Metering Cloud Connect wM-BUS (MEC-A06)

Operation Manual

grandcentrix GmbH | Holzmarkt 1, 50676 Cologne | +49 221-677 86 00 | products@grandcentrix.net

Metering Cloud Connect
wM-BUS (MEC-A06)
Operation Manual

Onboarding/Configuration

The self-service portal for all onboarding and configuration options can be reached at www.meteringcloudconnect.net.
If you have any questions or problems, you can reach our service desk at https://service.grandcentrix.net.

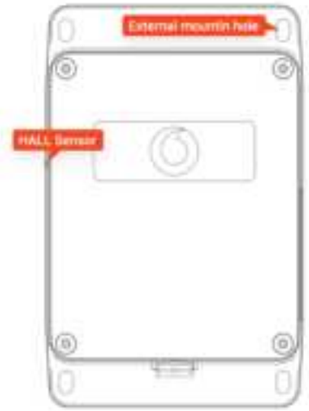
Responsible for the content: grandcentrix GmbH, Holzmarkt 1 D-50676 Cologne Germany, www.grandcentrix.net

Table of Contents

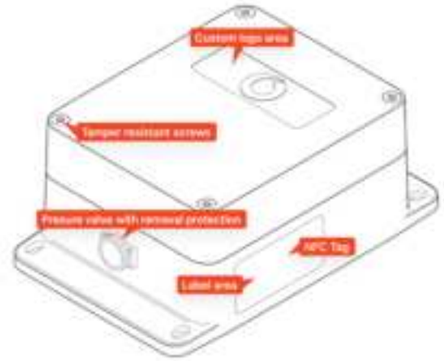
Intended use

The product is intended for reading and processing data from meters using the wireless M-Bus and transferring the data via NB-IoT networks. The device is intended exclusively for this purpose. Any application other than that described above, as well as modifications to the product, are considered improper use.

Product graphics



Enclosure top view



Enclosure side view

components on the PCBA

Inside view of the gateway

Read the **Safety Information** chapter of this user guide before using this device. Failure to comply with safety warnings can result in serious injury.

Data sheet

(nominal operating conditions unless otherwise noted)

Variant name	wM-Bus One-Cell	wM-Bus Two-Cell
Dimensions	112x175x71 mm	
Attachment	4 screw holes & flat surface for adhesive	
Weight	~510g	~610g
Battery	One cell LiSoCl2 3.6 V 19 Ah	Two cells LiSoCl2 3.6 V 38 Ah
Minimum battery lifetime	~20 years	~40 years
	(20 second listening time / hourly readout / daily transmission / ECL 0)	
Input voltage range	2.5 V - 5 V	
Onboard storage	up to 20000 frames	
Tamper detection	electronic & physical	
Temperature sensor	Onboard	
Maximum power consumption	2W	
Main IC	Nordic Semiconductor nRF9160	
Network / Band	LTE Cat NB1/NB2 (Narrowband IoT) - Bands 8, 20, 28	
Antenna	High performance omnidirectional onboard antenna	
SIM card	MFF2(eSIM) - plastic SIM possible	
Storage and operating temperature	-20 °C to +70 °C	
Air humidity	max. 95 % relative, non condensing	
Water / Dust & UV	IP67, UL-F1	
Certifications	CE, ROHS, RED, GCF	
Protocols supported	Wireless M-Bus (868-MHz) T, C, S (Unidirectional) Frame formats A / B	
Number of meters supported	up to 50	
Readout and transmission interval	5 minutes - 4 weeks	
Firmware updates (FOTA)	via Portal or API (both device- and modem firmware can be updated)	
Communication protocol (between gateway and middleware)	OMA LwM2M via UDP (between gateway and middleware) HTTPS (between the middleware and your infrastructure)	
Meter configuration	Whitelist per gateway (via portal or API)	
Installation feedback	Visible (LEDs inside the enclosure) & audible (Buzzer)	
Gateway identification	via NFC Tag or Label	
Gateway operation	Remote (portal or API) / Button (inside) / Magnet (from outside)	

Quick start guide

1. Login to the customer portal at https://meteringcloudconnect.net/or request access to the customer portal if you don't have an account yet by writing to products@grandcentrix.net or scanning the QR code.
2. Set the gateway group to your desired readout and send interval (default: read and send hourly).
3. Define meter whitelist for the gateway including wM-Bus mode and listening time (optionally you can also schedule a wM-Bus scan to receive a list of all meters in range).
4. Define where your metering data should be sent by configuring a cloud adapter and allocate it to a gateway group to (default: data is discarded).
5. Activate the gateway from warehouse mode via the hall sensor by moving a magnet next to the N/S symbol on the enclosure.
6. Wait for a double beep indicating a successful cloud connection and refresh the customer portal shortly afterwards to see the current state of the gateway reflected. If you scheduled a wM-Bus scan, you need to wait for the configured scan time and refresh the page again to see the found meters.
7. Your gateway should now listen in the defined read interval for the configured meters and send the received frames to your defined cloud adapter at the configured send interval.

General information

This user manual describes the usage and behaviour of the gateways with the grandcentrix middleware (REST API) and customer portal. Hardware and behaviours may be explained in more detail than needed when relying on the provided connectivity and middleware. This is done for customers planning on integrating the gateways using their own middleware and/or connectivity.

Setup overview and integration options

Metering Cloud Connect as a standard product includes the hardware (gateway), the connectivity (with a preinstalled SIM) as well as the middleware with the Portal and API. Connectivity is included to ensure a safe and easy setup process together with a default middleware including:

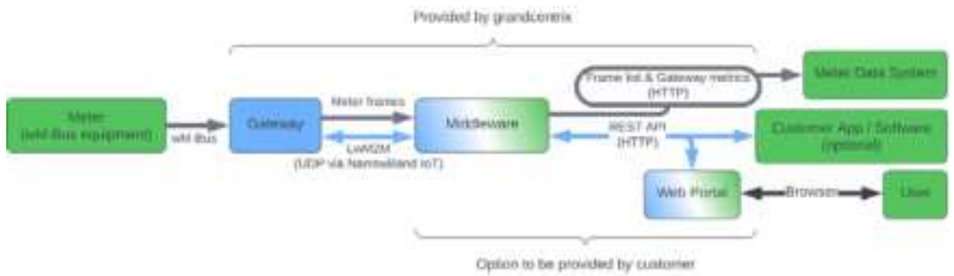
- A secure tunnel between the mobile network operator and the middleware
- DTLS encryption of the data in transport
- LwM2M session management and UDP communication
- Easy to use Web Portal and REST APIs to work with the gateways
- Easy to integrate Webhooks / Cloud Adapters to send data to your systems

However, should the customer wish to run own LwM2M servers and/or provide own connectivity, a custom hardware offer can be made for customer specific production batches.

