TK100

Version:
v1.0.0

Date:
22.06.2023

Contents

1 TK100 Series - Introduction

Copyright notice

Trademarks

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.

It is possible that this user manual contains technical or typographical errors. Corrections are made regularly without being pointed out in new versions.

Technical support contact information

Welotec GmbH

Zum Hagenbach 7

48366 Laer

Tel.: +49 2554 9130 00

Fax.: +49 2554 9130 10

[*Email: support@welotec.com*]

Description

The TK100 series industrial routers provide stable, high-speed connectivity between remote devices and customer sites over LAN and (depending on model) LAN or 3G/4G networks. They can operate in a voltage range of 9 to 36 V DC and have a temperature range of -20°C to 70°C with a relative humidity of 95%, ensuring high stability and reliability under severe conditions. The TK100 can be used on the workstation or mounted on DIN rails.

TK100 series products support VPN (IPSec/PPTP/L2TP/GRE/SSL VPN), which guarantees secure connections between remote devices and customer sites.

Important safety notice:

This product is not suitable for the following applications:

• Areas where radio applications (such as cell phones) are not allowed

• Hospitals and other places where the use of cell phones is not allowed

• Gas stations, fuel depots and places where chemicals are stored

• Chemical plants or other locations with explosion hazards Metal surfaces that can weaken the radio signal level

WEEE notice

The European Directive on Waste Electrical and Electronic Equipment (WEEE), which came into force on February 13, 2003, has led to major changes with regard to the reuse and recycling of electrical equipment.

The main objective of this directive is to prevent waste from electrical and electronic equipment and to promote reuse, recycling and other forms of recovery. The WEEE logo (see figure on the left) on the product or packaging indicates that the product must not be disposed of with other household waste. You are responsible for disposing of all discarded electrical and electronic equipment at appropriate collection points. Separate collection and sensible

recycling of your electronic waste helps to use natural resources more sparingly. In addition, proper recycling of waste electrical and electronic equipment ensures human health and environmental protection.

For more information on disposal, recycling, and collection points for waste electrical and electronic equipment, contact your local municipality, waste disposal companies, the distributor, or the manufacturer of the equipment.

1.1 Content checklist

Each TK100 wireless router is delivered in a package with standard accessories. Additional accessories can be ordered. Check the contents of your package carefully and if anything is missing or damaged, contact your sales partner from Welotec GmbH.

Scope of delivery:

Standard accessories:

Accessories	Quantity	Description
TK100-Router	1	TK100 series industrial router
Network cable	1	Network cable CAT5, 1,5 Meter
Manual	1	Data medium with manual
License terms	1	“Third Party Software Notifications and Licenses”
Power supply		
Terminal block	1	2-pole terminal for power supply

Components set (depending on model)

Product	Quantity	Description
TK100-Router	1	TK100 series industrial router
Network cable	1	Network cable CAT5, 1,5 Meter
Cellular antenna	1	5 m Magnetic base antenna 2G/3G/4G
Manual	1	Data medium with manual
License terms	1	“Third Party Software Notification and Licenses”
Power supply		
	1	Table power supply, input 100-240 V AC, output 12 V DC (for TK100), incl. 2-pole terminal block
	1	Plug, European standard

1.2 Product information

1.2.1 Environmental requirements

Operating temperature: -20 to 70°C

Relative humidity during operation: 5 to 95 % (non-condensing)

Storage temperature: -40 to +85°C

1.2.2 Power supply

Power supply: 1 terminal strip (2-pole) incl. voltage socket and serial connection

Input voltage: 9 - 36 V DC

1.2.3 Physical properties

Housing: steel, protection class IP30

Weight: 259 g

Dimensions (mm): 90 x 90 x 25 mm

2 Installation Manual

2.1 Typical use

With TK100 series routers, you can connect devices to the Internet with Ethernet, via GPRS/HSUPA/ UMTS/LTE. To ensure security and uninterrupted access, the TK100 series supports VPN connections, enabling remote access and secure data transmission over the Internet.

2.2 Connection plan

Interface	Description
Power connection	9 - 36 V DC
Ethernet ports	Zwei 10/100 Base-TX RJ45-Ports
Antenna connection (mobile radio)	SMA (f)
SIM card slot	Two slots for SIM card insertion

2.2.1 Meaning of the LED lights

Power	Status	Mobile	Bedeutung
Off	Off	Off	Turned off
On	Off	Off	System error
On	On	Off	The module or SIM card is not recognized
On	On	Flashing	Dial up
On	On	On	Dial up successful
On	Flashing	On	System upgrade
On	Flashing->On	Off	Reset

Signal strength

Color	Signal strength
Red	Signal 0 - 10
Yellow	Signal 11 - 20
Green	Signal 21 - 30

2.3 Fast internet connection

2.3.1 Inserting the SIM card

Open the TC router SIM/UIM slot at the top of the device and insert the SIM card into the card holder.

2.3.2 Antenna installation

After installing the TK100, connect the antenna and screw the antenna tight. Place the antenna where a good signal strength is achieved.

Note: Position and angle may affect signal strength.

2.3.3 Power supply

Connect the power supply included in the package to the device and check whether the LED display for “Power” lights up. Contact Welotec technical support if no indicator lights up. You can configure the TK100 when the power indicator is flashing.

2.3.4 Connecting

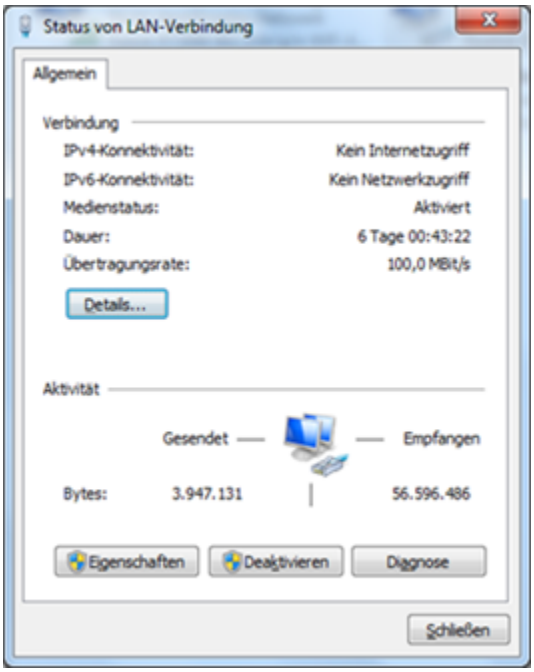
Connect the TK100 to the PC:

1. Connect the Ethernet cable of the TK100 to the PC.
2. Then one LED indicator of the RJ45 interface lights up green and the other indicators flash.

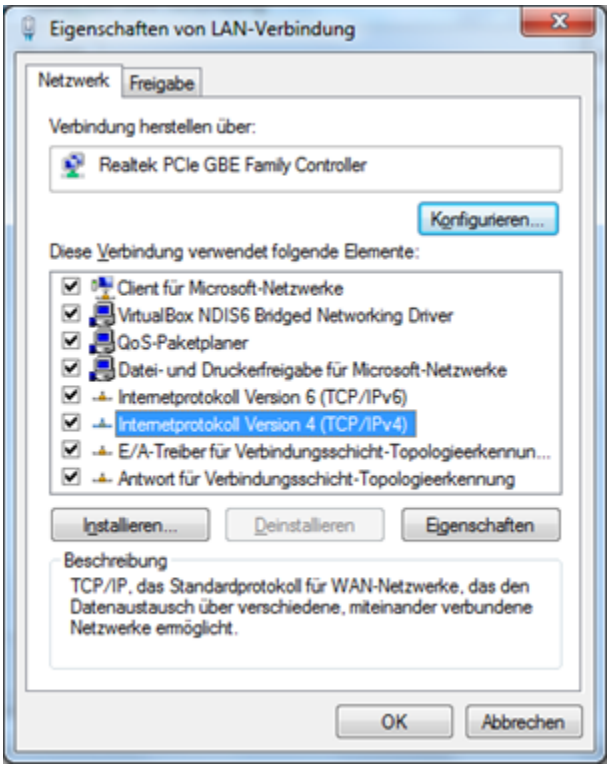
2.3.5 Connecting the TK router device to the PC for the first time

The TK100 router can assign IP addresses for the PC automatically. Set up the PC so that IP addresses are retrieved automatically via DHCP. (Basis is 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 “***LAN Connection***” and open the “***Status of LAN Connection***” screen:

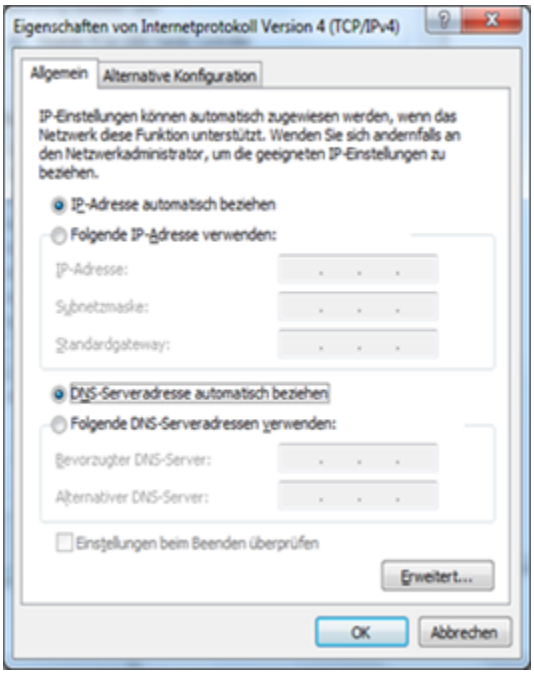


3. Click "***Properties***" and open the LAN connection properties screen:



1. 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, e.g. IP: 192.168.2.10, netmask: 255.255.255.0, default gateway: 192.168.2.1)

By clicking "***OK***", the TK router assigns an IP address to the PC: 192.168.2.X, and the gateway: 192.168.2.1 (the default address of the TK100).



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 without errors. The following is an example of running the ping command under Windows 7 :

Windows key+R -> enter "***cmd***" -> Enter key -> enter "***Ping 192.168.2.1***" -> Enter key For this display:

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\[redacted]>ping 192.168.2.1

Ping wird ausgeführt für 192.168.2.1 mit 32 Bytes Daten:
Antwort von 192.168.2.1: Bytes=32 Zeit=1ms TTL=64
Antwort von 192.168.2.1: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.2.1: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.2.1: Bytes=32 Zeit<1ms TTL=64

Ping-Statistik für 192.168.2.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 1ms, Mittelwert = 0ms

C:\Users\[redacted]>_
```

The connection between the PC and the router has been established correctly.

In the following example there are errors:

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\[redacted]>ping 192.168.2.1

Ping wird ausgeführt für 192.168.2.1 mit 32 Bytes Daten:
PING: Fehler bei der Übertragung. Allgemeiner Fehler.
PING: Fehler bei der Übertragung. Allgemeiner Fehler.
PING: Fehler bei der Übertragung. Allgemeiner Fehler.
PING: Fehler bei der Übertragung. Allgemeiner Fehler.

Ping-Statistik für 192.168.2.1:
    Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4
    (100% Verlust),

C:\Users\[redacted]>_
```

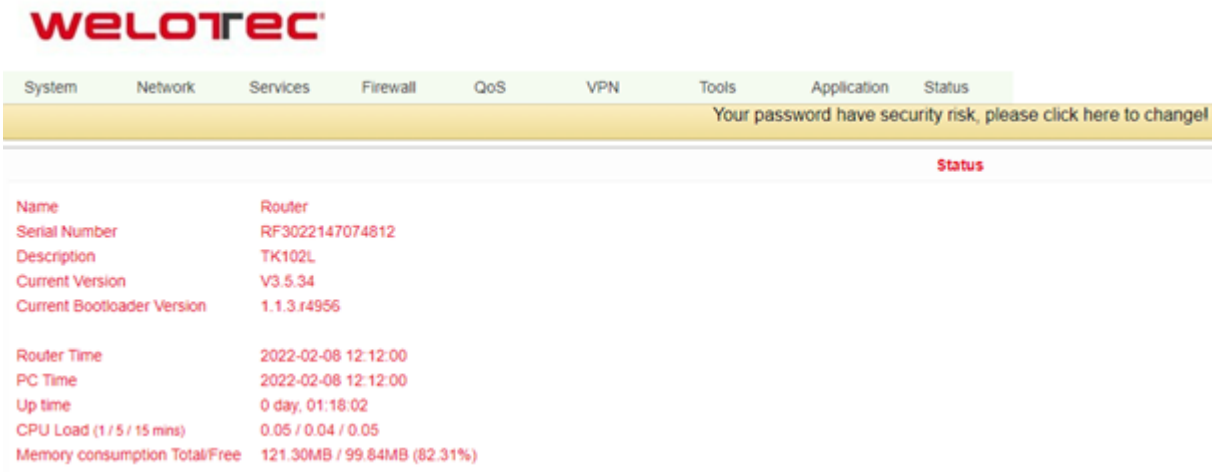
The connection is not working properly and you should go through the instructions again and check your settings.

2.3.6 Configuring the TK100 (Optional)

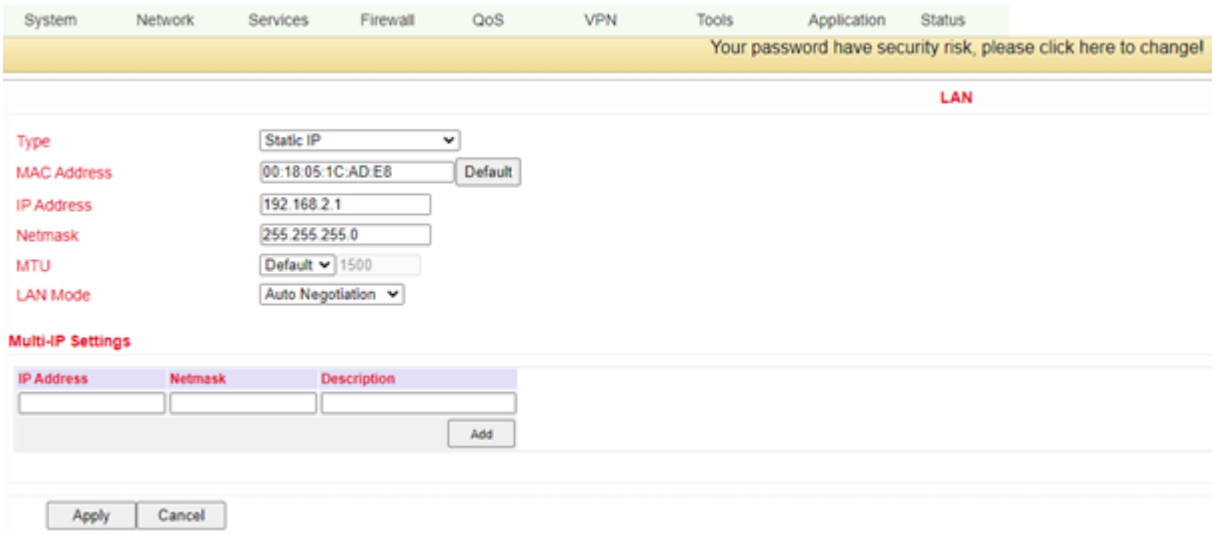
After you have performed the steps described in the previous chapter, you can configure the router:

1. Open any Internet browser (e.g. 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 password (default: 123456), and then click "***Login***" to open the configuration screen.

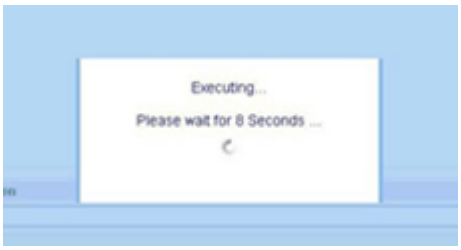


If you want to set your own IP for the router: Click ***Network >LAN***.



Change the IP address to ***192.168.1.254***, for example.

Click "***Apply***" and the following screen will be displayed:



The IP address of the TK100 has been changed. So that you can now 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 Connecting the TK router to the Internet

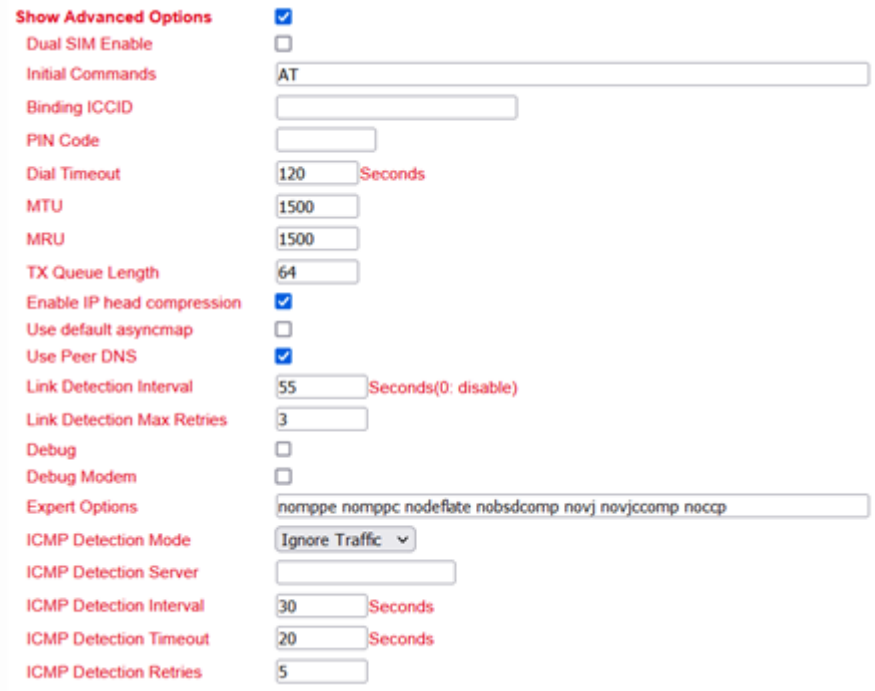
Perform the following configuration steps to establish a connection between the TK100 and the Internet.

Click ***Network*** > ***Cellular***, and enable the function with ***Enable***:

Check the entries and select a preset network provider under **SIM1 Network Provider**, or add a self-created profile of a provider:

You can obtain the APN, dial-in number, user name and password from your local network provider. Ask them for the details.

Via ***Show Advanced Options*** you can make further settings, such as the PIN code if it is set on the SIM card.



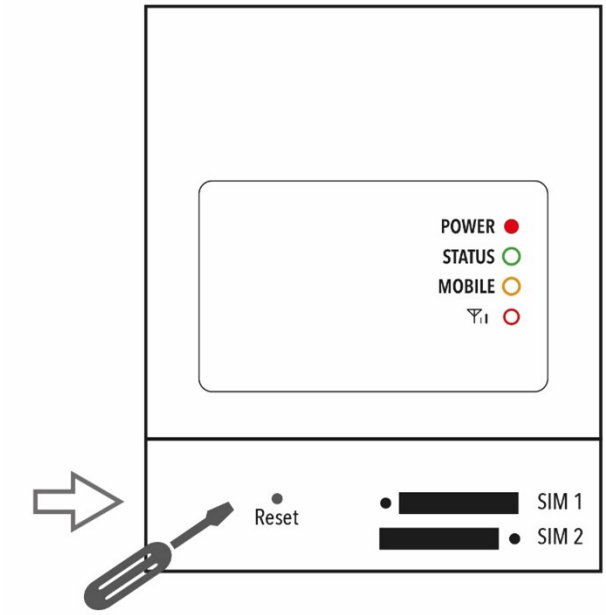
If you have set the correct configuration, the TK100 can now connect to the Internet. Open an Internet browser, type "[**www.welotec.com**][*www.welotec.com*]" and the Welotec website will open.

