

mbNET.

Installation instructions/User manual

V 6.3.0 - from HW02 - en | Aug. 11th, 2021



MDH810, MDH811, MDH814, MDH815, MDH816, MDH819, MDH830, MDH831,
MDH834, MDH835, MDH841, MDH849, MDH850, MDH855, MDH858, MDH859

CE  LISTED US PROG. CNTLR.
E482663

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** Router MDH 810 – MDH 859 from hardware version HW02 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.

Copyright © MB connect line GmbH 1997 - 2021

Table of contents

1	General.....	9
2	Information about cyber-security.....	13
3	Warning signs.....	14
4	Security information.....	14
5	Maintenance.....	17
6	Legal notice.....	18
7	Functional overview.....	19
8	Technical data.....	20
9	Scope of Supply.....	28
10	Display, controls and connectors.....	29
	10.1 Front view of device.....	29
	10.2 View at the top of the device.....	32
	10.3 View of underside of device.....	33
11	Interface assignment.....	34
	11.1 Pin assignment of terminal blocks X1 and X2 on the top of the device.....	34
	11.2 Pin assignment of the RJ11 socket on the bottom of the device.....	34
	11.3 Pin assignment serial interfaces COM1/COM2 (front of device).....	34
	11.4 Pin assignment LAN/WAN port on front of device.....	35
	11.5 Pin assignment USB port on front of device.....	36
12	Router Installation.....	37
13	Starting the router.....	38
14	Connect router to configuration PC.....	39
15	Calling up the mbNET web Interface.....	40
16	First Start.....	41
17	Portal server - First start.....	42
	17.1 Internet - Configuring the Internet connection.....	43
	17.1.1 External Router/Firewall WAN settings.....	43
	17.1.2 DSL Settings.....	45
	17.1.3 Modem Connection Settings.....	46
	17.1.4 Wi-Fi Connection Settings.....	47
	17.2 Portal Server - Settings.....	48
	17.3 Finish - Apply settings.....	49
18	Quick Start - Cloud Status Page.....	51

18.1	Quick Start.....	51
18.2	Diagnosis.....	53
18.3	IoT.....	54
19	Classic router - configuring the mbNET via the web interface.....	56
19.1	Description of the graphical user interface (configuration interface).....	56
19.2	Description of buttons, icons and fields.....	57
20	System - settings and basic router configuration.....	58
20.1	System > Info.....	59
20.2	System > CTM (Configuration Transfer Manager).....	61
20.3	System > Settings.....	63
20.3.1	System > Settings > System Settings.....	64
20.3.2	System > Settings > Time Settings.....	65
20.3.3	System > Settings > NTP Settings.....	66
20.3.4	System > Settings > Mail Settings.....	68
20.3.5	System > Settings > Device-API.....	69
20.3.6	System > Settings > System Service.....	70
20.4	System > WEB.....	71
20.4.1	System > Web > HTTPS access for device configuration.....	73
20.4.2	System > Web > System Services.....	74
20.5	System > User.....	75
20.5.1	Added/Edited User.....	76
20.6	System > Certificates.....	78
20.6.1	Own certificate.....	79
20.6.1.1	Import own certificate.....	79
20.6.2	CA certificate (root certificate).....	81
20.6.2.1	Importing CA certificate (root certificate).....	81
20.6.3	Partner certificate (IPSec).....	82
20.6.3.1	Import partner certificate.....	82
20.6.4	CRL (revocation list).....	84
20.6.4.1	Import CRL (revocation list).....	84
20.7	System > Memory devices.....	85
20.7.1	USB.....	85
20.7.1.1	USB Settings.....	85
20.7.1.2	USB access from the network.....	86
20.7.1.3	USB devices.....	86
20.7.2	SD Access from network.....	87
20.8	System > Logging.....	88
20.8.1	General Settings.....	88
20.8.2	External logging (server settings).....	89
20.9	System > Configuration (backup and restore).....	90
20.10	System > Firmware (Firmware update).....	91
20.10.1	Firmware update.....	92
21	Network - connection settings and options.....	93

21.1	Network > LAN.....	95
21.1.1	Interface.....	95
21.1.2	Routes.....	97
21.2	Network > WAN.....	99
21.2.1	Interface - set WAN interface type.....	99
21.2.2	Routes.....	100
21.3	Network > Wi-Fi.....	103
21.3.1	Interface - set Wi-Fi interface type.....	103
21.3.2	Wi-Fi Settings.....	104
21.4	Network > Modem.....	108
21.4.1	Analogue modem configuration.....	108
21.4.1.1	Modem Settings.....	109
21.4.1.2	Outgoing (configuration for outgoing connections).....	110
21.4.1.3	Incoming.....	112
21.4.1.4	Call Back.....	114
21.4.2	GSM modem configuration.....	115
21.4.2.1	Modem Settings.....	115
21.4.2.2	Outgoing SIM 1/SIM 2 (configuration for outgoing connections).....	116
21.4.2.3	General SIM Settings.....	119
21.4.2.4	SMS (Remotely control services via SMS Send SMS if,...).....	121
21.5	Network > Internet (Internet connection and Internet settings).....	124
21.5.1	Configure Internet connectivity.....	124
21.5.2	Internet settings (connection settings).....	128
21.6	Network > DHCP.....	132
21.6.1	LAN/WAN DHCP server settings.....	133
21.6.2	LAN/WAN DHCP static lease server settings.....	134
21.7	Network > DNS-Server.....	135
21.8	Network Hosts.....	138
21.9	Network > DynDNS.....	140
21.9.1	System DynDNS settings (MB Connect Line DynDNS service).....	140
21.9.2	Public DynDNS service.....	141
22	Serial (serial ports COM1/COM2).....	143
22.1	COM1/COM2 in the RS232/485 version.....	144
22.1.1	COM1 (COM2) settings.....	144
22.1.2	COM1 (COM2) network settings.....	145
22.2	COM2 in the MPI/PROFIBUS version.....	146
22.2.1	COM2 Settings.....	146
22.2.2	COM2 Network settings.....	148
23	Security settings.....	149
23.1	Security Settings > Firewall General.....	150
23.2	Security Settings > WAN LAN (configuration of the firewall rules).....	152
23.2.1	Edit firewall rule.....	155
23.3	Security Settings > LAN-WAN (configuration of the firewall rules).....	157
23.3.1	Edit firewall rule.....	160

23.4	Security Settings > Forwarding.....	162
23.4.1	Edit Forwarding Rule.....	165
23.5	Security settings > NAT.....	167
23.5.1	SimpleNAT.....	167
23.5.1.1	Edit SimpleNAT Rule.....	168
23.5.2	1:1 NAT.....	170
23.5.2.1	Edit 1:1 NAT rule.....	171
24	VPN.....	173
24.1	IPSec.....	173
24.1.1	Configure IPSec connections.....	173
24.1.2	IPSec settings.....	182
24.2	PPTP.....	183
24.2.1	PPTP server configuration.....	183
24.2.2	PPTP client configuration.....	185
24.3	OpenVPN.....	187
24.3.1	Configure OpenVPN connections.....	188
24.3.1.1	Connection type: Client router connection.....	188
24.3.1.2	Connection type: Router-router connection - server mode.....	197
24.3.1.3	Connection type: Router-router connection -client mode.....	207
24.4	Static key (key management).....	219
25	IO-Manager.....	221
25.1	Configuring the PLC connection.....	222
25.2	Logging - configuration.....	224
25.3	Status.....	225
25.4	Create tags.....	226
25.5	Diagnosis.....	228
26	Alarm Management.....	228
26.1	Digital inputs - Configuration.....	229
26.2	Digital outputs - Configuration.....	231
27	Extras.....	233
27.1	LUA.....	233
27.2	IoT > Control (mbEDGE).....	236
27.2.1	IoT > Control > Docker - activate mbEDGE.....	236
27.2.2	IoT > Control - after activating mbEDGE.....	238
27.2.3	IoT > Control - activate Docker Management.....	240
27.2.3.1	Link to User Interface.....	241
27.2.4	Flows and Dashboard.....	242
27.2.4.1	Activate flows and dashboard.....	242
27.2.4.1.1	Link to Flows (Node-RED).....	243
27.2.4.1.2	Link to Dashboard (Node-RED).....	244
27.2.5	Backup and Delete flows.....	245
27.3	Network.....	246
27.4	Key Management.....	247

27.4.1	Create Backup-Key.....	248
27.5	Firmware.....	249
27.6	RoKEY.....	250
28	Status (information and analysis).....	252
28.1	Status > Interfaces.....	252
28.2	Status > Network.....	254
28.2.1	General.....	254
28.2.2	Firewall.....	255
28.2.3	Network participants.....	256
28.3	Status > Modem.....	257
28.3.1	GSM information.....	257
28.3.2	Modem.....	258
28.4	Wi-Fi.....	259
28.5	Internet.....	260
28.6	DHCP.....	261
28.7	DNS Server.....	262
28.8	DynDNS.....	263
28.9	NTP.....	264
28.10	VPN-IPSec.....	265
28.11	VPN-PPTP.....	266
28.11.1	VPN PPTP server.....	266
28.11.2	VPN PPTP clients.....	267
28.12	VPN-OpenVPN.....	268
28.13	IoT.....	269
28.13.1	IoT > Docker.....	269
28.13.2	IoT > Docker Management.....	270
28.13.3	IoT > Flows and Dashboard.....	271
28.14	Runtime.....	272
28.15	Diagnostics - Network Resources.....	273
28.16	Storage media.....	274
28.17	Alarm Manager.....	275
28.18	System.....	276
28.18.1	System-Usage.....	276
28.18.2	System Information.....	277
28.18.3	MQTT debug list.....	279
29	Firmware update via the USB interface.....	280
30	Programming the mbCONNECT24 portal configuration via the USB interface.....	281
31	Factory settings when delivered.....	282
31.1	IP address of the mbNET.....	282
31.2	User name and password - for access to the mbNET Web Interface.....	282
32	Load factory settings.....	283
33	Device restart (Reset).....	284

34	Annex.....	285
34.1	Set computer address (IP address) in Windows 10.....	285
34.2	Modem initialization (AT commands).....	287
34.3	Country codes for devices with analogue modem.....	289


1 General

Purpose of the documentation

This document describes the installation, use and functions of the mbNET Router MDH810 - MDH859. 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** (MDH810, MDH811, MDH814, MDH815, MDH816, MDH819, MDH830, MDH831, MDH834, MDH835, MDH841, MDH849, MDH850, MDH855, MDH858, MDH859) - **from firmware version V 6.2.4 and from hardware version HW02***

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
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/mbSPIDER) 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/ mbSPIDER data modem) 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 6.0.0	Mar. 12 th , 2018	Start-Version
V 6.0.0 DR01	Oct. 11 th , 2018	Wiring diagrams for I/O terminals added (Chap.: "View at the top of the device").
V 6.0.5	Jan. 17 th , 2019	Note on the increase of the random access memory to 512 MB and the resulting possibility to use the optional mbEDGE functions for devices as of hardware version HW03 (Chap.: "Technical data"). Add the "HTTP proxy, skip the certificate check" option if the outgoing connection uses an HTTP proxy server (Chap.: "System > CTM (Configuration Transfer Manager)").
V 6.0.6	Apr. 9 th , 2019	Add the IoT function in the Quickstart section Add the SNAT (WAN) feature in Security Settings > Firewall General . Correction of the description in chapter Security Settings > > WAN-LAN (configuration of the firewall rules) > LAN-WAN (configuration of the firewall rules) > Forwarding "Input of ranges" in the input fields for IP addresses and "Input of ranges or enumerations" in the input fields for ports. Add the description "SD Access from network" (System > Memory Devices) Extended functionality under System > Firmware . Add the submenus IoT and RoKEY in the Extras section.
V 6.0.8	Jun. 19 th , 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 device" Add the description for the menu "IO-Manager". See chapter: "IO-Manager"

Version	Date	Comments
V 6.1.0	Oct. 1 st , 2019	Note on the function SIMPLY.connect in the chapters <ul style="list-style-type: none">• "General > Validity"• "Display, controls and connectors" > "Front view of 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. 5 th , 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. 11 th , 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. 22 nd , 2020	Add the processor performance data in the technical data.
V 6.1.4	July 6 th , 2020	Add the transmission power of radio modules in the technical data.
V 6.2.0	Oct. 19 th , 2020	General revision Additions to the menu: Extras > IoT (mbEDGE)
V 6.2.0 DR01	Mar. 17 th , 2021	General corrections, update / change of the encryption method and encryption algorithms.
V 6.3.0	Aug. 11 th , 2021	General corrections Change / extension of the technical data

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>.

2 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.

3 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.

4 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 intercepted 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.

ENF 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.

5 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

6 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.

Devices with **LTE (4G)** modems - **AT&T** (MDH 850 AT&T, MDH 855 AT&T, MDH 858 AT&T, MDH 859 AT&T)

NOTICE

Device types MDH 850 AT&T, MDH 855 AT&T, MDH 858 AT&T, MDH 859 AT&T bear no CE marking and may not be used or put into operation in the European economic area (EEA)!

7 Functional overview

Brief description

mbNET industrial routers offer maximum flexibility with maximum security.

mbNET industrial routers are specifically designed for industrial use. They enable secure and reliable connection of machines and systems over the Internet. They support various security protocols and are universally applicable. However, their full capacity is revealed when they are connected to the **mbCONNECT24** remote service platform.

The built-in firewall ensures optimum access protection by only enabling remote access by identified and authenticated users.

With a variety of interfaces and device drivers, **mbNET** industrial routers provide enormous flexibility for remote maintenance of different control systems, drives, control panels, frequency converters and other modules.

The router is configured via the **mbconnect24** portal (mymbCONNECT24.mini, -.midi, -.maxi, -.hosted, -.virtual) or the web interface of the router.

Performance features:

- Fully configurable using Web interface via locally connected computer, or remotely via **mbCO-NENCT24**.
- Deployable worldwide using different modem connections, (analog, mobile broadband) 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).
- Alarm management:
 - Fully configurable digital inputs and outputs, and the ability to send via email, SMS or Internet dial-up.
 - 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.
- Dual LEDs for a more detailed display on the function and status display.
- As of firmware version 6.0.5, all **mbNET** routers, as of hardware version **HW03**, can use 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

8 Technical data

mbNET® Industrial router

MDH 810, MDH 811, MDH 814, MDH 815, MDH 816, MDH 819, MDH 830, MDH 831, MDH 834, MDH 835, MDH 841, MDH 849, MDH 850 EU, MDH 850 AT&T, MDH 855 EU, MDH 855 AT&T, MDH 858 EU, MDH 858 AT&T, MDH 859 EU, MDH 859 AT&T - from hardware version: **HW 02**

You can find the hardware version on the device rating plate.

Housing dimensions

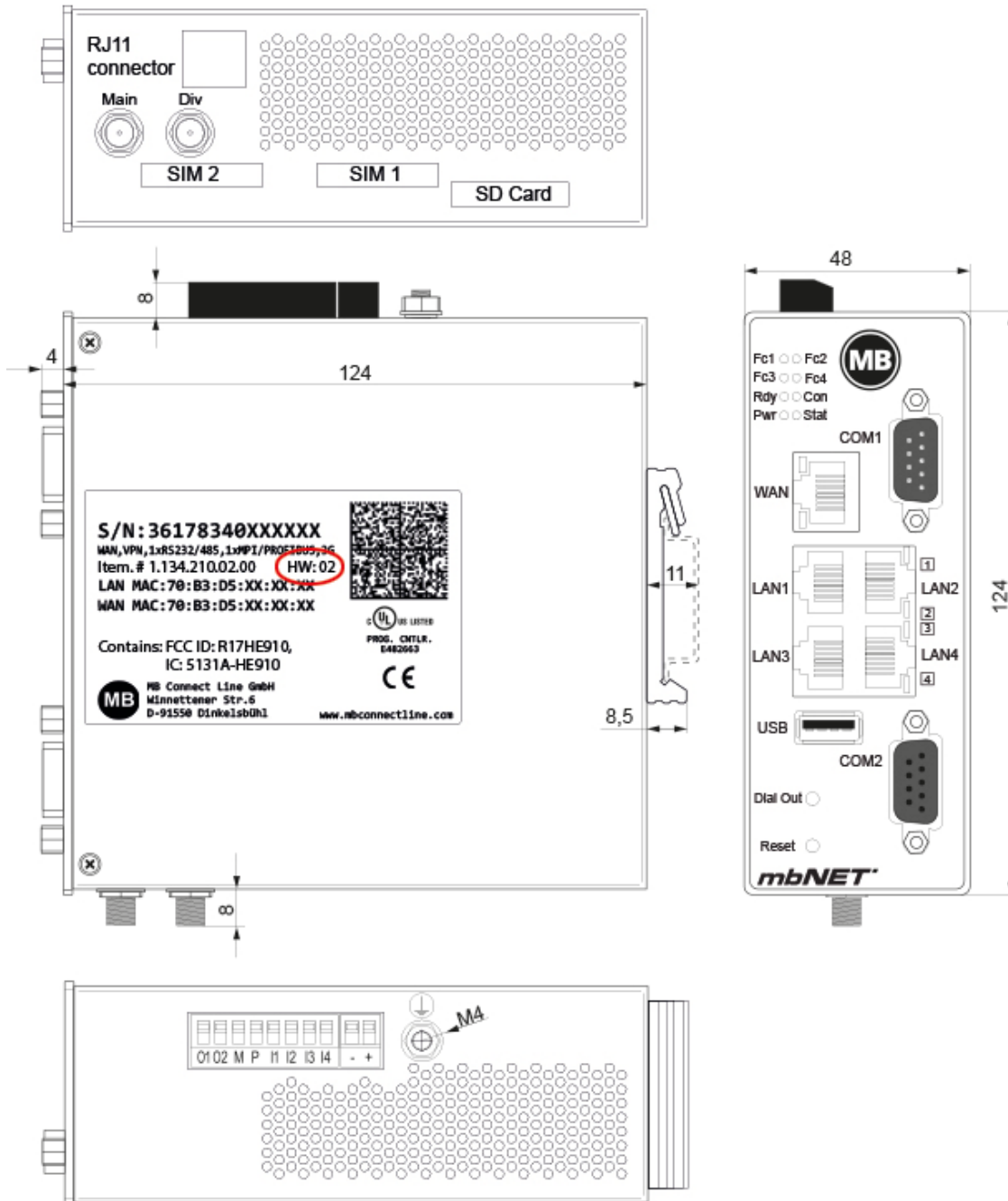


Image 1: Devices and interfaces vary depending on the device type.

Release note

Version	Date	Comment
V 6.2	Feb. 26 th , 2020	Previous version: V 6.0 from June 4 th , 2019 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. 22 nd , 2020	Add processor performance data.
V 6.2 DR02	July 6 th , 2020	Adding the transmission power for radio modules.
V 6.2 DR03	Feb. 8 th , 2021	Update / change of the encryption method and encryption algorithms.
V 6.2 DR04	July 14 th , 2021	Adding the performance data for devices with Wi-Fi module from HW 05.
V 6.3.0	Aug. 11 th , 2021	Adding the performance data for devices with LTE module (EU) from HW 05.

General Data

Performance data	
Voltage — V (DC)	10 – 30 V DC (ext. power supply or SELV power supply, 10-30 V DC, Max. 40A)
Current consumption	max. 500 mA @ 24 V
Dissipated power	max. 6 W
Random access memory	Devices up to hardware version HW02 : 256 MB Devices from hardware version HW03 : 512 MB
Processor	Devices up to 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 interfaces

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
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	For SD cards (32.0 mm x 24.0 mm x 2.1 mm) SDHC max. 32 GB; FAT/FAT32

NOTICE

As of firmware version **6.0.6** and hardware version from **HW03**, all devices can use the **mbEDGE** function.

VPN

VPN protocol	IPsec/PPTP/OpenVPN, 64 Tunnel	MDH 810, MDH 811, MDH 814, MDH 830, MDH 831, MDH 834, MDH 850 EU, MDH 850 AT&T, MDH 855 EU, MDH 855 AT&T
VPN protocol	OpenVPN, 1 Tunnel	MDH 815, MDH 816, MDH 819, MDH 835*, MDH 841, MDH 849, MDH 858 EU, MDH 858 AT&T, MDH 859 EU, MDH 859 AT&T
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	

*can only be operated with my / mbCONNECT24.

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

WAN interfaces	10/100MBit/s full and half duplex operation, automatic detection patch cable / cross-over cable (auto detection)
Interface 1 (COM1)	RS-232/485 (software-switchable)
Interface 2 (COM2) - device-dependent -	RS-232/485 (software-switchable) or MPI/PROFIBUS - 12 MBit/s
SIM card slots	2 pieces SIM card reader with ejector (for mini-SIM)


Communication
Devices with LTE (4G) module EU (MDH 850 EU, MDH 855 EU, MDH 858 EU, MDH 859 EU)

Devices with hardware version HW 05	
Target region	EMEA
GSM/GPRS/EDGE	900 (B8), 1800 (B3) MHz; max. 236 kbps
HSxPA	900 (B8), 1800 (B3), 2100 (B1) MHz; Downlink max. 42 Mbps, Uplink max. 5,76 Mbps
LTE	800 (B20), 900 (B8), 1800 (B3), 2100 (B1), 2600 (B7), 700 (B28A) MHz; Downlink max. 150 Mbps, Uplink max. 50 Mbps
RF parameters	
Output power - typical values for max output level	Sensitivity - typical sensitivity levels
<ul style="list-style-type: none"> • 2G: LB: 33 dBm; HB: 30 dBm • 3G/TD-SCDMA: 24dBm • 4G (FDD & TDD): 23dBm @1RB 	<ul style="list-style-type: none"> • -108 dBm @ 2G • -113.5 dBm @ 3G • -103 dBm @ 4G FDD (BW=5 MHz)
TAC	35162610

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 up to 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


Devices with hardware version up to **HW 03**

Transmit 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) module - AT&T (MDH 850 AT&T, MDH 855 AT&T, MDH 858 AT&T, MDH 859 AT&T)

NOTICE

Device types MDH 850 AT&T, MDH 855 AT&T, MDH 858 AT&T, MDH 859 AT&T bear 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
Transmit 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

Devices with Wi-Fi module (MDH 811, MDH 831, MDH 841) from HW 05


Wi-Fi	IEEE 802.11b/g/n	
Frequency bands	2.4 GHz, channel 1 - 13* (2.412 GHz - 2.472*)	
Channel bandwidth	20 MHz	
Data rates	802.11b	1, 2, 5.5 and 11 Mbps
	802.11g	6, 9, 12, 18, 24, 36, 48 and 54 Mbps
	802.11n	MCS0-MCS7 (max 72.2Mbps)
Hardware supported Encryptions/Decryption	AES/CCMP, AES/CMAC, WAPI, WEP/TKIP	
Max. output power	19 dBm EIRP**	
Max. sensitivity	-97 dBm EIRP**	
FCC	FCC ID: XPYLILYW1 IC: 8595A-LILYW1	
IC	IC: 8595A-LILYW1	

* Maximum, depends on the region. ** RF power including maximum antenna gain (3 dBi).

Devices with Wi-Fi module (MDH 811, MDH 831, MDH 841) up to HW 04

Devices with Wi-Fi modem (MDH 811, MDH 831, MDH 841)	
Wi-Fi	IEEE802.11b/g & 802.11n (1T1R mode), up to 150 MBit/s
Wi-Fi specification	<ul style="list-style-type: none"> · EU (2.412 GHz-2.472 GHz, 1-13 Channel) · USA (2.412 GHz-2.462 GHz, 1-11 Channel) · WPA/WP2, 64/128/152bit WEP, WPS · 802.11b: 1, 2, 5.5, 11 Mbps · 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps · 802.11n: (20 MHz) MCS0-7, up to 72 Mbps · 802.11n: (40 MHz) MCS0-7, up to 150 Mbps
Transmit output power (typical)	11b: 19+/- 1.0 dBm @ 11 Mbps 11g: 16+/- 1 dBm @ 54 mbps 802.11n: (HT20), 15 +/- 1dBm, 802.11n: (HT40), 15 +/- 1dBm
Receive sensivity (typical)	11b: -84dBm @ 11 Mbps; 11g: -70dBm @ 54 Mbps 802.11n: (HT20), -66 dBm @ MSC7, (HT40), -62 dBm @ MSC7
Antenna connection	1 piece RP SMA socket 
FCC	Contains FCC ID: YWTWFXM05

Devices with UMTS (3G) module (MDH 814, MDH 819, MDH 834, MDH 849)

Countries where used	Global
GSM/GPRS/EDGE	850, 900, 1800, 1900 MHz; Downlink max.296 kbps, Uplink max. 236.8 kbps
HSxPA	800/850, 900, AWS 1700, 1900, 2100 MHz; Downlink max. 21 Mbps, Uplink max. 5.76 Mbps
Transmit output power	Class 4 (2 W, 33 dBm) @ GSM 850 / 900 Class 1 (1 W, 30 dBm) @ GSM 1800 / 1900 Class 3 (0.25 W, 24 dBm) @ UMTS Class E2 (0.5 W, 27 dBm) @ EDGE 850 / 900 Class E2 (0.4 W, 26 dBm) @ EDGE 1800 / 1900
Reception sensitivity	-108 dBm @ UMTS -107 dm @ GSM 850 / 900 MHz -106 dBm @ DCS1800 / PCS1900 MHz
Antenna connection	1-piece SMA socket 
FCC	Contains FCC ID: R17HE910
TAC	35613607

Devices with analogue modem (MDH 810, MDH 815, MDH 830)

Countries where used	240 countries
Modulation types	V.21, V.22, V22bis, V.23, V.32, V.32bis, V.34
Data compression	V.42bis, MNP5
Error correction	MNP 2-4, V.42 LAPM
Dialling procedure	MFV/IWV
Modem port	RJ11 socket
FCC	Contains Part 15 & Part 68

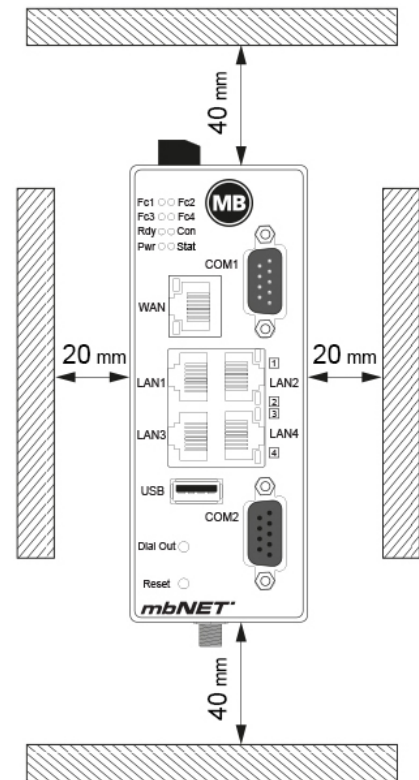
The router is designed to be mounted on DIN top hat rails (in accordance with DIN EN 50 022) and for installation in a control cabinet.

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!



Markings / Listings / Certifications



PROG. CNTLR.
E482663

Certificates (CE, UL, etc.) can be downloaded at www.mbconnectline.com.

SIMPLIFIED EU DECLARATION OF CONFORMITY









MB connect line GmbH hereby declares that the radio system type MDH 811, MDH 814, MDH 819, MDH 831, MDH 841, MDH 834, MDH 849, MDH 850 EU, MDH 855 EU, MDH 858 EU, MDH 859 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

9 Scope of Supply

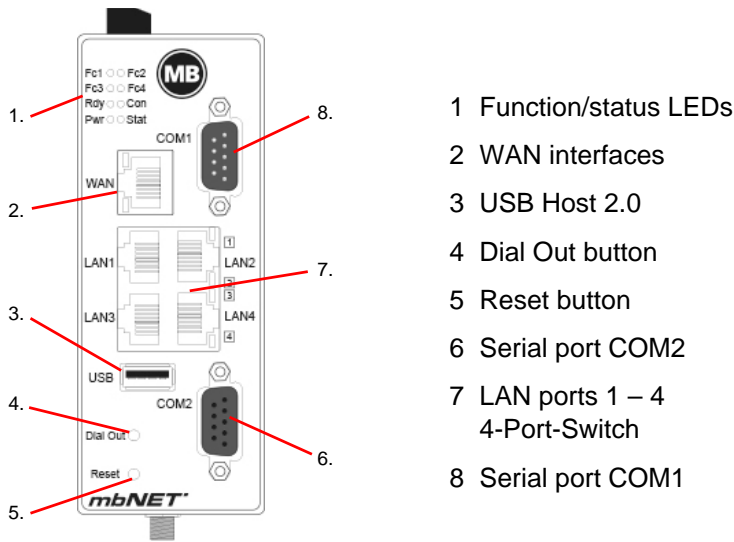
Check the package contents for completeness:

All types of devices			
			
1 x mbNET 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.: 8.002.701.03.00	1 x Device ID card Item No.: 8.002.707.00.00
Device types with analogue modem		Device types with GSM modem	
MDH 810; MDH 815; MDH 830		MDH 814; MDH 819; MDH 834; MDH 849; MDH 850; MDH 855; MDH 858; MDH 859	
			
1 x telephone cable RJ11 - RJ11 Item No.: 8.02.113.00.00	1 x TAE adapter Item No.: 8.002.112.00.00	1 x GSM antenna Item No.: 8.002.101.00.00	
Device types with Wi-Fi modem	NOTE:		
MDH 811; MDH 831; MDH 841	<p>If one of these parts is missing or damaged, contact the following address:</p> <p style="text-align: center;">MB connect line GmbH Winnettener Str. 6 D-91550 Dinkelsbühl, Germany</p> <p style="text-align: center;">Tel.: +49 (0)9851/58 25 29 0 Fax: +49 (0)9851/58 25 29 99</p>		
			
1 x Wi-Fi antenna; Item No.: 8.002.107.00.00			

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.

