TK100

Ausführung:
v3.5.56

Datum:
09.12.2024

Inhaltsverzeichnis

1 TK100-Serie - Einführung 3
- 1.1 Checkliste für Inhalt . . . 4
- 1.2 Produktinformationen . . . 5

2 Installationshandbuch 6
- 2.1 Typische Anwendung . . . 6
- 2.2 Anschlussplan . . . 6
- 2.3 Schneller Internetanschluss . . . 7
- 2.4 Zurücksetzen auf Werkseinstellungen . . . 12
- 2.5 Werkseitige Standardeinstellungen: . . . 14

3 System 15
- 3.1 Vorbereitung . . . 15
- 3.2 System . . . 17
- 3.3 Basic Setup . . . 17
- 3.4 Time . . . 18
- 3.5 Admin Access . . . 18
- 3.6 System Log . . . 20
- 3.7 Configuration Management . . . 20
- 3.8 Scheduler . . . 21
- 3.9 Upgrade . . . 21
- 3.10 . . . 22
- 3.11 Reboot . . . 22
- 3.12 Logout . . . 22

4 Netzwerk 23
- 4.1 Cellular . . . 23
- 4.2 WAN/LAN Switch . . . 25
- 4.3 Link Backup . . . 29
- 4.4 VRRP . . . 30
- 4.5 IP Passthrough . . . 32
- 4.6 Static Route . . . 33

5 Services 34
- 5.1 DHCP Service . . . 34
- 5.2 DNS . . . 35
- 5.3 DNS Relay . . . 35
- 5.4 DDNS (Dynamic DNS) . . . 36
- 5.5 SMS . . . 38
- 5.6 Traffic Manager . . . 40
- 5.7 Alarm Manager . . . 40

6 Firewall 42
- 6.1 Basic . . . 42
- 6.2 Filtering . . . 42
- 6.3 Content Filtering . . . 43
- 6.4 Port Mapping . . . 43
- 6.5 Virtual IP Mapping . . . 44
- 6.6 DMZ . . . 45
- 6.7 MAC-IP Bundling . . . 46

6.8 NAT . . . 46

7 QoS **47**
7.1 IP BW Limit . . . 47

8 VPN **48**
8.1 IPSec Settings . . . 48
8.2 IPSec Tunnels . . . 49
8.3 GRE Tunnels . . . 51
8.4 L2TP Clients . . . 52
8.5 PPTP Clients . . . 54
8.6 OpenVPN Tunnels . . . 56
8.7 OpenVPN Advanced . . . 58
8.8 Certificate Management . . . 59

9 Tools **61**
9.1 PING . . . 61
9.2 Traceroute . . . 62
9.3 Link Speed Test . . . 62
9.4 TCPDUMP . . . 63

10 Application **64**
10.1 SMART-EMS . . . 64

11 Status **65**
11.1 System . . . 65
11.2 Modem . . . 65
11.3 Traffic Statistics . . . 66
11.4 Alarm . . . 66
11.5 Network Connections . . . 66
11.6 Route Table . . . 67
11.7 Device List . . . 68
11.8 Log . . . 68
11.9 Third Party Software . . . 68

12 Technische Daten **70**
12.1 Geräteeigenschaften . . . 70
12.2 Umgebungsbedingungen . . . 70
12.3 Funkfrequenzen . . . 70

13 Support **73**

14 CE Konformitätserklärung **74**

1 TK100-Serie - Einführung

Hinweis zum Copyright

Copyright © 2018 Welotec GmbH Alle Rechte vorbehalten.

Eine Vervielfältigung ohne Genehmigung ist nicht gestattet.

Marken

Welotec ist eine eingetragene Marke von der Welotec GmbH. Andere in diesem Handbuch genannte Marken sind Eigentum der jeweiligen Unternehmen.

Rechtlicher Hinweis

Die Informationen in diesem Dokument können ohne Vorankündigung geändert werden und sind für die Welotec GmbH nicht verbindlich.

Es ist möglich, dass dieses Benutzerhandbuch technische oder typografische Fehler enthält. Es werden regelmäßig Korrekturen vorgenommen, ohne dass darauf in neuen Versionen hingewiesen wird.

Kontaktinformationen für technischen Support

Welotec GmbH

Zum Hagenbach 7

48366 Laer

Tel.: +49 2554 9130 00

Fax.: +49 2554 9130 10

[*Email: support@welotec.com*]

Beschreibung

Die Router der TK100-Serie für den Industriebereich stellen eine stabile Hochgeschwindigkeitsverbindung zwischen Remotegeräten und Kundenstandorten über LAN und (modellabhängig) über LAN bzw. 3G/4G Netzwerke bereit. Sie können in einem Spannungsbereich von 9 bis 36 V DC betrieben werden und verfügen über einen Temperaturbereich von -20°C bis 70°C bei einer relativen Luftfeuchtigkeit von 95 %, wodurch eine hohe Stabilität und Zuverlässigkeit unter strengen Bedingungen gewährleistet ist. Der TK100 kann auf dem Arbeitsplatz verwendet werden oder auf DIN-Schienen montiert werden.

Produkte der TK100-Serie unterstützen VPN (IPSec/PPTP/L2TP/GRE/SSL VPN), was sichere Verbindungen zwischen Remotegeräten und Kundenstandorten garantiert.

Wichtiger Sicherheitshinweis:

Dieses Produkt ist für folgende Einsatzbereiche nicht geeignet:

• Bereiche, in denen keine Funkanwendungen (wie Handys) erlaubt sind

• Krankenhäuser und andere Orte, an denen der Einsatz von Handys nicht zulässig ist

• Tankstellen, Treibstofflager und Orte, an denen Chemikalien gelagert werden

• Chemische Anlagen oder andere Orte mit Explosionsgefahr Metalloberflächen, die den Funksignalpegel schwächen können

WEEE-Hinweis

Die am 13. Februar 2003 in Kraft getretene europäische Richtlinie zur Entsorgung elektrischer und elektronischer Altgeräte (WEEE) hat zu großen Veränderungen hinsichtlich der Wiederverwendung und des Recyclings elektrischer Geräte geführt.

Das Hauptziel dieser Richtlinie ist die Vermeidung von Abfällen von Elektro- und Elektronikgeräten sowie das Fördern der Wiederwendung, des Recyclings und anderer Formen der Wiederverwertung. Das WEEE-Logo (siehe Abbildung links) auf dem Produkt oder der Verpackung weist darauf hin, dass das Produkt nicht im normalen Hausmüll entsorgt werden darf. Sie sind dafür verantwortlich, alle ausgedienten elektrischen und elektronischen Geräte an entsprechenden Sammelstellen zu entsorgen. Eine getrennte Sammlung und sinnvolle Wiederverwertung Ihres Elektroschrotts hilft dabei, sparsamer mit den natürlichen Ressourcen umzugehen. Zudem stellt eine sachgemäße Wiederverwertung elektrischer und elektronischer Altgeräte die menschliche Gesundheit und den Schutz der Umwelt sicher.

Weitere Informationen zur Entsorgung, Wiederverwertung sowie zu Sammelstellen elektrischer und elektronischer Altgeräte erhalten Sie bei Ihrer örtlichen Stadtverwaltung, den Entsorgungsbetrieben, dem Vertreiber oder dem Hersteller des Geräts.

1.1 Checkliste für Inhalt

Jeder TK100-Funkrouter wird in einem Paket mit Standardzubehör ausgeliefert. Weiteres Zubehör kann bestellt werden. Überprüfen Sie den Inhalt Ihres Pakets sorgfältig, und falls etwas fehlt oder beschädigt ist, wenden Sie sich an Ihren Vertriebspartner von der Welotec GmbH.

Lieferumfang:

Standardzubehör:

Zubehör	Anzahl	Beschreibung
TK100-Router	1	Industrieller Router der Serie TK100
Netzwerkkabel	1	Netzwerk-Kabel CAT5, 1,5 Meter
Handbuch	1	Datenträger mit Handbuch
Lizenzbedingungen	1	“Third Party Software Notifications and Licenses”
Stromversorgung		
Terminalblock	1	2-Polige Anschlussklemme für Stromversorgung

Bestandteile Set (Modellabhängig)

Produkt	Anzahl	Beschreibung
TK100-Router	1	Industrieller Router der Serie TK100
Netzwerkkabel	1	Netzwerk-Kabel CAT5, 1,5 Meter
Mobilfunkantenne	1	5 m Magnetfußantenne 2G/3G/4G
Handbuch	1	Datenträger mit Handbuch
Lizenzbedingungen	1	“Third Party Software Notification and Licenses”
Stromversorgung		
	1	Tischnetzteil, Eingang 100-240 V AC, Ausgang 12 V DC (für TK100), inkl. 2-poliger Terminalblock
	1	Stecker, europäischer Standard

1.2 Produktinformationen

1.2.1 Umgebungsbedingungen

Betriebstemperatur: -20 bis 70°C

Relative Luftfeuchtigkeit während des Betriebs: 5 bis 95 % (nicht kondensierend)

Lagertemperatur: -40 bis +85°C

1.2.2 Stromversorgung

Stromversorgung: 1 Klemmleiste (2-polig) inkl. Spannungsbuchse und serieller Anschluss

Eingangsspannung: 9 - 36 V DC

1.2.3 Physikalische Eigenschaften

Gehäuse: Stahl, Schutzart IP30

Gewicht: 259 g

Abmessungen (mm): 90 x 90 x 25 mm

2 Installationshandbuch

2.1 Typische Anwendung

Mit Routern der TK100-Serie können Sie Geräte mit Ethernet, über GPRS/HSUPA/ UMTS/LTE mit dem Internet verbinden. Zur Gewährleistung der Sicherheit und eines unterbrechungsfreien Zugriffs unterstützt die TK100-Serie VPN-Verbindungen und ermöglicht somit den Remotezugriff und eine sichere Datenübertragung über das Internet.

2.2 Anschlussplan

Schnittstelle	Beschreibung
Stromanschluss	9 - 36 V DC
Ethernet-Ports	Zwei 10/100 Base-TX RJ45-Ports
Antennenanschluss (Mobilfunk)	SMA (f)
SIM-Kartenfach	Zwei Fächer zum Einlegen von SIM-Karte

2.2.1 Bedeutung der LED-Leuchten

Power	Status	Mobile	Bedeutung
Aus	Aus	Aus	Ausgeschaltet
An	Aus	Aus	Systemfehler
An	An	Aus	Das Modul oder die SIM-Karte wird nicht erkannt
An	An	Blinkend	Einwahl
An	An	An	Einwahl erfolgreich
An	Blinkend	An	Systemupgrade
An	Blinkend->An	Aus	Reset

Signalstärke

Farbe	Signalstärke
Rot	Signal 0 - 10
Gelb	Signal 11 - 20
Grün	Signal 21 - 30

2.3 Schneller Internetanschluss

2.3.1 Einstecken der SIM-Karte

Öffnen Sie das TK-Router SIM/UIM-Fach oben am Gerät und legen Sie die SIM-Karte in den Kartenträger ein.

2.3.2 Installation der Antenne

Verbinden Sie nach der Installation des TK100 die Antenne und schrauben Sie die Antenne fest. Stellen Sie die Antenne dort auf, wo eine gute Signalstärke erreicht wird.

⚠ **Hinweis**: Position und Winkel können sich auf die Signalstärke auswirken.

2.3.3 Stromversorgung

Verbinden Sie die im Lieferumfang enthaltene Spannungsversorgung mit dem Gerät, und achten Sie darauf, ob die LED-Anzeige für „Power“ aufleuchtet. Wenden Sie sich an den technischen Support von Welotec, wenn keine Anzeige aufleuchtet. Sie können den TK100 konfigurieren, wenn die Power-Anzeige blinkt.

2.3.4 Verbinden

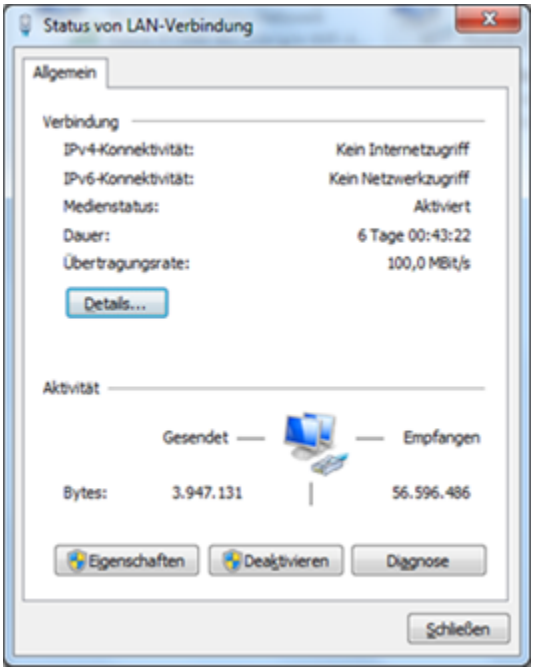
Verbinden Sie den TK100 mit dem PC:

1. Schließen Sie das Ethernet Kabel des TK100 an den PC an.
2. Anschließend leuchtet eine LED-Anzeige der RJ45-Schnittstelle grün auf und die anderen Anzeigen blinken.

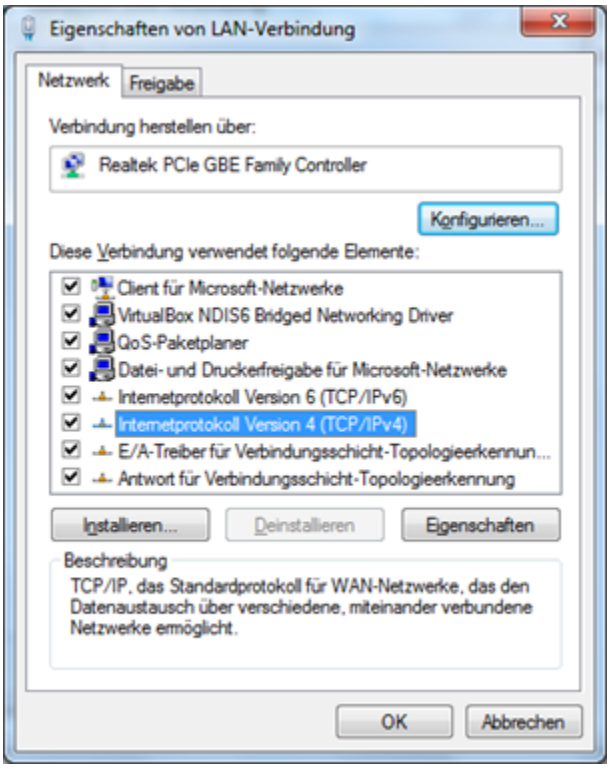
2.3.5 Erstes Anschließen des TK-Router-Geräts an den PC

Der TK100-Router kann IP-Adressen für den PC automatisch vergeben. Richten Sie den PC so ein, dass IP- Adressen über DHCP automatisch abgerufen werden. (Grundlage ist das Windows-Betriebssystem):

1. Öffnen Sie die Systemsteuerung, doppelklicken Sie auf das Symbol „***Netzwerk- und Freigabecenter***“ und öffnen Sie so den Bildschirm „***Netzwerk- und Freigabecenter***“.
2. Klicken Sie auf „***LAN-Verbindung***“ und öffnen Sie den Bildschirm mit dem „***Status von LAN-Verbindung***“:

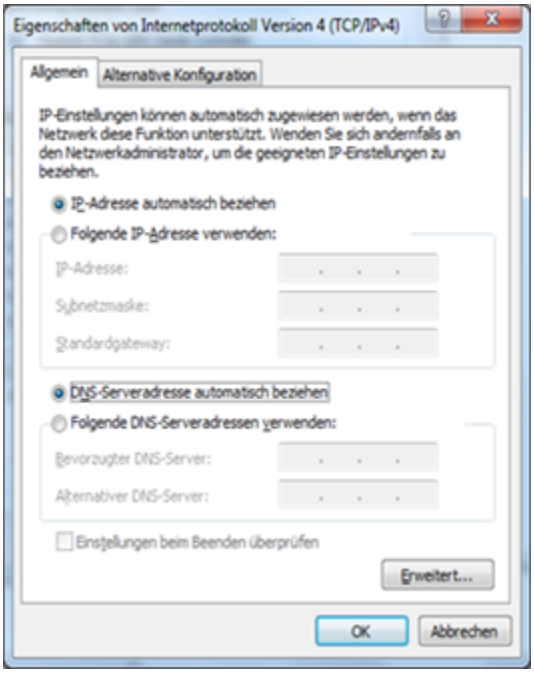


3. Klicken Sie auf „***Eigenschaften***“, und öffnen Sie den Bildschirm mit den Eigenschaften der LAN-Verbindung:



1. Wählen Sie „***Internetprotokoll Version 4 (TCP/IPv4)***“ aus, klicken Sie auf die Schaltfläche „***Eigenschaften***“, und überprüfen Sie, ob Ihr PC IP- und DNS-Adresse automatisch beziehen kann.
   (Sie können den PC auch im Subnetz einrichten: 192.168.2.0/24, z. B. IP: 192.168.2.10, Netzmaske: 255.255.255.0, Standardgateway: 192.168.2.1)

Durch Klicken auf „***OK***“ weist der TK-Router dem PC eine IP-Adresse zu: 192.168.2.X, sowie das Gateway: 192.168.2.1 (die Standardadresse des TK100).



Nach dem Konfigurieren der TCP/IP-Protokolle können Sie mit dem Ping-Befehl überprüfen, ob die Verbindung zwischen PC und Router fehlerfrei aufgebaut wird. Es folgt ein Beispiel für das Ausführen des Ping-Befehls unter

Windows 7 :

Windows-Taste+R -> Eingabe „*cmd*“ -> Entertaste -> Eingabe „*Ping 192.168.2.1*“ -> Entertaste Bei dieser Anzeige:

```
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]>_
```

Die Verbindung zwischen PC und Router wurde richtig aufgebaut.

Im folgenden Beispiel gibt es Fehler:

```
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]>_
```

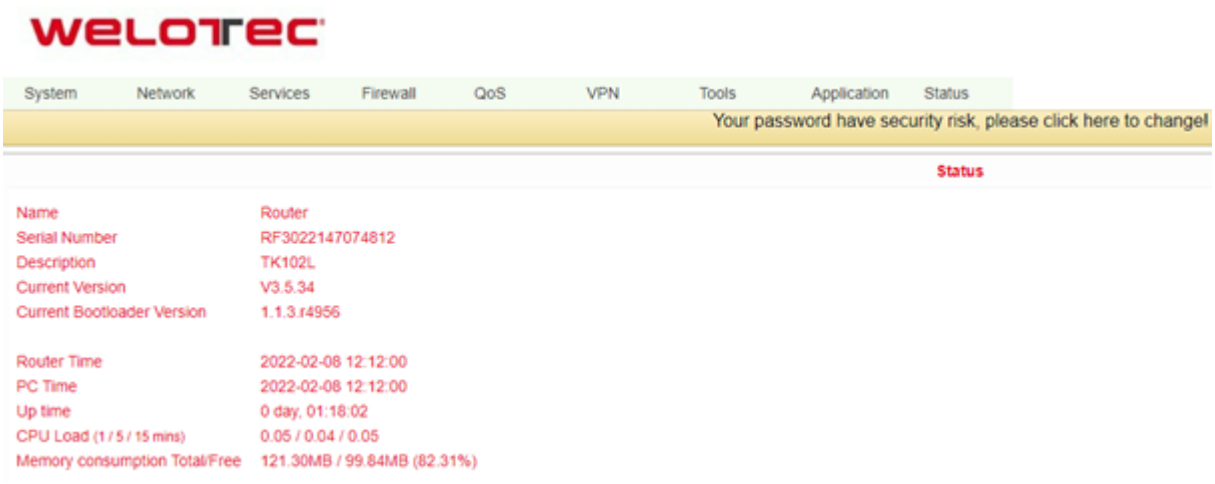
Die Verbindung funktioniert nicht richtig, und Sie sollten die Anweisungen erneut durchgehen und Ihre Einstellungen überprüfen.

2.3.6 Konfigurieren des TK100 (Optional)

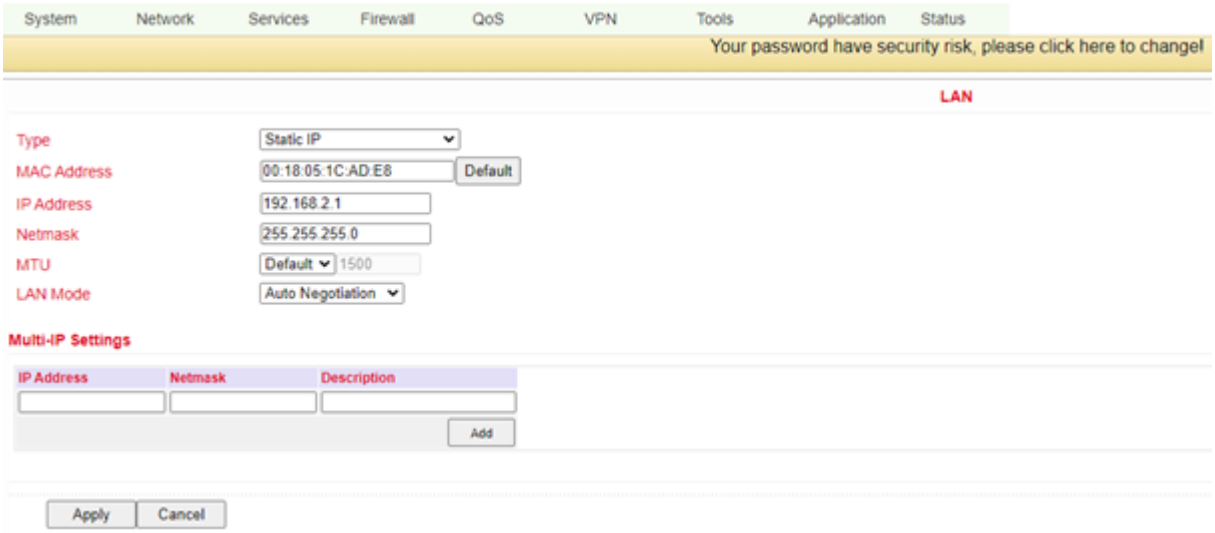
Nachdem Sie die im vorherigen Kapitel beschriebenen Schritte ausgeführt haben, können Sie den Router konfigurieren:

1. Öffnen Sie einen beliebigen Internet Browser (z.B. Google Chrome) und geben Sie die Standard-IP-Adresse des Routers ein: [**http://192.168.2.1***.*] Es wird folgende Anmeldeseite geöffnet:

Geben Sie den Benutzernamen (Standard: adm) sowie das Kennwort (Standard: 123456) ein, und klicken Sie dann auf „***Login***“, um den Konfigurationsbildschirm zu öffnen.

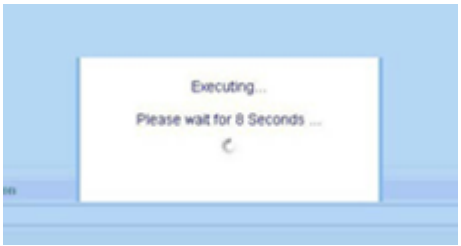


Wenn Sie eine eigene IP für den Router festlegen möchten: Klicken Sie auf ***Network >LAN***.



Ändern Sie die IP-Adresse bspw. in ***192.168.1.254***.

Klicken Sie auf „***Apply***“, und folgender Bildschirm wird angezeigt:



Die IP-Adresse des TK100 wurde geändert. Damit Sie nun wieder auf die Konfigurationsseite zugreifen können, muss der PC in demselben Subnetz eingerichtet sein, beispielsweise: ***192.168.1.10/24*** – Geben Sie dann die geänderte IP-Adresse ***(192.168.1.254)*** in Ihrem Browser ein.

2.3.7 Den TK-Router mit dem Internet verbinden

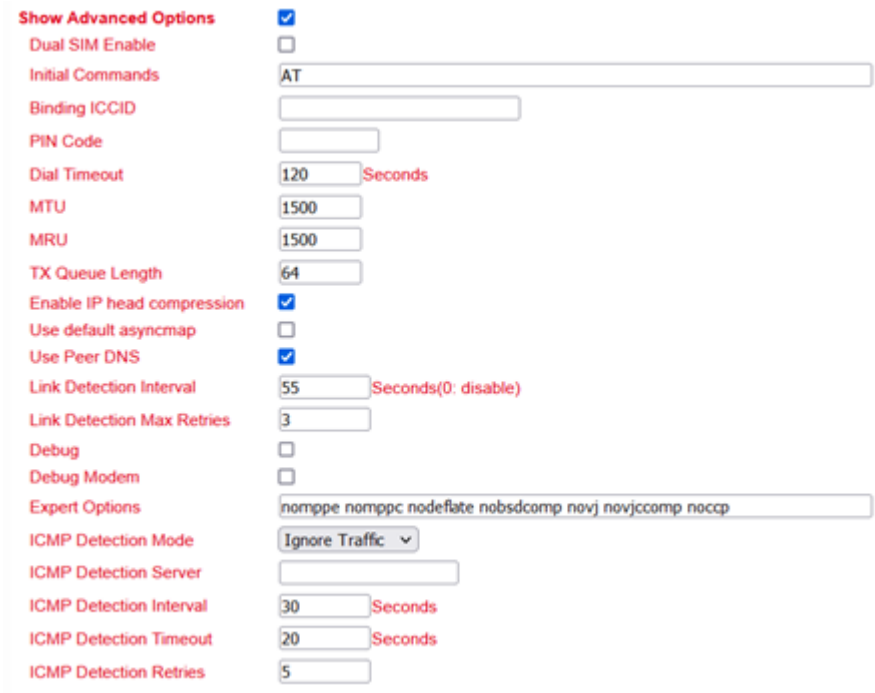
Führen Sie die folgenden Konfigurationsschritte aus, um eine Verbindung zwischen dem TK100 und dem Internet herzustellen.

