LANSEN

Configuration Manual

Wireless M-BUS Gateway 5 LTE-M1 or CAT1/4G

Lansen Systems AB

Version 2.3, 2026-05-12

Table of Contents

Introduction

Welcome to the configuration manual for the Wireless M-Bus Gateway 5. This document is designed to serve as a comprehensive reference guide for installers, technicians, and technical professionals responsible for the operational setup of the device.

This manual provides the detailed, technical instructions required for configuring the Wireless M-Bus Gateway 5 using the *Lansen Configurator* software. It covers all aspects of device programming, including communication settings, timer management, and advanced features such as encryption and debugging.

Please note that instructions for the physical installation, mounting, and initial connection of the device are provided separately in the main User Manual.

This document applies to devices using firmware version **1024**.

Document conventions

This document uses the following formatting to highlight information.

Italics	Important concepts
Bold	Configuration parameters
[Text]	User interface buttons
`Monospace`	Verbatim data

The following admonitions are used throughout the document.

Note

Additional information that helps you use the product efficiently.

Important

You *must* follow this instruction to *complete a task* successfully.

Warning

You *must* follow this instruction to prevent *damage to equipment* or *injury to persons*.

About Wireless M-Bus Gateway 5

The Gateway 5 is a lightweight device designed to receive Wireless M-Bus (wM-Bus) data and forward it to an MQTT server over LTE-M1 or CAT-1/4G, depending on the model.

Key characteristics

- Received data is timestamped and sent to the MQTT service at specified intervals.
- Configuration is protected by a pre-programmed AES128 encryption key. To maintain full data integrity, the dataflow through the gateway is not decrypted.
- Packets are sent with QoS level 0; TCP/IP handles transmission and acknowledgment automatically.
- Configuration is done through the wM-Bus interface, the MQTT interface, or a USB-C cable.
- Models are available for mains power or battery operation.
- Firmware upgrades can be done in-field via MQTT or wM-Bus interfaces.

Intended use

The Lansen Wireless M-Bus Gateway 5 is a wireless infrastructure device designed for collecting and forwarding utility meter data.

- *Data Reception:* The gateway receives and timestamps Wireless M-Bus (wM-Bus) data packets from nearby meters and sensors.
- *Data Forwarding:* It forwards the collected data to an external Message Queueing Telemetry Transport (MQTT) server using cellular communication (LTE-M1 or CAT-1/4G). This enables remote data analysis and integration.
- *Connectivity Bridge:* The gateway acts as the essential link between a local wireless metering network and a wide-area network or cloud service.

In summary, the gateway functions as a *data bridge*, ensuring secure, reliable, and standardized transmission of wM-Bus information to a centralized data platform.

Do not use this product in critical applications where failure could result in risk to life or property.

Product overview

The Gateway 5 is available in several different hardware configurations. Find the version you have by looking at the model number on the product label.

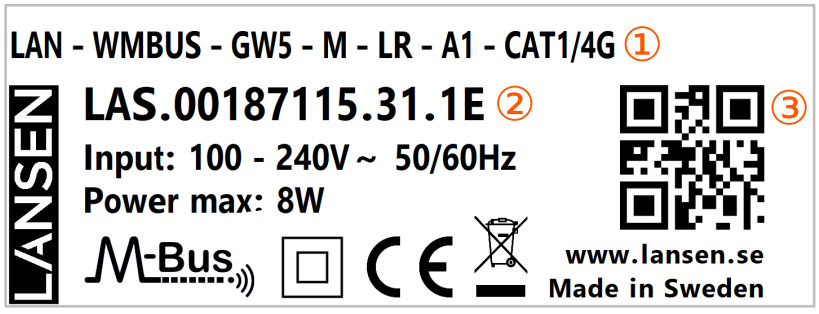


Figure 1. Product label for model LAN-WMBUS-GW5-M-LR-A1-CAT1/4G

① Model number

② Serial number

③ QR-code

The structure of the model number is seen below.

Table 1. Gateway 5 wM-Bus versions

Manufacturer	Input	Series	Power option	Receiver type	IP rating	Antenna (wM-Bus)	Cellular interface	Antenna (cellular)
LAN	**LAN-WMBUS**	**GW5**	**M**	**(blank)**	**A1**	**X**	**CAT1/4G**	**X**
Lansen	wM-Bus		Mains		IP40	SMA connector for external antenna	LTE CAT 1 modem	SMA connector for external antenna
LAN	**LAN-WMBUS**	**GW5**	**BE**	**LR**	**A2**	**(blank)**	**CATM1**	**(blank)**
Lansen	wM-Bus	Gateway gen. 5	Battery & supercap	Extra receiver sensitivity	IP65 & IP67	Internal antenna	LTE CAT M1 modem	Internal antenna

For example, *LAN-WMBUS-GW5-M-LR-A1-CAT1/4G* is a *Lansen Gateway 5 wM-Bus* model. It is a *mains-operated device* that includes a *high-sensitivity wM-Bus radio*, an *IP40 rating*, and uses built-in antennas for wM-Bus and cellular connection. It has a CAT1/4G modem. Available hardware configurations can be found at www.lansen.io.

Physical features

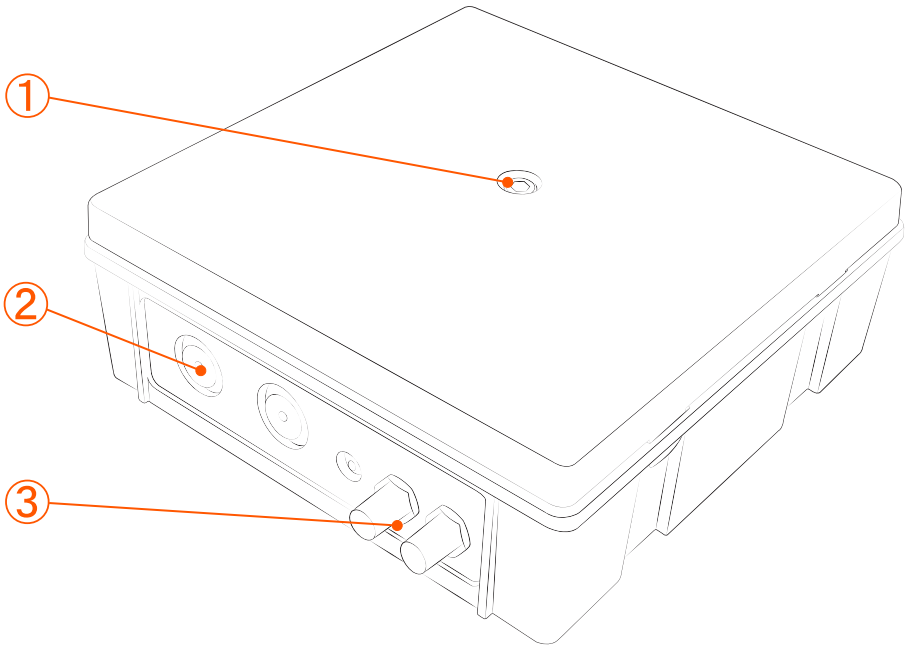


Figure 2. External overview

Gateway 5 can have the following physical interfaces accessible by the user, depending on the hardware configuration:

① **Center screw**

Holds the *top cover* in place. Remove to release the top cover.

② **Cable inlet**

Optional inlet for mains cable on *mains-operated* models.

③ **Antenna connectors**

Optional *SMA connectors* for up to two external antennas used for wM-Bus or cellular communication.

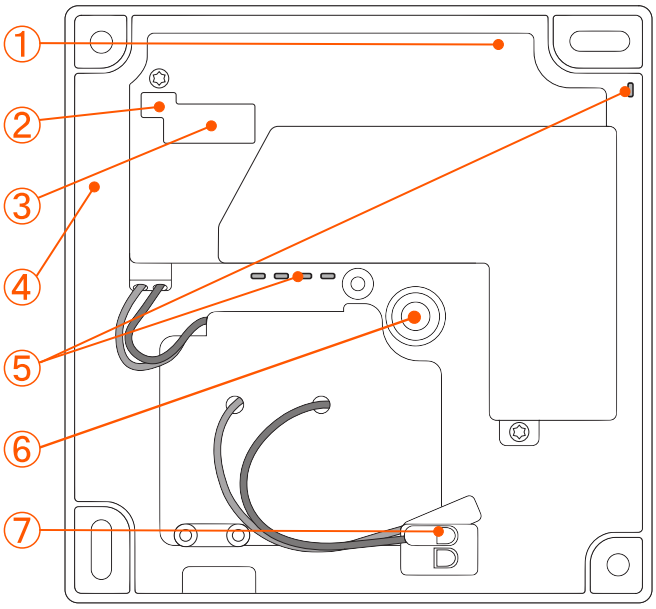


Figure 3. Internal overview

① **SIM card holder**

For data SIM cards. Located under the *PCB cover*.

② **USB-C connector**

Located on the *main PCB*. Remove the top cover to access this connector. Use this connector for configuration.

③ **Battery connector**

For battery-operated versions.

④ **Extension card connector**

For an optional extension card.

⑤ **Status LEDs**

Provides visual confirmation about the current status of the Gateway 5.

⑥ **Cable inlet**

For mains-operated versions. Optional inlet for mains cable.

⑦ **Mains connector**

For mains-power. Available on mains-operated product versions only.

Network interfaces

The Wireless M-Bus Gateway 5 can have the following network interfaces depending on the hardware configuration:

wM-Bus

Used for both configuration of the device and collection of meter data.

CAT-M1

A low-power cellular connection used for communication with the internet.

CAT-1

A medium-power cellular connection used for communication with the internet.

Ethernet

Wired connection for communication with the internet.

Accessories

- LAN-WMBUS-D2-TC configuration dongle
- Lansen Configurator software
- Pole mounting kit
- Magnet with telescopic shaft
- Sealing kit for A2 enclosure
- Antennas and antenna cables

General knowledge

Waking the Gateway 5

To configure a *battery-operated* Gateway 5, it must be in a listening state. To activate it, hold a magnet against the housing on the left side of the serial number label. When the device detects the magnet, it starts beeping and a red LED flashes once per second (only visible with the top cover removed). This indicates that the *reed timer* has started.

If the device is *mains-operated*, you can disregard this procedure, as these devices are configured by default to always be in a listening state and to forward packets.

When the reed timer has started, the Gateway 5 will stay in listen mode and repeat incoming data until the timer expires. You can configure the duration of this mode in the section Timers tab.

For the first 60 seconds after you activate the Gateway 5 with a magnet, it will only listen and respond to configuration data. This can be useful in environments with high traffic, where it can be difficult to establish contact with the Gateway 5.

If the **Automatic meter installation** parameter is enabled, the *internal routing list* is cleared when you apply the magnet.

Start-up sequence

When the Gateway 5 receives power, it performs a start-up sequence before entering standard operation.

1. **Power-On** All four status LEDs turn on. The device beeps.
2. **Memory clear** If *automatic meter installation* is set to 'true', the device clears the *flash memory*. The process takes approximately 2 minutes. When the memory is cleared, the device beeps and the *IP-COM LED* turns off.
3. **Dongle listen period (4 min)** The *wM-Bus LED* starts flashing. The device listens for incoming data from the *dongle* for 4 minutes. The device continues to send *status packets* every minute.
4. **IP connection period** The *IP-COM LED* begins to blink. The device attempts to connect to an MQTT server.

By default, the device only listens for devices in the *Internal routing list*, which is empty at first start.

1. **Standard operation** After a successful MQTT connection, the device enters standard operation according to its configuration.

Indications of the Gateway 5

The Gateway 5 uses both visual and sound indications to show its current status, such as the progress of the *startup sequence* or any errors encountered after startup.

Visual Indications

The Gateway 5 has five status LEDs. Four are located near the central screw post. A single cellular network status LED is located in one of the corners. See Figure 3.

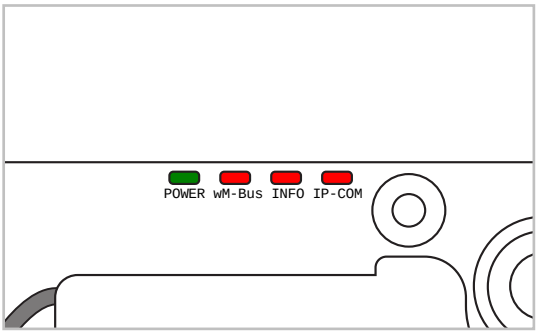


Figure 4. The central LED-strip with four status LEDs.

LED Strip			
POWER		Steady on	The Gateway 5 has power.
POWER INFO wM-Bus IP-COM		All steady on	Startup sequence active.
POWER INFO wM-Bus IP-COM		All blinking	APN incorrect, unable to access network.
INFO		Steady on	wM-Bus radio on/listen for radio packets.
wM-Bus		Quick flash	New packet received by the wM-Bus radio.
IP-COM		Steady on Blinking	Active connection to the MQTT server. Modem active but not connected to the MQTT server.

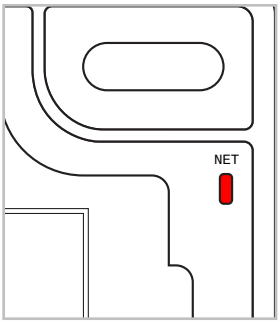


Figure 5. The net status LED.

Cellular network LED		
	Flash every 300 ms (0.3 s)	The Gateway 5 is sending data.
	Steady on/Off	Not registered to a network, rebooting, attempting to connect to a network.
	Flash every 300 ms (0.3 s) in intervals.	Connected to a network.

For battery version the LED indication will be turned off after 30 min to save power. The indication will be active again for 30 min if waking the Gateway 5 using a magnet.

Audio Indications

The Gateway 5 is equipped with a buzzer to give aural indication of its current status.

Device Status	Indication	Buzzer
Start-up sequence initiated	One long beep	
Start-up complete	One long beep	
Wake-up with magnet	Three beeps	
wM-Bus status packet after wake-up	One beep	
Certificate download complete	Three slow beeps	

SIM card and PIN

The Gateway 5 supports nano SIM cards and eSIM. If eSIM is required then the SIM must be mounted during production, thus must be ordered in advance.

The SIM card must not have any PIN code, thus the PIN must be inactivated.

For improved security, the SIM card should be locked to the specific modem using the network provider webservice or similar. There is usually also an option to lock the SIM card to the first device it is powered up in.