10 Display, controls and connectors

10.1 Front view of device



- 1 Function/status LEDs
- 2 WAN interfaces
- 3 USB Host 2.0
- 4 Dial Out button
- 5 Reset button
- 6 Serial port COM2
- 7 LAN ports 1 – 4 4-Port-Switch
- 8 Serial port COM1

Function / status LEDs

LED	LED colour	LED Status	Description
Fc1	Orange	off	No data traffic on COM1 - incoming
		flashes	Data traffic on COM1 - incoming
	Green	off	No data traffic on COM1 - outgoing
		flashes	(slowly 1 Hz) Data traffic on COM1 - outgoing
		flashes	(very fast 5 Hz) after the device starts with factory settings: SIMPLY.connect* ready but disabled . This means: The SIMPLY.connect function is supported by the device. As long as the function is not activated by pressing the Dial Out button, the device remains in "normal mode" and no further action takes place. If you do not want to use the Simply.connect function, simply ignore this display.
on	SIMPLY.connect* ready and activated . Activation takes place by pressing the Dial Out button. The device tries to establish a connection to the SIMPLY.connect server. This function is only available if the device is set to its factory settings.		
Fc2	Orange	off	No data traffic on COM2 - incoming
		flashes	Data traffic on COM2 - incoming
		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
		flashes	GSM devices: Blink frequency 1 Hz == 20 % – 50 % reception quality
	Green	off	GSM devices: Reception quality display depends on Fc4

LED	LED colour	LED Status	Description
		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
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 mbCONNECT24 portal: User is connected to the device.

***SIMPLY.connect** is a web application that helps you to set up a device (mbNET) in the Remote **Service Portal mbCONNECT24**.

To activate the function, press the Dial Out button until Fc1 lights up. If you do not want to use SIMPLY.connect, simply ignore the flashing LED Fc1.

More information is available at: <https://simplyconnect.mbconnectline.com/>

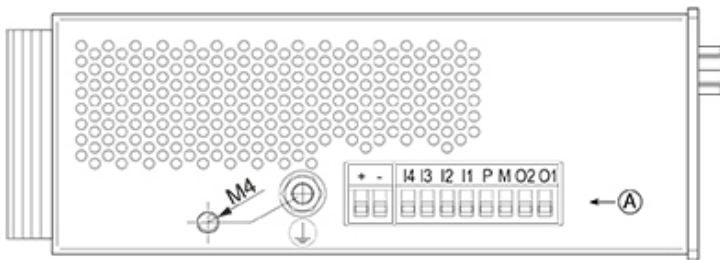
Interfaces

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
COM1	–	COM1 port for connecting devices with RS232/RS485, RS422 interface.
COM2	–	COM2 port for connecting devices with RS232/RS485, RS422 interface, or depending on the router type, devices with MPI /PROFIBUS interface.

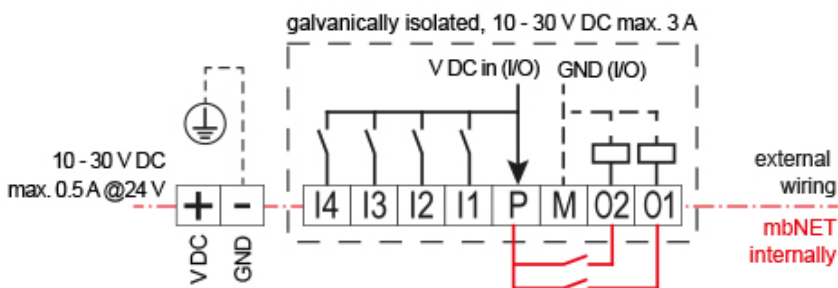
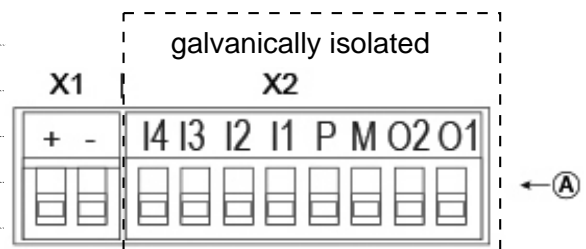
Button

Designation	Description
Dial out	This button is used among other things, to <ul style="list-style-type: none"> a) establish an Internet or VPN connection (keep the button pressed until the LED Con starts flashing) or b) activate the SIMPLY.connect function, wenn LED Fc1 is flashing (5 Hz).
Reset	After pressing the button, the router is restarted (cold start).

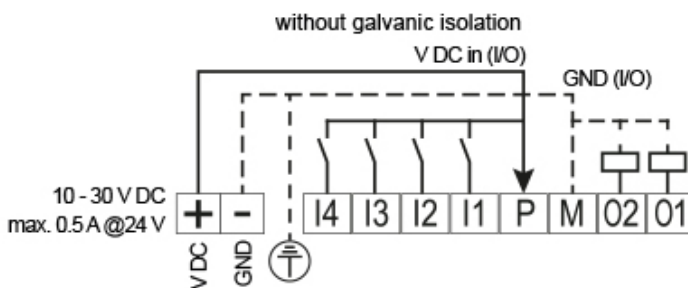
10.2 View at the top of the device



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

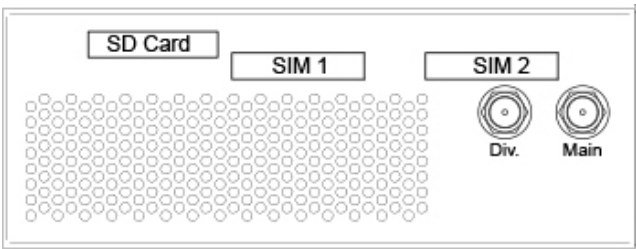
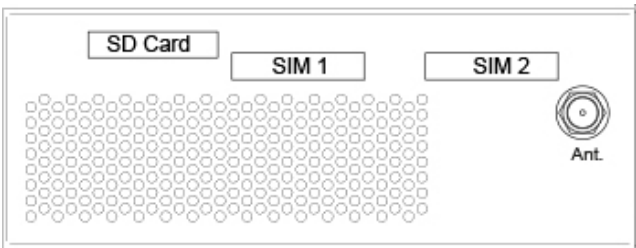
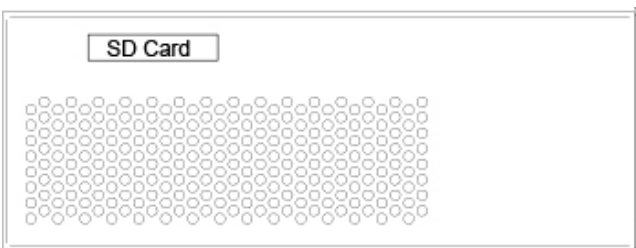


Circuit diagram **with** galvanic isolation of X1 and X2



Circuit diagram **without** galvanic isolation of X1 and X2

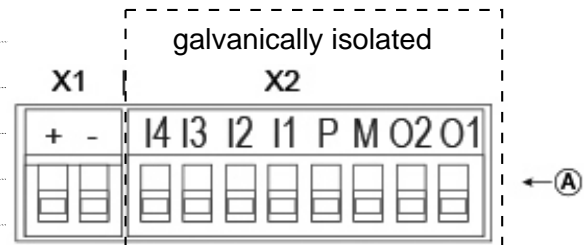
10.3 View of underside of device

Devices with LTE (4G) modem	Type	Equipment
	MDH 850 MDH 855 MDH 858 MDH 859	1 x SD card slot 2 x SIM card slot 2 x SMA socket for GSM antenna (MIMO)
Devices with UMTS (3G) modem	Type	Equipment
	MDH 814 MDH 818 MDH 834 MDH 849	1 x SD card slot 2 x SIM card slot 1 x SMA socket for GSM antenna
Devices with Wi-Fi modem	Type	Equipment
	MDH 811 MDH 831 MDH 841	1 x SD card slot 1 x RP-SMA socket for Wi-Fi antenna
Devices with analogue modem	Type	Equipment
	MDH 810 MDH 815 MDH 830	1 x SD card slot 1 x RJ11 socket
Standard devices	Type	Equipment
	MDH 816 MDH 835	1 x SD card slot

11 Interface assignment

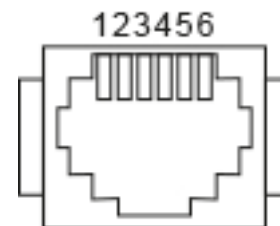
11.1 Pin assignment of terminal blocks X1 and X2 on the top of the device

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



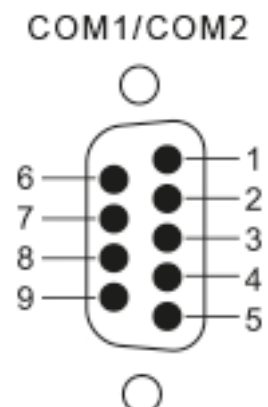
11.2 Pin assignment of the RJ11 socket on the bottom of the device

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



11.3 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.

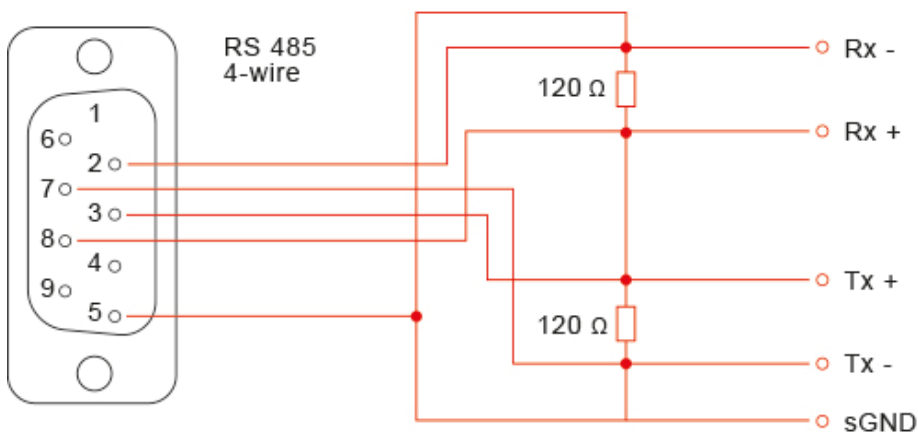


Image 2: Connection example for the 4-wire operation

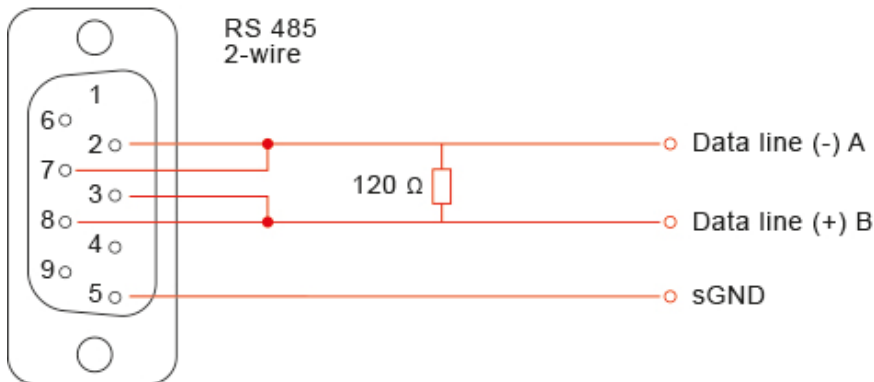
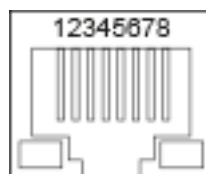


Image 3: Connection example for the 2-wire operation

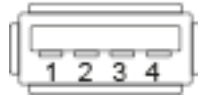
11.4 Pin assignment LAN/WAN port on front of device

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



11.5 Pin assignment USB port on front of device

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



12 Router Installation

Installation position/minimum clearances

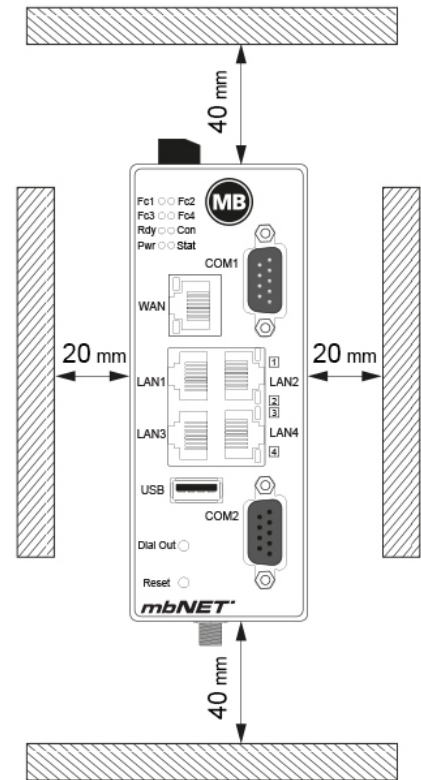
The router is designed to be mounted on DIN top hat rails (in accordance with DIN EN 50 022) and for installation in a control cabinet.

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

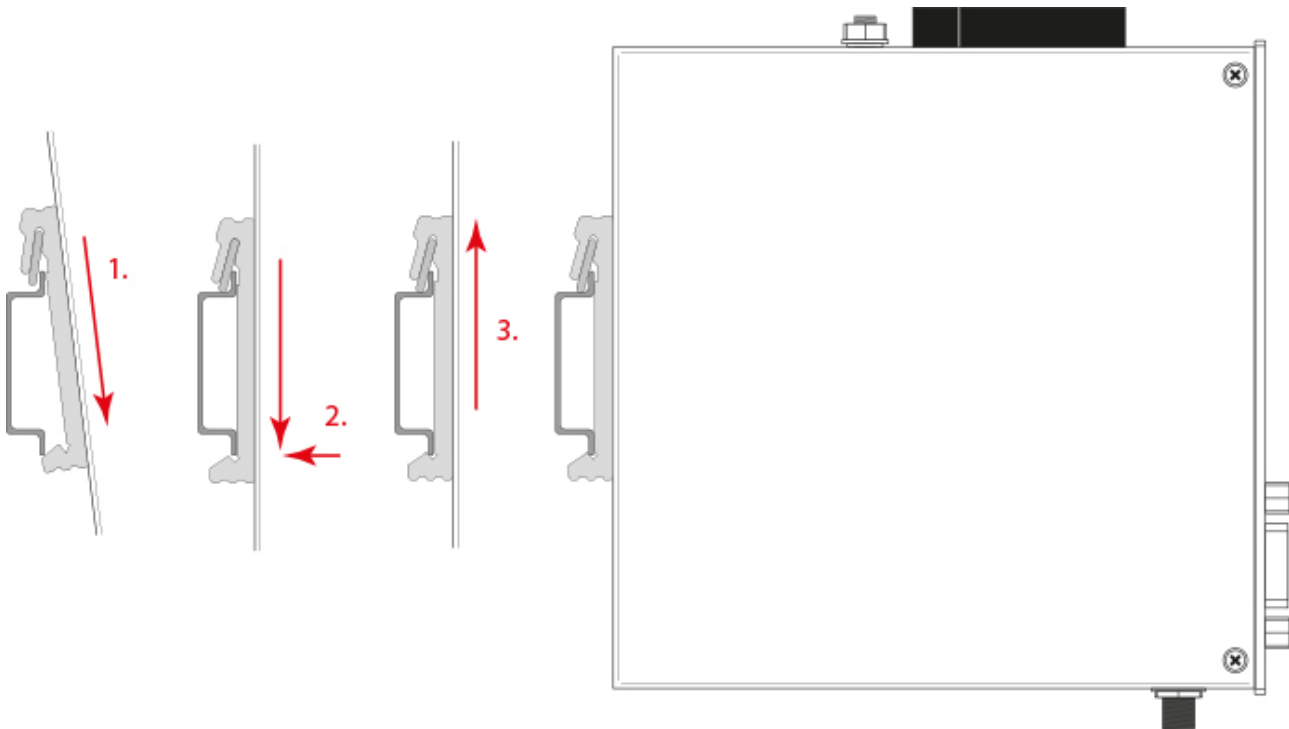
The router may be only mounted vertically as described.

NOTICE

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



Top hat rail mounting

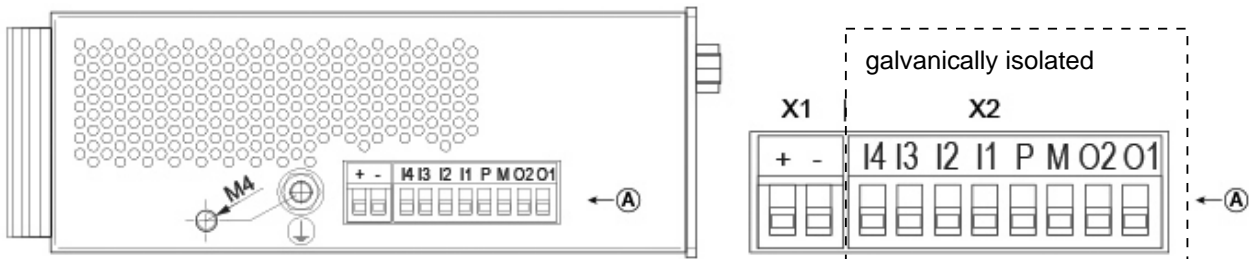


Click the router into the DIN top hat rail. To do this, attach the upper guide to the top hat rail and then press the router down against the top hat rail until it fully engages.

13 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.

Note that the grounding screw and the device housing with the 0 V potential of the power supply are electrically connected to terminal X1.

- 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

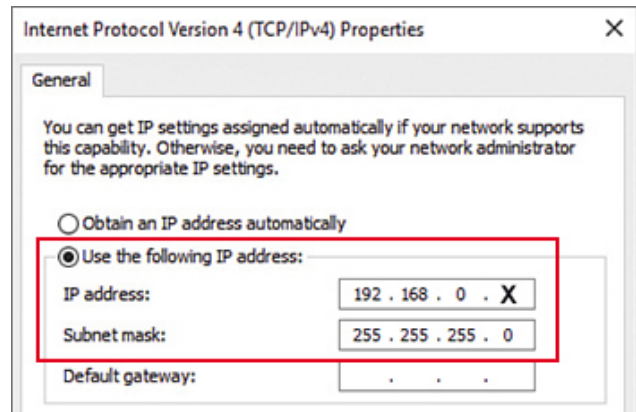
You can obtain further information about the **mbNET** industrial router and support on our homepage in the Support-Forum at www.mbconnectline.com

14 Connect router to configuration PC

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

Requirement:

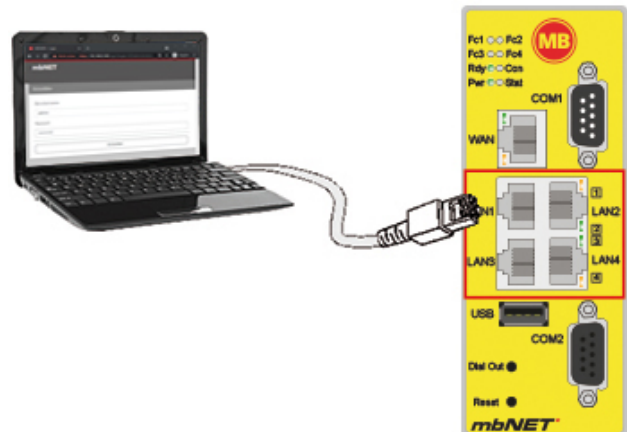
- PC with network card
- Internet browser (HTML5 compatible)
- The IP address of the computer must be in the same network as the mbNET - 192.168 in this case. 0 . X (X = variable) - and not be occupied by any other network user.
- The netmask must be 255.255.255.0.



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.

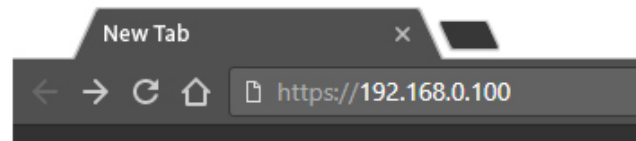
When your mbNET is ready for operation (LED Pwr + Rdy light up), connect the PC to one of the LAN interfaces of the device. To do this, use the supplied network cable.



15 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).

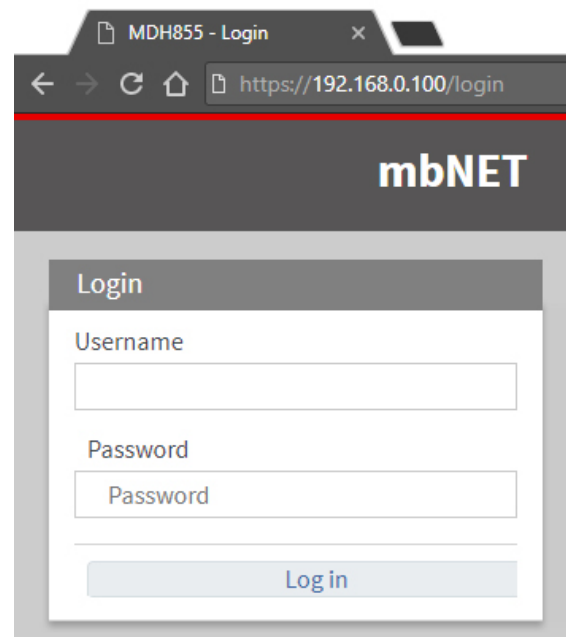
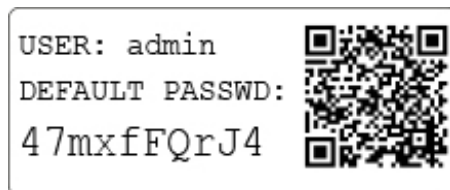
Log in to the router -

Factory setting is:

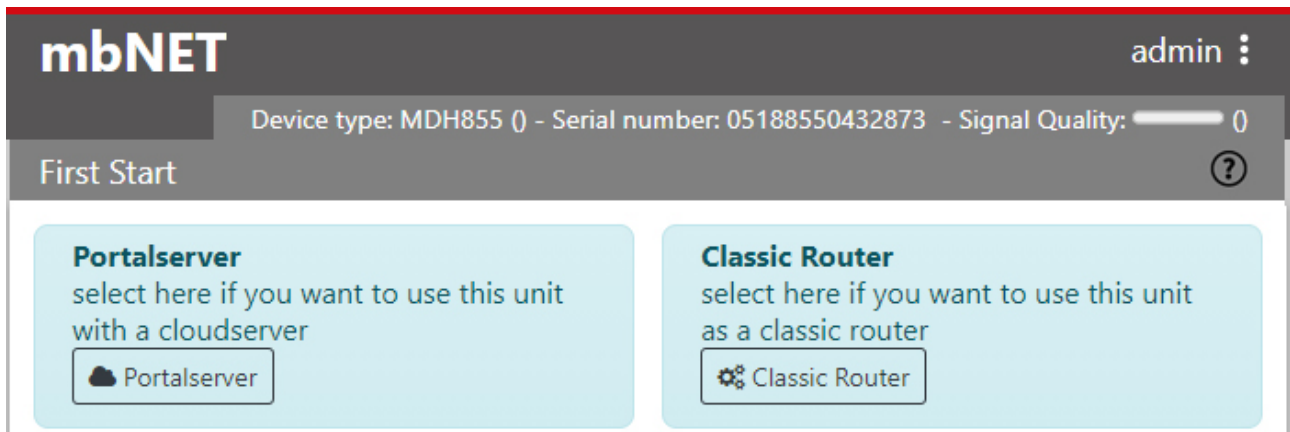
User name: admin

Password:

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



16 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.

17 Portal server - First start

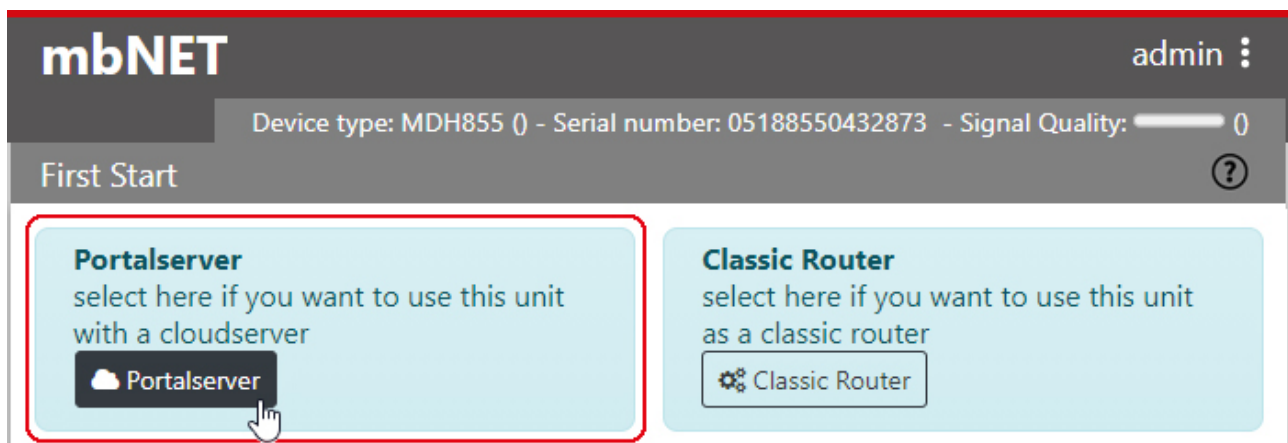
Setting the connection data to the Cloudserver (optional)

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

- to the Internet and
- 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.

17.1 Internet - Configuring the Internet connection

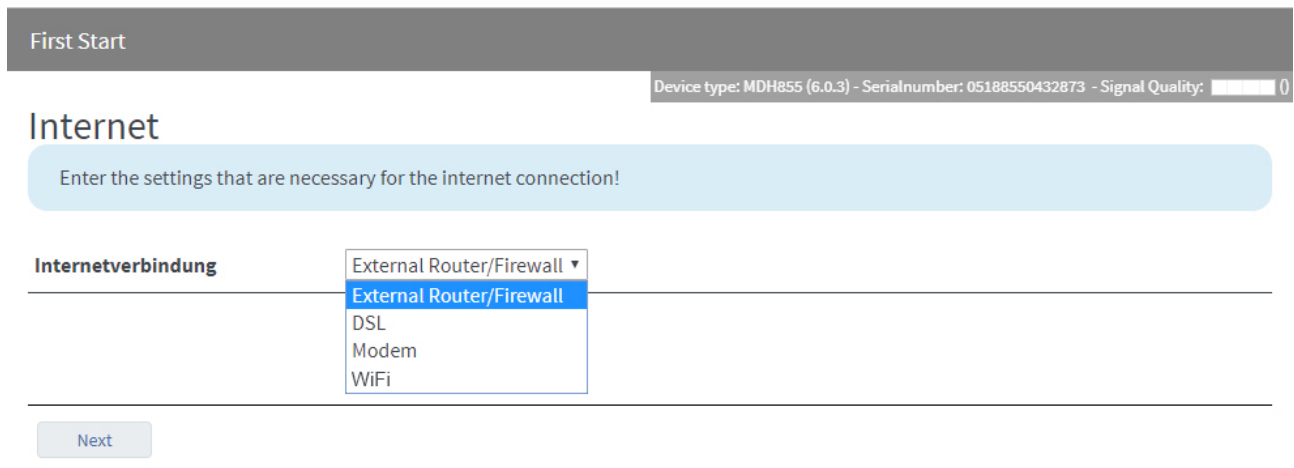


Image 4: the selection may vary depending on the device type

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

Depending on the device type, the selection is

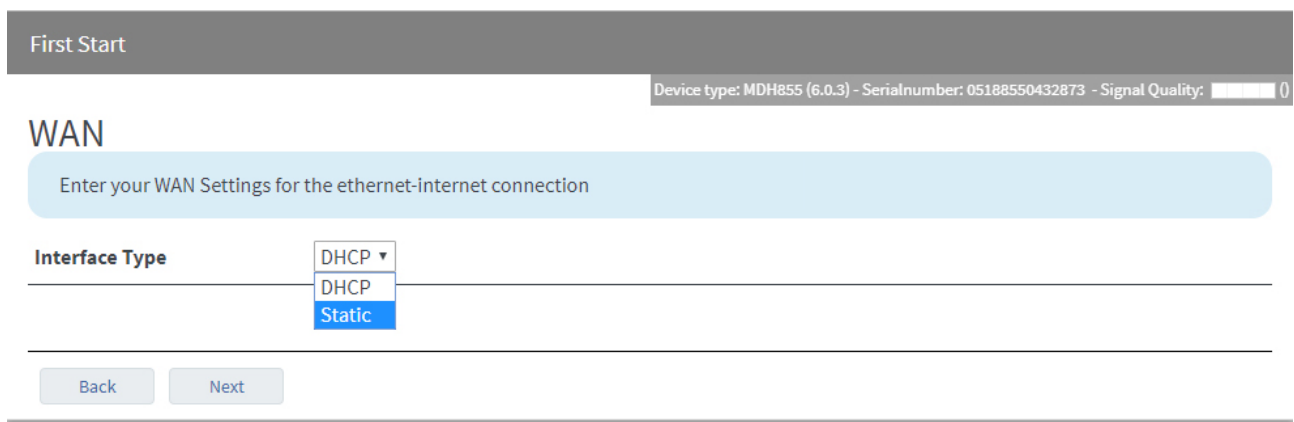
- **External Router/Firewall**
- **DSL**
- **Modem**
- **Wi-Fi**

17.1.1 External Router/Firewall WAN settings

Interface type selection

Options are:

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



DHCP

If interface type **DHCP** 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.

First Start

Device type: MDH855 (6.0.3) - Serialnumber: 05188550432873 - Signal Quality: 0

WAN

Enter your WAN Settings for the ethernet-internet connection

Interface Type	<input type="text" value="Static"/>
WAN IP Address	<input type="text" value="192.168.1.100"/>
Subnetmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.1.1"/>

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**.

17.1.2 DSL Settings

First Start
Device type: MDH855 (6.0.3) - Serialnumber: 05188550432873 - Signal Quality: 0

DSL

Enter your WAN Settings for the ethernet-internet connection

PPP Type	<input type="text" value="PPPoE"/>
User	<input type="text" value="User"/>
Password	<input type="text" value="Password"/>
Password confirmation	<input type="text" value="Password confirmation"/>

Back
Next

Designation	Description
PPP Type	Selection field for the PPP-type: <ul style="list-style-type: none"> PPPoE enable Point-to-Point Protocol over Ethernet. Protocol used to connect via ADSL to the Internet. PPTP enable Point-to-Point Tunnelling Protocol. Protocol used for a transmission method with tunnelling.
User	Enter the user name and password for your point-to-point connection. This information is provided by your Internet Service Provider (ISP).
Password	
Password Confirmation	

NOTICE

If you use this setting, then the router expects that a DSL modem is directly connected to the WAN interface!

