

Manual

NB1 Gateway SWAN2-R

Part 1: Hardware and commissioning



Created by
WEPTech elektronik GmbH
Maria-Goeppert-Mayer 4
76829 Landau

Revision history

Item number:		A001-0119-001 / A001-0134-001	
Revision	Date	Description	Author
1.0	30.05.2023	Initial release for A001-0119-001 and A001-0134-001	MW3/RW/GZ
1.1	12.12.2023	Changes to chapter 4 for delivery in mode „SM“	HH3
1.2	16.01.2024	Revision for delivery in shipping mode	GZ

Contents

1	General information	4
1.1	Identification of the manufacturer	4
1.2	Identification of the product	4
1.3	Scope of delivery	4
1.4	Validity	4
2	Safety	5
2.1	Signal words and graphic symbols	5
2.1.1	Signal words & warnings	5
2.1.2	Hints in this user manual	6
2.1.3	Structure of warning notices	6
2.1.4	Symbols	6
2.2	Intended use	7
2.3	Precautionary handling	7
2.4	Predictable misapplication	7
2.5	General safety instructions	8
	Even if the device is handled safely and foreseeable misuse is avoided, there may still be functional hazards for the user or third parties when handling the device, or the device and other property may be damaged.	8
2.5.1	Risk of injury	8
2.5.2	Risk of material damage	8
2.6	Qualification of personnel	9
2.7	Storage of the user manual	9
3	Product information	10
3.1	Product features	10
3.2	Technical features	11
3.2.1	Technical data	11
3.2.2	Used radio frequencies and bands	13
3.3	Type plate	14
3.4	View on electronics	15
3.5	Technical drawing	16
3.6	Transportation	16
3.7	Storage	16
4	Initial commissioning & mounting	17
4.1	Opening the housing	17

4.2	Inserting the SIM card.....	17
4.3	Turning the device on	18
4.4	Closing the device	18
4.5	Mounting of the device.....	19
5	Troubleshooting during commissioning.....	21
5.1	Error: No reaction of the device when the jumper is plugged in	21
5.2	Error: Battery error during self-test.....	21
5.3	Error: Other self-test errors.....	22
5.4	Errors that cannot be resolved	22
6	Maintenance	23
6.1	Maintenance	23
6.2	Battery replacement	23
6.2.1	Suitable battery types.....	23
6.2.2	Replacing the batteries	23
6.3	Cleaning	28
7	Guidelines, laws and standards	29
7.1	Declaration of Conformity.....	29
8	Supporting documents	30
9	Disposal.....	30
10	Copyright protection	31
11	Warranty information	31
12	Disclaimer	31
13	Restriction of use	32

List of Tables

Table 1: Product features.....	11
Table 2: Technical data.....	13
Table 3: Used radio frequencies.....	13
Table 4: Content of nameplate	14

List of Figures

Figure 1: View on electronics	15
Figure 2: Technical drawing of housing.....	16

Figure 3: Device orientation 20

1 General information

1.1 Identification of the manufacturer

Manufacturer	WEPTECH elektronik GmbH		
Address	Maria-Goeppert-Mayer-Straße 4		
	D-76829 Landau		
	Tel: +49 6341 9255-0		Fax: +49 6341 9255-100
	https://www.weptech.de		info@weptech.de

1.2 Identification of the product

Device	Series	Article number
NB1 Gateway SWAN2 wMBus	• SWAN2-R	• A001-0119-001
NB1 Gateway SWAN2 wMBus for Maddalena S.p.A.	• SWAN2-R	• A001-0134-001

1.3 Scope of delivery

- NB1 Gateway SWAN2 wM-Bus, removable battery (SWAN2-R, A001-0119-001 or SWAN2-R for Maddalena S.p.A., A001-0134-001) pre-assembled in housing
- 2x lithium battery type Fanso ER26500M (preinstalled)
- Housing incl. 1 rubber seal and 6 x M2 -16 screws
- 1x jumper (preinstalled)
- Quick Start Guide

1.4 Validity

This user manual applies exclusively to the products specified in section 1.

The operating instructions consist of two parts:

1. This part 1 describes the hardware, installation and commissioning of the device for each variant.
2. Part 2 of the manual [1] explains the configuration of the device independently of the variant.

This manual in English is a direct translation of the German manual for this device. For this reason, this manual is based on German laws and regulations.



Hint

The latest version of these operating instructions can be found on our website under the corresponding product.

<https://www.weptech.de/en/>

2 Safety

The user manual is an integral part of the product and must be read carefully before use. Keep this user manual and all other applicable documents in a safe place so that they are always available when required.

2.1 Signal words and graphic symbols

This user manual contains warnings and symbols, which are explained in the following chapters.

Warnings are intended to warn of residual dangers and exist in three levels. The classification of the warnings depends on the severity of the damage that can occur if the warnings are ignored and the recommended actions are not followed.

2.1.1 Signal words & warnings

Warnings are introduced with one of the following signal words and marked with a corresponding signal color.



Danger

Indicates a hazard with a high degree of risk, an imminently hazardous situation which, if not avoided, will result in death or serious injury.

Imminent danger resulting in serious bodily injury or death.



Warning

Indicates a hazard with a medium degree of risk, an imminently hazardous situation which, if not avoided, will result in death or serious injury.

Potentially hazardous situation that could result in serious bodily injury or death.



Caution

Indicates a hazard with a low degree of risk, an imminently hazardous situation which, if not avoided, will result in death or serious injury.

Potentially dangerous situation that could result in minor bodily injury.

Attention

Identifies specific warnings, notices, or comments of special interest that relate to hazards where physical injury is not a reasonable possibility.

Situation that may result in possible property damage to the product.

2.1.2 Hints in this user manual

The following symbols are used in this manual to emphasize important information:

Hint

Indicates usage tips and particularly useful information about the product.

2.1.3 Structure of warning notices

Warning

The first line describes the type and source of the hazard.

The second line describes the consequences if no security measures are taken.

- ✓ The last line describes measures to prevent hazards.

Example:

Caution

Risk of injury due to disregard of the safety symbols.

Failure to observe the warnings in the user manual can lead to injuries and further hazards.

- ✓ Pay attention to the warnings in the user manual.

2.1.4 Symbols

Symbol	Meaning	Symbol	Meaning
	General warning		Warning of electrical voltage

	Warning of hazards due to battery charging		Warning of flammable substances
	Follow user manual		Observe general advice
	Warning of electrostatic hazard, may cause serious damage to the product		General note / information

2.2 Intended use

The SWAN2 is used to collect WM-Bus meter telegrams and send the collected telegram data to a configured server via the mobile network. The product may only be used as intended; any kind of misuse is not permitted. Intended use also includes compliance with all the information in these instructions. Any use beyond the intended use or any other use is considered misuse.

The product must not be modified in any way without the written permission of WEPTech elektronik GmbH. Unauthorized modifications to the product can lead to malfunctions and are prohibited for safety reasons.



Warning

Misuse of the device can lead to dangerous situations.

- ✓ Only use the device for its intended purpose.

2.3 Precautionary handling

The product was built in accordance with the state of the art and recognized safety regulations. Nevertheless, its use may result in functional hazards for the user or third parties or damage to the device and other material assets.

Only use the product when it is in perfect working order and in accordance with its intended use, safety and hazard awareness, and in compliance with the operating instructions. In particular, faults that impair safety must be rectified immediately.

2.4 Predictable misapplication

Reasonably predictable misapplications that may involve hazards for the user, third parties or for the SWAN2 are:

- ✓ Using the SWAN2 and accessories other than for their intended purpose.
- ✓ Operating the SWAN2 in a way that is contrary to the instructions in the user manual with regard to safety instructions, installation, operation, maintenance and servicing.
- ✓ Operating the SWAN2 with obvious malfunctions.

2.5 General safety instructions

Even if the device is handled safely and foreseeable misuse is avoided, there may still be functional hazards for the user or third parties when handling the device, or the device and other property may be damaged.



Warning

Failure to follow the safety instructions may result in fire, electric shock and other injury or damage to the instrument and other property. (The housing is made of plastic with sensitive electronic components and batteries inside).

2.5.1 Risk of injury



Risk of explosion

Live parts of the product can generate electrical sparks even at low voltages (e.g. when opening and closing electrical circuits) and act as ignition sources. In potentially explosive atmospheres, this can trigger an explosion that can injure individuals.

- ✓ Do not use the device in potentially explosive areas.



Battery

Please be sure to follow these instructions for handling lithium batteries:

- ✓ Do not expose the battery to fire or moisture!
- ✓ Do not attempt to charge the lithium battery!
- ✓ Do not pierce, break, crush or cut the device or the battery! Do not disassemble the battery!
- ✓ Do not short-circuit the battery contacts!
- ✓ Never operate batteries outside the designated product specification!

2.5.2 Risk of material damage



Electrostatic discharge

The highly sensitive electronic components can be damaged by electrostatic discharge or overvoltage. Damaged devices may no longer function correctly or at all.

- ✓ Do not mount the device in rooms with electrostatic charge.
- ✓ Do not touch electronic components without ESD clothing.
- ✓ Wear ESD clothing and footwear.
- ✓ Only use suitable tools.



Heavy vibrations

Heavy vibrations can damage mechanical and electronic components of the device. Damaged devices may no longer function correctly or at all.

- ✓ Do not drop the device on the floor, hard surfaces or hard objects.



Liquids

Water and other liquids can damage the electronic components of the device. Damaged devices may no longer function correctly or at all.

- ✓ Protect the electronic components from water and other liquids.



Climatic Effects

Climatic effects such as heat, cold and moisture can damage the device. Damaged devices may no longer function correctly or not at all.

- ✓ Observe the maximum/minimum permitted temperatures and the information on humidity during operation. See part 1 of the user manual of the respective device variant for this information.

2.6 Qualification of personnel

The device may only be transported, unpacked, assembled, operated, maintained, disposed of and otherwise used by suitable, qualified, instructed and authorized personnel.

2.7 Storage of the user manual

The user manual is an integral part of the product and must be read carefully before use and be available at all times.

Keep these operating instructions and all other applicable documents in a safe place so that they are available when required.



Attention

Read carefully before use.

Keep for future reference.

3 Product information

The SWAN2 is a gateway that connects wireless M-Bus devices to the cellular network using LTE Cat-NB1 technology.

The wireless M-Bus interface (radio standard according to DIN EN 13757-4) operates at 868 MHz and supports the modes S, T and C as well as the frame formats A and B. On the mobile side, the gateway supports LTE bands 3, 8 and 20 as well as the UDP, HTTP/S and LwM2M protocols.

The device is configured via an NFC interface. The configuration can also be performed remotely when using the HTTP/S and LwM2M protocols. Details regarding the configuration can be found in part 2 of the user manual [1].

At configurable intervals, the gateway will switch to receive mode, store the incoming wireless M-Bus meter telegrams in a non-volatile memory, and either subsequently, or at configurable times, send the data via LTE Cat-NB1 mobile radio to the configured server.



Hint

A customized variant of the gateway can also be manufactured on request. In addition to pre-configuring the device straight from the factory, it is also possible to equip the gateway with a SIM card or eSIM provided by the customer and to customize the label on the housing. In addition to all parameters that can be configured via NFC, such a pre-configuration can also include further adjustments, e.g. reset-proof device-specific NFC default passwords. Requests in this regard can be sent to sales@weptech.de.

3.1 Product features

Some functions of the device are listed below.

Device properties
Data reception via wireless M-Bus (868 MHz)
Useable in wM-Bus-Modes S, T and C
Collects data from up to 250 wM-Bus devices
Whitelisting (define wM-Bus devices that should be received)
Configurable schedule for data collection and data transmission
Data transmission via LTE Cat. NB IoT technology (Band 3, 8 & 20)
Supported protocols: UDP, HTTP/S und LwM2M
3GPP licensed
Micro SIM (3FF)
Power supply: Batteries (Up to 10 years battery life)
Configuration and firmware update over NFC-Android-App or remotely (HTTP/S, LwM2M)

Protection class IP67

Replaceable batteries for extended product life

Table 1: Product features

3.2 Technical features

3.2.1 Technical data

Technical data		
General		
	Type	SWAN2-R
	Order name	NB1 Gateway SWAN2 wM-Bus removable battery
	Item number	A001-0119-01 / A001-0134-001
Metering		
	Wireless M-Bus	S1, C1/T1 Mode
	RX frequencies	868.3 MHz, 868.95 MHz
	Standard	DIN EN 13757-4
	Configuration	Configurable data reception and transmission
Mobile communications		
	LTE networks	Cat-NB1, Cat-M1
	LTE bands	B3, B8, B20
	TX power	≤23 dBm
	Typical Range	Typical Range Network dependent
	SIM card	SIM card 3FF (Micro SIM)
Antenna		
	Internal type	Multiband PCB antenna for Mobile Radio
	Internal type	Multiband wire antenna for metering
	Internal type	PCB antenna for NFC configuration
Supply		
	Type	Lithium metal batteries
	Voltage	3,6 V
	Capacity	2 x 6000 mAh *
	Connection	replaceable
	Lithium content	2 x 1,6 g *
		* type-specific, values apply to the batteries shipped with the device

Technical data		
Housing		
	Dimensions	approx. 150 x 110 x 40 mm
	Material / Color	Polycarbonate (ASA) / White
	Weight	approx. 300 g
	Protection class	IP67
Environmental conditions		
Be sure to follow!	Rel. humidity	0...95 % (non-condensing)
	Operating temperature	-20 °C to 55 °C
	Storage temperature	-20 °C to 30 °C
	Installation height	≤2000 m (above sea level)

Table 2: Technical data

3.2.2 Used radio frequencies and bands

Harmonized radio bands used by the gateway, max. occupied bandwidths (BW) and transmission powers (TX Power). Unless otherwise indicated, the specified frequencies are used for both the transmit (TX, UL) and receive (RX, DL) directions.

Band	Modulation	BW <i>kHz</i>	Frequency <i>MHz</i>	TX Power <i>dBm</i>
M	FSK	600	868.3 (S-Mode)	Only RX
N	FSK	500	868.95 (T-Mode)	Only RX
N	FSK	500	868.95 (C-Mode)	Only RX
Band 8	Cat-NB1	200	UL: 880...915 DL: 925...960	23
Band 20	Cat-NB1	200	UL: 832...862 DL: 791...821	23
Band 3	Cat-NB1	200	UL: 1710...1785 DL: 1805...1880	23

Table 3: Used radio frequencies

3.3 Type plate



1	Company logo & manufacturer
2	Product name
3	Item number
4	IMEI / product serial number
5	Manufacturer address
6	QR Code (serial number and configuration LTE modem)
7	Housing protection type
8	Read user manual
9	CE marking
10	Disposal instructions (WEEE directive)

Table 4: Content of nameplate

3.4 View on electronics

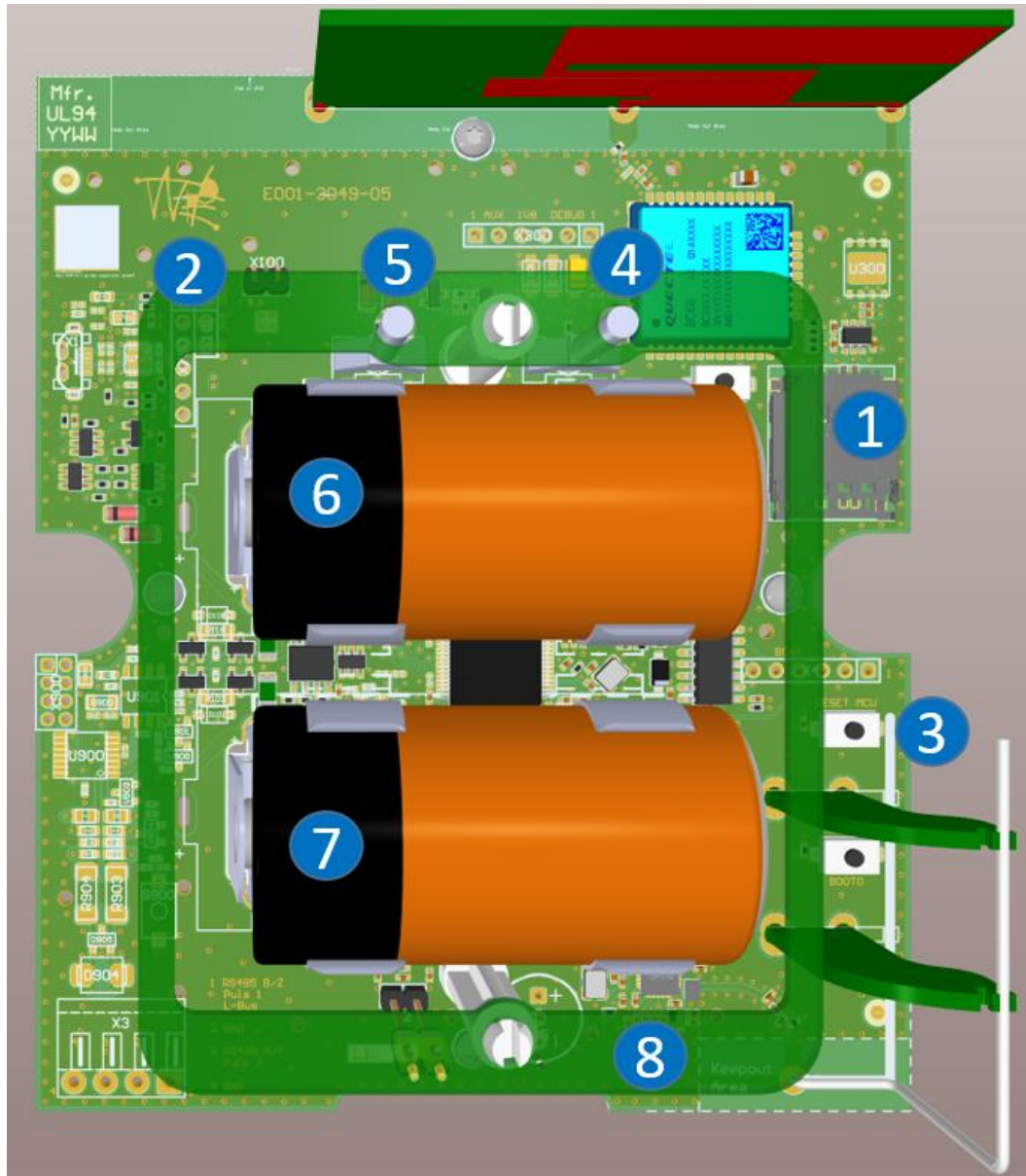


Figure 1: View on electronics

Device			
1	SIM cardholder	2	Jumper
3	Reset-Button Microcontroller	4	LED 1: Blue
5	Red	6	Battery 1
7	Battery 2	8	NFC antenna (removable)

3.5 Technical drawing

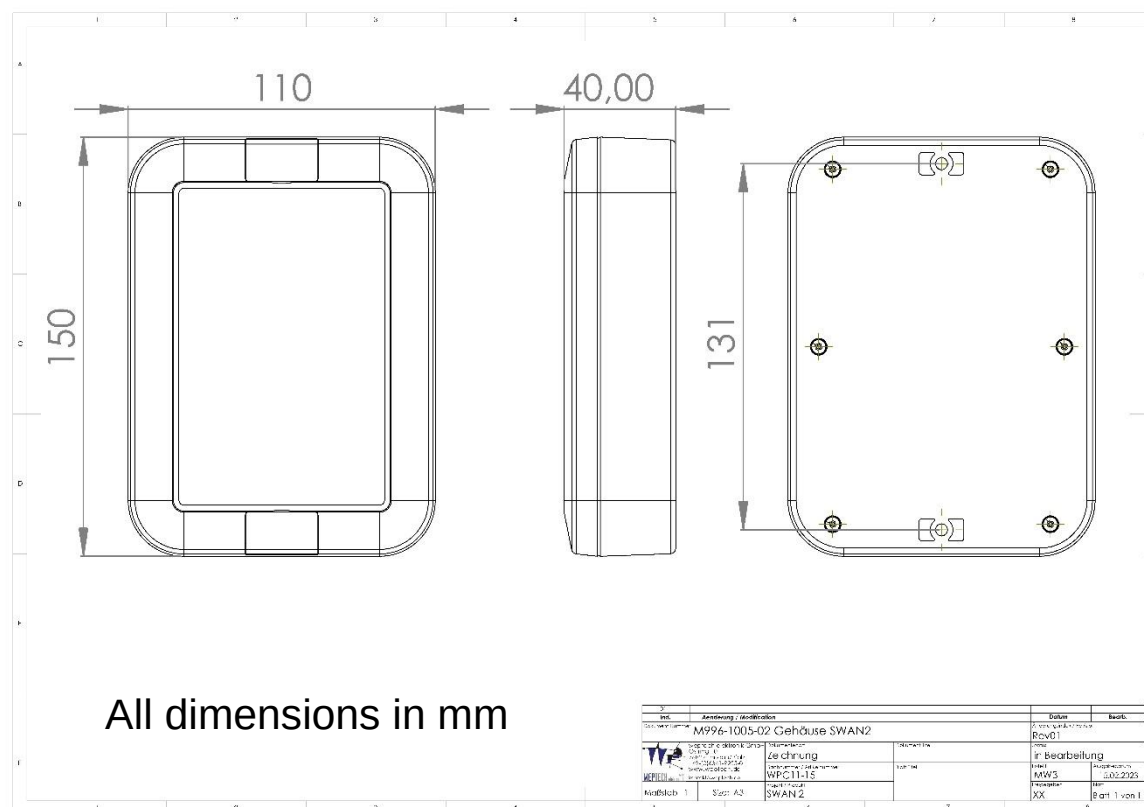


Figure 2: Technical drawing of housing

3.6 Transportation

The lithium metal batteries inside the device are subject to the requirements of dangerous goods legislation. The devices can be transported by road by the user without any further requirements. When shipping by third parties (e.g. shipping company), special requirements for packaging and labeling must be complied with! Talk to your shipping service provider.

Only ship devices if the housing or the batteries they contain are not damaged. Pack the device so that it cannot move inside of the packaging. Please comply with other national as well as international requirements.

During transport the storage conditions specified in section 3.2.1 must be adhered to.

3.7 Storage

The ambient conditions specified in section 3.2.1 must be adhered to for storage.

The device should be stored in a well-ventilated, cool place, out of direct sunlight and protected against moisture, ideally with a "Protect against heat!" warning sign.

4 Initial commissioning & mounting



Warning

Installation must be carried out by qualified personnel in compliance with the applicable safety regulations.



Caution

Take appropriate protective measures against electrostatic discharge when installing the equipment.

The batteries and the jumper are already fitted on delivery (see Figure 1). The device is operating in shipping mode, a low-power mode intended for transportation and storage of the device. Further details regarding the various operating modes of the device are explained in Part 2 of the instructions (see [1]).

4.1 Opening the housing

- Upon delivery, the housing is not tightened with screws.
- To open the device, remove the rubber band and take off the lid.

4.2 Inserting the SIM card



Hint

For communication via the mobile network, an LTE Cat-NB1-capable SIM card (format 3FF "Micro") is required. In Germany, WEPTech recommends a card from Deutsche Telekom for this purpose, alternatively we also recommend the provider 1NCE: <https://1nce.com/>

An LTE Cat-NB1-capable SIM card from any other mobile network provider can be used.



Attention

Electrostatic discharges

Failure to comply may result in damage to the device.

- ✓ Wear suitable ESD clothing and footwear during assembly.

