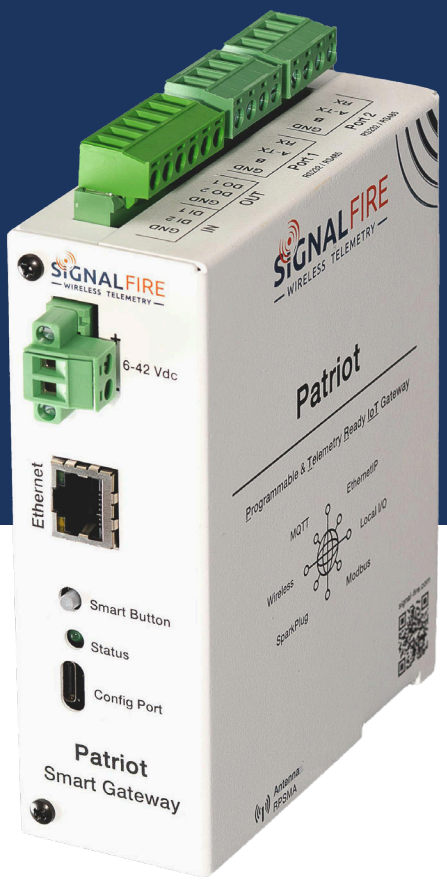
PATRIoT Gateway Manual



Specifications

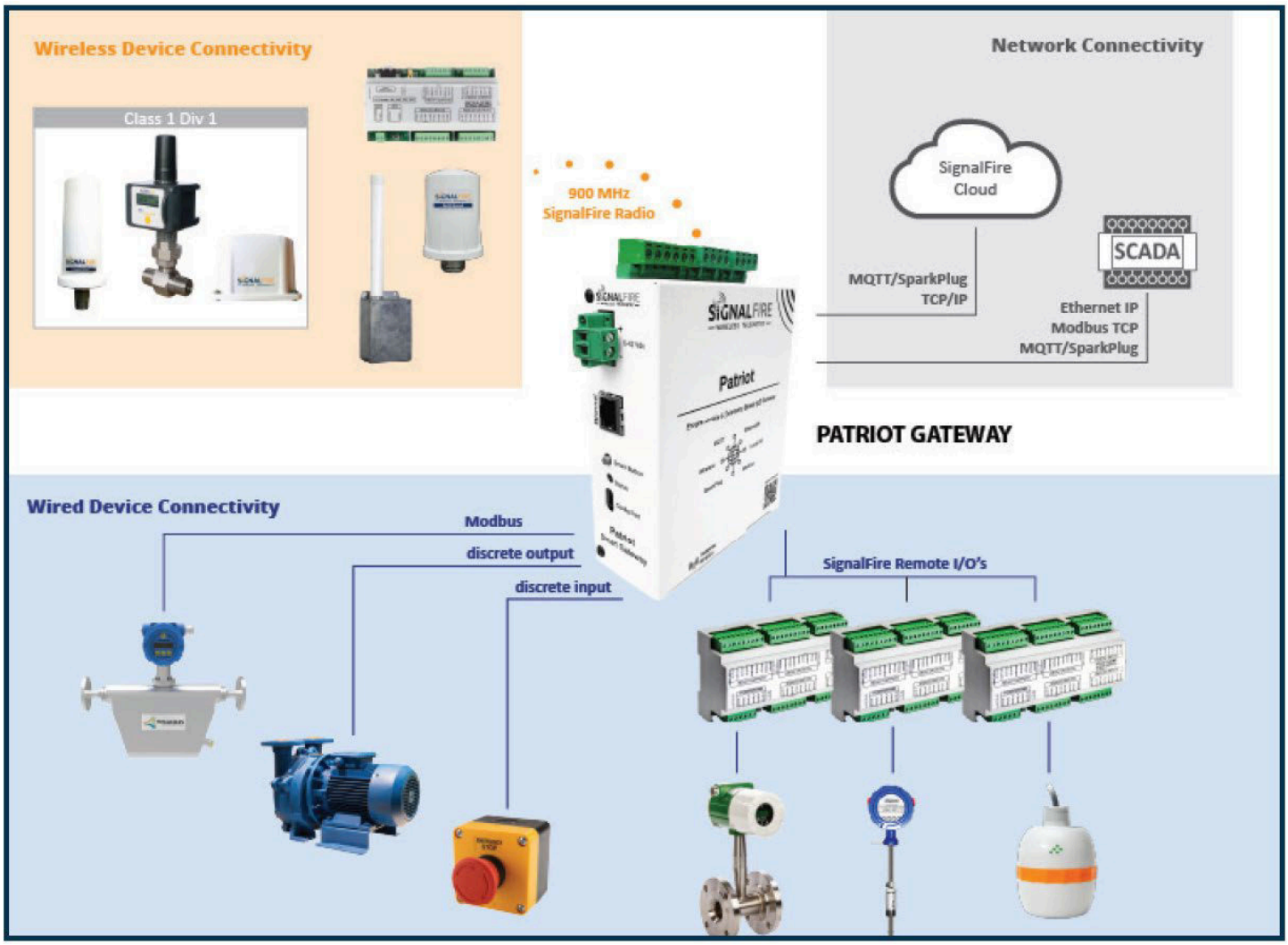
Physical Specifications	
Dimensions	5.6” (142mm) Tall x 1.6” (41mm) Wide x 5.2” (132mm) Deep
Weight	2 Lbs (0.9Kg)
Housing Material	Powder Coated Steel
Mechanical installation	DIN Rail Mount
Electrical Specifications	
Input Power	6 to 42 Vdc
Power Consumption @ 12Vdc	No Ethernet: 66mA Average, 75mA Max With Ethernet: 85mA Average, 95mA Max
Power Consumption @ 24Vdc	No Ethernet: 35mA Average, 43mA Max With Ethernet: 45mA Average, 53mA Max
Wire Termination	Screw Terminals. 18AWG-22AWG
Clock	Clock and RSD Control Registers Maintained For 30 Days Without Power
Environmental	
Ambient Operating Temperature	-40 to +185°F (-40°C to 85°C)
Humidity	0% - 95% Non-Condensing
Wired Communication Interfaces	
2x RS485/RS232	2 Serial Ports. Individually software Configurable For RS485 or RS232. Server Mode (Client Mode Pending)
1x RJ45	10/100 Ethernet Port with TCP/IP, Modbus TCP , Ethernet/IP (pending)
1x USB-C	USB-C High Speed Interface For Local Configuration With SignalFire Toolkit
Wired Communication Protocols	
Modbus RTU	30,000 Tags 2000 Remappable Tags Mode: Server Mode: Client (Pending)
Modbus TCP	30,000 Tags 2000 Remappable Tags 8 Concurrent Clients Mode: Server Mode: Client (Pending)
Ethernet IP (Pending)	CIP I/O Connections: 2 CIP Coil / Discrete Assemblies: 2x240 CIP Register Assemblies: 12x248
MQTT/SparkPlug	1000 Tags 200,000 Store/Forward Tag Buffer Configurable MQTT Brokers (3) TLS Encryption 1.2

Wireless Communication Interface	
SignalFire 900MHz Star/Mesh Network	Radio Power: 500mW Antenna: External, Omnidirectional Frequency Band: 902MHz - 928MHz ISM License Free, Compliant With FCC Part 15 And Industry Canada Up To 3 Mile Range (Depends on SignalFire Node Type & Condition)
Antenna	RP-SMA Antenna connector
Wireless Communication Protocol	
SignalFire	Mode: Start/Mesh Self Organizing and Self Healing Nodes: 240 (Depends On Update Rate Interval Of Each Node) Remote Configuration Of Nodes Using Over-The-Air Technology
Security	128 Bit AES Encryption, Pre-shared Key Frequency Hopping Replay Prevention
Local Automation	
Remote Shutdown Logic	Configurable With Up To 128 rules
Networking	
Modbus TCP Connections	8 Modbus Concurrent Clients
Web Admin Interface	Configurable Login Credentials and Enable/Disable Control Setting
MQTT/SparkPlug	Configurable Broker (3) with TLS 1.2 Security
IP	Static or DHCP
Network Time	NTP Sync
I/O Expansion Modules	
SignalFire Analog/Relay Output Module	Up to 2 Modules. Each Module Has 8 Analog Outputs and 2 Relay Outputs
SignalFire Digital Output Relay Module	Up to 2 Modules. Each Module Has 12 Digital Outputs
Approvals	
Hazardous Locations (pending)	Class 1 Division 2 Certified, Groups A,B, C, D. Temperature Code T5 Certified to CSA C22.2 No. 213:2017, Conforms to UL 121201:2017
ISM Band	Compliant with FCC Part 15, IC (Industry Canada)

Table of Contents

Product Description

The PATRIoT Gateway is a versatile hub that connects wireless and wired devices into SCADA, cloud, and monitoring systems with ease. Supporting Modbus TCP, EtherNet/IP, and MQTT/SparkPlug, it seamlessly integrates data from SignalFire's 900 MHz wireless nodes, Modbus devices, and field I/O modules for a flexible, cost-effective solution. With ultra-low power consumption, large-scale tag support, and secure cloud-ready connectivity, the PATRIoT delivers reliable performance in even the most remote applications. Whether you need to shorten cable runs, enable local automation, or scale to thousands of devices, the PATRIoT Gateway provides a powerful platform to modernize and simplify industrial monitoring.



FEATURES

- Integrates wireless + wired signals into SCADA, cloud, or remote systems
- Publishes to MQTT/SparkPlug with no licensing required
- Supports SignalFire Cloud for turnkey monitoring and control
- Ultra-low power consumption (<50mA) for solar-friendly installations
- Large-scale deployment capabilities with up to 30,000 Modbus tags
- Remote shutdown logic with 128 configurable rules for automation
- Expansion modules for analog and relay outputs

Connections and Components

PATRIoT Gateway Connections

The PATRIoT Gateway has 4 pluggable terminal blocks. They provide power, serial communication and I/O. The connections are as follows:

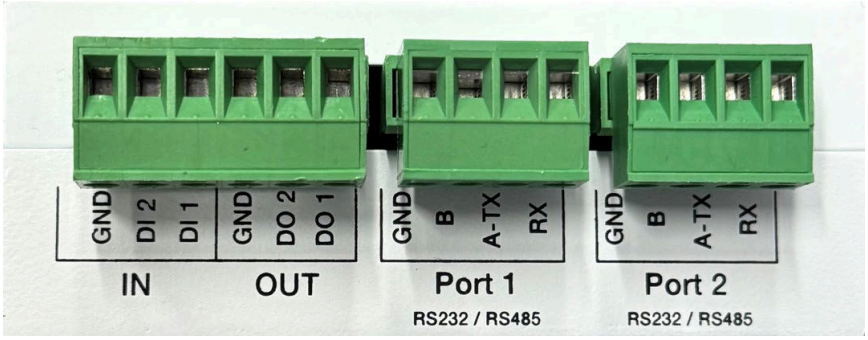
Terminal Name	Connection
6-42VDC +	Positive Power (6 to 42 VDC)
6-42VDC -	Power Ground

The PATRIoT Gateway has local I/O connections on the 6-position pluggable terminal block. The connections are as follows, left to right:

Terminal Name	Connection
GND	Digital Input Ground
DI2	Digital Input 2
DI1	Digital Input 1
GND	Digital Output Ground
DO2	Digital Output 2
DO1	Digital Output 2

Serial ports are available on two 4-position pluggable terminal blocks. The connections are as follows, left to right:

Terminal Name	Connection
GND	Ground
B -	RS485 B Terminal
A + / TX	RS485 A Terminal / RS232 TX
RX	RS232 RX



A USB-C port is available for local connection to the SignalFire Toolkit for configuration and diagnostics.

An ethernet port is available for access from a remote terminal for Toolkit configuration and Modbus-TCP commands.

The PATRIoT Gateway has an RP-SMA connection for use with an external 900MHz antenna, purchased from SignalFire or separately. Contact your local SignalFire sales rep for antenna options.

Status LED

The PATRIoT Gateway has a Status LED that blinks as follows:

STATUS LED	Description
Slow Flash (3 second pause)	System is running and has one or more nodes on network
Fast Flash (0.5 second pause)	System is running but no nodes found on network
Solid On	System Fault needs service or rescue bootloader

Smart Button

The button on the front of the PATRIoT Gateway supports the following functions.

Reboot – While running, press and hold the button for 10 seconds to reboot the Gateway
Force Bootloader – With power removed from the Gateway, press and hold while applying power. Release button after Gateway powers on. The bootloader allows for firmware update recovery.
Reset to factory defaults - With power removed from the Gateway, press and hold while applying power, continue to hold the button for 30-seconds.

Operation

The PATRIoT Gateway is designed to support all remote 900MHz SignalFire nodes, making all remote sensor data available in Modbus format. This functionality allows for seamless integration and communication between various remote sensors and the central gateway.

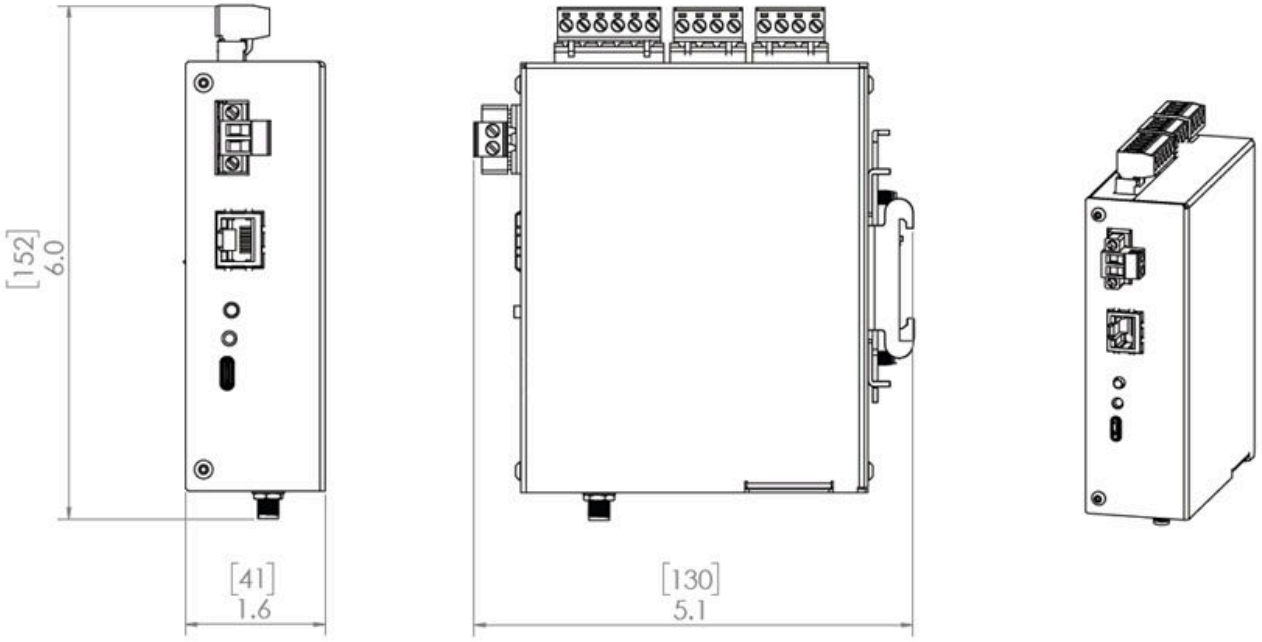
Data Retrieval

The register data from remote sensor nodes can be accessed by requesting the remote node's Modbus ID and register address from that node's register map. The gateway will respond with the most recent copy of the data from the remote node. This ensures that the data is up-to-date and accurate, providing reliable information for monitoring and control purposes.

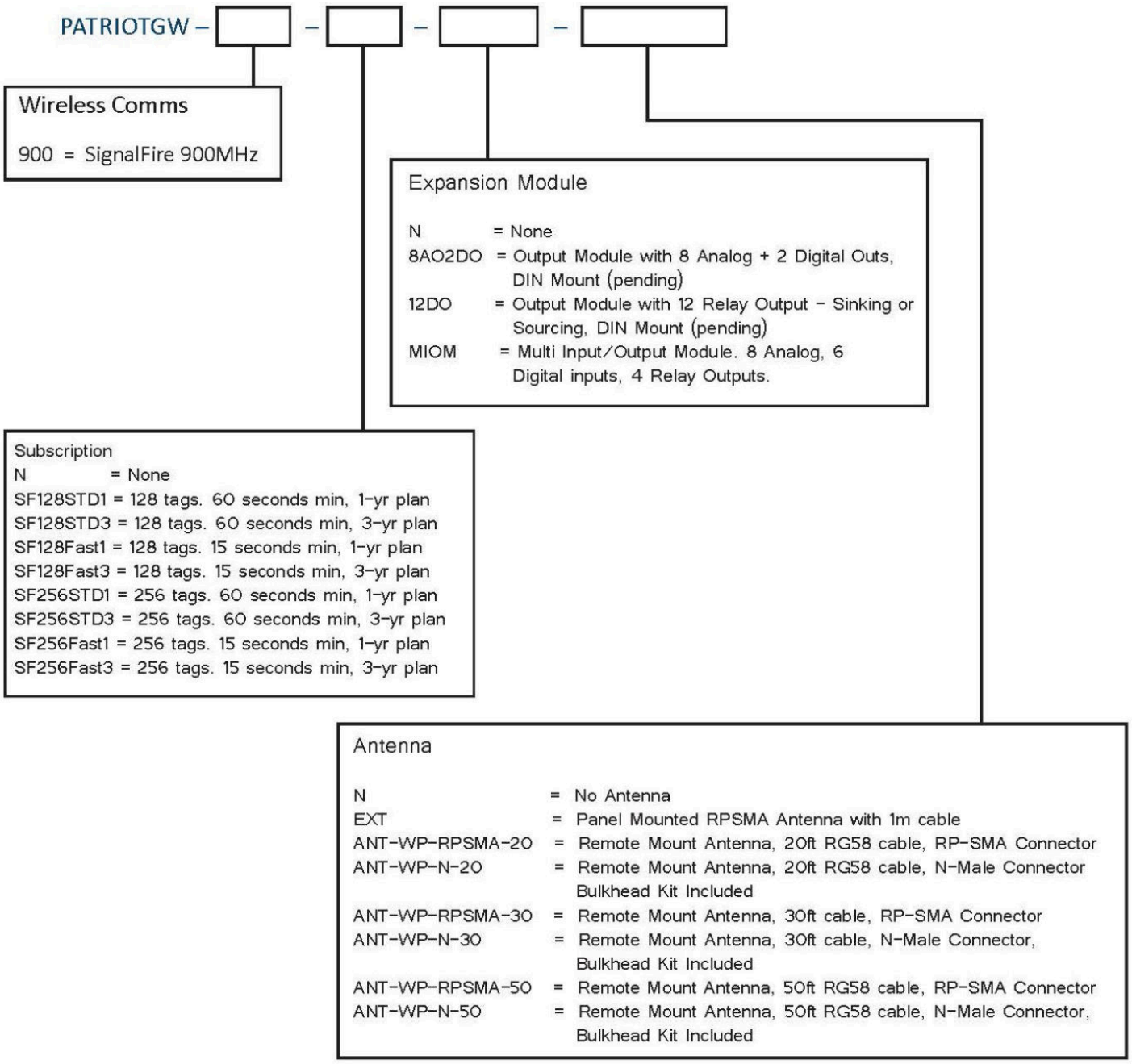
Data Timeout

To maintain data integrity and ensure that outdated information is not used, the gateway will automatically time-out data from a remote node if it stops receiving data from that node. This feature helps in identifying and troubleshooting communication issues with remote nodes, ensuring that only valid and current data is used in the system.