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

17.1.3 Modem Connection Settings

First Start
Device type: MDH855 (6.0.3) - Serialnumber: 05188550432873 - Signal Quality: 0

Modem

Enter your WAN Settings for the modem-internet connection

Network (Provider)	<input type="text" value="United Mobile"/>
APN (Access Point Name)	<input type="text"/>
SIM Pin	<input type="text" value="0"/>
User	<input type="text" value="user"/>
Password	<input type="password" value="...."/>

Back
Next

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**.

17.1.4 Wi-Fi Connection Settings

First Start
Device type: MDH831 (6.0.3) - Serialnumber: 13188310034248 - Signal Quality: (0)

WiFi

Enter your WAN Settings for the wifi-internet connection

SSID	<input style="width: 95%;" type="text"/>
Authentication Mode	<input style="width: 95%;" type="text" value="WPA2PSK"/>
Encryption Mode	<input style="width: 95%;" type="text" value="AES"/>
WLAN - Key	<input style="width: 95%;" type="text"/>
Interface Type	<input style="width: 95%;" type="text" value="Static"/>
WLAN IP Address	<input style="width: 95%;" type="text"/>
Subnetmask	<input style="width: 95%;" type="text"/>
Gateway	<input style="width: 95%;" type="text"/>

Back
Next

Designation	Description
SSID	Enter the name of the Wi-Fi network to which the device should connect.
Authentication mode	Select the authentication method from the drop-down list.
Encryption method	Select the encryption method from the drop-down list.
Wi-Fi key	Enter the authentication key.
Interface type	Selection field for the interface type <ul style="list-style-type: none"> • DHCP • Static
Wi-Fi 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**.

17.2 Portal Server - Settings

First Start
Device type: MDH855 (6.0.3) - Serialnumber: 05188550432873 - Signal Quality: 0

Portalserver

Cloudserver settings

Cloudserverlist	<input type="text" value="rsp.mbCONNECT24.us (US/CAN)"/>
Host address or DNS	<input type="text" value="rsp.mbCONNECT24.us"/>
Session-Key	<input type="text"/>
Portalserver Certificate	<input type="button" value="Browse..."/> No file selected.

Designation	Description
List of portal servers (For more information see the "mbCONNECT24 Server List" table)	List of available portal servers: <ul style="list-style-type: none"> Europe USA/Canada 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
Europe	vpn2.mbconnect24.net	mbCONNECT24 V1* - server location: Europe
USA/Canada	vpn.mbconnect24.us	mbCONNECT24 V1* - server location: USA
rsp.mbCONNECT24.net (EU)	rsp.mbCONNECT24.net	Remote-Service-Portal mbCONNECT24 V2** - server location: Europe

Table 1: mbCONNECT24 server list

mbCONNECT24 server list		
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	<i>customer-specific</i>	mymbCONNECT24

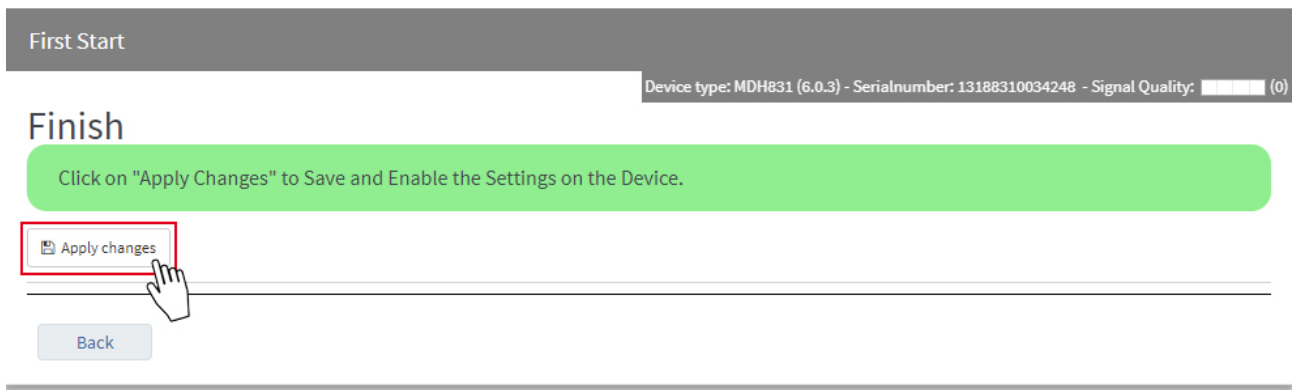
Table 1: mbCONNECT24 server list

* mbCONNECT24 V1 is the previous version of V2 and will not be developed further. However, continued unlimited support and a permanent security upgrade will be provided where the technology allows.

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

17.3 Finish - Apply settings

Save changes



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


Complete

First Start

Device type: MDH831 (6.0.3) - Serialnumber: 13188310034248 - Signal Quality: (0)

Finish

Click on "Apply Changes" to Save and Enable the Settings on the Device.

Take over Firststart configuration	●	 wait ..
Internet	●	
CTM	●	

last configuration check

Redirect to Cloudstatus page	<input type="button" value="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.

18 Quick Start - Cloud Status Page

18.1 Quick Start

MDH831WiFi admin ?

Quickstart Diagnosis IoT

Gerätetyp: MDH831 (6.0.3) - Seriennummer: 13188310034248 - Signalstärke: [signal bar] (-69 dBm)

1. MDH831 ✓
2. ↓ ✓
3. 🌐 ⚠
4. ↓ ✓
5. ☁ ✓

● **WLAN :**
IP Adresse : 192.168.2.179
Subnetzmaske : 255.255.255.0
Gateway : 192.168.2.253
DNS : 172.25.255.250, 8.8.8.8, 172.25.255.250
[WLAN Protokollierung]

● **WAN (DHCP)**
IP Adresse :
Subnetzmaske :
Gateway : 172.25.255.253
DNS : 172.25.255.250, 8.8.8.8, 172.25.255.250

Firmwareversion : 6.0.3
Datum/Uhrzeit lokal : Thu Jun 21 10:47:21 UTC 2018

Diagnose


[Erweiterte Protokollierung]
[Netzwerk]
[Firewall]
[Support Daten]



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.

1. MDH831  In **Step 1**, you will receive an overview of interfaces and general system information.

2.   **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: Click on the "Start CTM" button to initiate a manual query for an available portal configuration.

last configuration check:

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.

18.2 Diagnosis

The screenshot shows the MDH831WiFi diagnostic interface. At the top, there's a header with 'MDH831WiFi' and 'admin' with a help icon. Below the header are navigation tabs: 'Quickstart', 'Diagnosis', and 'IoT'. A status bar indicates 'Device type: MDH831 (6.0.3) - Serialnumber: 13188310034248 - Signal Quality: [signal strength icon] (-67 dBm)'. The main content area has several sections, each with a text input field and a button:

- Ping:** Input field contains 'google.com', button is 'Ping'.
- TraceRoute:** Input field contains 'google.com', button is 'TraceRoute'.
- NS Lookup:** Input field contains 'google.com', button is 'NS Lookup'.
- TCPDUMP:** Input field contains '-i eth0 not port 443', button is 'TCPDUMP'.
- Return Message:** Below this section, the output of the 'TraceRoute' command is shown:


```
tracert to google.com (172.217.23.174), 30 hops max, 38 byte packets
 1tracert: sendto: Operation not permitted
```

Image 5: 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.

Designation	Description
TCPDUMP	<p>In order to closely monitor the network traffic, you can use the "TCPDUMP" command. Some examples of the use of this command are:</p> <ul style="list-style-type: none"> • -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. <p>You can find detailed TCPDUMP documentation at www.tcpdump.org</p>
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.

18.3 IoT

MDH831WiFi
admin ⋮ ?

Quickstart Diagnose IoT

Gerätetyp: RKH210 (6.0.6) - Seriennummer: 08192100042754

Informationen	
Seriennummer	E000016
Lizenz-Typ	advance
Docker	
Service	Aktiviert
Daemon	●
Docker Management	
Service	Deaktiviert
Link zu User Interface	🔗 Management
Flows und Dashboard	
Service	Aktiviert
Daemon	●
Link zu Flows(Node-Red)	🔗 Flows
Link zu Dashboard(Node-Red)	🔗 Dashboard

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>

19 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.

19.1 Description of the graphical user interface (configuration interface)

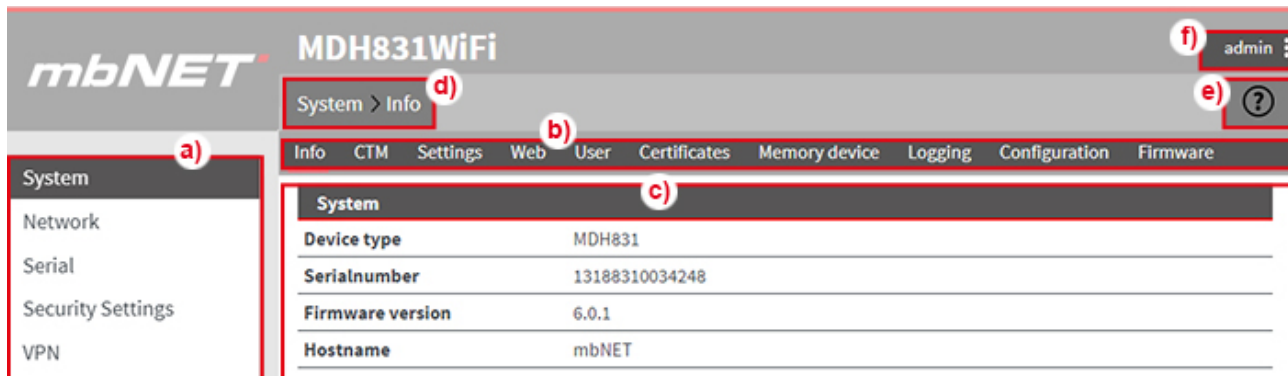













Image 6: Basic structure of the graphical user interface

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.								
		<table border="1"> <tr> <td>Log out</td> <td>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.</td> </tr> <tr> <td>Quick start/ Administration</td> <td>Link to "Quick Start"/to configuration Interface</td> </tr> <tr> <td>Reboot</td> <td>If you click on this link, mbNET will be restarted.</td> </tr> <tr> <td>Language</td> <td>Selection field for the user language of the web interface The options are: German and English</td> </tr> </table>	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
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									


19.2 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.
	Selection field/Drop-down list to select a predefined value/parameter.
	The Editbutton 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 Deletebutton .
	Clicking on the "Save" button temporarily saves the current entries/changes. However, the changes are not active.
	Clicking on the "Close" button discards the current input/changes.

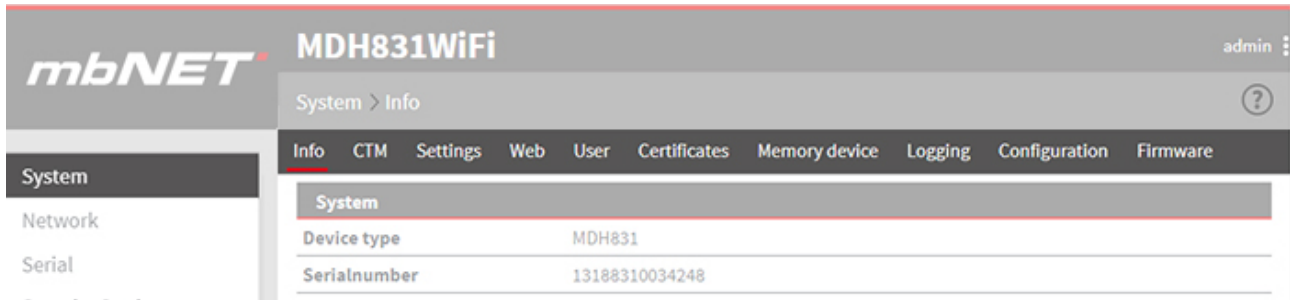
NOTICE

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.

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

20 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 <i>mbNET</i> 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.

20.1 System > Info

System > Info ?

Info CTM Einstellungen Web Benutzer Zertifikate Speichermedien Protokollierung Konfiguration Firmware

System	
Device type	MDH855
Serialnumber	27198160046490
Firmware version	6.2.4
Hostname	mbNET
last error message	[Mar 22 09:55:52] > : CME Error [10]: SIM not inserted

Network			
Interface	Cable	IP Address	MAC Address
LAN	●	192.168.0.100	70:B3:D5:8D:90:C6
WAN	●	172.16.20.191	70:B3:D5:8D:90:C7

Internet	
External Router/Firewall	● Connection established

Interfaces			
Interface	RS-Type	Driver	Port
COM1	RS232	Allen Bradley 19200	7001
COM2	MPI/PROFIBUS	MPI/PROFIBUS Network Driver	7002

Flash drive	SD Card
●	●

Image 7: Example display, content can vary depending on the type of device.

System	<p>Here you will find information about</p> <ul style="list-style-type: none"> Device type Serial number Firmware version Device name in the network <p>Warnings or/and the most recent error are also displayed here.</p>
Network	<p>Here you will find information about</p> <ul style="list-style-type: none"> 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 <ul style="list-style-type: none">• the selected Internet connection<ul style="list-style-type: none">◦ 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. <p style="text-align: right;">* depending on the type of device and equipment.</p>
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.

20.2 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.

System > CTM ?

Info CTM Settings Web User Certificates Memory device Logging Configuration Firmware


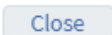
CTM ✎

CTM is	Inactive
Host address or DNS	ctm.mbconnect24.net

Click the Edit icon  to edit the corresponding function.

CTM

Active	<input type="text" value="No"/>
Host address or DNS	<input type="text" value="rsp-vpn.mbconnect24.net"/>
Session-Key	<input type="text"/>
Enable connection through a HTTP proxy	<input type="text" value="Yes"/>
HTTP proxy, skip the certificate check	<input type="checkbox"/>
HTTP proxy name	<input type="text"/>
HTTP proxy port	<input type="text"/>
HTTP proxy username	<input type="text"/>
HTTP proxy password	<input type="text"/>

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" <i>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."</i> 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
	Clicking on " Save " temporarily saves the current entries/changes. But the changes are not yet enabled.
	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_\(Rechnernetz\)](https://de.wikipedia.org/wiki/Proxy_(Rechnernetz)), 18.01.2018


20.3 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	<ul style="list-style-type: none"> Assign a device name in the network Configure a device reboot
Time settings	<ul style="list-style-type: none"> Set the local time (date/time) Select the time zone
NTP Settings	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> • 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.

20.3.1 System > Settings > System Settings

System settings

Hostname	<input type="text" value="mbNET"/>
Host Description	<input type="text" value="mbNET"/>
Automatic reboot	<input checked="" type="checkbox"/>
Reboot at	<input type="text" value="00:00"/>

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.

<input type="button" value="Save"/>	Clicking on "Save" temporarily saves the current entries/changes. But the changes are not yet enabled.
<input type="button" value="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.

20.3.2 System > Settings > Time Settings

Time Settings ✎	
Date Time (UTC)	Tue Dec 3 15:05:09 UTC 2019
Locale Date Time	Tue Dec 3 16:05:09 CET 2019
Set locale Date Time	2019.02.20-09:02:21
Timezone	Berlin,Germany

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.

Time Settings

Set locale Date Time	<input type="text" value="2019.02.20-09:02:21"/>
Timezone	<input type="text" value="Berlin,Germany"/>

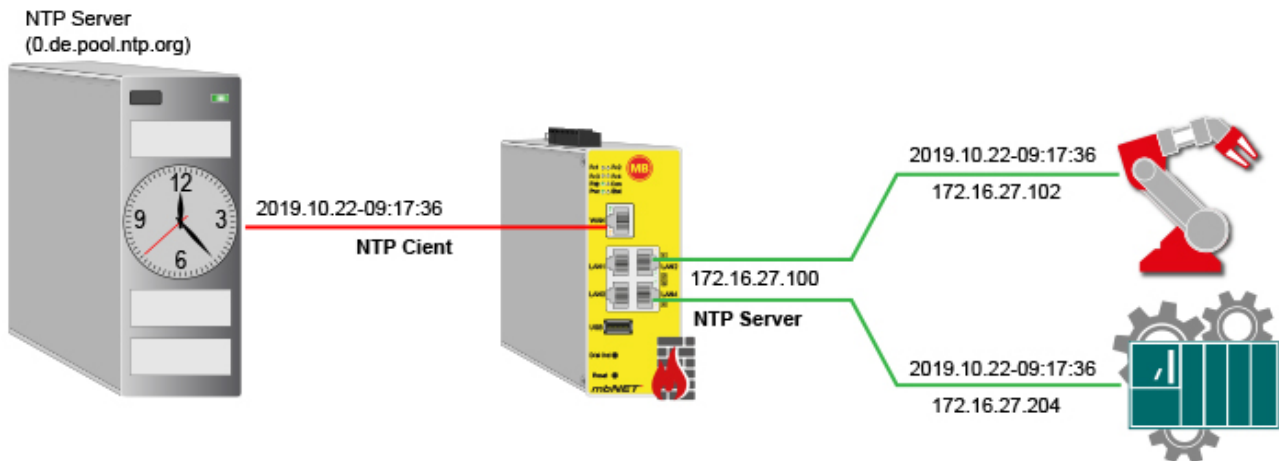
Designation	Description
Date/Time (UTC)	Displays the current system time in UTC (Coordinated Universal Time).
Local Date Time	Displays the current system time based on the selected time zone.
Set local Date Time	Enter the system time here, if no automatic time synchronization is possible or is to take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

<input type="button" value="Save"/>	Clicking on "Save" temporarily saves the current entries/changes. But the changes are not yet enabled.
<input type="button" value="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.

20.3.3 System > Settings > NTP Settings


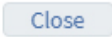


The Network Time Protocol (NTP) is a standard for synchronizing clocks in computer systems via package-based communication networks. When time synchronization, the NTP client gets the current time from an NTP server.

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. <div style="text-align: center;">NOTICE</div> 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.
	Clicking on " Save " temporarily saves the current entries/changes. But the changes are not yet enabled.
	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.

20.3.4 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.

Mail Settings	
Activate automatic Mail	<input type="text" value="No"/>
SMTP Server	<input type="text"/>
SMTP Port	<input type="text" value="25"/>
E-Mail address	<input type="text"/>
SMTP requires Authentication	<input type="checkbox"/>
User	<input type="text"/>
Password	<input type="text"/>

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 Authentication	Activate the checkbox if the SMTP server requires authentication.
User /Password	In these two fields, enter the login information for your E-mail account.
<input type="button" value="Save"/>	Clicking on " Save " temporarily saves the current entries/changes. But the changes are not yet enabled.
<input type="button" value="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.

20.3.5 System > Settings > Device-API

The mbNET can be used as an MQTT broker.

Device-API Settings

Enable MQTT access to status topics

MQTT Password

MQTT-Username

Attention: This setting opens Port 1883/TCP on LAN interface

Designation	Description
Enable MQTT access to status topics	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!

<input type="button" value="Save"/>	Clicking on "Save" temporarily saves the current entries/changes. But the changes are not yet enabled.
<input type="button" value="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.

Status > System ?

< DynDNS NTP VPN-OpenVPN IoT Runtime Diagnosis Memory devices Alarm manager System

System-Usage System information MQTT Debug List

Topic	Value
/network/lan/state/led	2
/network/lan/mac	70:B3:D5:F9:43:EB
/network/lan/ip	192.168.0.100

20.3.6 System > Settings > System Service

System Services

Networkconfiguration disable (Conftool)	<input type="checkbox"/>
SimplyConnect (SC3) service enable	<input type="checkbox"/>
Manufacturer access enable	<input type="checkbox"/>

Save

Close

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.

20.4 System > WEB

System > Web ?

Info CTM Settings Web User Certificates Memory devices Logging Configuration Firmware

HTTPS device configuration access ✎

HTTPS Port	443
------------	-----

System Services ✎

Enable access to Quickstart WITHOUT credentials	No
Enable login via GET-Arguments	No
Disable Communication Webservice (SMS/Email)	Yes
Disable Web configuration (only changeable via factory settings reload!)	No

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

HTTPS device configuration access	
Function	Description/content
HTTPS Port	Here you can <ul style="list-style-type: none"> • change the default port (443), through which the HTTPS server is accessed. <ul style="list-style-type: none"> ◦ 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 Communication 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.

20.4.1 System > Web > HTTPS access for device configuration

System Services

Enable access to Quickstart WITHOUT credentials	<input type="checkbox"/>
Enable login via GET-Arguments	<input type="checkbox"/>
Disable Communication Webservice (SMS/Email)	<input checked="" type="checkbox"/>
Disable Web configuration (only changeable via factory settings reload!)	<input type="checkbox"/>

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!

<input type="button" value="Save"/>	Clicking on " Save " temporarily saves the current entries/changes. But the changes are not yet enabled.
<input type="button" value="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.

20.4.2 System > Web > System Services


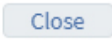
System Services

Enable access to Quickstart WITHOUT credentials	<input type="checkbox"/>
Enable login via GET-Arguments	<input type="checkbox"/>
Disable Communication Webservice (SMS/Email)	<input checked="" type="checkbox"/>
Disable Web configuration (only changeable via factory settings reload!)	<input type="checkbox"/>

Save

Close

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. <code>https://192.168.0.100/login?username=[USERNAME]&password=[PASSWORD]</code>
Disable Communication 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.
	Clicking on " Save " temporarily saves the current entries/changes. But the changes are not yet enabled.
	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.




20.5 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.

User-name	Password	Full name	Adminis-tration	Quick-start	Modem Dialin	VPN Dialin	Flows(Node Red) Admin	Docker Management Admin	
admin	*****	Administrator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	 

By clicking on the relevant button users can be

- 1 added 
- 2 edited 
- 3 deleted 

20.5.1 Added/Edited User

User management	
Username	<input type="text" value="admin"/>
Full name	<input type="text" value="Administrator"/>
Administration	<input checked="" type="checkbox"/>
Quickstart	<input checked="" type="checkbox"/>
Modem Dialin	<input checked="" type="checkbox"/>
VPN Dialin	<input checked="" type="checkbox"/>
Flows(Node Red) Admin	<input type="checkbox"/>
Old password	<input type="text"/>
Change password	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

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	Check boxes to enable/disable the type of access by the user to the web interface of the mbNET.
Dial-up modem	<ul style="list-style-type: none"> Administration => access via HTTPS
VPN dial-up	<ul style="list-style-type: none"> Dial-up modem => access via dial-up modem
Flows(Node Red) Admin	<ul style="list-style-type: none"> VPN dial-up => access by dialling through a VPN tunnel Flows(Node Red) Admin => access Node-Red and Dashboards
Docker Management Admin	<ul style="list-style-type: none"> 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).

<input type="button" value="Save"/>	Clicking on "Save" temporarily saves the current entries/changes. But the changes are not yet enabled.
<input type="button" value="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.

20.6 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.

Name	Subject	Issuer	Valid
------	---------	--------	-------

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.

20.6.1 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 PKCS12 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 PKCS12 file consists of a *.crt file and a * key .pem file.

20.6.1.1 Import own certificate

import new certificate

File	<input type="button" value="Datei auswählen"/> Clientcert1.p12
Name for this certificate (optional)	<input type="text" value="Clientcert1"/>
Password	<input type="password"/>
<input type="button" value="Import"/>	

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**.

System > Certificates ?

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

Own Certificate CA Certificate Partner Certificate CRL

list of imported certificates +

Name	Subject	Issuer	Valid	
Clientcert1	C=DE	C=DE	Jun 26	
	ST=Bayern	ST=Bayern	07:52:00	
	L=Dinkelsbuehl	L=Hamburg	2018 GMT	
	O=MB	O=CustomerA	Jun 26	
	OU=Documentation	OU=Service	07:52:00	
	CN=MasterCertificate	CN=Client1	2019 GMT	
	Address=doku@mbconnectline.com	Address=support@customera.de		

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

20.6.2 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.

20.6.2.1 Importing CA certificate (root certificate)

import new certificate

File DocuCertificate.crt

Name for this certificate (optional)

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**.

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

Own Certificate
CA Certificate
Partner Certificate
CRL

list of imported certificates +

Name	Subject	Issuer	Valid
DocuCertificate	C=DE	C=DE	Jun 25
	ST=Bayern	ST=Bayern	06:10:00
	L=Dinkelsbuehl	L=Dinkelsbuehl	2018 GMT
	O=MB	O=MB	Jun 25
	OU=Documentation	OU=Documentation	06:10:00
	CN=MasterCertificate	CN=MasterCertificate	2023 GMT
	Address=doku@mbconnectline.com	Address=doku@mbconnectline.com	

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

20.6.3 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.

20.6.3.1 Import partner certificate

import new certificate

File	<input type="button" value="Datei auswählen"/> PartnerCertificate.crt
Name for this certificate (optional)	<input type="text" value="PartnerCertificate"/>
<input type="button" value="Import"/>	

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**.

System > Certificates ?

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

Own Certificate CA Certificate **Partner Certificate** CRL

list of imported certificates +

Name	Subject	Issuer	Valid
DocuCertificate	C=DE	C=DE	Jun 25
	ST=Bayern	ST=Bayern	06:10:00
	L=Dinkelsbuehl	L=Dinkelsbuehl	2018 GMT
	O=MB	O=MB	Jun 25
	OU=Documentation	OU=Documentation	06:10:00
	CN=MasterCertificate	CN=MasterCertificate	2023 GMT
	Address=doku@mbconnectline.com	Address=doku@mbconnectline.com	

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

20.6.4 CRL (revocation list)

The recover/revocation list (**C**ertificate **R**evocation **L**ist CRL, for short) checks whether the certificates of 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.

20.6.4.1 Import CRL (revocation list)

import new certificate

File DocuCertificate.pem

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

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

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

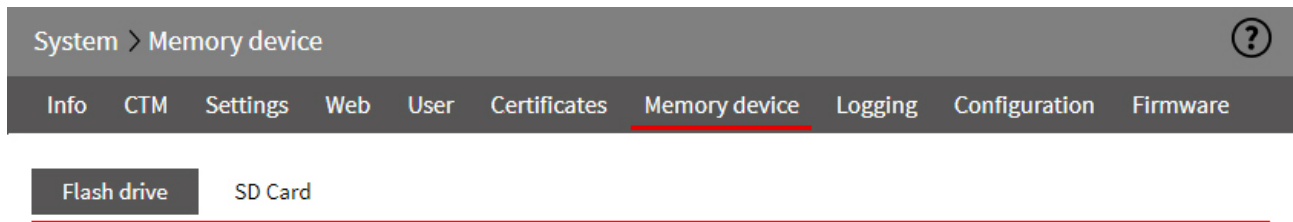
Own Certificate CA Certificate Partner Certificate CRL

list of imported certificates +

Issuer	Update address	Last update	Next update	
C=DE ST=Bayern L=Dinkelsbuehl O=MB OU=Documentation CN=MasterCertificate emailAddress=doku@mbconnectline.com		Jun 27 14:01:00 2018 GMT	Jul 27 14:01:00 2018 GMT	x

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

20.7 System > Memory devices

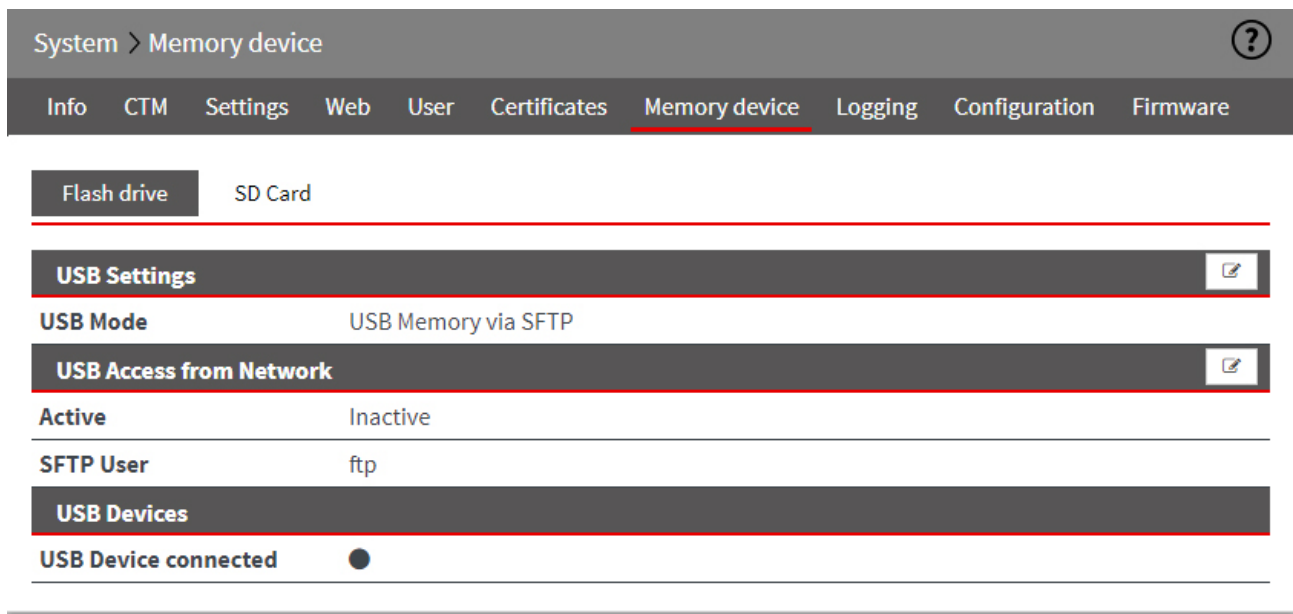


The mbNET has

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

20.7.1 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.



20.7.1.1 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**

20.7.1.2 USB access from the network

USB Access from Network

Active	<input checked="" type="checkbox"/>
SFTP User	ftp
SFTP Password	...
SFTP Password confirmation	

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**.

20.7.1.3 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.

USB Devices

USB Device connected



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.

20.7.2 SD Access from network

SD Access from Network

Active



SFTP User

nodered

SFTP Password

.....

SFTP Password confirmation

.....

Save

Close

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**.

20.8 System > Logging

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

System > Logging ?


