# SOLVIMUS
## METERING SOLUTIONS

## MBUS-GEV - USER MANUAL

# MBUS-GEV
# Gateway for
# Smart Metering

Version: 1.1
Date: 23 February 2024

Firmware Version 1.36

Authors:
Remo Reichel, Frank Richter
solvimus GmbH
Ratsteichstr. 5
98693 Ilmenau
Germany

...we solve.                                   www.solvimus.de

Page intentionally left blank

Page 2/81

Version: 1.1

Frank Richter, 23 February 2024

UG_EN_MBUS-GEV.pdf

Released

© solvimus GmbH

# Table of Contents

Page 4/81

UG_EN_MBUS-GEV.pdf

Version: 1.1

Released

Frank Richter, 23 February 2024

© solvimus GmbH

# 1 Notes and conventions

## 1.1 About this document

This manual provides guidance and procedures for a fast and efficient installation and start-up of the units described in this manual. It is imperative to read and carefully follow the safety guidelines.

## 1.2 Legal basis

### 1.2.1 Placing on the market

Manufacturer of the MBUS-GEV is the solvimus GmbH, Ratsteichstraße 5, 98693 Ilmenau, Germany.

### 1.2.2 Copyright protection

This documentation, including all illustrations contained therein, is protected by copyright. The author is solvimus GmbH, Ilmenau. The exploitation rights are also held by solvimus GmbH. Any further use that deviates from the copyright regulations is not allowed. Reproduction, translation into other languages, as well as electronic and phototechnical archiving and modification require the written permission of solvimus GmbH. Violations will result in a claim for damages. The solvimus GmbH reserves the right to provide for any alterations or modifications that serve to increase the efficiency of technical progress. All rights in the event of the granting of a patent or the protection of a utility model are reserved by solvimus GmbH. Third-party products are always mentioned without reference to patent rights. The existence of such rights can therefore not be excluded.

### 1.2.3 Personnel qualification

The product use described in this documentation is intended exclusively for qualified electricians or persons instructed by these. They must all have good knowledge in the following areas:

- Applicable standards
- Use of electronic devices

### 1.2.4 Intended use

If necessary, the components or assemblies are delivered ex works with a fixed hardware and software configuration for the respective application. Modifications are only permitted within the scope of the possibilities shown in the documentation. All other changes to the hardware or software as well as the non-intended use of the components result in the exclusion of liability on the part of solvimus GmbH. Please send any requests for a modified or new hardware or software configuration to solvimus GmbH.

### 1.2.5 Exclusion of liability

Study this manual and all instructions thoroughly prior to the first use of this product and respect all safety warnings, even if you are familiar with handling and operating electronic devices.

The solvimus GmbH accepts no liability for damage to objects and persons caused by erroneous operation, inappropriate handling, improper or non-intended use or disregard for this manual, especially the safety guidelines, and any warranty is void.

### 1.2.6 Disclaimer

All products, company names, trademarks and brands are the property of their respective holders. Their use serves only to describe and identify the respective company, product or service. Use of them does not imply any affiliation with, commercial relationship with or endorsement by them.

Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.

Chrome™ browser is a trademark of Google Inc.

Microsoft Excel is a trademark of the Microsoft group of companies.

7-Zip Copyright (C) 1999-2022 Igor Pavlov.

Wireshark: Copyright 1998-2022 Gerald Combs <gerald@wireshark.org> and contributors.

## 1.3 Symbols

- ❌ Danger: It is essential to observe this information in order to protect persons from injury.
- ⚠ Caution: It is essential to observe this information in order to prevent damage to the device.
- ⓘ Notice: Boundary conditions that must always be observed to ensure smooth and efficient operation.
- ⚠ ESD (Electrostatic Discharge): Warning of danger to components due to electrostatic discharge. Observe precautionary measures when handling components at risk of electrostatic discharge.
- ✔ Note: Routines or advice for efficient equipment use.
- ➡ Further information: References to additional literature, manuals, data sheets and internet pages.

## 1.4 Font conventions

Names of paths and files are marked in italics. According to the system the notation is using slash or backslash.
e. g.: *D: \Data*

Menu items or tabs are marked in bold italics.
e. g.: ***Save***

An arrow between two menu items or tabs indicates the selection of a sub-menu item from a menu or a navigation process in the web browser.
e. g.: ***File → New***

Buttons and input fields are shown in bold letters.
e. g.: **Input**

Key labels are enclosed in angle brackets and shown in bold with capital letters.
e. g.: ⟨**F5**⟩

Programme codes are printed in Courier font.
e. g.: `ENDVAR`

Variable names, identifiers and parameter entries are marked in italics.
e. g.: *Value*

## 1.5 Number notation

Numbers a noted according to this table:

| Numbering system | Example | Comments |
|---|---|---|
| Decimal | 100 | Normal notation |
| Hexadecimal | 0x64 | C-like notation |
| Binary | '100' | In apostrophes |
| | '0110.0100' | Nibbles separated by dots |

Table 1: Numbering systems

Page 6/81
UG_EN_MBUS-GEV.pdf
Version: 1.1
Released
Frank Richter, 23 February 2024
© solvimus GmbH

## 1.6 Safety guidelines

✖ Observe the recognized rules of technology and the legal requirements, standards and norms, and other recommendations.

✖ Study the instructions for the extinction of fire in electrical installations.

✖ The power supply must be switched off before replacing components and modules.

If the contacts are deformed, the affected module or connector must be replaced, as the function is not guaranteed in the long term.

The components are not resistant to substances that have creeping and insulating properties. These include e.g. aerosols, silicones, triglycerides (ingredient of some hand creams). If the presence of these substances in the vicinity of the components cannot be excluded, additional measures must be taken:

- Install the components in an appropriate casing.
- Handle components with clean tools and materials only.

⚠ Only use a soft, wet cloth for cleaning. Soapy water is allowed. Pay attention to ESD.

⚠ Do not use solvents like alcohol, acetone etc. for cleaning.

⚠ Do not use a contact spray, because in an extreme case the function of the contact point is impaired and may lead to short circuits.

⚠ Assemblies, especially OEM modules, are designed for installation in electronic housings. Do not touch the assembly when it is live. In each case, the valid standards and directives applicable to the construction of control cabinets must be observed.

⚠ The components are populated with electronic parts which can be destroyed by an electrostatic discharge. When handling the components, ensure that everything in the vicinity is well earthed (personnel, workplace and packaging). Do not touch electrically conductive components, e.g. data contacts.

## 1.7 Scope

This documentation describes the device manufactured by solvimus GmbH, Ilmenau, and stated on the title page.

## 1.8 Abbreviations

| Abbreviation | Meaning |
| --- | --- |
| 2G | Mobile radio standard, synonym for GSM or GPRS |
| 3G | Mobile radio standard, synonym for UMTS |
| 4G | Mobile radio standard, synonym for LTE |
| ACK | Acknowledge |
| AES | Advanced Encryption Standard |
| AFL | Authentication and Fragmentation Layer |
| AI | Analog Input |
| ANSI | American National Standards Institute |
| AO | Analog Output |
| APN | Access Point Name |
| ASCII | American Standard Code for Information Interchange |
| ASHRAE | American Society of Heating, Refrigerating and Air-Conditioning Engineers |
| BACnet | Building Automation and Control networks |
| BBMD | BACnet Broadcast Management Device |
| BCD | Binary-coded decimal numbers |
| BDT | Broadcast Distribution Table |
| BMS | Building Management System |
| CA | Certification Authority |
| CHAP | Challenge Handshake Authentication Protocol |
| CI | Control Information |
| CLI | Command line interface |
| COSEM | COmpanion Specification for Energy Metering |
| CPU | Central processing unit |
| CRC | Cyclic redundancy check |
| CSV | Character-Separated Values |

*Continued on next page*

Table 2 – *Continued from previous page*

| Abbreviation | Meaning |
|---|---|
| CTS | Clear to send |
| D0 | D0 interface (optical interface, IEC 62056-21) |
| DDC | Direct Digital Control |
| DHCP | Dynamic Host Configuration Protocol |
| DI | Digital Input, digital input terminal |
| DIF | Data information field |
| DIFE | Data information field extensions |
| DIN | Deutsches Institut für Normung, German Institute for Standardization |
| DLDE | Direct Local Data Exchange (EN 62056-21, IEC 1107) |
| DLDERS | DLDE communication via RS-232 or RS-485 |
| DLMS | Device Language Message Specification |
| DNS | Domain Name System |
| DO | Digital Output, digital output terminal |
| EEG | German Renewable Energy Sources Act |
| EIA/TIA | Electronic Industries Alliance/Telecommunications Industry Association |
| ELL | Extended Link Layer |
| EMC | Electromagnetic compatibility |
| EN | European norm |
| ESD | Electrostatic Discharge |
| FCB | Frame Count Bit |
| FCV | Frame Count Valid Bit |
| FNN | Forum Netztechnik/Netzbetrieb, subgroup of VDE |
| FSK | Frequency Shift Keying |
| FTP | File Transfer Protocol |
| FTPS | FTP via TLS |
| GB | Gigabyte |
| GMT | Greenwich Mean Time |
| GPRS | General Packet Radio Service |
| GSM | Global System for Mobile Communications |
| HCA | Heat cost allocator |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| I2C | Inter-Integrated Circuit |
| I/O | Input/Output |
| ICCID | Integrated Circuit Card Identifier |
| ICMP | Internet Control Message Protocol |
| ID | Identification, Identifier, unique marking |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| IoT | Internet of Things |
| IP | Internet Protocol or IP address |
| ISO | International Organization for Standardization |
| JSON | JavaScript Object Notation |
| LAN | Local area network |
| LED | Light-Emitting Diode |
| LSB | Least significant byte |
| LSW | Least significant word |
| LTE | Long Term Evolution |
| M2M | Machine-to-Machine |
| M-Bus | Meter-Bus (EN 13757, part 2, 3 and 7) |
| MAC | Medium Access Control or MAC-Adresse |
| MB | Megabyte |
| MCR | Multi Channel Reporting |
| MCS | Modulation and Coding Scheme |
| MDM | Meter Data Management |
| MEI | Modbus Encapsulated Interface |
| MHz | Megahertz |
| MQTT | Message Queuing Telemetry Transport |
| MSB | Most Significant Byte |
| MSW | Most Significant Word |
| MUC | Multi Utility Communication, MUC controller |
| NB-IoT | Narrow Band Internet of Things |
| OBIS | Object Identification System |
| OEM | Original Equipment Manufacturer |
| OMS | Open Metering System |
| PAP | Password Authentication Protocol |
| PEM | Privacy Enhanced Mail |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| PLC | Programmable Logic Controller |
| PLMN | Public Land Mobile Network |

*Continued on next page*

Page 8/81
UG_EN_MBUS-GEV.pdf
Version: 1.1
Released
Frank Richter, 23 February 2024
© solvimus GmbH

Table 2 – *Continued from previous page*

| Abbreviation | Meaning |
|---|---|
| PPP | Point-to-Point Protocol |
| PPPoE | Point-to-Point Protocol over Ethernet |
| PUK | Personal Unblocking Key |
| RAM | Random Access Memory |
| REQ_UD | Request User Data (Class 1 or 2) |
| RFC | Requests For Comments |
| RSP_UD | Respond User Data |
| RSRP | Reference Signal Received Power |
| RSRQ | Reference Signal Received Quality |
| RSSI | Received Signal Strength Indicator |
| RTC | Real-Time Clock |
| RTOS | Real-Time Operating System |
| RTS | Request to send |
| RTU | Remote Terminal Unit |
| S0 | S0 interface (pulse interface, EN 62053-31) |
| SCADA | Supervisory Control and Data Acquisition |
| SCP | Secure Copy |
| SFTP | SSH File Transfer Protocol |
| SIM | Subscriber Identity Module |
| SML | Smart Message Language |
| SMTP | Simple Mail Transfer Protocol |
| SND_NKE | Send Link Reset |
| SND_UD | Send User Data to slave |
| SNTP | Simple Network Time Protocol |
| SPST | Single Pole Single Throw Relay (closing switch) |
| SRD | Short Range Device |
| SSH | Secure Shell |
| SSID | Service Set Identifier |
| SSL | Secure Sockets Layer |
| TCP | Transmission Control Protocol |
| THT | Through-Hole Technology |
| TLS | Transport Layer Security |
| U | Unit width of the housing (1 U = 18 mm) |
| UART | Universal Asynchronous Receiver Transmitter |
| UDP | User Datagram Protocol |
| UL | Unit load for M-Bus |
| UMTS | Universal Mobile Telecommunications System |
| UTC | Universal Time Coordinated |
| VDE | Verband der Elektrotechnik Elektronik Informationstechnik e.V., German Association for Electrical, Electronic & Information Technologies |
| VHF | Very high frequency |
| VIF | Value information field |
| VIFE | Value information field extensions |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WLAN | Wireless Local Area Network |
| wM-Bus | Wireless Meter-Bus (EN 13757, part 3, 4 and 7) |
| XML | eXtensible Markup Language |
| XSLT | eXtensible Stylesheet Language Transformation |

Table 2: Abbreviations

# 2 Introducing the device

## 2.1 General information

The M-Bus (Meter-Bus) is an established and well-known interface for automated meter reading. Especially the ease of installation (simple two-wire system with powering by the bus) and the robustness are important features. These are also special attributes that are of interest for use in industrial environments.

The M-Bus is defined in the standard EN 13757. It establishes an own physics as well as an own protocol. For connecting it to other systems, a translation is necessary.

Oftentimes, the interpretation of the protocol and of the data is done in a PC or another host system with M-Bus software. Thus, the physics of the M-Bus must be connected to available interfaces. This is commonly achieved with level converters for the RS-232 interface. However, the communication via RS-232 is limited to short distances.

Ethernet as a means of communication enables larger distances and is already widely employed. It is thus advantageous to read out data from distributed installations via Ethernet. Hence, any PC with an Ethernet interface can be made a (physical) bus master. With the products MBUS-GE20V and MBUS-GE80V (in the sequel MBUS-GEV for brevity), two gateways are available that transmit M-Bus data via Ethernet in a transparent mode. A driver for a virtual COM port, interfacing to a PC is intuitive and integrates into existing software solutions.

The device supports operating 20 respectively 80 unit loads (UL, mostly equivalent to the number of meters) at the wired M-Bus. The communication is controlled entirely by the software on the PC. The MBUS-GEV merely transmits the data.

The MBUS-GEV comes in a housing 2 U (modules) wide and is intended for top hat rail mounting (DIN rail 35 mm).

The serial number of the devices of the solvimus GmbH can be read from the housing.

## 2.2 Delivery variants and scope of delivery

The MBUS-GEV is offered in a range of variants, and so can easily be adapted to the requirements of the particular property.

| Variant | Order number | M-Bus |
|---|---|---|
| MBUS-GE20V | 500332 | 20 UL |
| MBUS-GE80V | 500333 | 80 UL |

Table 3: Delivery variants

The scope of delivery contains the device and a Quick Start Guide.

## 2.3 Connectors

The various interfaces of the MBUS-GEV are on different sides of the device.

The following figure shows the device.

Page 10/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH

Figure 1: MBUS-GEV

The following connectors are available at the MBUS-GEV:

| Connector | Designation | Pin assignment | Comments |
|---|---|---|---|
| Power supply | 24VDC, GND | 24VDC: positive power supply<br>GND: negative power supply | 24VDC ($\pm$5%), screw terminal, cross section 2.5 mm$^2$ |
| M-Bus connector | MBUS+, MBUS- | MBUS+: positive bus line (2x)<br>MBUS-: negative bus line (2x) | screw terminal, cross section 2.5 mm$^2$, MBUS+ and MBUS- each joined internally |
| Ethernet connector | Ethernet | 1: TX+<br>2: TX-<br>3: RX+<br>4:<br>5:<br>6: RX-<br>7:<br>8: | EIA/TIA 568A/B |

Table 4: Pin assignment

## 2.4 Status LEDs

The MBUS-GEV is equipped with 2 status LEDs. These indicate the following states:

| LED | Colour | Description |
|---|---|---|
| Cover, present in all variants | | |
| Active (ACT) | off<br>orange (blinking)<br>green (flashing) | Inactive, idle state<br>Searching meters (scanning)<br>meter reading |
| State (ST) | off<br>green<br>orange<br>red | Software is not started<br>Main programme is running<br>Initialisation<br>Error |

Table 5: Status LEDs (all variants)

In the operating state, the *State-LED* is green and the *Active-LED* flashes green briefly during the readout.

## 2.5 First steps

### 2.5.1 Power supply

The MBUS-GEV requires an external power supply 24 VDC. The MBUS-GEV starts automatically after connection to the supply voltage.

By default, the following calls are made on system startup:

- Configuration of the network interface (Ethernet) via DHCP or static configuration
- One-time generation of SSL device keys (needs some time)

- Obtaining the system time via SNTP
- Start of system services
- Start of the main programme

The main programme then provides the entire functionality, including the web-based front end of the MBUS-GEV.

The following figure shows a typical usage of a MBUS-GEV:
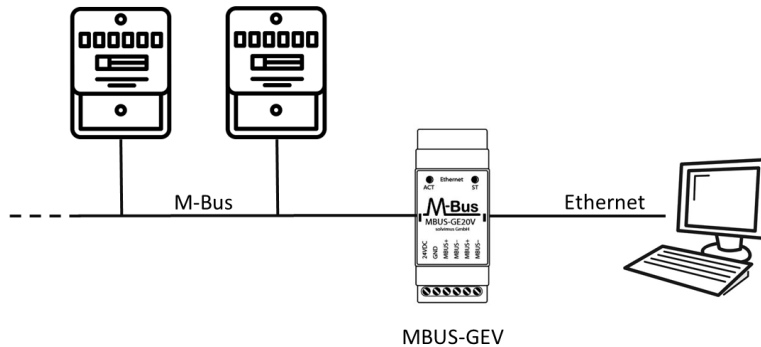


Figure 2: Typical usage of the MBUS-GEV, exemplified here with a PC

Further steps are not required for commissioning the device. All other settings must be performed on the logical master, e.g. a PC.

The MBUS-GEV is fully transparent to the data communication on the M-Bus. This means that the device is not visible as an M-Bus slave and baud rate changes of the M-Bus master do not need any user interaction.

### 2.5.2 Network configuration and first steps

The MBUS-GEV can be completely configured via the network interface. Therefore, it has to be configured according to your network. If necessary, ask your administrator.

✔ The MBUS-GEV is set by default to the static IP address 192.168.1.101 (subnet mask: 255.255.255.0, gateway: 192.168.1.254).

For intuitive operation, a configuration website is available on the device, which can be accessed via the IP address of the MBUS-GEV called in a web browser.

➡ Website on the MBUS-GEV, e.g.: http://192.168.1.101/

ℹ When handling multiple devices under same IP (e.g. commissioning) or with different software versions (e.g. update), you should always clear the cache of the browser (e.g. ⟨**CTRL+F5**⟩) to prevent an inconsistent display of the website.

The following page opens in the browser:

Page 12/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH
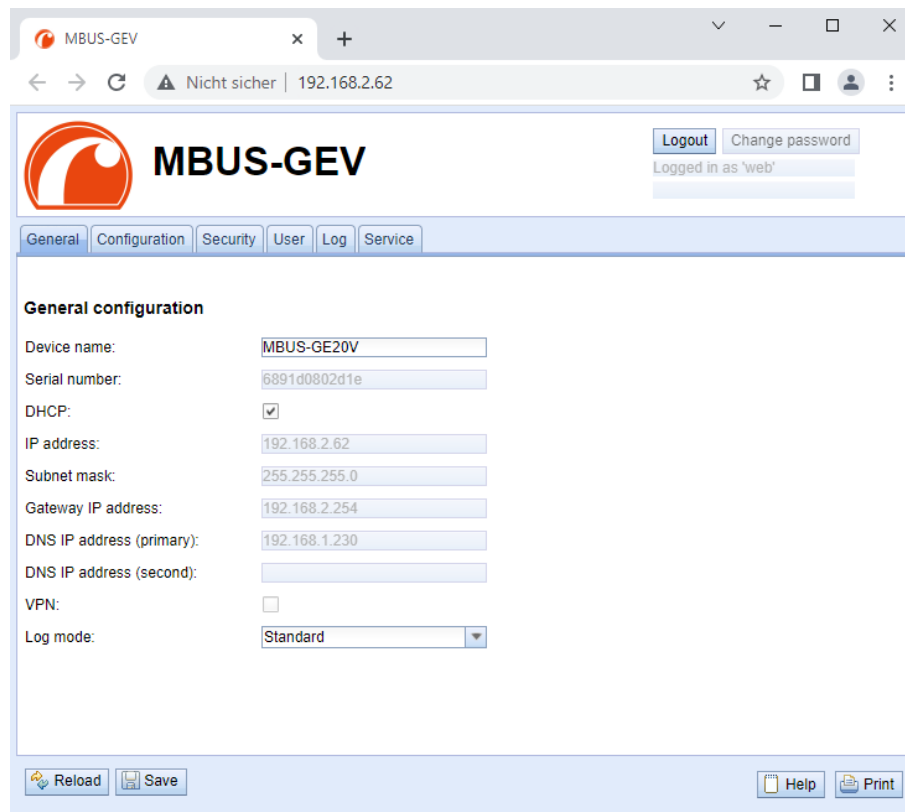
Figure 3: Website of the MBUS-GEV

The web-based front end is described separately in Chapter 4. There you will find a detailed overview of the functionalities of the web-based front end.

In addition, access via SFTP, SCP, FTPS (file transfer) or via SSH (console) is also possible by default (see Chapter 3):



Figure 4: WinSCP main window after establishing the connection

## 2.6 Specific troubleshooting

In case the MBUS-GEV does not work as described in this document, it is useful to locate the malfunction in order to resolve the issue and to recover the full functionality again.

### 2.6.1 All LEDs remain off, the device does not respond.

⚠ Only trained and appropriately qualified personnel are allowed to check the electric power supply (see Section 1.2.3).

Switch off the power supply and remove the device. Remove all cables and antennas. Test the MBUS-GEV under laboratory conditions, that means at an isolated and separate measurement installation. Switch on the power supply at that measurement installation. It must adhere to the requirements given in Section 2.7.2.

If the problem persists, ensure that there are no faults in the power supply caused by the infrastructure, circuit breakers or residual current devices.

If errors could not be eliminated, please contact our customer support:
E-Mail: support@solvimus.de
Phone: +49 3677 7613065

### 2.6.2 Cyclic flashing of COL, TX, RX of a 3 U wide variant.
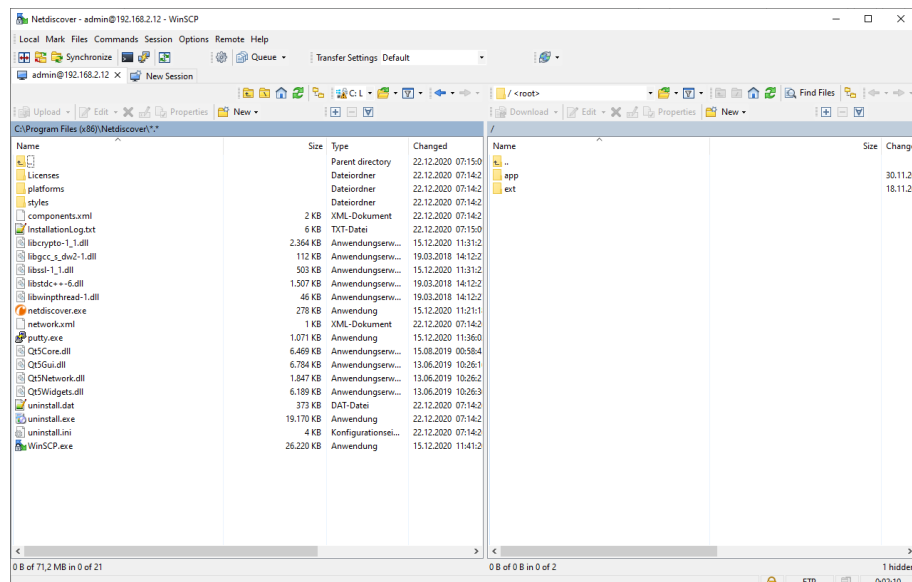
⚠ Only trained and appropriately qualified personnel are allowed to check the electric power supply (see Section 1.2.3).

Switch off the power supply. Remove all cables except the power supply. Now switch on the power supply and check whether the LEDs are now not flashing together cyclically any more.

Connect all cables one after the other and check after each step if the LEDs restart to flash cyclically.

If the error occurs when connecting a specific cable, proceed to check this one more thoroughly. The error may reside in the external wiring, e.g. a short circuit or overload. Replace the faulty cable if necessary. Check the external power supply.

If errors could not be eliminated, please contact our customer support:
E-Mail: support@solvimus.de
Phone: +49 3677 7613065

## 2.7 Technical data

### 2.7.1 General specifications

**Dimensions/Mass**

The devices have the following dimensions and the following mass:

- Width: 35 mm
- Height: 90 mm
- Depth: 59 mm
- Mass: approx. 85 g

**Mounting**

The device is intended for mounting in a control cabinet or a distribution board:

- Temperature range for operation: 0..50 °C (daily average)
- Temperature range for transport and storage: -20..70 °C (short-time)
- Air humidity: 0..95 % relH, non-condensing
- Degree of protection: IP20 (IEC 60529)
- Top hat rail mounting (DIN rail 35 mm, IEC 60715)

Page 14/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH

### 2.7.2 Electrical specifications

**Power supply**

The device is powered by an external power supply (pin assignment see Section 2.3):

- Voltage: 21.6..24.5 VDC, screw terminals ($\leq$2.5 mm$^2$, tightening torque 0.5 Nm)
- Power consumption: 2 W (idle state), max. 10 W
- Safety: reverse polarity protected M-Bus, overvoltage protection (transients), protection class III (IEC 61140), electronic resettable fuse
- Peak inrush-current: approx. 3 A

**Meter interfaces**

The devices have an M-Bus meter interface (pin assignment see Section 2.3):

- Compliant to EN 13757-2, Umark=36 V, Uspace=24 V, screw terminals ($\leq$2.5 mm$^2$, tightening torque 0.5 Nm)
- max. 20 unit loads (UL) for MBUS-GE20V, max. 80 unit loads (UL) for MBUS-GE80V
- max. Baud rate: 19200 bps

**Communication interfaces**

The device has an Ethernet communication interface (pin assignment see Section 2.3):

- Ethernet: compliant to IEEE 802.3, 10/100-Base-TX, RJ45 connector incl. status LEDs, Auto-MDIX

### 2.7.3 Further specifications

**Galvanic isolation**

The Ethernet communication interface is separated from the meter interface:

- Galvanic isolation: 1000 V

**Processing unit**

The central unit is a microprocessor system:

- CPU: ARM9 architecture, 454 MHz clock frequency
- Memory: 128 MB RAM, 4 GB internal eMMC Flash
- Operating system: Linux
- Integrated RTC: backed-up for up to 7 days
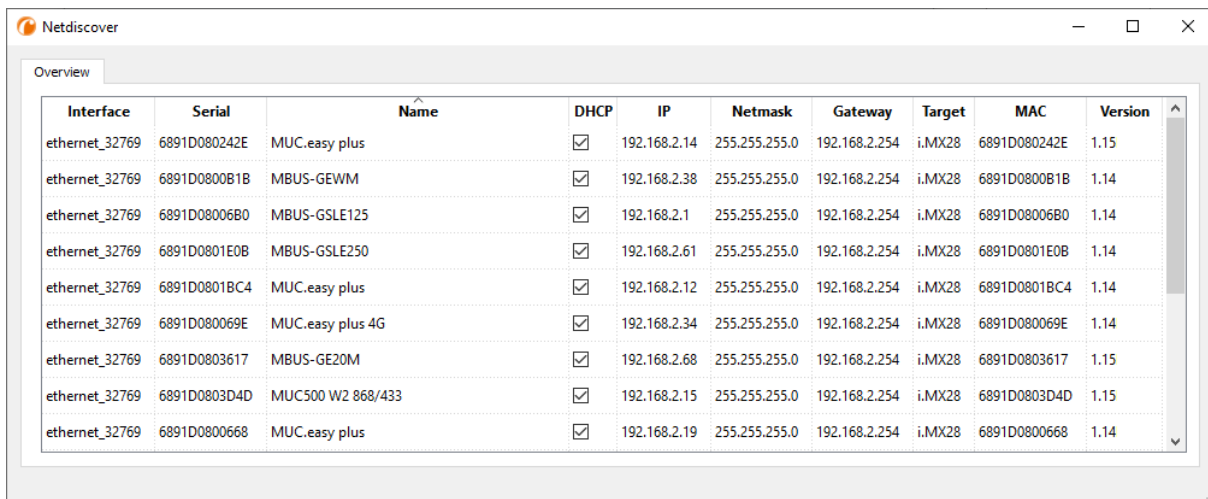
# 3 Tool Netdiscover

## 3.1 General information

The solvimus GmbH provides its customers with the tool Netdiscover for easier management of products in the customer network. This tool, available for Windows and Linux, allows you to find devices of solvimus GmbH in the local network and to manage them.