Dimensions



How To Order


PATRIOTGW – – – –
Wireless Comms
900 = SignalFire 900MHz
Expansion Module
N = None
8AO2DO = Output Module with 8 Analog + 2 Digital Outs, DIN Mount (pending)
12DO = Output Module with 12 Relay Output – Sinking or Sourcing, DIN Mount (pending)
MIOM = Multi Input/Output Module. 8 Analog, 6 Digital inputs, 4 Relay Outputs.
Subscription
N = None
SF128STD1 = 128 tags. 60 seconds min, 1-yr plan
SF128STD3 = 128 tags. 60 seconds min, 3-yr plan
SF128Fast1 = 128 tags. 15 seconds min, 1-yr plan
SF128Fast3 = 128 tags. 15 seconds min, 3-yr plan
SF256STD1 = 256 tags. 60 seconds min, 1-yr plan
SF256STD3 = 256 tags. 60 seconds min, 3-yr plan
SF256Fast1 = 256 tags. 15 seconds min, 1-yr plan
SF256Fast3 = 256 tags. 15 seconds min, 3-yr plan
Antenna
N = No Antenna
EXT = Panel Mounted RPSMA Antenna with 1m cable
ANT-WP-RPSMA-20 = Remote Mount Antenna, 20ft RG58 cable, RP-SMA Connector
ANT-WP-N-20 = Remote Mount Antenna, 20ft RG58 cable, N-Male Connector Bulkhead Kit Included
ANT-WP-RPSMA-30 = Remote Mount Antenna, 30ft cable, RP-SMA Connector
ANT-WP-N-30 = Remote Mount Antenna, 30ft cable, N-Male Connector, Bulkhead Kit Included
ANT-WP-RPSMA-50 = Remote Mount Antenna, 50ft RG58 cable, RP-SMA Connector
ANT-WP-N-50 = Remote Mount Antenna, 50ft RG58 cable, N-Male Connector, Bulkhead Kit Included

1. Setup

The PATRIoT Gateway can be configured in one of three ways, via the ToolKit over the USB-C connection, via the ToolKit over the Ethernet connection, or all basic settings are available from a web browser using the Ethernet connection. Advanced features such as register remapping, Remote Shutdown configuration and MQTT/Sparkplug mapping must be done using the ToolKit software.

Default Settings

The default IP and user credentials are below.

IP Address:	192.168.1.100
Host Name:	PATRIoT-"MAC ADDRESS"
Modbus TCP Port:	502
SignalFire Toolkit Port:	10002
File Transfer port	10003
Web Config Username:	admin
Web Config Password:	signalfire

The SignalFire ToolKit port is user configurable, but the File transfer port will always be one higher than the configured ToolKit port. For example, if you change your ToolKit port to 1000, 1001 would be used as the file transfer port. Please make sure both ports are applied to any port forwards your network may require for full remote ToolKit capability.

1.1 Using the SignalFire Toolkit

The SignalFire Toolkit application can be downloaded at https://www.signal-fire.com/signalfire-toolkit-software/. After installation, launch the software and the main toolkit window will open:

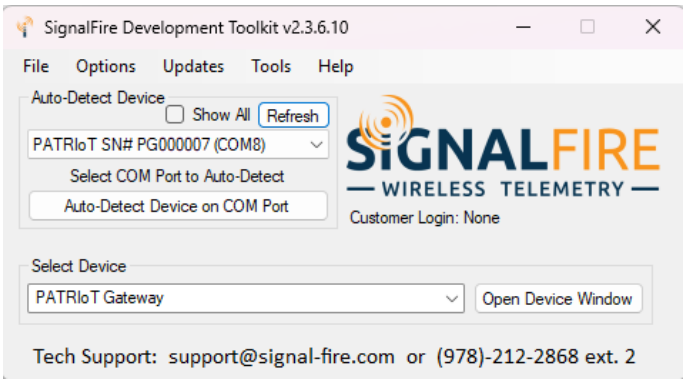


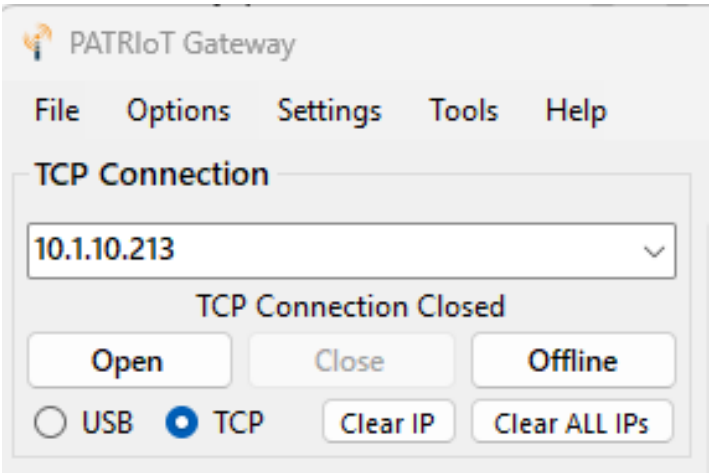
Figure 1

USB-C Connection

After connecting the USB-C cable, select the PATRIoT Gateway in the drop-down list and click "Auto-Detect Device on COM Port." This will open the Gateway configuration window, where all settings can be configured.

Ethernet ToolKit Connection

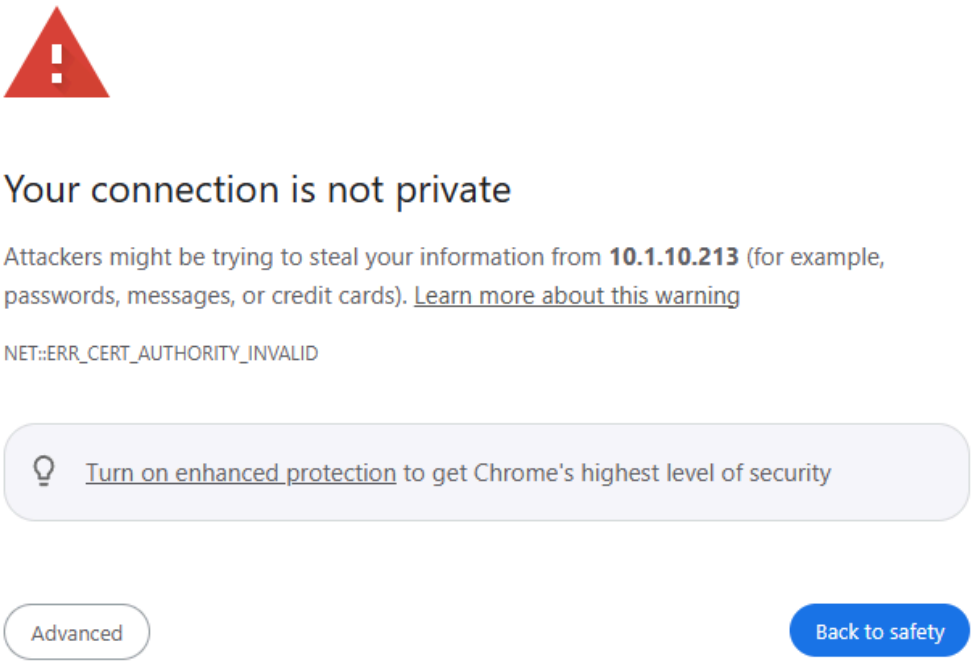
To connect to the PATRIoT Gateway with the ToolKit over the Ethernet connection, first ensure that your PC is connected to the same network as the Gateway and is configured for the same IP address space. Then select the "PATRIoT Gateway" from the Select Device drop down list and click Open Device Window. Select "TCP", enter the IP address of the Gateway and click Open.



1.2 Web Browser Configuration

The final method of configurating the Gateway is via the PATRIoT's built-in web configuration application. This allows users to set basic settings, view the Gateway status, download log files and update firmware without the need for any special software. To access the web configuration page, enter the IP address of the PATRIoT Gateway in your web browser.

Note your browser may show a security warning, click "Advanced" and click proceed to connect to the Gateway



1.3 Web and ToolKit Dashboard Overview

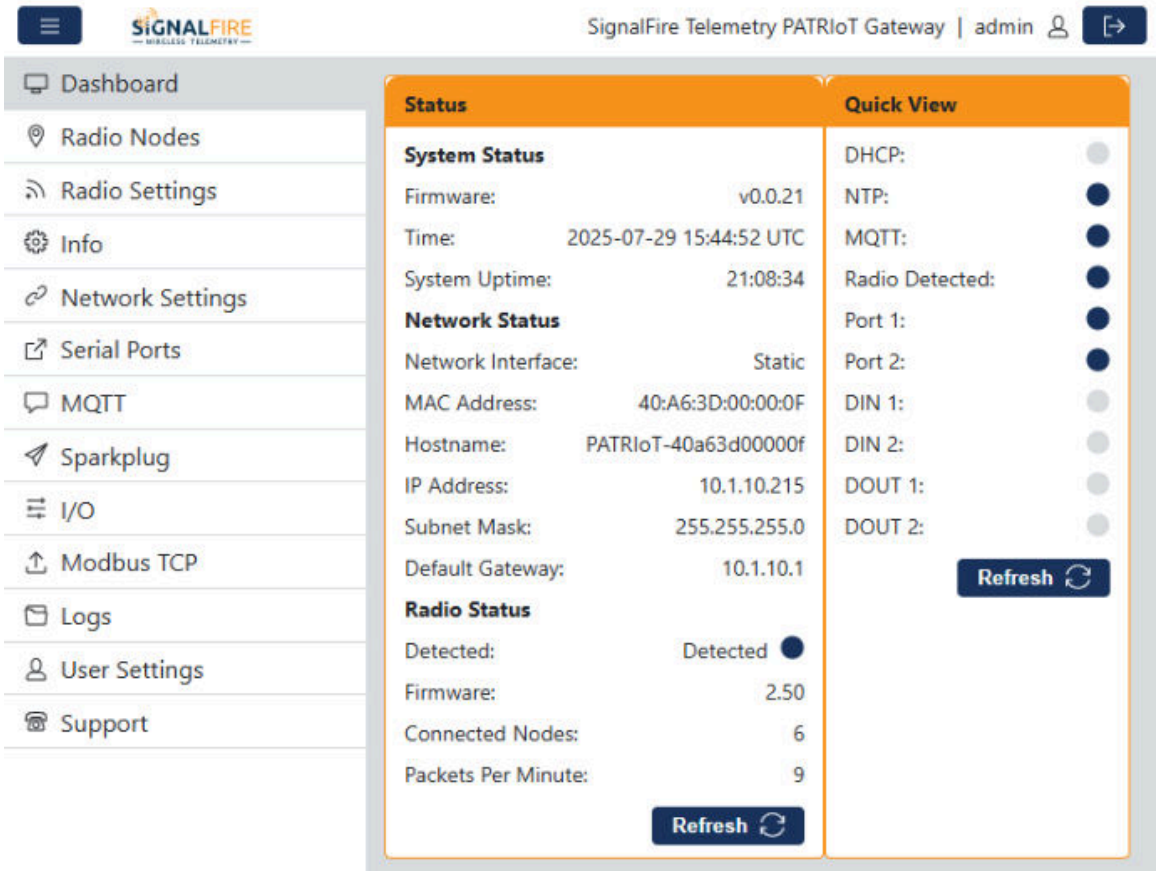
Upon logging into the PATRIoT Gateway web interface, the Dashboard provides a high-level summary of system and network status. This information is also available on the left side of the ToolKit window

System Status:
- Firmware Version: displays the firmware version of the PATRIoT
- System Time: Displays the current UTC time (e.g., 2025-07-29 15:44:52 UTC)
- System Uptime: Shows how long the system has been running since the last reboot

Network Status:
- Network Interface: Indicates whether the device is using a static IP or DHCP
- MAC Address: Unique hardware identifier
- Hostname: Device hostname
- IP Address: Current IP address
- Subnet Mask: Network mask
- Default Gateway: Router IP

Radio Status:
- Detected: Indicates if a radio module is detected
- Firmware: Displays radio firmware version (if available)
- Connected Nodes: Number of connected radio nodes
- Packets Per Minute: Number of Packets per minute received by the remote nodes, should be less than 60

Quick View:
This section provides a snapshot of key I/O and communication statuses:
- DHCP, NTP, MQTT: Show whether these services are active
- Radio Detected: Indicates radio module presence
- Port1, Port2, DIN1, DIN2, DOUT1, DOUT2: Status of digital and serial ports

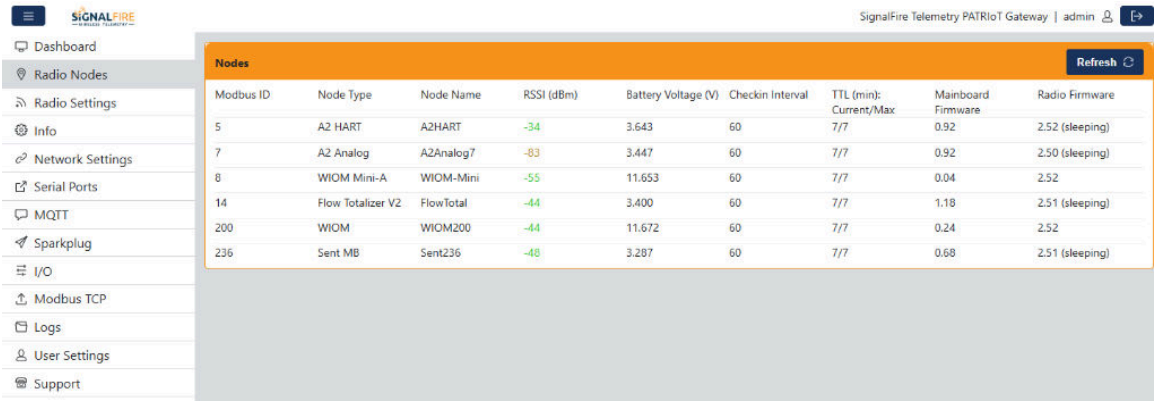


2. Radio Nodes Overview

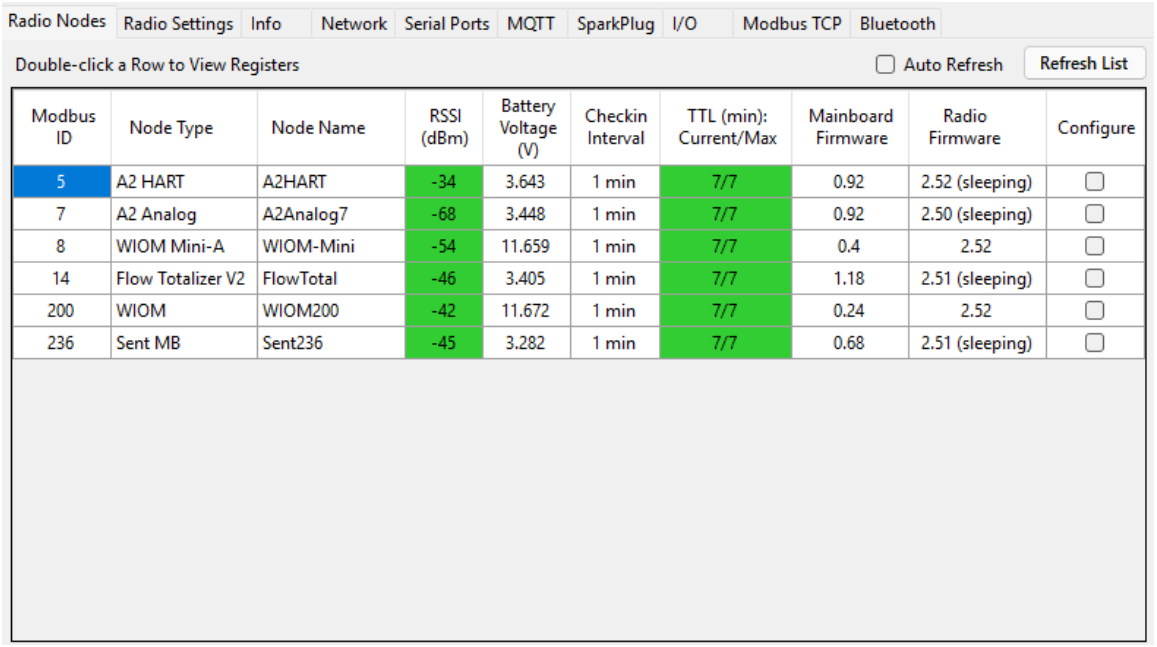
The **Radio Nodes** tab provides a real-time view of all connected wireless nodes and their operational status. This is essential for monitoring signal strength, battery health, and firmware versions.

