MB CONNECT LINE
remote maintenance solutions

mbNET.mini

USER MANUAL

MDH861

MDH860

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.

This user manual (please read carefully and keep safely) describes the functions and use of the ***mbNET.mini*** router MDH86x.

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

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

MB Connect Line hereby confirms that the device ***mbNET.mini*** (MDH86x) complies with the basic requirements and all other relevant regulations of the European Directive 1999/5/EC. You can view the Declaration of Conformity at: www.mbconnectline.de

Issued by:
MB Connect Line GmbH
Remote Maintenance Solutions
Raiffeisenstraße 4
74360 Ilsfeld, Germany

Tel.: +49 (0) 700 MBCONNECT
+49 (0) 700 62 26 66 32
Website: www.mbconnectline.com

Table of contents

1. General

1.1 Brief description

The industrial router ***mbNET.mini*** offers you optimum flexibility and security, making remote communication with your systems both easy and secure. Thanks to its compact design, the ***mbNET.mini*** 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***.

1.2 Features

- The router can be fully configured via the portal mbCONNECT24.
- Can connect to machines and systems via LAN, WAN 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 with AES, DES/3DES and Blowfish encryption.
- Two digital inputs to initiate the connection to the portal server or send a warning text message/email.

1.3 Prerequisites/components:

mbCONNECT24	from V 1.6.2
mbDIALUP*	from V 3.1
mbCHECK*	from V 1.1.2
mbNET.mini*	from V 1.1.0 firmware

* The latest version can be downloaded from www.mbconnectline.com.

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.

3. Included in delivery

Please check that your delivery is complete:

MDH861	
	
mbNET.mini (MDH860)	**Quick Start Guide**

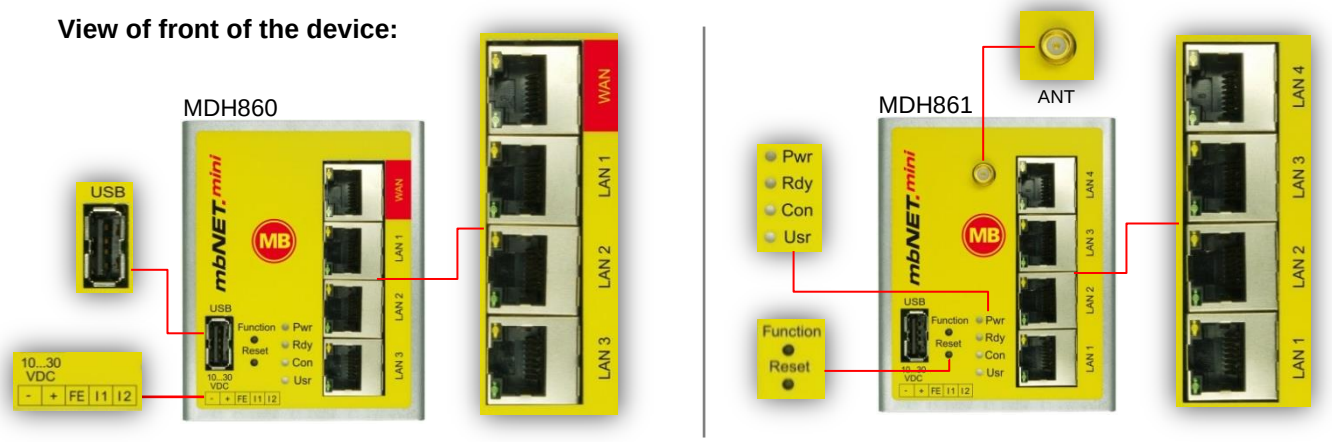
MDH860		
		
mbNET.mini (MDH861)	**GSM antenna**	**Quick Start Guide**

MB CONNECT LINE GMBH
Winnettener Straße 6
D-91550 Dinkelsbühl
Tel.: +49(0)700/MBCONNECT
+49(0)700/622 666 32
Web: www.mbconnectline.com

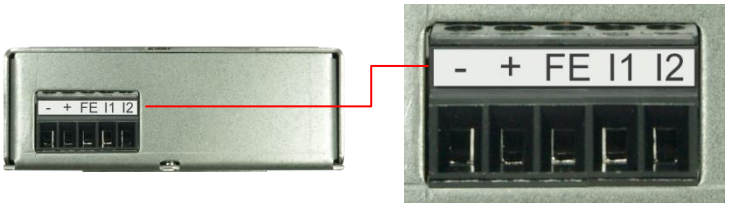
Please keep the original box and the original packaging in case you need to send the device for repair at a later date.

4. Displays, controls and connections

4.1 View of front of the device:

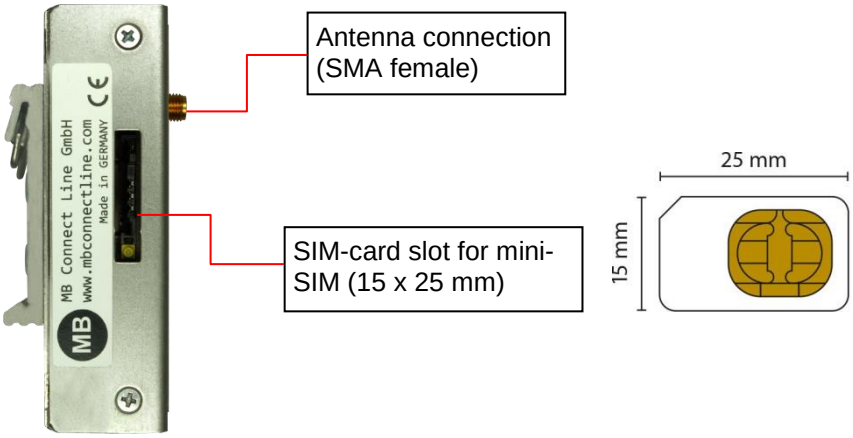


4.2 View of bottom of device

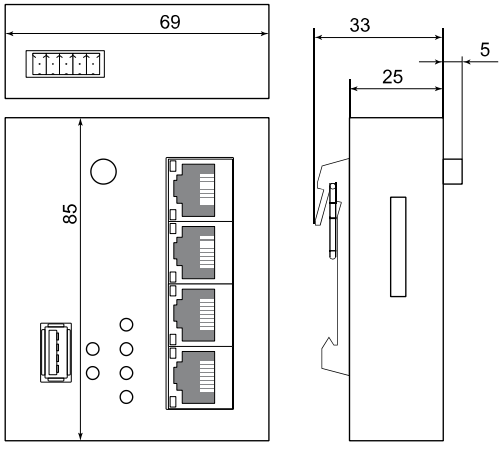


-	0V DC connection
+	Power source connection 10-30V DC
FE	Functional earth
I1	Digital input I1 (10-30V DC)
I2	Digital input I2 (10-30V DC)

4.3 View of device from left



4.4 Device dimensions

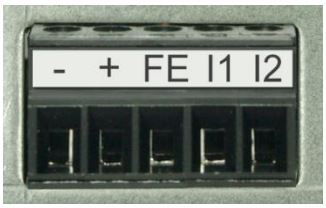


Designation	Status	Description
Pwr (Power)	LED off	Device power source is switched off or device is not connected to power source/power pack.
	LED on	Power source is connected to terminal block and switched on.
Rdy (Ready)	LED flash-ing	As soon as the system has been checked and started (duration approx. 25 sec), the LED flashes for the duration of the starting up process (approx. 90 sec).
	LED on	The device is ready for operation.
Con (Connect)	This LED shows whether the device is connected to the Internet and the portal server.	
	LED off	No connection to Internet or portal.
	LED flash-ing (3Hz)	Internet or VPN connection being established.
	LED flash-ing (1.5Hz)	Connection to portal server has been established.
	LED on	Connection to the Internet has been established.
Usr (User)	LED flash-ing (3Hz)	Firmware on USB stick ready to be updated.
	LED flash-ing (1.5Hz)	Portal configuration on USB stick ready to be transferred.
	LED on	Firmware or configuration is being copied to the device.
WAN	-	Router WAN connection (customer network, DSL router).
WAN LED	Green LED lights up	Network connection available.
WAN LED	Orange LED flash-ing	Network data transfer active.
LAN 1 - 4	-	Local network connection (e.g. machine network, network data transfer).
LAN LED 1 – 4 (Dual LED)	LED lights up	Network connection available.
USB	-	Transfer of configuration from USB stick to mbNET.mini. Transfer of firmware from USB stick to mbNET.mini. Access to free application data via SFTP.
Function	This button has three 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
Reset	-	Pushing this button restarts the device (so-called cold start).
–	-	0 V DC connection
+	-	Power supply connection 10 – 30 V DC.
FE	-	Functional earth to connect the equipotential bonding.
I1	-	Digital input 1 - is used to establish a connection when there is a high signal.
I2	-	Digital input 2 - used to send emails, text messages, Internet text messages or to start a re-boot.

5. Interface assignment

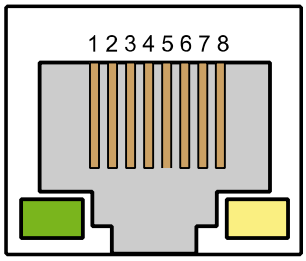
5.1 Pinout of the terminal block on the bottom of the device

-	0V DC connection
+	Power source connection 10-30V DC
FE	Functional earth
I1	Digital input I1 (10-30V DC)
I2	Digital input I2 (10-30V DC)



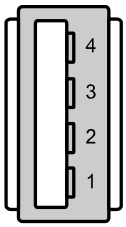
5.2 Pinout of LAN/WAN ports on the front panel of the device

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



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

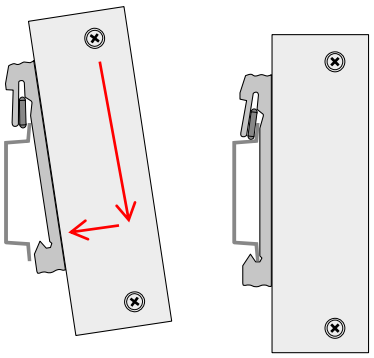
	Signal
1	VCC (+5V)
2	- Data
3	+Data
4	GND



6. 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).

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.

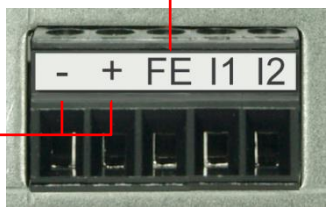


6.1 Connect the *mbNET.mini* to the power supply

Please note:
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).

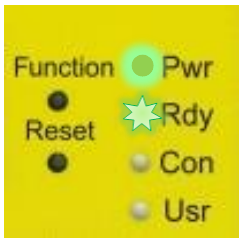
Connect the ***mbNET.mini*** to a power supply (10 – 30 VDC).



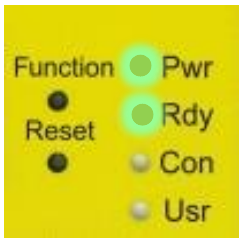
Make sure the polarity is correct.

After turning on the power supply, the LED **Pwr**lights up.
As soon as the system has been checked and started (duration approx. 25 sec), the **Rdy LED** flashes for the duration of the starting up process (approx. 90 sec). The ***mbNET.mini*** is now ready for operation.

T_0



T + 25 sec



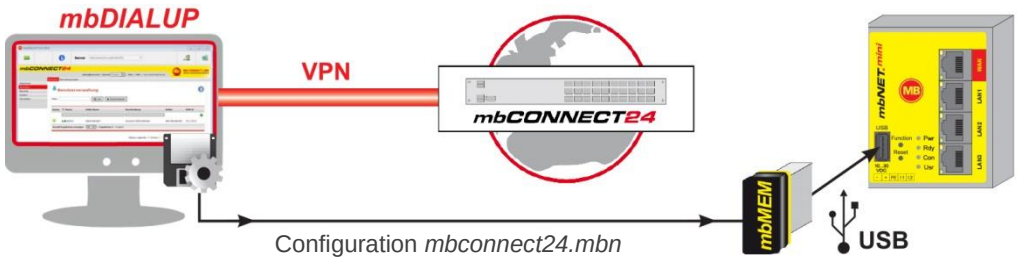
T + 90 sec

For further support on the ***mbNET.mini***, visit our online support forum at www.mbconnectline.com

7. Initial configuration

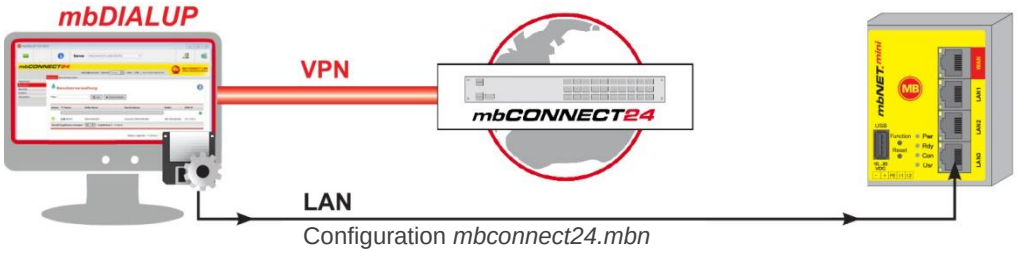
Because the ***mbNET.mini*** was designed as a portal device, the initial start-up takes place via the web portal ***mbCONNECT24***.
To do this, enter your ***mbNET.mini*** into the portal as a new device and create the initial configuration.
After entering the device into the portal, you have three ways to transfer the configuration:

1.) "Download configuration to PC" - via USB



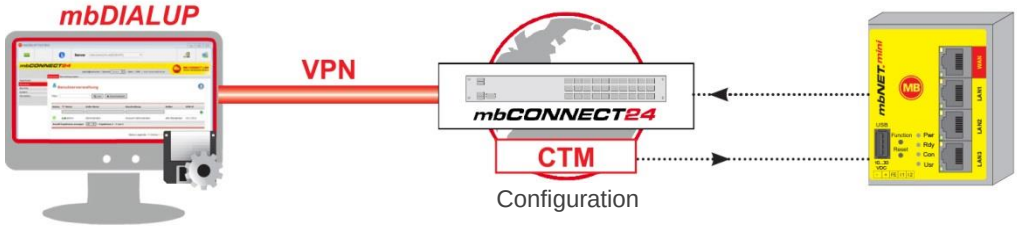
- Create an ***mbCONNECT24*** configuration and save it to a USB stick
- Insert USB stick into the USB port of the ***mbNET.mini***
- Transfer configuration to the***mbNET.mini***
  See ***section 8.1***

2.) "Transfer configuration to the device" - via *mbDIALUP*



- Create ***mbCONNECT24*** configuration
- Transfer configuration to the ***mbNET.mini***
  See ***chapter 8.2***

3.) "Transfer configuration to the CTM (Configuration Transfer Manager)" - via CTM



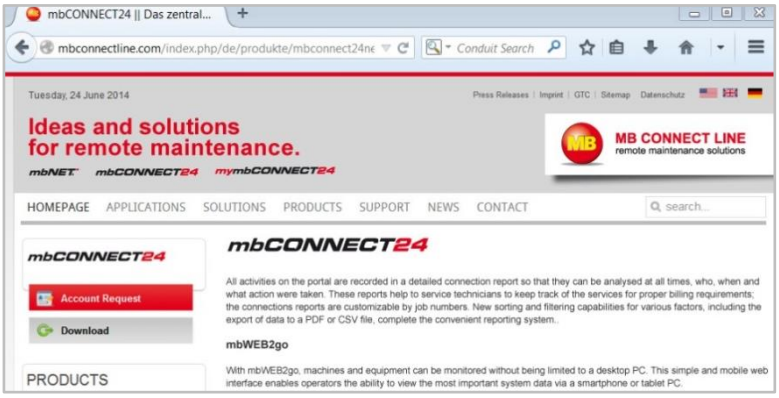
- Create an ***mbCONNECT24*** configuration and save it to the CTM
- Connect PC to ***mbNET.mini*** and call up WEB-Gui 192.168.0.100.
- Carry out the initial configuration following the wizard
- After the configuration has been carried out successfully, the ***mbNET.mini*** will collect the configuration saved on the CTM itself
  See ***section 8.3***

7.1 Login mbCONNECT24.net

Please go to www.mbconnect24.net to download the software required for secure connection to the portal.