Klicken Sie auf ***Network > Cellular***, und aktivieren Sie die Funktion durch ***Enable***:

Überprüfen Sie die Einträge und wählen Sie unter **SIM1 Network Provider** einen voreingestellten Netzwerk-Provider aus, oder fügen Sie ein selbsterstelltes Profil eines Providers hinzu:

Sie erhalten die APN, die Einwahlnummer, den Benutzernamen und das Kennwort von Ihrem lokalen Netzwerkanbieter. Erkundigen Sie sich dort nach den Einzelheiten.

Über ***Show Advanced Options*** können Sie weitere Einstellungen tätigen, wie z.B. den PIN Code, wenn dieser auf der SIM-Karte gesetzt ist.



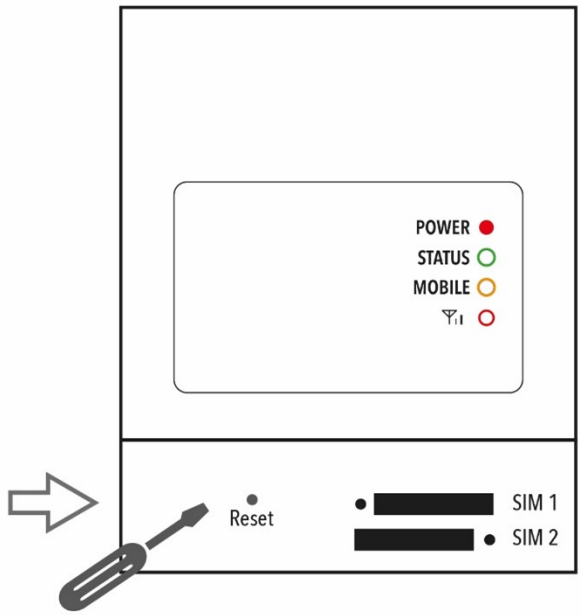
Wenn Sie die richtige Konfiguration festgelegt haben, kann der TK100 nun eine Verbindung mit dem Internet herstellen. Öffnen Sie einen Internet Browser, geben Sie „[**www.welotec.com**][*www.welotec.com*]“ ein, und die Website von Welotec wird geöffnet.

2.4 Zurücksetzen auf Werkseinstellungen

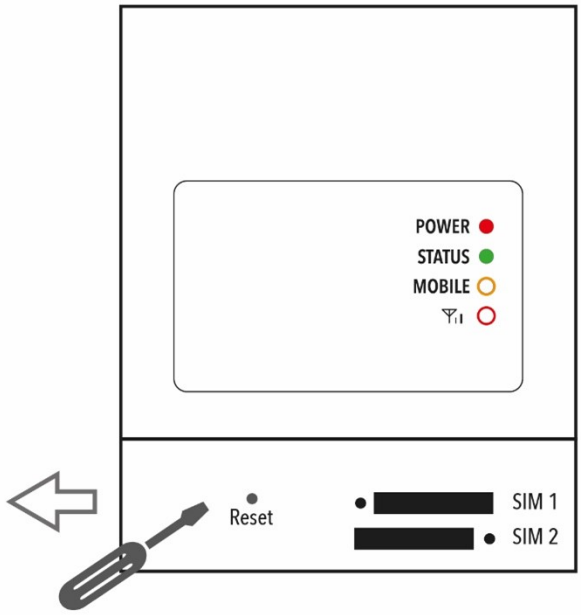
2.4.1 Hardwaremethode

= LED leuchtet = LED leuchtet nicht = LED blinkt

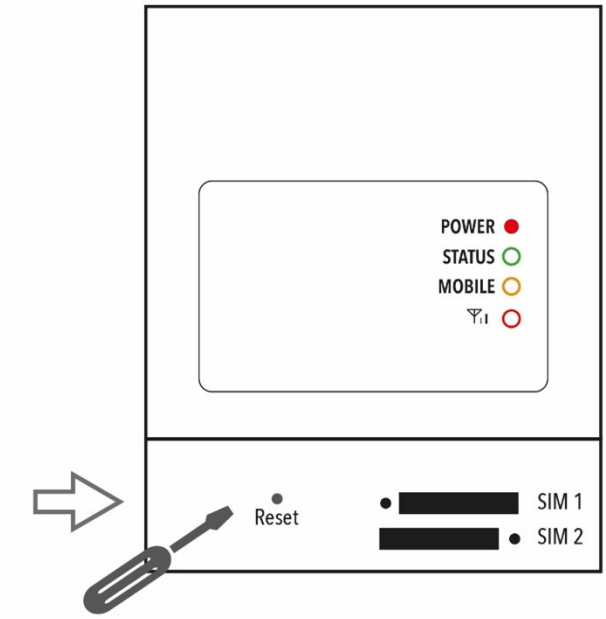
1. Drücken Sie die ***RESET-Taste***, während Sie den TK100 einschalten:



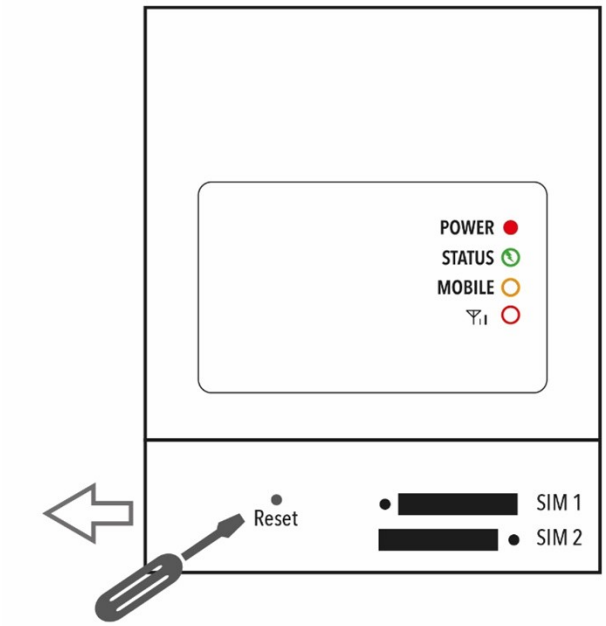
2. Sobald die LED-Leuchte **Status** aufleuchtet (ca. 15 Sekunden nach dem Einschalten), lassen Sie die ***RESET-Taste*** los:



3. Nach einigen Sekunden hört die LED-Leuchte **Status** auf zu leuchten. Nun drücken Sie erneut die ***RESET-Taste***:



4. Daraufhin blinkt die LED-Leuchte **Status**, was bedeutet, dass das Zurücksetzen auf die Standardeinstellung erfolgreich war.



2.4.2 Webmethode

1.) Melden Sie sich an der webbasierten Benutzeroberfläche des TK100 an und wählen Sie ***System*** > ***Config Management*** aus:

2.) Klicken Sie auf ***Restore default configuration***, um den TK100 auf seine Werkseinstellungen zurückzusetzen. Danach wird der Router neu gebootet.

2.5 Werkseitige Standardeinstellungen:

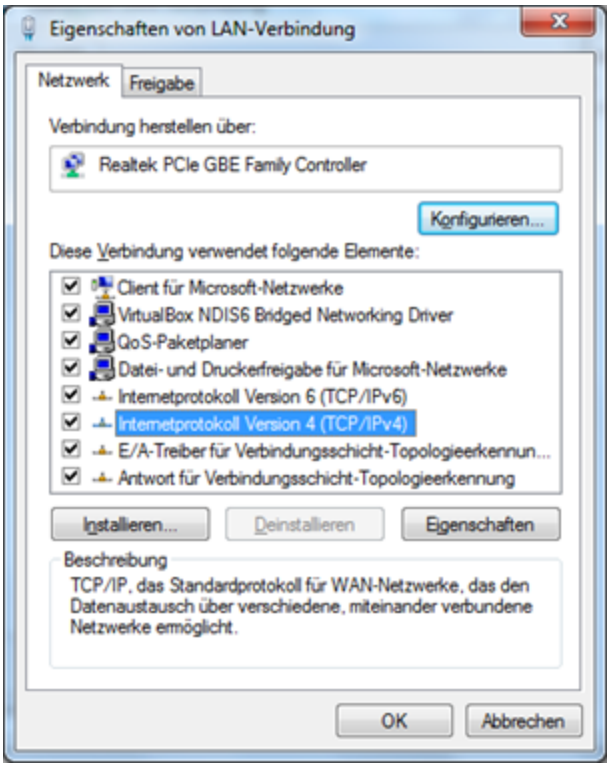
- **IP**: 192.168.2.1
- **Netzmaske**: 255.255.255.0
- **Benutzername**: adm
- **Passwort**: 123456
- **Serieller Parameter**: 115200-N-8-1

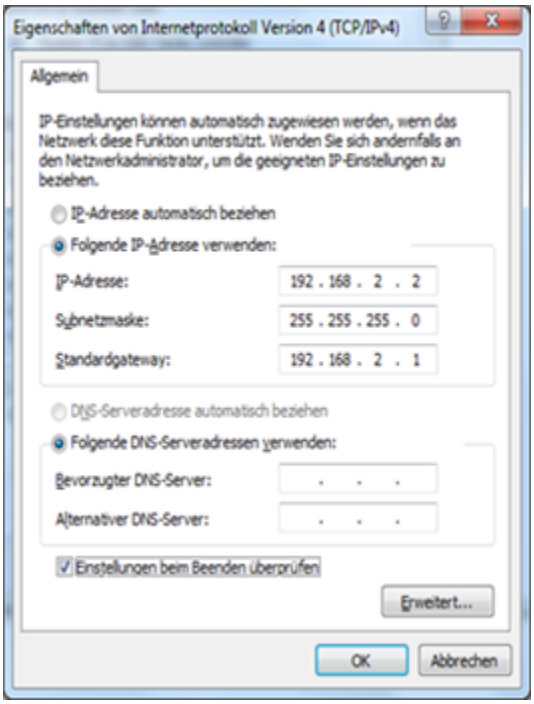
3 System

Der TK-100 Router muss vor der Verwendung ordnungsgemäß konfiguriert sein. In diesem Kapitel wird die webbasierte Konfiguration beschrieben.

3.1 Vorbereitung

Verbinden Sie Ihre Geräte zunächst per Kabel oder Hub (Switch) mit dem TK100 und legen Sie die IP-Adresse für den PC und TK100 in demselben Subnetz fest, z. B.: legen Sie die PC-IP-Adresse auf 192.168.2.2 fest, Netzmaske: ***255.255.255.0***, Gateway (Standard-IP des TK100: ***192.168.2.1***):

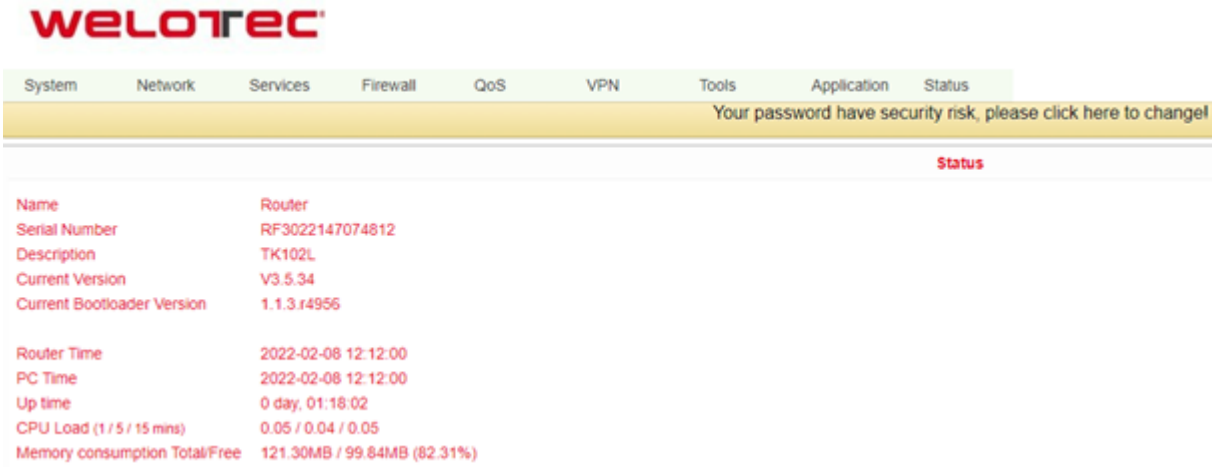




Öffnen Sie einen Internet Browser, und geben Sie die IP-Adresse des TK100 ein: [**http://192.168.2.1**][**http://192.168.2.1***.*] (Standard-IP des TK100).

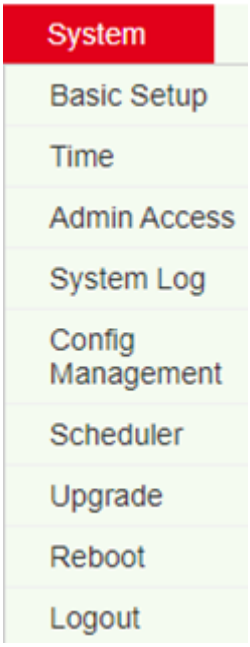
Auf der folgenden Anmeldeseite müssen Sie sich als Administrator anmelden. Geben Sie den Benutzernamen und das Kennwort ein (Standard: ***adm/123456***).

Klicken Sie auf „***Login***“, um die Konfigurationsseite zu öffnen.



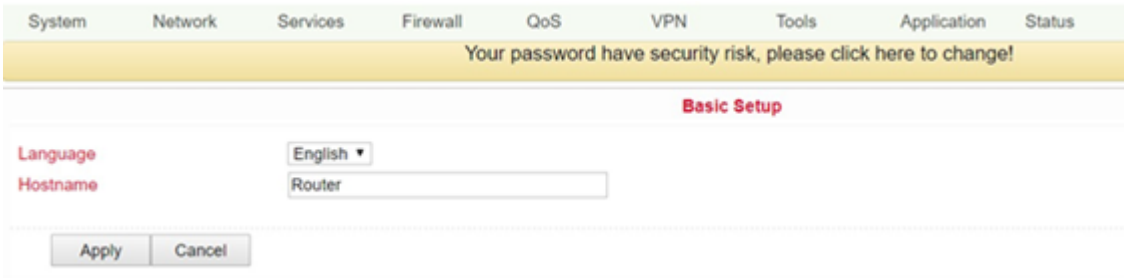
3.2 System

Die Systemeinstellungen umfassen die folgenden 9 Bereiche: Basic Setup, Time, Admin Access, System Log, Config Management, Scheduler, Upgrade, Reboot und Logout.



3.3 Basic Setup

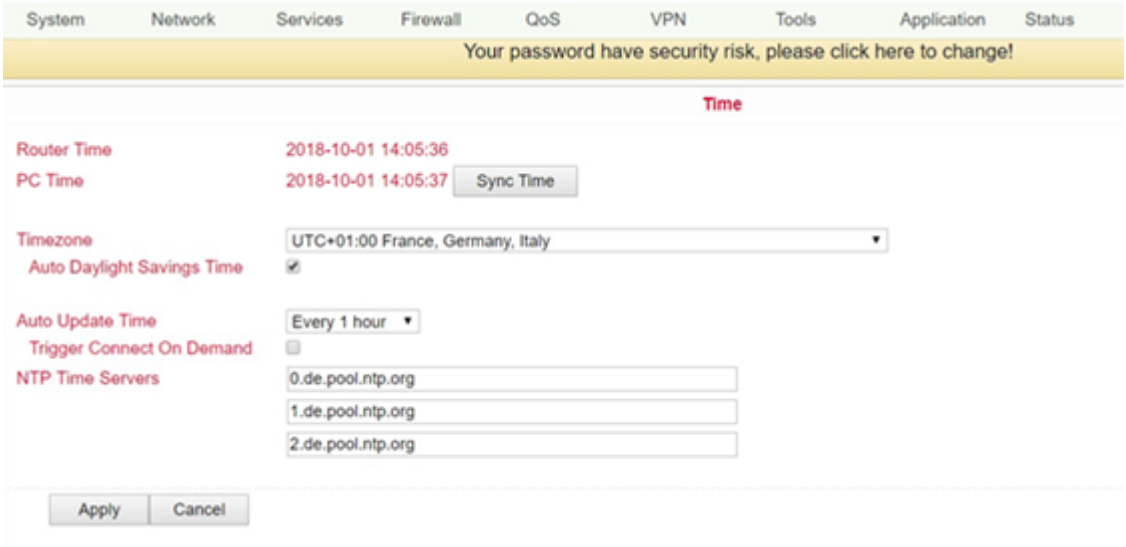
Im Basic Setup können Sie die Sprachführung des Menüs, sowie den Hostnamen anpassen. Erreichbar ist dieser Menüpunkt über ***System > Basic Setup***.



Parametername	Beschreibung	Standard
Language	Sprache für Konfigurationsseite festlegen	Englisch
Host Name	Hostname TK100	Router

3.4 Time

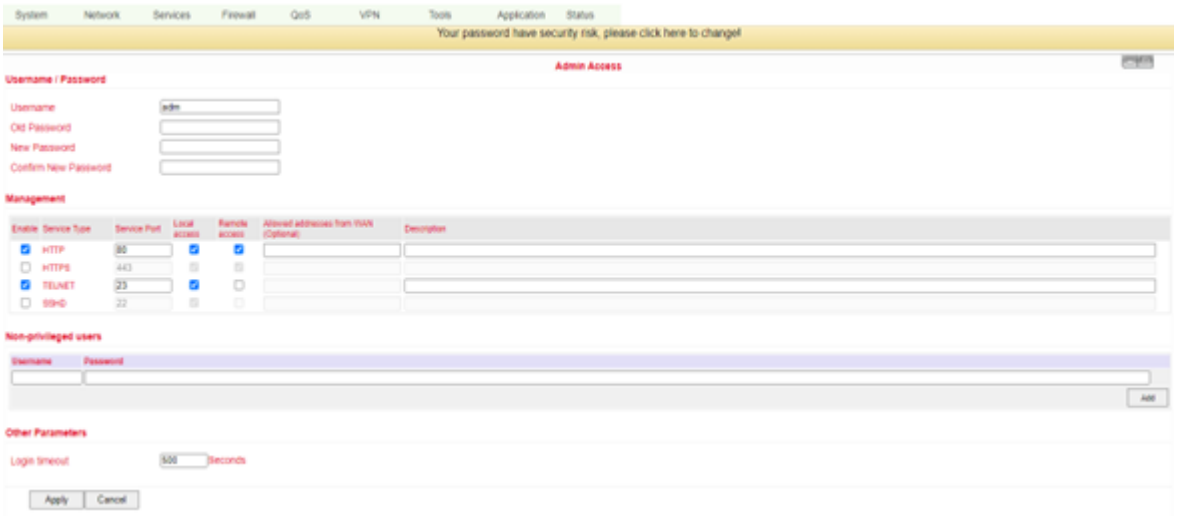
In diesem Menüpunkt lässt sich die Systemzeit des Routers anpassen. Weiter ist es hier möglich einen Zeitserver (NTP Time Server) einzurichten um die Systemzeit automatisch aktuell zu halten.



Name	Beschreibung	Standard
Router Time	Uhrzeit des Routers	2017-08-01 16:00:00
PC Time	Uhrzeit des PCs (bzw. die Uhrzeit des mit dem Router verbundenen Geräts)	Über den Button Sync Time lässt sich die Zeit mit dem angeschlossenen Gerät synchronisieren
Timezone	Zeitzone festlegen	Wählbare Zeitzone
Auto Daylight Savings Time	Automatische Umstellung Sommerzeit/Winterzeit	Deaktiviert
Auto Update Time	Zeitpunkt der automatischen Uhrzeitaktualisierung	Deaktiviert
NTP Time Servers (nach Aktivierung der Option „Auto Update Time“)	Einstellung für NTP-Zeitserver (Höchstens drei Einträge)	pool.ntp.org

3.5 Admin Access

In diesem Bereich können Sie wichtige Einstellungen ändern bzw. anpassen, wie z.B. das Kennwort des Administrators oder die Portbelegung für den Zugriff auf den Router. Zu erreichen sind diese Einstellungen über ***System > Admin Access***.



Name	Beschreibung	Standard
Username/Password		
Username	Benutzername für Anmeldung an der Konfigurationsseite	adm
Old Password	Zum Ändern des Kennworts ist die Eingabe des alten Kennworts erforderlich	123456
New Password	Neues Kennwort eingeben	
Confirm New Password	Neues Kennwort erneut eingeben	
Connection Management		
Enable	Zum Aktivieren auswählen	Aktiviert
Service Type	HTTP/HTTPS/TELNET/SSH	80/443/23/22
Local Access	Aktiviert - Zulassen, dass Router über LAN verwaltet wird (z.B : HTTP)	Aktiviert
Remote Access	Aktiviert - Zulassen, dass der TK100 über WAN verwaltet wird (z.B : HTTP)	Aktiviert
Description	Verwaltungsparameter beschreiben (ohne Auswirkung auf den TK100)	
Non-privileged users		
Username	Benutzername ohne Administrator-Rechte anlegen	
Password	Passwort für Benutzer ohne Administrator-Rechte anlegen	
Andere Parameter		
Login Timeout	Protokollzeitüberschreitung festlegen, nach diesem Wert wird die Verbindung der Konfigurationsseite getrennt und man muss sich neu einloggen	

3.6 System Log

Einstellungsmöglichkeiten für das Protokollieren von Log-Dateien. Sie erreichen diese über ***System > System Log***.

Name	Beschreibung	Standard
Log to Remote System	Remoteprotokollserver aktivieren	Deaktiviert (wenn aktiviert, kann IP-Adresse und Port eingegeben werden)
IP Adress/Port (UDP)	IP-Adresse und Port des Remoteprotokollservers festlegen	Port: 514
Log to Console	Ausgabe des Logs auf der seriellen Schnittstelle	Deaktiviert

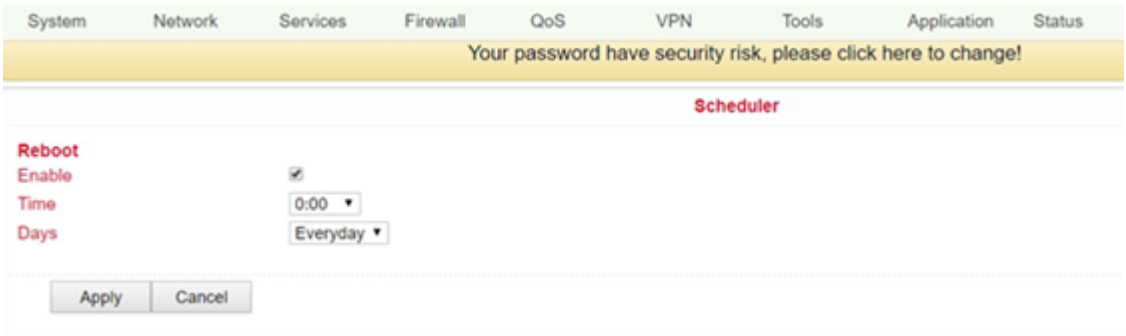
3.7 Configuration Management

Sichern und Importieren von Router Konfigurationen, sowie zurücksetzen auf Werkseinstellungen des Routers und sichern bzw. wiederherstellen der Provider-Daten. Sie können diesen Menüpunkt über ***System > Config Management*** erreichen.

Name	Beschreibung
Router Configuration	Konfigurationsdatei für Import/Backup hochladen/speichern
restore default configuration	Zum Zurücksetzen des TK100 anklicken (zum Aktivieren der Standardkonfiguration muss der TK100 neu gestartet werden.)
Network Provider (ISP)	Zum Importieren oder sichern von APN, Benutzername, Kennwort und anderer Parameter von herkömmlicher Betreiber
Durchsuchen	Mit dem Durchsuchen-Button können Sie die Datei mit den Einstellungen auswählen, die über Import hochgeladen werden sollen

3.8 Scheduler

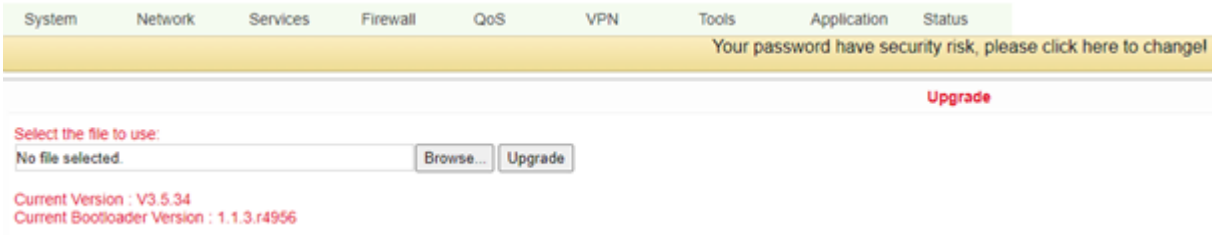
Der Scheduler dient dazu den automatischen Reboot für den Router einzustellen. Sie können die Einstellungen dafür über ***System > Scheduler*** festlegen.



