Manual

PiiGAB 900T/LTE
PiiGAB 900S

Table of contents

1 Overview

This manual provides guidance on how to install, connect, and configure the PiiGAB 900S/T gateway.

1.1 Description

PiiGAB 900S/T is a flexible smart gateway designed for data collection in building and properties. It supports up to 120 M-Bus loads, offers simultaneous access for up to 4 clients, and 900S features both RS-232 and RS-485 ports for versatile serial communication. The gateway enables seamless protocol conversion and virtual meter handling and can be configured to communicate using a wide range of standard protocols.

PiiGAB 900S/T is easily configured through its web interface and supports integration with external systems via Modbus TCP/RTU, MQTT, BACnet IP, QuickPost, and HAN. This makes it ideal for integration in energy monitoring, building automation, and industrial control environments.

1.2 Security

The PiiGAB 900 Gateway is designed for secure operation in professional industrial and metering environments. To maintain a high level of data integrity and protection, especially when handling sensitive information such as consumption values used for billing, several security mechanisms and best practices must be followed.

1.2.1 Physical Access Control

All fieldbus interfaces such as M-Bus, RS485, and RS232 are considered physically secure interfaces. These ports must only be accessible within locked, tamper-proof technical enclosures. Unauthorized physical access to these ports could allow interception or manipulation of transmitted data. It is therefore essential that:

- The device is installed in secured environments, such as locked electrical cabinets or metering stations.
- M-Bus cabling must not be externally accessible or exposed to open public spaces.
- Access to the device and its connectors should be limited to authorized personnel only.

1.2.2 Network Access Control

Default credentials must be changed at first login, and encrypted connections (e.g., HTTPS, SFTP) should always be used for data transfer.

1.3 Network Installation Requirements

To ensure secure operation and compliance with cybersecurity best practices, the device must only be deployed within logically segmented and protected networks. The following installation requirements apply:

- The device shall never be connected directly to public or untrusted networks, including the open Internet or flat LAN environments without segmentation.
- All Ethernet-based deployments must use firewall protection, VLANs, or dedicated metering networks that restrict access to trusted systems only.
- Inbound access from external networks must be blocked, unless explicitly required and protected by strong authentication and encryption.

Devices with LTE connectivity must be provisioned within a private APN (Access Point Name) managed by the mobile operator. The APN must ensure that:

- The device is not reachable from public IP addresses
- Only approved backend systems can access the device over cellular data
- No unsolicited inbound connections are possible

Important: Exposing the device to open networks without adequate isolation poses significant security risks. It is the responsibility of the system integrator or end user to ensure proper network design, segmentation, and firewall policies.

2 Device Overview

The PiiGAB 900 gateway consists of several interfaces and connections that enable flexible integration with M-Bus networks and Ethernet systems. The unit is equipped with status LEDs, communication ports, power supply connectors, and reset functionality.

Ethernet port: 1 × RJ45 connector for communication with TCP/IP or UDP/IP networks.

M-Bus Slave inputs: Two parallel inputs for connection to an existing M-Bus loop (polarity independent).

M-Bus Master outputs: Four parallel outputs for M-Bus loops (up to 120 units depending on configuration).

RS232: Tx, Rx, and GND terminals for serial communication (Only 900 S)

RS485: A and B terminals for RS485 connections (Only 900 S)

Relay output: Terminals for NO, COM, and NC (Only 900 S)

Power supply: 24 V AC/DC connector(Only 900 S)

2.1 LED

The front panel of the PiiGAB 900 is equipped with several LEDs that provide quick information about the unit’s status and communication. The indicators show power supply status, errors such as short circuits or overload on the M-Bus, as well as activity on the master and slave ports. By interpreting the LED signals, it is easy to monitor operation and troubleshoot the installation

LED	Description
Pwr	- At startup, it **flashes red/green** for about 10 seconds until the processor has started correctly. - After that, it stays **solid green**. - Flashes **red fast** when there is a short circuit on the M-Bus loop. - Flashes **orange slowly** when the loop is overloaded. - Flashes **orange slowly** when the license key is not installed.
C1	No function in the current version.
C2	Modbus2MBus (Tx).
C3	Modbus2MBus (Rx).
M (Tx)	Flashes when the Master port sends data.
M (Rx)	Flashes when the Master port receives data.
P1 (Rx)	Flashes when Slave port 1 receives data.
P1 (Tx)	Flashes when Slave port 1 sends data.
P2 (Rx)	Flashes when Slave port 2 receives data.
P2 (Tx)	Flashes when Slave port 2 sends data.
P3 (Rx)	Flashes when Slave port 3 receives data.
P3 (Tx)	Flashes when Slave port 3 sends data.
P4 (Rx)	Flashes when Slave port 4 receives data.
P4 (Tx)	Flashes when Slave port 4 sends data.

2.2 Reset Button

A multifunctional reset button is located between the supply voltage connector and the Ethernet port. It can be used to restart the gateway, restore factory settings, reset network configuration, or clear login credentials.

Count the number of LEDs on the left side of the gateway and follow the instructions below:

2.2.1 Reset with 14 LEDs

A multifunctional reset button is located between the supply voltage connector and the Ethernet port. It can be used to restart the gateway, restore factory settings, reset network configuration, or clear login credentials.

Functions:

- Push button 1 time to restart Gateway
- Push button 5 times to reset Ethernet settings
- Push button 6 times to reset Password to factory default (Sticker on the side)
- Push button 7 times to reset all settings to factory default

2.2.2 Reset with 4 LEDs

2.2.3 Reset with 0 LEDs

A multifunctional reset button is located between the supply voltage connector and the Ethernet port. It can be used to restart the gateway, restore factory settings, reset network configuration, or clear login credentials.

Functions:

- Push button for 10 Seconds to restart Gateway, reset Ethernet settings, reset Password to factory default (Sticker on the side)

3 Installation

3.1 Mounting Location

The PiiGAB 900S/T is designed to be installed in electrical cabinets, enclosures, or other closed spaces. The unit must always be mounted in a protected environment to ensure both operational reliability and security.

Ensure sufficient space around the unit to allow for proper heat dissipation. The recommended clearance is at least 5 cm (2 inches) around the device. Avoid installation in areas with poor airflow, direct sunlight, or in proximity to other heat-generating components without adequate cooling.

The PiiGAB 900 S/T can be installed on DIN-rail or fixed inside an enclosure, depending on the application. All cables should be routed neatly and secured to avoid mechanical strain on the connectors. Verify that grounding and shielding are carried out according to local electrical installation standards.

3.1.1 Safety Notes

Do not power up the unit before it is securely mounted and all connections have been properly made. The installation environment should comply with the specified operating temperature and humidity limits. The installer is responsible for ensuring that all relevant electrical safety and EMC regulations are followed.

3.2 Power Supply Requirements

The PiiGAB 900S/T must be powered by an external power supply providing:

- 24 V AC or 24 V DC
- Minimum power rating: 36 W

Only use a certified and reliable power supply to ensure safe and stable operation. The power source must be installed according to applicable electrical safety standards and should only be connected by authorized personnel.

3.3 Wiring diagram

Power Supply (Port 18/19)

Use an external 24 V AC or 24 V DC supply with a minimum rating of 36 W.

For DC:

+ [18] = +24 V

–[19] = 0 V.

For AC:

Connect one conductor to [18] and the other to [19].

It is recommended to place a fuse close to the power supply. Always connect the GND terminal to protective earth to ensure safety, reduce EMC disturbances, and provide stable operation.

3.3.1 Ethernet (RJ45)

Connect the RJ45 port to a LAN switch or router (Ethernet 10/100/1000). Use a straight patch cable (Cat5e or better). Keep Ethernet cables separated from power wiring to reduce EMC disturbances.

3.3.2 M-Bus (Master interface)

The Master ports are the terminals where you connect your M-Bus loops, i.e. the cables going to your meters.

The gateway provides four parallel master outputs (terminal 22–29), and you can use one or several of them depending on how many loops you need. It is recommended to split longer M-bus loops in several to easier troubleshooting.

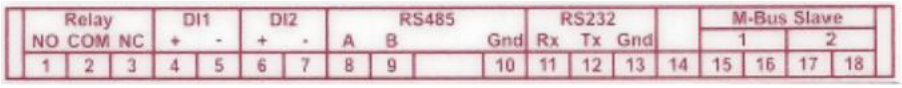
All master ports deliver the same signal and are powered by a common M-Bus driver stage, so you can choose any port pair for each loop. The output voltage is normally around 39–40 V and is sufficient to supply the number of meters licensed for your gateway.

3.3.3 Safety note:

Never connect two M-Bus masters to the same loop. Doing so can damage the equipment and cause communication errors. Always ensure that each M-Bus loop is powered and controlled by only one master.

3.4 900S interfaces

PiiGAB 900S has several interfaces on the top of the gateway. These are described in following text.



3.4.1 M-Bus (Slave interface)

Connect port 15&16 and port 17&18 to your M-Bus loop to read values via serial M-bus as a slave device (bus topology). M-Bus is non-polarized, but follow device labeling where indicated. Use a twisted pair cable for reliable communication.

3.4.2 RS-232

Point-to-point communication only. Connect TX → RX, RX → TX, and GND → GND between the PiiGAB 900S/T and the external RS-232 device. Cable length should not exceed ~15 m.

3.4.3 RS-485

Multi-drop communication bus (half-duplex). Connect A → A, B → B, and GND → GND to all devices on the bus. Use twisted pair cable; maximum length depends on baud rate (typically up to 1200 m). Termination resistors may be required at both ends of the bus.

3.5 Wizard

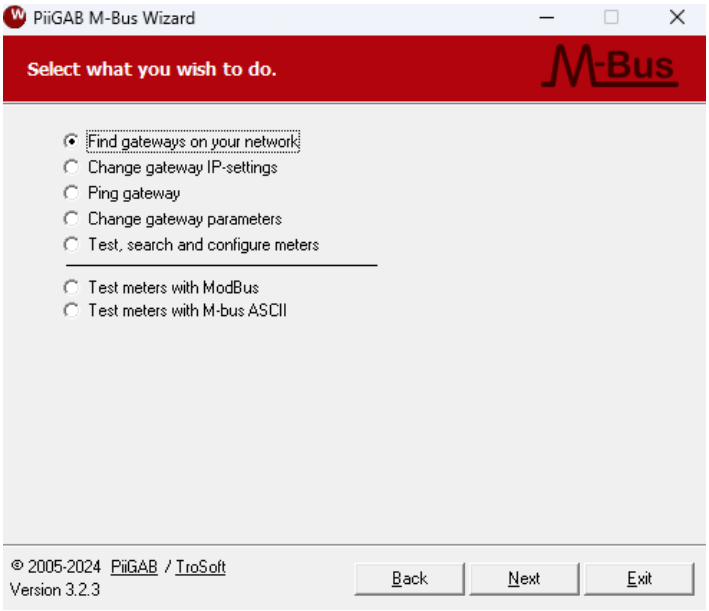
The M-Bus Wizard is a software that can be downloaded from the PiiGAB website. It helps locate the PiiGAB 900S/T on the network and test the M-Bus loop. Further configuration is done through the Web interface.

3.5.1 Start PiiGAB M-Bus Setup Wizard

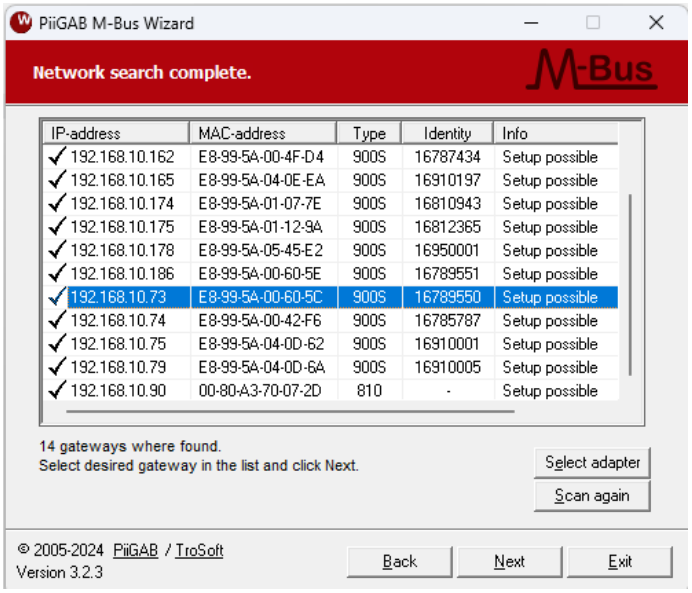
Upon launching the wizard for the first time, select your preferred language. This can be changed later.

3.5.2 Find the gateway on the network

If you know that the gateway has an IP address that can be found via the network, you will choose Find gateways on your network from the main menu.