- First disconnect the power supply by removing the jumper from the pin header, see Figure 1 pos. 2. Do not throw away the jumper, it is required to switch the device back on.
- The sim card holder is located at pos. 1 in Figure 1.
- Open the cover of the SIM card holder according to the marking ("Open") on its top.
- Insert the SIM card with the contacts facing down.

- Close the cover of the SIM card holder (marking: "Lock").

4.3 Turning the device on



Attention

Electrostatic discharges

Failure to comply may result in damage to the device.

- ✓ Wear suitable ESD clothing and footwear during assembly.

- To switch the device on, reinstall the previously removed jumper onto the pin header (Figure 1 Pos.2).
- After switching on, the device performs a self-test:
 - Blue LED is flashing
- If a fault is detected during the self-test:
 - Red LED lights up for two seconds
- After the self-test, the LEDs will turn off and the device will enter Shipping Mode, which is a low-power mode intended for transport or storage of the device. Further details regarding the different operating modes of the device are explained in part 2 of the manual (see [1]).
- In case of an error see section 5.
- The result of the self-test can and should be read out afterwards via the configuration interface in the event of an error (see part 2 of the manual [1]).



Hint

- The default password for access via the NFC Configurator app is: "0123"
- As long as the LTE Cat-NB1 settings are not configured or the device time is not set, no processing of configured events takes place.

4.4 Closing the device



Hint

A PH1 Phillips screwdriver is required to open and close the housing.

- When placing the cover, make sure that the two cutouts in the cover are located above the light guides (Pos. 4 & 5).



Attention

Tighten the body screws with a torque of 0.25 - 0.35 Nm. Ensuring compliance with the torque is mandatory for tightness.

- Screw the housing with the 6 housing screws.
- Further commissioning takes place via the NFC Configurator app.
- The configuration and further details about programming are described in part 2 of the manual [1].



Hint

As long as the LTE Cat-NB1 settings are not configured and the time in the device is not set, no processing of configured events will take place.

4.5 Mounting of the device

The housing can be mounted on the wall or ceiling when closed.

To do this, simply open the two tabs at the top and bottom of the housing.

The distance between the two drill holes is 131mm (see 0 "Technical drawing").



Attention

- Metallic obstacles near the device can have a negative effect on the RF performance.
- When mounting the device, make sure that it is only mounted in the orientation shown in Figure 3.
- Screws and dowels are not included.

The following screws and dowel size have to be used:

3 x 30 mm (screws), 5 x 25mm (dowels). Mounting must be done on a suitable surface.

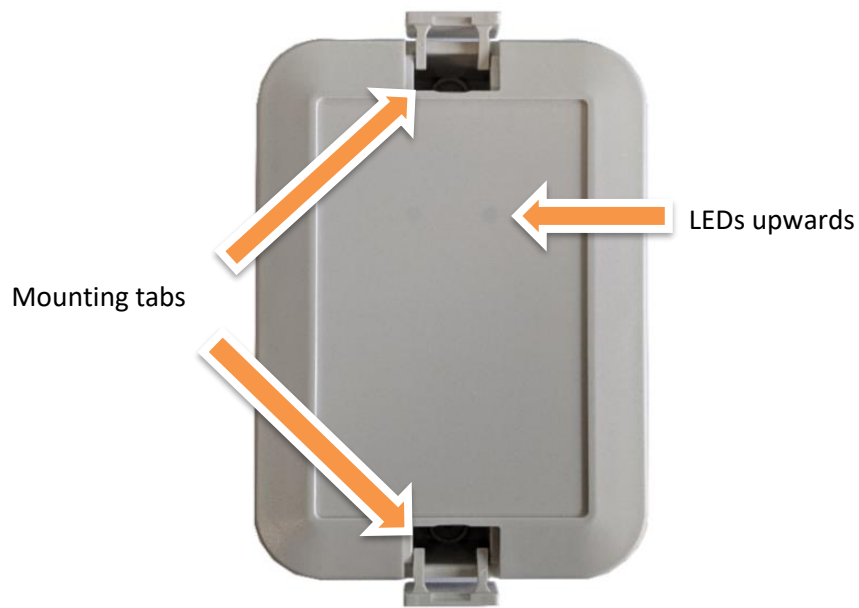


Figure 3: Device orientation

5 Troubleshooting during commissioning

5.1 Error: No reaction of the device when the jumper is plugged in

After the jumper is put on, the blue LED does not light up or flash. This means that there is no indication for a self-test.

Possible causes:

- Device is in standby or shipping mode before removing and placing the jumper
- Batteries are completely drained
- Batteries have insufficient contact
- Permanent defect of the device

Possible solution:

Remove jumper, press reset button of microcontroller (Figure 1 Pos. 3) and reattach jumper. If the error pattern persists, the device is defective or the batteries are discharged.

If the device has already been in intensive use, so that the batteries are discharged, the batteries should be replaced.

5.2 Error: Battery error during self-test

After placing the jumper, the blue LED flashes. The red LED then lights up for two seconds. In the NFC Configurator app, the entry "Failed: Battery" is displayed in "Device Status" under "Self-Test".

Possible causes:

- Battery depassivation failed
- Batteries too heavily discharged
- Batteries have insufficient contact

Possible solution:

Perform another attempt for depassivation of the battery. Remove jumper, press reset button of microcontroller (Figure 1 Pos. 3) and reattach the jumper. This process may need to be repeated several times, depending on how strongly the batteries are passivated. The degree of passivation depends, among other things, on the battery model, storage duration and storage conditions.

If the batteries are already partially discharged, the error may remain permanently. In this case, the device can still be used, but the expected service life may not be achieved. Instead, replace the batteries and then test again.



The battery test is intended for the initial start-up of the device with fresh batteries. If the device is restarted after it has been in operation with the same set of batteries for a long time, an advanced discharge of the batteries and thus a battery error during the self-test are to be expected and do not represent a defect in the device.

5.3 Error: Other self-test errors

After placing the jumper, the blue LED flashes. The red LED then lights up for two seconds. In the NFC Configurator app, no battery error ("Failed: Battery") is displayed in "Device Status" in "Self-Test", but any other error.

Possible causes:

- Temporary defect of the device
- Permanent defect of the device

Possible solution:

Perform another attempt for depassivation of the battery. Remove jumper, press reset button of microcontroller (Figure 1 Pos. 3) and reattach jumper. If the error pattern persists, the device is defective.

5.4 Errors that cannot be resolved



Hint

If the SWAN2 does not operate correctly, please contact us via the contact form on our website:
<https://www.weptech.de/en/support/we-can-help.html>

6 Maintenance

6.1 Maintenance

The device is free of maintenance. Ongoing or periodic maintenance is not necessary.

Only replacing the batteries may be necessary depending on the device configuration.

In the event of damage, e.g. due to transport and/or storage, no repairs may be carried out by unauthorized personnel.

6.2 Battery replacement



Warning

Installation must be carried out by qualified personnel in compliance with the applicable safety regulations.

6.2.1 Suitable battery types



Hint

Only the batteries listed below may be used.

Failure to do so may result in safety and functionality restrictions.

Only the following battery types may be used:

- Fanso ER26500M
- Saft LSH 14
- HCB Battery ER26500M

6.2.2 Replacing the batteries

This chapter explains how to replace the batteries.



Attention

Electrostatic discharges

Failure to comply may result in damage to the device.

- ✓ Wear suitable ESD clothing and footwear during assembly.
- ✓ Use appropriate tools.

Step 1: Dismount device

- Dismount the device from its current location
- The fastening screws are located under the two mounting lugs (see chapter 6.2.2)

 **Hint**

A PH1 Phillips screwdriver is required to open and close the housing.

Step 2: Open housing

- The device is opened by loosening the six screws on the back of the housing.



Step 3: Remove jumper

Remove the jumper from the pin header (see also Figure 1 Pos.2).



Step 4: Remove NFC antenna (optional)

The NFC antenna can be dismantled for easier battery replacement.

- Carefully remove the NFC antenna from the holder. If necessary, lightly press the two plastic lugs in or together with a pair of needle-nose pliers.



Hint

When removing and inserting the batteries, be careful not to damage them.

Step 5: Remove old batteries

- The batteries can be removed either by hand or with the aid of a suitable tool.



Hint

Wait approx. 1 minute before inserting the new batteries.

Step 6: Insert new batteries

- Insert the batteries one after the other according to the polarization markings on the circuit board.



Step 7: Reinstall NFC antenna

- Reinstall the NFC antenna, while making sure that the contact pins are inserted correctly.



Step 8: Plug on jumper

Plug the jumper onto the pin header (see also Figure 1 Pos.2).



Step 9: Close housing & mount device

- Reassemble and remount the device. Make sure that the housing is closed correctly (see chapter 4.4)



6.3 Cleaning

Cleaning of the device is only permitted from the outside and when the housing is closed. Dirty devices can be cleaned with a dry cloth. If this is not sufficient, a moistened cloth can be used.

**Attention**

- Under no circumstances may corrosive agents or solvents be used for cleaning.
- Do not clean the opened device.

7 Guidelines, laws and standards

The use of radio frequencies is subject to national regulations. This device has been designed in accordance with the requirements of RED (Radio Equipment Directive) 2014/53/EU and ROHS (Restriction of Certain Hazardous Substances) 2011/65/EU.

7.1 Declaration of Conformity



We, the manufacturer

Declaration of Conformity



Weptech elektronik GmbH
Ostring 10
76829 Landau
Germany

declare under our sole responsibility that the product:

Item: SWAN2-R
Item Number: A001-0119-001, A001-0134-001
Description: NB1 Gateway SWAN2 wMBus

is in conformity with the provisions of the following EU directives and standards if used for its intended purpose and in accordance with the manufacturers operating instructions.

Applied directives and harmonized standards

Type	Document	Issue / Version
RED Directive	2014/53/EU	
Health & Safety (Art. 3(1)(a))	EN 62368-1	2014 / AC: 2015
	EN 62311	2019
EMC (Art. 3(1)(b))	ETSI EN 301 489-1	V2.2.3
	ETSI EN 301 489-3	V2.2.3
	ETSI EN 301 489-52	V2.2.3
Spectrum (Art. 3(2))	ETSI EN 301 908-1	V13.1.1
	ETSI EN 301 908-13	V13.1.1
	ETSI EN 300 220-1	V3.1.1.
	ETSI EN 300 220-2	V3.1.1.
	ETSI EN 300 330	V2.1.1
	IEC 60529	2013
ROHS Directive	2011/65/EU	

Landau, 2022-05-30

Manufacturer / Authorized representative
Ulrich Schmitt

President: Oswald Maurer
Commercial Register Landau HRB 2583

WEPTECH elektronik GmbH
Ostring 10
76829 Landau, Germany

8 Supporting documents

The following documents contain information to certain features and functionalities of the SWAN2 Gateway. These documents can be requested via sales@weptech.de.

Ref.	Document name	Version	Datum
1	<i>Manual - NB1 Gateway SWAN2 and NB1 Gateway SWAN3</i> Part 2: Configuration	3.2	12.05.2023

9 Disposal



In the legal territory of the EU, the symbol of the "crossed-out wheeled bin" shown on the left identifies products which, at the end of their life, should not be discarded as unsorted waste but must be sent to separate collection facilities for recovery and recycling.

For batteries or accumulators containing mercury (Hg), cadmium (Cd) or lead (Pb), you will find the respective chemical symbol below the symbol of the crossed-out trash can.

Owners of old electrical and electronic equipment (WEEE) are required by law to have it collected separately.

WEPTech elektronik GmbH sells its devices exclusively to commercial users. However, it is possible for these devices to end up as WEEE in private households. Our devices are therefore "WEEE from private households" within the meaning of Article 3(h) of Directive 2012/19/EU.

In Germany there are free collection points in your area for the return of WEEE from private households and possibly additional collection points for the reuse of old appliances. You can obtain their addresses from your city or municipal administration.

In addition, distributors who have a sales area for electrical and electronic equipment of at least 400 square meters and food retailers who have a total sales area of at least 800 square meters and also offer electrical and electronic equipment several times a calendar year or on a permanent basis are obliged to take back WEEE from private households. Distributors who sell their products using means of distance communication are obliged to take back electrical and electronic equipment if the storage and shipping areas for electrical and electronic equipment are at least 400 square meters.

The above distributors will take back the equipment free of charge if a new unit of the same type is purchased. Devices whose external dimensions do not exceed 25 cm each can be returned to the above distributors free of charge, irrespective of the purchase of a new device. This return is limited to three old devices per type of device.

Electrical and electronic equipment often contains sensitive personal data. The end user is responsible for deleting all personal data from waste equipment before handing it over for disposal or recycling.

End-users of waste equipment containing batteries, accumulators or lamps must, as a rule, remove them from the waste equipment before handing it in at a collection point and dispose of them separately, provided that these batteries, accumulators or lamps can be removed without being destroyed. The requirement for removal also does not apply if the waste equipment is prepared for reuse with the participation of a public waste management authority.

Owners of batteries and accumulators are legally obliged to return old batteries and accumulators after use. You can do this free of charge at the retail store, shipping warehouse or at another collection point in your area. Addresses of suitable collection points can be obtained from your city or municipal administration.

This device contains permanently installed, non-rechargeable lithium metal batteries (lithium thionyl chloride) which cannot be removed non-destructively by the end user and therefore do not have to be removed before returning the old device. When handing over the old device at a collection point, please indicate the batteries contained in the device to the staff so they can be removed by qualified personnel.

10 Copyright protection

Transmitting, as well as copying, of this document and utilization of its contents are not permitted, if not explicitly allowed. Violation obligates compensation. We reserve all rights in this document and in the subject matter and illustrations contained therein.

11 Warranty information

Great care was taken in preparing this manual. No guarantee is given for the correctness of the contents of this manual since errors, in spite of all efforts, can never be completely avoided.

12 Disclaimer

WEPTech elektronik GmbH is not liable or warranted for any damages resulting from improper installation, assembly and improper use of the product or failure to comply with the operating instructions and/or safety instructions.

Parts of the pages or the complete publication including all offers and information might be extended, changed or partly or completely deleted by WEPTech elektronik GmbH without separate announcement.

This disclaimer is to be regarded as part of the operating instructions from which reference was made to this page. If sections or individual terms of this statement are not legal or correct, the content or validity of the other parts remain valid by this fact.

13 Restriction of use

WEPTech elektronik GmbH products are not approved for use in life support or life sustaining systems or units, or other systems where malfunction can be expected to result in substantial personal injury to the user or third parties. WEPTech elektronik GmbH products are further not approved for use as an essential part of any life support or life sustaining system or unit, the malfunction of which may cause the failure of the life support or life sustaining system or unit, or affect its safety or effectiveness. Customers who use these products in such applications or sell them for such uses do so at their own risk and must exempt WEPTech elektronik GmbH from all damages resulting from the sale for inappropriate purposes or the inappropriate use.

By using WEPTech elektronik GmbH products, the user is bound by these terms and conditions.

WEPTech elektronik GmbH

Maria-Goeppert-Mayer 4

D-76829 Landau

<http://www.weptech.de/>

info@weptech.de

Tel: +49 6341 9255-0

Fax: +49 6341 9255-100

Note:

The information, instructions and descriptions in this manual refer to the actual operating and service conditions herein.

For technical questions, safety notes or technical failure, please contact WEPTech elektronik GmbH.

We reserve the right to technical modifications.

Manual

NB1 Gateway SWAN2

-

NB1 Gateway SWAN3

Part 2: Configuration

Created by
WEPTeCH elektronik GmbH
Ostring 10 / 76829 Landau
Germany



Revision history

Firmware-Version:		3.14.2	
NFC-App-Version:		2.5.8 (76)	
Revision	Date	Description	Author
1.0	11.04.2019	Initial Release	UK
1.1	23.04.2019	Addition Vodafone contact	UK
1.2	22.08.2019	Update LED-behavior	UK
1.3	18.11.2019	Update FW Release 1.5.0	UK
1.4	12.02.2020	Update FW Release 1.6.0	UK
1.5	18.08.2020	Update FW Release 3.2.3	UK/ EH2
1.6	04.11.2020	Update FW Release 3.4.3	UK / EH2
1.7	10.12.2020	Update FW Release 3.6.0	EH2/RW
1.8	30.04.2021	Update after PCB design changes and firmware update 3.8.2	MW/EH2/RW
1.9	17.06.2021	Description of CSV-String-Format	RW
2.0	28.07.2021	Addition DoC	SN2
2.1	09.08.2021	Update FW Release 3.10.0	RW
2.2	07.03.2022	Update FW Release 3.12.0	RW
2.3	22.07.2022	Update FW Release 3.12.5	RW
3.0	28.02.2023	Split manual into "Part 1: Hardware" and "Part 2: Configuration" Update for FW Release 3.14.0 - Configuration of synchronous Reception - Configuration of alarm detection - Configuration of week based events - Description of synchronous Reception - Additional Fields in CSV-String-Format	RW
3.1	19.04.2023	Update FW Release 3.14.2 Update password change for App version 2.5.8	RW
3.2	15.06.2023	Additional devices in product identification	RW

Contents

1	General information	6
1.1	Identification of the manufacturer	6
1.2	Identification of the product	6
1.3	Guidelines, laws and standards	6
1.4	Validity	6
1.5	Support	7
2	Safety	7
2.1	Signal words and graphic symbols	7
2.1.1	Signal words & warnings	7
2.1.2	Hints in this user manual	8
2.1.3	Structure of warning notices	8
2.1.4	Symbols	8
2.2	Intended use	9
2.3	Precautionary handling	9
2.4	Predictable misapplication	9
2.5	General safety instructions	10
2.5.1	Risk of injury	10
2.5.2	Risk of material damage	10
2.6	Qualification of personnel	11
2.7	Storage	11
3	Description of the device	12
3.1	Product information	12
3.2	Description of the receive mode	12
3.3	Description of the transmission mode	13
3.4	Description of the operating behavior	13
3.4.1	Switch-on phase	13
3.4.2	Shipping Mode	13
3.4.3	Standby Mode	14
3.4.4	NFC Configuration	14
3.4.5	Time synchronization via NTP	14
3.4.6	Receive mode	14
3.4.7	Transmission mode	15
4	Configuration of the device via NFC (Android)	16
4.1	General use of NFC	16

4.2	Connect to the device	17
4.3	Save and load configuration.....	17
4.4	Mobile network configuration	20
4.5	Configuration of transmission mode	21
4.5.1	Server configuration	21
4.5.2	Configuration of the transmission interval.....	24
4.6	Configuration of continuous receive mode	27
4.6.1	General receive mode.....	27
4.6.2	Receive mode interval	30
4.7	Configuration of synchronous receive mode.....	32
4.8	Time setting.....	34
4.9	Additional configuration options.....	35
4.10	Credentials	37
4.11	Address Management	38
4.11.1	Manually adding a device to the whitelist	38
4.11.2	Description of the wireless M-Bus address	39
4.11.3	Wireless M-Bus device with Wildcard.....	39
4.11.4	Radio Scan List (RSL) & Whitelist	40
4.12	Device Installation	42
4.12.1	Set device time via NTP.....	42
4.12.2	Receive mode (Collect Data)	42
4.12.3	Transmission mode (Upload Data)	43
4.12.4	Build Radio Scan List (RSL)	43
4.13	Device Status	44
4.14	Change Password.....	45
4.15	Firmware Update.....	46
4.16	Activate Shipping Mode	47
4.17	Factory Reset.....	48
5	Remote-Configuration and Firmware-Update.....	49
6	Protocols for data upload	49
6.1	UDP	49
6.2	HTTP and HTTPS	49
6.2.1	Server requirements.....	50
6.2.2	HTTP/S-Header.....	51
6.2.3	Upload-Request-Method	51
6.3	LwM2M	52

7	Synchronous receive mode.....	54
7.1	Initial Configuration and Synchronization	54
7.2	Process for Synchronization	54
7.3	State of synchronization	55
8	Data formats	56
8.1	Raw Data (binary)	56
8.2	Raw Data (hex encoded)	56
8.3	Upload as CSV-String.....	56
8.3.1	Packet type 1 "Initialization":.....	57
8.3.2	Packet type 2 "Sensor data"	59
8.3.3	Packet type 3 "Ending"	60
8.3.4	Status Flags in CSV String	62
8.3.5	Estimation of battery state of charge	63
8.4	CSV String with Acknowledge.....	63
9	Use of different Platforms	64
9.1	IoT Platform.....	64
9.1.1	Device Management in the IoT Platform	64
9.1.2	Devices in the IoT Platform	65
9.2	WEPTech's "Real time" Monitor with MQTT	67
9.2.1	WEPTech MQTT Client App	67
9.2.2	Eclipse Paho MQTT Spy	68
9.2.3	Use of Mosquitto.....	69
10	Supporting documents	70
11	Copyright protection	70
12	Warranty information	70
13	Disclaimer	70
14	Restriction of use	71

List of Tables

Table 1: Description of the wireless M-Bus address components	39
Table 2: Recommended server connection parameters	50
Table 3: Supported cipher suites.....	50
Table 4: HTTP Content-Type.....	51
Table 5: PUT request filename format	52
Table 6: State of synchronous receive mode	55
Table 7: Description of CSV string - packet type 1	58
Table 8: Description of CSV string - packet type 2	59

Table 9: Description of CSV string - packet type 3	61
Table 10: Status Flags.....	62

List of Figures

Figure 1: Information symbol app.....	16
Figure 2: Connect to the device	17
Figure 3: Save and load configuration (1)	18
Figure 4: Save and load configuration (2)	18
Figure 5: Clone configuration	19
Figure 6: Configuration LTE Cat-NB1 network	21
Figure 7: Configuration of transmission mode.....	23
Figure 8: Configuration of the transmission interval	25
Figure 9: Upload on alarm detection	26
Figure 10: Configuration of receive mode	29
Figure 11: Configuration of the receive mode interval.....	31
Figure 12: Configuration of synchronous receive mode	33
Figure 13: Configuration Time Setup	34
Figure 14: Additional configuration parameters.....	36
Figure 15: Credentials Menu	37
Figure 16 Add wireless M-Bus devices	38
Figure 17: Description Wildcard.....	39
Figure 18: RSL & Whitelist	40
Figure 19: Save and load whitelist	41
Figure 20: Format Whitelist	41
Figure 21: Device Installation	42
Figure 22: Parameters for Build Radio Scan List	43
Figure 23: Device Status	44
Figure 24: Change password	45
Figure 25: Firmware Update	46
Figure 26: Activate Shipping Mode	47
Figure 27: Factory Reset.....	48
Figure 28: Format Specification	56
Figure 29: Device Management	64
Figure 30: Device Management - Live Payloads.....	65
Figure 31: Edge Connector – IoT platform	65
Figure 32: Edge Connector – Live Payloads.....	66
Figure 33: Edge Connector – Device ID/ Data	66
Figure 34: Edge Connector – Device ID	67
Figure 35: MQTT Client App	68
Figure 36: Eclipse Paho MQTT Spy URL.....	68
Figure 37: Eclipse Paho MQTT Login	69
Figure 38: Eclipse Paho MQTT Spy TLS.....	69

1 General information

1.1 Identification of the manufacturer

Manufacturer	Weptech elektronik GmbH		
Address	Ostring 10		
	D-76829 Landau		
	Tel: +49 6341 9255-0		Fax: +49 6341 9255-100
	https://www.weptech.de		info@weptech.de

1.2 Identification of the product

Device	Series	Article number
NB1 Gateway SWAN2	• SWAN2-C	• A001-0117-001
	• SWAN2-R	• A001-0119-001
		A001-0134-001
	• SWAN2-C-S	• A001-0127-001
	• SWAN2-C-E	• A001-0127-002
	• SWAN2-R-E	• A001-0127-003
	• SWAN2-C-V	• A001-0132-001
NB1 Gateway SWAN3	• SWAN3-W-230V-X-X	• A001-0130-001

1.3 Guidelines, laws and standards

The use of radio frequencies is covered by national regulations. This device has been designed in accordance with the requirements of RED (Radio Equipment Directive) 2014/53/EU.