Lansen Configurator

Lansen Configurator is a Windows application from Lansen that lets you configure infrastructure devices from Lansen through a Graphical User Interface (GUI). You can download the software from http://www.lansen.io/download.

Installing Lansen Configurator

1. Download the latest version of Lansen Configurator from http://www.lansen.io/download.
2. Extract the downloaded zip-file to a folder on the computer.
3. Double click on the executable file called LansenConfigurator.exe
   The start-up screen will open.

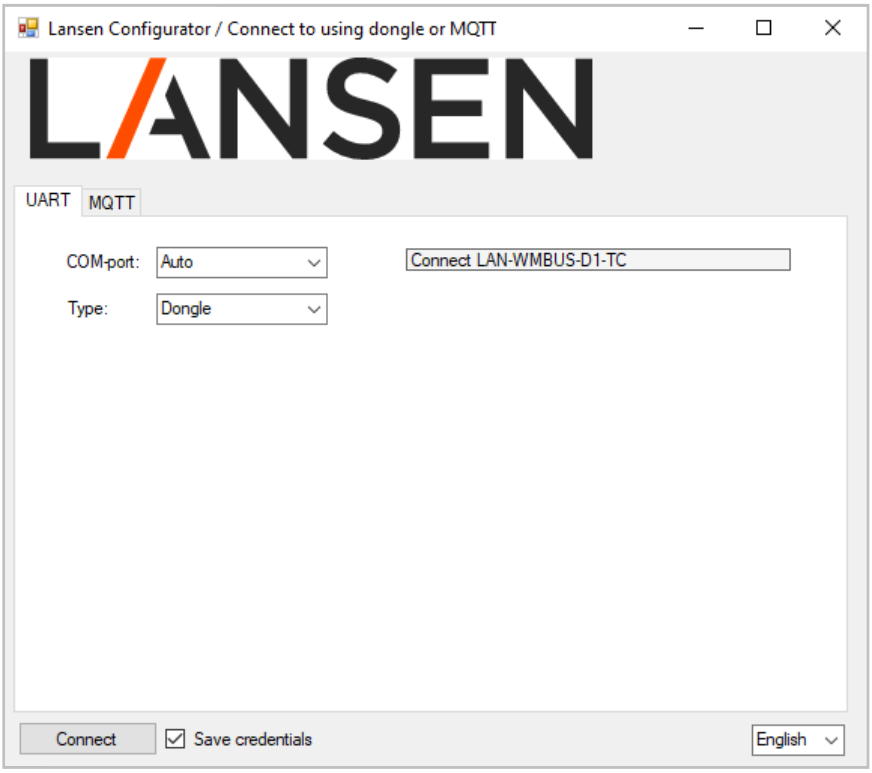


Figure 6. The Lansen Configurator start-up screen. Here you can select connection type, COM-port and language.

Configuration methods

You can configure the Gateway 5 with the Lansen Configurator software the following ways:

- Using a USB-C cable inserted into the Gateway 5.
- Through wM-Bus (using a USB dongle).
- Through an MQTT server.

Configuration is done in two steps:

1. Connect the Lansen Configurator program to your chosen configuration interface.
2. Log in to the Gateway 5.

Configuring the Gateway 5 with a USB-C cable

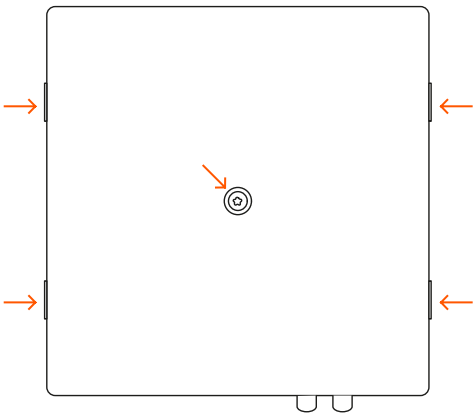
Use a USB-C cable for the most reliable connection to the Gateway 5. This method is ideal for initial setup, troubleshooting, or for environments where wireless communication is not possible. A direct wired connection ensures that you can always configure the device, regardless of its wireless communication status.

When you use a USB-C cable, the cable supplies power to the Gateway 5. The cable overrides the battery power supply.

Using Lansen configurator with a USB-C cable

Required equipment: *Screwdriver* with *security Torx T20H*, USB-A to USB-C cable.

1. Open the housing of the Gateway 5



   a. Unscrew the *center screw* using the *Torx T20H* screwdriver.

   b. Push the clips on both sides of the cover to remove it.

2. Connect a USB-C cable to the USB-C connector. See Figure 3.
3. Connect the USB cable to your computer.
4. Select **Wired Connection** in the **Type** dropdown menu.

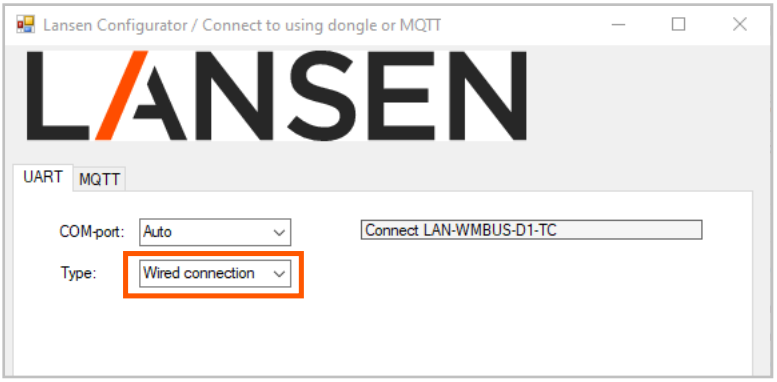


Figure 7. Start-up window with **Wired connection** *selected*

5. Click **[Connect]**.

1. If the program cannot connect to the Gateway 5, manually select the COM-port. Change the field from **Auto** to the COM-port of the cable.
2. Make sure the startup sequence is finished before you click **[Connect]**.

6. Proceed to Connecting to the Gateway 5 to finish the configuration.

Configuring the Gateway 5 using wM-Bus

Use the wM-Bus interface to configure the Gateway 5 in the field without connecting a cable. To make changes, you must be within the wM-Bus reception range. Recommended range is 1-10m.

Connecting Lansen Configurator to the USB-dongle

1. Insert the Lansen USB-dongle (**LAN-WMBUS-D2-TC**) into a USB-port of your computer.
2. Select **Dongle** in the **Type** drop-down menu

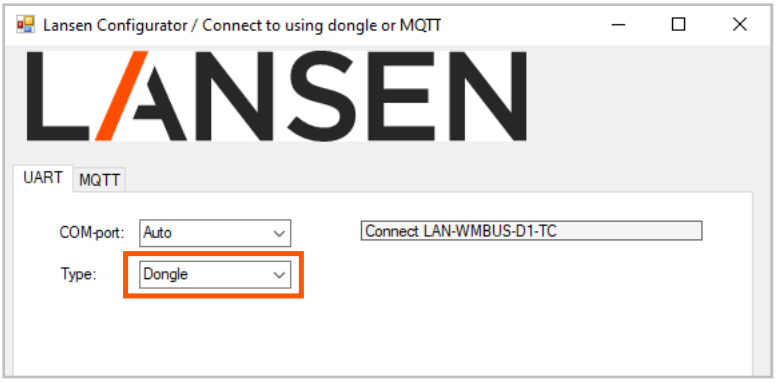


Figure 8. Start-up screen with **Dongle** *selected.*

3. Click **[Connect]**.

   The main screen appears when the connection to the dongle is successful.

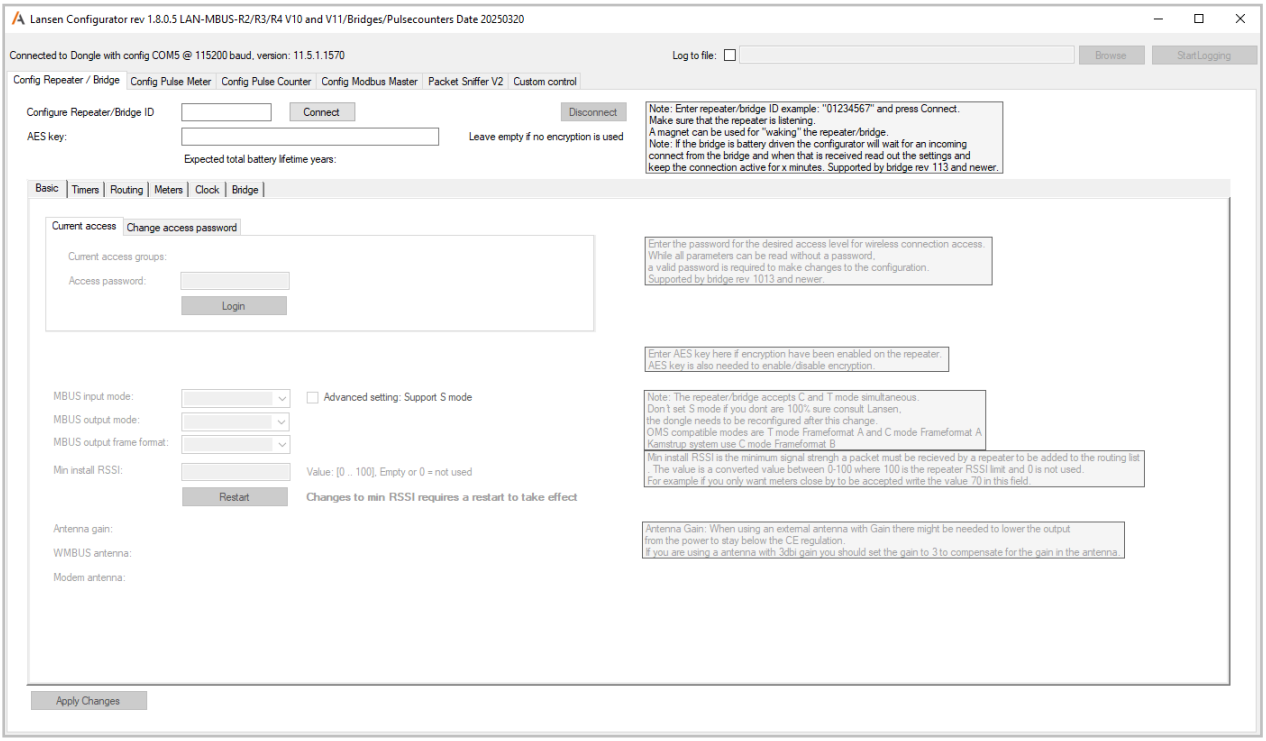


Figure 9. Main screen of Lansen Configurator

4. Proceed to Connecting to the Gateway 5.

If the program fails to connect to the dongle:

1. Manually select the COM-port by changing the field from **Auto** to the correct COM-port.
2. Identify the correct COM-port by comparing the list of available COM-ports before and after inserting the dongle. The correct COM-port is only visible when the dongle is inserted.
3. (Optional) If the program still fails to connect, your computer might be missing the correct driver. Visit http://www.lansen.io/download to download the appropriate driver for your dongle.

Configuring the Gateway 5 using MQTT

Use an MQTT connection to make changes to the configuration of the Gateway 5 remotely over an internet connection.

To configure the Gateway 5 over MQTT, it must be set up to communicate with the MQTT server that you will use for configuration. If the device has not been configured for you at the factory you must perform the initial setup using wM-Bus or USB-C. Please see Configuring the Gateway 5 using wM-Bus and Configuring the Gateway 5 with a USB-C cable

Connecting Lansen Configurator to an MQTT server

To configure the Gateway 5 through an MQTT server, you must connect the Lansen configurator to the server. This requires all MQTT settings to be correct.

1. Start the Lansen Configurator.
2. Select the tab MQTT and enter the settings to your MQTT server.

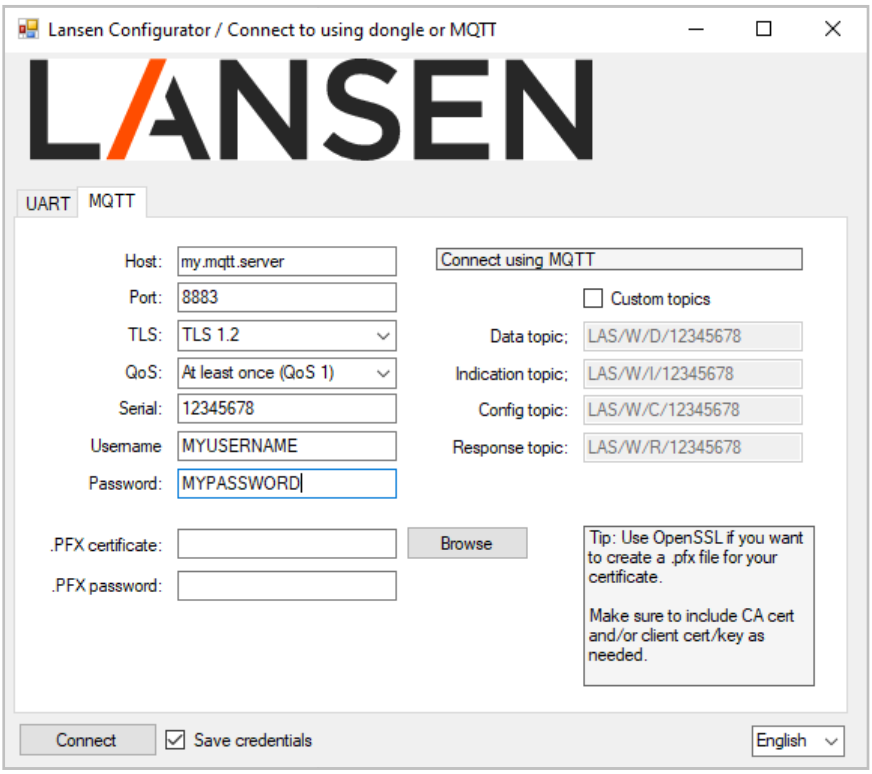


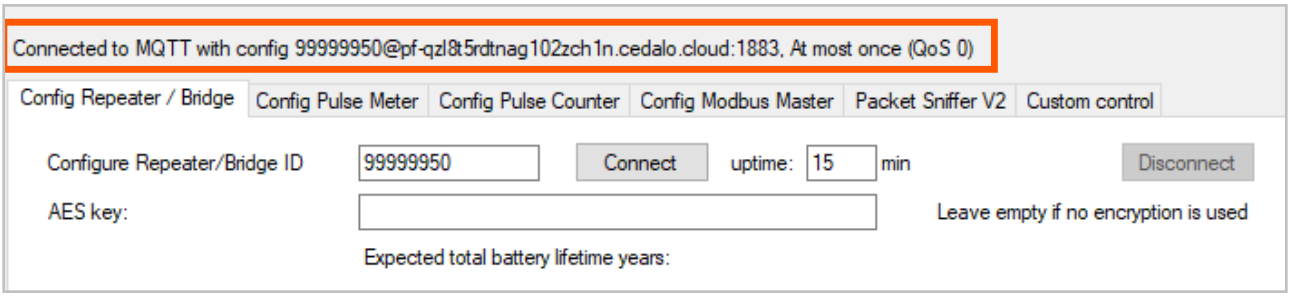
Figure 10. Example MQTT settings

Host: The MQTT server address, for example, my.mqtt.server.
Port: The port number for the MQTT server. Port 1883 is typical for non-encrypted connections.
TLS: Select this option to use TLS for the connection between Lansen Configurator and the MQTT server.
QoS: Quality of Service. Normally set to 'At least once (QoS 1)'. The value might need to be changed,

depending on your MQTT server.
Serial: The serial number of the Gateway 5, for example, 01234567.
Username: The username to connect to the MQTT server.
Password: The password to connect to the MQTT server.
.PFX certificate: To connect to the Gateway 5 using certificates create and upload a PFX file to gain full access.
.PFX password: Enter the password for the PFX file here.