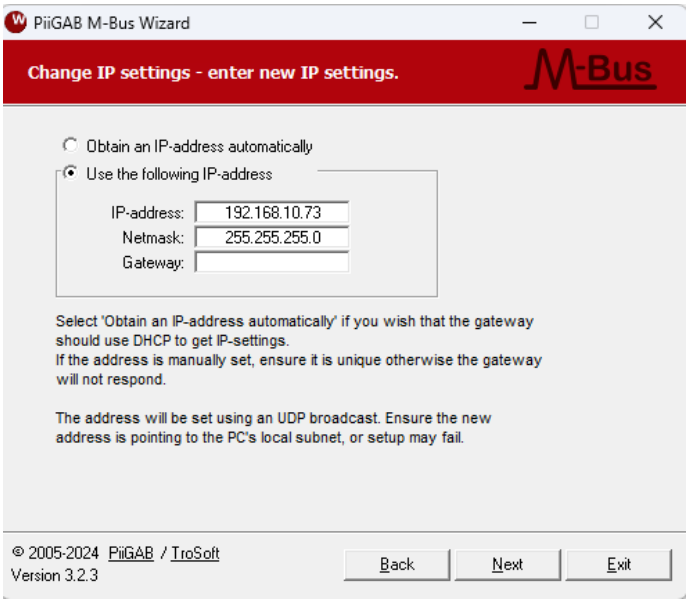
By double clicking on PiiGAB M-Bus 900S/T alternatively on 'Next' a message box with the below text will appear. If you choose Yes, your standard web browser will start and if you choose no you will continue to work in the PiiGAB M-Bus Setup Wizard.



3.5.3 Network settings via PiiGAB M-Bus Wizard

You can change the IP settings in PiiGAB M-Bus 900 via the PiiGAB M-Bus Setup Wizard as well as the Web interface. Notice that PiiGAB M-Bus Setup Wizard doesn't support settings and changing of the netmask and gateway in PiiGAB M-Bus 900S/T.

Click "Next" to choose connection method. In the PiiGAB M-Bus 900 it is only possible to set network parameters via IP. Set an IP-address and Netmask and no gateway. Click next and apply.



3.6 Logging in

1. Open your web browser and enter the IP address of the gateway in the address bar.
2. Proceed past the security warning most browsers will display a security warning. *Click "Advanced" (or equivalent, depending on your browser).*Then select "Proceed to [IP address]" to continue to the login page.
3. Log in using the default credentials:

- Username: Admin
- Password: The default password is printed on a label on the side of the device. It may also be found in your order confirmation or shipping documents.

4. Important: Change the default password

For security reasons, we strongly recommend that you change the default password immediately after logging in. A strong, unique password helps protect your device from unauthorized access.

Tip: Save the password in PiiGAB Portal

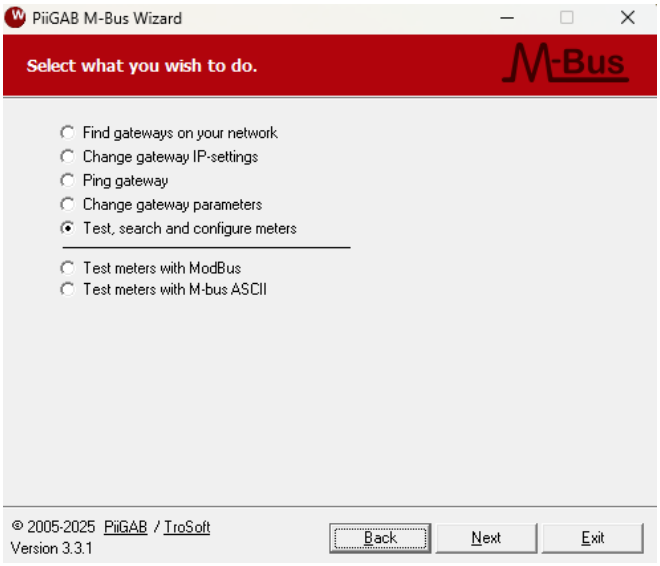
To simplify future access and management of your devices, you can store the password securely in the PiiGAB Portal. This allows for easier login and configuration directly from the portal in the future.

3.6.1 Search for meters

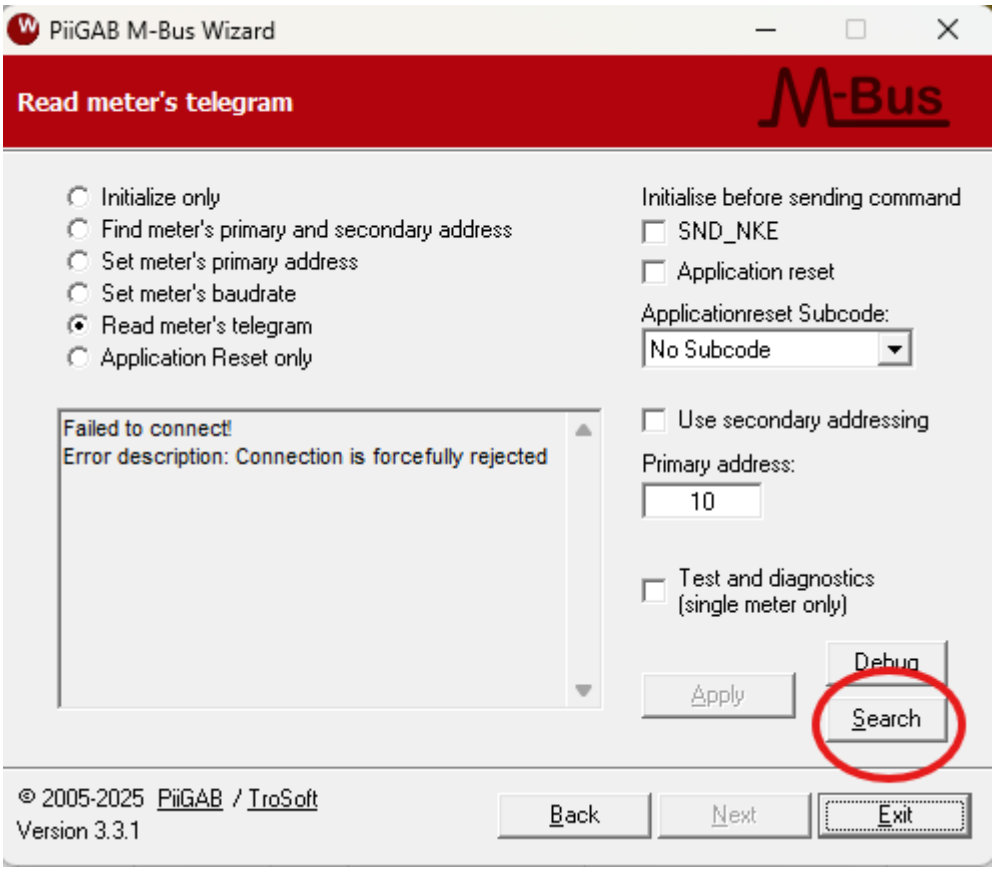
We recommend you to search for the meters in the 900 S/T Webinterface instead of using the Mbus Wizards

If you are going to use the Mbus Wizard to search for meters, you either need to raise the Mbus Timeout in the wizard higher than the Master/slave timeout in the Mbushub or, lower the timeouts in the Mbushub to lower than Mbus wizard timeout (800 ms as default). All communication from external devices and internal applications will disturb the results.

1. *Press "Test search and configure meters"*



2. *Add your IP and make sure to use the correct port. (See Slaveport in Mbushub) as well as whether to use UDP pr TCP*
3. *Press the Search button in the bottom right corner of the windows.*



4. *Choose whether to use primary or secondary search, press the "Start search" button and press "yes" on the dialog.*

4 Getting Started with you PiiGAB 900 S/T

Now that you have connected to your gateway, you can begin the configuration process. Always start by updating the device firmware to ensure you have the latest features and fixes. Next, verify that your basic settings are correct and match your network requirements. Next, confirm all desired meters are in the meter list. After confirmation, you may proceed to establish reading schedules, conversions, and data streams as required.

5 Settings

Before installing, ensure the gateway runs the latest software and correct settings. This ensures stable operation and prevents communication issues with your M-Bus meters. You can find the settings page on the menu to your left.

5.1 Software Update

5.1.1 If the gateway has Internet access:

1. Go to Settings → Update Software.
2. Click **Update List** to fetch available versions.
3. Choose application → Click **Upgrade,** wait for the upgrade to finish.
4. After upgrade → Scroll down and click **Reboot.**

5.1.2 If the gateway has no Internet access:

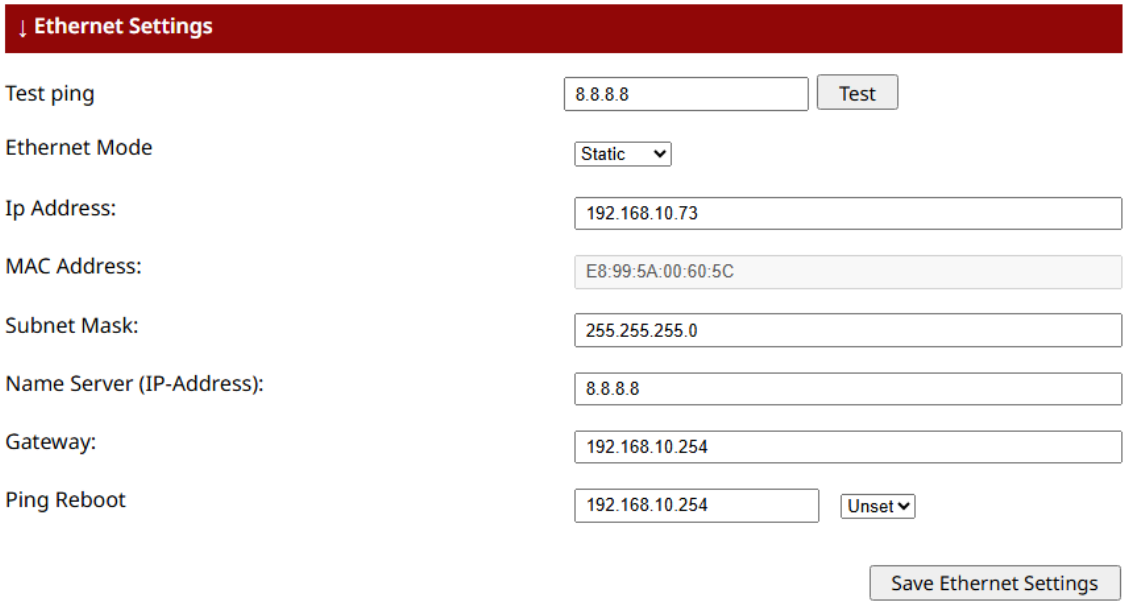
1. Download update bundle from PiiGAB website.
2. In the web UI → Click **Upload Bundle**, select the file.
3. Click **Update List** to fetch available versions.
4. Choose application in the list→ Click **Upgrade/install,** wait for the upgrade to finish.
5. After upgrade → Scroll down and click **Reboot.**

5.2 Ethernet settings

If you are going to use LTE this settings will only be used when accessing the gateway via the ehternet port. For LTE settings see the LTE chapter.

Setting up the basic network parameters allows the Metering Gateway to establish a network connection. This function transmits meter data accurately to external servers. PiiGAB M-Bus 900 can be set to static IP or dynamic IP address. The PiiGAB 900 T LTE generally operates with default settings when a SIM card is installed.

1. Go to Settings -> Ethernet Settings
2. If selecting Static, enter IP-Adress, Subnet Mask, Server IP and Gateway.
3. Save Ethernet settings (The unit will restart with the new settings).



5.2.1 Ping Reboot

This feature continuously monitors the connection by pinging a specified IP address. If it fails to receive a response this triggers a system reboot.

The main purpose is to ensure reliable network connectivity. If the device loses connection due to a temporary network issue, this mechanism allows it to recover automatically without manual intervention — improving stability, uptime, and remote accessibility.

5.2.2 Proxy settings

The gateway supports HTTPS communication via a proxy server. This is useful in network environments where direct internet access is restricted.

Configuration:

1. Navigate to Settings → HTTPS Proxy

2. Enter the proxy server address and port

3. Click "Set proxy"

When enabled, all outgoing HTTPS traffic will be routed through the configured proxy.

5.2.3 Time settings

Keeping the device time updated can be important for certain web functions and will simplify troubleshooting by providing accurate log information.

Select Time zone.

To set your local time zone:

1. Use the dropdown menu to select the appropriate time zone (e.g., Europe/Stockholm).
2. Click Set Time Zone to apply the change.

The selected time zone affects how the system converts UTC time into local time.

5.2.4 Time and Date

To manually set the current system time:

1. Enter the correct date and time in the field provided.
2. Click Set time to save your changes.

Use this option if NTP is unavailable or if you need to apply a specific time manually.

5.2.5 Network Time Protocol (NTP)

To synchronize the device's clock with an internet time server:

1. Enter the address of an NTP server (e.g., 0.pool.ntp.org) in the field.
2. Click Set NTP to activate automatic time synchronization.

Note: The NTP hostname must be resolvable via DNS. Ensure the device has access to a valid nameserver.

5.3 Backup

You can create and restore complete backups of the gateway's configuration:

- **Create backup**: Save current configuration to a file.
- **Upload backup**: Restore from a previously saved backup.

Tip: Always create a backup before performing major configuration changes or firmware upgrades.

5.3.1 Automatic backup

The system automatically creates a backup once a day whenever changes are made to the configuration.

