

LANSEN

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

Lansen Systems AB

Version 2.4, 2026-10-30

Table of Contents

Introduction	1
Document conventions	1
About Wireless M-Bus Gateway 5	2
Key characteristics	2
Intended use	2
Product overview	2
General knowledge	5
Configuring the Gateway 5	8
Commission a new gateway	8
Change an existing gateway remotely	9
Lansen Configurator	10
Installing Lansen Configurator	10
Configuration methods	10
Configuring the Gateway 5 with a USB-C cable	11
Configuring the Gateway 5 using wM-Bus	12
Configuring the Gateway 5 using MQTT	13
Connecting to the Gateway 5	14
Access Passwords	15
Access Groups	15
Logging in with an Access password	15
Changing an Access password	15
Logging out	16
Changing and applying settings	17
Apply a change	17
Restore a setting that has not been applied	18
Common configuration tasks	19
Set up MQTT uploads	19
Set up FTP uploads	22
Set up HTTP uploads	23
Collect data from meters	25
Schedule meter collection and uploads	31
Maintain the gateway	36
Troubleshooting tools	39
Appendix A: Settings in the Gateway 5	46
Basic tab	46
Timers tab	48
Routing tab	51
Meters tab	52
Clock tab	54
Bridge tab	54
Timers tab	57
Certificates tab	57
Firmware upgrade tab	58
Extension card tab	59
Appendix B: Sending Configuration Packets to the Gateway 5	61

Option 1: M-BUS header for encrypted and non-encrypted configuration packets	61
Option 2: M-BUS header for only non-encrypted configuration packets	62
Appendix C: Upload templates	64
Template 101	64
Template 201	65
Template 301 (FTP only)	66
Template 301 (HTTP only)	68
Template 401 (FTP only)	69
Index	71
Copyright and Legal Disclaimer	73

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 troubleshooting.

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 **1030**.

Document conventions

This document uses the following formatting to highlight information.

<i>Italics</i>	Important technical concepts
Text	User interface tabs, fields and settings
[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 a configured MQTT, FTP or HTTP endpoint.

Key characteristics

- Received data is timestamped and sent to the configured endpoint 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 can be updated from a URL or locally from a file over USB-C.

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 sends collected data to a configured MQTT, FTP or HTTP endpoint over the network interface supported by that method. 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.

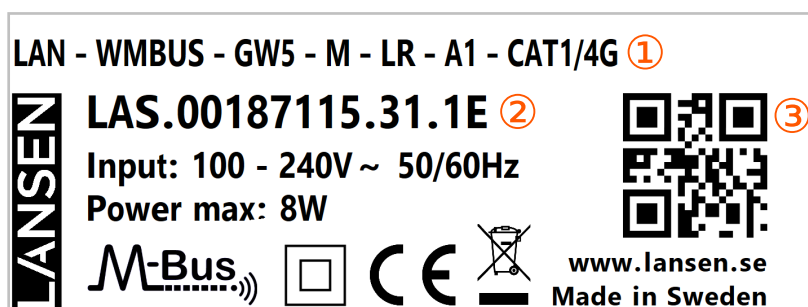


Figure 1. Product label for model LAN-WMBUS-GW5-M-LR-A1-CAT1/4G

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

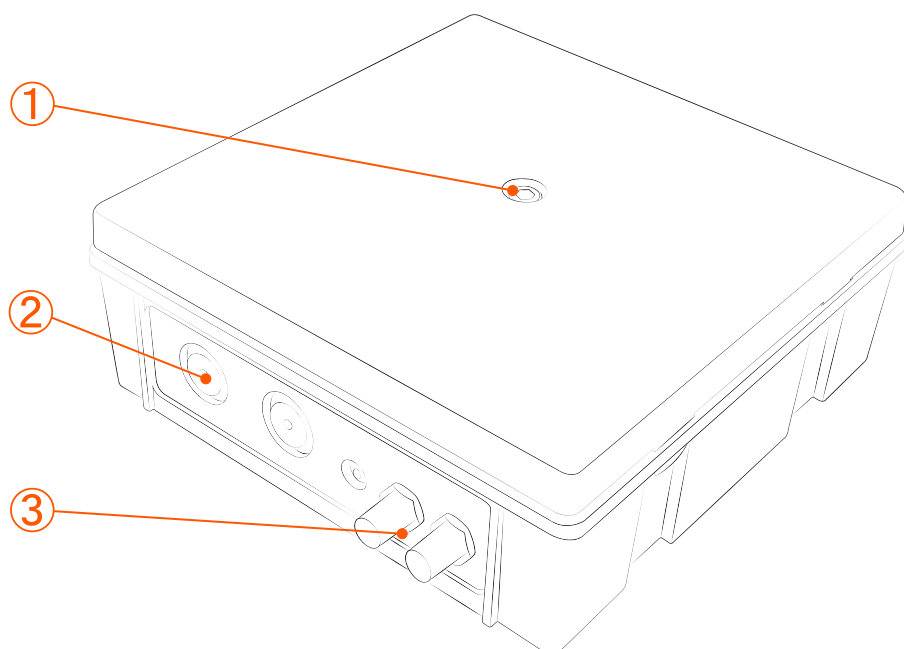


Figure 2. External overview

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.

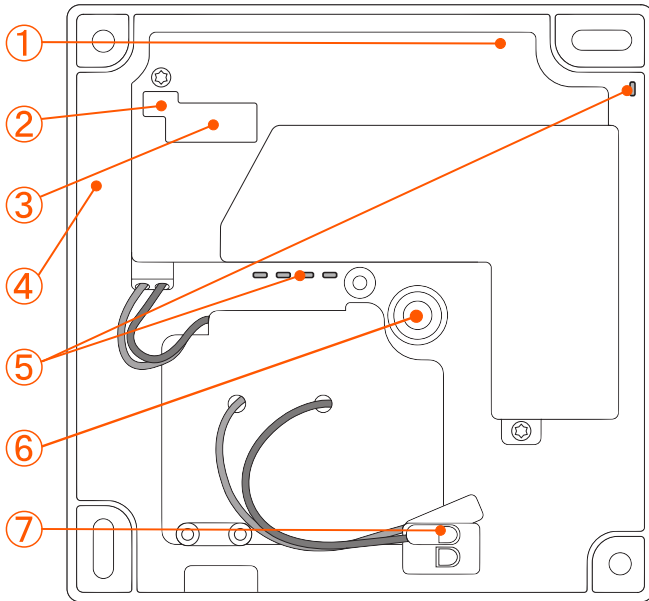


Figure 3. Internal overview

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 configuration of the device and collection of meter data.

M-Bus (With extension card)

Used for 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.

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](#).

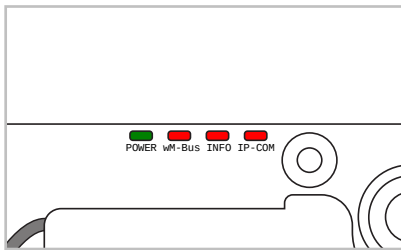


Figure 4. The central LED-strip with four status LEDs.

LED Strip			
POWER		Steady on	The Gateway 5 has power.
POWER		All steady on	Startup sequence active.
POWER			
INFO			
wM-Bus			
IP-COM			
POWER		All blinking	APN incorrect, unable to access network.
POWER			
INFO			
wM-Bus			
IP-COM			
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	Active connection to the MQTT server.
		Blinking	Modem active but not connected to the MQTT server.

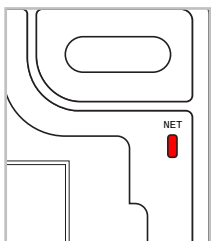


Figure 5. The net status LED.

Cellular network LED		
	Flash every 300 ms (0.3 s)	The Gateway 5 is sending data.

Cellular network LED

	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	
M-Bus search in progress	Two beeps per second for the duration of the search	
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.

Extension cards

The Gateway 5 supports extension cards installed in the extension card slot; see [the product overview](#). These cards add additional physical communication interfaces.

Installing extension cards

Installation of extension cards is offered as a service by Lansen. Please contact your local representative or support team for assistance.

Configuring the Gateway 5

Configuring of the product is done with the Lansen [Lansen Configurator](#) tool. The workflow depends on whether you are commissioning a new device or performing remote maintenance on an existing one.

Commission a new gateway

Before you start, have the following available:

- The device serial number and [Lansen Configurator](#) installed on your computer.
- A USB-C cable or a supported Lansen USB dongle.
- For a dongle connection, the device *AES key*. Use this key to change encrypted settings and read complete server settings. Find the AES key on [lansenonline.com](#).
- An eight-digit *access password* with permission to change the required settings. Find the default passwords on [lansenonline.com](#).
- For MQTT uploads, the server address, port, credentials and topic prefix from your server administrator.
- For FTP uploads, the server address, port, credentials, destination directory and required template.
- For HTTP uploads, the server address, port, required POST content type and template. If the endpoint requires authentication, obtain its username and password.
- For MQTT with TLS or HTTPS, the required TLS settings and certificates from your server administrator.
- For cellular communication, a SIM with its PIN disabled. If your network provider requires an APN, obtain it.
- The intended meter list, reception mode, listening times and upload times for the installation.

Follow these steps to commission the new gateway:

1. Prepare the SIM and antennas for the installed model.

See [the SIM requirements](#) and [the internal device overview](#).

2. Choose the device connection method:

- a. If you use a USB-C cable, follow [the USB-cable connection instructions](#).
- b. If you use a USB dongle, follow [the USB-dongle connection instructions](#).
- c. Follow [the device connection procedure](#).

3. Log in to the device:

- a. Open **Config Repeater / GW / Bridge > Basic > Current access**.
- b. Enter the access password under **Current access** and click [**Login**].
- c. Confirm that you are in the correct *access groups* before changing settings.

See [the access password instructions](#) and [the instructions for applying changes](#).

4. Configure the server's upload method:

- a. If your server uses MQTT, follow [the MQTT upload setup procedure](#).
- b. If your server uses FTP, follow [the FTP upload setup task](#).
- c. If your server uses HTTP, follow [the HTTP upload setup task](#).

5. Configure meter collection:

- a. Select the meter reception mode and filters in the **Basic** and **Routing** tabs.

- b. Select automatic installation in the **Meters** tab or follow [the manual meter installation procedure](#).
 - c. If the installation uses wired M-Bus meters, follow [the wired meter collection procedure](#).
6. Set an upload schedule; follow [the collection and upload scheduling procedure](#).
7. Verify data upload:
- a. If your server uses MQTT, follow [the MQTT upload verification procedure](#).
 - b. If your server uses FTP, follow [the FTP upload verification procedure](#).
 - c. If your server uses HTTP, follow [the HTTP upload verification procedure](#).
8. Restore normal operation:
- a. If you changed settings for testing, restore the intended listening and upload settings.
 - b. If a battery-powered unit no longer needs short-term online testing, disable **Always online**.



A USB-C connection powers the Gateway 5 and overrides its battery supply. After disconnecting the cable, verify operation on the intended power supply and schedule.

Change an existing gateway remotely

Confirm that the Gateway 5 already communicates with the MQTT server you use for configuration. Have the serial number, MQTT server connection details and any required client certificate available. If the device does not yet communicate with this server, commission it locally before attempting remote maintenance. Use this workflow only while **Transport type** is set to **MQTT**. To switch to FTP or HTTP, arrange a local USB-C or dongle connection before changing the transport type.

1. Connect Lansen Configurator to the MQTT server and select the target Gateway 5. See [MQTT connection instructions](#) and [device connection procedure](#).
2. Confirm that the device settings are available and identify the access group required for each planned change.
3. Apply the intended changes and confirm that the device accepts them. Reconnect to verify that each changed setting retains its intended value.

For MQTT server changes, use [the MQTT connection verification procedure](#) to check the new connection.

4. Confirm that the device remains reachable through its configuration MQTT connection.
5. Verify that the MQTT server receives meter data using [the MQTT upload verification procedure](#).



MQTT configuration cannot recover a device with incorrect server settings. Before making remote connection changes, arrange access through USB-C or a dongle in case the device disconnects.

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.

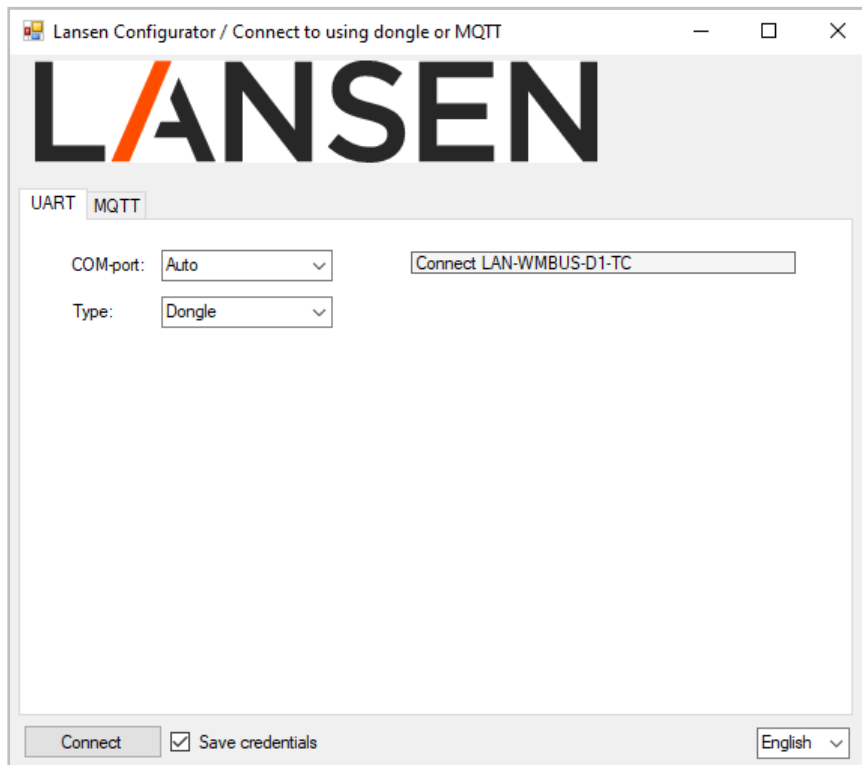


Figure 6. The Lansen Configurator start-up screen. Here you can select connection type, COM-port and language.

