



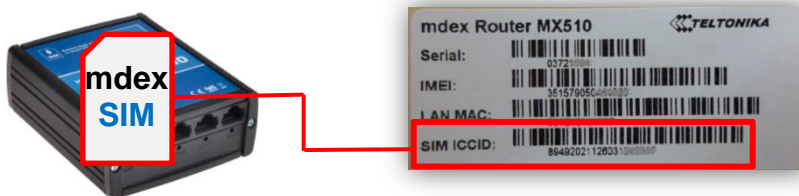
Quick Guide

MX510 & mdex fixed.IP+ via OpenVPN
MX510 & mdex public.IP via OpenVPN

This guide describes the quick configuration of the mdex Router MX510 to have a remote access to one or more terminals with your own SIM-card by using the service **mdex fixed.IP+** (via OpenVPN) or **mdex public.IP** (via OpenVPN).

MX510 Preferences:

- **mdexSIM**-Vodafone is pre-installed.



➔ This pre-installed mdexSIM-Vodafone must be replaced with your own SIM-card.

- The MX510 configuration is preset to access one connected terminal:
 - The MX510 DHCP server assigns the IP address 192.168.0.100 to the terminal.
 - All incoming data packets are forwarded from the MX510 to 192.168.0.100.
- ➔ The “source zone” at MX510 forwarding must be changed to „VPN“! → **Step 10a**
- Other MX510 preferences:
 - LAN IP address and HTTP port: **192.168.0.1:8080**
 - Username / Password: **admin / admin01**
 - Remote HTTP Access: **enabled**
 - NTP (time server): **time.mdex.de**
 - Ping reboot: **ping.mdex.de** (ping every 5 min., 3x failed ping= MX510 reboot)
 - Daily reboot: at **23:30 CET**

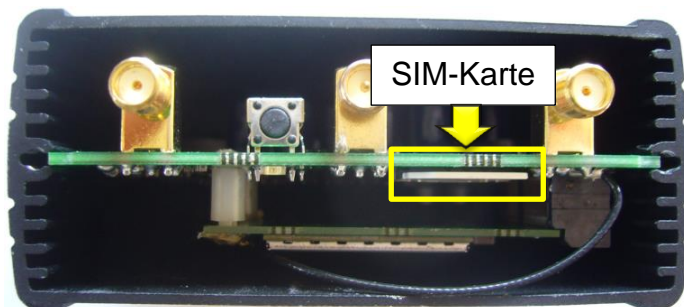
Step 1 Insert your SIM card

An inactive mdexSIM-Vodafone is pre-installed in the MX510. Replace this pre-installed SIM card with your own SIM card.

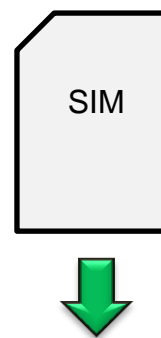
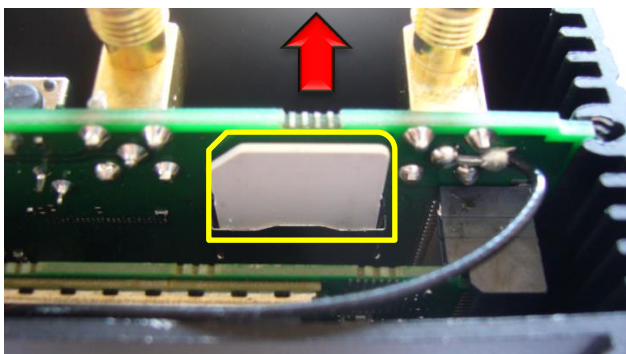
1. Loosen the two screws on the back of the MX510 router (antenna side).



