TK600

Ausführung:
v1.0.0

Datum:
13.10.2023

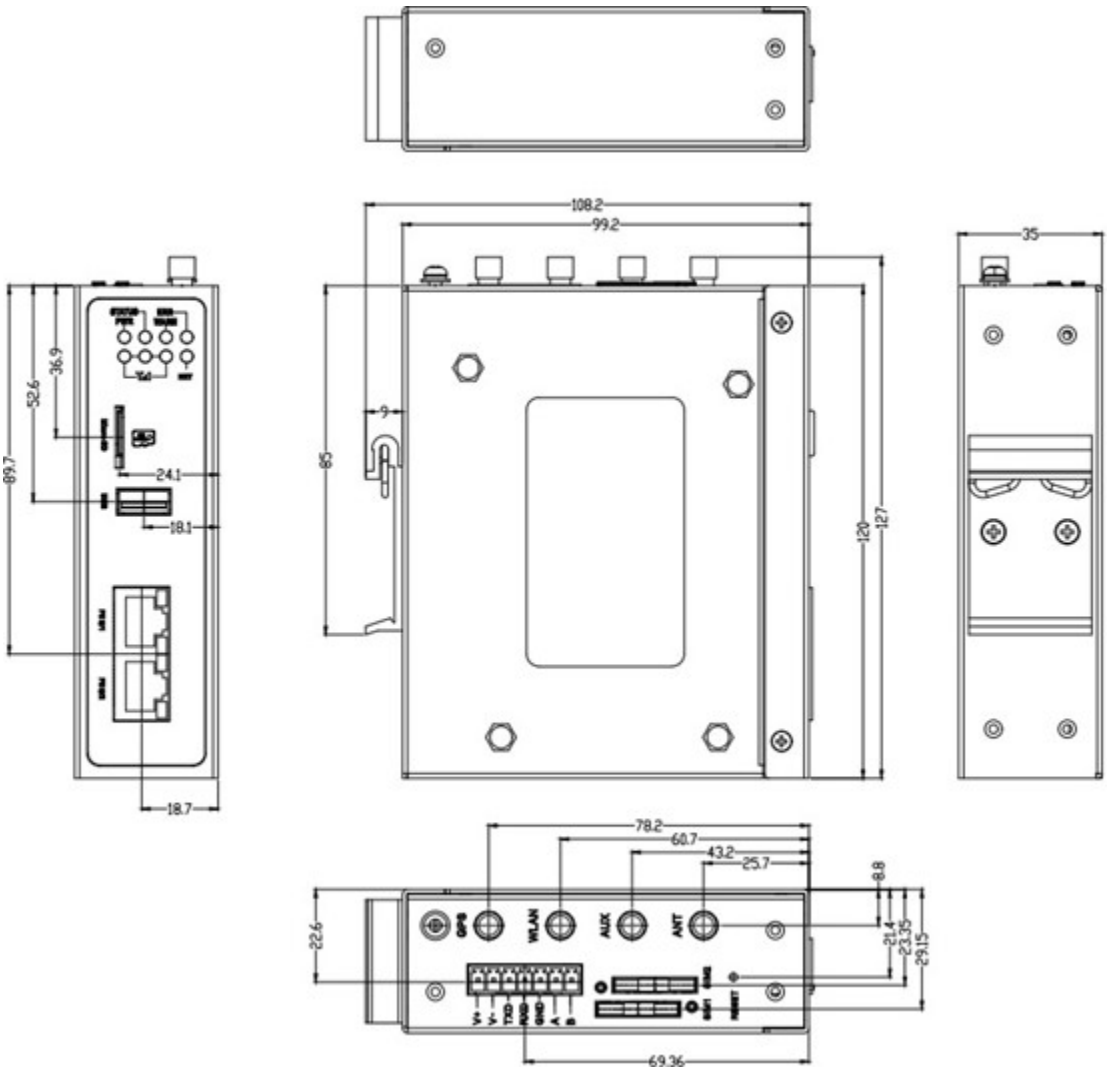
Inhaltsverzeichnis

1 Einleitung

Dieses Dokument beschreibt die Installation und den Betrieb des Routers der TK600-Serie. Bevor Sie diese Produkte verwenden, vergewissern Sie sich, dass das Produktmodell und die Anzahl der in der Verpackung enthaltenen Zubehörteile korrekt sind, und erwerben Sie eine SIM-Karte bei Ihrem örtlichen Netzanbieter.

1.1 Panel

1.2 Aufbau und Abmessungen



2 Installation

2.1 Vorsichtsmaßnahmen:

- Stromversorgungsanforderungen: 24V DC (12 - 48V DC).
- Umgebungsbedingungen: Betriebstemperatur -20°C bis 70°C; Lagertemperatur -40°C bis 85°C; Luftfeuchtigkeit 5% bis 95% (nicht kondensierend). Die Temperatur auf der Geräteoberfläche kann hoch sein. Installieren Sie das Gerät in einem unzugänglichen Bereich und prüfen Sie die Umgebung.
- Vermeiden Sie direkte Sonneneinstrahlung und halten Sie das Gerät fern von Wärmequellen oder Bereichen mit starken elektromagnetischen Inteferenzen.
- Installieren Sie den Router auf einer industriellen DIN-Schiene.
- Prüfen Sie, ob die erforderlichen Kabel und Stecker angeschlossen sind.

2.2 Montage und Demontage des Geräts auf einer DIN-Schiene

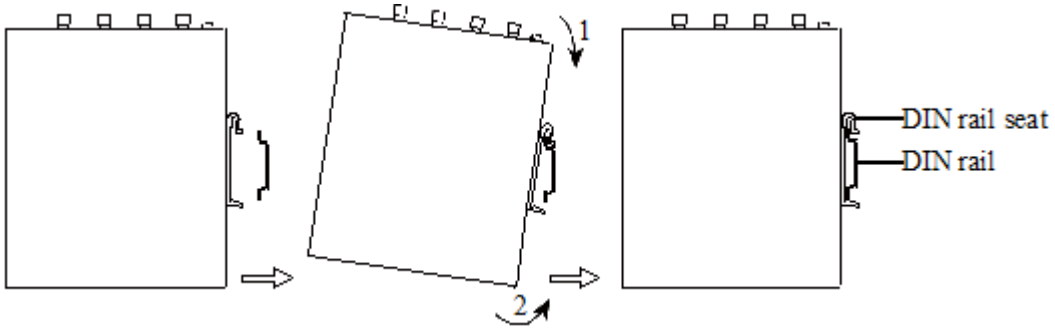
2.2.1 Montage mit einer DIN-Schiene

Vorgehensweise:

Schritt 1: Wählen Sie einen Montageort und planen Sie genügend Platz für die Montage ein.

Schritt 2: Setzen Sie den oberen Teil des DIN-Schienensitzes auf die DIN-Schiene. Nehmen Sie das untere Ende des Geräts an und drehen Sie es mit leichtem Druck nach oben in Richtung des Pfeils 2, um den DIN-Schienensitz auf die DIN-Schiene zu setzen.

Prüfen Sie, ob das Gerät korrekt auf der DIN-Schiene sitzt, wie in der folgenden Abbildung rechts dargestellt.

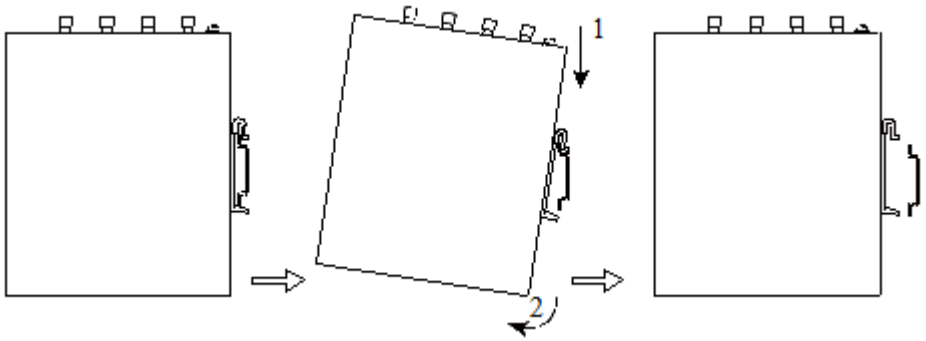


2.2.2 Demontage mit einer DIN-Schiene

Vorgehensweise:

Schritt 1: Drücken Sie das Gerät in der durch Pfeil 1 angegebenen Richtung nach unten, um einen Spalt in der Nähe des unteren Endes des Geräts zu schaffen, so dass das Gerät von der DIN-Schiene getrennt wird.

Schritt 2: Drehen Sie das Gerät in die mit Pfeil 2 angegebene Richtung, halten Sie das untere Ende des Geräts fest und bewegen Sie es nach außen. Heben Sie das Gerät an, wenn das untere Ende von der DIN-Schiene getrennt ist. Nehmen Sie dann das Gerät von der DIN-Schiene ab.



2.3 Installieren einer SIM Karte

TK600 unterstützt Dual-SIM-Karten.

