mbNET.mini

User Manual

Version: 2.2.0 - EN | June 28th, 2021

MDH860, MDH862 EU, MDH 862 AT&T, MDH863, MDH 866 EU, MDH 866 AT&T, MDH 867
from hardware version HW 02 with firmware from V 2.2.0

By purchasing the ***mbNET.mini*** router, you have chosen a product made in Germany.
Our products are produced exclusively in Germany, which guarantees the highest quality and safeguards jobs in Europe.

The latest information and updates can be found on our homepage www.mbconnectline.com.
We welcome comments, suggestions for improvement or constructive criticism at any time.

SIMPLIFIED EU DECLARATION OF CONFORMITY

Hereby, MB connect line GmbH declares that the radio equipment types MDH 862 EU; MDH 863; MDH 866 EU; MDH 867 are in compliance with Directive 2014/53/EU.
The full text of the EU declaration of conformity is available at the following internet address:
www.mbconnectline.com

Issued by:
MB Connect Line GmbH
Fernwartungssysteme
Winnettener Str. 6
91550 Dinkelsbühl, Germany

Tel:
+49 (0) 700 622 666 32 /
+49 (0) 700MBCONNECT

Website:
www.mbconnectline.com

Table of contents

1 General

Purpose of this documentation

This user manual describes the functions and use of the mbNET.mini router MDH86x.

Please read carefully and retain this information.

Validity of this documentation

This manual is valid for the router ***mbNET.mini*** MDH 860, MDH 862 EU, MDH 862 AT&T, MDH863, MDH 866 EU, MDH 866 AT&T, MDH 867, from hardware version **HW02*** with firmware version from **V 2.2.0**.

Prerequisites / additional required components

The following end devices are suitable for connecting to the mymbCONNECT24.virtual server:

- standard Windows PC with network interface (ethernet interface)
- USB stick recommended format: FAT32 or ext3; maximun size: 4 GB (FAT32), 16 GB (ext3)
- network cable
- internet access

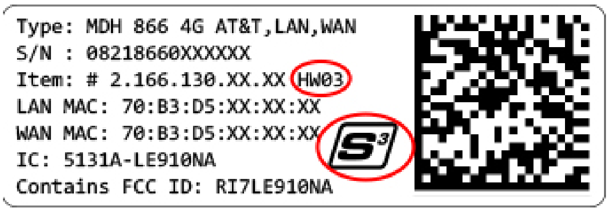
Additional required software

- ***mbCONNECT24***
  mbCONNECT24 is the central portal for secure remote maintenance on the internet.

- ***mbDIALUP*** ** from version V 3.8
  To establish a secure VPN connection to the portal ***mbCONNECT24*** you need the remote client software ***mbDIALUP***.

- ***mbCHECK*** ** from version V 1.1.2
  The program checks that at least one of the 80TCP, 443TCP or 1194TCP ports is enabled in the firewall. One of these ports is needed by mbDIALUP and the device (router) in conjunction with mbCONNECT24. You will then be notified whether connection via mbDIALUP to the portal is possible.

The **Simplify^3**-Logo on the nameplate indicates that the ***SIMPLY.connect*** function is available on the device. ***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/



```
Type: MDH 866 4G AT&T,LAN,WAN
S/N : 08218660XXXXXX
Item: # 2.166.130.XX.XX HW03
LAN MAC: 70:B3:D5:XX:XX:XX
WAN MAC: 70:B3:D5:XX:XX:XX
IC: 5131A-LE910NA
Contains FCC ID: RI7LE910NA
```

* You will find the hardware version on the device nameplate.
** The latest version can be downloaded free of charge from www.mbconnectline.com

Release notes:

Version	Date	Comment
V 1.9 DR01	June 12th, 2017	Previous version V 1.9
V 1.9 DR02	Jan. 25th, 2018	General changes (text and graphics)
V 1.9 DR03	May 4th, 2018	Note in the Technical Specifications on missing CE conformity for MDH 862 AT&T.
V 2.0	Mar. 11th, 2019	The following new device types have been added: MDH 865, MDH 866 EU, MDH 866 AT & T and MDH 867. Technical feature of the new types: 3 x LAN interface, 1 x WAN interface with failover function WAN > Modem / Wi-Fi.
V 2.0 DR01	Apr. 29th, 2019	Correction in chapter 11.3 Initial configuration via the device web interface: *"You must enter the IP address of the mbNET.mini (192.168.0.253) as the default gateway and as the preferred DNS server."* This information is incorrect and has been deleted.
V 2.0 DR02	Oct. 1st, 2019	The chapter ""Maintenance"" has been added, with the remark to check at regular intervals the actuality of the firmware installed on the device.
V 2.0.6	Nov. 18th, 2019	For devices with hardware version HW 02 and firmware from V 2.0.6 , the two I/Os can be configured independently of each other as a digital input or digital output.
V 2.0.6 DR01	Jan. 14th, 2020	Changed data (frequencies and target region) for devices with LTE (4G) module (MDH 862 EU, MDH 866 EU) with hardware version: HW03
V 2.0.8	May 11th, 2020	Change of access data for the device web interface (see chapter "Factory settings on delivery"). An individual device password now applies to the devices described above under "Validity of this documentation". You will find this password on the back of the device.
V 2.0.8 DR01	July 6th, 2020	Add the transmission power of radio modules in the technical data.
V 2.0.8 DR02	Jan 20th, 2021	Adding chapter 12.4, "Digital I/O" Change of alarm management for devices with freely selectable I/Os (only in conjunction with the remote service portal V 2.x). See chapter 12.5, "Alarm management". Change of server locations for RSP mbCONNECT24 => server location CHINA has been replaced by server location ASIA. Please refer chapter 11.8.1, "First Start" > Cloudserver.
V 2.2.0	June 28th, 2021	Description of the ***SIMPLY.connect*** functionality (***S***^{3}). Extension of the LED light codes for devices with ***SIMPLY.connect*** functionality (***S***^{3}). Description of the API for the status display in chap. Device State.

Additional documentation

- First steps mbCONNECT24
  This document describes the initial steps and actions that are necessary to connect an mbNET industrial router to the portal with the remote client mbDIALUP.

Currently manuals and more information

The latest manuals and more information about products related to secure remote maintenance can be found on www.mbconnectline.com

Use of open source software

General

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

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

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

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

Special liability provisions

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

Open source software used

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

2 Safety instructions

- The router is built to the latest technological standards and recognized safety standards (see Declaration of Conformity).
- The router must be installed in a dry location. No liquid must be allowed to get inside the router, as this could result in electric shocks or short circuits.
- The router is for indoor use only.
- Never open the router chassis. Unauthorized opening and improper repair can pose a danger to the user. Unauthorized modifications are not covered by the manufacturer's warranty. Opening up the device voids the warranty.
- The router must be disposed of in line with European regulations and German legislation on electronics and electronic devices and not in general household waste. The device should be disposed of accordingly.

In the present operating instructions the following notes are used:

Notice type	*Description*
ADVICE	An advice signifies additional information and indications such as cyber-security that assists in the assured handling with the system.
ATTENTION	This note indicates a possible risk of damage to hardware and / or software.

3 Legal information

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 those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use
The mbNET.mini router may be used only as described in the manual.

Disclaimer
In this manual all technical information, data and instructions for installation, operation and maintenance are based on our previous experience and insights to the best knowledge. For the details, illustrations and descriptions in these instructions, no claims can be deduced. We assume no liability for damage due to:

- disregard of these operating instructions
- improper use
- technical modifications

Subject to technical and content changes.

Trademarks
The use of any trademark not listed herein is not an indication that it is freely available for use.

4 Notes on Cyber-Security

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

General

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

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

Physical access

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

Security of the software

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

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

Passwords

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

5 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 Functional Overview / Specifications

Brief description

The industrial router ***mbNET.mini*** offers you optimum flexibility and security, making remote communication with your systems both easy and secure. It offers secure IP-based access to Ethernet devices and networks through the remote service platform mbCONNECT24. Therefore, it is not only suitable for remote maintenance applications but also for tasks such as alerts and M2M communication.

Thanks to its compact design, the router will fit into any switch cabinet and provides the perfect system for connecting to different components. The router can be configured via the portal ***mbCONNECT24*** (mymbCONNECT24.mini, -.midi, -.maxi, -.hosted, -.virtual).

Performance characteristics

- The router can be fully configured via the portal mbCONNECT24, mymbCONNECT24.mini, -.midi, -.maxi, -.hosted, -.virtual.
- Can connect to machines and systems via LAN, WAN, Wi-Fi or modem.
- Deployable worldwide using mobile communications plus access via LAN and Internet.
- Secure connection using an integrated firewall with IP filter, NAT, port forwarding and VPN.
- ***USB over IP*** capable
  With the function USB over IP the USB port of the mbNET.mini is transmitted or made available directly to the PC of the mbDIALUP user. All devices connected to the USB port of the mbNET.mini (USB memory, PLC, webcams, etc.) are automatically available on this PC.
- ***SEARCHoverIP*** capable
  With the SEARCHoverIP function, you can also find your PLC via remote maintenance in the network. For example, "virgin" SIEMENS controllers can be found and configured remotely in the network. Furthermore the search function for controls of the brands SchneiderElectric, Rockwell, Beckhoff and Pilz is supported.
- Integrated Ethernet switch 3-port or 4-port - depending on the device type -
- 4G versions support GPRS, EDGE, UMTS, HSPA+, LTE
- 2 pieces I/Os. These connectors can be independently configured as a digital input or digital output.
- OpenVPN security protocol
- Solid metal case for DIN rail mounting
- Ideal for M2M applications
- Secure connection to the **R**emote **S**ervice **P**ortal ***mbCONNECT24***

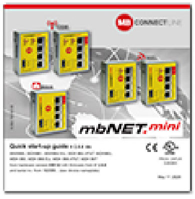
7 Included in delivery

Included in delivery

Please check that your delivery is complete:

mbNET.mini Type ➔	**MDH 860** 3 x LAN 1 x WAN	**MDH 862** 4 x LAN 4G module	**MDH 863** 4 x LAN Wi-Fi	**MDH 866** 3 x LAN 1 x WAN 4G module	**MDH 867** 3 x LAN 1 x WAN Wi-Fi
Supplied accessories ⬇					
Quick start guide	**1 x**	**1 x**	**1 x**	**1 x**	**1 x**
GSM antenna Item No.: 8.002.101.00.00		**1 x**		**1 x**	
Wi-Fi antenna Item No.: 8.002.107.00.00			**1 x**		**1 x**

Quick start guide



GSM antenna

Item No.:
8.002.101.00.00

Wi-Fi antenna

Item No.:
8.002.107.00.00

Should any of these parts are missing or damaged, please contact the following address:

MB connect line GmbH
Winnettener Str. 6
D-91550 Dinkelsbühl
Tel.: +49 (0)9851/282529-0
Fax: +49 (0)9851/282529-99

Please keep the original box and the original packaging in case you need to send the device for repair at a later date.

8 Displays, controls and connections

View of front of the device

MDH 860

3 x LAN
1 x WAN

USB

MDH 862

4 x LAN

4G module
USB

MDH 863

4 x LAN

Wi-Fi
USB

MDH 866

3 x LAN
1 x WAN
4G module
USB

MDH 867

3 x LAN
1 x WAN
Wi-Fi
USB

Connections, interfaces and buttons

Designation	Description
ANT	SMA antenna connector: • SMA ● (MDH 861, MDH 862, MDH 865, MDH 866) • RP SMA ⊙ (MDH 863, MDH 867)
Main	SMA antenna connector for use with one antenna
Div.	SMA antenna connector (combined with "Main") of • a second antenna (macrodiversity) • a MIMO antenna (microdiversity)
WAN	Router WAN connection (customer network, DSL router).
LAN 1 - 3	Local network connection (e.g. machine network, network data transfer).
USB	• Transfer of configuration from USB stick to the device. • Transfer of firmware from USB stick to the device. • Access to free application data via SFTP. • Connection of USB devices (USB memory, PLC, webcams, etc.)
Function	This button has 4 functions and is used according to the status. 1 Establishing connection to portal (depending on configuration) 2 Accepting firmware or configuration from USB stick 3 Loading factory settings 4 Activate the ***SIMPLY.connect **** function
Reset	Pushing this button restarts the device (so-called cold start).

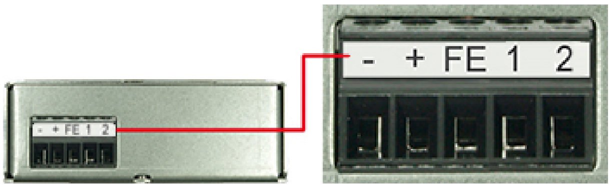
LED light codes

Designation	LED-Status	Description
Pwr (Power) green	off	Device power source is switched off or device is not connected to power source/power pack.
	on	Power source is connected to terminal block and switched on.
Rdy (Ready) green	flashing	After the system has been checked and started (duration approx. 25 sec), the LED flashes for the duration of the starting up process (approx. 90 sec).
	on	The device is ready for operation.
Con (Connect) orange	*The **Con** LED signals the connection status to the Internet and portalserver.*	
	off	No connection to Internet or portal.
	flashing (3Hz)	Internet or VPN connection being established.
	flashing (1,5Hz)	Connection to portal server has been established.
	on	Connection to the Internet has been established.
Usr (User) orange	*Light codes of the LED **Usr** directly after the start of **SIMPLY.connect** *-capable devices:*	
	flashes briefly at intervals (500 msec on - 1500 msec off)	***SIMPLY.connect*** is available but not activated. This means: The ***SIMPLY.connect*** * function is supported by the device. As long as the function is not activated by pressing the **Function** 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 **** is activated. ***SIMPLY.connect*** * is active after the function button has been pressed. The device tries to establish a connection to the ***SIMPLY.connect **** server.
Usr (User) orange	*Light codes of the LED **Usr** during operation:*	
	flashing (3Hz)	Firmware on USB stick ready to be updated.
	flashing (1,5Hz)	Portal configuration on USB stick ready to be transferred.
	on	Firmware or configuration is being copied to the device.
WAN LED	orange flashing	Network data transfer active
	green on	Transfer rate = 100 MBit/s
	green off	Transfer rate = 10 MBit/s
LAN LED 1 – 3	orange flashing	Network data transfer active
	green on	Transfer rate = 100 MBit/s
	green off	Transfer rate = 10 MBit/s

* ***SIMPLY.connect*** is a web application that supports you when creating a device (industrial router mbNET) in the **R**emote **S**ervice **P**ortal ***mbCONNECT24***.

You can find more information about ***SIMPLY.connect*** on our website at: https://simplyconnect.mbconnectline.com/

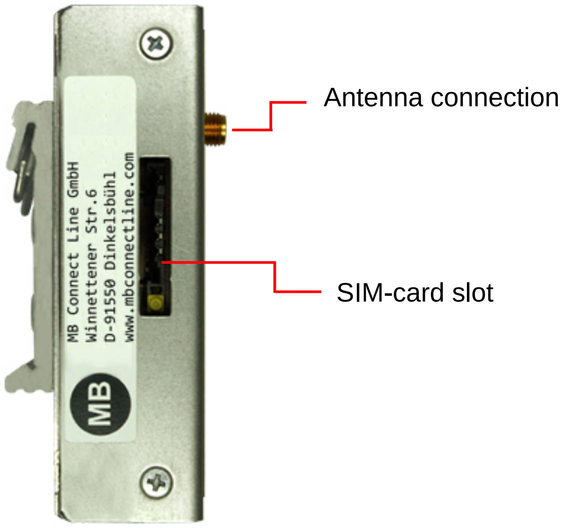
View of bottom of device



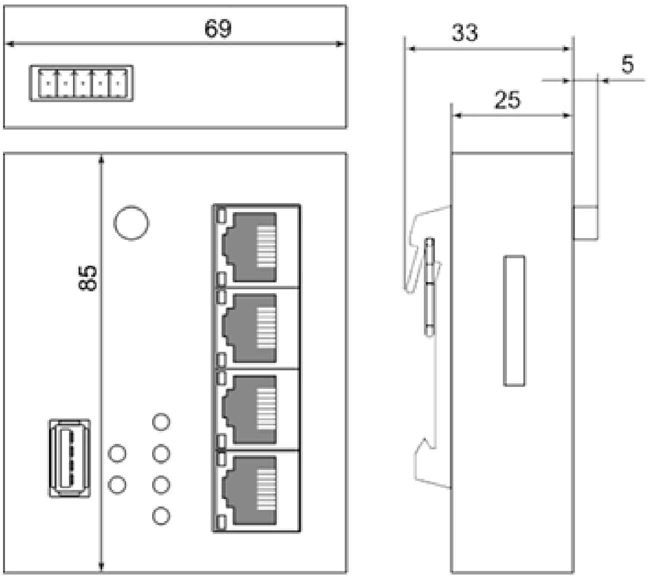
-	0 V DC connection
+	Power source connection 10 - 30 V DC
FE	Functional earth
1*	I/O 1
2*	I/O 2

* I/O 1 and I/O 2 can be configured independently of each other as digital input or digital output.

View of device from left



Device dimensions - mm



9 Interface assignment

9.1 Pinout of the terminal block on the bottom of the device

-	0V DC connection
+	Power source connection 10-30V DC
FE	Functional earth
	I/O
1*	Digital Input 1 (10 - 30V DC)
	Digital Output 1 (max. 0.5 A @24 V)
2*	Digital Input 1 (10 - 30V DC)
	Digital Output 1 (max. 0.5 A @24 V)

* I/O 1 and I/O 2 can be configured independently of each other as digital input or digital output.

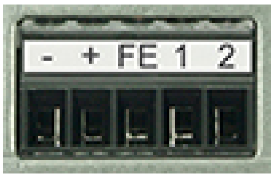


Image 1: Terminal strip on the bottom side

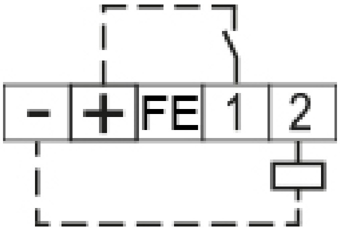
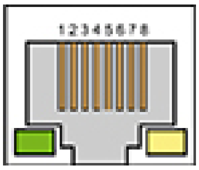


Image 2: Example: I/O 1 = input, I/O 2 = output

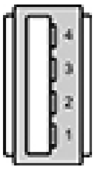
9.2 Pinout of LAN/WAN ports on the front panel of the device

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



9.3 Pinout of the USB port on the front panel of the device

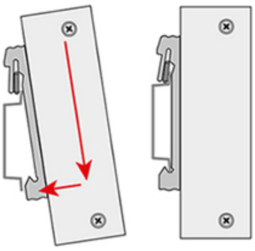
	Signal
1	VCC (+5V)
2	- Data
3	+Data
4	GND



10 Getting started

The device is intended to be installed in switch cabinets and designed to be mounted on top-hat rails (according to DIN EN 50 022).

DIN rail mounting:
Insert the device into the DIN rail. To do this, position the upper guide of the bracket on the rail on the back of the device and then press the device downwards against the rail until fully inserted.



Depending on the device, connect an antenna, and insert a SIM card.

NOTICE

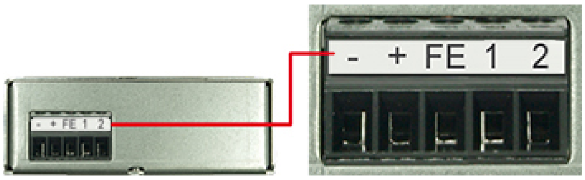
The SIM card used must be Internet- / VPN-enabled. If you have any questions, contact your cell phone operator.

Connect the *mbNET.mini* to the power supply

NOTICE

Before connecting the device to a network or PC, first ensure that it is properly connected to a power supply, otherwise it may cause damage to other equipment.
You should therefore follow the instructions given below.

- Connect equipotential bonding to the functional earth (**FE**).
- Then connect the device to a supply voltage (10 - 30 VDC).
  Make sure the polarity is correct!

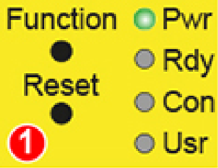


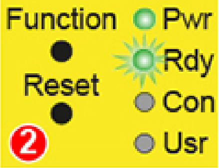
-	0 V DC connection
+	Power source connection 10 - 30 V DC
FE	Functional earth
1*	I/O 1
2*	I/O 2

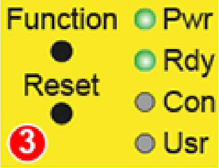
* I/O 1 and I/O 2 can be configured independently of each other as digital input or digital output.

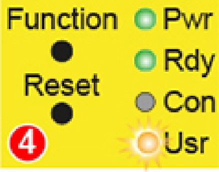
Start sequence

1. After turning on the power supply, the LED **Pwr** lights up.
2. As soon as the system has been checked and started (duration approx. 25 sec), the **Rdy** LED flashes for the dura-tion of the starting up process (approx. 90 sec).
3. When both LEDs - Pwr and Rdy - light up, the ***mbNET*** is ready for operation.
4. With ***SIMPLY.connect*** * capable devices, the **Usr** LED flashes briefly at intervals (500 msec ON - 1500 msec OFF). That means: ***SIMPLY.connect*** is available but deactivated.









* The ***SIMPLY.connect*** function is only available for devices with the **Simplify^3** logo * S^3 (see device nameplate).

SIMPLY.connect is a web application that supports you when creating a device (mbNET) in the Remote Service Portal ***mbCONNECT24***. You can find more information at: https://simplyconnect.mbconnectline.com/

NOTICE

If you want to forego the support of ***SIMPLY.connect***, ignore the flashing LED **Usr** and simply continue with the commissioning / configuration of the device.

*For further support on the **mbNET.mini**, visit our website on www.mbconnectline.com*

11 Initial configuration

Because the ***mbNET.mini*** was designed as a portal device, the initial start-up takes place via the web portal.

- **RSP *mbCONNECT24* V 2.x**

  or

- ***mbCONNECT24* V 1.x**

Generally following procedure applies:

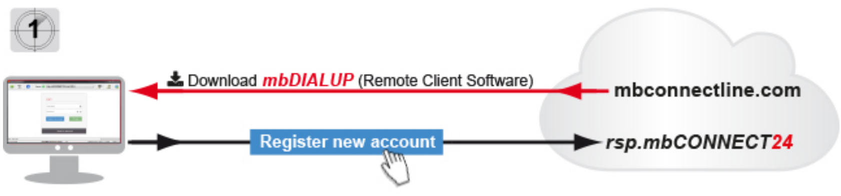
- Add the ***mbNET.mini*** in the portal as a new device.
- Enter the necessary basic data, so that the device can connect to the portal (for example, device name, network settings, connection information, etc.).
- Transfer the device configuration from the portal into the ***mbNET.mini***.

  Alternatively, you can enter the necessary connection basic data direct on the web interface of the device (see chapter: Initial configuration via the device web interface).
  If the mbNET can establish a connection to the Internet, it logs on to mbCONNECT24 with this connection data and fetches its configuration.

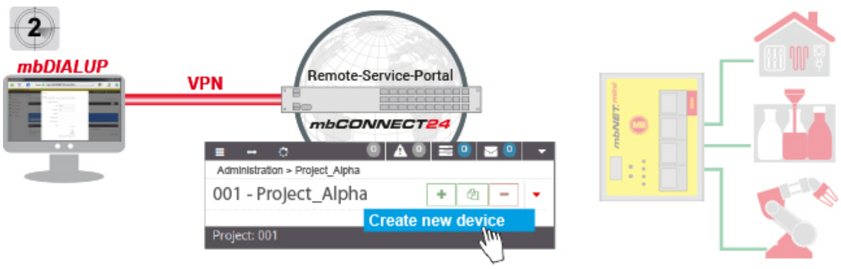
* Some features, such as "USB over IP", "SEARCHoverIP" or the configuration of I/O 1 and I/O 2 as digital input / digital output are not available in portal version V 1.x.

11.1 Initial configuration via RSP mbCONNECT24 V 2.0

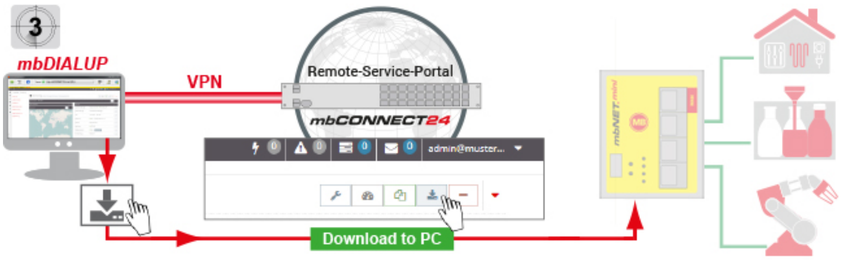
If you not have an account for the remote service portal, here given the necessary information on how to request your access to ***mbCONENCT24*** and how you connect to the portal.



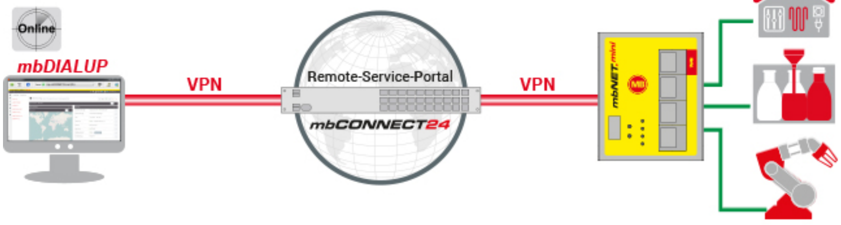
Here you can find out how to create a device and perform the initial configuration for your ***mbNET.mini***.



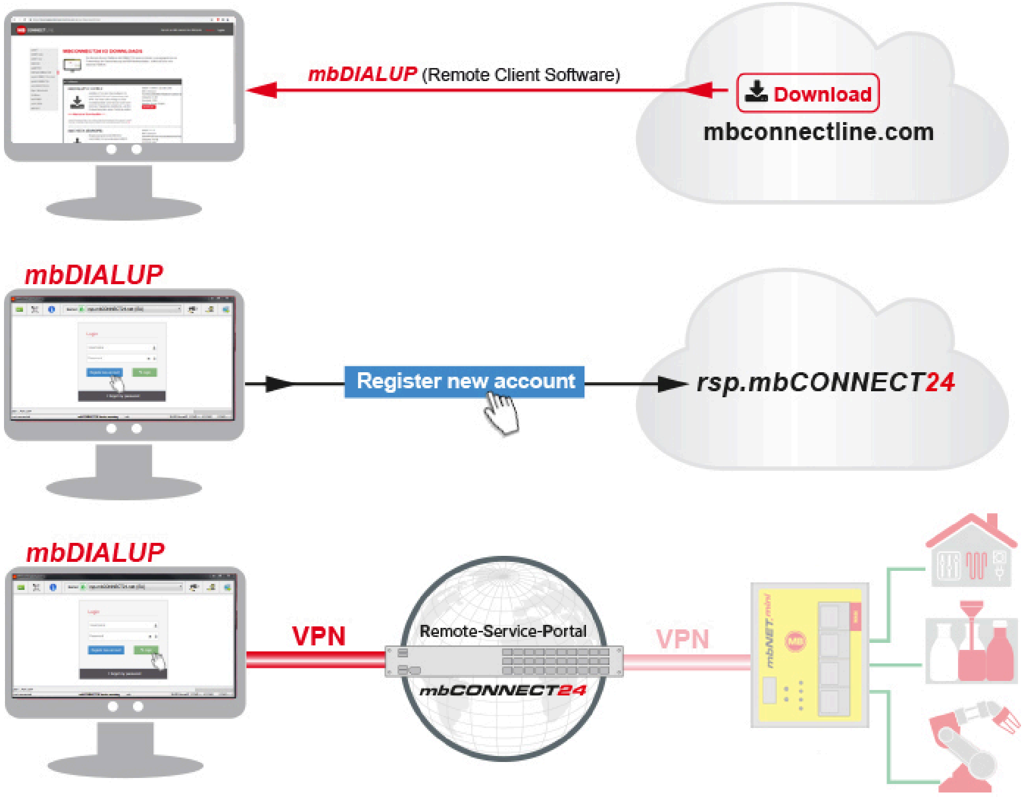
In this section you will learn the different methods, how to transfer the configuration to the ***mbNET.mini***.



In the last section we show you how to connect to devices and machines, and how you finish your ***mbCONNECT24*** session tidy.



11.1.1 Account request - Software download



This chapter describes the steps required to register on the **R**emote **S**ervice **P**ortal ***mbCONENCT24***.

11.1.2 Download mbDIALUP

For the registration on the Remote Service Portal mbCONNECT24, you need the remote client software ***mbDIALUP***.
Download the installation package for ***mbDIALUP*** free of charge from our download area at www.mbconnectline.com.

11.1.3 Install mbDIALUP

Unpack the installation package and run the **setupmbDIALUP.exe** file.

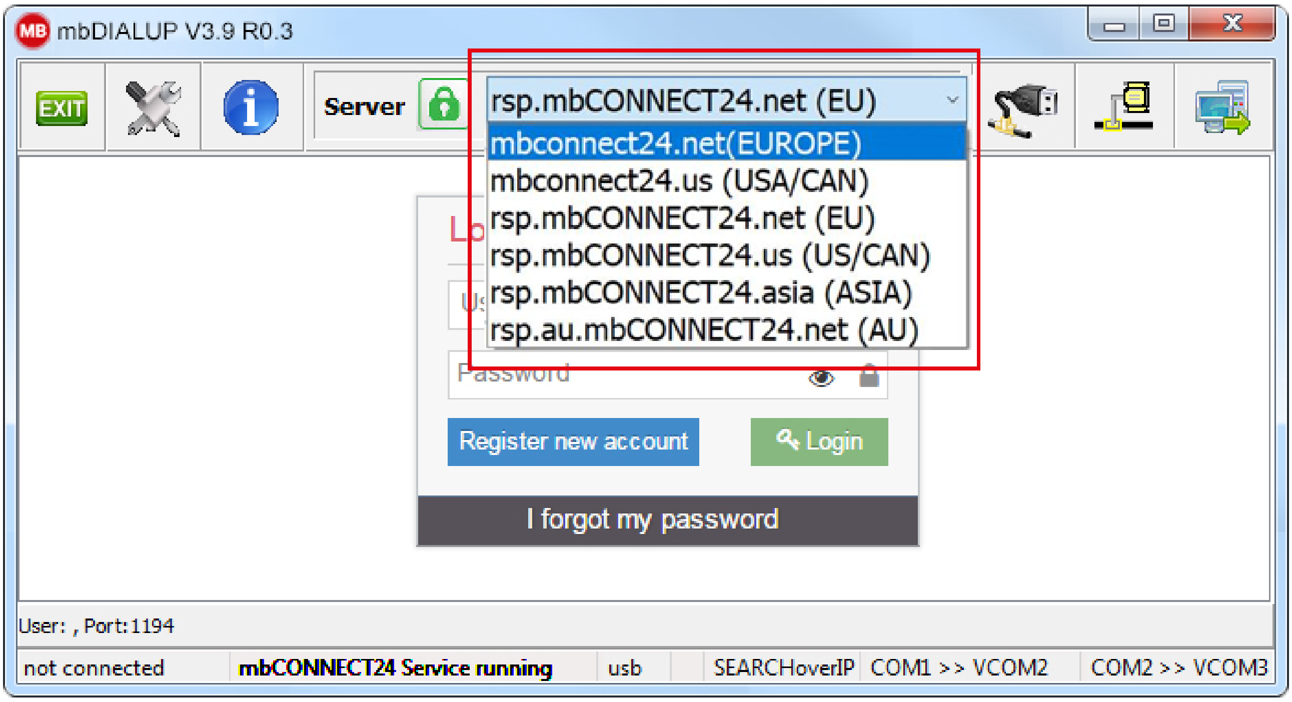
This requires administrator rights on the PC!

When you install mbDIALUP for the first time, you are prompted by the installation assistant to agree to the installation of additionally required third-party software.

Software	Publisher	Function / purpose
WINPcap	Riverbed Technology	This software is required for the "SEARCHoverIP" function.
USB Gate Networks	Eltima Software	This software is required for the "USBoverIP" function.
TAP Windows Provider V9 Network adapter	OpenVPN Technologies, Inc.	This virtual network adapter is required to establish a VPN connection.

11.1.4 Register your account for mbCONNECT24

Start the mbDIALUP program



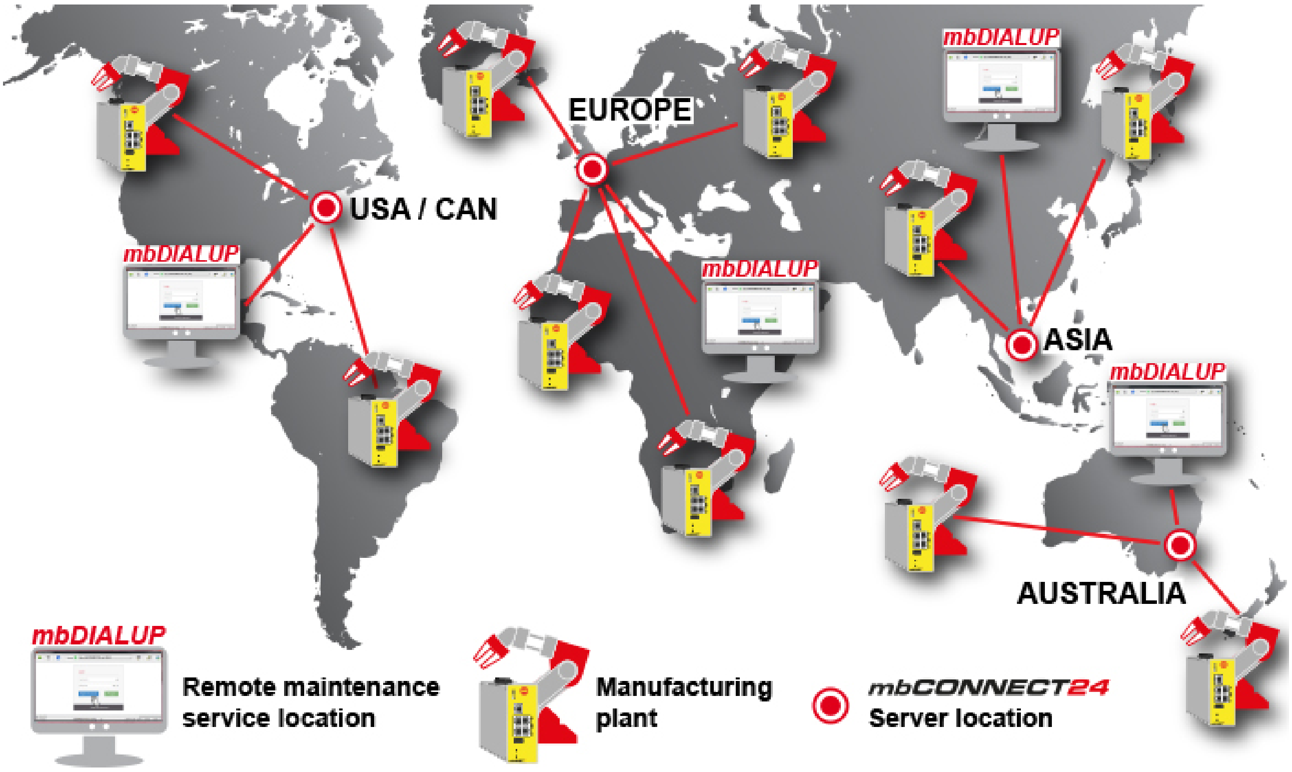
mbDIALUP V3.9 R0.3

User: , Port:1194

not connected | mbCONNECT24 Service running | usb | SEARCHoverIP | COM1 >> VCOM2 | COM2 >> VCOM3

NOTICE

Before starting the registration process, you must select the geographically / strategically more favorable server location for you.

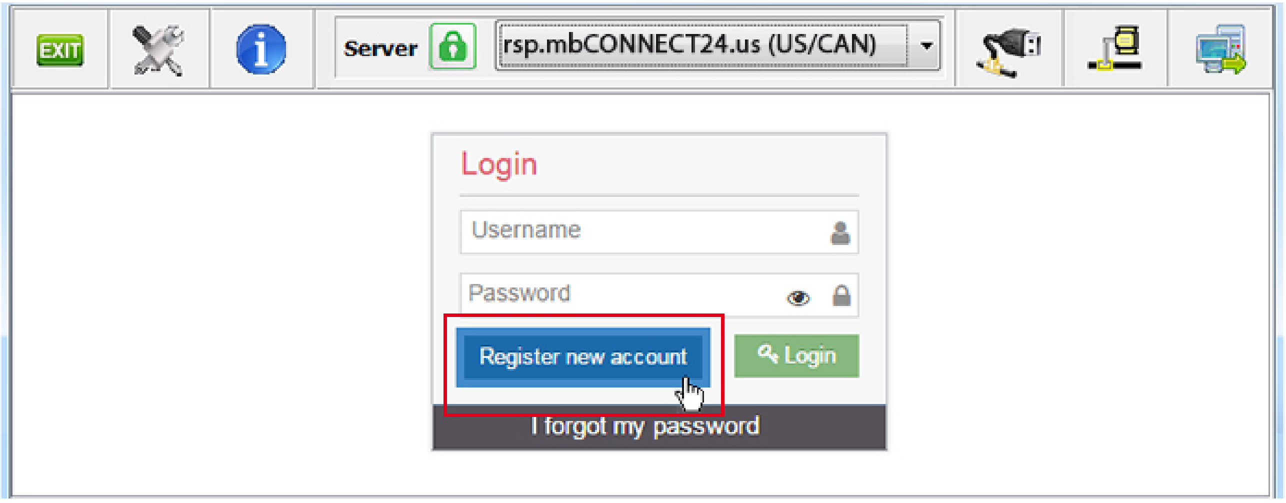


You can choose from the following server locations:

- Server location Europe: **rsp.mbCONNECT24.net (EU)**
- Server location USA / Canada: **rsp.mbCONNECT24.us (US/CAN)**
- Server location Asia: **rsp.mbCONNECT24.asia (ASIA)**
- Server location Australia: **rsp.au.mbCONNECT24.net (AU)**

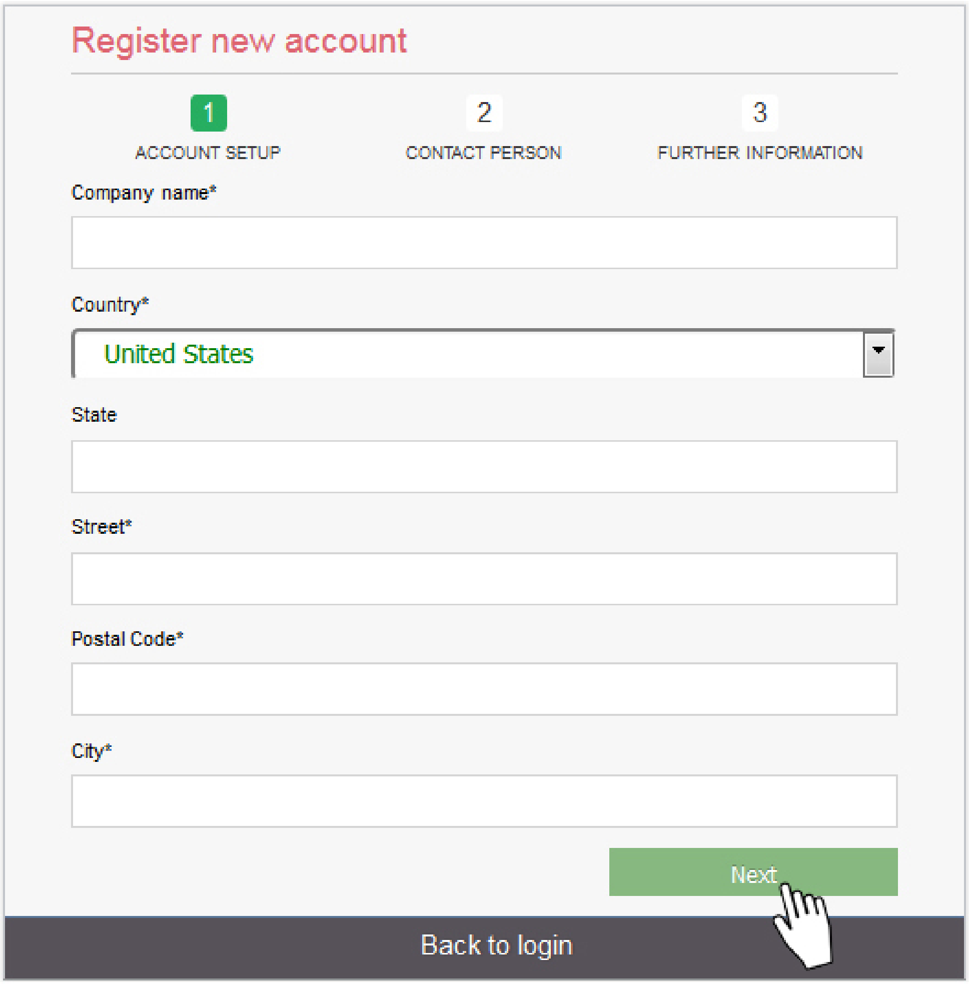
NOTICE

The selected server location can not be changed after registration!



Click the "**Register new account**" button and follow the registration wizard.

11.1.4.1 1 / 3 "Account Setup"

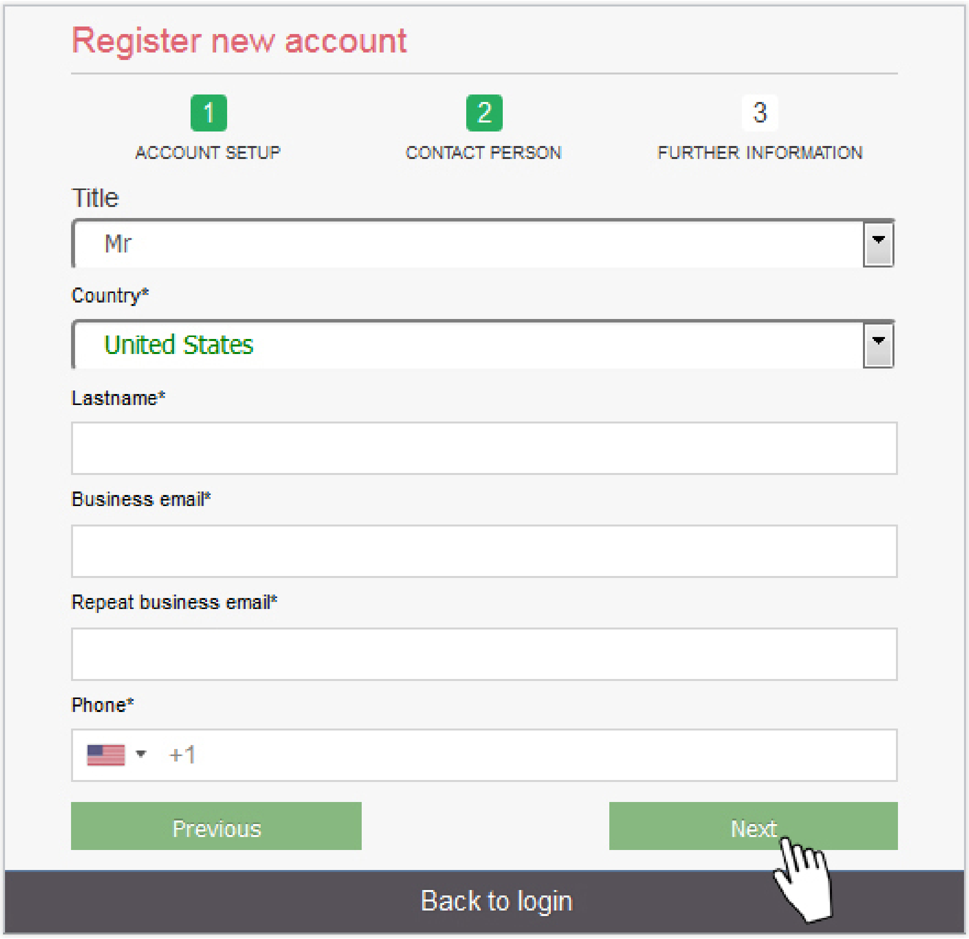


Country*: United States

Company name*	Input field for the company name.
Country*	Selection field for the company location.
State	Input field for the state.
Street*	Input field for the street.
Postal Code*	Input field for the postal code.
City*	Input field for the city.

* Required fields

11.1.4.2 2 / 3 "Contact Person"



Register new account

1 ACCOUNT SETUP

2 CONTACT PERSON

3 FURTHER INFORMATION

Title: Mr

Country*: United States

Lastname*

Business email*

Repeat business email*

Phone*: +1

Title	Selection field for the salutation.
First name*	Input field for the first name.
Last name*	Input field for the surname.
Business email*	Input field for the e-mail address.
Repeat business email*	Re-enter the e-mail address.