ℹ️ Depending on the product and thus on the hardware resp. the software installed on your device, not all the functions and parameters referred to in the text, in tables and figures are available. The screenshots are intended to show examples. A gateway for instance does not have a report interface for data push or a cellular modem.

The installation comes with two additional programmes. The applications *Putty* and *WinSCP* are utilities for SSH and (S)FTP access. The integration into the tool Netdiscover enables the easy access to the devices from a central location.

## 3.2 Discovering and accessing devices

After the tool is started, it uses UDP broadcast via UDP port 8001 to discover all devices from solvimus GmbH accessible in the local network and displays them in the main window.



| Interface | Serial | Name | DHCP | IP | Netmask | Gateway | Target | MAC | Version |
|---|---|---|---|---|---|---|---|---|---|
| ethernet_32769 | 6891D080242E | MUC.easy plus | ☑ | 192.168.2.14 | 255.255.255.0 | 192.168.2.254 | i.MX28 | 6891D080242E | 1.15 |
| ethernet_32769 | 6891D0800B1B | MBUS-GEWM | ☑ | 192.168.2.38 | 255.255.255.0 | 192.168.2.254 | i.MX28 | 6891D0800B1B | 1.14 |
| ethernet_32769 | 6891D08006B0 | MBUS-GSLE125 | ☑ | 192.168.2.1 | 255.255.255.0 | 192.168.2.254 | i.MX28 | 6891D08006B0 | 1.14 |
| ethernet_32769 | 6891D0801E0B | MBUS-GSLE250 | ☑ | 192.168.2.61 | 255.255.255.0 | 192.168.2.254 | i.MX28 | 6891D0801E0B | 1.14 |
| ethernet_32769 | 6891D0801BC4 | MUC.easy plus | ☑ | 192.168.2.12 | 255.255.255.0 | 192.168.2.254 | i.MX28 | 6891D0801BC4 | 1.14 |
| ethernet_32769 | 6891D080069E | MUC.easy plus 4G | ☑ | 192.168.2.34 | 255.255.255.0 | 192.168.2.254 | i.MX28 | 6891D080069E | 1.14 |
| ethernet_32769 | 6891D0803617 | MBUS-GE20M | ☑ | 192.168.2.68 | 255.255.255.0 | 192.168.2.254 | i.MX28 | 6891D0803617 | 1.15 |
| ethernet_32769 | 6891D0803D4D | MUC500 W2 868/433 | ☑ | 192.168.2.15 | 255.255.255.0 | 192.168.2.254 | i.MX28 | 6891D0803D4D | 1.15 |
| ethernet_32769 | 6891D0800668 | MUC.easy plus | ☑ | 192.168.2.19 | 255.255.255.0 | 192.168.2.254 | i.MX28 | 6891D0800668 | 1.14 |

Figure 5: Main window of the tool Netdiscover

✔️ The UDP broadcast finds all devices in the local network, regardless of IP settings and subnet masks. Therefore, this function is initially recommended.

ℹ️ The UDP broadcast is usually not forwarded by routers. Therefore, this tool will only find all devices in the local network, in front of the router.

In addition to the MAC address of the devices and their network configuration, the names of the devices and also the version of the operating system are shown. Thus, all devices to be managed can be clearly identified and matched.

✔️ The name of the devices corresponds to the **Device name** in *General* tab (see Section 4.3).

Various functions can be called using the context menu that appears by right-clicking on one of the devices:

- **Ping**: starts the ping via ICMP to the device in a separate tab. So, testing of connectivity via TCP is possible.
- **Web**: opens the default browser with the IP of the device. The web-based front end should open (see Chapter 4).

Page 16/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH

- **FTP**: starts *WinSCP* with the IP of the device or blank. The login data or also the IP must be entered before connecting to the FTP/SFTP server of the device.
- **FTP (default)**: starts *WinSCP* with the IP of the device and connects via FTPS with default login information of the user *admin*.
- **SSH**: startet *Putty* with the IP of the device. The login data must be entered to connect to the SSH console.
- **Deploy**: starts the mass deployment for devices in a separate tab.
- **Import device list**: imports a device list into the main window.
- **Net configuration**: starts a separate tab for changing the network configuration of the device via UDP broadcast.
- **Version**: information about the version of the tool Netdiscover (displayed only if no device is selected).
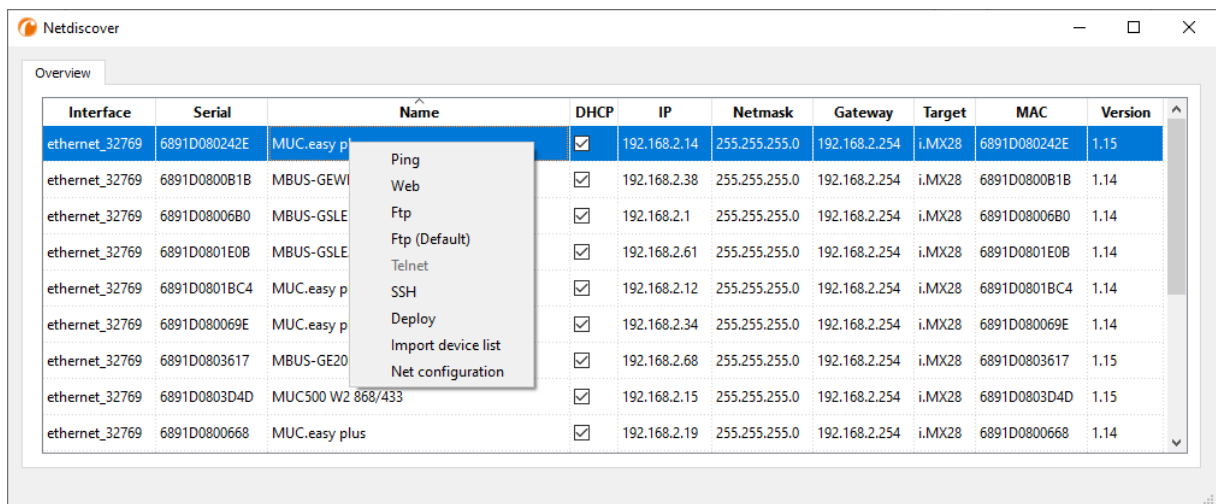


Figure 6: Context menu in the tool Netdiscover

- Depending on the network settings of your PC or your general network infrastructure, the UDP port 8001 may be blocked. Then calls of the tool are blocked and the main window remains empty.
- If a firewall is used in your network (also directly on the PC), there has to be an appropriate firewall rule. This rule should unblock this port to be able to list the devices.
- Ask your administrator about the firewall and network configuration.
- If access via UDP broadcast is denied, a list can be imported with the **Import device list** function in order to still be able to use all other functions via TCP.

Some important functions are described more in detail in the following subsections.

## 3.3 Network configuration

It is often necessary to adjust the network settings of the devices for further work, especially when commissioning devices.

The command **Net configuration** from the context menu in the tool Netdiscover opens another tab for the network configuration. Thus, IP address, subnet mask or gateway address can be changed to static or DHCP can be activated for obtaining these settings automatically from a DHCP server.

Frank Richter, 23 February 2024
© solvimus GmbH

Version: 1.1
Released

Page 17/81
UG_EN_MBUS-GEV.pdf

Figure 7: Network configuration via the tool Netdiscover

Modified configurations can be committed pressing the button **Send**. Modifications are only accepted with the password of the user *admin*, the admin password must be inserted in the field **Password**.

If automatic network configuration (DHCP) is selected, all parameters (**IP address**, **Subnet mask** and **Gateway IP address**) will be read from a DHCP server. The respective fields are deactivated then.
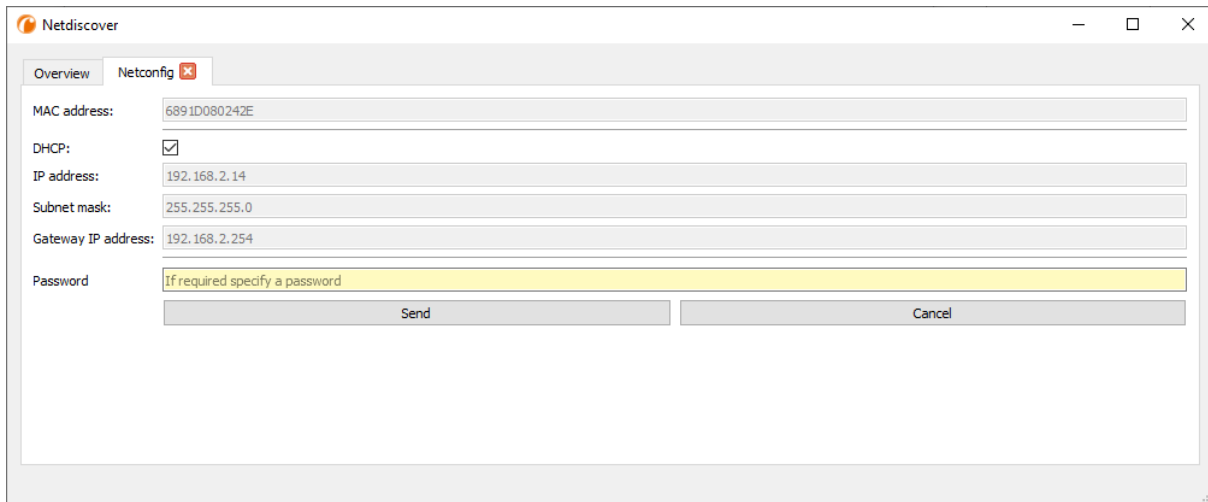
The assigned IP address can be identified at the DHCP server from the unique MAC address of the MBUS-GEV. This address is displayed in the field **MAC address** in the main window of the tool Netdiscover as well as in the tab **General** (see Section 4.3) in the field **Serial number**.

Is the automatic configuration not possible in your network (no DHCP server available), the device will pick a standard address (169.254.xxx.xxx) according to RFC3927.

ⓘ The standard password in the default factory setting is described in the tab **User** (see Section 4.10).

ⓘ Changing the network parameters of the device can affect the accessibility. If the network parameters have already been set correctly by an administrator, they should not be changed.

## 3.4 Access to the web-based front end via HTTP

A web server is integrated on the devices from solvimus GmbH. This enables the configuration of the devices via an integrated, web-based front end (see Chapter 4).

Use the command **Web** from the context menu in the tool Netdiscover to quickly and easily call it in the default browser.

➡ If the web-based front end does not open, please follow the instructions in Section 4.14.

## 3.5 Access to the file system via FTP

The devices from solvimus GmbH can be accessed via FTP to work directly on the file system level. This enables updates, special configurations and extended functionality (see Chapter 6). The integrated FTP server of the devices supports both FTP and SFTP.

✔ If access via FTP or SFTP is not possible, check especially the IP settings and the opened ports, 21 for FTP and 22 for SFTP.

➡ In case of access issues, ask your administrator.

The commands **FTP** and **FTP (default)** from the context menu in the tool Netdiscover start the *WinSCP* programme and use the IP address of the selected device. Calling the command with a selected device, *WinSCP* always accesses the device via FTP. To use an SFTP connection, the context menu must be called without selecting a device before. Then, only the command **FTP** is available, opening a not pre-configured

Page 18/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH

*WinSCP* window. So, there is the choice between FTP, SFTP or SCP.

The mode **FTP (default)** tries to log in with the default login information of the user *admin*, while in the mode **FTP** any access data can be entered.
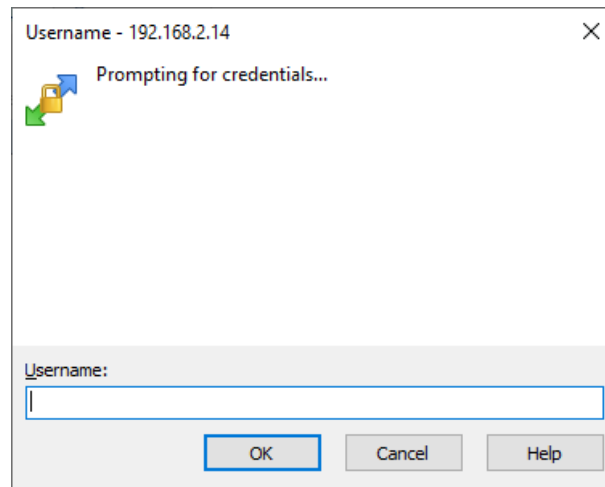


Figure 8: Entering user name when logging in via SFTP

✔ If the login information of the user *admin* is modified, the command **FTP (default)** can not be used.

*WinSCP* now establishes an SFTP or unsecure/secured FTP connection. When a connection is established to a specific device with SFTP, its authenticity is checked using stored certificates. Normally, the devices from solvimus GmbH are coming with an individual, self-signed certificate upon delivery. This certificate is usually classified as untrusted by your PC. Therefore, a security prompt with information about the device's certificate is displayed. The user must verify the validity of the certificate and then approve it to establish a secure connection. The confirmed certificate is stored in the PC for future connections.
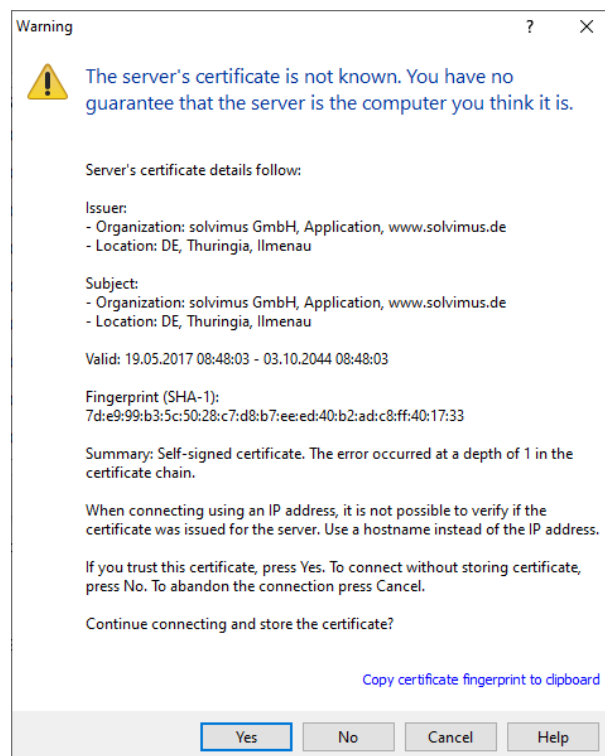


Figure 9: Security prompt for the certificate of the device

*WinSCP* offers a dual-pane file manager after logging in successfully. This allows files to be uploaded to or downloaded from the device. File commands can be executed via a context menu, e. g. copying, renaming or editing. Drag&Drop for uploading and downloading is also supported.
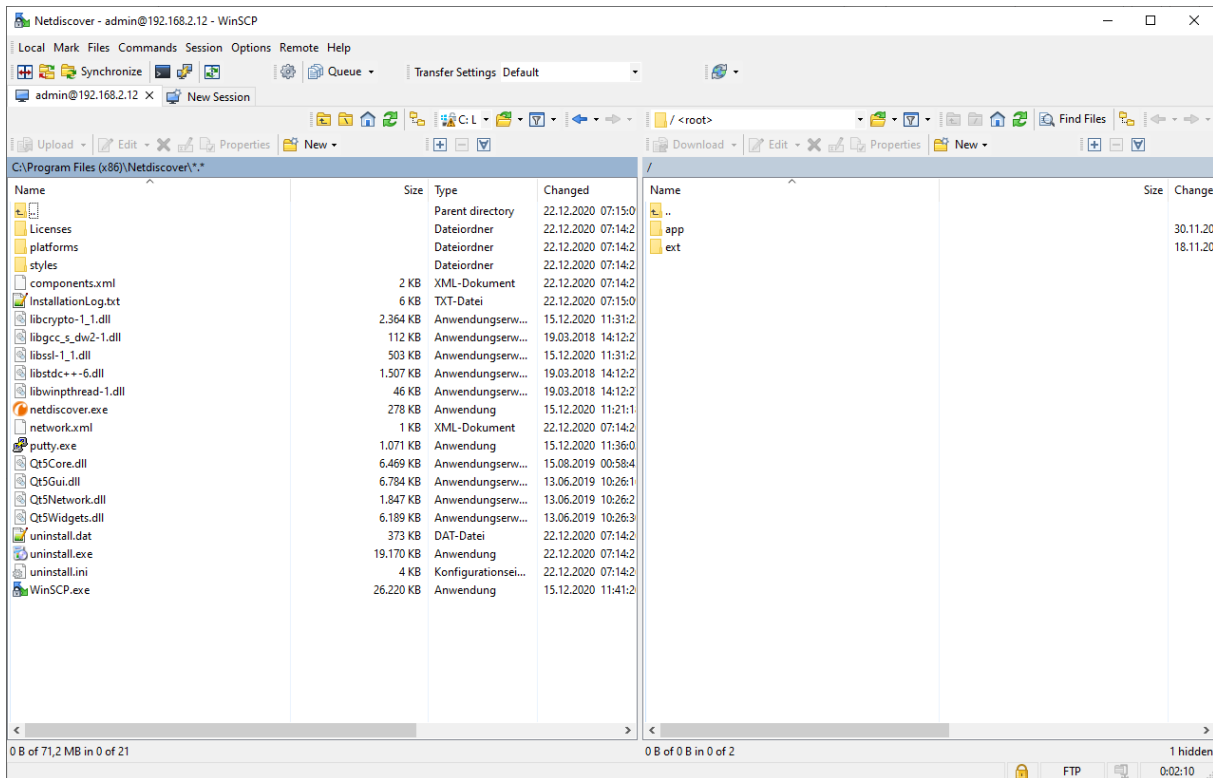
Figure 10: File manager view in *WinSCP*

🛈 Changing files or the file system can affect the functionality of the system.

➡ The default login information, as delivered, is contained in Section 4.10.

## 3.6 Access to the command line via SSH

Access to the command line interface (CLI) of the device is suitable for maintenance purposes.

The command **SSH** from the context menu in the tool Netdiscover opens the integrated *Putty* client and establishes a connection to the device

When a connection is established to a specific device with SSH, its authenticity is checked using stored certificates. Normally, the devices from solvimus GmbH are coming with an individual, self-signed certificate upon delivery. This certificate is usually classified as untrusted by your PC. Therefore, a security prompt with information about the device's certificate is displayed. The user must verify the validity of the certificate and then approve it to establish a secure connection. The confirmed certificate is stored in the PC for future connections.

Page 20/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH
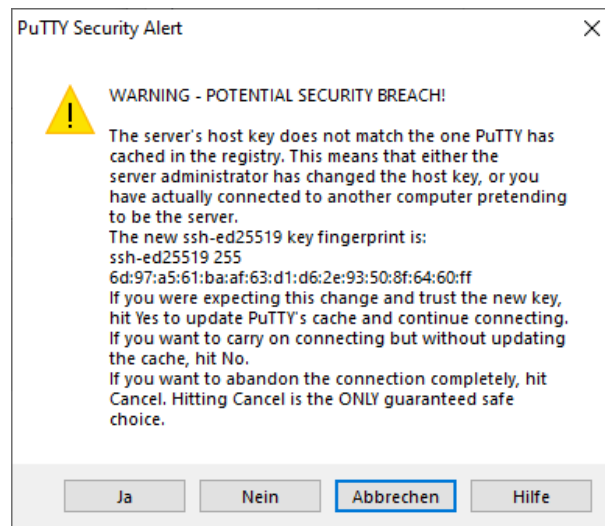
Figure 11: Security prompt for the certificate of the device

Now the *Putty* client opens and the login information for the user *admin* has to be entered. Then, the command line is ready for input via SSH. The password is not displayed on the screen.
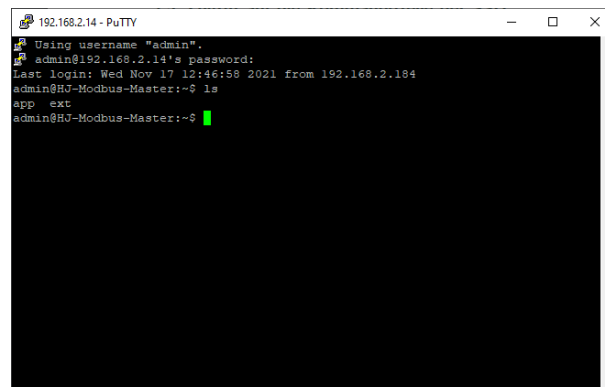

Figure 12: Command line in the *Putty* client

ⓘ Inputs on the command line can affect the functionality of the system.

➡ The default login information, as delivered, is contained in Section 4.10.

## 3.7 Mass deployment

This function allows performing certain device configurations or firmware updates in parallel for all devices displayed in Netdiscover. For example, is is possible to import an previosly exported device configuration to multiple other devices at the same time. Another example would be importing certificate files needed on multiple devices to export meter data. A third and final example would be updating the application software on multiple devices in parallel.

ⓘ The configuration or update should explicitly only be deployed on similar devices.

In this case mark the devices in the tool Netdiscover on which you want to perform a configuration or firmware update in parallel.
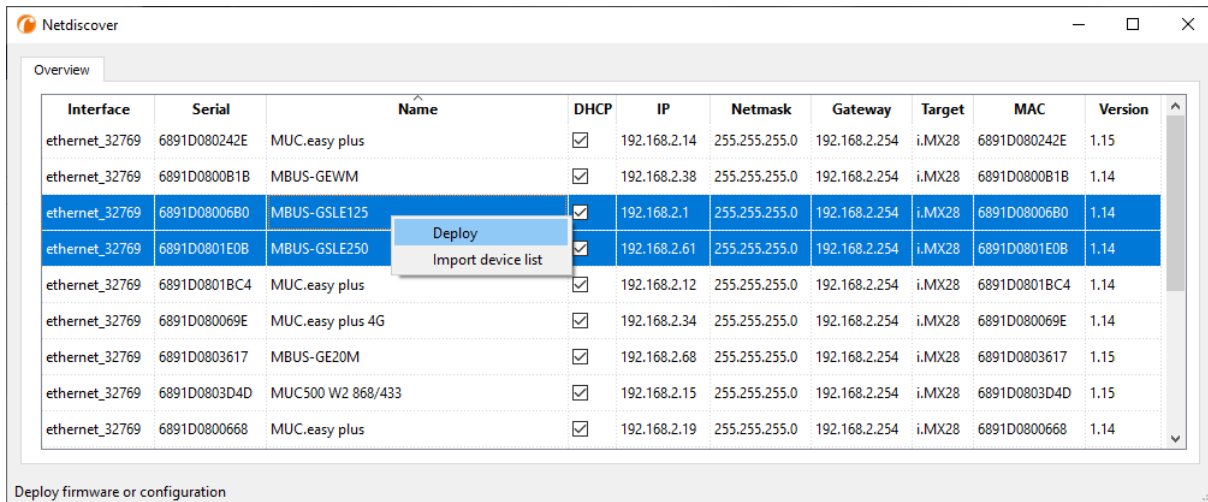
Figure 13: Selection of devices and initiation of the mass deployment

The command **Deploy** from the context menu in the tool Netdiscover opens another tab for mass deployment.
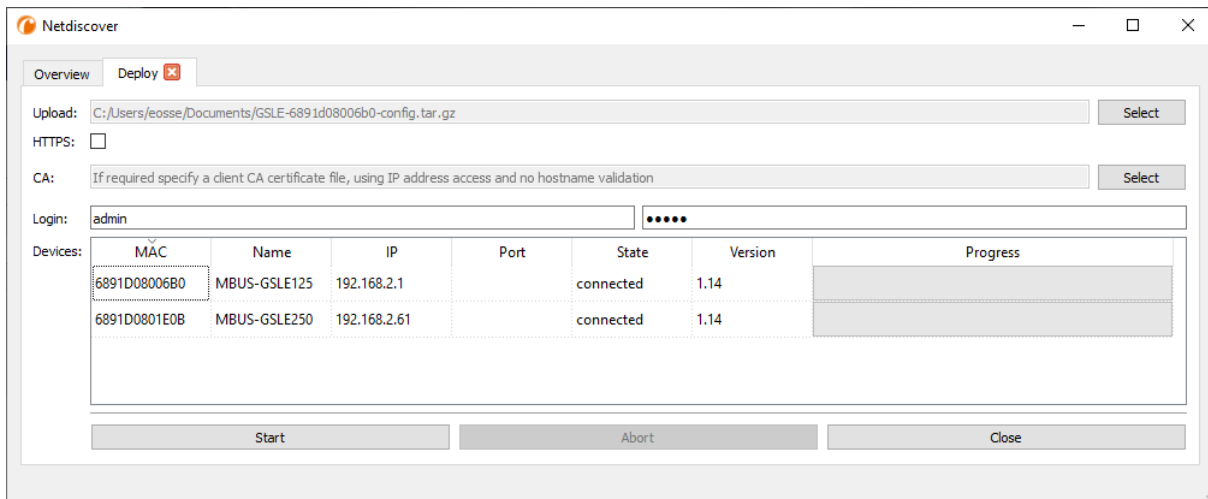


Figure 14: Mass deployment via the tool Netdiscover

The following input fields and buttons are available here:

- **Upload**: the configuration or update to be uploaded.
- **HTTPS**: selection field whether HTTP or HTTPS should be used.
- **CA**: the CA certificate to verify the client certificate of the devices for HTTPS-based work.
- **Login**: user name and password for the user *admin*.
- **Start**: starts the process.
- **Abort**: aborts the process.
- **Close**: closes the mass deployment tab.

In the central part, there is a list view with information about the devices and the status/progress of the process.

ⓘ Exclusively *. tar. gz archives are intended for the import of a device configuration or a certificate file.

ⓘ The generation of a *. tar. gz file with the device configuration is described in Section 4.12.

ⓘ Exclusively *. enc files are intended for the update of the firmware.

ⓘ An update of the firmware is also possible via the web site as described in Section 4.12.