2.4 Reset to factory settings

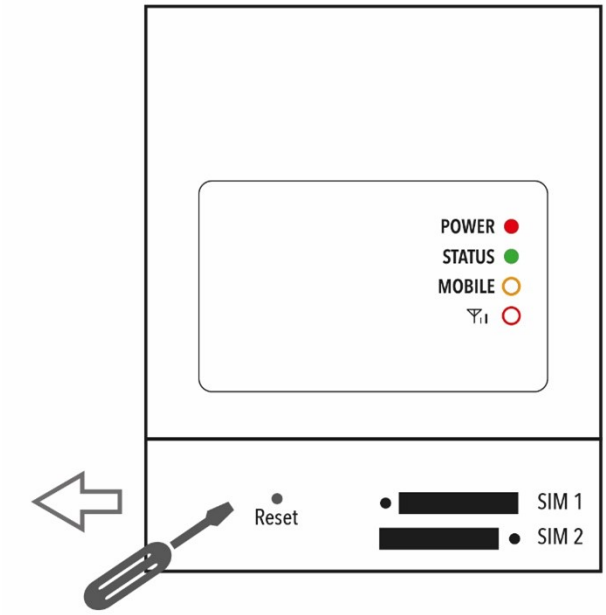
2.4.1 Hardware method

 = LED leuchtet  = LED leuchtet nicht  = LED blinkt

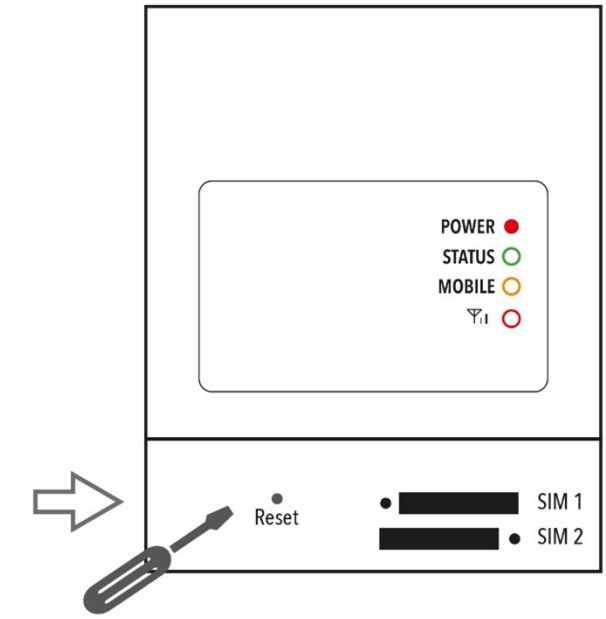
1. Press the ***RESET key*** while turning on the TK100:



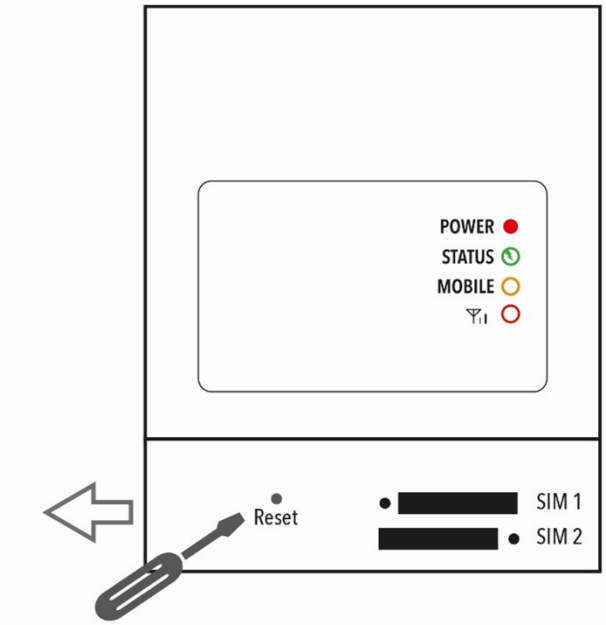
2. As soon as the **Status** LED lights up (approx. 15 seconds after switching on), release the ***RESET button***:



3. After a few seconds, the **Status** LED light will stop glowing. Now press the ***RESET button*** again:



4. The **Status** LED light will then flash, indicating that the reset to the default setting was successful.



2.4.2 Web method

1.) Log in to the TK100 web-based user interface and select ***System > Config Management***:

2.) Click ***Restore default configuration*** to reset the TK100 to its factory settings. After that the router will be re-booted.

2.5 Factory default settings:

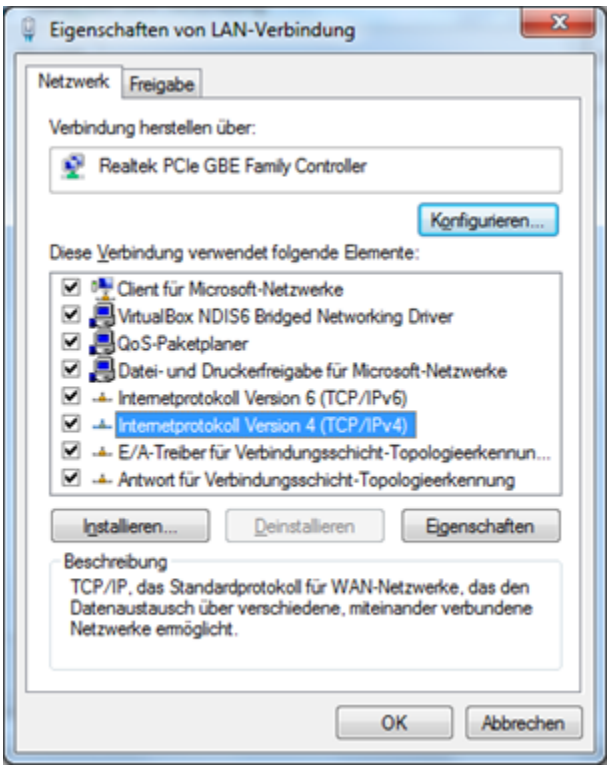
- **IP**: 192.168.2.1
- **Netmask**: 255.255.255.0
- **Username**: adm
- **Password**: 123456
- **Serial Parameter**: 115200-N-8-1

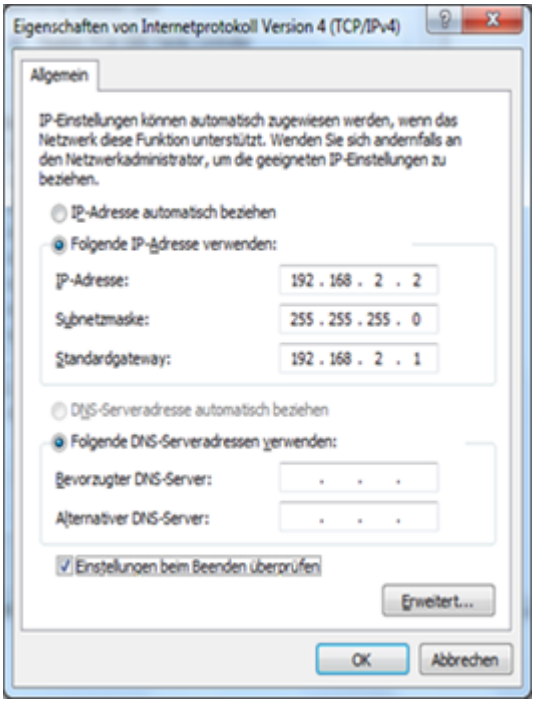
3 System

The TK-500 Router must be properly configured before use. This chapter describes the web-based configuration.

3.1 Preparation

First connect your devices to the TK100 via cable or hub (switch) and set the IP address for the PC and TK100 in the same subnet, e.g.: set the PC IP address to 192.168.2.2, netmask: ***255.255.255.0***, gateway (default IP of TK100: ***192.168.2.1***):

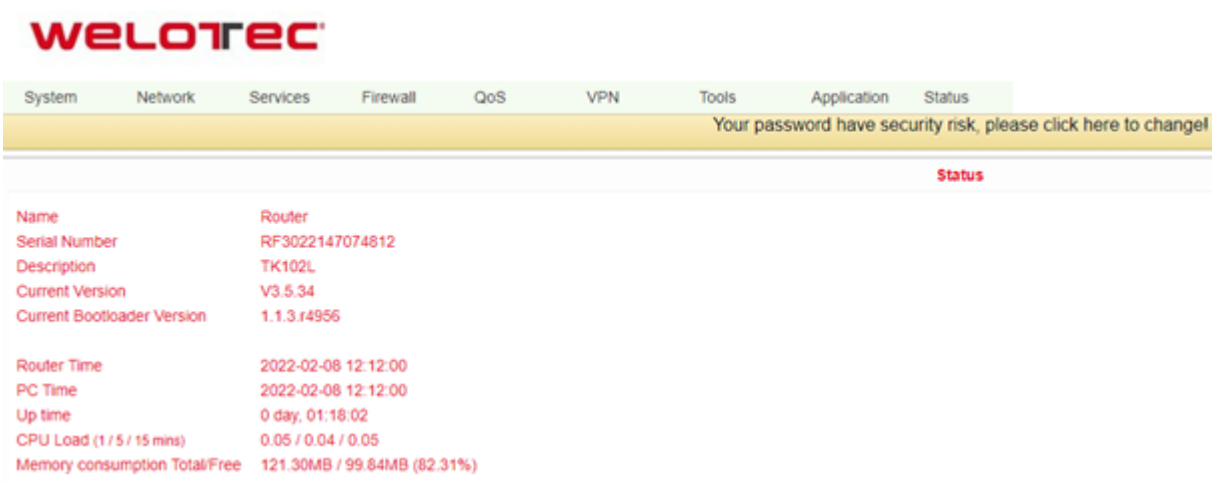


20Pics


Open an Internet browser and enter the IP address of the TK100: [**http://192.168.2.1**][**http://192.168.2.1***.*] (default IP of the TK100).

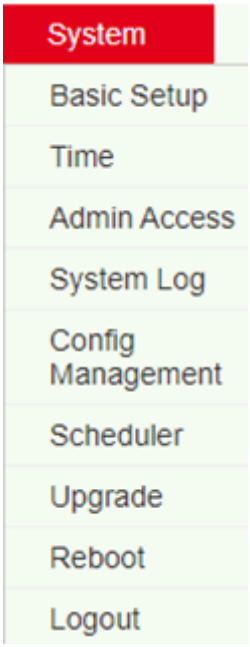
On the following login page, you must log in as an administrator. Enter the user name and password (default: ***adm/123456***).

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



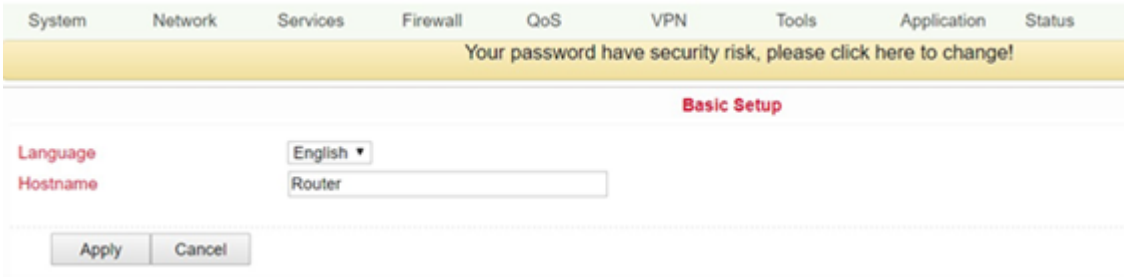
3.2 System

The system settings include the following 9 areas: Basic Setup, Time, Admin Access, System Log, Config Management, Scheduler, Upgrade, Reboot and Logout.



3.3 Basic Setup

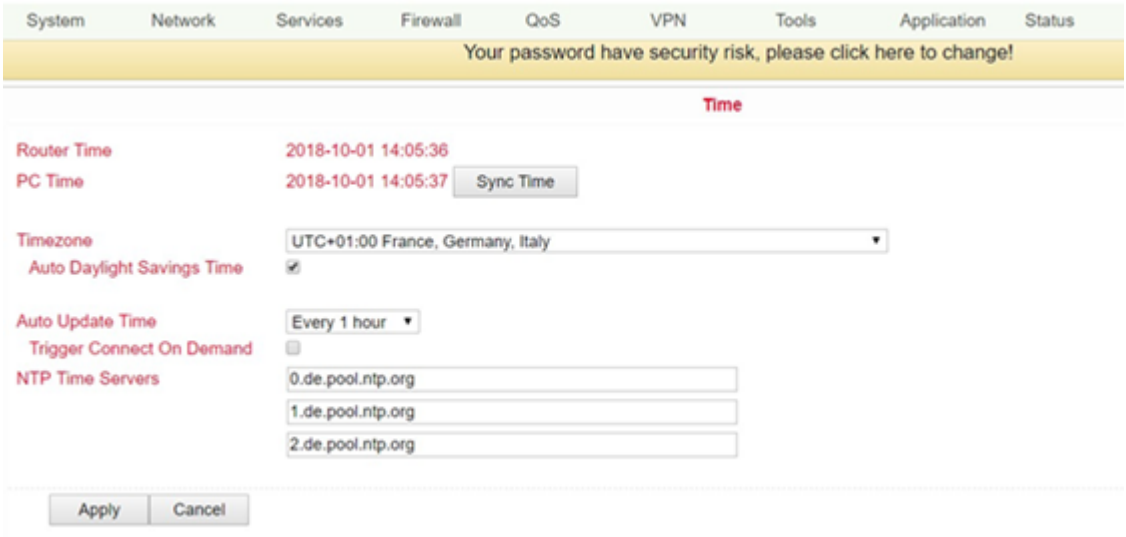
In the Basic Setup you can change the language of the menu and the host name. This menu item can be accessed via ***System > Basic Setup***.



Parameter Name	Description	Standard
Language	Set language for configuration page	English
Host Name	Hostname TK100	Router

3.4 Time

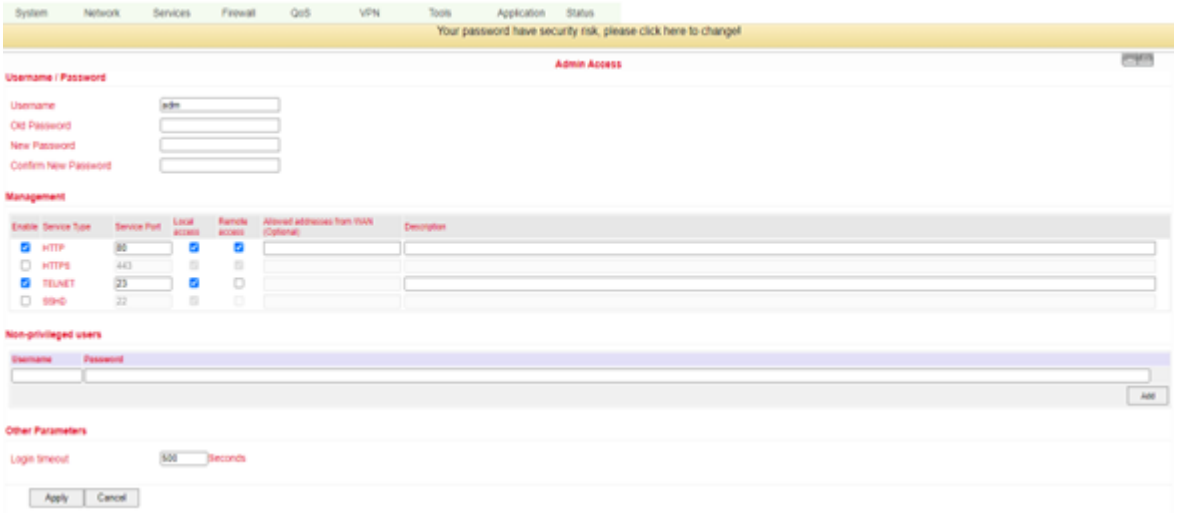
In this menu item the system time of the router can be adjusted. It is also possible to set up a time server (NTP Time Server) to automatically keep the system time up to date.



Name	Description	Standard
Router Time	Router time	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 can be used to synchronize the time with the connected device.
Timezone	Set time zone	Selectable time zone
Auto Daylight Savings Time	Automatic changeover summer time/winter time	Disabled
Auto Update Time	Time of the automatic time update	Disabled
NTP Time Servers (after enabling the “Auto Update Time” option)	Setting for NTP time server (maximum three entries)	pool.ntp.org

3.5 Admin Access

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



Name	Description	Standard
User-name/Password		
Username	Username for login to the configuration page	adm
Old Password	To change the password, it is necessary to enter the old password	123456
New Password	Enter new password	
Confirm New Password	Enter new password again	
Connection Management		
Enable	Select to enable	Enabled
Service Type	HTTP/HTTPS/TELNET/SSH	80/443/23/22
Local Access	Enabled - allow router to be managed over LAN (e.g. : HTTP)	Enabled
Remote Access	Enabled - Allow the TK100 to be managed over WAN (e.g. : HTTP)	Enabled
Description	Describe management parameters (without effect on TK100)	
Non-privileged users		
Username	Create username without administrator rights	
Password	Create password for user without administrator rights	
Andere Parameter		
Login Timeout	Set log timeout, after this value the configuration page will be disconnected and you have to log in again	

3.6 System Log

Settings 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 Adress/Port (UDP)	Set IP address and port of the remote protocol server	Port: 514
Log to Console	Output of the log on the serial interface	Disabled

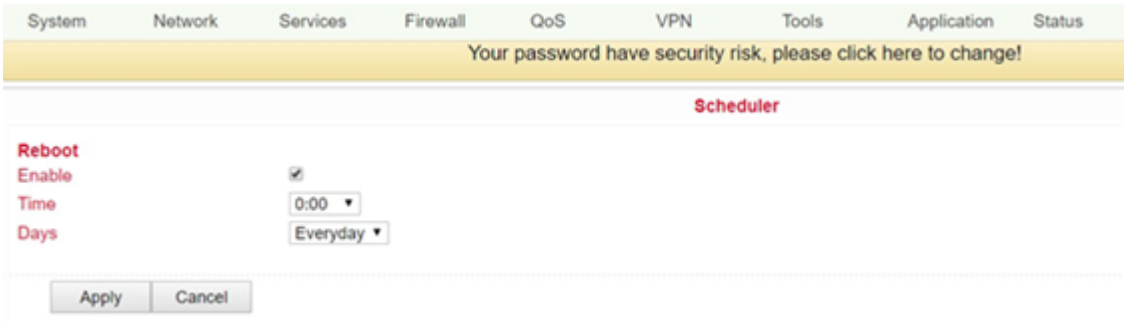
3.7 Configuration Management

Backup and import of router configurations, as well as reset to factory settings of the router and backup or restore the provider data. You can reach this menu item via ***System > Config Management***.

Name	Description
Router Configuration	Upload/save configuration file for import/backup
Restore default configuration	Click to reset the TK100 (to activate the default configuration, the TK100 must be restarted)
Network Provider (ISP)	To import or save APN, username, password and other parameters from traditional operator
Browse	With the Browse button you can select the file with the settings to be uploaded via Import

3.8 Scheduler

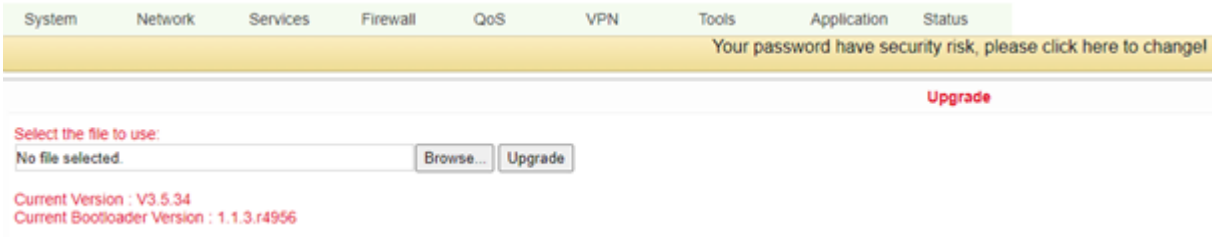
The scheduler is used to set the automatic reboot for the router. You can define the settings for this via ***System > Scheduler***.



Name	Description
Enable	Switches the Auto Reboot on or off
Time	Time when the TK100 router should be rebooted
Days	Select “Everyday” for daily rebooting

3.9 Upgrade

In this area, the router provides you with an interface for updating the firmware. To be reached via **System > Upgrade**.



To update the system, use the ***Select file*** button to select the update file (e.g. TK100-V3.5.xxx.bin) in your file system.