NOTICE

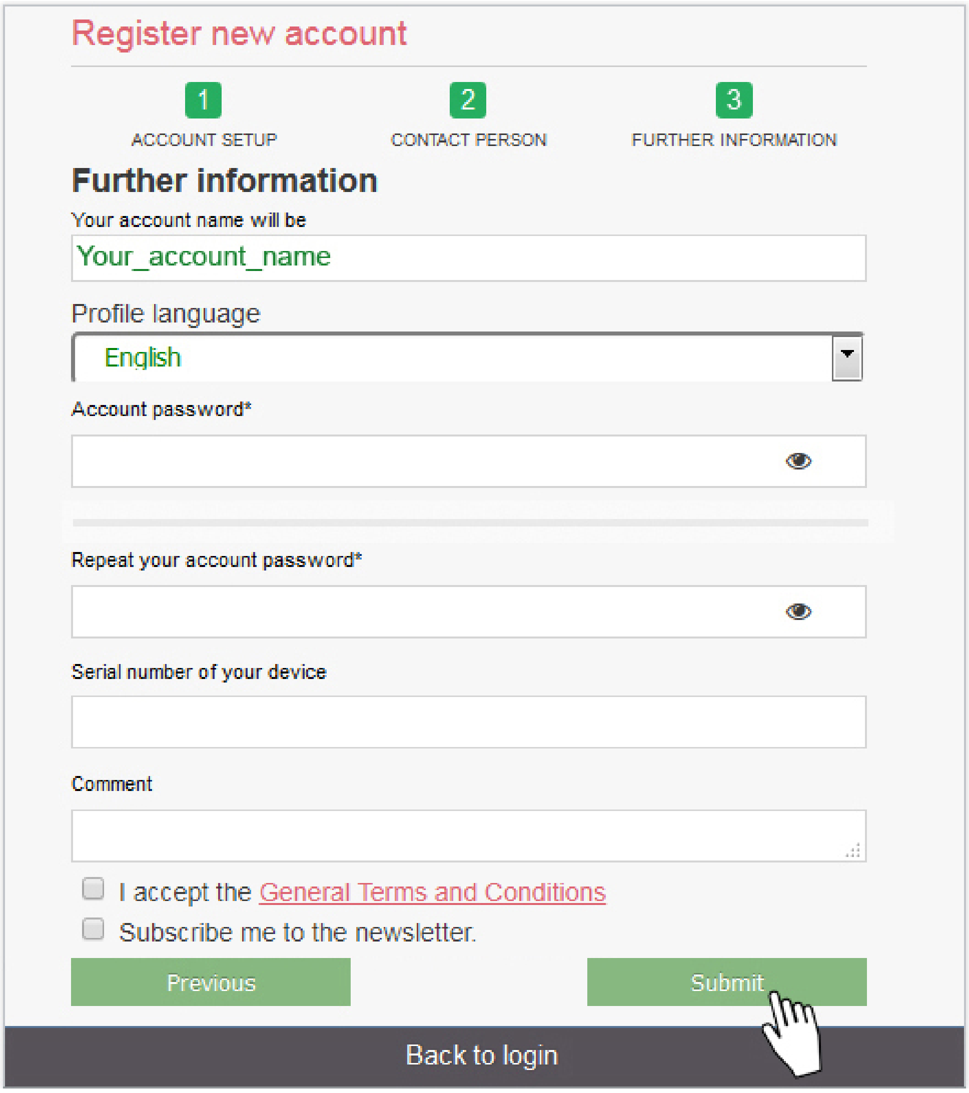
The account name is generated from the global part / domain of the e-mail address (john@doefactory.com => Your account name = doefactory).

Phone* Combine field field for

- country code selection
- entering the telephone number

* Required fields

11.1.4.3 3 / 3 "Further Information"



Register new account

1 ACCOUNT SETUP | 2 CONTACT PERSON | 3 FURTHER INFORMATION

Further information

Your account name will be: Your_account_name

Profile language: English

Account password*

Repeat your account password*

Serial number of your device

Comment

□ I accept the General Terms and Conditions

□ Subscribe me to the newsletter.

Your account name will be
Here your future account name is displayed.

Profile language
Selection field for the standard language in your account (the profile language can be changed at any time later).

Account password*
Set a password, with high password strength, for your account (see chapter "**Notes on Cyber-Security**")

Repeat your account password*
Repeat the input of the password.

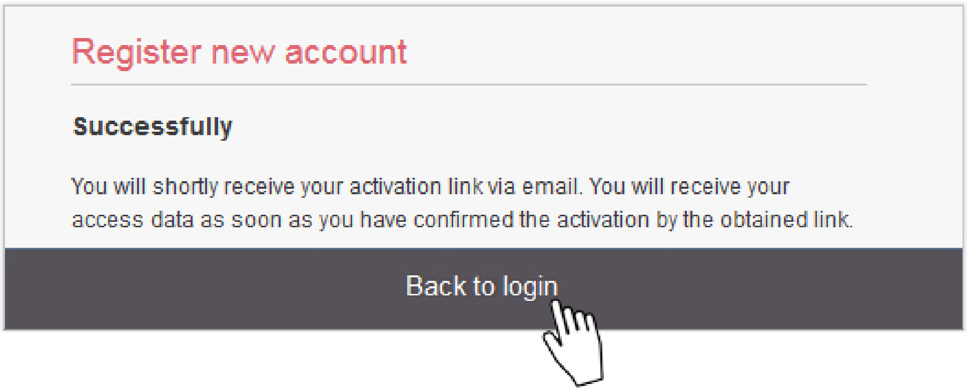
Serial number of your device
Enter the serial number of a device (mbNET, mbSPIDER ...).

Comment
Here you can post a comment of any kind, for our support department.

I accept the General Terms and Conditions
Check the checkbox to accept the terms and conditions.

Subscribe me to the newsletter.
Check this checkbox if you would like to receive our newsletter.

* Required fields



Register new account

Successfully

You will shortly receive your activation link via email. You will receive your access data as soon as you have confirmed the activation by the obtained link.

When all steps have been completed successfully, you will receive the following message:

"**Successfully**
You will shortly receive your activation link via email. You will receive your access data as soon as you have confirmed the activation by the obtained link."

Click "**Back to login**".

11.1.5 Completion of registration

Check your e-mail box and open the confirmation e-mail.

In the message you will find the summary of your entries (except your password) and a confirmation link to activate the new user account.

NOTICE

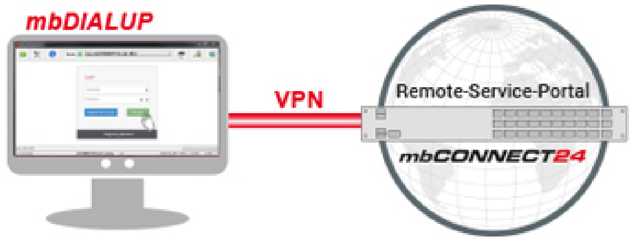
The email is sent by "MB connect line", so you can search for it quickly and easily. If it is not in your Inbox, check your other folders. If the email was moved because of a spam filter or an email rule, it could be in the Spam, Advertising, Trash, Deleted Items, or Archive folder.

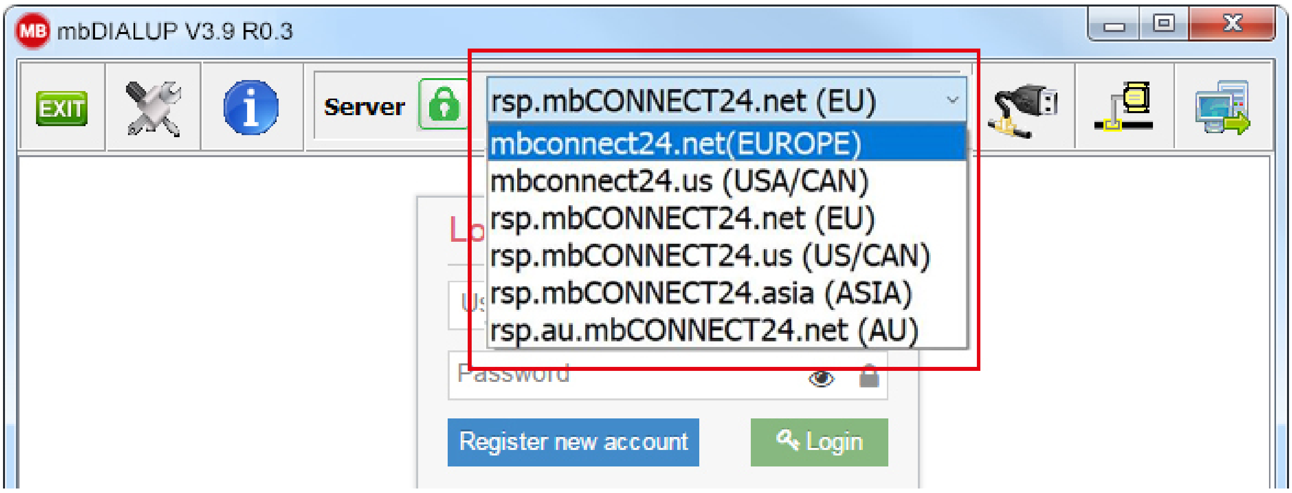
If you can not find the confirmation e-mail, contact the MB connect line support.

After successful activation of the user account, you will receive a second e-mail with your user name (for example: admin @ your_Account_name).
Along with the password that you created during registration, your access data to log on to the Remote Service Portal mbCONNECT24 are now complete.

11.2 Connect to RSP *mbCONNECT24*

Selecting the Server





- Start mbDIALUP and select from the pull-down menu "**Server**" your ***mbCONNECT24*** server.

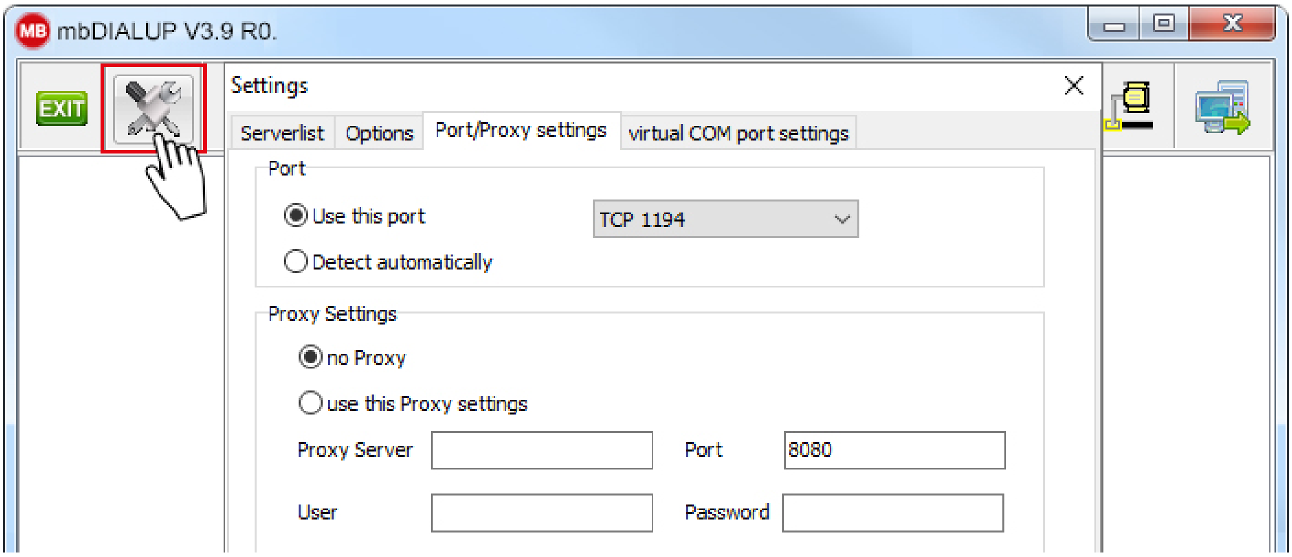
mbCONNECT24 server list	
Server name	**Note**
mbconnect24.net(EUROPE)	mbCONNECT24 **V1** - server location: Europe
mbconnect24.us(USA/CAN)	mbCONNECT24 **V1** - server location: USA / Canada
rsp.mbCONNECT24.net(EU)	RSP mbCONNECT24 **V2*** - server location: Europe
rsp.mbCONNECT24.us(US/CAN)	RSP mbCONNECT24 **V2*** - server location: USA / Canada
rsp.mbCONNECT24.asia (ASIA)	RSP mbCONNECT24 **V2*** - server location: Asia
rsp.au.mbCONNECT24.net (AU)	RSP mbCONNECT24 **V2*** - server location: Australia
User defined	**my**mbCONNECT24

* The **R**emote-**S**ervice-**P**ortal mbCONNECT24 V2 is the current version for secure remote maintenance, data acquisition, M2M communication and networking via the Internet.

NOTICE

The server location can be seen in the confirmation e-mail for subscribing to mbCONNECT24.

Access via the proxy server



mbDIALUP V3.9 R0.

Settings

Serverlist | Options | Port/Proxy settings | virtual COM port settings

Port

● Use this port: TCP 1194

○ Detect automatically

Proxy Settings

● no Proxy

○ use this Proxy settings

Proxy Server:

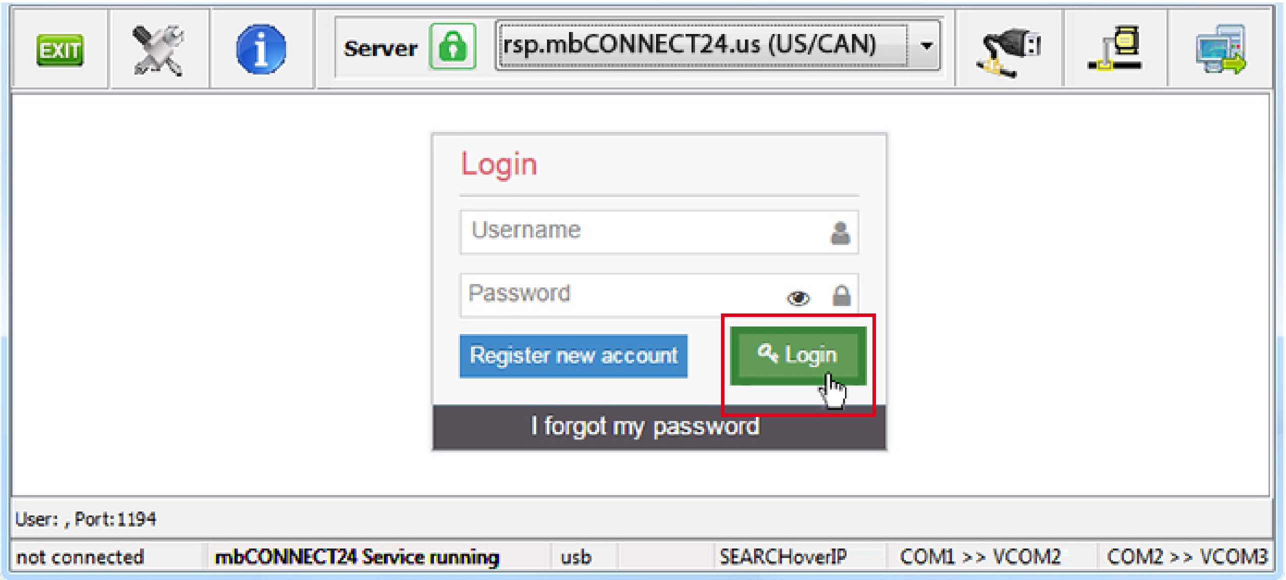
Port: 8080

User:

Password:

If the Internet can only be accessed via a proxy server, the relevant settings can be applied in the menu "**Settings**", submenu "**Port/Proxy settings**".

Login mbCONNECT24



Server: rsp.mbCONNECT24.us (US/CAN)

Login

Username

Password

Register new account | Login

I forgot my password

User: , Port: 1194

not connected | mbCONNECT24 Service running | usb | SEARCHoverIP | COM1 >> VCOM2 | COM2 >> VCOM3

Log in to the portal with your user data (Username + Password).

NOTICE

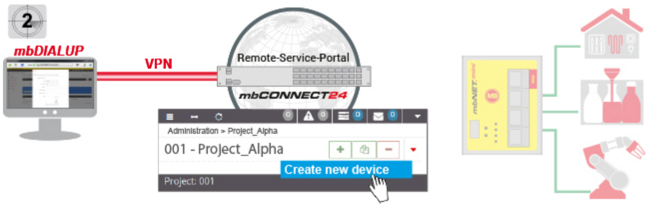
Your user name has been sent to you by e-mail when registering your mbCONNECT24 user account for. The user name is a combination of "admin@" and your account name. Your password you assigned when registering. Do not forget to change your password at regular intervals.

A secure VPN connection to your account on ***mbCONNECT24*** is now established.

11.3 *mbCONNECT24* Configuration

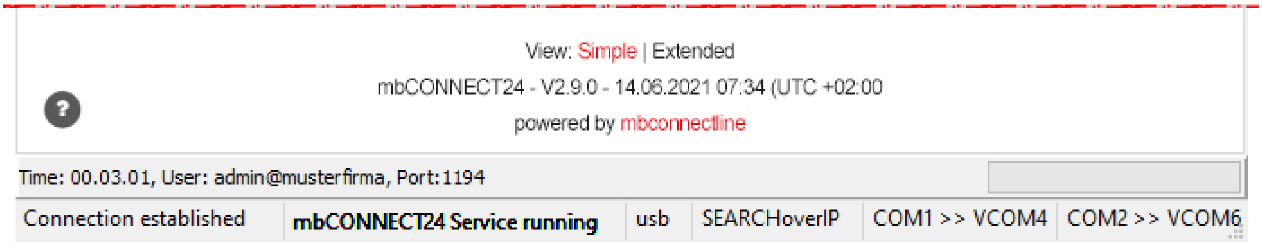
Here you do

- change your password
- create a new project
- create a new device
- generate a configuration file and
- transfer it to your ***mbNET.mini***



NOTICE

The following description refers to the mbCONNECT24 view mode **Extended**.



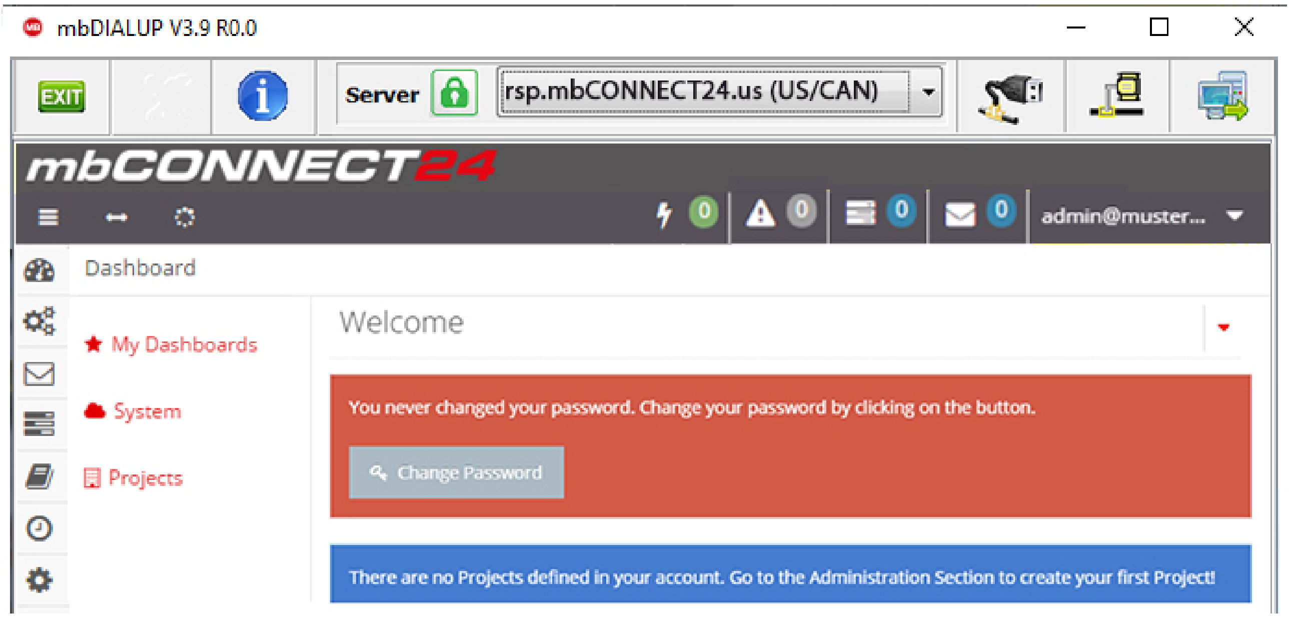
View: Simple | Extended
mbCONNECT24 - V2.9.0 - 14.06.2021 07:34 (UTC +02:00
powered by mbconnectline

Time: 00.03.01, User: admin@musterfirma, Port:1194

Connection established | mbCONNECT24 Service running | usb | SEARCHoverIP | COM1 >> VCOM4 | COM2 >> VCOM6

You can switch between the two view modes at any time. To do this, click in the footer for "View" on **Simple** or **Advanced**.

11.3.1 Changing your password

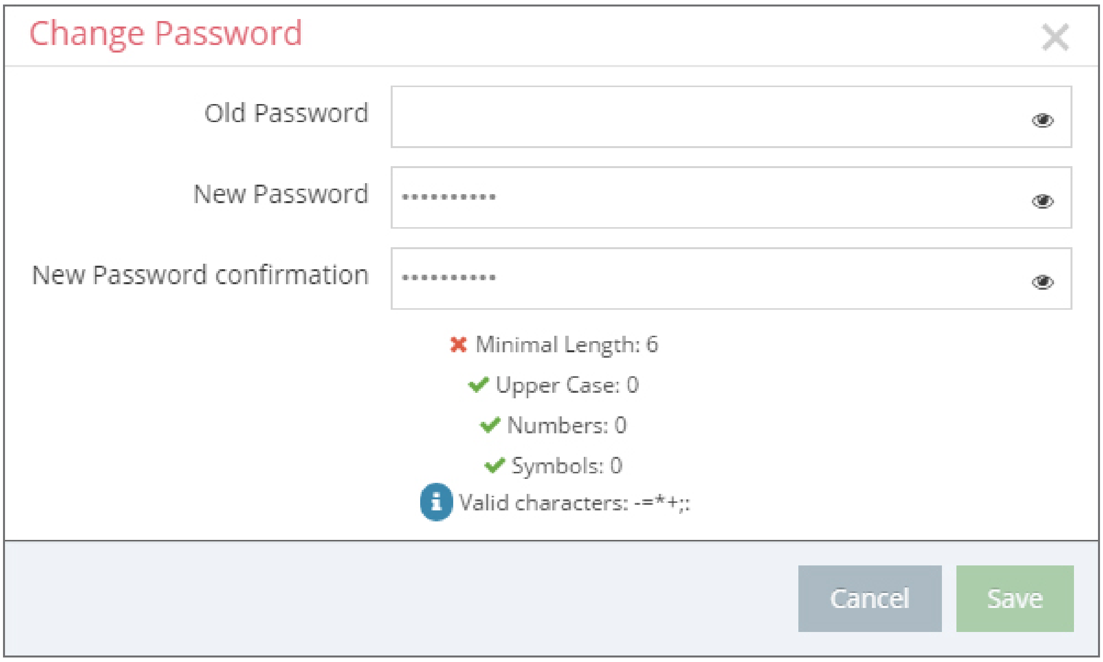


You never changed your password. Change your password by clicking on the button.

There are no Projects defined in your account. Go to the Administration Section to create your first Project!

After your first Login at the portal, you are required to change your password.
This is a safety-related matter and should definitely be completed.
As long as you do not change your password, this prompt is displayed each time the start page is accessed.

Click on "Change Password".



Change Password

Old Password

New Password ••••••••••

New Password confirmation ••••••••••

✗ Minimal Length: 6

✓ Upper Case: 0

✓ Numbers: 0

✓ Symbols: 0

ℹ Valid characters: -=*+;:

Notice that your password has to fit the password guideline.

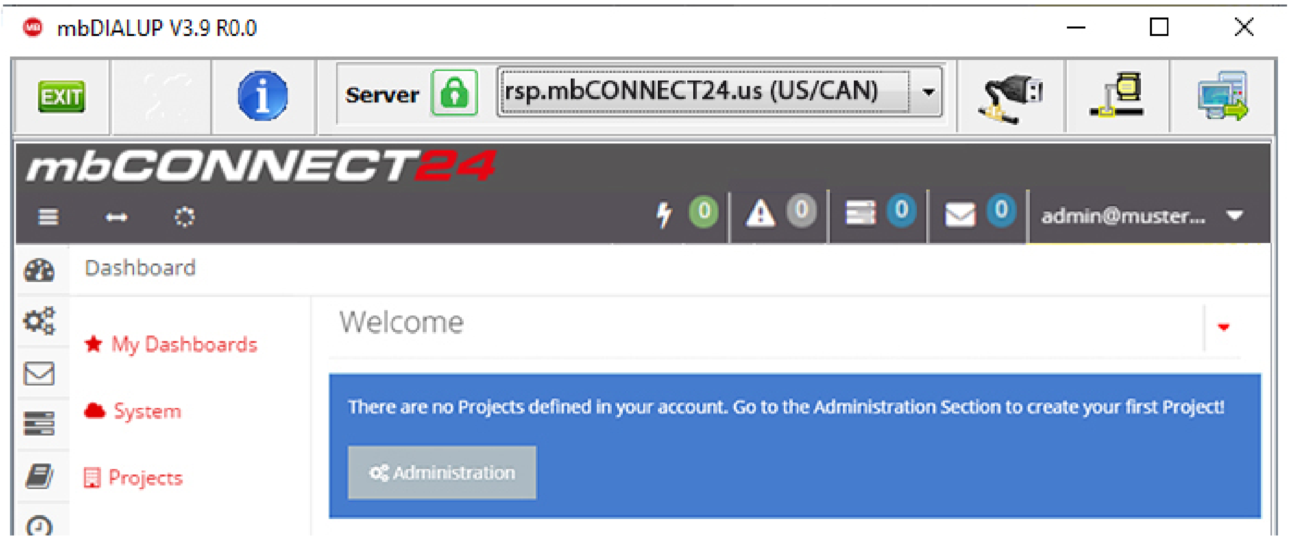
Your password is active, when you reconnect to the portal.

11.3.2 Creating a project

A project is the highest entity to implement the following tasks:

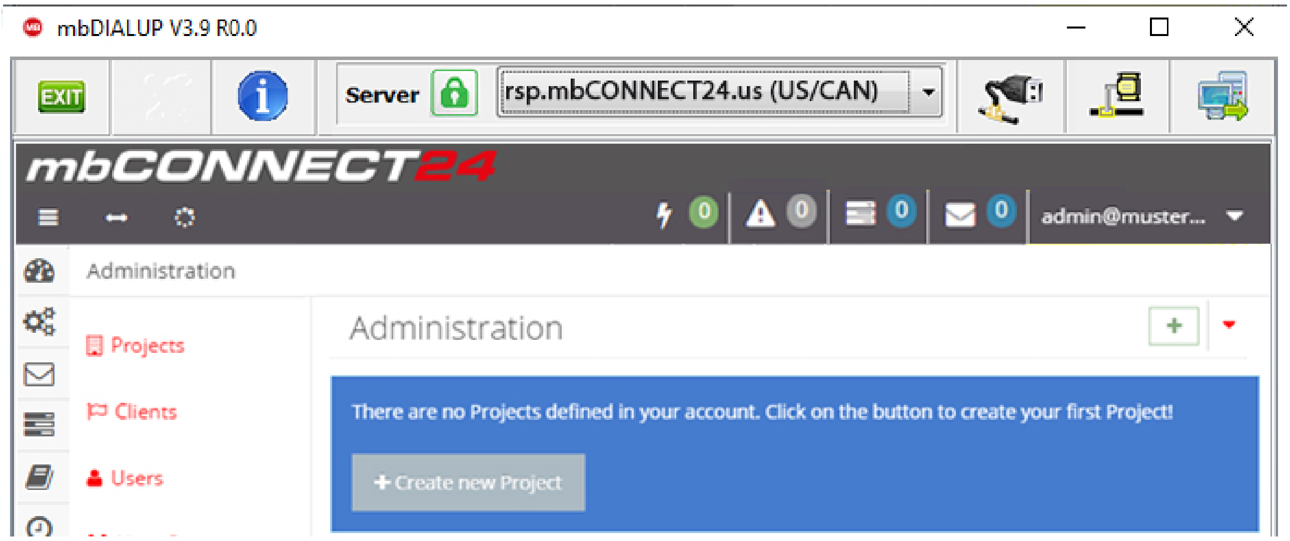
- remote maintenance
- monitoring and alarming
- data-logging
- visualization

A device (router) is assigned to a project, directly. It is possible to assign several devices to one project.



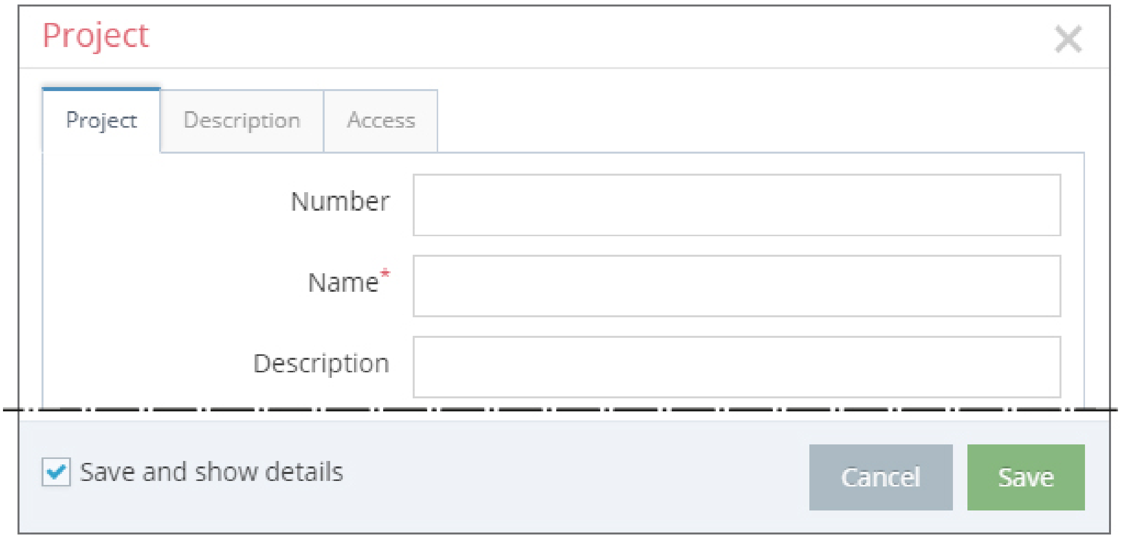
There are no Projects defined in your account. Go to the Administration Section to create your first Project!

Click the "**Administration**" button under the Note:
"There are no projects defined in your account. Go to the Administration Section to create your first project!"



There are no Projects defined in your account. Click on the button to create your first Project!

On the next window, click "**+ Create new Project**".



Project

Project | Description | Access

Number:

Name*:

Description:

☑ Save and show details

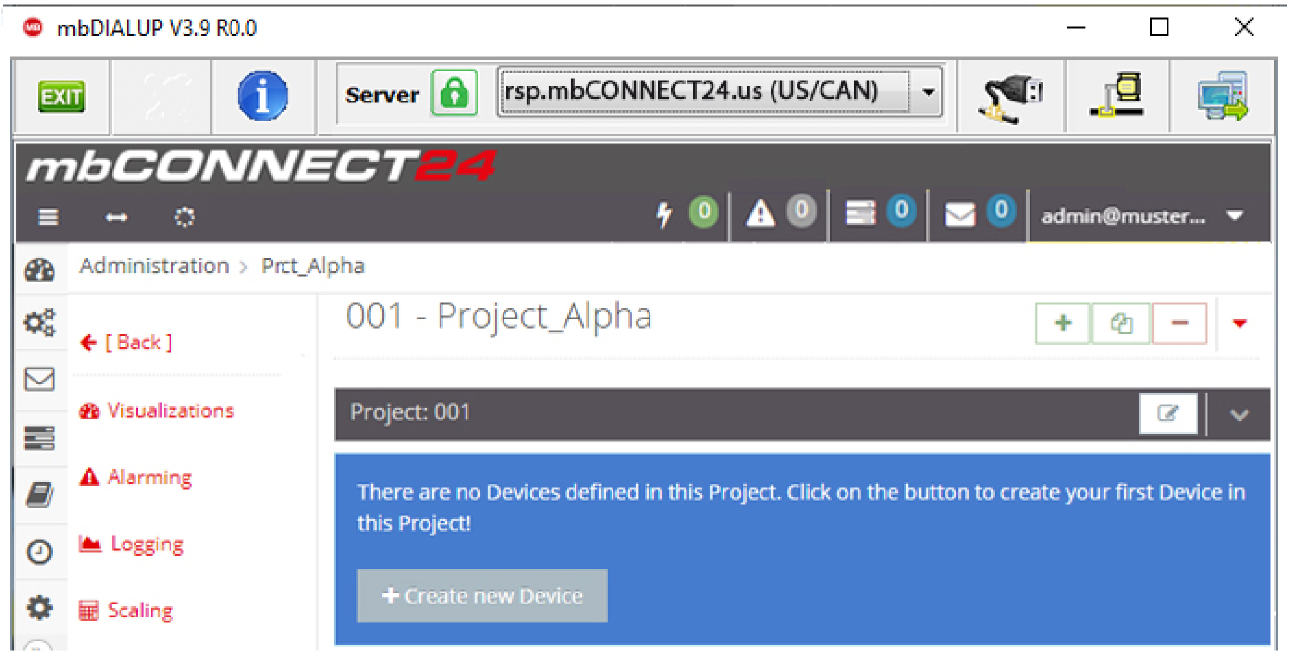
For the basic configuration, it is necessary to fill in the following information:

- Number
- Name*
- Description

The tabs „Description“ and „Access“ are necessary for the extended configuration.

Term	Description
Number*	**Optional field** - Input value = alphanumeric
Name	**Mandatory field** - Input value = alphanumeric
Description	**Optional field** - Input value = alphanumeric. The short description entered is displayed in the project overview.
Cancel	By clicking on Cancel, the process is terminated. All entries / settings also in the other tabs (Description, Access), will be lost.
Safe	By clicking on Save, the process is finished. All entries / settings also in the other tabs (Description, Access) are stored.

11.3.3 Create a new device

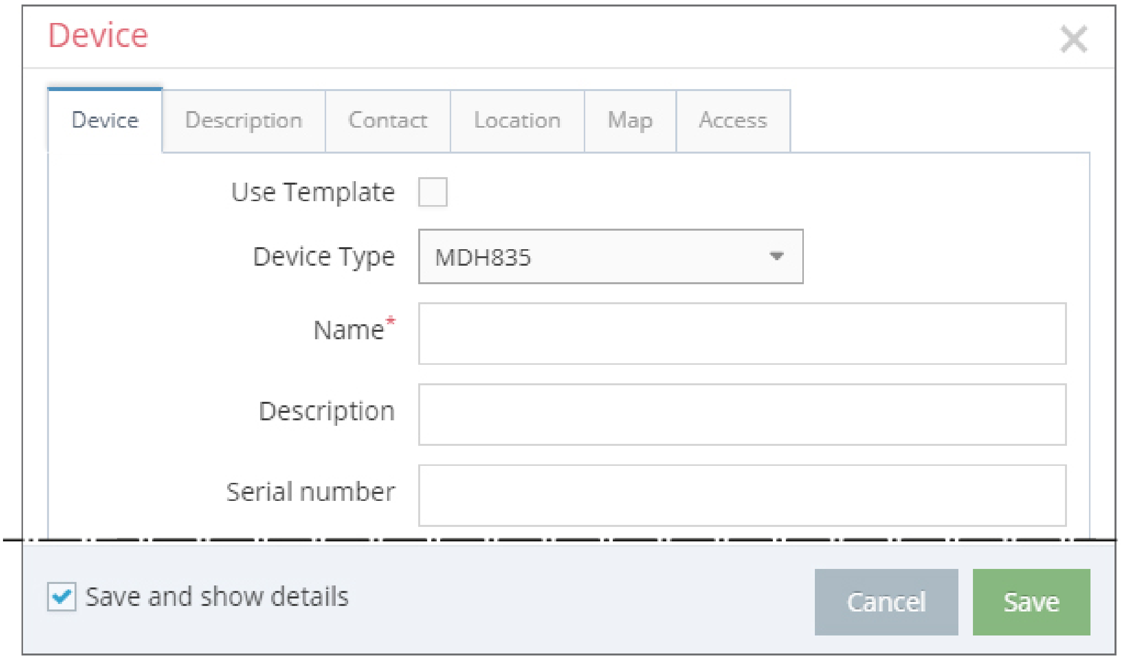


001 - Project_Alpha

There are no Devices defined in this Project. Click on the button to create your first Device in this Project!

After you have defined a Project, it appears following announcement: :
"*There are no Devices defined in this Project. Click on the button to create your first Device in this Project!*"

Click on the button „**+ Create new Device**“.



Use Template □

Device Type: MDH835

Name*

Description

Serial number

☑ Save and show details

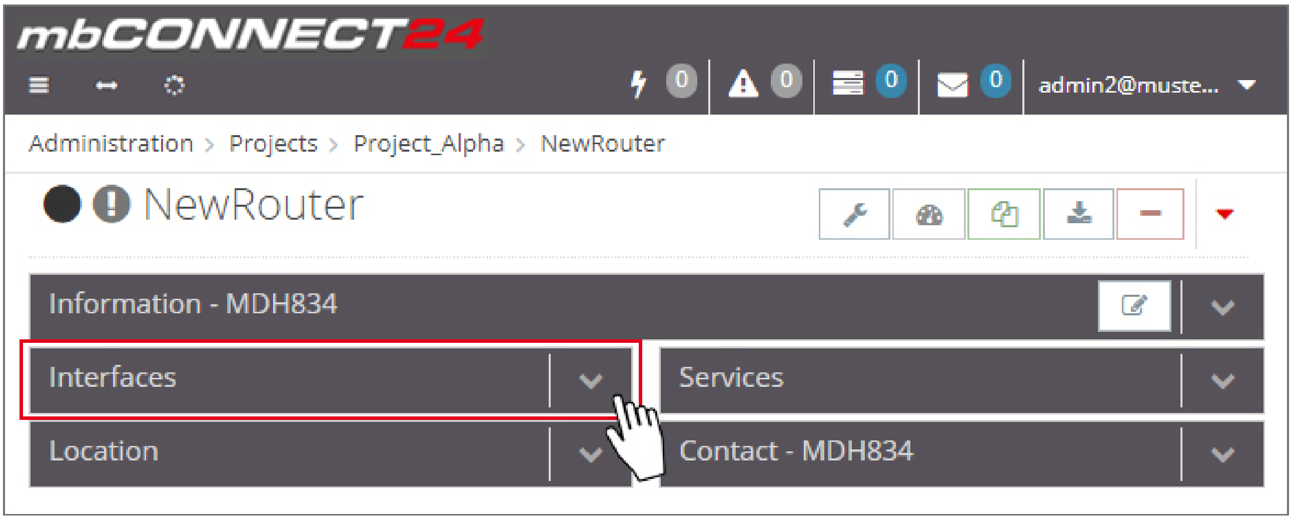
For the basic configuration, you only need the following data in the tab “Device”.

- Device Type
- Name*
- Description
- Serial number

The tabs „Description“, „Contact“, „Location“, „Map“ and „Access“ are necessary for the extended configuration.

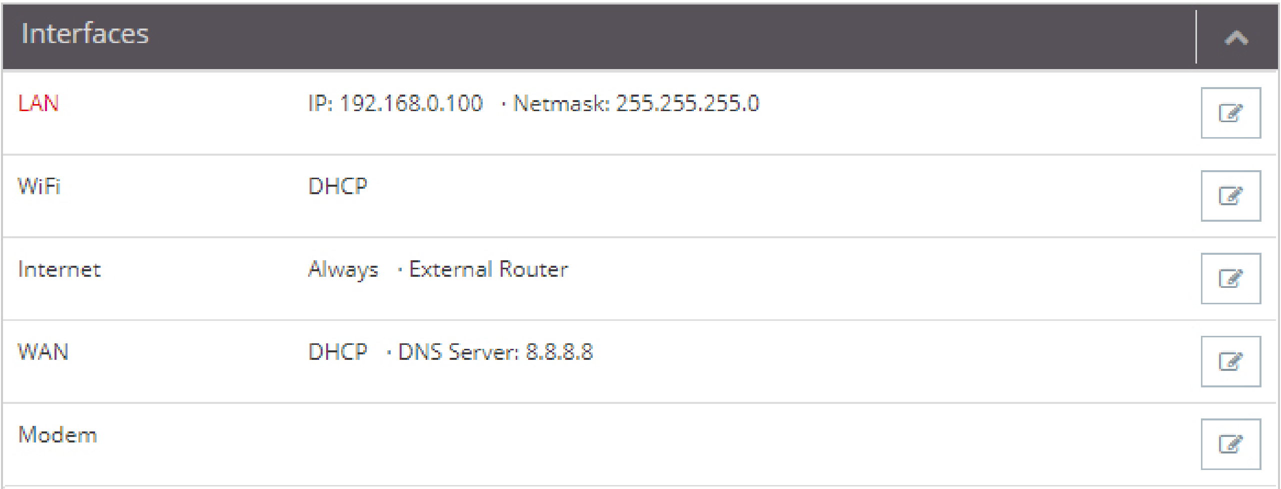
Type	**Selection field** with all device types you can create in the portal. The device type (eg Typ: MDH 834) can be found on the device nameplate, side of the unit.
Name*	**Mandatory field** to enter a unique device name. You can create your own name for your Device. Following numbers and letters are allowed: **0** to **9**, **A** to **Z**, **a** to **z** (avoid blanks).
Description	**Optional field** to enter a brief description for the device. The description can be freely selected and will be displayed later in the device overview. All numbers, words, blank spaces or additional characters are allowed.
Serial number	a) **Optional field**: If you transfer the configuration to the device ("Download to PC" or "Submit to device"), you can leave this field empty. Once the device connects for the first time with the portal, the serial number is entered automatically. b) **Mandatory field**: If the device at the first connection to the portal get its configuration ("Prepare for Synchronization"), you must enter the serial number of the device here. The serial number (eg S/N: 211383405693) can be found on the device nameplate, side of the unit.

11.3.4 Create a configuration



After you have created a Device, the actual configuration menu appears.

For the initial configuration (minimum configuration), only the "Interfaces" widget with the following submenus is relevant.



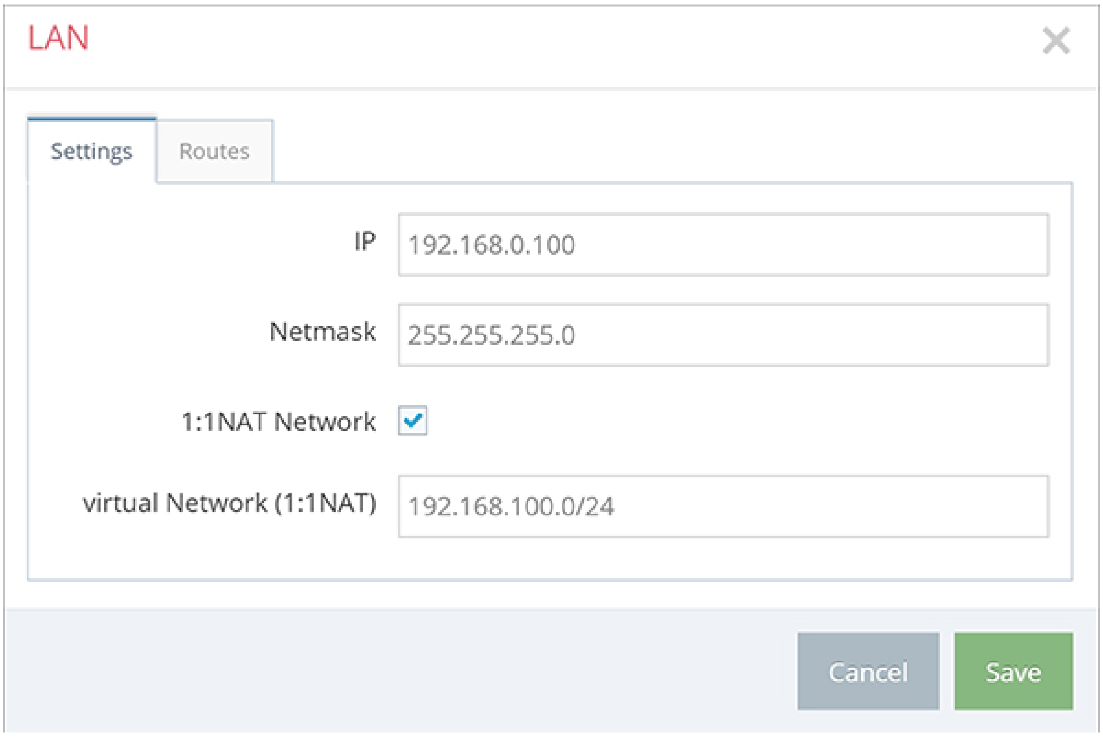
Interfaces

LAN	IP: 192.168.0.100 · Netmask: 255.255.255.0
WiFi	DHCP
Internet	Always · External Router
WAN	DHCP · DNS Server: 8.8.8.8
Modem	

Image 3: Depending on the device type selected, the display may vary here.

Click the edit icon ✎ to make the settings on the submenus.

11.3.4.1 LAN Settings



IP: 192.168.0.100

Netmask: 255.255.255.0

1:1NAT Network: ☑

virtual Network (1:1NAT): 192.168.100.0/24

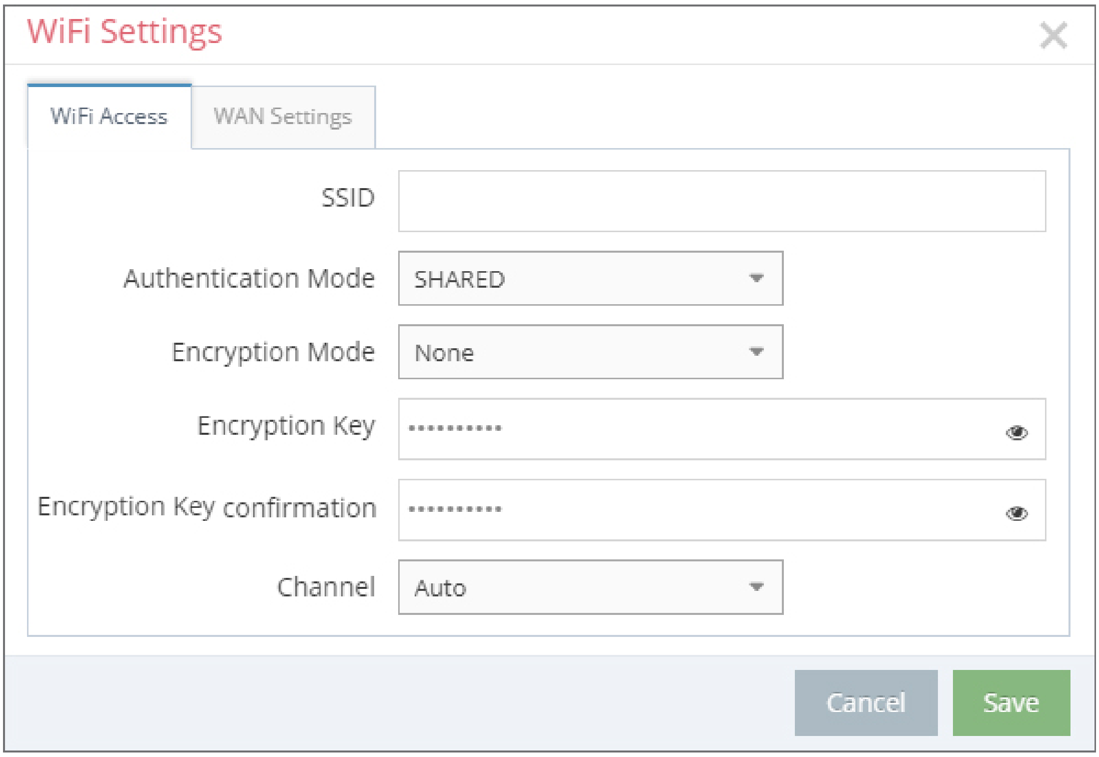
Enter a free LAN IP address and the Netmask from your system or machine network.

