# TK500 ROUTER SERIES
# MANUAL

Version 2.1.1


**Welotec GmbH**
Zum Hagenbach 7, D-48366 Laer
T: +49 (0)2554/9130-00
F: +49 (0)2554/9130-10
info@welotec.com

**www.welotec.com**

# TABLE OF CONTENTS

# 1. TK500-SERIES - INTRODUCTION



**Brands**
Welotec is a registered trademark of Welotec GmbH. Other trademarks mentioned in this manual are the property of their respective companies.

**Legal notice**
The information in this document is subject to change without notice and is not binding for Welotec GmbH. This manual may contain technical or typographical errors. Corrections are made regularly without being mentioned in new versions.

**Contact information for technical support**
Welotec GmbH
Zum Hagenbach 7
D-48366 Laer
Phone: +49 2554 9130 00
Fax: +49 2554 9130 10
Email: support@welotec.com

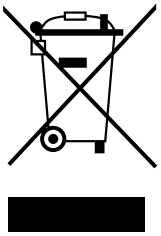
**Description**
The TK500 industrial routers provide a stable, high-speed connection between remote devices and customer locations over LAN and (depending on the model) over Wi-Fi or 2G / 3G / 4G networks. They can be used in a voltage range of 12 to 24 V DC and have a temperature range of -15 °C to +70 °C with a relative humidity of 95%, which ensures high stability and reliability under severe conditions. The TK500 can be used on the workplace or mounted on DIN rails.
TK500 series products support VPN (IPSec / PPTP / L2TP / GRE / SSL VPN), ensuring secure connections between remote devices and customer sites.

**Important safety instructions**
**This product is not suitable for the following applications**
- areas where no wireless applications (such as mobile phones) are allowed
- hospitals and other places where the use of mobile phones is not permitted
- petrol stations, fuel depots and places where chemicals are stored
- chemical plants or other places with a explosion hazard
- metal surfaces which can weaken the radio signal level

**Warning**
This is a class A product. In living areas, the use of this equipment can lead to radio interference, which the user must remedy with appropriate measures.

## WEEE notice

The European Directive on the Disposal of Waste Electrical and Electronic Equipment (WEEE), which entered into force on 13 February 2003, has led to major changes in the reuse and recycling of electrical equipment. The main objective of this Directive is the prevention of waste electrical and electronic equipment and the promotion of re-use, recycling and other forms of recycling. The WEEE logo on the product or packaging indicates that the product must not be disposed of in normal household waste. It is your responsibility to dispose of all used electrical and electronic equipment at appropriate collection points. Separate collection and sensible recycling of your electronic waste helps to conserve natural resources. In addition, proper recycling of waste electrical and electronic equipment ensures human health and environmental protection.



For further information on disposal, recycling and collection points for electrical and electronic equipment, please contact your local city office, waste disposal service, or the device's distributor or manufacturer.

# 1.1. Package checklist

Each TK500 wireless router comes bundled with standard accessories. Additional accessories can be ordered. Carefully check the contents of your package, and if something is missing or damaged, contact your distributor from Welotec GmbH.

**Delivery:**

**Standard equipment:**

| Equipment | Amount | Description |
|---|---|---|
| TK500 router | 1 | TK500 series industrial router |
| Network cable | 1 | Network cable CAT5, 1.5 meter |
| Manual | 1 | Disk with manual |
| License conditions | 1 | "Third Party Software Notifications and Licenses" |
| Power supply | | |
| Terminal block | 1 | 7-pin terminal for power supply |

**Components Set (depending on model)**

| Product | Amount | Description |
|---|---|---|
| TK500 router | 1 | TK500 series industrial router |
| Network cable | 1 | Network cable CAT5, 1.5 meter |
| Cellular antenna | 1 | 5 m magnetic base antenna (TK515L, TK515L-W, TK505U) 2G/3G |
| Wi-Fi antenna | 2 | Plug-on antenna (Wi-Fi) (TK515L-W) |
| Manual | 1 | Disk with manual |
| License conditions | 1 | "Third Party Software Notification and Licenses" |
| Power supply | | |
| | | Desktop power supply, input 100-240 V AC, output 12 V DC (for TK5xx), incl. 7-pin terminal block |
| | 1 | Plug, european standard |

# 1.2. Product information

## 1.2.1. Environmental conditions

Operating temperature: -15°C to +70°C
Relative humidity during operation: 5 to 95% non-condensing
Storage temperature: -40°C to +85°C

## 1.2.2. Power supply

Power supply: 1 Terminal block (7-pin) incl. voltage socket and serial connection
Input volatge: 12 - 24 V DC

## 1.2.3. Physical characteristics

Housing: steel, protection class IP30
Weight: 450 g
Dimensions (mm): 35 x 127 x 108.2 mm

# 2. INSTALLATION MANUAL

## 2.1. Typical application

With TK500 series routers you can connect devices with Ethernet, Wi-Fi or RS-232/485 to the Internet via GPRS / HSUPA / UMTS / LTE. To ensure security and uninterrupted access, the TK500 Series supports VPN connections, enabling remote access and secure data transmission over the Internet.

## 2.2. Connection plan

| Interface | Description |
|---|---|
| Power supply | 12-24 V DC |
| Serial | Serial Interface |
| Ethernet ports | Five 10/100Base-TX RJ45 ports |
| Antenna connection (cellular) | SMA (f) |
| Antenna connection (Wi-Fi) | SMA-R (f) |
| SIM card slot | Slot for inserting the SIM card (TK525L-W, TK525L, TK525U) |

### 2.2.1. Connection of serial interfaces and I/O's

**Description of LED lights**

 = LED on

 = LED off

 = LED flashing

Legend: glows: on-- glows not: off-- flashes: flashing--

| Signal | On | Off | Flashing |
|---|---|---|---|
| Turn on | PWR, STATUS, WARN | ERR | |
| Execution of firmware | PWR, WARN | ERR | STATUS |
| Dial-up to Internet | PWR | ERR | SATUS, WARN |
| Establish connection | PWR | WARN, ERR | STATUS |
| Firmware update | PWR | | STATUS, WARN. ERR |
| Factory reset | PWR | WARN | STATUS, ERR |

## Description of LED signal

**Signal: 1-9**
(bad signal, the router cannot operate properly. Please check the antenna connection and the local signal strength of the mobile network.)

**Signal: 10-19**
(router is operating normally)

**Signal: 20-31**
(perfect signal level)

# 2.3. Fast internet connection

## 2.3.1. Insert the SIM card

Open the TK-Router SIM / UIM tray at the top of the device and insert the SIM card into the card carrier.

## 2.3.2. Installation of the antenna

After installing the TK500, connect the antenna and screw the antenna tight. Place the antenna where good signal strength is achieved.

**Note**

Position and angle can affect signal strength.

## 2.3.3. Power supply

Connect the supplied power supply to the unit, and make sure that the Power LED is on. Contact Welotec Technical Support if no indicator lights up. You can configure the TK500 when the power indicator is flashing.

## 2.3.4. Connect

Connect the TK500 with your PC:

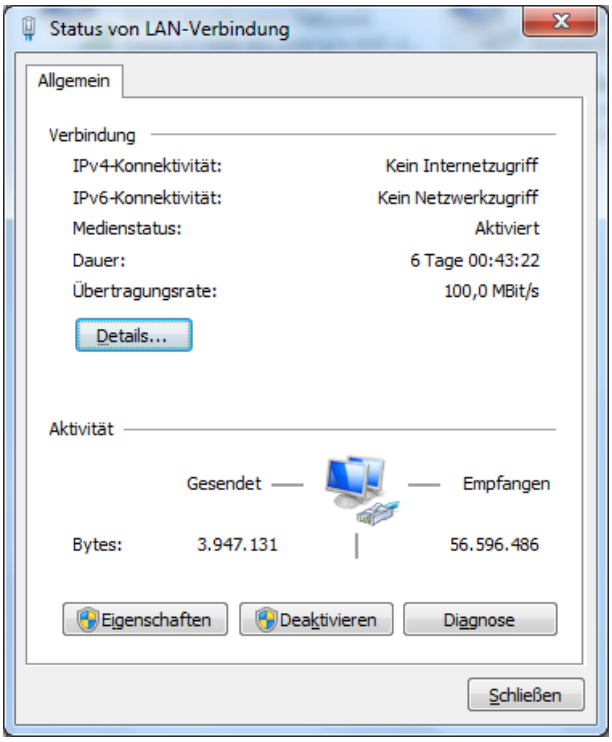
1) Connect the Ethernet cable of the TK500 to the PC.
2) Then an LED indicator of the RJ45 interface lights up in green and the other displays are flashing.

## 2.3.5. First connecting of the TK-Router device to the PC

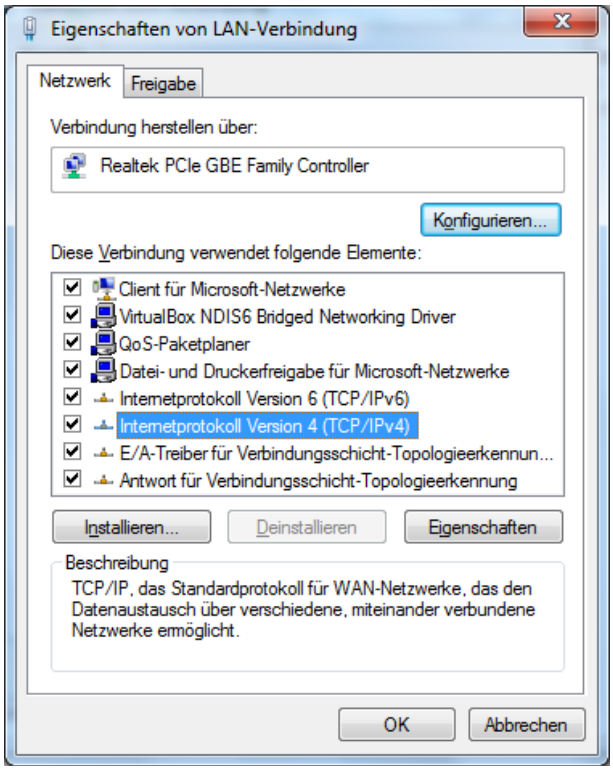
The TK500 router can automatically assign IP addresses for the PC. Set up the PC so that IP addresses are automatically retrieved via DHCP. (Based on the Windows operating system):

1) Open the Control Panel, double-click the „***Network and Sharing Center***" icon to open the „***Network and Sharing Center***" screen.

2) Click on „***LAN connection***" and open the screen with the "***Status of LAN connection***":

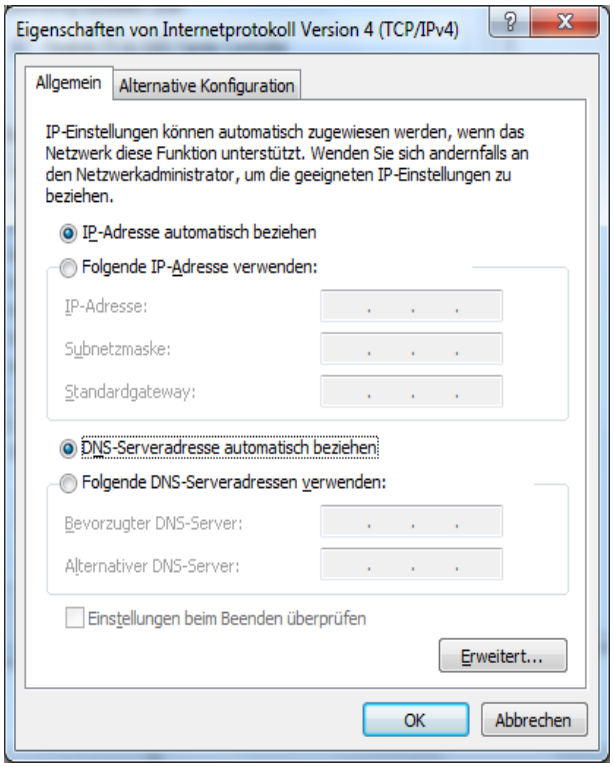



3) Click on „***Properties***" and open the LAN connection properties screen:



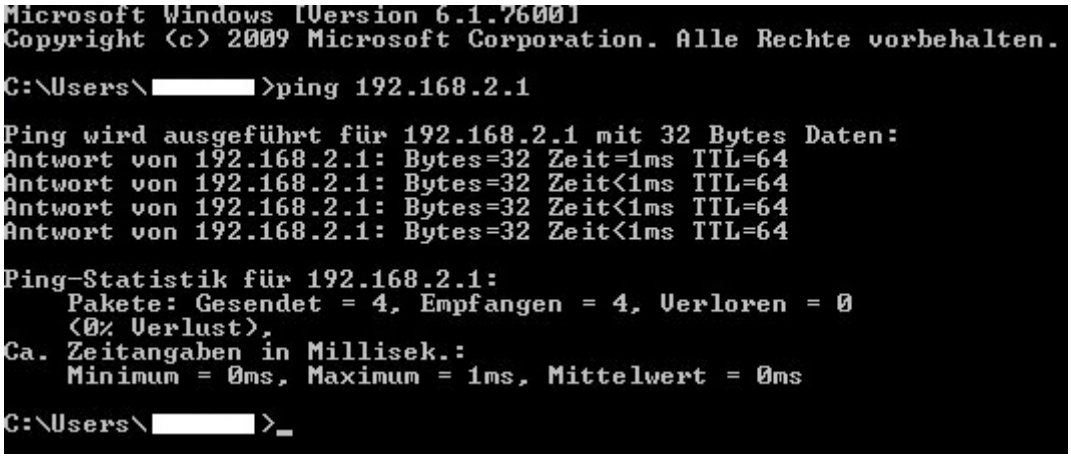
4) Select „***Internet Protocol Version 4 (TCP / IPv4)***", click the „***Properties***" button, and check if your PC can obtain IP and DNS address automatically. (You can also set up the PC in the subnet: 192.168.2.0/24, eg IP: 192.168.2.10, Netmask: 255.255.255.0, Default Gateway: 192.168.2.1)

Clicking on „***OK***" the TK router assigns the PC an IP address: 192.168.2.X, as well as the gateway: 192.168.2.1 (the default address of the TK500).



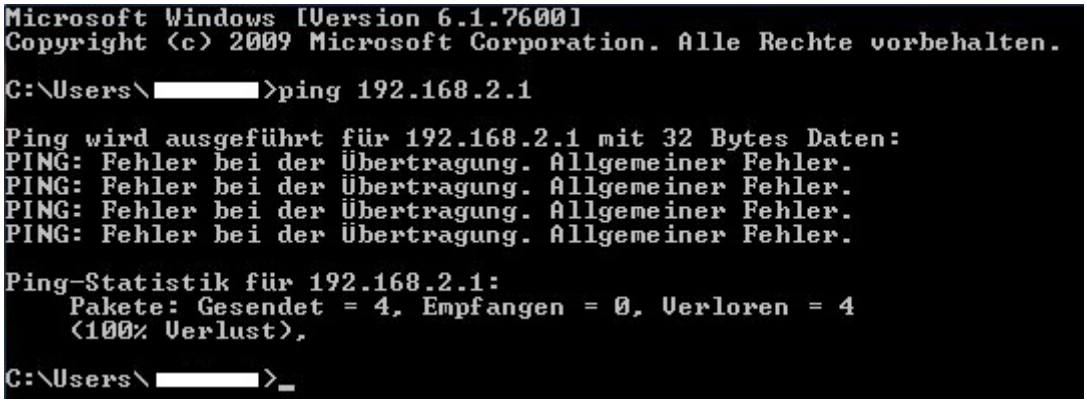

After configuring the TCP/IP protocols, you can use the ping command to check whether the connection between the PC and the router is established correctly. Here is an example of running the ping command on Windows 7:

Windows-Key+R -> Input "***cmd***" -> Enter key -> Input "***Ping 192.168.2.1***" -> Enter with this display:




The connection between PC and router has been set up correctly.

The following example has errors:

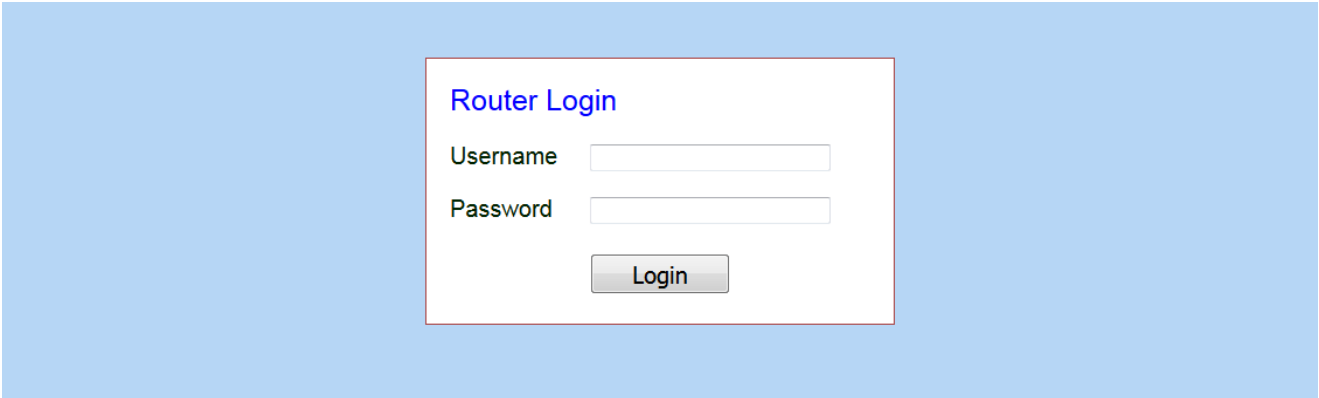



The connection is not working properly and you should review the instructions and improve your settings.

## 2.3.6. Configuring the TK500 (optional)

After completing the steps in the previous chapter, you can configure the router:

1) Open any internet browser (such as Google Chrome) and enter the default IP address of the router: ***http://192.168.2.1***. The following login page opens:

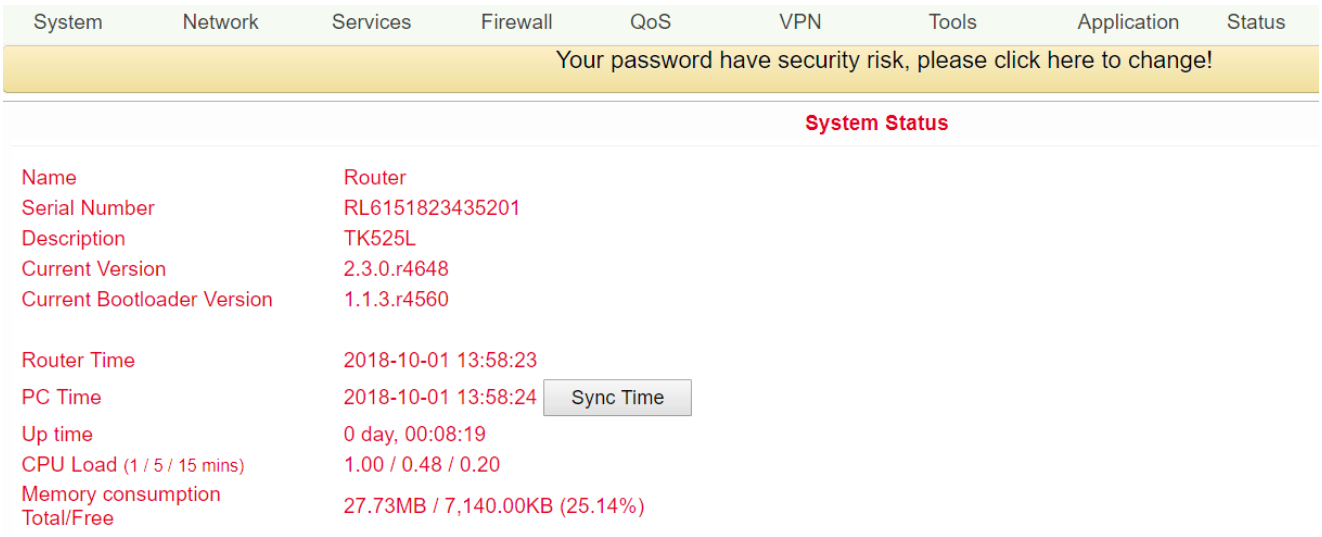



Enter the user name (default: adm) and the password (default: 123456), and then click „***Login***" to open the configuration screen.

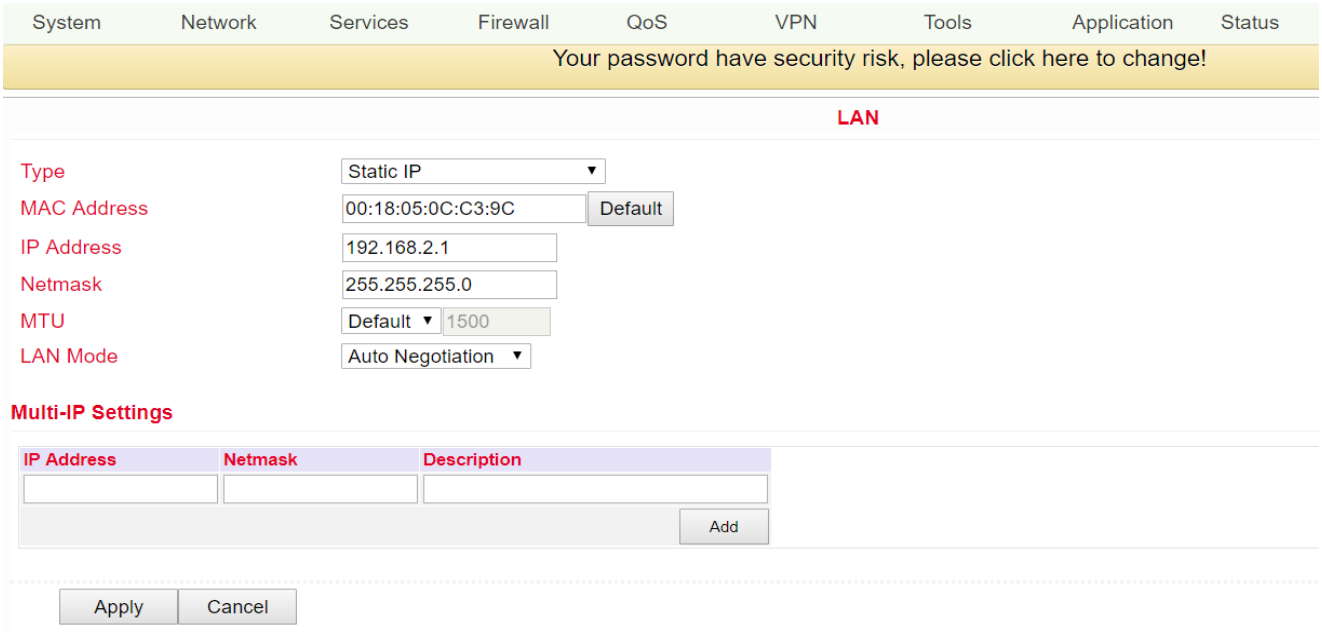
2) Change the IP configuration:

**Note**

After configuring, click „***Apply***" to activate the configuration.
If you want to set your own IP, follow the instructions below:




Click on ***Network >LAN***. Change the IP address in ***192.168.1.254***:



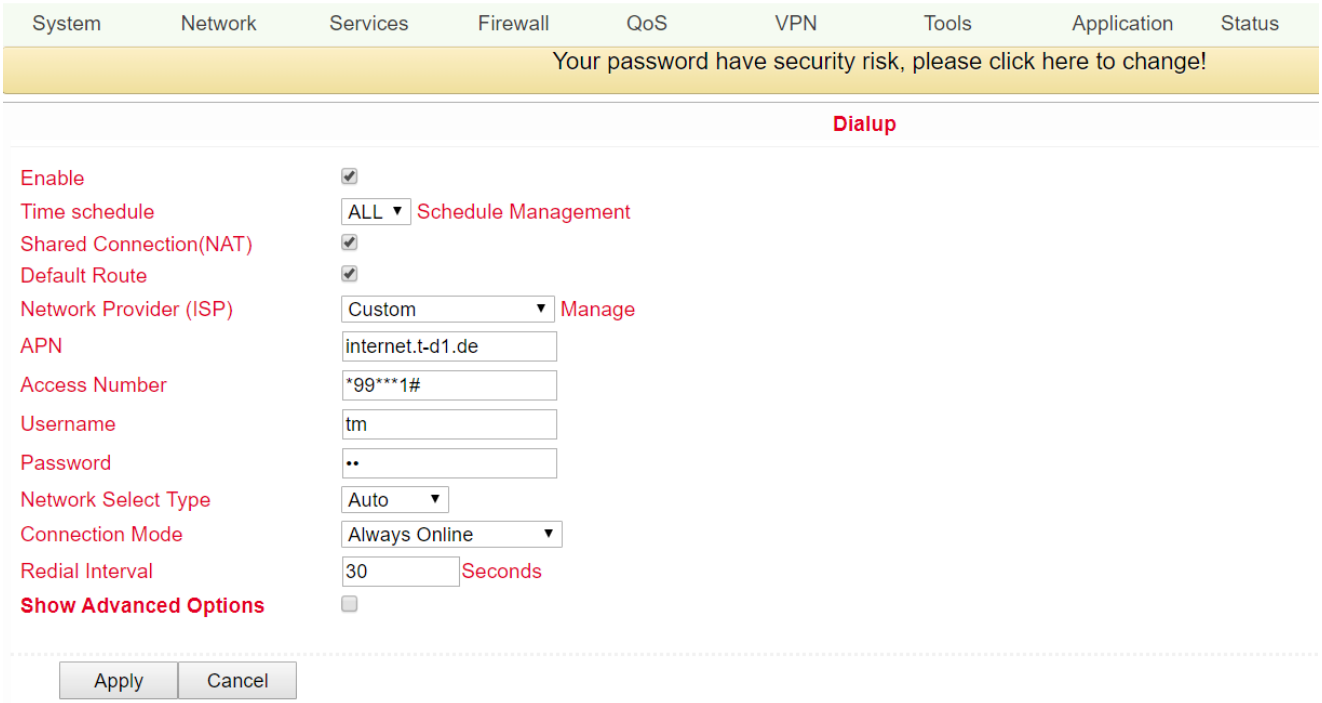
3) Click on „***Apply***“, and you will see the following:


The IP address of the TK500 has been changed. In order to access the configuration page again, the PC must be set up in the same subnet, for example: ***192.168.1.10/24*** – Then enter the changed IP address ***(192.168.1.254)*** in your browser.

## 2.3.7. Connect the TK router with the Internet

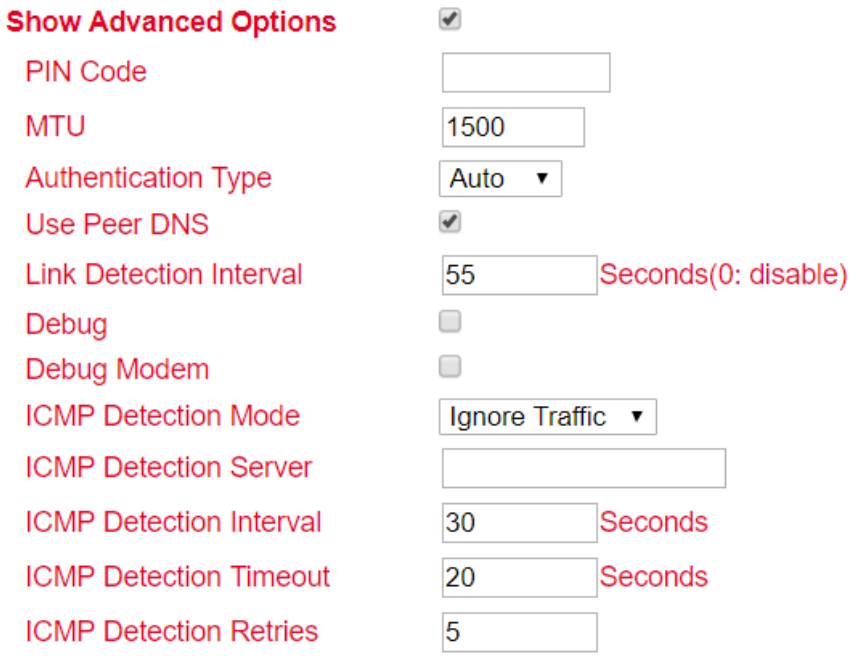
Complete the following configuration steps to establish a connection between the TK500 and the Internet.

Click on ***Network > Dialup*** and activate ***Enable***:




Check the entries for APN, dial-in number, username and password:
You will receive the dial-in number, username and password from your local network provider. Inquire about the details there.

***Show Advanced Options*** allows you to make additional settings, such as the PIN code if this is set on the SIM card.



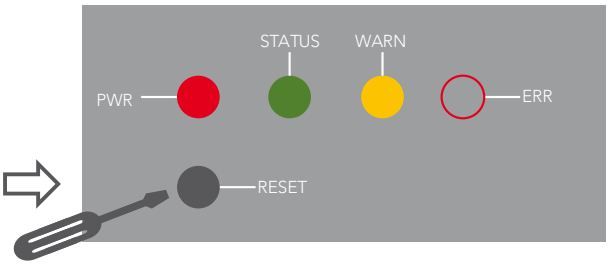

Once you have set the correct configuration, the TK500 can now connect to the Internet. Open an Internet browser, enter „***www.welotec.com***" and the Welotec website will open.