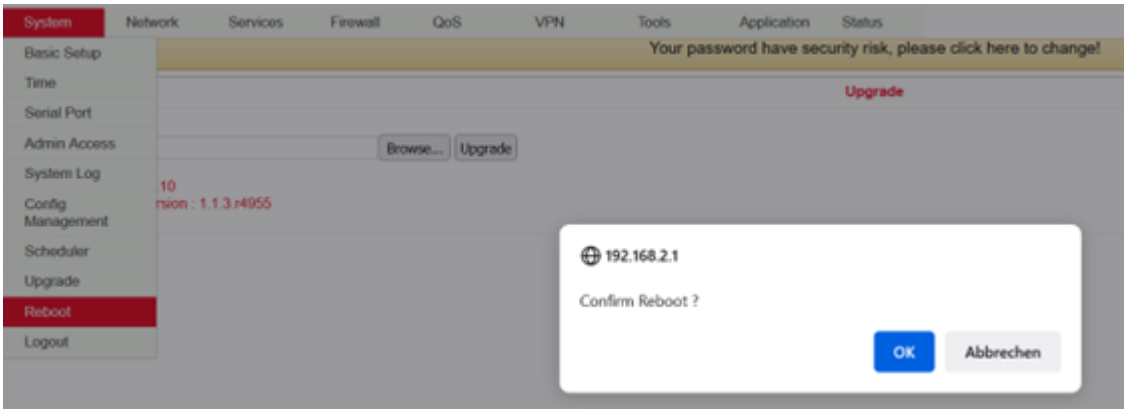
Click the “***Upgrade***” button and confirm the start of the upgrade

After successfully updating the firmware, click ***Reboot*** to restart the TK100.

3.10

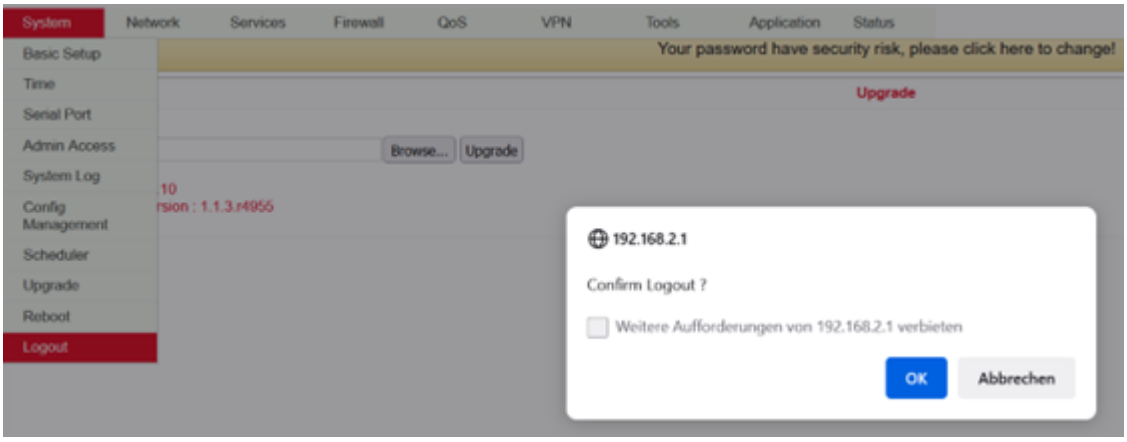
3.11 Reboot

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



3.12 Logout

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



4 Network

Use the network settings to configure Cellular, WAN/LAN Switch, LAN, Link Backup, VRRP, IP Passthrough, Static Route

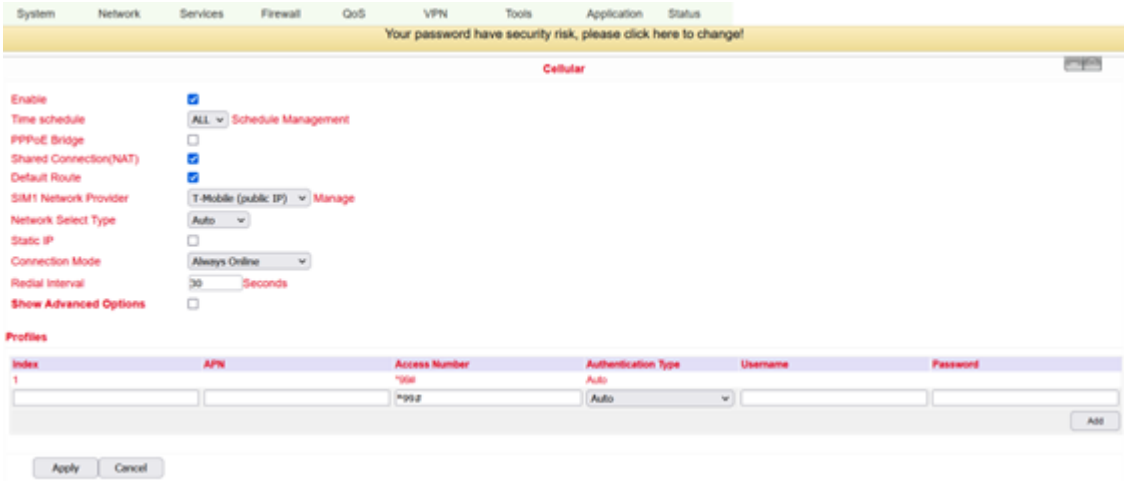
4.1 Cellular

In this menu area you define and configure the dial-up of your router. Can be reached via ***Network > Cellular***.

Check the entries and select a preset network provider under **SIM1 Network Provider**, or add a self-created profile of a provider:

You can obtain the APN, dial-in number, user name and password from your local network provider. Ask them for the details.

Via ***Show Advanced Options*** you can make further settings, such as the PIN code if it is set on the SIM card.

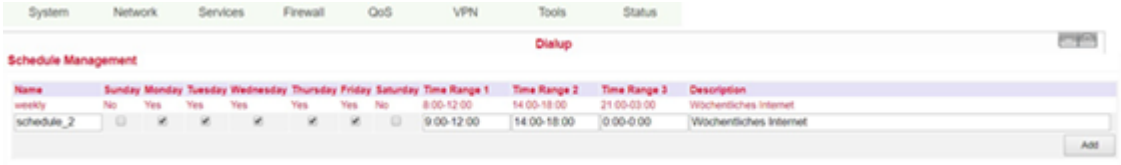


Name	Description	Standard
Enable	Enables the dialup function	Enabled
Time Schedule	Set time for online and offline (see also 3.2.1.1)	All
Shared Connection (NAT)	Enabled - device connected to router	Enabled
Default Route	Mobile radio interface as standard route to the Internet	Enabled
Network Provider (ISP)	Select local ISP, if not listed here select “Custom”	Custom
APN	APN parameters supplied by the provider	internet.t-d1-de (Telekom)
Access Number	Dial-up 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 dial-up fails, the TK router dials again after this interval	30 seconds
Show Advanced Options	Allows configuring advanced options	Disabled
PIN Code	Field for the PIN number of the SIM card	Empty
MTU	Set MTU (Maximum Transmisson Unit)	1500
Authentication Type	PAP, CHAP	Auto
Use Peer DNS	Enable the 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 detection; empty field means none is available	Empty
ICMP Detection Interval	Set interval for ICMP detection	30 seconds
ICMP Detection Timeout	Set timeout for ICMP detection (TK100 is restarted on ICMP timeout)	20 seconds
ICMP Detection Retries	Set maximum number of retries if ICMP fails	5

4.1.1 Schedule Management

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

Here you can run your own dialup strategy, i.e. you can specify here over three time ranges when the router should be online.

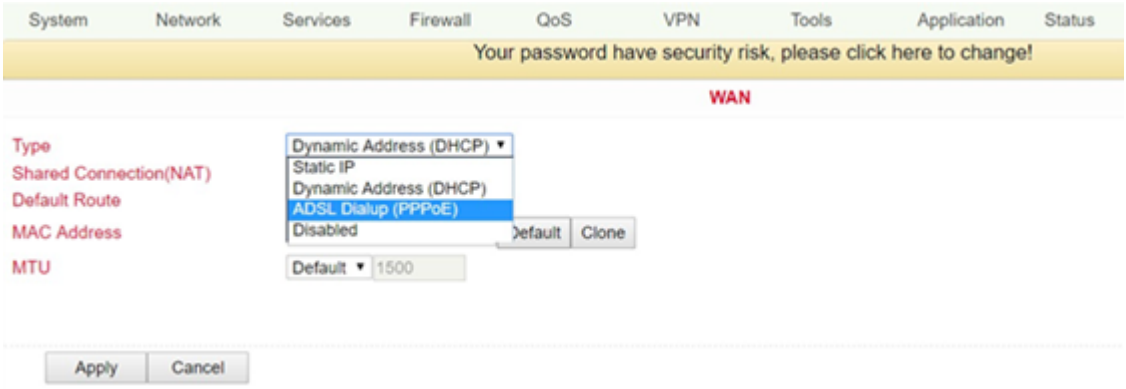


Name	Description	Standard
Name	Name for the schedule	Schedule_1
Sunday	Sunday	Empty
Monday	Monday	Enabled
Tuesday	Tuesday	Enabled
Wednesday	Wednesday	Enabled
Thursday	Thursday	Enabled
Friday	Friday	Enabled
Saturday	Saturday	Empty
Time Range 1	Set time range 1	9:00 - 12:00
Time Range 2	Set time range 2	14:00 - 18:00
Time Range 3	Set time range 3	0:00 - 0:00
Description	Describe configuration	Empty

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

4.2 WAN/LAN Switch

Here you can set up a new WAN (Wide Area Network) or make settings for your LAN. To be reached via ***Network > WAN/LAN Switch***. Under this tab you can decide whether the port should be used for WAN or LAN.



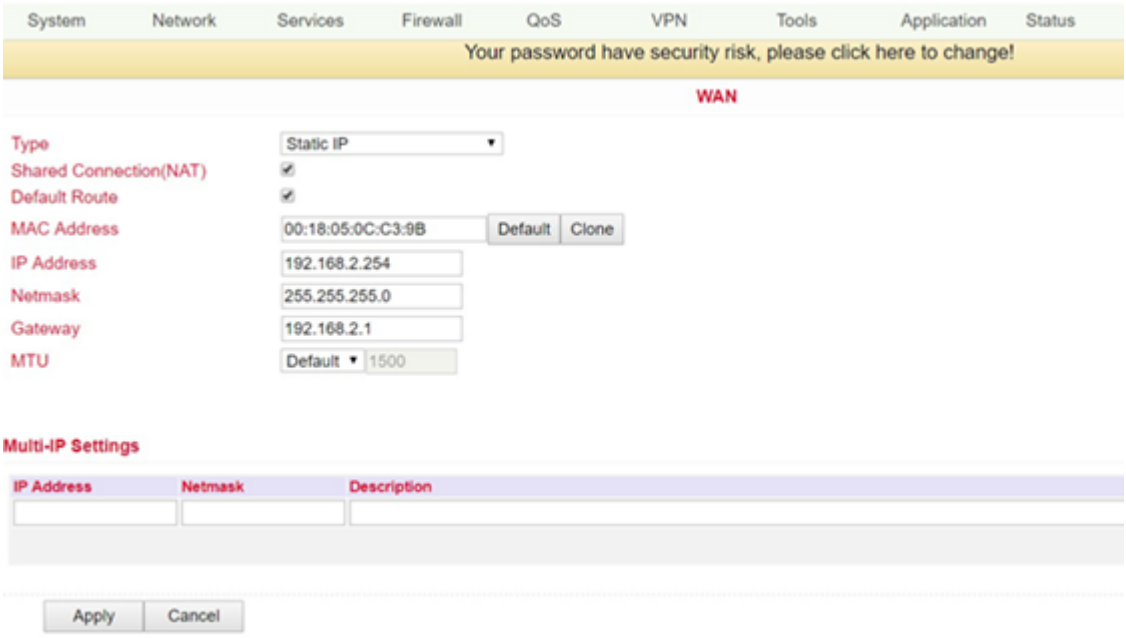
On this page the type of the WAN port can be set:

Name	Description	Standard
Type	Static IP Dynamic Address (DHCP) ADSL Dialup (PPPoE) Disabled	Disabled

Only one WAN type can be enabled at a time. Enabling one type disables another.

4.2.1 Static IP

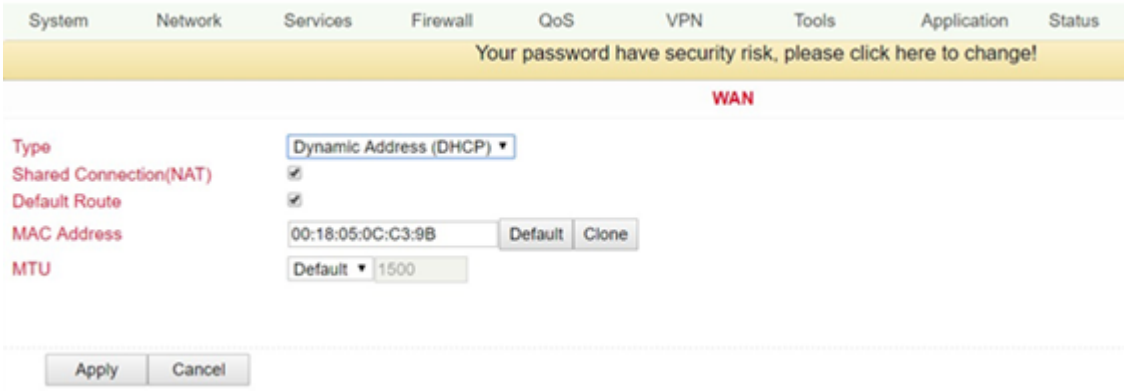
Static IP can also be used for configuring the LAN.



Name	Description	Stan-dard
Type	Static IP	Dis-abled
Shared Connection (NAT)	Enabled - local device connected to router can access the Internet	En-abled
Default Route	Mobile radio interface as standard route to the Inter-net	En-abled
MAC Adress	Set MAC address (button Default = standard, 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	Set the Maximum Transmission Unit (MTU), the op-tions “Default” and “Manual” are possible.	Default = 1500
Multi-IP Settings (a maximum of 8 addi-tional IP addresses can be defined)		
IP Address	Set another IP address for LAN	Empty
Netmask	Set netmask	Empty
Description	Describe settings	Empty

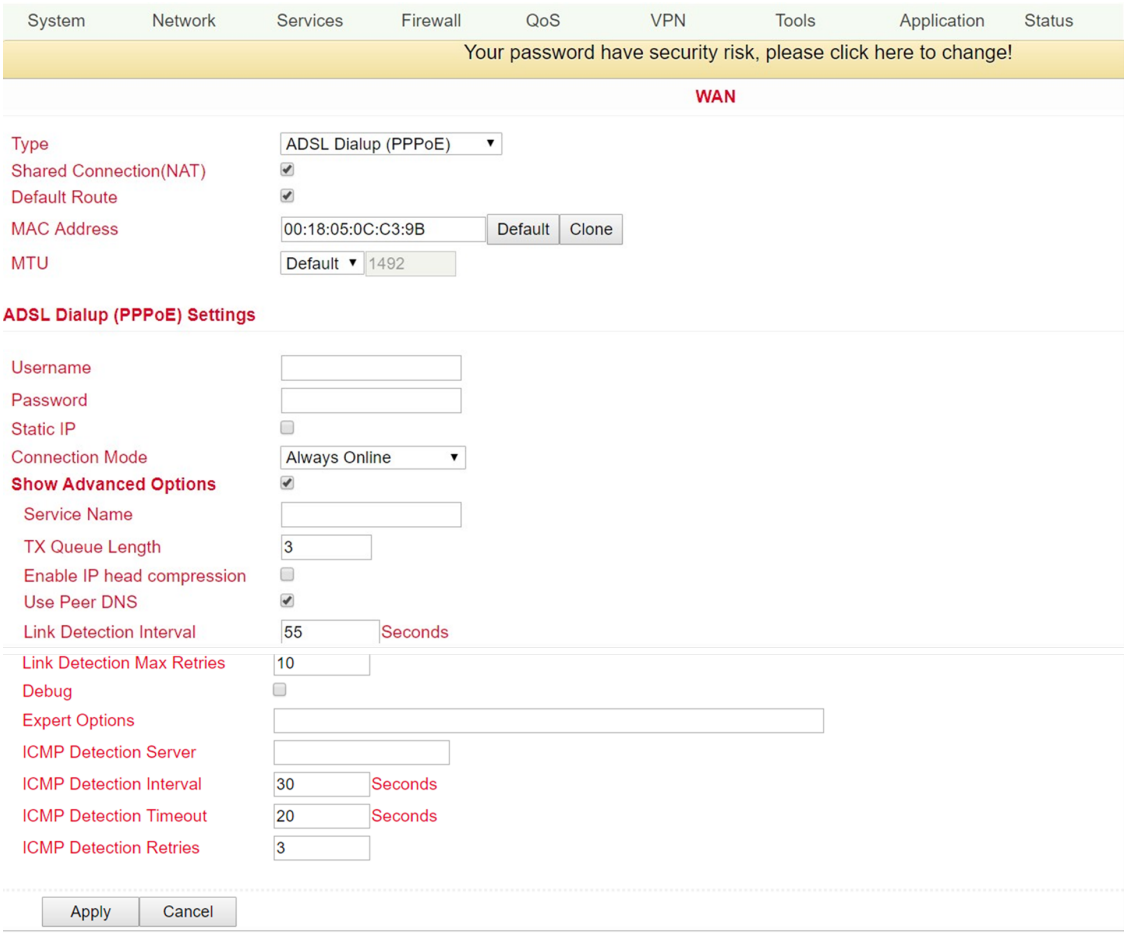
4.2.2 Dynamic Address (DHCP)

Dynamic Address can also be used for LAN settings.