1.4 Validity

This user manual applies exclusively to the products specified in section 1.2.

The operating instructions consist of two parts:

- Part 1 describes the hardware, installation and commissioning of the device for each variant.
- Part 2 of the operating instructions explains the configuration of the device independently of the variant. The operating instructions refer to the firmware version and NFC app version specified in the revision history.

This manual in English is a direct translation of the German manual for this device. For this reason, this manual is based on German laws and regulations. Figures showing screenshots of the Android App may differ from newer versions of the Android App.

1.5 Support



Hint

If you need help with the configuration, please contact us using the contact form on our website:

<https://www.weptech.de/en/support/we-can-help.html>

2 Safety

The user manual is an integral part of the product and must be read carefully before use. Keep this user manual and all other applicable documents in a safe place so that they are always available when required.

2.1 Signal words and graphic symbols

This user manual contains warnings and symbols, which are explained in the following chapters.

Warnings are intended to warn of residual dangers and exist in three levels. The classification of the warnings depends on the severity of the damage that can occur if the warnings are ignored and the recommended actions are not followed.

2.1.1 Signal words & warnings

Warnings are introduced with one of the following signal words and marked with a corresponding signal color.



Danger

Indicates a hazard with a high degree of risk, an imminently hazardous situation which, if not avoided, will result in death or serious injury.

Imminent danger resulting in serious bodily injury or death.



Warning

Indicates a hazard with a medium degree of risk, an imminently hazardous situation which, if not avoided, will result in death or serious injury.

Potentially hazardous situation that could result in serious bodily injury or death.



Caution

Indicates a low-risk hazard, an imminently hazardous situation which, if not avoided, will result in death or serious injury.

Potentially dangerous situation that could result in minor bodily injury.

Attention

Identifies specific warnings, notices, or comments of special interest that do not relate to physical and practical injuries where physical injury is not a reasonable possibility.

Situation that may result in possible property damage to the product.

2.1.2 Hints in this user manual

The following symbols are used in this manual to emphasize important information:

Hint

Indicates usage tips and particularly useful information about the product.

2.1.3 Structure of warning notices

Warning

The first line describes the type and source of the hazard.

The second line describes the consequences if no security measures are taken.

- ✓ The last line describes measures to prevent hazards.

Example:

Caution

Risk of injury due to disregard of the safety symbols.

Failure to observe the warnings in the user manual can lead to injuries and further hazards.

- ✓ Pay attention to the warnings in the user manual.

2.1.4 Symbols

Symbol	Meaning	Symbol	Meaning
	General warning		Warning of electrical voltage

	Warning of hazards due to battery charging		Warning of flammable substances
	Follow user manual		Observe general advice
	Warning of electrostatic hazard, may cause serious damage to the product		General note / information

2.2 Intended use

The product is used to collect wM-Bus meter telegrams and send the collected telegram data to a configured server via the mobile network. The product may only be used as intended; any kind of misuse is not permitted. Intended use also includes compliance with all the information in these instructions. Any use beyond the intended use or any other use is considered misuse.

The product must not be modified in any way without the written permission of WEPTech elektronik GmbH. Unauthorized modifications to the product can lead to malfunctions and are prohibited for safety reasons.



Warning

Misuse of the device can lead to dangerous situations.

- ✓ Only use the device for its intended purpose.

2.3 Precautionary handling

The product was built in accordance with the state of the art and recognized safety regulations. Nevertheless, its use may result in functional hazards for the user or third parties or damage to the device and other material assets.

Only use the product when it is in perfect working order and in accordance with its intended use, safety and hazard awareness, and in compliance with the operating instructions. In particular, faults that impair safety must be rectified immediately.

2.4 Predictable misapplication

Reasonably predictable misapplications that may involve hazards for the user, third parties or for the SWAN2 are:

- ✓ Using the SWAN2 and accessories other than for their intended purpose.
- ✓ Operating the SWAN2 in a way that is contrary to the instructions in the user manual with regard to safety instructions, installation, operation, maintenance and servicing.
- ✓ Operating the SWAN2 with obvious malfunctions.

2.5 General safety instructions

Nevertheless, the use of the device may cause function-related hazards for the user or third parties or may result in damage to the device and other material assets.

2.5.1 Risk of injury



Risk of explosion

Live parts of the product can generate electrical sparks even at low voltages (e.g. when opening and closing electrical circuits) and act as ignition sources. In potentially explosive atmospheres, this can trigger an explosion that can injure individuals.

- ✓ Do not use the device in potentially explosive areas.



Battery

Please be sure to follow these instructions for handling lithium batteries:

- ✓ Do not expose the battery to fire or moisture!
- ✓ Do not attempt to charge the lithium battery!
- ✓ Do not pierce, break, crush or cut the device or the battery! Do not disassemble the battery!
- ✓ Do not short-circuit the battery contacts!
- ✓ Never operate batteries outside the designated product specification!

2.5.2 Risk of material damage



Electrostatic discharge

The highly sensitive electronic components can be damaged by electrostatic discharge or overvoltage. Damaged devices may no longer function correctly or at all.

- ✓ Do not mount the device in rooms with electrostatic charge.
- ✓ Do not touch electronic components without ESD clothing.
- ✓ Wear ESD clothing and footwear.
- ✓ Only use suitable tools.



Heavy vibrations

Heavy vibrations can damage mechanical and electronic components of the device. Damaged devices may no longer function correctly or at all.

- ✓ Do not drop the device on the floor, hard surfaces or hard objects.



Liquids

Water and other liquids can damage the electronic components of the device. Damaged devices may no longer function correctly or at all.

- ✓ Protect the electronic components from water and other liquids.



Climatic Effects

Climatic effects such as heat, cold and moisture can damage the device. Damaged devices may no longer function correctly or not at all.

- ✓ Observe the maximum/minimum permitted temperatures and the information on humidity during operation. See part 1 of the user manual of the respective device variant for this information.

2.6 Qualification of personnel

The device may only be transported, unpacked, assembled, operated, maintained, disposed of and otherwise used by suitable, qualified, instructed and authorized personnel.

2.7 Storage

The user manual is an integral part of the product and must be read carefully before use and be available at all times.

Keep these operating instructions and all other applicable documents in a safe place so that they are available when required.



Attention

Read carefully before use.

Keep for future reference.

3 Description of the device

In this manual, the operating modes of the gateway are first explained independently of the variants. Subsequently, the configuration of the gateway is described.



Hint

The technical data for the corresponding devices can be found in Part 1, Chapter 3.2 I 1 of the respective variant-specific user manual.

3.1 Product information

The SWAN2 is a battery-powered gateway or in the case of the SWAN3 a gateway, that is powered by an external power supply. The gateway directly links wireless M-Bus devices to the cellular network using the new LTE Cat-NB1 technology. The number of storable telegrams depends on the device variant and is specified in part 1 of the manual.

The device is configured via the NFC interface. WEPTech provides an Android application for this (see section 4). This app also allows an update of the firmware of the device. Additionally there is the option for remote configuration and Firmware-Update-Over-The-Air (see section 5).

The wireless M-Bus interface (radio standard according to DIN EN 13757-4) works with 868 MHz and supports modes S, T and C as well as frame formats A and B. The gateway supports LTE bands 3, 8 and 20 as well as the protocols UDP, HTTP/S and LwM2M.

The device will switch to receive mode at adjustable intervals. The incoming wireless M-Bus meter telegrams are stored in a non-volatile memory ("*RECEIVE MODE*"). Following this or at configurable times, the data is sent via LTE Cat-NB1 mobile radio to the previously selected server (see section 4.5.1) ("*TRANSMISSION MODE*").

3.2 Description of the receive mode

In receive mode, incoming wM-Bus telegrams are received, depending on the configured operating mode and filtered ("*whitelist*") and then stored in the internal memory. The following algorithm is used here:

1. During radio reception, first the checksums are removed from the wM-Bus telegrams.
2. If the whitelist is not empty, incoming telegrams are discarded without a corresponding entry (when using a radio adapter, the address in the transport layer – i.e. the actual meter address – is used for comparison).
3. Subsequently, all telegrams run through a duplicate filter: Radio telegrams with already "known" addresses and telegram lengths are discarded. Therefore, only the first telegram received by each meter is processed (if the radio telegrams have different lengths, multiple transmissions from a device can be processed).
4. The telegram is then stored in the internal memory.

The receive mode ends, either when

- the configured maximum duration has been reached, *or*
- the configured number of telegrams has been stored in the device memory (after address filtering and duplicate filtering of all received telegrams).

3.3 Description of the transmission mode

The transmission mode consists of three phases:

1. Logging into the LTE Cat-NB1 mobile network with the configured LTE Cat-NB1 settings.
2. Sending of the meter data saved in receive mode to the configured server.
3. Logging out of the LTE Cat-NB1 mobile network.

Different flashing cycles of the blue LED represent each phase.



Hint

The upload of the meter telegrams to the user server is performed with the selected protocol and the configured data format. There is **no decryption** or other processing of the meter data in this device.

3.4 Description of the operating behavior

3.4.1 Switch-on phase

After switching on the device (see part 1 of the manual) the blue LED will light up for one second and flash with a frequency of 16 Hz during the self-test of the device. Battery-powered variants will also perform a battery measurement as part of the self-test and if the voltage of the battery with load is below 3,25V the device will try to de-passivate the battery. The self-test takes at most 60 seconds and if an error is detected during the self-test the red LED will light up for two seconds. The error cause can be checked with the NFC-Configurator-App in the “Device Status” in this case (see section 4.13).

Regardless whether if there was an error or not, the device will enter the Shipping Mode after the self-test is done. The entry into the Shipping Mode is indicated by a slow fade out of the blue LED.

3.4.2 Shipping Mode

The Shipping Mode is a Low-Power-Mode which can be used for storage or transportation of the device. While the device is in Shipping Mode, no processing of configured events will occur, which means that there will be no data collection and no data upload. Battery-powered variants will discharge the battery periodically to prevent its passivation in this mode.

The gateway will enter this mode under the following conditions:

- Turning device on via the power jumper *or*
- Device time is not set and device enters Low-Power-Mode *or*
- Command via the NFC-Configurator-App even if device time is set (see section 4.16)

The Shipping Mode will be deactivated by the following actions:

- Authentication via the NFC-Configurator-App *or*
- Pushing “Reset MCU” button on the board of the device *or*

- If the “Fast NFC Installation” Option is enabled any NFC-antenna can be used to leave the shipping mode without the need for authentication via the NFC-Configurator-App. The NFC-antenna has to be connected with the device for 10 seconds (see section 4.9).

After the Shipping Mode was deactivated and the device time is configured, the device will enter the Standby Mode when the device is done with the processing of configured data collection- and upload events.

3.4.3 Standby Mode

The Standby Mode is a Low-Power-Mode which allows the device to still process the data collection- and upload events at the configured time. There is no periodic discharge of the battery in battery-powered variants in this mode as it is already discharged via the configured events.

In the Standby Mode, the blue LED flashes approx. every 20 seconds. The flashing can be deactivated via Quiet mode in the NFC Configurator App (see chapter 4.9).

3.4.4 NFC Configuration

When an NFC field is detected, the device exits the low-power mode (Shipping or Standby Mode) and waits for authentication via the NFC Configurator App (see section 4.2).

After successful authentication, the red LED flashes at a frequency of 2 Hz and is ready for configuration via app. The device exits the NFC configuration mode and changes back to low-power mode if there is no communication via the NFC interface for a period of 20 seconds.

3.4.5 Time synchronization via NTP

The time of the device is set via the configured NTP server. Since an LTE Cat-NB1 connection is required for this, the corresponding LTE Cat-NB1 configuration must have already been carried out. The time can be set using the NFC configurator app (see chapter 4.12.1) or by pressing the reset button. After starting the process, the module will first try to log into the cellular network. The first login process after switching on the device or after waking up from shipping mode (see chapter 4.16) has a timeout of 15 minutes. If the first login process is successful, all following login processes have a timeout of 5 minutes. During the actual process of logging into the LTE Cat-NB1 network to set the time, the blue LED flashes quickly once per second.

As soon as the device is logged into the cellular network, an attempt is made to synchronize the time via NTP (60 seconds timeout). During this process, the blue LED flashes once every two seconds.

If the time cannot be set (e.g. NTP server cannot be reached), the red LED on the device flashes for 5 seconds in a cycle of 2 Hz. If the process for setting the time was started using the reset button, the device sets its internal clock to 01/01/2020, 00:00:00.

3.4.6 Receive mode

In this operating mode, the red LED lights up once for each meter received (storage in nonvolatile memory) and flashes approx. every 6 seconds.

The receive mode is ended, if either

- the configured number of devices has been received (and stored in the memory) *or*
- the configured time has expired.

3.4.7 Transmission mode

In this phase, the blue LED flashes once per second during the login process into the cellular network. The first login process after switching on the device or after waking up from shipping mode (s. chapter 4.16) has a timeout of 15 minutes. If the first login process is successful, all following login processes have a time out of 5 minutes. If the login process is successful, the data will be uploaded.

During the actual data upload (which should only take a few seconds), the blue LED flashes, for each packet sent. After sending all data, the blue LED flashes slowly every 2 seconds until the LTE Cat-NB1 connection is released from the network.

4 Configuration of the device via NFC (Android)

android 

To configure the device via NFC, please download the Android application “NFC Configurator” from the Play Store and install it:

<https://play.google.com/store/apps/details?id=de.weptech.nfcconfigurator&hl=de>

Hint

1. For the device to function, it is essential to set the server to which the data is to be uploaded (see section 4.5) as well as the APN of the mobile network provider (see section 4.3) and to set the time in the device (see section 4.3).
2. Various fields in the app provide an info symbol. Clicking on this symbol opens a field which explains the corresponding configuration in more detail.
3. In the following description menu points in the main menu are **ORANGE** and sub menus of the configuration are **BLUE**.

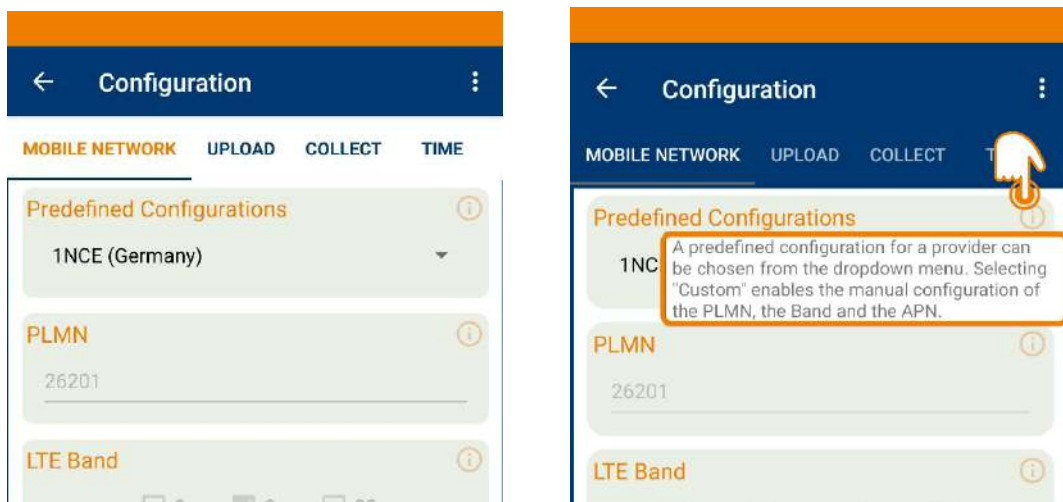


Figure 1: Information symbol app

4.1 General use of NFC

Please note the following when configuring via NFC:

- The NFC touchpoints must be placed one above the other. To do this, you must find out where the NFC touchpoint of your Android device is located. The NFC touchpoint is centered on the front of the device.
- If the devices are connected successfully, you will be informed via a haptic signal from your Android device (vibration).
- All changes made in the app must be confirmed using the **WRITE/EXECUTE** button and transferred to the device. A new NFC connection may be required for this.
- Depending on the configuration, the loading process may take longer. A loading progress bar indicates this. Please maintain the connection of the NFC interfaces until completion.

4.2 Connect to the device

1. Open the “NFC Configurator” app and place the NFC touchpoint of your Android device directly over the NFC touchpoint of the gateway. The NFC touchpoint is centered on the front of the device.
2. If the connection is successful, you will be asked to enter your password. The default password depends on the device variant and is given in part 1 of the manual. This default password should be changed later (see section 4.14).
3. After the password has been entered correctly, you will be asked to reconnect and the main menu of the app will be displayed.

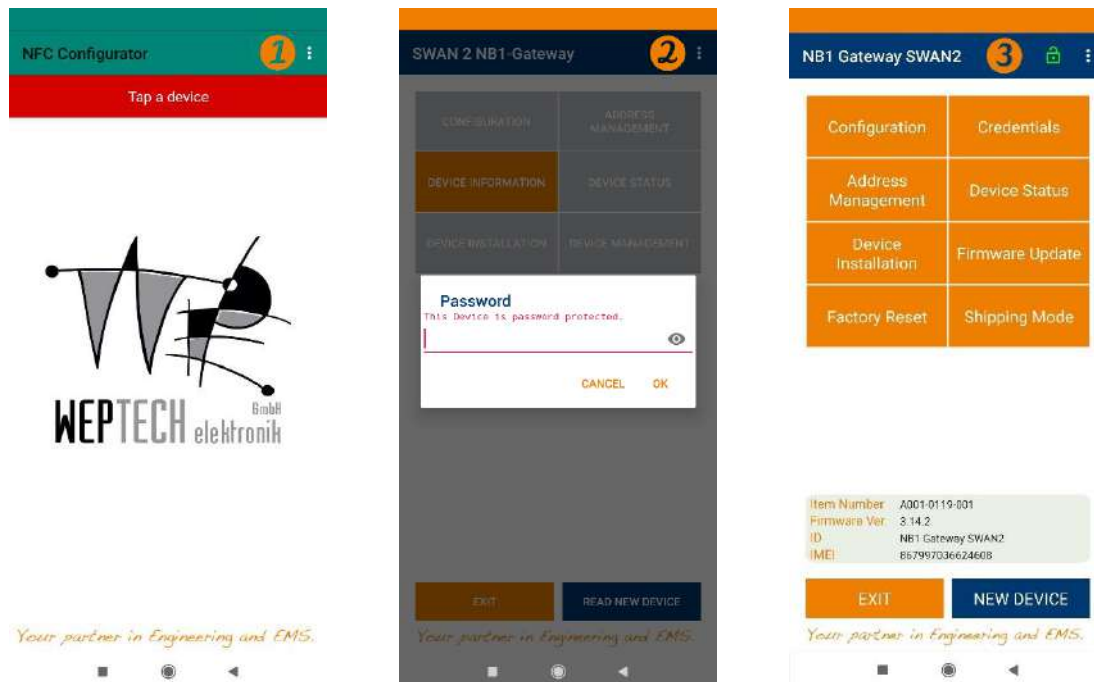


Figure 2: Connect to the device



Hint

To return to the main menu and perform the configurations explained below, always proceed as described above.

4.3 Save and load configuration

You have the option to save your configurations and transmit them to another device. You can proceed in two different ways:

1. Go to **CONFIGURATION** in the main menu.
2. Tap the 3 dots in the top right corner. A drop-down menu opens.
3. You now have two options for transferring your configuration to another device:

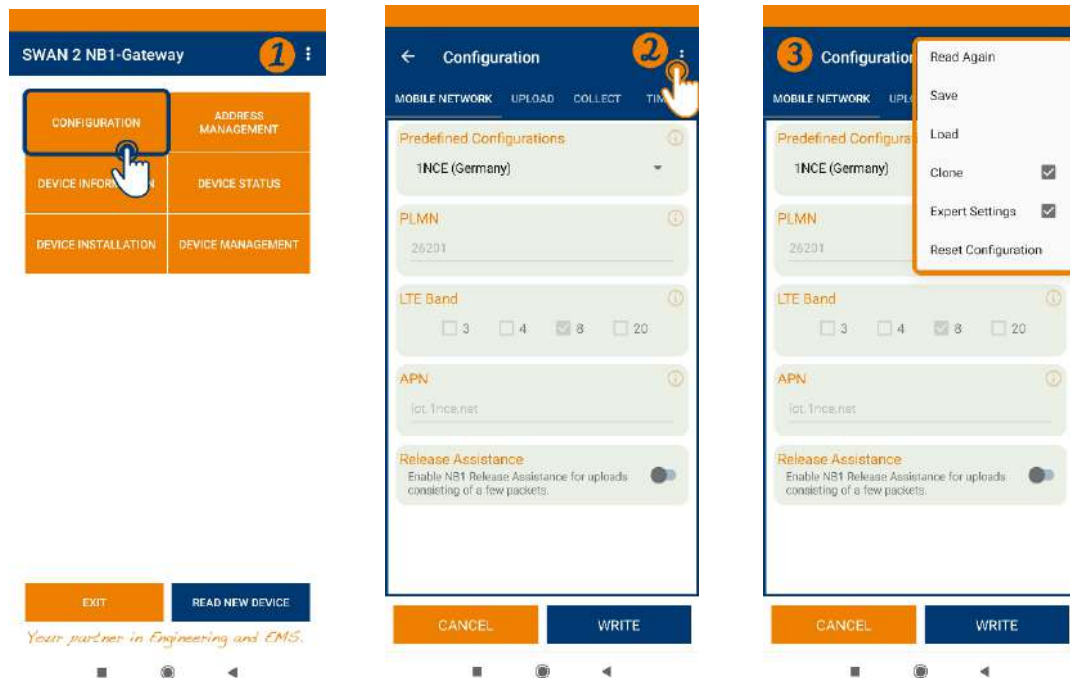


Figure 3: Save and load configuration (1)

1. Option

- a. Tap on **“Save”**
- b. Give your configuration a name and save it. The configuration is now saved in the app and can be transmitted to another device.
- c. To do this, go to **“Load”** and select the corresponding configuration, then tap on **“SELECT”**.
- d. Press **WRITE** to transmit the configuration to your device afterwards.