Name	Beschreibung
Enable	Schaltet den Auto Reboot ein oder aus
Time	Uhrzeit, wann der TK100 Router neu gebootet werden soll
Days	Auswahl „Everyday“ für tägliches rebooten

3.9 Upgrade

In diesem Bereich bietet Ihnen der Router eine Schnittstelle zum Aktualisieren der Firmware. Zu erreichen über **System > Upgrade**.



Wählen Sie zum Aktualisieren des Systems über den Button ***Datei auswählen*** die Aktualisierungsdatei (z.B. TK100-V3.5.xxx.bin) in Ihrem Dateisystem aus.

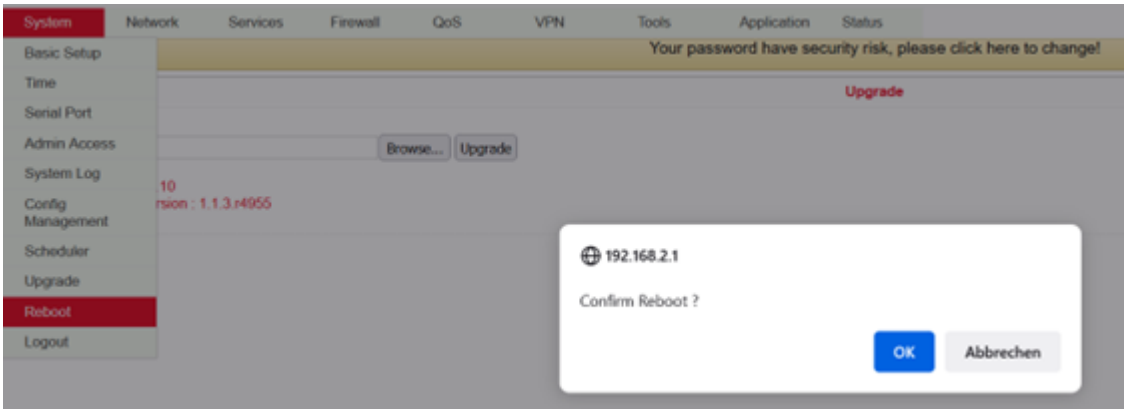
Klicken Sie auf den Button „***Upgrade***“, und bestätigen Sie den Start der Aktualisierung

Klicken Sie nach erfolgreicher Aktualisierung der Firmware auf ***Reboot***, um den TK100 neu zu starten.

3.10

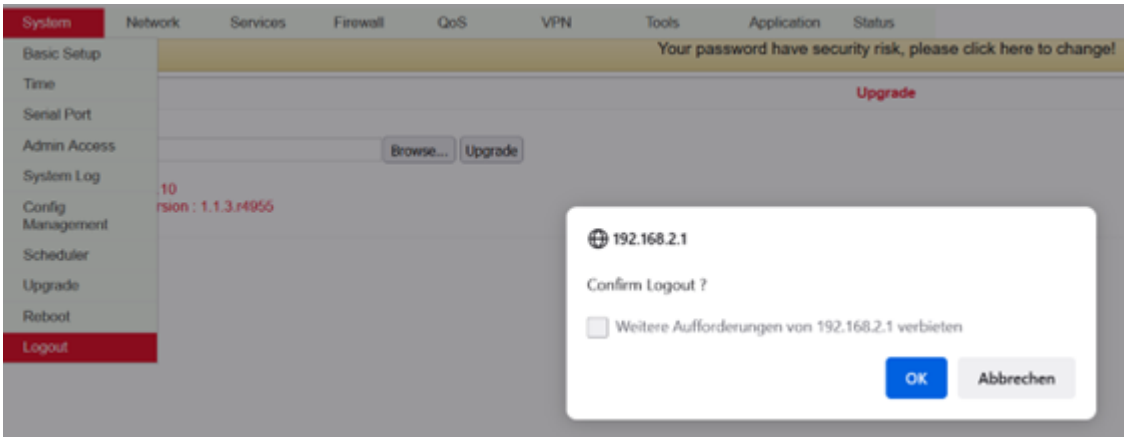
3.11 Reboot

Wenn Sie einen Neustart Ihres Routers durchführen müssen, wählen Sie ***System > Reboot*** aus. Klicken Sie dann auf „***OK***“, um das System neu zu starten.



3.12 Logout

Klicken Sie zum Abmelden vom System auf ***System > Logout*** und bestätigen Sie das Abmelden mit „***OK***“.



4 Netzwerk

Über die Netzwerkeinstellungen konfigurieren Sie Cellular, WAN/LAN Switch, LAN, Link Backup, VRRP, IP Passthrough, Static Route

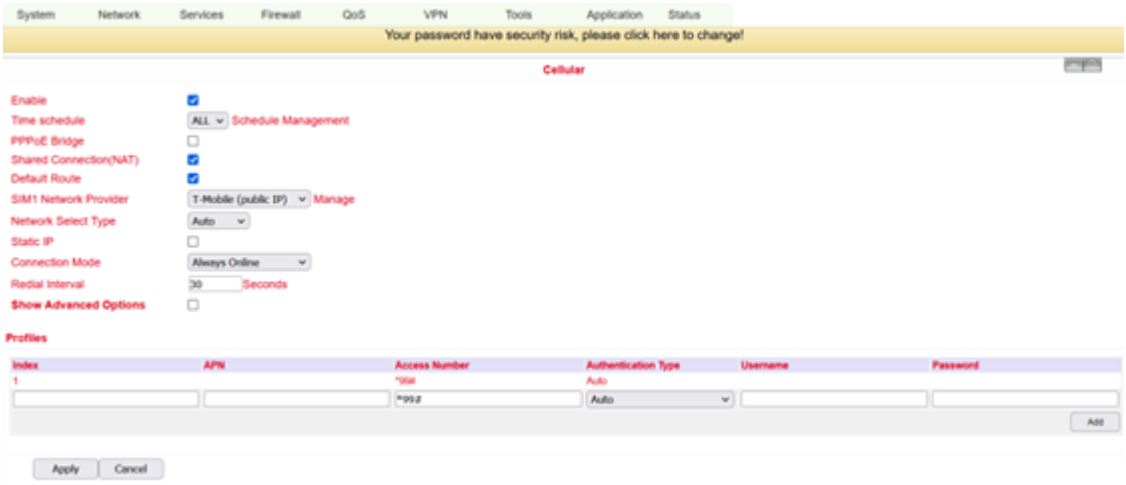
4.1 Cellular

In diesem Menübereich legen Sie die Einwahl Ihres Routers fest und konfigurieren diese. Zu erreichen über ***Network > Cellular***.

Überprüfen Sie die Einträge und wählen Sie unter **SIM1 Network Provider** einen voreingestellten Netzwerk-Provider aus, oder fügen Sie ein selbsterstelltes Profil eines Providers hinzu:

Sie erhalten die APN, die Einwahlnummer, den Benutzernamen und das Kennwort von Ihrem lokalen Netzwerkanbieter. Erkundigen Sie sich dort nach den Einzelheiten.

Über ***Show Advanced Options*** können Sie weitere Einstellungen tätigen, wie z.B. den PIN Code, wenn dieser auf der SIM-Karte gesetzt ist.



Name	Beschreibung	Standard
Enable	Aktiviert die Dialup Funktion	Aktiviert
Time Schedule	zeit für online und offline festlegen (s. auch 3.2.1.1)	All
Shared Connection (NAT)	Aktiviert - mit Router verbundenes Gerät	Aktiviert
Default Route	Mobilfunk Interface als Standard Route ins Internet	Aktiviert
Network Provider (ISP)	Lokalen ISP auswählen, falls hier nicht aufgeführt „Custom“ auswählen	Custom
APN	APN-Parameter, die vom Provider geliefert wird	internet.t-d1-de (Telekom)
Access Number	Einwahlparameter, die vom lokalen ISP bereitgestellt werden	99**1#
Username	Benutzername, der vom Provider bereitgestellt wird	tm
Password	Kennwort das vom lokalen ISP bereitgestellt wird	tm
Network Select Type	Mobilen Netzwerktyp auswählen (2G, 3G, 4G only)	Auto
Connection Mode	Verbindungsmodus: Router ist immer online	Always Online
Redial Interval	Wenn das Einwählen fehlschlägt, wählt der TK-Router nach diesem Intervall erneut an	30 Sekunden
Show Advanced Options	Ermöglicht das Konfigurieren erweiterter Optionen	Deaktiviert
PIN Code	Feld für die PIN-Nummer der SIM-Karte	Leer
MTU	MTU (Maximum Transmisson Unit) festlegen	1500
Authentication Type	PAP, CHAP	Auto
Use Peer DNS	Die Option aktivieren, um Peer-DNS zu akzeptieren	Aktiviert
Link Detection Interval	Intervall für Verbindungserkennung festlegen (0 = deaktiviert)	55 Sekunden
Debug	Debug-Modus aktivieren	deaktiviert
Debug Modem	Debug-Modem aktivieren	deaktiviert
ICMP Detection Mode	Monitor Traffic: Nur wenn keine Daten fließen wird in regelmäßigen Abständen ein Keep Alive Ping gesendet	Monitor Traffic
ICMP Detection Server	Server für ICMP-Erkennung festlegen; leeres Feld bedeutet, es ist keiner vorhanden	Leer
ICMP Detection Interval	Intervall für ICMP-Erkennung festlegen	30 Sekunden
ICMP Detection Timeout	Zeitüberschreitung für ICMP-Erkennung festlegen (TK100 wird bei ICMP-Zeitüberschreitung neu gestartet)	20 Sekunden
ICMP Detection Retries	Höchstanzahl der Wiederholungen festlegen, wenn ICMP fehlschlägt	5

4.1.1 Schedule Management

Zeitplanverwaltung (neben *„Time schedule“*):

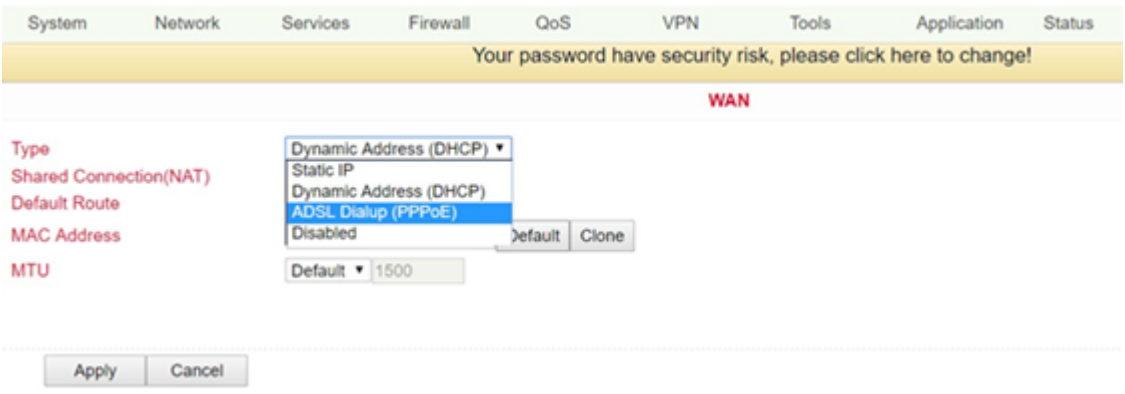
Hier kann eine eigene Dialup-Strategie gefahren werden, d.h. Sie können hier über drei Zeitbereiche festlegen, wann der Router online sein soll.

Name	Beschreibung	Standard
Name	Name für den Zeitplan	Schedule_1
Sunday	Sonntag	Leer
Monday	Montag	Aktiviert
Tuesday	Dienstag	Aktiviert
Wednesday	Mittwoch	Aktiviert
Thursday	Donnerstag	Aktiviert
Friday	Freitag	Aktiviert
Saturday	Samstag	Leer
Time Range 1	Zeitbereich 1 festlegen	9:00 - 12:00
Time Range 2	Zeitbereich 2 festlegen	14:00 - 18:00
Time Range 3	Zeitbereich 3 festlegen	0:00 - 0:00
Description	Konfiguration beschreiben	Leer

Sie können auch mehrere Zeitpläne erstellen, wenn z.B. an einem Arbeitstag andere Arbeitszeiten gelten.

4.2 WAN/LAN Switch

Hier können Sie ein neues WAN (Wide Area Network) einrichten oder Einstellungen für ihr LAN vornehmen. Zu erreichen über ***Network > WAN/LAN Switch***. Unter diesem Reiter können Sie entscheiden ob der Port für WAN oder LAN genutzt werden soll.



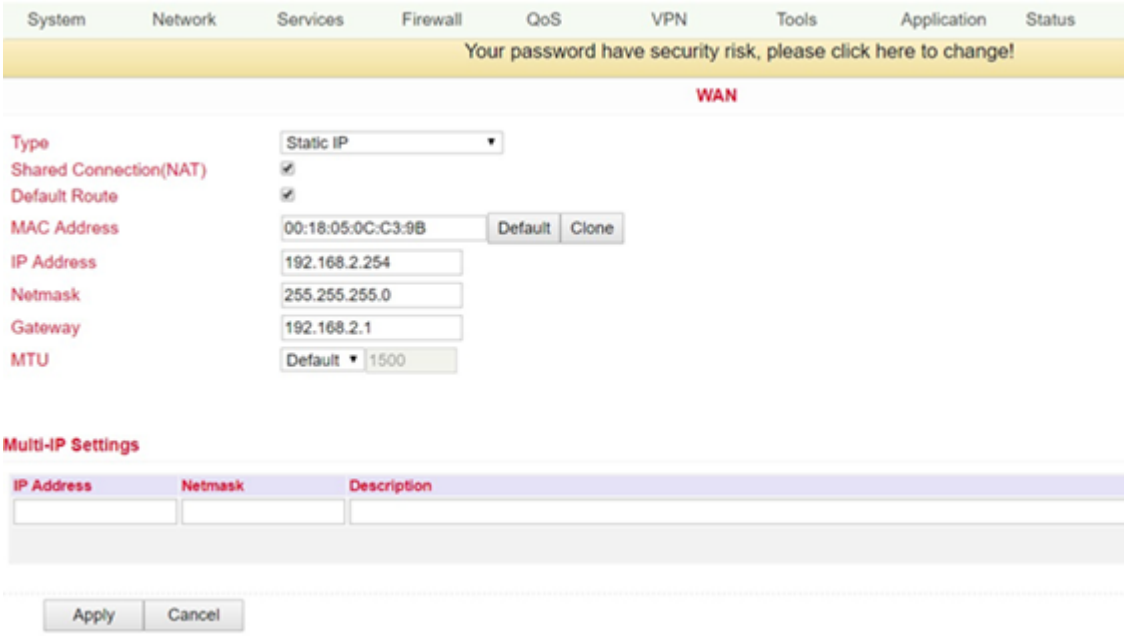
Auf dieser Seite kann der Typ des WAN-Ports festgelegt werden:

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

Es kann immer nur ein WAN-Typ aktiviert sein. Durch die Aktivierung eines Typs wird ein anderer deaktiviert.

4.2.1 Static IP

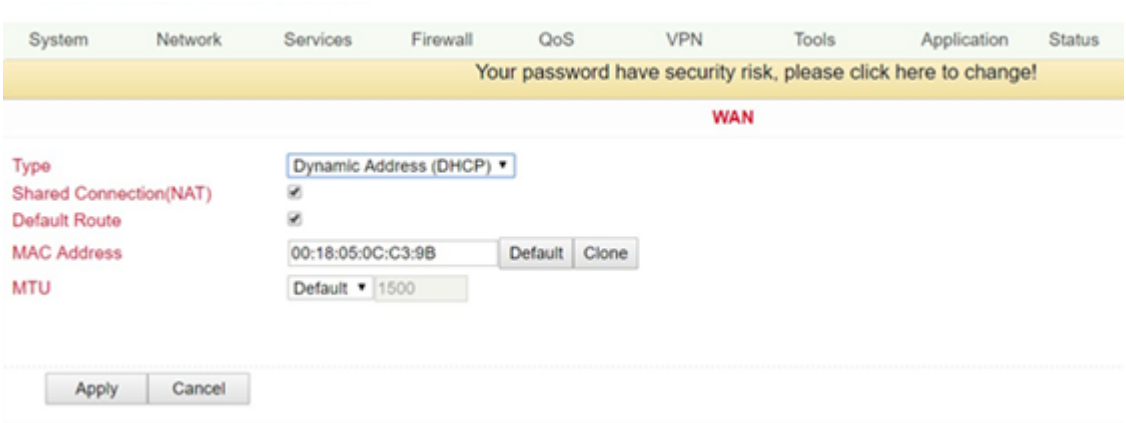
Static IP kann auch für die Konfiguration des LAN genutzt werden.



Name	Beschreibung	Standard
Type	Static IP	disabled
Shared Connection (NAT)	Aktiviert - mit Router verbundenes lokales Gerät kann auf das Internet zugreifen	Aktiviert
Default Route	Mobilfunk Interface als Standard Route ins Internet	Aktiviert
MAC Adress	MAC-Adresse festlegen (Button Default = Standard, Clone = neuerstellte MAC-Adresse)	Default
IP Address	IP-Adresse für WAN-Port festlegen	192.168.1.29
Netmask	Netzmaske für WAN-Port festlegen	255.255.255.0
Gateway	WAN-Gateway festlegen	192.168.1.1
MTU	Maximum Transmission Unit (MTU) festlegen, möglich sind die Optionen „Default“ und „Manual“	Default = 1500
Multi-IP Settings (es können höchstens 8 weitere IP-Adressen festgelegt werden)		
IP Address	Weitere IP-Adresse für LAN festlegen	Leer
Netmask	Netzmaske festlegen	Leer
Description	Einstellungen beschreiben	Leer

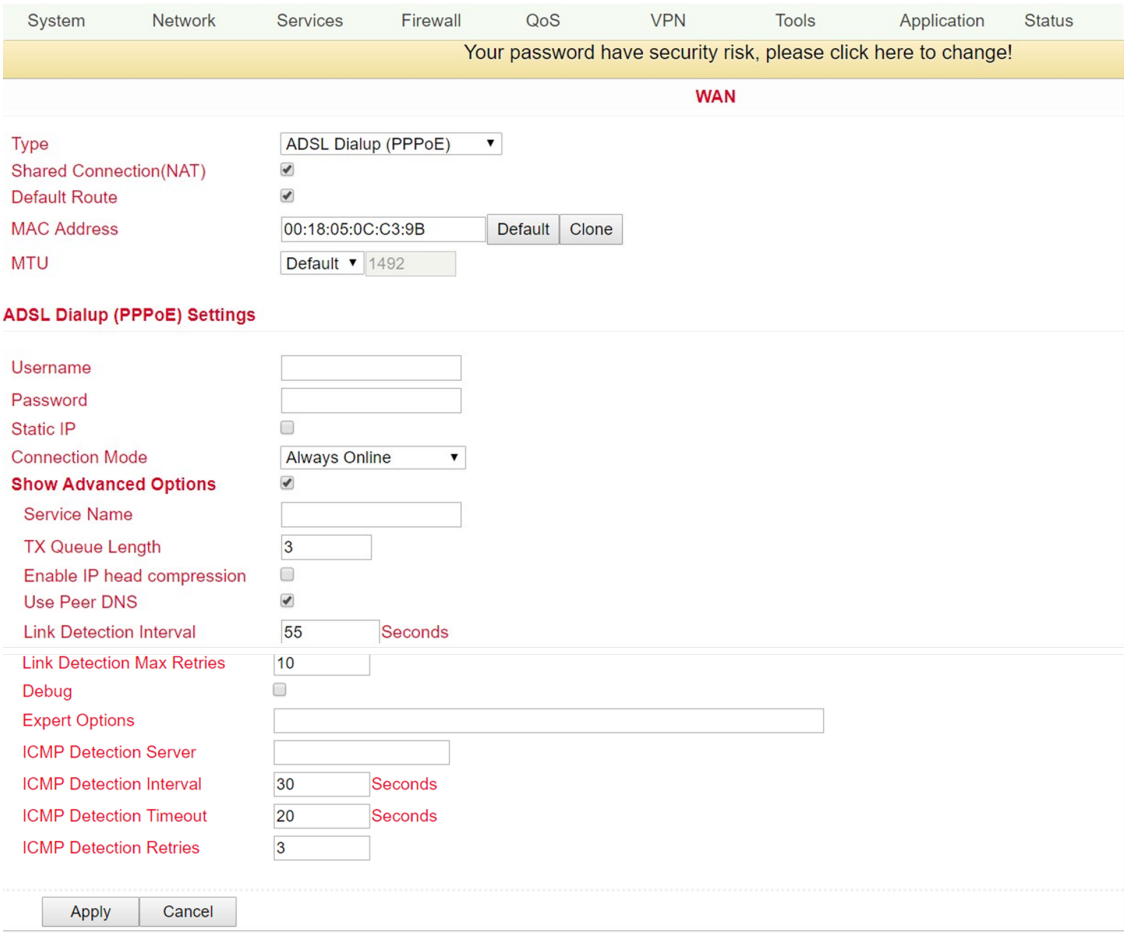
4.2.2 Dynamic Address (DHCP)

Dynamic Address kann auch für die LAN-Einstellungen genutzt werden.