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 three steps:

1. Connect the Lansen Configurator program to your chosen configuration interface.
2. Connect the Lansen Configurator program to the Gateway 5.
3. Log in to the Gateway 5 with the appropriate access password.

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.

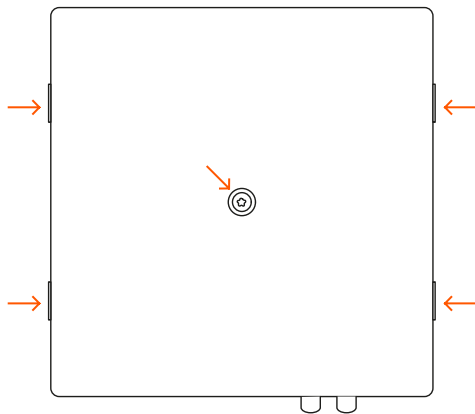


When you use a USB-C cable, the cable supplies power to the Gateway 5. The cable overrides the battery power supply.

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.

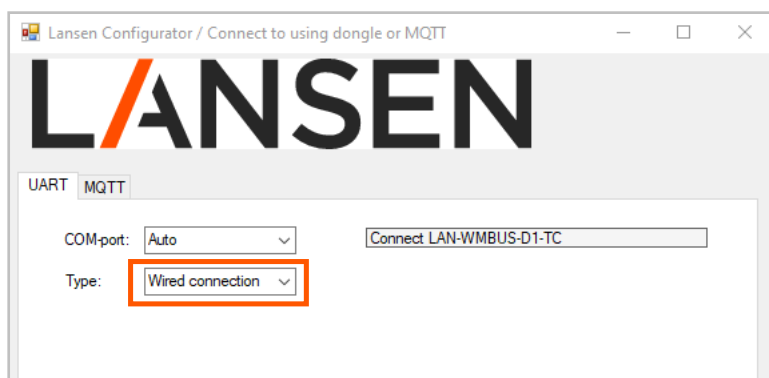


Figure 7. Start-up window with **Wired connection** selected

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

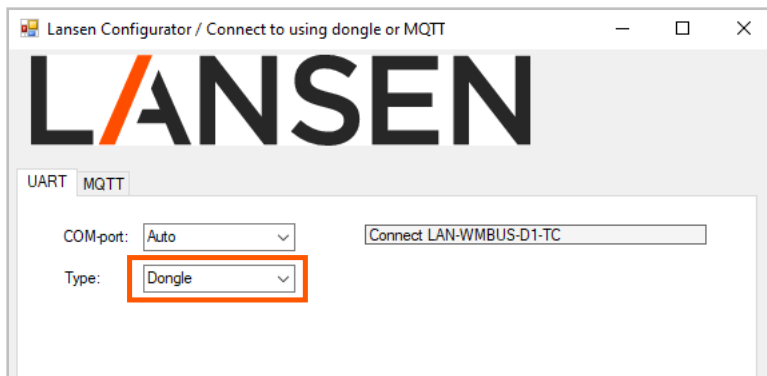


Figure 8. Start-up screen with **Dongle** selected.

3. Click [**Connect**].

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

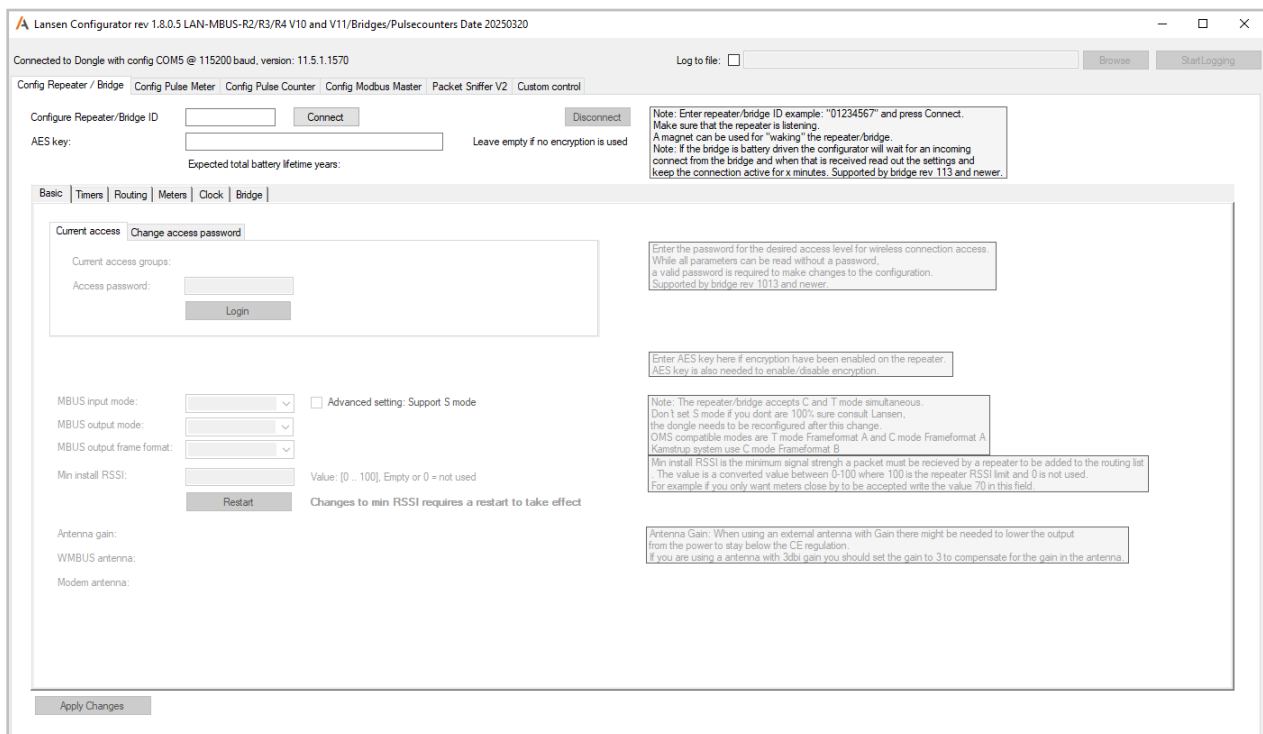


Figure 9. Main screen of Lansen Configurator

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.

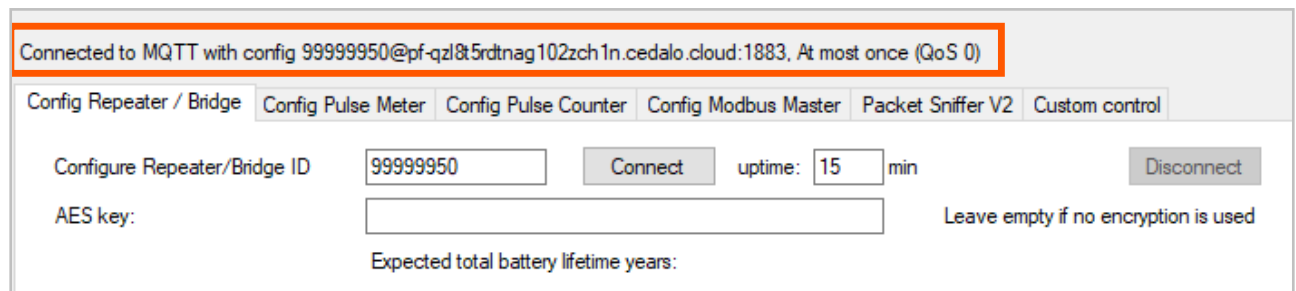
Password: The password to connect to the MQTT server.

.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.

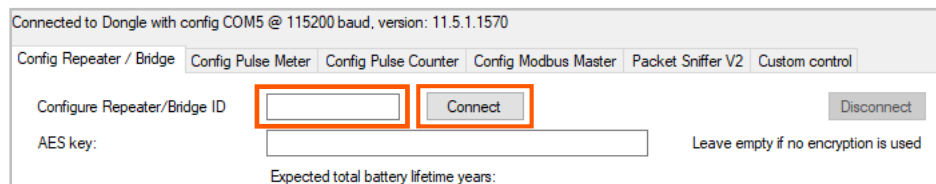
The main screen opens with information about the active MQTT connection.



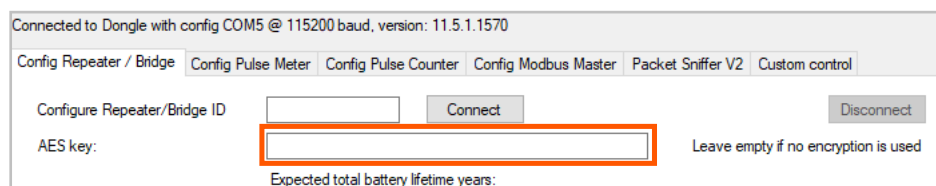
4. Proceed to [Connecting to the Gateway 5](#).

Connecting to the Gateway 5

1. Open the **Config Repeater / GW / 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**].

Access Passwords

To log in to the Gateway 5, use one of its three eight-digit access passwords. lansenonline.com lists the default passwords.

Each password has assigned access groups. LansenConfigurator uses the assigned groups to decide which parameter changes to accept. Access groups are assigned to each password during production. The user cannot change these assignments.

Access Groups

After login, LansenConfigurator displays assigned groups under **Current access groups**.

When a setting requires a group that the current password does not include, LansenConfigurator displays the required group.

Changing a password changes the credential, not its assigned access groups.

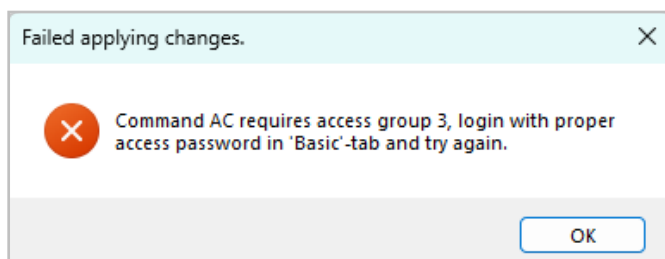


Figure 11. Error message showing the required access group.

Customized configurations for access groups are available upon request.

Logging in with an Access password

1. Open **Config Repeater / GW / Bridge > Basic > Current access**.
2. Enter the *Access password* in the password field.

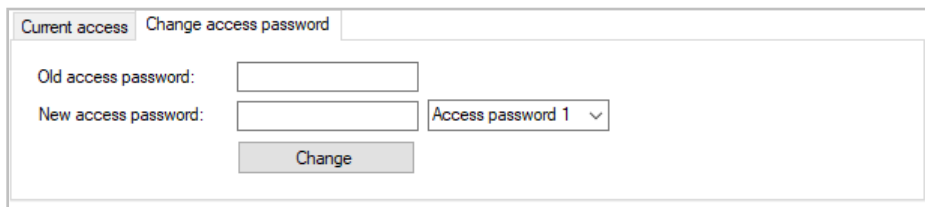
3. Press Enter or click [**Login**]. The assigned groups appear under **Current access groups**.



The login session expires after 15 min of inactivity.

Changing an Access password

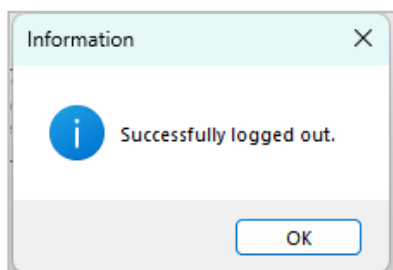
Open **Config Repeater / GW / Bridge > Basic > Change access password** to change a password. Each password must contain eight digits.



1. Enter the current password under **Old access password**.
2. Enter the new password under **New access password**.
3. Select the corresponding password in the dropdown menu.
4. Press Enter or click [**Change**].

Logging out

1. Open **Config Repeater / GW / Bridge > Basic > Current access**.
2. Click [**Logout**].
Pop-up confirming successful logout appears.



The current access groups are changed to "None", indicating that no access password is active.

Changing and applying settings

Use this procedure to change and apply a device setting.

Apply a change

1. Open the **Config Repeater / GW / Bridge** tab.
2. Open the tab that contains the setting.
3. Change the value in the setting field.
The field will be highlighted red to indicate that it has been edited.

Interval: Always On ▾

Listen/pause timers: 1 / 0 Minutes: [0 .. 65000]. 0 = Not used

Listen timer min interval: 0 Hours: [0 .. 255]

Listen timer max value: 0 Minutes: [0 .. 255]

Magnet/reed timer: 15 ← Minutes: [1 .. 1000]

Monthly reading start time: ☐ 08:21 on the 1st ▾ of each month

Monthly reading listen time: 0 Minutes: [0 .. 65000]. 0 = Not used

Apply Changes

Figure 12. Edited settings appear in red

4. Click [**Apply Changes**].
5. Wait for the device to respond.

If the setting was accepted, a popup confirms that the changes have been applied.

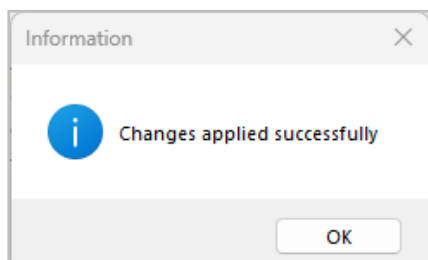


Figure 13. Confirmation that the device applied the change

If the device rejects the setting, a pop-up with an error message appears and the input field remains red.

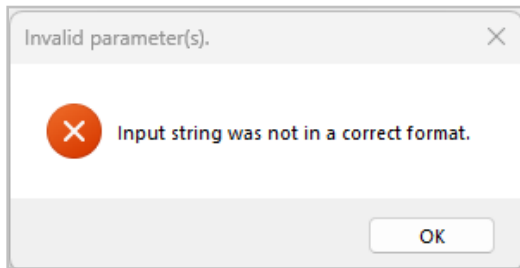


Figure 14. Error shown when the device rejects a setting

Restore a setting that has not been applied

1. Disconnect Configurator from the device.
2. Reconnect by following [the device connection procedure](#).

After reconnecting, green fields show the values read from the device.

Common configuration tasks

This section covers common configuration tasks for the Gateway 5, including server setup, meter collection, scheduling, and maintenance.