[Info](#) [CTM](#) [Settings](#) [Web](#) [User](#) [Certificates](#) [Memory device](#) [Logging](#) [Configuration](#) [Firmware](#)

General ✎

Set debug output to syslog	Inactive
Log also to USB-Device	Inactive

Remote Logging ✎

Enable Remote logging	Inactive
Remote IP Address	192.168.0.1
Remote Port	514

Click the Edit icon  to edit the corresponding function.

20.8.1 General Settings

General

Set debug output to syslog	<input type="checkbox"/>
Log also to USB-Device	<input type="checkbox"/>

Save
Close

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.

20.8.2 External logging (server settings)

Remote Logging

Enable Remote logging	<input type="checkbox"/>
Remote IP Address	<input type="text" value="192.168.0.1"/>
Remote Port	<input type="text" value="514"/>

Save
Close

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.

20.9 System > Configuration (backup and restore)

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


System > Configuration ?

Info CTM Settings Web User Certificates Memory device Logging Configuration Firmware

Backup Configuration ✎

Name this configuration mbNET


Restore Configuration ✎

Click the Edit icon  to edit the corresponding function.

20.10 System > Firmware (Firmware update)

System > Firmware ?	
Info CTM Settings Web User Certificates Memory devices Logging Configuration Firmware	
Firmware Device	
Firmware version	6.2.3
Active Bootvolume	VOL1
Firmware update ✎	
Upgrade Method	Autoupdate server
Firmware version status	stable
Available Firmware version	6.2.4 i
Start firmware update	<input type="button" value="▶ Start"/>
Progress	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>
automatic Firmware version check and update ✎	
Active	No

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.

Firmware update	
Upgrade Method	Autoupdate server ▼
Firmware version status	Firmware Status: stable ▼

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

automatic Firmware version check and update 

Active

No

Firmware update

Check every 24 hours if there is a new Firmware and install it

No

Save

Close

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.

20.10.1 Firmware update

Firmware update

Upgrade Method

Autoupdate server

Firmware version State

Firmware State: stable

Available Firmware version 6-2-4

Start

Close

Designation	Description
Upgrade Method	Selection field with the following options: <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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).

21 Network - connection settings and options

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

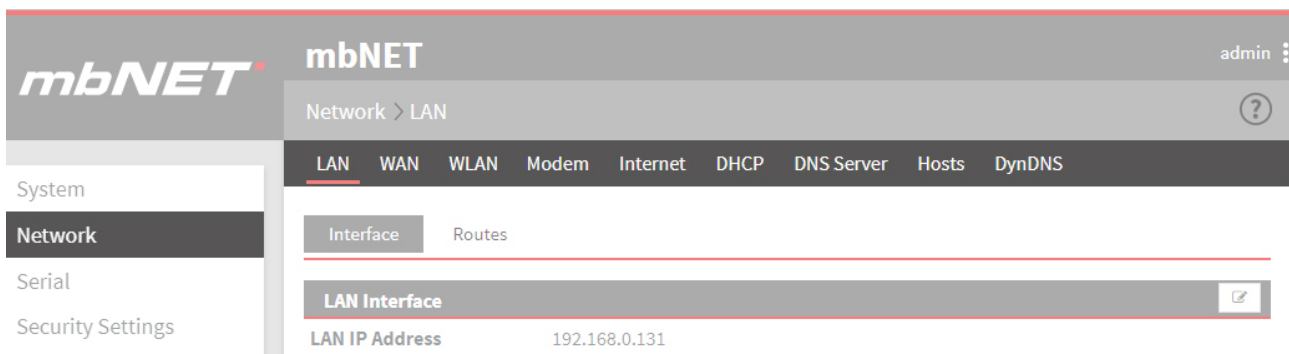


Image 8: Example display, content can vary depending on the type of device.

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.


21.1 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.

21.1.1 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.

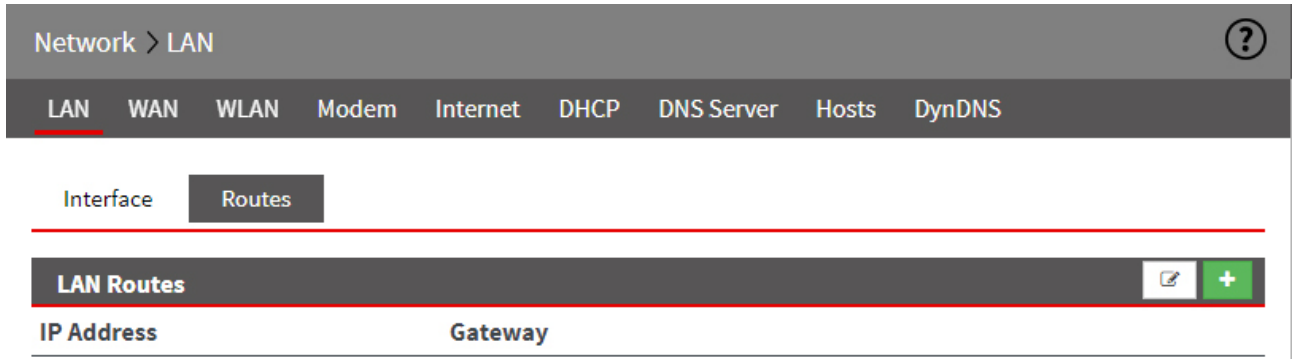
Network participants	
Monitors network participants	Disabled <input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	
Designation	Description
Monitors network participants	Selection box to <ul style="list-style-type: none"> • Disable • Passive
<input type="button" value="Save"/>	Clicking on " Save " temporarily saves the current entries/changes. But the changes are not yet enabled.
<input type="button" value="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.

21.1.2 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

LAN Routes

IP Address	Gateway

Save
Close

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.

Network > LAN ?

[LAN](#) [WAN](#) [WLAN](#) [Modem](#) [Internet](#) [DHCP](#) [DNS Server](#) [Hosts](#) [DynDNS](#)

Interface
Routes

LAN Routes

IP Address	Gateway		
172.27.17.0/24	192.168.0.100		
172.16.20.158	192.168.0.100		

Click the Edit icon , to edit the corresponding entry.

Click the Delete icon , to delete the corresponding entry.

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


21.2 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.

21.2.1 Interface - set WAN interface type

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

The screenshot shows the 'Network > WAN' configuration page. At the top, there are tabs for 'LAN', 'WAN', 'WLAN', 'Modem', 'Internet', 'DHCP', 'DNS Server', 'Hosts', and 'DynDNS'. The 'WAN' tab is selected. Below the tabs, there are two sub-sections: 'Interface' and 'Routes'. The 'Interface' section is active and shows a 'WAN Interface' header with an edit icon. Below this, there is a table with one row: 'Interface Type' with the value 'DHCP'.

Click the Edit icon  to edit the corresponding function.

Select interface type

The options are

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

The screenshot shows the 'WAN Interface' configuration form. It has a header 'WAN Interface' and a sub-section 'Interface Type' with a dropdown menu currently set to 'DHCP'. At the bottom right of the form, there are two buttons: 'Save' and 'Close'.

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.

WAN Interface	
Interface Type	Static
WAN IP Address	192.168.1.100
Subnetmask	255.255.255.0
Gateway	192.168.1.1

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.

21.2.2 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.

Network > WAN ?


LAN
WAN
WLAN
Modem
Internet
DHCP
DNS Server
Hosts
DynDNS

Interface
Routes

WAN Routes

IP Address	Gateway

Click the Add  button to add a route.

Click the Edit icon , to edit the corresponding route.

Add WAN route

WAN Routes

IP Address	Gateway

Save
Close

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.

Network > WAN ?


LAN WAN WLAN Modem Internet DHCP DNS Server Hosts DynDNS



Interface Routes

+

IP Address	Gateway	
192.168.0.0/24	192.168.0.100	✎ ✕
192.168.0.125	192.168.0.100	✎ ✕

Click the Edit icon , to edit the corresponding entry.

Click the Delete icon , to delete the corresponding entry.

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

21.3.1 Interface - set Wi-Fi 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**
- **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.
Static	Select this type if an existing router connects to the Internet and this does not act as a DHCP server, or no address assignment is specified by a server. Select this type, if you have received a static address from your ISP (Internet Service Provider) - e.g., in the case of a dedicated line. Also note that with this type of connection, a DNS server must be entered (see Section Network - DNS servers).

Configuring the Wi-Fi Interface

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

WLAN Interface	
Interface Type	Static ▼
WLAN IP Address	<input type="text"/>
Subnetmask	<input type="text"/>
Gateway	<input type="text"/>

Designation	Description
Wi-Fi IP address	Enter the Wi-Fi 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.

21.3.2 Wi-Fi Settings

You can configure the wireless connection to a wireless router or access point here.



WLAN Settings	
SSID	<input type="text"/>
Authentication Mode	WPA2PSK ▼
Encryption Mode	AES ▼
WLAN - Key	<input type="text"/>
Extended Settings	No ▼

Designation	Description
SSID	Wireless router or access point name.

Designation	Description
Authentication mode	<p>OPEN With this authentication, each mobile station can connect to a Wi-Fi access point, if the SSID match each other. Some Wi-Fi clients know the ALL or ANY options for establishing a connection to each access point regardless of the SSID, provided it is configured as "Open System".</p> <p>SHARED With this authentication, the access point and the mobile station must use the same WPA2 password. If the password does not match the set password, then the access point denies the authentication of the station. A connection cannot be established in that case.</p> <p>WEPAUTO The setting is not unique. It can have different effects depending on the manufacturer or access point. The authentication setting is usually not done by setting the option. Details about the encryption, the code and maybe the encryption strength have to be provided.</p> <p>WPAPSK WPA-PSK is an encryption method that sends data by a pattern, which completely changes the signal. It can be read only if you also have the same pattern with the key (code/key), which you can determine yourself.</p> <p>WPA2PSK WPA2-PSK is the implementation of a high safety standard according to the Wi-Fi standards. It is the successor to WPA and one of the most secure methods of encryption.</p> <p>WPANONE No authentication</p>
Encryption method	<p>NONE No encryption</p> <p>AES AES decryption necessarily requires that the same steps as for encryption must be taken, but in reverse order. In some ways, this is a weakness of AES.</p> <p>WEP WEP is an encryption method based on an RC4 encryption. This is a secure key stored in any Wi-Fi-enabled device, which should not be known to anyone and also not traceable. WEP provides functions for packet encryption and authentication. It is considered outdated and relatively insecure.</p> <p>TKIP TKIP uses the same algorithm as WEP. TKIP also ensures that each data packet gets a different key. Packages that do not fit the algorithm will be discarded immediately.</p>
Wi-Fi key	Enter the Wi-Fi key for the wireless router or access point.
Advanced settings (Expert)	Selection field No/Yes If you select Yes, you can perform more/detailed settings.

Advanced settings (Expert)

Extended Settings	Yes
Operating Frequency	Channel 1-13
Operating Band	Band 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 152
Channel	1
B/G Protection	Auto
RTS Threshold	2347
Frag Threshold	2346
Wmm Capable	Disabler WMM

Designation	Description
Operating frequency	<p>Selection field for setting the channels.</p> <p>Depending on how many devices and base stations need to share the frequency spectrum, you can use the channel settings to split the 2.4 GHz frequency range.</p> <p>Channels 1-11 - This considers Channels 1-11 Channels 1-13 - This considers Channels 1-13 Channels 10,11 - This considers Channels 10 and 11 Channels 10-13 - This considers Channels 10-13 Channels 3-9 - This considers Channels 3-9 Channels 5-13 - This considers Channels 5-13</p>
Operating band	Selection field for the operating band to be used according to IEEE 802.11 Standard
Channel	<p>Selection field for the default channel to be used</p> <p>Auto: The default channel is 1-11: Here you can select a channel from 1 to 11.</p>
Protected Mode in B/G	<p>The Protected Mode selection field</p> <p>Auto always ON always OFF</p>
RTS threshold value	<p>Request-to-send: The RTS is a handshake protocol to prevent data collisions. If the device detects a slower packet, it asks in advance, before the packet is sent. The process can slow down the data throughput. A value of 500 is recommended during use.</p> <p>The default setting is the maximum value of 2347 bytes</p>
Threshold query	<p>Fragmentation affects the data throughput. Here you can set the packet size into which the data packets will be fragmented.</p> <p>Default value is 2346 bytes.</p>
WMM enabled	<p>Selection field if WMM certification is active or inactive.</p> <p>Active WMM: WMM Certification Active Inactive WMM: WMM certification inactive</p>
	Clicking on " Save " temporarily saves the current entries/changes. But the changes are not yet enabled.
	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 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.

21.4.1 Analogue modem configuration

Network > Modem ?

LAN WAN Modem Internet DHCP DNS Server Hosts DynDNS

Modem Settings ✎

Modemtyp	ANALOG
Modem Init	+GCI=FD
Modem Init	X3

Outgoing Incoming Call Back

Credentials ✎

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

Authentication ✎

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


21.4.1.1 Modem Settings

Network > Modem ?

LAN WAN Modem Internet DHCP DNS Server Hosts DynDNS

Modem Settings ✎

Modemtyp	ANALOG
Modem Init	+GCI=FD
Modem Init	X3

Click the Edit icon  to edit the corresponding function.

Modem Settings

Modem Init	<input type="text" value="+GCI=FD"/>
Modem Init	<input type="text" value="X3"/>

Designation	Description
Modem initialization	Input field for the country code, the default is +GCI=FD (FD for Europe)



NOTICE


A list of country codes for devices with analogue modem can be found in the Appendix.

Modem initialization	The command X3 (do not wait for dial tone) is preset here.
-----------------------------	--

21.4.1.2 Outgoing (configuration for outgoing connections)

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

Outgoing				Incoming	Call Back
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.

Access data (selection of inputs)

Credentials			
Input select	Phone Number	User	Password
Yes	*99***1#	user	egal
Value 1			
Value 2			
Value 3			
			<input type="button" value="Save"/> <input type="button" value="Close"/>

Designation	Description
Selection of inputs	<p>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 because of 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.</p>

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.

Designation	Description
	<p>Under Network > Internet , set the Internet settings to "On Request" and then switch the option "Connect if the input is active" to input 1.</p> <ul style="list-style-type: none"> • 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 dial-up timeout.

Authentication

Authentication via PAP

Authentication via PAP

Timeout Dialout [s]

Designation	Description
Authentication via PAP	Authentication protocol with which your login data are transmitted (P assword A uthentication P rotocol). 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 are transmitted in order to protect this data (C hallenge H andshake A uthentication P rotocol). 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.
<input type="button" value="Save"/>	Clicking on " Save " temporarily saves the current entries/changes. But the changes are not yet enabled.
<input type="button" value="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.

21.4.1.3 Incoming

Here you approve the access to the router (mbNET) by a client computer.

Outgoing **Incoming** Call Back

Settings 	
Dialin enable	No

Click the Edit icon to edit the corresponding function.

Incoming Settings	
Dialin enable	<input type="checkbox"/>
PPP Server IP-Adress (here)	<input type="text"/>
PPP Server IP-Adress (here)	<input type="text"/>
Authentication via PAP	<input checked="" type="checkbox"/>
Authentication via CHAP	<input checked="" type="checkbox"/>
close connection after inactivity of [s]	<input type="text" value="300"/>
Dialin Authentication	<input type="text" value="Only following user"/>
Username	<input type="text"/>
Password	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

Designation	Description
Dial-up is enabled	Check box for enabling/disabling this function. If the checkbox is enabled, access to the router (mbNET) is approved by a client computer.
PPP server IP address (here)	Enter the address of the router (mbNET) here. You can use the same network domain as the local network. However, you should avoid using an existing address, as this can lead to an address conflict.
PPP Client IP address	Here, Enter the IP address that the router assigns the client (calling remote terminal) when a PPP connection is established. The router and the other remote terminal form their own network after the connection.

Designation	Description
Authentication via PAP	Check box for enabling/disabling this function. Accept the factory default setting. PAP is an authentication type. Use the same setting as the dialling partner. If PAP is disabled, this authentication will not be accepted, and your data can be read by others.
Authentication using CHAP	Check box for enabling/disabling this function. Accept the factory default setting. CHAP is an authentication type. Use the same setting as the dialling partner. Disabling CHAP has the consequence that this authentication will not be accepted and your data can be read by others.
Disconnect connection after [s] inactivity	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 active.
Dial-in authentication	Drop-down menu: <ul style="list-style-type: none">• Only the following user Only the user registered in the following input fields is entitled to dial in to the router (mbNET).• Any user with dial-in rights Every user who has been activated in the User Management > User (system) for a "modem dial-up", is entitled to establish a connection.
User name	Enter the username for the PPP dial-in.
Password	Enter the associated password for the PPP dial-in.


21.4.1.4 Call Back

When this capability is activated, the mbNET is ready to connect to the Internet when a call is made.

Outgoing Incoming **Call Back**

Settings 

Call Back enable No

Click the Edit icon  to edit the corresponding function.

Incoming Settings

Call Back enable

How To Callback

Designation	Description
Callback activated	Check box for enabling/disabling this function. When this checkbox is activated, the mbNET is ready to connect to the Internet when a call is made.
We should be called back	Drop-down menu: <ul style="list-style-type: none"> • Activate callback via telephone if you choose this setting, the mbNET connects to the Internet if it is called from a phone. So that the connection can be established, the mbNET must be alerted by ringing with four times. Subsequently, the mbNET hangs up and starts the process to dial in to the Internet. This may take up to 30-40 seconds. • Log in and press the button if you select this setting, the mbNET connects to the Internet once you have set up a dial-up connection to the mbNET and in the user interface, in the Menu System > Info press the Call Back button. You then have 30 seconds to disconnect your dial-up connection, because afterwards the mbNET establishes the connection to the Internet.

21.4.2 GSM modem configuration

Network > Modem ?

LAN WAN Modem Internet DHCP DNS Server Hosts DynDNS

Modem Settings ✎

Modemtyp	GSM
Modem Init	+GCI=FD
Modem Init	X3

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

21.4.2.1 Modem Settings


Here, you can perform the basic modem settings.

Network > Modem ?

LAN WAN Modem Internet DHCP DNS Server Hosts DynDNS

Modem Settings ✎

Modemtyp	GSM
Modem Init	+GCI=FD
Modem Init	X3

Click the Edit icon  to edit the corresponding function.




Modem Settings	
Modem Init	<input type="text" value="+GCI=FD"/>
Modem Init	<input type="text" value="X3"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	


NOTICE

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

21.4.2.2 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	<input type="text" value="1234"/>		
Provider	<input type="text" value="T-mobile"/>		
Credentials 			
Input select	Phone Number	User	Password
No	<input type="text" value="*99***1#"/>	<input type="text" value="user"/>	<input type="text" value="*****"/>
Authentication 			
Authentication via PAP	<input type="text" value="Yes"/>		
Authentication via PAP	<input type="text" value="Yes"/>		
Timeout Dialout [s]	<input type="text" value="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.

SIM Settings	
SIM Pin	<input type="text" value="1234"/>
Provider	<input type="text" value="Other Provider"/>
APN (Access Point Name)	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

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)

Credentials			
Input select	Phone Number	User	Password
<input type="text" value="Yes"/>	<input type="text" value="*99***1#"/>	<input type="text" value="user"/>	<input type="text" value="egal"/>
Value 1	<input type="text"/>	<input type="text"/>	<input type="text"/>
Value 2	<input type="text"/>	<input type="text"/>	<input type="text"/>
Value 3	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>			

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.	
	<p>Under Network > Internet , set the Internet settings to "On Demand" and then switch the option "Connect if the input is active" to input 1.</p> <ul style="list-style-type: none"> • 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.

Authentication	
Authentication via PAP	<input checked="" type="checkbox"/>
Authentication via PAP	<input checked="" type="checkbox"/>
Timeout Dialout [s]	<input type="text" value="300"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

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.

<input type="button" value="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.

21.4.2.3 General SIM Settings

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

Outgoing SIM 1
Outgoing SIM 2
General SIM Settings
SMS

Settings SIM

Select primary SIM card SIM card slot 1

Switch to secondary SIM card when roaming is detected No

Switch to secondary SIM card when there is a failure with the primary SIM card Yes

Click the Edit icon to edit the corresponding function.

Settings SIM



Select primary SIM card SIM card slot 1 ▼

Switch to secondary SIM card when roaming is detected

Switch to secondary SIM card when there is a failure with the primary SIM card

Save
Close

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

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


Outgoing SIM 1 Outgoing SIM 2 General SIM Settings **SMS**

Remote Service Control via SMS 

Enable Service Control via SMS No

Send a SMS when... 

Internetconnection established No

Click the Edit icon  to edit the corresponding function.

Remotely control services via SMS

Remote Service Control via SMS

Enable Service Control via SMS

Check the Phone Number of the Sender

Senders Phone Number

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).

<input type="button" value="Save"/>	Clicking on " Save " temporarily saves the current entries/changes. But the changes are not yet enabled.
<input type="button" value="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.
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)

Remote Service Control via SMS

Internetconnection established

Receivers Phone Number

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).

21.5 Network > Internet (Internet connection and Internet settings)

Network > Internet ?

LAN WAN Modem Internet DHCP DNS Server Hosts DynDNS

Internet connection

Internet settings

Failover

✎

Failover	No
-----------------	----

Internet connection

Internet connection	External Router/Firewall
----------------------------	--------------------------

Connection monitoring

Ping IP	No
----------------	----

21.5.1 Configure Internet connectivity

Internet connection

Internet settings


Failover

✎

Failover	No
-----------------	----

Internet connection

Internet connection	External Router/Firewall
----------------------------	--------------------------

Click the Edit icon  to edit the corresponding function.

Reliability

Failover

Failover	No
-----------------	----

Save
Close

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 -

Failover ✎

Failover No

Internet connection ✎

Internet connection External Router/Firewall

Click the Edit icon  to edit the corresponding function.

Internet connection

Internet connection

External Router/Firewall ▾

External Router/Firewall

DSL

Modem

WiFi

Save

Close

Image 9: 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: <ul style="list-style-type: none"> External Router/Firewall DSL Modem Wi-Fi

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


Failover ✎

Failover Yes

Failover of Internet interfaces ✎

Retry interface before switch to next interface 1

Internet Interface priority list	Priority	Active	Internet interface

Click the Edit icon  to edit the corresponding function.

Failover

Retry interface before switch to next interface

Add Internet Interface to priority list Reset Modem ▼

+

Internet Interface priority list Internet via Modem ✖

Image 10: 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	<ul style="list-style-type: none"> ▶ 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 11: 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.

Connection monitoring	
Ping IP	Yes
PING IP or host address 1	
PING interval 1 [s]	5
PING IP or host address 2	
PING interval 2 [s]	5
PING IP or host address 3	
PING interval 3 [s]	5

Save Close

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)

Designation	Description
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**.

Quickstart Diagnose

Device type: MDH831 (6.0.2) - SerialNumber: 13188310034248 - Signal Quality: (0)

1. MDH831 ✓

2. ✓

- Internet : Connection established
Interface : External Router/Firewall
- Ping : 8.8.4.4 - (9.331ms)

21.5.2 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,

Network > Internet ?

LAN WAN WLAN Internet DHCP DNS Server Hosts DynDNS

Internet connection Internet settings

Connection settings ✎

Connection Mode	keep connection
lock connection	dont lock
broadcast IP-Adress via email	No

Click the Edit icon to edit the corresponding function.

Connection settings,

- Internet Settings,

Internet settings	
Connection Mode	keep connection ▼
lock connection	Don't lock ▼
broadcast IP-Adress via email	<input type="checkbox"/>
E-Mail address	<input type="text"/>

Designation,	Description,
Connection,	<p>Selection field for the type of connection when the mbNET should connect the Internet.</p> <ul style="list-style-type: none"> – 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): <ul style="list-style-type: none"> ◦ Connection for data transfer ◦ Connection via the "Dial Out" button ◦ Connect if input active
Lock connection	<p>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.</p> <ul style="list-style-type: none"> • 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	<p>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.</p>
E-mail address	<p>Enter the email address to which the IP address should be sent, if you enabled the function "Transfer IP address via email".</p>

- **Settings on Demand**

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

On demand settings	
Connect on traffic	<input checked="" type="checkbox"/>
Ignore traffic on LAN	<input type="checkbox"/>
Ignore traffic from internal services	<input type="checkbox"/>
Connect on "Dial-Out"	<input type="checkbox"/>
Connect on Sign 1 at Input	Input 1
close connection after inactivity of [s]	

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	<p>You can use this selection field to specify whether and via which digital input of the mbNET the internet connection should be established.</p> <ul style="list-style-type: none"> • 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.

21.6 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.

Network > DHCP ?

LAN
WAN
Modem
Internet
DHCP
DNS Server
Hosts
DynDNS

LAN
WAN

LAN DHCP-Server Settings

DHCP Server active	No
<hr/>	
Begin	<hr/>
End	<hr/>
Subnetmask	<hr/>
Broadcast address	<hr/>
Gateway	<hr/>
DNS Server	<hr/>
NetBIOS/WINS-Server	<hr/>
Lease Timeout	<hr/>

LAN DHCP-Server static lease settings

+

MAC Address	IP Address
<hr/>	<hr/>

Click the Edit icon to edit the corresponding function.

21.6.1 LAN/WAN DHCP server settings

LAN DHCP-Server Settings

DHCP Server active

Begin

End

Subnetmask

Broadcast address

Gateway

DNS Server

NetBIOS/WINS-Server


Lease Timeout

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.

21.6.2 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.

LAN DHCP-Server static lease settings	
MAC Address	IP Address

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

LAN DHCP-Server Settings	
MAC Address	IP Address
<input type="text"/>	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

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.








LAN DHCP-Server static lease settings		
MAC Address	IP Address	
00:50:C2:71:76:18	192.168.0.200	 
70:83:05:80:90:C6	172.16.20.200	 
70:B3:D5:2C:F2:7F	192.168.0.254	 

Image 12: Example of an assignment list.

Click the Edit icon , to edit the corresponding entry.

Click the Delete icon , to delete the corresponding entry.

21.7 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 (ISP).

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

Network > DNS Server

LAN WAN Modem Internet DHCP DNS Server Hosts DynDNS


By default the DNS-Servers will be given by the ISP. If you are using a static connection here you can add the nameservers. They will be used before the given servers from the ISP.


Server Settings

DNS Server

IP Address

172.25.255.250

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

LAN DHCP-Server Settings

DNS Server IP-Address

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.


Server

Settings

DNS Server settings



No Hosts	No
Strict Order	No
Filter WIN2K	No
Domain	
Cache Size	0

Click the Edit icon  to edit the corresponding function.

LAN DHCP-Server Settings

No Hosts	<input type="checkbox"/>
Strict Order	<input type="checkbox"/>
Filter WIN2K	<input checked="" type="checkbox"/>
Domain	<input type="text"/>
Cache Size	<input type="text" value="0"/>

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, (<i>Network > Internet > Internet Settings > Connection Type</i>), 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.

21.8 Network Hosts

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

Network > Hosts ?

LAN WAN Modem Internet DHCP DNS Server Hosts DynDNS

Here you can insert relations between IPs and names to answer requests direct.

Host Settings +

IP Address	Name
------------	------

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.

Host Settings

IP Address	Name
<input type="text"/>	<input type="text"/>

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.

Network > Hosts ?

LAN WAN Modem Internet DHCP DNS Server Hosts DynDNS

Here you can insert relations between IPs and names to answer requests direct.

Host Settings +








IP Address	Name		
172.16.20.1	PC-DOKU.venus.local		
127.0.0.1	user-PC.venus.local		

Image 13: Example entries in the Host Settings

Click the Edit icon  , to edit the corresponding entry.

Click the Delete icon  , to delete the corresponding entry.

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

21.9.1 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.

own-Device-name admin

Network > DynDNS

LAN WAN Modem Internet DHCP DNS Server Hosts DynDNS

System DynDNS Settings

The DNS name is made up of the serialnumber.hostname.SMTP-Server. Change the hostname to get your own name. The serialnumber could not be changed.


Get access to the unit via: **05188550432873.own-Device-name.mymbnet.biz**


Enable System Dynamic DNS No

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

21.9.2 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.

public DynDNS Service 	
Active	No
Provider	
User	
Password	*****
Host Name	
Interval [s]	

Click the Edit icon  to edit the corresponding function.

public DynDNS Service	
Active	<input type="checkbox"/>
Provider	ez-ip ▼
User	<input type="text"/>
Password	<input type="text"/>
Host Name	<input type="text"/>
Interval [s]	<input type="text"/>

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.
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.

22 Serial (serial ports COM1/COM2)

General

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

The **COM1** 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 either **COM2** or **COM1** or 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 12Mbps.

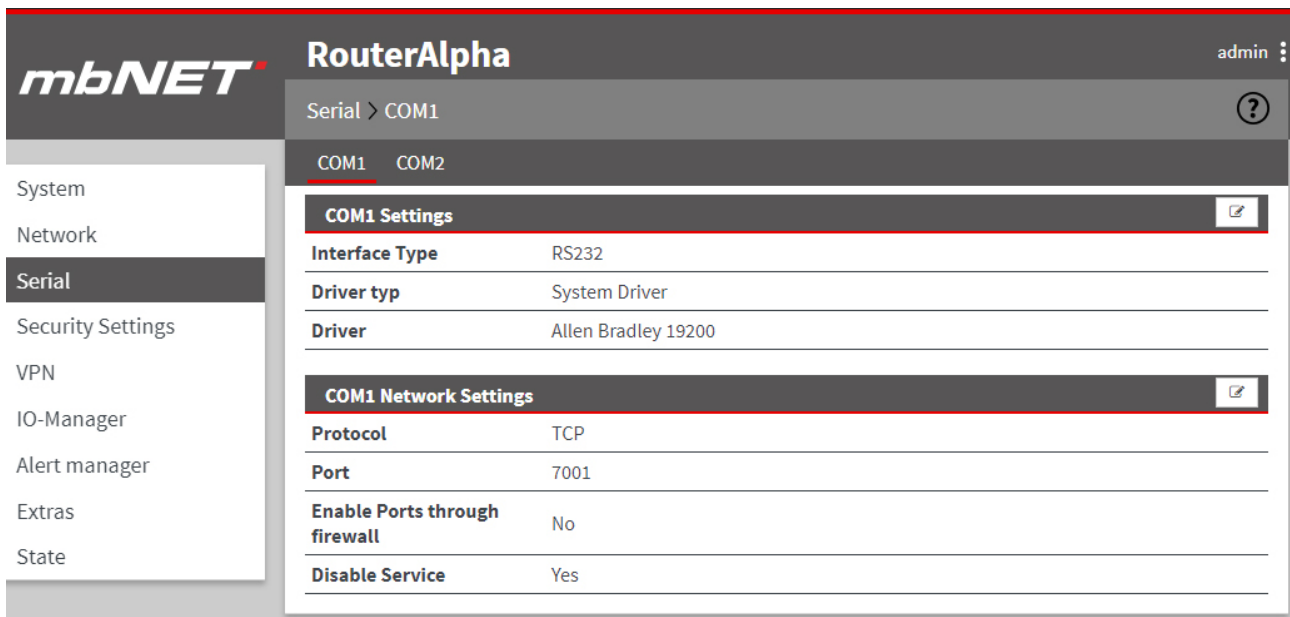



Image 14: The "Serial" menu depends on the device type and can vary.