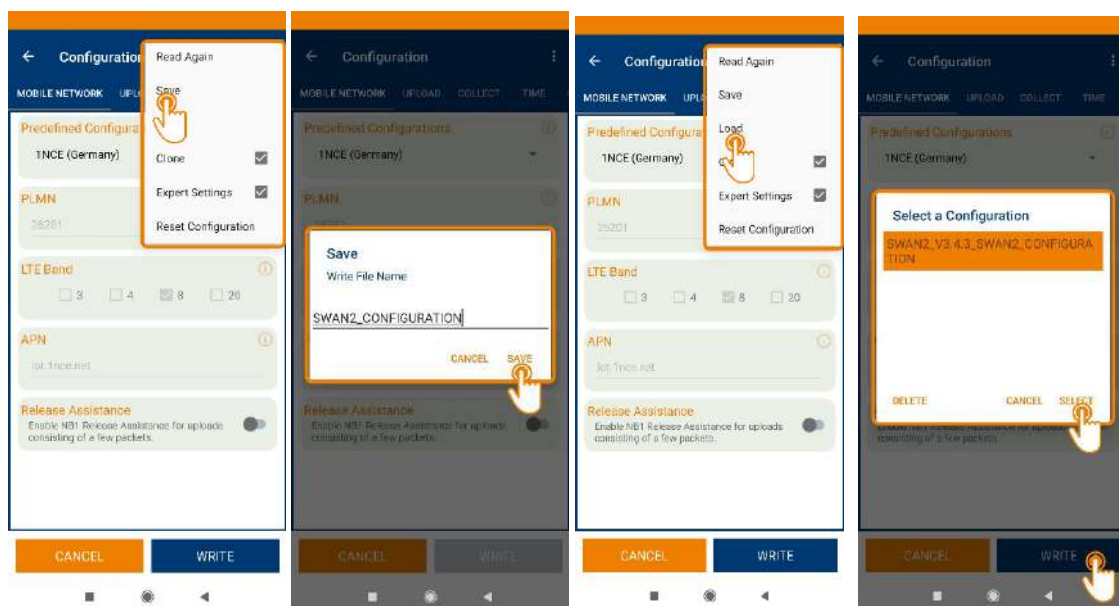


Figure 4: Save and load configuration (2)

2. Option

- Check the **“Clone”** box.
- Press **WRITE** to transmit the configuration to any device. The app remains in **“pairing-mode”** until you exit it with **CANCEL**.

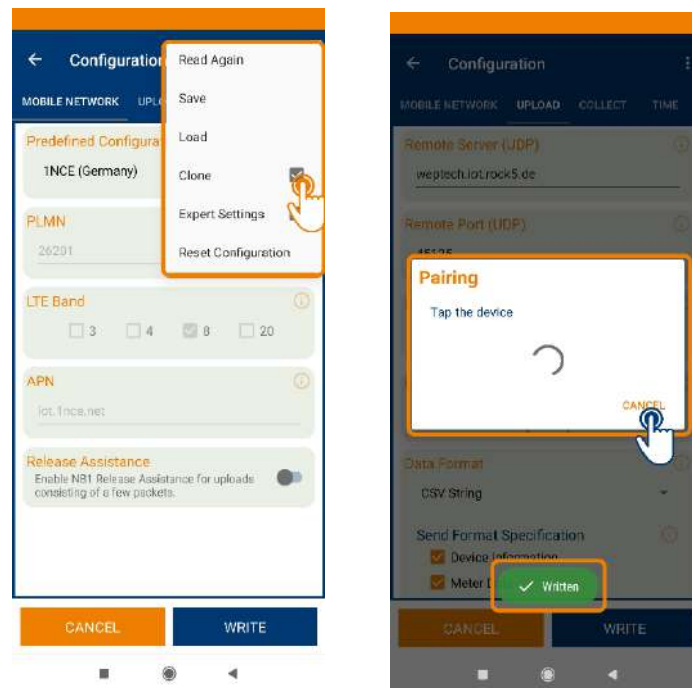


Figure 5: Clone configuration

Hint

- In order to “clone” the configuration onto several devices, all devices must be of the same variant and have the same firmware version.
- If the passwords differ between the devices, you will be prompted to enter the password of the current device.

4.4 Mobile network configuration

A functioning LTE Cat-NB1 cellular connection is required to receive device data and upload it to a server. The required parameters are configured as follows:

1. Go to **CONFIGURATION** in the main menu.
2. In the **MOBILE NETWORK** tab, select “Custom” under **Predefined Configurations**. The following parameters must now be entered according to the provider of the SIM card inserted (If necessary, ask your provider).
 - a. **PLMN** (Public Land Mobile Network): This parameter is optional, but should be set to optimize the dial-in process to the cellular network. This configured PLMN is preferred, but if dial-in with this PLMN is not possible and HPLMN or EPLMN lists are not set on the SIM automatic network selection will be enabled and indicated with bit 7 in the Status-Flags (see section 8.3.4). Germany has the following PLMNs:
 - i. **26201** for the network of Deutsche Telekom (also 1NCE)
 - ii. **26202** for the Vodafone network
 - b. **LTE band**: Normally, exactly 1 band should be selected here. For Germany this is:
 - i. **Band 8** for the network of Deutsche Telekom (also 1NCE)
 - ii. **Band 20** for the Vodafone network
 - c. **APN** (Access Point Name): This parameter must be set (in the event that you are using a private APN). For Germany this is:
 - i. **internet.nbiot.telekom.de** for the Deutsche Telekom network
 - ii. **iot.1nce.net** for the provider 1NCE
 - iii. **nb.inetd.gdsp** for the Vodafone network
 - d. **APN Credentials**: Access parameters for the APN can be provided here if an APN is configured. The Access parameters consists of a username and a password and have to be configured in the “Credentials” menu (section 4.10) beforehand.
 - e. **Release Assistance**: Enables the LTE Cat-NB1 Release Assistance for uploads consisting of up to three packets. This allows the device to disconnect faster from the LTE Cat-NB1 Network for small uploads, which increases power efficiency. Uploads consisting of more packets still require a slower disconnection process to ensure that all packets are transmitted to the LTE Cat-NB1 Network.
3. Alternatively, you can select preset settings for the respective provider under **Predefined Configurations**. All parameters are filled in automatically.



SWAN2 supports automatic network search if APN and PLMN are not configured. Automatic network search takes longer compared to providing APN and PLMN manually so the first connection to the network can take up to 15 minutes.

Press **WRITE** to apply the configuration and transfer it to the device. A new NFC connection may be required for this.

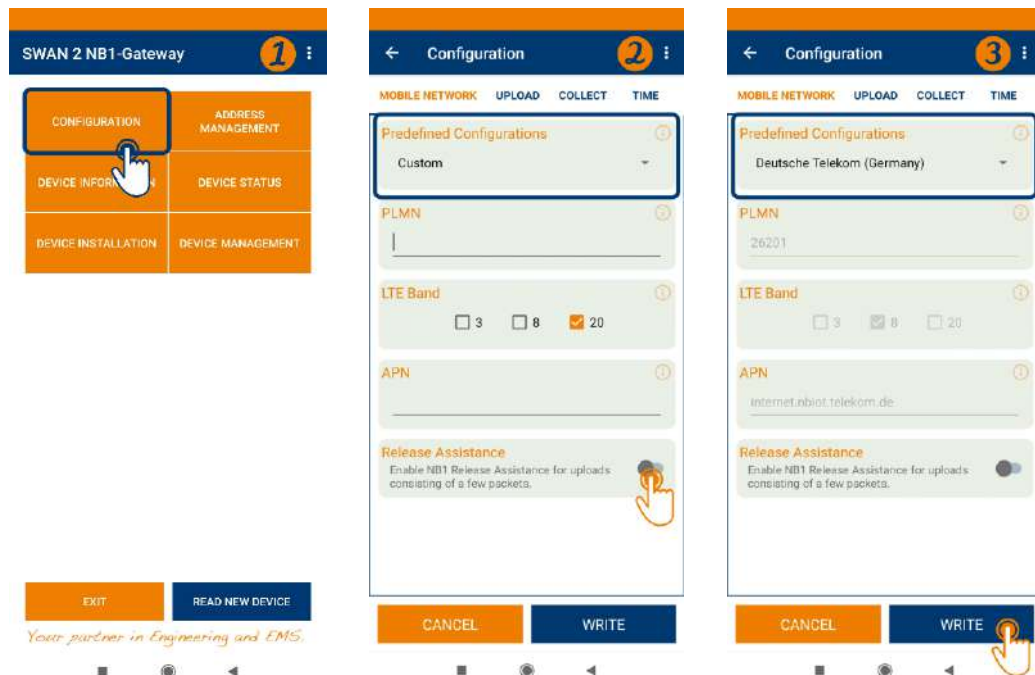


Figure 6: Configuration LTE Cat-NB1 network

Hint

The first dial-in process into the cellular network takes place during the synchronization of the device time. You can either do the dial-in process manually via the NFC app or press the reset button. For this purpose, go to the **DEVICE INSTALLATION** menu item and select **Set Device Time via NTP** (see section 4.12.1).

4.5 Configuration of transmission mode

In order to determine on which server and at what time the data should be transferred, the following parameters must be configured. Proceed as follows:

4.5.1 Server configuration

1. Go to **CONFIGURATION** in the main menu
2. The following server parameters must now be entered in the **UPLOAD** tab:
 - a. **Protocol**: The protocol for the data upload can be selected here. The protocols are described in detail in section 6.
 - b. **HTTP/S Upload Method**: If HTTP or HTTPS is selected as the upload protocol this parameter can be used to select the Request-Method for the data upload. See section 6.2.3 for more details.

- c. **LwM2M:** If LwM2M is selected as the Protocol additional parameters of the LwM2M client can be configured with the following settings:
- i. **Idle Time:** After registration of the client to the server the client is available for interactions for the time (in seconds) configured here. Each interaction resets this time. The connection quality and latency time has to be considered during configuration of this parameter. For energy efficiency a time of 10 to 15 seconds is recommended.
 - ii. **Notification Acknowledgement:** If this option is enabled, the client will send notifications with an acknowledgement request. The server has to acknowledge these notifications. This ensures that all send data arrived at the server, but also increases the energy consumption, due to the acknowledgement packet.
 - iii. **Notification Timeout:** Sets the wait time (in seconds) for an acknowledgement of the server after a notification.
 - iv. **Notification Retries:** Sets the maximum number of notification retries if no acknowledgement is received.
 - v. **Life Time:** Life Time in seconds of the LwM2M Client that is sent to the server during registration. This controls the intervals of the LwM2M pings, to show that the client is still available.
- d. **Credentials:** If HTTPS is selected as the upload protocol a username and password combination can be selected here so the device can authenticate itself when establishing the server connection (Basic Authentication). Additional details are described in section 4.10.
- If LwM2M is used as the protocol, the credentials are used as the PSK-ID and the PSK.
- e. **Remote Server:** The server for the data upload is provided here. Depending on the selected protocol a certain format is expected for the input. See section 6 for more information about the format.



Hint

It is recommended to provide the remote server as an IPv4 address (if the server has a known, static address) as this means no DNS-Query is required thus allowing to save energy.

- f. **Remote Port:** The port of the server the data will be sent to.
- g. **Local Port:** The port of the gateway the data will be sent from.
- h. **Upload Retries:** If this is configured, the device will automatically perform new upload attempts, if a regularly scheduled upload fails. An upload is considered to have failed, if not all the data can be uploaded (caused by a missing LTE Cat-NB1-connection or an unresponsive server). If there is a regular event scheduled before the planned retry to collect or upload data, the retry of the upload will be discarded. The retries are scheduled as follows:
 - First retry: Within 1 to 3 hours after the initially scheduled upload.

- Second retry: Within 3 to 7 hours after the initially scheduled upload.
 - Third retry: Within 7 to 15 hours after the initially scheduled upload.
- i. **Data Format:** The format of the data that will be uploaded can be selected here. The possible data formats depend on the selected protocol. The data formats are described in section 7.

Press **WRITE** to apply the configuration and transfer it to the device. A new NFC connection may be required for this.

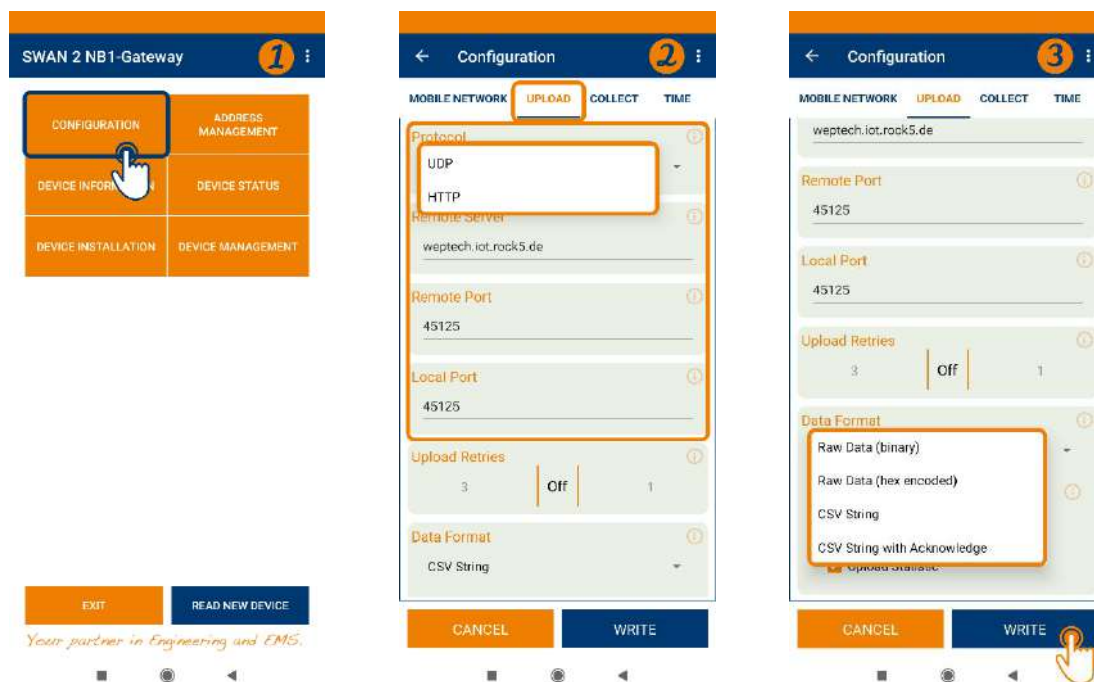


Figure 7: Configuration of transmission mode

Hint

The data is transmitted to your server using the configured protocol and selected data format. Make sure that your server can process the incoming data.

4.5.2 Configuration of the transmission interval



Hint

To configure events on a daily basis you have to activate the “**Expert Settings**”. Therefore press the 3 dots in the top right corner and check the box at “**Expert Settings**”.

However, the following must be considered:

1. **Battery-powered variants:** Frequent uploads will reduce battery life. The battery life of > 10 years is designed for operation of receiving and uploading data of the maximum number of telegrams twice per month.
2. Additionally the data volume of the used SIM card should also be considered before configuring frequent uploads.

In the **UPLOAD SETTINGS**, you can set the data upload interval.

1. With **Months** you can select the desired months.
2. With **Days** you can select the days for the event. There are two ways to define the days:
 - a. **Day of month based:** Configures the days of a month for the event.
 - b. **Day of week based:** Configures the weekdays and weeks of a month for the event. E.g. if Monday and Week 1 is selected the event will occur on the first Monday each month. This configuration is only possible if no days are configured for **Day of month based**.
3. With **Time**, you can set the start time (**Start Time**), the number of collection processes per hour (**Events per hour**) and the respective hours of the day (**Hours of day**).
4. With **Max. Event Delay (Minutes)** an additional time frame in minutes for the execution of the event can be configured. The event will occur at a random point in time within this time frame. The execution of the event will be delayed by a random time but at most by the value configured here. This can be used to prevent that multiple SWAN2 Gateways with identical configuration attach to the network and server at the same time and overload the network or server.

Example: If a daily upload is configured at 15:30 and **Max. Event Delay (Minutes)** contains a value of 120 minutes, the event will occur daily at any point in time between 15:30 and 17:30. The exact point in time will be random from day to day and device to device.

Press **WRITE** to apply the configuration and transfer it to the device. A new NFC connection may be required for this.



Figure 8: Configuration of the transmission interval

Hint

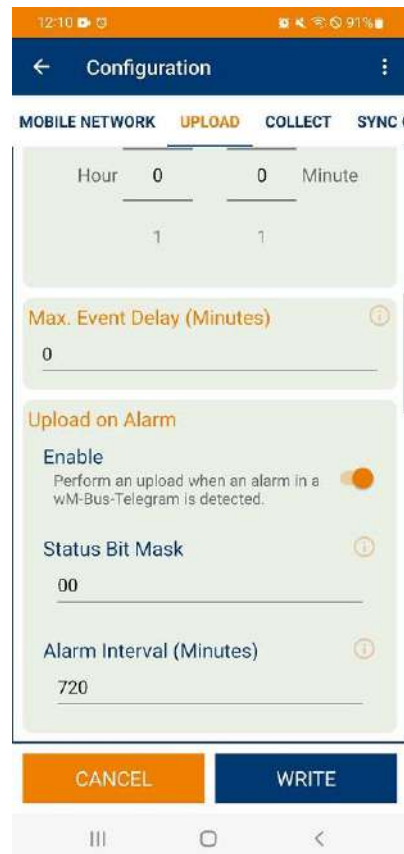
In the example shown above, the gateway transmits the data to the configured server every month (all months are selected), daily (“**Day of month**” all selected) and at each hour of the day (all hours of the day and one event per hour are selected).

Additionally to the time controlled uploads, it is also possible to perform an upload automatically if an alarm is detected in a wM-Bus-Telegram. To detect alarms the Status-Byte (see “Open Metering System Specification Vol. 2 – Primary Communication” Section 7.2.3) of each telegram is evaluated. The bits of Status-Byte show if there is abnormal behavior (alarm) in the device or if there are permanent or temporary errors and warnings for the power supply of the meter. Other bits are reserved for the manufacturer. The alarm detection of the gateway can be configured as follows:

- Enable:** This parameter enables the alarm detection. If alarm detection is disabled, all following parameters are not shown and have no effect.
- Status Bit Mask:** This parameter controls how the alarm is detected. To be able to detect multiple independent error states in the Status-Byte the parameter configured here is a mask that is combined with the Status-Byte of the incoming telegrams. If the result of this operation is not 0 an alarm is detected and an upload is performed.

To trigger an alarm message both Status-Bits in the Status-Byte have to be set. The Gateway ignores the Status-Bits if only one Status-Bit 0 or Status-Bit 1 is set, as this shows an error in bidirectional communication. A mask of 0x01, 0x02, or 0x03 configures the same behavior: The upload is performed if both Status-Bits in the Status-Byte are set. For every other bit in the Status-Byte the assignment is distinct.

- c. **Alarm Interval (Minutes):** After an alarm is detected the next alarm can only be detected after the time in minutes defined here has passed.



12:10 91%

← Configuration

MOBILE NETWORK **UPLOAD** COLLECT SYNC

Hour 0 Minute 0

1 1

Max. Event Delay (Minutes) 0

Upload on Alarm

Enable
Perform an upload when an alarm in a WM-Bus-Telegram is detected. ☒

Status Bit Mask 00

Alarm Interval (Minutes) 720

CANCEL WRITE

Figure 9: Upload on alarm detection

4.6 Configuration of continuous receive mode

In the **COLLECT** settings, you adjust the parameters for the continuous receive mode of the SWAN2.

In this mode, the gateway will activate the receiver at configurable times for a certain duration or until a certain number of telegrams were received. The continuous reception mode is suited for frequent readings (e.g. 12 times a day) for a large number of meters with a short transmission interval (< 30 seconds) or also for infrequent readings (e.g. 2 times a month) of a large number of meters with a long transmission interval (> 5 Minutes). If frequent readings of a specific meter are required the synchronous receive mode (see section 4.7) can be used to conserve energy for battery-powered variants of the gateway. The continuous receive mode is only active when the synchronous receive mode is disabled.

The continuous receive mode has the following configuration options:

4.6.1 General receive mode

1. Go to **CONFIGURATION** in the main menu.
2. In addition to various parameters, two different events can also be configured independently of one another in the **COLLECT** tab. For example, devices in S-Mode and T&C Mode can be collected. To do this, go to **EVENT 2** and activate it. The configured parameters are copied from **EVENT 1** to **EVENT 2**.
3. The following parameters can be adjusted here:
 - a. **wM-Bus Mode**: Set the wM-Bus Mode that should be collected by the device.
 - b. **Use Whitelist as stop condition**: This option allows to stop data collection after a telegram was received by each of the wM-Bus-Meters that are part of the Whitelist. If a wM-Bus-Meter in the Whitelist sends more than one telegram with a different lengths and all of them should be received, this parameter cannot be used. The same applies to a Whitelist that contains entries with Wildcards. In both of this cases this parameter, the **Max. Number of Telegrams** parameter, has to be used to manually configure the number of telegrams that should be received, before the data collection can stop.
 - c. **Max. Number of Telegrams**: Enter a value between 1 and 250 (SWAN2-C). This parameter saves energy by allowing the device to end receive mode before the receiving time configured below is reached. The number of telegrams includes the number of sources (wM-Bus-Meter) as well as the number of telegrams send by each of the sources.
 - d. **Duration (Seconds)**: Duration of the data collection in seconds. The minimum value is 15 seconds. This parameter depends on the transmission interval of the devices that should be received. It should be twice as long as the longest transmission interval of the wM-Bus-Meters d, as collisions of telegrams cannot be ruled out.
 - e. **Min. RSSI Limit (dBm)**: The device will not collect wM-Bus telegrams that are received with an RSSI lower than this value. A higher threshold improves reception performance in noisy environments. *This option is only available if "Expert settings" are enabled and should only be changed if there is a problem with receiving the wM-Bus telegrams.*
 - f. **DLL**: This option can improve the reception of wM-Bus-Devices in T-Mode in a noisy environment. However the tolerance to deviations to the nominal data rate of 100kcps

is reduced so it has to be ensured that the wM-Bus-Devices, which should be received by the SWAN2, send with a data rate of 100kcps. *This option is only available if “**Expert settings**” are enabled and should only be changed if there is a problem with receiving the wM-Bus telegrams due to interference in noisy environments.*

- g. **Upload after Collect:** This option can be enabled to upload the data to the configured server immediately after the collection event is done.
- h. **Append:** If this option is disabled, each collection event will clear previously collected data before starting to collect data. If this option is enabled and multiple collection events are configured before an upload event, each collection event will append collected data to the data of previous collection events. The collected data is cleared after the upload. There is still a limit of 250 (SWAN2-C) wM-Bus-Telegrams in the storage of the device. If this limit is reached, no further data can be stored and the collection event will stop immediately.
- i. **Keep data on failed upload:** If the **Append** option is activated, this option can also be activated. If an error occurs during the planned upload, the data will still be kept in the cache. Data from further collections is then added. The next time the upload is successful, the data from the failed upload will also be uploaded. The above mentioned limit of 250 (SWAN2-C) wM-Bus telegrams still exists.
- j. **Storage Interval (Hours):** If the **Append** option is activated, this parameter can be used to define the maximum validity period in hours of meter telegrams in the telegram storage. If telegrams of a meter are already in the memory before a collection event and a further collection event is carried out, then telegrams of this meter are only stored if the most current telegram of this meter in the memory is older than the time defined here. Example: If there is a collection event once per week and an upload event every two weeks and this parameter is configured to 336 hours (2 weeks), only the first received telegram of each meter is stored and uploaded. This means, if a meter could be received during the first collection event, the telegrams of this meter will be ignored in the second collection event, as long as the time configured here did not pass since the last reception of the meter telegram.



Example for configuration continuous receive mode:

- Telegrams of 5 wM-Bus-Meters should be received
- All 5 meters are included in the Whitelist
- Longest transmission interval (of all five meters) is 28 seconds
- 3 of the meters send 2 telegrams with different lengths

With the conditions from above, the following settings should be used to keep the energy consumption during the receive mode at a minimum:

- **Use Whitelist as stop condition:** Disabled

This option cannot be used as there are meters that send more than one telegram.

- **Max. Number of Telegrams:** 8

A total of 8 telegrams have to be collected if 2 of the 5 meters send one telegram and the other 3 meters send 2 telegrams ($2 \times 1 + 3 \times 2$).