Set up MQTT uploads

Use this task to send meter data to an *MQTT* server or change an existing MQTT connection. Configure the device's server settings in the **Bridge** tab. These settings differ from the MQTT settings that connect Lansen Configurator to the server.

Before you start

Connect to the Gateway 5 using [Lansen Configurator](#) and obtain permission to change the required settings. For more information, see [Access Passwords](#). For initial setup, follow [the local commissioning workflow](#). For an established MQTT connection, follow [the remote-maintenance workflow](#).

Have the following available:

- The server host, port, username, password and topic prefix from your server administrator.
- The required *TLS* authentication and SNI settings.
- The root certificate, client certificate and client key required by the selected authentication method.
- For cellular communication, a SIM with its PIN disabled and any provider-specific APN.
- For remote connection changes, a local recovery method.



Lansen Configurator sends **Host**, **Username**, **Password** and **Port** together. The device updates all four settings, even when you change only one field. Confirm all four displayed values before applying changes.

Without an *AES* key, a dongle connection retrieves only the first letter of each MQTT setting. When updating the server connection, do not use these incomplete values. Reconnect with the correct AES key first.

Load certificates

Before enabling server or client authentication that requires certificates, load the required certificates.

1. Open **Config Repeater / GW / Bridge > Bridge > Certificates**.
2. Select the required certificate type from the **Certificate Type** dropdown menu: **Root**, **Client Key** or **Client**.
3. Click [**Browse**] to select the certificate file.
4. Click [**Apply certificate(s)**].
5. Repeat for each certificate or key required by your authentication method.



[**Apply Changes**] does not upload certificates. Use [**Apply certificate(s)**] for each selected certificate or key.

Figure 15. The certificate controls

Configure the gateway connection

1. Open **Config Repeater / GW / Bridge > Bridge > Settings**.

Figure 16. The gateway communication settings

2. For cellular communication with a provider-specific APN, enter the required value under **APN**.

For cellular communication without a provider-specific APN, leave the field empty. The LTE gateway retrieves the APN from the network.



An incorrect APN prevents a mobile data connection. After four failed connection attempts, the Gateway 5 waits one hour before retrying. Rebooting does not clear or shorten this backoff period.

3. Set **Transport type** to **MQTT**.
4. Enter **Host**, **Port**, **Username**, **Password** and **Topic Prefix** using your administrator's settings.

Use the configured server port. Typical ports are 1883 for MQTT without TLS and 8883 for MQTT with TLS.

5. Select the required TLS option under **Internet Security**.

For authentication that requires certificates, follow [the certificate upload procedure](#) first.

6. Select or clear the **SNI** checkbox according to the server requirements.
7. If the installation requires a specific NTP server, enter it under **NTP**.
8. Before configuring schedules, verify the device's UTC clock under the **Clock** tab.

- Configure the connection and upload schedule for the device's power supply:

Scheduled battery operation

Disable **Always online**. Set the upload schedule under the **Bridge** tab after the [configured listening period](#).

Continuous mains-powered operation

If the installation requires continuous online operation, enable **Always online**. The upload time schedule has no effect while this setting is enabled.

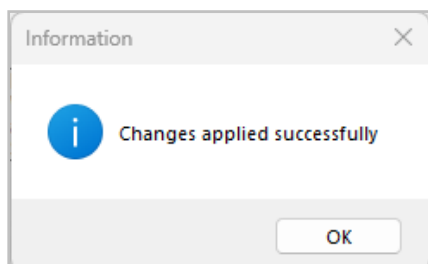


Always online increases power consumption. For short-term battery-powered testing, enable **Always online** only while testing. After testing, restore the operational schedule.

Apply and verify the connection settings

- Open **Config Repeater / GW / Bridge > Bridge > Settings**.
- Confirm all four connection fields again: **Host**, **Username**, **Password** and **Port**.
- Click [**Apply Changes**] and wait for the Gateway 5 to respond.

A pop-up confirms that the changes have been applied.



- Before restarting, check the current settings using [the settings check instructions](#).

If the remote connection has ended, reconnect using the new server details or the arranged local recovery method.

- If the displayed values differ, resolve any access or configuration error before proceeding.
- If you changed the transport protocol, restart the device using [**Restart**] under the **Basic** tab.

Server-address changes take effect at the next internet connection. If these changes must take effect immediately, restart the device. For a remote change, confirm the values before restarting. A restart can end the current session.

- If you restarted the device, reconnect. Use the new server details for an MQTT connection.
- Follow [the upload verification procedure](#).

Verify that meter data reaches the receiving application

Before this verification, configure the intended meters and listening schedule. Use automatic installation or follow [the manual meter installation procedure](#).

- Allow the Gateway 5 to listen during the configured listening window and reach its next upload time.

For an online unit, verify data arrival while it is connected.

- Confirm that the MQTT server receives data from this gateway under the configured topic prefix.

3. Identify the gateway and intended meters in the received data.

A server login alone does not confirm successful meter collection.

4. Confirm that readings arrive for the listening period you test.
5. If the receiving application is separate from the MQTT server, confirm that it processes the data.
6. If meter data is missing, verify the meter list, filters, schedules, network connection and MQTT/TLS settings.

Packet Sniffer V2 over MQTT shows packets that the gateway transmits. A dongle sniffer shows packets that the dongle detects. These packets do not confirm gateway reception or upload.

7. If you temporarily enabled **Always online** on a battery-powered unit, disable it.
8. If you changed settings, click [**Apply Changes**].
9. Confirm another upload using the operational schedule.

The task is complete when Configurator shows the intended settings after reconnecting and the receiving application receives the intended meter data. Verify this result using the operational schedule.

Set up FTP uploads

Use this task when the receiving server accepts FTP uploads. FTP is available only when the network interface is the modem.

Before you start

Connect to the Gateway 5 using [Lansen Configurator](#) and get permission to change its settings. For more information, see [Access Passwords](#). For remote configuration, use an existing MQTT connection. Arrange local access before changing server details remotely.

Have the following details from your server administrator:

- Server address, port, username and password.
- Destination directory and required template.
- A provider-specific APN, if cellular service requires one.



The Lansen Configurator sends **Host**, **Username**, **Password** and **Port** together. The device updates all four values, even if you change only one. Check all four values before applying changes.

Configure the FTP connection

1. Open **Config Repeater / GW / Bridge > Bridge > Settings**.
2. If your provider requires a specific APN, enter it under **APN**.
3. Confirm that **Network interface** displays the modem.
4. Enter the server address in **Host**.
5. Enter the server's port. Use port 21 if your administrator does not provide one.
6. Set **Transport type** to **FTP**.
7. Select the template required by the receiving server:
 - Select **Template 101** for the SensusRF CSV format.

- Select **Template 201** for the Elvaco CSV format.
- Select **Template 301 (FTP only)** for the Diehl XML format.
- Select **Template 401 (FTP only)** for the Diehl XML format with hyTertiary version 1.2.

See [the upload template reference](#) for examples.

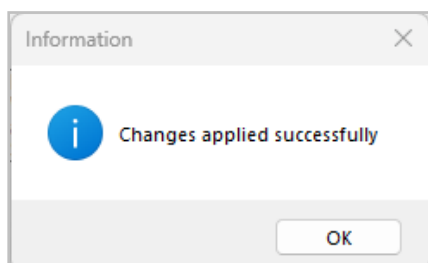
- Enter the server username and password in **Username** and **Password**.
- Enter the destination under **Directory**.



The device supports one directory level.

- Follow [the upload scheduling procedure](#) to schedule uploads after meter collection.
- Check **Host**, **Username**, **Password** and **Port** before applying changes.
- Click [**Apply Changes**] and wait for the device to respond.

A pop-up confirms that the changes have been applied.



- Reconnect and check the current settings using [the settings check instructions](#).
- If you changed the transport protocol, restart the device using [**Restart**] under the **Basic** tab.
- If you changed the server address and need it to take effect now, restart the device.

Server-address changes take effect at the next internet connection.

- If you restarted the device, reconnect.
- Follow [the FTP upload verification procedure](#) after you configure the meter list and schedule.

Verify FTP uploads

- Wait for the device's scheduled upload.
- Confirm that the FTP server receives a file in the selected directory.
- Confirm that the file uses the selected template and contains data from the intended meters.
- If the file is missing or incorrect, check the modem connection, server settings, directory, template, meter list and schedule.

Set up HTTP uploads

Use this task when the receiving server accepts HTTP uploads. HTTP is available only when the network interface is the modem.

Before you start

Connect to the Gateway 5 using [Lansen Configurator](#) and get permission to change its settings. For remote

configuration, use an existing MQTT connection. Arrange local access before changing server details remotely.

Have the following details from your server administrator:

- Server address and port.
- Username and password, if the endpoint requires authentication.
- Required TLS settings and certificates, if the endpoint uses HTTPS.
- Required POST content type and template.
- A provider-specific APN, if cellular service requires one.



The Lansen Configurator sends **Host**, **Username**, **Password** and **Port** together. The device updates all four values, even if you change only one. Check all four values before applying changes.

Configure the HTTP connection

1. Open **Config Repeater / GW / Bridge > Bridge > Settings**.
2. If your provider requires a specific APN, enter it under **APN**.
3. Confirm that **Network interface** displays the modem.
4. Enter the server address in **Host**.
5. Enter the server's port. Use port 80 for HTTP or port 443 for HTTPS if your administrator does not provide one.
6. Set **Transport type** to **HTTP**.
7. If the endpoint requires authentication, select **HTTP authentication**.
8. If the endpoint requires HTTPS, select the required TLS option under **Internet Security**.

If the server requires certificates, follow [the certificate upload procedure](#).

9. Select the content type required by the endpoint under **HTTP POST Content type**.

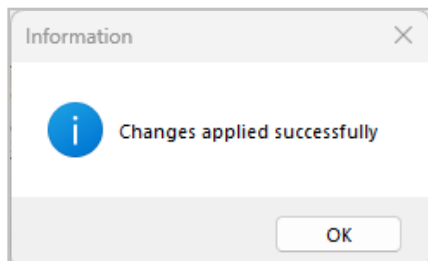
Use **application/octet-stream** unless the endpoint requires **multipart/formdata**.

10. Select the template required by the receiving server:
 - Select **Template 101** for the SensusRF CSV format.
 - Select **Template 201** for the Elvaco CSV format.
 - Select **Template 301** for the Elvaco CSV format.

See [the upload template reference](#) for examples.

11. If the endpoint requires authentication, enter the username and password in **Username** and **Password**.
12. Follow [the upload scheduling procedure](#) to schedule uploads after meter collection.
13. Check **Host**, **Username**, **Password** and **Port** before applying changes.
14. Click [**Apply Changes**] and wait for the device to respond.

A pop-up confirms that the changes have been applied.



15. Reconnect and check the current settings using [the settings check instructions](#).
16. If you changed the transport protocol, restart the device using [**Restart**] under the **Basic** tab.
17. If you changed the server address and need it to take effect now, restart the device.

Server-address changes take effect at the next internet connection.
18. If you restarted the device, reconnect.
19. Follow [the HTTP upload verification procedure](#) after you configure the meter list and schedule.

Verify HTTP uploads

1. Wait for the device's scheduled upload.
2. Confirm that the HTTP endpoint receives the request.
3. Confirm that the receiving application processes data from the intended meters.
4. If an upload fails, check the modem, server settings, security, content type, template, meter list and schedule.

Collect data from meters

Use this task to choose which *Wireless M-Bus* meters the Gateway 5 stores. Set the reception mode, add meters and confirm that the device receives their data.

Before you start

Connect to the device with [Lansen Configurator](#). Follow [the local commissioning workflow](#) or [the remote-maintenance workflow](#). Get permission to change the settings. Set the listening and upload schedules before you verify meter data. For S-mode meters, complete the other settings before following [the S-mode procedure](#).

Have the following available:

- The meters' transmission modes and manufacturer codes.
- For manual installation, each meter's manufacturer ID, serial number, device type and version.
- For CSV import, a CSV-file with the details for each meter
- For an external antenna, its type and gain.
- The intended listening schedule and server connection settings for upload verification.

Set up wireless meter reception

1. Open **Config Repeater / GW / Bridge > Basic**.
2. For C-mode or T-mode meters, select the matching mode under **MBUS input mode**.

The default **TC** input accepts C-mode and T-mode packets. For S-mode meters, complete the other settings before following [the S-mode procedure](#).

3. Select the installed internal or external antenna for Wireless M-Bus reception.
4. For models with an external Wireless M-Bus antenna, enter its gain under **Antenna gain**.

The device adjusts its output power to meet legal limits.

5. Enter the minimum signal strength under **Min install RSSI**.

This value controls which meters enter the *internal routing list*. Do not use it to exclude nearby meters without a reason.

6. Open the **Routing** tab.
7. Enter the required manufacturer codes under **Accept Manufacturer ID**.

If you accept all manufacturers, leave the fields empty.

8. Select the required option under **Route messages**:

Route only OMS messages

The device accepts packets only from OMS-compatible meters.

Route all messages

The device accepts packets from OMS-compatible and non-OMS-compatible meters.

9. Click [**Apply Changes**].
10. Reconnect and check the settings using [the settings check instructions](#).
11. If you changed **Min install RSSI**, restart the device using [**Restart**] under the **Basic** tab.

Restart the device to update the internal routing list.

12. If you restarted the device, reconnect.

Select a meter installation method

The internal routing list holds up to 2000 unique meters. Choose how to add meters:

Automatic discovery

Use [the automatic installation procedure](#) to add meters that the device detects.

Manual whitelist

Use [the manual installation procedure](#) to add selected meters one at a time.

CSV whitelist

Use [the CSV import procedure](#) to add meters from a file.



When automatic installation is off and the list is empty, the device stores no meter data. Add the meters before you verify collection.

Discover meters automatically

1. Open **Config Repeater / GW / Bridge > Meters**.
2. Select the **Automatic meter installation** checkbox.

Automatic meter installation: ☒ YES

Figure 17. Automatic meter installation enabled

- Click [**Apply Changes**].
- Allow the device to receive meter packets during its [configured listening period](#).
- Click [**Load all meters**] to display the internal routing list.

Number of meters: 1074 free slots

Figure 18. Meter count and free slots

A pop-up confirms that all meters have been loaded.

- Compare the displayed meters with your list. Check the meter count and free slots.
- Follow [the meter verification procedure](#).

