mbNET.rokey

Manual

V 6.2.0 DR01 - en | Mar. 17th, 2021

RKH 210, RKH 216, RKH 235, RKH 259EU, RKH 259 AT&T

By purchasing an ***mbNET*** router, you've selected a Made in Germany product. Our products are manufactured exclusively in Germany, to guarantee the highest quality and to secure jobs in Europe.

This manual describes the functions and operation of the ***mbNET.rokey*** Router RKH 210, RKH 216, RKH 235 andRKH 259 from hardware version HW03 and from firmware version 6.2.4.

Please read it carefully and keep in a safe place.

Find the latest information and updates on our website at www.mbconnectline.com.

We always welcome and are grateful for comments, suggestions for improvement and constructive criticism.

Trademarks and company logos

The use of a trademark and company logo not shown here is not an indication that it is freely available for use.

Publisher:
MB connect line GmbH
Remote Maintenance Solutions
Winnettener Str. 6
91550 Dinkelsbühl
GERMANY

Tel.: +49 (0) 700 MBCONNECT
+49 (0) 700 622 666 32
Website: www.mbconnectline.com

The latest information can be found on our website. We are always grateful for suggestions and proposed improvements.

Table of contents

1 General

Purpose of the documentation

This document describes the installation, use and functions of the **mbNET.rokey** industrial router RKH 210, RKH 216, RKH 235 und RKH 259.
The document serves as a reference guide. Please read carefully and keep in a safe place.

Validity

The document is valid for industrial routers ***mbNET.rokey*** RKH 210, RKH 216, RKH 235 und RKH 259 - **from firmware version V 6.2.4 and from hardware version HW03***

The ***SIMPLY.connect***** function is only available for devices with the **Simplify³**-Logo* .

* see device rating plate.

**SIMPLY.connect is a web application that helps you to set up a device (mbNET) in the Remote Service Portal mbCONNECT24. More information is available at: https://simplyconnect.mbconnectline.com/

Prerequisite/additionally required components

- Standard Windows PC with network card
- USB stick - recommended format: FAT32 or ext3;
  recommended maximum size: 4 GB (FAT32), 16 GB (ext3)
- Internet access

Additionally required software

If you run ***mbNET*** as a portal server device in the remote service portal ***mbCONNECT24***:

- ***mbCONNECT24*** from version V 2.4.1
  mbCONNECT24 is the central portal for secure remote maintenance via the Internet.
- ***mbDIALUP*** * from version V 3.8
  remote client to establish a secure VPN connection to the mbCONNECT24 portal.
- ***mbCHECK*** * from version V 1.1.2
  The program checks, among other things, whether at least one of the TCP ports 80TCP, 443TCP or 1194TCP in the firewall is enabled. At least one of these ports is required by mbDIALUP and the device (mbNET) in connection with mbCONNECT24.

* Current version can be downloaded at:www.mbconnectline.com.

Related documents

Getting started with mbCONNECT24

This document describes the first steps and measures necessary to get a device (mbNET router) connected via the Remote Client (mbDIALUP) to the portal server mbCONNECT24.

Current manuals and other information

The latest manuals and more information about products related to secure remote maintenance can be found in the download portal at www.mbconnectline.com

Release note

Version	Date	Comments
V 6.0.6	Apr. 11th, 2019	Start-Version
V 6.0.8	Jun. 19th, 2019	**Add** connection and termination examples for serial interfaces in RS 485 2- and 4-wire operation. See Chapter: "Pin assignment serial interfaces COM1/COM2 (front of device)" **Note on** "Last error message" when the red **Stat** LED lights up. See Chapter: "Front view of the device" **Add** the description for the menu "IO-Manager". See chapter: "IO-Manager"
V 6.1.0	Oct. 1st, 2019	Note on the function SIMPLY.connect in the chapters • "General > Validity" • "Display, controls and connectors" > "Front view of the device" The chapter ""Maintenance"" has been added, with the remark to check at regular in-tervals the actuality of the firmware installed on the device.
V 6.1.1	Dec. 5th, 2019	As of FW 6.1.1, the mbNET can function both as an NTP client and as an NTP server. See "System > Settings > NTP Settings"
V 6.1.2	Mar. 11th, 2020	Correction of the current consumption: old = 1300 mA => new = 500 mA Add the performance data for new LTE module, for devices with hardware version HW04.
V 6.1.3	Apr. 22nd, 2020	Add the processor performance data in the technical data.
V 6.1.4	July 6th, 2020	Add the transmission power of radio modules in the technical data.
V 6.2.0	Oct. 19th, 2020	General revision Additions to the menu: Extras > IoT (mbEDGE)
V 6.2 DR01	Mar. 17th, 2021	General corrections, update / change of the encryption algorithms.

2 Brief description

The ***mbNET*** industrial router offers you optimum flexibility and security, making remote communication with your systems both easy and secure. Thanks to its compact design, the ***mbNET*** router will fit into any switch cabinet, and with its multiple interfaces and drivers, is the perfect solution for integrating different control systems. The configuration of the router is done via the Web interface of the device or via the remote maintenance portal ***mbCONNECT24***.

3 Features

- Fully configurable using Web interface via locally connected computer, or remotely via ***mbCONENCT24***.
- Deployable worldwide using optional mobile modem connections (optional) plus access via LAN and Internet.
- Secure connection using an integrated firewall with IP filter, NAT and port forwarding, VPN with AES (256-, 192-, 128-Bit), Blowfish (128-Bit), 3DES (168-Bit), DES (56-Bit) encryption, and authentication via pre-shared key (PSK), static key or certificate (X.509).
- On-board 2-level remote access key
  - Pos. **REM**: trigger remote access connection
  - Pos. **ONL**: alarms, dashboards & router administration
  - Pos. **OFF**: no connection with mbCONNECT24
- Alarm management:
  - Fully configurable digital inputs and outputs, and the ability to send via email, SMS or Internet dialup.
  - Via remote output switching in the event of a fault or with an active Internet connection.
- Integrated server secures all settings, keys and certificates and allows data sharing within the network via connected USB flash or connected SD card.
- Variable RS232, RS485, RS422 RS interface or optional MPI/PROFIBUS for connecting control systems.
- Using the optional ***mbEDGE*** * function.

* ***mbEDGE*** is a software kit that makes it possible to extend the ***mbNET*** industrial router to an Edge Gateway. More information about ***mbEDGE*** can be found at www.mbconnectline.com

Use of open source software

General
Our products include, among other things, open source software, which is manufactured by a third party and has been published for free use by anyone. The open-source software is available under special open-source software licences and copyright of third parties. In principle, each customer can use open source software free of charge under the licence terms of the respective manufacturers. The customer's right to use the open source software for purposes other than those for which our products were intended is regulated in detail by the relevant open source software licences. The customer may freely use the open source software as set out in the respective valid licence, beyond the intended purpose of the open source software in our products. In the event that there is a contradiction between the licensing terms of one of our products and the respective open source software licence, the respective applicable open source software licence shall take priority over our licensing terms if the respective open source software is affected by this.

Use of the open source software is free of charge. We do not charge any usage fees or similar charges for the use of open source software included in our products. Customer use of open source software in our products is not part of the profit that we obtain from the contractual remuneration. All open source software programs contained in our products are in the available list. The most important open source software licenses are listed in the Licences section at the end of this publication.

If programs that are included in our products are under the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), the Berkeley Software Distribution (BSD), the Massachusetts Institute of Technology (MIT), or other open source software license, which requires that the source code be made available, and this software was not already supplied with our product on a disk or in the source code, we will send this at any time upon request. If we are required to send this on a disk, there will be a flat rate charge of €35.00. Our offer to send the source code upon request, shall automatically end 3 years after delivery of the respective product to the customer.

Requests must, where possible, be sent to the following address with the product's serial number:
MB connect line GmbH Fernwartungssysteme · Winnettener Str. 6 · 91550 Dinkelsbühl GERMANY
Tel. +49 (0) 98 51/58 25 29 0 · Fax +49 (0) 98 51/58 25 29 99 · info@mbconnectline.com

Special liability provisions
We assume no responsibility or liability if the open-source software programs included in our products are used by customers in a manner that no longer corresponds to the purpose of the contract which serves as the basis for the purchase of our products. This applies in particular to any use of the open source software programs outside of our products. The warranty and liability provisions, which stipulate the applicable open source software license for the corresponding open source software, as listed below, apply to the use of open-source software beyond the contractual purpose. In particular, we are also not liable if the open source software in our products or the entire software configuration in our products is changed. The warranty contained in the contract, which forms the basis for the purchase of our products, applies only to unchanged open source software and the unchanged software configuration in our products.

Open source software used
For a list of the open source software used in our products, visit https://www.mbconnectline.com/downloads/open-source-software-licenses.txt.

4 Information about cyber-security

To prevent unauthorized access to facilities and systems, observe the following security recommendations:

General

- Periodically ensure that all relevant components meet these recommendations and any additional internal security policies.
- Perform a security assessment of the entire system. Use a cell protection concept with suitable products.
  For example, "ICS-Security-Kompendium" from the BSI (Federal Office for Security in Information Technology, Bundesamt für Sicherheit in der Informationstechnik)
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.html

  shortened URL: http://bit.ly/1rP9znm

Physical access

- Restrict physical access to security-relevant components to qualified personnel.

Security of the software

- Keep software/firmware updated.
  - Stay informed about security updates for the product.
  - Stay informed about product updates.

You can find information about this at: www.mbconnectline.com

Passwords

- Define rules for the use of the devices and assigning passwords.
- Change passwords regularly, to increase security.
- Use only passwords with a high password strength. Avoid weak passwords such as "password1", "123456789".
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- Do not use the same password for different users and systems.

5 Warning signs

The following information signs and signal words are used in this document:

NOTICE
Note - indicates a potentially dangerous situation that can lead to property damage if not avoided.

TIP
A tip indicates additional information and guidance, for example on cyber security, which facilitates secure use of the system.

6 Security information

General

- mbNET industrial routers are only used as part of an overall system.
- A machine operator is responsible for compliance with the specific application and regionally applicable safety and accident prevention guidelines.
- When configuring the application, specific and local safety and accident prevention guidelines must be observed.
- EN 60204-1 / IEC 204 compliant emergency stop devices must remain effective in all operating modes of the machine system. There must be no undefined restart of the system.
- Faults that occur in the machinery, which can cause material or personal damage, must be intercept-ed by additional external devices. These devices must ensure a safe operating state in case of failure. Such devices include electromechanical safety switches, mechanical interlocks, etc.
- This manual is intended for project engineers, users and installers who use the mbNET Industrial router. The operation of the mbNET industrial router and the signalling functions should be explained to users. Installers should be provided with all the necessary data for installation.
- mbNET industrial routers are used only in connection with a complete system. For this reason, the standards, safety and accident prevention guidelines for each application should be observed by the project engineer, users and installers. The automation system operator is responsible for complying with these guidelines.

Intended use

mbNET industrial routers should only be used as described in the manual.

Avoid improper use!

Safety-relevant functions should not be controlled via the mbNET industrial router alone. Uncontrolled restarts must be completely excluded by programming.

Technical limits

The product is only intended for use within the technical limits specified in the data sheets.

EN/F Safety instructions

- Assembly, installation and commissioning of the router should be carried out only by qualified personnel. The respective national safety and accident prevention regulations must be observed.
- The router is built in accordance with the latest technology and all recognised safety rules (see declaration of conformity).
- The router is designed exclusively for use in the control cabinet and with safety extra-low voltage (SELV) in accordance with IEC 60950/EN 60950/VDE 0805.
- The router should only be connected to devices that meet the requirements of EN 60950.
- The router is only intended for use within buildings, not outdoors.
- Never open the router housing. Unauthorized opening and improper repair can be dangerous for users of the router. The manufacturer is not responsible for unauthorized modifications.

  The warranty becomes void if the device is opened!
- The router should not be disposed of with normal domestic waste in accordance with European standards (WEEE) and the German Electrical and Electronic Equipment Act. The device must be disposed of accordingly.

ATTENTION! Electrostatic discharge!
Note the necessary precautions when handling electrostatically sensitive components (EN 61340-5-1 and IEC 61340-5-1)!

mbNET routers are maintenance-free units. If an mbNET router is damaged or malfunctions, the device must be taken out of operation immediately and secured against unintended operation.

NOTICE

The MDH810, MDH815 and MDH830 should only be operated and connected via telephone systems and not operated directly on the public telephone network.

(F) Consignes de sécurité:

- Le routeur est construit selon l'état actuel de la technique et les règles techniques reconnues en matière de sécurité (voir la déclaration de conformité).
- Le routeur doit être monté à un endroit sec. Aucun liquide ne doit pénétrer dans le routeur, car cela pourrait occasionner des chocs électriques ou des courts-circuits.
- Le routeur est uniquement prévu pour l'utilisation dans des bâtiments et non pas à l'extérieur.
- Ne jamais ouvrir le boîtier du routeur. L'ouverture du routeur ou des réparations non adaptées peuvent mettre en danger l'utilisateur du routeur. Le fabricant n'assure aucune garantie concernant les modifications arbitraires.

  La garantie devient caduque en cas d'ouverture de l'appareil !
- Conformément aux prescriptions européennes et à la loi allemande relative à l'électronique et les appareils électroniques, il est interdit de mettre au rebut l'appareil avec les déchets domestiques normaux. L'appareil doit être éliminé dans le respect des prescriptions.

AVERTISSEMENT

Les modèles MDH810, MDH815 et MDH830 doivent être utilisés et raccordés uniquement via des centrales téléphoniques. Il est interdit de les faire fonctionner directement sur le réseau téléphonique public.

7 Maintenance

Our devices are maintenance-free units. If a device shows signs of damage or malfunctions, the device must be put out of operation immediately and secured against unintentional operation.

NOTICE

Regardless of the maintenance-free hardware, there is a need for action in terms of IT security.

- Keep the software / firmware up to date.
- Note the "Information about cyber-security".
- Keep yourself informed about security updates of the product.

Information can be found at: www.mbconnectline.com

8 Legal notice

Qualified personnel
The product/system described in this documentation may be operated only by personnel qualified for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are persons who, due to their training, experience, instruction in and knowledge of the relevant standards, regulations and accident prevention regulations have been authorized by the person responsible for the safety of the machine to carry out the required activities and who have the ability to recognize and avoid potential hazards.

Intended use
The device should only be used as described in the manual.

Limitation of liability
All technical information, data and notes about installation, operation and maintenance contained in the operating instructions are provided under consideration of our previous experience and findings to the best of our knowledge. No claims may be derived from the information, figures and descriptions in this operating manual. MB connect line GmbH assumes no liability for damages due to:

- Non-compliance with these instructions
- unintended use
- technical changes

Subject to content and technical modifications.

Trademarks
The use of a trademark and company logo not shown here is not an indication that it is freely available for use.

NOTICE

The device type RKH 259 AT&T is **not** CE marked and may not be used or put into service in the European Economic Area (EEA).

9 Technical Data

mbNET.rokey industrial router

RKH 210, RKH 216, RKH 235, RKH 259 EU, RKH 259 AT&T - from Hardware version: **HW 03**
You can find the hardware version on the device rating plate.

Housing dimensions and views

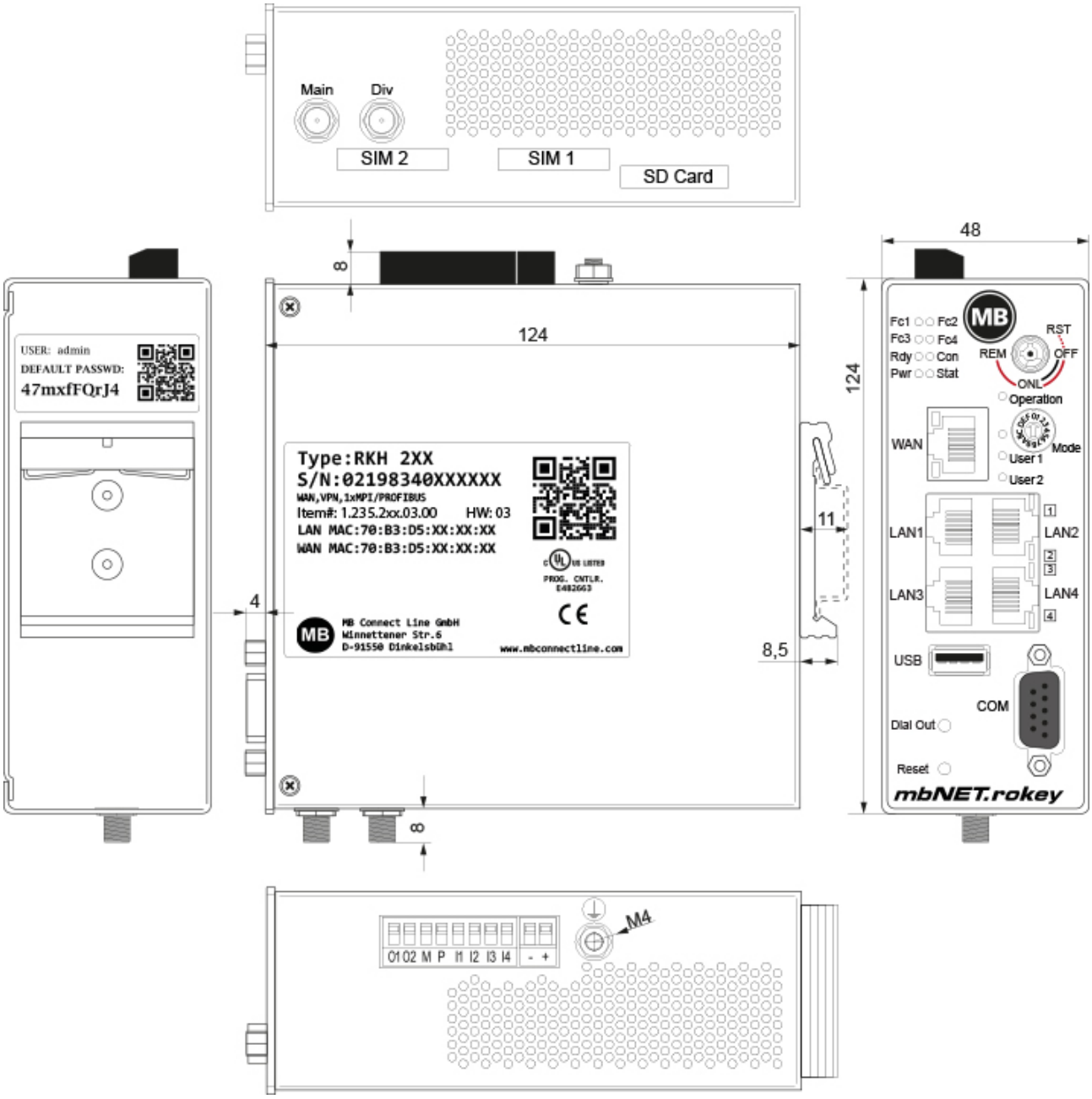


Image 1: Devices and interfaces vary depending on the device type.

Release note

Version	Date	Comment
V 6.2	Febr. 26th, 2020	Previous version: V 1.0 from Nov. 2nd, 2018 Correction of the current consumption: old = 1300 mA => new = 500mA Add the performance data for new LTE module, for devices with hardware version HW04.
V 6.2 DR01	Apr. 22nd, 2020	Add processor performance data.
V 6.2 DR02	July 6th, 2020	Adding the transmission power for radio modules.
V 6.2 DR03	Feb. 10th, 2021	Update / change of the encryption algorithms.

General Data

Performance data		
Voltage ⎓ V (DC)	10 – 30 V DC (ext. power supply or SELV power supply, 10-30 V DC, max. 40 A)	
Current consumption	max. 500 mA @ 24 V	
Dissipated power	max. 6 W	
Random Access Memory	512 MB	
Processor	Devices **with** hardware version **HW03**: ARM Cortex®-A8 up to **600MHz** Devices **from** hardware version **HW04**: ARM Cortex®-A8 up to **1GHz**	
IP Protection class	IP 30*	* at full occupancy of all connections and interfaces. Alternatively, unused interfaces can be covered with dust protection plugs.
Area of use	Dry environment	
Temperature (operating)	-40 – +75 °C	
Temperature (storage)	-40 – +85 °C	
Humidity	0 – 95% non-condensing	
Real-time clock	In the event of a power failure, the date and time are maintained for up to 7 days (depending on the ambient temperature).	
Dimensions (max.)	48 mm x 137 mm x 140 mm (W x D x H)	
Weight (max.)	650 g	
Housing/material	Metal	
Installation	DIN-top hat rail mounting	

I/Os and standard interfacesGeneral Data

Digital inputs	4 pieces, 1030 V DC (electrically isolated), (low 0 – 3.2 V DC, high 8 – 30 V DC)
Digital outputs	2 pieces, 10-30 V DC (electrically isolated), to a maximum of 1.5 A per output
WAN interfaces	10/100MBit/s full and half duplex operation, automatic detection patch cable/cross-over cable (auto detection)
LAN interfaces	4 pieces, 10/100MBit/s full and half duplex operation, automatic detection patch cable/cross-over cable (auto detection)
USB interfaces	USB Host 2.0
SD card slot	Für SD cards (32 x 24 x 2.1 mm) SDHC max. 32 GB; FAT/FAT32 or for holding ***mbEDGE*** *.

* ***mbEDGE*** is a software kit that extends the mbNET and mbNET.rokey industrial routers to an IOT gateway.

VPN

VPN protocol	IPsec/PPTP/OpenVPN, 64 Tunnel
Encryption method	AES (256-, 192-, 128-Bit), Blowfish (128-Bit), 3DES (168-Bit), DES (56-Bit)
Hash algorithms	SHA-2 (SHA-256, SHA-512), SHA-1, MD5
Authentication	Pre-Shared-Key, X.509

Network/security

Firewall	1:1 NAT, IP-Filter, port forwarding, stateful inspection
IP router	NAT-IP, TCP/IP routing, IP forwarding
Services	DHCP server, DHCP client, DNS server, NTP client, PPP server, DynDNS
Time levelling	NTP server

Optional Interfaces

COM	MPI/PROFIBUS - 12 MBit/s (RKH 235) or
	RS-232/485 (software-switchable) (RKH 210)
SIM card slots	2 pieces SIM card reader with ejector (for mini-SIM)

Communication

Devices with LTE (4G) modem EU (RKH 259 EU)

Devices with hardware version **HW 04**	
Countries where used	Europe
GSM/GPRS/EDGE	900 (B8), 1800 (B3) MHz; max. 236 kbps
HSxPA	900 (B8), 2100 (B1) MHz; Downlink max. 42 Mbps, Uplink max. 5,76 Mbps
LTE	800 (B20), 900 (B8),1800 (B3), 2100 (B1), 2600 (B7) MHz; Downlink max. 150 Mbps, Uplink max. 50 Mbps
Transmit output power	CLass 3 (0.2 W, 23 dBm) @ LTE CLass 3 (0.25 W, 23 dBm) @ 3G Class 4 (2 W) @ GSM 900 Class 1 (1 W) @ DCS 1800
Antenna connections	2 pieces SMA socket
TAC	35162207

Devices with hardware version **HW 03**	
Countries where used	Europe, Australia
GSM/GPRS/EDGE	900, 1800 MHz; max. 236 kbps
HSxPA	850, 900, 2100 MHz; Downlink max. 42 Mbps, Uplink max. 5,76 Mbps
LTE	800 (B20), 1800 (B3), 2600 (B7) MHz; downlink max. 100 Mbps, uplink max. 50 Mbps
Transmission output power	Class 4 (2 W, 33 dBm) @ GSM 850 / 900 Class 1 (1 W, 30 dBm) @ GSM 1800 / 1900 Class E2 (0.5 W, 27 dBm) @ EDGE 850 / 900 Class E2 (0.4 W, 26 dBm) @ EDGE 1800 /1900 Class 3 (0.25 W, 24 dBm) @ UMTS Class 3 (0.2 W, 23 dBm) @ LTE
Antenna connections	2 pieces SMA socket
TAC	35985205

Devices with LTE (**4G**) modems - **AT&T** (RKH 259 AT&T)

NOTICE

The device type RKH 259 AT&T bears no CE marking and may not be used or put into operation in the European economic area (EEA)!

Countries where used	North America
GSM/GPRS/EDGE	850, 1900 MHz; max. 236 kbps
HSxPA	1900 (B2), 850 (B5) MHz; Downlink max. 21 Mbps, Uplink max. 5,76 Mbps
LTE	1900 (B2), AWS 1700 (B4), 850 (B5), 700 (B17) MHz; downlink max. 100 Mbps, uplink max. 50 Mbps
Transmission output power	Class 4 (2 W, 33 dBm) @ GSM 850 / 900 Class 1 (1 W, 30 dBm) @ GSM 1800 / 1900 Class E2 (0.5 W, 27 dBm) @ EDGE 850 / 900 Class E2 (0.4 W, 26 dBm) @ EDGE 1800 /1900 Class 3 (0.25 W, 24 dBm) @ UMTS Class 3 (0.2 W, 23 dBm) @ LTE
Antenna connections	2 pieces SMA socket
FCC	Contains FCC ID: R17LE910NA

Markings / Listings / Certifications

PROG. CNTLR.
E482663

SIMPLIFIED EU DECLARATION OF CONFORMITY

MB connect line GmbH hereby declares that the radio system type RKH 259 EU corresponds to the 2014/53/EU directive.
A copy of the EU declaration of conformity is available at the following Internet address:
www.mbconnectline.com

NOTICE

The device type RKH 259 AT&T is **not** CE marked and may not be used or put into service in the European Economic Area (EEA).

10 Scope of Supply

Check the package contents for completeness:

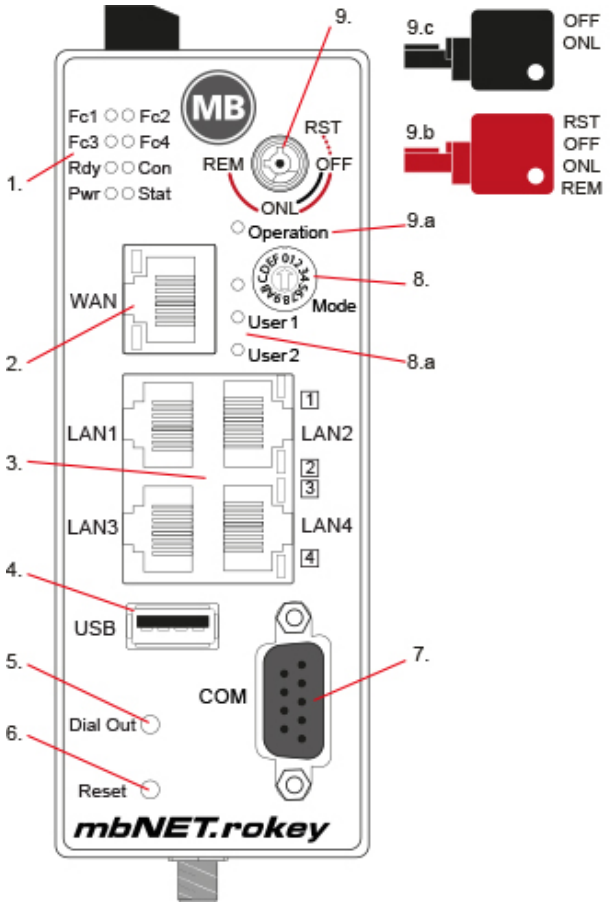
All types of devices		
		
1 x ***mbNET.rokey*** industrial router (Fig. representative)	1 x Ethernet cable 1:1, 2 m Item No.: 8.002.201.00.00	1 x Quick Start Guide Item No.: 8.002.704.00.00

Device types with GSM modem	HINWEIS
RKH 259	If one of these parts is missing or damaged, contact the following address: **MB connect line GmbH** Winnettener Str. 6 D-91550 Dinkelsbühl Tel.: +49 (0)9851/58 25 29 0 Fax: +49 (0)9851/58 25 29 99
	
1 x GSM antenna Item No.: 8.002.101.00.00	

Keep the original box as well as the original packaging material in case you need to send the device in for repair at a later date.

11 Display, controls and connectors

11.1 Front view of the device



1. Function / status LEDs
2. WAN interface
3. LAN interfaces 1 – 4 (4 port switch)
4. USB Host 2.0
5. Dial Out button
6. Reset button
7. Serial interface COM
8. Coding switch hexadecimal (Function in preparation)

8.a Function / status LEDs for coding switch

9. Key switch

9.a Function / status LEDs for key switch

9.b Key (red) for switch positions
OFF, **ONL**, **RST** *, **REM**

9.c Key (black) for switch positions
OFF, **ONL**

* The switch position RST has just a tactile function.

Function / Status LEDs

LED	LED colour	LED status	Description
Fc1	orange	flashes	• Together with Fc2 if a portal configuration has been detected via the USB interface. • Together with Fc3 if a firmware has been detected via the USB interface.
Fc2	orange	off	No data traffic on COM2 - incoming
		flashes	Data traffic on COM2 - incoming • Together with Fc1 if a portal configuration has been detected via the USB interface.
		on	For MPI: Bus communication OK
	green	off	No data traffic on COM2 - outgoing
		flashes	Data traffic on COM2 - outgoing For MPI: Data traffic on the bus
Fc3	orange	off	GSM devices: no reception

LED	LED colour	LED status	Description
		flashes	GSM devices: Blink frequency 1 Hz == 20 % – 50 % reception quality • Together with Fc1 if a firmware has been detected via the USB interface.
	green	off	GSM devices: Reception quality display depends on Fc4
		on	GSM devices: Fc3 green + Fc4 green: 71 % – 100 % reception quality
Fc4	orange	off	GSM devices: no reception
		flashes	GSM devices: Fc4 orange + Fc3 orange): 1Hz == 51 % – 70 % reception quality
	green	off	GSM devices: Reception quality display depends on Fc3
		on	GSM devices: Fc4 green + Fc3 green: 71 % – 100 % reception quality
		flashes	During the activation phase of ***mbEDGE*** the LED Fc4 flashes at a frequency of **3 Hz** (fast). After completion of activation at a frequency of **1.5 Hz** (slow).
Rdy	orange	off	Waiting for bootloader or signature successfully tested
		on	Checks signature, loads kernel
	green	off	Waiting for kernel
		flashes	System loading rootFs
		on	Boot process complete, the device can be used.
Con	orange	off	No VPN connection started
		on	Internet connection is established + VPN connection is started
		flashes	Blink frequency 1.5 Hz: VPN connection is established
	green	off	No Internet connection
		flashes	Blink frequency 3 Hz: Internet connection is started
		on	Internet connection is established
Pwr	green	off	The power supply to the router is interrupted/the router is not connected to the power supply.
	green	on	The power supply is connected to the terminal box and switched on.
Stat	red	flashes	Error in memory
		on	Error found The error type can be viewed on the WebGUI of the mbNET under **System> Info> "Last error message"**.
	green	on	In conjunction with the mbCONENCT24 portal: User is connected to the device.
Operation	green	on	For key switch position: OFF / ONL
	red	on	For key switch position: RST / REM
User 1	-	-	Currently without function.
User 2	-	-	Currently without function.

Interfaces

Designation	Status	Description
WAN	**–**	WAN port on the router (customer network, DSL modem,...)
WAN LED	green flashes	Network connection available
	orange flashes	Network traffic active
LAN 1 - 4	**–**	Local network connection (e.g. machine network)
LAN-LED 1 – 4 (Dual LED)	green flashes	Network connection available
	orange flashes	Network traffic active
USB	**–**	Connection for USB stick
COM	–	COM2 port for connecting devices with RS232/RS485, RS422 interface, or depending on the router type, devices with MPI /PROFIBUS interface.

Button

Designation	Description
Dial out	This button is required if a portal configuration or a firmware is to be transferred to the mbNET via the USB interface.
Reset	After pressing the button, the router is restarted (cold start).

Coding switch hexadecimal

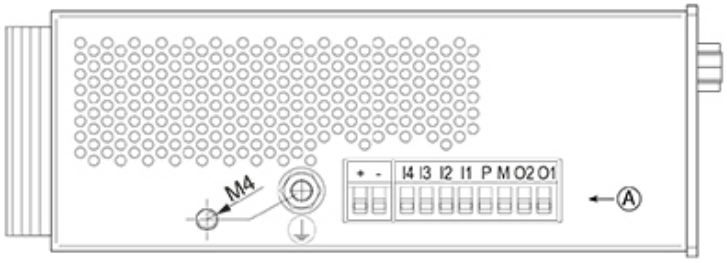
NOTICE

Function in preparation.

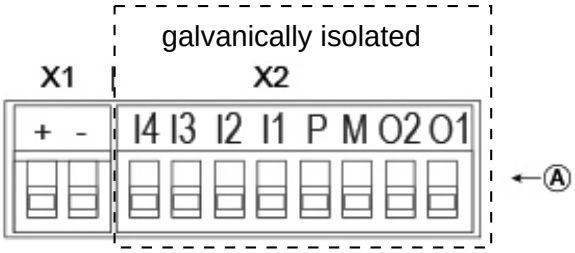
Key switch with two keys, for switching different functions.

Switch position	Key color	LED status "Operation"	Function
RST	red	red	Loading the factory settings
OFF	red / black	green	It is **not** possible to establish a VPN connection. Modem devices **cannot** connect to the Internet.
ONL	red / black	green	It **can** be established a VPN connection from the ***mbNET*** to ***mbCONNECT24***. With modem devices an Internet connection **can** be established. = Data Logging
REM	red	red	It **can** be established a VPN connection from the ***mbNET*** to ***mbCONNECT24*** including routing to the LAN side of the router. With modem devices an Internet connection can be established including routing to the LAN side of the router. = VPN connection with routes = Data logging = Remote Maintenance

11.2 View at the top of the device



X1	**+**	Supply voltage connection 10-30 V DC
	–	Connection 0 V DC
X2	**I4**	Digital input E4 (10-30 V DC)
	I3	Digital input E3 (10-30 V DC)
	I2	Digital input E2 (10-30 V DC)
	I1	Digital input E1 (10-30 V DC)
	P	Secure Voltage 10-30 V DC
	M	Connection 0 V DC
	O2	Digital output A2 (max. 1.5 A)
	O1	Digital output A1 (max. 1.5 A)



Circuit diagram with galvanic isolation of X1 and X2

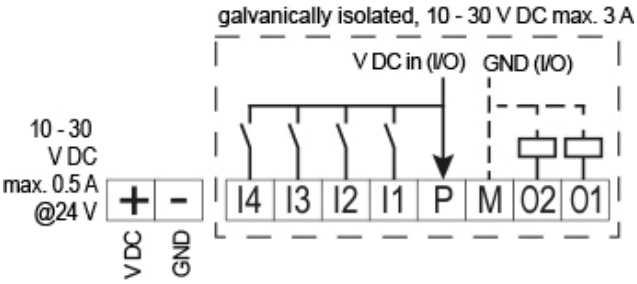


Image 2: Wiring diagram when using the galvanic isolation of X1 and X2

Circuit diagram without galvanic isolation of X1 and X2

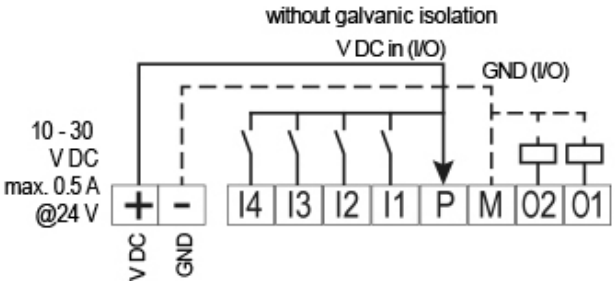
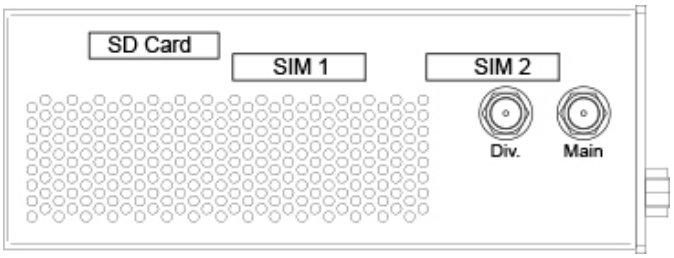
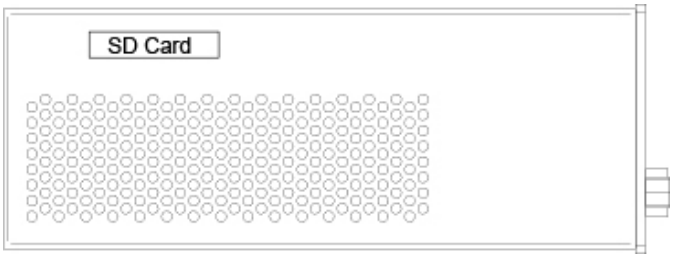


Image 3: Connection diagram for the bypass of the galvanic isolation of X1 and X2

11.3 View of underside of device

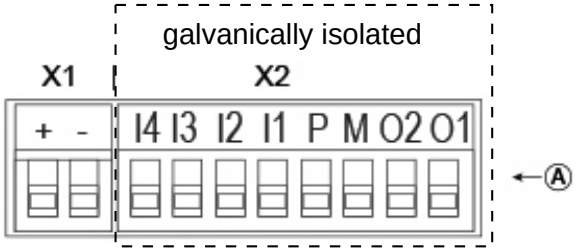
Devices with LTE (4G) modem	Type	Equipment
	RKH 259	1 x SD card slot 2 x SIM card slot 2 x SMA socket for GSM antenna (MIMO)

Standard devices	Type	Equipment
	RKH 210 RKH 216 RKH 235	1 x SD card slot

12 Interface assignment

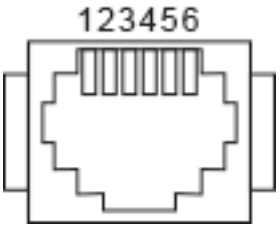
12.1 Pin assignment of terminal blocks X1 and X2 on the top of the device

X1	**+**	Supply voltage connection 10-30 V DC
	–	Connection 0 V DC
X2	**I4**	Digital input E4 (10-30 V DC)
	I3	Digital input E3 (10-30 V DC)
	I2	Digital input E2 (10-30 V DC)
	I1	Digital input E1 (10-30 V DC)
	P	Secure Voltage 10-30 V DC
	M	Connection 0 V DC
	O2	Digital output A2 (max. 1.5 A)
	O1	Digital output A1 (max. 1.5 A)



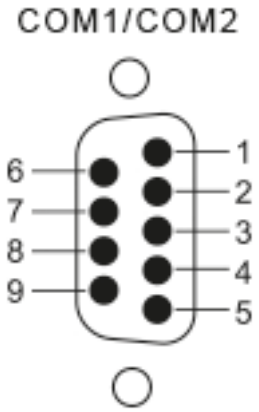
12.2 Pin assignment of the RJ11 socket on the bottom of the device

Pin	ISDN	Analogue
1	Not assigned	Not assigned
2	TX+	Not assigned
3	RX+	Lb/b
4	RX-	La/a
5	TX-	Not assigned
6	Not assigned	Not assigned



12.3 Pin assignment serial interfaces COM1/COM2 (front of device)

Pin	RS 232	RS 485	MPI
1	DCD Data Carrier Detect	Not assigned	Not assigned
2	RxD Receive Data	RxD– Receive Data	GND 24 V
3	TxD Transmit	TxD+ Transmit Data	Data line B
4	DTR Data Terminal Ready	+ 5 volts (4-wire operation only)	Send request
5	Signal Ground	Signal Ground	GND 5 V (200 mA)
6	DSR Data Set Ready	Not assigned	5V output
7	RTS Request To Send	TxD– Transmit Data	24 V power input
8	CTS Clear To Send	RxD+ Receive Data	Data line A
9	RI Ring Indicator	Not assigned	Send request



In RS 485 mode, terminations must be carried out using terminating resistors in accordance with the number of conductors.
Below you can see example circuits for 4-wire and 2-wire operation.

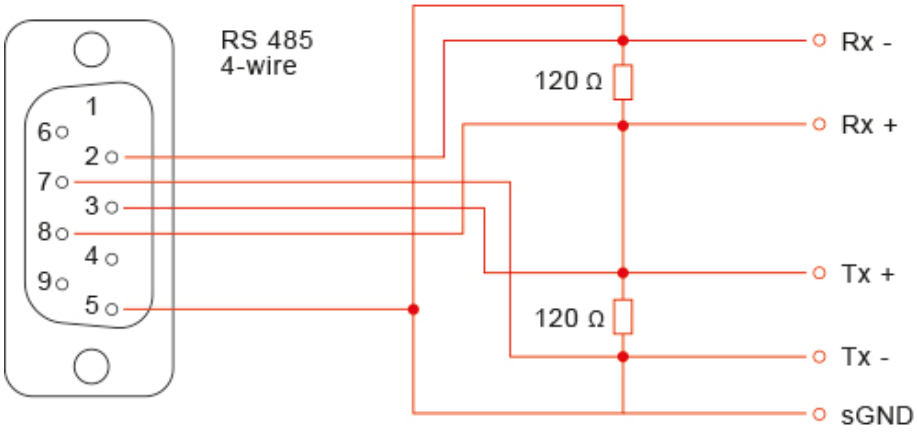


Image 4: Connection example for the 4-wire operation

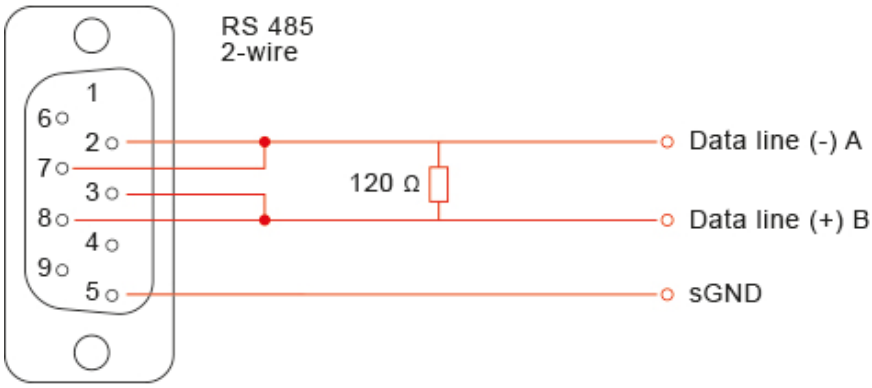
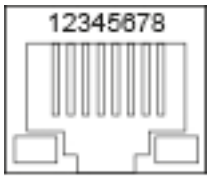


Image 5: Connection example for the 2-wire operation

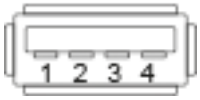
12.4 Pin assignment LAN/WAN port on front of device

	Signal
1	TX+
2	TX-
3	RX+
4	Not assigned
5	Not assigned
6	RX-



12.5 Pin assignment USB port on front of device

	Signal
1	VCC (+ 5 V)
2	– Data
3	+Data
4	GND



13 Router Installation

Installation position/minimum clearances

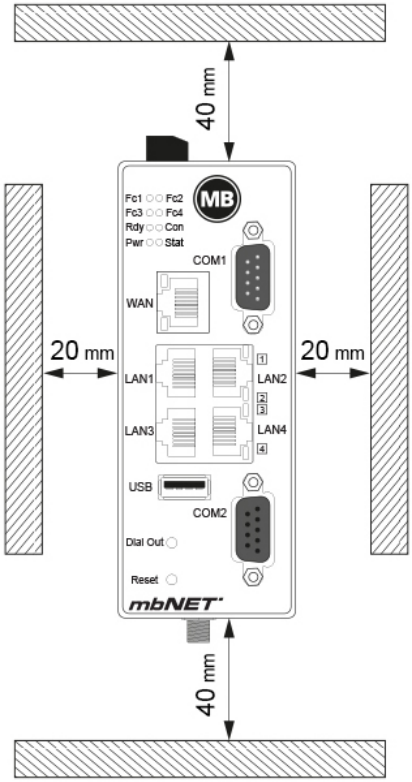
The router is designed to be mounted on DIN top hat rails (in accordance with DIN EN 50 022) and for installation in a control cabinet.

The installation and assembly must be carried out according to VDE 0100/IEC 364.

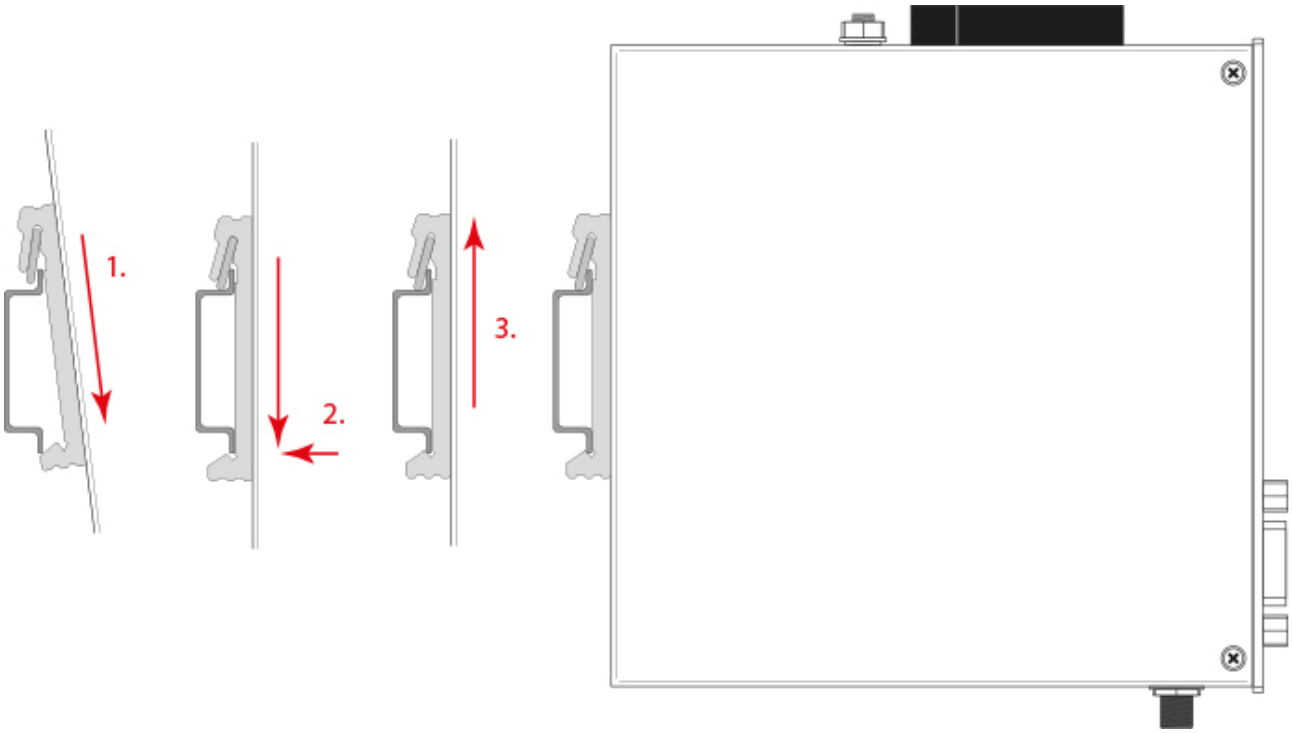
The router may be only mounted vertically as described.

NOTICE

Non-compliance with the minimum distances can destroy the device at high
ambient temperatures!



Top hat rail mounting

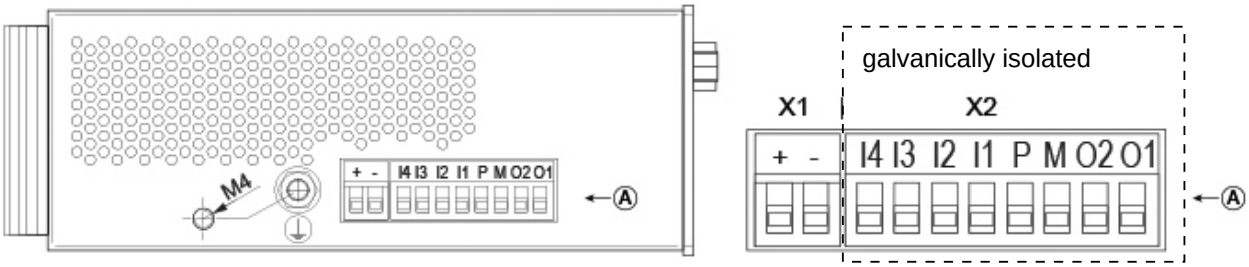


Click the router into the DIN top hat rail. To do this, attach the upper guide to the top hat rail and then press the router down against the top hat rail until it fully engages.

14 Starting the router

NOTICE

Before you connect the router to a network or a PC, make sure that the router is properly connected to the power supply. Otherwise, other devices may be damaged.



1 Connect the equipotential bonding to the grounding screw on the top side of the router.

2 Connect the power supply (10-30 V DC) to **terminals X1** of the router.

NOTICE

Ensure polarity is correct!

3 Now, switch on the power supply.

- After switching on the power supply, the **Pwr**LED is permanently lit.
- After about 90-120 seconds (depending on the device type), the **Rdy** LED is permanently lit.

4 The ***mbNET*** is now ready for operation.

TIP

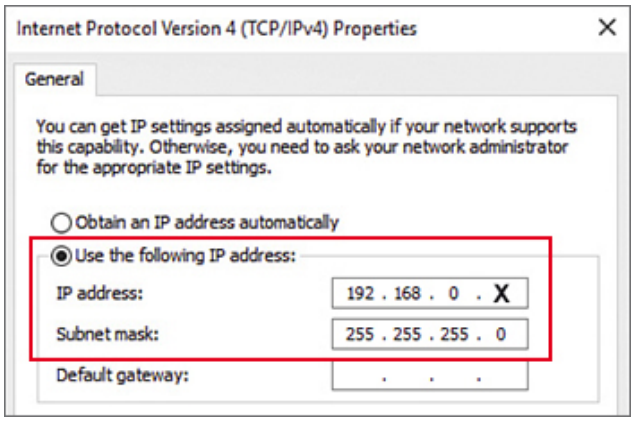
You can obtain further information about the ***mbNET*** industrial router and support on our homepage in the Support-Forum at www.mbconnectline.com

15 Connect router to configuration PC

You can access the web interface of the mbNET directly via a PC.

Requirement:

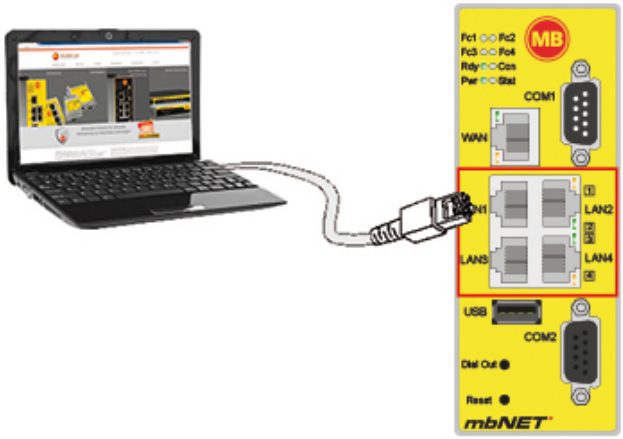
- PC with network card
- Internet browser (HTML5 compatible)
- The IP address of the computer must be in the same network as the mbNET - 192.168 in this case. 0 . X (X = variable) - and not be occupied by any other network user.
- The netmask must be 255.255.255.0.



NOTICE

The step-by-step guide on how to perform the required settings on a PC can be found in the appendix of this document.

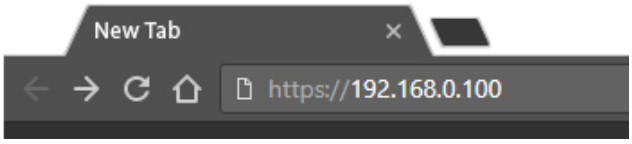
When your mbNET is ready for operation (LED Pwr + Rdy light up), connect the PC to one of the LAN interfaces of the device. To do this, use the supplied network cable.



16 Calling up the mbNET web Interface

Start the Web browser on your PC and type the required IP address of the router in the address bar.

Factory setting is: 192.168.0.100



NOTICE

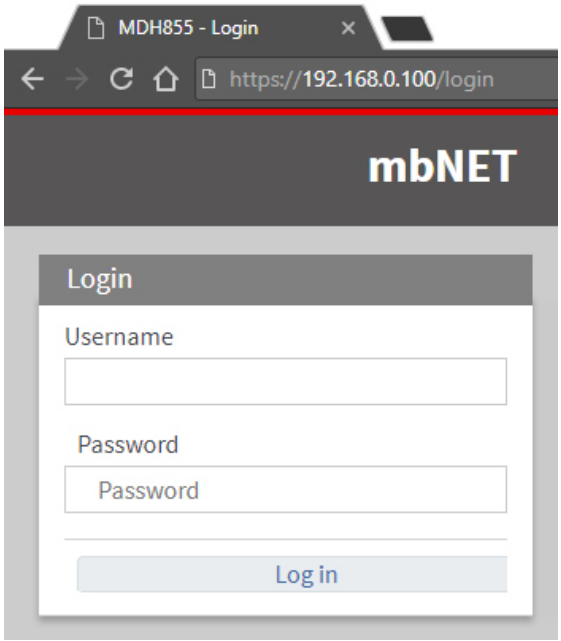
Please note that access to the web interface is possible only via the HTTPS protocol (https://192.168.0.100).

Log in to the router -
Factory setting is:

User name: admin

Password:
You will need the individual device password (Default Password). The device password can be found on the back of the mbNET.

USER: admin
DEFAULT PASSWD:
47mxfFQrJ4



17 First Start

When you first start the device web interface, you can choose how you want to use your mbNET in the future:

- **Cloudserver**
  When selecting "Portal Server" the ***mbNET*** is linked to the ***mbCONNECT24*** portal and configured and operated from there.

  If you want to preconfigure the ***mbNET*** to connect to the ***mbCONNECT24*** portal, click on the "**Cloud-server**" button.
  The following menu allows you to specify the connection data with which ***mbNET*** can log on to the portal, to “pick up” its provided portal configuration.

NOTICE

This step is optional and can be skipped because the mbNET can be configured directly from the mbCONNECT24 portal.
To cancel this operation, simply unsubscribe from the web interface (*admin* > *Logout*).

Information about the benefits of using mbCONNECT24 can be found on our website www.mbconnectline.com or contact your MB connect line distribution partner.

- **Classic Router**
  Selecting "classic router" creates a separate router without connecting to the mbCONNECT24 portal.
  Configuration of the mbNET is done completely via the device web interface.
  It is also possible to create your own VPN connections.

  By clicking on the "**classic router**" button, you will be automatically redirected to the mbNET configuration interface, where you can configure the mbNET fully for its intended use.

NOTICE

A decision about whether you want to operate in the mbNET portal or as a classical router can only be changed by resetting to the factory setting.

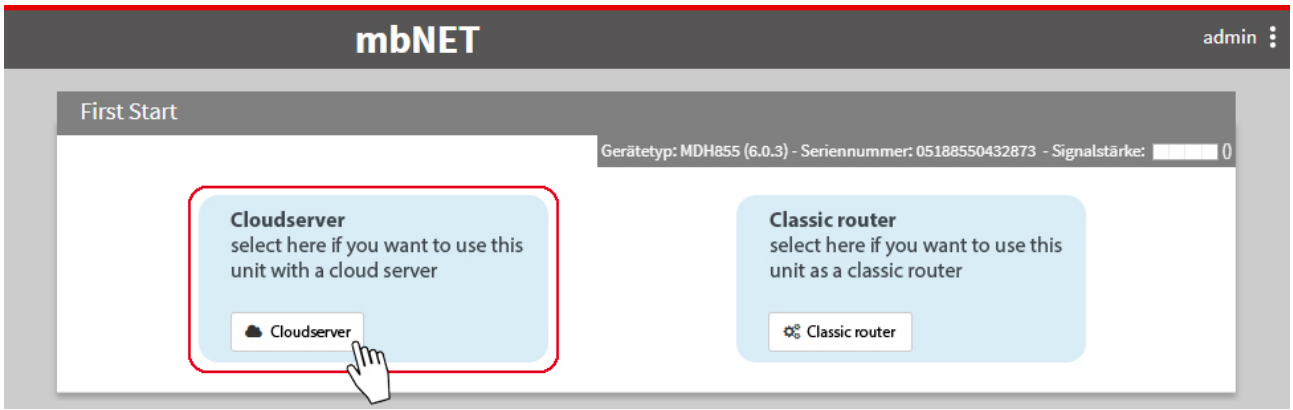
18 Portal server - First start

Setting the connection data to the portal server (optional)

NOTICE

This step is optional and can be skipped because the mbNET can be configured directly from the mbCONNECT24 portal.
To cancel this operation, simply logout from the web interface (*admin* > *Logout*).

Information about the benefits of using mbCONNECT24 can be found on our website www.mbconnectline.com or contact your MB connect line distribution partner.



Use the **Cloudserver** to configure the mbNET for a connection

a) to the Internet and

b) to the mbCONNECT24 portal.

With this connection data, once mbNET is connected to the Internet and can establish a connection to the mbCONNECT24 portal, it can "pick up" its configuration provided in the portal.

Requirements:

- You have a mbCONNECT24 user account
- and you have created the mbNET as a new device (with its serial number) in your user account.

NOTICE

You can get support with the configuration of your mbNET in the ***mbCONNECT24*** portal

- in the mbCONNECT24 online help
- or in our help desk.

18.1 Internet - Configuring the Internet connection

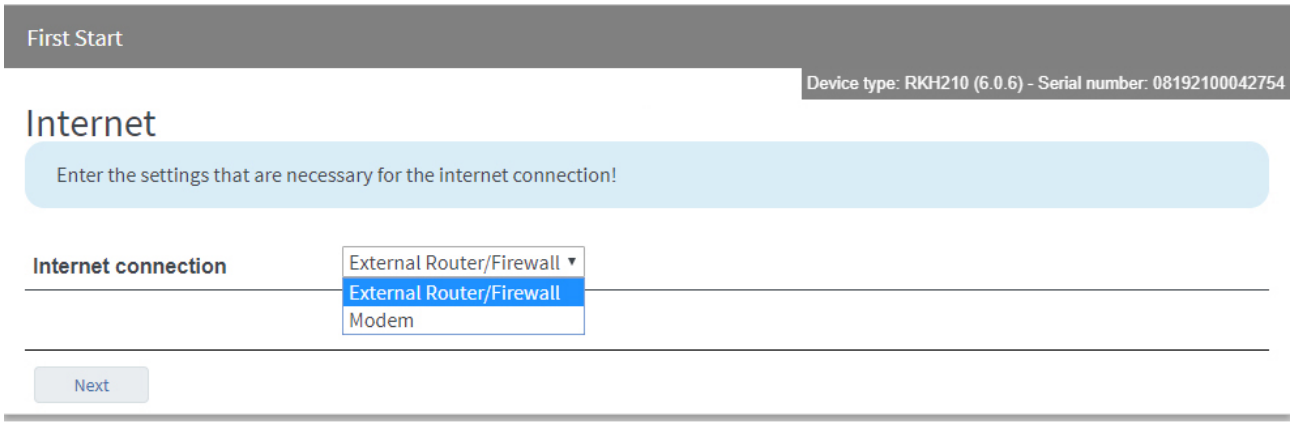


Image 6: the selection may vary depending on the device type

Here, you can select how to connect to the Internet. And click on "**Next**".

Depending on the device type, the selection is

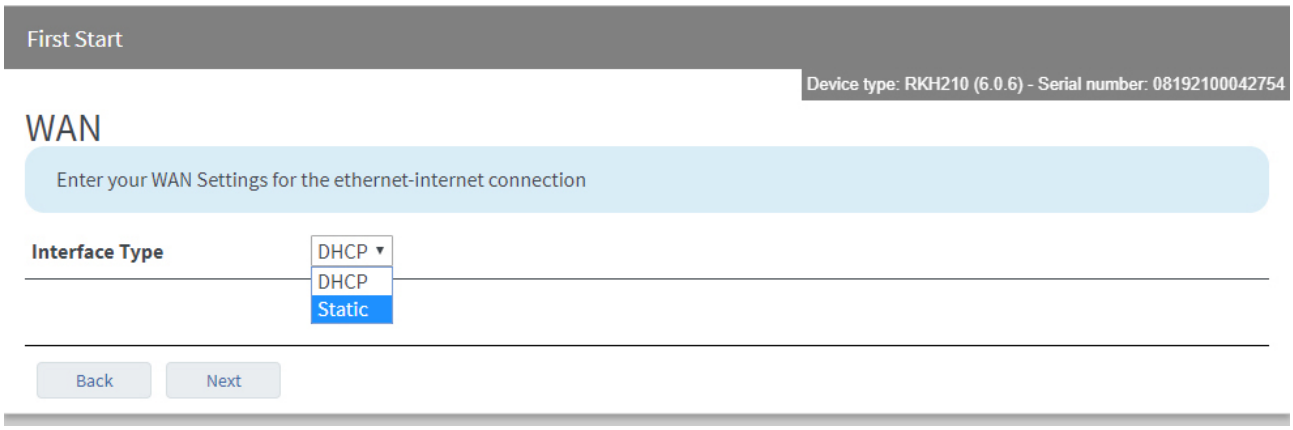
- **External Router/Firewall**
- **Modem**

18.1.1 External Router/Firewall WAN settings

Interface type selection

Options are:

- **DHCP**
- **Static**



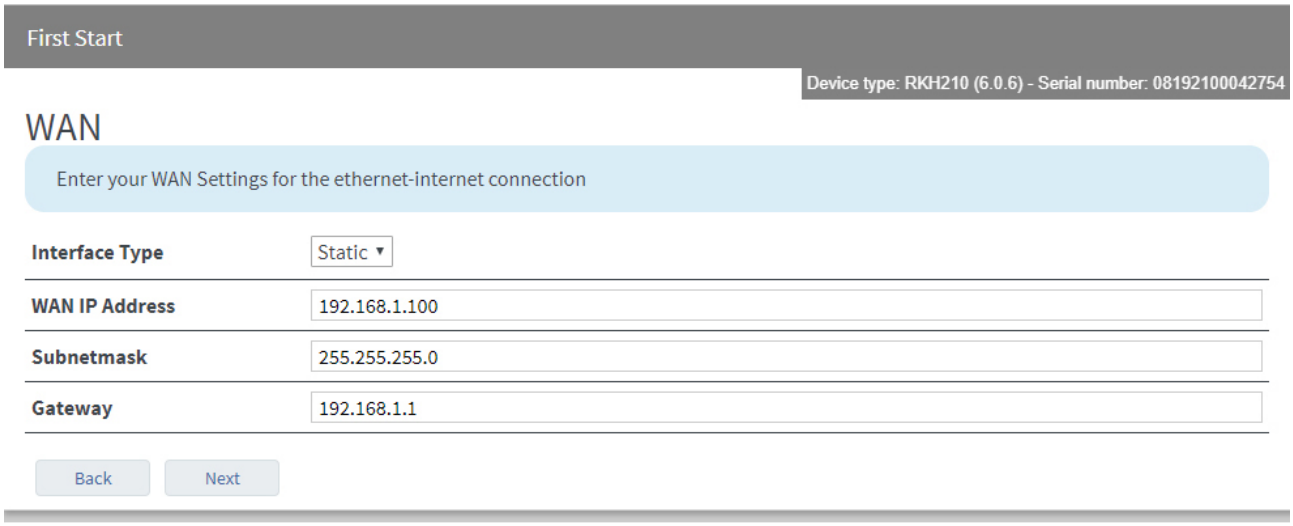
DHP

If interface type **DHP** is selected, the router receives its connection information such as IP address and subnet mask via DHCP.
No further settings are required.

Clicking on "**Next**" will take you to the **Portal Server settings**.

Static

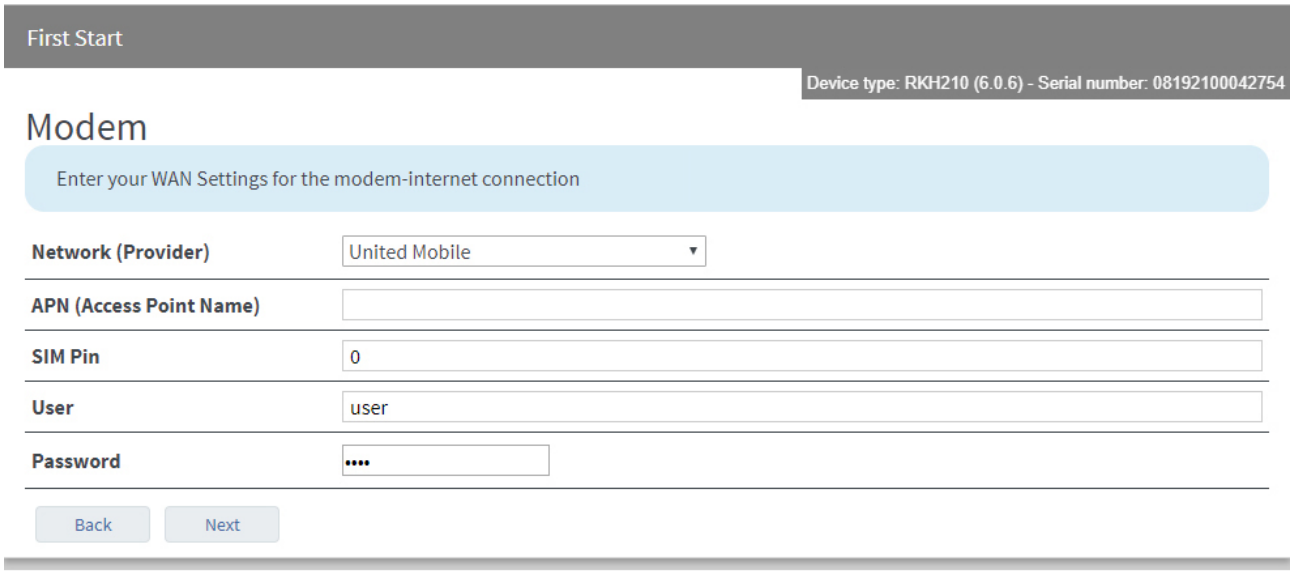
If interface type **Static** is selected, enter your WAN settings for the Ethernet-Internet connection.



Designation	Description
Interface type	Selection field for the interface type: - DHCP - Static
WAN IP address	Enter the WAN IP address.
Subnet mask	Define the subnet mask.
Gateway	Enter the IP address of the gateway.

Clicking on "**Next**" will take you to the **Portal Server settings**.

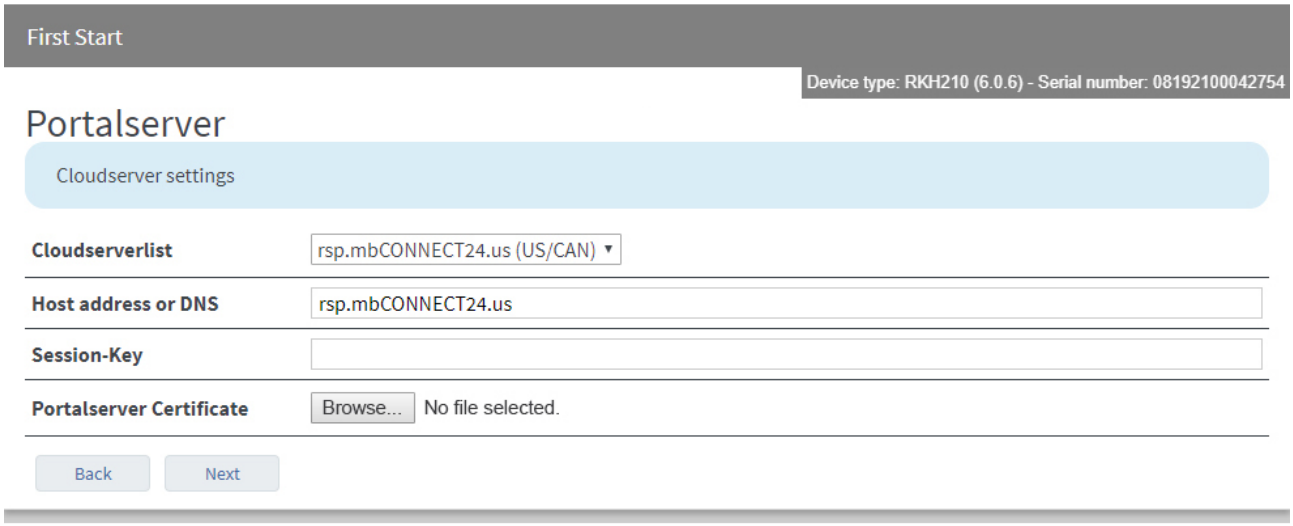
18.1.2 Modem Connection Settings



Designation	Description
Network (provider)	Selection field for the service provider
APN (Access Point Name)	Enter the APN of your provider here, if necessary.
SIM Pin	Enter the SIM PIN of the SIM card used.
User	If necessary, enter your user name and password.
Password	

Clicking on "**Next**" will take you to the **Portal Server settings**.

18.2 Portal Server - Settings



Designation	Description
List of portal servers (For more information see the "mbCONNECT24 Server List" table)	List of available portal servers: • **rsp.mbconnect24.net (EU)** • **rsp.mbconnect24.us (US/CAN)** • **rsp.mbCONNECT24.asia (ASIA)** • **rsp.au.mbCONNECT24.net (AU)** • **User defined**
Host address or DNS name	The matching host address of the portal server selection will be shown here. When you select "**User defined**" you must enter the host address or DNS name of your portal server.
Session Key	If you have set a session key when providing the portal configuration, you must enter the session key here.
Portal Server Certificate	When you select "**User defined**" from the list of portal servers, you can select a CA certificate here. Self-issued certificates must be previously integrated in the setup menu of the router (System > Certificates).
Click"**Next**" to complete the setup.	

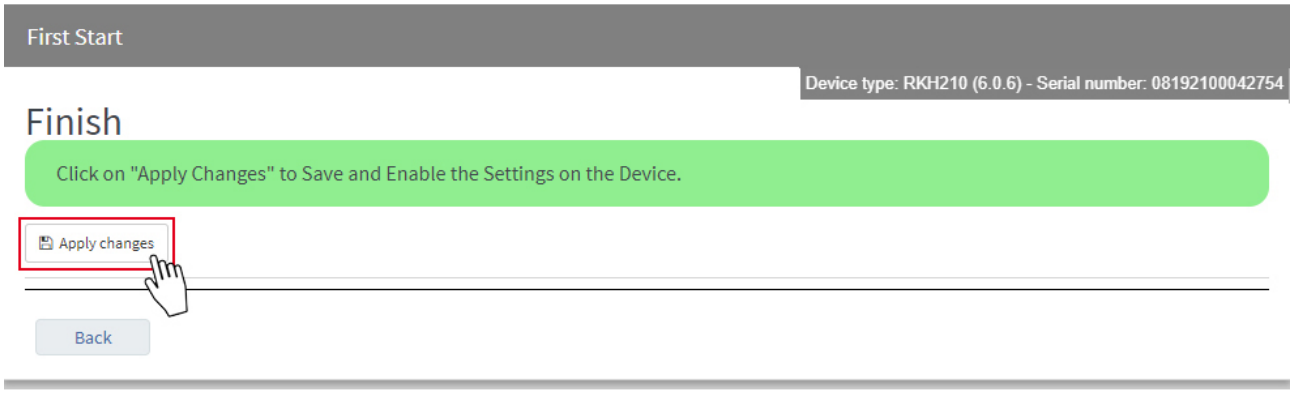
mbCONNECT24 server list		
Server name	**Host Address** or **DNS Name**	**Note**
rsp.mbCONNECT24.net (EU)	rsp.mbCONNECT24.net	Remote-Service-Portal mbCONNECT24 **V2*** - server location: Europe
rsp.mbCONNECT24.us (US/CAN)	rsp.mbCONNECT24.us	Remote-Service-Portal mbCONNECT24 **V2*** - server location: USA
rsp.mbCONNECT24.asia (ASIA)	rsp.mbCONNECT24.asia	Remote-Service-Portal mbCONNECT24 **V2*** - server location: Asia
rsp.au.mbCONNECT24.net (AU)	rsp.au.mbCONNECT24.net	Remote-Service-Portal mbCONNECT24 **V2*** - server location: Australia
User defined	*customer-specific*	**my**mbCONNECT24

Table 1: mbCONNECT24 server list

* The Remote-Service-Portal mbCONNECT24 V2 is the current version for secure remote maintenance, data acquisition, M2M communication and networking via the Internet.

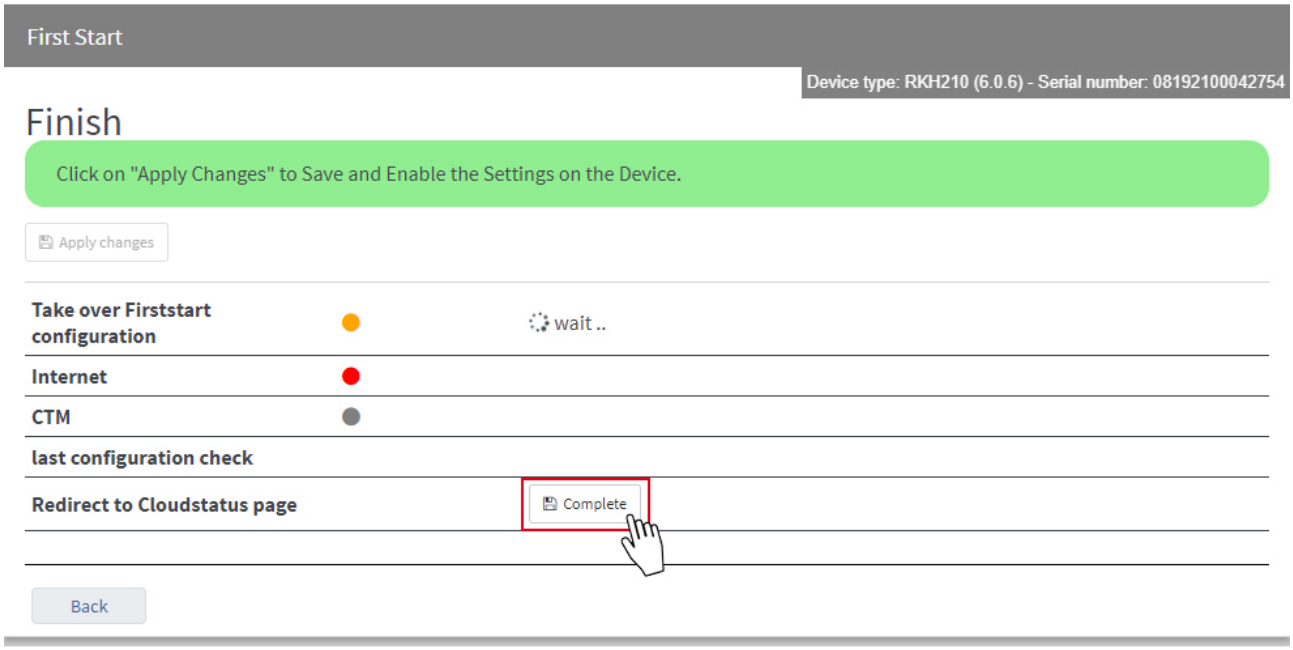
18.3 Finish - Apply settings

Save changes



Save the settings by clicking on "**Save Changes**".

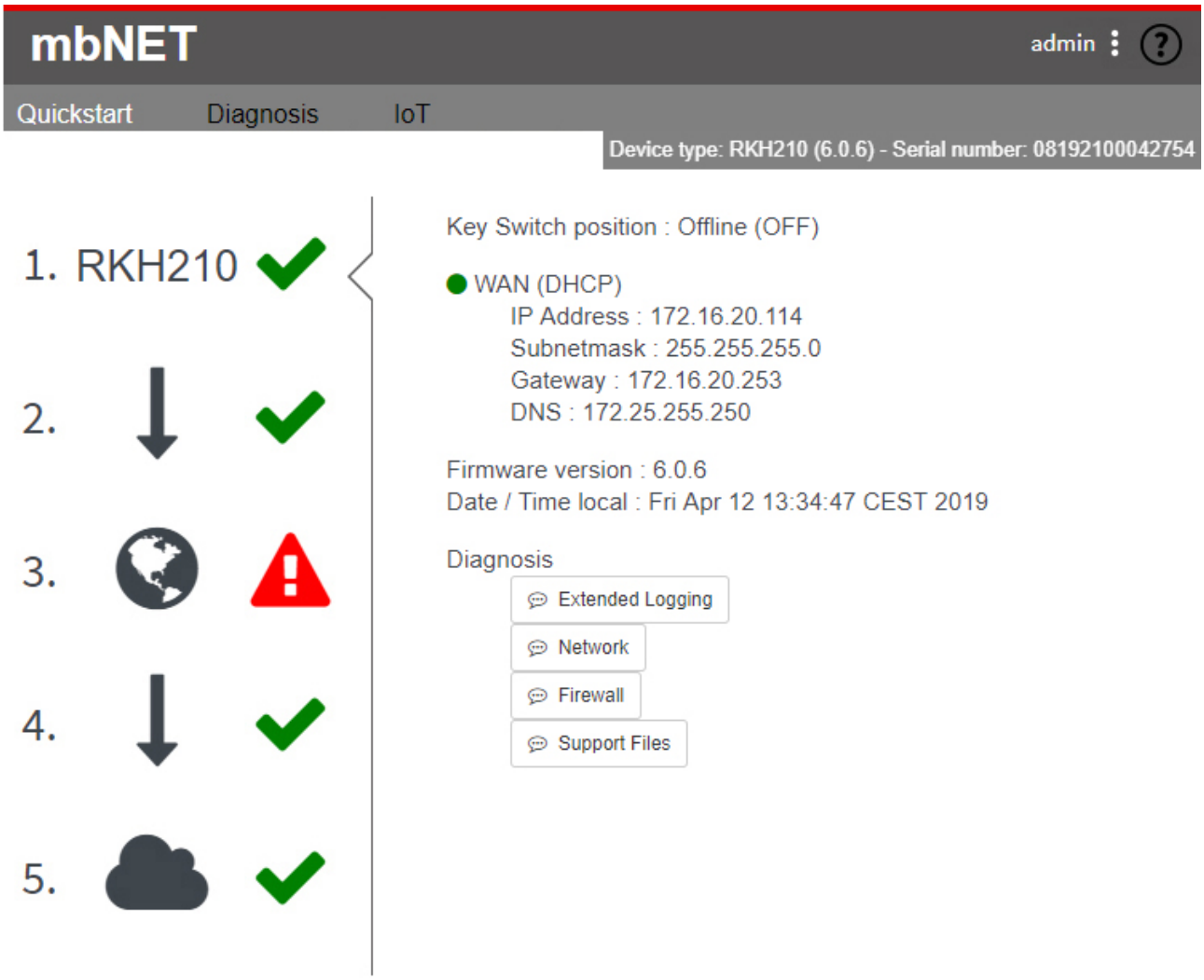
Complete



Click"**Complete**" to complete the process.
You will be taken to the "**Cloudstatus Page**" (**Quick start**). Here you can find information (including connection errors and their cause) for each connection to the Internet, and the Portal Server.

19 Quick Start - Cloud Status Page

19.1 Quick Start



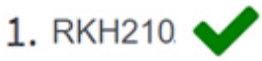
This display appears

a) each time you call up the mbNET web interface, if you have created the mbNET as a portal device

b) from the configuration interface via the "admin" Menu

Here, you can detect connection errors and determine the cause. To obtain more detailed information, click on the respective icon.

If there is an error during connection or in the network settings, a red triangle is displayed. If it is correctly configured, the points are shown with a green tick.



In **Step 1**, you will receive an overview of interfaces and general system information.

Step 2 provides information about the status of the connection to the Internet.

3. In **Step 3**, you will see the result from the DNS and NTP check as well as the port check (port 80/443/1194) for the remote maintenance portal.

4. **Step 4** displays the status of the connection to the portal server.

5. In **Step 5**, you will receive a connection overview for the portal server.

- Portal Server
  Account name: sample company
  Device name: MDH831WiFi

- CTM no config available
  Last update of the configuration:
  last configuration check:
  ▶ CTM start

  Click on the "Start CTM" button to initiate a manual query for an available portal configuration.
  If there is an available, portal configuration, this will be transferred to the mbNET.

- Portal User:

  If a user has an active user portal connection to this device, the user name will be displayed here and the LED icon changes colour to green.

