from other Gateways and monitors sharing radio proximity. This is achieved by designating a specific group of Gateway and monitors to an "Isolation Group" (2). Note that both the Gateway and nodes must share the same radio isolation group for successful communication. Modification of radio isolation groups should only be done with guidance from Hubbell.

Node Firmware Update

The Node Firmware Update feature allows the Gateway to wirelessly broadcast firmware updates to all monitoring nodes communicating with a given Gateway. This is an inherently safe feature since firmware is transmitted redundantly over time and is not actually deployed until a complete image has been received and verified to be correct. Due to the variability of the radio connections and network load, firmware updates may take from a few hours to a day, depending on the size of the network. During the update process the monitors will continue to function normally. When completed, the monitors will automatically reboot and switch to new firmware.

Note that different monitoring node types use different firmware images. In a firmware version designation the first number (e.g. "5" in 5.28) denotes node type and the second number (i.e. "28") denotes the firmware version. Nodes of a given type will only receive firmware images of the matching type. If multiple firmware images need to be upgraded (e.g. upgrading 5.28 to 5.29 and 23.12 to 23.14), upgrades have to be done sequentially (initiate one upgrade, wait for it to complete, then initiate the next upgrade).

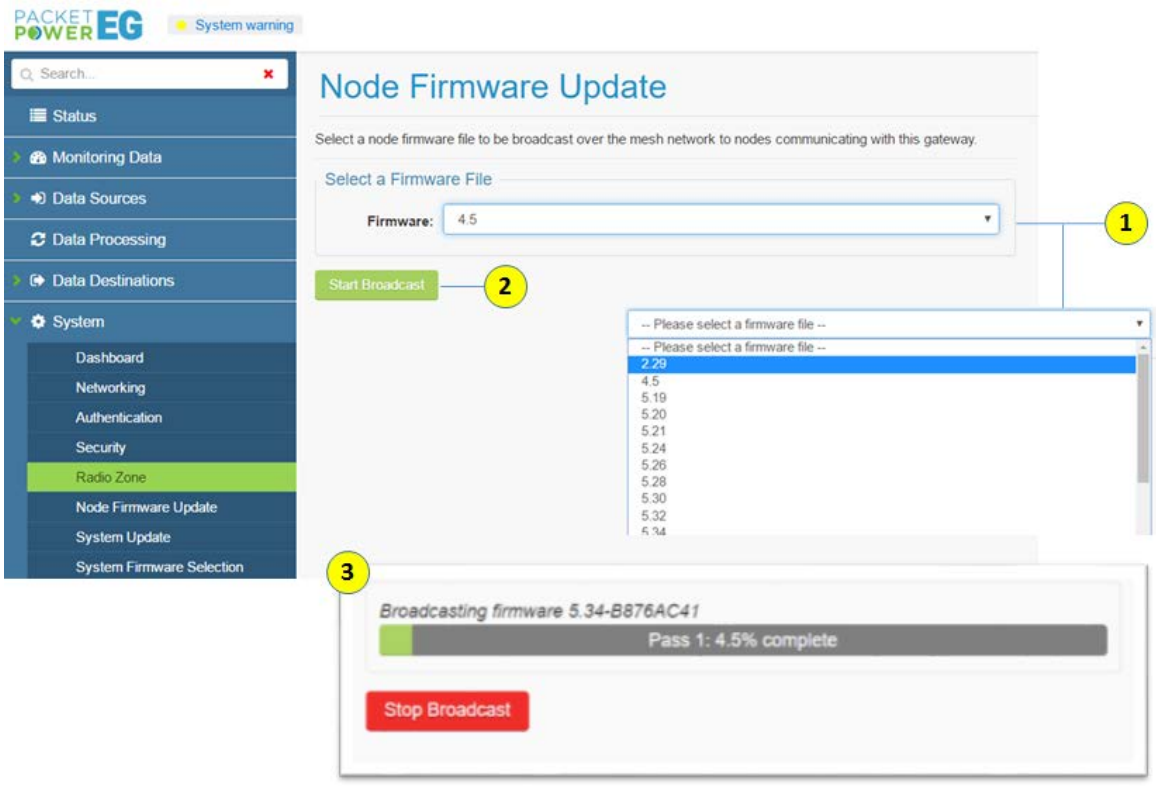
Updating firmware on monitoring nodes:

1. Select the appropriate firmware version from the "Firmware" drop down menu (1). A list of firmware updates can be found here.
2. Click the "Start Broadcast" button (2)

The progress of the update will be shown on a bar chart (3). The update transmission may be terminated at any time by clicking on the "Stop Broadcast" button.

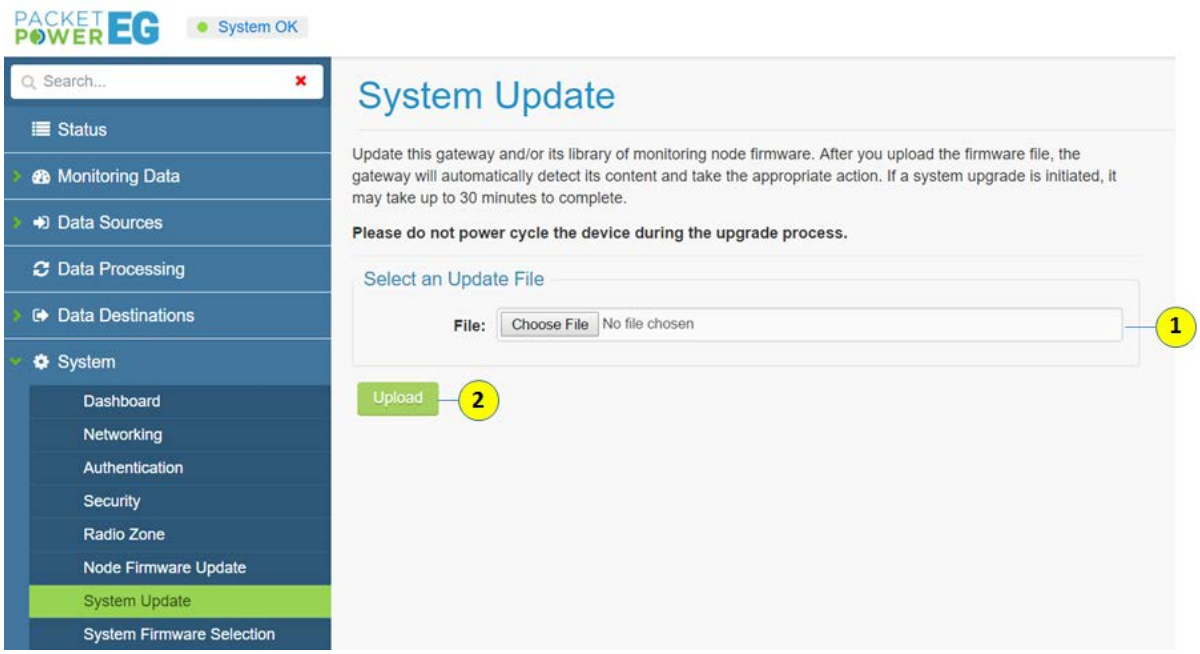
Note that a node firmware update may take a long time. During the uploading process the node will be fully operational using the existing firmware. Once the upload is complete the node will automatically reboot and revive with the newer firmware version. The node may be offline for a very short time during the reboot process.

In the event that a firmware upload is interrupted, it will resume at its last position without losing the initial data uploads. The upload status can also be viewed on the main Gateway Console screen next to the "System Status" indicator.



System Update (Update Firmware on Gateway)

The System Update feature provides the latest Gateway firmware along with an updated library of monitoring node firmware. After the firmware file is uploaded, the Gateway will automatically detect its content and automatically integrate the new firmware.



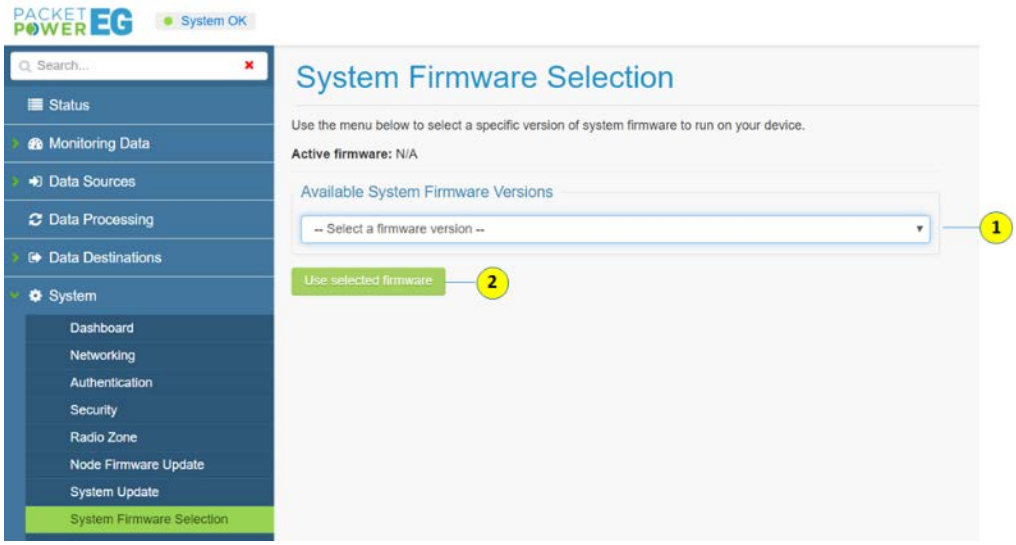
To initiate a system update:

1. Select an "Update File" by clicking the "Choose File" button (1). Update files are provided from Hubbell.
2. Click the "Upload" button (2).

The system upgrade may take upwards of 30 minutes.

System Firmware Selection

The System Firmware Selection tab allows users to implement alternate versions of firmware residing on the Gateway. The firmware must be loaded onto the Gateway using the "System Update" feature.



To change a Gateway firmware operation version:

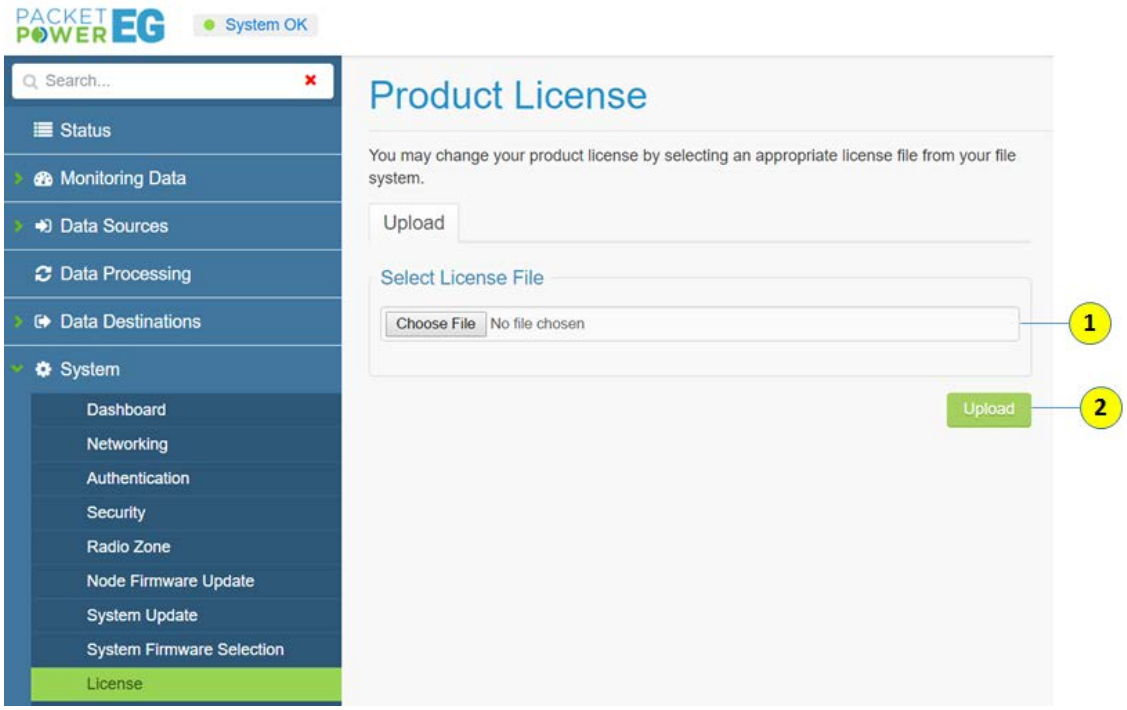
1. Select a firmware version from the "Available System Firmware Versions" drop down menu (1).
2. Click on "Use selected firmware" button (2).

Note that the exchange process may require a reboot in some cases.

License

Various features of the Gateway will require a separate product license. These licenses can be implemented by uploading the license file provided by Hubbell or an authorized partner. Licensed features include:

- SNMP
- Modbus
- Virtual Panel Mapping
- Gateway Capacity (limited versus standard)
- Monitor Mode



To implement a product license:

1. Select the license file by clicking on the "choose file" button under "Select License File" (1).
2. Click on the "Upload" button.
3. A reboot of the device will be required to make the license effective.

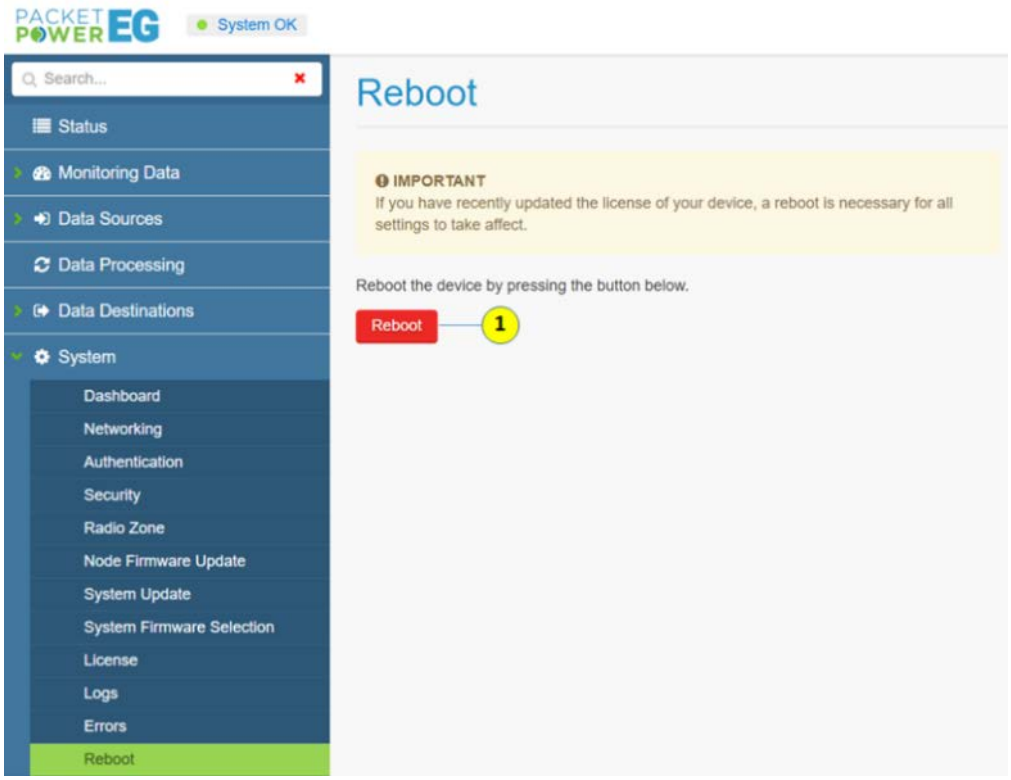
Reboot

In some cases the Gateway may require "rebooting". To reboot the Gateway:

1. Select the "Reboot" tab from the left menu.
2. Click the red "Reboot" button (1).

The Gateway will go offline and will reboot and reconnect to the network and all monitoring nodes once the reboot process is finished. This does not erase any configuration settings.

WARNING: Monitoring data will not be gathered from the nodes during a Gateway reboot unless there is a redundant Gateway that can assume the network traffic.