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

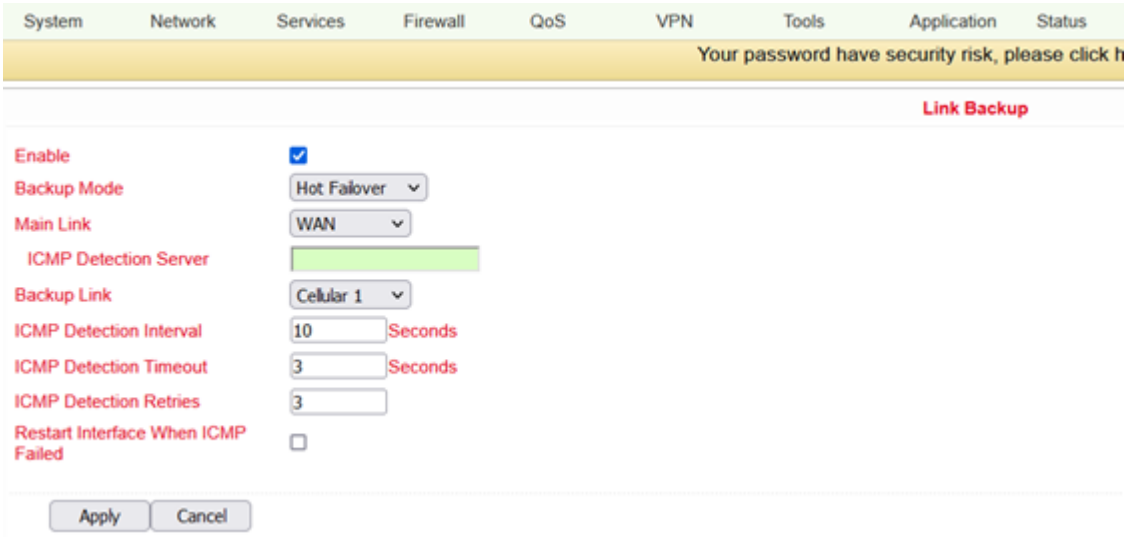
4.2.3 ADSL Dialup (PPPoE)



Name	Description	Standard
Type	ADSL Dialup (PPPoE)	Disabled
Share Connection (NAT)	Enabled - local device connected to router can access the Internet	Enabled
Default Route	Mobile radio interface as standard route to the Internet	Enabled
MAC Address	Set MAC address	
MTU	Set the maximum transmission unit (MTU), the options “Default” and “Manual” are possible	Default = 1492
ADSL Dialup (PPPoE) Settings		
Username	Set username for dialing in	Empty
Password	Set password for dialing in	Empty
Static IP	Enable static IP addresses	Disabled
Connection Mode	Set connection mode (“Connect on Demand”/”Always Online”/”Manual”)	Always Online
Show Advanced Options		
Show advanced options	Enable advanced configuration	Disabled
Service Name	Here you can enter a name for the service	Empty
TX Queue Length	Set the length of the transfer queue	3
Enable IP head compression	Click to enable IP header compression	Empty
Use Peer DNS	Enable peer DNS for users	Disabled
Link Detection Interval	Set interval for connection detection	55 seconds
Link Detection Max Retries	Set maximum number of retries for link detection	10 (times)
Debug	Select to enable debug mode	Disabled
Expert Options	Set 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 maximum number of retries for ICMP detection	3

4.3 Link Backup

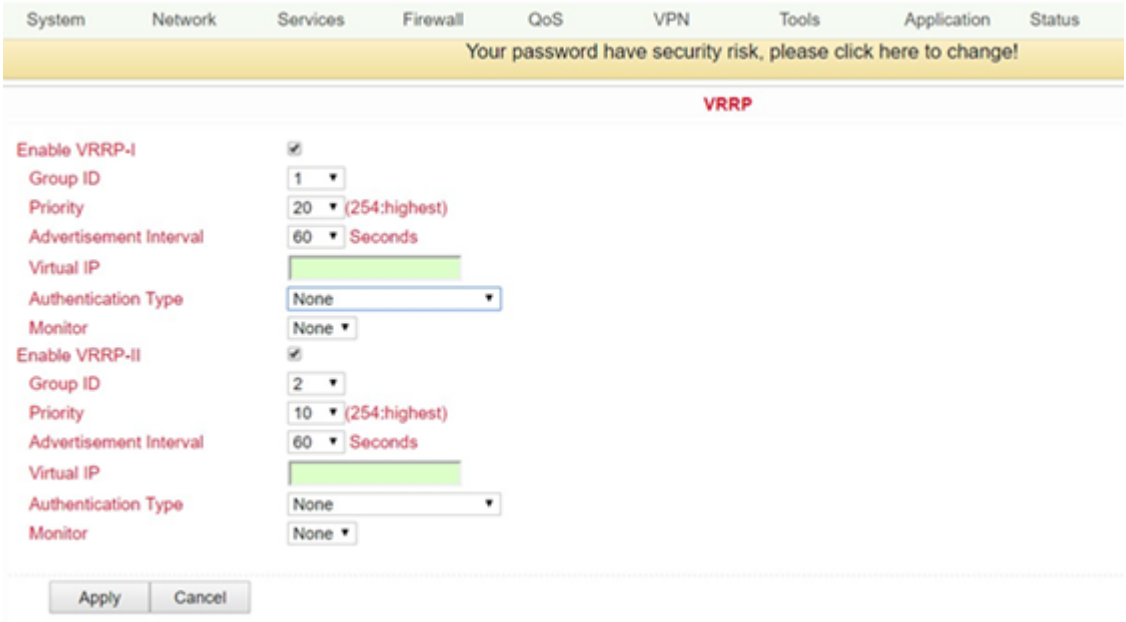
This option secures connections between wireless WAN and Ethernet WAN. If one WAN fails, the TK100 automatically uses the other. You can configure this under ***Network > Link Backup***.



Name	Description	Standard
Enable	Enable the connection backup service	Disabled
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	Enabled
ICMP Detection Interval	Time interval between ICMP packets	10
ICMP Detection Timeout	Timeout for the individual ICMP packets	3 (seconds)
ICMP Detection Retries	If no retry of ICMP detection was successful, the backup connection is selected	3
Backup Link	Select backup link	Dialup
Backup Mode	Hot Backup / Cold Backup	Hot Backup

4.4 VRRP

The Virtual Router Redundancy Protocol (VRRP) is a method for increasing the availability of important gateways in local networks by means of 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, the logical router is assigned a virtual IP address and a virtual MAC address. One of the routers within the group is defined as the virtual master router, which then binds the virtual MAC address and the virtual IP address to its network interface and informs the other routers of the group, which act as virtual backup routers. You can set up this function under ***Services > VRRP***.

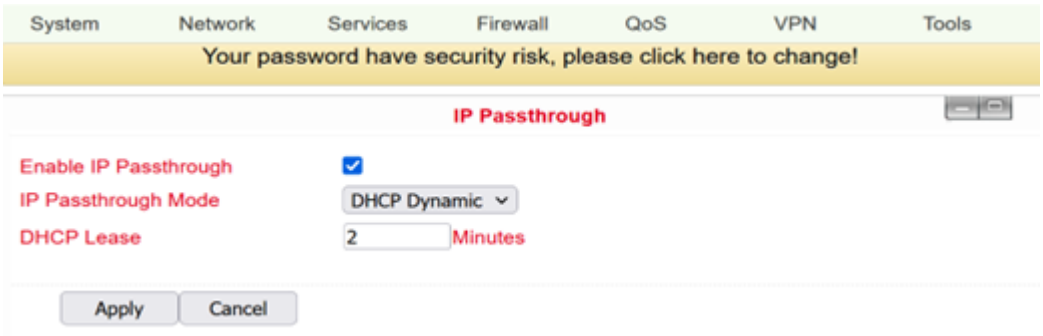


The TK100 series offers the possibility to create two different VRRP (VRRP I and VRRP II) groups.

Name	Description	Standard
Enable VRRP-I	Select to enable VRRP	Disabled
Group ID	Select group ID for router (range 1-255)	1
Priority	Select priority for router (range 1-254)	20 (the larger the number, the higher the priority)
Advertisement Interval	Set advertisement interval	60 seconds
Virtual IP	Set virtual IP address 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	Disabled
Monitor	Checking the WAN connection	None
Enable VRRP-II	Select to activate VRRP	Disabled
Group ID	Select group ID for router (range 1-255)	2
Priority	Select priority for router (range 1-254)	10 (the larger the number, the higher the priority)
Advertisement Interval	Set advertisement interval	60 seconds
Virtual IP	Set virtual IP for the 2nd 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	Disabled
Monitor	Checking the WAN connection	None

4.5 IP Passthrough

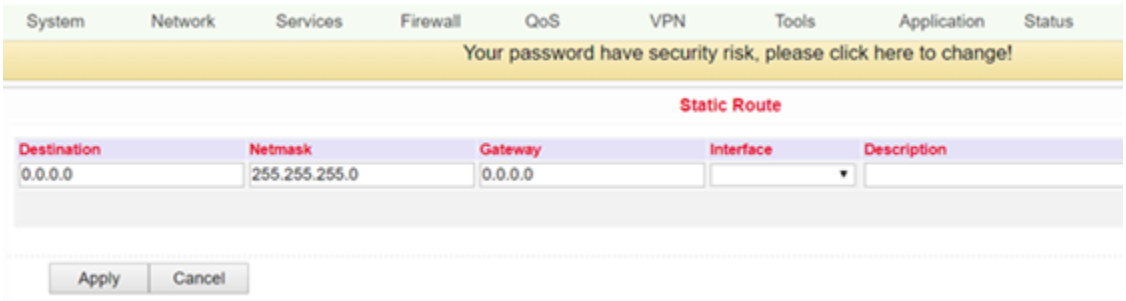
Here you can assign the WAN IP to a device connected to a LAN port.



Only one device can get this IP address and access the Internet. The LAN port should be of the Static type. The function does not work with a link backup.

4.6 Static Route

Here it is possible to add static routes. Static routes provide your router with additional routing information. Under normal circumstances, the router has sufficient information when configured for Internet access, and no additional static routes need to be configured. Static routes need to be set only in exceptional circumstances, such as when your network contains multiple routers or IP subnets. You can add static routes under ***Network > Static Route*** by clicking the Add button.



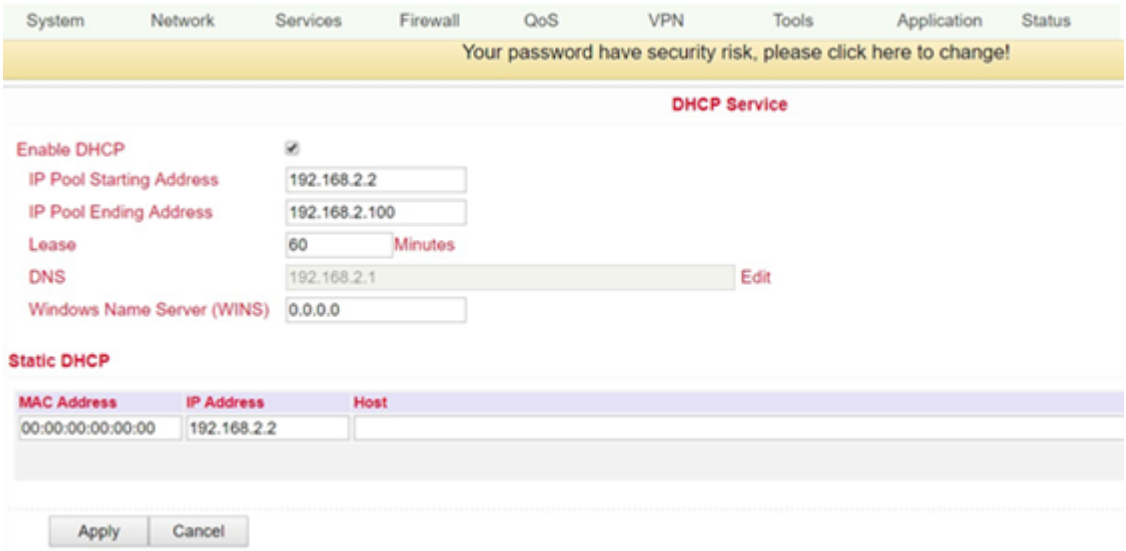
Name	Description	Standard
Destination	Set IP address of the destination	Empty
Netmask	Set subnet mask of the destination	255.255.255.0
Gateway	Set gateway of the destination	Empty
Interface	Optional LAN/WAN port access to destination	Empty
Description	Freely selectable name for the static route	Empty

5 Services

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

5.1 DHCP Service

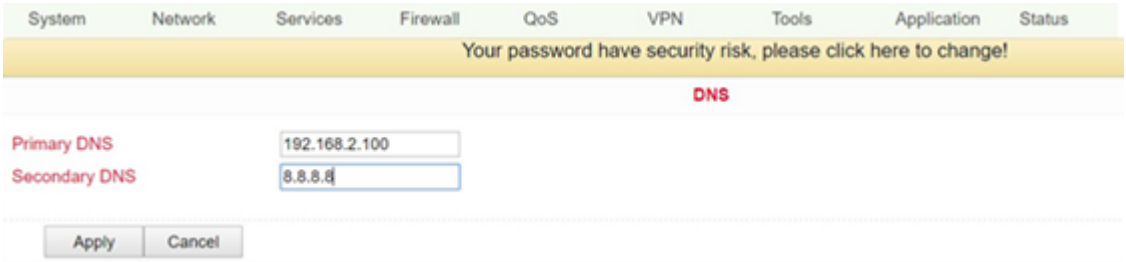
The Dynamic Host Configuration Protocol (DHCP) is a communication protocol in network technology. It enables the assignment of the network configuration to clients by a server. In this way, devices in the network can be assigned IP addresses dynamically. You can reach this service under ***Services >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



Name	Description	Standard
Enable DHCP	Click to enable DHCP	Enabled
IP Pool Starting Address	Set start IP address of the DHCP pool	192.168.2.2
IP Pool Ending Address	Set 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 (a maximum of 20 IP addresses can be set)		
MAC Address	Set MAC address of a designated IP address	Empty
IP Address	Set static IP address	192.168.2.2
Host	Set hostname	Empty

5.2 DNS

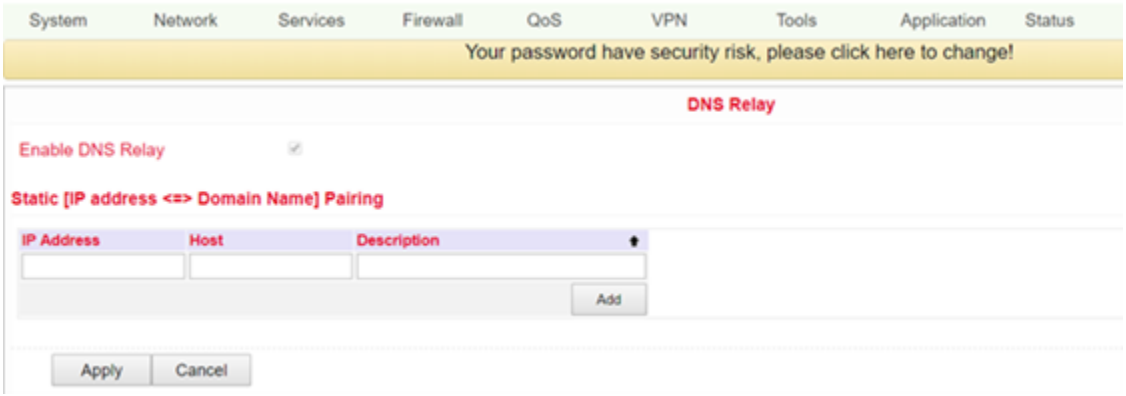
Up to two DNS servers can be entered here if the router is part of a domain network that uses DNS for address resolution. You can enter the data under ***Network > DNS***.



Name	Description	Standard
Primary DNS	Set Primary DNS	Empty
Secondary DNS	Set Secondary DNS	Empty

5.3 DNS Relay

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

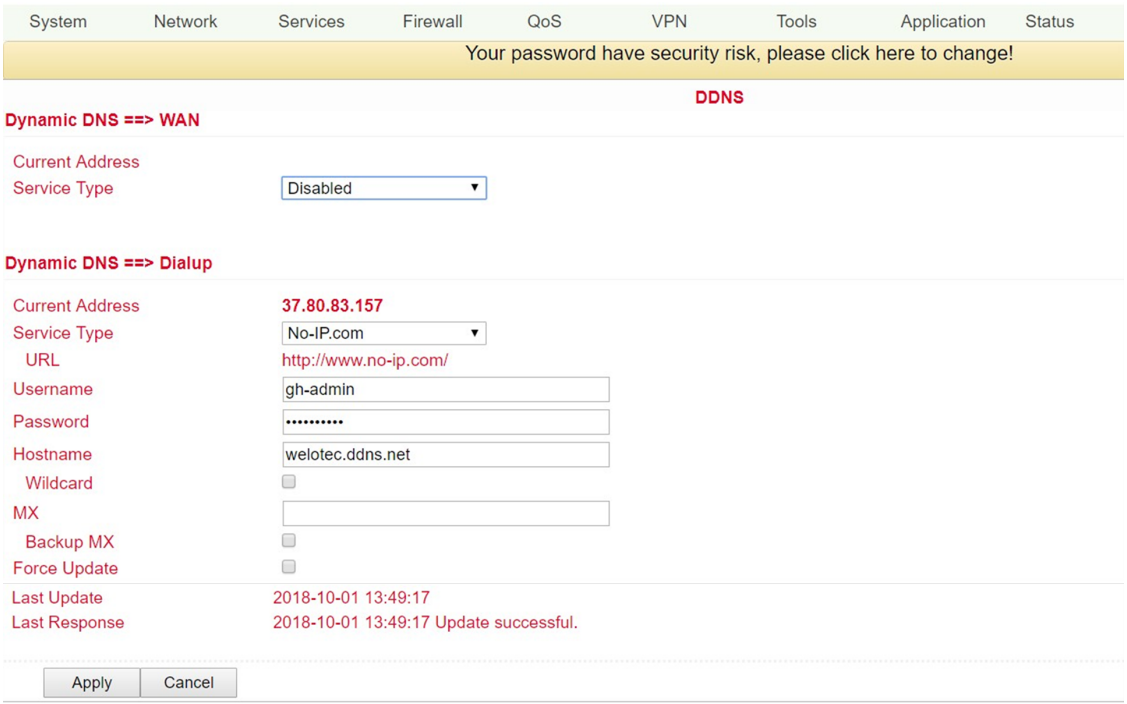


With the ***Add*** button up to 20 DNS pairs can be created.

Name	Description	Standard
Enable DNS Relay	Click to enable DNS forwarding	Enabled (after enabling DHCP)
Static (IP Address <-> Domain Name) Pairing (höchstens 20 DNS-Paare)		
IP Address	Set IP address <-> DNS pairs	Enable
Host	Set IP address name <-> DNS pairs	Empty
Description	Describe IP address <-> DNS pairs	Empty

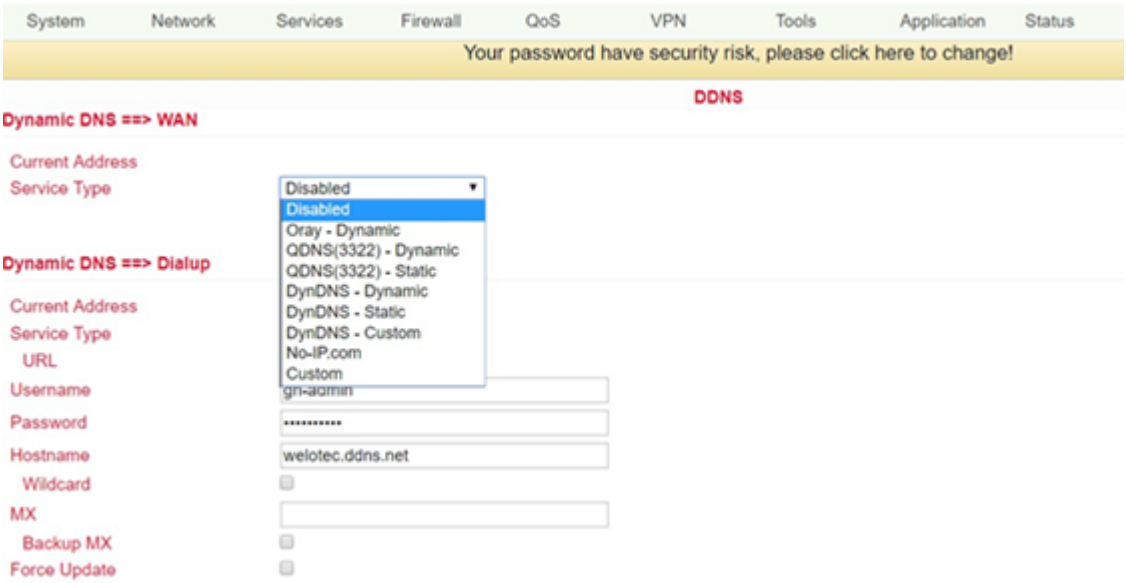
5.4 DDNS (Dynamic DNS)

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, a secure setup, e.g. of a VPN tunnel, is not possible. Therefore one uses providers of dynamic DNS servers, which make sure that your WAN connection always gets the IP address. You can reach the configuration via ***Network > DDNS***.

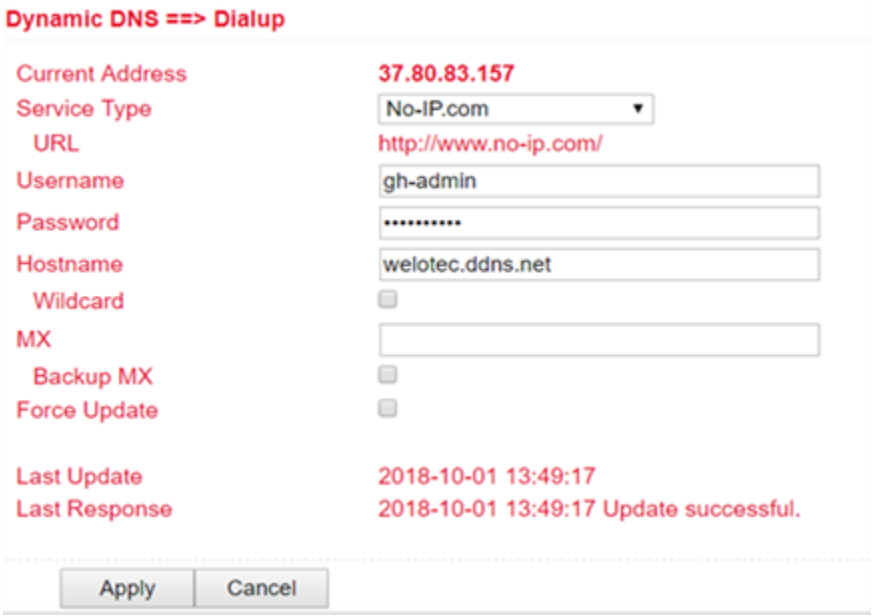


Name	Description	Standard
Current Address	Show current IP address	Empty
Service Type	Select DDNS provider	Disabled

There are various setting options for different DDNS service providers. These are selected via the service type.