- **Duration (Seconds):** 60 seconds

The longest transmission interval is 28 seconds. In order to reduce the probability of telegram collisions during the reception period and to ensure that all telegrams will be received, this parameter should be set at least twice as long as the longest transmission interval.

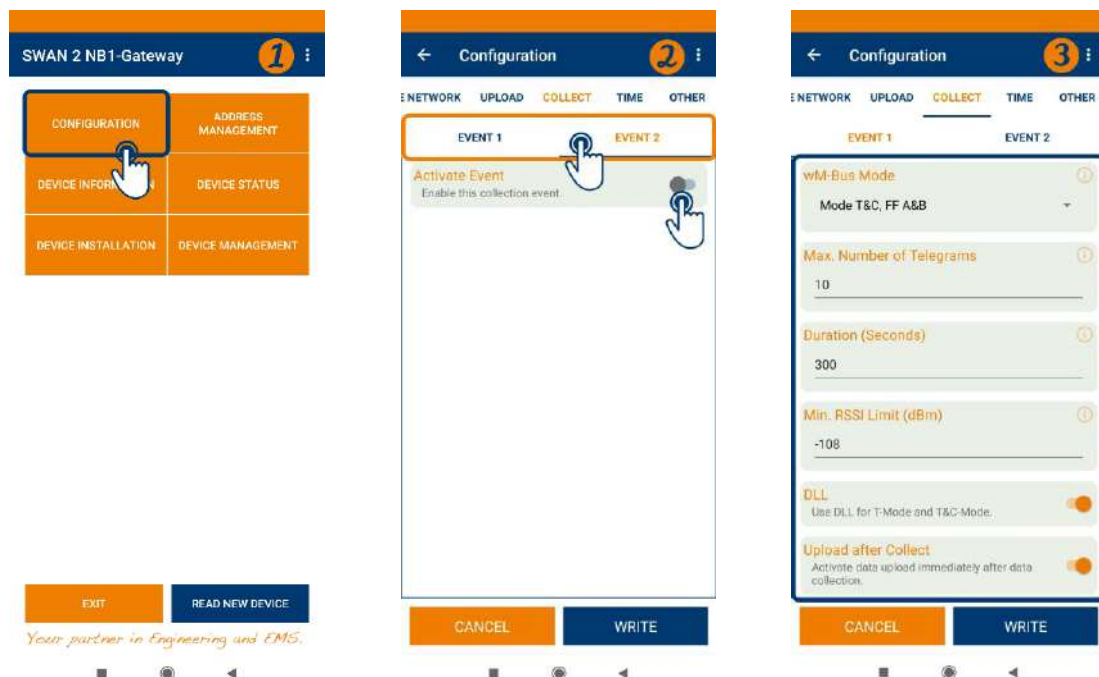


Figure 10: Configuration of receive mode

Press **WRITE** to apply the configuration and transfer it to the device. A new NFC connection may be required for this.

4.6.2 Receive mode interval



Hint

To configure events on a daily basis you have to activate the “**Expert Settings**”. Therefore press the 3 dots in the top right corner and check the box at “**Expert Settings**”.

However, the following must be considered:

1. **For battery-powered variants:** Frequent and/or long readings of meters will reduce battery life. The battery life of > 10 years is designed for operation of receiving and uploading data twice per month.
2. Additionally the data volume of the used SIM card should also be considered before configuring frequent uploads.

In the **COLLECT** settings, you also have the option of setting the interval for receiving.

1. With **Months** you can select the desired months.
2. With **Days** you can select the days for the event. There are two ways to define the days:
 - a. **Day of month based:** Configures the days of a month for the event.
 - b. **Day of week based:** Configures the weekdays and weeks of a month for the event. E.g. if Monday and Week 1 is selected the event will occur on the first Monday each month. This configuration is only possible if no days are configured for **Day of month based**.
3. Under **Time** you can set the start time (**Start time**), the number of collection processes per hour (**Events per hour**) and the respective hours of the day (**Hours of the day**).
4. With **Max. Event Delay (Minutes)** an additional time frame in minutes for the execution of the event can be configured. The event will occur at a random point in time within this time frame. The execution of the event will be delayed by a random time but at most by the value configured here. This can be used to prevent that multiple SWAN2 Gateways with identical configuration attach to the network and server at the same time and overload the network or server.

Example: If a daily upload is configured at 15:30 and **Max. Event Delay (Minutes)** contains a value of 120 minutes, the event will occur daily at a point in time between 15:30 and 17:30. The exact point in time will be random from day to day and device to device.

Press **WRITE** to apply the configuration and transfer it to the device. A new NFC connection may be required for this.



Figure 11: Configuration of the receive mode interval

Hint

In the example shown above, the gateway transmits the data to the configured server every month (all months are selected), daily (all days of month are selected) and at each hour of the day (all hours of the day and one process per hour are selected).

4.7 Configuration of synchronous receive mode

The **SYNC COLLECT** settings allow the configuration of the synchronous receive mode. If the synchronous receive mode is enabled, the continuous receive mode is disabled.

In contrast to the continuous receive mode, the gateway does not receive for a fixed period of time in synchronous receive mode, but only for a fraction of a second if a meter with which synchronicity has previously been established carries out a synchronous telegram transmission. This makes it possible to receive meters with a long transmission interval (> 2 minutes) relatively frequently (e.g. 2 times per hour) and to use significantly less energy compared to continuous reception, which increases the battery life of battery-powered variants. The disadvantage, however, is that the number of meters that can be received in synchronous receive mode is significantly limited compared to continuous receive mode. Synchronous reception also only works in wM-Bus modes T and C. Section 7 contains additional information on synchronous receive mode.



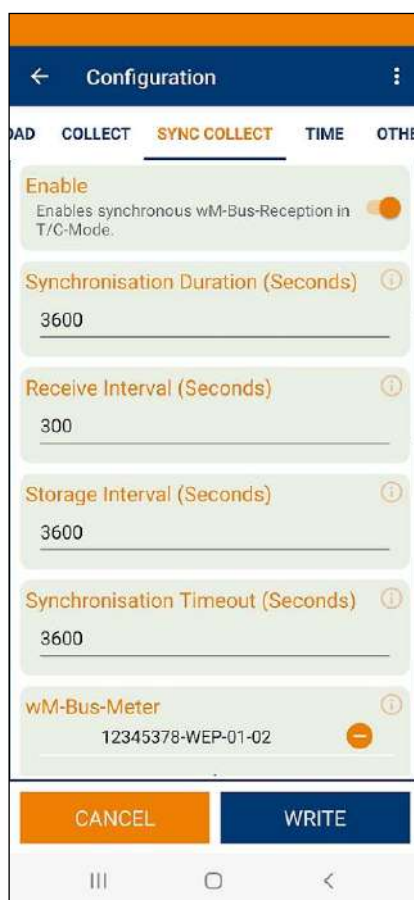
Hint

Before synchronicity can be established with a meter, it is imperative that the device time of the gateway is set.

1. Select **CONFIGURATION** in the main menu.
2. The following settings are available in the **SYNC COLLECT** tab.
 - a. **Enable:** Activates the synchronous receive mode. All of the following parameters are only displayed if this parameter is active. Continuous receive mode is disabled when this parameter is active. After this parameter has been enabled, the gateway will start a synchronization process 5 seconds after going into standby mode from configuration mode.
 - b. **Synchronization Duration (Seconds):** The maximum duration for a sync operation in seconds. To establish synchronization, a synchronization process must be carried out in which two synchronous telegram transmissions from the desired meter are received. Accordingly, this parameter must be configured to be at least twice as long as the transmission interval of the meter so that synchronization with the meter can be established.
 - c. **Receive Interval (Seconds):** Time in seconds that must pass after reception of the last synchronous telegram from a meter before the gateway carries out a synchronous telegram reception again. Not every synchronous telegram transmission has to be received in order to maintain synchronization with the meter. By using this parameter, it is also possible to receive meters with a relatively short transmission interval (< 30 seconds) energy-efficiently in synchronous reception mode. A value of 290 seconds is recommended. With the recommended value every 5th transmitted telegram is received from a meter with a transmission interval of 60 seconds.
 - d. **Storage Interval (Seconds):** Time in seconds that must elapse since the last telegram stored for transmit operation before the currently received telegram is stored. With a value of 3600 seconds, one telegram of the meter is stored per hour, even if the synchronous receive operation is performed more frequently to

maintain synchronization. The data size for the send operation is thus defined via this parameter.

- e. **Synchronization Timeout (Seconds):** If no synchronous telegram of a meter is received during this time in seconds, the synchronicity to the meter is considered to be interrupted and a new synchronization attempt is made.
- f. **wM-Bus-Meter:** Address of the counter to which synchronism is to be established. The format of the meter address is described in section 4.11.2. Wildcards are not permitted. Specifying a meter address is mandatory when synchronous receive mode is activated.



The screenshot shows a mobile application interface for configuring a device. The title bar is orange with a back arrow and the word 'Configuration'. Below the title bar is a navigation bar with tabs: 'READ', 'COLLECT', 'SYNC COLLECT' (selected), 'TIME', and 'OTHER'. The main content area has a light green background and contains several settings:

- Enable:** A toggle switch is turned on. Below it, the text reads: 'Enables synchronous wM-Bus-Reception in T/C-Mode.'
- Synchronisation Duration (Seconds):** A text input field containing '3600'.
- Receive Interval (Seconds):** A text input field containing '300'.
- Storage Interval (Seconds):** A text input field containing '3600'.
- Synchronisation Timeout (Seconds):** A text input field containing '3600'.
- wM-Bus-Meter:** A text input field containing '12345378-WEP-01-02'.

At the bottom of the screen are two buttons: 'CANCEL' (orange) and 'WRITE' (blue). Below the buttons is a standard Android navigation bar with three icons: a square, a circle, and a triangle.

Figure 12: Configuration of synchronous receive mode

Press **WRITE** to apply the configuration and transfer it to the device. A new NFC connection may be required for this.

4.8 Time setting

For the synchronization of the time stamp of the gateway via internet, the corresponding NTP (Network Time Protocol) server must be entered in the configurations. To do this, proceed as follows:



Hint

A functioning cellular connection is required for synchronization with the NTP server. It must be configured as described in section 4.4.

1. Go to **CONFIGURATION** in the main menu
2. The following parameters must be entered in the **TIME** settings tab.
 - a. **NTP Server**: The IPv4 or the domain name of the NTP-Server.
 - b. **NTP Auto Sync (Days)**: Indicates after how many days the time in the device should be synchronized again with the configured NTP server. Automatic time synchronization is only performed after an upload. If the value is "0", there is no automatic synchronization.
 - c. **NTP port**: The port of the NTP Server (NTP-Default is 123).
 - d. **Time Zone (UTC offset)**: The offset of the device time to UTC can be selected here.
 - e. **Enable Daylight Saving Time**: The automatic change between winter and summer time can be activated here.
 - f. **Device Time**: Current time of the device.

Press **WRITE** to apply the configuration and transfer it to the device. A new NFC connection may be required for this.

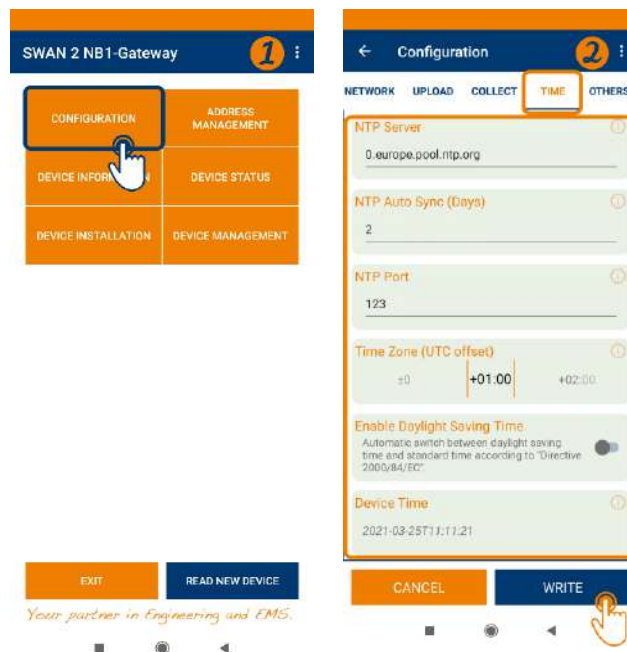


Figure 13: Configuration Time Setup

4.9 Additional configuration options

1. Go to **CONFIGURATION** in the main menu.
2. Under **OTHER** you have the following configuration options:
 - a. **Device Tag:** additional information / identification can be entered in this field. This information (e.g. location) is transmitted in the CSV string (see section 8.3) and can be read out. This might be helpful to identify the device on a server.
 - b. **Quiet mode:** If this is enabled all LEDs will show no activity when the device starts a process to collect or upload data due to a configured event. During configuration of the device via the NFC-Configurator-App or when starting a process manually (e.g. via the NFC-Configurator-App or by pressing the Reset-Button) the LEDs will always show activity no matter if Quiet-Mode is enabled or not.
 - i. Deactivated: blue LED flashes briefly every 20 seconds
 - ii. Activated: blue LED does not flash
 - c. **Fast NFC Installation:** If this option is enabled, the device will start the Device Installation modes “Set device time via NTP”, “Collect Data” and “Upload Data” when it is in Shipping Mode (see section 3.4.2) and an NFC-Field is put near the device for 10 seconds. The blue LED will blink once per second during the 10 seconds. After the 10 seconds pass, the red and blue LED will light up slowly to indicate that the installation mode was started.
 - d. **Activate UART Interface:** If this option is enabled, the UART Interface on the board of the device can be used for configuration. This option should be disabled for productive use.
 - e. **Autostart After Power-On:** This option allows the activation of the SWAN2 Gateway right after turning the device on (placing the power jumper). If this option is enabled, the device will not enter Shipping Mode after power-on but instead synchronize device time and perform a data collection and upload. The device will be ready to process the configured events.
 - f. **Clear Status Flag:** If this option is active, then the status and debug flags of the gateway will be reset after a successful upload.
 - g. **wM-Bus CI-Field Blacklist:** A blacklist for certain CI-Field values can be provided here. This blacklist can hold up to four values. Received wM-Bus Telegrams that have one of the CI-Field values provided here ,will be discarded. An entry is made in hexadecimal format.
 - h. **Prefilter Devicetype:** With this, it is possible to receive only meters of a certain device type. All other device types are ignored and also not included in the radio scan list. Up to four device types can be configured. If all fields are empty, this filter is disabled.
 - i. **Prefilter Manufacturer:** This filter allows to receive only wM-Bus meters from manufacturers configured here. Meters from other manufacturers are ignored and also not included in the radio scan list. Up to four manufacturers can be configured. If all fields are empty, this filter is disabled.

Hint

The prefilters (**Prefilter Devicetype** and **Prefilter Manufacturer**) take effect before the radio scan list and before the whitelist. If these prefilters are active, only meters that match this prefilter are received and processed further, and only these meters are added to the radio scan list. In contrast to whitelist filtering, this allows filtering of the radio scan list created in the background and thus reduces the size of the radio scan list to the relevant meters.



Figure 14: Additional configuration parameters

4.10 Credentials

In this menu account, credentials consisting of a username and a password can be created and transferred to the device. The credentials can then be used by the device for authentication to the server if an upload protocol is selected that has such a feature (e.g. HTTPS or LwM2M).

The Plus-Symbol has to be pressed to create new Credentials. The username and the password have to be provided in the popped up dialog. After pressing **Add**, the dialog will be closed and the created credentials will be shown. The username is shown plaintext while the password is concealed. Up to four credentials can be created in this way. Each credentials entry has an index (1 to 4). Existing credentials can be deleted by pressing the Minus-symbol.

After modification of the credentials, they have to be written to the device using the **WRITE** button. The created credentials can then be selected in the **UPLOAD** settings in the **CONFIGURATION** menu.

If the credentials should be used for LwM2M, the user name is used as the PSK-ID and the password as the PSK. The password has to be provided as a hexadecimal string. There is no minimum length for the PSK. Example for PSK:

0102030405060708090A0B0C0D0E0F



Figure 15: Credentials Menu

4.11 Address Management

It is possible to configure which wM-Bus-Meters are collected by the SWAN2. This is done via **ADDRESS MANAGEMENT**, where specific wM-Bus-Meters can be added to a “positive list” (Whitelist). Only wM-Bus-Meters in the Whitelist will be processed further during data collection.

4.11.1 Manually adding a device to the whitelist

1. Go to **ADDRESS MANAGEMENT** in the main menu.
2. Press the three dots in the upper right corner and then “**Add wM-Bus Device**”.
3. A window now opens in which you can enter the wireless M-Bus address of your device. (The format is explained in section 4.11.2). When all relevant data has been entered, press “**ADD**”.
4. The device then appears in the list and must now be written to the device.

Press **WRITE** to apply the configuration and transfer it to the device. A new NFC connection may be required for this.

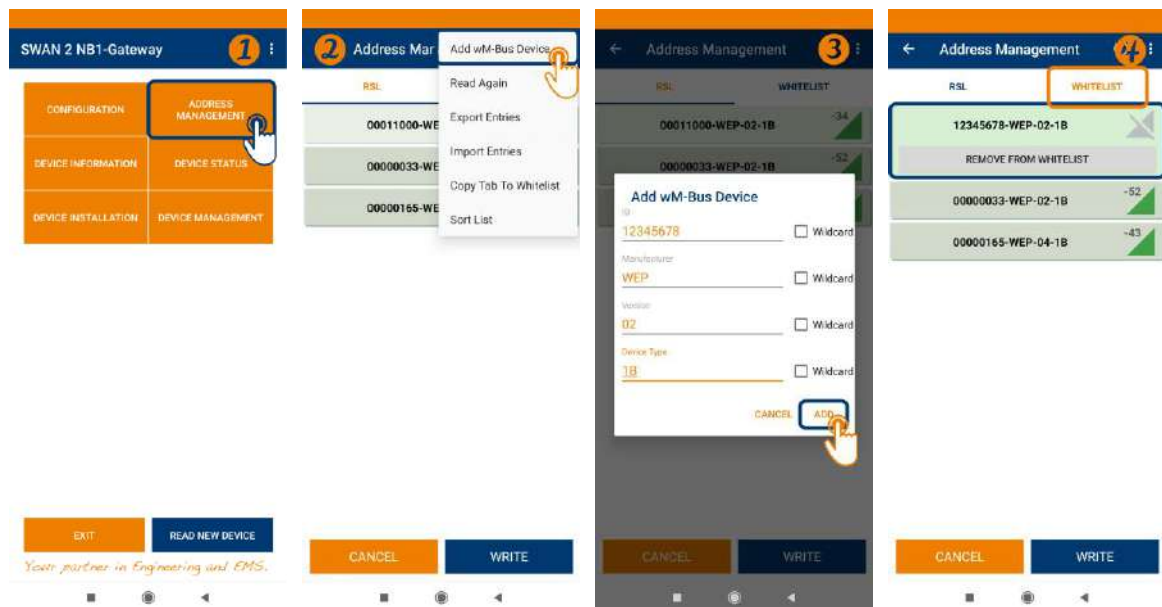


Figure 16 Add wireless M-Bus devices



As soon as only one single entry is created in the whitelist, all meters without a matching entry are discarded!

4.11.2 Description of the wireless M-Bus address

ID	-	Manufacturer	-	Version	-	Device type
[XXXXXXXX]	-	[MMM]	-	[VV]	-	[DD]

Parameter	Description	Example
ID	The ID (serial number) of the wM-Bus meter, consisting of 8 digits in the range of 0 to 9.	01234567
Manufacturer	The manufacturer of the wM-Bus meter, consisting of 3 letters in the range of 'A' to 'Z' (see also https://www.dlms.com/flag-id).	WEP
Version	The version of the wM-Bus meter in hexadecimal notion, consisting of 2 characters of digits in the range of 0 to 9 and letters in the range of 'A' to 'F' (upper- and lowercase).	8B
Device type	The device type of the wM-Bus-Meter in hexadecimal notion, consisting of 2 characters of digits in the range of 0 to 9 and letters in the range of 'A' to 'F' (upper- and lowercase).	C1

Table 1: Description of the wireless M-Bus address components

4.11.3 Wireless M-Bus device with Wildcard

Each of the four parts (serial number, manufacturer, version, device type) of the wM-Bus-meter-address can be replaced with a wildcard, which is represented as a '?'. In this case, this component is ignored in the address comparison.

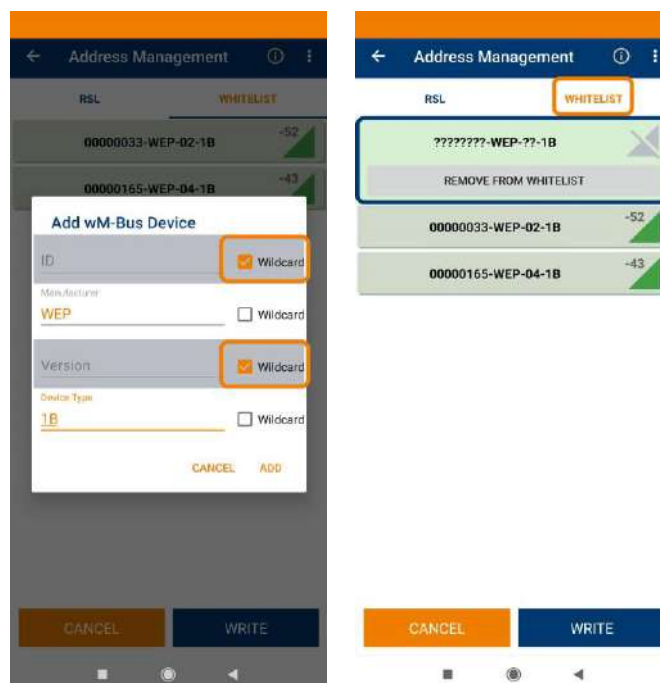


Figure 17: Description Wildcard

In the example shown above, all devices from the manufacturer “WEP” with device type “1B” are collected.

4.11.4 Radio Scan List (RSL) & Whitelist

The Radio Scan List can be used to create a list of all wireless M-Bus / OMS devices within range. The RSL can be created manually. This process is described in section 4.12.4.

Additionally the Radio Scan List is updated during every data collection event. Addresses of meters that are not in the Radio Scan List will be appended to the current Radio Scan List. If a Whitelist is configured, only the telegrams that match the Whitelist will be stored for the upload to the server. But the Radio Scan List will contain the address of each meter that was received during the data collection. If a data collection event is triggered manually (e.g. via the NFC-Configurator-App), the Radio Scan List is cleared before data collection.

The Radio Scan List can hold a maximum of 450 entries. If more meters are received than can fit into the Radio Scan List the oldest entries will be removed.

1. The lists can then be viewed in **ADDRESS MANAGEMENT**. There is also the option of adding devices from the Radio Scan List (**RSL**) to the **WHITELIST**.
2. Go to “Address Management” in the main menu.
3. Go to **RSL**. All devices within range will be displayed. Select the relevant devices and transfer them to the whitelist with “Add to Whitelist”
4. Go to “**WHITELIST**”. The device selected in step 2 now appears in the whitelist.

Press **WRITE** to apply the configuration and transfer it to the device. A new NFC connection may be required for this.