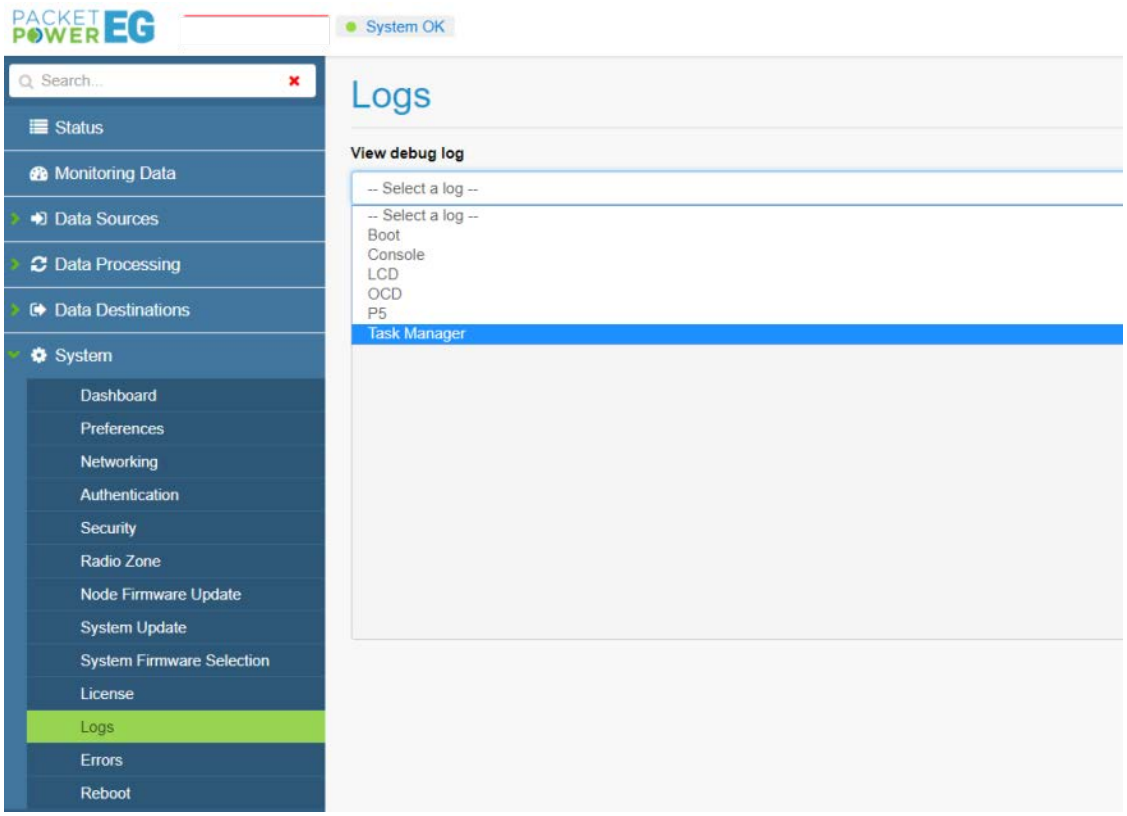


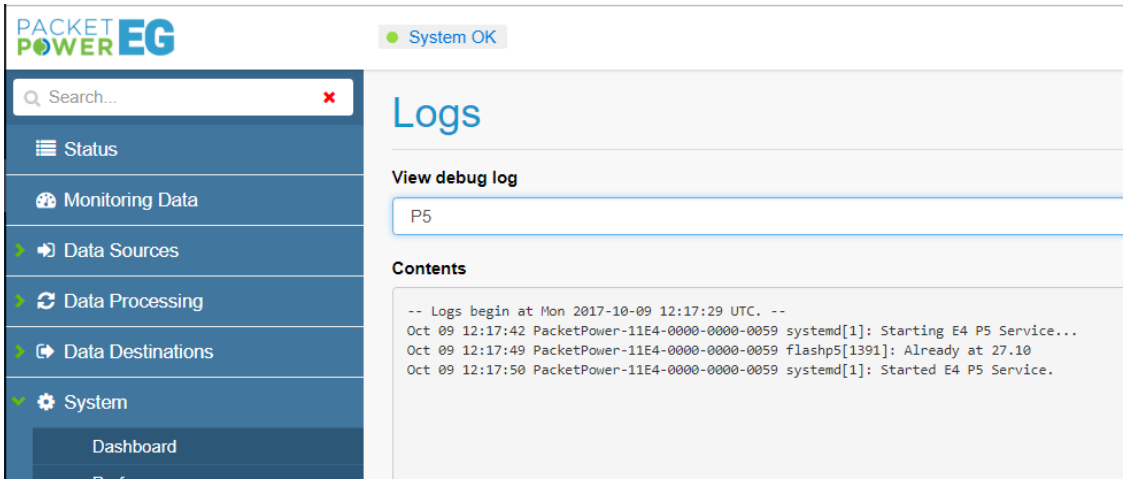
Logs

Logs provide critical operational details relating to the Gateway operation. They are retrieved for debugging purposes and used strictly by Hubbell engineers.

To obtain a log file:

1. Select the [Logs] tab from the [System] menu on the right hand task bar.
2. Select the log to be accessed under the "View debug log" menu. The log file will then appear in the dialog box where it can be copied and pasted as required. Note that there are six unique logs: Boot, Console, LCD, OCD, P5, and Task Manager.


PACKET POWER EG
System OK
Search...
Status
Monitoring Data
Data Sources
Data Processing
Data Destinations
System
Dashboard
Preferences
Networking
Authentication
Security
Radio Zone
Node Firmware Update
System Update
System Firmware Selection
License
Logs
Errors
Reboot
Logs
View debug log
-- Select a log --
-- Select a log --
Boot
Console
LCD
OCD
P5
Task Manager


PACKET POWER EG
System OK
Search...
Status
Monitoring Data
Data Sources
Data Processing
Data Destinations
System
Dashboard
Logs
View debug log
P5
Contents
-- Logs begin at Mon 2017-10-09 12:17:29 UTC. --
Oct 09 12:17:42 PacketPower-11E4-0000-0000-0059 systemd[1]: Starting E4 P5 Service...
Oct 09 12:17:49 PacketPower-11E4-0000-0000-0059 flashp5[1391]: Already at 27.10
Oct 09 12:17:50 PacketPower-11E4-0000-0000-0059 systemd[1]: Started E4 P5 Service.

Firmware Upgrades

The Ethernet Gateway Version 4 provides a means of performing firmware upgrades to both itself and to most Hubbell wireless monitoring units. Upgrades are performed via the "System" page of the web console. Detailed instructions can be found in the Web Console - System section.

SNMP Implementation

The following are step-by-step instructions for implementing SNMP using the Ethernet Gateway Version 4. These instructions are intended for SNMP versions 1 and 2. The Version 4 Gateway does support version 3 SNMP. For details on version 3 implementation please contact techserv@hubbell.com.

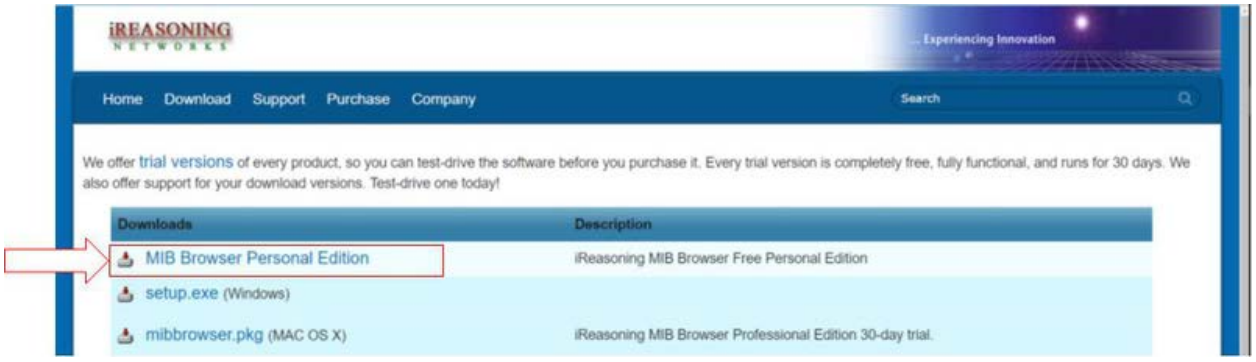
Required Files and Tools

MIB Files: MIB files can be downloaded directly on the Gateway or from the links below
General MIB File (click to download)
MIB file for use with VIPs (Virtual IP addressing) (click to download)
iReasoning Browser: iREasoning MIB Browser is a utility that allows you to view MIB files.

Data Output from SNMP Gateways

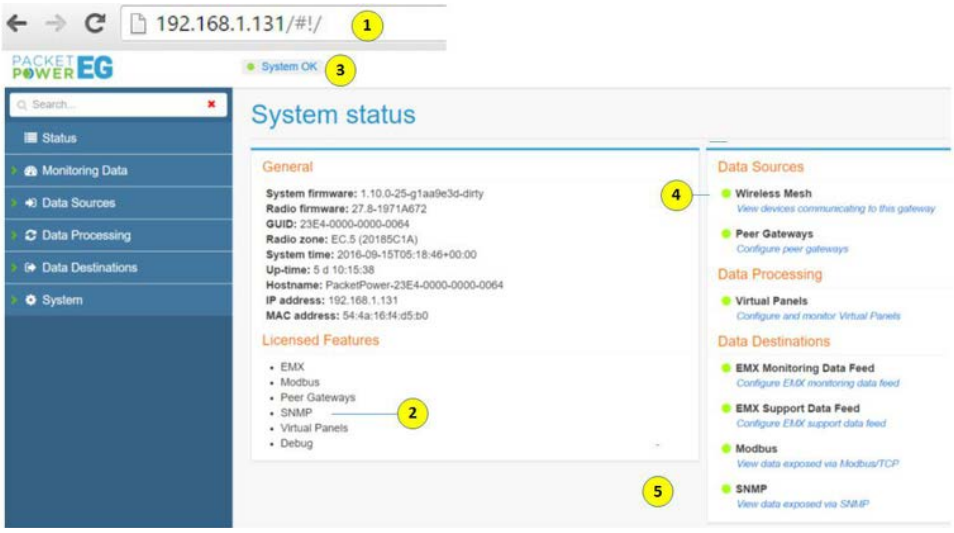
Requirements

- Download iREasoning MIB Browser (http://www.ireasoning.com/download.shtml)



- The Gateway is configured and communicating with the wireless nodes
- The Gateway has a license for SNMP

Accessing the Gateway Console



Make sure your Gateway is configured with an IP address and accessible on your network. The Gateway must be connected to a switch /router on an accessible network.
It may not be accessible directly through a PC Ethernet to Gateway connection. For Gateway network configuration instructions follow this link.

(1) Enter the IP address of the Gateway on any browser to access the Gateway Console

(2) Make sure SNMP is listed as a licensed feature. If not see the licensing section on how to add a license

(3) Make sure that the system is communicating properly with the monitoring nodes as indicated by a green status light

(4) Click the link under Wireless Mesh to see monitoring nodes that are currently communicating with the Gateway

(5) SNMP Data will be able to be viewed through the SNMP data link; this light will be green once the SNMP agent is enabled

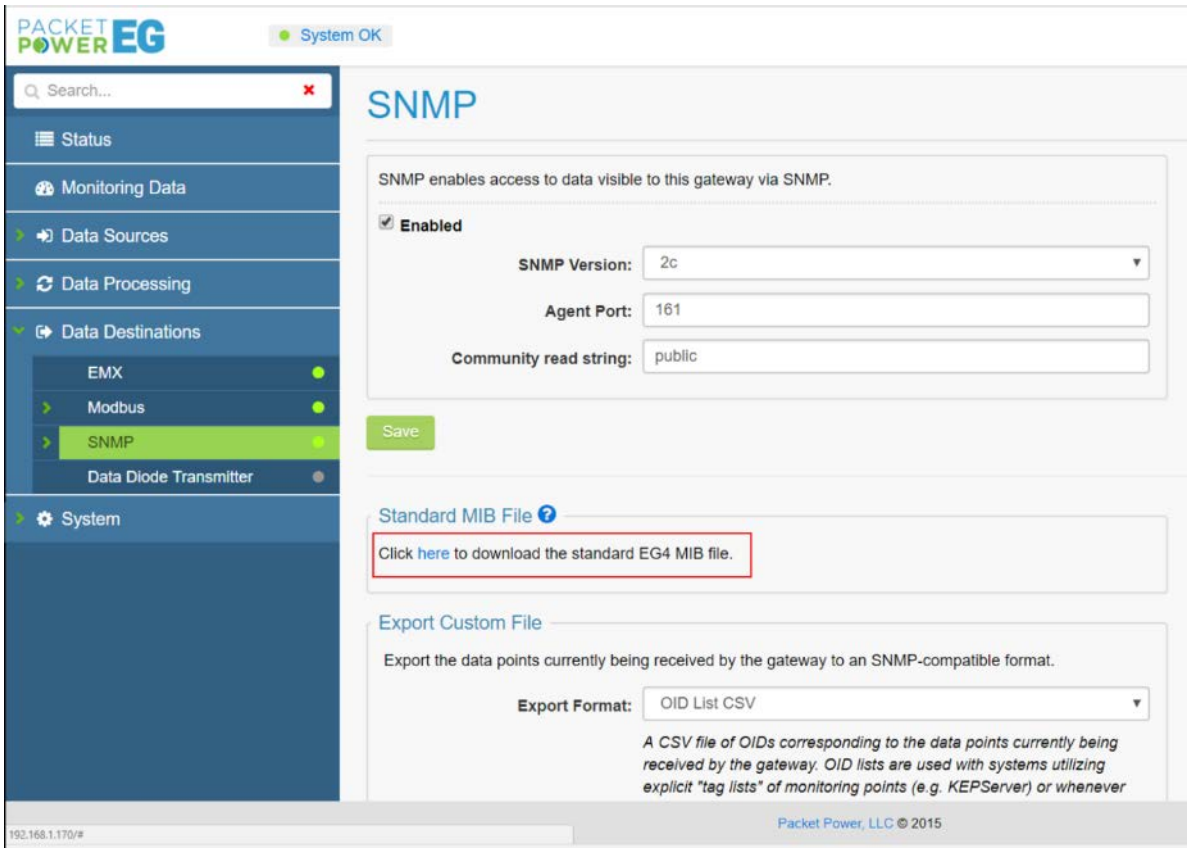
Accessing the MIB files from Gateway Console

MIB files can be downloaded directly from the Gateway Console. There are two MIB files. The standard EG4 file is for use in standard SNMP applications. The VIP MIB file is used when using Virtual IP addresses for each monitoring node instead of the standard 16 digit GUID embedded in the OID.

If the link is not available on the console this may require that the Gateway firmware be upgraded to version 1.12 or higher.

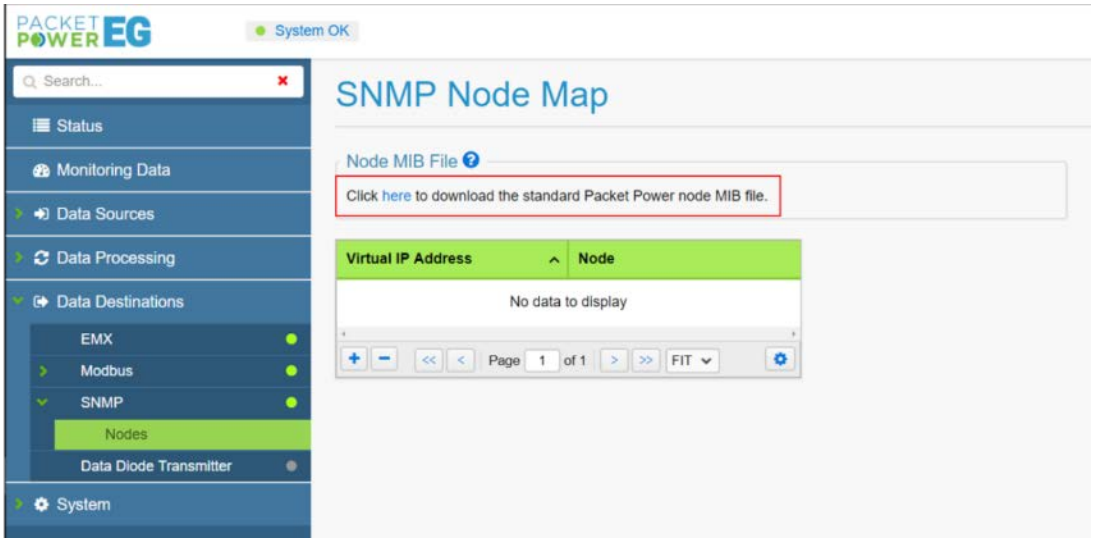
Downloading the standard MIB file

On the Gateway console go to Data Destinations>SNMP on the left menu and then click on the standard MIB file.



Downloading the MIB file for use with virtual IP addressing

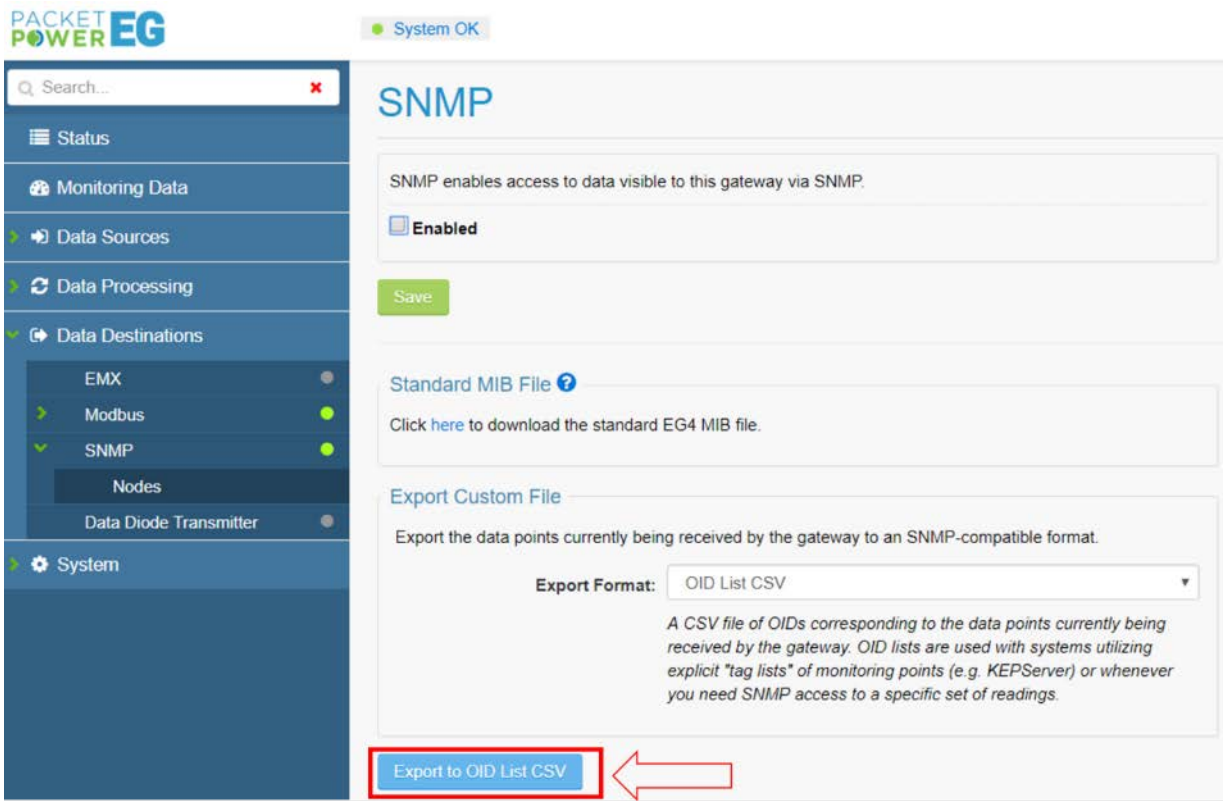
On the Gateway console go to Data Destinations>SNMP>Nodes on the left menu and then click to download the MIB file.



