Setup Guide

MX880 Anleitungen

Seite 2

MX880 Manuals

Page 2

mdex Router

MX530 | MX880

Release: October 02, 2020 (v.2.5)

This Setup Guide describes the commissioning of the **mdex Router** MX530 and **mdex Router** MX880 with the commonly used functions.

These setup instructions may differ on delivery of the MX530/MX880 with individual configuration, in the project business or as an mdex package/bundle (e.g. with an mdex fixed.IP+/public.IP via OpenVPN or an mdexSIM with public.IP). Please observe the enclosed supplementary instructions and/or the additional router labels.

MX880 Anleitungen

Diese MX530/880 Einrichtungsanleitung sowie weitere Anleitungen des MX530/880 Routers stehen als PDF-Datei unter nachfolgendem Link oder QR-Code zum Download bereit:

www.mdex.de/MX880-Anleitungen

MX880 Manuals

The English MX530/880 Setup Guide and other available MX530/880 manuals can be downloaded as PDF file from the following link or QR code:

www.mdex.de/MX880-Manuals

Further support information for all mdex products can be found at **wiki.mdex.de**.

Table of contents

1 Specifications

The **MX530** is a Dual-SIM UMTS mobile router for the 2G and 3G mobile networks.

The **MX880** is a Dual-SIM LTE mobile router and intended for the 2G, 3G and 4G mobile networks. The MX880 has additional interfaces (RS232, RS485, USB) for optional special functions and offers the possibility to connect an optional GPS antenna.

For further details see chapter **1.2 Technical specifications** (Page 5).

1.1 Scope of Delivery

Accessories:	**MX530**	**MX880**
230V plug-in power supply with router connector	Quantity: 1	Quantity: 1
Additional power cable with router connector (Only required with MX530 to connect an external power supply.)	Quantity: 1	-
Mobile rod antenna	-	Quantity: 2
Mobile antenna – with ccable and magnetic base	Quantity: 1	Quantity: 2
WiFi rod antenna	Quantity: 2	Quantity: 2
Network cable (Ethernet)	Quantity: 1	Quantity: 1
DIN rail bracket (including 2 fixing screws)	Quantity: 1	Quantity: 1
Blind plug for WAN socket	Quantity: 1	Quantity: 1
mdexSIM Vodafone (already preinstalled in ‘SIM1’ Slot) (1	Quantity: 1	Quantity: 1
mdexSIM Telekom (already preinstalled in ‘SIM2’ Slot) (1	Quantity: 1	Quantity: 1
MX530/MX880 Setup Guide	Quantity: 1	Quantity: 1
I/O connector (10-pin)	-	Quantity: 1
RS485 connector (6-pin)	-	Quantity: 1

(1 For the use of the respective **mdexSIM** see chapter **1.5 Preinstalled mdexSIM** (Page 8).

1.2 Technical specifications

Hardware:	**MX530**	**MX880**
Dimensions L x W x H:	80 mm x 106 mm x 46 mm (without DIN rail bracket)	
Weight:	about 280g (without DIN rail bracket)	
CPU / RAM:	560 MHz MIPS CPU, 128MB RAM	
Input voltage:	9 - 30VDC, max. 7W	
4-port switch: (3 x LAN, 1 x WAN/configurable)	10/100 Mbps BASE-T, Auto MDI/MDIX	

Environmental conditions:

Temperature range (operation):	-40° to +70° C
Humidity (operation):	10% to 90%, non-condensing
Temperature range (storage):	-45° to +80° C
Humidity (storage):	5% to 95%, non-condensing

Mobilfunk & WIFI:

4G LTE:	-	max. 150 Mbit/s Download / 50 Mbit/s Upload
3G HSPA+:	-	max. 42,2 Mbit/s Download / 5,76 Mbit/s Upload
3G HSPA:	max. 14,4 Mbit/s Download / 5,76 Mbit/s Upload	
3G UMTS:	max. 384 kbit/s Download / 384 kbit/s Upload	
2G GPRS/EDGE:	max. 236,8 kbit/s Download / 236,8 kbit/s Upload	
WIFI:	IEEE 802.11 b/g/n (2,4 GHz), WEP/WPA/WPA2 encryption, 2T2R (max. 300 Mbit/s)	

1.3 Preconfiguration (factory defaults)

The MX530/MX880 is preconfigured for the operation of the **mdexSIM Vodafone** (SIM1) and for the accessibility of a connected terminal device. Here you will find the factory defaults in detail.

> ⚠ Please note that the preconfiguration of the MX530/MX880 may differ for orders with individual configuration, in the project business or as another mdex product (for example, 'mdex mobile.LAN packet' or 'mdex LTE per packet').

Network settings

LAN IP address:	192.168.0.1
LAN access:	HTTP Port: 8080 | HTTPS Port: 443 | SSH Port: 22
Remote access:	HTTP Port 8080: enabled (via WAN IP of the SIM card) HTTPS Port 443: locked | SSH port 22: locked
Login Username / Password:	admin / admin01
DHCP Server:	enabled (IP address 192.168.0.100 is assigned)
Port-Forwarding:	Host forwarding to 192.168.0.100
Wireless LAN (WIFI):	disabled
NTP (Time Server):	Time synchronization enabled (Time Server: time.mdex.de)

Mobile settings	**SIM 1** (primary SIM)	**SIM 2**
SIM card (preinstalled):	**mdexSIM Vodafone**	**mdexSIM Telekom**
APN:	m2m.cda.vodafone.de	mdex.ic.m2mportal.de
Username:	mdex@m2m.mdex.de	mdex@mdex.de
Password:	mdex	mdex
PIN:	without	without

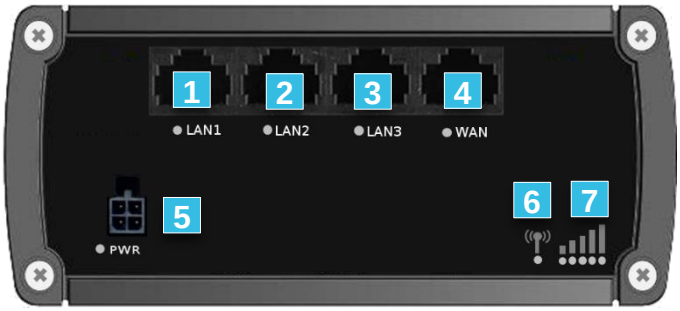
Settings for stable connection

Daily restart (Daily reboot):	enabled (daily at 23:00 pm)
Ping reboot:	enabled (every 5 minutes)
Ping Server:	ping.mdex.de ⚠ The server **ping.mdex.de** is only accessible from the mdex network! See Chapter **3.2.1 Important notes about the Ping Reboot** (Page20).

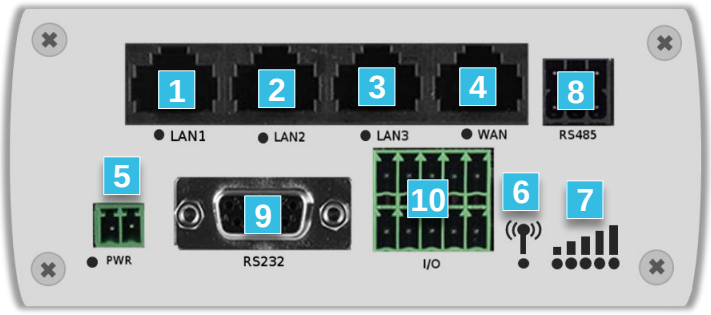
1.4 Connectors and Interfaces

⚠ **No PoE** (Power over Ethernet) powered network cable may be connected to the LAN/WAN sockets! The PoE voltage would destroy the MX530/MX880!

MX530 front panel

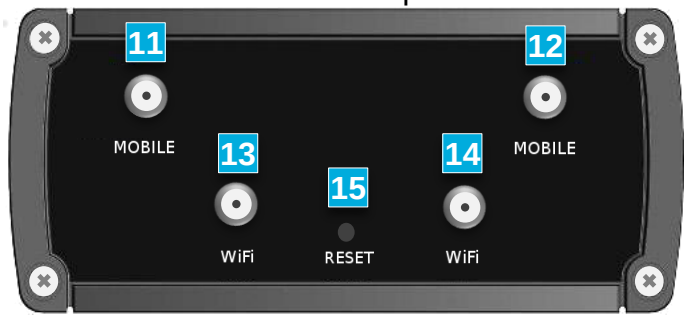


MX880 front panel

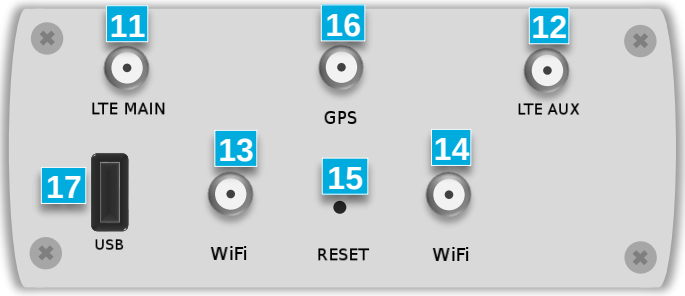


1 2 3	LAN Ethernet ports with status LED for connecting a PC or terminal devices
4	WAN Ethernet port with status LED for special function to connect the MX530/MX880 to external networks or routers
5	Connection for power supply (9-30V DC, 7W) with power LED
6	Mobile connection Status Display 'Led Status Display' → **4.2.1 LED Status indicators** (Page 39)
7	Mobile strength display 'Led Status Display'→ **4.2.1 LED Status indicators** (Page 39)
8	RS485 contacts for special functions (MX880 only)
9	RS232 socket for special functions for connecting serial devices (MX880 only)
10	I/O contacts for input and output for special functions (MX880 only)

MX530 back panel



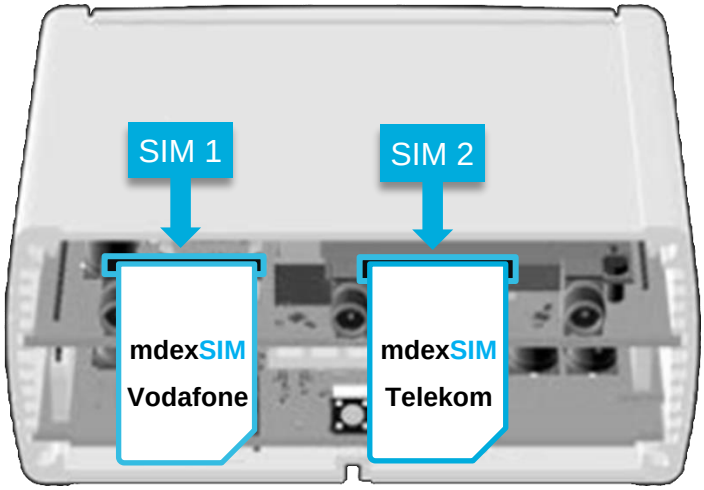
MX880 back panel



11	SMA connector for main mobile antenna (MAIN)
12	SMA connector for additional mobile antenna (AUX)
13 14	RP-SMA connectors for WIFI antenna
15	RESET button for restart and resetting to factory defaults
16	SMA connector for optional GPS antenna (MX880 only)
17	USB connector for special functions (MX880 only)

1.5 Preinstalled mdexSIM

The MX530/MX880 comes with two preinstalled mdex SIM cards.



The ICCIDs of the preinstalled mdex SIM cards can be found on the label of the box or the bottom of the MX530/MX880:

1.5.1 mdex SIM Vodafone (SIM1)

For the use of the preinstalled **mdexSIM Vodafone** , please note the following:

- The mdex SIM Vodafone is preinstalled in **SIM1** Slot of the MX530/MX880.
- The desired tariff of this mdex SIM Vodafone must be ordered from mdex.
- The mobile settings are already preconfigured to operate the mdex SIM Vodafone.

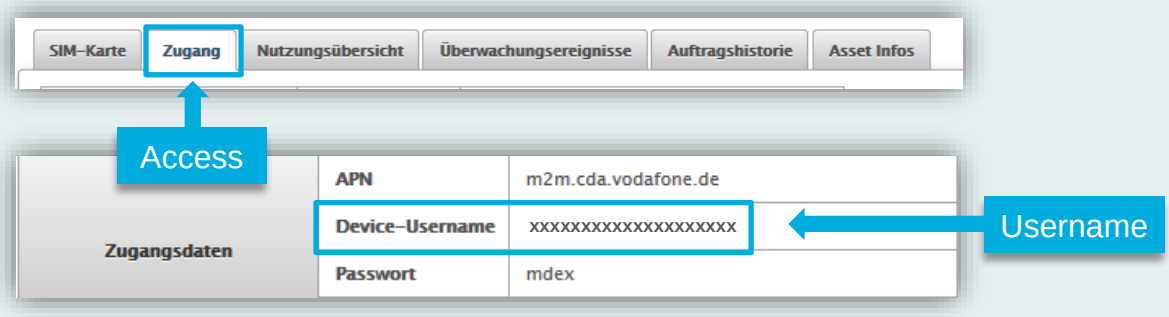
  When using the **mdexSIM Vodafone** incl. **mdex public.IP**, a different SIM card username may be required according to the chapter **3.5 Mobile settings** (Page22).

  ⓘ The required username of the mdex SIM can be found in the order confirmation which was sent to you by e-mail. Alternatively, you can also read the username in the mdex Management Portal as described on the following page.

- The mdex SIM must be unlocked according to chapter **1.5.3 Unlock mdexSIM** (Page10).
- To avoid unnecessary costs, the mdex SIM is monitored by an alarm profile.
  See **https://wiki.mdex.de/Support/DOCKostenfallenVerhindern**
- Further information on using a mdex SIM can be found in the mdex Support Wiki at **https://wiki.mdex.de** → **mdex SIM**

Read the SIM card username in the mdex Management Portal

1. Log into themdex Management Portal: **https://manager.mdex.de**.
   (Your access data have been sent to you via email.)
2. Click on **SIM Cards → brows SIM cards**.
3. Clicking on **Start Search** displays all mdex SIM cards.
   (You can limit the search by, for example, entering the ICCID of the mdex SIM.)
4. Click on the respective SIM card and switch to the **Access** tab.
   Under **Access data** you will find APN, username and password of your mdex SIM.



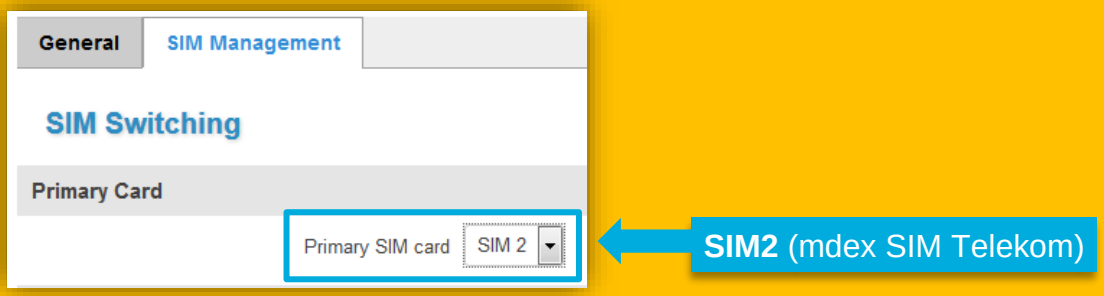
1.5.2 mdex SIM Telekom (SIM2)

To use the preinstalled **mdexSIM Telekom** please note the following:

- The mdex SIM Telekom is preinstalled in **SIM2** Slot of the MX530/MX880.

⚠ To use the **mdexSIM Telekom** (SIM2) the following settings are required:

1. Click on the **Network → Mobile (SIM): SIM Management**.
2. Set the **Primary SIM card** to **SIM 2** and click on **Save**.