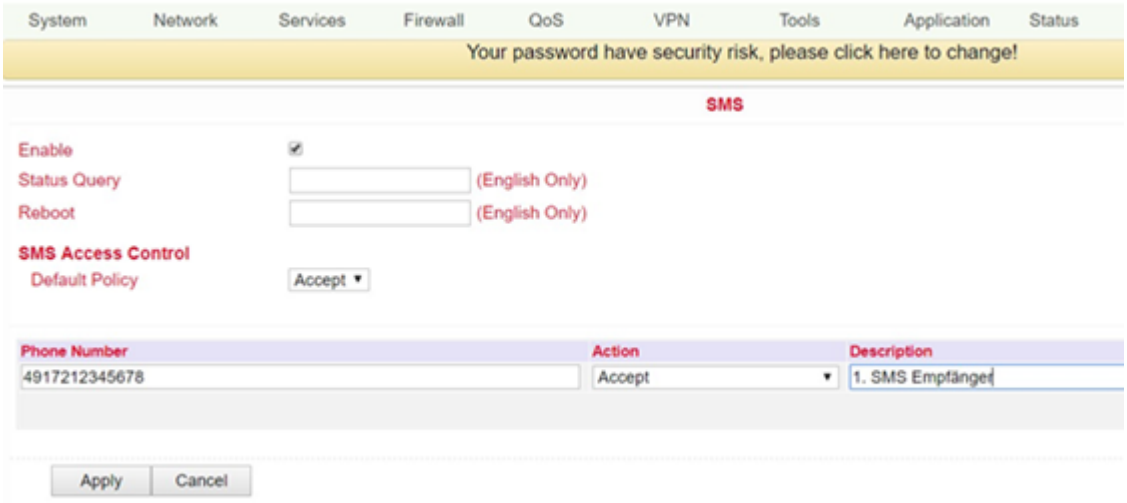
No-IP is used here as an example for the setup. For this, you need a No-IP account, which you have to create yourself. There are various providers here, some of which are free of charge, but some of which are subject to a charge. The assignment of the Dynamic DNS can be assigned to the WAN as well as to the dialup connection.



Name	Description	Standard
Service Type	DynDNS - Dynamic	Disabled
URL	http://www.dyndns.com/	gesetzt
Username	Registrierter Benutzername für DDNS	Empty
Password	Registriertes Kennwort für DDNS	Empty
Hostname	Registrierter Hostname für DDNS	Empty
Wildcard	Kann aktiviert werden, wenn Wildcard genutzt werden soll	Disabled
MX	Eintragen eine MX-Records	Empty
Backup MX	Can be activated if MX-Record should run as backup	Disabled
Force Update	Forces the account to be updated	Disabled
Last Update	Shows when the IP address was last changed	
Last Response	Indicates when the service was last communicated with	

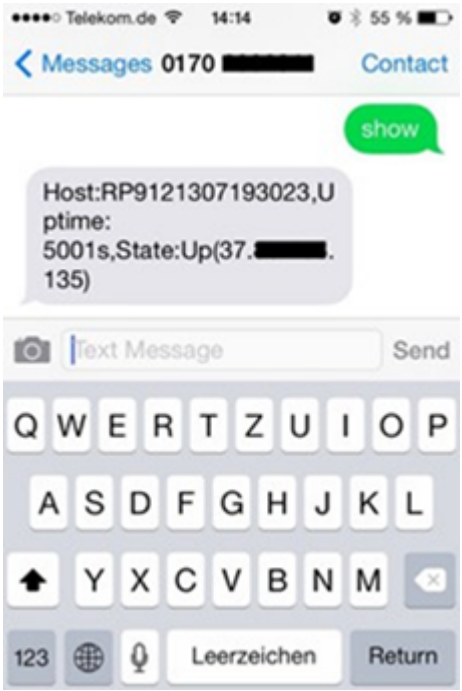
5.5 SMS

The TK100 can be reached via SMS from the 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	Disabled
Status Query	Set status request SMS to display the status of the router via SMS (e.g. : show status)	Empty
Reboot	Lets the router reboot	Empty
SMS Access Control		
Default Policy	Block or Accept control SMS from specific phone.	Accept
Phone Number	Enter the phone numbers for sending SMS to the router. The format for the mobile number is 491712345678 (please do not enter +49 or 0049)	Empty
Action	Accept or block the previously entered phone number	Accept
Description	Description for the created data set	Empty

To be able to send an SMS to the router, the mobile number of the inserted card must be known. The SMS is then sent to this number.



SMS that you receive on your cell phone:

Host: (SN);

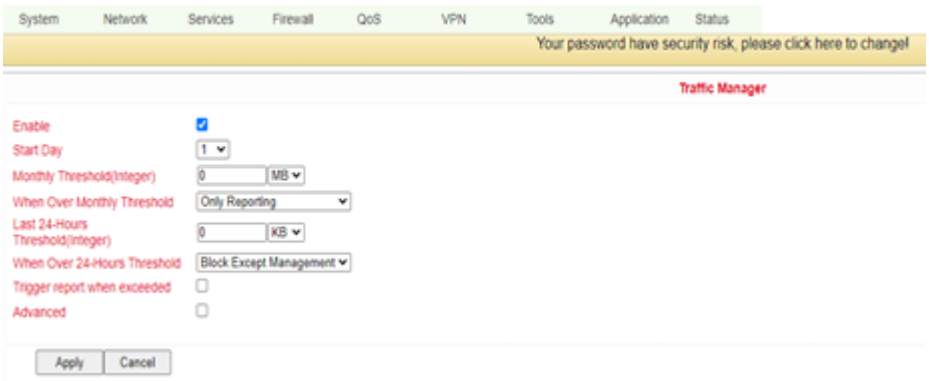
Uptime: (the operating time of the router at the time of this restart);

State: (Online/Offline) (Wireless WAN IP)

LAN: (Ready) (LAN-IP)

5.6 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***.

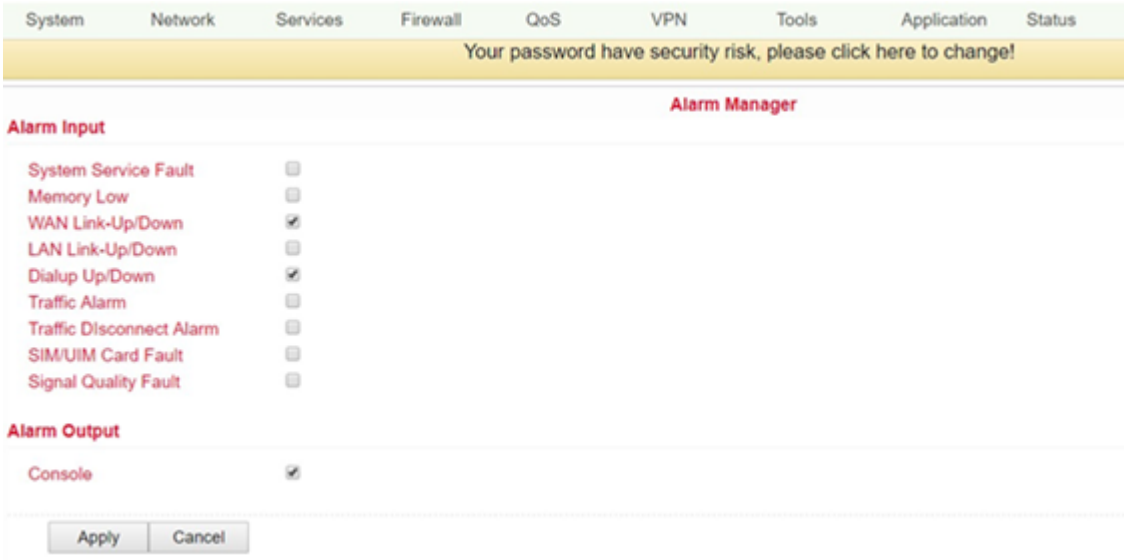


Name	Description	Standard
Enable	Click to enable or disable SMS control	Disabled
Alarm Threshold	Sets the amount of data in MB per month at which an alarm should be generated. If 0 is set as the value, no alarm is generated	Empty
Disconnect Threshold	Wird der eingestellte Wert erreicht, wird die Einwahlverbindung unterbrochen	Empty

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

5.7 Alarm Manager

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



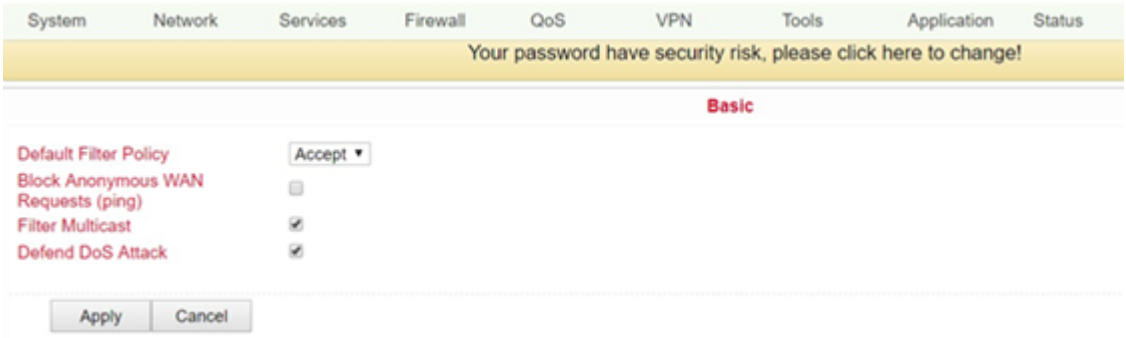
Name	Description	Standard
Alarm Inout	Select here the areas for which an alarm is to be generated	None
Alarm Output	Here you can choose whether the alarms should be issued via the console or not	Selected

6 Firewall

The ***Firewall*** menu item allows you to set the parameters for the router's firewall. Various settings are possible here.

6.1 Basic

Here you can configure the basic settings of the firewall.



Name	Description	Standard
Default Filter Policy	The options "Accept" and "Block" are possible.	Accept
Block Anonymous WAN Request (ping)	Enable to block ping requests generated anonymously from the network	Disabled
Filter Multicast	Click to enable filtering of Multicast	Enabled
Defend DoS Attack	Click to enable Defend against DoS attacks	Enabled

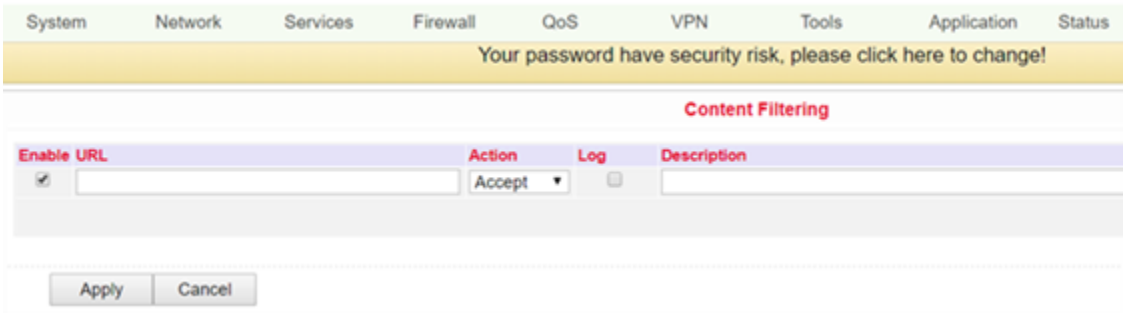
6.2 Filtering

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

Name	Description	Standard
Enable	Click to enable filtering	Enabled
Protocol	Selection of the protocol. Possible options are “TCP” / “UDP” / “ICMP”	All
Source	Set source IP address	Empty
Source Port	Set source port if corresponding protocol was selected	Empty
Destination	Set destination IP	Empty
Destination Port	Set destination port if corresponding protocol was selected	Empty
Action	Selection whether settings should be allowed (Accept) or blocked (Block)	Accept
Log	Click to enable logging of settings	Disabled
Description	Describe configuration	Empty

6.3 Content Filtering

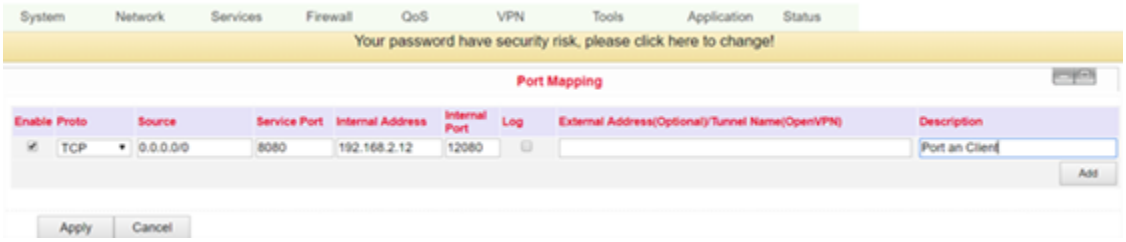
The content filter in the firewall allows to filter the call of special URL’s, which can then be blocked or allowed. You can create the configuration under ***Firewall > Content Filtering***.



Name	Description	Standard
Enable	Enable or disable the content filter function	Enabled
URL	Enter the URL to block or filter	Empty
Action	Selection whether URL is blocked (Block) or allowed (Accept)	Erlaubt
Log	Can be enabled for logging	Disabled
Description	Describe configuration	Empty

6.4 Port Mapping

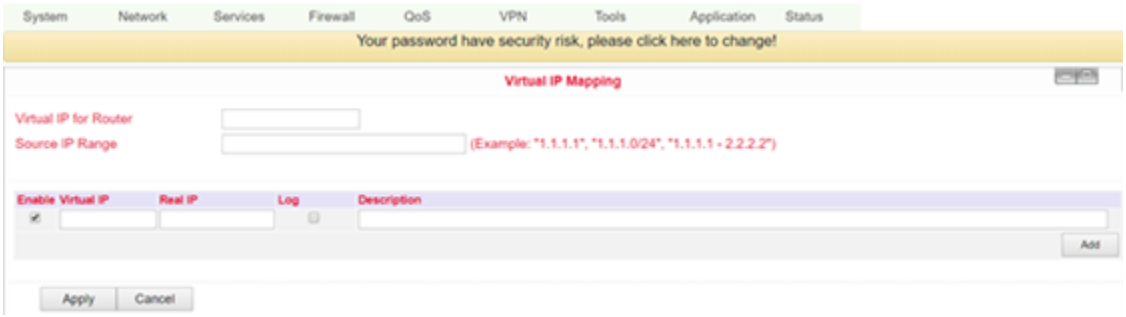
NAT-PMP (NAT Port Mapping) allows a computer in a private network (behind a NAT router) to automatically configure the router so that devices behind the router can be reached from outside the private network. It essentially controls what is known as port forwarding. NAT-PMP, like UPnP, allows a program to request all incoming data from outside on a specific TCP or UDP port. You can perform the configuration under ***Firewall > Port Mapping***.



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

6.5 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 under ***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	Disabled
Description	Describe configuration	Empty

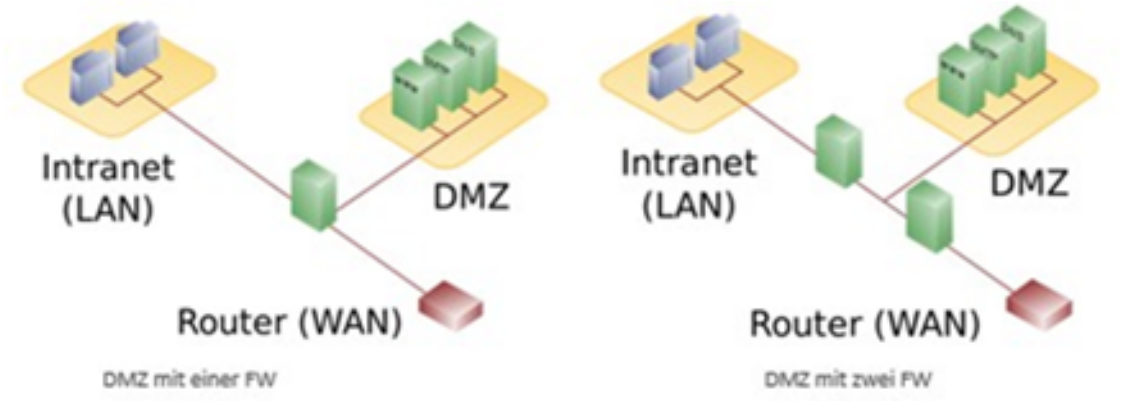
6.6 DMZ

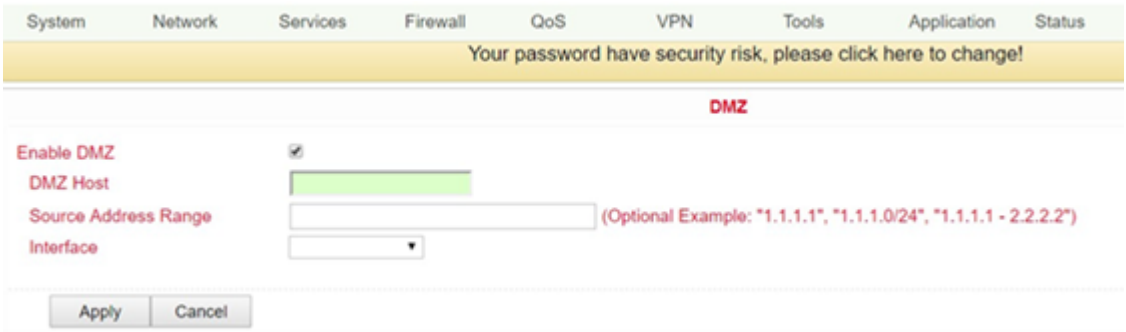
A Demilitarized Zone ***(DMZ)*** refers to a computer network with security-controlled access to the servers connected to it.

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 accessible services while protecting the internal network (LAN) from unauthorized access from the outside.

The purpose is to make services of the computer network available to both the Internet (WAN) and the intranet (LAN) on a secure basis.

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





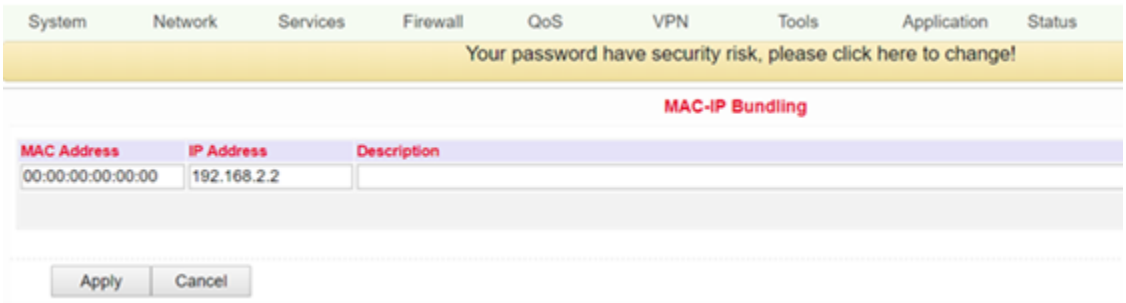
By mapping all ports and the external PC, you can access all ports of the device connected to the TK100.

With this function it is not possible to assign the management port of the TK100 (e.g.: 80 TCP) to the port of the device. To forward port 80, change the management port of the router under ***System > Admin Access***.

Name	Description	Standard
Enable DMZ	Click to enable DMZ	Disabled
DMZ Host	Set DMZ host IP	Empty
Source Address Range	Set IP address with restricted IP access	Empty
Interface	Selection of the corresponding interface	Empty

6.7 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 can 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 will gain access to the external network.

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

6.8 NAT

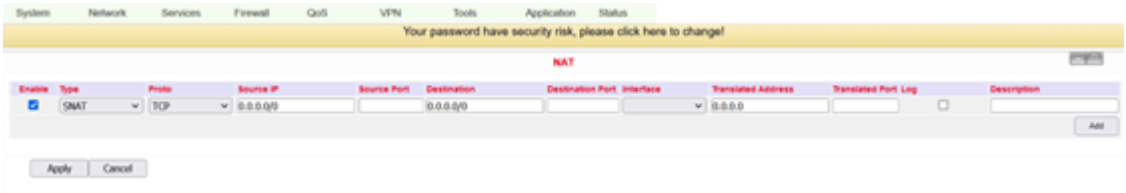
In computer networks, Network Address Translation (NAT) is the collective term for procedures that automatically replace address information in data packets with other information in order to connect different networks. They are therefore typically used on routers.