If you still cannot access the portal, simply register under "**Request Access**".
Once you have registered, you will receive an email containing your access details.

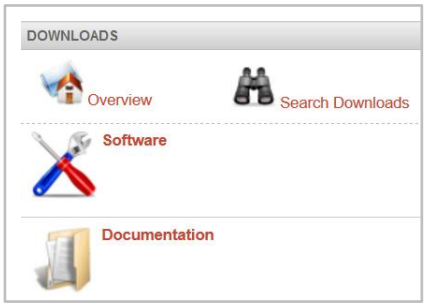
Click on "**Download**" to access the secure Downloads area.



7.2 Software installation

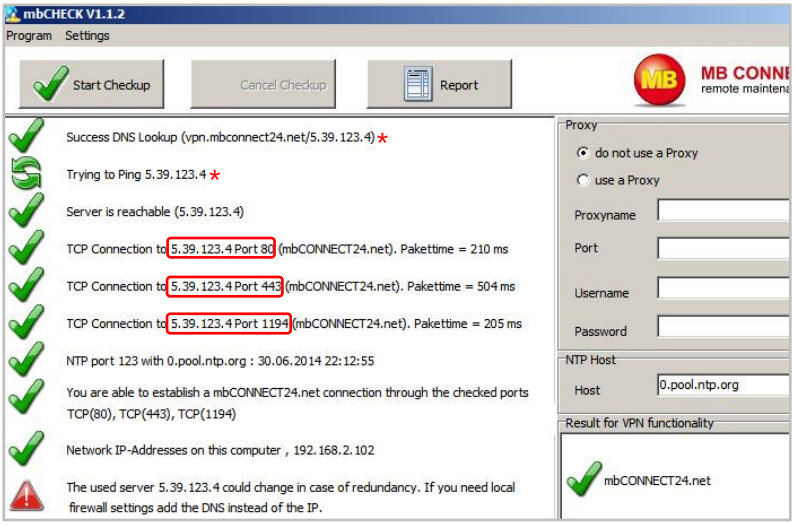
Under the category "**Software**", download the programs
"*setupmbdialup*" and
"*mbcheck USA / CAN*"
or
"*mbcheck EUROPE*".

If, when logging in to ***mbCONNECT24***, you selected the server location **USA/Canada** you will need the "*mbcheck USA / CAN*" file.
If you selected the **Europe** server location, you will need the "*mbcheck EUROPE*" file.



7.3 mbCHECK

After downloading and extracting the two files, you will first need to run the "*mbcheck.exe*" program.
The program checks that at least one of the 80TCP, 443TCP or 1194TCP ports is enabled in the firewall.
At least one of these ports is needed by ***mbDIALUP*** and the ***mbNET.mini*** for connection to ***mbCONNECT24***.
You will then be notified whether connection via ***mbDIALUP*** to the ***mbCONNECT24*** portal is possible.



* The data vary depending on the server selected:
(vpn.mbconnect24.net/5.39.123.4) = EUROPE server selected
(vpn.mbconnect24.us/198.50.162.20) = USA/CAN server selected

7.4 mbDIALUP

The ***mbDIALUP*** client software enables you to establish a secure VPN connection to the ***mbCONNECT24*** portal server.

To install ***mbDIALUP***, run the "*setupmbdialup.exe*" program and then start the program.

During the installation process, you must ensure that you are logged in as Administrator.

7.4.1 Selecting the server

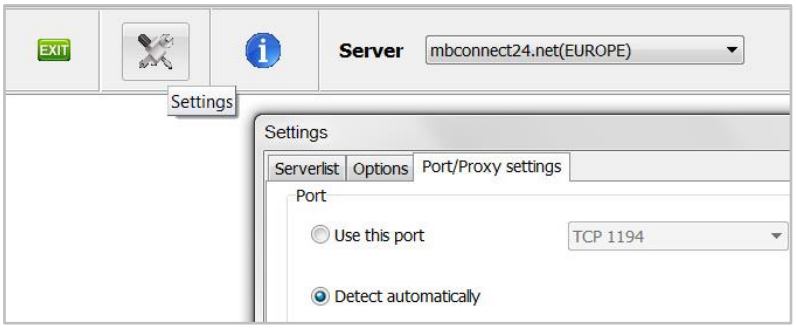
Before you connect to the portal server for the first time, please select your mbconnect24.net server.
Please also make sure that you select the same server as when you logged in to mbCONNECT24 under "Server Location".

If you select the wrong server, it is not possible to establish a connection.

If, for example, you selected Europe as the server location when logging in to ***mbCONNECT24*** and you now select "mbconnect24.us (USA/CAN)", you will receive an "Authentication failed" error message when trying to connect to the portal.

7.4.2 Access via the proxy server

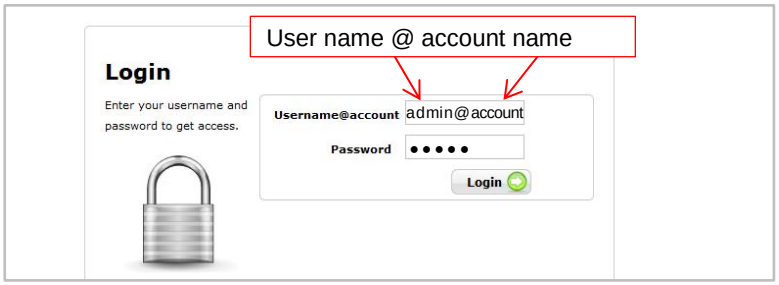
If the Internet can only be accessed via a proxy server, the relevant settings can be applied in the menu "**Settings**", submenu "**Port/Proxy settings**".



7.5 mbCONNECT24 login

You can now log in to the portal with the user data (username, password) that were sent to you when you registered.

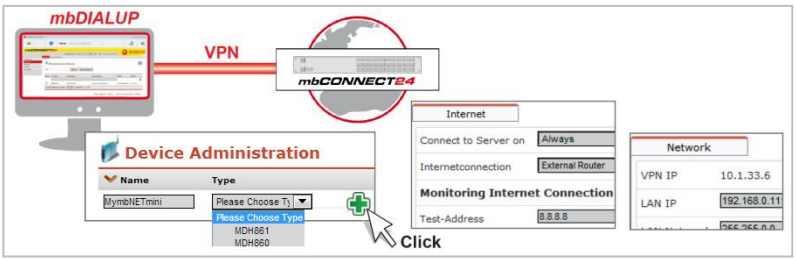
A secure VPN connection to your account on ***mbCONENCT24*** is now established.



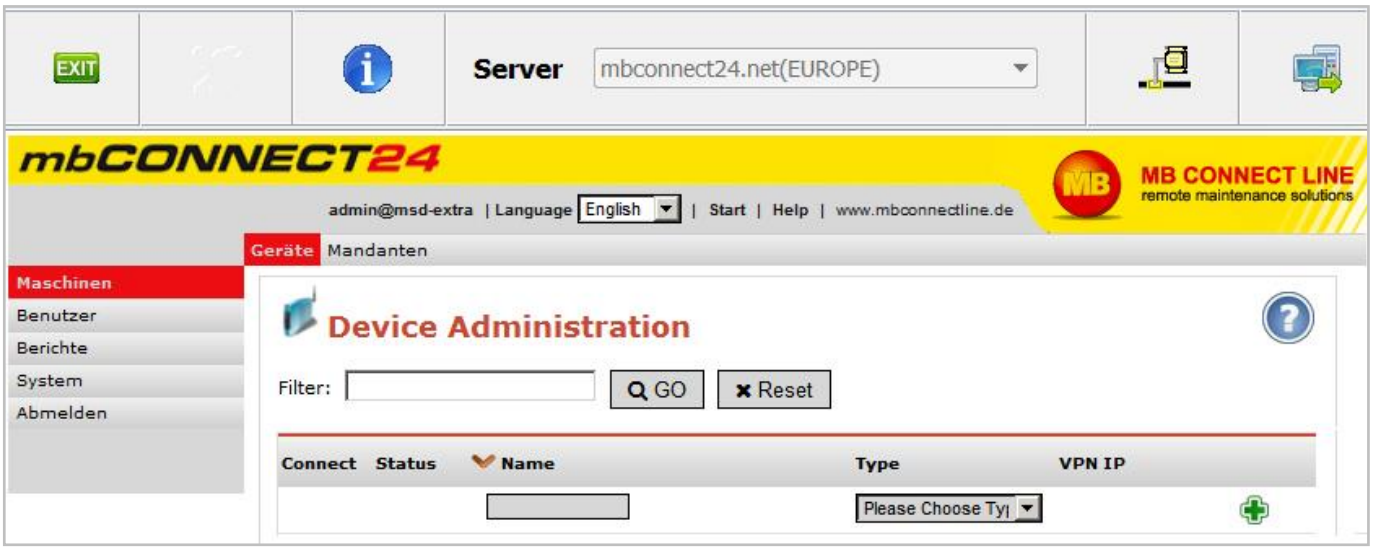
7.6 *mbCONNECT24 Configuration*

Here you can:

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

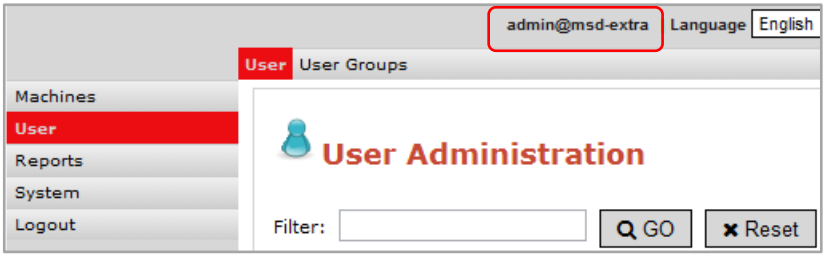


If the VPN connection is established, the browser window of your account opens on ***mbCONNECT24***.

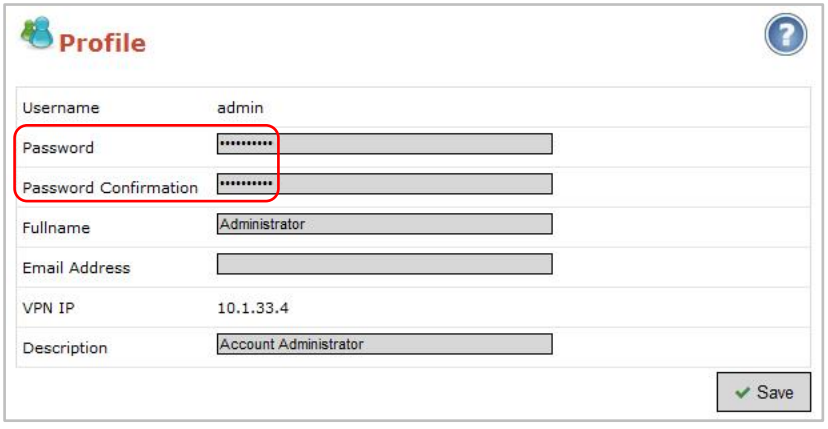


7.7 Changing your user data/password

Before you start the configuration, you must first go to **User Administration** (User) and change your password.
To do this, click on your username in the information bar at the top



and change your password in the **Profile** window that appears next.



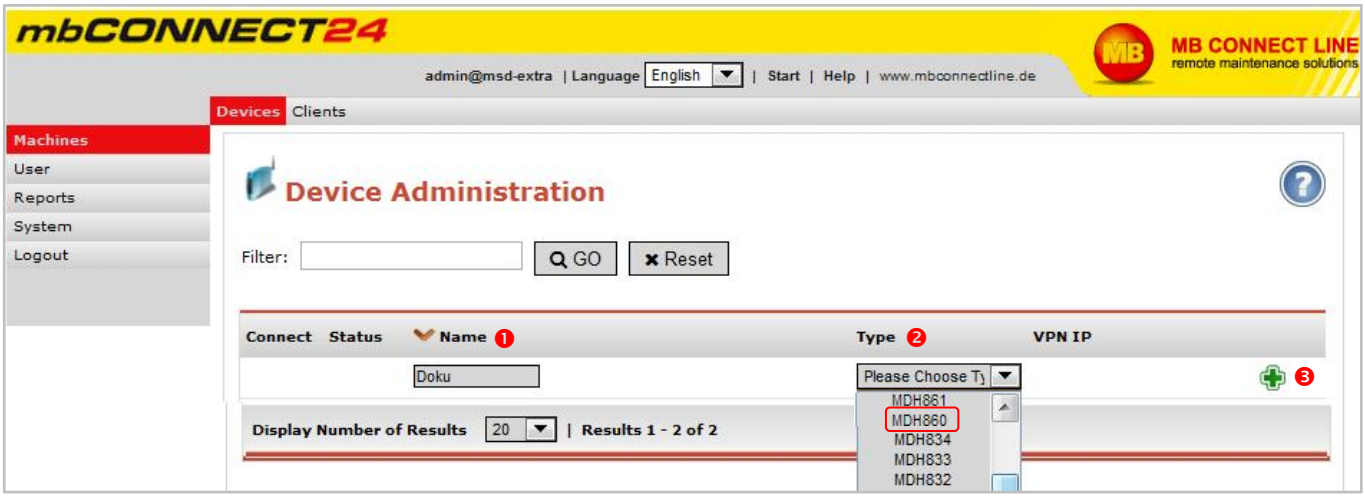
Once you have saved the changes, your new password is effective the next time you log in to the portal.

7.8 Adding a new device

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

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.



7.8.1 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!