Figure 18: RSL & Whitelist

4.11.4.1 Save and load Whitelist

You have the option of saving a whitelist from one device and loading it onto another device, for example. This means that a whitelist can also be created manually and loaded onto a device. This is described below:

Go to **ADDRESS MANAGEMENT** and touch the 3 dots in the top right corner. In the opening Drop-Down menu you can choose **“Export Entries”** to save the created whitelist locally to your android device. With **“Import Entries”**, you can load a saved or a manually created whitelist. The description for the manually created whitelist can be found below.



Figure 19: Save and load whitelist

In order to load a whitelist, a text file (*.txt) has to be created. All wM-Bus addresses of the required meters are filled in as shown in Figure 20. Each line represents a new entry in the whitelist. You can find more information about the wM-Bus address in chapter 4.11.2. By adding a “#” in a line, a comment can be added which will be ignored while loading the whitelist to the device.

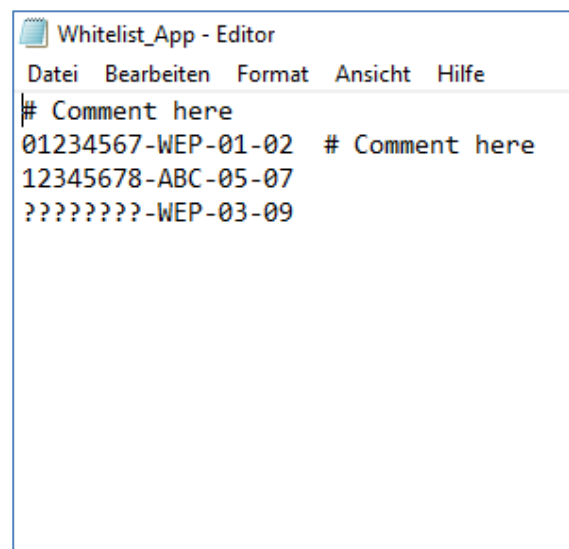


Figure 20: Format Whitelist

4.12 Device Installation

In the course of installing the device, there is the option of starting various actions manually and consequently, verifying the correct functionality of the device. These different options are described below.

To carry out the above actions, proceed as follows:

1. To do this, go to **DEVICE INSTALLATION** in the main menu.
2. Check the box for the action you want to perform and tap **EXECUTE**.

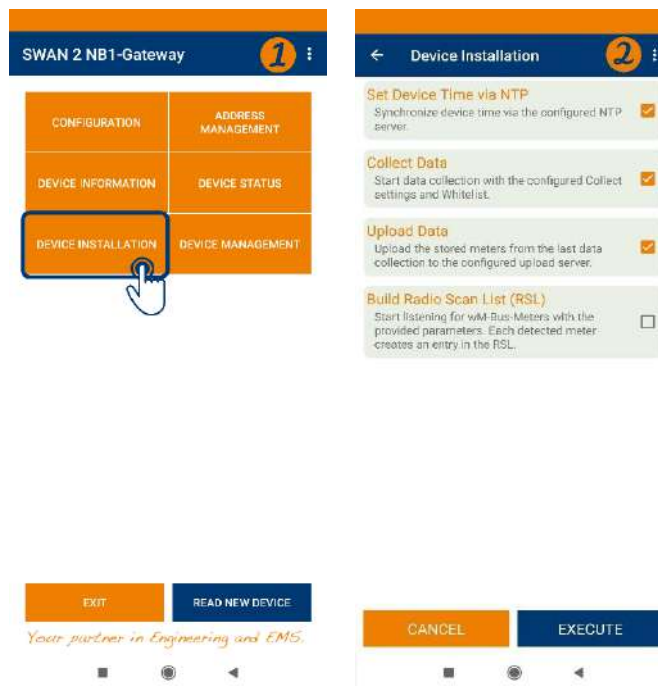


Figure 21: Device Installation

After an action has been started, the LEDs on the SWAN2 flash according to the operating status. After all actions have been completed, the LEDs are inactive.

4.12.1 Set device time via NTP

This function allows the synchronization of the SWAN2 device time via the NTP server. The time settings are used for this. A working LTE Cat-NB1 connection is required. The synchronization can be checked in the main menu under **DEVICE STATUS** or in **CONFIGURATION** under **TIME SETUP**.

4.12.2 Receive mode (Collect Data)

SWAN2 collects data via the wM-Bus interface. The parameters entered in the Collect configurations (see section 4.6) and in Address Management are used for this. The data will be saved until the next transmission.

4.12.3 Transmission mode (Upload Data)

SWAN2 starts transmitting using the parameters entered in the upload configurations (see section 4.5). The last saved data is uploaded. A working LTE Cat-NB1 connection is required.

4.12.4 Build Radio Scan List (RSL)

The “Build Radio Scan List” function creates a list of all wireless M-Bus devices within range. This list can be requested in the main menu under **ADDRESS MANAGEMENT**. The devices shown can also be transferred to the whitelist. The behavior of the LEDs in this mode corresponds to the behavior in receive mode.

After the selection of this action, additional parameters are shown to configure the scan process for the Radio Scan List:

- d. **Listening Period:** This sets the time in minutes that the device will be in received mode to create the Radio Scan List.
- e. **wM-Bus Mode:** The wM-Bus-Mode that should be used for the creation of the Radio Scan List.
- f. **Apply Whitelist:** If this option is disabled all wM-Bus-Meters will be added to the Radio Scan List, no matter if they are part of the Whitelist or not. Enabling this option will only add meters to the Radio Scan List, which are also part of the Whitelist. This can be used to check if all meters in the Whitelist can be received.
- g. **Append:** If this option is disabled, the Radio Scan List will be cleared before the start of a scan process for generation of a new Radio Scan List. After enabling this option, the Radio Scan List will not be cleared and new wM-Bus-Meters will be appended to the current Radio Scan List.

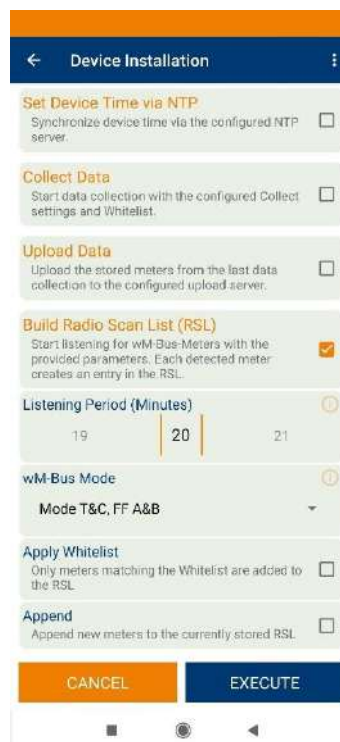


Figure 22: Parameters for Build Radio Scan List

4.13 Device Status

Further information about the device (A) and the LTE Cat-NB1 connection (B) can be viewed in **DEVICE STATUS**

1. Go to the **DEVICE STATUS** menu item.
2. You will find the relevant information in the overview
 - a. **General Information:** Here you can find information such as article number, firmware version, battery voltage or the temperature of the device. The displayed time stamp ("Timestamp") is the device time at which the values for battery voltage and temperature were recorded. This also contains a report about the self-test. Note that the self-test is only performed on initial power-up of the device after closing of the power-jumper.
 - b. **NB1 Status:** The LTE Cat-NB1 connection can be reviewed here. The time stamp indicates the last time the LTE Cat-NB1 connection was established. Signal strength (RSRP, RSRQ and RSSI) and other parameters can also be viewed. If there is no LTE Cat-NB1 connection, "No connection" is displayed.
 - c. **Last Upload Status:** Contains information about the State of the last upload.
 - d. **WM-Bus Sync Status:** Information about synchronous receive operation is displayed here. In addition to the current state, a counter is also displayed, which is incremented if the synchronicity to the meter was interrupted (resets after a change of configuration).
 - e. **Sensor Status:** Information about battery voltage and temperature of the gateway.



Figure 23: Device Status

4.14 Change Password

A password is required to connect to the device. (The preset password is “0123”). This password can and should be changed in the settings. Proceed as follows:

1. Go to the main menu of the App.
2. Select the Lock symbol at the top of the main menu.
3. Enter the old password and your newly selected password (The password must consist of at least 4 and a maximum of 15 characters.)
4. The password also can be removed. Therefore touch the 3 dots in the top right corner and check the box at “**Remove Password**”.

Press **WRITE** to apply the configuration and transfer it to the device. A new NFC connection may be required for this.

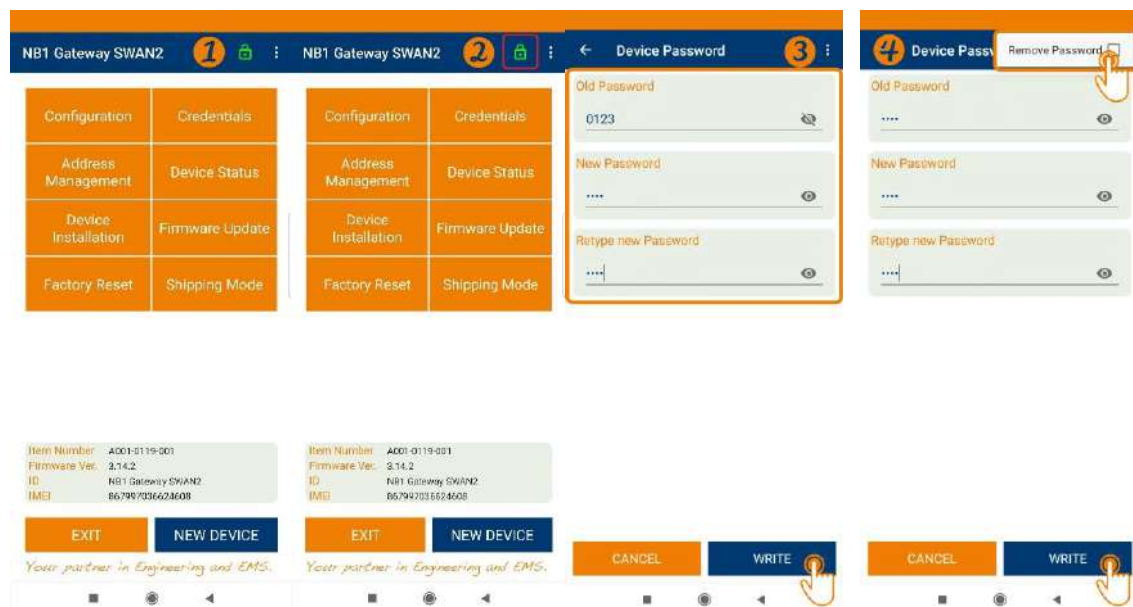


Figure 24: Change password

4.15 Firmware Update

You can update the firmware using the NFC app.

1. Go to the main menu of the App.
2. Go to **FIRMWARE UPDATE**.
3. Here you can choose between 3 variants. With "Check/Browse"
 - a. **Built-in**: Use the firmware version that is part of the NFC-Configurator-App. Each release of the NFC-Configurator-App contains the latest firmware for the device at the time of the release of the App.
 - b. **Online**: Look online (Internet access required) for a new firmware version for the device.
 - c. **Local**: Select a local firmware file for the update. This option is only required in exceptional cases.
4. You can also downgrade the firmware version. Therefore touch the 3 dots in the top right corner and check the box at "**Allow Downgrade**" and confirm with "**Proceed**". After that choose one of the above mentioned options to be able to perform a downgrade.

Press **WRITE** to apply the configuration and transfer it to the device. A new NFC connection may be required for this.



Hint

The NFC-Touchpoints of your devices must remain connected until the update was completely transferred to the gateway. A progress indicator is displayed.



Figure 25: Firmware Update

Hint

The latest firmware update will always be available online and can be checked and downloaded to the device using the “**Online**” function.

4.16 Activate Shipping Mode

This menu allows to activate the Shipping Mode of the device. For more information about the Shipping Mode see section 3.4.2.

1. Go to the main menu of the App.
2. Go to **SHIPPING MODE**.
3. Press **ACTIVATE** to activate the shipping mode.

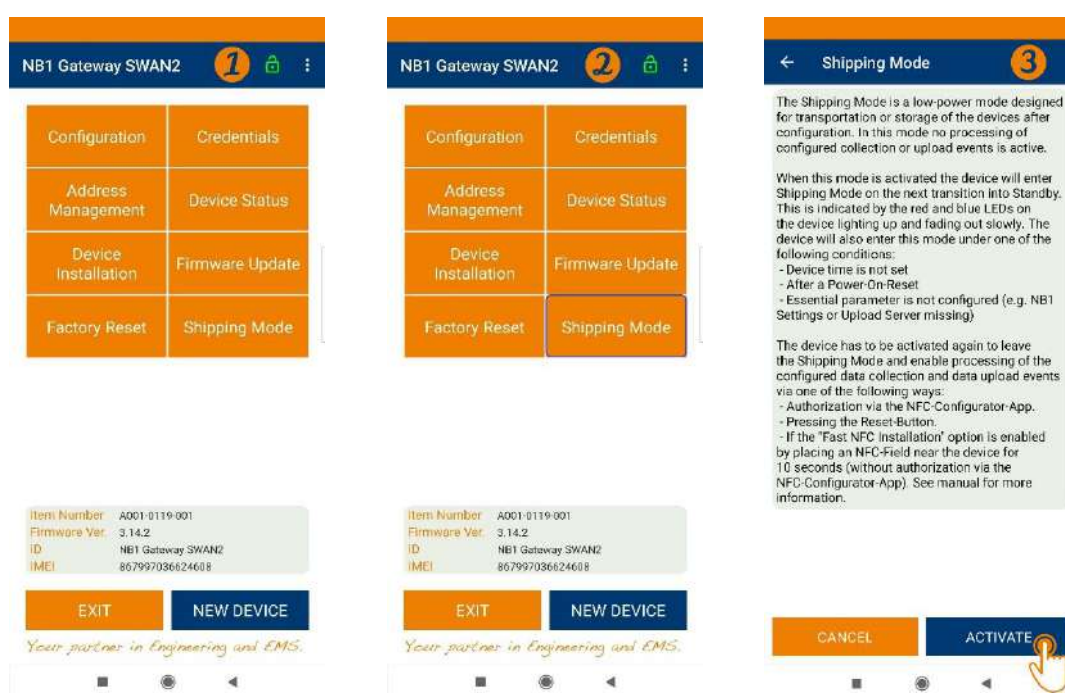


Figure 26: Activate Shipping Mode

Hint

Battery-powered variants: When the device is in Shipping Mode, the device will prevent passivation of the lithium batteries by drawing a constant current for one second every 24 hours.

4.17 Factory Reset

This menu allows to reset the configuration to the factory default values and clear the Whitelist, the Radio Scan List and reset the status- and error-flags of the device. The following steps have to be performed for the reset of settings:

1. Switch to the main menu of the app.
2. Go to **FACTORY RESET**.
3. Check the box for your preferred option and press **EXECUTE**.



Figure 27: Factory Reset



In case you forgot your password for the device, you are able to execute a manual Factory reset using the hardware buttons. Proceed as follows (see also part 1 of the manual): Press the “RESET MCU” button shortly. Immediately afterwards, while the blue LED is on, press and hold the “BOOT0” button for 10 seconds. The red LED will blink once per second while the “BOOT0” button is pressed. After the successful reset, the red LED flashes two times.

The following parameters will be reset:

- Reset to standard configurations
- Deleting the whitelist
- Deleting the radio scan list
- Reset of the device time
- **NFC-Password will be reset to the IMEI of the device.**

5 Remote-Configuration and Firmware-Update

Additionally to the configuration via the NFC-Configurator-App, it is also possible to send commands to the device after the device performed an upload. These commands can trigger:

- Download of a new configuration and upload of the current configuration
- Download of a whitelist and upload of the current whitelist
- Build a Radio-Scan-List and upload of the Radio-Scan-List
- Download and perform a Firmware-Update

The interface for processing commands is currently only available if the HTTP/S is used as the upload protocol. The commands are transmitted to the device in the server's response after the data is uploaded.

Document [1] describes the communication process to transfer the commands and the format of all available commands in detail.

LwM2M as a protocol also allows device management (configuration, performing actions) and firmware updates using dedicated objects. Additional details are described in section 6.3 and in the SWAN2 LwM2M specification [4].

6 Protocols for data upload

This section describes the configurable protocols for the data upload: UDP, HTTP/S and LwM2M. It should be noted that the protocol used has a significant impact on the energy required for data upload to the server, which in turn affects the battery life of the device.

6.1 UDP

When using UDP as the upload protocol, the data will be transmitted in the payload of a UDP-Frame to the configured server and port. Each wM-Bus-Telegram will be transmitted in a single UDP Frame. The content of the UDP-Frame depends on the selected data format and all data formats are supported with this protocol.

The upload server can be provided as a domain name or an IPv4 address.

It is not guaranteed that a UDP frame arrives at its destination. When using the data format “CSV String with Acknowledge” (see section 8.4), it is still possible to detect it, if all of the upload data was received by the server. The server needs to be able to handle this data format.

The energy demand for this protocol is relatively low.

6.2 HTTP and HTTPS

HTTP and HTTP with TLS (HTTPS) ensures that all data arrives at the server.

For the upload server, a complete URI has to be provided, consisting of a server (IPv4 or domain name) and a path (e.g. “weptech-iot.de/swan2”). The Prefix “http://” or “https://” can be omitted as it is implied by the selected protocol.

Only the data format “CSV String” is currently available for upload via HTTP/S.

The upload of data via HTTP/S by the SWAN2 can either be done via a PUT request or a POST request. With POST, the request is sent directly to the provided URI, while PUT extends the URI

with a filename. The difference between these two methods concerning the upload of data by the SWAN2 is described in section 6.2.3.

HTTP has a relatively low energy demand and is comparable to the energy demand of UDP with the data format “CSV String with Acknowledge”.

HTTPS has a relatively high energy demand because of the required TLS handshake. Especially when transferring only a small amount of meter data (less than 20 meters), the TLS handshake is the biggest part of the energy consumption for the upload.

6.2.1 Server requirements

The server has to meet certain requirements, which are described in the following sections, so that an efficient and secure communication between SWAN2 and the server can be performed.

The SWAN2 does not support a client certificate and does not support server certificate verification.

6.2.1.1 Server connection parameters

Due to the high latency times and low data rates in NB1, it is recommended that the server supports keeping a connection alive for multiple HTTP/S requests. With this feature, the server will keep the connection open until all the HTTP/S requests were sent by the SWAN2 and the communication is complete. This, in turn, saves energy and improves battery life of the SWAN2 by avoiding a new HTTP/S handshake for each HTTP/S request. The following settings are recommended:

Parameter	Min. value	Description
Keep alive timeout	60 seconds	The connection should be kept open for this duration after an HTTP/S request.
Client requests per connection	50	The server should support this number of requests before closing the connection.
TLS handshake Timeout	60 seconds	Similar to the “Keep alive timeout” the “TLS handshake timeout” should be long enough to regard the latency of NB1.

Table 2: Recommended server connection parameters

6.2.1.2 Cipher Suites (HTTPS)

The server must support one of the cipher suites shown in Table 3, enabling a secure HTTPS connection between the SWAN2 and the.

TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA

Table 3: Supported cipher suites

6.2.1.3 Authentication

Only basic authentication is supported by the SWAN2. The account credentials (username and password) for this authentication method must be configured in the SWAN2 beforehand. Two different account credentials can be configured in the SWAN2 for the case that certain resources

on the server require different credentials (e.g. upload of data and download of resource using different credentials). See section 4.10 for more information about credentials.

6.2.2 HTTP/S-Header

This section describes additional HTTP/S headers which are added to the HTTP/S requests by the SWAN2. Default HTTP/S headers, which are not required for data interpretation, are omitted.

6.2.2.1 Content-Type

The content type header is a default HTTP/S header that indicates the type of the resource in the HTTP/S body. The SWAN2 supports the following content types:

Type	Related Requests
text/csv	Upload of data, format CSV-String
application/json	Notification after command execution

Table 4: HTTP Content-Type

Example:

```
Content-Type: text/csv
```

6.2.2.2 WEP-IMEI

This custom header contains the IMEI of the device and can be used for device identification.

Example:

```
WEP-IMEI: 867997030568652
```

6.2.3 Upload-Request-Method

The upload of data via HTTP/S by the SWAN2 can either be done via a PUT request or a POST request. The difference between these two methods concerning the upload of data by the SWAN2 is described in the following section. The server can add commands to the response regardless of which request method is used by the SWAN2 for the upload.

6.2.3.1 POST-Request

If the data upload is done via a POST request, the server has to handle the data that arrives at the URI, configured as the upload server. The server can use the information from the HTTP/S header (e.g. the IMEI) to decide how the data has to be processed further. The URI configured in the upload server is not changed, except that the protocol is prepended according to the configuration and the port is added. Example:

```
Upload-Server: weptech-iot.de/Upload  
Port: 21021  
Protocol: HTTPS  
Request-Method: POST
```

```
Full URI:  
https://weptech-iot.de:21021/Upload
```

6.2.3.2 PUT-Request

Upload of data via a PUT request by the SWAN2 is analogous to creating a new file on the server at the specified URI. The HTTP/S body of the request will be written to this resource. If this request

method is used, the SWAN2 appends a filename to the URI configured as the upload server. The format of the full URI is:

<UPLOAD_SERVER>/<IMEI>_<SESSION_ID>_<UPLOAD_TIMESTAMP>_<FILE_COUNTER>.csv

Tag	Description
<UPLOAD_SERVER>	The upload server that is configured in the device.
<IMEI>	The IMEI of the SWAN2 of this upload.
<SESSION_ID>	The session id of this upload.
<UPLOAD_TIMESTAMP>	The device timestamp of this upload in the format <YYYY_MM_DD_HH_mm_ss>.
<FILE_COUNTER>	An index incremented for each PUT request of the same upload (if multiple PUT requests are required for the upload data).

Table 5: PUT request filename format

Example:

Upload-Server: weptech-iot.de/Upload
Port: 21021
Protocol: HTTPS
Request-Method: PUT

Full URI:
https://weptech-
iot.de:21021/Upload/867997030568652_41_2021_04_27_09_37_59_1.csv

The server must support PUT requests for the resource specified by the full URI.

6.3 LwM2M

The LwM2M Client of the SWAN2 Gateway allows the read out of the stored meter data and additionally enables the remote configuration and firmware update of the device. Furthermore certain actions can be executed by interacting with specific LwM2M objects of the client, e.g. to build the Radio Scan List.

Just like with the other protocols, the registration to the parameterized LwM2M Server is performed at configurable points in time. After the registration at the server, the client is available for interactions using the LwM2M objects for a customizable time. After this time passes without any transactions, the client will deregister from the server and enter the Standby Mode until the next event occurs. Communication between the LwM2M Client and server is only possible during the registration period.

The configured upload server corresponds to the LwM2M server on which the registration will be performed. This server can be provided as a domain name or an IPv4 address.

DTLS with PSK is used as a channel encryption. The user name in the selected credentials is used as the PSK-ID and the password as PSK. The password must be provided as a hexadecimal string in the credentials.

Document [4] contains the full specification of the LwM2M Client and the objects of the SWAN2 Gateway. The LwM2M object description in XML-Format can be obtained from the WEPTech website.

The energy requirement is comparable to UDP, if the read out of the meter data is performed using Observe-Notify and the option for acknowledgements of notifications is disabled. If notification acknowledgement is enabled, the energy requirement will increase significantly, if a large number of meters has to be transmitted as each transmitted data packet has to be acknowledged by the server.

7 Synchronous receive mode

The synchronous receive mode of the gateway is based on the standard DIN EN 13757-4. Among other things, this standard specifies the synchronous transmission for wM-Bus meters. Based on this standard and the calculation rule defined there, it is possible to predict at which time the next synchronous telegram transmission of a meter will take place. OMS-certified wM-Bus meters must support the synchronous transmission of meter messages from OMS generation 3.