- The desired tariff of this mdex SIM Telekom must be ordered from mdex.
- The mdex SIM must be unlocked according to chapter **1.5.3 Unlock mdexSIM** (Page 10).
- To avoid unnecessary costs, the mdex SIM is monitored by an alarm profile.
  See **https://wiki.mdex.de/Support/DOCKostenfallenVerhindern**
- Further information on using a mdex SIM can be found in the mdex Support Wiki at **https://wiki.mdex.de → mdex SIM**

1.5.3 Unlock mdexSIM

For safety reasons, the mdex SIM cards are locked on delivery and must first be unlocked before being used for the first time.

This step is required only when using a preinstalled **mdex**SIM !

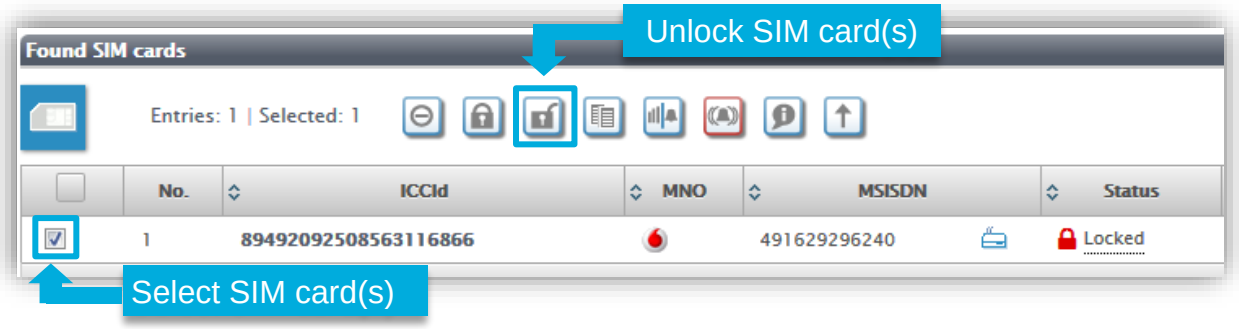
- The tariff for the desired SIM card must have been ordered from mdex.
- The ICCIDs of the preinstalled SIM cards are located on the router label.
  SIM1: **mdexSIM Vodafone** SIM2: **mdexSIM Telekom**

Unlock SIM card:

1. Log into **mdex Management Portal** at **https://manager.mdex.de**.
   (Your login access data have been sent to you via email.)

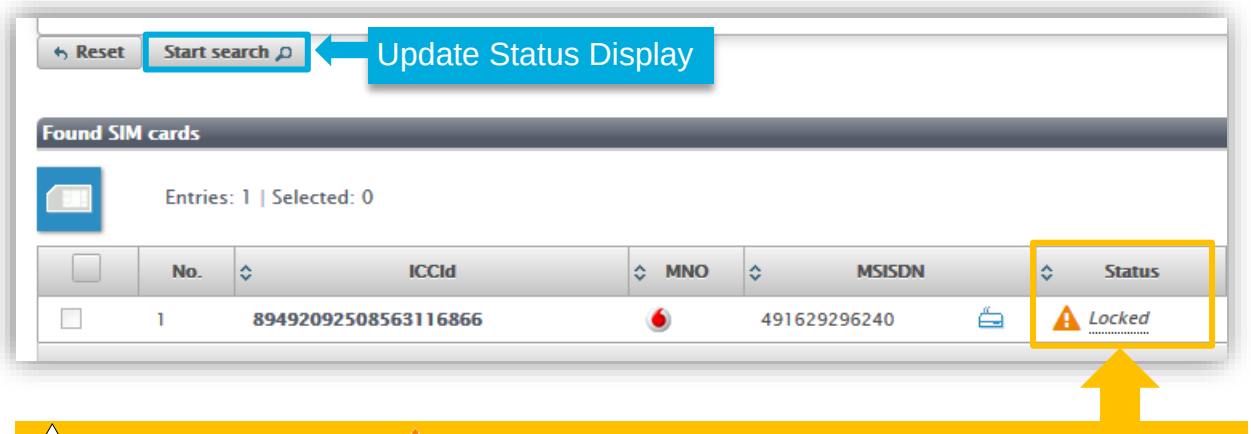
2. Click on **SIM Cards → Locked SIM Cards**.

   Check the SIM card(s) and click on the icon (Unlock SIM cards).



3. Follow the instructions on the portal to unlock the SIM card(s) and then click on Back to Search button.

4. Full unlocking of the SIM card can take up to 20 minutes.
   After a few minutes, check the SIM card status by clicking on Start search button.



As long as the status ***Locked*** is displayed, the process is still in progress.

To update the status display, click on **Start Search** button again.
As soon as the status **Enabled** is displayed, the SIM card is ready for use.

2 Installation

Please pay attention to the notes in the chapter **5 Important information** (Page 45).

2.1 Quick Start

Depending on the intended use of the MX530/MX880, here you will find the necessary setup steps for quick commissioning.
For more individual settings, see the chapters **3 Configuration** and **4 Additional functions** relevant descriptions.

2.1.1 Own SIM card without mdex IP service

Using the MX530/MX880 as an Internet router with your own SIM card, without mdex IP service (fixed.IP+ / public.IP) for remote access to a connected terminal device.

1. Install your SIM card according to chapter **2.2 Replace SIM card** (Page 13).
2. Connect LTE mobile antennas according to chapter **2.3 Connect antennas** (Page 14).
3. Connect power supply according to chapter **2.4 Powering** (Page 15).
4. Change the login password according to chapter **3.4 Login Password** (Page 22).
5. Set the mobile settings in MX530/MX880 (APN, username, password, PIN) for your SIM card according to the chapter **3.5 Mobile settings** (Page 22).
6. Expand the DHCP IP address range according to chapter **3.8 DHCP-Server** (Page 30) for the number of connected network devices.
7. Disable the 'DMZ configuration' according to chapter **3.9 Forwarding** (Page 32).
8. As per chapter **3.11 Ping Reboot** (Page 36) a publicly accessible server must be set as Ping Server e.g. ‚public-ping.mdex.de' (185.39.176.22).
9. If remote access is not required, it should be disabled for security reasons according to chapter **3.10 Configuration Access / Remote Access** (Page 34).
10. Connect terminal devices according to chapter **2.6 Connection of terminal** devices (Page 17).

2.1.2 With mdexSIM & mdex IP service

Using the MX530/MX880 with the preinstalled **mdexSIM Vodafone** or **mdexSIM Telekom**, optionally with a mdex IP service (fixed.IP+ / public.IP).

1. Carry out the measures as per chapter **1.5 Preinstalled mdexSIM** (Page 8)
2. Connect LTE mobile antennas according to chapter **2.3 Connect antennas** (Page 14).
3. Connect power supply according to chapter **2.4 Powering** (Page 15).
4. Change the login password according to chapter **3.4 Login Password** (Page 22).
5. If remote access is not required, it should be disabled for security reasons according to chapter **3.10 Configuration Access / Remote Access** (Page 34).
6. Connect terminal device(s) according to chapter **2.6 Connection of terminal** devices (Page 17).

2.1.3 Own Vodafone/Telekom SIM card & mdex IP service

Using the MX530/MX880 with your own Vodafone/Telekom SIM card with mdex IP service fixed.IP+ / public.IP as network type ‘Vodafone’ or ‘Telekom’.

1. Install your SIM card according to chapter **2.2 Replace SIM card** (Page 13).
2. Connect LTE mobile antennas according to chapter **2.3 Connect antennas** (Page 14).
3. Connect power supply according to chapter **2.4 Powering** (Page 15).
4. Change the login password according to chapter **3.4 Login Password** (Page 22).
5. If remote access is not required, it should be disabled for security reasons according to chapter **3.10 Configuration Access / Remote Access** (Page 34).
6. Set the mobile settings in MX530/MX880 (APN, username, password, PIN) for your SIM card according to the chapter **3.5 Mobile settings** (Page 22).
7. Connect terminal device(s) according to chapter **2.6 Connection of terminal** devices (P. 17).

2.1.4 Own SIM card & mdex IP service, fixed.IP+ via OpenVPN'

Using the MX530/MX880 with your own (any) SIM card and the mdex IP service ‘public.IP’ as network type ‚OpenVPN‘.

1. Install your SIM card according to chapter **2.2 Replace SIM card** (Page 13).
2. Connect LTE mobile antennas according to chapter **2.3 Connect antennas** (Page 14).
3. Connect power supply according to chapter **2.4 Powering** (Page 15). Change the login password according to chapter **3.4 Login Password** (Page 22).
4. Set the mobile settings in MX530/MX880 (APN, username, password, PIN) for your SIM card according to the chapter **3.5 Mobile settings** (Page 22).
5. Setup the integrated OpenVPN Client according to chapter **3.6 mdex OpenVPN-Client** (Page 27) with the Role ‚**mdex fixed.IP+**‘.
6. Set the **Source zone** to **VPN** for forwarding according to chapter **3.9 Forwarding** (Page 32).
7. Set the **Source zone** to **VPN** for remote access according to chapter **3.10 Configuration Access / Remote Access** (Page 34) or disable it for security reasons if no remote access is required.
8. Connect terminal device(s) according to chapter **2.6 Connection of terminal** devices (P. 17).

2.1.5 Own SIM card & mdex IP service, public.IP via OpenVPN‘

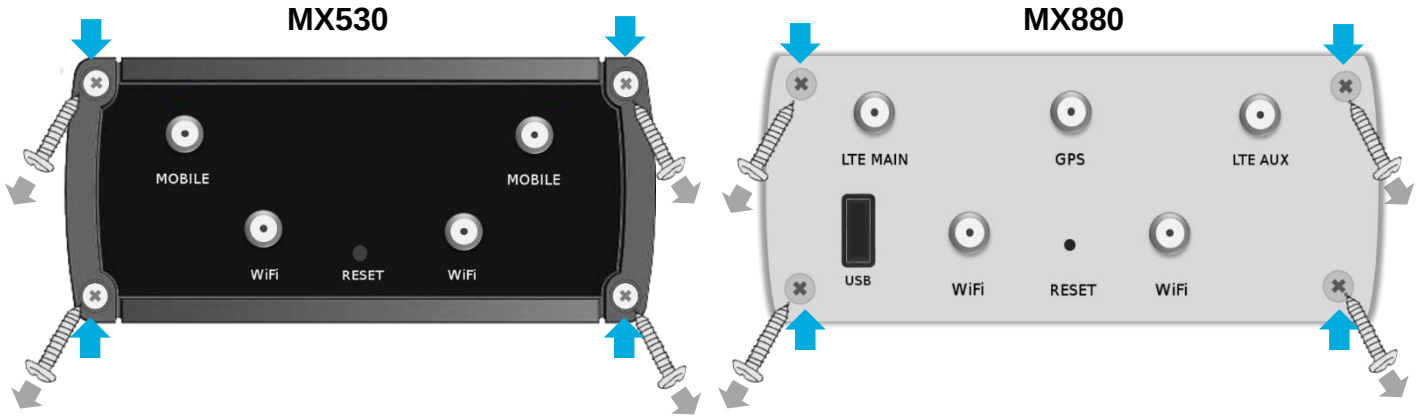
Using the MX530/MX880 with your own (any) SIM card and the mdex IP service ‘public.IP’ as network type ‚OpenVPN‘.

1. Install your SIM card according to chapter **2.2 Replace SIM card** (Page 13).
2. Connect LTE mobile antennas according to chapter **2.3 Connect antennas** (Page 14).
3. Connect power supply according to chapter **2.4 Powering** (Page 15).
4. Change the login password according to chapter **3.4 Login Password** (Page 22).
5. Set the mobile settings in MX880 (APN, username, password, PIN) for your SIM card according to the chapter **3.5 Mobile settings** (Page 22).
6. Setup the integrated OpenVPN Client according to chapter **3.6 mdex OpenVPN-Client** (Page 27) with the Role ‚**mdex public.IP**‘.
7. Set the **Source zone** to **VPN** for forwarding according to chapter **3.9 Forwarding** (Page 32).
8. Set the **Source zone** to **VPN** for remote access according to chapter **3.10 Configuration Access / Remote Access** (Page 34) or disable it for security reasons if no remote access is required.
9. Connect terminal device(s) according to chapter **2.6 Connection of terminal** devices (P. 17).

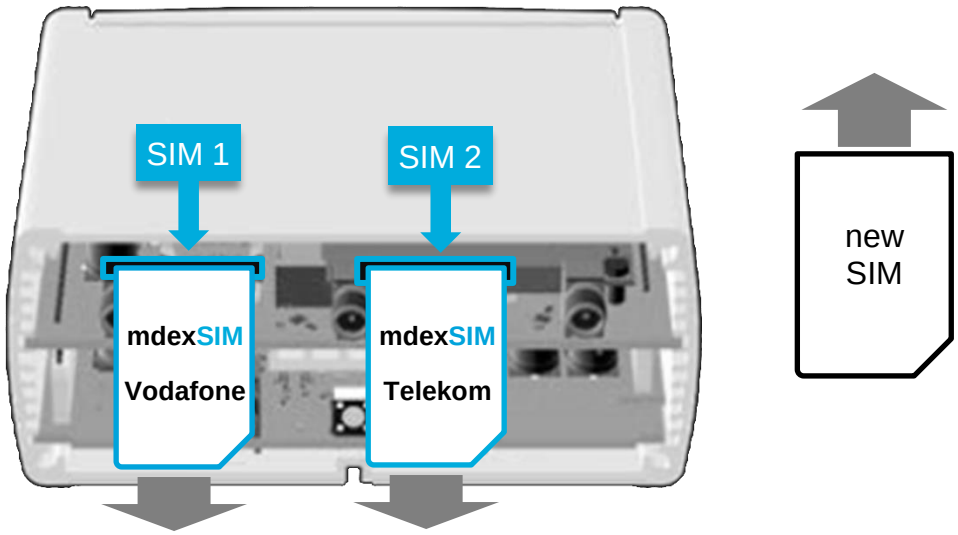
2.2 Replace SIM card

This step can be skipped when using the preinstalled mdex SIM card(s).
To insert another SIM card, follow the steps below.

1. Unscrew the 4 screws on the back of the router (antenna side) and remove the back cover.



2. Pull out the preinstalled SIM card(s) and insert the new SIM card(s) into the desired SIM card slot (preferably SIM 1).

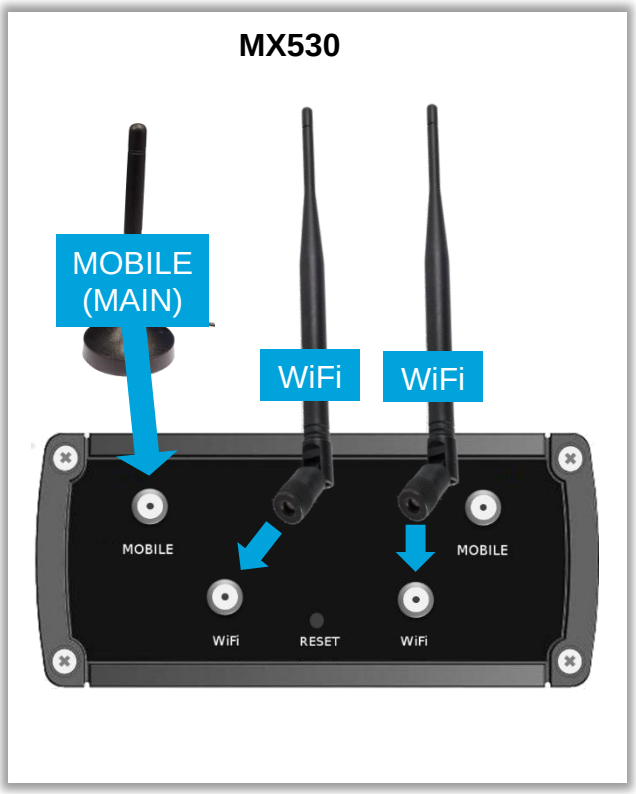


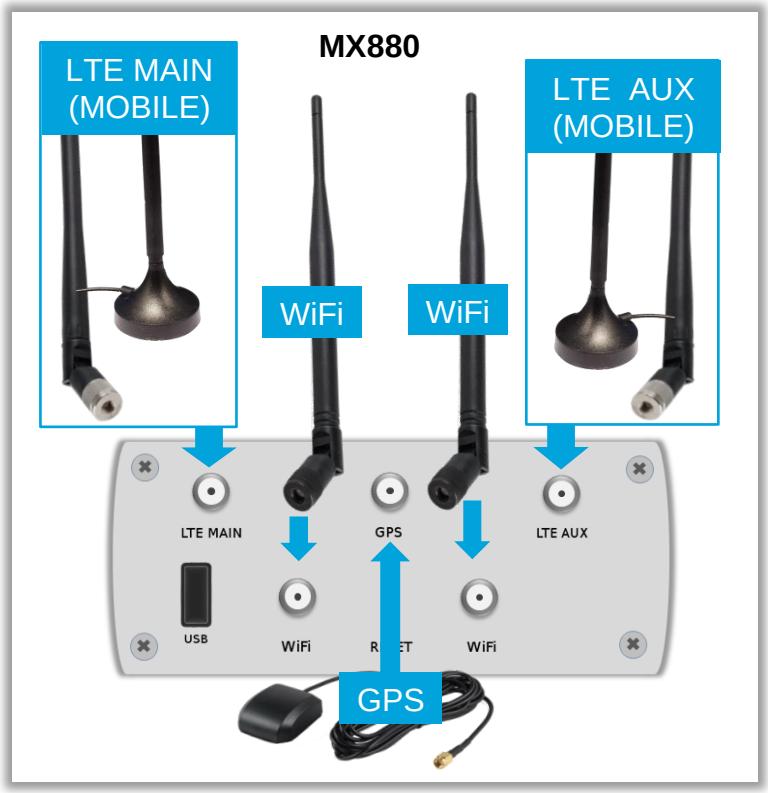
3. Secure the back cover with the four screws.