The file is unpacked on the device after the upload, and processed. The device is then restarted.

Page 22/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH

## 3.8 Import of a device list

Devices cannot always be discovered automatically. Firewalls, routing settings or even the deactivation of the function **Network discovery active** in the *Security* tab (see Section 4.9) are possible reasons.

Therefore, a device list can be imported. This enables managing devices via the tool Netdiscover even without automatic dicovery.
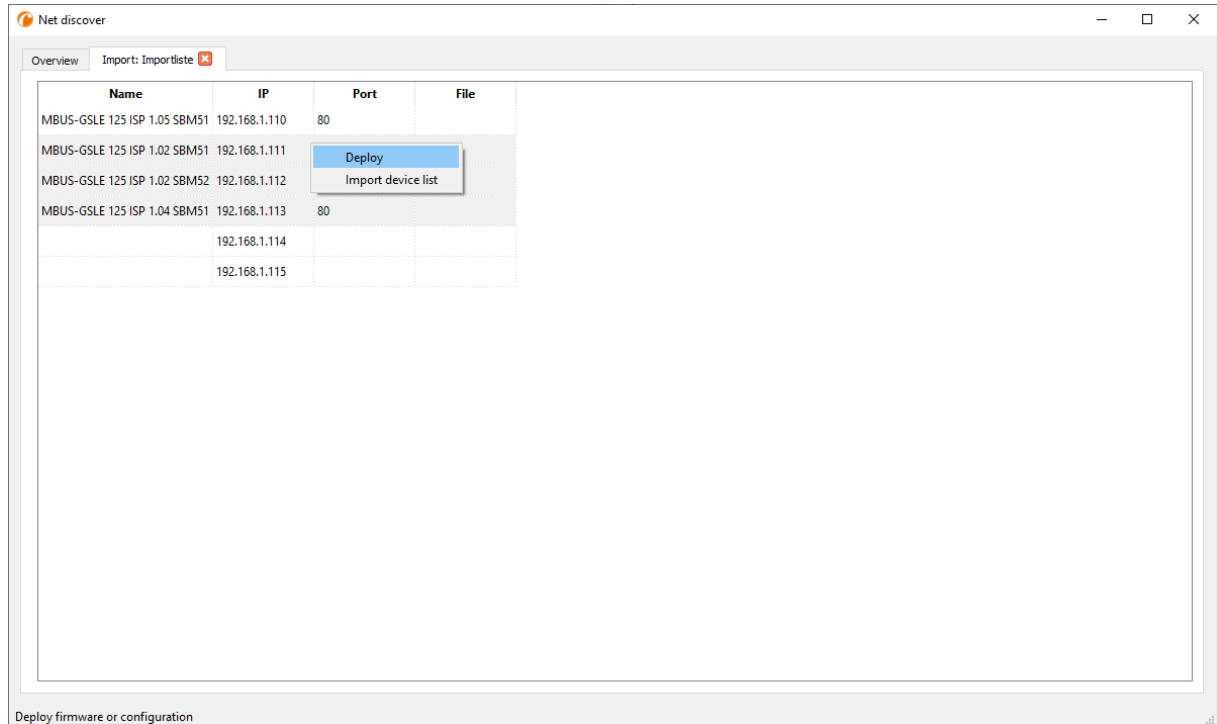


Figure 15: Viewing and using an imported list in the tool Netdiscover tool

First, a suitable CSV file has to be created before the actual import. In the CSV file, a comma or a semicolon can be used as a separator. The device data is entered here according to the following example to obtain the above list in the tool Netdiscover:

```
Port;Name;Password;Username;IP;File
80;MBUS-GSLE 125 ISP 1.05 SBM51;admin;admin;192.168.1.110;
80;MBUS-GSLE 125 ISP 1.02 SBM51;admin;admin;192.168.1.111;
80;MBUS-GSLE 125 ISP 1.02 SBM52;admin;admin;192.168.1.112;
80;MBUS-GSLE 125 ISP 1.04 SBM51;admin;admin;192.168.1.113;
;;admin;;192.168.1.114;
;;;;;192.168.1.115;
```

> ℹ️ The header of the CSV file has to be identical to the one above.

> ➡️ Only the *IP* column is mandatory. The other columns can be left empty and are set to default for special functions (*Port*: 80, *Password*: admin, *Username*: admin).

## 3.9 Troubleshooting network

### 3.9.1 No network connection

If no network connection to the device can be established, make a Ping connectivity test first (see Section 3.2).

If a Ping response is not detected, test the device via a direct network connection with a PC, provided the device is connected via a bigger network. Depending on the functions, a cross-over cable may need to be employed in case of a direct connection between PC and device.

Check the physical network connection between the device and the PC, if the cable is correctly joined and inserted.

✔ The network connection must be inserted in the connector for Ethernet.

At the network connection the *hyperlink-LED* must be lit yellow and the *Active-LED* must flash green from time to time. Check also the corresponding LEDs at the remote station (PC, hub etc.). If need be, repeat the connectivity test with switched cables.

If all LEDs are lit correctly, check if the device is detected in the tool Netdiscover (see Section 3.2). A prerequisite is that the device is connected to the PC via a local area network.

If the device being searched is not contained in the list (allocation via serial number), ensure that the communication is not prevented by a firewall.

If the device is in the list, configure it with a unique IP address available in the local network (see Section 3.3). Ask your administrator about this.

For a direct connection between PC and network, the following example configuration can be employed, provided no other participant is connected to the network with these addresses:

| PC | |
|---|---|
| IP | 192.168.1.10 |
| Network mask | 255.255.255.0 |
| **Device** | |
| IP | 192.168.1.101 |
| Network mask | 255.255.255.0 |

Table 6: Example IP addresses

If errors could not be eliminated, please contact our customer support:
E-Mail: support@solvimus.de
Phone: +49 3677 7613065

## 3.9.2 The device can not be accessed via website respectively FTP(S)

If the device can not be accessed via a browser, make a Ping connectivity test first (see Section 3.2) or log on tentatively via FTPS (see Section 3.5). If a network communication with the device is not possible in general, follow the instructions in section Section 3.9.1. If a single service is not available, check the passwords and the firewall configuration at the PC respectively in the network.

Is the web page displayed whereas a login is not possible, check if you can log on with the *admin* account. Clear the cache in the browser and reload the website (e. g. key ⟨**F5**⟩ respectively ⟨**CTRL+F5**⟩).

If errors could not be eliminated, please contact our customer support:
E-Mail: support@solvimus.de
Phone: +49 3677 7613065

Page 24/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH

# 4  Web-based front end

## 4.1  General information

Many products from solvimus GmbH, especially data concentrators and gateways for smart metering, are coming with an integrated web server and provide a website for the configuration. The devices can be configured easily and in a user-friendly manner via this website. Device parameters, meter configuration as well as services can be displayed or changed on this website.

This chapter gives an overview on how to use the web-based front end.

> ⓘ Depending on the product and thus on the hardware resp. the software installed on your device, not all the functions and parameters referred to in the text, in tables and figures are available. The screenshots are intended to show examples. A gateway for instance does not have a report interface for data push or a cellular modem.

The web-based front end can easily be opened in the browser by entering the device's IP address. Alternatively, right-click on the device in our tool Netdiscover (see Chapter 3) and select the command **Web** in the context menu to launch the browser.

> ➜ We are testing the web-based front end in different browsers. We recommend using Chrome™ and Firefox browsers for optimal user experience. For the legally secure and data protection compliant setting of your browser, please ask your administrator.

The browser automatically tries to log in the user to the website using the default login information. The user „web" with the password „web" is used for this purpose. This user has initially full access to the website. This facilitates the initial commissioning.

When the default user „web" has been modified in the configuration via the **User** tab, for example by changing the password, the automatic login is not possible anymore. Only entering the new, correct login information will allow accessing the front end. A login dialogue will then always appear:
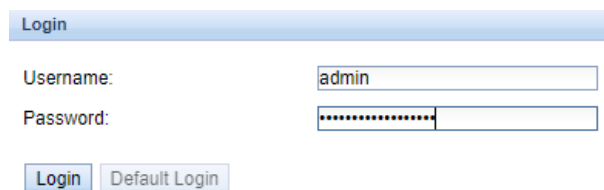


Figure 16: Login dialogue

> ⓘ For switching to another user (e. g. from the default user), the **Logout** button at the top right of the web-based front end can be clicked.
> ⓘ The default login information, as delivered, is contained in Section 4.10.

If the logged-in user has write access, the user has to log out after the configuration is finished. If the connection remains active, no other write access to the web-based front end is available. Only one session with write access is possible at a time.

> ✔ When a session is terminated without logging out previously, e. g. by closing the browser window, it remains active for approx. 1 min. Afterwards it is automatically closed and write access is possible again.

On the website of the device (see Figure 17), the functions are grouped into different tabs. So, the clarity can be maintained despite the large number of parameters. All modifications in one of the tabs must be saved before changing tabs, otherwise the modifications will be lost. The functions and parameters of the individual tabs are described below.

The **Print** button (see Figure 17, bottom right) can be used for getting an entire overview of the configuration or for exporting it via the clipboard. Details are given in Section 4.13.

The solvimus GmbH provides a manual in PDF format directly on the device. Click the **Help** button (see Figure 17, bottom right) to open the included PDF file.

## 4.2 Access via HTTPS

Normally, the web-based front end is accessible via HTTP (port 80) as well as via HTTPS (port 443). Depending on the requirements, one of the services can be deactivated (see Section 4.12).

Compared to HTTP, HTTPS offers both encryption and authentication methods and thus enables secure access to the devices in insecure networks.

The devices from solvimus GmbH are delivered with certificates and keys for preparing HTTPS access:

- `app/keys/http_host_cert`: self-generated certificate of the device to verify the identity of the device, server-side authentication
- `app/keys/http_host_key`: private key of the device

The user can upload another certificate to the device to fully secure the communication and for mutual authentication.

- `app/keys/http_host_ca`: root certificate to check the client certificate of the browser and thus the identity of the client, client-side authentication

Based on these files, the communication partners can securely identify and authenticate each other before a symmetric session key is negotiated.

- Access to the web-based front end via HTTPS can be blocked by installing incorrect or invalid certificates.
- Deactivating HTTPS or HTTP is only available via the respectively other access variant.
- Optionally, customer-specific certificates can be uploaded during production.

## 4.3 Tab General

The **General** tab displays general properties of the device and its network configuration.

Page 26/81
UG_EN_MBUS-GEV.pdf
Version: 1.1
Released
Frank Richter, 23 February 2024
© solvimus GmbH

Figure 17: Tab General

The following parameters are shown and can be changed here:

| Column name | Description |
|---|---|
| Device name | Name of the device (as assigned in the tool Netdiscover, max. 50 characters) |
| Serial number | Serial number of the device (MAC address), not editable |
| DHCP | Enable automatic network configuration. If no DHCP-server is available for the network configuration, the tick is set to inactive and the network interface can be configured using a free IP in the address space 169.254.0.0/16 (Zeroconf). |
| IP address | IP address of the device, not configurable when using DHCP |
| Subnet mask | Subnet mask of the device, not configurable when using DHCP |
| Gateway IP address | IP address of the standard gateway, not configurable when using DHCP |
| DNS IP address (primary) | IP address of the primary DNS server, not configurable when using DHCP |
| DNS IP address (secondary) | IP address of the secondary DNS server, not configurable when using DHCP |
| VPN | Activates the OpenVPN client functionality |
| Free space log (kB) | Free disk space for logging, not editable |
| Free space Flash (kB) | Free disk space for applications, not editable |
| System date (local) | Current, localized system date |
| System time (local) | Current, localized system time |
| SNTP Server | Address of the time server |
| Log mode | Level of detail of the log entries of the application<br><br>• *None*: The application does not generate any log entries.<br>• *Standard*: The application generates log entries for errors and warnings.<br>• *All*: The application generates log entries for all events. |

Table 7: Fields in the General tab

The **Save** button is used to save the configuration. The **Reload** command loads the last saved parameters and resets current changes.

If the network configuration is changed, the device will be available under the new IP right after processing the changes. All active sessions will be closed and users will be logged out automatically then.

&#9432; Changing the network parameters of the device can affect the accessibility. If the network parameters have already been set correctly by an administrator, they should not be changed.

&#9432; The device is automatically reinitialized by accepting the parameters via the **Save** button.

ⓘ Date and time are always processed as UTC time (without time zone shift). When shown on the website, the browser converts it according to the time zone of the respective computer. In Central Europe, for example, this is Central European Time or Central European Summer Time. If a different time zone is used here, the time shown on the website will be displayed accordingly.

➡ The use of OpenVPN is described in the Section 6.5.

## 4.4 Tab Meter

The **Meter** tab displays an overview of the connected meters. It offers further possibilities to the user: searching meters automatically, adding meters manually and configuring meters that are already present. The meter list can additionally be exported through it.



Figure 18: Tab Meter

The meter list is displayed in tabular format. Meter entries and the corresponding meter value entries are displayed one below the other. The individual columns have the following meaning:

| Column name | Description |
|---|---|
| Interface | Interface to the meter<br>• *M-Bus*: wired M-Bus according to EN 13757-2/-3/-7 and OMS<br>• *wM-Bus*: wireless M-Bus according to EN 13757-4/-3/-7 and OMS<br>• *DLDE*: wired serial interface according to IEC 62056-21 or IEC 1107/61107<br>• *Modbus*: interface via RS-485 (Modbus RTU) or Ethernet (Modbus TCP, according to IEC 61158)<br>• *S0*: wired counting/pulse input interface according to IEC 62053-31 or for simple contact outputs<br>• *System*: Monitoring of internally measured values from the device |
| S (Status) | Shows the status of the meter or the meter value<br>• *!*: meter or meter values cannot be read, meter values are not up-to-date.<br>• *E*: meter/meter value edited<br>• *A*: meter/meter value added<br>• *\**: Meter value list of that meter is limited (see *Maximum value count* parameter in **Configuration** tab) |
| Serial | Serial number of the meter (meter number, secondary ID) |
| MAN | Manufacturer of the meter (abbreviation), DLMS Flag-ID |
| Medium | Meter medium, see second column in Table 21 |
| Version | Version number of the meter |
| Link | Primary address of a meter (M-Bus) or received signal strength indicator (RSSI) in case of wM-Bus |
| Value | Meter reading or measured value (unscaled) |

*Continued on next page*

Page 28/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH

Table 8 – *Continued from previous page*

| Column name | Description |
|---|---|
| Scale | Scaling factor (scientific notation). The value is defined by $$Value \rightarrow Value \cdot Scale$$ |
| User Scale | Scaling factor (scientific notation). It complements the *Scale* provided or set by the meter, but does not replace it. It is suitable if an additional scaling is necessary. The value is defined by $$Value \rightarrow Value \cdot Scale \cdot User\ Scale$$ A column for *User Scale* is displayed only if *User Scale* deviates from the default value of *1e+0* (see Table 20). |
| Unit | Unit, see second column in Table 23 |
| OBIS-ID | OBIS code in the format X-X:X.X.X*X (X=0..255) |
| Encryption key | Key for encrypted wM-Bus meters. Supported modes: 5 and 7 |
| Cycle | Readout interval in seconds (with 0, the general readout cycle is used, see **Configuration** tab) |
| User label | User-defined description of the meter value, this allows an application-specific mapping. Allowed characters are: A-Z, a-z, 0-9, !, §, \$, %, &, /, (, ), =, ?, + and *. A comma is also allowed.<br>Illegal characters are: ⟨, ⟩ and ".<br>If using the CSV format, the semicolon (or the corresponding separator) should not be used. |
| Description | Description of the meter value according to the second column in Table 22. The display of storage number, tariff, value type and raw data can be configured via the *Description mode* parameter in the **Configuration** tab. |
| Idx | Index/position of meter/meter value in the meter list |
| Register | Offset of the register set belonging to the value when using the Modbus server * |
| BACnet | Object number of the value when using the BACnet server * |
| Active | Activates a meter or meter value for reporting to a server or logging. |

*if device is equipped with this interface/function

Table 8: Columns in Meter tab

The meter configuration can be changed with the buttons at the bottom or via the context menu. According to the limitations of the interface used (M-Bus, wM-Bus etc.), individual meters or meter values can be automatically scanned or manually created, deleted or changed.

The meters or meter values in the list can be selected by a simple mouse click. A range can be selected with the ⟨**SHIFT**⟩ key held down, or multiple meters can be selected (individually) with the ⟨**CTRL**⟩ key held down.

Duplicates of the serial number are marked yellow for easier checking of the meter list. Using the **Search** button, the complete meter list can be searched for a text. The search comprises as well meter values hidden by closing the symbol in front of the interface type.

**Reload** loads the last saved parameters, resets current changes, and correspondingly updates the meter values.

Upon delivery, the device has an empty meter list. If meters are connected via the external interfaces of the device, the **Scan** button can be used to start an M-Bus scan. The scan mode *M-Bus mode* is configured in the **Configuration** tab. More information on this can be found in Section 4.6.

✔ Depending on the mode and the number of connected meters, this may take a very long time.

The process can be interrupted using the **Cancel** button, whereby the meters already found are saved in the meter configuration. After the scan, the meter configuration is immediately applied, and only needs to be saved again after further changes. The scan procedure is only adding meters to the existing list, it is not deleting or changing already configured meters. Newly found M-Bus meters and their values are automatically activated after the scan and are assigned to a Modbus address or a BACnet number. The scan also permanently adds newly received wM-Bus meters to the configuration, provided that the parameter *wM-Bus listen* in the **Configuration** tab is activated. Since wM-Bus meters are not necessarily your own, they are not automatically activated, unlike M-Bus meters. The listen mode initially only lists all received meters without permanently saving them to the list.

✔ The meter values of M-Bus and wM-Bus meters are arranged in the same order as the data is present in the protocol. So, the meaning of the values can be directly compared with the data sheet of the relevant meter. Alternatively, the raw data of the meter values (see parameter *Description mode* in the **Configuration** tab, see Section 4.6) can be used for mapping the values.

✔ The timestamps transmitted in the M-Bus or wM-Bus protocol are automatically assigned to the individual measured values, and therefore not listed in the meter list by default. The configuration parameter

*MUC_SHOWTIMESTAMPENTRIES* in the configuration file `app/chip.ini` allows to manually activate the explicit representation of all timestamps (see Section 6.3).

🛈 Newly received wM-Bus meters are deactivated by default, and have to be manually activated and saved in order to be integrated into the reports and log data. Unsaved wM-Bus meters are lost after a restart.

Meters which cannot be found as well as meters connected to interfaces which do not enable automated scanning can be added manually using the **Add** button or using the ***Add meter*** item in the context menu. The number of meters is limited. The button **Add** and ***Add meter*** in the context menu are automatically deactivated once the maximum number of meters is attained.

For configuring individual meters or meter values, double click an entry or call the editing dialogue with the ***Edit*** context menu item. The naming of the input fields corresponds to the columns of the meter list (see Table 8). Individual fields are activated or deactivated according to the interface.

Among other things, a *User label* can be assigned to all entries here, so the meter or meter value can be mapped to a specific application. The individual readout interval of the meters can be set via the parameter *Cycle* as well. The key required for decoding can also be set for wM-Bus meters in the Meter editing dialogue.

🛈 S0 meters are internally processed with the number of pulses. The representation on the website in the *Value* column is nevertheless scaled to provide better readability. The *Scale* column contains the pulse value and, in contrast to other meter interfaces, does not have to be additionally multiplied. If a value of 280.09 and a scaling of 1e-4 is displayed in the **Meter** tab, 2800900 pulses are recorded internally. However, this unscaled meter value (280.09) appears in the report data analogously to those of other meters, such as the CSV or the XML files.

🛈 Meter values of S0 meters can only be set in the Add or Edit dialogue if the *Set value* checkbox is activated. The *Set value* checkbox must be deactivated if a configuration is not meant to change or overwrite the current meter value (e. g. change of the user label). The input of a meter value needs to be scaled.

🛈 Before saving the entered value of a S0 meter value, it is calculated back to the pulse count and rounded to whole pulses. Inaccuracies can result from the floating point data types.

The configuration can be finished with the **Ok** button or cancelled with the **Cancel** button.

For reporting and logging, individual meters and meter values can be directly activated or deactivated with the checkbox in the *Active* column. The meter values are automatically activated or deactivated by the configuration of a meter corresponding to the hierarchy. In the same way, an inactive meter is automatically activated if one of its meter values is activated. Multiple selected meters or meter values can be set with the context menu items ***Activate*** and ***Deactivate***.

All selected meters and meter values can be deleted by using the **Delete** button or the context menu item with the same name. Deleted wM-Bus meters are then created again if the parameter *wM-Bus listen* in the **Configuration** tab is activated.

➡ Individual meter values of an M-Bus or wM-Bus meter cannot be deleted.

The meter list is saved by using the **Save** button.

✔ Saving a meter configuration creates a new internal database file for logging the meter values aligned to this updated configuration.

The **Export** button can be used to export the meter list as a CSV file in the mode *Meter list* or to export the data pertaining to a particular instant as CSV, XML, JSON or User file in the mode *Log data (all meters)* resp. *Log data (selected meters)*, if Reporting is active in the **Server** tab with the settings defined therein. The time frame for the export of the meter data stretches from **Date (local)** and **Time (local)** to **End date (local)** and **End time (local)**.

✔ Logged meter data can only be exported if data was recorded for the specified period, i. e. at least one report was active during this period (see Section 4.8).

Page 30/81

UG_EN_MBUS-GEV.pdf

Version: 1.1

Released

Frank Richter, 23 February 2024

© solvimus GmbH

Figure 19: Exporting log data in the Meter tab

### 4.4.1 System meter

The system meter is a special function for providing device-specific operating parameters. These parameters are displayed via the system meter like normal meter values and can thus be monitored and analysed. The system meters must be added manually in the tab **Meter** using the **Add** button or using the **Add meter** item in the context menu.

Depending on the device, the parameters in the following table are available. Here, x denotes the S0 inputs (pulse inputs) and y the digital outputs.

| Entry | Description |
|---|---|
| Digital input <x> | State of the digital input, channel x (S0 inputs) |
| Digital output <y> | State of the digital output, channel y |
| Operating time | Operating time counter, in seconds |
| Reset counter | Power outage counter |
| Temperature | Board temperature, uncalibrated |
| Ampere | Bus load on M-Bus |
| On time | Time counter since last power outage, in seconds |
| CPU | CPU load |
| Memory | Free RAM |
| Memory <1> | Free memory of the application partition |
| Memory <2> | Free memory of the database partition |
| RSSI | Field strength of the cellular network in dBm (-113 to -51 dBm, -114 corresponds to be not connected) |

Table 9: Values of the system meter



Figure 20: System meter in Meter tab

➡ The system meter can be extended by further meter values via scripts. This is described in Section 6.7.3.

## 4.5 Tab Output

The tab **Output** lists, independent from the interface, an overview of the switchable digital outputs of all connected meters from the tab **Meter**. These digital outputs can be switched via a checkbox.

**Output Configuration**

| Interface | S | Serial | MAN | Medium | Version | Link | Value | | Unit | User label | Description | | Idx |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ⊟ System | | D0801BC4 | SLV | Communication controller | 135 | 0 | [01.09.22, 08:37] | | | | | | 0 |
| — | | | | | | | 0 | ☐ | None | | Digital output | | 3 |
| ⊟ M-Bus | | 00000026 | SLV | Electricity | 1 | 0 | [01.09.22, 08:37] | | | | | | 1 |
| — | | | | | | | 1 | ☑ | Bin | | Digital output | | 0 |
| — | | | | | | | 0 | ☐ | Bin | | Digital output | | 1 |
| — | | | | | | | 0 | ☐ | Bin | | Digital output | | 2 |
| — | | | | | | | 0 | ☐ | Bin | | Digital output | | 3 |

Figure 21: Tab Output

By default, only the S0 inputs and the digital output of the system meter can be switched. Information on the system meter is given in Section 4.4.1. If need be, the settings can be extended via the configuration file *chip.ini* (see Section 6.3). In the **Group [SOLVIMUS]**, the parameter *MUC_SETDEVICES* must be set.

## 4.6  Tab Configuration

The *Configuration* tab allows the parametrization of the meter interfaces of the device.