19.2 Diagnosis

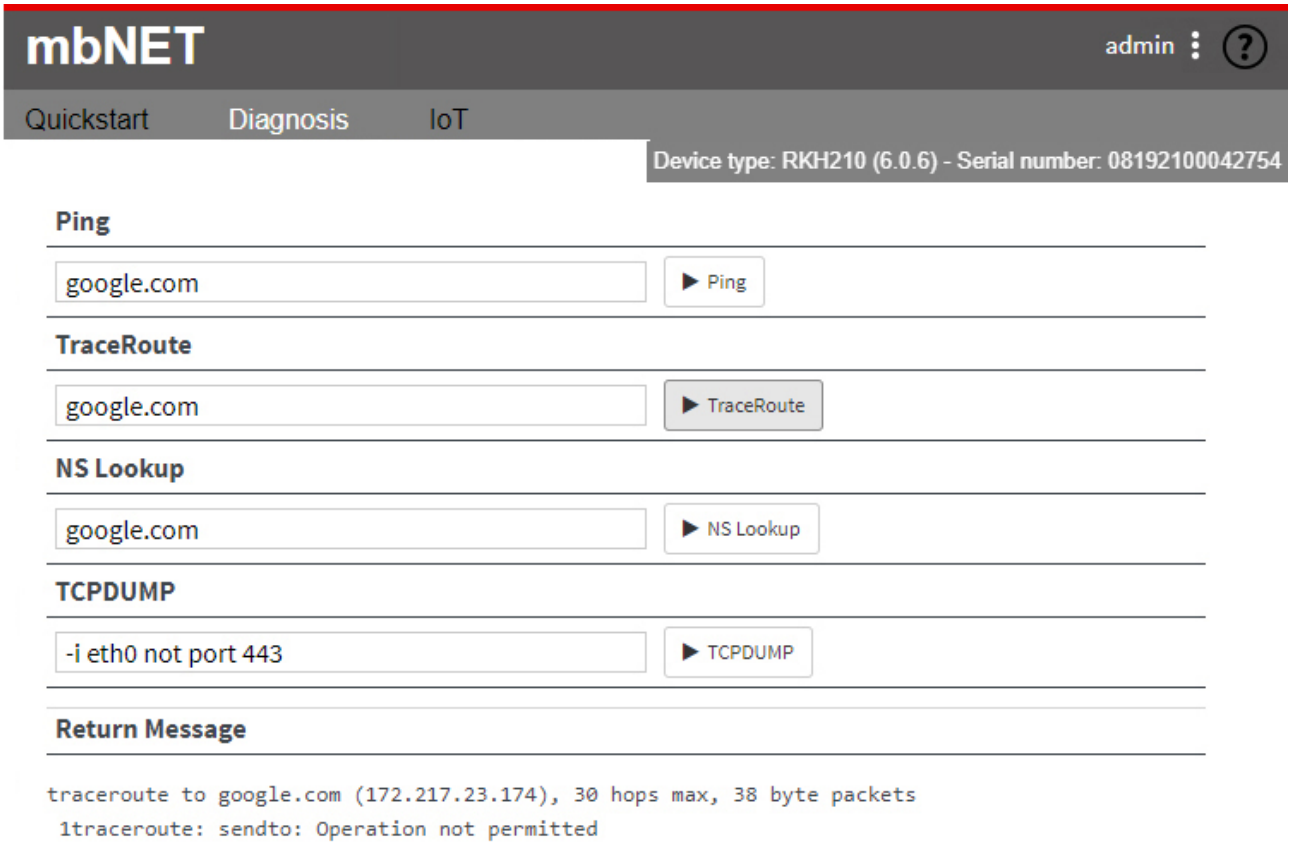
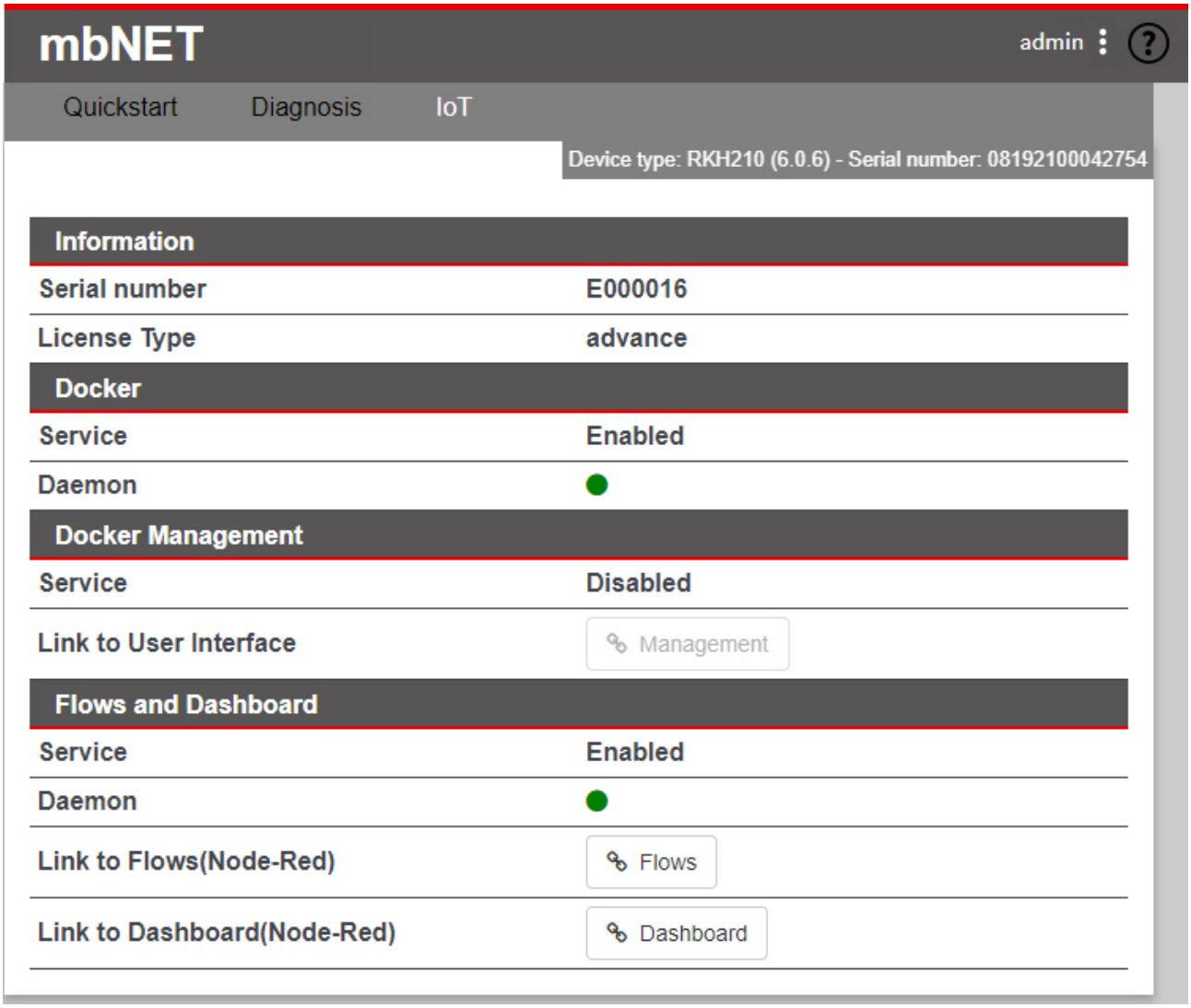


Image 7: Diagnostic example with executed command: Route monitoring

Designation	Description
Ping	After entering an internet address or an IP address, you can use the ping command (Click on the "**Ping**" button) to determine whether the corresponding address is accessible. Among other things, for example, you can easily determine whether an Internet connection exists.
Route monitoring	This command provides you with detailed information about the network connection between the mbNET and a remote host or other routers. Route monitoring is carried out and made visible here.
DNS names resolve (nslookup)	With this function, you can check whether name resolution (https://www.google.de = 216.58.209.206) takes place. If after executing the command “DNS name resolve(nslookup)” no result is output, check whether in your mbNET a DNS server address is entered under network-DNS, or if the DNS server of your network is accessible.
TCPDUMP	In order to closely monitor the network traffic, you can use the "**TCPDUMP**" command. Some examples of the use of this command are: • **-i eth0 not port 80** Displays all TCP/IP connections to the (-i) LAN (eth0) interface, except (not) those using Port 80 (port 80) when incoming or outgoing. • **-i eth1 port 23** Displays all TCP/IP connections to the (-i) WAN (eth1) interface using Port 23 (port 23) when incoming or outgoing. • **-vvv -i eth1** Displays all traffic in verbose mode, Level3 (-vvv) on the (-i) WAN (eth1) interface. You can find detailed TCPDUMP documentation at www.tcpdump.org
Port Check	You can use this function to check the status of a port (open / not open) in connection with an Internet or IP address.

19.3 IoT



Here you can see an overview

- of the serial number and the license type of the ***mbEDGE*** SD card used
- of the status of the IoT service (Docker)
- of the Docker Management Status
- of the status of activation for Flows and Dashboard

Click on the "Flows" button to get to the NodeRed working environment.

Use the "Dashboard" button to call up a previously created dashboard.

NOTICE

Information on the configuration and setting options of **mbEDGE** can be found in the relevant manual on https://www.mbconnectline.com/de/support/downloads.html

20 Classic router - *configuring the mbNET via the web interface* -

If you use the ***mbNET*** as a classic router, the complete configuration and setup is performed via the web interface of the device.

20.1 Description of the graphical user interface (configuration interface)

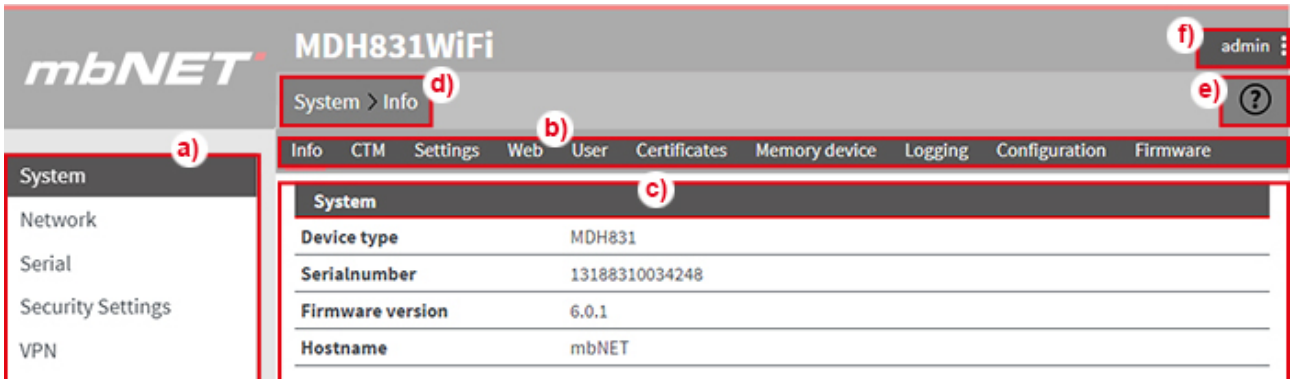
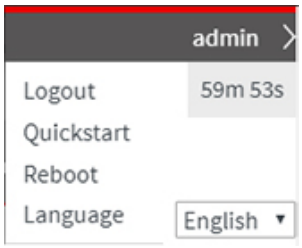


Image 8: Basic structure of the graphical user interface

a)	Main Navigation	First-level navigation for the operational user interface.
b)	Subnavigation	Second-Level-Navigation
c)	Display/work area	Here, you will perform all the configuration settings.
d)	Breadcrumb navigation	Displays the user and branch within the user interface.
e)	Help button	Link to online help for devices.
f)	User navigation  	Navigation for the administrative user interface. **Log out**: This is where you log out of the system properly. In addition, a timer is displayed. If there is no activity on the surface, you will be logged out automatically after the preset time (60 minutes). Clicking on the timer will reset it to 60 minutes. **Quick start/ Administration**: Link to "Quick Start"/to configuration Interface **Reboot**: If you click on this link, ***mbNET*** will be restarted. **Language**: Selection field for the user language of the web interface The options are: German and English

20.2 Description of buttons, icons and fields

Here, you will find an overview of the display elements, input/selection fields and buttons.

Symbol	Description
	Display element- greyLED example: a link is inactive, a cable or USB device is not connected, Output1 is inactive etc.
	Display element- greenLED example: a link is active, a cable or USB device is connected, Output1 is active etc.
	Display element- redLED **example:** inactive connection, WAN cable is not plugged in, etc.
	Checkbox for enabling/disabling the associated function.
	Input field for manual input of information/values.
S7_ISOTCP	**Selection field/Drop-down list** to select a predefined value/parameter.
	The Edit**button** can be used to change input/values in an element/row.
	Button for adding a new element (e.g. a new rule in the security settings or new VPN connection)
	An element/row is deleted by clicking the Delete**button**.
Save	Clicking on the **"Save" button** temporarily saves the current entries/changes. **However, the changes are not active**.
Close	Clicking on the **"Close" button** discards the current input/changes.

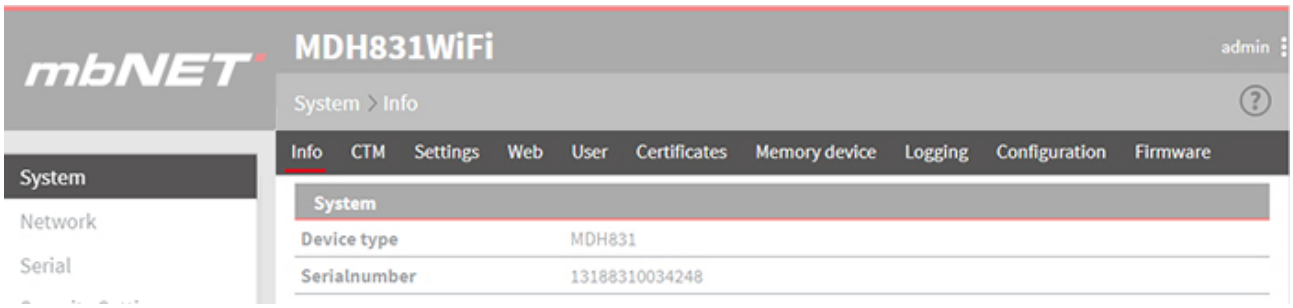
NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

Apply changes	Clicking on the **"Save changes" button** will apply all stored settings/changes and store them permanently on the router.
Clear Changes	The "**Discard changes** "**button** will reset/discard all temporarily stored settings/changes.

21 System - settings and basic router configuration

Here, you will find general system information and settings.



Under the **System** menu the following submenus are listed:

Submenu	Description
Info	General system information
CTM*	Configuring the CTM (Config Transfer Manager).
Settings	General system configuration (e.g. time and mail settings).
Website	HTTPS access configuration in the ***mbNET***web interface.
User	User management (password and rights management)
Certificates	Creating and managing certificates.
Storage media	Configuring the USB port and SD card slots.
Logging	Settings for the logging function.
Configuration	Backing up and restoring the device configuration.
Firmware	Updating the Firmware (firmware upgrade).

* The CTM function is only relevant if you are running the ***mbNET*** in the mbCONNECT24 portal (Cloudserver). This function is described in the mbCONNECT24 online help.

21.1 System > Info

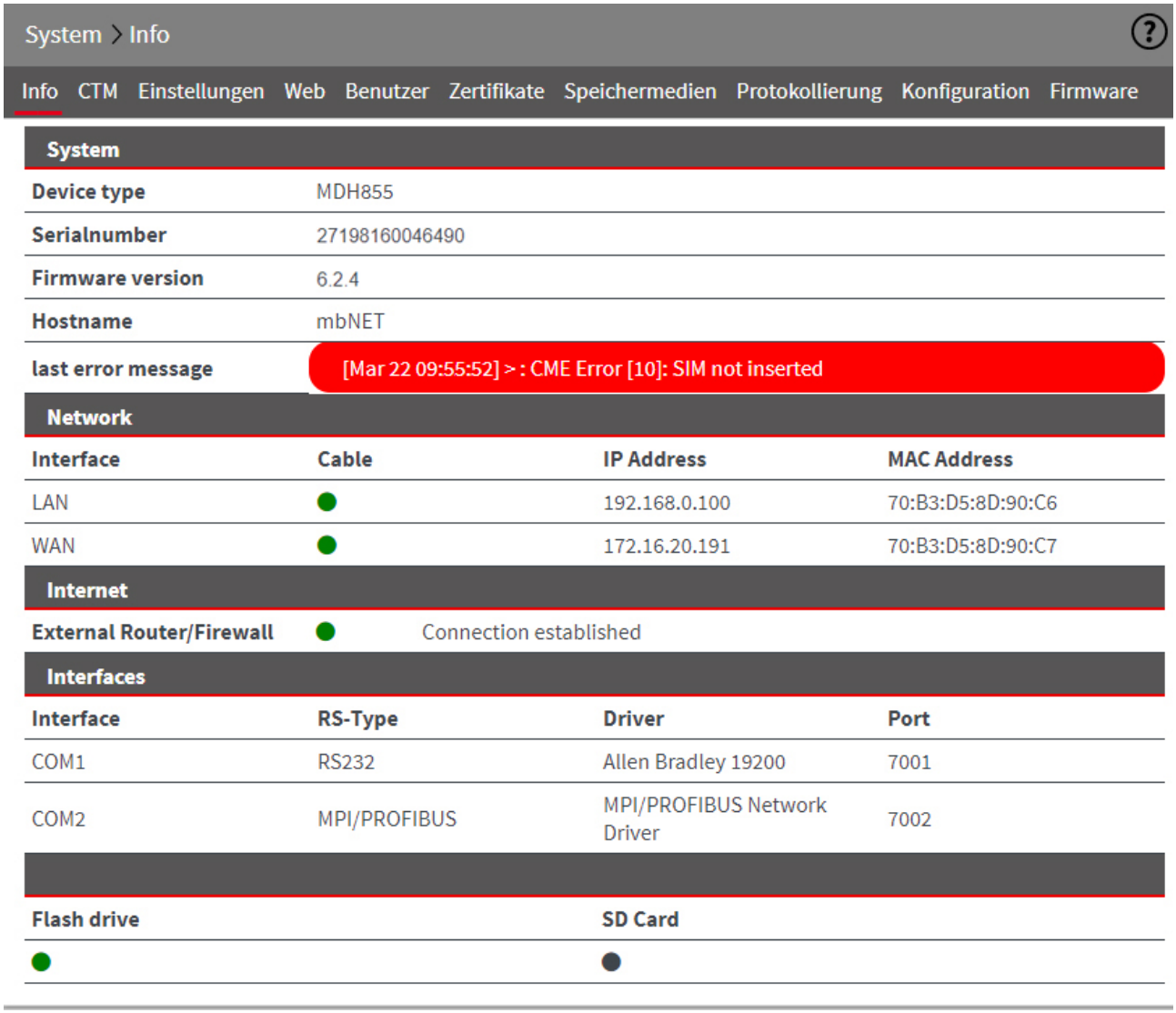


Image 9: Example display, content can vary depending on the type of device.

System	Here you will find information about • Device type • Serial number • Firmware version • Device name in the network Warnings or/and the most recent error are also displayed here.

Network	Here you will find information about • **Interface** LAN and WAN displays which network ports are linked/connected at the moment to the existing network via the corresponding sockets. An existing connection is indicated by a green icon.

Internet	Here, you can see • the selected **Internet connection** ° External Router/Firewall ° DSL ° Modem ° Wi-Fi • The **connection status** A currently active connection to the Internet is represented by the green LED icon.

Interfaces	Here, the current configuration of the COM1 * and COM2 * interfaces is displayed.
	If you operate a device with a MPI/PROFIBUS connection, the information will be displayed in COM2. * depending on the type of device and equipment.

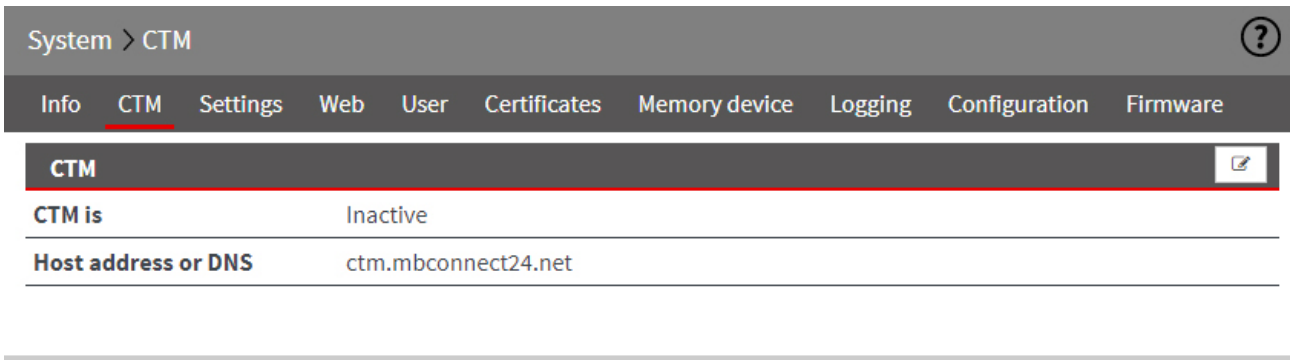
Storage media	Status of the USB port and SD card slot
	When a USB flash drive and/or an SD card is inserted in mbNET, this is indicated by the green LED symbol.

21.2 System > CTM (Configuration Transfer Manager)

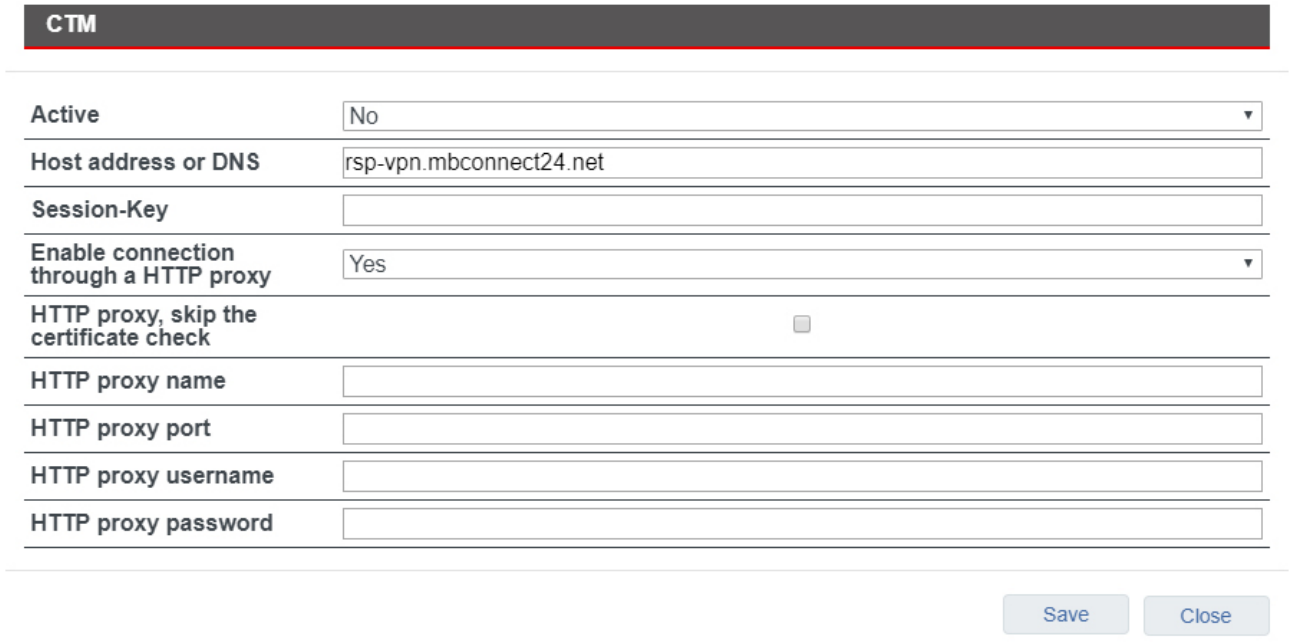
The CTM allows the ***mbNET*** to transfer the portal configuration via the active Internet connection, i.e. the ***mbNET*** picks up its configuration from the ***mbCONNECT24*** portal, as soon as it comes online. In order to ensure the transfer, CTM must be activated on the ***mbNET***.

NOTICE

The CTM function is only relevant if you are running the router in the ***mbCONNECT24*** portal (Cloudserver). This function is described in the ***mbCONNECT24*** online help.



Click the Edit icon to edit the corresponding function.



Designation	Description
Active	"Yes / No" selection field to activate/deactivate this function.
Host address or DNS name	Enter the host address or DNS name.
Session Key	Enter the session key generated by the portal.
Use a HTTP proxy server as the outgoing connection	"Yes/No" selection field - select "Yes" if you want to use an HTTPS proxy server as the outgoing connection.
HTTP proxy, skip the certificate check	Check box for enabling/disabling this function. *"**SSL termination*** *An HTTPS connection can be broken down (scheduled) by means of a web proxy in order to also check its contents for pests. Further encryption to the client (browser) then takes place with a certificate offered by the proxy. The problem with this is that the user of the browser no longer gets to see the original certificate of the web server and has to trust the proxy server that he has taken a validation of the web server certificate."*[1] One way to avoid this problem is to enable this feature.
Name of the HTTP proxy server (DNS or IP)	Input field for the host name or the IP address of the proxy server.
Port of the HTTP proxy-server	Input field for the port.
Login name on the HTTP proxy server	User name input field If required, the domain name (domain\username), as well as the authentication method are also here (for "NTLM": Username#AUTH-NTLM or for "NTLMv2": Enter Username#AUTH-NTLM2).
Login password on the HTTP proxy server	Server password input field

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

[1] Proxy (Rechnernetz), https://de.wikipedia.org/wiki/Proxy_(Rechnernetz), 18.01.2018

21.3 System > Settings

System > Settings

Info | CTM | Settings | Web | User | Certificates | Memory device | Logging | Configuration | Firmware

System settings	
Hostname	mbNET
Host Description	mbNET
Automatic reboot	inactive
Reboot at	00:00
Time Settings	
Date Time (UTC)	Mon Jul 20 19:19:12 UTC 2020
Locale Date Time	Mon Jul 20 21:19:12 CEST 2020
Set locale Date Time	
Timezone	Berlin,Germany
NTP Settings	
Time synchronization over NTP	inactive
Server address	0.de.pool.ntp.org
Update interval (h)	2
NTP Server on LAN	inactive
Mail Settings	
Activate automatic Mail	Yes
Device-API	
Enable MQTT access to status topcis	No
System Services	
Networkconfiguration disable (Conftool)	No
SimplyConnect (SC3) service enable	Yes
Manufacturer access enable	No

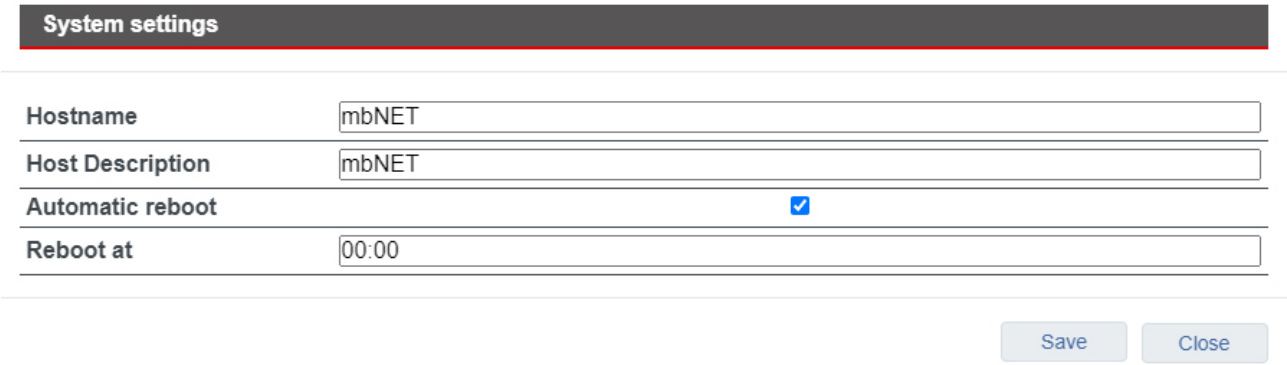
In the **Settings** submenu you can configure the following functions:

Function	Description/content
System settings	• Assign a device name in the network • Configure a device reboot
Time settings	• Set the local time (date/time) • Select the time zone
NTP Settings	• NTP configuration • NTP Server on LAN => the mbNET acts as an NTP server here.
Mail Settings	Configuring the "Automatic Mail Setting" function
Device-API	Enable MQTT access to status topcis "No / Yes"

Function	Description/content
System Service	• Disable network configuration (Conftool) "No / Yes" • SimplyConnect (SC3) service enable "Yes / No" • Enable manufacturer access "No / Yes"

Click the Edit icon , to edit the corresponding function.

21.3.1 System > Settings > System Settings



Designation	Description
Hostname	Enter here a name that allows the router to be reached on the network.

NOTICE

The mbNET can only be reached under this Hostname, if the DNS server that is registered on your PC knows the device name and the IP address of the mbNET.
If the DNS server is an mbNET, you must observe the following: In order to reach the network name of the mbNET by a PING from your PC, you'll need to add at the end an (".") (e.g.: ping myrouter.).

Host Description	To better identify the router on a network, you can enter a meaningful description here.
Automatic reboot	Checkbox to activate / deactivate the reboot function.
Reboot at	Enter a time here at which the device is to be restarted automatically. 24 hour format: hh : mm | 12-hour format: hh : mm AM / PM

NOTICE

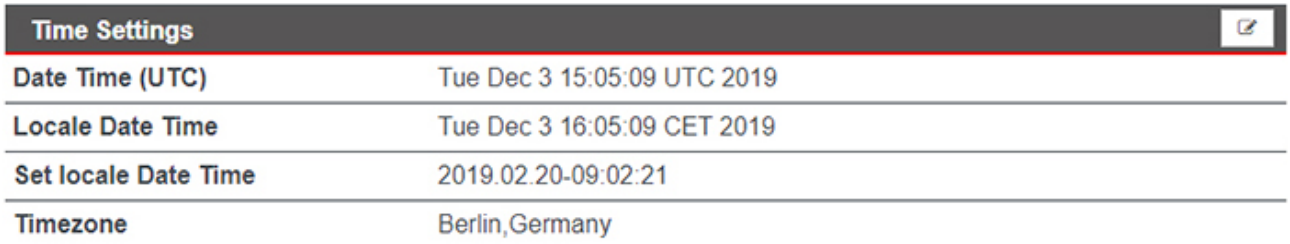
If there is an active connection for a restart at the specified time, the restart is delayed until the active connection is ended.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

21.3.2 System > Settings > Time Settings



Designation	Description
Date/Time (UTC)	Displays the current system time in UTC (Coordinated Universal Time).
Local Date Time	Displays the current system time based on the selected time zone.
Set local Date Time	Displays the system time, which is used, if no automatic time adjustment is to take place, or is not possible. Input format: YYYY.MM.DD-HH:MM:SS
Timezone	Displays the time zone in which the mbNET is operated.

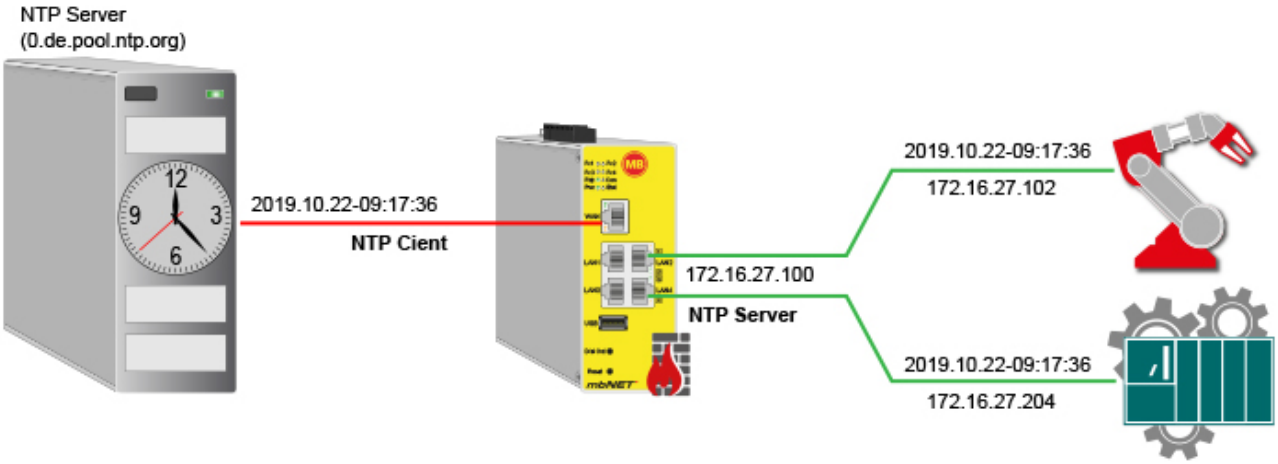
Designation	Description
Date/Time (UTC)	Displays the current system time in UTC (Coordinated Universal Time).
Local Date Time	Displays the current system time based on the selected time zone.
Set local Date Time	Enter the system time here, if no automatic time synchronization is possible or is to take place. Input format: YYYY.MM.DD-HH:MM:SS
Timezone	Select the time zone from the selection field, in which the mbNET is operated.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

21.3.3 System > Settings > NTP Settings



The Network Time Protocol (NTP) is a standard for synchronizing clocks in computer systems via package-based communication networks. When time synchronization, the NTP client gets the current time from an NTP server.

The ***mbNET*** can act both as an NTP client and as an NTP server.

NTP Settings	
Time synchronization over NTP	active
Server address	0.de.pool.ntp.org
Update interval (h)	2
NTP Server on LAN	inactive

To change the NTP settings, click the edit icon

Designation	Description
Time synchronization over NTP	Checkbox for enabling/disabling the NTP function. If this checkbox is activated, the mbNET acts as an NTP client.
Server Address	Enter the IP address or the name of the time server (default address: 0.de.pool.ntp.org). When entering a name, a DNS server must be entered in the network settings, or you must be connected to the Internet. The NTP server must be easily accessible.
Update interval (h)	Enter the value for the NTP polling interval (in hours). Input => natural numbers [hr] > 0. **NOTICE** When 0 or "blank" is entered, there is no time synchronization.
NTP Server on LAN	Checkbox to activate / deactivate the function. If this function is activated, the ***mbNET*** transfers its local system time via an NTP server via the LAN interfaces to devices connected to it.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

21.3.4 System > Settings > Mail Settings

In the case of certain events (e.g. from the alarm management) you can send automatically generated messages from the system via email.

Here you set whether the ***mbNET*** should use the mail server of **MB connect line**, with fixed specifications, or whether you want to use your own SMTP server.

Designation	Description
Enable automatic mail settings	"Yes / No" selection field to activate/deactivate this function. If you select "Yes", the router will use the mail server of MB connect line, with fixed specifications. If 'No', you have to enter the information for your mail server (for further information please contact your service provider).
SMTP Server	Enter the IP address or the name of the SMTP server of your mail provider.
SMTP Port	Enter the port via which the E-mails are sent.
E-mail address	Enter the sender address email address here.
SMTP requires Authentification	Activate the checkbox if the SMTP server requires authentication.
User /Password	In these two fields, enter the login information for your E-mail account.

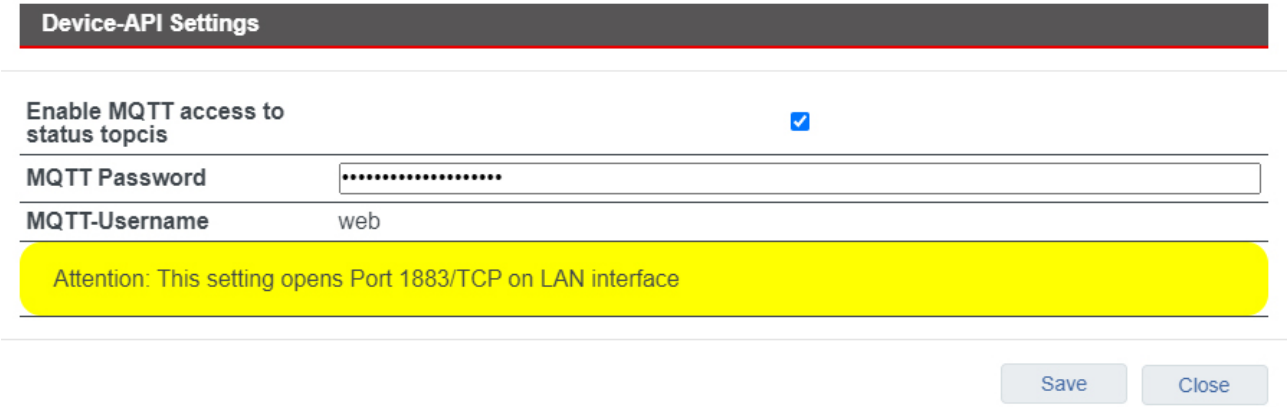
Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

21.3.5 System > Settings > Device-API

The mbNET can be used as an MQTT broker.



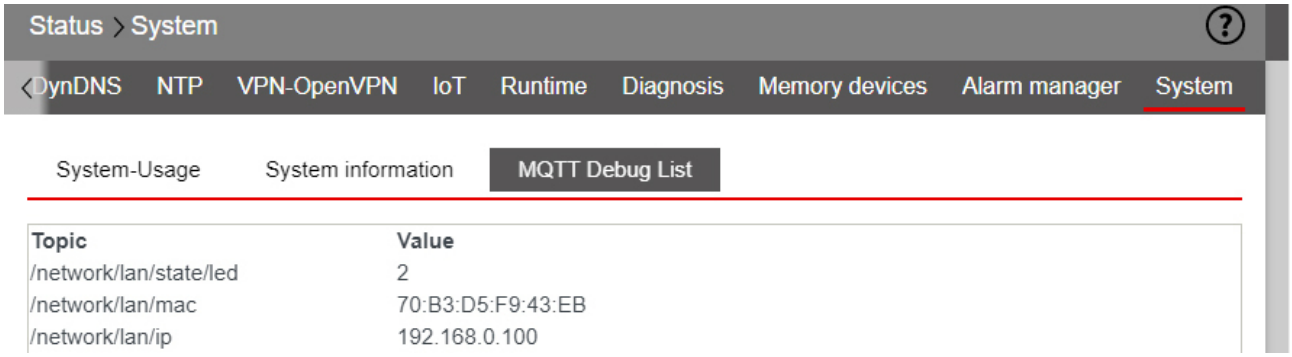
Designation	Description
Enable MQTT access to status topcis	**Checkbox** zum Aktivieren/Deaktivieren dieser Funktion.
MQTT Password	**Mandatory field** for entering a password. No default password is specified here.
MQTT-Username	The default username "web" cannot be changed.

NOTICE

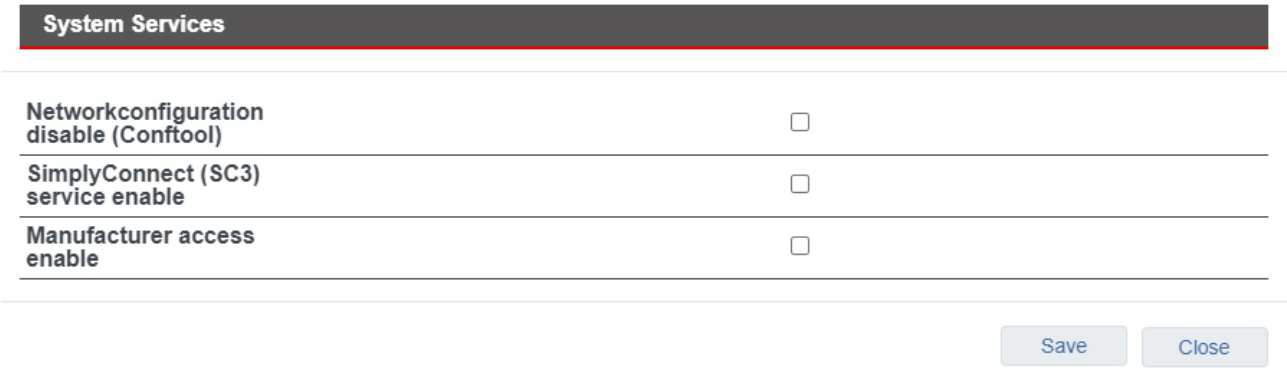
Attention: If this function is activated and the settings are saved, port 1883 / TCP is opened for the LAN interface!

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

After activating the "MQTT access to status topics" function, you can query the values from the "MQTT Debug List" under Status > System.



21.3.6 System > Settings > System Service



Designation	Description
Disable network configuration (Conftool)	Check box for enabling/disabling this function.

NOTICE

The "Disable Network Configuration (Conftool)" function is only relevant if you operate the router on the portal mbCONNECT24. This function is described in the mbCONNECT24 online help.

SimplyConnect (SC3) service enable	Check box for enabling/disabling this function.

NOTICE

The "SimplyConnect (SC3) Activate Service" function is only relevant if you operate the router in the mbCONNECT24 portal.
You can find information about SimplyConnect on our website at www.mbconnectline.com or at https://simply-connect.me.

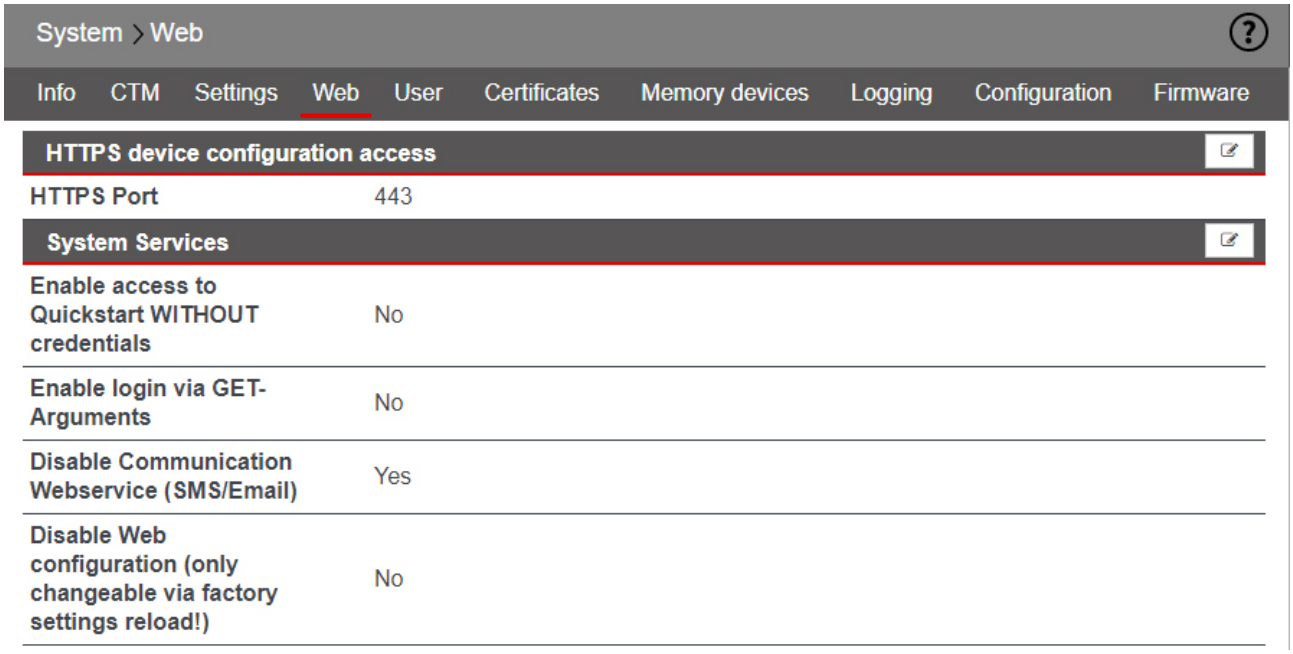
Enable manufacturer system access	Check box for enabling/disabling this function.

NOTICE

Enable this function in a support case when you want to allow the device manufacturer to access the mbNET via SSH. The activation starts the SSH server for the ROOT access to the mbNET, which is handled via PKI.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

21.4 System > WEB



In the **Web** submenu you can configure the following functions:

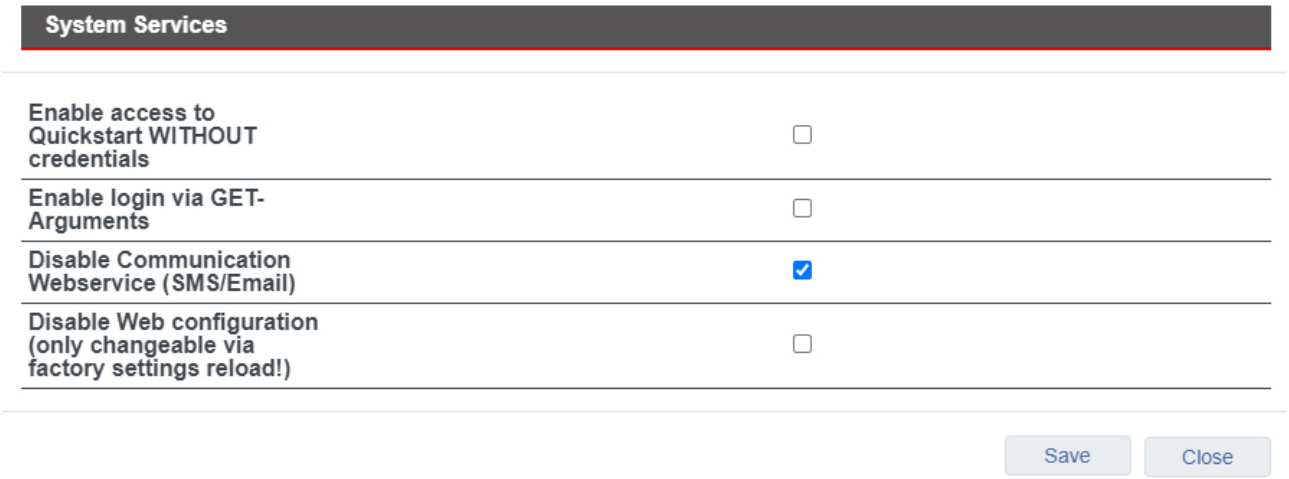
HTTPS device configuration access	
Function	Description/content
HTTPS Port	Here you can • change the default port (443), through which the HTTPS server is accessed. ° **Important!** If you change the default ports, you must specify the new port in the browser's address bar (e.g.:192.168.0.100:**84**). • upload your own certificate • upload a key for the certificate.

System Services	
Function	Description/content
Enable access to Quickstart WITHOUT credentials	This function is only relevant if you operate the router in the mbCONNECT24 portal (Cloudserver). You can find a description of this function in the mbCONNECT24 online help.
Enable login via GET-Arguments	Checkbox to activate / deactivate this function. Beyond the login, no other parameters are taken into account. https://192.168.0.100/login?username=[USERNAME]&password=[PASSWORD]
Disable Communi-cation Webservice (SMS/Email)	Checkbox to deactivate / activate the function. If this function is activated, neither an SMS nor an e-mail can be sent from the device.

System Services	
Disable Web configuration (only changeable via factory settings reload!)	You can disable the complete web configuration here. **ATTENTION**: Once the web configuration is disabled, it can only be restored to its factory settings by rebooting the mbNET.

Click the Edit icon , to edit the corresponding function.

21.4.1 System > Web > HTTPS access for device configuration



Designation	Description
HTTPS Port	Here you can change the default port (443), through which the HTTPS server is accessed. **Important!** If you change the default ports, you must specify the new port in the browser's address bar (e.g.:192.168.0.100:**84**).
Upload own certificate	Select your certificate using the Browse button button.
Upload own key for certificate	Use the Browse button to select your key for the selected certificate.
Import	The selected files are uploaded by clicking the "Import" button.

NOTICE

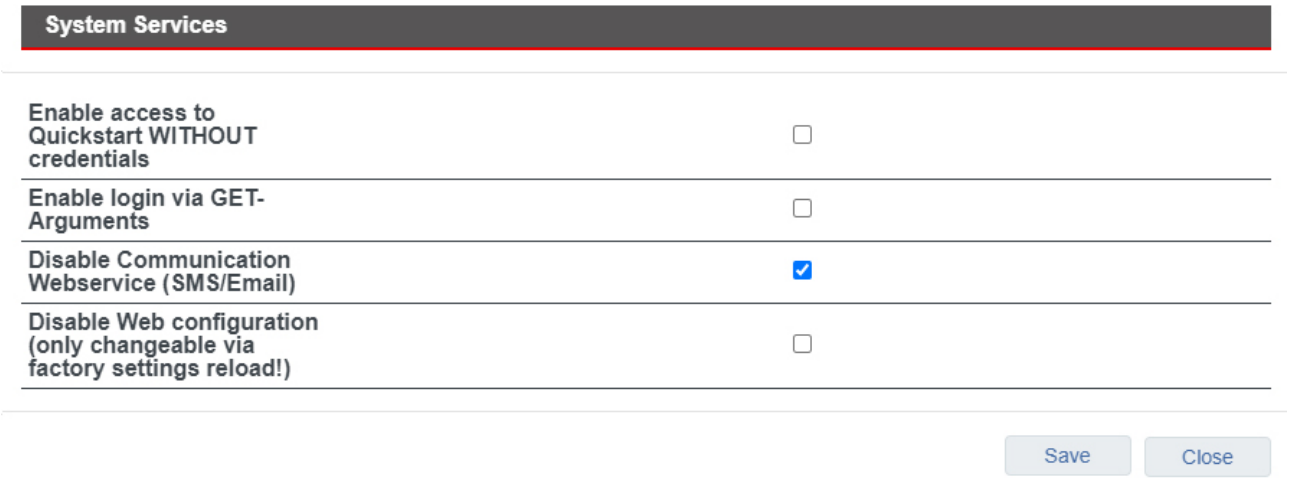
ATTENTION! If you upload a wrong certificate or key it could be possible that the webpage is no more reachable!

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

21.4.2 System > Web > System Services



System Services	
Function	Description/content
Enable access to Quickstart WITHOUT credentials	This function is only relevant if you operate the router in the mbCONNECT24 portal (Cloudserver). You can find a description of this function in the mbCONNECT24 online help.
Enable login via GET-Arguments	Checkbox to activate / deactivate this function. Beyond the login, no other parameters are taken into account. https://192.168.0.100/login?username=[USERNAME]&password=[PASSWORD]
Disable Communi-cation Webservice (SMS/Email)	Checkbox to deactivate / activate the function. If this function is activated, neither an SMS nor an e-mail can be sent from the device.
Disable Web configuration (only changeable via factory settings reload!)	By activating the checkbox, access to the mbNET web interface is completely blocked. **ATTENTION**: Once the web configuration is disabled, it can only be restored to its factory settings by rebooting the mbNET.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

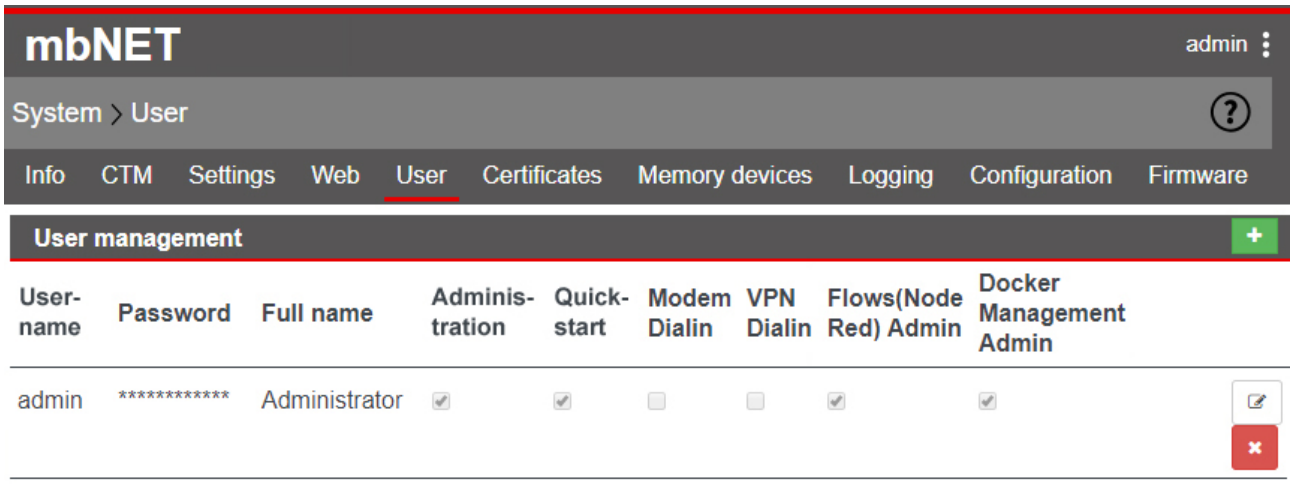
NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

21.5 System > User

Here you can manage the users who have access to the configuration interface of the mbNET.

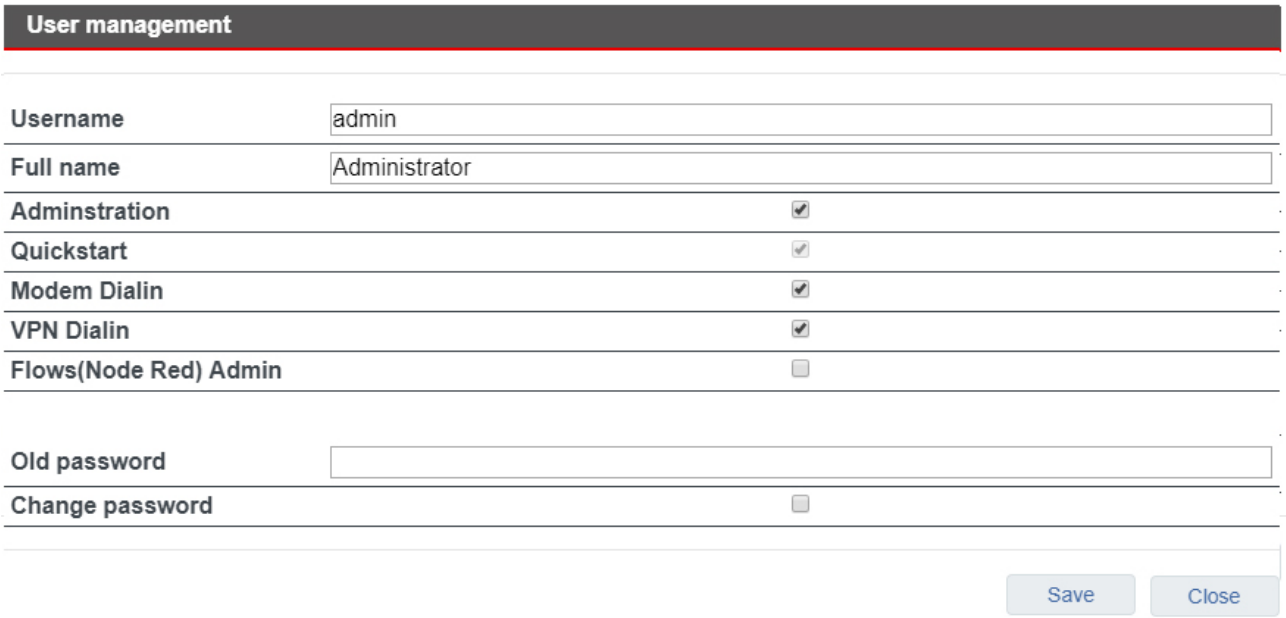
- By default, the user "admin", is created with all rights.
- The user "admin" is associated with the device password.
- The user "admin" cannot be deleted.



By clicking on the relevant button users can be

1. added
2. edited
3. deleted

21.5.1 Added/Edited User



Designation	Description
User name	Mandatory field for entering a user name (for example, User1)
Full Name	Mandatory field for entering a name (for example, Peter Schmidt)
Administration Dial-up modem VPN dial-up Flows(Node Red) Admin Docker Management Admin	Check boxes to enable/disable the type of access by the user to the web interface of the mbNET. • Administration => access via HTTPS • Dial-up modem => access via dial-up modem • VPN dial-up => access by dialling through a VPN tunnel • Flows(Node Red) Admin => access Node-Red and Dashboards • Docker Management Admin = > access the Docker Management
New password	Mandatory field for entering a password
Repeat password	Mandatory field - Retype password

NOTICE

The password should consist of at least 8 characters, including uppercase letters, numbers and special characters (example: aZ?34%s8).

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

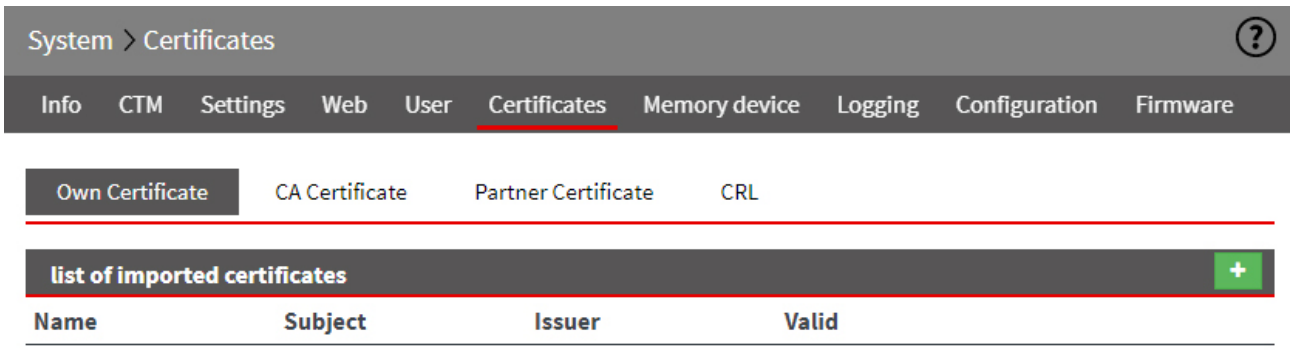
NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

21.6 System > Certificates

The main component for VPN connections using IPSec or OpenVPN is the trust between two or more communication partners.

An authenticity test is required for secure communications. This is done using PKI (public key infrastructure). Certificates will ensure that the "right" partners communicate with each other. With a certificate, the certificate holder (subject) proves their identity. The certificate may be issued by a higher authority (the Certificate Authority (CA)) or by the certificate holder itself.
The certificate **owner** will therefore be designated as **Subject** and the **certificate** issuer **as** Issuer. Below the screen mask with the tabs of the relevant certificates and the option of importing new certificates.



In the Certificates menu you see an overview of the imported certificates

- Own certificate
- CA certificate
- Partner certificate
- CRL (Certificate Revocation List)

Here you can import  and delete  the appropriate certificates.

21.6.1 Own certificate

Own certificates are used by the certificate holder. These are issued and signed by a higher authority (CA Root Certificate). In order for the mbNET to be able to use its own certificate at a remote terminal so as to show it there, the appropriate PKCS12 file (certificate including private key) must be selected, in order to import this. One or more PKCS12 files can be imported.

NOTICE

As an own certificate always has an associated key, a PKS12 file with the file name extension *.p12 must be used.

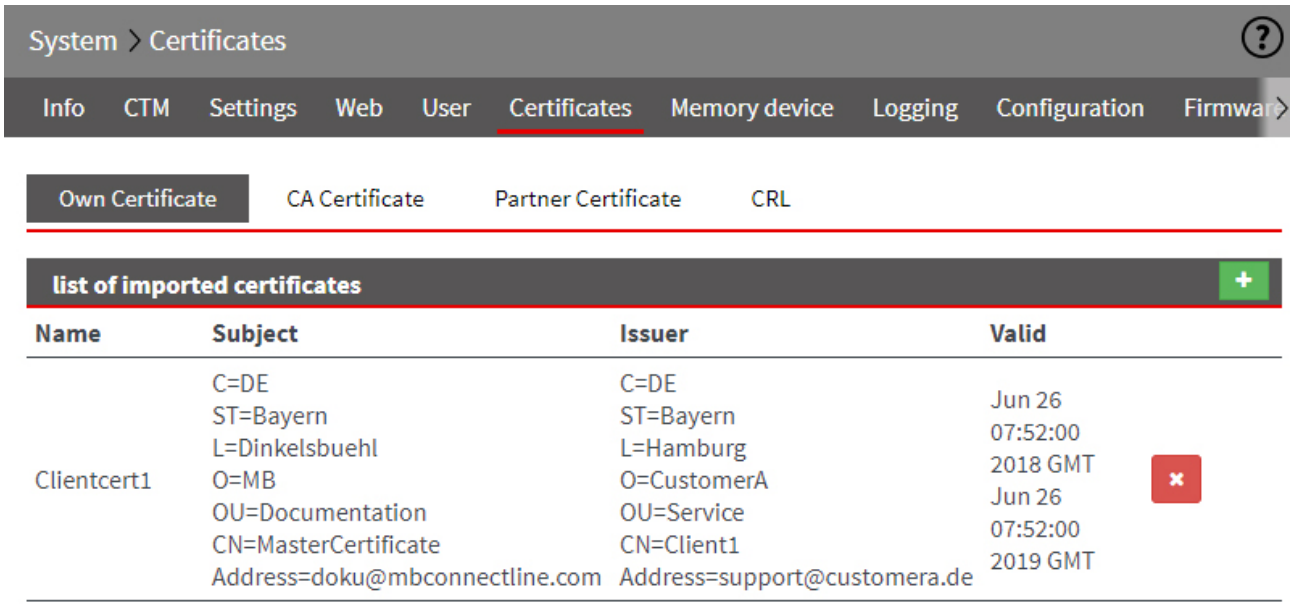
An own certificate also always has a key. A PKCS12 file must therefore be imported. This consists of a .crt file and a .pem key file.

A PKS12 file consists of a * .crt file and a * key .pem file.

21.6.1.1 Import own certificate

Designation	Description
File	Click "Select file" and select the required *.p12 file (in this example, "Clientcert1.p12"
Certificate name (optional)	The name for the imported certificate can be freely forgiven/changed.
Password	Enter the password that was assigned to this file.

Click **Import** and then **Close**.



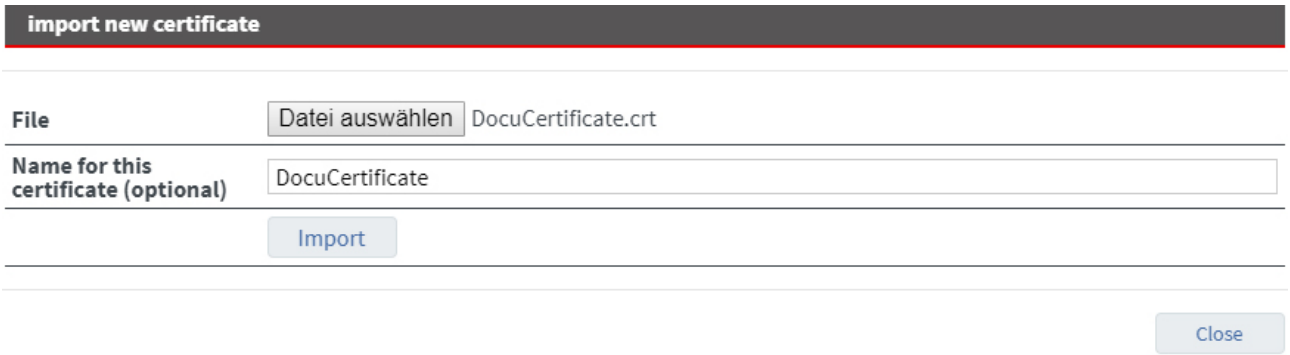
In the overview, you can see certificates imported thus far.

21.6.2 CA certificate (root certificate)

A root certificate verifies that the remote site certificate is signed.
Such a stem cell certificate must be imported, if under the VPN settings "**by means of a certificate from the same CA**" is selected as the authentication method.

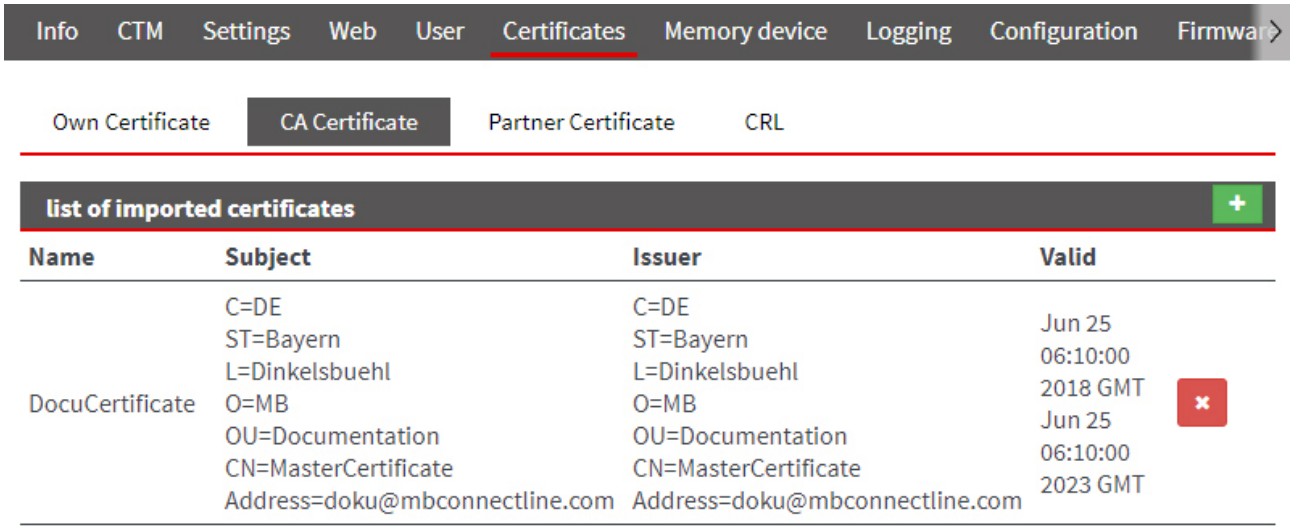
The entry from the root certificate will be used as a criterion to decide whether the certificate of the in-dialling device is valid. The CA certificate contains information about whether the certificate of the remote terminal is valid or not.
The CA certificate is available as * .crt file and must be imported into the mbNET.

21.6.2.1 Importing CA certificate (root certificate)



Designation	Description
File	Click "Select file" and select the required *.crt file (in this example: "DokuCertificate.crt"
Name for this certificate (optional)	The name for the imported certificate can be freely forgiven/changed.

Click **Import** and then **Close**.



In the overview, you can see certificates imported thus far.

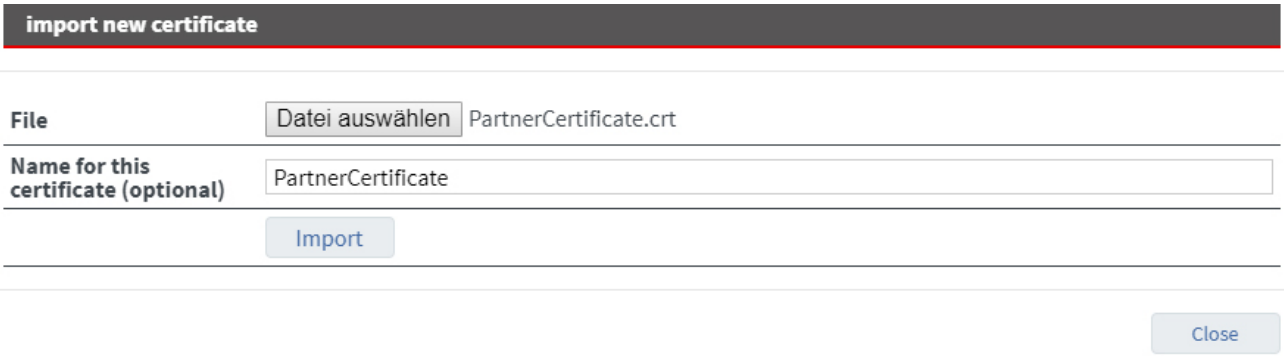
21.6.3 Partner certificate (IPSec)

Partner certificates are certificates of the remote terminal. They are only required if the VPN settings "Authentication via partner certificate" have been selected.
In this case, the criterion for deciding the validity of a certificate is that a copy of this partner certificate exists locally.

The certificate of the remote terminal must be selected by the corresponding crt file and then imported. Multiple crt files can be imported.

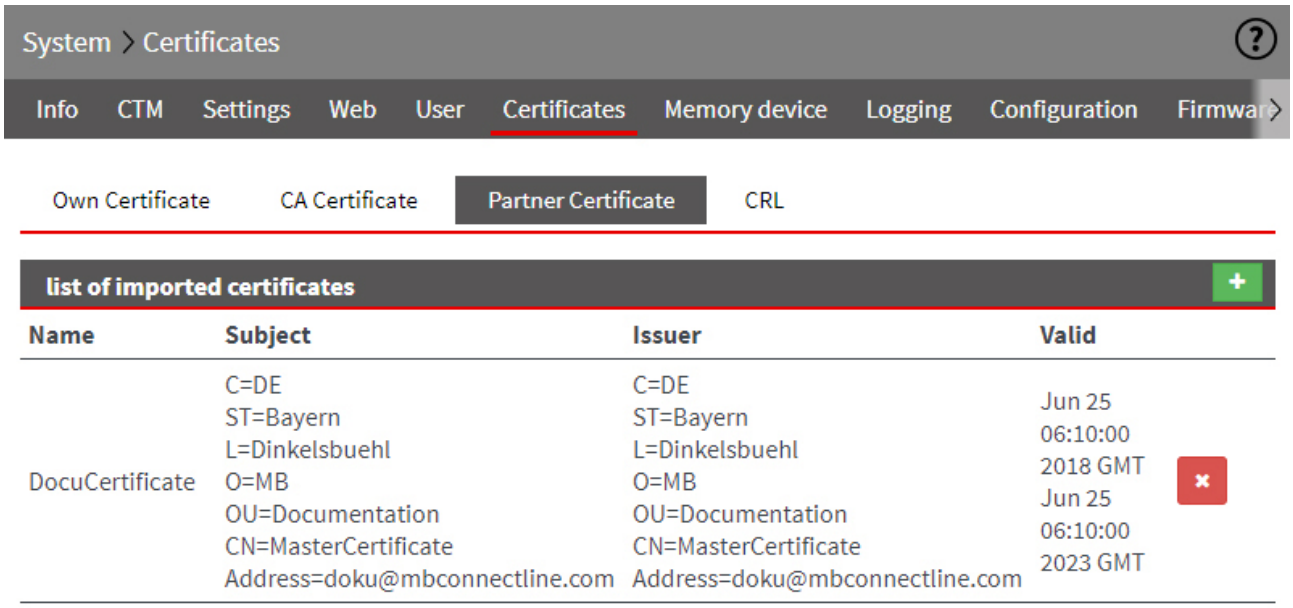
The entry from the root certificate will be used as a criterion to decide whether the certificate of the in-dialling device is valid. The CA certificate contains information about whether the certificate of the remote terminal is valid or not.
The CA certificate is available as * .crt file and must be imported into the mbNET.

21.6.3.1 Import partner certificate



Designation	Description
File	Click "Select file" and select the required *.crt file (in this example: "DokuCertificate.crt"
Name for this certificate (optional)	The name for the imported certificate can be freely assigned / changed.

Click **Import** and then **Close**.

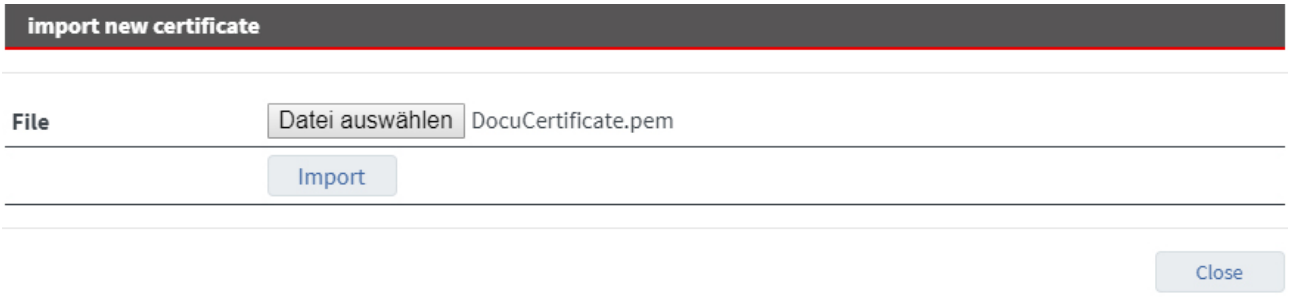


In the overview, you can see certificates imported thus far.

21.6.4 CRL (revocation list)

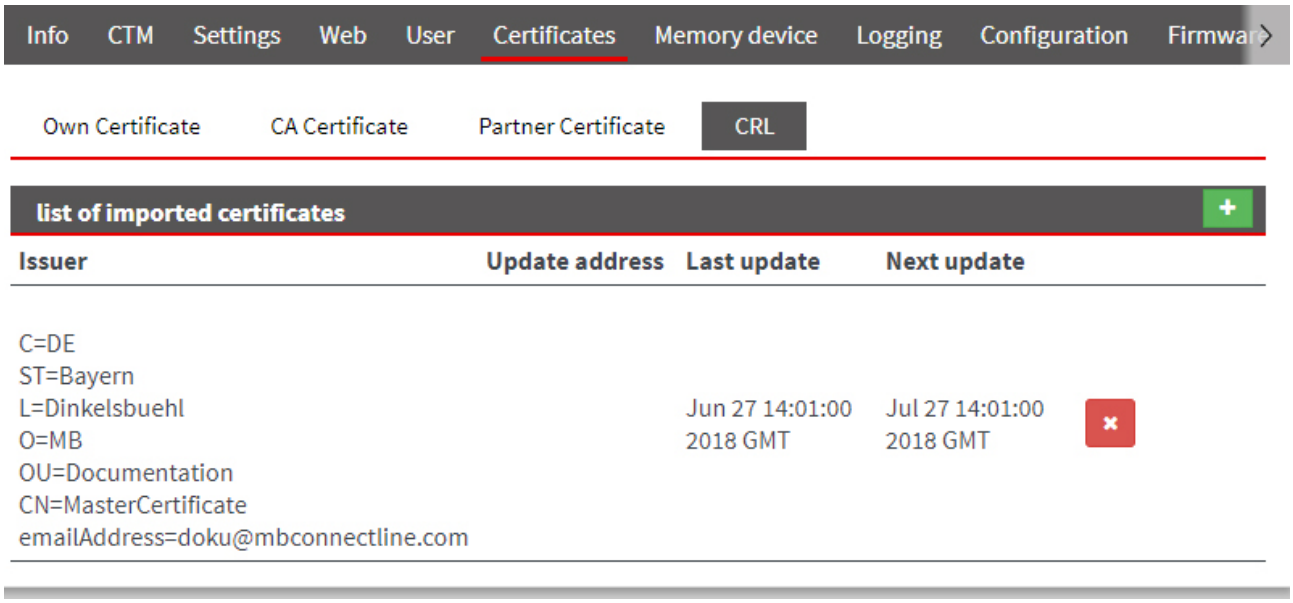
The recover/revocation list (**C**ertificate **R**evocation **L**ist CRL, for short) checks whether the certificates of in-dialling computers are valid or not. The CRL contains the serial numbers of certificates that should be blocked. So if one wants to deprive people of permission to dial into the mbNET or the underlying PLC, it is only necessary to create a CRL.

21.6.4.1 Import CRL (revocation list)



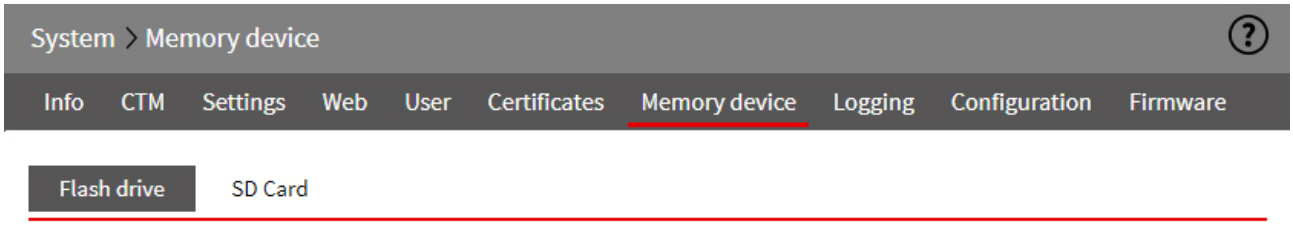
Designation	Description
File	Click "Select file" and select the required *.pem file (in this example: "DokuCertificate.pem"

Click **Import** and then **Close**.



In the overview, you can see certificates imported thus far.

21.7 System > Memory devices

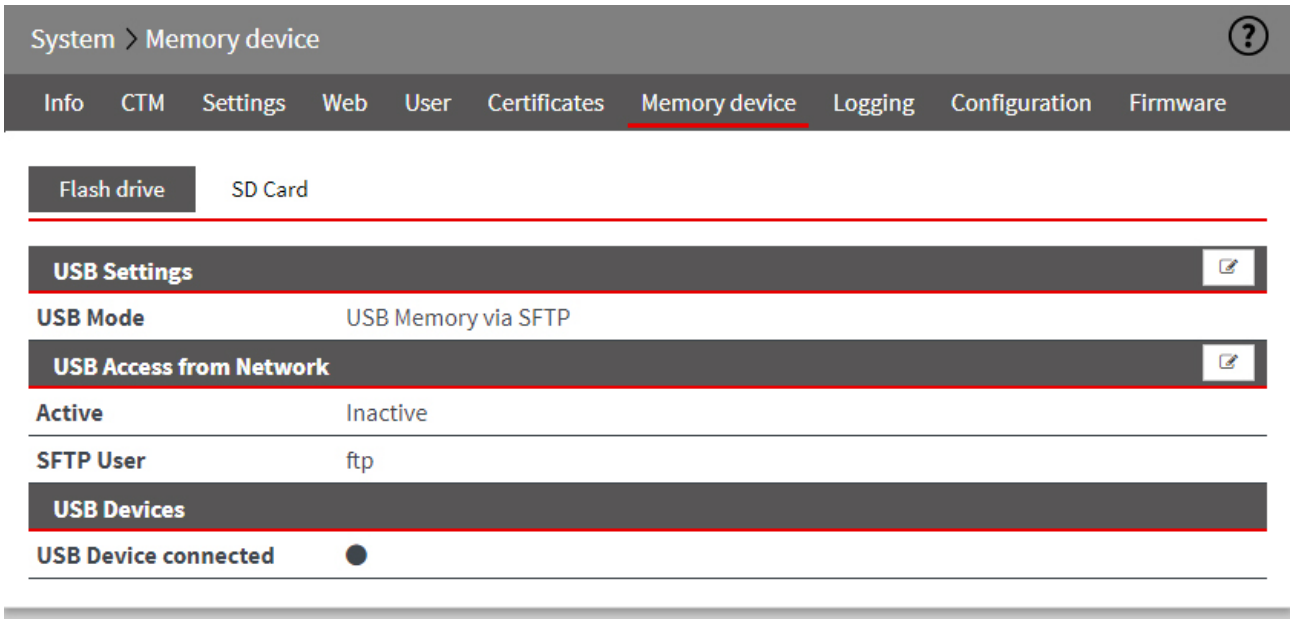


The mbNET has

- a USB port (USB Host 2.0) on the front of the device and
- an SD card slot on the bottom of the device

21.7.1 USB

You can connect a USB device (USB stick or USB hard drive) to the USB port on the Industrial router. The USB storage medium can be accessed via SFTP.



21.7.1.1 USB Settings

Within **USB Settings** you can select **USB Mode**:

- **USB Transparent (USBOverIP)**

NOTICE

USB mode "USB Transparent (USBOverIP)" is only relevant/functional in conjunction with the ***mbCONNECT24*** Remote-Service-Portal and the Remote Client ***mbDIALUP*** .

Related settings can only be made via ***mbCONNECT24*** and ***mbDIALUP***.

You can find further information in the ***mbCONNECT24***online help.

- **USB memory via SFTP**

21.7.1.2 USB access from the network

Designation	Description
Active	Check box for enabling/disabling this function. If the checkbox is activated, a connected USB storage medium is integrated by the mbNET.
SFTP User	Input field for the SFTP user name
SFTP password	Input field for the SFTP password
SFTP Password confirmation	Input field for confirmation of the SFTP User Password.

NOTICE

To access to the USB-storage medium via SFTP, enter the IP address of the mbNET server, preceded by sftp://….
Example: sftp://192.168.0.100

The default user name is: **ftp**.

The default password is: **ftp**.

21.7.1.3 USB devices

You can connect a USB device (USB stick or USB hard drive) to the USB port on the Industrial router.
The USB storage medium can be accessed via SFTP.

A LED icon will display if a USB storage medium is connected to the mbNET or has been detected.

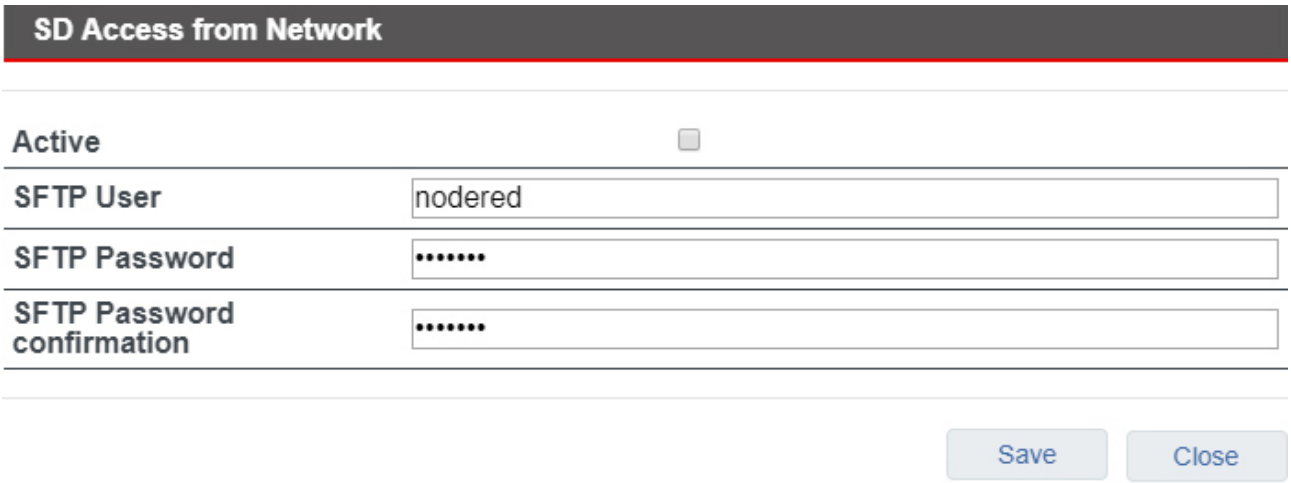
USB Device connected

- Green LED symbol = **USB storage medium available**
- Gray LED symbol = **No USB storage device connected**

NOTICE

Please keep in mind that the connected FAT/FAT32 storage medium must be formatted.
With a different file system such as NTFS, it may cause problems.

21.7.2 SD Access from network



Designation	Description
Active	Check box for enabling/disabling this function. If the checkbox is activated, a connected SD card is integrated by the mbNET.
SFTP User	Input field for the SFTP user name
SFTP password	Input field for the SFTP password
SFTP Password confirmation	Input field for confirmation of the SFTP User Password.