2. Remove the Rear Cover.



3. Pull out the preinstalled mdex SIM card and insert your SIM card into the SIM card slot according to the picture.



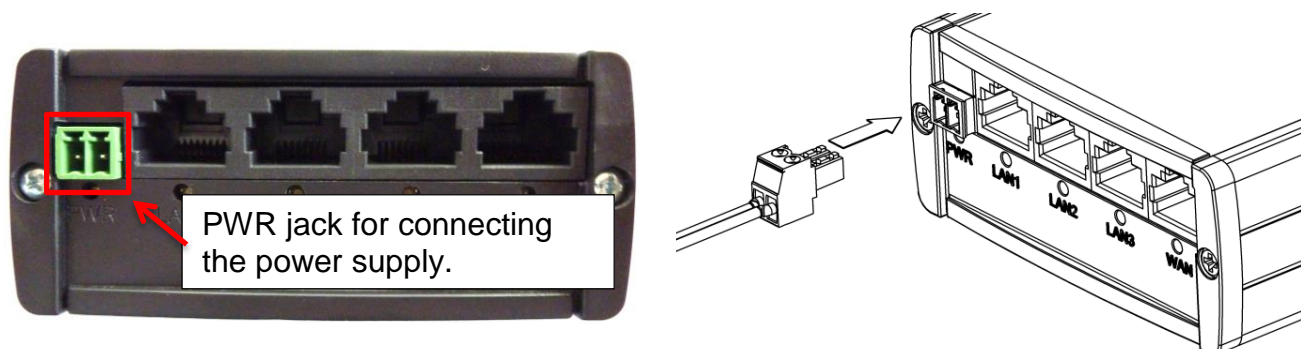
4. Fasten the rear cover with the two screws.

Step 2 Connect the GSM antenna to **GSM MAIN**

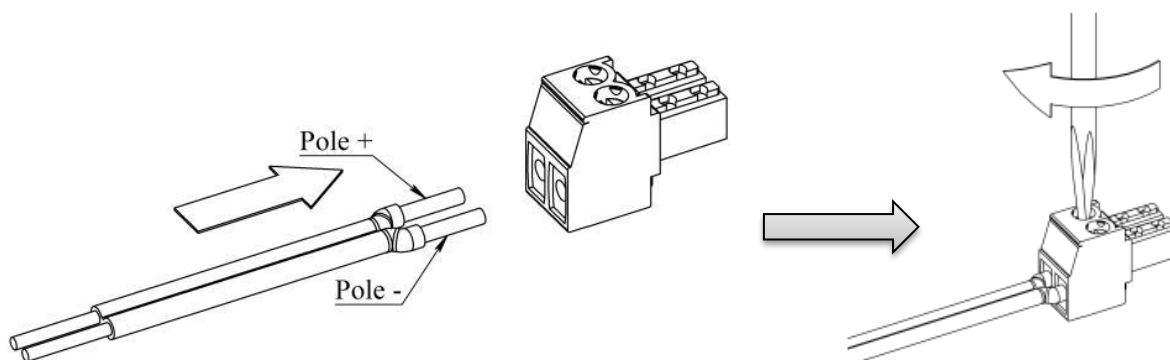


Step 3 Connect the power supply

Plug in the connector from the power supply into the MX510 PWR jack.



The MX510 can be alternatively supplied with another power supply (7V - 30V DC). In this case please remove the power adapter cables from the green connector (loosen the screws) and connect the cables from your own power supply.



Step 4 Change the default MX510 password

1. Make a connection with your web browser to the MX510: <http://192.168.0.1:8080> (Username: admin / Password: admin01)
2. After the first login to MX510 the wizard instructs you to change the router password. It's strongly recommended to change the default password to another save password.

You can change the password later at **System** → **Admin Account**.

Step 5 Connection settings of your SIM card

The MX510 default SIM card settings must be replaced with the settings from your SIM card. Please ask the mobile operator of your SIM card about the current access details (APN, Username and Password) for an internet connection.

1. **Network** → **Connection settings (WAN)**: Common configuration

Common configuration

General Setup

APN: xxxxxxxx

PIN number:

Authentication method: PAP

Username: xxxxxxxx

Password:

Connection type: automatic

Network selection: auto

APN of your SIM card

PIN of your SIM card

Username of your SIM card

Password of your SIM card

2. Click on **Save**.
3. The SIM card connection status can be checked at **Status** → **Network Information**.

GPRS/UMTS

State	connected
IMEI	
Sim card state	OK
Signal strength	-77 dBm
Operator	Vodafone
Connection type	3G (HSDPA)
Bytes recieved	11412
Bytes sent	9269

Step 6 Setup MX510 OpenVPN Client

The "mdex_OpenVPN" client of the MX510 is preset.