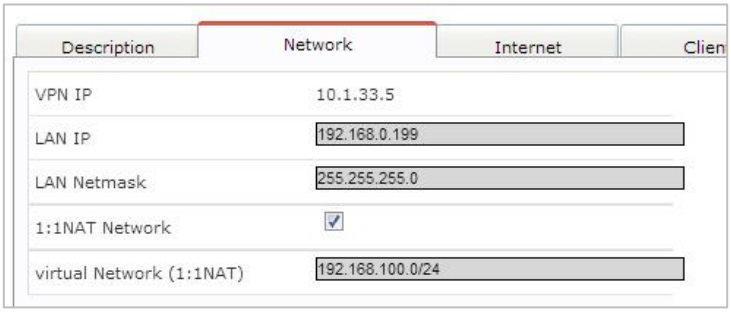
Serial number
The device's serial number can be entered here. However, as soon as the device connects to the portal for the first time, it is automatically entered.

Description
For a better overview, enter a short description of the device here.

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

7.8.2 Network

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



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

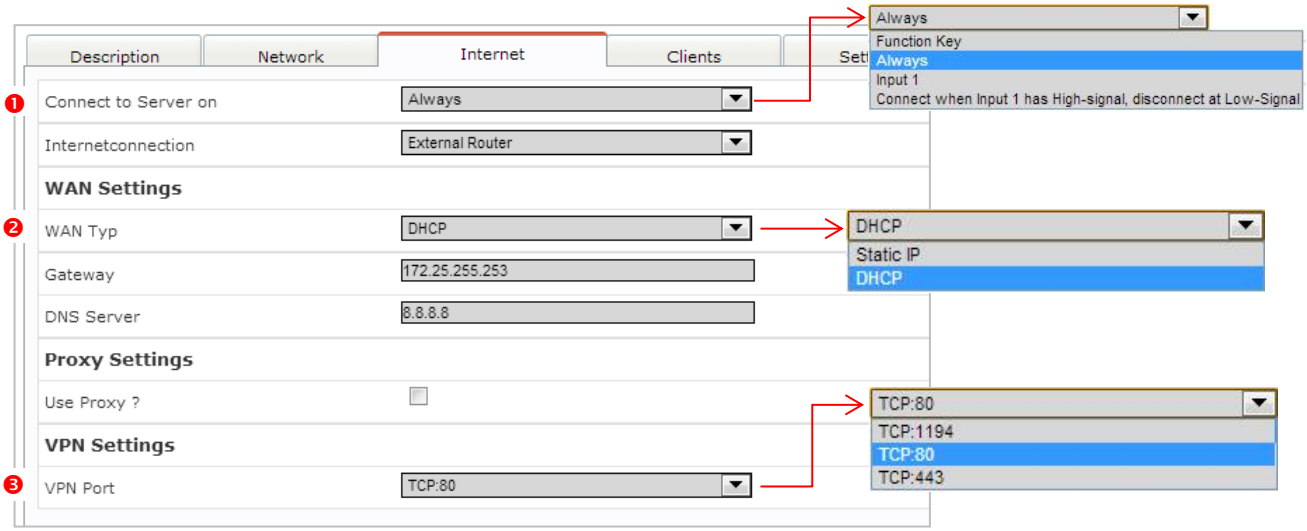
Activate the "1:1NAT Network" when both tunnel end points have the same network address to enable communication through both networks.

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

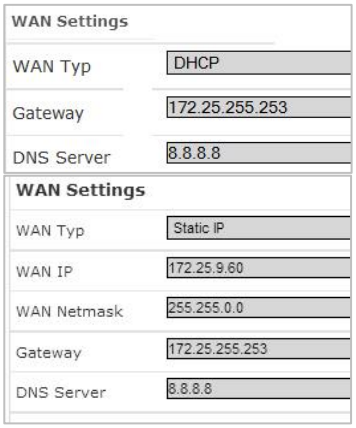
7.8.3 Internet

7.8.4 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
❸ Which VPN port should be used (which of the three ports is free has been established via ***mbCHECK***)



❷ 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.

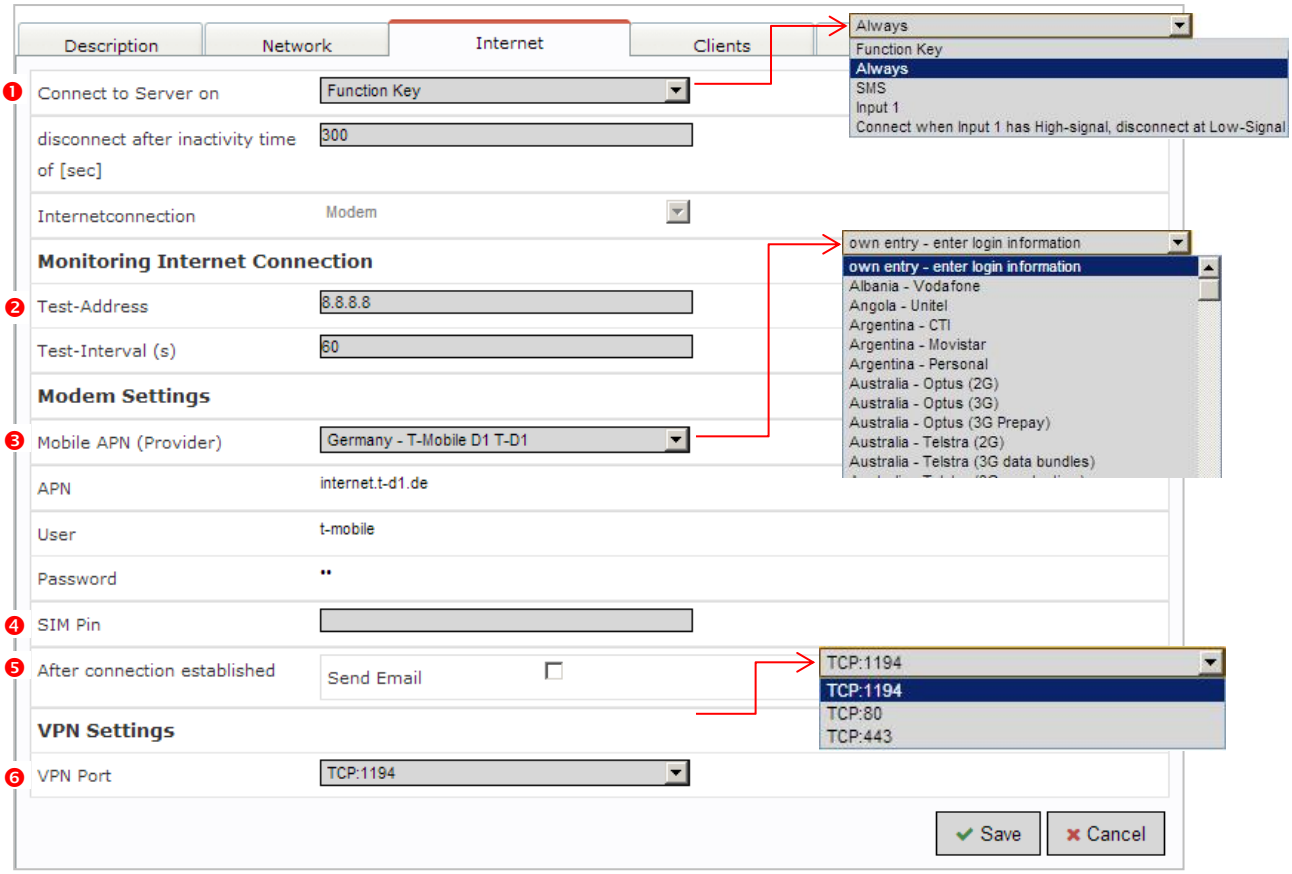


❷ WAN settings for **static IP**
Select this setting if connection to the Internet is already established via an existing router that is not acting as a DHCP sever, or if no server is set up to assign addresses. You should also select this setting if you have received a static address from your ISP, e.g. if you have a leased line. A DNS server address must however still be entered.

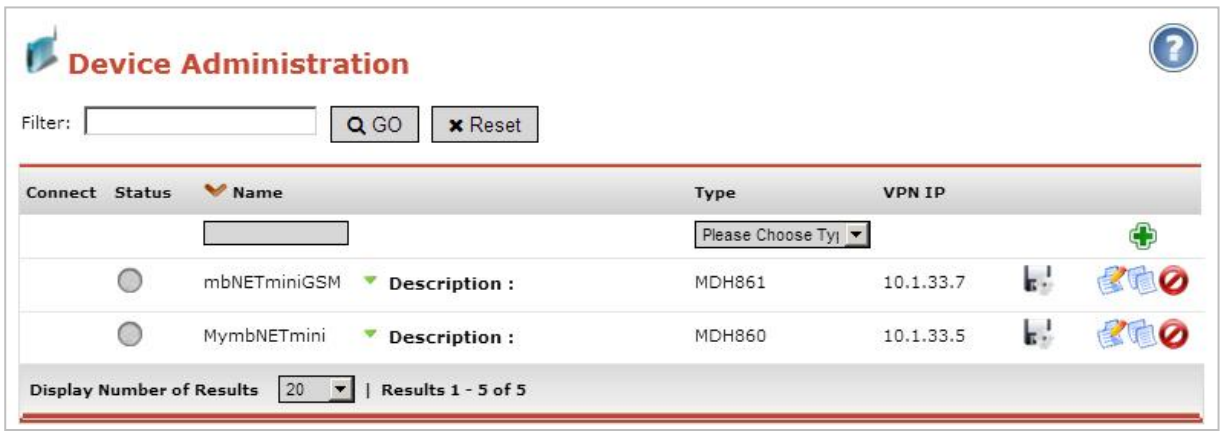
WAN IP: IP address of the router connected to the WAN port.
WAN subnet mask: Enter the subnet mask.
Gateway: Enter the gateway
that connects you to the Internet, i.e. the IP address of the existing router here.

7.8.3.2 GSM device (MDH 861)

❶ Select when the device should be connected to the portal.
❷ Select a test address and the test interval to monitor the Internet connection.
❸ 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.
❹ If required, you can enter the SIM card PIN of the SIM card used here.
❺ If you want to be notified by email that you have successfully connected, check the box and enter your email address.
❻ Select which VPN port should be used (which of the three ports is free was determined by ***mbCHECK***).



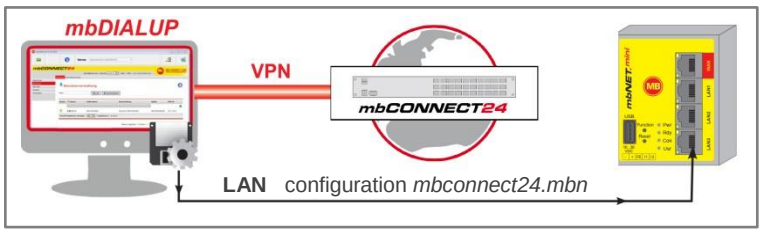
After saving your settings, you will see the new device in the Device Administration window.



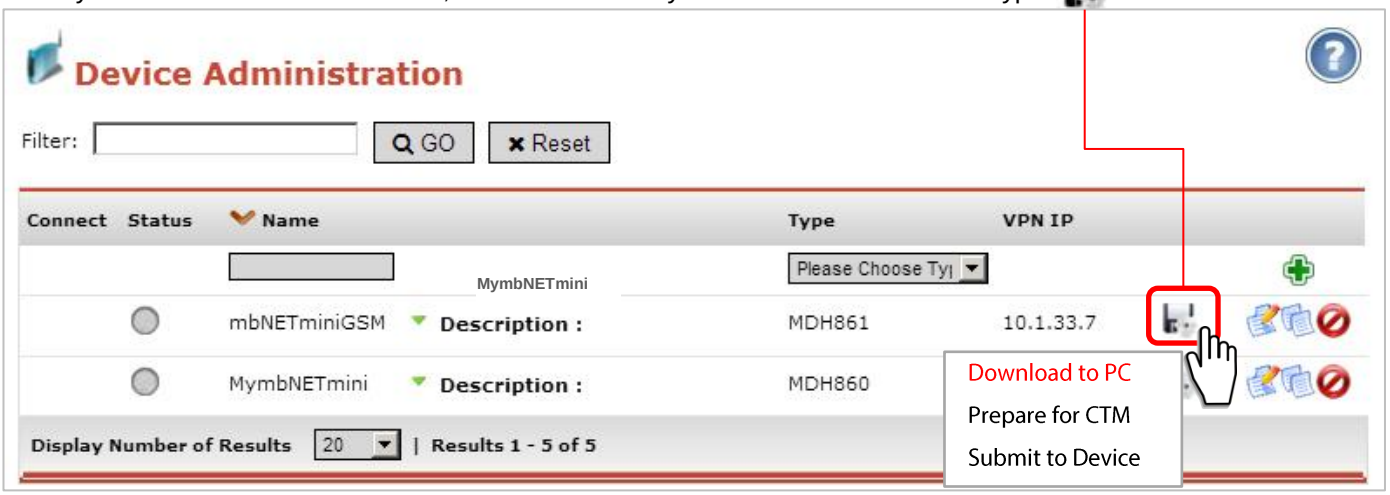
8. Transferring the configuration to *mbNET.mini*

The following options are available for transferring the configuration file:

- **Downloading configuration to PC**
- **Submit configuration to device**
- **Submit configuration to CTM**



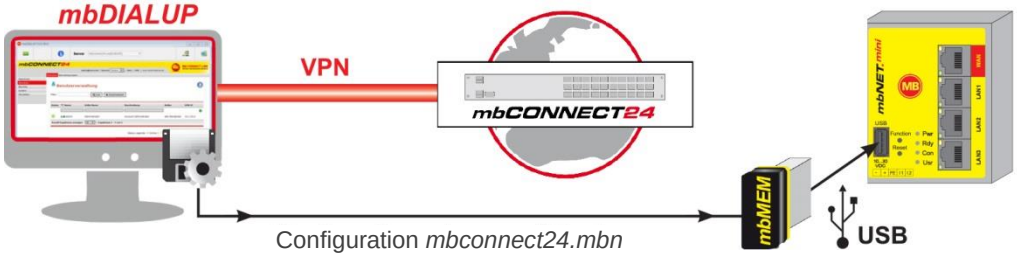
Once you have created a new device, click on the disk symbol to select the transfer type.



8.1 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 connected to it.



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.