If you want a fixed list, clear **Automatic meter installation** after discovery. Click [**Apply Changes**]. Follow [the meter removal procedure](#) to remove unwanted entries.

Add specific meters manually

- Open **Config Repeater / GW / Bridge > Meters**.
- Clear the **Automatic meter installation** checkbox.
- Click [**Apply Changes**].
- Reconnect and check that automatic installation is off using [the settings check instructions](#).

Add meter data:		Manufacturer	Serial number	Device type	Version
				Wildcard	
				Wildcard	
				Wildcard	
				Wildcard	
				Wildcard	
				Wildcard	
				Wildcard	

Figure 19. Manual meter entry fields

- Enter the manufacturer ID, serial number, device type and version under **Add meter data**.

Use [the device-type reference](#) to choose the device type.

- Click [**Add meter(s)**].

The program confirms when it adds the meter.

Information

 Successfully added manual meters.

7. Repeat for each intended meter.
8. Click [**Load all meters**] and compare the identifiers with your list.
9. Follow [the meter verification procedure](#).

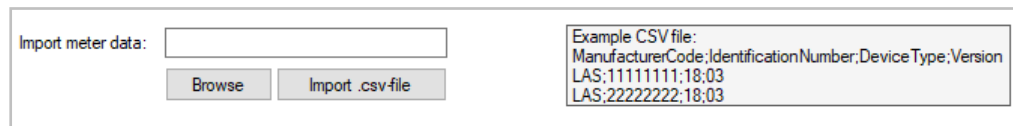
Import a meter list from CSV

1. Prepare a CSV file with this exact first row:

```
ManufacturerCode;IdentificationNumber;DeviceType;Version
```

Separate the four fields with semicolons. Put each meter on a separate row. Use [the device-type reference](#) to choose each device type.

2. Open **Config Repeater / GW / Bridge > Meters**.
3. Clear the **Automatic meter installation** checkbox.
4. Click [**Apply Changes**].
5. Reconnect and check that automatic installation is off using [the settings check instructions](#).



The screenshot shows a web interface for importing meter data. On the left, there is a section titled 'Import meter data:' containing a text input field, a 'Browse' button, and an 'Import .csv-file' button. On the right, there is a box labeled 'Example CSV file:' containing the following text: 'ManufacturerCode;IdentificationNumber;DeviceType;Version', 'LAS;11111111;18;03', and 'LAS;22222222;18;03'.

Figure 20. CSV meter import controls and example header

6. Click [**Browse**] and select the CSV file.
7. Click [**Import .csv-file**] to upload the meter list.
8. After the import, click [**Load all meters**].
9. Compare the displayed identifiers with the CSV file. Confirm that the intended meters appear in the list.
10. Follow [the meter verification procedure](#).



The program does not upload the file if its first row does not match the required header.

Remove unwanted meters

1. Open **Config Repeater / GW / Bridge > Meters**.
2. Clear the **Automatic meter installation** checkbox and click [**Apply Changes**].

This stops the device from adding the removed meters again.

3. Click [**Load all meters**].

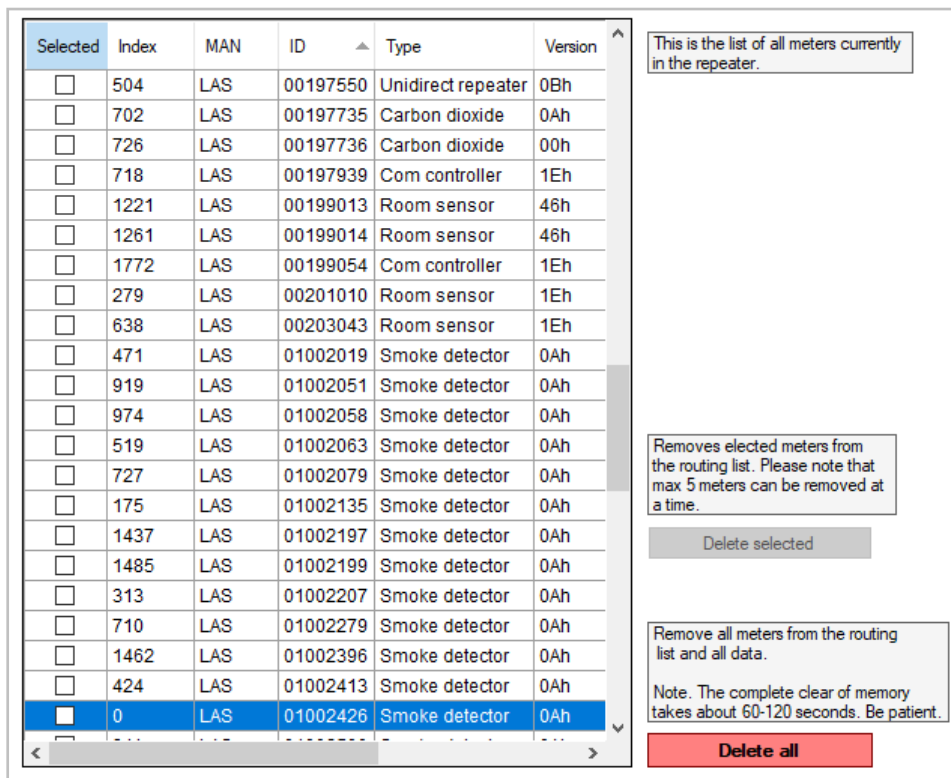


Figure 21. The internal routing list.

4. Select the meters you want to remove.
5. Click [**Delete selected**].
6. Click [**Load all meters**] again. Confirm that the unwanted meters are gone and the intended meters remain.
7. Follow [the meter verification procedure](#).

Clear the entire meter list

Turn on **Automatic meter installation** before you use [**Delete all**]. The device can add detected meters to the list again while this setting is on.

1. Open **Config Repeater / GW / Bridge > Meters**.
2. Select the **Automatic meter installation** checkbox and click [**Apply Changes**].
3. Click [**Delete all**].

The device takes about two minutes to clear the list.

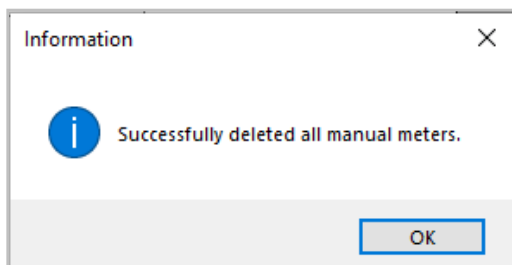


Figure 22. Delete confirmation

4. If you want to keep the list empty, clear **Automatic meter installation** and click [**Apply Changes**].
5. Click [**Load all meters**] and confirm that the list is empty.

Switch to S-mode after configuration

Complete the server settings, meter list and listening schedule before you switch to S-mode.



The LAN-WMBUS-D1/D2 dongle cannot configure an S-mode device unless it also sends in S-mode. Contact Lansen for setup instructions before you switch the device. Use a USB-C connection if the dongle cannot communicate in S-mode.

1. Open **Config Repeater / GW / Bridge > Basic**.
2. Select the **Advanced setting** checkbox.
3. Select **S-mode** under **MBUS input mode**.
4. Click [**Apply Changes**].
5. Reconnect using USB-C, a correctly configured dongle or an established MQTT connection.
6. Check the input mode in Configurator using [the settings check instructions](#).
7. Follow [the meter verification procedure](#).

Collect data from wired M-Bus meters

Use an M-Bus extension card to connect wired M-Bus meters. The wired and wireless meter lists are independent. Each list holds up to 2000 meters.

Before you start, make sure that:

- An M-Bus extension card is installed.
- The M-Bus line is connected using the instructions for that card.

On mains-powered gateways, start the search manually. On battery-powered gateways, the search starts automatically at start-up. When **Enabled sound indications** is selected, the device beeps twice per second during the search.

1. Open **Config Repeater / GW / Bridge > Bridge > Extension card > M-Bus master settings**.
2. Confirm that **Extension card** shows **M-Bus**.

Basic | Timers | Routing | Meters | **Config** | Bridge | Moty

Settings | Timers | Ethernet settings | Certificates | Firmware upgrade | Extension card

Extension card: mBus
Read interval (s): 30

Note: This field indicates the extension card installed on the bridge – Pulse Counter, Modbus, or M-Bus. The Read interval determines the polling frequency for that card.

Pulse counter settings | Modbus master settings | **mBus master settings**

Number of meters: 1704 / 296 free slots
Load all meters
Read all meters that are in the routing list of the repeater

Search control:
Stop search
Running
Refresh status

Wired response time: 1 [0..255] seconds
Current measurement: 1163 uA
Refresh measurement

Wired mBUS meters:

Selected	Index	MAN	ID	Type	Version	Baudrate
☒	0	N\	00000100	46	00h	68
☐	1	B@D	09888888	122	1Bh	205
☐	2	H@@	65322F2F	Other	00h	114
☐	3		006501B2	Com controller	00h	251
☐	4	!H@	B1001BFB	251	01h	27
☐	5	HXB	00B096C2	Other	00h	0
☐	6	WN	0002003A	Other	00h	45
☐	7	LAS	02000482	Room sensor	07h	122
☐	8		022F2F20	58	65h	8
☐	9	RSE	65018208	Heat Cost Al.	62h	2
☐	10	E@Z	1AFB4201	Oil	90h	130
☐	11	FW	00C50183	Other	00h	0
☐	12	72	00000000	Other	00h	25

This is the list of all wired mBUS meters currently in the repeater.

Removes selected meters from the routing list.
Delete selected

Remove all meters from the routing list and all data.
Note: The complete clear of memory takes about 60-120 seconds. Be patient.
Delete all

Figure 23. The M-Bus master search and wired meter list

3. If the installation requires a different response time, set **Wired response time** to a value from 0 to 255 seconds.



A value of 0 for **Wired response time** disables reading from the M-Bus line.

4. If the gateway is mains-powered, click [**Start search**].
5. Click [**Refresh status**] to see the search status.
6. If the search finds the intended meters, click [**Stop search**].
7. If the search stops before finding all intended meters, click [**Refresh current measurement**] and check the line load.
The device stops the search if the line load exceeds 6 mA.
8. Click [**Load all meters**] to display the wired meter list.
9. Confirm that the intended meters appear in the list.

The table shows each meter's index, manufacturer ID, ID, type, version, baud rate and status.

10. Verify that wired meter data reaches the receiving application:
 - a. If the device uploads over MQTT, follow [the MQTT upload verification procedure](#).
 - b. If the device uploads over FTP, follow [the FTP upload verification procedure](#).
 - c. If the device uploads over HTTP, follow [the HTTP upload verification procedure](#).

Click [**Delete selected**] to remove selected meters from the wired list. Click [**Delete all**] to remove all wired meters and their data. This takes about 60 to 120 seconds.

Verify meter collection and delivery

1. Open **Config Repeater / GW / Bridge > Meters**.
2. Click [**Load all meters**].
3. Confirm that the intended wireless meters appear in the internal routing list.
4. Allow the device to listen during the configured listening period.
5. Confirm that new readings from the intended wireless meters reach the receiving application.

For MQTT uploads, follow [the MQTT upload verification procedure](#). For FTP uploads, follow [the FTP upload verification procedure](#). For HTTP uploads, follow [the HTTP upload verification procedure](#).

6. If readings are missing, verify the input mode, manufacturer filter, OMS filter, RSSI threshold and listening schedule.



An entry in the internal routing list does not prove that the device still receives data from that meter. **Packet Sniffer V2** over USB-C shows packets that the gateway detects. A dongle sniffer shows packets that the dongle detects. Neither check alone proves that the device stores or uploads the data.

The task is complete when the receiving application gets new data from the intended wireless meters.

Schedule meter collection and uploads

Use this task to coordinate meter reception and data uploads for the Gateway 5. Configure the clock, listening periods and upload times separately. Use *suppression timers* to control how often the device stores packets from each meter.

Before you start

Connect to the device using [Lansen Configurator](#) and obtain permission to change the required settings. Before verifying the schedule, configure the server connection and meter installation method. See the setup procedure for the selected upload method: [the MQTT upload setup procedure](#), [the FTP upload setup procedure](#) or [the HTTP upload setup procedure](#). See [the meter collection instructions](#).

Have the following available:

- The intended listening times, durations, weekdays and repeat intervals.
- The intended upload times and dates.
- The meters' transmission intervals and the required reading frequency.
- For a specific NTP server, its address and network availability.

Verify the clock before scheduling

1. Open **Config Repeater / GW / Bridge > Clock**.
2. Compare **Repeater clock (UTC)** with the current UTC time.
3. Review **Clock diff (s)** to compare the device clock with the computer clock.
4. If the installation requires a specific NTP server, enter its address under **NTP** in the **Bridge** tab.
5. If you changed the NTP setting, click [**Apply Changes**].
6. Reconnect and check the NTP address using [the settings check instructions](#).
7. If you need manual clock synchronization, verify the computer clock and click [**Sync clock with PC**].
8. Before entering listening times, verify the device's UTC clock again.

The device uses the configured NTP server for clock synchronization. It synchronizes when it connects to the internet or every 12 hours. Enter listening start times in UTC, not local time.

Set listening periods

1. Open **Config Repeater / GW / Bridge > Timers > Listen timers**.
2. Select the **Start time schedule** checkbox.
3. Enter the intended listening start time in UTC.
4. Select the active weekdays and clear the other weekdays.
5. Select the required repeat schedule under **Repeat start time schedule**.
6. If you select **On certain dates**, select the required dates as well as the active weekdays.
7. Select the listening interval for the installation.

The start time must not exceed the selected interval.

8. Enter the listening and pause durations in minutes under **Listen/pause timers**.

For a daily 30-minute listening period, use a 24-hour interval with 30 minutes listening and 1410 minutes paused.

9. Enter the required **Magnet/Reed timer** duration for local configuration and temporary listening.
10. Click [**Apply Changes**].
11. Reconnect and check the listening schedule using [the settings check instructions](#).

Figure 24. The listening start-time controls

The listening interval, start time and listen/pause durations work together. See [the detailed listening timer settings](#) for additional options.

Schedule uploads after collection

For scheduled uploads, use this procedure. For battery operation, schedule an upload after the listening period finishes. Leave time between collection and upload, as shown in [the daily schedule example](#).