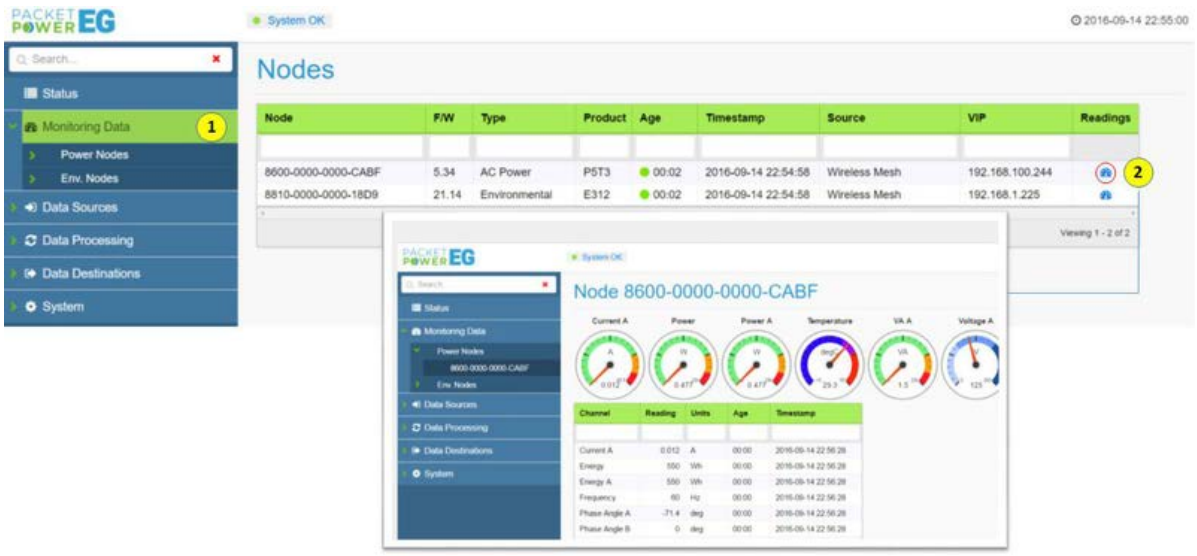
Accessing active OIDs

It is possible to download a CSV file that contains only the active data points being received by the Gateway in an SNMP compatible format. This will vary as nodes are added and removed from the system. OID lists are used with systems utilizing explicit "tag lists" of monitoring points (e.g. KEPServer) or whenever you need SNMP access to a specific set of readings.

To access the file go to the [Data Destinations] tab on the left menu and select [SNMP]. On the main screen select the button [Export OID List CSV]. This will download the OID



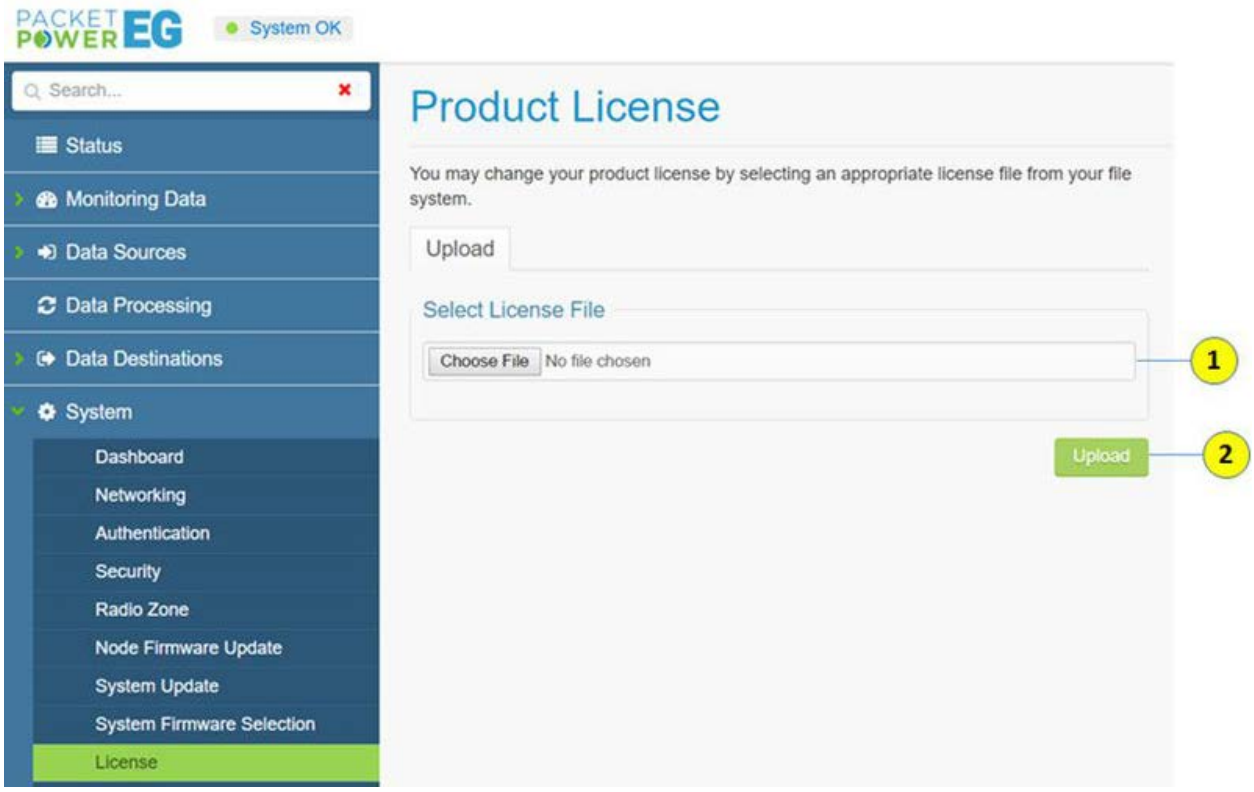
Viewing monitoring node readings on the Gateway Console



(1) Confirm that monitoring nodes are active and returning data to the Gateway by selecting the "Monitoring Data" tab; this will display all connected nodes

(2) Click on the "readings" icon to expose the real time readings for a specific monitoring node

Uploading an SNMP license to the Gateway



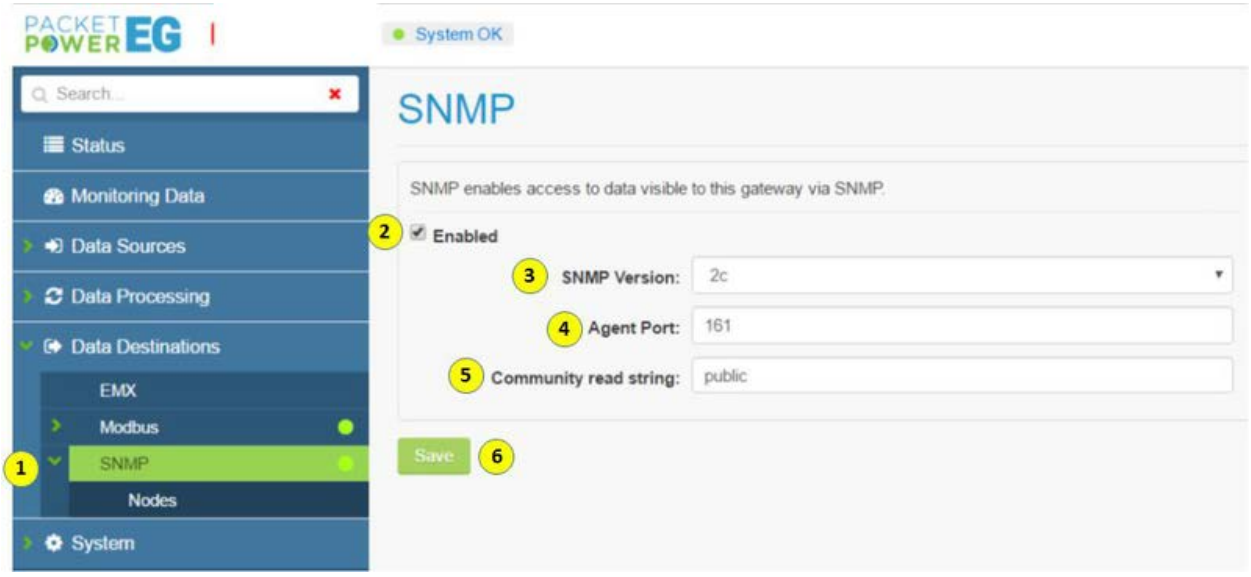
(1) To activate a product license, select the license file by clicking on the "choose file" button under "Select License File" in the "System" menu

(2) Click on the "Upload" button and point to the location of the license provided by Hubbell

A reboot of the device will be required to make the license effective. The reboot tab can be found under the "System" menu.

In the event that SNMP is not a licensed feature you will need to obtain a license from Hubbell techserv@hubbell.com.

Enabling and configuring the SNMP Agent



(1) Click on the SNMP tab under the Data Destinations tab

(2) Make sure SNMP is enabled in the check box

(3) Select the correct SNMP version. This guide is for SNMP V1 and V2; for SNMP V3 implementation see the SNMP 3 guide

(4) Set the Agent port to 161 or as needed

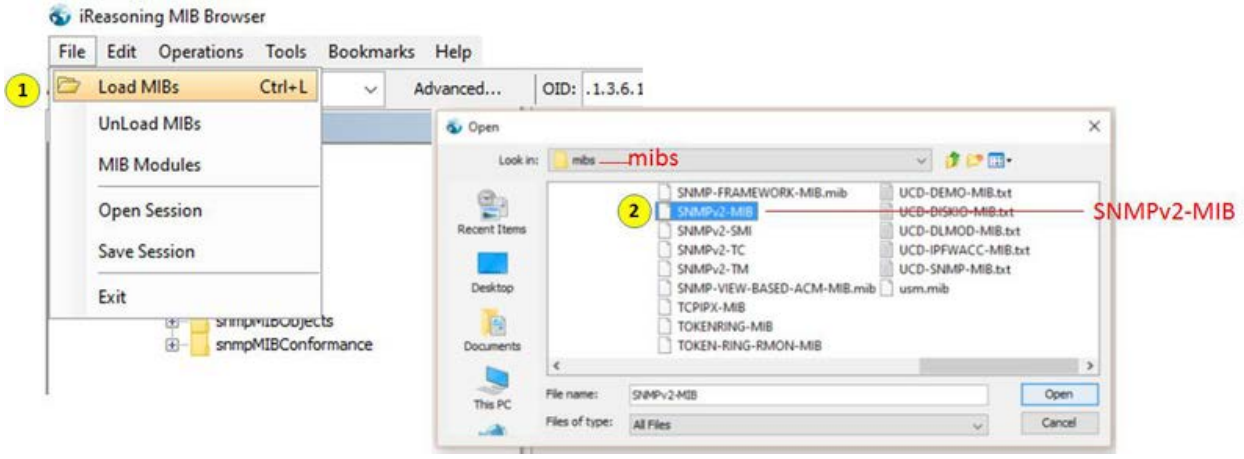
(5) The Community read string (used for authentication) should be "public"

(6) Click "Save" to save settings

(7) The SNMP status light in the left menu will be green indicating the onboard SNMP agent is active

Using the iReasoning MIB browser

Loading general MIB files on to the iReasoning browser

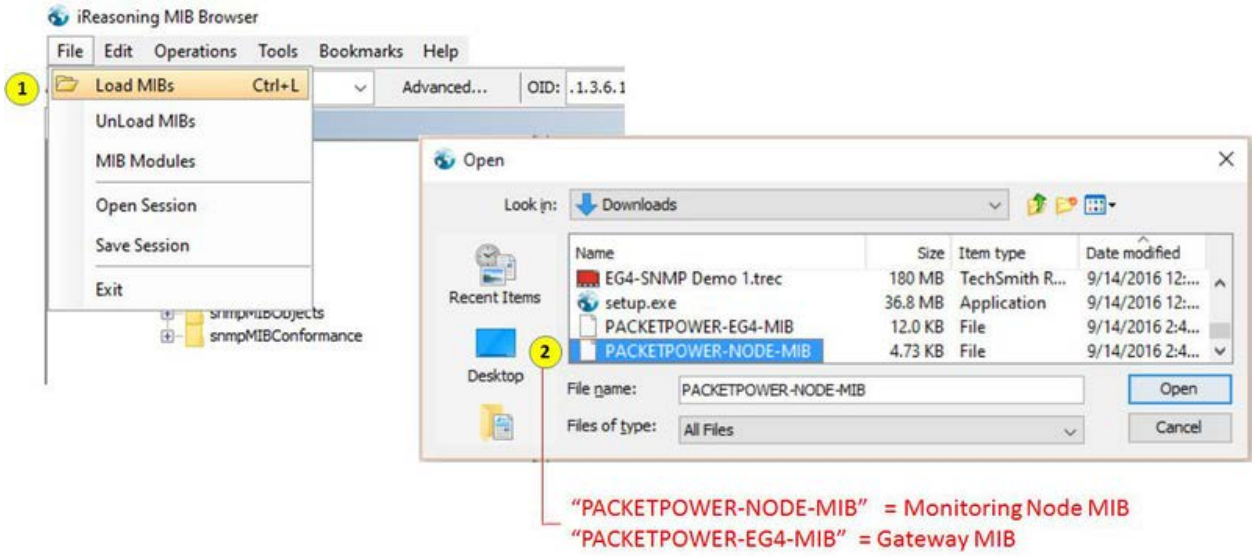


(1) Load the MIB for "General SNMP management" using the [Load MIBs] function under the [FILE] menu

(2) This is the "SNMPv2-MIB" file if using SNMP V2. For older SNMP versions use the appropriate MIB file supplied in the MIB directory.

This file will automatically be supplied with iReasoning in the "mibs" directory.

Loading Gateway and node MIB files on to the iReasoning browser

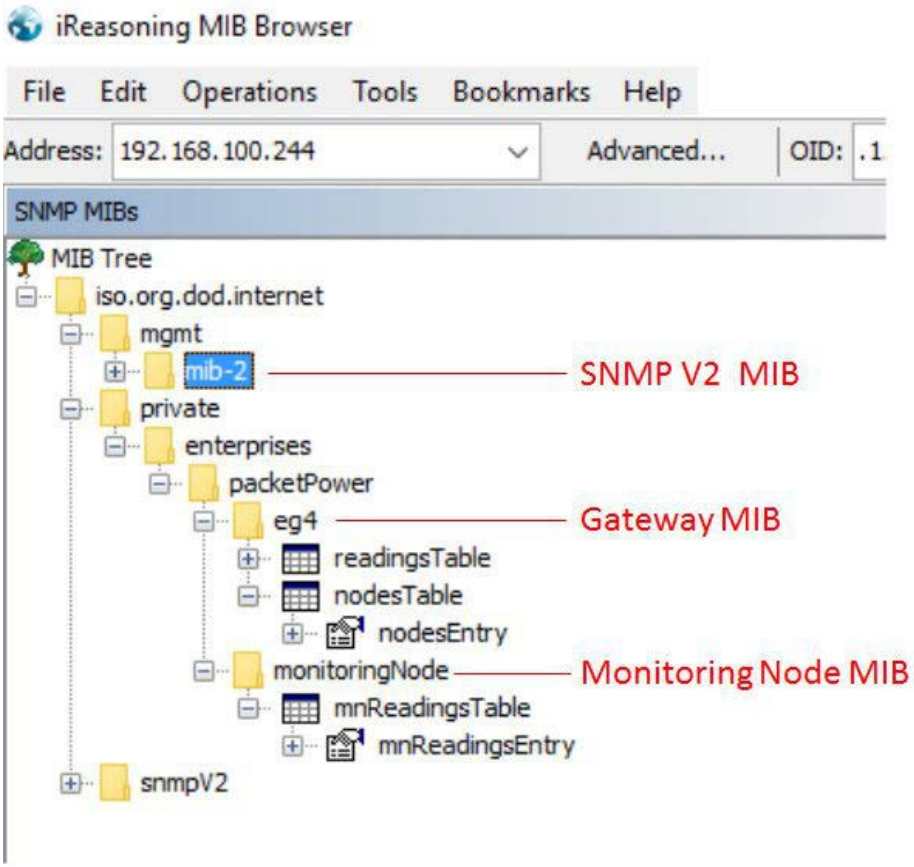


(1) Load the MIB for Gateway and monitoring nodes using the [Load MIBs] function under the [FILE] menu

(2) PACKETPOWER-EG4-MIB is for the Gateway and PACKETPOWER-NODE-MIB is for the monitoring nodes

Download these MIB files.