4. The MX530/MX880's mobile settings must be adjusted to use the new SIM card(s) as per chapter **3.5 Mobile settings** (Page 22).

2.3 Connect antennas

There are labels on the antennas with the name of the associated antenna connection.





LTE (MX880)	The MX880 comes with 4 LTE antennas (MOBILE/LTE). Depending on the installation site, you can either attach the LTE antennas directly on the router using the articulated joint or set the two magnetic base antennas with the connection cable and magnetic base slightly away from the router, e.g. when the MX880 is mounted in an IT cabinet. To establish a mobile connection, LTE antenna must be connected to the **LTE MAIN** socket. By using the additional LTE antenna to **LTE AUX** the LTE download rate can be increased.
MOBILE (MX530)	The MX530 comes with a mobile antenna (with connection cable and magnetic base) for connecting to the left **MOBILE** (MAIN) socket. (see figure) (The other socket, MOBILE '(AUX) serves to connect another (optional) mobile antenna, for example to increase the download rate in mobile use.)
WiFi	Only when using the WIFI according to chapter **4.1 WiFi (Wireless Access Point)** (Page 38) the two WiFi antennas must be connected to the **WiFi** sockets.
GPS (MX880)	The MX880 has a GPS receiver to determine the current position. The optional GPS antenna needs to be connected only when using the GPS function and is located in a GPS reception area.

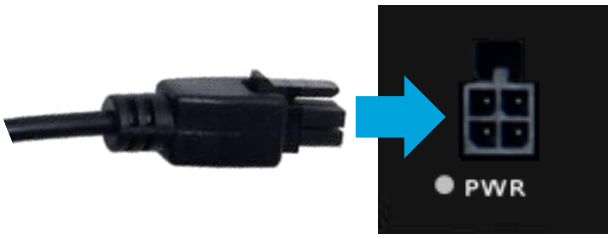
The magnetic base antennas have the best reception strength when mounted on a metal surface. You can also use outdoor antennas in order to further enhance mobile reception.

2.4 Powering the router

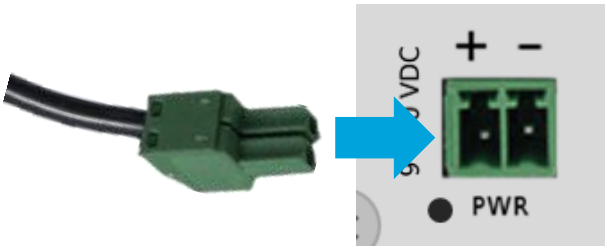
Power is supplied to the MX530/MX880 using the supplied plug-in power supply.
(Temperature range of the plug-in power supply: 0° to + 40° Celsius)

The router connector of the plug-in power supply is plugged into the **PWR** socket.

MX530



MX880



2.4.1 Using another power supply

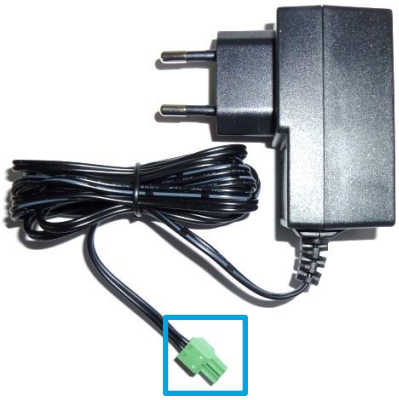
As an alternative to the enclosed plug-in power supply, the MX530/MX880 can also be supplied with a DIN rail power supply or own power supply (9V to 30V DC, 7W).

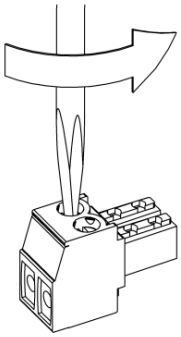
MX530

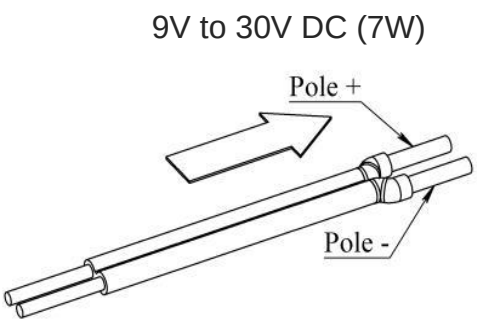
Use the supplied power cable and attach the red wire (+) and black wire (-) to the external power supply. Pay attention to the correct polarity!

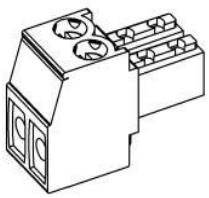
MX880

Unscrew the screws of the green router connector plug attached to the power supply and attach the wires to the external power supply.
Pay attention to the correct polarity!



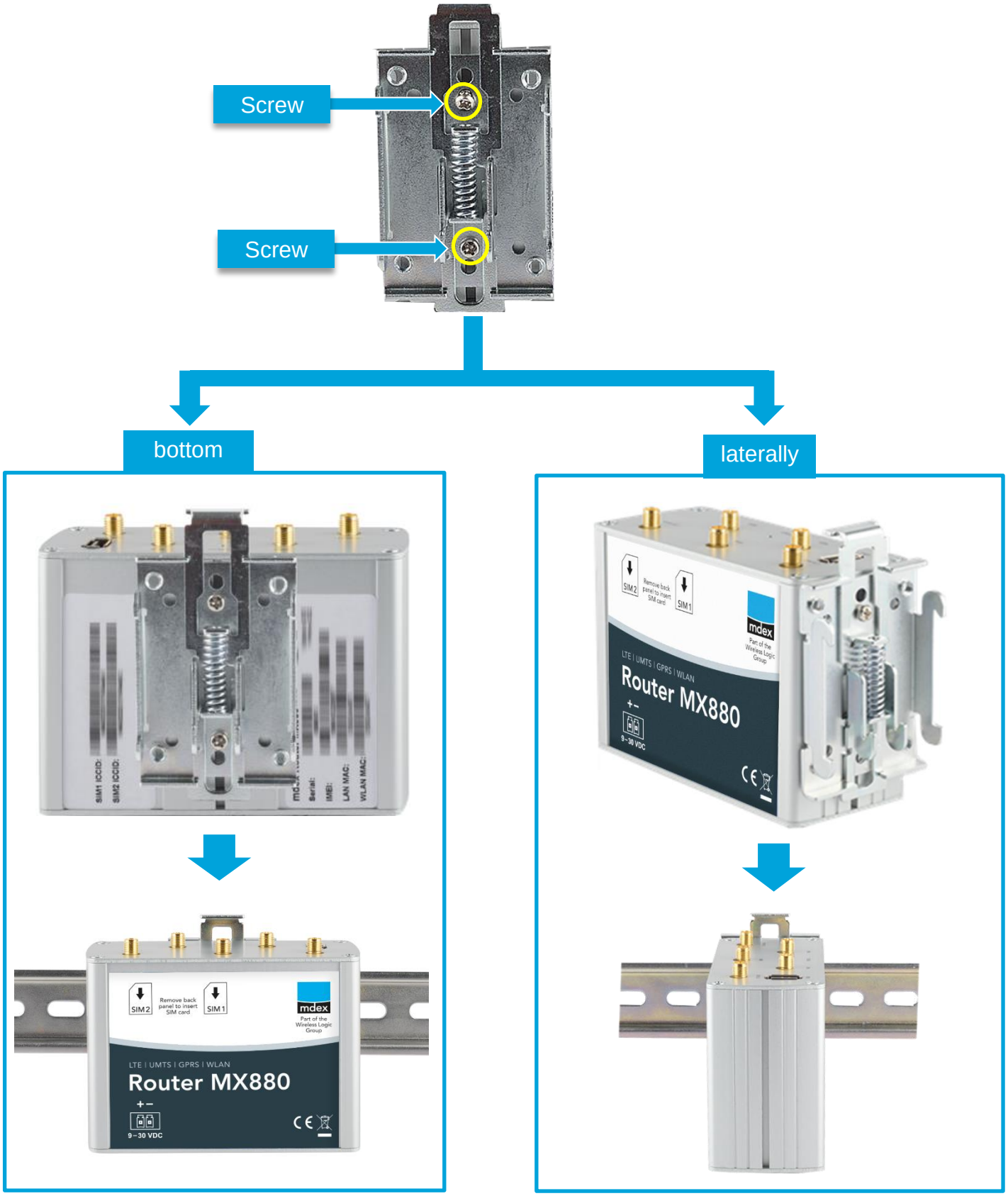






2.5 DIN rail mounting

The MX530/MX880 can be mounted on a DIN rail using the supplied DIN rail bracket. The DIN rail bracket is fastened in the groove to the bottom or side of the router with the two supplied screws. (Mounting the DIN rail bracket on the MX530 is the same as mounting on the MX880.)



2.6 Connection of terminal devices

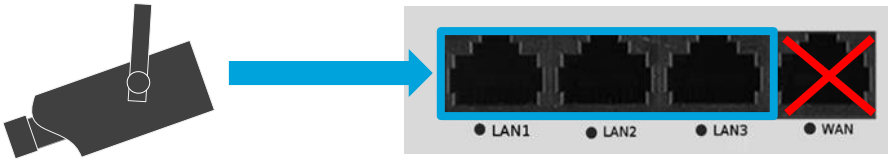
There are 3 LAN sockets available for connecting the terminal devices. The WAN socket is reserved for special functions and is not intended for the connecting terminal devices.

⚠ **No PoE** (Power over Ethernet) powered network cable may be connected to the LAN/WAN sockets! The PoE voltage would destroy the MX530/MX880!

2.6.1 Connection of only one terminal device

The MX530/MX880 is already preconfigured for connecting a terminal device.
Please note the following information.

1. Connect the terminal device to a free LAN socket (LAN1, LAN2 or LAN3) with a network cable. The WAN socket is not intended for connecting terminal devices!



2. Network setting of the connected terminal device:

   The terminal device can be set to '*Obtain an **IP address automatically***'. The MX530/MX880 is preconfigured for dynamic assignment of IP addresses (DHCP) and then assigns the IP address **192.168.0.100**.

   ⚠ **By default, the MX530/MX880 assigns only one IP address!**

   If you have connected a PC to the router for configuration, the IP address 192.168.0.100 assigned to the PC will be assigned to another connected terminal device after 5 minutes (timer preset Lease time) once the PC has been removed. Restarting the router releases the IP address immediately.

   Alternatively, the network settings can also be set permanently in the terminal device:
   - IP address: 192.168.0.100
   - Default Gateway: 192.168.0.1 (LAN IP address of the MX530/MX880)
   - DNS Server: 192.168.0.1 (LAN IP address of the MX530/MX880)

   The IP address range of the DHCP-server should then be changed according to chapter **3.8 DHCP-Server** (Page 30) as 192.168.0.100 is no longer assigned automatically.

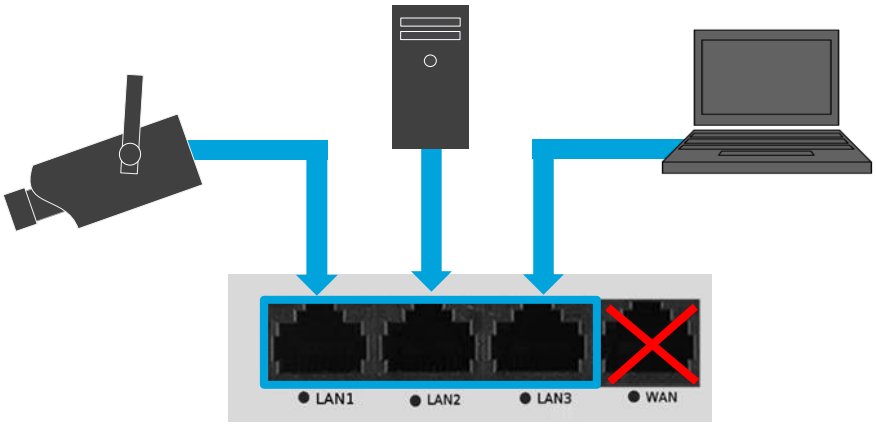
3. All incoming data packets to the WAN IP address of the MX530/MX880 will be forwarded to the IP address **192.168.0.100**. This terminal device is thus accessible via remote access.

   ⚠ When using a **public.IP**, access is possible without restrictions via the Internet. For security reasons, the terminal device should therefore be secured with a firewall against unauthorised access. Additional protection is required if port forwarding is set up only for the required ports according to the Chapter **3.9.2 Port-Forwarding** (Page 33).

2.6.2 Connection of several terminal devices

To connect multiple terminal devices to the MX530/MX880, note the following:

1. Connect the terminal devices to a free LAN socket (LAN1, LAN2 or LAN3) with a network cable. The WAN socket is not intended for connecting terminal devices!



   If more than 3 terminal devices are to be connected, an additional (commercially available) Ethernet switch must be used which is connected to a free LAN port (LAN1, LAN2 or LAN3) of the MX530/MX880.

2. Set the network settings of the connected terminal devices:

   If the terminal devices are to obtain their IP addresses automatically from the MX530/MX880, you must expand the DHCP-server to assign additional IP addresses according to chapter **3.8 DHCP-Server** (Page 30) and, if necessary, set up a fixed assignment according to the chapter **3.8.1**

   Fixed assignment of IP addresses (Page 31).

   Alternatively, you can also set the IP addresses in the terminal devices permanently.

IP address:	192.168.0.2 to 192.168.0.255	
Default Gateway:	192.168.0.1	(LAN IP address of the MX530/MX880)
DNS Server:	192.168.0.1	(LAN IP address of the MX530/MX880)

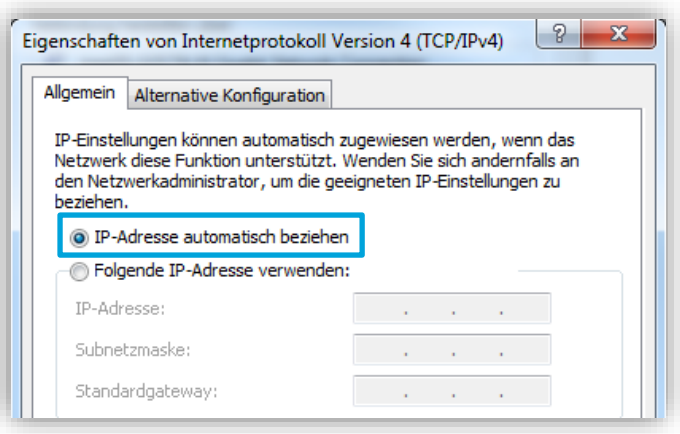
3. If several connected terminals should be accessible remotely, a forwarding according to chapter **3.9.2 Port-Forwarding** (Page 33) must be configured in the router.