# 2.4. Reset to factory settings

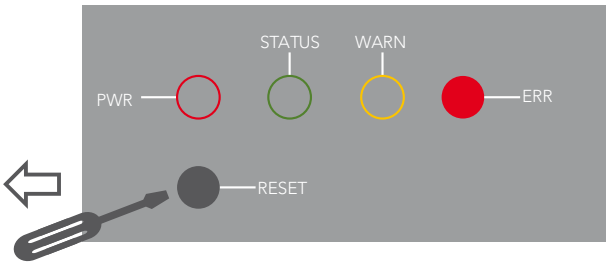
## 2.4.1. Hardware method

= LED on = LED off = LED flashing

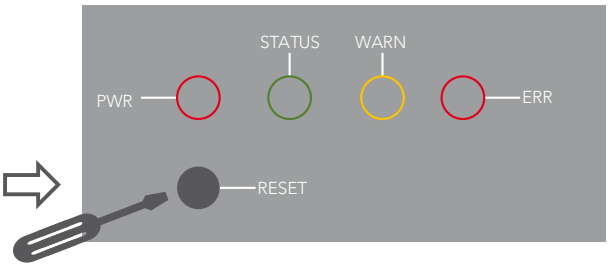
1) Press the ***RESET button*** while turning on the TK500:



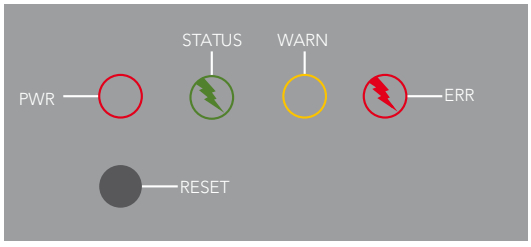

2) As soon as the ERROR LED lights (about 10 seconds after switching on), release the ***RESET button***:




3) After a few seconds, the ERROR LED light stops lighting. Now press the ***RESET button*** again:



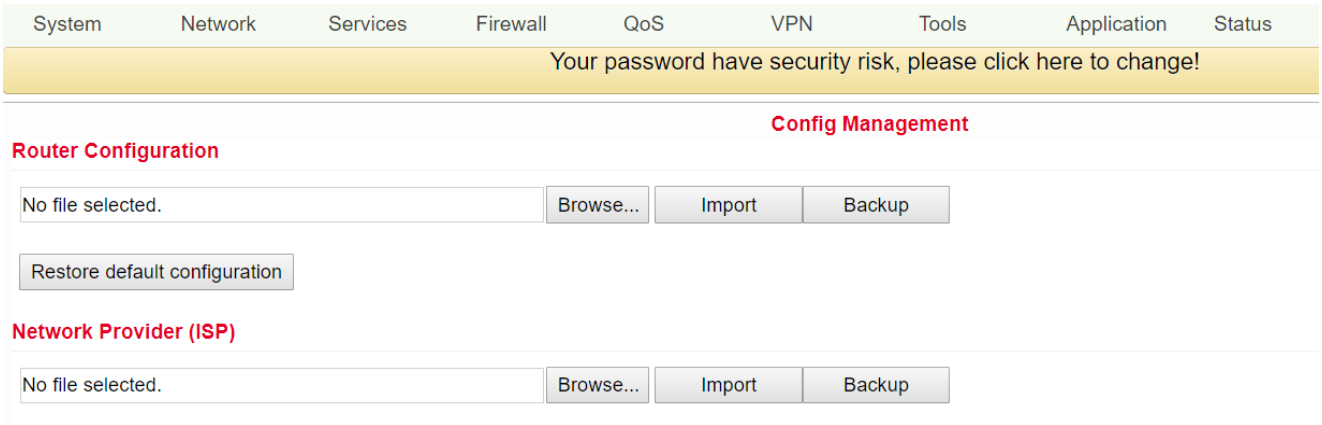

4) The ERROR and STATUS LED will flash, indicating that the default setting was successful.




| Factory default settings | |
|---|---|
| IP: | 192.168.2.1 |
| Net mask: | 255.255.255.0 |
| Username: | adm |
| Password: | 123456 |
| Serial parameter: | 115200-N-8-1 |

## 2.4.2. Web method

1.) Log in to the web-based UI of the TK500 and select ***System > Config Management***:

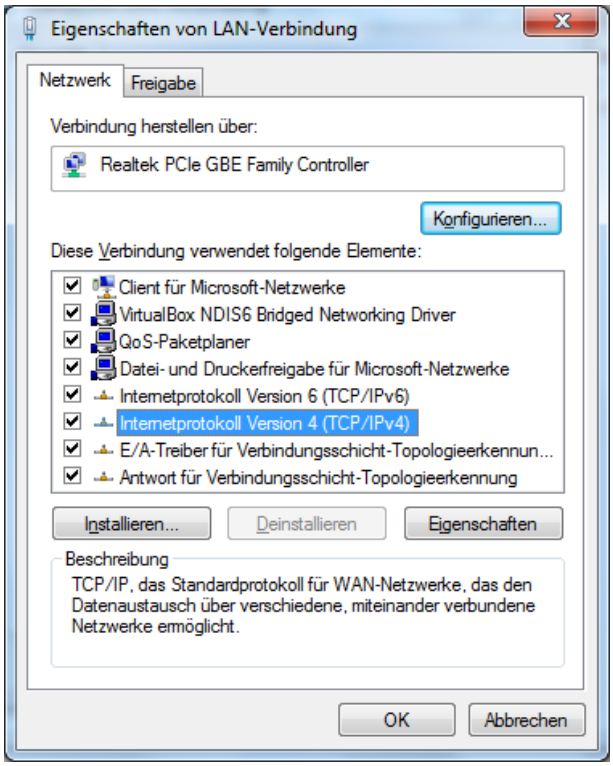


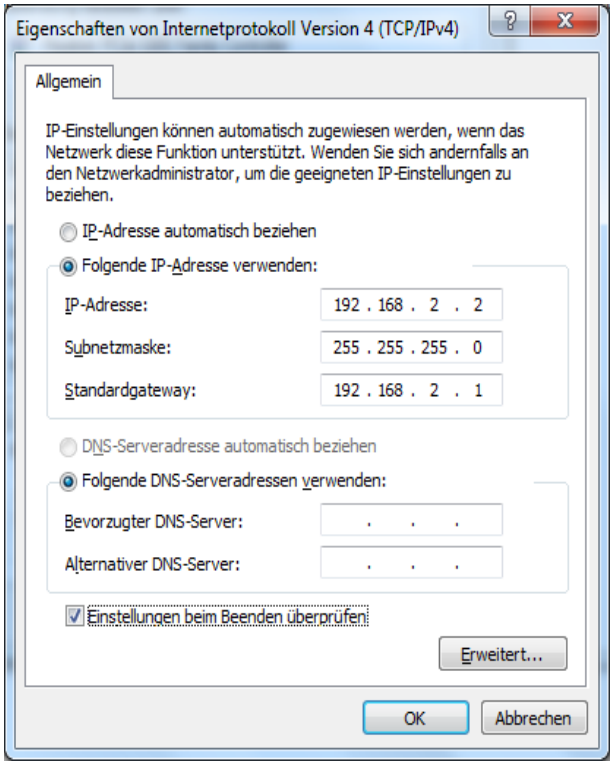

2.) Click ***Restore default configuration*** to reset the TK500 to its factory defaults. Then the router is re-booted.

# 3. SYSTEM

Before using the TK500 router it must be properly configured. This chapter describes the web-based configuration.

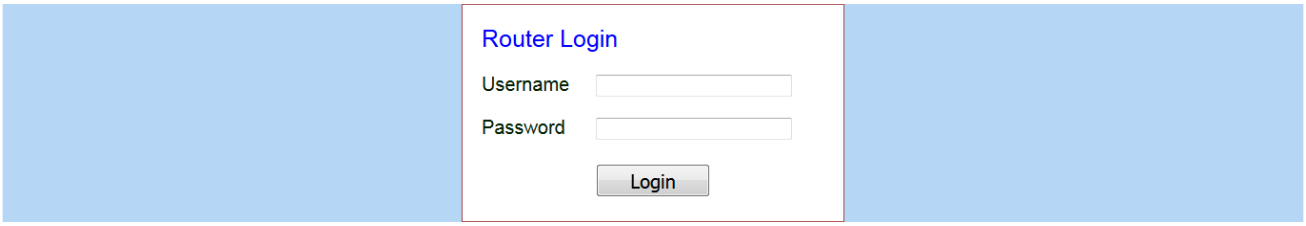
**Preparation**
First connect your devices to the TK500 via cable or hub (switch) and set the IP address for the PC and TK500 on the same subnet, for example: set the PC IP address to 192.168.2.2, Netmask: ***255.255.255.0***, Gateway (default IP of the TK500: ***192.168.2.1***):



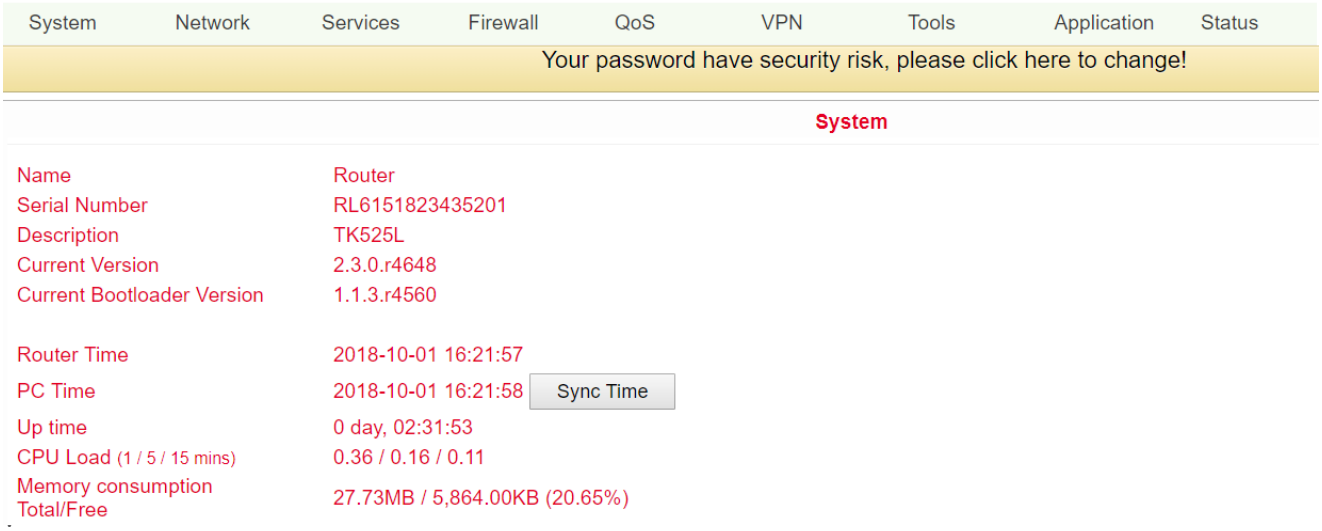



Open an Internet browser and enter the IP address of the TK500: ***http://192.168.2.1*** (default IP of the TK500).

On the following login page, you must log in as an administrator. Enter the username and password (default: ***adm/123456***).

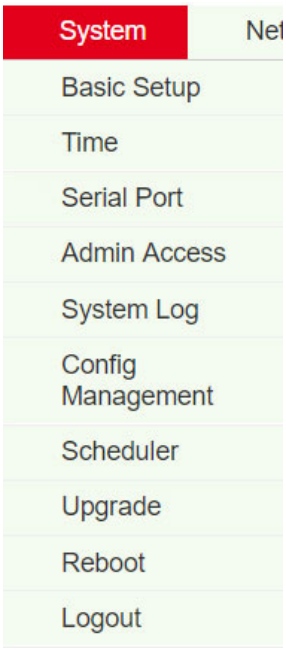



Click on „***Login***" to open the configuration page.



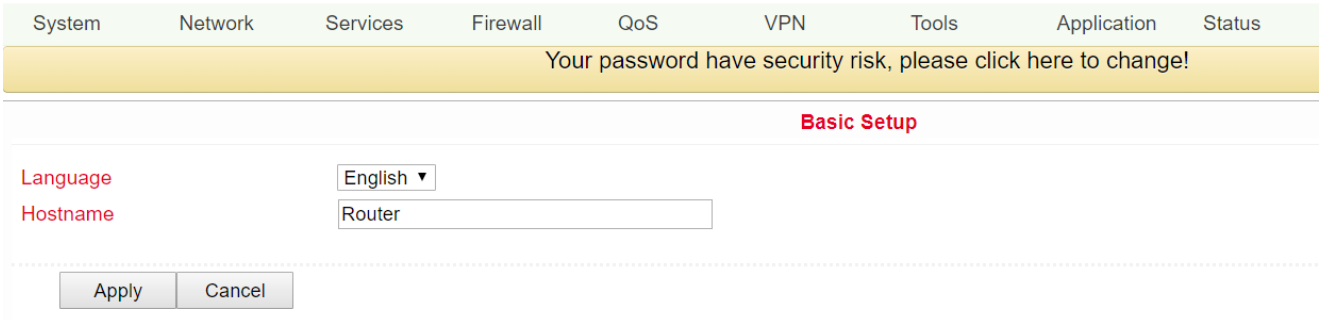
# 3.1. System

The system settings include the following nine sections: Basic Setup, Time, Serial Port, Admin Access, System Log, Config Management, Scheduler, Upgrade, Reboot, and Logout.




## 3.1.1. Basic Setup

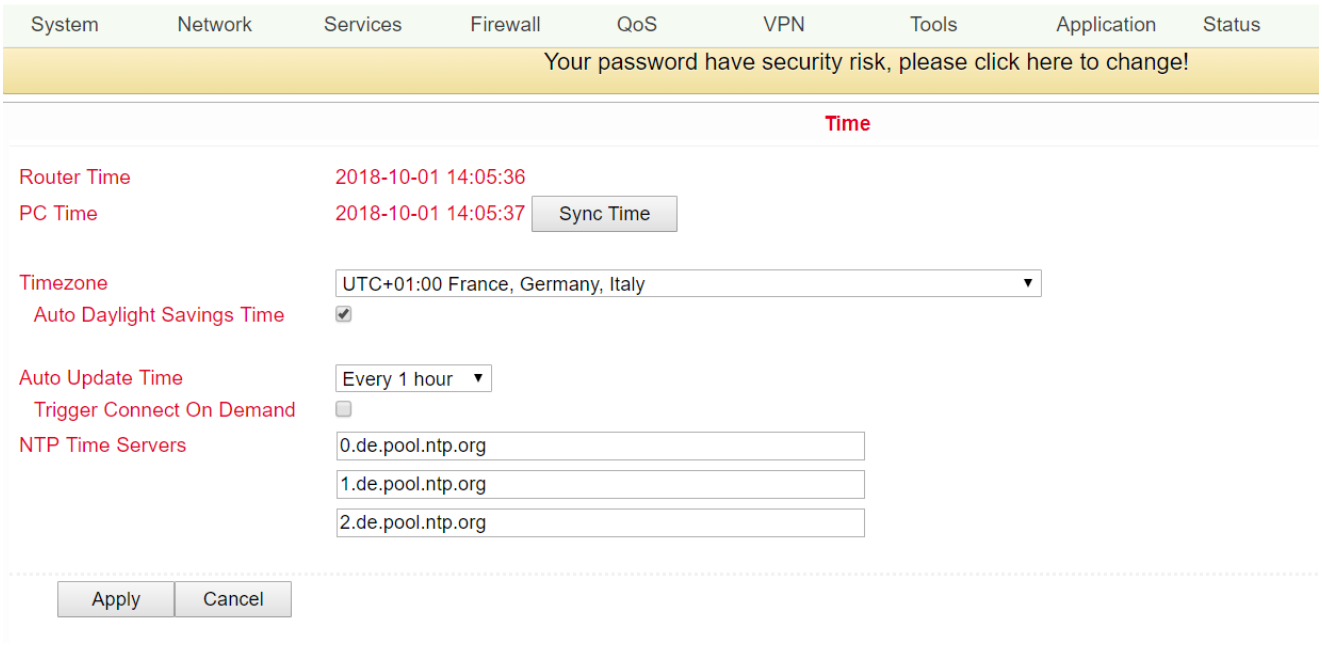
In the Basic Setup you can adjust the voice guidance of the menu as well as the host name. This menu item can be accessed via ***System > Basic Setup***.




| Parameter name | Description | Standard | Example |
|---|---|---|---|
| Language | Set language for configuration page | English | English |
| Host Name | Hostname of TK500 | Router | My Router |

## 3.1.2. Time

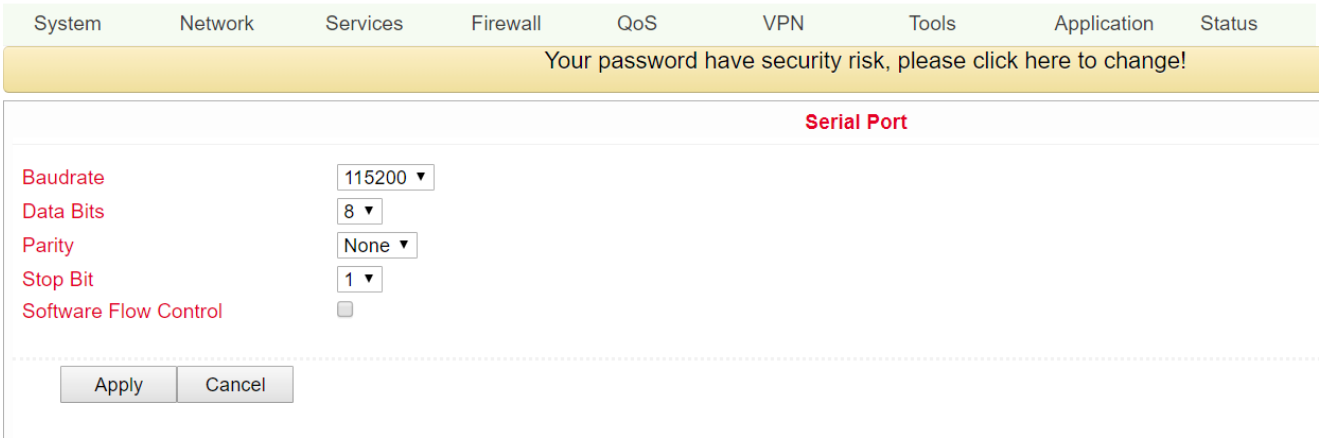
This menu item allows you to adjust the system time of the router. Furthermore, it is possible to set up a time server (NTP Time Server) to automatically keep the system time up to date.




| Name | Description | Standard |
|---|---|---|
| Router Time | Time of the router | 2017-08-01 16:00:00 |
| PC Time | Time of the PC (or the time of the device connected to the router) | The Sync Time button synchronizes the time with the connected device |
| Time zone | Set time zone | selectable time zone |
| Auto Daylight Savings Time | Automatic change summer time / winter time | disabled |
| Auto Update Time | Time of automatic time update | disabled |
| NTP Time Servers (after activating the „Auto Update Time“ option) | Setting for NTP time server. (maximum three entries) | pool.ntp.org |

## 3.1.3. Serial Port

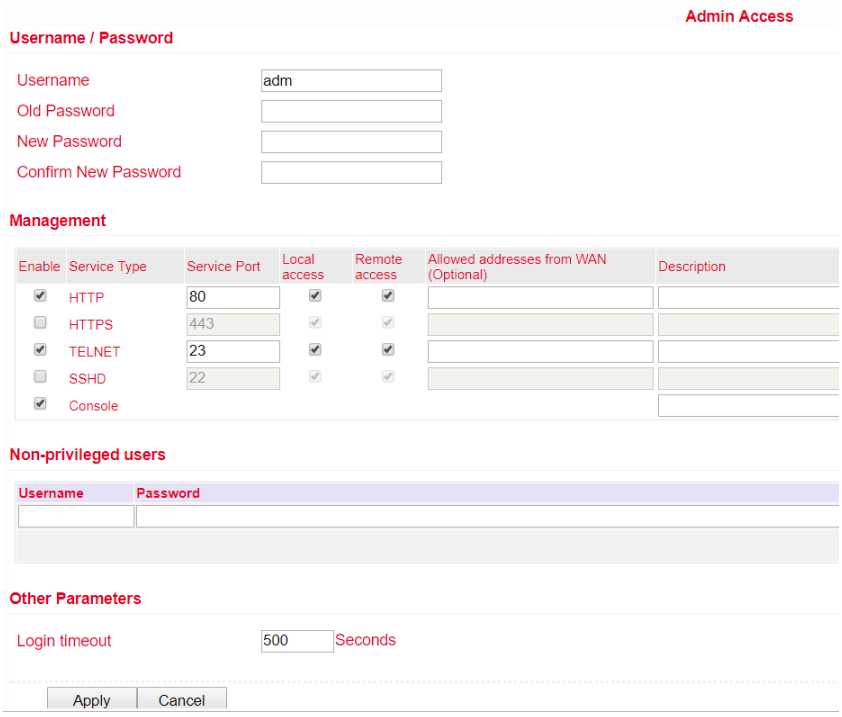
You can adjust the settings for the serial interface of the router via the menu item ***System > Serial Port***.




| Name | Description | Standard |
|---|---|---|
| Baud rate | Serial baud rate | 115200 |
| Data Bits | Serial data bits | 8 |
| Parity | Set parity bit of serial data | None |
| Stop Bit | Set stop bit of serial data | 1 |
| Software Flow Control | Software Flow Control | disabled |

## 3.1.4. Admin Access

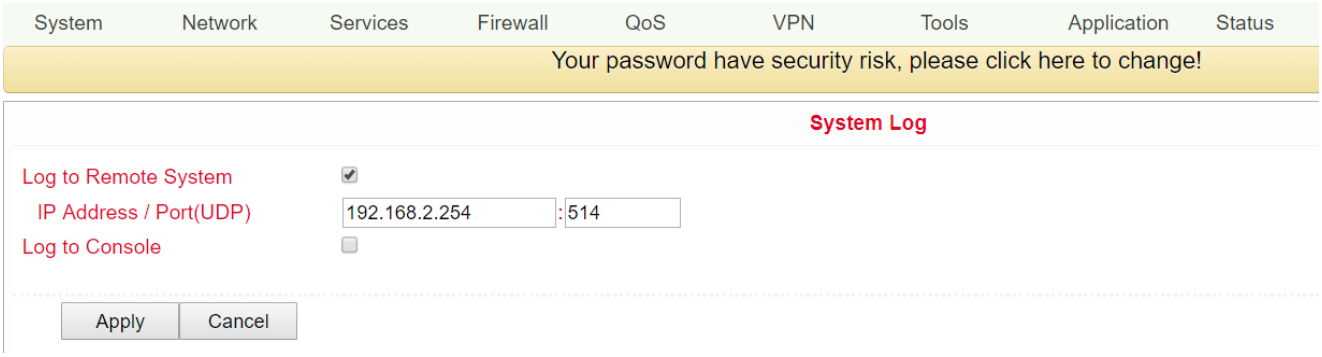
In this area, you can change or adjust important settings, such as the password of the administrator or the port assignment for accessing the router. These settings can be reached ***System > Admin Access***.



| Name | Description | Standard |
|---|---|---|
| Username/Password | | |
| Username | Username for login to the configuration page | adm |
| Old Password | Changing the password requires entering the old password | 123456 |
| New Password | Enter new password | |
| Confirm New Password | Enter new password again | |
| Management | | |
| HTTP/HTTPS/TELNET/SSHD/Console | | |
| Enable | Select to activate | enabled |
| Service Type | HTTP/HTTPS/TELNET/SSHD/Console | 80/443/23/22/Blank |
| Local Access | Enabled - Allow router to be managed over LAN (eg: HTTP) | enabled |
| Remote Access | Enabled - Allow the TK500 to be managed over WAN (for example: HTTP) | enabled |
| Allowed addresses from WAN (Optional) | Sets the range of allowed IP addresses for WAN | Control Services servers can be set, such as 192.168.2.1/30 or 192.168.2.1 |
| Description | Describe management parameters (without affecting the TK500) | |
| Non-privileged users | | |
| Username | Create user name without administrator rights | |
| Password | Create password for users without administ-rator rights | |
| Other parameter | | |
| Login Timeout | Set log timeout, after this value connection with the configuration page is disconnected and you have to log in again | 500 seconds |

## 3.1.5. System Log

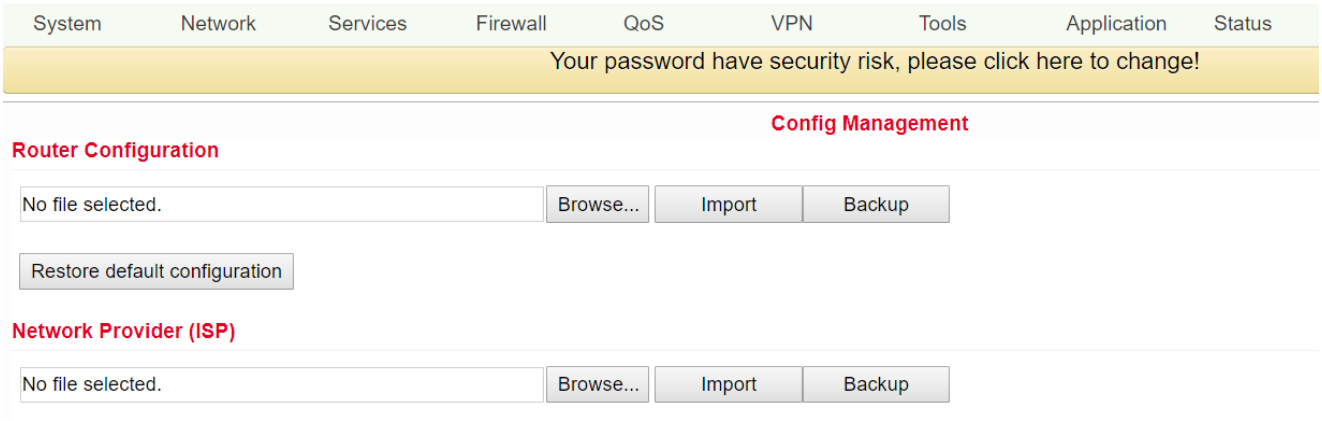
Setting options for logging log files. You can reach these via ***System > System Log***.



| Name | Description | Standard |
|---|---|---|
| Log to Remote System | Enable remote log server | Disabled (if enabled, IP address and port can be entered) |
| IP Address/Port (UDP) | Set the IP address and port of the remote log server | Port: 514 |
| Log to Console | Output of the log on the serial interface | Disabled |

## 3.1.6. Config Management

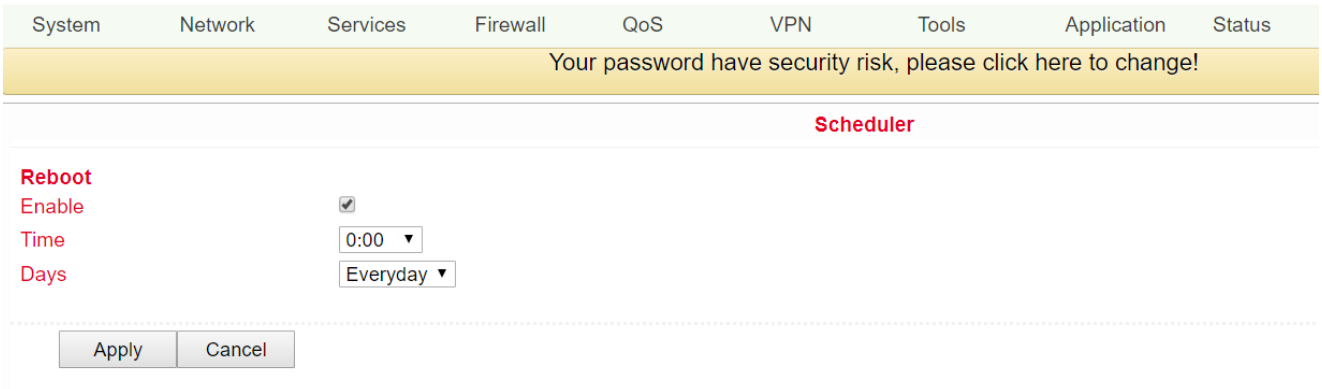
Backing up and importing router configurations, as well as reverting to the factory settings of the router and saving or restoring the provider data. You can select this menu item under ***System > Config Management***.




| Name | Description |
|---|---|
| Router Configuration | Upload / save configuration file for import / backup |
| Restore default configuration | Click to reset the TK500 (to enable the default configuration, the TK500 must be restarted.) |
| Network Provider (ISP) | To import or save APN, username, password and other parameters from conventional operators |
| Durchsuchen | With the Browse button you can select the file with the settings that should be uploaded via Import |

## 3.1.7. Scheduler

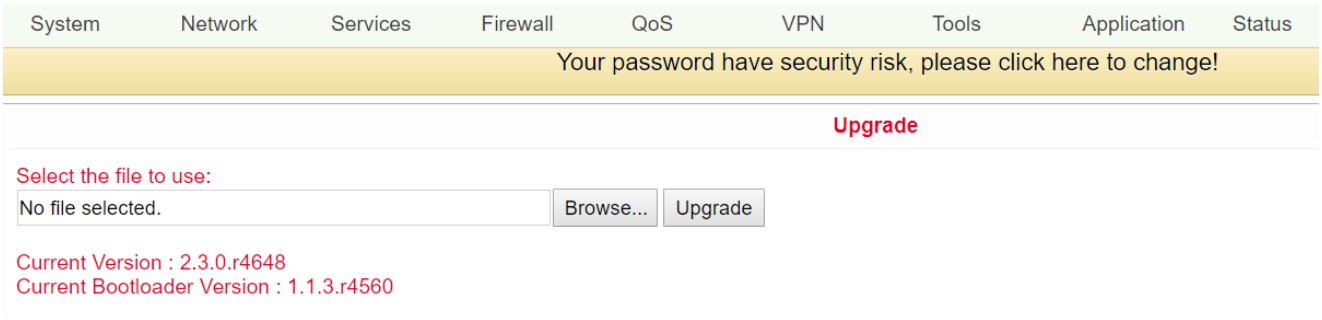
The scheduler is used to set the automatic reboot for the router. You can specify the settings via ***System > Scheduler***.



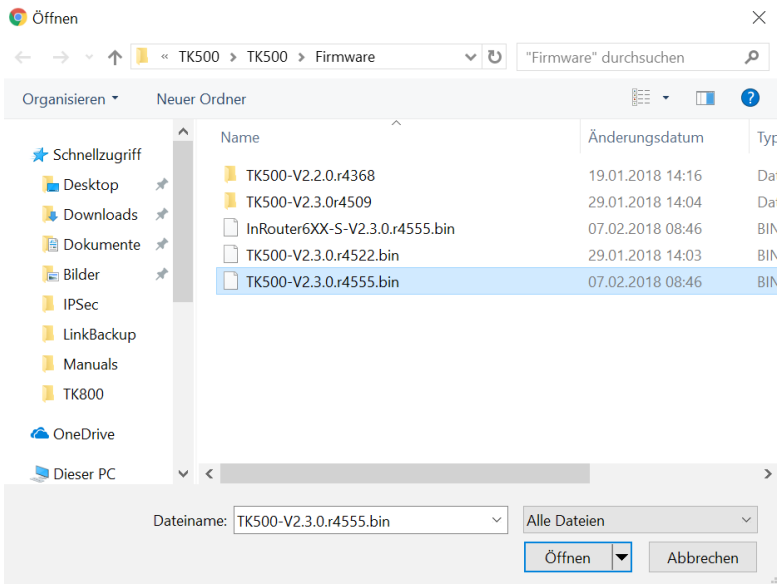
| Name | Description |
|---|---|
| Enable | Turn the auto reboot on or off |
| Time | Time at which the TK500 router should be rebooted |
| Days | Selection Everyday for the daily restart |

## 3.1.8. Upgrade

In this area, the router provides an interface for updating the firmware. Select ***System > Upgrade***.




To update the system, select the update file (e.g., TK500-V2.2.0v4xxx.bin) in your file system using the ***Select File*** button.

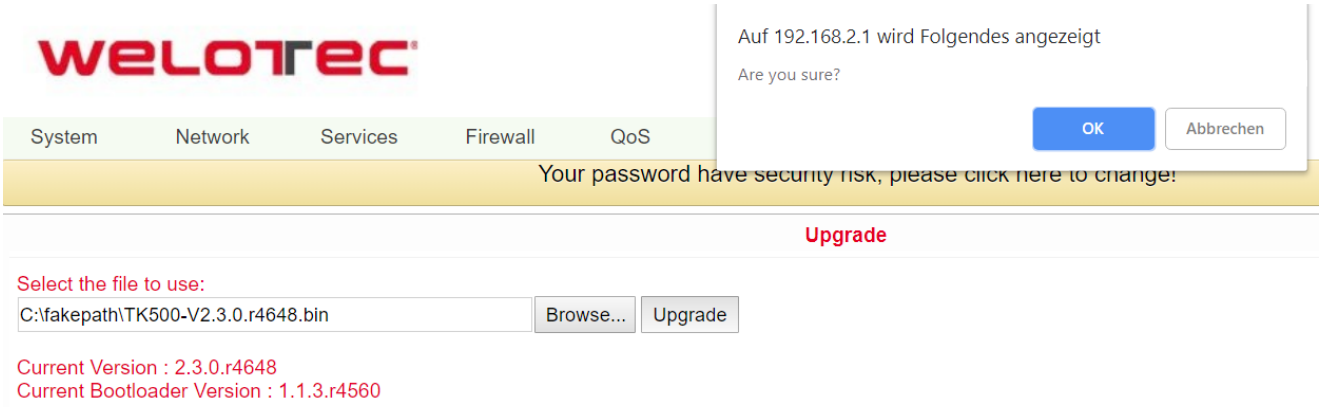



Click on the „***Upgrade***" button and confirm the start of the update


After successfully updating the firmware, click ***Reboot*** to restart the TK500.