Accessing MIB files on the iReasoning Browser

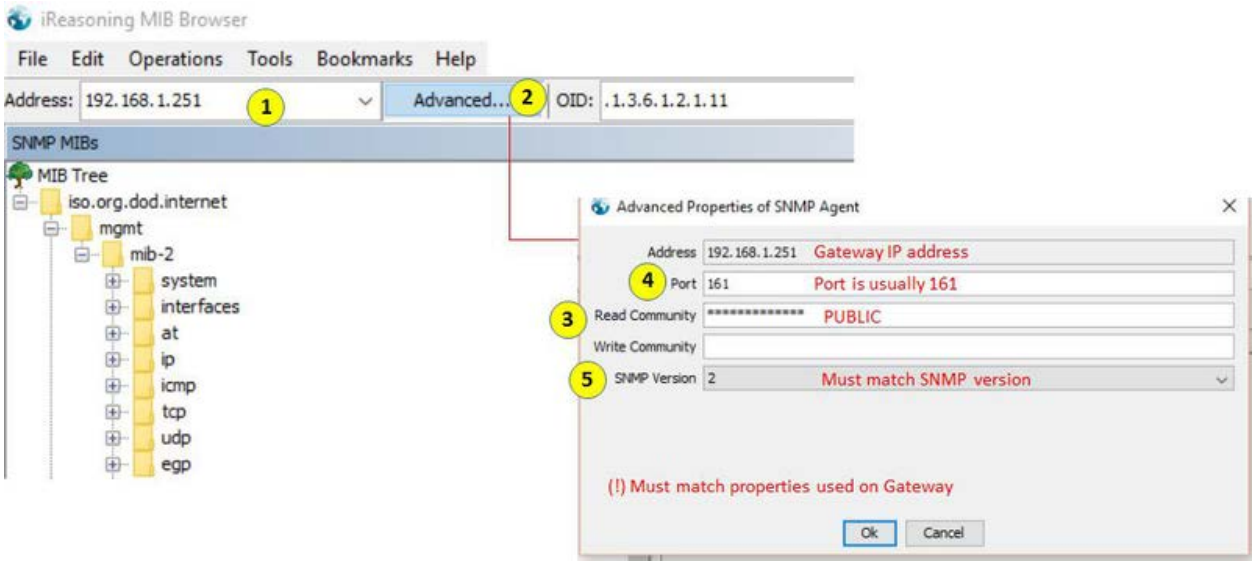


The SNMP management MIB can be found under the "mgmt." file of the MIB tree

The Gateway MIB file can be found under the "eg4" directory under the "private" directory

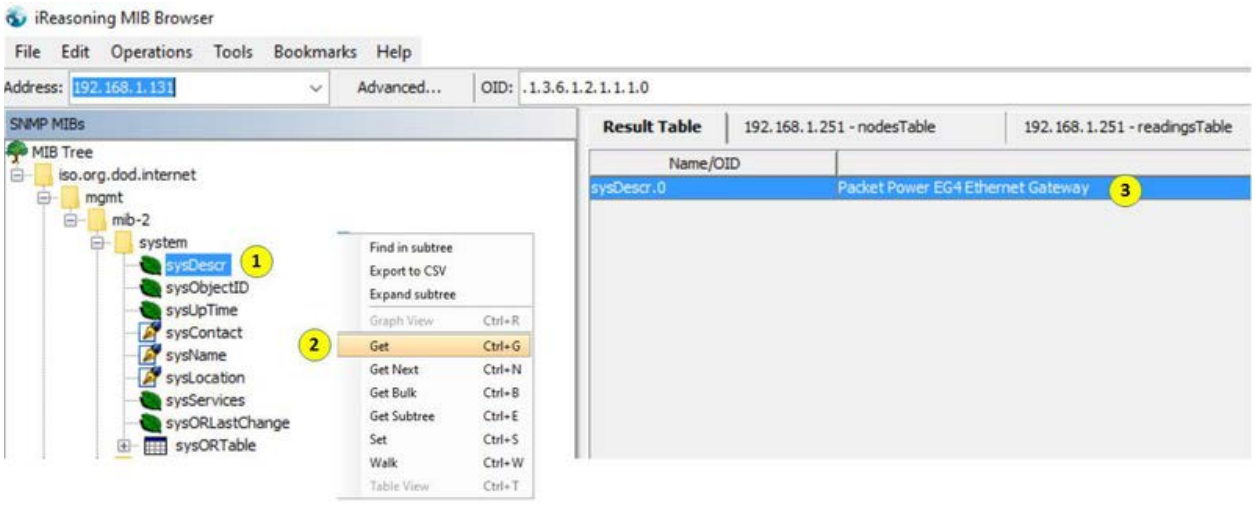
The monitoring nodes MIB file can be found under the "monitoringNode" directory under the "private" directory

Accessing the Gateway using the iReasoning browser



(1) Enter the IP address of the Gateway in the address bar
(2) Click on the "Advanced" tab
(3) Make sure SNMP is configured for the same read community string (public)
(4) Confirm port is correct (161)
(5) Confirm that the SNMP version matches the settings used on the Gateway Console SNMP settings (i.e. SNMP version)
Leave "Write Community" blank

Confirming communication with the Gateway

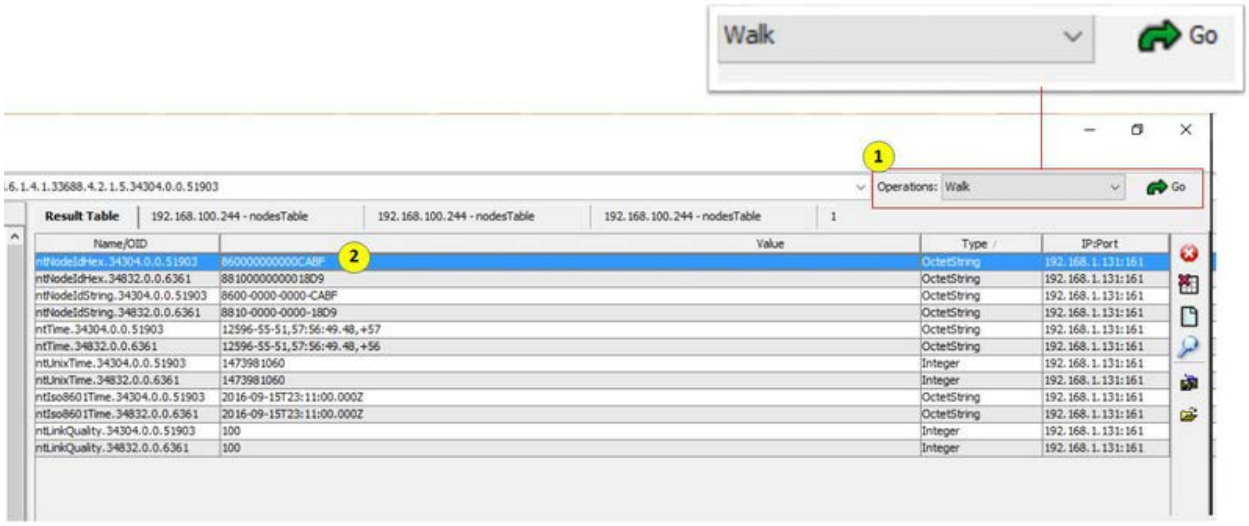


(1) Check the system description by clicking on the the "SysDescr" file on the MIB tree mgmt.>mib-2> SysDescr

(2) Right click on the sysDescr file and and select "Get" from the pop up menu

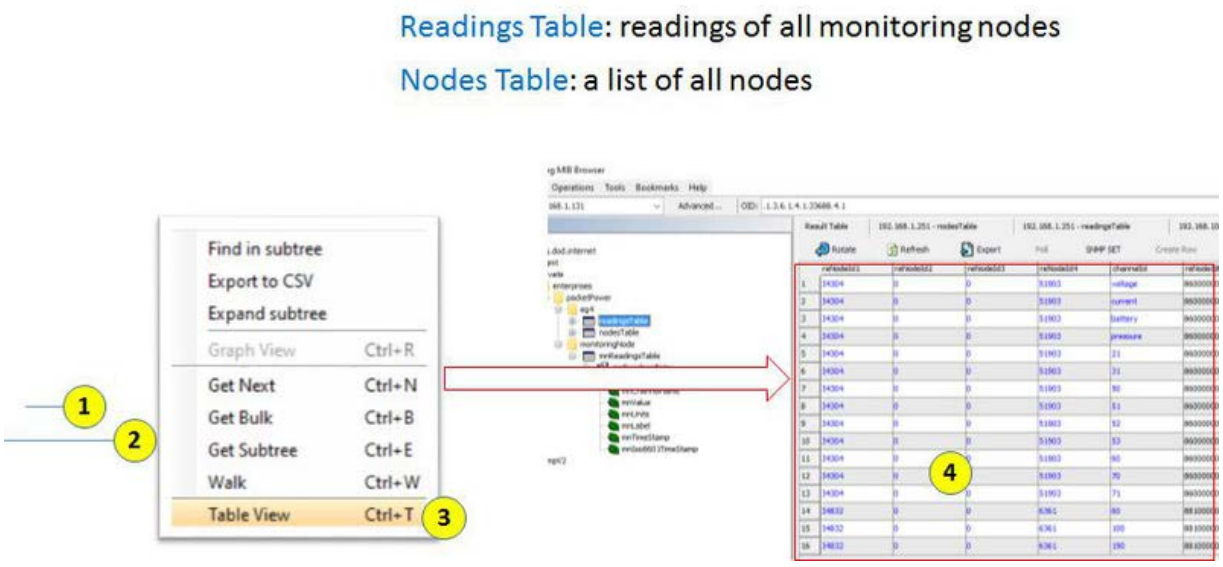
(3) The right hand menu should now display "Hubbell EG4 Ethernet Gateway"

Performing an SNMP "Walk" to confirm data flow



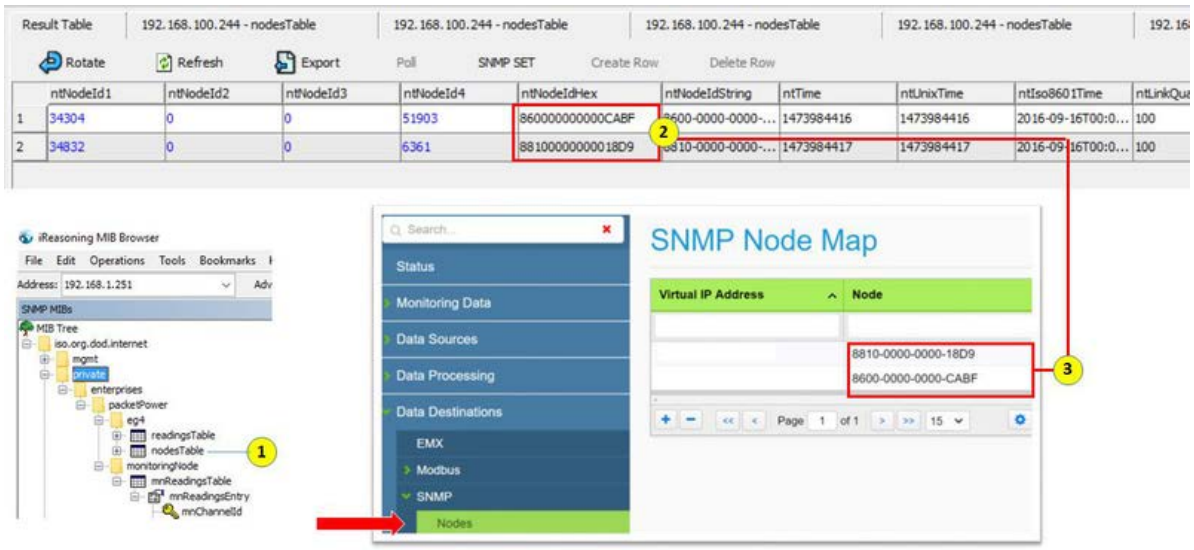
(1) Click "Walk" on the Operations bar and then click "Go"; a table will be generated returning all MIBs
Note that Windows firewall may have to be turned "off" for proper communications
(2) Node "GUIDs" will be displayed in the table; these node IDs will correspond to the Node IDs on the Gateway Console
To see the data in a more structured format use "Table View"

Generating readings tables and nodes tables (Table View)



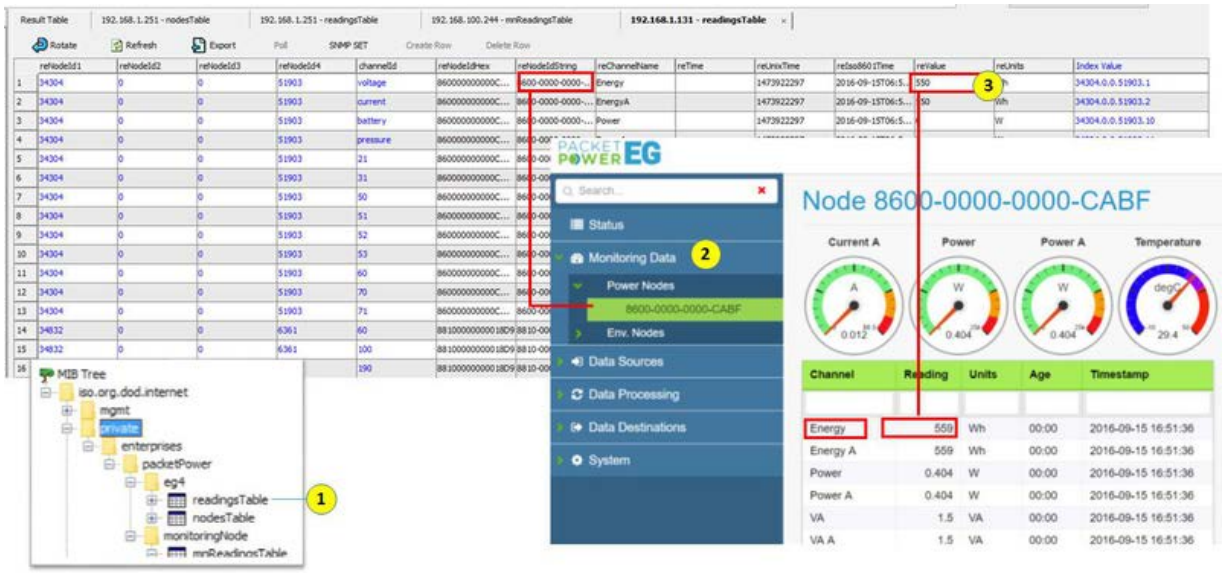
(1) (2) To get data in a more structured format select the "readingsTable" or "nodesTable" under the EG4 directory [private>packetPower]
(3) Right click and select "Table View"
(4) The table will appear in the right window

Node Tables / Node Map



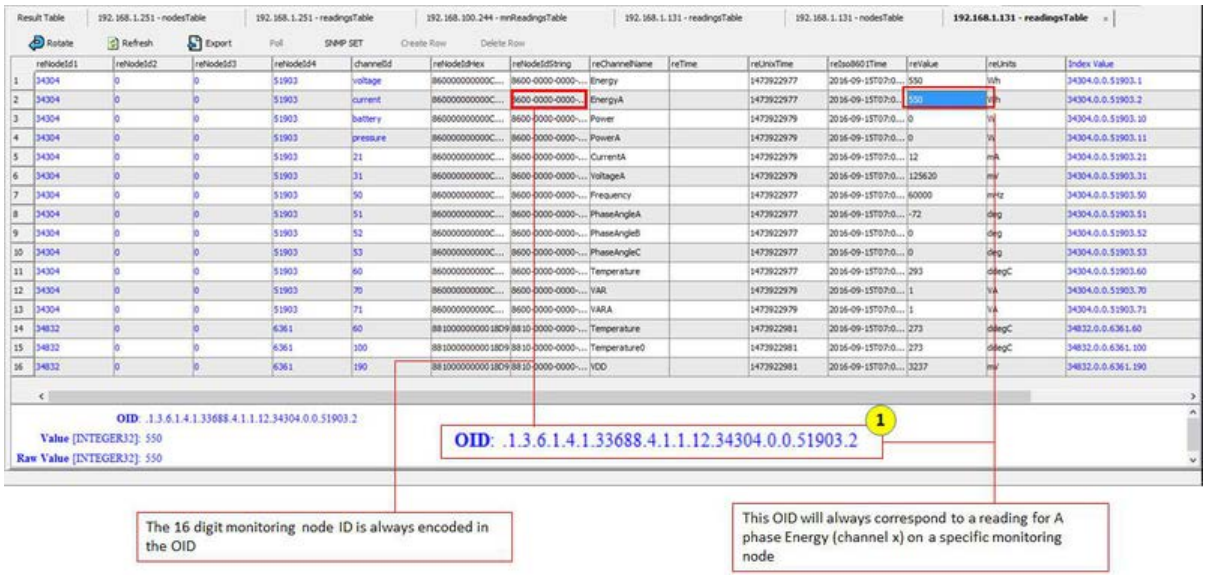
(1) After performing a "TableView" on "Nodes Table" by selecting the "nodesTable" file, right click and select table view, it will reveal a listing of all nodes associated with the Gateway
(2) Node "GUIDs" will be displayed in the table
(3) These node IDs will correspond to the Node IDs on the Gateway Console accessed by selecting Data Destinations > SNMP > Nodes

Readings Table / Readings for all Nodes



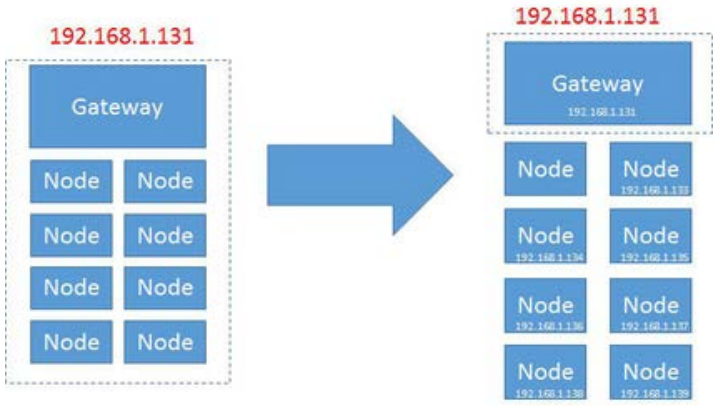
(1) Performing a "TableView" on "Readings Table" by selecting the "readingsTable" file, right click and select [Table View] from the pop up menu, it will reveal a listing of all readings for all nodes associated with the Gateway
(2) Node IDs will correspond to the node readings on the Gateway Console accessed by selecting the Monitoring Data menu and highlighting the corresponding node
(3) Values from the Gateway Console will match those on the Readings Table
All readings share a common table until a virtual IP address can be defined per node allowing nodes to be segregated by IP address