2.1 Table Columns Explained

Column	Description
Modbus ID	Unique identifier for each node on the Modbus network.
Node Type	Type of device (e.g., A2 HART, A2 Analog, WIOM, Flow Totalizer).
Node Name	User-defined or default name for the node.
RSSI (dBm)	Received Signal Strength Indicator. Higher (less negative) values indicate better signal.
Battery Voltage (V)	Current battery voltage of the node.
Check-in Interval (min)	How often the node checks in with the gateway.
TTL (min): Current/Max.	Time-to-live values showing how long the node remains active before timing out.
Mainboard Firmware	Firmware version of the node's mainboard.
Radio Firmware	Firmware version of the radio module. "(sleeping)" indicates the node is in low-power mode and will not act a repeater for other nodes. Devices not marked as sleeping will automatically act as repeater nodes in the network



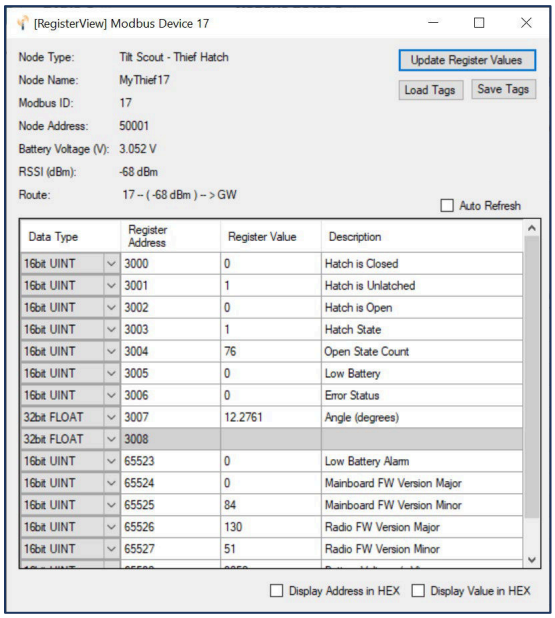
When connected via the ToolKit, you can view the register data by double clicking on any of the connected remote nodes.



If one or more remote nodes are configured with the correct network settings, they will send their data to the gateway. Clicking **Refresh List** will populate the list with all connected remote nodes. The gateway displays the node type, node name (if it has been set), RSSI signal strength, check-in interval, the Time-To-Live (TTL), and the node's radio and main firmware versions.

The RSSI and TTL values are color coded (Green, yellow, orange, red) to indicate relative link quality of a node. The 'TTL Current' indicates the number of minutes remaining until the node is timed out of the gateway if no updates are received. The 'TTL Max' indicates the maximum TTL for that node and is equal to the node's check-in interval times 5 plus 2. The 'TTL Current' will reset to the 'TTL Max' each time an update is received from that node. The 'TTL Current' will decrease once a minute.

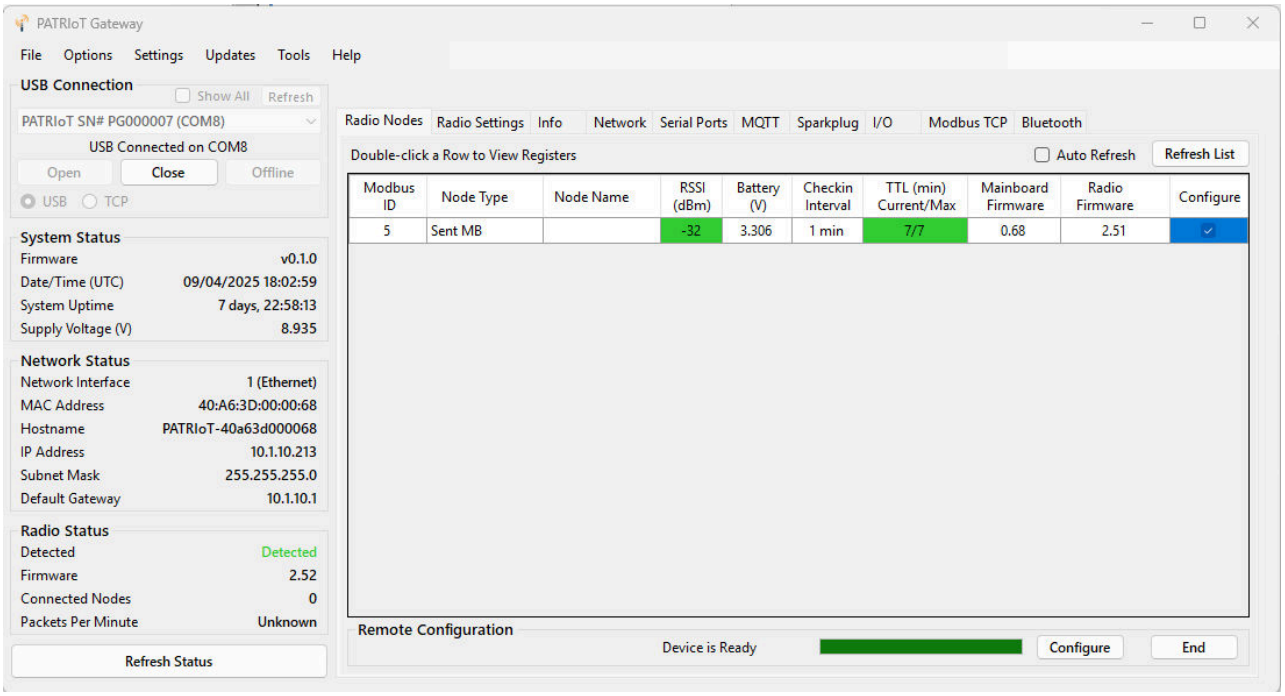
Double clicking on one of the nodes in the list will bring up additional detail including the register data from the remote node.



Remote Node Configuration

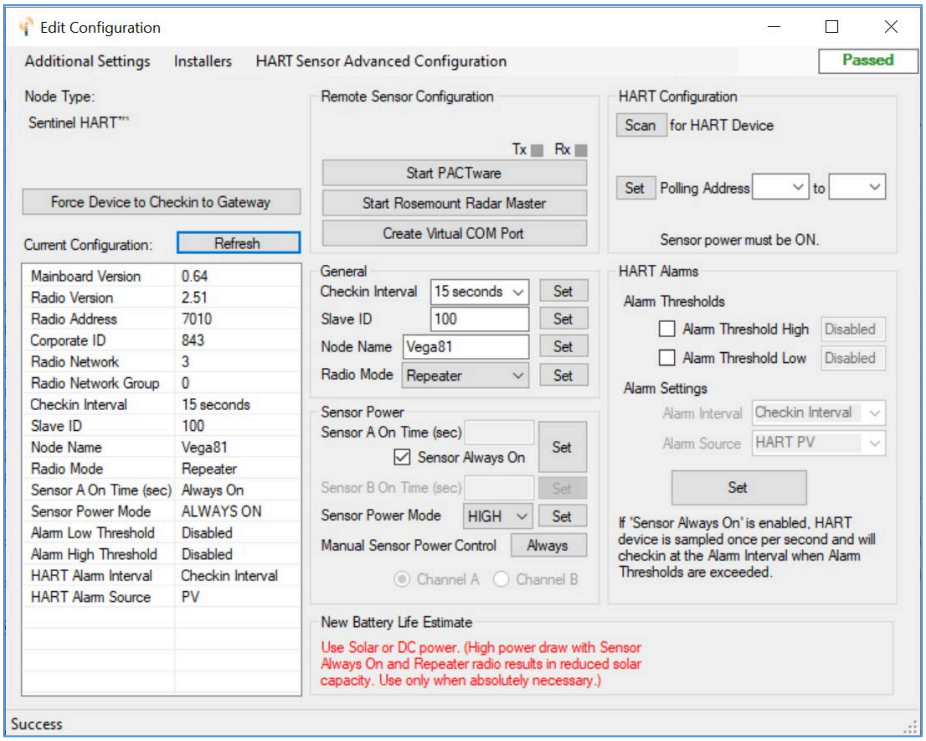
The SignalFire Gateway allows configuration changes to be made to any of the connected SignalFire remote nodes wirelessly.

To start a remote configuration session with a remote node, select the checkbox next to the node to configure.



If the device has a non-sleeping radio the remote configuration session will be ready immediately. If it is a sleeping device, you must wait for the node to either check-in or send a "beacon" so that it can be commanded into configuration mode. The Sentinel nodes send a beacon every two and a half minutes, while all other sleeping nodes send a beacon every five and a half minutes. When the device has entered a remote configuration session you will see a message indicating the device is ready. Click **Configure** to open the configuration window

Make any necessary changes and click the **Apply All Settings** button to save the changes. When finished with the configuration, close the configuration window and then click the **End** button in the Gateway window to end the session. The session will also automatically time-out after 15 minutes of inactivity and the Node will resume normal operation.



Example Remote Configuration Window

Further information on how to remotely configure a HART device through the ToolKit using PACTware can be found in the "Remote HART Sensor Configuration Manual".

Remote Modbus Sticks and Sentinel-Modbus (non-sleeping radio only) Nodes

Remote nodes, that have been pre-configured, forward their set of registers to the Modbus gateway on a pre-defined schedule (1 minute to 5 minutes is typical). The register data is then buffered in the gateway and is available to be read by the RTU at any time.

If a Modbus request is received by the gateway for a Modbus ID and address for which buffered data does not exist, but the Modbus ID is known, the Modbus request will be forwarded to the remote Modbus node over the SignalFire network. The response is returned to the RTU.

If a request for multiple registers is issued by the RTU, and if the gateway does not have all registered data buffered, an exception will be returned. The system will not combine buffered and transparent data within a single Modbus response.

3. Radio Settings

The **Radio Settings** page allows you to configure the wireless communication parameters of the PATRIoT Gateway's internal radio module. This is essential for ensuring secure and reliable communication with remote nodes.

3.1 Radio Status

This section provides a quick overview of the radio module's current state:

- **Radio Module:** Indicates whether the radio hardware is detected
- **Firmware Version:** Displays the current firmware version of the radio
- **Node Address:** Unique identifier for the radio node (e.g., *98787*)

3.2 Device Settings

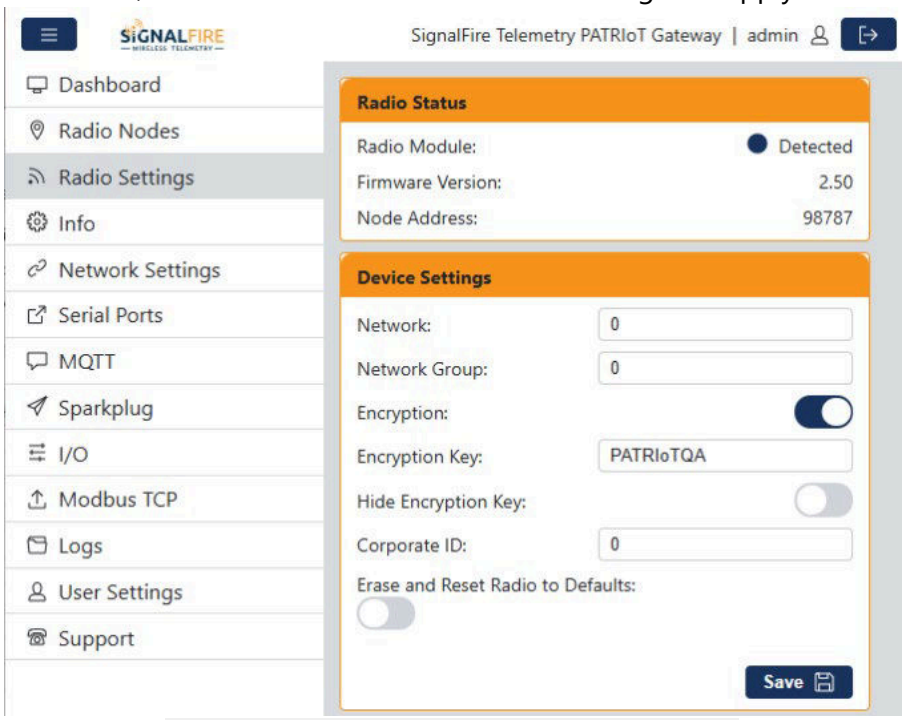
These settings define how the radio communicates within the network:

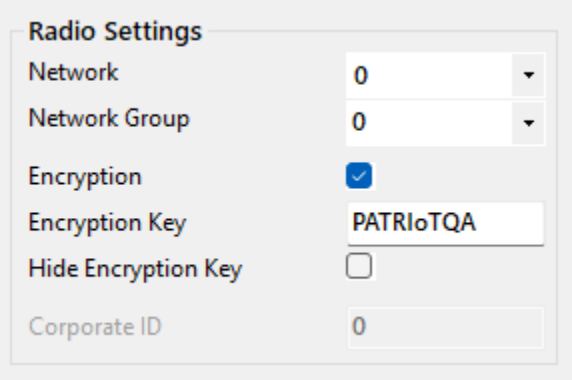
Setting	Description
Network	Configures the Radio Network Setting
Network Group	Configures the Radio Network Group Setting
Encryption Key	Security key used to encrypt radio communications
Hide Encryption Key	Toggle to hide the encryption key and make it unreadable
Corporate ID	For legacy systems not using encryption
Erase and Reset Radio to Defaults	Toggle to factory reset the radio settings

🔒 **Note:** Always ensure the Radio Network, Radio Network Group and Encryption key is consistent across all devices in the same network to maintain secure communication.

3.3 Save Changes

After making any modifications, click the **Save** button at the bottom right to apply the new settings.





4. Info Tab

The **Info** tab provides detailed diagnostics, configuration options, and maintenance tools for the PATRIoT Gateway. It is divided into five key sections:

4.1 Device Status

This section displays real-time system metrics and firmware details

4.2 Device Actions

These buttons allow you to manage firmware and restart the device:

1. **Reboot Device** – Immediately restarts the gateway.
2. **Upload Firmware to Gateway** – Allows manual firmware upload from a local file.
3. **Download Firmware From Update Server** – Automatically fetches the latest firmware from the SignalFire update server.

From the SignalFire ToolKit these options are in the **Updates** and **Tools** menu.

4.3 Device Settings

Customize the gateway's identity and communication ID:

- **Device Name:** Editable field (default: *SignalFire PATRIoT Gateway*)
- **Gateway Modbus ID (241–255):** Numeric input (e.g., *247*)
- **Erase Name & Modbus and Set to Defaults:** Toggle switch to reset these fields to factory defaults.

4.4 Clock Setting

Manually adjust the system clock:

- **Current Date and Time:** Editable fields (e.g., *07/29/2025 08:34 PM*)
- **Save Button:** Applies the new time settings.

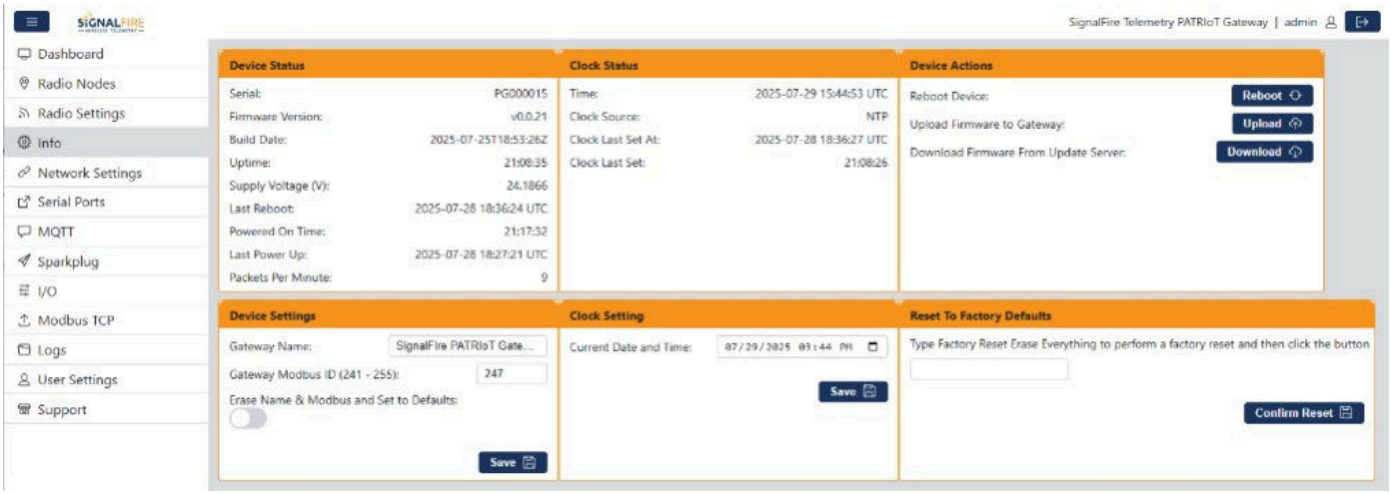
4.5 Reset to Factory Defaults

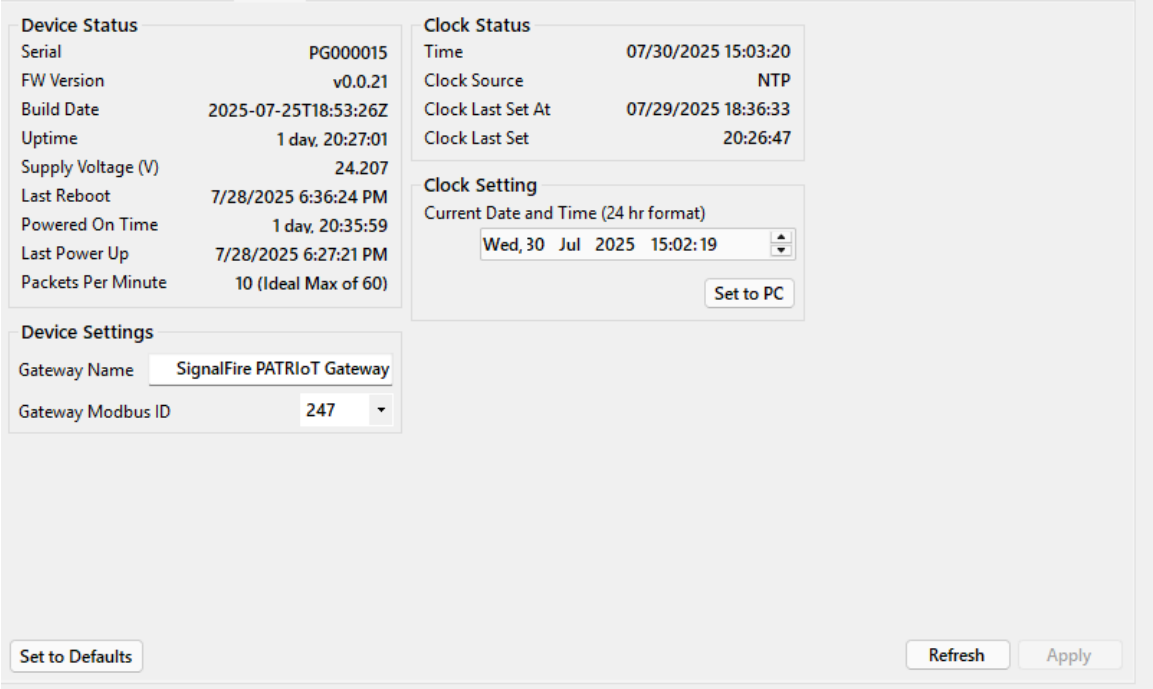
To perform a full factory reset:

1. Type the phrase: **Factory Reset Erase Everything**
2. Click the **Confirm Reset** button

From the SignalFire ToolKit this option is in the **Tools** menu.