You have to enter only the mdex OpenVPN Username and Password of your mdex fixed.IP+/mdex public.IP according to the confirmation e-mail or the Management Portal (<https://manager.mdex.de>) and enable the OpenVPN client.

1. Please click on **VPN** → **OpenVPN**, then on the button **Edit**.

The screenshot shows the 'OpenVPN' management page. At the top, there's a red 'Edit' button. Below it, a table lists configured OpenVPN instances. The table has columns: Tunnel Name, Tun/Tap, Protocol, Port, Status, and actions (Edit, Delete). The instance 'mdex_OpenVPN' is listed with Tun/Tap 'TUN0', Protocol 'UDP', Port '9300', and Status 'Disabled'. The 'Edit' button for this instance is highlighted with a red box. Below the table, there's a 'Role' dropdown set to 'mdex', a 'New configuration name' field, and an 'Add New' button.

Tunnel Name	Tun/Tap	Protocol	Port	Status	
mdex_OpenVPN	TUN0	UDP	9300	Disabled	Edit Delete

2. Make the following OpenVPN settings:

The screenshot shows the 'Main settings' form for the OpenVPN client. Several settings are highlighted with red boxes and arrows pointing to explanatory text boxes:

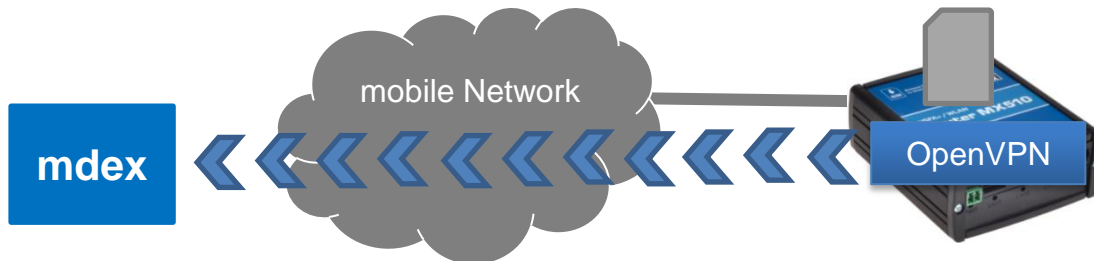
- The 'Enable' checkbox is checked and highlighted. A red arrow points to a box that says 'Enable'.
- The 'Override gateway' checkbox is highlighted with a red dashed box. A red arrow points to a box that says: 'Only in case of using mdex public.IP it's important to enable this option!'. Below this, it says 'Override gateway' with a checkbox icon. Another red arrow points to a box that says: '(If you are using mdex fixed.IP+ please let this option disabled!)'.
- The 'Username' and 'Password' fields are highlighted with a red box. A red arrow points to a box that says: 'Enter the Username and Password from your mdex OpenVPN device.'.

Other visible settings include: Protocol (UDP), Port (9300), Enable LZO compression (checked), Remote host/IP address (fixedip.mdex.de), Cipher (BF-CBC), Maximum fragment size (1300), Limit TCP packet size (checked), Enable VPN NAT (checked), Allow remote peer's IP change (checked), Do not bind to local address (checked), Key renegotiation interval (86400), Exit message count (2), and Extra options (empty).

3. Click on **Save**.
4. You should now reboot the MX510 at **System** → **Reboot**. (or turn-off -> turn-on power)

Step 7 MX510 establishes a connection to mdex

The MX510 establishes a connection to the mobile network using the inserted SIM card. When the MX510 has internet access the OpenVPN Client establishes a connection to mdex.



The MX510 OpenVPN connection status can be checked at **Status** → **Network Information**

OpenVPN information <i>mdex_OpenVPN</i>	
Enabled	enabled
State	connected
IPv4 address	172.21.100.104

Step 8 Enter mdex DNS Servers

This step can be skipped in case of using mdex fixed.IP+ (via OpenVPN).

In case of using **mdex public.IP** (via OpenVPN) it's important to enter the following custom DNS servers to the MX510. Otherwise the MX510 (and terminals) can't resolve DNS names.