This ensures that a recent working configuration is always available and simplifies recovery in case of incorrect settings or system issues.

Note:

Automatic backups are stored together with manually created backups and can be downloaded from the backup list.

5.4 License update

To upgrade the license, you will receive a license string. Enter this string under:

Settings → Basic Settings → License.

5.5 Users

To create a new user, go to:

Basic Settings → Users → Create User.

Fill in the user details and click **Save** to add the user.

To delete a user, go to:

Basic Settings → Users → delete.

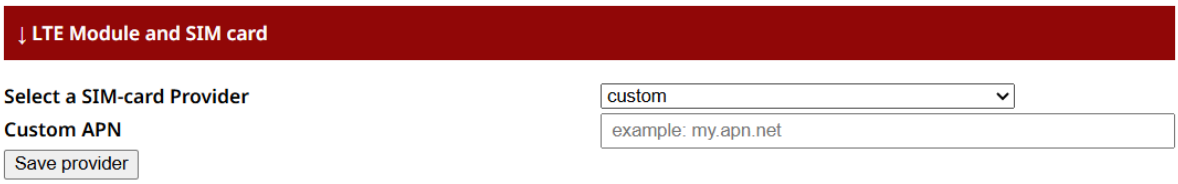
5.6 Manage Configuration Files

You can upload, download, remove or view configuration files used by the system. Supported file formats are .csv, .xml, and .ini.

- View .ini files: Select and click Show.
- Upload: Choose a file → Click Upload.
- Download: Select file → Click Download.
- Remove: Select and click Remove.

5.7 LTE set-up

1 Go to "Installed software" and choose LTE
2 On "Select a SIM-card Provider" choose your provider or choose custom to enter an APN manually. Then press save.



3 On "Network, choose LTE Model On/Off" to "ON" and press Save.
4 Wait for a few minutes to verify LTE connection.

6 Logging

The Logs page provides access to system logs for troubleshooting and monitoring the gateway. The log page gathers information on all applications in the gateway including audit logging.

6.1 Log view

At the top of the page, you can filter and control the log output:

Application – Select which service to view logs from (e.g. MBusHub).

Level – Choose the log level (e.g. Trace, Debug, Info, Error).

Auto refresh – Automatically updates the log view.

Refresh – Manually reload the log window.

Clear log – Clears the current log view (does not delete stored log files).

6.2 Download logs

Stored log files can be downloaded from the Download Logs section.

Logs are saved per day (e.g. Log_YYYY-MM-DD.log)

File size is shown for each log file

An auditlog.csv is also available for system audit events

Click on a file name to download it.

6.3 Advanced actions (Only advanced users)

Recreate CSV files from database

Rebuilds CSV configuration files from the internal database.

View configuration files

Select a file (e.g. myconfig.csv) and click View to inspect it.

See import log

Displays logs related to configuration imports.

Re-import old configuration

Restores previously imported configuration files.

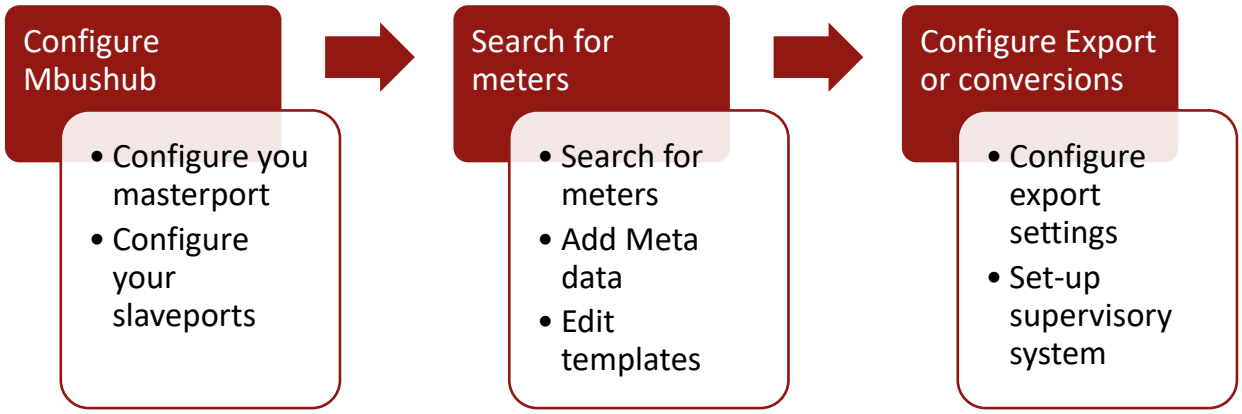
Remove database

Deletes the internal database (use with caution).

7 Configration

To configure the PiiGAB 900S follow these three main steps to get your system up and running:

1. Set master and slave ports to configure communications with Mbushub.
2. Search for meters – Detect connected meters, add metadata, and apply templates.
3. Configure Export or Conversions – Define export settings and connect to a supervisory system.



The gateway is preconfigured to read serial M-Bus and Wireless M-Bus (wM-Bus) meters by default. If you are required to read additional types of meters, utilize an alternative communication interface, or if your meters are not being detected, please consult the MBusHub chapter and confirm that the communication settings are properly configured.

7.1 Meter list

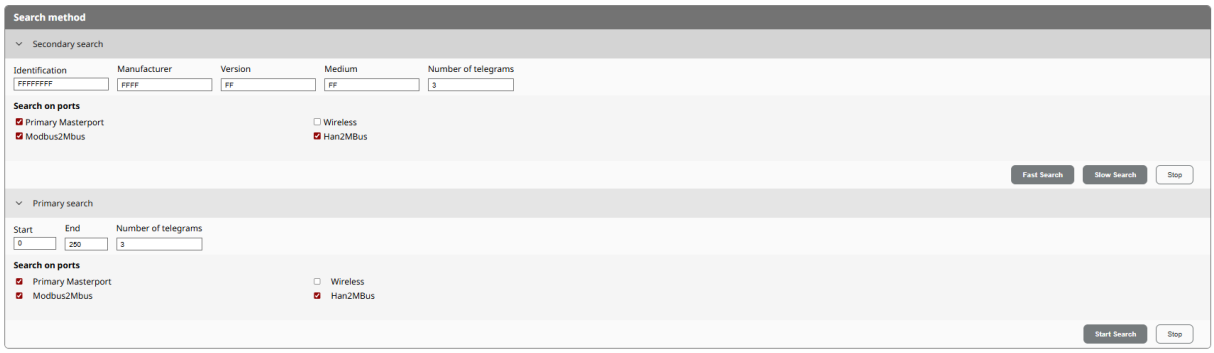
To manage your connected meters, navigate to the **Meters** page. This list provides an overview of the connect meters. By default, all verified meters in the meterlist will be available for readouts.

7.1.1 Add Meters

Click **Add Meter** and choose from:

- Search meters:

You can perform primary and secondary search. By choosing FFFFFFFF, the gateway goes through all addresses.



- **Add single meter:** Enter meter details manually.

Import meterlist:

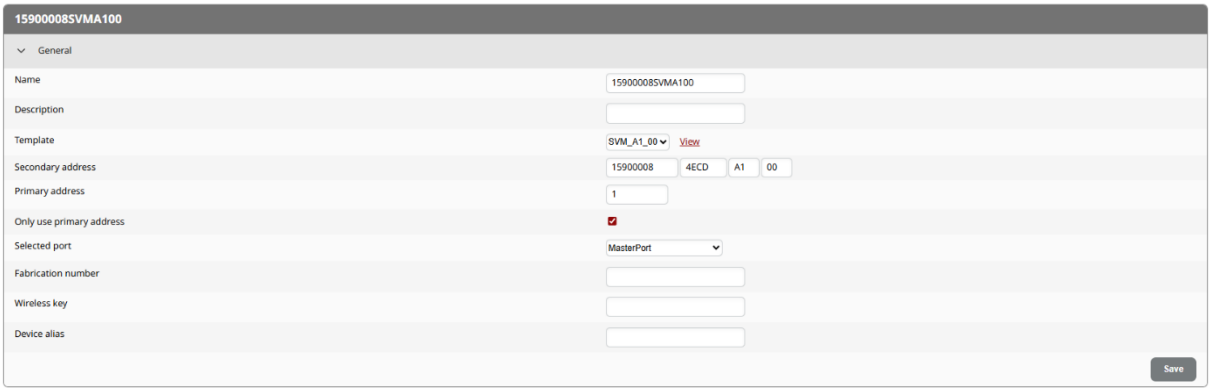
Upload a pre-defined meter list file to import multiple meters at once. Import meterlist works with borg CSV or Excel format.

7.1.2 Download

- On Download you can download the current meter list for faster editing.
- Download Project report

7.1.3 Device settings

In device settings you can change and read the meta data for the meter.



Field Name	Description
Name	Displays the device ID or name. Often auto-filled based on the device address.
Description	An optional field where you can enter a description to help identify the device.
Template	Allows you to select a predefined template for quick configuration, if available.
Secondary address	Shows the secondary M-Bus address, split into ID, manufacturer code, version, and medium.
Primary address (Read only)	The primary M-Bus address (a numeric ID, typically between 0–250).

Only use primary address	This setting is used to force the gateway to use primary addressing instead of secondary addressing.
Selected Port	This is assigned when searching for new meters. If a Masterport is set, only this will be used to communicate with the meter. This can also be set anytime if there is already a configuration.
Fabrication number	Used to specify an Wm-bus node on where to read the meter.
Wireless key	Used for wireless M-Bus communication if required by the device.
Save button	Saves any changes made in the form.

7.1.4 Change name of multiple devices

5 Download the meterlist.
6 Change the names in Excel.
7 Import the meterlist again.

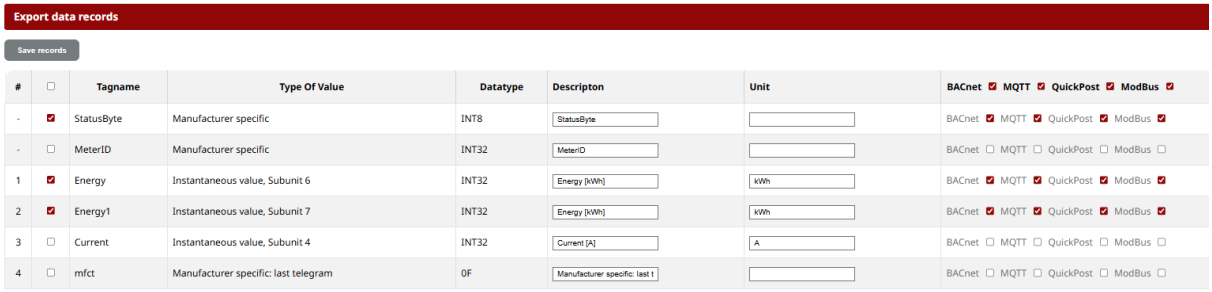
7.1.5 Replace an existing meter with the same type

1. Go the replaced meter.
2. Open the general settings.
3. Change the secondary address.
4. Press save.

7.1.6 Templates

Templates help group similar device types into the same configuration and provide options for selecting which data records you want in your final export.

To customize individual device settings, click on the device name in the list. From there, you can adjust various parameters and choose exactly which data records to read and export. You can easily add different template for the same meter type on the device meny.



7.1.7 Change template for a device

1. Open the template for the desired device type.
2. Adjust the parameters as needed: for example, uncheck all unnecessary data records and select only Energy.
3. Save the template to apply your changes for all meters connected to the template.

7.1.8 Settings Parameter Descriptions

Setting	Description

Time format	Defines the timestamp format used when exporting data. Example: `yyyy-mm-ddTHH:MM:SS`.
Tag type	Sets the data structure label format (e.g., "Record" for structured logging).

7.1.9 Readout Settings

Setting	Description
Maximum telegrams to read	Sets the maximum number of M-Bus telegrams read per cycle.
Read period (s)	Interval between automatic readouts, in seconds.
Read offset (s)	Time (in seconds) added before each scheduled read cycle starts. (Used to update cache before a periodic readout like QuickPost).
Cache Lifetime (ms)	Duration (ms) that cached data remains valid before being refreshed.
Request Timeout (ms)	Maximum wait time (in ms) for a response from a meter before timeout is triggered.
Max request retries	Number of retry attempts if a request fails.
Initialization mode	Defines whether initialization is used before readout
Subcode	Optional command modifier for certain meter types.
Manual Initialization	Allows manual input of a hexadecimal init string for specific meters (advanced use only).