NOTICE

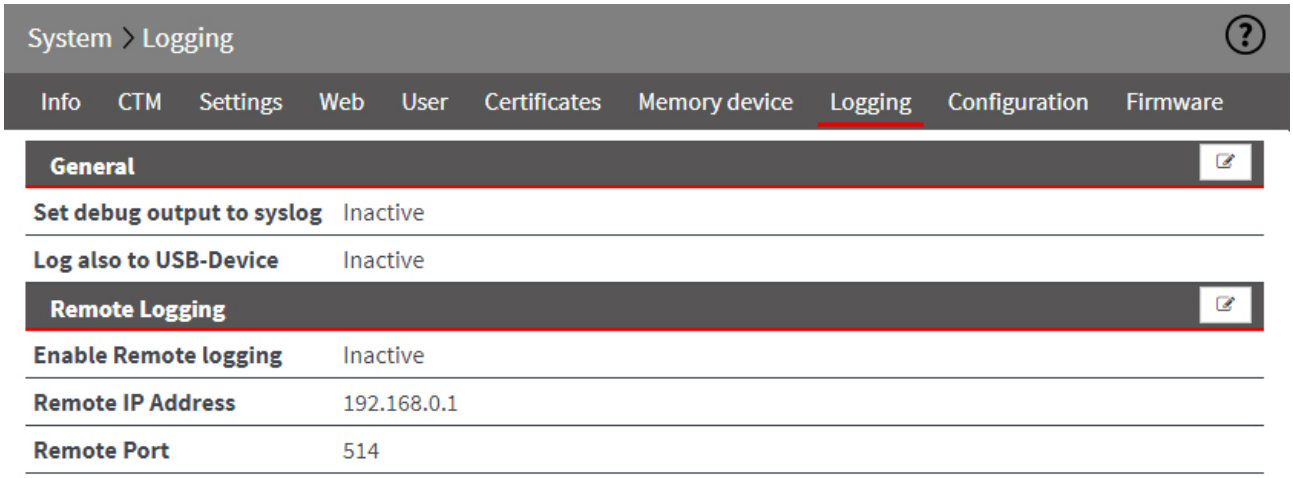
To access to the USB-storage medium via SFTP, enter the IP address of the mbNET server, preceded by sftp://….
Example: sftp://192.168.0.100

The default user name is: **nodered**.

The default password is: **nodered**.

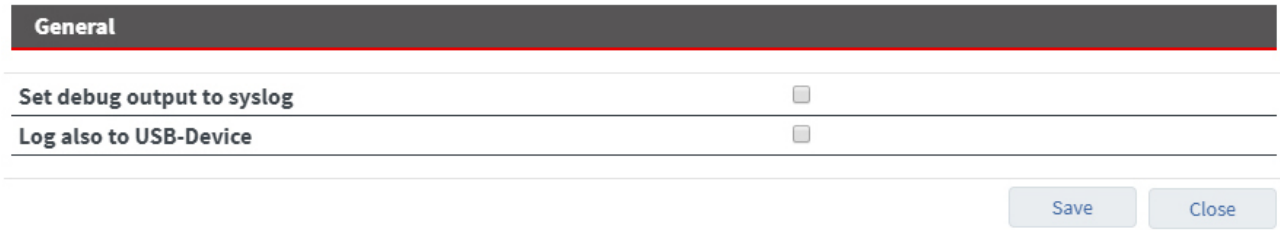
21.8 System > Logging

The system logging of the ***mbNET*** can be outsourced to another computer using a logging server.



Click the Edit icon to edit the corresponding function.

21.8.1 General Settings



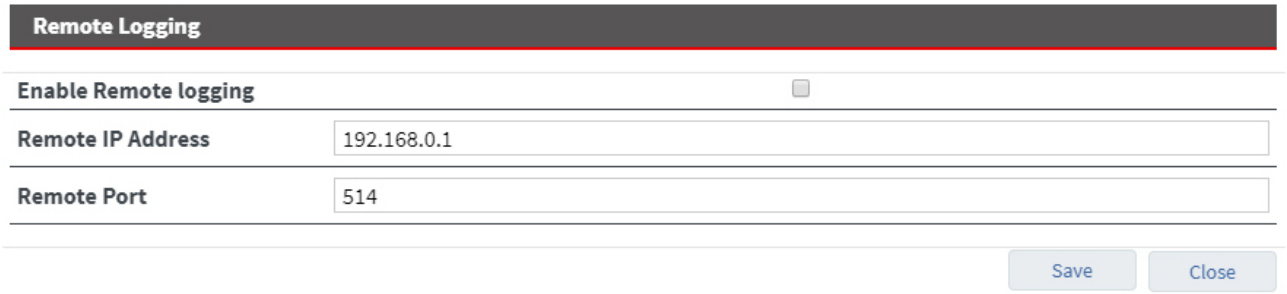
Designation	Description
Output debug information to the logging server	Check box for enabling/disabling this function. If this checkbox is enabled, debug information is output on the logging server.
Also output logging on USB stick	Check box for enabling/disabling this function. If this checkbox is enabled, the logs are also stored on a USB stick.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

21.8.2 External logging (server settings)



Designation	Description
Enable external logging server	Check box for enabling/disabling this function. When this check box is selected, the system logging of the mbNET is out-sourced to an external computer.
IP address of the External Logging Server	Enter the IP address of the external logging server here.
Port of the External Logging Server	Specifies the port number of the Logging Server. Here: Port 514

NOTICE

We recommend not changing this port, unless you have an application that responds to a completely different port.

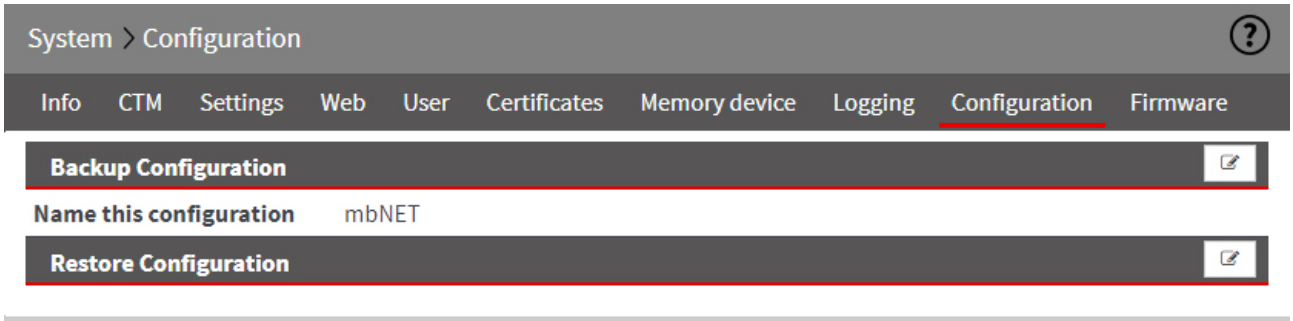
Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

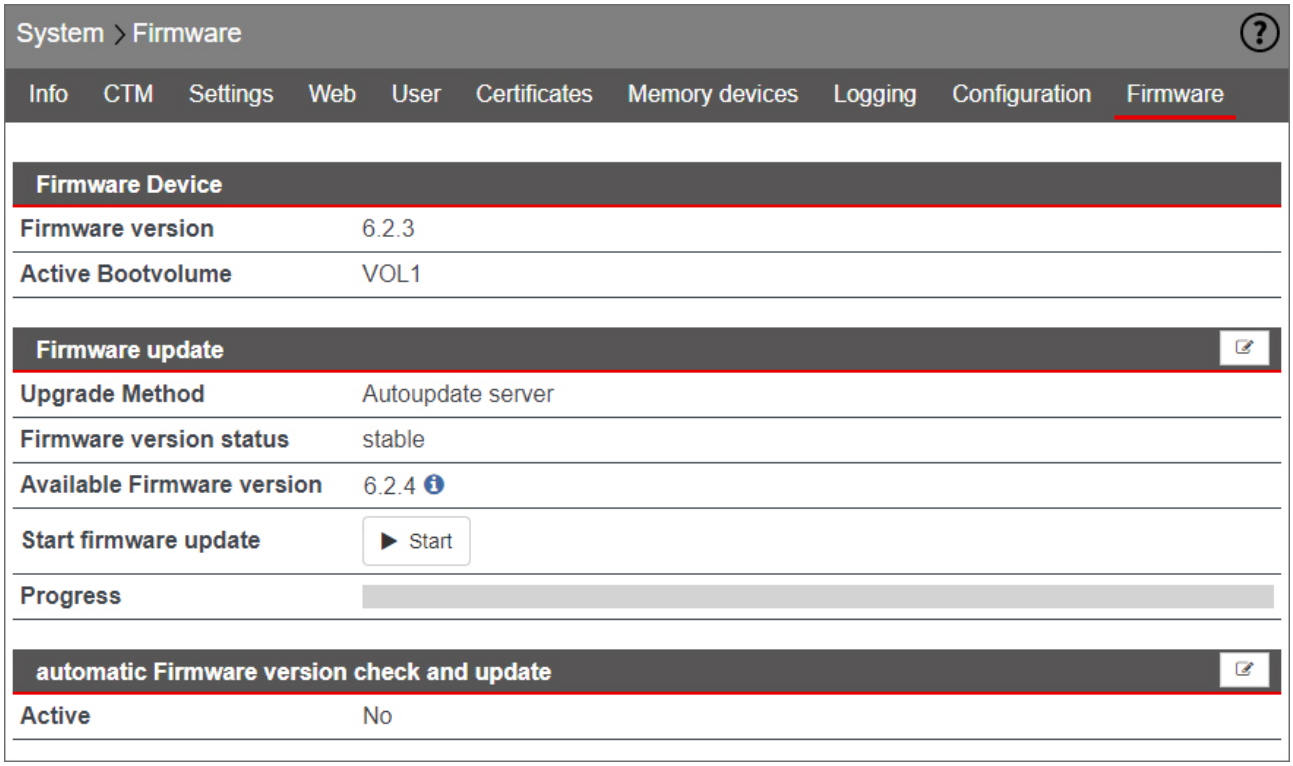
21.9 System > Configuration (backup and restore)

Here you can download a backup copy of the system configuration (Backup) and, if necessary, restore (Restore).



Click the Edit icon to edit the corresponding function.

21.10 System > Firmware (Firmware update)



Here you can check the actuality of the installed firmware version and if necessary upgrade to a higher version.

Click the Edit icon to edit the corresponding function.

Upgrade Method Selection box for the upgrade method

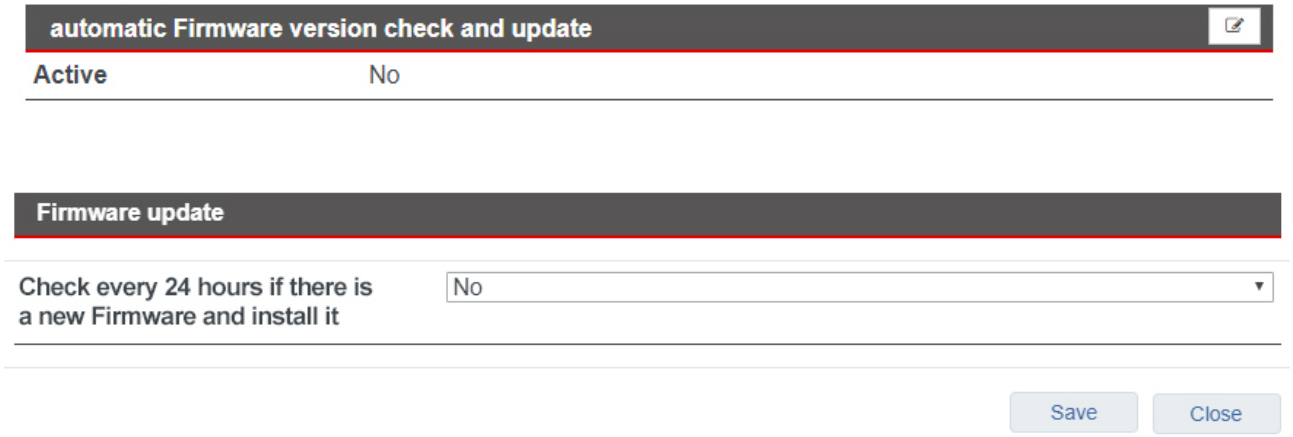
- Autoupdate server
- Flash drive
- Network

Firmware version status Selection box for the status of the available firmware

- stable
- beta (It is recommended to use the **stable** status!)

Start firmware update By clicking on the button, the firmware update starts with the previously selected settings.

automatic Firmware version and update



After activating this function, the actuality of the installed firmware is checked every 24 hours.
If a newer version is available on the Autoupdate server, it will be automatically installed.

NOTICE

An automatic update will only take place if "Autoupdate server" was selected when selecting the upgrade method.

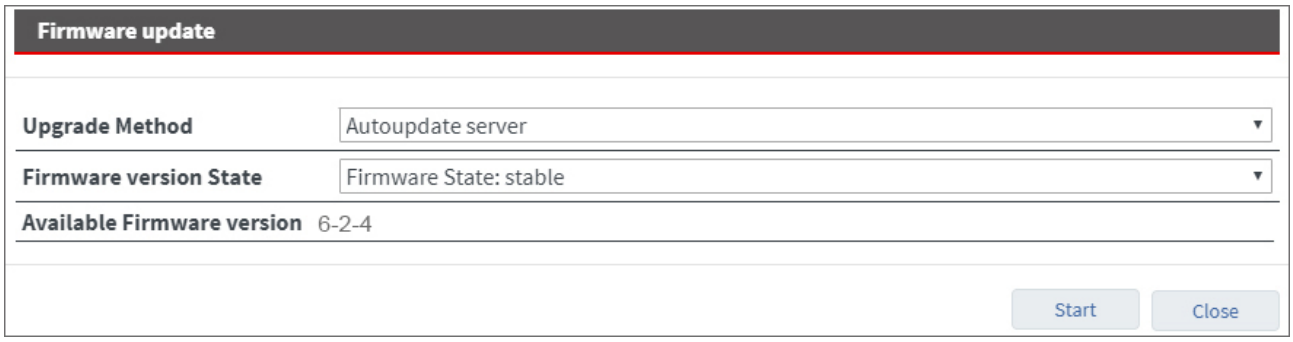
The used firmware version status (stable or beta) depends on the previously made selection.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

21.10.1 Firmware update



Designation	Description
Upgrade Method	Selection field with the following options: • **Auto Update Server** => this requires an internet connection to be established. • **USB stick** => this requires that a USB stick with the new firmware - in the root directory - is connected to mbNET. • **Network** => for this, the mbNET must be accessible on the LAN side.
Firmware Version Status	Selection field for the firmware status • Firmware Status: **Stable** • Firmware Status: **Beta**
Available firmware version	After selecting **Upgrade Method** and **Firmware Version Status**, the available firmware version is displayed here.

Click on the **Start button** to perform the firmware update and follow the instructions (for example, perform a device reboot).

22 Network - connection settings and options

Here, you define the connection settings for your mbNET-type.

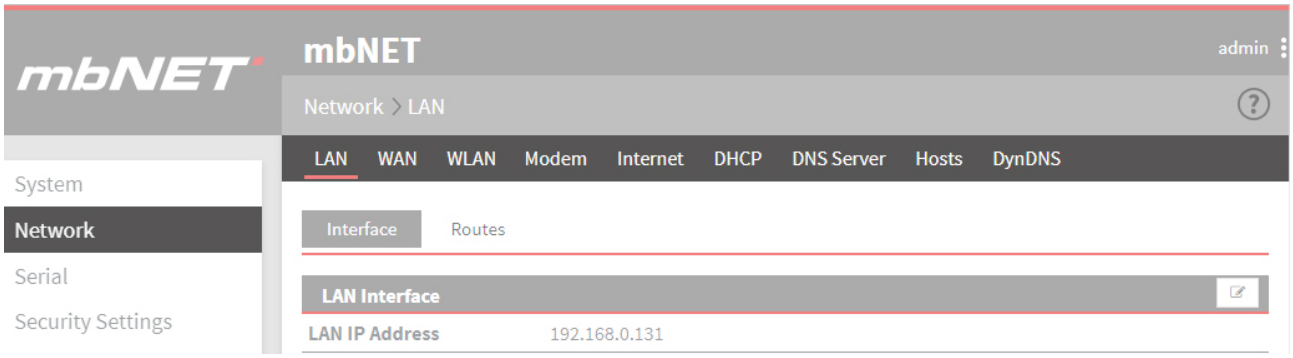


Image 10: Example display, content can vary depending on the type of device.

Under the **Network** menu the following submenus are listed:

Submenu	Description
LAN	Here you can set the LAN IP address and the subnet mask of the router (***mbNET***). This IP address accesses the router in the LAN. You can also specify both network routes in CIDR format (x.x.x.0/24) and host routes here.
WAN	Using the ***mbNET***'s WAN interface, you can connect a local network to another local network or a public network, such as the Internet. The WAN interface can be configured depending on the application. Optionally, you can network routes here in CIDR format (x.x.x.0/24) or define routes to individual network nodes.
Wi-Fi	Here you specify the interface type (DHCP or static) and configure the interface, if necessary. You can also configure the Wi-Fi connection to a Wi-Fi router or access point.

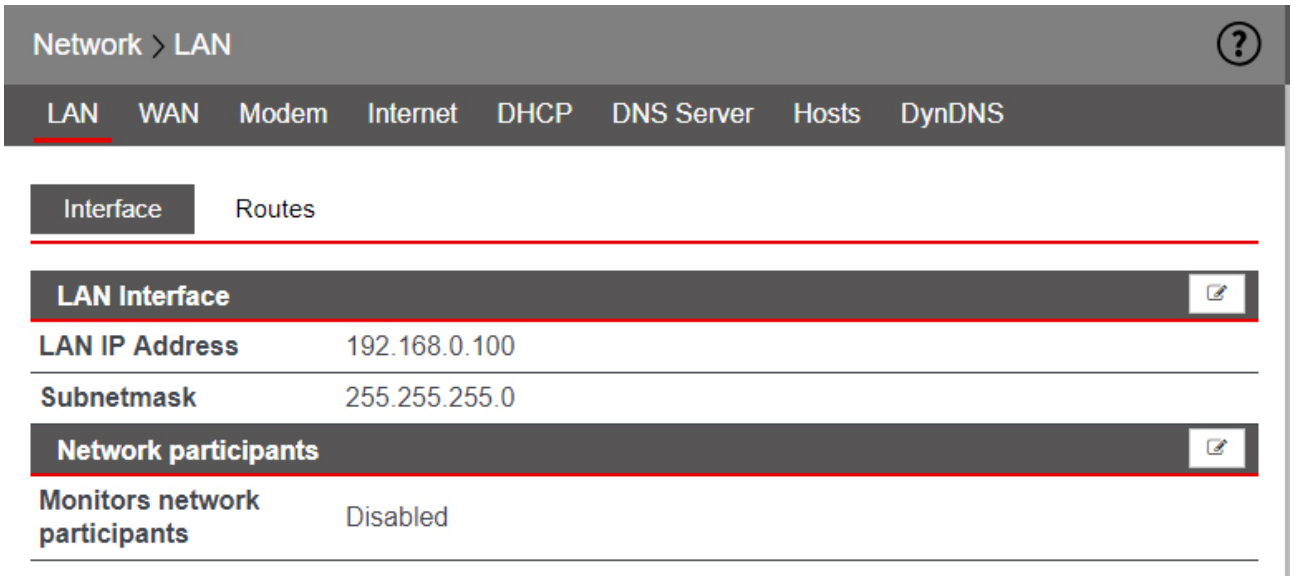
Submenu	Description
Modem	Here you can configure dial-up or Internet connections, depending on the type of modem (analogue modem or GSM modem).
Internet	For connecting to the Internet, you can configure the ***mbNET*** here for the specific connection and depending on certain events.
DHCP	Here you can configure the *mbNET* as a DHCP server on the LAN or WAN network.
DNS Server	If the ***mbNET*** should maintain a connection permanently, you can add your own DNS server here.
Hosts	To answer DNS queries directly, you can click here to assign an IP address to a specific name.
DynDNS	Here, you can set up a public dynamic DNS service.

22.1 Network > LAN

Here you can set the LAN IP address and the subnet mask of the router (mbNET). This IP address accesses the router in the LAN network.
You can also specify both network routes in CIDR format (x.x.x.0/24) and host routes here.

22.1.1 Interface

Here you can set the LAN IP address and the subnet mask of the router (mbNET). This IP address accesses the router in the LAN network.



Click the Edit icon to edit the corresponding function.

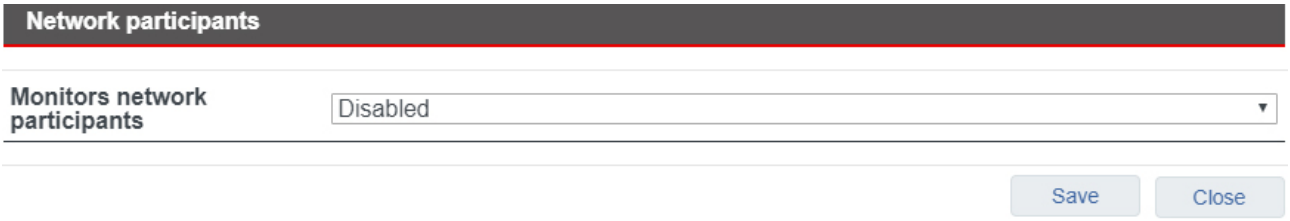
Configuring the LAN Interface

Here you can set the LAN IP address and the subnet mask of the router (mbNET). This IP address accesses the router in the LAN network.

Designation	Description
LAN IP address	Enter the IP address for accessing the router.
Subnet mask	Enter the subnet mask of the network that the router should be integrated into.

Network participants

Here you can monitor the Network participants.



Designation	Description
Monitors network participants	Selection box to • Disable • Passive

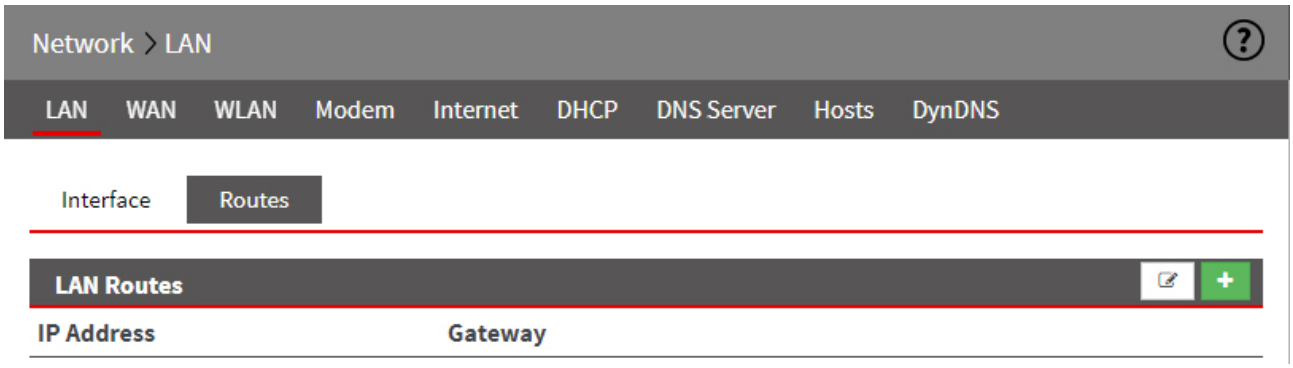
Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

22.1.2 Routes

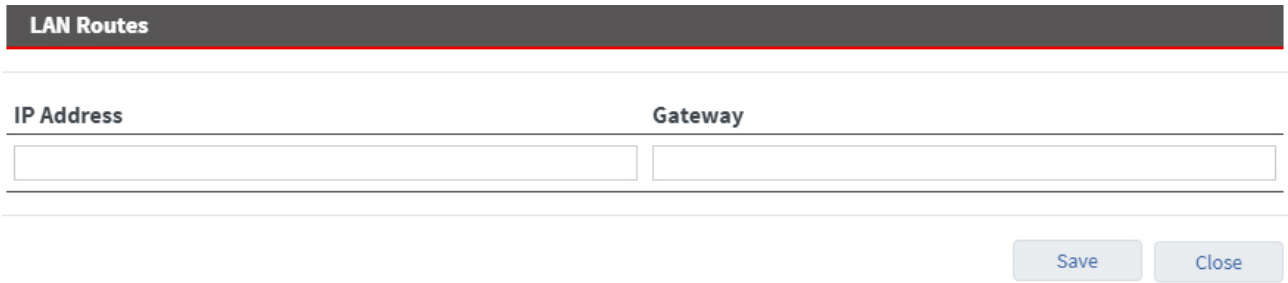
You can also specify network routes in CIDR format (x.x.x.0/24) and also host routes here.



Click the Add button to add a route.

Click the Edit icon , to edit the corresponding route.

Add LAN route



Designation	Description
IP address	Enter the network IP address in CIDR format (x.x.x.0/24) or the host IP address.
Gateway	The gateway to be entered is usually the IP address of the router (mbNET).

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

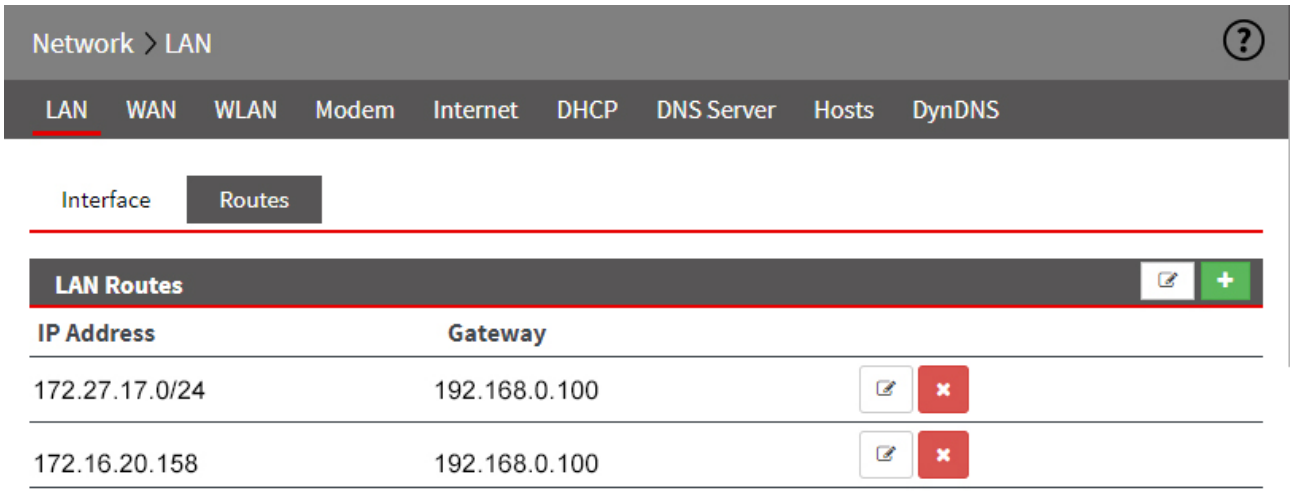
NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

After you confirm your entry by clicking on the "Save" button, your entries appear in the overview of the LAN-routes.

Edit/Delete LAN route

After you confirm your entry by clicking on the "Save" button, your entries appear in the overview of the LAN-routes.



Click the Edit icon , to edit the corresponding entry.

Click the Delete icon , to delete the corresponding entry.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

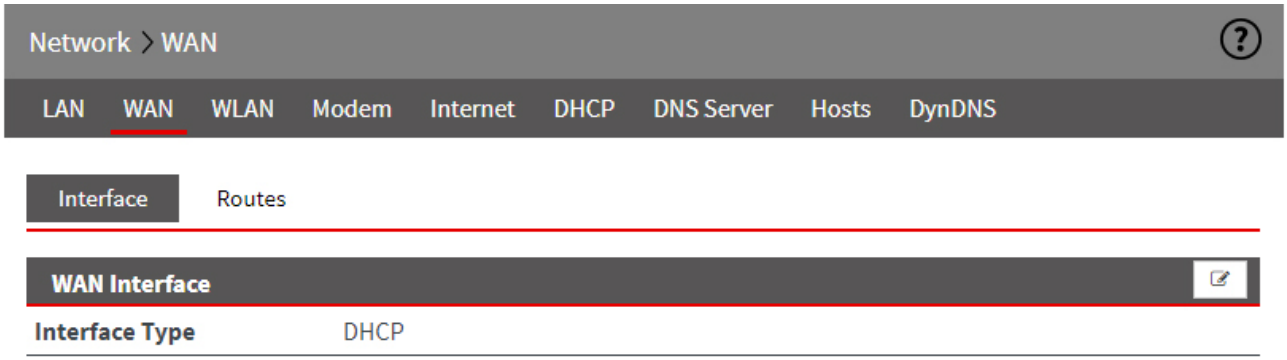
Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

22.2 Network > WAN

Using the ***mbNET***'s WAN interface, you can connect a local network to another local network or a public network, such as the Internet. The WAN interface can be configured depending on the application.
Optionally, you can network routes here in CIDR format (x.x.x.0/24) or define routes to individual network nodes.

22.2.1 Interface - set WAN interface type

Here you can specify the type of interface and configure the interface.

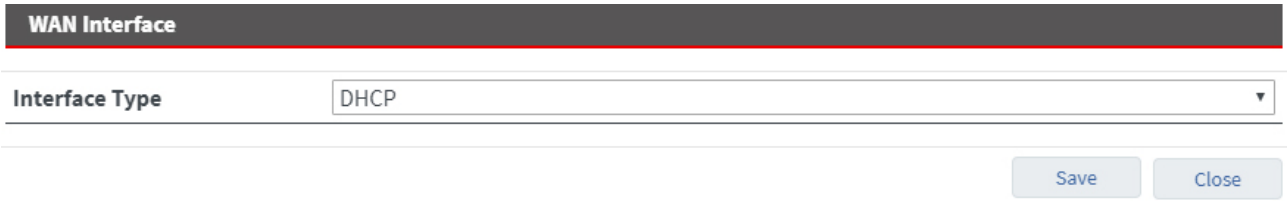


Click the Edit icon to edit the corresponding function.

Select interface type

The options are

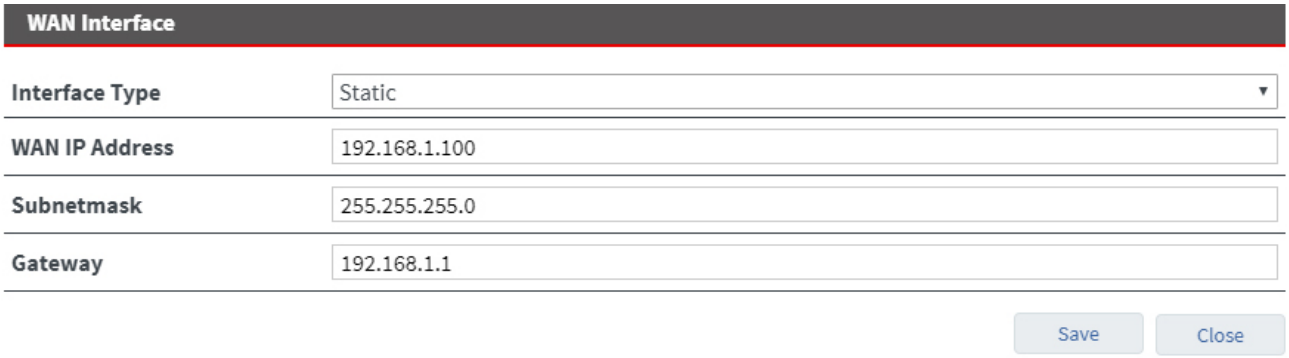
- **DHCP**
- **DSL**
- **Static**



Interface Type	Description
DCHP	Select this type if a DHCP server is present in the network and thus automatically assigns an IP address to the router (mbNET). **Contact your network administrator if necessary.**
DSL	Select this type if your router (mbNET) is connected directly to a DSL modem that provides the connection to the Internet.
Static	

Configuring the WAN Interface

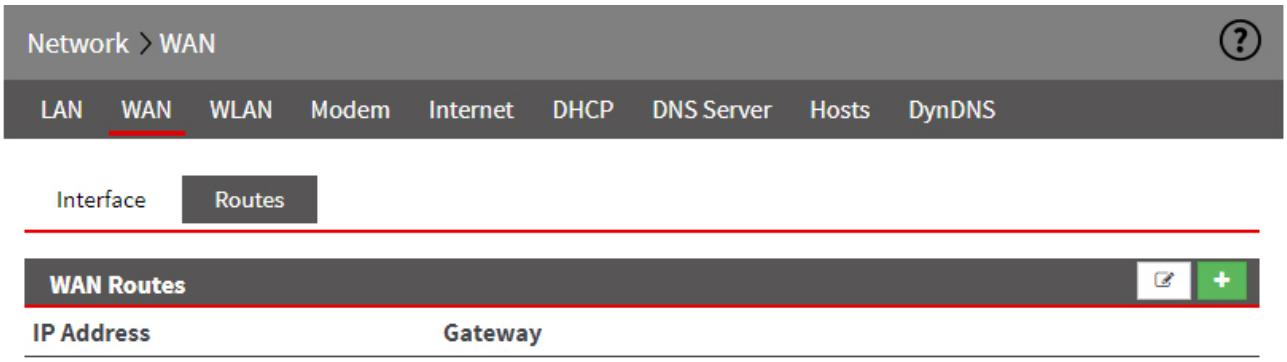
When selecting interface type **Static,** you must configure the interface.



Designation	Description
WAN IP address	Enter the WAN IP address of the router (mbNET).
Subnet mask	Enter the subnet mask of the network that the router should be integrated into.
Gateway	Enter the IP address of the gateway that connects to the Internet.

22.2.2 Routes

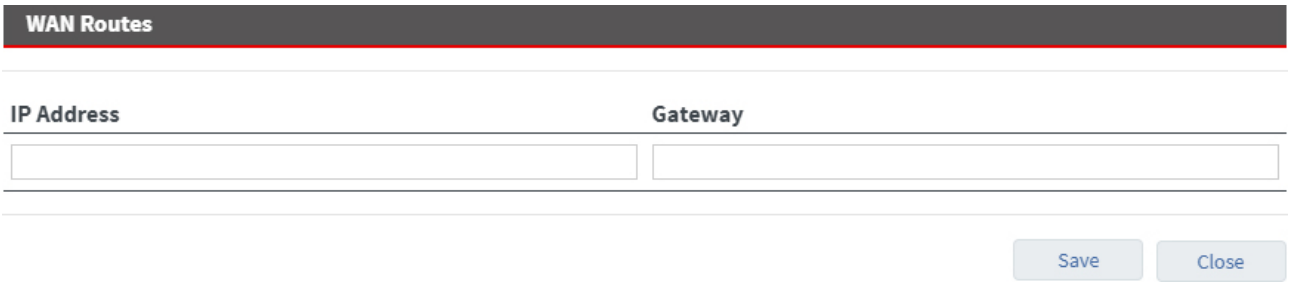
If further sub-networks are connected to the locally connected network, you can define additional routes here. Here, you can specify network routes in CIDR format (x.x.x.0/24) or define routes to individual network users.



Click the Add button to add a route.

Click the Edit icon , to edit the corresponding route.

Add WAN route



Designation	Description
IP address	Enter the IP address for the network routes in CIDR format (x.x.x.0/24) or the IP address of the network subscriber.
Gateway	The gateway to be entered is usually the IP address of the router (mbNET).

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

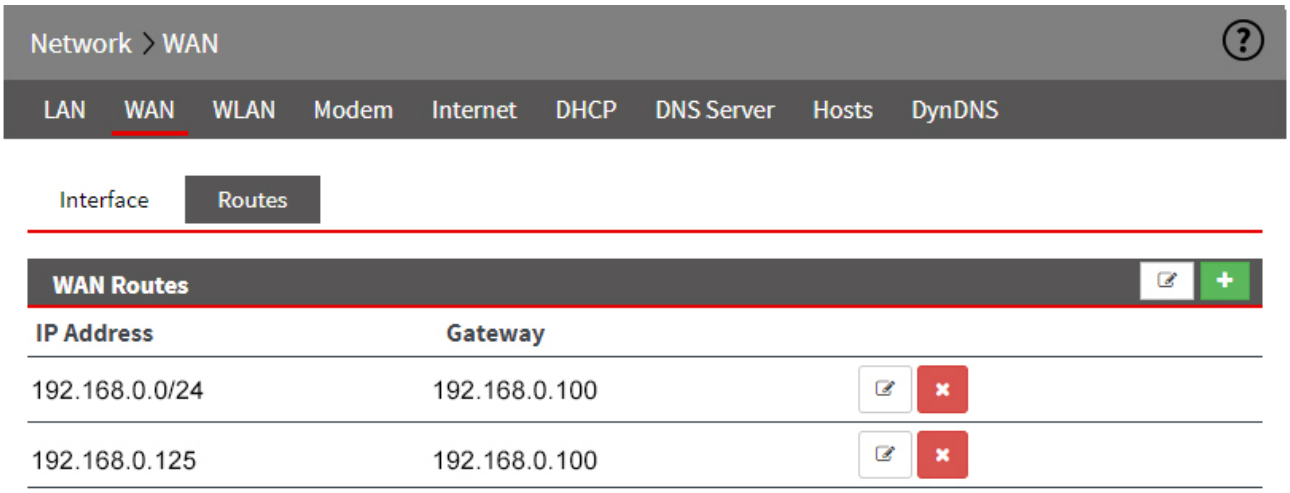
NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

After you confirm your entry by clicking on the "Save" button, your entries appear in the overview of the WAN-routes.

Edit/Delete WAN route

After you confirm your entry by clicking on the "Save" button, your entries appear in the overview of the WAN-routes.



Click the Edit icon , to edit the corresponding entry.

Click the Delete icon , to delete the corresponding entry.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

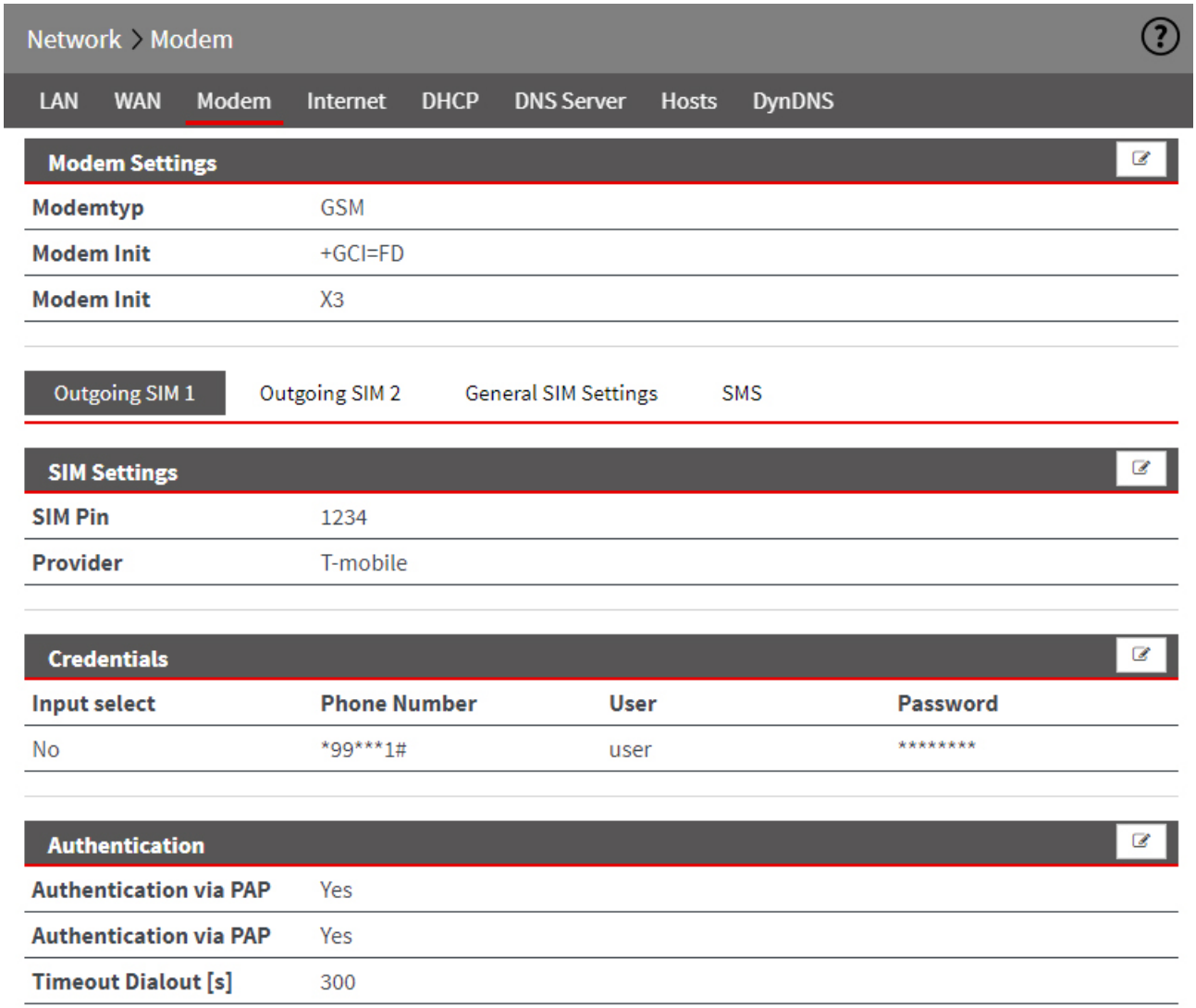
22.3 Network > Modem

The built-in mbNET modem (analogue or GSM) is provided for dial-up and/or Internet connections if no corresponding DSL or network connection is available.

NOTICE

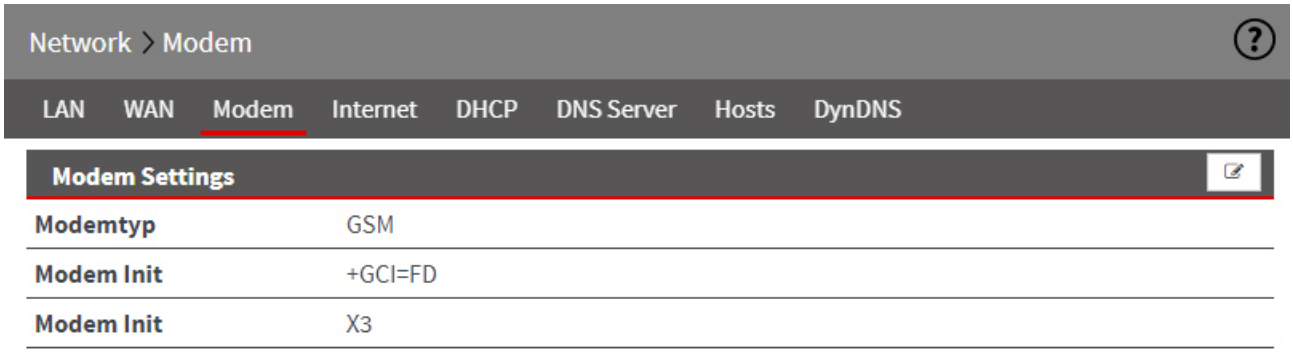
If the modem is used for an outgoing internet connection, no incoming connection can be made.

22.3.1 GSM modem configuration



22.3.1.1 Modem Settings

Here, you can perform the basic modem settings.



Click the Edit icon to edit the corresponding function.

Modem Settings	
Modem Init	+GCI=FD
Modem Init	X3

Save Close

NOTICE

For a GSM connection, none of the two initializations is necessary to guarantee error-free connection.

22.3.1.2 Outgoing SIM 1/SIM 2 (configuration for outgoing connections)

Here you can configure the SIM settings, the access data and the authentication for outgoing connections.

Outgoing SIM 1 | Outgoing SIM 2 | General SIM Settings | SMS

SIM Settings	
SIM Pin	1234
Provider	T-mobile

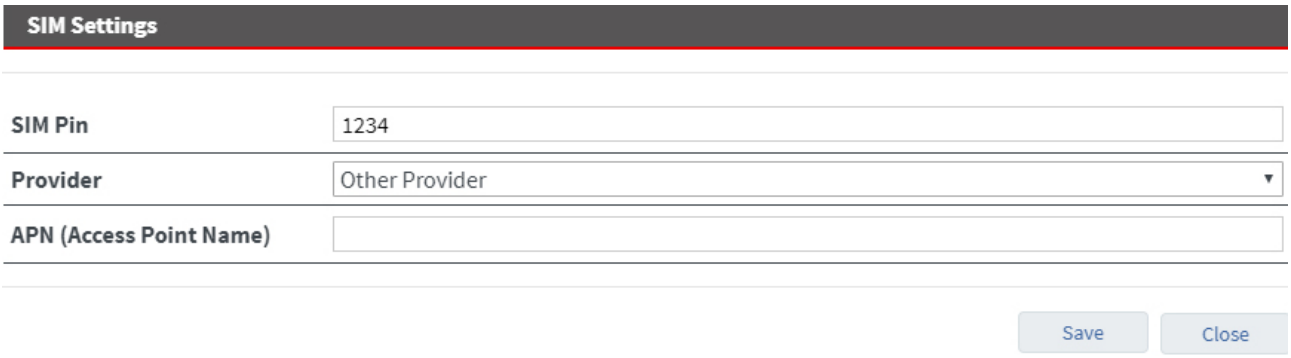
Credentials			
Input select	Phone Number	User	Password
No	*99***1#	user	********

Authentication	
Authentication via PAP	Yes
Authentication via PAP	Yes
Timeout Dialout [s]	300

Click the Edit icon to edit the corresponding function.

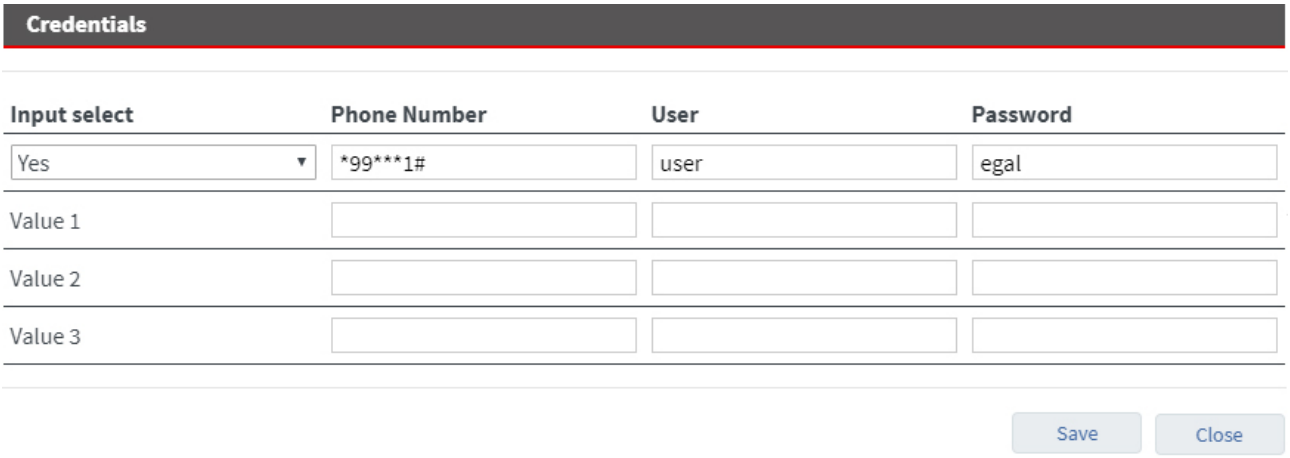
SIM Settings

Here you enter the SIM PIN of the respective SIM card and select your wireless service provider.



Designation	Description
SIM PIN	Enter your personal identification number (PIN) of the respective SIM card to provide access. You need a mobile phone to switch the PIN on or off.
Provider	Selection field with a list of the most common wireless service providers. If your wireless service provider does not appear in the selection, choose “Other provider". In the following field, you can enter the APN.
APN (Access Point Name)	Input field for a private APN.

Access data (selection of inputs)



Designation	Description
Selection of inputs	Selection field no/yes Select Yes if you want to call several stations. Three more lines for entering the necessary access data will appear. Each of these additional lines is selected based on signals to digital inputs I2 to I4. Now enter the numbers and the user data for the PPP dial-up in the additional fields. Switch the first and one or two of the other three inputs to begin dialling. Please note that you must first switch one or two of the other 3 inputs before switching the first input.

Designation	Description
	NOTICE The mbNET acts only as a PPP client. The PPP server must use a different industrial router (mbNET) or a computer that can process the request.
	Under Network > Internet , set the Internet settings to "**On Demand**" and then switch the option "**Connect if the input is active**" to input 1. • To call the first number => switch input I1 • To call the second number => switch input I2 and then input I1 • To call the third number => switch input I3 and then input I1 • To call the fourth number => switch input I2+I3 and then input I1
Phone number	Here, enter the call/dial-in number of the corresponding provider.
User	Enter the user name required to dial the corresponding provider. Further information can be obtained directly from your provider.
Password	Enter the password required to dial in to the corresponding provider. Further information can be obtained directly from your provider.

Authentication

Here you can select the authentication protocol for the dial-up connection and set the time limit for dial attempts.

Designation	Description
Authentication via PAP	Authentication protocol with which your login data is transferred (Password Authentication Protocol). However, we recommend using the secure variant CHAP, as in PAP your password is sent unencrypted.
Authentication using CHAP	Authentication protocol with your login data transmitted in order to protect this data (Challenge Handshake Authentication Protocol). CHAP is normally the procedure which is performed when logging on to the internet at the Internet Service Provider (ISP) via a modem.
Timeout when dialling in [s]	After this set time, the dialling attempt is aborted and a new selection is started.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.

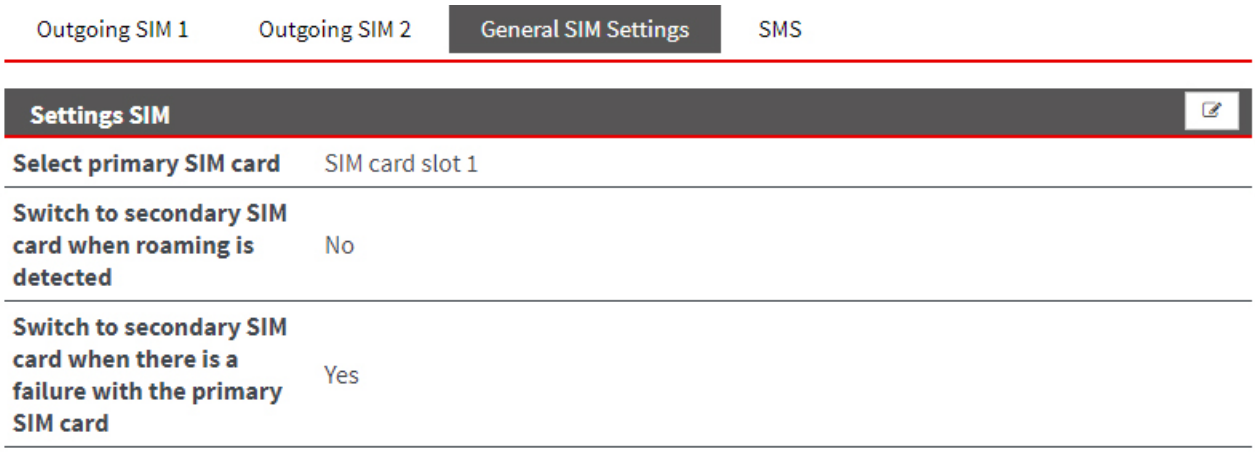
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

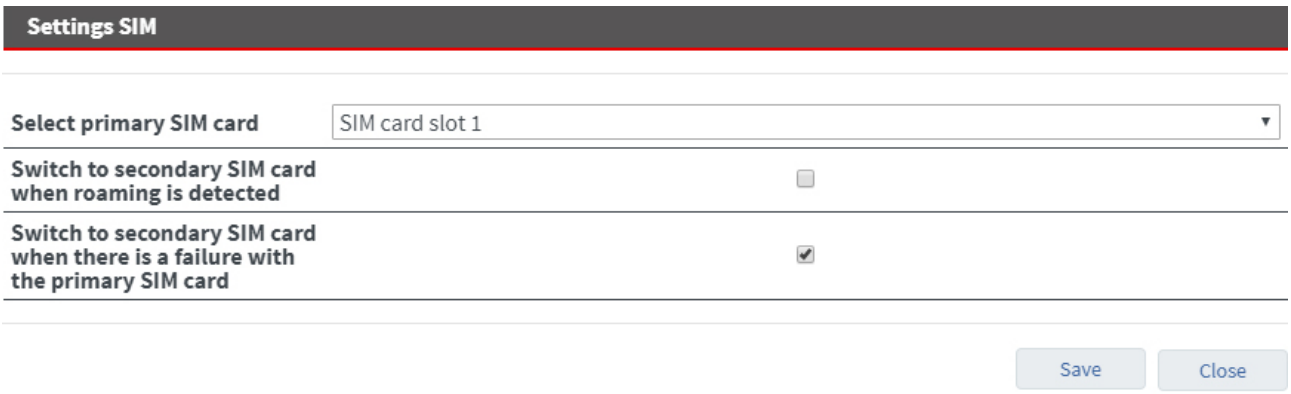
Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

22.3.1.3 General SIM Settings

Here you can specify which SIM card or which of the two SIM card slots is to be used primarily.



Click the Edit icon to edit the corresponding function.



Designation	Description
Select Primary SIM Card	Selection field for the SIM card slot, that should be addressed/ used first.

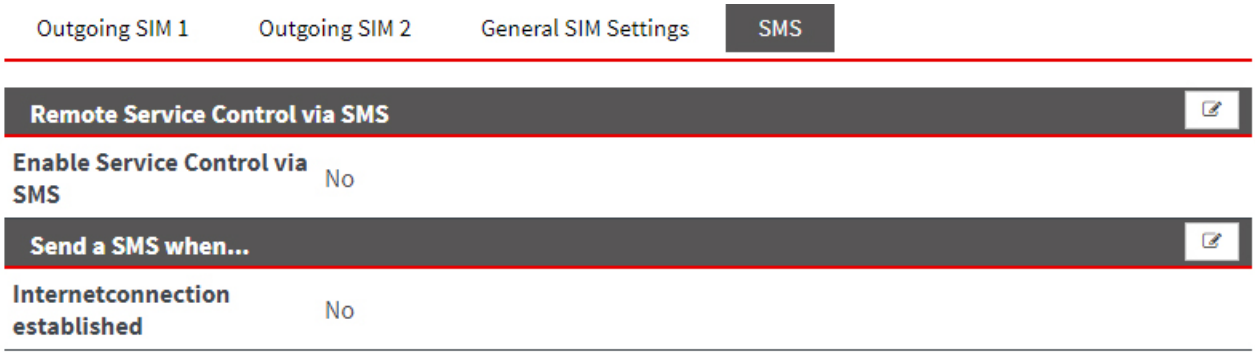
Designation	Description
Switch to the secondary SIM card, if network roaming has been detected	Check box for enabling/disabling this function.
Switch to the secondary SIM card, if the primary SIM card cannot be initialized	Check box for enabling/disabling this function.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

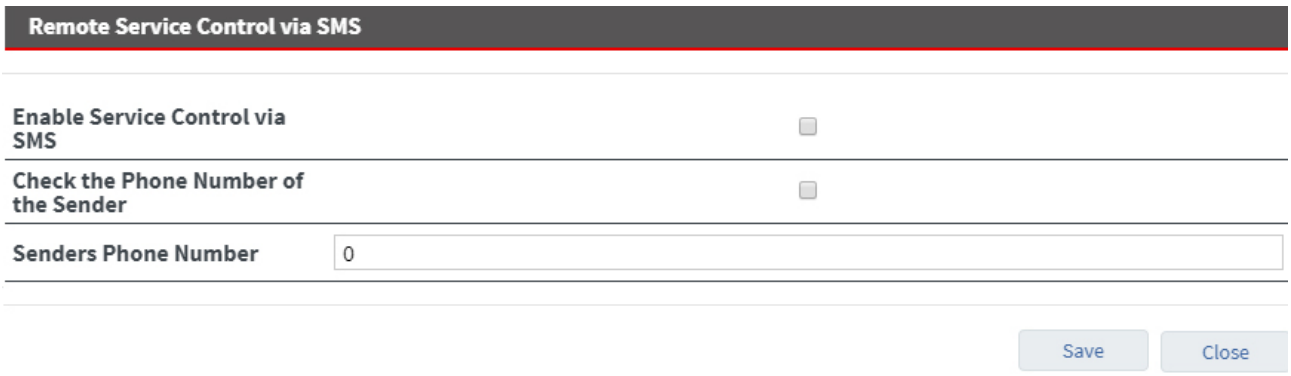
Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

22.3.1.4 SMS (Remotely control services via SMS Send SMS if,...)



Click the Edit icon to edit the corresponding function.

Remotely control services via SMS



Designation	Description
Allow remote control	Check box for enabling/disabling this function.
The telephone number of the sender is checked	Check box for enabling/disabling this function. Enable this feature to ensure that the mbNET only executes commands that come from a specific number. You will need this telephone number in the “Sender’s phone number” field.
Sender’s phone number	Here, enter the phone number from which the mbNET accepts and executes control commands via SMS. All other telephone numbers will be ignored by the device.

NOTICE

The phone number must not start with 0 (zero).
The entry must be preceded by a country code (example: +49 30 1234567).

Save	Clicking on **"Save”** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close”** discards the current input/changes.

NOTICE

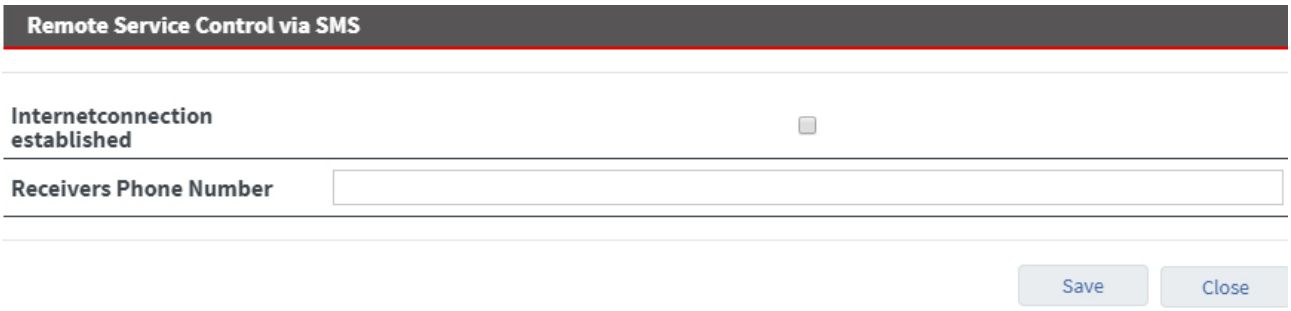
Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via “**Apply Changes**", will the changes be applied (activated) and stored permanently.

Command set for remote control of the mbNET via SMS

Command	Note
INET START or ***INET STOP***	Control of the internet connection of the Industrial router. Note that only one set of active internet connections can be controlled by the established industrial router.
IPSEC START [connection name] or ***IPSEC STOP [connection name]*** ***PPTP START [connection name]*** or ***PPTP STOP [connection name]*** ***OPENVPN START [connection name]*** or ***OPENVPN STOP [connection name]***	No matter which VPN type has been selected, the connection name must always be specified accordingly(example: ***OPENVPN START Wizard***). Furthermore, you need to note that the connection name is case sensitive!
REBOOT	The industrial router will restart with this command. Please note that your industrial router will not execute any other commands during this time.

Command	Note
OUT ON or ***OUT OFF***	With the command ***OUT ON [output no.]*** or ***OUT OFF [output no.]*** you can also switch the outputs of your router on or off via SMS (example: ***OUT ON 1***, switches on Output 1 - ***OUT OFF 1***, switches off Output 1).
IN STATUS	***IN STATUS***, this command responds by supplying the status of the inputs.
GSM CMD	With the command ***GSM CMD [at-command]*** it is possible to send to the router modem any AT commands. The response of the modem is sent via SMS to the sender address (example: "***GSM CMD AT+cops?***" responds by providing information about the network and the provider).
Please note that only the first 160 characters of the modem response will be transferred.	

Send an SMS if... (the Internet connection was established)

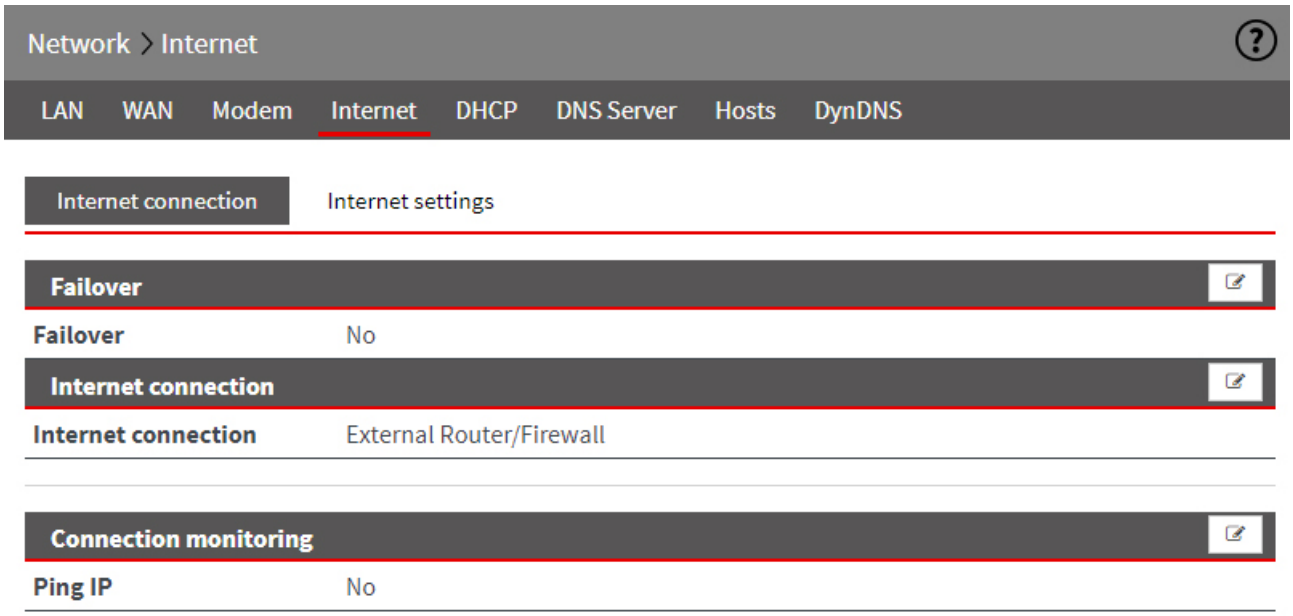


Designation	Description
the Internet connection was established	Check box for enabling/disabling this function. When the function is enabled, the mbNET sends an SMS notification once the mbNET has established a connection to the Internet.
Recipient's phone number	Recipient's phone number to whom the notification should be sent.

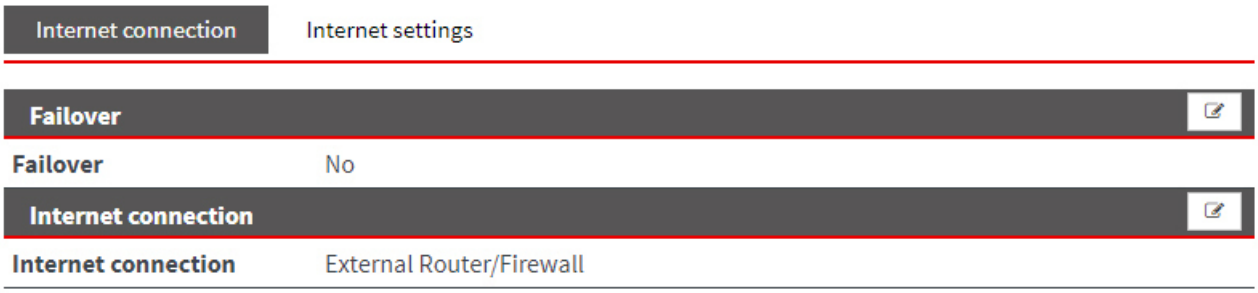
NOTICE

The phone number must not start with 0 (zero).
The entry must be preceded by a country code (example: +49 30 1234567).

22.4 Network > Internet (Internet connection and Internet settings)

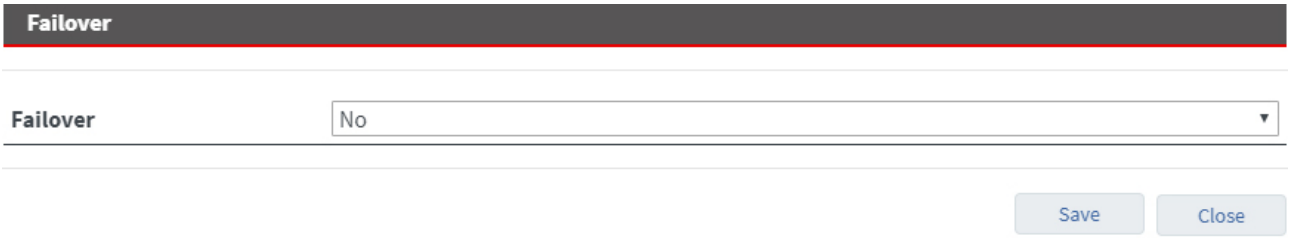


22.4.1 Configure Internet connectivity



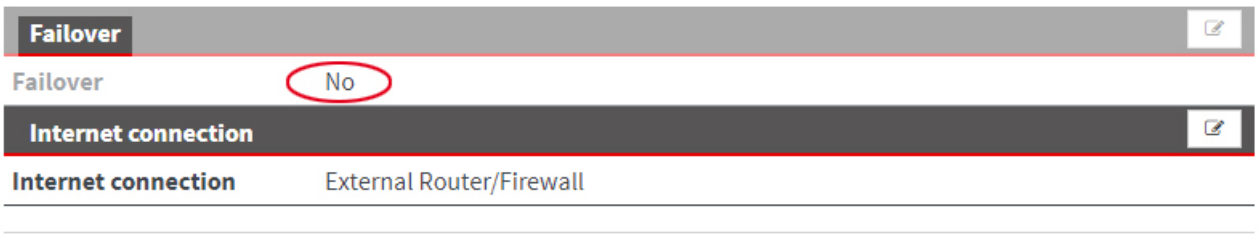
Click the Edit icon to edit the corresponding function.

Reliability



Designation	Description
Reliability	"Yes / No" selection field to activate/deactivate this function. The reliability function allows switching between different Internet connections. If this function is enabled, the Internet interfaces in the desired priority can be entered according to the device type.

Internet connection - failsafe reliability = No -



Click the Edit icon to edit the corresponding function.

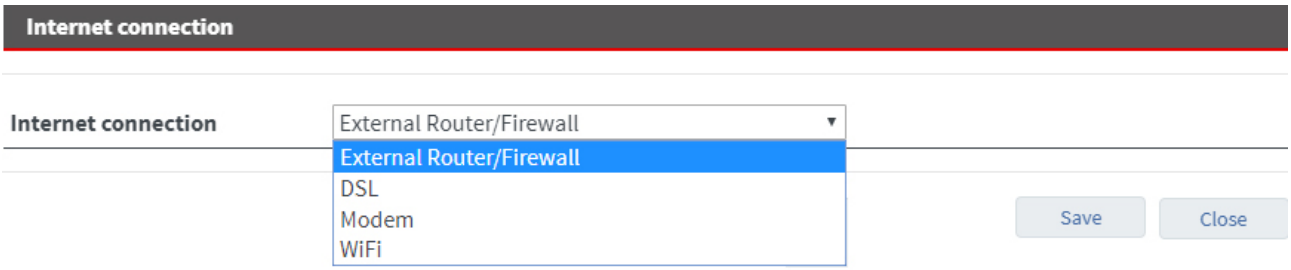
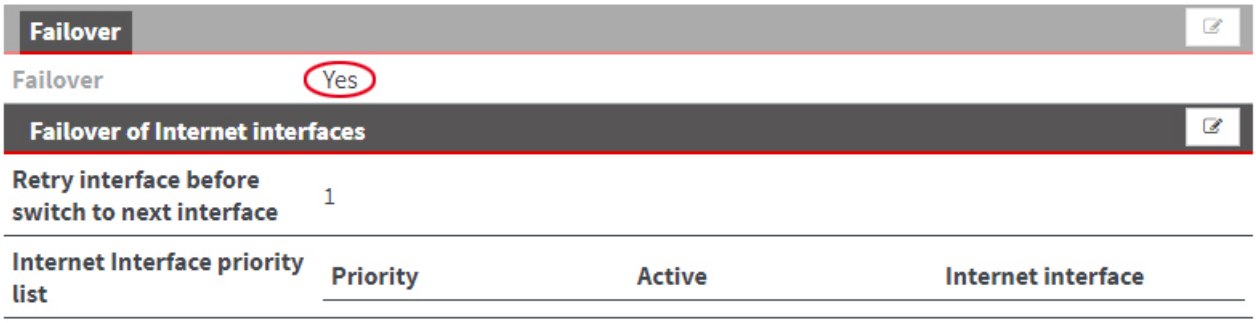


Image 11: The choice of available Internet interfaces depends on the device type and can vary.

Designation	Description
Internet access	Here you select the Internet interface, with which the mbNET should connect to the Internet. Depending on the device type, the following Internet interfaces can be selected: • External Router/Firewall • DSL • Modem • Wi-Fi

Internet connection - failsafe reliability = = Yes -
(failsafe reliability of the Internet interfaces)



Click the Edit icon to edit the corresponding function.

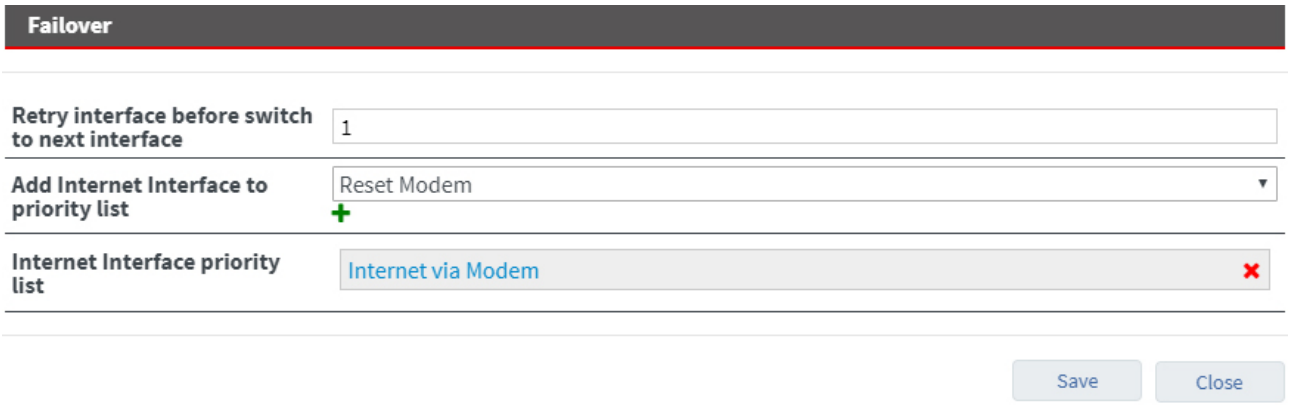


Image 12: The choice of available Internet interfaces depends on the device type and can vary.

Designation	Description
The number of attempts before switching to the next interface	Enter here the number of connection attempts after which the next Internet interface/action is then selected.
Add Internet interface to priority list	▶ Here you can select an Internet interface/action from the selection field. ▶ Click the green plus sign ✚ to add the selected interface/action to the priority list. ▶ Repeat this process as necessary until no interface/action is available.
Internet Interface Priority List	The selected interfaces/actions are listed in order of priority here. By clicking on the red cross ✘ at the end of the line, the relevant interface/action can be deleted.

Internet interface priority list - Example

Failover

Failover	Yes

Failover of Internet interfaces

Retry interface before switch to next interface	1

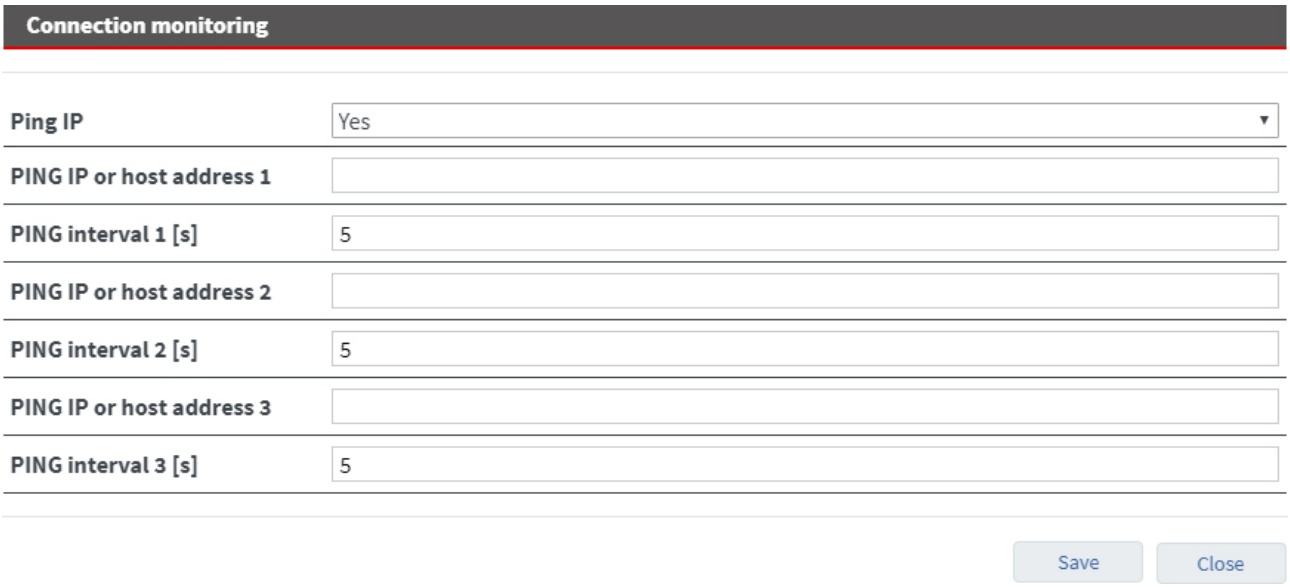
Internet Interface priority list

Priority	Active	Internet interface
1	✔	Internet via WAN
2	✔	Internet via Modem
3	✔	System restart

Image 13: Example of an "Internet interface priority list".

Check the Internet connection (ping IP)

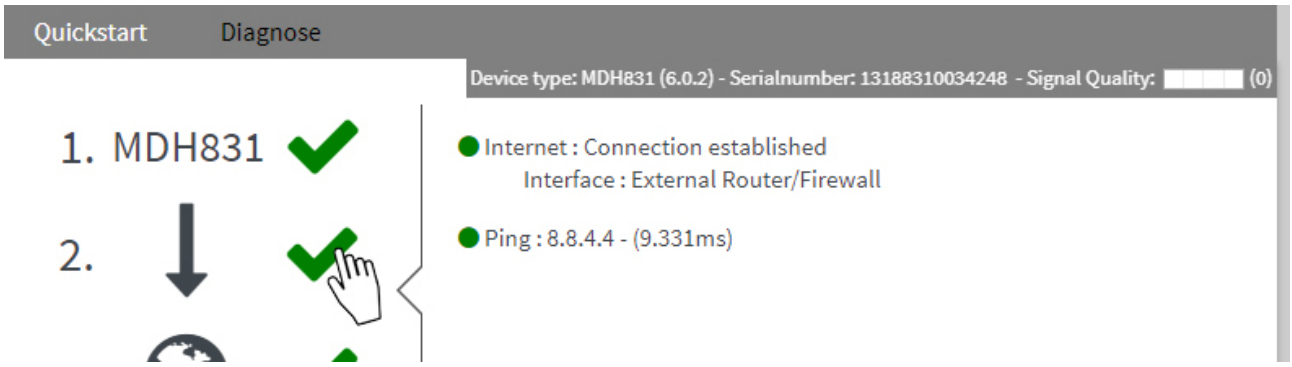
Here you can also check the availability of the internet connection by pinging an IP address.
You can enter up to three different IP addresses with different intervals. The entries are executed one after the other.



Designation	Description
Ping IP	"Yes / No" selection field to activate/deactivate this function.
Ping IP/Host Address 1	Input field for the IP/Host Address. Example: **8.8.4.4** (google-public-dns-b.google.com)
PING Time Interval 1 [s]	Input field for the PING time interval. Example: If you enter "5", the IP/Host Address is pinged every 5 seconds.

NOTICE

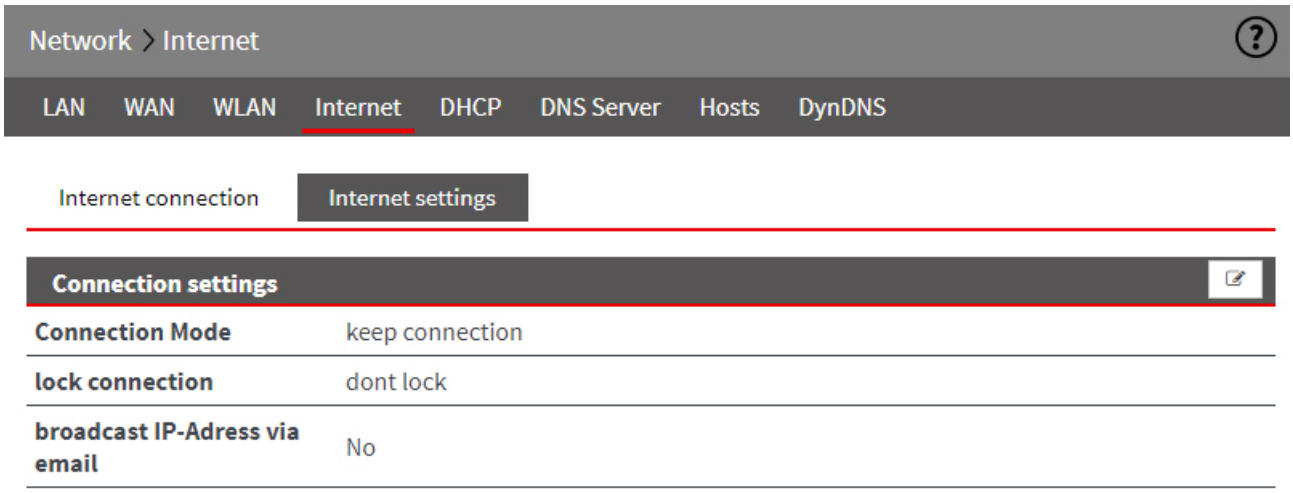
You can see the ping result on the quick start page under **step 2.**



22.4.2 Internet settings (connection settings)

Here, you can specify:

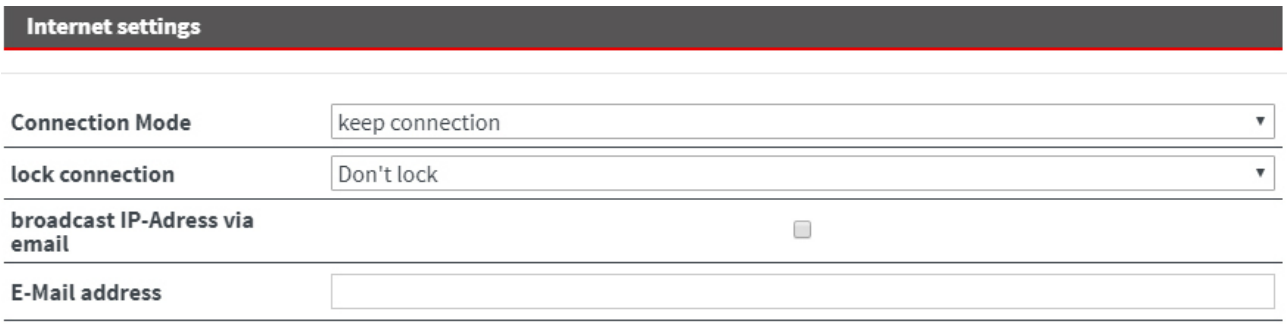
- When the mbNET should connect to the Internet,
- Whether, how and when to disconnect the Internet connection,



Click the Edit icon to edit the corresponding function.

Connection settings,

- **Internet Settings,**



Designation,	Description,
Connection,	Selection field for the type of connection when the mbNET should connect the Internet. – **Maintain connection always** Select this setting if the mbNET should connect to the Internet immediately after switching on/device reboot. **WARNING**: The Internet connection remains permanently on! – **If necessary,** Select this setting if the router will establish a connection to the Internet if one of the following options is selected and executed (a multiple selection is possible): ° Connection for data transfer ° Connection via the "Dial Out" button ° Connect if input active
Lock connection	You can use this selection field to specify whether and on which digital input of the mbNET you want to lock/disconnect the internet connection. • **Do not lock** in this setting, there is no separation by one of the four inputs. • **Input 1; Input 2; Input 3; Input 4** When selecting one of the four digital inputs, the Internet connection is interrupted if the selected input receives a high signal. If the input
Send IP address via email	Check box for enabling/disabling this function. When this function is enabled, the current public IP address will be emailed as soon as an Internet connection is established.
E-mail address	Enter the email address to which the IP address should be sent, if you enabled the function "**Transfer IP address via email**".

- **Settings on Demand**
  *This menu appears when you click on the Internet settings for **Connection type** On Demand.*

Designation	Description
Connection for data transfer	If a subscriber should be accessed via the LAN interface of the mbNET which is not located in the LAN network, a connection to the Internet will be established when the function is enabled.
Ignore traffic from the LAN	If this checkbox is enabled, no connection different to the setting under "Connection type" can be established (for example by a subscriber connected on the LAN who is using the mbNET as a gateway).
Ignore traffic from internal services	If this checkbox is enabled, no connection can be established that is different to the setting under "Connection type" (for example, if an email should be sent through the mbNET or automatic time synchronization should be executed.
Connection via the "Dial Out" button	Enable this function if the connection to the Internet should be established by pressing the "**Dial Out**" button.

NOTICE

Keep the **Dial Out**button pressed until the LED Con starts flashing.

Connect if input active	You can use this selection field to specify whether and via which digital input of the mbNET the internet connection should be established. • **Do not connect** with this setting, there is no connection to the Internet by one of the four digital inputs. • **Input 1; Input 2; Input 3; Input 4** When one of the four digital inputs is selected, the Internet connection is established once the selected input receives a high signal.
Disconnect connection after [s] inactivity	Enter the time period in seconds after which the internet connection will be automatically disconnected if there is no activity (no more data packets are sent).