1. Open **Config Repeater / GW / Bridge > Bridge > Settings**.
2. For scheduled uploads, disable **Always online**.
3. Open **Bridge > Timers**.
4. Select the **Upload time schedule** checkbox and enter the intended upload time.
5. Select the active weekdays and the required repeat schedule.
6. If you select **On certain dates**, select the required upload dates as well as the active weekdays.
7. Select the required **Modem upload time interval**.
8. Compare the upload days with the listening days.

Each scheduled upload must follow the collection period whose data it sends.

9. Click **[Apply Changes]**.
10. Reconnect and check the upload schedule using [the settings check instructions](#).
11. Follow [the schedule verification procedure](#).



If **Always online** is enabled, the upload time schedule has no effect. Use continuous online mode only for mains-powered units or short-term battery-powered testing.

Figure 25. The upload scheduling controls

Example of a daily collection and upload schedule

This example uses the listening and upload times documented for battery operation. Adjust the schedule to match the meters and the installation's reading requirements.

Table 2. Daily schedule example

Setting	Location	Example value
Listening start time	Timers tab	05:20 UTC
Listening interval	Timers tab	24 hours
Listen/pause durations	Timers tab	30/1410 minutes
Upload time	Bridge tab, Timers	06:00
Modem upload time interval	Bridge tab, Timers	24 hours
Always online	Bridge tab	Disabled

The listening period ends at 05:50. The upload starts later, at 06:00. Select matching active days for listening and uploading. Before leaving the installation, verify the resulting schedule on the device.

Configure monthly or selected-date collection

Choose the scheduling method that matches the installation:

One monthly reading period

Use the separate **Monthly reading start time** timer for a reading period on one day each month.

Several selected dates

Select **On certain dates** in the repeat schedule for listening and uploading.

Set a monthly reading period

1. Open **Config Repeater / GW / Bridge > Timers > Listen timers**.
2. Select the **Monthly reading start time** checkbox.
3. Enter the start time and select the required day of the month.
4. Enter the collection duration under **Monthly reading listen time**.
5. Click [**Apply Changes**].
6. Reconnect and check the monthly timer using [the settings check instructions](#).
7. Follow [the upload scheduling procedure](#) to arrange an upload after the monthly reading period.
8. Follow [the schedule verification procedure](#).

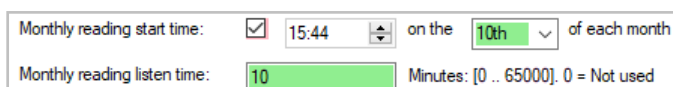


Figure 26. The monthly reading controls

Set selected listening and upload dates

Use this task to collect and upload data on selected dates each month. Set the listening periods and upload times before choosing the dates. See [the listening task](#) and [the upload task](#).

1. Open **Config Repeater / GW / Bridge > Timers > Listen timers**.
2. Set **Repeat start time schedule** to **On certain dates**.
3. Select the listening dates and active weekdays.
4. Click [**Apply Changes**].
5. Open **Bridge > Timers**.

6. Set **Repeat start time schedule** to **On certain dates**.

7. Select the upload dates and active weekdays.

For uploads on the 1st and 15th on weekdays, select **1**, **15** and **Mo** through **Fr**. If the 1st falls on a weekend, the upload moves to the next selected weekday.

8. Compare the listening and upload dates, including any dates that move to a weekday.

9. Confirm that each upload follows the listening period whose data it sends.

10. Click [**Apply Changes**].

11. Follow [the schedule verification procedure](#).

Set how often the device stores meter packets

Suppression controls packet storage, not the listening start time or server connection schedule. Choose values that match the required reading frequency.

1. Open **Config Repeater / GW / Bridge > Timers > Global suppression timer**.

2. Enter the required suppression interval and select minutes or hours.

3. If you need the internal 10-second suppression delay, set the global value to 0.

Select the **Internal suppression timer** checkbox.

4. If you need no global or internal suppression, set the global value to 0.

Clear the **Internal suppression timer** checkbox.

5. If a device type needs a different interval, follow [the device-type suppression task](#).

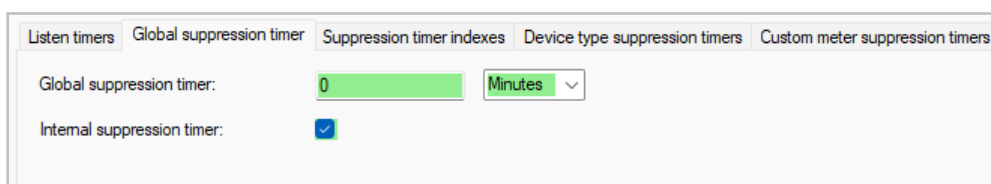
6. If individual meters need different intervals, review the custom-meter rules before applying changes.

See [the detailed suppression timer settings](#).

7. Click [**Apply Changes**].

8. Reconnect and check the suppression settings using [the settings check instructions](#).

9. Follow [the schedule verification procedure](#) to verify the resulting readings.



The screenshot shows a configuration window with five tabs: 'Listen timers', 'Global suppression timer', 'Suppression timer indexes', 'Device type suppression timers', and 'Custom meter suppression timers'. The 'Global suppression timer' tab is selected. It contains two settings: 'Global suppression timer:' with a green input field containing '0' and a 'Minutes' dropdown menu, and 'Internal suppression timer:' with a checked checkbox.

Figure 27. The global and internal suppression controls



The internal suppression timer applies a 10-second delay when enabled. You can change its enabled state only when the global suppression value is 0. Review device-type and custom-meter rules as part of the installation's suppression configuration.

Assign a suppression timer to a device type

Use this task when all meters of one device type need the same suppression interval. Choose the device type and timer index before you start. Index 0 uses the global timer; indexes 1-3 are configurable, and indexes 4-7 are predefined. See [the suppression timer reference](#) for the index settings.

1. Open **Config Repeater / GW / Bridge > Timers > Device type suppression timers**.
2. Click [**Load all**] to view the stored mappings.
3. Select the **Device type** under **Add new mapping**.

See [the device-type reference](#) for available device types.

4. Select the **Suppression timer index** for that device type.
5. Click [**Add**] to create the mapping.
6. Click [**Load all**] again.
7. Confirm that the list shows the selected device type and timer index.
8. Follow [the schedule verification procedure](#) to verify the resulting readings.

Verify the operational schedule

1. Reconnect and check the clock, listening schedule, upload schedule and suppression settings using [the settings check instructions](#).
2. Open the **Config Repeater / GW / Bridge** tab to view these settings.
3. Compare the displayed values with the installation's requirements.
4. If you changed settings for temporary testing, restore the operational values and click [**Apply Changes**].
5. If a battery-powered unit no longer needs short-term online testing, disable **Always online** and apply the change.
6. If you used USB-C during setup, disconnect the cable and verify operation on the intended power supply.
7. Allow the device to complete a listening period and its following upload using the operational schedule.
8. Confirm that the receiving application receives new readings from the intended meters for that collection period.

For MQTT uploads, follow [the upload verification procedure](#).

9. If readings are missing, verify the UTC clock, active days, date selections, listening durations and upload settings.
10. If reading frequency differs from the requirements, review global, internal, device-type and custom-meter suppression settings.

The task is complete when the operational schedule delivers the required meter readings to the receiving application.

Maintain the gateway

Use these tasks to update credentials, configuration encryption or firmware. Use the extension-card procedures only when a card is installed. Before each task, connect to the Gateway 5 using [Lansen Configurator](#) and follow [the remote-maintenance workflow](#) or a local connection method. Obtain permission to change the required settings.

Change an access password

For password-change instructions, follow [the access password chapter](#). Each password grants access to a different set of parameters. Use an eight-digit password.

Change configuration encryption

The **Encryption** setting protects configuration communication. It does not encrypt incoming data packets from meters. The meters encrypt their own packets separately when configured to do so.

1. Before changing the encryption setting over a dongle, obtain the correct device *AES key*.
2. Open **Config Repeater / GW / Bridge > Basic**.
3. Enter the correct key in the **AES key** field.
4. Select the approved option from the **Encryption** dropdown menu.



Figure 28. Encryption options in the Basic tab

5. Click [**Apply Changes**] and wait for the device to respond.
6. Reconnect using the supported connection method.
7. Check the **Encryption** field and confirm that you can access the device.

The correct AES key is required for the device to apply parameter changes when configuration encryption is enabled. The AES key is not needed when you configure the device through MQTT. See [the encryption settings reference](#) for the available options and their effects.

Update gateway firmware

Choose how to supply the firmware:

Firmware URL

Follow [the firmware URL update procedure](#).

Local file over USB-C

Follow [the local firmware update procedure](#).

Update gateway firmware from a URL

Obtain the valid firmware URL and version for this device before starting the update. For a remote update, arrange local recovery access before changing firmware.

1. Open **Config Repeater / GW / Bridge > Bridge > Firmware upgrade**.

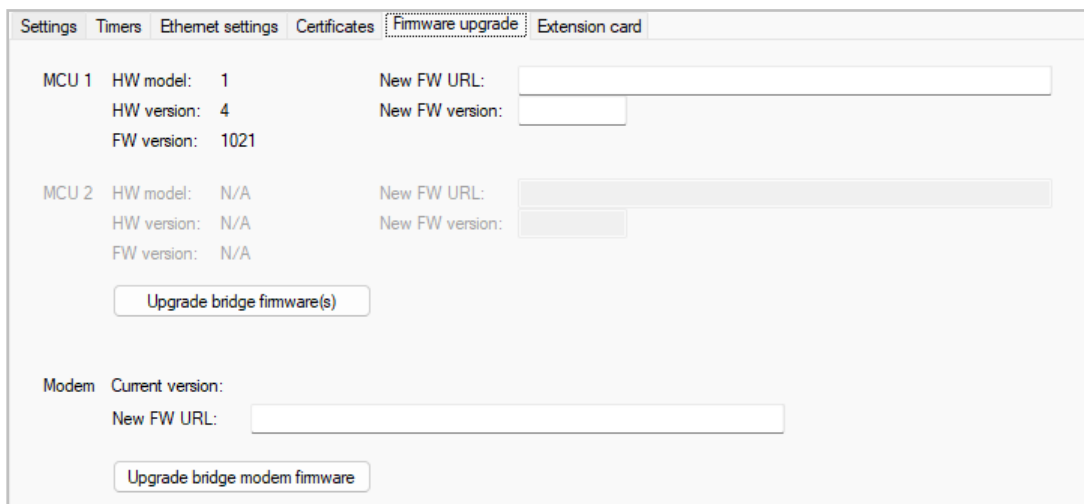


Figure 29. Gateway and modem firmware controls

2. Enter the gateway firmware URL under **New FW URL**.
3. Enter the firmware version under **New FW version**.
4. Confirm that the URL and version match the firmware intended for this device.
5. Click [**Upgrade bridge firmware(s)**].
6. Confirm that **FW version** shows the intended version.
7. Reconnect to the device and confirm that it is available for configuration.

Update gateway firmware from a local file

Use this procedure to upload firmware from your computer over USB-C. Have the firmware file and its version for this gateway available on your computer.

1. Connect to the gateway using [the USB-C connection procedure](#).
2. Open **Config Repeater / GW / Bridge > Bridge > Firmware upgrade > Local**.



The screenshot shows a web interface for updating gateway firmware from a local file. At the top, there are three tabs: 'Bridge', 'Bridge modem', and 'Local', with 'Local' being the active tab. Below the tabs, there are two columns of fields. The left column contains 'HW model: 1', 'HW version: 4', and 'FW version: 1030'. The right column contains 'New FW file:' followed by a text input field and a 'Browse' button, and 'New FW version:' followed by a text input field. At the bottom left, there is an 'Upgrade firmware' button.

Figure 30. Local firmware update over USB-C

3. Compare **HW model** and **HW version** with the firmware requirements.
4. Click [**Browse**] and select the firmware file on your computer.
5. Confirm that **New FW file** shows the selected file.
6. Enter the firmware version under **New FW version**.
7. Confirm that the file and version match the firmware intended for this gateway.
8. Click [**Upgrade firmware**].
9. Wait for the update to finish.
10. Reconnect using [the device connection procedure](#).
11. Open **Bridge > Firmware upgrade > Local**.
12. Confirm that **FW version** shows the new firmware version.



Keep the USB-C cable connected until the firmware update finishes.

Update modem firmware

Use this procedure only when the modem firmware needs an update. Obtain a valid modem firmware URL for this device before starting. For a remote update, arrange local recovery access before changing firmware.

1. Open **Config Repeater / GW / Bridge > Bridge > Firmware upgrade**.
2. See [the gateway and modem firmware controls](#).
3. Enter the modem firmware URL under the modem's **New FW URL** field.

4. Confirm that the URL is intended for the modem.
5. Click [**Upgrade bridge modem firmware**].
6. Confirm that **Current version** shows the intended modem firmware version.
7. Reconnect to the device and confirm that it is available for configuration.

Configure an installed extension card

Use these procedures only when the device has an extension card installed. The **Extension card** tab displays the detected card type.

Settings Timers Ethernet settings Certificates Firmware upgrade **Extension card**

Extension card: None

Version: 30.0, HW M3 V0

Read interval (s): 30

Pulse counter settings Modbus master settings mBus master settings

Pulse voltage: Not supported

Port 0:

Pulse length (ms):	Not supported
Pulse count:	Not supported
Pulse factor:	Not supported
Pulse pull-up:	Not supported

Port 1:

Pulse length (ms):	Not supported
Pulse count:	Not supported
Pulse factor:	Not supported
Pulse pull-up:	Not supported

Figure 31. The detected extension card and available settings tabs

1. Open **Config Repeater / GW / Bridge > Bridge > Extension card**.
2. Confirm that the displayed card type matches the installed card.
3. Follow the applicable procedure for the detected card type.

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.