In any of those scenarios, the metering data itself (the frames sent by the meters) will need to be processed by the customer.
grandcentrix forwards received frames via HTTP / Webhook (other formats on request) to customer systems without decoding by default.
The meter frames will need to be decoded using the meters decryption key (if the meter sends encrypted frames) and processed as needed.
The grandcentrix middleware only reads the unencrypted header information from the frames to add additional metadata to the list of frames from the meter to ease processing of the frames.

grandcentrix does not store received meter data longer than needed for forwarding to the customers servers. Meter frames may be lost in case of a downtime of the customers receiving server, as we don't store frames for retransmission.

System and communication diagram



Customer Portal

To easily manage and see the capabilities of the gateways, customers can use the grandcentrix Metering Cloud Connect portal at https://meteringcloudconnect.net/. Meter data is not displayed there, as it will only be forwarded to customer systems via cloud adapters (those can be set up via the portal soon, until then only via REST API).

Demo dashboard (meter data system example)

If no customer system is available to send the meter data to during the testing phase, grandcentrix can optionally provide a demo dashboard where the device data is exported to and can be analysed over time. This is a limited (non-standard) service, not intended for permanent use and needs to be requested from grandcentrix.

See example at p. 20 Demo dashboard example.

REST API

For customers who want to integrate gateway operations (like provisioning of new gateways, setting or changing whitelists for example) into their own processes and systems, we offer a REST API specification to integrate the gateways easily into existing systems or automations.

The specification is available at
https://meteringcloudconnect.net/api-documentation.

Gateway Materials

Part	Material	Notes
Enclosure	PC/ABS	• Fire retardant • Corrosion resistant • UL-746C F1 certified (outdoor suitable) • IP67
Screws	A2 304 Stainless steel	• Torx-TR (with Security Pin)
Inserts	Brass	
Batteries	Li-SOCI2	• Low self-discharge (<1% annual) • High temperature range • Long storage life • 10 years storage at room temperature • Hermetic glass-to-metal sealing • Non-flammable electrolyte • Meets IEC86-4 safety standard • Safe to export MSDS, UN38.3 certificate
PCBA		• RoHS / WEEE / REACH compliant
Air vent	PA66 & EPTFE	• IP67

Customisations (Logo / Label / Identifiers)

By default, the Vodafone Logo is embossed on the lid of the gateway.
The embossed logo can be changed upon request and order.
The gateway registers at the middleware using the IMEI of the internal modem. The Serial Number can be changed depending on customer request. Any changes on logo, label or identifiers will take time to change the production process and tooling and will require a certain order volume.

wM-Bus

The gateway supports wireless M-Bus unidirectional communication (receive) in the modes T, C and S at 868 MHz. It supports frame formats A and B, with the limitation that the backend cannot decode frame format B yet.

Additional modes and capabilities may be supplied via future firmware updates and can be requested if needed. All frame data is transmitted as it is collected, without manipulation.

The gateway does not decode any frame information, it only reads the unencrypted header parts of the messages to be able to filter communication of unwanted devices.

All frames read from meters are sent by the middleware via an HTTP cloud adapter to the customers systems. Metadata about the readout is added like "receivedAtGateway" with a timestamp of the synchronized clock of the gateway when the meter frame was read and a "receivedAtCloudAdapter" timestamp with the information when the gateway delivered the readings to our systems (this may differ from the receivedAtGateway time due to the transmission intervals or potential network issues where the gateway stores the frames for later transmission).

Firmware updates

Gateway and modem firmware can be updated for a group of gateways soon via the customer portal or REST API. Individual gateway can also be updated remotely if needed.
Modem firmware and respective changelogs are provided by Nordic Semiconductor (https://www.nordicsemi.com/Products/nRF9160/Download#infotabs).
Gateway firmware and respective changelogs are provided by grandcentrix and can be found at the end of this document and soon also in the customer portal.
Until firmware updates are available in the customer portal, grandcentrix will update gateways when requested or needed.

Additional variant options

Metering Cloud Connect exists as a standard product with Vodafone logo which can be ordered and tested quickly on demand in the variants wM One-Cell and wM Two-Cell (1 or 2 batteries).
Additional options as specified below can be ordered for a custom variant with custom pricing depending on the order size.
All options are also available for our UNE 82326:2010 device variant.

External power supply

The gateways can be ordered with a 5 V external power supply instead of the batteries and an additional cable gland in the enclosure.
The external power supply is connected via the 1X2 XHP-2 connector on the PCBs V_IN(+) and V_IN(-) 1X2 JST B2B-XH-A socket (the same socket used for the batteries).

External button with external LED

If needed, a variant with an external button can be ordered.
The button is equipped with an LED ring and connected to an additional connector on the PCB.

General behaviour

Once connected to power the gateway boots up and enters the warehouse mode. After leaving the warehouse mode with a magnet swipe, it connects to NB-IoT using the attached SIM card and registers with the middleware via a DNS lookup to the default DNS server provided in the network. Upon registration, the gateway transmits its own gateway status information to the middleware, receives the initial configuration and timestamp from the middleware with the information about readout and transmission intervals before going into deep sleep to save battery until the next scheduled readout time. The gateway wakes up at least every 24 hours, signals its status information and waits for commands from the middleware before going into power saving mode (PSM) again.

Gateway status information

The gateway sends additional status information about its state daily and on certain events like bootup, tampering and during manual activations of the hall sensor. This data is also forwarded through the cloud adapter in the GatewayStatusUpdate message type. The data is meant for analysis of network quality, battery health, environmental changes, firmware update status, cloud communication analysis, meter reading analysis, manual activation monitoring and observation of the tampering indicator.
Here is the current list of metrics provided by the middleware through the cloud adapter:

Value	Description	Example
ambientTemperatureDegreeCelsius	Ambient temperature, measured by the gateway – not measured by the meters	23.45
powerSourceVolt	Either battery voltage or voltage of connected power supply	3.282
batteryCapacityMilliAmpHour	Capacity of the installed battery in mAh	19000
lastDataSent	Last time the gateway sent any data to the middleware	2024-09-27T12:38:06Z
lastClockSync	Last update of the internal clock from the server	2024-09-27T12:38:06Z
lastRegistration	Last time the gateway (re-) registered with the middleware	2024-09-27T12:38:06Z
storedMeterDataMessages	Number of frames stored in memory from readouts without transmission	24
totalReadoutDurationSeconds	Number of seconds in RX on wM-Bus	20
totalReadouts	Number of Readouts	24
cloudConnections	Number of connections to the middleware	1
cloudConnectionsFailed	Number of failed connections to the middleware	0
messagesReceived	Number of packets received from the middleware	1
messagesSent	Number of packets sent to the middleware	24
messagesSentWithoutAck	Number of packets sent without receiving an ACK from the middleware	0
networkRegistrations	Number of registrations at the middleware	0
networkRegistrationsFailed	Number of failed registrations to the middleware	0
totalTransmissionDuration	Number of seconds in TX on NB-IoT	11
totalTransmissionWindows	Number of wakeups for transmission of meter data to the middleware	1
timespan.from	Start time of the recorded metrics	2024-09-26T12:37:01Z
timespan.to	Time of sending and resetting of the metrics	2024-09-27T12:38:06Z
cellId	Currently registered Cell ID	18249317
iccid	ICCID of the SIM	89882390000775659157
mcc	Mobile country code of the country currently registered in	262
mnc	Mobile network code of the operator currently used to signal	2
tac	Tracking area code	47849
ecl	Enhanced Coverage Level currently used	0
rsrp	Reference Signal Received Power	-88
rsrg	Reference Signal Received Quality	-10
snr	Signal-to-noise ratio	6
onSiteActivation.dailyLimit	Currently set limit for manual activations via the hall sensor per day	10
onSiteActivation.lastActivation	Last activation of the hall sensor	2024-08-26T09:12:19Z
onSiteActivation.todaysActivations	Number of activations of the hall sensor during the day	0
lastTamperingAlarm	Date where the gateway was last opened	2023-08-25T18:32:42Z
tampered	Status of tamper detection (1 for tampered, can be reset to 0 by the customer)	0

Mobile network connection

The default MFF2 SIM from Vodafone uses multiple network operators per country, to ensure maximum coverage in all supported countries (see country list at https://grandcentrix.net/en/products/documentations/). The gateway uses blank APN/default APN from the network (no specific APN configuration needed).
The gateway also does not set a network code or list of network codes but adheres to the SIMs preferences used or just selects to the strongest signal if no preferences are set in the SIM. Release assistance indication (RAI) is enabled by default. Network timers like RRC IDLE (T3324 – requested to be 30 seconds by the gateway) and Periodic Tracking Area Update (TAU T3412 - requested to be 50 hours by the gateway) are default as well.
Configuration details can be requested to be changed if needed.

Manual readout

A manual readout and subsequent transmission can be triggered by holding a magnet near the location of the hall-effect sensor (see p. 14 Triggering a manual readout). This functionality can be limited to a certain daily maximum or completely disabled via the API in case of misuse or other requirements.

Tamper detection

A detected tampering event (opening of the lid) will instantly wake the gateway up and signal to the middleware. After every opening of the gateway by a technician, the tamper state will need to be reset as the gateway will remember that it has been opened and always report that it has been opened until the status is reset.
In addition to the digital tamper detection, a physical detection mechanism can be achieved via a special sticker applied around the corner of the gateway which leaves marks when being removed to visually indicate opening of the gateway.

Data storage

Meter readings are stored in non-volatile memory and are automatically rotated in a LIFO (last in, first out) manner. The storage is limited to 20 000 frames. Meter readings older than 20 days are dropped automatically. Parameters like the tamper state etc. will be stored in non-volatile memory and can be reset via the customer portal or the REST API.

Whitelisting and meter readings

The wM-Bus is read as specified in the wM-Bus standard.
Which meters should be read, needs to be specified via a whitelist, sent to the gateway from the middleware. The gateway will listen for the specified listening time in every readout session but will stop listening once it received all whitelisted meters successfully to save battery.
All meter readings are collected and stored in non-volatile memory until the next scheduled transmission window. How exactly to set the whitelist is described in the respective section in remote operation.

Data Transmission

When a transmission window or manual activation of a data transmission occurs, the gateway will send out all the stored readings and once a day also the device status information to the middleware. The transmission occurs via NB-IoT on bands 8, 20, or 28.
After the transmission, the gateway will go into RRC IDLE state until timer T3324 expires (30 seconds requested by the gateway). During this period Discontinuous Reception (DRX) is performed, and the gateway listens for commands from the middleware (any scheduled commands form the customer portal or API like configuration changes for example).
The Periodic Tracking Area Update (TAU) - T3412 timer is set to 180000 seconds (50 hours), so it will not trigger due to the daily heartbeat to signal device health. To avoid unnecessary connections, the device can schedule the heartbeat up to 3 hours in advance to match a regular transmission window.
If a connection to the middleware has not been established within 7 days (for whatever reason), a watchdog restarts the gateway.
Release assistance indication (RAI) is enabled by default.
Every transmission of frames is limited to a maximum of 10 minutes, retries to the middleware are done for a maximum of 3 times before going back to power saving mode.

Readout interval / scheduling

By default, the gateway is configured to read the bus every hour, starting when the time was synced with the middleware to ensure that all readings have the correct timestamp. This interval will be overwritten at the same time of the clock sync by the customer specified settings of the assigned gateway group.
Note: Readouts are only executed if a whitelist has been configured and received by the gateway. Readouts are time synchronized, based on 00:00 UTC time.
The gateway also supports an advanced readout scheduling, which will overwrite/replace the basic readout interval, for example, reading every hour between 6AM and 12PM. To ensure easy management of these advanced readout schedules, the API and portal only offer presets to choose from. If your use case is not supported there, please let us know via products@grandcentrix.net, so we can add your scenario.

Transmission interval / scheduling

The default firmware configuration is, that the gateway transmits data every day at around midnight UTC. This interval is overwritten by the setting of the assigned gateway group when the gateway registers with the middleware.

Transmissions configured in the customer portal or via the API are time synchronized, based on 00:00 UTC time. The gateway also supports an advanced transmission scheduling, which will overwrite/replace the basic transmission interval, for example, sending every hour between 9AM and 5PM. To still ensure a somewhat randomized transmission (avoiding network congestion), a “time_shift” between 0- and 300 seconds variation in transmission time is applied.

Security

DTLS

DTLS is enabled by default on all gateways connected to the grandcentrix middleware (from FW version 1.6 onwards). Using DTLS ensures secure authentication between the middleware and the gateways as well as encryption and security against other attack vectors like replay attacks. The gateway is provisioned with an initial key during production to be imported for a secure connection from the start. The key can be rotated if needed.

Private APN

The default installed MFF2 SIM card uses a private APN to isolate the gateways from the public internet and encrypts transmission between the mobile network operator and the middleware without additional battery usage. The private network comes equipped with a DNS server and a record pointing prod.meteringcc.gcx to the middleware servers IP address.