2.4 Installieren einer Antenne

Drehen Sie den beweglichen Teil der SMA-Metallschnittstelle mit leichter Kraft, bis er sich nicht mehr drehen lässt und das Außengewinde des Antennenanschlusskabels nicht mehr sichtbar ist. Verdrehen Sie die Antenne nicht mit Gewalt, indem Sie die schwarze Kunststoffabdeckung anfassen.

2.5 Installieren des Netzteils

2.5.1 Vorgehenswese:

Schritt 1: Entfernen Sie den Terminalblock vom Router.

Schritt 2: Lösen Sie die Sicherungsschraube am Terminalblock.

Schritt 3: Schließen Sie das Netzkabel an den Terminalblock an und befestigen Sie die Sicherungsschraube.

2.6 Installieren des Erdungsschutzes

2.6.1 Vorgehensweise:

Schritt 1: Lösen Sie die Erdungsschraubkappee.

Schritt 2: Legen Sie die Erdungsschleife des Schrankerdungskabels auf den Erdungspfosten.

Schritt 3: Befestigen Sie die Erdungsschraubenkappe.

Caution

Erden Sie den Router, um seine Inteferenzresistenz zu verbessern. Schließen Sie das Erdungskabel je nach Betriebsumgebung an den Erdungspfosten des Routers an.

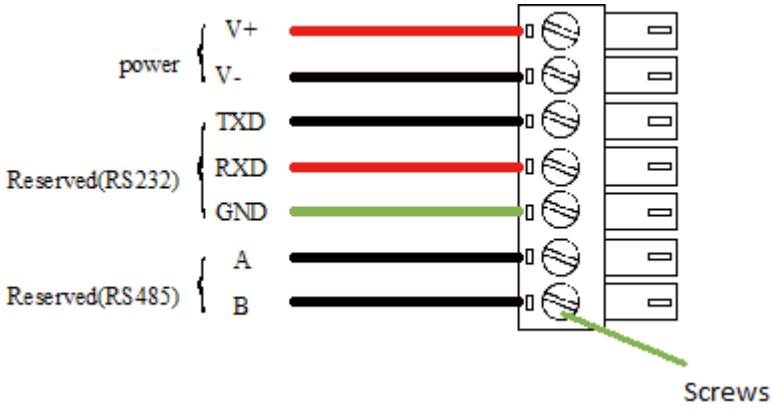
2.7 Anschließen des Netzwerkkabels

Schließen Sie den Router mit dem Ethernet-Kabel direkt an einen PC an.

2.8 Anschlussterminals

2.8.1 Stromversorgung / Serielle Terminals

Die Terminals bieten die Schnittstellenmodi RS232 und RS485. Schließen Sie die Kabel an die entsprechenden Terminals an, bevor Sie die Schnittstellen verwenden. Entfernen Sie bei der Installation die Terminals vom Gerät, lösen Sie die Sicherungsschrauben an den Terminals, schließen Sie die Kabel an die entsprechenden Terminals an und ziehen Sie die Schrauben wieder fest. Sortieren Sie die Kabel in der richtigen Reihenfolge.

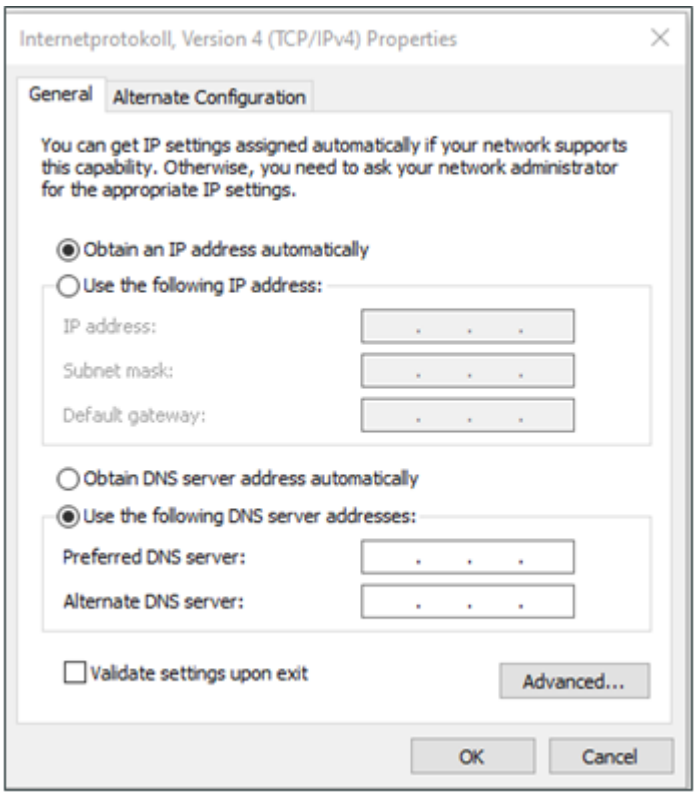


3 Netzwerkverbindung konfigurieren

3.1 Verbindung zum Router herstellen

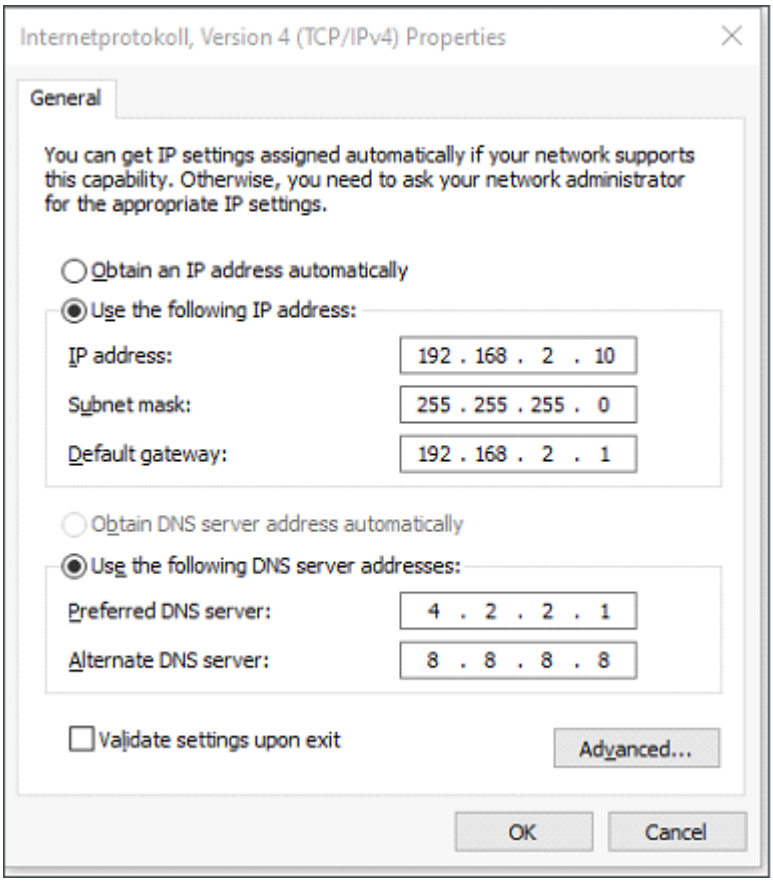
Schritt 1: Standardmäßig ist die IP-Adresse des TK600 für WAN/LAN 192.168.1.1; die IP-Adresse des TK600 für LAN ist 192.168.2.1. In diesem Dokument wird der LAN-Port für den Zugriff auf den TK600 als Beispiel verwendet. Stellen Sie die IP-Adresse des PCs so ein, dass sie sich im gleichen Subnetz wie das LAN befindet.

Methode 1: Automatisch eine IP-Adresse erhalten (empfohlen)



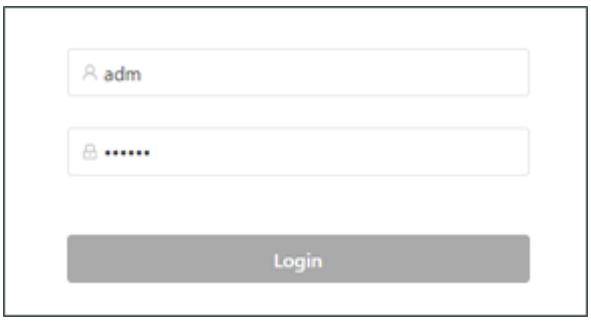
Methode 2: Festlegen einer festen IP-Adresse

Wählen Sie **Folgende IP-Adresse verwenden**, geben Sie eine IP-Adresse (standardmäßig eine beliebige von 192.168.2.2 bis 192.168.2.254), eine Subnetzmaske (standardmäßig 255.255.255.0), ein Standard-Gateway (standardmäßig 192.168.2.1) und eine DNS-Serveradresse ein und klicken Sie auf OK.



3.2 Einloggen beim Router

Schließen Sie den PC über das Netzwerkkabel direkt an den Router an, starten Sie den Webbrowser, geben Sie **https://192.168.2.1** in die Adressleiste ein, und drücken Sie **Enter**, um die Webanmeldeseite aufzurufen. Geben Sie den Benutzernamen (Standard: **adm**) und das Kennwort (Standard: **123456**) ein, und klicken Sie auf **OK** oder drücken Sie **Enter**, um die Webkonfigurationsseite aufzurufen.