   ⚠ If remote access is not desired for any connected terminal device, the default 'DMZ Configuration' should be disabled for security reasons according to Chapter **3.9.1 Host-Forwarding (DMZ Configuration)** (Page 32).

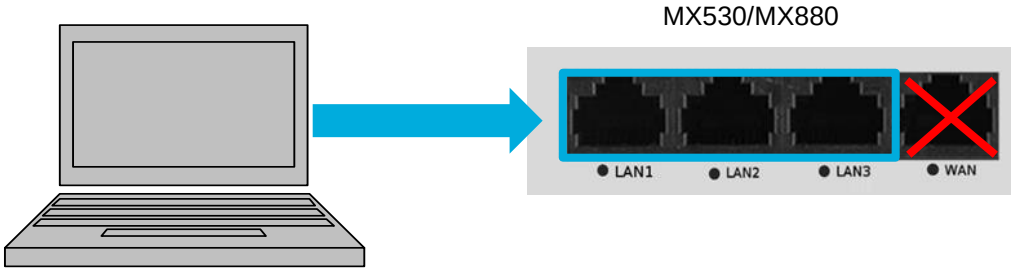
3 Configuration

3.1 Connecting the PC

The network card of the PC can be set to ***Obtain an IP address automatically***.



Plug the network cable of the PC into a **LAN** socket (LAN1, LAN2 or LAN3) of the MX530/MX880. (The WAN socket is not intended for connecting terminal devices!)



The MX530/MX880 is preconfigured for the dynamic assignment of IP addresses (DHCP) and automatically assigns the IP address **192.168.0.100** to the connected PC.

⚠ By default, the MX530/MX880 assigns only one IP address (192.168.0.100) to a connected network device!

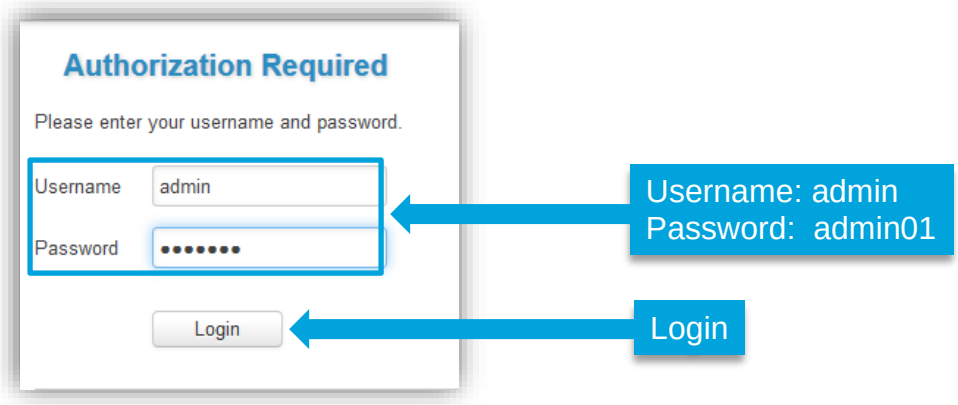
- If another network device is connected that already has the IP address 192.168.0.100, remove this device again.
- The IP address 192.168.0.100 will be **released after 5 minutes** and then assigned to your connected PC. Restarting the MX530/MX880 immediately releases the IP address and then assigns it to your connected PC.
- Alternatively, you can also set the PC NIC to a fixed IP address from the IP address range 192.168.0.2 to 192.168.0.255 (for example, 192.168.0.20).

The PC and MX530/MX880 are now in the same IP address range, allowing the PC to access the MX530/MX880 WebUI using a web browser.

3.2 Login to WebUI

Enter this URL in your web browser: http://**192.168.0.1:8080**
(Or the current IP address of the MX530/MX880, if it has been changed.)

Username: **admin**
Password: **admin01**
(Or the current password, if already changed)



3.2.1 Important notes about the Ping Reboot

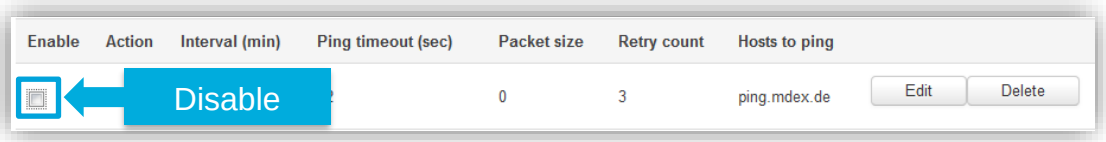
Please note the following about the default Ping Reboot.

⚠ In the MX530/MX880, the automatic ping connection check for the Ping Server **ping.mdex.de** is enabled by default.

Without mobile reception or without connection to mdex, an automatic reboot of the MX530/MX880 is performed every 15 minutes.

- During the MX530/MX880 configuration, Ping Reboot should be **temporarily** disabled to prevent the router from rebooting.

  Services → Ping/Periodic Reboot: tab Ping Reboot



  The changed setting must be saved by clicking on Save.

- The "Ping Reboot" should then be enabled again for normal operation.
- The default server '*ping.mdex.de*" is only accessible from the mdex network!

  If you use the MX530/MX880 without mdex IP service (fixed.IP+ / public.IP) or without mdex SIM, be sure to set a publicly accessible server with Edit, e.g. **public-ping.mdex.de** (185.39.176.22).

ⓘ Detailed instructions can be found in the Chapter **3.11 Ping Reboot** (Page 36).

3.3 Setup Wizard

The Setup Wizard starts when you log in for the first time, allowing you to make the following settings. The Setup Wizard can also be called-up later again at **System → Setup Wizard**.

Step 1 - General

It is imperative that you change the login password of the MX530/MX880 to a secure password. Further details can be found in the Section **3.4 Login Password** (Page 22).

You can set the Time Zone under 'Time Zone Settings'. (For Germany: Europe/Berlin)
More details can be found in the Section **4.3 NTP time server (automatic time synchronization)** (Page 41).

Step 2 - Mobile

Here you can set the mobile settings for the operation of the 'SIM card 1'.

- APN
- PIN number
- Authentication method: None, PAP, CHAP
  ('PAP' must be set for a mobile connection to mdex.)
- Username
- Password
- Service mode: Setting the desired mobile network

More details can be found in the Section **3.5 Mobile settings** (Page 22).

Step 3 - LAN

The network settings of the MX530/MX880 can be customised.
More details can be found in the Section **3.7 Router LAN IP address** (Page 29).

Step 4 - WiFi

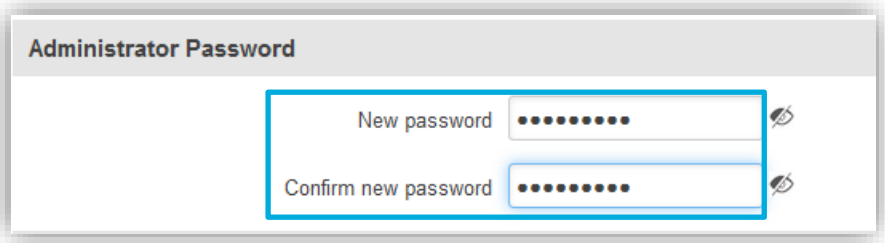
The WIFI network is disabled by default. You can enable and set the WIFI of the MX530/MX880.
More details can be found in the Section **4.1 WiFi (Wireless Access Point)** (Page 38).

3.4 Login Password

The Login password is used to access the WebUI and SSH interface of the MX530/MX880.

⚠ In particular, if the MX530/MX880 is accessible via a public IP address over the Internet, a secure login password must be set for security reasons!

System → Admin Settings:



With **New Password** and **Confirm new password** enter the new MX530/MX880 login password and accept it by clicking on Save.

By clicking on you can display the set password in plain text.

3.5 Mobile settings (SIM)

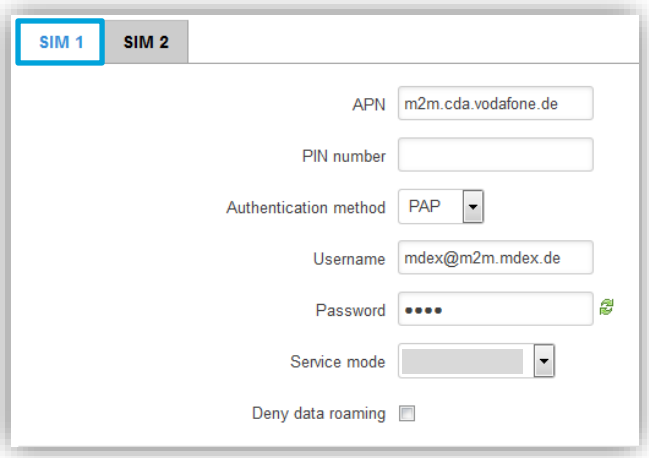
ⓘ The router is preset to operate the preinstalled **mdexSIM Vodafone** (SIM1).

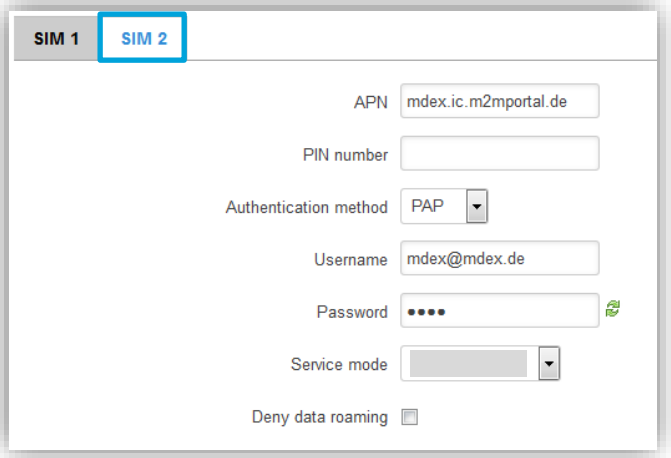
3.5.1 SIM Basic Settings (General)

The mobile settings are preconfigured for **mdexSIM Vodafone** (SIM1) and **mdexSIM Telekom** (SIM2).

When using a different SIM card, the mobile settings must be adjusted accordingly.

Network → Mobile (SIM): tab General





APN:	Access point of your mobile provider for the mobile connection. For use with mdex, please refer to your mdex order confirmation e-mail or the mdex Management Portal. ⓘ The APN is already set for the preinstalled **mdexSIM**.
PIN number:	PIN of the SIM card. As a mdex SIM usually has no active PIN, please leave this field blank when using a mdex SIM. We recommend that you do not provide your SIM card with a PIN. Otherwise, if the PIN is wrong, the SIM card will be locked immediately.
Authentication method:	Authentication method (PAP, CHAP or None). To log into mdex, PAP must be set.
Username:	Username (Username/Device-Username) of the mobile operator. For use with mdex, please refer to your mdex order confirmation e-mail or the mdex Management Portal. ⓘ For the preinstalled **mdexSIM** the username is already preset. When using the, **mdexSIM** Vodafone' incl. **mdex public.IP** a different username may be required as per Chapter **1.5.1 mdex SIM Vodafone (SIM1)** (Page 8).
Password:	Enter the APN password of your mobile network operator here. For the use of a mdex service, please refer to your mdex order confirmation e-mail or the mdex Management Portal. ⓘ For the preinstalled **mdexSIM** the password **mdex** is already preset.
Service mode:	Here you can set the priority for the desired mobile network to establish mobile connection. **4G + 3G + 2G:** MX880 only: The mobile connection is established with the following priority depending on network availability: 4G (LTE) → 3G Network (UMTS/HSPA) → 2G Network (GPRS/EDGE). **4G + 3G**: MX880 only: The mobile connection is established with the following priority depending on network availability: 4G network (LTE) → 3G network (UMTS/HSPA). (1 **4G + 2G:** MX880 only: The mobile connection is established with the following priority depending on network availability: 4G (LTE) → 2G network (GPRS/EDGE). (1 **3G + 2G:** The mobile connection is established with the following priority depending on network availability: 3G network (UMTS/HSPA) → 2G network (GPRS/EDGE). (1

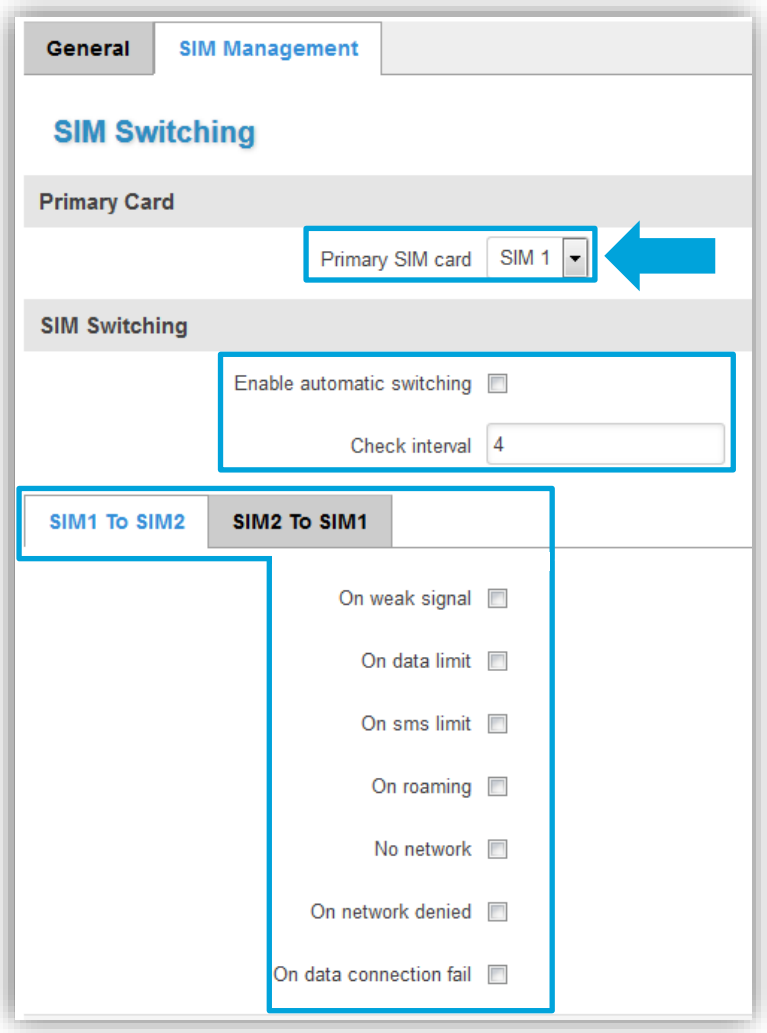
	4G only: MX880 only: The connection is made only to the 4G mobile network (LTE). [1)] **3G (UMTS) only:** The connection is made only to the 3G mobile network (HSPA/UMTS). [1)] **2G (GPRS) only:** The connection is made only to the 2G mobile network (GPRS/EDGE). [1)] **Automatic:** The best possible mobile connection is established. (recommended)
Deny data roaming:	Roaming block to prevent a mobile connection to third party mobile networks. ☐ Roaming is possible if the SIM card is authorized. (default setting) ⚠ By roaming, foreign mobile networks (e.g. abroad or border regions) can be used, which can lead to high mobile costs depending on the SIM card tariff! ☑ Roaming is not allowed by router. The SIM card may only use its own mobile network

1) These settings only make sense if specific mobile networks are to be used selectively (for example, with incompatible SIM cards, reception problems or interference in certain mobile networks).

3.5.2 SIM Management

In the menu 'SIM Management' settings can be made for the use and switching of the installed SIM cards.