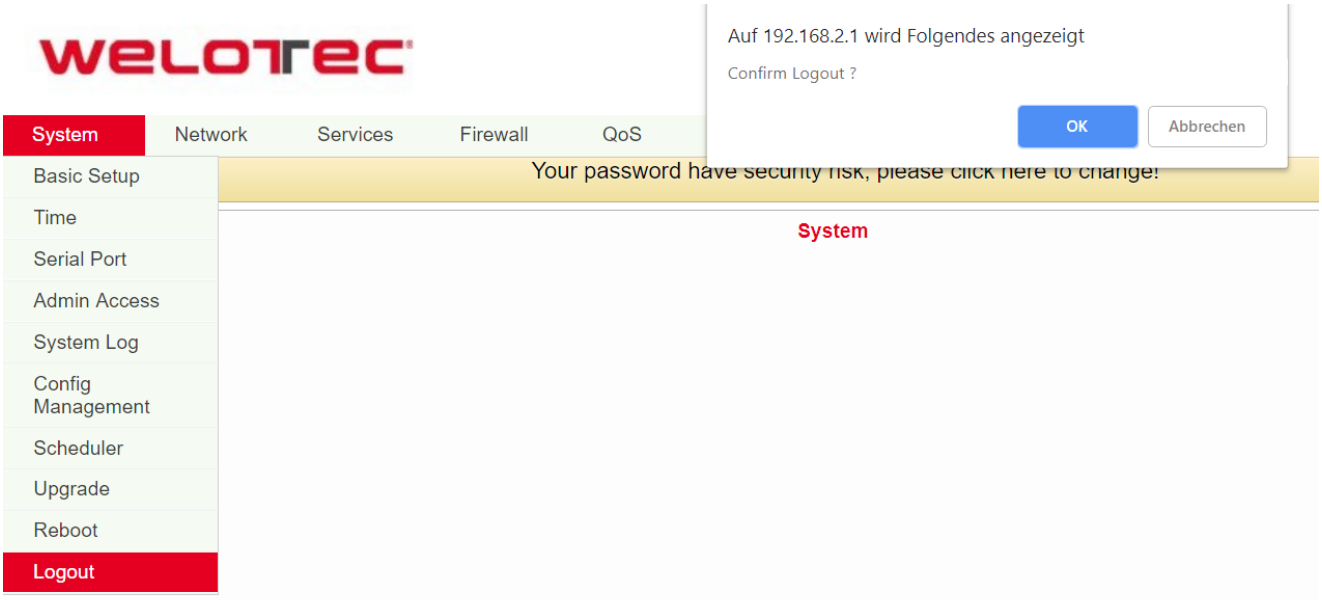
## 3.1.9. Reboot

If you need to reboot your router, select ***System > Reboot***. Then click „***OK***" to reboot the system.




## 3.1.10. Logout

To log out of the system, click on ***System > Logout*** and confirm the logout with „***OK***".

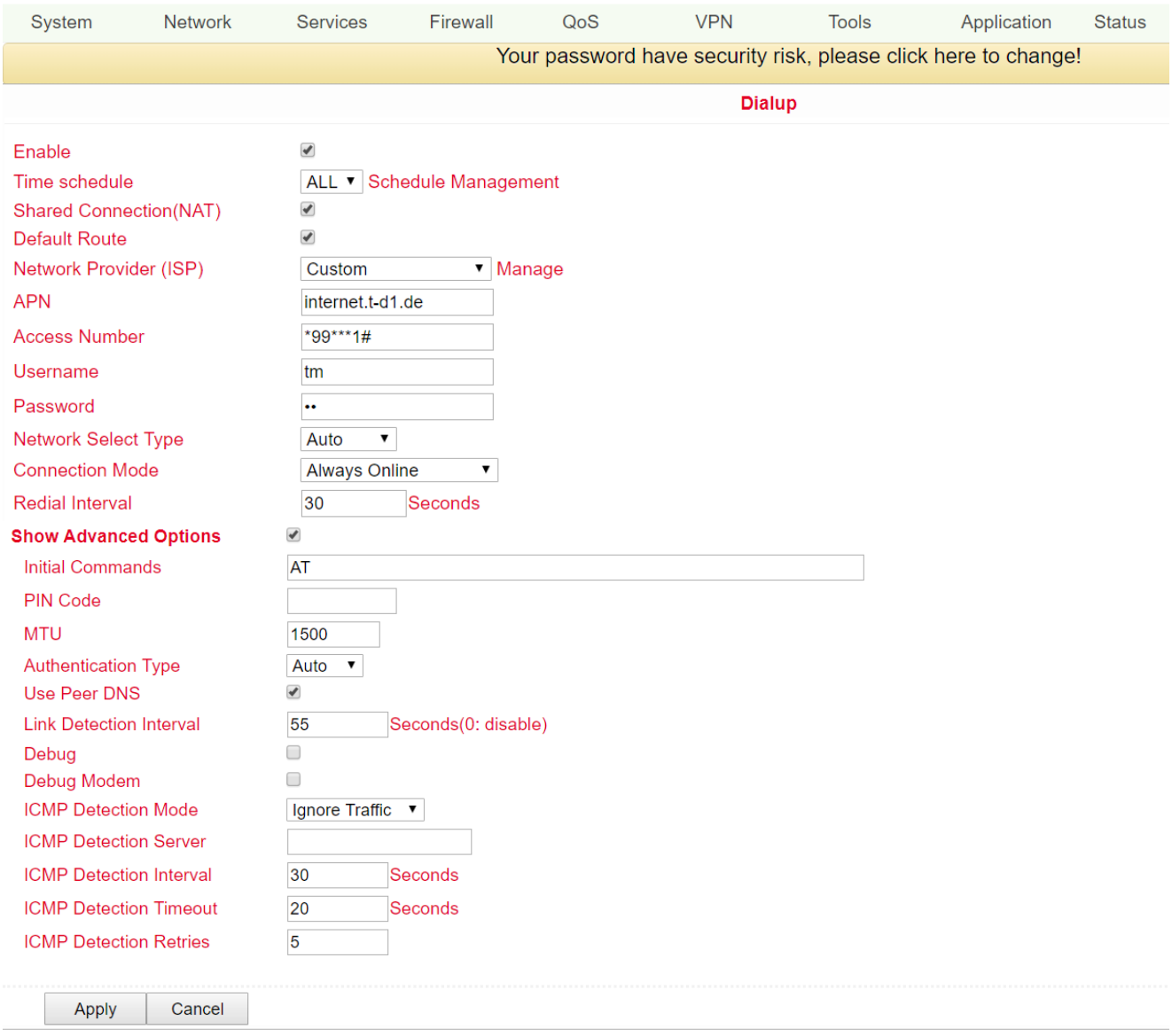


# 3.2. Network

Network settings allow you to configure Dial-up, WAN, Link Backup, LAN, WLAN, DNS, DDNS, Static route, etc.

## 3.2.1. Dialup

In this menu area, you define and configure the dial-in of your router. Select ***Network > Dialup***.

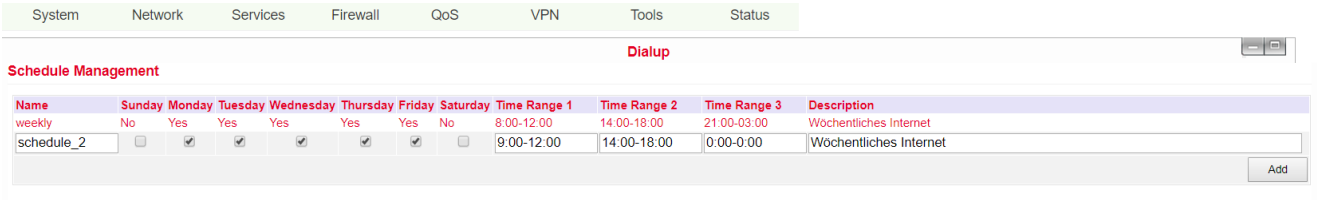


| Name | Description | Standard |
|---|---|---|
| Enable | Enables the dialup function | enabled |
| Time Schedule | Set time for online and offline (see also 3.2.1.1) | ALL |
| Shared Connection (NAT) | Enabled - device connected to router | enabled |
| Default Route | Mobile interface as a standard route to the Internet | enabled |
| Network Provider (ISP) | Select Local ISP, if not listed here, select "Custom" | Custom |
| APN | APN parameter supplied by the provider | internet.t-d1.de (Telekom) |
| Access Number | Dial-in parameters provided by the local ISP | *99***1# |
| Username | Username provided by the provider | tm |
| Password | Password provided by the local ISP | tm |
| Network Select Type | Select mobile network type (2G, 3G, 4G only) | Auto |
| Connection Mode | Connection mode: Router is always online | Always Online |
| Redial Interval | If dialing fails, the TK router will dial again after this interval | 30 seconds |
| Show Advanced Options | Allows you to configure advanced options | disabled |
| PIN Code | Field for the PIN number of the SIM card | empty |
| MTU | Set MTU (Maximum Transmission Unit) | 1500 |
| Authentication Type | PAP, CHAP | Auto |
| Use Peer DNS | Enable this option to accept peer DNS | enabled |
| Link Detection Interval | Set interval for connection detection (0 = disabled) | 55 seconds |
| Debug | Enable debug mode | disabled |
| Debug Modem | Enable debug modem | disabled |
| ICMP Detection Mode | Monitor Traffic: Only when no data is flowing a Keep Alive Ping is sent at regular intervals. | Monitor Traffic |
| ICMP Detection Server | Set server for ICMP discovery; empty field means there is none | empty |
| ICMP Detection Interval | Set interval for ICMP detection | 30 seconds |
| ICMP Detection Timeout | Set timeout for ICMP discovery (TK500 is restarted on ICMP timeout) | 20 seconds |
| ICMP Detection Retries | Set the maximum number of retries if ICMP fails | 5 |

### 3.2.1.1. Schedule Management

Schedule management (next to ***"Time schedule"***):


Here you can run your own dialup strategy, which means that you can specify over three time periods here when the router should be online.

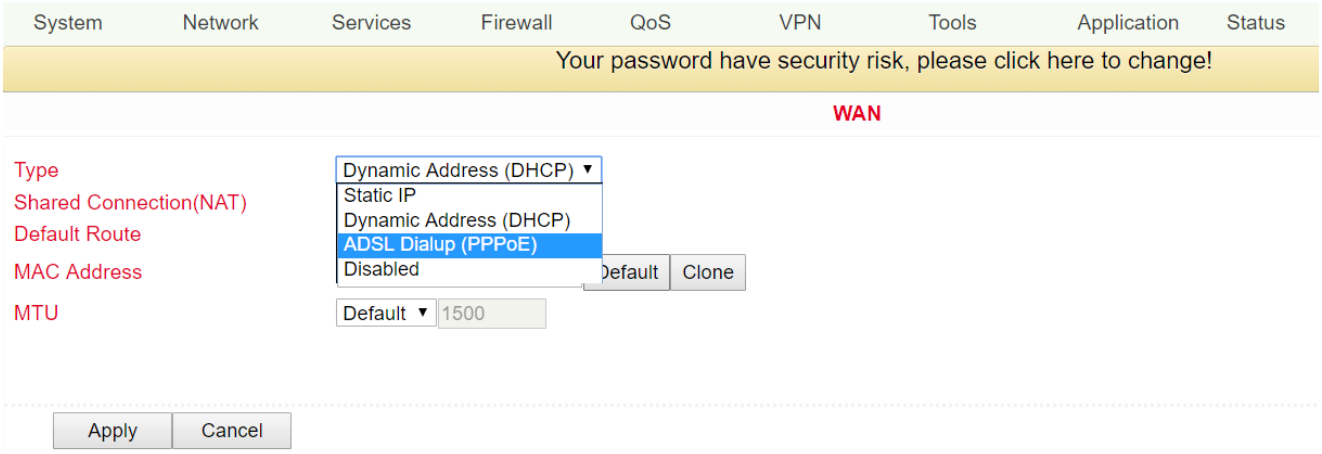



| Name | Description | Standard |
|---|---|---|
| Name | Name for time schedule | Schedule_1 |
| Sunday | Sunday | empty |
| Monday | Monday | enabled |
| Tuesday | Tuesday | enabled |
| Wednesday | Wednesday | enabled |
| Thursday | Thursday | enabled |
| Friday | Friday | enabled |
| Saturday | Saturday | empty |
| Time Range 1 | Set Time Range 1 | 9:00-12:00 a.m. |
| Time Range 2 | Set Time Range 2 | 02:00-06:00 p.m. |
| Time Range 3 | Set Time Range 3 | 0:00-0:00 |
| Description | Describe the configuration | empty |

You can also create multiple schedules, if for example different working times apply on a working day.

## 3.2.2. WAN (only for TK5x5L-W, TK5x5L, TK5x5U)

Here you can set up a new WAN (Wide Area Network). Accessible via ***Network > WAN***.



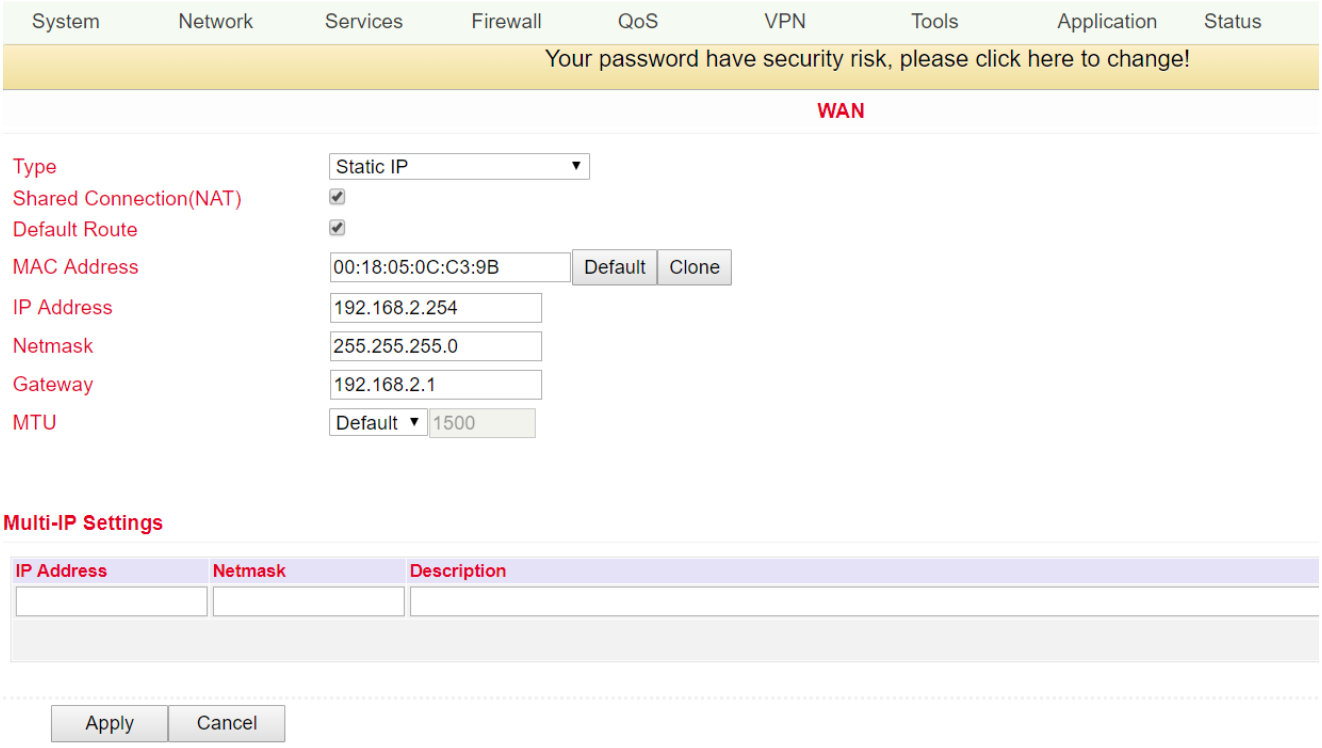

On this page you can specify the type of WAN port:

| Name | Description | Standard |
|---|---|---|
| Type | Static IP<br>Dynamic Address(DHCP)<br>ADSL Dialup(PPPoE)<br>Disabled | Disabled |

**Note**

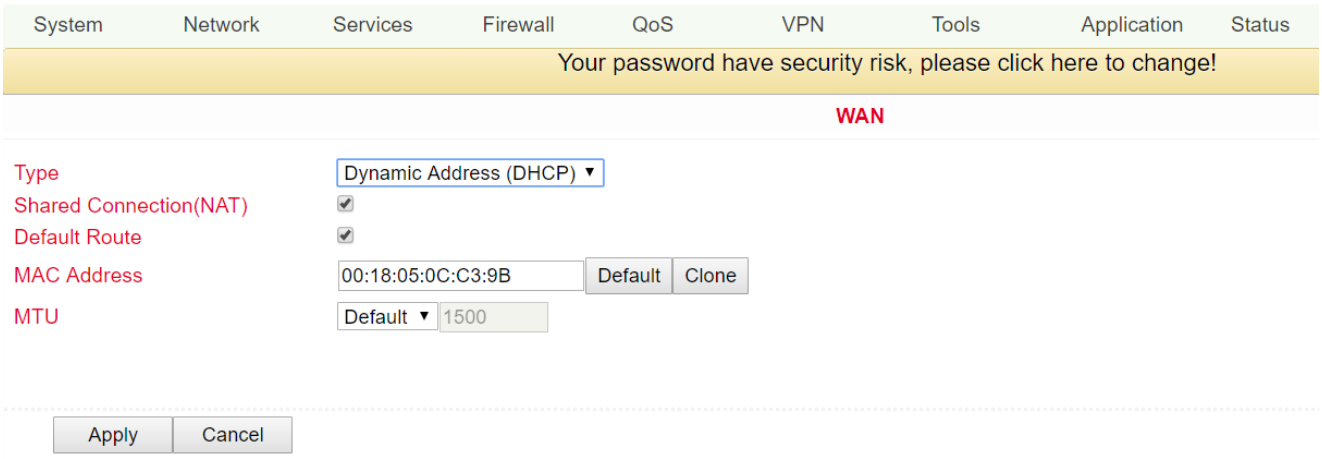
Only one WAN type can be activated at a time. Activating one type deactivates another type.

### 3.2.2.1. Static IP



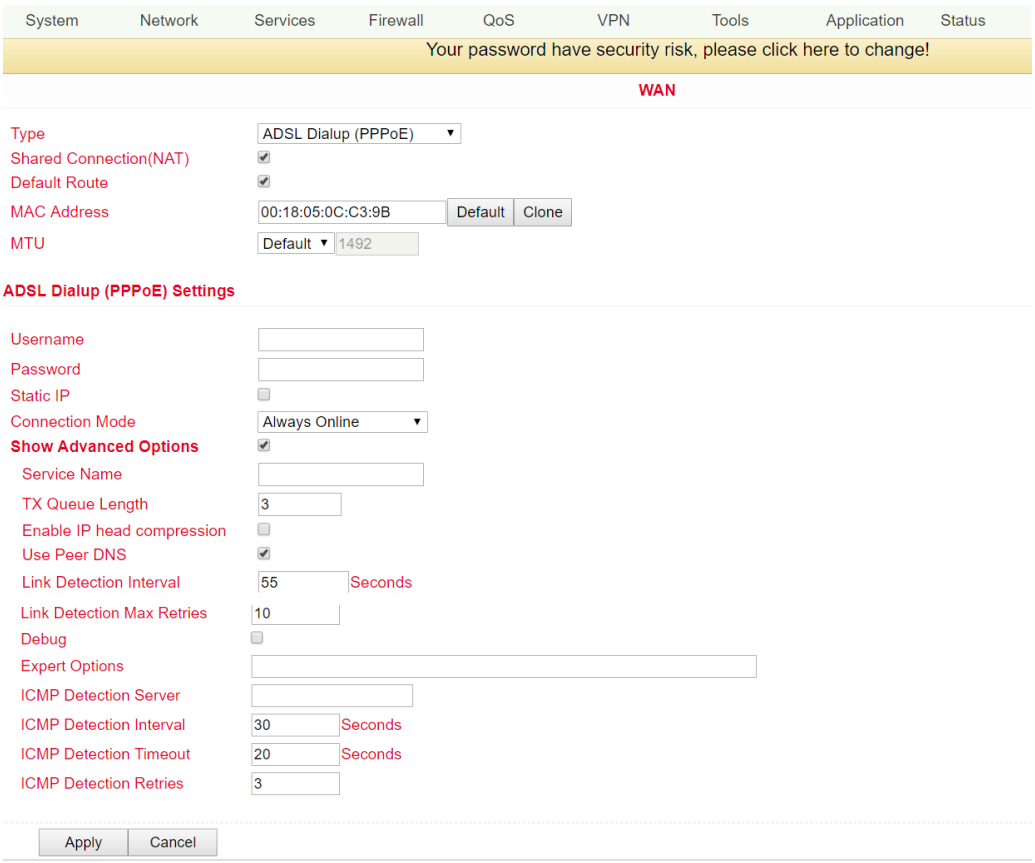
| Name | Description | Standard |
|---|---|---|
| Type | Static IP | disabled |
| Shared Connection (NAT) | Enabled - local device connected to the router can access the Internet | enabled |
| Default Route | Mobile interface as standard route to the Internet | enabled |
| MAC Address | Set MAC address (button Default = default, clone = newly created MAC address) | Default |
| IP Address | Set IP address for WAN port | 192.168.1.29 |
| Netmask | Set netmask for WAN port | 255.255.255.0 |
| Gateway | Set WAN gateway | 192.168.1.1 |
| MTU | Maximum Transmission Unit (MTU), the options "Default" and "Manual" are possible. | Default = 1500 |
| „Multi-IP Settings" (a maximum of 8 additional IP addresses can be specified) | | |
| IP Address | Set an additional IP address for LAN | empty |
| Netmask | Set Netmask | empty |
| Description | Describe settings | empty |

### 3.2.2.2. Dynamic Address (DHCP)




| Name | Description | Standard |
|---|---|---|
| Type | Dynamic Address (DHCP) | |
| Share Connection (NAT) | Enabled - local device connected to the router can access the Internet | enabled |
| Default Route | Mobile interface as standard route to the Internet | enabled |
| MAC Address | Set MAC address | |
| MTU | Set Maximum Transmission Unit (MTU), the options "Default" and "Manual" are possible. | Default = 1500 |

## 3.2.2.3. ADSL Dialup (PPPoE)

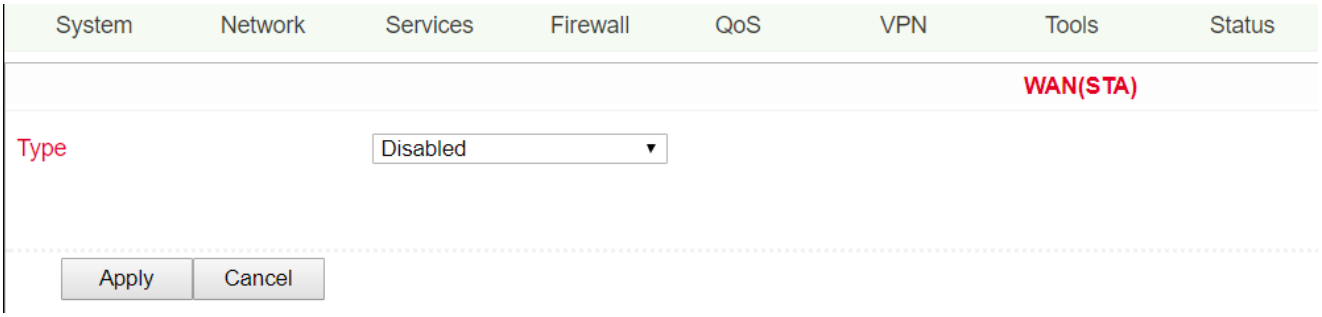



| Name | Description | Standard |
|---|---|---|
| Type | ADSL Dialup (PPPoE) | |
| Share Connection (NAT) | Enabled - local device connected to the router can access the Internet | Enabled |
| Default Route | Mobile interface as standard route to the Internet | Enabled |
| MAC Address | Set MAC address | |
| MTU | Set Maximum Transmission Unit (MTU), the options "Default" and "Manual" are possible. | Default = 1492 |
| ADSL Dialup (PPPoE) Settings | | |
| Username | Set user name to dial in | empty |
| Password | Set password to dial in | empty |
| Static IP | Activate static IP address | disabled |
| Connection Mode | Set connection mode ("Connect on Demand"/"Always Online"/"Manual") | Always Online |
| Show Advanced Options | | |
| Show advanced options | Enable advanced options | disabled |
| Service Name | Here you can assign a name for the service | empty |
| TX Queue Length | Specifying the length of the transfer queue | 3 |
| Enable IP head compression | Click to enable IP head compression | disabled |
| User Peer DNS | Activate Peer DNS for User | disabled |
| Link Detection Interval | Setting the connection detection interval | 55 Seconds |
| Link Detection Max Retries | Set maximum number of repetitions for connection detection | 10 (times) |
| Debug | Select to activate Debug mode | disabled |

| | | |
|---|---|---|
| Expert Options | Determine expert parameters | empty |
| ICMP Detection Server | Set server for ICMP detection | empty |
| ICMP Detection Intervall | Set time for ICMP detection | 30 |
| ICMP Detection Timeout | Set timeout for ICMP detection | 3 |
| ICMP Detection Retries | Set the Maximum Number of Repetitions for ICMP Detection | 3 |

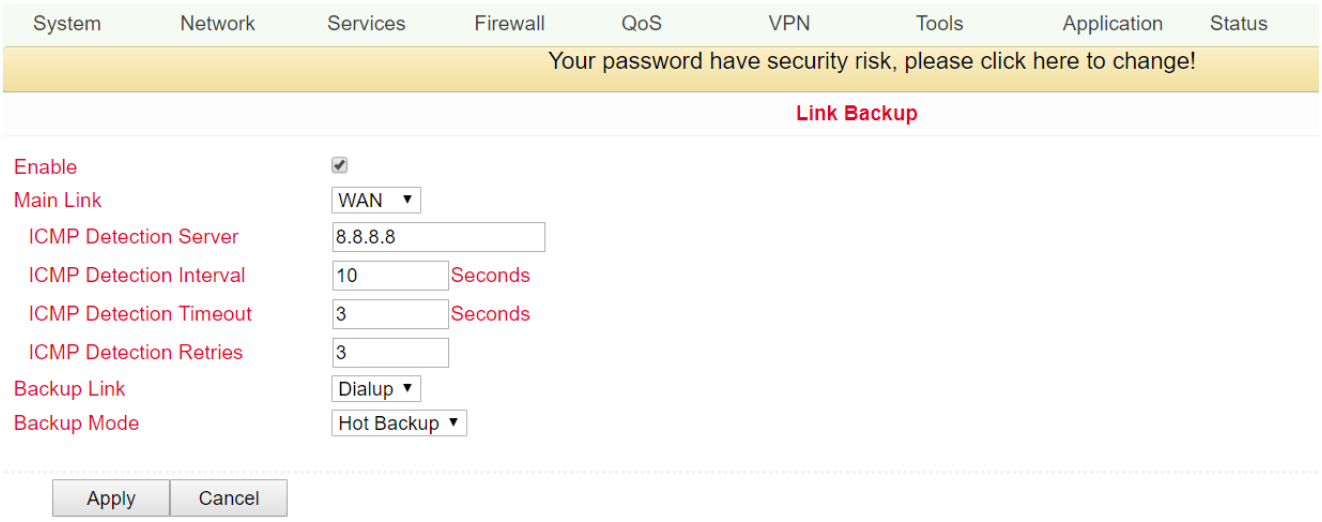
## 3.2.3. WAN(STA)

Under this menu item ***Network > WAN(STA)*** you can configure the TK500 as a WAN station.




## 3.2.4. Link Backup

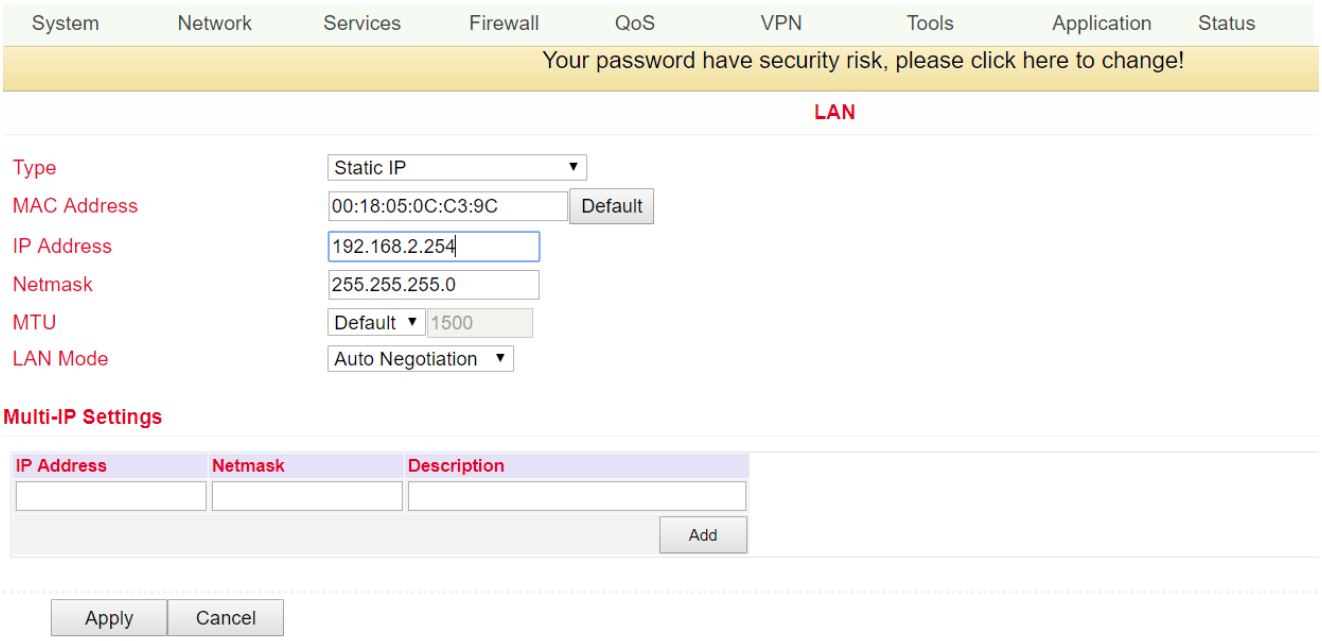
This option secures connections between radio WAN and Ethernet WAN. If one WAN fails, the TK500 automatically uses the other. You can configure this under ***Network > Link Backup***.




| Name | Description | Standard |
|---|---|---|
| Enable | Activate Service for Connection Backup | Deactivated |
| Main Link | Selection of WAN, Dialup and WAN(STA) as main WAN possible | WAN |
| ICMP Detection Server | ICMP can ensure a connection to a specific destination | Empty |
| ICMP Detection Interval | Time interval between ICMP packets | 10 |
| ICMP Detection Timeout | Timeout for the individual ICMP packets | 3 (Seconds) |
| ICMP Detection Retries | If the ICMP detection was not repeated successfully, the backup connection is selected. | 3 |
| Backup Link | Select Backup Connection | Dialup |
| Backup Mode | Hot Backup / Cold Backup | Hot Backup |

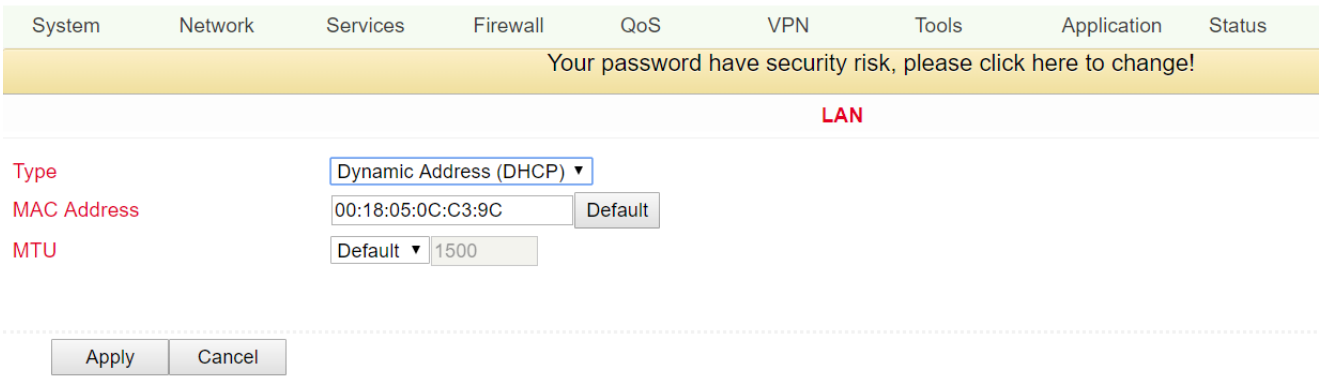
## 3.2.5. LAN

Use the LAN menu area to adjust the settings for the LAN connection of the router and add Multi-IP settings. Accessible via ***Network > LAN***.