Firmware protection

To protect the firmware from extraction and to prevent anyone from accessing data which they are not supposed to, the Nordic nrf9160 “Access port protection mechanism” is enabled. This mechanism prevents read and write accesses to the flash memory from the local programming interface without issuing an “ERASEALL” command which erases the flash, UICR, and RAM, including the flag itself.

Battery lifetime

Battery lifetime heavily depends on many factors like

- Readout frequency
- Transmission frequency
- Meter sending frequency (and respective listening time of the gateway)
- Network signal at the location of installation
- Network parameters supported/set by the mobile network operator
- Amount of data transmitted and received
- Frequency of manual activation

This is why battery lifetime is always an estimate within a certain range and specific parameters. To get an estimate of the battery lifetime of the gateway in your planned scenario, download/copy and modify the parameters using the MECC - Battery lifetime calculator: https://t.ly/0yrl9

Modem and NB-IoT Network details

The gateway uses the Nordic nRF9160 module which is a combined MCU and Modem. The modem is GCF, PTCRB, FCC, CE, UKCA, ISED, SRRC, ACMA RCM, NCC, IMDA, MIC certified and tested around the world in different networks.
See: https://www.nordicsemi.com/Products/Wireless/Low-power-cellular-IoT/nRF91-Series-certifications/nRF9160-Global-and-regulatory?lang=en#infotabs
and https://www.nordicsemi.com/Products/Wireless/Low-power-cellular-IoT/nRF91-Series-certifications/Mobile-network-operator?lang=en#infotabs.
The LTE modem is compliant with 3GPP LTE release 13 Cat-M1 and Cat-NB1, as well as the 3GPP LTE release 14 Cat-NB2 standard.
See: https://infocenter.nordicsemi.com/pdf/nRF9160_PS_v2.1.pdf.

The gateway supports the following 3GPP NB-IoT Release 14 features:

- MAC inactivity monitoring
- RSRQ in connected mode
- AS-RAI
- NB2 Dual HARQ
- NB2 TBS

The modem supports eDRX. It is disabled by default and can be activated if the network operator supports it.

In person operation

Indications during warehouse mode

If the battery is already connected upon receiving the gateway, it will be in warehouse mode and completely inactive in deep sleep to save battery until put into working mode via the HALL sensor activation. If the battery is not connected upon receiving the gateway, the gateway will enter the warehouse mode once the batteries are installed. This will be indicated by a short beep and both internal LEDs flashing once.
When leaving the warehouse mode via the hall sensor, the gateway will start normal operation and trigger a manual readout as described in Triggering a manual readout.

LED and Buzzer indications

The gateway indicates its status visually and audible at the same time to accommodate for different environments during operation when activated via the HALL sensor or when the gateway is open as a technician is assumed to be present.
During normal operation (scheduled readouts or transmissions), the gateway remains silent, and the internal LEDs are turned off to save battery.

Equipment	Indicating
Yellow Cloud LED	Cloud (NB-IoT) activity
Green metering LED	wM-Bus activity
Buzzer	Simultaneous indicating cloud connectivity and metering bus activity for easy installation and cases when the LEDs can’t be seen easily.

Signal	Meaning	Proposed action
Short meter indication every 5 sec (Green Meter LED & Buzzer)	Readout in progress	Wait until all the meters have sent their data or the RX on time is over
Short cloud indication every 5 sec (Yellow Cloud LED & Buzzer)	Transmission / connection in progress	Wait until the gateway connected to the backend, sent the data and received an ACK
2 Short meter indications (Green Meter LED & Buzzer)	Successfully readout at least one meter value	-
2 Short cloud indications (Yellow Cloud LED & Buzzer)	Successful connection to the middleware & Data sent	-
1 Long meter indication (Green Meter LED & Buzzer)	Frames could not be received from meters	Check if you have meters whitelisted
1 Long cloud indication (Yellow Cloud LED & Buzzer)	Connection to middleware failed (Frames could not be sent / Connection failed)	Reset the gateway at a different location to ensure it has network coverage
1 Short indication (Both LEDs & Buzzer)	Warehouse mode entered	Close the gateway and store it until it is needed
3 Long indications (Yellow Cloud LED & Buzzer)	The gateway has a severe error and might be broken	Try a different gateway and if this does not solve the issue, contact customer support

Inserting or changing the battery

Place the single or double battery pack upright into the holder beside the PCBA and connect the JST 1X2 XHP-2 connector to the PCBs 1X2 JST B2B-XH-A socket. The polarity of **V_IN(+)** and **V_IN(-)** should be adhered to and the connector should not need to be forced into the socket.
If the battery pack you are using has been supplied by a third party, please make sure that the polarity of the cable and the connector is correct before connecting it to the board. You should hear a “click”, indicating that the battery connector is securely connected.
Upon first insertion of a battery, the gateway will enter warehouse mode (indicated by a single indication). Only after the activation of the hall sensor, the gateway will boot up. During battery replacement, the gateway won’t enter the warehouse mode again.

Triggering a manual readout / Wakeup from warehouse mode

Use a magnet to trigger the Hall-sensor on the left side of the device. The sensor location is indicated by the magnet-symbol **N | S** on the outside of the enclosure. Triggering this sensor will always enable the indications (which are shut off in normal operation when the gateway is closed), so it can be understood what the gateway is doing.
The HALL sensor will activate the gateway from warehouse mode (if it was in warehouse mode). In this case, the gateway will first connect to the middleware to receive its configuration and sync its clock before proceeding with a readout of the bus and then signalling the results to the cloud again.
When the gateway is already in operation, activating the HALL sensor will trigger a manual readout, listening for the configured wM-Bus meters and transmitting their data to the cloud. The manual readout will fail (with a long meter indication) if a whitelisted meter can’t be received.

Local reset of the gateway

The reset button is placed on the inside of the device on the PCBA.
Press the button for at least 4 seconds.
While you press the button, both LEDs should be ON.
If the LEDs are not lighting up, the device either has no power or the gateway is in the warehouse mode.

Local reset to warehouse mode

If the gateway should be reset back to warehouse mode locally (not via the REST API or customer portal), the tamper switch needs to be held down while resetting the gateway by holding down the reset button as well until both LEDs turn off.

Gateway identification and product label

The gateway is bound to an IMEI that belongs to the modem inside it. The IMEI can be found on the Label on the side of the device, as well as on the NFC tag (located behind the label).
When registering with the middleware, the gateway will use the IMEI as the unique identifier.

The serial number on the gateway can also be used to uniquely identify a gateway.
The default serial number is formatted like the following:

MEC	-	A06	-	0002	-	24190	-	0324
Product	-	Variant	-	Production Version	-	Test date (YYWW) and number of test machine	-	Sequence number of that week and line

The product label contains the following information:

Alternative content can be definded per order if required.