Network → Mobile: tab **SIM Management**



Preconfiguration:

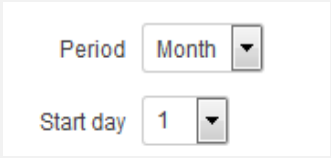
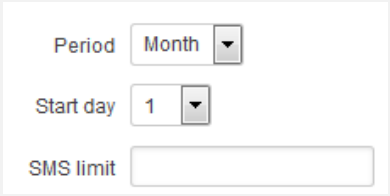
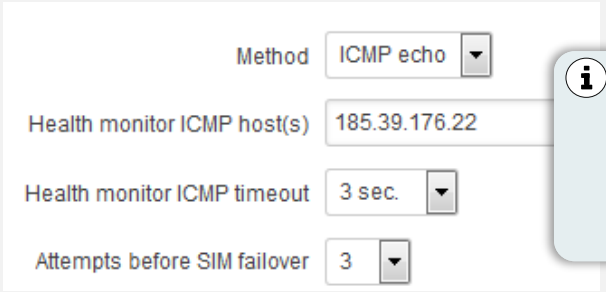
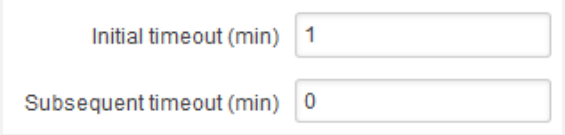
SIM 1: **mdexSIM Vodafone**
SIM 2: **mdexSIM Telekom**

Primary SIM card:	Defining the SIM card for the primary establishment of the mobile connection (SIM 1 or SIM 2).

SIM Switching:

Enable automatic switching:	☑ Automatic switching of SIM cards enabled. With a defined event, the mobile connection of the primary SIM card is terminated and automatically established with the secondary SIM card.
Check interval:	Time interval (in seconds) for checking if a defined SIM card switching event has occurred.

SIM1 TO SIM2: Adjustable events for switching from SIM1 to SIM2.
SIM2 TO SIM1: Adjustable events for switching from SIM2 to SIM1.

On weak signal:	If the signal strength is worse than in the field, the 'signal strength (dBm)' is adjusted. (Input of signal strength in dBm, e.g. -100)
On data limit:	If the data volume is reached in the set period. 
On sms limit:	If the number of SMS has been reached in the set period. 
On roaming:	If roaming has been detected.
No network:	If no mobile network has been found for this SIM card.
On network denied:	If the mobile connection was rejected.
On data connection fail:	**ICMP Echo** Method (recommended): If the set target device at Health Monitor ICMP host(s) has not responded to ping within the 'Health Monitor ICMP timeout period' and the number of failed attempts has been reached:  **185.39.176.22** (official mdex ping server) is accessible from the internet and mobile network. **LCP Echo** Method: Monitoring the internal modem connection. (Data connection is not recommended for monitoring the SIM card.)
Switch back to primary SIM card after timeout:	After expiry of the timer '**Initial timeout (min)**', the mobile connection is established again with the 'Primary SIM''. If this connection fails with the 'Primary SIM', the next connection attempt will not be made until the timer '**Initial timeout (min)**' + the timer ,**Subsequent timeout (min)**' expires. 

3.6 mdex OpenVPN-Client

The built-in OpenVPN Client of the router is designed to use an mdex IP-service via OpenVPN, e.g.:

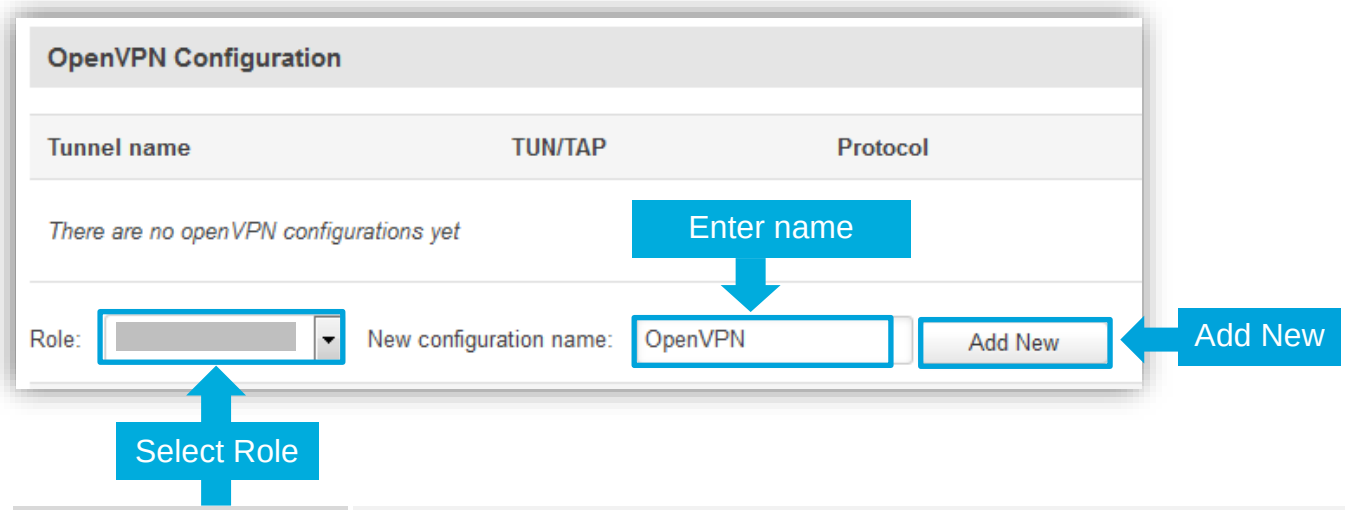
- mdex fixed.IP+ **via OpenVPN**
- mdex public.IP **via OpenVPN**
- mdex mobile.LAN

⚠ The access data of the **mdex control centre tunnel** are intended only for PCs/smartphones and must not be used in the OpenVPN Client of the MX530/MX880!

When using a **mdexSIM** or a mdex mobile access, where connecting to mdex is done directly with the SIM card, the use of the OpenVPN Client in the MX530/MX880 is not required!

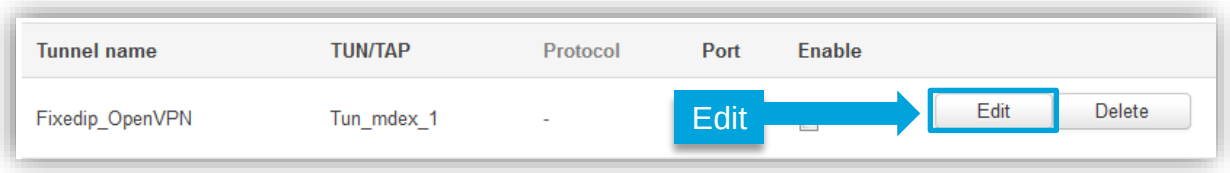
Configure OpenVPN-Client:

1. Under **VPN → OpenVPN** at '**Role**' select the **mdex OpenVPN Access** for the ordered mdex service (mdex fixed.IP+ or mdex public.IP), enter a name (e.g. OpenVPN) and click on button Add New.

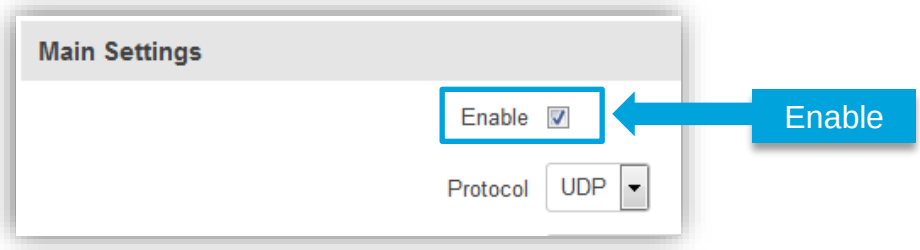


mdex fixed.IP+:	For using mdex fixed.IP+ via OpenVPN or mdex mobile.LAN.
mdex public.IP:	Only for using mdex public.IP via OpenVPN. ⚠ To increase data throughput, OpenVPN encryption is disabled. Since only a public.IP requires no encryption, please don´t use this role for a 'fixed.IP+ via OpenVPN'!

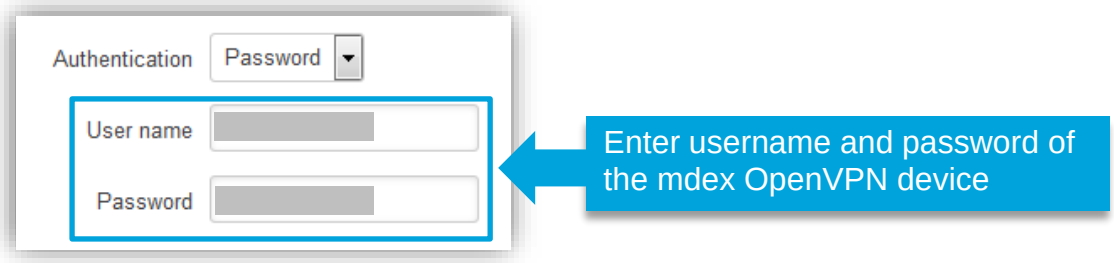
2. Once the OpenVPN Client is added, click on the Edit button.



3. The OpenVPN Client must be enabled by activating the check box: **Enable** ☑.



4. Enter the **Username** and **Password** of the desired mdex OpenVPN access.



⚠ The access data of the **mdex control centre tunnel** may not be used here!

ⓘ The OpenVPN access data (Username & Password) of the mdex OpenVPN access can be found in the mdex order confirmation e-mail or in the mdex Management Portal at **https://manager.mdex.de**.

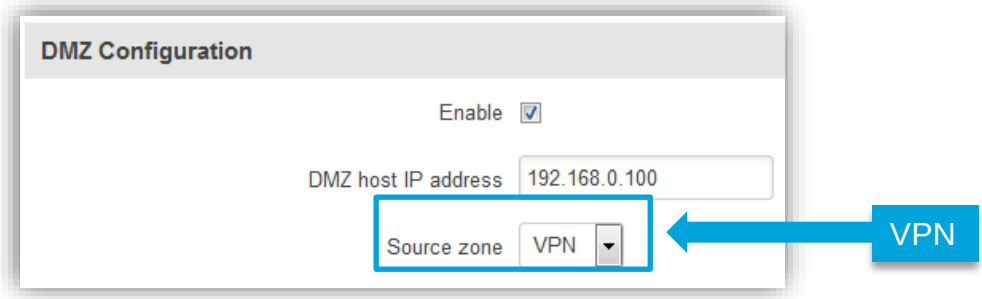
5. Save the OpenVPN settings by clicking on Save.
The MX530/MX880's OpenVPN Client now establishes an OpenVPN connection to mdex via the MX530/MX880's Internet connection (e.g. SIM card).

ⓘ The OpenVPN status can be queried under **Status → Network:** OpenVPN.
More details can be found in the Chapter **4.2.3 OpenVPN Status** (P. 41).

6. For forwarding, the **Source zone** must be switched to **VPN**.

⚠ With the source zone setting '**WAN**' no forwarding is performed when using the 'mdex fixed.IP+ / public.IP' via OpenVPN.

Network → Port-Forwarding: DMZ Configuration

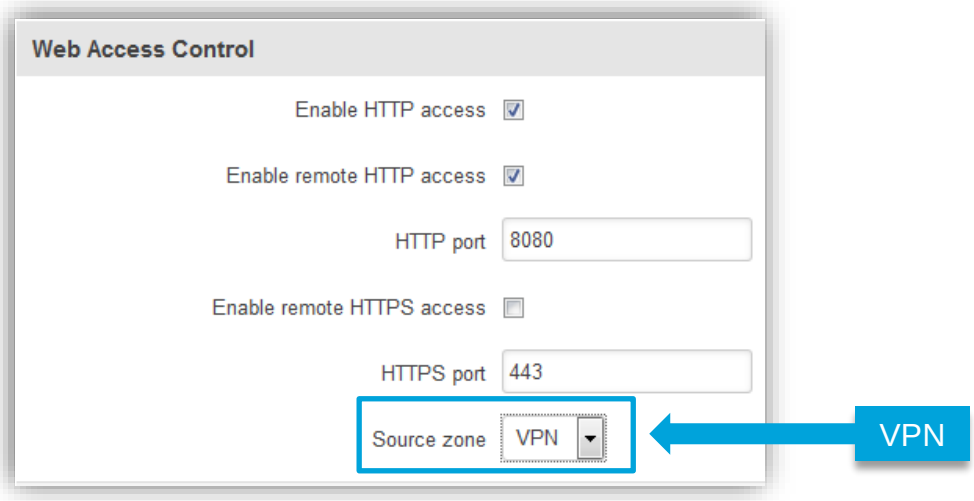


Even when using individual port forwarding according to the chapter **3.9 Forwarding** (Page 32) basically the 'VPN' must now be used as the 'source zone'.

7. For the MX530/MX880 remote access, the **Source zone** must be switched to **VPN**.

⚠ If the source zone **WAN** is selected, the MX530/MX880 router is not accessible by remote with mdex fixed.IP+ / public.IP via OpenVPN!

Services → HTTP/SSH: Web Access Control



ⓘ More information on configuring the MX530/MX880 remote access can be found in the Chapter **3.10 Configuration Access / Remote Access** (Page 34).

3.7 Router LAN IP address

The default LAN network address (192.168.0.1) of the MX530/MX880 can be changed.

Network → LAN: Configuration

IP address:	Current LAN IP address of the MX530/MX880
IP netmask:	Netmask of the MX530/MX880

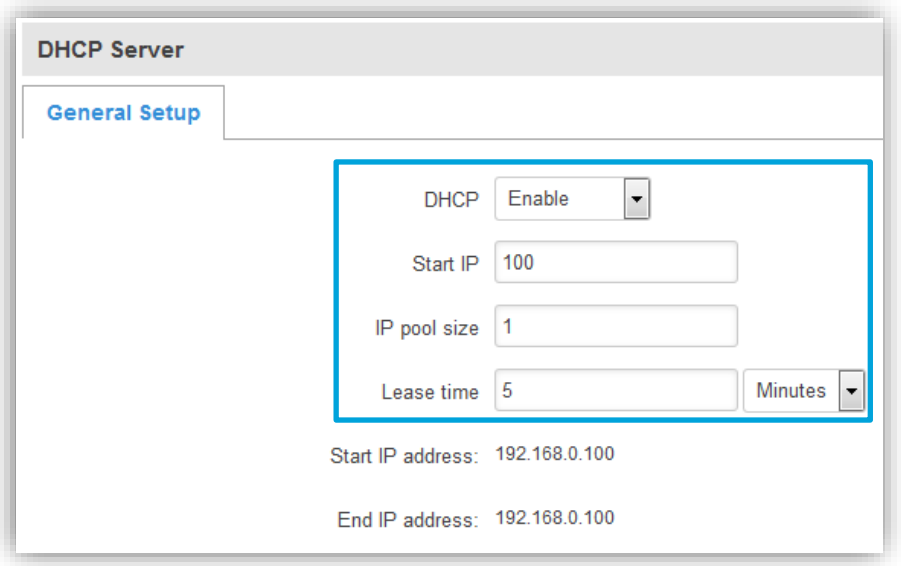
3.8 DHCP-Server

The integrated DHCP-server automatically assigns an IP address to the connected network device. The network device must be set to '*Obtain an IP address automatically*' (DHCP).

The DHCP-server is preset to assign the IP address **192.168.0.100**.

The default settings of the DHCP-server can be changed under *Network → LAN*.

Network → LAN: DHCP-Server



DHCP:	Enables or Disables the DHCP-server.
Start IP:	First IP address of the configured MX530/MX880 netmask, which the DHCP-server should assign to a connected network device.
IP pool size	Number of IP addresses to be assigned by the DHCP-server. **Example** LAN 'IP address': 192.168.1.250 LAN 'IP netmask': 255.255.255.0 DHCP 'Start IP': 51 DHCP 'IP pool size': 10 The DHCP-server assigns 10 IP addresses, starting with 51. IP address of the set netmask: 192.168.1.51 to 192.168.1.60
Lease time:	For this period of time in minutes or hours, an assigned IP address remains reserved for a terminal device. Only after this timer has elapsed can another terminal device automatically obtain this IP address.