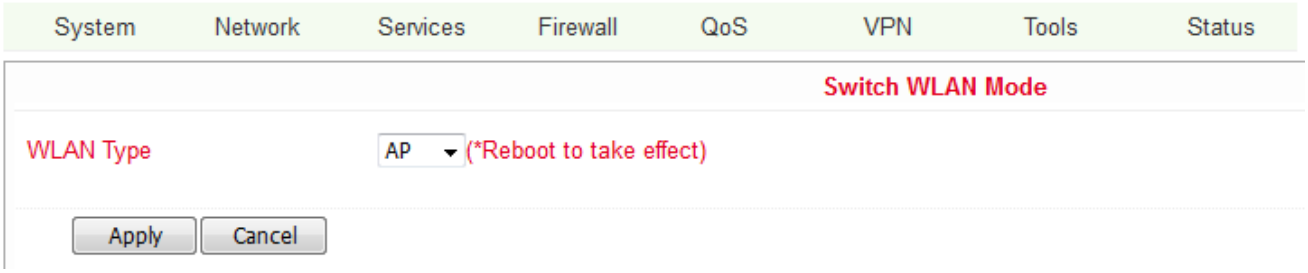

| Name | Description | Standard |
|---|---|---|
| Type | Selection between static IP address (Static IP) or DHCP (Dynamic Address) | Static IP |
| MAC Address | The MAC address in the LAN | Default can be restored via Button |
| IP Address | Set IP address in the LAN | 192.168.2.1 (If it has been changed, you have to enter the new address on the configuration site) |
| Netmask | Set network mask of the LAN | 255.255.255.0 |
| MTU | St MTU-Length. Possible Options are "Manual" or "Default" | Default 1500 |
| LAN Mode | Auto Negotiation, automatically selects connection type | Auto Negotiation |
| „Multi-IP Settings" (a maximum of 8 additional IP addresses are supported) | | |
| IP Address | Set further IP address for LAN | Empty |
| Description | Description of this IP address | Empty |

If ***Dynamic Address (DHCP)*** is selected, the router is assigned a dynamic IP address.




## 3.2.6. Switch WLAN Mode

You can make settings for the WLAN type here. A distinction is made between Access Point (AP) and Station (STA). You can reach it under ***Network > Switch WLAN Mode***.

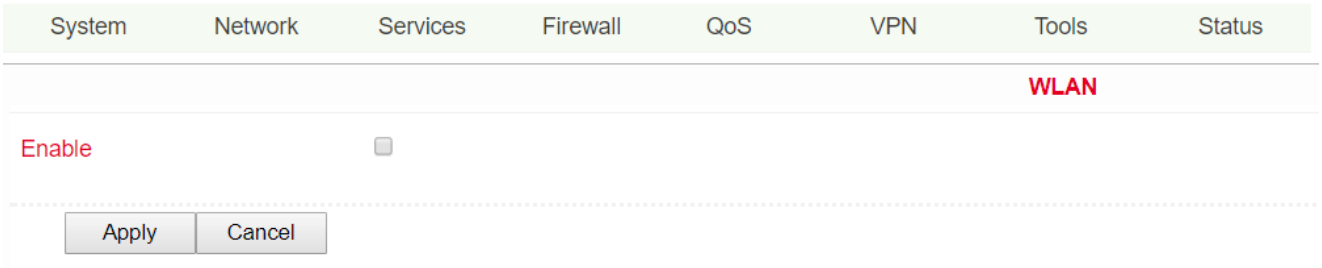



| Name | Description | Standard |
|---|---|---|
| AP | Access Point Modus | AP |
| STA | Client Modus | |

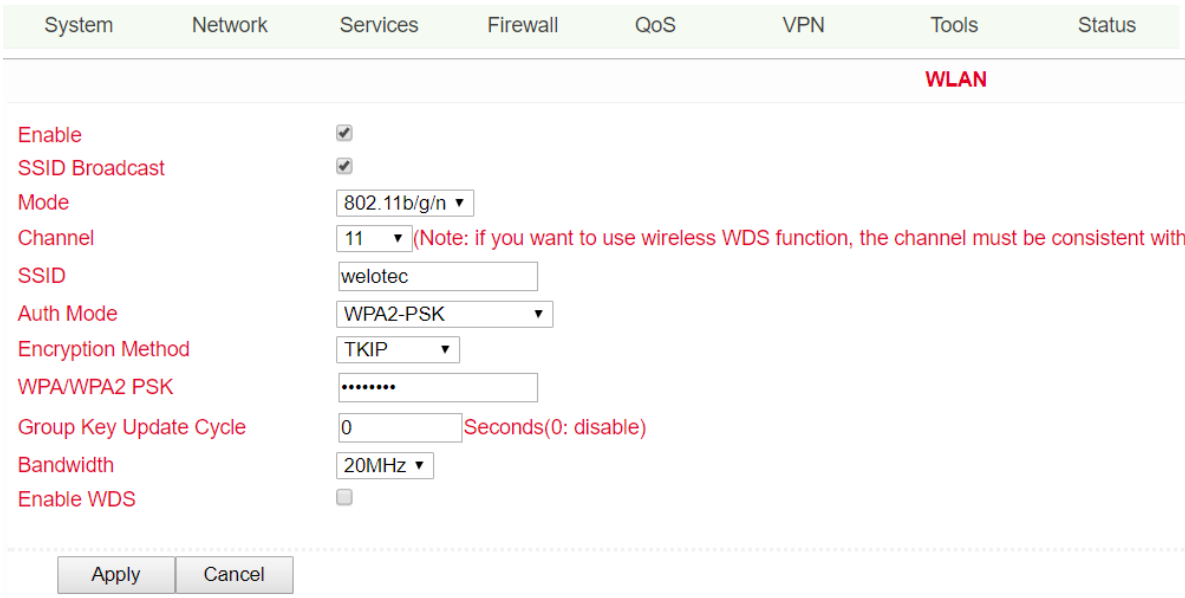
If ***STA*** is selected as WLAN TYPE (for station), the menu changes under ***Network***. It is then possible to configure WAN(STA) under 3.2.3.3 and only one client for an existing WLAN under 3.2.6.a ***WLAN Client***.

## 3.2.7. WLAN

The WLAN can be configured in this area of the router. It is deactivated as standard. You can start the configuration via ***Network > WLAN***.



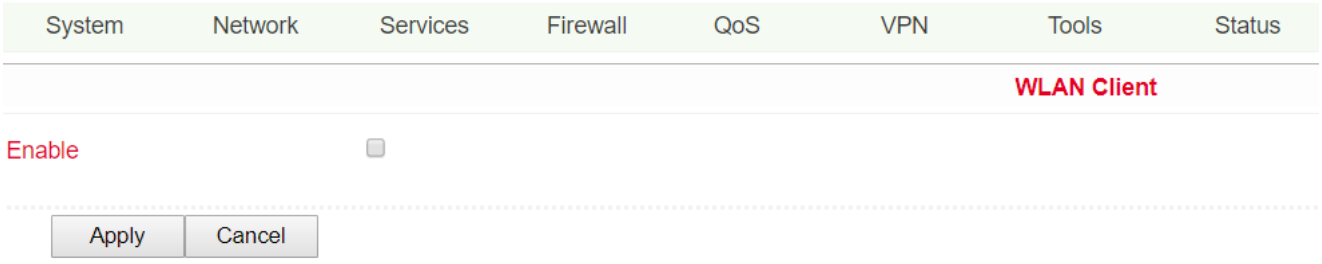

To turn on the WLAN, click on the ***Enable*** selection field.



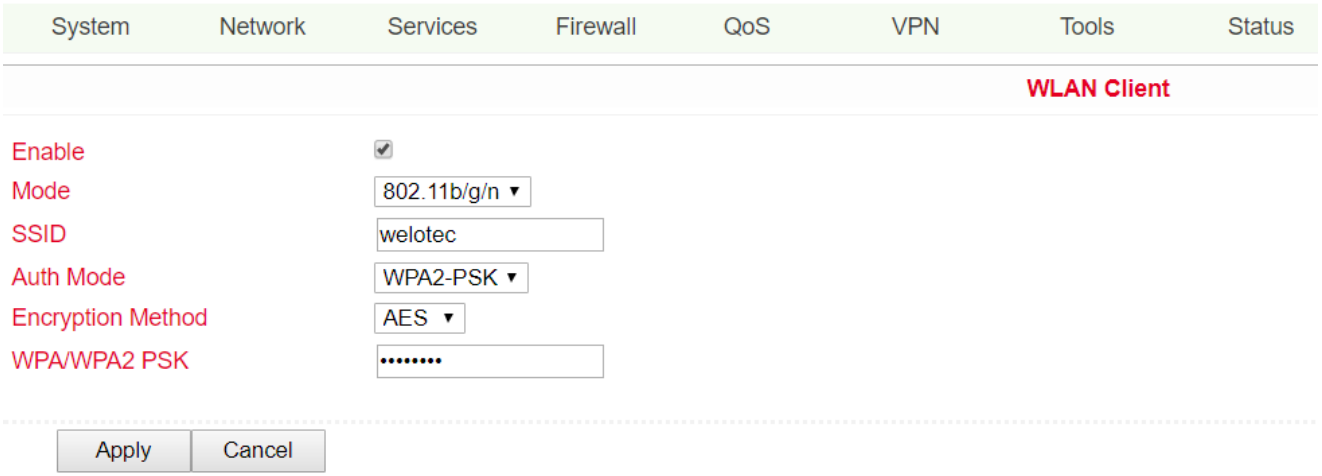

| Name | Description | Standard |
|---|---|---|
| Enable | Switching WLAN on/off | off |
| SSID Broadcast | When enabled, the SSID is sent | enabled |
| Mode | Choice between various WLAN modes, e.g. 802.11 b/g/n | 802.11 b/g/n |
| Channel | Transmission channel. Selection between 1 and 13 or automatic | 11 |
| SSID | Service Set Identifier or SSID for short stands for the WLAN name | welotec |
| Auth. Mode | Authentication mode for the WLAN, the selection fields change depending on the selection | OPEN |
| Encryption Method | Encryption method. TKIP, AES or TKIP/AES selection | none |
| WPA/WPA2 PSK | Enter the key to be used for accessing the WLAN | none |
| Group Key Update Cycle | Cycle for updating the group key in seconds | 0 |
| Bandwith | WLAN bandwidth. 29 or 40 MHz are selectable | 20MHz |
| Enable WDS | Enables WDS on the Router | off |
| Depending on the selection of the Auth. Mode, the input fields can vary greatly. We are happy to offer you our support in the creation of an ideal and secure WLAN. | | |

### 3.2.7.1. WLAN Client

If the point ***STA*** was selected as WLAN type when configuring the ***Switch WLAN Mode*** (s. 3.2.6.) WLAN configuration is no longer possible. Then you can only configure the TK 500 as WLAN Client. This can be done under ***Network > WLAN Client***.



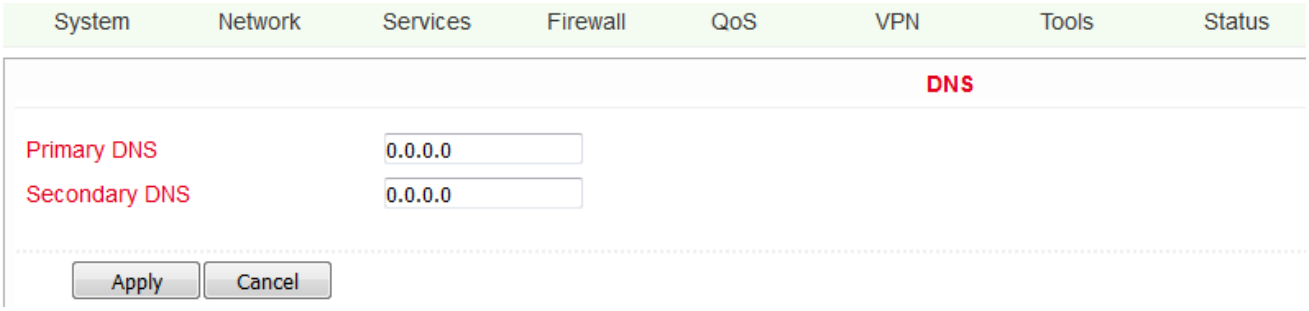

Please activate ***Enable*** to configure the Router as WLAn client.




Enter the data to connect the TK500 to an existing WLAN.

## 3.2.8. DNS

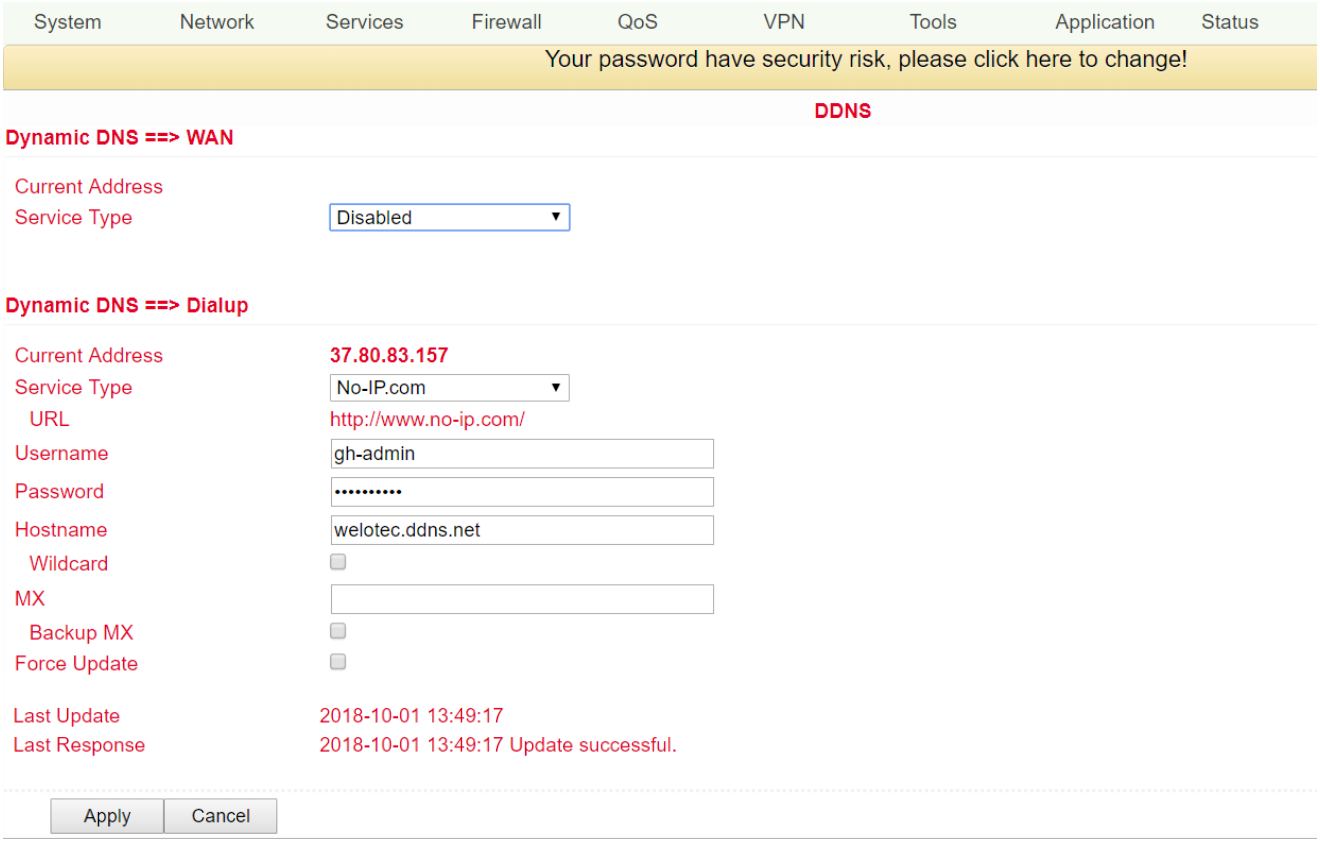
Up to two DNS servers can be entered here if the router is part of a domain network that uses DNS for address resolution. You can enter the data under ***Network > DNS***.




| Name | Description | Standard |
|---|---|---|
| Primary DNS | Set primary DNS | Empty |
| Secondary DNS | Set secondary DNS | Empty |

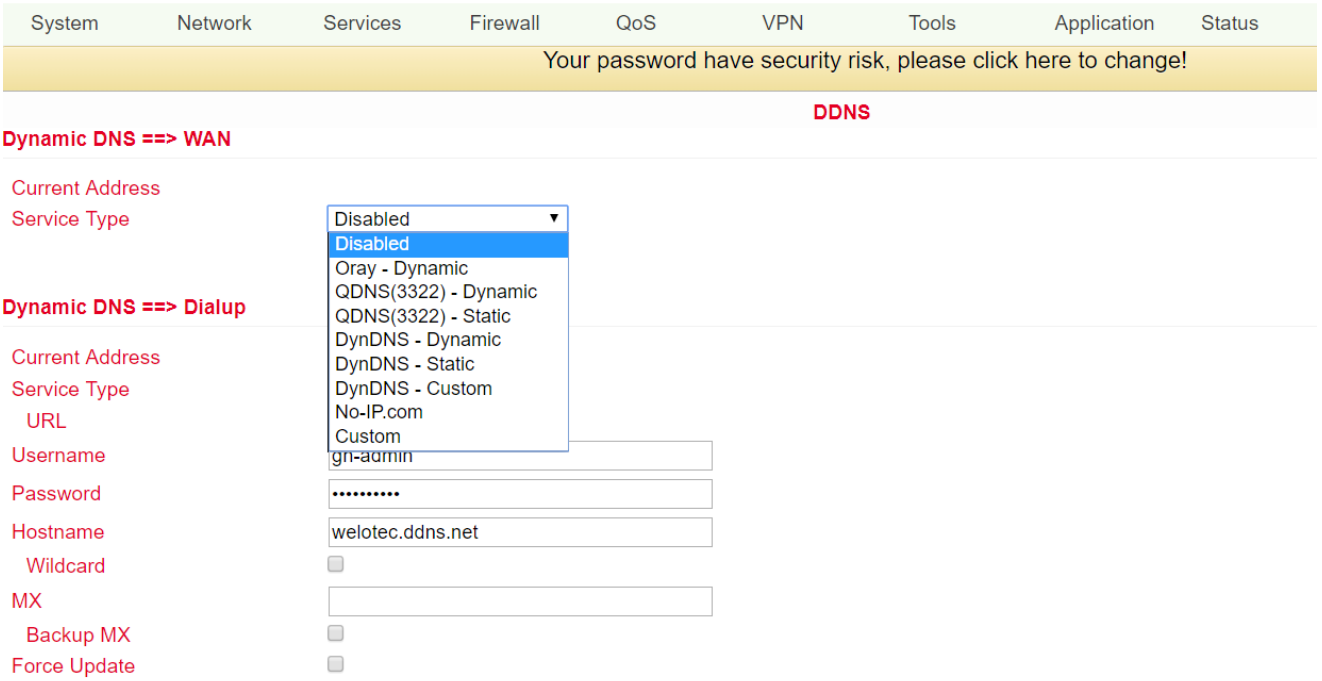
## 3.2.9. DDNS (Dynamic DNS)

DDNS or dynamic DNS is used if the WAN connection does not have a fixed public IP address, but services are still to be accessed externally. Since the IP address of the provider can change again and again with a normal WAN connection, it is not possible to set up a secure VPN tunnel, for example. Therefore, providers of dynamic DNS servers are used, which ensure that your WAN connection always gets the IP address. The configuration can be reached via ***Network > DDNS***.

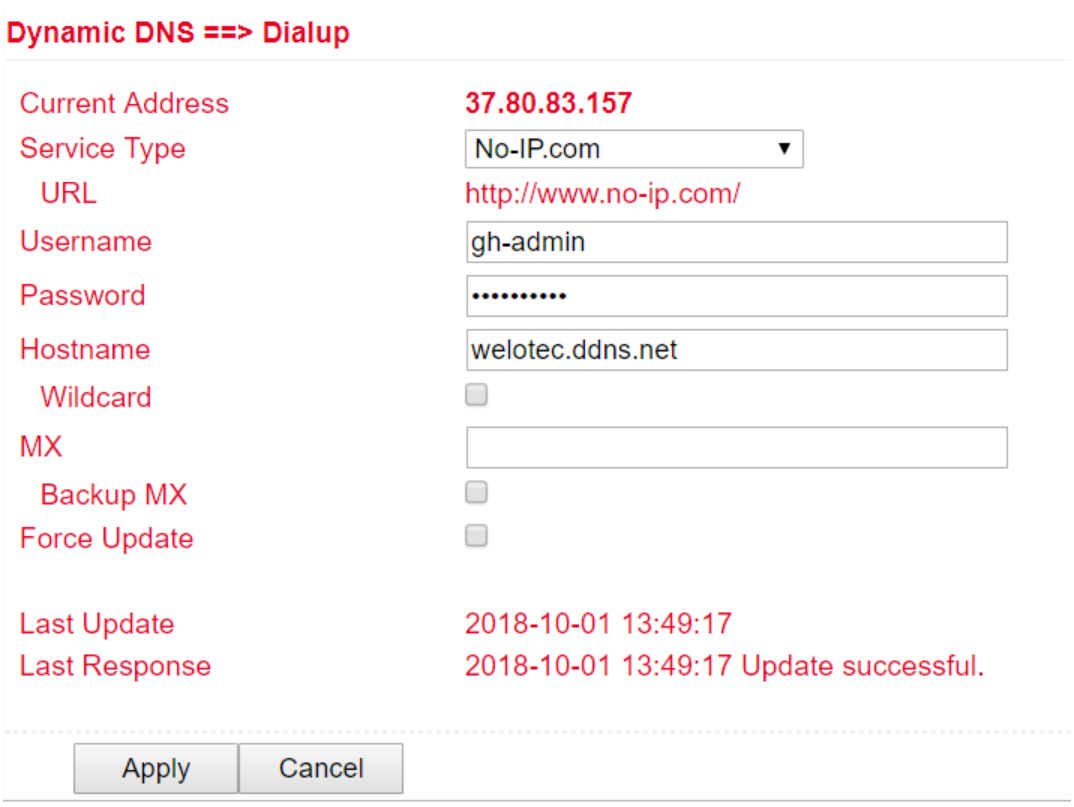



| Name | Description | Standard |
|---|---|---|
| Current Address | Display current IP-address | Empty |
| Service Type | Select DDNS-Provider | Deactivated |

There are various setting options for various providers of DDNS services. You select these using the service type.




No-IP is used here as an example for the setup. For this you need a No-IP account, which you have to create yourself. Here there are various providers, some of which are free, but also liable to pay costs. The assignment of the Dynamic DNS can be assigned to the WAN as well as to the Dialup connection.

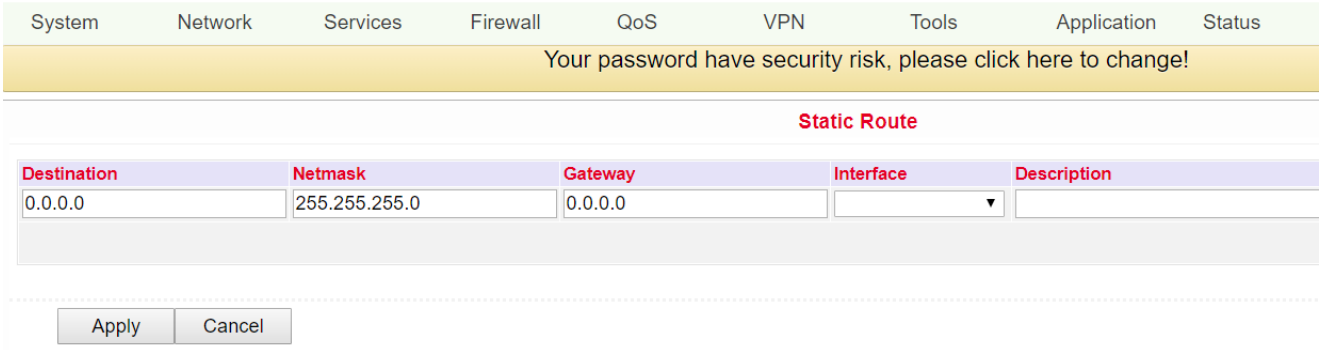



| Name | Description | Standard |
|---|---|---|
| Service Type | DynDNS - Dynamic | disabled |
| URL | http://www.dyndns.com/ | dignified |
| Username | Registered Username for | |

| | | |
|---|---|---|
| DDNS | Empty | |
| Password | Registered Password for DDNS | Empty |
| Hostname | Registered Hostname for DDNS | Empty |
| Wildcard | Can be activated if wildcard should be used | Deactivated |
| MX | Entering an MX Record | Empty |
| Backup MX | Can be activated if MX-Record is to be activated | Deactivated |
| Force Update | Forces the Update of the Account | Deactivated |
| Last Update | Shows when the IP address was last changed | |
| Last Response | Shows the last time the Service was communicated with | |

## 3.2.10. Static Route

Here you can add static routes. Static routes provide your router with additional routing information. Under normal circumstances, the router has sufficient information if configured for Internet access, and no further static routes need to be configured. Static routes only need to be specified in exceptional cases, for example, if your network contains multiple routers or IP subnets. You can add static routes under ***Network > Static Route*** by clicking the Add button..



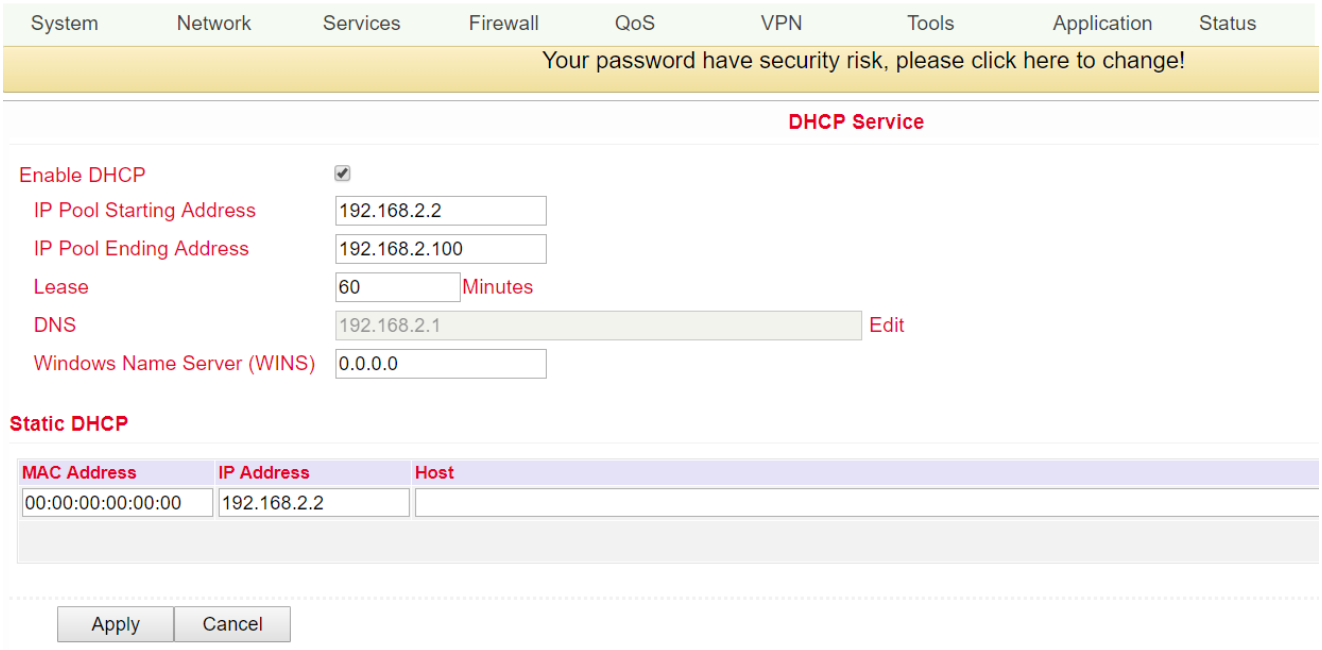

| Name | Description | Standard |
|---|---|---|
| Destination | Set the IP address of the destination | Empty |
| Netmask | Specifying the target's subnet mask | 255.255.255.0 |
| Gateway | Defining the Gateway of the Destination | Empty |
| Interface | Optional LAN/WAN port access to destination | Empty |
| Description | Freely selectable name for the static route | Empty |

# 3.3. Services

Within the service settings, configure the DHCP service, DNS forwarding, VRRP and other related parameters.

## 3.3.1. DHCP Service

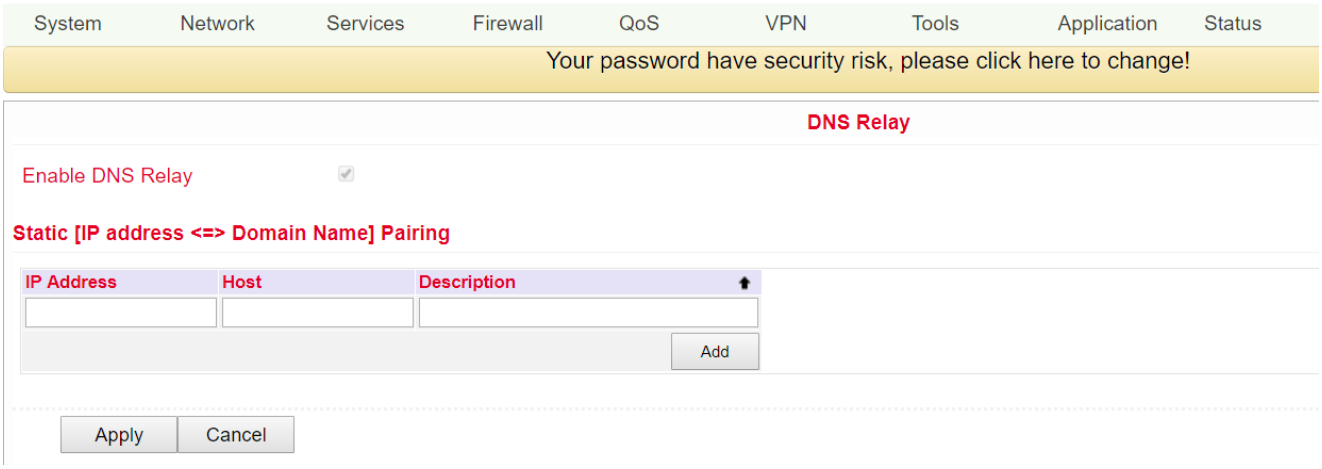
The Dynamic Host Configuration Protocol (DHCP) is a communication protocol in network technology. It allows the assignment of the network configuration to clients by a server. This allows devices in the network to be dynamically assigned IP addresses. You can access this service under ***Services > DHCP Service***.




| Name | Description | Standard |
|---|---|---|
| Enable DHCP | Click to enable DHCP | Enabled |
| IP Pool Starting Address | Setting the start IP address of the DHCP pool | 192.168.2.2 |
| IP Pool Ending Address | Setting the end IP address of the DHCP pool | 192.168.2.100 |
| Lease | Set valid lease time for the IP address received from the DHCP server | 60 Minutes |
| DNS | Set DNS server (click on Edit) | 192.168.2.1 |
| Windows Name Server | Set WINS | Empty |
| Static DHCP (only 20 IP-addresses can be set up) | | |
| MAC Address | Specify the MAC address of a intended IP address | Empty |
| IP Address | Set static IP | 192.168.2.2 |
| Host | Set Hostname | Empty |

## 3.3.2. DNS Relay

If DNS relay is enabled (by default, if DHCP is set up), DHCP clients are assigned the IP address of the router as DNS server. All DNS requests to the router are sent to your Internet service provider's DNS servers. If DNS relay is disabled, the router assigns the Internet service provider's DNS servers to the DHCP clients. You can access these settings via ***Services > DNS Relay***.