Click the Edit icon  to edit the corresponding function.

22.1 COM1/COM2 in the RS232/485 version

NOTICE

If your mbNET type has two serial interfaces in the RS232/485 version, the settings for COM2 as the same as for COM1.

22.1.1 COM1 (COM2) settings

Driver type: System driver

COM1 Settings	
Interface Type	RS232 ▼
Driver typ	System Driver ▼
Driver	Allen Bradley 19200 ▼

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

COM1 Settings	
Interface Type	RS232 ▼
Driver typ	User settings ▼
Baudrate	300 ▼
Dataformat	8 Databits, None Parity, 1 Stopbit ▼
Handshake	no Handshake ▼
Receive loops	<input type="text"/>

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.
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.

22.1.2 COM1 (COM2) network settings

COM2 Settings

Protocol	TCP
Port	7002
Enable Ports through firewall	<input type="checkbox"/>
Disable Service	<input type="checkbox"/>

Save
Close

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 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.

22.2 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)

22.2.1 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.

COM2 Settings

Protocol	MPI/PROFIBUS Network Driver
Enable RFC1006	<input checked="" type="checkbox"/>
Own station address	<input type="text"/>
Enable RFC1006 Routing	<input type="checkbox"/>
Station address of the routing gateway	<input type="text"/>

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.

Designation	Description
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.

COM2 Settings

Protocol	VCOM-LAN2/PC-Adapater ▼
Protocol	Settings from PG/PC-Interface ▼

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.

22.2.2 COM2 Network settings

COM2 Settings	
Protocol	TCP
Port	7002
Enable Ports through firewall	<input type="checkbox"/>
Disable Service	<input type="checkbox"/>

Designation	Description
Protocol	Select the appropriate driver for your connected devices.
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.
<input type="button" value="Save"/>	Clicking on " Save " temporarily saves the current entries/changes. But the changes are not yet enabled.
<input type="button" value="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 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	<p>"SimpleNAT" allows you to grant access to an IP address from the LAN Power Plant 1:1 in the WAN Ethernet network.</p> <p>Using the "1:1 NAT" Is it possible to connect two networks that are in the same address range with each other.</p>

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.

23.1 Security Settings > Firewall General

Firewall general
WAN - LAN
LAN - WAN
Forwarding
NAT

Firewall Settings
✎



maximum Security

All incoming Packages (Data from Internet) are **rejected**

All outgoing Packages (Data from LAN) are **rejected**

except: DNS, FTP, IMAP, HTTP, HTTPS, POP3, SMTP, Telnet, NTP

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

Firewall Settings	
Interface Type	maximum Security ▼
Replace the senders IP-address of all outgoing (LAN) packages with the LAN-IP address of this router (SNAT)	<input checked="" type="checkbox"/>
Replace the senders IP-address of all outgoing (WAN) packages with the WAN-IP address of this router (SNAT)	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

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.

<input type="button" value="Save"/>	Clicking on " Save " temporarily saves the current entries/changes. But the changes are not yet enabled.
<input type="button" value="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.

23.2 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.

Firewall general								
WAN - LAN								
Active	Action	WAN Interface	Source IP	Source Port	Protocol	LAN Interface	Destination IP	Destination Port

Click on the green plus , to add a rule.

WAN - LAN Rule	
Active	<input type="checkbox"/>
Action	Drop
WAN Interface	Internet
Source IP	
Source Port	
Protocol	All
LAN Interface	Internal services
Destination IP	
Destination Port	

Save Close

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

Designation	Description
Campaign	<p>Selection field for the applicable action. The options are:</p> <ul style="list-style-type: none"> • 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	<p>You can use this selection field to determine which WAN interface* should normally be used. The options are:</p> <ul style="list-style-type: none"> • Internet • WAN Ethernet • OpenVPN • IPsecVPN • PPTPVPN • All <p>* The selection field for the WAN interface can vary depending on the type of router.</p>
Origin IP	<p>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.</p>
Origin port	<p>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.</p>
Protocol	<p>Selection field for the transfer protocol to use. The options are:</p> <ul style="list-style-type: none"> • 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	<p>You can use this selection field to determine which LAN interface* should normally be used. The options are:</p> <ul style="list-style-type: none"> • Internal services • LAN Ethernet • All
Destination IP	<p>Enter the IP address to which data packets are to be forwarded.</p>
Destination-Port	<p>Enter the ports to which the data packets are to be forwarded.</p>

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 15: The firewall rule example entry

23.2.1 Edit firewall rule

Change the entered rule order





Firewall general									
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		 


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


WAN - LAN Rule						
	WAN Interface	Source IP Source Port	Protocol	Destination IP Destination Port	LAN Interface	
✓	Internet	172.25.15.101:30	▶▶ All	▶▶ 192.168.0.220:30	All	
✓	WAN Ethernet	192.168.1.104:	▶▶ TCP	▶▶ 192.167.15.22:	Internal services	 
✓	OpenVPN	10.28.8.12:	▶▶ All	▶▶ 182.27.14,23:	Internal services	

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

Change/delete firewall rule

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		 



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.

23.3 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.

Firewall general WAN - LAN <u>LAN - WAN</u> Forwarding NAT									
LAN - WAN Rule  									
Active	Action	LAN Interface	Source IP	Source Port	Protocol	WAN Interface	Destination IP	Destination Port	

Click on the green plus , to add a rule.

LAN - WAN Rule	
Active	<input type="checkbox"/>
Action	Drop ▼
LAN Interface	Internal services ▼
Source IP	<input type="text"/>
Source Port	<input type="text"/>
Protocol	All ▼
WAN Interface	Internet ▼
Destination IP	<input type="text"/>
Destination Port	<input type="text"/>

Designation	Description
Active	Checkbox for enabling/disabling this firewall rule.
Campaign	Selection field for the applicable action. The options are: <ul style="list-style-type: none"> • 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	<p>You can use this selection field to determine which LAN interface* should normally be used. The options are:</p> <ul style="list-style-type: none"> • Internal services • LAN Ethernet • All
Origin IP	<p>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.</p>
Origin port	<p>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.</p>
Protocol	<p>Selection field for the transfer protocol to use. The options are:</p> <ul style="list-style-type: none"> • 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	<p>You can use this selection field to determine which WAN interface* should normally be used. The options are:</p> <ul style="list-style-type: none"> • Internet • WAN Ethernet • OpenVPN • IPsecVPN • PPTPVPN • All <p>* The selection field for the WAN interface can vary depending on the type of router.</p>
Destination IP	<p>Enter the IP address to which data packets are to be forwarded.</p>
Destination-Port	<p>Enter the ports to which the data packets are to be forwarded.</p>

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.

<input type="button" value="Save"/>	Clicking on "Save" temporarily saves the current entries/changes. But the changes are not yet enabled.
<input type="button" value="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								<input type="button" value="edit"/> <input type="button" value="+"/>
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 16: The firewall rule example entry

23.3.1 Edit firewall rule

Change the entered rule order







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	


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

LAN - WAN Rule						
	WAN Interface	Source IP Source Port	Protocol		Destination IP Destination Port	LAN Interface
✓	Internet	192.168.0.155-192.168.0.250:	⇨ All ⇨		192.167.15.22:	Internal services
✓	WAN Ethernet	172.25.15.101:30	⇨ TCP ⇨		192.168.104:	Internal services
✗	OpenVPN	182.27.14.23:	⇨ All ⇨		10.28.8.12:	Internal services

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.

23.4 Security Settings > Forwarding

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

Active	Source IP	Source Port	Protocol	Destination IP	Destination Port	Interface	Forward to IP	Forward to Port
<div style="float: right;">   </div>								

Click on the green plus , to add a rule.

Forwarding Rule	
Active	<input type="checkbox"/>
Source IP	<input type="text"/>
Source Port	<input type="text"/>
Protocol	All ▼
Destination IP	<input type="text"/>
Destination Port	<input type="text"/>
Interface	Internet ▼
Forward to IP	<input type="text"/>
Forward to Port	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

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	<p>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.</p> <ul style="list-style-type: none"> • 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	<p>You can use this selection field to determine which interface the forwarding should normally be used. The options are:</p> <ul style="list-style-type: none"> • Internet • WAN Ethernet • OpenVPN • IPSecVPN • PPTPVPN • LAN Ethernet • All <p>* The selection field for the interface can vary depending on the type of router.</p>
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 <u>Forwarding</u> 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 17: Forwarding Entry Example

23.4.1 Edit Forwarding Rule

Change the entered rule order







Firewall general WAN - LAN LAN - WAN <u>Forwarding</u> 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	 


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


Forwarding Rule									
	Protocol	Source IP Source Port		Destination IP Destination Port		Forward to IP Forward to Port		Interface	
	All	172.16.20.158:	▶▶	192.168.0.155:	▶▶	172.16.20.120:		LAN Ethernet	
	TCP	172.16.20.158:443	▶▶	192.168.0.155:443	▶▶	172.16.20.205:443		LAN Ethernet	 
	All	10.28.8.12:	▶▶	172.16.20.105,172.16.20.205:	▶▶	17.25.16.158:		WAN Ethernet	

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

Change/delete firewall rule

Firewall general WAN - LAN LAN - WAN <u>Forwarding</u> 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	 

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.

23.5 Security settings > NAT

23.5.1 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".

Firewall general
WAN - LAN
LAN - WAN
Forwarding
NAT

SimpleNAT
1:1 NAT

SimpleNAT Rules
+

Active	WAN IP Address	LAN IP Address	Comment
<div style="display: flex; align-items: center; justify-content: center;"> + Click on the green plus </div>			

SimpleNAT Rules	
Active	<input type="checkbox"/>
WAN IP Address	<input style="width: 90%;" type="text"/>
LAN IP Address	<input style="width: 90%;" type="text"/>
Comment	<input style="width: 90%;" type="text"/>

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.

SimpleNAT
1:1 NAT

SimpleNAT Rules
+

Active	WAN IP Address	LAN IP Address	Comment
Yes	192.168.1.101	192.168.0.1	PLC

✎

✖



Image 18: Example entry





23.5.1.1 Edit SimpleNAT Rule


Change the entered rule order

Firewall general WAN - LAN LAN - WAN Forwarding **NAT**








SimpleNAT 1:1 NAT

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  in the header of the overview to change the sequence of the entered change rules.


SimpleNAT Rules


	WAN IP Address	LAN IP Address	Comment	
	192.168.1.101	192.168.0.1	PLC	
	172.16.20.100	172.16.20.158	PC	 
	174.20.15.110	174.20.15.2	NAS	


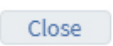
Here you can move up and down (drag and drop) to change the sequence of the entered rules.

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.

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

23.5.2 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.

Firewall general WAN - LAN LAN - WAN Forwarding NAT

SimpleNAT 1:1 NAT

1:1 NAT Rules ✎ +

Active	LAN Netaddress	NAT Netaddress	Peer Netaddress
--------	----------------	----------------	-----------------

Click on the green plus , to add a rule.

1:1 NAT Rules

Active	<input type="checkbox"/>
LAN Netaddress	<input type="text"/>
NAT Netaddress	<input type="text"/>
Peer Netaddress	<input type="text"/>

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.

SimpleNAT 1:1 NAT

1:1 NAT Rules				 
Active	LAN Netaddress	NAT Netaddress	Peer Netaddress	
Yes	192.168.0.0/24	192.168.2.0/24	192.168.1.0/24	 







Image 19: Example entry


23.5.2.1 Edit 1:1 NAT rule





Change the entered rule order

Firewall general WAN - LAN LAN - WAN Forwarding NAT

SimpleNAT 1:1 NAT

1:1 NAT Rules				 
Active	LAN Netaddress	NAT Netaddress	Peer Netaddress	
Yes	192.168.0.0/24	192.168.2.0/24	192.168.1.0/24	 
Yes	172.16.0.0/24	172.16.2.0/24	172.16.1.0/24	 

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

1:1 NAT Rules				
	LAN Netaddress	NAT Netaddress	Peer Netaddress	
✓	192.168.0.0/24	192.168.2.0/24	192.168.1.0/24	
✓	172.16.0.0/24	172.16.2.0/24	172.16.1.0/24	 
✗	198.20.0.0/24	198.20.2.0/24	198.20.1.0/24	







Save Close


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


Change/delete 1:1 NAT rule

Firewall general WAN - LAN LAN - WAN Forwarding NAT

SimpleNAT **1:1 NAT**

1:1 NAT Rules				 
Active	LAN Netaddress	NAT Netaddress	Peer Netaddress	
Yes	192.168.0.0/24	192.168.2.0/24	192.168.1.0/24	 
Yes	172.16.0.0/24	172.16.2.0/24	172.16.1.0/24	 

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.**

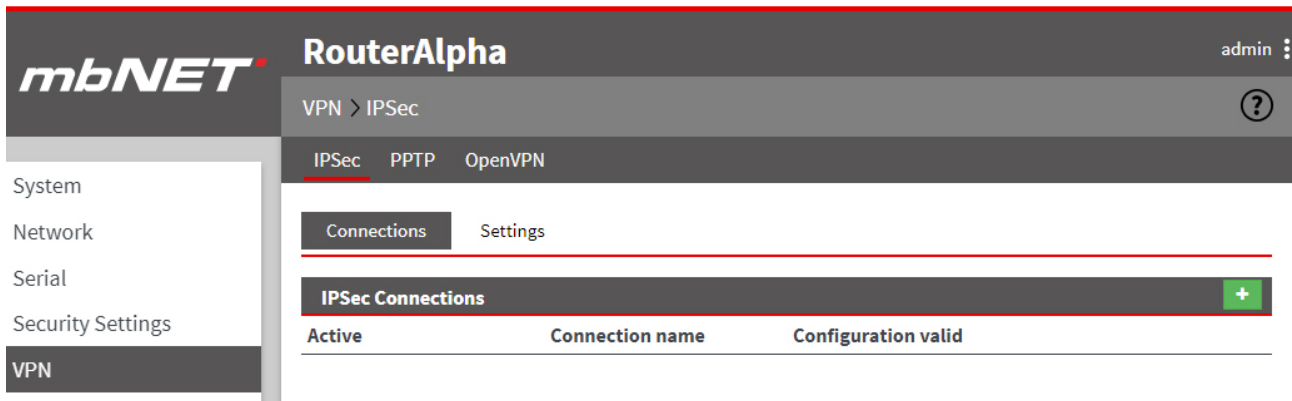
Close

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 VPN



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

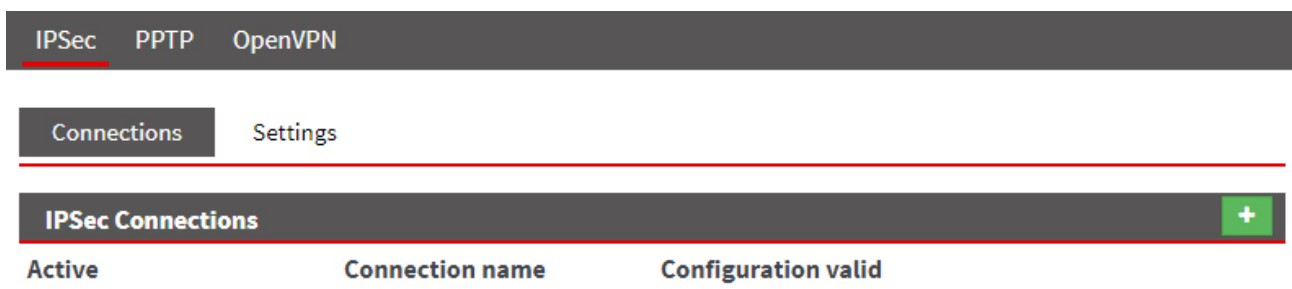
- **IPSec**
- **PPTP**
- **OpenVPN**

24.1 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.

24.1.1 Configure IPSec connections



Click on the green plus  to add a connection.

To establish a VPN connection, follow the Configuration Wizard.

1 Connection settings

IPSec Connections

1

Connection settings

2

Network settings

3

Authentication

4

Protocol settings

Active

Connection name	<input type="text"/>
Connection type	Router - Router Connection ▼
Connection Mode	Connect immediately ▼
Peer Address (IP,DNS)	<input type="text"/>

Next

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 <ul style="list-style-type: none"> 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. <p>The following options are available:</p> <ul style="list-style-type: none"> - 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 <p style="text-align: center; font-size: small;">* refers to digital inputs I1-I4 of the mbNET. ** Dial Out button on the mbNET front panel</p>
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

IPSec Connections

Local network	<input style="width: 90%;" type="text"/>
Peer network	<input style="width: 90%;" type="text"/>
NAT-Traversal	<input type="checkbox"/>

Back
Next

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)

IPSec Connections

1
Connection settings

2
Network settings

3
Authentication

4
Protocol settings

Authentication process	<input type="text" value="PSK"/>
PSK (Preshared Key)	<input type="text"/>
Local ID	<input type="text"/>
Peer ID	<input type="text"/>

Designation	Description
Authentication procedure	Selection field for the authentication procedure <ul style="list-style-type: none"> 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.
<input type="button" value="Next"/>	Click the Next button to continue the configuration.

(Authentication procedure = X.509)

IPSec Connections

1
Connection settings

2
Network settings

3
Authentication

4
Protocol settings

Authentication process	X.509 ▼
Certificate process	Authentication by peer certificate ▼

Unit 1 has...

One Certificate with the private key, certified by CA1 (own certificate)

One copy of the Certificate from Unit 2 without the private key (remote certificate)

Unit 2 has...

One Certificate with the private key, certified by CA2 (own certificate)

One copy of the Certificate from Unit 1 without the private key (remote certificate)

Own Certificate	no valid certificates imported
Partner Certificate	no valid certificates imported

Designation	Description
Authentication procedure	Selection field for the authentication procedure <ul style="list-style-type: none"> PSK X.509
Certificate Procedure	Selection field for the certificate procedure <ul style="list-style-type: none"> 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 <i>Section: System – Certificates</i>). 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 <i>creating certificates and revocation lists with XCA</i>). 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 <i>creating certificates and revocation lists with XCA</i>).
Next	Click the Next button to continue the configuration.

4 Protocol settings

IPSec Connections

Phase 1 (IKE ISAKMP)

Coding algorithm	3DES-192
Hash total algorithm	SHA1
Lifetime of ISAKMP SA [seconds]	3600
Aggressive Mode	<input type="checkbox"/>

Phase 2 (ESP IPsec SA)

Coding algorithm	3DES-192
Hash total algorithm	SHA1
PFS (Perfect Forward Secrecy) active	<input checked="" type="checkbox"/>
Lifetime of IPsec SA [seconds]	28800
Do initiate Renegotiation keys before end (rekey) active	<input checked="" type="checkbox"/>
Number of tries for connection startup [0= no limit]	3
Rekeymargin [seconds]	540
Rekeyfuzz	100

DPD (Dead Peer Detection)

Delay [seconds]	30
Timeout [seconds]	120
Action after dead peer detected	Hold

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).

VPN | Page 179 of 292

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


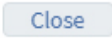
The setting "**Perfect Forward Secrecy (PFS) enabled**" is only allowed for the router-to-router connection. If you want to set up a client-router connection, PFS must be disabled.

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

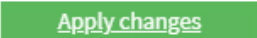

Designation	Description
Delay [seconds]	Each time the set time period expires, a review of the connection is made. If within the time window (timeout) there is no positive result, the action set for " Action after detection of the connection error " is executed.
Timeout [seconds]	After expiration of 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	<p>You can use this selection field to specify how you want to proceed with connection if timeout has been reached.</p> <p>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).</p> <p>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.</p>

Click on "Save", after completing all settings.

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

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

24.1.2 IPsec settings

IPSec
PPTP
OpenVPN

Connections
Settings

✎
L2TP Server Configuration

Local IP Address

Remote IP Address Begin

Remote IP Address End


✎
IPSEC Debug settings

klipsdebug no debug

plutodebug no debug

✎
IPSEC settings

MTU

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.

L2TP Server Configuration

Local IP Address

Remote IP Address Begin




Remote IP Address End


Save
Close

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	

24.2 PPTP

24.2.1 PPTP server configuration

IPSec <u>PPTP</u> OpenVPN	
Server <u>Clients</u>	
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	<input type="checkbox"/>
automatic configuration	<input type="text" value="No"/>
Local IP Address or Range	<input type="text" value="192.168.0.100"/>
remote IP Address or Range	<input type="text" value="192.168.0.101-110"/>
Give DNS Address to the Client	<input type="text"/>
Give WINS Address to the Client	<input type="text"/>

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

Encryption Configuration

Encryption

Designation	Description
Encryption	Selection field for the type of encryption: <ul style="list-style-type: none"> • 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).

Authentication Configuration	
Authentication via PAP	<input checked="" type="checkbox"/>
Authentication via CHAP	<input type="checkbox"/>
Authentication via MS-CHAP	<input checked="" type="checkbox"/>
Authentication via MS-CHAP V2	<input type="checkbox"/>

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.

<input type="button" value="Save"/>	Clicking on " Save " temporarily saves the current entries/changes. But the changes are not yet enabled.
<input type="button" value="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.

24.2.2 PPTP client configuration

IPSec
PPTP
OpenVPN



Server
Clients

PPTP Clients +				
Active	Name	Host Name or IP	IP local	IP remote

Click on the green plus  to add a client.

PPTP Clients	
Active	<input type="checkbox"/>
Name	<input type="text"/>
Host Name or IP	<input type="text"/>
IP local	<input type="text"/>
IP remote	<input type="text"/>
Authentication	PAP ▼
Encryption	None ▼
Username	<input type="text"/>
Password	<input type="text"/>
Start Connection on..	Connect immediately ▼

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: <ul style="list-style-type: none"> • None • MPPEV2/40 • MPPEV2/128 • MPPEV2/all

Designation	Description
NOTICE	
<p>IMPORTANT: You should always enable encryption of your VPN connections, otherwise unauthorized access to networks, machines, etc. is possible!</p>	
User name	Enter a user name
Password	Enter a new password
Start connection for	<p>selection field, when, or under what condition the connection should be started.</p> <ul style="list-style-type: none"> - 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 <p style="text-align: right; margin-right: 20px;">* refers to digital inputs I1-I4 of the mbNET. ** Dial Out button on the mbNET front panel</p>
	Clicking on " Save " temporarily saves the current entries/changes. But the changes are not yet enabled.
	Clicking on " Close " discards the current input/changes.
NOTICE	
<p>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.</p>	

24.3 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.

24.3.1 Configure OpenVPN connections

The screenshot shows a web interface for configuring VPN connections. At the top, there are tabs for 'IPSec', 'PPTP', and 'OpenVPN'. Below these, there are sub-tabs for 'Connections' and 'Static Keys'. A table titled 'OpenVPN Connections' is displayed with columns for 'Active', 'Connection name', and 'Configuration valid'. A green plus icon is located in the top right corner of the table area.

Click on the green plus  to add a connection.

To establish a VPN connection, follow the Configuration Wizard.

24.3.1.1 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

OpenVPN Connections

1

Connection settings

2

Network settings

3

Authentication

4

Protocol settings

Active

Connection name

Connection type Client - Router Connection ▼

Next

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 <ul style="list-style-type: none"> 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).
	Choose here the Connection Type Client - Router connection.
Next	Click the Next button to continue the configuration.

2 Network settings

OpenVPN Connections

1
2
3
4

Connection settings
Network settings
Authentication
Protocol settings

Local IP Address of the VPN tunnel

Peer IP Address of the VPN tunnel

Client NAT behind the local network
(The client will send the IP of the gateway for traffic through the local network)

Back
Next

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)

OpenVPN Connections

1
2
3
4

Connection settings

Network settings

Authentication

Protocol settings

Authentication process

Back
Next

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 <ul style="list-style-type: none"> 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)

OpenVPN Connections

1
2
3
4

Connection settings

Network settings

Authentication

Protocol settings

Authentication process

static key

▼

Static Keys

▼

Back

Next

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 <ul style="list-style-type: none"> 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)

OpenVPN Connections

1
2
3
4

Connection settings
Network settings
Authentication
Protocol settings

Authentication process

CA Certificate

Own Certificate

Additional user and password verification

Use only CA and User/password for client verification

Back
Next

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 <ul style="list-style-type: none"> 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



Networkadapter

Adaptertype

Protocol

Coding algorithm

Protocol

Local VPN port

Peer VPN port

Miscellaneous

Bind the local IP-address and port

Allow the peer to change the IP-address dynamically

LZO compress active

Ping interval [s]

Ping restart [s]

MTU [bytes]

Fragment the UDP packets in... [bytes]

Regenerate a new key after... [s]

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.

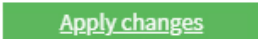

Miscellaneous	
Designation	Description
Enable connection through a HTTP proxy	Check box for enabling/disabling this function. If this function is activated, the outgoing connection attempts to pass through a proxy server. The following fields must be completed for this purpose.
HTTP proxy name	Input 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 user-name	If the proxy server requires authentication, enter the user data for the proxy.
HTTP proxy password	If you do not know this data, ask your network administrator.

Click on "Save", after completing all settings.

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

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

24.3.1.2 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:



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

OpenVPN Connections

1
2
3
4

Connection settings

Network settings

Authentication

Protocol settings

Active

Connection name

Connection type Router - Router Connection

Link connection Wait for incoming Connection

Next

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 <ul style="list-style-type: none"> • 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

OpenVPN Connections

1
2
3
4

Connection settings
Network settings
Authentication
Protocol settings

Local IP Address of the VPN tunnel

Peer IP Address of the VPN tunnel

Local network

Peer network

Back
Next

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)

OpenVPN Connections

Authentication process

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 <ul style="list-style-type: none"> • No Authentication • Static key • X.509
<input type="button" value="Next"/>	Click the Next button to continue the configuration.

(Authentication procedure = static key)

OpenVPN Connections

Authentication process	static key	▼
Static Keys		▼

Back
Next

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 <ul style="list-style-type: none"> 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

OpenVPN Connections

1
2
3
4

Connection settings
Network settings
Authentication
Protocol settings

Authentication process

CA Certificate

Own Certificate

Additional user and password verification

Use only CA and User/password for client verification

Back
Next

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 <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> ◦ 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.

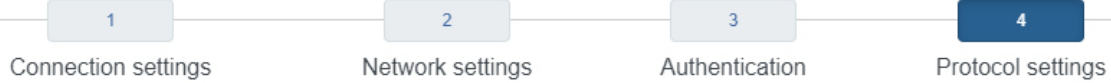
NOTICE

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

OpenVPN Connections



Networkadapter

Adaptertype

Protocol

Coding algorithm

Protocol

Local VPN port

Peer VPN port

Miscellaneous

Bind the local IP-address and port

Allow the peer to change the IP-address dynamically

LZO compress active

Ping interval [s]

Ping restart [s]

MTU [bytes]

Fragment the UDP packets in... [bytes]

Regenerate a new key after... [s]

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](#)

Network interface controller

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

Protocol

Designation	Description
Encryption algorithm	<p>Selection field for the method used by the mbNET to encrypt OpenVPN data:</p> <ul style="list-style-type: none"> - 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	<p>Selection field for the transfer protocol:</p> <ul style="list-style-type: none"> - UDP - TCP
Local VPN port	<p>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.</p> <p>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!</p>
Partner VPN port	

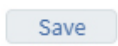
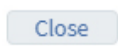
Miscellaneous

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

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.
Login password on the HTTP proxy server	If you do not know this data, ask your network administrator.

Click on "Save", after completing all settings.

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

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

24.3.1.3 Connection type: Router-router connection -client 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]	

Client mode

To establish a connection, select one of the **active** connection options from the selection list.

The active connection options include all options **except** = "**Wait for incoming connection**".

The mbNET is therefore in "**client mode**" and will be referred to as "client" in the further documentation.

1 Connection settings

OpenVPN Connections

1

Connection settings

2

Network settings

3

Authentication

4

Protocol settings

Active

Connection name

Connection type

Link connection

Remote maintenance active on

One of this routers has to be set to wait mode!

Peer address (IP,DNS)

Disconnect connection after inactivity [s]

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 <ul style="list-style-type: none"> • Router - Router connection • Client router connection

Link connection	Selection field for when or under which conditions the connection should be started. <ul style="list-style-type: none"> - Connection immediately - Start with an active internet connection - Wait for incoming connection - Connect when input* 1 has High-signal - Connect when input 2 has High-signal - Connect when input 3 has High-signal - Connect when input 4 has High-signal - Connect when input 1 has High-signal, disconnect at Low-Signal - Connect when input 2 has High-signal, disconnect at Low-Signal - Connect when input 3 has High-signal, disconnect at Low-Signal - Connect when input 4 has High-signal, disconnect at Low-Signal - Connect while pushing "Dial Out" button**
------------------------	---

** refers to digital inputs I1-I4 of the mbNET. ** Dial Out button on the mbNET front panel

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".

Designation	Description
-------------	-------------

NOTICE

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

Remote maintenance active on	You can choose from: <ul style="list-style-type: none">- Digital Input 1 (High)- Digital Input 2 (High)- Digital Input 3 (High)- Digital Input 4 (High)
-------------------------------------	--

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. "[For description](#)".

Peer address (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.
<input type="button" value="Next"/>	Click the Next button to continue the configuration.