⚠ **Warning:** This action will erase all configuration data and restore the gateway to its original factory state.





5. Network Settings

The **Network Settings** tab allows you to configure Ethernet connectivity, DNS, NTP synchronization, and web access for the PATRIoT Gateway.

5.1 Network Status

This section displays the current state of the Ethernet interface

5.2 Network Time Protocol (NTP) Status

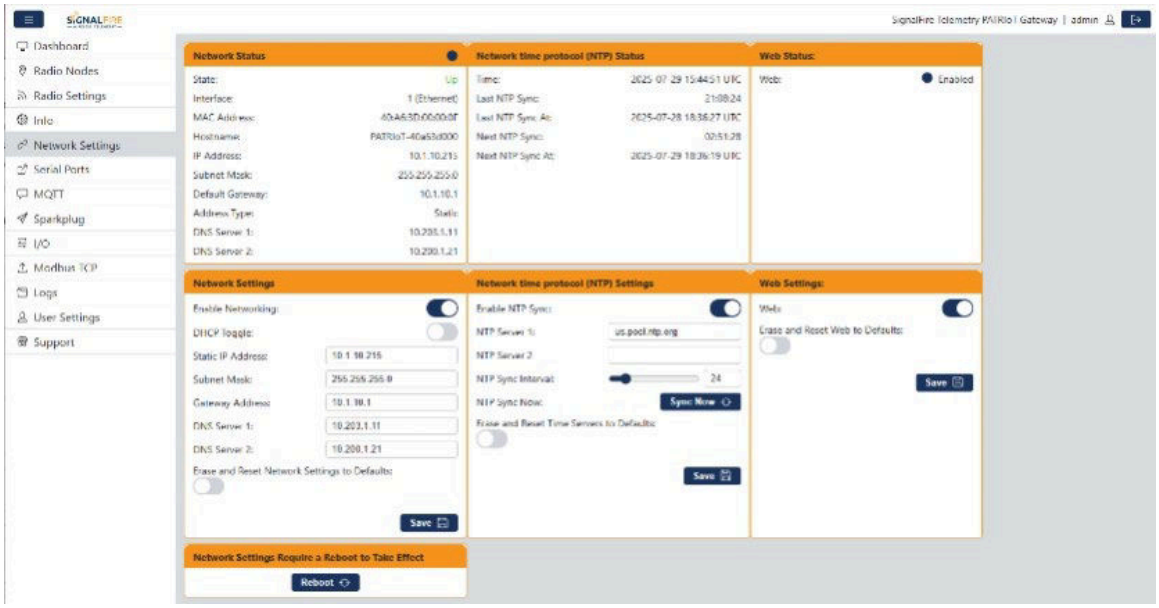
This section displays the current state of the Time server

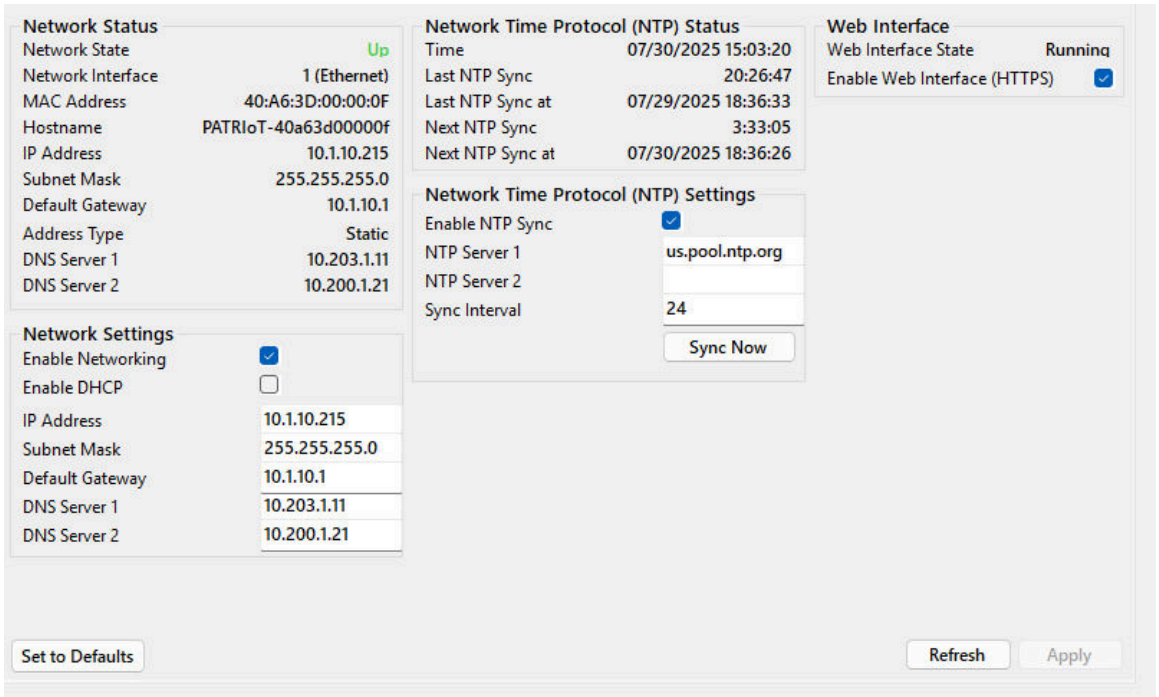
5.3 Web Status

- **Web Enabled:** Indicates that the web interface is currently active.

5.4 Editable Network Settings

Setting	Description
Enable Networking	Toggle to activate/deactivate the Ethernet network interface
DHCP	Toggle to enable dynamic IP assignment
Static IP Address	Manually assigned IP
Subnet Mask	Network mask
Gateway Address	Router IP
DNS Server 1 & 2	Primary and secondary DNS servers





6. Serial Port Settings

The **Serial Ports** tab allows you to configure the communication parameters for the gateway's physical serial interfaces. These settings are essential for integrating with Modbus RTU devices or other serial-based equipment.

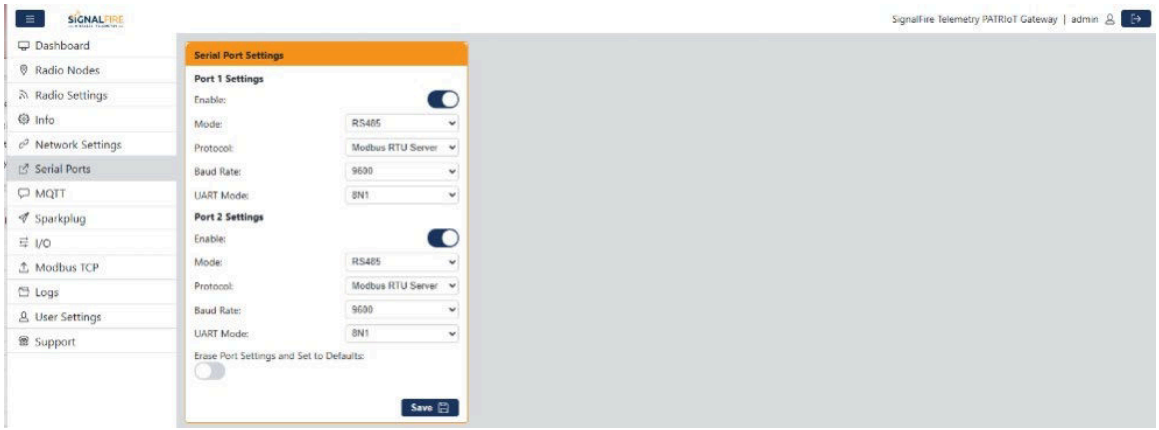
6.1 Port 1 and Port 2 Configuration

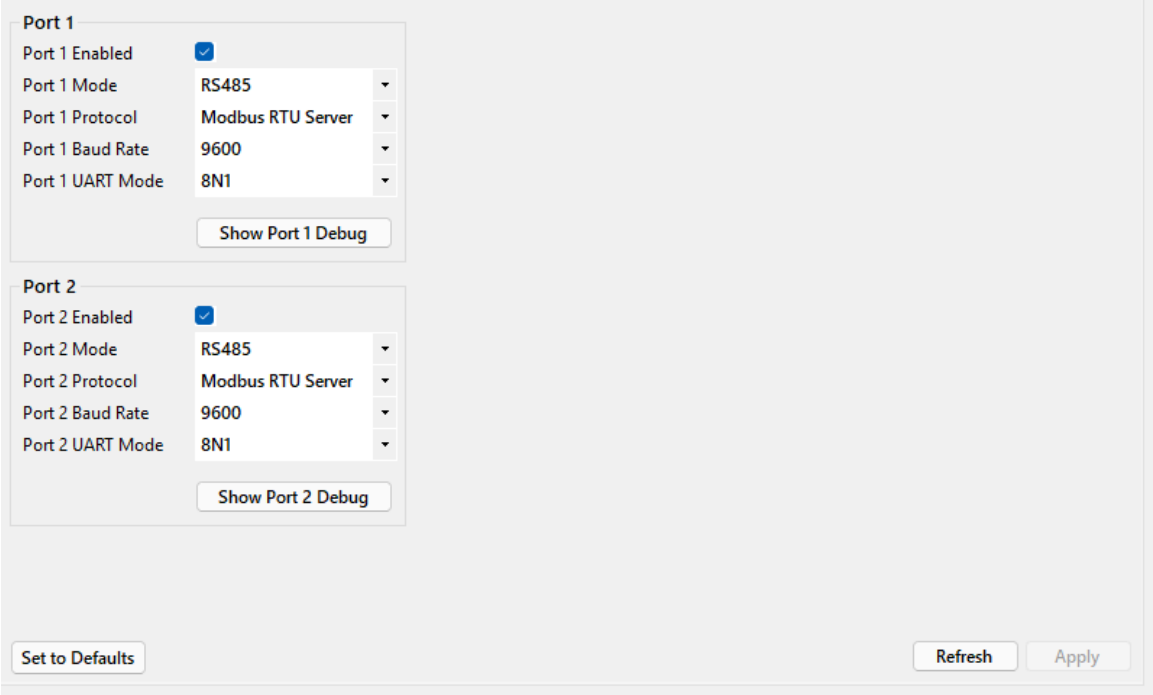
Setting	Description
Enable	Toggle switch to activate Port
Mode	Electrical interface type (e.g., *RS485, RS232, RS485 with termination resistor*)
Protocol	Communication protocol (e.g., *Modbus RTU Server*)
Baud Rate	Transmission speed (e.g., *9600 bps*)
UART Mode	Data format (e.g., *8N1* = 8 data bits, No parity, 1 stop bit)

💡 **Tip:** Ensure that the baud rate and UART mode match the settings of the connected Modbus devices to avoid communication errors.

6.2 Reset and Save Options

- **Erase Port Settings and Set to Defaults:** Toggle switch to restore factory defaults for both ports.
- **Save Button:** Applies all changes made to the serial port configurations.





7. MQTT Configuration

The **MQTT** tab allows you to configure how the PATRIoT Gateway communicates with MQTT brokers for telemetry data transmission. This includes connection status, broker settings, and security options.

7.1 MQTT Status (Left Panel)

Field	Description
State	Indicates current connection status (e.g., *CONNECTED*)
Broker Hostname	DNS name of the connected broker
Broker Address	IP address or URL of the broker
TLS Encryption	Whether Transport Layer Security is enabled
TLS Certificate	Certificate used for secure communication
QoS (Quality of Service)	Level of message delivery assurance
Keepalive Interval	Time interval (in seconds) to maintain connection with broker

7.2 MQTT Client Enable Settings (Right Panel)

You can configure up to three MQTT brokers. The PATRIoT will only connect to one broker at a time, but if the connection is lost it will move to the next broker in the list in a round-robin fashion.
Each broker has the following fields:

Setting	Description
Hostname	Broker's DNS name or IP address
Port	Communication port (typically 1883 for non-TLS, 8883 for TLS)
Client ID	Unique identifier for the gateway on the broker

Setting	Description
QoS	Message delivery level (0, 1)
Keepalive Interval	Time in seconds to keep the connection alive
TLS Level	Security level for encrypted communication
Security Tag	Optional tag for managing certificates or credentials
Username	Username for the MQTT connection
Password	Password for the MQTT connection

7.3 Reset and Save Options

- **Erase and Reset MQTT to Defaults:** Restores all MQTT settings to factory defaults.
- **Save Button:** Applies all changes made to the MQTT configuration.

Tip: Always verify TLS and certificate settings when connecting to secure brokers to ensure encrypted data transmission.

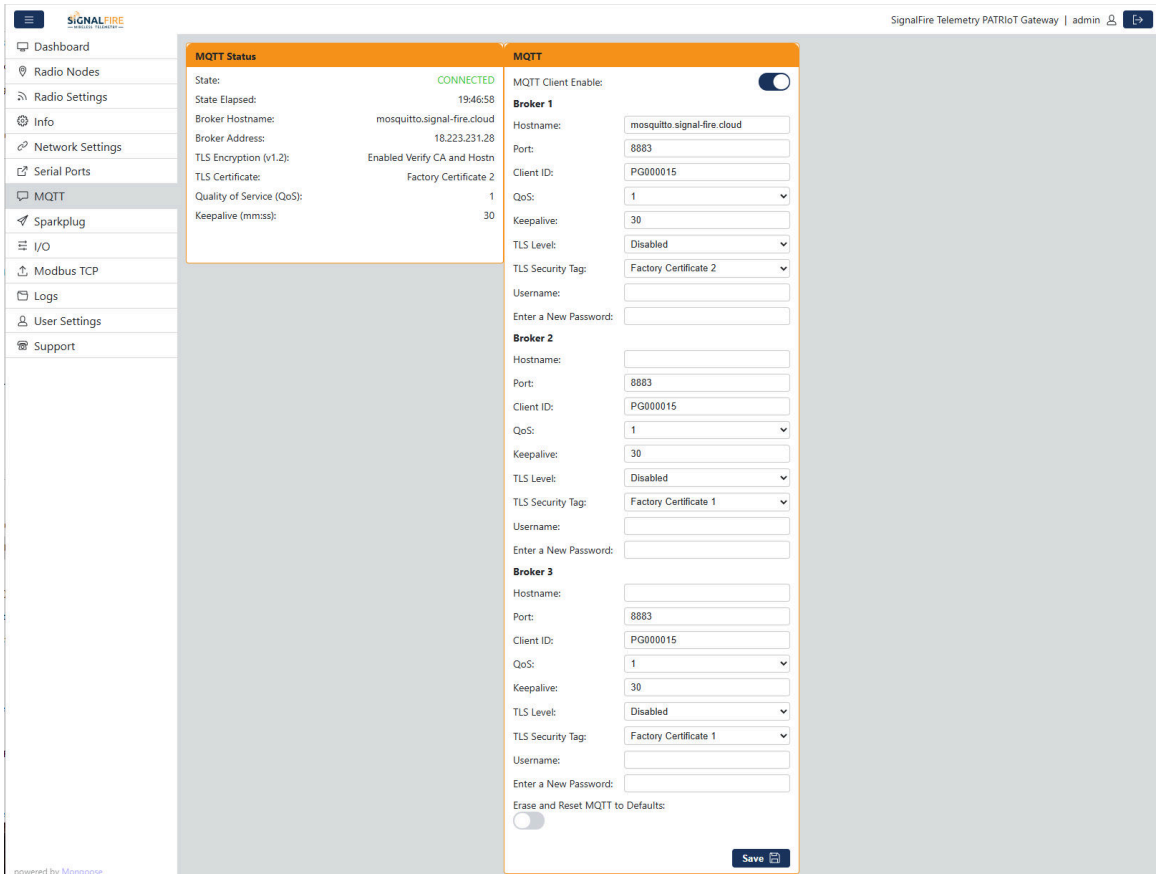
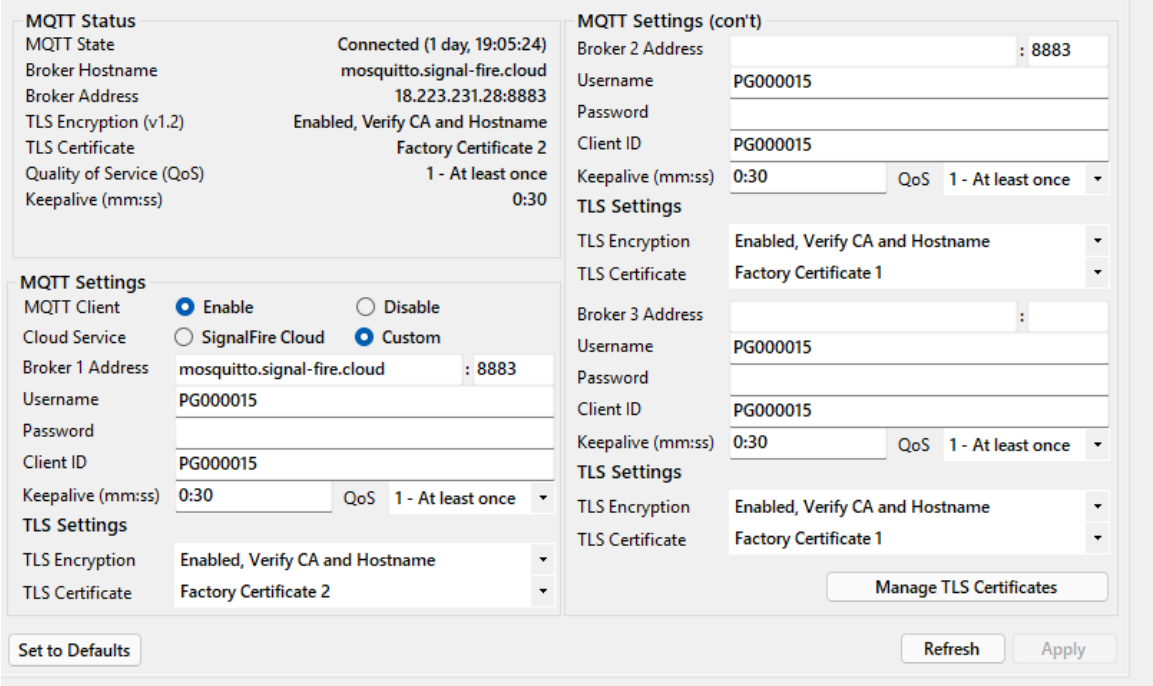


Figure 2



8. Sparkplug Configuration

The **Sparkplug** tab is used to configure the gateway's behavior when publishing telemetry data using the Sparkplug B protocol over MQTT. This is particularly useful for integration with SCADA systems and IIoT platforms like Ignition.