NOTICE

Notice, that the LAN and WAN IP-address should use a different address range.

LAN Settings	
IP	Enter the IP-address of your Device
Netmask	Enter the Subnet mask where your Device should be integrated.
1:1NAT Network	Activate „1:1NAT Network“, if both contacts use the same Net address and want to communicate with each other.
virtual Network (1:1NAT)	Enter your address of your network (e.g. 192.168.100.0/24). Make sure you use the CIDR spelling for the IP-address!
SEARCHoverIP	Checkbox for activating / deactivating the function SEARCHoverIP.

11.3.4.2 Wi-Fi Settings



SSID

Authentication Mode: SHARED

Encryption Mode: None

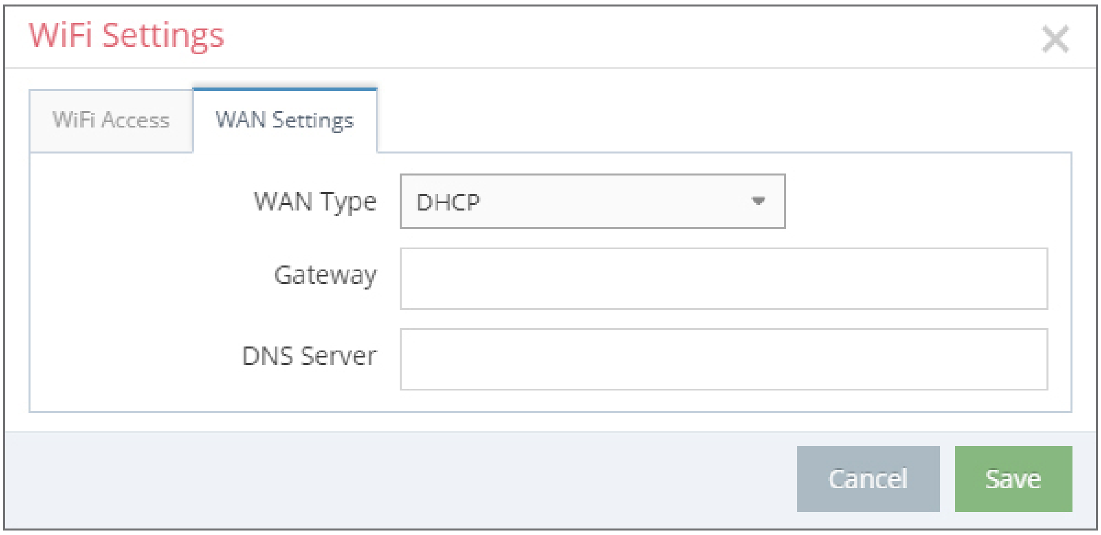
Encryption Key: ••••••••••

Encryption Key confirmation: ••••••••••

Channel: Auto

If you want to configure a device with a Wi-Fi module, enter the information of your Router or Access-point.

Wi-Fi Access	
SSID	**Mandatory field:** Enter the name of the Wi-Fi network to which the device should connect.
Authentication Mode	**Selection field** for the authentication mode.
Encryption Mode	**Selection field** for the encryption mode.
Encryption Key	**Mandatory field:** Enter the encryption key.
Encryption Key confirmation	**Mandatory field:** Enter the encryption key again.
Channel	**Selection field** for the Wi-Fi channel.

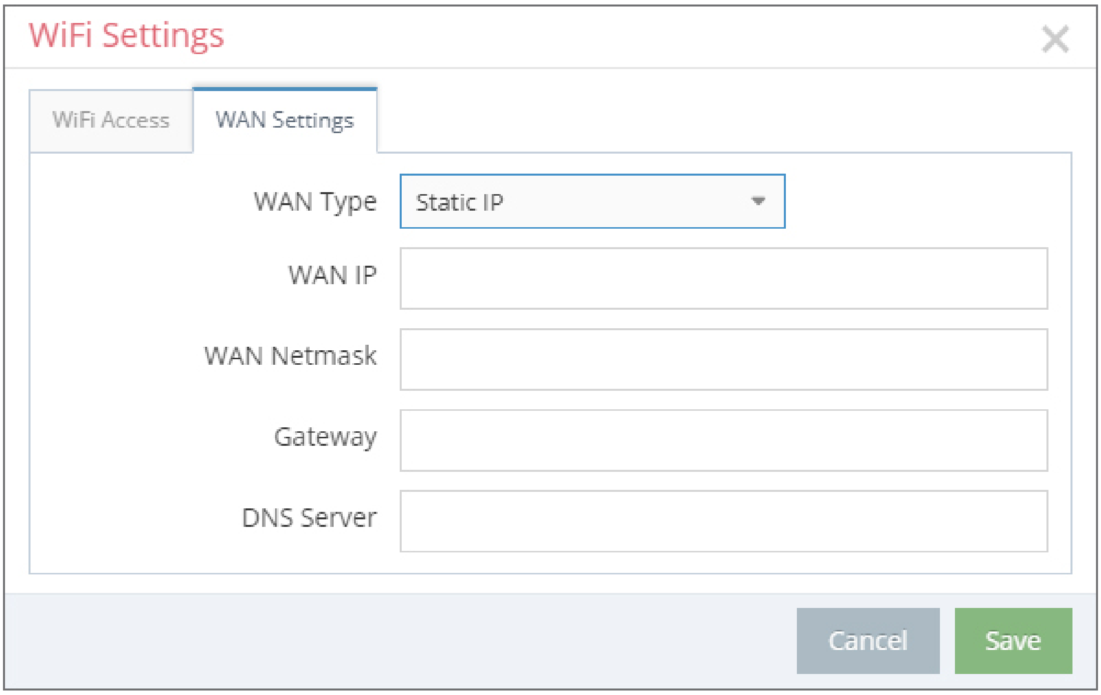


WAN Type: DHCP

Gateway

DNS Server

WAN settings – Type: DHCP	
Select this setting if a DHCP server exists in the network and the device is thus assigned an IP address automatically (contact your network administrator about this!).	
Gateway	Enter details of the Gateway that connects you to the Internet, e.g. the IP address of the existing device.
DNS Server	Here, select the DNS server assigned to you by your Internet service provider or enter your own DNS server. You can enter up to five DNS servers here. The individual addresses must be separated by a space (z. B. "8.8.8.8 8.8.4.4").



WiFi Settings

WAN Type: Static IP

WAN IP

WAN Netmask

Gateway

DNS Server

WAN settings – Type: Static IP	
Select this setting if connection to the Internet is via an existing device that is not acting as a DHCP server, or if no server is set up to assign addresses. You should also select this setting if you have received a static address from your ISP, e.g. if you have a leased line. Note also that this type of connection requires you to enter a DNS server.	
IP	Here, enter the IP address of the device connected to the WAN port.
Netmask	Enter the subnet mask of the appropriate network, into which the device is to be integrated.
Gateway	Enter details of the gateway that connects you to the Internet, e.g. the IP address of the existing device.
DNS Server	Here, select the DNS server assigned to you by your Internet service provider or enter your own DNS server. You can enter up to five DNS servers here. The individual addresses must be separated by a space (z. B. "8.8.8.8 8.8.4.4").

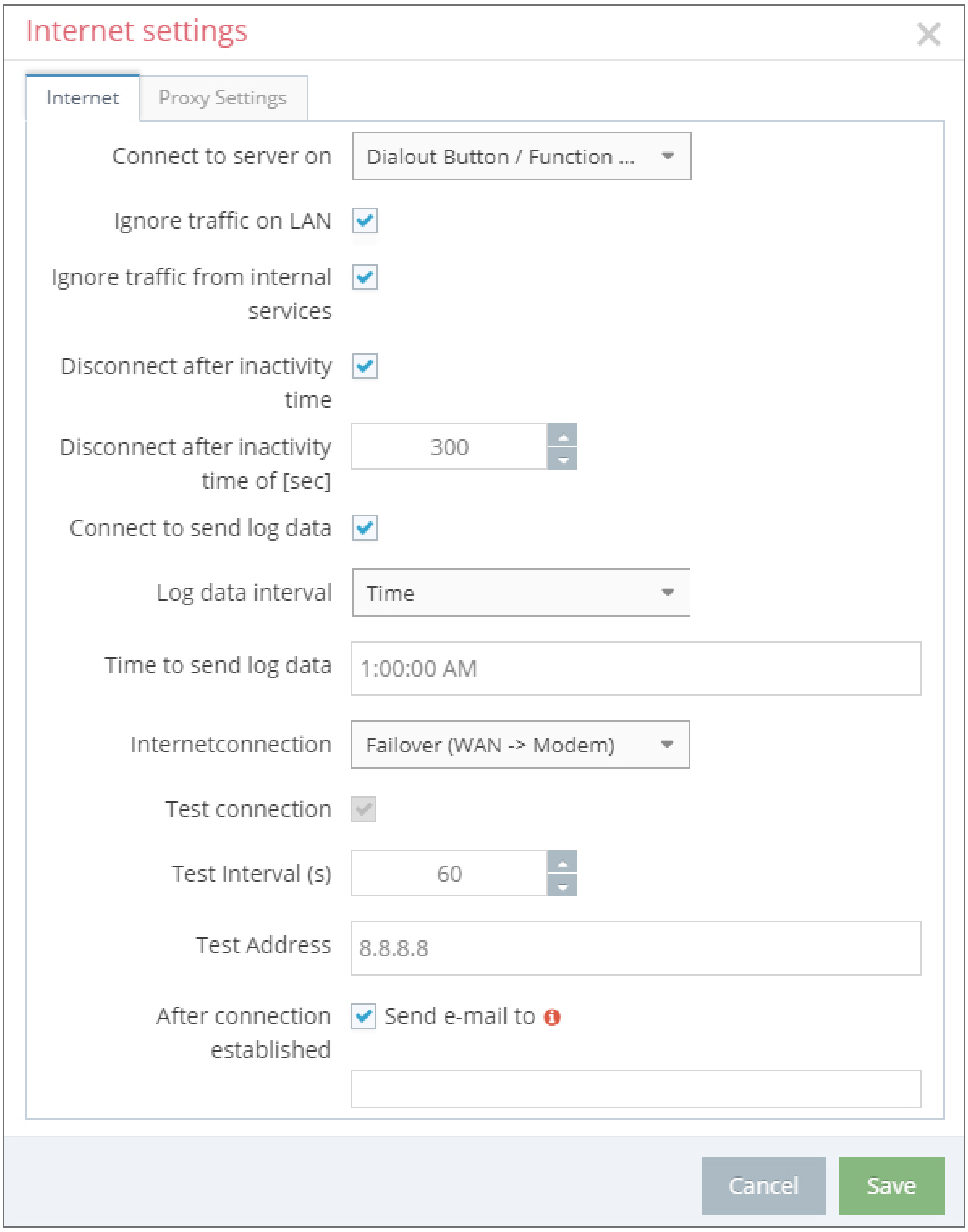
11.3.4.3 Internet Settings

NOTICE

The individual input / selection fields and checkboxes can vary, depending on the device, type and selected settings.

NOTICE

For the First Configuration it is advisable to select „**Always**“ in the Tab „**Connect to Server on**“. Only in this setting, the device automatically tries to establish a connection to the portal.



Internet settings

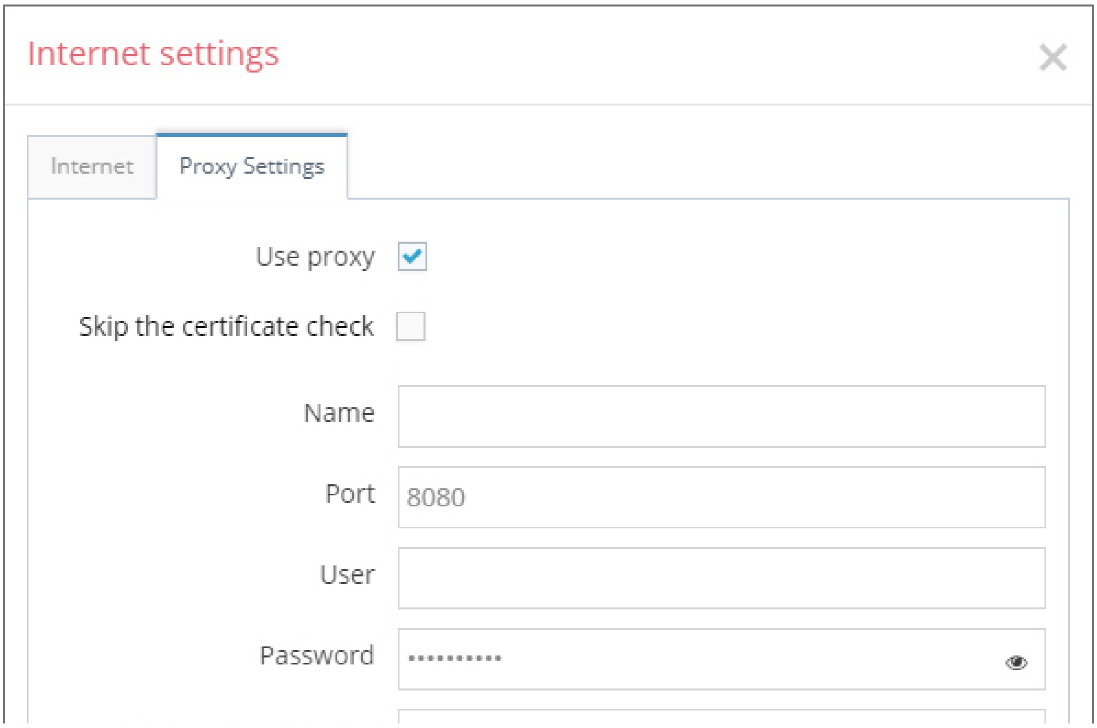
Connect to server on	Dialout Button / Function ... ▾
Ignore traffic on LAN	☑
Ignore traffic from internal services	☑
Disconnect after inactivity time	☑
Disconnect after inactivity time of [sec]	300
Connect to send log data	☑
Log data interval	Time ▾
Time to send log data	1:00:00 AM
Internetconnection	Failover (WAN -> Modem) ▾
Test connection	☑
Test Interval (s)	60
Test Address	8.8.8.8
After connection established	☑ Send e-mail to ℹ

Internet	
Connect to Server on	Selection field for when and under which conditions the device should connect to the server. **Dialout/Function Button** Pressing the "Dialout" or "Function" button on the appropriate device establishes a connection to the server. **Always** A connection is established as soon as the device is switched on and ready for operation. **SMS** The command to establish a connection is sent to the device via a text message. **Start when Input 1 is active (1 signal)** Depending on the device and type, the connection can be controlled using one or more digital inputs. **Start when Input 1 is active (1 signal), stop on 0 signal** Depending on the device and type, the connection can be controlled using one or more digital inputs.
Ignore traffic on LAN	If this check box is activated, no connection that differs from the setting under "**Connect to server on**" can be established. For example, a component connected to the LAN uses the device (router) as a gateway.
Ignore traffic from internal services	If this check box is activated, no connection that differs from the setting under "**Connect to server on**" can be established. For example, if an e-mail is to be sent by the device (router) or an automatic time synchronization is to be executed.
Disconnect after inactivity time of [sec]	When the preset time has elapsed (timeout), the connection between the server and device is disconnected.
Connect to send Log Data	The device connects to the server to send log data, irrespective of the selection of when and under which conditions the device is to establish a connection (with the exception of the selection "Always"). The connection is disconnected after the preset timeout.
Log Data Interval	Selection field for the interval (1 hr., 2 hrs., 4 hrs., 8 hrs., 12 hrs., 24 hrs.) of the data logged during this period of time.
Time to Send Log Data	Initial time, from which the log data is sent in the preset interval.

	Internet	
Internet Connection	Selection field with the available options (depending on the device and device type) for how the connection to the Internet should be established.	
	External Route	To connect the device via an external router, you must assign the device an IP address from the area of the external router. Enter the external router under "Standard Gateway". In addition, you must specify the address of the DNS server to ensure name clarification.
	External DSM Modem	You require login data for a connection to the Internet via a DSL modem. You will have received this data from your Internet service provider (ISP). Enter the login data in the fields Username and Password.
	Wi-Fi	Depending on the device and device type, the connection is made to the Internet via an Access Point.
	Failover (WAN -> Wi-Fi)	Depending on the device and device type, the connection takes place primarily via the WAN interface. If the connection can not be established or is interrupted, the device switches to connect using an Access Point (Wi-Fi).
	Modem	Depending on the device and device type, the connection to the Internet may be established via the internal modem.
	Failover (WAN -> Modem)	Depending on the device and device type, the connection is primarily established via the WAN interface. Should the connection not be established or be interrupted, then the device will switch to the connection via the internal modem.
Test Connection	If this checkbox is ticked, then the entered test address will be pinged at the specified test interval. Ensure that the entered test address is permanently available.	
Test Interval (s)	Interval, in which the entered test address is pinged.	
Test Address	Test address pinged at the specified test interval. Ensure that the entered test address is permanently available.	
After connection established – Send e-mail to	If this checkbox is ticked, then you will receive an e-mail message when a connection to the Internet has been established. For this, enter a valid e-mail address.	

"SSL termination
An HTTPS connection can be broken down (scheduled) by means of a web proxy in order to also check its contents for pests. Further encryption to the client (browser) then takes place with a certificate offered by the proxy. The problem with this is that the user of the browser no longer gets to see the original certificate of the web server and has to trust the proxy server that he has taken a validation of the web server certificate."[1]
One way to avoid this problem is to enable this feature.

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



Internet settings

Use proxy ☑

Skip the certificate check □

Name

Port 8080

User

Password ••••••••••

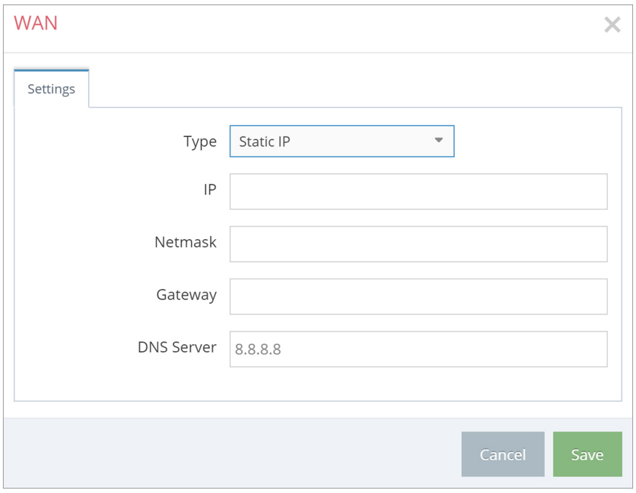
If you wish to use an HTTP proxy for your connections, then set the checkbox for "Use Proxy". Then, additional fields for entering the IP address, DNS name, port and authentication data are displayed. If your HTTP proxy does not require authentication, then you can leave the fields for the user data of the proxy server empty.

Proxy Settings	
Use Proxy	Checkbox to activate / deactivate the function.
Skip the certificate check	Check box for enabling/disabling this function. *"**SSL termination*** *An HTTPS connection can be broken down (scheduled) by means of a web proxy in order to also check its contents for pests. Further encryption to the client (browser) then takes place with a certificate offered by the proxy. The problem with this is that the user of the browser no longer gets to see the original certificate of the web server and has to trust the proxy server that he has taken a validation of the web server certificate."*[2] One way to avoid this problem is to enable this feature.
Name	Input field for the Host name or the IP address of the proxy server.
Port	Input field for the port (Port 8080 is preset).
User	Input field for the User. If necessary, the domain name (Domain\Username) as well as the authentication method (for NTLM: Username#AUTH-NTLM or NTLMv2: Username#AUTH-NTLM2) are entered.
Password	Input field for the server password.
Password Confirmation	Input field for repeating the password.

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

11.3.4.4 WAN Settings

Enter a free WAN IP address and the net mask from your system or machine network. It is not compelling to make an entry, just if you have plugged in the WAN-connector. If you have a Device with a modem module, you do not need the WAN IP-address.



WAN

Settings

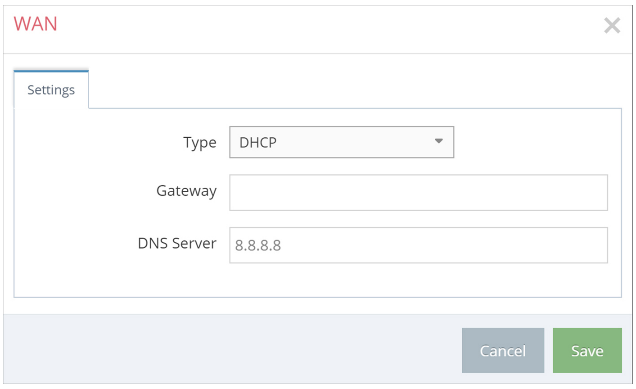
Type: Static IP

IP:

Netmask:

Gateway:

DNS Server: 8.8.8.8



WAN

Settings

Type: DHCP

Gateway:

DNS Server: 8.8.8.8

You can select between static IP and DHCP.

Type: **Static IP**

Use the static IP-address if you do not have a DHCP-Server in your Network. Notice that you have to use a DNS-Server.

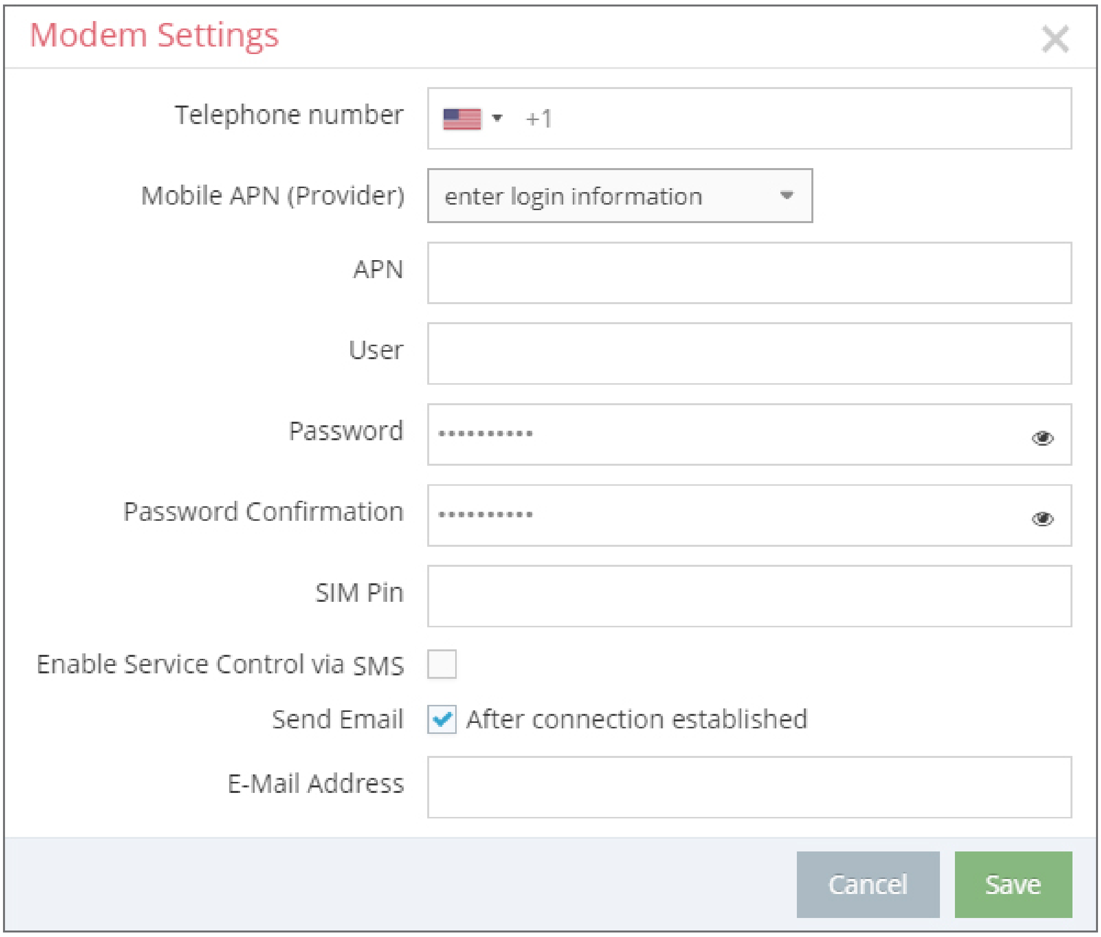
IP	Enter the IP-Address of the external Router.
Netmask	Enter the subnet mask of the corresponding network, in which the device is to be integrated.
Gateway	Enter the respective gateway that connects you to the Internet, so the IP address of the existing device.
DNS Server	Select the DNS server that was assigned to you by your Internet service provider (ISP), or enter your own DNS server.

Type: **DHCP**

Select this, if a DHCP server exists in the network and is assigned to the device automatically get an IP address (contact in this regard also to your network administrator!).

Gateway	Enter the respective gateway that connects you to the Internet, so the IP address of the existing device.
DNS Server	Select the DNS server that was assigned to you by your Internet service provider (ISP), or enter your own DNS server.

11.3.4.5 Modem Settings



Modem Settings

Telephone number: +1

Mobile APN (Provider): enter login information

APN

User

Password: ••••••••••

Password Confirmation: ••••••••••

SIM Pin

Enable Service Control via SMS □

Send Email ☑ After connection established

E-Mail Address

Modem Settings	
Telephone number	Enter the mobile number of your device.
Mobile APN (Provider)	Select the APN of your Provider, if it is in the list.
APN	Enter the APN of your provider manually.
User	If necessary, enter your Username.
Password	If necessary, enter your Password.
Password Confirmation	Confirm the password.
SIM Pin	If necessary, enter your SIM-Pin.
Enable Service Control via SMS	If this checkbox is hooked, you can send an SMS to the device for eg restart, input query etc.
Send Email After connection established	Activate the checkbox and enter a valid e-mail address if you want to be notified after a connection is established.
E-Mail Address	Enter the email address.

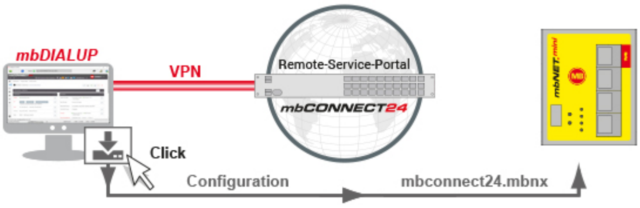
11.4 Transferring the configuration to the Device

The following options are available for transfer of the configuration file (**mbconnect24.mbn / -.mbnx**):

a) **Download to PC**

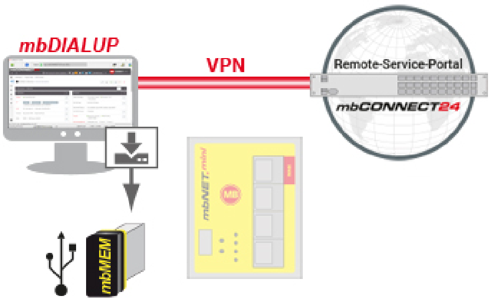
b) **Prepare for Synchronization**

c) **Submit to Device**



a. Download to PC

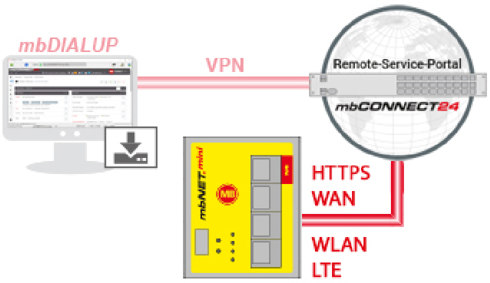
Here you download the configuration to your PC or directly to a USB stick. The configuration is then transferred to the device via the USB stick.



Prerequisite / conditions:
- The configuration PC has a **VPN connection** to the portal
- The **Device** has **no LAN connection**
- The **Device** has **no connection** to the portal

b. Prepare for Synchronization

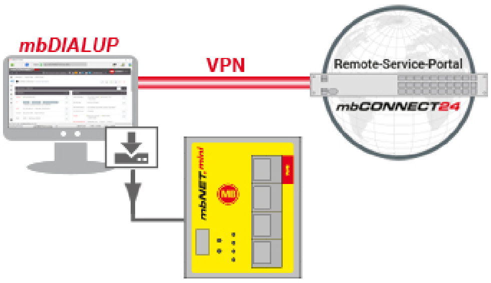
You deposit the configuration in the portal for collection by the device. As soon as the device connects to the portal, the configuration is automatically transferred to the device.



Prerequisite / conditions:
- The **Device** has **a connection** to the portal
- a **valid server address** is entered in the device

c. Submit to Device

Here you transfer the configuration via mbDIALUP directly to the device.

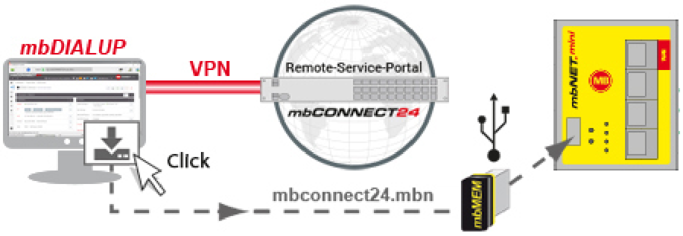


Prerequisite / conditions:
- The configuration PC has **a VPN connection** to the portal
- The device has been pre-configured with the connection data (Firststart using the device web GUI)
- The device is **connected** to the PC **via LAN**

NOTICE

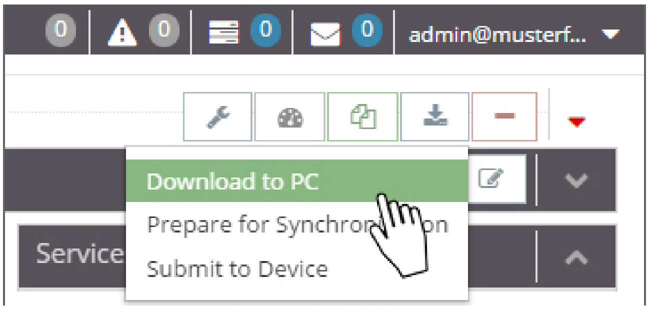
For the initial configuration we recommend "**Download to PC**" method.

11.4.1 Download to PC



Select this transfer type if the device is neither connected to a computer via LAN nor has a connection to the ***mbCONNECT24*** portal.

Click the icon ⤓ to select the transmission type, and then "Download to PC".
The configuration file "mbconnect24.mbn / -.mbn" will be downloaded to the configuration PC or directly to a USB flash drive connected to it.

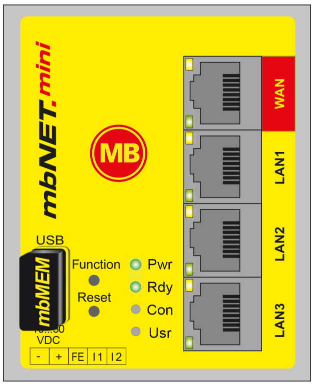


NOTICE

IMPORTANT: The downloaded "mbconnect24.mbn/.mbnx" configuration file may not be renamed and must be stored in the top-level directory of the USB drive. The USB drive must have the file format FAT!

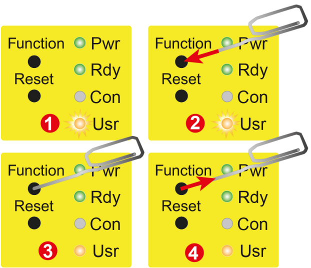
11.4.1.1 Importing the configuration into the device

When the ***mbNET.mini*** is connected to the power supply and is ready for operation, insert the USB stick with the configuration file on it into the USB port of the device. The device will recognize the configuration file and indicate this by the slowly flashing **LED Usr** (flashing frequency: 1.5 Hz).

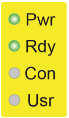


As soon as the **LED Usr starts to flash** ❶, you must press the **Function button** ❷ within 10 seconds.
Hold down u**ntil the LED Usr lights up** ❸.

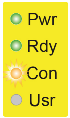
Now release the **Function** button ❹.



When the **LED Usr goes off** and the **LED Pwr + Rdy light up**, then the configuration transfer is complete.



When the ***mbNET.mini*** can connect to the Internet (e.g. network cable, SIM card, antennae installed), the device will subsequently log in to your account. This is displayed by the **flashing LED Con**.

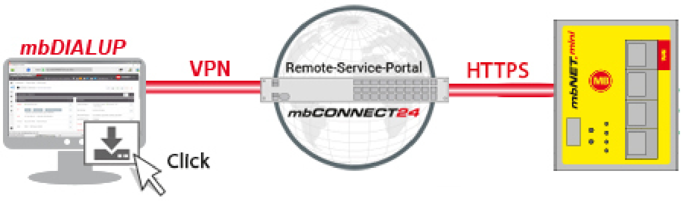


If the flashing frequency of the LED Con is 3 Hz, the device is attempting to log into the portal. If the login has been successful, the flashing frequency is reduced to 1.5 Hz.frequenz auf 1,5 Hz.

NOTICE

In rare instances, the design of the portable USB drive used may make it unsuitable for this procedure. If this should happen, please use another USB stick. Once the configuration file has been imported, it is automatically renamed and is now stored on the USB drive as "**X**mbconnect24.mbn/-.mbnx".

11.4.2 Prepare for Synchronization

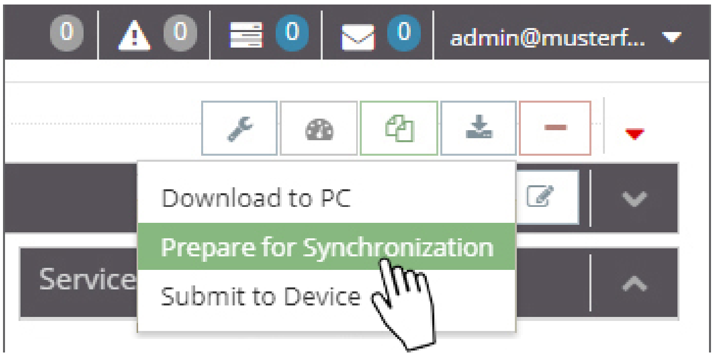


Here you leave the configuration in the portal for collection by the device.Once the device is connecting to the portal, the configuration is automatically transferred to the device.

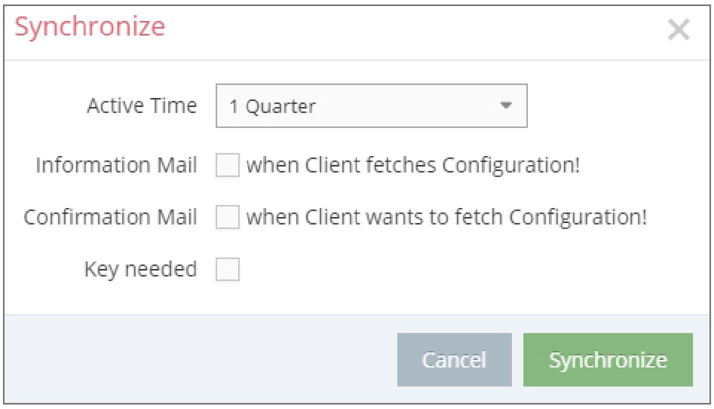
Prerequisite / conditions:

- The device has a connection to the Internet (WAN, Wi-Fi, Modem)
- The device has been pre-configured with the portal connection data (Initial configuration using the device surface)
- a valid server address is registered in the device

Click on the icon ⭳ to select the transfer type, and then click "Prepare for Synchronization".



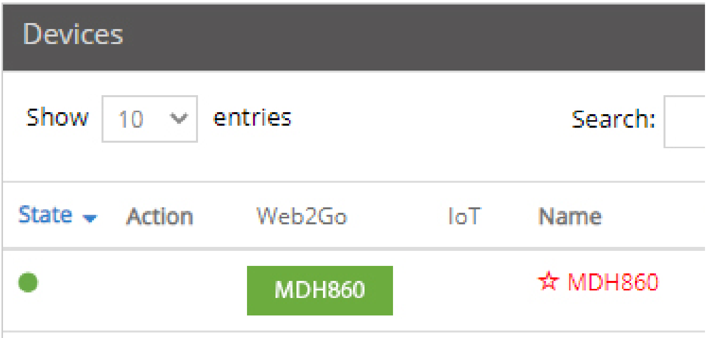
No further settings are necessary for the basic configuration.
Click on "Synchronize".



Synchronize

Active Time	1 Quarter
Information Mail	□ when Client fetches Configuration!
Confirmation Mail	□ when Client wants to fetch Configuration!
Key needed	□

Once the mbNET.mini has logged into the portal, the configuration is transferred to the device.
Your mbNET.mini is now online.

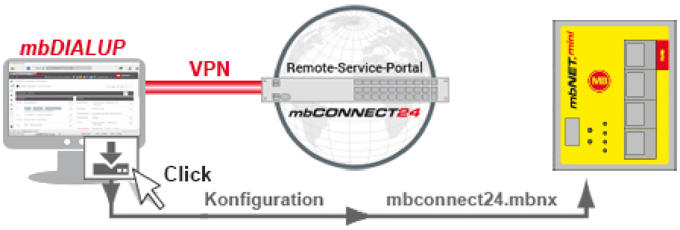


Devices

Show 10 entries Search:

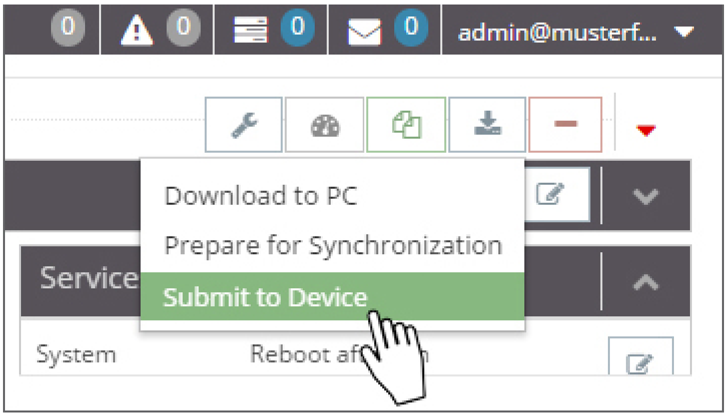
State	Action	Web2Go	IoT	Name
●		MDH860		☆ MDH860

11.4.3 Transferring configuration to the device - via mbDIALUP

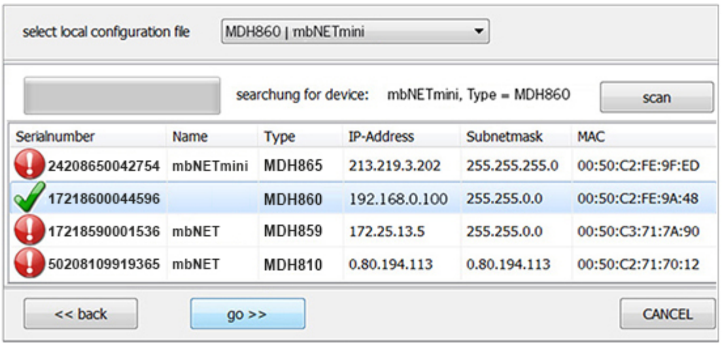


For this, the mbNET.mini must be accessible from a PC on the LAN, irrespective of its LAN IP, and the computer must have a connection to ***mbCONNECT24*** portal.

Click "**Submit configuration to device**"

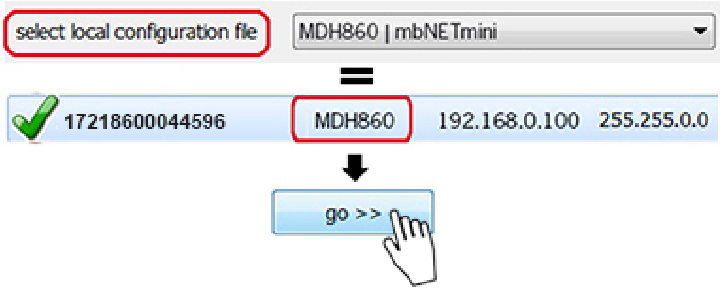


The system now performs a scan and displays all mbNETs that are connected to the LAN.

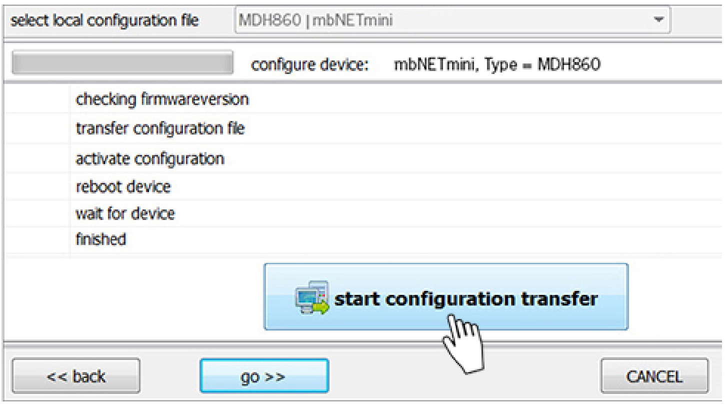

select local configuration file
MDH860 | mbNETmini
searchung for device: mbNETmini, Type = MDH860
scan
<< back
go >>
CANCEL

Serialnumber	Name	Type	IP-Address	Subnetmask	MAC
24208650042754	mbNETmini	MDH865	213.219.3.202	255.255.255.0	00:50:C2:FE:9F:ED
✓ 17218600044596		MDH860	192.168.0.100	255.255.0.0	00:50:C2:FE:9A:48
17218590001536	mbNET	MDH859	172.25.13.5	255.255.0.0	00:50:C3:71:7A:90
50208109919365	mbNET	MDH810	0.80.194.113	0.80.194.113	00:50:C2:71:70:12

If the assignment of the configuration file to the identified device is correct, click on "**go >>**" to confirm.

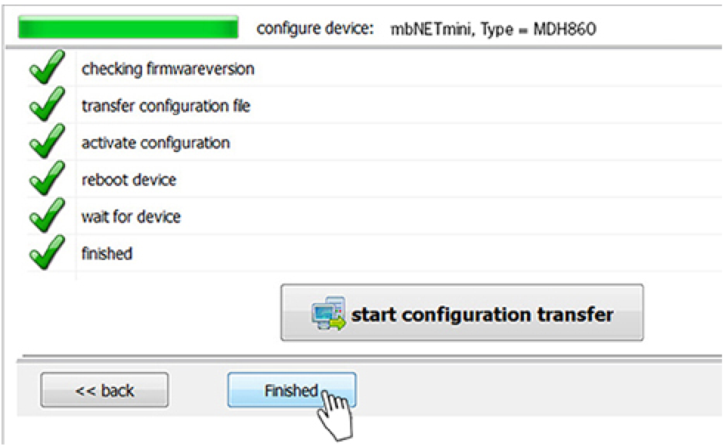


In the next window click on „**start configuration transfer**“.


select local configuration file
MDH860 | mbNETmini
configure device: mbNETmini, Type = MDH860
checking firmwareversion
transfer configuration file
activate configuration
reboot device
wait for device
finished
start configuration transfer
<< back
go >>
CANCEL

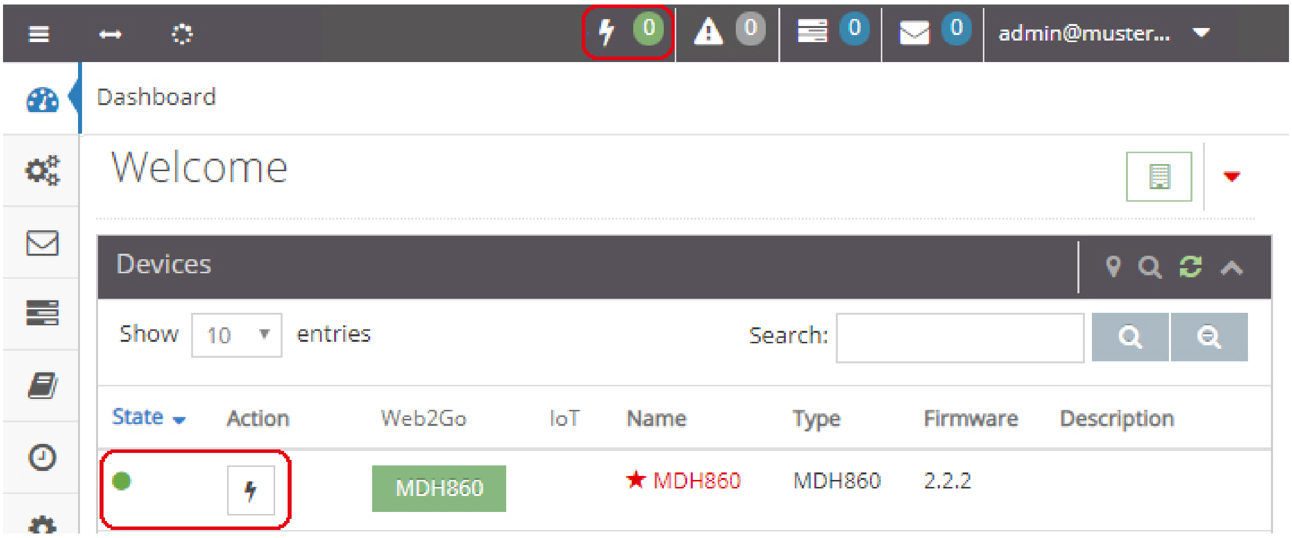
The settings from ***mbCONNECT24*** are now copied to the device.