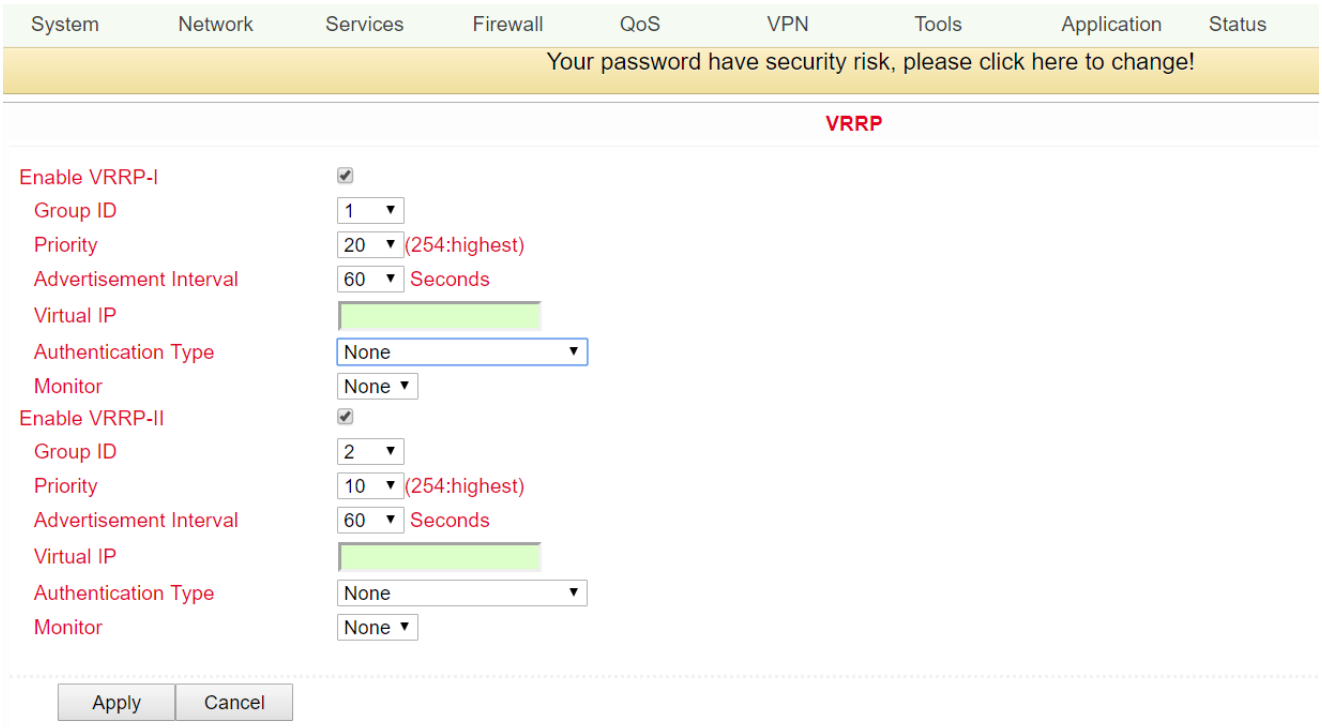



With the ***Add*** button up to 20 DNS-pais can be created.

| Name | Description | Standard |
|---|---|---|
| Enable DNS Relay | Click to enable DNS forwarding | Activated (after activation of DHCP) |
| Static (IP Address <-> Domain Name) Pairing (maximum 20 DNS Pairs) | | |
| IP Address | IP Address <-> Set DNS pairs | Empty |
| Host | Set names of IP-addresses<->DNS-Pairs | Empty |
| Description | Describe IP-Adresse<->DNS-Pairs | Empty |

## 3.3.3. VRRP

The Virtual Router Redundancy Protocol (VRRP) is a method for increasing the availability of important gateways in local networks through redundant routers. Several physical routers are combined into a logical group. This group of routers now presents itself in the network as a logical virtual router. For this purpose, a virtual IP address and a virtual MAC address are assigned to the logical router. One of the routers within the group is defined as the virtual master router, which then binds the virtual MAC and virtual IP addresses to its network interface and informs the other routers in the group that act as virtual backup routers. You can set up this function under ***Services > VRRP***.

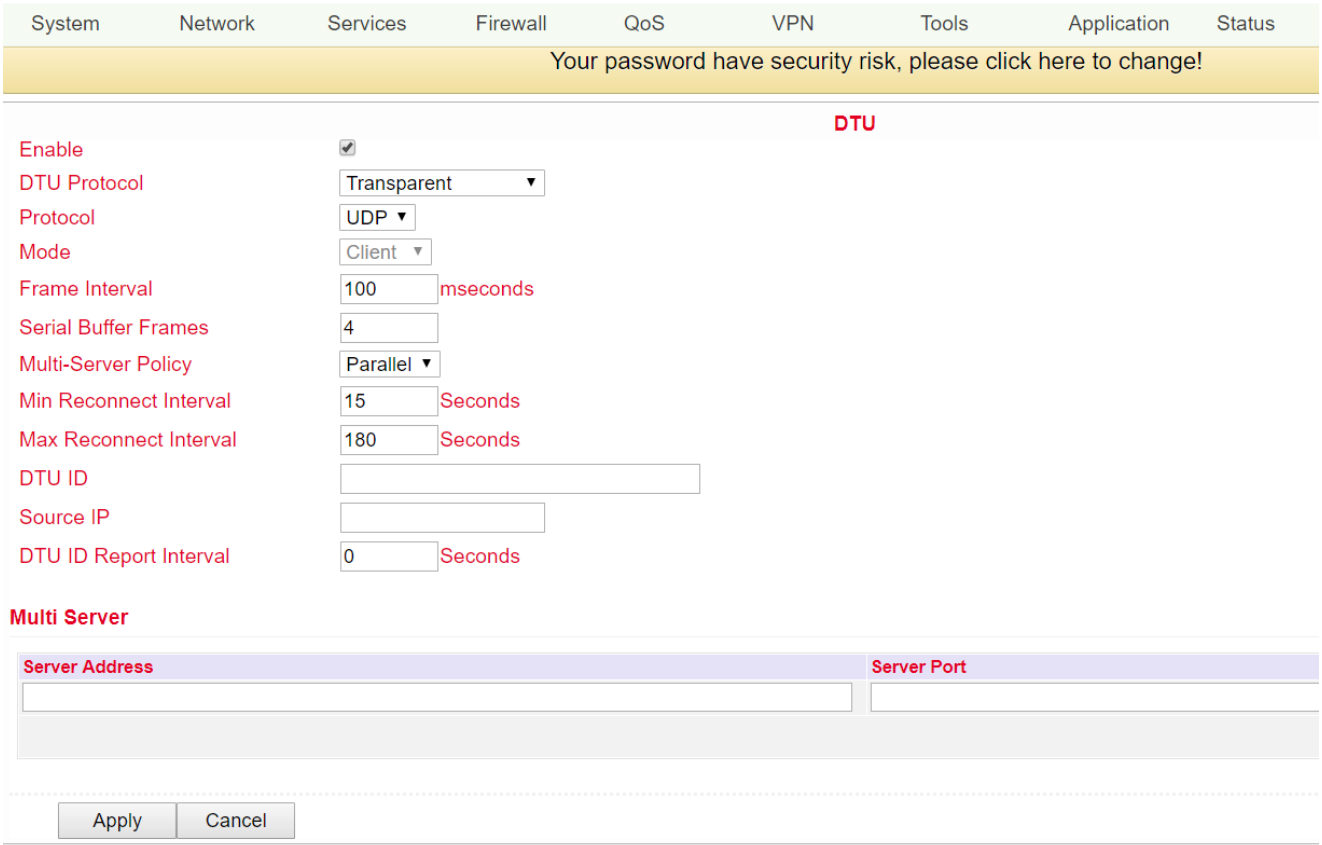



The TK500 Series offers the opportunity to build two different groups VRRP (VRRP I and VRRP II).

| Name | Description | Standard |
|---|---|---|
| Enable VRRP-I | Select to activate VRRP | Deactivated |
| Group ID | Select group ID for router (range 1-255) | 1 |
| Priority | Choose Priority for Router (range 1 - 254) | 20 (the larger the number, the higher the priority) |
| Advertisement Interval | Set display interval | 60 Seconds |
| Virtual IP | Set virtual IP for the group | Empty |
| Authentication Type | Optional: Typ „None/Password Authentication" | None. If Password Authentication is selected, a password can be assigned |
| Virtual MAC | Virtual MAC Address | Deactivated |
| Monitor | Checking the WAN connection | None |
| Enable VRRP-II | Select to activate VRRP | Deactivated |
| Group ID | Select group ID for router (range 1-255) | 2 |
| Priority | Choose Priority for Router (range 1 - 254) | 10 (the larger the number, the higher the priority) |
| Advertisement Interval | Set display interval | 60 Seconds |
| Virtual IP | Set virtual IP for the group | Empty |
| Authentication Type | Optional: Typ „None/Password Authentication" | None. If Password Authentication is selected, a password can be assigned |
| Virtual MAC | Virtual MAC Address | Deactivated |
| Monitor | Checking the WAN connection | None |

## 3.3.4. DTU

DTU stands for Data Terminal Unit and is used to connect devices with a serial interface (RS-232 and RS-485). You can create the configuration under ***Services > DTU***. When DTU is enabled, the console port is automatically disabled.



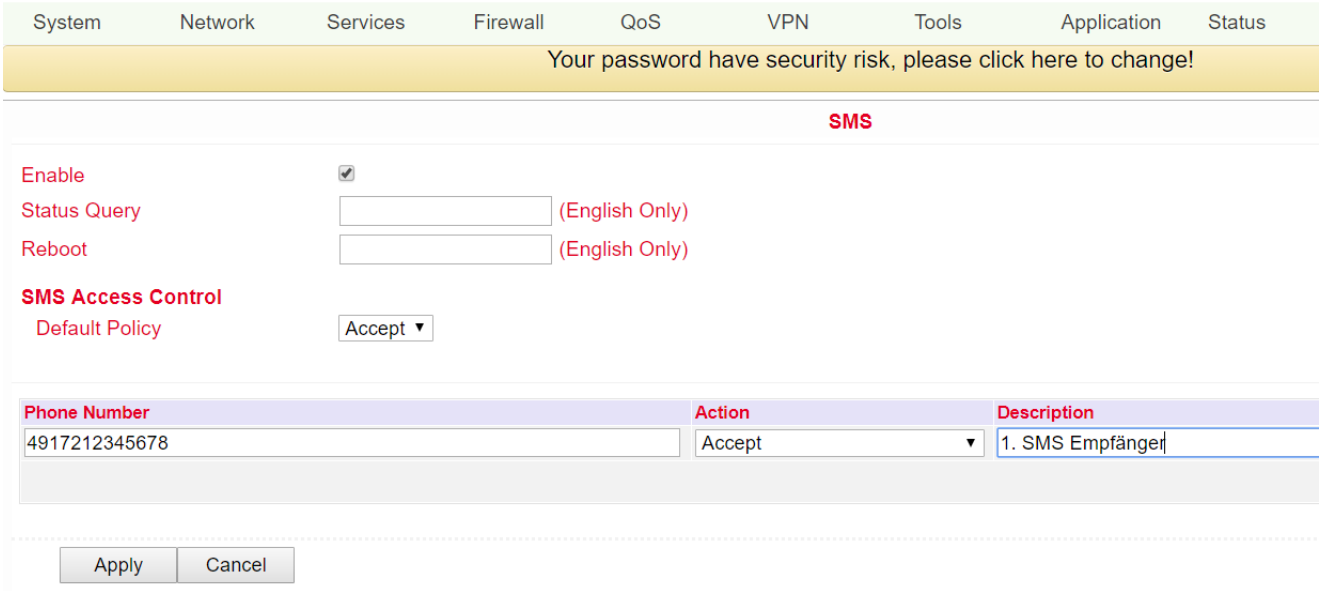

| Name | Description | Standard |
|---|---|---|
| Enable | Click to activate DTU protocol | Deactivated |
| DTU Protocol | Set DTU protocol | Transparent |
| Protocol | The options "TCP" and "UDP" are possible | UDP |
| Mode | Set DTU as client or server, depending on DTU protocol selection | Client |
| Frame Interval | Setting the frame interval in milliseconds | 100 msec |
| Serial Buffer Frames | Specification of buffer frames | 4 |
| Multi-Server Policy | Selection Parallel und Poll | Parallel |
| Min Reconnect Interval | Minimal Connection Intervall | 15 Sec |
| Max Reconnect Interval | Maximal Connection Intervall | 180 Sec |
| DTU ID | Specification of an ID for the DTU | Empty |
| Source IP | IP address of the source computer | Empty |
| DTU ID Report Interval | Time Interval for sending the DTU ID | 0 |
| Multi Server | | |
| IP-Adresse | Setting up an IP address for receiving data | Empty |
| Server Port | Setting up a server port for receiving data | Empty |

**Note**

The selection fields may vary depending on the selection of the DTU protocol.

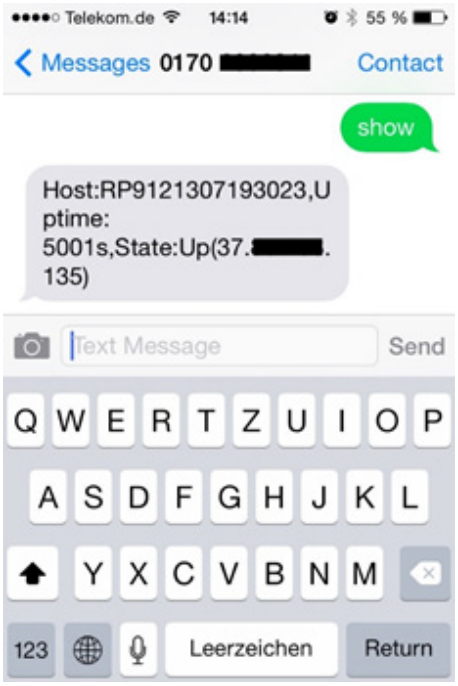
## 3.3.5. SMS

The TK500 can be reached via SMS from outside and reacts to various commands sent via SMS. You have the possibility to query the status of the device or to restart the device. The router is configured via ***Services > SMS***.




| Name | Description | Standard |
|---|---|---|
| Enable | Click to enable or disable SMS control | Deactivated |
| Status Query | Set Status request SMS to show the status of the router (e.g.: show status). | Empty |
| Reboot | Restarts the router (e.g. reboot) | Empty |
| SMS Access Control | | |
| Default Policy | Block or accept control SMS from a specific phone | Accept |
| Phone Number | Enter the phone numbers to send SMS to the router. The format for the mobile number is 491712345678 (please do not enter +49 or 0049) | Empty |
| Action | Setting of Allow (Accept) or Block (Block) of the previously entered phone number | Accept |
| Description | Description for the created data record | Empty |

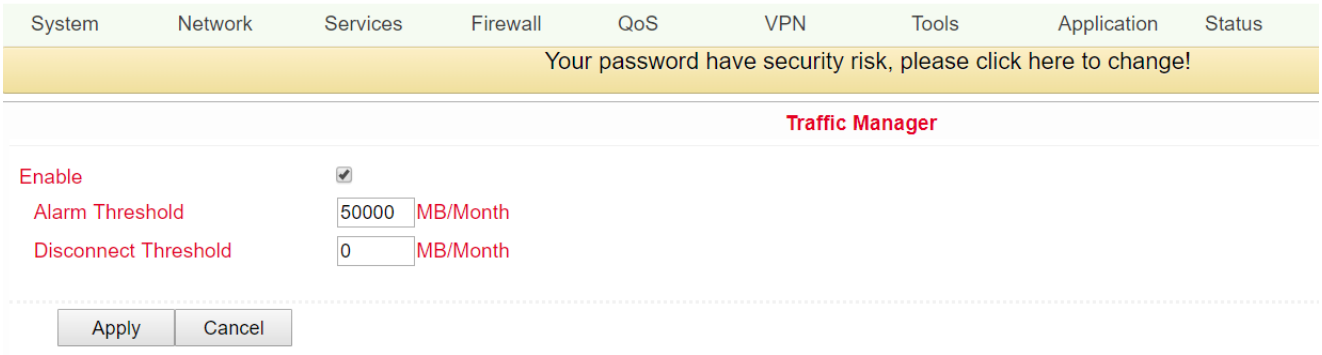
To send an SMS to the router, the mobile number of the inserted card must be known. Then the SMS is sent to it.




SMS that you receive on your mobile phone:
Host: (SN);
Uptime: (the operating time of the router at the time of this reboot);
State: (Online/Offline) (Wireless WAN IP)
LAN: (Ready) (LAN-IP)

## 3.3.6. Traffic Manager

The Traffic Manager can be used to provide the data consumption of the dial-up connection interface. You can configure this service under ***Services > Traffic Manager***.

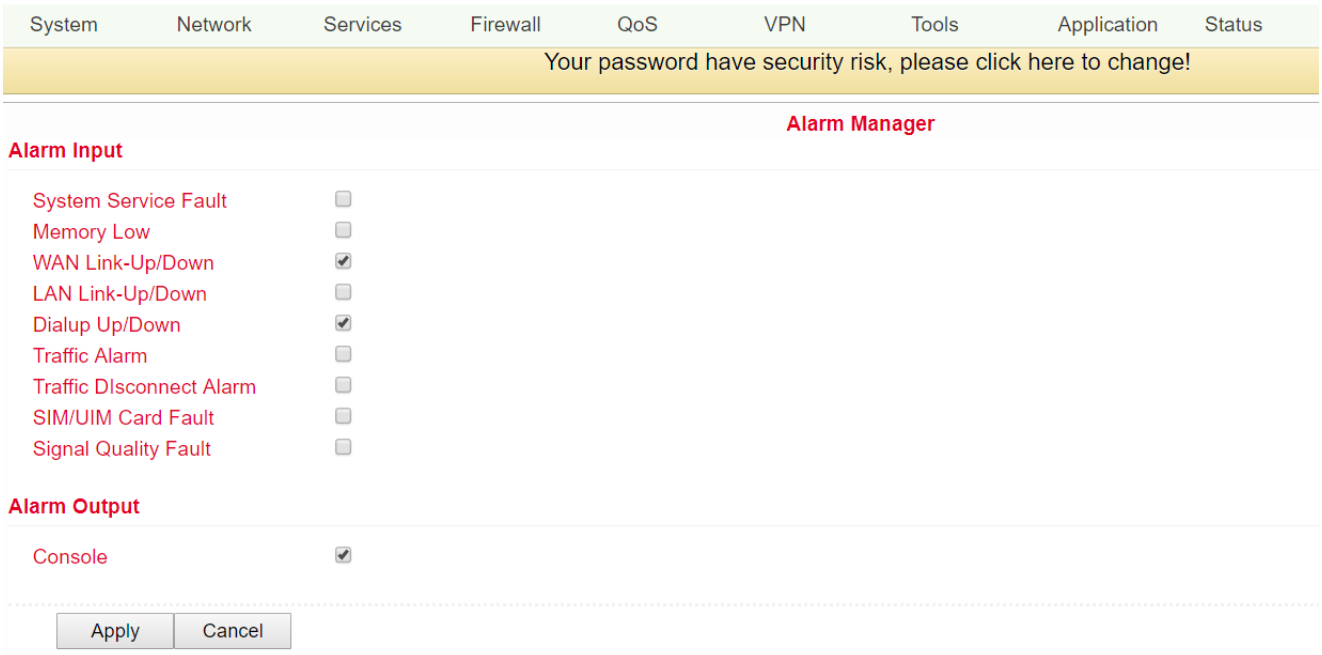



| Name | Description | Standard |
|---|---|---|
| Enable | Click to activate or deactivate SMS Control | Deactivated |
| Alarm Threshold | Defines the amount of data in MB per month for which an alarm is to be generated. If 0 is set as value, no alarm is generated. | Empty |
| Disconnect Threshold | If the set value is reached, the dial-up connection is interrupted. | Empty |

The amount of data used can be checked at any time under the Traffic Statistic (see 3.8.3)

## 3.3.7. Alarm Manager

The Alarm Manager can be used to generate various alarms. You can configure this option under ***Services > Alarm Manager***.



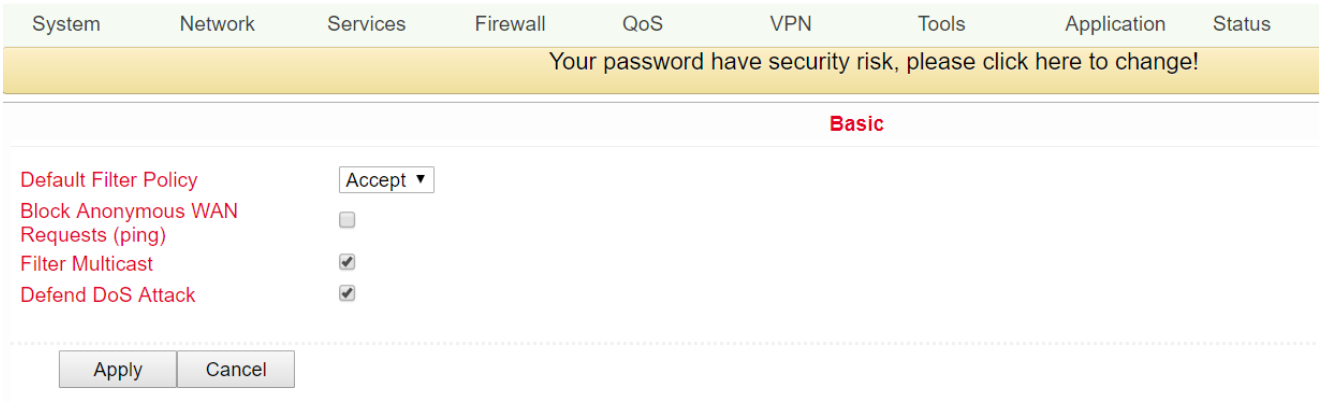

| Name | Description | Standard |
|---|---|---|
| Alarm Input | Here you select the areas for which an alarm is to be generated. | none |
| Alarm Output | Here you can select, whether the alarms should or should not be output via the console. | selected |

# 3.4. Firewall

Via the ***Firewall*** menu item you can set the parameters for the firewall of the router. Various settings are possible here.

## 3.4.1. Basic

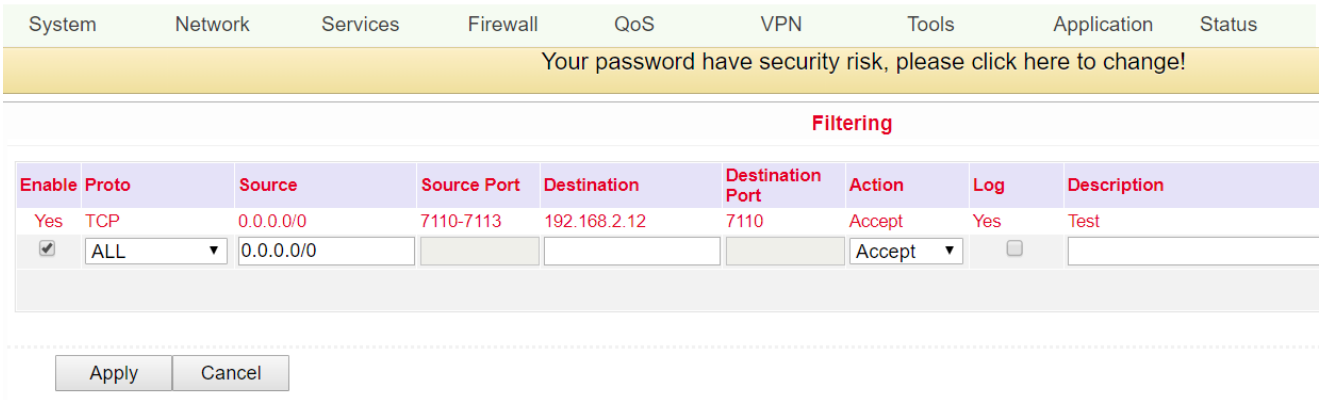
Here you can configure the basic settings of the firewall.




| Name | Description | Standard |
|---|---|---|
| Default Filter Policy | The options „Accept“ and „Block“ are possible | Allow |
| Block Anonymous WAN Request (ping) | Activate to block ping requests that are generated anonymously from the network. | Deactivated |
| Filter Multicast | Click to enable multicast filtering | Enabled |
| Defend DoS Attack | Click to enable blocking of DoS attacks | Enabled |

## 3.4.2. Filtering

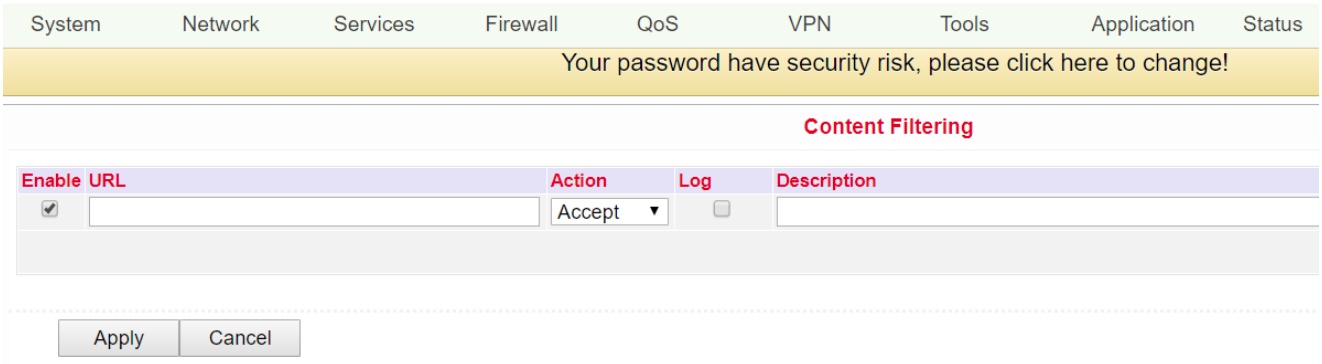
At this point you can filter what you want the firewall to let through and what not. Various configurations are possible here, which you can access via ***Firewall > Filtering***.



| Name | Description | Standard |
|---|---|---|
| Enable | Click to enable filtering | Enabled |
| Proto | Selection of the protocol. The options "TCP"/"UD-P"/"ICMP" are possible. | All |
| Source | Set source IP address | Empty |
| Source Port | Set source port if appropriate protocol is selected | Empty |
| Destination | Set Target IP | Empty |
| Destination Port | Set destination port if appropriate protocol is selected | Empty |
| Action | Selection whether setting should be allowed (Accept) or blocked (Block) | Accepted |
| Log | Click to enable logging of the setting | Deactivated |
| Description | Describe Configuration | Empty |

## 3.4.3. Content Filtering

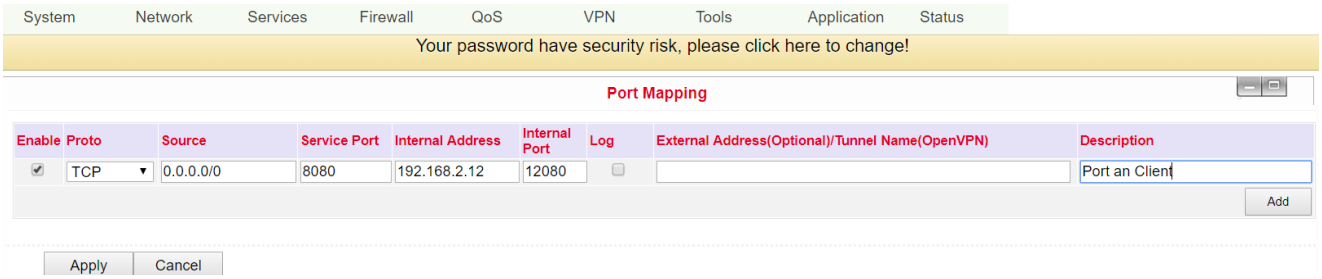
The content filter in the firewall allows to filter the call of special URL´s, which can then be blocked or allowed. You can create the configuration under ***Firewall > Content Filtering***.




| Name | Description | Standard |
|---|---|---|
| Enable | Activating or deactivating the content filter function | Enabled |
| URL | Enter the URL to be blocked or filtered | Empty |
| Action | Selection whether URL is blocked (block) or allowed (accept) | Accepted |
| Log | Can be activated for logging | Deactivated |
| Description | Describe Configuration | Empty |

## 3.4.4. Port Mapping

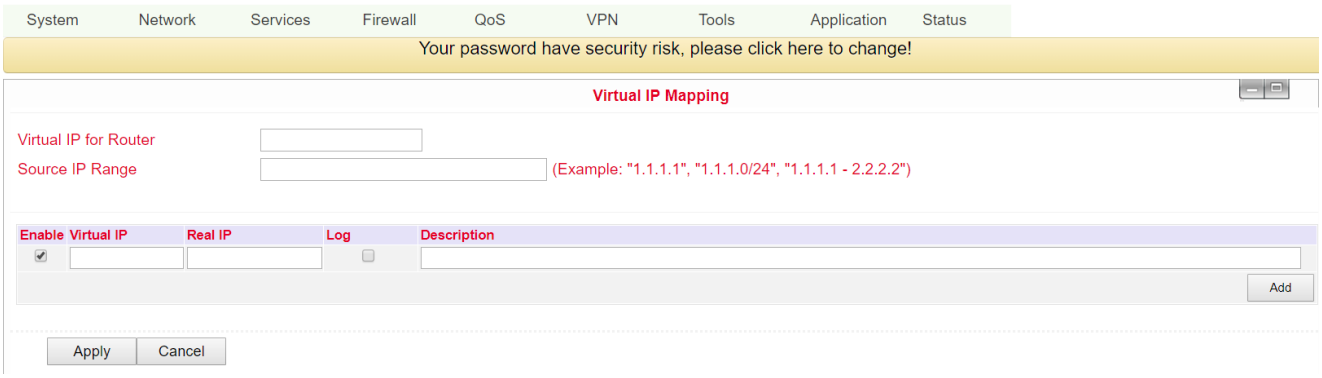
NAT-PMP (NAT Port Mapping) allows a computer on a private network (behind a NAT router) to automatically configure the router so that devices behind the router are accessible from outside the private network. It essentially regulates the so-called port forwarding. NAT-PMP, like UPnP, and allows a program to request all externally incoming data on a specific TCP or UDP port. You can perform the configuration under ***Firewall > Port Mapping***.