8.1 Sparkplug Status

Field	Description
Server State	Indicates the current connection status (e.g., *ONLINE*)
Server State Elapsed	Duration the server has been online
Server Host ID	Identifier of the MQTT broker or host
Namespace	Sparkplug namespace (e.g., *spBv1.0*)
Group ID	Logical group for Sparkplug messages
Edge Node ID	Unique ID for this gateway (e.g., *PG000015*)
Birth/Death Sequence	Sequence number for lifecycle events
Publish Sequence	Sequence number for data messages
Report Count	Number of published message

8.2 Sparkplug Settings

Setting	Description
Group ID	Logical group name for Sparkplug messages
Edge Node ID	Unique identifier for the gateway (e.g., *PG000015*)

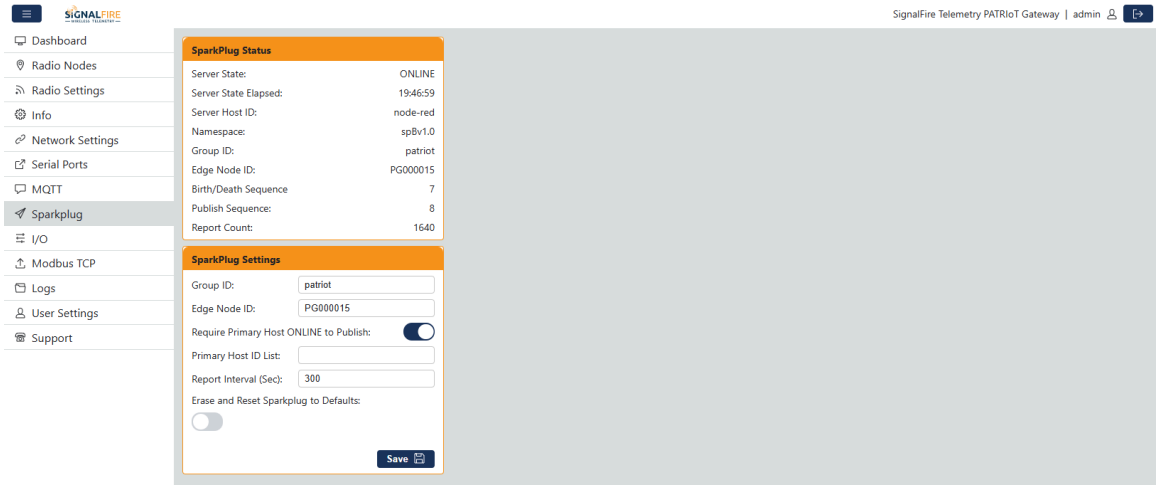
Setting	Description
Require Primary Host ONLINE to Publish	Toggle to restrict publishing unless the primary host is online (enabled)
Primary Host ID List	Optional list of host IDs that must be online before publishing
Report Interval (Sec)	Frequency of data publishing in seconds (e.g., *300*)

Erase and Reset Sparkplug to Defaults: Toggle to restore default Sparkplug settings

8.3 Save Changes

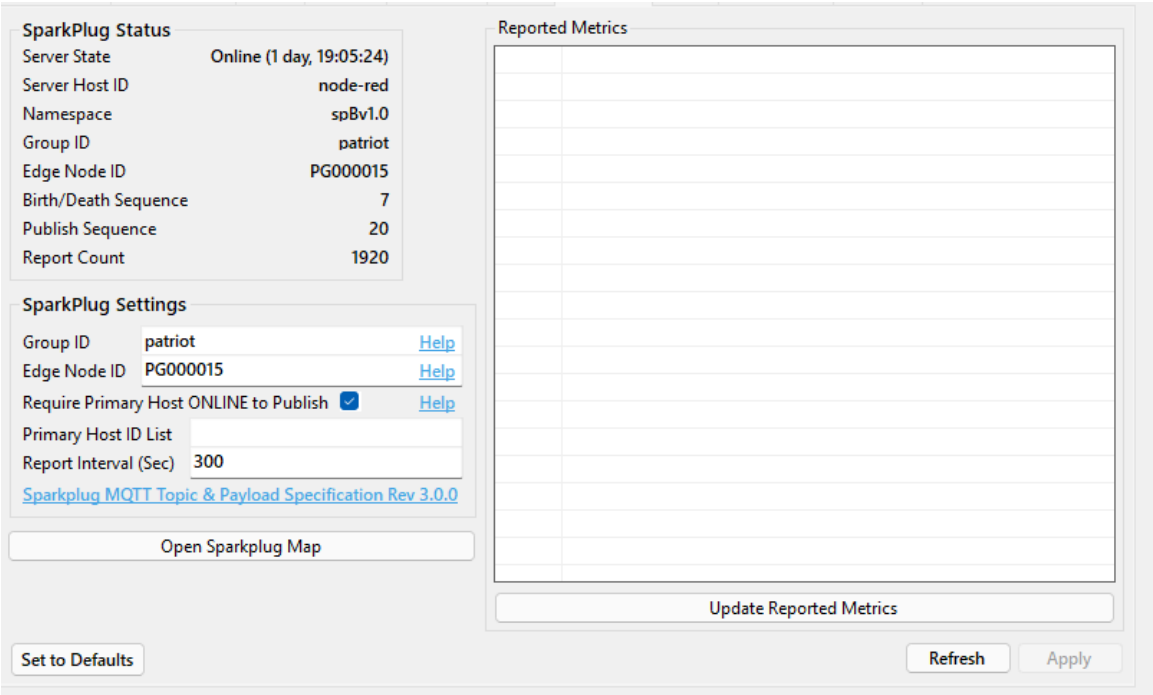
Click the **Save** button to apply any changes made to the Sparkplug configuration.

Tip: Ensure the Group ID and Edge Node ID are unique within your Sparkplug network to avoid data collisions.



8.4 Reported Metrics

The ToolKit also displays a list of the reported Sparkplug metrics if configured.



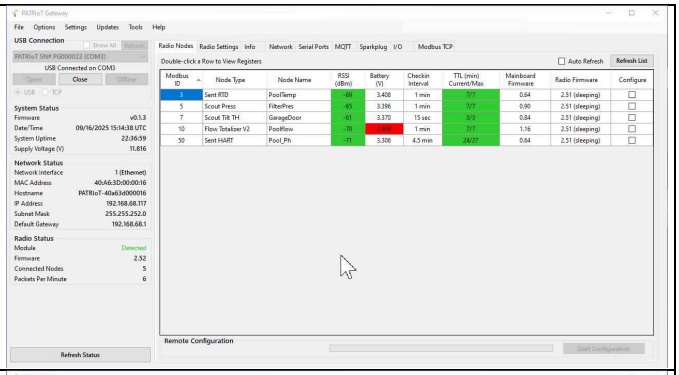
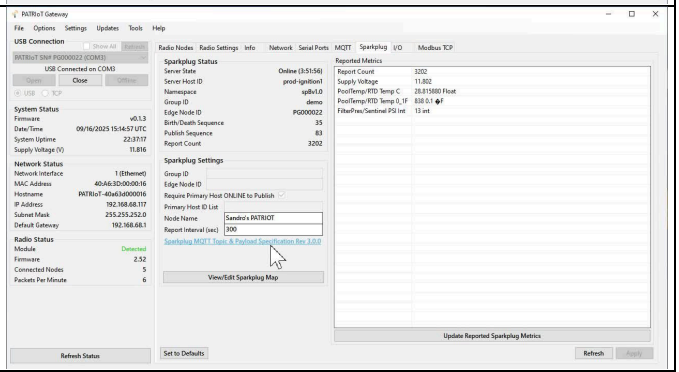
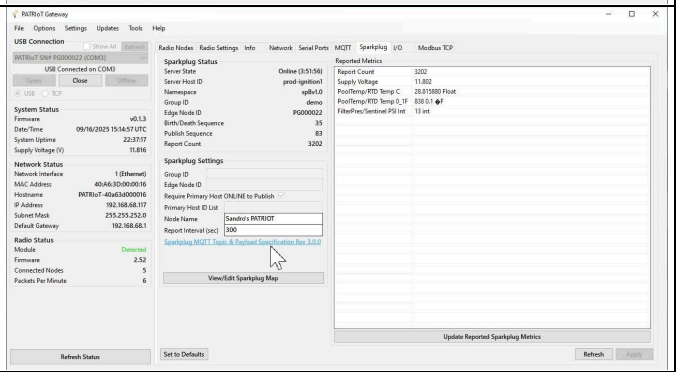
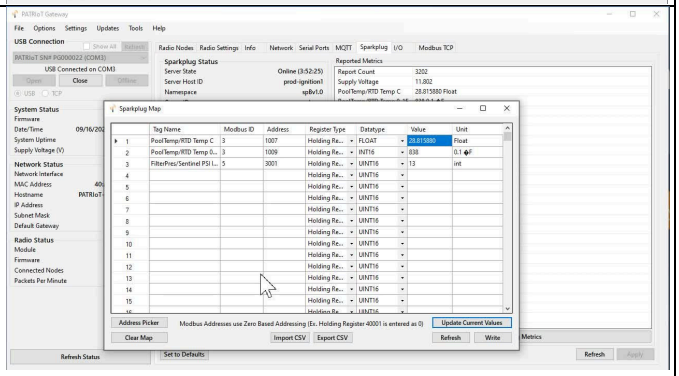
8.5 Configuring SparkPlug Using SignalFire Toolkit

Creating a Sparkplug Map in PATRIoT Gateway

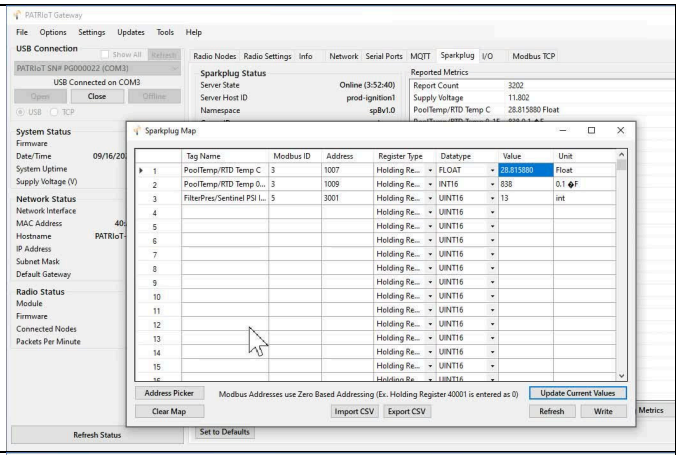
The PATRIoT gateway can publish all measurements using the MQTT/SparkPlug standard. In order to publish to MQTT the connection to the MQTT broker must be established, and all data to publish must be added to the Sparkplug map.

The following steps are necessary to publish the measurements, also known as MQTT Tags.

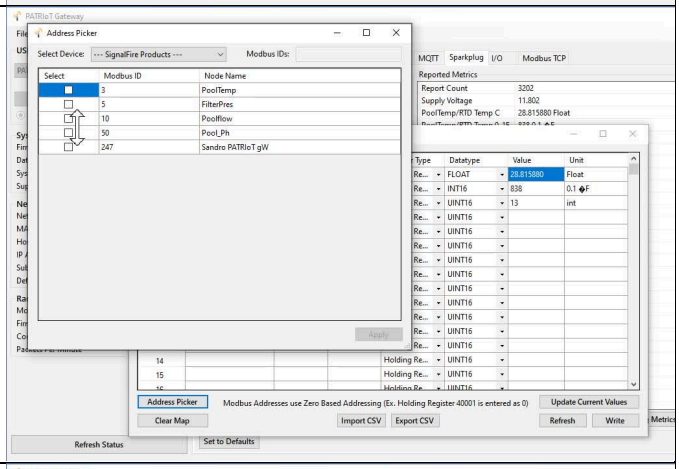
Configure MQTT Settings	This step is to setup the gateway to publish the data to an MQTT Broker. The MQTT Broker is hosted by SignalFire when using the SignalFire Cloud and it is already setup in the PATRIoT gateway. A subscription to the SignalFire Cloud is necessary. Contact SignalFire to obtain a subscription When using a different broker, it is necessary to setup the gateway's MQTT communication settings so that the PATRIoT can successfully connect to the MQTT Broker.
Configure SparkPlug Settings	This step is to setup the Node Name as it will appear to a Broker and a Subscriber. It is also to setup how often the data is sent to the broker (Report Interval). When using a broker other than SignalFire's, additional setup is necessary for the GroupID and EdgeNodeID. The SparkPlug specification contains information on how to use the GroupID and EdgeNodeID.
Create A List Of Tags To Be Published	This is the step to associate the PATRIoT's measurements or output signals with corresponding SparkPlug Tags. Using the SignalFire Toolkit Software, the tags are created using the Address Picker. When connecting to a broker, these tags will be published for a subscriber to use.

Step 1: Access the Sparkplug Section Open the PATRIoT Gateway window. Click on the Sparkplug section to begin the configuration.	
Step 2: Configure the PATRIoT Gateway Name Change the Node name of the PATRIoT Gateway. This name will be presented to the MQTT Sparkplug host.	
Step 3: Set the Report Interval Adjust the report interval for how often MQTT tags will be published to the Sparkplug-ready host.	
Step 4: Create the Sparkplug Map You can use a CSV file to create the list of Sparkplug Tags. Click on EXPORT CSV to get a template to use. Then fill in the Template and import into the table by clicking IMPORT CSV. or Click on the Address Picker to open the table that displays the tags generated from Modbus IDs and addresses available at the Gateway. From there you can select the Modbus IDs and associated tags. See Step 5.	

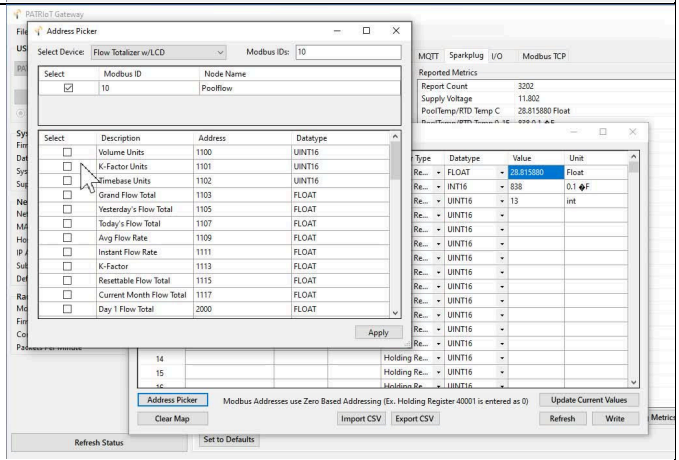
Step 5: Use the Address Picker
Click on the address picker to view all available Modbus IDs connected to the PATRIoT Gateway.



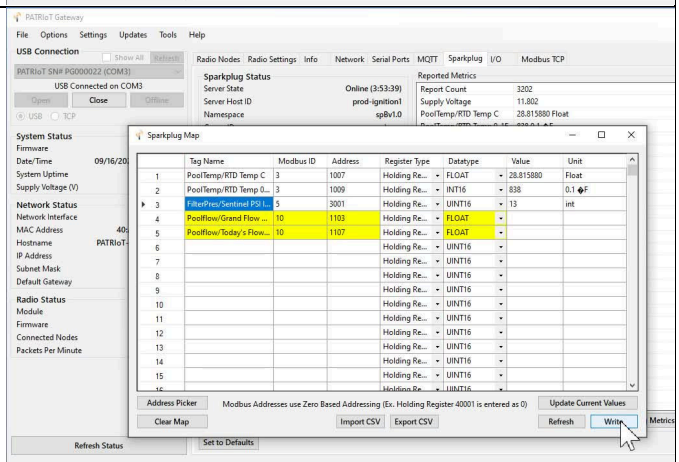
Step 6: Select a Modbus ID
Click on a Modbus ID to view relevant Modbus tags associated with it.