NOTICE

If you leave this field blank, this function is inactive and the internet connection remains active.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

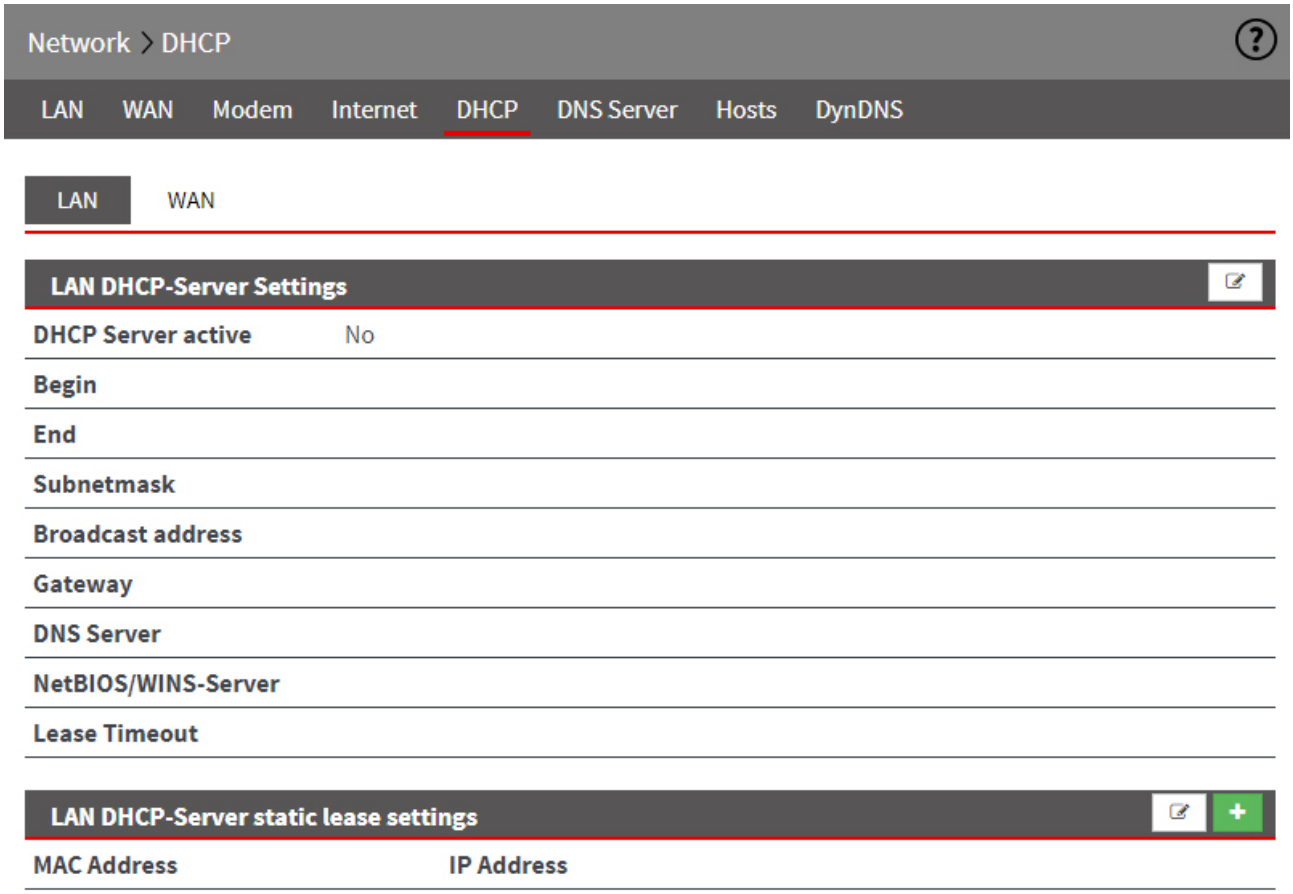
Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

22.5 Network > DHCP

The mbNET can be configured as a DHCP server on the LAN or WAN network.
If this service is active, the router will assign IP addresses to clients from the network independently.
In addition, you can configure the service for the LAN and/or WAN interface. For example, you can supply several devices with it. However, please note that these devices are then connected to the WAN interface and configured under network WAN to DHCP.

NOTICE

Keep in mind that these devices then must be connected to the WAN interface and configured under network WAN to DHCP.



Click the Edit icon to edit the corresponding function.

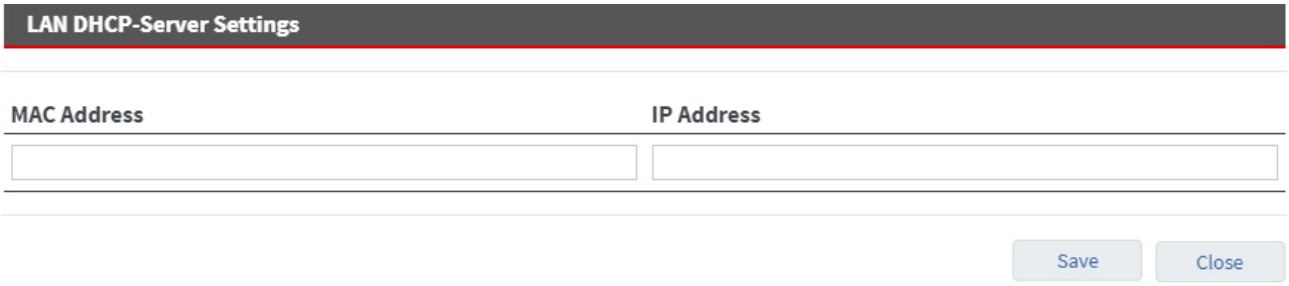
22.5.1 LAN/WAN DHCP server settings

Designation	Description
DHCP Server active	Check box for enabling/disabling this function. By enabling the function the mbNET can be set up as a DHCP server to the corresponding interface.
Start	Enter the start address of the address range managed by the DHCP server.
End	End address of the range managed by the DHCP server.
Subnet mask	Subnet mask of the range managed by the DHCP server.
Broadcast address	The broadcast address of the range managed by the DHCP server.
Gateway	You can optionally enter here the LAN IP address of a router that connects the clients present on the network to the Internet or another network.
DNS Server	You can optionally enter here the LAN IP address of a DNS server on the network. The mbNET can also accept both services, DHCP and DNS.
NetBIOS/WINS Server	You can optionally enter here the address of an existing NetBIOS/WINS server on the network.
Period of validity [s]	Enter the time period [in seconds] for how long a client is assigned a specific IP address by a DHCP server.

22.5.2 LAN/WAN DHCP static lease server settings

Here you can create fixed mappings between IP addresses and MAC addresses. i.e. a device with a specific MAC address always receives the same IP address.

Click on the green plus , in order to create and add an assignment.



Designation	Description
MAC address	Enter the MAC address here. The MAC address must be entered in the format 00:00:00:00:00:00 (colon as separator).
IP address	Enter the IP address that should be assigned to the device.

Confirm your entries by clicking on the **Save** button and repeat the process for another assignment.

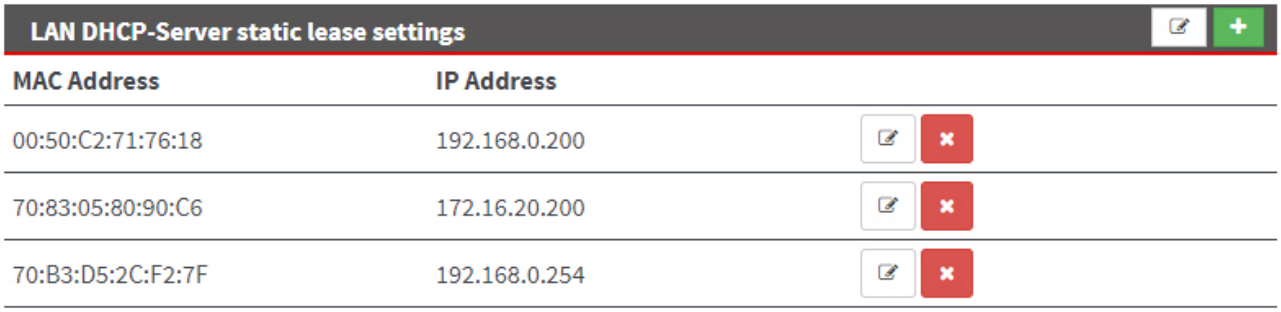


Image 14: Example of an assignment list.

Click the Edit icon , to edit the corresponding entry.

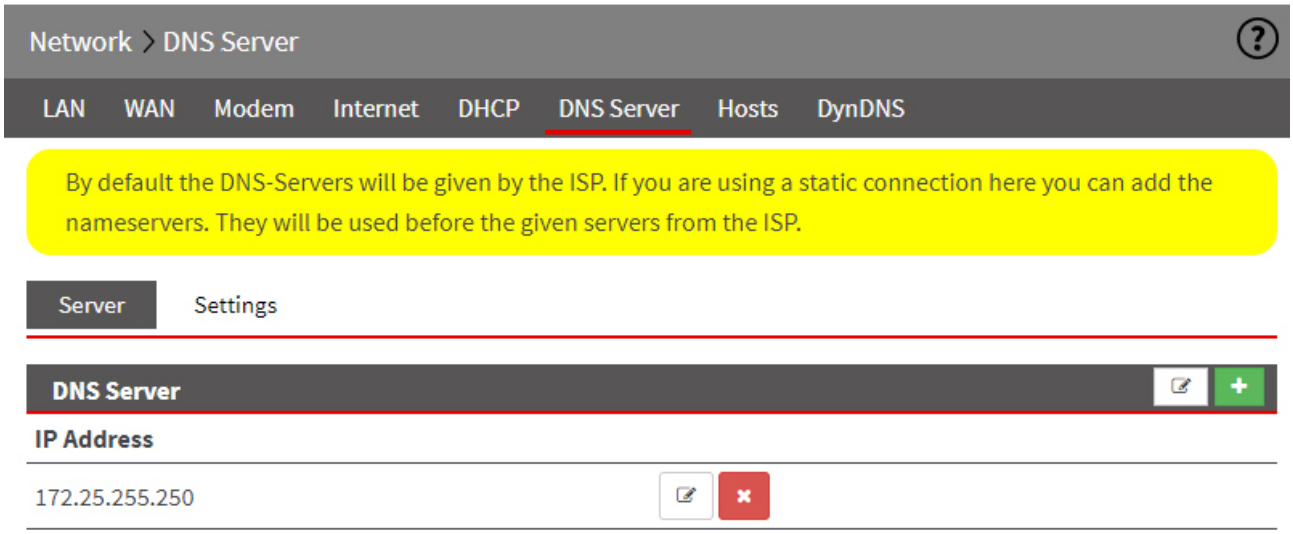
Click the Delete icon , to delete the corresponding entry.

22.6 Network > DNS-Server

Using DNS, IP addresses are converted into names.

At the factory, the mbNET is configured in such a way that the DNS server is assigned by the Internet service provider (IPS).
For permanent connection of the industrial router, a dedicated DNS server can be added here. This is then used before the server assigned by the internet service provider.

Server

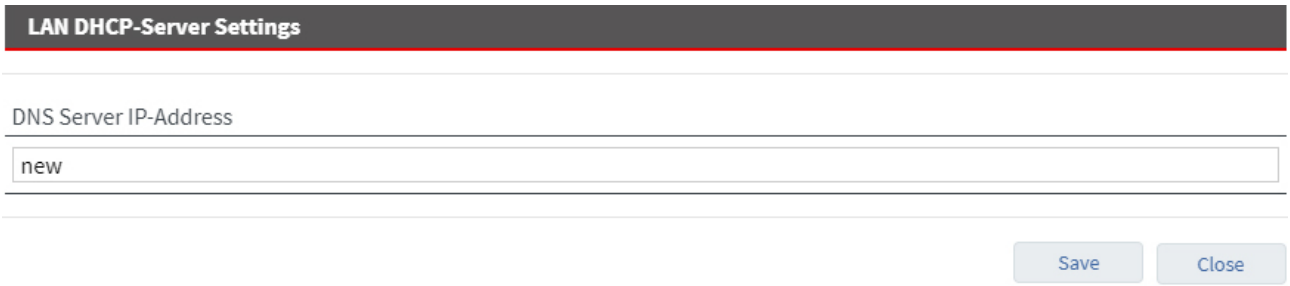


Click on the green plus  , in order to create and add an assignment.

Click the Edit icon  , to edit the corresponding entry.

Click the Delete icon  , to delete the corresponding entry.

Add server



Designation	Description
DNS Server IP Address	Enter the IP address of your DNS server.

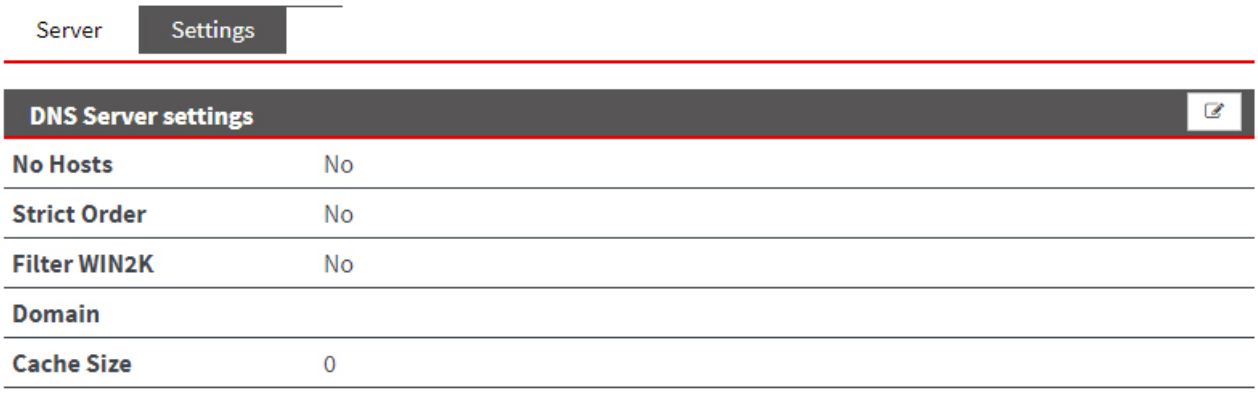
Confirm your entries by clicking on the Save button and repeat the process for further DNS server entries.

NOTICE

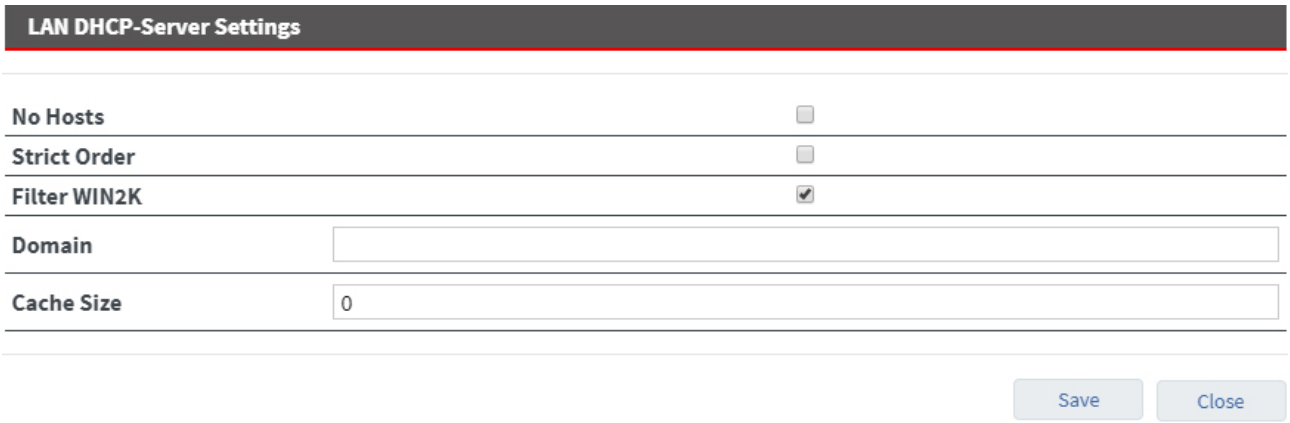
A total of up to five DNS servers can be entered.

Settings

Here, you specify the basic settings for the DNS server.



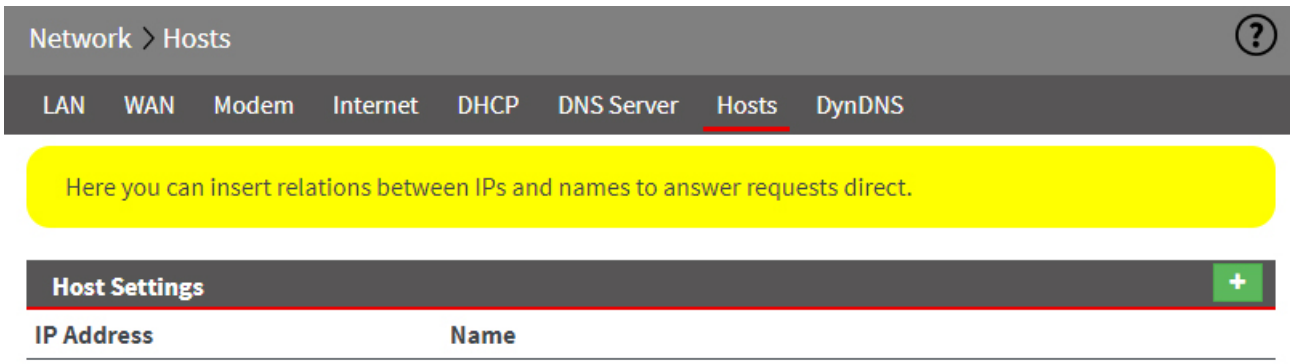
Click the Edit icon to edit the corresponding function.



Designation	Description
No Hosts	Check box for enabling/disabling this function. If this checkbox is activated, the computer names entered under network hosts are not taken into account.
Strict arrangement	Check box for enabling/disabling this function. If this checkbox is activated, the sequence of the entries is exactly as described under "Server".
Filter WIN2K	Check box for enabling/disabling this function. If this checkbox is activated, constant and unnecessary requests from older Windows Clients are filtered. If connection type "On demand" is selected, (*Network* > *Internet* > *Internet Settings* > *Connection Type*), this setting is useful as an internet connection is not established for every request.
Domain	Optional input field for entering a private domain for the network participants.
Memory Size	Enter number of stored names (hosts) here. How to specify how many names can be cached with IP address.

22.7 Network Hosts

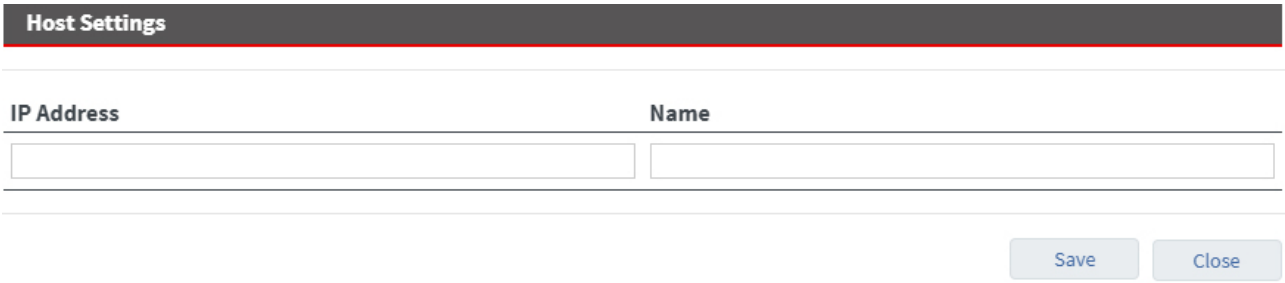
This setting allows you to always assign a specific name to exactly one IP address. DNS queries can therefore be answered directly.



Click on the green plus  to add an assignment.

Host Settings

This setting allows you to always assign a specific name to exactly one IP address. DNS queries can therefore be answered directly.



Designation	Description
IP address	Enter the IP address of the network node (PC, router, etc.), which should be cancelled (e.g.: 172.16.20.1).
Name	Enter the corresponding name of the network user (e.g.: PC-DOKU.venus.local).

NOTICE

In order that a name server request can be answered in Windows, the name must be followed by a dot "." Example: PC-DOKU.venus.local.) is entered. Otherwise, the existing default domain is used.

After clicking on the "Save" button, the new assignment appears in the overview.

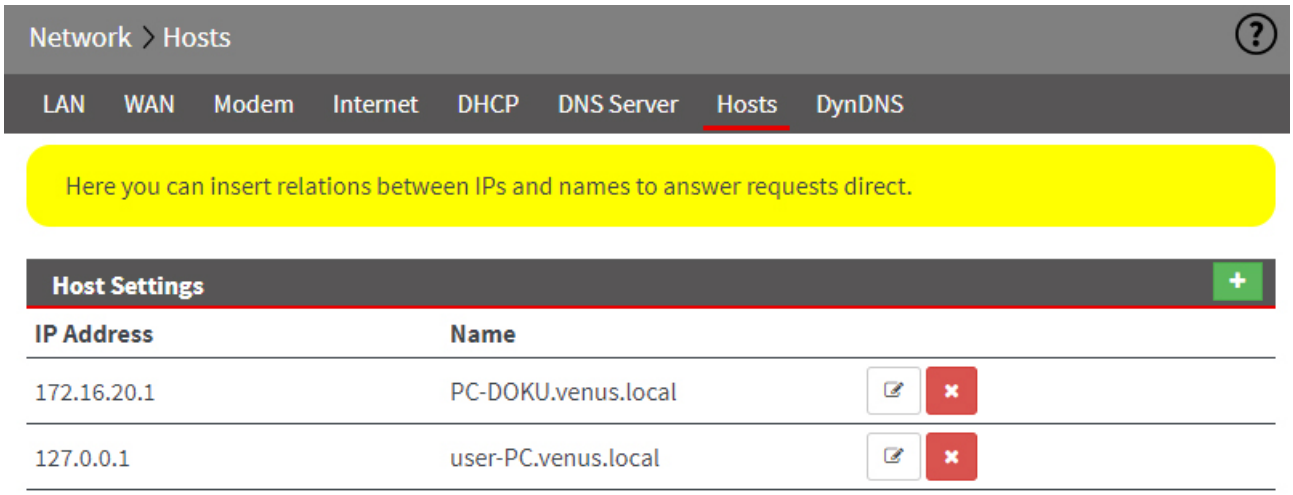


Image 15: Example entries in the Host Settings

Click the Edit icon , to edit the corresponding entry.

Click the Delete icon , to delete the corresponding entry.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

22.8 Network > DynDNS

General

Because the mbNET is assigned a unique IP when dialling to the Internet, it can be found from a client PC using this IP.
Once the mbNET interrupts the connection to the Internet and dials in again, it also receives a new IP address.
The DynDNS service means that the mbNET is always available under the same name. It is used for converting addresses into names and vice versa.

22.8.1 System DynDNS settings (MB Connect Line DynDNS service)

By enabling this function, you use the automatic DynDNS service of MB connect line.
Logging in or registration are not required.
In this case, the name structure is fixed and can only be modified/adapted by the host name (device name).

The name structure is as follows: mbNET serial number.*Device name*.mymbnet.biz The serial number is fixed and the device name can be freely selected.

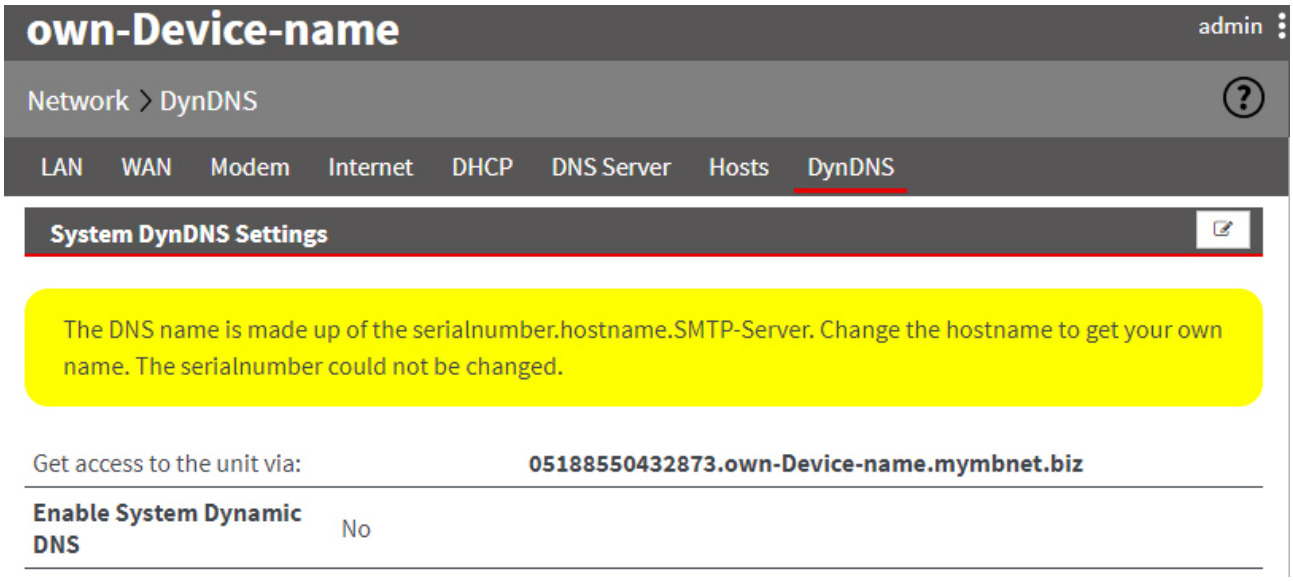
Example:
Serial number: "05188550432873"

\+ **Device name:** "Own-Device name"

= **Name on the Internet:** "05188550432873.own device name.mymbnet.biz"

NOTICE

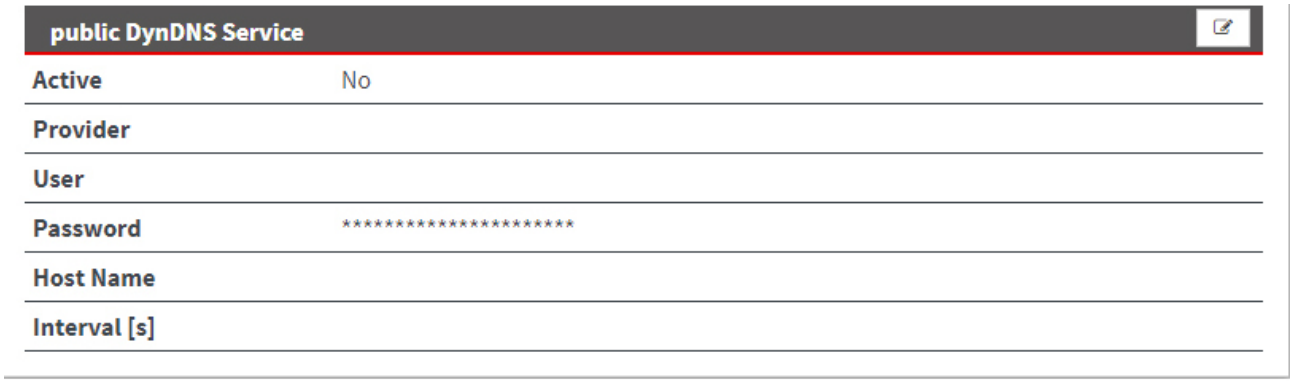
Approx. 1-2 minutes after the mbNET dials into the Internet, the name is available worldwide.



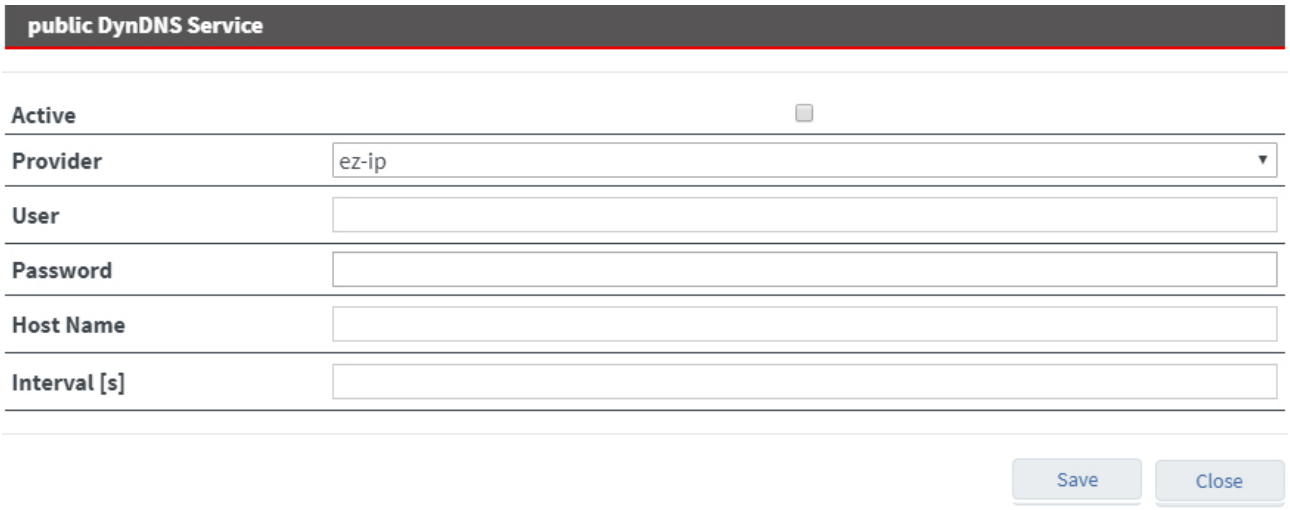
Click the Edit icon to edit the corresponding function and enable the MB connect line DynDNS service.

22.8.2 Public DynDNS service

In order to be able to use a public DynDNS service, you must register/have registered for one of the services that are supported by the mbNET. Registration is normally free.



Click the Edit icon to edit the corresponding function.



Designation	Description
Active	Enable this checkbox if you are registered with a DynDNS service, from the selection list from the drop down list in the provider field and the mbNET should use this service. The mbNET reports the next time it dials into the Internet the current IP address that it has received from the Internet service provider to the DynDNS service.
Provider	Here you can select the DynDNS service for which you are registered.
User	Enter the user name that you entered during registration with your DynDNS service.
Password	Enter the password that you assigned during registration.
Host name	Enter the name that you entered for the mbNET DynDNS service.

Designation	Description
Updating the name after ... [s]	Enter here the interval [seconds] after which the host name should be updated.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

23 Serial (serial port COM)

General

If the IP address of the mbNET is known, the serial interface of the device can be accessed via a dial-up connection or via the Internet.

The **COM** serial port can be configured directly via the web interface to RS232, RS485 and RS422 and the corresponding control commands redirected, e.g. to a connected controller or a connected device.

Depending on the device type, the interface is executed as a **MPI/PROFIBUS** interface.
Via the MPI/PROFIBUS interface, it is possible to remotely access controllers (e.g. S7-300/400). The MPI/PROFIBUS interface supports baud rates of up to 12 Mbps.

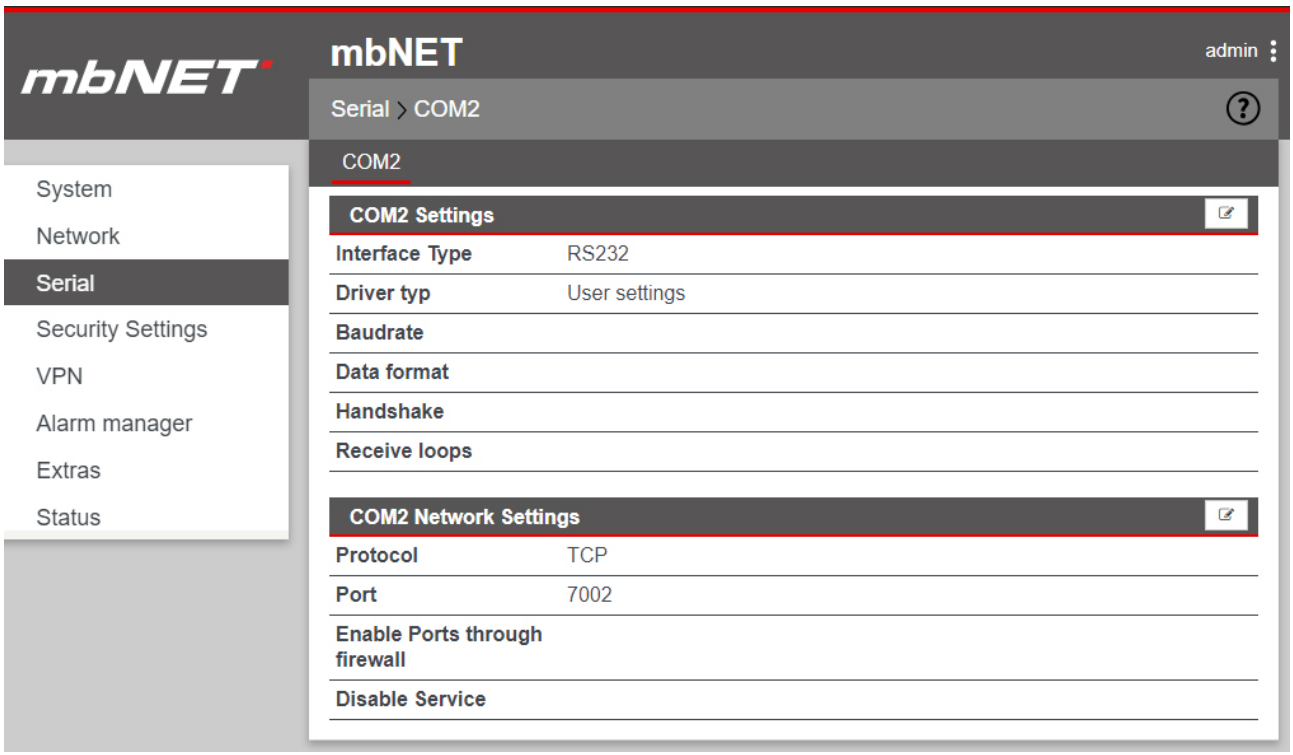
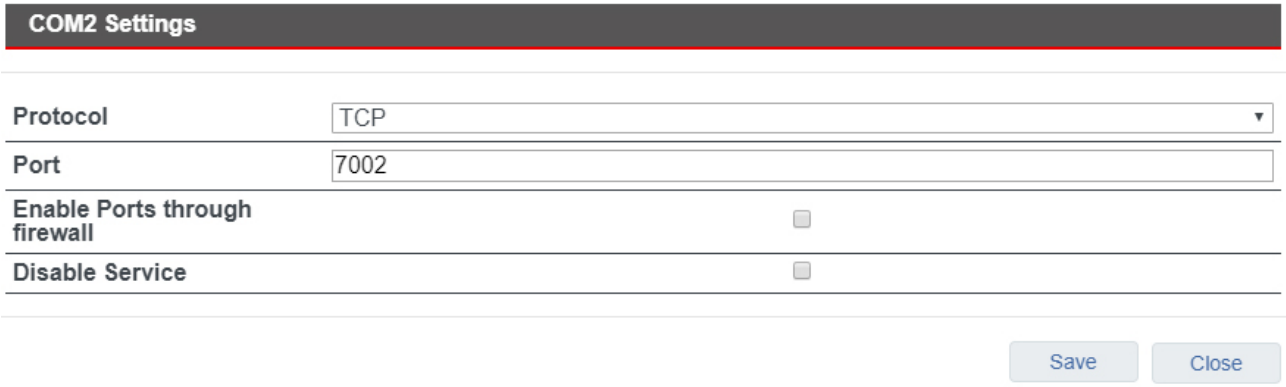


Image 16: The "Serial" menu depends on the device type and can vary.

Click the Edit icon to edit the corresponding function.

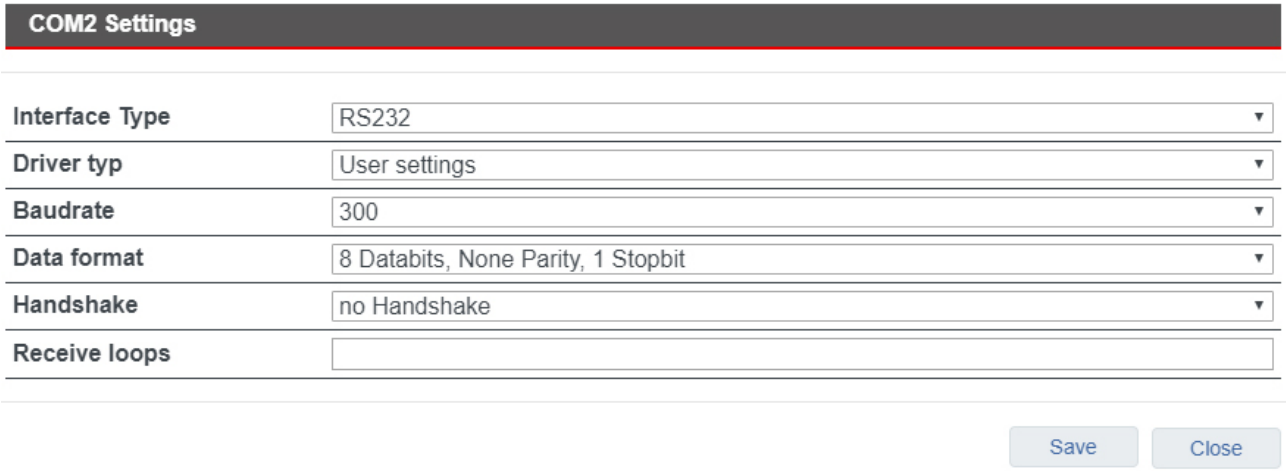
23.1 COM settings

Driver type: System driver



Designation	Description
Interface type	Use this selection field to set the interface type. The options are: RS232, RS485 2-wire, RS485 4-wire, RS422
Driver type	When choosing a **System Driver**, a range of product- and company-specific device drivers are available to control your serial devices.
Driver	selection field with product and company-specific device drivers, for controlling serial gates.

Driver type: User settings



Designation	Description
Interface type	Use this selection field to set the interface type. The options are: RS232, RS485 2-wire, RS485 4-wire, RS422
Driver type	Select the driver type **User Preferences**, if no matching driver is available in the drop-down list or if you want to make your own settings.
Bit rate	Enter the baud rate of the communication here.
Data format	Select one of the settings for data bits, parity and stop bits.

Designation	Description
Flow control	Select the type of flow control.
Number of receive queries for generating a telegram	This is a reception counter for the serial signals. Enter here the number of cycles that the system runs through until the data packet is sent.

23.2 COM network settings

Designation	Description
Protocol	Select the appropriate driver for your connected devices.
Port	Enter the port for the network or Internet communications. The port can be chosen freely, but it must match the settings in the VCOMLAN2.
Enable ports in the firewall	The checkbox must be enabled so that you can communicate via the specified port. Otherwise, all signals/packages are blocked/discarded. This rule is only applicable when you access the serial interfaces using the public address. If there is an existing VPN connection you communicate via the local network address.
Lock service	Check box for enabling/disabling this function. If this function is enabled, the serial driver to communicate between mbDIALUP/VCOM-LAN and serial port is not started.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

23.3 COM2 in the MPI/PROFIBUS version

Communication with the S7 via

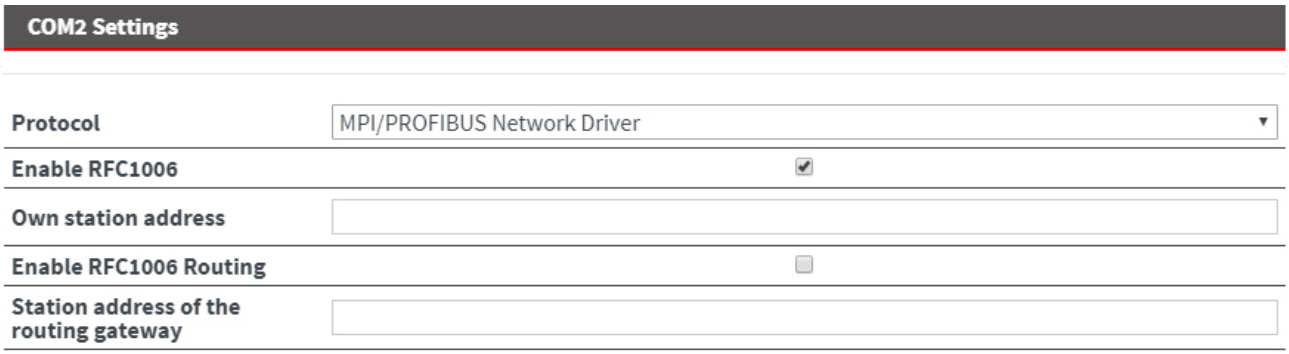
- VCOM LAN2 (PC adapter in the SIMATIC Manager)
- RFC1006
- mbNETS7 driver (installable directly in the SIMATIC Manager)

23.3.1 COM2 Settings

Protocol: MPI/PROFIBUS Network Driver

NOTICE

The Protocol Choice **MPI/PROFIBUS network driver** requires the installation of a network driver on the client PC beforehand! Only in conjunction with the option RFC1006 can a separate driver installation be dispensed with and the "TCP/IP (Auto)" option under the PG/PC interface used. RFC1006 uses TCP port 102.



Designation	Description
Protocol	Protocol selection field. You can choose between a connection via **MPI/Profibus network driver** or **VCOM LAN2/PC adapter**.
Enable RFC1006 protocol	Check box for enabling/disabling this function.
own station address	If RFC1006 is enabled, enter a unique MPI/DP station address for the router (mbNET).

NOTICE

With this station address, the connected routers in the MPI/DP network logs on. This is necessary if the communication is exclusively via RFC1006. In a mixed operation of connections with network drivers and RFC1006, the router always logs in using the address specified in the first connection used.

Enable routing via RFC1006	Check box for enabling/disabling this function. The activated function enables routing via RFC1006.
Station address of the Routing Gateway	If routing function is enabled via RFC1006, you must enter the address of the routing gateway here. (Address 14 in the example below).

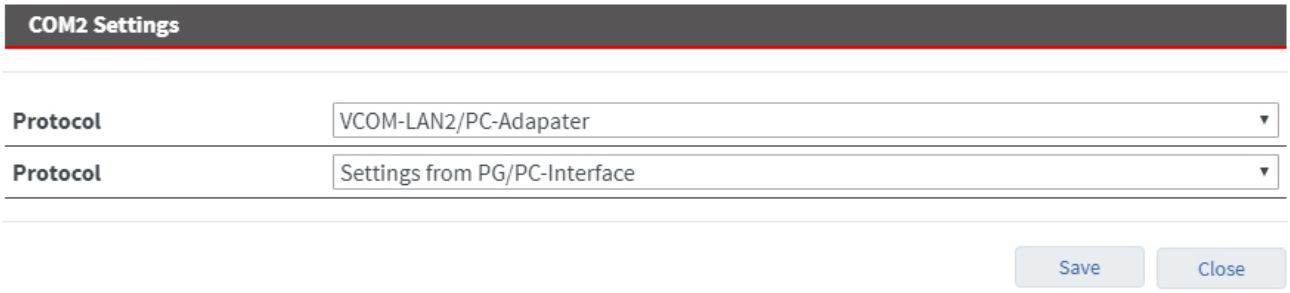
NOTICE

If a bus participants (slave) is to be accessed on a subordinate station that is not directly connected to the network, the station address of the PLC must be registered as a routing gateway in the router with the gateway (master).

Example:
If the PLC (master) is connected to the router (address 13) via MPI-bus (address 14), a participant (address 5) is connected to the Profibus of the master (address 4). The routing must be enabled in order to now access the Profibus using the router (address 13) via MPI on the participants with address 5 on the Profibus.

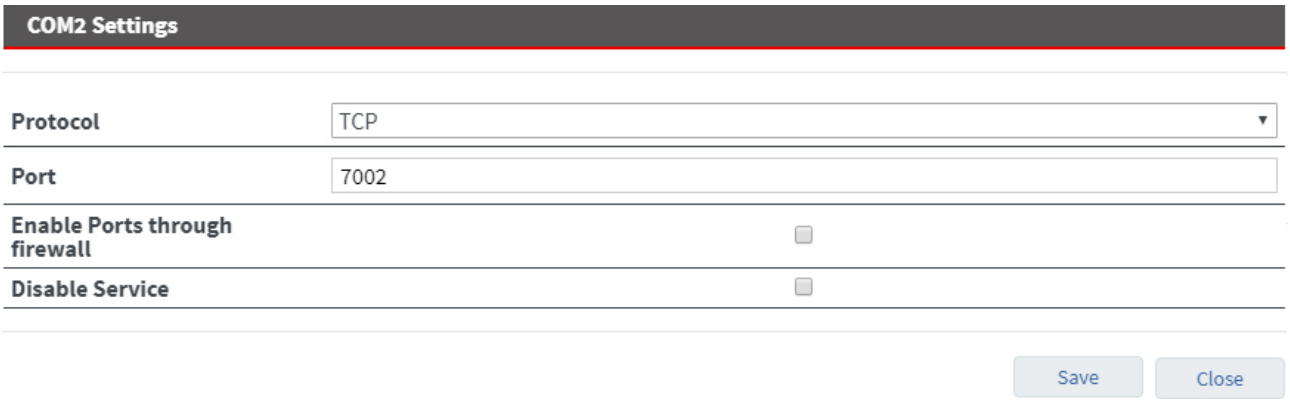
Protocol: VCOM LAN/PC Adapter

In the case of protocol choice **VCOM LAN2/PC Adapter**, the PG/PC interface must be set to a PC adapter (MPI/PROFIBUS). If the bus speed is higher than 1.5 MBit/s, this must be specified manually.



Designation	Description
Protocol	Protocol selection field. You can choose between a connection via **MPI/Profibus network driver** or **VCOM LAN2/PC adapter**.
Protocol	MPI/PROFIBUS baud rate selection field.

23.3.2 COM2 Network settings



Designation	Description
Protocol	Select the appropriate driver for your connected devices.

Designation	Description
Port	Enter the port via which the communication should take place here.
Enable ports in the firewall	If this checkbox is enabled, the port indicated above is enabled for direct access from the Internet in the firewall.
Lock service	Check box for enabling/disabling this function. If this function is enabled, the serial driver to communicate between mb-DIALUP/VCOM-LAN and serial port is not started.

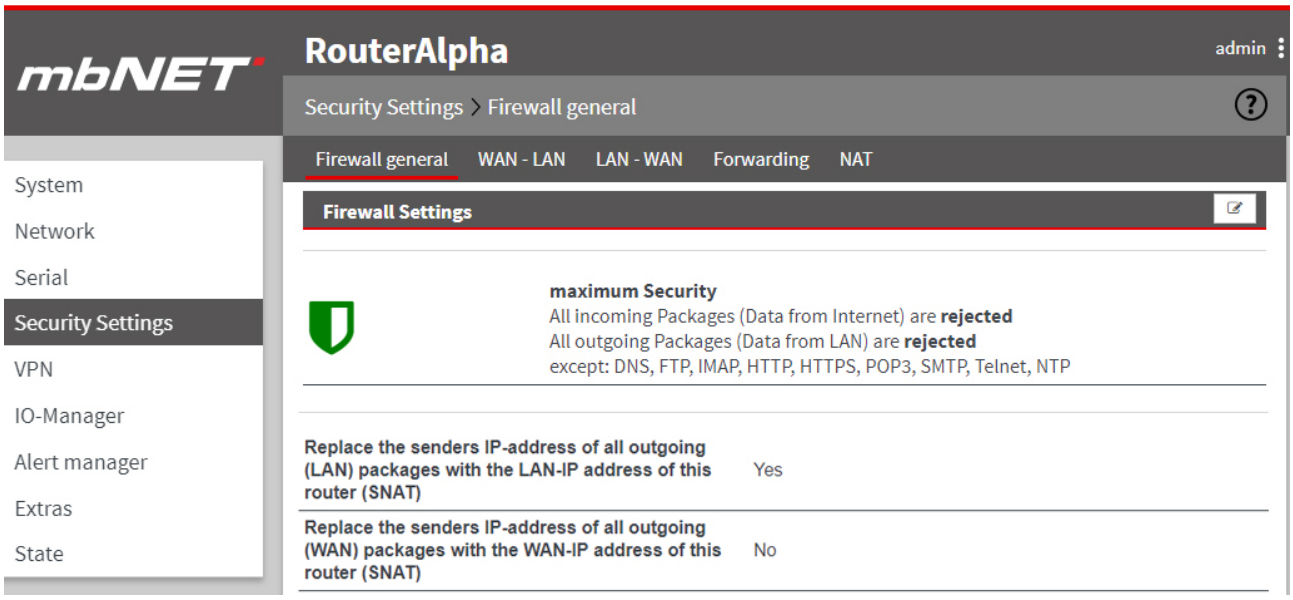
Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

24 Security settings

The mbNET has a built-in firewall to protect against strange or/and unauthorized access/connection attempts. Incoming and outgoing data traffic is monitored, logged and enabled/disabled via this firewall.



The following submenus are listed under the **Security settings** menu:

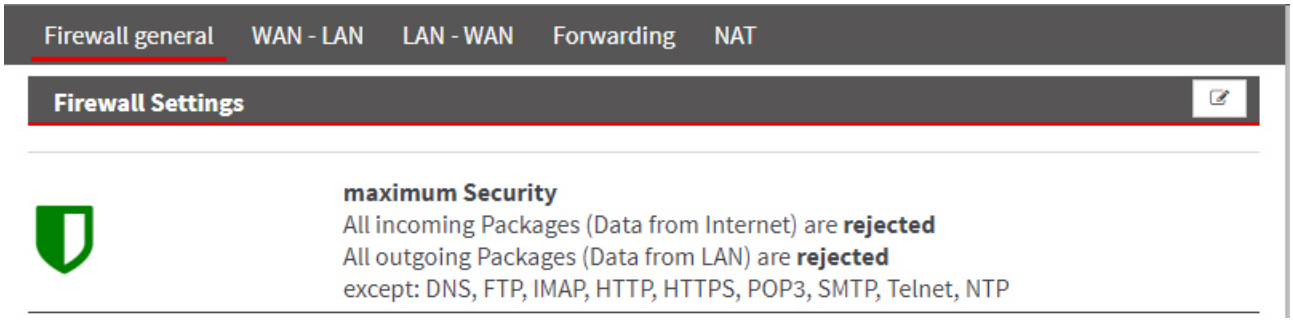
Submenu	Description
Firewall General	Here you can specify the basic firewall settings.
WAN - LAN	This setting is used to regulate the **incoming** traffic.
LAN - WAN	This setting is used to regulate the **outgoing** traffic.
Forwarding	Here you can forward requests from specific IP addresses and ports to redefined IP addresses and ports.
NAT	"**SimpleNAT**" allows you to grant access to an IP address from the LAN Power Plant 1:1 in the WAN Ethernet network. Using the "**1:1 NAT**" Is it possible to connect two networks that are in the same address range with each other.

Click the Edit icon , to edit a function or an element.

Click the Add icon to add an item.

Click the Delete icon to delete/remove an item.

24.1 Security Settings > Firewall General



The firewall can generally be configured in one of the following four variants:

- **Maximum security level**
  all incoming packets (data from the Internet) will be **rejected**
  all outgoing packets from the LAN (data) will be **rejected**
  except: DNS, FTP, IMAP, POP3, SMTP, HTTP, HTTPS, Telnet, NTP

  Enable signals for the data traffic must be configured accordingly. Both incoming and outgoing traffic will be blocked. To access the web interface (from outside!), the TCP protocol and destination port 443 entered and activated in the **WAN - LAN** *rules. However, if you start a VPN connection, access will be enabled accordingly for the data packets from the VPN tunnel.*

- **Normal security level**
  All incoming packets (data from the Internet) will be **rejected**
  All outgoing packets from the (LAN data) will be **accepted**

  In this variant, the incoming traffic (data from the Internet) is blocked while the outgoing data will be accepted.

- **Minimum level of security**
  All incoming packets (data from the Internet) will be **accepted.**
  All outgoing packets (LAN data) will be **accepted**.

  In this variant, all incoming and outgoing data is accepted.

- **Firewall off**
  All incoming packets (data from the Internet and WAN Ethernet*****) will be **accepted.**
  All outgoing packets (LAN data) will be **accepted.**
  Routing between all interfaces is **switched on**.

  When you select this variant, all incoming and outgoing data is accepted. In addition, all entered firewall rules are deactivated and routing between **WAN-LAN** *and* **WAN-LAN** *is active.*

*****In the case of devices without a WAN Ethernet interface, this is only "Data from the Internet".

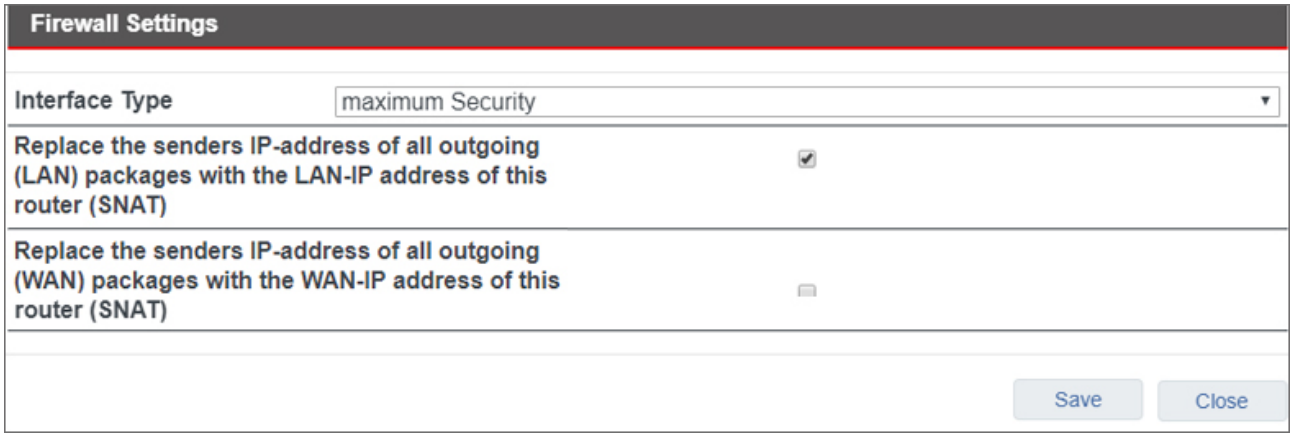
NOTICE

The "**Minimum security level**" and "**Firewall off**" variants should only be selected for a short period of time and for test purposes or at initial start-up, if you want to ensure that a configured rule should not apply.

ATTENTION! Any data traffic from inside to outside and external access are possible! The integrity of your mbNET and the connected devices is threatened when you select one of these two variants!

Click the Edit icon , to set a security level.

Firewall settings



Designation	Description
Interface type	Selection field for one of the four security levels
Replace all sender IP addresses of all outgoing LAN packets with the own LAN IP address of the router (SNAT)	Enabling this function (SNAT) allows access from the outside (e.g. via VPN) to LAN participants, without them having to set the mbNET as a default gateway. The actual source IP in an incoming IP packet is thereby replaced by the IP of the mbNET LAN interface. This is a significant benefit when integrating the remote maintenance into existing network structures, because they don't need to be changed.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

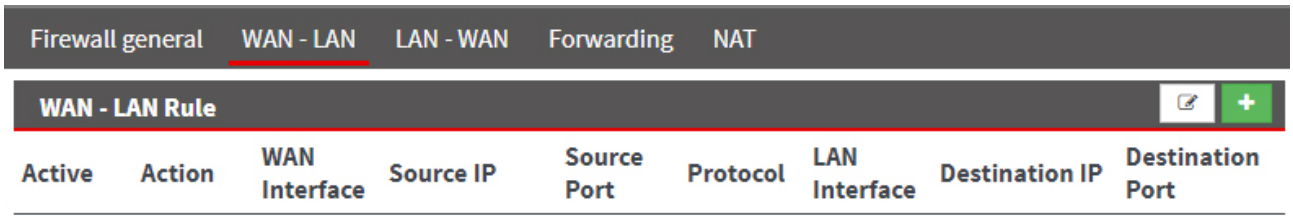
24.2 Security Settings > WAN LAN (configuration of the firewall rules)

This setting controls the **incoming** traffic, i.e. the following settings only apply to incoming traffic from the outside.

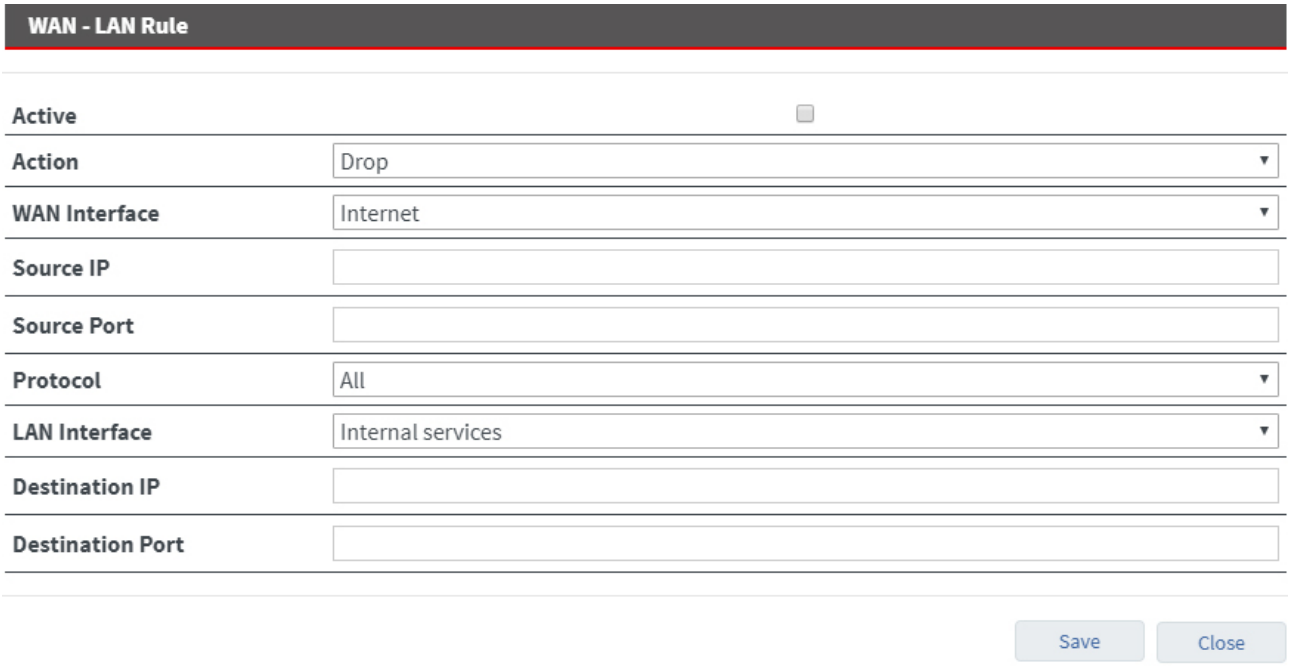
From the point of view of the mbNET Firewall is "**WAN**" always the currently active interface to the Internet. Depending on the setting under "**Network > Internet**" the following rule results:

Internet connection:

- **Connect to the Internet via WAN (external router)**
  Here the WAN Ethernet port is the interface to the Internet. The firewall controls the traffic from the WAN Ethernet to the LAN Ethernet.
- **Connect to the Internet via modem**
  Here the modem is the interface to the Internet. The firewall controls the data traffic from the modem to the LAN Ethernet. The entire data traffic on the WAN Ethernet interface will be blocked.
- **Connect to the Internet via WAN**
  here is the "DSL data traffic" over the WAN Ethernet is the interface to the Internet. The firewall controls the traffic from the DSL modem to the LAN Ethernet. The other data traffic on the WAN Ethernet interface will be blocked.



Click on the green plus  , to add a rule.



Designation	Description
Active	Checkbox for enabling/disabling this firewall rule.

Designation	Description
Campaign	Selection field for the applicable action. The options are: • **Discard**When you select this action, no data packets can pass and the packets will be deleted immediately. The sender receives no information about the whereabouts of the data packets. • **Reject** The data packets are rejected. The sender receives a signal that the data packets have been rejected. • **Accept** Here, the data packets are allowed through.
WAN interfaces	You can use this selection field to determine which WAN interface* should normally be used. The options are: • **Internet** • **WAN Ethernet** • **OpenVPN** • **IPsecVPN** • **PPTPVPN** • **All** * The selection field for the WAN interface can vary depending on the type of router.
Origin IP	Enter the source IP addresses of incoming data packets for which the firewall rule applies. If you leave this field empty (blank), these rules will be applied to all data traffic and only on the selected interface.
Origin port	Enter the source ports of incoming data packets for which the firewall rule applies. If you leave this field empty (blank), these rules will be applied to all data traffic and only on the selected interface.
Protocol	Selection field for the transfer protocol to use. The options are: • **All** - the set rule applies to **ALL** protocols • **TCP** - the set rule applies only to the TCP protocol • **UDP** - the set rule applies only to the UDP protocol • **ICMP** - the set rule applies only for the ICMP protocol
LAN interfaces	You can use this selection field to determine which LAN interface* should normally be used. The options are: • **Internal services** • **LAN Ethernet** • **All**
Destination IP	Enter the IP address to which data packets are to be forwarded.
Destination-Port	Enter the ports to which the data packets are to be forwarded.

NOTICE

You can enter address **ranges** in the input fields for the **IP** address.
Example of address ranges: 192.168.0.100-192.168.0.110 or 192.168.0.20/30

Address listings are **not** possible!

In the input fields for the **ports**, you can enter **ranges or enumerations**.
Example of a port range: 502-504
Example of port enumeration: 502,677,555
Both, range and enumeration **can not** be used simultaneously in the same field.

NOTICE

Ranges must be separated by a **hyphen** (-) and **enumerated** by **comma** (,).

No spaces between the elements to be separated!

NOTICE

The input of IP and port is not mandatory. If neither an IP nor a port is specified, a rule applies only to the selected interfaces.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

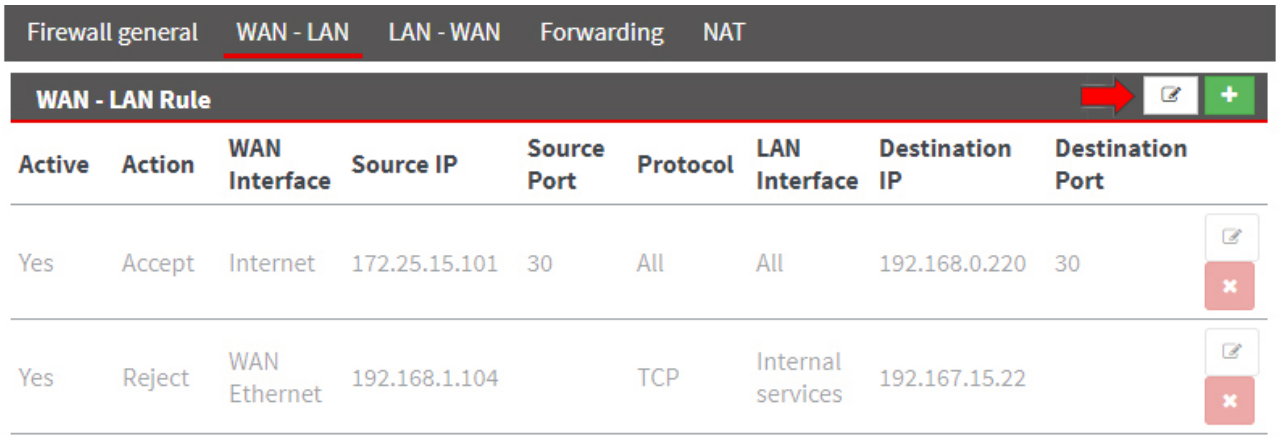
WAN - LAN Rule

Active	Action	WAN Interface	Source IP	Source Port	Protocol	LAN Interface	Destination IP	Destination Port
Yes	Accept	Internet	172.25.15.101	30	All	All	192.168.0.220	30
Yes	Reject	WAN Ethernet	192.168.1.104		TCP	Internal services	192.167.15.22	

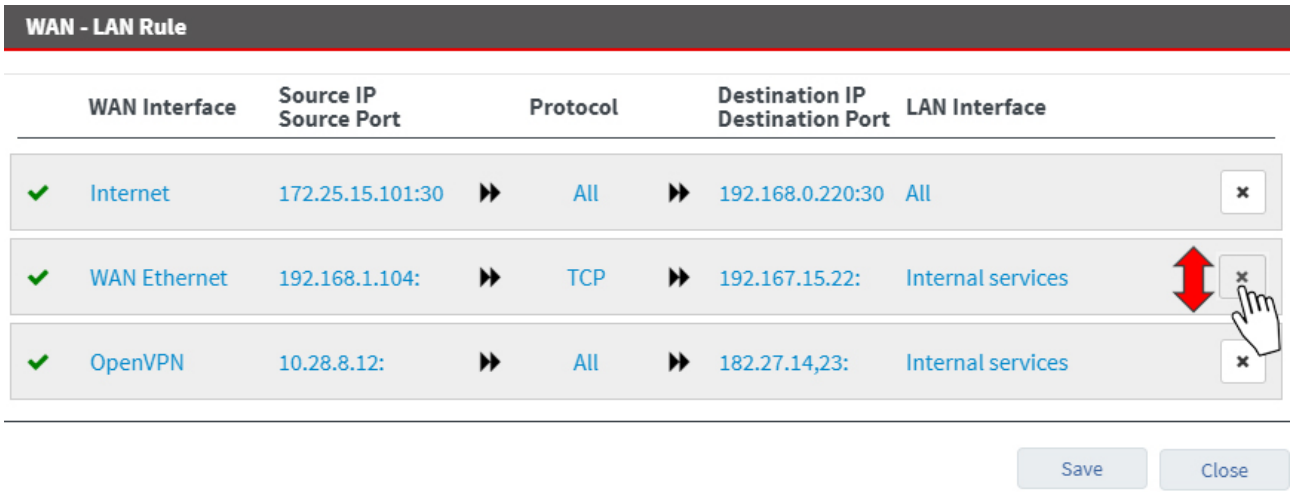
Image 17: The firewall rule example entry

24.2.1 Edit firewall rule

Change the entered rule order

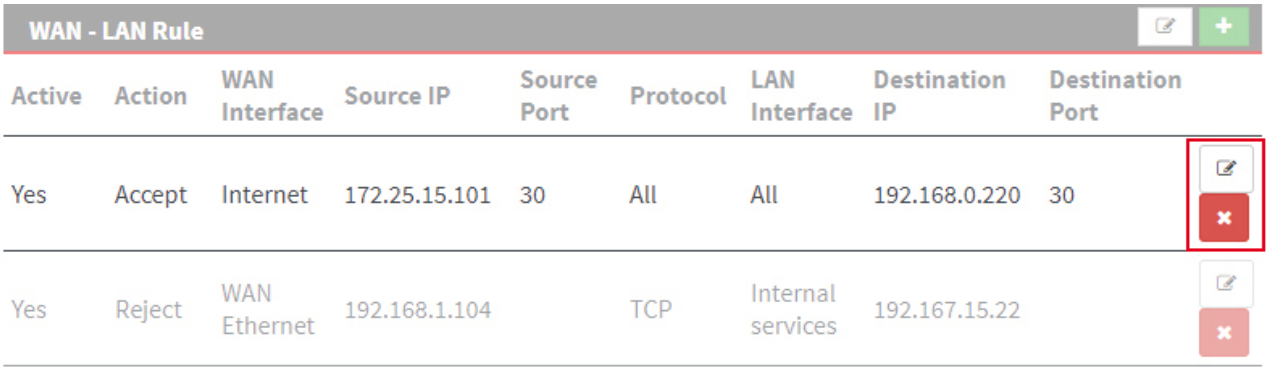


Click on the Edit icon in the header of the overview to change the sequence of the entered change rules.



Here you can move up and down (drag and drop) to change the sequence of the firewall rules.

Change/delete firewall rule



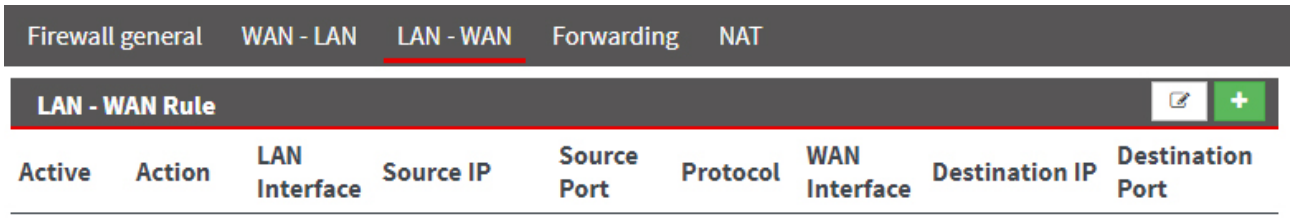
Click on the Edit icon at the end of the line of the registered rule to edit it.

Click the Delete icon , to delete the corresponding entry.

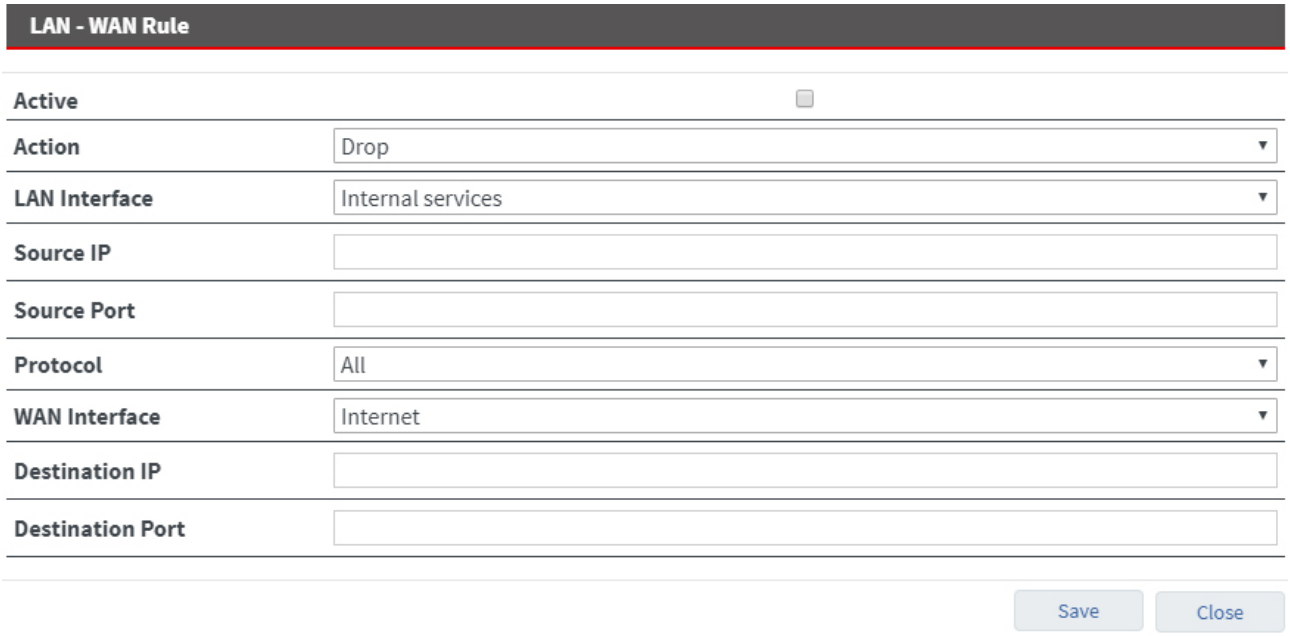
24.3 Security Settings > LAN-WAN (configuration of the firewall rules)

This setting controls the **outgoing** traffic, i.e. the following settings only apply to outgoing traffic.

From the point of view of the mbNET Firewall is "**WAN**" always the currently active interface to the Internet.



Click on the green plus  , to add a rule.



Designation	Description
Active	Checkbox for enabling/disabling this firewall rule.
Campaign	Selection field for the applicable action. The options are: • **Discard** When you select this action, no data packets can pass and the packets will be deleted immediately. The sender receives no information about the whereabouts of the data packets. • **Reject** The data packets are rejected. The sender receives a signal that the data packets have been rejected. • **Accept** Here, the data packets are allowed through.

Designation	Description
LAN interfaces	You can use this selection field to determine which LAN interface* should normally be used. The options are: • **Internal services** • **LAN Ethernet** • **All**
Origin IP	Enter the source IP addresses of incoming data packets for which the firewall rule applies. If you leave this field empty (blank), these rules will be applied to all data traffic and only on the selected interface.
Origin port	Enter the source ports of incoming data packets for which the firewall rule applies. If you leave this field empty (blank), these rules will be applied to all data traffic and only on the selected interface.
Protocol	Selection field for the transfer protocol to use. The options are: • **All** - the set rule applies to **ALL** protocols • **TCP** - the set rule applies only to the TCP protocol • **UDP** - the set rule applies only to the UDP protocol • **ICMP** - the set rule applies only for the ICMP protocol
WAN interfaces	You can use this selection field to determine which WAN interface* should normally be used. The options are: • **Internet** • **WAN Ethernet** • **OpenVPN** • **IPsecVPN** • **PPTPVPN** • **All** * The selection field for the WAN interface can vary depending on the type of router.
Destination IP	Enter the IP address to which data packets are to be forwarded.
Destination-Port	Enter the ports to which the data packets are to be forwarded.

NOTICE

You can enter address **ranges** in the input fields for the **IP** address.
Example of address ranges: 192.168.0.100-192.168.0.110 or 192.168.0.20/30

Address listings are **not** possible!

In the input fields for the **ports**, you can enter **ranges or enumerations**.
Example of a port range: 502-504
Example of port enumeration: 502,677,555
Both, range and enumeration **can not** be used simultaneously in the same field.

NOTICE

Ranges must be separated by a **hyphen** (-) and **enumerated** by **comma** (,).

No spaces between the elements to be separated!

NOTICE

The input of IP and port is not mandatory. If neither an IP nor a port is specified, a rule applies only to the selected interfaces.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

Firewall general | WAN - LAN | LAN - WAN | Forwarding | NAT

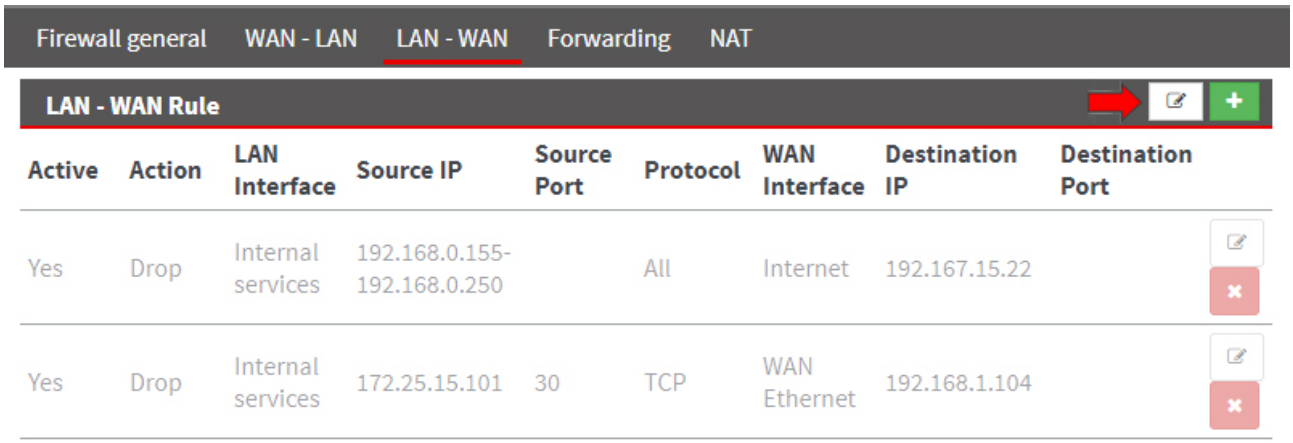
LAN - WAN Rule

Active	Action	LAN Interface	Source IP	Source Port	Protocol	WAN Interface	Destination IP	Destination Port
Yes	Drop	Internal services	192.168.0.155-192.168.0.250		All	Internet	192.167.15.22	
Yes	Drop	Internal services	172.25.15.101	30	TCP	WAN Ethernet	192.168.1.104	

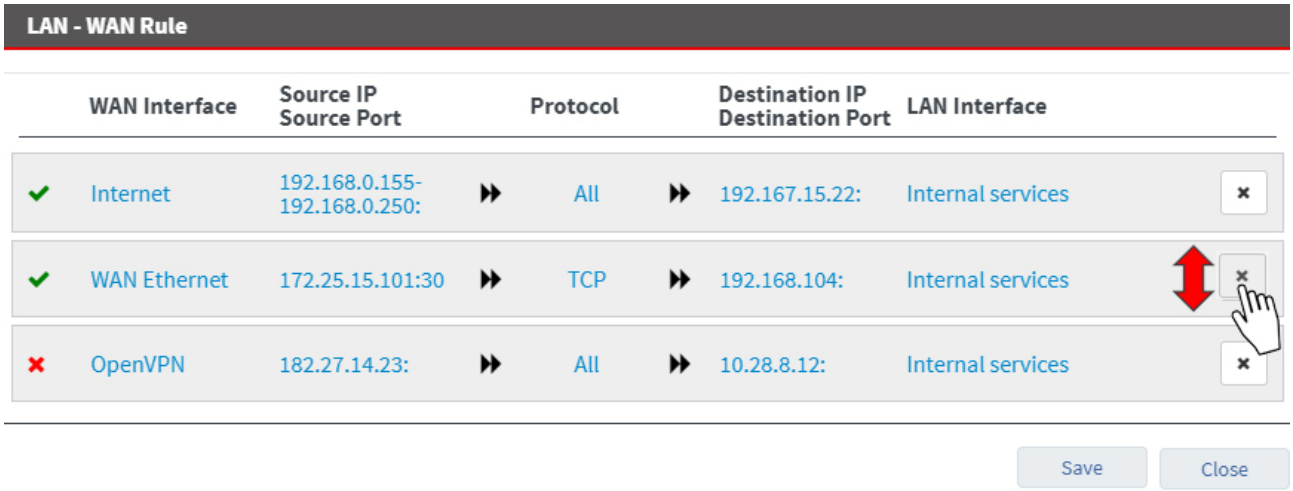
Image 18: The firewall rule example entry

24.3.1 Edit firewall rule

Change the entered rule order

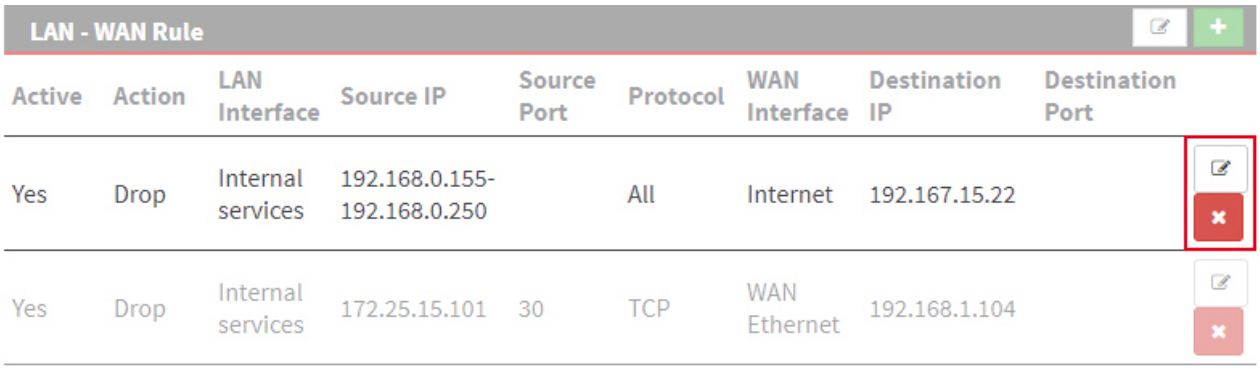


Click on the Edit icon in the header of the overview to change the sequence of the entered change rules.



Here you can move up and down (drag and drop) to change the sequence of the firewall rules.

Change/delete firewall rule



LAN - WAN Rule

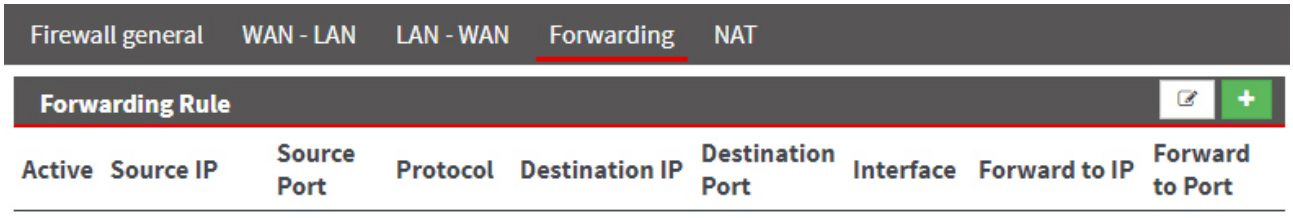
Active	Action	LAN Interface	Source IP	Source Port	Protocol	WAN Interface	Destination IP	Destination Port
Yes	Drop	Internal services	192.168.0.155-192.168.0.250		All	Internet	192.167.15.22	
Yes	Drop	Internal services	172.25.15.101	30	TCP	WAN Ethernet	192.168.1.104	

Click on the Edit icon at the end of the line of the registered rule to edit it.

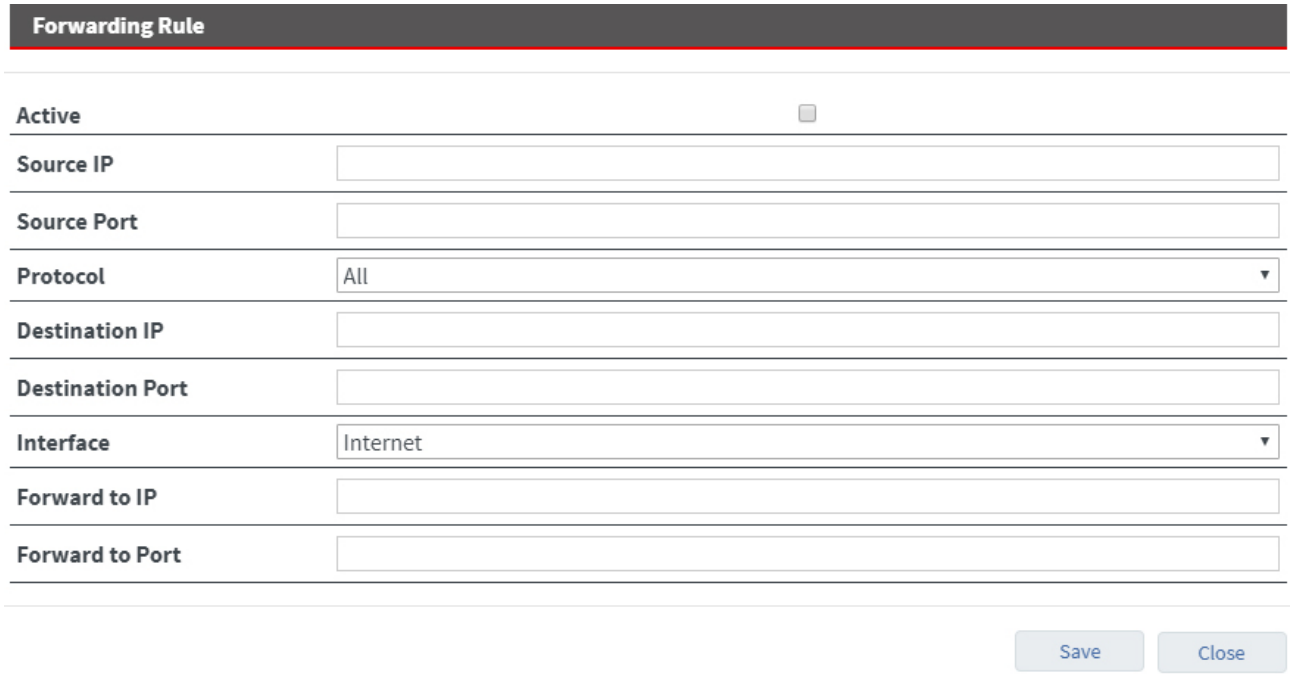
Click the Delete icon , to delete the corresponding entry.