1. Click to **Network** → **LAN**.
2. Enter the following DNS Server at **Use custom DNS servers**.

The screenshot shows the 'Common Configuration' window with the 'General Setup' tab selected. The 'Protocol' is set to 'Static address'. The 'IPv4 address' is '192.168.0.1', 'IPv4 netmask' is '255.255.255.0', and 'IPv4 gateway' is empty. The 'IPv4 broadcast' is also empty. The 'Use custom DNS servers' section is highlighted with a red box and contains two entries: '46.16.220.98' and '46.16.216.25'. A red arrow points from this section to a red box on the right.

Use custom DNS servers:

- 46.16.220.98
- 46.16.216.25

3. Click on **Save**.

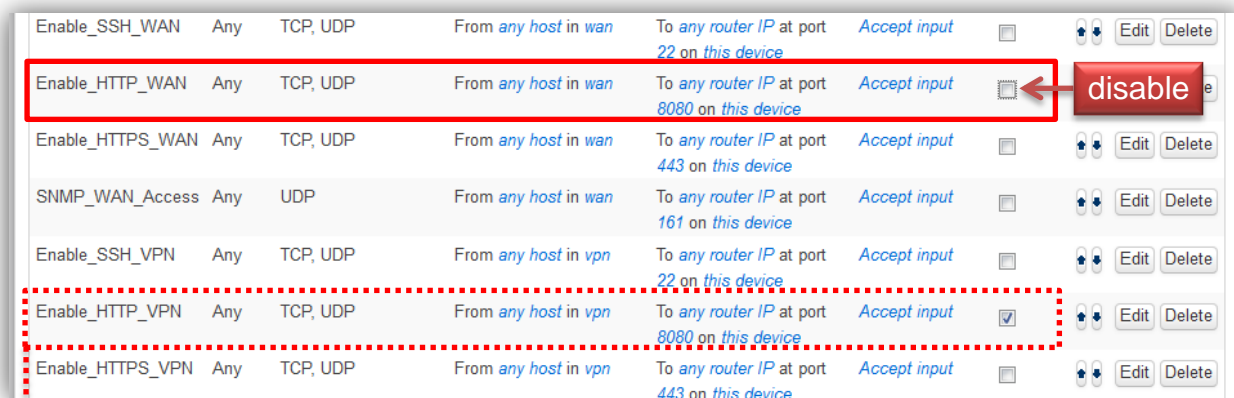
Step 9 Remote access to MX510

To prevent unauthorized access over the WAN IP address it's strongly recommended to disable the rule "Enable_HTTP_WAN" in the MX510 firewall.

1. Click on **Network** → **Firewall**, then on **Traffic Rules**



2. Disable the rule "Enable_HTTP_WAN" and click on **Save**



- **Enable_SSH_WAN:**
Access to MX510 SSH interface over WAN IP address of your SIM-card.
This SSH access over WAN is already disabled as default.
- **Enable_HTTP_WAN:**
Access to MX510 HTTP interface over WAN IP address of your SIM-card.
This HTTP access over WAN should be disabled!
- **Enable_HTTPS_WAN:**
Access to MX510 HTTPS interface over WAN IP address of your SIM-card.
This HTTPS access over WAN is already disabled by default.
- **Enable_SSH_VPN:**
Access to MX510 SSH interface over the OpenVPN tunnel (disabled by default).
- **Enable_HTTP_VPN:**
Access to MX510 HTTP interface over the OpenVPN tunnel.
- ➔ **In case of using mdex public.IP:** The MX510 HTTP web interface is reachable from the whole Internet! IF you don't need access to the MX510 web interface, please disable this rule. Otherwise it's important to change the MX510 router password as described in **Step 4)**
- **Enable_HTTPS_VPN:**
Access to MX510 HTTPS interface over the OpenVPN tunnel (disabled by default).