8.1.1 Importing the configuration into the device

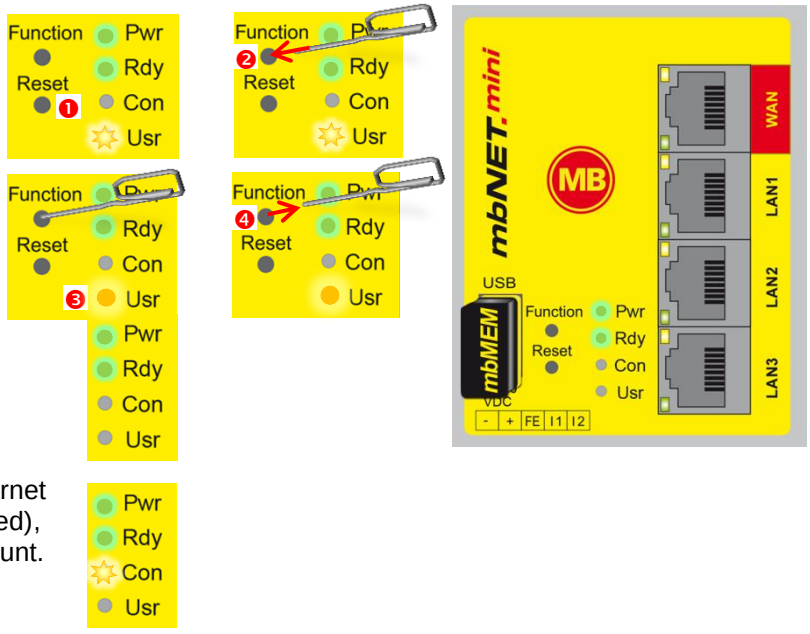
When the ***mbNET.mini*** is read to operate, insert the USB stick into the USB port of the device. The device will recognize the configuration file and show that through the slowly flashing LED **Usr** (flashing frequency: 1.5 Hz).

As soon as the LED **Usr starts to flash*** ❶, you must press the **Function** button ❷ within 10 seconds
*Flashing frequency = 1.5 Hz

and hold down **until** 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**".

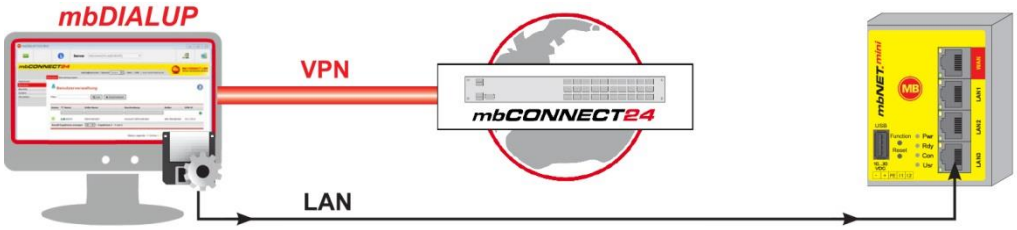


If the flashing frequency of the LED **Con** is 3 Hz, the device is attempting to log into the portal. If the login has been successful, the flashing frequency is reduced to 1.5 Hz.

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 portable USB stick.
Once the "mbconnect24.mbn/-.mbnx" configuration file has been imported, it is automatically renamed and is now stored on the USB drive as "***X***mbconnect24.mbn/-.mbnx".

8.2 Transferring configuration to the device - via mbDIALUP

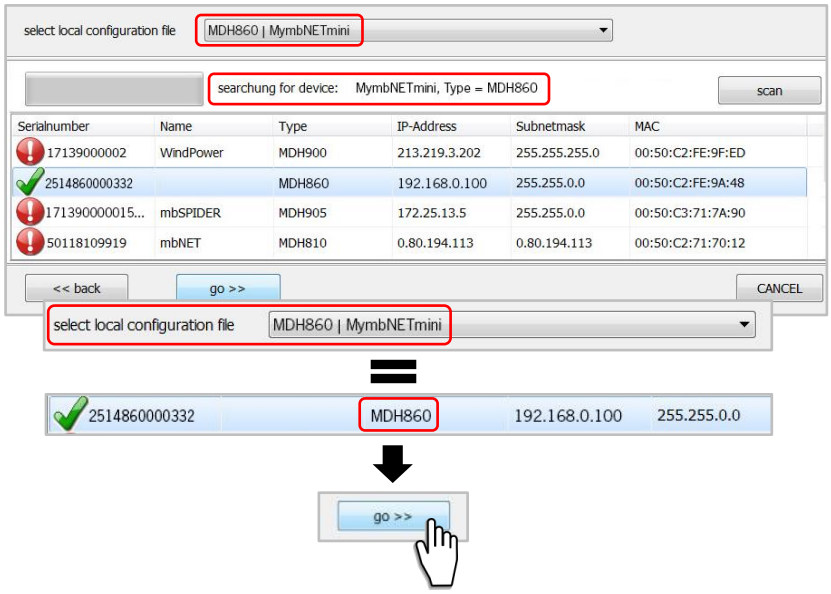
*For this, the**mbNET.mini** must be accessible from a PC on the LAN, irrespective of its LAN IP, and the computer must have a connection to **mbCONNECT24** portal.*



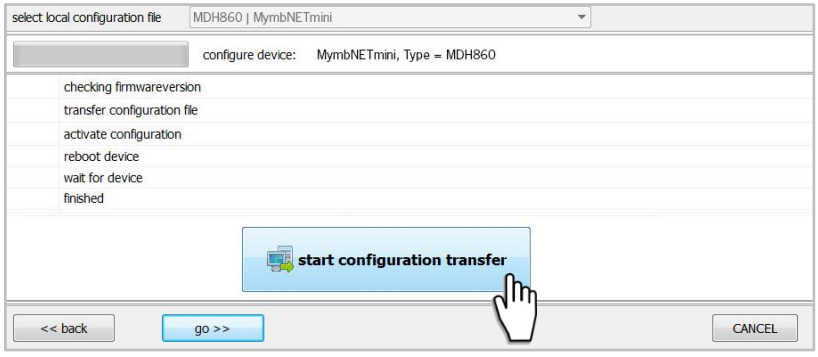
Configuration *mbconnect24.mbn*

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

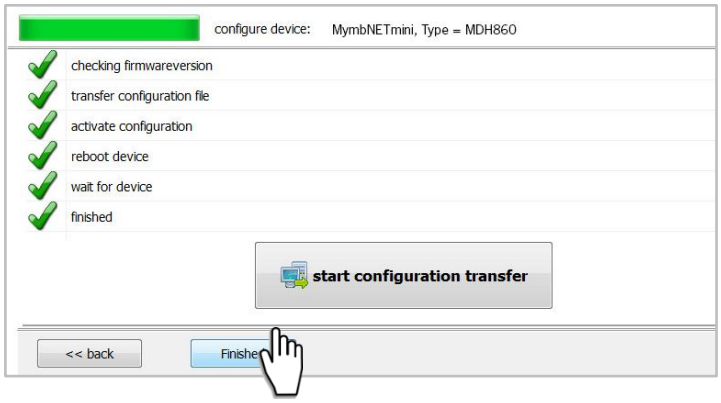


In the next window click on "**start configuration transfer**"



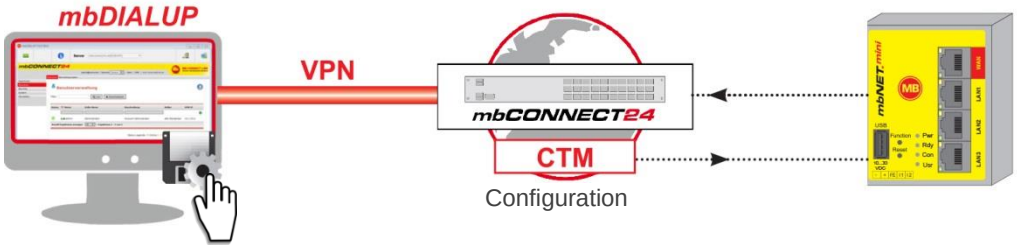
The settings from ***mbCONNECT24*** are now copied to the device.

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



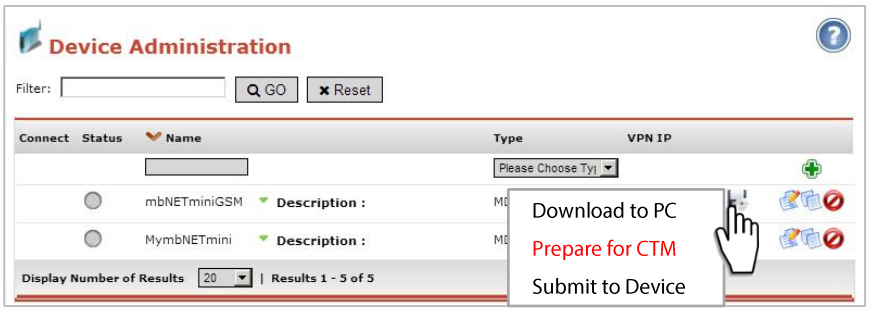
8.3 Transfer configuration to the device - via CTM (Configuration Transfer Manager)

*Here the **mbCONNECT24** configuration is placed in the CTM 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.*

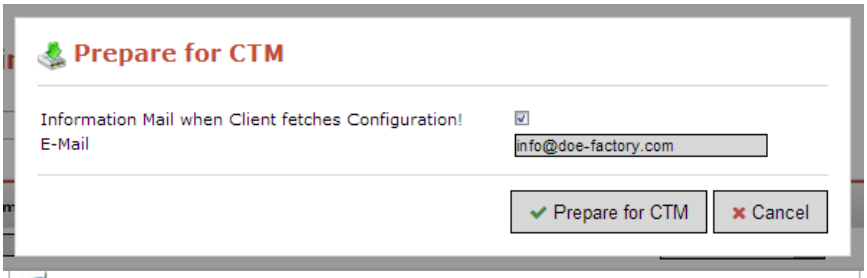


8.3.1 Creating the portal configuration for the CTM

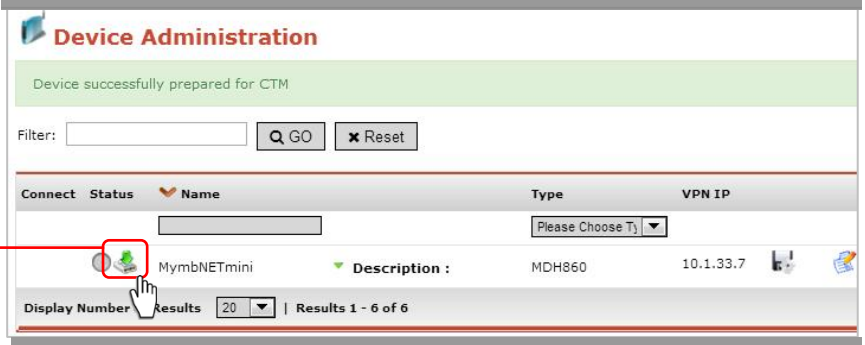
After creating the configuration (see section **7.8 Adding a new device**), when you enter the serial number of your ***mbNET.mini*** (menu tab **Description**, see section 7.8.1), select the option *"Submit configuration to CTM"*.



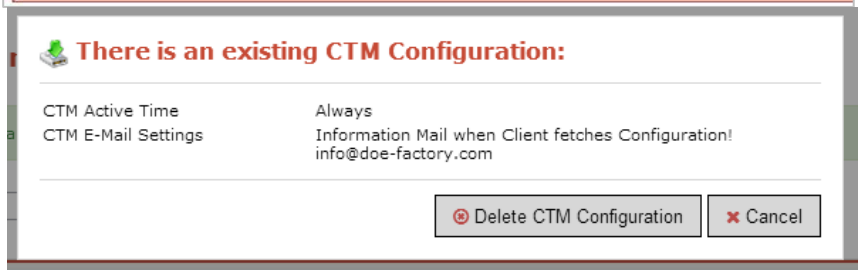
In the next window, select whether a notification email should be sent and to which address as soon as the device has collected the configuration.



After confirming via the interface *"Transfer configuration to the 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.



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



8.3.2 Initial configuration via the web interface of the mbNET.mini

Connect one the ***mbNET.mini*** to the power supply and connect the device to the Ethernet interface on your configuration PC.

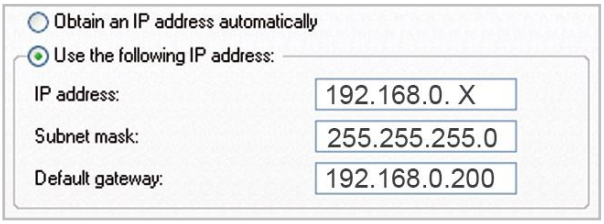
The configuration PC and the ***mbNET.mini*** must be in the IP address range (192.168.0.X).

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).

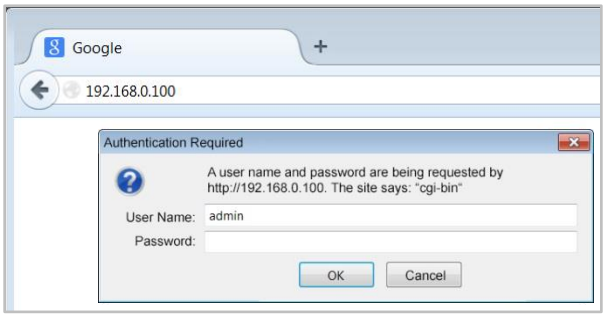
- Your computer's IP address must be in the address range "192.168.0.X", the subnet mask must be identical to that of the ***mbNET.mini*** (255.255.255.0). You must enter the IP address of the ***mbNET.mini*** (192.168.0.253) as the default gateway and as the preferred DNS server.



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

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

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

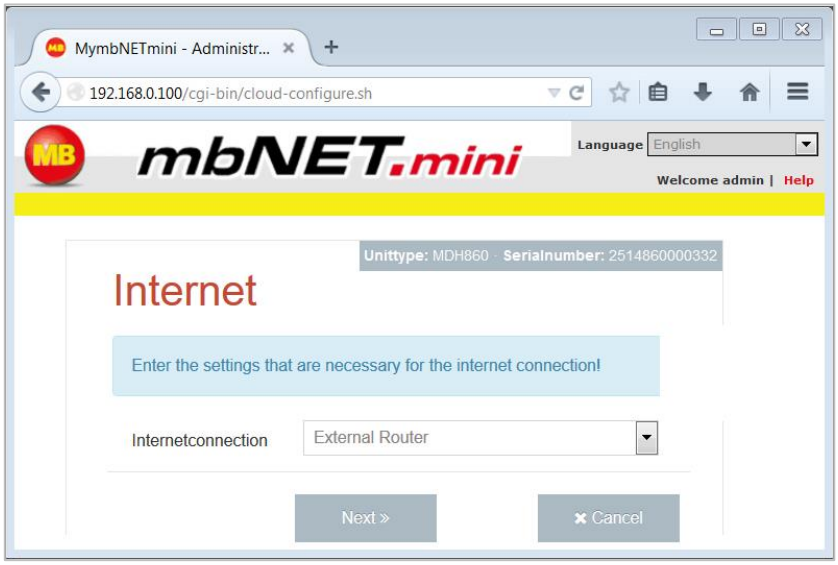


Please enter the following details to log into the ***mbNET.mini***:
User name: admin
Password: (no password required)

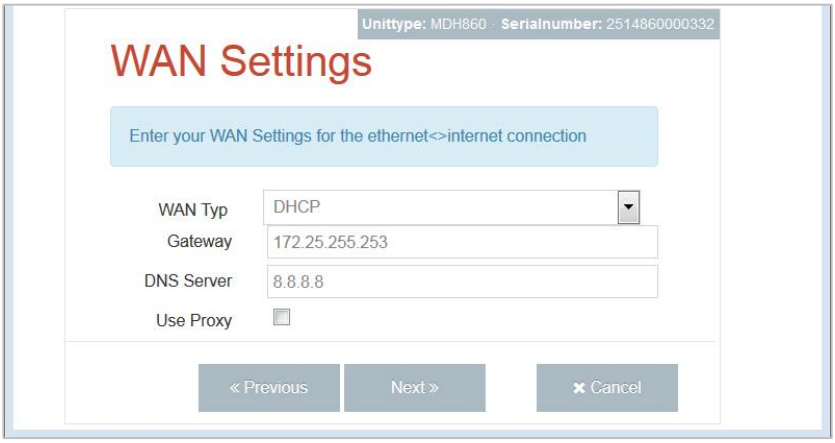
When selecting the **Internet connection** for WAN devices (MDH860), you can only select the option "External router/Firewall".