24.4 Security Settings > Forwarding

Forwarding is used to forward requests from specific IP addresses and ports to IP addresses and ports defined in turn.



Click on the green plus  , to add a rule.



Designation	Description
Active	Check box for enabling/disabling this function.
Origin IP	Here you can enter the IP addresses from which data packets are received. If there is an entry here, only packets from these addresses are forwarded.
Origin port	Here you can specify the ports through which data packets are received. Here is an entry, then only packets specifically sent via these ports are forwarded.
Protocol	The following protocols are available: •All - the set rule applies to all protocols. •Tcp - the set rule applies only to the TCP protocol. •Udp - the set rule applies only to the UDP protocol. • **All** - the set rule applies to all protocols. • **Tcp** - the set rule applies only to the TCP protocol. • **Udp** - the set rule applies only to the UDP protocol. • **ICMP** - the set rule applies only to the ICMP protocol.
Destination IP	Enter the IP address to which data packets are to be sent initially.

Designation	Description
Destination-Port	Enter the ports through which data packets are sent to the destination IP.
Interface	You can use this selection field to determine which interface the forwarding should normally be used. The options are: • **Internet** • **WAN Ethernet** • **OpenVPN** • **IPSecVPN** • **PPTPVPN** • **LAN Ethernet** • **All** * The selection field for the interface can vary depending on the type of router.
Forward to the IP	Enter the IP addresses to which data packets should actually be forwarded.

NOTICE

If there is an active forwarding-rule, at least one IP address must always be to which the data traffic should be forwarded.

Forward to port	Enter the ports through which the data packets will be forwarded.

NOTICE

You can enter address **ranges** in the input fields for the **IP** address.
Example of address ranges: 192.168.0.100-192.168.0.110 or 192.168.0.20/30

Address listings are **not** possible!

In the input fields for the **ports**, you can enter **ranges or enumerations**.
Example of a port range: 502-504
Example of port enumeration: 502,677,555
Both, range and enumeration **can not** be used simultaneously in the same field.

NOTICE

Ranges must be separated by a **hyphen** (-) and **enumerated** by **comma** (,).

No spaces between the elements to be separated!

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

Firewall general | WAN - LAN | LAN - WAN | Forwarding | NAT

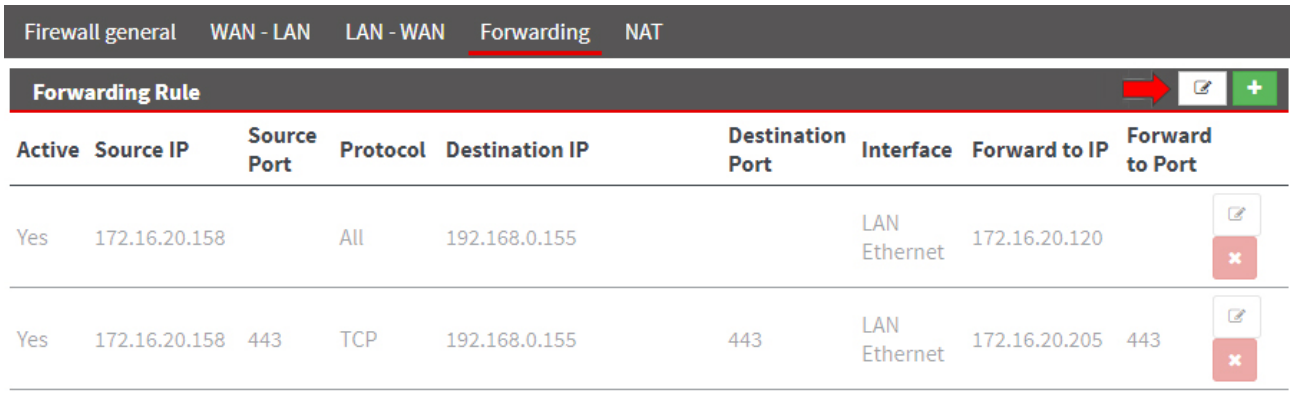
Forwarding Rule

Active	Source IP	Source Port	Protocol	Destination IP	Destination Port	Interface	Forward to IP	Forward to Port
Yes	172.16.20.158		All	192.168.0.155		LAN Ethernet	172.16.20.120	
Yes	172.16.20.158	443	TCP	192.168.0.155	443	LAN Ethernet	172.16.20.205	443
No	10.28.8.12		All	172.16.20.105,172.16.20.205		WAN Ethernet	17.25.16.158	

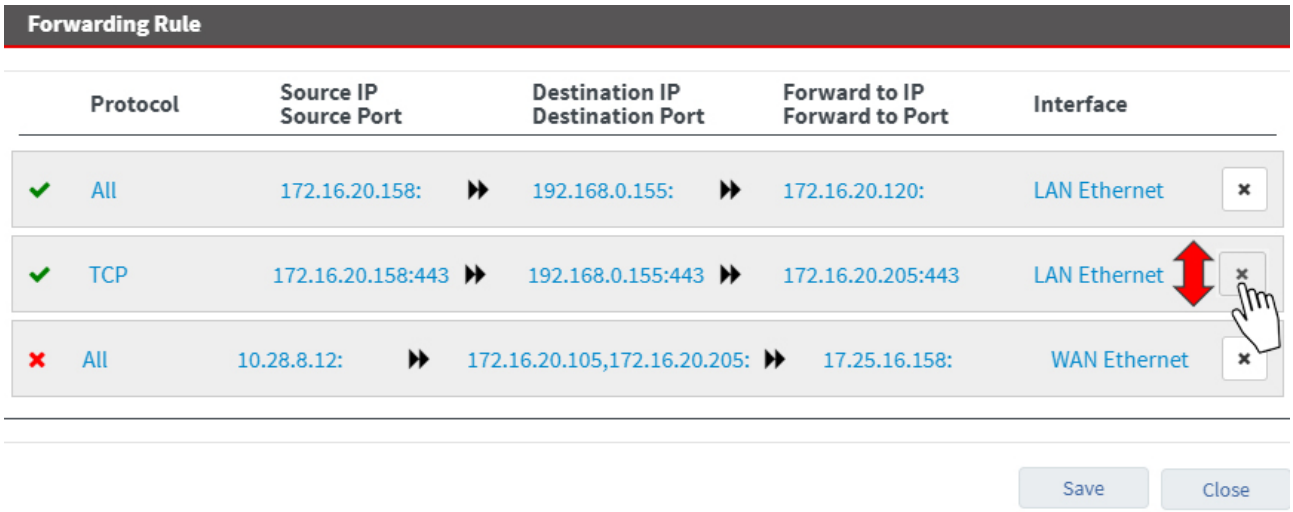
Image 19: Forwarding Entry Example

24.4.1 Edit Forwarding Rule

Change the entered rule order

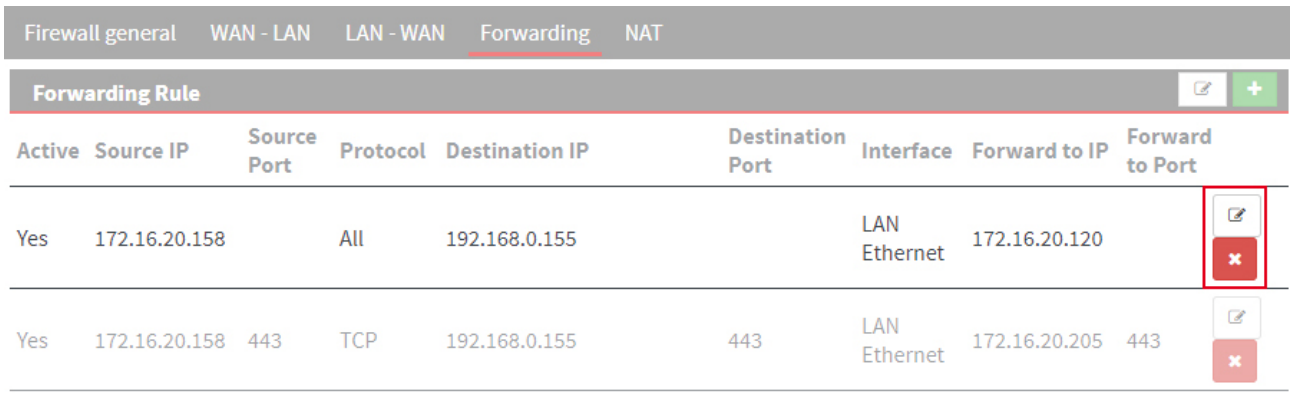


Click on the Edit icon in the header of the overview to change the sequence of the entered change rules.



Here you can move up and down (drag and drop) to change the sequence of the firewall rules.

Change/delete firewall rule



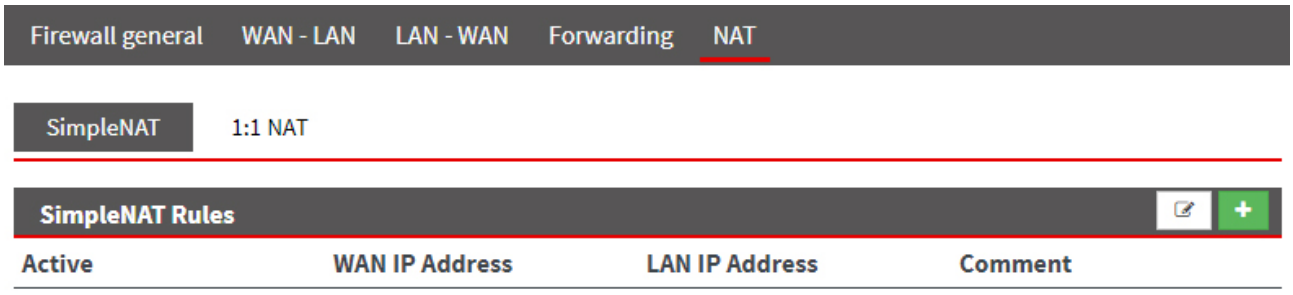
Click on the Edit icon at the end of the line of the registered rule to edit it.

Click the Delete icon , to delete the corresponding entry.

24.5 Security settings > NAT

24.5.1 SimpleNAT

"SimpleNAT" allows you to grant access to an IP address from the LAN Network 1:1 in the WAN Ethernet network. To do this, a free WAN Ethernet address from the WAN network is registered as WAN IP. This IP address is then added to the WAN interface and directly "natted" to the registered LAN IP address" mapped 1:1. i.e. the LAN IP address can be accessed directly from the IP address of the WAN. This has the advantage that no ports etc. need to "forward".



Click on the green plus , to add a rule.

Designation	Description
Active	Check box for enabling/disabling this function.
WAN IP address	Enter here a free WAN Ethernet address from the WAN network.
LAN IP address	Enter here the LAN IP address that you want to make accessible.
Comments	Here you can enter a comment for this rule.

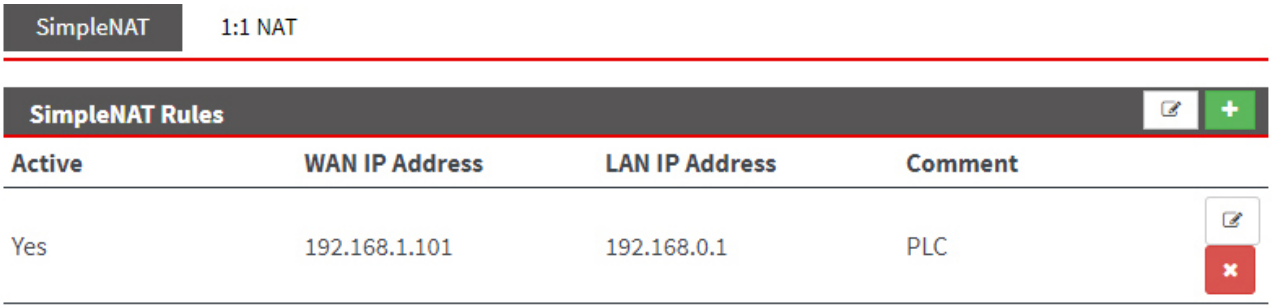
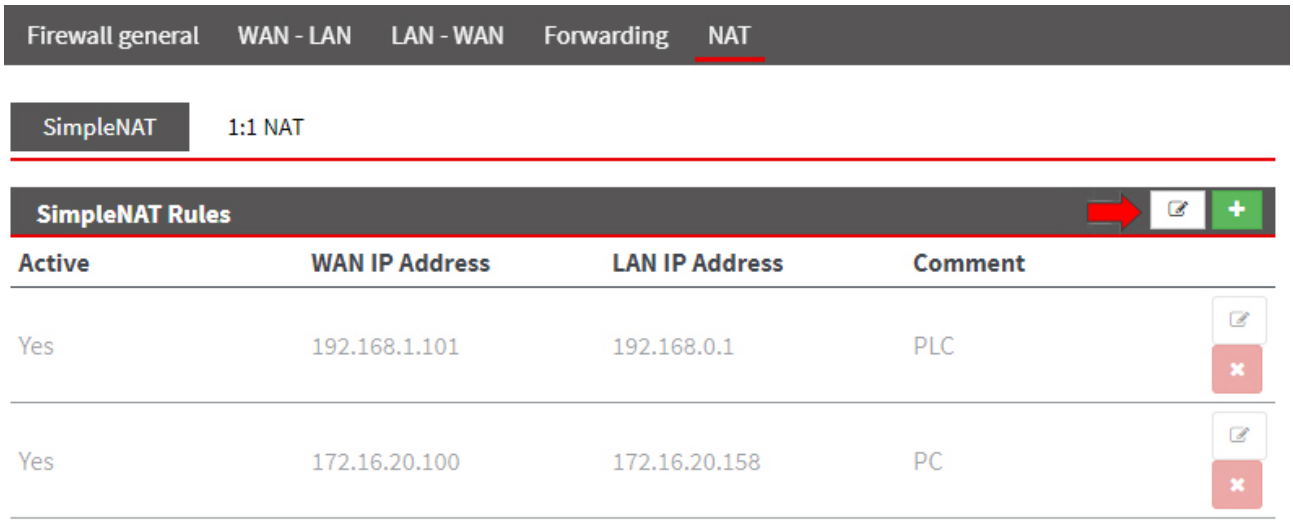


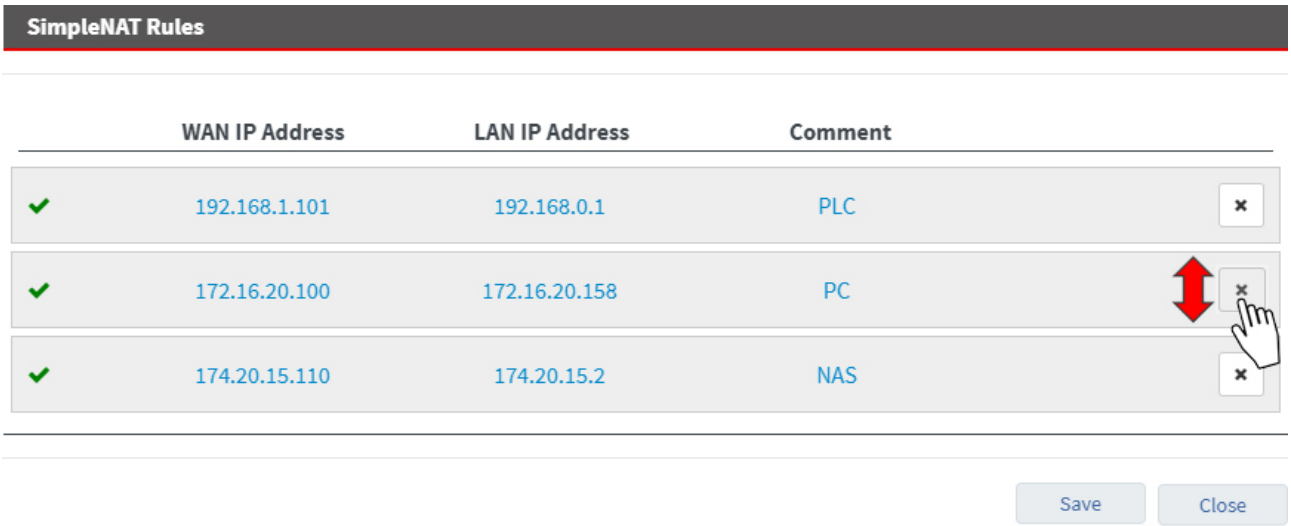
Image 20: Example entry

24.5.1.1 Edit SimpleNAT Rule

Change the entered rule order

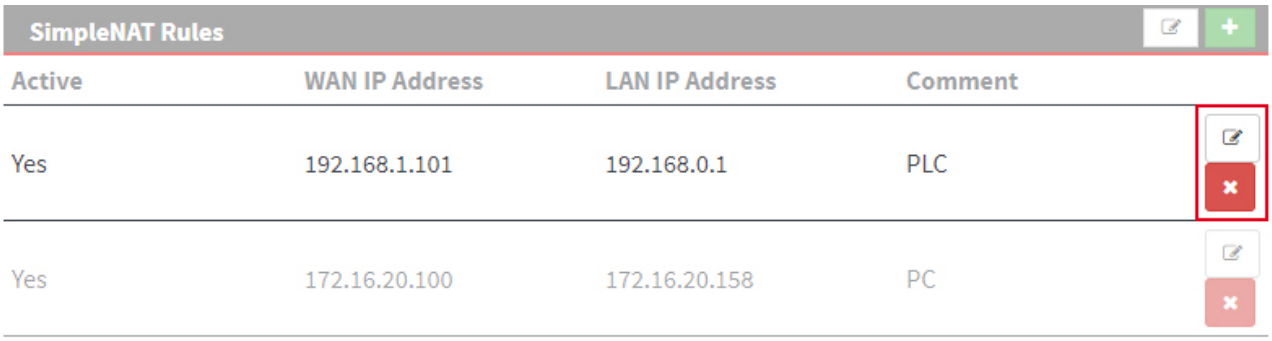


Click on the Edit icon in the header of the overview to change the sequence of the entered change rules.



Here you can move up and down (drag and drop) to change the sequence of the entered rules.

Change/delete SimpleNAT Rule



SimpleNAT Rules

Active	WAN IP Address	LAN IP Address	Comment
Yes	192.168.1.101	192.168.0.1	PLC
Yes	172.16.20.100	172.16.20.158	PC

Click on the Edit icon at the end of the line of the registered rule to edit it.

Click the Delete icon , to delete the corresponding entry.

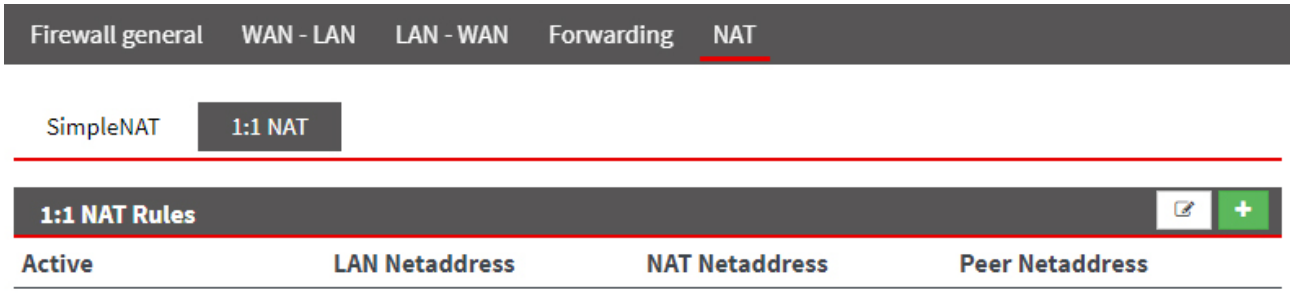
Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

24.5.2 1:1 NAT

Using "1:1 NAT" it is possible to connect two networks that are in the same address range with each other. For example, if a network with the address 192.168.0.0/24 is to be connected to a network with the same address, this is only possible if one of the two networks is assigned a different address. With the help of NAT technology this is easy to do, because only the real network address (LAN network address) and the replacement address (NAT network address) are required. The NAT algorithm then ensures that the addresses in the packets accordingly are only replaced for the communication of these two networks. So you don't have to adapt the entire own network addressing.



Click on the green plus  , to add a rule.

Designation	Description
Active	Check box for enabling/disabling this function.
LAN network address	Enter here a free LAN Ethernet address from the LAN network.
NAT network address	Enter here the LAN IP address that you want to make accessible.
Remote terminal network address	Enter the address of the network to which the translated packets are to be routed here. If the remote station also uses address translation, the NAT address of the remote station must be entered here.

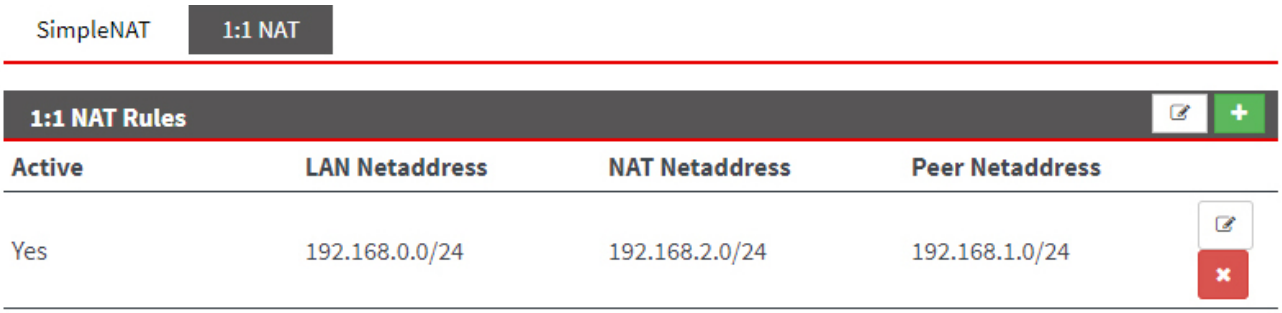
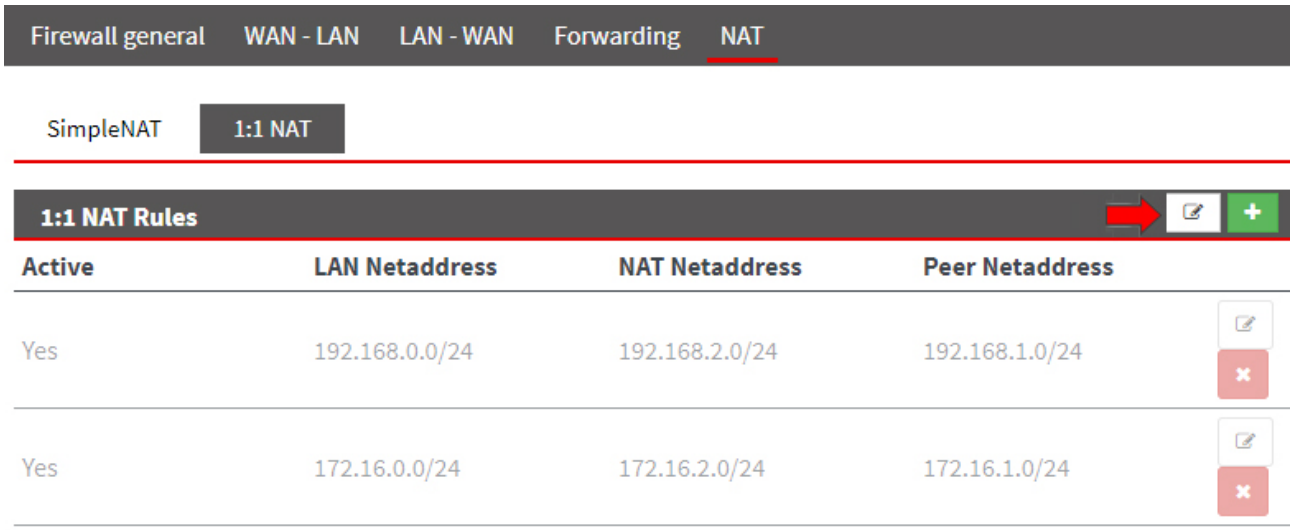


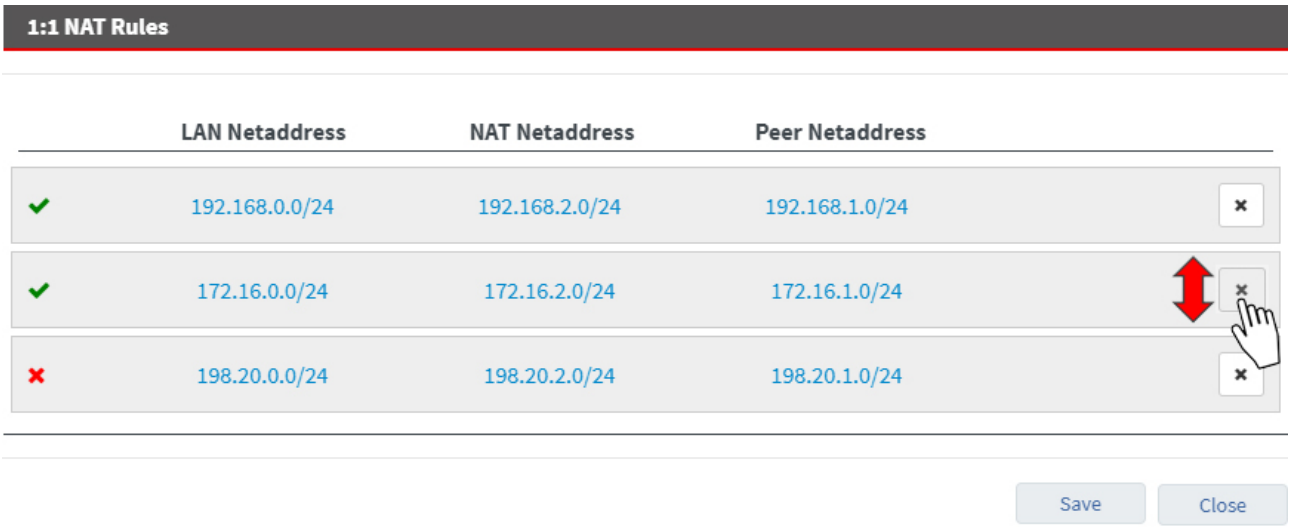
Image 21: Example entry

24.5.2.1 Edit 1:1 NAT rule

Change the entered rule order

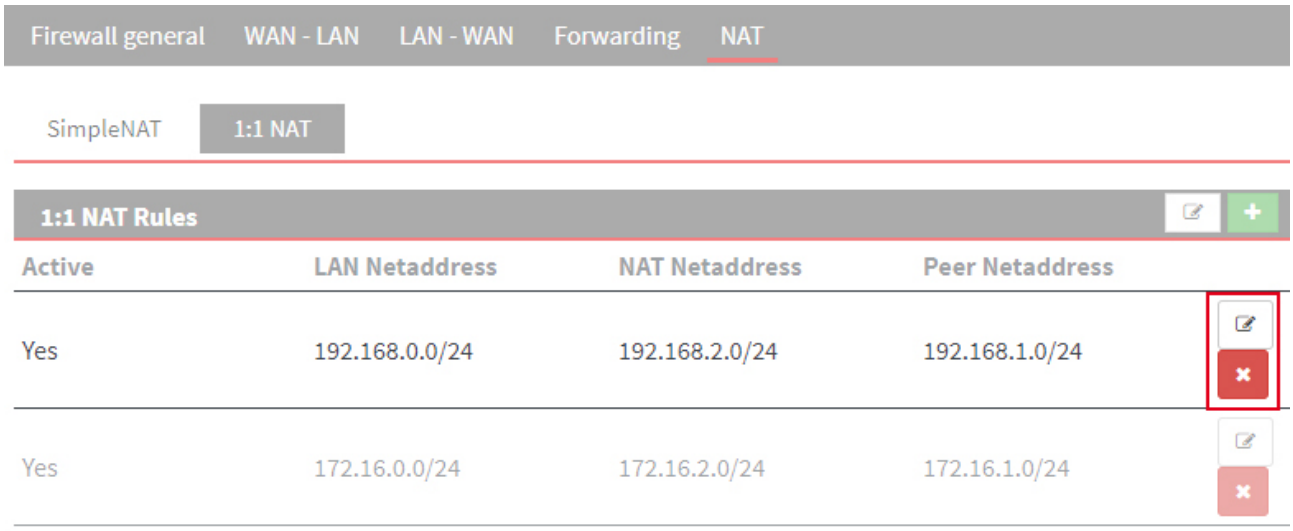


Click on the Edit icon in the header of the overview to change the sequence of the entered change rules.



Here you can move up and down (drag and drop) to change the sequence of the entered rules.

Change/delete 1:1 NAT rule



Click on the Edit icon at the end of the line of the registered rule to edit it.

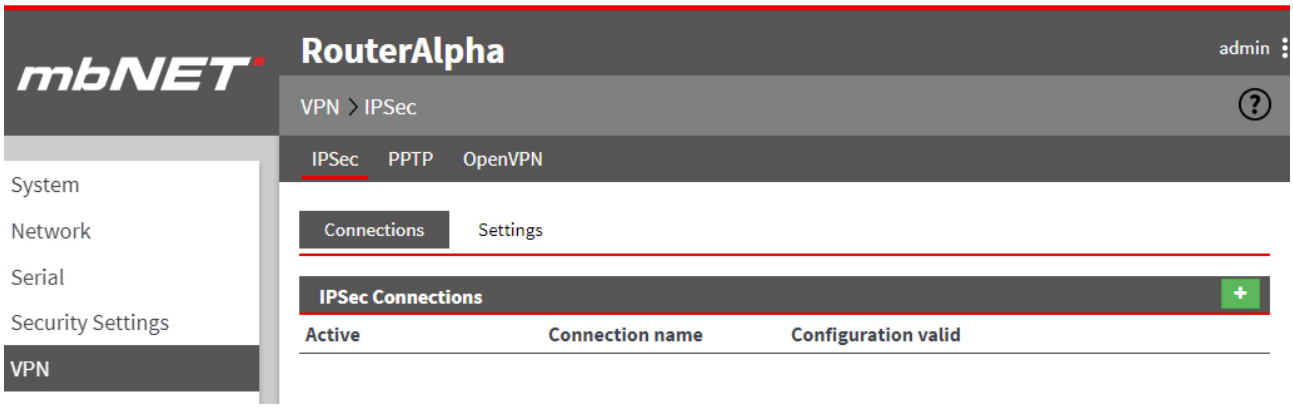
Click the Delete icon , to delete the corresponding entry.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

25 VPN



Here you can configure the communication via a VPN tunnel. You can choose from the following protocols:

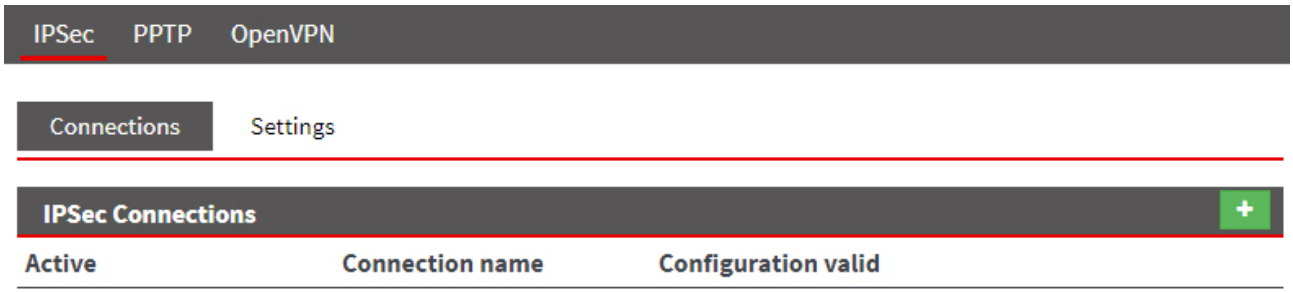
- **IPSec**
- **PPTP**
- **OpenVPN**

25.1 IPSec

NOTICE

As a rule, to enable communication via a VPN tunnel with IPSec, you need to enable the **500 UDP** and **4500 UDP**
ports for your network.

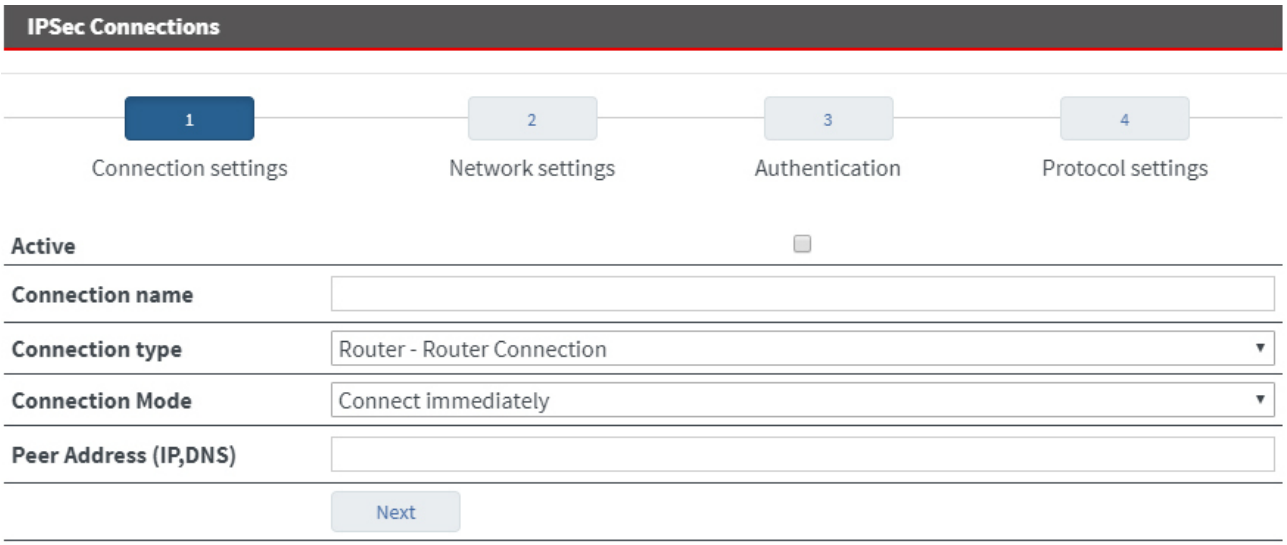
25.1.1 Configure IPSec connections



Click on the green plus  to add a connection.

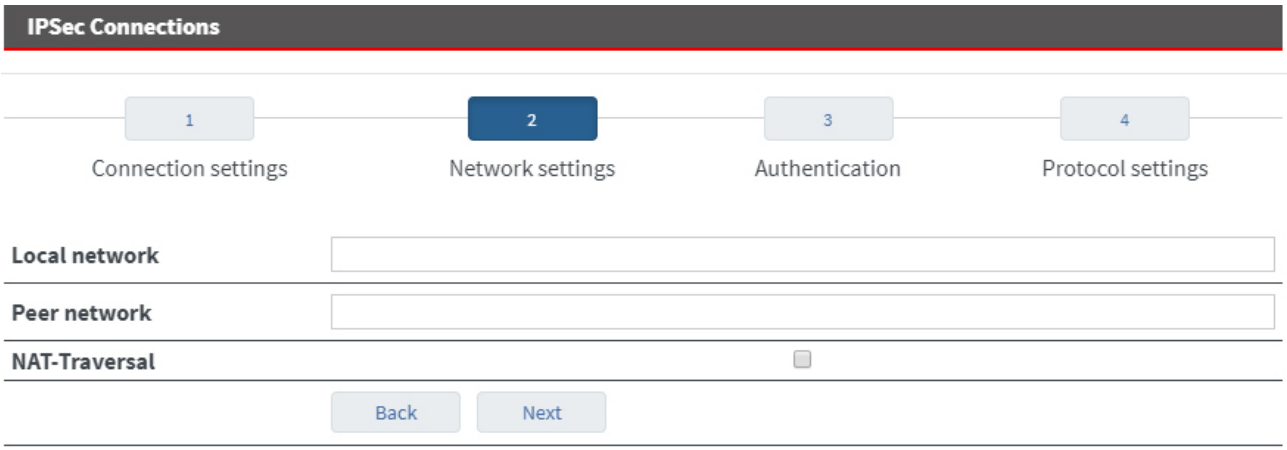
To establish a VPN connection, follow the Configuration Wizard.

1 Connection settings



Designation	Description
Active	Check box for enabling/disabling this function.
Connection Name	In the text box, enter a name for the connection.
Connection Type	Selection field for the connection type • **Router - Router connection** select this connection type to connect two complete networks together. • **Client - Router Connection,** select this connection type if you want to connect a single PC to the router (mbNET).
Connection type	In the connection type selection = **router - router connection** you can use this selection field to specify when the connection is to be established. The following options are available: - Set up connection immediately - Set up connection for data traffic - Start with an active internet connection - Wait for incoming connection - Start when input* 1 is active (1 signal) - Start when input 2 is active (1 signal) - Start when input 3 is active (1 signal) - Start when input 4 is active (1 signal) - Start when input 1 is active (1 signal), stopping at 0-Signal - Start when input 2 is active (1 signal), Stop at 0-Signal - Start when input 3 is active (1 signal), Stop at 0-Signal - Start when input 4 is active (1 signal), Stop at 0-Signal - Start when Dialout button** was pressed * refers to digital inputs I1-I4 of the mbNET. ** Dial Out button on the mbNET front panel
Partner Addresses (IP, DNS)	You must specify the appropriate partner address at the router responsible for outgoing connections. This can be an IP address or the DNS name under which the opposite router is reachable.
Next	Click the Next button to continue the configuration.

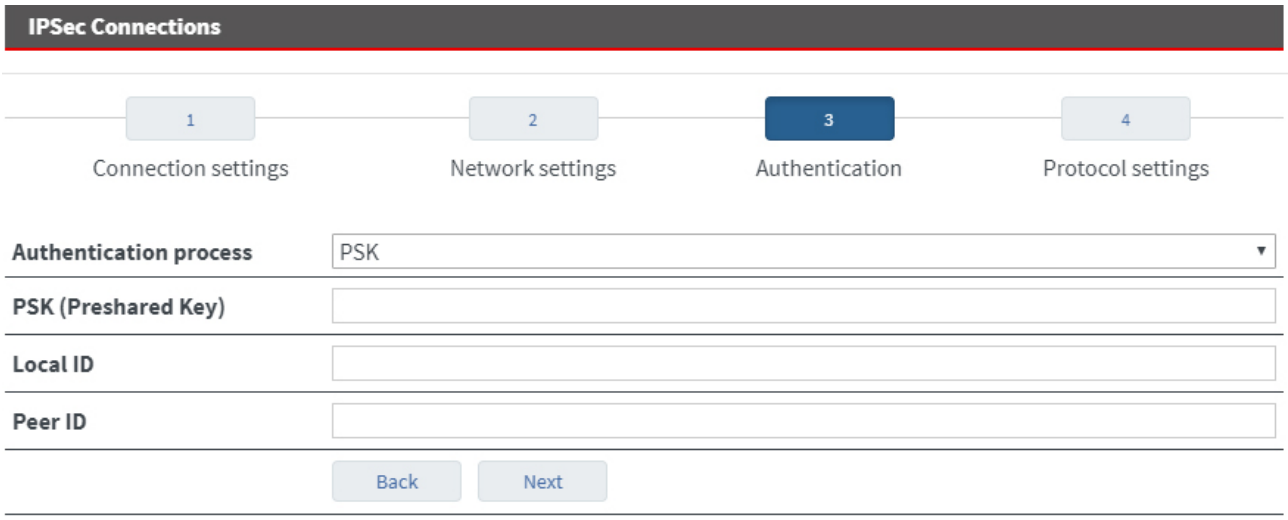
2 Network settings



Designation	Description
Local network	Enter here the address range of the local network in CIDR notation. e.g. 192.168.0.0/24
Partner Network (only for router - router connection)	Enter here the address range of the local network in CIDR notation. e.g. 192.168.10.0/24
Enable NAT transfer (only for router - router connection)	Check box for enabling/disabling this function. This setting is required if the VPN connection is established via the Internet and “natted” between the LAN and WAN (NAT: Network Address Translation). This setting is normally enabled.
Client has a fixed IP address or name (only for client router connection)	Check box for enabling/disabling this function.
Win2000/XP client (L2TP) (only for client router connection)	Check box for enabling/disabling this function. Enable this function if the client is a PC with a Windows 2000 or XP operating system
Enable NAT transfer (only for client router connection)	Check box for enabling/disabling this function.
Next	Click the Next button to continue the configuration.

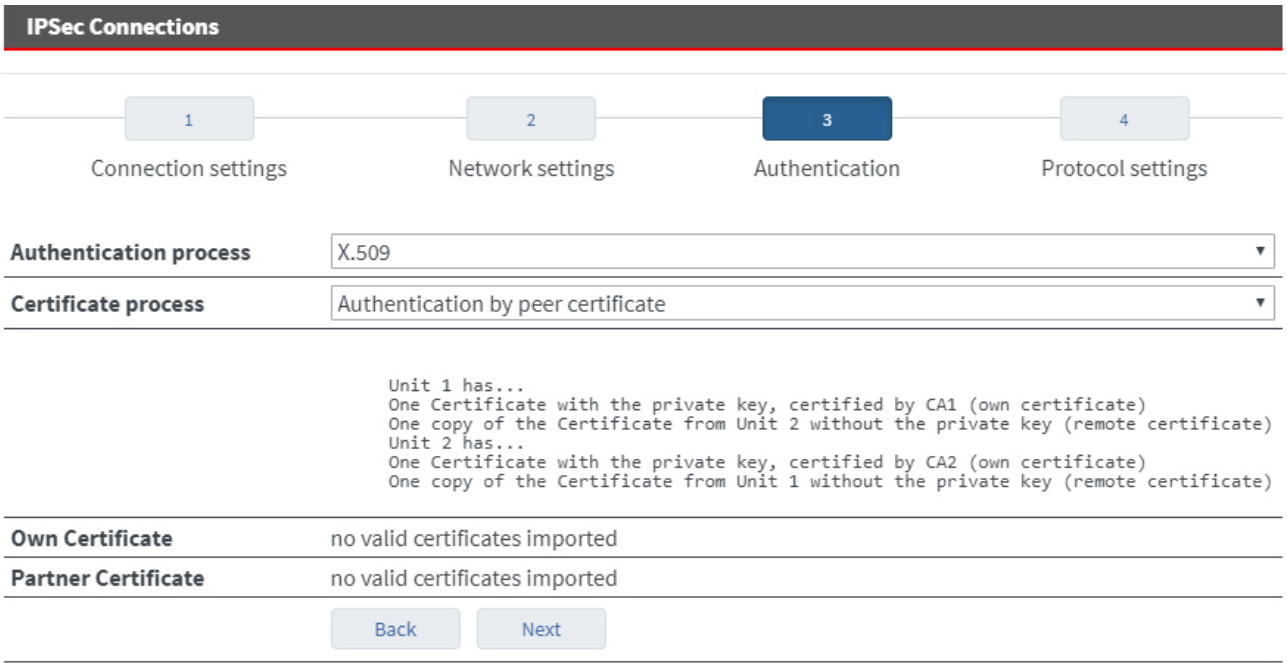
3 Authentication

(Authentication procedure = PSK)



Designation	Description
Authentication procedure	Selection field for the authentication procedure • **PSK** Both keys must be known before the exchange of data between the client and the router. The longer the key is, the more secure the connection. Only one key can be specified. Even if several PSK connections are entered, the key is valid for only the **first** connection. • X.509
PSK (Preshared Key)	Enter your pre-shared key here.
Local ID	Enter a name for your router here. This name must be communicated to the partner.
Partner ID	Enter the name of the partner here.
Next	Click the Next button to continue the configuration.

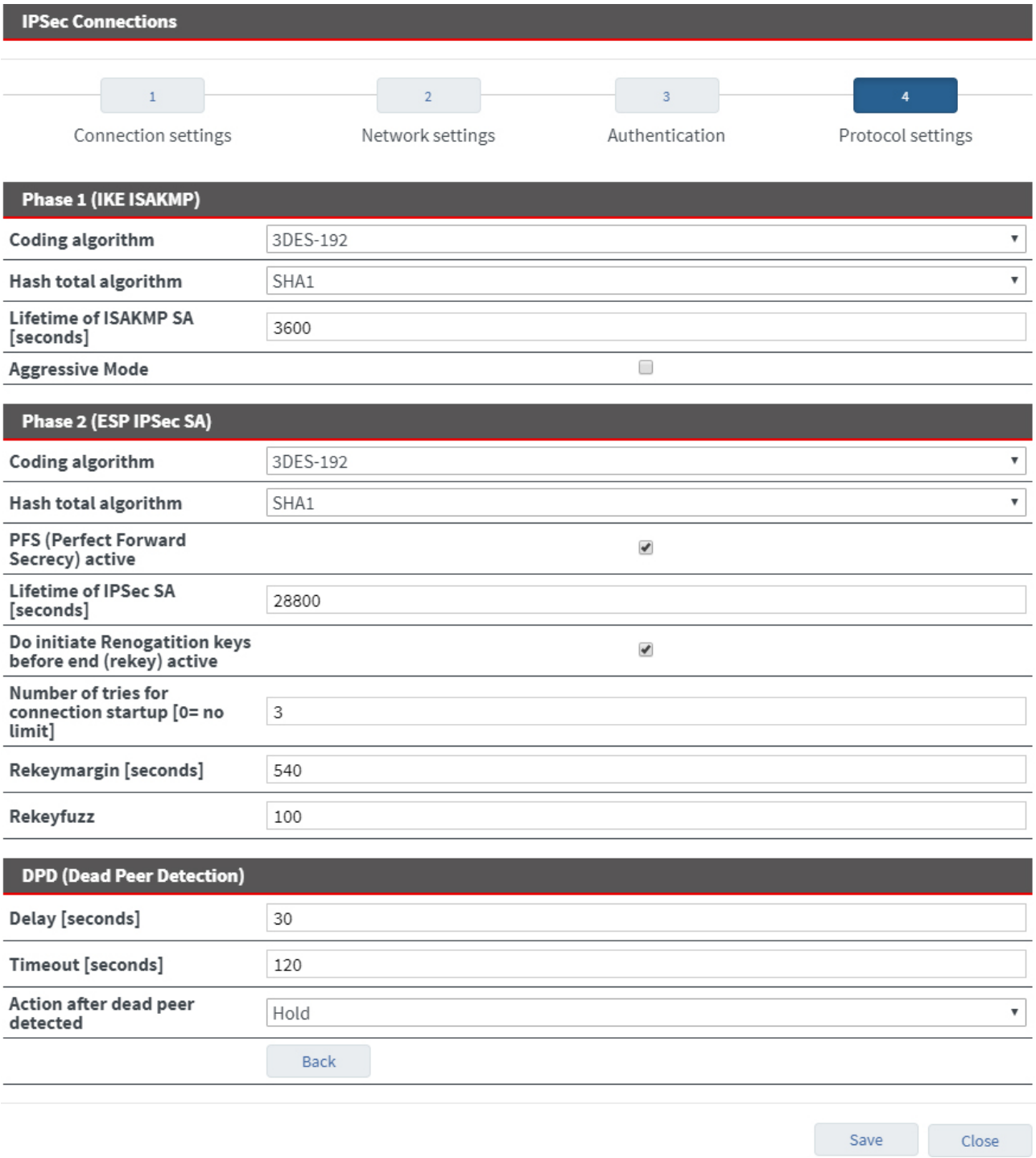
(Authentication procedure = X.509)



Designation	Description
Authentication procedure	Selection field for the authentication procedure • PSK • **X.509**
Certificate Procedure	Selection field for the certificate procedure • **Authentication by partner certificate** Here, the certificates can be signed by different CAs. A private certificate + key (.p12 file) must be imported to each router. As well as a copy of the relevant partner certificate (.crt file) - of course **without** key. • **Authentication by a certificate from the same CA** The root certificate (Signatory Authority, short CA) must be sent to the router and its own certificate including key (.p12 file) imported (*see Section: System – Certificates*). The body must have the same root certificate and a certificate signed by the CA, including key.
Own certificate	Select the own certificate via the selection area.
Partner Certificate (for Certificate procedure = authentication by partner certificate)	Here you can select the certificate of the partner.

Designation	Description
Partner ID (for Certificate procedure = authentication by a certificate from the same CA)	In the event that you establish the connection, you must specify the ID of the partner. This ID is selected when creating the certificate (*see creating certificates and revocation lists with XCA*). It is the so-called subject of the certificate and must be entered in the following manner: **/C**=*Country***/ST**=*German federal state***/L**=*city*/O=*company***/OU**=*department***/ CN**=*name_certificate***/E**=*Email address* If when creating the certificate not all fields under the subject tab are filled in, the corresponding entries should be left out (*see creating certificates and revocation lists with XCA*).
Next	Click the Next button to continue the configuration.

4 Protocol settings



Phase 1 (IKE ISAKMP) - Key Exchange	
Designation	Description
Encryption algorithm	Select one of the algorithms in order to protect the key exchange. If you change the algorithm, then you will need to adapt those on the opposite side (router-router only).
Checksum algorithm	When the algorithm is set, the calculated keys and values are checked for correctness. If you change the algorithm, then you will need to adapt it on the opposite side (router-router only).

Phase 1 (IKE ISAKMP) - Key Exchange	
Designation	Description
Service life of the ISAKMP SA [seconds]	After expiration of the set time, key Phase 1 is discarded and the tunnel must be completely rebuilt.

NOTICE

This time must be greater than the option **Rekeymargin [seconds]** in **phase 2**.

Aggressive Mode	Check box for enabling/disabling this function.

Phase 2 (ESP IPSec SA) - IPSec security negotiation	
Designation	Description
Encryption algorithm	Select one of the algorithms in order to protect the tunnel. If you change the algorithm, then you will need to adapt it on the opposite side.
Checksum algorithm	When the algorithm is set, the calculated keys and values are checked for correctness. If you change the algorithm, then you will need to adapt those on the opposite side (router-router only).
PFS (Perfect Forward Secrecy) enabled	Check box for enabling/disabling this function. In cryptography, this feature means the property of encryption methods that cannot be detected from a disclosed key on previous or subsequent keys of a communication channel. The function significantly increases the security of your tunnel, but also the quantity and generation rate of the key.

NOTICE

The setting "**Perfect Forward Secrecy (PFS) enabled**is only allowed for the router-to-router connection. If you want to set up a client-router connection, PFS must be disabled.

Lifespan of the session key [seconds]	After the expiry of that time period, a new key for the current session key is generated and the previously used key is declared invalid.
Initiate renegotiation of the key before expiry (Rekey) enabled	Check box for enabling/disabling this function. If the checkbox is enabled, a renegotiation is started after the expiry of the time period specified above. When disabled, the previous key is continued to be used.
Number of connection attempts [0=no limit]	Here you can set how many attempts the mbNET should make in order to access the remote terminal until no further attempts are made. If you enter "0" (zero), the ***mbNET*** continuously attempts to access the remote terminal.
Rekeymargin [seconds]	After the expiry of the time period, a renegotiation is initiated.
Rekeyfuzz [%]	This percentage is the maximum rate of increase for the specified intervals. By default, this value is set to 100 percent, so that the intervals can be increased up to twice.

DPD (Dead Peer Detection) - Detection for broken links	
Designation	Description
Delay [seconds]	Each time the set time period expires, a review of the connection is made. If within the time window (**timeout**) there is no positive result, the action set for "**Action after detection of the connection error**" is executed.
Timeout [seconds]	After expiration of the set time period of time in which no PING or data packet has passed through the tunnel, the selected action is executed under "**Action after detection of the connection error**".
Action after detection of the connection error	You can use this selection field to specify how you want to proceed with connection if **timeout has** been reached. In the case of the mbNET, it is recommended that you stop the connection, as the terminal could only start a new connection attempt (for instance in the event of a power failure). You can also delete this current connection immediately after detecting the connection error. In this case, only session-specific data, such as hash values or session key are discarded. The entire connection itself remains in the Manet.

Click on "Save", after completing all settings.

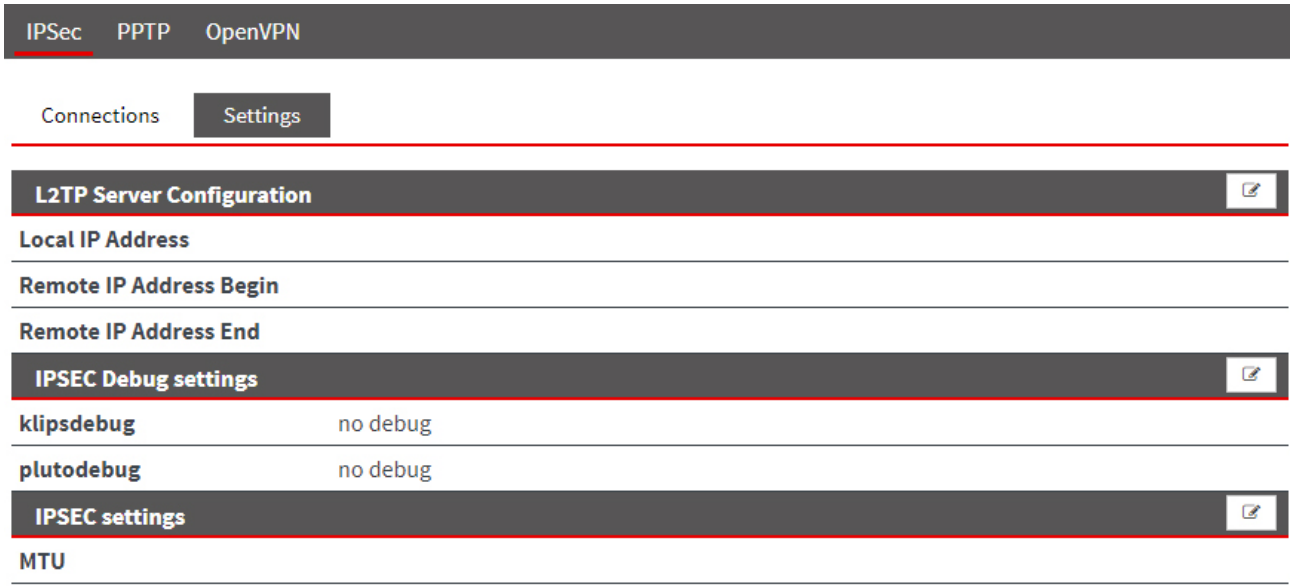
Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

Apply changes	Clicking on **"Apply changes"** will apply all stored settings/changes and store them permanently on the router.
Clear Changes	"**Discard changes**" will reset/discard all temporarily stored settings/changes.

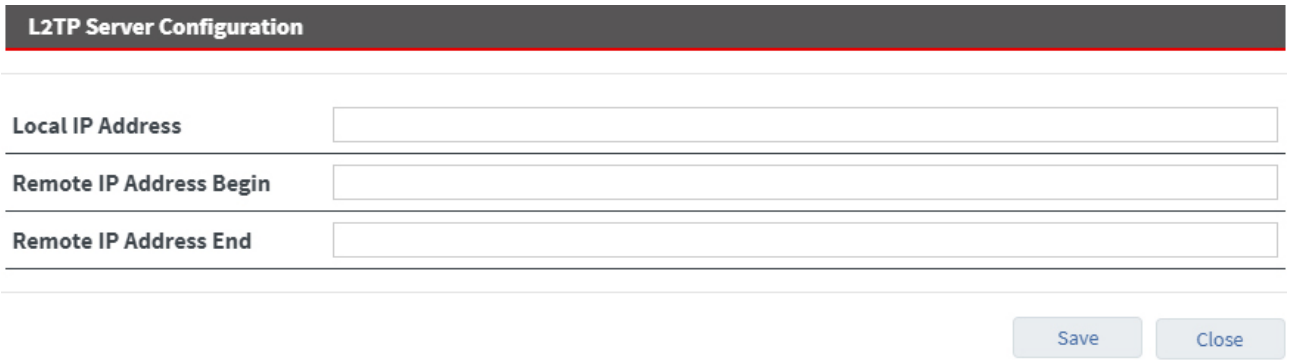
25.1.2 IPSec settings



Click the Edit icon to edit the corresponding function.

L2TP server -configuration

For VPN IPSEC communication between the ***mbNET*** and a windows client, it is possible to use the L2TP server.



Designation	Description
Local IP address	Enter the name or IP address that the server should have while communicating with the Windows Client (example: 192.168.0.103). You can also use an address from the IP range of the LAN interface. You just need to make sure that this address is not already assigned to another computer in the LAN.
Lower range for the remote IP address	Here you can find a freely selectable range of IP addresses from the network of the server. The server assigns IP addresses to the VPN clients from this area. When selecting the IP range, note that client addresses must be in the same network, such as the above selected "local IP address"
Upper range for the remote IP address	

25.2 PPTP

25.2.1 PPTP server configuration

IPSec PPTP OpenVPN

Server Clients

PPTP Server configuration	
Active	No
automatic configuration	Yes
Encryption Configuration	
Encryption	MPPEV2/all
Authentication Configuration	
Authentication via PAP	Yes
Authentication via CHAP	No
Authentication via MS-CHAP	Yes
Authentication via MS-CHAP V2	No

Click the Edit icon to edit the corresponding function.

PPTP server configuration

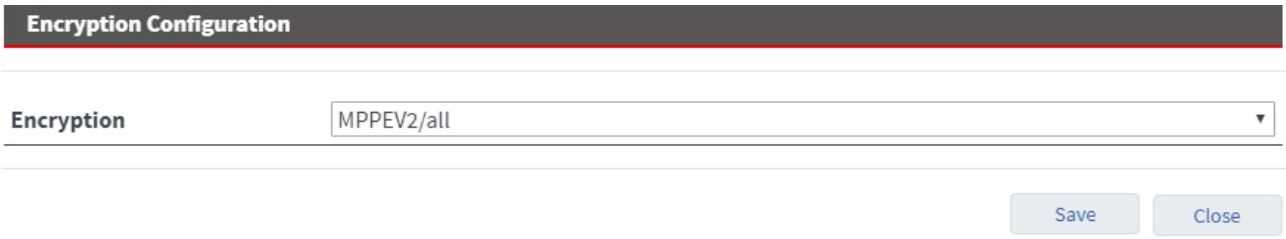
PPTP Server configuration

Active	☐
automatic configuration	No
Local IP Address or Range	192.168.0.100
remote IP Address or Range	192.168.0.101-110
Give DNS Address to the Client	
Give WINS Address to the Client	

Save Close

Designation	Description
Active	Check box for enabling/disabling this function.
automatic configuration	"Yes / No" selection field to activate/deactivate this function. If this option is set to "YES", the PPTP server is configured automatically. (Suitable addresses for the remote PCs are used in a similar way to the LAN address of the router).
local IP address or range	Enter the LAN IP of the router.
Remote IP address or range	Enter either an IP address or an address pool from the LAN IP range of the router (for example: LAN-IP = 192.168.0.100 --> entry = 192.168.0.101-110).
DNS Server IP Address to Client	Enter the IP address of the DNS server here. In the normal case, this is the same local IP address previously chosen for the router.
WINS Server IP Address to Client	Enter the IP address of the WINS server here. Leave this field empty or enter the same IP address, as in the case of "local IP address or range" and "DNS Server IP Address to client".

Encryption configuration



Designation	Description
Encryption	Selection field for the type of encryption: • None • MPPEV2/40 • MPPEV2/128 • MPPEV2/all

NOTICE

IMPORTANT: You should **always** enable encryption of your VPN connections, otherwise unauthorized access to networks, machines, etc. is possible!

Authentication configuration

You can use the following checkboxes to select the authentication protocols (PAP,CHAP,MSCHAP,MSCHAP V2).

Designation	Description
Authentication via PAP	Here the Client User Name/Password combination is sent to the host for the necessary time to accept or reject the client authentication.
Authentication using CHAP	Here, the authentication is controlled by the host. If client has dialled in, then it will be prompted for authentication by the host. The combination of user name and password is then transmitted encrypted by the client via MD5. If the user data is sent with that of the host computer, then the authentication is accepted. If not, it will be rejected. If the authentication is accepted, the user data is constantly checked periodically during the connection.
Authentication via MS-CHAP	Microsoft-developed authentication protocol.
Authentication via MS-CHAP V2	Microsoft-developed authentication protocol.

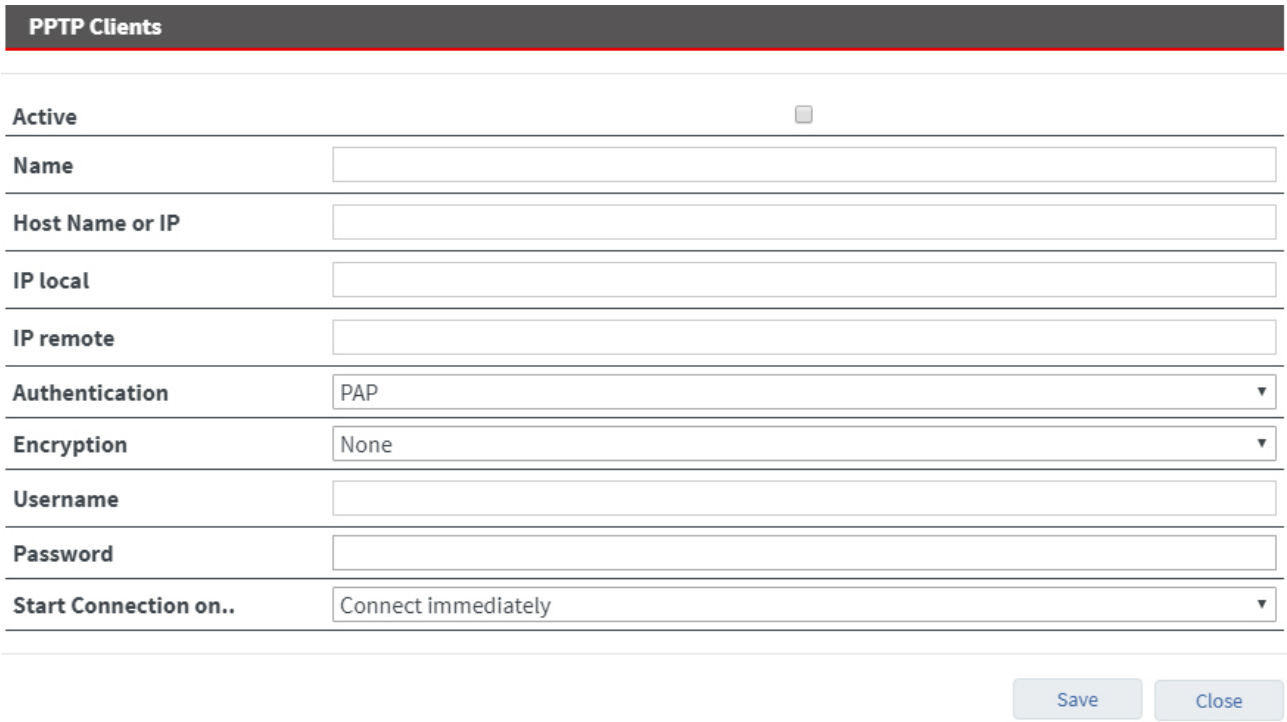
Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

25.2.2 PPTP client configuration

Click on the green plus to add a client.



Designation	Description
Active	Check box for enabling/disabling this function. Enable this feature if you want to use as the mbNET as a VPN client.
Name	Enter a name for the client here.
Host name or IP	Enter the name or IP address used by the client to access the server. Example 123456789@mbNET.mymbnet.biz or 80.187.33.55
Local IP	Option input field If no address range for remote IPs is registered on the server, you can specify a freely selectable local IP for the VPN connection.This setting option is used here for compatibility with other routers.
IP remote terminal	Enter the network address of the server in CIDR notation (example: 192.168.0.0/24) to have a route to the server network. In the case of a router to router connection the real network address of the server must be entered here. For client router connections, the field remains empty.
Authentication	
Encryption	Selection field for the type of encryption: • None • MPPEV2/40 • MPPEV2/128 • MPPEV2/all

Designation	Description

NOTICE

IMPORTANT: You should **always** enable encryption of your VPN connections, otherwise unauthorized access to networks, machines, etc. is possible!

User name	Enter a user name
Password	Enter a new password
Start connection for	selction field, when, or under what condition the connection should be started. - Set up connection immediately - Set up connection for data traffic - Start with an active internet connection - Wait for incoming connection - Start when input* 1 is active (1 signal) - Start when input 2 is active (1 signal) - Start when input 3 is active (1 signal) - Start when input 4 is active (1 signal) - Start when input 1 is active (1 signal), stopping at 0-Signal - Start when input 2 is active (1 signal), Stop at 0-Signal - Start when input 3 is active (1 signal), Stop at 0-Signal - Start when input 4 is active (1 signal), Stop at 0-Signal - Start when Dialout button** was pressed * refers to digital inputs I1-I4 of the mbNET. ** Dial Out button on the mbNET front panel

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

25.3 OpenVPN

OpenVPN Basics

- OpenVPN basically works with two tunnel IP addresses. That is, each connection has two IP addresses, over which the traffic is handled.
- Depending on the authentication method OpenVPN either works in point-to-point procedure (in the case of static key or no authentication), or server/client mode (in the case of X.509 certificates).
- OpenVPN can have three different authentication methods:

- **none:** No certificate or key is necessary. This method is mainly used to test the connection. The tunnel data will **NOT** be encrypted.
- **static key:** A 1024 bit key that each partner needs is generated for the connection. Similar to the password.
- **X.509 certificates:** For certificates, a distinction is made between the following variants:

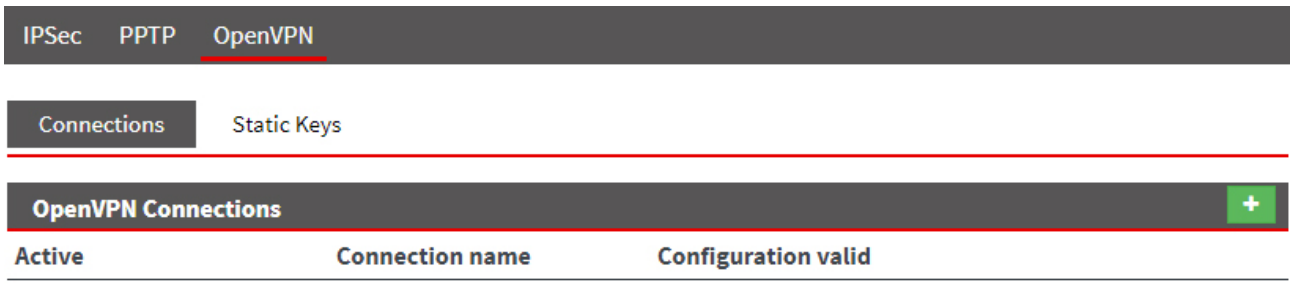
  a) Each participant needs the same RootCA and an own certificate signed by RootCA.

  b) As a) but with additional user and password prompt.

  c) As b) but without own certificate. This means that the participants need only a RootCA and user/ password.

- OpenVPN can use an http proxy server as an outgoing connection.
  - Important for the integration into existing company networks with internet access -
- The setting of the transmission protocol (UDP or TCP) is freely adjustable with OpenVPN. As well as the port numbers to be used.

25.3.1 Configure OpenVPN connections



Click on the green plus  to add a connection.

To establish a VPN connection, follow the Configuration Wizard.

25.3.1.1 Connection type: Client router connection

Select the connection type if you want to connect one single PC to the router (mbNET).

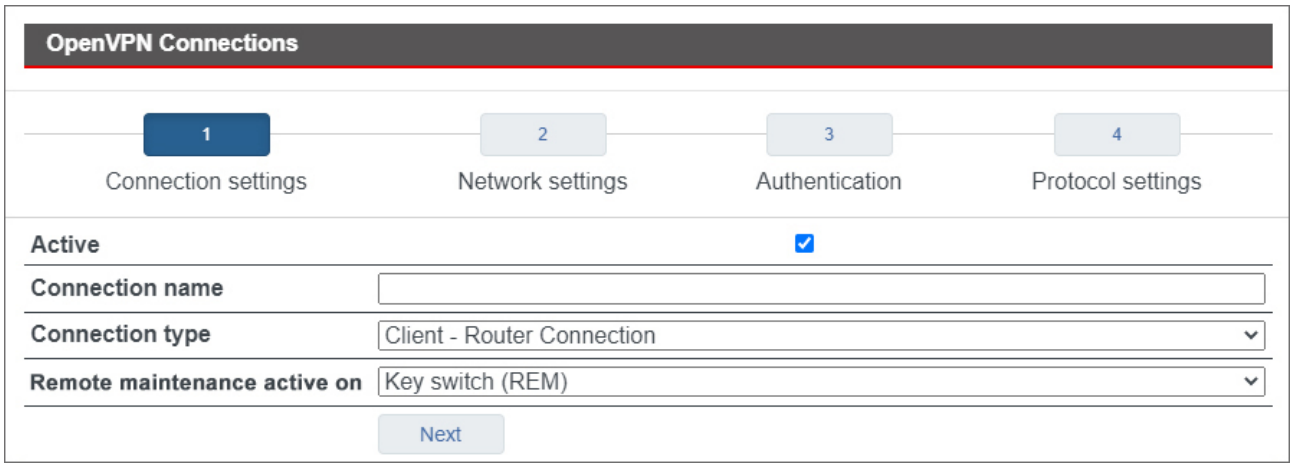
NOTICE

Only **one** "client to network" connection can be created. Depending on the authentication method, the client obtains an IP from a specified range or each participant gives its required address.

Example:

Client PC	mbNET
[10.1.0.6]VPN – TUNNEL	[10.1.0.5] <> ROUTING <> LAN [192.168.0.100]

1 Connection settings



Designation	Description
Active	Check box for enabling/disabling this function.
Connection Name	In the text box, enter a name for the connection.
Connection Type	Selection field for the connection type • **Router - Router connection** select this connection type to connect two complete networks together. • **Client - Router connection,** select this connection type if you want to connect a single PC to the router (mbNET).
Remote maintenance active on	Only the "**Key switch (REM)**" option is available here.

NOTICE

An active connection to systems can only be established in the key switch position **REM**.
The **Key switch (REM)** function is part of the 2-stage security concept.
A description of the **2-level security** can be found after this table.

Next	Click the Next button to continue the configuration.

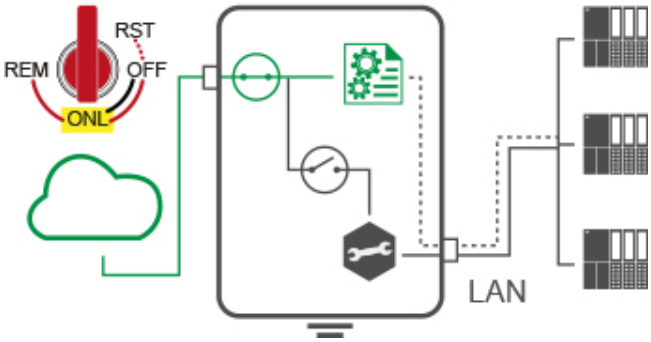
2-Level Security

You use the control mechanism of the 2-level access control to control or regulate remote access to a device and the components connected to it.

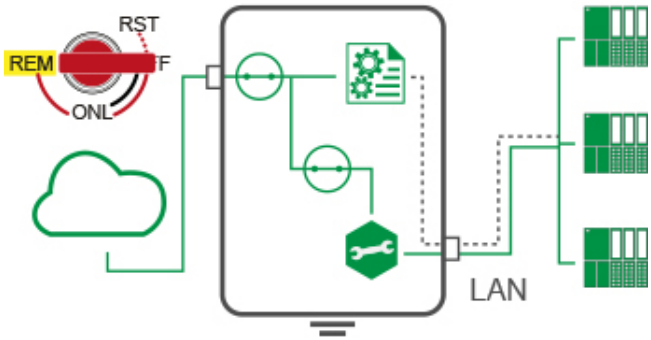
NOTICE

To prevent remote access locally is a recommendation from cybersecurity authorities such as the German BSI, the French ANSSI or the European ENISA.
The 2-level access control corresponds to the recommendations for secure remote access.

1st Level:
In the switch position "**ONL**" the mbNET (router) connects to the Internet.
The remote maintainer now has access to the router's internal services (web server, data monitoring, etc.). The remote maintenance provider **cannot** route into the LAN segment.

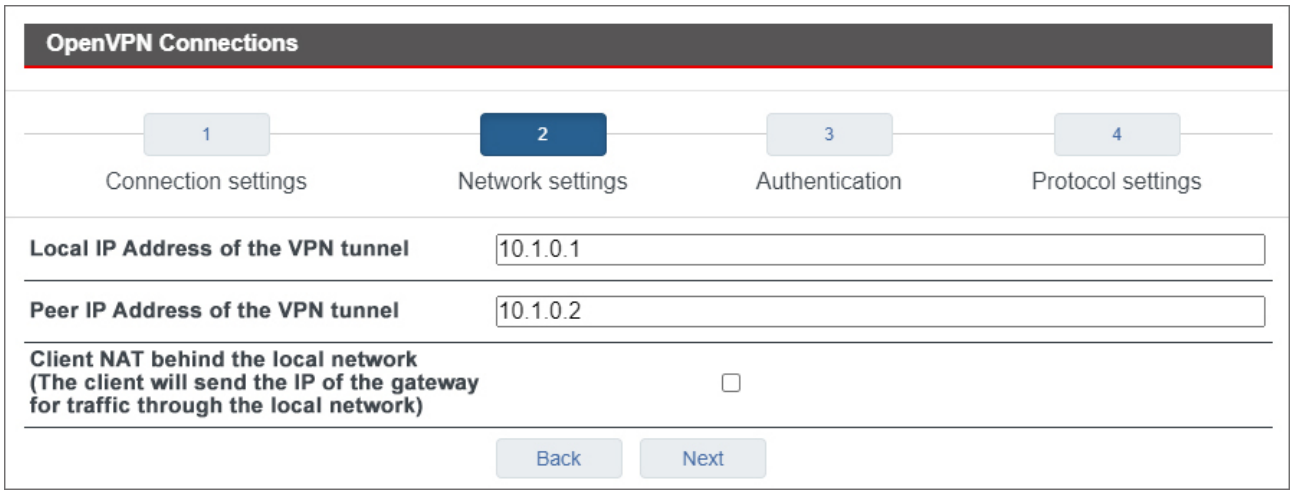


2nd Level: In the "**REM**" switch position, the routing between the remote maintenance and the LAN segment is enabled. All participants in the LAN segment can now be reached transparently. By resetting to "**ONL**", the operator can interrupt remote maintenance on site at any time.



In the "**OFF**" position, the connection to the Internet is completely disconnected. The router is offline.

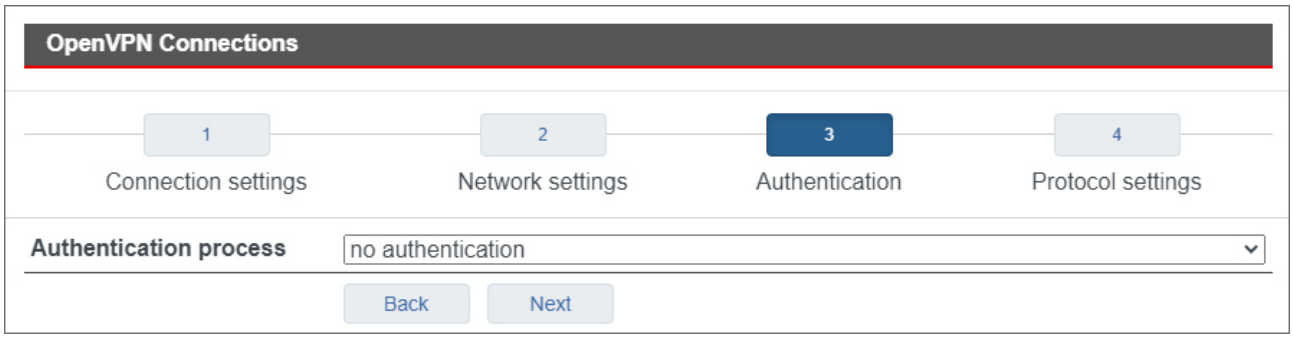
2 Network settings



Designation	Description
Local IP Address of the VPN tunnel	Enter the IP address of the local VPN tunnel endpoint. e.g. 10.1.0.5
Partner IP address of the VPN tunnel	Enter the IP address of the partner VPN tunnel endpoint. e.g. 10.1.0.6
Replace the sender IP address of the client by the LAN IP address (SNAT)	Check box for enabling/disabling this function. All packages in the LAN network receive the sender IP of the mbNET. You can then actually no longer distinguish in the LAN which sender it is now, but participants in the LAN must then also NOT have entered the mbNET as a gateway.
Next	Click the Next button to continue the configuration.

3 Authentication

(Authentication method = no authentication)

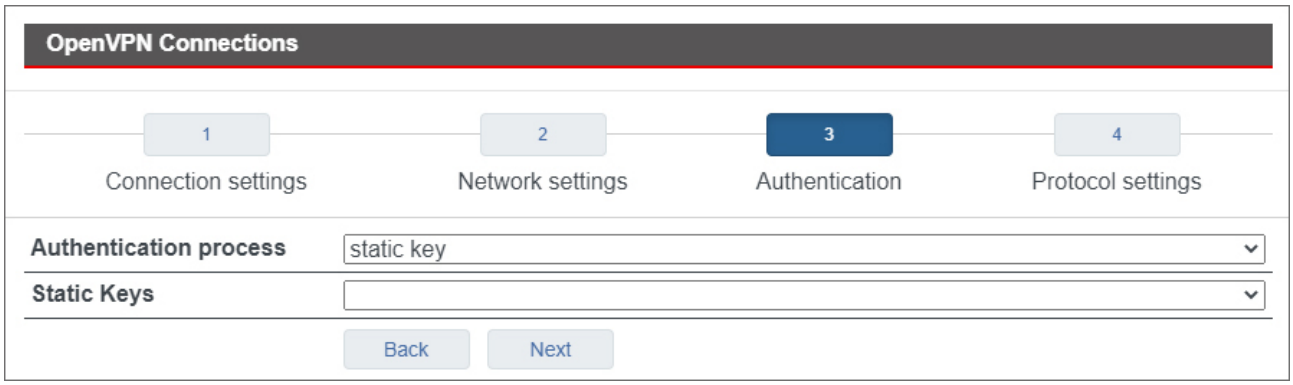


NOTICE

Select this method only to test the connection, as **all the data is transmitted in clear text**!
Always enable encryption of your VPN connections, otherwise unauthorized access to networks, machines, etc. is possible!

Designation	Description
Authentication procedure	Selection field for the authentication procedure • **No Authentication** this type should only be selected to test the connection, as **all the data is transmitted in clear text**! **Always** enable encryption of your VPN connections, otherwise unauthorized access to networks, machines, etc. is possible! • Static key • X.509
Next	Click the Next button to continue the configuration.

(Authentication procedure = static key)

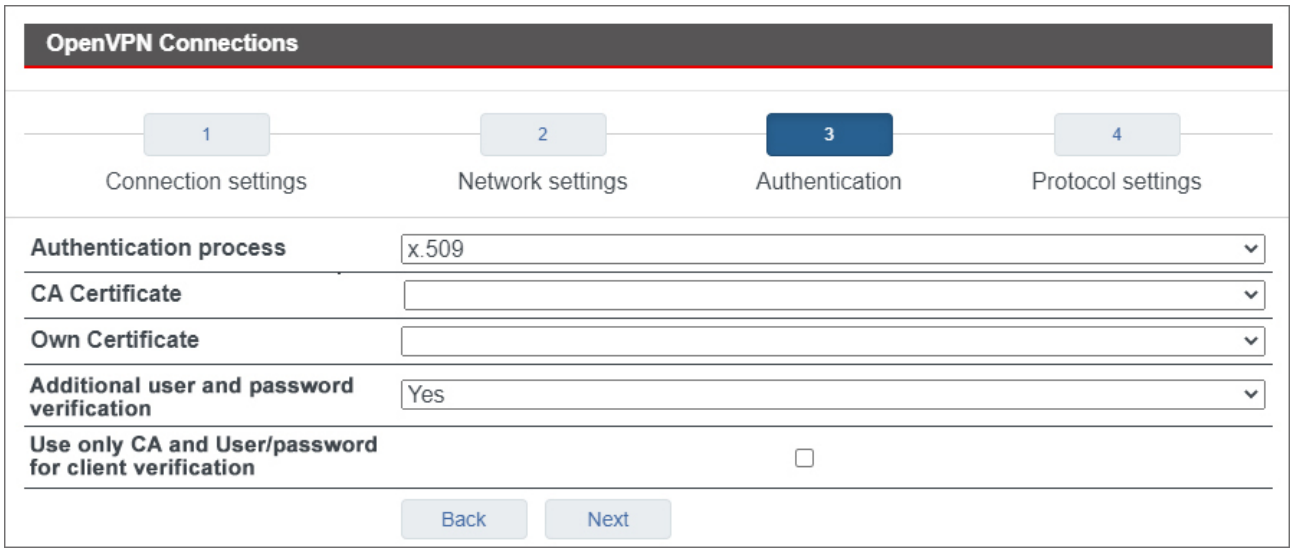


NOTICE

For symmetric encryption with a static key, you first need to generate a key (VPN OpenVPN static key) or import a previously created one. Note, however, that each participant needs to receive the key in a secure manner.