Name	Beschreibung	Standard
Type	Dynamic Address (DHCP)	disabled
Share Connection (NAT)	Aktiviert - mit Router verbundenes lokales Gerät kann auf das Internet zugreifen	Aktiviert
Default Route	Mobilfunk Interface als Standard Route ins Internet	Aktiviert
MAC Address	MAC-Adresse festlegen	
MTU	Maximum Transmission Unit (MTU) festlegen, möglich sind die Optionen “ Default“ und „Manual“	Default = 1500

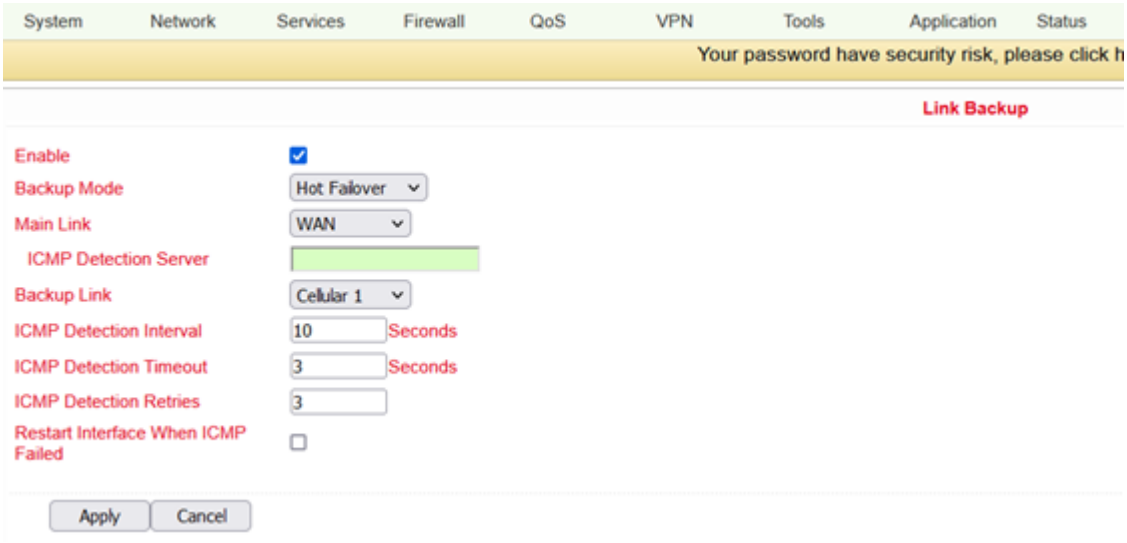
4.2.3 ADSL Dialup (PPPoE)



Name	Beschreibung	Standard
Type	ADSL Dialup (PPPoE)	disabled
Share Connection (NAT)	Aktiviert - mit Router verbundenes lokales Gerät kann auf das Internet zugreifen	Aktiviert
Default Route	Mobilfunk Interface als Standard Route ins Internet	Aktiviert
MAC Address	MAC-Adresse festlegen	
MTU	Maximum Transmission Unit (MTU) festlegen, möglich sind die Optionen „Default“ und „Manual“	Default = 1492
ADSL Dialup (PPPoE) Settings		
Username	Benutzername zum Einwählen festlegen	Leer
Password	Kennwort zum Einwählen festlegen	Leer
Static IP	Statische IP-Adressen aktivieren	Deaktiviert
Connection Mode	Verbindungsmodus festlegen („Connect on Demand“/“Always Online“/“Manual“)	Always Online
Show Advanced Options (erweiterte Optionen)		
Show advanced options	Erweiterte Konfiguration aktivieren	Deaktiviert
Service Name	Hier kann ein name für den service vergeben werden	Leer
TX Queue Length	Länge der Übertragungswarteschlange festlegen	3
Enable IP head compression	Klicken, um die IP-Headerkomprimierung zu aktivieren	Leer
Use Peer DNS	Peer-DNS für Benutzer aktivieren	Deaktiviert
Link Detection Interval	Intervall für Verbindungserkennung festlegen	55 Sekunden
Link Detection Max Retries	Höchstanzahl der Wiederholungen für Verbindungserkennung festlegen	10 (Mal)
Debug	Auswählen, um Debug-Modus zu aktivieren	Deaktiviert
Expert Options	Expertenparameter festlegen	Leer
ICMP Detection Server	Server für ICMP-erkennung festlegen	Leer
ICMP Detection Intervall	Zeit für ICMP-Erkennung festlegen	30
ICMP Detection Timeout	Zeitüberschreitung für ICMP-Erkennung festlegen	3
ICMP Detection Retries	Höchstanzahl der Wiederholungen für ICMP-Erkennung festlegen	3

4.3 Link Backup

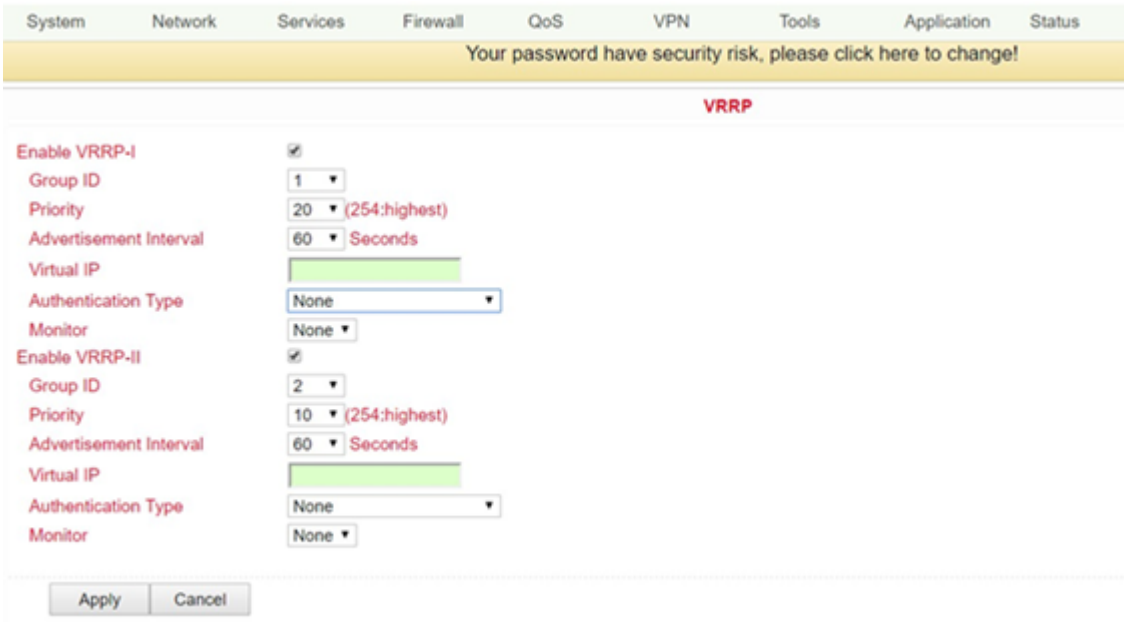
Mit dieser Option werden Verbindungen zwischen Funk-WAN und Ethernet-WAN gesichert. Fällt ein WAN aus, wird vom TK100 das jeweils andere automatisch verwendet. Sie können dies unter ***Network > Link Backup*** konfigurieren.



Name	Beschreibung	Standard
Enable	Den Service für Verbindungs-Backup aktivieren	Deaktiviert
Main Link	Auswahl von WAN, Dialup und WAN (STA) als Haupt-WAN möglich	WAN
ICMP Detection Server	ICMP kann eine Verbindung zu einem bestimmten Ziel sicherstellen	Leer
ICMP Detection Interval	Zeitintervall zwischen ICMP-Paketen	10
ICMP Detection Timeout	Zeitüberschreitung für die einzelnen ICMP-Pakete	3 (Sekunden)
ICMP Detection Retries	War keine Wiederholung der ICMP-Erkennung erfolgreich, wird die Backup-Verbindung angewählt	3
Backup Link	Backup-Verbindung auswählen	Dialup
Backup Mode	Hot Backup / Cold Backup	Hot Backup

4.4 VRRP

Das Virtual Router Redundancy Protocol (VRRP) ist ein Verfahren zur Steigerung der Verfügbarkeit wichtiger Gateways in lokalen Netzen durch redundante Router. Mehrere physische Router werden zu einer logischen Gruppe zusammengefasst. Diese Gruppe von Routern präsentiert sich im Netzwerk nun als ein logischer virtueller Router. Hierzu wird dem logischen Router eine virtuelle IP-Adresse und eine virtuelle MAC-Adresse zugeordnet. Einer der Router innerhalb der Gruppe wird als der virtuelle Master-Router definiert, dieser bindet daraufhin die virtuelle MAC- und die virtuelle IP-Adresse an sein Netzwerkinterface und informiert die anderen Router der Gruppe, die als virtuelle Backup-Router agieren. Diese Funktion können Sie unter ***Services > VRRP*** einrichten.

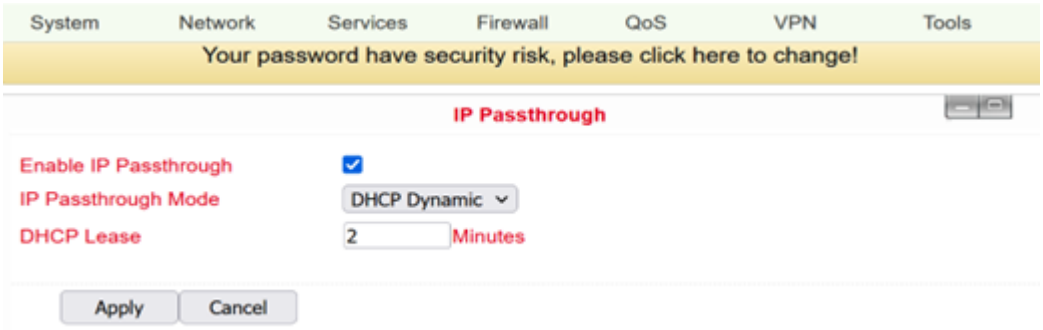


Die TK100 Serie bietet die Möglichkeit zwei unterschiedliche VRRP (VRRP I und VRRP II) Gruppen zu bilden.

Name	Beschreibung	Standard
Enable VRRP-I	Zum Aktivieren von VRRP auswählen	Deaktiviert
Group ID	Gruppen-ID für Router auswählen (Bereich 1-255)	1
Priority	Priorität für Router auswählen (Bereich 1-254)	20 (je größer die Zahl, desto höher die Priorität)
Advertisement Interval	Anzeigenintervall festlegen	60 Sekunden
Virtual IP	Virtuelle IP-Adresse für die Gruppe festlegen	Leer
Authentication Type	Optional: Typ „None/Password Authentication“	None. Wenn Password Authentication gewählt ist, kann ein Kennwort vergeben werden
Virtual MAC	Virtuelle MAC-Adresse	Deaktiviert
Monitor	Überprüfen der WAN Verbindung	None
Enable VRRP-II	Zum Aktivieren von VRRP auswählen	Deaktiviert
Group ID	Gruppen-ID für Router auswählen (Bereich 1-255)	2
Priority	Priorität für Router auswähle (Bereich 1-254)	10 (je größer die Zahl, desto höher die Priorität)
Advertisement Interval	Anzeigenintervall festlegen	60 Sekunden
Virtual IP	Virtuelle IP für die 2. Gruppe festlegen	Leer
Authentication type	Optional: Typ „None/Password Authentication“	None. Wenn Password Authentication gewählt ist, kann ein Kennwort vergeben werden
Virtual MAC	Virtuelle MAC-Adresse	Deaktiviert
Monitor	Überprüfen der WAN-Verbindung	None

4.5 IP Passthrough

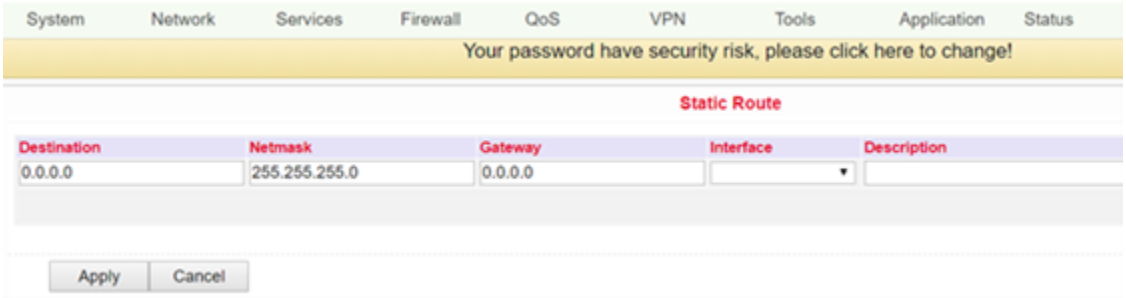
Hier können Sie die WAN IP an ein Gerät vergeben, das an einem LAN Port angeschlossen ist.



Nur ein Gerät kann diese IP-Adresse erhalten und auf das Internet zugreifen. Der LAN-Anschluss sollte vom Typ Static sein. Die Funktion funktioniert nicht mit einem Link Backup.

4.6 Static Route

Hier ist das Hinzufügen von statischen Routen möglich. Statische Routen liefern Ihrem Router zusätzliche Routinginformationen. Unter normalen Umständen verfügt der Router über ausreichende Informationen, wenn er für den Internetzugang konfiguriert wurde, und es müssen keine weiteren statischen Routen konfiguriert werden. Statische Routen müssen nur in Ausnahmefällen festgelegt werden, z. B. wenn Ihr Netzwerk mehrere Router oder IP-Subnetze enthält. Sie können statische Routen unter ***Network*** > ***Static Route*** hinzufügen, indem Sie den Add Button anklicken.



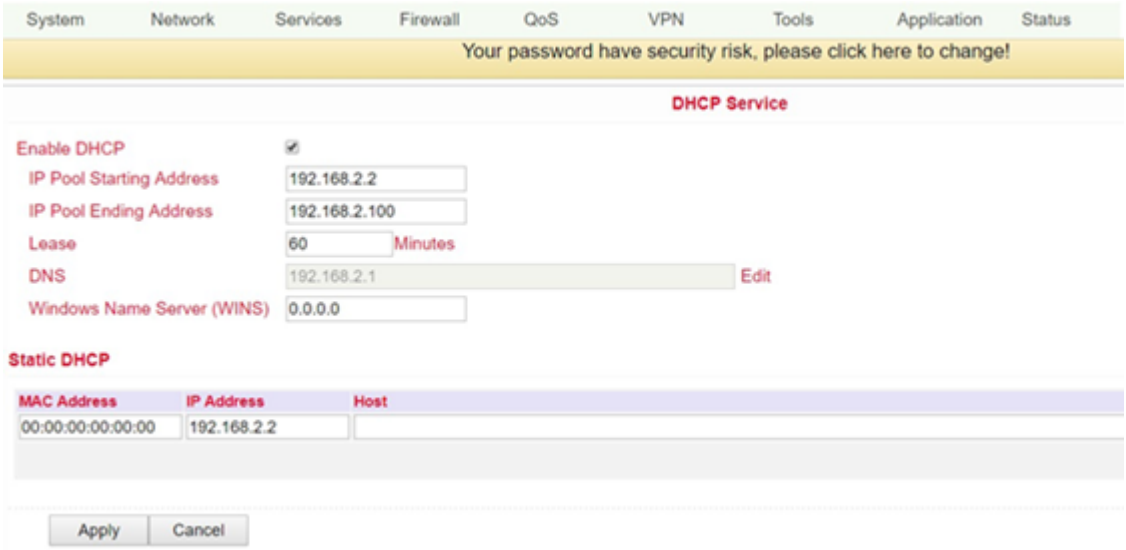
Name	Beschreibung	Standard
Destination	IP-Adresse des Ziels festlegen	Leer
Netmask	Subnetzmaske des Ziels festlegen	255.255.255.0
Gateway	Gateway des Ziels festlegen	Leer
Interface	Optionaler LAN/WAN-Portzugriff auf Ziel	Leer
Description	Frei wählbarer Name für die statische Route	Leer

5 Services

Im Rahmen der Serviceeinstellungen konfigurieren Sie den DHCP-Dienst, die DNS-Weiterleitung und andere zugehörige Parameter.

5.1 DHCP Service

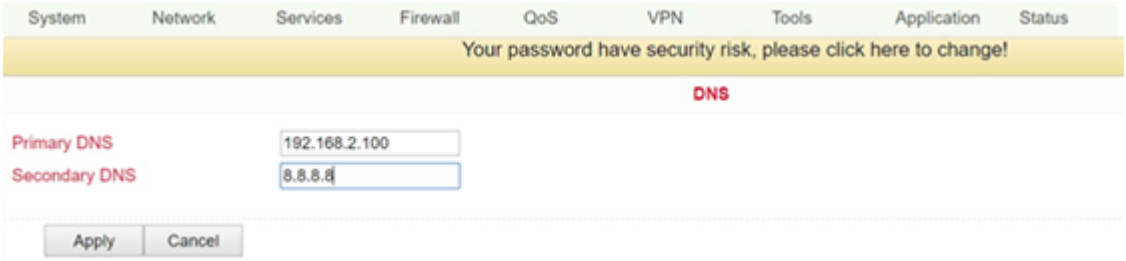
Das Dynamic Host Configuration Protocol (DHCP) ist ein Kommunikationsprotokoll in der Netzwerktechnik. Es ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server. So können Geräten im Netzwerk dynamisch IP-Adressen zugewiesen werden. Sie erreichen diesen Dienst unter ***Services > DHCP Service***.



Name	Beschreibung	Standard
Enable DHCP	Klicken, um DHCP aktivieren	Aktiviert
IP Pool Starting Address	Start-IP-Adresse des DHCP-Pools festlegen	192.168.2.2
IP Pool Ending Address	End-IP-Adresse des DHCP-Pools festlegen	192.168.2.100
Lease	Gültige Lease-Time für die vom DHCP-Server erhaltene IP-Adresse festlegen	60 Minuten
DNS	DNS-Server festlegen (klick über Edit)	192.168.2.1
Windows Name Server	WINS festlegen	Leer
Static DHCP (es können höchstens 20 IP-Adressen festgelegt werden)		
MAC Address	MAC-Adresse einer vorgesehenen IP-Adresse festlegen	Leer
IP Address	Statische IP-Adresse festlegen	192.168.2.2
Host	Hostnamen festlegen	Leer

5.2 DNS

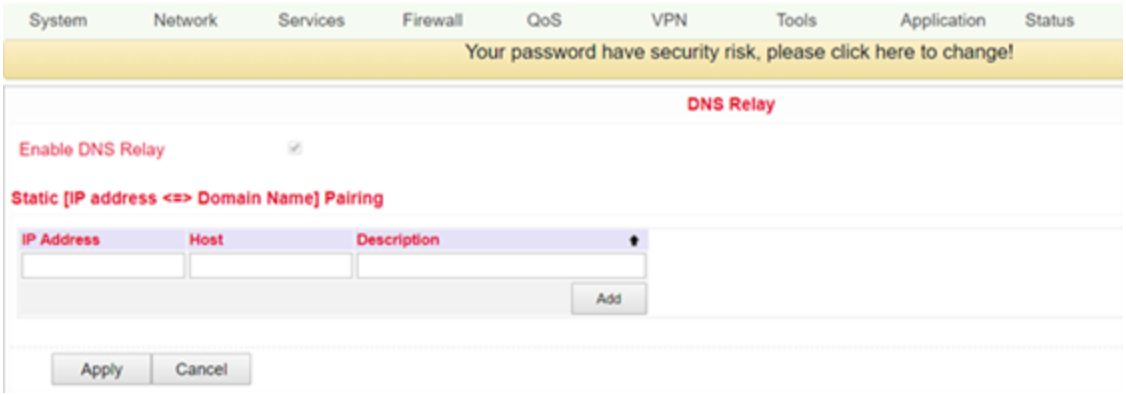
Hier können bis zu zwei DNS Server eingetragen werden, wenn der Router Teil eines Domänen-Netzwerks ist, das DNS zur Adressauflösung nutzt. Sie können die Daten unter ***Network > DNS*** eintragen.



Name	Beschreibung	Standard
Primary DNS	Primären-DNS festlegen	Leer
Secondary DNS	Sekundären-DNS festlegen	Leer

5.3 DNS Relay

Wenn DNS-Relay aktiviert ist (standardmäßig, wenn DHCP eingerichtet ist), wird den DHCP-Clients die IP-Adresse des Routers als DNS-Server zugeteilt. Alle DNS-Anfragen an den Router werden an die DNS-Server Ihres Internet-Diensteanbieters weitergeleitet. Wenn DNS-Relay deaktiviert ist, werden den DHCP-Clients vom Router die DNS-Server des Internet-Diensteanbieters zugewiesen. Sie können diese Einstellungen über ***Services > DNS Relay*** erreichen.

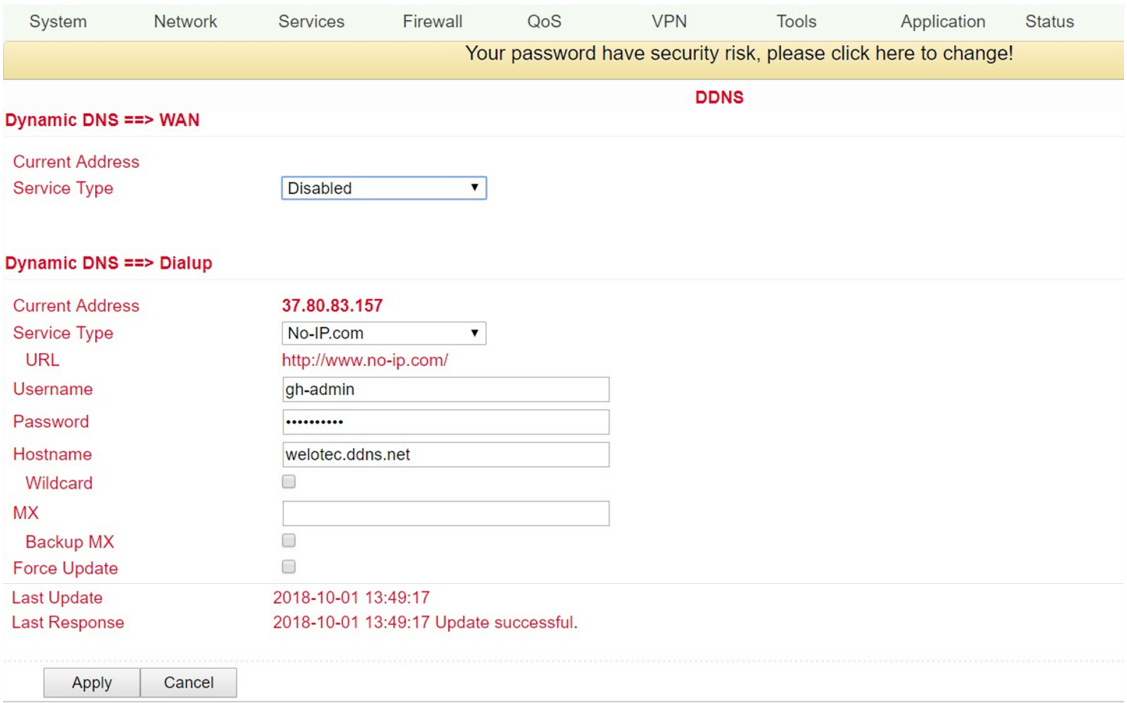


Mit dem ***Add*** Button können bis zu 20 DNS-Paare angelegt werden.

Name	Beschreibung	Standard
enable DNS Relay	Klicken, um DNS-Weiterleitung zu aktivieren	Aktiviert (nach Aktivierung von DHCP)
Static (IP Address <-> Domain Name) Pairing (höchstens 20 DNS-Paare)		
IP Address	IP-Adresse <-> DNS-Paare festlegen	Leer
Host	Namen der IP-Adresse <-> DNS-Paare festlegen	Leer
Description	IP-Adresse <-> DNS-Paare beschreiben	Leer

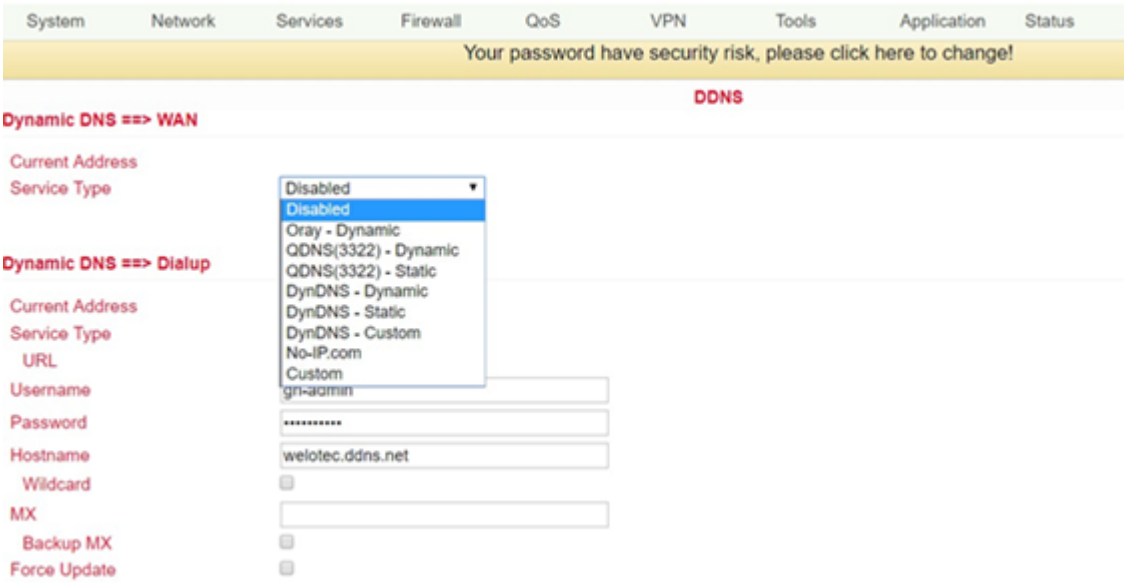
5.4 DDNS (Dynamic DNS)

DDNS oder auch dynamisches DNS wird genutzt, wenn der WAN-Anschluss keine feste öffentliche IP-Adresse hat, aber dennoch von extern auf Dienste zugegriffen werden soll. Da sich bei einem normalen WAN-Anschluss die IP-Adresse des Providers immer wieder ändern kann, ist ein gesicherter Aufbau z.B. eines VPN-Tunnels nicht möglich. Daher nutzt man Anbieter von dynamischen DNS Servern, die dafür sorgen, dass Ihr WAN-Anschluss immer über die IP-Adresse bekommt. Die Konfiguration erreichen Sie über ***Network > DDNS***.

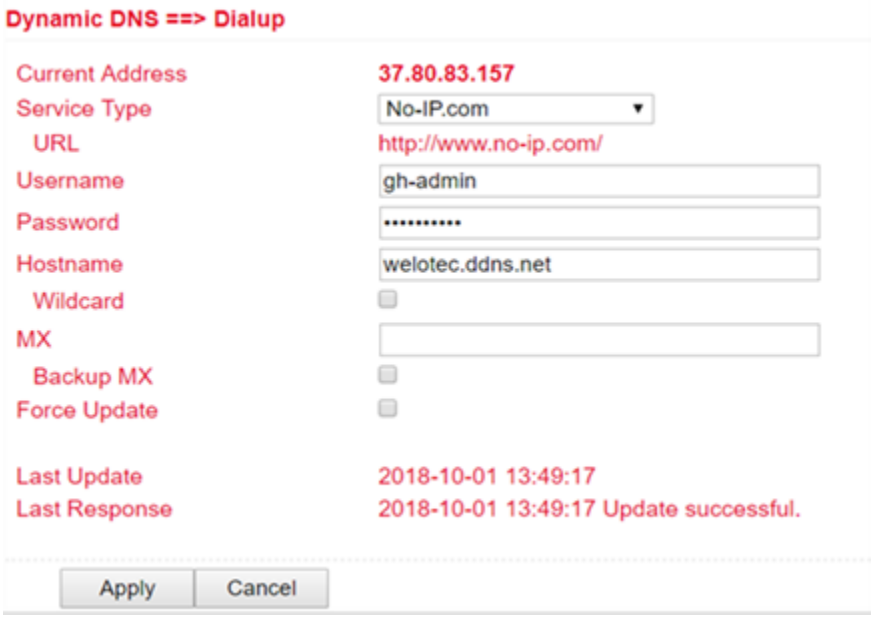


Name	Beschreibung	Standard
Current Address	Aktuelle IP-Adresse anzeigen	Leer
Service Type	DDNS-Anbieter auswählen	Deaktiviert

Es gibt diverse Einstellungsmöglichkeiten für diverse Anbieter von DDNS-Diensten. Diese wählt man über den Service Type aus.