If all items have been processed, acknowledge the transfer by clicking the "**Finished**" button.


configure device: mbNETmini, Type = MDH860
✓ checking firmwareversion
✓ transfer configuration file
✓ activate configuration
✓ reboot device
✓ wait for device
✓ finished
start configuration transfer
<< back
Finished

If the mbNET.mini is able to connect to the Internet (e.g. network, telephone cable, SIM card, antennae installed), the device will subsequently log in to your account. This is displayed by the flashing LED Con.
If the flashing frequency of the LED Con is 3 Hz, the device attempts to log into the portal. When the login is successful, the flashing frequency is reduced to 1.5 Hz.

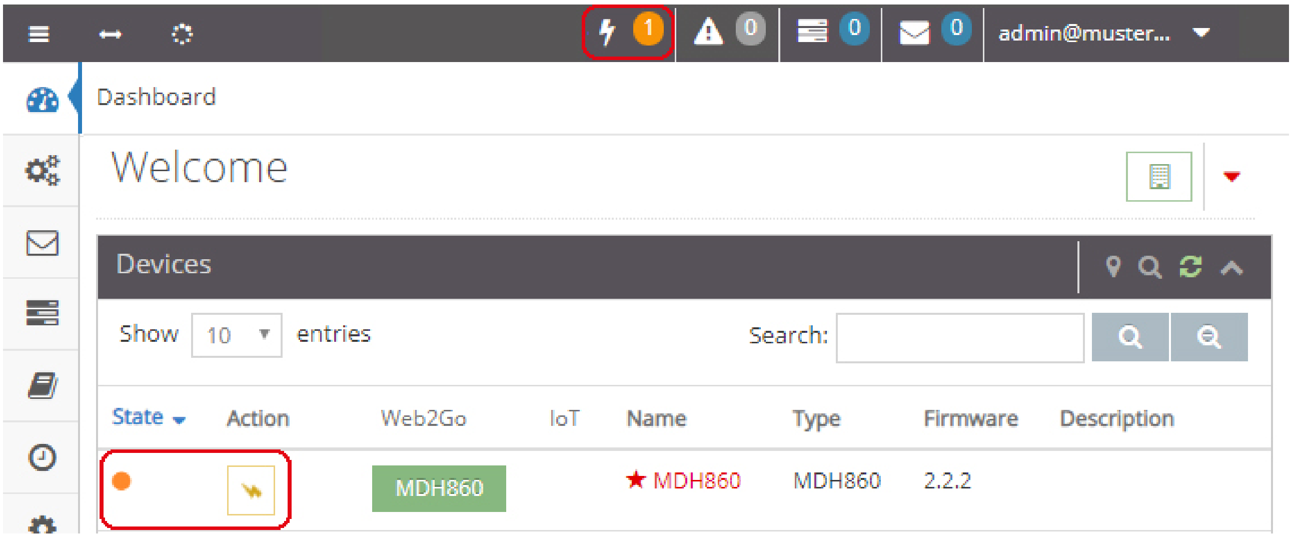
11.5 Access to devices and machines



State	Action	Web2Go	IoT	Name	Type	Firmware	Description
●	⚡	MDH860		★ MDH860	MDH860	2.2.2	

If the ***mbNET.mini*** has an internet connection and the device is signed in, the LED shines green in the status bar.

If you want a connection to a machine you have to click the „Connection“-Icon ⚡.

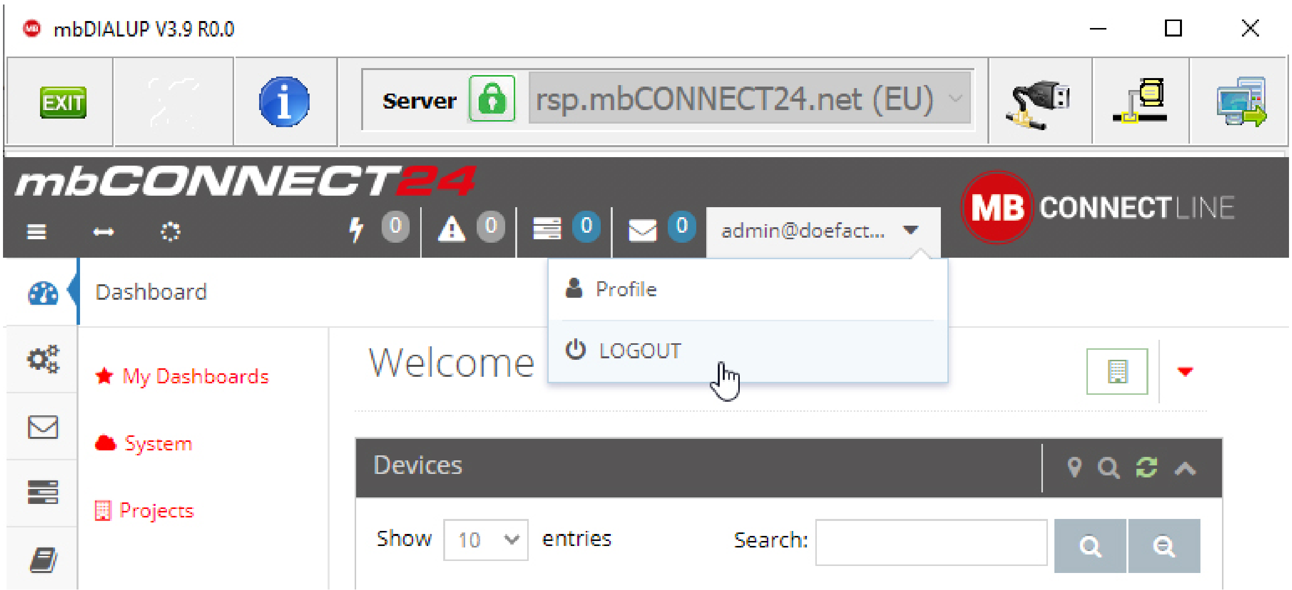


State	Action	Web2Go	IoT	Name	Type	Firmware	Description
●	⚡	MDH860		★ MDH860	MDH860	2.2.2	

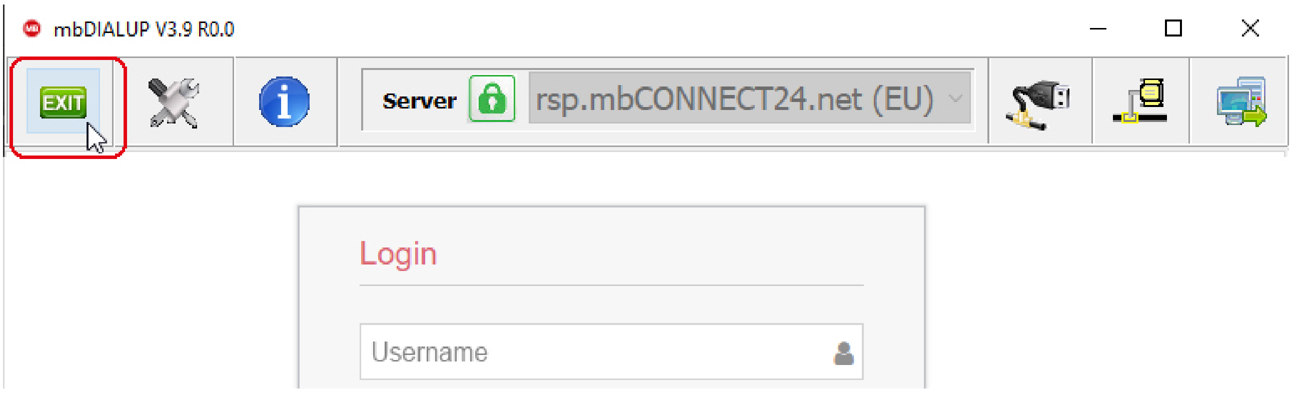
After the connection is established, the LED changes the color from green to orange.
The “Connection”-Icon also changes its color from black to orange and rotates around its axis.
Your connection to the machine is ready.

If you want to disconnect, you have to click the rotating “Connection”-Icon ⚡.

11.6 Quit the *mbCONNECT24* session



If you want to sign out your ***mbCONNECT24*** session properly, click on the button “LOGOUT”.



If you click on the button „**EXIT**“ your client software ***mbDIALUP*** closes.

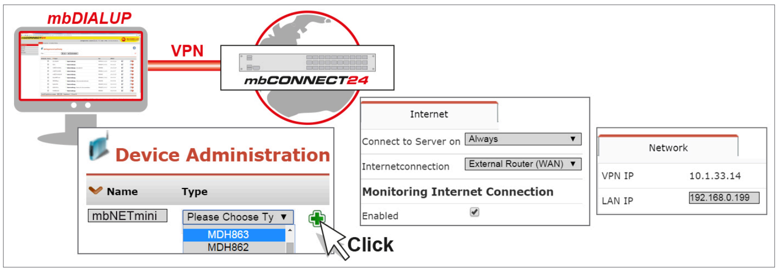
NOTICE

You can find more detailed information in the ***mbCONNECT24*** online help.

11.7 Initial configuration via *mbCONNECT24* V 1.x

Here you can:

- add a new device
- generate a configuration file and
- transfer it to your mbNET.mini



Prerequisites

- an account on ***mbCONNECT24***
  contact your mbCONNECT24 Administrator
- Windows PC with installed remote client ***mbDIALUP***
  The mbDIALUP client software enables you to establish a secure VPN connection to the mbCONNECT24 portal server.
  Alternatively, you can connect via a web browser over a secure https VPN connection to the Portal Server.
- Type and serial number of your ***mbNET.mini***

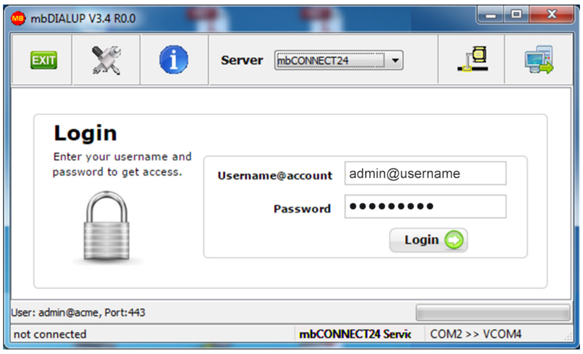
NOTICE

For more information about mbCONNECT24 V 1.x see mbconnectline.com.

Login *mbCONNECT24*

Establish via mbDIALUP or https (eg. Https://vpn2.mbconnect24.net) a connection to the portal mbCONNECT24.

Log in to the portal with your user data (username, password).



Login

Enter your username and password to get access.

Username@account: admin@username

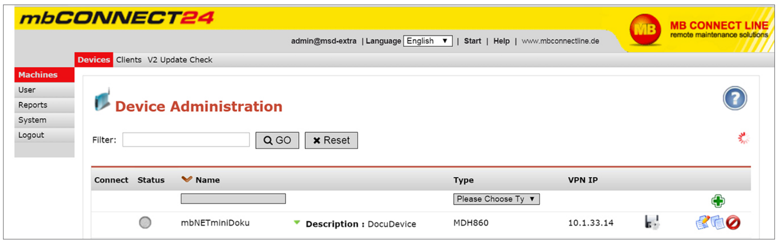
Password: ●●●●●●●●●

Login

User: admin@acme, Port:443

not connected | mbCONNECT24 Servic | COM2 >> VCOM4

If the VPN connection is established, the browser window of your account opens on ***mbCONNECT24***.


mbCONNECT24
MB CONNECT LINE
remote maintenance solutions
admin@msd-extra | Language English | Start | Help | www.mbconnectline.de
Devices
Clients
V2 Update Check
Machines
User
Reports
System
Logout
Filter:
GO
Reset

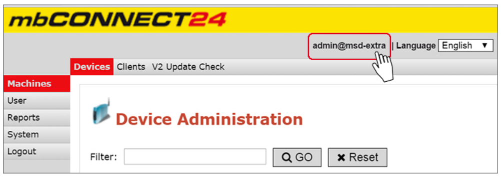
Device Administration

Connect	Status	Name		Type	VPN IP
				Please Choose Ty	
	○	mbNETminiDoku	Description : DocuDevice	MDH860	10.1.33.14

NOTICE

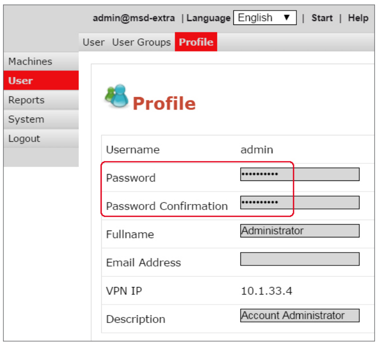
Change unconditionally and without delay your password after your first login.

To do this, click your user in the top menu bar.



Change your password in the "Profile" window that appears next.

Once you have saved the changes, your new password is effective the next time you log in to the portal.



Username	admin
Password	••••••••••
Password Confirmation	••••••••••
Fullname	Administrator
Email Address	
VPN IP	10.1.33.4
Description	Account Administrator

11.7.1 Adding a new device (mbCONNECT24 V 1.x)

NOTICE

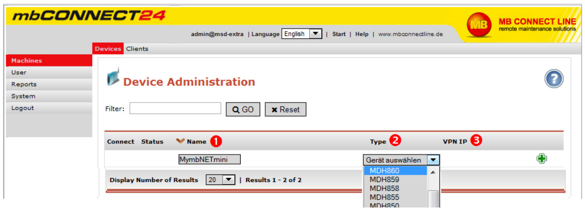
Here, the necessary basic settings for a minimal configuration will be described, so that the device can connect to the portal. For more information see the Portal online help.

Go to the **Machines > Devices** menu and assign a unique designation under **Name** ❶.

NOTICE

You can choose any designation – although only the following numbers and/or letters are allowed: **0** to **9**, **A** to **Z**, **a** to **z**

Select your device from the drop-down field **Type** ❷ and click on **Add** ❸.


mbCONNECT24
MB CONNECT LINE
remote maintenance solutions
admin@msd-extra | Language English | Start | Help | www.mbconnectline.de
Devices Clients
Machines
User
Reports
System
Logout
Device Administration
Filter:
GO
Reset
Connect Status Name 1 Type 2 VPN IP 3
Gerät auswählen
MDH860
MDH859
MDH858
MDH855
MDH850
Display Number of Results 20 | Results 1 - 2 of 2

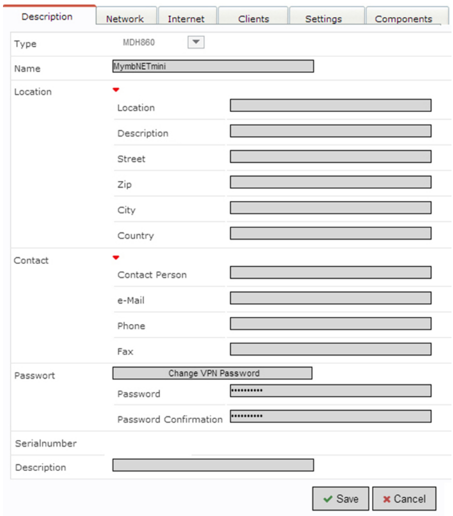
Name: MymbNETmini

11.7.1.1 Description - all devises

Description

Once you have added the new device, the actual configuration menu opens. Depending on the device type selected, the input/drop-down fields may vary here.

Location
Enter your device's location here.
Contact
Enter your contact details here (e.g. a contact person in the device's location).
Password
The VPN password is generated automatically.
Please note that this password is used for authenticating the device.
Each device absolutely must be given an individual password!
Serial number
The device's serial number can be entered here. However, as soon as the device connects to the portal for the first time, it is automatically entered.
Description
For a better overview, enter a short description of the device here.



Type: MDH860

Name: MymbNETmini

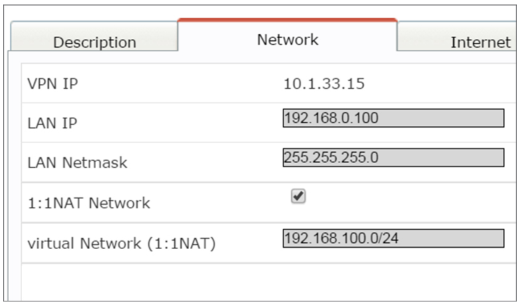
Then go to the tab "**Network**"

11.7.1.2 Network (MDH 860, 861, 862, 863)

Network
MDH 860, MDH 861, MDH 862, MDH 863

Enter a free **LAN IP** address and the subnet mask from your system or machine network here.

Activate the "**1:1NAT Network**" when both tunnel end points have the same network address to enable communication through both networks.



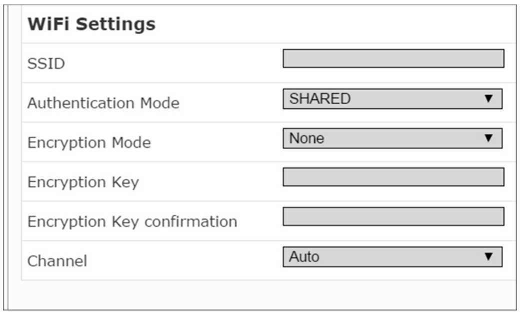
VPN IP	10.1.33.15
LAN IP	192.168.0.100
LAN Netmask	255.255.255.0
1:1NAT Network	☑
virtual Network (1:1NAT)	192.168.100.0/24

NOTICE

Make sure that the LAN IP and WAN IP are in different address ranges.

Wi-Fi Settings (MDH 863)

SSID	Enter the name of the wireless network to which the device should connected.
Authentication Mode	Select the authentication method from the selection list.
Encryption Mode	Select the encryption method.
Encryption Key	Enter the Encryption Key.
Encryption Key confirmation	Repeat the entered Encryption Key.
Kanal	Chose a Wi-Fi channel from the selection list.



WiFi Settings

SSID	
Authentication Mode	SHARED ▼
Encryption Mode	None ▼
Encryption Key	
Encryption Key confirmation	
Channel	Auto ▼

Then go to the "**Internet**" tab.

11.7.1.3 Internet

11.7.1.3.1 WAN device (MDH 860)

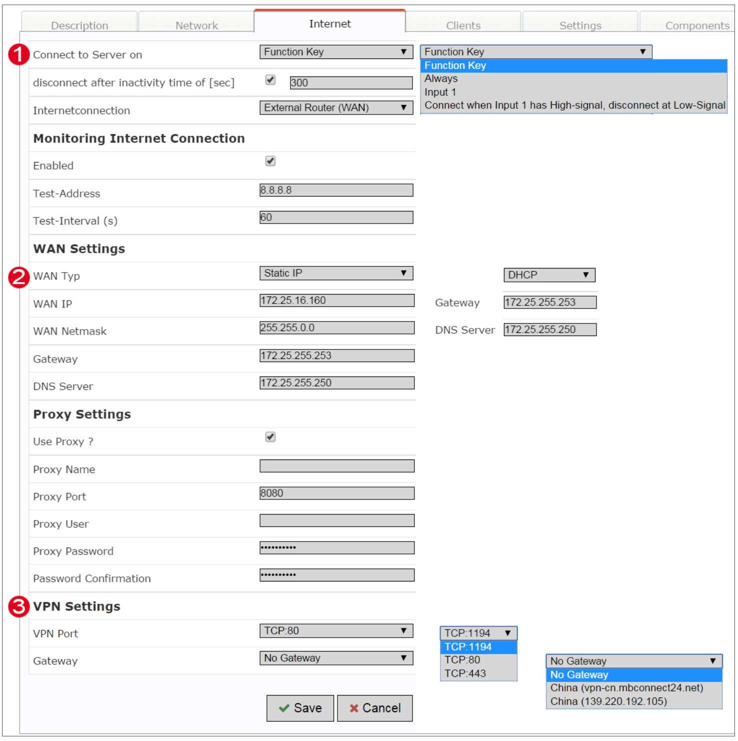
Select:

❶ When the device should be connected to the portal.

❷ Which interface type (DHCP or static IP) should be used.

WAN settings for **DHCP**
Select this setting if there is a DHCP server on the network, which is therefore automatically assigned a new IP address by the industrial router. Please also contact your network administrator to confirm this!
WAN settings for **static IP**
Select this setting if connection to the Internet is already established via an existing router that is not acting as a DHCP sever, or if no server is set up to assign addresses. You should also select this setting if you have received a static address from your ISP, e.g. if you have a leased line. A DNS server address must however still be entered.

❸ Which VPN port should be used (which of the three ports is free has been established via mbCHECK).



❶ Connect to Server on: Function Key ▼ (Function Key / Always / Input 1 / Connect when Input 1 has High-signal, disconnect at Low-Signal)

disconnect after inactivity time of [sec]: ☑ 300

Internetconnection: External Router (WAN) ▼

Monitoring Internet Connection

Enabled: ☑

Test-Address: 8.8.8.8

Test-Interval (s): 60

WAN Settings

❷ WAN Typ: Static IP ▼ (DHCP ▼ — Gateway: 172.25.255.253, DNS Server: 172.25.255.250)

WAN IP: 172.25.16.160

WAN Netmask: 255.255.0.0

Gateway: 172.25.255.253

DNS Server: 172.25.255.250

Proxy Settings

Use Proxy ?: ☑

Proxy Name:

Proxy Port: 8080

Proxy User:

Proxy Password: ••••••••••

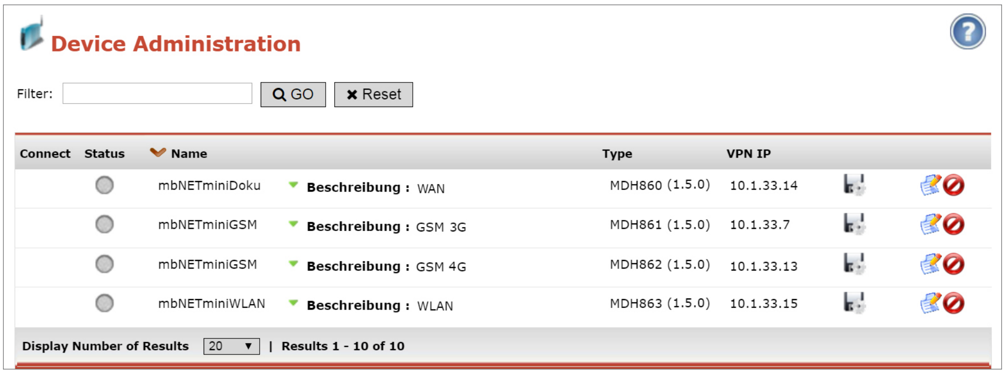
Password Confirmation: ••••••••••

❸ **VPN Settings**

VPN Port: TCP:80 ▼ (TCP:1194 / TCP:80 / TCP:443)

Gateway: No Gateway ▼ (No Gateway / China (vpn-cn.mbconnect24.net) / China (139.220.192.105))

After saving your settings, you will see the new device in the Device Administration window.



Connect	Status	Name		Type	VPN IP		
	○	mbNETminiDoku	**Beschreibung :** WAN	MDH860 (1.5.0)	10.1.33.14	💾	✎ ⊘
	○	mbNETminiGSM	**Beschreibung :** GSM 3G	MDH861 (1.5.0)	10.1.33.7	💾	✎ ⊘
	○	mbNETminiGSM	**Beschreibung :** GSM 4G	MDH862 (1.5.0)	10.1.33.13	💾	✎ ⊘
	○	mbNETminiWLAN	**Beschreibung :** WLAN	MDH863 (1.5.0)	10.1.33.15	💾	✎ ⊘

Display Number of Results 20 ▼ | Results 1 - 10 of 10

Click on the disk icon 💾 of that device to transfer the configuration or provide for collection by the device via CTM.

11.7.1.3.2 WAN device (MDH 861, 862)

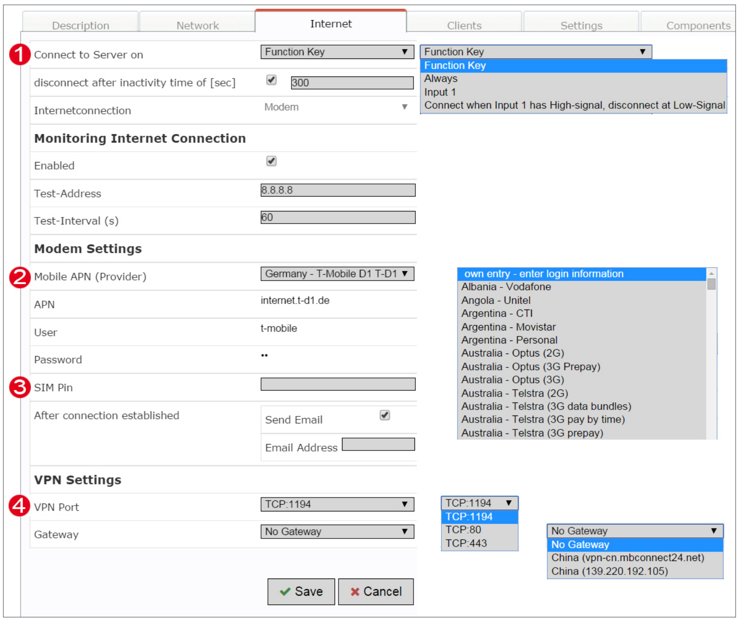
Basic settings:

❶ Determine when the device should connect to the portal.

❷ Select the mobile APN of your provider (if your provider does not appear in the list, you can also enter the APN (access point name) manually under "Own entry - enter login information"). You can obtain information on the APN from your mobile broadband provider.

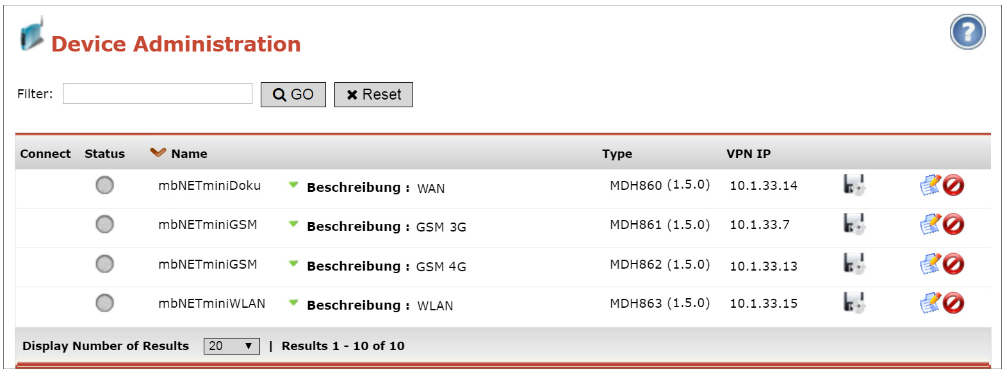
❸ If required, you can enter the SIM card PIN of the SIM card used here.

❹ Select which VPN port should be used (which of the three ports is free was determined by mbCHECK).



❶ Connect to Server on	Function Key ▼
disconnect after inactivity time of [sec]	☑ 300
Internetconnection	Modem ▼
Monitoring Internet Connection	
Enabled	☑
Test-Address	8.8.8.8
Test-Interval (s)	60
Modem Settings	
❷ Mobile APN (Provider)	Germany - T-Mobile D1 T-D1 ▼
APN	internet.t-d1.de
User	t-mobile
Password	••
❸ SIM Pin	
After connection established	Send Email ☑ Email Address
VPN Settings	
❹ VPN Port	TCP:1194 ▼
Gateway	No Gateway ▼

After saving your settings, you will see the new device in the Device Administration window.



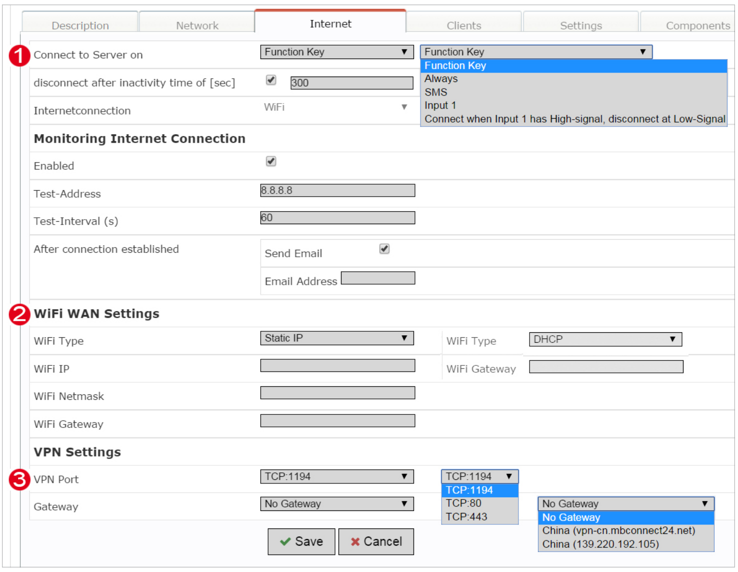
Connect	Status	Name		Type	VPN IP		
	○	mbNETminiDoku	**Beschreibung :** WAN	MDH860 (1.5.0)	10.1.33.14		
	○	mbNETminiGSM	**Beschreibung :** GSM 3G	MDH861 (1.5.0)	10.1.33.7		
	○	mbNETminiGSM	**Beschreibung :** GSM 4G	MDH862 (1.5.0)	10.1.33.13		
	○	mbNETminiWLAN	**Beschreibung :** WLAN	MDH863 (1.5.0)	10.1.33.15		

Display Number of Results 20 ▼ | **Results 1 - 10 of 10**

Click on the disk icon of that device to transfer the configuration or provide for collection by the device via CTM.

11.7.1.3.3 Wi-Fi device (MDH 863)

Select:



Description | Network | Internet | Clients | Settings | Components

❶ Connect to Server on: Function Key ▼ | Function Key ▼
Function Key
Always
SMS
Input 1
Connect when Input 1 has High-signal, disconnect at Low-Signal

disconnect after inactivity time of [sec]: ☑ 300

Internetconnection: WiFi ▼

Monitoring Internet Connection

Enabled: ☑

Test-Address: 8.8.8.8

Test-Interval (s): 60

After connection established: Send Email ☑; Email Address

❷ **WiFi WAN Settings**

WiFi Type: Static IP ▼ | WiFi Type: DHCP ▼

WiFi IP | WiFi Gateway

WiFi Netmask

WiFi Gateway

VPN Settings

❸ VPN Port: TCP:1194 ▼ | TCP:1194 ▼

Gateway: No Gateway ▼ | No Gateway ▼

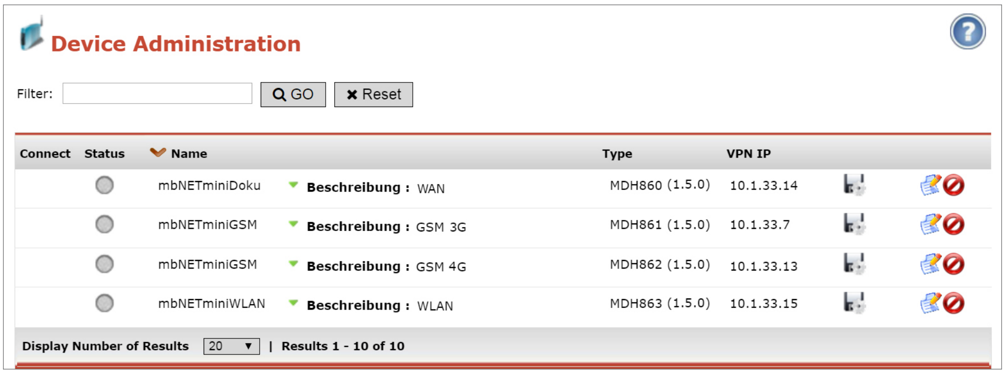
❶ When the device should be connected to the portal.

❷ Which interface type (DHCP or static IP) should be used.

Wi-Fi WAN settings for **DHCP**
Select this setting if there is a DHCP server on the network, which is therefore automatically assigned a new IP address by the industrial router. Please also contact your network administrator to confirm this!
Wi-Fi WAN settings for **static IP**
Select this setting if connection to the Internet is already established via an existing router that is not acting as a DHCP sever, or if no server is set up to assign addresses. You should also select this setting if you have received a static address from your ISP, e.g. if you have a leased line. A DNS server address must however still be entered.

❸ Which VPN port should be used (which of the three ports is free has been established via mbCHECK).

After saving your settings, you will see the new device in the Device Administration window.



Device Administration

Connect	Status	Name		Type	VPN IP		
	○	mbNETminiDoku	**Beschreibung :** WAN	MDH860 (1.5.0)	10.1.33.14		
	○	mbNETminiGSM	**Beschreibung :** GSM 3G	MDH861 (1.5.0)	10.1.33.7		
	○	mbNETminiGSM	**Beschreibung :** GSM 4G	MDH862 (1.5.0)	10.1.33.13		
	○	mbNETminiWLAN	**Beschreibung :** WLAN	MDH863 (1.5.0)	10.1.33.15		

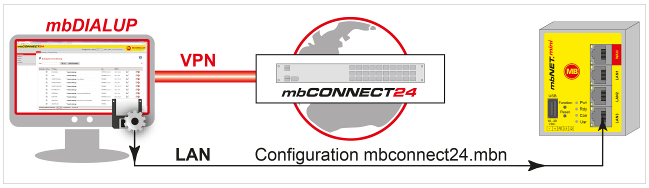
Display Number of Results 20 ▼ | **Results 1 - 10 of 10**

Click on the disk icon of that device to transfer the configuration or provide for collection by the device via CTM.

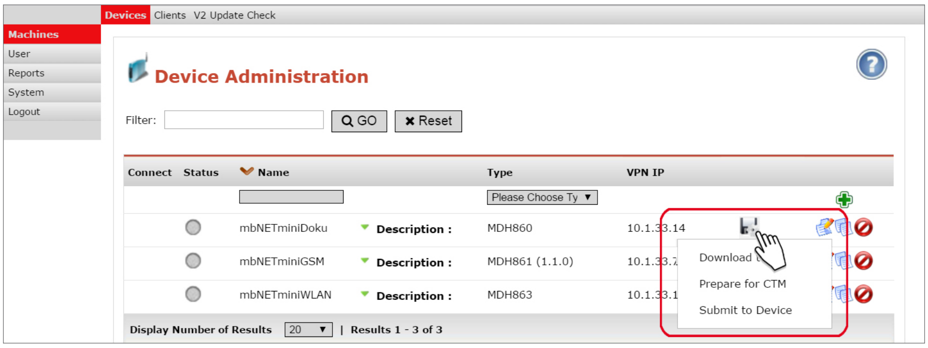
11.7.2 Transferring the configuration to *mbNET.mini*

The following options are available for transferring the configuration file:

- Download to PC
- Prepare for CTM
- Submit to Device



Once you have created a new device, click on the disk symbol to select the transfer type .



Device Administration

Filter: GO ✖ Reset

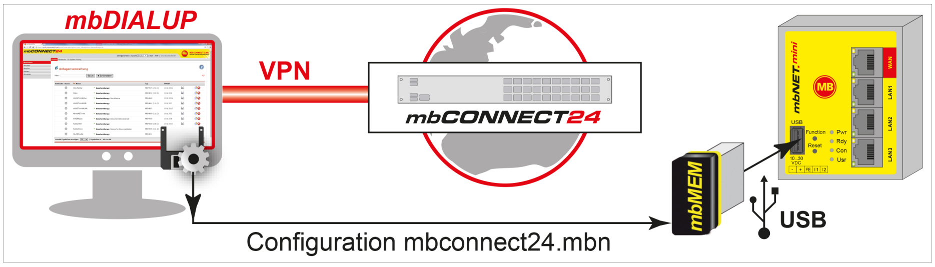
Connect	Status	Name		Type	VPN IP
				Please Choose Ty ▼	
	○	mbNETminiDoku	Description :	MDH860	10.1.33.14
	○	mbNETminiGSM	Description :	MDH861 (1.1.0)	10.1.33.7
	○	mbNETminiWLAN	Description :	MDH863	10.1.33.1

Display Number of Results 20 ▼ | Results 1 - 3 of 3

11.7.2.1 Download configuration to PC - via USB

Select this transfer type if the mbNET.mini is neither connected to a computer via LAN nor has a connection to the ***mbCONNECT24*** portal.

The "mbconnect24.mbn/-.mbnx" configuration file is saved on the configuration PC or directly on a USB drive con-nected to it.

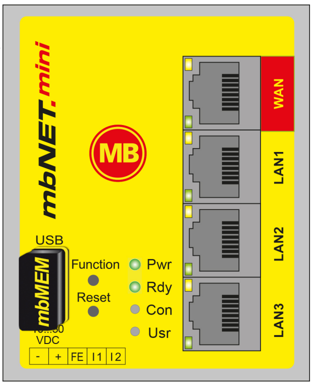


NOTICE

IMPORTANT: The downloaded "mbconnect24.mbn/.mbnx" configuration file may not be renamed and must be saved in the top-level directory of the USB drive. The USB drive must have the file format FAT.

Importing the configuration into the device

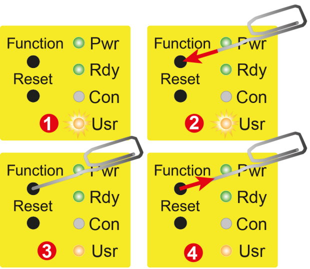
When the ***mbNET.mini*** is ready to operate, insert the USB stick into the USB port of the device. The device will recognize the configuration file and show that through the slowly flashing **LED Usr** (flashing frequency: 1.5 Hz).



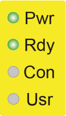
As soon as the **LED Usr starts to flash** ❶, you must press the **Function button** ❷ within 10 seconds.

Hold down u**ntil the LED Usr lights up** ❸.

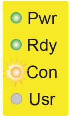
Now release the **Function** button ❹.



When the **LED Usr goes off** and the **LED Pwr + Rdy light up**, then the configuration transfer is complete.



When the ***mbNET.mini*** can connect to the Internet (e.g. network cable, SIM card, antennae installed), the device will subsequently log in to your account. This is displayed by the **flashing LED Con**.



If the flashing frequency of the LED Con is 3 Hz, the device is attempting to log into the portal. If the login has been successful, the flashing frequency is reduced to 1.5 Hz.

NOTICE

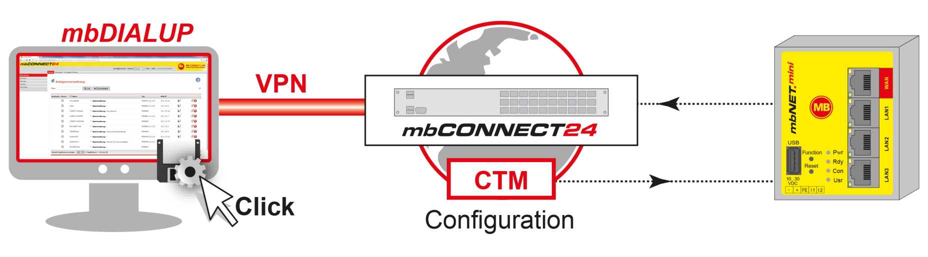
In rare instances, the design of the portable USB drive used may make it unsuitable for this procedure. If this should happen, please use another USB stick. Once the configuration file has been imported, it is automatically renamed and is now stored on the USB drive as "**X**mbconnect24.mbn/-.mbnx".

11.7.2.2 Transfer configuration to the device - via CTM

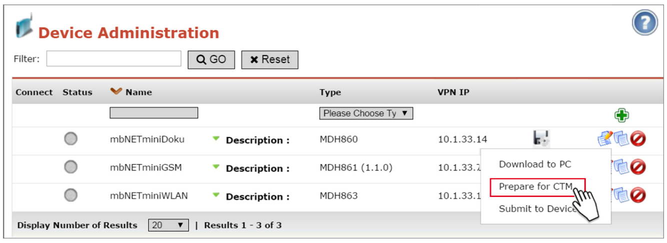
Here the ***mbCONNECT24*** configuration is placed in the CTM (Configuration Transfer Manager) to be collected by the ***mbNET.mini***. On the interface of the ***mbNET.mini***, create an initial configuration so the device can connect to the portal. The ***mbNET.mini*** will then collect its portal configuration from the CTM there.

NOTICE

For this transfer when creating a device, the device serial number **must** be entered!



Click on the disk icon in the Device Administration and then on "**Prepare for CTM**".

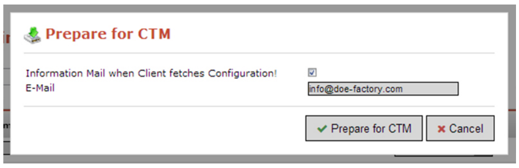

Device Administration

Filter: [ ] GO Reset

Connect	Status	Name		Type	VPN IP
				Please Choose Ty ▼	
	○	mbNETminiDoku	Description :	MDH860	10.1.33.14
	○	mbNETminiGSM	Description :	MDH861 (1.1.0)	10.1.33.2
	○	mbNETminiWLAN	Description :	MDH863	10.1.33.1

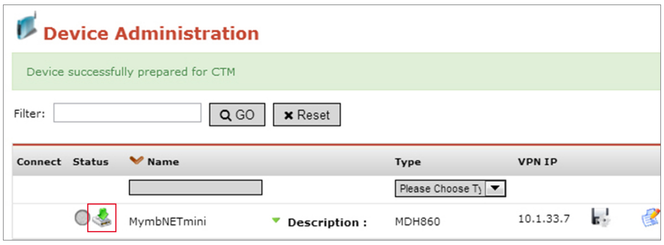
Display Number of Results 20 ▼ | Results 1 - 3 of 3

In the next window, select whether a notification email should be sent and to which address as soon as the device has collected the configuration.


Prepare for CTM

Information Mail when Client fetches Configuration! ☑
E-Mail info@doe-factory.com

After confirming via the interface "**Prepare for CTM**", a symbol shows that the configuration is ready to be collected in the CTM.
As soon as the ***mbNET.mini*** is connected to the portal, it will collect its configuration.

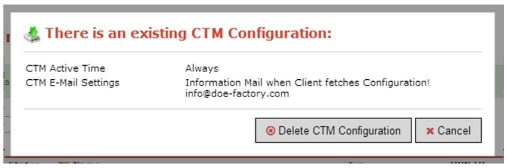

Device Administration

Device successfully prepared for CTM

Filter: [ ] GO Reset

Connect	Status	Name		Type	VPN IP
				Please Choose Ty ▼	
	○	MymbNETmini	Description :	MDH860	10.1.33.7

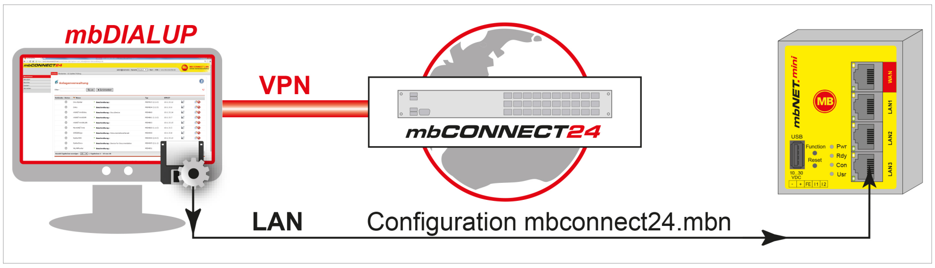
By clicking on this symbol the data saved in the CTM are shown.
The configuration can still be deleted from the CTM.


There is an existing CTM Configuration:

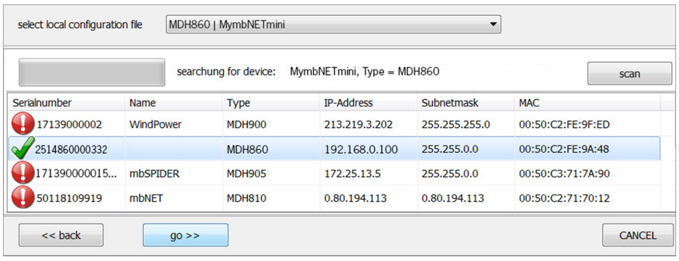
CTM Active Time Always
CTM E-Mail Settings Information Mail when Client fetches Configuration!
info@doe-factory.com

11.7.2.3 Transferring configuration to the device - via mbDIALUP

For this, the ***mbNET.mini*** must be accessible from a PC on the LAN, irrespective of its LAN IP, and the computer must have a connection to ***mbCONNECT24*** portal.

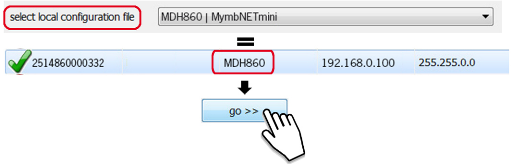


After clicking "Submit configuration to device", the system performs a scan of all devices connected to the LAN interface (mbNET/mbSPIDER) and displays them.
If the assignment of the configuration file to the identified device is correct, click on "**go >>**" to confirm.


select local configuration file: MDH860 | MymbNETmini

searchung for device: MymbNETmini, Type = MDH860

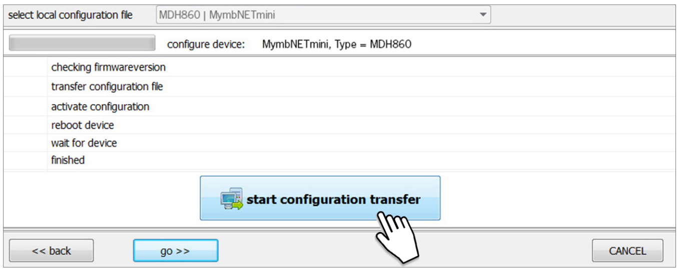
Serialnumber	Name	Type	IP-Address	Subnetmask	MAC
! 17139000002	WindPower	MDH900	213.219.3.202	255.255.255.0	00:50:C2:FE:9F:ED
✓ 2514860000332		MDH860	192.168.0.100	255.255.0.0	00:50:C2:FE:9A:48
! 171390000015...	mbSPIDER	MDH905	172.25.13.5	255.255.0.0	00:50:C3:71:7A:90
! 50118109919	mbNET	MDH810	0.80.194.113	0.80.194.113	00:50:C2:71:70:12


select local configuration file: MDH860 | MymbNETmini

=

✓ 2514860000332 | MDH860 | 192.168.0.100 | 255.255.0.0

In the next window click on „**start configuration transfer**“.