Identifying the gateway via QR-Code or NFC

A QR code of minimum 20mm x 20mm is located on the side of the gateway. It contains the IMEI of the modem.
It is intended to be used as a visual scanning alternative to the NFC tag.

Alternative content can be defined per order if required.

An NFC tag is located behind the label (visible on the outside of the enclosure). It contains the following information separated by “_” IMEI, Serial Number, Manufacturer:

350457790801516_MEC-A06-0002-24190-0324_grandcentrix-GmbH

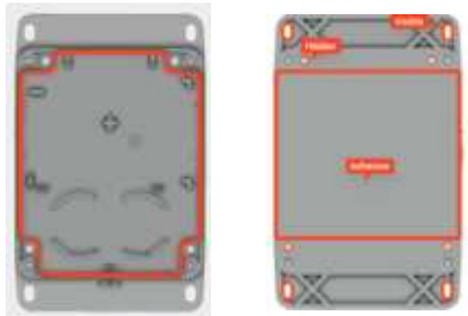
Alternative content can be definded per order if required.

Opening and closing the gateway

When opening the lid of an operational gateway, the tamper detection will be triggered. The gateway will instantly send the tampering event and device information to the middleware and store the tamper state until a reset command is received from the middleware. If a sticker seal is applied, this will mark the gateway as tampered as well.

The gateway lid screws are M4x40 ISO 14581 screws which either feature a standard T20 Torx screw, or a tamper resistant T20 Pin Torx-TR (depending on customer request).
Before inserting the screws, check that the lid is oriented correctly and that the logo is on the opposite side of the pressure valve.

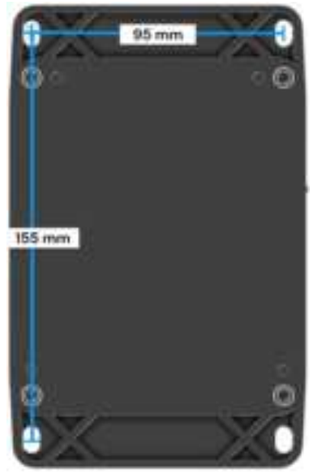
The screws should be tightened with a force of 0,7 Nm (Newton meters) to ensure optimal compression of the seal and minimal stress on the threaded inserts. If desired, a seal can be stuck over the corner of the device where the lid and the base meet. Clean and dry the location of the sticker first and press the sticker on firmly to make sure it sticks well.



Mounting

The gateway should be mounted vertically, so the air vent is pointing downwards to have the logo in the correct direction.
It can be mounted on a load-bearing substructure by using adhesive, hidden mounting (only accessible when the gateway is open) or visible mounting.

Mounting equipment is not included with the product.



Accessible Mounting

With this mounting option, the screws are accessible when the gateway is closed. We recommend using 5mm diameter screws and ISO 7089 M5 washers.
The mounting holes are 95mm by 155mm apart.

HIdden screw mounting

With this mounting option, the screws can only be accessed when the gateway is open. The four mounting holes are below the lid of the enclosure, next to the threaded inserts.
We recommend using 3mm screws and ISO 7089 M3 washers.

Adhesive mounting

This mounting option can be done with a double-sided adhesive pad for example.
The maximum dimensions of the pad should be 130mm x 90mm or 110mm x 100mm.

Changing the SIM card

By default, our gateways ship with a preconfigured non-replaceable MFF2 SIM card, securely connected to the grandcentrix middleware.
If you ordered your gateways with a SIM slot, just replace the 4FF SIM card in the SIM slot on the PCBA.
Make sure that the SIM is activated by the network, allowed to connect to NB-IoT and that there is a provider in the country of operation supporting NB-IoT.
No APN needs to be configured.

After installation of the SIM, hold down the reset button on the PCBA as described in the section Local reset of the gateway.
After the reset, the gateway should start booting up again and indicate connection to the middleware.

Make sure that the middleware can be reached by the new network. For further details see the Middleware section. The grandcentrix LwM2M middleware is isolated in a secured network and cannot be reached from the public internet.

Remote operation

This section lists the actions which can be performed on a gateway from a distance.
Please keep in mind that the gateway is in deep sleep for most of the time, so any command to the gateway you send, will be executed and acknowledged by the gateway once it connects to the cloud the next time to transmit data. This can take up to 25 hours.

Customer portal

To easily manage and see the capabilities of the gateways, customers can use the grandcentrix Metering Cloud Connect portal at https://meteringcloudconnect.net/. Meter data is not displayed there, as it will only be forwarded to customer systems via cloud adapters (those can be set up via the portal soon).

Login

As the customer portal is still very new, individual user logins are not yet supported. Instead, the gateway operator name (customer name) and access key are used as common credentials for the whole account.

Gateway group list view

All gateways are organized in gateway groups for easier management of larger fleets. These groups are shown on the home screen and can be added, renamed, described and deleted (if no gateways and cloud adapters are assigned).
A default group is created upon assignment of the first gateway to the customer account.

Gateways can be assigned by clicking the “Gateway Assignment” button, selecting the two groups to move gateways from and to, selecting the gateways to move and then clicking the arrow button to move the selected gateway to the other group.

Gateway group detail view

When clicking on a gateway group on the gateway group list view, the respective detail page of that group will open. In this group detail view, the readout and transmission interval as well as the daily on-site readout limit (maximum allowed manual readouts per day using the magnet) can be set for all assigned gateways of that group.

Below the configuration is the list of all currently assigned gateways of the selected gateway group. Soon, the firmware version and cloud adapter connection can be configured in this view as well.
Adding and removing gateways from groups will also be added soon.

Update gateway group

To update the readout and transmission profile, edit the gateway group. The edit gateway group popup should open where the interval can be configured, or a time window preset can be selected.

If the required use case cannot be fulfilled via the intervals of available presets, please contact customer support to add your case to the presets.

The field below allows to change the daily on-site readout limit (number of activations allowed per day via the HALL-sensor).
This change will reset the daily readout limit counter. All gateways of that group will allow manual activations again until the configured limit is reached again on that day.
Setting the daily on-site readout limit to 0 will deactivate the option to trigger manual readouts via the HALL-sensor.

Gateway detail page

When clicking on a gateway on the gateway list, the respective detail page of that gateway will open.
On the gateway detail page, the gateway can be renamed (small icon after the gateway name), and commands can be scheduled to be sent to the gateway when it wakes up the next time and communicates with the middleware.
Only one command of each type can be scheduled at a time, so if there is already a scheduled reboot for example, another reboot can't be scheduled.
The gateway detail page also lists the last seen information of the gateway (see screenshot below for details).