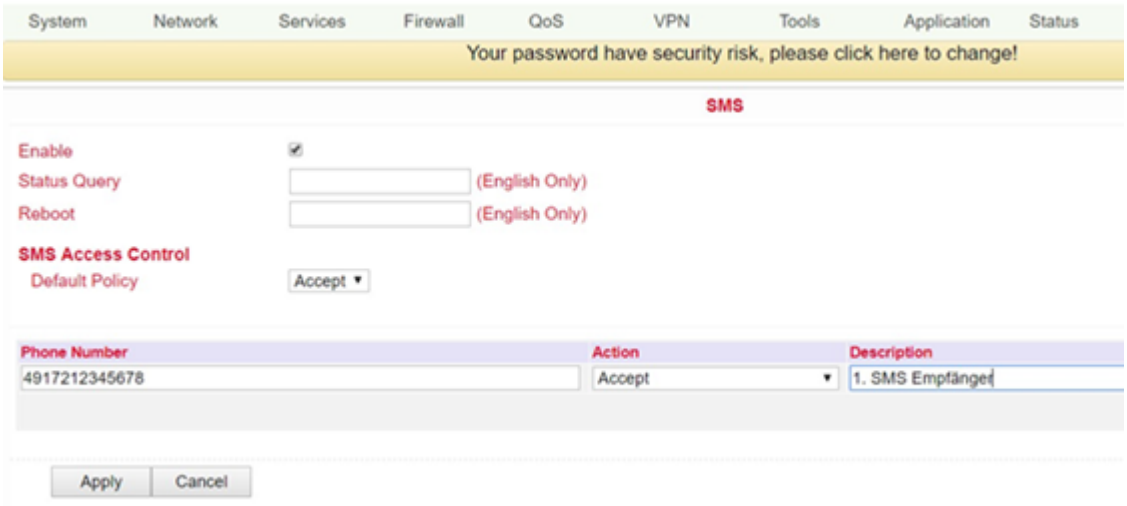
Als Beispiel für die Einrichtung dient hier No-IP. Hierfür benötigen Sie einen No-IP-Account, den Sie sich selbst anlegen müssen. Hier gibt es diverse Anbieter, die teilweise kostenlos, aber auch kostenpflichtig sind. Die Zuordnung des Dynamischen DNS kann sowohl dem WAN als auch dem Dialup-Anschluß zugeordnet werden.



Name	Beschreibung	Standard
Service Type	DynDNS - Dynamic	Deaktiviert
URL	http://www.dyndns.com/	gesetzt
Username	Registrierter Benutzername für DDNS	Leer
Password	Registriertes Kennwort für DDNS	Leer
Hostname	Registrierter Hostname für DDNS	Leer
Wildcard	Kann aktiviert werden, wenn Wildcard genutzt werden soll	Deaktiviert
MX	Eintragen eine MX-Records	Leer
Backup MX	Kann aktiviert werden, wenn MX-Record als Backup laufen soll	Deaktiviert
Force Update	Erzwingt die Aktualisierung des Accounts	Deaktiviert
Last Update	Zeigt an, wann die IP-Adresse das letzte Mal geändert wurde	
Last Response	Zeigt an, wann das letzte Mal mit dem Service kommuniziert wurde	

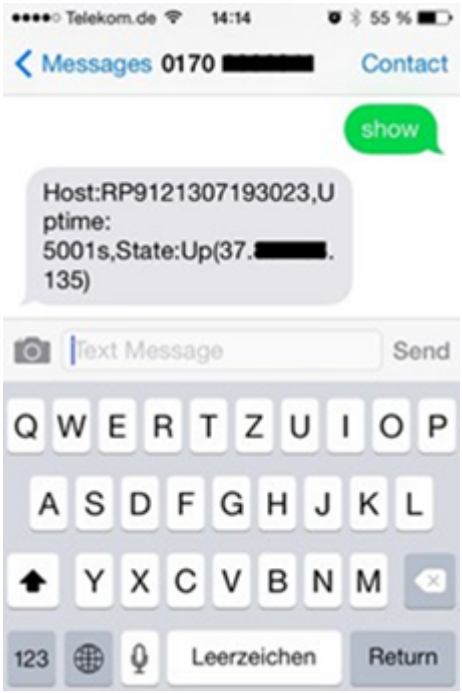
5.5 SMS

Der TK100 ist per SMS von außen erreichbar und reagiert auf verschiedene Befehle, die per SMS gesendet werden. Sie haben dabei die Möglichkeit, den Status des Gerätes abzufragen oder das Gerät neu zu starten. Konfiguriert wird der Router über ***Services*** > ***SMS***.



Name	Beschreibung	Standa
Enable	Klicken, um SMS-Kontrolle zu aktivieren oder zu deaktivieren	Deaktiviert
Status Query	Statusabfrage-SMS festlegen, um den Status des Routers per SMS anzuzeigen (z. B. : show status)	Leer
Reboot	Lässt den Router neu starten (z. B. : reboot)	Leer
SMS Access Control		
Default Policy	Kontroll-SMS von bestimmten telefon blockieren (Block) oder akzeptieren (Accept)	Accept
Phone Number	Eingabe der Telefonnummern zum Senden von SMS an router. Das Format für die Mobilnummer lautet 491712345678 (bitte kein +49 oder 0049 eingeben)	Leer
Action	Einstellung von Zulassen (Accept) oder Blockieren (Block) der zuvor eingegebenen Telefonnummer	Accept
Description	Beschreibung für den angelegten Datensatz	Leer

Um eine SMS an den Router schicken zu können, muss die Mobilnummer der eingesetzten Karte bekannt sein. An diese wird dann die SMS versendet.



SMS, die Sie auf Ihrem Mobiltelefon erhalten:

Host: (SN);

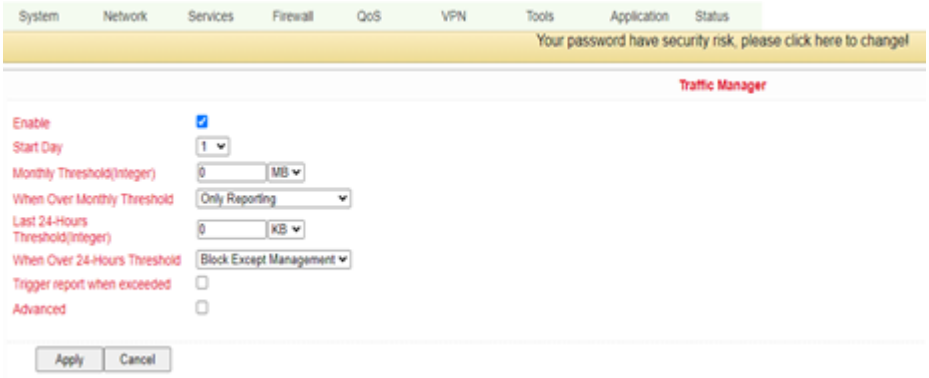
Uptime: (die Betriebszeit des Routers zum Zeitpunkt dieses Neustarts);

State: (Online/Offline) (Funk-WAN-IP)

LAN: (Bereit) (LAN-IP)

5.6 Traffic Manager

Der Traffic Manager kann genutzt werden um den Datenverbrauch des Einwahl-Verbindungsinterfaces zur Verfügung zu stellen. Sie können diesen Dienst unter ***Services > Traffic Manager*** konfigurieren.

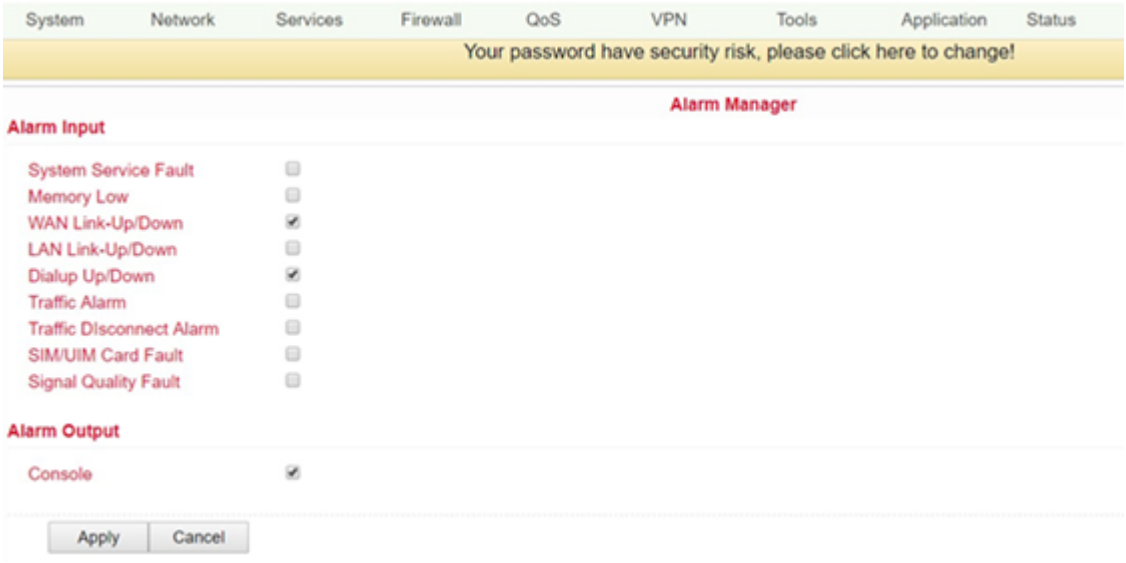


Name	Beschreibung	Standar
enable	Klicken, um SMS-Kontrolle zu aktivieren oder zu deaktivieren	Deaktiviert
Alarm Threshold	Legt die Datenmenge in MB pro Monat fest zu der ein Alarm generiert werden soll. Wird 0 als Wert gesetzt, wird kein Alarm generiert	Leer
Disconnect Threshold	Wird der eingestellte Wert erreicht, wird die Einwahlverbindung unterbrochen	Leer

Die genutzte Datenmenge kann jederzeit unter der Traffic Statistic nachgesehen werden (s. 3.8.3)

5.7 Alarm Manager

Der Alarm Manager kann genutzt werden um verschiedene Alarme zu generieren. Sie können diesen Dienst unter ***Services > Alarm Manager*** konfigurieren.



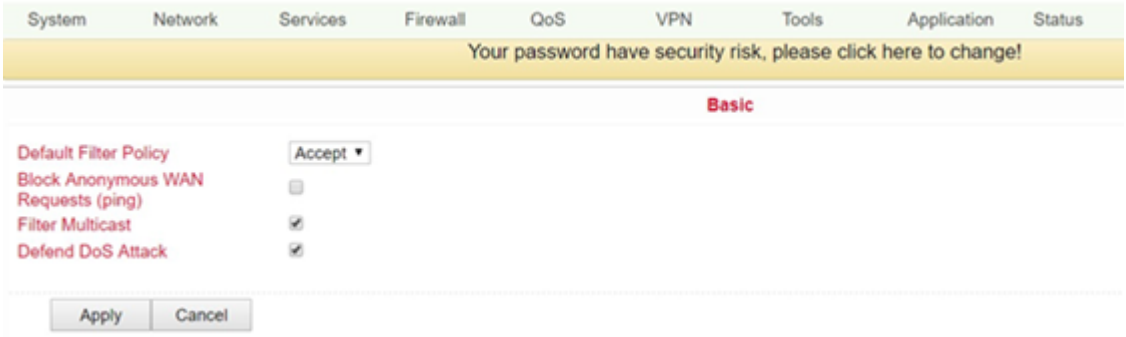
Name	Beschreibung	Standard
Alarm Inout	Wählen Sie hier die Bereiche aus, für die ein Alarm generiert werden soll	Keiner
Alarm Output	Hier können Sie wählen, ob die Alarme über die Konsole ausgegeben werden sollen oder nicht	Ausgewählt

6 Firewall

Über den Menüpunkt ***Firewall*** können Sie die Parameter für die Firewall des Routers festlegen. Hier sind verschiedene Einstellungen möglich.

6.1 Basic

Hier können die Basis-Einstellungen der Firewall konfiguriert werden.



Name	Beschreibung	Standard
Default Filter Policy	Möglich sind die Optionen „Accept“ und „Block“ also zulassen oder blockieren	Zulassen
Block Anonymous WAN Request (ping)	Aktivieren um Ping-Anforderungen, die Anonym aus dem Netz generiert werden, zu blocken	Deaktiviert
Filter Multicast	Klicken, um Filtern von Multicast zu aktivieren	Aktiviert
Defend DoS Attack	Klicken, um Abwehren von DoS-Angriffen zu aktivieren	Aktiviert

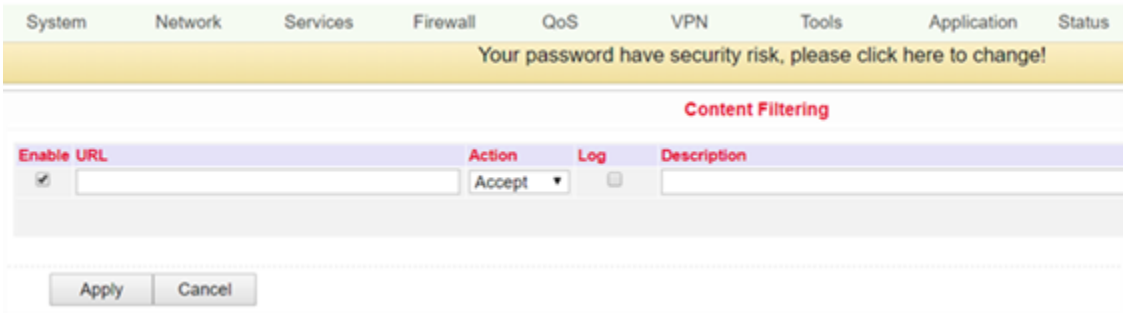
6.2 Filtering

An dieser Stelle kann gefiltert werden, was die Firewall durchlassen soll und was nicht. Hier sind verschiedene Konfigurationen möglich, die Sie über ***Firewall > Filtering*** erreichen können.

Name	Beschreibung	Standard
enable	Klicken, um das Filtering zu aktivieren	Aktiviert
Protocol	Auswahl des Protokolls. Möglich sind die Optionen „TCP“ / „UDP“ / „ICMP“	All
Source	Quell-IP-Adresse festlegen	Leer
Source Port	Quell-Port festlegen, wenn entsprechendes Protokoll gewählt wurde	Leer
Destination	Ziel-IP festlegen	Leer
Destination Port	Ziel-Port festlegen, wenn entsprechendes Protokoll gewählt wurde	Leer
Action	Auswahl, ob einstellungen erlaubt (Accept) oder geblockt (Block) werden soll	Erlaubt
Log	Klicken, um das Loggen der Einstellungen zu aktivieren	Deaktiviert
Description	Konfiguration beschreiben	Leer

6.3 Content Filtering

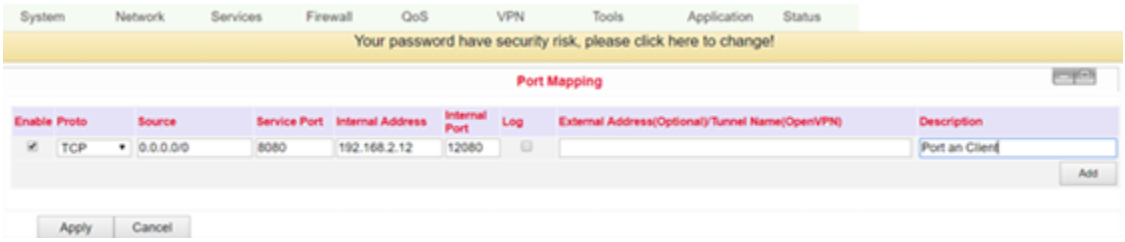
Der Content Filter in der Firewall erlaubt es den Aufruf spezieller URL´s zu filtern, die dann geblockt oder zugelassen werden können. Die Konfiguration können Sie unter ***Firewall > Content Filtering*** erstellen.



Name	Beschreibung	Standard
Enable	Aktivieren oder deaktivieren der Content Filterfunktion	Aktiviert
URL	Eintragen der zu sperrenden bzw. filternden URL	Leer
Action	Auswahl ob URL geblockt (Block) oder erlaubt (Accept) wird	Erlaubt
Log	Kann zum Loggen aktiviert werden	Deaktiviert
Description	Konfiguration beschreiben	Leer

6.4 Port Mapping

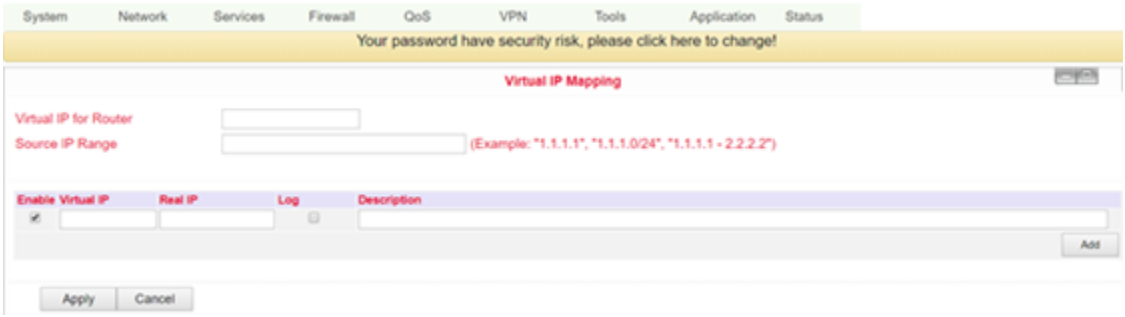
NAT-PMP (NAT Port Mapping) ermöglicht es einem Computer, in einem privaten Netzwerk (hinter einem NAT-Router) den Router automatisch so zu konfigurieren, dass Geräte hinter dem Router von außerhalb des privaten Netzwerks erreichbar sind. Es regelt im Wesentlichen das sogenannte Port Forwarding. NAT-PMP, wie UPnP auch, ermöglicht es einem Programm, alle von außen ankommenden Daten auf einem bestimmten TCP- oder UDP-Port anzufordern. Die Konfiguration können Sie unter ***Firewall > Port Mapping*** durchführen.



Name	Beschreibung	Standa
Enable	Portzuordnung aktivieren oder deaktivieren	aktiviert
Protocol	Auswahl der Protokolle TCP, UDP oder TCP&UDP	TCP
Source	Quell-IP eintragen	0.0.0.0/0
Service-Port	Port des Dienstes eintragen	8080
Internal Address	Interne IP für Zuordnung festlegen	Leer
Internal Port	Portzuordnung auf „inter“ festlegen	8080
Log	Klicken, um Protokollierung der Portzuordnung zu aktivieren	Deaktiviert
External Address (Optional) / Tunnel Name (OpenVPN)	Wird in Verbindung mit VPN genutzt. Für die Portweiterleitung mit VPN muss hier die virtuelle IP-Adresse des TK-Routers eingetragen werden	Leer
Description	Bedeutung der einzelnen Zuordnungen beschreiben	Leer

6.5 Virtual IP Mapping

Die IP eines internen PCs kann einer virtuellen IP zugeordnet werden. Über diese virtuelle IP-Adresse kann ein externes Netzwerk auf den internen PC zugreifen. Sie können diese Konfiguration unter ***Firewall > Virtual IP Mapping*** einrichten.



Name	Beschreibung	Standard
Virtual IP for Router	Virtuelle IP für Router festlegen	Leer
Source IP range	Bereich von Quell-IP-Adressen festlegen	Leer
Virtual IP	Virtuelle IP festlegen	Leer
Real IP	Reale IP festlegen	Leer
Log	Protokollierung für virtuelle IP aktivieren	Deaktiviert
Description	Konfiguration beschreiben	Leer

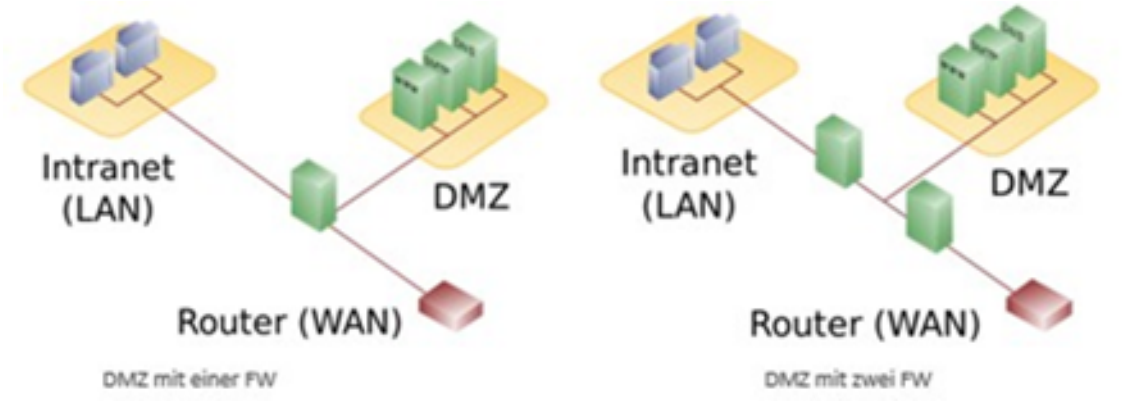
6.6 DMZ

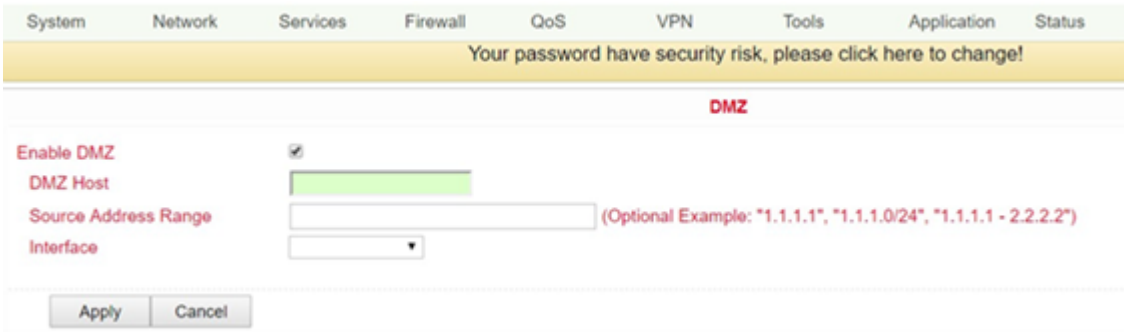
Eine Demilitarized Zone ***(DMZ, auch ent- oder demilitarisierte Zone)*** bezeichnet ein Computernetzwerk mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server.

Die in der DMZ aufgestellten Systeme werden durch eine oder mehrere Firewalls gegen andere Netze (z.B. Internet, LAN) abgeschirmt. Durch diese Trennung kann der Zugriff auf öffentlich erreichbare Dienste gestattet und gleichzeitig das interne Netz (LAN) vor unberechtigten Zugriffen von außen geschützt werden.

Der Sinn besteht darin, auf möglichst sicherer Basis Dienste des Rechnerverbundes sowohl dem Internet (WAN) als auch dem Intranet (LAN) zur Verfügung zu stellen.

Schutzwirkung entfaltet eine DMZ durch die Isolation eines Systems gegenüber zwei oder mehr Netzen.





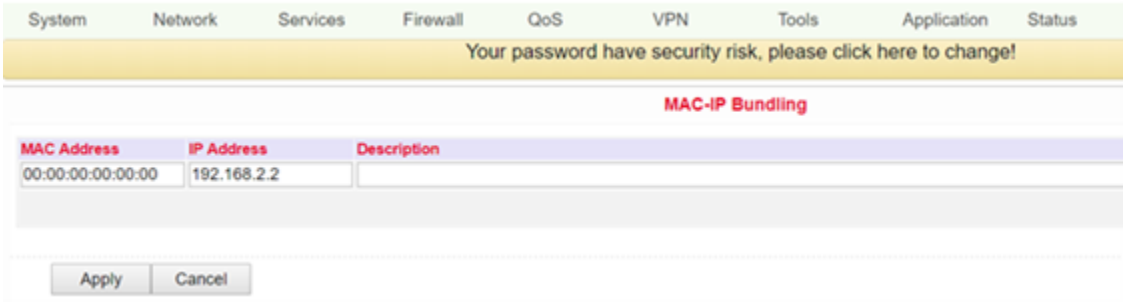
Durch die Zuordnung aller Ports und des externen PCs können Sie auf alle Ports des mit dem TK100 verbundenen Geräts zugreifen.