3.3 Bedienung der Navigationsleiste

3.3.1 Zurück zur Homepage

Sie können auf das Welotec-Logo in der Ecke oben links auf jeder Webseite des TK600 klicken, um schnell zur **Übersicht** zurückzukehren.

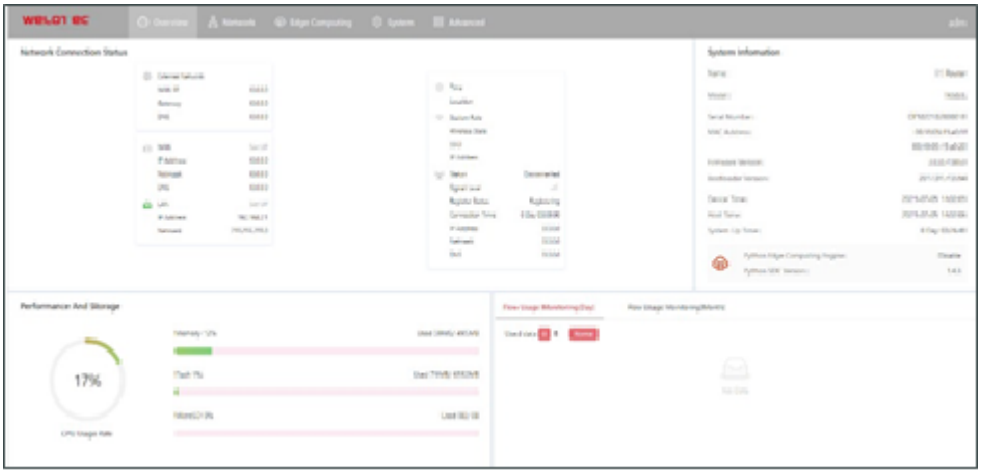
3.3.2 Ausloggen

Um sich von dem TK600 abzumelden, klicke auf den Benutzernamen in der Ecke oben rechts.

3.4 Übersicht (Overview)

Die Übersichtsseite zeigt Informationen über den TK600 an, z. B. den Status der Netzwerkverbindung, Systeminformationen und die Datennutzung. Auf dieser Seite können Sie schnell den Betriebsstatus des TK600 abrufen, nachdem Sie sich auf der TK600-Webseite angemeldet haben. Die Übersichtsseite wird standardmäßig angezeigt. Sie können auch auf Overview klicken, um diese Seite anzuzeigen. Auf dieser Seite werden die folgenden Informationen angezeigt:

Network Connection Status: Zeigt den Netzwerkverbindungsstatus und die Netzwerkkonfiguration des TK600 an.



3.5 Netzwerk (Network)

3.5.1 Netzwerkinterface (Network interface)

Cellular

Die Seite **Cellular** zeigt die Konfiguration und den Status des Dial-up Interface des TK600 an. Auf dieser Seite können Sie Parameter für die Einwahlschnittstelle einstellen, um den TK600 mit einem Mobilfunknetz zu verbinden, oder Details über die Einwahlschnittstelle anzeigen. Führen Sie die folgenden Schritte aus, um die Einwahlschnittstelle zu konfigurieren:

1. Wählen Sie **Network > Nework Interfaces > Cellular**, um die Seite **Cellular** anzuzeigen.
2. Wählen Sie **Enable Cellular**.

3. Stellen Sie die Parameter ein (Standardeinstellungen empfohlen).
4. Klicken Sie auf **Submit**, um die Konfiguration des Dial-up Interface abzuschließen. Die Parameter des Mobilfunknetzes werden im Folgenden beschrieben:

- Enable cellular: Aktiviert oder deaktiviert die Verbindung zum Mobilfunknetz.
- Profil
  - Network Type: gibt den Typ des Mobilfunknetzes an, mit dem der Router verbunden ist. Es kann sich um GSM oder CDMA handeln.
  - APN: gibt den Namen des Zugangspunkts („Access Point Name“, APN) an, der den Diensttyp eines WCDMA/LTE-Netzes kennzeichnet. Ein WCDMA/LTE-System bietet Dienste auf der Grundlage des APN des verbundenen WCDMA/LTE-Netzes an.
  - Access Number: gibt die vom Netzbetreiber bereitgestellte Wählzeichenfolge an. Erfragen Sie diese Zeichenfolge bei Ihrem Netzbetreiber.
    * Wenn Ihre 3G/LTE-Datenkarte WCDMA oder LTE unterstützt, lautet die Standard-Wählzeichenfolge *99***1#.
    * Wenn Ihre 3G-Datenkarte CDMA 2000 unterstützt, lautet die Standard-Wählzeichenfolge #777.
  - Auth Methode
    * Auto: Wählt automatisch eine Authentifizierungsmethode aus.
    * PAP: spezifiziert das Password Authentication Protocol, ein einfaches Klartext-Authentifizierungsverfahren, das durch Zwei-Wege-Handshakes implementiert wird.
    * CHAP: spezifiziert das Challenge Handshake Authentication Protocol, eine Sicherheitsauthentifizierungsmethode, die Nachrichten-Digests durch Drei-Wege-Handshakes verifiziert.
    * MS-CHAP: spezifiziert den von Microsoft definierten CHAP-Standard.
    * MS-CHAPv2: gibt die aktualisierte Version von MS-CHAP an, die eine zweiseitige Authentifizierung erfordert.
  - Username: gibt den Benutzernamen an, der für die Verbindung mit dem öffentlichen Datennetz („Public Data Network“, PDN) verwendet wird. Er wird von Ihrem Netzbetreiber bereitgestellt.
  - Password: gibt das Passwort des PDN-Benutzers an. Es wird von Ihrem Netzbetreiber bereitgestellt. Dual-SIM-Aktivierung: aktiviert oder deaktiviert den Dual-SIM-Kartenmodus.
  - Main SIM: gibt die verwendete Haupt-SIM-Karte an. Die Optionen sind SIM1, SIM2, Zufällig und Sequentiell.
  - Max Number Of Dial: gibt die maximale Anzahl von Einwahlversuchen auf SIM1 an. Wenn die Anzahl der Einwahlversuche diese Zahl erreicht, wechselt der Router zu SIM2.
  - Min Connected Time: gibt die minimale Dauer der Netzwerkverbindung an, nachdem der Router sich erfolgreich eingewählt hat. Innerhalb dieser Zeit wird die Anzahl der Einwahlversuche gezählt. Wenn die Verbindungsdauer den eingestellten Wert überschreitet, wird die Anzahl der Einwahlversuche zurückgesetzt. Wenn der Wert auf 0 gesetzt wird, ist diese Funktion deaktiviert.
  - Backup SIM Timeout: gibt die Zeitüberschreitung der aktuell verwendeten Backup-SIM-Karte an. Der Router schaltet auf die Haupt-SIM-Karte um, wenn die Timeout-Zeit der Backup-SIM-Karte erreicht ist.

Network Type: Gibt den Netzwerktyp für die SIM-Karte an. Die Optionen sind Auto, 3G, 4G und 2G. Sie können einen bestimmten Netzwerktyp auswählen, der für Ihren Router und Ihre SIM-Karte geeignet ist, oder den Automodus wählen, bei dem sich der Router automatisch bei einem geeigneten Netz anmeldet.

Profil: gibt den Index des Einwahlparametersatzes an.

Roaming: Aktiviert die Roaming-Funktion, um dem Router die Einwahl im Roaming-Zustand zu ermöglichen, oder deaktiviert die Roaming-Funktion, um zu verhindern, dass sich der Router im Roaming-Zustand einwählt. Wenn

eine lokale SIM-Karte verwendet wird, wird die Einwahlfunktion nicht beeinträchtigt, egal ob diese Option aktiviert oder deaktiviert ist.

PIN-Code: gibt die persönliche Identifikationsnummer der SIM-Karte an. Wenn Sie den PIN-Code aktivieren, aber keinen PIN-Code oder einen falschen PIN-Code einstellen, kann der Router keine Verbindung herstellen. Mit einem gültigen PIN-Code kann sich der Router in ein Netzwerk einwählen.

Static IP: aktiviert oder deaktiviert die Verwendung einer statischen IP-Adresse. Wenn Sie diese Option wählen, geben Sie eine IP-Adresse manuell an. Der Router bezieht dann bei jeder Einwahl in ein Netzwerk die angegebene statische IP-Adresse.

Connection Mode

- Always Online: gibt an, dass der Router bei ordnungsgemäßem Betrieb online bleibt und nur dann getrennt und neu angewählt wird, wenn über die Einwahlschnittstelle innerhalb von 30 Minuten kein Datenverkehr übertragen wird. Dies ist der Standardverbindungsmodus des Systems.
- On-demand Dial
  - Data Trigger: zeigt an, dass der Router standardmäßig offline ist und sich automatisch einwählt, wenn Daten an das Internet gesendet werden.
- Manual Dial: zeigt an, dass die Netzwerkverbindung durch Klicken auf **Connect** oder **Disconnect** im Bereich **Status** hergestellt oder beendet werden kann.

Redial Interval: gibt die Zeitspanne an, die der Router wartet, bevor er sich erneut einwählt.