3. Click **[Connect]** to initiate the connection.

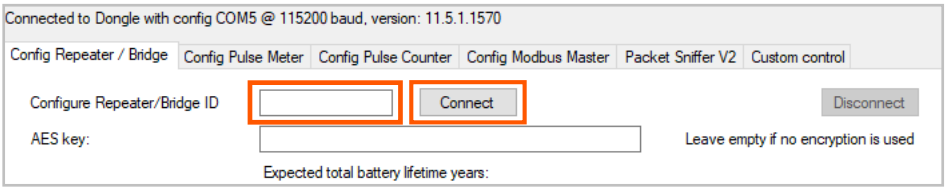
   The main screen opens with information about the active MQTT connection.



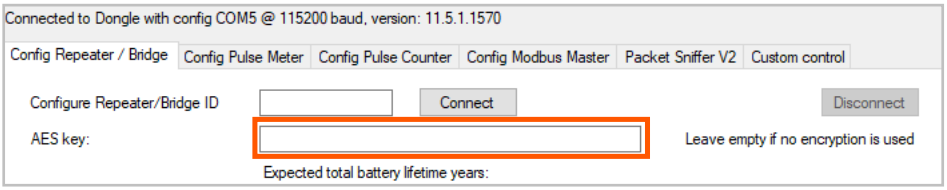
4. Proceed to Connecting to the Gateway 5.

Connecting to the Gateway 5

1. Go to the **Config Repeater / Bridge** tab.
2. Enter the eight-digit serial number of the Gateway 5. You can find the number on the label on the PCB cover or the front of the housing. If you are connecting from MQTT, the serial number is filled in for you.



3. (Optional) If you connect with a dongle, enter the AES key. The AES key is found on lansenonline.com.



You can read all device settings without the AES key. The program then shows only the first letter of each MQTT setting.

4. Click **[Connect]**. The connection takes 20 to 60 s.

   After the program connects, you can change all settings and parameters.

1. If the program cannot connect, touch a magnet to the left of the front label of the Gateway 5 to make sure it is not in sleep mode.
2. Make sure the Gateway 5 and the dongle are at least one meter apart.
3. Click **[Connect]**.

Troubleshooting tools

The *Lansen Configurator* includes several tools for *troubleshooting* and advanced configuration: a *packet sniffer*, a *debug log*, and a *custom control interface*. The *sniffer* monitors *Wireless M-Bus* packets. The *debug log* monitors internal *AT commands* used by the Gateway 5. The **Custom control** tab allows users to send custom *ENAPI commands* to the device.

The debug log is available when you connect with a USB-C cable.

Monitor routed messages with the Packet Sniffer V2

Lansen Configurator includes the **Packet Sniffer V2** tab. Use this tool to monitor all packets sent by meters and repeaters. The sniffer behavior depends on the connection method:

USB-dongle Monitor packets that the dongle detects.

MQTT server Monitor packets that the Gateway 5 transmits over the MQTT interface.

USB-C cable Monitor packets that the Gateway 5 detects.

The sniffer is independent of the internal routing list. All detected packets will be shown.

The **Packet Sniffer V2** tab contains two lists: a *Primary list* (left side) and a *Secondary list* (right side). The Primary list shows information about the packets that the sniffer detects. The Secondary list contains tabs that change the information shown in the Primary list.

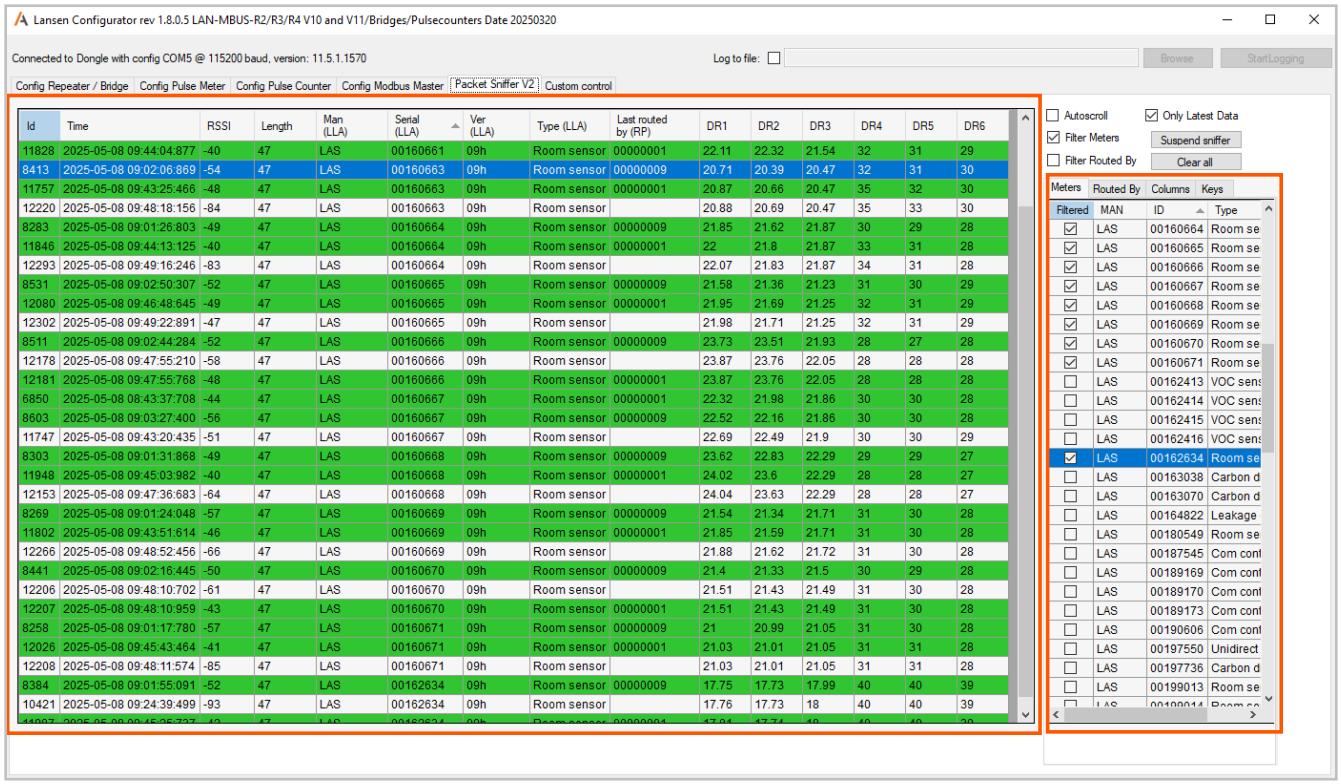


Figure 11. Packet Sniffer V2 with the Primary and Secondary lists highlighted.

Primary list

The Primary list displays all packets received so far. The format of the packets and their information depends on the options selected in the *Sniffer options* and the columns tab under the Secondary list.

Color coding

Each row is color-coded to provide additional information about the received packet. The reception quality depends on the **RP: RSSI**-column, indicating the signal strength between a repeater and a meter.

You can sort the rows in this list by clicking on the header of the column you wish to sort. For example, clicking on **Serial** sorts all meters and repeaters by serial number, from low to high.

Table 2. Meanings of each row color in the sniffer. The reception is measured between repeater and meter.

Color meaning	Color
Good reception between meter and repeater	
Okay reception between meter and repeater	
Medium reception between meter and repeater	
Bad reception between meter and repeater	
Really bad reception between meter and repeater	
Meter packet picked up directly by USB-dongle	
Status packet sent by a repeater (not meter data)	

Secondary list

This list complements the *Sniffer options* and controls what is displayed in the Primary list. There are four tabs in this list: **Meters**, **Routed By**, **Columns** and **Keys**.

Meters

This tab contains four columns. For each new meter received, the sniffer creates a new row containing the manufacturer code, serial number, and meter type.

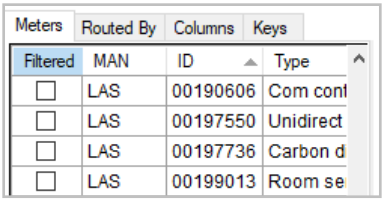


Figure 12. The **Meters** *tab*

Filtered

With the **Filter Meters** option enabled, select the checkboxes of the meters to be displayed in the primary list. This feature is useful when focusing on specific meters in areas with many devices.

MAN

View the manufacturer code for each meter. Click **MAN** to sort the list alphabetically by manufacturer code.

ID

View the serial number for each meter. Click **ID** once to sort from lowest to highest serial number. Click twice to sort from highest to lowest.

Type

View the type of each meter. Click **Type** to sort the list alphabetically by meter type.

Sniffer options

Use the options in the upper right corner to control which packets appear in the *Primary list*.

Autoscroll

Select this option to keep the *Primary list* scrolled to the newest packet. Clear this option to review earlier

packets without the list moving automatically.

Filter Meters

Select this option to show only packets from the meters you select in the **Meters** tab in the *Secondary list*. Use this option to focus on one or more specific meters in areas with many devices.

To apply this filter, select the checkboxes next to the meters in the *Secondary list*.

This option filters based on the serial numbers shown in the **Serial** column of the *Primary list*.

Filter Routed By

Select this option to show only packets routed by the repeaters you select in the **Routed by** tab in the *Secondary list*.

This option filters based on the serial number shown in the **Last Routed By** column of the *Primary list*.

Only Latest Data

Select this option to show only the latest packet for each meter and repeater. Clear this option to show all packets received.

Clear All

Select this option to remove all packets from the *Primary list*.

Routed By

This tab shows a checkbox and a serial number for each repeater the sniffer detects. When the sniffer receives data from a repeater for the first time, the tab adds a new checkbox with that repeater's serial number.

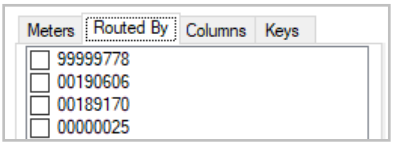


Figure 13. The **Routed by** *tab*

Use this tab together with the **Filter Routed By** option. When the filter is active, the *Primary list* shows only the packets that the selected repeaters transmit or retransmit.

Columns

Use this tab to select which columns appear in the Primary list. Each available option is shown in Table 3. For more information about the DR1-31 alternatives, refer to the WMBUS data format guide for your product on www.lansen.io.

Table 3. Description of the available columns in the primary list.

Column name	Meaning
Id	ID number of the received packet. Each time a new packet is received, the ID is incremented by 1.
Time	The timestamp when the computer received the packet.
RSSI	The signal strength of the packet that the repeater or meter sent and the USB dongle received. The value ranges from 0 (strong signal) to larger negative values (weaker signal).
MBUS mode	The MBus mode (S, C, or T-mode) in which the device sent this packet.
Frame format	The Frame Format (A- or B-format) in which the device sent this packet.
Freq Error (kHz)	The approximate deviation from the center frequency (868.95 MHz) of the repeater or meter when it sent this packet.

Column name	Meaning
Length	The number of bytes in the received data packet.
Man (LLA)	The manufacturer ID of the device (repeater or meter) that first sent the packet.
Serial (LLA)	The serial number of the device (repeater or meter) that first sent the packet.
Version (LLA)	The version of the device (repeater or meter) that first sent the packet.
Type (LLA)	The type of device (repeater or meter) that first sent the packet.
NWK	Shows if this packet uses a short header (0x7A) or a long header (0x72) in the CI-field. Note: If a long header is used, you can find more information in the ALA columns.
Enc. Mode	Shows if this packet is encrypted (0x05) or not (0x00).
Status	The status byte (also called Status Field) of the *original transmitter* of this packet.
Acc	The access number of the *original transmitter* of this packet.
Man (ALA)	The manufacturer ID of the device to which the meter data of this packet belongs. Note: Only appears if the packet was sent with a long header in the CI-field.
Serial (ALA)	The serial number of the device to which the meter data of this packet belongs. Note: Only appears if the packet was sent with a long header in the CI-field.
Ver (ALA)	The version of the device to which the meter data of this packet belongs. Note: Only appears if the packet was sent with a long header in the CI-field.
Type (ALA)	The type of device to which the meter data of this packet belongs. Note: Only appears if the packet was sent with a long header in the CI-field.
RP: Last routed by	The serial number of the repeater that retransmitted the data most recently.
RP: Hops	The number of times repeaters have retransmitted the packet.
RP: RX state	Shows the current transmission state of the repeater. TRUE = Listening and FALSE = Pausing. Note: If you use a magnet to wake up the repeater, it can transmit data even if this column is FALSE.
RP: Time to change	The number of seconds left until the repeater changes its RX-state.
RP: Current time	The current time on the repeater.
RP: Start time	The time set for the **Start time** parameter if it is active.
RP: Listen days	The weekdays selected for the **Start time** parameter if it is active.
RP: Microrepeater	Shows if the repeater is a microrepeater (1) or a normal repeater (0).
RP: Mains connected	Shows if the repeater is mains-operated (1) or battery-operated (0).
RP: Listen active reason	The current reason for listening. See Table 4 for more details. Note that multiple reasons can be active at the same time.
RP: Relative RSSI	The signal strength of the packet sent by a repeater or meter and received by the repeater. The value ranges from 0 (strong signal) to larger negative values (weaker signal).
Raw packet	Shows all bytes in the received packet.