Designation	Description
Authentication procedure	Selection field for the authentication procedure • no authentication • **Static key** For a symmetrical encryption with a static key, you must first generate a key (VPN OpenVPN static key) or import a previously created one. Note, however, that each participant needs to receive the key in a secure manner. • X.509
Static Key	Selection field with all imported keys to date.
Next	Click the Next button to continue the configuration.

(Authentication procedure = X.509)



NOTICE

For this authentication method, you must first create/import your certificates (see: System > Certificates)

Designation	Description
Authentication process	Selection field for the authentication process • no authentication • Static key • **X.509**
CA certificate	Selection field with all certificates imported to date. This shows the selected root cell certificate. If you have not yet imported a certificate, import your root cell certificates or create one of your own (see Section: System > Certificates).
Own certificate	Selection field with all certificates created to date. This displays your own certificate. If you have not yet imported a certificate, import your certificate now or create one of your own.
Additional user and password verification	"Yes / No" selection field to activate/deactivate this function. If you select "Yes", user data is requested from the client. These credentials must match an entry from "System users" from the OpenVPN server.
Use only CA and User/password for client verification	Check box for enabling/disabling this function. In this case only the CA certificate and the user login are used for authentication.

NOTICE

Note that you still need to have your own certificate and it must be selected!

Next	Click the Next button to continue the configuration.

4 Protocol settings

OpenVPN Connections

1 Connection settings | 2 Network settings | 3 Authentication | 4 Protocol settings

Networkadapter	
Adaptertype	TUN
Protocol	
Coding algorithm	Blowfish wtih CBC (128 bit)
Protocol	UDP
Local VPN port	1194
Peer VPN port	1194
Miscellaneous	
Bind the local IP-address and port	☑
Allow the peer to change the IP-address dynamically	☐
LZO compress active	☑
Ping interval [s]	10
Ping restart [s]	60
MTU [bytes]	1500
Fragment the UDP packets in... [bytes]	
Regenerate a new key after... [s]	3600
Send more Information to the System Protocol	☐
Miscellaneous	
Enable connection through a HTTP proxy	☐
HTTP proxy name	
HTTP proxy port	
HTTP proxy username	
HTTP proxy password	

Back

Save Close

Networkadapter	
Designation	Description
Adaptertype	Selection field for the virtual kernel driver: - TUN - TAP

Protocol	
Designation	Description
Coding algorithm	Selection field for the method used by the mbNET to encrypt OpenVPN data: - Blowfish with CBC (128 bit) - DES with CBC (64 bit) - RC2 with CBC (128 bit) - DES-EDE with CBC (128 bit) - DES-EDE3 with CBC (192 bit) - DESX with CBC (192 bit) - Blowfish with CBC (128 bit) - RC2 with CBC (40 bit) - CAST5/128 with CBC (128 bit) - RC2 with CBC (64 bit) - AES with CBC (128 bit) - AES with CBC (192 bit) - AES with CBC (256 bit)

NOTICE

Note that each of the communication partners must use the same method.

Protocol	Selection field for the transfer protocol: - UDP - TCP
Local VPN port	Select the port for the OpenVPN connection (example: Port 80 TCP or 1194 UDP). However, you can also freely select the port numbers, if they are not already in use by another program. It is also possible for the server and client to use different ports (Server: 1194 UDP -- Client: 20500 UDP). Note that both know the port of other and these are also set!
Peer VPN port	

Miscellaneous	
Designation	Description
Bind the local IP-address and port	Check box for enabling/disabling this function. This corresponds to the "bind" setting of OpenVPN. OpenVPN cannot dynamically change the ports during the connection.
Allow the peer to change the IP-address dynamically	Check box for enabling/disabling this function. This corresponds to the OpenVPN setting "float" and allows the partner to change the address.
LZO compress active	Check box for enabling/disabling this function. This corresponds to the OpenVPN "comp"-lzo setting.

Miscellaneous	
Designation	Description
Ping interval [s]	Input field for a time period [in seconds] If the VPN tunnel is not used by the end of the period, a ping is sent to the VPN partner. This corresponds to the OpenVPN "ping” setting.
Ping restart [s]	Input field for the time period [in seconds] if a ping or a data packet is not received from the VPN partner within the time period, the OpenVPN tunnel is restarted. This corresponds to the OpenVPN setting "ping-restart".Maximum
MTU [bytes]	Maximum Transver Size This corresponds to the setting "tun-mtu". The default size is 1500 bytes.
Fragment the UDP packets in... [bytes]	All UDP packets that are larger than ... [bytes] are divided into several packages (fragment). This corresponds to the setting "fragment". The default setting is that the packages are not split (" ").
Regenerate a new key after... [s]	Renew the security key after ... [seconds] (reneg-sec) This corresponds to the OpenVPN setting "reneg-sec". By default, this time is set to 3600 seconds.
Send more Information to the System Protocol	Check box for enabling/disabling this function. This corresponds to the setting "verb 3" of OpenVPN. This feature is disabled by default.

Miscellaneous	
Designation	Description
Enable connection through a HTTP proxy	Check box for enabling/disabling this function. If this function is activated, the outgoing connection attempts to pass through a proxy server. The following fields must be completed for this purpose.
HTTP proxy name	Input field for the DNS names or the IP address of your proxy server.
HTTP proxy port	Input field for the port number on which your proxy server receives requests. A common port number, for example, would be 8080 (in the case of Linux Proxy "Squid", it would be 3128 by default).
HTTP proxy username	If the proxy server requires authentication, enter the user data for the proxy. If you do not know this data, ask your network administrator.
HTTP proxy password	

Click on "Save", after completing all settings.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

Apply changes	Clicking on **"Apply changes"** will apply all stored settings/changes and store them permanently on the router.
Clear Changes	"**Discard changes**" will reset/discard all temporarily stored settings/changes.

25.3.1.2 Connection type: Router-router connection - server mode

Select this connection type to connect two complete networks together.

Here you can create a "network to network" connection. Depending on the authentication method, the dialing party receives an IP from a defined area or each participant specifies his required address.

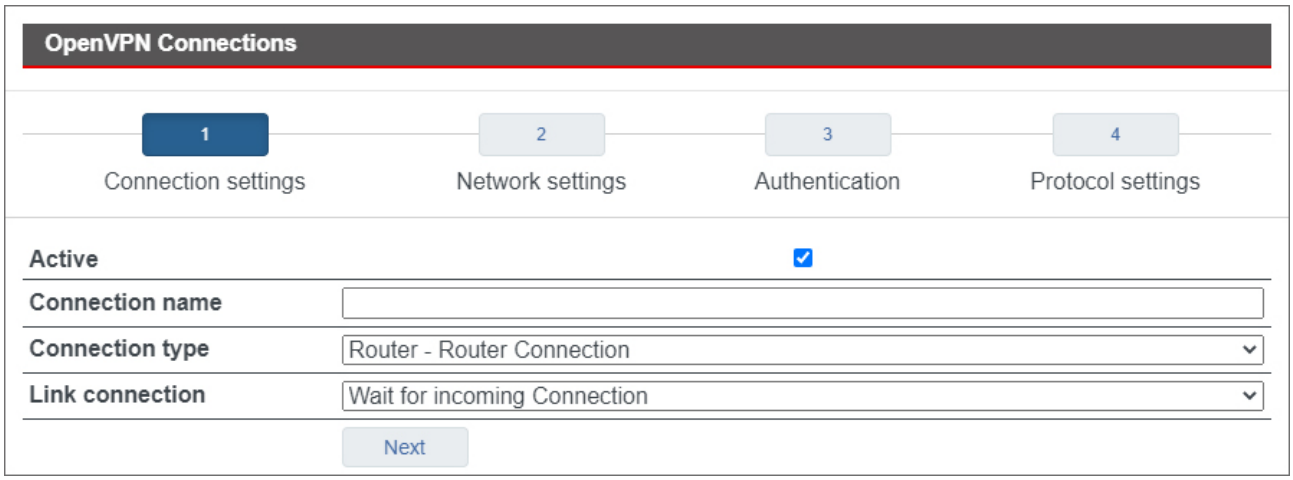
Example:

LAN	mbNET Client		mbNET Server	LAN
[192.168.9.100] <>ROUTING<>	[10.1.0.2]	**VPN-TUNNEL**	[10.1.0.1] <>ROUTING<>	[192.168.0.100]

Server mode

To establish the connection, select = "Wait for incoming connection" from the selection list. The mbNET is therefore in "server mode" and will be referred to as "server" in the further documentation.

1 Connection settings



Designation	Description
Active	Check box for enabling/disabling this function.
Connection name	In the text box, enter a name for the connection.
Connection type	Selection field for the connection type • **Router - Router connection** • Client router connection
Link connection	Selection field for when or under which conditions the connection should be started. Choose here: **Wait for incoming connection**

NOTICE

If "Wait for incoming connection" was selected to establish the connection, this mbNET is in server mode and is referred to as "server" in the further documentation.

The mbNET is in the "wait mode" when "Waiting for incoming connection" is selected.

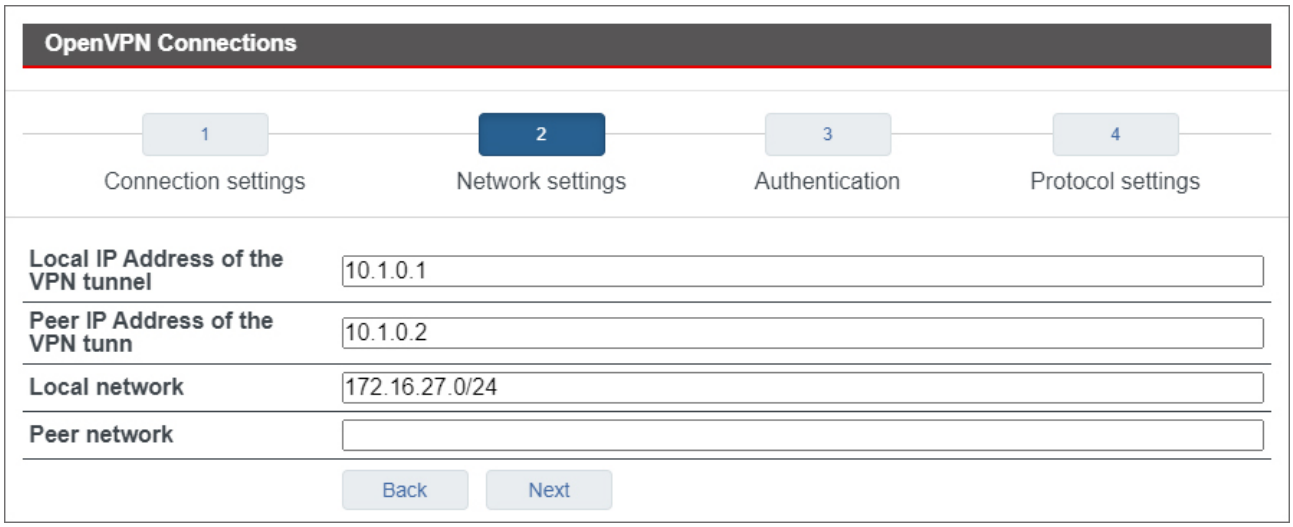
With all other options, this mbNET is in "client mode" and is referred to as "client". In this case, the mbNET on the other side is in "waiting position".

NOTICE

One of the routers must be in "wait mode"!

Next	Click the Next button to continue the configuration.

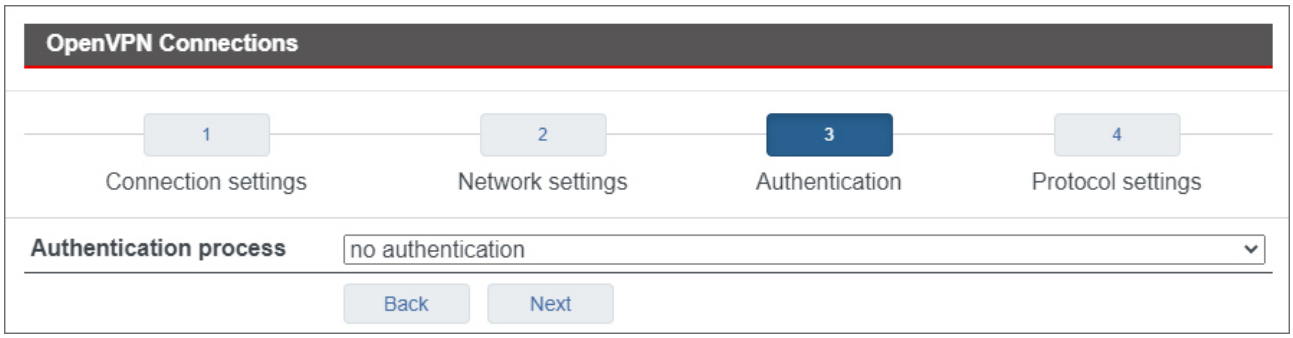
2 Network settings



Designation	Description
Local IP Address of the VPN tunnel	Enter the IP address of the local VPN tunnel endpoint. e.g. 10.1.0.5
Peer IP Address of the VPN tunnel	Enter the IP address of the partner VPN tunnel endpoint. e.g. 10.1.0.6
Local network	Enter your own network address in CIDR notation (as standard for the router: 192.168.0.0/24)
Peer network	Enter the network address of the subscriber (client) in CIDR notation (192.168.5.0/24).
Next	Click the Next button to continue the configuration.

3 Authentication

(Authentication method = no authentication)

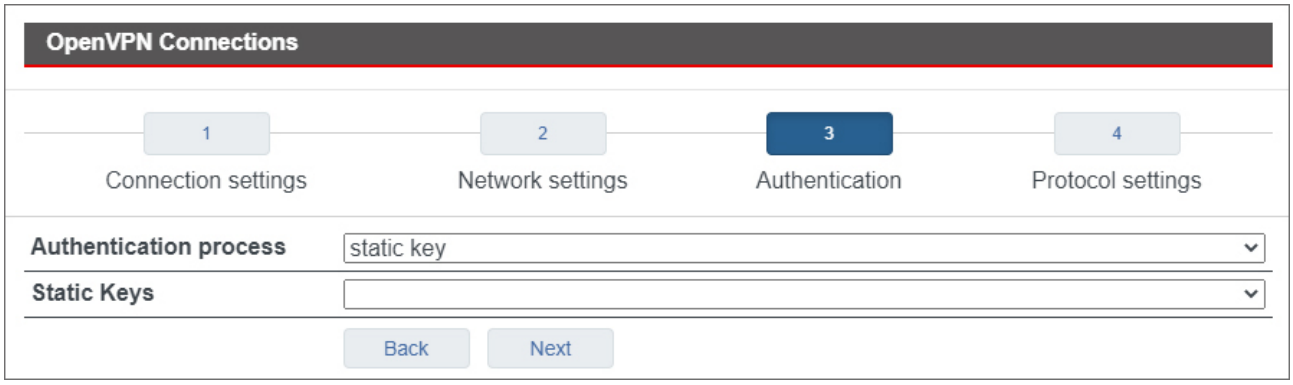


NOTICE

This type should only be selected to test the connection, as **all the data is transmitted in clear text**! **Always** enable encryption of your VPN connections, otherwise unauthorized access to networks, machines, etc. is possible!

Designation	Description
Authentication procedure	Selection field for the authentication procedure • **No Authentication** • Static key • X.509
Next	Click the Next button to continue the configuration.

(Authentication procedure = static key)



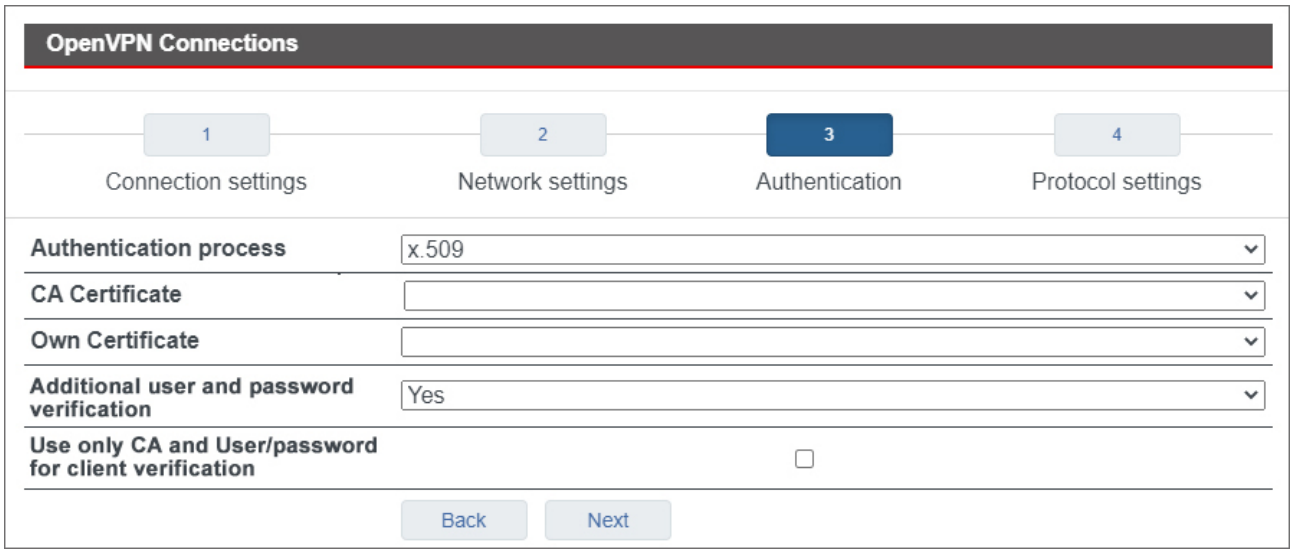
NOTICE

For symmetric encryption with a static key, you first need to generate a key (VPN OpenVPN static key) or import a previously created one. Note, however, that each participant needs to receive the key in a secure manner.

Designation	Description
Authentication process	Selection field for the authentication procedure • no authentication • **Static key** • X.509
Static Keys	Selection field with all imported keys to date.
Next	Click the Next button to continue the configuration.

(Authentication procedure = X.509 - server mode)

If "**Wait for incoming connection**" was selected to establish the connection, this mbNET is in server mode



NOTICE

For this authentication method, you must first create/import your certificates (see: "System > Certificates")

Designation	Description
Authentication procedure	Selection field for the authentication procedure • no authentication • Static key • **X.509** If you do not have any certificates, then you first need to create your own certificates using the XCA program. ° **CA certificate**: This shows the selected root cell certificate. If you have not yet imported a certificate, import your root cell certificates or create one of your own (see Section: System > Certificates). ° **Own certificate**: This displays your own certificate. If you have not yet imported a certificate, import your certificate now or create one of your own. ° **additional query of the VPN user name and password**: This is how the user data is requested by the client. These credentials must match an entry from "System users" from the OpenVPN server.
CA Certificate	Selection field with all certificates imported to date.
Own Certificate	Selection field with all certificates created to date.
Additional user and password verification	"Yes / No" selection field to activate/deactivate this function. If you select "Yes", user data is requested from the client. These credentials must match an entry from "System users" from the OpenVPN server.

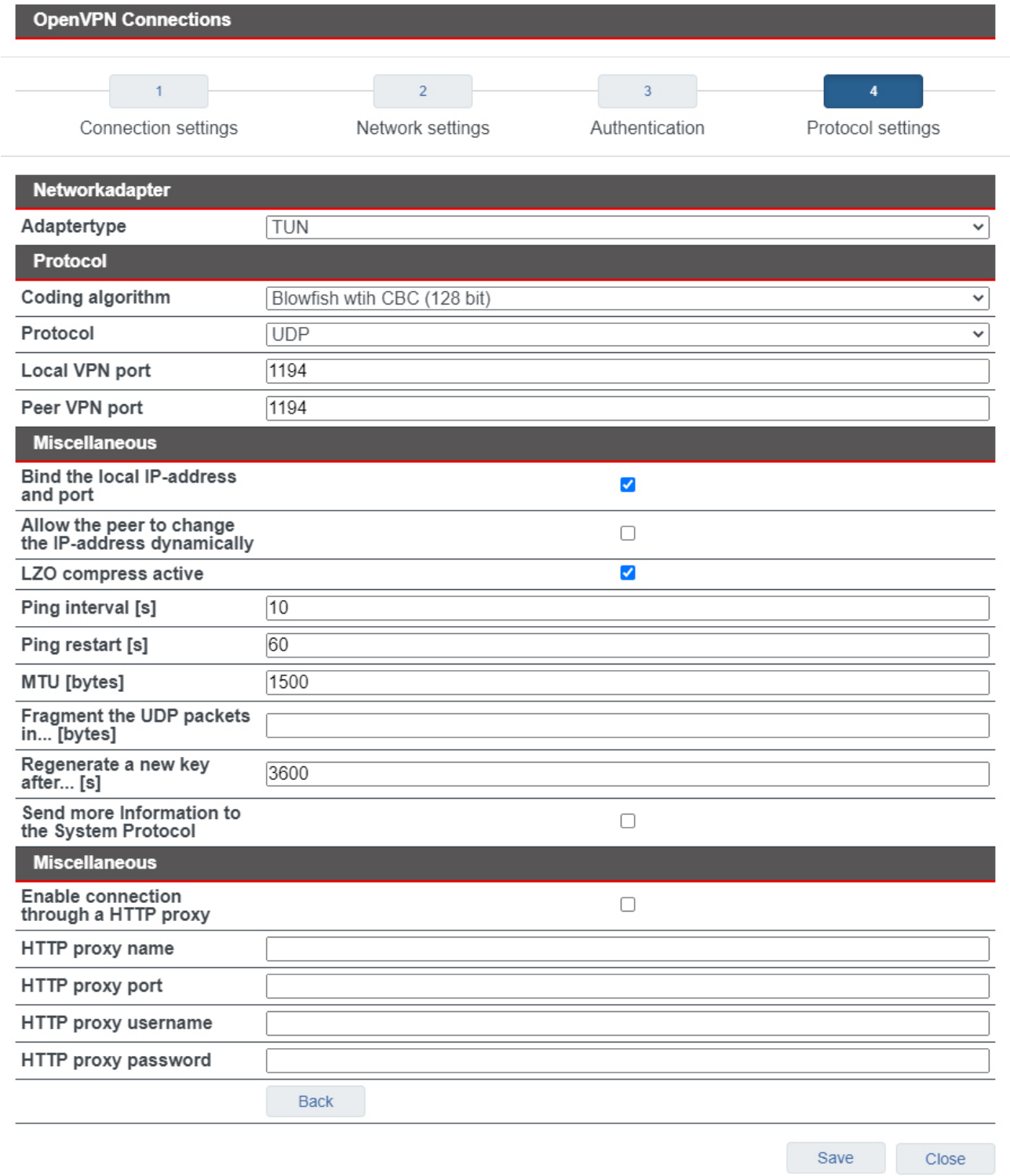
Designation	Description
Use only CA and User/password for client verification	Check box for enabling/disabling this function. In this case only the CA certificate and the user login are used for authentication.

NOTICE

Note that you still need to have your own certificate and it must be selected!

Next	Click the Next button to continue the configuration.

4 Protocol settings



Network interface controller	
Designation	Description
Encryption algorithm	Selection field for the virtual kernel driver: - TUN - TAP

Protocol	
Designation	Description
Encryption algorithm	Selection field for the method used by the mbNET to encrypt OpenVPN data: - Blowfish with CBC (128 bit) - DES with CBC (64 bit) - RC2 with CBC (128 bit) - DES-EDE with CBC (128 bit) - DES-EDE3 with CBC (192 bit) - DESX with CBC (192 bit) - Blowfish with CBC (128 bit) - RC2 with CBC (40 bit) - CAST5/128 with CBC (128 bit) - RC2 with CBC (64 bit) - AES with CBC (128 bit) - AES with CBC (192 bit) - AES with CBC (256 bit)

NOTICE

Note that each of the communication partners must use the same method.

Encryption algorithm	Selection field for the transfer protocol: - UDP - TCP
Local VPN port **Partner VPN port**	Select the port for the OpenVPN connection (example: Port 80 TCP or 1194 UDP). However, you can also freely select the port numbers, if they are not already in use by another program. It is also possible for the server and client to use different ports (Server: 1194 UDP -- Client: 20500 UDP). Note that both know the port of other and these are also set!

Miscellaneous	
Designation	Description
The local IP address and local port will be fixed (bind)	Check box for enabling/disabling this function. This corresponds to the "bind" setting of OpenVPN. OpenVPN cannot dynamically change the ports during the connection.
Allows the partners to dynamically change the IP address (float)	Check box for enabling/disabling this function. This corresponds to the OpenVPN setting "float" and allows the partner to change the address.
Use LZO compression (comp-lzo)	Check box for enabling/disabling this function. This corresponds to the OpenVPN "comp"-lzo setting.
Connect every ... [s] check (ping)	Input field for a time period [in seconds] If the VPN tunnel is not used by the end of the period, a ping is sent to the VPN partner. This corresponds to the OpenVPN "ping” setting.
Restart connection after ... [s] of inactivity (ping-restart)	Input field for the time period [in seconds] if a ping or a data packet is not received from the VPN partner within the time period, the OpenVPN tunnel is restarted. This corresponds to the OpenVPN setting "ping-restart".

Miscellaneous	
Designation	Description
Maximum transfer size (MTU) in... [bytes] (tun-mtu)	This corresponds to the setting "tun-mtu". The default size is 1500 bytes.
All UDP packets that are larger than ... [bytes] are divided into several packages (fragment)	This corresponds to the setting "fragment". The default setting is that the packages are not split (" ").
Renew the security key after ... [seconds] (reneg-sec)	This corresponds to the OpenVPN setting "reneg-sec". By default, this time is set to 3600 seconds.
Send more output information to the logging system (verb 3)	Check box for enabling/disabling this function. This corresponds to the setting "verb 3" of OpenVPN. This feature is disabled by default.

Miscellaneous	
Designation	Description
Use a HTTP proxy server as the outgoing connection	Check box for enabling/disabling this function. If this function is activated, the outgoing connection attempts to pass through a proxy server. The following fields must be completed for this purpose.
Name of the HTTP proxy server (DNS or IP)	Input field for the DNS names or the IP address of your proxy server.
Port of the HTTP proxy server	Input field for the port number on which your proxy server receives requests. A common port number, for example, would be 8080 (in the case of Linux Proxy "Squid", it would be 3128 by default).
Login name on the HTTP proxy server	If the proxy server requires authentication, enter the user data for the proxy. If you do not know this data, ask your network administrator.
Login password on the HTTP proxy server	

Click on "Save", after completing all settings.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

Apply changes	Clicking on **"Apply changes"** will apply all stored settings/changes and store them permanently on the router.
Clear Changes	"**Discard changes**" will reset/discard all temporarily stored settings/changes.

25.3.1.3 Connection type: Router-router connection - client mode

With the "router-router connection" you create a "network to network" connection.
Depending on the authentication method, the dialing party receives an IP from a defined area or each participant specifies his required address.

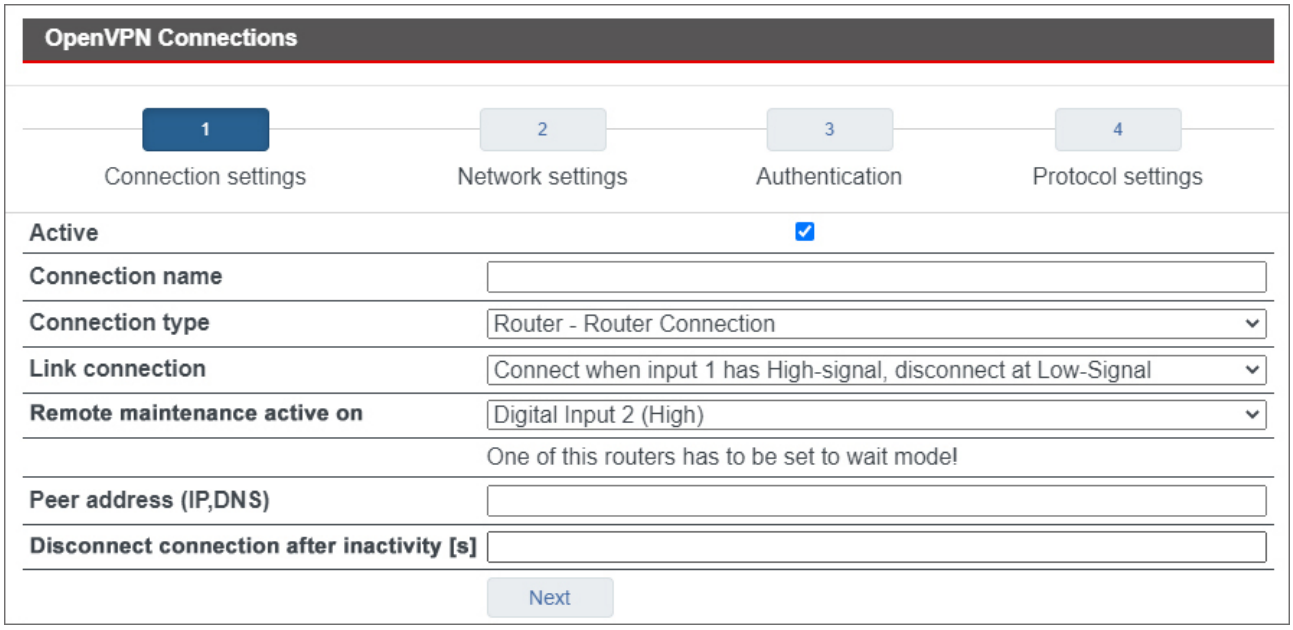
Example:

LAN	mbNET Client		mbNET Server	LAN
[192.168.9.100] <>ROUTING<>	[10.1.0.2]	**VPN-TUNNEL**	[10.1.0.1] <>ROUTING<>	[192.168.0.100]

Client mode

To establish a connection, select "**Connect while enable Key Switch position "Online (ONL)"**".
The mbNET is therefore in "**client mode**" and will be referred to as "client" in the further documentation.

1 Connection settings



Designation	Description
Active	Check box for enabling/disabling this function.
Connection name	In the text box, enter a name for the connection.
Connection type	Selection field for the connection type • **Router - Router connection** • Client router connection
Link connection	Selection field for when or under which conditions the connection should be started. - Connect while enable Key Switch position "Online (ONL)" - Wait for incoming connection

NOTICE

If one of the active connection options was selected to establish the connection, then this mbNET is in "client mode" and will be referred to as "client" in the further documentation.

The mbNET on the other side is in "waiting position".

NOTICE

One of the routers must be in "wait mode"!

Designation	Description
Remote maintenance active on	You can only choose from:: - Key switch (REM)

NOTICE

The **Link connection** and **Remote maintenance active on** functions are part of the concept of **2-level security**.

A description of the **2-level security** can be found after this table.

Peer addresse (IP, DNS)	Here, in the case of the OpenVPN client, the public IP address or DynDNS name (example: 0987654321@mbnet.mymbnet.biz) of the OpenVPN server must be entered.
Disconnect connection after inactivity [s]	Enter the time after which an existing connection is terminated if no data packets are transmitted during this time. If nothing is entered, or if the entry is "0", the connection remains.
Next	Click the Next button to continue the configuration.

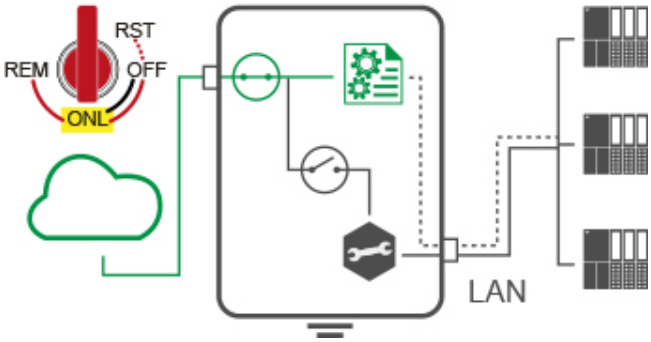
2-level security

You use the control mechanism of the 2-level access control to control or regulate remote access to a device and the components connected to it.

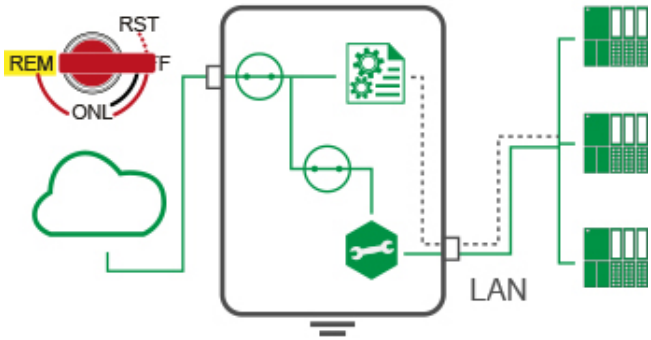
NOTICE

To prevent remote access locally is a recommendation from cybersecurity authorities such as the German BSI, the French ANSSI or the European ENISA.
The 2-level access control corresponds to the recommendations for secure remote access.

1st Level:
In the switch position "**ONL**" the mbNET (router) connects to the Internet.
The remote maintainer now has access to the router's internal services (web server, data monitoring, etc.). The remote maintenance provider **cannot** route into the LAN segment.

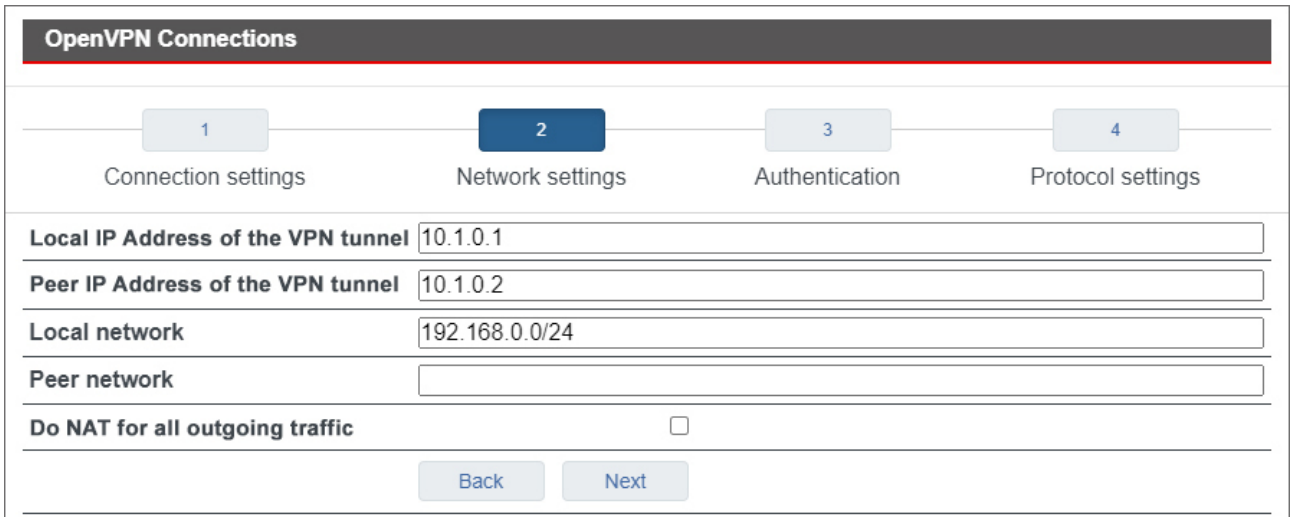


2nd Level: In the "**REM**" switch position, the routing between the remote maintenance and the LAN segment is enabled. All participants in the LAN segment can now be reached transparently. By resetting to "**ONL**", the operator can interrupt remote maintenance on site at any time.



In the "**OFF**" position, the connection to the Internet is completely disconnected. The router is offline.

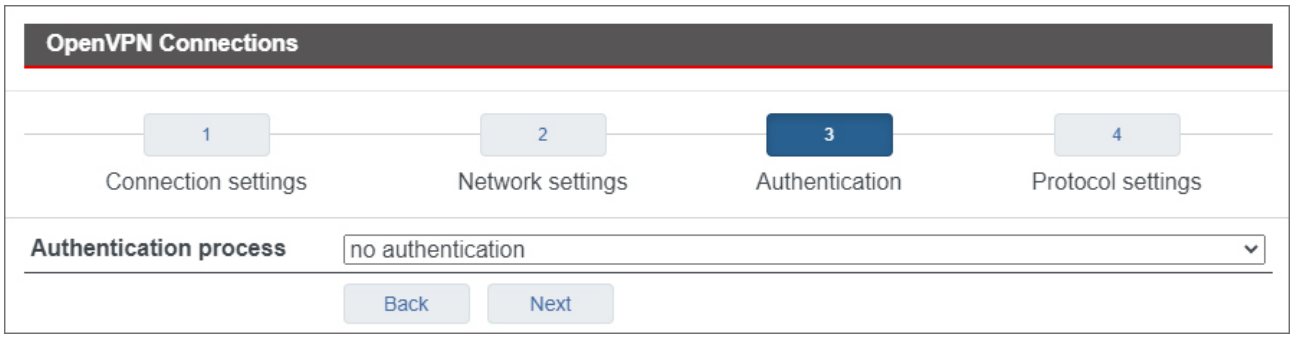
2 Network settings



Designation	Description
Local IP Address of the VPN tunnel	Enter the IP address of the local VPN tunnel endpoint. e.g. 10.1.0.5.
Peer IP Address of the VPN tunnel	Enter the IP address of the partner VPN tunnel endpoint. e.g. 10.1.0.6.
Local network	Enter your own network address in CIDR notation (as standard for the router: 192.168.0.0/24).
Peer network	Enter the network address of the subscriber (client) in CIDR notation (192.168.5.0/24)
Do NAT for all outgoing traffic	Check box for enabling/disabling this function. The option replaces the sender's address with the current Internet IP address. This is necessary for compatibility with "**mdex**".
Next	Click the Next button to continue the configuration.

3 Authentication

(Authentication method = no authentication)

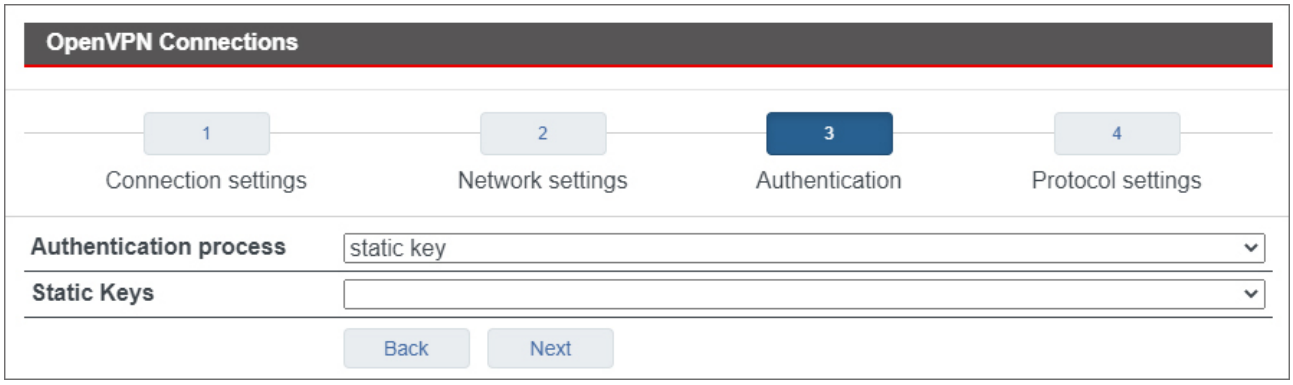


NOTICE

This type should only be selected to test the connection, as **all the data is transmitted in clear text**! **Always** enable encryption of your VPN connections, otherwise unauthorized access to networks, machines, etc. is possible!

Designation	Description
Authentication procedure	Selection field for the authentication procedure • **No Authentication** • Static key • X.509
Next	Click the Next button to continue the configuration.

(Authentication procedure = static key)



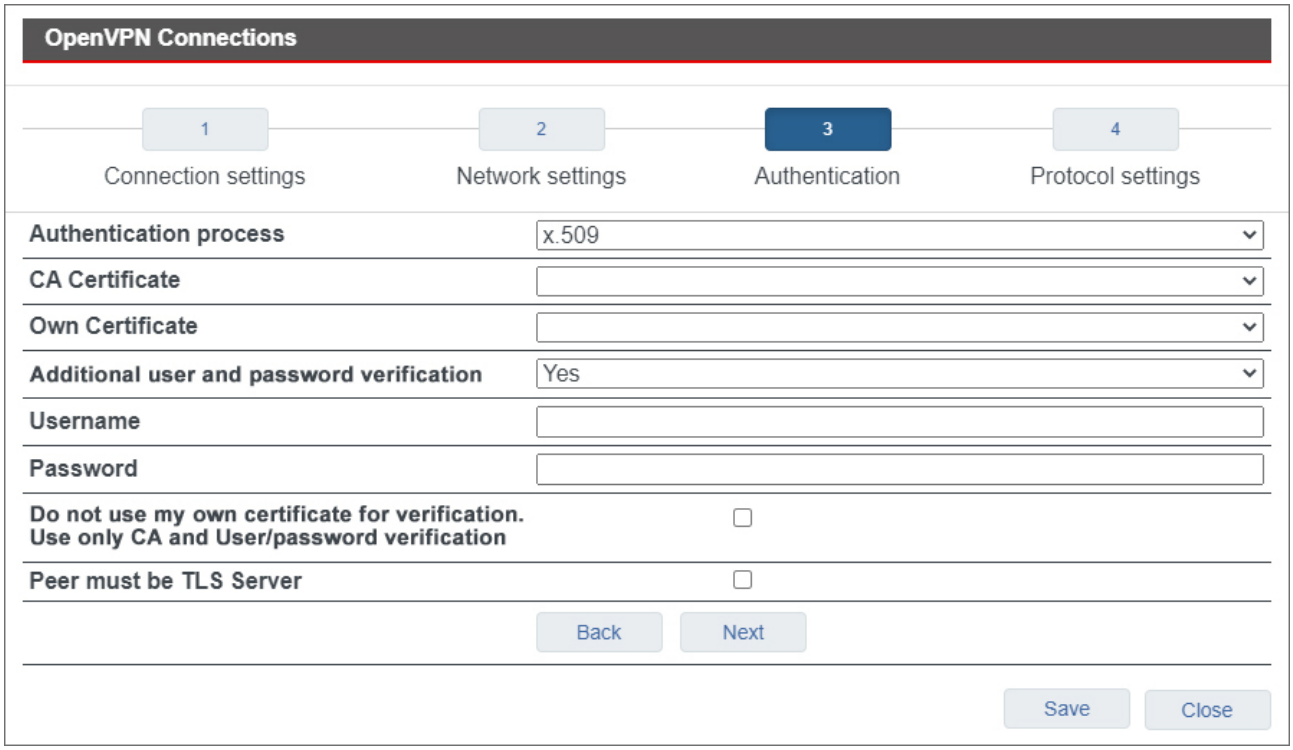
NOTICE

For symmetric encryption with a static key, you first need to generate a key (VPN OpenVPN static key) or import a previously created one. Note, however, that each participant needs to receive the key in a secure manner.

Designation	Description
Authentication procedure	Selection field for the authentication procedure • no authentication • **Static key** • X.509
Static Key	Selection field with all imported keys to date.
Next	Click the Next button to continue the configuration.

(Authentication procedure = X.509)

If you selected the option "**Connect while enable Key Switch position "Online (ONL)"**". The mbNET is therefore in "client mode" and will be referred to as "client" in the further documentation.



NOTICE

For this authentication method, you must first create/import your certificates (see: System > Certificates)

Designation	Description
Authentication procedure	Selection field for the authentication procedure • no authentication • Static key • **X.509** If you do not have any certificates, then you first need to create your own certificates using the XCA program. ° **CA certificate**: This shows the selected root cell certificate. If you have not yet imported a certificate, import your root cell certificates or create one of your own (see Section: System > Certificates). ° **Own certificate**: This displays your own certificate. If you have not yet imported a certificate, import your certificate now or create one of your own. ° **additional query of the VPN user name and password**: This is how the user data is requested by the client. These credentials must match an entry from "System users" from the OpenVPN server.
CA certificate	Selection field with all certificates imported to date.

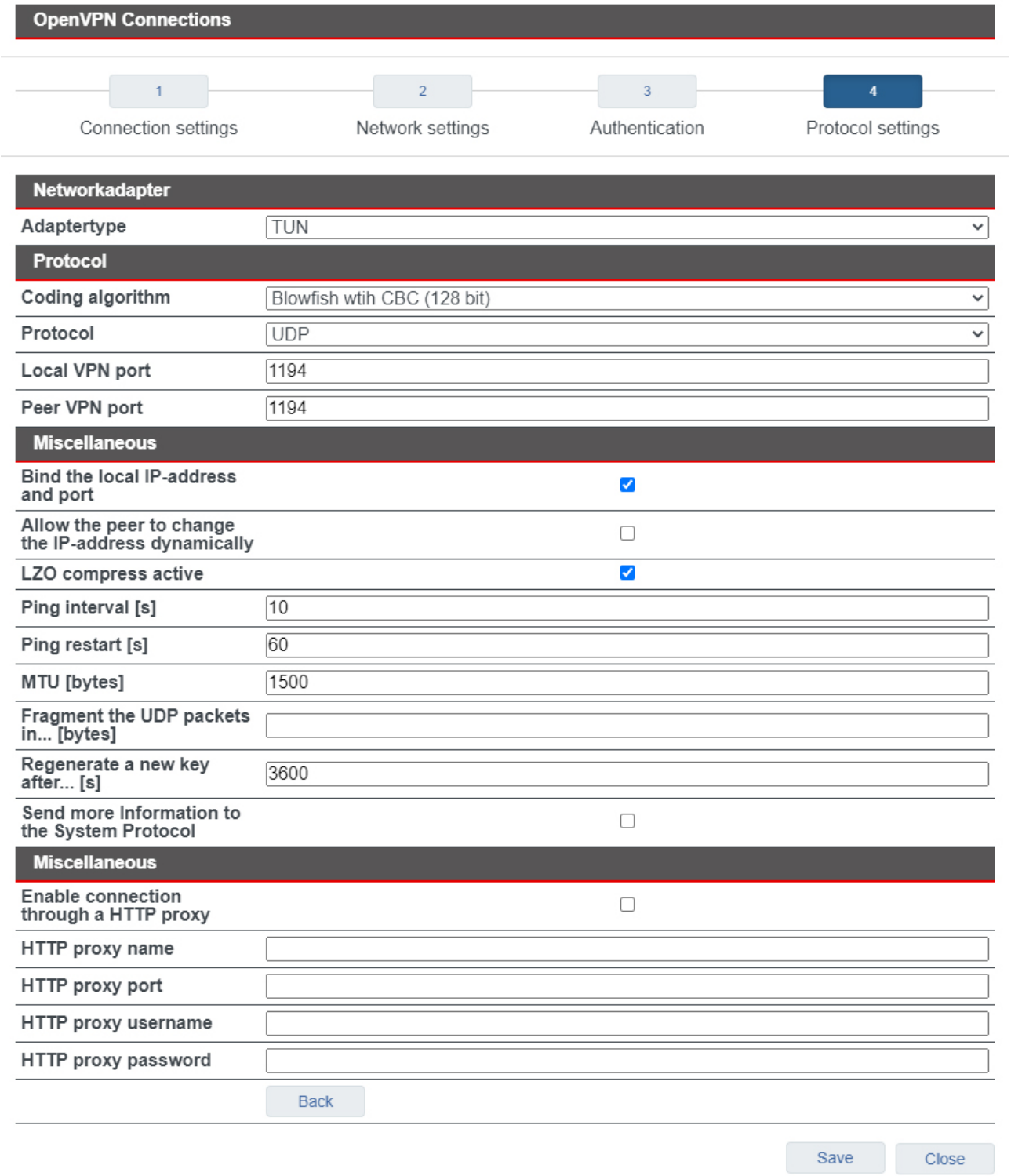
Designation	Description
Own certificate	Selection field with all certificates created to date.
Additional user and password verification	"Yes / No" selection field to activate/deactivate this function. If you select "Yes", user data is requested from the client. These credentials must match an entry from "System users" from the OpenVPN server.
User name	These credentials must match an entry from "System users" from the OpenVPN server!
Password	
Do not use my own certificate for verification. Only use the CA and user/password	Check box for enabling/disabling this function. In this case only the CA certificate and the user login are used for authentication.

NOTICE

Note that you still need to have your own certificate and it must be selected!

Peer must be TLS server	Check box for enabling/disabling this function. This additional security option checks whether the server certificate has the entry "Netscape Certificate Type: SSL Server". If this suffix to the server certificate is **not present**, the pairing process will be aborted.
Next	Click the Next button to continue the configuration.

4 Protocol settings



Network interface controller	
Designation	Description
Encryption algorithm	Selection field for the virtual kernel driver: - TUN - TAP

Protocol	
Designation	Description
Encryption algorithm	Selection field for the method used by the mbNET to encrypt OpenVPN data: - Blowfish with CBC (128 bit) - DES with CBC (64 bit) - RC2 with CBC (128 bit) - DES-EDE with CBC (128 bit) - DES-EDE3 with CBC (192 bit) - DESX with CBC (192 bit) - Blowfish with CBC (128 bit) - RC2 with CBC (40 bit) - CAST5/128 with CBC (128 bit) - RC2 with CBC (64 bit) - AES with CBC (128 bit) - AES with CBC (192 bit) - AES with CBC (256 bit)

NOTICE

Note that each of the communication partners must use the same method.

Encryption algorithm	Selection field for the transfer protocol: - UDP - TCP
Local VPN port **Partner VPN port**	Select the port for the OpenVPN connection (example: Port 80 TCP or 1194 UDP). However, you can also freely select the port numbers, if they are not already in use by another program. It is also possible for the server and client to use different ports (Server: 1194 UDP -- Client: 20500 UDP). Note that both know the port of other and these are also set!

Miscellaneous	
Designation	Description
The local IP address and local port will be fixed (bind)	Check box for enabling/disabling this function. This corresponds to the "bind" setting of OpenVPN. OpenVPN cannot dynamically change the ports during the connection.
Allows the partners to dynamically change the IP address (float)	Check box for enabling/disabling this function. This corresponds to the OpenVPN setting "float" and allows the partner to change the address.
Use LZO compression (comp-lzo)	Check box for enabling/disabling this function. This corresponds to the OpenVPN "comp"-lzo setting.
Connect every ... [s] check (ping)	Input field for a time period [in seconds] If the VPN tunnel is not used by the end of the period, a ping is sent to the VPN partner. This corresponds to the OpenVPN "ping” setting.

Miscellaneous	
Designation	Description
Restart connection after ... [s] of inactivity (ping-restart)	Input field for the time period [in seconds] if a ping or a data packet is not received from the VPN partner within the time period, the OpenVPN tunnel is restarted. This corresponds to the OpenVPN setting "ping-restart".
Maximum transfer size (MTU) in... [bytes] (tun-mtu)	This corresponds to the setting "tun-mtu". The default size is 1500 bytes.
All UDP packets that are larger than ... [bytes] are divided into several packages (fragment)	This corresponds to the setting "fragment". The default setting is that the packages are not split (" ").
Renew the security key after ... [seconds] (reneg-sec)	This corresponds to the OpenVPN setting "reneg-sec". By default, this time is set to 3600 seconds.
Send more output information to the logging system (verb 3)	Check box for enabling/disabling this function. This corresponds to the setting "verb 3" of OpenVPN. This feature is disabled by default.

Miscellaneous	
Designation	Description
Use a HTTP proxy server as the outgoing connection	Check box for enabling/disabling this function. If this function is activated, the outgoing connection attempts to pass through a proxy server. The following fields must be completed for this purpose.
Name of the HTTP proxy server (DNS or IP)	Input field for the DNS names or the IP address of your proxy server.
Port of the HTTP proxy server	Input field for the port number on which your proxy server receives requests. A common port number, for example, would be 8080 (in the case of Linux Proxy "Squid", it would be 3128 by default).
Login name on the HTTP proxy server	If the proxy server requires authentication, enter the user data for the proxy. If you do not know this data, ask your network administrator.
Login password on the HTTP proxy server	

Click on "Save", after completing all settings.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

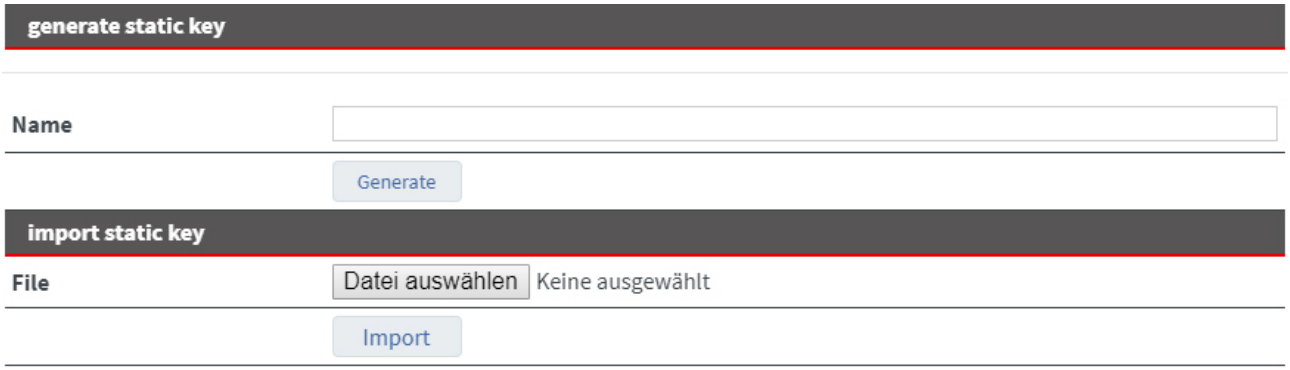
Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via “**Apply Changes**", will the changes be applied (activated) and stored permanently.

Apply changes	Clicking on **“Apply changes”** will apply all stored settings/changes and store them permanently on the router.
Clear Changes	"**Discard changes**” will reset/discard all temporarily stored settings/changes.

25.4 Static key (key management)

Here you can import or even generate static keys. All keys contained can be downloaded as a copy under "Download".

Click on the green plus  to add a key.



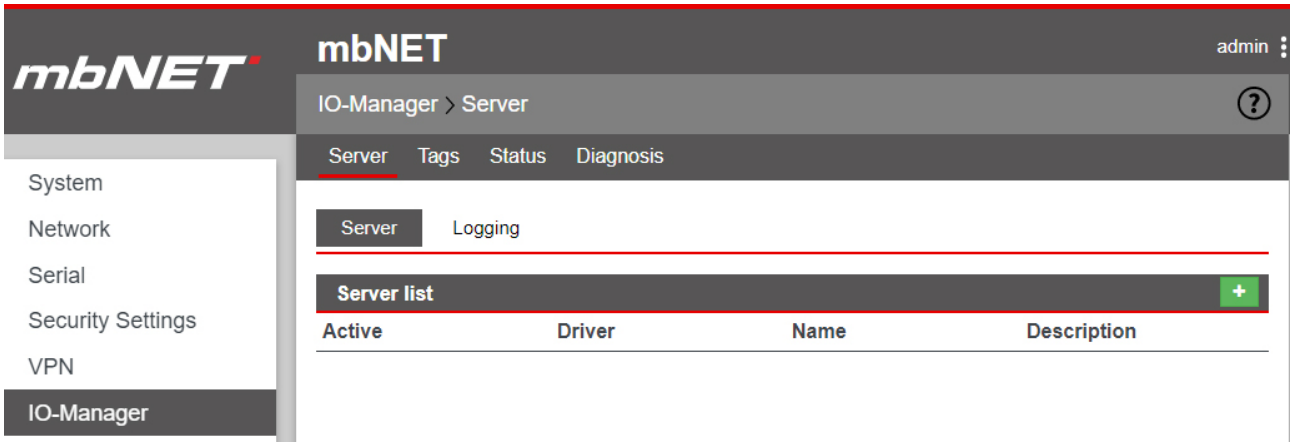
Generate static key	
Name	Enter a name for the key here
Generate	To generate the key, click the "Generate" button.

Import static key	
File	Click the "Select file" button and navigate to the save location of the key file.
Import	To import a key, click the "Import" button.

To download a key, click on the Download button  .

To delete a key, click on the Delete button 

26 IO-Manager



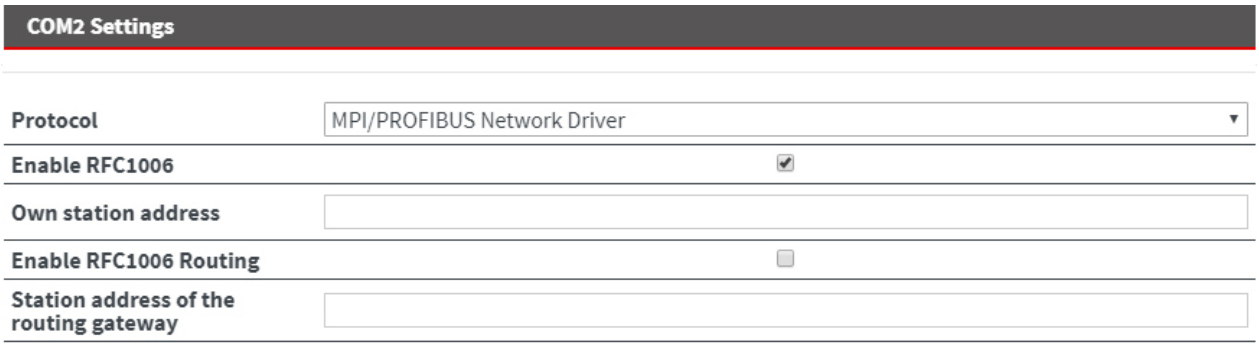
The I / O Manager integrated in the router fulfills the following tasks:

- Display of PLC variables
- Read PLC variables and, within a preset interval, save them on a USB stick (logging).
- Store the logged archives (GZIP) on an external FTP server.

Currently tags of the type flag, timer, counter, input, output, data block and peripheral can be read by an S7 controller via RFC1006.
Communication between the mbNET and the PLC takes place via the Ethernet interface or the MPI/PROFIBUS interface of the router.

NOTICE

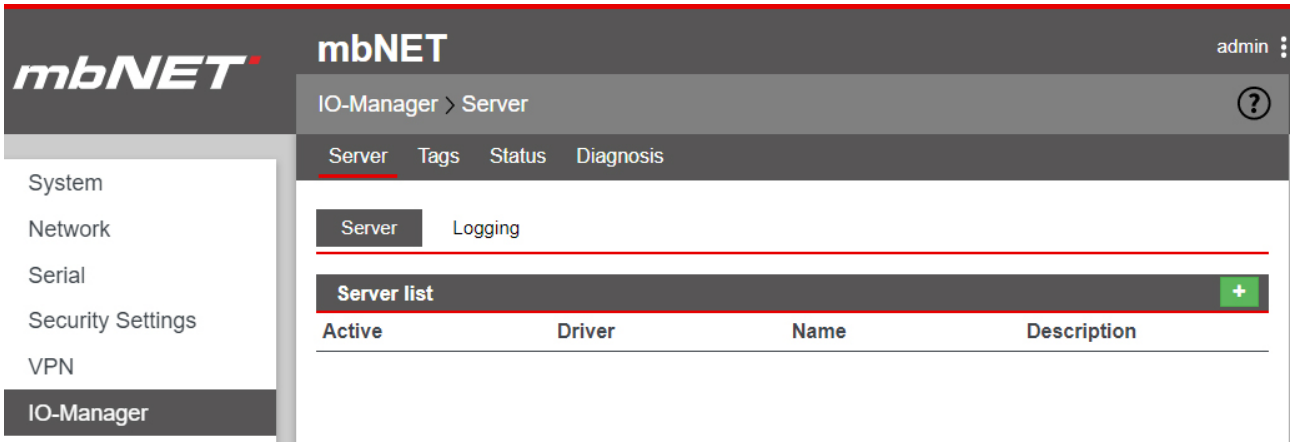
If communication is to take place via the MPI / PROFIBUS interface, the RFC1006 protocol must be activated in the settings for COM2 (Serial> COM2> COM2 Settings).



Limits:

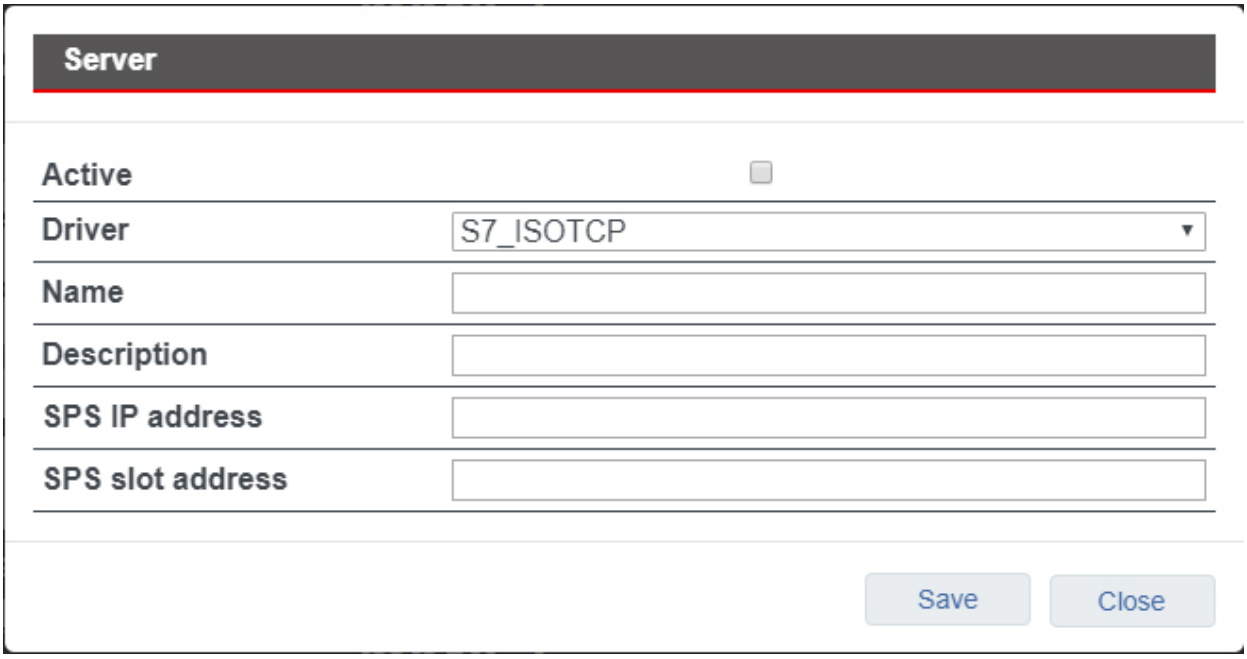
- Max. four connections to the controllers
- Max. 256 tags points (variables) per connection
- Max. size of a tag = 32 bits (DWORD)

26.1 Configuring the PLC connection



▶ Click the Add button to add a PLC connection..

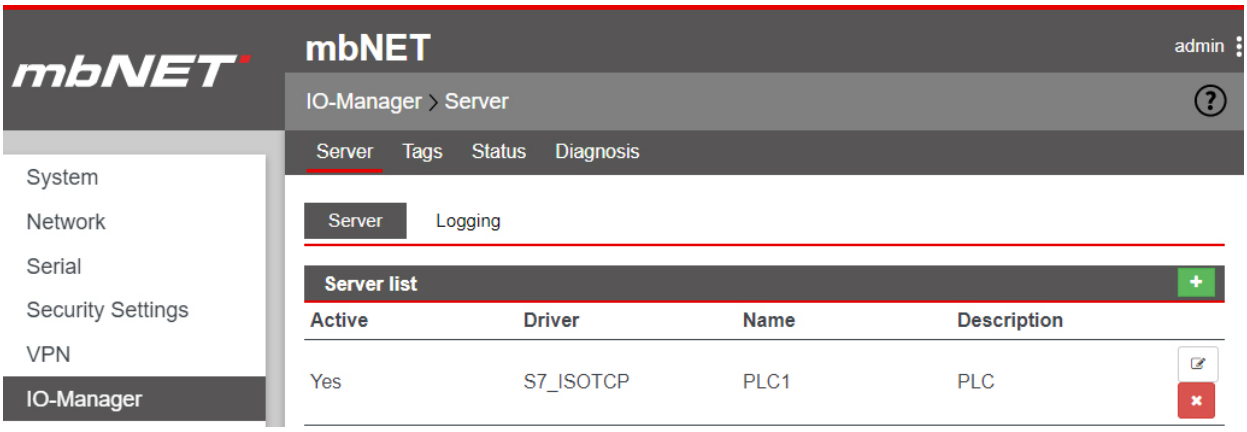
▶



Designation	Description
Active	Checkbox to enable / disable this connection.
Driver	Selected driver (only S7 ISOTCP is available here).
Name	Enter a unique name for this connection. This field can not contain any spaces or special characters.
Description	Enter a description for this connection.
SPS IP address	• When using the MPI/PROFIBUS interface, you must specify the IP address of the LAN interface of the mbNET here. • If communication is via Ethernet, enter the IP address of the PLC here.

Designation	Description
SPS slot address	• For MPI/PROFIBUS communication, the PLC slot address is the same as the bus address. • For Ethernet communication, this is the slot space of the PLC on the rack (usually 2).

▶ Click on Save (Save) to accept the input / changes.

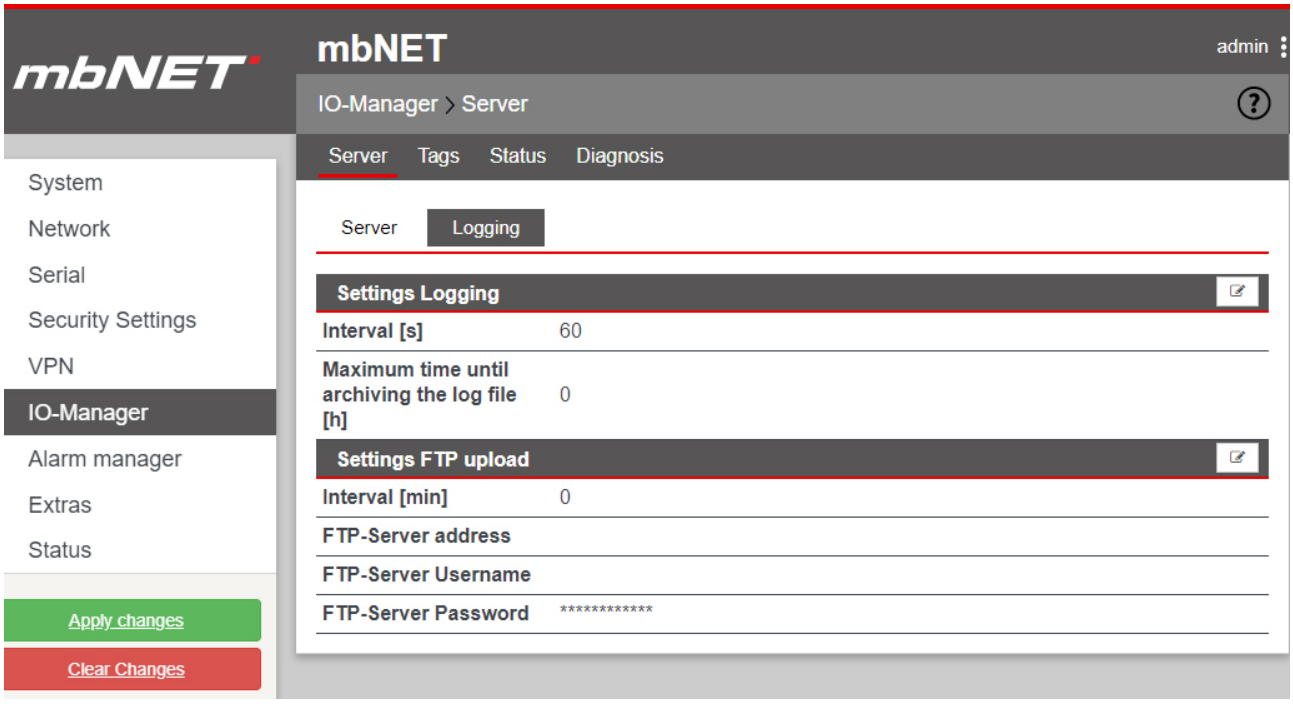


To add a PLC connection, click the add button .

To edit a PLC connection, click on the edit button .

To delete a PLC connection, click the delete button .

26.2 Logging - configuration



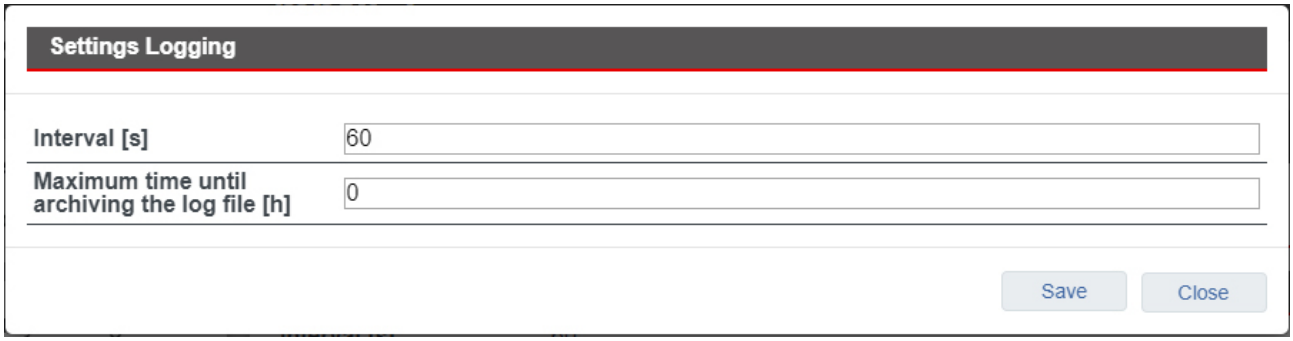
Click on the respective edit button to configure the logging settings and the settings for the FTP upload.

NOTICE

The logging settings apply to all PLC connections.

For logging, it is necessary that a storage medium (USB stick) is connected to the USB socket of the mbNET.

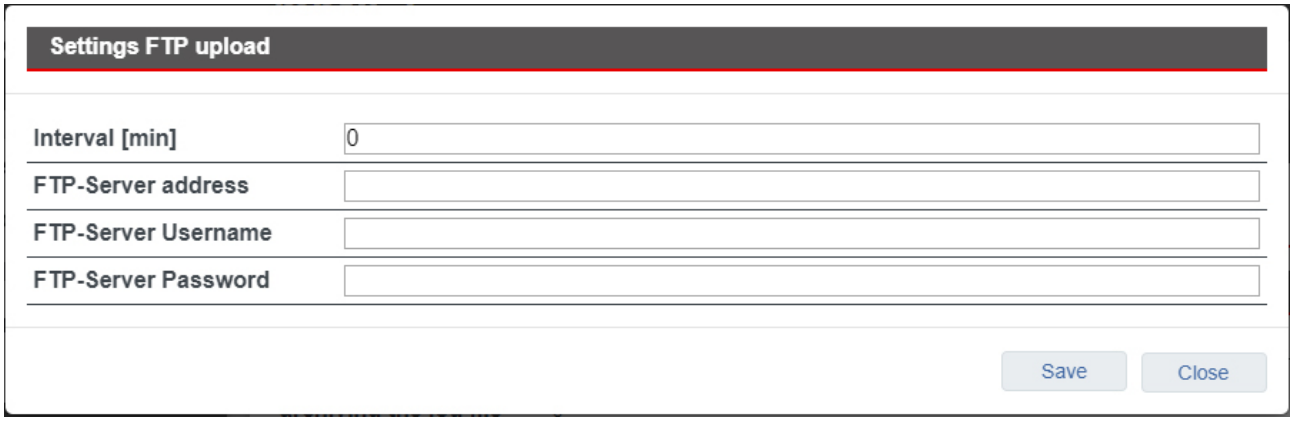
Settings Logging



Designation	Description
Interval [s]	Enter here the interval (in seconds) after which the tags are to be written to the storage medium.
Maximum time until archiving the log file [h]	After this period of time (in hours), the log file is archived and a new log file is started.

Settings FTP upload

The logged tags can additionally be archived on an FTP server. The following settings are necessary for this.

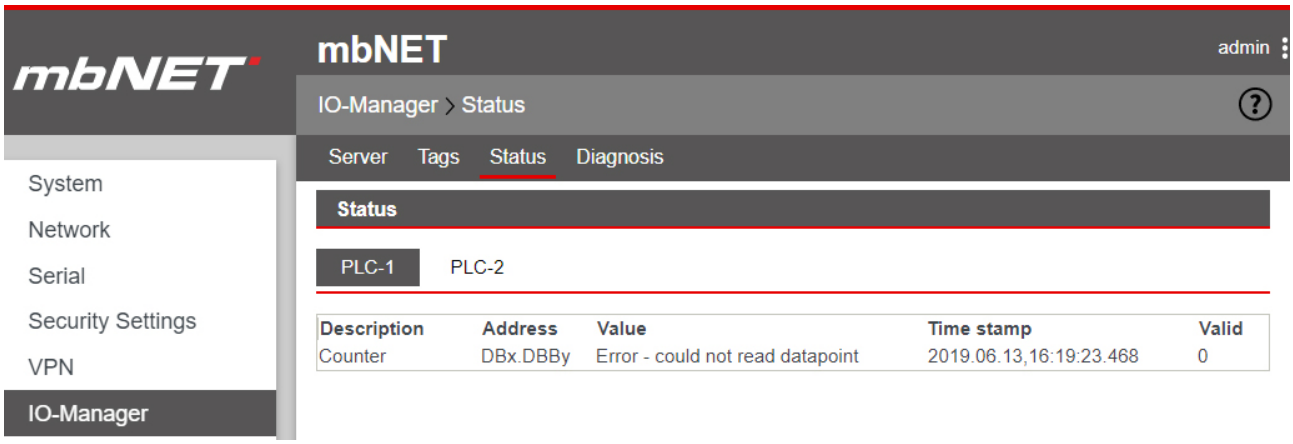


Designation	Description
Interval [min]	Enter the interval (in minutes) after which the log file is to be compressed and uploaded to the FTP server. The log file remains compressed - in addition to the storage medium (USB stick).
FTP-Server address	Enter the address of the FTP server here.
FTP-Server Username	Enter the user name for authentication on the FTP server here.
FTP-Server Password	Enter the password for authentication at the FTP server here.

NOTICE

The format of the log files corresponds to the CSV format. The current file always has the name logfile.log and is stored in the subdirectory \logfiles\ on the USB stick. Archived files are organized as follows: "logfile.log. [Date (yyyymmdd)] _ [time (hhmmssms)]. Gzip

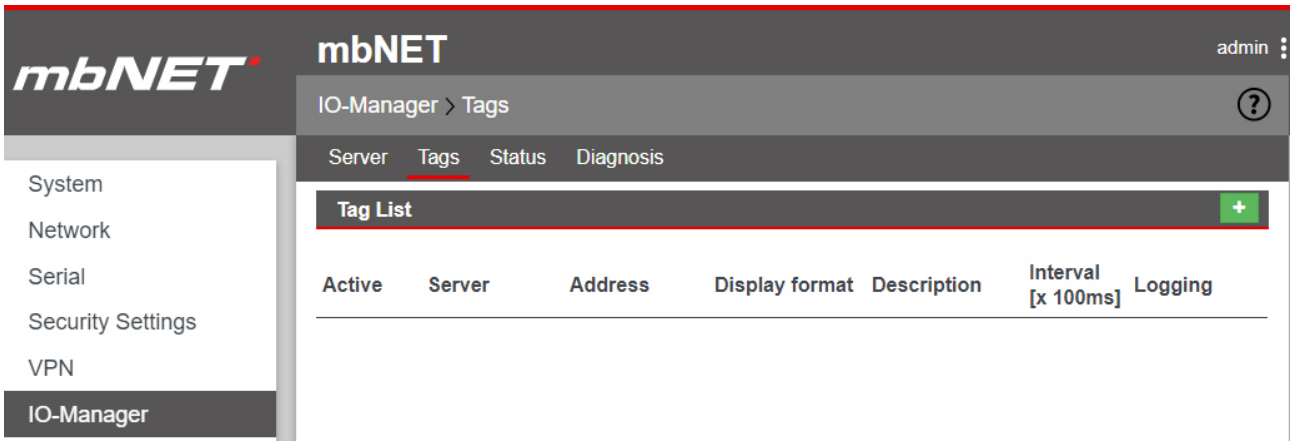
26.3 Status



Here, the status of each tag is displayed for all created PLC connections.

Designation	Description
Description	Display of the description given under "Tags".
Address	The address of a tag
Value	Displays the tag value in the display format chosen when the tag was created (BIN, DEZ, HEX, FLOAT). If the value is invalid or if the data point value can not be read, an error message appears: "Error - could not read datapoint"
Time stamp	Time when the tag was read out. If the data point is invalid or can not be read, the current device time is displayed here.
Valid	Display whether the data point value is valid / achievable (1) or invalid (0).

26.4 Create tags



NOTICE

Before you can create one or more tags, a PLC connection must be created.

To create a tag, click on the add button  .

Designation	Description
Active	Checkbox for activating / deactivating the created datapoint.
Server	Selection box with all previously created PLC connections.
Address	Enter the tag address for this PLC connection here. For the address syntax of the driver, see table below.
Display format	Selection box for the desired display format (BIN, DEZ, HEX, FLOAT). This format is used in the status display and in the logging data.
Description	Free input field.
Interval [x 100ms]	In this interval, this data point is read by the PLC.
Logging	If this option is activated, this tag is enabled to be logged. If this option is not activated, the data point is only displayed on the status display.

Address syntax for the driver S7_ISOTCP

DBx.DBXy.z =	data block x, data bit y.z, BOOL	IDy =	input double word y, DWORD
DBx.DBBy =	data block x, data byte y, BYTE	Oy.z =	output bit y.z, BOOL
DBx.DBWy =	data block x, data word y, WORD	OBy =	output byte y, BYTE
DBx.DBDy =	data block x, data double word y, DWORD	OWy =	output word y, WORD
Fy.z =	flag bit y.z, BOOL	ODy =	output double word y, DWORD
FBy =	flag byte y, BYTE	PIy.z =	peripheral input bit y.z, BOOL
FWy =	flag word y, WORD	PIBy =	peripheral input byte y, BYTE
FDy =	flag double word y, DWORD	PIWy =	peripheral input word y, WORD
Iy.z =	input bit y.z, BOOL	PIDy =	peripheral input double word y, DWORD
IBy =	input byte y, BYTE	Ty =	Timer y, TIMER
IWy =	input word y, WORD	Cy =	Counter y, COUNTER

Table 2: Address syntax for the driver S7_ISOTCP

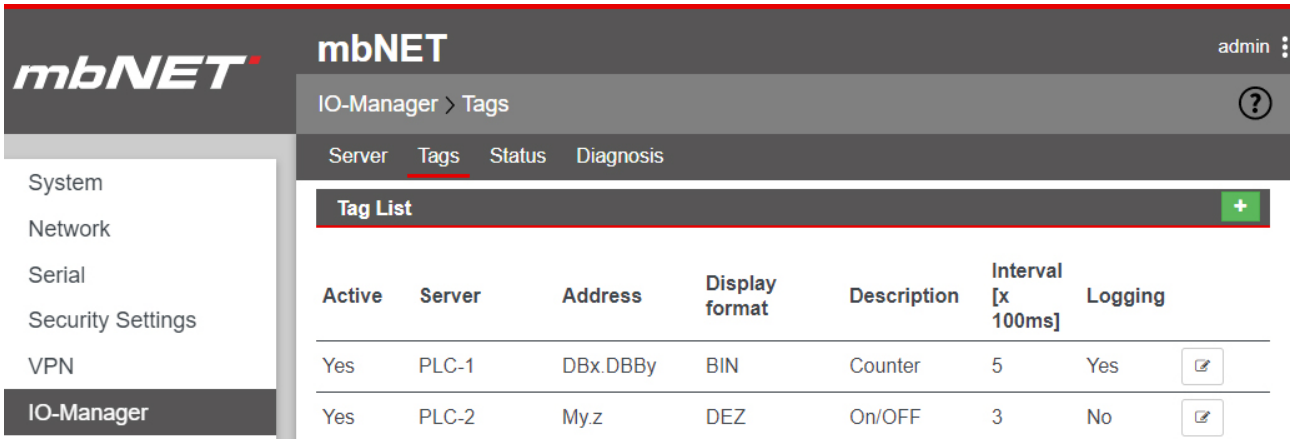
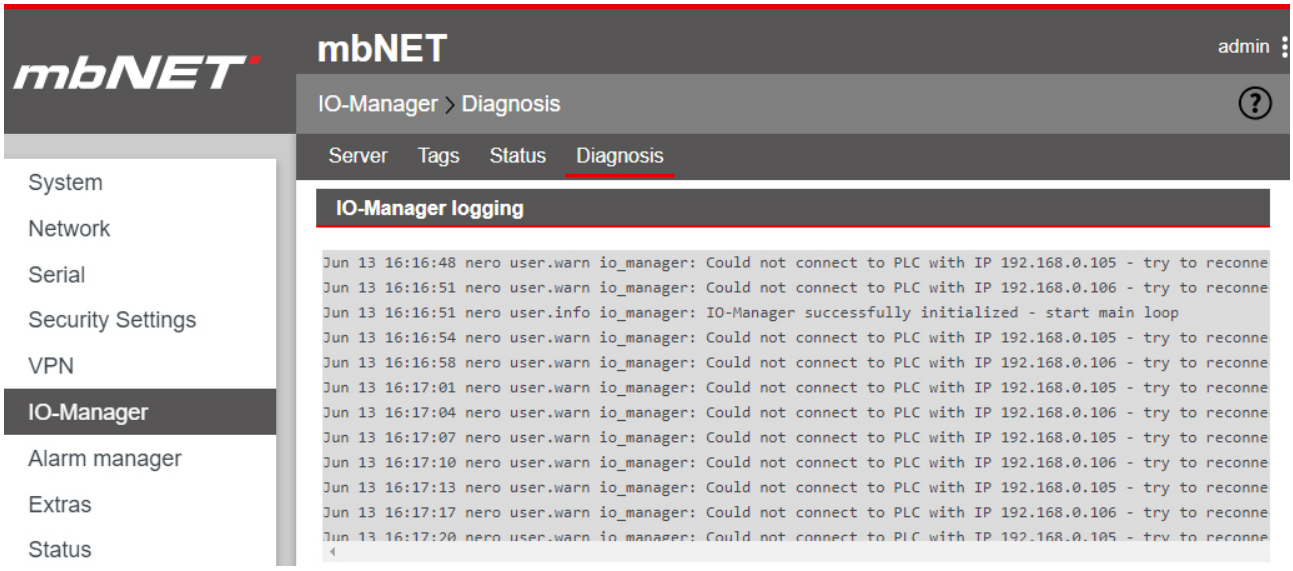


Image 22: Beispiel-Datenpunkte

To edit a data point, click the edit button .