7.1.10 Modbus Conversion

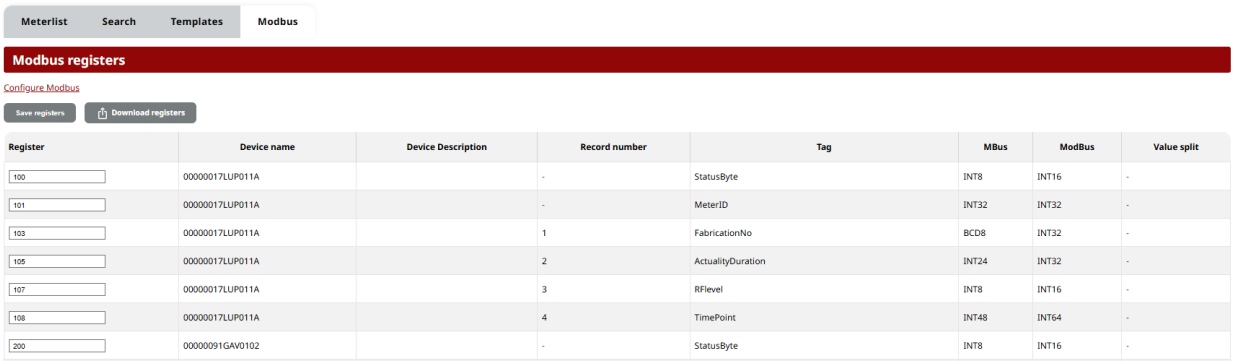
Setting	Description
Modbus conversion of INT64, INT48 and BCD12	Enables automatic format conversion of complex data types to Modbus-compatible values.

7.1.11 Initialization codes

Option	**Description**
No Init	No initialization command is sent before reading. Use this if the meter does not require any specific initialization sequence.
SND_NKE	Sends a standard *SND_NKE* (Send Initialization) command to wake up or prepare the M-Bus slave device. Common for most compliant M-Bus meters.
App reset	Sends an application reset command before reading. This is sometimes needed to restart the meter's communication session.
SND_NKE + App reset	Sends both *SND_NKE* and *App reset* before reading. Ensures maximum compatibility for meters that require a reset and initialization.
Manual initstring	Allows you to manually define a hexadecimal initialization string (entered under "Manual Initialization"). Use only for advanced/specific cases.
SND_NKE + Manual initstring	Combines *SND_NKE* with a user-defined manual init string. Useful for meters requiring both standard and customized commands.
Slave Select + SND_NKE	Selects a specific slave ID (secondary addressing) and then sends *SND_NKE*. Required for some multi-address or cascade systems.

7.1.12 Modbus registers

Adding a meter to the meterlist creates Modbus registers for each data record, enabling Modbus readout. The registers are accessible for review and manual modification in the **Modbus** tab, if required. To read out Modbus remember to set your slave port to Modbus in the Mbushub



Register	Device name	Device Description	Record number	Tag	MBus	ModBus	Value split
100	00000017LUP011A		-	StatusByte	INT8	INT16	-
101	00000017LUP011A		-	MeterID	INT32	INT32	-
103	00000017LUP011A		1	FabricationNo	BCD8	INT32	-
105	00000017LUP011A		2	ActualityDuration	INT24	INT32	-
107	00000017LUP011A		3	RFlevel	INT8	INT16	-
108	00000017LUP011A		4	TimePoint	INT48	INT64	-
200	00000091GAV0102		-	StatusByte	INT8	INT16	-

7.1.13 Export WebPort Config

The system supports exporting configuration data in WebPort format.

To export:

1. Navigate to the Modbus registers page

2. Click "Download"

3. Select "WebPort report"

This file can be used for integration with WebPort.

7.1.14 BACnet registers

When a meter is added, BACnet registers can be automatically generated from the BACnet application for each data record to enable BACnet readout. These registers can be reviewed in the BACnet tab.

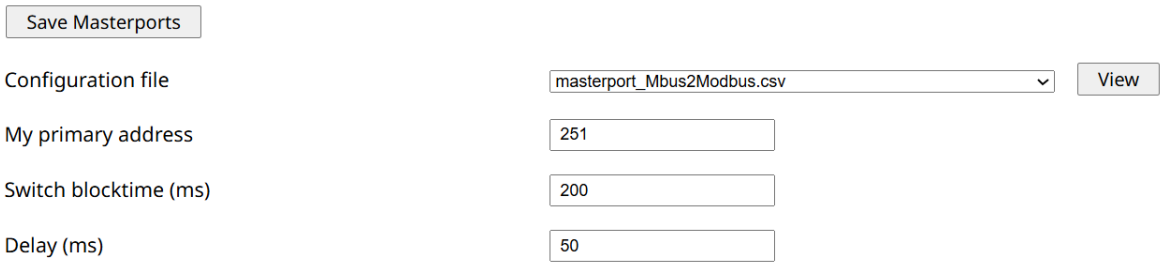
7.2 Mbushub

Masterport settings define communication with the meters.

Slaveport settings define communication with external systems.

The **Mbushub** section is where you configure the communication interfaces for both meter input (Master port) and output to external systems such as PLCs or SCADA (Slave ports). The default settings are for serial M-bus that works for most cases.

7.2.1 Master port configuration



Default settings usually work without adjustment. Change the Configuration file only for specific setups. (e.g. masterport_Mbus2Modbus.csv)

Configuration file – Only change this if you have created a special .csv file.

Primary Master port / Name – You can give the port a name to make it easier to identify in the interface.

Enable – Make sure the port is enabled before use.

Type – Choose how the master communicates:

Serial – for the built-in M-Bus master output (local connection to your M-Bus loops).

TCP – for communication over an IP network with a fixed connection.

UDP – for communication over IP using datagrams.

7.2.2 Additional timing settings

Switch blocktime – This defines how long the master waits for a follow-up telegram to the same meter (multi-telegram meters) before the M-Bus hub moves on to the next request.

Delay – This is the waiting time between two questions sent to the same meter, helping to avoid overload and ensuring stable communication.

7.2.3 Configure Communication Parameters

- **Com port**: Select M-Bus master (for serial) or enter IP and port (for TCP/UDP).
- **Baud rate**: Select the correct baud rate (e.g., 2400).
- **Timeout (ms)**: Define the timeout value before the operation fails (e.g., 2000).
- **Reconnect (s)**: Define how often to retry if disconnected (e.g., 1000).
- Click **Save Masterports** to apply all settings.

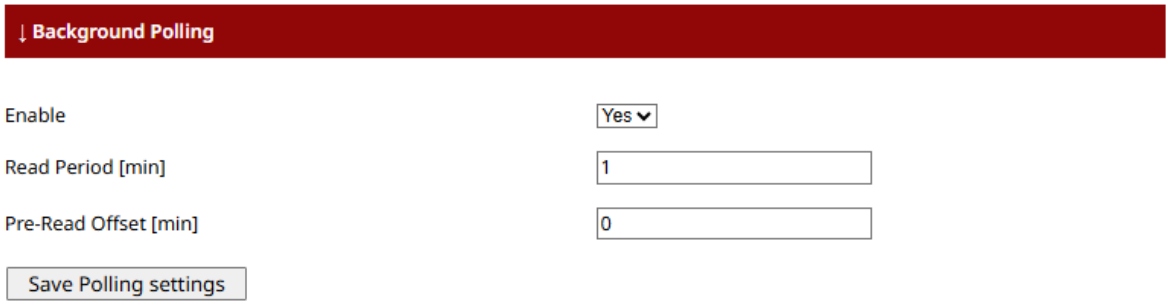
7.2.4 Background polling

Background polling is a function that continuously reads data from connected M-Bus meters in the background without external requests. The gateway periodically collects meter data and stores it internally, making it quickly available for systems that request the data.

To use background polling, enable the function in the configuration and define which meters to include along with the polling interval. A shorter interval gives more up-to-date data but increases bus traffic, while a longer interval reduces load on the M-Bus network.

To read out the cached values, choose "Cached M-Bus" as protocol on the slave configuration.

Enable background polling



To activate background polling:

1. Go to Background Polling in Masterport set up.
2. Set Enable to Yes.
3. Enter the desired Read Period [min] (how often meters should be read). Usually 1 second per read telegram. (Default is 3 telegram per meter).
4. (Optional) Set Pre-Read Offset [min] if needed. This is the time, in minutes, in advance the poling is set to read. (Used to fill Quickpost for example if the Read period is set to 60 minutes).
5. Click Save Polling settings to apply the configuration.

7.2.5 Slavport configuration

The slave port is used to connect the gateway to external control systems, such as PLCs or SCADA, using Modbus or other supported protocols.

Step 1: Enable and Name the Port

- Expand a slave port (e.g., **SlavePort 1**).
- Enter a **Name** (optional).
- Check **Enable** to activate it.
- Set the **Timeout (ms)** (e.g., 2000).

Step 2: Select Communication Type

- Under **Type**, choose:
  - Serial: for wired connections (RS-232, RS-485, M-Bus Slave)
  - TCP
  - UDP

If Serial is selected:

- **Com port**: Select interface (e.g., RS-232, M-Bus Slave 1)
- **Baudrate**: Choose appropriate speed (e.g., 2400)
- **Bit number**: Usually 8
- **Parity**: Choose Even, Odd, or None
- **Stop bit**: Usually 1

If TCP/UDP is selected:

- **Local port**: Enter the port number the slave service will listen to
- Under **Protocol**, choose Protocol.
- **Configuration file**: Select the .csv file that maps data to Modbus registers (e.g., slaveport_Mbus2Modbus.csv). To review or customize registers see Modbus section
- **Slave address**: Enter the Modbus slave ID (e.g., 1)
- **Float Mode**: Choose format (e.g., Big endian, ABCD)
- **Integer Mode**: Choose integer format (e.g., Big endian, ABCD)
- **Timeout Mode**: Select communication behavior on timeout (e.g., Mode 0)
- Click **Save slaveports** to confirm and apply all settings.

8 Data Export

The PiiGAB 900 series supports multiple export methods for transferring collected data to external systems. Available options include:

QuickPost: A flexible export method that can send measurement data via HTTP/HTTPS, or FTP/SFTP. Data is commonly structured in CSV or JSON formats and can be transmitted to local servers, cloud platforms, or designated custom endpoints.

FTP/SFTP (CSV): Automatically export structured data as CSV files to a designated FTP or SFTP server at scheduled intervals.

MQTT: Publish data to a generic MQTT broker or directly to Azure IoT Hub, allowing for real-time data transfer to IoT platforms or cloud services.

8.1 QuickPost

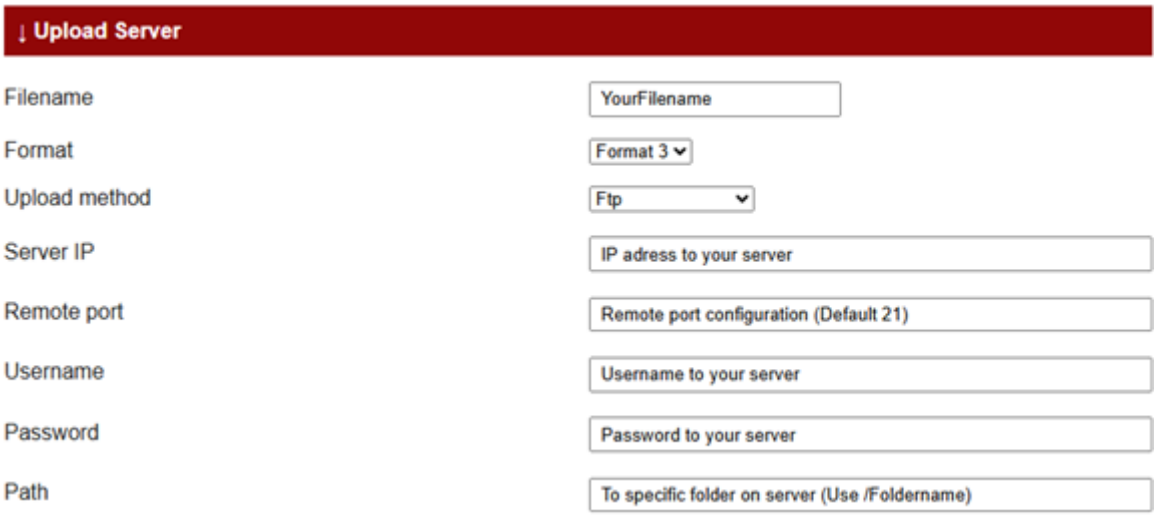
Start by configuring your QuickPost parameters (server, port, user credentials, and target path).

If you are using SFTP, remember that the first step is to go to the Security section and verify the host key. Without this verification, the connection will fail.

After verifying security, go to the QuickPost configuration page to finish setup.

8.1.1 Configuration options

Important settings include:



Note: No spaces in the filename, an timestamp will be added to the filename when the file is created.

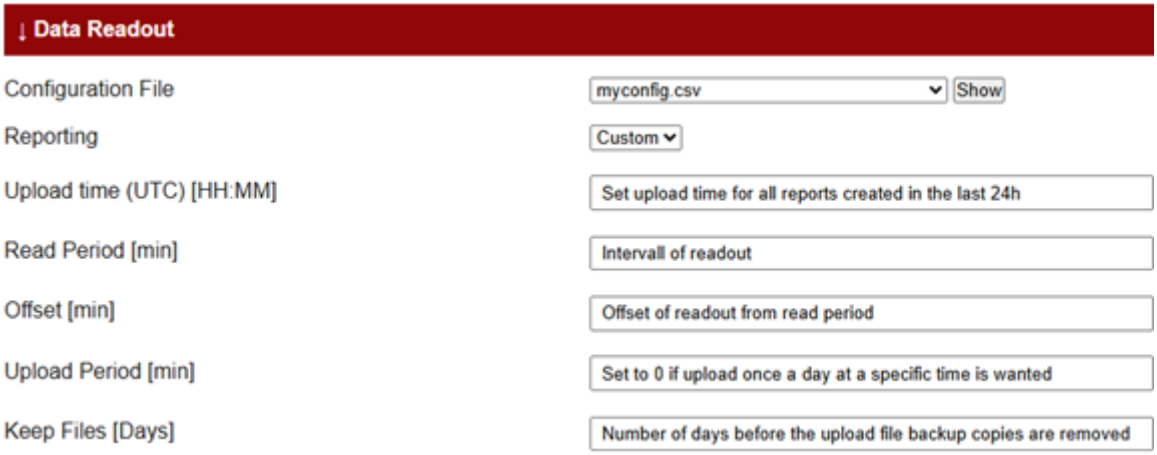
If configuration uses SFTP the Key must be used under the security-page

Remote port is standard “21” for ftp and “22” for sftp. If you use any other port this must be configured.