Figure 22: Tab Configuration

The following parameters are available:

| Column name | Description |
|---|---|
| **General readout and display parameters** | |
| Readout cycle mode | Format for specifying the standard readout cycle (for all meters, unless otherwise specified for individual meters in the **Meter** tab via the parameter *Cycle*). |
| | ▪ *Second*: Readout cycle is specified in seconds |
| | ▪ *Minute*: Readout cycle is specified in minutes |
| | ▪ *Hour*: Readout cycle is specified in hours |
| | ▪ *Daily*: daily readout at the specified time |
| | ▪ *Weekly*: weekly readout on the specified weekday and at the specified time |
| | ▪ *Monthly*: monthly readout on the specified day of the month and at the specified time |
| | ▪ *Quarterly*: quarterly readout on the specified day and month of the quarter and at the specified time (month 1..3 per quarter) |
| | ▪ *Yearly*: yearly readout on the specified day and month and at the specified time |
| Readout cycle | Standard readout cycle of the meters (unit according to *Readout cycle mode* in seconds, minutes or hours; only for *Readout cycle mode* in *Second*, *Minute*, *Hour*) |
| Readout cycle date (local) | First readout day in case of daily to yearly specification of the standard readout cycle, depending on the interval format the entered month is used, the year is not relevant |
| Readout cycle time (local) | Readout time for daily to annual specification of the standard readout cycle |
| Description mode | Mode for displaying the meter value description on the website: |
| | ▪ *None*: empty meter value description |
| | ▪ *Standard*: simple meter value description (see Table 22) |
| | ▪ *Extended*: extended meter value description (parameters are only shown if not zero): Notation: description [storage number] ⟨tariff⟩ {value type} Example: Energy [2] ⟨1⟩ {max} |
| | ▪ *Extended with DIF/VIF*: extended meter value description added by raw DIF/VIF data: Notation: description [storage number] ⟨tariff⟩ {value type} # XX XX XX . . . Example: Energy [2] ⟨1⟩ # 8C 11 04 |
| | ▪ *Extended with raw data*: extended meter value description added by complete raw data for this entry. Notation corresponds to *Extended with DIF/VIF*: Example: Energy [2] ⟨1⟩ # 8C 11 04 96 47 06 00 |
| | ▪ *DIF/VIF*: raw DIF/VIF data in description field |
| | ▪ *Raw data*: complete raw data for this entry in description field |
| Maximum device count | Limits the number of meters being added upon scanning (0: no limit). Already configured meters are included by this parameter. |
| Maximum value count | Limits the number of meter values for a meter during a readout process (0: no limit). Already configured meters keep their original configuration after initial scan or saving. |
| Store meter values | Setting if the read out values are to be written into the database when no report is active. |
| | ▪ *Automatic*: storage only if a report is active |
| | ▪ *On*: always storage |
| | This selection is only offered if the device supports reports and database storage. |
| Raw log active | Activating the logging of raw data from the interfaces |
| **Specific parameters of the M-Bus-Master*** | |
| M-Bus mode | Configuration of the communication. The following modes are available: |
| | ▪ *Disabled*: The M-Bus interface is deactivated. |
| | ▪ *Master*: The device is M-Bus master and can read out meters. |
| | ▪ *Transparent/TCP*: The M-Bus interface is available for a transparent communication via TCP. |
| | ▪ *Transparent/UDP*: The M-Bus interface is available for a transparent communication via UDP. |
| | ▪ *Master & Transparent/TCP*: The device is M-Bus master and can read out meters. The interface is at the same time available for a transparent communication via TCP. |
| M-Bus addressing | Configuration how the device searches meters during an M-Bus scan and how these meters are addressed (details see Section 5.3.2). The following modes are available: |
| | ▪ *Primary Scan*: Search for primary address |
| | ▪ *Secondary scan*: Search for secondary address |
| | ▪ *Secondary scan reverse*: Search for secondary address in inverted order |
| Primary start address | Sets the start address for the primary search. |
| Primary final address | Sets the final address for the primary search. |
| Secondary address mask | Sets the address mask for the secondary search, 8 digits; wildcards are indicated by the letter "F"; missing characters are filled up with leading 0 from the left. |
| M-Bus baud rate | M-Bus communication baud rate |
| M-Bus timeout | M-Bus timeout until first data is received (in ms) |

*Continued on next page*

Table 10 – *Continued from previous page*

| Column name | Description |
|---|---|
| M-Bus idle timeout | M-Bus timeout for detecting the end of communication (in ms) |
| M-Bus full timeout | M-Bus timeout (total) for the reception of a data telegram (in ms) |
| M-Bus request mode | Mode of the M-Bus readout process (REQ_UD2):<br><br>• *Standard*: Readout process using REQ_UD2<br><br>• *Extended 1*: Readout process using Get-All-Data (DIF/VIF 0x7F 0x7E) and REQ_UD2<br><br>• *Extended 2*: Readout process using Get-All-Data (DIF 0x7F) and REQ_UD2 |
| M-Bus reset mode | Mode of the M-Bus reset (before scan and readout process):<br><br>• *None*: No reset<br><br>• *Standard*: SND_NKE to the primary address of the meter or to the broadcast address 0xFF in case of secondary addressing<br><br>• *Extended 1*: SND_NKE to the primary address 0xFD, followed by a SND_NKE to the primary address of the meter or to the broadcast address 0xFF in case of secondary addressing<br><br>• *Extended 2*: SND_NKE to the primary address 0xFD, followed by an application reset to the broadcast address 0xFF, followed by a SND_NKE to the primary address of the meter or to the broadcast address 0xFF in case of secondary addressing |
| M-Bus max. multipage | Limits the number of multipage requests |
| M-Bus transparent port | Network port of the transparent M-Bus mode |
| **Specific parameters of the M-Bus-Slave*** | |
| M-Bus slave mode | Sets the mode of the M-Bus slave (M-Bus, TCP or UDP) or deactivates the interface. |
| M-Bus slave baud rate | Sets the baud rate of the outer M-Bus network |
| M-Bus slave port | Network port of the M-Bus slave slave in case of TCP or UDP |
| M-Bus slave mode (2nd) | Sets the mode of the M-Bus slave (instance 2; TCP or UDP only) or deactivates the interface. |
| M-Bus slave port (2nd) | Network port of the M-Bus slave (instance 2) |
| **Specific parameters of the wM-Bus*** | |
| wM-Bus frequency | Frequency band for the communication with the wM-Bus meters |
| wM-Bus network role | Function of the wM-Bus interface. The following mode are available:<br><br>• *Disabled*: The wM-Bus interface is deactivated.<br><br>• *Master (Concentrator)*: The wM-Bus interface is used to read out meters.<br><br>• *Slave (Meter)*: The wM-Bus interface is used to transmit meter data. |
| wM-Bus mode | Sets the wM-Bus communication mode of the OMS interface (T, S, C or C/T-Mode) or deactivates the interface. |
| wM-Bus transparent mode | Activates and sets the transparent mode of the wM-Bus communication (Transparent/TCP or Transparent/UDP or Disabled). |
| wM-Bus transparent port | Network port of the transparent wM-Bus mode |
| wM-Bus listen | Activates the processing and listing of unconfigured and newly received wM-Bus devices |
| Show encryption keys | Displays the keys in plain text after saving the list. |
| **Specific parameters of the wM-Bus (channel 2)*** | |
| wM-Bus2 frequency | Frequency band for the communication with the wM-Bus meters (channel 2) |
| wM-Bus2 mode | Sets the wM-Bus communication mode of the OMS interface (T, S, C or C/T-Mode) or deactivates the interface (channel 2). |
| wM-Bus2 transparent mode | Activates and sets the transparent mode of the wM-Bus communication (Transparent/TCP or Transparent/UDP or Disabled, channel 2) |
| wM-Bus2 transparent port | Network port of the transparent wM-Bus mode (channel 2) |
| **Specific parameters of the pulse inputs*** | |
| S0 mode | Sets absolute or relative pulse counting or deactivates the interface. |
| **Specific parameters of the serial interface*** | |
| Serial mode | Sets the operating mode of the serial interface (DLDE, Modbus RTU, Transparent/TCP or Transparent/UDP) or deactivates the interface. |
| Serial baud rate | Serial communication baud rate |
| Serial data bits | Serial communication data bits |
| Serial stop bits | Serial communication stop bits |
| Serial parity | Serial communication parity |
| Serial first timeout | Serial communication timeout until first data is received (in ms). In push mode the meter has to be silent for this configured timeout (corresponds to idle time) |
| Serial idle timeout | Serial communication timeout for detecting the end of communication (in ms) |
| Serial full timeout | Serial communication timeout (total) for the reception of a data telegram (in ms) |
| Serial transparent port | Network port for the transparent serial communication |

*Continued on next page*

Page 34/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH

Table 10 – *Continued from previous page*

| Column name | Description |
|---|---|
| DLDE mode | Procedure of serial DLDE communication:<br><br>• *Request*: request according to mode A or mode B defined in IEC 62056-21 (static baud rate)<br>• *Request (C-Mode)*: request and handshake according to mode C defined in IEC 62056-21 (static baud rate)<br>• *Push*: reception of cyclically pushed data from the meter |

*if device is equipped with this interface/function

Table 10: Fields in the Configuration tab

The **Save** button is used to save the configuration. The **Reload** command loads the last saved parameters and resets current changes.

🛈 The device is automatically reinitialized by accepting the parameters via the **Save** button.

## 4.7 Tab WAN

The **WAN** tab allows the parametrization of the WAN connection for devices with integrated cellular modem. This is permanently set up when the device is restarted and is kept permanently active.



Figure 23: Tab WAN

The following parameters are available:

| Column name | Description |
|---|---|
| WAN active | Activation of the WAN module |
| SIM PIN | PIN of the SIM card |
| APN | Name of the access point (APN) |
| APN auth mode | Authentication mode of the APN |
| APN username | User name for authentication at the APN |
| APN password | Password for authentication at the APN |
| Use WAN network time | Updates the system time when connecting with the radio network. This time is not updated regularly. SNTP (see Table 7) can be used for regular updating. |
| Reconnect Monitor | Additional monitoring of the radio connection and forced disconnection as well as renewal of the radio connection if the condition is not met. The following modes are available:<br><br>• *off*: no additional monitoring<br>• *Data Received*: data were received by radio in the indicated time frame<br>• *Any report successful*: an arbitrary report was at least once successful in the indicated time frame<br>• *All reports successful*: all reports were at least once successful in the indicated time frame<br>• *Selected report successful*: the selected report was at least once successful in the indicated time frame |
| Reconnect (days) | Interval in days which is monitored. Rationale numbers are also valid here, e. g.: *0.25*. |
| Report Instance | Report Instance which is monitored if the mode *Selected report successful* is used (otherwise greyed out). |
| WAN signal strength test mode | Sets the WAN interface in a mode to monitor the signal strength to optimize the antenna positions. In this mode, the parameters Provider, Network and the signal indicators (RSSI, RSSQ, RSRQ) are updated at high frequency for all devices. In devices with just one modem channel (see note underneath this table), no data connection exists via the WAN interface in this mode. |
| Status | Status of the WAN connection (connected / not connected) |
| Provider | Diplays, with WAN connected, the PLMN code or the name of the provider with whom the device is connected. See note underneath this table. |
| Network | Network technology of the radio connection. See note underneath this table. |
| Network band | Displays the mobile radio band (frequency band) in use. See note underneath this table. |
| RSSI (dbm) | Field strength of the cellular network in dBm (-113 to -51 dBm, -114 corresponds to be not connected). See note underneath this table. |
| RSRP (dbm) | Reference Signal Received Power. See note underneath this table. |
| RSRQ (dbm) | Reference Signal Received Quality. See note underneath this table. |
| IP address | IP address in the WAN |
| Gateway IP address | Remote station in the WAN |
| DNS IP address (primary) | Primary DNS server for the name resolution |
| DNS IP address (secondary) | Secondary DNS server for the name resolution |
| SIM card ICCID | Displays the number/ICCID of the inserted SIM card with active WAN connection |

Table 11: Fields in the WAN tab

✔ Hint with respect to *WAN signal strength test mode*:

– Updates of the fields Provider, Network, Network band, RSSI, RSSP, RSSQ depend on the device hardware. They are regularly updated in devices with several channels to the modem (MUC.easy[plus] 4G/NB-IoT). In devices with just one channel to the modem, the values are read only when establishing the connection (MUC.easy[plus] 2G/3G, MUC.one). For these devices, the test mode can be used to benefit from regular values when the antenna position is to be optimized. This mode should only be activated in case of local connection as there is no data connection in these devices for this mode.

– Only RSSI, RSSP and RSSQ are updated automatically in the web-based front end. The button **Reload** can be used for updating the remaining parameters.

The necessary parameters for the WAN connection should be provided by the cellular network provider of your SIM card.

ⓘ Please check whether the cellular network contract includes the expected quantity of data, otherwise increased costs or a blocking of the SIM card may follow.

ⓘ Please check whether the parameters are correct. Incorrect parameters can lead to increased costs or blocking of the SIM card.

ⓘ If an invalid PIN is entered, it will be used only once per software startup. Thus, the remaining attempts for entering the PIN are not depleted and a new PIN can be entered via the website.

Page 36/81
UG_EN_MBUS-GEV.pdf
Version: 1.1
Released
Frank Richter, 23 February 2024
© solvimus GmbH

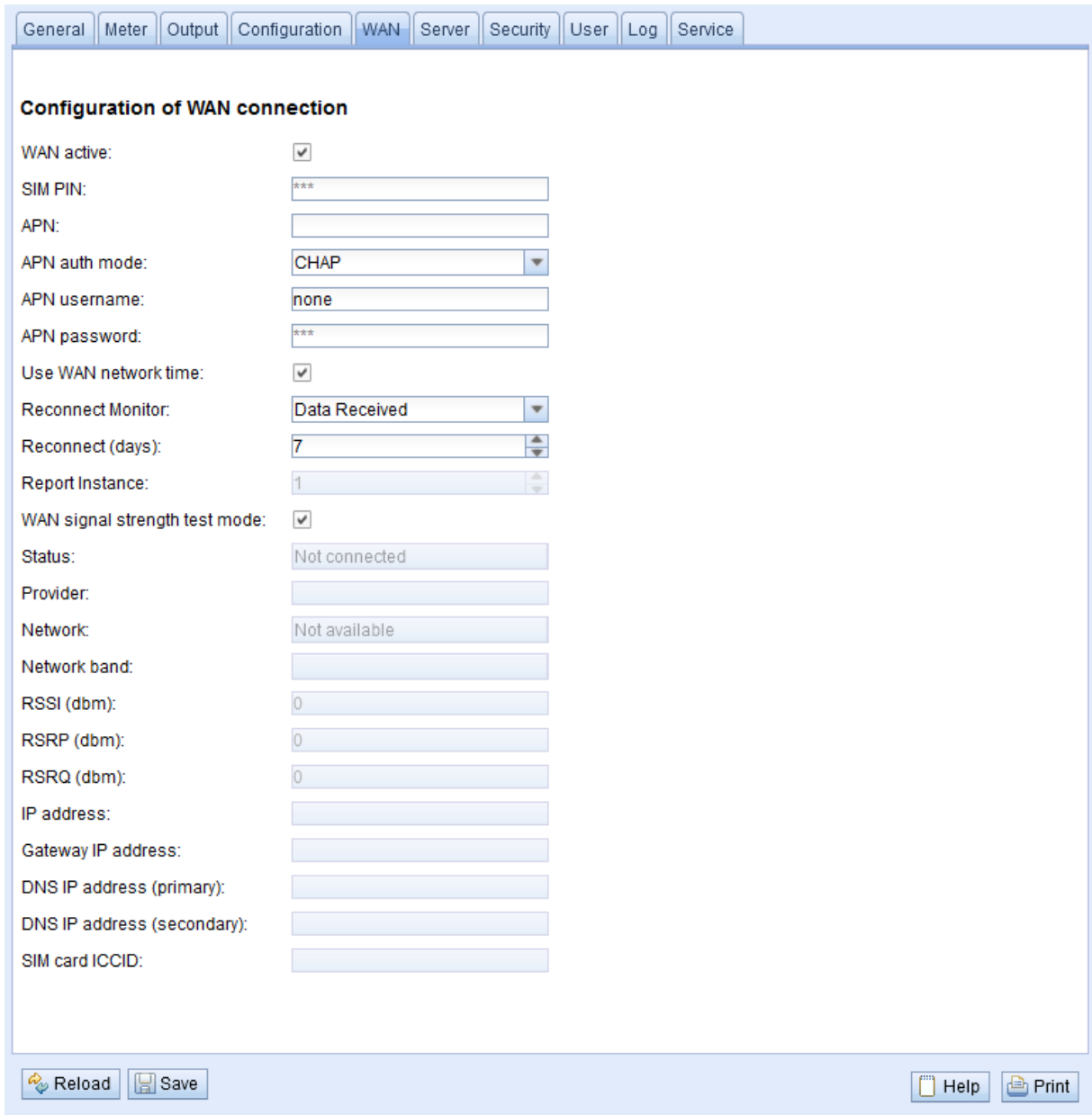⚠ Changing the WAN configuration via an active cellular network connection is not recommended, as the device may no longer be accessible after a changed or invalid configuration.

The **Save** button is used to save the configuration. The **Reload** command loads the last saved parameters and resets current changes.

🛈 The device is automatically reinitialized by accepting the parameters via the **Save** button. An existing WAN connection is terminated and re-established.

## 4.8  Tab Server

The *Server* tab allows the parametrization of the data reports to third-party systems. In some data concentrators, the function „Multi Channel Reporting" (MCR) permits to send reports with meter data to up to 10 different and independent instances (configurations) that can be executed in parallel .



Figure 24: Tab Server

The following parameters are available:

| Column name | Description |
|---|---|
| **Parameters for data concentrators with Report functionality** | |
| Report instance | Selection of the respective instance |
| Report mode | Sets the operating mode of the respective instance or deactivates it. The following modes are available: <br><br> • *TLS*: active data push via encrypted TCP channel to the specified server <br> • *TCP*: active data push via unencrypted TCP channel to the specified server <br> • *SMTP*: active data push via email to the specified address. The report is in the text of the email. <br> • *SMTP with Attachment*: active data push via email to the specified address. The report is in the attachment to the email, the text of the email is void. <br> • *FTP (client active)*: active file transfer via FTP to the specified server (encrypted or unencrypted). In case of unencrypted FTP, the data connection is established from the server. The files are stored in a specified directory on the server. For a MUC.easy$^{plus}$ results: <br>    – File name: `<target path>/MUC_Easy_ID_<ID>_TS_<timestamp>.csv` <br>    – Example: `/upload/MUC_Easy_ID_6891d0800d89_TS_1372759627.csv` <br> The parameters in angle brackets denote respectively the configured target path, the serial number (ID) of the device and the timestamp (Unix timestamp) at the instant of data transmission. The meter data are transmitted in the CSV format. <br> • *FTP (client passive)*: active file transfer via FTP to the specified server (encrypted or unencrypted). In case of unencrypted FTP, the data connection is established from the device. The storage location and the naming convention of the files is identical to *FTP (client active)*. <br> • *MQTT*: active data push via MQTT client to the specified server/broker (encrypted or unencrypted) <br> • *Local File*: writing local files to internal memory for later data pull by third party systems (e. g. via FTP) <br> • *User*: user-specific report mechanism based on a BASH script (see Section 6.7.2) |
| Report format | Sets the data format used for the transmission of the respective instance. Several predefined formats are available. Further, the format *User* can be selected in order to define an own format of the data using a XSLT script. |
| Report cycle mode | Format for specifying the report cycle of the respective instance <br><br> • *Second*: Report cycle is specified in seconds <br> • *Minute*: Report cycle is specified in minutes <br> • *Hour*: Report cycle is specified in hours <br> • *Daily*: daily report at the specified time <br> • *Weekly*: weekly report on the specified weekday and at the specified time <br> • *Monthly*: monthly report on the specified day of the month and at the specified time <br> • *Quarterly*: quarterly report on the specified day and month of the quarter and at the specified time (month 1..3 per quarter) <br> • *Yearly*: yearly report on the specified day and month and at the specified time <br> • *On Readout*: Report will be sent directly after readout. The report interval is identical to the readout interval. |
| Report cycle | Report cycle of the respective instance (unit according to *Report cycle mode* in seconds, minutes or hours; only for *Report cycle mode* in *Second*, *Minute*, *Hour*). Not active if Report cycle mode is *On Readout*. |
| Report cycle date (local) | First report day of the respective instance in case of daily to yearly specification of the report cycle, depending on the interval format the entered month is used, the year is not relevant. Not active if Report cycle mode is *On Readout*. |
| Report cycle time (local) | Report time of the respective instance for daily to annual specification of the report cycle. Not active if Report cycle mode is *On Readout*. |
| Report address | Host address of the remote station or mail server (outgoing mail server) |
| Report port | Network port of the remote station to connect to |
| Report directory | Path on the remote station |
| Report username | User name for server access |
| Report password | Password for server access |
| Report source address | Address of the sender (Email) |
| Report destination address | Address of the recipient (Email) |
| Report user parameter 1 | User-specific parameter 1 (for user-specific format or mode) |
| Report user parameter 2 | User-specific parameter 2 (for user-specific format or mode) |
| Report user parameter 3 | User-specific parameter 3 (for user-specific format or mode) |
| Insecure | Allow insecure encrypted communication by disabling certificate and hostname verification |
| Debug transfer | Additional logging for transmitting reports in order to investigate more thoroughly problems in the communication with the server. |
| **Parameters for Modbus-Server\*** | |

*Continued on next page*

Page 38/81

UG_EN_MBUS-GEV.pdf

Version: 1.1

Released

Frank Richter, 23 February 2024

© solvimus GmbH

Table 12 – *Continued from previous page*

| Column name | Description |
|---|---|
| Modbus mode | Sets the operating mode to Modbus TCP, Modbus UDP or deactivates the service. In operating mode *Modbus TCP*, up to 5 parallel connections from different Modbus TCP masters are accepted. |
| Modbus port | Network port on which the service is waiting for incoming connections from a remote station (the Modbus TCP client) |
| Modbus test | Dummy mode for representing the test process data via Modbus |
| Modbus swap | Changes the word order from MSW first (default) to LSW first (option checked) |
| Modbus float only | Reduces the Modbus register layout from 10 registers per value to 2 registers per value by only representing the serial number of the meter and the floating point value of the corresponding meter value |
| Modbus multi slave | Activates the multi-slave feature, where the data of a meter can be accessed as individual virtual Modbus slave using a unique Modbus address |
| **Parameters for BACnet server*** | |
| BACnet active | Activates the BACnet functionality |
| BACnet config network | Activates a second virtual network interface for the BACnet service |
| BACnet IP | IP address of the second virtual network interface for BACnet |
| BACnet netmask | Subnet mask of the second virtual network interface for BACnet |
| BACnet broadcast | Broadcast address of the second virtual network interface for BACnet |
| BACnet BBMD | IP address of a BACnet Broadcast Management Device (BBMD) for routing across local network boundaries |
| BACnet port | UDP port number of the BACnet service (default port: 47808) |
| BACnet device ID | ID number of the BACnet device |
| BACnet device name | Device name of the BACnet device |
| BACnet location | Location information of the BACnet device |

*if device is equipped with this interface/function

Table 12: Fields in the Server tab

Depending on the operating mode of the server interface, individual parameters required for the configuration are enabled.

🛈 When using encrypted connections (TLS, MQTTS, SMTPS, FTPS), the server certificate or the Root CA certificate for the server must be saved on the device. This is achieved by **Config Import** of the certificates in PEM format in the tab *Service*.

The **Save** button is used to save the configuration. The **Reload** command loads the last saved parameters and resets current changes. The **Report** button allows immediate transmission of the data previously read out.

🛈 Setting the parameters via the button **Save** causes a reinitialization of the device.

🛈 Mind a correct system time before activating the report if Report cycle mode is not *On Readout*. If the system time is synchronized later, e. g. via a SNTP service, gaps may occur in the log. These gaps may cause empty files to be transmitted to the server.

## 4.9 Tab Security

The *Security* tab allows the parametrization of the network services by the device.

Figure 25: Tab Security

The following parameters are available:

| Column name | Description |
|---|---|
| HTTP server active | Activation of the internal HTTP server of the device. Deactivation is possible only by selecting HTTPS. |
| HTTPS server active | Activation of the internal HTTPS server of the device. Deactivation is possible only by selecting HTTP. |
| FTP server active | Activates the internal HTTP server of the device. If deactivated, there is no FTP access to the device. |
| SSH server active | Activates the internal SSH server of the device (administrative access). |
| Network discovery active | Activates the internal discovery server of the device. If deactivated, the device is no longer displayed in the Netdiscover tool (see Chapter 3) |
| Network discovery password | Password for setting the network parameters via the Netdiscover tool |
| Modbus server active | Modbus server active, read-only, depending on the **Server** tab |
| BACnet server active | BACnet server active, read-only, depending on the **Server** tab |

Table 13: Fields in the Security tab

The **Save** button is used to save the configuration. The **Reload** command loads the last saved parameters and resets current changes.

ⓘ The device is automatically reinitialized by accepting the parameters via the **Save** button. An existing WAN connection is terminated and re-established.

## 4.10 Tab User

The **User** tab allows the parametrization of different users and their permissions for the website.



Figure 26: Tab User

The following users are preconfigured upon delivery:

| User name | Password | Comments |
|---|---|---|
| admin | admin | Administrative user with full access to all services of the device (HTTP, FTP, SSH, IP configuration). |

*Continued on next page*

Page 40/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH

Table 14 – *Continued from previous page*

| User name | Password | Comments |
|---|---|---|
| web | web | Default user for the website. If a user with this name and password exists, the web interface automatically logs in using these credentials. Otherwise, the user is prompted to enter individual credentials. Per default, this user has full access to the website of the device. |
| ftp | ftp | User for unencrypted FTP access restricted to the log in path `/ext/Log` |

Table 14: User accounts upon delivery

On the website, the existing configuration is shown in a table and can be changed respectively:

| Column name | Description |
|---|---|
| Name | User name |
| Overwrite password | It is set if a (new) password has been set for the user in the editing dialogue. |
| Change Password | Setting whether the user is allowed to change his password |
| Require change Password | Setting whether the user has to change his password at the next login |
| Sessions | Number of currently active sessions of this user |
| Maximum sessions | Setting how often the user may be logged in at the same time in parallel (-1=unlimited) |
| Read General | Read permission to the General tab |
| Write General | Write permission to the General tab |
| Read Meter | Read permission to the Meter tab |
| Write Meter | Write permission to the Meter tab |
| Read Output | Read permission to the Output tab |
| Write Output | Write permission to the Output tab |
| Read Config | Read permission to the Configuration tab |
| Write Config | Write permission to the Configuration tab |
| Read WAN | Read permission to the WAN tab |
| Write WAN | Write permission to the WAN tab |
| Read Server | Read permission to the Server tab |
| Write Server | Write permission to the Server tab |
| Read Security | Read permission to the Security tab |
| Write Security | Write permission to the Security tab |
| Read Log | Read permission to the Log tab |
| Read Service | Read permission to the Service tab |
| Write Service | Write permission to the Service tab |
| Write User | Read and write permission to the User tab |
| FTP | Permission of the user to log in via FTP (maximum 2 users) |

Table 15: Fields in the User tab

The user configuration can be changed with the buttons at the bottom or via the context menu. Except from the *admin* user, other users can be created, deleted or changed.

The users in the list can be selected by a simple mouse click. A range can be selected with the ⟨**SHIFT**⟩ key held down, or multiple users can be selected (individually) with the ⟨**CTRL**⟩ key held down.

The **Reload** command loads the last saved parameters and resets current changes.

When write permission to a tab is granted, read permission is also granted automatically.

⚠ The *admin* user cannot be changed or deleted in the user configuration. The administrator password can only be changed by using the **Change password** button when the *admin* user is logged in.

⚠ If the administrator password is lost, the device can only be reset to factory defaults by solvimus GmbH as file access on the device is limited for safety reasons. When resetting, all configuration data and meter data are lost.

ℹ Only the *admin* user has full access to the file system of the device via encrypted FTP (SFTP). The second FTP user can access only the path `/ext/Log`, even without encryption.

New users can be added via the **Add** button or via the context menu item with the same name. The following dialogue will open:

Figure 27: Input dialogue for adding new users

In addition to the user name and password, you can specify how often a user may log in at the same time (-1=unlimited). Besides the user *admin*, another user can have FTP access to the device. The unencrypted FTP access only allows access to the log data on the device (path: */ext/Log*). This permission can only be enabled at the time the user is created.

ⓘ A separate FTP user (e. g. *ftp*) allows a remote client to download the stored log data (manually or automatically), whithout having access to other services or data on the device.

For reconfiguring an already existing user, the editing dialogue can be opened by double clicking its entry or via the context menu item **Edit**. This dialogue has the same structure as the dialogue for adding a user. For resetting the password of an existing user, the **Set Password** checkbox has to be set. If the **Set Password** checkbox is not set, the user password is not changed or reset during this configuration process. A user password cannot be read.

The configuration can be finished with the **Ok** button or cancelled with the **Cancel** button.

The permissions of a user are directly set in the user list. If a user has write permission to a tab, the user automatically gets the permission to see the tab (read access).

Using the button **Delete** or the context menu item with the same name, all selected users (with the exception of the *admin* user) can be deleted.

The **Save** button is used to save the user configuration.

## 4.11 Tab Log

The *Log* tab allows accessing log information and status outputs. That facilitates the analysis of the behaviour and troubleshooting.

ⓘ The extent of the log entries depends largely on the settings in the **Log mode** field in the *General* tab (see Section 4.3).

ⓘ For viewing the raw data logs of the meter interfaces, the **Raw data log** field in the *Configuration* tab must be activated (see Section 4.6).