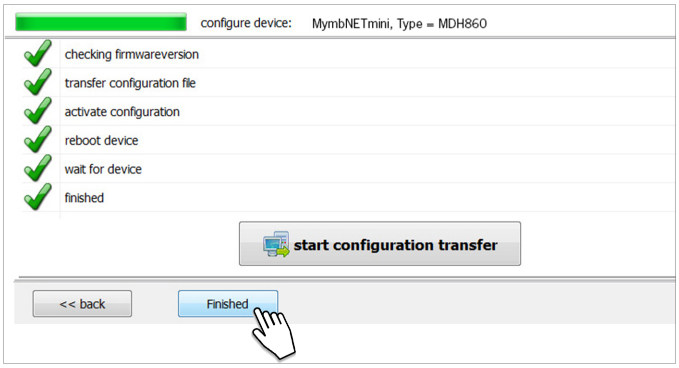

select local configuration file: MDH860 | MymbNETmini

configure device: MymbNETmini, Type = MDH860

checking firmwareversion
transfer configuration file
activate configuration
reboot device
wait for device
finished

The settings from ***mbCONNECT24*** are now copied to the device.

If all items have been processed, acknowledge the transfer by clicking the "**Finished**" button.


configure device: MymbNETmini, Type = MDH860

✓ checking firmwareversion
✓ transfer configuration file
✓ activate configuration
✓ reboot device
✓ wait for device
✓ finished

11.8 Initial configuration of the router via its device web interface

You can preconfigure the mbNET with its portal connection data (see chapter Firststart).

If the mbNET can establish a connection to the Internet, it logs on to your mbCONNECT24 account with this data and fetches the configuration it has provided.

Requirement

- The mbNET is ready for operation and can establish a connection to the Internet.
- The connection data in the mbNET are congruent with the connection data that you have stored for this mbNET in mbCONNECT24.

Connect the ***mbNET.mini*** to the power supply.
Connect the ***mbNET.mini*** via one of the LAN interfaces to the Ethernet interface on your configuration PC.

NOTICE

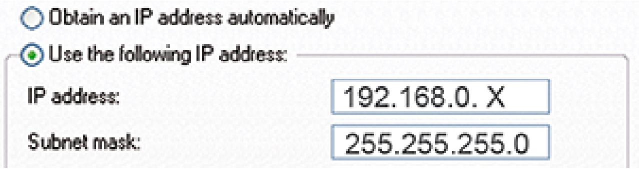
The configuration PC and the ***mbNET.mini*** must be in the IP address range (192.168.0.X).

For this purpose, where necessary, carry out the following settings on your computer:

The ***mbNET.mini*** is shipped with the IP address **192.168.0.100.** You must therefore assign the same address range to your computer. This applies for the IP address as well as for the subnet mask.

To do this, open the properties for your LAN connection. You can set your computer’s IP address under the properties for the Internet protocol (TCP/IP).

Your computer's IP address must be in the address range “192.168.0.X”, the subnet mask must be identical to that of the ***mbNET.mini*** (255.255.255.0).



○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192.168.0. X
Subnet mask: 255.255.255.0

Default settings for ***mbNET.mini***

IP address	192.168.0.100
Subnet mask	255.255.255.0
Login	admin
Password	(no password required)

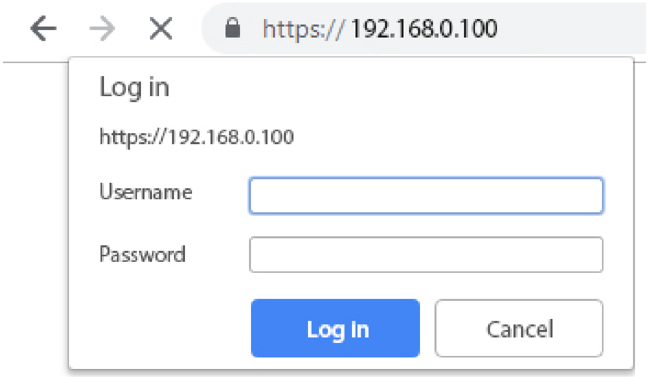
NOTICE

Change at the next opportunity unconditionally and without delay, the default login information!

Open your browser and enter the ***mbNET.mini's*** required IP address (192.168.0.100) in the address line.

Please enter the following details to log into the ***mbNET.mini***:

Username:	admin
Password:	(no password required)



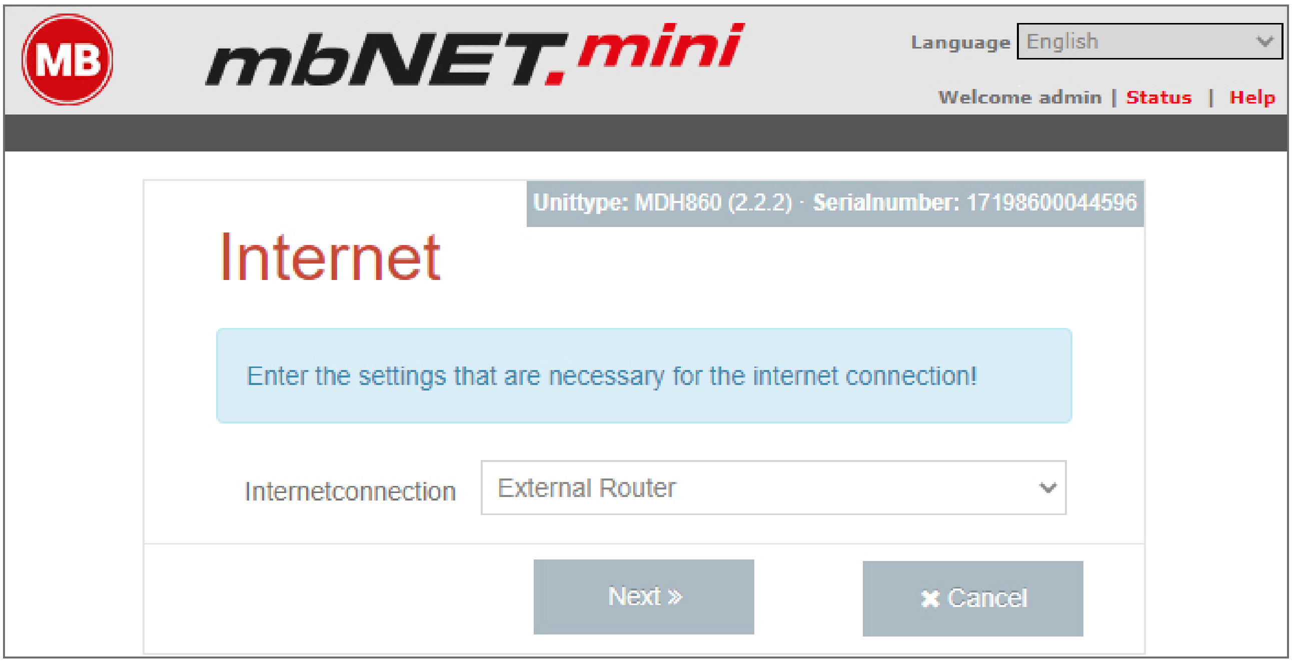
https:// 192.168.0.100

Log in

https://192.168.0.100

Username

Password



Unittype: MDH860 (2.2.2) · Serialnumber: 17198600044596

Internet

Enter the settings that are necessary for the internet connection!

Internetconnection: External Router

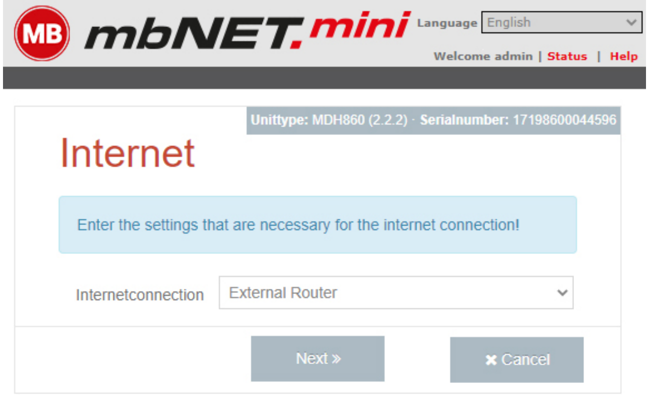
11.8.1 First Start

After the device login you will be guided step by step through the "First Start" menu.
In the **language selection** of the menu header, you can choose between German and English.
The **Help** button provides access to the device online help.

Internet (all types)

In the selection box "Internetconnection", see the default value the respective device. This value cannot be changed.

- **External router** when using WAN and Wi-Fi devices (MDH 860, MDH 863, MDH 867)
- **Modem** when using modem devices (MDH861, MDH 862, MDH865, MDH 866)



Language: English

Unittype: MDH860 (2.2.2) · Serialnumber: 17198600044596

Internet

Enter the settings that are necessary for the internet connection!

Internetconnection: External Router

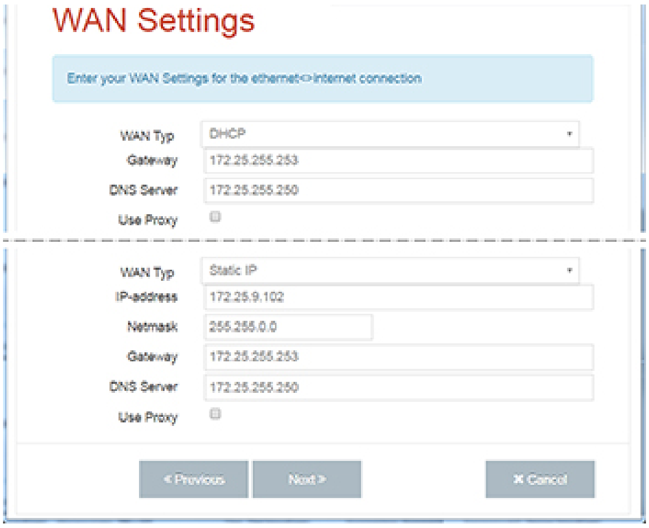
To continue click on „Next>>“

WAN Settings (MDH 860, MDH 865, MDH 866, MDH 867)

In the selection box **WAN Type** you have the following options:

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

When using a proxy server, select the check box "**Use Proxy**".



WAN Settings

Enter your WAN Settings for the ethernet<>internet connection

WAN Typ: DHCP
Gateway: 172.25.255.253
DNS Server: 172.25.255.250
Use Proxy: □

WAN Typ: Static IP
IP-address: 172.25.9.102
Netmask: 255.255.0.0
Gateway: 172.25.255.253
DNS Server: 172.25.255.250
Use Proxy: □

To continue click on „Next>>“

Proxy

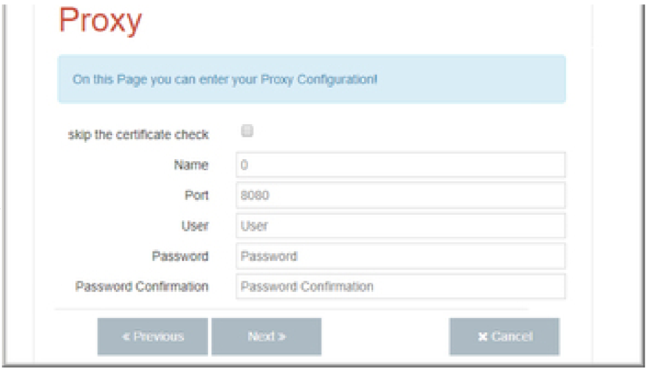
Enter the information for your proxy.

skip the certificate check

"**SSL termination**

An HTTPS connection can be broken down (scheduled) by means of a web proxy in order to also check its contents for pests. Further encryption to the client (browser) then takes place with a certificate offered by the proxy. The problem with this is that the user of the browser no longer gets to see the original certificate of the web server and has to trust the proxy server that he has taken a validation of the web server certificate."[1]

One way to avoid this problem is to enable this feature.



Proxy

On this Page you can enter your Proxy Configuration!

skip the certificate check □

Name: 0

Port: 8080

User: User

Password: Password

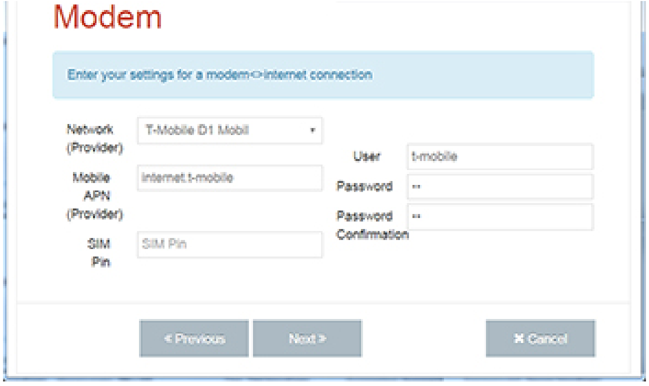
Password Confirmation: Password Confirmation

To continue click on „Next>>“

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

Modem (MDH 861, MDH 862, MDH 865, MDH 866)

Enter the APN provider and the SIM PIN here. That is possible in "Network (Provider)" a list of providers. If your provider can not be found in the list, you can fill in each field individually.



Modem

Enter your settings for a modem<>internet connection

Network (Provider): T-Mobile D1 Mobil ▾

Mobile APN (Provider): internet.t-mobile

SIM Pin: SIM Pin

User: t-mobile

Password: ••

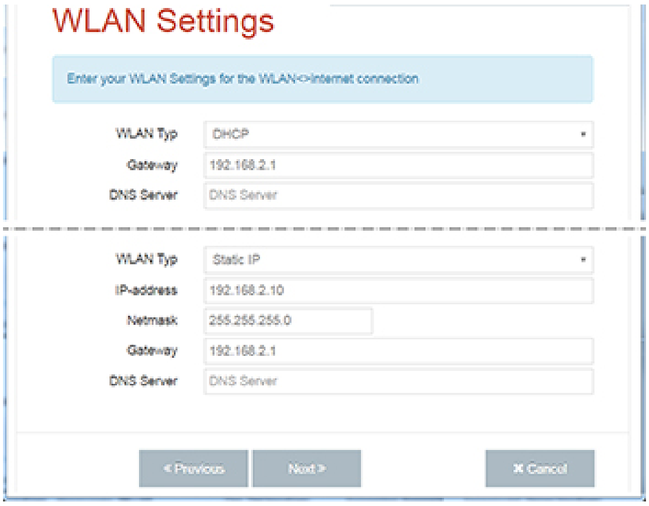
Password Confirmation: ••

To continue click on „Next>>“

WLAN Settings - Connection to the Internet (MDH 863, MDH 867)

In the selection box **WLAN Type** you have the following options:

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



WLAN Settings

Enter your WLAN Settings for the WLAN<>internet connection

WLAN Typ: DHCP ▾

Gateway: 192.168.2.1

DNS Server: DNS Server

WLAN Typ: Static IP ▾

IP-address: 192.168.2.10

Netmask: 255.255.255.0

Gateway: 192.168.2.1

DNS Server: DNS Server

To continue click on „Next>>“

WLAN Settings - Connection with the Access Point (MDH 863, MDH 867)
Enter the necessary data in order to connect to the Access Point.

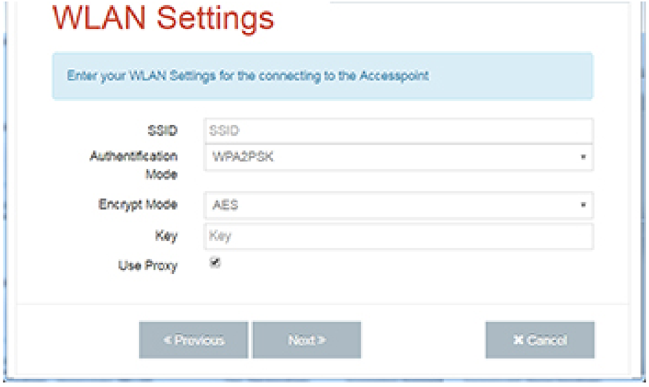
SSID **Mandatory field**: Enter the name of the Wi-Fi network to which the device should connect.

Authentication Mode **Selection field** for the authentication mode.

Encrypt Mode **Selection field** for the encryption mode.

Key **Mandatory field**: Enter the encryption key again.

Use Proxy When using a proxy server, select the **check box** "**Use Proxy**".



WLAN Settings

Enter your WLAN Settings for the connecting to the Accesspoint

SSID: SSID

Authentification Mode: WPA2PSK

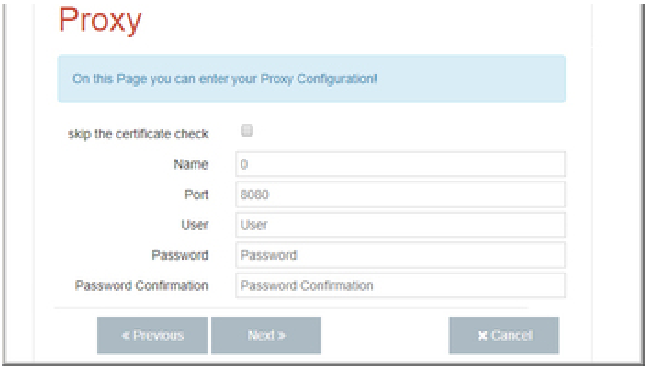
Encrypt Mode: AES

Key: Key

Use Proxy ☑

To continue click on „Next>>“

Proxy
Enter the information for your proxy.
skip the certificate check
"**SSL termination**
An HTTPS connection can be broken down (scheduled) by means of a web proxy in order to also check its contents for pests. Further encryption to the client (browser) then takes place with a certificate offered by the proxy. The problem with this is that the user of the browser no longer gets to see the original certificate of the web server and has to trust the proxy server that he has taken a validation of the web server certificate."[1]
One way to avoid this problem is to enable this feature.



Proxy

On this Page you can enter your Proxy Configuration!

skip the certificate check □

Name: 0

Port: 8080

User: User

Password: Password

Password Confirmation: Password Confirmation

To continue click on „Next>>“

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

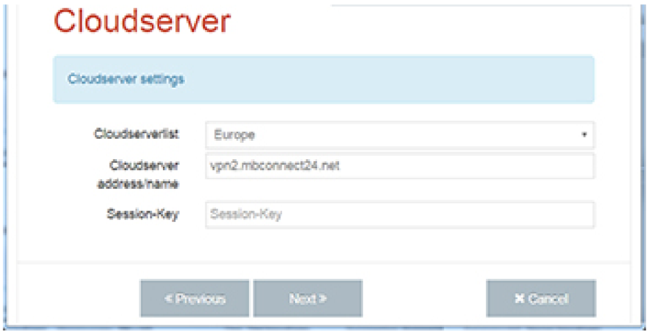
Cloudserver (MDH 860, MDH 861, MDH 862, MDH 863, MDH 865, MDH 866, MDH 867)

Choose your portal server from the **Cloudserver** list. The choice depends on

a) the server location you specified when you register to mbCONNECT24

b) Your portal version

- mbCONNECT24 V 1.x
- RSP mbCONNECT24 V 2.x



Cloudserver

Cloudserver settings

Cloudserverlist: Europe

Cloudserver address/name: vpn2.mbconnect24.net

Session-Key: Session-Key

Cloud server list	Cloud server address / name	Cloud server version
Europe	vpn2.mbconnect24.net	mbCONNECT24 V 1.x
USA/Canada	vpn.mbconnect24.us	mbCONNECT24 V 1.x
rsp.mbconnect24.net (EU)	rsp-vpn.mbconnect24.net	RSP mbCONNECT24 V 2.x
rsp.mbconnect24.net (US/CAN)	rsp-vpn.mbconnect24.us	RSP mbCONNECT24 V 2.x
rsp.mbCONNECT24.asia (ASIA)	rsp.mbCONNECT24.asia	RSP mbCONNECT24 V 2.x
rsp.au.mbCONNECT24.net (AU)	rsp.au.mbCONNECT24.net	RSP mbCONNECT24 V 2.x
User Defined	Cloud server address / name / URL	mymbCONNECT24*-Server V 1.x/2.x

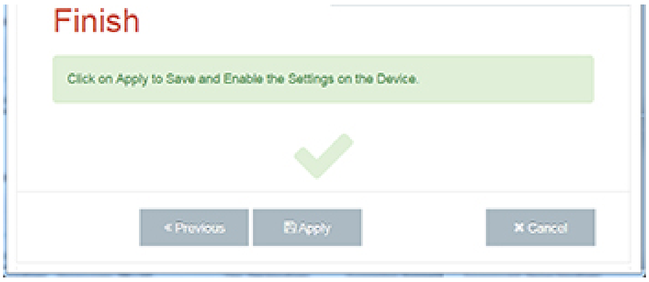
*mymbCONNECT.mini/-.midi/-.maxi/-.hosted/-.virtual

EU = Europe; US/CAN = USA / Canada; ASIA = Asia; AU = Australia

Session-Key
As an additional safety feature can be generated in the portal a session key. With this key, the device reads from his portal configuration. If a session key is generated it **must** be entered here. Each key is valid only once.

To continue click on „Next>>“

Finish (all types)
Clicking the "Apply" button saves your settings.
The ***mbNET.mini*** now tries to establish a connection to the portal in order to download its portal configuration.
For this purpose, the display of the web interface switches to the status display.



Finish

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

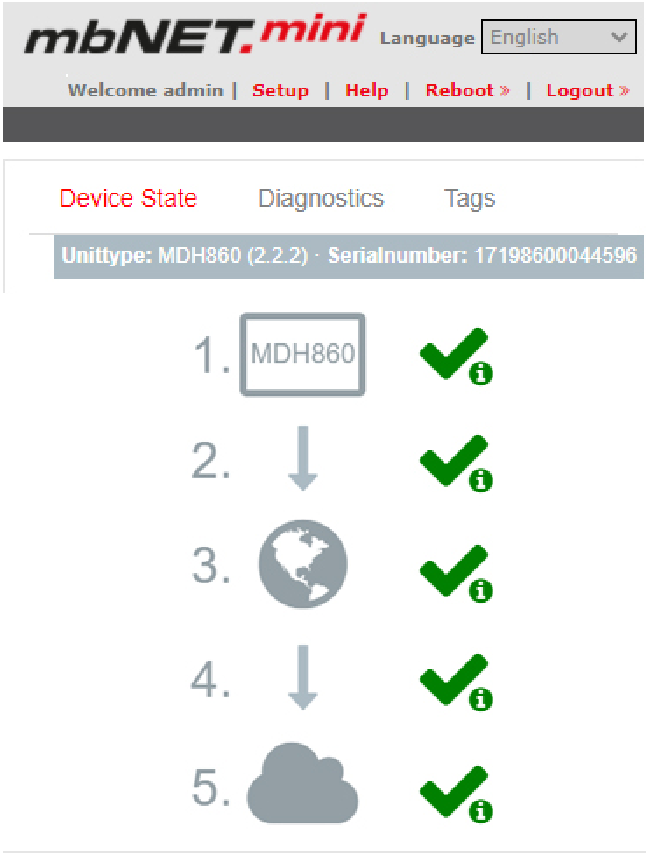
11.8.2 Device State

The status page of the device opens automatically

a) after completing the "First Start" menu by clicking the "Apply" button

b) at each future access to the web interface of the device

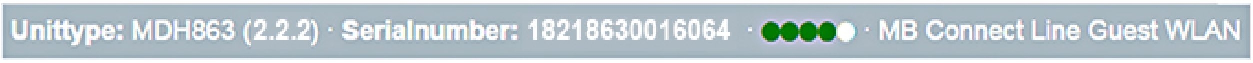
Here all steps are shown, which are necessary so that the device can establish a connection to portal. After all steps have been successfully completed, each step has a green check mark.
If there is a device configuration on the portal ready for download, the device download now its configuration.



Unittype: MDH860 (2.2.2) · Serialnumber: 17198600044596

In the header of the Status page, see the following fields / buttons:

Language	Selection field for the user language
| **Setup** |	Calling the setup menu (Firststart)
| **Help** |	Calling the device online help
| **Reboot >>** |	Triggering a device restart
| **Logout >>** |	End session properly



Unittype: MDH863 (2.2.2) · Serialnumber: 18218630016064 · ●●●●○ · MB Connect Line Guest WLAN

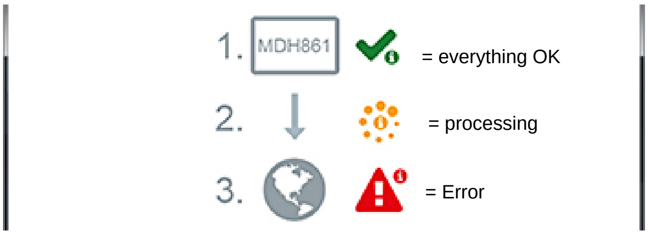
In the device status bar following information is displayed:

all device types	**Device type and (Firmware version)** - **Serial number**
MDH 861, MDH 862, MDH 865, MDH 866	additionally **Signal strength** (GSM) - **GSM network** - **Provider**
MDH 863, MDH 867	additionally **Signal strength** (WLAN) **- SSID**

Five Step Status Check

Here you can read out each step details. Click on the icon (right of each progress), shown as:

✓ green hook, ● orange circle, ▲ red triangle



11.8.2.1 Five Step Status Check

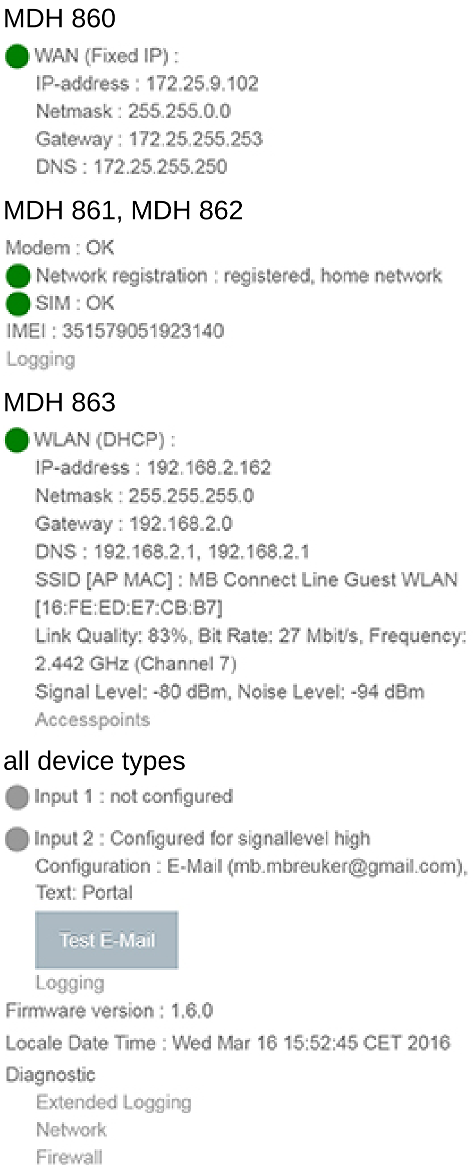
1. MDH863 ✓ Device

Here the device network settings and basic data is requested.

Input 1 can only be configured for establishing the connection. Is it configured accordingly, it is displayed here.
The state of the signal is shown with the prepended soft-LED (grey = 0/low, green = 1/high).

Input 2 can be used to send emails, SMS, Internet SMS or to start a reboot. Is it configured accordingly, it is displayed here.
The state of the signal is shown with the prepended soft-LED (grey = 0/low, green = 1/high).
If an email, SMS or Internet SMS has been configured, the button "Test" appears. Clicking this button will carry out a test on the setting.

Additional information can be obtained by clicking on the "**Logging**" or the "Diagnostic" link. These data help us to provide additional support when dealing with problems.



MDH 860

● WAN (Fixed IP) :
IP-address : 172.25.9.102
Netmask : 255.255.0.0
Gateway : 172.25.255.253
DNS : 172.25.255.250

MDH 861, MDH 862

Modem : OK
● Network registration : registered, home network
● SIM : OK
IMEI : 351579051923140
Logging

MDH 863

● WLAN (DHCP) :
IP-address : 192.168.2.162
Netmask : 255.255.255.0
Gateway : 192.168.2.0
DNS : 192.168.2.1, 192.168.2.1
SSID [AP MAC] : MB Connect Line Guest WLAN [16:FE:ED:E7:CB:B7]
Link Quality: 83%, Bit Rate: 27 Mbit/s, Frequency: 2.442 GHz (Channel 7)
Signal Level: -80 dBm, Noise Level: -94 dBm
Accesspoints

all device types

● Input 1 : not configured

● Input 2 : Configured for signallevel high
Configuration : E-Mail (mb.mbreuker@gmail.com), Text: Portal

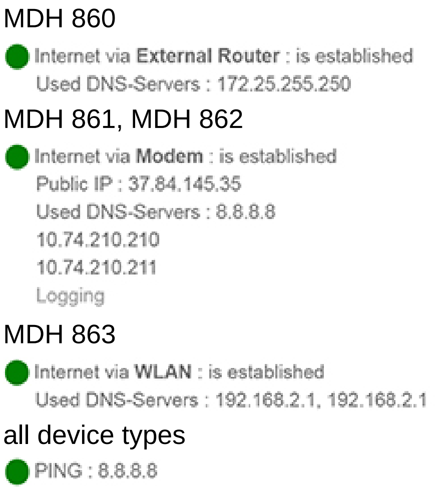
Logging
Firmware version : 1.6.0
Locale Date Time : Wed Mar 16 15:52:45 CET 2016
Diagnostic
Extended Logging
Network
Firewall

2. ↓ ✓ Connecting to the Internet

Here the connection is requested to the Internet and display the connection data.

Additional information can be obtained by clicking on the "**Logging"** link. These data help us to provide additional support when dealing with problems.

„PING:“ here the test server entered is displayed.
The LED signals the connectivity (grey = not pinged yet, green = available, red = not available).



MDH 860

● Internet via **External Router** : is established
Used DNS-Servers : 172.25.255.250

MDH 861, MDH 862

● Internet via **Modem** : is established
Public IP : 37.84.145.35
Used DNS-Servers : 8.8.8.8
10.74.210.210
10.74.210.211
Logging

MDH 863

● Internet via **WLAN** : is established
Used DNS-Servers : 192.168.2.1, 192.168.2.1

all device types

● PING : 8.8.8.8

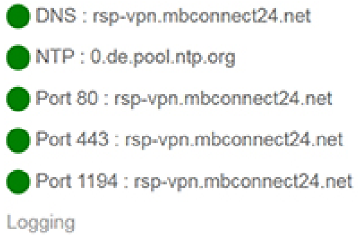
3. Availability of the Portal Server

Here the current accessibility of the Portal Server is requested and displayed the results.

DNS: Portal Server address
NTP: NTP time server (the NTP is checked only if it is enabled in the configuration).
Port 80/443/1194: At least one of the three ports is needed to establish the connection to the portal.

Additional information can be obtained by clicking on the "**Logging**" link. These data help us to provide additional support when dealing with problems.

all device types



● DNS : rsp-vpn.mbconnect24.net
● NTP : 0.de.pool.ntp.org
● Port 80 : rsp-vpn.mbconnect24.net
● Port 443 : rsp-vpn.mbconnect24.net
● Port 1194 : rsp-vpn.mbconnect24.net
Logging

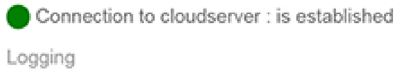
4. Connecting to the Portal Server

Here, the connection status to the Portal Server is requested and displayed.

Additional information can be obtained by clicking on the **"Logging"** link. These data help us to provide additional support when dealing with problems.

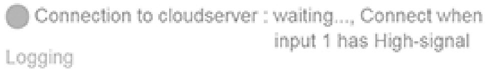
all device types

Connection is established



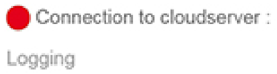
● Connection to cloudserver : is established
Logging

waiting for event for the connection



● Connection to cloudserver : waiting..., Connect when input 1 has High-signal
Logging

Error



● Connection to cloudserver :
Logging

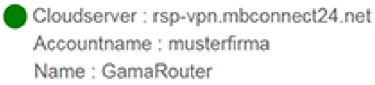
5. Information on the CTM, cloud server and user

Here, the following information is displayed:

all device types

Connection status to the Portal Server and Portal Address
Account name
Device name

Portal Server

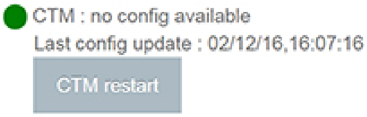


● Cloudserver : rsp-vpn.mbconnect24.net
Accountname : musterfirma
Name : GamaRouter

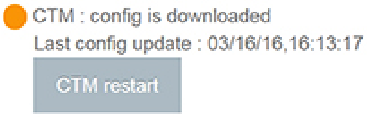
Information whether a portal configuration is available for download.

Date of the last update of the configuration.
(By clicking the button **CTM restart**, another request will start to look for a recent configuration.)

CTM / Synchronization status



● CTM : no config available
Last config update : 02/12/16,16:07:16



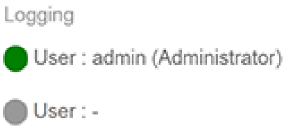
● CTM : config is downloaded
Last config update : 03/16/16,16:13:17

Additional information can be obtained by clicking on the "**Logging**" link. These data help us to provide additional support when dealing with problems.

The **User** who currently has an active VPN connection to this device.

If there is no active connection, this is indicated by a gray LED.

User



Logging

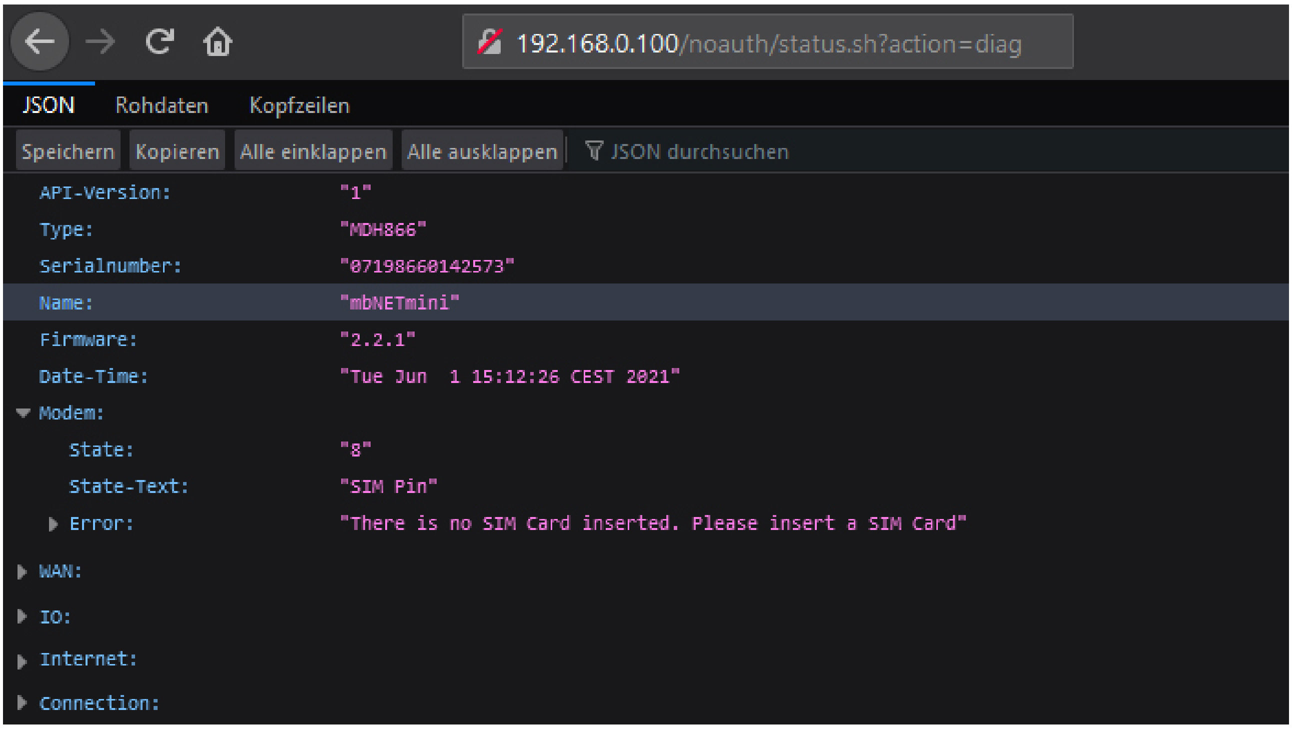
● User : admin (Administrator)

● User : -

11.8.2.2 API for status queries

As of FW V2.2.1, an API is available that can be used to call up basic information that is also available in the "Device State".

Since no sensitive information / data is output here, the call is made directly via the LAN-IP of the mbNET.mini: http: // [Router-IP] /noauth/status.sh?action=diag.

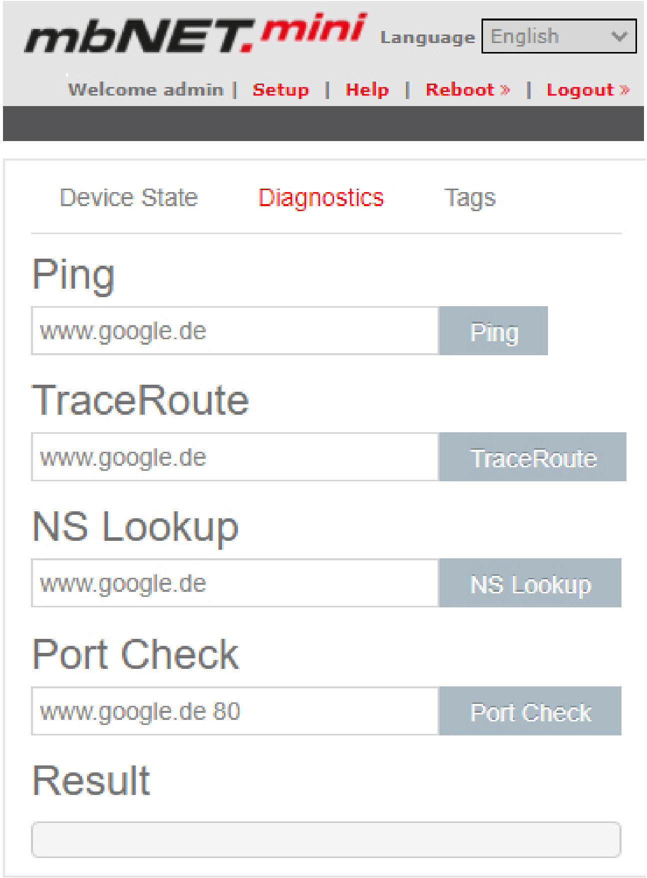


```
API-Version:          "1"
Type:                 "MDH866"
Serialnumber:         "07198660142573"
Name:                 "mbNETmini"
Firmware:             "2.2.1"
Date-Time:            "Tue Jun  1 15:12:26 CEST 2021"
▼ Modem:
    State:            "8"
    State-Text:       "SIM Pin"
  ▶ Error:            "There is no SIM Card inserted. Please insert a SIM Card"
▶ WAN:
▶ IO:
▶ Internet:
▶ Connection:
```

Image 4: Sample output

11.8.3 Diagnostics

In case of a failed connection setup, the diagnostic page supports for troubleshooting.



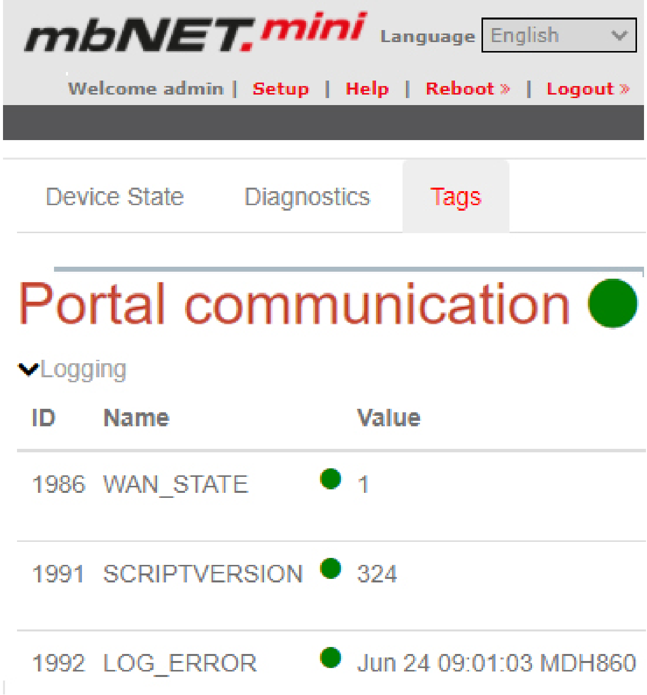
Ping	Here, it is possible to enter an internet page or an IP address. When actuating the "Ping" button, the ping command is executed. This ping command easily determines whether an internet communication exists or whether a specific computer is available.
TraceRoute	Here, it is possible to enter an internet page or an IP address. When actuating the "TraceRoute" button, the routing command is executed. This command starts a route tracing and visualizes it. This allows you to get much more information on a network connection.
NS Lookup	Check the function of the nameserver with the button "NS Lookup". There's no matter what kind of internet connection you have chosen.
Port Check	By entering the test address with an attached port, determine whether this port is enabled at the receiving end.
Result	In this box, the result of the respective function is displayed. **NOTICE** Please note that only one result is displayed from an action. Each action will overwrite the result of a previous query.

11.8.4 Tags

If the mbNET.mini has established a connection to the portal (indicated by the green LED symbol next to "Portal com-munication"), all available Tags for the portal are listed here.

In addition to the name of a Tag, its status (using the LED symbol*) and the respective Tag value are displayed.

* green LED symbol = data point can be read grey LED symbol = data point cannot be read



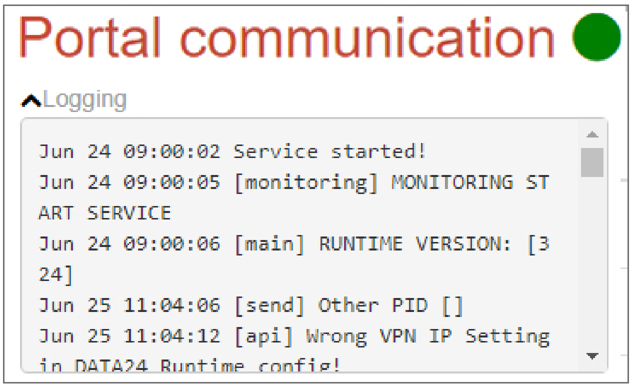
Portal communication ●

Logging

ID	Name		Value
1986	WAN_STATE	●	1
1991	SCRIPTVERSION	●	324
1992	LOG_ERROR	●	Jun 24 09:01:03 MDH860

Logging

In case of errors / difficulties, possible causes of errors can be detected by "Logging".
This data is for further support in case of problems or hints in our FAQ.



Portal communication ●

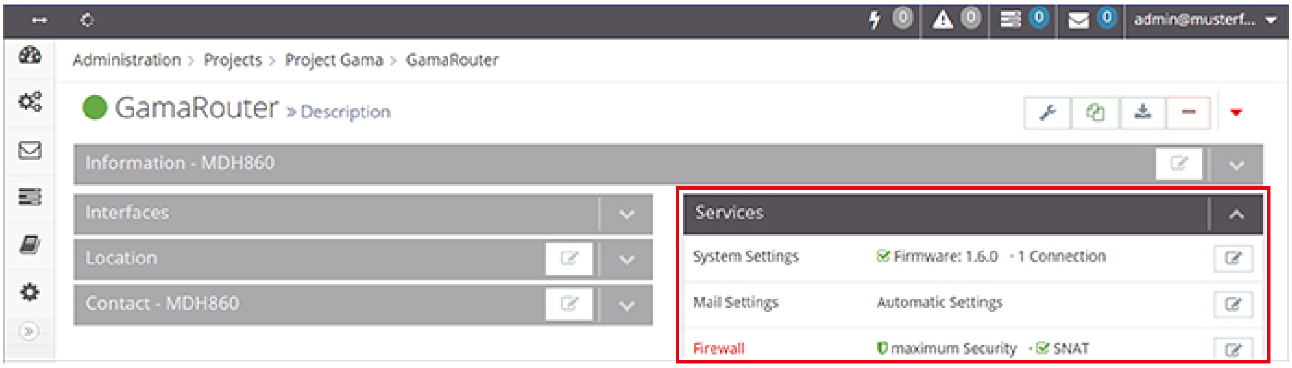
Logging

```
Jun 24 09:00:02 Service started!
Jun 24 09:00:05 [monitoring] MONITORING ST
ART SERVICE
Jun 24 09:00:06 [main] RUNTIME VERSION: [3
24]
Jun 25 11:04:06 [send] Other PID []
Jun 25 11:04:12 [api] Wrong VPN IP Setting
in DATA24 Runtime config!
```

12 Configuring your Router in the Remote Service Portal (V 2.x)

The router can be fully configured only by using the Remote Service Portal ***mbCONNECT24***.

Navigation: Administration > Projects > *Project Gama (selected project)* > *GamaRouter (selected device)* > Services



admin@musterf...

Administration > Projects > Project Gama > GamaRouter

GamaRouter » Description

Information - MDH860

Interfaces

Location

Contact - MDH860

Services

System Settings	☑ Firmware: 1.6.0 · 1 Connection
Mail Settings	Automatic Settings
Firewall	maximum Security · ☑ SNAT

In the menu item **Services**, the following settings can be made.