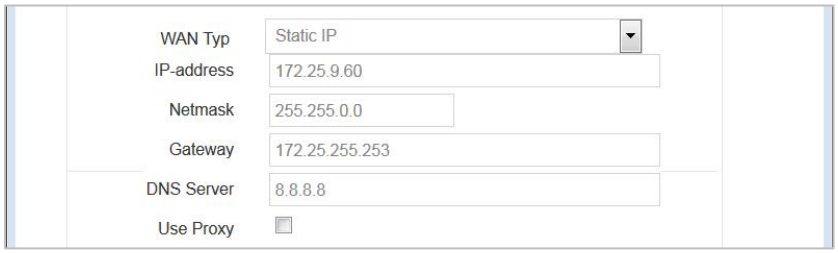
For GSM devices (MDH861), you can only select the option "Modem".

Click "Next>>" to continue.

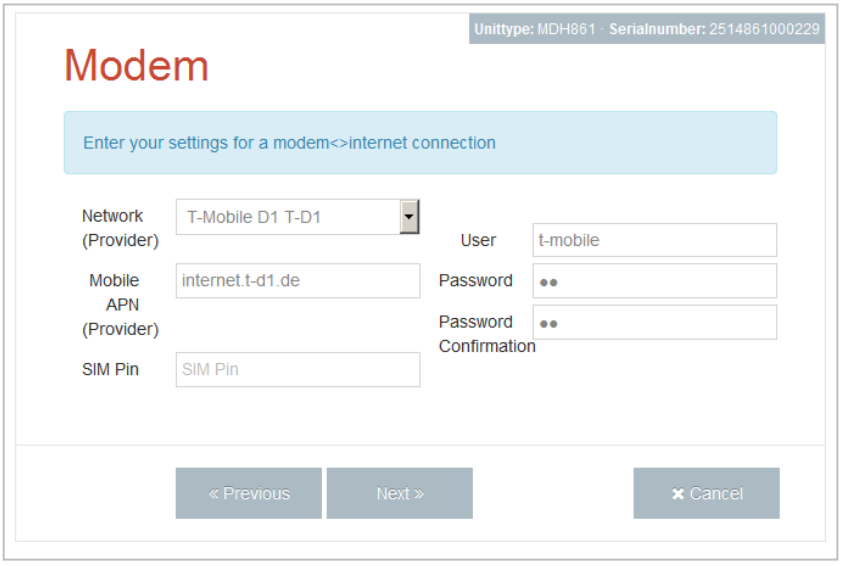


WAN devices (MDH860):
In **WAN Type** choose between DHCP and Static IP.





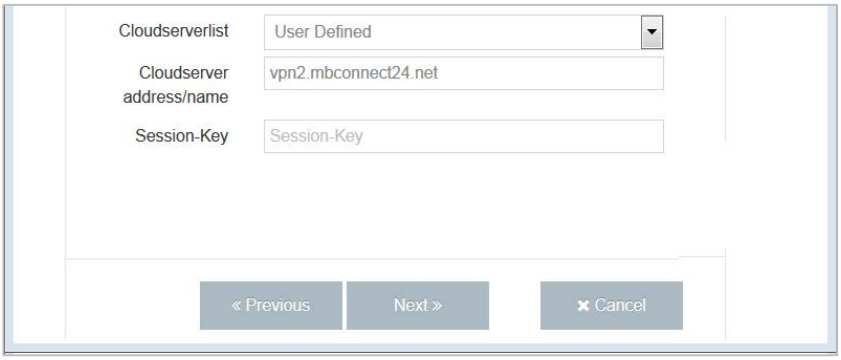
GSM devices (MDH861):
Enter the APN provider and the SIM PIN here.



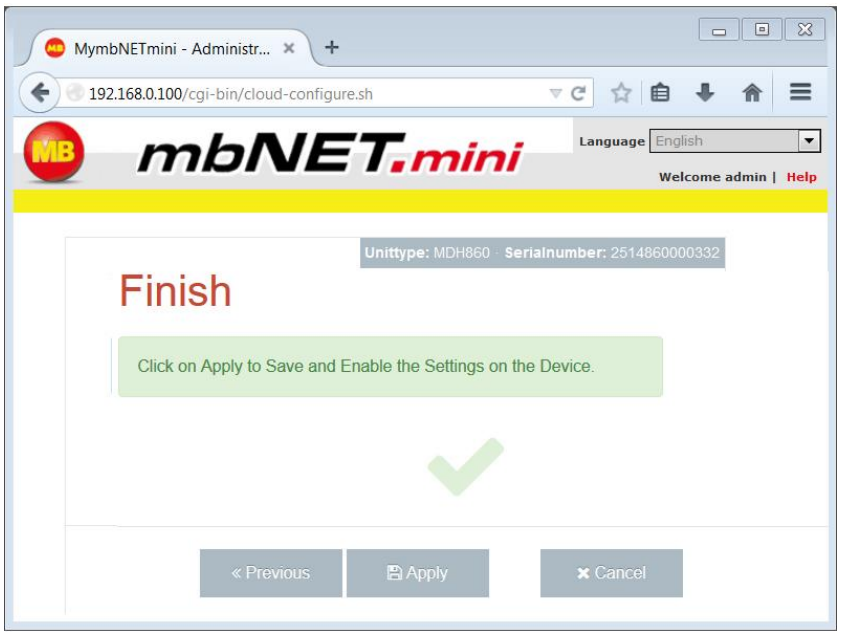
All devices:
Choose your portal server from the **Cloud-serverlist**.

This selection should correspond to the server location you entered when registering with ***mbCONNECT24***.
For the servers "Europe" and "USA/Canada", the addresses are preset.

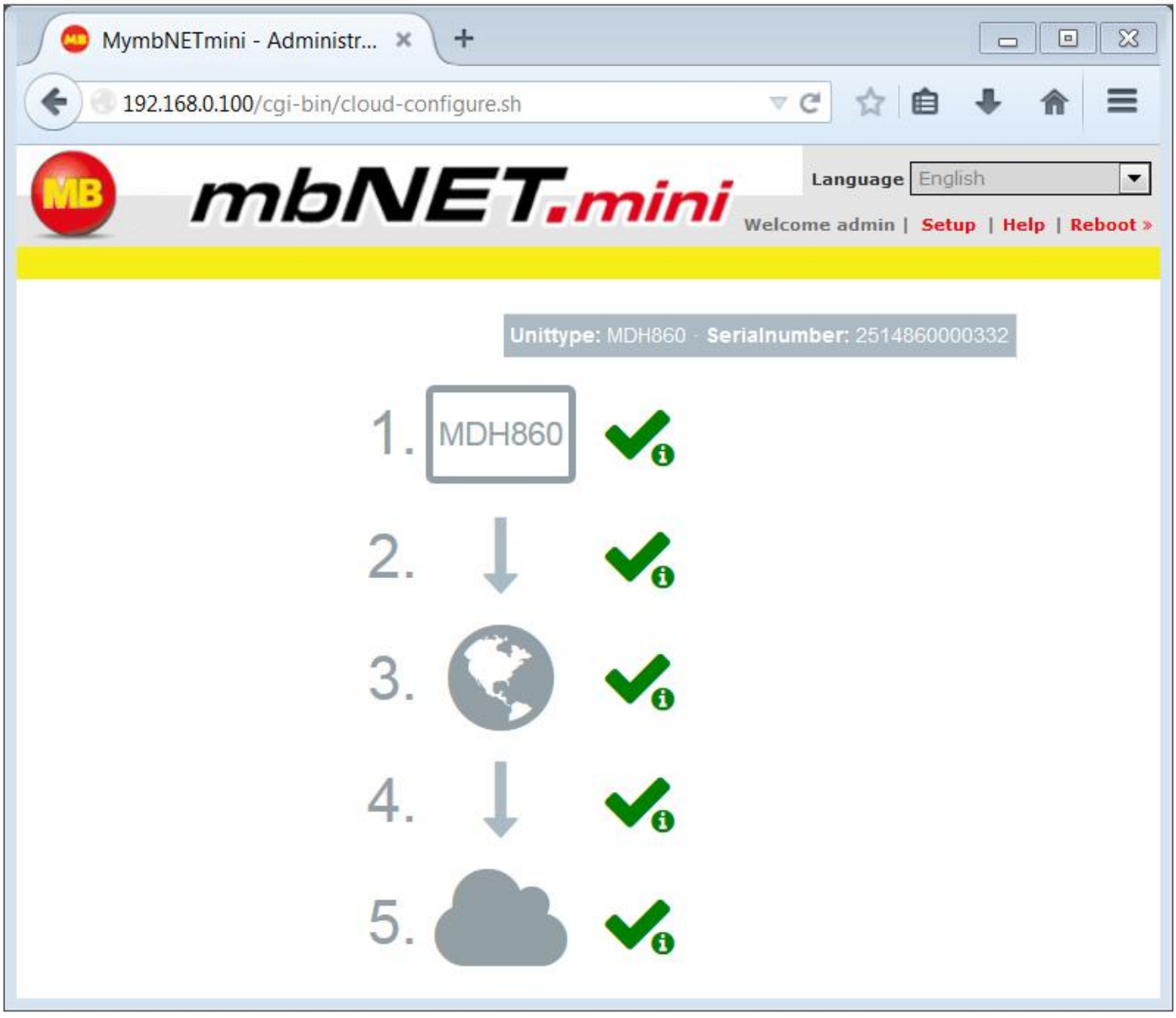
If you operate your own server (mymbCONNECT.midi/-.maxi/-.hosted), you must enter your URL in **Cloudserver address/name**.



All devices:
By clicking Apply, the ***mbNET.mini*** status page will be shown on the screen.



All devices:
On the status page, all steps required to set up a connection between the ***mbNET.mini*** and the portal are shown.
When all steps have been successfully completely, each step has a green check mark.
The ***mbNET.mini*** now established a connection to the portal and collects its configuration from the CTM.



9. Operation

Once the router has been configured, the status page always starts with the list of steps.
In the upper part of the page you will find the following items:

Language selection German/English

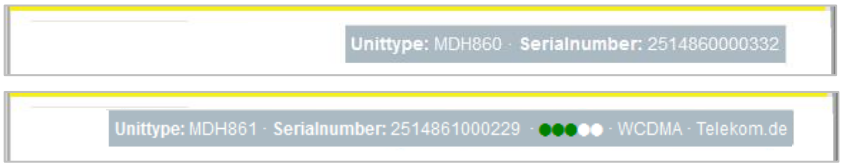
Open the set-up menu

Reboot the device

Depending on the type of device, the following is shown here:

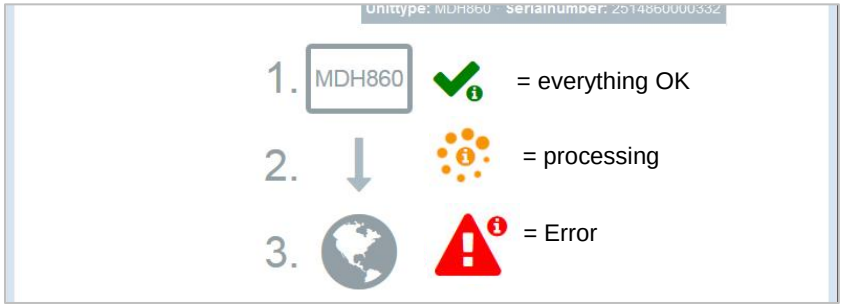
WAN: Type of device, serial number

GSM: Type of device, serial number, signal strength, network, provider



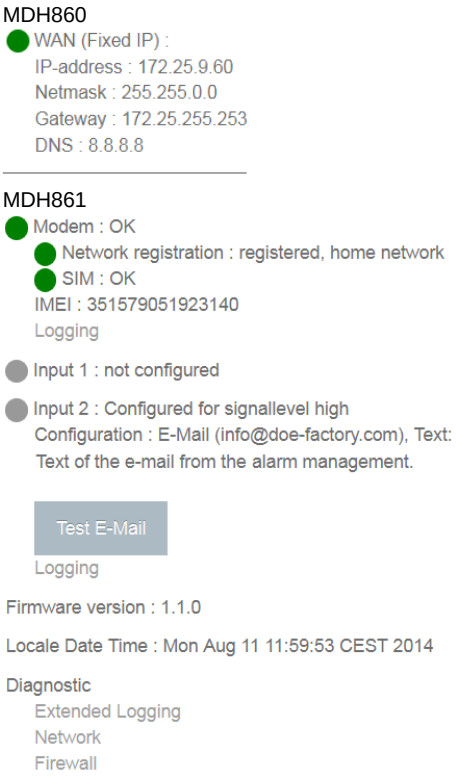
You can see detailed information about the individual steps here.
Information on the individual steps can Be obtained by clicking on the symbol shown as:

green check mark, orange circle or red triangle



9.1 Step 1 – Device

Depending on the type of device, all WAN or modem interface data are shown first.



Input 1 can only be configured for establishing the connection. 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).

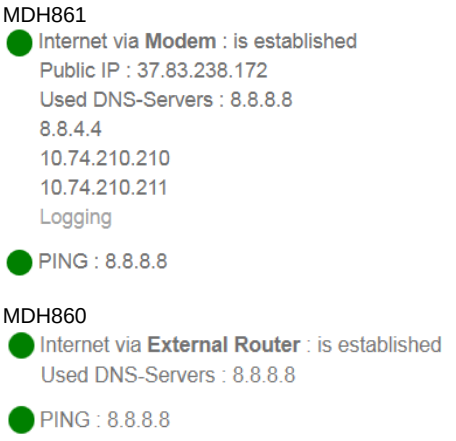
Input 2 can be used to send emails, text messages, Internet text messages or to start a reboot. Once it has been configured accordingly, the description "Input 2" is shown.
The state of the signal is shown with the prepended soft-LED (grey = 0/low, green = 1/high). **Configuration**
If an email, text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

Displays the **firmware version**
Displays the **date/time**

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 and information in our FAQ.