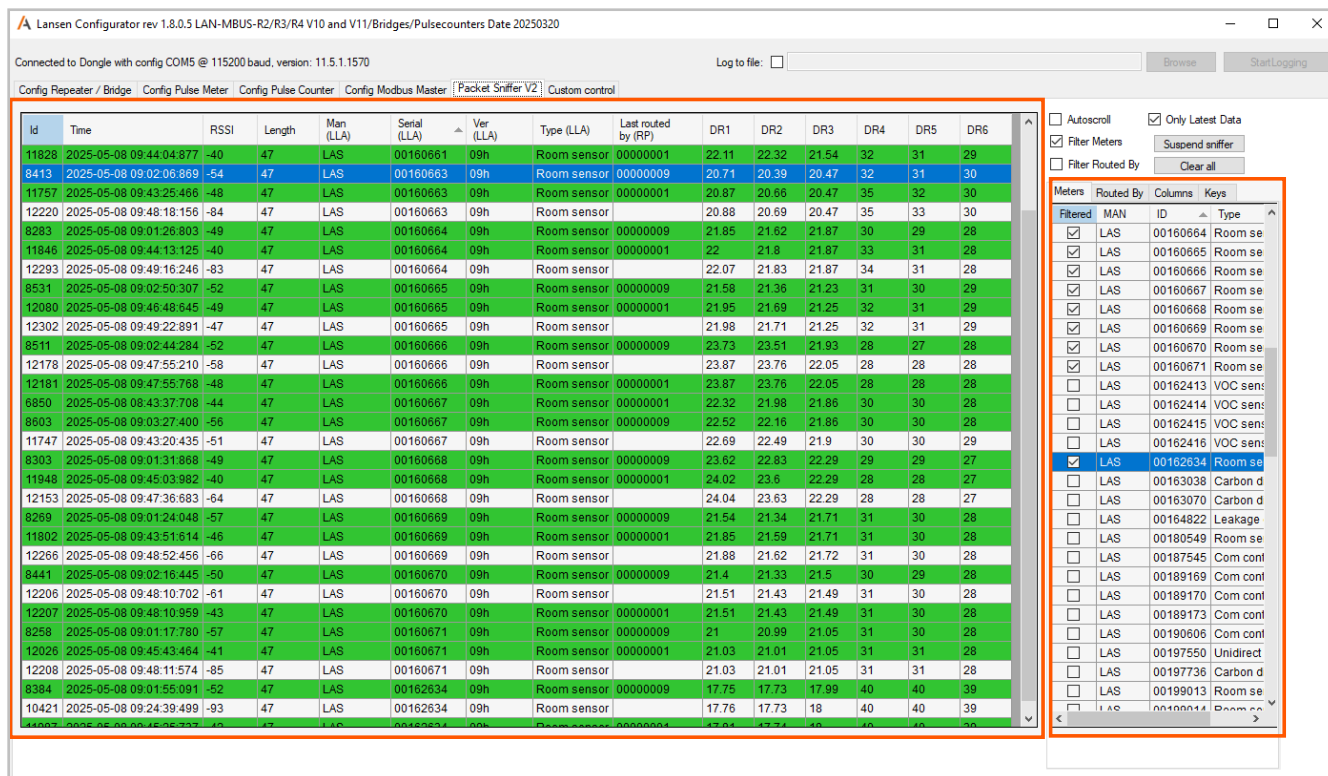


Figure 32. Packet Sniffer V2 with the Primary and Secondary lists highlighted.

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 3. 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.

Meters	Routed By	Columns	Keys
Filtered	MAN	ID ▲	Type ▲
☐	LAS	00190606	Com conf
☐	LAS	00197550	Unidirect
☐	LAS	00197736	Carbon d
☐	LAS	00199013	Room se

Figure 33. 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.

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.

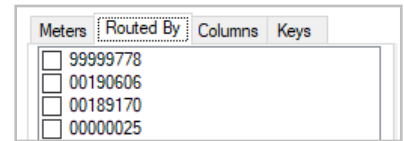


Figure 34. The **Routed by** tab

Columns

Use this tab to select which columns appear in the Primary list. Each available option is shown in Table 4. For more information about the DR1-31 alternatives, refer to the WMBUS data format guide for your product on www.lansen.io.

Table 4. 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.
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 <i>original transmitter</i> of this packet.
Acc	The access number of the <i>original transmitter</i> 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.

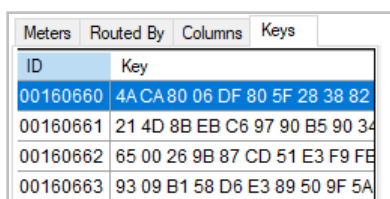
Column name	Meaning
Ver (ALA)	The version of the device to which the meter data of this packet belongs. Note: Only appears if the packet was sent with a long header in the CI-field.
Type (ALA)	The type of device to which the meter data of this packet belongs. Note: Only appears if the packet was sent 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 5 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 5. Description of the different values in columns **RP: Listen active reason**.

Bit	Meaning
0 (0x01)	Listen timer running
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.



Meters	Routed By	Columns	Keys
ID	Key		
00160660	4A CA 80 06 DF 80 5F 28 38 82		
00160661	21 4D 8B EB C6 97 90 B5 90 34		
00160662	65 00 26 9B 87 CD 51 E3 F9 FE		
00160663	93 09 B1 58 D6 E3 89 50 9F 5A		

Figure 35. The secondary 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;XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

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 36. 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.

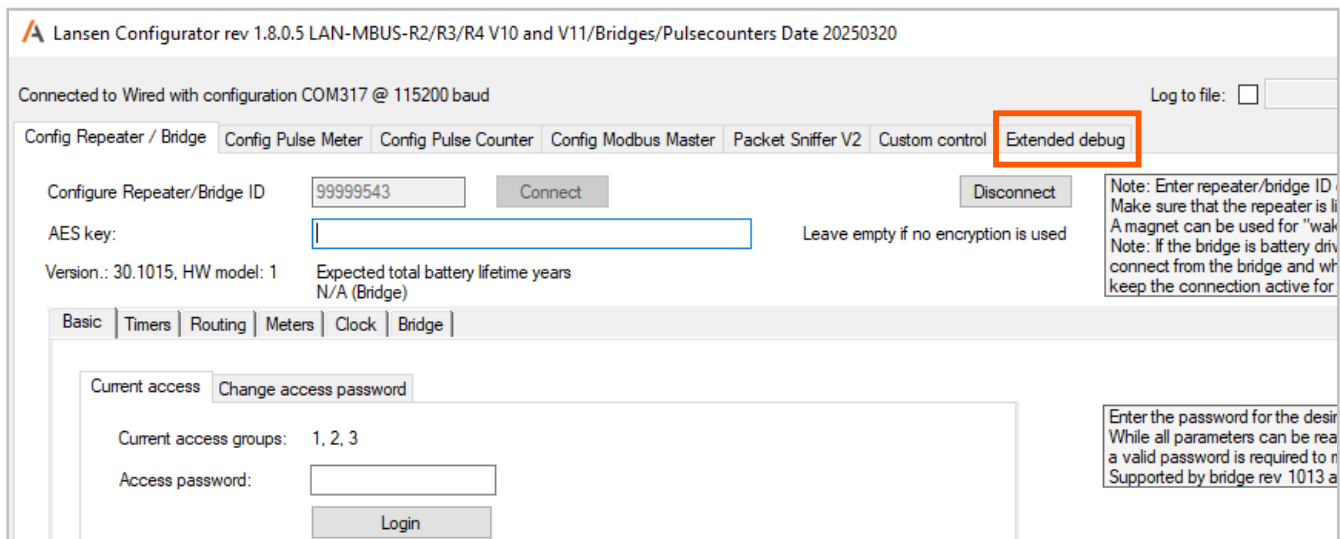
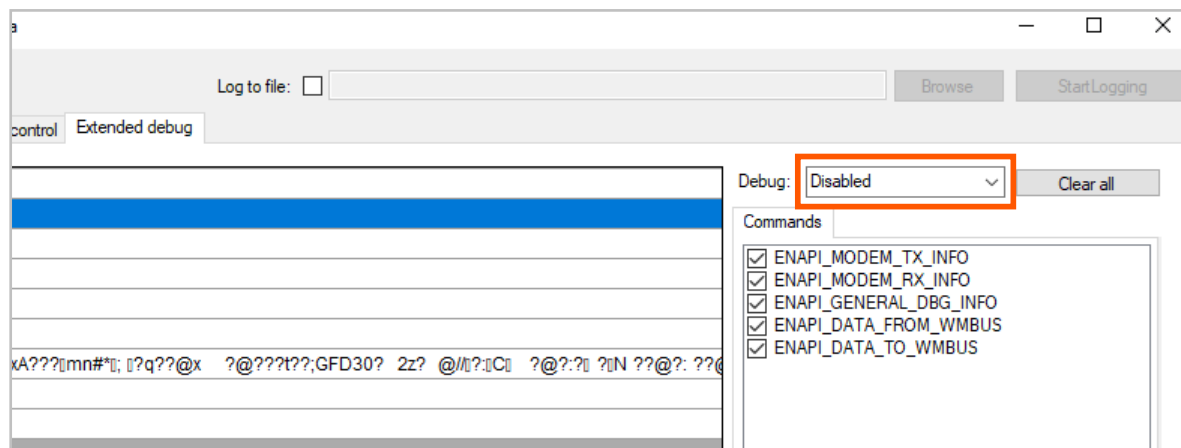


Figure 37. The **Extended debug** tab.

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.

Appendix A: Settings in the Gateway 5

This chapter explains all available settings in detail.

Basic tab

This tab contains basic settings, including **Encryption**, **MBUS mode**, and **Min install RSSI**.

Current access

Contains the access-password field, assigned access groups and login and logout buttons.

Current access groups

Shows the groups assigned to the active access password. These groups determine which settings you can change. The field shows **None** when no access password is active.

Access password

Enter one of the device's three eight-digit access passwords. The field hides the digits you enter.

[Login]

Starts a session with the entered access password and its assigned access groups. Log in again after 15 minutes of inactivity.

[Logout]

Ends the current access-password session. After logout, **Current access groups** shows **None**.

Change access password

Contains the controls for changing any of the three access passwords. Changing a password does not change its assigned access groups.

Old access password

Enter the current eight-digit password.

New access password

Enter the new eight-digit password.

Password selector

Select **Access password 1**, **Access password 2** or **Access password 3**. The selection determines which password the change applies to.

[Change]

Applies the new password to the selected access password.

See [the access password tasks](#) for login, password-change and logout instructions.



Encryption information

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. If meter data encryption is required, the end devices must be configured to use encryption.



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

Encryption

Select one of four encryption options. Enter the correct key in **AES key** to apply configuration changes.



Encryption: No encryption enabled ▼

Figure 38. The encryption drop-down menu with four options.

No encryption enabled

This option disables all encryption.

Leave the **AES key** field empty when you change parameters with encryption disabled. The device sends all settings over the air in plain text, where others can intercept them. Use this option only when other measures protect the communication.

Enabled for configuration

This option enables encryption for configuration by default.

Enter the correct key in the **AES key** field to apply parameter changes.

Enabled: OMS time sync

Select this option to enable encryption for OMS time synchronization.

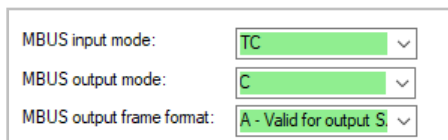
Select this option when you require encrypted time synchronization packets. The Gateway 5 sends these packets in the OMS time synchronization format.

Enabled: OMS time sync and configuration

This option combines **Enabled for configuration** and **Enabled: OMS time sync**.

MBUS mode

Use these settings to set the input and output communication formats of the Gateway 5.



MBUS input mode: TC ▼
 MBUS output mode: C ▼
 MBUS output frame format: A - Valid for output S ▼

Figure 39. The wM-Bus mode settings.

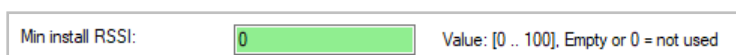
By default, the Gateway 5 accepts incoming data in C- and T-mode. You can set the output mode to S-, C-, or T-mode with frame format A or B. Recommended settings:

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

Follow [the S-mode switching task](#) to configure the Gateway 5 for S-mode.



If you use the LAN-WMBUS-D1/D2 dongle to configure the Gateway 5, complete other settings before selecting S-mode. In S-mode, configure the USB dongle to transmit in S-mode before you configure the Gateway 5. Contact Lansen for more information.



Min install RSSI: 0 Value: [0 .. 100]. Empty or 0 = not used

Min install RSSI

Set the minimum RSSI for a meter to enter the *internal routing list*. The Gateway 5 then retransmits only

meters with a good signal. 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, restart the Gateway 5 to update the internal routing list. Disconnect and reconnect the power, or click [**Restart**] under **Basic** in the Lansen Configurator.

Antenna gain:	Not supported
WMBUS antenna:	<div>Internal</div>
Modem antenna:	<div>Internal</div>

Antenna gain

Set this parameter to the gain of the external antenna. The Gateway 5 adjusts its output power to stay within legal transmission limits. This helps the device operate correctly with an external antenna.

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, select the lowest antenna gain that maintains a reliable connection. This helps conserve battery life.

wM-Bus antenna

Select the desired antenna configuration for wM-Bus communication.

Internal

Use the internal diversity antenna.

External (single)

Use a single external antenna.

External (dual diversity)

Use dual external antennas for diversity.

Modem antenna

Select the desired antenna configuration for cellular communication.

Internal

Use the internal antenna.

External

Use an external antenna.

Enabled sound indications

Select this checkbox to enable sound feedback from the buzzer.

Erase flash

Select **All** to erase all flash data, or select **Logs** to erase log data. Click [**Erase**] to erase the selected data.



Confirm the selected erase option before you click [**Erase**].

Timers tab

This tab contains timer-based parameters, such as listen/pause timers and suppression timers. Configure the Gateway 5 to wake on specific days, weeks, or dates. For example, select Mondays or the 15th of each month.

Listen timers | Global suppression timer | **Suppression timer indexes** | Device type suppression timers | Custom meter suppression timers

Start time schedule: ☐ 00:00 on ☒ Mo ☒ Tu ☒ We ☒ Th ☒ Fr ☒ Sa ☒ Su

Repeat start time schedule: Every week

Listen timers

Configure the wake-up schedule, for the Gateway 5 by selecting monthly, weekly, daily, or specific dates. Adjust the magnet/reed timer to set the listening duration after you apply a magnet.