Interpreting Readings Data from Table View



(1) The 16 digit node ID (GUID) that identifies each Hubbell device (node) is encoded within the OID
Clicking on a reading will allow you to associate it with a specific node ID via the OID
Any reading OID will always correspond to a specific channel for specific node (ie. energy on phase A for a particular node)

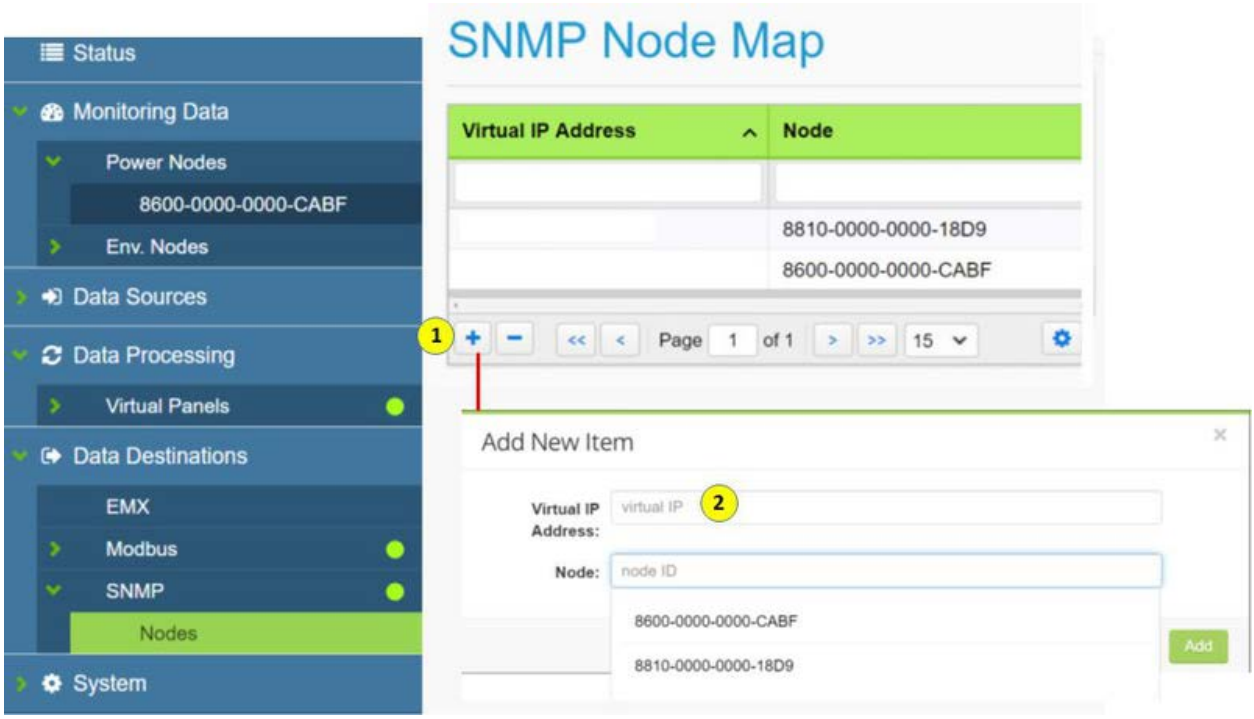
Virtual IP addressing / Assigning Virtual IPs to monitoring nodes



Monitoring nodes and the Gateway will show up under a single IP address. Many monitoring systems using SNMP require that each device / node have a unique IP address.

It is possible to assign a Virtual IP address to each monitoring node using the Gateway Console. This will segregate the nodes so they can be revealed individually.

Assigning Virtual IPs to monitoring nodes

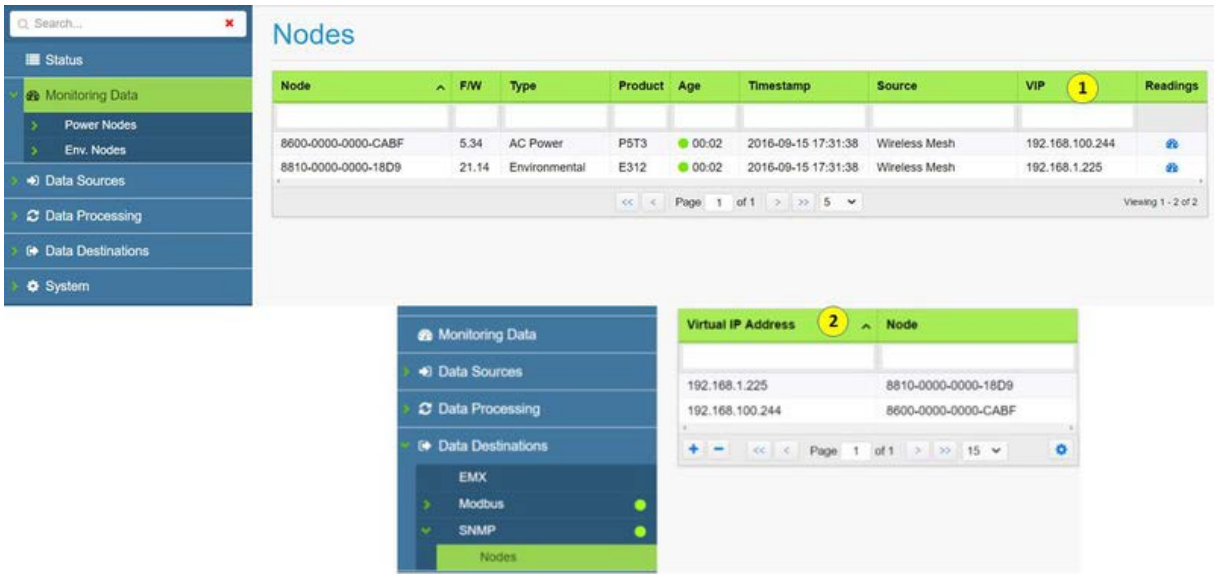


To apply a Virtual IP address to a specific node open the Gateway Console and select "SNMP" under the "Data Destinations" menu, then select the "Nodes" menu. This will expose all of the nodes for the Gateway

(1) Click on the "+" icon to reveal the Virtual IP addressing pop-up
(2) Select the Node to be addressed using the drop down "Node" menu (nodes are identified by their 16 digit GUID)
Enter a virtual IP address; this must be valid within the network its being used on
Click "Add" to save

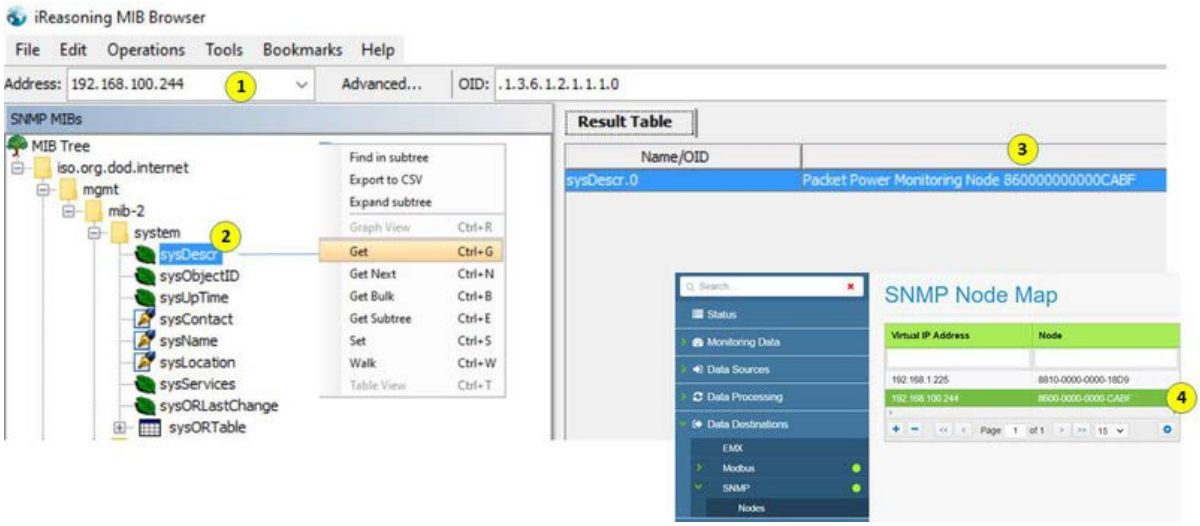
Repeat for all nodes.

Viewing nodes by Virtual IP address on Gateway Console

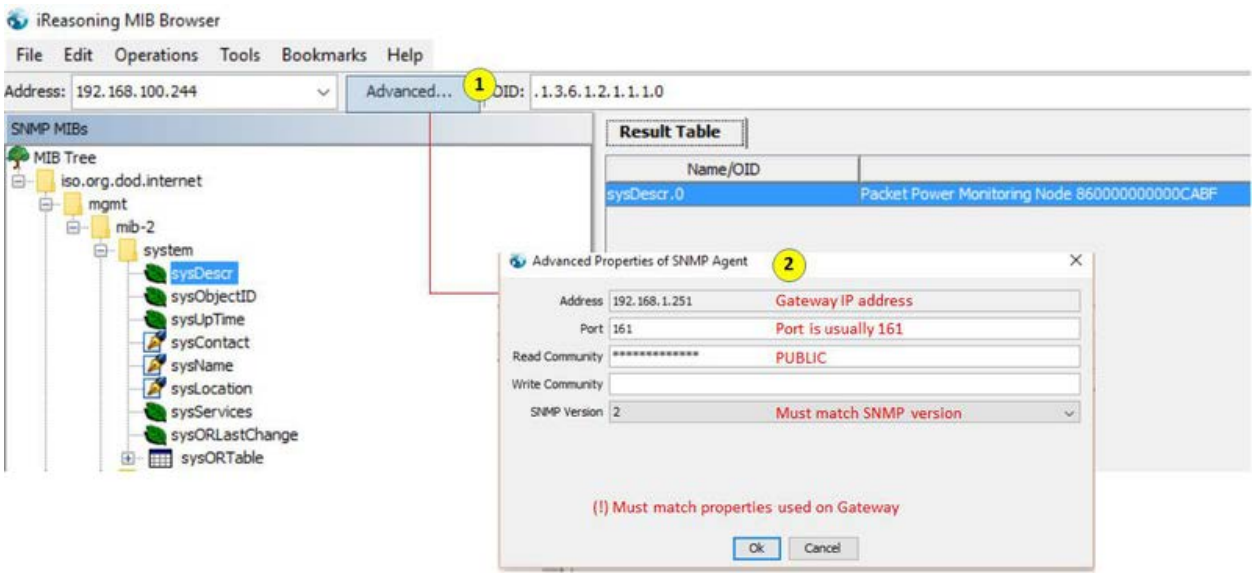


(1) Each node will now have a VIP (virtual IP) as well as 16 digit GUID
(2) These can be found on the "Monitoring Data" tab of the Gateway Console or the "Node" tab under the "SNMP" tab in the "Data Destinations" menu
IPs will become visible at the same port as the Ethernet Gateway
The Gateway will have a unique IP and agent and each node will have a unique IP and agent

Viewing nodes by Virtual IP address on iReasoning Browser



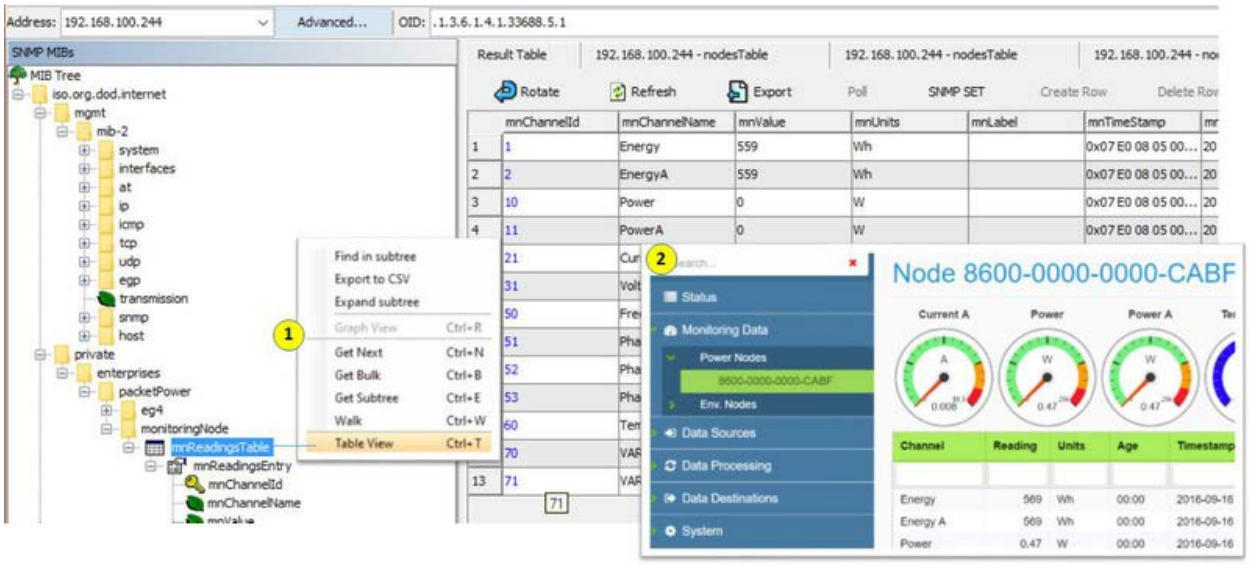
(1) Enter VIP in the address tab
(2) Go to "SysDescr" file in the MIB tree (under the mgmt.>mib-2>system folders) and right click for a "Get"
(3) The monitoring node's ID will be returned on the table to the right
(4) This corresponds with the VIP and GUID in the Gateway Console for the specific node



(1) and (2) Note that after a new IP address is entered it may be necessary to click on the "Advanced" tab and re-enter the properties of the SNMP agent for each unique IP address.

THIS IS ONLY WHEN USING the iReasoning browser tool to view different IP addresses.

Viewing node Readings by Virtual IP address on iReasoning Browser



(1) Using the same VIP for the particular node in the IP Address bar, highlight the "mnReadings" Table MIB under "monitoringNode" file.

Right click and select "Table View"; this will expose the readings table for the specific monitoring node in the table view

(2) These readings correspond to those on the Gateway Console; access the "Monitoring Data" menu and select the same node

Result Table | 192.168.1.251 - nodesTable | 192.168.1.251 - readingsTable | **192.168.100.244 - mnReadingsTable**

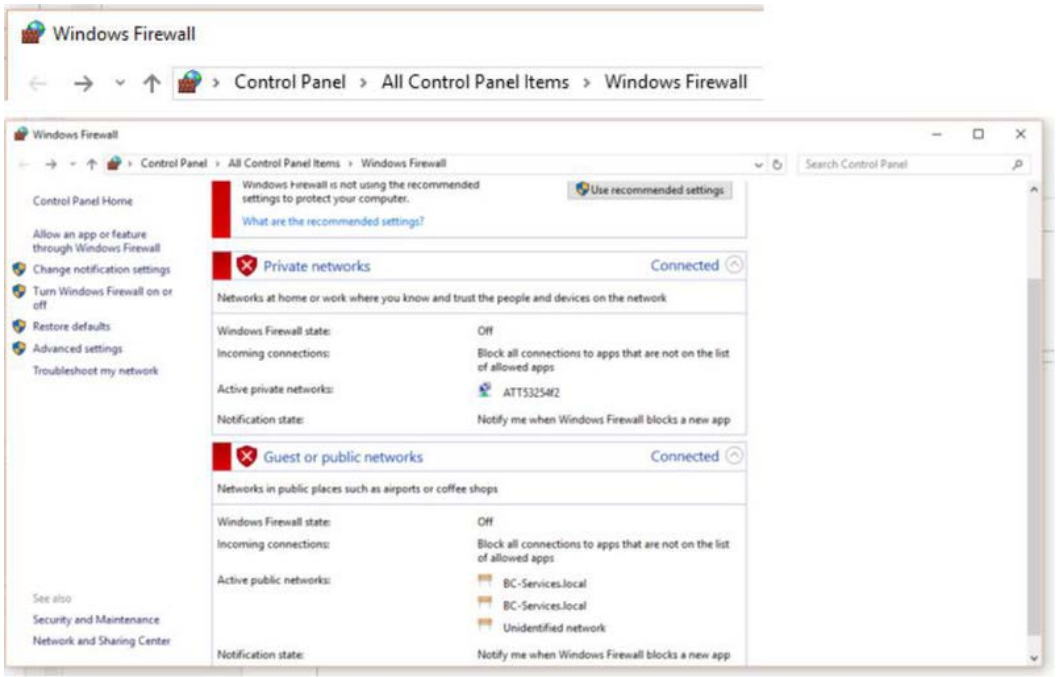
Rotate | Refresh | Export | Poll | SNMP SET | Create Row | Delete Row

	mnChannelId	mnChannelName	mnValue	mnUnits	mnLabel	mnTimeStamp	mnIso8601Tim...	Index Value
1	1	Energy	549	Wh		0x07 E0 08 04 04...	2016-09-15T04:0...	1
2	2	EnergyA	549	Wh		0x07 E0 08 04 04...	2016-09-15T04:0...	2
3	10	Power	0	W		0x07 E0 08 04 04...	2016-09-15T04:0...	10
4	11	PowerA	0	W		0x07 E0 08 04 04...	2016-09-15T04:0...	11
5	21	CurrentA	12	mA		0x07 E0 08 04 04...	2016-09-15T04:0...	21
6	31	VoltageA	125234	mV		0x07 E0 08 04 04...	2016-09-15T04:0...	31
7	50	Frequency	59950	mHz		0x07 E0 08 04 04...	2016-09-15T04:0...	50
8	51	PhaseAngleA	-74	deg		0x07 E0 08 04 04...	2016-09-15T04:0...	51
9	52	PhaseAngleB	0	deg		0x07 E0 08 04 04...	2016-09-15T04:0...	52
10	53	PhaseAngleC	0	deg		0x07 E0 08 04 04...	2016-09-15T04:0...	53
11	60	Temperature	295	ddegC		0x07 E0 08 04 04...	2016-09-15T04:0...	60
12	70	VAR	1	VA		0x07 E0 08 04 04...	2016-09-15T04:0...	70
13	71	VAR	1	VA		0x07 E0 08 04 04...	2016-09-15T04:0...	71

Readings Definitions

mnChannel ID: Identical for all like monitoring devices
mnChannel Name: Describes the function of the channel, i.e., Energy for phase A
mnValue: Measurement value for the channel
mnUnits: Units of measurement, i.e., Watt hours
mnTime Stamp: Time when the value was received

Turning Windows Firewall "off"



Windows Firewall will block the iReasoning MIB browser from accessing other IP addresses such as virtual IP addresses.