ICMP Probes

- ICMP Detection Server: gibt die IP-Adresse oder den Domänennamen des entfernten ICMP-Servers an, der überprüft werden soll. (Wenn zwei ICMP-Server aktiviert sind, wird empfohlen, hier die IP-Adressen oder Domänennamen beider Server einzugeben). Der Router unterstützt zwei ICMP-Server: einen Primärserver und einen Backup-Server. Nachdem zwei Server konfiguriert wurden, prüft der Router zuerst den Primärserver. Er prüft den Sekundärserver erst dann, wenn die Anzahl der Prüfversuche auf dem Primärserver den Maximalwert erreicht hat. Wenn beide Server nicht erkannt werden, wählt sich der Router erneut ein und beginnt eine neue Runde von ICMP-Tests.
- ICMP Detection Interval: gibt das Intervall zwischen den vom Router gesendeten ICMP-Testpaketen an.
- ICMP Detection Timeout: gibt die Timeout-Periode einer ICMP-Testphase an. Wenn der Router innerhalb dieses Zeitraums kein ICMP-Antwortpaket empfängt, geht er davon aus, dass die ICMP-Testphase abgelaufen ist.
- ICMP Detection Max Retries: gibt die maximale Anzahl der Wiederholungsversuche nach einem fehlgeschlagenen ICMP-Test an. (Der Router wählt sich erneut ein, wenn die Anzahl der Wiederholungsversuche diesen Wert erreicht).
- ICMP Detection Strict: Aktiviert oder deaktiviert den strikten ICMP-Testmodus. In diesem Modus sendet der Router keine ICMP-Testpakete, wenn sein Dial-up Interface Datenverkehr überträgt. Er sendet ICMP-Testpakete nur, wenn das Dial-up Interface inaktiv ist.

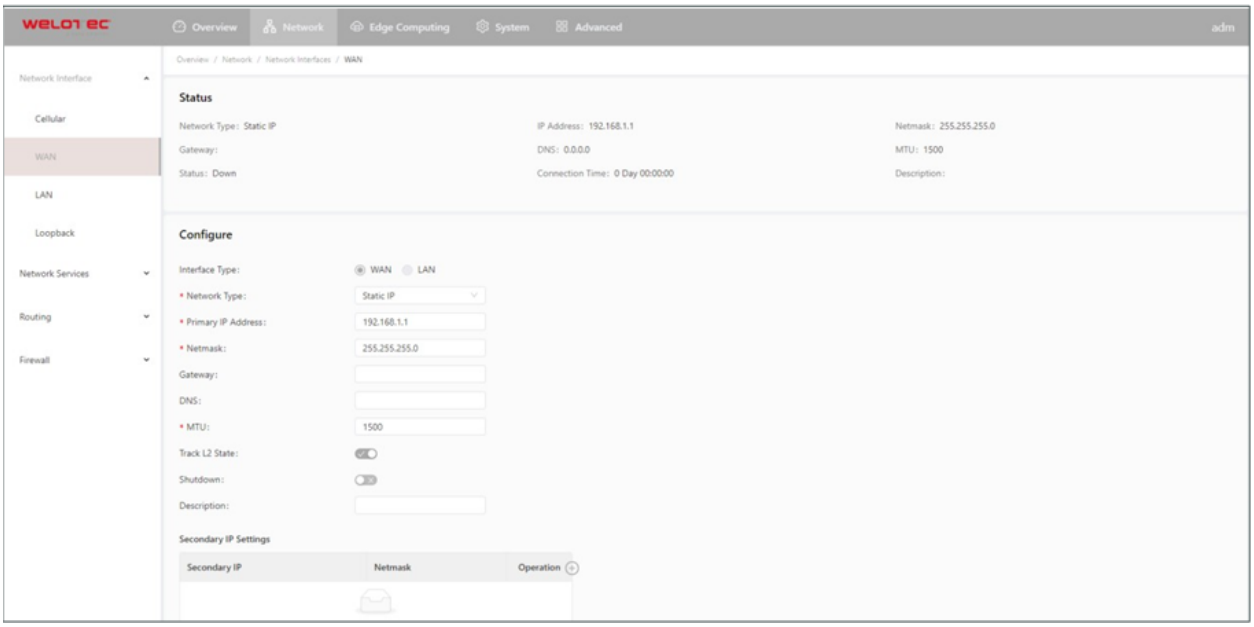
Advanced Settings

- Initial Commands: gibt einige AT-Befehle an, die zur Überprüfung des Modulstatus verwendet werden.
- RSSI Poll Interval: legt das Intervall fest, in dem der Router den Signalstatus nach erfolgreicher Einwahl überprüft. Das Intervall ist zum Beispiel auf 60s eingestellt. Wenn Sie die Antennen entfernen, nachdem sich der Router erfolgreich eingewählt hat, bleibt die Signalstärke in den ersten 60 Sekunden unverändert und nimmt dann in den folgenden 60 Sekunden ab. Wenn das Intervall auf 0 eingestellt ist, ist die RSSI-Abfrage deaktiviert.
- Dial Timeout: Gibt die Zeitüberschreitung für die Einwahl an. Wenn der Router innerhalb dieser Zeitspanne keine Verbindung zu einem Netzwerk herstellen kann, wird die Einwahl abgebrochen. In diesem Fall prüft der Router den Modulstatus und wählt sich erneut in das Netzwerk ein.
- MRU (Maximum Receive Unit): gibt die maximale Empfangseinheit an, die in Bytes ausgedrückt wird.

- MTU (Maximum Transmit Unit): gibt die maximale Übertragungseinheit an, die in Bytes ausgedrückt wird.
- Use Default Asyncmap: aktiviert oder deaktiviert die Standard-Asyncmap.
- Use Peer DNS: Aktiviert oder deaktiviert die Verwendung des im angeschlossenen Netzwerk zugewiesenen DNS-Servers.
- LCP Interval: gibt das Intervall an, in dem der Router überprüft, ob die Mobilfunkverbindung normal ist.
- LCP Max Retries: gibt die maximale Anzahl der Einwahlversuche nach einer Unterbrechung der Verbindung an.
- Infinitely Dial Retry: Ermöglicht es dem Router, bei einem Einwahlfehler eine unbegrenzte Anzahl von Wahlwiederholungen durchzuführen.
- Debug: ermöglicht die Anzeige detaillierterer Systemprotokolle.
- Expert Options: Hier können Sie Befehlsparameter einstellen.

WAN

Die folgende Abbildung zeigt die Konfiguration von **WAN/LAN**, wobei **Interface Type** auf **WAN** eingestellt ist.



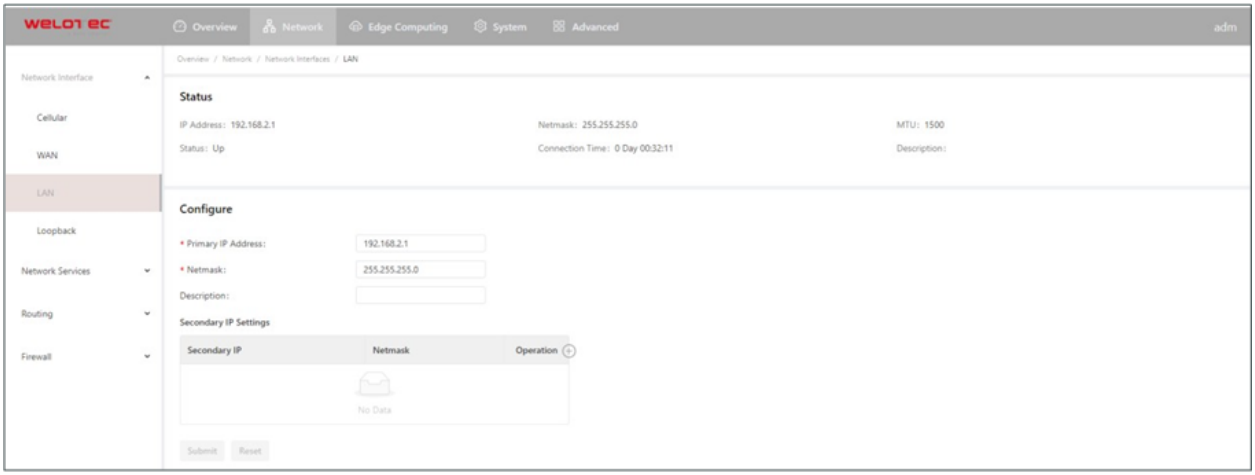
Die Ethernet-Parameter sind wie folgt beschrieben:

- Netzwerktyp (standardmäßig statische IP)
  - Static IP: verwendet eine manuell konfigurierte IP-Adresse, eine entsprechende Subnetzmaske und andere Informationen für die Ethernet-Schnittstelle.
  - Dynamische Adresse (DHCP): Konfiguriert die Schnittstelle als DHCP-Client, um eine IP-Adresse, die entsprechende Subnetzmaske und andere Informationen über DHCP zu beziehen.
- Statischer IP-Modus
  - Primary: gibt die IP-Adresse der Ethernet-Schnittstelle an. Standardmäßig lautet die IP-Adresse von WAN/LAN 192.168.1.1 und die IP-Adresse von LAN 192.168.2.1.
  - Netzmaske: gibt die Subnetzmaske der Ethernet-Schnittstelle an.
  - MTU: gibt die maximale Übertragungseinheit an, die in Bytes ausgedrückt wird. Der Standardwert ist 1500.
  - Geschwindigkeit/Duplex, einschließlich:
    * Auto-Verhandlung

  - 100M Vollduplex
  - 100M Halbduplex
  - 10M Vollduplex
  - 10M Halbduplex

- Track L2 State: Aktiviert oder deaktiviert die Verfolgung des L2-Schnittstellenstatus. Wenn diese Funktion aktiviert ist, ist die Schnittstelle **Down**, wenn sie nicht physisch verbunden ist, und **Up**, wenn sie physisch verbunden ist. Wenn diese Funktion deaktiviert ist, wird der Schnittstellenstatus als UP angezeigt, unabhängig davon, ob die Schnittstelle physikalisch verbunden ist.
- Shutdown: Deaktiviert die Schnittstelle.
- Description: gibt die beschreibenden Informationen an, die die Ethernet-Schnittstelle identifizieren.
- Secondary IP Settings: Sie können bis zu 10 sekundäre IP-Adressen zusätzlich zur primären IP-Adresse festlegen.