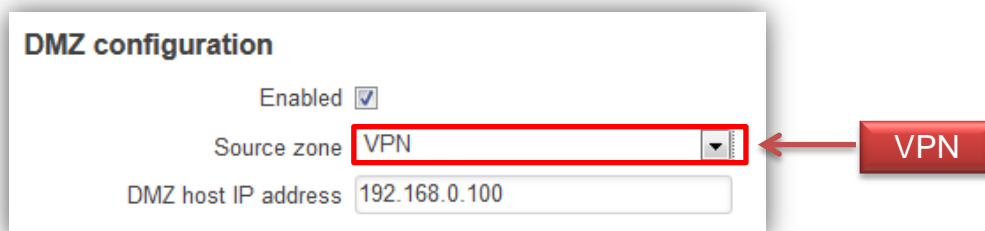
Step 10a Remote access to only one terminal

The following steps are required if only one terminal is connected to the MX510.

1. Setup Forwarding at MX510

A host forwarding (all data packets and protocols) is already preset to the IP address 192.168.0.100. You must change only the **source zone** from "WAN" to "VPN".

1. Click on **Network** → **Port Forwarding**.
2. Change at "DMZ configuration" the "**Source zone**" to **VPN**.



DMZ configuration

Enabled ☒

Source zone **VPN**

DMZ host IP address 192.168.0.100

3. Click on **Save**.

Now all incoming data packets and protocols are forwarded over the MX510 OpenVPN tunnel to the local IP address 192.168.0.100 (terminal).

2. Connect your terminal to a LAN socket

Remove your computer from the MX510 and connect your terminal to the **LAN1**, **LAN2** or **LAN3** socket of the MX510.



- Your terminal should be set to DHCP client (automatically obtain an IP address). The MX510 is preconfigured for dynamic assignment of IP addresses (DHCP) and automatically assigns the IP address **192.168.0.100** to your connected terminal. Alternatively, the IP address 192.168.0.100 can be set manually in your terminal.
- All incoming data packets over the MX510 OpenVPN tunnel are forwarded to the IP address 192.168.0.100 (terminal).

Note

The MX510 is preconfigured for the allocation of only one IP address (192.168.0.100). This IP address is reserved for another 5 minutes after this terminal was removed. So remove any terminal (eg your computer) from the MX510 router and wait at least 5 minutes (or do a reboot of the MX510) before connecting the desired terminal to the MX510.


Step 10b Remote access to more than one terminal

This step can be skipped, if you are connecting only one terminal to the MX510 as in **step 10a**. The following steps are required if more than one terminal should be accessible by remote.

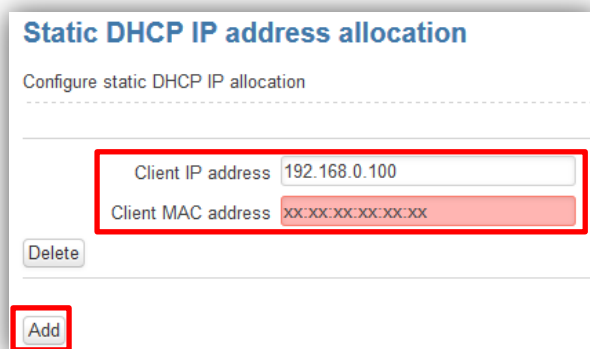
1. LAN IP addresses for terminals

The integrated MX510 DHCP Server can assign the local IP addresses to the terminals.

1. Click to **Network** → **LAN**
2. Increase the IP address range that should be assigned to the connected terminals.



3. Click on **Save** to save the entered IP address range.
4. To allocate the IP addresses to the terminals click on **Configure**, then on **Add**.
5. Enter the IP address and MAC address from the terminal, then click on **Add**.



➔ Now the terminal with this assigned MAC address get always the same IP address from the MX510 DHCP Server. To enter more terminals click again on the button **Add**.

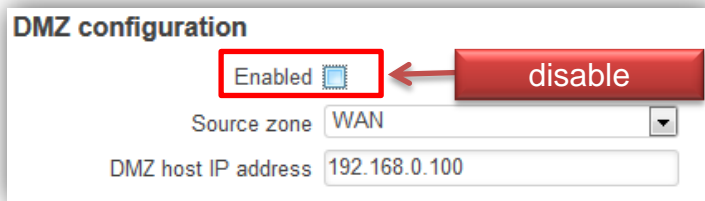
6. After all allocations where done, click on **Save**.