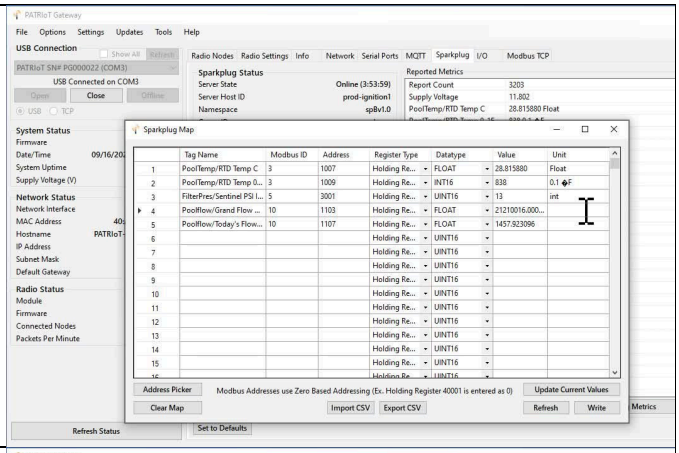
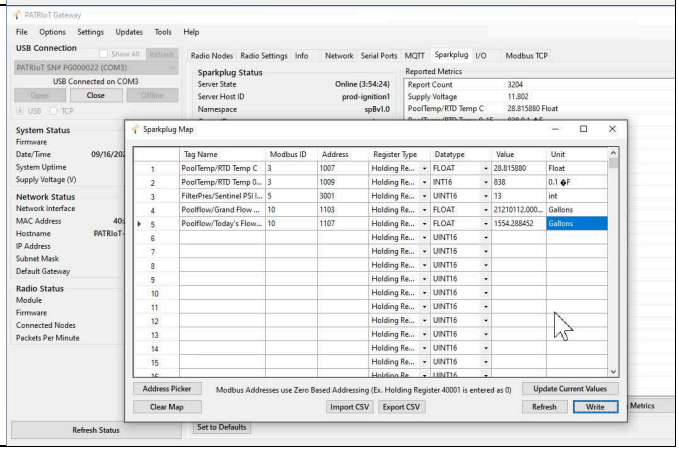


Step 7: Choose Modbus Registers
Select one or more Modbus registers of interest.
Click 'Apply' to add them as MQTT tags.



Step 8: Write the New Map
Modify the Tag Name as needed. The default Tag Name will be the Modbus Registers Name for SignalFire Devices. Note that the forward slash can be used to organize the tags in folders on the MQTT host.
Click 'Write' to save the new map to the PATRIoT Gateway.
The row will be colored Yellow for pending changes.
Verify that the current value of the Modbus register appears as an MQTT tag value.



Step 9: Enter Units for MQTT Tags Registers added from SignalFire nodes will have the default units already filled in. For data coming from Modbus devices, type in the units for each MQTT tag in the designated column. Click 'Write' again to save the units.	
Step 10: Finalize the Sparkplug Map Review the Sparkplug map to ensure all Modbus registers from various Modbus IDs are correctly added.	

9. I/O Configuration

The **I/O** tab provides real-time status monitoring and manual control of the gateway's digital input and output channels. This is useful for diagnostics, remote control, and integration with external devices.

9.1 I/O Status

This panel displays the current state of each digital input and output:

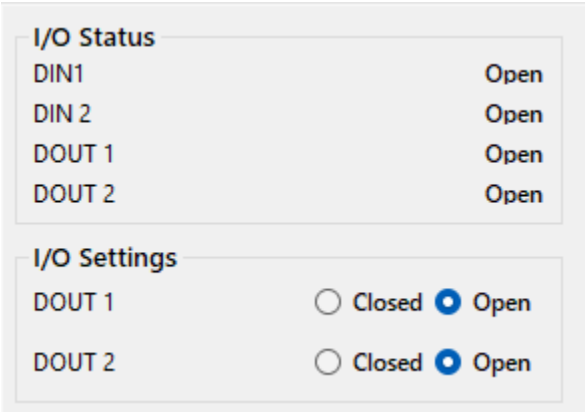
Channel	Status
DIN1	Open
DIN2	Open
DOUT1	Open
DOUT2	Open

9.2 I/O Settings

This panel allows manual control of the digital outputs:

Output	Control
DOUT1	Toggle switch (currently OFF)
DOUT2	Toggle switch (currently OFF)

Save Button: Applies any changes made to the output states.



10. Modbus TCP Configuration

The **Modbus TCP** tab allows you to monitor and configure the gateway's Modbus TCP server, which enables communication with SCADA systems and other Modbus-compatible clients over Ethernet.

10.1 Modbus TCP Status

This panel provides real-time metrics on server activity:

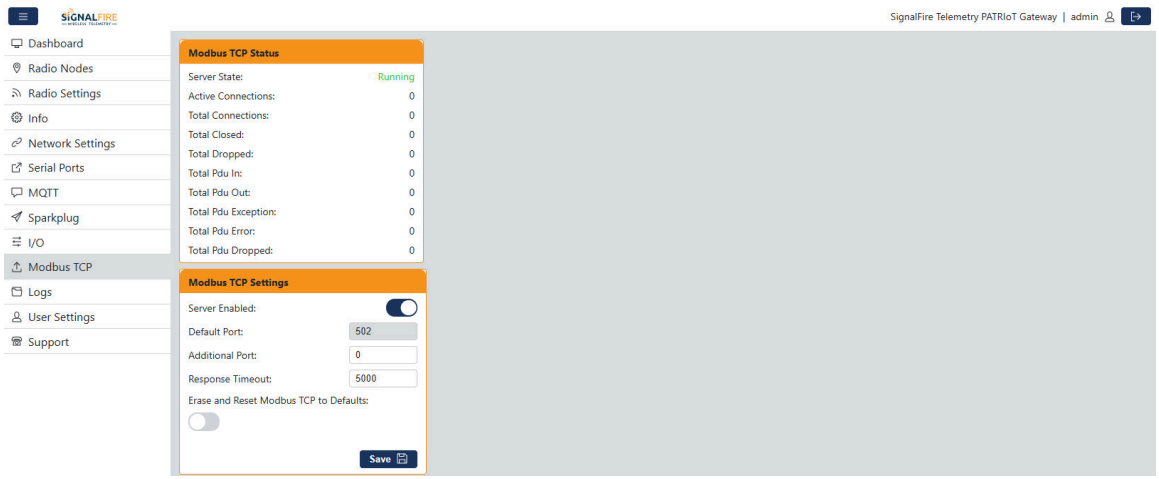
Metric	Description
Server State	Indicates if the Modbus TCP server is active (e.g., Running)
Active Connections	Number of currently connected clients (e.g., 0)
Total Connections	Total number of connections since startup
Total Closed	Number of connections that were closed normally
Total Dropped	Number of connections dropped due to errors or timeouts
Total PDU In	Protocol Data Units received
Total PDU Out	Protocol Data Units sent
Total PDU Exception	Number of Modbus exception responses sent
Total PDU Error	Number of Modbus error responses
Total PDU Dropped	Number of PDUs dropped due to errors or timeouts

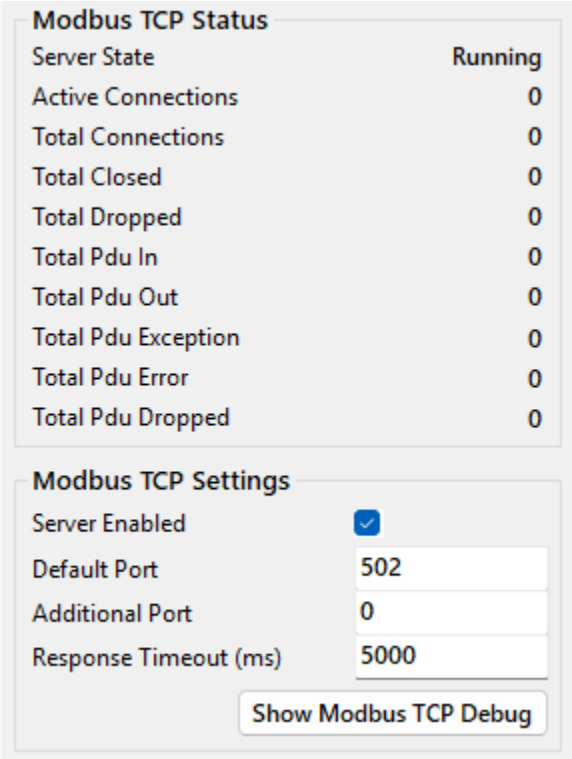
10.2 Modbus TCP Settings

Setting	Description
Server Enabled	Toggle to activate or deactivate the Modbus TCP server
Default Port	Standard Modbus TCP port (always available if Modbus-TCB is enabled)
Additional Port	Optional secondary Modbus-TCP port
Response Timeout (ms)	Time to wait for a response before timing out

10.3 Reset and Save Options

- **Erase and Reset Modbus TCP to Defaults:** Checkbox to restore factory settings.
- **Save Button:** Applies all changes made to the Modbus TCP configuration.





11. Logs

The **Logs** tab provides access to diagnostic and operational logs that are essential for troubleshooting, system auditing, and performance analysis. From the ToolKit logs are available from the **Tools** menu.

11.1 Log Categories

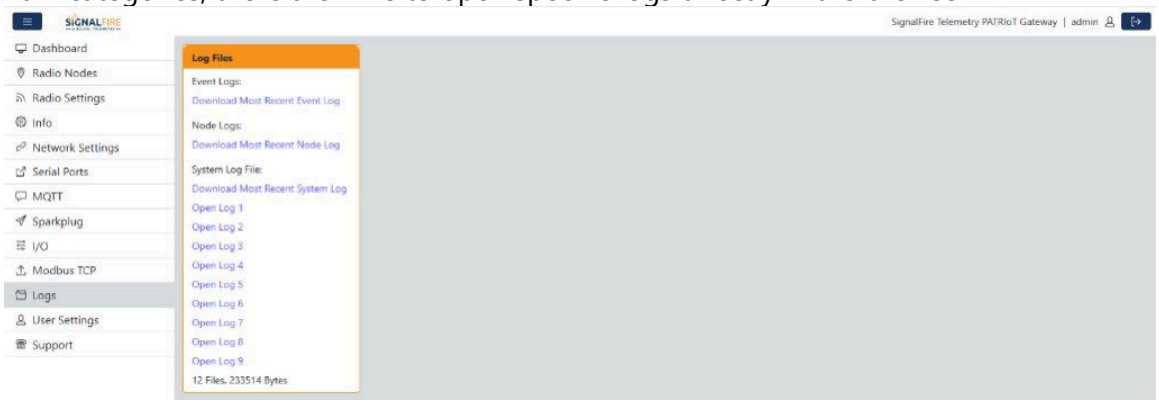
Log Type	**Description**
Event Logs	Captures system-level events such as reboots, configuration changes, and alerts.
Node Logs	Records activity and communication from connected radio nodes.
System Log File	Contains detailed system diagnostics and runtime information.

Each category includes a link to:

- **Download Most Recent [Log Type]** – Retrieves the latest log file for offline review.

11.2 Individual Log Access

Below the main categories, there are links to open specific logs directly in the browser



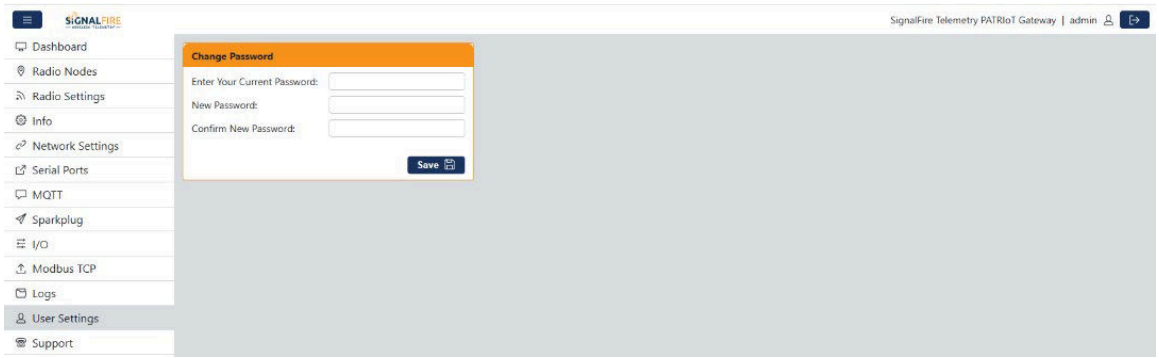
12. User Settings

The **User Settings** tab allows administrators to manage account security by updating the login password for the web interface.
In the ToolKit the password setting is in the **Settings** menu.

12.1 Change Password

To update your password:

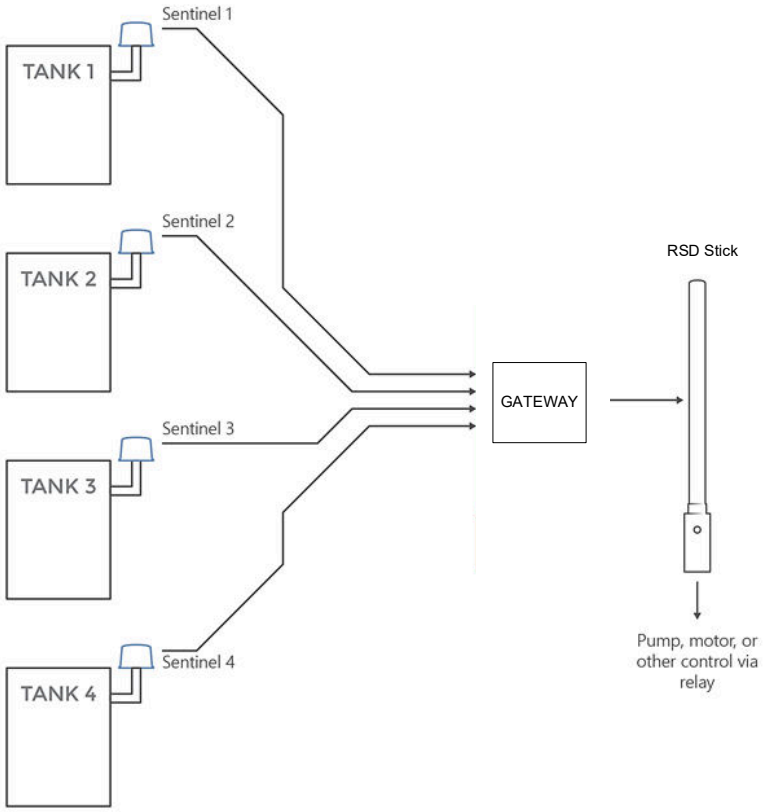
1. **Enter Your Current Password** – Required to authorize the change.
2. **New Password** – Enter your desired new password.
3. **Confirm New Password** – Re-enter the new password to confirm.
4. **Save Button** – Click to apply the password change.



13. Remote Shutdown (RSD)

The SignalFire Gateway supports **Internal Logic Control** capability which enables the Gateway to control output relays on any SignalFire device with Digital Outputs including the RSD stick, WIOM, WIOM-Mini, Gateway Output modules and the Gateway's built in DO's. The PATRIoT Gateway supports a maximum of 128 logic rules for remote shutdown.

The PATRIoT Gateway receives data from multiple remote nodes. It can use the data from those remote nodes to set the relay output on one or more remote relays. An example of the topology is shown in the following figure:

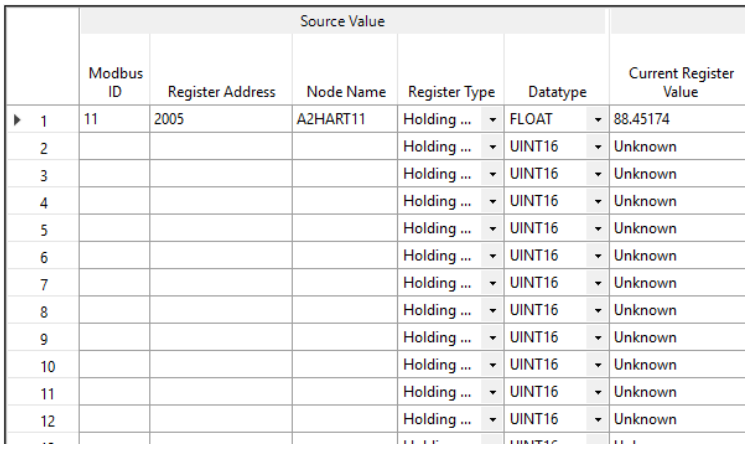


13.1 RSD Configuration

From the Gateway configuration window within the SignalFire Toolkit, go to the **Settings** menu and select **Remote Shutdown Settings**. This will open the RSD configuration window.

Source Value

The 'Source Value' section is used to select the source register for the logic rule.



	Source Value					
	Modbus ID	Register Address	Node Name	Register Type	Datatype	Current Register Value
▶ 1	11	2005	A2HART11	Holding ...	FLOAT	88.45174
2				Holding ...	UINT16	Unknown
3				Holding ...	UINT16	Unknown
4				Holding ...	UINT16	Unknown
5				Holding ...	UINT16	Unknown
6				Holding ...	UINT16	Unknown
7				Holding ...	UINT16	Unknown
8				Holding ...	UINT16	Unknown
9				Holding ...	UINT16	Unknown
10				Holding ...	UINT16	Unknown
11				Holding ...	UINT16	Unknown
12				Holding ...	UINT16	Unknown

Modbus ID – The Modbus ID of the source node.

Register Address – Enter the register address for the data to use for the logic, or manually enter the Address Picker to automatically populate.