2-level security

Link connection	Connect when input 1 has High-signal, disconnect at Low-Signal	▼
Remote maintenance active on	Digital Input 2 (High)	▼

If you have selected one of the options under "**Link connection**"

- Connect when input 1 has High-signal, disconnect at Low-Signal
- Connect when input 2 has High-signal, disconnect at Low-Signal
- Connect when input 3 has High-signal, disconnect at Low-Signal
- Connect when input 4 has High-signal, disconnect at Low-Signal

you can also select one of these options in combination under "**Remote maintenance active on**":

- Digital Input 1 (High)
- Digital Input 2 (High)
- Digital Input 3 (High)
- Digital Input 4 (High)

Example:

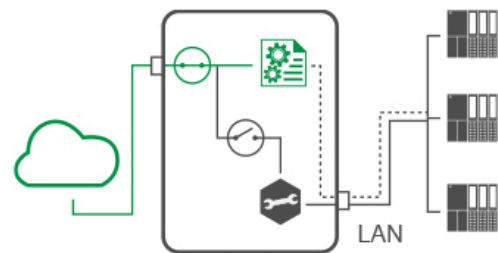
A connection is established by connecting input 1.

Level 1

The router is connected.

The remote service technician now has access to the router's internal services (web server, data monitoring, etc.).

However, the service technician cannot route into the LAN segment.



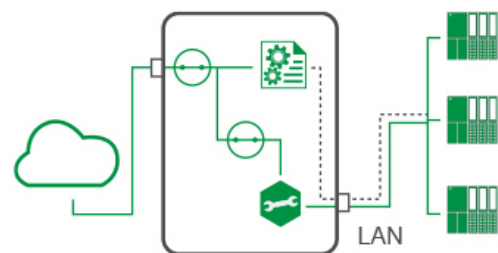
Remote maintenance is only active when digital input 2 is also activated (High).

Level 2

The routing between the remote maintenance provider and the LAN segment is enabled.

All participants in the LAN segment can now be reached transparently.

By resetting the signal in input 2 to Low, remote maintenance is interrupted again.



2 Network settings

OpenVPN Connections

1
2
3
4

Connection settings
Network settings
Authentication
Protocol settings

Local IP Address of the VPN tunnel

Peer IP Address of the VPN tunnel

Local network

Peer network

Do NAT for all outgoing traffic

Back
Next

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)

OpenVPN Connections

1
2
3
4

Connection settings
Network settings
Authentication
Protocol settings

Authentication process no authentication

Back
Next

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 <ul style="list-style-type: none"> No Authentication Static key X.509
Next	Click the Next button to continue the configuration.

(Authentication procedure = static key)

OpenVPN Connections

Authentication process	static key	▼
Static Keys		▼

Back
Next

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 <ul style="list-style-type: none"> 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 - client mode)

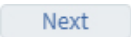
If one of the following options was selected for "Link connection", this mbNET is in client mode and is referred to as "Client".

- Connection immediately
- Start with an active internet connection
- Connect when input 1 has High-signal
- Connect when input 2 has High-signal
- Connect when input 3 has High-signal
- Connect when input 4 has High-signal
- Connect when input 1 has High-signal, disconnect at Low-Signal
- Connect when input 2 has High-signal, disconnect at Low-Signal
- Connect when input 3 has High-signal, disconnect at Low-Signal
- Connect when input 4 has High-signal, disconnect at Low-Signal
- Connect while pushing "Dial Out" button

OpenVPN Connections	
1	2
Connection settings	Network settings
3	4
Authentication	Protocol settings
Authentication process	x.509 <input type="button" value="v"/>
CA Certificate	<input type="button" value="v"/>
Own Certificate	<input type="button" value="v"/>
Additional user and password verification	Yes <input type="button" value="v"/>
Username	<input type="text"/>
Password	<input type="text"/>
Do not use my own certificate for verification. Use only CA and User/password verification	<input type="checkbox"/>
Peer must be TLS Server	<input type="checkbox"/>
<input type="button" value="Back"/> <input type="button" value="Next"/>	
<input type="button" value="Save"/> <input type="button" value="Close"/>	

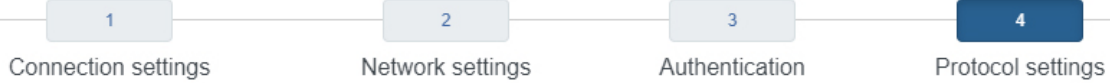
NOTICE

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

Designation	Description
Authentication procedure	<p>Selection field for the authentication procedure</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> ◦ 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.
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.
	Click the Next button to continue the configuration.

4 Protocol settings

OpenVPN Connections



Networkadapter

Adaptertype

Protocol

Coding algorithm

Protocol

Local VPN port

Peer VPN port

Miscellaneous

Bind the local IP-address and port

Allow the peer to change the IP-address dynamically

LZO compress active

Ping interval [s]

Ping restart [s]

MTU [bytes]

Fragment the UDP packets in... [bytes]

Regenerate a new key after... [s]

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](#)

Network interface controller

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

Protocol

Designation	Description
Encryption algorithm	<p>Selection field for the method used by the mbNET to encrypt OpenVPN data:</p> <ul style="list-style-type: none"> - 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	<p>Selection field for the transfer protocol:</p> <ul style="list-style-type: none"> - UDP - TCP
Local VPN port	<p>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.</p> <p>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!</p>
Partner VPN port	



Miscellaneous

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

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.

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

24.4 Static key (key management)

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

IPSec
PPTP
OpenVPN

Connections
Static Keys

list of imported static keys
+

Name

Click on the green plus  to add a key.

generate static key

Name

Generate

import static key

File Datei auswählen Keine ausgewählt

Import

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.

IPSec PPTP OpenVPN

Connections

Static Keys

list of imported static keys




Name


mystatickey



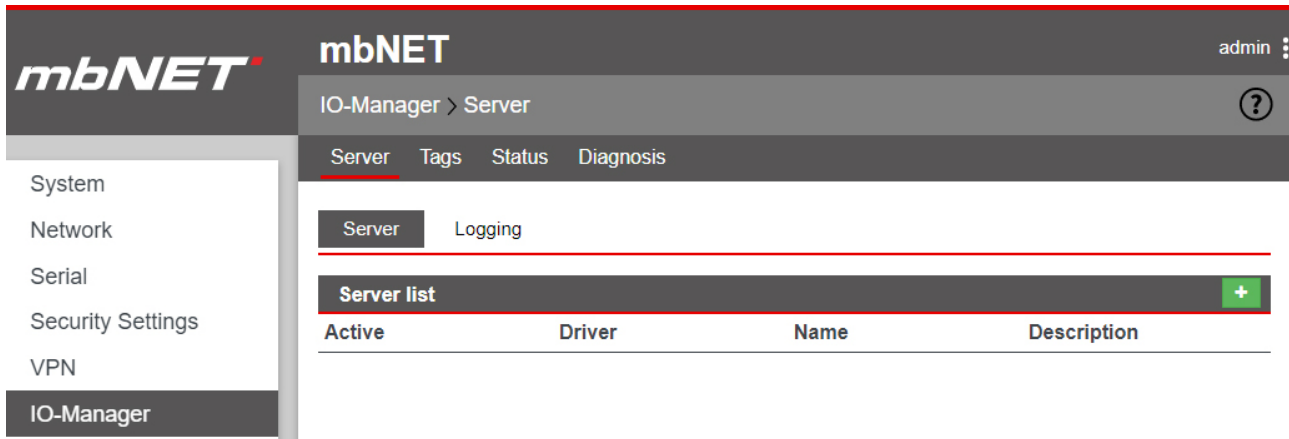
importstatickey



To download a key, click on the Download button .

To delete a key, click on the Delete button .

25 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).

COM2 Settings	
Protocol	MPI/PROFIBUS Network Driver
Enable RFC1006	<input checked="" type="checkbox"/>
Own station address	<input type="text"/>
Enable RFC1006 Routing	<input type="checkbox"/>
Station address of the routing gateway	<input type="text"/>

Limits:


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

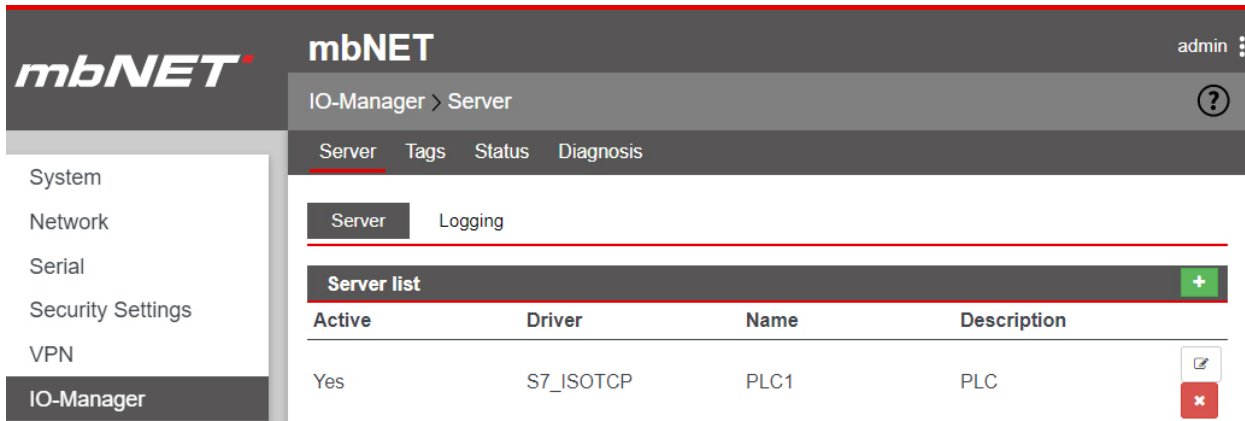
25.1 Configuring the PLC connection

▶ 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none">• 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) to accept the input / changes.



mbNET admin

IO-Manager > Server


Server Tags Status Diagnosis


Server Logging


Server list +

Active	Driver	Name	Description
Yes	S7_ISOTCP	PLC1	PLC


✎ ✕

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 .

25.2 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

Settings Logging	
Interval [s]	<input type="text" value="60"/>
Maximum time until archiving the log file [h]	<input type="text" value="0"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

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.

Settings FTP upload

Interval [min]	<input type="text" value="0"/>
FTP-Server address	<input type="text"/>
FTP-Server Username	<input type="text"/>
FTP-Server Password	<input type="text"/>

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

25.3 Status

mbNET

IO-Manager > Status

admin

Server Tags Status Diagnosis

Status

PLC-1 PLC-2

Description	Address	Value	Time stamp	Valid
Counter	DBx.DBBy	Error - could not read datapoint	2019.06.13,16:19:23.468	0

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).

25.4 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 .

Server

Active

Server

Address

Display format

Description

Interval [x 100ms]

Logging

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.DBWz =	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	Ply.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

The screenshot shows the mbNET web interface. The top navigation bar includes the mbNET logo, the user name 'admin', and a help icon. Below the navigation bar, the breadcrumb 'IO-Manager > Tags' is visible. A secondary navigation bar contains 'Server', 'Tags' (which is underlined), 'Status', and 'Diagnosis'. On the left side, there is a vertical menu with options: System, Network, Serial, Security Settings, VPN, and IO-Manager (which is highlighted). The main content area is titled 'Tag List' and contains a table with two data points. Each row in the table has an 'Active' checkbox, a 'Server' dropdown, an 'Address' text field, a 'Display format' dropdown, a 'Description' text field, an 'Interval [x 100ms]' dropdown, a 'Logging' checkbox, and an edit icon.

Active	Server	Address	Display format	Description	Interval [x 100ms]	Logging
<input checked="" type="checkbox"/>	PLC-1	DBx.DBBy	BIN	Counter	5	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	PLC-2	My.z	DEZ	On/OFF	3	<input type="checkbox"/>

Image 20: Beispiel-Datenpunkte

To edit a data point, click the edit button  .

25.5 Diagnosis

The screenshot displays the mbNET web interface. On the left is a sidebar menu with the following items: System, Network, Serial, Security Settings, VPN, **IO-Manager** (highlighted), Alarm manager, Extras, and Status. The main header area shows the mbNET logo, the user 'admin', and a navigation breadcrumb 'IO-Manager > Diagnosis'. Below the breadcrumb is a sub-menu with 'Server', 'Tags', 'Status', and 'Diagnosis' (underlined). The main content area is titled 'IO-Manager logging' and contains the following log entries:

```

Jun 13 16:16:48 nero user.warn io_manager: Could not connect to PLC with IP 192.168.0.105 - try to reconne
Jun 13 16:16:51 nero user.warn io_manager: Could not connect to PLC with IP 192.168.0.106 - try to reconne
Jun 13 16:16:51 nero user.info io_manager: IO-Manager successfully initialized - start main loop
Jun 13 16:16:54 nero user.warn io_manager: Could not connect to PLC with IP 192.168.0.105 - try to reconne
Jun 13 16:16:58 nero user.warn io_manager: Could not connect to PLC with IP 192.168.0.106 - try to reconne
Jun 13 16:17:01 nero user.warn io_manager: Could not connect to PLC with IP 192.168.0.105 - try to reconne
Jun 13 16:17:04 nero user.warn io_manager: Could not connect to PLC with IP 192.168.0.106 - try to reconne
Jun 13 16:17:07 nero user.warn io_manager: Could not connect to PLC with IP 192.168.0.105 - try to reconne
Jun 13 16:17:10 nero user.warn io_manager: Could not connect to PLC with IP 192.168.0.106 - try to reconne
Jun 13 16:17:13 nero user.warn io_manager: Could not connect to PLC with IP 192.168.0.105 - try to reconne
Jun 13 16:17:17 nero user.warn io_manager: Could not connect to PLC with IP 192.168.0.106 - try to reconne
Jun 13 16:17:20 nero user.warn io_manager: Could not connect to PLC with IP 192.168.0.105 - try to reconne

```

Here you can view and analyze the logging.

26 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

26.1 Digital inputs - Configuration

NOTICE

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

The screenshot shows the mbNET web interface. The left sidebar contains a navigation menu with items: System, Network, Serial, Security Settings, VPN, Alert manager (highlighted), Extras, and State. The main content area is titled 'Alert manager > Inputs' and has a search icon. Below the title are tabs for 'Inputs' and 'Outputs'. Under 'Inputs', there are sub-tabs for 'Input 1', 'Input 2', 'Input 3', and 'Input 4'. The 'Input 1 Settings' section is active, showing a table of configuration options:

Active	No
Query on	Low (0)
Action	E-mail
Text	
E-Mail address	


Below the settings is a 'current State' section with a table showing the status of various inputs:

Input 1	●
Input 2	●
Input 3	●
Input 4	●
Dial Out	●

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.

Input 1 Settings

Active	<input type="checkbox"/>
Query on	Low (0) ▼
Action	E-mail ▼
E-Mail address	<input type="text"/>
Text	<input type="text"/>

Save

Close

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: <ul style="list-style-type: none"> • 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 , ; . : - _ # + * ~ ^ ° ! () = ? § \$ % & / < >
<input type="button" value="Save"/>	Clicking on " Save " temporarily saves the current entries/changes. But the changes are not yet enabled.
<input type="button" value="Close"/>	Clicking on " Close " discards the current input/changes.

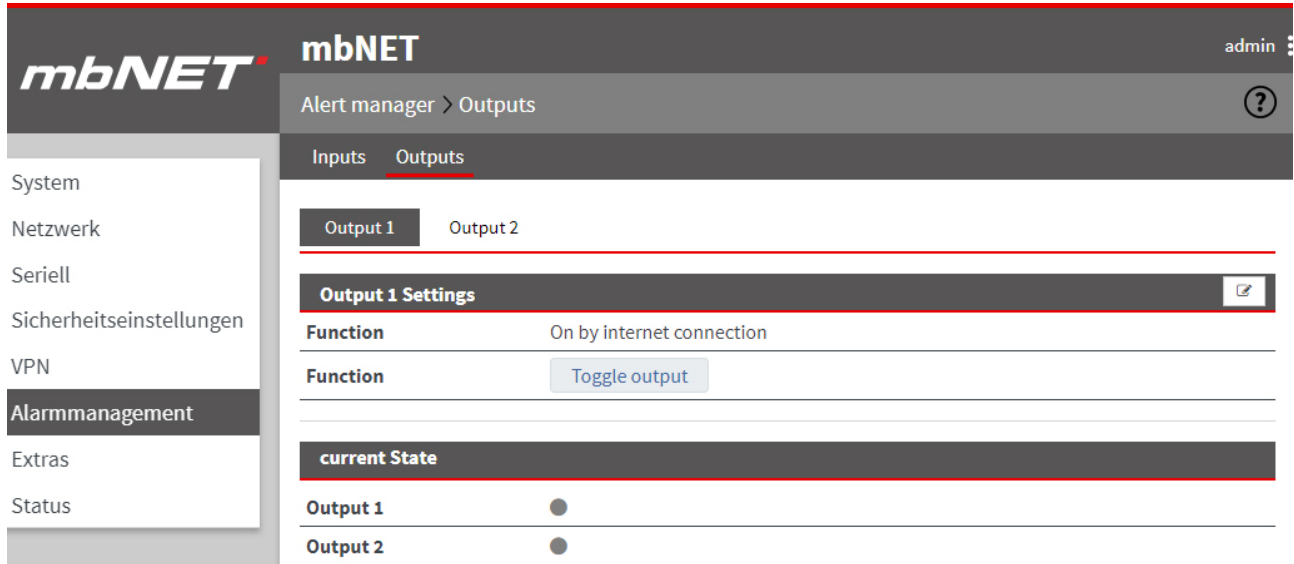
NOTICE

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.

26.2 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.

Output 1 Settings

Function

On by internet connection

Save

Close

Designation	Description
Function	<p>Selection field for the condition for switching the selected output:</p> <ul style="list-style-type: none"> • 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.

27 Extras



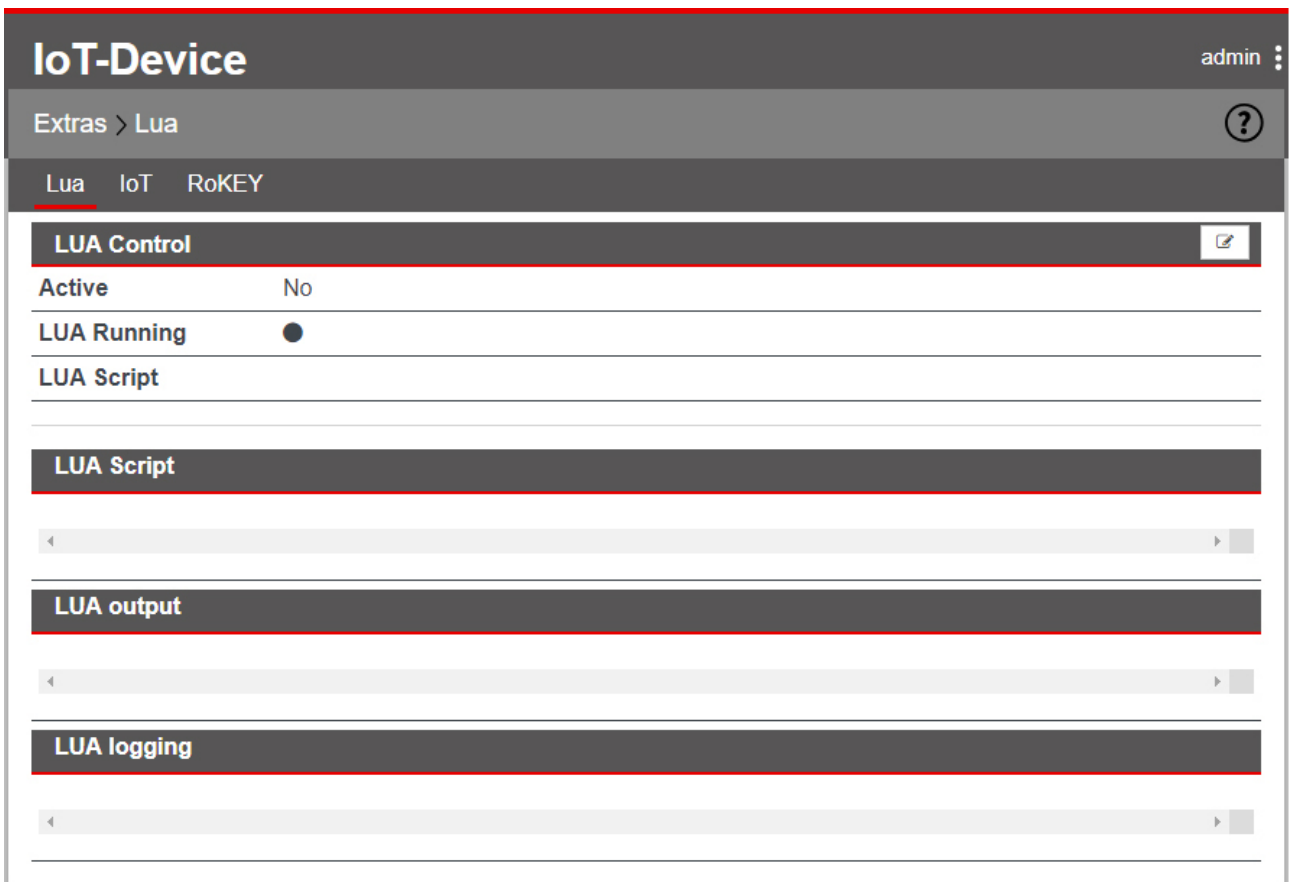
In the category Extras you will find the submenus

- Lua
- IoT
- RoKEY

27.1 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

Lua

✎
LUA Control

Active	No
LUA Running	

Click the Edit icon  to edit the corresponding function.

LUA Settings

Active	<input checked="" type="checkbox"/>
Import	<input type="text" value="Datei auswählen"/> Keine ausgewählt
	<input type="button" value="Import"/>

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

< >

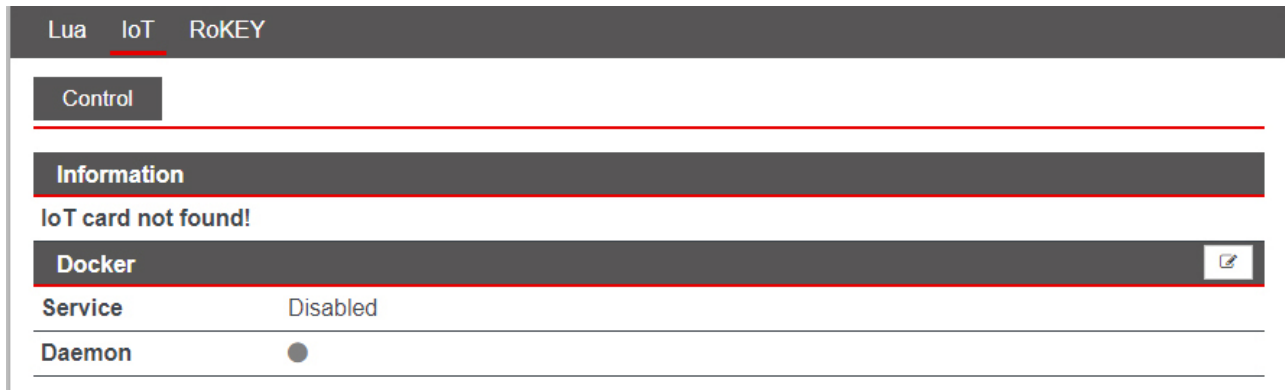
All error messages are shown here.

27.2 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.



The screenshot shows the IoT Control interface. At the top, there are tabs for 'Lua', 'IoT', and 'RoKEY'. Below the tabs is a 'Control' button. Underneath is an 'Information' section with the message 'IoT card not found!'. The 'Docker' section is highlighted, showing a table with the following content:

Service	Status
Service	Disabled
Daemon	<input type="radio"/>

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

27.2.1 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.



This screenshot is identical to the one above, but with a red arrow pointing to the edit icon (a square with a pencil) located in the top right corner of the Docker section.

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

Docker Settings

Enable

Save Close

- ▶ [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.

Lua IoT RoKEY

Control Network Key Management Firmware

Information

Serial number	EA000175
License Type	advance

Docker 

Service	Enabled
---------	---------

27.2.2 IoT > Control - after activating mbEDGE

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

Lua IoT RoKEY	
Control Network Key Management Firmware	
Information	
Serial number	EA000175
License Type	advance
Docker	
Service	Enabled
Daemon	●
Docker Management	
Service	Disabled
Link to User Interface	Management
Flows and Dashboard	
Service	Disabled
Use HTTP instead of HTTPS (only mbEDGE)	
Link to Flows(Node-Red)	Flows
Link to Dashboard(Node-Red)	Dashboard
Backup and Delete flows	

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.

27.2.3 IoT > Control - activate Docker Management

NOTICE

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

System > User ?								
Info CTM Settings Web <u>User</u> Certificates Memory devices Logging Configuration Firmware								
User management +								
Username	Password	Full name	Adminis- tration	Quick- start	Modem Dialin	VPN Dialin	Flows (Node Red) Admin	Docker Management Admin
admin	*****	Administrator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

NOTICE

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

- ▶ Click on the edit icon to activate Docker Management.

Docker Management ✎	
Service	Disabled
Link to User Interface	Management


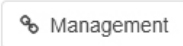
- ▶ Activate the Docker Management.
Click on "Save" to save the change.

Docker Management Settings	
Enable	<input checked="" type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

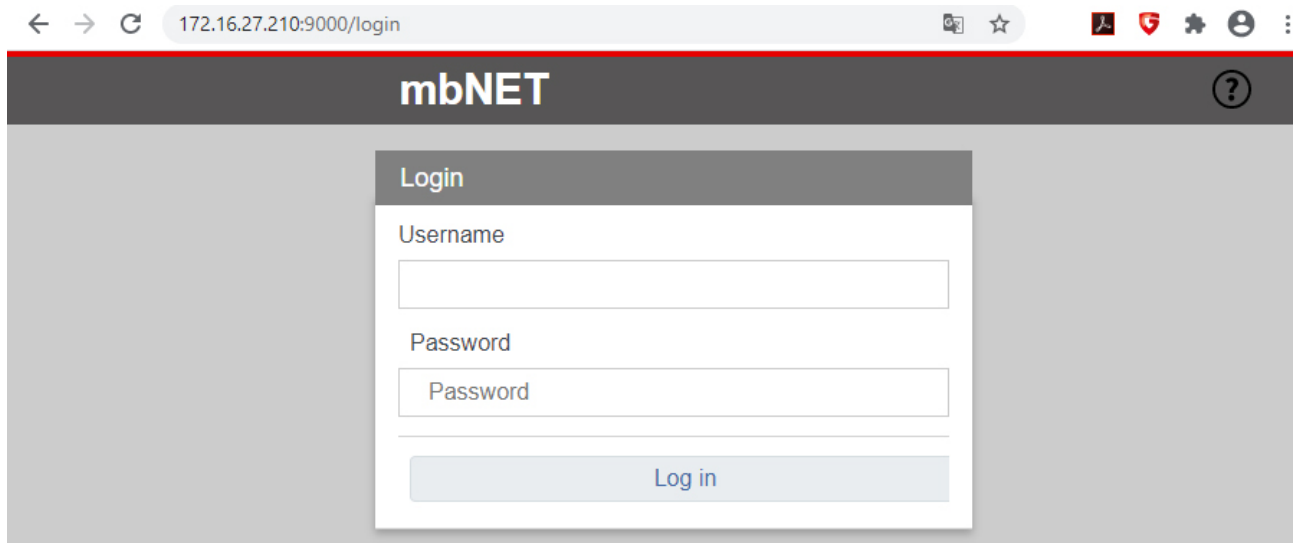
- ▶ [Apply changes](#)

Confirm the activation by clicking on "Apply changes".

27.2.3.1 Link to User Interface

Docker Management 	
Service	Enabled
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:

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

27.2.4 Flows and Dashboard

27.2.4.1 Activate flows and dashboard

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

Flows and Dashboard	
Service	Disabled
Use HTTP instead of HTTPS (only mbEDGE)	
Link to Flows(Node-Red)	Flows
Link to Dashboard(Node-Red)	Dashboard

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

Flows und Dashboard Einstellungen	
Aktivieren	<input checked="" type="checkbox"/>
Verwende HTTP anstatt HTTPS (nur für mbEDGE)	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

▶ [Apply changes](#)

Confirm the activation by clicking on "Apply changes".

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

Flows and Dashboard	
Service	Enabled
Use HTTP instead of HTTPS (only mbEDGE)	
Link to Flows(Node-Red)	Flows
Link to Dashboard(Node-Red)	Dashboard

NOTICE

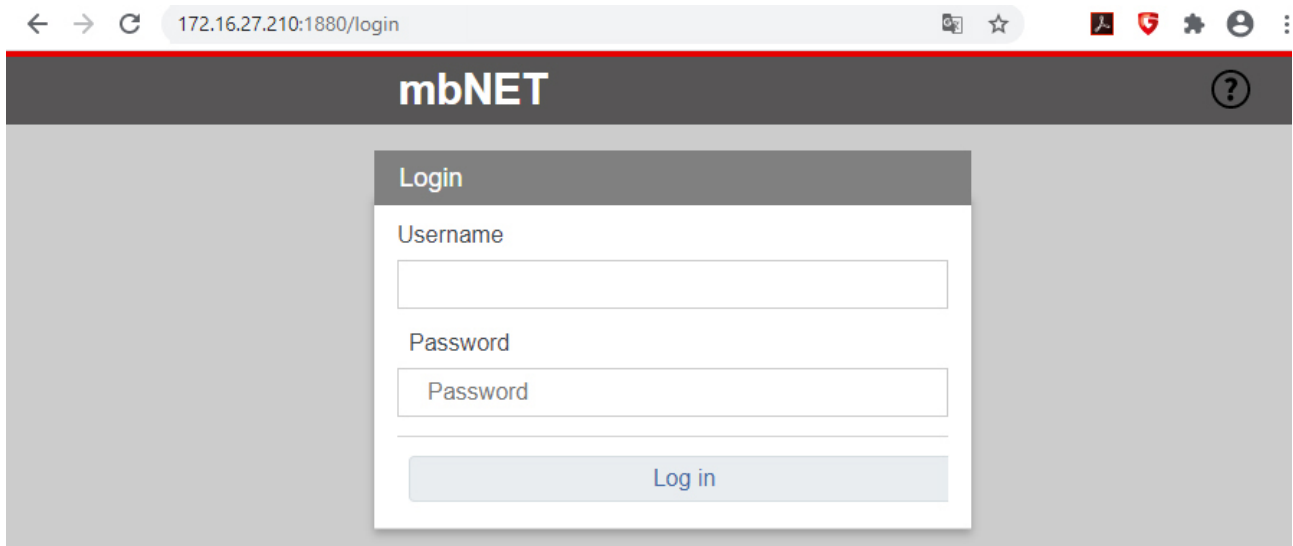
If you want to access the flows and dashboard via an unsecured HTTP connection, activate the checkbox "Use HTTP instead of HTTPS (only for mbEDGE)".