System Settings - setting the period of time for the device to reboot and starting the firmware update.

Mail Settings - **a)** Mail server of the portal, with fixed specifications or **b)** own SMTP server.

Firewall - define the global settings of the firewall security (security levels of the firewall) and create the firewall rules.

Digital I/O - define I/O 1 and I/O 2 - independently of one another - as a digital input or output.

Alarmmanagement - configuring a digital input and / or a digital output.

VPN - selection of a VPN port and a VPN gateway.

User Administration - change the password for access to the device interface of the mbNET.mini.

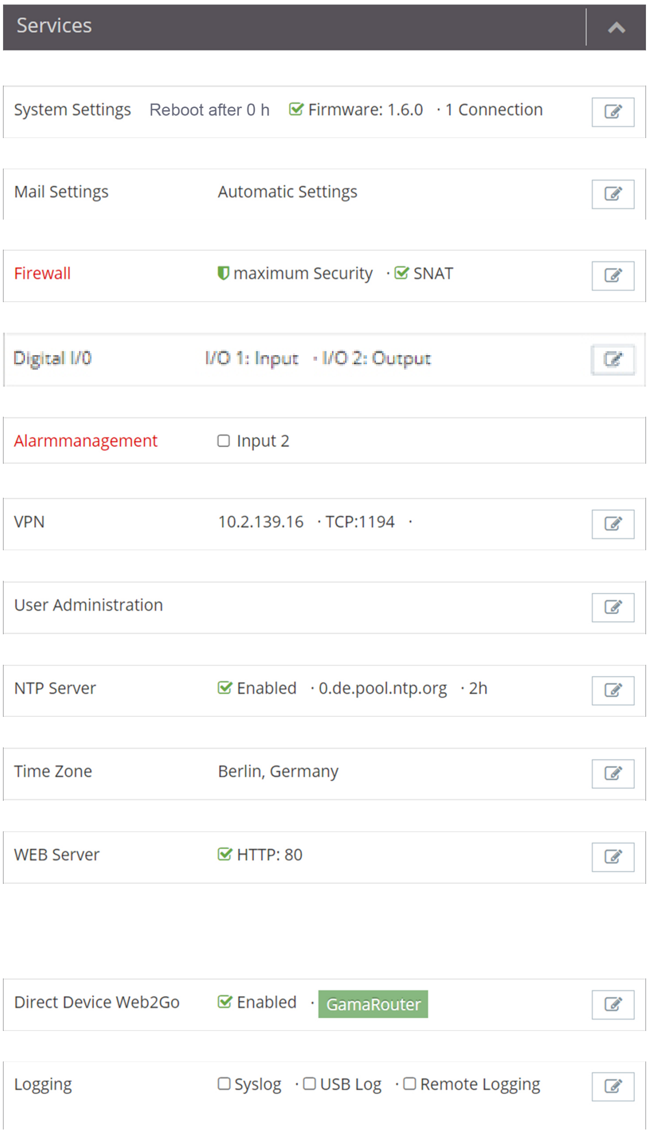
NTP Server - specify the NTP server and time span for automatic time synchronization.

Time Zone - **a)** Entry of standard time and date and **b)** Selection of the time zone.

WEB Server - **a)** Selection of the connection type (HTTP or HTTPS) for access to the web server,
b) change the default port and
c) Block / enable manufacturer web service.

Direct Device Web2go- activate / deactivate direct access via Web2go to the device's web interface.

Logging - set the logging options.



Services

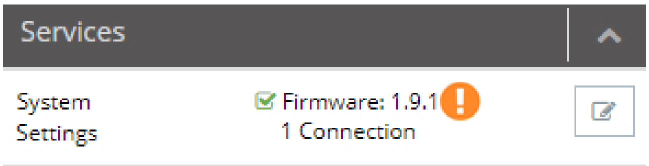
System Settings	Reboot after 0 h · ☑ Firmware: 1.6.0 · 1 Connection
Mail Settings	Automatic Settings
Firewall	maximum Security · ☑ SNAT
Digital I/0	I/O 1: Input · I/O 2: Output
Alarmmanagement	□ Input 2
VPN	10.2.139.16 · TCP:1194 ·
User Administration	
NTP Server	☑ Enabled · 0.de.pool.ntp.org · 2h
Time Zone	Berlin, Germany
WEB Server	☑ HTTP: 80
Direct Device Web2Go	☑ Enabled · GamaRouter
Logging	□ Syslog · □ USB Log · □ Remote Logging

12.1 System Settings

Navigation: Administration > Projects > *Project Gama* (*selected project*) > *GamaRouter (selected device)* > Services > System Settings

The overview shows

- After which time the device is to perform a reboot automatically
- The currently installed firmware version, with a note of its actuality



Services

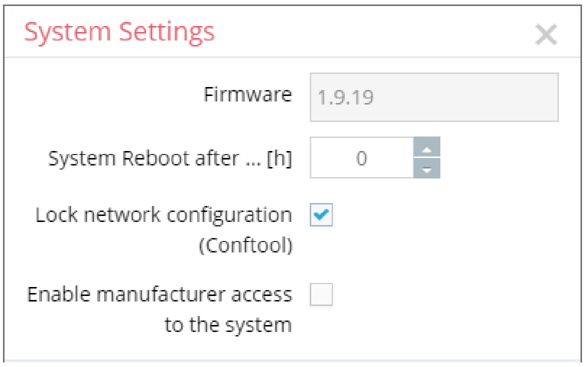
System Settings ✓ Firmware: 1.9.1❗ 1 Connection

NOTICE

The orange LED ❗ is displayed when a newer firmware version is available.

By clicking on the LED symbol an automatic firmware update is performed.

To change the settings, click on the Edit button ✎



System Settings

Firmware: 1.9.19

System Reboot after ... [h]: 0

Lock network configuration (Conftool) ☑

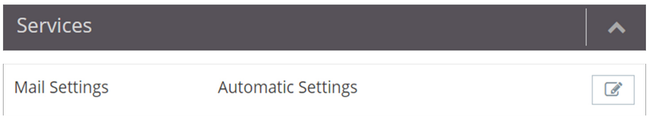
Enable manufacturer access to the system □

<table>
<tr><th>Designation</th><th>Description</th></tr>
<tr><td><b>Firmware</b></td><td>Display of the firmware currently installed on the device.</td></tr>
<tr><td><b>System Reboot after ... [h]</b></td><td>Enter a period of time (in hours), after which the device performs an automatic reboot.</td></tr>
<tr><td colspan="2"><b>NOTICE</b>
The time interval is not linear to the operating time of the router, but counts every full hour. That is, if you enter 2 hours, a device reboot is performed every second hour.
<b>Exception:</b> If you enter <b>24 hours</b>, the device is rebooted <b>every time at 00:00</b>.</td></tr>
<tr><td><b>Lock network configuration (Conftool)</b></td><td><b>NOTICE</b>
If this function is activated, the method to transfer the configuration to the device "Submit to Device" is disabled.</td></tr>
<tr><td><b>Enable manufacturer access to the system</b></td><td>Activate this feature if you want the device manufacturer to have access to the devices system settings (for example, in the case of support).</td></tr>
</table>

12.2 Mail Settings

Navigation: Administration > Projects > *Project Gama (selected project)* > *GamaRouter (selected device)* > Services > Mail Settings

In the Mail Settings, you can choose whether the device should use the mail server of the portal with fixed specifications or whether you use your own SMTP server.

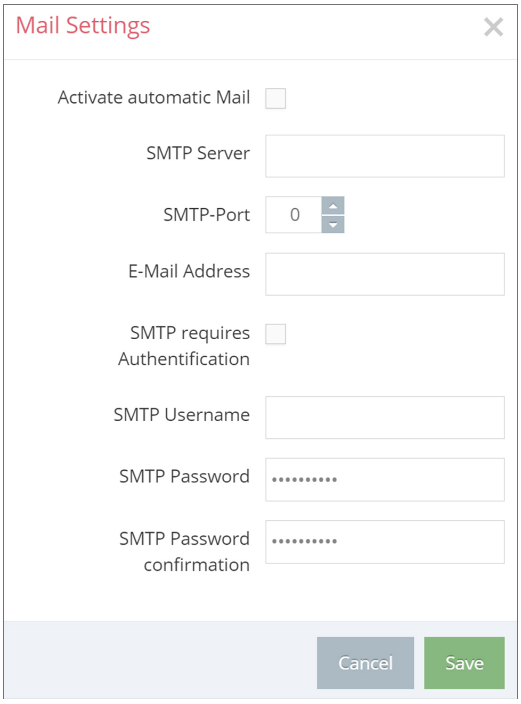


Services

Mail Settings Automatic Settings

To change the settings, click on the Edit button

Designation	Description
Activate automatic Mail	Checkbox to enable / disable the automatic mail settings.
SMTP Server	The SMTP server is required for the device to be able to send e-mails (you can obtain more detailed information on this from your service provider).
SMTP-Port	Enter the port used to send e-mails (usually port 25).
E-Mail Address	Enter the e-mail address to serve as the sending address.
SMTP requires Authentification	Checkbox for whether the selected SMTP server requires authentication.
SMTP Username	Enter the username required for authentication on the SMTP server.
SMTP Password	Enter the password for authentification.
SMTP Password confirmation	Repeat the entered password.



Mail Settings

Activate automatic Mail □

SMTP Server

SMTP-Port 0

E-Mail Address

SMTP requires Authentification □

SMTP Username

SMTP Password ••••••••••

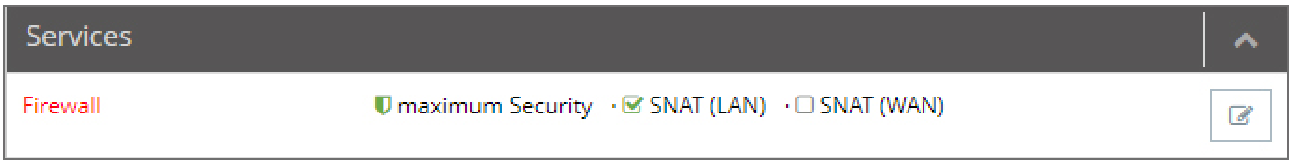
SMTP Password confirmation ••••••••••

NOTICE

Changes in the portal, which concern the device, will take effect after the Portal configuration has been transferred to the device.
If the device configuration is out of date, this is indicated by a gray LED symbol before the device name ● ◐ GamaRouter.

12.3 Firewall

Navigation: Administration > Projects > *Project Gama (selected project)* > *GamaRouter (selected device)* > Services > Firewall



Services

Firewall maximum Security · ☑ SNAT (LAN) · □ SNAT (WAN)

Here you

- define the global firewall settings (firewall security levels)

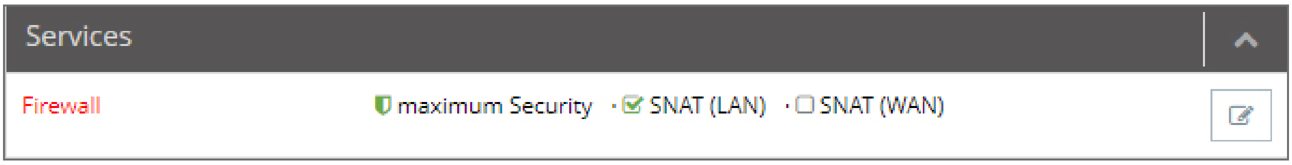
  - therefor click on the edit icon

- create firewall rules and manage them

  - therefor click on "Firewall"

12.3.1 Global Firewall Settings

Navigation: Administration > Projects > ProjectAlpha (*selected project*) > RouterAlpha (*selected device*) > Services > Firewall

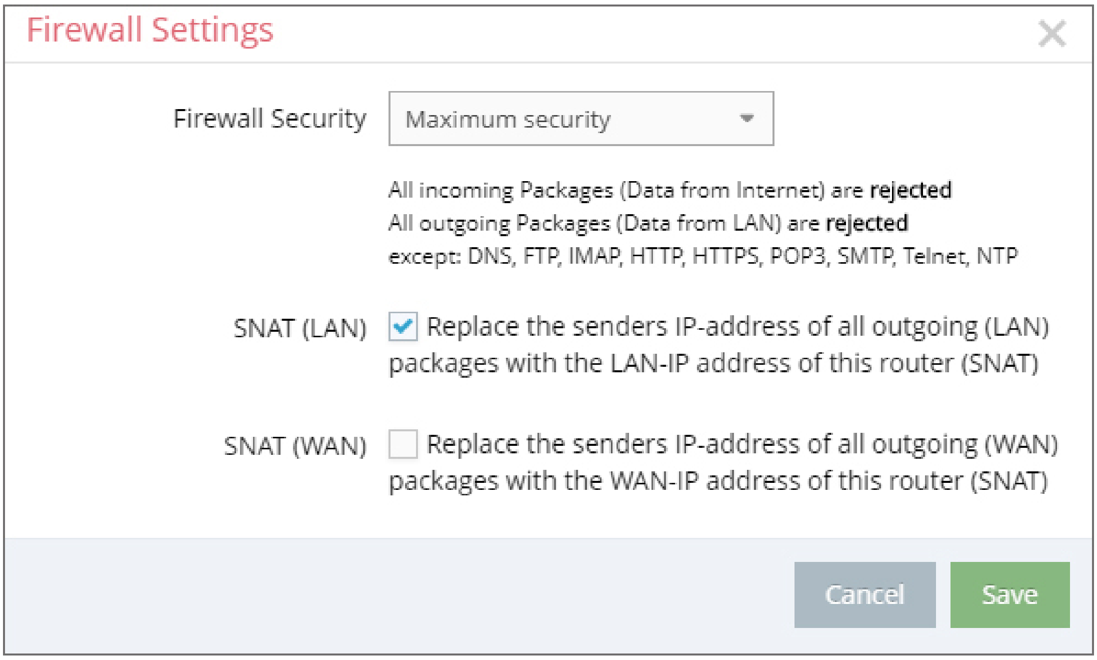


Services

Firewall maximum Security · ☑ SNAT (LAN) · □ SNAT (WAN)

Here, you can specify the global settings for Firewall security (Firewall Security Levels).

Clicking the Edit button takes you to the global Firewall settings.



Firewall Settings

Firewall Security: 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

SNAT (LAN): ☑ Replace the senders IP-address of all outgoing (LAN) packages with the LAN-IP address of this router (SNAT)

SNAT (WAN): □ Replace the senders IP-address of all outgoing (WAN) packages with the WAN-IP address of this router (SNAT)

Firewall Security	
Maximum security	All incoming packages (data from the Internet) are **rejected**. All outgoing packages (data from the LAN) are **rejected** except: DNS, FTP, IMAP, HTTP, HTTPS, POP3, SMTP, Telnet, NTP
Normal security	All incoming packages (data from the Internet) are **rejected**. All outgoing packages (data from the LAN) are **accepted**.
Minimum security	All incoming packages (data from the Internet) are **accepted**. All outgoing packages (data from the LAN) are **accepted**.
Firewall off	All incoming Packages (Data from Internet and WAN ethernet) are **accepted.** All outgoing Packages (Data from LAN) are **accepted.** Routing between all interfaces is on. * For devices without a WAN Ethernet interface, this is only "Data from Internet".

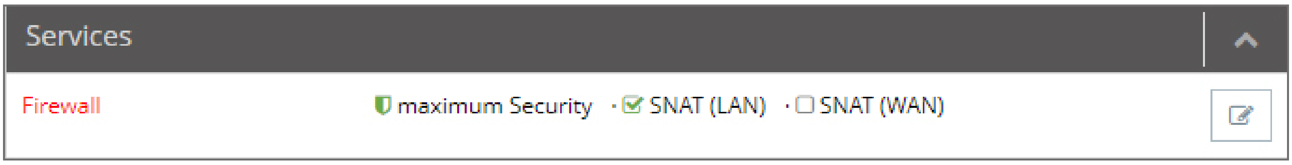
NOTICE

The **Minimum security** and the **Firewall off** option should only be set temporarily for test purposes, since it allows all data traffic from inside to outside the network, as well as access from outside the network.
This setting puts the integrity of your device and the connected components at risk!

SNAT (LAN)	Checkbox for activating/deactivating this function. This function forwards the incoming data traffic from Internet or VPN connections transparently to the LAN network. Thus, all the data packages going to the LAN have the IP address of the device as the sender address. This means that none of the LAN subscribers needs the device as a "gateway". This is a considerable advantage when integrating remote maintenance into existing network structures as it means that these structures do not need to be changed.
SNAT (WAN)	Checkbox for activating/deactivating this function. If this checkbox is activated, incoming traffic from LAN participants is transparently forwarded to the WAN network. This means that all data packets sent to the WAN receive the sender address as the WAN IP address of the router.

12.3.2 Firewall Rules

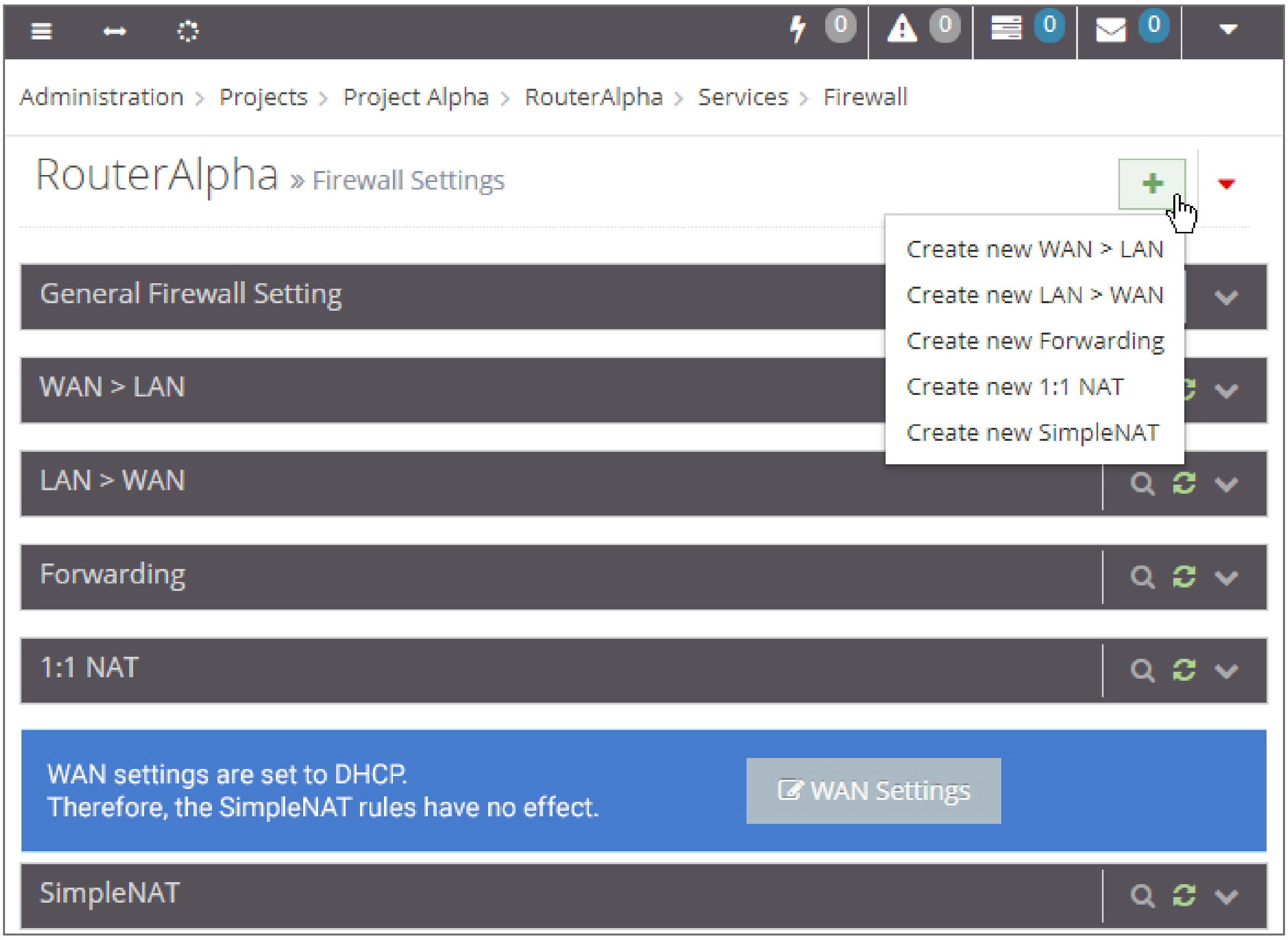
Navigation: Administration > Projects > ProjectAlpha (*selected project*) > RouterAlpha (*selected device*) > Services > Firewall



Services

Firewall · maximum Security · ☑ SNAT (LAN) · □ SNAT (WAN)

Here, you can create Firewall rules, change existing rules or delete them.
The Firewall link takes you to the menu for creating and editing individual Firewall rules.



Administration > Projects > Project Alpha > RouterAlpha > Services > Firewall

RouterAlpha » Firewall Settings

WAN settings are set to DHCP.
Therefore, the SimpleNAT rules have no effect.

You can add new rules using the Add button +

Create new **WAN > LAN**

Create new **LAN > WAN**

Create new **Forwarding**

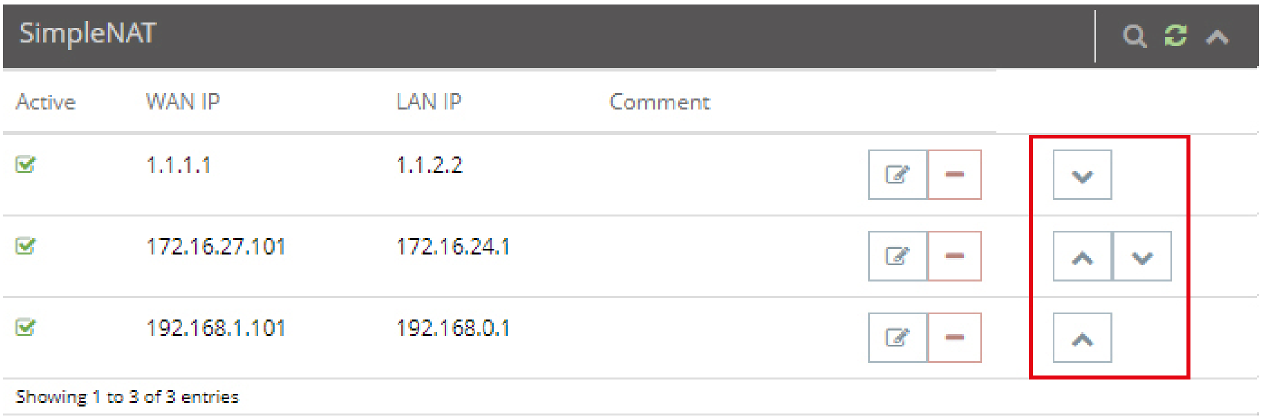
Create new **1:1 NAT**

Create new **SimpleNAT**

NOTICE

The following applies to all created rules:

Several rules can be sorted according to the order of their execution.
The rules are processed from top to bottom.



SimpleNAT

Active	WAN IP	LAN IP	Comment
✓	1.1.1.1	1.1.2.2	
✓	172.16.27.101	172.16.24.1	
✓	192.168.1.101	192.168.0.1	

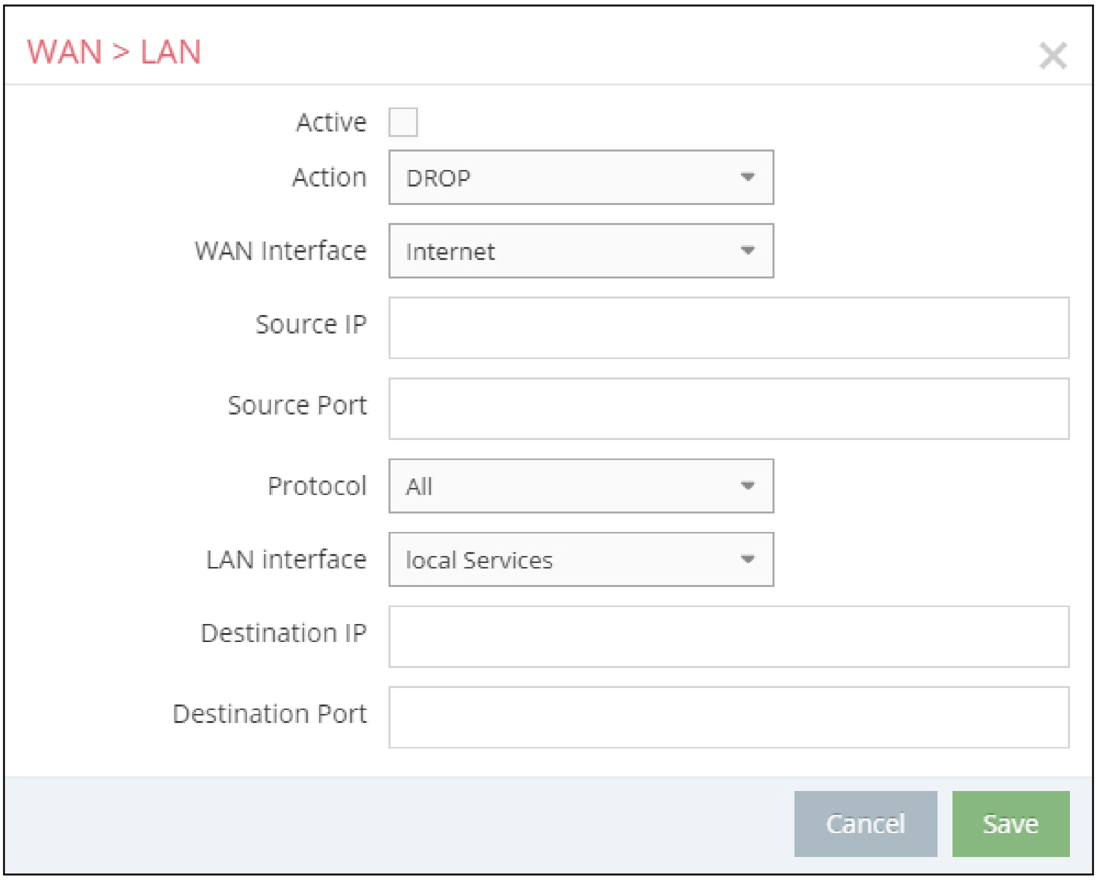
Showing 1 to 3 of 3 entries

Image 5: Sample rules

12.3.2.1 Firewall Settings - Create new WAN > LAN

Navigation: Administration > Projects > *ProjektAlpha (selected project)* > *RouterAlpha (selected device)* > Services > Firewall

This setting governs the incoming data traffic, i.e. the following settings only apply to data traffic arriving from outside the network.



WAN > LAN

Active	□
Action	DROP
WAN Interface	Internet
Source IP	
Source Port	
Protocol	All
LAN interface	local Services
Destination IP	
Destination Port	

Image 6: Depending on the device and type, individual display / selection fields may vary.

“WAN” is always the currently active interface with the Internet as far as the mbNET firewall is concerned. The following rule is determined by the setting under **„Administration > Projects > *ProjektAlpha (selected projekt)* > *RouterAlpha (selected device)* > Internet settings“**:

Internetconnection:

External Router
Here the WAN Ethernet is the interface to the Internet. The firewall therefore checks the data traffic from WAN Ethernet to LAN Ethernet.

Modem
The modem is the interface with the Internet here. The firewall therefore checks the data traffic from the modem to the LAN Ethernet. All data traffic on the WAN Ethernet interface is denied with this setting.

WAN > LAN	
Active	Checkbox for activating / deactivating this rule.
Action	The following options are available for selection: • **DROP** If this option is selected, it means that no data packets can pass and the packets are also deleted immediately. The sender is not notified about the whereabouts of the data packets. • **REJECT** If this option is selected, the data packets are rejected. The sender is notified that the data packets have been rejected. • **ACCEPT** If this option is selected, the data packets can pass.
WAN Interface	This setting defines the WAN interface to which the rule is to be applied. • **Internet** • **WAN Ethernet** • **OpenVPN** • **All**
Source IP	Here, enter the IP addresses for whose incoming data packets one of the set actions is to be executed. If you leave the field blank, the set action applies to all IP addresses (only on the selected interface).
Source Port	Enter the ports via which the data packets arrive here.
Protocol	The following options are available for selection: • **All** - the set rule applies to all protocols. • **TCP** - the set rule only applies to the TCP protocol. • **UDP -** the set rule only applies to the UDP protocol. • **ICMP** - the set rule only applies to the ICMP protocol.
LAN interface	Use this selection field to specify the LAN interface to which the rule is to be applied. You can choose from: • **local Services** • **LAN ethernet** • **All**
Destination IP	Enter the IP addresses to which the data packets are to be forwarded here.
Destination Port	Enter the ports via which the data packets are forwarded here.

WAN > LAN

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!

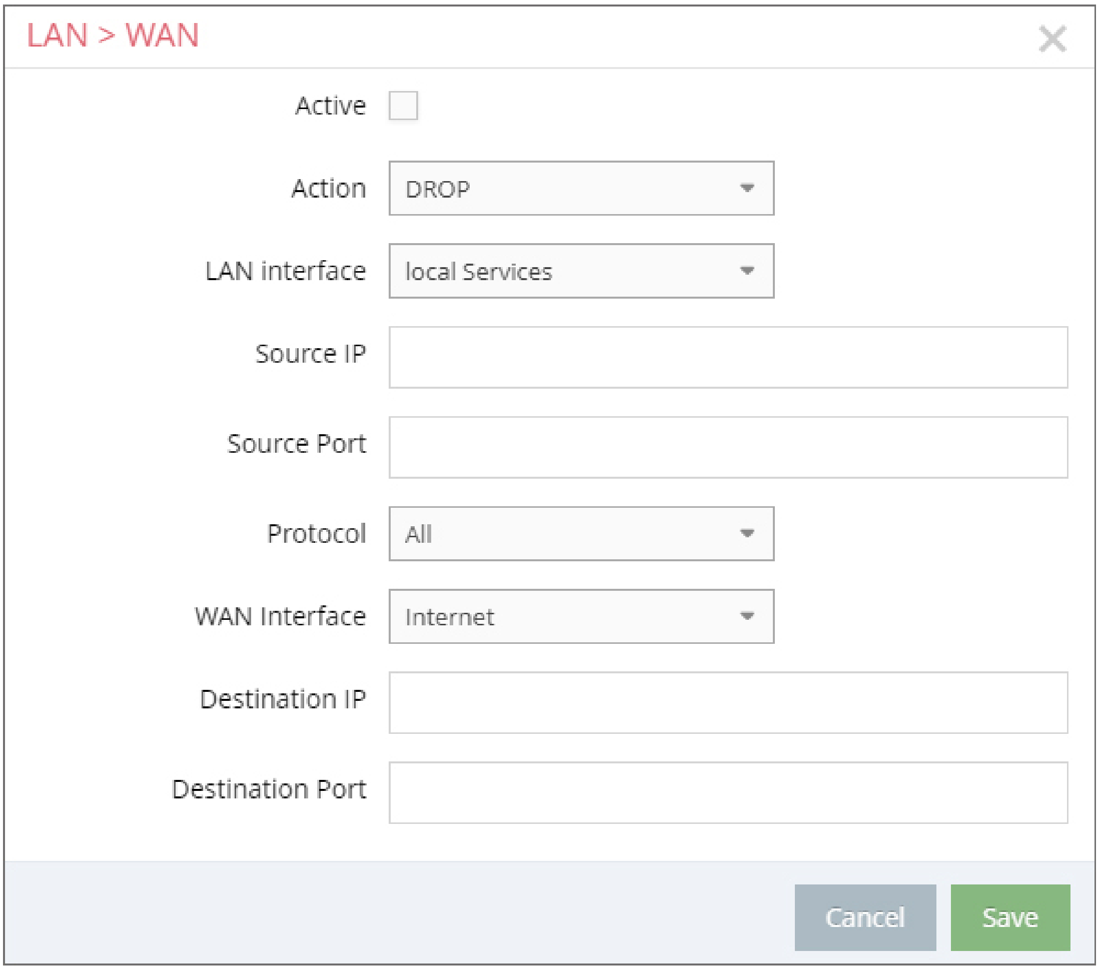
NOTICE

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.

12.3.2.2 Firewall Settings - Create new LAN > WAN

Navigation: Administration > Projects > *ProjektAlpha (selected project)* > *RouterAlpha (selected device)* > Services > Firewall

This setting governs the outgoing data traffic, i.e. the following settings only apply to outgoing data traffic.



LAN > WAN

Active	□
Action	DROP
LAN interface	local Services
Source IP	
Source Port	
Protocol	All
WAN Interface	Internet
Destination IP	
Destination Port	

Image 7: Depending on the device and type, individual display / selection fields may vary.

WAN > LAN	
Active	Checkbox for activating / deactivating this rule.
Action	The following options are available for selection: • **DROP** If this option is selected, it means that no data packets can pass and the packets are also deleted immediately. The sender is not notified about the whereabouts of the data packets. • **REJECT** If this option is selected, the data packets are rejected. The sender is notified that the data packets have been rejected. • **ACCEPT** If this option is selected, the data packets can pass.

WAN > LAN	
LAN interface	Use this selection field to specify the LAN interface to which the rule is to be applied. You can choose from: • **local Services** • **LAN ethernet** • **All**
Source IP	Here, enter the IP addresses for whose incoming data packets one of the set actions is to be executed. If you leave the field blank, the set action applies to all IP addresses (only on the selected interface).
Source Port	Enter the ports via which the data packets arrive here.
Protocol	The following options are available for selection: • **All** - the set rule applies to all protocols. • **TCP** - the set rule only applies to the TCP protocol. • **UDP** - the set rule only applies to the UDP protocol. • **ICMP** - the set rule only applies to the ICMP protocol.
WAN interface	This setting defines the WAN interface to which the rule is to be applied. • **Internet** • **WAN Ethernet** • **OpenVPN** • **All**
Destination IP	Enter the IP addresses to which the data packets are to be forwarded here.
Destination Port	Enter the ports via which the data packets are forwarded here.

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!

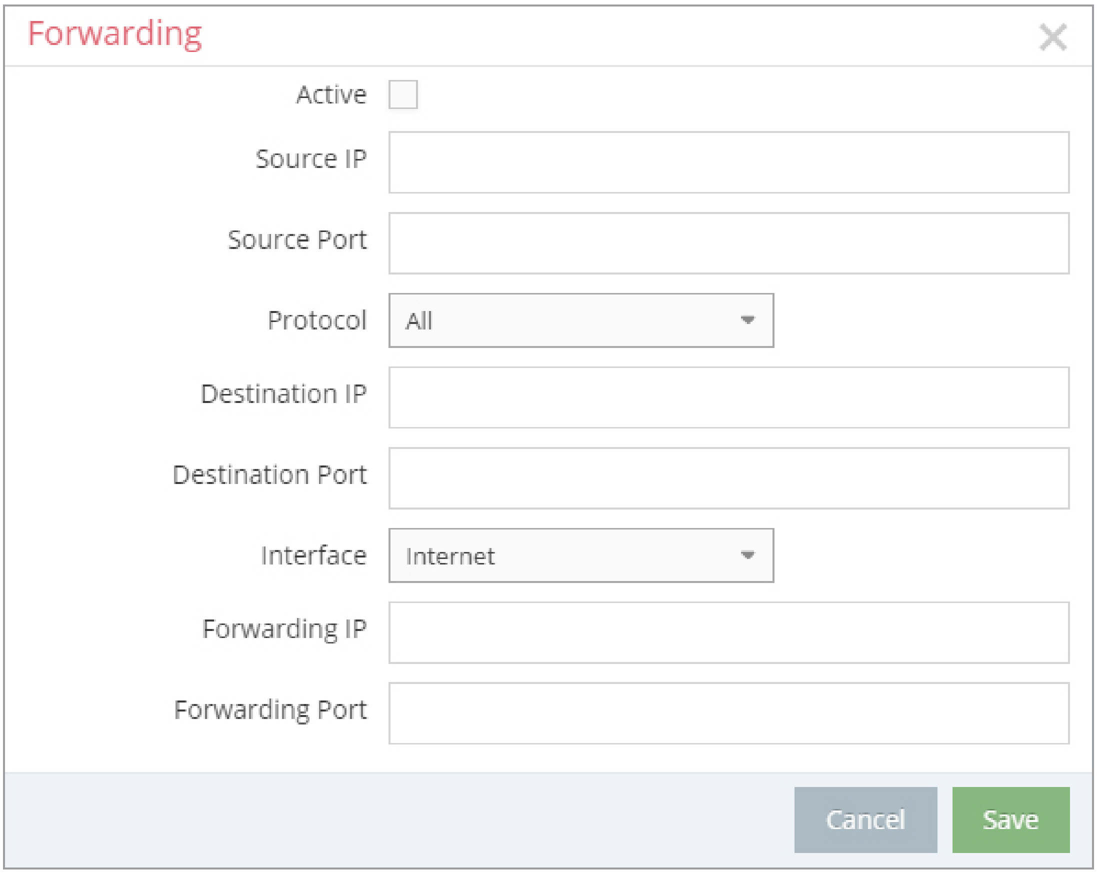
NOTICE

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.

12.3.2.3 Firewall Settings - Create new Forwarding

Navigation: Administration > Projects > *ProjektAlpha (selected project)* > *RouterAlpha (selected device)* > Services > Firewall

This setting is forwarding requests from specific IP addresses and ports to defined IP addresses and ports.



Forwarding

Active	□
Source IP	
Source Port	
Protocol	All
Destination IP	
Destination Port	
Interface	Internet
Forwarding IP	
Forwarding Port	

Image 8: Depending on the device and type, individual display / selection fields may vary.

Forwarding	
Active	Checkbox for activating / deactivating this rule.
Source IP	You can enter the IP addresses from which data packets are received here. If an entry is made here, only packets from these addresses are forwarded.
Source Port	You can specify the ports via which the data packets arrive here. If an entry is made here, only packets specifically sent via this port are forwarded.
Protocol	The following options are available for selection: • **All** - the set rule applies to all protocols. • **TCP** - the set rule only applies to the TCP protocol. • **UDP** - the set rule only applies to the UDP protocol. • **ICMP** - the set rule only applies to the ICMP protocol.
Destination IP	Enter the IP addresses to which the data packets were originally to be sent here.
Destination Port	Specify the ports via which the data packets are sent to the destination IP here.

Forwarding	
Interface	Use this selection field to specify the interface to which the forwarding is to be applied. You can choose from: • **Internet** • **WAN Ethernet** • **OpenVPN** • **All**
Forwarding IP	Enter the IP to which the data packets are actually to be sent here.
Forwarding Port	Specify the port via which the data packets are actually forwarded here.

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!

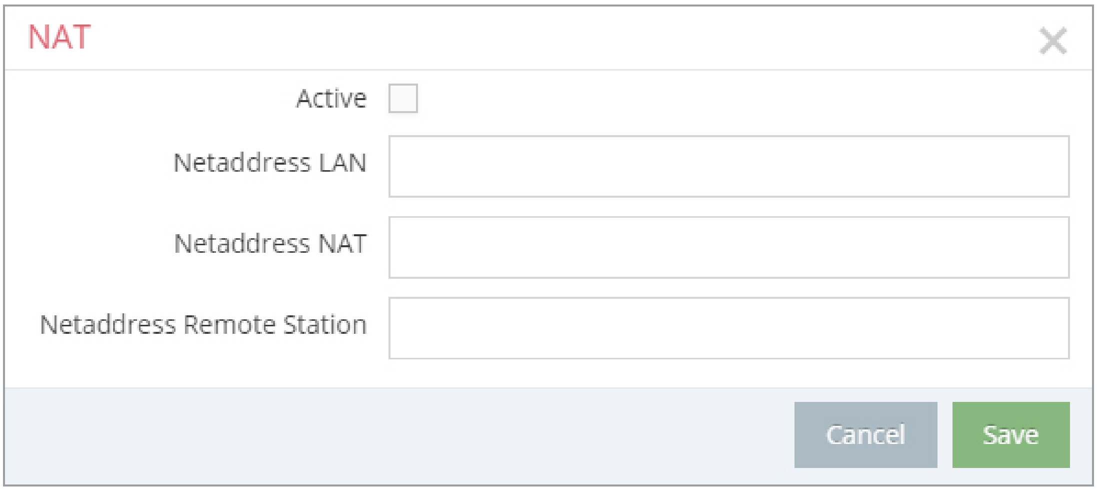
NOTICE

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.

12.3.2.4 Firewall Einstellungen - Create new 1:1 NAT

Navigation: Administration > Projects > *ProjektAlpha (selected project)* > *RouterAlpha (selected device)* > Services > Firewall

This setting enables two networks in the same address range to be connected. If, for example, a network with the address 192.168.0.0/24 is to be connected to a net-work with the same address, this is only possible if one of the two networks is assigned another address. NAT technology is an easy way of achieving this since only the real network address (LAN address) and the substitute address (NAT network address) are required. The NAT algorithm makes sure that the addresses in the data packets are only substituted in communications between these two networks. This means that you do not have to adapt your entire network addressing scheme.



NAT

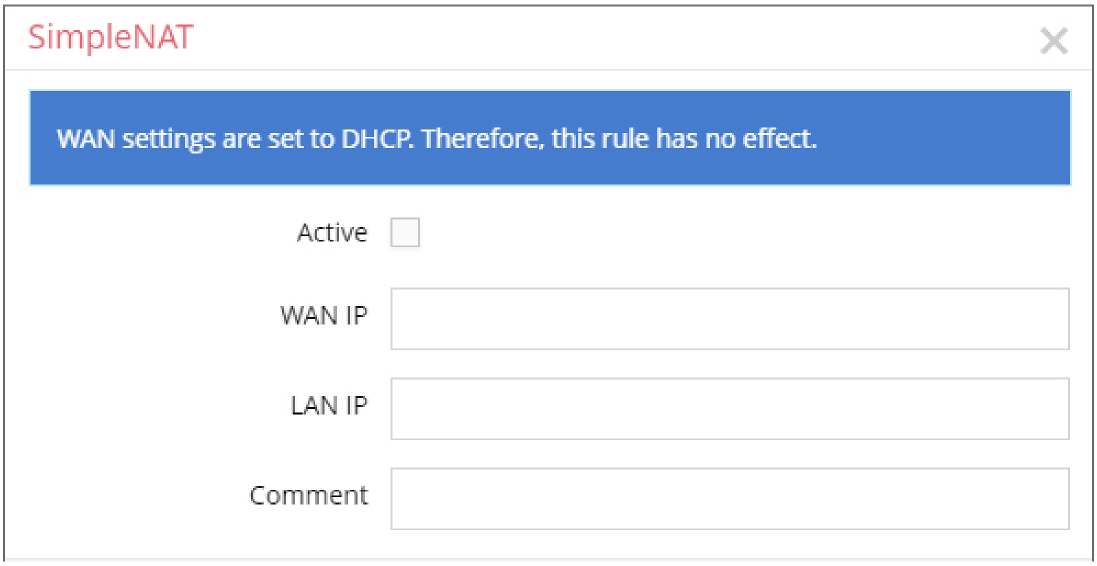
Active	□
Netaddress LAN	
Netaddress NAT	
Netaddress Remote Station	

1:1 NAT	
Active	Checkbox zum Aktivieren/Deaktivieren der Funktion.
Netaddress LAN	Enter the real address of the network here (e.g.192.168.0.0/24). **Note that the IP address must be entered in CIDR notation.**
Netaddress NAT	Enter the translated address of your network here (e.g. 192.168.1.0/24). **Note that the IP address must be entered in CIDR notation.**
Netaddress Remote Station	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.

12.3.2.5 Firewall Einstellungen - Create new SimpleNAT

Navigation: Administration > Projects > *ProjektAlpha (selected project)* > *RouterAlpha (selected device)* > Services > Firewall

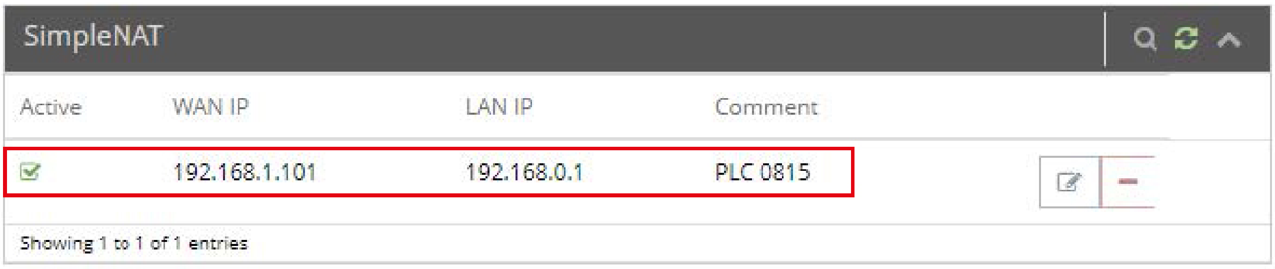
SimpleNAT is about making an IP from the LAN network 1:1 accessible in the WAN Ethernet network. For this purpose, a free WAN Ethernet address from the WAN network is entered as WAN IP. This IP address is then added in addition to the WAN interface and is mapped directly to the registered LAN IP "1:1". I. e. the IP from the WAN reaches directly the IP of the LAN. This has the advantage that you do not have to forward ports etc.



SimpleNAT

WAN settings are set to DHCP. Therefore, this rule has no effect.