The standard defines the synchronous telegram transmission for the operating modes T, C and S as well as R, N, F, H. However, the gateway supports synchronous receive mode only for operating modes T and C. The maximum nominal transmission interval is thus limited to 15 minutes.

After a synchronization process in which two synchronous telegram transmissions are received by the gateway, the receiver of the gateway only has to be activated for a short period of time to receive the further synchronous telegram transmissions of the meter. This requires significantly less energy than the continuous receive mode, which extends the service life of battery-powered variants of the gateway.

The configuration parameters defined in section 4.7 can also be used to specify the interval at which the synchronous transmission is to be received. Since not every synchronous telegram transmission from the meter has to be received in order to maintain synchronism, this can save additional energy.

7.1 Initial Configuration and Synchronization

The configuration of the synchronous receive mode can be done via NFC-Configurator-App and via remote access (HTTP/S, LwM2M) to the gateway. After configuration, which consists at least of activating synchronous receive mode and setting a meter address for synchronous reception, a synchronization process must be performed. The first synchronization process takes place automatically 5 seconds after the transition to standby mode following the configuration change, but can also be triggered manually via the NFC-Configurator-App (see 4.12.3). The synchronization process is described in Section 7.2.

After the synchronization process is completed, a corresponding synchronization status is set. The synchronization status is described in section 7.3 and can be determined on the one hand via the NFC Configurator app and on the other hand via the CSV string data format (section 8.3.3) for data transmission to the server.

During interaction with the gateway via the app, no synchronous telegram reception is performed. After completing the interaction with the app, synchronous telegram reception is resumed. During the transmission of the data to the server, synchronous telegram reception is also not performed. After the data transfer is completed, synchronous telegram reception is resumed.

7.2 Process for Synchronization

The synchronization process is necessary for determining the nominal transmission interval with which the next transmission time of the synchronous telegram of a meter can be calculated. During the synchronization process, the gateway goes on reception and remains active until two synchronous telegrams of the relevant meter have been received. The nominal transmission interval is calculated from the access numbers of the telegrams and the reception time stamps. The synchronization process is thus successfully completed.

In addition to the premature termination of the synchronization process after the reception of two synchronous telegrams, this process is also limited to the time configured via the **Synchronization Duration** parameter (section 4.7). If no synchronization can be established between gateway and meter within this time, the synchronization process is aborted and has thus failed.

In autonomous operation, if the synchronization process fails, the synchronization is attempted again 6 hours later. If the synchronization process is still unsuccessful for the fifth time in succession, a data transfer to the server takes place, in which the synchronization status contains a corresponding error code. Subsequently, no further synchronization process is undertaken and the cause of the error must be determined. Usually, such a case should only occur if a meter can no longer be received at all, for example, due to a change in the environment.

Renewed synchronization processes are necessary for the following reasons:

- No synchronous telegram received for a duration configured via **Synchronization Timeout** (section 4.7)
- Change of device time, e.g. due to automatic summer/winter time changeover or due to automatic/manual readjustment of time via NTP server or NFC-Configurator-App.
- Configuration changes that affect the synchronous receive mode
- Firmware update of the gateway

Of course, switching off the gateway and activating the shipping mode will also cause the synchronicity to be lost and a new initial synchronization process will have to be performed afterwards.

7.3 State of synchronization

The synchronization status can be read out via the NFC Configurator app (section 4.13). Likewise, the synchronization status is part of the CSV string data format for the upload (Section 8.3.3). The following states can occur:

Wert	Status
0	Deactivated
1	Synchronization required
2	Synchronized
-13	Error: Invalid Device Time
-14	Error: Too many failed synchronizations
-15	Error: No meter address configured for synchronization

Table 6: State of synchronous receive mode

In addition to the status, there is also a counter that provides information about how stable the synchronization is to the configured meter. The counter is reset when a configuration change is made that requires a new synchronization process and is incremented every time synchronization is interrupted during autonomous operation.

8 Data formats

Regardless of the configured data format, the following applies to uploading the collected meter data: wM-Bus-telegrams are forwarded as received, but the CRC is removed independently of the frame format (A or B).

8.1 Raw Data (binary)

The data is transmitted as described above without additional information in raw data form.

8.2 Raw Data (hex encoded)

The data is transmitted as described above without additional information but the raw data is encoded as a hexadecimal character sequence. Example:

```
2E 44 33 30 70 62 01 00 07 1B 7A 9B 00 20 25 24 13 9E 0C 3C A4 70 99 FE 23 05 6F
F9 26 AF AE FC E4 99 CA 51 8E BE A6 B1 D3 E6 17 7A F5 2B F9
```

8.3 Upload as CSV-String

The meter data and other data relating to the device are transmitted as a CSV character string. There are three types of packets and each packet type contains different comma separated values. Packet type 1 (Device Information Packet) and packet type 3 (Upload Statistic Packet) contain information about the gateway and broadcast. The packet type 2 contains information about the sensor data. A checksum (CRC32) is integrated at the end of all packet types. This checksum can be deactivated by checking the box at "Suppress CRC in Packets".



Figure 28: Format Specification

8.3.1 Packet type 1 "Initialization":

This packet contains device information about SWAN2.

Example with activated checksum (CRC32):

```
1, "867997036624608", 21, 0, 0, "2023-01-23T12:00:28+01:00", "WEPTECH ELEKTRONIK", "NB1 Gateway SWAN2", "3.13.3", 10, 0xBBE7180B, 0xBA21678A, 3525, 1, 3666, 21, 3502, 5, 26201, "100.85.21.125", 54001, 29403150, 8, 0, 0, -71, -6, -65, "BC66NBR01A11", "8988280660010705228", "901405101070522", 915, 0, 647, 23, 5, 0xFD472555
```

8.3.1.1 Description Telegram Packet type 1

Pos.	Description	Data type	Example
1	Packet-Type-ID	Unsigned Integer	1
2	IMEI of device	String	"867997036624608"
3	Session-ID, incremented with every upload	Unsigned Integer	21
4	Sequence-ID, incremented for each packet	Unsigned Integer	0
5	Status Flags (section 8.3.4)	Unsigned Integer	0
6	Transmission time stamp (ISO 8601 Format)	String	"2023-01-23T12:00:28+01:00"
7	Device Tag, individually configurable	String	"WEPTECH ELEKTRONIK"
8	Device type	String	"NB1 Gateway SWAN2"
9	Firmware-Version	String	"3.13.3"
10	Number of telegrams in device memory	Unsigned Integer	10
11	CRC32 of Radio-Scan-List ¹	Unsigned Integer (Hexadecimal)	0xBBE7180B
12	CRC32 of Configuration ¹	Unsigned Integer (Hexadecimal)	0xBA21678A
13	Voltage in mV of currently unused Battery ²	Unsigned Integer	3525
14	Currently used battery ²	Unsigned Integer	1
15	Open-Circuit-Voltage in mV of currently used battery ³	Unsigned Integer	3666
16	Temperature in degrees Celsius	Unsigned Integer	21

¹ Allows to detect a change of the radio scan list (e.g. new meter) or configuration

² Only for battery-powered variants with replaceable battery

³ Only for battery-powered variants

17	Battery voltage in mV with load ³	Unsigned Integer	3502
18	Registration-State for network (1 = Home network; 5 = Roaming)	Unsigned Integer	5
19	PLMN of Operator	Unsigned Integer	26201
20	IP address of device	String	"100.85.21.125"
21	Tracking Area Code "TAC"	Unsigned Integer	54001
22	Cell-ID	Unsigned Integer	29403150
23	Used NB1 Band	Unsigned Integer	8
24	NB1 Operating Mode (0: In band same PCI, 1: In band different PCI, 2: Guard band, 3: Standalone)	Unsigned Integer	0
25	ECL-Mode (Enhanced Coverage Level)	Unsigned Integer	0
26	RSRP-Value in dBm	Signed Integer	-71
27	RSRQ-Value in dBm	Signed Integer	-6
28	RSSI-Value in dBm	Signed Integer	-65
29	FW-Release of NB-IoT-Module	String	"BC66NBR01A11"
30	ICCID of SIM card	String	"89882806660010705228"
31	IMSI of SIM card	String	"901405101070522"
32	Number of events for receive mode	Unsigned Integer	915
33	Counter of failed NB1 Connections	Unsigned Integer	0
34	Number of Uploads in ECL0	Unsigned Integer	647
35	Number of Uploads in ECL1	Unsigned Integer	23
36	Number of Uploads in ECL2	Unsigned Integer	5
37	CRC32 over the CSV-String up to this value	Unsigned Integer (Hexadecimal)	0xFD472555

Table 7: Description of CSV string - packet type 1

8.3.2 Packet type 2 "Sensor data"

One telegram per meter is transmitted. The following line shows an example of a packet of type 2, which contains the wM-Bus-Meter data.

Example with activated checksum (CRC32):

```
2,"867997036624608",21,3,0,"2023-01-23T12:00:28+01:00",2,"10000003-IIF-01-03",
"00QmJQMAABABN4wgcZAPACw1EUwSAIsF8w7Ntv1mcgMAABAmJQEDcSAQBxC4/IZpXZrOMMD1qAQdTKuj",-
33,"2023-01-23T12:00:02+01:00",,,,,,,,,,,,,,,,,,,,,,,,,,0xB0D54244
```

8.3.2.1 Description telegram Packet type 2

Pos.	Description	Data type	Example
1	Packet-Type-ID	Unsigned Integer	2
2	IMEI of device	String	"867997036624608"
3	Session-ID, incremented with every upload	Unsigned Integer	21
4	Sequence-ID, incremented for each packet	Unsigned Integer	3
5	Status Flags (section 8.3.4)	Unsigned Integer	0
6	Transmission time stamp (ISO 8601 Format)	String	"2023-01-23T12:00:28+01:00"
7	Packet number of this telegram in device memory	Unsigned Integer	2
8	OMS-Address of the sensor	String	"10000003-IIF-01-03"
9	Sensor data ((w)M-Bus raw), base 64 encoded	String	"00Qm ... Iuj"
10	RSSI of the received telegram	Signed Integer	-33
11	Reception time stamp (ISO 8601 Format)	String	"2023-01-23T12:00:02+01:00"
12 - 36	Reserved	/	/
37	CRC32 over the CSV-String up to this value	Unsigned Integer (Hexadecimal)	0xB0D54244

Table 8: Description of CSV string - packet type 2

8.3.3 Packet type 3 “Ending”

A telegram with information on the completed transmission operation is transmitted.

Example with activated checksum (CRC32):

```
3, "867997036624608", 21, 11, 0, "2023-01-23T12:00:29+01:00", 11, 11, 0, 2708,
56100, 187, 42750, 254, 73, , 299250, 128250, 6400, 1600, -12, 0, 0, 0, , -71, -6, -
65, 0, 1, 1617, 5969, 0, 0, , , 0x3EA2CA40
```

8.3.3.1 Description telegram Packet type 3

Pos.	Description	Data type	Example
1	Packet-Type-ID	Unsigned Integer	3
2	IMEI of device	String	"867997036624608"
3	Session-ID, incremented with every upload	Unsigned Integer	21
4	Sequence-ID, incremented for each packet	Unsigned Integer	11
5	Status Flags (section 8.3.4)	Unsigned Integer	0
6	Transmission time stamp (ISO 8601 Format)	Unsigned Integer	"2023-01-23T12:00:29+01:00"
7	Number of packets that should have been sent	Unsigned Integer	11
8	Number of packets that were sent (including repeated packets)	Unsigned Integer	11
9	Number of packets that have been lost	Unsigned Integer	0
10	Number of transmitted bytes	Unsigned Integer	2708
11	Total time in receive mode	Unsigned Integer	56100
12	Total consumed charge quantity during receive mode in mAh ⁴	Unsigned Integer	187
13	Total time in upload mode ⁴	Unsigned Integer	42750
14	Total consumed charge quantity during upload in mAh (estimated) ⁴	Unsigned Integer	254
15	Estimation of battery state of charge in percent (see section 8.3.5)	Vorzeichenlose Ganzzahl (UINT32)	73
16	Reserved	/	/
17	Total Rx-time of modem in ms ⁴	Unsigned Integer	299250
18	Total Tx-time of modem in ms ⁴	Unsigned Integer	128250

⁴ This information allows to estimate the state of charge of the battery.

19	Rx-time of modem in ms of last connection	Unsigned Integer	6400
20	Tx-time of modem in ms	Unsigned Integer	1600
21	Tx-power of Modem in dBm	Signed Integer	-12
22	State of synchronous receive mode (section 7.3)	Signed Integer	0
23	Counter for lost synchronizations since last upload	Unsigned Integer	0
24	Counter for lost synchronizations since last configuration change	Unsigned Integer	0
25	Reserved	/	/
26	RSRP in dBm	Signed Integer	-71
27	RSRQ in dBm	Signed Integer	-6
28	RSSI in dBm	Signed Integer	-65
29	MAC-Tx-BLER (Block Error Rate) of modem during upload	Unsigned Integer	0
30	MAC-Rx-BLER (Block Error Rate) of modem during download	Unsigned Integer	1
31	Number of bytes (MAC) of modem during upload	Unsigned Integer	1617
32	Number of bytes of modem during download	Unsigned Integer	5969
33	Counter of failed NB1 Connections	Unsigned Integer	0
34	Debug-Flags	Unsigned Integer	0
35,36	Reserved	/	/
37	CRC32 over the CSV-String up to this value	Unsigned Integer (Hexadecimal)	0xF6828BA5

Table 9: Description of CSV string - packet type 3

8.3.4 Status Flags in CSV String

The battery status is checked before each upload. In the process, certain flags are set in a status register to document the state of the battery in the device. The status flags also contain further information about the state of the device. The status flags are located at position 5 in the CSV strings and are defined in the following table.

Bit	Name	Description
0	BATTERY1_LOW ⁵	Measured battery voltage under load of primary battery < 2.95 V
1	BATTERY1_CRITICAL ⁵	Measured battery voltage under load of primary battery < 2,75V
2	BATTERY1_END_OF_LIFE ⁵	Measured battery voltage under load of primary battery < 2,65V, Upload is canceled
3	BATTERY1_BC66_VOLTAGE_DROP ⁵	Voltage drop of primary battery while using the modem during the upload
4	BATTERY1_POWER_FAIL ⁵	Voltage monitoring has detected a voltage of the primary battery of < 2.3 V
5	DUBLETTE_FILTER_OVERFLOW	More wM-Bus-Telegrams were received than can be checked for duplicated telegrams. This flag is reset before each collection. If this flag is set there might be multiple identical telegrams in this upload.
6	TIME_SYNC_FAILED	Error while requesting the time via NTP or from Network. Resets after next successful request.
7	PLMN_AUTO_MODE	Connection with the configured PLMN not possible. Automatic Network selection is enabled.
8	SOFTWARE_ERROR	Software-Error detected. Explicit error is described via debug flags.
9	HARDWARE_ERROR	Hardware-Error detected. Explicit error is described via debug flags.
10	BATTERY_SWITCH_FAILED ⁶	Switching to other battery failed.
11	BATTERY2_LOW ⁶	Measured battery voltage under load of secondary battery < 2.95 V
12	BATTERY2_CRITICAL ⁶	Measured battery voltage under load of secondary battery < 2,75V
13	BATTERY2_END_OF_LIFE ⁶	Measured battery voltage under load of secondary battery < 2,65V, Upload is canceled
14	BATTERY2_BC66_VOLTAGE_DROP ⁶	Voltage drop of secondary battery while using the modem during the upload
15	BATTERY2_POWER_FAIL ⁶	Voltage monitoring has detected a voltage of the secondary battery of < 2.3 V

Table 10: Status Flags

⁵ Only for battery-powered variants

⁶ Only for battery-powered variants with replaceable batteries

 Hint

1. There is an option to automatically reset the status flags and debug flags after a successful upload. This option is usually activated in the delivery state and described in section 4.9.
2. The Flags can be reset to default with a Power-On-Reset (pull jumper for 60s). Additionally it is possible to reset the flags using the NFC-App (see section 4.17).
3. If a status flag was set, the number at position 5 in the CSV-String is not equal to 0, which means one of the flags described above was set.
4. If debug flags are set, they can be read out (along with the meaning) in the “Extended Information” in the “Device Status” of the NFC configurator app.

8.3.5 Estimation of battery state of charge

An estimate of the battery status in percent is transmitted in packet type 3 at position 15. This value is only present for battery-powered variants produced after June 2023. This value is not available in previous versions of the battery-powered variants. The battery state of charge is specified in a value range from 0 to 100%. Values that fall outside of this range indicate that the estimation could not be performed due to an error.

8.4 CSV String with Acknowledge

This upload format can be used to determine whether all data from an upload has arrived on the server. The existing CSV string format will be expanded. Certain telegram IDs inform the server that the device is expecting a response packet. In this response packet, the server can tell the device which data packets did not reach the server, so that the device only has to send these missing data packets again. The extension of the Telegram IDs, the format of the response packets of the server and further details regarding this upload format are described in document [2].

9 Use of different Platforms

9.1 IoT Platform

So far, all data sent by the SWAN2 via the LTE Cat-NB1 mobile network is transmitted via UDP, HTTP/S or LwM2M.

In cooperation with the company ROCK5, it is possible to visualize and / or forward the data received and sent by the SWAN2 on an IoT platform. In this context, we provide a sample case containing our gateway SWAN2 and our temperature and humidity sensors MUNIA and ROBIN for a trial period of 4 weeks free of charge. We already configure and integrate the devices so that they can start immediately.

If you are interested, please contact us.

9.1.1 Device Management in the IoT Platform

Please log in to the ROCK5 platform with the login data sent to you. Click on the project created for you in the left column and go to the “IOT devices” tab. There you will find an overview of the devices that have already been set up: our wireless M-Bus / OMS sensors (MUNIA & ROBIN) and our NB-IoT gateway (SWAN2). Here you can find the status, the signal quality, the battery level and other information. Click on the respective device to access the device's menu.

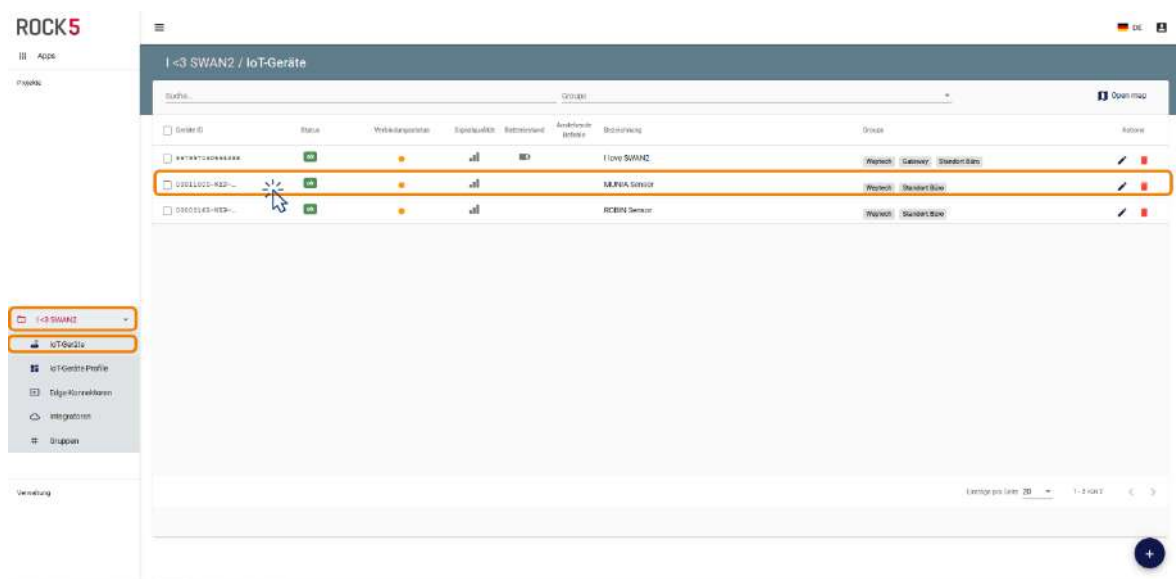
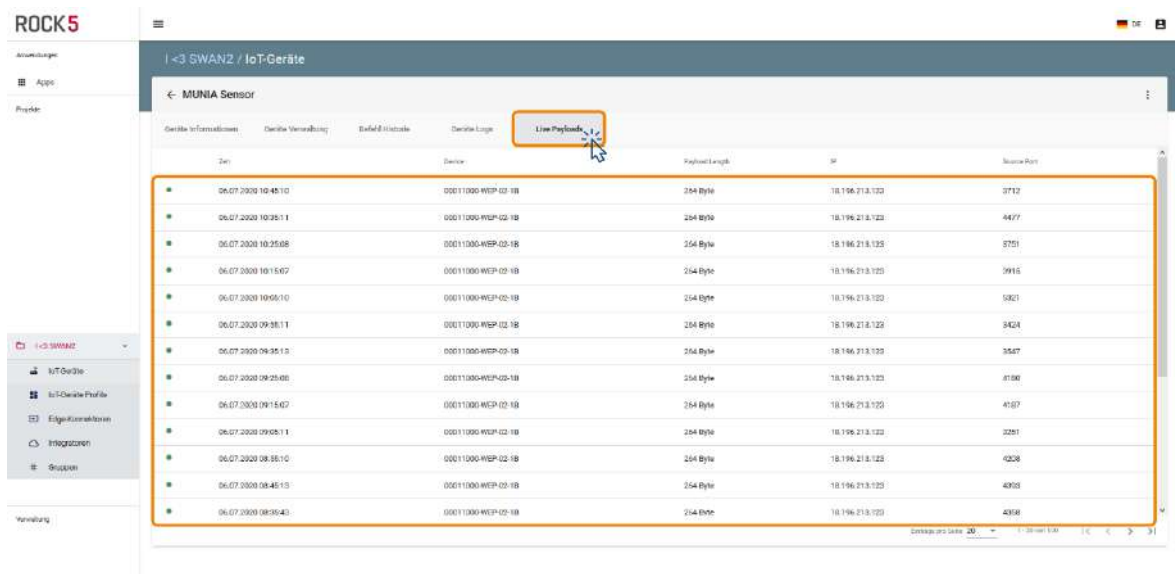


Figure 29: Device Management

Via “Live Payloads” in the upper tab, you can view its incoming data and e.g. check them for mistakes.



Time	Device	Payload Length	IP	Source Port
06.07.2020 10:45:10	00E11000-WESP-02-1B	264 Byte	18.196.21.3.123	3712
06.07.2020 10:25:11	00E11000-WESP-02-1B	264 Byte	18.196.21.3.123	4477
06.07.2020 10:25:08	00E11000-WESP-02-1B	264 Byte	18.196.21.3.123	3751
06.07.2020 10:15:07	00E11000-WESP-02-1B	264 Byte	18.196.21.3.123	3915
06.07.2020 10:05:10	00E11000-WESP-02-1B	264 Byte	18.196.21.3.123	5321
06.07.2020 09:58:11	00E11000-WESP-02-1B	264 Byte	18.196.21.3.123	3424
06.07.2020 09:35:12	00E11000-WESP-02-1B	264 Byte	18.196.21.3.123	3547
06.07.2020 09:25:08	00E11000-WESP-02-1B	264 Byte	18.196.21.3.123	4180
06.07.2020 09:15:07	00E11000-WESP-02-1B	264 Byte	18.196.21.3.123	4187
06.07.2020 09:05:11	00E11000-WESP-02-1B	264 Byte	18.196.21.3.123	2281
06.07.2020 08:55:10	00E11000-WESP-02-1B	264 Byte	18.196.21.3.123	4238
06.07.2020 08:45:13	00E11000-WESP-02-1B	264 Byte	18.196.21.3.123	4353
06.07.2020 08:30:43	00E11000-WESP-02-1B	264 Byte	18.196.21.3.123	4358

Figure 30: Device Management - Live Payloads

9.1.2 Devices in the IoT Platform

Please log in to the ROCK5 platform with the login data sent to you. In the left menu under “Projects” click on your project and on “Edge connectors”. Then click on the existing configuration.