Mit dieser Funktion ist es nicht möglich, den Verwaltungsport des TK100 (z. B.: 80 TCP) dem Port des Geräts zuzuordnen. Um Port 80 weiterzuleiten, ändern Sie den Verwaltungsport des Routers unter ***System > Admin Access***.

Name	Beschreibung	Standard
Enable DMZ	Klicken, um DMZ zu aktivieren	Deaktiviert
DMZ Host	DMZ-Host-IP festlegen	Leer
Source Address Range	IP-Adresse mit eingeschränktem IP-Zugriff festlegen	Leer
Interface	Auswahl des entsprechenden Interfaces	Leer

6.7 MAC-IP Bundling

MAC IP Bundling bedeutet, einer definierten MAC-Adresse eine vorgegebene IP-Adresse zuzuweisen. Somit bekommt die vorgegebene MAC-Adresse immer die gleiche IP-Adresse. Sie erreichen diesen Menüpunkt unter ***Firewall > MAC-IP Bundling***.



Wird durch eine Firewall der gesamte Zugriff auf das externe Netzwerk blockiert, erhalten nur PCs mit MAC-IP Bundling Zugriff auf das externe Netzwerk.

Name	Beschreibung	Standard
MAC Address	MAC-Adresse für Bündelung festlegen	Leer
IP Address	IP-Adresse für Bündelung festlegen	192.168.2.2
Description	Konfiguration beschreiben	Leer

6.8 NAT

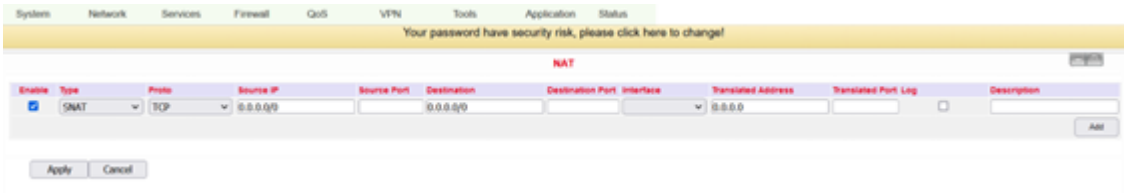
Network Address Translation (NAT) Network Address Translation ist in Rechnernetzen der Sammelbegriff für Verfahren, die automatisiert Adressinformationen in Datenpaketen durch andere ersetzen, um verschiedene Netze zu verbinden. Daher kommen sie typischerweise auf Routern zum Einsatz.

Verwendung von Source-NAT (SNAT)

Es ermöglicht Geräten mit privaten Netzwerkadressen, eine Verbindung ins Internet aufzubauen. Private IP-Adressen können üblicherweise nicht vom Provider geroutet werden, daher müssen diese in eine öffentliche, routbare IP-Adresse übersetzt werden. Der TK100 hat diese Funktion implementiert, wodurch eine Kommunikation zwischen verschiedenen Netzen ermöglicht wird. Außerdem findet sich im NAT ein relevanter Sicherheitsaspekt, da eine öffentliche IP-Adresse nicht auf die dazugehörige private IP-Adresse zurückgeführt werden kann.

Verwendung von Destination-NAT (DNAT)

Dies wird eingesetzt, um Servicedienste, die auf Computern betrieben werden, unter einer einzigen IP-Adresse anzubieten. Häufig wird es als Port-Mapping oder Port-Forwarding bezeichnet.



Konfiguration - Zur Konfiguration von NAT geht man über den Menüpunkt ***Firewall*** in den Unterpunkt ***NAT*** - Hier findet sich eine Auflistung aller vorhandenen NAT-Regeln - Über den ***Add*** Button können neue NAT-Regeln hinzugefügt werden

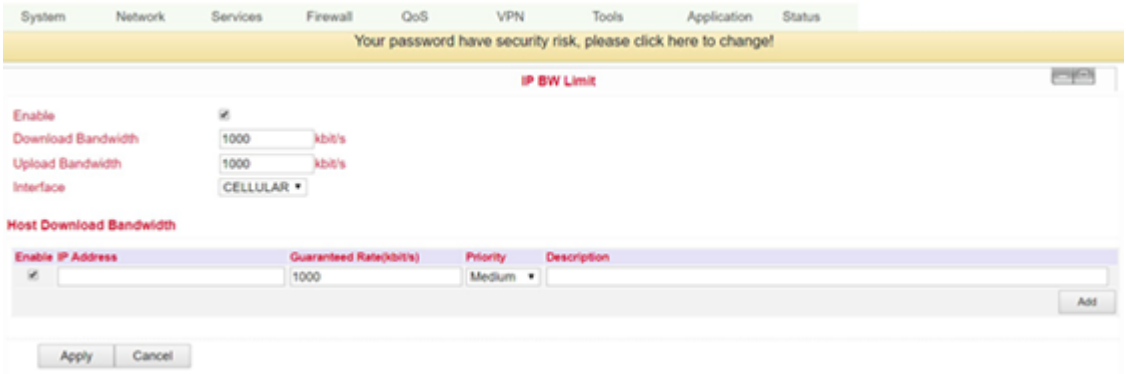
7 QoS

QoS beschreibt in der TCP/IP-Welt die Güte eines Kommunikationsdienstes aus Sicht des Anwenders. Dabei wird häufig die Netzwerk-Service-Qualität anhand der Parameter Bandbreite, Verzögerung, Paketverluste und Jitter definiert.

Die Netzbelastung beeinflusst dabei die Qualität der Übertragung. Wie lange dauert es z.B. bis ein Datenpaket beim Empfänger ankommt? Deshalb wird versucht Datenpakete mit entsprechenden Dienstklassen zu kennzeichnen. Priorisierte Datenpakete werden in Routern oder Switchen dann bevorzugt weitergeleitet. In der TK 500 Serie ist es daher möglich die Bandbreiten entsprechend zu begrenzen und zuzuordnen. Sie können dies über „***QoS***“ einrichten.

7.1 IP BW Limit

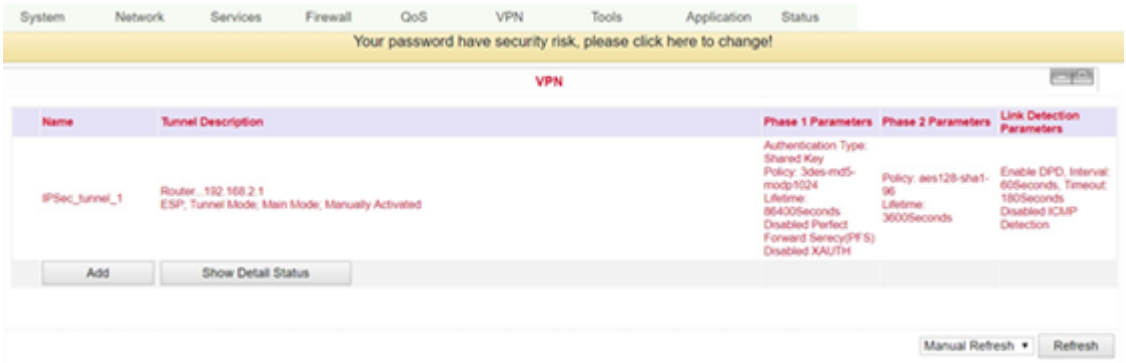
Unter dem Menüpunkt ***QoS > IP BW Limit*** können Sie die Down- bzw. Upload Bandbreite beschränken und an IP-Adressen binden, sowie diese dann priorisieren.



Name	Beschreibung	Standard
Enable	Zum Aktivieren klicken	Deaktiviert
Download Bandwith	Festlegen der Bandbreite für den Download	1000 kbit/s
Upload Bandwith	Festlegen der Bandbreite für den Upload	1000 kbit/s
Interface	Auswahl der Interfaces dem die Bandbreite zugeordnet werden soll	Cellular
Host Download Bandwith		
Enable	Aktivieren der Funktion	aktiviert
IP Address	Angabe der IP-Adresse für die Zuordnung	Leer
Guaranteed Rate (kbit/s)	Angabe der garantierten Bandbreite in kbit/s	1000
Priority	Zuweisung der Priorität	Medium
Description	Beschreibung der Regel	Leer

8 VPN

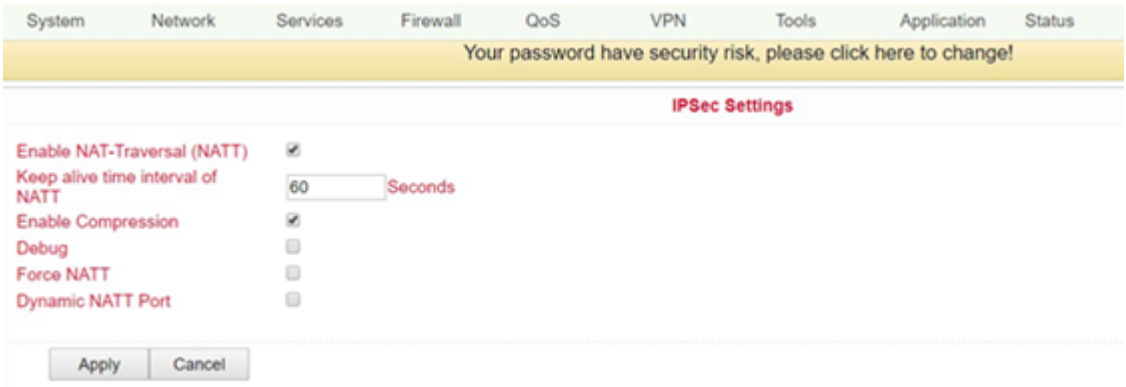
Bei einem VPN (Virtuelles privates Netzwerk) handelt es sich um ein geschlossenes logisches Netzwerk, bei dem die Teilnehmer räumlich voneinander getrennt, über einen IP-Tunnel verbunden sind. Mit diesem VPN kann man von unterwegs oder dem Home-Office auf ein lokales Netzwerk zugreifen, z.B. dem Firmennetzwerk. Dazu wird eine VPN-Software benötigt, die sowohl mit dem Router des Netzwerks kommuniziert als auch auf dem Computer installiert ist, mit dem Sie auf das Netzwerk zugreifen möchten. Es gibt verschiedene Arten von VPN-Verbindungen (Tunnel), die unter diesem Menüpunkt bei der TK 100 Serie konfiguriert werden können.



Übersicht über die vorhandenen VPN-Verbindungen. Mit ***Add*** kann ein neuer Tunnel erstellt werden, siehe 3.6.2.

8.1 IPSec Settings

In diesem Menüpunkt konfigurieren Sie die Einstellungen für das IPSec. Zu erreichen über ***VPN > IPSec Settings***.



Name	Beschreibung	Standard
Enable NAT-Traversal (NATT)	Zum Aktivieren klicken	Deaktiviert
Keep alive time interval of NATT	Festlegen der Dauer für die Aufrechterhaltung des NATT	60 Seconds
Enable Compression	Komprimierung ein- bzw. ausschalten	Aktiviert
Debug	Debugmodus ein- bzw. ausschalten	Deaktiviert
Force NATT	NATT forcieren ein- bzw ausschalten	Deaktiviert
Dynamic NATT Port	Ein- bzw. Ausschalten eines dynamischen NATT Ports	Deaktiviert

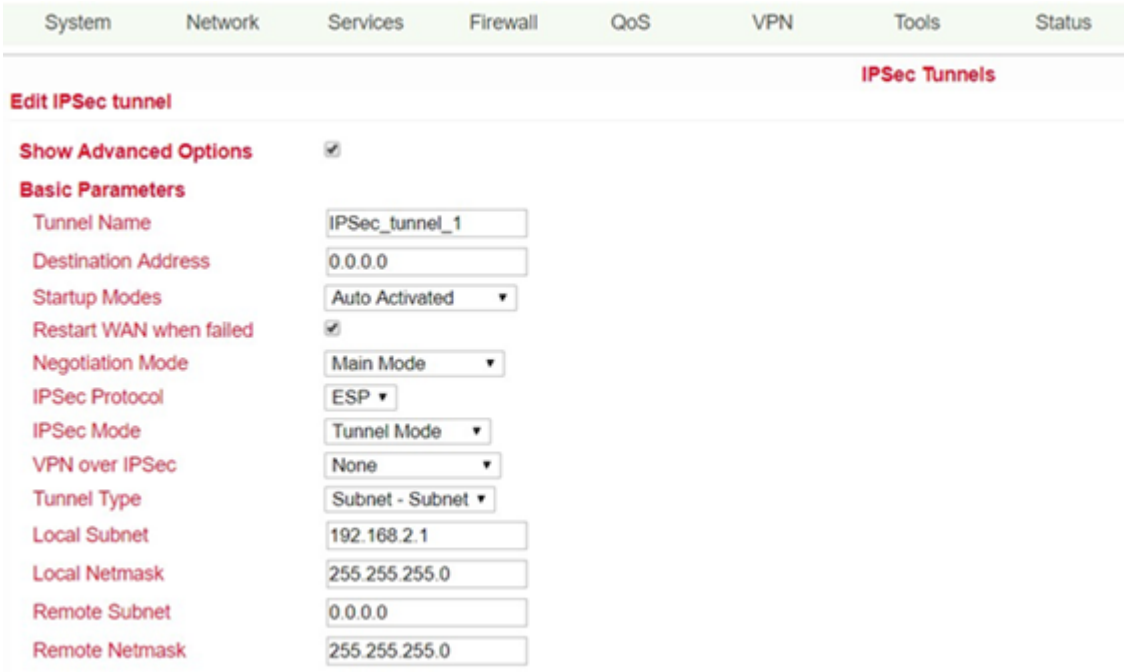
Die Adressänderung über NAT wird von einem VPN-Gateway als sicherheitskritische Veränderung der Datenpakete gewertet, die VPN-Verhandlung scheitert, es kommt keine Verbindung zustande. Diese Probleme treten z.B. bei der Einwahl über manche UMTS-Mobilfunknetze auf, bei denen die Server des Netzbetreibers die Adress-Umsetzung in Verbindung mit IPSec-basierten VPNs nicht unterstützen.

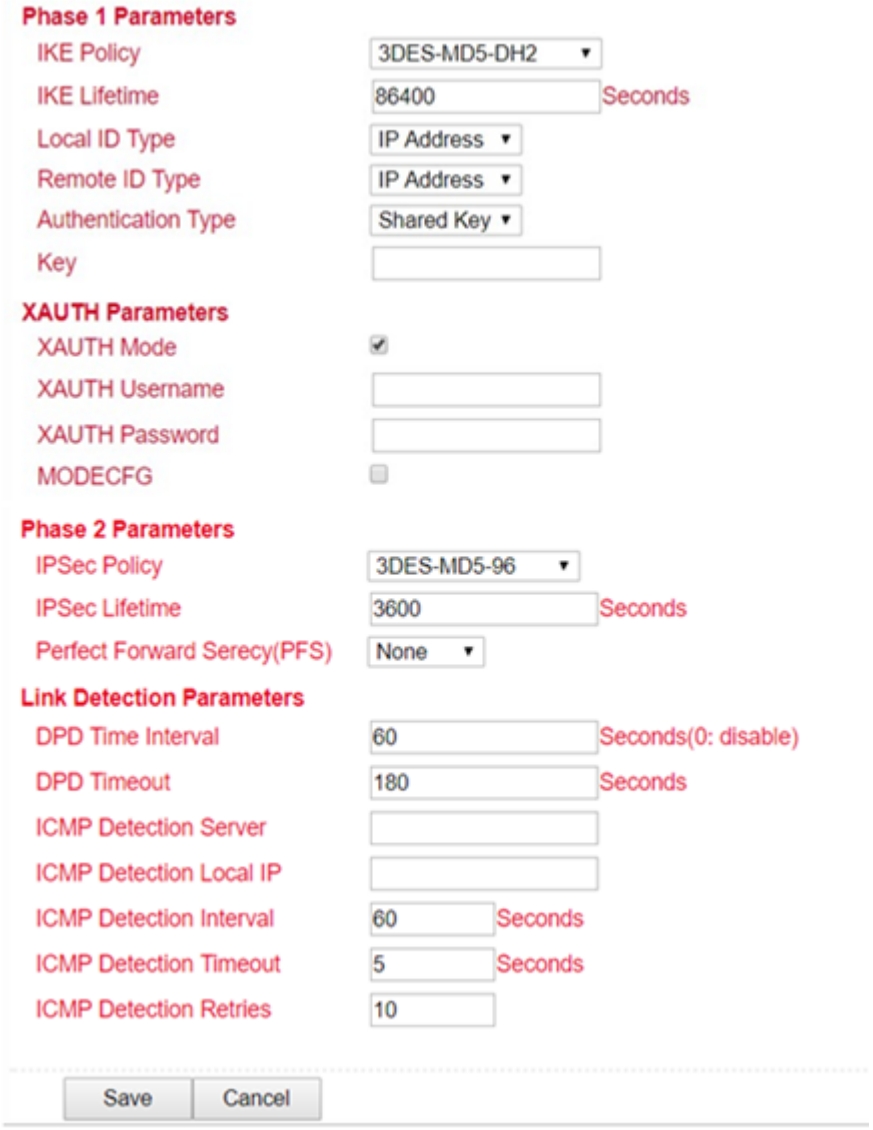
Um in diesen Fällen eine VPN-Verbindung erfolgreich aufbauen zu können, steht mit NATT (NAT Traversal) ein Verfahren bereit, diese Probleme bei der Behandlung von Datenpaketen mit geänderten Adressen zu überwinden.

NATT kann nur bei VPN-Verbindungen eingesetzt werden, die zur Authentifizierung ESP (Encapsulating Security Payload) verwenden. ESP berücksichtigt im Gegensatz zu AH (Authentication Header) bei der Ermittlung des Hashwertes zur Authentifizierung nicht den IP-Header der Datenpakete. Der vom Empfänger berechnete Hashwert entspricht daher dem in den Paketen eingetragenen Hashwert

8.2 IPSec Tunnels

Über ***VPN > IPSec Tunnels*** können Sie einen entsprechenden Tunnel einrichten.





Auf dieser Seite werden die webbasierten Parameter für den TK100 vorgestellt.

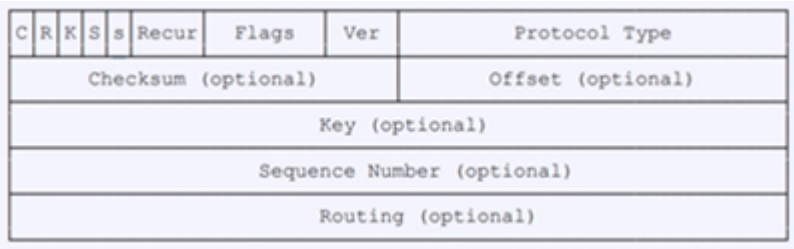
Name	Beschreibung
Show Advanced Options	Klicken, um weitere Optionen zu aktivieren
Basic Parameters	
Tunnel Name	Name für den Tunnel
Destination Address	Zieladresse des IPSec-VPN-Servers festlegen
Startup Modes	Mögliche Modi sind „Auto Active“ / „Triggered by Data“ / „Passive“ /
Restart WAN when failed	WAN interface wird bei fehlgeschlagenem Tunnelaufbau neu gestar
Negotiation Mode	Optional: „Main Mode“ oder „Aggressive Mode“
IPSec Protocol	Optional: „ESP“ oder „AH“
IPSec Mode	Optional: „Tunnelmode“ oder „Transport Mode“
VPN over IPSec	L2TP oder GRE over IPSec
Tunnel Type	Auswahlfeld für div. Einstellungsmöglichkeiten

Tab. 1 – Fortsetzung der vorherigen Seite

Name	Beschreibung
Local Subnet	Geschütztes IPSec-Subnetz festlegen (Lokal)
Local Netmask	Geschützte IPSec-Subnetzmaske festlegen (Lokal)
Remote Subnet	Geschütztes IPSec-Subnetz festlegen (Remote)
Remote Netmask	Geschützte IPSec-Subnetzmaske festlegen (Remote)
	Phase 1 Parameters
IKE Policy	Multiauswahl für die Policy
IKE Lifetime	IKE-Gültigkeitsdauer festlegen
Local ID Type	Auswahl von „FQDN“ ; „USERFQDN“ oder „IP-Address“ möglich
Remote ID Type	Auswahl von „IP-Address“ ; „USERFQDN“ ; oder „FQDN“ möglich
Authentication Type	Auswahl von „Shared Key“ oder „Certificate“ möglich
Key (Bei Auswahl des Authentifizierungstyps „Shared Key“)	IPSec-Schlüssel für VPN-Verhandlung festlegen
	XAUTH Parameters
XAUTH Mode	XAUTH Aktivieren
XAUTH Username	XAUTH Username
XAUTH Password	XAUTH Password
MODECFG	MODECFG
	Phase 2 Parameters
IPSec Policy	Multi-Auswahlliste für die Policy
IPSec Lifetime	IPSec-Gültigkeitsdauer festlegen
Perfect Forward Secrecy (PFS)	Optional „Disable“; „Group1“; „Group2“; „Group5“
	Link Detection Parameters
DPD Time Interval	DPD Zeitintervall festlegen
DPD Timeout	DPD Zeitüberschreitung festlegen
ICMP Detection Server	Server für ICMP-Erkennung festlegen
ICMP Detection Local IP	Lokale IP für ICMP-Erkennung festlegen
ICMP Detection Interval	Intervall für ICMP-Erkennung festlegen
ICMP Detection Timeout	Timeout für ICMP-Erkennung festlegen
ICMP Detection Max Retries	Höchstanzahl der Wiederholungen für ICMP-Erkennung festlegen

8.3 GRE Tunnels

Das Generic Routing Encapsulation (GRE) ist ein Netzwerkprotokoll, das von der Firma Cisco entwickelt wurde und im RFC 1701 definiert ist. Über GRE können andere Protokolle eingepackt und so in einem IP-Tunnel transportiert werden. GRE verwendet das IP Protokoll 47, der GRE-Header ist wie folgt aufgebaut:



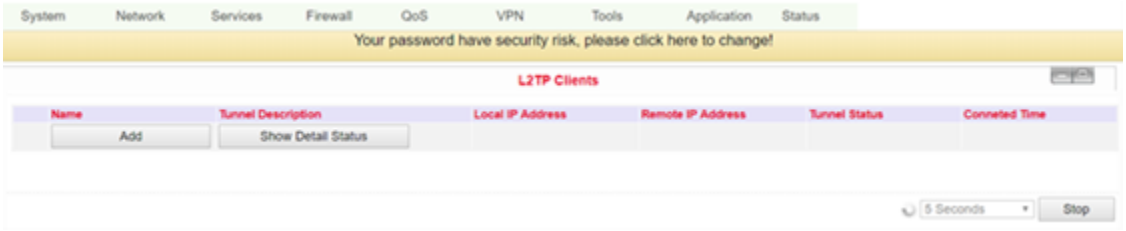
Ein GRE-Paket setzt sich also aus einem IP-Header, einem GRE-Header und der eigentlichen Nutzlast zusammen.

Einrichten können Sie diesen GRE Tunnel unter ***VPN > GRE Tunnels***.