| Name | Description | Standard |
|---|---|---|
| Enable | Enable or disable port assignment | Enabled |
| Proto | Selection of the protocols TCP, UDP or TCP&UDP | TCP |
| Source | Quell-IP eintragen | 0.0.0.0/0 |
| Service Port | Enter the Port of the service | 8080 |
| Internal Address | Set internal IP for assignment | Empty |
| Internal Port | Set port mapping to "internal | 8080 |
| Log | Click to enable Port mapping logging | Deactivated |
| External Address (Optional) / Tunnel Name (OpenVPN) | Used in conjunction with VPN. For port forwarding with VPN, the virtual VPN IP address of the TC router must be entered here. | Empty |
| Description | Describe the meaning of the individual assignments | Empty |

## 3.4.5. Virtual IP Mapping

The IP of an internal PC can be assigned to a virtual IP. An external network can access the internal PC via this virtual IP address. You can set up this configuration in ***Firewall > Virtual IP Mapping***.



| Name | Description | Standard |
|---|---|---|
| Virtual IP for Router | Set virtual IP for router | Empty |
| Source IP Range | Set range of source IP addresses | Empty |
| Virtual IP | Set virtual IP | Empty |
| Real IP | Set real IP | Empty |
| Log | Enable logging for virtual IP | Deactivated |
| Description | Describe Configuration | Empty |

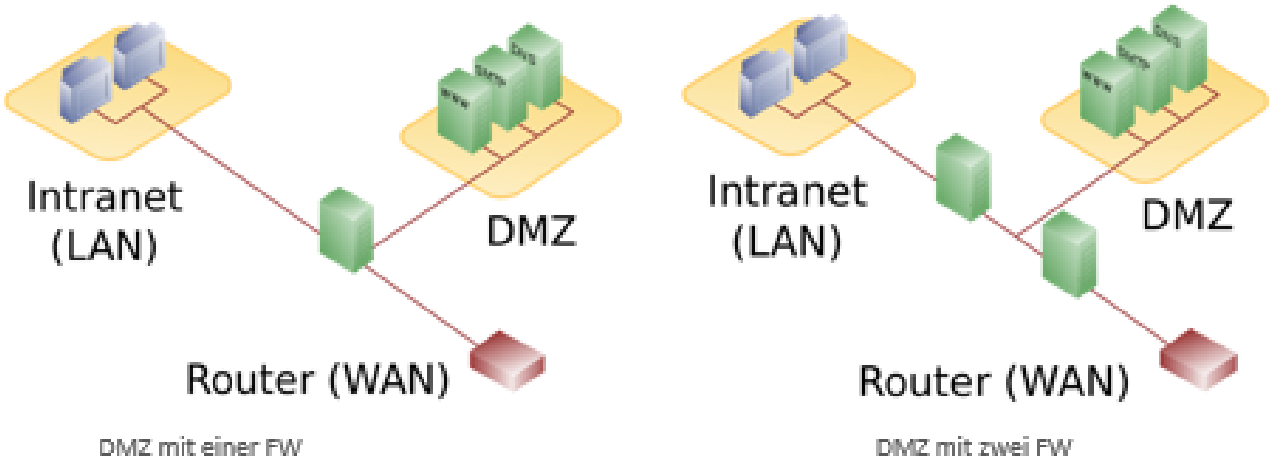
## 3.4.6. DMZ

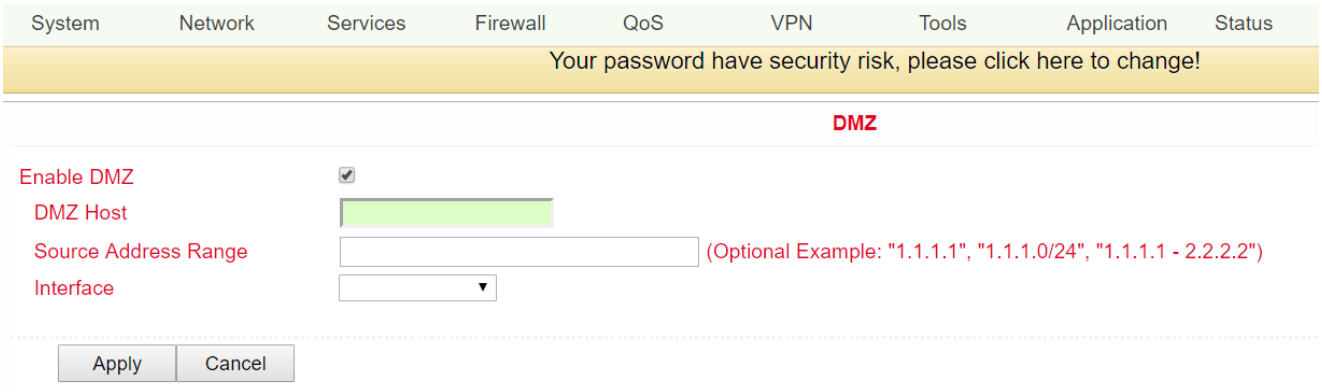
A demilitarized zone ***(DMZ)*** is a computer network with security controlled access to the connected servers.

The systems set up in the DMZ are shielded from other networks (e.g. Internet, LAN) by one or more firewalls. This separation allows access to publicly available services and at the same time protects the internal network (LAN) from unauthorized external access.

The purpose is to provide services of the computer network to both the Internet (WAN) and the Intranet (LAN) on the most secure basis possible.

A DMZ provides protection by isolating one system from two or more networks.




By assigning all ports and the external PC, you can access all ports of the device connected to the TK500.

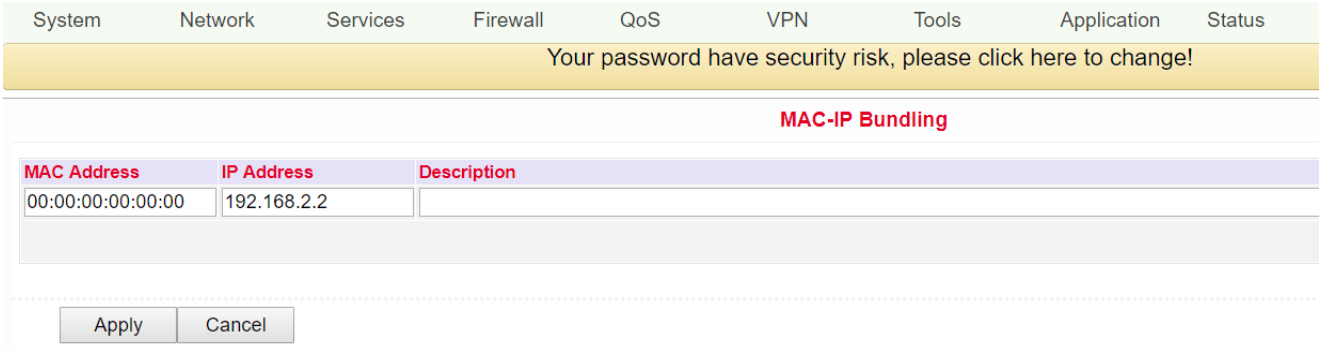
**Note**

With this function it is not possible to assign the management port of the TK500 (e.g.: 80 TCP) to the port of the device. To forward port 80, change the router's management port in ***System > Admin Access***.

| Name | Description | Standard |
|---|---|---|
| Enable DMZ | Click to activate DMZ | Deactivated |
| DMZ Host | Set DMZ host IP | Empty |
| Source Address Range | Set IP address with restricted IP access | Empty |
| Interface | Auswahl des entsprechenden Interfaces | Empty |

## 3.4.7. MAC-IP Bundling

MAC IP Bundling means assigning a predefined IP address to a defined MAC address. Thus the given MAC address always gets the same IP address. You reach this menu item under ***Firewall > MAC-IP Bundling***.




If a firewall blocks all access to the external network, only PCs with MAC-IP bundling have access to the external network.

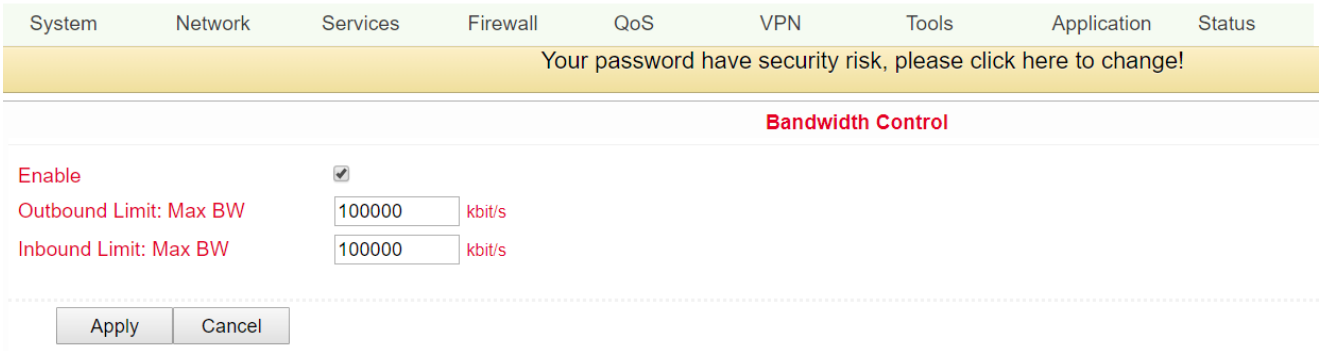
| Name | Description | Standard |
|---|---|---|
| MAC Address | Set MAC address for bundling | Empty |
| IP Address | Specify IP address for bundling | 192.168.2.2 |
| Description | Describe configuration | Empty |

# 3.5. QoS

In the TCP/IP world, QoS describes the quality of a communication service from the user's point of view. The network service quality is often defined by the parameters bandwidth, delay, packet loss and jitter.
The network load influences the quality of the transmission. For example, how long does it take for a data packet to reach the recipient? For this reason, an attempt is made to identify data packages with corresponding service classes. Prioritized data packets are then preferably forwarded in routers or switches. In the TK 500 series it is therefore possible to limit and allocate the bandwidths accordingly. You can set this up via „***QoS***".

## 3.5.1. Bandwidth Control

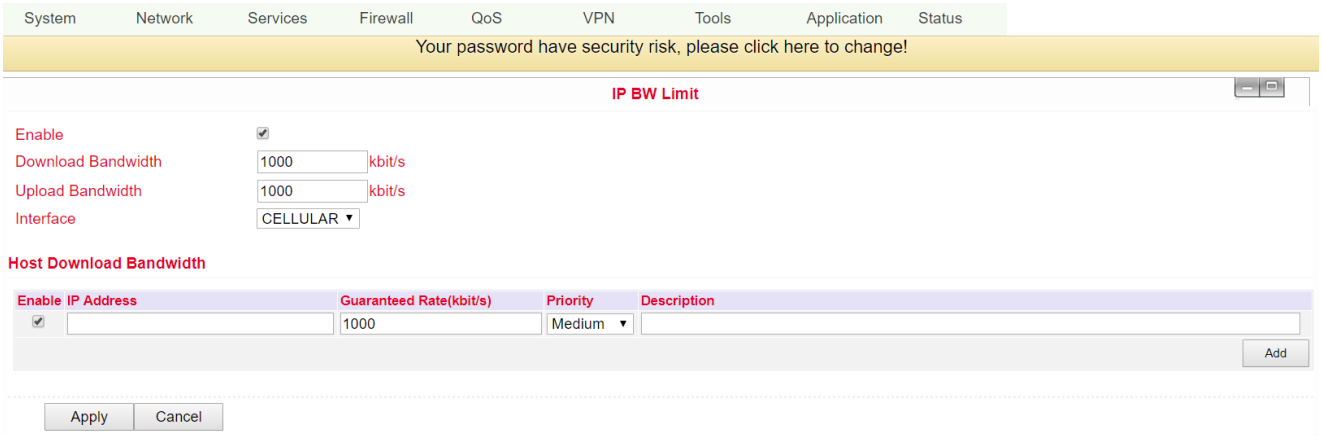
Here you can limit the bandwidth inbound or outbound. This can be configured under ***QoS > Bandwith Control***.




| Name | Description | Standard |
|---|---|---|
| Enable | Click to activate | Deactivated |
| Outbound Limit Max BW | Setting Outbound Bandwidth Limits | 100000 kbps |
| Inbound Limit Max BW | Set incoming bandwidth limit | 100000 kbps |

## 3.5.2. IP BW Limit

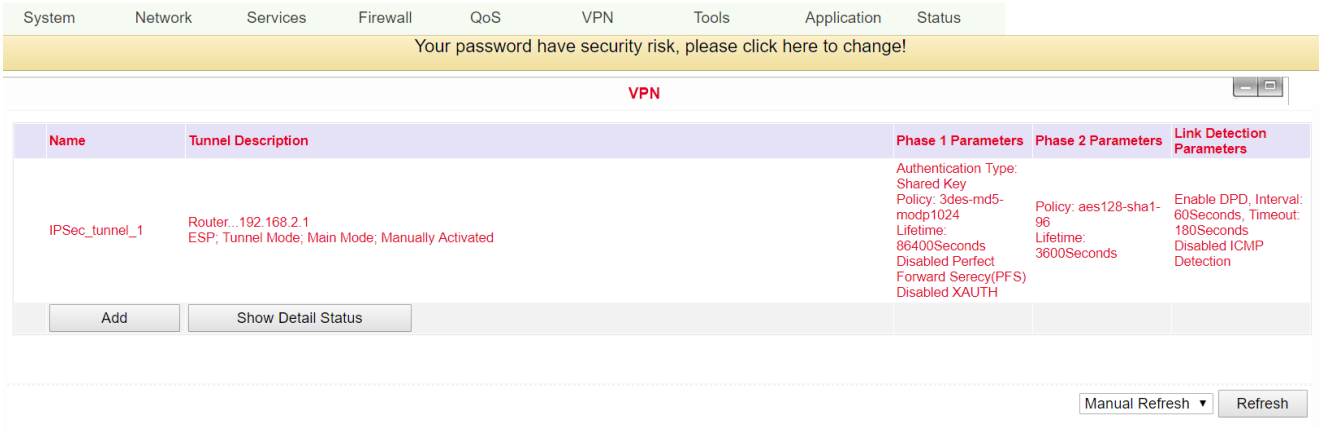
Under the menu item ***QoS > IP BW Limit*** you can limit the download or upload bandwidth and bind it to IP addresses and then prioritize them.



| Name | Description | Standard |
|---|---|---|
| Enable | Click to activate | Deactivated |
| Download Bandwith | Specifying the bandwidth for the download | 1000 kbps |
| Upload Bandwith | Setting the bandwidth for the upload | 1000 kbps |
| Interface | Selection of the interface to which the bandwidth is to be assigned | Cellular |
| Host Download Bandwidth | | |
| Enable | Activating the function | Enabled |
| IP Adresse | Specification of the IP address for the assignment | Empty |
| Guaranteed Rate (kbit/s) | Indication of the guaranteed bandwidth in kbit/s | 1000 |
| Priority | Assignment of priority | Medium |
| Description | Description of the rule | Empty |

# 3.6. VPN

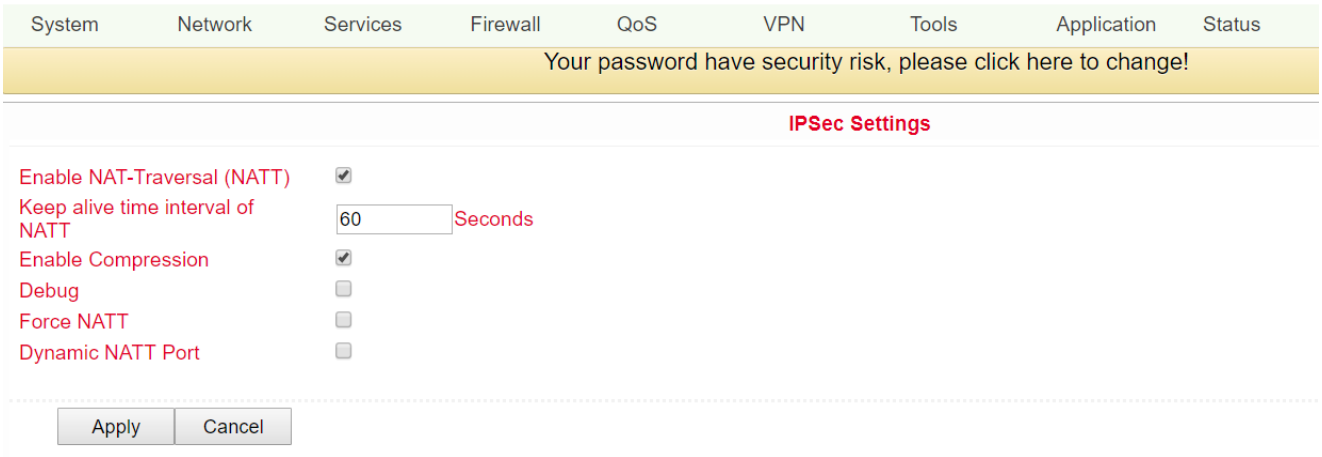
A VPN (Virtual Private Network) is a closed logical network in which the subscribers are spatially separated from each other and connected via an IP tunnel. With this VPN you can access a local network, e.g. the company network, on the road or from your home office. This requires VPN software that communicates with the router of the network and is installed on the computer with which you want to access the network. There are different types of VPN connections (tunnels) that can be configured in this menu item for the TK500 series.




Overview of existing VPN connections. With ***Add*** a new tunnel can be created, see 3.6.2.

## 3.6.1. IPSec Settings

In this menu item you configure the settings for the IPSec, which can be accessed via ***VPN > IPSec Settings***.




| Name | Description | Standard |
|---|---|---|
| Enable NAT-Traversal (NATT) | Click to enable | Deactivated |
| Keep alive time interval of NATT | Determining the duration for the maintenance of NATT | 60 Seconds |
| Enable Compression | Switch compression on/off | Enabled |
| Debug | Switch debug mode on or off | Deactivated |
| Enable | Activating the function | Enabled |
| Force NATT | Forcing NATT on/off | Deactivated |
| Dynamic NATT Port | Switching a dynamic NATT Port on or off | Deactivated |

The change of address via NAT is evaluated by a VPN gateway as a security-critical change of the data packets, the VPN negotiation fails, no connection is established. These problems occur, for example, when dialing in via some UMTS mobile networks where the network operator's servers do not support address conversion in connection with IPSec-based VPNs.

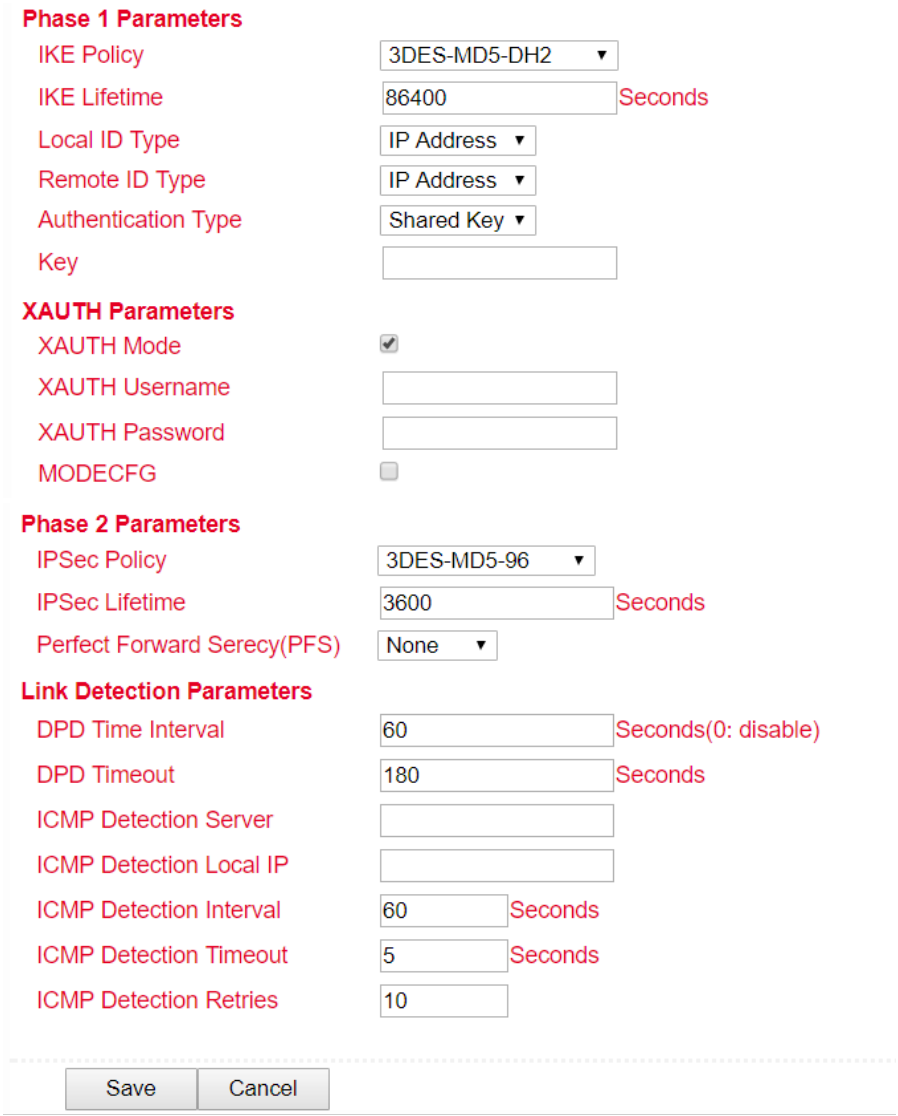
In order to successfully establish a VPN connection in these cases, NATT (NAT Traversal) provides a method to overcome these problems when handling data packets with changed addresses.

**Note**

NATT can only be used for VPN connections that use ESP (Encapsulating Security Payload) for authentication. Unlike AH (Authentication Header), ESP does not take the IP header of the data packets into account when determining the hash value for authentication. The hash value calculated by the recipient therefore corresponds to the hash value entered in the packets.

## 3.6.2. IPSec Tunnels

Construct the corresponding tunnel under ***VPN > IPSec Tunnels***.



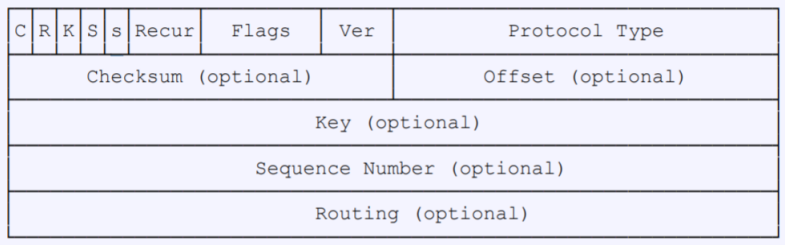

On this page the web-based parameters for the TK500 are presented.

| Name | Description | Standard |
|---|---|---|
| Show Advanced Options | Click to activate advanced options | Deactivated |
| Basic Parameters | | |
| Tunnel Name | Name for the tunnel | IPSec_tunnel_1 |
| Destination Address | Specifying the destination address of the IPSec VPN server | Empty |
| Startup Modes | Possible modes are "Auto Activa-te"/"Triggered by Data"/"Passive"/"-Manually Activated". | Enabled |
| Restart WAN when failed | WAN interface is restarted in case of failed tunnel construction. | Enabled |
| Negotiation Mode | Optional: „Main Mode“ or „Aggressive Mode“ | Main Mode |
| IPSec Protocol | Optional: „ESP“ orr „AH“ | ESP |
| IPSec Mode | Optional: „Tunnel Mode“ or „Transport Mode“ | Tunnel Mode |
| VPN over IPSec | LT2P oder GRE over IPsec | None |

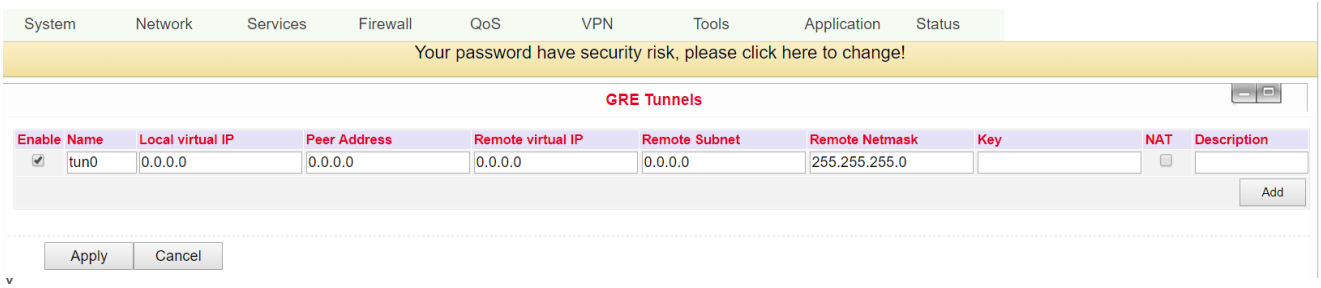
| | | |
|---|---|---|
| Tunnel Type | Selection field for various setting options | Subnet – Subnet Mode |
| Local Subnet | Set Protected IPSec Subnet (Local) | 192.168.2.1 |
| Local Netmask | Set Protected IPSec Subnet Mask (Local) | 255.255.255.0 |
| Remote Subnet | Setting a Protected IPSec Subnet (Remote) | 0.0.0.0 |
| Remote Netmask | Set protected IPSec subnet mask (remote) | 255.255.255.0 |
| Phase 1 Parameters | | |
| IKE Policy | Multi-selection list for the policy | 3DES-MD5-96 |
| IKE Lifetime | Set IKE validity period | 86400 Seconds |
| Local ID Type | Selection of "FQDN", "USERFQDN" or "IP address" possible | IP Address |
| Remote ID Type | Selection of "IP address", "User FQDN" or "FQDN" possible | IP Address |
| Authentication Type | Selection of "Shared Key" or "Certificate" possible | Shared Key |
| Key (bei Auswahl des Authentifizierungstyps „Shared Key“) | Set IPSec key for VPN negotiation | Empty |
| XAUTH Parameters | | |
| XAUTH Mode | Enable XAUTH | Deactivated |
| XAUTH Username | XAUTH Username | Empty |
| XAUTH Password | XAUTH Password | Empty |
| MODECFG | Enable MODECFG | Deactivated |
| Phase 2 Parameters | | |
| IPSec Policy | Multi-selection list for the policy | 3DES-MD5-96 |
| IPSec Lifetime | Set IPSec validity period | 3600 Sekunden |
| Perfect Forward Secrecy (PFS) | Optional: „Disable“, „GROUP1“, „GROUP2“, „GROUP5“ | Deactivated (Enable advanced options) |
| Link Detection Parameters | | |
| DPD Time Interval | Set DPD time Interval | 60 Seconds |
| DPD Timeout | Set DPD timeout | 180 Seconds |
| ICMP Detection Server | Specify server for ICMP detection | Empty |
| ICMP Detection Local IP | Set local IP for ICMP | Empty |
| ICMP Detection Interval | Set interval for ICMP Detection | 60 Seconds |
| ICMP Detection Timeout | Set timeout for ICMP Detection | 5 Seconds |
| ICMP Detection Max Retries | Setting the Maximum Number of Repetitions for ICMP Detection | 10 |

## 3.6.3. GRE Tunnels

Generic Routing Encapsulation (GRE) is a network protocol developed by Cisco and defined in RFC 1701. Via GRE other protocols can be packed and transported in an IP tunnel. GRE uses the IP protocol 47, the GRE header is structured as follows:



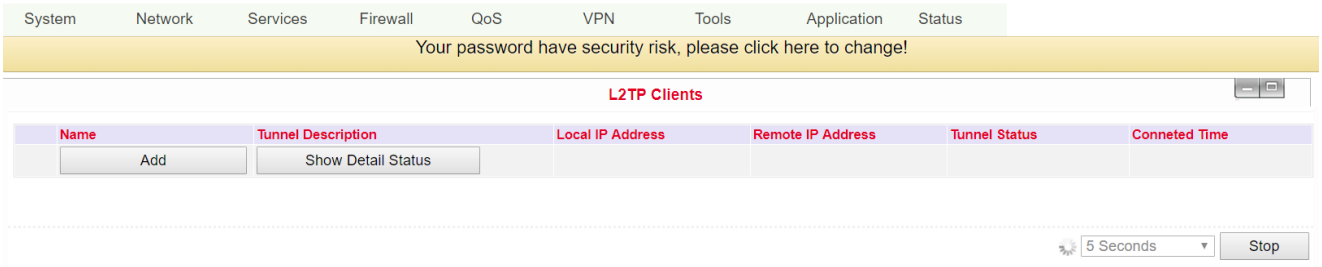

A GRE package consists of an IP-Header, a GRE-Header and the actual payload. You can set up this GRE tunnel under ***VPN > GRE Tunnels***.



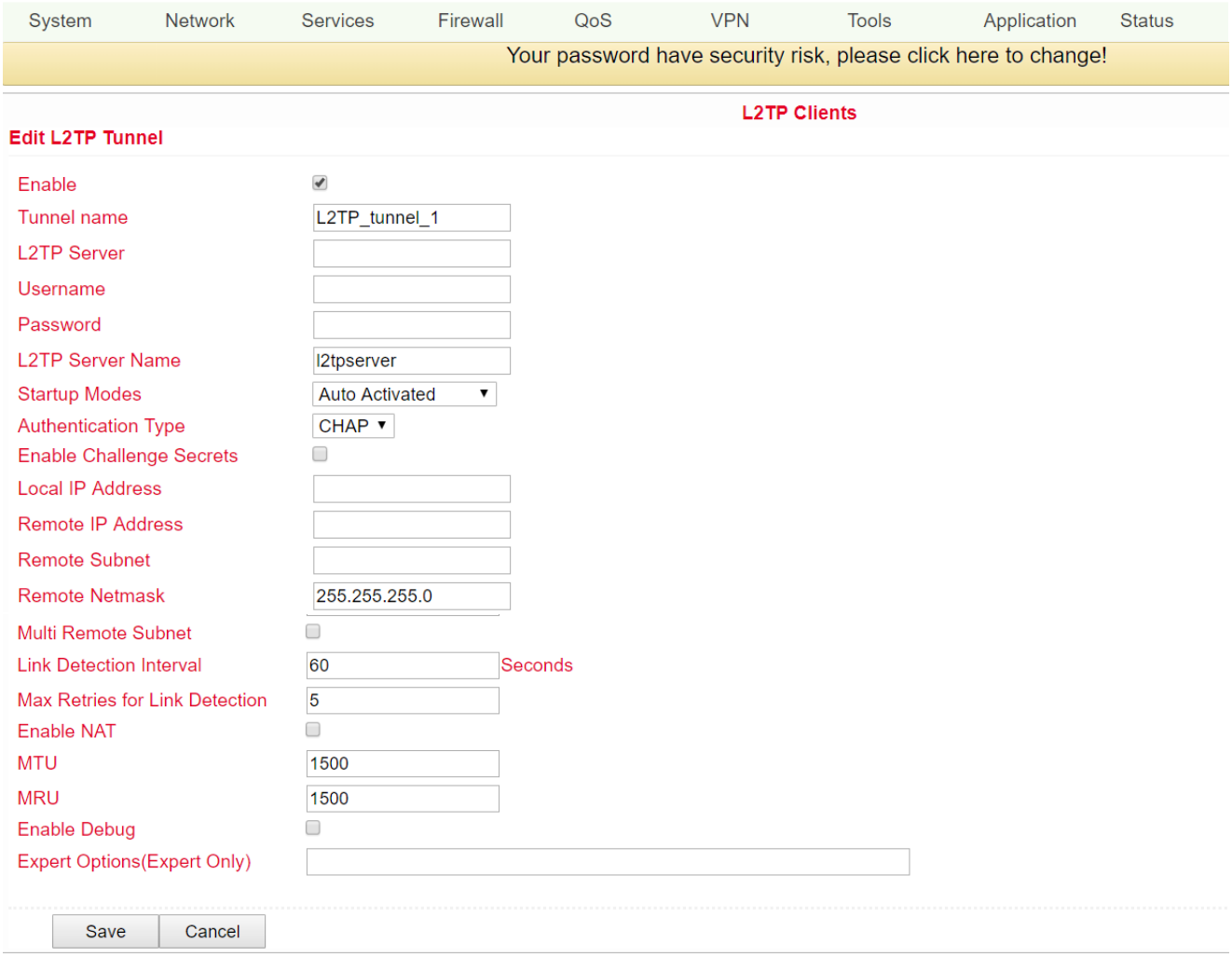

| Name | Description | Standard |
|---|---|---|
| Enable | Click to enable | Enabled |
| Tunnel Name | Define names for GRE tunnels | tun0 |
| Local Virtual IP | Set local virtual IP | 0.0.0.0 |
| Peer Address | Set peer address | 0.0.0.0 |
| Remote Virtual IP | Specifying the virtual IP of the remote network | 0.0.0.0 |
| Remote Subnet Address | Set Remote Subnet Address | 0.0.0.0 |
| Remote Subnet Netmask | Defining a Remote Subnet Mask | 255.255.255.0 |
| Key | Define the key for encrypting the tunnel | Empty |
| NAT | Click to enable NAT function | Deactivated |
| Description | Add Description | Empty |

## 3.6.4. L2TP Clients

Layer 2 Tunneling Protocol (L2TP) is a network protocol that tunnels frames of OSI model backup layer protocols through routers between two networks over an IP network. L2TP routers and the IP connections between them appear as L2 switches. The L2TP client establishes the connection to the L2TP server. You reach the configuration via ***VPN > L2TP Clients***.