LAN



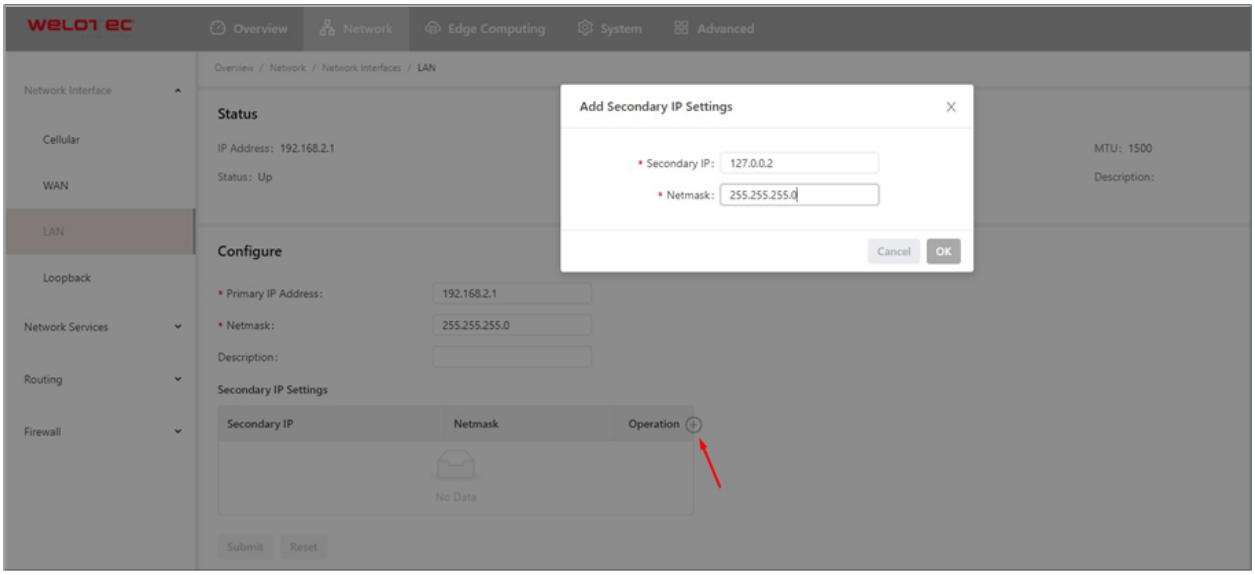
- Primary IP: gibt die primäre IP-Adresse der Schnittstelle an.
- Netmask: gibt die Subnetzmaske der Schnittstelle an.
- Secondary IP Settings: Sie können bis zu 10 sekundäre IP-Adressen zusätzlich zur primären IP-Adresse festlegen.

Loopback

Die Loopback-Schnittstelle ist eine logische, virtuelle Schnittstelle auf dem TK600. Nachdem Sie die Loopback-Schnittstelle erstellt und konfiguriert haben, können Sie ihre IP-Adresse anpingen oder eine Telnet-Verbindung zu ihr aufbauen, um die Netzwerkkonnektivität zu testen. Sie können die Parameter der Loopback-Schnittstelle auf der Seite **Loopback** einstellen oder ansehen. Gehen Sie folgendermaßen vor, um die Loopback-Schnittstelle zu konfigurieren:

1. Wählen Sie **Network > Network Interfaces > Loopback**, um die Seite **Loopback** anzuzeigen. Auf dieser Seite können Sie Parameter für die Loopback-Schnittstelle festlegen oder anzeigen.
2. Klicken Sie in der Tabelle unter **Secondary IP Settings** auf das Symbol Hinzufügen, um eine sekundäre IP-Adresse für die Loopback-Schnittstelle hinzuzufügen. (Die Standard-IP-Adresse lautet 127.0.0.1.)
3. Geben Sie die sekundäre IP-Adresse und die Subnetzmaske ein.
4. Klicken Sie auf **Submit**, um die Konfiguration der Loopback-Schnittstelle abzuschließen.

Wie in der folgenden Abbildung dargestellt, wird für die Loopback-Schnittstelle eine sekundäre IP-Adresse 127.0.0.2 festgelegt.

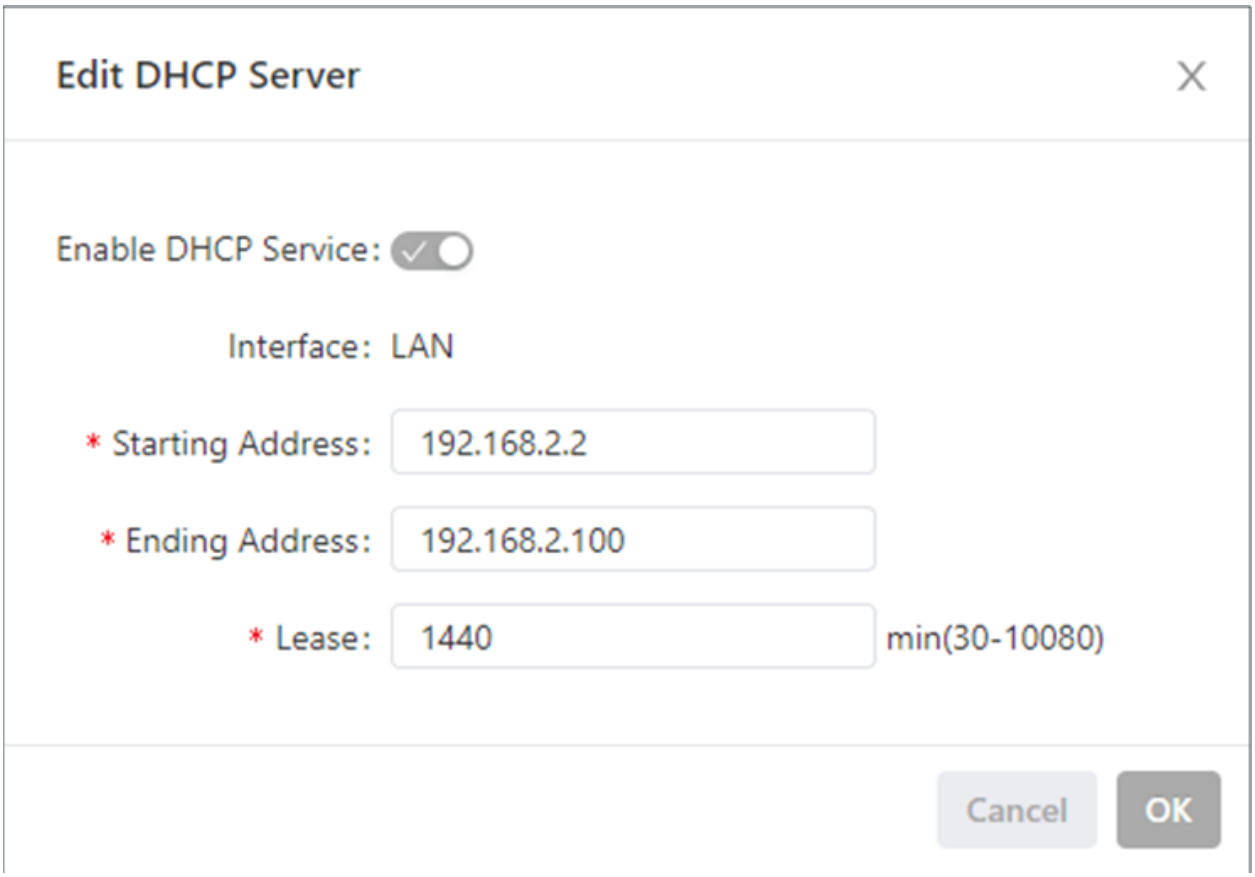


3.5.2 Network Services

DHCP

Das Dynamic Host Configuration Protocol (DHCP) verwendet das Client/Server-Kommunikationsmodell. Der Client sendet eine Konfigurationsanfrage an den Server, und der Server antwortet mit der dem Client zugewiesenen IP-Adresse und anderen Konfigurationsinformationen. Auf diese Weise werden die IP-Adresse des Clients und andere Konfigurationsinformationen dynamisch zugewiesen. Sie können einen DHCP-Server konfigurieren und seine Konfiguration auf der Seite **DHCP Server** anzeigen. Gehen Sie folgendermaßen vor, um einen DHCP-Server zu konfigurieren:

1. Wählen Sie **Network > Network Services > DHCP > DHCP Server**, um die Seite **DHCP Server** anzuzeigen.
2. Klicken Sie auf das Symbol **Add** oder **Edit**, um den DHCP-Server zu konfigurieren.
3. Stellen Sie die Parameter ein.
4. Klicken Sie auf **OK**, um die Konfiguration zu speichern, und dann auf **Submit**, um die Konfiguration anzuwenden. Die folgende Abbildung zeigt die Konfiguration des DHCP-Servers.