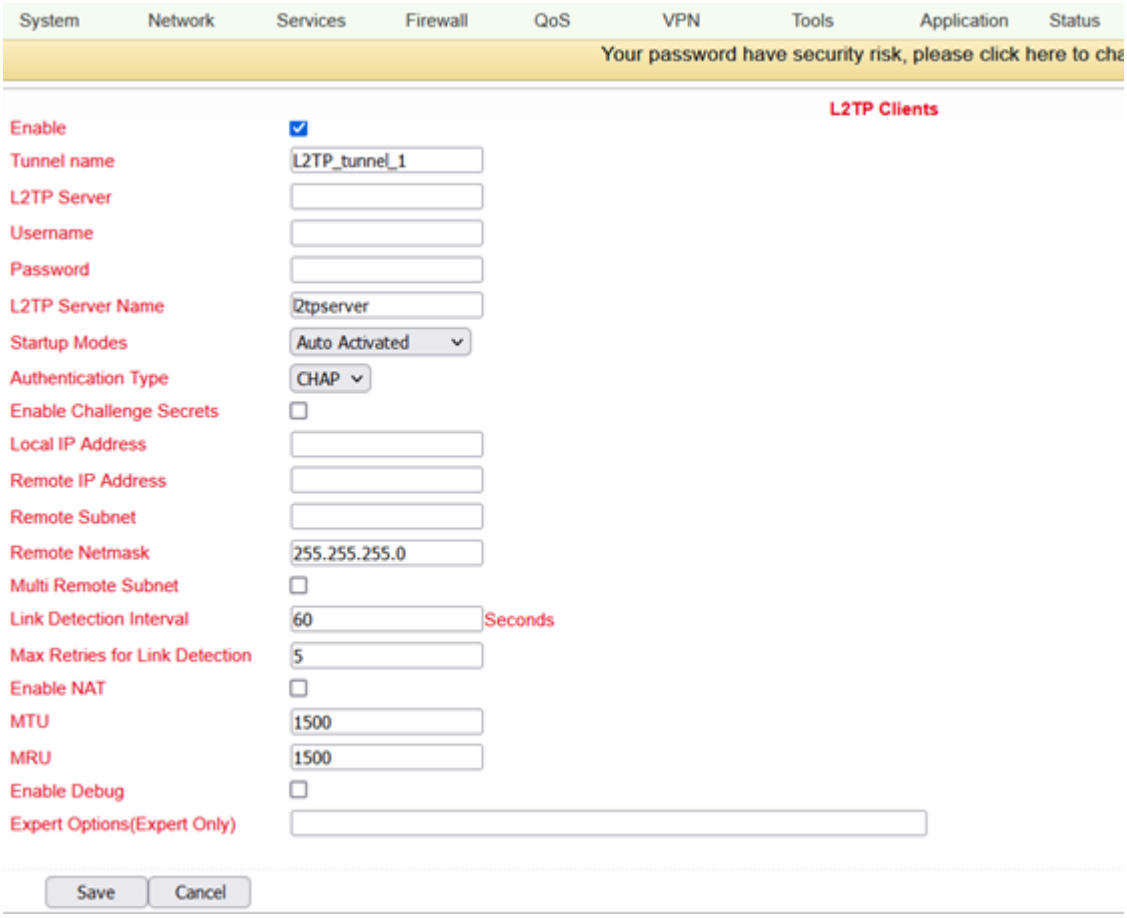
Name	Beschreibung	Standard
Enable	Zum Aktivieren klicken	Aktiviert
Tunnel Name	Namen für GRE-Tunnel festlegen	tun0
Local Virtual IP	Lokale virtuelle IP festlegen	0.0.0.0
Peer Address	Peer-Adresse festlegen	0.0.0.0
Remote Virtual IP	Virtuelle-IP des remote Netzwerks festelegen	0.0.0.0
Remote Subnet Address	Remote-Subnetzadresse festlegen	0.0.0.0
Remote Subnet Netmask	Remote-Subnetzmaske festlegen	255.255.255.0
Key	Schlüssel für die Verschlüsselung des Tunnels festlegen	Leer
NAT	Klicken, um NAT-Funktion zu aktivieren	Deaktiviert
Description	Beschreibung hinzufügen	Leer

8.4 L2TP Clients

Layer 2 Tunneling Protocol (L2TP) ist ein Netzwerkprotokoll, das Frames von Protokollen der Sicherungsschicht des OSI-Modells durch Router zwischen zwei Netzwerken über ein IP-Netz tunnelt. L2TP-Router sowie die IP-Verbindungen zwischen diesen erscheinen als L2-Switch. Der L2TP Client baut hier die Verbindung zum L2TP-Server auf. Sie erreichen die Konfiguration über ***VPN > L2TP Clients***.



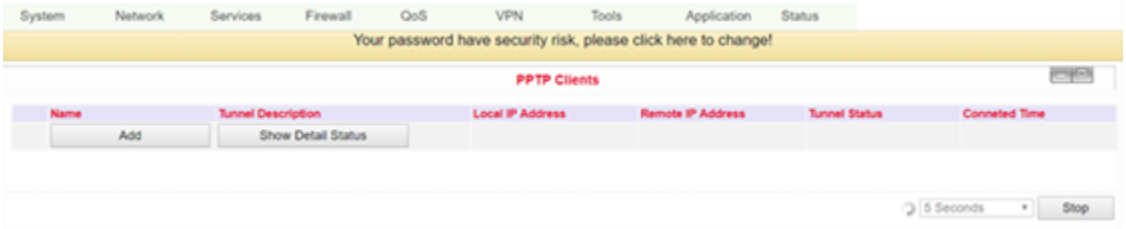
Durch klicken auf den ***Add***-Button startet man die Konfiguration des L2TP Clients.


System
Network
Services
Firewall
QoS
VPN
Tools
Application
Status
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

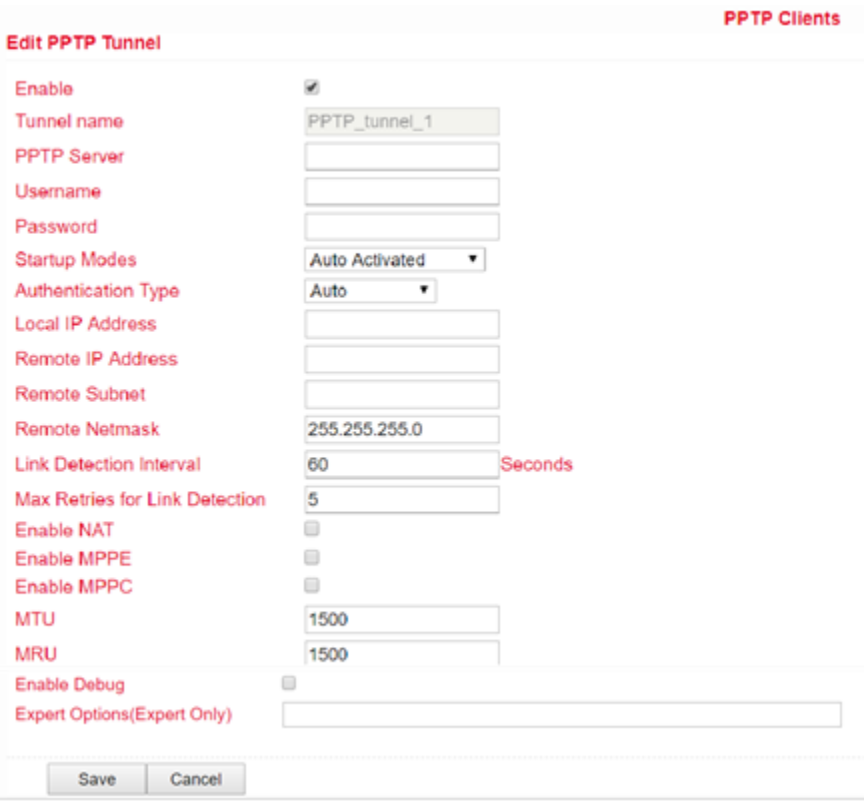
Name	Beschreibung	Standard
Enable	Aktiviert die Tunnel-Einstellungen	Aktiviert
Tunnel Name	Namen für Tunnel festlegen	L2TP_TUNNEL_1
L2TP Server	Adresse des L2TP-Server festlegen	Leer
Username	Benutzername für Server festlegen	Leer
Password	Kennwort für Server festlegen	Leer
L2TP Server Name	Namen für Server festlegen	l2tpserver
Startup Modes	Modi für Start festlegen: „Auto Activated“; „Triggered by Data“; „Manually Activated“; „L2TP0-verIPSec“	Auto Activated
Authentication Type	Authentifizierungstyp festlegen „CHAP“; „PAP“	CHAP
Enable Challenge Secrets	Zum Aktivieren von geheimen Schlüsseln (Challenge) auswählen	Deaktiviert
Challenge Secrets	Wenn Enable Challenge Secrets aktiviert ist, kann hier der geheime Schlüssel eingetragen werden	Leer
Local IP Address	Lokale IP-Adresse festlegen	Leer
Remote IP Address	Remote-IP-Adresse festlegen	Leer
Remote Subnet	Remote-Subnetz festlegen	Leer
Remote Subnet Netmask	Remote-Subnetzmaske festlegen	255.255.255.0
Link Detection Interval	Intervall für Verbindungserkennung festlegen	60
Max Retries for Link Detection	Höchstanzahl der Wiederholungen für Verbindungserkennung festlegen	5
Enable NAT	Klicken, um NAT zu aktivieren	Deaktiviert
MTU	MTU-Parameter festlegen	1500
MRU	MRU-Parameter festlegen	1500
Enable Debug Mode	Klicken, um Debug-Modus zu aktivieren	Deaktiviert
Expert Options	Expertenoptionen festlegen	Leer

8.5 PPTP Clients

PPTP (Point to Point Tunneling Protocol) ist ein VPN-Tunneling-Verfahren für Remote-Access-Verbindungen. Es baut auf den Remote Access Server für Microsoft Windows NT inklusive der Authentisierung auf. Ein PPTP-Client ist nicht nur in Windows, sondern auch in Linux und MacOS integriert. Richten Sie unter ***VPN > PPTP Clients*** den PPTP Client ein.



Zur Einrichtung eines neuen PPTP Clients klicken Sie auf den Add Button. Um Details zu einem bereits bestehenden PPTP Client einzusehen, klicken Sie bitte auf den ***Show Detail Status*** Button. Wenn Sie auf den ***Add*** Button geklickt haben, können Sie folgende Konfigurationseinstellungen machen.


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

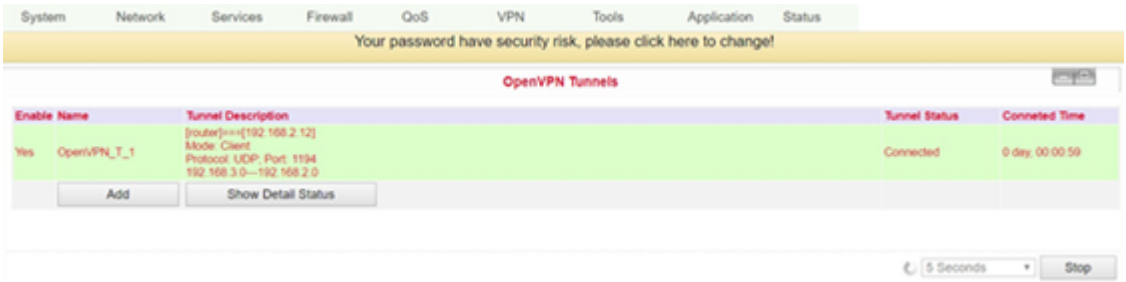
Name	Beschreibung	Standard
Enable	Zum Aktivieren klicken	Aktiviert
Tunnel Name	der name für den Tunnel (automatisch gesetzt)	PPTP_tunnel_1
PPTP Server	Adresse für PPTP-Server festlegen	Leer
Username	Benutzername für Server festlegen	Leer
Password	Kennwort für Server festlegen	Leer
Startup Mode	Modi für Start festlegen „Auto Activated“; „Triggered by Data“; „Manually Activated“	Auto Activated
Authentication Type	Authentifizierungstyp festlegen: „PAP“; „CHAP“; „MS-CHAPv1“; „MS-CHAPv2“	Auto
Local IP Address	Lokale IP-Adresse festlegen	Leer
Remote IP Address	Remote-IP-Adresse festlegen	Leer
Remote Subnet	Remote-Subnetz festlegen	Leer
Remote Subnet Netmask	Remote-Subnetzmaske festlegen	255.255.255.0
Link Detection Interval	Intervall für Verbindungserkennung festlegen	60
Max Retries for Link Detection	Höchstanzahl der Wiederholungen für Verbindungserkennung festlegen	5
Enable NAT	Klicken, um NAT zu aktivieren	Leer
Enable MPPE	Klicken, um MPPE (Microsoft Point to Point Encryption) zu aktivieren	Leer
Enable MPPC	Klicken, um MPPC (Microsoft Point to Point Compression) zu aktivieren	Leer
MTU	MTU-Parameter festlegen	1500
MRU	MRU-Parameter festlegen	1500
Enable Debug Mode	Klicken, um Debug-Modus zu aktivieren	Leer
Expert Options	Nur für Welotec R&D	Leer

8.6 OpenVPN Tunnels

OpenVPN ist eine freie Software zum Aufbau eines Virtuellen Privaten Netzwerkes (VPN) über eine verschlüsselte TLS-Verbindung. Zur Verschlüsselung wird die Bibliothek OpenSSL benutzt. OpenVPN verwendet wahlweise UDP oder TCP zum Transport.

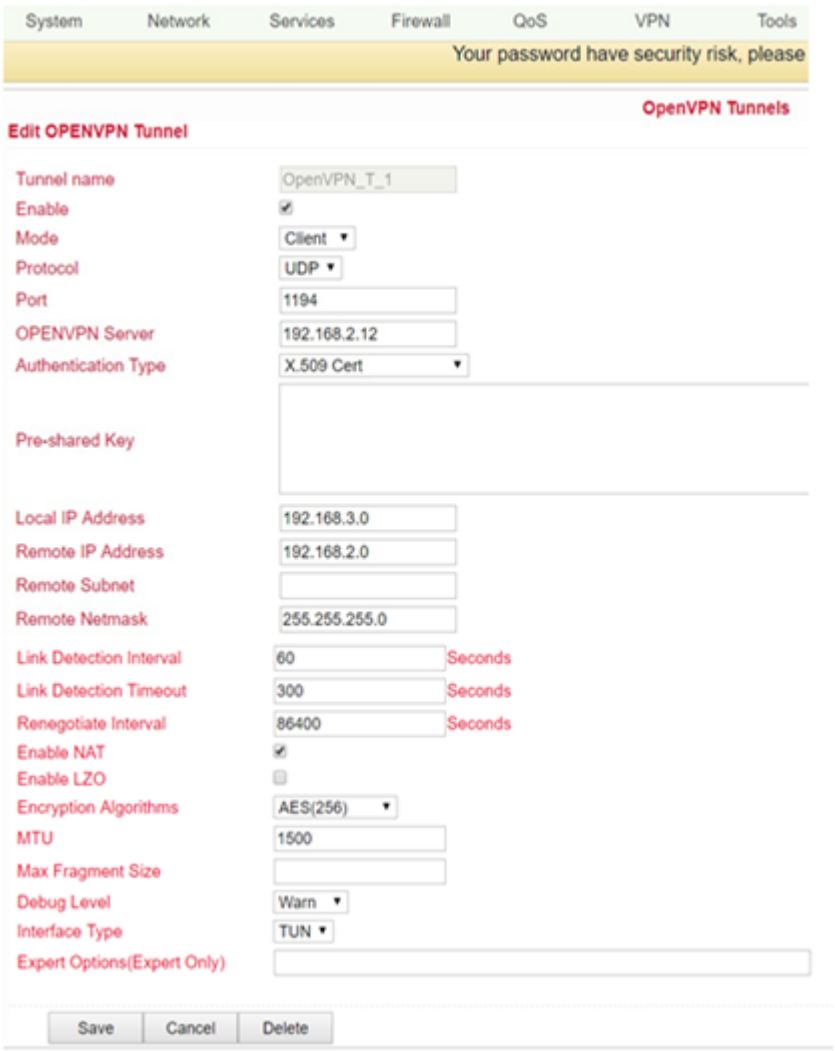
OpenVPN steht unter der GNU GPL und unterstützt Betriebssysteme, wie z.B. Linux, Windows, iOS und eine Vielzahl von angepassten Linux-basierten Endgeräten, wie z.B. Router der Serien TK 500 und TK 800.

Wählen Sie auf der Konfigurationsseite des TK100 die Optionen ***VPN > Open VPN Tunnels***, wie unten gezeigt:



Klicken Sie auf ***Add***, um einen neuen OpenVPN-Tunnel hinzuzufügen. Mit ***Show Detail Status*** können Sie sich den

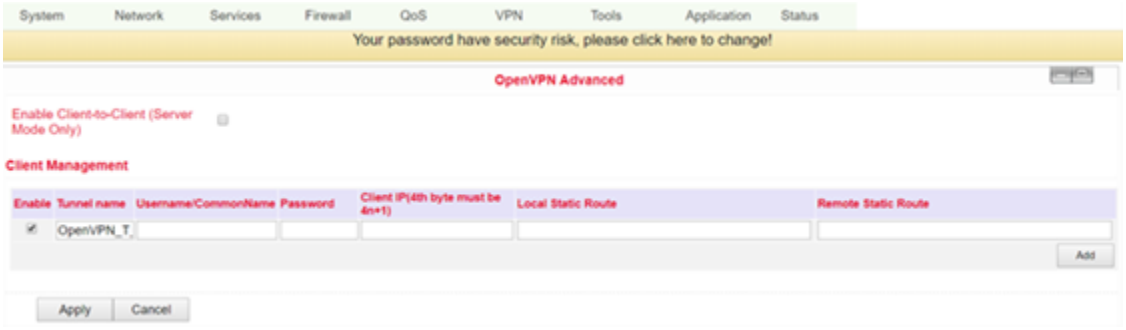
Status eines bereits konfigurierten OpenVPN Tunnels ansehen.



Name	Beschreibung
Tunnel name	Vorgegeben
Enable	Diese Konfiguration aktivieren
Mode	„Client“ oder „Server“ Modus wählen
Protocol	Auswahl des Protokolls „UDP“ oder „TCP“
Port	Standard Port für OpenVPN ist 1194
OPENVPN Server	IP oder DNS des OpenVPN-Servers
Authentication Type	Auswahl des Authentifizierungstyps. Je nach Auswahl stehen unterschiedliche Felder zur Verfügung
Pre-shared Key	Bei Auswahl Pre shared Key, gemeinsamen Schlüssel oder TLS-AUTH statisches Kennwort festlegen
Remote Subnet, Remote Netmask	Statische Route des Routers festlegen, immer in Richtung Subnetz des Peers
Username/Password	Bei Auswahl User/Password werden in diesen Feldern die entsprechenden Daten eingegeben
Link Detection Interval, Link Detection Timeout	Immer Standard verwenden
Renegotiate Interval	Immer Standard verwenden
Enable NAT	NAT-Modus festlegen, zwischenzeitlich wird Routing-Modus deaktiviert
Enable LZO	LZO-Komprimierung aktivieren
Encryption Algorithms	Verschlüsselungs-Algorithmus festlegen, muss mit Server übereinstimmen
MTU	Immer Standard verwenden, 1500
Max Fragment Size	Maximale Größe einzelner Pakete
Debug Level	Auswahl der Debug Ausgaben im Log
Interface Type	TUN / TAP
Expert Options (Expert Only)	Weitere OpenVPN Befehle (nur für erfahrene Benutzer)

8.7 OpenVPN Advanced

Diese Konfigurationsseite wird nur für den OpenVPN-Server verwendet und stellt erweiterte Funktionen zur Verfügung. Sie können diesen Punkt erreichen über ***VPN > OpenVPN Advanced***.

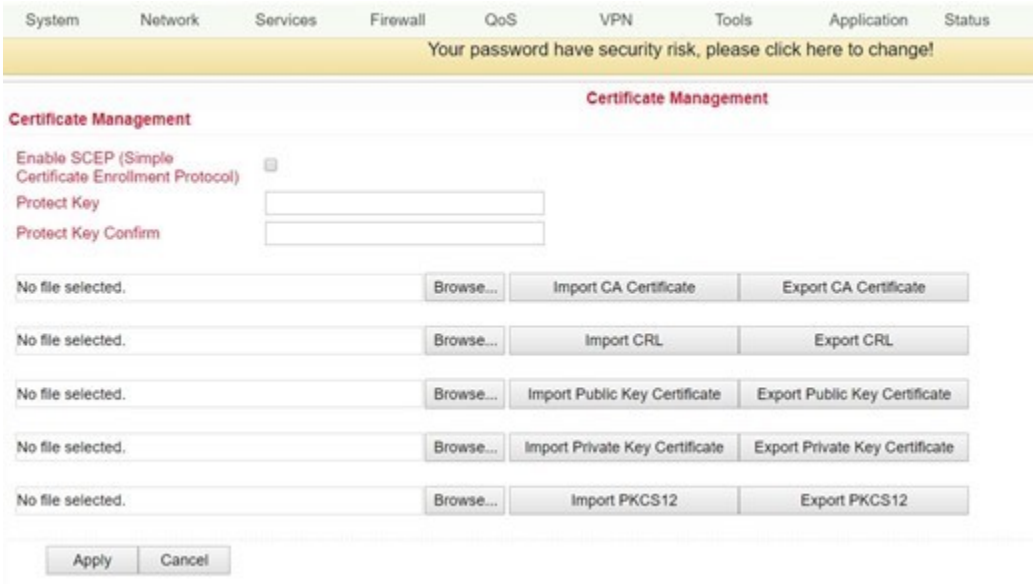


Name	Beschreibung
Enable Client-to-Client (Server Mode Only)	Clientzugriff auf andere Clients ermöglichen
Client Management	
Enable	Aktivieren der Funktion
Tunnel Name	Tunnelname des Clients
Username/Common Name	Benutzername (Verwendung des Modus „Username/Password“) oder allgemeiner Name in CA (CA-Modus)
Client IP	Angabe der Client IP-Adresse
Local Static Route	Subnetz des Clients
Remote Static Route	Subnetz des Servers

CA kann nur vom PC des Kunden erstellt werden, nicht vom TK100.

8.8 Certificate Management

Unter dem Menüpunkt ***VPN > Certificate Management*** können Sie die Zertifikate einbinden, die Sie für Ihre VPN-Verbindungen nutzen möchten. Ebenfalls können Sie bereits existierende Zertifikate exportieren.



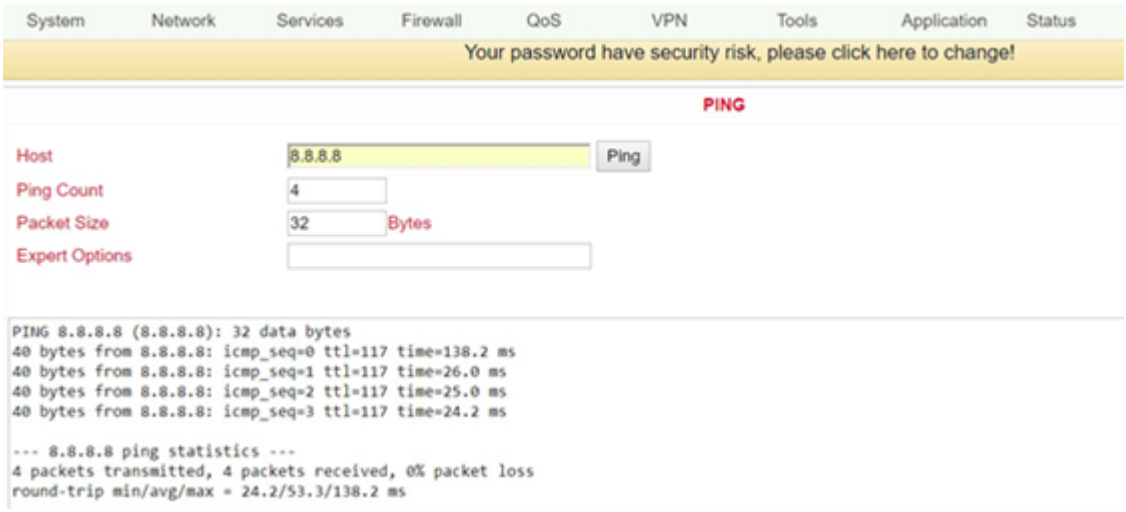
Name	Beschreibung	Standard
Enable SCEP	Zum Aktivieren klicken	
Protect Key	Festlegen eines Schlüssels zum Schutz der Zertifikate	Leer
Protect Key Confirm	Bestätigen des Schlüssels zum Schutz der Zertifikaten	Leer
Import/Export CA Certificate	CA-Zertifikat importieren oder exportieren	Leer
Import/Export Certificate (CRL)	CRL Zertifikat importieren oder exportieren	Leer
Import/Export Public Key Certifi- cate	Zertifikat für öffentlichen Schlüssel importieren/ exportieren	Leer
Import/Export Private Key Certificate	Zertifikat für privaten Schlüssel importieren oder exportieren	Leer
Import/Export PKCS12	PKCS12 (Privater Schlüssel und X.509 Zertifikat) importieren oder exportieren	Leer
Durchsuchen	Über Durchsuchen wird die jeweilige Datei ausgewählt und kann dann importiert werden	Keine Datei ausgewählt

9 Tools

Die Tools sind nützliche Werkzeuge und umfassen PING-Erkennung, Trace Route, Tests der Verbindungsgeschwindigkeit usw.

9.1 PING

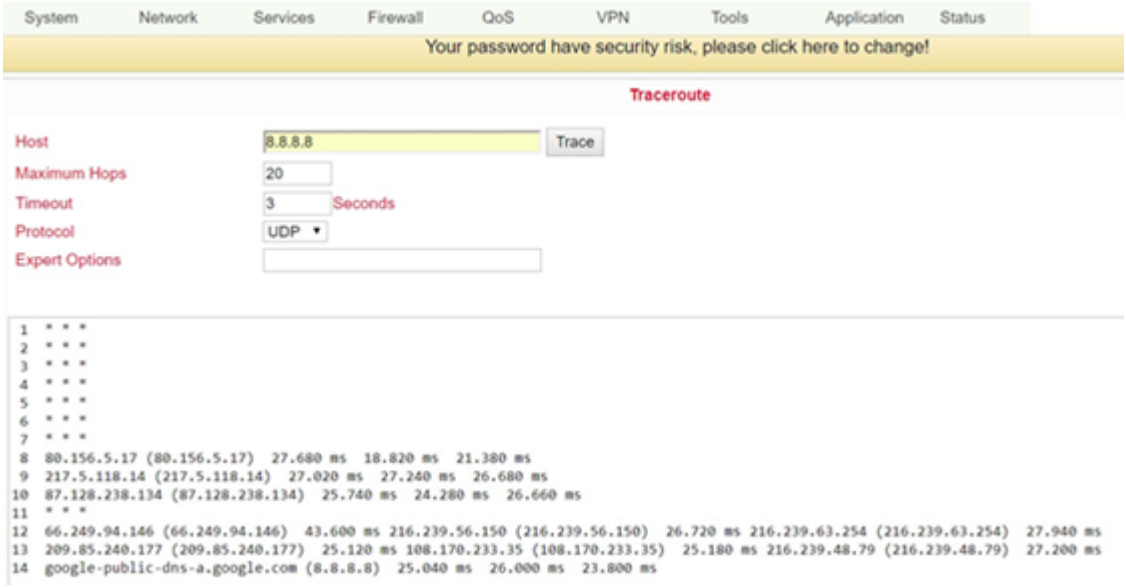
Wählen Sie den Punkt ***Tools > Ping*** wenn Sie testen möchten, ob eine Verbindung ins Netzwerk/Internet besteht.