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

27.2.4.1.1 Link to Flows (Node-RED)

Flows and Dashboard	
Service	Enabled
Use HTTP instead of HTTPS (only mbEDGE)	No
Link to Flows(Node-Red)	Flows
Link to Dashboard(Node-Red)	Dashb

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



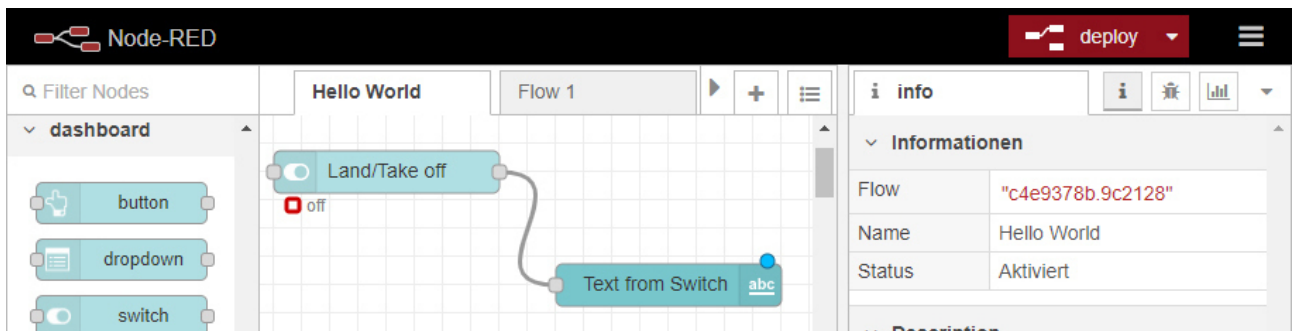
A new browser window, with a login, will open.

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

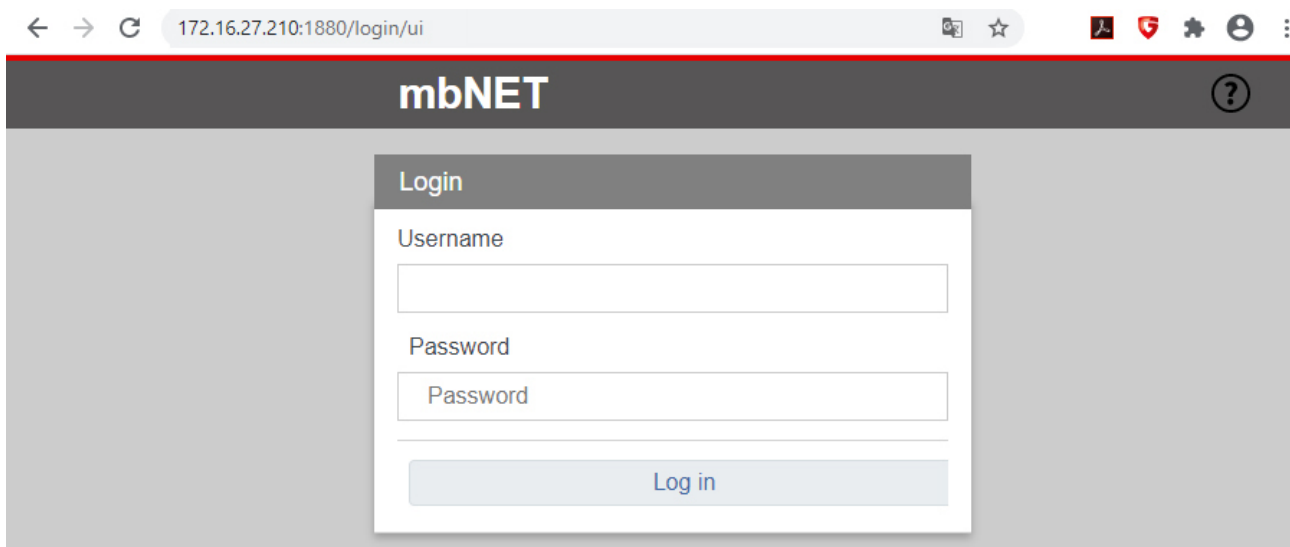
- b) the current user data for the administrator (device access data)
 - standard user name = admin
 - standard password = the device password of the mbNET (see label on the back of the mbNET)



27.2.4.1.2 Link to Dashboard (Node-RED)

Flows and Dashboard	
Service	Enabled
Use HTTP instead of HTTPS (only mbEDGE)	No
Link to Flows(Node-Red)	Flows
Link to Dashboard(Node-Red)	Dashboard

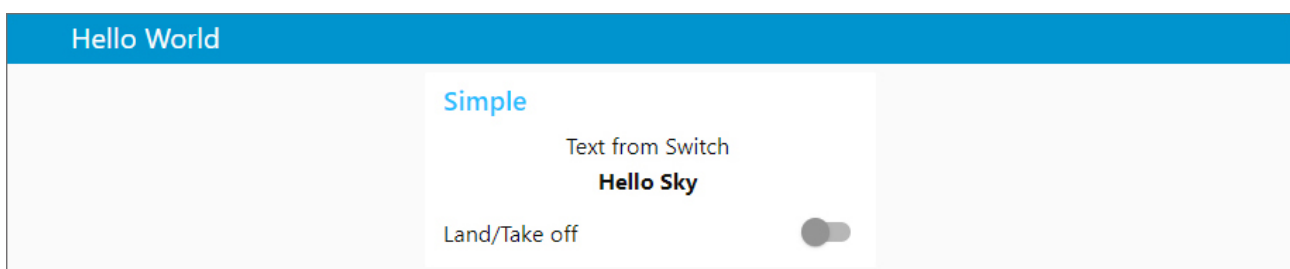
By clicking on the "Dashboard" button you will be redirected to Node-Red-Flows.



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

The access data for this are:

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



27.2.5 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.



Backup and Delete flows

Name of this configuration

- ▶ Choose an option (Download or Delete)

27.3 Network

Extras > IoT ?

Lua
IoT
RoKEY

Control
Network
Key Management
Firmware

Docker Interface ✎

Docker IP Address

Subnetmask

Firewall Settings for Node-Red ✎

Allow following TCP ports

Allow following UDP ports

- **Docker Interface**

Adjust the IP address of the Docker Daemon (runtime for the IoT services and Node-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 firewall rule.

Firewall Settings for Node-Red

TCP-Ports	<input style="width: 80%;" type="text"/>
UDP-Ports	<input style="width: 80%;" type="text"/>

Save
Close

- 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".

27.4 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.

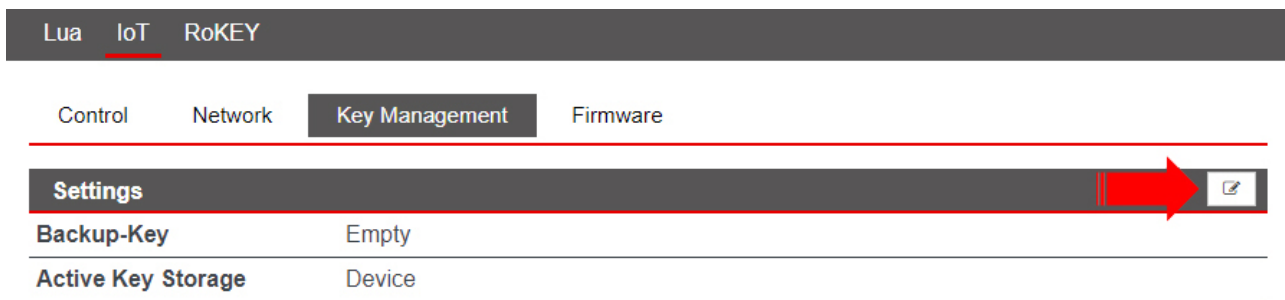
NOTICE

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


The screenshot shows a web interface for IoT settings. At the top, there is a breadcrumb 'Extras > IoT' and a help icon. Below this is a navigation bar with 'Lua', 'IoT', and 'RoKEY'. Underneath, there are tabs for 'Control', 'Network', 'Key Management', and 'Firmware'. A 'Settings' header is followed by a table with two rows: 'Backup-Key' with the value 'Empty' and 'Active Key Storage' with the value 'Device'. A settings icon is visible in the top right of the settings section.

Settings	
Backup-Key	Empty
Active Key Storage	Device

27.4.1 Create Backup-Key

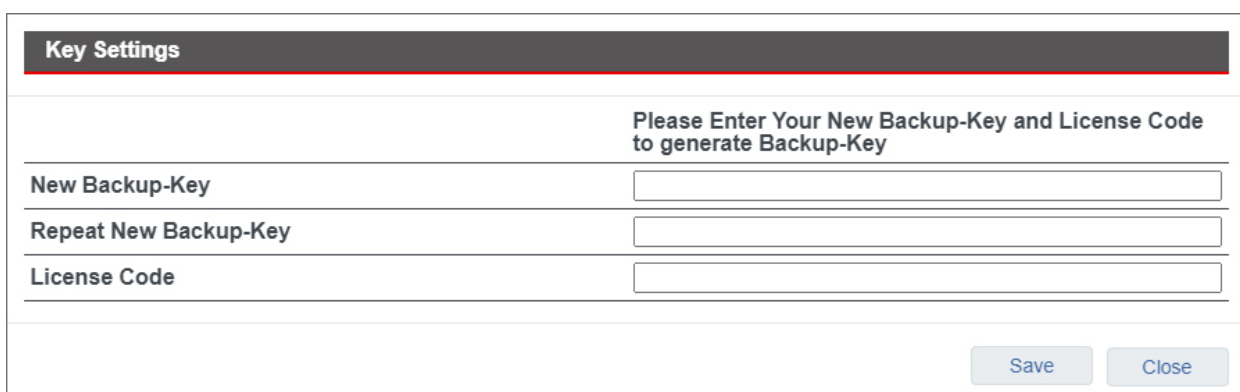


Control Network **Key Management** Firmware

Settings 

Backup-Key	Empty
Active Key Storage	Device

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




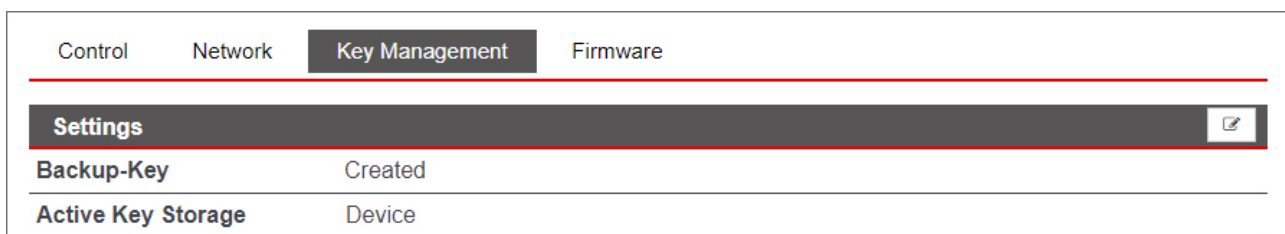
Key Settings

Please Enter Your New Backup-Key and License Code to generate Backup-Key


New Backup-Key	<input type="text"/>
Repeat New Backup-Key	<input type="text"/>
License Code	<input type="text"/>

Save Close

- ▶ 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".



Control Network **Key Management** Firmware

Settings 

Backup-Key	Created
Active Key Storage	Device

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

27.5 Firmware

Extras > IoT

Lua IoT RoKEY

Control Network Key Management Firmware


mbEDGE-NodeRED

Current Firmware Version	v1.0.0-advance
Latest Available Firmware Version	v1.0.0-advance

mbEDGE-Portainer.io

Current Firmware Version	1.24.0-1
Latest Available Firmware Version	1.24.0-1

Start Upgrade

Upgrade Progress/State  Finished Upgrade

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.

27.6 RoKEY

The screenshot shows the 'RoKEY' configuration page in the mbNET IoT-Device web interface. The page is titled 'IoT-Device' and has 'admin' in the top right corner. The breadcrumb is 'Extras > RoKEY'. The 'RoKEY' tab is selected. Under the 'Key Switch' section, the 'Key Switch position' is 'Online (ONL)' and a red key switch icon is shown. Under the 'Code Switch' section, the 'Code Switch Position' is '0' and a circular dial icon is shown.

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!**

28 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.

28.1 Status > Interfaces

WAN interfaces

State > Interfaces ?	
Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPT	
WAN Interface	
MAC Address	70:B3:D5:8D:90:C7
IP Address	192.168.1.100
Subnetmask	255.255.255.0
DNS Server 1	8.8.8.8
Gateway	192.168.1.1
Received Bytes	0.0B
Sent Bytes	0.0B

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	

28.2 Status > Network

28.2.1 General

State > Network ?

Interfaces Network WLAN Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP >

General Firewall Network participants

Physical Connections : Ethernet Connections

IP address	HW type	Flags	HW address	Mask	Device
192.168.0.2	0x1	0x2	d4:be:d9:48:45:fc	*	eth0

Routing table

Kernel IP routing table						
Destination	Gateway	Genmask	Flags	MSS Window	irtt	Iface
192.168.0.0	0.0.0.0	255.255.255.0	U	0 0	0	eth0

Router Listening Ports

Active Internet connections (only servers)					
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:9002	0.0.0.0:*	LISTEN
udp	0	0	127.0.0.1:514	0.0.0.0:*	
udn	0	0	0.0.0.0:25353	0.0.0.0:*	

Router Connections : Connections to the Router

Active Internet connections (w/o servers)					
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.1:52072	127.0.0.1:1883	TIME_WAIT
tcp	0	0	127.0.0.1:52030	127.0.0.1:1883	TIME_WAIT

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.

Page 254 von 292 | V 6.3.0 - from HW02 - en | Aug. 11th, 2021 |

28.2.2 Firewall

State > Network ?

Interfaces Network WLAN Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP >

General Firewall Network participants

IN / OUT / FORWARD

Chain INPUT (policy DROP 0 packets, 0 bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination	
1	0	0	DROP	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmptype 17 /*
2	0	0	DROP	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmptype 14 /*
3	0	0	DROP	icmp	--	*	*	0.0.0.0/0	0.0.0.0/0	icmptype 13 /*
4	112	4480	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state INVALID
5	445K	30M	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state RELATED

NAT

Chain PREROUTING (policy ACCEPT 14386 packets, 2070K bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination	
1	14386	2070K	NEW	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state NEW
2	14386	2070K	prerouting_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
3	14386	2070K	prerouting_fwd	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
4	0	0	prerouting_wan_eth	all	--		eth1	* 0.0.0.0/0	0.0.0.0/0	
5	0	0	prerouting_internet	all	--		eth1	* 0.0.0.0/0	0.0.0.0/0	

Chain INPUT (policy ACCEPT 1814 packets, 516K bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination

Chain OUTPUT (policy ACCEPT 13306 packets, 798K bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination

Chain POSTROUTING (policy ACCEPT 13306 packets, 798K bytes)

IN/OUT/FORWARD

Displays incoming and outgoing data traffic as well as forwarding.

NAT

Displays natted data traffic.

28.2.3 Network participants

Status > Network ?

Interfaces Network Internet DHCP DNS Server DynDNS NTP VPN-OpenVPN IoT Runtime >

General Firewall **Network participants**

Network participants

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
172.16.31.222	28:63:36:80:18:5f	1	60	Unknown vendor
172.16.31.34	70:b3:d5:64:2e:bd	1	60	MB Connect Line GmbH Fernwartungssysteme
0.0.0.0	e4:90:69:a7:53:c1	1	60	Unknown vendor

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

28.3 Status > Modem

28.3.1 GSM information

Manual control of the GSM modem

State > Modem ?

Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PP >

GSM Informations

Modem

Manual Control of the GSM modem

Restart

▶ Execute

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

Information

Information

Signal Quality	 77%
GSM Service	LTE
SIM card slot	SIM 1
SIM State	OK
Provider	Telekom.de
Logging	<pre style="font-family: monospace; font-size: 0.9em; margin: 0;"> Jun 6 00:50:41 nero user.info kernel: [25384.177480] option 2-1:1.0: GSM modem (1-port) converter Jun 6 00:50:41 nero user.info kernel: [25384.179060] usb 2-1: GSM modem (1-port) converter now att Jun 6 00:50:41 nero user.info kernel: [25384.181410] option 2-1:1.3: GSM modem (1-port) converter Jun 6 00:50:41 nero user.info kernel: [25384.189008] usb 2-1: GSM modem (1-port) converter now att </pre>

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.

28.3.2 Modem

Status > Modem ?

Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PP

GSM Informations Modem

Modem-Connection

User	Active	IP local	IP Remote
Information from the last connection			
Connected	●		
Sent Bytes			
Received Bytes			
Modem Commands			
Modem Command (without AT)	<input style="width: 100%;" type="text"/>		▶ Execute

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	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.
Bytes Received	

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.
---------------------------------------	--

28.4 Wi-Fi

Information

State > WLAN ?

Interfaces Network WLAN Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP

Information

Connected	●
SSID	
Signal Quality	<div style="border: 1px solid #ccc; width: 100px; height: 15px; display: flex; justify-content: space-between;"> </div> <p style="margin-top: 2px;">0 %</p>
Operating Frequency	0
IP Address	
Subnetmask	
Gateway	

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	
Subnet mask	Displays the settings on the Wi-Fi connection (local connection) of the router. The IP address is displayed if the router has a physical connection.
Gateway	

Available Wi-Fi networks

Available WLAN Networks			
	SSID	Signal Quality	
Cell 1	MB Connect Line Guest WLAN	-89 dBm	<input type="button" value="Q"/>
Cell 2	MB Entwicklung	-69 dBm	<input type="button" value="Q"/>

Available networks are listed here.

28.5 Internet

State > Internet

Interfaces Network Modem **Internet** DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PP >

Manual Control of the Internet Service

Restart

Internet connection

External Router/Firewall ● Connection established

Internet Logging

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.

28.6 DHCP

State > DHCP ?

Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PP >

DHCP Server LAN

Inactive

DHCP Server WAN

Inactive

Logging

<
>

DHCP Client WAN

IP Address	172.16.20.191
Subnetmask	255.255.255.0
Gateway	172.16.20.253
DNS	172.25.255.250

Logging

```
eth1 :: Tue Jun 5 19:29:18 UTC 2018
bound: IP=172.16.20.191/255.255.255.0 router=172.16.20.253 domain="mars.local" dns="172.25.255.250"
Error: Connection refused
```

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.

28.7 DNS Server

State > DNS Server ?

Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PP >

DNS Server

Name

IP Adress

Logging

System loggings ◀ ▶

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.

28.8 DynDNS

State > DynDNS ?

Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PP >

dyndns

Updated IP Address

Logging

System loggingsSystem
loggings

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.

28.9 NTP

State > NTP ?

Interfaces Network Modem Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PP >

Date and Time

Date Time (UTC) Tue Jun 5 18:15:14 UTC 2018

Locale Date Time Tue Jun 5 20:15:14 CEST 2018

Start NTP Update

Logging

NTP Logging

```
Jun  5 19:15:48 nero user.info settime: NTP is disabled!
Jun  5 20:00:01 nero user.info settime: NTP is disabled!
```

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.

28.10VPN-IPSec

State > VPN-IPSec ?

Interfaces Network WLAN Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP

Connections Inbound Outbound

Name	Active	Connection Data Local	Connection Data Peer	Status IPSec SA	Status ISAKMP SA	Start	Stop
	●			●	●	▶ Start	▶ Stop

System IPSec user logs

```

Jun  5 17:15:16 nero user.info kernel: [ 0.349047] klips_info:ipsec_init: KLIPS startup, Libreswan KLIPS :
Jun  5 17:15:16 nero user.info kernel: [ 0.351649] klips_info:ipsec_alg_init: KLIPS alg v=0.8.1-0 (EALG_M
Jun  5 17:15:16 nero user.info kernel: [ 0.351656] klips_info:ipsec_alg_init: calling ipsec_alg_static_in
Jun  5 17:15:16 nero user.warn kernel: [ 0.351673] ipsec_aes_init(alg_type=15 alg_id=12 name=aes): ret=0
Jun  5 17:15:16 nero user.warn kernel: [ 0.351683] ipsec_aes_init(alg_type=14 alg_id=9 name=aes_mac): ret=
Jun  5 17:15:16 nero user.warn kernel: [ 0.351693] ipsec_3des_init(alg_type=15 alg_id=3 name=3des): ret=0
Jun  5 17:15:16 nero user.info kernel: [ 1.429553] klips_info:ipsec_init: KLIPS startup, Libreswan KLIPS :
    
```

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.

28.11 VPN-PPTP

28.11.1 VPN PPTP server

State > VPN-PPTP ?

< NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnostic Memory device Alertmanager System

Server Clients

Connections Inbound Outbound

Connection	Active	IP local	IP Remote	Connection Status
	●			

System PPTP Server user logs

◀ ▶

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.

28.11.2 VPN PPTP clients

State > VPN-PPTP

< NTP VPN-IPSec **VPN-PPTP** VPN-OpenVPN Diagnostic Memory device Alertmanager System

Server **Clients**

Connections Inbound Outbound

Connection	Active	IP local	IP Remote	Connection Status	Start	Stop
	●				▶ Start	▶ Stop

System PPTP Client user logs

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.

28.12VPN-OpenVPN

State > VPN-OpenVPN ?

< NTP VPN-IPSec VPN-PPTP VPN-OpenVPN Diagnostic Memory device Alertmanager System

Connections Inbound Outbound

Name	Active	Connection Data Local	Connection Data Peer	Start	Stop
	●			▶ Start	▶ Stop

System OpenVPN user logs

◀
▶

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.

28.13IoT

Status > IoT ?

< PSec VPN-PPTP VPN-OpenVPN IoT Diagnosis Memory devices Alarm manager System

Docker Docker Management Flows and Dashboard

28.13.1 IoT > Docker

Status > IoT ?

< PSec VPN-PPTP VPN-OpenVPN IoT Diagnosis Memory devices Alarm manager System

Docker Docker Management Flows and Dashboard

Status

Name	Active	Stop
Service	●	<input type="button" value="▶ Stop"/>

License Type

advance

Logging

```
time="2019-04-02T13:52:17.168635437+02:00" level=warning msg="could not change group /var/run/docker.sock to
time="2019-04-02T13:52:17.351682396+02:00" level=info msg="libcontainerd: started new containerd process" pid
time="2019-04-02T13:52:17.352484854+02:00" level=info msg="parsed scheme: \"unix\"\" module=grpc
time="2019-04-02T13:52:17.352701146+02:00" level=info msg="scheme \"unix\" not registered, fallback to default
time="2019-04-02T13:52:17.525431271+02:00" level=info msg="ccResolverWrapper: sending new addresses to cc: [{
time="2019-04-02T13:52:17.525812562+02:00" level=info msg="ClientConn switching balancer to \"pick_first\"\" m
time="2019-04-02T13:52:17.526328479+02:00" level=info msg="pickfirstBalancer: HandleSubConnStateChange: 0x12f
time="2019-04-02T13:52:21.165743104+02:00" level=info msg="starting containerd" revision=9754871865f7fe2f4e74
time="2019-04-02T13:52:21.172500604+02:00" level=info msg="loading plugin \"io.containerd.content.v1.content\".
time="2019-04-02T13:52:21.174718979+02:00" level=info msg="loading plugin \"io.containerd.snapshotter.v1.btrfs
```

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**

28.13.2 IoT > Docker Management

Status			
Name	Active	Start	Stop
Service		<input type="button" value="▶ Start"/>	<input type="button" value="▶ Stop"/>

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.

28.13.3 IoT > Flows and Dashboard

Status > IoT ?

< P'Sec VPN-PPTP VPN-OpenVPN IoT Diagnosis Memory devices Alarm manager System

Docker Docker Management **Flows and Dashboard**

Status

Name	Active	Start	Stop
Service	●	▶ Start	▶ Stop

Logging

```
> node-red-docker@1.0.0 start /usr/src/node-red
> rm -rf /usr/src/node-red/.sessions.json && node $NODE_OPTIONS node_modules/node-red/red.js -v $FLOWS "--use

> node-red-docker@1.0.0 start /usr/src/node-red
> rm -rf /usr/src/node-red/.sessions.json && node $NODE_OPTIONS node_modules/node-red/red.js -v $FLOWS "--use

20 Feb 14:38:52 - [info]

Welcome to Node-RED
=====
<
```

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**

28.14 Runtime

NOTICE

This function is only relevant if you operate the mbNET in the mbCONNECT24 portal.

28.15Diagnostics - Network Resources

Status > Diagnosis ?

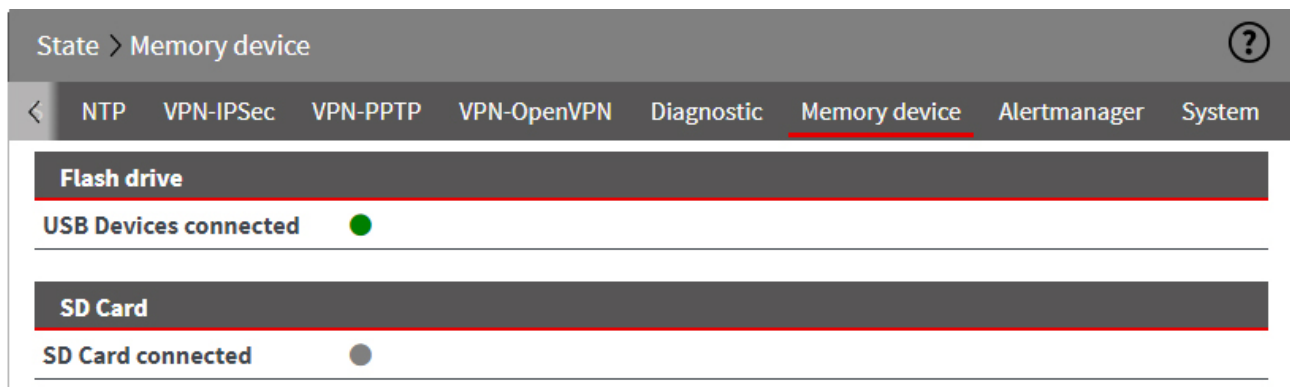
< PN-IPSec VPN-PPTP VPN-OpenVPN IoT Runtime Diagnosis Memory devices Alarm manager >

Network Utilities


Ping	<input type="text" value="google.com"/>	<input type="button" value="▶ Ping"/>
TraceRoute	<input type="text" value="google.com"/>	<input type="button" value="▶ TraceRoute"/>
NS Lookup	<input type="text" value="google.com"/>	<input type="button" value="▶ NS Lookup"/>
TCPDUMP	<input type="text" value="-i eth0 not port 443"/> <input type="checkbox"/> Save capture to usb	<input type="button" value="▶ TCPDUMP"/>
Port Check	<input type="text" value="www.google.com"/> : <input type="text" value="80"/>	<input type="button" value="▶ Port Check"/>

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: <ul style="list-style-type: none"> • -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. <p>You can find detailed TCPDUMP documentation at www.tcpdump.org</p>
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.

28.16 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

28.17 Alarm Manager

The screenshot shows the 'Alertmanager' configuration page. At the top, there is a breadcrumb 'State > Alertmanager' and a help icon. Below this is a navigation bar with tabs for 'NTP', 'VPN-IPSec', 'VPN-PPTP', 'VPN-OpenVPN', 'Diagnostic', 'Memory device', 'Alertmanager' (which is selected), and 'System'. The main content area is divided into three sections: 'Input/Output', 'System loggings', and 'System loggings'. The 'Input/Output' section is further divided into 'Inputs' and 'Outputs'. Under 'Inputs', there are four columns labeled 'Input 1', 'Input 2', 'Input 3', and 'Input 4'. Each column has a circular LED indicator below it. Input 2's indicator is green, while the others are grey. Under 'Outputs', there are two columns labeled 'Output 1' and 'Output 2', each with a grey circular LED indicator. The 'System loggings' section is currently empty.

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.
<p>The status query is performed and updated approximately every three seconds.</p> <p>green LED symbol  = status = 1</p> <p>grey LED symbol  = status = 0</p>	
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.).

28.18 System

28.18.1 System-Usage

State > System ?

<
NTP
VPN-IPSec
VPN-PPTP
VPN-OpenVPN
Diagnostic
Memory device
Alertmanager
System

System-Usage
System information
MQTT Debug List

CPU Informations

CPU Usage	15.2223%
------------------	----------

RAM in use

Total	504676 KB
Free	169616 KB
Used	<div style="display: flex; align-items: center;"> <div style="width: 66%; height: 15px; background-color: #4a90e2; margin-right: 5px;"></div> <div style="border: 1px solid #ccc; width: 10px; height: 10px; margin-right: 5px;"></div> <div style="border: 1px solid #ccc; width: 10px; height: 10px; margin-right: 5px;"></div> <div style="border: 1px solid #ccc; width: 10px; height: 10px; margin-right: 5px;"></div> <div style="border: 1px solid #ccc; width: 10px; height: 10px; margin-right: 5px;"></div> <div style="margin-left: 5px;">66% (335060 KB)</div> </div>

Flash in use

Configuration flash	511 KB
temporary flash (Log files)	300 KB

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.

28.18.2 System Information

The screenshot shows the 'System' status page in the mbNET interface. The top navigation bar includes 'Status > System' and a help icon. Below it, a menu contains 'Interfaces', 'Network', 'Internet', 'DHCP', 'DNS Server', 'DynDNS', 'NTP', 'VPN-IPSec', and 'VPN-PPTP'. The main content area has three tabs: 'System-Usage', 'System information' (which is selected), and 'MQTT Debug List'. The 'System information' section is divided into two main parts: 'System Kernel Logging' and 'System error log'. The 'System Kernel Logging' section displays a list of boot logs, including the Linux version (4.10.0-rc7), CPU details (ARMv7 Processor), and memory policy. The 'System error log' section shows a series of error messages from 'crond[1975]' indicating that it cannot open files in the '/etc/cron.d/*' directory. At the bottom of the error log section, there is a button labeled 'Clear Error Memory'.