- Die Parameter des DHCP-Servers sind wie folgt beschrieben:
  - Enable DHCP Service: aktiviert oder deaktiviert den DHCP-Dienst.
  - Interface: LAN
  - Starting Address: gibt die Start-IP-Adresse des IP-Adresspools für die Adresszuweisung an DHCP-Clients an.
  - Ending Address: gibt die End-IP-Adresse des IP-Adresspools für die Adresszuweisung an DHCP-Clients an.
  - Lease: gibt die Gültigkeitsdauer der zugewiesenen IP-Adressen an. Der DHCP-Server fordert die abgelaufenen IP-Adressen für die Neuvergabe zurück. Dieses Feld kann nicht leer gelassen werden.
- Windows Name Server (WINS): gibt die IP-Adresse des WINS-Servers an.
- Static IP Setting: ermöglicht es Ihnen, eine feste IP-Adresse an eine MAC-Adresse zu binden, wie in der folgenden Abbildung dargestellt.

DNS

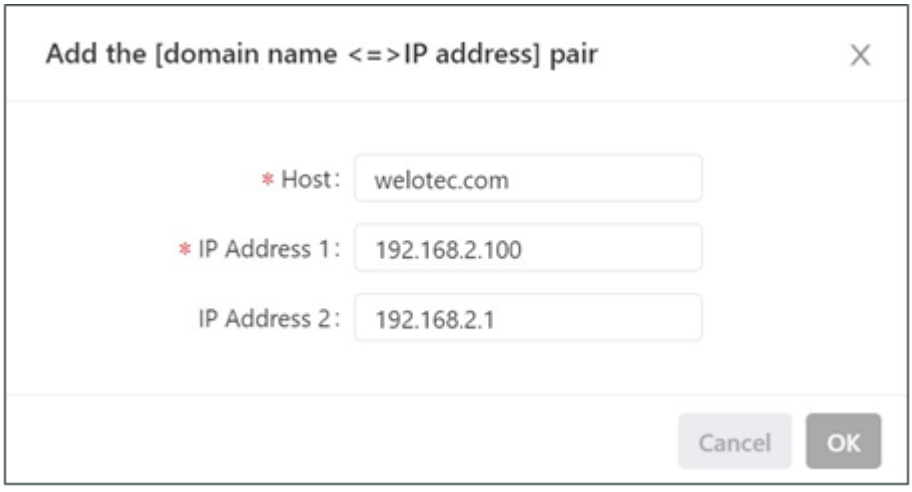
Ein Domänennamensystem (DNS) ist eine verteilte Datenbank, die für TCP/IP-Anwendungen verwendet wird und die Übersetzung zwischen Domänennamen und IP-Adressen ermöglicht. DNS ermöglicht Benutzern den Zugriff auf einige Anwendungen, indem sie leicht zu merkende, aussagekräftige Domänennamen verwenden, die dann von einem DNS-Server im Netzwerk in die richtigen IP-Adressen übersetzt werden. Sie können einen DNS-Server und den DNS-Relay-Dienst konfigurieren und die Konfiguration auf

die **DNS** Seite.

- So konfigurieren Sie einen DNS-Server:
  1. Wählen Sie **Network > Network Services > DNS**, um die Seite **DNS** anzuzeigen.
  2. Geben Sie die IP-Adresse des DNS-Servers ein.
  3. Klicken Sie auf **Submit**, um die Konfiguration zu übernehmen. Die folgende Abbildung zeigt die Konfiguration des DNS-Servers.

So konfigurieren Sie den DNS-Relay-Dienst:

1. Wählen Sie **Network > Network Services > DNS**, um die Seite **DNS** anzuzeigen.
2. Aktivieren Sie den DNS-Relay-Dienst. Der DNS-Relay-Dienst kann nicht deaktiviert werden, wenn die DHCP-Server-Funktion aktiviert ist.
3. Klicken Sie auf das Symbol Hinzufügen, um ein **[Domänenname <=> IP-Adresse] Paar** hinzuzufügen.
4. Geben Sie den Domänennamen oder die IP-Adresse eines Hosts ein und geben Sie die passende IP-Adresse an.
5. Klicken Sie auf **OK**, um die Konfiguration zu speichern, und dann auf **Submit**, um die Konfiguration anzuwenden. Die folgende Abbildung zeigt die Konfiguration des DNS-Relay-Dienstes.



Host List

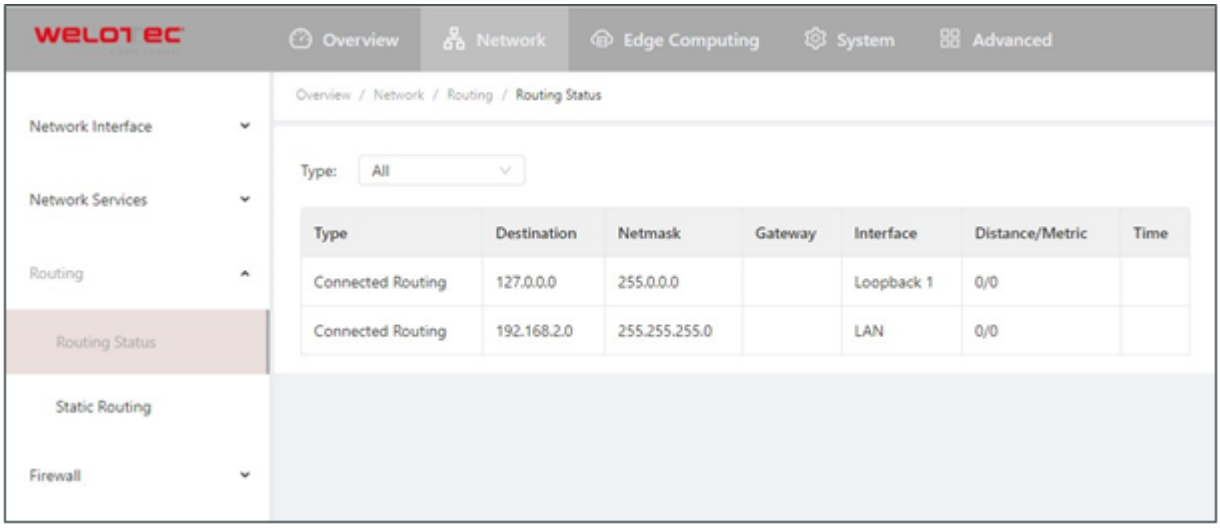
Sie können Informationen über Hosts, die mit dem TK600 verbunden sind, auf der Seite **Hostliste** anzeigen. Wählen Sie **Netzwerk > Netzwerkdienste > Host List**, um die Seite **Host List** anzuzeigen, wie in der folgenden Abbildung dargestellt.

Interface	MAC Address	IP Address	Host	Lease
LAN	d8:c4:97:c8:ed:26	192.168.2.76	DESKTOP-KRF8BHD	0 Day 23:02:00

3.5.3 Routing

Routingstatus

Wählen Sie **Network > Routing > Routing Status**, um die Seite **Routing Status** anzuzeigen. Auf dieser Seite werden Informationen über die auf dem TK600 konfigurierten statischen Routen angezeigt, wie in der folgenden Abbildung dargestellt.