To disable the Firewall (Windows 10) select control panel > all control panel items > windows firewall and turn the firewall off for both public and private networks. This does not have to be permanent – only during polling on this computer using iReasoning.

Modbus TCP/IP Implementation

NOTE: Modbus register maps are pre-loaded on Gateways with firmware versions 1.12.0 or higher. These register maps have static / pre-assigned register numbers. It is suggested that any Gateway (GW04) be upgraded to firmware version 1.12.0 or higher rather than importing register maps.

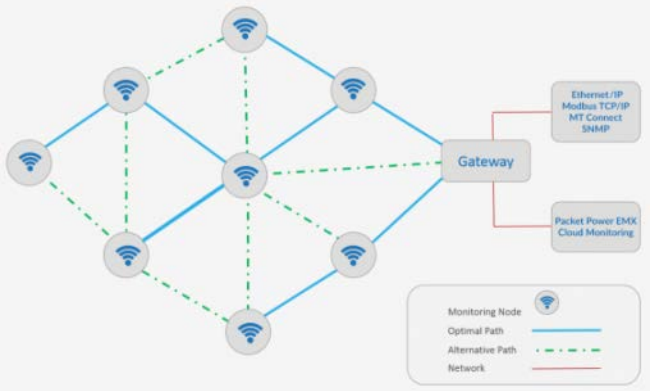
Legacy register maps may be download from the below links:

Modbus Register Map Download Modbus Register Map Definitions Modbus Reading Expression Syntax

Modbus Overview

The Ethernet Gateway Modbus interface makes all monitoring data received from Hubbell's wireless monitoring network accessible via standard Modbus TCP/IP protocol via the Ethernet port of the Gateway. The Gateway is capable of providing a Modbus data output and simultaneously serving data to EMX portal. This allows users to take advantage of the EMX portals features while also serving data to the third party monitoring system.

The Ethernet Gateway appears as a standard Modbus device listening on port 502 at the IP address of the Gateway. Individual monitoring nodes have distinct Modbus slave IDs. If more than 254 nodes are present, multiple nodes may report at the same slave ID under different register ranges (see Register Mapping section below). The Modbus protocol requires a single Master connection for all connected nodes.



Peering Gateways and Using a Master Gateway

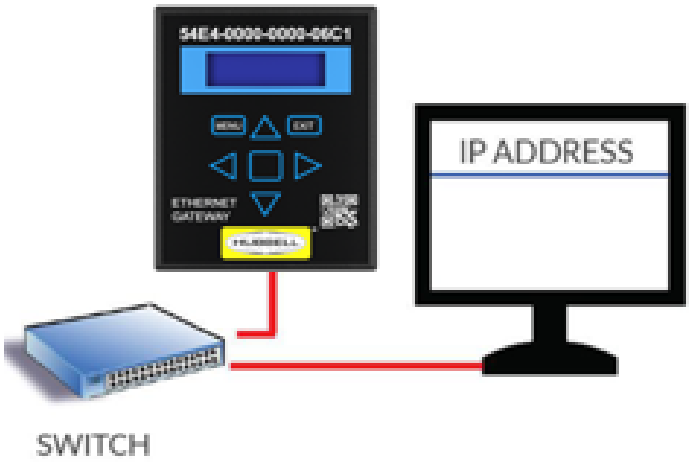
Hubbell Gateways can be deployed in a master / peer relationship. In this approach, the master gateway gathers data from all of its peers. This makes it easier for monitoring applications to access data as the monitoring application only needs to communicate with the master gateway. Note that all peered Gateways must have support for Modbus protocol conversion. Refer to the peering section of the Data Sources guide for instructions on peering Gateways.

Note that in a network consisting of a mix of V2, V3 and V4 Gateways, a Version 4 Gateway must be designated as the master.

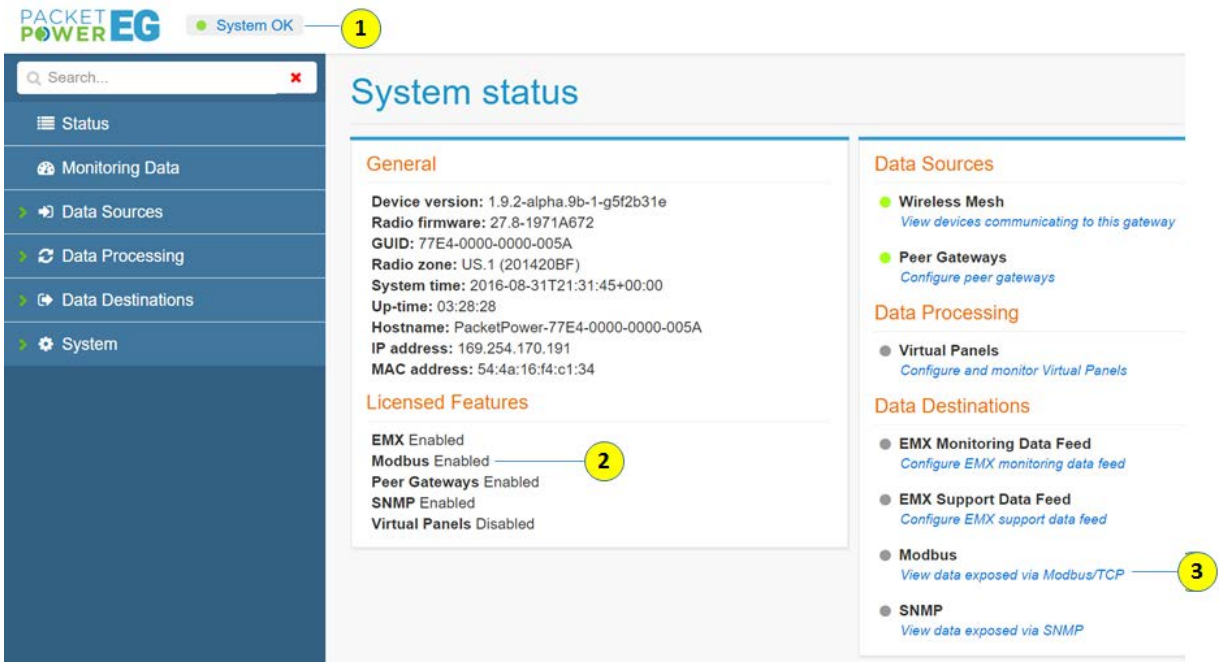
Enabling Modbus Output

To enable Modbus output, access the Gateway Console:

1. Make sure your Gateway is configured with an IP address and accessible on your network.
2. The Gateway must be connected to a switch /router on an accessible network. It may not be accessible directly through a PC Ethernet to Gateway connection in all cases.
3. Enter the IP address of the Gateway on any browser to access the Gateway Console.



Once the Console appears, it will present a System status screen. Validate:



(1) The system is communicating properly with the monitoring nodes as indicated by a green status light

(2) Modbus is listed as a licensed feature (2). If not,see the licensing section on how to add a license.

Enabling and Configuring the Modbus Driver

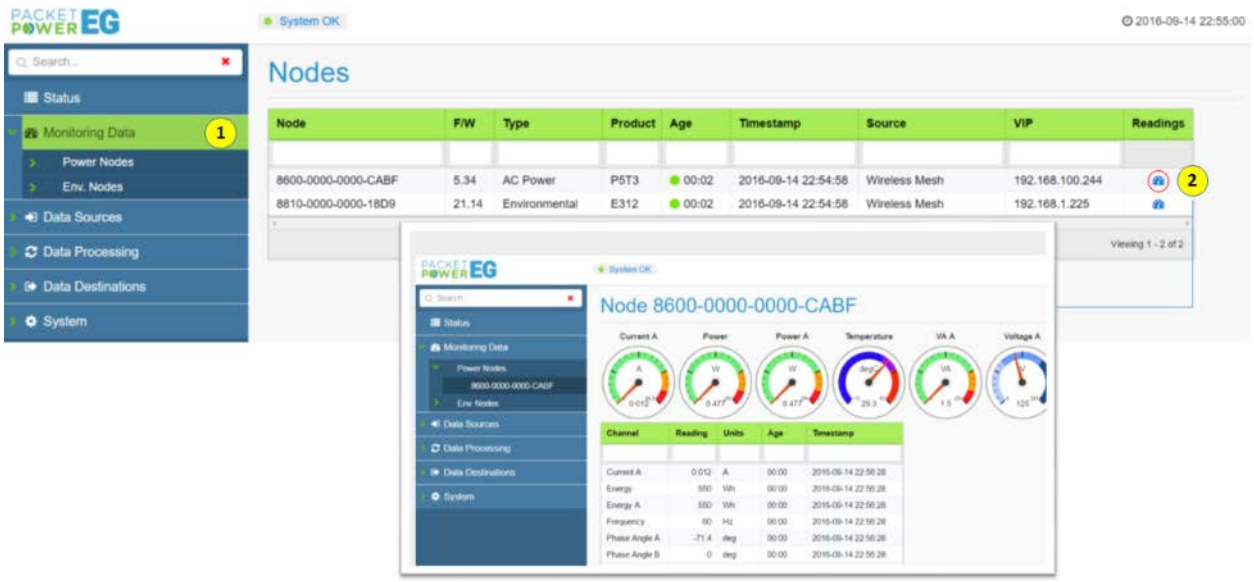
(1) To enable the Modbus driver, select Modbus tab under the Data Destinations menu in the Gateway Console

(2) Make sure that the "Enabled" check box (2) is checked

(3) Enter the port number to be used. This is typically port 502
Click "Save" to enable the selections.

(4) Once enabled, there will be a green light next to the Modbus tab

Viewing and Verifying Monitoring Data using the Gateway Console

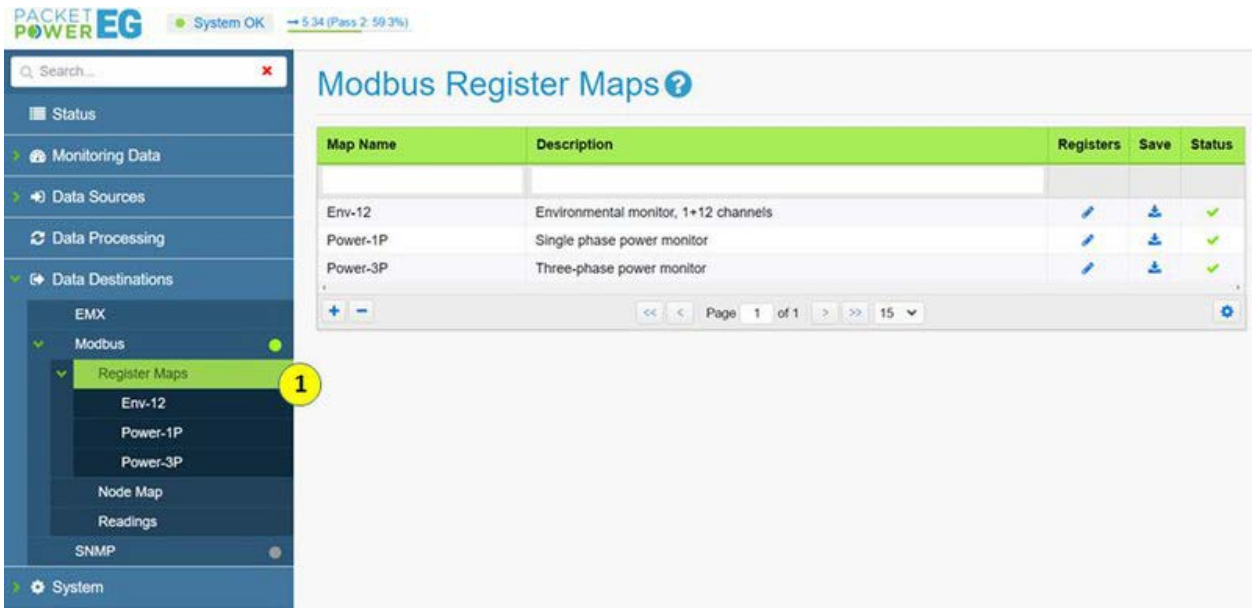


(1) To view data for monitoring nodes associated with the Gateway and confirm operation of specific nodes select the "Monitoring Data" tab (1) on the Gateway Console.
This will display all connected nodes which are organized by type (power and environmental) in the sub-menu
To search for a specific node enter the GUID (16 digit node ID) in the "Node" tab

(2) To access specific readings for each node click on the "readings" icon to expose the real time readings

Register Maps

Accessing Register Maps



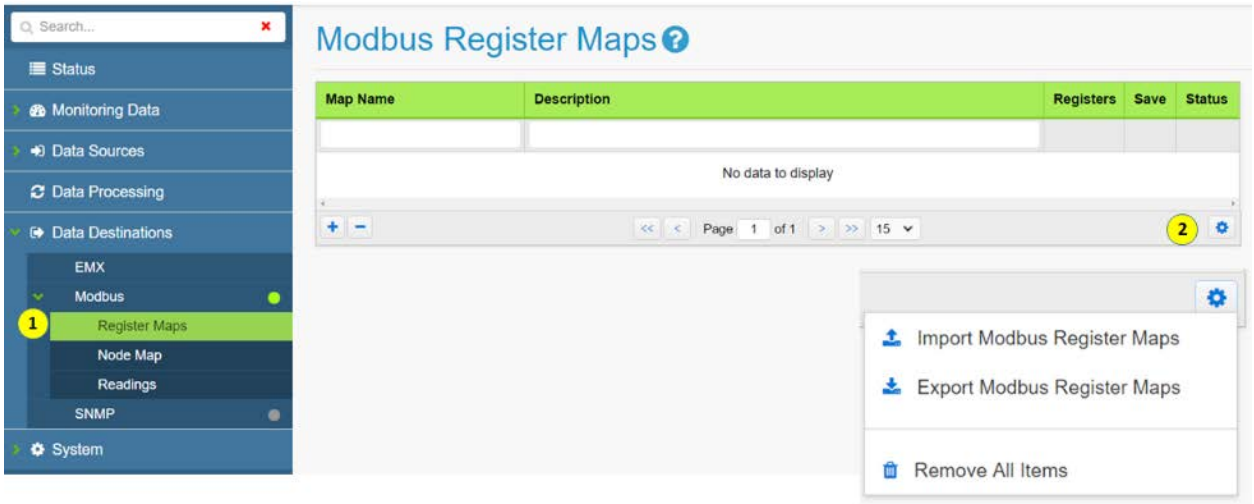
Depending on your Gateway, register maps may be pre-loaded on Gateways with firmware versions 1.12.0 or higher and will appear under the Modbus Register Maps table.

There are three main register map sets:

- Environmental monitor
- Single phase power monitor
- Three phase power monitor

Your register maps can be imported if they are not pre-populated.

Importing and Exporting Register Maps



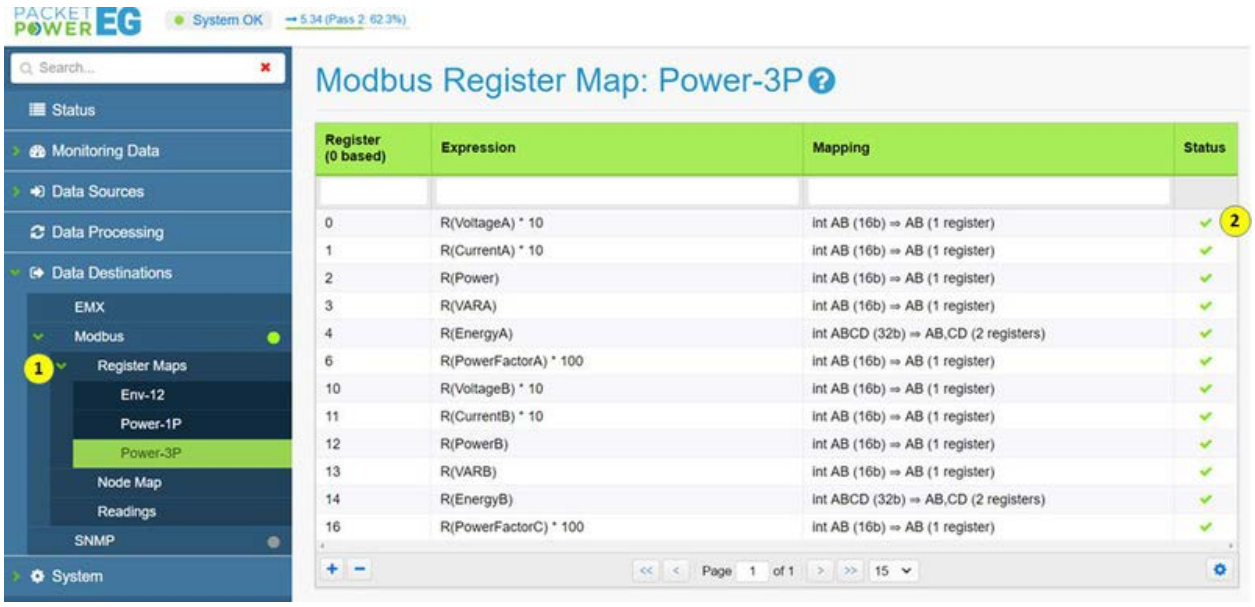
(1) To import a register map, select the "Register Maps" tab under the Data Destinations > Modbus menu

(2) Click on the utility icon under the Modbus Register Maps table

Highlight the import tab and specify the register file to be imported; the map will appear in the "Modbus Register Maps" table

This process can be used to export register maps for back-up and transfer to other Gateways.