Table 4. Description of the different values in columns **RP: Listen active reason**.

Bit	Meaning
0 (0x01)	Listen timer running

Bit	Meaning
1 (0x02)	Short listen window (60 s) for parameter **Start time** is running
2 (0x04)	Long listen window (time set in parameter **Listen/pause timer**) and parameter **Start time** is running
3 (0x08)	Monthly listen timer running
4 (0x10)	NOT USED
5 (0x20)	Magnet/reed timer running

Keys

Use this column to view AES keys that has been added to the packet sniffer. The keys are used to decrypt the data records in the Primary list.

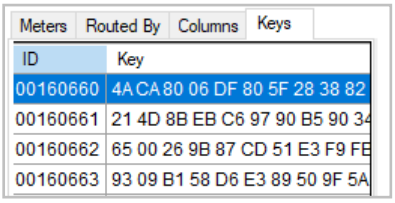


Figure 14. The seconday list with keys added

Adding AES keys to LansenConfigurator

Add AES keys to the packet sniffer to view the data records of encrypted packets. The keys need to be stored in a CSV file before they are added to the sniffer.

The format for the CSV file is:

```
Serialnumber;AESKey
00000001;XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

The AES key found is found on lansenonline.com.

To add keys:

- Under the Secondary list, click **[Load/add keys]** and select your CSV file.

To clear keys:

- Click **[Clear keys]** to remove ALL keys added to the sniffer.

This feature does not store any keys on the Gateway 5 or the dongle. You will need to upload them each time you connect to LansenConfigurator.

Logging data to File

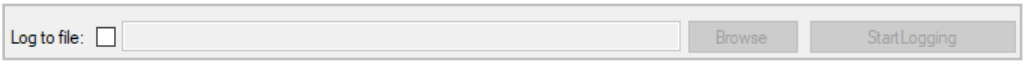


Figure 15. Select **Log to file** *to store the packet log to your computer.*

To log received packets to a file on your computer for further analysis in e.g. Excel:

1. Select the **Log to file** checkbox. This enables **[Browse]**.

2. Click **[Browse]**.
3. Navigate to the location on your computer where you want to save the file.
4. Enter a file name in the **File name** field.
5. Click **[Save]**. This enables **[Start logging]**.
6. Click **[Start logging]**. The program saves all packets shown in the primary list to the file.

Monitoring AT-commands with Extended debug

The *Extended debug* troubleshooting tool lets you monitor the low-level commands (*AT commands*) exchanged between the Gateway 5's processor and its cellular modem. Use this feature to diagnose cellular connection failures or confirm commands sent by the device.

Access this tab when you connect to the Gateway 5 with a USB-C cable. This tab is not accessible with other connection methods.

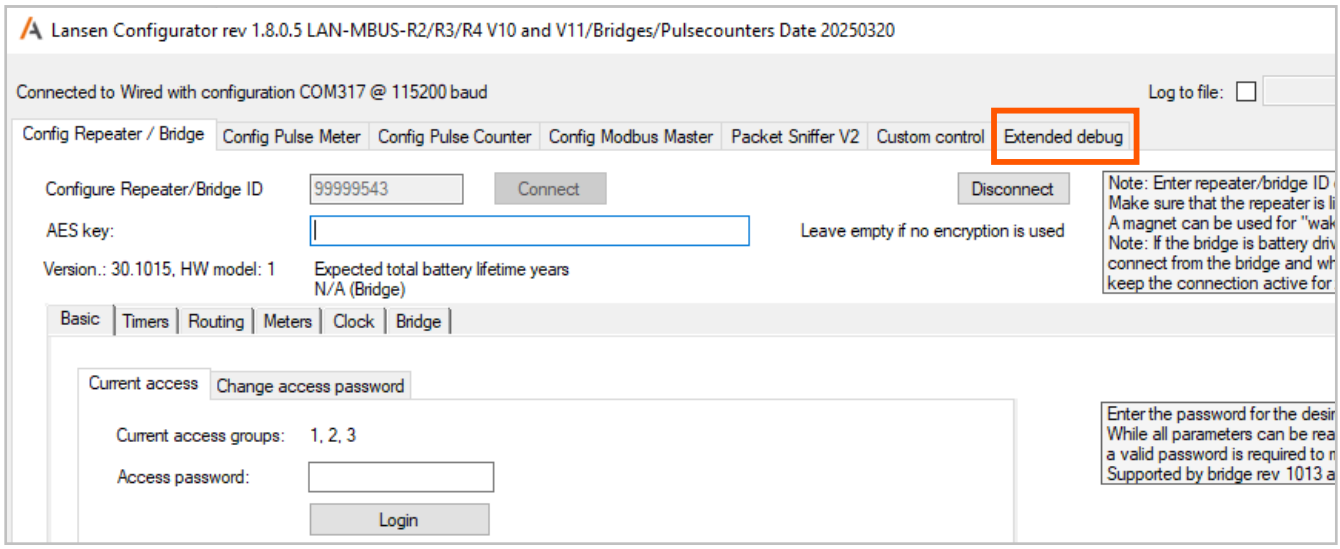
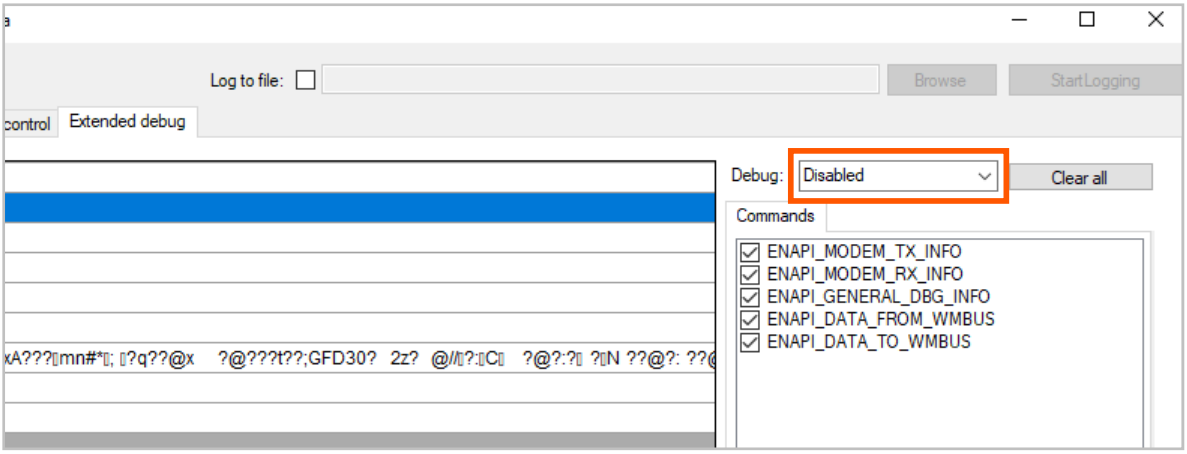


Figure 16. The **Extended debug** *tab.*

To start monitoring AT commands:

1. In the top right corner, select **Enabled** from the **Debug** drop-down menu.



   The extended debugger starts if MQTT is active on the Gateway 5.

2. When you are finished, select **Disabled** from the **Debug menu** to stop the debugger.

Configuring the Gateway 5

After you connect to the Gateway 5, you find device settings in these tabs: **Basic**, **Timers**, **Routing**, **Meters**, **Clock**, and **Bridge**.

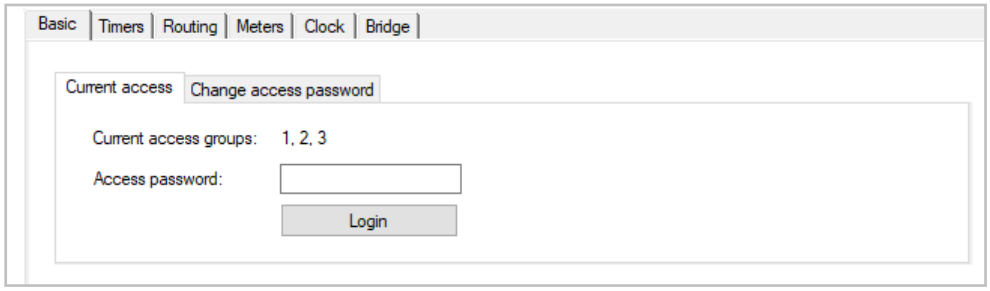


Figure 17. The settings are located under the tabs at the top

When you change a setting, its color changes from green to red. To apply the change, click **[Apply Changes]**. The Gateway 5 either accepts the new setting or keeps the original setting. The setting color returns to green after the Gateway 5 responds.

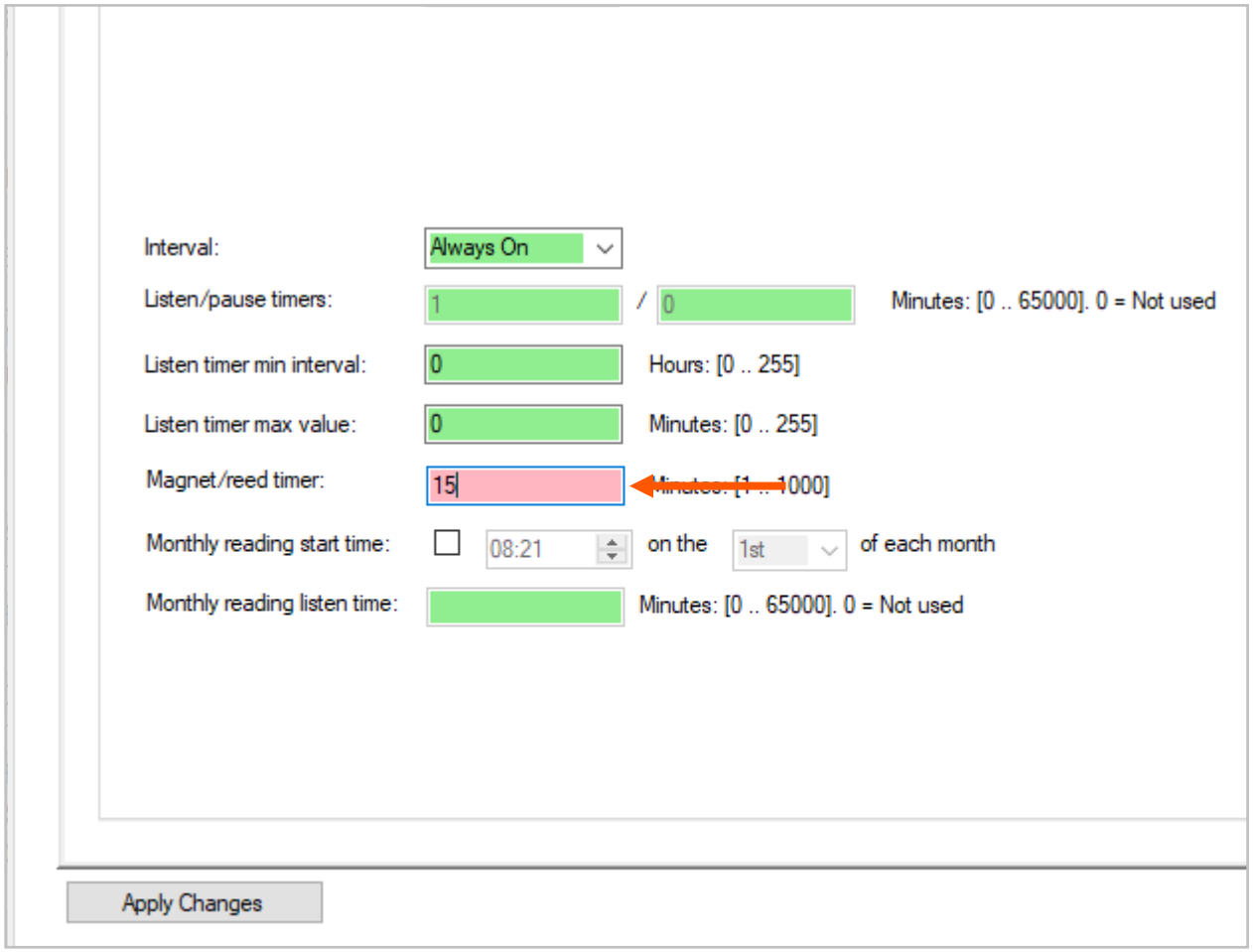


Figure 18. Changed settings have a red background

Access Passwords

To access the Gateway 5 through a dongle or USB-C, you must enter an eight-digit password. There are three customizable passwords. Each password gives you access to a different set of parameters. You can find the default passwords on lansenonline.com.

Access Groups

Access groups control which parameters you can change in LansenConfigurator. The groups are assigned to access passwords during device production. You cannot change them.

If you try to change a parameter that is not in your current access group, a pop-up message shows you the required access group.

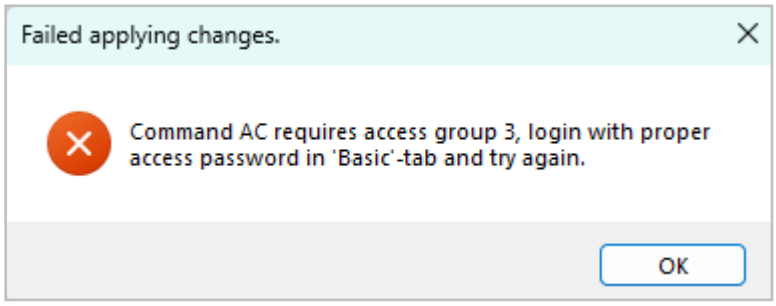


Figure 19. Error message showing the required access group.

Customized configurations for access groups are available upon request.

Entering an Access password

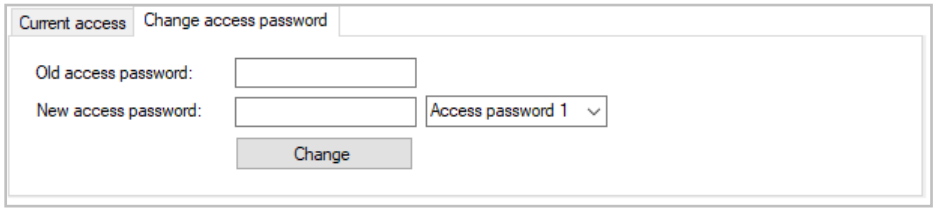
1. Enter the *Access password* in the password field under the tab **Current access**.

2. Press enter or click **[Login]**
   The access groups you have access to is visible under **Current access groups**.

> You will need to re-enter the password after 15 min of inactivity.

Changing Access password

The Access passwords 1-3 can be changed under the tab **Change access password**. The password must consist of eight digits.



1. Input the current password you wish to change under **Old access password**.
2. Input the new password under **New access password**.
3. Select the corresponding password in the dropdown menu.
4. Press enter or Click **[Change]**.

Settings in the Gateway 5

This chapter explains all available settings in detail.

Basic tab

This tab contains the basic parameters of the Gateway 5, such as **Encryption**, **MBUS mode**, **Min install RSSI** and more.

Encryption

Use this parameter to select the encryption options for the Gateway 5. The Gateway 5 uses encryption for configuration by default. This encryption does not apply to incoming data packets from sensors or meters. All data packets are forwarded without modification. The end devices encrypt the packets separately, if you enable it.

The AES key is not needed when you configure the Gateway 5 through MQTT.

The encryption dropdown menu has four options. To change from one option to another, you must enter the correct AES key in the **AES key** field.

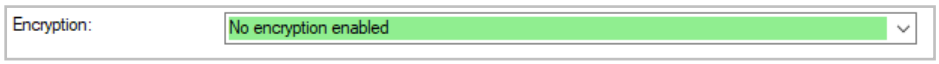


Figure 20. The encryption drop-down menu. Select encryption options by clicking the down-arrow on the right.

Table 5. Encryption options

Option	Meaning
No encryption enabled	All encryption is disabled. You do not need enter a key in the field **AES key** to change parameters for the Gateway 5. All settings are sent over the air in plain text and may be eavesdropped. Only use this options if you have other means to protect the communication.
Enabled for configuration	Encryption is enabled (default) The field **AES key** must contain the correct key for the GW to apply any parameter changes.
Enabled: OMS time sync	Enables the OMS time sync. Needs to be enabled if time synchronization should only be allowed if the time synchronization packet is encrypted. This packet is sent from the Gateway 5 using the OMS time synchronization format.
Enabled: OMS time sync and configuration	Combines the two options above, i.e., **Enabled for configuration** and **Enabled: OMS time sync**.

MBUS mode

These settings are used to set the input and output communication format of the Gateway 5.

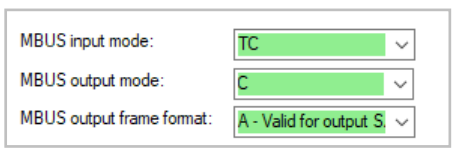


Figure 21. The various settings for the MBUS modes.

By default, the Gateway 5 always accepts incoming data in C- and T-mode. The output mode can be changed to S-, C-, or T-mode with frame format A or B. Recommended use is:

- Input = TC
- Output = C
- Frame format = A

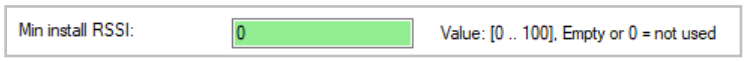
To set the Gateway 5 to listen for sensors in S-mode, follow these steps:

1. Enable **Advanced setting**.
2. Set the input mode to **S-mode**.

If you are using the LAN-WMBUS-D1/D2 dongle to configure the Gateway 5, complete all other configurations before setting it to S-mode. When in S-mode, you will not be able to configure the Gateway 5 until the USB-dongle has been configured to send in S-mode. Contact Lansen for more information on how to proceed.

Min install RSSI

Use this parameter to ensure the Gateway 5 only retransmits meters with good signal strength.

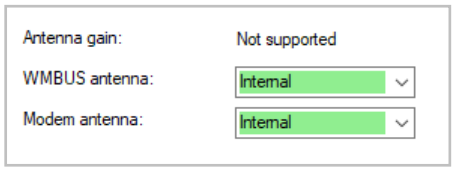


It sets the minimum RSSI required from a meter to be accepted into the *internal routing list*. Use this setting in environments with multiple gateways to ensure that only meters with a good connection are handled. This reduces the risk of data collisions due to fewer retransmissions.