Instead of using the DHCP server from MX510 you can enter also static IP addresses to the terminals:

- IP address: 192.168.0.2 to 192.168.0.255
- Default-Gateway & DNS Server: 192.168.0.1

2. Add Port Forwarding in MX510

1. Click to **Network** → **Port Forwarding** and disable **DMZ configuration**



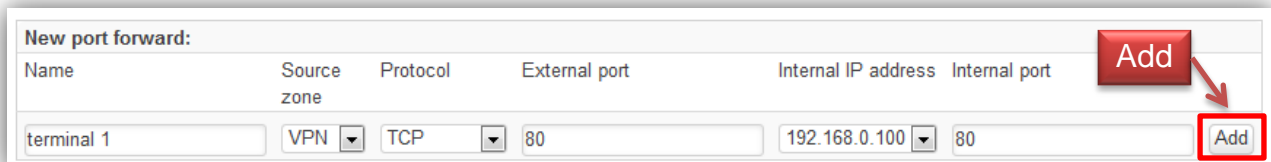
DMZ configuration

Enabled ☐ ← disabled ☐

Source zone: WAN

DMZ host IP address: 192.168.0.100

2. Click on **Save**.
3. Enter the needed port forwarding at “New port forward” and click on **Add**.
 - **Name:** You can enter a name of this forwarding.
 - **Source zone:** Select **VPN (important!)**
 - **Protocol:** Select the protocol (TCP and/or UDP).
 - **External port:** Enter the incoming port to access the destination terminal
 - **Internal IP address:** Enter the local address from the destination terminal.
 - **Internal port:** Enter the local port from the destination terminal.



Name	Source zone	Protocol	External port	Internal IP address	Internal port	Add
terminal 1	VPN	TCP	80	192.168.0.100	80	Add

4. When you added all needed forwardings, click on **Save**.

3. Connect your terminals to the MX510 LAN sockets

Connect your terminals to the **LAN1**, **LAN2** or **LAN3** socket of the MX510. More terminals can be connected by using an external switch that is connected to a LAN socket.



- If your terminals are set to DHCP client (automatically obtain an IP address), point 1 “**LAN IP addresses for terminals**” (page 9) must be done first.
- Without using DHCP you must enter static IP addresses in your terminals.
 - IP address: 192.168.0.2 to 192.168.0.255
 - Default-Gateway & DNS Server: 192.168.0.1

MX510 Quick Setup is finished

The MX510 router and the connected terminals are now accessible remotely.

mdex **fixed.IP+**

In case of using the service mdex fixed.IP+ the remote access to the MX510 web interface and the connected terminals is possible by using one of the following mdex services:

- **mdex [web.direct](#):**
You can access the web interface of the MX510 and the connected terminal by mdex web.direct link. You can configure the mdex web.direct link for your mdex device at the mdex Management Portal: <https://manager.mdex.de>
- **mdex [Leitstellentunnel](#)** (optional):
This service can be optionally booked for your fixed.IP+.
The mdex Leitstellentunnel is an OpenVPN tunnel from your computer to mdex to use it as control station. Over this OpenVPN tunnel all IP-based protocols (SSH, Telnet, FTP, SMTP, HTTP, etc.) can be transferred between the computer and the terminal.

You will find the setup files at for Windows, MAC OS X, Linux, Android and iOS (iPhone / iPad) at <https://wiki.mdex.de/Support/ANLmdexLeitstellentunnel>

mdex **public.IP**

In case of using the service mdex public.IP the remote access to the MX510 web interface and the connected terminals is possible by using the public.IP address. The assigned public.IP address for your mdex OpenVPN device can be found in the mdex order confirmation e-mail, or in the mdex Management Portal: <https://manager.mdex.de>.

Notes

- Because the MX510 web interface is accessible from the whole Internet, it's strongly recommended to change the default MX510 router password as described in [Step 4](#)).
- If you don't need a remote access to the MX510 web interface, please disable the MX510 firewall traffic rule "Enable_HTTP_VPN" as described in [Step 9](#)).

mdex GmbH
Bäckerbarg 6
22889 Tangstedt
Germany

Internet: <http://www.mdex.de>
E-Mail: support@mdex.de
Phone: +49 (0)4109-555 444