Active	□
WAN IP	
LAN IP	
Comment	



SimpleNAT

Active	WAN IP	LAN IP	Comment
☑	192.168.1.101	192.168.0.1	PLC 0815

Showing 1 to 1 of 1 entries

Image 9: SimpleNAT-example rule

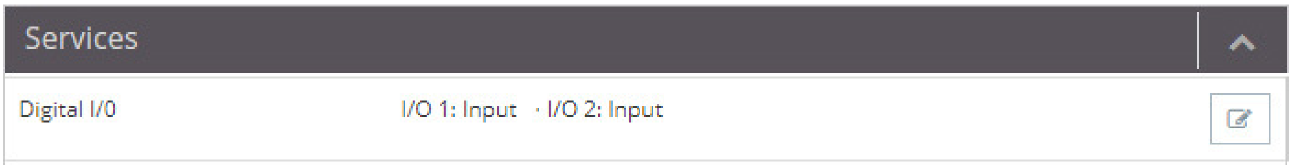
SimpleNAT	
Active	Checkbox zum Aktivieren/Deaktivieren der Funktion.
WAN IP	Enter here a free WAN ethernet address from the WAN network (e.g., 192.168.1.101).
LAN IP	Enter the LAN IP address that you want to reach (e.g., 192.168.0.1).
Comment	Here you can enter a comment about this rule.

NOTICE

The WAN settings must not be set to DHCP. Otherwise, the rule has no effect.

12.4 Digital I/O

Navigation: Administration > Projects > *Project Gama (selected project)* > *GamaRouter (selected device)* > Services > Digital I/O



Services

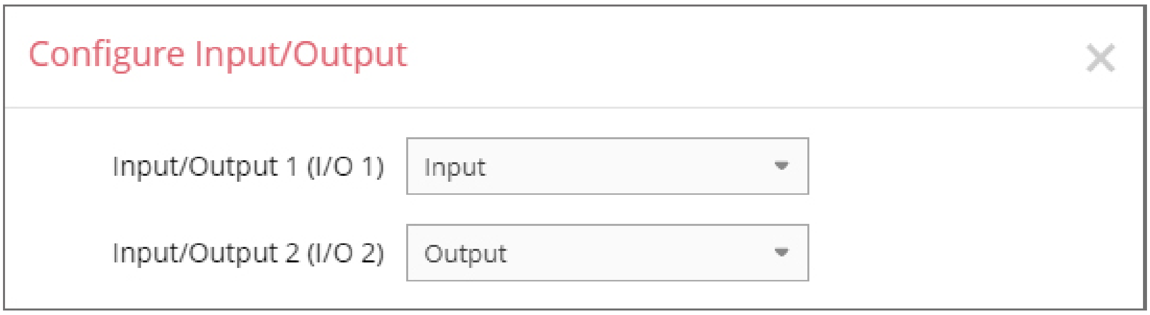
Digital I/0	I/O 1: Input · I/O 2: Input	

NOTICE

The **Digital I/O** menu is only available after the device has been logged into the portal (online).

Under Digital I/O you can define I/O 1 and I/O 2 - independently of each other - as a digital input or output.

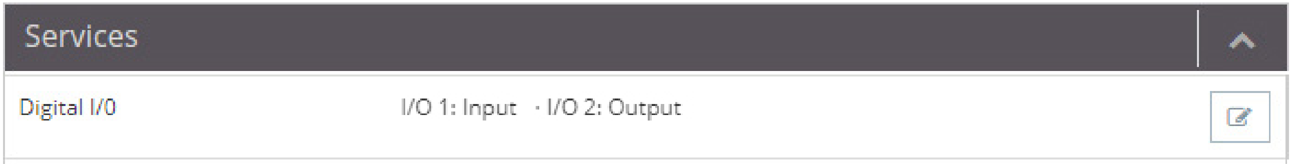
Configure Input/Output =>



Configure Input/Output

Input/Output 1 (I/O 1): Input

Input/Output 2 (I/O 2): Output

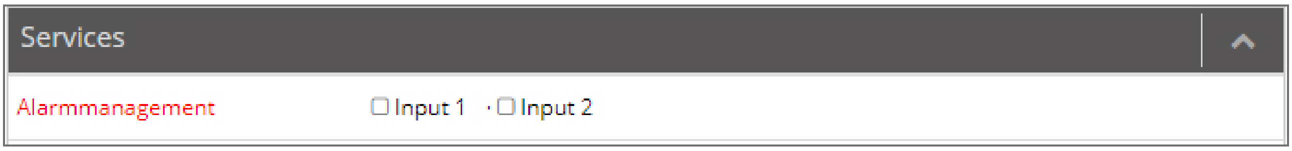


Services

Digital I/0	I/O 1: Input · I/O 2: Output	

NOTICE

The defined I/Os are configured using the alarm management.



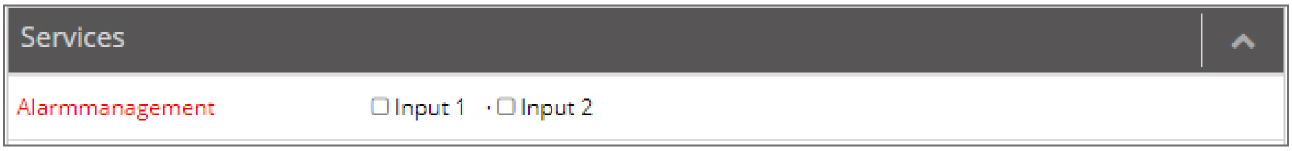
Services

Alarmmanagement	☐ Input 1 · ☐ Input 2

Click on the link "Alarmmanagement" to get to the configuration menu.

12.5 Alarm management

Navigation: Administration > Projects > *Project Gama (selected project)* > *GamaRouter (selected device)* Services > Alarmmanagement



Both I / O 1 and 2 can be configured independently of each other as either a digital input or a digital output.

The alarm management of the mbNET.mini provides the following functions:

- Status query (1 or 0) of an I/O configured as input with the option:
  - Sending an e-mail, an SMS *, an Internet SMS *
  - Perform a device restart

* with the SMS action up to three numbers can be stored. Multiple numbers are entered without spaces but separated by commas (123456,234567,345678).

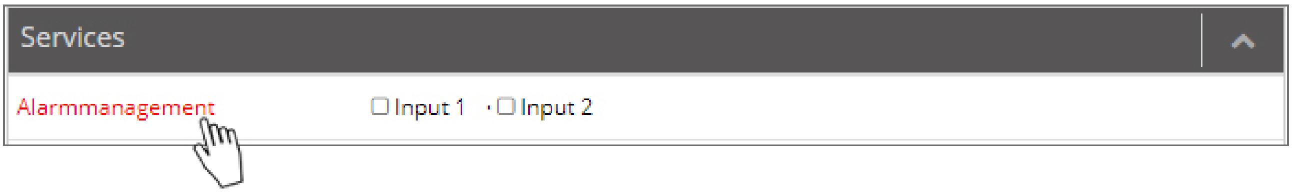
- Switching an I/O configured as an output for certain events:
  - Off
  - On by internetconnection
  - On by any VPN-connection
  - On by any active User-Cloudserver-connection

NOTICE

By default, the I/Os are defined as digital inputs.

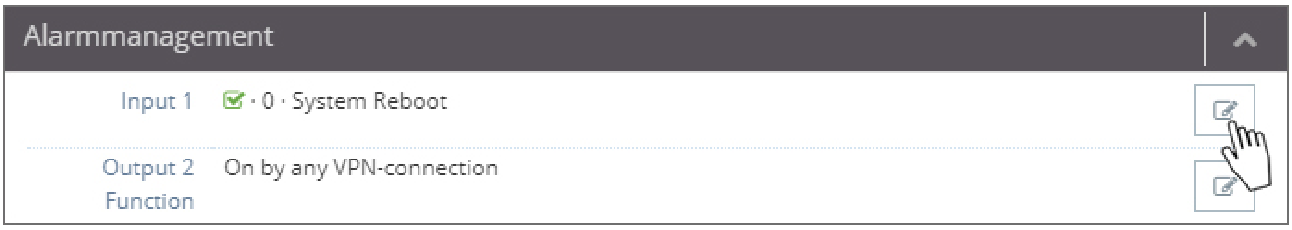
NOTICE

In the menu "Services > Digital I/O" you can define I/O 1 and I/O 2 - independently of one another - as digital input or digital output.



Click on the link "Alarmmanagement" to get to the configuration menu.

12.5.1 Functions for a digital input



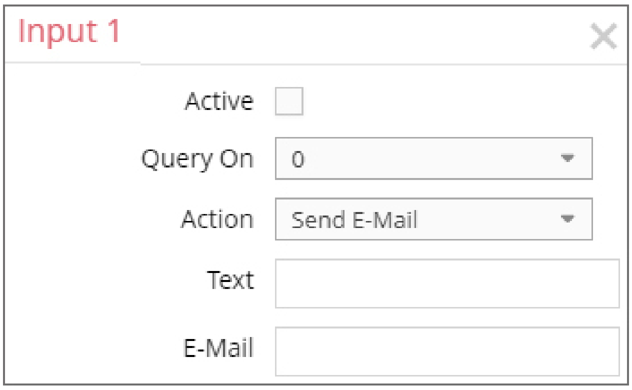
Alarmmanagement

Input 1 ✓ · 0 · System Reboot

Output 2 Function On by any VPN-connection

Click on the edit symbol ✎ to configure the function of a digital input.

- Send E-Mail
- System Reboot
- SMS/Internet-SMS



Input 1

Active	□
Query On	0
Action	Send E-Mail
Text	
E-Mail	

Designation	Description
Active	Checkbox to activate / deactivate the function.
Query On	Here, set the query state (0 or 1) at which an action should be taken.
Action	Select an action from the drop-down list (Send E-Mail, System Reboot, SMS or Internet SMS).
Text	Enter a message text here.
E-Mail	In the action selection "Send E-Mail" enter the recipient's e-mail address here.
SMS*	In the "SMS" action option, enter the number of the recipient here.
Internet-SMS*	In the "Internet-SMS" action option, enter the number of the recipient here.

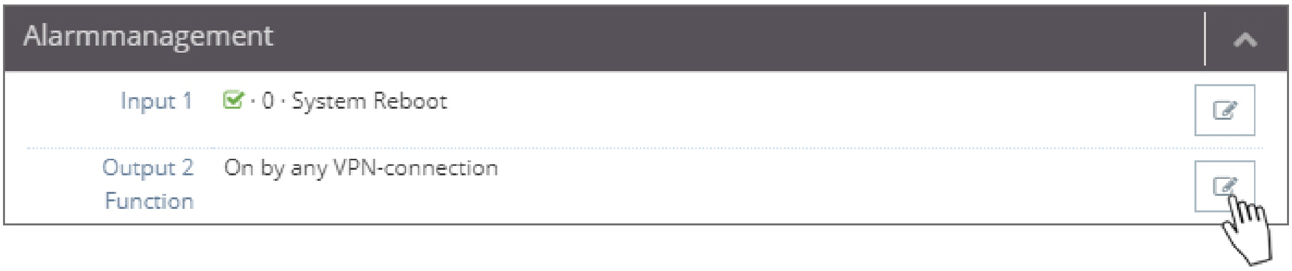
* with the SMS action up to 5 numbers can be stored. Multiple numbers are entered without spaces but separated by commas (123456,234567,345678).

NOTICE

Changes in the portal, which concern the device, will take effect after the Portal configuration has been transferred to the device.

If the device configuration is out of date, this is indicated by a gray LED symbol before the device name ● ⓘ GamaRouter.

12.5.2 Functions for a digital output

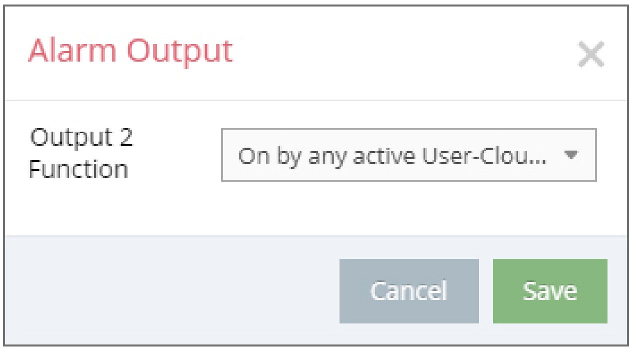


Alarmmanagement

Input 1 ✓ · 0 · System Reboot

Output 2 Function On by any VPN-connection

Click on the edit symbol 📝 to configure the function of a digital ouput.



Alarm Output

Output 2 Function: On by any active User-Clou...

To switch a digital output, the following actions are available:

- Off
- On by Internetconnection
- On by any VPN-connection
- On by any active User-Cloudserver-connection

- **Off**:
  Select this setting if you do not want to evaluate the output for possible switching operations.
- **On by Internetconnection**:
  Select this setting if the digital output of the device is to be set to 1 in the event of an active Internet connection.
  For example, an active Internet connection can then be indicated by an LED connected at output.
- **On by any VPN-connection**: Select this setting if the digital output of the device is to be set to 1 in the event of an active VPN connection. For example, the connection to the portal can then be indicated by a lamp connected at output.
- **On by any active User-Cloudserver-connection:**
  Select this setting if the digital output of the device is to be set to 1 in the event of an active User-Cloudserver-connection. For example, the connection to the portal can then be indicated by a lamp connected at output.

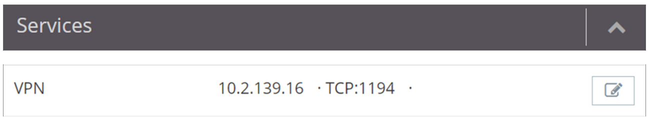
NOTICE

Changes in the portal, which concern the device, will take effect after the Portal configuration has been transferred to the device.
If the device configuration is out of date, this is indicated by a gray LED symbol before the device name ● ◐ GamaRouter.

12.6 VPN

Navigation: Administration > Projects > *Project Gama (selected project)* > *GamaRouter (selected device)* > Services > VPN

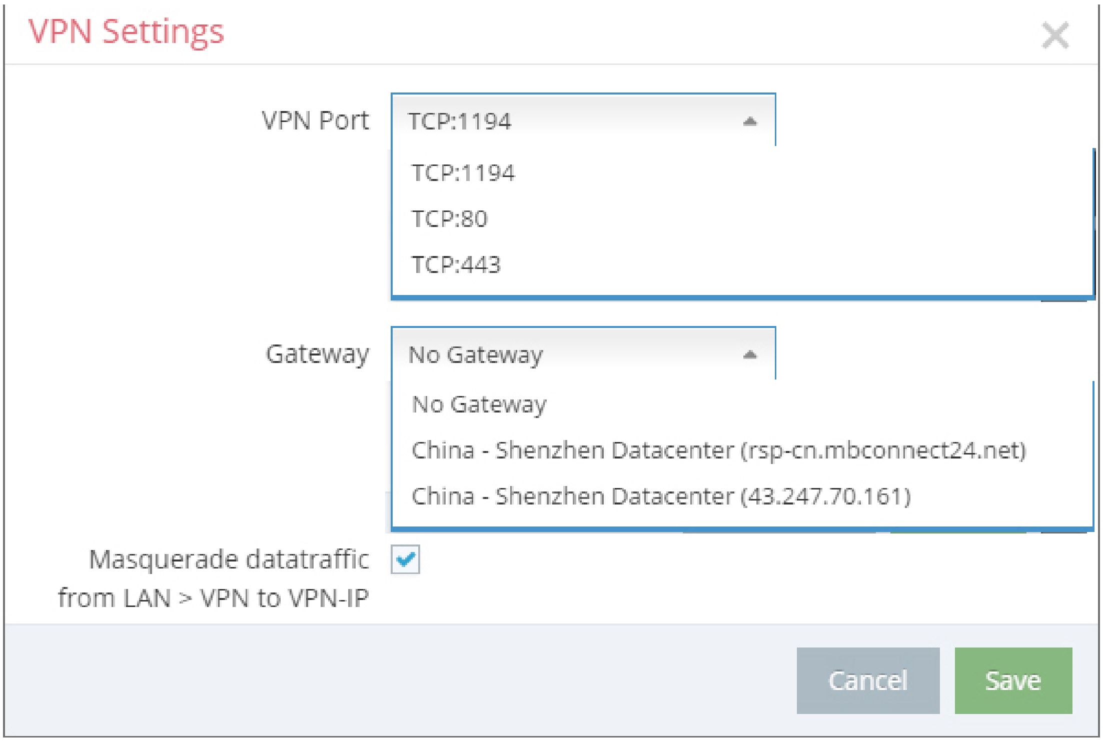
In the VPN settings, you can select a VPN port and, if necessary, a VPN gateway and activate the "Masquerade" function.



Services

VPN 10.2.139.16 · TCP:1194 ·

To change the settings, click on the Edit button



VPN Settings

VPN Port: TCP:1194
- TCP:1194
- TCP:80
- TCP:443

Gateway: No Gateway
- No Gateway
- China - Shenzhen Datacenter (rsp-cn.mbconnect24.net)
- China - Shenzhen Datacenter (43.247.70.161)

Masquerade datatraffic from LAN > VPN to VPN-IP ☑

VPN Port	Here you can select a vacant VPN port but make sure that this port is enabled in the firewall.
Gateway	Here, select a VPN Gateway (DNS name or IP).
Masquerade datatraffic from LAN > VPN to VPN-IP	Checkbox for activating / deactivating the "Masquerade" function. The Masquerade feature allows the implementation of multiple private IP addresses with only one public IP address.

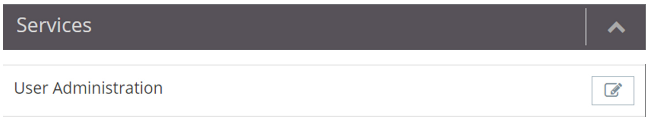
NOTICE

Changes in the portal, which concern the device, will take effect after the Portal configuration has been transferred to the device.
If the device configuration is out of date, this is indicated by a gray LED symbol before the device name ● ⓘ GamaRouter.

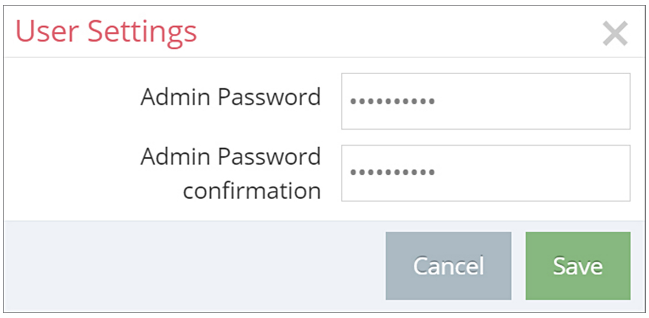
12.7 User Administration

Navigation: Administration > Projects > *Project Gama (selected project)* > *GamaRouter (selected device)* > Services> User Administration

Here you can change the password for accessing the device web interface.



To change the settings, click on the Edit button



Admin Password ••••••••••

Admin Password confirmation ••••••••••

Admin Password	Enter your new password.
Admin Password confirmation	Repeat your entry.

NOTICE

- Define rules for the use of equipment and assigning passwords.
- Regularly change the passwords to increase security.
- Always use passwords with high strength password. Avoid weak passwords such as "password1", "123456789" or the like.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- Never use one password for different users and systems.

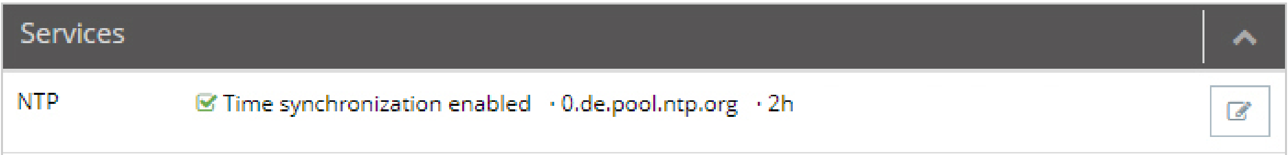
NOTICE

Changes in the portal, which concern the device, will take effect after the Portal configuration has been transferred to the device.
If the device configuration is out of date, this is indicated by a gray LED symbol before the device name ● ⓘ GamaRouter.

12.8 NTP

Navigation: Administration > Projects > *Project Gama* (*selected project*) > *GamaRouter (selected device)* > Services > NTP

The Network Time Protocol (NTP) is a standard for synchronizing clocks in computer systems via package-based communication networks.
The automatic time calibration takes place via an NTP server (preset address: 0.de.pool.ntp.org).



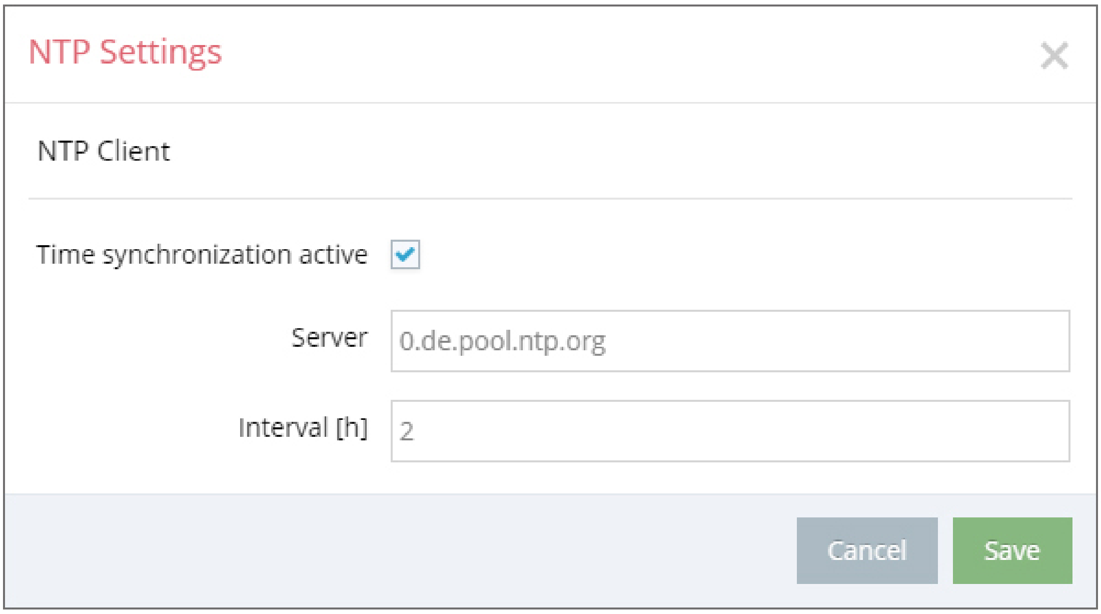
Services

NTP ☑ Time synchronization enabled · 0.de.pool.ntp.org · 2h

The overview shows:

- Whether the NTP function is activated
- The set NTP server (0.de.pool.ntp.org)
- The polling interval in hours (2 hrs)

To change the settings, click on the Edit button



NTP Settings

NTP Client

Time synchronization active ☑

Server 0.de.pool.ntp.org

Interval [h] 2

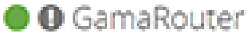
Time synchronization active	Checkbox for activating/deactivating the NTP function.
Server	Enter the NTP server here (preset address: 0.de.pool.ntp.org). You can enter a time server IP address instead of a name. If you enter a name, there must be a DNS server entered in the network settings, or an existing Internet connection. The NTP server simply needs to be available.

Interval [h]	Enter the value (in hours) for the NTP polling interval here. Input => natural numbers [h] > 0.

NOTICE

If you leave this blank or enter "0", there will be no time calibration.

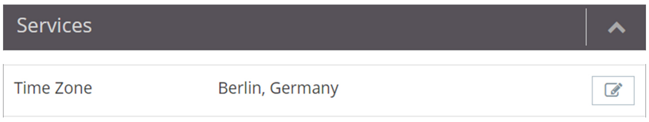
NOTICE

Changes in the portal, which concern the device, will take effect after the Portal configuration has been transferred to the device.
If the device configuration is out of date, this is indicated by a gray LED symbol before the device name .

12.9 Time Zone

Navigation: Administration > Projects > *Project Gama (selected project)* > *GamaRouter (selected device)* > Services > Time Zone

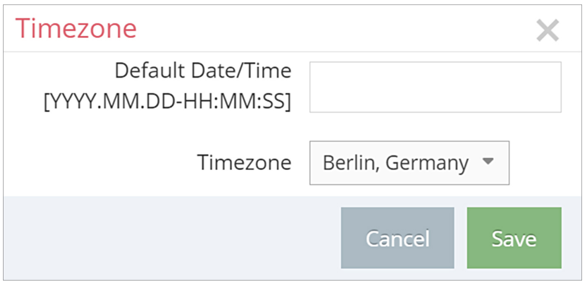
Here you enter the standard time and the de- fault date and select the time zone.



Time Zone	Berlin, Germany	

To change the settings, click on the Edit button ●

Standard date/time [YYYY.MM.DD-HH:M-M:SS]	Input of the date/time in the UTC format YYYY.MM.DD-HH:MM:SS (2015.03.06-19:23:48).
Timezone	Selection field for the time zone in which the device is located.



Default Date/Time [YYYY.MM.DD-HH:MM:SS]:

Timezone: Berlin, Germany

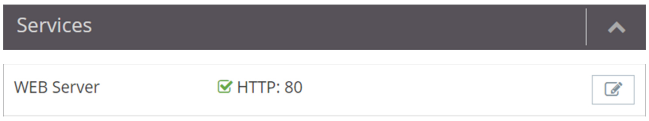
NOTICE

Changes in the portal, which concern the device, will take effect after the Portal configuration has been transferred to the device.
If the device configuration is out of date, this is indicated by a gray LED symbol before the device name ● ● GamaRouter.

12.10 Web Server

Navigation: Administration > Projects > *Project Gama (selected project)* > *GamaRouter (selected project)* > Services > Web Server

In the Web Server settings you select the connection type (HTTP or HTTPS) how you want to access the Web server, and if necessary, change the default port.

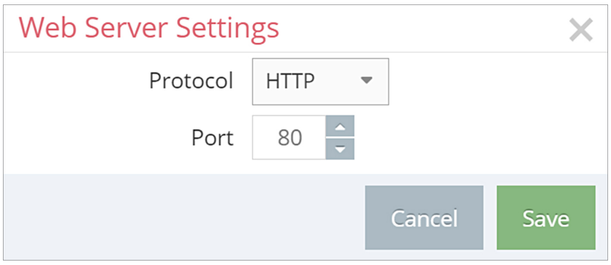


Services

WEB Server ☑ HTTP: 80

To change the settings, click on the Edit button ✎

Protocol	Selection field for the connection type with which you wish to access the web server. - HTTP (with preset standard port: 80) - HTTPS (with preset standard port: 443)
Port	If necessary, the standard port can be changed here.



Web Server Settings

Protocol: HTTP

Port: 80

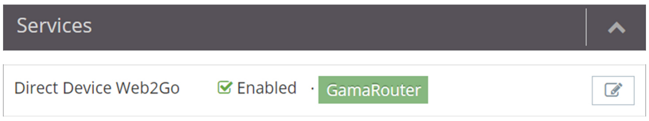
NOTICE

Changes in the portal, which concern the device, will take effect after the Portal configuration has been transferred to the device.
If the device configuration is out of date, this is indicated by a gray LED symbol before the device name ● ! GamaRouter.

12.11 Direct Device Web2go

Navigation: Administration > Projects > *Project Gama (selected project) > GamaRouter (selected device)* > Services > Direct Device Web2go

Using this function, you can access the web interface of the device directly by clicking the green button.



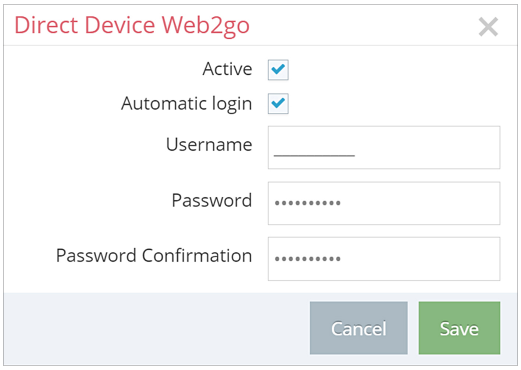
Services

Direct Device Web2Go ☑ Enabled · GamaRouter

To change the settings, click on the Edit button

Designation	Description
Active	Checkbox for activating/deactivating direct access to the web interface of the device.
Automatic login	Checkbox for activating/deactivating the automatic login to the web interface of the device.
Username	Enter the username for authentication on the device.
Password	Enter the corresponding password.
Password Confirmation	Repeat the password.

If all the parameters have been entered correctly, this will take you to the web interface of the device directly and without polling the access data.



Direct Device Web2go

Active ☑

Automatic login ☑

Username ________

Password ••••••••••

Password Confirmation ••••••••••

NOTICE

Changes in the portal, which concern the device, will take effect after the Portal configuration has been transferred to the device.

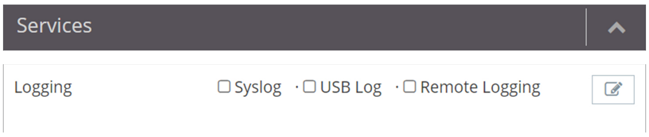
If the device configuration is out of date, this is indicated by a gray LED symbol before the device name ● ❗ GamaRouter.

12.12 Logging

Navigation: Administration > Projects > *Project Gama (selected project)* > *GamaRouter (selected device)* > Services > Logging

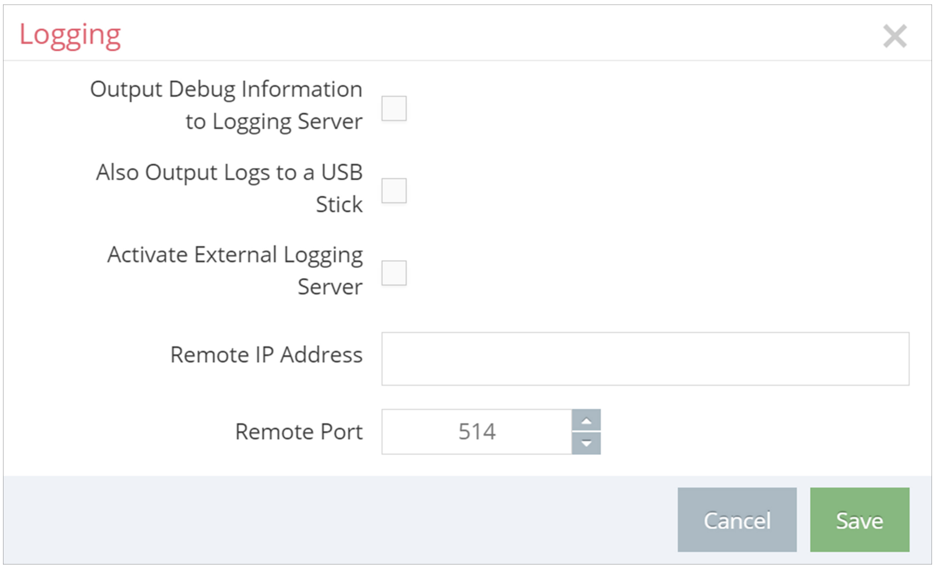
Here you define the logging options.

To change the settings, click on the Edit button



Services

Logging □ Syslog · □ USB Log · □ Remote Logging



Logging

Output Debug Information to Logging Server □

Also Output Logs to a USB Stick □

Activate External Logging Server □

Remote IP Address

Remote Port 514

Designation	Description
Output Debug Information to Logging Server	Checkbox for activating/deactivating Debug mode for various logging functions. This function allows extended logging.
Also Output Logs to a USB Stick	Checkbox for activating/deactivating the additional output of the logging. This is output solely to the USB stick that is connected to the device (file name of the logging file: "Device name.log").
Activate External Logging Server	Checkbox for activating/deactivating the additional output of the system logging. Using an external logging server, the device system logging can be can be outsourced to another computer.
Remote IP Address	Enter the IP address of the external logging server here.
Remote Port	Enter the port of the external logging server here. Port 514 is preset here. We recommend that you do not change this port, unless you are using a certain application that reacts to a different port.

NOTICE

Changes in the portal, which concern the device, will take effect after the Portal configuration has been transferred to the device.
If the device configuration is out of date, this is indicated by a gray LED symbol before the device name ● ◐ GamaRouter.

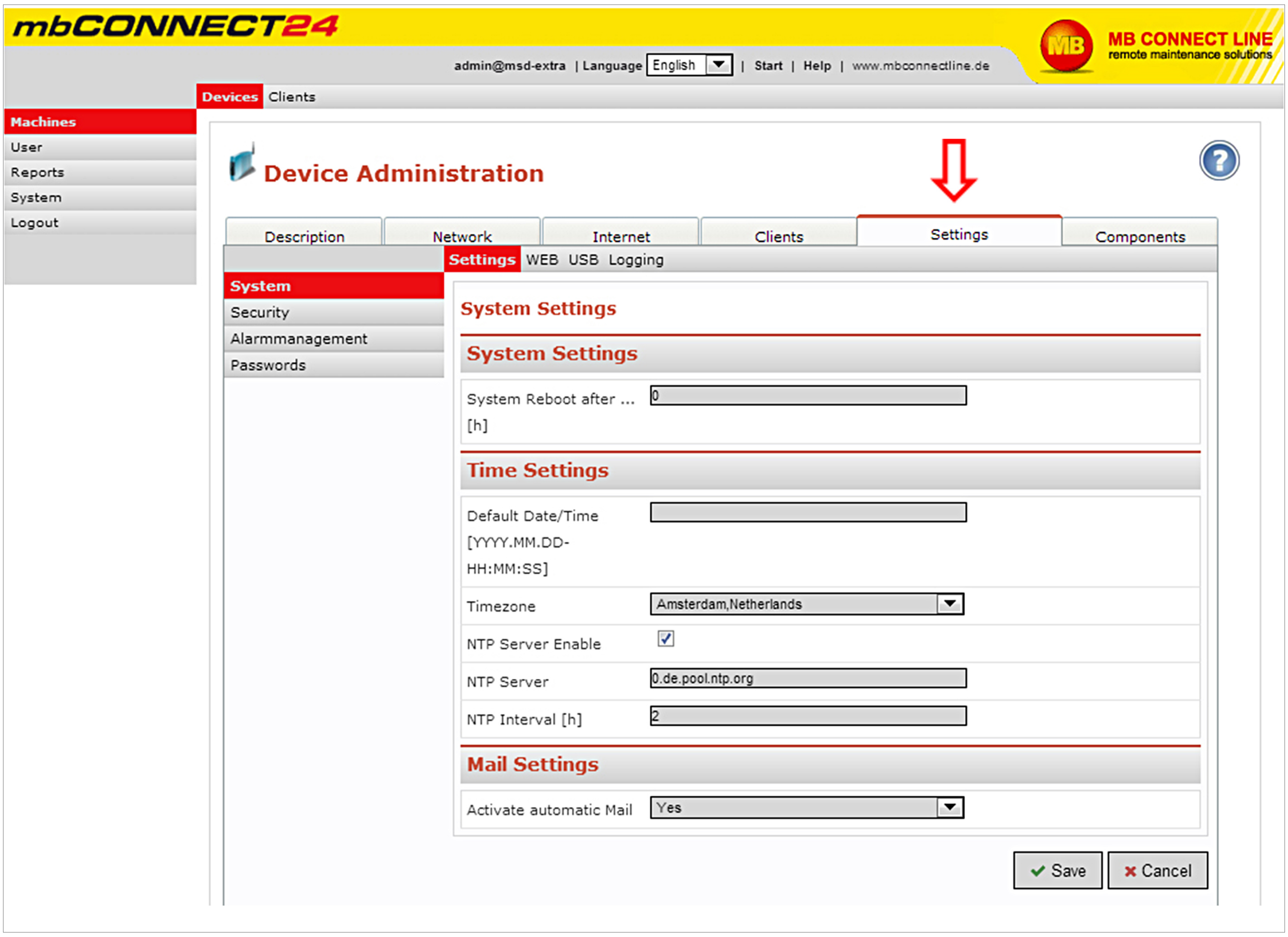
13 Configuring Your Router in the Portal (V 1.x)

The router can be fully configured only by using the Portal Server ***mbCONNECT24***.

1 Therefor, after logon at the Portal go to the menu **Machines** > **Devices**

2 Select that particular device for configuration via the edit button ✎

3 Change, if necessary, to the **Settings** tab



System Settings

System Settings

System Reboot after ... [h]	0

Time Settings

Default Date/Time [YYYY.MM.DD-HH:MM:SS]	
Timezone	Amsterdam,Netherlands
NTP Server Enable	☑
NTP Server	0.de.pool.ntp.org
NTP Interval [h]	2

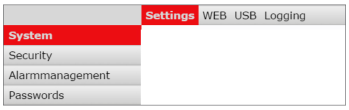
Mail Settings

Activate automatic Mail	Yes

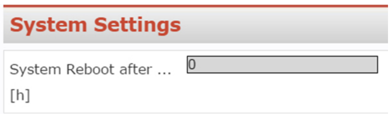
NOTICE

All settings and changes are only effective after they have been transferred as a configuration on the device (see chapter *Transferring the configuration to mbNET.mini*).

13.1 System > Settings



13.1.1 System Settings

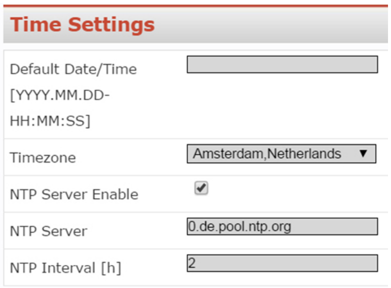


System Settings

System Reboot after ... [h]	0

Here you choose if and when the ***mbNET.mini*** should reboot.
Input => natural numbers [h]. If you leave this blank or enter 0, it will not reboot.

13.1.2 Time Settings



Time Settings

Default Date/Time [YYYY.MM.DD-HH:MM:SS]	
Timezone	Amsterdam,Netherlands ▼
NTP Server Enable	☑
NTP Server	0.de.pool.ntp.org
NTP Interval [h]	2

Enter the current **date** and **time** here, even if you are activating an NTP server.

Choose your **time zone**.

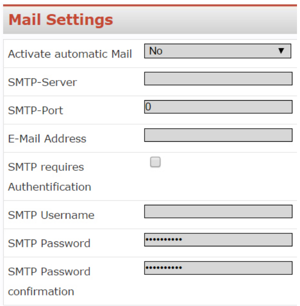
If "**NTP Server Enable**" has been checked, the device time will be synchronized automatically via the set NTP server (preset address: 0.de.pool.ntp.org).
A time server IP address may be entered instead of a name.
If a name is entered, there must be a DNS server entered in the network settings, or an existing Internet connection.
The NTP server simply needs to be available.
The time is only automatically synchronized when

- "NTP Server Enable" has been checked
- and a valid NTP server has been entered
- and the value for the NTP interval is > 0

Input => Natural numbers [h]. If you leave this blank or enter 0, the time will not synchronize.

13.1.3 Mail Settings

Selecting "**Yes**" in "**Activate automatic Mail**" means that the router will use MB connect line's mail server and fixed parameters.
Selecting "**No**" in "**Activate automatic Mail**" means that you must enter the necessary details of your mail server.

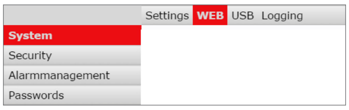


Mail Settings

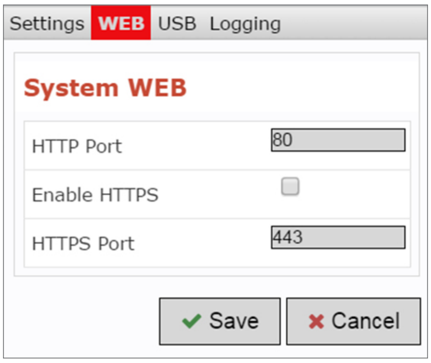
Activate automatic Mail	No ▾
SMTP-Server	
SMTP-Port	0
E-Mail Address	
SMTP requires Authentification	□
SMTP Username	
SMTP Password	••••••••••
SMTP Password confirmation	••••••••••

SMTP-Server	The SMTP server is needed for the router to send emails.
SMTP-Port	Enter the port used to send emails (usually port 25).
E-Mail Address	Enter the appropriate sender address for emails from the router here.
SMTP requires Authentification	The box should be checked or unchecked depending on the ISP. Ask your ISP for the correct setting.
SMTP Username **SMTP Password**	A user name and password is required for SMTP server authentication, i.e. if the router wants to send an email to the SMTP, it may have to first authentificate itself.

13.2 System > WEB



Enter the port here and select the type of connection that will enable you to access the Web-GUI of the mbNET.mini.

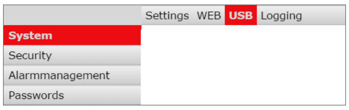


System WEB

HTTP Port	80
Enable HTTPS	□
HTTPS Port	443

HTTP Port	The standard port for HTTP requests is TCP 80. You can however select another port if you need this port for your OpenVPN connection or if it is already being used for another purpose. If you do this, please note that you will need to enter the selected port in the browser along with the address in the browser window.
Enable HTTPS	Clicking on the check box enables the secure Hypertext Transfer Protocol.
HTTPS Port	To allow access, you need to enter the router IP address and the port of the remote com-puter (here: port 443).

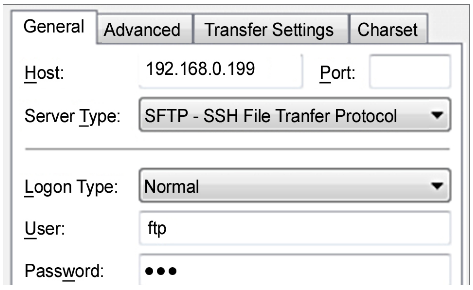
13.3 System > USB



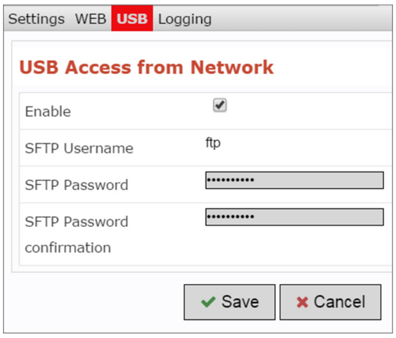
USB Access from Network

When "**Active**" is checked, the USB memory can be accessed via an SFTP client.

Default settings:
„SFTP Username“: ftp
„SFTP Password“: ftp

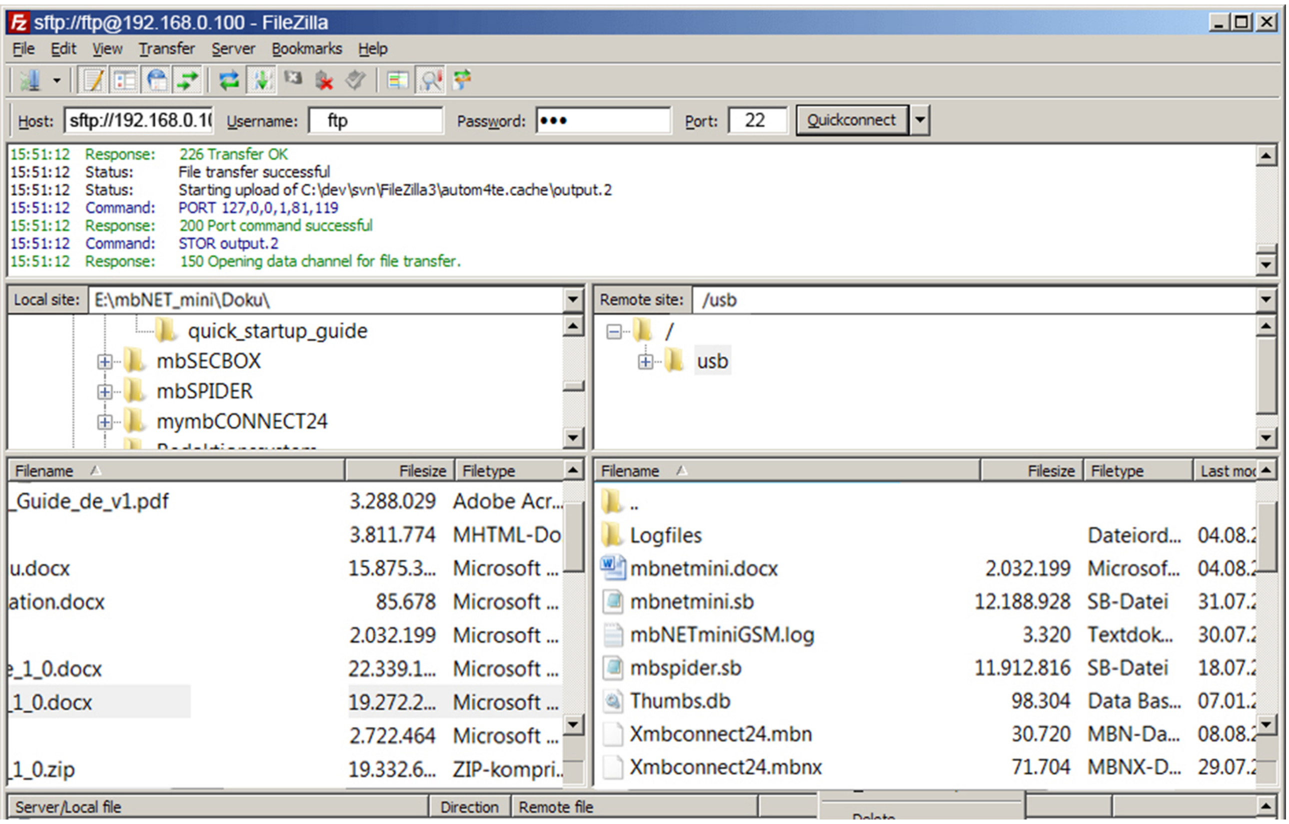


Host: 192.168.0.199
Port:
Server Type: SFTP - SSH File Tranfer Protocol
Logon Type: Normal
User: ftp
Password: ●●●



USB Access from Network

Enable ☑
SFTP Username ftp
SFTP Password ••••••••••
SFTP Password confirmation ••••••••••



Host: sftp://192.168.0.1(Username: ftp Password: ●●● Port: 22

```
15:51:12  Response:   226 Transfer OK
15:51:12  Status:     File transfer successful
15:51:12  Status:     Starting upload of C:\dev\svn\FileZilla3\autom4te.cache\output.2
15:51:12  Command:    PORT 127,0,0,1,81,119
15:51:12  Response:   200 Port command successful
15:51:12  Command:    STOR output.2
15:51:12  Response:   150 Opening data channel for file transfer.
```

Local site: E:\mbNET_mini\Doku\

- quick_startup_guide
- mbSECBOX
- mbSPIDER
- mymbCONNECT24

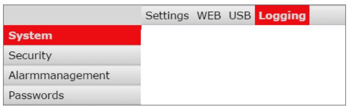
Remote site: /usb

- /
  - usb

Filename	Filesize	Filetype
_Guide_de_v1.pdf	3.288.029	Adobe Acr...
	3.811.774	MHTML-Do
u.docx	15.875.3...	Microsoft ...
ation.docx	85.678	Microsoft ...
	2.032.199	Microsoft ...
‿_1_0.docx	22.339.1...	Microsoft ...
1_0.docx	19.272.2...	Microsoft ...
	2.722.464	Microsoft ...
1_0.zip	19.332.6...	ZIP-kompri...