8.1.2 Data readout:

Default reporting intervals, 15min, 1h, 6h, 12h and 24h. if used the report will be sent when the readout is done.

Custom readout,



8.1.3 Security

SFTP supports both password and public/private key authentication.

Steps:

- Add your server IP and port.
- Write your server fingerprint (If your sftp provider has not provided you with this, it can sometime be scanned from the server).
- Press "Update Known Hosts".
- Go back to configure and save your configuration and restart your QuickPost.

8.1.4 Troubleshooting and verification

After completing the default QuickPost configuration, perform a meter readout and send a file.

The simplest way to verify that everything works is to check the "List file" view:

- If the file is updated correctly, contains no error codes, and is then moved under Result files → Stored files that have been successfully uploaded, the transfer has been successful.
- If the file is not moved down, but the full meter readout has been completed, go to the Log tab for more details.
- If you are using sftp, make sure your Fingerprint is correct.
- Make sure you have internet connection, some servers require the field "name server" in settings to be filled out.

8.1.5 Error codes in files

Can be seen in the QuickPost log and in the Mbushub log:

C = Checksum error

D = Wrong datatype

I = Unknown OPC item

M = Timeout (master port)

From QuickPost:

s = M-BusAscii client timeout

q/p/c = Incorrect ID or checksum

8.1.6 File formats

QuickPost supports five different file formats for exporting data. PiiGAB recommends Format 3 as the standard unless another system requires a specific format.

8.1.7 Format 1 – EMC (Legacy name)

Header:

command=DEVICE_STATUS OK,PiiGAB import file, Version 1.0

command=METER_READING delimiter=;

Content:

Channel_Device_Tag;Timestamp;Value

Time format: mm/dd/yyyy HH:MM:SS

Settings: timeformat=16, TagType=1 (or 8 for Record).

8.1.8 Format 2 – Simple CSV

No header row. Content:

Device;Timestamp;Value

Multiple tags per device may have identical names.

Time format: mm/dd/yyyy HH:MM:SS

8.1.9 Format 3 – PiiGAB Default

Header:

PiiGAB import file; FORMAT=3; Version=1.0

Content:

Channel;Device;Tag;Configurable Timestamp;Value;Unit;Medium;Description

Time format: configurable (8, 16, 24)

TagType: 1 (Value), 8 (Record).

8.1.10 Format 4 – Filename-Based

Filename:

<custom>_yyyymmddTHHMMSS.csv

Content:

Channel;Channel_Device;ISO8601 Timestamp;Floating point value

Note: Value must not use exponential notation.

8.1.11 Format 5 – Extended Format

Header:

PiiGAB import file; FORMAT=5; Version=1.0

Content:

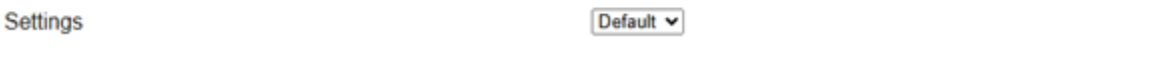
Channel;Device;Tag;Timestamp;Value;Unit;Medium;Tag Description;Device Description

8.1.12 Security

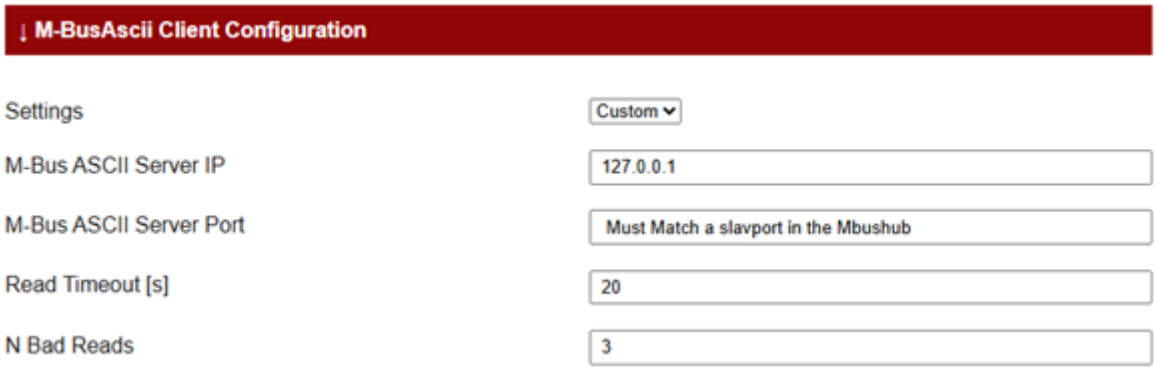
FTP lacks encryption and integrity protection. Use FTP only for non-sensitive data on trusted networks. If your gateway is online, use SFTP. FTP does not guarantee integrity protection; customers must ensure proper isolation.

8.1.13 Configuration of M-BusAscii Client:

By using the default setting an internal client port gets used without occupying a client port from the Mbushub. **This is only used for troubleshooting or special applications.**



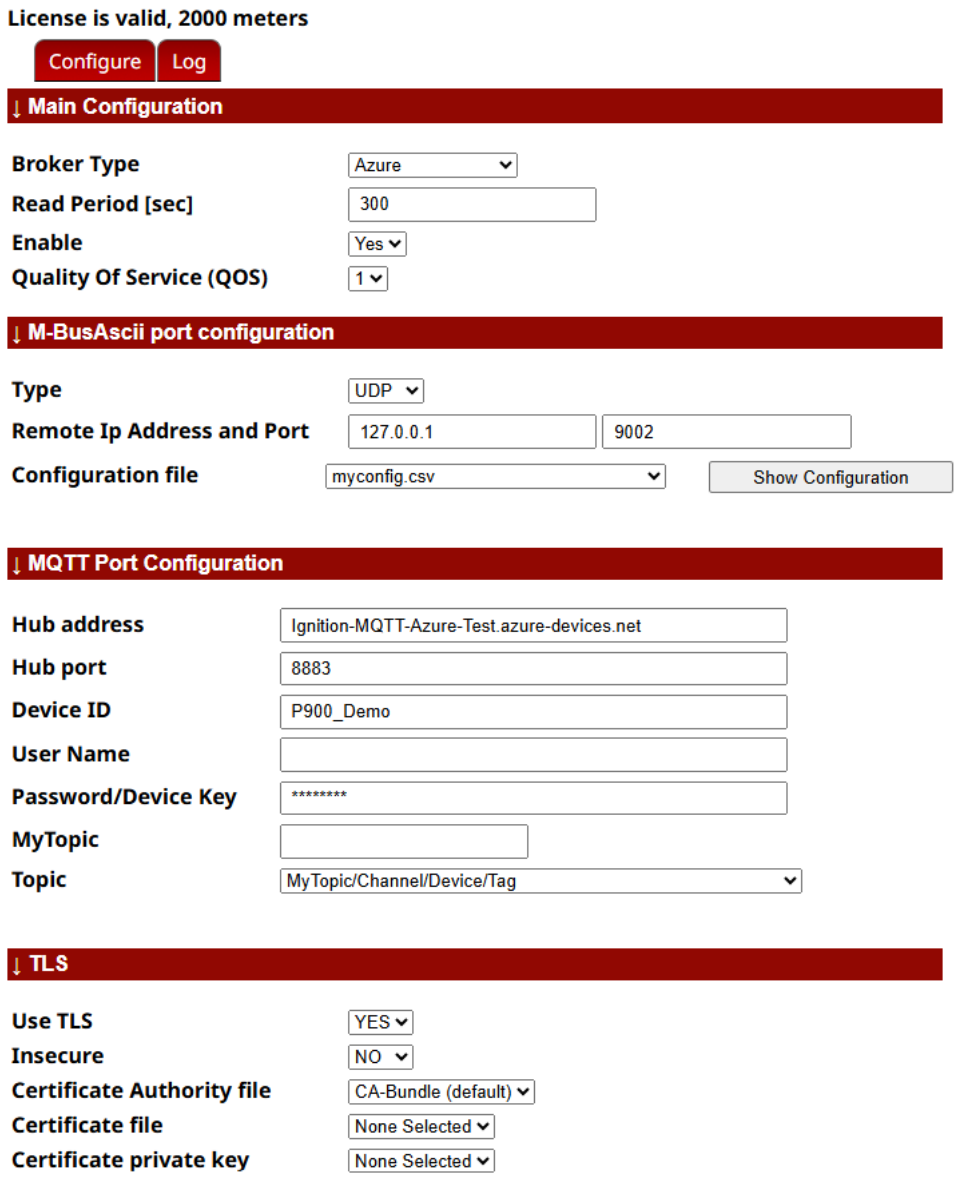
If set to custom:



This configuration can be used if the slave port timeout must be changed.

8.2 Mbus2Mqtt

This manual applies to MBus2MQTT version 1.1.4.2 or later. The application requires MBusHub version 2.4.6 or higher. It is used to publish M-Bus data to an MQTT broker using values read from MBusHub.



8.2.1 MQTT to Azure

Azure	
Parameter	Value
Broker Type	Azure
Read Period	600 (10-minute)
Enable	Yes
QOS	1
M-BusAscii Type	UDP
Remote IP and Port	127.0.0.1:9002
Configuration File	myconfig.csv
Hub Address	Azure address
Hub Port	8883
Device ID	Azure Device ID
Password/Device Key	Azure Device Key
Use TLS	YES
Insecure	NO
CA File	CA-Bundle (default)

8.2.2 Standard MQTT with/without TLS (Per meter/per record):

Parameter	**Value**
Broker Type	MQTT
Read Period	600 (10-minute)
Enable	Yes
QOS	User configurable
M-BusAscii Type	UDP
Remote IP and Port	127.0.0.1: 9002
Configuration File	myconfig.csv
Hub Address	Azure address
Hub Port	8883
Device ID	User configurable
MyTopic	User configurable
Topic	User configurable
Password/Device Key	User configurable
Use TLS	YES/NO
Insecure	NO
CA File	CA-Bundle (default)

8.2.3 MQTT with self-signed certificates:

Choose a file and Upload a Certificate in "MQTT Advanced parameters".

Parameter	Value
Broker Type	MQTT
Read Period	600 (10-minute)

Enable	Yes
QOS	User configurable
M-BusAscii Type	UDP
Remote IP and Port	127.0.0.1: 9002
Configuration File	myconfig.csv
Hub Address	Azure address
Hub Port	8883
Device ID	User configurable
MyTopic	User configurable
Topic	User configurable
Password/Device Key	User configurable
Use TLS	NO
Insecure	NO
CA File	Uploaded Certificate
Certificate file	Certificate file
Certificate private key	Certificate private key

8.2.4 MQTT Payload Format:

- Per Record: Each message contains one M-Bus data record
- Per Meter: All records from one meter in one message
- Azure: JSON array with records from multiple meters

Example payload:

Payload: {"v": 39.9, "u": "V", "ts": "2024-08-30T08:32:15Z", "q": "0x00C0"}

8.2.5 Troubleshooting:

1 Ensure correct configuration file is selected
2 Verify unique and correct Device ID
3 Remove Username and Topic for Azure
4 Set 'Insecure' to NO for production
5 Set TLS CA to 'CA-Bundle (default)' unless using self-signed certificates
6 Try different QOS levels if delivery fails

8.2.6 M-BusAscii Error Codes:

I: Unknown OPC item

T: Timeout from slaveport

M: Timeout from masterport

9 Conversions from M-bus

The PiiGAB 900 series supports advanced protocol conversion, enabling seamless data translation between systems using different communication standards as well as transparent Mbus.

M-Bus to Modbus: Converts M-Bus meter values into Modbus registers (RTU or TCP), allowing easy integration of M-Bus devices into Modbus-based SCADA or PLC/DUC systems.

M-Bus to BACnet: Translates M-Bus data into BACnet objects, making it possible to use metering data within building automation systems and BACnet-compatible monitoring platforms.

9.1 Mbus2Mbus Transpararent/Cached values

The MBus2MBus IP feature allows the PiiGAB 900 to share M-Bus data from its internal slave port to another M-Bus master over TCP/IP or an serial interface. This makes it possible to reuse existing M-Bus readouts in other systems without physically duplicating the bus.