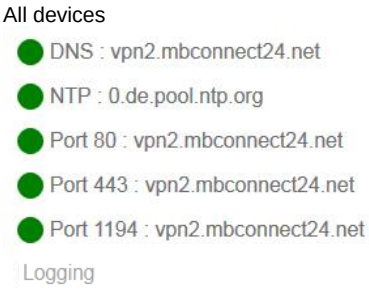
9.2 Step 2 – Connecting to the Internet

First the connection settings are displayed, depending on the type of connection; e.g. whether Input 1 is being waited for. With dial-up connections to the Internet (e.g. GSM), the provider assigns an IP address and DNS server. This can be seen in the second line.
The LED shows whether the device is connected to the Internet.
In the line "PING", the test server entered is displayed. The LED signals the connectivity (grey = not pinged yet, green = available, red = not available).
Additional information can be obtained by clicking on the "Logging" link. These data help us to provide additional support when dealing with problems and information in our FAQ.



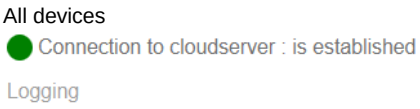
9.3 Step 3 – Availability of the portal server

Information about the current availability of the portal server and the NTP is shown here.
The LED signals the availability of the set server and the port (grey = not tested yet, green = available, red = not available).
The NTP will only be tested if it is also activated in the configuration.
Additional information can be obtained by clicking on the "Logging" link. These data help us to provide additional support when dealing with problems and information in our FAQ.



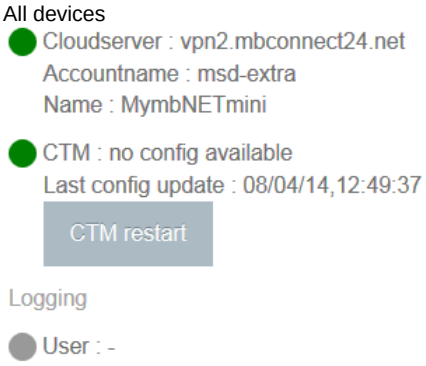
9.4 Step 4 – Connecting to the portal server

First the connection settings are displayed, depending on the type of connection; e.g. whether Input 1 is being waited for.
The LED signals the state of connection to the cloudserver (grey = not active, green = available, red = not available).
Additional information can be obtained by clicking on the "Logging" link. These data help us to provide additional support when dealing with problems and information in our FAQ.



9.5 Step 5 – Information on the CTM, cloudserver and user

Information about the CTM configuration, the cloudserver account data and last used connected can be checked here.
The button "Restart CTM" asks for a new configuration in the CTM again.
Additional information can be obtained by clicking on the "Logging" link. These data help us to provide additional support when dealing with problems and information in our FAQ.

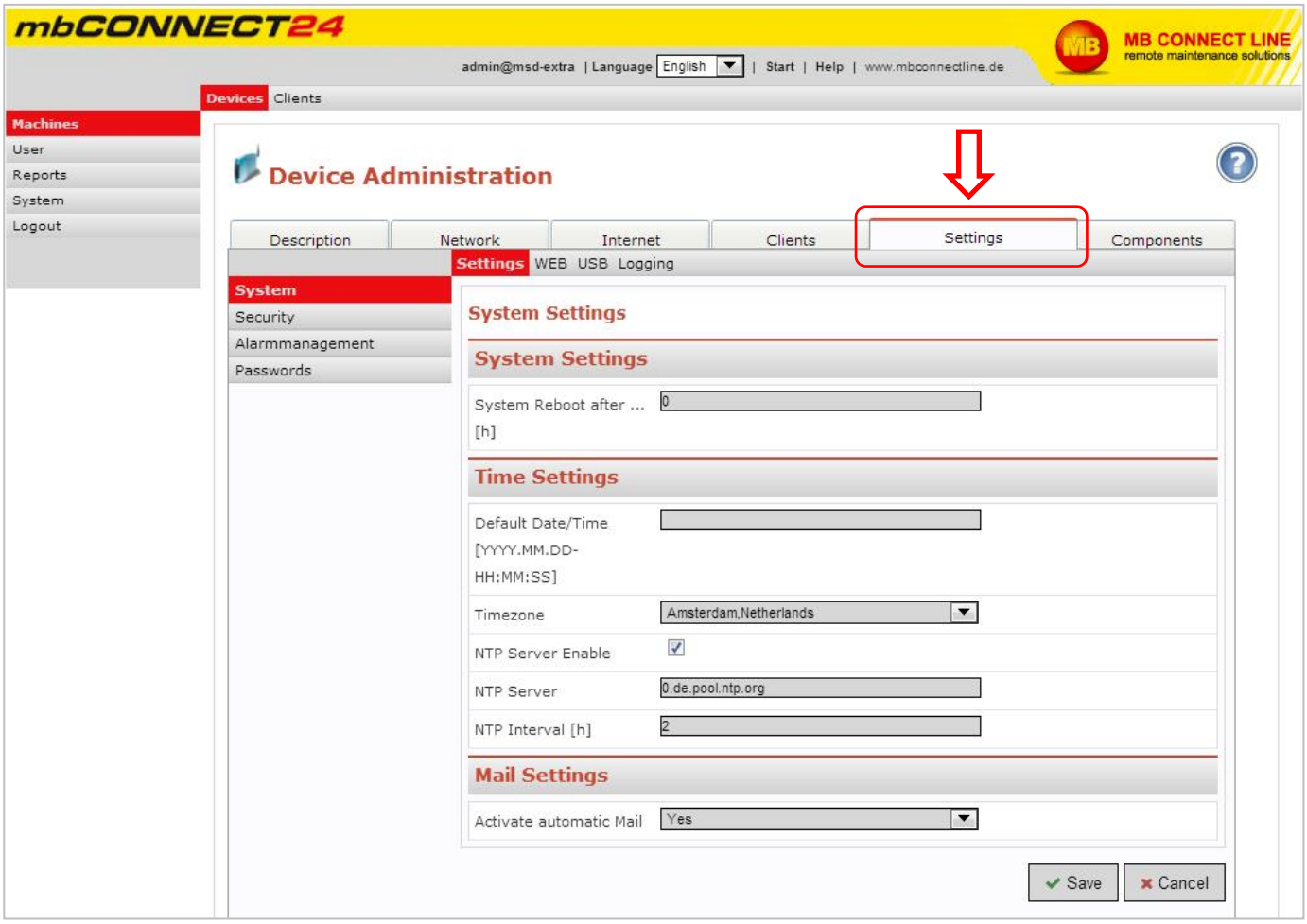


10. Configuring the router in the portal

The router can only be configured in the portal server. When the router is connected to the portal online, all settings are automatically transferred to the router via CTM and activated.
Depending on how you change the settings, it can result in ending the connection.
If the router is not online, the settings must be transferred to the CTM via the disk symbol. The router automatically gets the current configuration from the CTM the next time a connection is established.
If the router has never been configured, the portal settings must first be transferred to the router as described in Getting started (*see chapter 7. Getting started*).

The settings for the router can be chosen in the portal in *Machines/ Devices/* ***Settings*** */ System / Settings*.

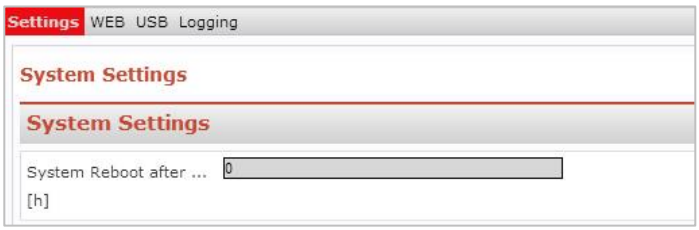
These and all changes that you make for the ***mbNET.mini*** in the portal will only take effect when the settings/changes made are transferred to the device as a configuration.



10.1 System – Settings

10.1.1 System settings

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.*

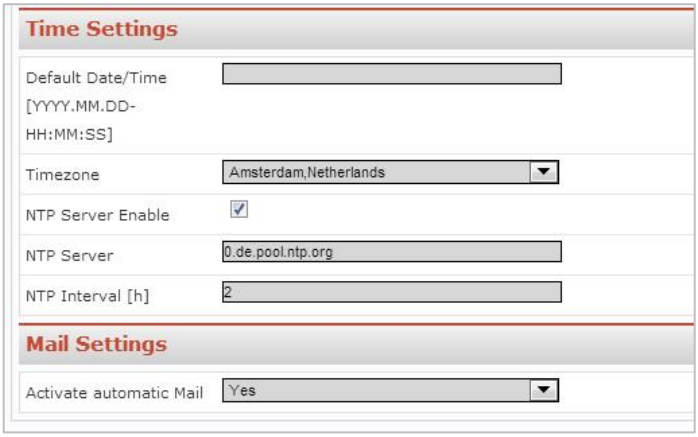


10.1.2 Time settings

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

Choose your time zone.

If "Activate NTP server" has been checked, the 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

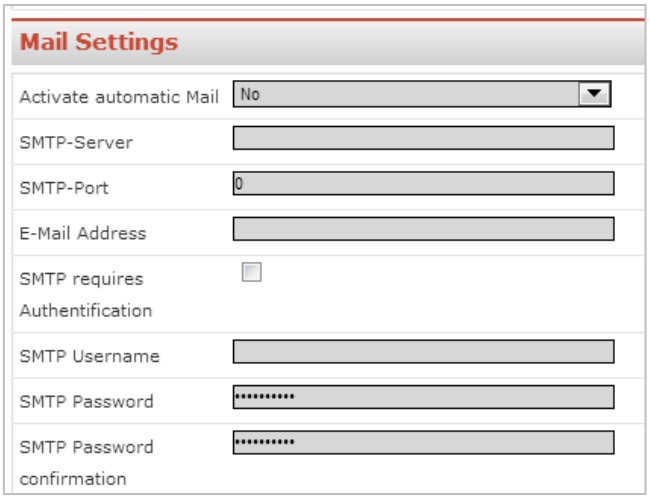
- "Activate NTP server" has been checked and
- a valid NTP server has been entered and
- the value for the NTP interval is > 0.

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

10.1.3 Email settings

Selecting "**yes**" in "Activate automatic mail" means that the router will use MB Connect Line's mail server and fixed parameters.

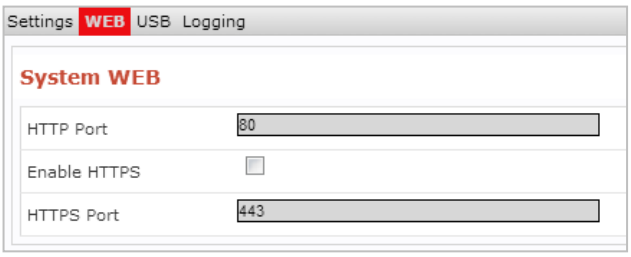
Selecting "**no**" in "Activate automatic mail" means that you must enter the necessary details of your mail server.



Designation	Function
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).
Email address	Enter the appropriate sender address for emails from the router here.
SMTP requires authentication	The box should be checked or unchecked depending on the ISP. Ask your ISP for the correct setting.
Users Password	A user name and password are required for SMTP server authentication, i.e. if the router wants to send an email to the SMTP, it may have to first authenticate itself.

10.2 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.

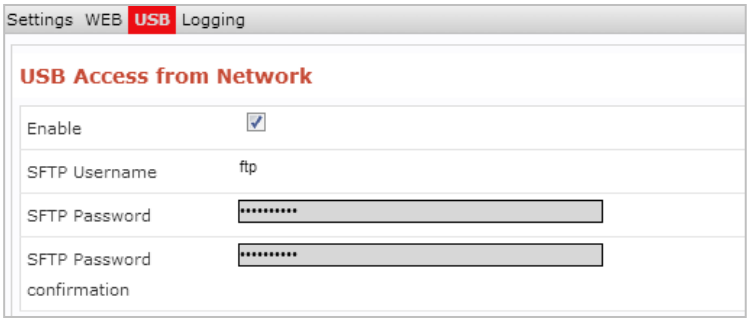


Designation	Description
HTTP Port	 The standard port for HTTP requests is TCP 80. You can however select another port if you need this port for your OpenVPN connection or if it is already being used for another purpose. If you do this, please note that you will need to enter the selected port in the 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 computer (here: port 443).

10.3 System – USB

10.3.1 USB access from the network

When *"Active"* is checked, the USB memory can be accessed via an SFTP client.
Default settings:
"SFTP user" ftp
"SFTP password" ftp

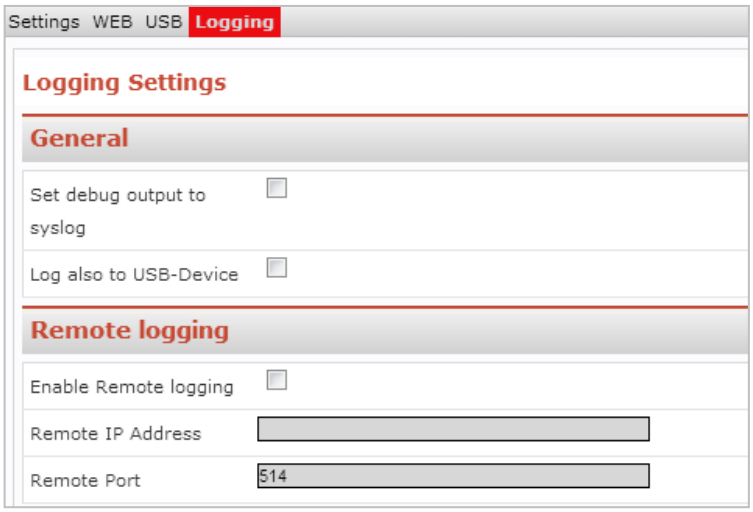


10.4 System – logging

10.4.1 General

The logging is extended by the "*Debug information*".

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").