Use of Source NAT (SNAT)

It allows devices with private network addresses to connect to the Internet. Private IP addresses cannot usually be routed by the provider, so they must be translated into a public, routable IP address. The TK100 has implemented this function, which enables communication between different networks. In addition, a relevant security aspect is found in NAT, since a public IP address cannot be traced back to the associated private IP address.

Use of Destination NAT (DNAT)

This is used to offer services that are operated on computers under a single IP address. It is often referred to as port mapping or port forwarding.



Configuration - To configure NAT, go to the ***Firewall*** menu item and select the ***NAT*** subitem - Here you will find a list of all existing NAT rules - New NAT rules can be added using the ***Add*** button

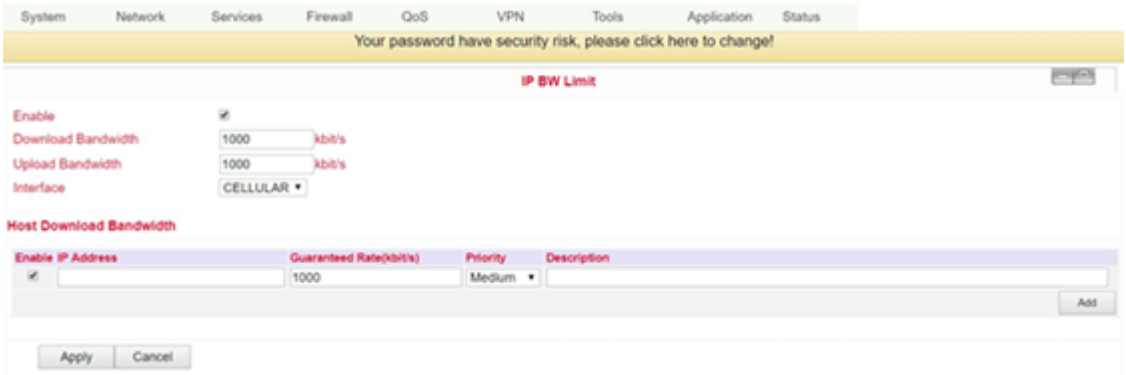
7 QoS

In the TCP/IP world, QoS describes the quality of a communication service from the user's point of view. Network service quality is often defined on the basis of 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, attempts are made to mark data packets with corresponding service classes. Prioritized data packets are then forwarded preferentially 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***".

7.1 IP BW Limit

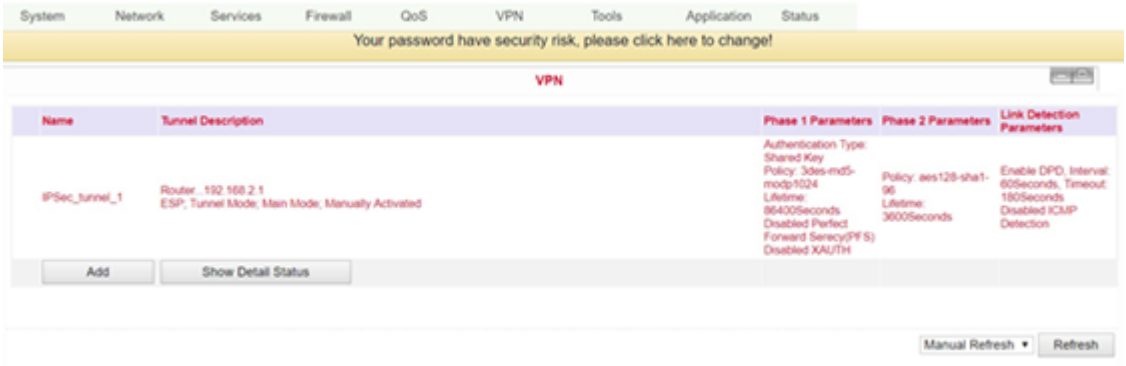
Under the menu item ***QoS*** > ***IP BW Limit*** you can limit the down- or upload bandwidth and bind it to IP addresses, as well as prioritize them.



Name	Description	Standard
Enable	Click to enable	Disabled
Download Bandwith	Set the bandwidth for download	1000 kbit/s
Upload Bandwith	Set the bandwidth for upload	1000 kbit/s
Interface	Selection of the interfaces to which the bandwidth is to be allocated	Cellular
Host Download Bandwith		
Enable	Enable the function	Enabled
IP Address	Specifying the IP address for mapping	Empty
Guaranteed Rate (kbit/s)	Specification of the guaranteed bandwidth in kbit/s	1000
Priority	Priority assignment	Medium
Description	Rule description	Empty

8 VPN

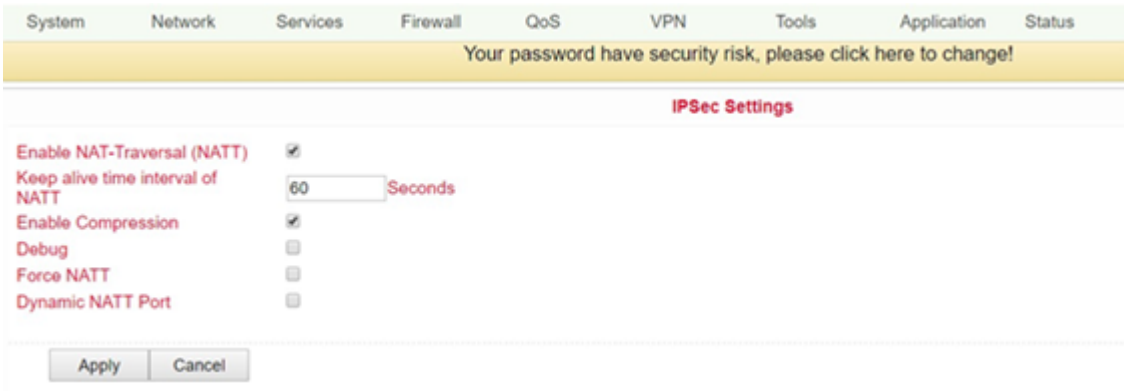
A VPN (virtual private network) is a closed logical network in which the participants are physically separated from each other and connected via an IP tunnel. With this VPN, you can access a local network, e.g. the company network, while on the road or from your home office. This requires VPN software that is both communicating with the network's router and installed on the computer you want to use to access the network. There are different types of VPN connections (tunnels) that can be configured under this menu item on the TK 500 series.



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

8.1 IPSec Settings

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



Name	Description	Standard
Enable NAT-Traversal (NATT)	Click to enable	Disabled
Keep alive time interval of NATT	Set the duration for maintaining the NATT	60 Seconds
Enable Compression	Enable or disable compression	Enabled
Debug	Switch debug mode on or off	Disabled
Force NATT	Switch Force NATT on or off	Disabled
Dynamic NATT Port	Enabling or disabling a dynamic NATT port	Disabled

The address change via NAT is interpreted by a VPN gateway as a security-critical change to the data packets, the VPN negotiation fails, and no connection is established. These problems occur, for example, when dialing in via

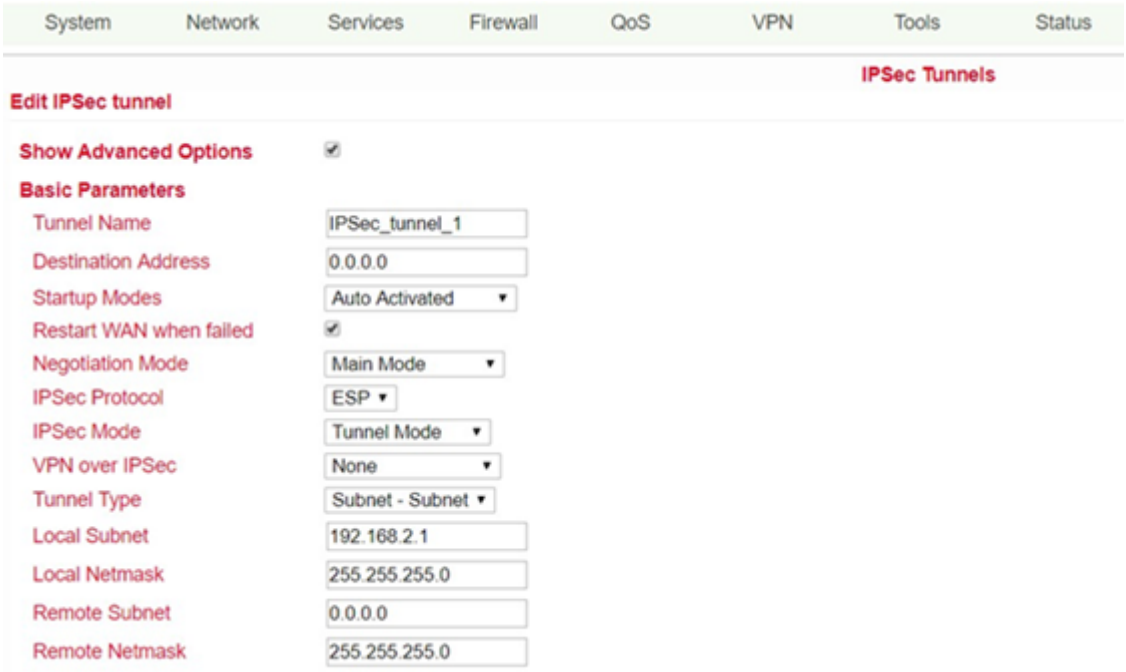
some UMTS mobile networks, where the network operator's servers do not support address conversion in connection with IPSec-based VPNs.

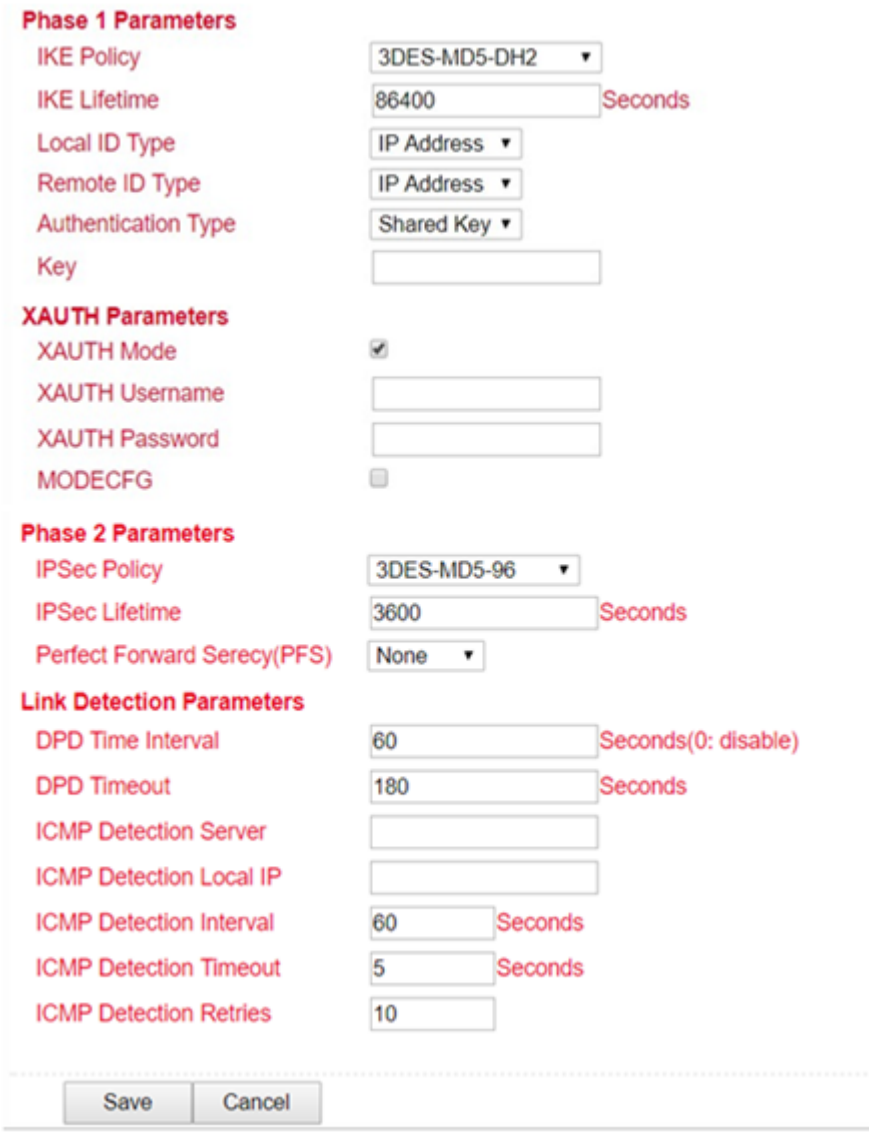
In order to be able to successfully establish a VPN connection in these cases, NATT (NAT Traversal) provides a method to overcome these problems when handling data packets with changed addresses.

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 receiver therefore corresponds to the hash value entered in the packets

8.2 IPSec Tunnels

Via ***VPN > IPSec Tunnels*** you can set up an appropriate tunnel.





This page presents the web-based parameters for the TK100.

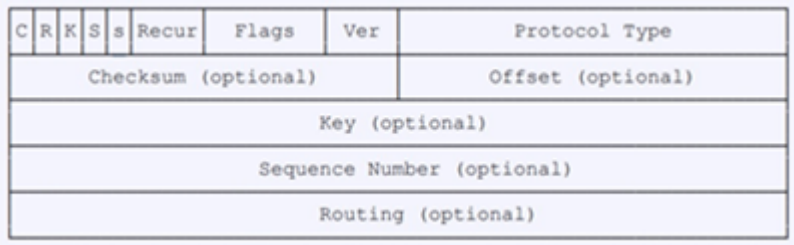
Name	Description
Show Advanced Options	Click to enable Advanced Options
Basic Parameters	
Tunnel Name	Name for the tunnel
Destination Address	Set the destination address of the IPSec VPN server
Startup Modes	Possible modes are “Auto Active” / “Triggered by Data” / “Passive” / “M
Restart WAN when failed	WAN interface is restarted if tunnel establishment fails
Negotiation Mode	Optional: “Main Mode” or “Aggressive Mode”
IPSec Protocol	Optional: “ESP” or “AH”
IPSec Mode	Optional: “Tunnelmode” or “Transport Mode”
VPN over IPSec	L2TP or GRE over IPSec
Tunnel Type	Selection field for various settings

Table 1 – continued from previous page

Name	Description
Local Subnet	Set protected IPSec subnet (Local)
Local Netmask	Set protected IPSec subnet mask (Local)
Remote Subnet	Set protected IPSec subnet (remote)
Remote Netmask	Set protected IPSec subnet mask (remote)
	Phase 1 Parameters
IKE Policy	Multi selection for the policy
IKE Lifetime	Set IKE validity period
Local ID Type	Selection of “FQDN” ; “USERFQDN” or “IP-Address” possible
Remote ID Type	Selection of “IP-Address” ; “USERFQDN” ; or “FQDN” possible
Authentication Type	Selection of “Shared Key” or “Certificate” possible
Key (If the authentication type “Shared Key” is selected)	Set IPSec key for VPN negotiation
	XAUTH Parameters
XAUTH Mode	Enable XAUTH
XAUTH Username	XAUTH Username
XAUTH Password	XAUTH Password
MODECFG	MODECFG
	Phase 2 Parameters
IPSec Policy	Multi-selection list for the policy
IPSec Lifetime	Set IPSec validity period
Perfect Forward Secrecy (PFS)	Optional “Disable”; “Group1”; “Group2”; “Group5”
	Link Detection Parameters
DPD Time Interval	Set DPD Time Interval
DPD Timeout	Set DPD Timeout
ICMP Detection Server	Set server for ICMP detection
ICMP Detection Local IP	Set local IP for ICMP detection
ICMP Detection Interval	Set interval for ICMP detection
ICMP Detection Timeout	Set timeout for ICMP detection
ICMP Detection Max Retries	Set maximum number of retries for ICMP detection

8.3 GRE Tunnels

Generic Routing Encapsulation (GRE) is a network protocol developed by the Cisco company and defined in RFC 1701. GRE can be used to wrap other protocols and thus transport them in an IP tunnel. GRE uses the IP protocol 47, the GRE header is structured as follows:



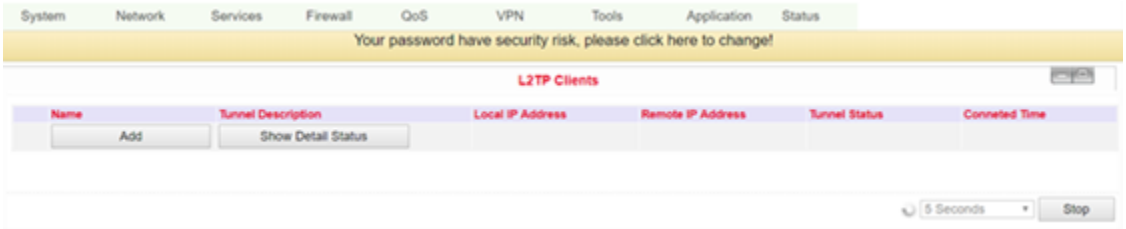
A GRE packet therefore consists of an IP header, a GRE header and the actual payload. You can set up this GRE

tunnel under ***VPN > GRE Tunnels***.

Name	Description	Standard
Enable	Click to enable	Enabled
Tunnel Name	Set name for GRE tunnel	tun0
Local Virtual IP	Set local virtual IP	0.0.0.0
Peer Address	Set peer address	0.0.0.0
Remote Virtual IP	Set virtual IP of the remote network	0.0.0.0
Remote Subnet Address	Set remote subnet address	0.0.0.0
Remote Subnet Netmask	Set remote subnet mask	255.255.255.0
Key	Set the key for the encryption of the tunnel	Empty
NAT	Click to enable NAT function	Disabled
Description	Add description	Empty

8.4 L2TP Clients

Layer 2 Tunneling Protocol (L2TP) is a network protocol that tunnels frames of OSI model link 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 here. You can reach the configuration via ***VPN > L2TP Clients***.



Click on the ***Add*** button to start the configuration of the L2TP client.