Page 42/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH
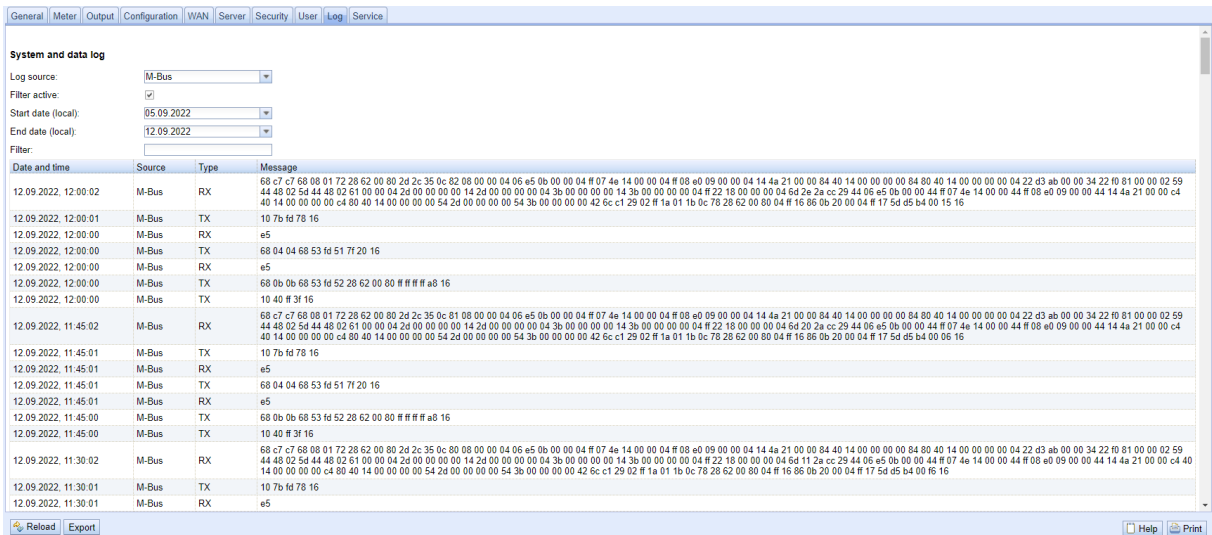
Figure 28: Tab Log

The following parameters are available:

| Column name | Description |
|---|---|
| Log source | Selects the source of the log entries.<br><br>• *System log*: Show the log entries of the system (Linux) and the application<br>• *Application*: Show the log entries of the application<br>• *M-Bus*: Show the raw data of the M-Bus interface (if **Raw data log** is active in the **Configuration** tab)<br>• *wM-Bus*: Show the raw data of the wM-Bus interface (if **Raw data log** is active in the **Configuration** tab)<br>• *DLDE*: Show the raw data of the DLDE interface (if **Raw data log** is active in the **Configuration** tab)<br>• *Modbus Master RTU*: Show the raw data of the Modbus Master RTU interface (if **Raw data log** is active in the **Configuration** tab)<br>• *Modbus Slave RTU*: Show the raw data of the Modbus Slave RTU interface (if **Raw data log** is active in the **Configuration** tab) |
| Filter active | Enables filtering by time range and string expression |
| Start date (local) | Start date of the time range for the log entries |
| End date (local) | End date of the time range for the log entries |
| Filter | String expression used for filtering the log (search for keyword or regular expression in the **Message** column) |

Table 16: Fields in the Log tab

The **Reload** button updates the log entries according to **Log source** and the filter settings (including the time range).

✔ Using the keyword *serial=* allows filtering for one meter's secondary ID in the raw data log, e. g. *serial=12345678*. Only telegrams from this meter are shown then.

✔ Depending of the extent of the log entries, it may take some time to generate the table.

✔ The filter settings are kept when changing between tabs. So, coming back to this tab, the old filter is still active. This will ease the troubleshooting but may cause increased load times for extensive logs.

ℹ If no log entries are shown, please check the filter settings. If necessary, extend the specified time range, reset the filter or deactivate it.

ℹ The number of log entries shown is limited to 500. Use the filter or the time range to reduce the entries.

The **Export** button generates a CSV file containing all log entries matching the filter and time range for downloading it. This download may take some time depending on the size of the log.

## 4.12 Tab Service

The **Service** tab allows maintenance and provides related information or functions:

Figure 29: Tab Service

The following parameters are available:

| Column name | Description |
|---|---|
| Product name | Product name |
| Hardware version | Version of the hardware |
| OS version | Version of the operating system |
| Software version | Version of the software |
| Website version | Version of the website |
| M-Bus load profile | If available and ticked: licence for load profile active |
| Modbus server | If available and ticked: licence for Modbus server active |
| BACnet server | If available and ticked: licence for BACnet server active |
| M-Bus slave | If available and ticked: licence for M-Bus slave active |

Table 17: Fields in the Service tab

The values are updated using the **Reload** button.

The **Config export** and **Config import** buttons allow to download the configuration from the device or upload the configuration to the device.

When exporting the configuration, a selection dialogue permits choosing which data is downloaded from the device:

- Certificates
- Device configuration
- Network configuration
- Device name
- Meter configuration

✔ The network configuration and the device name are part of the device configuration. If the device configuration is to be transferred to another device, it is recommended not to export the network configuration and the device name. Usually these should not be transferred to other devices.

Page 44/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH
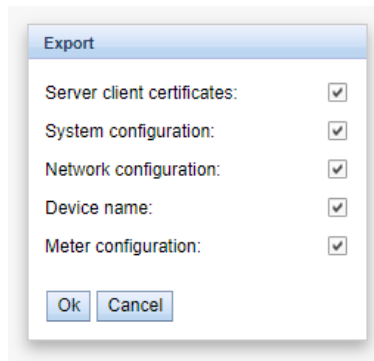
Figure 30: Options for exporting the configuration

The configuration is downloaded as a *.tar.gz file. This compressed archive is an excerpt from the file system of the device. It can be stored as a backup or modified for uploading it later to the same or another device. It is useful for transferring a valid configuration to a replacement device or for commissioning many similar devices (see Section 3.7).

When importing the configuration, a file selection dialogue comes up for selecting the corresponding *.tar.gz file.

Using the **Update firmware** button opens a file selection dialogue as well. An update file can be selected here. The solvimus GmbH provides updates as *.enc files on a regular basis. These files can then be uploaded to the device. After successfully uploading them, the update process is started automatically and the device is then restarted. An alternative procedure for updating the firmware is described in Section 3.7.

The device can be restarted using the **Reboot system** button. All internal processes are shut down and re-initialized after the restart. Meter data pending to be sent via the WAN interface is transferred after a restart. Use this button if you intend to manually modify the configuration via FTP(S) or after a manual update.

## 4.13  Print page

The **Print** button (see Figure 17, bottom right) can be used for getting an entire overview of the configuration or for exporting it via the clipboard. The website generates an additional browser window containing all available configured parameters and meters according to the access rights. The print page is automatically closed after a user has logged out from the website (at the top right of the web-based front end, if not already closed).

✔ The meter list displayed is also suitable for inserting it into a spreadsheet.

**MUC.easy<sup>plus</sup>**

**Configuration**

**General configuration**

| | |
|---|---|
| Device name: | MUC.easy plus 4G |
| Serial number: | 6891d0803d4d |
| DHCP: | on |
| IP address: | 192.168.3.21 |
| Subnet mask: | 255.255.255.0 |
| Gateway IP address: | 192.168.3.254 |
| DNS IP address (primary): | 192.168.1.161 |
| DNS IP address (secondary): | 192.168.1.162 |
| VPN: | 0 |
| Free space log (kB): | 2237116 |
| Free space Flash (kB): | 114670 |
| System date (local): | Thu Nov 02 2023 10:50:00 GMT+0100 (Mitteleuropäische Normalzeit) |
| SNTP server: | pool.ntp.org |
| Log mode: | All |

**Configuration of meter interfaces**

| | |
|---|---|
| Readout cycle mode: | Quarterly |
| Readout cycle: | 900 |
| Readout cycle date (local): | Wed Nov 01 2023 00:00:00 GMT+0100 (Mitteleuropäische Normalzeit) |
| Description mode: | Standard |
| Maximum device count: | 500 |
| Maximum value count: | 0 |
| Store meter values: | Automatic |
| Raw log active: | on |
| M-Bus mode: | Master |
| M-Bus addressing: | Secondary scan |
| Primary start address: | 0 |
| Primary final address: | 250 |
| Secondary address mask: | FFFFFFFF |
| M-Bus baud rate: | 2400 |
| M-Bus timeout (ms): | 500 |
| M-Bus idle timeout (ms): | 100 |
| M-Bus full timeout (ms): | 10000 |
| M-Bus request mode: | Standard |
| M-Bus reset mode: | Standard |
| M-Bus max. multipage: | 3 |
| M-Bus transparent port: | 5000 |

Figure 31: Print page of the device (excerpt), here the example of a MUC.easy<sup>plus</sup>

## 4.14 Troubleshooting the front end

Using a standard web browser for accessing the web server running on the device is an easy and intuitive way to manage the device. Nevertheless, impairments or unwanted behaviour may occur.

> ✔ One potential error source is the browser cache, especially if several devices are operated with the same IP address or after an update has been applied. To eliminate this error source, first terminate the web session by using the **Logout** button and then completely reload the website. Depending on the browser, this is initiated using a shortcut, e. g. ⟨**CTRL+F5**⟩ or ⟨**CTRL+R**⟩.

### 4.14.1 Website or front end cannot be accessed

The website cannot be loaded or the error message „webservice not available" appears.

Inspect the IP settings of the device and of your computer. The IP addresses should be in the same subnet or a route must be set up. If possible, change the IP addresses accordingly. Please ask your administrator. Alternatively, you can also use DHCP to assign a valid IP address (see Tool Netdiscover in Chapter 3). Below there are two examples of a valid configuration:

Page 46/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH

- Device: 192.168.1.101 (default IP), subnet mask: 255.255.255.0 → PC: 192.168.1.xxx (xxx = 0-254, except 101 and other already used IP addresses), recommended for direct connection 1:1 device and PC
- PC: 192.168.178.21, subnet mask: 255.255.255.0 → device: 192.168.178.xxx (xxx = 0-254, except 1, 21, 254 and other already used IP addresses), typical for connection to a router in the home network

Please check whether the device is listed in the Netdiscover tool (see Chapter 3). Please check the connectivity in general via a ping test integrated in the Netdiscover tool.

Please check whether a firewall is blocking the data transmission or whether the routing is configured accordingly. Please ask your administrator.

In the case of an HTTPS connection, the browser may block the access under certain circumstances. Please confirm the provided certificate in the browser or „trust" the website and its certificate if you are sure to access the correct device.

If errors could not be eliminated, please contact our customer support:
E-Mail: support@solvimus.de
Phone: +49 3677 7613065

### 4.14.2 Login to website is refused

Please check the user settings and permissions for the website as well as the user credentials.

There may be another user already logged in while the number of active sessions is limited. Then the login is denied. lease check the user credentials and the number of active sessions in the *User* tab.

If errors could not be eliminated, please contact our customer support:
E-Mail: support@solvimus.de
Phone: +49 3677 7613065

### 4.14.3 All input fields or buttons are greyed out

Buttons greyed out are indicating that write permission is not granted. Please note that only one logged in user gets write access.

Please check whether another session is already active. This can also occur if a browser window is just closed without logging out first. The session is then still active for a short time. Please log out again and wait about one minute. Please check the user's permissions and the number of active sessions in the *User* tab.

Please check whether the user has write permissions.

If errors could not be eliminated, please contact our customer support:
E-Mail: support@solvimus.de
Phone: +49 3677 7613065

### 4.14.4 Not all tabs are visible

Please check the user's read permissions. Only those tabs are available with granted read permission to the user. Please check the user's permissions in the *User* tab.

If errors could not be eliminated, please contact our customer support:
E-Mail: support@solvimus.de
Phone: +49 3677 7613065

### 4.14.5 Export of the meter readings of one/several meters is empty

Meter readings are only stored when a report is active in order to optimize the memory. Please check whether a report is active in the *Server* tab.

Please check the time range for the export. The chosen time of the report has to start before a valid readout. For example, for exporting the readout from 29/09/2020 01:15 pm, the time for export should be set to

29/09/2020 01:10 pm. The report then contains all readouts starting from 01:10 pm until the end of the **Report cycle** configured for instance 1 in the **Server** tab or 15 minutes.

If errors could not be eliminated, please contact our customer support:
E-Mail: support@solvimus.de
Phone: +49 3677 7613065

### 4.14.6 The Log is empty

Please check the filter settings. If no filter is active, entries should always be available for the **Log source** *System log*. If not, this indicates a misconfiguration on system level. This can be resolved by calling the command *solcmd config-partitions* in the SSH console (see Section 6.1.2).

Please check whether the raw data log for the interfaces is active (see **Configuration** tab). Only then the raw data for the **Log source**, e. g. *M-Bus*, will be generated.

If errors could not be eliminated, please contact our customer support:
E-Mail: support@solvimus.de
Phone: +49 3677 7613065

Page 48/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH

# 5 Reading meters via M-Bus

## 5.1 General information

A widely used interface for the automated meter reading is the wired M-Bus (Meter-Bus). This was originally specified in EN 1434-3. It was then moved to a separate standard EN 13757:

- EN 13757-2 Communication systems for meters - Part 2: Wired M-Bus communication
- EN 13757-3 Communication systems for meters - Part 3: Application protocols
- EN 13757-7 Communication systems for meters - Part 7: Transport and security services

Originally developed for heat meters, the M-Bus is now available for all types of consumption meters as well as sensors and actuators. Thus, it is very important for reading out consumption data.

Fundamental features and advantages of the M-Bus are:

- The M-Bus is a digital interface for the electronic meter reading.
- All consumption meters in a building/property can be operated and read via a single cable.
- All consumption meters are individually addressable.
- The readout is protected against transmission errors and is very robust.
- The data is machine-readable and therefore easy to process.
- The data is self-describing.
- High readout rates are possible.
- The M-Bus is manufacturer independent, there is a wide range of devices.

## 5.2 Signalling on the M-Bus

The M-Bus is a single master multiple slave bus. Therefore, a single bus master controls the bus and the data traffic on the bus. Several slaves, i.e. meters, can be connected to the bus.

🛈 A second physical master is not allowed on the M-Bus.

On a physical level, the M-Bus uses voltage and current modulation to transmit data. The master transmits telegrams by modulating the bus voltage, the slave transmits telegrams by modulating the current through the bus. This is shown schematically in the following figure (values of current and voltage may deviate):
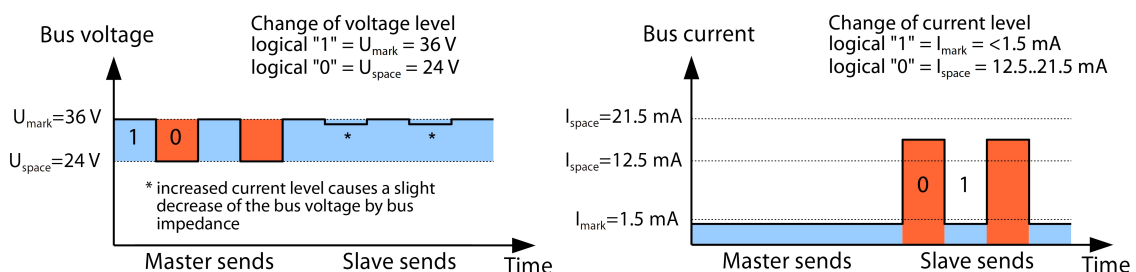


Figure 32: Signalling on the M-Bus

The M-Bus follows the principle of request-response, i. e. the master initiates the communication by a request/command which is then answered/confirmed by the slave. Spontaneous data transmission on the part of the slaves is not allowed.

Certain terms are used in the M-Bus standard. The basics of communication are taken from IEC 60870-5-101. Key terms are explained in the table below:

| Term | Description |
|---|---|
| ACK | ACKnowledge, confirmation of a command, transmitted over the M-Bus as a single character telegram with content 0xE5. |
| Application reset | Reset of the application layer, command to reset the meter to the default state and to reset the meter for consecutive telegrams (multipaging). |
| Broadcast | Broadcast, command or request is sent to all slaves, special addresses 0xFE and 0xFF are used. |
| C field | Command field, code that indicates the direction in which a telegram is exchanged and the meaning of the telegram. |
| Checksum | Check number for checking transmission errors, the checksum the M-Bus uses, results from the addition of the transmitted data (without telegram header, up to checksum). |
| Single character | One of the three telegram formats the M-Bus uses with a length of exactly 1 byte, telegram header and end, consisting of checksum and 0x16, are not present, used on the M-Bus for ACK |
| FCB | Frame Count Bit, bit in the C field, which is alternately set to 1 or 0 in consecutive telegrams, consecutive telegrams can be retrieved when the bit changes in the request. |
| $I_{mark}$ | Transmit current of the slave at logical 1, usually 1 UL. |
| $I_{space}$ | Transmit current of the slave at logical 0, usually 12.5-21.5 mA. |
| Short frame | One of the three telegram formats the M-Bus uses with a length of exactly 5 bytes, is only sent from the master to the slave (e. g. commands and instructions), the telegram header is 0x10 and the telegram ends with checksum and 0x16. |
| Long frame | One of the three telegram formats the M-Bus uses with a variable length, the telegram header consists of 0x68 LL LL 0x68 (LL is the length of the telegram in each case), the telegram ends with checksum and 0x16. |
| Multipaging | M-Bus method of distributing large amounts of data into several logically consecutive telegrams, use of the FCB for sequence control. |
| Primary address | M-Bus Link layer Address, this is used to address the requests/commands, address range 0-250, special addresses 253 (0xFD), 254 (0xFE) and 255 (0xFF). |
| REQ_UD2 | REQuest User Data type 2, request for consumption data, transmitted over the M-Bus by the master as a short frame telegram. |
| RSP_UD | ReSPond User Data, response of the meter to a request for data, transmitted over the M-Bus by the slave as a long frame telegram. |
| Secondary address | Worldwide unique identification number of the meter, consisting of manufacturer code, 8-digit serial number, medium ID and version number. |
| Slave select | Procedure for extending the address space to the secondary address of the meter, use of the SND_UD for selecting the meter via the application layer, then selected meter can be addressed via special address 0xFD. |
| Standard load | Defined idle current that a meter may draw from the M-Bus, according to the standard 1 UL=1.5 mA. |
| SND_NKE | Send Link Reset, initialization command to the slave (reset FCB bit and selection), transmitted by the master as a short frame telegram on the M-Bus. |
| SND_UD | SeND User data, sending data or commands to the meter, transmitted by the master as a long frame telegram on the M-Bus. |
| $U_{mark}$ | Mark voltage, upper voltage of the M-Bus signals at the master, representation of the logical 1, idle state, usually 24-42 V. |
| $U_{space}$ | Space voltage, lower voltage of the M-Bus signals at the master, representation of the logical 0, usually 12-30 V. |
| UL | Unit of standard load (see above) |

Table 18: M-Bus specific terms

## 5.3 Configuration of the interface on the web-based front end

### 5.3.1 M-Bus mode

The parameter **M-Bus mode** in the ***Configuration*** tab activates the M-Bus interface and defines the fundamental functionality. The following modes are available:

- *Disabled*
- *Master*
- *Transparent/TCP*
- *Transparent/UDP*
- *Master & Transparent/TCP*

The *Transparent* modes allow the access to the physics of the M-Bus interface via a TCP or UDP port. The data stream is forwarded from the M-Bus interface to an IP interface (network (LAN) or cellular radio (WAN)).

Page 50/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH

The device then works in a way similar to an Ethernet-M-Bus converter or even to a cellular router with an M-Bus interface. The network port to be used is defined in the parameter **M-Bus transparent port**.

✔ The transparent mode allows direct communication with meters via the M-Bus interface. This requires appropriate M-Bus software on the control system (host system). The device provides the physical connection. This allows to transfer any kind of data with the meter and to use manufacturer specific protocols.

The mode *Master & Transparent/TCP* allows a combination of the transparent transmission and the Master capability of the device. In the absence of a client to a transparent TCP port, the M-Bus master uses the interface and reads out the meters according to the configuration in the mode *Master*. Once a client connects to the TCP port, it gets exclusive access to the interface as in the mode *Transparent/TCP*. A readout of meters or a scan of the M-Bus by the device is not possible as long as a client is connected. A readout fails if configured in this time. Once the client disrupts the connection, the interface is once again run by the M-Bus master, and meters are read out. An inactive connection to the transparent port is closed after 60 seconds in order to rule out a jamming of the M-Bus by open connections. In this mode, a client should assure that the connection is unblocked after usage. As an initiated readout of a meter is first completed upon connection by a client, a larger timeout is recommended for the first communication by the client when establishing the connection ($\geq$5 seconds).

## 5.3.2 Addressing, scanning and scan range

The M-Bus differentiates between primary addressing and secondary addressing. The M-Bus interface allows also mixed addressing. Meters can be searched first using primary addressing, and a subsequent scan can detect meters using secondary addressing.

The primary address is used for access control on link layer level. It is the basis of communication between master and slaves on the M-Bus and is used for communication in every telegram except the single character frame. The secondary address is an extension of the addressing and additionally controls the access on application layer level.

The valid address range for the primary addresses is 0-250, whereby the address *0* is a special case. According to the standard, only unconfigured meters (ex works) are allowed to have it. The address *253* is a special address used for the secondary addressing, the addresses *254* and *255* are used for the broadcast with and without response. The addresses *251* and *252* are reserved.

The secondary address consists of 4 parts. These are the *secondary ID* (an 8-digit decimal number), the *manufacturer ID* (value of 0-65535), the *medium ID* (value of 0-255), and the *version number* (value of 0-255). Thus, the address space includes theoretically $115.19*10^{15}$ unique values.

➡ The *manufacturer ID* can be converted to a manufacturer code maintained by the *DLMS User Association*. An overview can be found here: www.dlms.com/flag-id/flag-id-list

In case of primary addressing, this slave responds whose primary address matches the address in the request. This allows a simple and quick communication.

ⓘ If the primary address is not unique, primary addressing will cause collisions and communication may be disturbed. Several slaves are then responding at the same time.

Secondary addressing, on the other hand, uses a so-called selection (slave select) on the basis of the secondary address. This selection allows addressing of a meter with a matching secondary via the primary address *253*. The non-matching meters are deselected in the same step. Therefore, the process is more complex since a selection with confirmation is required additonally. Communication takes a longer time. However, the address space is much larger. Collisions do not occur, and more than 250 meters can be addressed on one bus system. In addition, commissioning is faster because not every meter has to be configured to a unique primary address.
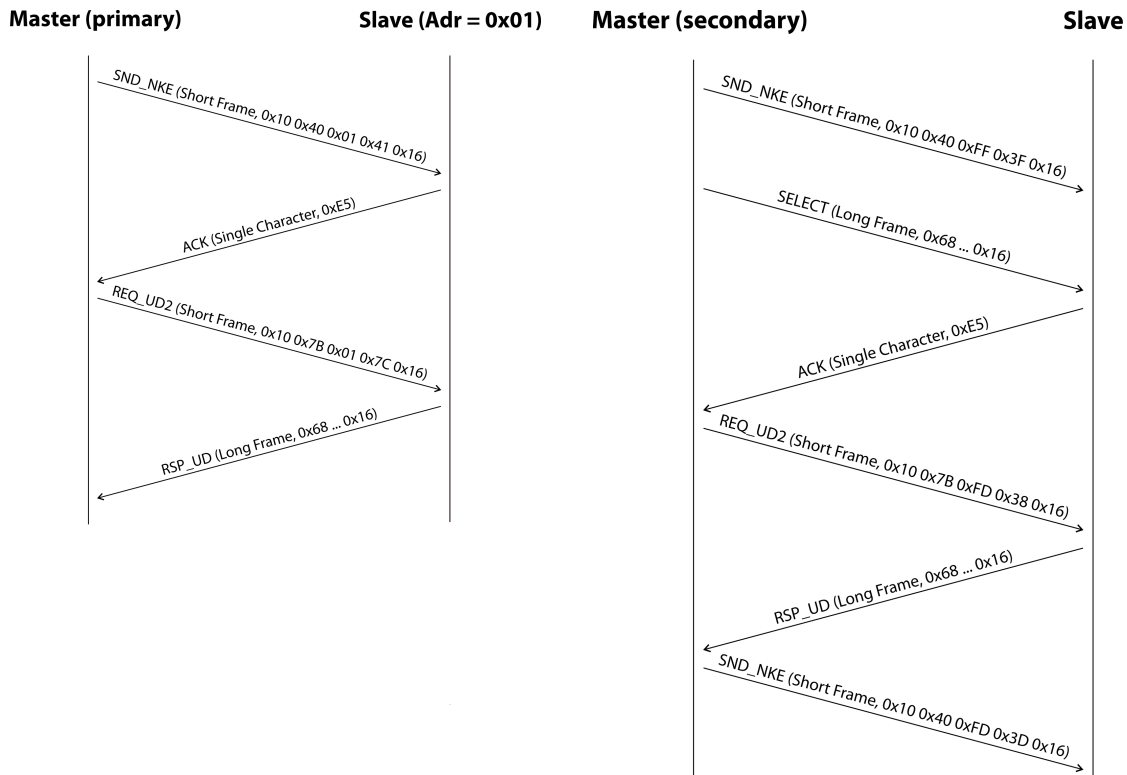
Figure 33: Example of primary and secondary addressing in comparison

Secondary addressing is supporting wildcards. For example, this allows using the 8-digit *secondary ID* for selection only. The other parts are masked with the placeholder 0xFF (255) or 0xFFFF (65535). Individual digits of the *secondary ID* can be masked with 0xF (16) as well.

> ✔ The M-Bus uses the BCD notation for the *secondary ID*. The 8-digit decimal number is encoded by an 8-digit hexadecimal number. Per each digit the characters A-F can be mapped to special features, but only the *F* is used as a placeholder at the respective digit.

The placeholders are the basis of the secondary scan. This divides the secondary address space piece by piece using the placeholders and checks whether there are meters in the respective part. If so, this part is further subdivided until there is at most only one meter per part or further subdivision is not possible. The common procedure here is to mask the *manufacturer ID*, *medium ID* and *version number* and to scan the 8-digit number range of the *secondary ID* only.

The range 00000000-99999999 is divided by sending the selection to *0FFFFFFF*, i. e. selecting all meters with a *0* at the first digit of the *secondary ID*. A request is then sent to the selected meters using the primary address *253*. If no response is received, no meter is in this range. So, the least significant, unmasked digit can then be incremented and the process continues with *1FFFFFFF*. If you get an undisturbed response, there is only one meter in this range. This meter is found here and could be registered. The process will then continue with the next step by incrementing the least significant, unmasked digit. If a disturbed response or collision is received, the process switches to the next, still masked digit and runs it from *0* to *9*. It is difficult to estimate what time a secondary scan will take in advance. There is a variability of the process depending on the meters and the distribution of the *secondary ID* in the address space.

Primary scan, in contrast, is very direct and determinate. Every primary address is requested and depending on a valid answer a meter is then registered or not. Thus, 250 requests are always necessary for a complete scan.

The parameter **Primary start address** and **Primary final address** in the *Configuration* tab limit the primary scan by specifying the start and end. The parameter **Secondary address mask** is used to mask the *secondary ID* for limiting the scan to a certain address range. For example, a mask *33FFFFFF* limits the scan to all meters having a *secondary ID* starting with *33*.

### 5.3.3 M-Bus baud rate

The parameter **M-Bus baud rate** in the *Configuration* tab is used to configure the bit presentation on the M-Bus interface. The baud rate essentially determines the speed of the data transmission.

Page 52/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH

✔ M-Bus usually uses 2400 bps. Other common baud rates are 300 bps and 9600 bps. Many meters detect the baud rate automatically.

✔ The other parameters for the bit presentation on the M-Bus interface are fixed to 8 data bits, even parity and 1 stop bit (8-E-1).

## 5.3.4 M-Bus timeouts

The M-Bus interface comes with three different timeouts: **M-Bus timeout**, **M-Bus idle timeout** as well as **M-Bus full timeout** (in transparent mode **M-Bus idle timeout** only). These can be parameterized in the **Configuration** tab.