By clicking the ***Add*** button you start the configuration of the L2TP client.

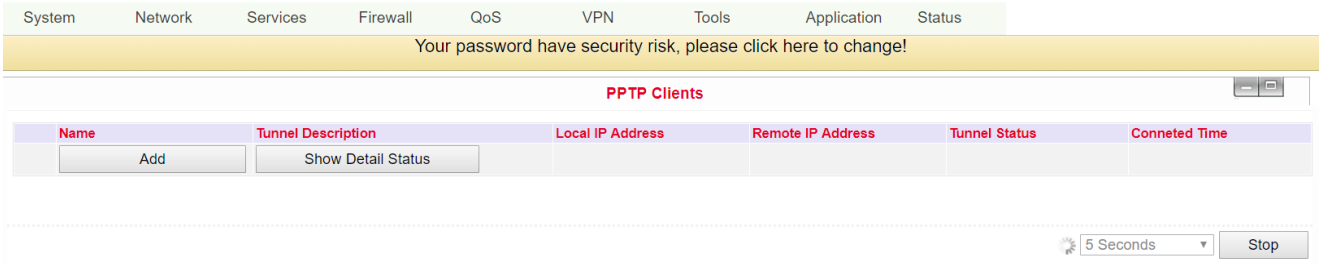



| Name | Description | Standard |
|---|---|---|
| Enable | Enables the tunnel settings | Enables |
| Tunnel Name | Define Tunel Name | L2TP_TUNNEL_1 |
| L2TP Server | Enter the address of the L2TP Server | Empty |
| Username | Set Username for Server | Empty |

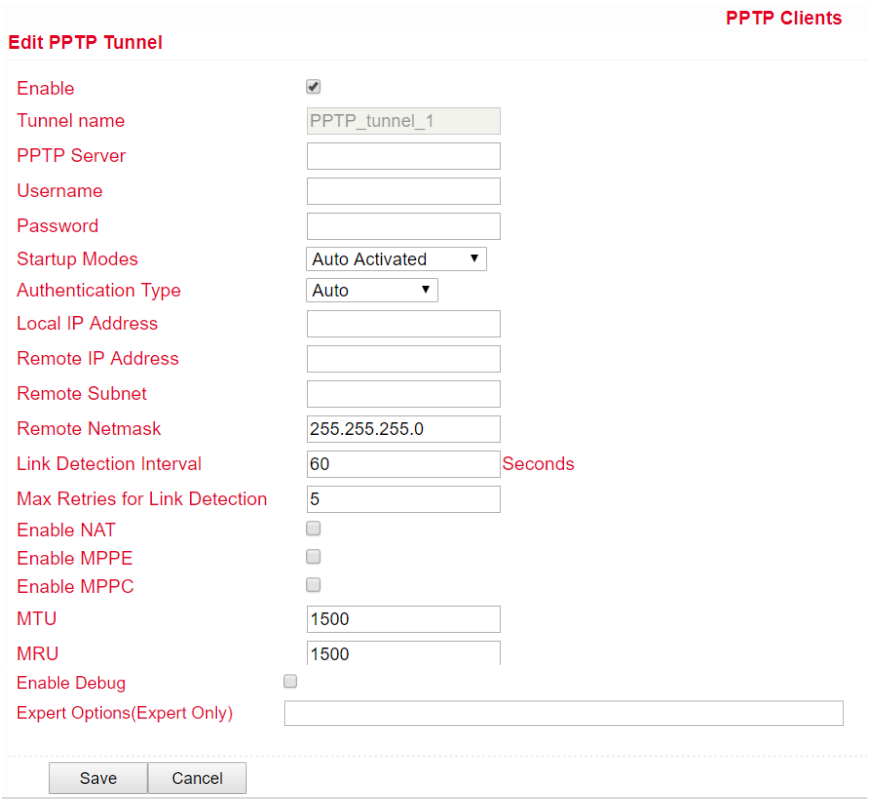
| | | |
|---|---|---|
| Password | Set Password for Server | Empty |
| L2TP Server Name | Define names for Servers | l2tpserver |
| Startup Modes | Set start modes: "Auto Activated", "Triggered by Data", "Manually Activated", "L2TPOverIP-Sec". | Auto Activated |
| Authentication Type | Set the authentication type: "CHAP", "PAP". | CHAP |
| Enable Challenge Secrets | To activate secret keys (Challenge) select | Deactivated |
| Challenge Secrets | If Enable Challenge Secrets is activated, the secret key can be entered here | Empty |
| Local IP Address | Set local IP address | Empty |
| Remote IP Address | Set Remote IP address | Empty |
| Remote Subnet | Set a Remote Subnet | Empty |
| Remote Subnet Netmask | Define a Remote Subnet Mask | 255.255.255.0 |
| Link Detection Interval | Set Interval for connection detection | 60 |
| Max Retries for Link Detection | Setting the Maximum Number of Repetitions for Connection Detection | 5 |
| Enable NAT | Click to enable NAT | Deactivated |
| MTU | Set MTU parameters | 1500 |
| MRU | Set MRU parameters | 1500 |
| Enable Debug Mode | Click to activate debug mode | Deactivated |
| Expert Options | Set Expert options | Empty |

## 3.6.5. PPTP Clients

PPTP (Point to Point Tunneling Protocol) is a VPN tunneling procedure for remote access connections. It is based on the Remote Access Server for Microsoft Windows NT including authentication. A PPTP client is not only integrated in Windows, but also in Linux and MacOS. Set up the PPTP client under ***VPN > PPTP Clients***.




To set up a new PPTP client, click the Add button. To view details of an existing PPTP client, please click on the ***Show Detail Status*** button. Once you have clicked on the ***Add*** button, you can make the following configuration settings.

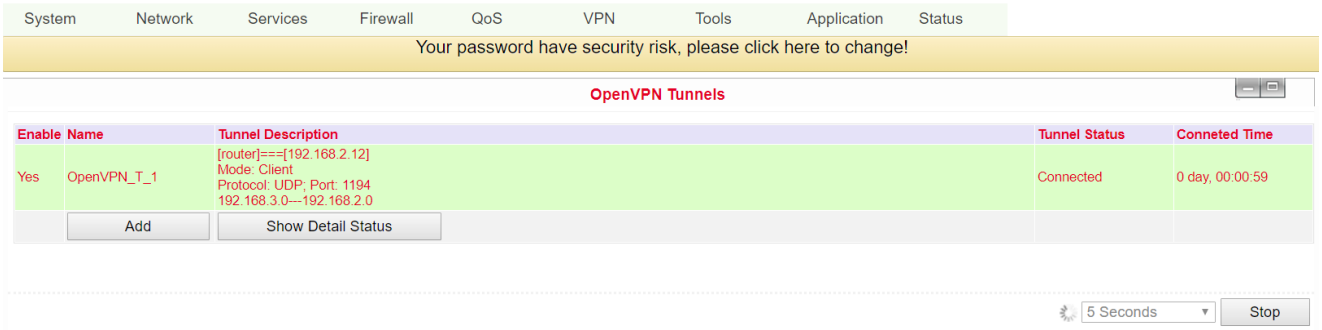



| Name | Description | Standard |
|---|---|---|
| Enable | Click to enable | Enabled |
| Tunnel Name | The name for the tunnel (set automatically) | PPTP_tunnel_1 |
| PPTP Server | Specify Address for PPTP Server | Empty |
| Username | Set Username for Server | Empty |
| Password | Set Password for Server | Empty |
| Startup Mode: | Set start modes "Auto Activated", "Triggered by Data", "Manually Activated". | Auto Activated |
| Authentication Type | Set authentication type: "PAP", "CHAP", "MS-CHAPv1", "MS-CHAPv2 | Auto |
| Local IP Address | Set local IP-address | Empty |
| Remote IP Address | Set Remote IP-address | Empty |
| Remote Subnet | Defining a Remote Subnet Mask | Empty |
| Remote Subnet Net-mask | Defining a Remote Subnet Mask | 255.255.255.0 |
| Link Detection Interval | Setting the connection detection interval | 60 |
| Max Retries for Link Detection | Set the Maximum Number of Repetitions for Connection Detection | 5 |
| Enable NAT | Click to enable NAT | Empty |
| Enable MPPE | Click to enable MPPE (Microsoft Point to Point Encryption) | Empty |
| Enable MPPC | Click to enable MPPC (Microsoft Point to Point Compression) | Empty |
| MTU | Set MTU parameters | 1500 |
| MRU | Set MRU parameters | 1500 |
| Enable Debug Mode | Click to enable Debug Mode | Empty |
| Expert Options | Only for Welotec R&D | Empty |

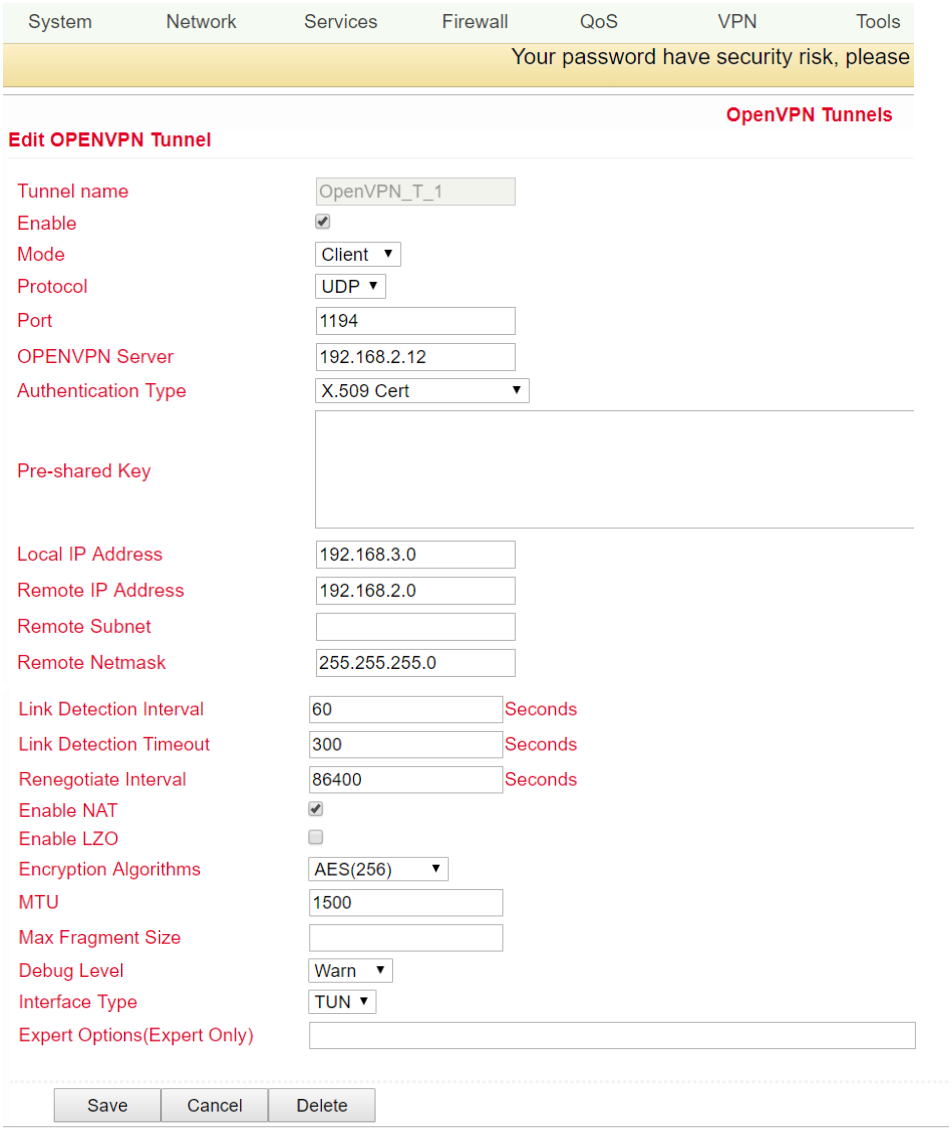
## 3.6.6. OpenVPN Tunnels

OpenVPN is free software for setting up a Virtual Private Network (VPN) via an encrypted TLS connection. The OpenSSL library is used for encryption. OpenVPN uses either UDP or TCP for transport.

OpenVPN is under the GNU GPL and supports operating systems such as Linux, Windows, iOS and a variety of customized Linux-based devices, such as routers of the TK 500 and TK 800 series.
Choose the options ***VPN > Open VPN Tunnels***, on the configuration page of the TK500, as shown below:



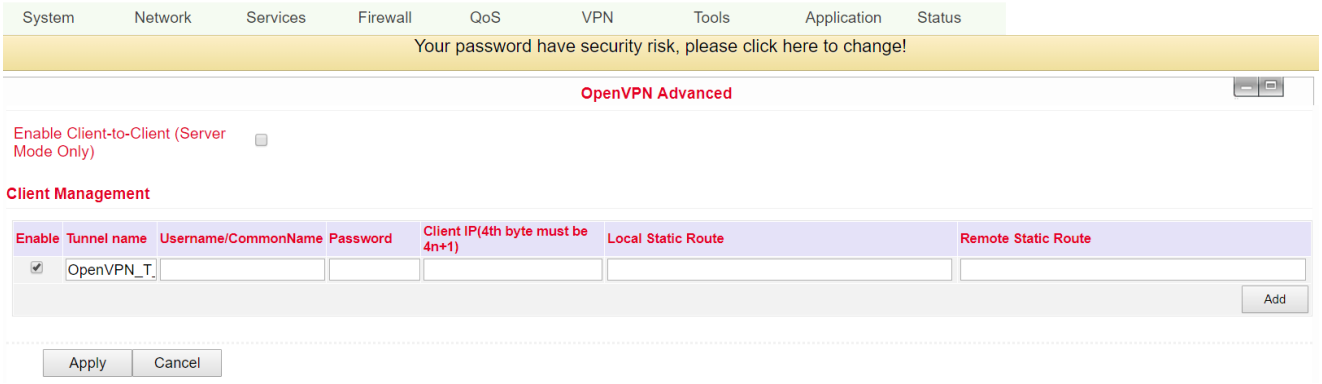

Click ***Add*** to add a new OpenVPN tunnel. With ***Show Detail Status*** you can view the status of an already configured OpenVPN tunnel.



| Name | Description |
|---|---|
| Tunnel name | Given |
| Enable | Activate this configuration |
| Mode | "Select "Client" or "Server" mode |
| Protocol | Selection of the "UDP" or "TCP" protocol |
| Port | Standard port for OpenVPN is 1194 |
| OPENVPN Server | IP or DNS of OpenVPN-Servers |
| Authentication Type | Select the Authentication Type |
| Pre-shared Key | If Pre shared key, common key or TLS-AUTH is selected, set static password |
| Remote Subnet, Remote Netmask | Set static route of router, always in direction of peer subnet |
| Username/Password | If User/Password is selected, the corresponding data is entered in these fields |
| Link Detection Interval, Link Detection Timeout | Always use standard |
| Renegotiate Interval | Always use standard |
| Enable NAT | Set NAT mode, routing mode is deactivated in the meantime |
| Enable LZO | Enable LZO-compression |
| Encryption Algorithms | Encryption Algorithm must match the server |
| MTU | Always use standard, 1500 |
| Max Fragment Size | Maximum size of individual packages |
| Debug Level | Selection of Debug Output in Log |
| Interface Type | TUN / TAP |
| Expert Options (Expert Only) | Other OpenVPN commands (for advanced users only) |

## 3.6.7. OpenVPN Advanced

This configuration page is only used for the OpenVPN server and provides advanced features. You can reach this point via ***VPN > OpenVPN Advanced***.



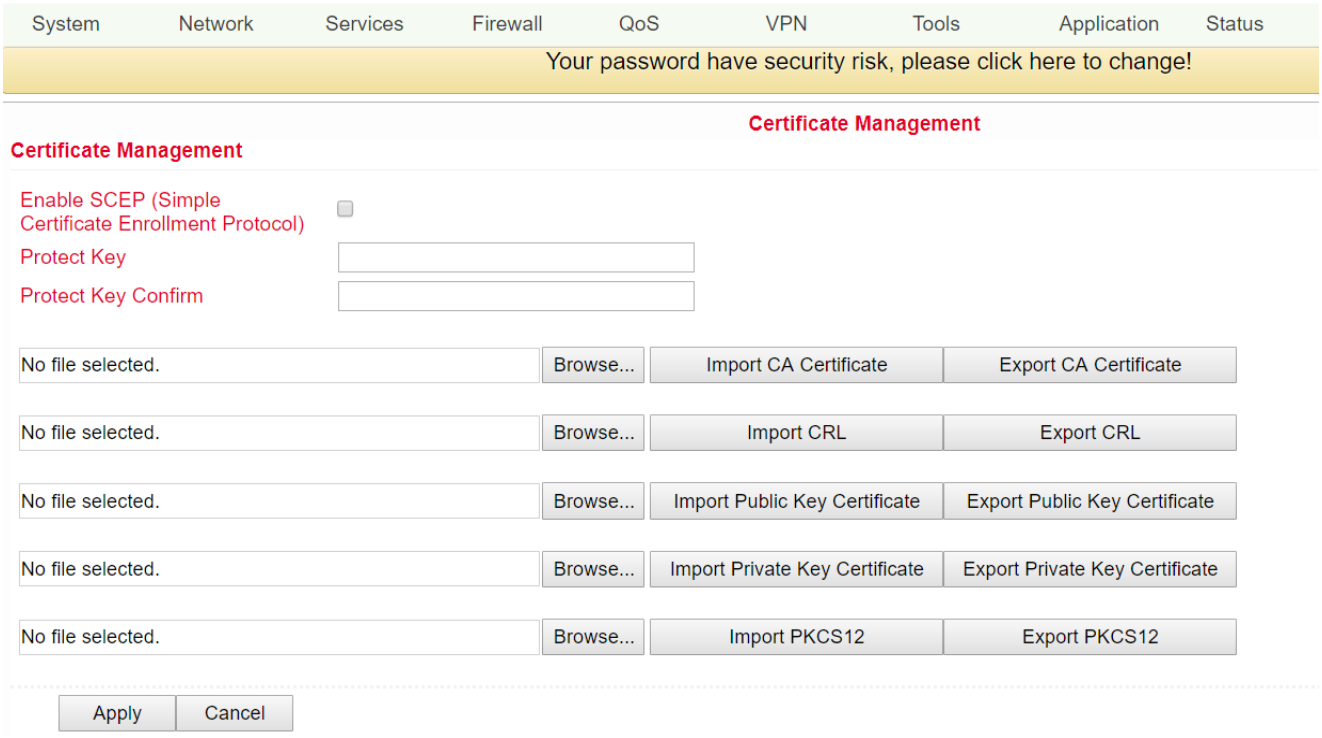
| Name | Description |
|---|---|
| Enable Client-to-Client (Server Mode Only) | Allow client access to other clients |
| Client Management | |
| Enable | Activating the function |
| Tunnel Name | Tunnel name of the client |
| Username/Common Name | User name (using the "User name/Password" mode) or general name in CA (CA mode) |
| Client IP | Specification of the client IP address |
| Local Static Route | Subnet of the client |
| Remote Static Route | Subnet of the server |

**Note**

CA can only be created by the customer's PC, not by the TK500.

## 3.6.8. Certificate Management

Under the menu item ***VPN > Certificate Management*** you can integrate the certificates that you want to use for your VPN connections. You can also export existing certificates.




| Name | Description | Standard |
|---|---|---|
| Enable SCEP | Click to activate | |
| Protect Key | Set a key to protect the certificate | Empty |
| Protect Key Confirm | Confirm the key to protect the certificates | Empty |
| Import/Export CA Certificate | Import or export CA Certificates | Empty |
| Import/Export Certificate (CRL) | Import or export CRL certificate | Empty |
| Import/Export Public Key Certificate | Import or export private key certificate | Empty |

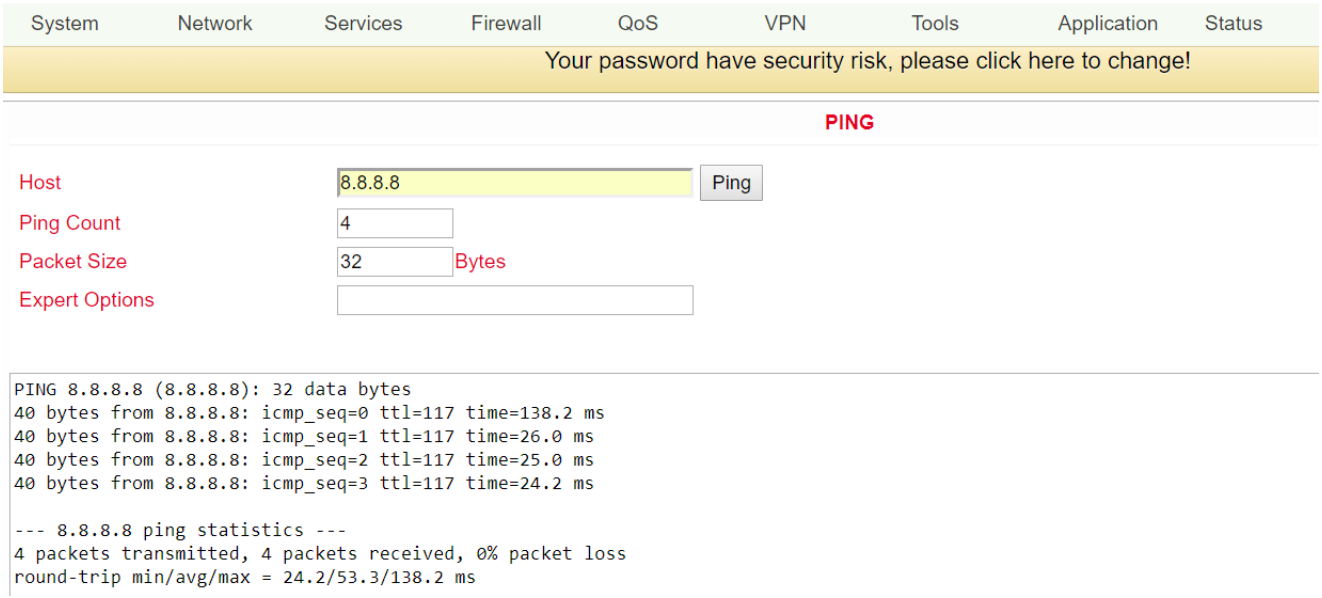
| | | |
|---|---|---|
| Import/Export Private Key Certificate | Import or export PKCS12 (private key and X.509 certificate) | Empty |
| Import/Export PKCS12 | Import or export PKCS12 (private key and X.509 certificate) | Empty |
| Searching | The respective file is selected via Browse and can then be imported | No file selected |

# 3.7. Tools

The tools are useful tools and include PING detection, trace route, connection speed tests, etc.

## 3.7.1. PING

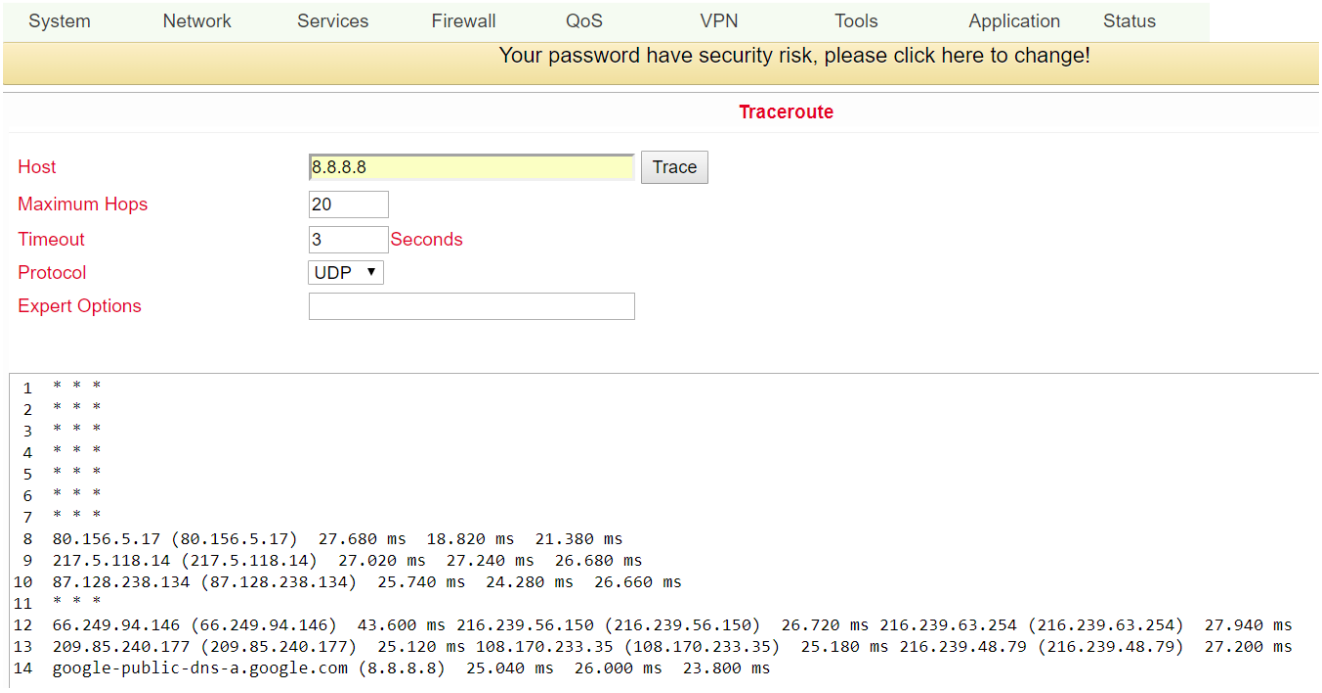
Select ***Tools > Ping*** if you want to test whether a connection to the network/internet is established.




| Name | Description | Standard |
|---|---|---|
| Host | Target for PING | Empty |
| Ping Count | Set number of PINGS | 4 times |
| Packet Size | Set packet size for PING | 32 Byte |
| Expert Options | Advanced parameters | Empty |

## 3.7.2. Traceroute

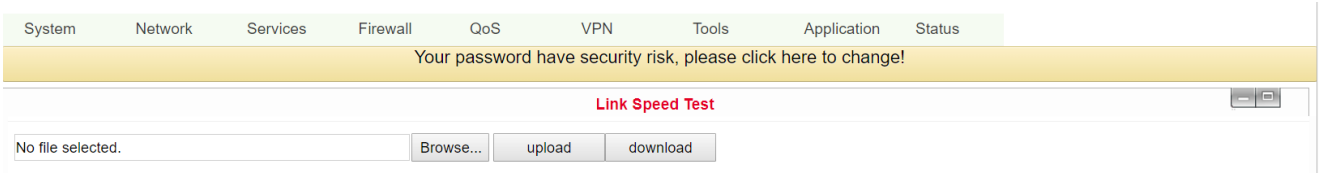
Traceroute (tracert) determines via which router and Internet node IP data packets reach the queried computer. You can enter the data under ***Tools > Traceroute***.




| Name | Description | Standard |
|---|---|---|
| Host | Target for Trace Route | Empty |
| Max Hops | Set Maximun number of Hops | 20 |
| Time Out | Set Timeout | 3 Seconds |
| Protocol | Optional: „ICMP"/„UDP" | UDP |
| Expert Options | Advanced Parameters | Empty |

## 3.7.3. Link Speed Test

Test the connection speed via upload or download. Please select this area via ***Tools > Link Speed Test***.



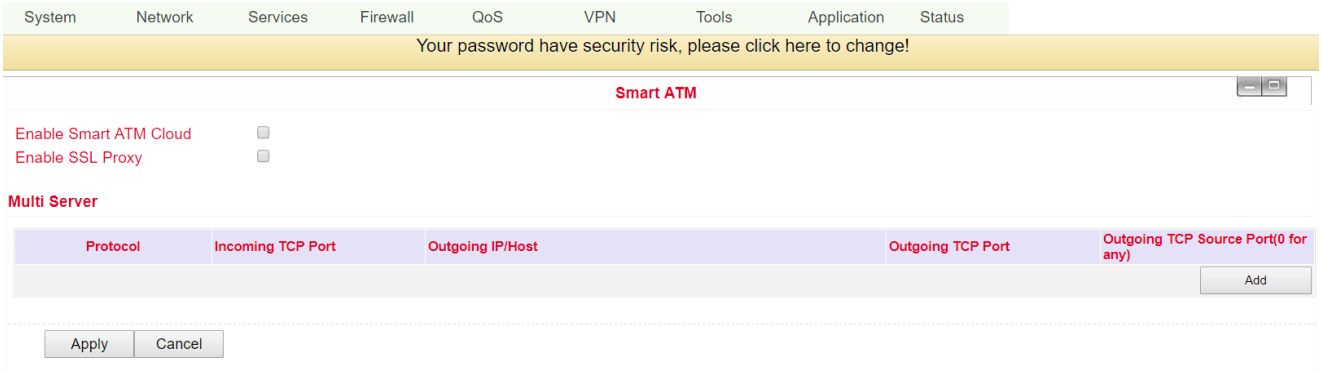

Use the ***Browse*** button to upload a file from your computer. The file should be between 10 and 2000MB in size. After selecting the file, click the ***Upload*** button. The result is then displayed.

# 3.8. Application

The menu item „***Application***" is currently not supported.

## 3.8.1. Smart ATM

The Smart ATM point is not supported by us at the moment. This is a special function for vertical markets.