9.1.1 Workflow

1. Navigate to the M-Bus Hub section on the Slaveport page.
2. Select which slave port you want to expose over MBus2MBus IP (The slave port acts as a virtual M-Bus device presenting internal data to remote masters.)
3. Configure the Slave Port (Define communication parameters
4. Save the Settings, the slave port will now be available for transparent or cached Mbus
5. Verify the Readout using for example M-bus Wizard

9.2 Mbus2Modbus

The M-Bus2Modbus functionality allows the PiiGAB 900S/T to act as a bridge between M-Bus meters and external Modbus-based systems (such as PLCs, SCADA, or BMS). This function is configured through the Mbushub section by defining one or more slave ports that expose M-Bus meter data as Modbus registers. When a meter is added, Modbus registers are automatically generated for each data record to enable Modbus readout. These registers can be reviewed and manually modified under the Modbus tab in meterlist if needed.

To expose meter data to Modbus clients, configure a **Slave Port** using the following steps:

Step 1: Enable Slave Port

1. Navigate to Mbushub → Slaveports
2. Check **Enable** to activate the port.
3. Enter a descriptive **Name** (e.g., *Modbus Slave*).
4. Set the **Timeout (ms)** value, e.g., 2000.
5. Select Port Type

- **Type**: Choose Serial, TCP, or UDP based on your setup.
  - **Serial** for RS-232/RS-485 communication.
  - **TCP** for Ethernet-based Modbus TCP server.
  - **UDP** if required by the Modbus client.

If using **Serial**:

- Select **Com port** (e.g., RS-485).
- Set **Baudrate** (e.g., 2400), **Bit number** (8), **Parity** (Even), and **Stop bit** (1).

If using **TCP or UDP**:

- Enter the **Local port** to be used (e.g., 502 for Modbus TCP).
- Under **Protocol**, select **Modbus TCP** (or **Modbus RTU** for serial).

9.3 Mbus2Bacnet

MBus2Bacnet is an application that converts M-Bus data to BACnet analog-input objects, allowing integration of M-Bus meters into BACnet-based systems. This guide explains how to configure and operate the MBus2Bacnet application effectively.

9.3.1 Overview

Function: Converts M-Bus data to BACnet analog-input objects.

Data Handling: Values are read periodically (based on UpdateInterval) and remain constant until the next readout.

Error Handling: If a meter fails to respond, MBus2Bacnet retries up to the configured number. On failure, the Reliability property is set accordingly.

9.3.2 Configuration Workflow

1 Create Configuration from myconfig.csv
2 Enable BACnet application
3 Navigate to the MBus2Bacnet interface
4 Choose BACnet Object Name format
5 Press "Create From myconfig" to generate BACnet configuration automatically (Existing configuration will be overwritten.)
6 Press "Save configuration"

9.3.3 BACnet Object Name Formats:

BACnet object names are auto-generated based on one of three formats:

Format	Example
Device.Tag	12345678PII0102.StatusByte
DeviceDescription.Tag	MainMeter.StatusByte
DeviceDescription.TagDescription	MainMeter.Status

Device Description and Tag Description are taken from the Startup Config and Template pages respectively. If a description is missing, it falls back to Device and Tag.

9.3.4 Main Configuration Buttons

Create From myconfig: Generates the entire configuration from the current myconfig.csv.

Export EDE: Exports configuration in Siemens EDE format

Restart: Restarts the BACnet application (does not save changes)

Reset Config: Restores factory default settings

Enable Bacnet: Enables or disables the application (default: Disabled). Should remain disabled if not in use to conserve M-Bus bandwidth.

9.3.5 Configuration Parameters

Parameter	Description	Default Value
ServerName	Sets the Object Name of the BACnet Device Object. This is the visible name in BACnet clients and should be unique within the network.	Pi900-<serialno>
ServerIdentifier	Defines the BACnet Device Instance number. It must be unique within the BACnet network to avoid conflicts.	250001
ServerDescription	A textual description of the BACnet device. Displayed in some BACnet clients for reference, but not required for functionality.	"M-Bus to Bacnet"
ServerLocation	Describes the physical or logical location of the device. Helps with identification in larger BACnet systems.	Sweden
UpdateInterval	Specifies how often the M-BusAscii server is polled, in seconds. This interval also determines the "Max Age" of the BACnet object value for clients.	300 (5 minutes)
Channel	Sets the OPC channel name. This must match the channel name used in the myconfig.csv file to link with the correct tag definitions.	Gateway ID as default
BBMD_Address	IP address of the **BACnet Broadcast Management Device (BBMD)**. Required if the BACnet network spans multiple IP subnets (e.g., VLANs or routed networks). A BBMD allows BACnet broadcast traffic (used for device discovery and communication) to cross subnet boundaries. Leave empty if all BACnet devices are on the same subnet.	(empty)
Bacnet Port	The UDP port used for BACnet/IP communication. The standard port is 47808 (hex: BAC0), and it typically does not need to be changed unless another port is specifically required.	47808 as default
APDU_Timeout	Timeout in milliseconds for waiting on a BACnet Application Protocol Data Unit (APDU) response. Increase if the network has high latency.	(optional)
APDU_Retries	Number of retries if no APDU response is received within the timeout. Helps increase communication reliability on bad networks.	(optional)

Timeout	Timeout for M-Bus communication in milliseconds. 2500 ms is a recommended value for dedicated slave ports. Lower values can be used on shared (non-exclusive) ports.	2500
Retries	Number of retry attempts made if a M-Bus read operation times out. This increases robustness for unstable M-Bus devices.	3

9.3.6 Config file

Allows users to add custom configurations.

9.3.7 BACNET Log

The log is used for finding error in the BACnet.

10 Conversions to M-Bus

10.1 Wireless M-Bus to M-bus

10.1.1 Setting a primary address on a wireless meter

1 Go to Settings and click on "Download .csv, .xml, .ini files".
2 Download the file named wireless_include_startup_config.csv.
3 Open the file using Excel or a text editor (e.g., Notepad).
4 Set the primary addresses according to the values below (Column 2):

00037825.3033.0A.2B;1;809686E989EF7867F986F1C21D2C5653

00080553.3033.09.1B;2;68BBDD5B91613210ACF05DBCD1E71F5B

00153945.3033.09.1B;3;3AF39C336017002B7D66F515832C94A8

00153946.3033.09.1B;4;BB471D5A5C6B01F90D6464C7FBBCBAF9

02005514.3033.07.1B;5;0B2466FA2070048A2379D7B2158A268A

04010954.3033.0A.2A;6;858C435B1ADFD8CFF12FC2B9088B96DE

04011020.3033.0A.2A;7;58FDE313F1818A80DF2801EC60B87021

5 Save the file with a new name and upload it back to the gateway.
6 Go to the Wireless application (under Installed Software).
7 Select your new include file and click Save.

10.2 Modbus2Mbus

Connect the Modbus Meter to the PiiGAB 900

Physically connect the Modbus meter to one of the supported communication ports on the PiiGAB 900, such as RS-232, RS-485 or Ethernet, depending on the meter's interface and protocol support.

Identify the Registers You Want to Read

Use the Modbus meter's documentation to determine the correct registers:

1 Locate the required register addresses
2 Check the data type of each register (e.g., float32, integer)
3 Confirm the unit of measurement (e.g., Wh, m³, °C)

10.2.1 Verify Communication with the Meter

You can test communication via the **Modbus Reader** in the PiiGAB 900 web interface.

- Select a test register from the meter's documentation.
- Verify whether the meter uses 0-based or 1-based addressing.
- Choose and test the correct register format:
  - Big Endian (ABCD)
  - Little Endian (DCBA)Mbus2
  - Register Swap (CDAB)

- Byte Swap (BADC)

This helps ensure the correct decoding of register values.

10.2.2 Create the Meter Configuration using the PiiGAB Modbus2MBus Config Tool

Add a Device

1. Open the PiiGAB Modbus2MBus Config application.
2. Click **Add Device**. Each device corresponds to a physical Modbus meter.
3. Enter a **Secondary Address** and **Name** for the device.
4. Select the correct **Medium** (e.g., Electricity, Heat, Water).
5. Set Modbus-specific parameters:
   - Slave Address
   - **Init Function** (e.g., Function 3 – Read Holding Register)
   - **Init Register** (starting register)
   - **Base**: choose 0 or 1 based on address offset
   - **Float Mode**: specify byte order (e.g., 0 = ABCD)
   - Modbus Protocol: TCP or RTU

Add an Object

1. Select the device you created.
2. Click Add Object.
3. Each object represents one Modbus register you wish to map to M-Bus.

10.2.3 Define Object Properties

For each object, fill in the following fields (refer to the meter's register map):

- **Name**: Descriptive name for the object
- **Object ID**: Unique ID
- **Read Register**: Modbus register address
- **Data Type**: Based on the meter (FLOAT, INTEGER, etc.)
- **VIB / VIF**: M-Bus coding for the measured value
- **Function**: Typically "3 – Read Holding Register"
- **Unit**: Based on physical value (e.g., W, m³/h, °C)

10.2.4 Transfer the Configuration to the PiiGAB 900

1. Save the configuration file from the Config tool (*.xml).
2. Upload the file to the PiiGAB 900 via the **Modbus2MBus** section in the web interface or in Upload file in Settings page.
3. Under **Configuration File**, select the uploaded CSV.
4. Configure Modbus Port configuration in Modbus2mbus based on how meters are connected.
5. Register each virtual Modbus meter under **Meter Parameters** by entering the matching **ID number** used in the config file in meterlist by adding single meter.
6. Click **Save**.

After this step, the Modbus-based values will appear as virtual M-Bus meters and can be read/exported accordingly.

10.3 DLMS2Mbus

The DLMS2MBus application enables protocol conversion from DLMS/COSEM to M-Bus, allowing a limited types of DLMS-compatible meters to be integrated into M-Bus-based systems.

Meters are connected via RS485, and the application reads selected data from each DLMS meter and exposes it through a virtual M-Bus interface in the gateway.

10.3.1 Configuration Workflow

1 Connect the meters via RS485 to the communication port on the device.
2 Enable the DLMS2Mbus application by setting "Enable" to Yes in the interface.
3 Create and upload a CSV file with headers Primary,Meter Type,ID,Free text,Description and example rows like 1,NORAX10,60197046,M_60197046,TEST1.
4 Save settings to apply the configuration and start periodic meter readouts.
5 Go to meter list and in the "search tab", choose to include "DLMS2Mbus" and start the search.

10.3.2 Results tab

Monitor meter data in the Results tab.

10.3.3 Logs

View communication logs in the Log tab.

1 Start the log by clicking the "Start" button.
2 Wait for activity to be recorded (e.g., meter readouts or communication events) .
3 Click "Show" to display the current log entries.
4 Click "Clear" to erase the log contents.

10.4 Han2Mbus

The Han2Mbus program converts M-Bus messages from your smart electricity meter into virtual M-Bus meters. These virtual meters can then be configured and read in your systems through a PiiGAB 900S gateway.

10.4.1 RJ45 Connection

- Your smart meter must first be activated by your grid operator.
- The meter sends M-Bus data through a modified RJ45 cable, which is connected to the M-Bus slave ports of your 900S device.
- With Han2Mbus it is possible to read up to two smart meters per 900S.
- Note: Han2Mbus will overwrite any previous configuration on slave port 1 and 2 of the M-Bus hub.
- To use slave ports for other readings, additional client ports must be activated via license.

Important: Do not connect the RJ45 cable to the Master ports of the gateway.

Visit HANporten.se for detailed instructions on how to build the cable. Polarity of the slave port connections does not matter.

10.4.2 Configuration Steps

- Go to Installed Software and select Han2Mbus.
- Open the Configuration tab.
- If you connected your meter to M-Bus slave port 1, configure port 1. If you connected to slave port 2, configure port 2.
- Identify your smart meter brand and refer to the recommended settings below:

Meter type	Baudrate	Bit number	Parity	Stop bit
Aidon	2400	8	E	1
Kaifa	2400	8	E	1
Kamstrup	2400	8	N	1

- Select Meter Type and enable the port for HAN meter reading by setting Enable = Yes.
- M-Bus Primary Address (0–254): This will be the address of the virtual M-Bus meter in your configuration. The address is visible on the overview page and in other connected systems.
- M-Bus Secondary Address: Enter a unique 8-character combination. This will be the secondary address of the virtual M-Bus meter. It will also be visible in the overview page and other connected systems.
- Click Save Settings to store the configuration.
- Verify that data is received under the Results tab. The meter usually sends new data every 10 seconds.
- Once you confirm that data is read correctly, click Add Meters at the bottom of the Configuration page. This adds the virtual meters to the meter list, allowing you to configure them as standard M-Bus meters and generate your own configuration

10.4.3 Troubleshooting

- **No data in the log:** Check with your grid operator to ensure the meter has been activated.
- **Incorrect data in Results:** Adjust **Bit number, Parity, and Stop bit** parameters.
- **No voltage in the meter contact:** The meter follows the M-Bus standard and should supply **24–40V** on the bus line.

11 Getting Started with the PiiGAB API

The PiiGAB API allows external systems to access meter data, configuration, and logs from the 900 Series gateway in a secure and automated way.