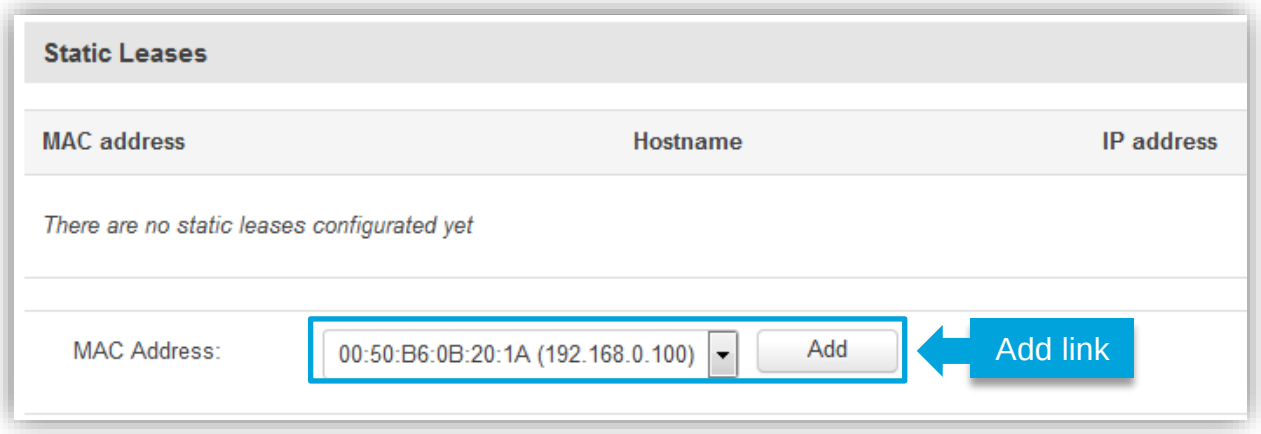
3.8.1 Fixed assignment of IP addresses

If certain terminal devices are always to receive the same IP address from the MX530/MX880's DHCP-server, they can be assigned permanently using the MAC address.

This fixed assignment is e.g. required if port forwarding for certain terminal devices has been set for remote access and the respective terminal device is to obtain its IP address automatically.

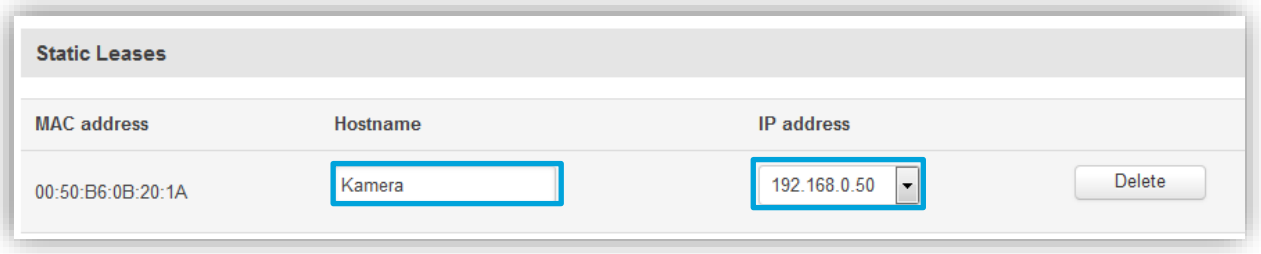
1. The terminal device must have communicated with the MX530/MX880 router, e.g. to have already obtained an IP address automatically from the MX530/MX880.

2. Select at **Network → LAN** under **Static Leases** in the dropdown box **MAC Address** the desired terminal device and add it by clicking on button **Add**.



At **Status → Network** in tab **LAN** all connected terminal devices (including MAC address, IP address and lease time) that have currently obtained an IP address from the MX530/MX880 DHCP-server are displayed for **DHCP Leases**.

3. At **Host name** enter a name for the link and under **IP address** select the desired IP address which should be assigned to this terminal device.



With 'IP address' you can also enter another IP address outside the defined IP address range of the MX530/MX880 DHCP-server, e.g. 192.168.0.50. The terminal device with this MAC address will henceforth be assigned this set IP address.

- All IP addresses must be in the LAN IP address range of the router.
- If necessary, adjust the port forwarding according to Chapter **3.9 Forwarding** (Page 32) so that this terminal device can be reached remotely.

4. If necessary, repeat this process until all desired links are set in the router.
To save the links, click on **Save**.

3.9 Forwarding

For remote access to the connected terminal devices, the incoming data packets must be forwarded to the local IP address of the terminal device.

By default, all incoming ports and protocols to the IP address of the SIM card (WAN) are forwarded to the local IP address **192.168.0.100**.

When using the integrated **mdex OpenVPN-Client** (Chapter **3.6**, Page 27) the **Source zone** must be switched to **VPN**!

The MX530/MX880 considers incoming ports in the following priority:

1. Remote access ports according to chapter **3.10 Configuration Access / Remote Access**
2. Defined ports according to chapter **3.9.2 Port-Forwarding**
3. All other ports to the forwarding target as per **3.9.1 Host-Forwarding (DMZ Configuration)**

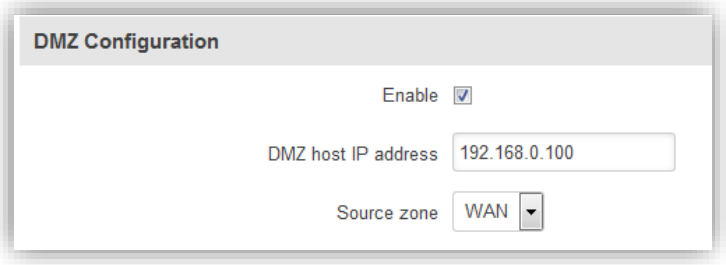
3.9.1 Host-Forwarding (DMZ Configuration)

All ports and protocols are forwarded to the selected target device.

Only the enabled ports for MX530/MX880 remote access (according to **3.10**, Page 34) and configured port forwarding (according to chapter **3.9.2 Port-Forwarding** (Page 33) are not forwarded to the 'DMZ host IP address'.

When using a **public.IP**, access is possible without restrictions via the Internet.
The terminal device should therefore be secured against unauthorised access via the Internet with a firewall. More protection is available, if instead only the required ports are forwarded according to Chapter **3.9.2 Port-Forwarding** (Page 33).

Network → Port-Forwarding: **DMZ Configuration**

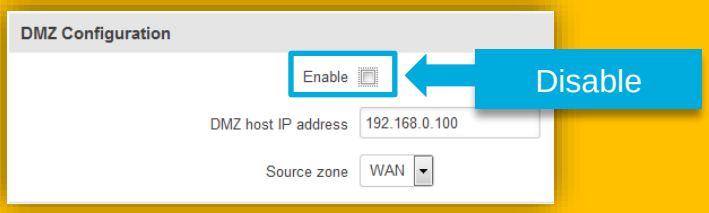


Enable:	☑ Forwarding of all ports and protocols enabled ☐ Forwarding of all ports and protocols disabled
DMZ host IP address:	All data packets are forwarded to this IP address.
Source zone:	Interface of incoming data packets for remote access: **WAN:** Remote access to terminal device is possible via the fixed.IP+/public.IP of the SIM card (or external WAN IP address). **VPN:** Remote access to terminal device is possible via the fixed.IP+/public.IP of the **mdex OpenVPN-Client** (chapter **3.6**, Page 27).

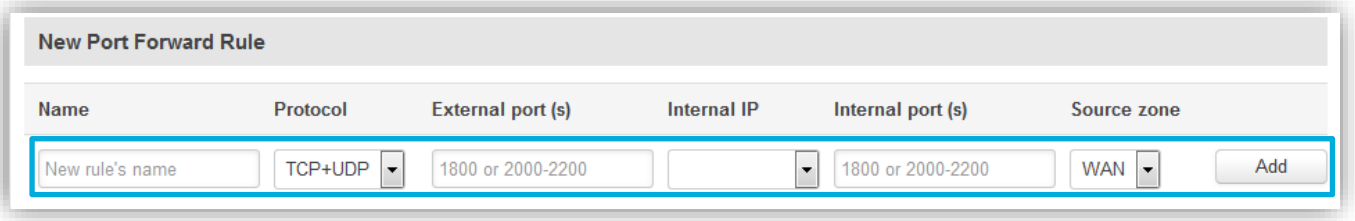
3.9.2 Port-Forwarding

With port forwarding, you can connect multiple devices to the MX530/MX880 and remotely reach them via the external IP address using the respective port.

⚠ Undefined ports are forwarded to the target device 'DMZ host IP address'.
If this is not desired **DMZ Configuration** must be disabled.



Network → Port-Forwarding: New Port-Forwarding Rule



Name:	Desired name of this forwarding.
Protocol:	Set the desired protocol (TCP/UDP).
External port(s):	Incoming port for forwarding. Port ranges can also be set. Example: 2000-2200 = For ports 2000, 2001,2002, ... to 2200
Internal IP:	Target IP address of the terminal device.
Internal port(s):	Target port of the terminal devices. Port ranges can also be defined. Example: 2000-2200 = For ports 2000, 2001,2002, ... to 2200
Source zone:	Interface of incoming data packets for remote access: **WAN:** Remote access to terminal device is possible via the fixed.IP+/public.IP of the SIM card (or external WAN IP address). **VPN:** Remote access to terminal device is possible via the fixed.IP+/public.IP of the **mdex OpenVPN-Client** (chapter **3.6**, Page 27).
Add :	The forwarding is added to **Port-Forwarding Rules** and can later be adjusted with Edit or removed with Delete.
Save :	All changed settings are accepted and saved.

3.10 Configuration Access / Remote Access

Local configuration access and remote access to the MX530/MX880 can be customised.

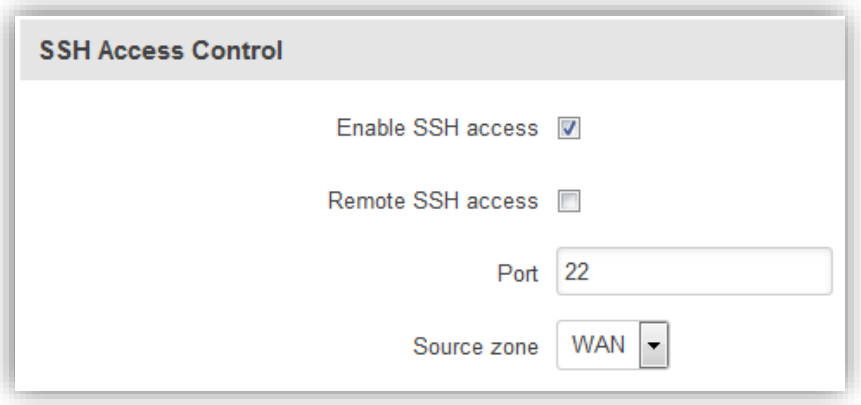
ⓘ The web interface is already accessible locally and remotely via port 8080.

⚠ When using the integrated **mdex OpenVPN-Client** (Chapter **3.6**, Page 27) the **Source zone** must be switched to **VPN**!

3.10.1 SSH access

Local and remote access to the Secure Shell (SSH) interface of the MX530/MX880 can be set. SSH access is only required in special cases. The SSH-Login is done with the username "root".

Services → HTTP/SSH: SSH Access Control



Enable SSH access:	Enables local SSH access to the MX530/MX880. ☑ SSH access enabled ☐ SSH access disabled
Remote SSH Access:	Enables SSH remote access to the MX530/MX880. ☑ SSH remote access enabled[1] ☐ SSH remote access disabled For security reasons, SSH remote access should be disabled.
Port:	Port for SSH access (port 22 is the default port)
Source zone:	Interface of incoming data packets for remote access: **WAN:** Remote access to the router is possible via the fixed.IP+/public.IP of the SIM card (or external WAN IP address) **VPN:** Remote access to the router is possible via the fixed.IP+/public.IP of the **mdex OpenVPN-Client** (chapter **3.6**, Page 27).

1) Remote access to the set port will be answered by the MX530/MX880, even if a forwarding to another device has been set up for this port.

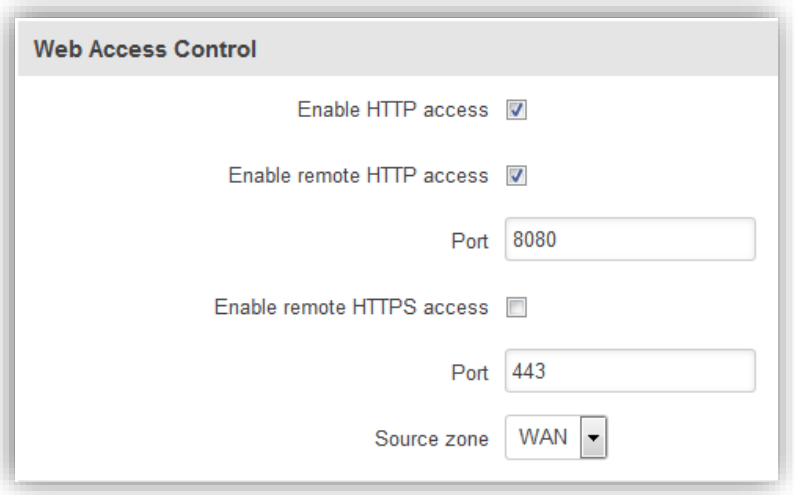
3.10.2 Access to the WebUI

Local access and remote access to the WebUI of the MX530/MX880 can be customised.

The web interface is already accessible locally and remotely via port 8080.

When using the integrated **mdex OpenVPN-Client** (Chapter 3.6, Page 27) the **Source zone** must be switched to **VPN**!

Services → HTTP/SSH: **Web Access Control**



Enable HTTP access:	Enables local HTTP access to the WebUI ☑ HTTP access enabled ☐ HTTP access disabled
Enable remote HTTP access:	Enables HTTP remote access to the WebUI ☑ HTTP remote access enabled [1 ☐ HTTP remote access disabled
HTTP Port:	HTTP port for access to the WebUI.
Enable remote HTTPS access:	Enables HTTPS remote access to the WebUI ☑ HTTPS remote access enabled [1 ☐ HTTPS remote access disabled
HTTPS Port:	HTTPS port for accessing the WebUI
Source zone:	Interface of incoming data packets for remote access: **WAN:** Remote access to the router is possible via the fixed.IP+/public.IP of the SIM card (or external WAN IP address) **VPN:** Remote access to the router is possible via the fixed.IP+/public.IP of the **mdex OpenVPN-Client** (chapter 3.6, Page 27).

1) Remote access to the set port will be answered by the MX530/MX880, even if a forwarding to another device has been set up for this port.

3.11 Ping Reboot

In order for the MX530/MX880 and the terminal devices to always be reliably accessible, even after maintenance work or malfunctions in the mobile network, the ping reboot should be enabled.