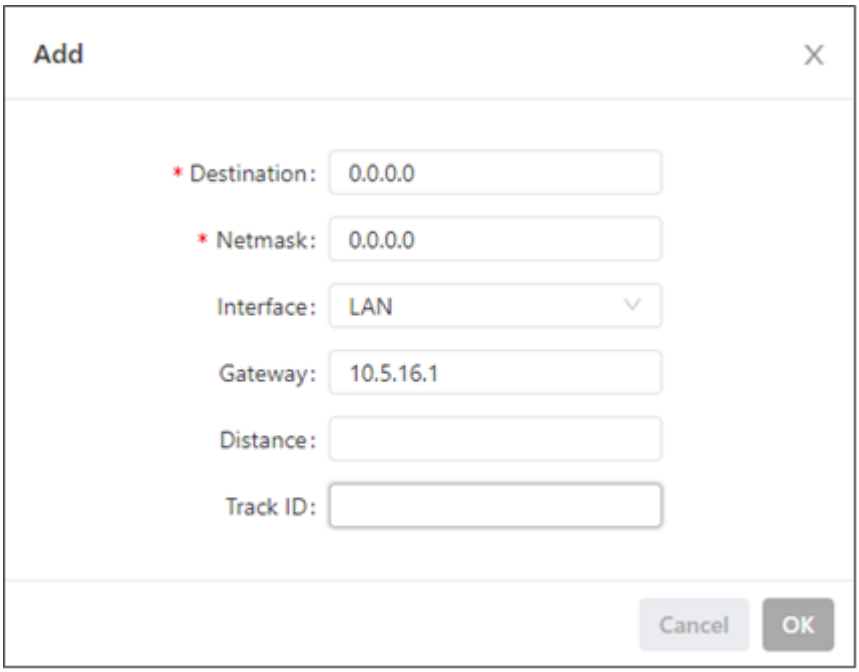


Static Routing

Sie können statische Routen auf der Seite **Static Routing** konfigurieren. Dann werden Pakete, die an ein bestimmtes Ziel gesendet werden, über die angegebene Route weitergeleitet. (In der Regel müssen Sie keine statischen Routen konfigurieren.) Gehen Sie wie folgt vor, um eine statische Route zu konfigurieren:

1. Wählen Sie **Network > Routing > Static Routing**, um die Seite **Static Routing** anzuzeigen.
2. Klicken Sie auf das Symbol **Add**, um eine statische Route hinzuzufügen.
3. Stellen Sie die Parameter ein.
4. Klicken Sie auf **OK**, um die Konfiguration zu speichern, und dann auf **Submit**, um die Konfiguration zu übernehmen.

Die folgende Abbildung zeigt die Konfiguration einer statischen Route.



Im Folgenden werden die Parameter einer statischen Route beschrieben:

- Destination: gibt die Ziel-IP-Adresse an, an die die Pakete gesendet werden.
- Netmask: gibt die Subnetzmaske der Ziel-IP-Adresse an.
- Interface: gibt die Schnittstelle an, über die die Datenpakete an das Zielnetz weitergeleitet werden.
- Gateway: gibt die IP-Adresse des nächsten Routers an, den die Datenpakete durchlaufen, bevor sie die Ziel-IP-Adresse erreichen.
- Distance: gibt die Priorität der Route an. Ein kleinerer Wert bedeutet eine höhere Priorität.
- Track ID: gibt den Track-Index oder die ID an.

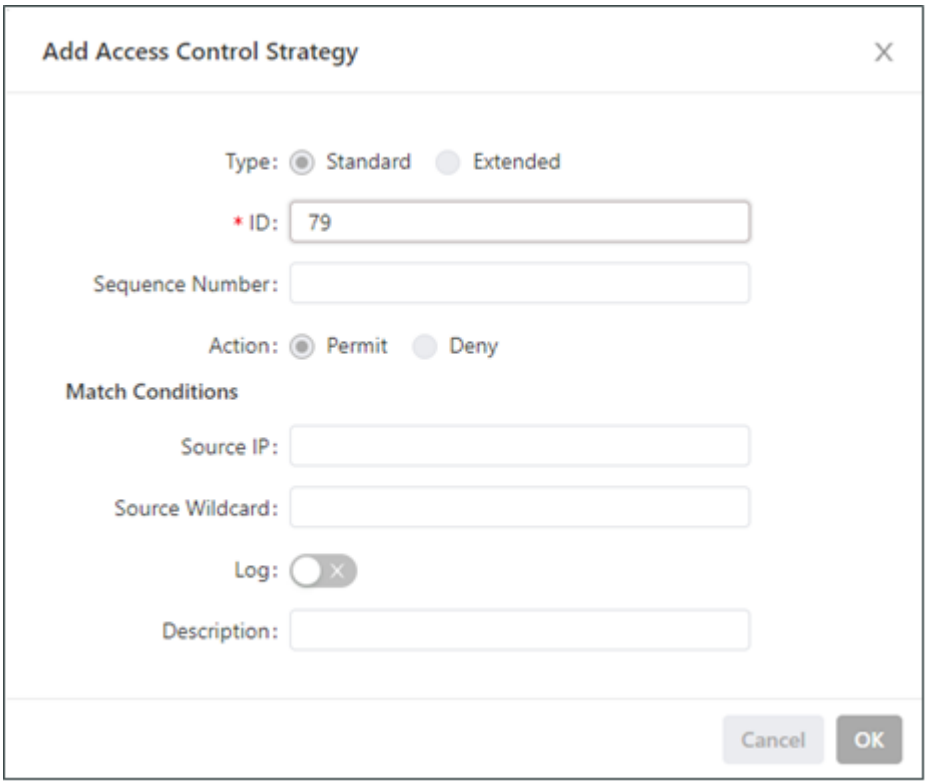
3.5.4 Firewall

ACL

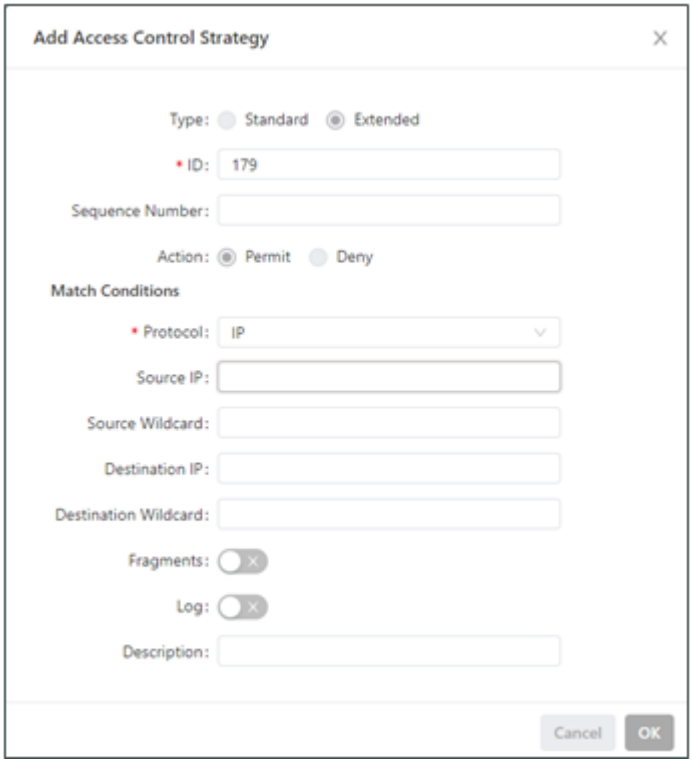
Eine Zugriffskontrollliste („Access Control List“, ACL) erlaubt oder verweigert bestimmte Datenflüsse (z. B. den Datenfluss von einer bestimmten Quell-IP-Adresse oder einem bestimmten Konto) auf der Grundlage einer Reihe von übereinstimmenden Regeln, um die Daten zu filtern, die eine Netzwerkschnittstelle erreichen. Sie können eine Datenfilterungsrichtlinie für eine Netzwerkschnittstelle auf der Seite **ACL** konfigurieren. Das Konfigurationsverfahren ist wie folgt:

1. Wählen Sie **Network > Firewall > ACL**, um die Seite **ACL** anzuzeigen.
2. Klicken Sie unter **Access Control Policy** auf das Add Symbol, um eine Zugangskontrollrichtlinie hinzuzufügen.
3. Stellen Sie die Parameter ein.
4. Klicken Sie auf das Symbol Hinzufügen oder Bearbeiten unter **ACL**, um eine Zugriffskontrollliste für eine bestimmte Schnittstelle hinzuzufügen.
5. Stellen Sie die Parameter ein.
6. Klicken Sie auf **OK**, um die Konfiguration zu speichern, und dann auf **Submit**, um die Konfiguration anzuwenden.

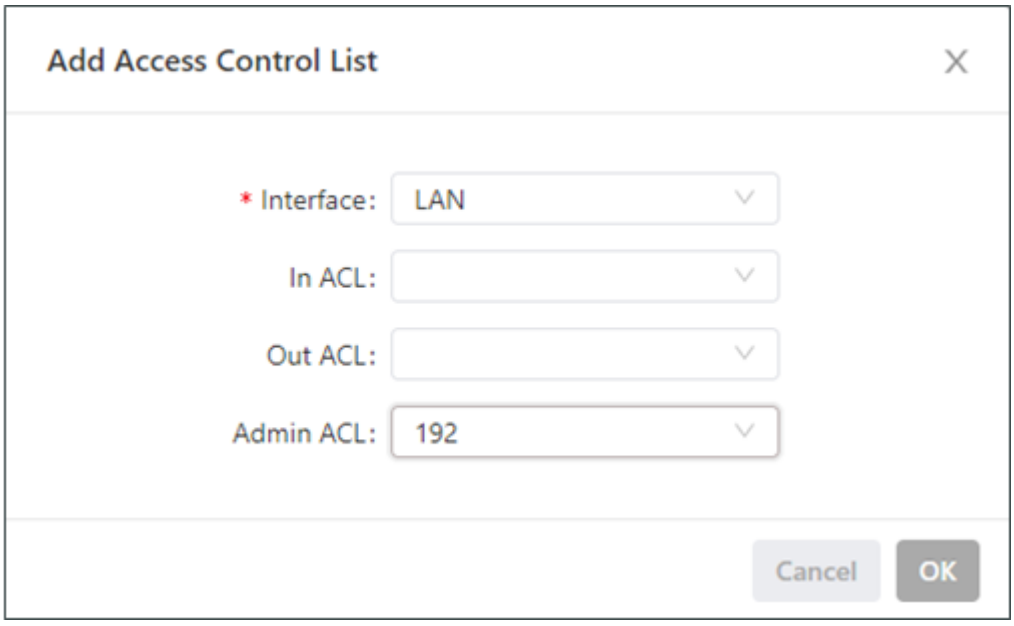
Die folgende Abbildung zeigt die Konfiguration einer Standard-Zugriffskontrollrichtlinie.