Start time schedule: ☐ 07:31 on ☒ Mo ☒ Tu ☒ We ☒ Th ☒ Fr ☒ Sa ☒ Su

Repeat start time schedule: Every week

Figure 40. Start time scheduler

Start time schedule

Select this checkbox to activate the **Start time** parameter. Set when and how often the Gateway 5 listens by selecting weekdays, weeks, or specific dates. The schedule works with the *Interval* and *Listen/pause timers* settings.

Time field

Set the daily wake-up time in UTC. Set a time equal to or earlier than the selected interval. The Gateway 5 listens for the duration set under **Listen/pause timers**.

Active days

Select the days the Gateway 5 listens, and clear the other days. If you select **On certain dates** under **Repeat start time schedule**, select the dates to use. Selected dates also use the selected weekday restrictions. Follow [the selected-date scheduling task](#) to set listening and upload dates. 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 setting 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 between 10 min to 24 h. Select **Custom** to specify exact wake-up times in the [.ui]Listen/Pause timers# field.

Listen/pause timers

Set the listening and pause durations in minutes. For example, 30/1410 means 30 minutes of listening in a 24-hour period.

Magnet/Reed timer

The Gateway 5 then listens for wM-Bus and configuration packets for the set duration. Place a magnet on the left side of the front label to activate this timer.

Monthly reading start time

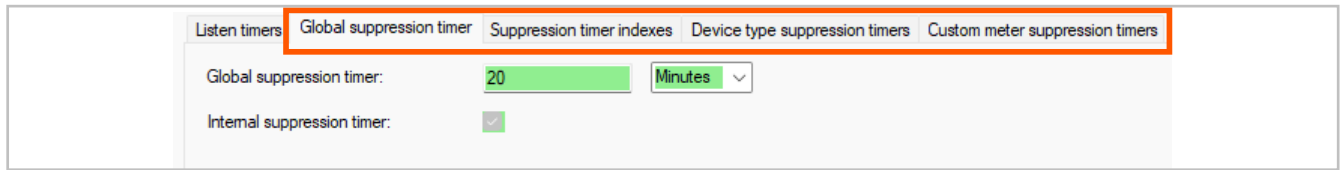
Set the date and time when the Gateway 5 wakes once a month. Use this setting when you need meter data at a specific time each month.

Monthly reading start time: ☒ 15:44 on the 10th of each month

Monthly reading listen time: 10 Minutes: [0 .. 65000]. 0 = Not used

Suppression timers

These settings reduce how often the Gateway 5 stores packets from each meter. You can set the time in minutes or hours and configure timers for each detected sensor, meter, or repeater.



Listen timers **Global suppression timer** Suppression timer indexes Device type suppression timers Custom meter suppression timers

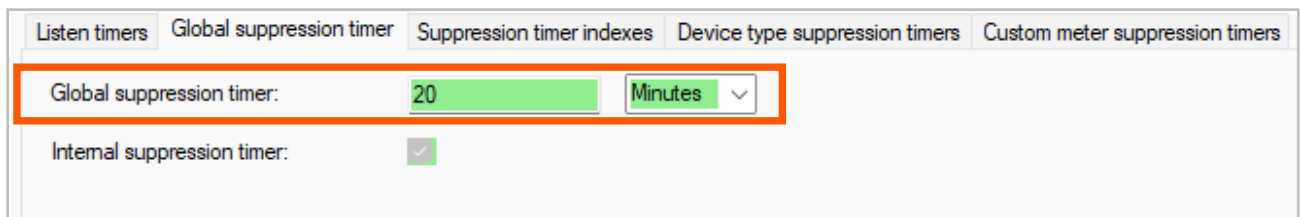
Global suppression timer: 20 Minutes

Internal suppression timer: ☒

Figure 41. The suppression timers are accessible through the suppression timer tabs.

Global suppression timer

This is the default setting unless you specify otherwise. The Gateway 5 sends only the latest meter data every 20 minutes, even if meters send data more frequently.



Listen timers **Global suppression timer** Suppression timer indexes Device type suppression timers Custom meter suppression timers

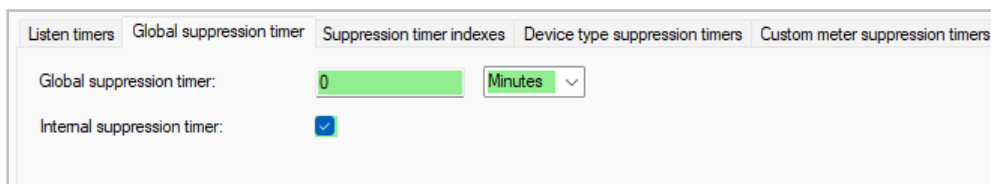
Global suppression timer: 20 Minutes

Internal suppression timer: ☒

Internal suppression timer

Activate or deactivate this timer only when the global suppression timer is 0. When activated, the internal suppression timer applies a 10-second delay.

Follow [the suppression timer task](#) to change or disable these timers.



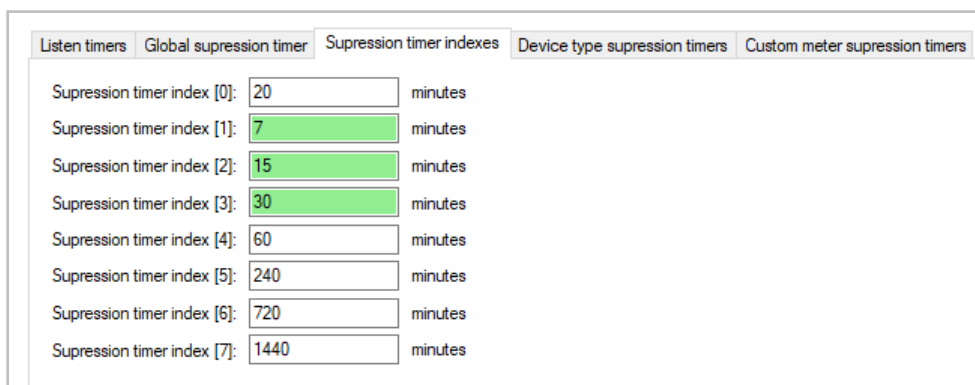
Listen timers **Global suppression timer** Suppression timer indexes Device type suppression timers Custom meter suppression timers

Global suppression timer: 0 Minutes

Internal suppression timer: ☒

Suppression timer indexes

View and create preconfigured timer indexes for meters or sensors. **Suppression timer index [0]** is the default **Global suppression timer**. Indexes 1-3 are configurable, and indexes 4-7 are predefined.



Listen timers **Global suppression timer** **Suppression timer indexes** Device type suppression timers Custom meter suppression timers

Suppression timer index [0]:	20	minutes
Suppression timer index [1]:	7	minutes
Suppression timer index [2]:	15	minutes
Suppression timer index [3]:	30	minutes
Suppression timer index [4]:	60	minutes
Suppression timer index [5]:	240	minutes
Suppression timer index [6]:	720	minutes
Suppression timer index [7]:	1440	minutes

Device type suppression timers

Assign specific device types to a suppression timer index. For example, you can assign Room Sensors a specific index to handle them differently from other device types.

Number of mappings

The total number of device type mappings currently configured.

[Load all]

Loads the stored device-type mappings.

Add new mapping

Contains the device type and timer index for a new mapping.

Device type

The device type for the new mapping. See [the device-type reference](#) for available device types.

Suppression timer index

The timer index assigned to the selected device type.

[Add]

Creates a mapping with the selected device type and timer index.

Follow [the device-type suppression task](#) to add a mapping.

Custom meter suppression timers

View and set suppression timers for individual meters or sensors. You can configure each device using its manufacturer code, serial number, device type, and version.

You can use *wildcards* for flexibility. For example, a manufacturer-code wildcard applies the timer to matching serial numbers, device types, and versions. The manufacturer code does not affect these matches.



Toggle the **Wildcard** checkbox to unlock the **Manufacturer code** or **serial number** parameter.

Routing tab

Use the Routing tab to filter by manufacturer ID. You can also route only OMS messages or all messages that the Gateway 5 detects.

Accept Manufacturer ID

Enable *manufacturer code filtering*. The Gateway 5 then stores packets only from meters with the specified

manufacturer code. This is useful in areas with meters from different companies. If all fields are empty, the Gateway 5 stores packets from all meters.

Accepted Manufactur IDs: Example: LAS

Route messages

Select the type of wM-Bus packets the Gateway 5 receives and stores. This helps ensure OMS compliance or accept 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.

Route messages:

Route only OMS messages

Meters tab

The settings and options in this tab concern the Gateway 5's *internal routing list*. You can view, add, and remove meters in this tab.

Automatic meter installation:

☒ YES

Automatic meter installation

Select this checkbox to add received meters automatically to the internal routing list. The list stores a maximum of 2000 unique entries.



If this setting is disabled and the *internal routing list* is empty, the Gateway 5 does not store meters. Add meters manually in this case. See [Routing list management](#).

Number of meters:

926

 1074 free slots

Load all meters

Number of meters

Display the number of meters in the internal routing list and the number of free slots.

[Load all meters]

Click to load all meters in the wireless routing list into the table. The list appears on the right side of the program.

Routing list management

To control which meters are stored, add them manually to the *internal routing list*. This process is called whitelisting.

	Manufacturer	Serial number	Device type	Version
Add meter data:	<input type="text"/>	<input type="text"/>	Wildcard <input type="button" value="v"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	Wildcard <input type="button" value="v"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	Wildcard <input type="button" value="v"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	Wildcard <input type="button" value="v"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	Wildcard <input type="button" value="v"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>	Wildcard <input type="button" value="v"/>	<input type="text"/>
<input type="button" value="Add meter(s)"/>				

Follow [the manual meter installation task](#).

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

To add multiple meters, import them from a CSV file.

Import meter data:	<input type="text"/>	Example CSV file: ManufacturerCode;IdentificationNumber;DeviceType;Version LAS;11111111;18;03 LAS;22222222;18;03
<input type="button" value="Browse"/> <input type="button" value="Import .csv file"/>		

Follow [the CSV meter import task](#). To delete a meter, remove it from the *internal routing list*.

Follow [the task for removing selected meters](#) or [the task for clearing the entire meter list](#).

Clock tab

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

Repeater clock (UTC)	2020-07-03 08:11:55
Clock diff (s):	0
<button>Sync clock with PC</button>	

Repeater clock (UTC)

Display the device's internal clock in UTC.

Clock diff (s)

Display the difference between the device and PC clocks, in seconds.

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, temperature-compensated onboard clock. It drifts less than 0.5 seconds per day.

Bridge tab

This tab contains settings for the internet connection and communication.

Select MQTT, FTP, or HTTP as the internet transport protocol. Enter the corresponding 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 use the LAN-WMBUS-D1/D2-TC dongle without an AES key, the program retrieves only 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.

The screenshot shows the 'Settings' tab of a configuration interface. It includes fields for Host (p), port (1), Transport type (MQTT), template (Wmbus), Username (L), Password (D), Topic prefix, Internet security (TLS off), APN, NTP (pool.ntp.org), HTTP authentication (Not supported), Always online (checked YES), GPRS enabled (Not supported), Modem version, Network interface (Modem), and Network interface policy (Not supported).

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*.



To enable HTTPS, select a TLS option in the **Internet security** drop-down menu. Then set the port to 443.



FTP and HTTP transport types are available only when the network interface is Modem.

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 (FTP only)

Use Format 3 when operating in an Diehl-based environment. This format follows the XML structure used by Diehl meters and systems. It is available only for FTP uploads.

Template 301 (HTTP only)

Use Format 3 when operating in an Elvaco-based environment. This format follows the CSV structure used by Elvaco meters and systems. It is available only for HTTP uploads.

See [Appendix C](#) 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 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.

HTTP POST Content type

Select the content type for HTTP POST requests.

application/octet-stream

Default content type.

multipart/formdata

Wraps the payload as form data (**multipart/form-data**) for web endpoints that expect file-upload fields.



Use **multipart/formdata** only if your server/API explicitly requires it. For most integrations, **application/octet-stream** is preferred because it sends the payload in a simpler raw format.

Always online

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



When you disable **Always online** and select FTP, the Gateway 5 uploads meter data 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.

Timers tab

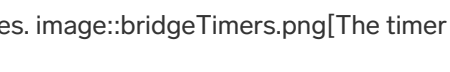
Upload time schedule

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



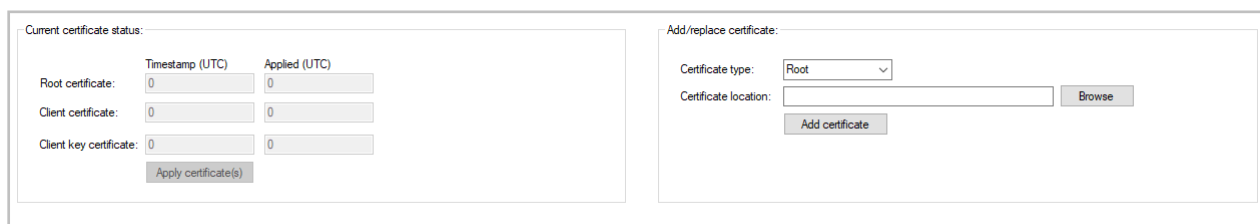
Do not set the modem upload time to the same value as the **Listen/pause timer**. Find this timer under [the Listen timers tab](#).

For battery operation, the upload time should follow the listening period.

See [the daily schedule example](#) for coordinated listening and upload times. [The timer settings under the Bridge-tab,width=635, pdfwidth=75iw]

The upload schedule uses both the selected dates and active weekdays. Follow [the selected-date scheduling task](#) to configure them. If the 1st falls on a weekend, the upload takes place on the next selected weekday.

Certificates tab



The screenshot shows the 'Certificates tab' interface. It is divided into two main sections: 'Current certificate status' and 'Add/replace certificate:'.
 The 'Current certificate status' section contains a table with two columns: 'Timestamp (UTC)' and 'Applied (UTC)'. There are three rows for 'Root certificate', 'Client certificate', and 'Client key certificate', each with input fields for both columns. Below the table is an 'Apply certificate(s)' button.
 The 'Add/replace certificate:' section contains a 'Certificate type' dropdown menu (set to 'Root'), a 'Certificate location' text input field with a 'Browse' button, and an 'Add certificate' button.

Figure 42. Overview of the Certificates tab

Upload certificates to the Gateway 5 from this tab.