Before you begin, ensure that your device firmware is up-to-date and that HTTPS access is enabled.

A complete description of available API endpoints is included in the downloadable documentation:

Security → API Tokens → Download API documentation

This document describes:

Base URL structure and authentication header format

Meter readout endpoints (GET/POST)

Configuration upload/download

Log retrieval and system status queries

11.1.1 Testing meters

You can easily test reading a meter directly via the gateway's REST API and at the same time view the JSON structure.

Open a web browser and enter the following address:

http://IP/api/v2/devices/10000001.4129.10.0e

Where:

IP = the IP address of your PiiGAB 900

10000001.4129.10.0e = the meter's secondary address (adjust according to your meter)

When you access this URL:

The gateway performs a readout of the specified meter.

This is a quick way to:

- Verify that communication with the meter is working
- Confirm that the correct secondary address is being used
- Inspect the exact data structure before integrating with a supervisory or third-party system

11.1.2 Generate an API Token

1. *Log in to the web interface of the gateway as an administrator.*
2. *Navigate to Security → API Tokens.*
3. *In the Description field, enter a short note identifying where the token will be used (for example QuickPost Integration or Building SCADA).*
4. *Click Generate API Token.*
5. *Copy and store the token safely — it will only be displayed once.*
6. *The list below shows all active tokens with creation date and the option to delete them.*

Treat API tokens like passwords. Tokens provide direct access to gateway functions and should only be issued to trusted systems.

Error codes and response formats (JSON)

Typical requests use the HTTPS protocol and include the token in the header:

GET https://<device-ip>/api/meters

Authorization: Bearer <your_token>

11.1.3 Example Use Case

To retrieve a list of meters from the gateway:

curl.exe -k -X GET `

"https://10.13.0.60/api/v2/devices" `

-H "accept: application/json" `

-H "Authorization: Bearer eee290b067311bd3431d1f1dabd604bf6be34cbec4ef6e370cc2f2f2338199ae"

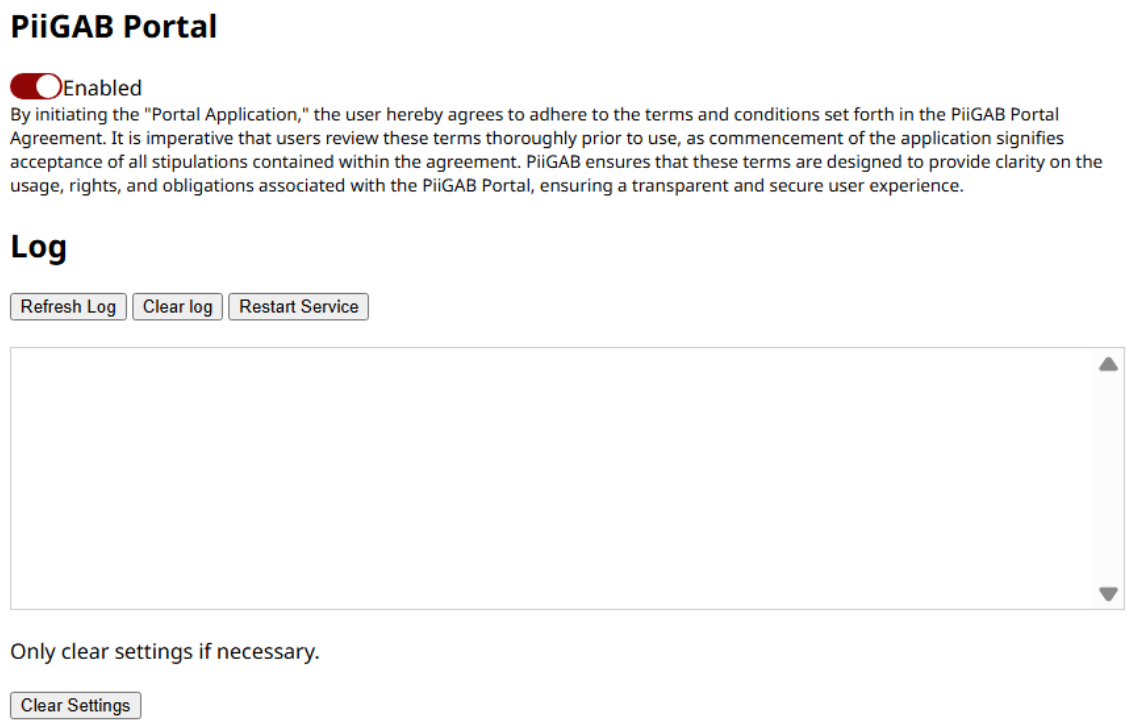
The server will return a JSON list of all meters configured in the device.

To start a secondary search:

curl.exe -k -X POST "https://192.168.10.162/api/v2/search/secondary" -H "Authorization: Bearer eee290b067311bd3431d1f1dabd604bf6be34cbec4ef6e370cc2f2f2338199ae" -H "Content-Type: application/json"

12 Portal client

This application manages the VPN connection as well as all communication with the cloud. Enable it to establish communication with PiiGAB Connect or when using PiiGAB PLUS!



13 Trouble shooting

This section provides guidance for identifying and resolving common issues related to communication, configuration, and data readouts. Use it to quickly diagnose problems and restore normal operation.

Remember to always update the software to the latest versions. We continuously update the software to create an better experience for the user, if you do not update the software you risk unnecessarily spend time on trouble shooting errors fixed in newer versions.

Check you license, many issues are related to the license, either you miss the license for the application, or the license is limited in your device. Please contact PiiGAB for a license upgrade.

13.1.1 Cannot find the gateway on the network?

1. Connect the gateway directly to your computer.
2. Set a static IP address on your computer within the 192.168.10.100 range.
3. Go to "Find Gateways" in the network section and check if your gateway appears.
4. If the gateway is not found, go to the Wizard and change the gateway's IP settings.
5. Enter the gateway's MAC address (found on the side of the unit).
6. Choose Static IP.
7. Enter the IP address 192.168.10.80.
8. Enter the subnet mask 255.255.255.0.
9. Leave the gateway field empty.
10. Click "Next" and apply the settings. There will be a message that the gateway doesn't respond.
11. Check again with "Find gateways" in the Wizard to see if the gateway appears.

13.1.2 No LEDs on the Network Port?

1. The network cable may be damaged. Try to replace the cable.
2. Try placing a switch or router between the PC and the gateway to test the connection.
3. The IP address on the PC may not have changed. Make sure you IP is set to static.
4. In the Wizard, check that the network adapter is available in the adapter list.

13.1.3 Cant find my M-bus meters or read the values

1. Verify module and system version, as well as the current license status of the gateway.
2. Check the electrical information for M-Bus Meters, verify voltage and current levels on the M-Bus loop. Voltage should be around 39 V and current levels is 1.5 mA per connected load.
3. Check you license for how many loads you are allowed to read.
4. Review M-Bus Hub settings, including port assignment and baud rate. Go to chapter Mbushub for default set up.
5. Use "Search for meters" in the Wizard to detect meters by Primary/Secondary Address. If you find them in M-bus Wizard, but not in the web interface search, try adding them as a single meter to see if they respond. On read meters you can change readout settings.

6. Test Changing the Local Port, sometime there is disturbance on the UDP/TCP port. Ensure there are no overlapping requests causing communication collisions.
7. If traffic is high, temporarily switch off all other slave ports for testing purposes.
8. Review Timeout Settings on Slave Ports and Master port. Ensure the timeout value is sufficient, especially at low baud rates.
9. Check that Slave port timeout should be same or larger than master port timeout.

13.1.4 My meter responds on slave select but I get no telegram

1. Does the meter respond to Slave Select? Check the log and see master Out from SlavePort: 68 0b 0b 68 xx xx xx .. The expected response from the meter is E5.
2. Try using the primary address instead
3. Try changing the request type.
4. If the secondary address contains FF you meters are faulty, however we can, for a service fee, reconfigure the gateway to use primary addressing instead.

13.1.5 Short circuit or disrupting meters

If you have a short circuit this means one or more of your meters are overloading your M-bus line. This method for finding the errors can be used to narrow the problematic meters down.

Note: This method only works if multiple loops are correctly used and configured on the device.

1. Initial Check: Make sure that multiple M-Bus loops are actively in use and correctly configured on the device.
2. Divide and Isolate: Disable half of the active M-Bus loops.
3. Click "Save hardware settings", then test the communication with your meters again.
4. Evaluate and Repeat: If the issue persists, continue to disable the other half of the remaining active loops and enable the first half.
5. Repeat the process until you identify which specific loop is affected.

This step-by-step isolation method helps narrow down and identify which loop or connected meter is causing interference or communication issues on the M-Bus network.

13.1.6 Meters stops responding, after resetting the meter it works again for a while

This can be done

1. Go to Mbushub, scroll down to Hardware settings
2. Change periodic rest to ”Yes”. This allows the gateway to power of the M-bus line periodically once every 24 h.

13.1.7 Loosing values sporadically

If you are regularly losing meter values, the easiest solution is to periodically read and cache the values in the gateway. To do this, follow these steps:

1. Go to M-Bus Hub and open the MasterPort tab.
2. Enable the option “Background polling”.
3. In the Template settings, adjust the “Max request retries” parameter – In some cases, up to 10 retries per meter may be necessary.
4. If there is still issues in readout, look into to the Mbushub log, if the error is related to the slaveport timeout, try increasing the slaveport timeout, if it is Masterport timeout, increase both the slaveport timeout and masterport timeout.
5. If this is not working, there is a delay on the Mastertport configuration, try adjusting it, some meters and extenders require up to 400 ms delay.

13.1.8 Cannot find my wM-bus meters

1. Start by going to the wM-bus application
2. Go to “meterlist” page, and see whether you can find your meter
3. If not, use a wireless M-mbus sniffer to see whether the meter is avaible at the location of the gateway.

13.1.9 I can see my wM-bus meters in the wM-bus application, but not in the meterlist

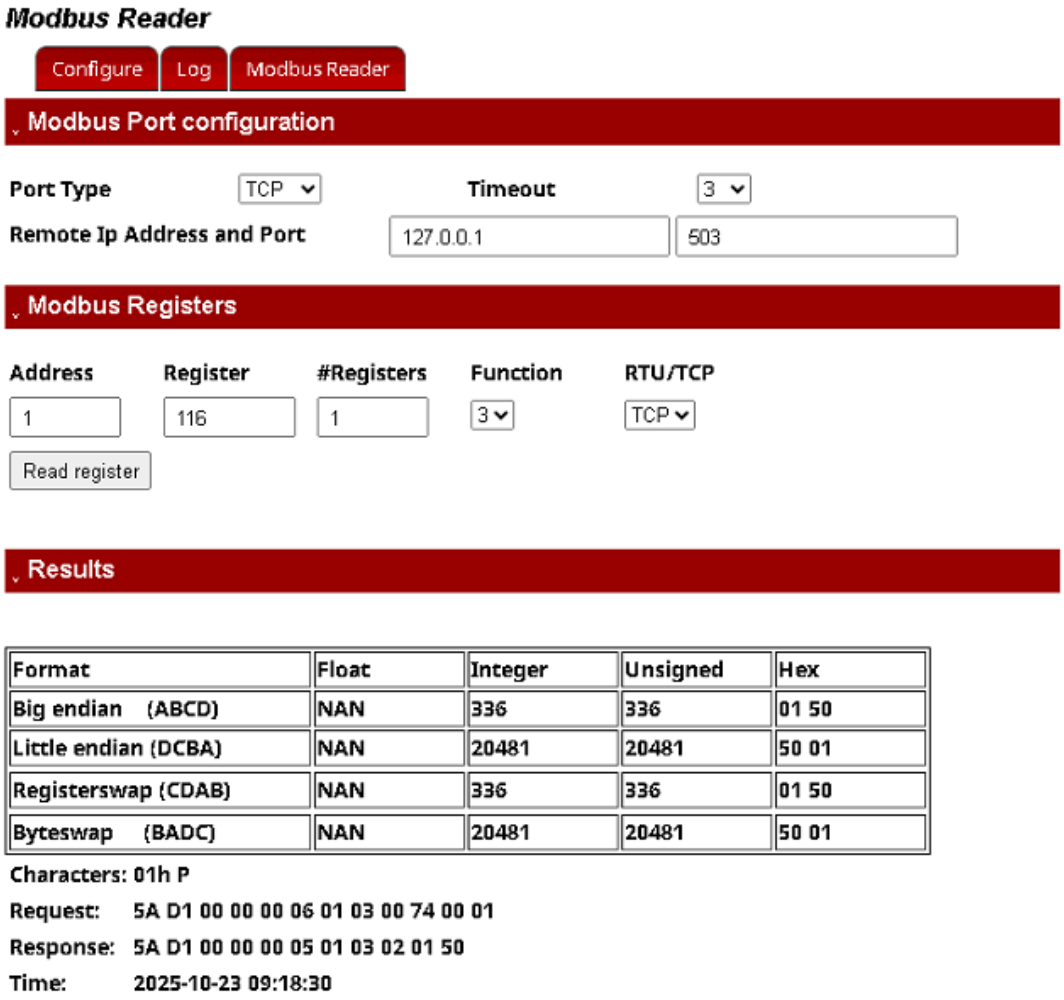
1. Check how many wireless meters your allowed in your license, if there is to many meters in the air, you need to change the include and exclude file, or upgrade you license.
2. Make sure there are no strange letters or numbers in the secondary address

13.1.10 I get no values on Modbus readout

1. Check that the M-Bus meters are properly detected and properly configured in the meterlist.
2. Make sure that you are receiving correct values by opening the meters in the meterlist. If you receive no values, go to **“Cant find my M-bus meters or read the values”.**
3. Verify the Modbus configuration file to see which registers are being queried.
4. Under MasterPort, ensure the masterport config file is set to masterport_mbus2modbus.
5. Under SlavePort, make sure MasterPort is set to slaveport_mbus2modbus.
6. Use the M-Bus Wizard or the internal Modbus reader to read the register that is being requested.
7. Check the Mbushub log whether there is communication from the slaveports.
8. If you are using RS485, try switching cables and make sure you got the correct polarity.