Meter configuration

To connect a meter, a whitelist needs to be configured per gateway which contains the wM-Bus mode to be used as well as the maximum listening time in seconds. Possible modes are unidirectional S, T and C.

The whitelist also allows to define decoding parameters (if enabled for your account), as well as defining when the gateway should transmit values instantly due to an alarm received from a meter (see Instant transmission on alarm detection).
To ease configuration, it is also possible to scan for available meters and configure them with a simple button press.

Whitelisting wM-Bus meters

Make sure to set the correct wM-Bus mode of your meters, this needs to be the same mode for all meters in your whitelist. In most cases whitelisting the meter id (an 8-digit number written on the meter) is sufficient. The listening interval should be the maximum transmission interval of your meter multiplied by 1.2 (20% buffer) to make sure to catch every meter configured in the whitelist.

For example: if you have 15 meters with a transmission interval of 16 seconds and one with a transmission interval of 60 seconds, set your listening time to 60*1.2 = 72 seconds.
The gateway will listen until all meters are received, but at a maximum for the configured listening time. To be sure to not waste battery, this listening time should not be increased unnecessarily, as it will be used when the whitelist contains a meter which is not reachable for whatever reason.

If no meter is whitelisted, the gateway will not start listening for any meter.

Scanning for meters

The gateway supports scanning the radio frequency to check which meters are in range to be read or to see if a meter responds within a longer listening interval.
A scan can be scheduled to be executed for a configurable amount of time on the specified wM-Bus mode and will return found meters after completion.
The scan result will contain all seen meters with their respective ID, manufacturer, version and device type and signal strength as well as the last seen date.
These meters can easily be added to the whitelist if needed.
The scan is limited to 150 meters maximum.

wM-Bus frame decoding (experimental)

As an experimental feature, wM-Bus decoding can be enabled per customer account by grandcentrix if needed.
In this case, also the correct driver and cryptographic key (if frames are encrypted) of each meter needs to be provided in the whitelist. This key won't be transmitted to the gateways, but will remain on the backend, where the decryption is done. The decoded frame content is attached to the cloud adapter JSON content.
Since every meter supports different fields in different formats, a driver needs to be selected per meter. See supported meters and drivers to be used at:

https://github.com/wmbusmeters/wmbusmeters?tab=readme-ov-file.

Should decoding not be possible with any of the drivers available, please contact customer support and request the driver for your specific meters to be developed.

Instant transmission on alarm detection

If your use case requires time sensitive alarming, but the gateways should usually send data infrequently to increase battery lifetime, the gateways can be configured to listen for a specific bit in the unencrypted part of the wM-Bus frame to identify an alarm. If this alarm is detected, the gateway will trigger an instant transmission instead of going back to sleep until the next scheduled transmission time.

To configure this alarm bitmask, please check the manual of your meter to see which bits represent which alarm or error and configure the bitmask in the metering cloud connect portal accordingly.

Remote resetting of the warehouse mode

Should the gateway(s) wake up for any reason within the warehouse when they are not supposed to be active, they can remotely be returned to the warehouse mode to preserve battery and prevent connectivity cost.

Re-entering warehouse mode needs to be done via the API as it will mean that you lose remote access to the gateway. This feature was developed as a precaution and should ideally never be needed as the HALL-sensor should be insensitive enough to not trigger from a distance. If a reset to warehouse mode is- or was scheduled, it will be displayed in the customer portal.

Cloud Adapter / Meter data export

As meter data is only forwarded to your servers, a cloud adapter is needed to define the server and HTTP command to use when new metering data is forwarded.
Each gateway group can have a cloud adapter assigned to which all metering data of the gateways in that group will be forwarded.
A cloud adapter will also forward data of actionable or noteworthy events, like tampering alarms and errors, so you can react quickly and monitor them.
In a future API update, those events can be split out and be sent to different systems for processing than your meter data system.

Demo dashboard example

Grandcentrix provides a demo dashboard on request. This can be found on at https://demo.meteringcloudconnect.net/ The demo dashboards consist of two types of dashboards.
The “Gateway Dashboard” shows the debug parameters of the gateway to quickly glance any issues with connectivity, meters, etc.
“Meter Dashboards” are created for every specific connected meter, since the provided data from all meters differ.
Please reach out to us via products@grandcentrix.net to help you set up a dashboard for the meters you want to connect.

REST API

The grandcentrix REST API ensures, that you can easily and programmatically manage your gateways and setup. Depending on your use case, requirements and installation procedure, the API can easily be integrated into your apps, software or services.

To send metering data collected by the gateways to your systems, we use so called “Cloud Adapters”, also known as webhooks or HTTP callbacks. Those Cloud Adapters send JSON formatted meter data (including the raw frames received) via HTTP to the server of your choice.

The Cloud Adapter HTTP JSON format can be found in the REST API specification under “createCloudAdapter” -> “Callback payload samples”.

Middleware

The middleware handles all the translation of low-level LwM2M via UDP device commands to JSON sent via the Cloud Adapter using HTTPS to customer systems.

The middleware (according to LwM2M) is responsible to do session handling (with or without DTLS), device data processing, firmware update handling and device communication capabilities to allow two-way communication with the gateways.

The REST API documentation can be found at: https://meteringcloud-connect.net/api-documentation

For customers who don’t have a meter data system, we can set up a demo dashboard to show how the data can be received and monitored. Alternatively, tools like https://requestcatcher.com can be used to just see the data coming in without a lot of effort. https://webhook.site/ or automation tools like https://zapier.com, https://www.make.com can be used to receive, view, modify or store metering data in any way needed without any development effort.

grandcentrix also offers support with building custom solutions or integrating data in any way needed. See what we offer at https://grandcentrix.net/en/services/backend/. We also work with partners like https://device-insight.com/ and https://datacake.co/ to increase the deployment speed and reduce cost of custom use cases.

Safety instructions

Signal words

The following signal words are used in this manual:

WARNING!
This classifies a hazard of medium risk level. Failure to comply with the warning may result in serious injury.

Please note:
This is a warning about possible damage to property.

Proper use

Please read the safety instructions for this Metering Cloud Connect Gateway, hereinafter only referred to as MECC, carefully before use in order to be able to deploy it properly. The intended use is to employ the MECC only as described in this manual to locate an object. Please bear in mind that it is a criminal offence to monitor meters without consent of the respectful owner. If you use it in any other way, this is considered improper use and can lead to damage to property or even personal injury.

Please note that the MECC is not a toy for children and should therefore be mounted out of reach. In other countries and regions there are different laws on digital positioning and localization objects. Grandcentrix is not responsible if such laws or regulations are violated, this is the sole responsibility of the user.

Please note: The manufacturer and dealer accept no liability for damage caused by improper or incorrect use.

Safety

WARNING! RISK OF ELECTROCUTION!