Your password have security risk, please click here to cha

L2TP Clients

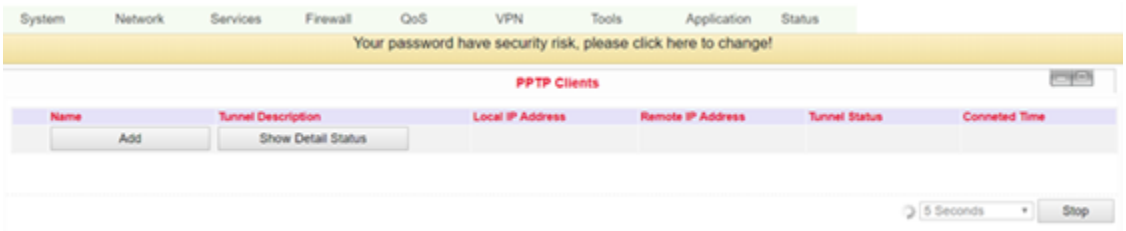
Enable	☑
Tunnel name	L2TP_tunnel_1
L2TP Server	
Username	
Password	
L2TP Server Name	l2tpserver
Startup Modes	Auto Activated
Authentication Type	CHAP
Enable Challenge Secrets	☐
Local IP Address	
Remote IP Address	
Remote Subnet	
Remote Netmask	255.255.255.0
Multi Remote Subnet	☐
Link Detection Interval	60 Seconds
Max Retries for Link Detection	5
Enable NAT	☐
MTU	1500
MRU	1500
Enable Debug	☐
Expert Options(Expert Only)	

Save Cancel

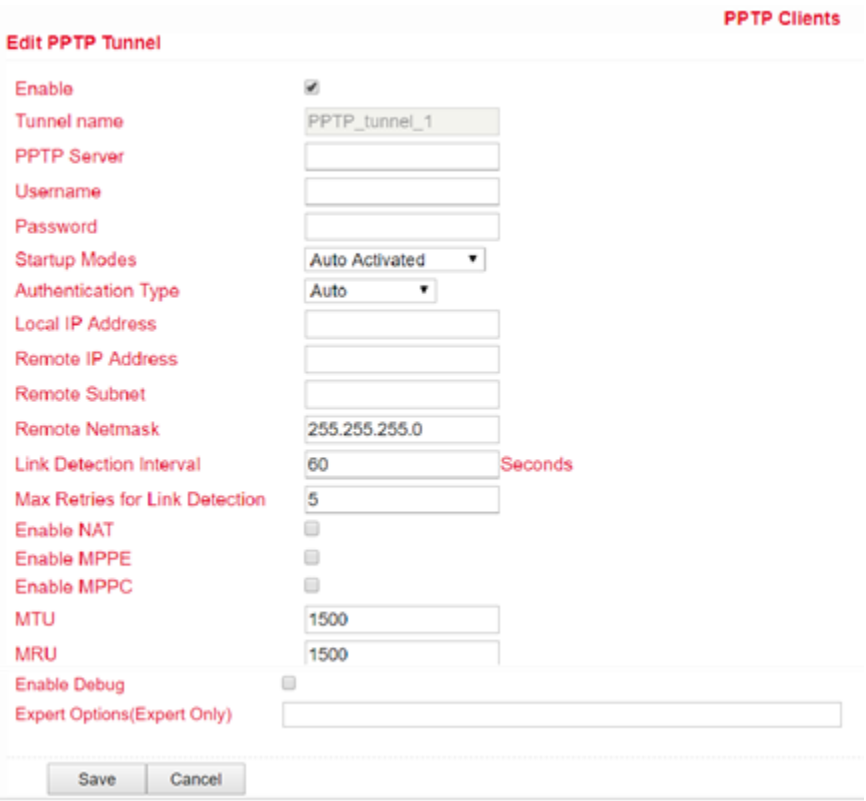
Name	Description	Standard
Enable	Enables the tunnel settings	Enabled
Tunnel Name	Set name for the tunnel	L2TP_TUNNEL_1
L2TP Server	Set the address of the L2TP server	Empty
Username	Set username for server	Empty
Password	Set password for server	Empty
L2TP Server Name	Set names for server	l2tpserver
Startup Modes	Set modes for startup: “Auto Activated”; “Triggered by Data”; “Manually Activated”; “L2TP0-verIPSec”	Auto Activated
Authentication Type	Set authentication type “CHAP”; “PAP”	CHAP
Enable Challenge Secrets	Select to enable secret keys (challenge)	Disabled
Challenge Secrets	If Enable Challenge Secrets is enabled, 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 remote subnet	Empty
Remote Subnet Netmask	Set remote subnet mask	255.255.255.0
Link Detection Interval	Set interval for link detection	60
Max Retries for Link Detection	Set maximum number of retries for link detection	5
Enable NAT	Click to enable NAT	Disabled
MTU	Set MTU parameters	1500
MRU	Set MRU parameters	1500
Enable Debug Mode	Click to enable debug mode	Disabled
Expert Options	Set expert options	Empty

8.5 PPTP Clients

PPTP (Point to Point Tunneling Protocol) is a VPN tunneling method for remote access connections. It is based on the Remote Access Server for Microsoft Windows NT including authentication. A PPTP client is integrated not only 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 on the Add button. To view details of an existing PPTP client, click the ***Show Detail Status*** button. After clicking the ***Add*** button, you can make the following configuration settings.


Edit PPTP Tunnel
Enable
Tunnel name
PPTP_tunnel_1
PPTP Server
Username
Password
Startup Modes
Auto Activated
Authentication Type
Auto
Local IP Address
Remote IP Address
Remote Subnet
Remote Netmask
255.255.255.0
Link Detection Interval
60
Seconds
Max Retries for Link Detection
5
Enable NAT
Enable MPPE
Enable MPPC
MTU
1500
MRU
1500
Enable Debug
Expert Options(Expert Only)
Save
Cancel

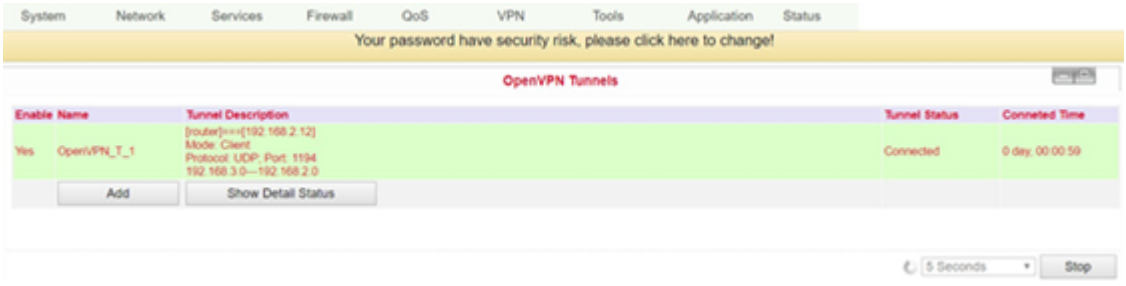
Name	Description	Standard
Enable	Click to enable	Enabled
Tunnel Name	the name for the tunnel (set automatically)	PPTP_tunnel_1
PPTP Server	Set address for PPTP server	Empty
Username	Set username for server	Empty
Password	Set password for server	Empty
Startup Mode	Set modes for start: “Auto Activated”; “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	Set remote subnet	Empty
Remote Subnet Netmask	Set remote subnet mask	255.255.255.0
Link Detection Interval	Set interval for link detection	60
Max Retries for Link Detection	Set maximum number of retries for link 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

8.6 OpenVPN Tunnels

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

OpenVPN is licensed under the GNU GPL and supports operating systems such as Linux, Windows, iOS and a variety of customized Linux-based endpoints such as TK 500 and TK 800 series routers.

On the TK100 configuration page, select the ***VPN > Open VPN Tunnels*** options 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.

Your password have security risk, please

OpenVPN Tunnels

Edit OPENVPN Tunnel

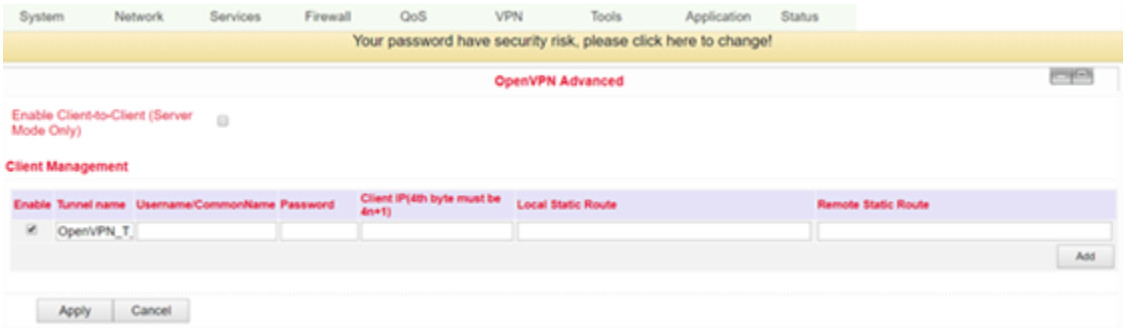
Tunnel name	OpenVPN_T_1
Enable	☑
Mode	Client
Protocol	UDP
Port	1194
OPENVPN Server	192.168.2.12
Authentication Type	X.509 Cert
Pre-shared Key	
Local IP Address	192.168.3.0
Remote IP Address	192.168.2.0
Remote Subnet	
Remote Netmask	255.255.255.0
Link Detection Interval	60 Seconds
Link Detection Timeout	300 Seconds
Renegotiate Interval	86400 Seconds
Enable NAT	☑
Enable LZO	☐
Encryption Algorithms	AES(256)
MTU	1500
Max Fragment Size	
Debug Level	Warn
Interface Type	TUN
Expert Options(Expert Only)	

Save Cancel Delete

Name	Description
Tunnel name	Preset
Enable	Enable this configuration
Mode	Select “Client” or “Server” mode
Protocol	Selection of the “UDP” or “TCP” protocol
Port	Default port for OpenVPN is 1194
OPENVPN Server	IP or DNS of the OpenVPN server
Authentication Type	Selection of the authentication type. Depending on the selection, different fields are available
Pre-shared Key	Set static password if Pre shared Key, shared key or TLS-AUTH is selected
Remote Subnet, Remote Netmask	Set static route of the router, always in the direction of the peer’s subnet
Username/Password	If User/Password is selected, the corresponding data is entered in these fields
Link Detection Interval, Link Detection Timeout	Always use default
Renegotiate Interval	Always use default
Enable NAT	Set NAT mode, in the meantime routing mode is disabled
Enable LZO	Enable LZO compression
Encryption Algorithms	Set encryption algorithm, must match server
MTU	Always use default, 1500
Max Fragment Size	Maximum size of individual packets
Debug Level	Selection of debug outputs in the log
Interface Type	TUN / TAP
Expert Options (Expert Only)	More OpenVPN commands (only for experienced users)

8.7 OpenVPN Advanced

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

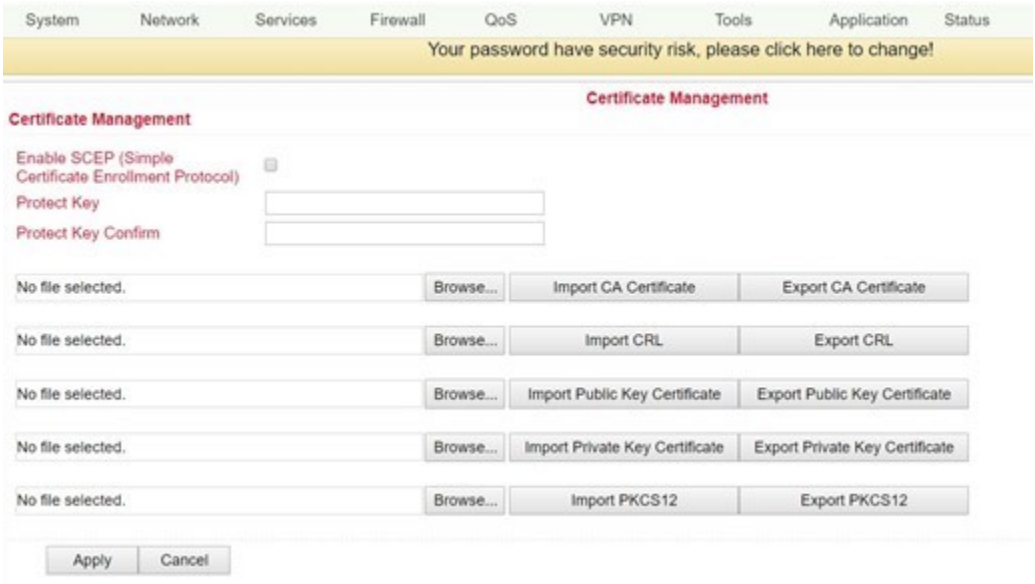


Name	Description
Enable Client-to-Client (Server Mode Only)	Enable client access to other clients
Client Management	
Enable	Enabling the function
Tunnel Name	Tunnel name of the client
Username/Common Name	Username (using username/password mode) or common name in CA (CA mode)
Client IP	Specify the client IP address
Local Static Route	Subnet of the client
Remote Static Route	Subnet of the server

CA can only be created from the customer's PC, not from TK100.

8.8 Certificate Management

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



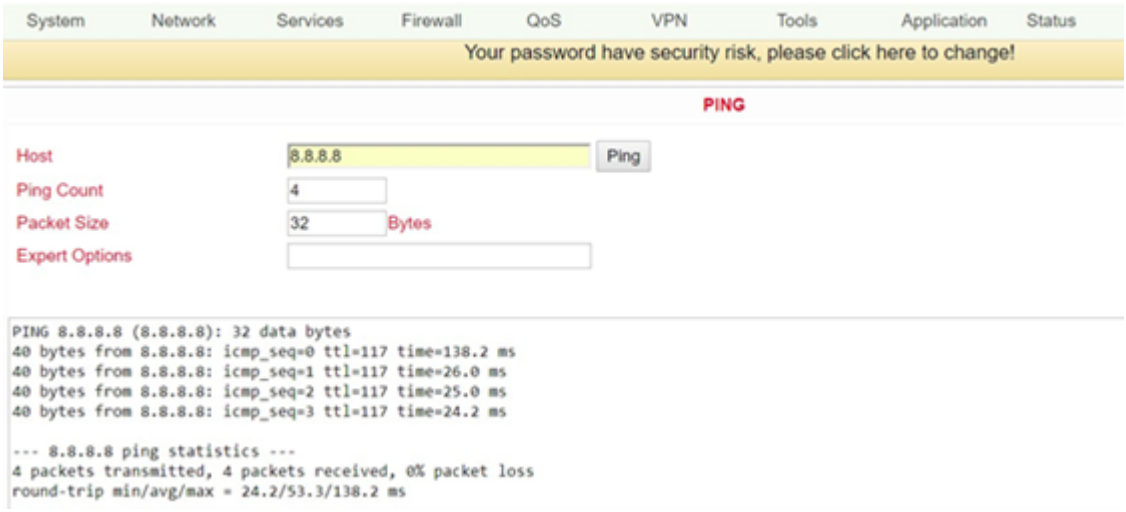
Name	Description	Standard
Enable SCEP	Click to enable	
Protect Key	Set a key to protect the certificates	Empty
Protect Key Confirm	Confirm the key to protect the certificates	Empty
Import/Export CA Certificate	Import or export CA certificate	Empty
Import/Export Certificate (CRL)	Import or export CRL certificate	Empty
Import/Export Public Key Certificate	Import/export public key certificate	Empty
Import/Export Private Key Certificate	Import or export private key certificate	Empty
Import/Export PKCS12	Import or export PKCS12 (private key and X.509 certificate)	Empty
Browse	Via Browse the respective file is selected and can then be imported	No file selected

9 Tools

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

9.1 PING

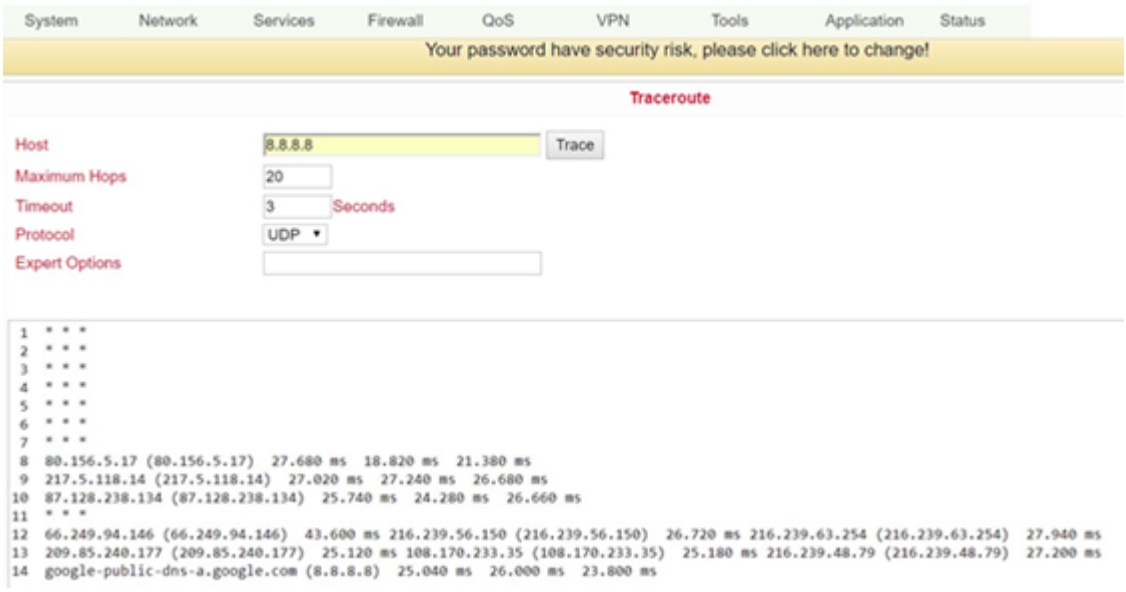
Select the item ***Tools*** > ***Ping*** if you want to test if there is a connection to the network/Internet.



Name	Description	Standard
Host	Destination for PING	Empty
Ping Count	Set number of PINGs	4 times
Packet Size	Set packet size for PING	32 Byte
Expert Options	Expert Options	Empty

9.2 Traceroute

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



Name	Description	Standard
Host	Destination for Trace Route	Empty
Max Hops	Set maximum number of hops	20
Time Out	Set timeout	3 seconds
Protocol	Optional: „ICMP“/„UDP“	UDP
Expert Options	Expert Options	Empty

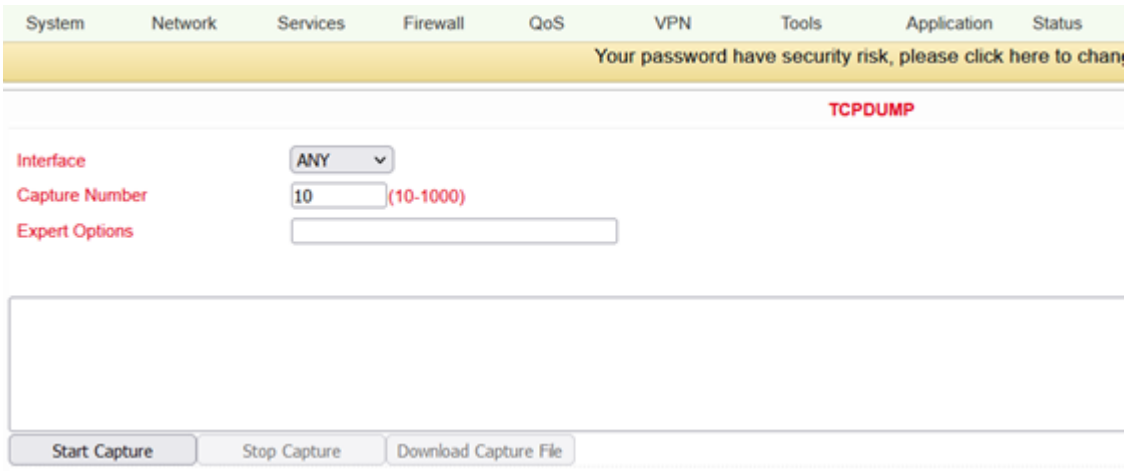
9.3 Link Speed Test

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

Via the ***Browse*** button you can upload a corresponding file from the computer. The file should be between 10 and 2000MB in size. After selecting the file, click on the ***Upload*** button. The result will be displayed

9.4 TCPDUMP

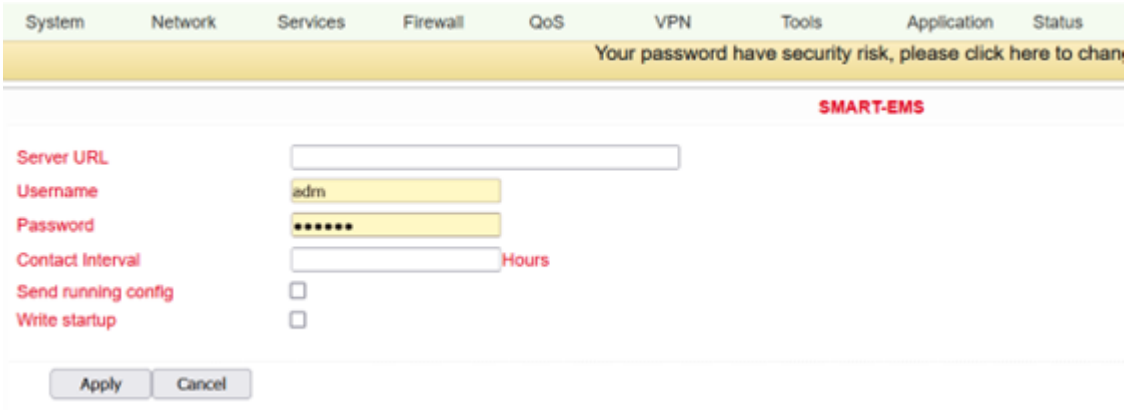
The TCPDUMP function reads data in the form of packets sent over the network and displays them on the screen or saves them to files.



10 Application

Under the menu item Application you will find the possibility to connect your router with the management solution SMART EMS of the company Welotec.