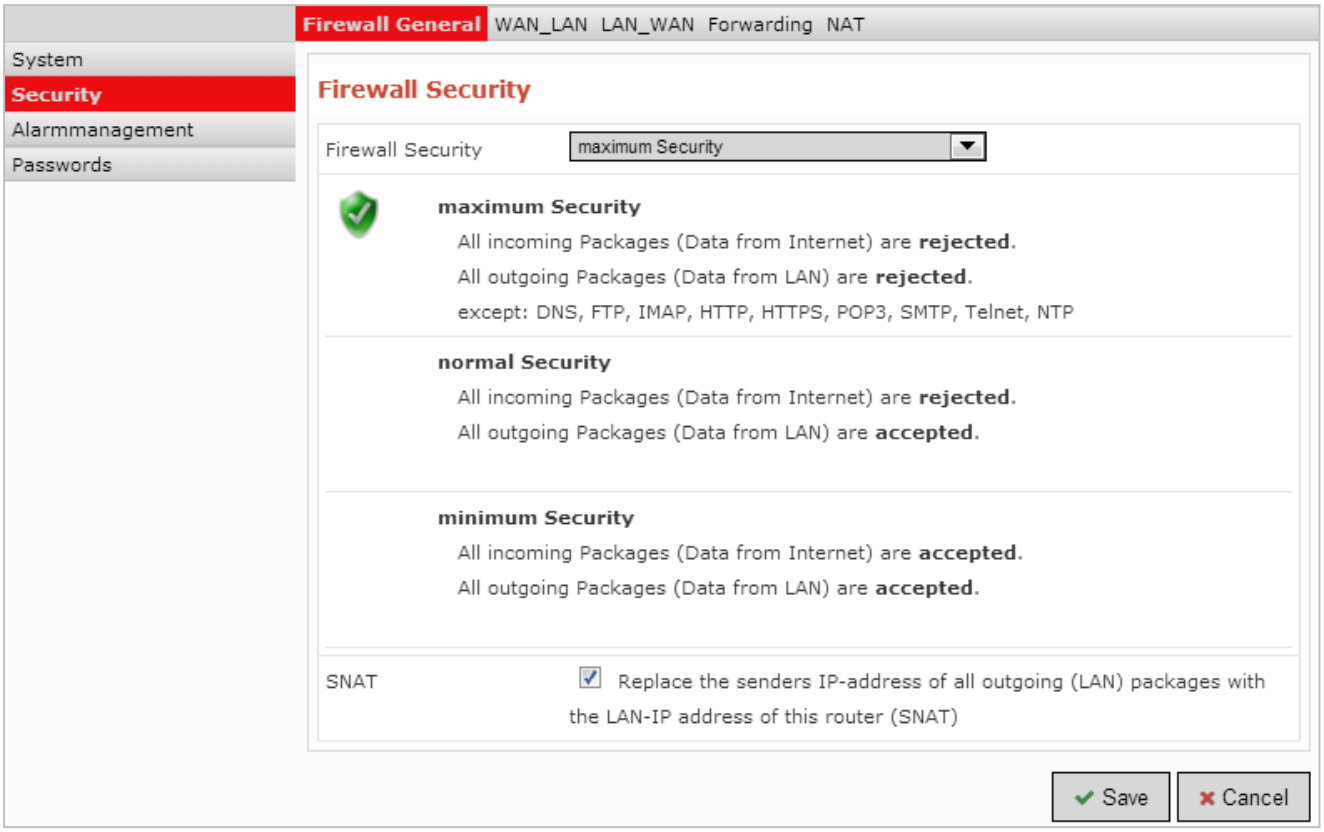
10.4.2 External logging server

Using an external logging server, the ***mbNET.mini*** system logging can be can be outsourced to another computer.

"External logging server IP Address"

"External logging server 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.

10.5 Security settings – firewall general



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:

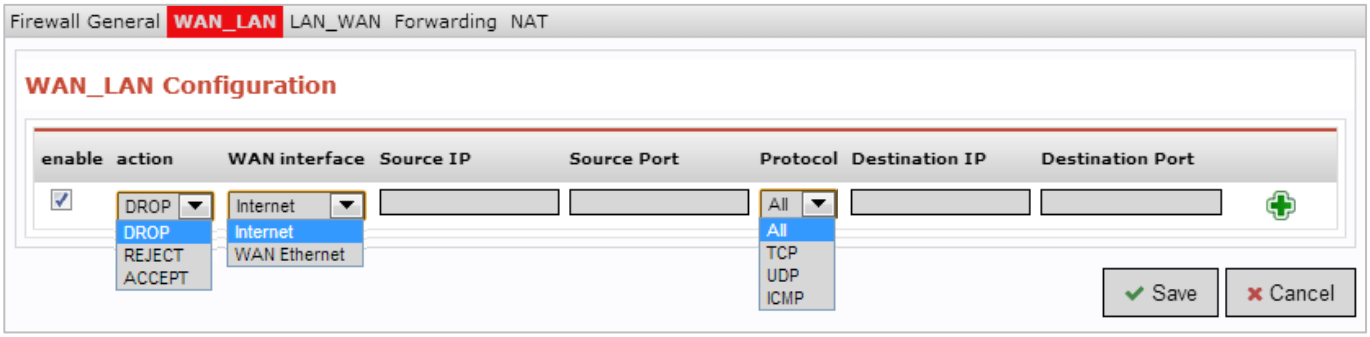
- **Maximum security**
  Which data traffic is allowed must be configured accordingly in this setting. Both incoming and outgoing data traffic is denied.
  To access the web interface (from outside the network), the **TCP protocol** and the **destination port 80** must be entered and enabled in the **WAN >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.

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.

10.6 Security settings – WAN > LAN

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



Sample settings

The following rule applies according to the device type (WAN MDH860 or GSM MDH861):

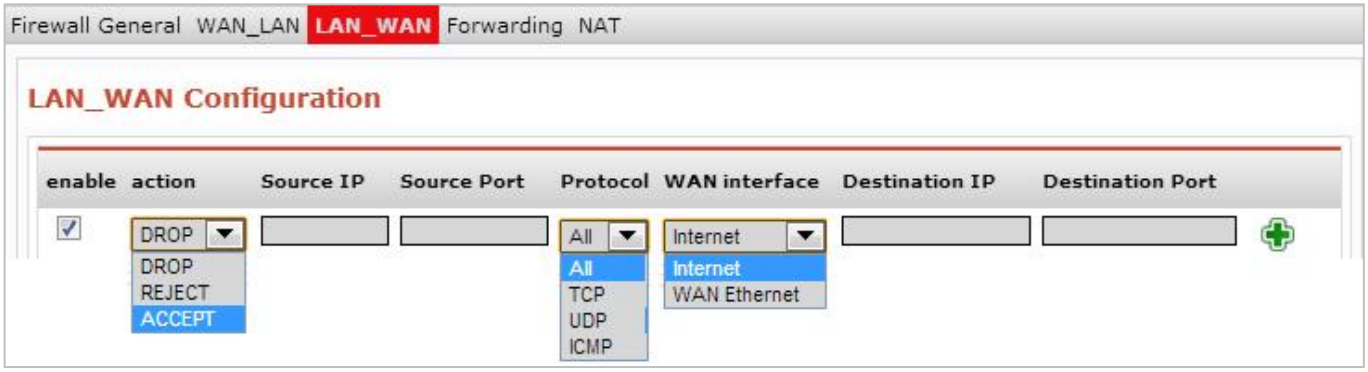
Internet connection: Establish Internet connection via WAN (external router, fixed line) (MDH860)
The WAN Ethernet connection is the interface with the Internet here. The firewall therefore checks the data traffic from the WAN Ethernet to the LAN Ethernet.

Internet connection: Establish Internet connection via modem (MDH861)
The modem is the interface with the Internet here. The firewall therefore checks the data 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

10.7 Security settings – LAN > WAN

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



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

10.8 Security settings – forwarding

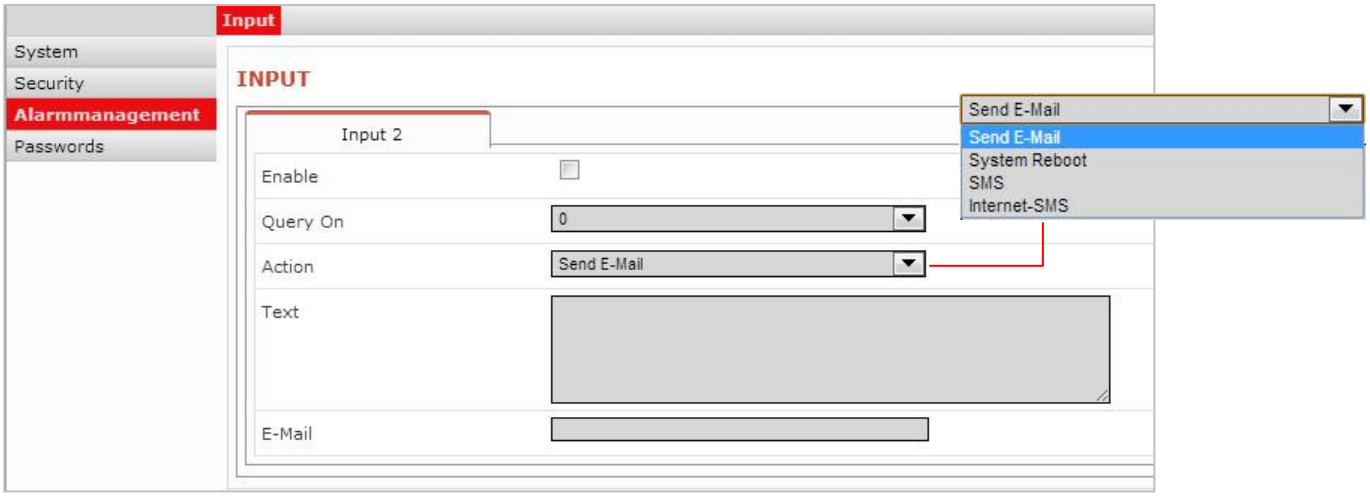
Designation	Description
Enable	If the box has been checked, the following settings will be active after saving.
Source IP	You can enter the IP from which data packets are to be received here. If an entry is made here, only packets from this one address are forwarded.
Source port	You can specify the port via which the data packets arrive here. If an entry is made here, only packets specifically sent via this port are forwarded.
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 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.
Apply to all connections	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

10.9 Security settings – NAT

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 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.

Designation	Description
Enable	If the box has been checked, the following settings will be active after saving.
Net address LAN	Enter the real address of the network here (e.g.192.168.0.0/24). **Please note that the IP address must be entered in CIDR notation.**
Net address NAT	Enter the translated address of your network here (e.g.192.168.0.0/24). **Please note that the IP address must be entered in CIDR notation.**
Net address 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 the new settings and temporarily stores them.
	Edits the settings in the current line.
	Deletes setting

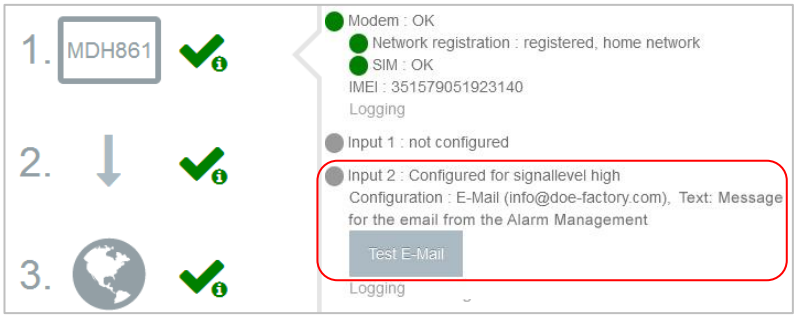
10.10 Alarm management - input



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

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.

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.



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).

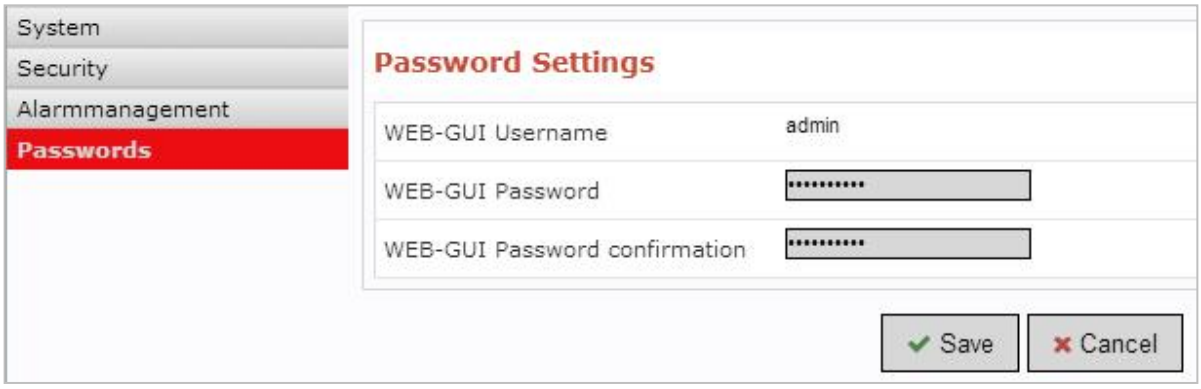
10.11 Passwords

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

"WEB-GUI user": admin

"WEB-GUI user": no password required

⚠ Please change the device password to prevent unauthorized access to the device.



ℹ 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.

11. Loading the factory settings

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

When the router is switched on and ready to operate,

❶ click the button **Reset** once.

❷ Then press **Function** straight afterwards

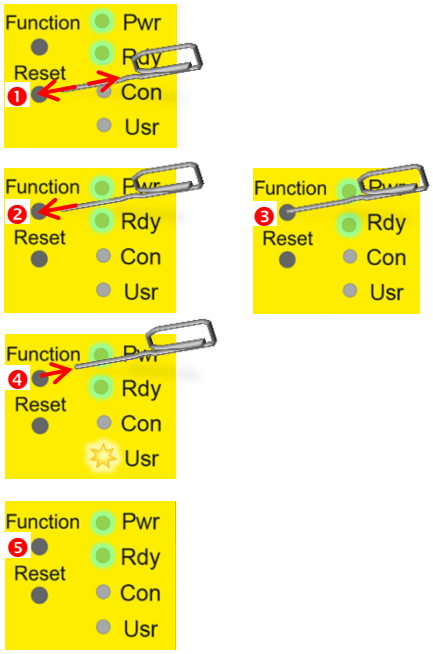
❸ and keep it pressed down.

❹ When the LED **Usr** flashes slowly (approx. 1.5 Hz), take your finger off the button.

The factory settings will now be loaded.

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

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



IMPORTANT: 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.

12. Firmware update

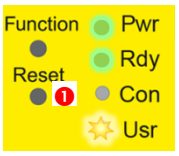
Firmware updates are generally carried out via USB.

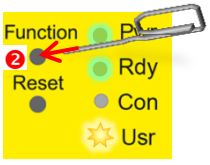
The latest firmware version can be downloaded from www.mbconnectline.com.

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.

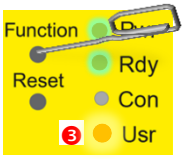
When the ***mbNET.mini*** is read to operate, insert the USB stick into the USB port of the device. The device will recognize the configuration file and show that through the slowly flashing LED **Usr** (flashing frequency: 3 Hz).

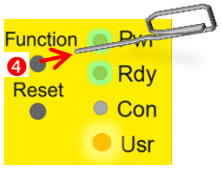
As soon as the LED **Usr starts to flash*** ❶, you must press the **Function** button ❷ within 10 seconds
*Flashing frequency = 3 Hz



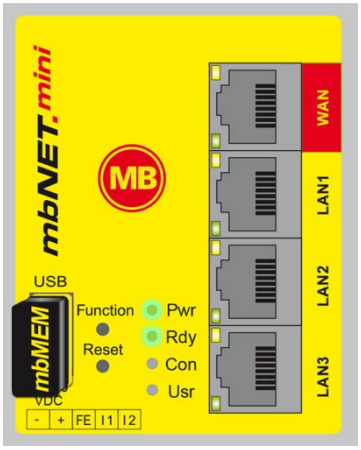


and hold it down, **until** the LED **Usr lights up**❸.





Now release the **Function** button❹.



When the LED **Usr goes** off and the LED **Pwr** + **Rdy** light up, then the configuration transfer has been completed.

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.

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".