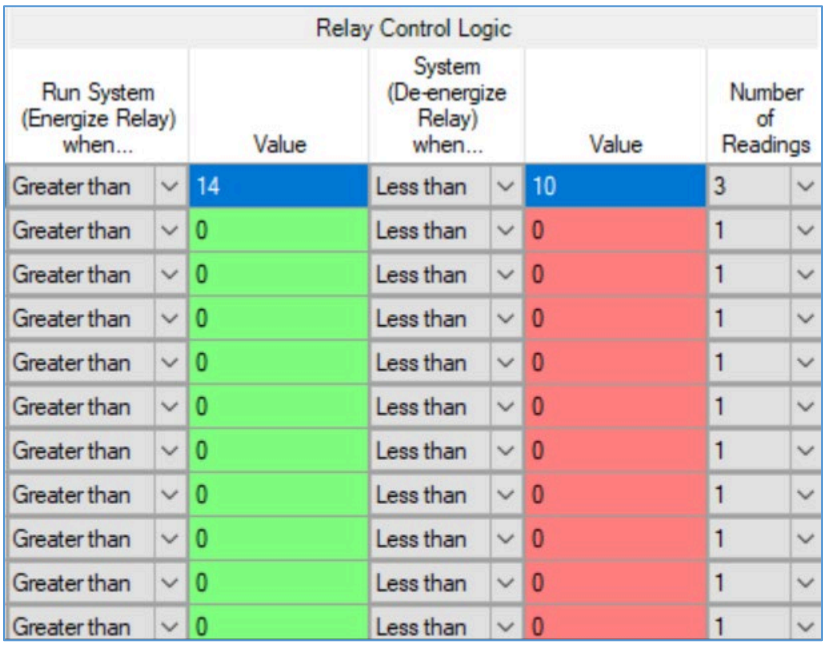
Node Name – This will be populated with the configured Node Name

Register Type – The correct register data type will be automatically selected if the Address Picker is used, if the address is manually entered select the correct data type here.

Current Register Value – Displays the value of the selected source data register. Clicking the **Update** button will refresh this value after the table has been saved to the Gateway

13.2 Relay Control Logic

The 'Relay Control Logic' section is used to set the trigger thresholds for the selected source data register.



Run System (Energize Relay) – Select the logic operand to use for the "energize" logic evaluation.

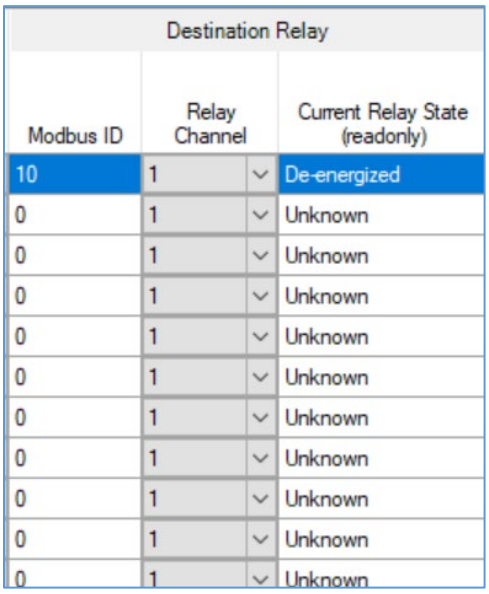
Value – The value that the relay will be energized. Note that the energized state is the normal "operating" state of the relay.

Shutdown System (De-Energize Relay) – The logic operand to use for the "de-energize" logic evaluation. This will automatically be the opposite of the selection for the energize case. Note that the de-energized state is the SAFE state of the relay.

Value – The value that the relay will be de-energized. Note that the de-energize state is the "safe" state of the relay.

Number of Readings – This field contains the number of check-in packets that must be received in a row that are above (or below) the logic threshold for the de-energize condition. This is useful so that a single (possibly a glitch) reading does not cause a shut-down. The default is 1 where each check-in will cause the rule to be evaluated and acted on. A single reading that satisfies the run system (energize) condition will cause the relay to energize.

13.3 Destination Relay



Modbus ID – The Modbus ID of the remote relay node (RSD Stick, WIOM Module Etc.) or the Modbus ID of the Gateway (default 247) for the local digital outputs or attached Gateway output modules.

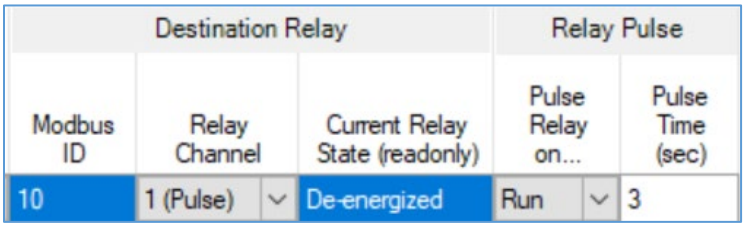
Relay Channel – Select the relay or digital output channel to switch

Current Relay State – Shows the last value of the relay or digital output as reported to the gateway. Clicking the Update button will refresh this value.

After filling out the table click **Write to PATRIoT** to store the setting in the Gateway.

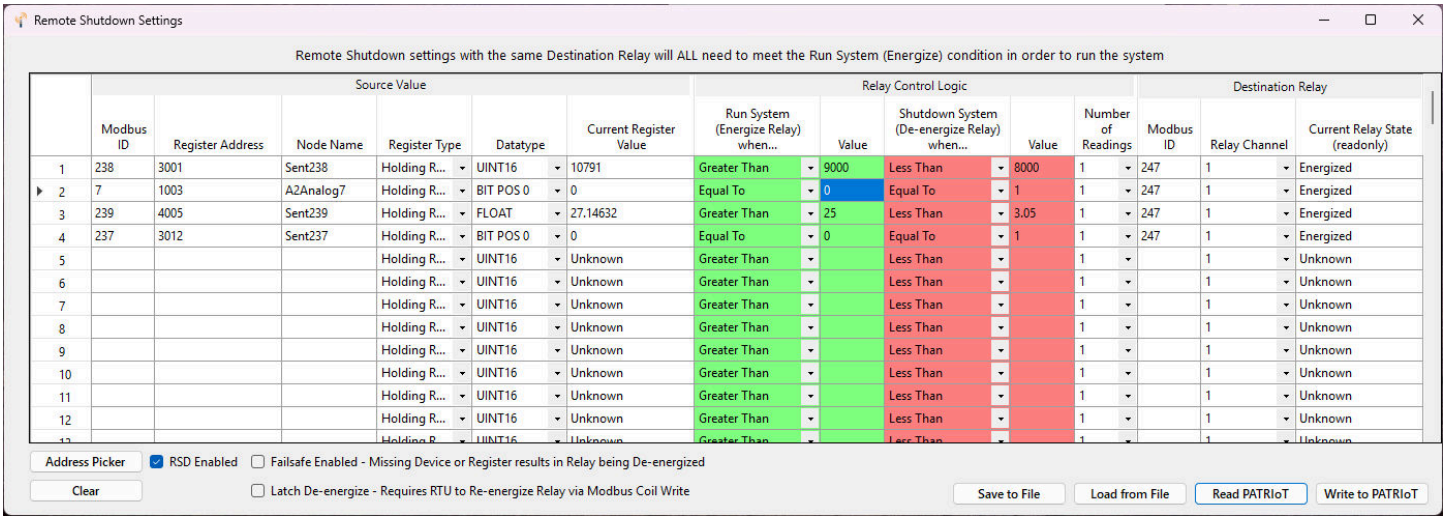
Relay Pulse

Destination relays can be configured to pulse instead of being permanently energized or de-energized. To do so, in the **Relay Channel** drop-down menu, select the same relay but in "(Pulse)" mode. Specify whether to pulse during run or shutdown, and specify the pulse duration.



13.4 RSD Table Example

Line 1 has been configured with a source data node as a Sentinel-Analog with the loop current (in µA) as the selected register. The relay will energize when the loop current is above 9000µA (9mA) and de-energize when the loop current is below 8000µA (8mA). Note that this configuration has a 1000µA (1mA) hysteresis factor.



In this example all 4 source nodes are assigned to the same destination Modbus ID and relay channel so the following statement applies:

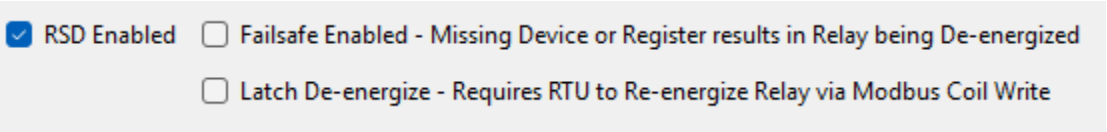
> **If more than one rule is assigned to the same destination RSD Stick and relay channel, then all the rules must meet the energize condition for the remote relay to be energized. In other words, the RSD table logic is a Boolean AND.**
>
> **Alternatively, this means that if any one of the four source node's logic results in the "de-energize" condition being true the relay will be de-energized (safe).**

13.5 RSD Event log

The RSD events will be stored in the gateway internal event log which can be read using the ToolKit. Additionally, a basic RSD event log containing the last 5 RSD events is available to be read via Modbus from registers 7000-7024. See the Modbus register map for details. The Modbus event log it not maintained through gateway resets.

13.6 Additional RSD Options

There are three check boxes for additional logic options.



RSD Enabled – For the RSD logic to run, the RSD Enabled check box must be selected. Unselect this box to pause/stop the RSD logic from running.

Failsafe Enabled – If this option is selected **all** rules must have valid data for the relay to be energized. If one or more of the nodes times-out or does not exist the relay will be de-energized.

If this option is not selected, then a node that is not installed or fails to check in will be ignored and the relay will be energized using logic only from the units that are active.

Latch De-Energized – If this option is selected the rules may only de-energize the relay. For the relay to be energized again a Modbus write from a PLC to the gateway for the destination RSD stick relay must occur. This is useful if manual intervention is required before the relay is energized after an event. In the example above, a Modbus coil write to Modbus ID 5 relay channel 1 (which is register 1) is required to energize the relay. See the RSD Stick manual for a detailed register map. If this option is selected, the relay(s) will be forced de-energized when the RSD settings are saved to the gateway, requiring a PLC write to the relay to energize the relay and enter the run state.

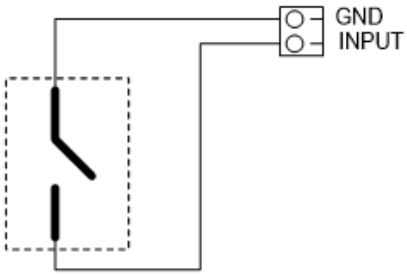
The "Normal" state of the relay or digital output is the un-energized state and this state should be used to set the controlled system (pump, motor,…) in the "safe" or "off" state. In the un-energized state the relay COM will be connected to the relay NC terminal. The device should be wired so that when the relay is in this state the system is running. When energized (shut down state) the relay COM will be connected to the NO terminal

14. Local Input/Output

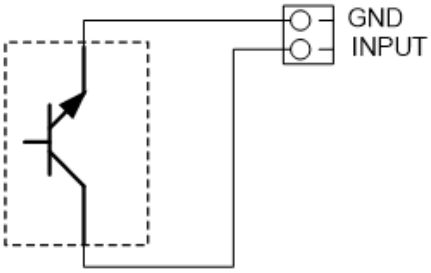
The PATRIoT Gateway v2 has I/O capability built into it locally, with 2 digital inputs, and 2 digital outputs. The state of these inputs and outputs can be viewed by clicking on the **I/O tab in the ToolKit**.

14.1 Digital Inputs

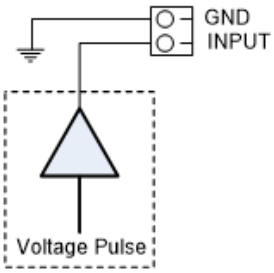
The Gateway has 2 digital inputs, sharing a GND terminal. Digital outputs may be connected to the Gateway as shown in the following diagrams:



Dry Contact Connection



Open Collector Connection

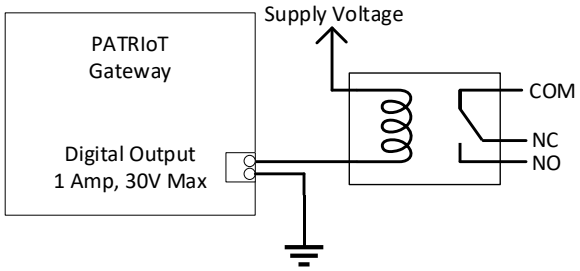


Voltage Pulse Connection

14.2 Digital Outputs

The PATRIoT Gateway has two local open collector. These can be controlled either like any other digital output using the RSD logic table seen above, by writing to registers on the Gateway.

The open collector output can control a relay when wired as shown below.

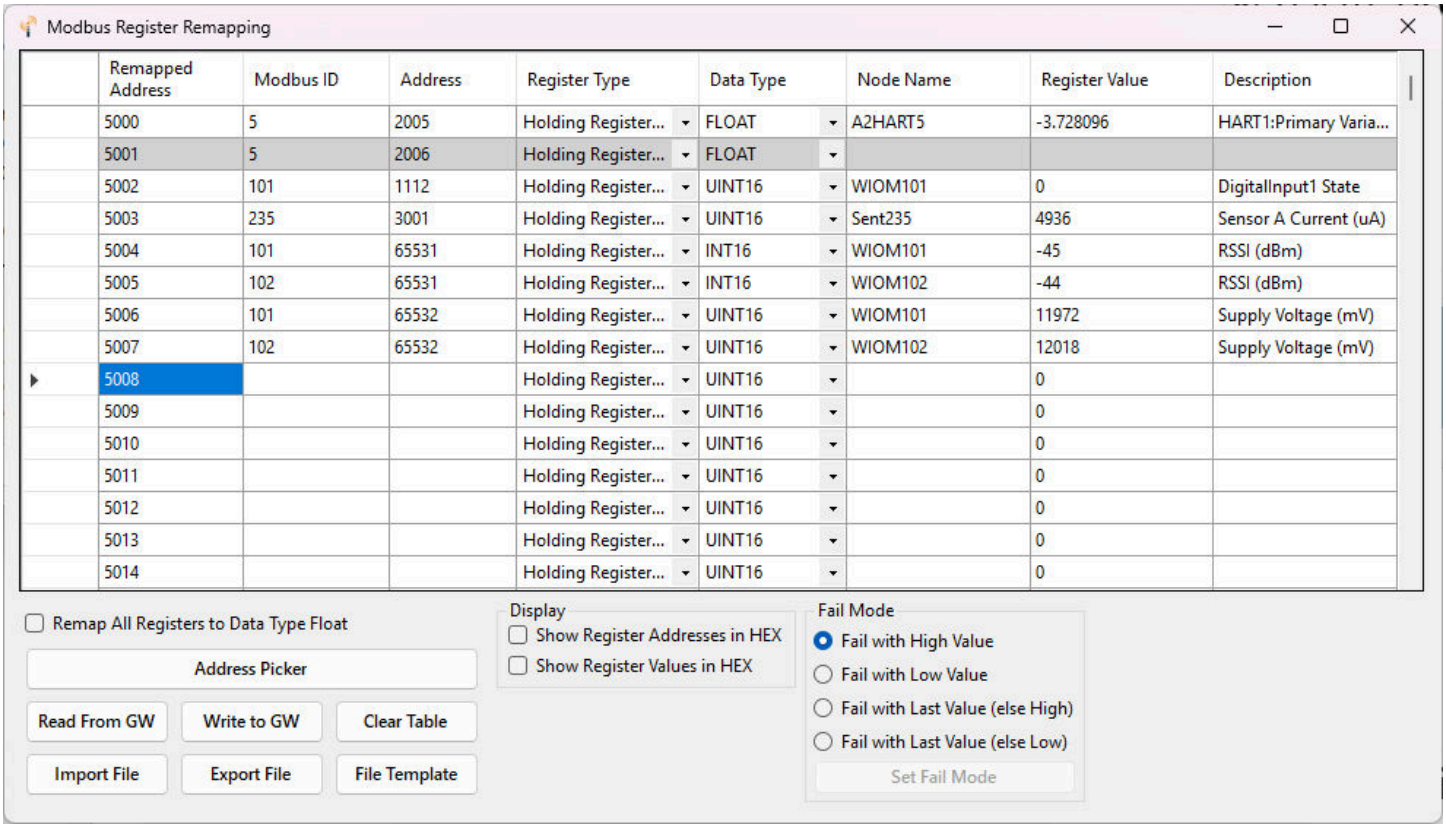


Note: The digital outputs on the gateway have built in protection and can drive relays and inductive loads directly.

15. Modbus Register Remapping

The PATRIoT gateway allows any of the remote register data to be remapped to a single block of registers available at the Gateway's Modbus ID (default is 247). This is useful for collecting a subset of register data from multiple nodes and making it readable in a single block of registers. Up to 2000 registers can be remapped to the gateway's Modbus ID starting at register 5000.

To configure the remapping, first select **Modbus Register Remapping** from the **Settings** dropdown menu.

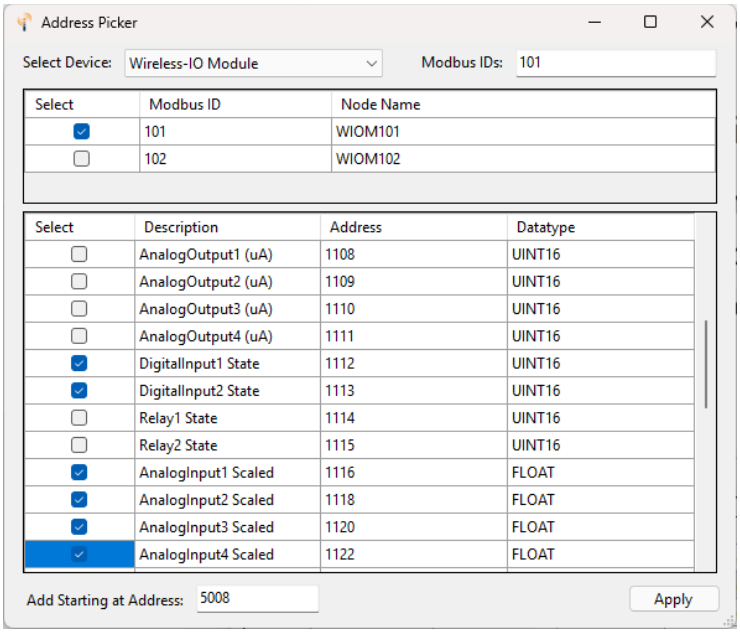


Enter the remote Modbus ID and register address to map to each gateway register and click **Write to GW** to remap the register(s).

The **Data Type**, **Node Name**, **Register Value**, and **Description** fields will automatically be filled in by the gateway once the mapping is written to the gateway.

The ToolKit also supports an Address Picker feature; this will allow you to select from a list of connected nodes or select any SignalFire Node type from the drop down. Then you can simply select the registers you want to add to the remap table by clicking on them and entering the starting address to add them.