After changing this parameter, the Gateway 5 must be restarted to update the internal routing list. To restart, disconnect and reconnect the power/battery, or click **[Restart]** in the Lansen Configurator under the **Basic** tab.

Antenna gain

Use these settings when the Gateway 5 is connected to an external antenna with gain.



Set the antenna gain parameter to the gain of the external antenna. The Gateway 5 then adjusts its output power to stay within legal transmission limits. This ensures correct operation when an external antenna is used.

This setting applies only to models with an external wM-Bus antenna. These models have an “-X” in the product name. You can find the product name on the device label.

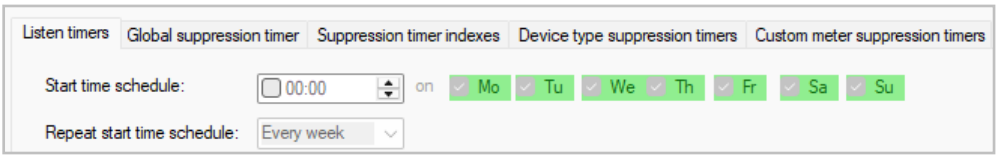
On battery-powered devices, use the lowest antenna gain that still gives a reliable connection to conserve battery life.

WMBUS antenna and modem antenna parameters

Use these parameters to select whether the Gateway 5 should use the internal or an external antenna for WMBUS and cellular communication respectively.

Timers tab

This tab contains parameters for the Gateway 5 which are timer-based, such as listen/pause timers and suppression timers. It is also possible to configure the Gateway 5 to wake up on specific days, weeks, or dates. E.g. Mondays or the 15th of every month.



Listen timers

Configure the wake-up schedule for the Gateway 5 by selecting monthly, weekly, daily, or specific dates. Additionally, you can adjust the magnet/reed timer to set the duration the Gateway 5 listens for data after a magnet has been applied to its reed switch.

Start time schedule

Use this setting to control when and how often the Gateway 5 listens on selected weekdays, weeks, or specific dates. This setting works together with the *Interval* and *Listen/pause timers* to define the wake-up pattern.

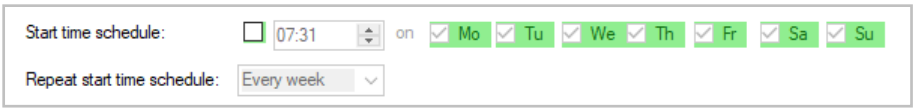


Figure 22. Start time scheduler

Start time schedule

Select this checkbox to activate the **Start time** parameter. The Gateway 5 starts listening at the specified time, interval, and days.

Time field

Set the daily wake-up time in UTC. Make sure the time is equal to or less than the selected interval. The Gateway 5 listens for the duration defined in the **Listen/pause timers** parameter.

Active days

Select the days the Gateway 5 listens and clear the others. If **Repeat start time schedule** is set to **On certain dates**, select the dates the Gateway 5 should use. For example, to upload on the 1st and 15th of each month on weekdays only, select **1** and **15** and select **Mo** to **Fr**. If the 1st falls on a weekend, the upload moves to the next selected weekday.

Repeat start time schedule

Select the weekly interval for wake-ups or select **On certain dates**. This parameter defines how often the Gateway 5 starts its listening cycle.

Interval

Select how often the Gateway 5 listens, starting from the time in the **Time field**. Select a predefined interval or select **Custom** to specify exact wake-up times. This parameter links directly to the **Listen/pause timers** parameter.

Listen/pause timers

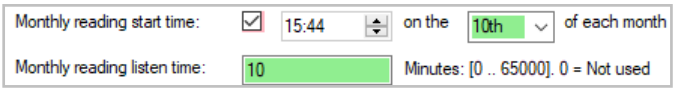
Set the listen and pause durations in minutes. For example, 30/1410 results in 30 minutes of listening within a 24-hour period. In this example, the **Interval** is 24 hours.

Magnet/Reed timer

Set how long the Gateway 5 listens for wM-Bus and configuration packets when activated with a magnet on the left side of the front label.

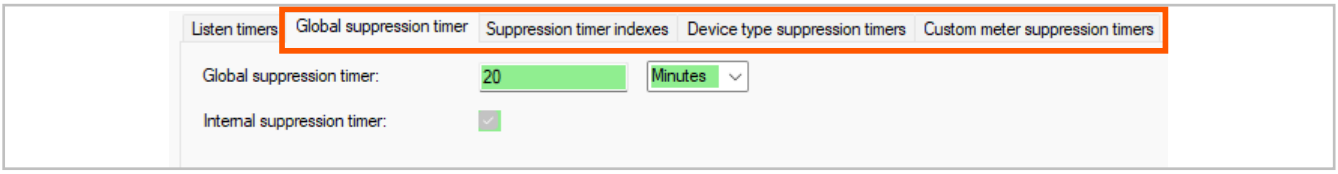
Monthly reading start time

This setting is a separate timer which is used to wake the Gateway 5 at a specific date and time once a month and is useful in systems where meter data is also needed at a specific date and time every month.



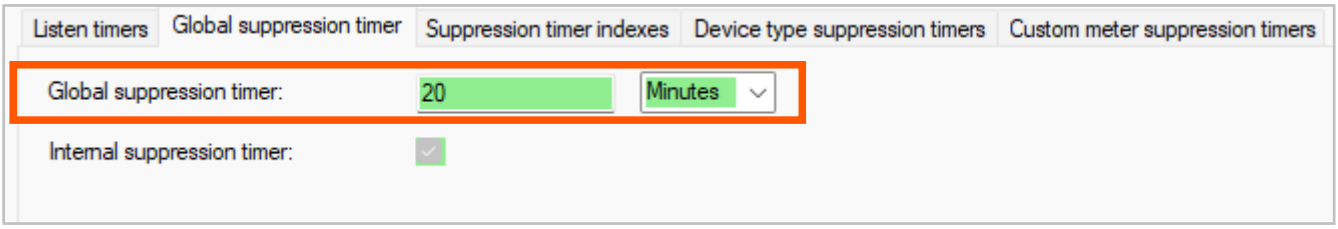
Suppression timer

This setting is used to reduce how often packets from each meter is stored by the Gateway 5 and the time can be set in either minutes or hours. It is a highly configurable parameter with several tabs to allow you freedom to configure each sensor/meter or repeater picked up by the Gateway 5.



Global suppression timer

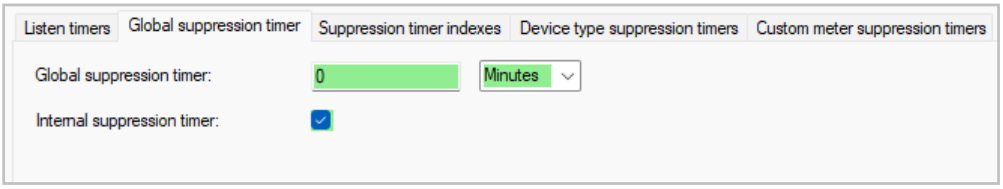
The **Global suppression timer** is the default setting for the Gateway 5 unless you specify otherwise. This means the Gateway 5 sends only the latest meter data every 20 min, even if the meters send data, for example, every 2 min.



Internal suppression timer

You can only activate or deactivate the **Internal suppression timer** if the global suppression timer is set to 0. When activated, the internal suppression timer applies a 10-second delay, even if the global suppression timer is set to 0.

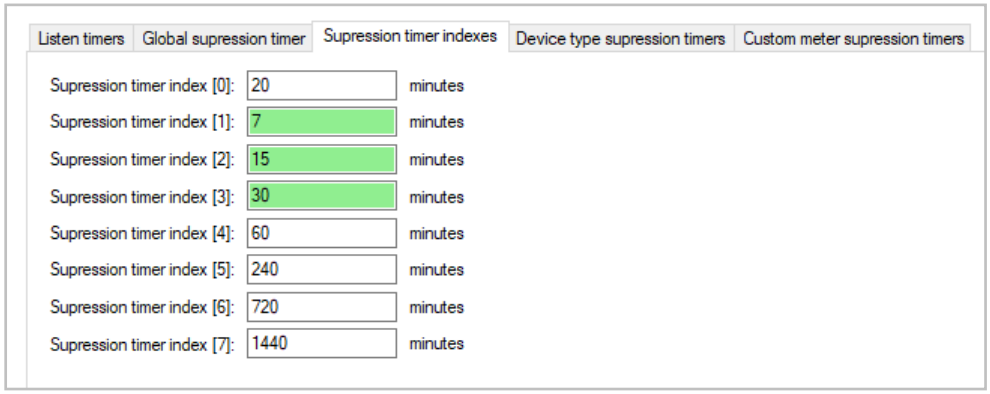
To disable all suppression timers entirely, turn off the internal suppression timer and set the global suppression timer to 0.



Suppression timer indexes

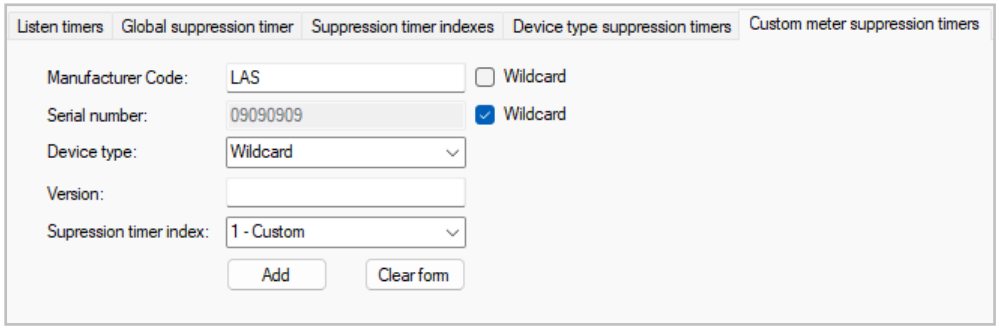
This tab allows you to view and create create your own preconfigured indexes of suppression timers that you can apply for your meters or sensors. **Suppression timer index [0]** is the **Global suppression timer** (default), indexes

1-3 are configurable, and indexes 4-7 are predefined.



Device type suppression timers

This tab allows you to set specific device types to follow an index. E.g., if the Gateway 5 is picking up Room Sensors, you can configure it to always handle those devices with a specific suppression timer index compared to another type of device.

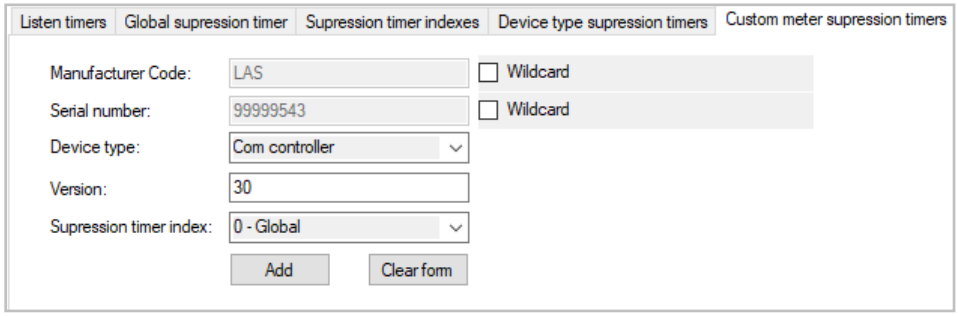


Custom meter suppression timers

This tab allows you to set and view suppression timers for specific meters or sensors individually. You can set specific suppression timers for each device linked to the Gateway 5 by using the manufacturing code, serial number, device type, and version.

You can use *wildcards* for flexibility. For example, if you set a wildcard for the manufacturing code, all meters with the same serial number, device type, and version will use the specified timer, regardless of the manufacturer code.

To unlock the **Manufacturer code** or **serial number** parameter, toggle the **Wildcard** checkbox on and off.



Routing tab

The Routing tab lets you filter by manufacturer ID or set whether to route only OMS messages or all messages that the Gateway 5 detects.

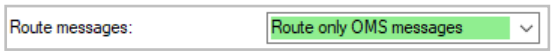
Accept Manufacturer ID

Use this parameter to enable *manufacturer code filtering*. This feature ensures the Gateway 5 stores packets only from meters with a specific manufacturer code. This is useful in areas containing meters from different companies. If all fields are empty, the Gateway 5 stores packets from all meters.

Route messages

Use this parameter to control the type of wM-Bus packets the Gateway 5 receives and stores. This is critical for ensuring compliance to OMS or accepting data from non-compliant meters.

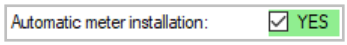
- Route only OMS messages: The Gateway 5 stores packets only from meters that are *OMS-compatible*.
- Route all messages: The Gateway 5 stores both *OMS-compatible* and *non-OMS-compatible* packets.



Meters tab

The settings and options in this tab concerns the *internal routing list* of the Gateway 5. In this tab, meters can be viewed, added, and removed.

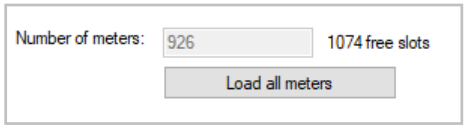
Automatic meter installation



If you select the **Automatic meter installation** checkbox, the Gateway 5 automatically adds received meters to its internal routing list. The list stores a maximum of 2000 unique entries.

If this setting is disabled and no meters are stored in the *internal routing list*, the Gateway 5 will not store any meters. In this case, you must add meters manually. See Add meter(s) manually to internal routing list.

Number of meters

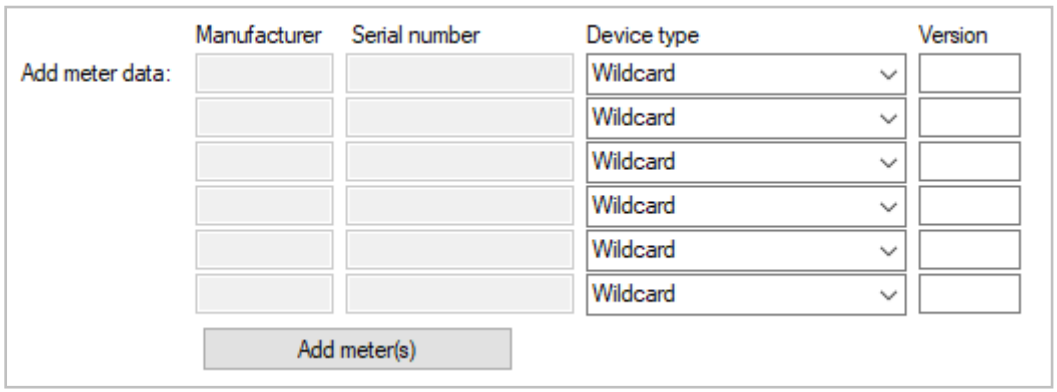


This field shows how many meters are in the internal routing list. On the right side, you can see the number of free slots left.

To view all meters in the routing list, click **[Load all meters]**. The list on the right side of the program will be filled.

Add meter(s) manually to internal routing list

To have full control of which meters are stored you can manually add meters to the *internal routing list*. This procedure is known as whitelisting.