A faulty electrical installation or an excessive mains voltage may cause an electric shock.

- If you notice any visible damage to your MECC, do not use it.
- Never place the MECC near an open fire or hot surfaces.
- The MECC is only protected against humidity and water within IP67 when properly closed. Please protect the insides from direct water exposure.
- Do not open the housing of the MECC except for replacing the batteries or rebooting the gateway. Leave the repair to qualified specialists. However, if you carry out repairs yourself, connect the MECC incorrectly or operate it incorrectly, liability and warranty claims are excluded.

Battery mode

WARNING! DANGER OF EXPLOSION and FIRE!

Below you will find information and instructions on how to use the battery:

- The MECC runs by a Li-metal battery (LiSOCl2 to be specific). It is not rechargeable and must be removed once it's empty.
- Use only the original battery packs supplied as a power source. If the battery cable is damaged, replace it only with original accessories from the manufacturer.
- Make sure that the MECC is kept away from heat sources and high temperature. Disregard of this instruction may result in destruction of the battery and overheating, explosion, and fire. Do not burn or pierce the MECC. Protect it from mechanical damage.
- Do not remove the battery-pack with sharp or pointed objects. Do not drop, disassemble or modify it.
- If a child swallows the battery, seek medical aid immediately!

WARNING! DANGER OF CAUTERIZATION!

Batteries that leak due to damage may cause burns in contact with the skin. Therefore, never open the battery. However, if the battery leaks, please wear protective gloves.

Electromagnetic compatibility

Please observe all rules and prohibitions and switch off the MECC immediately in danger areas and if it might cause interference. Furthermore, it should not be used in the vicinity of, for example, medical equipment, fuels, and chemicals, or in blasting areas.
With mobile devices, malfunction due to interference may occur and affect performance. Transformers and very strong magnetic fields must be avoided. Otherwise, there may be deviations in the transmission. Disregard of these instructions may cause unintended readouts and drain the battery life.

Cleaning

WARNING! RISK OF DAMAGE!

Below you will find information and instructions on how to clean the MECC:

- Do not use aggressive cleaning agents or brushes for cleaning. Do not clean the MECC with metallic cleaning objects (e.g. knife, metal sponge). This may damage the surface.
- Never put the MECC in a dishwasher (or the like) and do not use a steam cleaner.

Correct cleaning:

- The surface may be wiped clean with a slightly damped cloth.
- The MECC should then be wiped dry completely.

Dangers for children and people in need of help

Please do not let people (including children) with limited physical, sensory or mental abilities use the MECC. It is considered an exception if they have previously received instructions from a person responsible for their safety on how to use the device. Please be sure that they do not play with small parts (e.g. accessories, etc.). These may be swallowed, leading to suffocation. Inform your child about the dangers and about how to use the MECC.

Storage

If you are not using the MECC for a lengthy period, disconnect the battery-pack and place the device in its original packaging or in a carton of the same size. Protect the MECC from dirt and humidity. Keep out of the reach of children. The battery voltage may lower over time due to battery passivation. The passivation effect will vanish after a while of using the battery again.

Declaration of conformity

grand centrix
A Vodafone Company

EU-Konformitätserklärung / EU Declaration of Conformity

CE

Wir, der Hersteller

grandcentrix GmbH
Holzmarkt 1
50676 Köln

erklären in alleiniger Verantwortung, dass die Produkte / Modelle

Metering Cloud Connect, Modelle MEC-A04, MEC-A06

auf die sich diese Erklärung bezieht, den relevanten Richtlinien und Verordnungen entsprechen. Die Konformität bezüglich der notwendigen Eigenschaften wurde anhand der folgenden Normen und normativen Dokumenten überprüft.

Norm	Richtlinie / Anforderungen
EN 62368-1:2014 EN 62311:2008	2014/53/EU Funkanlagenrichtlinie Artikel 3 (1) a) Gesundheit und Sicherheit
EN 301 489-1 V1.9.2 EN 301 489-3 V2.1.1 EN 301 489-52 V1.2.1 EN 61000-6-2:2005	2014/53/EU Funkanlagenrichtlinie Artikel 3 (1) b) Elektromagnetische Verträglichkeit
EN 301 908-1 V15.2.1 EN 301 908-13 V13.2.1 EN 300 220-2 V3.1.1	Artikel 3 (2) Effektive und effiziente Nutzung des Funkspektrums
EN IEC 63000:2018	2011/65/EU RoHS + 2015/863

Köln, 07.12.2023

Roland Hänel (CTO)

We, the manufacturer

grandcentrix GmbH
Holzmarkt 1
50676 Köln

declare under our sole responsibility that the products / type models

Metering Cloud Connect, models MEC-A04, MEC-A06

to which this declaration relates conform to the relevant directives and regulations. The conformity with the essential requirements has been demonstrated against the following standards.

Standard	Directive / Requirement
EN 62368-1:2014 EN 62311:2008	2014/53/EU Radio Equipment Directive Article 3 (1) a) Health and Safety
EN 301 489-1 V1.9.2 EN 301 489-3 V2.1.1 EN 301 489-52 V1.2.1 EN 61000-6-2:2005	2014/53/EU Radio Equipment Directive Article 3 (1) b) Electromagnetic Compatibility
EN 301 908-1 V15.2.1 EN 301 908-13 V13.2.1 EN 300 220-2 V3.1.1	Article 3 (2) Effective and Efficient Use of Radio Spectrum
EN IEC 63000:2018	2011/65/EU RoHS + 2015/863

Cologne, 07.12.2023

Roland Hänel (CTO)

Declaration of comformity

Should a migration to a customer-owned middleware be required at any time, this can easily be done as the gateway is programmed from factory to connect to prod.meteringcc.gcx which can be routed via the middleware of choice in a private network.

Disposal of packaging

Dispose of the packaging according to type.
Add cardboard to the paper bank, plastics to the recyclables collection.

Disposal of used batteries

The following instruction is aimed at those who use batteries or products with built-in batteries and do not resell them in the form supplied to them (End-users).