Status > System ?

Interfaces Network Internet DHCP DNS Server DynDNS NTP VPN-IPSec VPN-PPTP >

System-Usage **System information** MQTT Debug List

System Kernel Logging

```
[ 0.000000] Booting Linux on physical CPU 0x0
[ 0.000000] Linux version 4.10.0-rc7 (yocto@0529c6efeaf8) (gcc version 6.4.0 (GCC) ) #1 Tue Jul 14 09:0
[ 0.000000] CPU: ARMv7 Processor [413fc082] revision 2 (ARMv7), cr=10c5387d
[ 0.000000] CPU: PIPT / VIPT nonaliasing data cache, VIPT aliasing instruction cache
[ 0.000000] OF: fdt:Machine model: MB Connect Line GmbH - NeRo
[ 0.000000] cma: Reserved 16 MiB at 0x9e800000
[ 0.000000] Memory policy: Data cache writeback
```

System error log

```
[Jul 20 19:02:01] > crond[1975]: (root) CAN'T OPEN (/etc/cron.d/*): No such file or directory
[Jul 20 19:03:01] > crond[1975]: (root) CAN'T OPEN (/etc/cron.d/*): No such file or directory
[Jul 20 19:04:01] > crond[1975]: (root) CAN'T OPEN (/etc/cron.d/*): No such file or directory
[Jul 20 19:05:01] > crond[1975]: (root) CAN'T OPEN (/etc/cron.d/*): No such file or directory
[Jul 20 19:06:01] > crond[1975]: (root) CAN'T OPEN (/etc/cron.d/*): No such file or directory
[Jul 20 19:12:01] > crond[1975]: (root) CAN'T OPEN (/etc/cron.d/*): No such file or directory
[Jul 20 19:13:01] > crond[1975]: (root) CAN'T OPEN (/etc/cron.d/*): No such file or directory
```

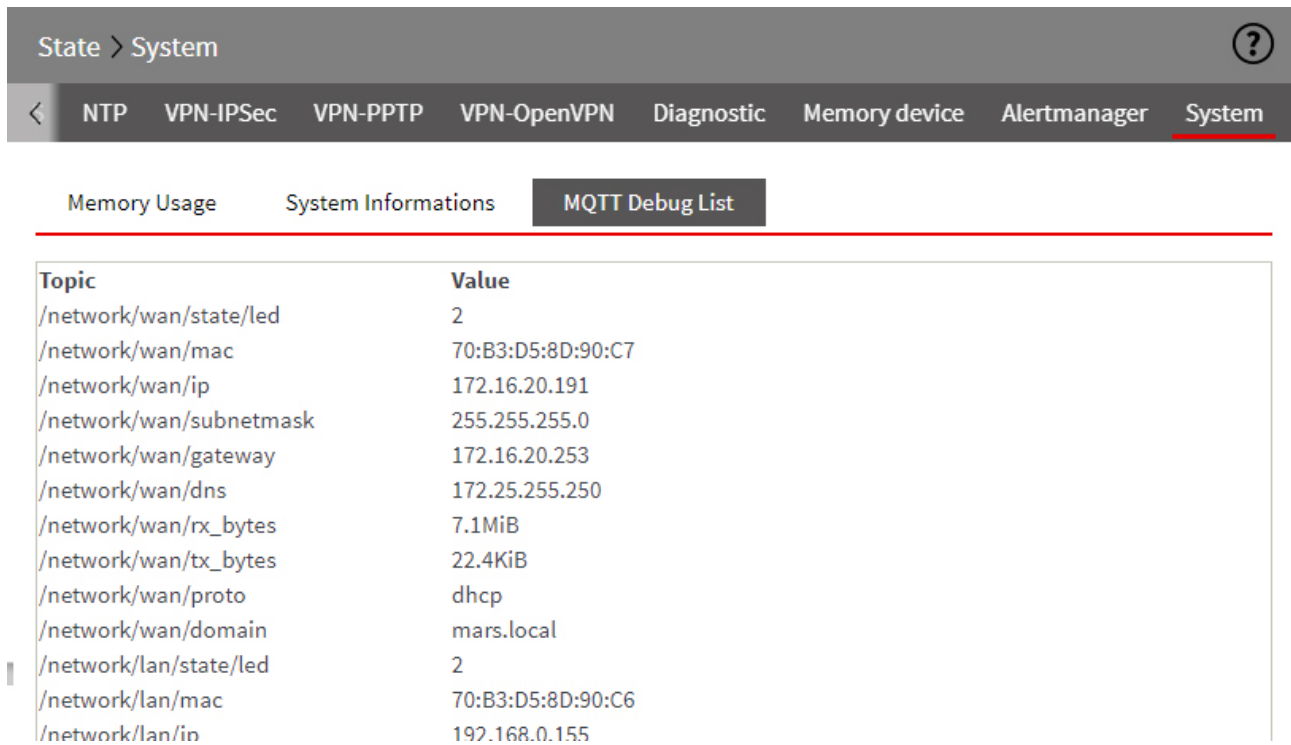
System Kernel Logging

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.

28.18.3 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/in	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".

29 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** 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:

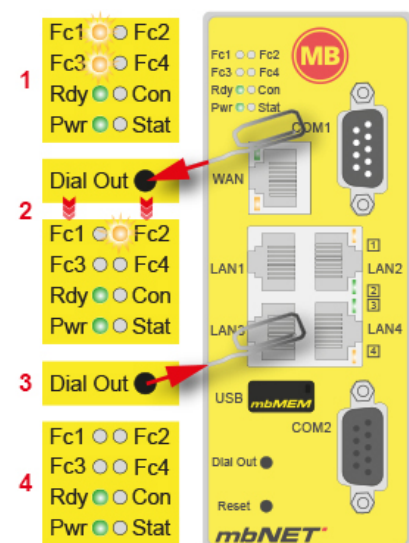
When the **mbNET** is ready for operation (**LED Pwr + Rdy light up**), connect the USB stick to one of the USB ports of the device.

- 1 As soon as the firmware file has been detected by the **mbNET**, **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.

30 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

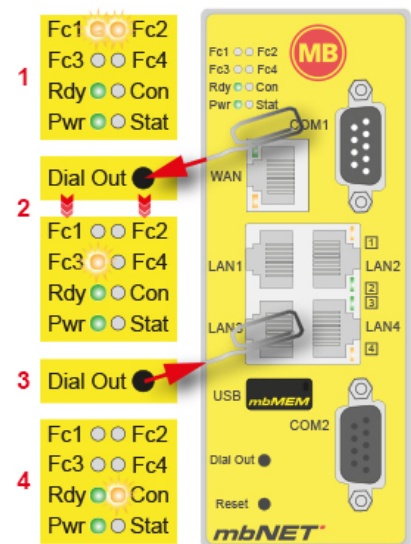
Execution:

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.

31 Factory settings when delivered

31.1 IP address of the mbNET

The **mbNET** is set to the following IP address in the factory:

IP address 192.168.0.100

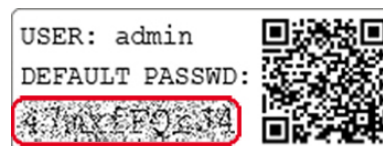
Subnet mask 255.255.255.0

31.2 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!

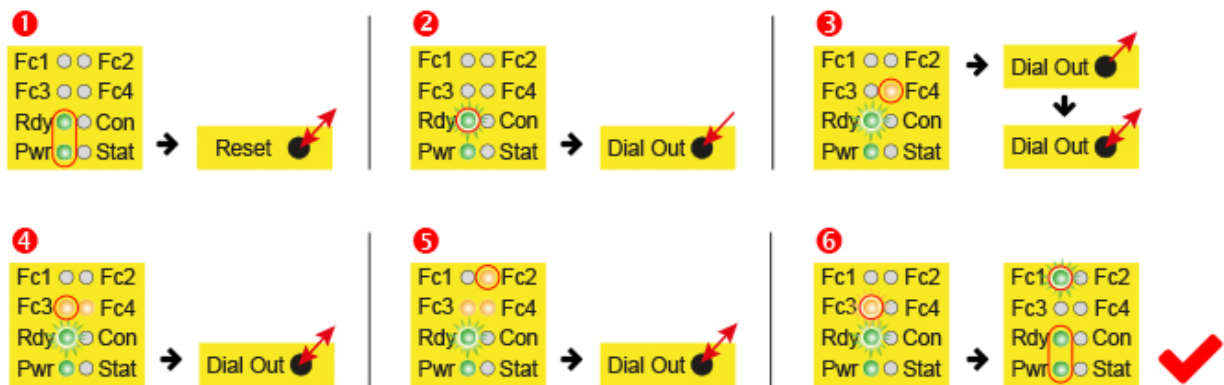
32 Load factory settings

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.
- The device must be ready for operation (Pwr + Rdy LEDs light up).

Execution:



- 1 Switch on the mbNET or press the **Reset** button.
- 2 When LED **Rdy** flashes (green) => **Press and hold** the **Dial Out** button.
- 3 When LED **Fc4** is lit => release the **Dial Out** button and press again.
- 4 When LED **Fc3** is lit => press the **Dial Out** button again.
- 5 When LED **Fc2** is lit => press the **Dial Out** button again.
- 6 After approximately 10 - 20 sec. LED **Fc3** flashes.

When both, the **Pwr** and **Rdy** LEDs **light up** and the **Fc1** LED **flashes*** (5Hz), the mbNET is reset to its factory settings and can/must be reconfigured.

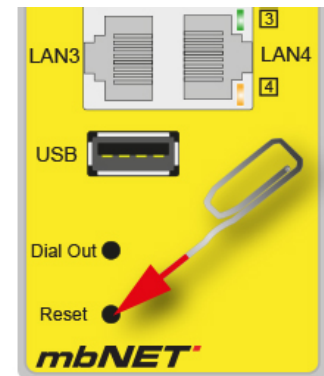
* only for devices with **SIMPLY.connect** function.

33 Device restart (Reset)

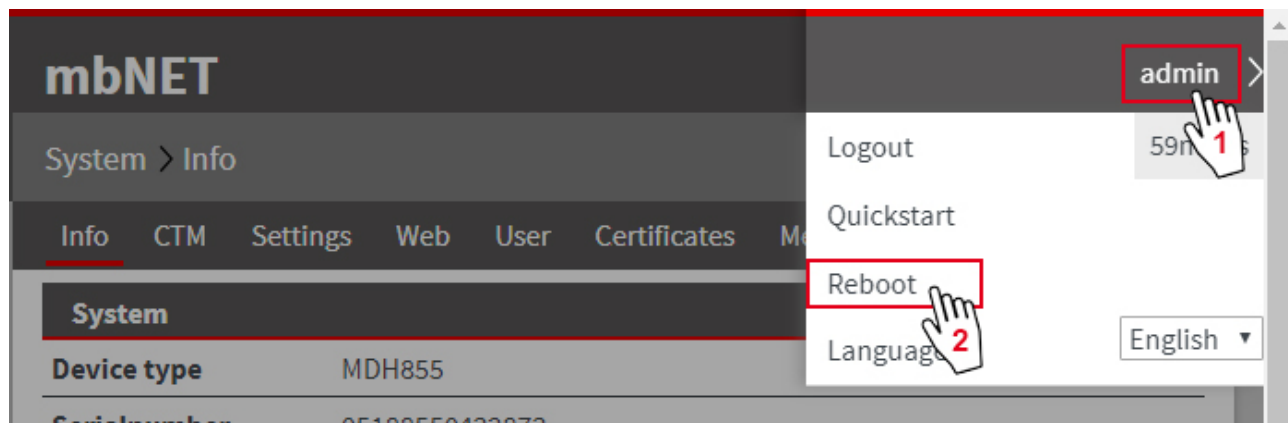
Directly on the device (mbNET) using the reset button

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"

34 Annex

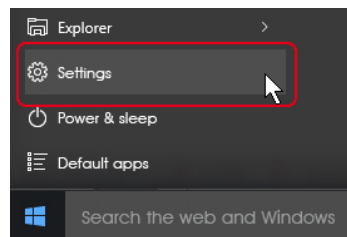
34.1 Set computer address (IP address) in Windows 10

NOTICE

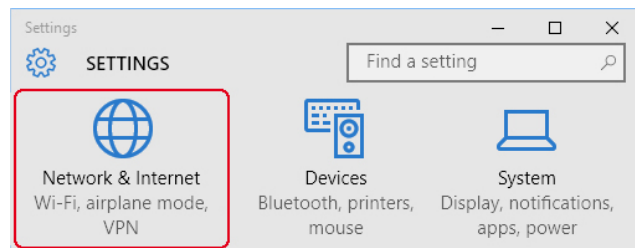
If you want to access the web interface of the mbNET via a configuration PC, the following conditions must be met:

- 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.

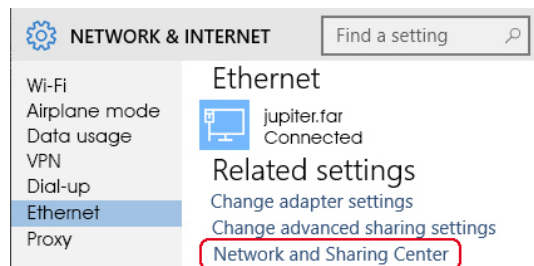
- Open the **Windows Start menu** and go to the **settings**.



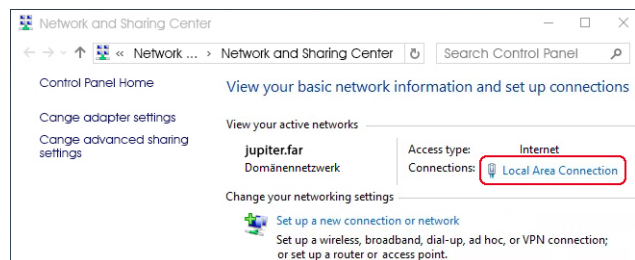
- In Settings, click the **Network and Internet** section.



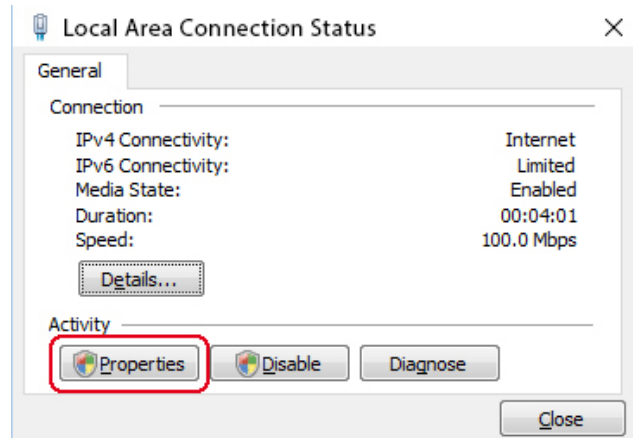
- Under **Network and Internet** click the section **Network and Sharing Centre**.



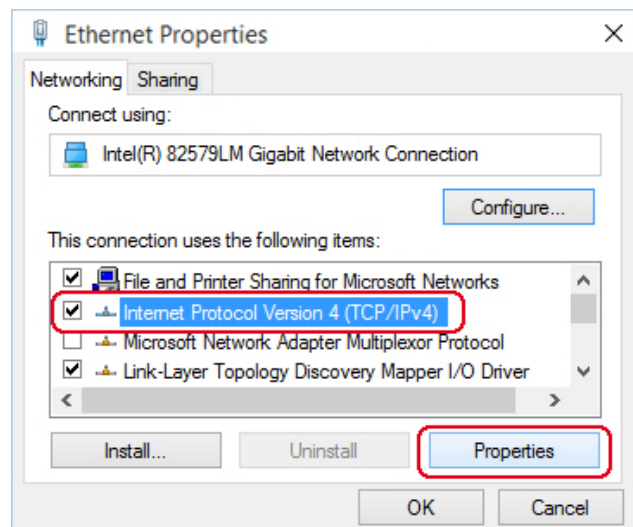
- In the **Network and Sharing Centre**, click on the current **connection** (LAN connection in this case).



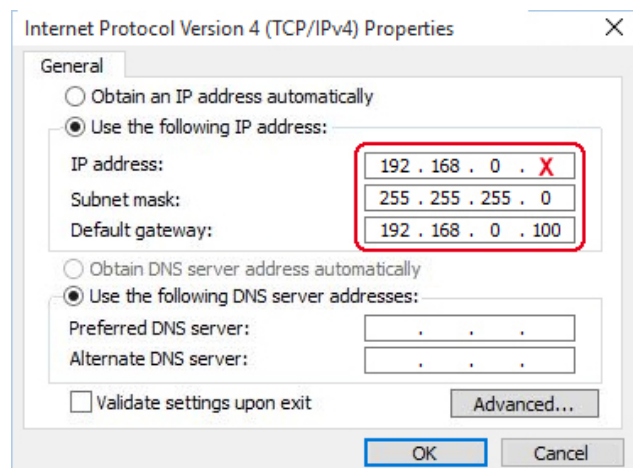
- Click on **properties** in the next window (**Status of LAN connection**).



- 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.

34.2 Modem initialization (AT commands)

General notes on AT commands

The commands can be entered under **Network > Modem > Modem Settings** in the input fields "Modem Initialization".

NOTICE

The **prefix** of a command always consists of the characters "AT".
 These two characters (AT) do not have to be entered in the fields.

- A command is made up of individual characters, which can be described as follows.
- The command consists of an abbreviation and, where appropriate, associated values.
- It is not case-sensitive.
- Multiple commands can be combined into one command line.

Example: L1M1N5

Commands of the analogue modem

B Select communication standard

ATB0 CCITT Modulation
ATB1 Bell Modulation

\B Treatment of the break signal

ATBn Send a break signal to the remote terminal

n= 0-9 in 100 ms units(default **AT\b3**) only possible for a connection that is not error-corrected.

%C Setting the data compression

AT%C0 Data compression inactive
AT%C1 Data compression active

+GCI Country-specific settings

This command is used to configure the analogue modem to country-specific settings.

Example: AT+GCI=B5

L Speaker volume

ATL0, 1 low volume
ATL2 medium volume
ATL3 high volume

M Speaker mode

ATM0 Speaker always OFF.
ATM1 Speaker ON, until data carrier signal is detected.
ATM2 Speaker ON, if the modem is ready to dial.
ATM3 Speaker OFF while the number is dialled, then ON after dialling until a data carrier signal is detected.

+MS Select the modulation type

This command sets the modulation type and the bit rate to be negotiated between the local and the remote modem.

Syntax:

+MS=[<carrier>[,<automode>[,<min_tx_rate>[,<max_tx_rate>[,<min_rx_rate>[,<max_rx_rate>]]]]]

Example:

AT+MS= V34,1,9600,33600,9600,33600

Modulation	<carrier>	Possible baud rates
Bell 103	B103	300
Bell 212	B212	1200 Rx 75 Tx or 75 Rx/1200 Tx
V.21	V21	300
V.22	V22	1200
V.22 to	V22B	1200, 2400
V.23	V23C	1200
V.32	V23C	4800, 9600
V.32 to	V32B	4800, 7200, 9600, 12000, 14400
V.34	V34	2400, 4800, 7200, 9600, 12000, 14400, 16800, 19200, 21600, 24000, 26400, 28800, 31200, 33600
Automode	0 = disabled 1 = enabled (default)	
AT+MS?	Display of current setting	

W Select error correction

- ATN0** Error correction is turned off.
- ATN1** Transparent transmission of any data widths via the serial interface without data buffering and error correction.
- ATN2** V.42LAP-M or MNP 4 error correction. If an error-corrected connection cannot be established, the modem hangs up.
- ATN3** V.42LAP-M or MNP 4 error correction. If an error-corrected connection cannot be established, non-error-corrected connection is attempted.
- ATN4** V.42LAP-M error correction, if this is not possible, the modem hangs up.
- ATN5** MNP error correction, if this is not possible, the modem hangs up.

X Output of messages, dial tone detection

- This command controls how the modem responds to the dial tone and busy signal and how it displays the CONNECT messages.
- ATX0** No busy tone and dial tone detection. I.e., NO CARRIER is displayed following an unsuccessful attempt to dial.
Messages: OK, CONNECT, RING, NO CARRIER, ERROR and NO ANSWER
 - ATX1** Like ATX0 but CONNECTxxx messages with speed information.
 - ATX2** Busy tone detection is disabled, dial tone detection is enabled.
Messages: OK, CONNECT, RING, NO CARRIER, ERROR, NO ANSWER and NO DIAL TONE
 - ATX3** Busy tone is activated, dial tone detection is disabled.
Messages: OK, CONNECT xxx, RING, NO CARRIER, ERROR, NO ANSWER
 - ATX4** Busy signal and dial tone detection is enabled.
Messages: OK, CONNECTxxx, RING, NO CARRIER, ERROR, NO ANSWER and NO DIAL TONE

34.3 Country codes for devices with analogue modem

When initialising the modem with the AT command + GCI, you need the country code.

Example: AT+GCI=B5

No.	Country	Country Code	No.	country	Country Code
1	Afghanistan	B5	2	Albania (AL)	B5
3	Algeria (DZ)	B5	4	American Samoa (AS)	B5
5	Andorra (AD)	B5	6	Angola (AO)	B5
7	Anguilla (AI)	B5	8	Antarctica (AQ)	B5
9	Antigua and Barbuda (AG)	B5	10	Argentina (AR)	07
11	Armenia (AM)	B5	12	Aruba (AW)	B5
13	Australia (AU)	09	14	Austria (AT)	FD
15	Azerbaijan (AZ)	B5	16	Bahamas (BS)	B5
17	Bahrain (BH)	B5	18	Bangladesh (BD)	B5
19	Barbados (BB)	B5	20	Belarus (BY)	B5
21	Belgium (BE)	FD	22	Belize (BZ)	B5
23	Benin (BJ)	B5	24	Bermuda (BM)	B5
25	Bhutan (BT)	B5	26	Bolivia (BO)	B5
27	Bosnia and Herzegovina (BA)	B5	28	Botswana (BW)	B5
29	Bouvet Island (BV)	B5	30	Brazil (BR)	16
31	British Indian Ocean Territory (IO)	B5	32	Brunei Darussalam (BN)	B5
33	Bulgaria (BG)	FD	34	Burkina Faso (BF)	B5
35	Burundi (BI)	B5	36	Cambodia (KH)	B5
37	Cameroon (CM)	B5	38	Canada (CA)	B5
39	Cape Verde (CV)	B5	40	Cayman Islands (KY)	B5
41	Central African Republic (CF)	B5	42	Chad (TD)	B5
43	Chile (CL)	B5	44	China (CN)	B5
45	Christmas Island (CX)	B5	46	Cocos (Keeling) Islands (CC)	B5
47	Colombia (CO)	B5	48	Comoros (KM)	B5
49	Congo (CG)	B5	50	Cook Islands (CK)	B5
51	Costa Rica (CR)	B5	52	Cote D'Ivoire (CI)	B5
53	Croatia (HR)	B5	54	Cuba (CU)	B5
55	Cyprus (CY)	FD	56	Czech Republic (CZ)	FD
57	Denmark (DK)	FD	58	Djibouti (DJ)	B5
59	Dominica (DM)	B5	60	Dominican Republic (DO)	B5
61	East Timor (TP)	B5	62	Ecuador (EC)	B5
63	Egypt (EG)	B5	64	El Salvador (SV)	B5
65	Equatorial Guinea (GQ)	B5	66	Eritrea (ER)	B5
67	Estonia (EE)	FD	68	Ethiopia (ET)	B5
69	Falkland Islands (Malvinas) (FK)	B5	70	Faroe Islands (FO)	B5

No.	Country	Country Code	No.	country	Country Code
71	Fiji (FJ)	B5	72	Finland (FI)	FD
73	France (FR)	FD	74	France-Metropolitan (FX)	FD
75	French Guiana (GF)	B5	76	French Polynesia	B5
77	French Southern Territories (TF)	B5	78	Gabon (GA)	B5
79	Gambia (GM)	B5	80	Georgia (GE)	B5
81	Germany (DE)	FD	82	Ghana (GH)	B5
83	Gibraltar (GI)	B5	84	Greece (GR)	FD
85	Greenland (GL)	B5	86	Grenada (GD)	B5
87	Guadeloupe (GP)	B5	88	Guam (GU)	B5
89	Guatemala (GT)	B5	90	Guinea (GN)	B5
91	Guinea-Bissau (GW)	B5	92	Guyana (GY)	B5
93	Haiti (HT)	B5	94	Heard and McDonald Islands (HM)	B5
95	Honduras (HN)	B5	96	Hong Kong (HK)	99
97	Hungary (HU)	FD	98	Iceland (IS)	FD
99	India (IN)	B5	100	Indonesia (ID)	99
101	Iran (Islamic Republic of) (IR)	B5	102	Iraq (IQ)	B5
103	Ireland (IE)	FD	104	Israel (IL)	B5
105	Italy (IT)	FD	106	Jamaica (JM)	B5
107	Japan (JP)	00	108	Jordan (JO)	B5
109	Kazakhstan (KZ)	B5	110	Kenya (KE)	B5
111	Kiribati (KI)	B5	112	Korea-Democratic People's Republic (KP)	B5
113	Korea-Republic of (KR)	B5	114	Kuwait (KW)	B5
115	Kyrgyzstan (KG)	B5	116	Laos (LA)	B5
117	Latvia (LV)	FD	118	Lebanon (LB)	B5
119	Lesotho (LS)	B5	120	Liberia (LR)	B5
121	Libyan Arab Jamahiriya (LY)	B5	122	Liechtenstein (LI)	FD
123	Lithuania (LT)	FD	124	Luxembourg (LU)	FD
125	Macau (MO)	B5	126	Macedonia (MK)	B5
127	Madagascar (MG)	B5	128	Malawi (MW)	B5
129	Malaysia (MY)	6C	130	Maldives (MV)	B5
131	Mali (ML)	B5	132	Malta (MT)	FD
133	Marshall Islands (MH)	B5	134	Martinique (MQ)	B5
135	Mauritania (MR)	B5	136	Mauritius (MU)	B5
137	Mayotte (YT)	B5	138	Mexico (MX)	B5
139	Micronesia(Federated States of) (FM)	B5	140	Moldova-Republic of (MD)	B5
141	Monaco (MC)	B5	142	Mongolia (MN)	B5
143	Montserrat (MS)	B5	144	Morocco (MA)	B5
145	Mozambique (MZ)	B5	146	Myanmar (MM)	B5
147	Namibia (NA)	B5	148	Nauru (NR)	B5

No.	Country	Country Code	No.	country	Country Code
149	Nepal (NP)	B5	150	Netherlands (NL)	FD
151	Netherlands Antilles (AN)	FD	152	New Caledonia (NC)	B5
153	New Zealand (NZ)	7E	154	Nicaragua (NI)	B5
155	Niger (NE)	B5	156	Nigeria (NG)	B5
157	Niue (NU)	B5	158	Norfolk Island (NF)	B5
159	Northern Mariana Islands (MP)	B5	160	Norway (NO)	FD
161	Oman (OM)	B5	162	Pakistan (PK)	B5
163	Palau (PW)	B5	164	Panama (PA)	B5
165	Papua New Guinea(PG)	B5	166	Paraguay (PY)	B5
167	Peru (PE)	B5	168	Philippines (PH)	B5
169	Pitcairn (PN)	B5	170	Poland (PL)	FD
171	Portugal (PT)	FD	172	Puerto Rico (PR)	B5
173	Qatar (QA)	B5	174	Reunion (RE)	B5
175	Romania (RO)	FD	176	Russian Federation (RU)	B5
177	Rwanda (RW)	B5	178	St. Helena (SH)	B5
179	Saint Kitts and Nevis (KN)	B5	180	Saint Lucia (LC)	B5
181	St. Pierre and Miquelon (PM)	B5	182	St. Vincent and the Grenadines (VC)	B5
183	Samoa (WS)	B5	184	San Marino (SM)	B5
185	Sao Tome and Principe (ST)	B5	186	Saudi Arabia (SA)	B5
187	Senegal (SN)	B5	188	Seychelles (SC)	B5
189	Sierra Leone (SL)	B5	190	Singapore (SG)	9C
191	Slovakia (SK)	FD	192	Slovenia (SI)	FD
193	Solomon Islands (SB)	B5	194	Somalia (SO)	B5
195	South Africa (ZA)	9F	196	Sth. Georgia, Sth. Sandwich Islands (GS)	B5
197	Spain (ES)	FD	198	Sri Lanka (LK)	B5
199	Sudan (SD)	B5	200	Suriname (SR)	B5
201	Svalbard and Jan Mayen Islands (SJ)	B5	202	Swaziland (SZ)	B5
203	Sweden (SE)	FD	204	Switzerland (CH)	FD
205	Syrian Arab Republic (SY)	B5	206	Taiwan-Province of China (TW)	FE
207	Tajikistan (TJ)	B5	208	Tanzania-United Republic of (TZ)	B5
209	Thailand (TH)	B5	210	Togo (TG)	B5
211	Tokelau (TK)	B5	212	Tonga (TO)	B5
213	Trinidad and Tobago (TT)	B5	214	Tunisia (TN)	B5
215	Turkey (TR)	FD	216	Turkmenistan (TM)	B5
217	Turks and Caicos Islands (TC)	B5	218	Tuvalu (TV)	B5
219	Uganda (UG)	B5	220	Ukraine (UA)	B5
221	United Arab Emirates (AE)	B5	222	United Kingdom (UK)	FD
223	United States (US)	B5	224	United States Minor Outlying Islands (UM)	B5

No.	Country	Country Code	No.	country	Country Code
225	Uruguay (UY)	B5	226	Uzbekistan (UZ)	B5
227	Vanuatu (VU)	B5	228	Vatican City State (Holy See) (VA)	B5
229	Venezuela (VE)	B5	230	Vietnam (VN)	99
231	Virgin Islands (British) (VG)	B5	232	Virgin Islands (U.S.) (VI)	B5
233	Wallis and Futuna Islands (WF)	B5	234	Western Sahara (EH)	B5
235	Yemen (YE)	B5	236	Yugoslavia (YU)	B5
237	Zaire (ZR)	B5	238	Zambia (ZW)	B5
239	Zimbabwe (ZW)	B5			