To add a meter:

1. Make sure the **Automatic meter installation** checkbox is cleared.
2. In the **Add meter data** fields, fill in the *manufacturer ID*, *serial number*, *device type* and *version*. See Table 6 for a list of wM-Bus device types.
3. Click **[Add meter(s)]**.

   If the operation is successful, a pop-up is displayed.

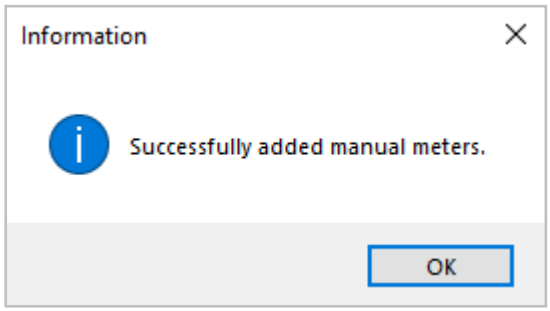


Table 6. Device type by hex

Type	Hex	Type	Hex
OTHER	0	AD_CONVERTER	19
OIL	1	SMOKE_DETECTOR	1A
ELECTRICITY	2	ROOM_SENSOR	1B
GAS	3	GAS_DETECTOR	1C
HEAT_OUTLET	4	DOOR_WINDOW	1D
STEAM	5	LEAKAGE_DETECTOR	1E
WARM_WATER	6	OCCUPANCY	1F
WATER	7	BREAKER	20
HCA	8	VALVE	21
COMPRESSED_AIR	9	CUSTOMER_UNIT	25
COOLING_OUTLET	A	WASTE_WATER	28
COOLING_INLET	B	WASTE	29
HEAT_INLET	C	CARBON_DIOXIDE	2A
SYSTEM_COMPONENT	D	VOC_SENSOR	2B
UNKNOWN_MEDIUM	E	COM_CONTROLLER	31
CALORIFIC	14	U_REPEATER	32

Type	Hex	Type	Hex
HOT_WATER	15	BI_REPEATER	33
COLD_WATER	16	RADIO_CONVERTER_SYSTEM	36
DUAL_WATER	17	RADIO_CONVERTER_METER	37
PRESSURE	18		

Add meter(s) from file to internal routing list

Instead of adding a meter one by one, you can import a CSV-file with multiple meters.

1. Make sure **Automatic meter installation** is *disabled*.
2. Click **[Browse]**
3. Select the CSV-file with the meters to be added.
4. Click **[Import CSV-file]** to start uploading the meters in the file.

The CSV-file *MUST* start the first row with the text:
`ManufacturerCode;IdentificationNumber;DeviceType;Version`
Otherwise, the file will not be uploaded.

Delete meter(s)

Delete a meter if it should not be retransmitted.

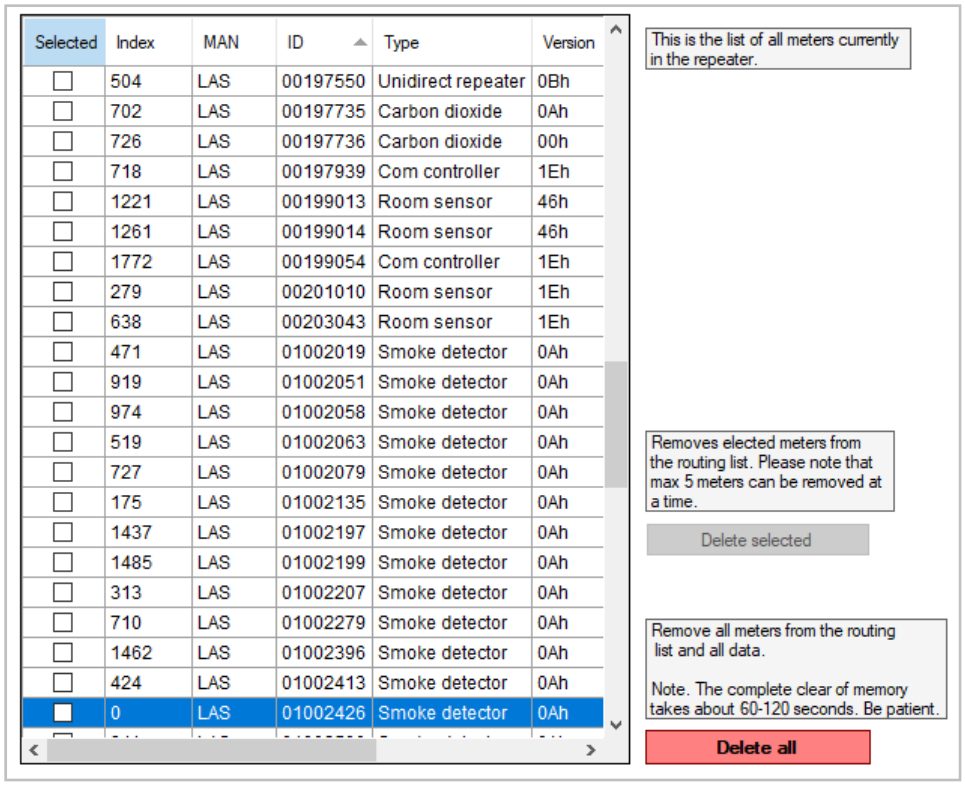


Figure 23. The internal routing list.

To remove *selected meters* from the internal routing list:

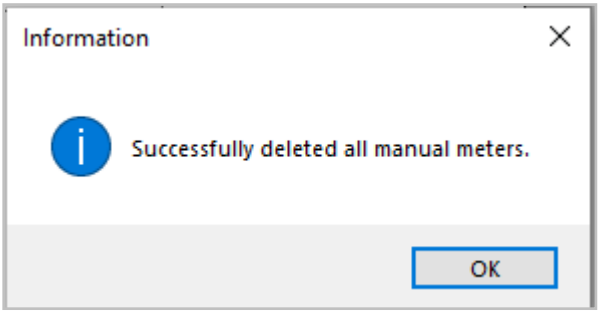
1. Make sure **Automatic meter installation** is *disabled*.
2. Click **[Load all meters]** to see this list of meters.
3. Select the meters you want to delete.
4. Click **[Delete selected]**.

To remove *all* meters:

1. Make sure **Automatic meter installation** is *enabled*.
2. Click **[Delete all]**.

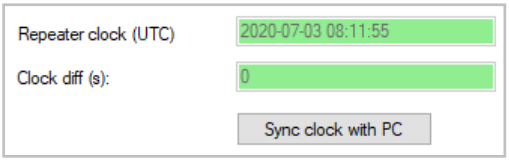
> The deletion process will take about 2 min.

If the operation is successful, a pop-up is displayed.



Clock tab

This tab shows information about the internal clock of the Gateway 5.



The upper field, **Repeater clock (UTC)**, displays the internal clock of the Gateway 5 as UTC-time while the lower field, **Clock diff (s)**, shows how many seconds the internal clock of the Gateway 5 differs from the current clock on the PC.

The Gateway 5 keeps synchronization using the configured NTP server so synchronization with PC is normally not needed.

To synchronize the Gateway 5 clock to the PC, click **[Sync clock with PC]**.

> The time synchronization is performed each time the Gateway 5 connects to the internet or every 12 h.
> The Wireless M-Bus Gateway 5 has a highly accurate onboard temperature compensated clock for minimum drift and the expected drift is less than 0.5 s/day.

Bridge Tab

This tab contains settings for the internet connection and communication.

Choose between MQTT, FTP or HTTP protocols for the internet communication and set the server addresses. Changes to the connection protocols take effect after device restart. Changes to the server address take effect the next time the Gateway 5 connects to the internet. Restart the Gateway 5 to apply settings immediately.

To restart, click **[Restart]** in the **Basic** tab.

When you connect using the LAN-WMBUS-D1/D2-TC dongle and do not enter an AES key, the program only retrieves the first letter of the MQTT settings.

When you change settings on a Gateway 5 in a remote location, make sure that all settings are valid. If the settings are incorrect, you will not be able to configure the Gateway 5 again through the internet interface.

Make sure that the four critical settings (**host**, **username**, **password**, and **port**) are set correctly. The program sends all four settings in the same configuration packet. If you only change one parameter, the three other parameters are still updated to the current value in the GUI.

Communication settings

These settings are only applicable for the LTE-M1 and CAT1/4G gateway.

Host

Enter the address for the remote server.

Port

Enter the port for the remote server.

Default ports are:

MQTT	1883
MQTT+TLS	8883
FTP	21

HTTP	80
HTTPS (HTTP+TLS)	443

Transport type

Select the protocol used for the internet connection. Available options are *MQTT*, *FTP* and *HTTP*.

Enable HTTPS by selecting one of the TLS options in the **Internet security** drop-down menu and setting the port to 443.

FTP and HTTP transport types are only available when network interface type is Modem. See Network Interface Policy.

Template

Select the template used for structuring the data uploaded over FTP and HTTP.

Template 101	Use Format 1 when operating in a SensusRF-based environment. This format follows the CSV-structure used by SensusRF equipment.
Template 201	Use Format 2 when operating in an Elvaco-based environment. This format follows the CSV-structure used by Elvaco meters and systems.
Template 301	Use Format 3 when operating in an Diehl-based environment. This format follows the XML-structure used by Diehl meters and systems.

See Appendix A for details on the template formats.

Username

Enter the password used for remote server authentication.

Password

Enter the password used for remote server authentication.

Directory (FTP only)

Specify the directory on the FTP server where data is stored. Only one directory level is supported.

Topic Prefix (MQTT only)

Enter the MQTT topic prefix.

Internet Security

- Enable TLS communication when using MQTT or HTTP.
- Server and client authentication requires preloaded certificates.
- **SNI** checkbox: Enable or disable Server Name Indication (SNI) when connecting to the MQTT broker.

APN

Enter a specific APN if required. For LTE, the Gateway 5 retrieves the APN from the network when this field is left empty.

If the APN is configured incorrectly, the Gateway 5 cannot establish a mobile data connection. The Gateway 5 performs four connection attempts. If all attempts fail, the gateway enters a mandatory one-hour backoff period before retrying. Rebooting the gateway does not clear or shorten the backoff period.

NTP

Enter a specific NTP server if required.

HTTP authentication

Enable HTTP authentication to use a username and password with the HTTP transport type.

Always online

Enable this parameter only for mains-powered units or for short-term testing with battery-powered units. Continuous online mode increases power consumption. The Gateway 5 automatically attempts to reconnect if the connection drops.

When **Always online** is disabled and FTP is selected as the transport protocol, the Gateway 5 uploads meter data to the FTP server in bulk. Multiple meter readings are combined into one file, up to a maximum size of 8 kB. If the combined data exceeds this limit, the Gateway 5 creates a new file. This reduces the number of files stored on the FTP server.

Modem version

View modem firmware version.

Network interface

View the active network interface. Modem or Ethernet.

Network interface policy

Select the fallback policy to use when the Gateway 5 is equipped with an Ethernet interface. If no Ethernet interface is installed the text *Not supported* is displayed.

Ethernet only	No fallback. Always use the Ethernet interface.
Ethernet Over Modem	Fallback to cellular connection if Ethernet connection is lost.
Modem only	No fallback. Always use the cellular interface.

Timers

Upload time schedule

This is the time that the modem connects to the remote server and uploads the stored data.

This is the time when the modem connects to the remote server and uploads the stored data. If **Always online** is enabled, this setting has no effect.

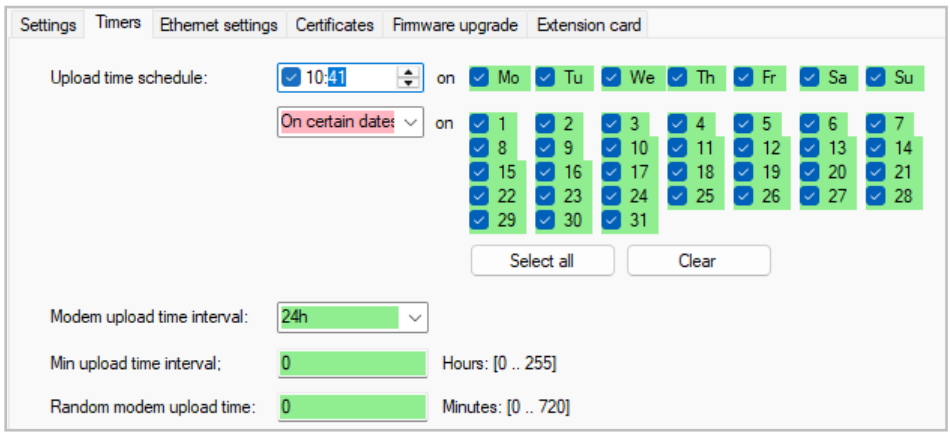
Do not set modem upload time to the same value as the **Listen/pause timer** under the Listen timers-tab.

For battery-powered Gateway 5, the recommended setup is to first listen for incoming wM-Bus data and then upload the collected data later the same day.