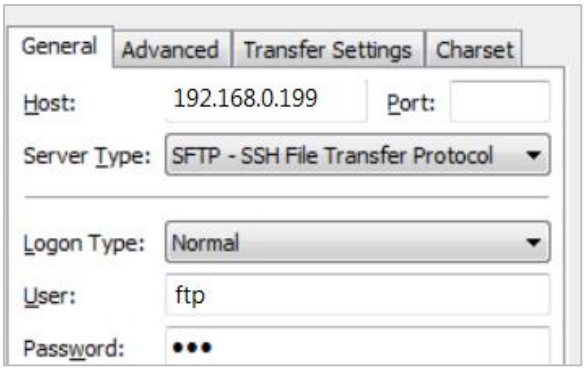
13. USB

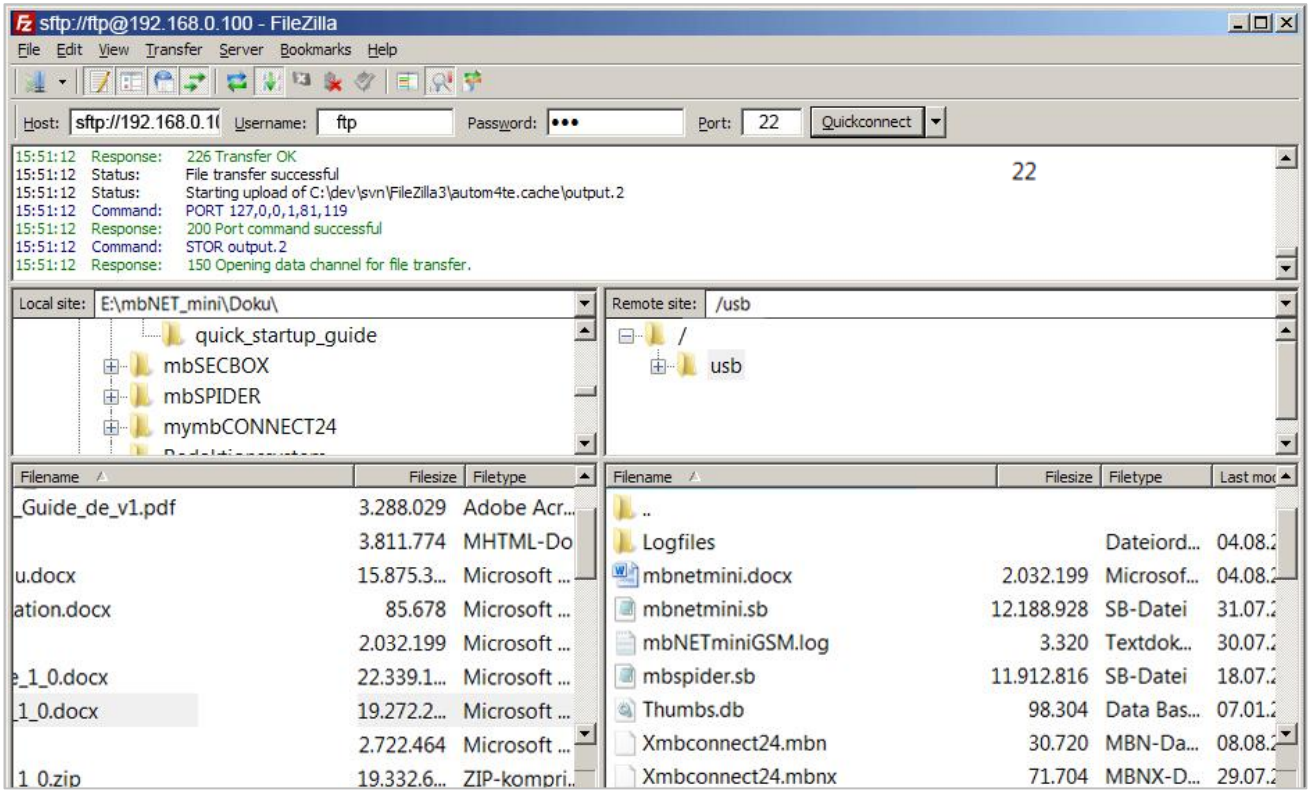
The USB memory can be reached via an SFTP client (e.g. FileZilla).
For this, the "Access from the network" must be active in the system settings Machines/Devices/Settings/System/USB (see section 10.3.1).

Preset user information:

SFTP user: ftp

SFTP password: ftp





14. Technical data

MDH 860 - *mbNET.mini* with WAN

- 1 x WAN
- 3 x LAN (3-port switch)
- 1 x USB host
- 2 x digital input
- Connection only possible to the portal (mbCONNECT24, mymbconnect24.hosted, .midi, .maxi)

MDH 860	
DC voltage	10 - 30 V DC
Power (at 24 V)	max. 250 mA
Protection class	IP 20
Area of application	Dry environments
Operating temperature range	32 - 122 °F
Storage temperature range	-4 - +140 °F
Humidity	0 - 95 % (non-condensing)
Weight	8.11 oz
Dimensions	2.72 in x 0.98 in x 3.35 in (W x D x H)
LAN interface (x 3)	10/100MBit/s full- and half-duplex mode, automatic recognition, patch cable / cross-over cable
WAN interface	10/100MBit/s full- and half-duplex mode, automatic recognition, patch cable / cross-over cable
Inputs (x 2)	Low 0-3.2V, high 8-30V)
VPN	Open VPN - connection only possible to the portal (mbCONNECT24, mymbconnect24.hosted, .midi, .maxi)
General certificates	EN 61000-6-4:2001,EN 61000-6-2:2001
Country of application	240 countries

MDH 861 - *mbNET.mini* with 3G modem

- 4 x LAN (4-port switch)
- 1 x USB host
- 2 x digital input
- 1 x SIM-card slot
- 1 x 3G modem
- Supported networks: GPRS | EDGE | UMTS | HSPA+
- Supported frequency bands: 800, 850, 900, AWS 1700, 1900, 2100 MHz
- HSxPA category: Downlink HSDPA Category 14 (21 Mbps), Uplink HSUPA Category 6 (5.76 Mbps)
- Country of application: Global
- Connection only possible to the portal (mbCONNECT24, mymbconnect24.hosted, .midi, .maxi)

MDH 861	
DC voltage	10 - 30 V DC
Power (at 24 V)	max. 250 mA
Protection class	IP 20
Area of application	Dry environments
Operating temperature range	32 - 122 °F
Storage temperature range	-4 - +140 °F
Humidity	0 - 95 % (non-condensing)
Weight	8.47 oz
Dimensions	2.72 in x 1.18 in x 3.35 in (W x D x H)
GPRS category	12 (max. 86.5 kBit/s)
EDGE category	12 (max. 236.8 kBit/s)
HSxPA category	Downlink HSDPA Category 14 (21 Mbps), Uplink HSUPA Category 6 (5.76 Mbps)
Supported frequency bands	800, 850, 900, AWS 1700, 1900, 2100 MHz
LAN interface (x 4)	10/100MBit/s full- and half-duplex mode, automatic recognition, patch cable / crossover cable
VPN	Open VPN - connection only possible to the portal (mbCONNECT24, mymbconnect24.hosted, .midi, .maxi)
Inputs (x 2)	Low 0-3.2V, high 8-30V)
FCC ID:	R17HE910
General certificates	EN 61000-6-4:2001,EN 61000-6-2:2001
Country of application	Dependent on available GSM network or provider

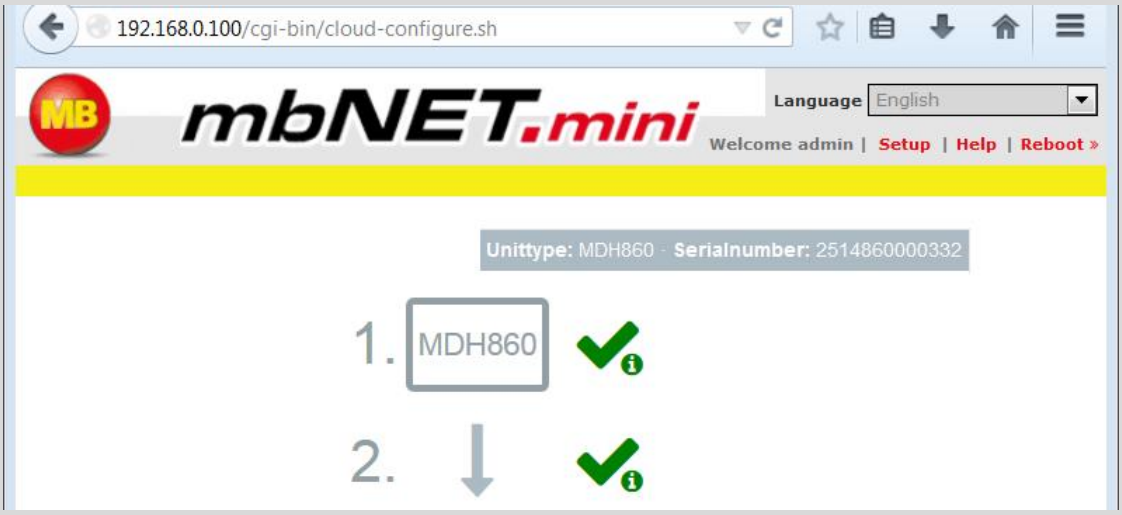
15. FAQ

Q	Can the configuration also be secured on the router?
A	No, that's not necessary. All settings are stored in the portal server.
Q	Can the firmware update be carried out via the web interface?
A	No, only via USB.
Q	Can I rename the configuration file?
A	**NO**, the configuration file may not **be renamed, as this will result in it not being recognized by the device.**
Q	There is both a firmware and a configuration file on the USB stick.
A	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".
Q	My APN provider is not on the list.
A	Enter the provider in "Own entry - enter login information" and enter the parameters according to the information provided by your provider (see section 7.8.3.2 Internet/GSM device).
Q	Which information do I have to provide in event of support?
A	In order to be able to provide the best possible support, we need the following information: The router's serial number The router's firmware version System logs () Accurate description of the fault - What caused the fault - Does the fault noticeably recur? - Did the fault occur after changing the settings or performing a firmware update?
Q	What is the difference between the two configuration files *mbconnect24.mbn* and *mbconnect24.mbnx*?
A	Unlike mbconnect24.mbn, the configuration file mbconnect24.mbnx is an encrypted file. An mbconnect24.mbn file can be transferred to any ***mbNET*** of the same type, as long as the device type is identical to the type in the configuration file and the configuration file does not contain a serial number. Example: If the device configuration was set up for an MDH860-type mbNET, the mbconnect24.mbn can be transferred to any MDH860-type device. An mbconnect24.mbnx file can only be transferred to an ***mbNET*** of the same type and with an identical serial number, as specified/contained in the configuration file.
Q	How do I create an encrypted configuration file?
A	Provided that the serial number of the device is entered in the device configuration in the portal and the device has already connected to the portal at least once, an encrypted configuration file is automatically created.
Q	Can I rename the configuration file?

A	**NO**, the configuration file may **not** be renamed, as this will result in it not being recognized by the device.
Q	What is an ***X****mbconnect24.mbn/.-mbnx* file?
A	Once the mbconnect24.mbn configuration file has been properly copied to the ***mbNET***, the file is automatically renamed to ***X****mbconnect24.mbn/.-mbnx*. This ensures that the configuration file is not recognized for a second time by the device and prevents endless importing of the configuration file.
Q	What do the different flashing codes for the LED **Con** mean?
A	LED **Con flashes rapidly** (approx. 3 Hz) = the device is attempting a) to connect to the Internet b) to establish a VPN connection to the portal LED **Con lights up** without flashing = the device has its own, active Internet connection LED **Con flashes slowly** (approx. 1.5 Hz) = the VPN connection to the portal is established
Q	What do the different flashing codes for the LED **Usr** mean?
A	LED **Usr flashes rapidly** (3 Hz) = the device has recognized a firmware file on the USB stick LED **Usr flashes slowly** (1.5 Hz) = the device has recognized a configuration file on the USB stick LED **Usr lights up** without flashing = the settings are being loaded
Q	How do I contact the web interface of my ***mbNET***?
A	To reach the ***mbNET*** web interface, it must be possible to contact the device from your computer via LAN. This means that your computer must be in the same address range as the ***mbNET***. This applies to both the IP address and your computer's subnet mask. Once you have entered the ***mbNET*** IP address - in any common web browser - you will be taken to the login page of the web interface. ***mbNET*** default settings: IP address 192.168.0.100 Subnet mask 255.255.255.0 Login admin Password no password
Q	Which browser should I use for administration purposes?
A	Please only use Chrome or Firefox. Due to the many differences in the versions, problems have repeatedly been reported when using the Internet Explorer.

16. Troubleshooting

Problem:	***mbCHECK*** cannot find a free VPN port
Solution:	Make sure that at least one of the three ports (80TCP, 443TCP or 1194TCP) is not blocked in the network firewall.
Problem:	**No connection to the portal, login failed** 
Solution:	• The access data were not entered correctly or are invalid • When selecting the server, a server different to that chosen when you requested your ***mbCONNECT24*** access was selected.  • The network adapter for ***mbDIALUP*** is missing or disabled. (Check the network adapter in your system settings *(Control Panel \ Network and Internet \ Network and Sharing Center \ Network Connections)*. If the adapter is disabled, enable it again. If the adapter is missing, re-install ***mbDIALUP***.). To set a detailed error diagnosis, you can activate extended logging in the ***mbDIALUP*** from the *"Settings/Options"* menu.  In the event of support, these log files are required by us in order to deal with your problem. You will find the log files on your computer under: • OpenVPN Log **Windows XP:** C:\Documents and Settings\All Users\User Data\MB Connect Line GmbH\mbDIALUP\ovpn\log • System Log **Windows XP:** C:\Program Files (x86)\MB Connect Line GmbH\mbDIALUP\vpnservicelog.txt • OpenVPN Log **Windows 7:** C:\ProgramData\MB Connect Line GmbH\mbDIALUP\ovpn\log • System Log **Windows 7:** C:\Program Files (x86)\MB Connect Line GmbH\mbDIALUP\vpnservicelog.txt
Problem:	**No connection from the device to the portal**
Solution:	Check the required peripheral components, depending on the device type. • Are the network cables and network connections correct? • Is a SIM card inserted? • Is the card used for data transfer enabled? • Is it necessary to enter a PIN? • Is an antenna installed? • Is the signal strength sufficient? (The signal strength can be requested via the ***mbNET*** web interface)



Check your network settings.

- WAN and LAN IP must **not** be in the same address range.
- The ***mbNET*** must be connected on the WAN.
- Is the ***mbNET*** connected to the Internet?

If in doubt, please contact your system administrator.

- Check
  • that one of the VPN ports (80TCP, 443TCP or 1194TCP) - see ***mbCHECK*** - is enabled in the firewall
  • that one of the enabled ports is also entered in the **Internet settings**
  • that NTP port 123 is enabled in the firewall

If one of the ports (TCP:1194, TCP:80, TCP:443) for the device is blocked in the network firewall, despite a positive message from ***mbCHECK,*** (IP/MAC address filter), please contact your system administrator.