26.5 Diagnosis



Here you can view and analyze the logging.

27 Alarm Management

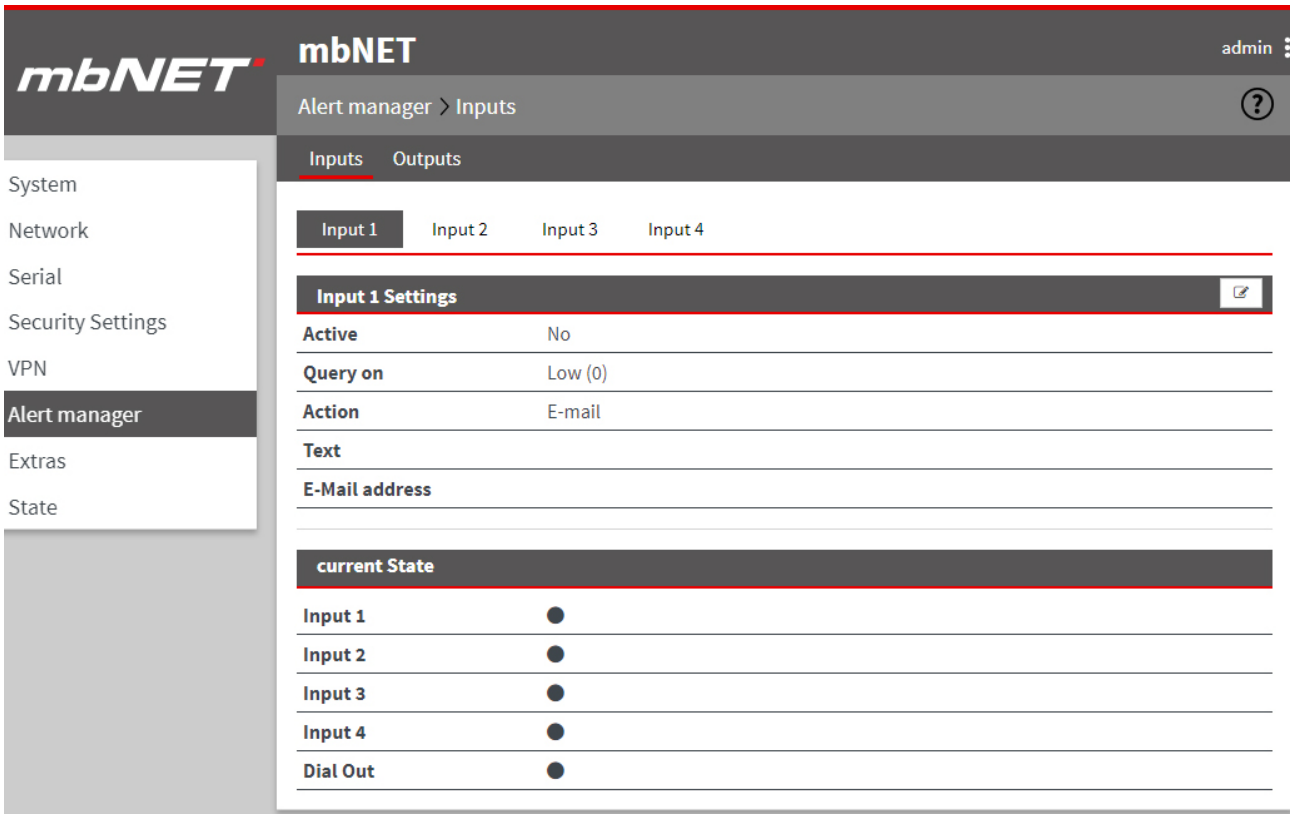
The mbNET alarm management provides the following functions:

- Status query (1/0) of the four digital inputs (I1 - I4) with subsequent action:
  - Send an email, SMS, an Internet SMS
  - Perform a device reboot
- independent switching of the two digital outputs for specific events:
  - On in the event of a device fault
  - On in the event of an active internet connection
  - On in the event of an active VPN connection
  - On in the event of an active user portal connection
  - Off

27.1 Digital inputs - Configuration

NOTICE

The configuration of input 1 is representative for inputs 2 - 4.

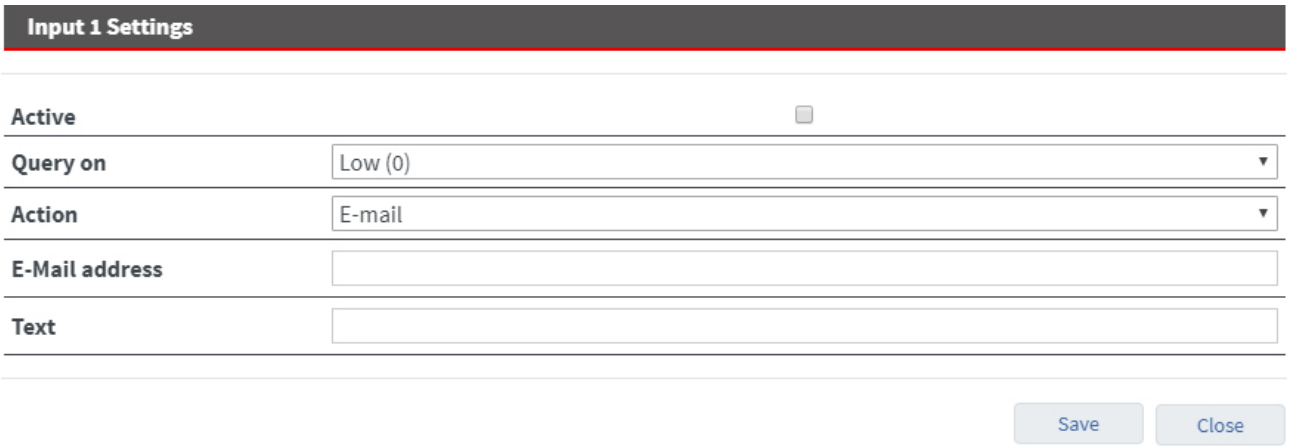


Input 1 settings displays the settings of the selected input.

Current status displays the current status (1 or 0) of the individual inputs, as well as an LED symbol for the Dial-out button.

●	grey LED symbol =	no signal (0)	Low = 0 - 3.2 V DC
●	green LED symbol =	Signal is present (1)	High = 8 - 30 V DC

Click the Edit icon , to configure the selected entry.



Designation	Description
Active	Check box for enabling/disabling this function. When this feature is enabled, the input is activated ("armed").
Query on status	Selection field "Low (0)/High (1)/No" to query the status of the relevant input.
Campaign	Selection field for the action to be performed when the selected status of the relevant input occurs: • **Email** - an email message is sent. • **Restart** - there is a device reboot. • **SMS** (only for Manet types with GSM modem) - here an SMS is sent. • **Internet SMS** - here an SMS is sent.
E-mail address	Enter the email addresses to which the alarm text should be sent.
Phone number	Enter the telephone number to which the alarm text should be sent via SMS/Internet SMS.

NOTICE

You can enter up to three telephone numbers (separated by a comma ",").

Text	Input field for the alarm text, to be sent by email or SMS. The following special characters are allowed in the text: **Ä Ü Ö , ; . : - _ # + * ~ ^ ° ! ( ) = ? § $ % & / < >**

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

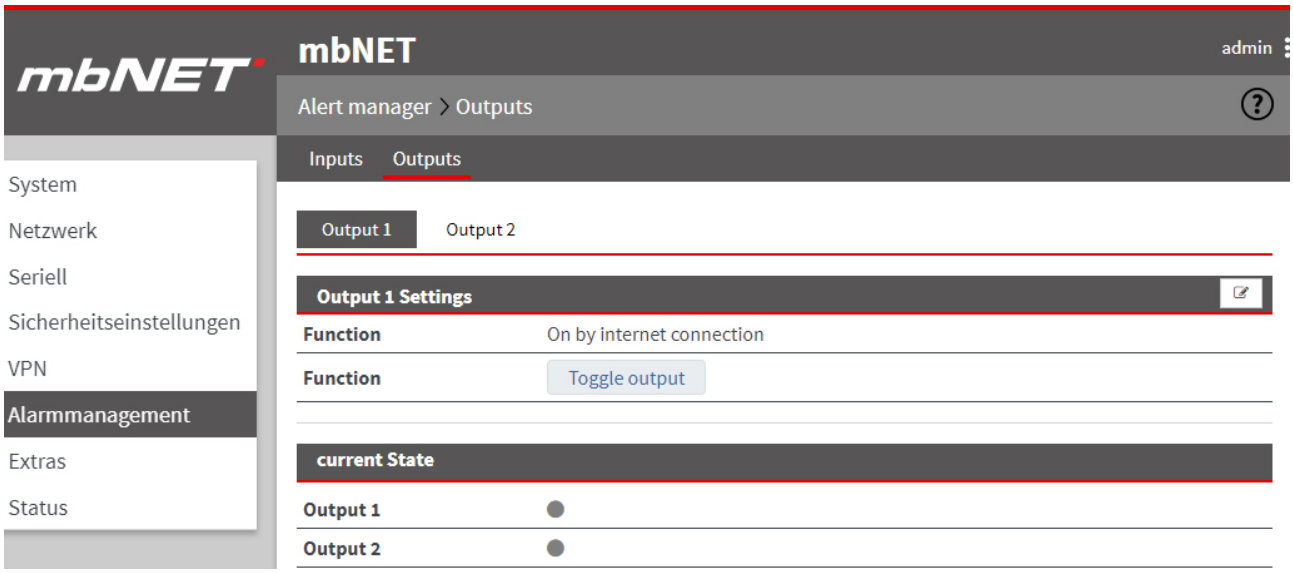
NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

27.2 Digital outputs - Configuration

NOTICE

The configuration of output 1 is representative for output 2.



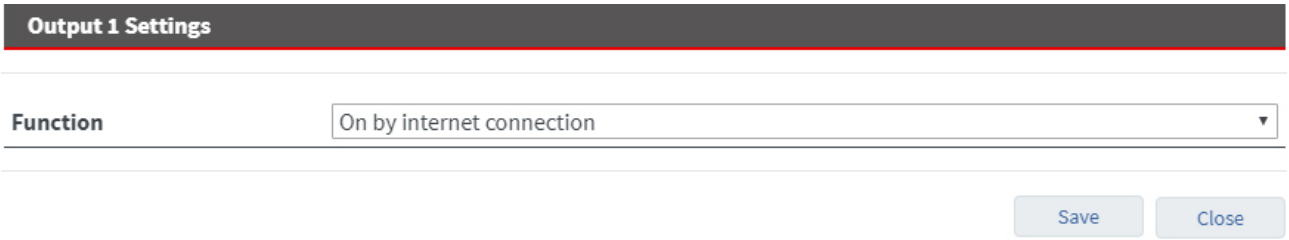
The settings of the selected output are under **Output 1 settings**.

By clicking on the button "**Switch output**", the status of the selected output mode is switched (from 0 to 1 or from 1 to 0).

Current status displays the current status (1 or 0) of the individual outputs by means of a LED symbol.

- ● grey LED symbol = Signal level 0 = Output not switched
- ● green LED symbol = Signal level 1 = Output switched

Click the Edit icon , to configure the selected output.



Designation	Description
Function	Selection field for the condition for switching the selected output: • **Off** Select these settings, if the selected output should not be switched. • **On, for a fault in a device** Select this setting in the event of a device fault if the selected output should be set to signal level 1. • **On, for an active internet connection,** Select this setting if the selected output should be set to 1 when connected to the Internet. For example, an active Internet connection can thus be signalled by a lamp connected to the corresponding output. • **On, for an active VPN connection,** Select this setting if the chosen output should be set to 1, once a user is connected to the mbNET via an active VPN connection. If the active connection is lost, the output is switched off again. For example, an active Internet connection can thus be signalled by a lamp connected to the corresponding output. • **On, for an active user portal connection,** Select this setting if the selected output should be set to 1, as soon as at least one mbCONNECT24 user has an active connection to the mbNET. If the active connection is lost, the output is switched off again. For example, an active Internet connection can thus be signalled by a lamp connected to the corresponding output.

Save	Clicking on **"Save"** temporarily saves the current entries/changes. **But the changes are not yet enabled**.
Close	Clicking on **"Close"** discards the current input/changes.

NOTICE

Temporary stored settings/changes are saved until a reboot of the router.
Only after you confirm via "**Apply Changes**", will the changes be applied (activated) and stored permanently.

28 Extras

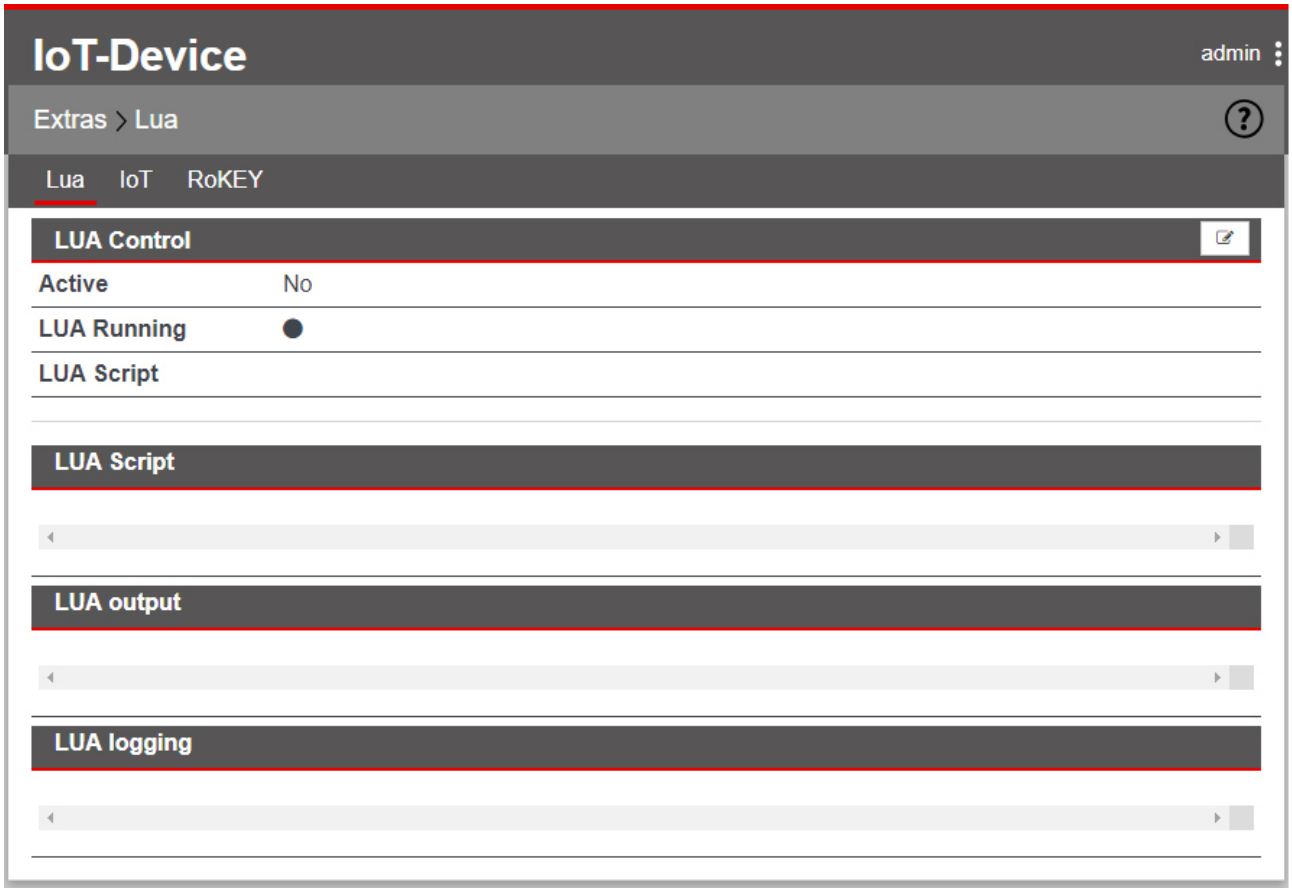
In the category Extras you will find the submenus

- Lua
- IoT
- RoKEY

28.1 LUA

LUA (programming language)

Via **Extras > LUA** LUA scripts can be imported and run.



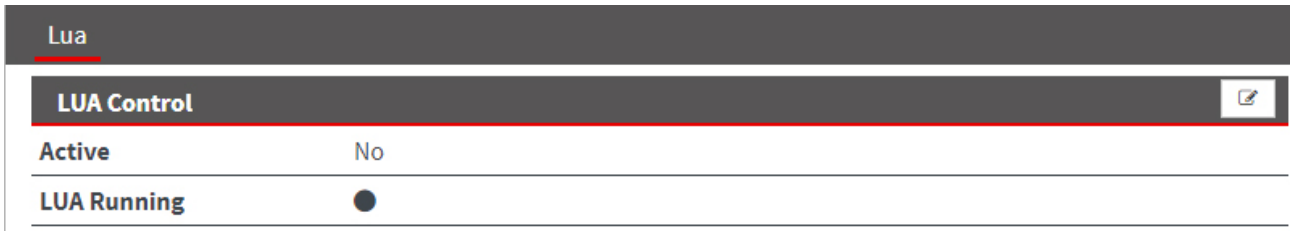
LUA Controller

Use the **LUA Control**

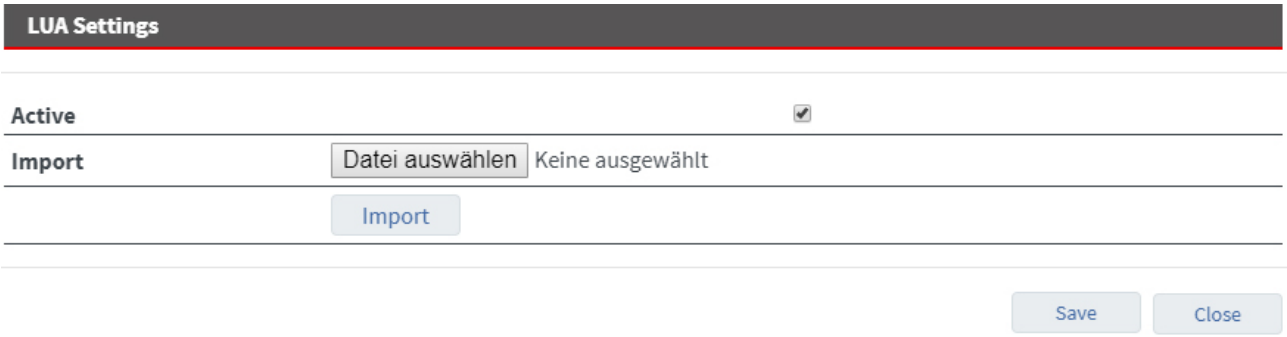
- to enable LUA
- import LUA scripts
- see whether LUA is currently running (**LUA running**)

  grey LED symbol = LUA is not running

  green LED symbol LUA running



Click the Edit icon to edit the corresponding function.



Designation	Description
Active	Check box for enabling/disabling this function. If this checkbox is activated, the LUA script runs after each router reboot.
Import	Choose a LUA-script via the file browser (* .lua) and confirm the action by clicking on the "Import" button.

NOTICE

There can only be uploaded and executed one LUA script at a time.
An imported script automatically overwrites an existing script without security confirmation.

LUA script

LUA Script

```
-- ------------------- --
-- function CONN_plc() --
-- ------------------- --
function CONN_plc(...)
local arg = {...};
local _ip = arg[1];
local _slot = arg[2];
local PLC_HANDLE = nil;

        PLC_HANDLE = plc_connect("ISOTCP", _ip, _slot);
        return PLC_HANDLE;
end;
```

Here you can see the source code of the currently imported LUA script.

NOTICE

This function is only used to display the current script. The source code cannot be edited here.

LUA output

LUA output

All readouts of the script are displayed here. For example, readouts with "print".

LUA logging

LUA logging

All error messages are shown here.

28.2 IoT > Control (mbEDGE)

In the submenu IoT you configure and manage the mbEDGE functionality.

NOTICE

mbEDGE is a software kit that extends the router mbNET and mbNET.rokey to an edge gateway. The basis for this is the container platform Docker, in which several user applications are executed separately. With Node-RED there is a graphic development tool with whose function blocks the user can create individual IOT applications.

NOTICE

Information on the configuration and setting options of **mbEDGE** can be found in the relevant manual on https://www.mbconnectline.com/de/support/downloads.html

NOTICE

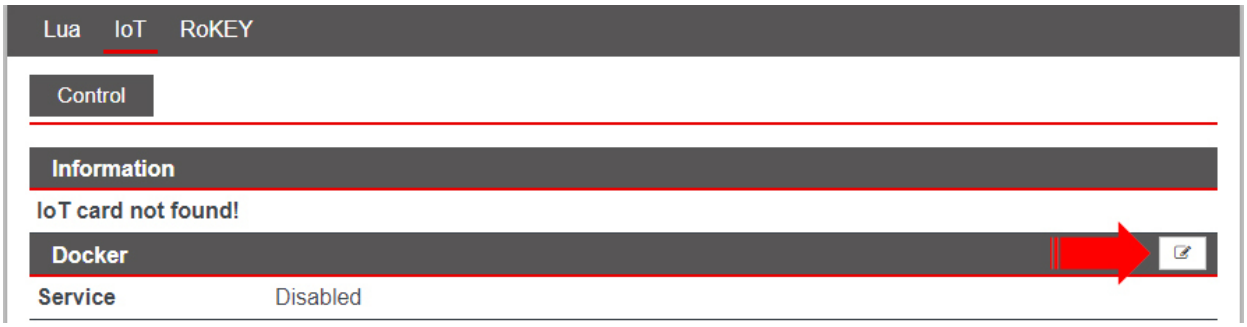
Further information such as application examples, FAQs, videos and product information about ***mbEDGE*** can be found in our Helpdesk at www.mbconnectline.com

28.2.1 IoT > Control > Docker - activate mbEDGE

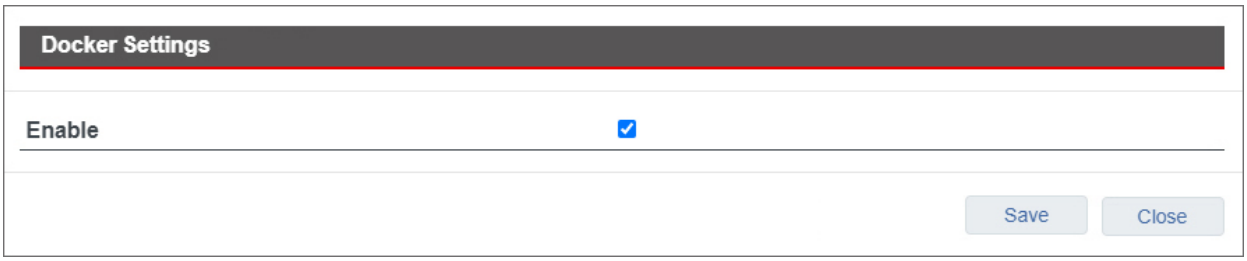
NOTICE

If you have not already done so, insert the mbEDGE SD card into the SD card slot of the mbNET.

- Click the edit icon to enable the Docker service.



- Enable the Docker settings. Click on "Save" to save the change.



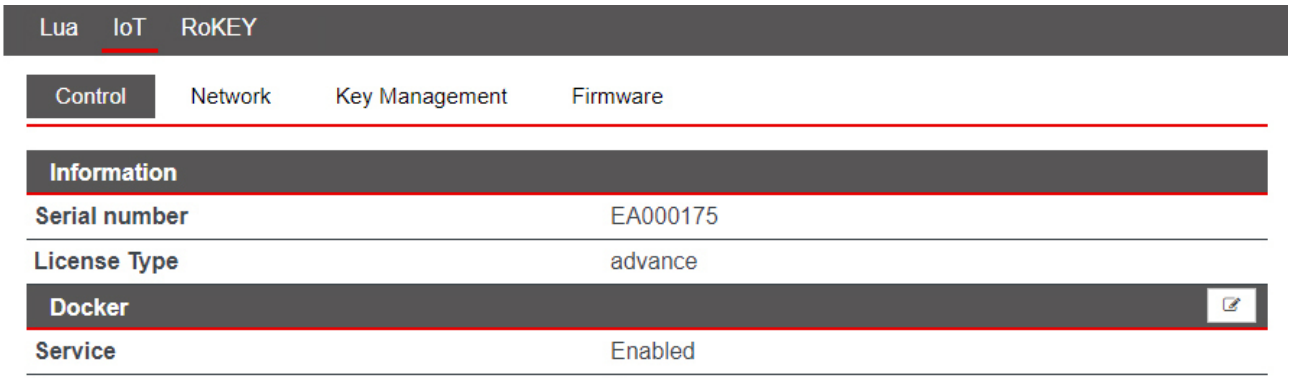
- Apply changes

  Confirm the activation by clicking on "Apply changes".

NOTICE

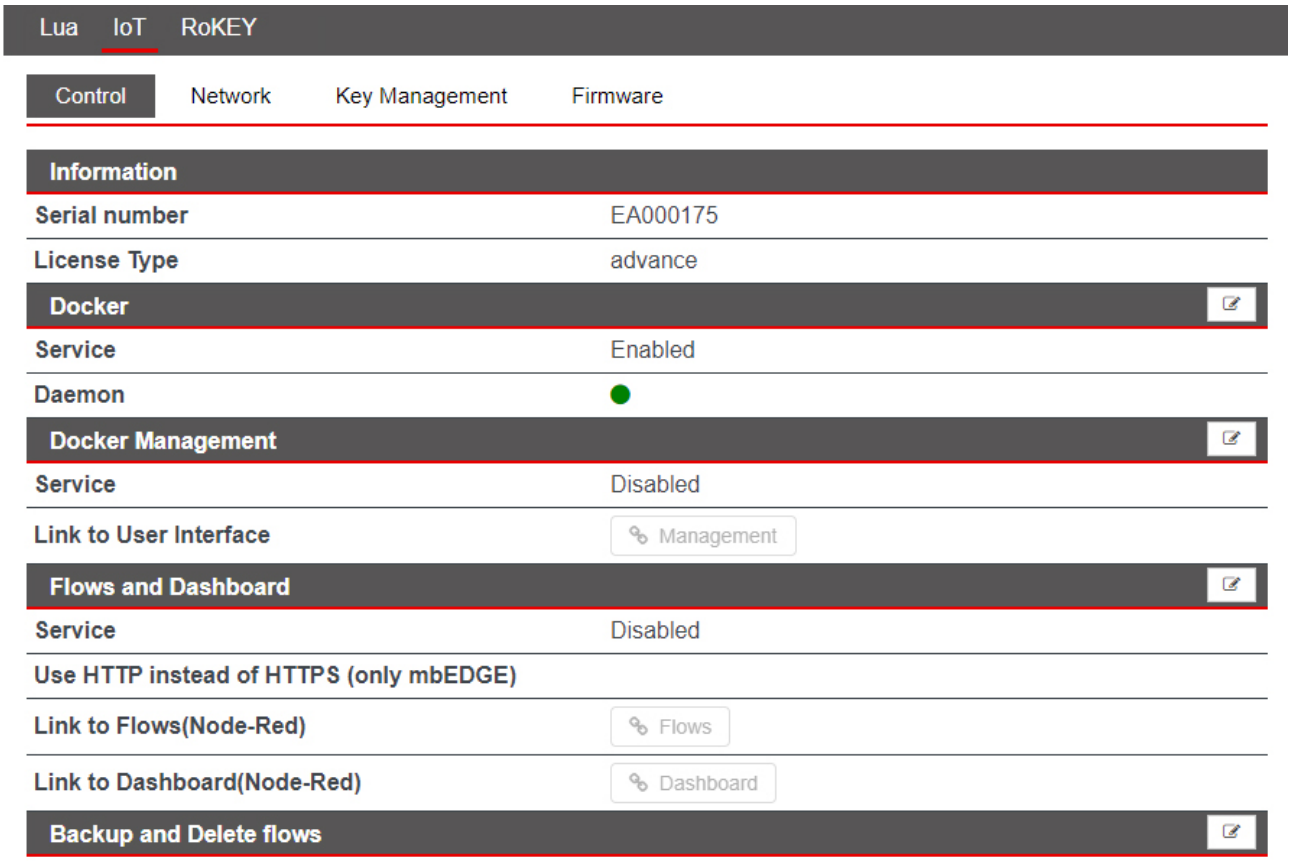
The mbEDGE service is now started. This may take a few minutes at the first activation.

In the now expanded menu, you can activate additional services and make settings.



28.2.2 IoT > Control - after activating mbEDGE

After activating mbEDGE, you will see the full scope of the IoT menu with all submenus.



Information

- Serial number of the mbEDGE card
- License Type
  Here you can see the license type of your mbEDGE card: mbEDGE.start or mbEDGE.advanced.

Docker

- Service
  Activate your mbEDGE license here.
- Daemon
  LED symbol indicates whether the Docker daemon is active (green symbol).

Docker Management

- Service
  Activate Docker Management here.
- Link to User Interface
  The "Management" button takes you to the container management.

Flows and Dashboard

- Service
  Here you activate access to your flows and your dashboard.
- Use HTTP instead of HTTPS (only mbEDGE)
  Here you can switch from HTTPS to an unencrypted connection (HTTP).
  The unencrypted connection only applies to Flows and Dashboard and not to access to the mbNET GUI.
- Link to Flows(Node-Red)
  The "Flows" button takes you to the Node-Red flows
- Link zu Dashboard(Node-Red)
  The "Dashboard" button takes you to the Node-Red dashboard.

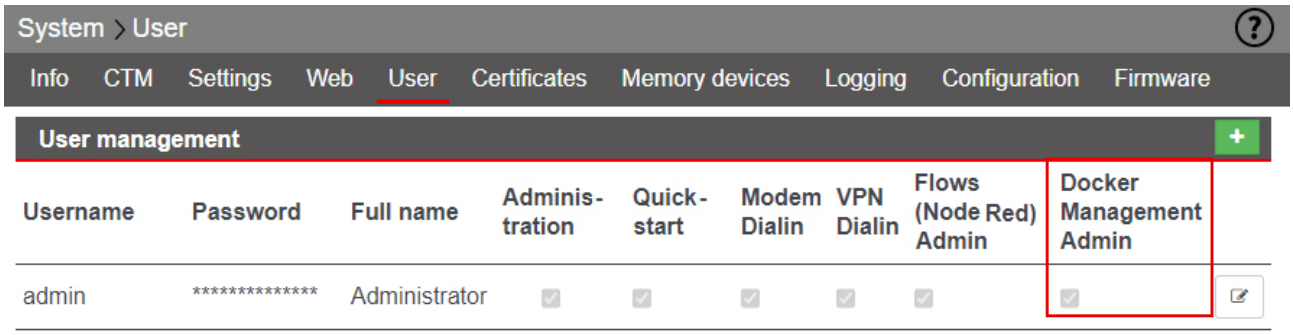
Backup and Delete flows

- Here you can save and / or delete the flows you have created.
  Saved flows can be read in again via Node-Red.

28.2.3 IoT > Control - activate Docker Management

NOTICE

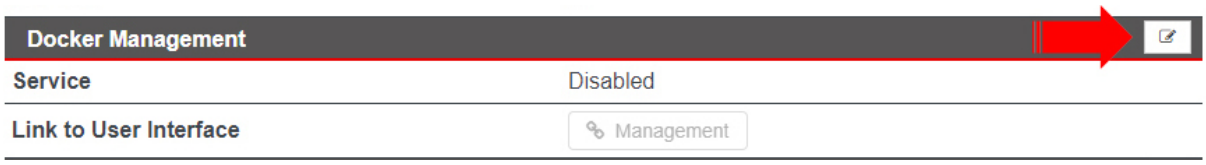
You can only activate Docker Management if you have activated "Docker Management Admin" under **System > Users**.



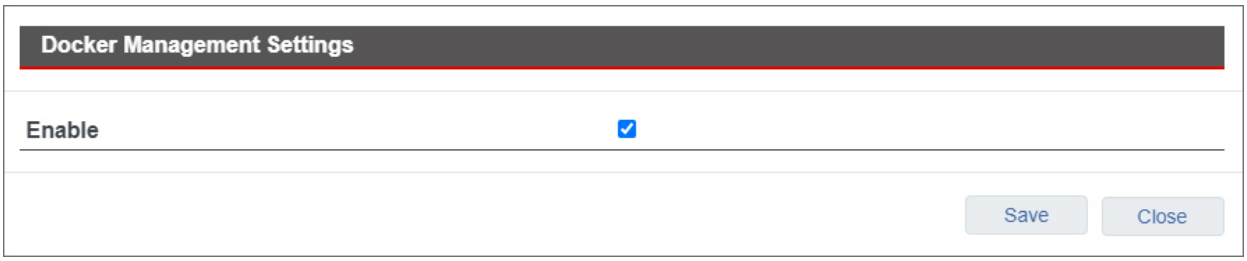
NOTICE

Activate Docker Management only if you have purchased an mbEDGE.advance license.

- Click on the edit icon to activate Docker Management.



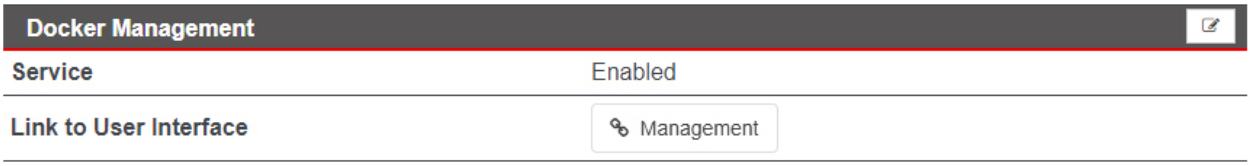
- Activate the Docker Management.
  Click on "Save" to save the change.



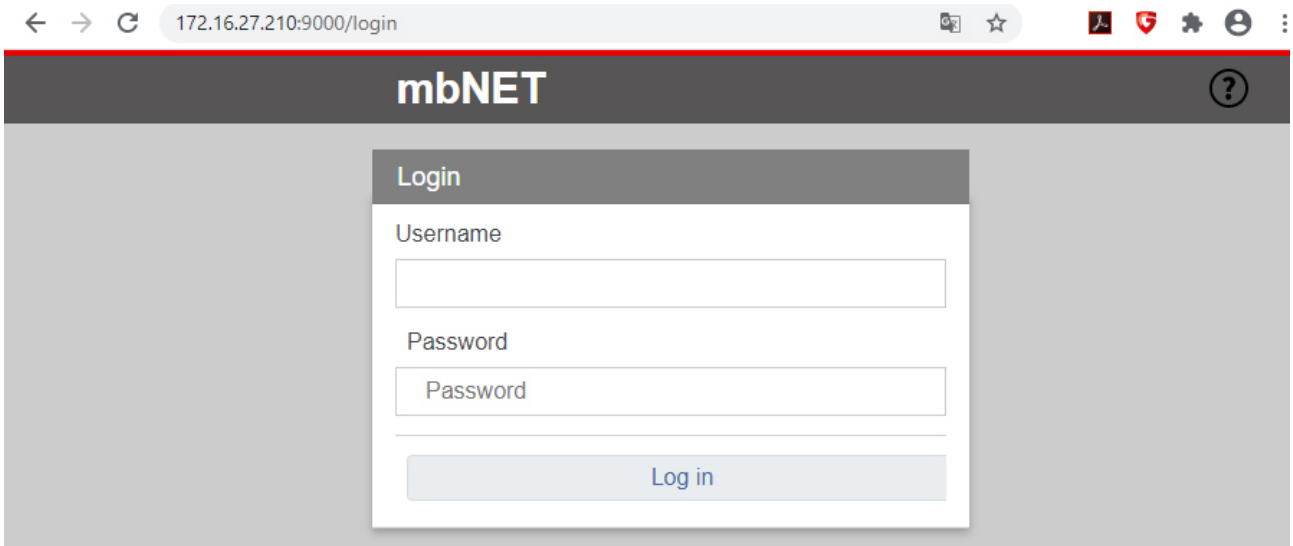
- Apply changes

  Confirm the activation by clicking on "Apply changes".

28.2.3.1 Link to User Interface



Click on the "Management" button to get to the container management.



A new browser window, with a login, will open.

The access data for this are:

a) User name and password for the user you created in the user management for accessing Node-Red

or

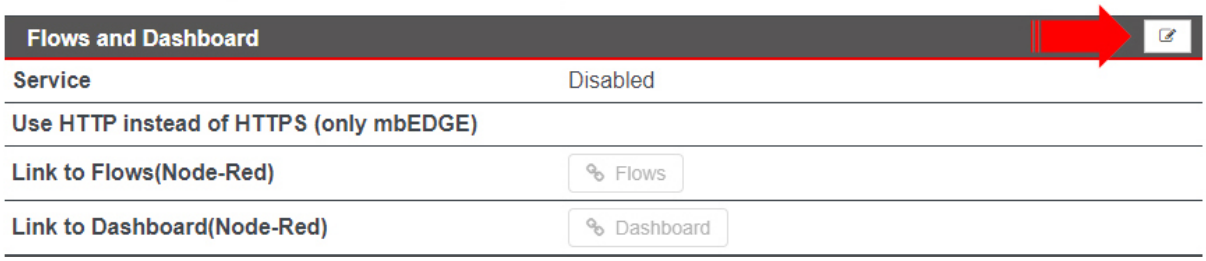
b) the current user data for the administrator (device access data)
standard user name = admin
standard password = the device password of the mbNET (see label on the back of the mbNET)

Further information such as application examples, FAQs, videos and product information about ***mbEDGE*** can be found in our Helpdesk at www.mbconnectline.com

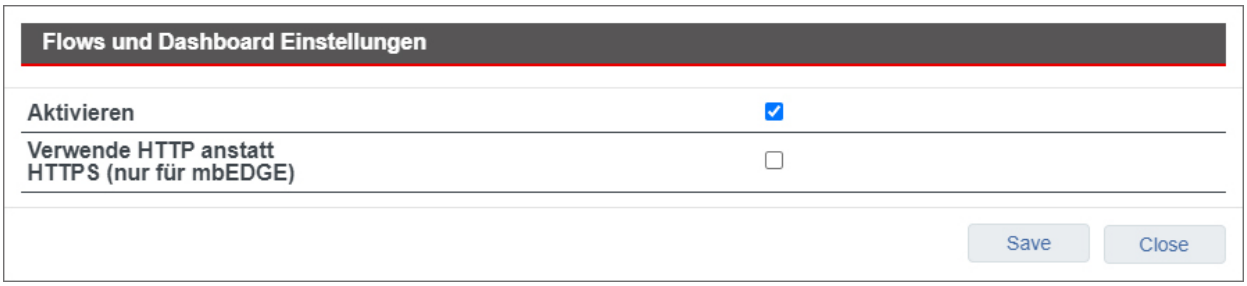
28.2.4 Flows and Dashboard

28.2.4.1 Activate flows and dashboard

- Click on the edit icon to activate the Flows and Dashboard Service.



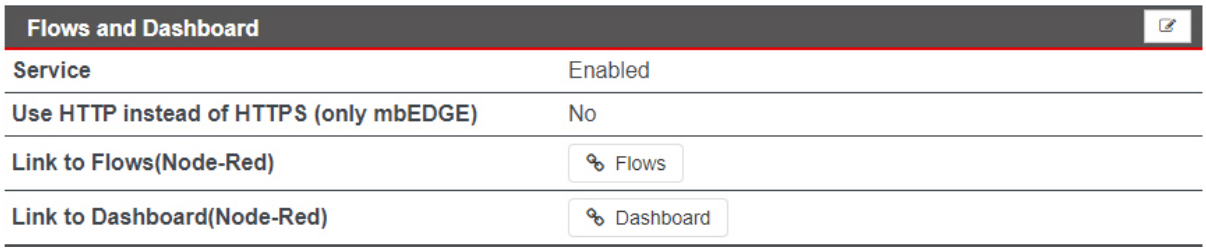
- Activate the flows and dashboard settings.
  Click on "Save" to save the change.



- 

  Confirm the activation by clicking on "Apply changes".

After activation, the links to "Flows(Node-Red)" and "Dashboard(Node-Red)" are activated.

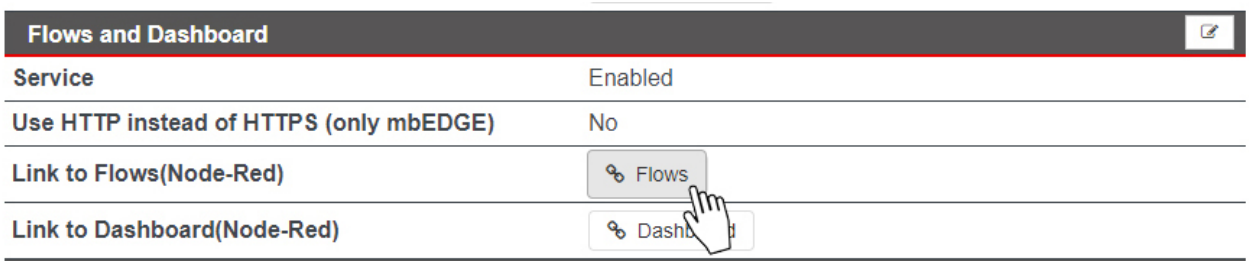


NOTICE

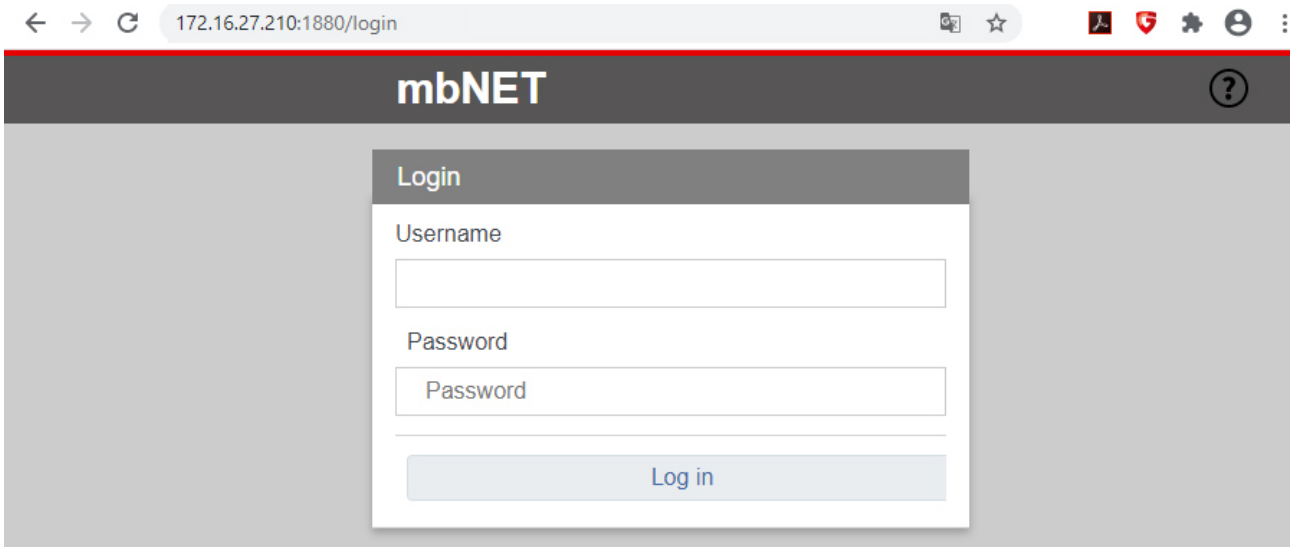
If you want to access the flows and dashboard via an unsecured HTTP connection, activate the checkbox "Use HTTP instead of HTTPS (only for mbEDGE)".

The unencrypted connection only applies to Flows and Dashboard and not to access to the mbNET GUI.

28.2.4.1.1 Link to Flows (Node-RED)



By clicking on the "Flows" button you will be redirected to Node-Red-Flows.



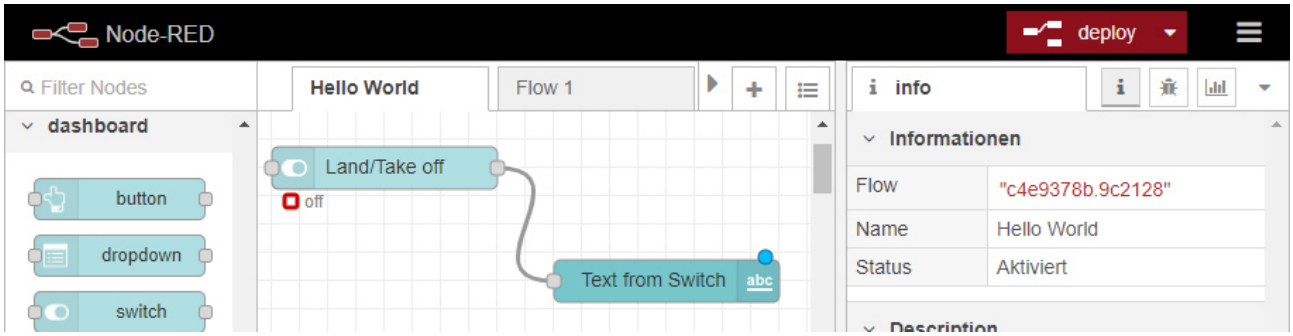
A new browser window, with a login, will open.

The access data for this are:

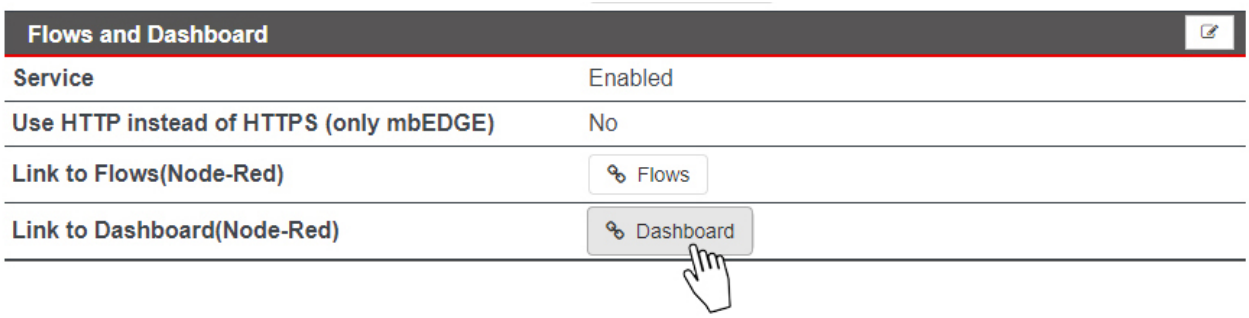
a) User name and password for the user you created in the user management for accessing Node-Red

or

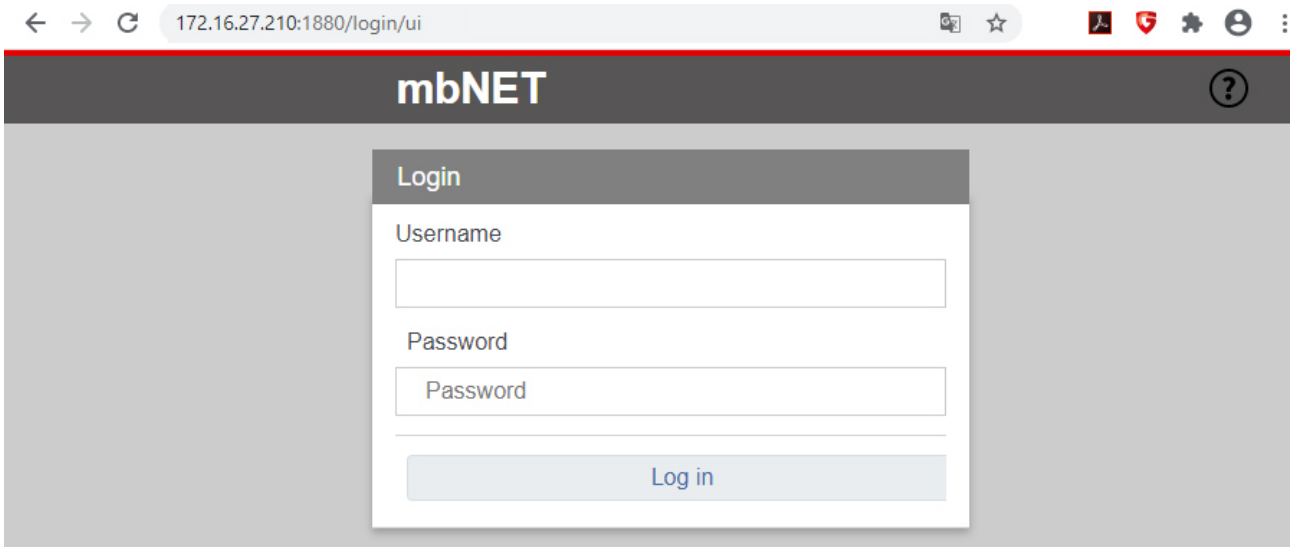
b) the current user data for the administrator (device access data)
standard user name = admin
standard password = the device password of the mbNET (see label on the back of the mbNET)



28.2.4.1.2 Link to Dashboard (Node-RED)



By clicking on the "Dashboard" button you will be redirected to Node-Red-Flows.



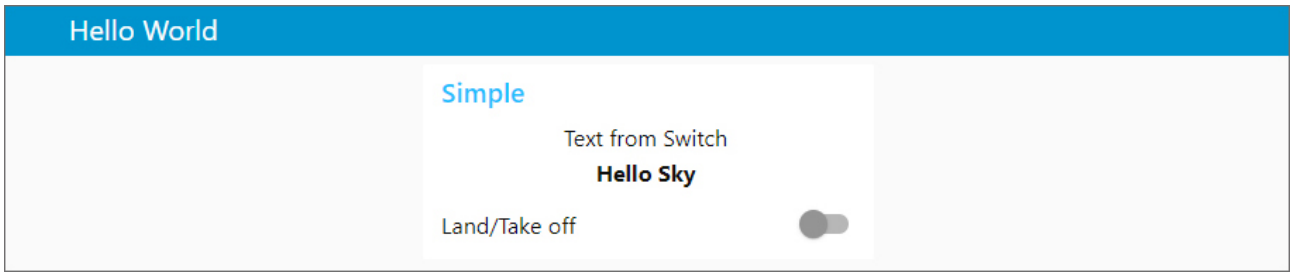
A new browser window, with a login, will open.

The access data for this are:

a) User name and password for the user you created in the user management for accessing Node-Red

or

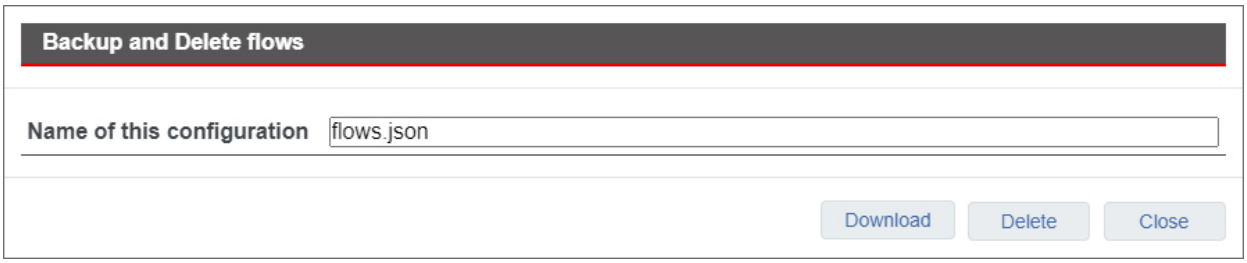
b) the current user data for the administrator (device access data)
standard user name = admin
standard password = the device password of the mbNET (see label on the back of the mbNET)



28.2.5 Backup and Delete flows

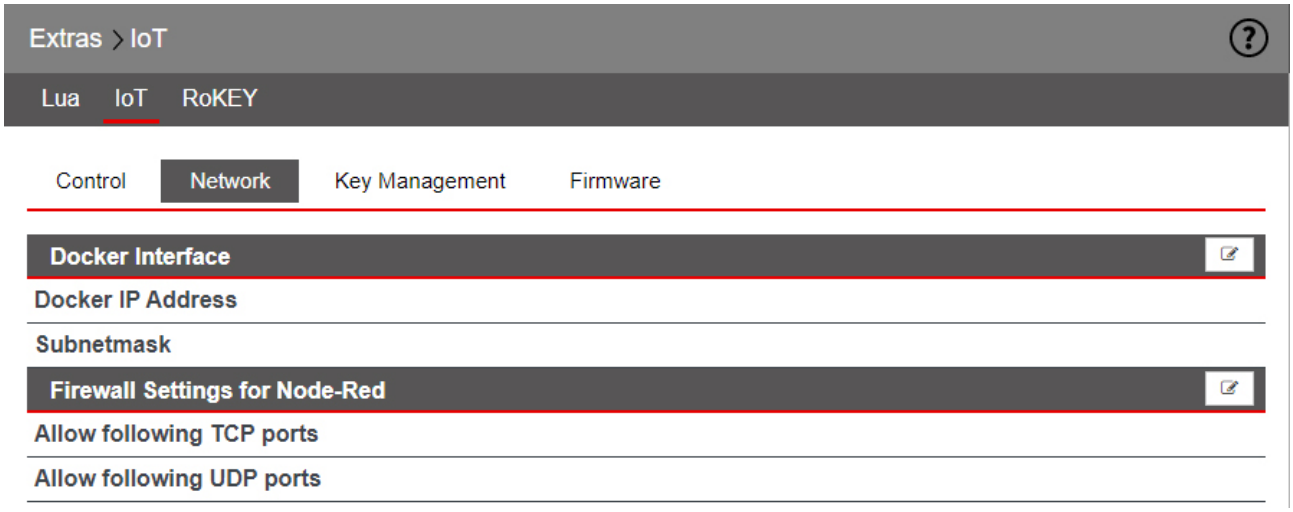
Here you can save and / or delete the flows you have created.
Saved flows can be read in again via Node-Red.

- Click the edit icon.



- Choose an option (Download or Delete)

28.3 Network



- **Docker Interface**
  Adjust the IP address of the Docker Daemon (runtimer for the IoT services and Nod-Red) if an address conflict with other network settings exists / is to be expected.
  The default setting is 172.16.0.1/24

- **Firewall Settings for Node-Red**
  Here, you add firewall rules to open ports for Node-RED.

  By default, a network socket node in Node-RED has access only from the inside out. Therefore, any "listener socket" created in Node- RED is not accessible via LAN / WAN. For example, an OPC UA server can not be reached via LAN / WAN. Unless you release the OPCUA server port here in a fire-wall rule.

- Enter the port number(s) that you want to enable.

NOTICE

Multiple entries of port numbers must be separated by commas.

▶ Apply changes

Confirm the changes by clicking on "Apply changes".

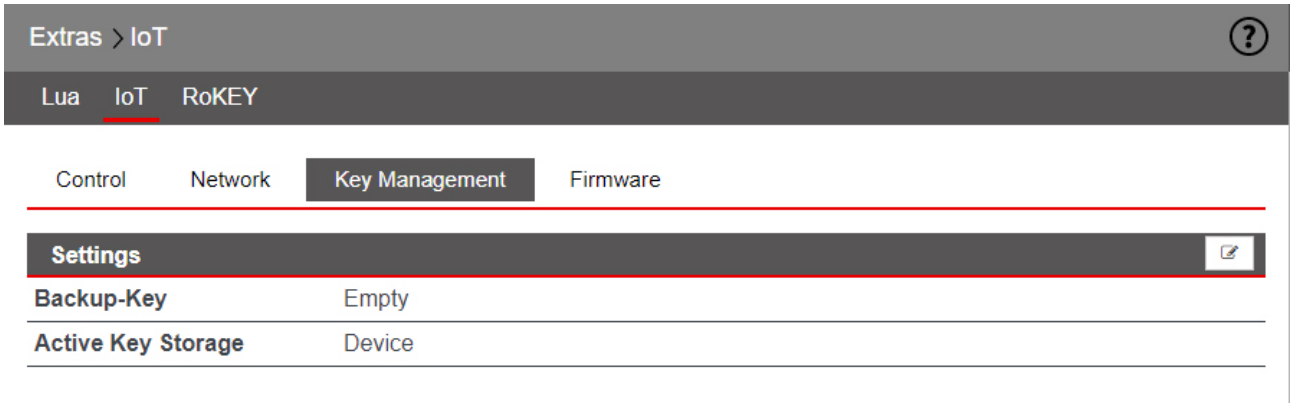
28.4 Key Management

Only the mbNET with which an mbEDGE card is paired can open the encrypted container. So that you can access your data at any time - even if the mbNET is no longer available - a **Backup-Key** is required.

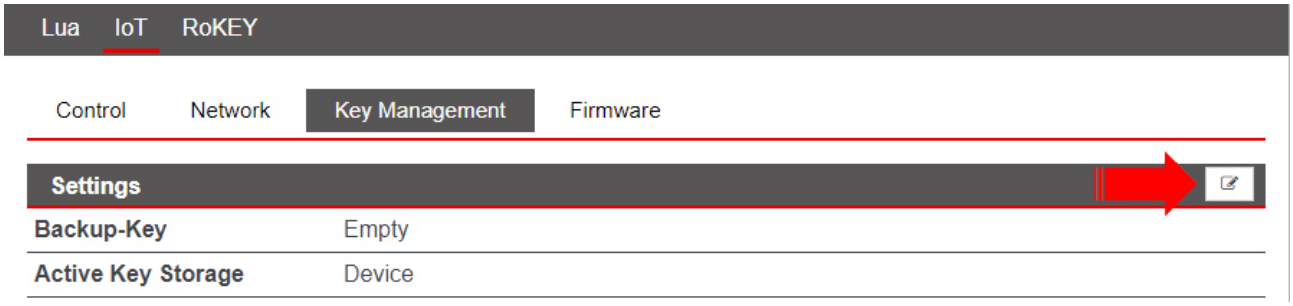
If the mbNET is no longer reachable before you have generated the Backup-Key (eg in the event of total failure due to damage), there is no way to access the card.

NOTICE

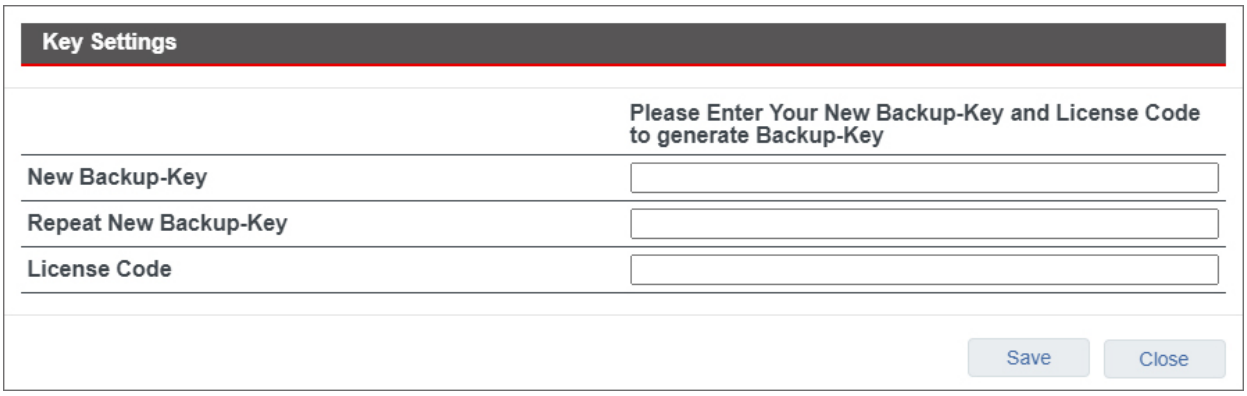
Immediately after initializing the mbEDGE card, assign a Backup-Key to avoid data loss!



28.4.1 Create Backup-Key

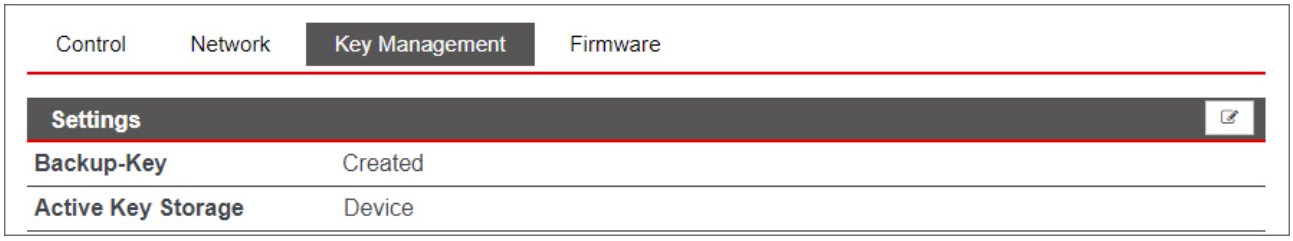


- Click on the edit icon in **Settings**.



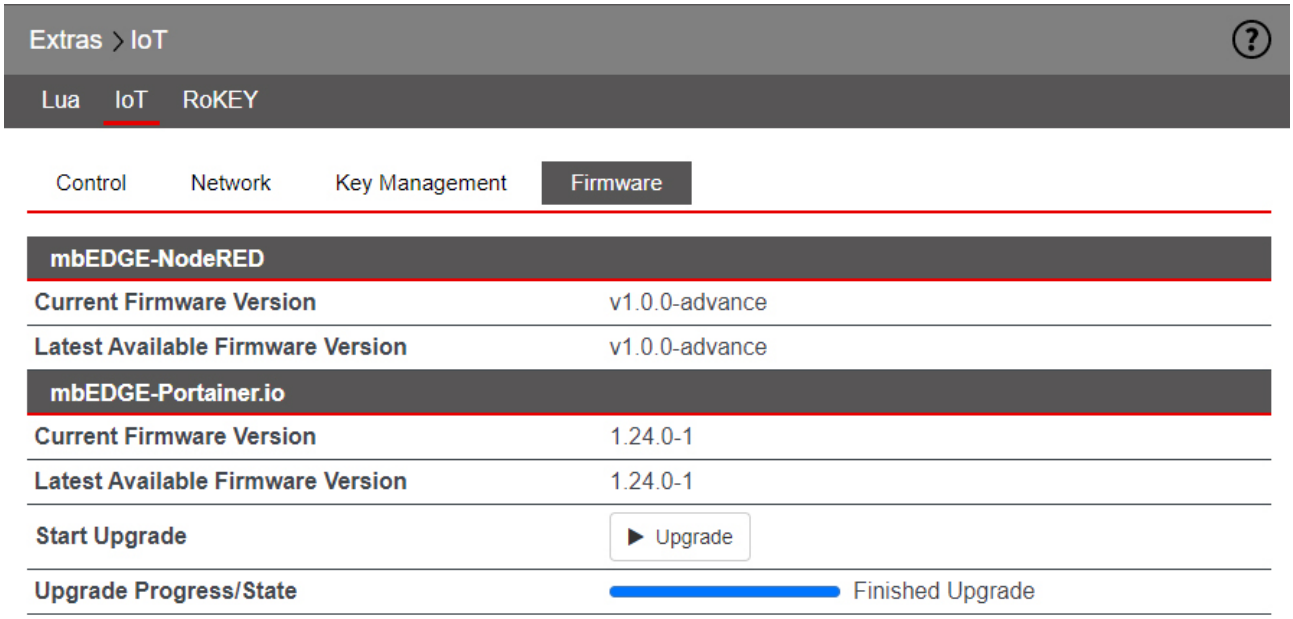
- Fill in the input fields under Key Settings.
  - The **Backup-Key** must consist of at least 8 characters.
  - You can find the **License Code** on the back of the mbEDGE packaging.
- Click on "Save"
- 

  Confirm the changes by clicking on "Apply changes".



After you have saved your entries, you can change or delete the Backup-Key.

28.5 Firmware



Under "Current Firmware Version" you can see

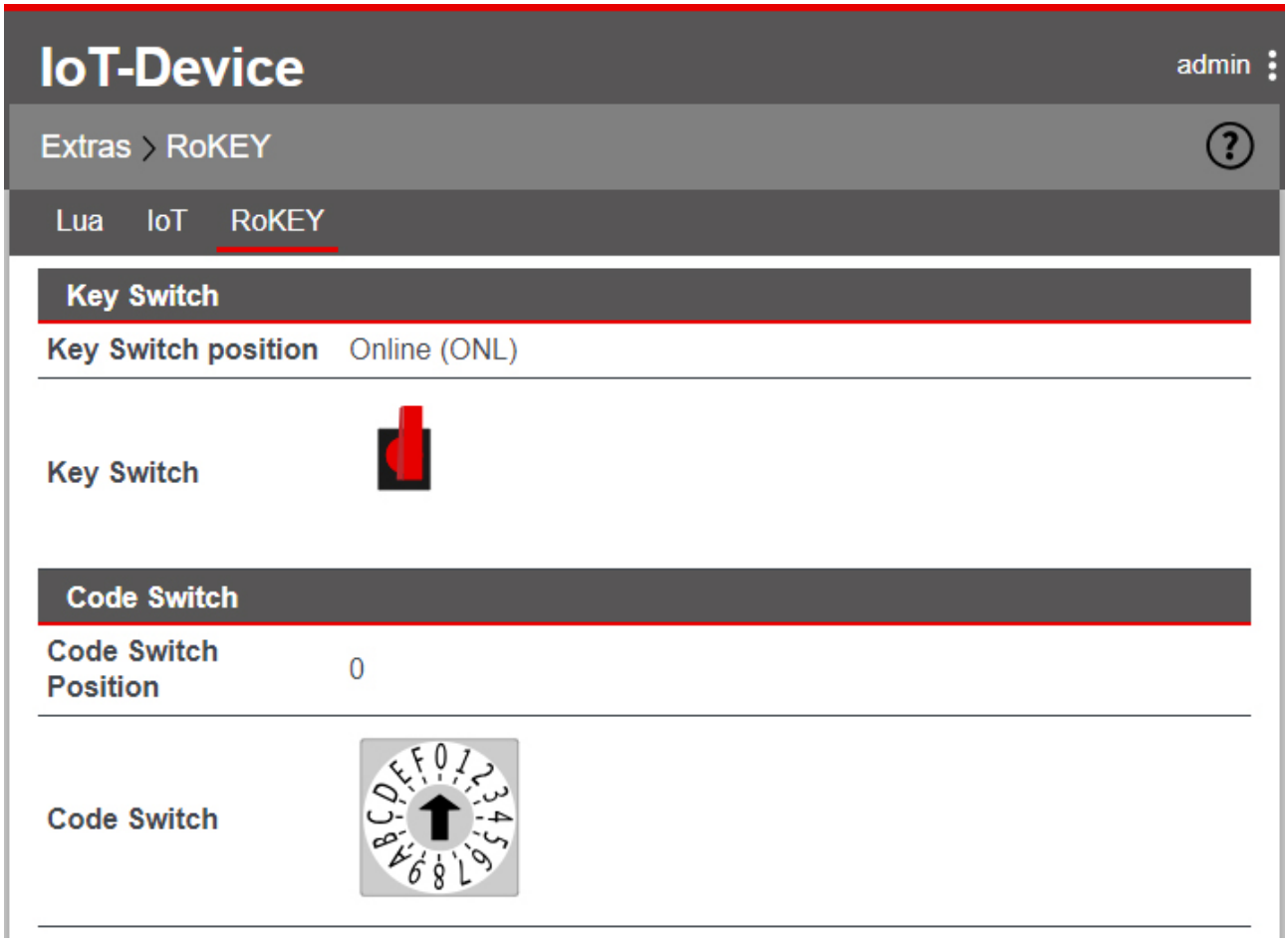
- the current firmware versions of
  - mbEDGE-NodeRED
  - mbEDGE-Portainer.io

The available firmware version is displayed under "Latest Available Firmware Version".

Requirement: The mbNET must be connected to the Internet.

▶ Click the "**Upgrade**" button to upgrade the firmware versions.

28.6 RoKEY



Key Switch position

Here, the current position of the ***mbNET.rokey*** key switch is displayed.

Switch position	Function
RST	Loading the factory settings
OFF	It is **not** possible to establish a VPN connection. Modem devices can not connect to the Internet.
ONL	It **can** be established a VPN connection. With modem devices an Internet connection can be established.
REM	It **can** be established a VPN connection. Including routing to the LAN side of the router. With modem devices an Internet connection **can** be established. Including routing to the LAN side of the router.

Code Switch Position

The coding switch is designed for future features, but **still without function**!

29 Status (information and analysis)

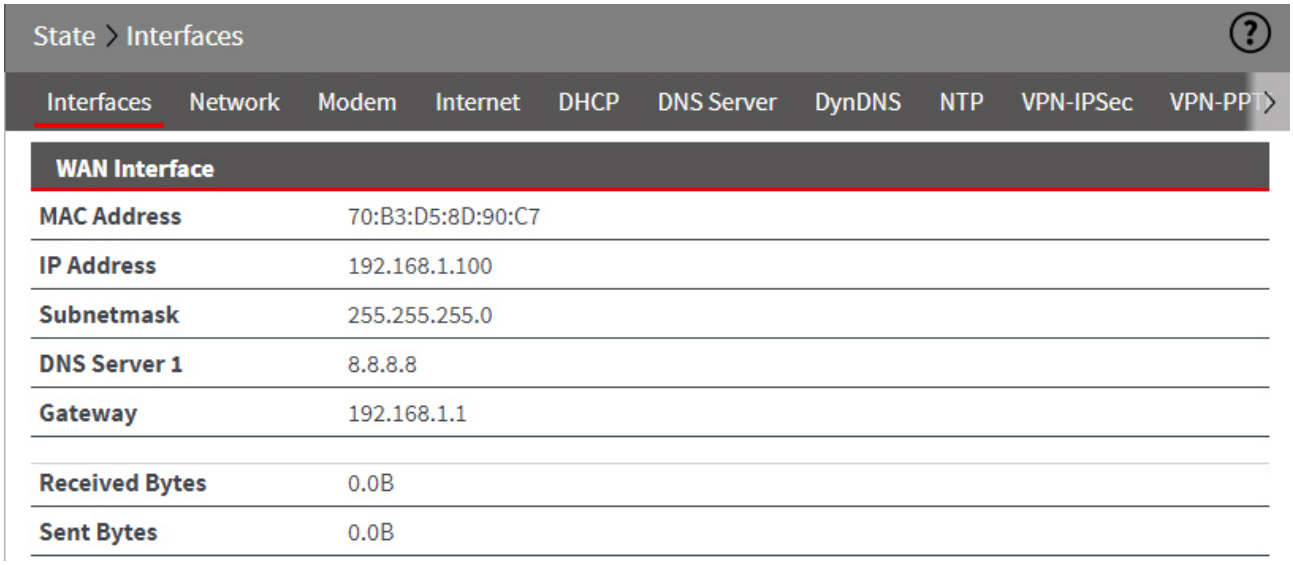
When errors/faults occur, these can be analysed on the basis of specific status information. Thus, for example, when the LED Stat (Status) is flashing, this indicates that a system error has occurred on the mbNET. For this purpose, e.g. via **Status > System** based on the listing it may be possible to determine the cause of the problem.

NOTICE

The display of the individual functions/submenus depends on the mbNET type and can vary.

29.1 Status > Interfaces

WAN interfaces



Designation	Description
MAC address	Display of the settings on the WAN connection (external connection) of the mbNET. As soon as the mbNET has a physical connection to the network, or the mbNET is assigned a static IP address, the IP address is displayed.
IP address	
Subnet mask	
DNS Server 1	
Gateway	
Bytes Received	Display the volume of data in received and sent data packets.
Sent Bytes	

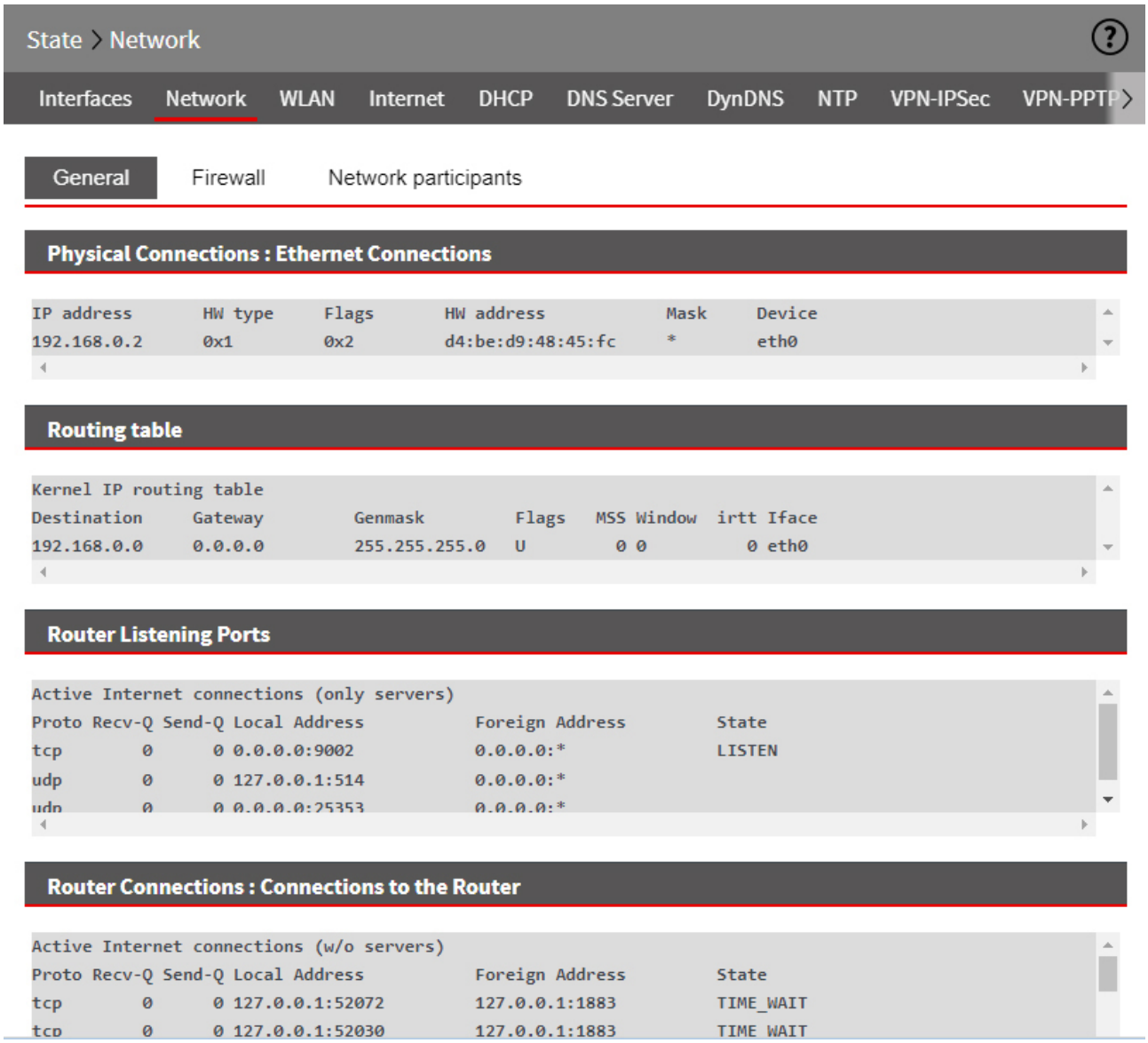
LAN interfaces

LAN Interface	
MAC Address	70:B3:D5:8D:90:C6
IP Address	192.168.0.155
Subnetmask	255.255.255.0
Received Bytes	3.7MiB
Sent Bytes	5.5MiB

Designation	Description
MAC address	Display of the settings on the LAN connection (local connection) of the mbNET. The IP address is then displayed if the mbNET has a physical connection.
IP address	
Subnet mask	
Bytes Received	Display the volume of data in received and sent data packets.
Sent Bytes	

29.2 Status > Network

29.2.1 General



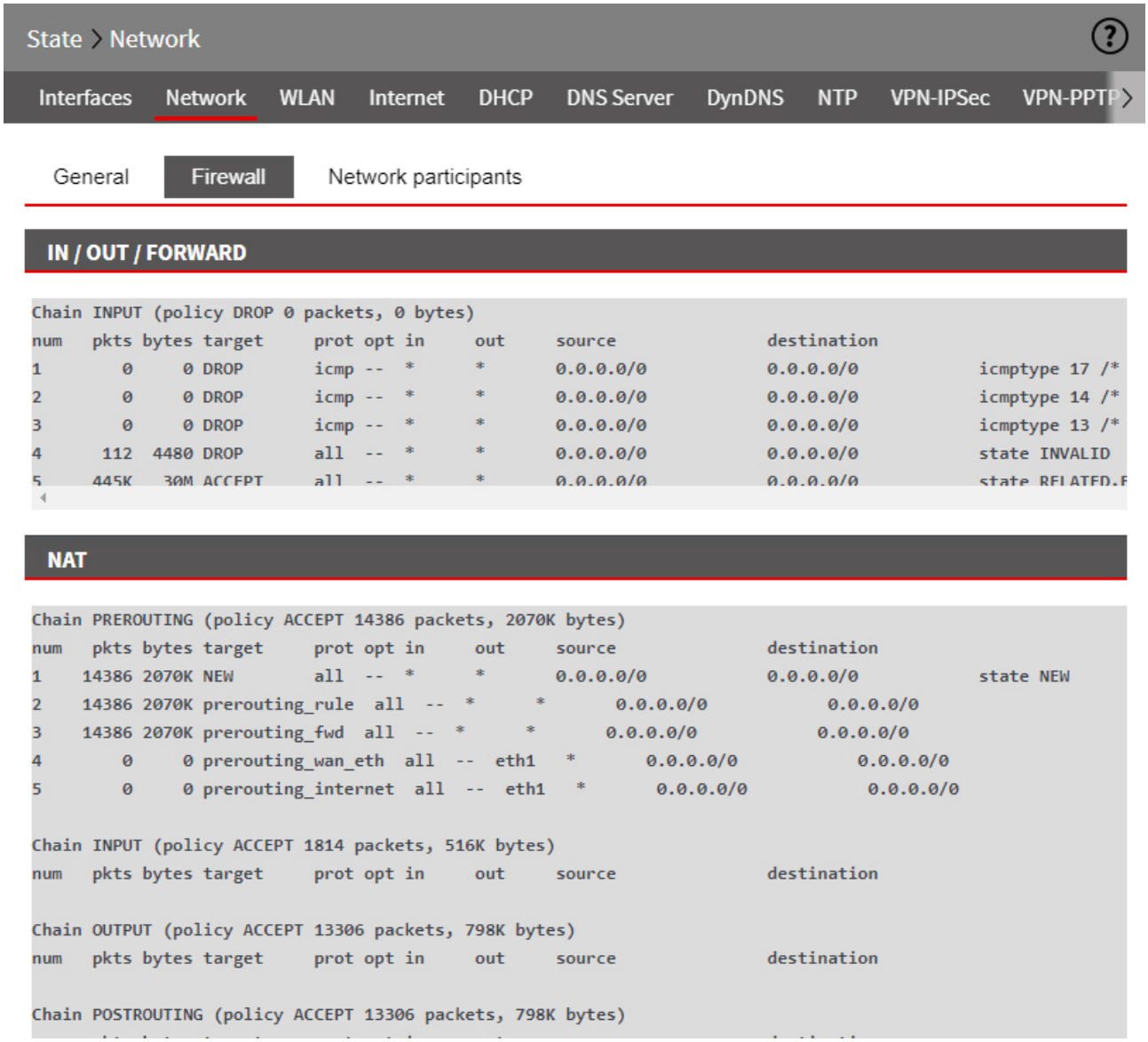
Physical connections: Ethernet connections
Displays the physical connections used to connect the router to other computers.

Route table
Displays all routes used.

Router monitored ports
Displays all monitored ports.

Router connections: Connections to the router
Displays all IP addresses of ports, such as of computers that are connected to the router.

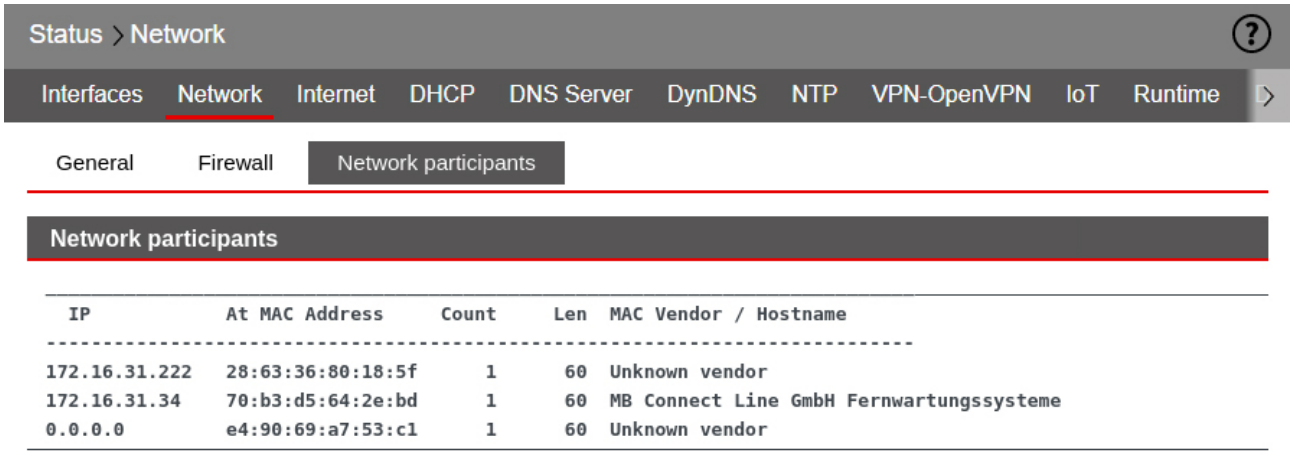
29.2.2 Firewall



IN/OUT/FORWARD
Displays incoming and outgoing data traffic as well as forwarding.