The **M-Bus idle timeout** specifies how long the M-Bus interface must be „idle", i. e. no data is sent/received, for detecting the end of a telegram (end of communication). It is mainly used for framing the packets of the M-Bus data stream, i. e. the assignment of incoming data to a logical unit (data packet).

The **M-Bus timeout** specifies how long the device is waiting for a response from the meter. If no data is received within this time after the request, the readout attempt is aborted.

The **M-Bus full timeout** specifies how long the device will accept incoming data. The reception is then aborted and the data is processed. This parameter also terminates reception if the **M-Bus idle timeout** is not reached because data is continuously received (without idle state, e. g. in case of faults).

## 5.3.5 M-Bus request mode

By default, the command REQ_UD2 is send from the master to the meter for reding it out. This is answered by the meter with the RSP_UD, which usually contains the meter data (consumption data).

In addition, the parameter **M-Bus request mode** in the **Configuration** tab can be used to explicitly define the requested data before the actual readout. Devices from solvimus GmbH can send a so-called global readout request to the meter before the actual request. A SND_UD is sent to the meter for this purpose. The user data then consists of only one or two characters. There are two implementations with the same functionality, depending on the manufacturer one or the other is supported:

- User data consisting of 2 Byte: DIF=0x7F, VIF=0x7E → **M-Bus request mode** *Extended 1*
- User data consisting of 1 Byte: DIF=0x7F → **M-Bus request mode** *Extended 2*

✔ This command is usually not necessary, because all meter values are transmitted by default using the normal request.

ⓘ Using this functionality may cause a change in the structure of the meter data.

## 5.3.6 M-Bus reset mode

The M-Bus there uses different variants and applications of a reset. A distinction is made between:

- Link layer reset → SND_NKE
- Application layer reset → Application reset using SND_UD

According to EN 13757, the link layer reset is only used for initializing the communication sequence on the link layer. Therefore, it resets the selection based on the secondary address, deselects the meter, and also resets the FCB mechanism (see Section 5.3.7).

The application layer reset, on the other hand, resets the application in the meter (or its communication application).

The parameter **M-Bus reset mode** in the **Configuration** tab can be used to select the variants and addressing of the resets. The resets are then sent at the beginning of a scan procedure and before each readout of a meter:

- *None*: Neither a link layer reset nor an application layer reset is sent.
- *Standard*: A link layer reset is sent to the broadcast address 0xFF and, in the case of primary addressing, also to the respective primary address.

- *Extended 1*: A link layer reset is explicitly sent to the selection address 0xFD before the link layer resets of the *Standard* mode.
- *Extended 2*: After the link layer reset to the selection address 0xFD, an application layer reset is sent to the broadcast address 0xFF. This is followed by the link layer resets of the *Standard* mode.

### 5.3.7 M-Bus multipaging

If the data of a meter do not fit into a single telegram (maximum 255 bytes user data), there is the possibility to split these data into several logically related, consecutive telegrams. The FCB mechanism according to IEC 60870-5-2 is used by the readout sequence. The solvimus GmbH calls this process „multipaging".

In order to request possibly existing telegrams from the meter, the master has to toggle the FCB with each new request REQ_UD2. The meter then replies with the next telegram. If the master does not toggle the FCB, the meter will always respond with the same telegram again. The REQ_UD2 then alternately have a C field of 0x5B or 0x7B.

The parameter **M-Bus max. multipage** in the ***Configuration*** tab restricts the maximum number of consecutively requested telegrams. Especially in the case of meters having a lot of data (e. g. load profiles, due date records), the readout time can be shortened, and less relevant values are not read out at all.

- ✔ For most applications, it is sufficient to use the first telegram of the telegram sequence.
- ⓘ The M-Bus does not provide a mandatory mechanism to directly access certain telegrams of the sequence. As a rule, the procedure always starts from the first telegram. At least all relevant telegrams have to be requested then.
- ⓘ An „Application reset" send to the meter reset the sequence to the first telegram.

## 5.4 Troubleshooting the M-Bus

### 5.4.1 Physical troubleshooting

In order to determine why meters on the M-Bus do not respond or are not found during the scan, it is recommended to check the M-Bus network physically. It is relatively easy to determine fundamental parameters, e. g. whether the M-Bus is at least correctly wired.

A standard multimeter is sufficient for simple measurements. The most important measurement is the voltage measurement between both M-Bus wires. The voltage measurement shows that:

- the M-Bus-Master correctly supplies the Bus: approx. 30-40 V are present
- the meter is correctly connected to the M-Bus: approx. 30-40 V are present
- the voltage drop is not too high: the voltage at the master is only slightly higher than at the meter
- the telegrams of the master are received at the meter: when master is sending, the value in the display of the multimeter „wobbles"

Another important measurement is the current measurement on the two M-Bus wires. The current measurement shows that:

- the load on the M-Bus is in a valid range: approx. (number of meters)*1.5 mA are flowing
- no external currents are present: current through both lines is identical
- the telegrams of the meter are received at the master: when meter is responding, the value in the display of the multimeter „wobbles"

Page 54/81
UG_EN_MBUS-GEV.pdf
Version: 1.1
Released
Frank Richter, 23 February 2024
© solvimus GmbH

**Voltage measurement:**
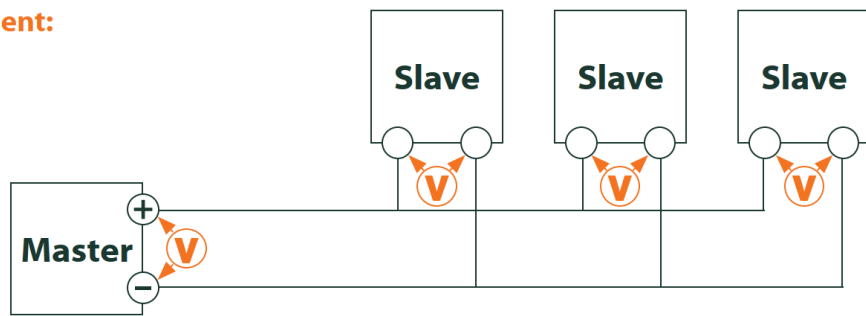


**Current measurement:**
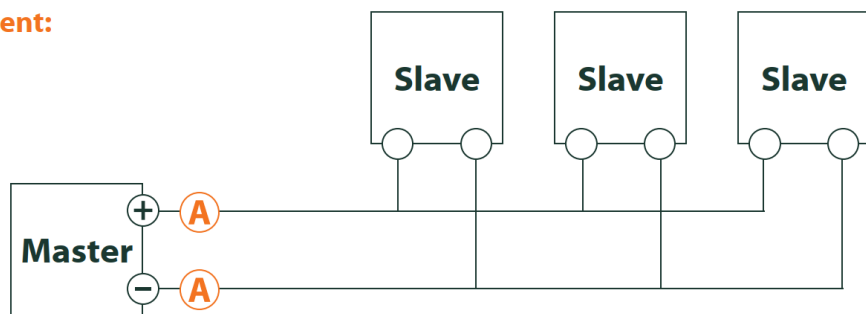


Figure 34: Troubleshooting the M-Bus by measurements with a multimeter

## 5.4.2 M-Bus meters are not found

Check the cables between the device and the meter, and replace faulty cables if necessary. While the device is switched on, please measure the M-Bus voltage (approx. 30-40 V) between the two M-Bus contacts at the device and also at the meter.

Ensure that the M-Bus interface is activated via the parameter **M-Bus mode** on the the web-based front end in the *Configuration* tab and that the scan mode configured therein (secondary or primary) is supported by the meter(s).

Please use an address mask or restrict the range for scanning the M-Bus step by step (e. g. **Primary start address**, **Secondary address mask**).

Additionally, the M-Bus requests can be adapted using the following parameters:

- **M-Bus request mode**
- **M-Bus reset mode**

Please scan again with different M-Bus baud rates (300, 2400 or 9600) or increase the timeouts.

Please remove other meters (if any) to eliminate a possible source of failure.

If another M-Bus meter (possibly of the same type) is available, you can perform another communication test with the other meter to localize the source of failure.

The number of attempts for an M-Bus request can also be increased. The extended configuration of the device in the file *app/chip.ini* (see Section 6.3) offers the parameter **MBUS_MAXRETRY**. This helps to find meters that do not answer every request. The default value here is 3. Please start the scan again.

If the same primary or secondary addresses are present more than once during the scan procedure, collisions can occur. Duplicated addresses are common when using primary addressing, especially in new installations. Therefore we are recommending secondary addressing. In this case collisions can occur as well, but are very unlikely. Due to the default value of the parameter **MBUS_SELECTMASK**=*14* (see Section 6.3), only the 8-digit serial number is searched for during the scan. It can be extended to the manufacturer, medium and version of the meter using other values for **MBUS_SELECTMASK**.

Please activate the raw data log by using **Raw data log** in the *Configuration* tab (see Section 4.6). The communication process can be analyzed very well using this raw data log.

If errors could not be eliminated, please contact our customer support:
Email: support@solvimus.de
Phone: +49 3677 7613065

### 5.4.3 M-Bus meters are found, but do not show any data

Some meters are sending incorrect secondary address or encryption information in the data telegram. As a result, they may not be addressable for readout or may be processed incorrectly.

The parameter **MBUS_SELECTMASK** (see Section 6.3) can be used for masking the invalid parts of the secondary address. The parameter **MBUS_DISABLEDECRYPTION**=*1* (see Section 6.3) can be used to disable the uncommon decryption of M-Bus telegrams if they pretend to be encrypted.

Please restart the scan or start a readout.

If errors could not be eliminated, please contact our customer support:
Email: support@solvimus.de
Phone: +49 3677 7613065

### 5.4.4 The scan takes a long time

The scanning for M-Bus meters can take a long time under certain circumstances. A duration of more than 1 hour is possible, especially when scanning for secondary addresses of meters with consecutive serial numbers.

Please use an address mask or restrict the range for scanning the M-Bus step by step (e. g. **Primary start address**, **Secondary address mask**).

Please decrease the value of the parameter **MBUS_MAXRETRY** in the file *app/chip.ini* (see Section 6.3) or decrease the timeouts.

Use a different scan mode in the *Configuration* tab (see Section 4.6). In particular, the reverse secondary scan *Secondary scan reverse* may help in this case. Please start the scan again.

In the event of interference on the M-Bus, long scan times may also occur. Interference may be processed as a received packet and thus a meter is assumed to be present in each single step.

If errors could not be eliminated, please contact our customer support:
Email: support@solvimus.de
Phone: +49 3677 7613065

### 5.4.5 Device restarts during scan

For safety reasons, the device uses an internal watchdog, which is intended to prevent the device from becoming unreachable. If the scan takes a very long time, this watchdog may cause the device to restart. If the scan takes a long time, it is recommended to increase the value of the parameter **WATCHDOG_SCAN** in the file *app/chip.ini* (see Section 6.3). Please start the scan again.

There may also be heavy collisions on the bus under certain circumstances, e. g. if all meters are responding at the same time. In exceptional cases, these heavy collisions and the associated large increase in current may cause the device to restart. Please use an address mask or restrict the range for scanning the M-Bus step by step (e. g. **Primary start address**, **Secondary address mask**). If necessary, split the M-bus into physical parts and scan the sections one after another.

If errors could not be eliminated, please contact our customer support:
Email: support@solvimus.de
Phone: +49 3677 7613065

Page 56/81
UG_EN_MBUS-GEV.pdf
Version: 1.1
Released
Frank Richter, 23 February 2024
© solvimus GmbH

# 6 Advanced configuration options

## 6.1 Linux operating system

The devices from solvimus GmbH are based on the Linux operating system. This ensures that the devices continuously follow the state of the art and that errors in the software are quickly found and corrected due to a large community. It also ensures a certain basic functionality and security for the user.

The Linux operating system is built using the Yocto/openembedded build environment. All components are included according to the latest version and security patches. The Linux itself is unchanged except a few specific tools and customizations (e. g. solcmd). Corresponding Linux documentation can thus be used directly. For customer-specific projects, additional components provided on the Yocto/openembedded platform can be made available on the target system.

### 6.1.1 User roles and user rights

Linux supports and offers user roles. The operating system internally comes with the user *root* having full access to all operating system functions. In addition, further users with restricted access can be created. Their permissions can be set by groups and names, mostly file access permissions (read, write or execute).

In addition to the user *root*, the devices from solvimus GmbH are coming with the user *admin*. This user has read and write access to the partitions `app` and `ext` and can execute files there. For the operator, *admin* is the user who can completely configure the device.

- ✔ The user *web* is created as the default user for the web interface, but has no access rights to the file system.
- ✔ For reasons of downward compatibility, the user *ftp* is created as the default user for FTP access to the directory `ext/Log`.
- ⓘ The user *root* has no external access to the device. This ensures security, privacy and safety for the operator. Only the user *admin* can grant access to the user *root*.
- ⓘ The password of the user *root* is generated randomly and device-specific during production and stored access-protected in a database.

### 6.1.2 Command line

On the devices from solvimus GmbH, the Linux operating system offers a command line based on *BASH*. It allows the user and also other applications to execute commands via the command line.

The user can access the command line via an SSH console. The Netdiscover tool (see Chapter 3) opens an SSH console using a Putty client.

**Standard commands**

The Linux operating system and the command line *BASH* provide certain built-in standard commands. Examples are:

- *help*: Display list of all integrated commands
- *cd*: Navigation in the directory tree
- *ls*: List directory contents
- *cat*: View file contents
- *cp*: Copying files/directories
- *mv*: Move/rename files/directories
- *rm*: Delete files/directories
- *sync*: Write the data from the RAM buffer to the FLASH memory

- *chmod*: Adjust access rights
- *grep*: Search for text content
- *echo*: Output text
- *date*: Display system date and time
- *ps*: List all running processes
- *tail*: Display last lines of a file
- *netstat*: Query the status of the network interfaces
- *ping*: Network connectivity test
- *nslookup*: Display of the DNS configuration
- */sbin/ifconfig*: Overview of the network interfaces

Further commands are provided by programmes:

- *tcpdump*: Recording network traffic
- *openssl*: Using encryption, certificates and PKI
- *curl*: Retrieval and transmission of files via HTTP, FTP or SMTP/e-mail
- *socat*: Connecting two interfaces
- *vi*: Editing files
- *xsltproc*: Executing XSL transformations

**solcmd command interpreter**

Due to the system access rights for users, solvimus GmbH adds a command interpreter *solcmd*. It offers special application functions via the command line. The interpreter can be called with various parameters and thus provides access to the application and allows controlling it.

The following parameters are supported:

- *format-partition-app*: Format the configuration partition `app`
- *format-partition-ext*: Format the logging partition `ext`
- *config-partitions*: Reset the access rights to the partitions
- *config-users*: Activate changed user settings
- *config-hostname*: Activate changed device name
- *config-timezone*: Activate changed time zone settings
- *restart-eth0*: Restart the Ethernet interface
- *restart-wifi*: Restart the WIFI interface (only if WIFI is available)
- *filter-vlan*: VLAN filter for network interface (only if switch is integrated)
- *start-ppp0*: Establish the PPP dial-in connection (mobile network)
- *stop-ppp0*: Terminate the PPP dial-in connection (mobile network)
- *start-vpn*: Establish a VPN connection (OpenVPN)
- *stop-vpn*: Terminate a VPN connection (OpenVPN)
- *manual-vpn*: Establish a VPN connection (OpenVPN) in the foreground, e. g. for entering the password manually
- *restart-server*: Restart the server services
- *regenerate-server-keys*: Re-create the keys for secured server services
- *start-solapp*: Start the main application
- *stop-solapp*: Stop the main application
- *start-transparent-tty*: Activate transparent data forwarding of a serial interface to an Ethernet port
- *stop-transparent-tty*: Deactivate transparent data forwarding of a serial interface to an Ethernet port
- *start-virtual-tty*: Activate a virtual interface via an Ethernet port

- *stop-virtual-tty*: Deactivate a virtual interface via an Ethernet port
- *update-rtc*: Write the system time to the buffered real-time clock
- *factory-reset*: Reset the device to factory settings
- *update-system*: Perform a system update
- *reboot-system*: Restart the system
- *help*: Command overview with explanation and examples

## 6.2 Update

The firmware can be updated manually or conveniently via the web interface (see Section 4.12).

For a manual update, access via SSH is necessary. In preparation, the easiest way to provide the update file on the system is to upload it via SFTP. The tools are provided by the Netdiscover tool (see Chapter 3).

First, the appropriate and signed update file `*.enc` has to be uploaded via SFTP into the directory `ext/Upd` (see Section 3.5). This is restricted to the user *admin*.

After uploading the file, the user has to log in as *admin* via SSH (see Section 3.6). In the command line (see Section 6.1.2), the command *solcmd update-system* has to be executed then. After completion, a reboot is necessary. This is triggered by the command *solcmd reboot-system*.

## 6.3 Configuration file chip.ini

The file `app/chip.ini` contains the general system parameters and is therefore the central configuration file. The parameters are grouped into different sections. If the parameters are not configured in `chip.ini`, the default values are used.

- ℹ️ The device needs to be rebooted after changing the file `chip.ini` manually for taking effect. Reboot can be triggered via the web-based front end using the button **Reboot system** in the **Service** tab or via the command line.
- ℹ️ Manual changes are permanently stored on the flash not instantly, but after a few minutes. As a result, changes are possibly lost if the device is rebooted by switching the power supply off and on.
- ℹ️ A range „0, 1" without further explication means: 0 = inactive/no, and 1 = active/yes.
- ✔️ The file `chip.ini` can be transferred to other devices via FTPS. Some settings like the network configuration (e. g. different IP address) needs to be taken into account.

| Parameter | Description | Range | Standard |
|---|---|---|---|
| **Group [IP]** | | | |
| ADDRESS | IP address of the device | 0.0.0.0-255.255.255.255 | 192.168.1.101 (explicit) |
| DHCP | Activation of the DHCP client | 0, 1 | 0 (explicit) |
| DHCP_HOSTNAME | Host name to log on to the DHCP server | Text, max. 255 characters, %SERIAL%: MAC address of the device | Name of the device from group [DEVICE] |
| GATEWAY | IP address of the gateway | 0.0.0.0-255.255.255.255 | 192.168.1.254 (explicit) |
| NETMASK | Subnet mask of the device | 0.0.0.0-255.255.255.255 | 255.255.255.0 (explicit) |
| **Group [DEVICE]** | | | |
| NAME | Name of the device in the tool Netdiscover | Text, max. 50 characters | *Product name* (explicit) |
| TIMEZONE | Time zone of the device | Text, max. 255 characters | Universal, corresponds to GMT |
| **Group [DNS]** | | | |
| NAME_SERVER1 | IP address of the primary DNS server, IP or host name | Text, max. 255 characters | Not set |
| NAME_SERVER2 | IP address of the secondary DNS server, IP or host name | Text, max. 255 characters | Not set |
| **Group [VPN]** | | | |
| CONFIGFILE | Path to the OpenVPN configuration file | Text, max. 255 characters | vpn/config.ovpn |
| ENABLE | Activation of the OpenVPN client | 0, 1 | 0 |

*Continued on next page*

Table 19 – *Continued from previous page*

| Parameter | Description | Range | Standard |
|---|---|---|---|
| **Group [WEB]** | | | |
| CERT_COMMON_NAME | The fully qualified domain name | Text, max. 255 characters | Not set |
| CERT_COUNTRY | Country code | Text, max. 255 characters | Not set |
| CERT_LOCATION | Location/city | Text, max. 255 characters | Not set |
| CERT_ORGANISATION | Legal name of the organisation | Text, max. 255 characters | Not set |
| CERT_ORGANISATION_UNIT | Unit/department | Text, max. 255 characters | Not set |
| CERT_STATE | State or region | Text, max. 255 characters | Not set |
| HTTP_ENABLE | Activation of the HTTP server | 0, 1 | 1 |
| HTTPS_ENABLE | Activation of the HTTPS server | 0, 1 | 1 |
| HTTP_PORT | Network port of the HTTP server | 0-65535 | 80 |
| HTTPS_PORT | Network port of the HTTPS server | 0-65535 | 443 |
| **Group [FTP]** | | | |
| CERT_COMMON_NAME | The fully qualified domain name | Text, max. 255 characters | Not set |
| CERT_COUNTRY | Country code | Text, max. 255 characters | Not set |
| CERT_LOCATION | Location/city | Text, max. 255 characters | Not set |
| CERT_ORGANISATION | Legal name of the organisation | Text, max. 255 characters | Not set |
| CERT_ORGANISATION_UNIT | Unit/department | Text, max. 255 characters | Not set |
| CERT_STATE | State or region | Text, max. 255 characters | Not set |
| ENABLE | Activation of the FTP server | 0, 1 | 1 |
| **Group [SSH]** | | | |
| ENABLE | Activation of the SSH server | 0, 1 | 1 |
| **Group [UDPCFG]** | | | |
| ENABLE | Activation of the UDP-based search and configuration protocol | 0, 1 | 1 |
| IPCFG_PASSWORD | Password for the modification of the IP address via the UDP configuration protocol | Text, max. 255 characters | Not set |
| **Group [SOLVIMUS]** | | | |
| BACNET_BBMD | IP of the BACnet BBMD (BACnet Broadcast Management Device) | Text, max. 255 characters | Not set |
| BACNET_BROADCAST | BACnet Broadcast IP address (system configuration will be used if not set) | Text, max. 255 characters | Not set |
| BACNET_CONFIGURE NETWORK | Activation of a BACnet-specific network configuration (additional IP address) | 0, 1 | 0 |
| BACNET_DEVICEID | BACnet device ID | 1-4294967295 | 1 |
| BACNET_DEVICENAME | BACnet device name | Text, max. 255 characters | Not set |
| BACNET_ENABLE | Activation of the BACnet communication | 0, 1 | 0 |
| BACNET_IP | BACnet IP (system configuration will be used if not set) | Text, max. 255 characters | Not set |
| BACNET_LOCATION | BACnet location information | Text, max. 255 characters | metering |
| BACNET_NETMASK | BACnet Network mask (system configuration will be used if not set) | Text, max. 255 characters | Not set |
| BACNET_PORT | BACnet network port | 0-65535 | 47808 |
| DLDERS_ADDRESS DISABLE | DLDE request with meter serial number (=0) respectively wildcard request (=1). In the latter case only 1 meter is permitted. | 0, 1 | 0 |
| DLDERS_BAUDRATE | Baud rate for the serial DLDE communication | 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800 | 9600 |

*Continued on next page*

Page 60/81
UG_EN_MBUS-GEV.pdf
Version: 1.1
Released
Frank Richter, 23 February 2024
© solvimus GmbH

Table 19 – *Continued from previous page*

| Parameter | Description | Range | Standard |
|---|---|---|---|
| DLDERS_DATABITS | Data bits for the serial DLDE communication | 7, 8 | 7 |
| DLDERS_DEVPATH | Linux path for the serial DLDE communication | Text, max. 255 characters | Not set |
| DLDERS_ENABLE | Activation of the serial DLDE interface | 0, 1 | 0 |
| DLDERS_FIRSTTIMEOUT | Request mode: timeout for initial reception of data from meter. Push mode: time without registration of data (Wait idle, in ms) | 0-65535 | 3000 |
| DLDERS_FIXEDLAYOUT | | 0, 1 | 0 |
| DLDERS_ FLOWCONTROL | Handshake for the serial DLDE communication: 0: none, 1: XON/XOFF when sending, 2: RTS/CTS, 8: XON/XOFF when receiving, 9: XON/XOFF when sending and receiving | 0, 1, 2, 8, 9 | 0 |
| DLDERS_FULLTIMEOUT | Maximum timeout for reading a meter (in ms) | 0-65535 | 30000 |
| DLDERS_IDLETIMEOUT | Idle time for detection of the end of communication (in ms) | 0-65535 | 100 |
| DLDERS_ LOADPROFILE_ MAXRDAYS | | 0-65535 | 366 |
| DLDERS_ LOADPROFILE_ SKIPINVALIDENTRY | | 0, 1 | 0 |
| DLDERS_MODE | Communication mode for the serial DLDE interface | REQUEST, REQUEST_ECHO, PUSH | REQUEST_ECHO |
| DLDERS_PARITY | DLDE parity: 0: none, 1: odd, 2: even, 3: mark, 4: space | 0-4 | 2 |
| DLDERS_RAWLOG ENABLE | Activation of the raw data logging to the directory *ext/* | 0, 1 | 0 |
| DLDERS_RS485ENABLE | Activation of the RS-485 interface for the DLDE communication | 0, 1 | 1 |
| DLDERS_SMLENABLE | Activation of processing SML protocol data | 0, 1 | 0 |
| DLDERS_STOPBITS | Stop bits for the serial DLDE interface | 1, 2 | 1 |
| DLDERS_TRANSPARENT | Activation of the transparent transmission of the serial DLDE interface to a network port: NONE: transmission deactivated, TCP: transmission of a TCP port, UDP: transmission to a UDP port | NONE, TCP, UDP | NONE |
| DLDERS_TRANSPARENT PORT | Network port for the transparent transmission via TCP or UDP | 0-65535 | 0 |
| FASTRESCAN_TIME | Cycle time for updating the temporary meter list of received wM-Bus meters (in s) | 1-4294967295 | 60 |
| I2C_DEBUGOUT | Activation of raw data output for the internal I2C communication in the system log | 0, 1 | 0 |
| MBUS_ALLOWINSECURE | Deactivates the authentication check when decrypting | 0, 1 | 0 |
| MBUS_BAUDRATE | Baud rate for the M-Bus communication | 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800 | 2400 |
| MBUS_DATABITS | Data bits for the M-Bus communication | 7, 8 | 8 |
| MBUS_DEVPATH | Linux path for the M-Bus interface | Text, max. 255 characters | Not set |
| MBUS_DISABLE DECRYPTION | Deactivation of decrypting the M-Bus packets (status field) | 0, 1 | 0 |
| MBUS_ENABLE | Activation of the M-Bus interface | 0, 1 | 1 |