Try using the internal Modbus reader:

1. Set one of the slaveports to Modbus TCP and choose the "slaveport_mbus2modbus".
2. Go to "Modbus2Mbus and the "Modbus reader" page.
3. Set the IP to 127.0.0.1 and the set port from the slaveport.
4. Try one of the Modbus registers. In the case below the register is a int16 amd the correct value is found in "Big endian" and "Integer" showing that the conversion is correct.
5. If you get the correct value in the Modbus reader but still receive the wrong value or error move to the next point.
   Note that after verifying the Modbus value with Modbus reader, the TCP socket it closed by the reader. Press "Save settings" on the Modbus application to reset the connection.



Using Modbus parser

1. Start the Mbushub log
2. Copy the Modbus request on the Slaveport
3. Paste it to a Modbus parser (Google for modbus parser)

Part of Data Package	Description	Value
45 C4	Transaction identifier	0x45C4 (17860)
00 00	Protocol identifier	0 = MODBUS protocol
00 06	Length	0x0006 (6)
01	Unit identifier	0x01 (1)
03	Function code	0x03 (3) - Read Holding Registers
00 64	Starting address	Physical: 0x0064 (100) Logical: 0x0065 (101)
00 01	Quantity	0x0001 (1)

4. Make sure the Modbus request matches your expectations and slaveport settings
5. Copy the Modbus response to the parser.

Part of Data Package	Description	Value
73 89	Transaction identifier	0x7389 (29577)
00 00	Protocol identifier	0 = MODBUS protocol
00 05	Length	0x0005 (5)
01	Unit identifier	0x01 (1)
03	Function code	0x03 (3) - Read Holding Registers
02	Byte count	0x02 (2)
00 00	Register value	0x0000 (0)

6. Check the Value if it is the expected Value. If the value is the expected number your issues is most likely related to the system reading Modbus
7. Look into the data types, does your system support the data type in the Modbus?
8. If the Value is different or error, the issue is most likely related to an internal difference in Modbus registers. Make sure the Slaveport and Masterport files are correct.

13.1.11 I can read the values in the Web interface but MQTT/QuickPost only shows error

1. Check if the application is running– This is easiest done by looking under the Log tab.
2. Enable the M-Bus Hub log– Then restart the export application (e.g. MQTT or QuickPost).
3. Check the M-Bus Hub log– Look for any incoming traffic from the export application.
4. If no traffic appears– Verify that the correct communication settings are configured in the application.
5. For QuickPost: M-Bus ASCII Server IP: 127.0.0.1 M-Bus ASCII Server Port: 9002
6. For MQTT: M-Bus ASCII Port Configuration: IP: 127.0.0.1 Port: 9004

13.1.12 Portal client is enabled but gateway is offline in the portal

1. Make sure your gateway has internet connection (Ping function found under ethernet settings), go to settings and ping Piigab.microservicebus.com.
2. Restart the service on the Portal application page.
3. Clear the settings file under the PiiGAB Portal application page and restart the Portal application again.
4. Check Gateway Status: Ensure that the service is online on the Gateway in the web interface. You can do this by pressing "Refresh Log" in the Portal Application to view the status and any error messages.
5. Verify that the gateway setting is correctly configured to enable communication with the PiiGAB Portal. Under "Administration" you can test ping piigab.microservicebus.com to ensure connection to the server. if your ping fails, you might have an issue with the resolution of hostname to ip. Please check that your hostname is correct. If you dont know what hostname to set, then we recommend to set it to 8.8.8.8.
6. Verify that you have the correct date and time in your gateway settings.
7. Contact PiiGAB's technical support for further assistance. Restart the Portal client, wait for approximately one minute and refresh the log. Send it to PiiGAB.

13.1.13 My SFTP server provider doesn't supply the server fingerprint

1. Open CMD/Terminal
2. Print the following: ssh-keyscan "URL" | ssh-keygen -lf –

Verifying an SFTP key is a critical security measure that ensures the integrity and authenticity of the connection between a client and a server. When an SFTP provider verifies the key, it confirms that the connection is being made to the correct and trusted counterpart, rather than to a malicious or unauthorized server.

Without key verification from the host, attackers could perform a ***man-in-the-middle (MITM)*** *attack—intercepting or altering the data being transferred without detection. This could lead to unauthorized access, data theft, or manipulation of sensitive information.*

Key verification also helps to ***maintain data confidentiality*** *and* ***prevent impersonation****. By confirming the server's identity, both parties can exchange data with confidence that it is protected by encryption and integrity checks.*

In summary, verifying the SFTP key ensures:

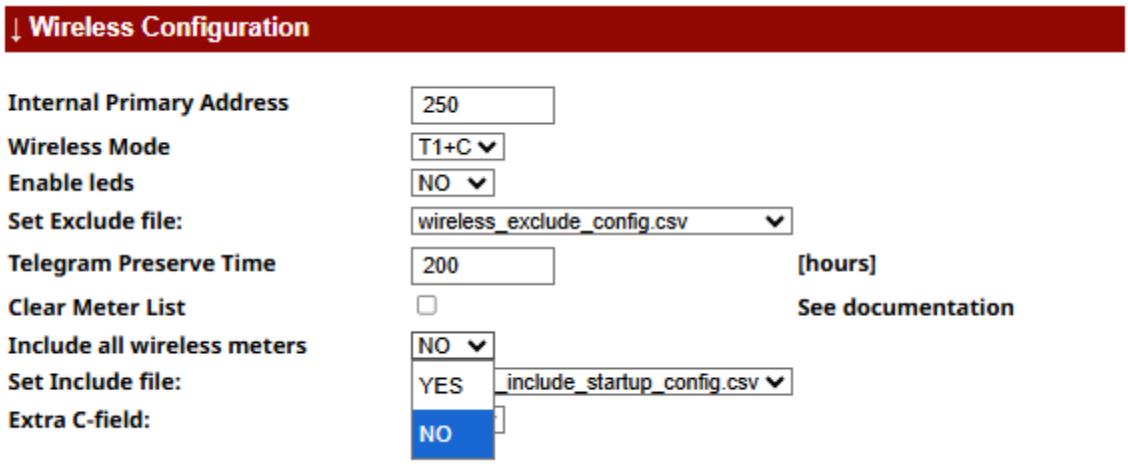
- *The connection is made to a trusted and intended server.*
- *Protection against interception or data tampering.*
- *Compliance with security best practices and data protection policies.*

Neglecting this step undermines the entire purpose of using SFTP as a secure file transfer protocol.

13.1.14 Disable Wireless M-bus

1. Open Wireless application in gateway

2. On "Include all Wireless meters", set "NO".



3. Set Exclude file to Wireless_exclude_config.csv"
    a. Format should be as below. Some older versions can have other formats. Edit the exclude file in the bottom of the page on "Edit Configuration Files":

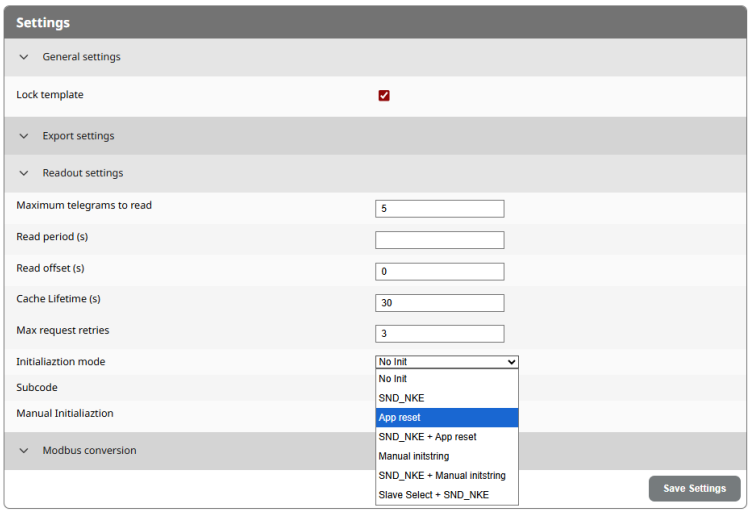
Secondary Address	Primary Address	Wireless Key	Active
FFFFFFFF.FFFF.FF.FF			1

    b. Set Include file to "No File".

13.1.15 Meter data-record structure mismatch

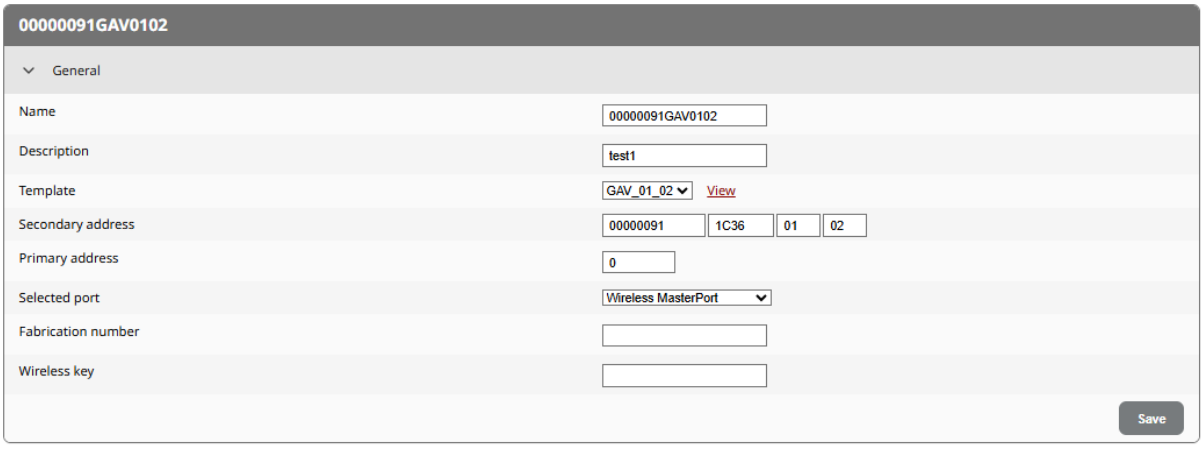
This error is likely to be caused by the wrong data being sent by the meter. It could be related to:

4. Telegram counter is not working properly in the meter
    a. The most common issue it that some meter requires the master to send an "Application reset".
    b. Go to "Template" and chose the template of the meter
    c. Under "Settings" change to "App reset"



d. Save Settings and go to the meter. On the meter, press "Read".

5. The meter alternates between datasets (multi-page / multi-frame responses)
    a. Go to the Mbushub and start the log
    b. Go to the meterlist, go to the affected meter and read the values, read multiple times and check for differences in the telegram structure.
        i. Check the amount of records in each telegram
        ii. Check for new error messages
    c. If there are differences in the data, check the settings for the meter whether it can be turned off.
    d. If the differences are below your data points of interest, verify your readouts and you can ignore the warning in the gateway if the values are correct.
    e. You can try toggling the different "Initialising" modes as seen above.
    f. You can try primary addressing to see whether it makes any difference (Use the Mbus Wizard for this)
6. If you like your templates to follow the variations:
    a. Go to templates
    b. Under "Settings", unmark the "Lock template" setting. This will allow the gateway to change template whenever a mismatch is occurring. Note that an template changes restarts all applications in the gateway.
7. There are multiple meters with the same ID.
    a. It can be the same wireless meter coming from different repeaters.
    b. If the meter has both a wireless frame and Wired frame, go to the meter settings and make sure you have the correct port chosen.



14 PiiGAB firewall configuration

Port	Adress	Traffic	Function
80	packages.piigab.com	Inwards/Outwards	Update and install the latest applications in the gateway
443	Piigab.microservicebus.com, piigab-iot.azure-devices.net	Outwards	Communications with PiiGAB Portal
51820	Ask PiiGAB for VPN relay	Outwards	VPN Connection via Wireguard
8883	Piigab.microservicebus.com	Outwards	Optional: Communication with PiiGAB Portal
8883	Preferred MQTT broker	Outwards	To send MQTT messages
21	Preferred FTP/ address	Outwards	QuickPost fileshare
22	Preferred SFTP server address	Outwards	QuickPost fileshare
443	HttpsPost	Outwards	QuickPost fileshare
80	httpPost	Outwards	QuickPost fileshare