Example 1. Timer settings:

Listen start time = 05:20
Listen time: 30 min

Modem Upload time: 06:00



If **Repeat start time schedule** is set to **On certain dates**, select the dates on which uploads should occur. For example, to upload on the 1st and 15th of each month on weekdays only, select **1** and **15** and then select **Mo**, **Tu**, **We**, **Th**, **Fr**. If the 1st falls on a weekend and the next weekday is the 2nd, the upload takes place on the 2nd.

Certificates

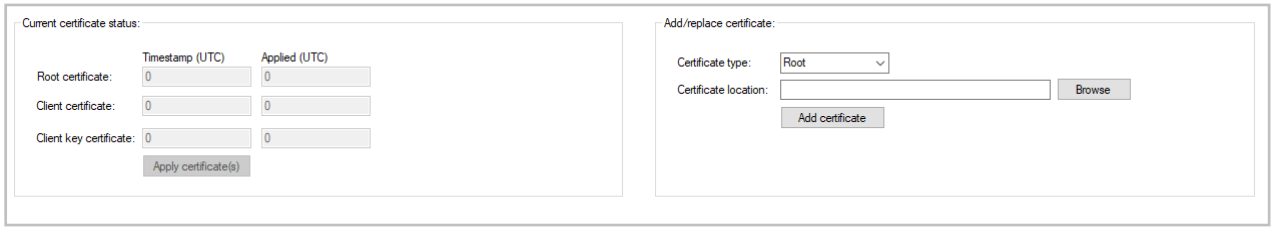


Figure 24. Overview of the Certificates tab

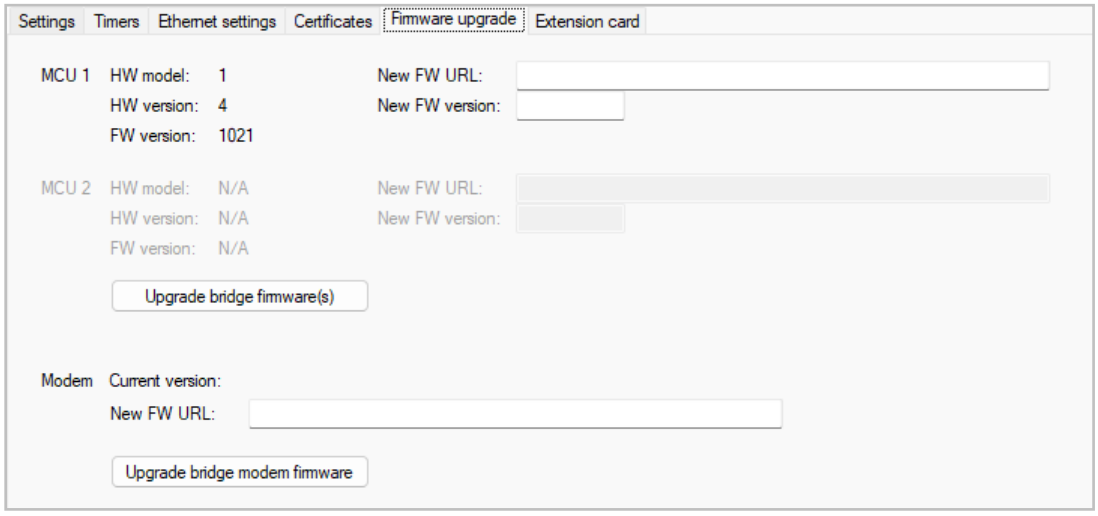
In the **Certificates** tab, you can upload certificates to the Gateway 5.

The dropdown menu on the right side lets you select three certificate types: **Root**, **Client Key**, and **Client**.

Upload the certificates one by one. After selecting each certificate, press **[Apply certificate(s)]** on the left-hand side to finish the upload.

Clicking **Apply Changes** instead of **Apply certificate(s)** will not upload the certificates.

Firmware upgrade



The firmware upgrade tab lets you manually update the firmware of the Gateway 5.

1. Enter a valid URL to the firmware in the **New FW URL** field
2. Enter the version number of the new firmware.
3. Click **[Upgrade bridge firmware(s)]** to start the upgrade.

Extension card

If an *extension card* is installed in the Gateway 5, the **Extension card** tab displays configuration options for the installed card. The device detects the card type automatically.

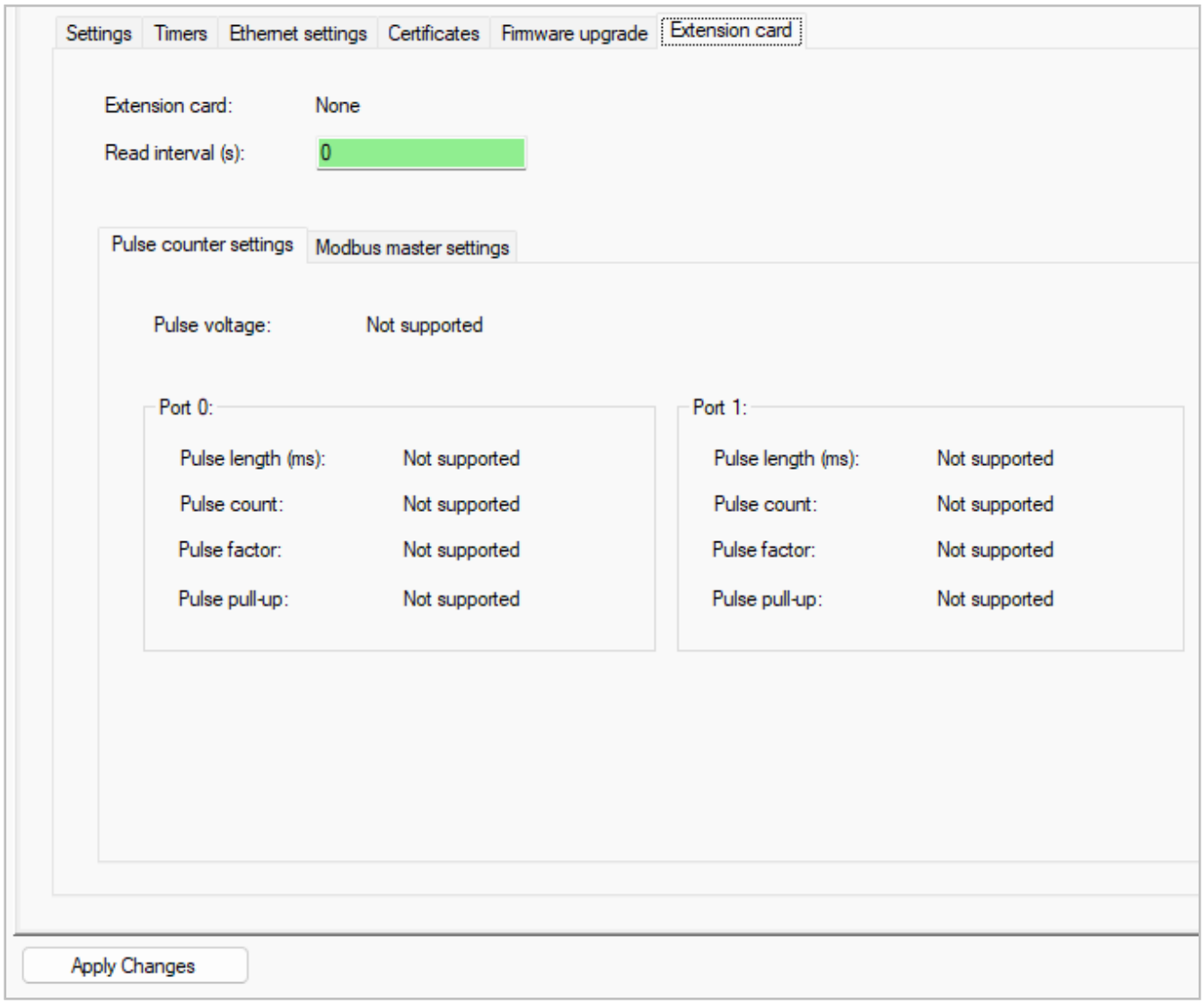


Figure 25. The **Extension card** *tab*

Extension card

Display the detected card type.

Settings are configurable only when a pulse card is installed.

Read interval (s)

Enter the polling interval for the installed pulse card.

Pulse counter settings

Configure parameters for the pulse card. Click **[Apply Changes]** to apply changed settings. The pulse card has

two ports: Port 0 and Port 1. Each port have the same configuration options.

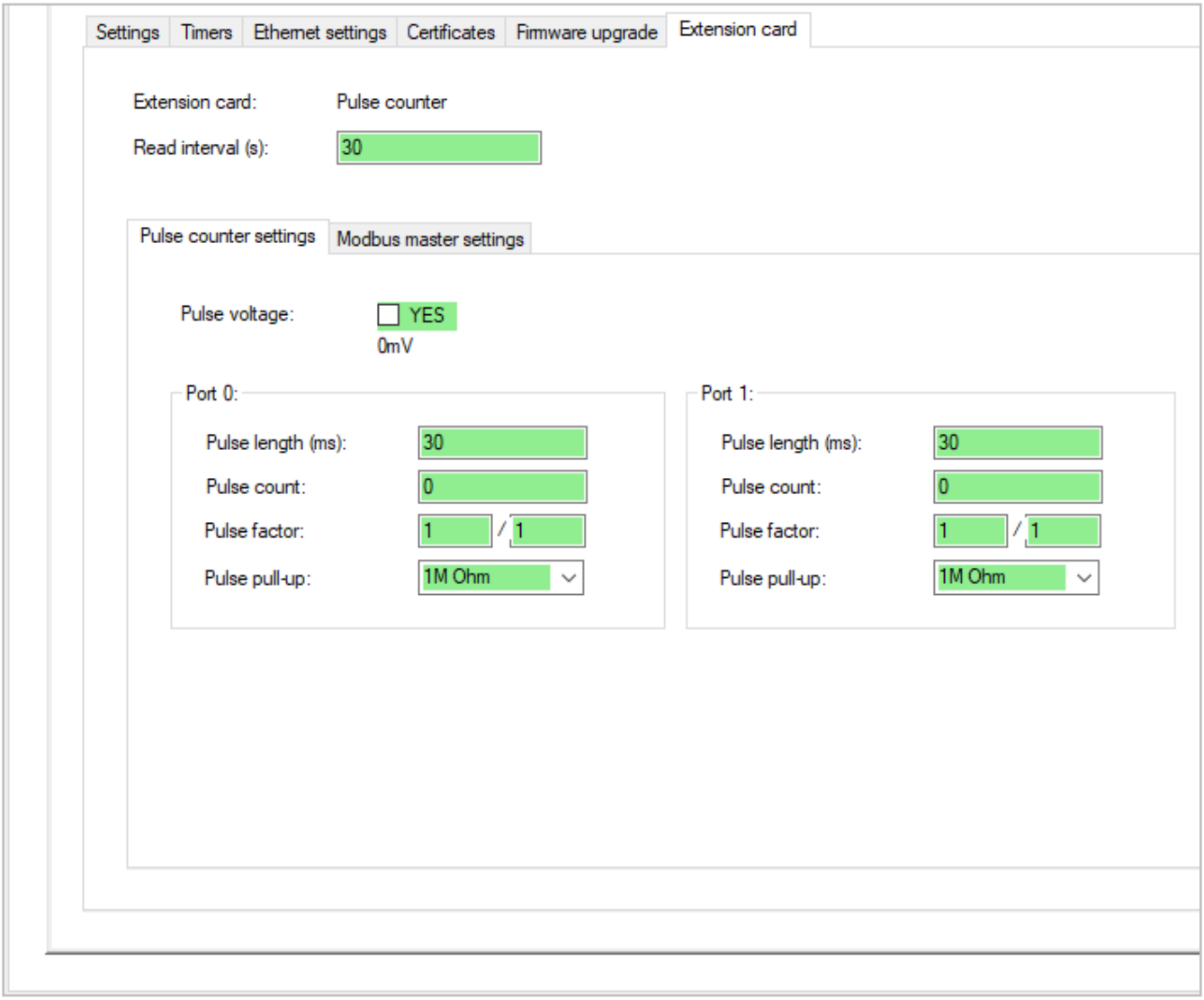


Figure 26. The pulse counter settings tab. The Pulse counter settings are only visible in a Pulse card in installed in the Gateway 5.

Pulse voltage

Select **YES** to display the voltage of the last received pulse.

Pulse length

Enter the minimum detectable pulse length.

Pulse count

View the number of detected pulses. Enter a value to offset the counter manually.

Pulse factor

Enter a numerator and denominator to scale the detected pulse count.

Pulse pull-up

Select the pull-up resistance for the pulse input: 10 MΩ or 56 kΩ.

Modbus master settings

The Modbus card can handle up to 64 modbus requests. Configure each request in the **Modbus request settings** table. Click **[Apply Changes]** to apply changed settings.

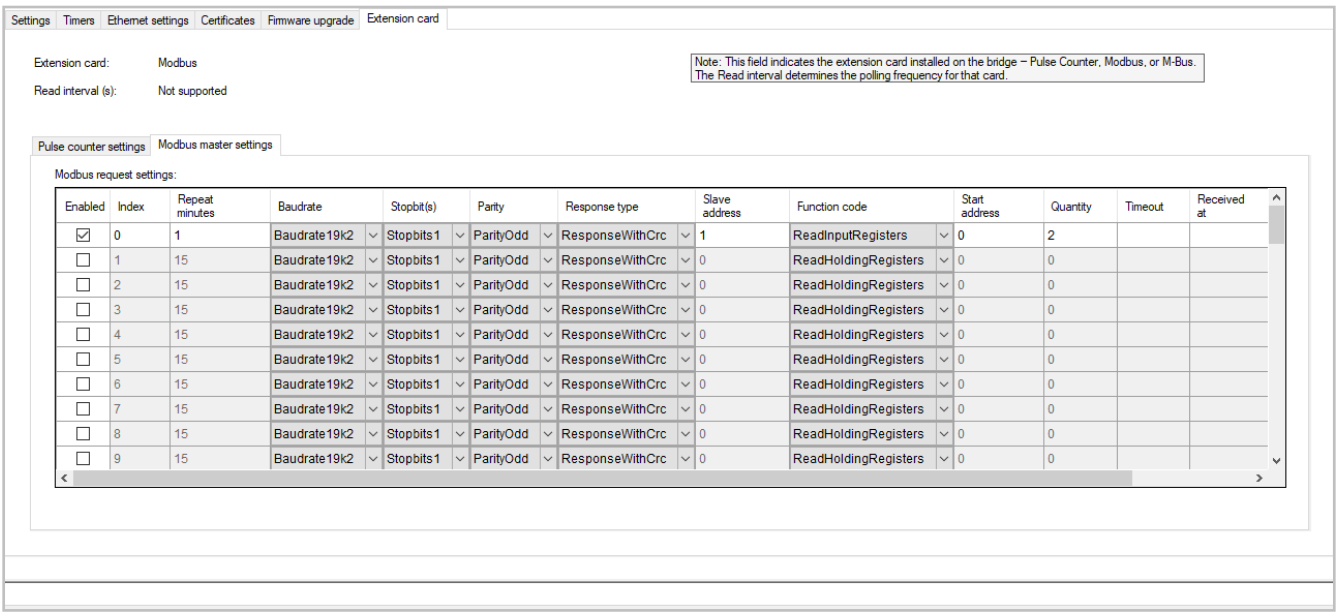


Figure 27. The Modbus master settings. The Modbus request settings are only visible if a Modbus card is installed in the Gateway 5.

Enabled

Select to activate the configured request.

Index

Display the request identifier.

Repeat minutes

Enter the number of minutes between repeated requests.

Baudrate

Select the baud rate used for the request.

Stopbit(s)

Select between 1 or 2 stop bits.

Parity

Select between none, even or odd parity.

Response type

Select the resonse type:

NoResponse

No MODBUS data response expected (TBI). No sanity check is done on the response or request packet.

ResponseWithCrc

MODBUS data response expected with CRC included in both the MODBUS packet request and response packet from the MODBUS master.

ResponseWithoutCrc

MODBUS data response expected without precalculated CRC included in the MODBUS data. CRC is instead generated in the MODBUS master and the CRC is NOT included in the response packet.

Slave address

Enter the slave address.

Function code

Select the function code to use:

ReadCoilStatus

Read the status of coils

ReadInputStatus

Read the status of inputs.

ReadHoldingRegisters

Read the value of holding registers.

ReadInputRegisters

Read the value of input registers.

Start address

Enter the address the request shall start with.

Quantity

Display the number of received reqests.

Timeout

Display a timeout notification if the request was not received.

Received at

Display the time the request was received.

Sending Configuration Packets to the Gateway 5

Configuration packets are always sent to the topic `LAS/W/C/12345678` where `12345678` is the serial number of the device to be configured. There are two types of M-Bus headers for configuration.

Option 1: M-BUS header for encrypted and non-encrypted configuration packets

Option 1 must be used if Gateway 5 has been set to only accept encrypted configuration packets. This is the default setting.

Use this header for for sending both *AES128 encrypted* and *non-encrypted* configuration data.

The serial number in bytes 12-15 must be the serial number of the device being configured (i.e., the same serial number found in the MQTT configuration header).

For best security, you should increment the access number (byte 20) by 1 for each packet sent to the device. However, configuration will still function even if you always use the same access number.

Example 2. M-Bus header - Encrypted and non-encrypted data

Data Link layer

Byte No.	Field Name	Content	Info	Byte data
1	L-Field	Length of data		0x43
2	C-Field	SND-UD2		0x43
3	M-Field	Meter Manufacturer Code	LAS	0x33
4	M-Field	Meter Manufacturer Code		0x68
5	A-Field	Serial number BCD (LSB)	**Example:** 0A0A0A0A	0x0A
6	A-Field	Serial number BCD		0x0A
7	A-Field	Serial number BCD		0x0A
8	A-Field	Serial number BCD (MSB)		0x0A
9	A-Field	Version	**Example:** 00	0x00
10	A-Field	Device type	**Example**: 00	0x00

Transport layer

Byte No.	Field Name	Content	Info	Byte data
11	CI-Field	Long network header		0x5B
12	Ident Nr.	Gateway serial number BCD (LSB)	**Example:** 12345678	0x78
13	Ident Nr.	Gateway serial number BCD		0x56
14	Ident Nr.	Gateway serial number BCD		0x34
15	Ident Nr.	Gateway serial number BCD (MSB)		0x12
16	Manufacturer	Manufacturer code (LSB)	LAS	0x33
17	Manufacturer	Manufacturer code (MSB)		0x30

Byte No.	Field Name	Content	Info	Byte data
18	Version	Version (Ignored by gateway)	This can be set to any value	0xFF
19	Device type	Device type (Ignored by gateway)	This can be set to any value	0xFF
20	Access number.	Access Number to gateway		0x75
21	Status	Errors and alerts		0x00
22	Config.	Configuration field	**Example:** Encryption off	0x00
23	Config.	Configuration field		0x00
24	AES-verify	Encryption verification		0x2F
25	AES-verify	Encryption verification		0x2F

Option 2: M-BUS header for only non-encrypted configuration packets

This format is simpler than option 1, but it supports only *non-encrypted* configuration data.

For best security, you should increment the access number (byte 12) by 1 for each packet sent to the device. However, configuration will still function even if you always use the same access number.

Example 3. M-Bus header - Non-encrypted data only

Data Link layer

Byte No	Field Name	Content	Info	Byte data (example)
1	L-Field	Length of data		
2	C-Field	SND-NR		0x44
3	M-Field	Meter Manufacturer Code	LAS	0x33
4	M-Field	Meter Manufacturer Code		0x30
5	A-Field	Serial number BCD (LSB)	**Example:** 0A0A0A0A	0x0A
6	A-Field	Serial number BCD		0x0A
7	A-Field	Serial number BCD		0x0A
8	A-Field	Serial number BCD (MSB)		0x0A
9	A-Field	Version		0x00
10	A-Field	Device type		0x00

Transport layer

Byte No.	Field Name	Content	Info	Byte data
11	CI-Field	Short network header		0x7A
12	Access no.	Access Number		0xA1
13	Status	Errors and alerts		0x00
14	Configuration		**Example:** Encryption off	0x00

Byte No.	Field Name	Content	Info	Byte data
15	Configuration			0x00
16	AES-verify	Encryption verification		0x2F
17	AES-verify	Encryption verification		0x2F

The configuration data is added after the header. This configuration data is also referred to as *ENAPI Data*.

Configuration data is sent the same way on the MQTT interface as with the dongle. A *Non-Disclosure Agreement (NDA)* is required to receive the commands and the structure.

Appendix A: CSV templates

Template 101

File name