10.1 SMART-EMS

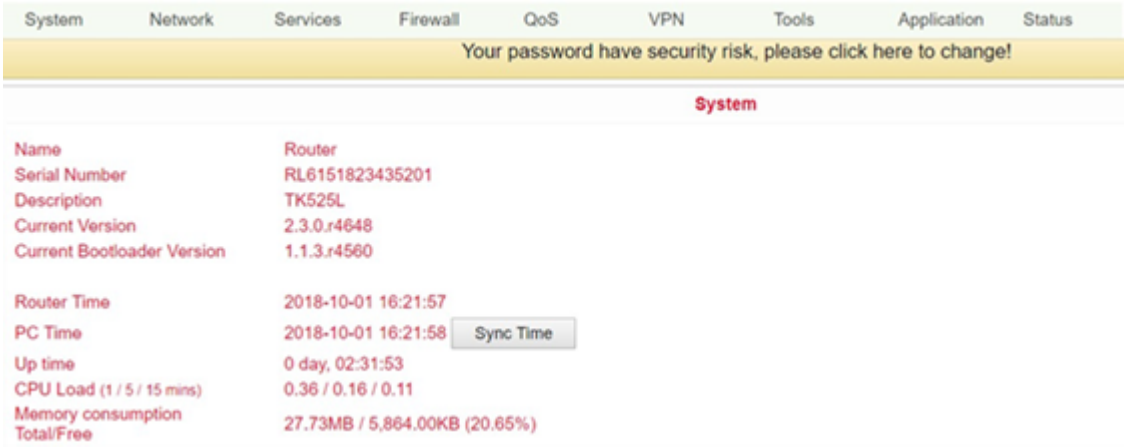


11 Status

Under "***Status***" you can view information about system, modem, network connections, routing table, device list and protocol.

11.1 System

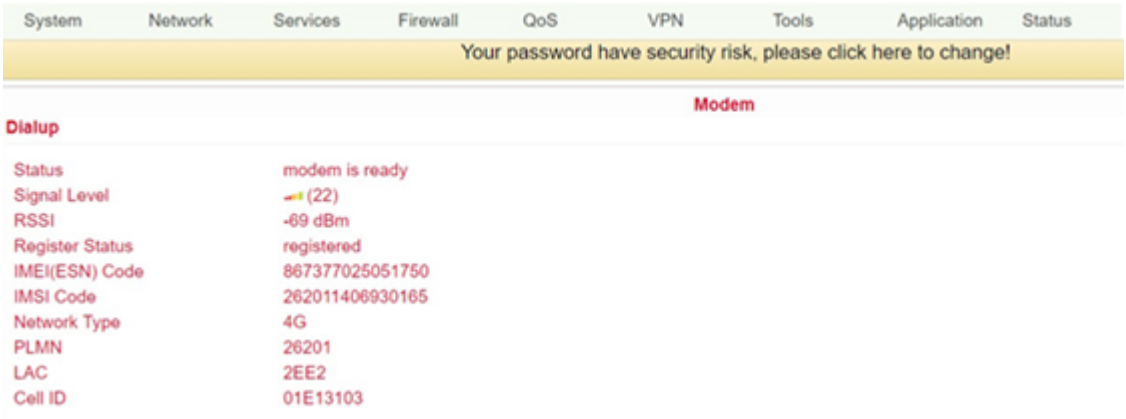
Select ***Status*** > ***System*** from the menu to retrieve information about your system.



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

11.2 Modem

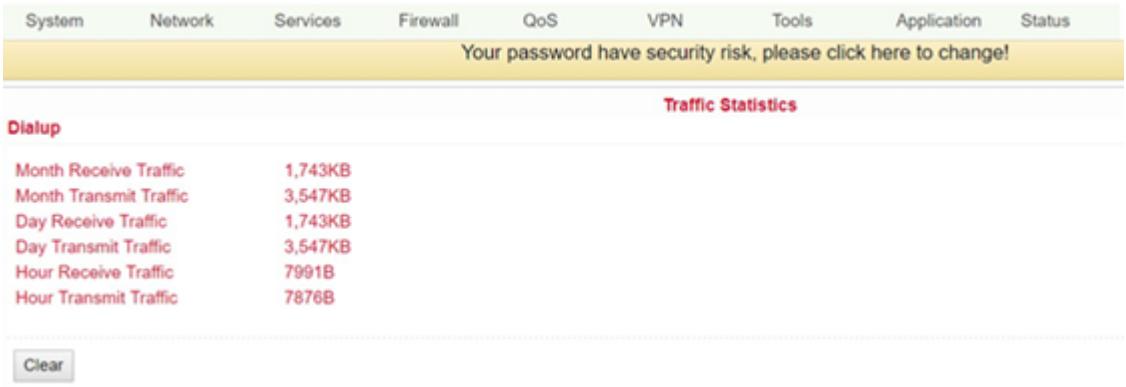
Check the status of your modem under ***Status*** > ***Modem***.



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

11.3 Traffic Statistics

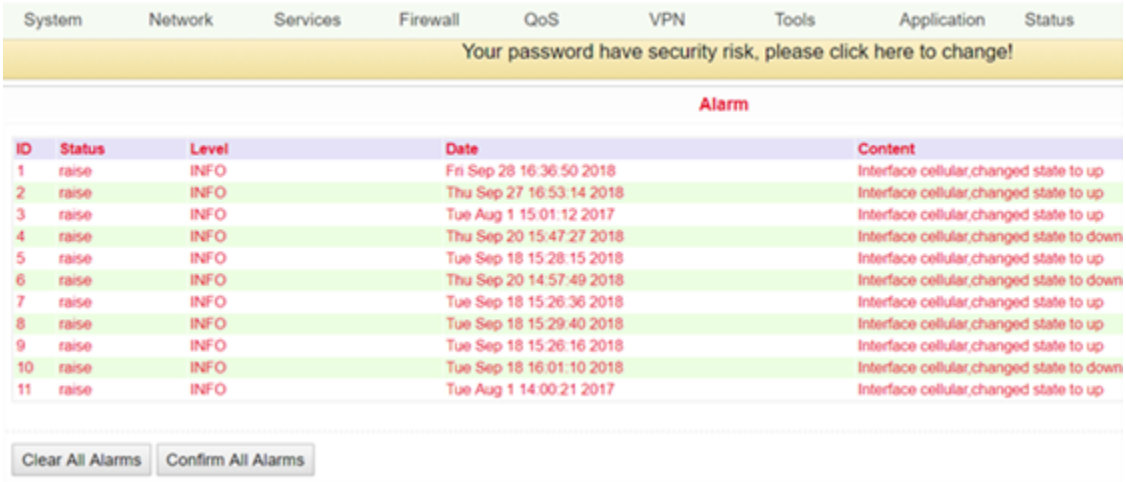
If you want to view the data consumption of the SIM card in the TK100, then you can do this under ***Status > Traffic Statistics***.



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

11.4 Alarm

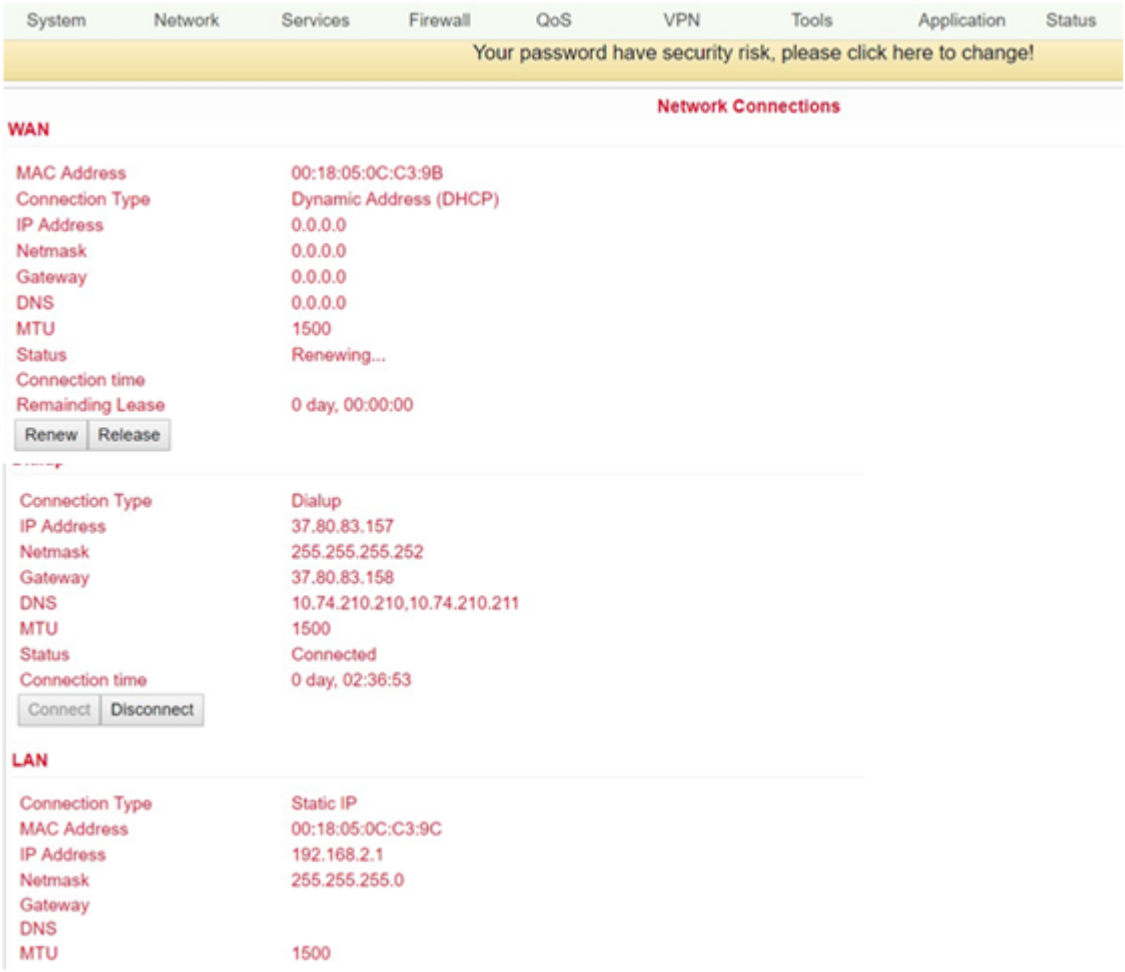
Check the alarms generated by the TK100, e.g. created under 3.3.7. in the Alarm Manager. You can access this menu item under ***Status > Alarm***.



In this example, the monthly limit of the SIM card has been reached. With the button "***Clear All Alarms***" you can clear all alarms and with "***Confirm All Alarms***" you confirm that you have taken note of the alarm.

11.5 Network Connections

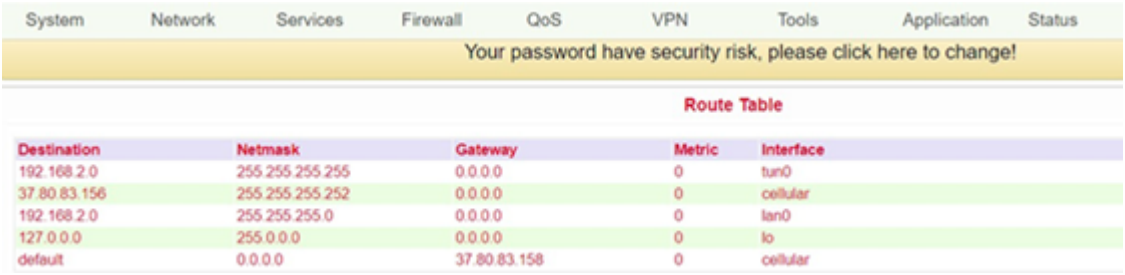
Via ***Status > Network Connections*** you can get an overview of the network connections of the TK100.



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

11.6 Route Table

If you want to have an overview of the routing table in TK100, select ***Status > Route Table*** from the menu.



After clicking on Route Table you will see the routing table of the TK100.

11.7 Device List

Under the menu item ***Status > Device List*** all devices connected to the TK100 are displayed.

Overview of the devices connected to the TK100.

11.8 Log

Documentation of the system events (logs) of the TK100. You can reach this area under ***Status > Log***.

This page displays the system log, which can be downloaded here.

It may happen that problems cannot be diagnosed and rectified immediately. In these cases, we ask you to send the diagnostic log to Welotec. To do this, click on "***Download System Diagnosing Data***", and then send us the log with a description of the error to [**support@welotec.com**][*Email: support@welotec.com*]

11.9 Third Party Software

Here are the software terms and licenses from all third party vendors related to the TK100 router series.

Your password have security risk, please click here to change!

Third Party Software Notices

The copyrights for certain portions of the Software may be owned or licensed by other third parties ("Third Party Software") and used and distributed under license. The Third Party Notices includes the acknowledgements, notices and licenses for the Third Party Software. The Third Party Notices can be viewed via the Web Interface. The Third Party Software is licensed according to the applicable Third Party Software license notwithstanding anything to the contrary in this Agreement. The Third Party Software contains copyrighted software that is licensed under the GPL/LGPL or other copyleft licenses. Copies of those licenses are included in the Third Party Notices. Welotec's warranty and liability for Welotec's modification to the software shown below is the same as Welotec's warranty and liability for the product this Modifications come along with. It is described in your contract with Welotec (including General Terms and Conditions) for the product. You may obtain the complete Corresponding Source code from us for a period of three years after our last shipment of the Software by sending a request letter to:

Welotec GmbH, Zum Hagenbach 7, 48366 Laer, Germany

Please include "Source for Welotec TK500" and the version number of the software in the request letter. This offer is valid to anyone in receipt of this information.

bridge-utils

V1.0.4

Copyright (C) 2000 Lennert Buytenhek

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, version 2 of the License. This program is distributed by the holder of the Copyright in the hope that it will be useful, but WITHOUT ANY WARRANTY by the holder of the Copyright; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

12 Technical Data

12.1 Device properties

Property	Value
Dimensions (W x H x D)	90 x 90 x 25 mm
Operating voltage	230 V AC to 9 V – 36 V DC
Approval	CE compliant

12.2 Environmental requirements

Property	Value
Operating temperature range	-20 to +70 °C
Air humidity	5 - 95 %, non condensing
Concussions	IEC 60068-2-27
Free fall	IEC 60068-2-32
Vibration	IEC 60068-2-6

12.3 Radio frequencies

12.3.1 Radio frequencies LTE Europe

Frequency	Frequency range and transmission power
Band 1	Frequency range Down: 2110 MHz – 2170 MHz Frequency range Up: 1920 MHz – 1980 MHz Max. transmission power: 200 mW
Band 3	Frequency range Down: 1805 MHz – 1880 MHz Frequency range Up: 1710 MHz – 1785 MHz Max. transmission power: 200 mW
Band 7	Frequency range Down: 2620 MHz – 2690 MHz Frequency range Up: 2500 MHz – 2570 MHz Max. transmission power: 200 mW
Band 8	Frequency range Down: 925 MHz – 960 MHz Frequency range Up: 880 MHz – 915 MHz Max. transmission power: 200 mW
Band 20	Frequency range Down: 791 MHz – 821 MHz Frequency range Up: 832 MHz – 862 MHz Max. transmission power: 200 mW
Band 28	Frequency range Down: 703 MHz – 748 MHz Frequency range Up: 758 MHz – 803 MHz Max. transmission power: 200 mW

12.3.2 Radio frequencies UMTS Europe

Frequency	Frequency range and transmission power
Band 1	Frequency range Down: 2110 MHz – 2170 MHz Frequency range Up: 1920 MHz – 1980 MHz Max. transmission power: 251 mW
Band 8	Frequency range Down: 925 MHz – 960 MHz Frequency range Up: 880 MHz – 915 MHz Max. transmission power: 251 mW

12.3.3 Radio frequencies GSM Europe

Frequency	Frequency range and transmission power
GSM 900	Frequency range Down: 925 MHz – 960 MHz Frequency range Up: 880 MHz – 915 MHz Max. transmission power: 1995 mW
GSM 1800	Frequency range Down: 1805 MHz – 1880 MHz Frequency range Up: 1710 MHz – 1785 MHz Max. transmission power: 40 mW

12.3.4 Radio frequencies LTE Asia

Frequency	Frequency range and transmission power
Band 1	Frequency range Down: 2110 MHz – 2170 MHz Frequency range Up: 1920 MHz – 1980 MHz Max. transmission power: 200 mW
Band 3	Frequency range Down: 1805 MHz – 1880 MHz Frequency range Up: 1710 MHz – 1785 MHz Max. transmission power: 200 mW
Band 7	Frequency range Down: 2620 MHz – 2690 MHz Frequency range Up: 2500 MHz – 2570 MHz Max. transmission power: 200 mW
Band 8	Frequency range Down: 925 MHz – 960 MHz Frequency range Up: 880 MHz – 915 MHz Max. transmission power: 200 mW
Band 20	Frequency range Down: 791 MHz – 821 MHz Frequency range Up: 832 MHz – 862 MHz Max. transmission power: 200 mW
Band 28	Frequency range Down: 703 MHz – 748 MHz Frequency range Up: 758 MHz – 803 MHz Max. transmission power: 200 mW

12.3.5 Radio frequencies UMTS Asia

Frequency	Frequency range and transmission power
Band 1	Frequency range Down: 2110 MHz – 2170 MHz Frequency range Up: 1920 MHz – 1980 MHz Max. transmission power: 251 mW
Band 8	Frequency range Down: 925 MHz – 960 MHz Frequency range Up: 880 MHz – 915 MHz Max. transmission power: 251 mW

12.3.6 Radio frequencies GSM Asia

Frequency	Frequency range and transmission power
GSM 900	Frequency range Down: 925 MHz – 960 MHz Frequency range Up: 880 MHz – 915 MHz Max. transmission power: 1995 mW
GSM 1800	Frequency range Down: 1805 MHz – 1880 MHz Frequency range Up: 1710 MHz – 1785 MHz Max. transmission power: 1000 mW

12.3.7 Radio frequencies UMTS Global

Frequency	Frequency range and transmission power
Band 1	Frequency range Down: 2110 MHz – 2170 MHz Frequency range Up: 1920 MHz – 1980 MHz Max. transmission power: 251 mW
Band 8	Frequency range Down: 925 MHz – 960 MHz Frequency range Up: 880 MHz – 915 MHz Max. transmission power: 251 mW

12.3.8 Radio frequencies GSM Global

Frequency	Frequency range and transmission power
GSM 900	Frequency range Down: 925 MHz – 960 MHz Frequency range Up: 880 MHz – 915 MHz Max. transmission power: 1995 mW
GSM 1800	Frequency range Down: 1805 MHz – 1880 MHz Frequency range Up: 1710 MHz – 1785 MHz Max. transmission power: 40 mW

13 Support

Send an email to the following address in case of problems with installation and operation: [*support@welotec.com*][*Email: support@welotec.com*]

14 CE Declaration

WELOTEC
a byte smarter

Declaration of conformity

Holder:
Welotec GmbH
Zum Hagenbach 7
48366 Laer
GERMANY

declares that the product:

Product:
Industrial Wireless Router

Identification:
TK1XXX-XX (with X 0 to 9 or A to Z or nothing)

Complies with:

- **Low Voltage Directive 2014/35/EU**
  - EN 62368-1 :2014 +A11:2017
- **Radio Equipment Directive 2014/53/EU:**
  - ETSI EN 301 328 V2.2.2 (2019-07)
  - ETSI EN 301 489-1 V2.2.3 (2019-11)
  - ETSI EN 301 489-17 V3.2.3 (2020-07)
  - ETSI EN 301 489-52 V1.1.0 (2016-11)
  - ETSI EN 301 511 V12.5.1 (2017-03)
  - ETSI EN 908-1 V13.1.1 (2019-11)
  - ETSI EN 908-2 V11.1.2 (2019-08)
  - ETSI EN 908-13 V13.1.1 (2019-07)
  - EN 62311:2008
- **EMC Directive 2014/30/EU**
  - EN 55032:2015
  - EN 55035:2017
  - EN 61000-3-2:2014
  - EN 61000-3-3:2013
- **RoHS 2 Directive 2011/65/EU & 2015/863/EU**

CE

The corresponding markings appear under the appliance.

Welotec GmbH
Zum Hagenbach 7
D-48366 Laer
Fon: +49(0)2554 9130 00
E-mail: info@welotec.com

December 21, 2021
Date

Signature
(Jos Zenner, CTO)

www.welotec.com | info@welotec.com