Acceptance of returned used batteries free of charge

Batteries must not be disposed of with household waste. You are legally obliged to return used batteries so that proper disposal can be guaranteed. You can dispose of used batteries at a municipal collection point or at a local retailer. As a distributor of batteries, we are also obliged to take back used batteries, whereby our obligation to take back only applies to the type of used batteries that we have or had as new batteries in our range. Used batteries of the type LiSOCl2 can therefore either be returned to us with sufficient prepayment or directly to our shipping warehouse at the following address free of charge: grandcentrix GmbH, Holzmarkt 1, 50676 Cologne, Germany

Meaning of the battery symbols

Batteries are marked with the symbol of a crossed-out dustbin (see following illustration). **This symbol indicates that batteries must not**

Glossary

Name	Description
MECC	Short for Metering Cloud Connect, also just called “gateway”.
Meter	Meter may stand for any connected device and may be a water meter, heat meter, smoke detector, heat cost allocator, or any other device communicating via wM-Bus.
HW	Abbreviation for Hardware (typically the PCBA – sometimes the Enclosure and all connected physical parts like the UNE cable as well).
FW	Abbreviation for Firmware (Software installed on the Gateway).
PCBA	A printed circuit board (PCB) is the board where all electronic components are mounted to and connected with each other. The PCB with components on it is called PCBA (A for assembled).
Cloud Adapter	URL configured in the grandcentrix middleware to forward metering data to. Otherwise known as webhook or HTTP callback.
Portal	The grandcentrix user interface or customer portal to configure the gateways as well as the cloud adapter. It can also be used to quickly check the status of gateways.
REST API	An HTTP application programmable interface to be used by web portals, apps, automation tools or any other application that is used to manage our gateways or meters connected to our gateways.
Middleware	The system which is securely connected via a tunnel to the private mobile network and communicates with authorized gateways using the LwM2M via UDP protocol. The grandcentrix middleware also offers a public REST API and Cloud Adapters.
Rev	Abbreviation for “Revision” (or change version).
LwM2M / OMA	Lightweight M2M is an open protocol from the Open Mobile Alliance (OMA) that is designed for addressing the needs of mobile low-power devices with very little compute power. LWM2M® is being adopted widely by telecom operators and is emerging as the standard protocol for device management and service enablement.
DLTS	Datagram Transport Layer Security (DTLS) is a communications protocol providing security to datagram-based applications by allowing them to communicate in a way designed to prevent eavesdropping, tampering, or message forgery. The DTLS protocol is based on the stream-oriented Transport Layer Security (TLS) protocol and is intended to provide similar security guarantees.
NB-IoT	GSMA definition: Narrowband-Internet of Things (NB-IoT) is a standards-based Low Power Wide Area (LPWA) technology developed to enable a wide range of new IoT devices and services. NB-IoT significantly improves the power consumption of user devices, system capacity and spectrum efficiency, especially in deep coverage.
HALL Sensor	HALL effect sensors record magnetic fields and translate them to electrical signals, so a magnet presence can be indicated.
NFC Tag	NFC (Near Field Communication) tags are wirelessly communicating previously stored information (like identification information) to a receiver.
ACK	Short for “Acknowledgement” where the receiving party sends back the “ACK” information, confirming that data was received correctly.
Heartbeat	Heartbeat defined a communication by the gateway to the middleware in a fixed interval (independent of the transmission configuration) to signal that the gateway is still operational.
Watchdog	Defines a process running even in deep sleep to wake the gateway from deep sleep - in case no connection to the middleware has happened. This process ensures that the gateways are reachable from the middleware and reset themselves if they are not for any reason to get back online.
WEEE	“Waste of Electrical and Electronic Equipment”.
TBD	Short for “to be defined”.
IMEI	The „International Mobile Equipment Identity” is a unique identifier of the modem used in the device which is transmitted to the network by default and stays the same for any network operator.
PSM	“Power saving mode” is a feature of NB-IoT which allows the device to go into a deep sleep mode for an extended time without needing to reconnect when waking up and signalling to the network again.
FOTA	“Firmware over the air” allows you to send a command from the middleware to the gateway with the location of the new firmware and the gateway will download it and apply the update without the need for the operator to physically be close to the gateway.
OMS®	The Open Metering System (OMS®) is based on M-Bus / wM-Bus. It is the only system definition across Europe which integrates all media (electricity, gas, heat and water incl. submetering) into one system. The OMS-Group e. V. is a nonprofit organization and interest group of meter manufacturers, utilities, meter operators, electronics manufacturers, communication firms, and IT companies. Metering Cloud Connect uses some OMS defined mechanisms when available from the meter.
UNE Bus	Metering Cloud Connect is also available with a cable using the UNE 82326:2010 bus specification for the Spanish market. UNE 82326:2010. This variant is not further described in this document, details can be requested or found here: https://grandcentrix.net/en/products/metering/.

Document version history

Version	Date	Change
V1.0	01. Oct 2022	Document creation
V1.1	02. Apr 2023	Installation feedback via LED and buzzer improved
V1.2	15. Aug 2023	Device to Cloud API updated: • Added readout and transmission scheduling • Added operating parameters
V1.3	26. Oct 2023	Device to Cloud API updated: • Added readout and transmission scheduling • Added operating parameters • Added storage reset option • Added manual readout limitations
V1.4	04. Nov 2023	Added images to describe functions and mounting Added input voltage range Added version history & glossary
V1.5	09. Dec 2023	Added debug connector usage description Updated installation feedback for HW rev V1.6 and firmware V1.3
V1.6	08. Apr 2024	Added warehouse mode description Added middleware connection description Added network parameter detail descriptions
V1.6.1	17. Apr 2024	Added debug port protection description
V1.6.2	29. Apr 2024	Added custom order options
V2.0	13. Aug 2024	Removed wM+ variant Added own middleware and REST API documentation Added customer portal documentation
V2.1	26.11.2024	Changed Demo dashboard example

Firmware changelog

FW Version	Modem FW Version	Release Date	Changes
V1.0	V1.3.5	Oct 2023	Initial product release
V1.1	V1.3.5	Dec 2023	• Registration using IMEI • External storage support • Debug access via RTT
V1.2	V1.3.5	Feb 2024	• Readout and transmission scheduling • Delete frames older than 20 days • Limit sending to 10 minutes • Cloud LED usage • Storage reset option
V1.3	V1.3.6	Mar 2024	• Option to limit manual activations • Option to update DTLS keys via middleware
V1.3.1	V1.3.6	Apr 2024	• Warehouse mode added
V1.4	V1.3.6	Jun 2024	• NB-IoT Release 14 features • Expose serial number to LwM2M • Expose HW revision to LwM2M • Maximum UDP message size increased • LEDs and buzzer enabled when gateway is open • wM-Bus scan feature
V1.5	V1.3.6	Aug 2024	• Persist fuel gauge, time, warehouse mode, whitelist, readout and send schedule, etc. on power loss • Warehouse mode reset option (local & remote) • Increase default send interval to 24h • wM-Bus driver improvements • Readouts require time sync • Immediate transmission on alarm feature • Report manual gateway activations
V1.6	V1.3.6	Oct 2024	• Enable DTLS by default with the middleware
V1.7	V1.3.6	Nov 2024	• FOTA indications optimisation • Command feedback improvements for warehouse mode and reboot