Root

Select this certificate type to upload the root certificate.

Client Key

Select this certificate type to upload the client key.

Client

Select this certificate type to upload the client certificate.

Follow [the certificate upload task](#) to load certificates.



Clicking **Apply Changes** does not upload certificates. Click [**Apply certificate(s)**] to upload them.

Firmware upgrade tab

Settings Timers Ethernet settings Certificates **Firmware upgrade** Extension card

MCU 1 HW model: 1 New FW URL:
HW version: 4 New FW version:
FW version: 1021

MCU 2 HW model: N/A New FW URL:
HW version: N/A New FW version:
FW version: N/A

Modem Current version:
New FW URL:

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

New FW URL

The address of the gateway firmware file.

New FW version

The version of the firmware at that address.

[Upgrade bridge firmware(s)]

Starts the gateway firmware update from the specified URL.

Follow [the firmware URL update task](#) to update the gateway.

Local firmware update over USB-C

The **Local** tab lets you upload gateway firmware from a file on your computer. A USB-C connection is required for local firmware updates. The tab is under **Bridge > Firmware upgrade > Local**.

Bridge Bridge modem **Local**

HW model: 1 New FW file:
HW version: 4 New FW version:
FW version: 1030

Figure 43. Local firmware update controls

HW model

Shows the gateway's hardware model.

HW version

Shows the gateway's hardware version.

FW version

Shows the gateway's current firmware version.

New FW file

Shows the firmware file selected from your computer. Click [**Browse**] to select the file.

New FW version

Enter the version of the firmware in the selected file.

[Upgrade firmware]

Click to upload the file and update the gateway firmware over USB-C.

Keep the USB-C cable connected until the firmware update finishes. Follow [the local firmware update procedure](#) for the complete task.

Extension card tab

An installed *extension card* adds configuration options to the tab. The device detects the card type automatically.

The screenshot shows the 'Extension card' tab selected in a configuration menu. The main settings area displays: 'Extension card: None', 'Version: 30.0, HW M3 V0', and 'Read interval (s): 30' (with a green input field). Below this, there are three sub-tabs: 'Pulse counter settings', 'Modbus master settings', and 'mBus master settings'. The 'Pulse counter settings' sub-tab is active, showing two columns for 'Port 0' and 'Port 1'. Each column contains four settings: 'Pulse length (ms): Not supported', 'Pulse count: Not supported', 'Pulse factor: Not supported', and 'Pulse pull-up: Not supported'.

Figure 44. The **Extension card** tab

Extension card

Display the detected card type.

Version

Shows the extension card's firmware version and hardware version, for example, 30.0, HW M3 V0.



These settings are only configurable when an extension card is installed.

M-Bus master settings

Basic | Timers | Routing | Meters | **Click** | Bridge | Moty

Settings | Timers | Ethernet settings | Certificates | Firmware upgrade | Extension card

Extension card: mBus

Read interval (s): 30

Note: This field indicates the extension card installed on the bridge - Pulse Counter, Modbus, or M-Bus. The Read interval determines the polling frequency for that card.

Pulse counter settings | Modbus master settings | **mBus master settings**

Number of meters: 1704 296 free slots

Load all meters

Read all meters that are in the routing list of the repeater

Search control: Stop search | Running | Refresh status

Wired response time: 1 [0..255] seconds

Current measurement: 1163 uA

Refresh measurement

Wired mBUS meters:

Selected	Index	MAN	ID	Type	Version	Baudrate
☒	0	N_\	00000100	46	00h	68
☐	1	B@D	09888888	122	1Bh	205
☐	2	H@@	65322F2F	Other	00h	114
☐	3		006501B2	Com controller	00h	251
☐	4	VH@	B1001BFB	251	01h	27
☐	5	HXB	00B096C2	Other	00h	0
☐	6	WNJ	0002003A	Other	00h	45
☐	7	LAS	02000482	Room sensor	07h	122
☐	8		022F2F20	58	65h	8
☐	9	RSE	65018208	Heat Cost Al.	62h	2
☐	10	E@Z	1AFB4201	Oil	90h	130
☐	11	FWJ	00C50183	Other	00h	0
☐	12	7CJ	00000000	Other	00h	25

This is the list of all wired mBUS meters currently in the repeater.

Removes selected meters from the routing list.

Delete selected

Remove all meters from the routing list and all data.

Note. The complete clear of memory takes about 60-120 seconds. Be patient.

Delete all

Figure 45. The M-Bus master settings.

Number of meters

Display the number of configured M-Bus meters. The maximum number of M-Bus meters that can be stored is 2000. Click [**Load all meters**] to load all wired meters into the table.

Search control

Manage the search for M-Bus meters. Click [**Start search**] to start searching for M-Bus meters. Click [**Stop search**] to stop searching for M-Bus meters. Click [**Refresh status**] to refresh the search status.



If the M-Bus line consumes more than 6mA the search will be stopped.

Wired response time

Set the response time for wired M-Bus communication. Choose a value between 0 and 255 s. 0 disables reading of the bus.

Current measurement

Display the load in uA (microamperes) on the M-Bus line. Click [**Refresh current measurement**] to update the measurement.

The wired meters routing list

The wired M-Bus routing list is separate from the wireless routing list in the Meters tab. Each list can store up to 2000 meters, allowing the repeater to store up to 4000 meters in total.

Wired mBUS meters

Display all wired M-Bus meters currently stored in the repeater.

The table shows each meter's index, manufacturer ID (MAN), ID, type, version, baud rate, and status. Click [**Delete selected**] to remove selected meters from the routing list or click [**Delete all**] to remove all meters from the routing list and all associated data. The complete memory clear takes about 60 to 120 seconds.

Appendix B: 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 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 1. 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		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	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

Byte No.	Field Name	Content	Info	Byte data
16	Manufacturer	Manufacturer code (LSB)	LAS	0x33
17	Manufacturer	Manufacturer code (MSB)		0x30
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 2. 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

Byte No.	Field Name	Content	Info	Byte data
13	Status	Errors and alerts		0x00
14	Configuration		Example: Encryption off	0x00
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 C: Upload templates

Template 101

Supported in Gateway 5 firmware version 1022 and above.

File name

Format

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

Example 3. File name

```
GTW_000000189170_OMS_RAW_20250430_160120.csv
```

File content

Format (Comma-separated values)

```
METER_ADDRESS,READING_DATE,RAW_TELEGRAM  
<meter-address>,<datetime>,<mbus_raw_data>
```

Example 4. File content

```
METER_ADDRESS,READING_DATE,RAW_TELEGRAM  
20705566,16:01:20  
30/04/2025,314497266655702041078C20997A20002025F30D72254FF5A9F1D3BF646381A895B8412  
55D5A03DBA43B026CB29589EB27B8
```

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

Supported in Gateway 5 firmware version 1022 and above.

File name

Format

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

Example 6. File name

```
0016010439_46159225_valuereport_20200423000656_2103.csv
```

File content

Format

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

Example 7. File content

```
0000000161;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 (FTP only)

Supported in Gateway 5 firmware version 1023 and above.

File name

Format

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

Example 9. File name

```
LAS00189170_1772629491.xml
```

File content

Format

```
<?xml version="1.0" encoding="UTF-8"?>
<hyTertiary version="1.3" xmlns="http://www.diehl-metering.com/">
  <info source="LAS<gateway_serial_number>" target="EDM" subtype="MDP"
time="<timestamp>">
    <identification>
      <identificationAddress>LAS<gateway_serial_number></identificationAddress>
      <deviceType>49</deviceType>
      <typeDescription>Lansen Gateway</typeDescription>
      <customizedName>GW5</customizedName>
      <hardwareVersion><gateway_model_version></hardwareVersion>
      <softwareVersion><gateway_software_version></softwareVersion>
      <serialNumber><gateway_serial_number></serialNumber>
    </identification>
  </info>
  <mdp version="1.2">
    <recData>
      <md deviceId="<meter_serial_number>" time="<timestamp>" moduleId="1"
rsi="<meter_rssi>">
        <ra><meter_raw_data></ra>
      </md>
    </recData>
  </mdp>
</hyTertiary>
```

Example 10. File 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>54443330512724000B327A1A0000402F2F04FD3A1A0100008240FD3A6E0002FD0F0D02818040FD
3A0084C040FD3A0000000042FD3A00008201FD3A0000C101FD3A7F8202FD3AFFFF066D320CC0010100
02FD46C70D</ra>
      </md>
    </recData>
  </mdp>
</hyTertiary>

```

Template 301 (HTTP only)

Supported in Gateway 5 firmware version 1028 and above.

File name

Format

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

Example 11. File name

```
000016010439_valuereport_20200423000656_3102.csv
```

File content

Format (Semicolon-separated values)

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

Example 12. File content

```
0000000161;05047168;2009-12-17  
00:00:00;00;08147268710405ac484103470000000c1480769604046dba092e1a426c
```



- The raw data shall be wired M-Bus data format.
- M-Bus raw data starts with the M-Bus C-field.
- Stop character and checksum are excluded.

Example 13. 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 401 (FTP only)

Supported in Gateway 5 firmware version 1029 and above.

File name

Format

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

Example 14. File name

```
LAS00189170_1772629491.xml
```

Format

```
<?xml version="1.0" encoding="UTF-8"?>
<hyTertiary version="1.2" xmlns="http://www.diehl-metering.com/">
  <info source="LAS<gateway_serial_number>" time="<timestamp>" subtype="MDP">
    <identification>
      <identificationAddress>LAS<gateway_serial_number></identificationAddress>
      <deviceType>49</deviceType>
      <typeDescription>Lansen Gateway</typeDescription>
      <customizedName>GW5</customizedName>
      <hardwareVersion><gateway_model_version></hardwareVersion>
      <softwareVersion><gateway_software_version></softwareVersion>
      <serialNumber><gateway_serial_number></serialNumber>
    </identification>
  </info>
  <mdp version="1.2">
    <recData>
      <md time="<timestamp>" rssi="<meter_rssi>">
        <ra><meter_raw_data></ra>
      </md>
    </recData>
  </mdp>
</hyTertiary>
```

Example 15. File content

```
<?xml version="1.0" encoding="UTF-8"?>
<hyTertiary version="1.2"
  xmlns="http://www.diehl-metering.com/">
  <info source="LAS00189170" time="1791792549" subtype="MDP">
    <identification>
```

```

        <identificationAddress>LAS00189170</identificationAddress>
        <deviceType>49</deviceType>
        <typeDescription>Lansen Gateway</typeDescription>
        <customizedName>GW5</customizedName>
        <hardwareVersion>2</hardwareVersion>
        <softwareVersion>1030</softwareVersion>
        <serialNumber>00189170</serialNumber>
    </identification>
</info>
<mdp version="1.2">
    <recData>
        <md time="1791792549" rssi="-79">

<ra>C4443330012322001E317A2F0000C02F2F04FD3A196C04008240FD3A060002FD0F0604818040FD
3A0184C040FD3AFFFFFFF7F42FD3A01008201FD3A0000C101FD3A7F8202FD3AFFFF066D0909284C3A00
02FD468813CD02FD3A01008D03FD3A010001FD718D01FD0C0101FD0D02022334000424B0F544008440
249E604500C103FD3A7F8204FD3AFFFC204FD3A0F008205FD3A2600C405FD3AFFFFFFFFF8106FD3A01
C406FD3AFFFFFFFFF8107FD3A01C107FD3A008208FD3A0000C108FD3A018209FD3A0700</ra>

        </md>
    </recData>
</mdp>
</hyTertiary>

```

Index

A

Access passwords, [15](#)
 Access groups, [15](#)
 Change, [15](#)
 Login, [15](#)
 Logout, [16](#)
 Antenna gain, [48](#)
 AT commands, [44](#)

B

Bridge tab, [54](#)

C

Cable inlet, [4](#)
 COM-port, [13](#)
 Commissioning, [8](#)
 Configuration
 Packets, [61](#)
 CSV
 file, [44](#)

E

ENAPI
 Commands, [39](#)
 Data, [63](#)
 Extension card, [59](#)

F

Firmware
 Gateway update, [37](#)
 Modem update, [38](#)
 FTP
 Address, [54](#)
 Upload setup, [22](#)
 Upload verification, [23](#)

H

HTTP
 Upload setup, [23](#)
 Upload verification, [25](#)
 HTTPS
 Address, [54](#)

I

Internal routing list, [5](#), [47](#)

L

Listen timers, [49](#)
 Active days, [49](#)
 Interval, [49](#)
 Listen/Pause timers, [49](#)
 Magnet/Reed timer, [49](#)

Repeat start time schedule, [49](#)
 Start time schedule, [49](#)
 Time field, [49](#)

M

M-Bus
 Wired meter collection, [30](#)
 Magnet/Reed timer, [5](#)
 Main PCB, [4](#)
 Maintenance, [36](#)
 Manufacturer code filtering, [51](#)
 MBUS mode, [47](#)
 Meter collection, [25](#)
 Modem antenna, [48](#)
 Monthly reading start time, [49](#)
 MQTT
 Address, [54](#)
 Server, [5](#), [13](#)
 Topic, [61](#)
 Upload setup, [19](#)
 Upload verification, [21](#)

N

Non-Disclosure Agreement
 NDA, [63](#)

P

Packet Sniffer V2, [39](#)
 PCB cover, [4](#)

R

Remote maintenance, [9](#)
 Routing tab, [51](#)

S

S-mode, [47](#)
 Scheduling, [31](#)
 SMA connector, [4](#)
 Suppression timer, [50](#)
 Device type, [50](#)
 Global, [50](#)
 Index, [50](#)
 Internal, [50](#)

T

Template
 Template 101, [55](#), [64](#)
 Template 201, [55](#), [65](#)
 Template 301 FTP, [56](#), [66](#)
 Template 301 HTTP, [56](#), [68](#)
 Template 401 FTP, [69](#)
 Timers, [57](#)
 Timers tab, [48](#)

TLS, [56](#)

Top cover, [3](#), [5](#)

U

USB-C, [11](#)

W

Whitelisting, [52](#)

Wildcards, [51](#)

wM-Bus antenna, [48](#)

Copyright and Legal Disclaimer

© 2026 by Lansen Systems AB

This document contains proprietary information belonging to Lansen Systems AB. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Lansen Systems AB.

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.