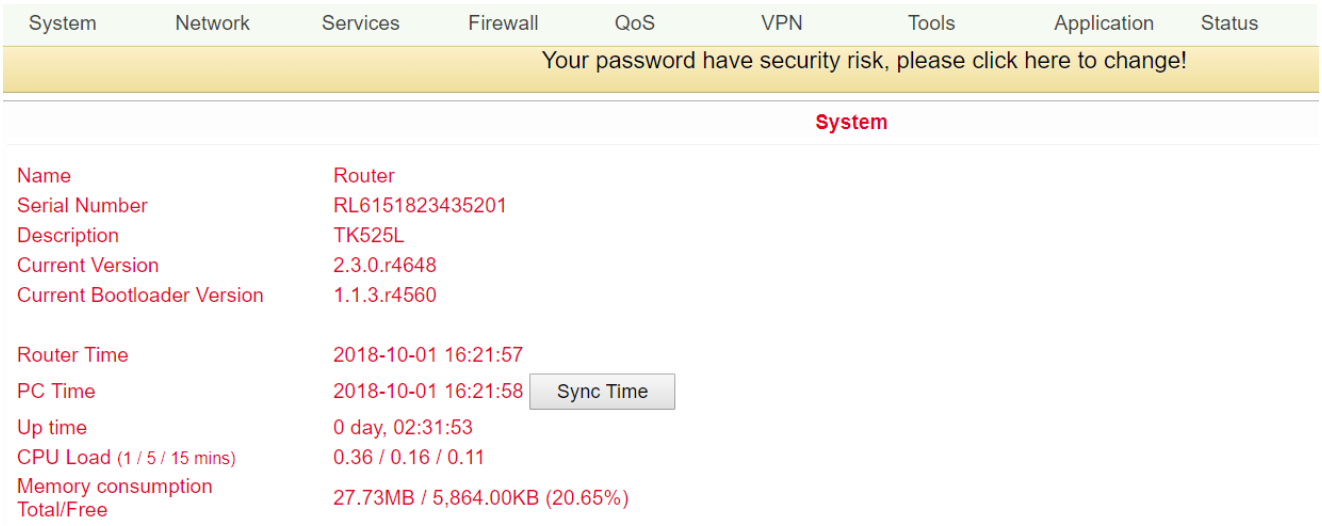


# 3.9. Status

Under „***Status***" you will find information on the system, modem, network connections, routing table, device list and protocol.

## 3.9.1. System

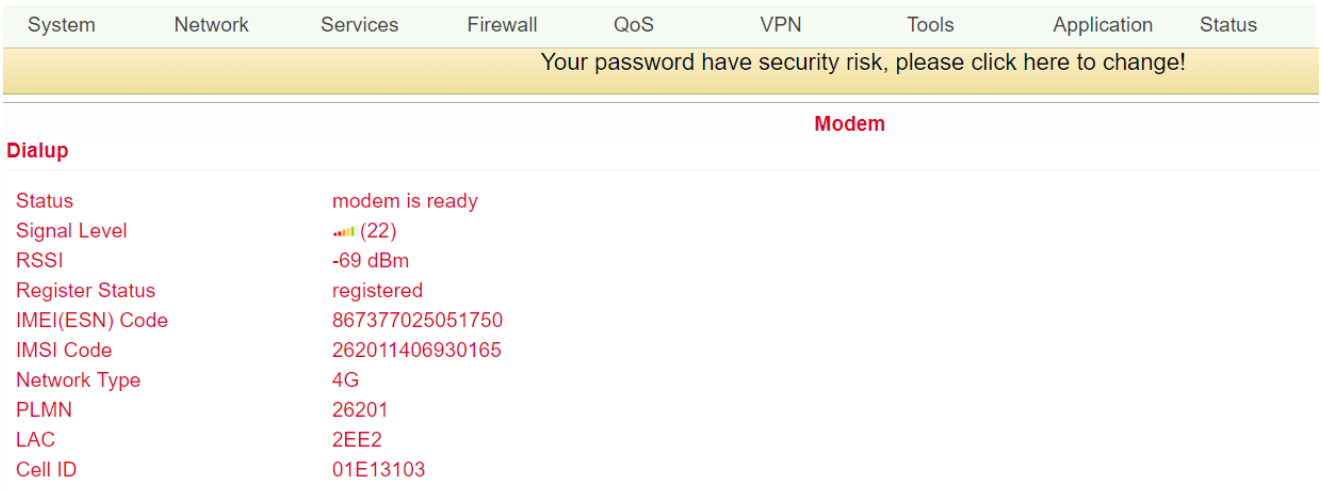
Select ***Status > System*** from the menu to retrieve information about your system.




This page displays the status of the system, including information on the name, model type, current version, etc.

## 3.9.2. Modem

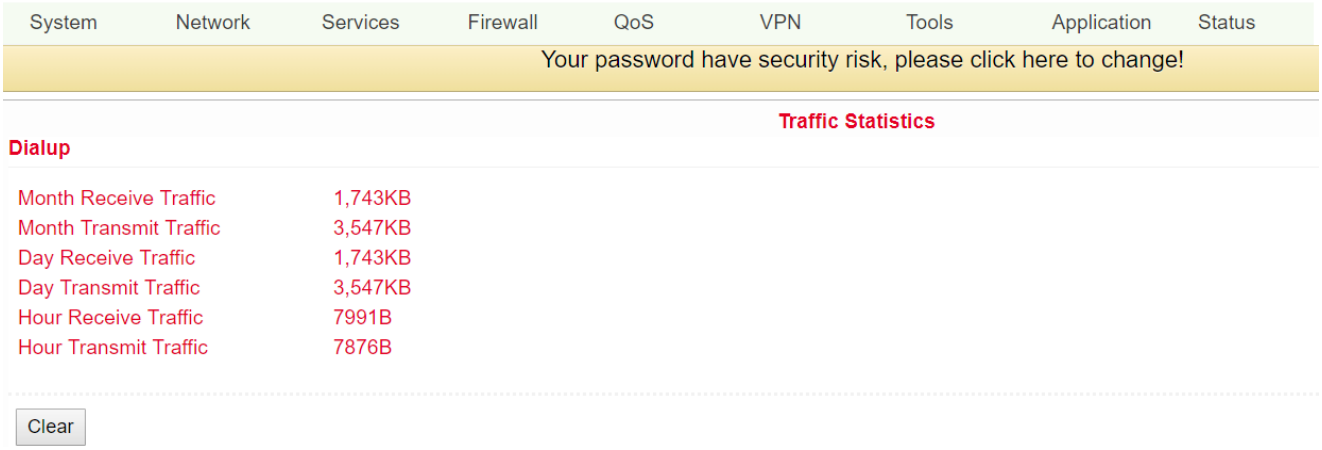
Check the status of your modem under ***System > Modem***.




Here you can display the status of the modem including the signal strength.

## 3.9.3. Traffic Statistics

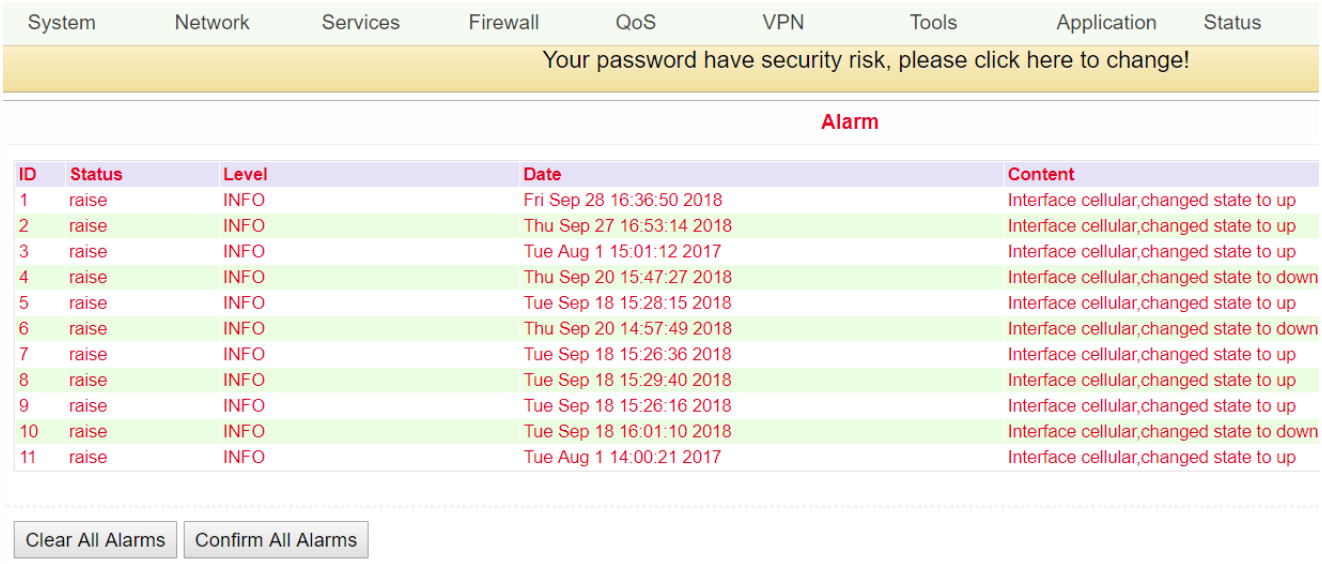
If you want to view the data consumption of the SIM card in the TK500, you can do this under ***Status > Traffic Statistics***.




Here you can see the data that was received or transmitted monthly, daily and hourly. Use the „***Clear***" button to reset the entries to 0.

## 3.9.4. Alarm

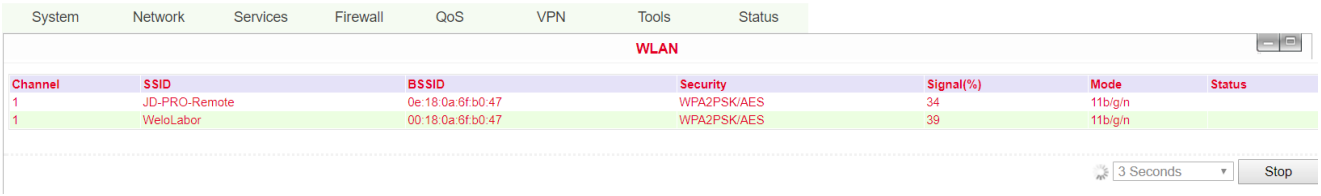
Check the alarms generated by the TK500, e.g. created under 3.3.7. in the Alarm Manager. You can access this menu item under ***Status > Alarm***.




In this example, the monthly limit of the SIM card has been reached. Use the „***Clear All Alarms***" button to delete all alarm messages and „***Confirm All Alarms***" to confirm that you have taken note of the alarm.

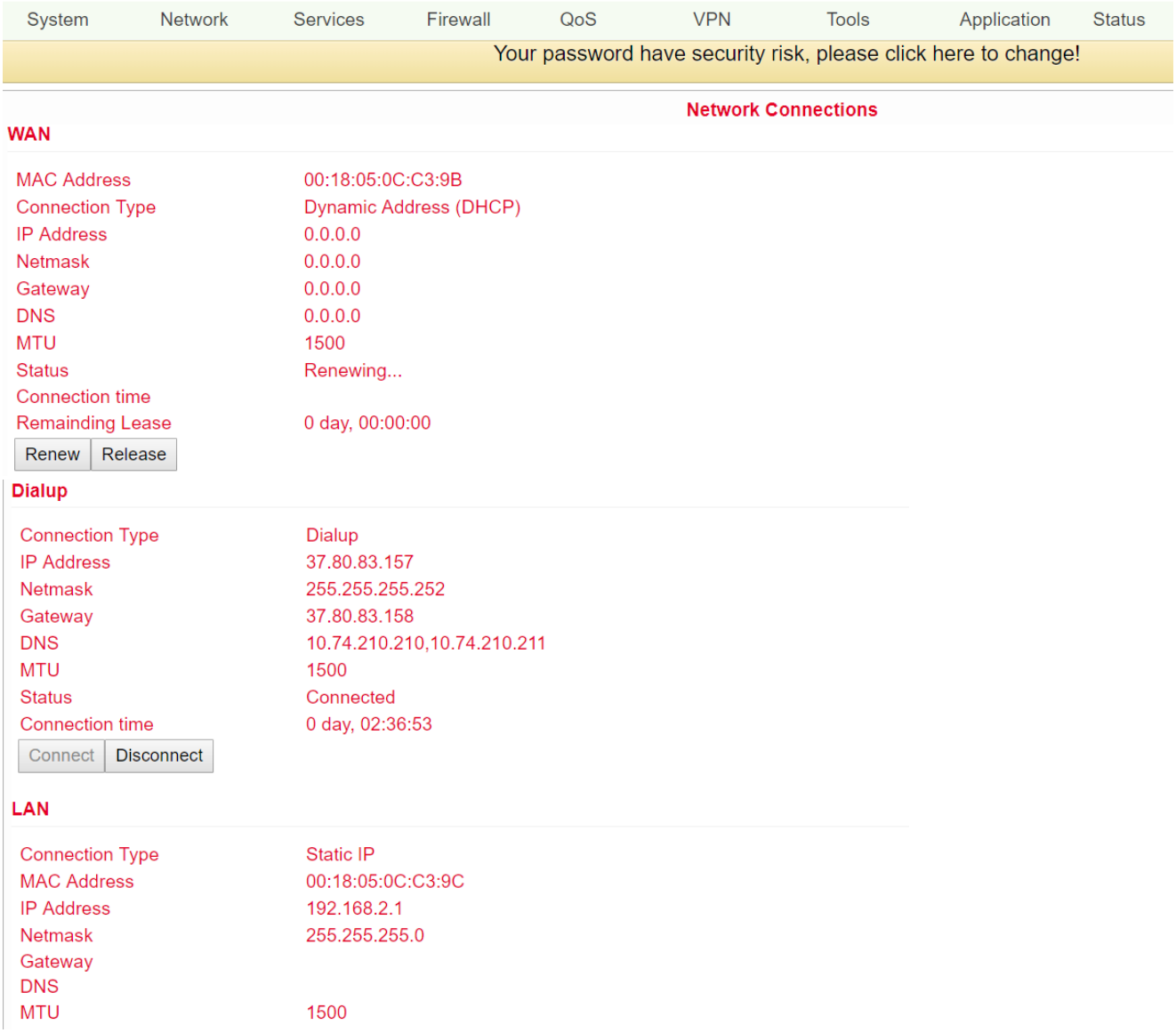
## 3.9.5. WLAN

Via ***Status > WLAN*** you can view all WLAN networks in the receiving area of the TK500. To do this, the WLAN function must be activated in the TK500 (see 3.2.6)




## 3.9.6. Network Connections

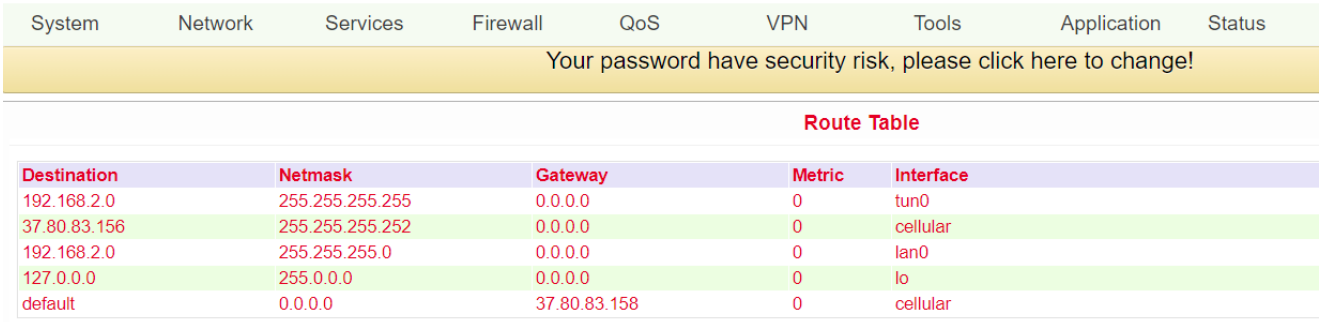
Via ***Status > Network Connections*** you can get an overview of the network connections of the TK500.




Here you can see at a glance the network connections via WAN, dialup or LAN.

## 3.9.7. Route Table

If you want an overview of the routing table in the TK500, select ***Status > Route Table***.

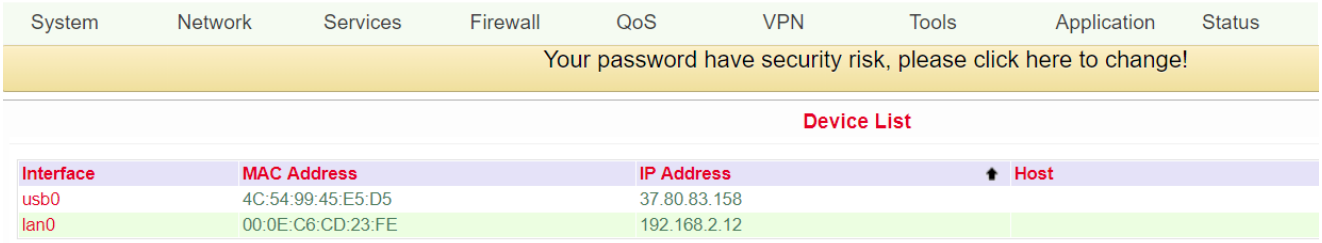



| Destination | Netmask | Gateway | Metric | Interface |
|---|---|---|---|---|
| 192.168.2.0 | 255.255.255.255 | 0.0.0.0 | 0 | tun0 |
| 37.80.83.156 | 255.255.255.252 | 0.0.0.0 | 0 | cellular |
| 192.168.2.0 | 255.255.255.0 | 0.0.0.0 | 0 | lan0 |
| 127.0.0.0 | 255.0.0.0 | 0.0.0.0 | 0 | lo |
| default | 0.0.0.0 | 37.80.83.158 | 0 | cellular |

After calling, you will see the routing table of the TK500.

## 3.9.8. Device List

All devices connected to the TK500 are displayed under the menu item ***Status > Device List***.




| Interface | MAC Address | IP Address | Host |
|---|---|---|---|
| usb0 | 4C:54:99:45:E5:D5 | 37.80.83.158 | |
| lan0 | 00:0E:C6:CD:23:FE | 192.168.2.12 | |

Overview of the devices connected to the TK500.

## 3.9.9. Log

Documentation of the system events (Log) of the TK500 can be found under ***Status > Log***.

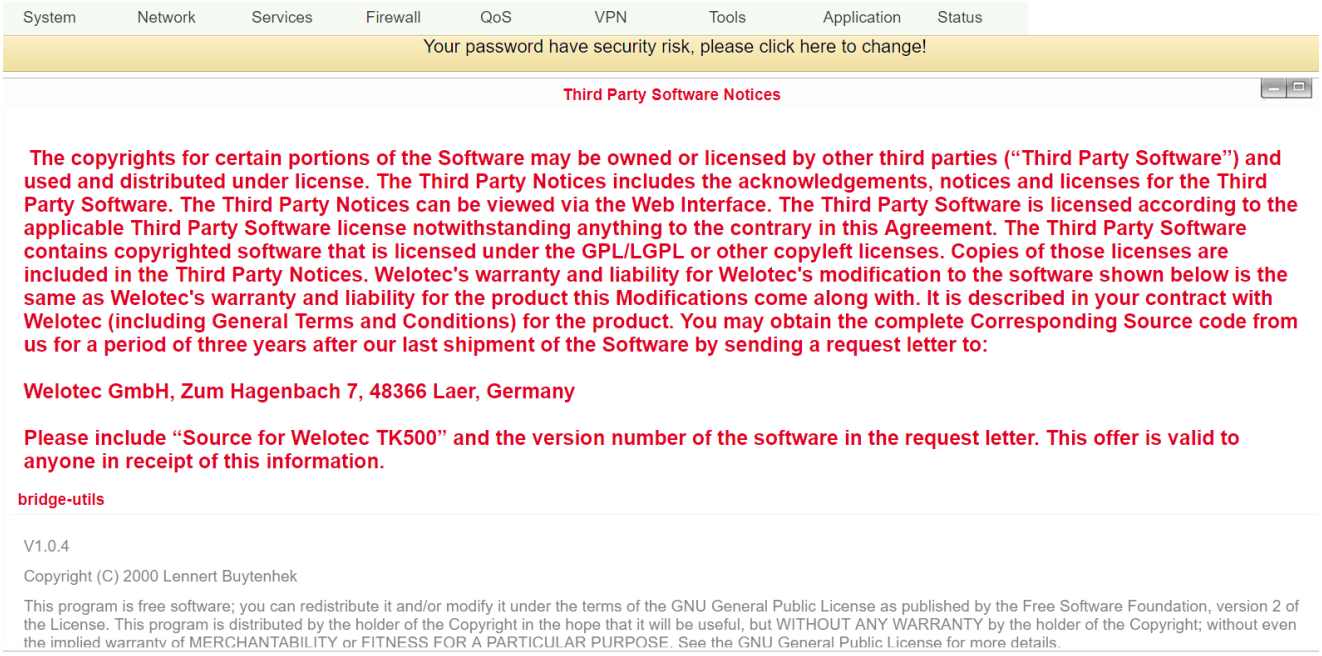

This page displays the system log that can be downloaded here

Problems may not be diagnosed and resolved immediately. In these cases, please send the diagnostic pro-

tocol to Welotec. To do this, click on „***Download System Diagnosing Data***“ and send us the protocol with a description of the error to ***support@welotec.com***

## 3.9.10. Third Party Software Notices

Here are the software terms and licenses of all third party vendors associated with the TK500 router series.



# 4. TECHNICAL DATA

## 4.1. Device characteristics

| Characteristic | Value |
|---|---|
| Dimensions (W x H x D) | 35 x 127 x 108.2 mm |
| Operating voltage | 230 V AC at 12 V – 24 V DC |
| Approval | CE-compliant |

## 4.2. Enviromental characteristics

| Characteristic | Value |
|---|---|
| Operating temperature range | -15 bis +70 °C |
| Humidity | 5 - 95 %, non-condensing |
| Shock | IEC 60068-2-27 |
| Free Fall | IEC 60068-2-32 |
| Vibration | IEC 60068-2-6 |

## 4.3. Radio frequencies

### 4.3.1. Radio frequencies 4G LTE Europe

| Frequency | Frequency range and transmission power | Router |
|---|---|---|
| Band 1 | • Frequency range Down: 2110 MHz – 2170 MHz<br>• Frequency range Up: 1920 MHz – 1980 MHz<br>• Max. transmission power: 200 mW | TK525U, TK525L, TK525L W, TK525W |
| Band 3 | • Frequency range Down: 1805 MHz – 1880 MHz<br>• Frequency range Up: 1710 MHz – 1785 MHz<br>• Max. transmission power: 200 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 7 | • Frequency range Down: 2620 MHz – 2690 MHz<br>• Frequency range Up: 2500 MHz – 2570 MHz<br>• Max. transmission power: 200 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 8 | • Frequency range Down: 925 MHz – 960 MHz<br>• Frequency range Up: 880 MHz – 915 MHz<br>• Max. transmission power: 200 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 20 | • Frequency range Down: 791 MHz – 821 MHz<br>• Frequency range Up: 832 MHz – 862 MHz<br>• Max. transmission power: 200 mW | TK525U, TK525L, TK525L W, TK525W |
| Band 28 | • Frequency range Down: 703 MHz – 748 MHz<br>• Frequency range Up: 758 MHz – 803 MHz<br>• Max. transmission power: 200 mW | TK525U, TK525L, TK525L-W, TK525W |

## 4.3.2. Radio frequencies 3G UMTS Europa

| Frequency | Frequency range and transmission power | Router |
|---|---|---|
| Band 1 | • Frequency range Down: 2110 MHz – 2170 MHz<br>• Frequency range Up: 1920 MHz – 1980 MHz<br>• Max. transmission power: 251 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 3 | • Frequency range Down: 1805 MHz – 1880 MHz<br>• Frequency range Up: 1710 MHz – 1785 MHz<br>• Max. transmission power: 251 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 8 | • Frequency range Down: 925 MHz – 960 MHz<br>• Frequency range Up: 880 MHz – 915 MHz<br>• Max. transmission power: 251 mW | TK525U, TK525L, TK525L-W, TK525W |

## 4.3.3. Radio frequencies 2G GSM Europe

| Frequency | Frequency range and transmission power | Router |
|---|---|---|
| GSM 900 | • Frequency range Down: 925 MHz – 960 MHz<br>• Frequency range Up: 880 MHz – 915 MHz<br>• Max. transmission power: 1995 mW | TK525U, TK525L, TK525L-W, TK525W |
| GSM 1800 | • Frequency range Down: 1805 MHz – 1880 MHz<br>• Frequency range Up: 1710 MHz – 1785 MHz<br>• Max. transmission power: 40 mW | TK525U, TK525L, TK525L-W, TK525W |

## 4.3.4. Radio frequencies 4G LTE Asia

| Frequency | Frequency range and transmission power | Router |
|---|---|---|
| Band 1 | • Frequency range Down: 1920 MHz – 1980 MHz<br>• Frequency range Up: 2110 MHz – 2170 MHz<br>• Max. transmission power: 200 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 3 | • Frequency range Down: 1805 MHz – 1880 MHz<br>• Frequency range Up: 1710 MHz – 1785 MHz<br>• Max. transmission power: 200 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 5 | • Frequency range Down: 869 MHz – 894 MHz<br>• Frequency range Up: 824 MHz – 849 MHz<br>• Max. transmission power: 200 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 7 | • Frequency range Down: 2620 MHz – 2690 MHz<br>• Frequency range Up: 2500 MHz – 2570 MHz<br>• Max. transmission power: 200 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 38 China | • Frequency range Down: 2570 MHz – 2620 MHz<br>• Frequency range Up: not known<br>• Max. transmission power: 200 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 39 China | • Frequency range Down: 1880 MHz – 1920 MHz<br>• Frequency range Up: not known<br>• Max. transmission power: 200 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 40 China | • Frequency range Down: 2300 MHz – 2400 MHz<br>• Frequency range Up: not known<br>• Max. transmission power: 200 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 41 China | • Frequency range Down: 2496 MHz – 2690 MHz<br>• Frequency range Up: not known<br>• Max. transmission power: 200 mW | TK525U, TK525L, TK525L-W, TK525W |

## 4.3.5. Radio frequencies 3G UMTS Asia

| Frequency | Frequency range and transmission power | Router |
|---|---|---|
| Band 1 | • Frequency range Down: 2110 MHz – 2170 MHz<br>• Frequency range Up: 1920 MHz – 1980 MHz<br>• Max. transmission power: 251 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 5 | • Frequency range Down: 869 MHz – 894 MHz<br>• Frequency range Up: 824 MHz – 849 MHz<br>• Max. transmission power: 251 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 8 | • Frequency range Down: 925 MHz – 960 MHz<br>• Frequency range Up: 880 MHz – 915 MHz<br>• Max. transmission power: 251 mW | TK525U, TK525L, TK525L-W, TK525W |

## 4.3.6. Radio frequencies 2G GSM Asia

| Frequency | Frequency range and transmission power | Router |
|---|---|---|
| GSM 900 | • Frequency range Down: 925 MHz – 960 MHz<br>• Frequency range Up: 880 MHz – 915 MHz<br>• Max. transmission power: 1995 mW | TK525U, TK525L, TK525L-W, TK525W |
| GSM 1800 | • Frequency range Down: 1805 MHz – 1880 MHz<br>• Frequency range Up: 1710 MHz – 1785 MHz<br>• Max. transmission power: 1000 mW | TK525U, TK525L, TK525L-W, TK525W |

## 4.3.7. Radio frequencies 3G UMTS global

| Frequency | Frequency range and transmission power | Router |
|---|---|---|
| Band 1 | • Frequency range Down: 2110 MHz – 2170 MHz<br>• Frequency range Up: 1920 MHz – 1980 MHz<br>• Max. transmission power: 251 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 2 | • Frequency range Down: 1930 MHz – 1990 MHz<br>• Frequency range Up: 1850 MHz – 1910 MHz<br>• Max. transmission power: 251 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 5 | • Frequency range Down: 869 MHz – 894 MHz<br>• Frequency range Up: 824 MHz – 849 MHz<br>• Max. transmission power: 251 mW | TK525U, TK525L, TK525L-W, TK525W |
| Band 8 | • Frequency range Down: 925 MHz – 960 MHz<br>• Frequency range Up: 880 MHz – 915 MHz<br>• Max. transmission power: 251 mW | TK525U, TK525L, TK525L-W, TK525W |

## 4.3.8. Radio frequencies 2G GSM global

| Frequency | Frequency range and transmission power | Router |
|---|---|---|
| GSM 850 | • Frequency range Down: 869 MHz – 894 MHz<br>• Frequency range Up: 824 MHz – 849 MHz<br>• Max. transmission power: 1995 mW | TK525U, TK525L, TK525L-W, TK525W |
| GSM 1900 | • Frequency range Down: 1930 MHz – 1990 MHz<br>• Frequency range Up: 1850 MHz – 1910 MHz<br>• Max. transmission power: 1000 mW | TK525U, TK525L, TK525L-W, TK525W |

## 4.3.9. Radio frequencies WLAN

| Frequency | Frequency range and transmission power | Router |
|---|---|---|
| 2.4 GHz | • Frequency range: 2400 MHz – 2483.5 MHz<br>• Max. transmission power: 40 mW | TK525L-W |

# 5. SUPPORT

If there are any problems with installation and operation, please send an e-mail to the following address:
support@welotec.com

# 6. CE DECLARATION

a byte smarter

## Declaration of conformity

**Holder:**
Welotec GmbH
Zum Hagenbach 7
48366 Laer
GERMANY

declares that the product(s):

**Product:**
Industrial Cellular Router

**Identification:**
**TK505U, TK515L, TK515L-W, TK505W, TK525U, TK525L, TK525L-W, TK525W**

**Complies with:**

**Radio Equipment Directive 2014/53/EU,**
ETSI EN 301 489-1 V2.1.1 (2017-02 – Class A)
ETSI EN 301 489-3 V1.6.1 (2013-08)
ETSI EN 301 489-17 V3.1.1 (2017-02)
ETSI EN 301 489-52 V1.1.0 (2016-11)
ETSI EN 301 511 V12.5.1 (2017-03)
ETSI EN 300 328 V2.1.1 (2016-11)
ETSI EN 301 908-1 V11.1.1 (2016-07)
ETSI EN 301 908-2 V11.1.1 (2016-07)
ETSI EN 301 908-13 V11.1.1 (2016-07)
EN 62311:2008
**Low Voltage Directive 2014/35/EU**
EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
**EMC Directive 2014/30/EU**
EN 55032:2012
EN 55024:2010
EN 61000-3-2:2014
EN 61000-3-3:2013
**RoHS 2 Directive 2011/65/EU**

**for use in industrial environments.**

CE

The corresponding markings appear under the appliance.

These devices are designed for the use in all countries of the EU, Switzerland, Norway, Lichtenstein and Iceland.

Welotec GmbH
Zum Hagenbach 7
D-48366 Laer
Fon: +49(0)2554-913000
www.welotec.com

2017-09-29
Date

Signature
(Jos Zenner, Business Development)

www.welotec.com

Welotec GmbH
Zum Hagenbach 7 · D-48366 Laer
Fon: +49 (0)25 54/91 30-00
Fax: +49 (0)25 54/91 30-10
info@welotec.com

Geschäftsführer: Dr. Reinhard Lülff
Handelsregister Steinfurt, HRB 3363
Ust-IdNr. DE121631449
Steuer-Nr. 311/5830/2243

Deutsche Bank AG Vreden
Konto-Nr. 3 920 840 · BLZ 403 700 24
IBAN DE 36403700240392084000
SWIFT DEUTDEDB403

Kreissparkasse Steinfurt
Konto-Nr 3 020 203 · BLZ 403 510 60
IBAN DE 13403510600003020203
SWIFT WELADED1STF