*Continued on next page*

Table 19 – *Continued from previous page*

| Parameter | Description | Range | Standard |
|---|---|---|---|
| MBUS_FIRST FCBBIT_NEG | Begins reading the M-Bus meters with a specific FCB-bit value: <br> 0: first FCB-bit set, <br> 1: first FCB-bit not set | 0, 1 | 0 |
| MBUS_FIXEDLAYOUT | | 0, 1 | 0 |
| MBUS_FLOWCONTROL | Handshake for the M-Bus communication: <br> 0: none, <br> 1: XON/XOFF when sending, <br> 2: RTS/CTS, <br> 8: XON/XOFF when receiving, <br> 9: XON/XOFF when sending and receiving | 0, 1, 2, 8, 9 | 0 |
| MBUS_FORCE | Compatibility mode for reading of faulty M-Bus meters, emulates correct ACK | 0-2 | 0 |
| MBUS_FREEZE STORAGENUM | Storage number for Freeze meter data | 0-4294967295 | 0 |
| MBUS_FULLTIMEOUT | Maximum timeout for reading a meter (in ms) | 0-65535 | 10000 |
| MBUS_IDLETIMEOUT | Idle time for detection of the end of communication (in ms) | 0-65535 | 100 |
| MBUS_IGNORECRCFIELD | Compatibility mode for reading faulty M-Bus meters, disregards the CRC field | 0, 1 | 0 |
| MBUS_IGNORELENGTH FIELD | Compatibility mode for reading faulty M-Bus meters, disregards the length field | 0, 1 | 0 |
| MBUS_LOADPROFILE MANUFACTURER | Manufacturer code for identification of load profile meters, according to M-Bus standard: „EMH"=(0xA8 0x15) → 0x15A8=5544 | 0-65535 | 5544 |
| MBUS_LOADPROFILE MAXCOUNT | Number of load profile entries initially requested by the meter | 1-65535 | 65535 |
| MBUS_LOADPROFILE MODE | Activation of load profile readings for electricity meters via M-Bus | DISABLED, DIZH, DIZG | DISABLED |
| MBUS_MAXMULTIPAGE | Limits the number of Multipage requests | 0-255 | 3 |
| MBUS_MAXPRIMARY ADDRESS | Upper address for the M-Bus primary search | 0-250 | 250 |
| MBUS_MAXRETRY | Retries for an M-Bus or Multipage request | 0-255 | 3 |
| MBUS_MINPRIMARY ADDRESS | Lower address for the M-Bus primary search | 0-250 | 0 |
| MBUS_NOADDRESS VERIFY | Deactivation of the address verification in primary addressing | 0, 1 | 0 |
| MBUS_PARITY | Parity of the M-Bus communication: <br> 0: none, <br> 1: odd, <br> 2: even, <br> 3: mark, <br> 4: space | 0-4 | 2 |
| MBUS_RAWLOGENABLE | Activation of the raw data logging to the directory *ext/* | 0, 1 | 0 |
| MBUS_REQUESTMODE | Request mode | ALL, EXT, ONLY, FREEZE | ONLY |
| MBUS_RESETMODE | Reset Modes: <br> 0: NKE after Select, <br> 1: NKE before Select <br> 2: No NKE <br> 3: NKE at 0xFD and NKE at 0xFF before the communication <br> 4: NKE at 0xFD, application reset at 0xFF and NKE at 0xFF before the communication | 0-4 | 0 |
| MBUS_RS485ENABLE | Activation of the RS-485 interface for the M-Bus communication | 0, 1 | 0 |

*Continued on next page*

Table 19 – *Continued from previous page*

| Parameter | Description | Range | Standard |
|---|---|---|---|
| MBUS_SCANMODE | Search algorithm for the M-Bus | PRIMARYSCAN, SECONDARYSCAN, SECONDARYSCAN ALLOC, SECONDARYSCAN REVERSE, SECONDARYSCAN ALLOCREVERSE | SECONDARYSCAN |
| MBUS_SECMASK MANUFACTURER | Predefined manufacturer ID for the secondary search | Precisely 4 characters, each 0-9/A-F | 0xFFFF |
| MBUS_SECMASK MEDIUM | Predefined medium ID for the secondary search | Precisely 2 characters, each 0-9/A-F | 0xFF |
| MBUS_SECMASKSERIAL | Secondary search for the meter serial number | Precisely 8 characters, each 0-9/A-F | 0xFFFFFFFF |
| MBUS_SECMASK VERSION | Predefined version number for the secondary search | Precisely 2 characters, each 0-9/A-F | 0xFF |
| MBUS_SELECTMASK | Ignoring of selected ranges, for these placeholders are used (setting via bit mask): +1: serial number +2: manufacturer +4: version field +8: medium | 0-15 | 14 |
| MBUS_SMLENABLE | Activation of processing SML protocol data | 0, 1 | 0 |
| MBUS_SOCPAGESELECT ENABLE | Activates Pageing according to the specification of the company Socomec | 0, 1 | 0 |
| MBUS_SOC MANUFACTURER | Manufacturer code for identification of meters with Socomec pageing, according to M-Bus standard: „SOC"=(0xE3 0x4D) → 0x4DE3=19939 | 0-65535 | 19939 |
| MBUS_SPXMETER CONVERT | Activation of manufacturer-specific decoding (manufacturer code SPX) | 0, 1 | 0 |
| MBUS_STOPBITS | Stop bits for the M-Bus communication | 1, 2 | 1 |
| MBUS_TIMEOUT | Timeout till first data are received from the meter (in ms) | 0-65535 | 2000 |
| MBUS_TRANSPARENT | Activation of the transparent transmission of the M-Bus interface to a network port or an M-Bus slave interface: NONE: transmission deactivated, MBUS: Master TCP: transmission to a TCP port, UDP: transmission to a UDP port, TCP_ONDEMAND: Master & Transparent/TCP | NONE, MASTER, TCP, UDP, TCP_ONDEMAND | NONE |
| MBUS_TRANSPARENT PORT | Network port for the transparent transmission via TCP or UDP | 0-65535 | 0 |
| MBUS_WAKEUPENABLE | Activation of the specific wakeup requests | 0, 1 | 0 |
| MBUSSLV_BAUDRATE | Baud rate for the M-Bus slave communication | 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800 | 2400 |
| MBUSSLV_DATABITS | Data bits for the M-Bus slave communication | 7, 8 | 8 |
| MBUSSLV_DEBUGOUT | Activation of the raw data output for the M-Bus slave communication in the system log | 0, 1 | 0 |
| MBUSSLV_DEVPATH | Linux path for the M-Bus slave interface | Text, max. 255 characters | Not set |

*Continued on next page*

Table 19 – *Continued from previous page*

| Parameter | Description | Range | Standard |
|---|---|---|---|
| MBUSSLV_ FLOWCONTROL | Handshake for the M-Bus slave communication:<br>0: none,<br>1: XON/XOFF when sending,<br>2: RTS/CTS,<br>8: XON/XOFF when receiving,<br>9: XON/XOFF when sending and receiving | 0, 1, 2, 8, 9 | 0 |
| MBUSSLV_ FULLTIMEOUT | Maximum timeout for the request of a meter (in ms) | 0-65535 | 10000 |
| MBUSSLV_ IDLETIMEOUT | Idle time for detection of the end of communication (in ms) | 0-65535 | 100 |
| MBUSSLV_PARITY | Parity for the M-Bus slave communication:<br>0: none,<br>1: odd,<br>2: even,<br>3: mark,<br>4: space | 0-4 | 2 |
| MBUSSLV_RS485ENABLE | Activation of the RS-485 interface for the M-Bus slave communication | 0, 1 | 0 |
| MBUSSLV_STOPBITS | Stop bits for the M-Bus slave communication | 1, 2 | 1 |
| MBUSSLVMETER_MODE | Activation of the M-Bus slave interface:<br>DEFAULT: product-specific activated,<br>NONE: deactivated,<br>TCP: activation via TCP port,<br>UDP: activation via UDP port,<br>MBUS: activation via the M-Bus slave interface | DEFAULT, NONE, TCP, UDP, MBUS | DEFAULT |
| MBUSSLVMETER_PORT | Network port for access to the M-Bus slave interface via TCP or UDP | 0-65535 | 5040 |
| MBUSSLVMETER_ WMBUSALLOW ENCRYPTED | Activation of the transfer of encrypted wM-Bus meters via the M-Bus slave interface | 0, 1 | 0 |
| MBUSSLVMETER_ WMBUSALLOW EXTENDEDHEADER | Activation of the transfer of specific wM-Bus header data (e. g. AFL/ELL) via the M-Bus slave interface | 0, 1 | 0 |
| MBUSSLVMETER_ WMBUSALLOWOTHER | Activation of the transfer in spite of unknown wM-Bus header data via the M-Bus slave interface | 0, 1 | 0 |
| MBUSSLV2METER_ MODE | Activation of the second M-Bus slave interface:<br>NONE: deactivated,<br>TCP: activation via a TCP port,<br>UDP: activation via a UDP port | NONE, TCP, UDP | NONE |
| MBUSSLV2METER_PORT | Network port for access to the second M-Bus slave interface via TCP or UDP | 0-65535 | 5050 |
| MBUSSLV2METER_ WMBUSALLOW ENCRYPTED | Activation of the transfer of encrypted wM-Bus meters via the second M-Bus slave interface | 0, 1 | 0 |
| MBUSSLV2METER_ WMBUSALLOW EXTENDEDHEADER | Activation of the transfer of specific wM-Bus header data (e. g. AFL/ELL) via the second M-Bus slave interface | 0, 1 | 0 |
| MBUSSLV2METER_ WMBUSALLOWOTHER | Activation of the transfer in spite of unknown wM-Bus header data via the second M-Bus slave interface | 0, 1 | 0 |
| METER_ADJUST TIMESTAMPS | | | 0 |
| METER_CYCLEMODE | | | SECOND |
| METER_CYCLE TIMESTAMP | | | Not set |
| METER_DELAY | Delay for reading of meter data according to the configured reading cycle (in s) | 0-4294967295 | 0 |

*Continued on next page*

Table 19 – *Continued from previous page*

| Parameter | Description | Range | Standard |
|---|---|---|---|
| METER_PRESENT VALUESONLY | | | 0 |
| METER_MAXALLVALUE COUNT | Limitation of total meter data (0: no limitation) | 0-65535 | 0 |
| METER_MAXDEVICE COUNT | Limitation of the number of meters (0: no limitation) | 0-65535 | 500 |
| METER_MAXVALUE COUNT | Limitation of meter values per meter (0: no limitation) | 0-65535 | 25 |
| METER_OBISGEN | Automatic generation of OBIS codes for meter values from DIF/VIF codes when creating M-Bus and wM-Bus meters 0: off, 1: on | 0, 1 | 0 |
| METER_RETRYDIVIDER | Reduces the quantity of values read and used for reporting. Only values every METER_RETRYDIVIDER are retained for reporting. All read values are used for visualisation and for other interfaces (Modbus resp. BACnet). | 0-65535 | 0 |
| METER_STAT_CONFIG | Path to the meter configuration file | Text, max. 255 characters | app/device_handle.cfg |
| METER_TIME | Cycle time for reading meters (unit according to METER_CYCLEMODE), caution: with small cycle times and a large quantity of meters, significant log files can be created | 1-4294967295 | 900 |
| METER_VIFSTRINGMODE | Placement of the VIF string in the data flow: 0: VIF string after last VIFE, 1: VIF string immediately after VIF string identification | 0, 1 | 1 |
| METERSYSTEM_ENABLE | Activation of the system meter function | 0, 1 | 1 |
| METERSYSTEM_SCRIPT TIMEOUT | Timeout after whose expiration the system meter scripts are aborted (in s) | 0-65535 | 0 |
| MODBUS_ADDRESS | Primary Modbus address resp. Unit identifier | 0-255 | 0 |
| MODBUS_APPLICATION | Application information within the device identification | Text, max. 255 characters | Modbus TCP Gateway |
| MODBUS_BAUDRATE | Baud rate for the serial Modbus communication (RTU) | 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800 | 19200 |
| MODBUS_CONNECTION TIMEOUT | Timeout of the Modbus TCP connection (in s) | 0-65535 | 60 |
| MODBUS_DATABITS | Data bits for the serial Modbus communication (RTU) | 7, 8 | 8 |
| MODBUS_DEBUGOUT | Activation of raw data output for the Modbus communication in the system log | 0, 1 | 0 |
| MODBUS_DEVPATH | Linux path for the serial Modbus interface | Text, max. 255 characters | Not set |
| MODBUS_DISCONNECT TIMEOUT | Timeout after whose expiration inactive Modbus TCP connections are aborted (in s) | 0-1000 | 60 |
| MODBUS_ENABLE | Activation of the Modbus slaves | 0, 1 | 0 |
| MODBUS_FLOWCONTROL | Handshake for the serial Modbus communication: 0: none, 1: XON/XOFF when sending, 2: RTS/CTS, 8: XON/XOFF when receiving, 9: XON/XOFF when sending and receiving | 0, 1, 2, 8, 9 | 0 |
| MODBUS_IP | | | Not set |
| MODBUS_MAXCONNECTIONS | Maximum number of parallel Modbus TCP connections | 0-80 | 5 |
| MODBUS_MODE | | Serial, TCP, UDP | TCP |

*Continued on next page*

Table 19 – *Continued from previous page*

| Parameter | Description | Range | Standard |
|---|---|---|---|
| MODBUS_MODEL | Device information within the device identification | Text, max. 255 characters | Standard |
| MODBUS_NWPORT | Network port of the Modbus TCP slaves | 0-65535 | 502 |
| MODBUS_PARITY | Parity of the serial Modbus communication:<br>0: none,<br>1: odd,<br>2: even,<br>3: mark,<br>4: space | 0-4 | 0 |
| MODBUS_PRODUCT CODE | Device code for the Modbus function „Read Device Identification" | Text | A code defined by solvimus GmbH and dependent on the device is returned. |
| MODBUS_RS485ENABLE | Activation of the RS-485 interface for the serial Modbus communication (RTU) | 0, 1 | 0 |
| MODBUS_SPAN | | | 1 |
| MODBUS_STOPBITS | Stop bits for the serial Modbus communication (RTU) | 1, 2 | 1 |
| MODBUS_VENDOR | Manufacturer information within the device identification | Text, max. 255 characters | solvimus GmbH |
| MODBUS_VENDORURL | Website information on manufacturer within the device identification | Text, max. 255 characters | www.solvimus.de |
| MODBUS_VERSION | Version of the firmware indicated by Modbus within the device identification. If not set explicitly, it corresponds to the software version on the configuration page. | Text, max. 255 characters | - |
| MODBUS_WRITEACCESS | | | READONLY |
| MODBUSMETER_ PROTOCOLVERSION | Protocol version of the Modbus meter data:<br>Bit 0: 2 registers per value (only floating point value),<br>Bit 1: Multislave activated,<br>Bit 2: Word-Swapping of 32-Bit floating point values,<br>Bit 3: Dummy mode activated | 0-16 | 0 |
| MUC_CONFIG_VER | Version of the configuration, corresponding to the firmware version that it had saved. Set exclusively by the application. | 0-65535 | - |
| MUC_ FORCESTOREREADOUT | Database mode to „Store meter values" (see Table 10)<br>0: automatic<br>1: on | 0, 1 | 0 |
| MUC_LOG | Sets the level of system output via system log | DEFAULT,<br>NONE,<br>ERRORONLY,<br>ALL | DEFAULT |
| MUC_LOGCYCLE DIVIDER | | | 1 |
| MUC_METER DESCRIPTION_ ENABLEFLAGS | Enable Flags for representing the description on the website:<br>Bit 0: Description<br>Bit 1: Storage number, tariff, value type<br>Bit 2: DIF/VIF raw data<br>Bit 3: All raw data of the data value entry | 0 - 16 | 1 |
| MUC_PASSMUC_ ENCMODE | Activation of the encryption of the passwords in the configuration files:<br>0: no encryption,<br>1: encryption without MAC,<br>2: encryption with MAC | 0, 1, 2 | 0 |
| MUC_REPORT FATALREBOOTTIMEOUT | | | 0 |
| MUC_REPORT SCRIPTABORTTIMEOUT | | | 30 |

*Continued on next page*

Page 66/81

UG_EN_MBUS-GEV.pdf

Version: 1.1

Released

Frank Richter, 23 February 2024

© solvimus GmbH

Table 19 – *Continued from previous page*

| Parameter | Description | Range | Standard |
|---|---|---|---|
| MUC_SCALEVALUES | Scaled values within the CSV and XML log data | 0, 1 | 0 |
| MUC_SETDEVICES | Activation of setting the meter values. The setting of meter values must be supported by the meters. INTERNAL: S0 and digital outputs of the system meter, INTERNALORDIGTALOUT: S0 and digital outputs, ALL: all meter values, NONE: no meter values | INTERNAL, INTERNALORDIGTAL-OUT, ALL, NONE | INTERNAL |
| MUC_SETDEVICETIME | | | 0 |
| MUC_SHOWDATAFRAME | Explicit listing of the raw data frame as meter value, for Multipage meters one entry is added per frame | 0, 1 | 0 |
| MUC_SHOWMETER STATUSBYTE | Explicit listing of the status byte of the meter (M-Bus and wM-Bus) as meter value | 0, 1 | 0 |
| MUC_SHOWTIMESTAMP ENTRIES | Explicit representation of the timestamps of a meter | 0, 1 | 0 |
| MUC_SHOWVENDOR RAWDATA | Explicit listing of manufacturer-dependent data as meter value | 0, 1 | 0 |
| MUC_SHOWVENDOR RAWDATAWEB | Representation of binary data on the website (manufacturer-dependent resp. data container) | 0, 1 | 0 |
| MUC_SHOWWMBUS RSSIVALUE | | | 0 |
| MUC_TRIMVALUES | | | 0 |
| MUC_USE_FREEZE | Activation of the Freeze command for reading meters | 0, 1 | 0 |
| SHOW_KEYS | Show decrypted data on the website | 0, 1 | 1 |
| SNTP_ENABLE | Activation of the reference via SNTP server | 0, 1 | 1 |
| SNTP_REQTIMEOUT | Timeout for a SNTP request (in ms) | 1-65535 | 15000 |
| SNTP_RETRY | Number of retries of a SNTP request | 0-255 | 2 |
| SNTP_TIMEOUT | Timeout for a renewed SNTP time query (explicit, in s) | 1-4294967295 | 86400 |
| SNTPIP | Address of the time server (SNTP) | Text, max. 255 characters | pool.ntp.org |
| SNULL_ENABLE | Activation of the S0 interface | 0, 1 | 0 |
| SNULL_MODE | Counting mode for S0 | RELATIVE, ABSOLUTE | RELATIVE |
| WAN_APN | Access point for WAN | Text, max. 255 characters | Not set |
| WAN_AUTH | Authentication procedure for accessing WAN | NONE, PAP, CHAP | CHAP |
| WAN_BAUDRATE | Baud rate for WAN communication | 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800 | 115200 |
| WAN_DATABITS | Data bits for the WAN communication | 7, 8 | 8 |
| WAN_DEBUGOUT | Activation of raw data output for the WAN communication in the system log 0: off (default), 1: display of the AT communication and of the power cycles, 2: as 1 and additional state requests at the modem like e. g. SIM card settings for preferred providers, 3: as 2 and additional Raw binary communication data and parsed replies | 0, 1, 2, 3 | 0 |
| WAN_DEVPATH | Linux path for the WAN interface | Text, max. 255 characters | Not set |

*Continued on next page*

Table 19 – *Continued from previous page*

| Parameter | Description | Range | Standard |
|---|---|---|---|
| WAN_ENABLE | Activation of the WAN communication (mobile radio) | 0, 1 | 0 |
| WAN_FLOWCONTROL | Handshake for the WAN communication:<br>0: none,<br>1: XON/XOFF when sending,<br>2: RTS/CTS,<br>8: XON/XOFF when receiving,<br>9: XON/XOFF when sending and receiving | 0, 1, 2, 8, 9 | 0 |
| WAN_FULLTIMEOUT | | | 0 |
| WAN_IDLETIMEOUT | | | 0 |
| WAN_MAXRETRY | Number of retries for establishing the WAN connection (0: no limit) | 0-255 | 0 |
| WAN_OLDBAUDRATE | Baud rate for the WAN communication, affects only older devices (0: inactive) | 0, 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800 | 0 |
| WAN_PARITY | Parity of the WAN communication:<br>0: none,<br>1: odd,<br>2: even,<br>3: mark,<br>4: space | 0-4 | 0 |
| WAN_PASSWORD | Password to access WAN | Text, max. 255 characters | Not set |
| WAN_PIN | PIN for the SIM card | Text, max. 255 characters | Not set |
| WAN_PROVIDER | | | Not set |
| WAN_PUK | PUK for the SIM card | Text, max. 255 characters | Not set |
| WAN_RADIOACCESS TECHNOLOGY | Manuel selection of Radio Access Technology:<br>0: default of the modem,<br>1: GSM only (MUC 3G, MUC 4G),<br>2: UMTS only (MUC 3G, MUC 4G rev. 3),<br>3: GSM first (MUC 3G),<br>4: UMTS first (MUC 3G, MUC 4G rev. 3),<br>5: LTE only (MUC 4G),<br>6: UMTS first, then LTE (MUC 4G rev. 3),<br>7: LTE first, then UMTS (MUC 4G rev. 3),<br>8: GSM first, then LTE (MUC 4G),<br>9: LTE first, then GSM (MUC 4G) | 0-9 | 0 |
| WAN_RECONNECT TIMEOUT | Seconds | 1800-4294967295 | 604800 |
| WAN_RS485ENABLE | Activation of the RS-485 interface for WAN communication | 0, 1 | 0 |
| WAN_RSSITEST | | | 0 |
| WAN_STOPBITS | Stop bits for the WAN communication | 1, 2 | 1 |
| WAN_TECHNOLOGY | Selected radio technology. The preset mode DEFAULT is interpreted as the intended resp. reasonable value according to the modem type. If the selected mode is not supported by the modem (e. g. LTE on NB-IoT), an error is logged and the modem remains in the prior state. | DEFAULT, LTE, GSM, UMTS, NBIOT, CATM, LTE_GSM, LTE_UMTS, UMTS_GSM, LTE_UMTS_GSM | DEFAULT |
| WAN_USER | Username for accessing WAN | Text, max. 255 characters | Not set |
| WATCHDOG_IDLE | Watchdog timeout for the idle state (in s) | 1-4294967295 | 120 |
| WATCHDOG_PROCESS | Watchdog timeout in the busy state (in s) | 1-4294967295 | 900 |

*Continued on next page*

Table 19 – *Continued from previous page*

| Parameter | Description | Range | Standard |
|---|---|---|---|
| WATCHDOG_READOUT | Watchdog timeout during readout (in s) | 1-4294967295 | Quadruple of the readout cycle, at least: WATCHDOG_PROCESS |
| WATCHDOG_SCAN | Watchdog timeout during scanning (in s) | 1-4294967295 | 43200000 |
| WEBCOM_PASSWORD PATTERN | | | Not set |
| WEBCOM_ ADMINLOGIN_ SWITCHREQ | | 0, 1 | 1 |
| WEBCOM_USESWITCH | | | Not set |
| WEBCOM_TIMEOUT | Timeout for a web session after automatic logout of a user (in ms) | 1-4294967295 | 60000 |
| WMBUS_ALLOW INSECURE | | | 0 |
| WMBUS_BAUDRATE | Baud rate for the wM-Bus communication | 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800 | 19200 |
| WMBUS_CACHESIZE | wM-Bus cache size for temporary storage of received meter data | 1-500 | 500 |
| WMBUS_CACHE TIMEOUT | Storage time of received wM-Bus packets in the cache list (in s, 0: no limit) | 0-4294967295 | 0 |
| WMBUS_DATABITS | Data bits for the wM-Bus communication | 7, 8 | 8 |
| WMBUS_DECRYPTUSE LINKLAYERID | | | 0 |
| WMBUS_DEVPATH | Linux path of the wM-Bus interface | Text, max. 255 characters | Not set |
| WMBUS_FIXEDLAYOUT | | 0, 1 | 0 |
| WMBUS_FLOW CONTROL | Handshake for the wM-Bus communication: 0: none, 1: XON/XOFF when sending, 2: RTS/CTS, 8: XON/XOFF when receiving, 9: XON/XOFF when sending and receiving | 0, 1, 2, 8, 9 | 0 |
| WMBUS_FULLTIMEOUT | Maximum time (in ms) for a „packet" in the transparent mode of the wM-Bus which will be transmitted via TCP/UDP in a consolidated form. The Idle Timeout defined by WMBUUS_ IDLETIMEOUT is respected. | 0-65535 | 1000 |
| WMBUS_IDLETIMEOUT | Idle time (in ms) after which the „packet" in the transparent mode of the wM-Bus, which will be transmitted via TCP/UDP in a consolidated form, is regarded as completed. | 0-65535 | 20 |
| WMBUS_MODE | Mode of the wM-Bus module | S, T, C, C_T | C_T |
| WMBUS_NETWORK_ ROLE | Function of the wM-Bus interface | DISABLED, MASTER, SLAVE | MASTER |
| WMBUS_PARITY | Parity of the wM-Bus communication: 0: none, 1: odd, 2: even, 3: mark, 4: space | 0-4 | 0 |
| WMBUS_ RAWDATAINCLUDERSSI | | 0, 1 | 0 |
| WMBUS_RAWLOG ENABLE | Activation of the raw data logging to the directory *ext/* | 0, 1 | 0 |
| WMBUS_RS485ENABLE | Activation of the RS-485 interface for the wM-Bus communication | 0, 1 | 0 |
| WMBUS_SMLENABLE | Activation of processing SML protocol data | 0, 1 | 0 |
| WMBUS_STOPBITS | Stop bits for the wM-Bus communication | 1, 2 | 1 |

Table 19 – *Continued from previous page*

| Parameter | Description | Range | Standard |
|---|---|---|---|
| WMBUS_TRANSPARENT | Activation of the transparent transmission of the wM-Bus interface to a network port:<br>NONE: transmission deactivated,<br>TCP: transmission of a TCP port,<br>UDP: transmission to a UDP port | NONE, TCP, UDP | NONE |
| WMBUS_TRANSPARENT PORT | Network port for the transparent transmission via TCP or UDP | 0-65535 | 0 |
| WMBUS_TRANSPARENT RSSI | Activation of the integration of the RSSI value in transparent mode | 0, 1 | 0 |
| WMBUS_TRANSPARENT STARTSTOP | Activation of the integration of a start byte and stop byte in transparent mode | 0, 1 | 0 |
| WMBUS_USE LINKLAYERID | Compatibility mode for reading of faulty wM-Bus meters, uses link layer address instead of extended link layer address | 0, 1 | 0 |
| WMBUS2_BAUDRATE | Baud rate for the wM-Bus communication (channel 2) | 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800 | 19200 |
| WMBUS2_DATABITS | Data bits for the wM-Bus communication (channel 2) | 7, 8 | 8 |
| WMBUS2_DEVPATH | Linux path of the wM-Bus interface (channel 2) | Text, max. 255 characters | Not set |
| WMBUS2_FLOW CONTROL | Handshake for the wM-Bus communication (channel 2):<br>0: none,<br>1: XON/XOFF when sending,<br>2: RTS/CTS,<br>8: XON/XOFF when receiving,<br>9: XON/XOFF when sending and receiving | 0, 1, 2, 8, 9 | 0 |
| WMBUS2_MODE | Mode of the wM-Bus module (channel 2) | S, T, C, C_T | C_T |
| WMBUS2_PARITY | Parity of the wM-Bus communication (channel 2):<br>0: none,<br>1: odd,<br>2: even,<br>3: mark,<br>4: space | 0-4 | 0 |
| WMBUS2_RS485ENABLE | Activation of the RS-485 interface for the wM-Bus communication (channel 2) | 0, 1 | 0 |
| WMBUS2_STOPBITS | Stop bits for the wM-Bus communication (channel 2) | 1, 2 | 1 |
| WMBUS2_ TRANSPARENT | Activation of the transparent transmission of the wM-Bus interface (channel 2) to a network port:<br>NONE: transmission deactivated,<br>TCP: transmission of a TCP port,<br>UDP: transmission to a UDP port | NONE, TCP, UDP | NONE |
| WMBUS2_ TRANSPARENTPORT | Network port for the transparent transfer of the wM-Bus interface (channel 2) via TCP or UDP | 0-65535 | 0 |
| WMBUS2_ TRANSPARENTRSSI | Activation of the integration of the RSSI value in transparent mode of the wM-Bus interface (channel 2) | 0, 1 | 0 |
| WMBUS2_ TRANSPARENT STARTSTOP | Activation of the integration of a start byte and stop byte in transparent mode of the wM-Bus interface (channel 2) | 0, 1 | 0 |
| MODBUS_TLSENABLE | | | 0 |
| MODBUS_CA_FILE | | | 0 |
| MODBUS_CERT_FILE | | | 0 |
| MODBUS_KEY_FILE | | | 0 |
| MODBUS_INSECURE | | | 0 |
| MBUS_TRANSPARENT_ TLSENABLE | | | 0 |