Name	Beschreibung	Standard
Host	Ziel für PING	Leer
Ping Count	Anzahl der PINGs festlegen	4 Mal
Packet Size	Paketgröße für PING festlegen	32 Byte
Expert Options	Erweiterte Parameter	Leer

9.2 Traceroute

Traceroute (tracert) ermittelt, über welche Router und Internet-Knoten IP-Datenpakete bis zum abgefragten Rechner gelangen. Die Daten können Sie unter ***Tools > Traceroute*** eingeben.



Name	Beschreibung	Standard
Host	Ziel für Trace Route	Leer
Max Hops	Höchstanzahl der Hops festlegen	20
Time Out	Zeitüberschreitung festlegen	3 Sekunden
Protocol	Optional: „ICMP“/„UDP“	UDP
Expert Options	Erweiterte Parameter	Leer

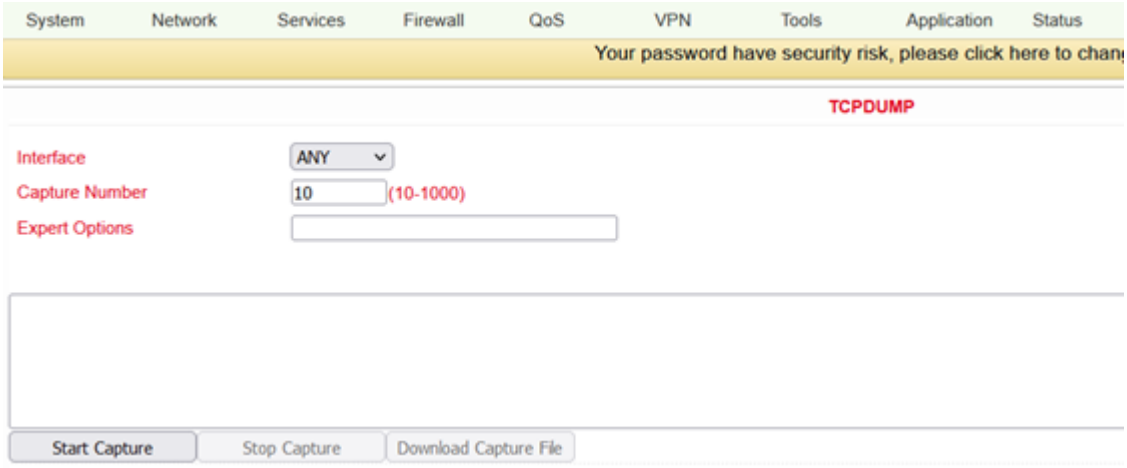
9.3 Link Speed Test

Test der Verbindungsgeschwindigkeit über Upload oder Download. Diesen Bereich wählen Sie bitte über ***„Tools > Link Speed Test.***

Über den Button ***Browse*** können Sie eine entsprechende Datei vom Rechner hochladen. Die Datei sollte zwischen 10 und 2000MB groß sein. Nach Auswahl der Datei klicken Sie auf den ***Upload*** Button. Das Resultat wird dann angezeigt

9.4 TCPDUMP

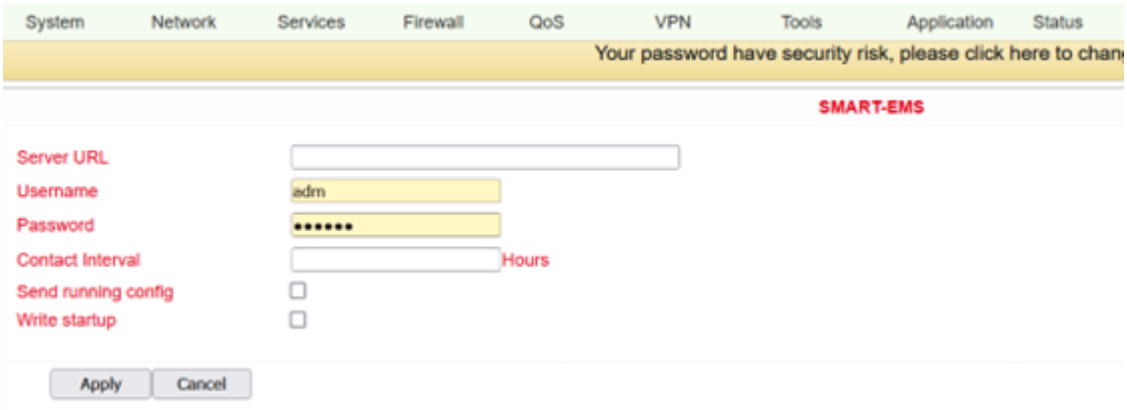
Die Funktion TCPDUMP liest Daten in Form von Paketen, die über das Netzwerk gesendet werden, und stellt diese auf dem Bildschirm dar oder speichert sie in Dateien.



10 Application

Unter dem Menüpunkt Application finden Sie die Möglichkeit ihren Router mit der Managementlösung SMART EMS der Firma Welotec zu verbinden.

10.1 SMART-EMS

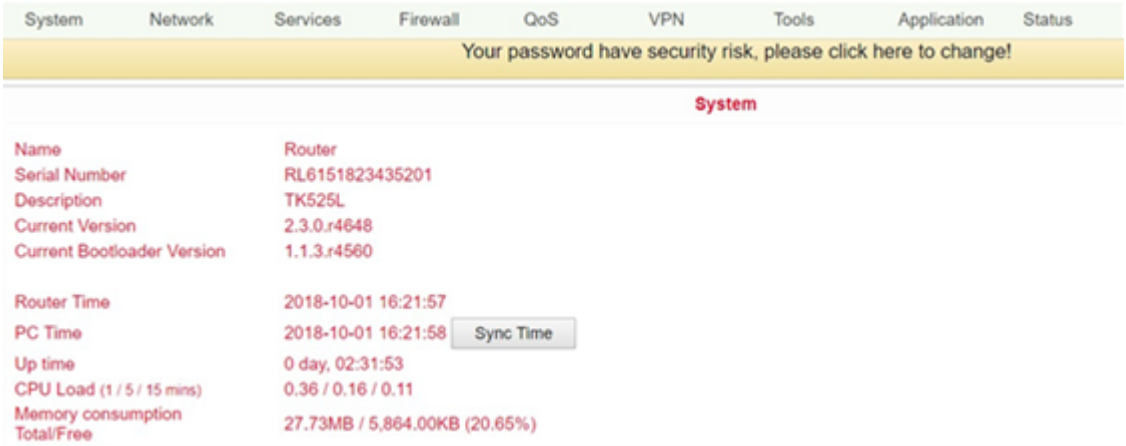


11 Status

Unter „***Status***“ erhalten Sie Informationen zu System, Modem, Netzwerkverbindungen, Routingtabelle, Geräteliste und Protokoll.

11.1 System

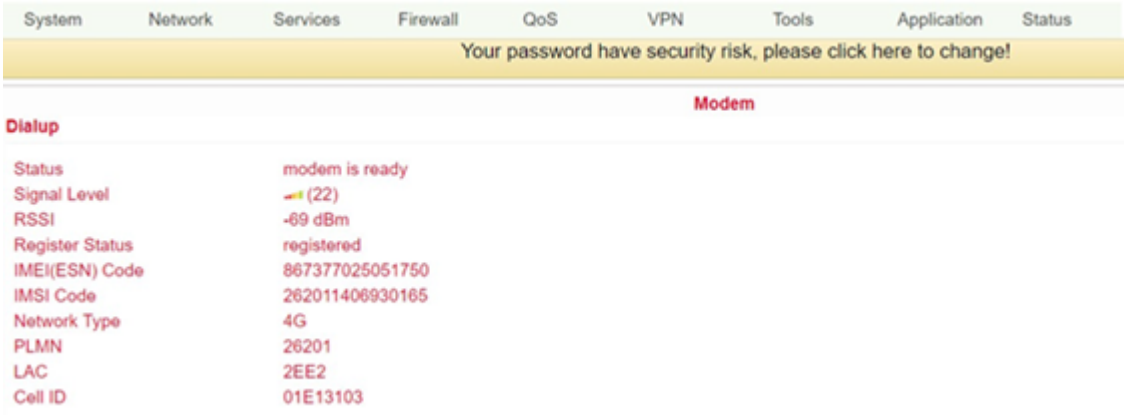
Wählen Sie aus dem Menü ***Status*** > ***System*** um Informationen über Ihr System abzurufen.



Auf dieser Seite wird der Status des Systems angezeigt, u. a. Informationen zum Namen, Modelltyp, zur aktuellen Version usw.

11.2 Modem

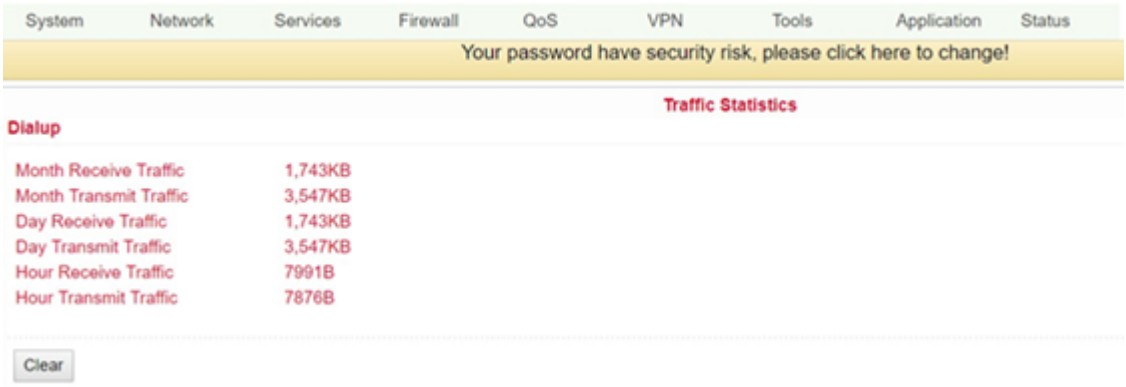
Prüfen Sie den Status Ihres Modems unter ***Status*** > ***Modem***.



Hier können Sie den Status des Modems einschließlich der Signalstärke anzeigen.

11.3 Traffic Statistics

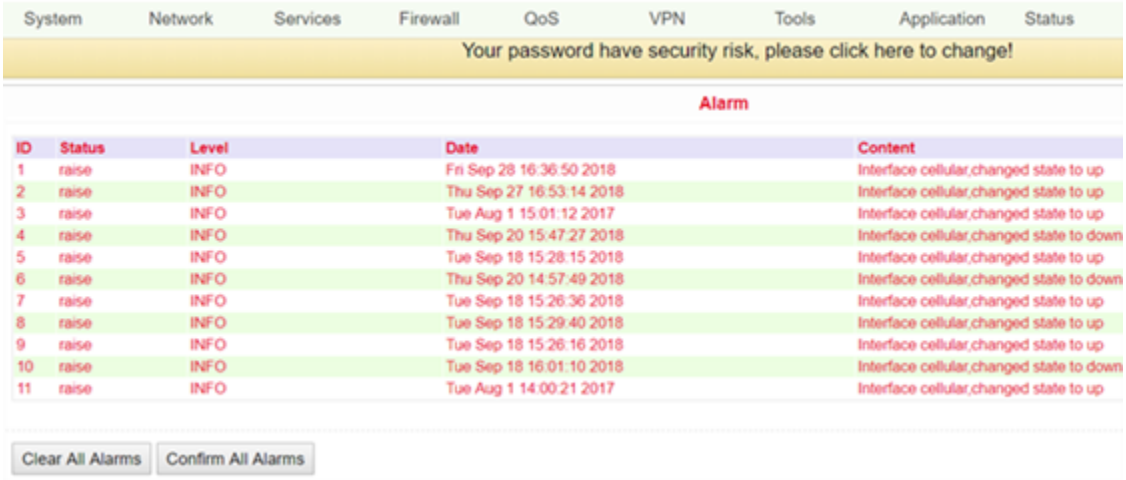
Wenn Sie den Datenverbrauch der SIM-Karte im TK100 ansehen möchten, dann können Sie dies unter ***Status*** > ***Traffic Statistics***.



Hier sehen Sie die Daten, die Monatlich, täglich und Stündlich empfangen bzw. übermittelt wurden. Über den Button „***Clear***“ können Sie die Einträge auf 0 zurücksetzen.

11.4 Alarm

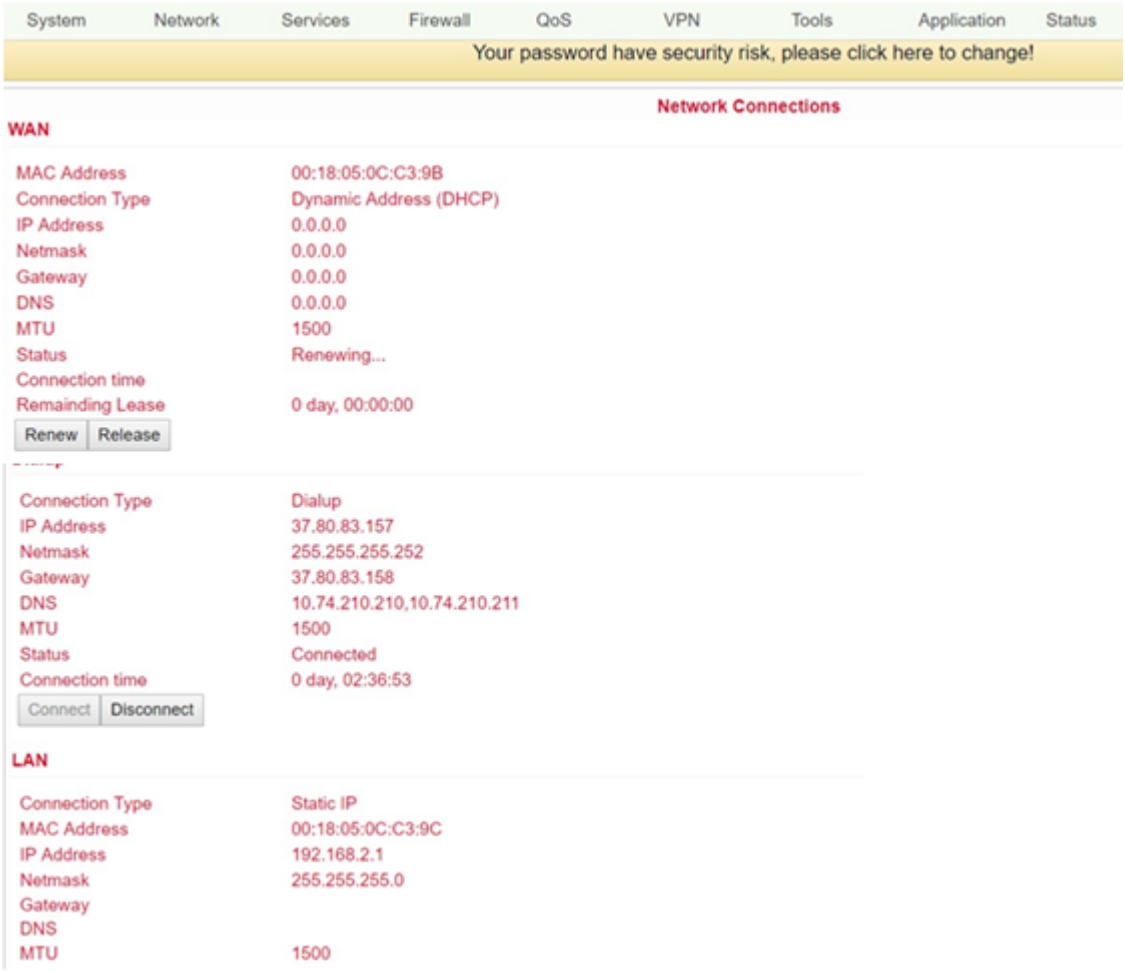
Überprüfen Sie die vom TK100 generierten Alarme, die z.B. unter 3.3.7. im Alarm Manager angelegt wurden. Sie können diesen Menüpunkt unter ***Status*** > ***Alarm*** aufrufen.



In diesem Beispiel wurde das monatliche Limit der SIM-Karte erreicht. Über den Button „***Clear All Alarms***“ können Sie alle Alarmmeldungen löschen und mit „***Confirm All Alarms***“ bestätigen Sie, dass Sie den Alarm zur Kenntnis genommen haben.

11.5 Network Connections

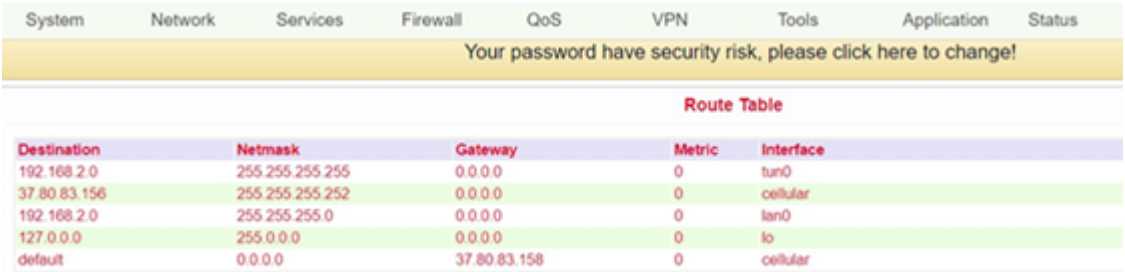
Über ***Status*** > ***Network Connections*** können Sie sich einen Überblick über die Netzwerk-Verbindungen des TK100 verschaffen.



Hier sehen Sie auf einen Blick die Netzwerkverbindungen über WAN, Dialup oder LAN.

11.6 Route Table

Wenn Sie einen Überblick über die Routingtabelle im TK100 haben möchten, wählen Sie aus dem Menü ***Status*** > ***Route Table***.



Nach Aufruf sehen Sie die Routingtabelle des TK100.

11.7 Device List

Unter dem Menüpunkt ***Status > Device List*** werden Ihnen alle Geräte angezeigt, die mit dem TK100 verbunden sind.

Überblick über die mit dem TK100 verbundenen Geräte.

11.8 Log

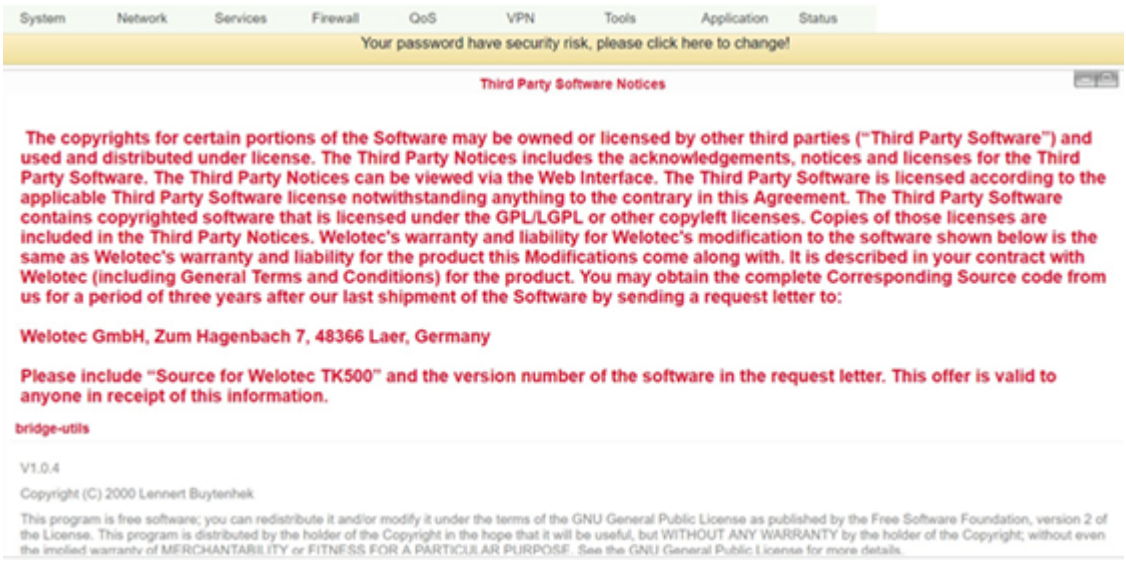
Dokumentation der System-Ereignisse (Logs) des TK100. Diesen Bereich erreichen Sie unter ***Status > Log***.

Auf dieser Seite wird das Systemprotokoll angezeigt, das hier heruntergeladen werden kann.

Es kann vorkommen, dass Probleme nicht sofort diagnostiziert und behoben werden können. In diesen Fällen bitten wir Sie, das Diagnoseprotokoll an Welotec zu senden. Klicken Sie dazu auf „***Download System Diagnosing Data***“, und schicken Sie uns das Protokoll mit einer Fehlerbeschreibung dann an [**support@welotec.com**][*Email: support@welotec.com*]

11.9 Third Party Software

Hier sind die Softwarebestimmungen und Lizenzen von allen Drittanbietern aufgeführt, die im Zusammenhang mit der Routerserie TK100 stehen.


System
Network
Services
Firewall
QoS
VPN
Tools
Application
Status
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 Technische Daten

12.1 Geräteeigenschaften

Eigenschaft	Wert
Abmessungen (B x H x T)	90 x 90 x 25 mm
Betriebsspannung	230 V AC auf 9 V – 36 V DC
Zulassung	CE-konform

12.2 Umgebungsbedingungen

Eigenschaft	Wert
Einsatztemperaturbereich	-20 bis +70 °C
Luftfeuchtigkeit	5 - 95 %, nicht kondensierend
Erschütterungen	IEC 60068-2-27
Freier Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6

12.3 Funkfrequenzen

12.3.1 Funkfrequenzen LTE Europa

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

12.3.2 Funkfrequenzen UMTS Europa

Frequenz	Frequenzbereich und Sendeleistung
Band 1	Frequenzbereich Down: 2110 MHz – 2170 MHz Frequenzbereich Up: 1920 MHz – 1980 MHz Max. Sendeleistung: 251 mW
Band 8	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung: 251 mW

12.3.3 Funkfrequenzen GSM Europa

Frequenz	Frequenzbereich und Sendeleistung
GSM 900	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung: 1995 mW
GSM 1800	Frequenzbereich Down: 1805 MHz – 1880 MHz Frequenzbereich Up: 1710 MHz – 1785 MHz Max. Sendeleistung: 40 mW

12.3.4 Funkfrequenzen LTE Asien

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

12.3.5 Funkfrequenzen UMTS Asien

Frequenz	Frequenzbereich und Sendeleistung
Band 1	Frequenzbereich Down: 2110 MHz – 2170 MHz Frequenzbereich Up: 1920 MHz – 1980 MHz Max. Sendeleistung: 251 mW
Band 8	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung: 251 mW

12.3.6 Funkfrequenzen GSM Asien

Frequenz	Frequenzbereich und Sendeleistung
GSM 900	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung: 1995 mW
GSM 1800	Frequenzbereich Down: 1805 MHz – 1880 MHz Frequenzbereich Up: 1710 MHz – 1785 MHz Max. Sendeleistung: 1000 mW

12.3.7 Funkfrequenzen UMTS Global

Frequenz	Frequenzbereich und Sendeleistung
Band 1	Frequenzbereich Down: 2110 MHz – 2170 MHz Frequenzbereich Up: 1920 MHz – 1980 MHz Max. Sendeleistung: 251 mW
Band 8	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung: 251 mW

12.3.8 Funkfrequenzen GSM Global

Frequenz	Frequenzbereich und Sendeleistung
GSM 900	Frequenzbereich Down: 925 MHz – 960 MHz Frequenzbereich Up: 880 MHz – 915 MHz Max. Sendeleistung: 1995 mW
GSM 1800	Frequenzbereich Down: 1805 MHz – 1880 MHz Frequenzbereich Up: 1710 MHz – 1785 MHz Max. Sendeleistung: 40 mW

13 Support

Senden Sie bei Problemen mit der Installation und dem Betrieb eine E-Mail an folgende Adresse: [*support@welotec.com*][*Email: support@welotec.com*]

14 CE Konformitätserklärung

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