```
GTW_<serial_number>_OMS_RAW_<datetime>.csv
```

Example 4. File name

```
GTW_00189170_OMS_RAW_20250430_160120.csv
```

File content

CSV (Comma separated)

```
METER_ADDRESS,READING_DATE,RAW_TELEGRAM
20705566,16:01:20
30/04/2025,3144972666557020410 78C20997A20002025F30D72254FF5A9F1D3BF646381A895B841255D5
A03DBA43B026CB29589EB27B8
```

Format

```
<meter-address>,<datetime>,<mbus_raw_data>
```

Example 5. HTTP header

```
POST /post HTTP/1.1
Host: <host url>
Content-Type: application/octet-stream
Authorization: Basic <Base64encoded username:password>
Content-Length: <datalength>
Connection: keep-alive
Filename: filename.csv
```

Template 201

File name

```
<serial-number>_<device-identification>_valuereport_<time>_<report-id>.csv
```

Example 6. File name

```
0016010439_46159225_valuereport_20200423000656_2103.csv
```

File content

Semicolon separated

```
<serial-number>;<meter_address>;<created>;<0x00>;<mbus_raw_data>
```

Example 7. File content

```
00000161;05047168;2009-12-17
00:00:00;00;08147268710405ac484103470000000c1480769604046dba092e1a426c
```

- M-Bus raw data starts with the M-Bus C-field
- Stop character and checksum are excluded

Example 8. HTTP header

```
POST /post HTTP/1.1
Host: <host url>
Content-Type: application/octet-stream
Authorization: Basic <Base64encoded username:password>
User-Agent: Lansen/<imei> Profile/GW5 Model/<model> Hardware/<hw> Firmware/<fw>
Application/<sw> Serial/<serial> Manufacturer/<manufacturer>
Content-Length: <datalength>
Connection: keep-alive
Filename: filename.csv
```

Template 301

File name format

```
LAS<serial-number>_<timestamp>.xml
```

Example 9. File name

```
LAS00189170_1772629491.xml
```

File content XML-format

```
<?xml version="1.0" encoding="UTF-8"?>
<hyTertiary version="1.3" xmlns="http://www.diehl-metering.com/">
    <info source="LAS00189170" target="EDM" subtype="MDP" time="1772629491">
        <identification>
            <identificationAddress>LAS00189170</identificationAddress>
            <deviceType>49</deviceType>
            <typeDescription>Lansen Gateway</typeDescription>
            <customizedName>GW5</customizedName>
            <hardwareVersion>2</hardwareVersion>
            <softwareVersion>1023</softwareVersion>
            <serialNumber>00189170</serialNumber>
        </identification>
    </info>
    <mdp version="1.2">
        <recData>
            <md deviceId="00242751" time="1772629491" moduleId="1" rssi="-43">

<ra>5444333051272400OB327A1A0000402F2F04FD3A1A0100008240FD3A6E0002FD0F0D02818040FD3A00
84C040FD3A0000000042FD3A00008201FD3A0000C101FD3A7F8202FD3AFFFF066D320CC001010002FD46C7
0D</ra>
            </md>
        </recData>
    </mdp>
</hyTertiary>
```

Example 10. File content content

```
<?xml version="1.0" encoding="UTF-8"?>
<hyTertiary version="1.3" xmlns="http://www.diehl-metering.com/">
    <info source="LAS00189170" target="EDM" subtype="MDP" time="1772629491">
        <identification>
            <identificationAddress>LAS00189170</identificationAddress>
            <deviceType>49</deviceType>
            <typeDescription>Lansen Gateway</typeDescription>
            <customizedName>GW5</customizedName>
            <hardwareVersion>2</hardwareVersion>
            <softwareVersion>1023</softwareVersion>
            <serialNumber>00189170</serialNumber>
        </identification>
    </info>
    <mdp version="1.2">
        <recData>
            <md deviceId="00242751" time="1772629491" moduleId="1" rssi="-43">

<ra>5444333051272400 0B327A1A0000402F2F04FD3A1A0100008240FD3A6E0002FD0F0D02818040FD
3A0084C040FD3A0000000042FD3A00008201FD3A0000C101FD3A7F8202FD3AFFFF066D320CC0010100
02FD46C70D</ra>
            </md>
        </recData>
    </mdp>
</hyTertiary>
```

Index

Copyright and Legal Disclaimer

Lansen Systems AB reserves the right to make changes without further notice to any products herein to improve reliability, function, or design. The information contained in this manual is believed to be accurate at the time of publication, but Lansen Systems AB makes no commitment and assumes no liability for any errors or omissions, loss, or damage resulting from the use of this manual or the products described herein.

Installation, operation, and maintenance of the product must be performed by qualified personnel who are familiar with local codes and regulations, and who have read and understood this manual. Lansen Systems AB is not responsible for any damage or injury resulting from improper installation or operation.