*Continued on next page*

Table 19 – *Continued from previous page*

| Parameter | Description | Range | Standard |
|---|---|---|---|
| MBUS_TRANSPARENT_CA_FILE | | | 0 |
| MBUS_TRANSPARENT_CERT_FILE | | | 0 |
| MBUS_TRANSPARENT_KEY_FILE | | | 0 |
| MBUS_TRANSPARENT_INSECURE | | | 0 |
| WMBUS_TRANSPARENT_TLSENABLE | | | 0 |
| WMBUS_TRANSPARENT_CA_FILE | | | 0 |
| WMBUS_TRANSPARENT_CERT_FILE | | | 0 |
| WMBUS_TRANSPARENT_KEY_FILE | | | 0 |
| WMBUS_TRANSPARENT_INSECURE | | | 0 |
| WMBUS2_TRANSPARENT_TLSENABLE | | | 0 |
| WMBUS2_TRANSPARENT_CA_FILE | | | 0 |
| WMBUS2_TRANSPARENT_CERT_FILE | | | 0 |
| WMBUS2_TRANSPARENT_KEY_FILE | | | 0 |
| WMBUS2_TRANSPARENT_INSECURE | | | 0 |
| DLDERS_TRANSPARENT_TLSENABLE | | | 0 |
| DLDERS_TRANSPARENT_CA_FILE | | | 0 |
| DLDERS_TRANSPARENT_CERT_FILE | | | 0 |
| DLDERS_TRANSPARENT_KEY_FILE | | | 0 |
| DLDERS_TRANSPARENT_INSECURE | | | 0 |
| MBUSSLVMETER_TLSENABLE | | | 0 |
| MBUSSLVMETER_CA_FILE | | | 0 |
| MBUSSLVMETER_CERT_FILE | | | 0 |
| MBUSSLVMETER_KEY_FILE | | | 0 |
| MBUSSLVMETER_INSECURE | | | 0 |
| MBUSSLV2METER_TLSENABLE | | | 0 |
| MBUSSLV2METER_CA_FILE | | | 0 |
| MBUSSLV2METER_CERT_FILE | | | 0 |
| MBUSSLV2METER_KEY_FILE | | | 0 |
| MBUSSLV2METER_INSECURE | | | 0 |
| **Group [REPORT_x]*** | | | |

*Continued on next page*

Table 19 – *Continued from previous page*

| Parameter | Description | Range | Standard |
|---|---|---|---|
| MODE | Mode of the report instance resp. deactivation | | DISABLED |
| FORMAT | Format employed of the report instance | | Not set |
| HOST | Remote station of the report instance | | Not set |
| PORT | Network port of the remote station of the report instance | | |
| PATH | Path for the remote station of the report instance | | Not set |
| USER | Username for the remote station of the report instance | | Not set |
| PASSWORD | Password for the remote station of the report instance | | Not set |
| TOADDRESS | Receiver address of the report instance, particularly SMTP | | Not set |
| FROMADDRESS | Sender address of the report instance, particularly SMTP | | Not set |
| PARAM1 | User-specific parameter (1) of the report instance, particularly user format or user mode | | Not set |
| PARAM2 | User-specific parameter (2) of the report instance, particularly user format or user mode | | Not set |
| PARAM3 | User-specific parameter (3) of the report instance, particularly user format or user mode | | Not set |
| BASENAME | Basic file name for files to be transmitted (XML or CSV) | | |
| CONTENTTYPE | | | |
| CONVERTARG | | | |
| EXTENSION | | | |
| INSECURE | | | 0 |
| CA_FILE | Path to the CA certificate for the report instance | | |
| CERT_FILE | Path to the device certificate for the report instance | | |
| KEY_FILE | Path to the device key for the report instance | | |
| CYCLEMODE | | | MINUTE |
| CYCLE | Cycle time for meter reading (unit according to CYCLEMODE) | | 15 |
| CYCLEDELAY | | | 0 |
| CYCLETIMESTAMP | | | Not set |
| RANDOMDELAY | | | |
| RETRY_INTERVAL | Interval for the retry of failed reports: -1: no repetition, failed reports are not retransmitted, 0: automatic (for cyclic reports retry after 1/10 of the Report Cycle Time with minimum 10 minutes, for reports with „On Readout" retry after 10 minutes), >0: time in seconds after which a failed report is retransmitted | -1, 0, arbitrary positive integer | 0 |
| MIN_SEND_INTERVAL | Minimum interval for sending the report. Assures that at least this delay (in seconds) is respected after the successful transmission of a report or the failure to send a report before transmitting the subsequent report. The parameter is not effective if reports are prompted by Readout or manually via the website. | 0, arbitrary positive integer | 0 |
| MAX_BACKLOG | Maximum time into the past for which reports are sent (in seconds). See complement underneath this table. | arbitrary positive integer | 0 |

*x denotes the report instance 1-10

Table 19: chip.ini parameters

Page 72/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH

✔ Complement to MAX_BACKLOG:

– For cyclic reports, only reports are transmitted whose data range is not entirely older than this period. If the beginning of the data range is older and the end newer than this time for a report, then the report will be transmitted with its entire data range.

– For a report triggered with „On Readout", the beginning of the data range is limited to the Backlog time.

– The analysis occurs upon system start, reconfiguration or the generation of a report by due date, retry after failure or readout. If reports fail continually, no retry of reports older than the indicated time will occur.

## 6.4 Configuration file Device_Handle.cfg

The file `app/Device_Handle.cfg` contains the meter configuration. If this file does not exist, it can be created via the web-based front end using the **Meter** tab. All wM-Bus meters collected during operation are integrated permanently into the list after a scan process or by manually saving the configuration. Only those parameters need to be stored in that file which deviate from the defined default values (version entry excluded).

⚠ The file has to be saved as UTF8 encoded XML file.

⚠ To devices with older software without a database (prior to 1.34) applies the following: When the meter configuration is changed, all files in the directory `ext/Tmp` have to be deleted manually (if present). Data which has not been reported is discarded when the meter configuration is changed.

⚠ To devices with newer software with a database (from 1.34) applies the following: When the file `Device_Handle.cfg` is changed manually, the parameter <*layoutversion*> stated therein has to be incremented.

ⓘ The device needs to be rebooted after changing the file `Device_Handle.cfg` manually for the change to take effect. The reboot can be triggered via the web-based front end using the button **Reboot system** in the **Service** tab or via the command line.

ⓘ Manual changes are permanently stored on the flash not instantly, but after a few minutes. As a result, changes are possibly lost if the device is rebooted by switching the power supply off and on.

✔ The file `Device_Handle.cfg` can be transferred to other devices via FTPS. The attached meters need to be taken into account.

The file is an XML file and has the following structure:

| Parent | Element | Description | Standard | Example |
|--------|---------|-------------|----------|---------|
| | root | Root element | - | - |
| root | version | Version number of the XML specification | Not set | 0x06 |
| root | layoutversion | Layout number of the database | Not set | 0x06 |
| root | meter | Parent element for each meter | - | - |
| meter | interface | Interface of the meter: M-Bus, wM-Bus, DLDERS, S0, Modbus | Not set | M-Bus |
| meter | serial | Meter number (serial number), BCD notation, leading „0x" | 0xFFFFFFFF | 0x30101198 |
| meter | manufacturer | Manufacturer code of the meter (wildcard 0xFFFF) | 0xFFFF | 0x3B52 (NZR) |
| meter | version | Version number of the meter | 0xFF | 0x01 |
| meter | medium | Medium of the meter, see second column in Table 21 (wildcard 0xFF, if not set) | Not set | Electricity |
| meter | primaryaddress | Primary address of the meter (M-Bus, S0 or Modbus) | 0 | 0x03 |
| meter | addressmode | Addressing mode<br>0: secondary,<br>1: primary | 0 | 0 |
| meter | readoutcycle | Specific readout cycle (in s) | 0 | 900 |
| meter | maxvaluecount | Limitation of the number of meter values | 0 | 12 |

*Continued on next page*

Table 20 – *Continued from previous page*

| Parent | Element | Description | Standard | Example |
|--------|---------|-------------|----------|---------|
| meter | encryptionkey | Key for encrypted communication, e.g.: AES for wM-Bus | Not set, 0 | 0x82 0xB0 0x55 0x11 0x91 0xF5 0x1D 0x66 0xEF 0xCD 0xAB 0x89 0x67 0x45 0x23 0x01 |
| meter | active | Activates the meter for logging or for reporting. | 1 | 1 |
| meter | rssi | RSSI value of the last reception (wM-Bus) | 0 | 123 |
| meter | register | Register assignment (e. g. Modbus slave) | 0 | 250 |
| meter | user | User-specific text (see **User label** column in the **Meter** tab) | Not set | Floor-1-Right |
| meter | dbid | Unique database key of the meter, if the meter is activated for reporting | Not set | 1 |
| meter | value | Parent element for each meter value of the meter | - | - |
| value | description | Description of the meter value, see second column in Table 22 | None | Energy |
| value | unit | Unit of the meter value, see second column in Table 23 | None | Wh |
| value | encodetype | Coding of the meter value | NODATA | INT32 |
| value | scale | Scaling factor of the meter value (scientific notation) | 1e0 | 1e-3 |
| value | userscale | User-specific scaling factor of the meter value (scientific notation) | 1e0 | 1e-1 |
| value | valuetype | Type of meter values: INSTANTANEOUS, MAXIMUM, MINIMUM, ERRORSTATE | instantaneous | instantaneous |
| value | storagenum | Storage number of the meter value | 0 | 2 |
| value | tariff | Tariff information of the meter value | 0 | 3 |
| value | confdata | Generic data, OBIS code of the meter value (X-X:X.X.X*X; X=0-255; see **OBIS-ID** column in the **Meter** tab) | Not set | 0x01 0x00 0x01 0x08 0x00 0xFF |
| value | rawdata | Raw data of the meter value for M-Bus and wM-Bus | Not set | 07 FB 0D 00 00 00 00 00 00 00 00 |
| value | dif | Data information fields of the meter value for M-Bus and wM-Bus | Not set | 07 |
| value | vif | Value information fields of the meter value for M-Bus and wM-Bus | Not set | FB 0D |
| value | active | Activates the meter value for logging or for reporting. | 1 | 1 |
| value | register | Register assignment (e. g. Modbus slave) | 0 | 250 |
| value | user | User-specific text (see **User label** column in the **Meter** tab) | Not set | Room 2 |
| value | bacnetreg | Object number for BACnet | Not set | 8 |

Table 20: Structure of the Device_Handle.cfg

## 6.5 OpenVPN Client

An OpenVPN client is integrated on the devices from solvimus GmbH for enabling an encrypted remote access. This offers a comfortable way to configure and operate the devices remotely. The configuration of the devices themselves is very simple and intuitive.

❌ The use of a VPN is restricted or even prohibited by law in some countries. Every user is obliged to inform himself about the laws applicable in his country.

### 6.5.1 Configuration of the device

Using the OpenVPN client is simple. Only the configuration file *config.ovpn* for the client has to be stored on the device in the directory *app/vpn*. This directory can be created when connecting via FTP. The configuration file can be obtained from the administrator of your VPN. The device needs to be restarted by pressing the button **Reboot system** in the **Service** tab or via the command line. The OpenVPN client is activated by using the checkbox **VPN** in the **General** tab (see Section 4.3).

🛈 Please be aware of the exact file name: *config.ovpn*.

Page 74/81
UG_EN_MBUS-GEV.pdf
Version: 1.1
Released
Frank Richter, 23 February 2024
© solvimus GmbH

When saving the configuration via the web-based front end, the OpenVPN client is started and the VPN connection is established.

  ⓘ OpenVPN usually uses the UDP port 1194. A firewall needs to allow this port.

  ➡ Please ask your administrator for providing a client configuration file.

## 6.6 Preconfiguration of the meter list

Manual editing of a meter list for large installations with many meters is demanding and time-consuming.

This can be automated with two approaches.

### 6.6.1 File meter-conf-import.csv

The first approach uses the `app/meter-conf-import.csv`. It is used to add meta information such as the **Encryption key** or the **User label** when scanning/listing a meter.

  ✔ If the meter is already listed or configured in the **Meter** tab, the data from the file will not be transferred. The meter has to be removed from the list first.

The file can be manually uploaded to the device via FTPS (see also Section 3.5). However, it is also possible to import it via the **Service** tab (see Section 4.12). The file has to be provided as packed `*.tar.gz` file.

  ➡ For creating a `*.tar.gz` archive, the free, open source software *7zip* can be used. First, the file `meter-conf-import.csv` needs to be packed without subdirectory into a `*.tar` ball and afterwards into a `*.gz` archive.

The following columns can be used in the CSV file:

  • Interface: the interface via which the meter is read out (M-Bus, wM-Bus).

  • Serial: 8-digit meter serial

  • Encryption key: Encryption key of the meter in hexadecimal byte notation (optional)

  • user label: User-specific label of the meter (optional)

  • Cycle: Readout interval of the meter (optional)

Here is an example:

```
Interface; Serial; Encryptionkey; user label
WMBUS;12345670;00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F;Apartment 01
WMBUS;12345671;01 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F;Apartment 02
WMBUS;12345672;02 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F;Apartment 03
WMBUS;12345673;03 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F;Apartment 04
WMBUS;12345674;04 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F;Apartment 05
WMBUS;12345675;05 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F;Apartment 06
WMBUS;12345676;06 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F;Apartment 07
WMBUS;12345677;07 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F;Apartment 08
WMBUS;12345678;08 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F;Apartment 09
WMBUS;12345679;09 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F;Apartment 10
```

### 6.6.2 File Device_Config.cfg

The second approach uses the file `app/Device_Config.cfg`.

## 6.7 Scripting

Extending the functional scope of the standard device by customer-specific functionalities is the main purpose for scripting. Its basis are source codes which are executed or interpreted on the target system, i.e. the device.

Standard environments such as *XSLTPROC* or *BASH* are available as interpreters on the devices from solvimus GmbH, wherein the transformation of the meter data to the destination format is performed by the transformation language XSL. Scripts can run in these environments and enable various functions.

### 6.7.1 XSLT parser

*XSLTPROC* is an interpreter for applying XSLT stylesheets to XML documents.

➡ More information can be found at: http://xmlsoft.org/XSLT/xsltproc.html

Extensible Stylesheet Language Transformation (XSLT) is a description language for transforming an XML document into another document. This can be an XML document, a text document (e. g. CSV file or JSON file) or even a binary file.

Source and target files are considered as logical trees in XSLT. The transformation rule describes which nodes of the tree are processed and how the new content is derived from them. Conditional statements and loops can also be used.

The main intention for offering XSLT on the devices from solvimus GmbH is the generation of user-specific data formats. The device internally uses a proprietary XML format to provide the meter data. In order to generate the format that the operator uses or prefers, an XSLT conversion rule is used. In this way, the standard formats are generated (see Section 4.8) and additional user-specific formats can be provided.

✔ Only one single user-specific format is available for the standard operating modes (e. g. TCP or FTP) of the report instances. If several different user-specific formats are required, other instances must be to set to *User* mode.

Here are some possible applications:

- CSV file per meter
- JSON data stream for IoT communication
- Time displayed as readable ASCII string instead of UNIX timestamp
- Fixed point notation in CSV file
- Changed column arrangement in CSV file
- Combine several meter values of identical type in one line if read out at the same time

The transformation files can be used either within the scripts for the transformation of the format or via the configuration website in the **Meter** tab (button **Export**, format: USER) for an export. These can be stored in the following paths. The `*.xsl` files are stored in `app/report`. The file name is specific to the instance and composed of *report_* and the number of the instance (n = 1-10). Thus, an individual user-specific format can be realized for each report instance: *report_1.xsl*, *report_2.xsl*, ... For a **Report format** *User* selected via the front end, the respective file `app/report/report_n.xsl` will be used for each instance (n = 1-10). If the file specific to the instance is not available, the path instance `app/report/report.xsl` will be used which is also employed for the export of the meter value data. The path check occurs when initializing the application.

### 6.7.2 Report script

In addition to the operator, the application can also issue commands via the command line (see Section 6.1.2). This allows implementing user-specific processes on the devices from solvimus GmbH.

If the mode of a report instance is set to *User*, this function comes into play. Instead of the hard-coded processes like TCP or FTP, the provided *BASH* script is now called. The command sequence contained therein is processed and then the script is terminated. In this way, third-party tools available for Linux can also be used for transferring data or for implementing orthogonal functionality. Here are some possible applications:

- MQTT for IoT communication
- Connectivity to an InfluxDB
- Request to server before sending data (conditional data transfer)
- Reporting to different file servers, depending on the **User label** set
- Checking thresholds and alarming

Page 76/81
UG_EN_MBUS-GEV.pdf
Version: 1.1
Released
Frank Richter, 23 February 2024
© solvimus GmbH

The script files are stored as *.sh in app/report. The file name is specific to the instance and composed of *report_* and the number of the instance (n = 1-10). Thus, an individual user-specific script can be realized for each report instance: *report_1.sh*, *report_2.sh*, ... For a **Report mode** *User* selected via the front end, the respective file *app/report/report_n.sh* will be used for each instance (n = 1-10). If the file specific to the instance is not available, the path instance *app/report/report.sh* will be used. The path check occurs when initializing the application.

The following example sends user-specific data via MQTT. Therefore, *XSLTPROC* is called before the MQTT call is made via *mosquitto_pub* (long lines are wrapped):

```
#!/bin/bash
exec 1> >(logger -t report) 2>&1
set -e
set -o pipefail

shopt -s nullglob
rm -rf /tmp/reportfiles || true
mkdir /tmp/reportfiles
mcsvtoxml -m -c | xsltproc --stringparam serial "$SOLAPP_SERIAL"
  --stringparam timestamp "$(date +%s)" /mnt/app/report/report.xsl -

for file in /tmp/reportfiles/*/*; do
  subpath=$(echo ${file#/tmp/reportfiles/} | cut -d "." -f 1)
  mosquitto_pub -u "$SOLAPP_REPORT_USER" -P "$SOLAPP_REPORT_PASSWORD"
    -h "$SOLAPP_REPORT_HOST" -p "$SOLAPP_REPORT_PORT"
    --cafile "/var/conf/app/cacert.pem" --cert "/var/conf/app/clicert.pem"
    --key "/var/conf/app/clikey.pem" -t "$SOLAPP_REPORT_PATH/$subpath"
    -f "$file" --id "$HOSTNAME" --insecure
done
```

### 6.7.3 System meter script

Like the report using report scripts (see Section 6.7.2), the system meter (see Section 4.4.1) can also be extended user-specifically with system meter scripts.

Here, a *BASH* script is called at the readout time. It could return a meter value after completion. The return value needs to contain the following values in this order, separated by *newline* characters:

- Description of the meter value, *Description* column
- Unit of the meter value, *Unit* column
- Value of the meter value *Value* column

Here are some possible applications:

- Measure ping times for network quality monitoring
- Display outdoor temperature via Web API access

The script files are stored as *.sh file in app/metersystem. The respective file name is composed of *value* and a consecutive number from *1* upwards. Thus, user-specific values can be realized: *value1.sh*, *value2.sh*, ...

The following example adds the ping time to example.com to the system meter:

```
#!/bin/bash
echo -ne "Ping\nms\n"
ping=$(ping -n -c 3 example.com 2> /dev/null)
if [ $? -eq 0 ]; then
  echo $ping | awk -F '/' 'END {print $4}'
else
  echo -1
fi
```

## 6.8 Media types, measurement types and units

In the EN 13757-3 standard, media types, measurement types (measurement value descriptions) and units and are predefined. The devices from solvimus GmbH are using it for allowing a uniform data display.

The following table contains the predefined values for the medium:

| Index | Description |
|---|---|
| 0 | Other |
| 1 | Oil |
| 2 | Electricity |
| 3 | Gas |
| 4 | Heat (outlet) |
| 5 | Steam |
| 6 | Warm water |
| 7 | Water |
| 8 | Heat cost allocator |
| 9 | Compressed air |
| 10 | Cooling (outlet) |
| 11 | Cooling (inlet) |
| 12 | Heat (inlet) |
| 13 | Combined heat / cooling |
| 14 | Bus / System component |
| 15 | Unknown medium |
| 16-19 | Reserved |
| 20 | Calorific value |
| 21 | Hot water |
| 22 | Cold water |
| 23 | Dual register (hot/cold) water |
| 24 | Pressure |
| 25 | A/D Converter |
| 26 | Smoke detector |
| 27 | Room sensor |
| 28 | Gas detector |
| 29-31 | Reserved |
| 32 | Breaker (electricity) |
| 33 | Valve (gas or water) |
| 34-36 | Reserved |
| 37 | Customer unit |
| 38-39 | Reserved |
| 40 | Waste water |
| 41 | Waste |
| 42 | Carbon dioxide |
| 43-48 | Reserved |
| 49 | Communication controller |
| 50 | Unidirectional repeater |
| 51 | Bidirectional repeater |
| 52-53 | Reserved |
| 54 | Radio converter (system side) |
| 55 | Radio converter (meter side) |
| 56-255 | Reserved |

Table 21: Media types

The following table contains the predefined measurement types (descriptions for the measured value). Depending on the meter's interface, user-specific text-based measurement types (indication by index 31) can also be configured.

| Index | Description |
|---|---|
| 0 | None |
| 1 | Error flags (Device type specific) |
| 2 | Digital output |
| 3 | Special supplier information |
| 4 | Credit |
| 5 | Debit |
| 6 | Volts |
| 7 | Ampere |
| 8 | Reserved |
| 9 | Energy |
| 10 | Volume |
| 11 | Mass |

*Continued on next page*

Page 78/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH

Table 22 – *Continued from previous page*

| Index | Description |
|-------|-------------|
| 12 | Operating time |
| 13 | On time |
| 14 | Power |
| 15 | Volume flow |
| 16 | Volume flow ext |
| 17 | Mass flow |
| 18 | Return temperature |
| 19 | Flow temperature |
| 20 | Temperature difference |
| 21 | External temperature |
| 22 | Pressure |
| 23 | Timestamp |
| 24 | Time |
| 25 | Units for H. C. A. |
| 26 | Averaging duration |
| 27 | Actuality duration |
| 28 | Identification |
| 29 | Fabrication |
| 30 | Address |
| 31 | Meter specific description (text based) |
| 32 | Digital input |
| 33 | Software version |
| 34 | Access number |
| 35 | Device type |
| 36 | Manufacturer |
| 37 | Parameter set identification |
| 38 | Model / Version |
| 39 | Hardware version |
| 40 | Metrology (firmware) version |
| 41 | Customer location |
| 42 | Customer |
| 43 | Access code user |
| 44 | Access code operator |
| 45 | Access code system operator |
| 46 | Access code developer |
| 47 | Password |
| 48 | Error mask |
| 49 | Baud rate |
| 50 | Response delay time |
| 51 | Retry |
| 52 | Remote control (device specific) |
| 53 | First storagenum. for cyclic storage |
| 54 | Last storagenum. for cyclic storage |
| 55 | Size of storage block |
| 56 | Storage interval |
| 57 | Vendor specific data |
| 58 | Time point |
| 59 | Duration since last readout |
| 60 | Start of tariff |
| 61 | Duration of tariff |
| 62 | Period of tariff |
| 63 | No VIF |
| 64 | wM-Bus data container |
| 65 | Data transmit interval |
| 66 | Reset counter |
| 67 | Cumulation counter |
| 68 | Control signal |
| 69 | Day of week |
| 70 | Week number |
| 71 | Time point of day change |
| 72 | State of parameter activation |
| 73 | Duration since last cumulation |
| 74 | Operating time battery |
| 75 | Battery change |
| 76 | RSSI |
| 77 | Day light saving |
| 78 | Listening window management |
| 79 | Remaining battery life time |
| 80 | Stop counter |
| 81 | Vendor specific data container |
| 82 | Reactive energy |

*Continued on next page*

Table 22 – *Continued from previous page*

| Index | Description |
|-------|-------------|
| 83 | Reactive power |
| 84 | Relative humidity |
| 85 | Phase voltage to voltage |
| 86 | Phase voltage to current |
| 87 | Frequency |
| 88 | Cold/Warm Temperature limit |
| 89 | Cumulative count max. power |
| 90 | Remaining readout requests |
| 91 | Meter status byte |
| 92 | Apparent energy |
| 93 | Apparent power |
| 94 | Security key |
| 95 | Data frame |
| 96-255 | Reserved |

Table 22: Measurement types

The following table contains the predefined units. Depending on the meter's interface, user-specific units can also be configured.

| Index | Unit | Symbol | Description |
|-------|------|--------|-------------|
| 0 | None | | None |
| 1 | Bin | | Binary |
| 2 | Cur | | Local currency units |
| 3 | V | V | Volt |
| 4 | A | A | Ampere |
| 5 | Wh | Wh | Watt hour |
| 6 | J | J | Joule |
| 7 | $m^3$ | $m^3$ | Cubic meter |
| 8 | kg | kg | Kilogram |
| 9 | s | s | Second |
| 10 | min | min | Minute |
| 11 | h | h | Hour |
| 12 | d | d | Day |
| 13 | W | W | Watt |
| 14 | J/h | J/h | Joule per Hour |
| 15 | $m^3/h$ | $m^3/h$ | Cubic meter per hour |
| 16 | $m^3/min$ | $m^3/min$ | Cubic meter per minute |
| 17 | $m^3/s$ | $m^3/s$ | Cubic meter per second |
| 18 | kg/h | kg/h | Kilogram per hour |
| 19 | Degree C | °C | Degree Celsius |
| 20 | K | K | Kelvin |
| 21 | Bar | Bar | Bar |
| 22 | | | Dimensionless |
| 23-24 | | | Reserved |
| 25 | UTC | | UTC |
| 26 | bd | bd | Baud |
| 27 | bt | bt | Bit time |
| 28 | mon | mon | Month |
| 29 | y | y | Year |
| 30 | | | Day of week |
| 31 | dBm | dBm | Decibel (1 mW) |
| 32 | Bin | | Bin |
| 33 | Bin | | Bin |
| 34 | kVARh | kVARh | Kilo voltampere reactive hour |
| 35 | kVAR | kVAR | Kilo voltampere reactive |
| 36 | cal | cal | Calorie |
| 37 | % | % | Percent |
| 38 | $ft^3$ | $ft^3$ | Cubic feet |
| 39 | Degree | ° | Degree |
| 40 | Hz | Hz | Hertz |
| 41 | kBTU | kBTU | Kilo british thermal unit |
| 42 | mBTU/s | mBTU/s | Milli british thermal unit per second |
| 43 | US gal | US gal | US gallon |
| 44 | US gal/s | US gal/s | US gallon per second |
| 45 | US gal/min | US gal/min | US gallon per minute |
| 46 | US gal/h | US gal/h | US gallon per hour |
| 47 | Degree F | °F | Degree Fahrenheit |
| 48-255 | | | Reserved |

Table 23: Units

Page 80/81
UG_EN_MBUS-GEV.pdf

Version: 1.1
Released

Frank Richter, 23 February 2024
© solvimus GmbH

# 7 Accessory

The solvimus GmbH recommends the external power supply PHOENIX CONTACT STEP-PS/1AC/24DC/0.5, order number of the solvimus GmbH: 103501.

⚠ The usage of accessories not recommended is at your own risk. It is imperative to mind Section 1.2.5.