Viewing Register Maps

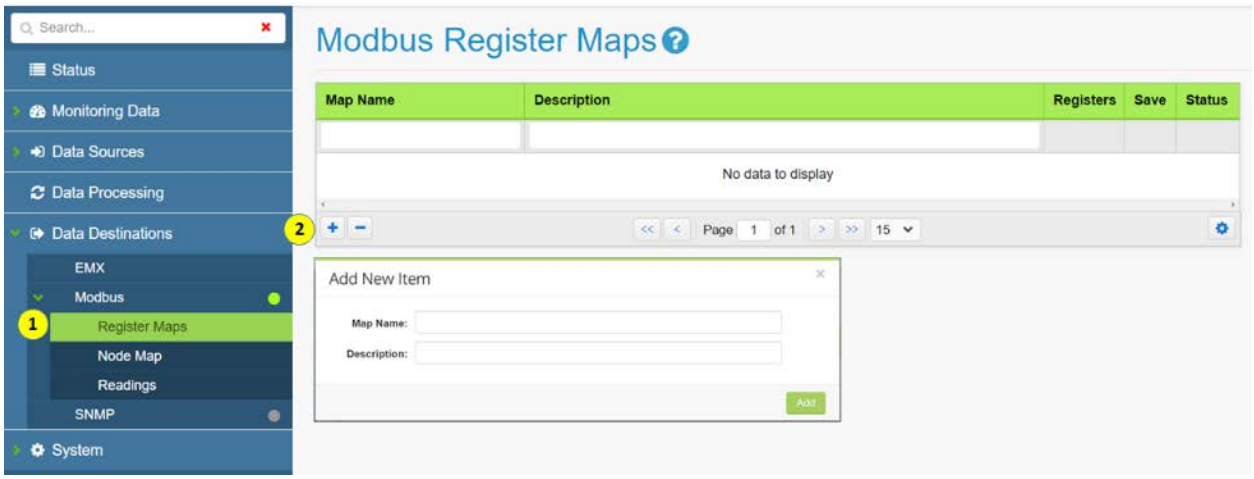


(1) Once a register map is loaded or populated it can be accessed in "Register Maps" under the Data Destinations > Modbus menu
(2) Each register has a status column to indicate the validity of the register; if the register is reading properly it will have a green check mark

Manually Assigning Registers and Register Maps

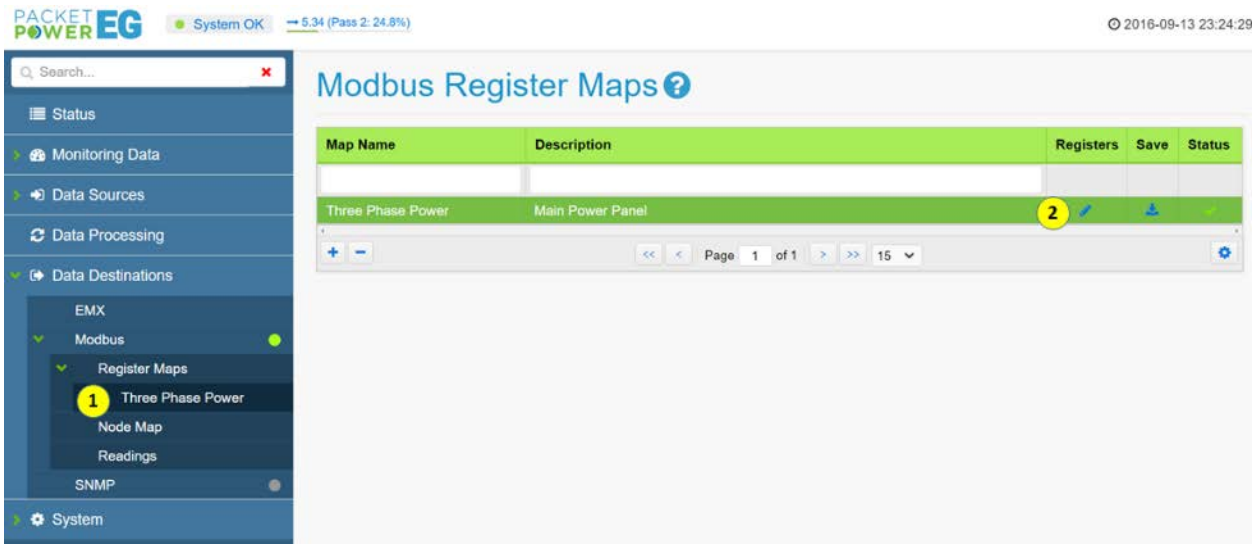
Creating Register Maps

Individual registers can be added or removed as needed. To create a new register map:



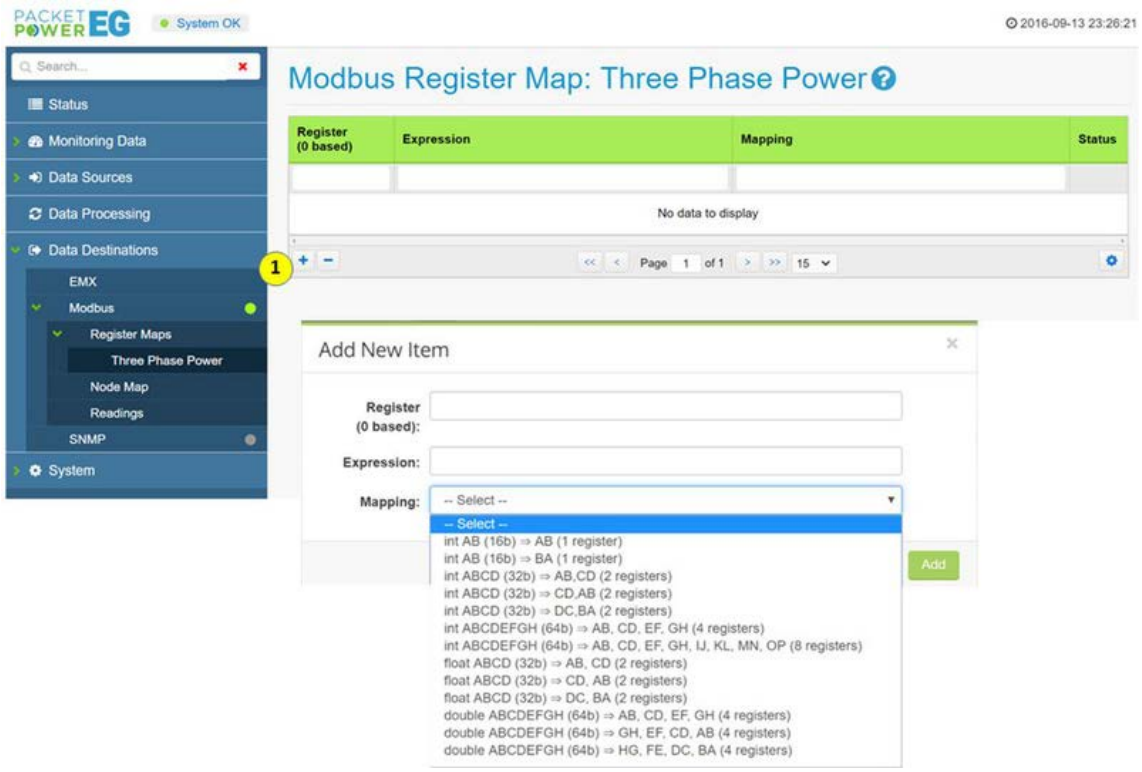
(1) Select the "Register Maps" tab from the menu under Data Destinations > Modbus
(2) Select the "+" icon on the Modbus Register Maps table and provide a Map Name and Description for the register map
Click "Add" to save the selection.

Creating Registers



(1) To access and add registers, select the "Register Maps" menu and highlight the specified register map
(2) Click on the "pencil" icon under the Register Maps table; this will expose the registers.

Adding Registers to Register Maps



To add individual registers to a register map:
(1) Select the "+" icon from the Register Map
(2) Enter the Register, Expression and Mapping

Modbus Device IDs

Node Maps serve to assign "device IDs" and register maps to specific monitoring nodes. Modbus is limited to 255 unique device IDs (0-254) per master. To allow more than 255 devices to serve under one master i.e. Gateways, different nodes can share a device ID but utilize register offset mapping.

Register Offset Node mapping

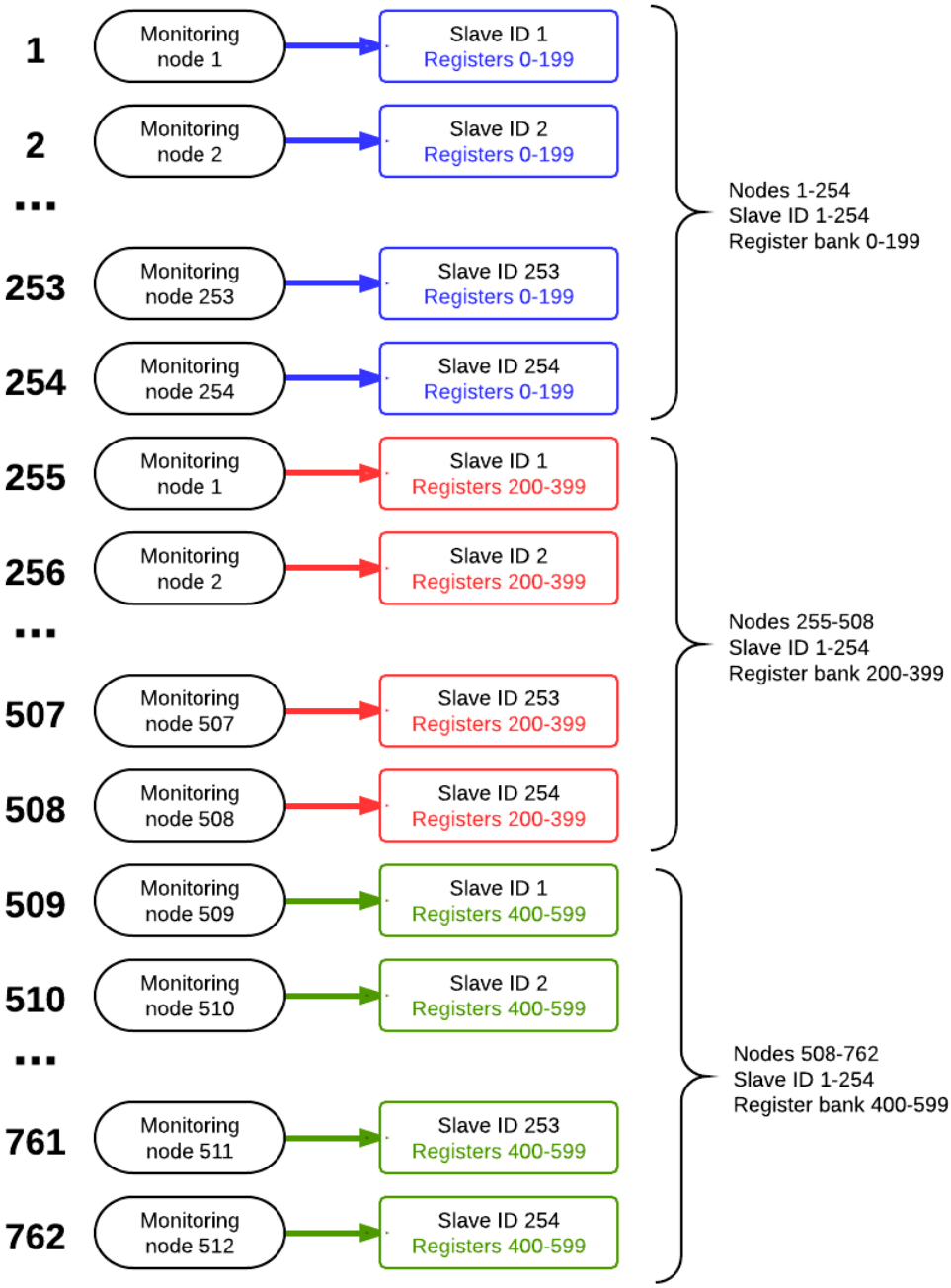
The Hubbell system supports large numbers of devices reporting through a single gateway. Up to 2000 nodes are supported in the Modbus Enterprise version.

In order to accommodate such large numbers of devices and maintain a simple, common register map for each node, the Hubbell Modbus interface uses multiple Modbus slave IDs and, if necessary, register offsets. Automatically assigning different host IDs to each nodes allows each node to have an identical register map. The number of host IDs is limited to 254 (1-254). For installations larger than 254 nodes register offsets are used.

Each register map is contained within a 200 register window (0-199). The register map, however, can be offset: the first 254 nodes use host IDs 1-254 with the register window located at address 0 (registers 0-199); the second 254 nodes also use host IDs 1-254, but with the register window located at address 200 (registers 200-399). This way 2000 nodes can be accommodated with at most 8 register windows using the following mapping:

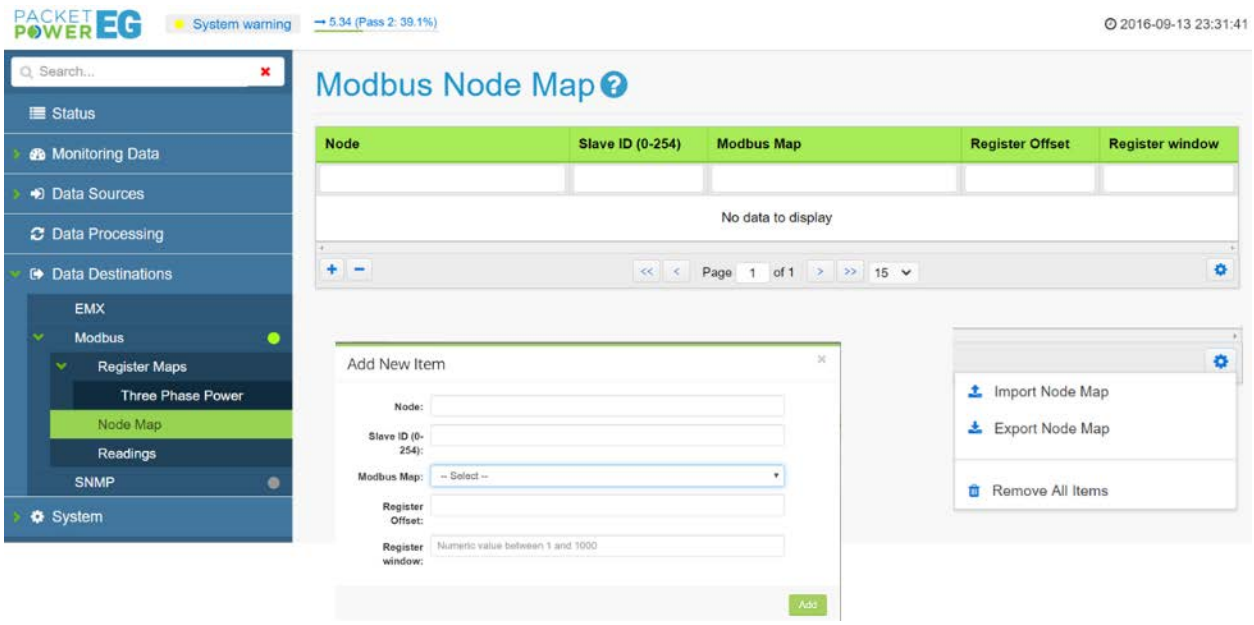
Nodes	Slave IDs	Register range
1-254	1-254	0-199
255-508	1-254	200-399
509-762	1-254	400-599
763-1016	1-254	600-799
1017-1270	1-254	800-999
1271-1524	1-254	1000-1199
1525-1778	1-254	1200-1399
1779-2000	1-254	1400-1599

The image on the following page illustrates the mapping process.