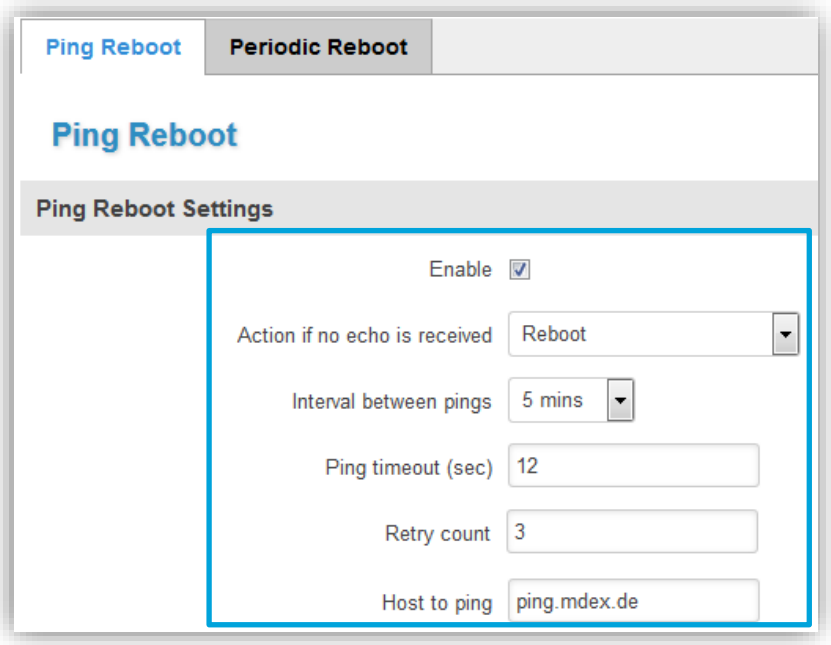
⚠ The Ping Reboot function is enabled for the ping server **ping.mdex.de**.

However, the server *ping.mdex.de* is only accessible from the mdex network!
If you use the MX530/MX880 with your own SIM card **without** mdex IP service (fixed.IP+ / public.IP), be sure to set up a publicly accessible server, e.g. **public-ping.mdex.de** (185.39.176.22).

The MX530/MX880 will periodically ping the target server. If there is no response from the target server within the defined time period, the router will assume a connection error and initiate a desired reconnect action.

Services → Ping/Periodic Reboot: tab **Ping Reboot**

The ping reboot function can be adjusted with Edit.



Enable:	Enables or disables the ping reboot feature
Action:	This action is performed with a detected connection error: Reboot: A restart of the MX530/MX880 is triggered. Modem restart: The mobile modem will be restarted. Restart mobile connection: The mobile connection is terminated and restored. (Re-)Register: Renewed registration in the mobile network. None: No action is triggered.

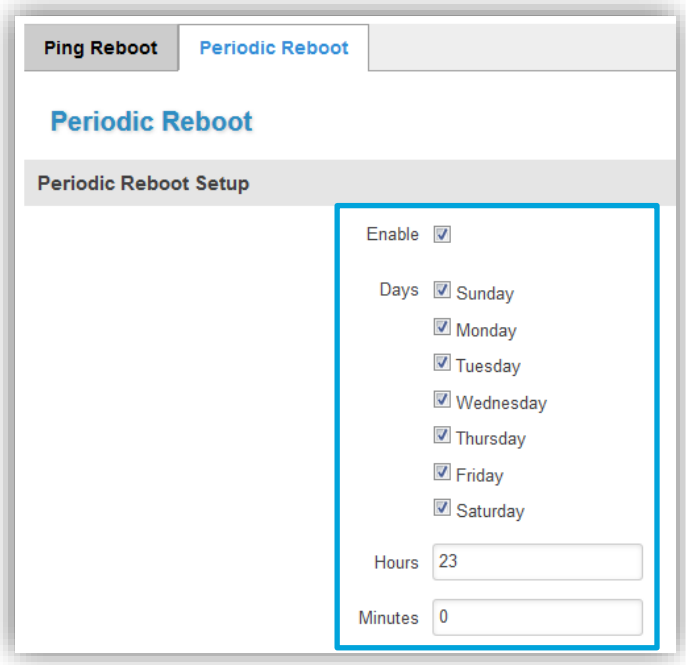
Interval between pings:	Interval in minutes at which the MX530/MX880 sends a ping to the selected target server. (Minimum setting is 5 minutes). Please note that each ping generates additional data. The smaller the interval is set, i.e. the more often a ping is sent, the more data is generated in the mobile network.
Ping timeout (sec):	If the target server does not respond within this time period (in seconds), it will be considered an unsuccessful ping attempt.
Retry count:	If after the set attempts no response has been received from the target server, the MX530/MX880 will trigger the set action.
Host to ping:	Target server for connection verification ⚠ If you use the MX530/MX880 with your own SIM card **without** mdex IP service (fixed.IP+ / public.IP), be sure to set up a publicly accessible server, e.g. **public-ping.mdex.de** (185.39.176.22).

3.12 Periodic Reboot

At the set time (Hours, Minutes), the router automatically reboots on the desired days of the week.

ⓘ According to pre-configuration, an automatic restart is triggered daily between 23:00 and 23:59 pm.

Services → Ping/Periodic Reboot: tab **Periodic Reboot**



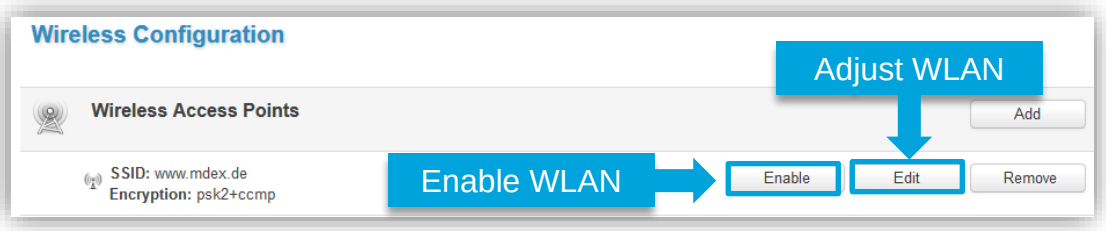
This feature can be disabled with the **Enable** ☐ setting.

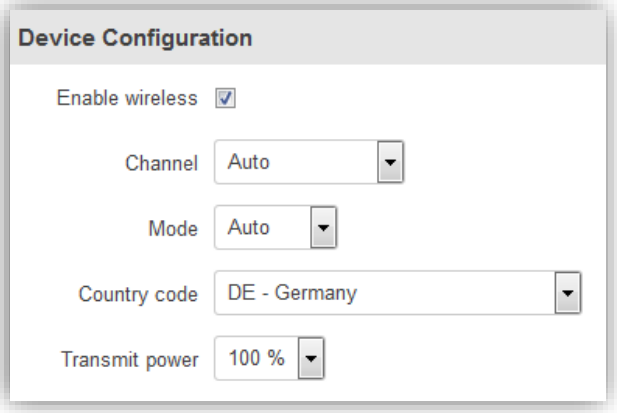
4 Additional functions

4.1 WiFi (Wireless Access Point)

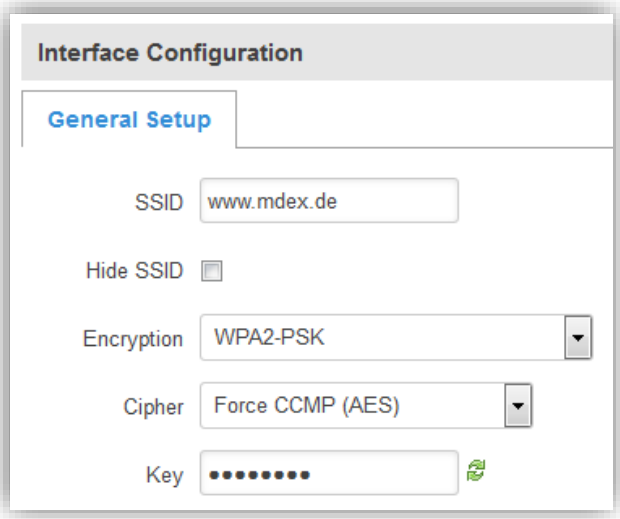
A **Wireless Access Point** can be enabled in the MX530/MX880 to connect network devices via WIFI. The WIFI is already preconfigured, but still disabled at delivery.

The WIFI access point of the router can be activated at **Network → WLAN** with Enable and configured with Edit.





Enable wireless:	Enables/disables WIFI
Channel:	WIFI channel
Mode:	WIFI mode Auto, 802.11b, 802.11g, 802.11 g+n
Country code:	MX530/MX880 location
Transmit power:	Desired transmission power



SSID:	WIFI Name
Hide SSID:	Hide WIFI name
Encryption:	Encryption protocol
Cipher:	Encryption algorithm
Key:	WIFI network key Display in plain text:

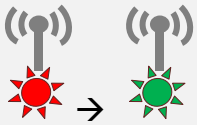
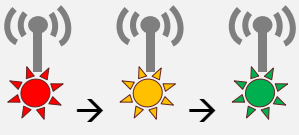
4.2 Connection status and signal strength

Mobile connection status and available signal strength can be read from different locations on the MX530/MX880.

4.2.1 LED Status indicators

Mobile signal strength
The current mobile signal strength is indicated by the green LEDs. If no LED lights up, there is currently no mobile reception.

Mobile connection status

LED display	Status
 lights up/flickers	**LED lights up continuously** (& flickers during data transmission) Mobile & data connection successfully established in the following network: ● **red**: 2G Network ● **orange**: 3G Network ● **green**: 4G Network
 1 S	**LED flashes in monochrome at one-second intervals** No data transmission possible! Only a mobile connection without data connection was established in the following network: **red**: 2G Network **orange**: 3G Network **green**: 4G Network Possible causes: Incorrect APN access data, SIM without data tariff
 0.5 S 0.5 S	**LED flashes red → green every 0.5 seconds** No data transmission possible! Mobile reception has been detected, but the mobile connection could not be established. Possible causes: ▪ SIM card inactive, locked, missing or wrong ‘primary SIM’ set. ▪ SIM PIN missing / wrong (only for SIMs with active SIM PIN protection)
 0.5 S 0.5 S 0.5 S	**LED flashes red → orange → green every 0.5 seconds** No data transmission possible! Router is in mobile setup, but the connection has not yet been established.
	**LED does not light up** No data transmission possible! No mobile network found. Possible causes: Antenna connected incorrectly, no reception

4.2.2 Mobile Status (WebUI)

To determine the current mobile reception power for a good data transmission, different reception values are relevant depending on the mobile network. A detailed display of the relevant values can be found in the MX530/MX880 at **Status → Network** in the Tab Mobile:

4G connection (only MX880)	
Mobile	
Data connection state	Connected
IMEI	
IMSI	
ICCID	
Sim card state	Ready
Signal strength	-59 dBm
Cell ID	0539D01
RSRP	-89 dBm
RSRQ	-9 dBm
SINR	-14 dBm
Operator	Vodafone.de
Operator state	Registered (home)
Connection type	4G (LTE)

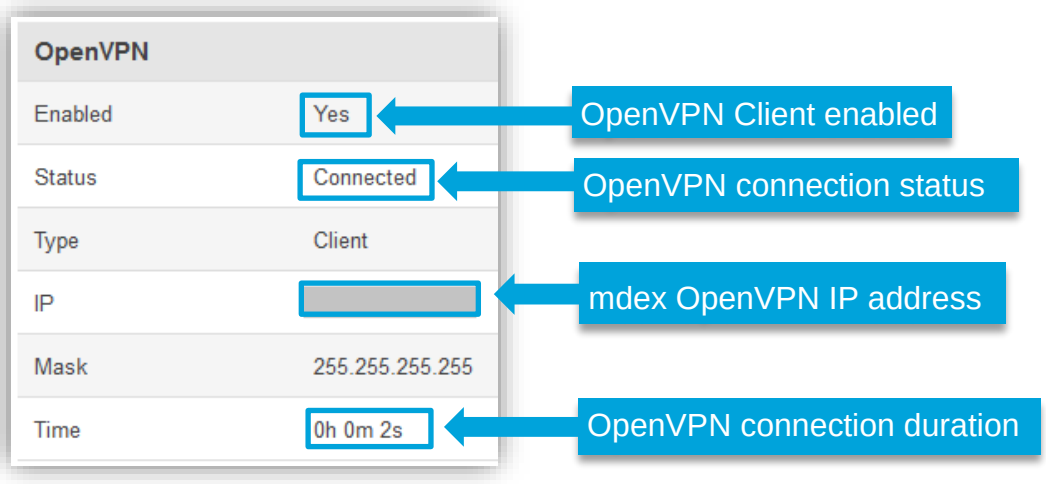
3G / 2G connection	
Mobile	
Data connection state	Connected
IMEI	
IMSI	
ICCID	
Sim card state	Ready
Signal strength	-75 dBm
Cell ID	29536E7
RSCP	-82 dBm
Ec/Io	-4 dBm
Operator	Vodafone.de
Operator state	Registered (home)
Connection type	3G (WCDMA)

RSRP (**R**eferece **S**ignal **R**eceived **P**ower)		**RSRQ** (**R**eference **S**ignal **R**eceived **Q**uality)		**RSSI** (3G) (**R**eceived **S**ignal **S**trength **I**ndicator)		**RSSI** (2G) (**R**eceived **S**ignal **S**trength **I**ndicator)	
dBm	Data transfer	dBm	Data transfer	dBm	Data transfer	dBm	Data transfer
-75	optimal	-3	optimal	-70	optimal	-60	optimal
-80		-6		-75	good	-65	
-85	good	-9	good	-80		-70	good
-90		-12		-85		-75	
-95		-15	possibly interrupted	-90	possibly interrupted	-80	possibly interrupted
-100	possibly interrupted	-18		-95		-85	
-105				-100		-90	
- 110	not possible		not possible	-105	not possible	-95	not possible

4.2.3 OpenVPN Status

Display the OpenVPN connection status of the MX530/MX880.

Status → Network: tab **OpenVPN**



4.3 NTP time server (automatic time synchronization)

The automatic time synchronization is already preset for the NTP Server **time.mdex.de** .

You can adjust or disable the settings under **Services → NTP** in tab **General**.

Under **Services → NTP** in tab **Time Servers** you can remove the default time server with Delete and add another time server with Add.

4.4 Backup & Restore configuration

The configuration of the MX530/MX880 can be saved as backup and restored.

System → Config Profiles: tab **Backup**

Backup configuration:

1. Under **Backup Configuration**, click on the button Download.
2. Select a location for the MX530/MX880 configuration file.
3. The MX530/MX880 configuration is saved as '**backup…..tar.gz**' file.

Restore configuration:

1. Under **Restore Configuration**, select **Upgrade from file**.
2. Click on button Browse... and select the desired configuration file.
3. Click on the button Upload archieve.
4. The configuration file will now be transferred and the router will be restarted.
   All current configuration settings will be overwritten!
5. After the restart, the loaded router configuration is enabled.
   (The router is now reachable with the IP address and port of the new configuration.)

4.5 Reboot

With rebooting of the MX530/MX880 the configuration settings are retained. Only the mobile connection (and possibly OpenVPN connection) is re-established.
The restart can be done with the following methods.

RESET button

Press the RESET button briefly (1-3 seconds) with a pointed object, then reboot the MX530/MX880. The stored settings of the router are retained.

⚠ If you press and hold the reset button for more than 5 seconds, all settings that have already been made will be deleted and the MX530/MX880 will be reset to factory defaultss.

WebUI

Under **System → Reboot** you can reboot the MX530/MX880 by clicking on the button Reboot.
The stored settings of the router are retained.

4.6 Reset to factory defaults

The MX530/MX880 can be reset to factory defaults using one of the following methods.

⚠ All settings already made will be deleted. The MX530/MX880 is reset to the default setting as per Chapter **1.3 Preconfiguration (factory defaults)** (Page 6).

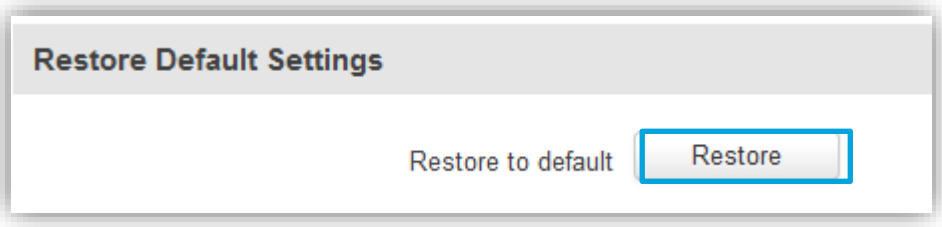
RESET button

The MX530/MX880 must be started. Once the boot process is complete, press the **RESET** button with a pointed object for **more than 5 seconds** until all 5 LEDs of 'Mobile signal strength' light up, then release.