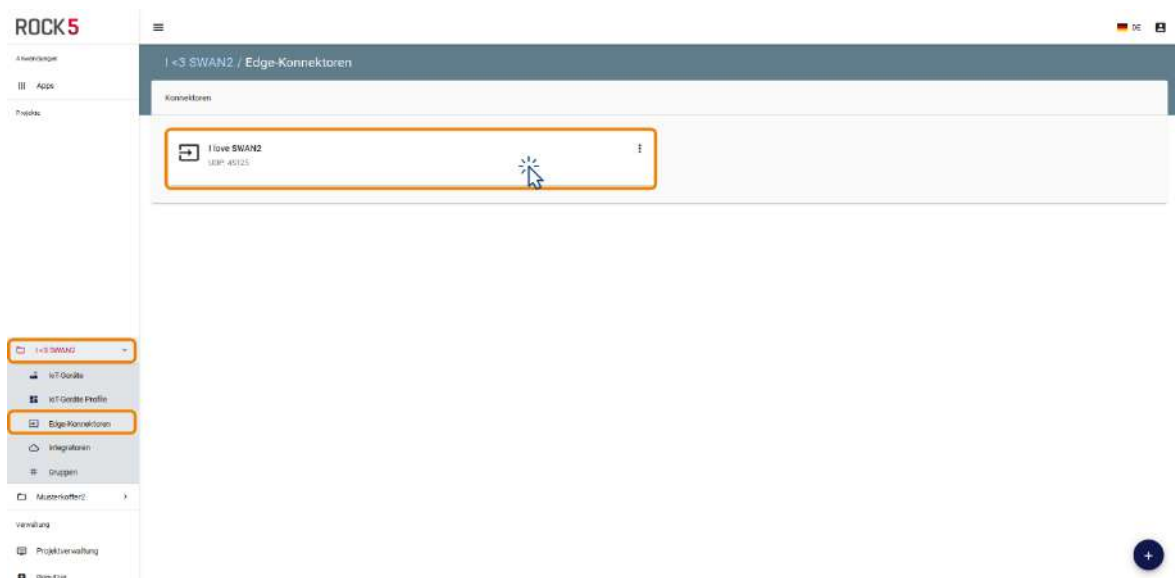


Figure 31: Edge Connector – IoT platform

In the “Live Payloads” tab, in addition to our previously set up sensors MUNIA and ROBIN, other wM-Bus devices collected by the SWAN2 gateway are listed.



Hint

The collection of a maximum of 10 devices is configured by default. If you want to receive more devices, this can be adjusted using our NFC configurator app (see section 4.6.1).

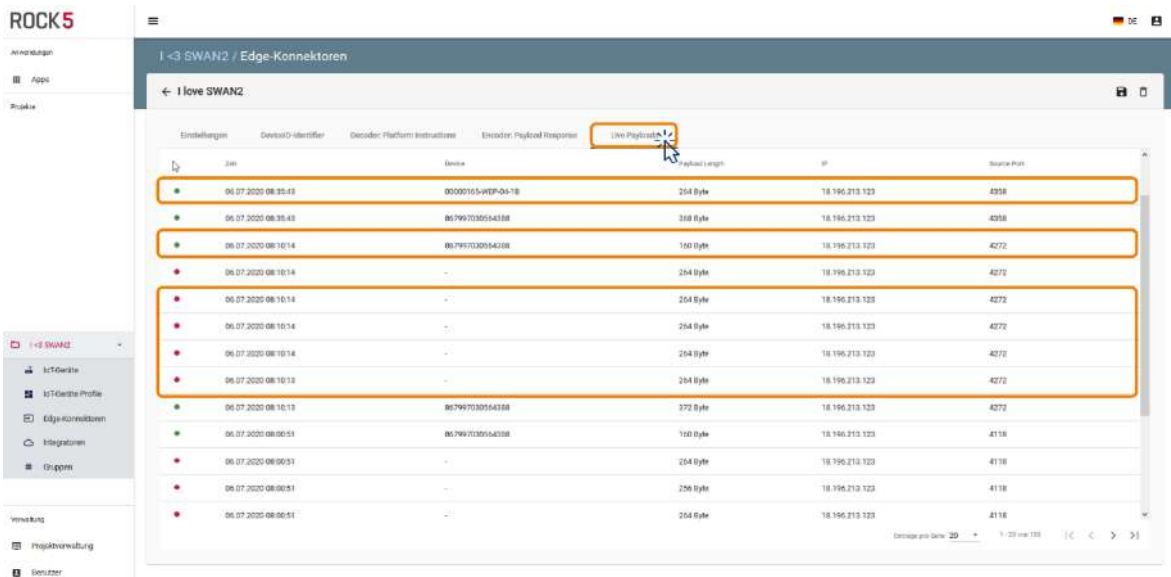


Figure 32: Edge Connector – Live Payloads

The devices marked with a green dot are the pre-configured sensors and the gateway. Devices with a red dot are your wireless M-Bus / OMS devices + possibly other devices that are within range and can be received.

Click on one of our sensors (devices with a green dot) to get a detailed view. There, you see the device ID and information concerning temperature and humidity from the “Incoming Payload” at the end of the frame (see illustration below). This information is then visualized.

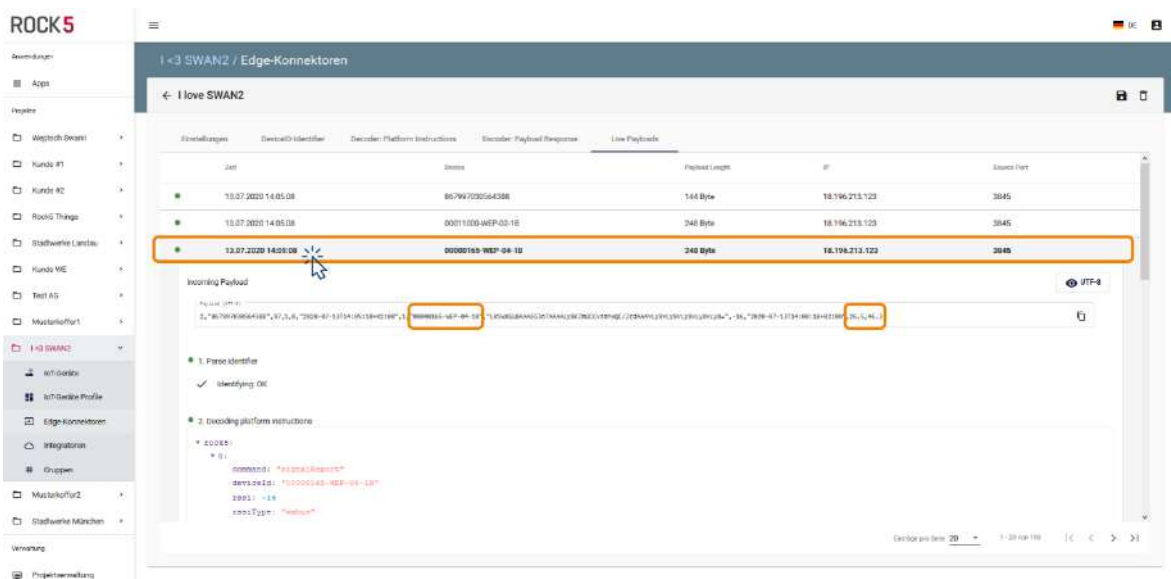


Figure 33: Edge Connector – Device ID/ Data

Click on a device / data package with a red dot to get a detailed view. In this view, you can read out the device ID (marked in the picture below) for your assignment. The error / red point occurs because the assignment to the device is not configured.

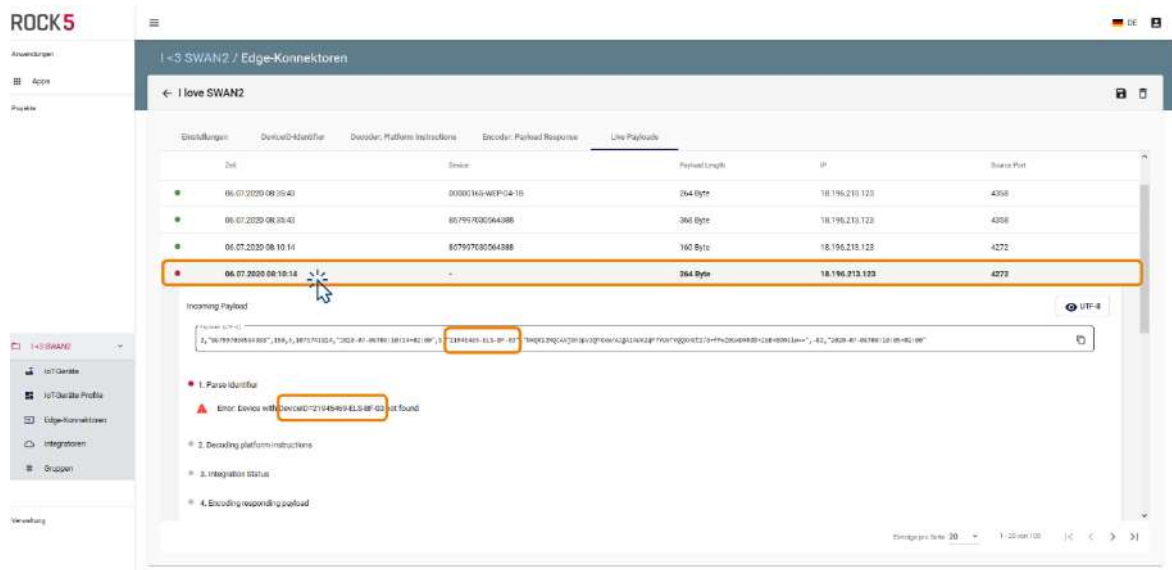


Figure 34: Edge Connector – Device ID

Did you find your device? Perfect! Your data will be collected and transferred to the platform. Your devices are not displayed? We will help you. Contact us!

9.2 WEPTECH's "Real time" Monitor with MQTT

To make it easier for the user to monitor the data on his PC or smartphone, WEPTECH offers a gateway service. This service analyzes incoming UDP packets that come from SWAN2 and forwards them to an MQTT broker with the device IMEI as content (publish). MQTT is a widely used protocol. There are many applications on the market with which you can subscribe to these messages and monitor the uploaded data in almost real time.

9.2.1 WEPTECH MQTT Client App

WEPTECH offers an Android App, which you can download here:

<https://play.google.com/store/apps/details?id=de.weptech.weptechmqttclient>

The UDP server is hosted on the following server:

- IP address / host name: "weptech.net"
- Port: 28028

The MQTT broker (which is hosted on the same host as the UDP server) uses TLS encryption. Therefore, a password and username must be used for each connection / subscription.

Please contact WEPTECH to receive the access data for your device.

Now proceed as follows:

1. Open the WEPTECH MQTT client app and tap on "Edit".
2. Complete the IMEI of your device in the input field and enter the password sent to you.
3. The app starts the search process for incoming data packets and displays them in the correspondingly selected data format (see description of data format).

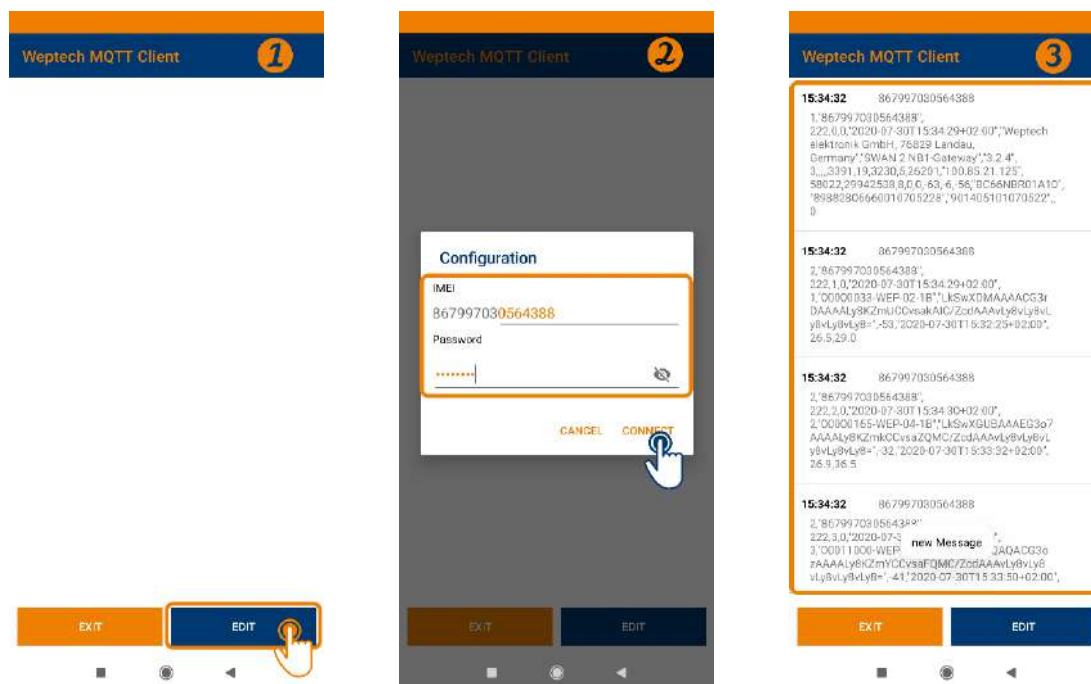


Figure 35: MQTT Client App

9.2.2 Eclipse Paho MQTT Spy

This is a Java application, so it can be used on most of the operating systems available today. You can download this program from the following link

<https://github.com/eclipse/paho.mqtt-spy/wiki/Downloads>

Please add a new connection with “wepotech.net” as server URL.

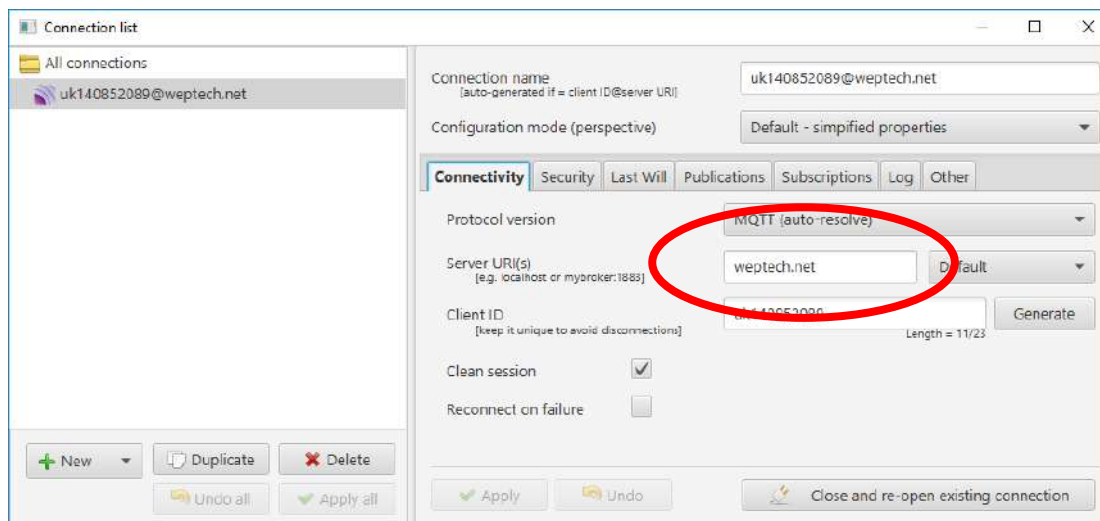


Figure 36: Eclipse Paho MQTT Spy URL

On the Security tab, select the User Authentication check box and enter the login information provided by WEPTECH.

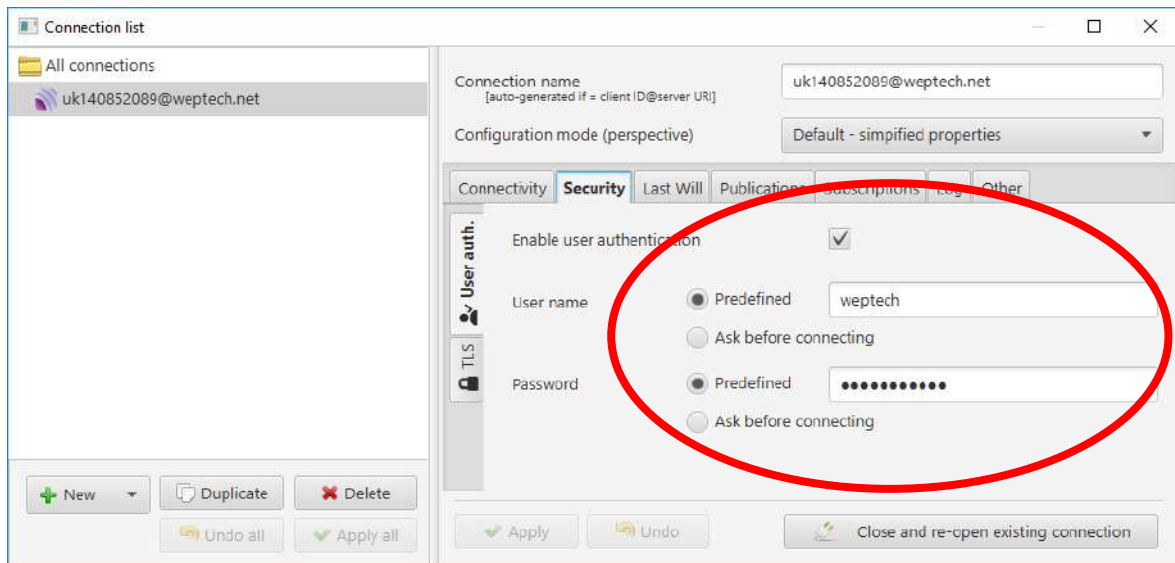


Figure 37: Eclipse Paho MQTT Login

Make sure that the TLS settings are configured correctly as shown in the following figure.

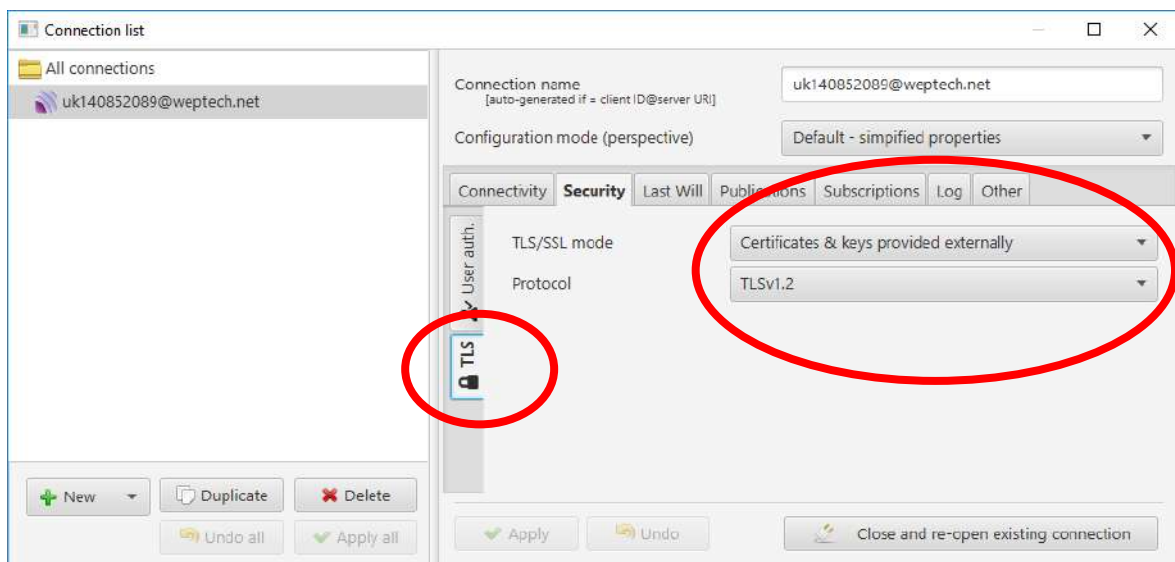


Figure 38: Eclipse Paho MQTT Spy TLS

9.2.3 Use of Mosquitto

The command line for calling the Mosquitto MQTT client is as follows:

```
mosquitto_sub -h weptech.net -u <IMEI> -P <Password> -p 8883 --  
capath /etc/ssl/certs/ -t '/weptech/imei/<IMEI>' -v
```

Please replace the IMEI and the password with the login information provided by WEPTech.

10 Supporting documents

The following documents contain information to certain features and functionalities of the SWAN2 Gateway. These documents can be requested via sales@weptech.de.

Ref.	Name of document	Version	Date
1	<i>Application Note - NB1 Gateway SWAN2</i> Remote Commands	1.2	21.02.2023
2	<i>Application Note - NB1 Gateway SWAN2</i> CSV-String with Acknowledgment over UDP	1.1	31.03.2021
3	<i>Application Note - NB1 Gateway SWAN2</i> Configuration Parameters	1.3	21.02.2023
4	<i>Application Note - NB1 Gateway SWAN2</i> LwM2M	1.4	21.02.2023

11 Copyright protection

Transmitting, as well as copying, of this document and utilization of its contents are not permitted, if not explicitly allowed. Violation obligates compensation. We reserve all rights in this document and in the subject matter and illustrations contained therein.

12 Warranty information

Great care was taken in preparing this manual. No guarantee is given for the correctness of the contents of this manual since errors, in spite of all efforts, can never be completely avoided.

13 Disclaimer

WEPTech elektronik GmbH is not liable or warranted for any damages resulting from improper installation, assembly and improper use of the product or failure to comply with the operating instructions and/or safety instructions.

Parts of the pages or the complete publication including all offers and information might be extended, changed or partly or completely deleted by WEPTech elektronik GmbH without separate announcement.

This disclaimer is to be regarded as part of the operating instructions from which reference was made to this page. If sections or individual terms of this statement are not legal or correct, the content or validity of the other parts remain valid by this fact.

14 Restriction of use

WEPTech elektronik GmbH products are not approved for use in life support or life sustaining systems or units, or other systems where malfunction can be expected to result in substantial personal injury to the user or third parties. WEPTech elektronik GmbH products are further not approved for use as an essential part of any life support or life sustaining system or unit, the malfunction of which may cause the failure of the life support or life sustaining system or unit, or affect its safety or effectiveness. WEPTech customers who use these products in such applications or sell them for such uses do so at their own risk and must exempt WEPTech elektronik GmbH from all damages resulting from the sale for inappropriate purposes or the inappropriate use.

By using WEPTech elektronik GmbH products, the user is bound by these terms and conditions.



Note:

The information, instructions and descriptions in this manual refer to the actual operating and service conditions herein.

For technical questions, safety notes or technical failure, please contact WEPTech elektronik GmbH.

We reserve the right to technical modifications.