In the example below, the user has selected a Wireless-IO Module at Modbus ID 101. Then you can simply select the registers you want to add to the remap table, and enter the address in the table to insert them (5008 in this case), then clock apply. These registers will automatically be added to the remap table.



15.1 Use Data Type Floats

The Gateway's Modbus Register Remapping provides an option to remap all registers to 32-bit floats. This allows the user to enter a register and its data type knowing that it will be read from the gateway via Modbus as two 16-bit registers.

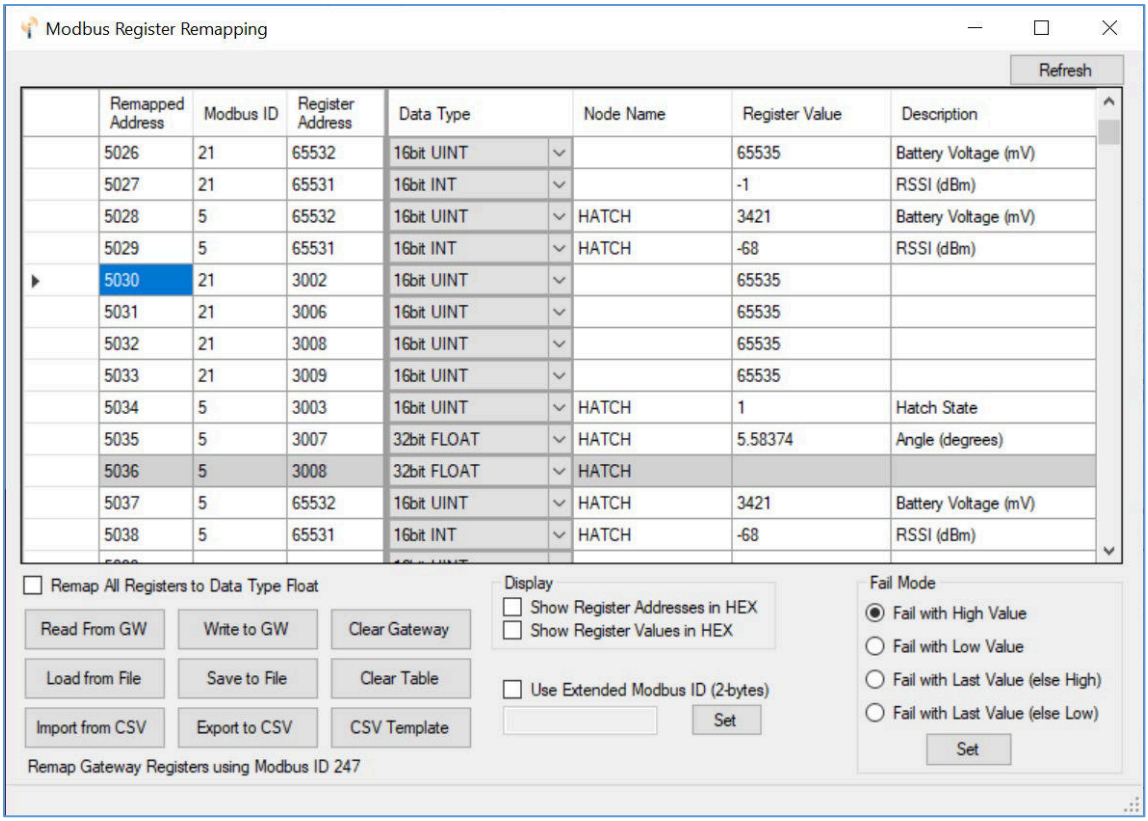
To use the floating-point remapping, select the 'Remap All Registers Data Type Float' check box in the lower right of the remap window. This will erase the current register remap in the Gateway; the user will be asked to confirm this action before proceeding.

For each even numbered register address in the remap table, enter the Modbus ID, Register Address, and select the data type. The data types are provided in a pull-down list. Click **Write to GW** to remap the register(s).

The **Node Name**, **Register Value**, and **Description** fields will automatically be filled in by the gateway once the mapping is written to the gateway.

15.2 Fail Mode

If the gateway does not have data for a remapped value it will respond with 0xFFFF, or 0x0000 for the register request, this is configurable globally with the **Fail Mode** settings.



Modbus ID 21 isn't reporting in, fail mode set to "high"

15.3 Import/Export CSV Files

The register map can also be exported or imported from CSV files in a specific format. Exporting the displayed remap information to a CSV file automatically writes the file in the required format. When creating a CSV file to import, use the template generated by clicking the 'CSV Template' button.

If the 'Use Data Type Float' checkbox is checked, the pre-formatted template will include the exact strings required for the data type column for easy 'cut & paste' operations.

16. Modbus Gateway Register Map

The SignalFire Modbus Gateway by default is assigned Modbus ID number 247. **Only the Gateway status/configuration and remapped registers are read at this address.** All remote node registers are read from the Modbus ID and register address of the remote node unless Modbus register remapping is used.

Coils

Read coils with Modbus opcode 0x01 (Read Coil). Write coils with Modbus opcode 0x05 (Write Single Coil) or 0x15 (Write Multiple Coils).

Register Address	Register Number	Description	R/W
0000	00001	System Reset: Resets the gateway and radio	R/W
0001	00002	Radio Reset: Resets the radio leaving the gateway on	R/W
0002	00003	Counter Reset: Resets all GW status counters to zero (See Read Only Registers 2026-2031)	R/W
0101	00102	Analog/Relay Output Module 1 Relay 1	R/W
0102	00103	Analog/Relay Output Module 1 Relay 2	R/W
0103	00104	Analog/Relay Output Module 2 Relay 1	R/W
0104	00105	Analog/Relay Output Module 2 Relay 2	R/W
0131	00132	Digital Output Module 1 Relay 1	R/W
0132	00133	Digital Output Module 1 Relay 2	R/W
0133	00134	Digital Output Module 1 Relay 3	R/W
0134	00135	Digital Output Module 1 Relay 4	R/W
0135	00136	Digital Output Module 1 Relay 5	R/W
0136	00137	Digital Output Module 1 Relay 6	R/W
0137	00138	Digital Output Module 1 Relay 7	R/W
0138	00139	Digital Output Module 1 Relay 8	R/W
0139	00140	Digital Output Module 1 Relay 9	R/W
0140	00141	Digital Output Module 1 Relay 10	R/W
0141	00142	Digital Output Module 1 Relay 11	R/W
0142	00143	Digital Output Module 1 Relay 12	R/W
0143	00144	Digital Output Module 2 Relay 1	R/W
0144	00145	Digital Output Module 2 Relay 2	R/W
0145	00146	Digital Output Module 2 Relay 3	R/W
0146	00147	Digital Output Module 2 Relay 4	R/W
0147	00148	Digital Output Module 2 Relay 5	R/W
0148	00149	Digital Output Module 2 Relay 6	R/W
0149	00150	Digital Output Module 2 Relay 7	R/W
0150	00151	Digital Output Module 2 Relay 8	R/W
0151	00152	Digital Output Module 2 Relay 9	R/W
0152	00153	Digital Output Module 2 Relay 10	R/W
0153	00154	Digital Output Module 2 Relay 11	R/W

Register Address	Register Number	Description	R/W
0154	00155	Digital Output Module 2 Relay 12	R/W
2034	02035	State of Gateway Digital Output 1 (0=open, 1=closed)	R/W
2035	02036	State of Gateway Digital Output (0=open, 1=closed)	R/W
7100	07101	RSD Force Shutdown	R/W

Discrete Inputs

Read discrete inputs with Modbus opcode 0x02 (Read Discrete Inputs).

Register Address	Register Number	Description	R/W
2036	12037	State of Gateway Digital Input 1 (0=open, 1=closed)	R
2037	12038	State of Gateway Digital Input 2 (0=open, 1=closed)	R

Holding Registers

Read holding registers with Modbus opcode 0x03 (Read Holding Registers) or 0x04 (Read Input Registers).
Write holding registers with Modbus opcode 0x06 (Write Single Register) or 0x16 (Write Multiple Registers).

Register Address	Register Number	Description	R/W
1000	41001	System Reset: Resets the gateway and radio	R/W
1001	41002	Radio Reset: Resets the radio leaving the gateway on	R/W
1002	41003	Counter Reset: Resets all GW status counters to zero (See Read Only Registers 2026-2031)	R/W
1003	41004	Radio Network	R
1004	41005	Radio Network Group	R
1005	41006	Radio Corporate ID	R
1101	41102	Analog/Relay Output Module 1 Relay 1	R/W
1102	41103	Analog/Relay Output Module 1 Relay 2	R/W
1103	41104	Analog/Relay Output Module 2 Relay 1	R/W
1104	41105	Analog/Relay Output Module 2 Relay 2	R/W
1119	41120	DIN GW Digital Output 1 Pulse (Seconds to pulse output on)	W
1120	41121	DIN GW Digital Output 2 Pulse (Seconds to pulse output on)	W
1121	41122	Analog/Relay Output Module 1 Relay 1 Pulse (Seconds to pulse relay on)	W
1122	41123	Analog/Relay Output Module 1 Relay 2 Pulse (Seconds to pulse relay on)	W
1123	41124	Analog/Relay Output Module 2 Relay 1 Pulse (Seconds to pulse relay on)	W
1124	41125	Analog/Relay Output Module 2 Relay 2 Pulse (Seconds to pulse relay on)	W
1131	41132	Digital Output Module 1 Relay 1	R/W
1132	41133	Digital Output Module 1 Relay 2	R/W

1133	41134	Digital Output Module 1 Relay 3	R/W
1134	41135	Digital Output Module 1 Relay 4	R/W
1135	41136	Digital Output Module 1 Relay 5	R/W
1136	41137	Digital Output Module 1 Relay 6	R/W
1137	41138	Digital Output Module 1 Relay 7	R/W
1138	41139	Digital Output Module 1 Relay 8	R/W
1139	41140	Digital Output Module 1 Relay 9	R/W
1140	41141	Digital Output Module 1 Relay 10	R/W
1141	41142	Digital Output Module 1 Relay 11	R/W
1142	41143	Digital Output Module 1 Relay 12	R/W
1143	41144	Digital Output Module 2 Relay 1	R/W
1144	41145	Digital Output Module 2 Relay 2	R/W
1145	41146	Digital Output Module 2 Relay 3	R/W
1146	41147	Digital Output Module 2 Relay 4	R/W
1147	41148	Digital Output Module 2 Relay 5	R/W
1148	41149	Digital Output Module 2 Relay 6	R/W
1149	41150	Digital Output Module 2 Relay 7	R/W
1150	41151	Digital Output Module 2 Relay 8	R/W
1151	41152	Digital Output Module 2 Relay 9	R/W
1152	41153	Digital Output Module 2 Relay 10	R/W
1153	41154	Digital Output Module 2 Relay 11	R/W
1154	41155	Digital Output Module 2 Relay 12	R/W
2000	42001	Node Address: node address/Radio ID (UINT32)	R
2002	42003	Gateway Radio Firmware Major Version	R
2003	42004	Gateway Radio Firmware Minor Version	R
2004	42005	Gateway Firmware Major Version	R
2005	42006	Gateway Firmware Minor Version	R
2006	42007	Gateway Firmware Revision	R
2007	42008	Number of Modbus Servers Allocated	R
2008	42009	Number of Modbus Registers Allocated	R
2009	42010	Modbus ID [15-0]: Bitmask for Modbus IDs 15-0 (LSB is 0)	R
2010	42011	Modbus ID [31-16]: Bitmask for Modbus IDs 31-16 (LSB is 16)	R
2011	42012	Modbus ID [47-32]: Bitmask for Modbus IDs 47-32 (LSB is 32)	R
2012	42013	Modbus ID [63-48]: Bitmask for Modbus IDs 63-48 (LSB is 48)	R
2013	42014	Modbus ID [79-64]: Bitmask for Modbus IDs 79-64 (LSB is 64)	R
2014	42015	Modbus ID [95-80]: Bitmask for Modbus IDs 95-80 (LSB is 80)	R
2015	42016	Modbus ID [111-96]: Bitmask for Modbus IDs 111-96 (LSB is 96)	R
2016	42017	Modbus ID [127-112]: Bitmask for Modbus IDs 127-112 (LSB is 112)	R
2017	42018	Modbus ID [143-128]: Bitmask for Modbus IDs 143-128 (LSB is 128)	R
2018	42019	Modbus ID [159-144]: Bitmask for Modbus IDs 159-144 (LSB is 144)	R
2019	42020	Modbus ID [175-160]: Bitmask for Modbus IDs 175-160 (LSB is 160)	R
2020	42021	Modbus ID [191-176]: Bitmask for Modbus IDs 191-176 (LSB is 176)	R
2021	42022	Modbus ID [207-192]: Bitmask for Modbus IDs 207-192 (LSB is 192)	R
2022	42023	Modbus ID [223-208]: Bitmask for Modbus IDs 223-208 (LSB is 208)	R
2023	42024	Modbus ID [239-224]: Bitmask for Modbus IDs 239-224 (LSB is 224)	R

2024	42025	Modbus ID [255-240]: Bitmask for Modbus IDs 255-240 (LSB is 240)	R
2025	42026	Supply Voltage: Gateway power supply voltage	R
2026	42027	Radio RX Count: Radio packets received count	R
2027	42028	Radio TX Count: Radio packets sent count	R
2028	42029	RS485RX Count: RS-485 messages received count	R
2029	42030	RS485TX Count: RS-485 messages sent count	R
2030	42031	RS485 Errors: Total Modbus errors from client and servers	R
2031	42032	Modbus Errors: Modbus exceptions from Modbus nodes	R
2032	42033	Radio packets received/transmitted per minute. (Recommended to be less than 60)	R
2033	42034	Radio packets per minute alert (0 if packets/min <= 60, 1 if packets/min > 60)	R
2034	42035	State of Digital Output 1 (0=open, 1=closed)	R/W
2035	42036	State of Digital Output 2 (0=open, 1=closed)	R/W
2036	42037	State of Digital Input 1 (0=open, 1=closed)	R
2037	42038	State of Digital Input 2 (0=open, 1=closed)	R
2038	42039	Unix Epoch Time (seconds since Janary 1st, 1970) (UINT32)	R
2040	42041	Seconds Since Power On (UINT32)	R
2042	42043	Seconds Since Last Reboot (UINT32)	R
2100	42101	Address test register. Always returns 2100	R
2101	42102	Address test register. Always returns 2101	R
2102	42103	Address test register. Always returns 2102	R
3000	43001	Write the radio address of a Modbus Stick node to this register to cause that Modbus Stick to perform a scan for attached Modbus sensors (by node address). (UINT32)	W
3002	43003	Write Modbus ID for a Modbus Client node to this register to cause that remote node to perform a scan for attached Modbus sensors (by Modbus ID). (UINT32)	W
4001	44002	Status of Modbus ID 1: Returns 1 if device is present and 0 if not present	R
4002	44003	Status of Modbus ID 2: Returns 1 if device is present and 0 if not present	R
…	…	…	R
4240	44241	Status of Modbus ID 240: Returns 1 if device is present and 0 if not present	R
5000	45001	Remapped Register 1	R/W
5001	45002	Remapped Register 2	R/W
…	…	…	R/W
6999	46500	Remapped Register 2000	R/W
7000	47001	RSD Event 1 Line #	R
7001	47002	RSD Event 1 Source Modbus ID	R
7002	47003	RSD Event 1 Destination Modbus ID	R
7003	47004	RSD Event 1 Destination Relay Channel	R
7004	47005	RSD Event 1 Type (1 = Energize, 0 = De-Energize)	R
7005	47006	RSD Event 2 Line #	R
7006	47007	RSD Event 2 Source Modbus ID	R
7007	47008	RSD Event 2 Destination Modbus ID	R
7008	47009	RSD Event 2 Destination Relay Channel	R

7009	47010	RSD Event 2 Type	R
7010	47011	RSD Event 3 Line #	R
7011	47012	RSD Event 3 Source Modbus ID	R
7012	47013	RSD Event 3 Destination Modbus ID	R
7013	47014	RSD Event 3 Destination Relay Channel	R
7014	47015	RSD Event 3 Type	R
7015	47016	RSD Event 4 Line #	R
7016	47017	RSD Event 4 Source Modbus ID	R
7017	47018	RSD Event 4 Destination Modbus ID	R
7018	47019	RSD Event 4 Destination Relay Channel	R
7019	47020	RSD Event 4 Type	R
7020	47021	RSD Event 5 Line #	R
7021	47022	RSD Event 5 Source Modbus ID	R
7022	47023	RSD Event 5 Destination Modbus ID	R
7023	47024	RSD Event 5 Destination Relay Channel	R
7024	47025	RSD Event 5 Type	R
7100	47101	RSD Force Shutdown (1=force all RSD relays off, 0=run RSD logic)	R/W
7101	47102	Scratch Pad Register, can be used for RSD Control Logic	R/W
7102	47103	Scratch Pad Register, can be used for RSD Control Logic	R/W
…	…	…	R/W
7132	47133	Scratch Pad Register, can be used for RSD Control Logic	R/W

17. Disposal Instructions

To ensure environmental safety and compliance, please follow these disposal instructions for the product and its components:

Electronic Components:
This product contains electronics must be recycled through approved e-waste recycling programs. Electronics can contain harmful materials and should be prevented from entering landfills. Do not place electronics in regular trash.

Metal Parts:
Any metal components can be separated and recycled through your local metal recycling facility.

Packaging Materials:
Recycle or reuse packaging materials such as cardboard or plastics, following local recycling guidelines.

For local disposal sites refer to:

- Call2Recycle (USA, Canada)
- Earth911 (USA, Canada)
- SERI (International)

In the USA or more information, visit:

- EPA's battery disposal guide
- EPA's electronics recycling page

By following these guidelines, you help reduce waste and support environmental sustainability.

Revision	Date	Changes/Updates
1.0	10/13/25	Initial release

Technical Support And Contact Information

SignalFire Telemetry
140 Locke Dr., Suite B
Marlborough, MA 01749

(978) 212-2868
support@signal-fire.com

SIGNALFIRE
WIRELESS TELEMETRY