The MX530/MX880 router is now reset to factory defaults.
The reset is complete as soon as you can reconnect to the URL **http://192.168.0.1:8080**.

WebUI

System → Admin Settings: Restore Default Settings



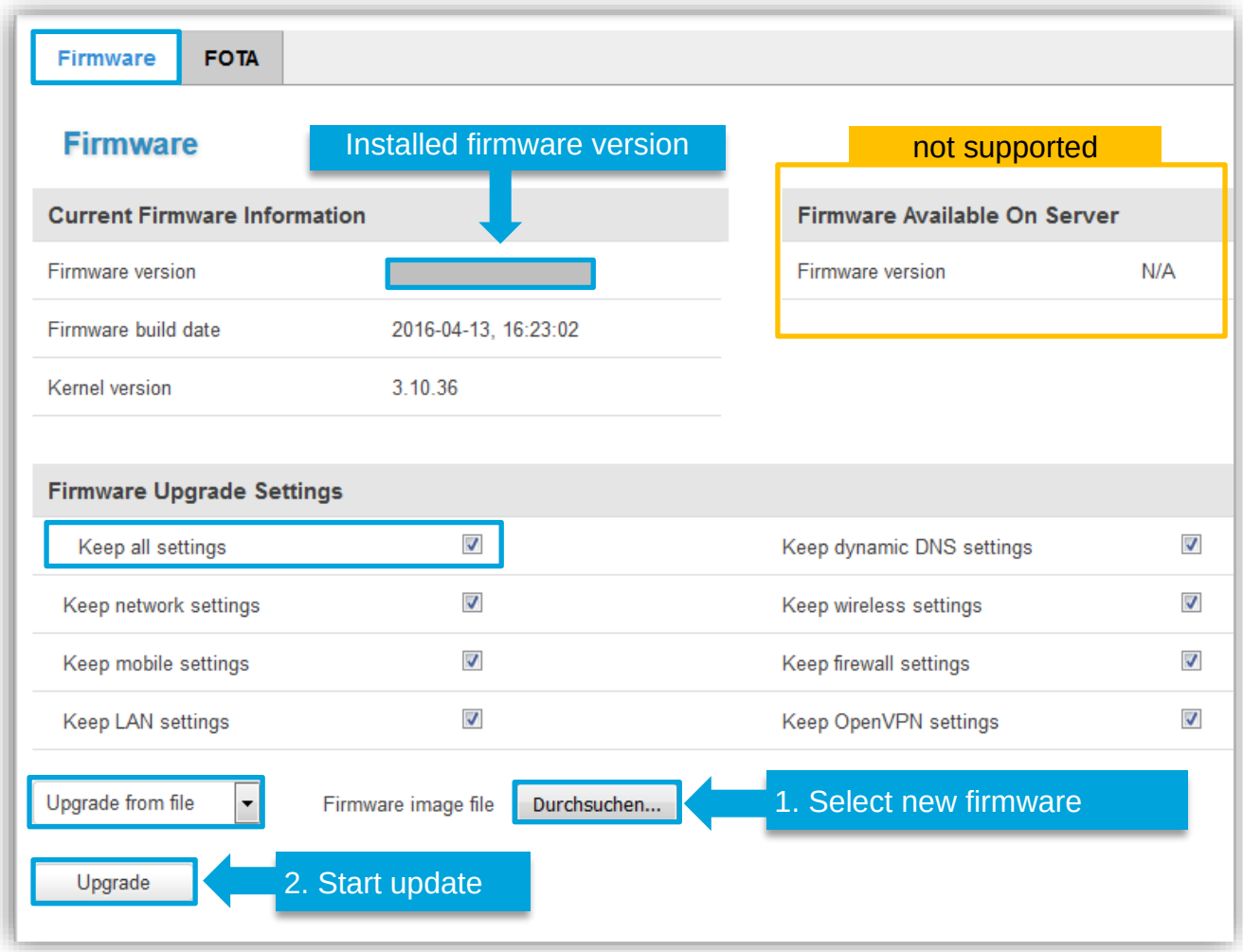
Click on the button Restore and confirm the message '*Really Restore all changes?*'.
The MX530/MX880 router is now reset to factory defaults.

4.7 Firmware Update

If a new firmware of the MX530/MX880 is available, it can be updated.

Current router firmware can be downloaded from the mdex Support page at **https://wiki.mdex.de** → **Downloads**

System → Firmware:



Perform firmware update:

1. The setting '**Keep all settings'** should be **enabled**.

   If the options available under **Firmware Upgrade Settings** are disabled, the current configuration settings are reset during the update!

2. Set **Upgrade from file** and select the new firmware file (*.bin) at Browse... .
3. To upgrade the firmware, click on button Upgrade and confirm the following message with Proceed. The update will be executed.

   The power supply must not be interrupted during the update!

4.8 Expert Mode

Experienced users will find additional setting options in Expert Mode for using additional functions of the MX530/MX880.

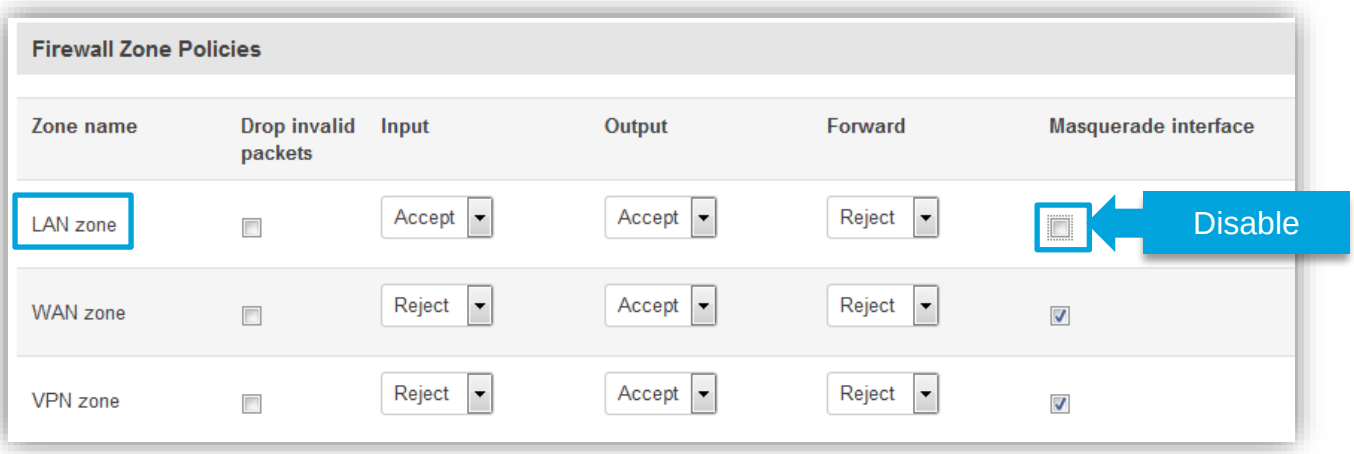
To enable the **Expert Mode** please click on **Expert Mode: off** at right top.
The status then changes to **Expert Mode: on.**

⚠ Please note, that the mdex Customer Service cannot provide support for the additional features of the Expert Mode.

4.9 IPsec connection (to plugged VPN-Router)

To establish an IPsec connection to your own IPsec VPN router connected to the MX530/MX880, please note the following setup steps:

1. Connect the IPsec VPN router to a LAN port and assign it an IP address. See also chapter **2.6.1 Connection of only one terminal device** (Page 17).
   Please note that the MX530/MX880 LAN IP must be used as default gateway and DNS server.
2. Set up a forwarding to the connected VPN router according to chapter **3.9.1 Host-Forwarding (DMZ Configuration)** (Page 32).
3. In the MX530/MX880 under **Network → Firewall:** **Firewall Zone Policies**, the "Masquerade Interface" for the **LAN zone** must be disabled.



4. In the IPsec VPN settings of your VPN routers/clients, enable the option **NAT Traversal** (NAT-T). Otherwise, it is usually not possible to establish an IPsec connection.
5. All further required settings for an IPsec VPN connection can be found in the instructions of your used IPsec VPN router.

⚠ The build-in IPsec client of MX530/MX880 is only available in **Expert Mode** and is not part of the mdex scope of services. The mdex Customer Service can't assist you with the commissioning and configuration of this build-in IPsec client.

5 Important information

Safety information

This chapter describes the safety instructions to be followed. These apply in the Federal Republic of Germany. When used in other countries, the relevant national regulations must be observed.

Disruptions of other devices

Using the router may interfere with other devices. The use of the router should be avoided in the following areas:

- Where there is a risk of disrupting the function of other electronic devices, such as in hospitals, airports, airplanes, etc.
- Where there is a risk of explosion, such as gas stations, oil refineries, etc.

It is your responsibility to comply with an applicable statutory regulations and environmental laws. Do not disassemble the router. Any indication of tampering will void the warranty. Follow the instructions for the correct wiring of the router. All devices should be connected to a stable power supply. The wiring should comply with safety and fire protection requirements.

Use and operation

Always handle the Router with care. Avoid direct contact with terminals and pins, as electrostatic discharges can damage the Router.
The system integrator is responsible for the functioning of the product; therefore, please pay attention to the external components of the Router and any installation problems, as there is a risk of interfering with external devices or system security.

- Do not open or disassemble the Router while it is in operation.
- Do not drop the Router and prevent shocks to prevent damage to the internal electronics. The Router must not be installed in areas where it is exposed to strong shocks and vibrations.
- Do not use any hard chemicals, solvents or cleaning agents to clean the Router.
- Do not expose the Router to liquids (rain, drinks, etc.). The Router is not waterproof.
- Ensure that the Router is operated under the specified temperature and humidity conditions.
- The router may not be used on offshore platforms or in water, air or rail vehicles. When used in motor vehicles, the router must be securely stored, easily accessible and removable without tools.
- Persons must maintain a minimum distance of 20 cm to the antennas of the router during operation.
- Do not install or operate the Router in dusty, dirty places. Connectors, plugs and other mechanical parts may be damaged.
- Do not install the Router in the area of electrical interference fields, such as those generated by fluorescent lamps, machines and televisions. Such sources of interference can affect the operation of the Router.
- The Router's power cord also serves as the main disconnect device.
- When using the AC adapter, the power outlet must be in the immediate vicinity of the Router for safety and should be easily accessible during operation.
- In case of smoke, unusual odor or noticeable noise, unplug the power cord from the wall outlet.
- Do not touch the Router or AC adapter with wet hands. Failure to do so may result in interference, short circuits, or electric shock.

- The Router includes detachable small parts that can pose a suffocation hazard. Keep the Router and its accessories away from children!
- No LAN/WAN (Power over Ethernet) powered network cable may be connected to the LAN/WAN sockets! The PoE voltage would destroy the MX530/MX880!

Operating conditions (environment)

Operation of the router is permitted in the following areas:

- Temperature range of the router: MX530: -40° to +70° Celsius | MX880: -30° to +60° Celsius)
- Temperature range of the plug-in power supply: 0° to +40° Celsius)
- The humidity should be in the range of 10% to 90% (non-condensing).
  Use the devices only in dry environments.

Attention: Operating outside the permissible range can significantly shorten the service life of the router.

EU Declaration of Conformity

The mdex MX530/MX880 router complies with the basic requirements of Directive 2014/53/EU. The complete EU Declaration of Conformity can be downloaded from **wiki.mdex.de/Support/DoC** .

Frequency bands and max. transmission powers

	MX530	**MX880**		
		Up to Serial **08**xxxxx	From Serial **10**xxxxxxxx	From Serial **1103**xxxxxx
LTE-FDD:	-	B1/B2/B3/B5/B7/ B8/B20, 23 dBm	B1/B3/B5/B7/B8/B20, 23 dBm	B1/B3/B7/B8/B20/ B28A, 23 dBm
LTE-TDD	-	-	B38/B40/B41, 23 dBm	B38/B40/B41, 23 dBm
UMTS:	900/2100 MHz, 24 dBm	850/900/ 1900/2100 MHz, 24 dBm	850/900/2100 MHz, 24 dBm	900/2100 MHz, 24 dBm
GSM:	850/900/1800/ 1900 MHz, 33/33/30/30 dBm	850/900/1800/ 1900 MHz, 33/33/30/30 dBm	900/1800 MHz, 33/30 dBm	900/1800 MHz, 33/30 dBm
WIFI:	2400 MHz bis 2483.5 MHz, 20 dBm			

Manufacturer's specifications.

The mdex MX530/MX880 router has been produced by Teltonika:
Teltonika UAB, Saltoniskiu st. 9B-1, LT-08105, Vilnius, Lithuania

Export Notes

This product is subject to European/German and/or US export regulations. Any export or re-export subject to authorisation therefore requires the approval of the competent authorities. According to current regulations, the following export classifications must be observed for this product: ECCN/AL: 5A002.a.1 and 5A991.c.10. The current version of the export list can be found on the website of the Federal Office of Economics and Export Control (BAFA).

Note: *The above export list item has been compiled for information purposes to the best of our knowledge and belief and should be used to classify the export together with the export provisions. Exporters are responsible for compliance with all trade regulations, including export regulations, and rely on this information at their own responsibility and risk.*

Customer service

Please contact mdex Support if the information in these safety instructions proves to be insufficient or the router does not work properly:

Address: Wireless Logic mdex GmbH, Bäckerbarg 6, 22889 Tangstedt, Germany
Internet: www.mdex.de
e-mail: support@mdex.de
Tel.: +49 (0)4109-555 444

Disposal

The router as well as all electronic parts included in the scope of delivery must not be disposed of in the household waste. This can be recognised by the marking with the crossed-out wheelie bin symbol . Please dispose of the router and the electronic parts supplied with it after expiry of their service life for reuse or recycling in accordance with the disposal regulations applicable at the installation site at the time. This will avoid harmful effects on the environment and human health.
You can also return the router and the electronic parts included in the scope of delivery to mdex at your expense for proper disposal:
Wireless Logic mdex GmbH, Bäckerbarg 6, D-22889 Tangstedt, Deutschland

Wireless Logic mdex GmbH
Bäckerbarg 6
22889 Tangstedt
Germany

Internet: http://www.mdex.de
e-mail: support@mdex.de

Open Source license notes

The MX Router product line also includes so-called Open Source Software, manufactured by third parties and released for free use by all. The Open Source Software is under special Open Source Software licenses and the copyright of third parties. The rights of the customer to use the Open Source Software are governed in detail by the respective open Source Software licenses.

The Open Source Software under GNU General Public License (GPL) or GNU Lesser General Public License (LGPL) is made available and used without any warranty or liability of the programmers who created the software. For details, please refer to the respective license terms.

You can find the Open Source Software when downloading the software in the Zip archive and when purchasing the product on the supplied data medium (USB stick or CD/DVD). The licenses mentioned above are directly available to you in the directory "Licenses". In the "Source code" directory, you will find the corresponding source code for the Open Source Software, with the licenses applicable to the various software components.

You may edit and reverse engineer any part of the Software for your own use, provided that such software components are linked to program libraries under the LGPL. Disclosure of the information obtained from the reengineering and the processed software, however, is not permitted.

If the software is subject to the GPL, LGPL or the Clarified Artistic License or if the license provisions otherwise stipulate that the source code must be made available, we will send it to you at any time upon request and make a binding offer to that extent. If in this case the delivery is required on a data medium, then the shipment takes place against payment of a flat rate amount of EUR 10.00. If our costs for the production and the dispatch of the data medium should be lower, we calculate only this smaller amount.

Our offer to ship the source code upon request is valid for a period of three years after the product has been distributed by us, or at least as long as we provide support and replacement parts for the product. In this respect, inquiries should be sent (if possible stating the serial number of the purchased product) to the following address:

Wireless Logic mdex GmbH
Bäckerbarg 6
22889 Tangstedt
Germany

Fax: +49 4109 555 55
e-mail: opensource-support@mdex.de