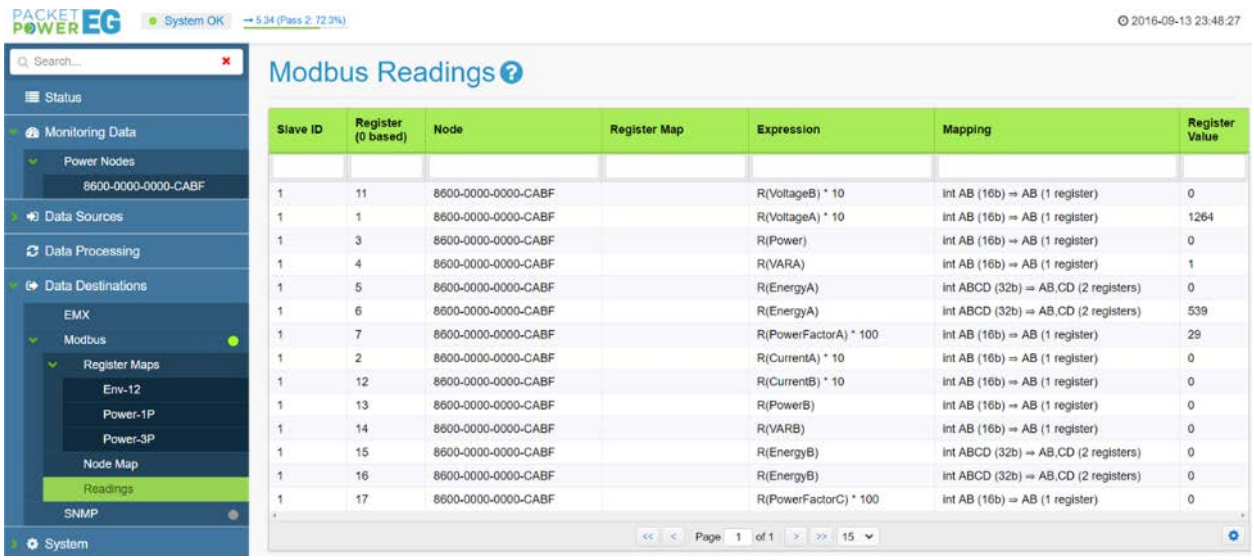


The gateway Modbus node to slave ID and register offset mapping can be automatically generated and customized if necessary.

Note: the "Map all nodes" button will remove all existing Slave ID mappings and re-assign them in the order of Node ID. If you want to preserve your existing Slave ID assignments (e.g. when you add more monitoring nodes to the system), you should edit the node mapping table directly, using the edit function at the bottom of the node mapping table.

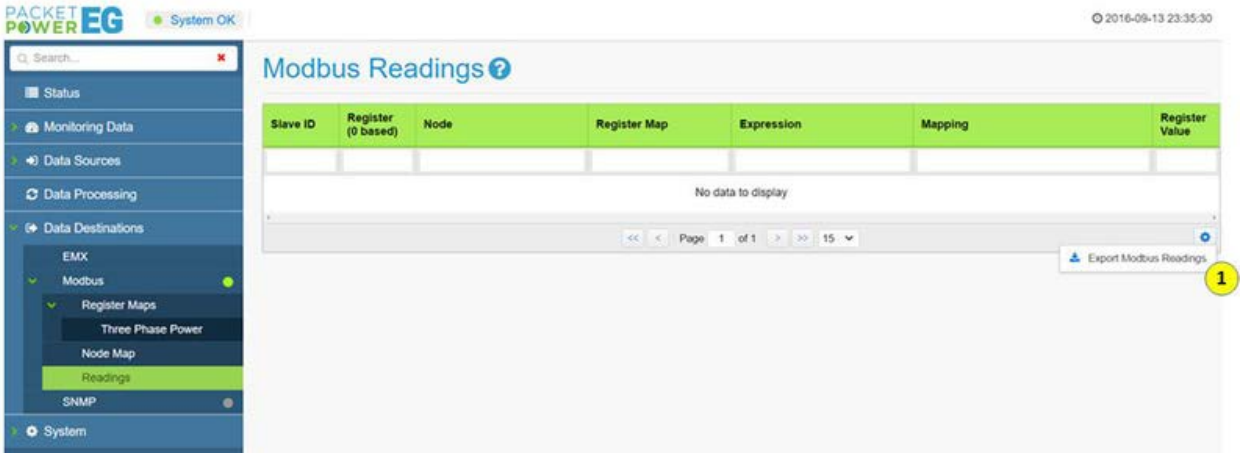


Accessing and Verifying Modbus Readings Using the Gateway Console



To access and verify Modbus readings:
Select the "Readings" tab under Data Destinations>Modbus>Register Maps>Readings.
A table containing all Modbus readings will be displayed allowing for easy verification.

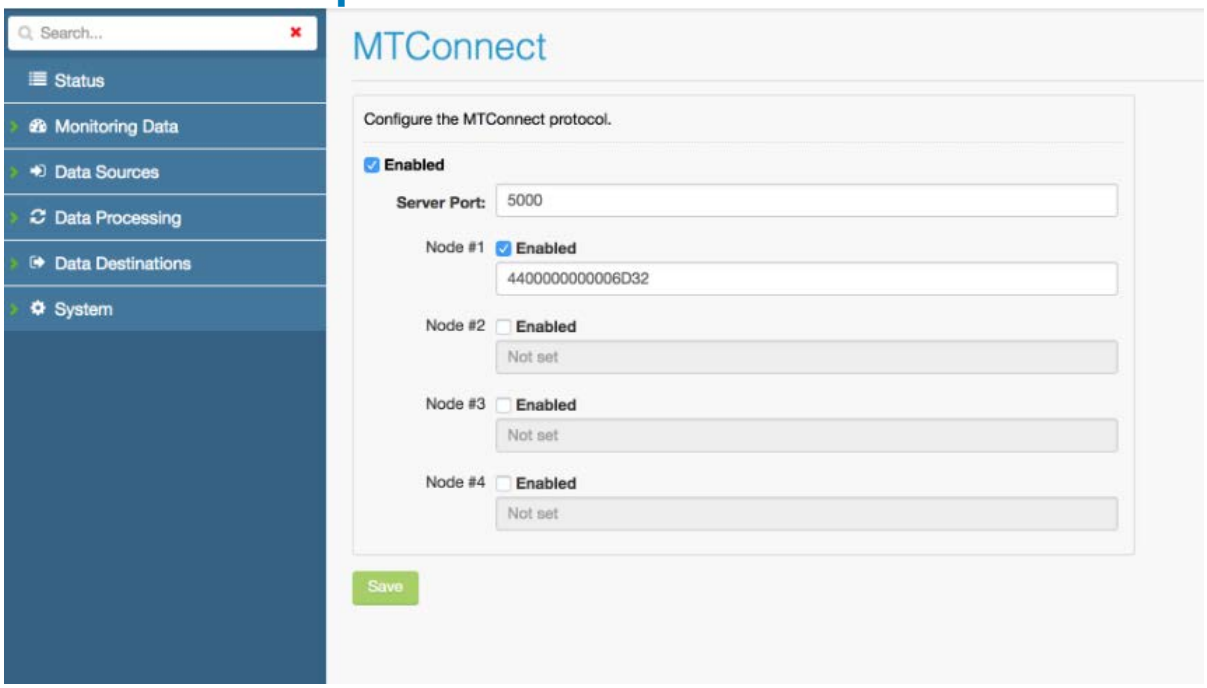
Exporting Modbus Readings



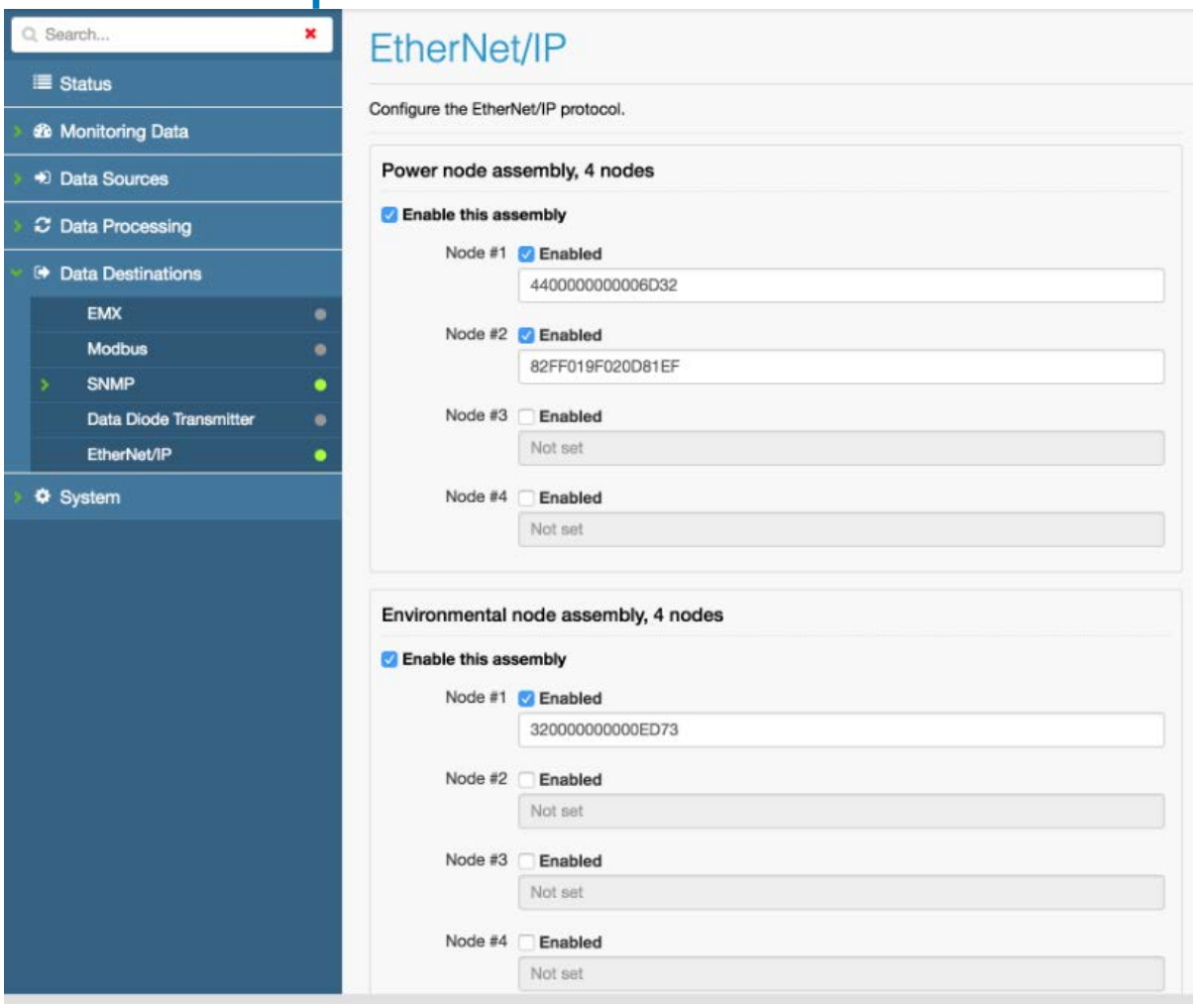
(1) Readings can also be exported by selecting the utility icon and selecting export all readings. The files are exported in .CSV format and can be viewed in a standard spread sheet.

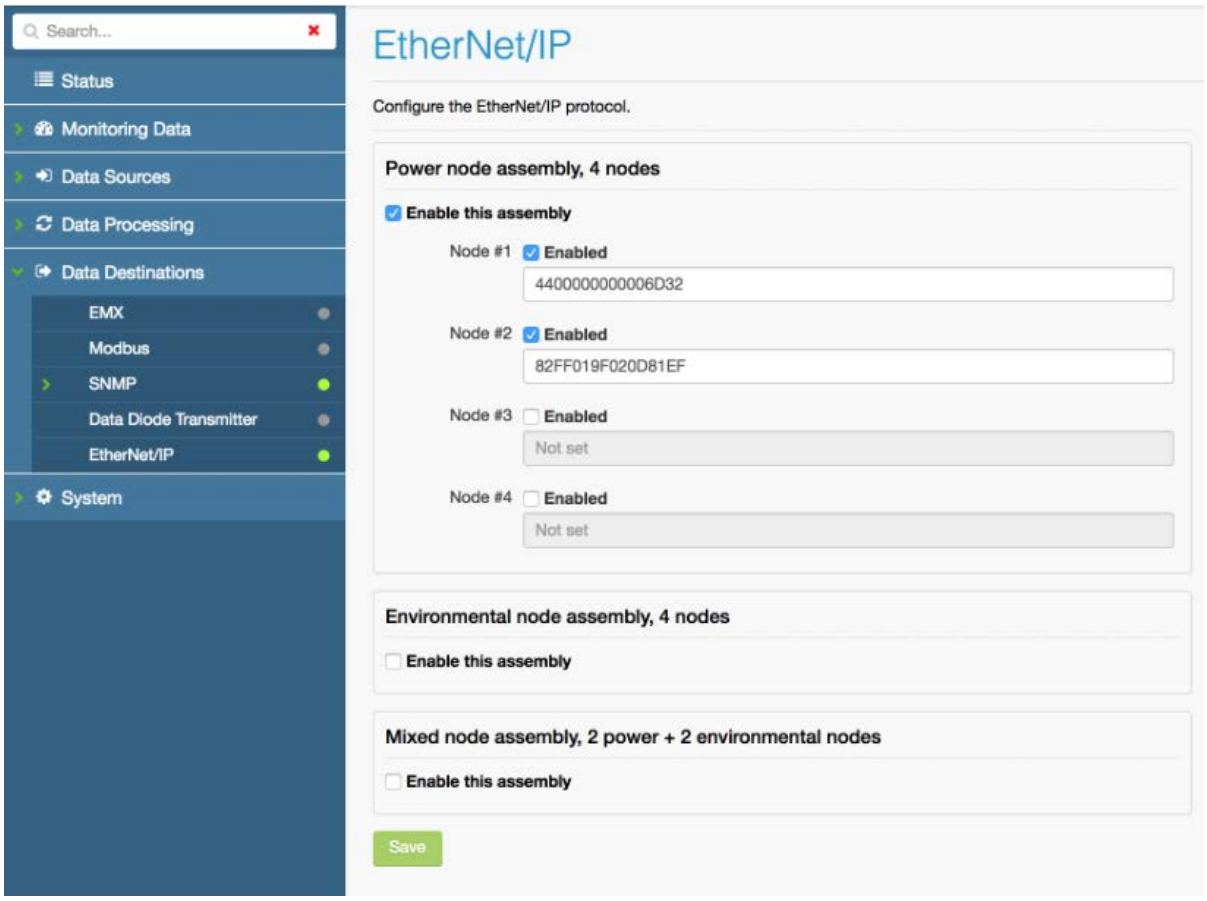
Note that readings should match the readings shown in the Monitoring Data tab.

MTConnect Implementation



EthernetIP Implementation




Search...
Status
Monitoring Data
Data Sources
Data Processing
Data Destinations
EMX
Modbus
SNMP
Data Diode Transmitter
EtherNet/IP
System
EtherNet/IP
Configure the EtherNet/IP protocol.
Power node assembly, 4 nodes
Enable this assembly
Node #1 Enabled
4400000000006D32
Node #2 Enabled
82FF019F020D81EF
Node #3 Enabled
Not set
Node #4 Enabled
Not set
Environmental node assembly, 4 nodes
Enable this assembly
Mixed node assembly, 2 power + 2 environmental nodes
Enable this assembly
Save

Technical Specifications

Communications

Operating frequency	860 to 930 MHz and 2.4 GHz (frequency used varies by region)
Wireless protocol	Frequency hopping self-configuring load-balancing mesh
Wired network protocol	Ethernet with SNMP and Modbus TCP/IP optional
Firmware updates	Wireless
Typical transmission range	10 to 30 meters indoors between any two devices in mesh network
Antenna	Fully enclosed, fixed configuration
Monitoring unit to gateway ratio	Up to 150 monitoring units per gateway
Gateways per site	Unlimited
Multi-site support	Yes
Encryption	AES 128-bit
Compatible devices	All Packet Power monitoring units
Local display	LCD for status and configuration; LED for general device status

Environmental & Mechanical

Operating temperature	0° to 40°C (32° to 104°F)
Operating humidity	10% to 90% non-condensing
Environmental rating	Indoor use / NEMA 1
Gateway size	Dimensions: 76mm x 94mm x 31mm; Weight: 136g (4.8 oz)
Placement	Top of server cabinet, under cable raceway, under raised floor
Mounting options	DIN rail, screw, cable tie
External power supply	100 to 240V AC input; 50/60 Hz (5V DC) output
Plug types	C14, NEMA 5-15, CEE-7 Schuko, AS/NZS 3112 2000, BS 1363A, BS 546A, China CPCS-CCC
Power consumption	3W
Power over Ethernet	Available, requires an external PoE splitter
Certifications	FCC, IC, CE; consult Packet Power for additional certifications

Regulatory Information and Labels

Regulatory Information

This product has been certified to meet the following requirements: UL / ANSI standards 61010-1,Second Edition, Dated July 12, 2004 with revisions through and including October 28,2008 CAN/CSA-C22.2 No. 61010-1, second edition, including Amendment 1, or a later version of the same standard incorporating the same level of testing requirements. Council Directive 2006/95/EC (December 12, 2006) on Low Voltage Equipment Safety; IEC 61010-1:2001 (Second Edition) and EN 61010-1:2001 (Second Edition) Council Directive 1999/05/EC - European Union (EU) Radio & Telecommunications Terminal Equipment Directive(R&TTE) ETSI EN 300 220-2, Issued:2006/04/01 and ETSI EN 301 489-3, Issued:2002/08/01 V1.4.1 Council Directive 2004/108/EC (December 15, 2004) on Electromagnetic Compatibility CENELEC EN 61326-1 Issued:2006/05/01; IEC 61326-1:2005;:1997 – AS/NZS 4268: 2008

Class B Device Statement / FCC Regulations

Section 15.105(a) of the FCC Rules: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Section 15.19 of the FCC Rules: This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Pursuant to Part 15.21 of the FCC Rules, any changes or modifications to this product not expressly approved by Hubbell LLC might cause harmful interference and void the FCC authorization to operate this product.

Pursuant to part 2.1091c of the FCC rules device is categorically excluded from routine RF Exposure regulations.

Industry Canada (IC) Compliance Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:(1) This device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser)gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.Per section RSS-102, 2.5 of Industry Canada regulations, this device is categorically excluded from Routine Evaluation Limits.

Industrie Canada (IC) Déclaration de conformité

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit

pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillageradioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Regulatory Label