Filename	Filesize	Filetype	Last moc
..			
Logfiles		Dateiord...	04.08.2
mbnetmini.docx	2.032.199	Microsof...	04.08.2
mbnetmini.sb	12.188.928	SB-Datei	31.07.2
mbNETminiGSM.log	3.320	Textdok...	30.07.2
mbspider.sb	11.912.816	SB-Datei	18.07.2
Thumbs.db	98.304	Data Bas...	07.01.2
Xmbconnect24.mbn	30.720	MBN-Da...	08.08.2
Xmbconnect24.mbnx	71.704	MBNX-D...	29.07.2

13.4 System > Logging



Logging Settings

General:

"Set debug output to syslog"
if this checkbox is activated, the logging is extended by the "Debug information".

"Log also to USB-Device"
additional logging outputs can only be accessed on the USB stick, which is connected to the mbNET.mini (file name of the logging file: "*Device name.log*").

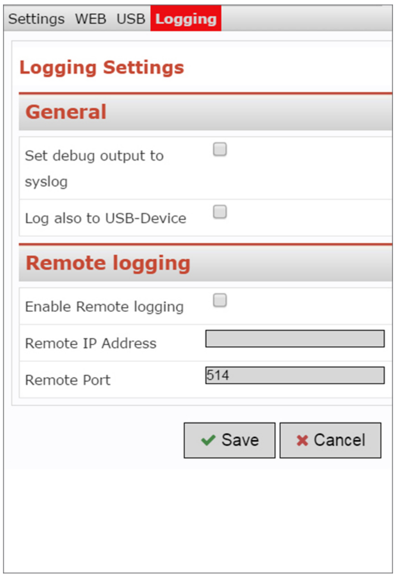
Remote Logging:

"Enable Remote logging"

if this checkbox is activated, the mbNET.mini system logging can be outsourced to another computer.

"Remote IP Address"
enter here the IP address of the external logging server.

"Remote Port"
port 514 is preset here.
We recommend that you do not change this port, unless you are using a certain application that reacts to a different port.



Logging Settings

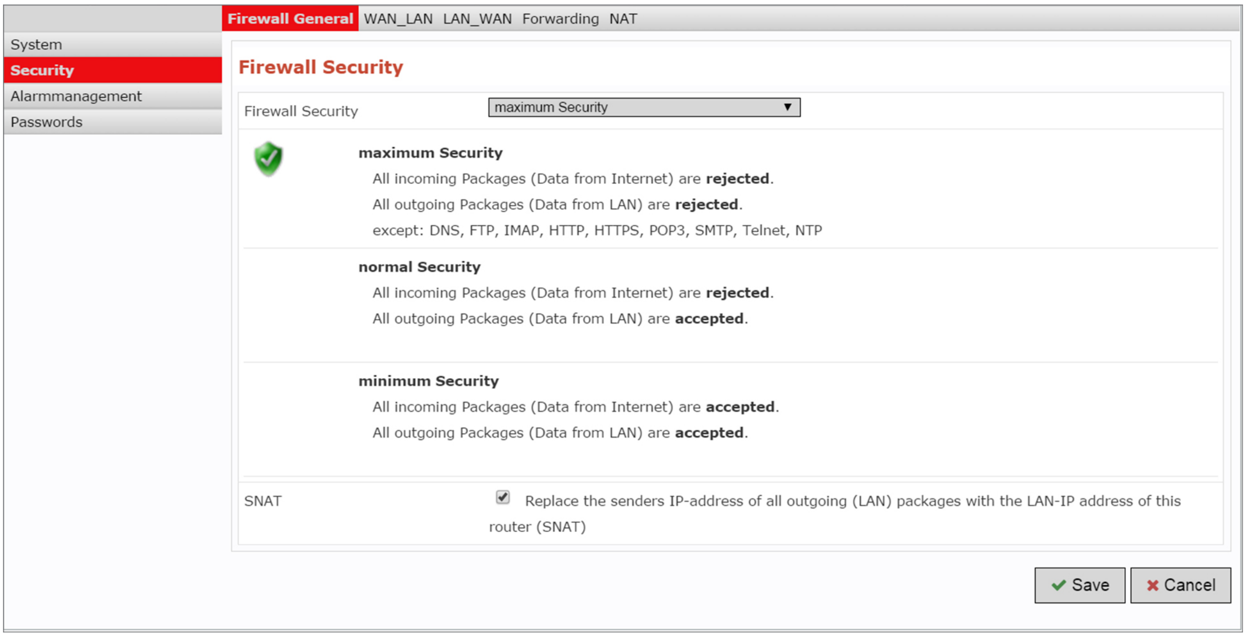
General

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

Remote logging

Enable Remote logging	□
Remote IP Address	
Remote Port	514

13.5 Security > Firewall General



Firewall Security

Firewall Security: maximum Security ▼

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

normal Security
All incoming Packages (Data from Internet) are **rejected**.
All outgoing Packages (Data from LAN) are **accepted**.

minimum Security
All incoming Packages (Data from Internet) are **accepted**.
All outgoing Packages (Data from LAN) are **accepted**.

SNAT ☑ Replace the senders IP-address of all outgoing (LAN) packages with the LAN-IP address of this router (SNAT)

The ***mbNET.mini*** has an integrated firewall to protect against third-party and unauthorized access and connection attempts. Incoming and outgoing data traffic is checked, logged and allowed or denied via this firewall.

The firewall can generally be configured with one of the following three settings:

- **Maximum security**
  Which data traffic is allowed must be configured accordingly in this setting. Both incoming and outgoing data traffic is denied.
  To access the web interface (from outside the network), the **TCP protocol** and the **destination port 80** must be entered and enabled in the **WAN >LAN** settings. If, however, you start a VPN connection, access is accordingly allowed for the data packets from the VPN tunnel.
- **Normal Security**
  With this setting, incoming data traffic (data from the Internet) is denied while outgoing data traffic is allowed.
- **Minimum Security**
  With this setting, all incoming and outgoing data traffic is allowed.

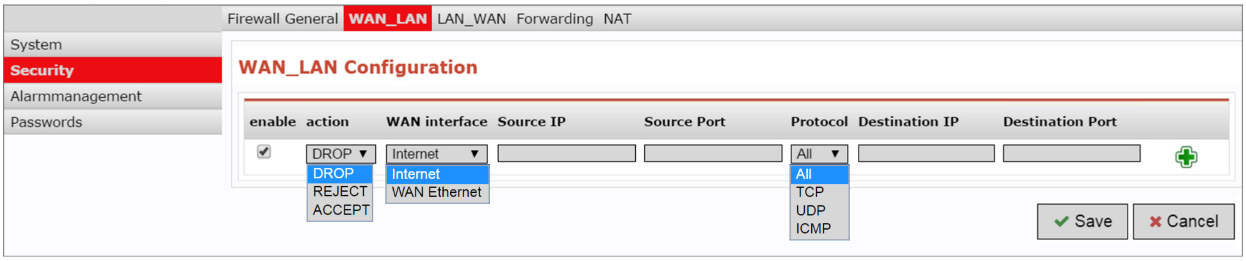
NOTICE

The "**minimum Security**" option should only be temporarily set for test purposes since it allows all data traffic from inside to outside the network as well as access from outside the network. This setting puts the integrity of your ***mbNET.mini*** and the connected devices at risk!

SNAT
This function transparently passes on the incoming data traffic from Internet or VPN connections to the LAN. In other words, all data packets going to the LAN are assigned the IP address of the router as the sender address. This means that none of the LAN subscribers need the router as a "gateway". This is a considerable advantage when integrating remote maintenance into existing network structures as it means that these structures do not need to be changed.

13.6 Security > WAN>LAN

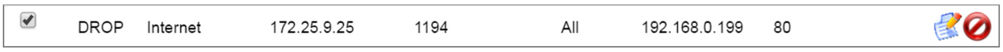
This setting governs the incoming data traffic, i.e. the following settings only apply to data traffic arriving from outside the network.



WAN_LAN Configuration

enable	action	WAN interface	Source IP	Source Port	Protocol	Destination IP	Destination Port	
☑	DROP ▼	Internet ▼			All ▼			✚

Sample setting



☑	DROP	Internet	172.25.9.25	1194	All	192.168.0.199	80	✎ ⊘

The following rule applies according to the device type:

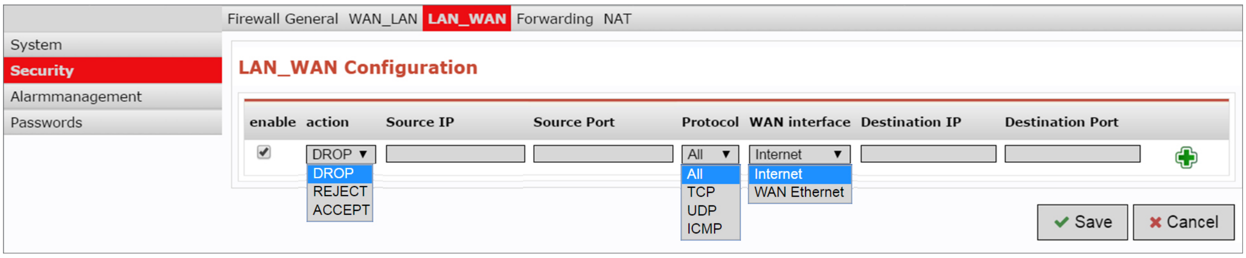
If the connection is established to the Internet via WAN (external router, fixed line), the WAN Ethernet port is the gateway to the Internet. Thus, the firewall controls the traffic from the WAN Ethernet to the LAN Ethernet.

If the connection is established to the Internet via Modem, the Modem is the gateway to the Internet. Thus, the firewall controls the traffic from the Modem to the LAN Ethernet.

Designation	Description
Enable	If the box has been checked, the following settings will be active after saving.
Action	The following options are available for selection: **Drop**: If this option is selected, it means that no data packets can pass and the packets are deleted immediately. The sender is not notified about the whereabouts of the data packets. **Reject**: If this option is selected, the data packets are rejected. The sender is notified that the data packets have been rejected. **Accept**: If this option is selected, the data packets can pass.
WAN interface	This defines the WAN interface to which the setting is to be applied. "**Internet**" or "**WAN Ethernet**" can be selected.
Source IP	Here, enter the IP for whose incoming data packets one of the set actions is to be executed. If you leave the field blank, the set action applies to all IP addresses.
Source Port	Enter the port via which the data packets arrive here.
Protocol	The following options are available for selection: **All**: This setting applies to all protocols. **TCP**: This setting only applies to the TCP protocol. **UDP**: This setting only applies to the UDP protocol. **ICMP**: This setting only applies to the ICMP protocol.
Destination IP	Enter the IP to which the data packets are to be forwarded here.
Destination Port	Enter the port via which the data packets are forwarded here.
✚	Accepts a new setting.
✎	Edits the settings in the current line.
⊘	Deletes setting

13.7 Security > LAN>WAN

The LAN_WAN Configuration governs the outgoing data traffic, i.e. the following settings only apply to outgoing data traffic.

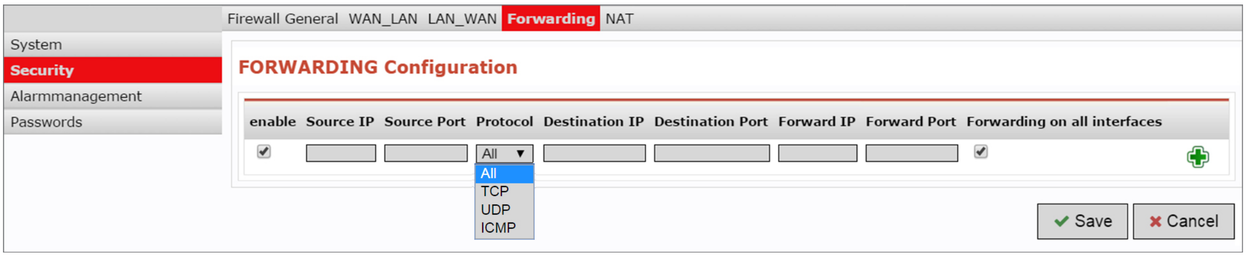


LAN_WAN Configuration

enable	action	Source IP	Source Port	Protocol	WAN interface	Destination IP	Destination Port	
☑	DROP ▼			All ▼	Internet ▼			✚

Designation	Description
Enable	If the box has been checked, the following settings will be active after saving.
Action	The following options are available for selection: **Drop**: If this option is selected, it means that no data packets can pass and the packets are deleted immediately. The sender is not notified about the whereabouts of the data packets. **Reject**: If this option is selected, the data packets are rejected. The sender is notified that the data packets have been rejected. **Accept**: If this option is selected, the data packets can pass.
Source IP	Enter the IP of a computer from which data packets are sent to the Internet here. If you leave the field blank, the set action applies to all IP addresses.
Source Port	Enter the port via which the data packets are sent into the Internet here.
Protocol	The following options are available for selection: **All**: This setting applies to all protocols. **TCP**: This setting only applies to the TCP protocol. **UDP**: This setting only applies to the UDP protocol. **ICMP**: This setting only applies to the ICMP protocol (ping).
WAN interface	This defines the WAN interface to which the setting is to be applied. You can select "**Internet**" or "**WAN Ethernet**".
Destination IP	Enter the Internet destination address of the data packets here.
Destination Port	Enter the port via which the data packets are sent to the destination IP here.
✚	Accepts a new setting.
✎	Edits the settings in the current line.
⊘	Deletes setting

13.8 Security > Forwarding



FORWARDING Configuration

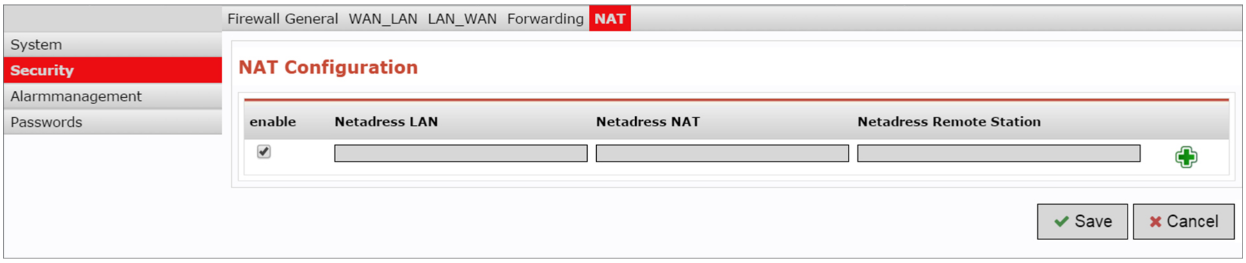
enable	Source IP	Source Port	Protocol	Destination IP	Destination Port	Forward IP	Forward Port	Forwarding on all interfaces
☑			All ▼					☑

All
TCP
UDP
ICMP

Designation	Description
Enable	If the box has been checked, the following settings will be active after saving.
Source IP	You can enter the IP from which data packets are to be received here. If an entry is made here, only packets from this one address are forwarded.
Source Port	You can specify the port via which the data packets arrive here. If an entry is made here, only packets specifically sent via this port are forwarded.
Protokoll	The following options are available for selection: **All**: This setting applies to all protocols. **TCP**: This setting only applies to the TCP protocol. **UDP**: This setting only applies to the UDP protocol. **ICMP**: This setting only applies to the ICMP protocol.
Destination IP	Enter the IP to which the data packets were originally to be sent here.
Destination Port	Specify the port via which the data packets are sent to the destination IP here.
Forward IP	Enter the IP to which the data packets are actually to be forwarded here.
Forward Port	Specify the port via which the data packets are actually to be forwarded here.
Forwarding on all interfaces	The "FORWARDING" setting is applied to all connections, i.e. even incoming VPN connections. If this option is not set, the setting only applies to incoming packet from the Internet, but not a VPN connection via the Internet.
✚	Accepts the new settings and temporarily stores them.
✎	Edits the settings in the current line.
⊘	Deletes setting

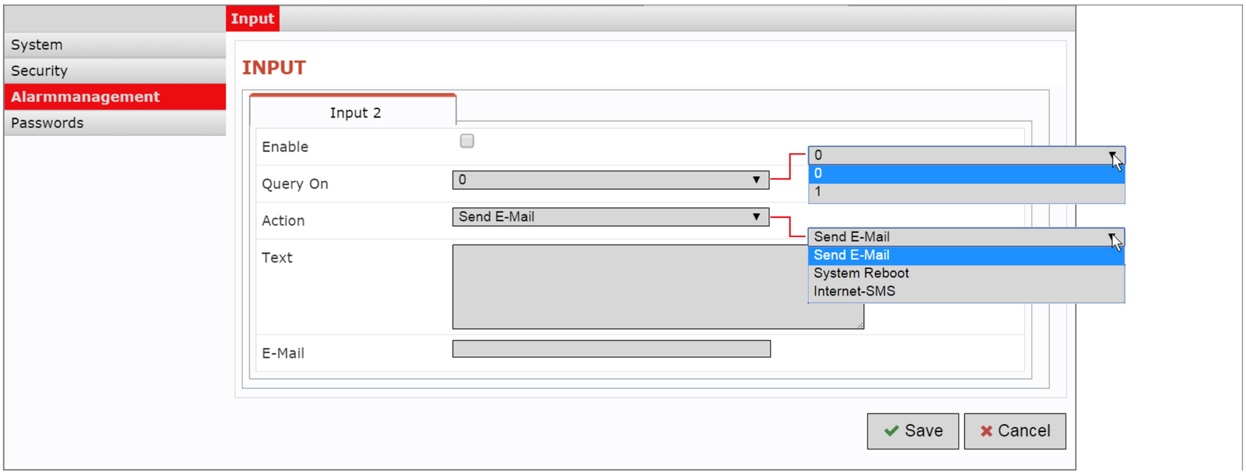
13.9 Security > NAT

The NAT Configuration enables two networks in the same address range to be connected. If, for example, 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 another address. NAT technology is an easy way of achieving this since only the real network address (LAN address) and the substitute address (NAT network address) are required. The NAT algorithm makes sure that the addresses in the data packets are only substituted in communications between these two networks. This means that you do not have to adapt your entire network addressing scheme.



Bezeichnung	Beschreibung
Enable	If the box has been checked, the following settings will be active after saving.
Netaddress LAN	Enter the real address of the network here (e.g.192.168.0.0/24). **NOTICE** Please note that the IP address must be entered in CIDR notation.
Netaddress NAT	Enter the translated address of your network here (e.g.192.168.1.0/24). **NOTICE** Please note that the IP address must be entered in CIDR notation.
Netaddress Remote Station	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.
✚	Accepts a new setting.
✎	Edits the settings in the current line.
⊘	Deletes setting

13.10 Alarm management > Input



Input

- System
- Security
- Alarmmanagement
- Passwords

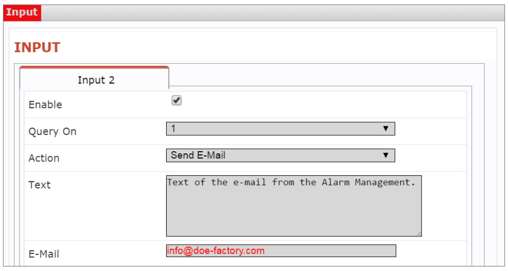
INPUT

Input 2

Enable	□
Query On	0
Action	Send E-Mail
Text	
E-Mail	

NOTICE

Only digital **input 2** can be used to send emails, text messages, Internet text messages or to restart the device.



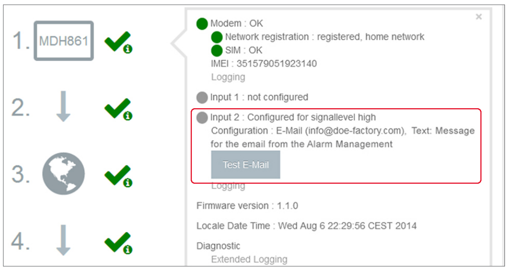
Input

INPUT

Input 2

Enable	☑
Query On	1
Action	Send E-Mail
Text	Text of the e-mail from the Alarm Management.
E-Mail	info@doe-factory.com

After the device has accepted the configuration, the configuration is shown on the start page of the **mbNET.mini** in the information under Step 1.



● Modem : OK
● Network registration : registered, home network
● SIM : OK
IMEI : 351579051923140
Logging

● Input 1 : not configured

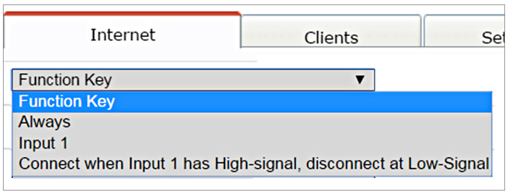
● Input 2 : Configured for signallevel high
Configuration : E-Mail (info@doe-factory.com), Text: Message for the email from the Alarm Management
Test E-Mail
Logging

Firmware version : 1.1.0

Locale Date Time : Wed Aug 6 22:29:56 CEST 2014

Diagnostic
Extended Logging

The state of Input 2's signal is shown with the prepended soft-LED (grey = 0/low, green = 1/high). If an email, text message or Internet text message has been configured, the button "Test email" appears. Clicking this button will carry out a test on the setting.



Internet
Clients
Set
Function Key
Function Key
Always
Input 1
Connect when Input 1 has High-signal, disconnect at Low-Signal

Input 1 can only be configured for establishing the connection, see Machines/Device Administration/Internet. Once it has been configured accordingly, the description "Input 1" is shown. The state of the signal is shown with the prepended soft-LED (grey = 0/low, green = 1/high).

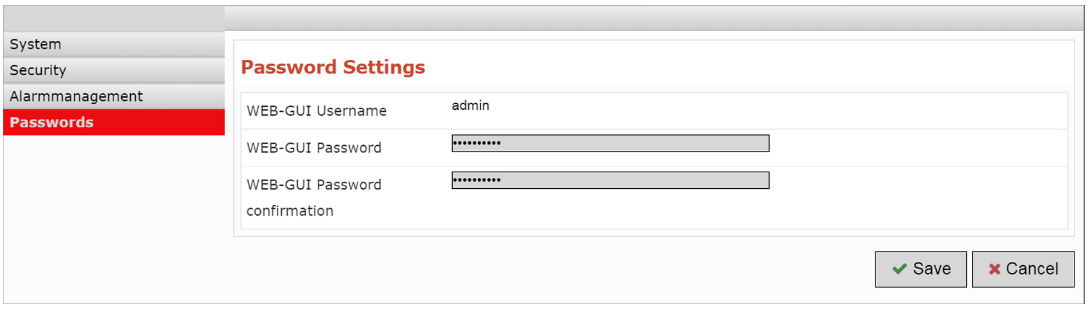
13.11 Passwords (Password Settings)

The router is shipped with the following usernames and password preset:

„WEB-GUI **Username**“: **admin**
„WEB-GUI **Password**“: No password required

NOTICE

Change the device password to prevent unauthorized access to the device.



Password Settings

WEB-GUI Username	admin
WEB-GUI Password	••••••••••
WEB-GUI Password confirmation	••••••••••

NOTICE

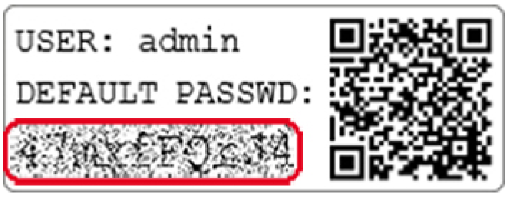
These and all changes that you make for the mbNET.mini in the portal will only take effect when the settings/changes made are transferred to the device as a configuration.

14 Factory settings on delivery

The ***mbNET.mini*** - from serial number S/N: 202086.... - is delivered with the following factory settings:

IP-Address	192.168.0.100
Subnet mask	255.255.255.0
Login (User)	admin
Password	individual device password

The device password can be found on the back of the device.



USER: admin

DEFAULT PASSWD:

[redacted]

15 Loading the factory settings

NOTICE

Before you reset the device to its factory settings, note the following:

- The device must be operational (LED Pwr + Rdy light up).
- The IP address of the router is reset to 192.168.0.100.
  You may have to adjust the network settings of the configuration computer accordingly.

To reset the ***mbNET.mini*** to factory settings, proceed as follows:

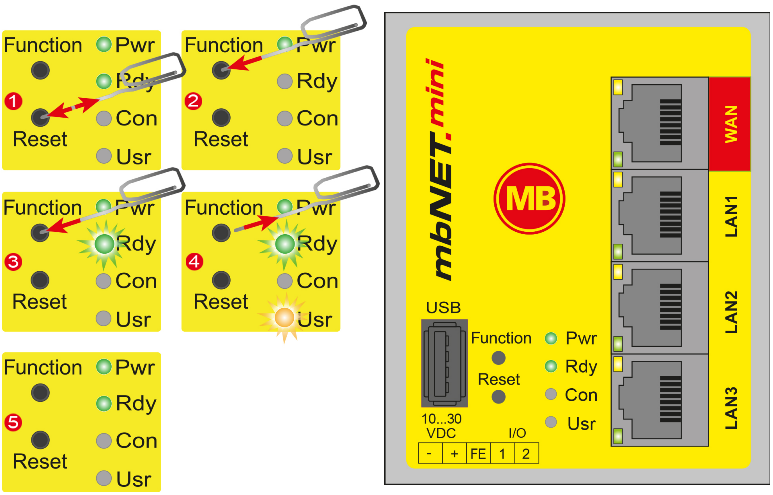
Click the button **Reset** once ❶.

Then press **Function** straight afterwards and keep it pressed down ❷.

After about 60-90 seconds, the **Rdy LED** starts flashing ❸.

As soon as the **Usr LED** starts to flash, release the button **Function** ❹.

When the **LED Pwr** and **Rdy** light up, the factory settings have been loaded ❺.



The ***mbNET.mini*** is now ready for operation and be configured again.

16 Firmware update

Generally you can perform a firmware update via the USB interface of the device.

The latest firmware version can be found in our download center on **www.mbconnectline.com**.

If you operate your ***mbNET.mini*** in association with the **RSP *mbCONNECT24*** version **2.x**, you can perform the firmware update via the portal. For this, you will be provided the latest firmware version by the portal.

16.1 Firmware update via USB

- Go to **www.mbconnectline.com** and download the latest firmware version (e.g. "FW_mbNETmini_V206.zip").
- After extracting can be found next the "Changelog.txt" file the actual firmware file "mbnetmini.sbs".
- Store the "mbnetmini.sbs" on a USB stick.

NOTICE

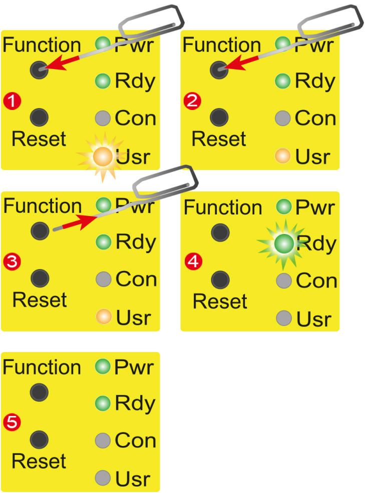
IMPORTANT: The downloaded "mbnetmini.sbs" firmware file may not be renamed and must be saved in the top-level directory of the USB drive. The USB drive must have the file format FAT!

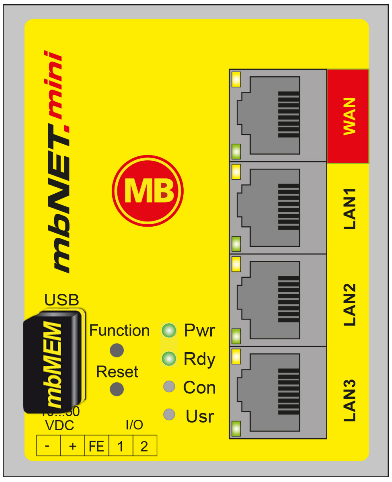
- When the ***mbNET.mini*** is ready for operation (LED Pwr + RDY light up), plug the USB stick into the USB port of the device. The device detects the firmware file and shows this by rapidly blinking **LED Usr** (flashing frequency: 3 Hz).

Now press, within 10 seconds, the button **Function** ❶ and keep it pressed until the **Usr LED** lights ❷.

When **Usr LED** lights, release the button **Function** ❸.
The device afterwards is going to restart ❹.

When the two **LED Pwr** and **Rdy** light up, the firmware update is finished ❺.





The ***mbNET.mini*** is now ready for operation again and can, as usual, be used.

NOTICE

If there is both a firmware file (mbnetmini.sbs) and a configuration file (mbconnect24.mbn/-.mbnx), the files are recognized as follows:

1. mbnetmini.sbs => LED Usr flashes quickly (flashing frequency: 3 Hz)
2. mbconnect24.mbn/-.mbnx=> LED Usr flashes slowly (flashing frequency: 1.5 Hz)

If, for example, only the configuration file mbconnect24.mbn/-.mbnx is to be loaded, wait approx. 10-20 sec after the automatic recognition of the firmware file, until the LED Usr has started to flash slowly. Now you can carry out the procedure "Load configuration file".

16.2 Firmware update via RSP *mbCONNECT24*

Navigation:

Administration > Projects > *Project Gama (selected project)* > *GamaRouter (selected device)* > Services

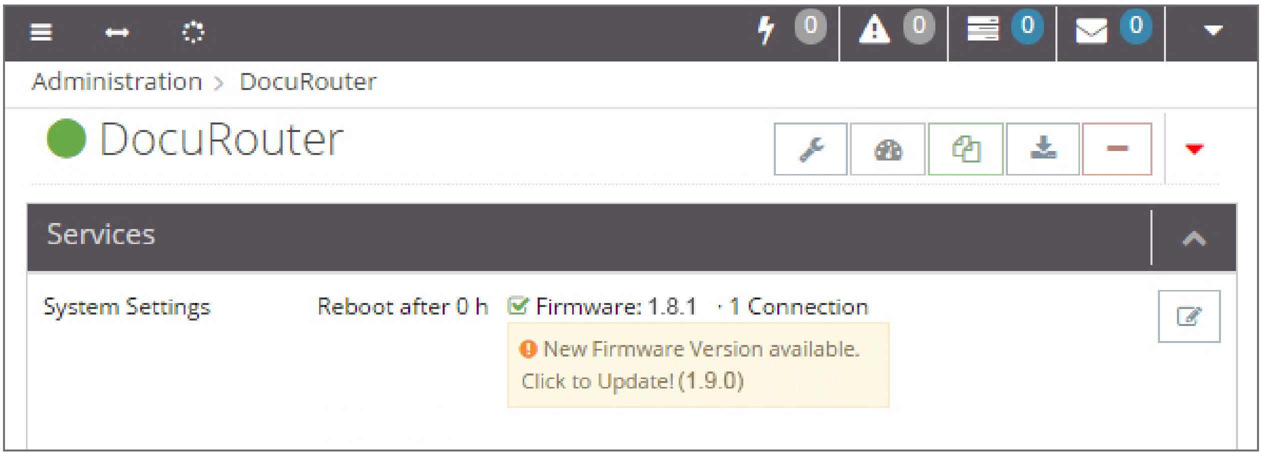
Prerequisites:

- You operate the device in the **RSP *mbCONNECT24*** V 2.x.
- The device is online in the portal.

How to do:

Call up the device settings of the relevant device.

1

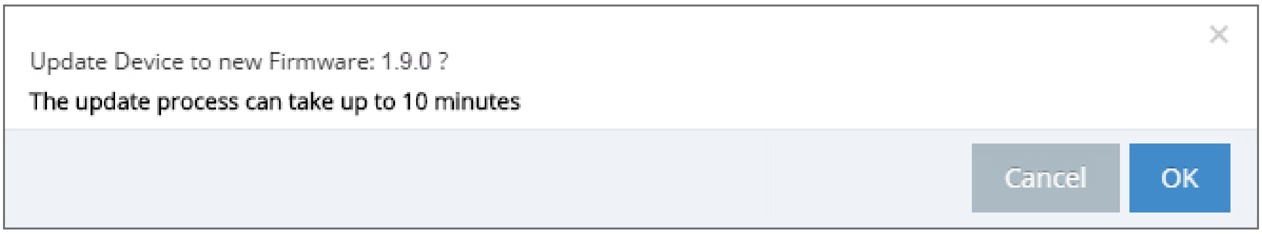


System Settings | Reboot after 0 h | Firmware: 1.8.1 · 1 Connection

New Firmware Version available. Click to Update! (1.9.0)

Under **Services > System Settings**, you will receive a hint as soon as the device firmware is no longer up-to-date, with the prompt by clicking on this note to perform a firmware update.

2

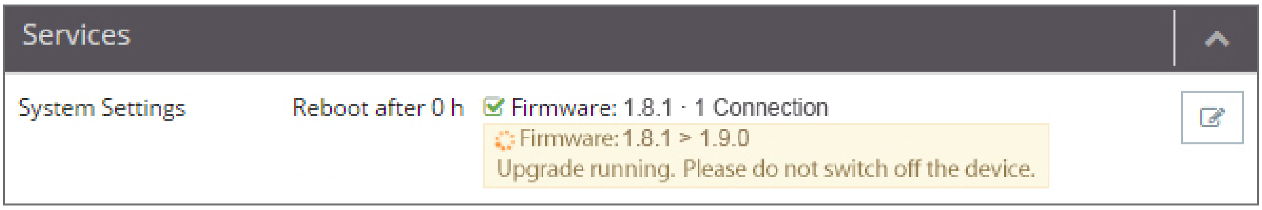


Update Device to new Firmware: 1.9.0 ?

The update process can take up to 10 minutes

In the following window, you are prompted to confirm the firmware update.

3



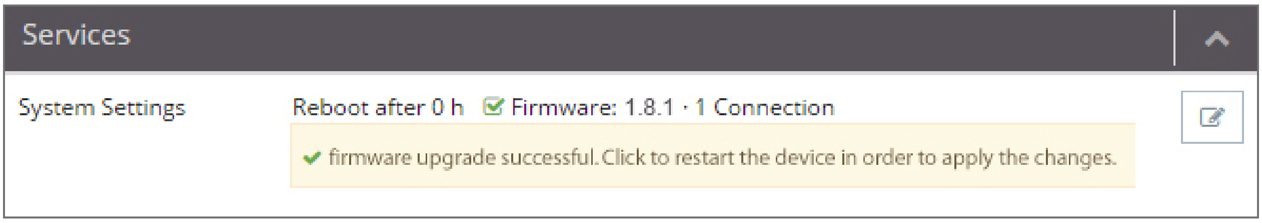
System Settings | Reboot after 0 h | Firmware: 1.8.1 · 1 Connection

Firmware: 1.8.1 > 1.9.0

Upgrade running. Please do not switch off the device.

Now you get the information about the firmware version (from version> to version) and that the device must not be switched off during the update.

4

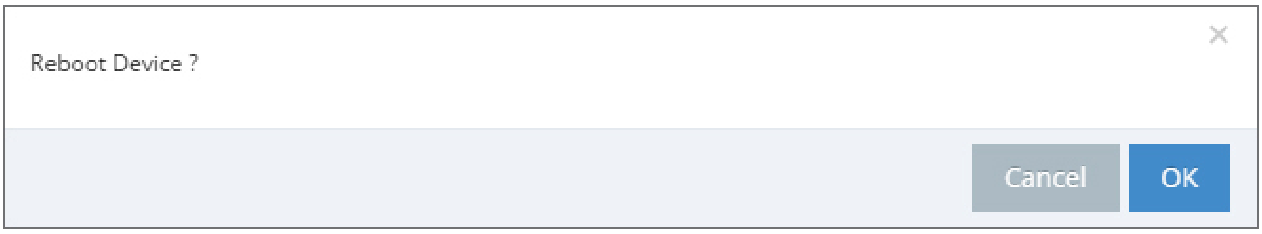


System Settings Reboot after 0 h ✓ Firmware: 1.8.1 · 1 Connection

✓ firmware upgrade successful. Click to restart the device in order to apply the changes.

After a successful firmware update, you will be prompted to restart the device for the change to take effect.

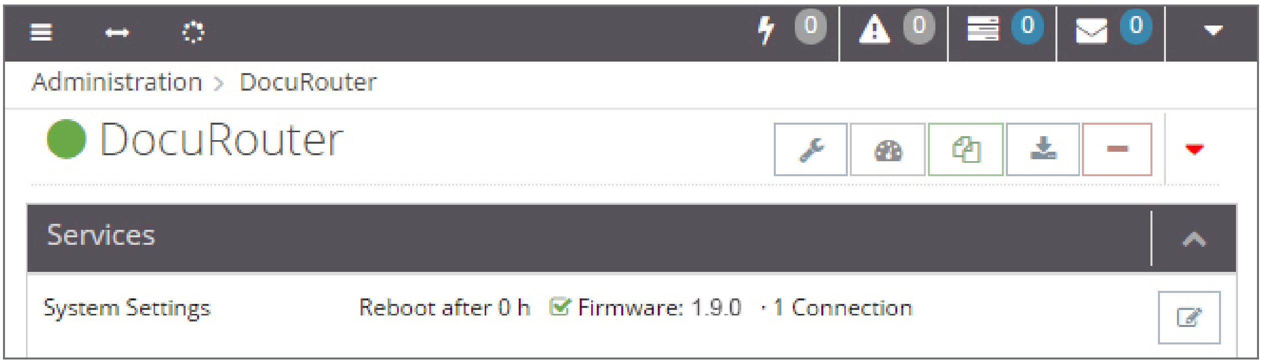
5



Reboot Device ?

In the following window, you are prompted to restart the device.

6

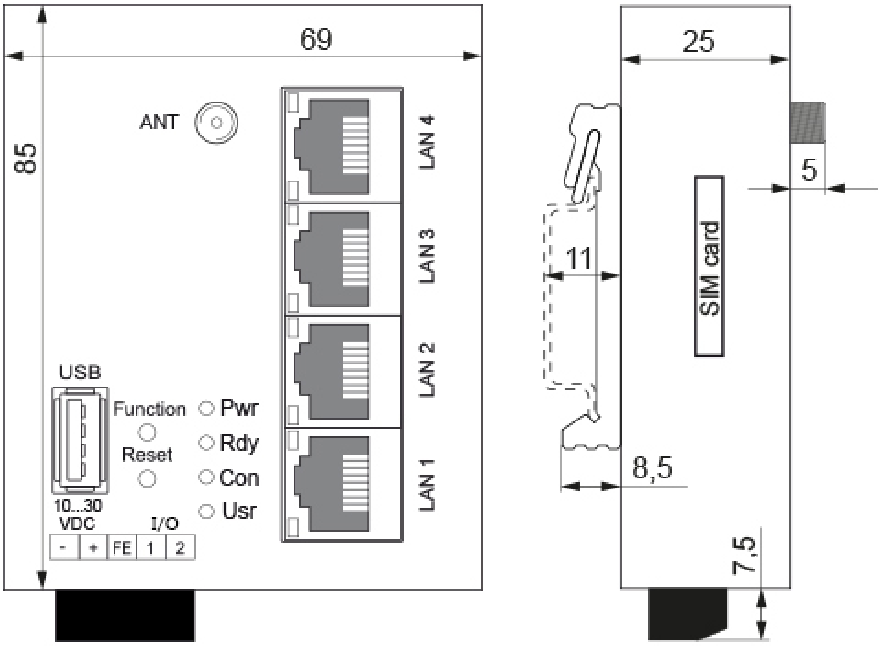


System Settings Reboot after 0 h ✓ Firmware: 1.9.0 · 1 Connection

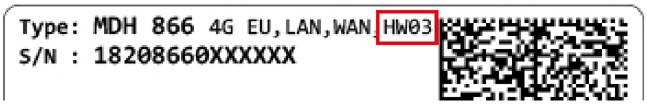
After the device has been restarted and the device has reconnected to the portal, the current firmware is displayed.

17 Technische Daten Industrie-Router *mbNET.mini* MDH 860 – MDH 867

(Type: MDH 860, MDH 862 AT&T, MDH 862 EU, MDH 863, MDH 866 AT&T, MDH 866 EU, MDH 867).
Ab Hardware-Version HW02, HW03* und Firmware-Version ab V 2.2.0



* You will find the hardware version on the device nameplate.



Type: MDH 866 4G EU,LAN,WAN,HW03
S/N : 18208660XXXXXX

General data

Voltage ⎓ V (DC)	10 - 30 V DC (SELV and Limited Energy circuit)
Power consumption (Normal mode)	250 mA @ 24 V - without additional consumers
Power consumption under full load	max. 1.8 A @ 24 V - (including 2 digital outputs + USB port)
Random Access Memory	128 MB
Processor speed	454 MHz
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 application	Dry environments
Operating temperature	-40 – +75 °C (Type: MDH 860, MDH 862, MDH 866) -40 – +75 °C (Type: MDH 863, MDH 867 - **HW 03**)
Operating temperature	0 – +60 °C (Type: MDH 863, MDH 867 - **HW 02**)
Storage temperature	-40 – +85 °C
Humidity	0 – 95% (non condensing)
Weight (max.)	240 g
Dimensions (max.)	69 mm x 38.5 mm x 92.5 mm (W x D x H)
Housing (material)	metal
Mounting	DIN rail mounting (based on DIN EN 50022)

Interfaces / Communication

	Type				
	MDH 860	**MDH 862 EU / AT&T**	**MDH 863**	**MDH 866 EU / AT&T**	**MDH 867**
USB interface	1 x	1 x	1 x	1 x	1 x
Digital inputs	2 x	2 x	2 x	2 x	2 x
LAN interface	3 x	4 x	4 x	3 x	3 x
WAN interface	1 x	–	–	1 x	1 x
SIM card reader (mini SIM)	–	1 x	–	1 x	–
SMA socket ◎	–	2 x	–	2 x	–
RP-SMA socket ⊙	–	–	1 x	–	1 x
GSM module 3G (UMTS)	–	–	–	–	–
GSM module 4G (LTE)	–	1 x	–	1 x	–
Wi-Fi modem	–	–	1 x	–	1 x
Failover WAN > Modem / Wi-Fi	–	–	–	✓	✓

Interface specification

LAN interface	10/100 Mbit/s full and half duplex operation, autodetection patch cable / crossover cable
WAN interface	10/100 Mbit/s full and half duplex operation, autodetection patch cable / crossover cable
USB interface	USB Host 2.0
2 pieces I/Os	These connectors can be independently configured as a digital input or digital output - only in the mbCONNECT24 **V2** portal.
Digital input	10 – 30 V DC (low 0 – 3.2 V DC, high 8 – 30 V DC)
Digital output	10 – 30 V DC to a maximum of 1.5 A per output

VPN

Can only be operated with (my)***mbCONNECT24* ***.	
VPN protocol	OpenVPN, 1 tunnel
Encryption parameter	Control Channel: TLSv1.2, cipher ECDHE-RSA-AES256-GCM-SHA384 Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Authorization	Pre-Shared-Key, X.509
* The types MDH 866 and MDH 867 can only be operated in the portal (my)mbCONNECT24 **V2**.	

Network /Security

Firewall	1:1 NAT, IP-Filter, Port-Forwarding, stateful inspektion
IP router	NAT-IP, TCP/IP routing, IP forwarding
Service	DHCP client, NTP client
Time synchronization	NTP server

Communication

> Devices with **LTE (4G)** module (MDH 862 EU, MDH 866 EU); hardware version: **HW 03**

Target region	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
Transmission 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
TAC	35162207

.

> Devices with **LTE (4G)** module (MDH 862 EU, MDH 866 EU); hardware version: **HW 04**

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 • 2G: LB: 33 dBm; HB: 30 dBm • 3G/TD-SCDMA: 24dBm • 4G (FDD & TDD): 23dBm @1RB	Sensitivity - typical sensitivity levels • -108 dBm @ 2G • -113.5 dBm @ 3G • -103 dBm @ 4G FDD (BW=5 MHz)
TAC	35162610

.

> Devices with **LTE (4G)** module - **AT&T* -** Type: MDH 862 AT&T, MDH 866 AT&T; hardware version: **HW 02**

Target region	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; downl. max. 100 Mbps, upl. max. 50 Mbps
Transmission output power	Class 4 (2 W, 33 dBm) @ GSM 850 / 900; Class 1 (1 W, 30 dBm) @ GSM 1800 / 1900 Class E2 (0.5 W, 27 dBm) @ EDGE 850 / 900; Class E2 (0.4 W, 26 dBm) @ EDGE 1800 /1900 Class 3 (0.25 W, 24 dBm) @ UMTS; Class 3 (0.2 W, 23 dBm) @ LTE
FCC	FCC ID: R17LE910NA

NOTICE

*The device types MDH 862 AT&T and MDH 866 AT&T are not CE marked and must not be operated or commissioned in the European Economic Area (EEA)!

> Devices with **Wi-Fi** module (MDH 863, MDH 867); hardware version: **HW 02**

Wi-Fi	IEEE802.11b/g & 802.11n (1T1R mode), up to 150 MBit/s
Wi-Fi specification	· 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
Transmission 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
Reception sensitivity (typical)	11b: -84dBm @ 11 Mbps; 11g: -70dBm @ 54 Mbps 802.11n: (HT20), -66 dBm @ MSC7, (HT40), -62 dBm @ MSC7
FCC	FCC ID: YWTWFXM05

.

> Devices with **Wi-Fi m**odule (MDH 863, MDH 867); hardware version: **HW 03**

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 Encryption/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).

PROG. CNTLR.
E482663