NAT
Displays natted data traffic.

29.2.3 Network participants

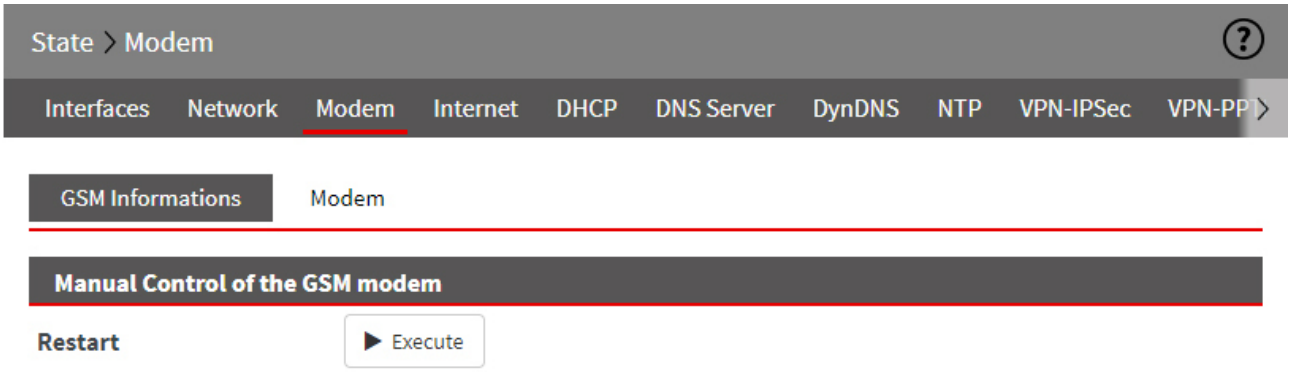


The LAN network participants that have been recognized via ARP reconnaissance are listed here.

29.3 Status > Modem

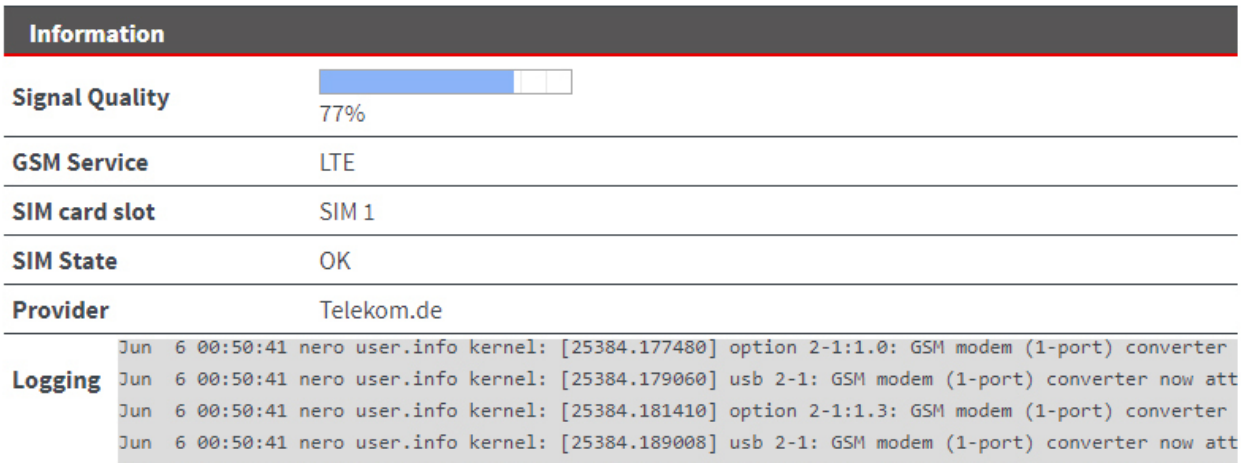
29.3.1 GSM information

Manual control of the GSM modem



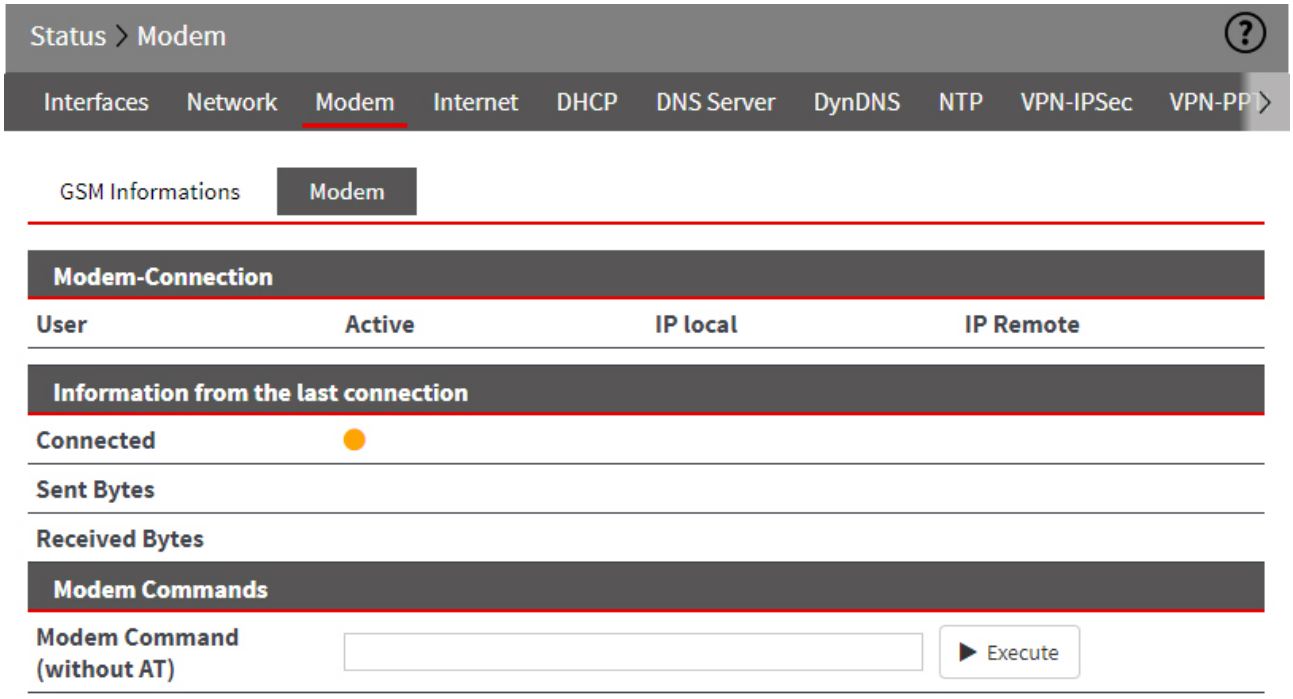
Reboot	Here you can click on the "Execute" button to restart the GSM modem.

Information



Designation	Description
Signal strength	Signal strength display (in %)
GSM transfer procedure	Display of the transfer procedure, depending on the type of modem, signal strength etc.
SIM card slot	Display of the active SIM card slot
SIM Status	Status of detected SIM Card
Provider	Displays the wireless service provider
Logging	All the events and errors of the GSM modems are listed here.

29.3.2 Modem



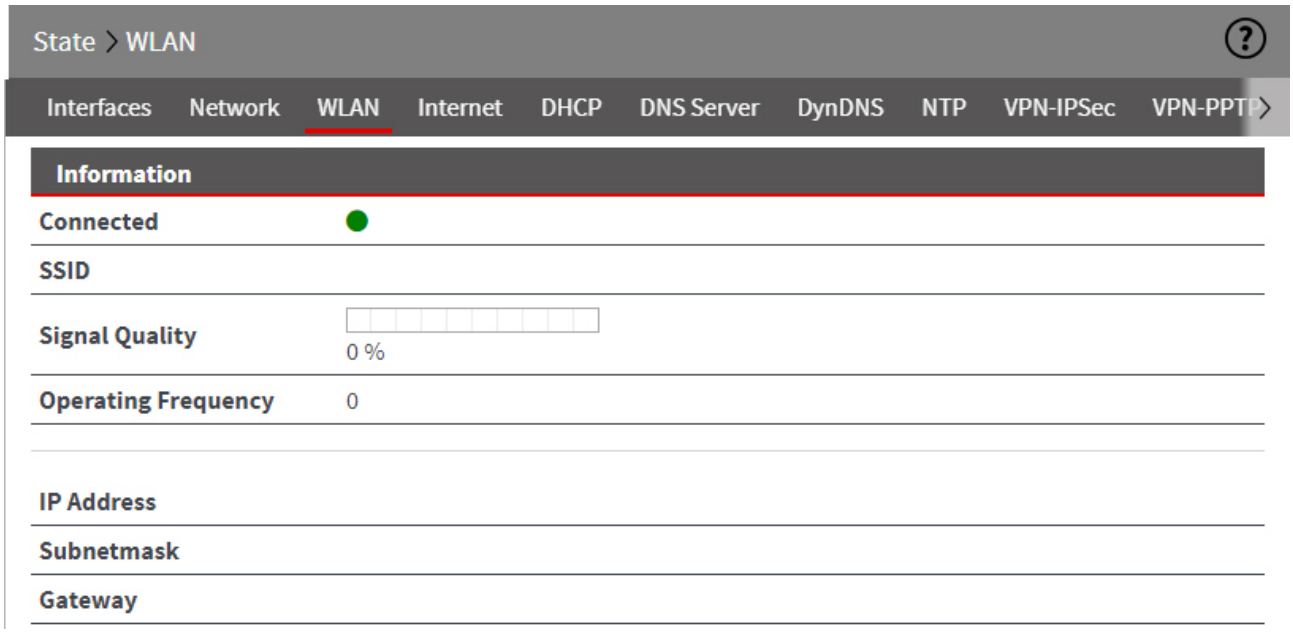
Modem Connection
Here, you can see which user has dialled in to the router via a modem. When the dial-up connection is successful, the IP address of the PPP server and the PPP client (remote) are displayed. This is always incoming connections. An active connection is symbolized by a solid green circle.

Information about the last connection	
Connected	An active connection is symbolized by a solid green circle.
Sent Bytes **Bytes Received**	Displays the connection time and the number of bytes sent and received in the last connection, as long as the router is not restarted or switched off in the meantime.

Modem command	
NOTICE	
Use this function only as instructed by the MB connect line support staff!	
Modem command (without AT)	Enter here the modem command and click on the "**Execute**" button.

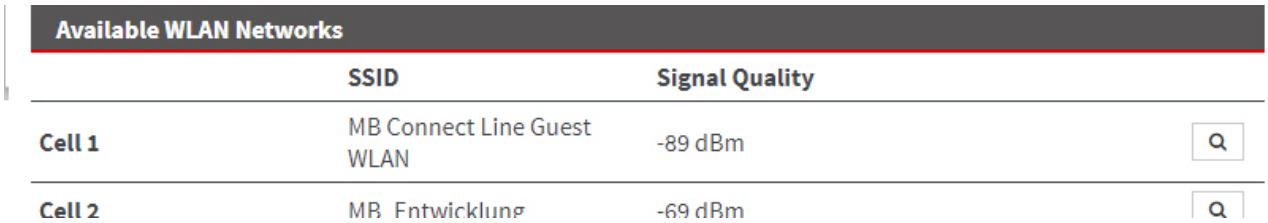
29.4 Wi-Fi

Information



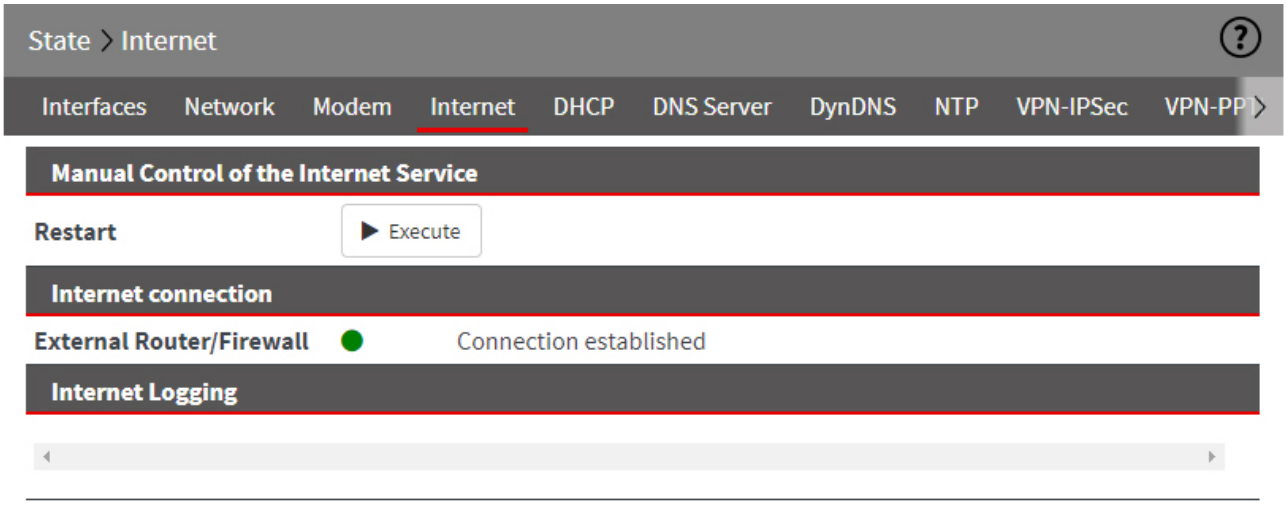
Designation	Description
Connected	Display of the connection status via an LED symbol
SSID	Display Wi-Fi Network Names
Signal strength	Signal strength display (in %)
Operating frequency	Operating frequency display
IP address	Displays the settings on the Wi-FiL connection (local connection) of the router. The IP address is displayed if the router has a physical connection.
Subnet mask	
Gateway	

Available Wi-Fi networks



Available networks are listed here.

29.5 Internet



Manual control of the dial-up Internet service

Here you can click on the "**Execute**" button to manually restart the Internet dial-up service and thus disconnect to enforce a new dial.

NOTICE

Use this function only as instructed by the MB connect line support staff!

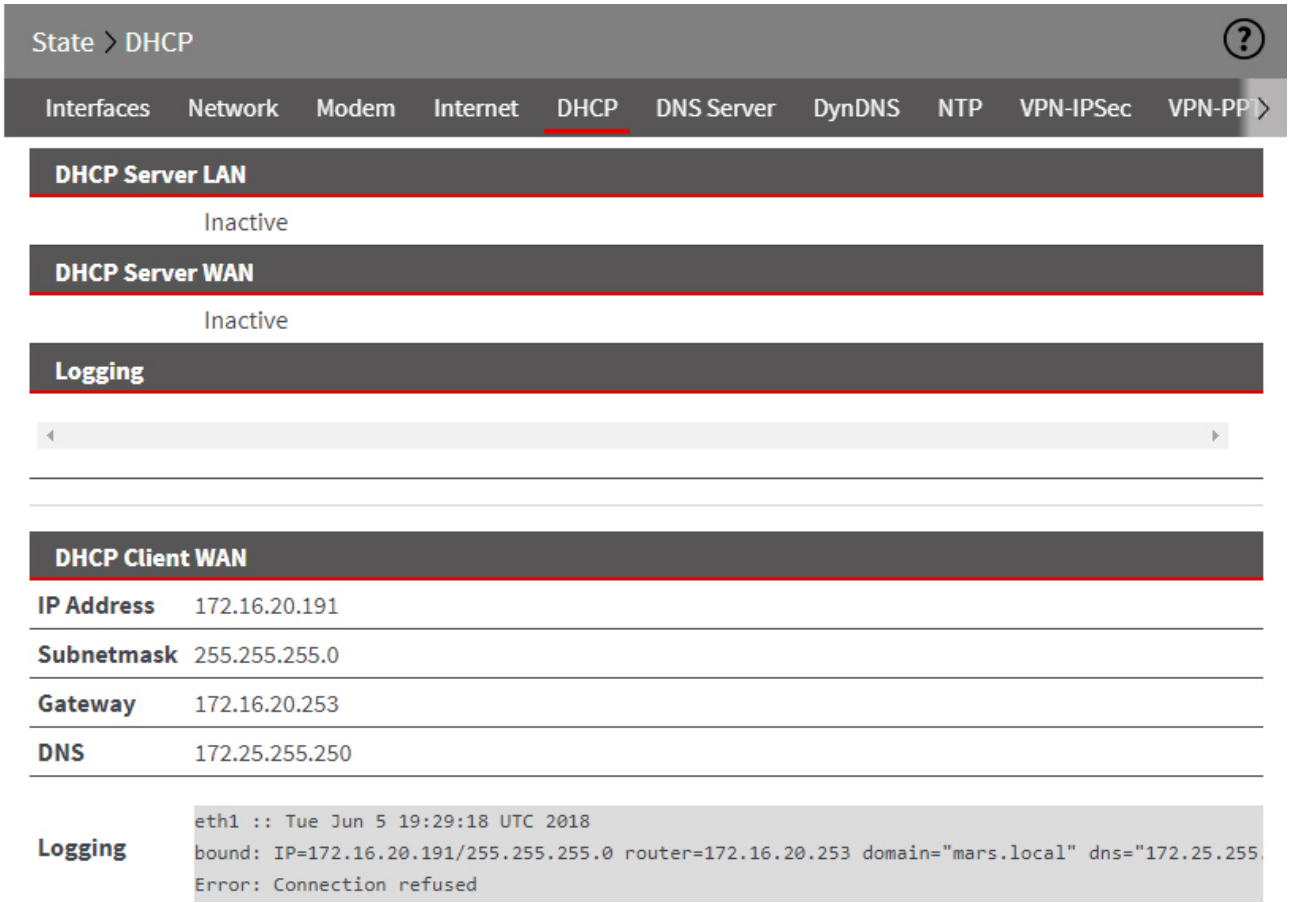
Internet access

This displays outgoing connections to the Internet. This can be both outgoing connections via the modem as well as connections over WAN.
An active connection is symbolized by a solid green circle.

Internet logging

Error messages regarding the internet connection will be listed here.

29.6 DHCP



DHCP Server LAN
Displays the IP addresses that the DHCP server assigns to connected clients.

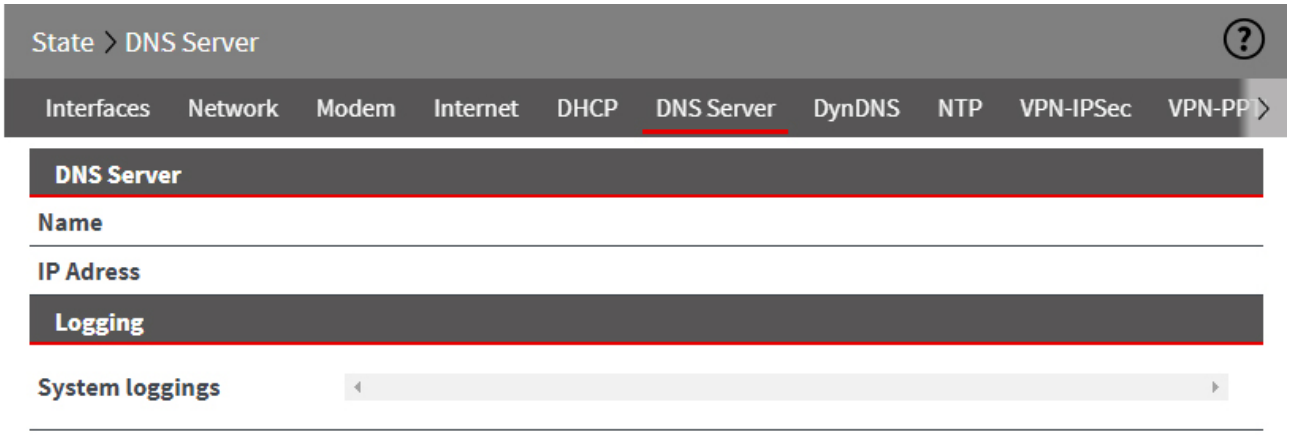
DHCP Server WAN
Displays the IP addresses that the DHCP server assigns to connected clients.

Logging
Displays the IP addresses that the DHCP assigns and which IP addresses are not allowed.

DHCP Client WAN
Information about clients connected via the WAN connection.

Logging
All the events and errors of the DHCP server and DHCP client are logged here.

29.7 DNS Server



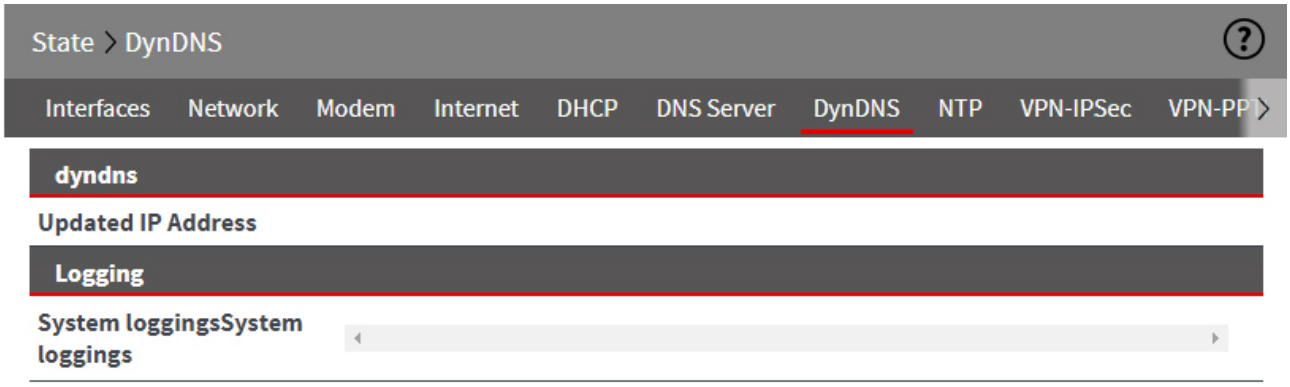
DNS Server

Designation	Description
Name	Displays the name of the DNS server (if not assigned by the Internet Service Provider).
IP address	Displays the IP address of the DNS server (if not assigned by the Internet Service Provider).

Logging

Designation	Description
System Logging	Display of the work steps executed by the DNS server.

29.8 DynDNS



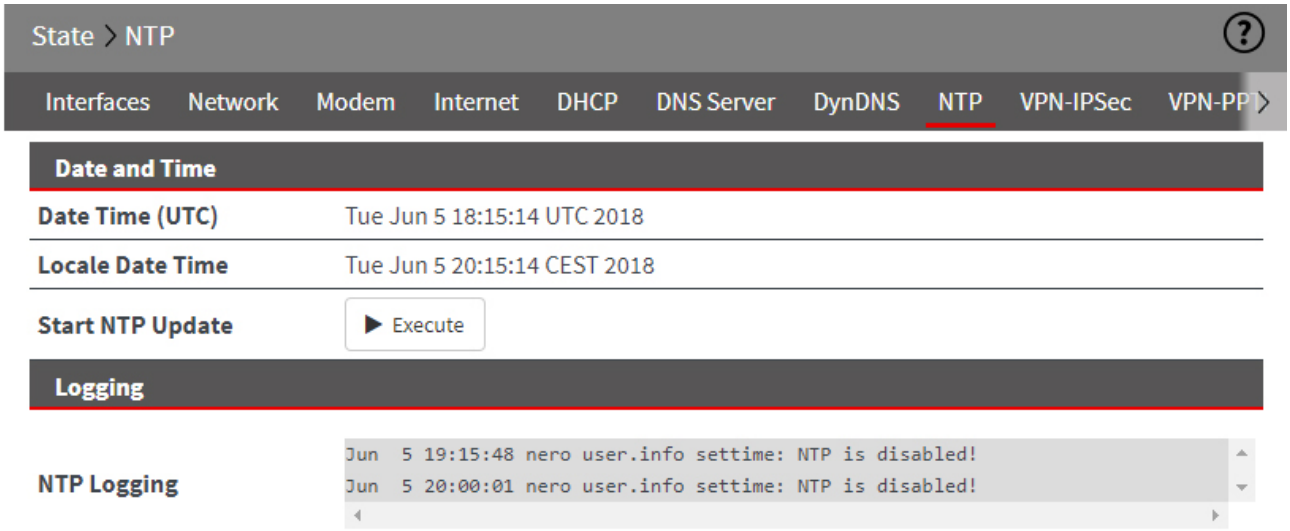
DynDNS

Designation	Description
Updated IP-address	Displays the current IP address that is assigned to the mbNET via the Internet.

Logging

Designation	Description
System Logging	Here all events and errors relating to the DynDNS service are displayed.

29.9 NTP



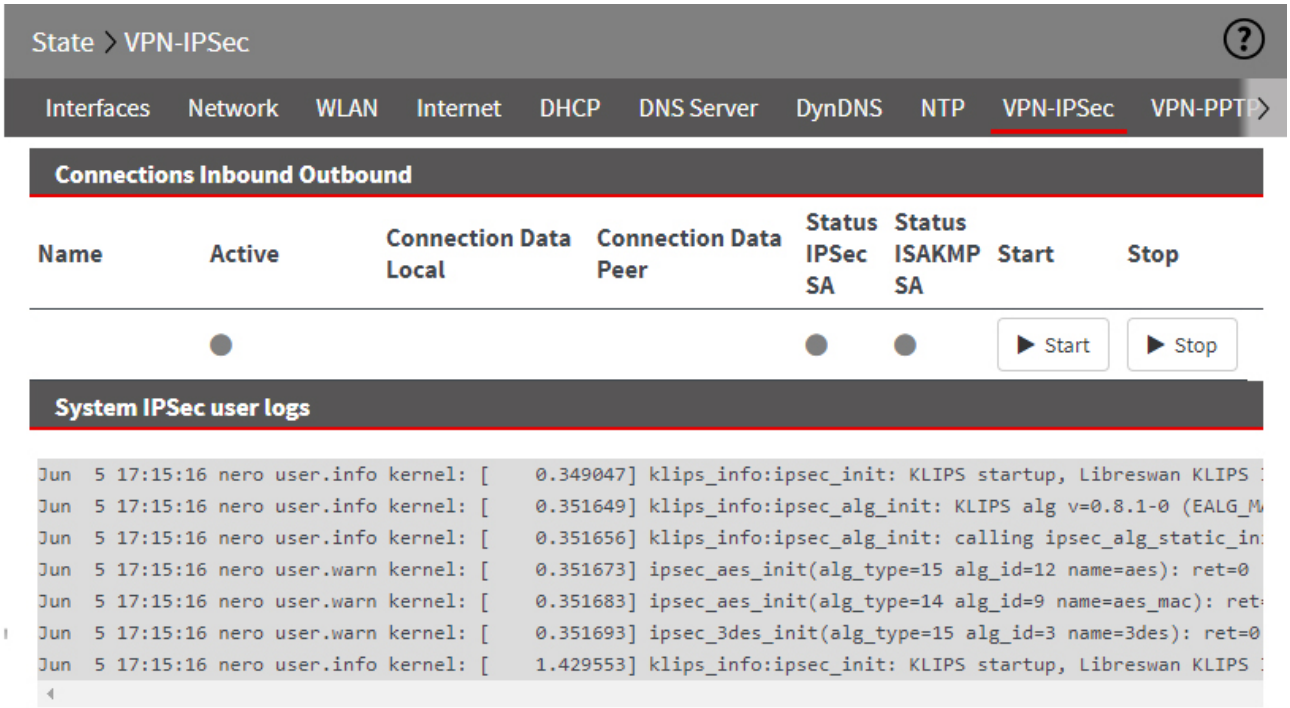
Date and time

Designation	Description
Date/Time (UTC)	Displays the current system time in Universal Time Coordinates (UTC).
Local date/time	
Time update	Clicking on the "**Execute**" button, synchronises the time with the NTP server stored and activated under **System > Settings > Time Settings**.

Logging

Designation	Description
NTP logging	All notifications and error messages of the service are displayed here.

29.10 VPN-IPSec



Incoming/outgoing connections

Both the incoming and the outgoing VPN connections of the router are displayed here.

An active connection is indicated by a green LED icon .

The duration of the connection and the dialled-in user are displayed.

After disconnection, the time during which the corresponding connection was active is displayed.

By clicking on the "Start" or "Stop" button, you can manually start or stop a connection.

NOTICE

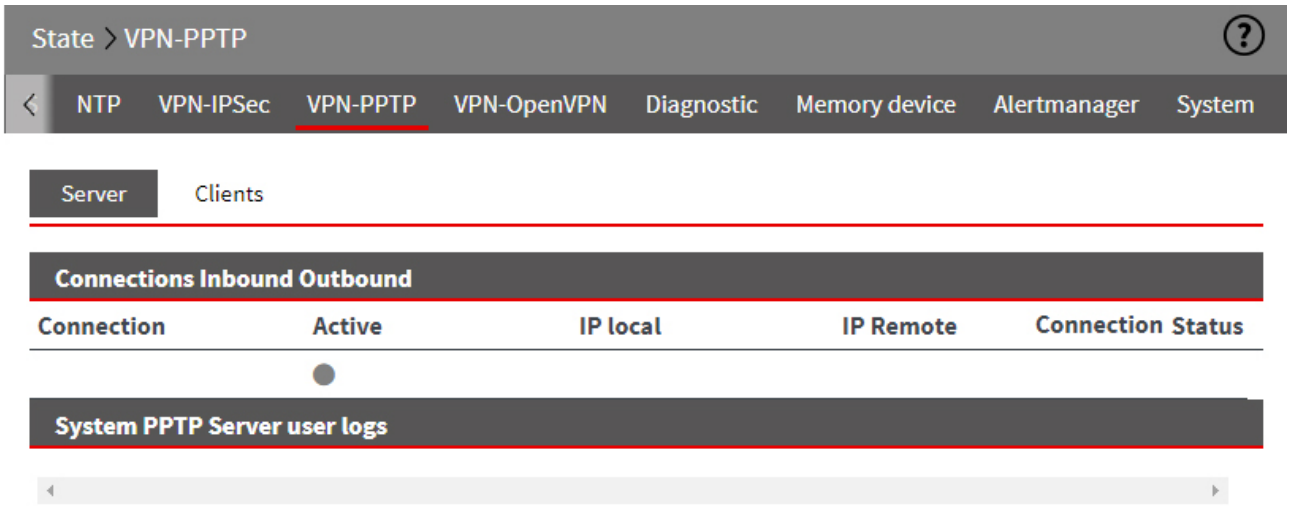
Use this function only as instructed by the MB connect line support staff!

System logging: Connection

The connection protocol is displayed here.

29.11 VPN-PPTP

29.11.1 VPN PPTP server



Incoming/outgoing connections

The incoming VPN connections of the mbNET are listed here.

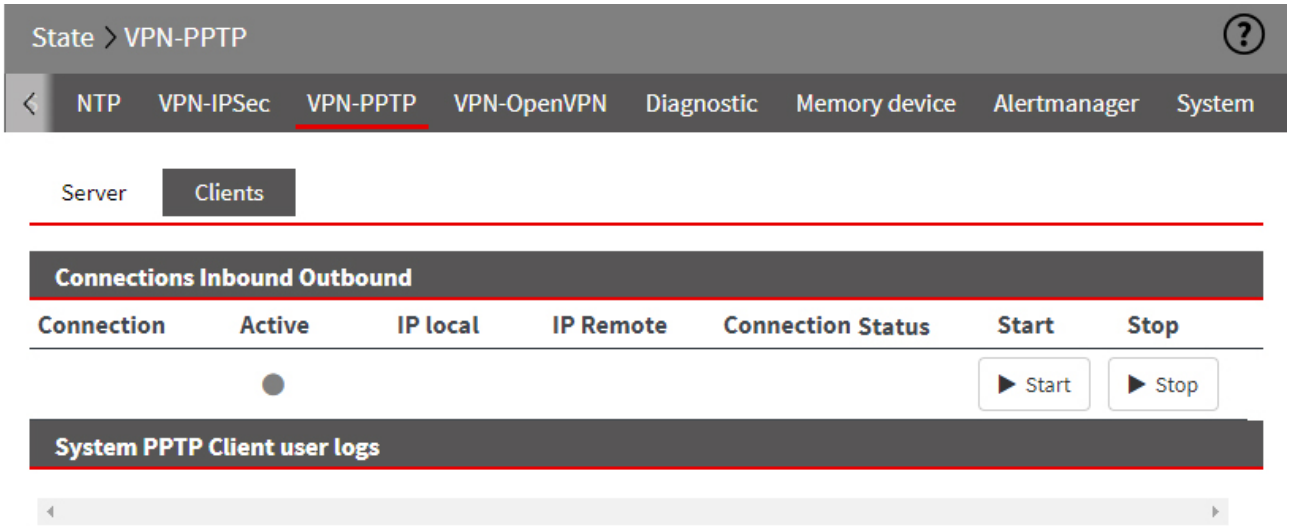
An active connection is indicated by a green LED icon .

The connection time, users dialled-in, local and remote IP address is displayed.
After disconnection, you can see the time during which the corresponding connection was active.

System logging: Connection

All notifications and error messages of the PPTP service are displayed here.

29.11.2 VPN PPTP clients



Incoming/outgoing connections

Outgoing VPN connections from the mbNET are displayed here.

An active connection is indicated by a green LED icon .

The connection time, users dialled-in, local and remote IP address is displayed.
After disconnection, you can see the time during which the corresponding connection was active.

By clicking on the "Start" or "Stop" button, you can manually start or stop a connection.

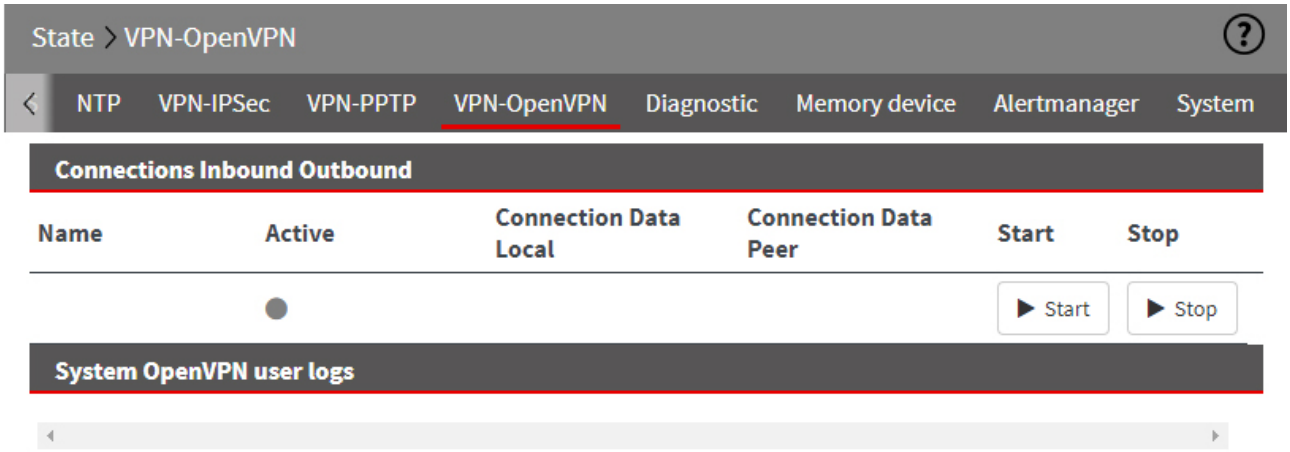
NOTICE

Use this function only as instructed by the MB connect line support staff!

System logging: Connection

All notifications and error messages of the PPTP service are displayed here.

29.12 VPN-OpenVPN



Incoming/outgoing connections

Both the incoming and the outgoing VPN connections of the mbNET are displayed here.

An active connection is indicated by a green LED icon .

Name, local addresses and partner addresses are displayed here.

By clicking on the "Start" or "Stop" button, you can manually start or stop a connection.

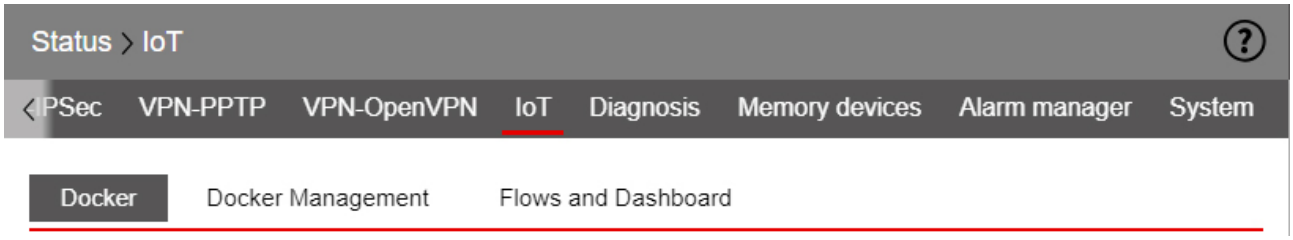
NOTICE

Use this function only as instructed by the MB connect line support staff!

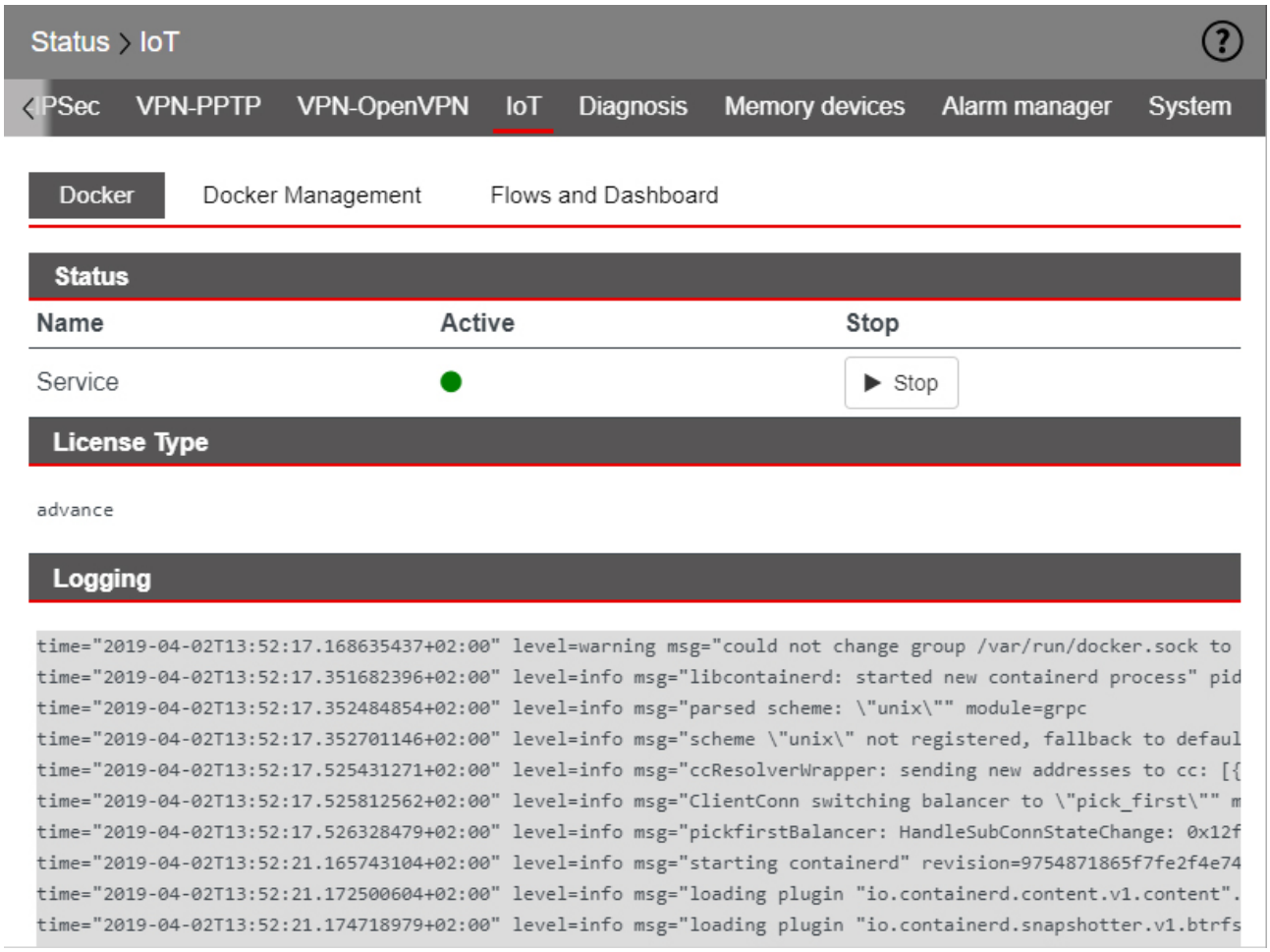
System logging: Connection

The connection protocol is displayed here.

29.13 IoT



29.13.1 IoT > Docker



Here you can see:

- The **Status** of your mbEDGE installation

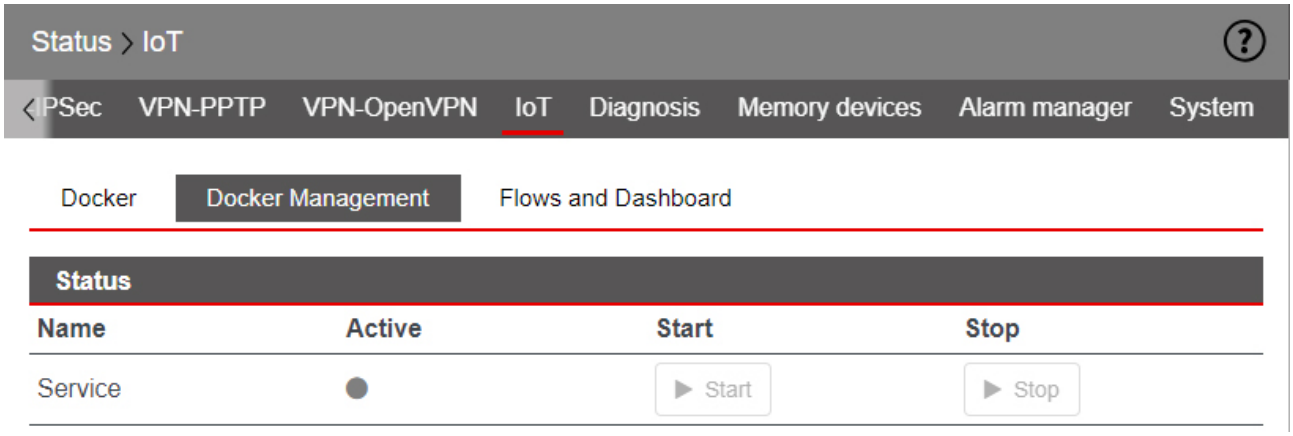
  - green LED icon= mbEDGE is active
  - gray LED icon = mbEDGE is not active

  By clicking on the "**Finish**" button mbEDGE is deactivated.
  Click on the "**Start**" button to reactivate mbEDGE.

- The **License Type**
  "**advanced**" or "**start**"

- The **Logging**

29.13.2 IoT > Docker Management



Here you can see

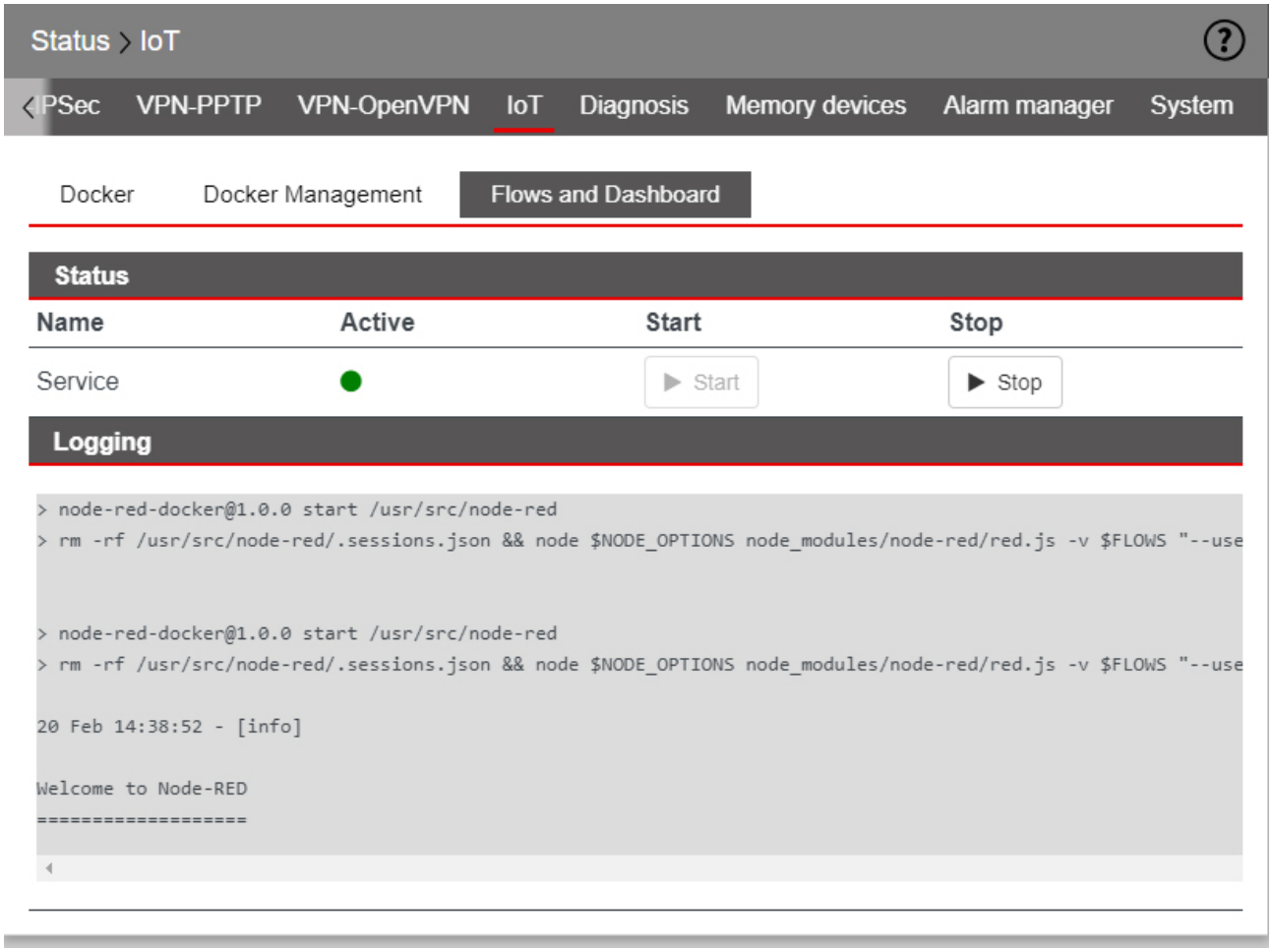
- the **Status** of Docker Management

  gray LED icon = Docker Management is **disabled**
  green LED icon= Docker Management is **activated**

  Click on the "**Start**" button to activate Docker Management.

  Click on the "**Stop**" button to deactivate Docker Management.

29.13.3 IoT > Flows and Dashboard



Here you can see

- the **Status** of accessing Flows and Dashboard.

  gray LED icon = Access to Flows and Dashboard is **disabled**.
  green LED icon= Access to Flows and Dashboard is **activated**.

  Click on the "**Start**" button to activate the access.

  Click on the "**Stop**" button to deactivate the access.

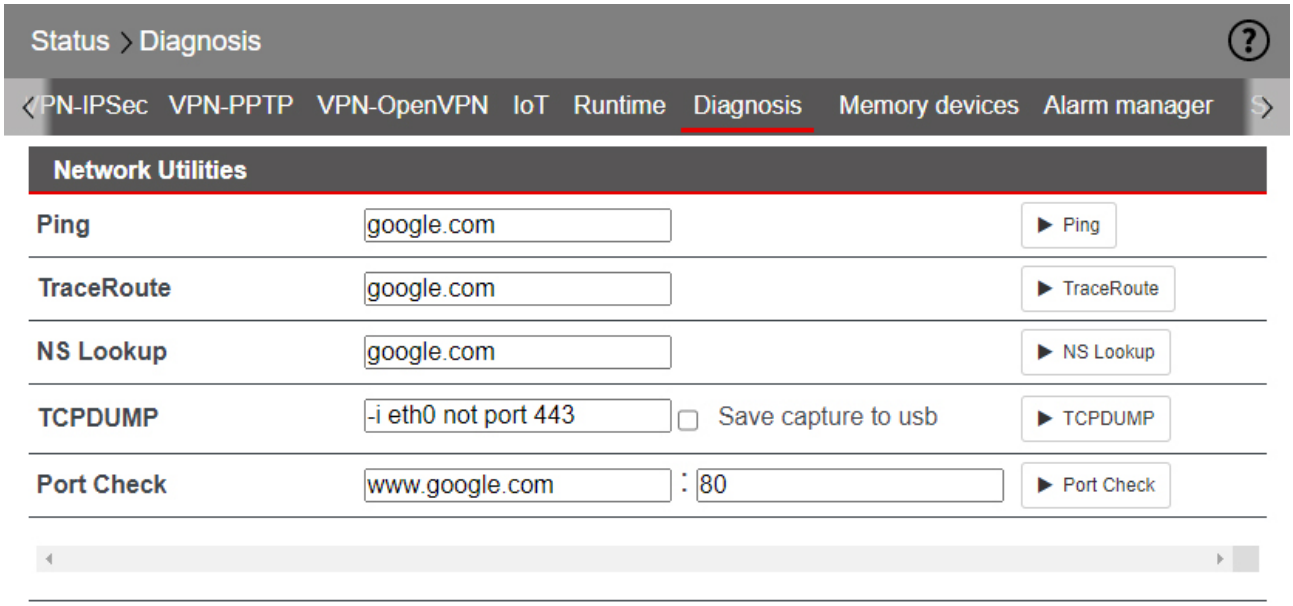
- The **Logging**

29.14 Runtime

NOTICE

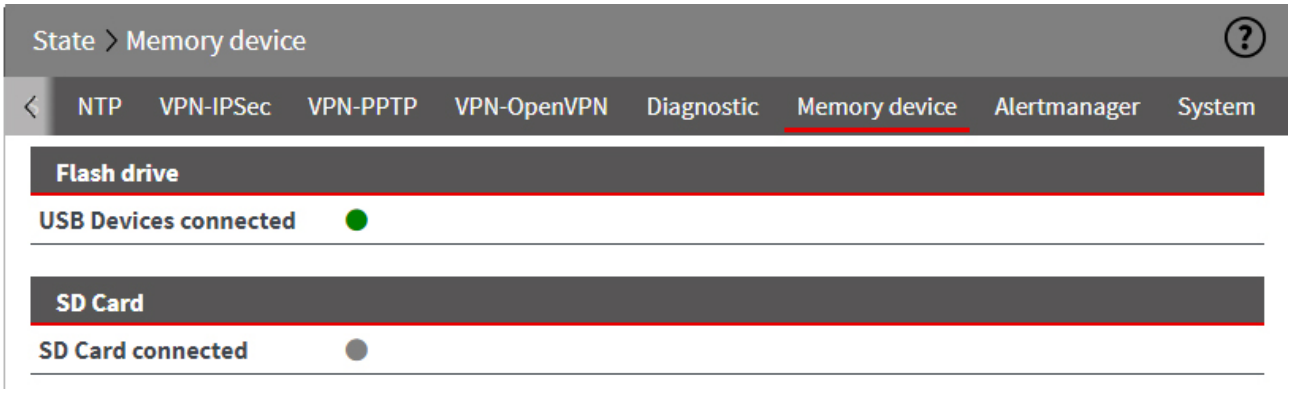
This function is only relevant if you operate the mbNET in the mbCONNECT24 portal.

29.15 Diagnostics - Network Resources



Designation	Description
Ping	After entering an internet address or an IP address, you can use the ping command (Click on the "**Ping**" button) to determine whether the corresponding address is accessible. Among other things, for example, you can easily determine whether an Internet connection exists.
Route monitoring	This command provides you with detailed information about the network connection between the mbNET and a remote host or other routers. Route monitoring is carried out and made visible here.
DNS names resolve (nslookup)	With this function, you can check whether name resolution (https://www.google.de = 216.58.209.206) takes place. If after executing the command “DNS name resolve(nslookup)” no result is output, check whether in your mbNET a DNS server address is entered under network-DNS, or if the DNS server of your network is accessible.
TCPDUMP	In order to closely monitor the network traffic, you can use the "**TCPDUMP**” command. Some examples of the use of this command are: • **-i eth0 not port 80** Displays all TCP/IP connections to the (-i) LAN (eth0) interface, except (not) those using Port 80 (port 80) when incoming or outgoing. • **-i eth1 port 23** Displays all TCP/IP connections to the (-i) WAN (eth1) interface using Port 23 (port 23) when incoming or outgoing. • **-vvv -i eth1** Displays all traffic in verbose mode, Level3 (-vvv) on the (-i) WAN (eth1) interface. You can find detailed TCPDUMP documentation at www.tcpdump.org
Port Check	You can use this function to check the status of a port (open / not open) in connection with an Internet or IP address.

29.16 Storage media

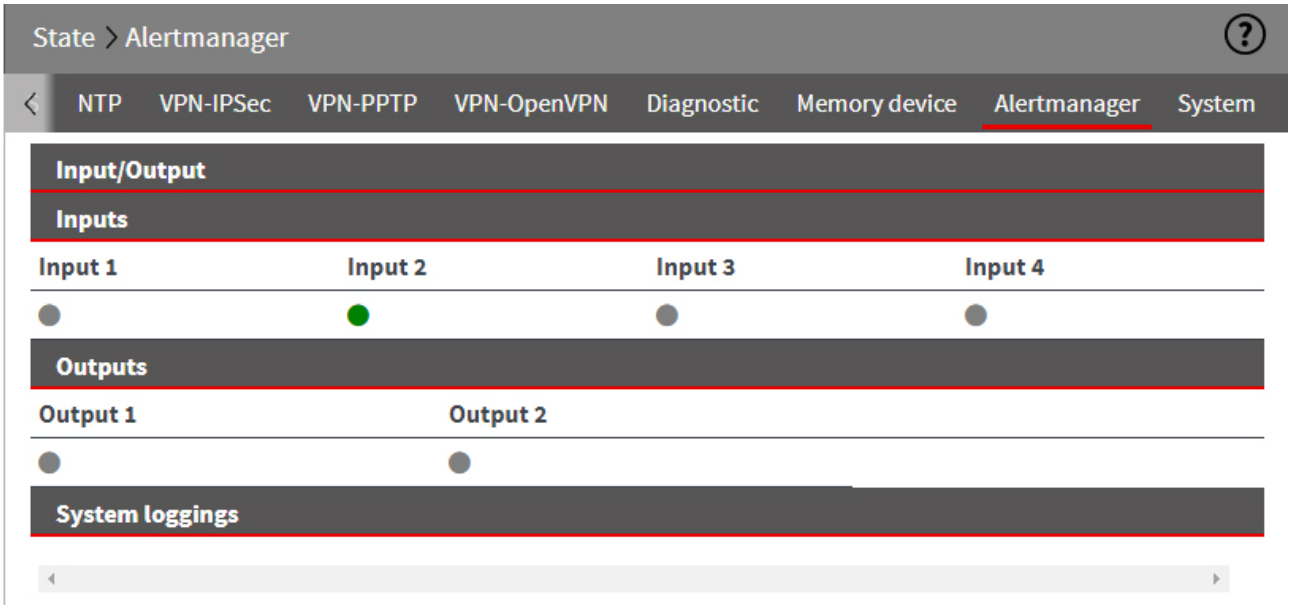


Status display showing whether a storage medium (USB stick or/and SC card) is connected to the mbNET.

green LED symbol = storage medium connected

Grey LED symbol = storage medium is not connected

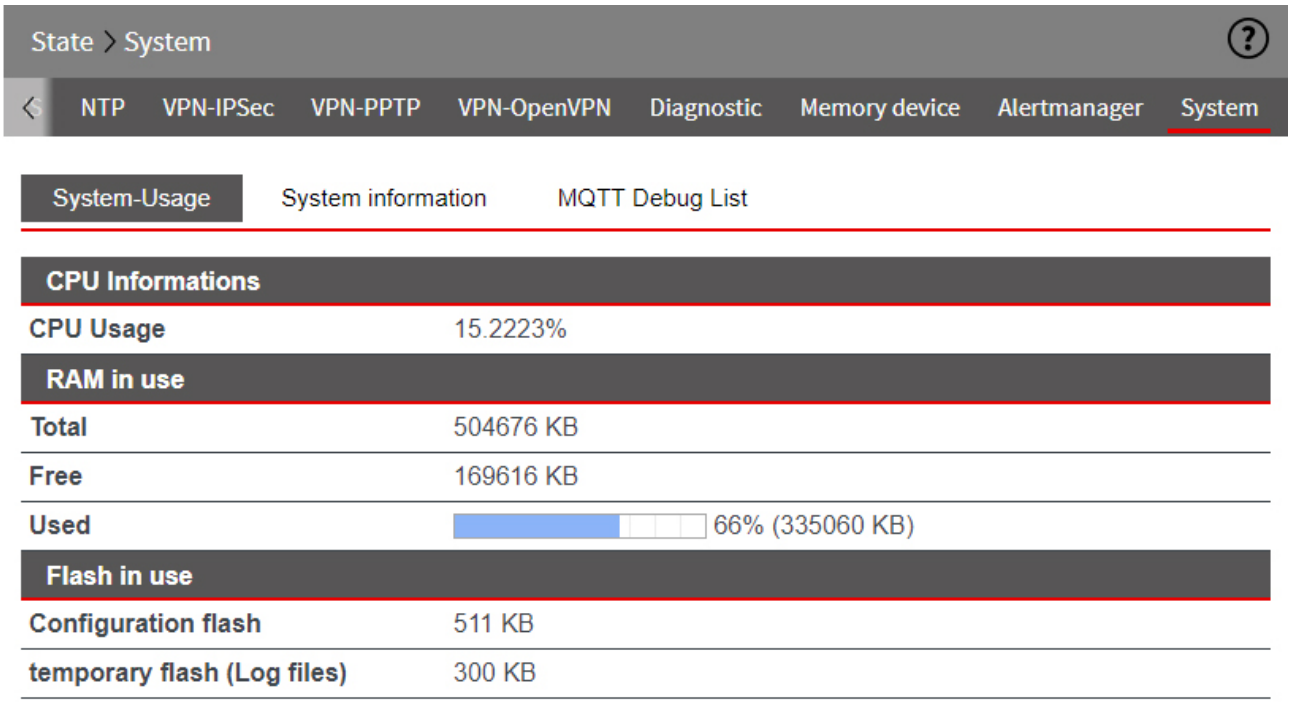
29.17 Alarm Manager



Designation	Description
Inputs	The statuses of the digital inputs are displayed here. The status query is performed and updated approximately every three seconds.
Outputs	The statuses of the digital outputs are displayed here. The status query is performed and updated approximately every three seconds.
The status query is performed and updated approximately every three seconds. green LED symbol = status = 1 grey LED symbol = status = 0	
System Logging	All the events and error messages relating to the alarm management are saved here (e.g.: Short message delivery, activity of inputs, etc.).

29.18 System

29.18.1 System-Usage



CPU Information

Display of the current utilization of the CPU.

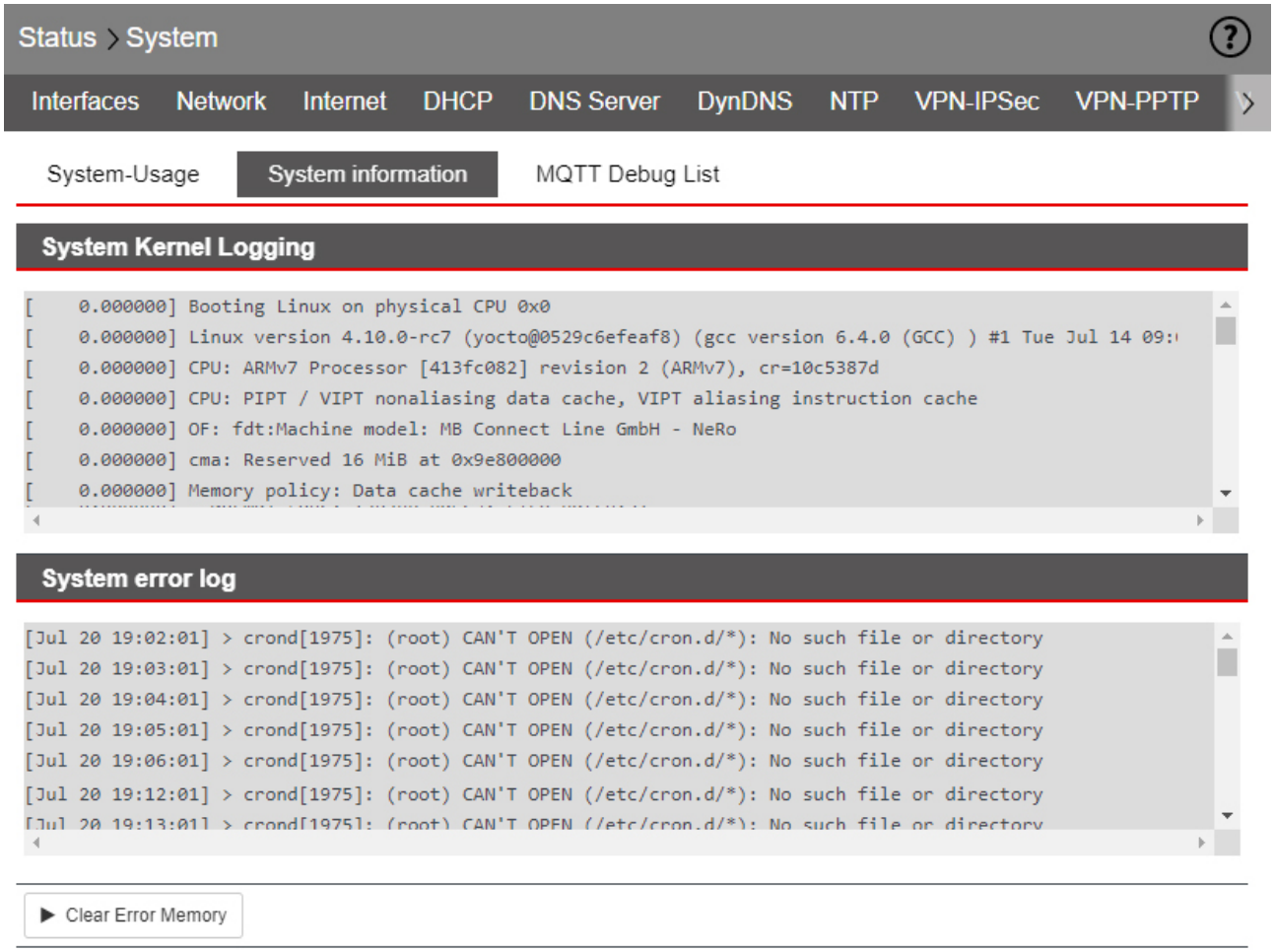
RAM usage

Displays the currently required /used RAM of the router.

Flash in use

Displays the capacity of the configuration memory and temporary memory.

29.18.2 System Information



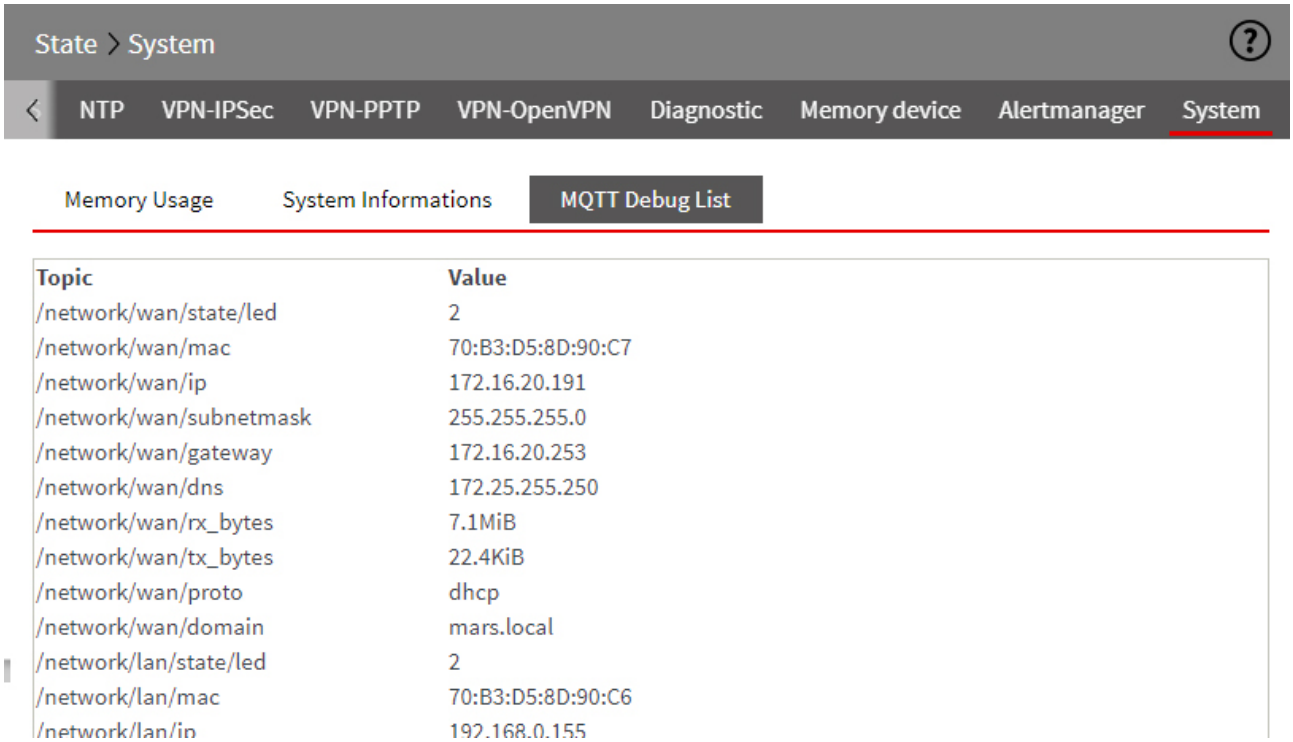
System Kernel Logging

Possible reasons for errors in the router can be found in the system information.

System error log

For example, if the Stat-LED on the front of the device is flashing, it may be possible to use the logging to discover the cause of the error.

29.18.3 MQTT debug list



Topic	Value
/network/wan/state/led	2
/network/wan/mac	70:B3:D5:8D:90:C7
/network/wan/ip	172.16.20.191
/network/wan/subnetmask	255.255.255.0
/network/wan/gateway	172.16.20.253
/network/wan/dns	172.25.255.250
/network/wan/rx_bytes	7.1MiB
/network/wan/tx_bytes	22.4KiB
/network/wan/proto	dhcp
/network/wan/domain	mars.local
/network/lan/state/led	2
/network/lan/mac	70:B3:D5:8D:90:C6
/network/lan/ip	192.168.0.155

The MQTT debug list outputs the system information in tabular form.

The mbNET can be used as an MQTT broker.

After activating the "MQTT access to status topics" function under "System > Settings > Device API", you can query the values from the "MQTT debug list".

30 Firmware update via the USB interface

You can update the ***mbNET*** directly via the USB interface. The device then automatically recognizes the firmware saved to a connected USB stick. Pressing the **Dial Out** button starts the firmware update.

Preparation:

- Go to **www.mbconnectline.com (downloads)** and download the latest firmware version (e.g. "mb-NET_FW_V624.zip").
- After extracting it, you will find the actual firmware file "**image.swux**" along with the "changelog.txt" and "open-source software licenses.txt" files.
- Save the "**image.swux**" file on a USB stick.

NOTICE

IMPORTANT: The "**image.swux**" firmware file must not be renamed and must be stored in the top-level directory of the USB stick! The USB stick must have the FAT file format!

Execution:

When the ***mbNET*** is ready for operation (**LED Pwr + Rdy light up**), connect the USB stick to one of the USB ports of the device.

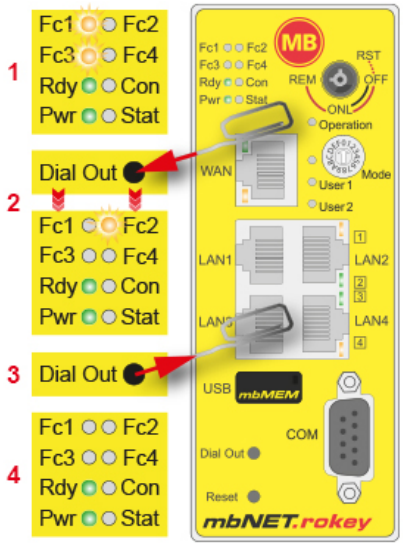
1 As soon as the firmware file has been detected by the ***mb-NET,*****LED fc1 + Fc3** start **flashing**.

2 Now press the **Dial Out** button and keep it pressed until **LED Fc2 flashes**.

3 Release the Dial Out button.

The ***mbNET*** now performs a device reboot.

4 If both the **Pwr and Rdy LEDs light up**, the firmware update is complete.



The ***mbNET*** is now ready for operation and can be used again as usual.

NOTICE

If both the firmware as well as a mbCONNECT24 portal configuration are on the USB stick, the **firmware** will always be detected by the mbNET (**Fc1 + Fc3 flash**). If you do not respond within 10 seconds, the Dial Out button switches the mbNET to **Portal Configuration** (**Fc1 + Fc2 flash**). If you do not respond within 10 seconds, the device will return to normal mode.

31 Programming the mbCONNECT24 portal configuration via the USB interface

If you created the ***mbNET*** device configuration in the ***mbCONNECT24*** service portal, you can scan this portal configuration directly via the USB interface into the ***mbNET***. The device automatically detects the portal configuration stored on a connected USB Stick ("mbconnect24.mbn/-.mbnx").
Pressing the **Dial Out** button starts the scan.

Requirement:

You have configured the ***mbNET*** in the ***mbCONNECT24*** portal and saved the configuration file via transfer type "*Download to PC configuration*" on a USB stick.

NOTICE

The configuration file "mbconnect24.mbn/-.mbnx" should not be renamed and must be stored in the top-level directory (root) of the USB stick!
The USB stick must have the FAT/FAT32 file format!

You can find information about ***mbCONNECT24*** on

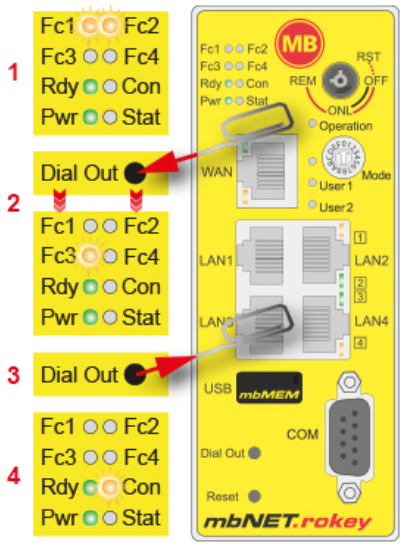
- our website at **www.mbconnectline.com**
- or in the ***mbCONNECT24***online help

Execution:

When the ***mbNET*** is ready for operation (**LED Pwr + Rdy light up**), connect the USB stick to one of the USB ports of the device.

1. As soon as the firmware file has been detected by the ***mbNET,*****LED fc1 + Fc2** start **flashing**.
2. Now press the **Dial Out** button and keep it pressed until **LED Fc3 flashes**.
3. Release the **Dial Out** button.

   Now, the settings from ***mbCONNECT24*** are applied in the ***mbNET***, and the device restarts.
4. If the ***mbNET*** can connect to the Internet (for example, network cable, SIM card, antennas installed) it logs on to your ***mbCONNECT24***-account. This is indicated by the **flashing Con** LED



NOTICE

If both the firmware as well as a mbCONNECT24 portal configuration are on the USB stick, the **firmware** will always be detected by the mbNET (**Fc1 + Fc3 flash**). If you do not press the Dial Out button within 10 seconds, the mbNET switches to **Portal Configuration** (**Fc1 + Fc2 flash**). If you do not respond within 10 seconds, the device will return to normal mode.

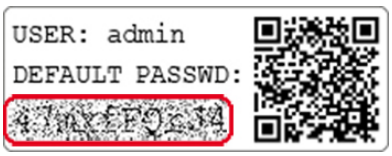
32 Factory settings when delivered

32.1 User name and password - for access to the mbNET Web Interface

The ***mbNET*** is delivered with the following user data:

User name admin

Password The default password can be found on the back of the device



NOTICE

Make sure you change the default access data immediately!

32.2 IP address of the mbNET

The ***mbNET*** is set to the following IP address in the factory:

IP address 192.168.0.100

Subnet mask 255.255.255.0

33 Load factory settings

NOTICE

Before you configure the device to its factory settings, you should note the following:

- Save your configuration **first**. After restoring the factory settings, all of your settings/changes will be deleted.
- The IP address of the device is reset to the original IP address (192.168.0.100).
  You may also need to modify the network settings of the configuration PC accordingly.
- The device password is reset to its individual default password. The default password can be found on the back of the unit.
- No USB stick/storage medium should be connected to the device.

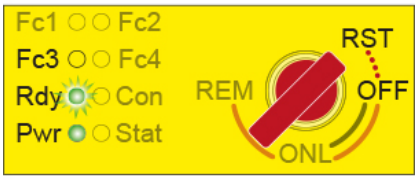
Execution:

1

a) Switch on the mbNET **or**

b) if the mbNET is ready for operation, press the **Reset** button.

2 When the LED **Rdy flashes** (green), turn the key switch - with the red key - to the switch position **RST** and hold this key position.



NOTICE

The key position **RST** has only a button function => you have to hold the key in this position.

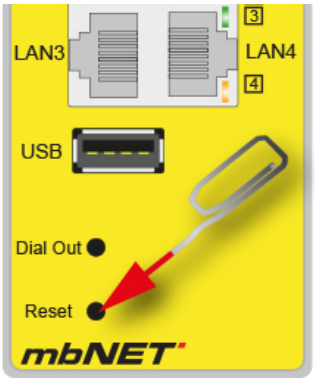
3 When LED **Fc3** is **flashing** (orange), release the key.

When both the **Pwr** and **Rdy** LEDs **light up**, the mbNET is reset to its „factory settings at the time of delivery" and can/must be reconfigured.

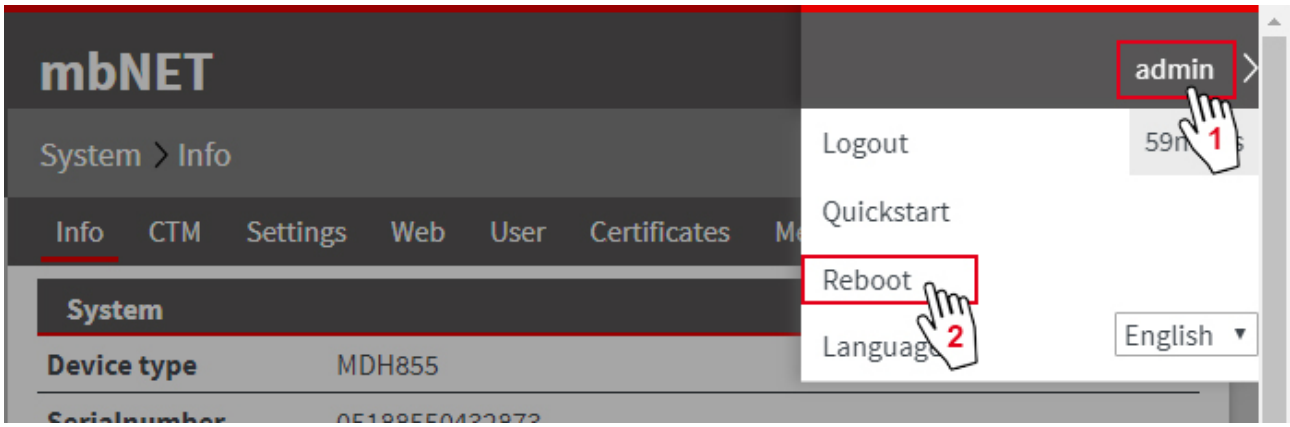
34 Device restart (Reset)

Directly on the device (mbNET) using the reset button

For example, use a paper clip and press the Reset button on the mbNET.
The device will now restart.
The restart is complete once both the "Rdy" and "Pwr" LEDs light up.



Via the mbNET web interface



1 Open the "**admin**" context menu

2 Click "**Restart**"

35 Annex

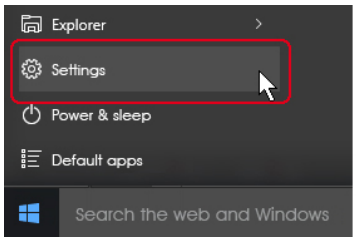
35.1 Set computer address (IP address) in Windows 10

NOTICE

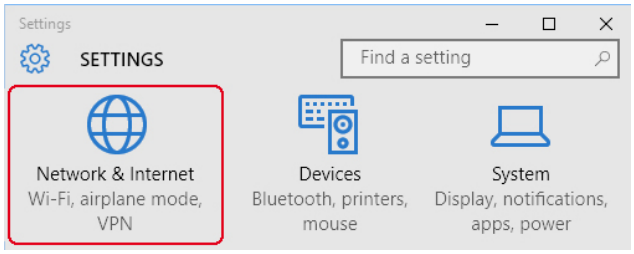
If you want to access the web interface of the mbNET via a configuration PC, the following conditions must be met:

- The mbNET must be connected to the PC via one of its LAN interfaces.
- Access to the web configuration is not blocked (System > Web > System Service).
- The IP address of the PC is set in such a way that it is in the same IP range as the mbNET (factory setting for the mbNET is 192.168.0.100), i.e. 192.168.0.**X**.
  => **X** = variable, where **X** should not already be occupied by any other network participants.

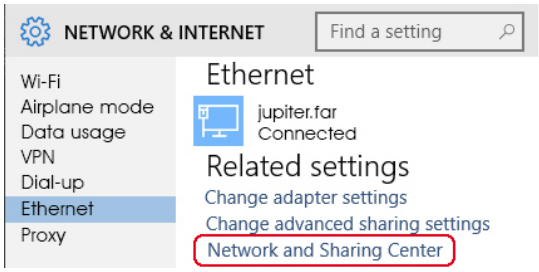
- Open the **Windows Start menu** and go to the **settings**.



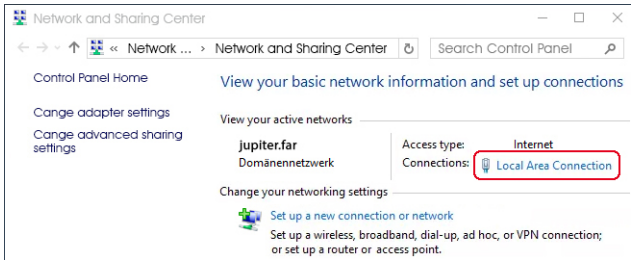
- In Settings, click the **Network and Internet** section.



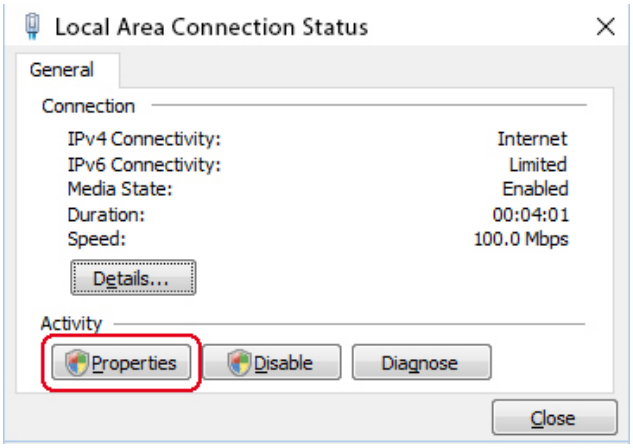
- Under **Network and Internet** click the section **Network and Sharing Centre**.



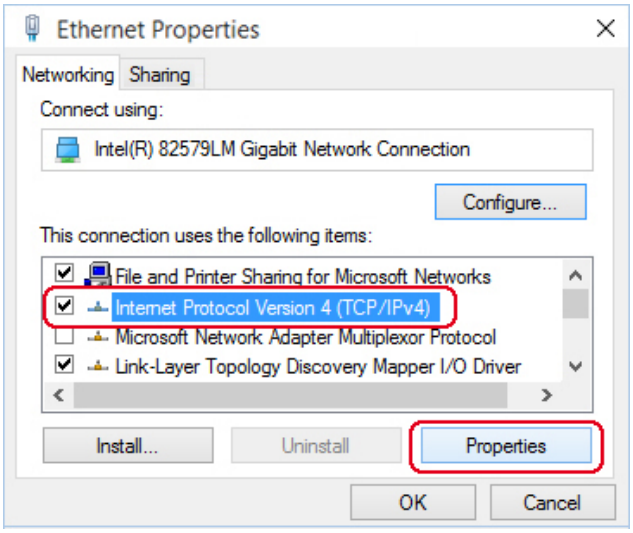
- In the **Network and Sharing Centre,click** on the current **connection** (LAN connection in this case).



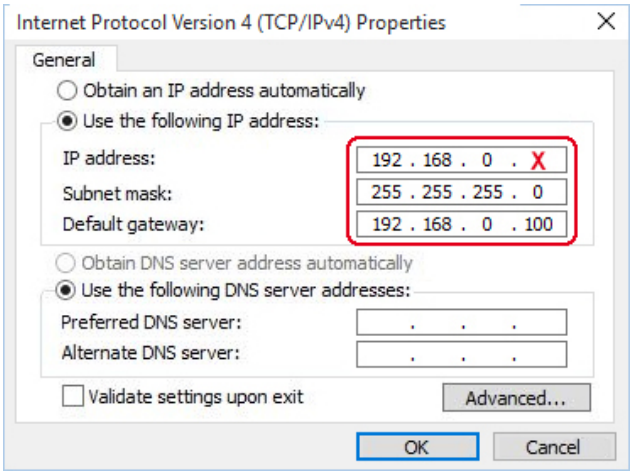
- Click on **properties** in the next window (**Status of LAN connection**).



- Here, under **Properties of the LAN-connection**, select the entry **Internet Protocol Version 4 (TCP/IPv4)**, and click on **Properties**.



- Here,
  - the IP address of the computer must be in the same network range as the mbNET,
  - the subnet mask 255.255.255.0 must be entered.
  - The entry for the default gateway has the same IP address as the mbNET (here 192.168.0.100).



Save your settings and close the single windows.