Die folgende Abbildung zeigt die Konfiguration einer erweiterten Zugriffskontrollrichtlinie.



Die folgende Abbildung zeigt die Konfiguration einer Zugriffskontrollliste.



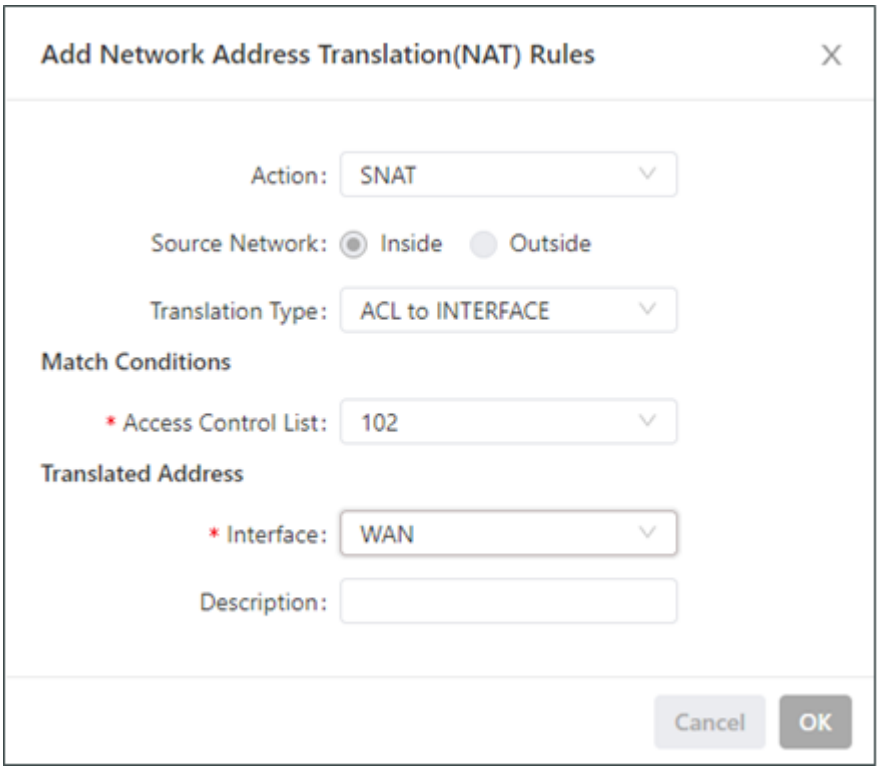
- Im Folgenden werden die Parameter einer Standard-Zugangskontrollpolitik beschrieben:
  - ID: gibt die ID einer ACL-Regel an, im Bereich von 1-99. Ein kleinerer Wert bedeutet eine höhere Priorität der Regel.
  - Sequence Number: gibt die Sequenznummer der ACL-Regel an. Ein kleinerer Wert bedeutet eine höhere Priorität der Regel.
  - Action: erlaubt oder verweigert die Weiterleitung passender Pakete.
  - Source IP: gibt die Source-IP-Adresse der Pakete in der ACL-Regel an. Wenn dieses Feld leer bleibt, passt die Regel auf Pakete aus allen Netzwerken.
  - Source Wildcard: gibt die Wildcard-Maske der Source-IP-Adresse in der ACL-Regel an.
  - Log: Aktiviert oder deaktiviert die Aufzeichnung von Zugangskontrollprotokollen.
  - Description: Zeichnet die Bedeutung der Zugangskontrollparameter auf.
- Die Parameter einer erweiterten Zugriffskontrollregelung werden wie folgt beschrieben:
  - ID: gibt die ID einer ACL-Regel an, im Bereich von 100-199. Ein kleinerer Wert bedeutet eine höhere Priorität der Regel.
  - Sequence Number: gibt die Sequenznummer der ACL-Regel an. Ein kleinerer Wert bedeutet eine höhere Priorität der Regel.
  - Action: permits or denies forwarding of matching packets.
  - Protokoll: gibt das Protokoll der Zugriffskontrolle an.
  - Source IP: gibt die Source-IP-Adresse der Pakete in der ACL-Regel an. Wenn dieses Feld leer bleibt, passt die Regel auf Pakete aus allen Netzwerken.
  - Source Wildcard: gibt die Wildcard-Maske der Source-IP-Adresse in der ACL-Regel an.
  - Source Port: gibt die Nummer des Source Ports der Pakete an. Der Wert **any** bedeutet, dass TCP/UDP-Pakete mit beliebigen Source Ports der Regel entsprechen. Dieser Parameter ist nur verfügbar, wenn das TCP- oder UDP-Protokoll ausgewählt ist.
  - Destination IP: gibt die Ziel-IP-Adresse der Pakete in der ACL-Regel an. Wenn dieses Feld leer bleibt, passt die Regel auf Pakete, die für alle Netzwerke bestimmt sind.
  - Destination Wildcard: gibt die Wildcard-Maske der Ziel-IP-Adresse in der ACL-Regel an.

  - Destination Port: gibt die Nummer des Zielports der Pakete an. Der Wert **any** bedeutet, dass TCP/UDP-Pakete mit beliebigen Zielports der Regel entsprechen. Dieser Parameter ist nur verfügbar, wenn das TCP- oder UDP-Protokoll ausgewählt ist.
  - Established Connection: gibt den Bereich der kontrollierten TCP-Pakete an. Wenn diese Option aktiviert ist, kontrolliert das System TCP-Pakete bei aufgebauten Verbindungen und nicht die bei nicht aufgebauten Verbindungen. Wenn diese Option deaktiviert ist, kontrolliert das System TCP-Pakete sowohl bei bestehenden als auch bei nicht bestehenden Verbindungen. Dieser Parameter ist nur verfügbar, wenn das TCP-Protokoll ausgewählt ist.
  - Fragments: aktiviert oder deaktiviert die Kontrolle über fragmentierte Datenpakete, die von der Schnittstelle gesendet werden.
  - Log: Aktiviert oder deaktiviert die Aufzeichnung von Zugangskontrollprotokollen.
  - Description: Zeichnet die Bedeutung der Zugangskontrollparameter auf.
- Im Folgenden werden die Parameter einer Zugriffskontrollliste beschrieben:
  - Interface: gibt den Namen der Schnittstelle an, für die die Zugriffskontrollrichtlinie konfiguriert ist.
  - Rule: gibt die eingehenden, ausgehenden und administrativen Regeln an.

NAT

Die Netzwerkadressübersetzung („Network Address Translation“, NAT) ermöglicht es mehreren Hosts in einem LAN, sich mit dem Internet zu verbinden, indem sie eine oder mehrere öffentliche IP-Adressen verwenden. Diese Funktion ordnet einige öffentliche IP-Adressen vielen privaten IP-Adressen zu, um öffentliche IP-Adressen zu sparen. Sie können NAT-Regeln auf der Seite **NAT** anzeigen und konfigurieren. Das Konfigurationsverfahren ist wie folgt:

1. Wählen Sie **Network > Firewall > NAT**, um die Seite **NAT** anzuzeigen.
2. Wählen Sie eine Schnittstelle aus der Dropdown-Liste **Interface**.
3. Klicken Sie auf das Symbol Hinzufügen unter **Network Address Translation (NAT) Rules**, um eine NAT-Regel hinzuzufügen und Parameter für die Regel festzulegen.
4. Klicken Sie auf **OK**, um die Konfiguration zu speichern, und dann auf **Submit**, um die Konfiguration anzuwenden.
5. Wie in der folgenden Abbildung dargestellt, erlaubt die NAT-Regel den an den TK600 angeschlossenen Hosts, sich über die IP-Adresse der Schnittstelle WAN mit dem Internet zu verbinden.



Die Parameter der NAT-Regel werden wie folgt beschrieben:

- Action
  - SNAT: verwendet die Funktion zur Übersetzung von Quell-Netzwerk-Adressen, die die Quell-IP-Adressen von Datenpaketen in eine andere IP-Adresse übersetzt. Im Allgemeinen wird diese Funktion für Datenpakete verwendet, die über den Router ins Internet gesendet werden.
  - DNAT: Verwendet die Funktion „Destination Network Address Translation“, die die Ziel-IP-Adressen von Datenpaketen in eine andere IP-Adresse übersetzt. Im Allgemeinen wird diese Funktion für Datenpakete verwendet, die über den Router an das private Netz gesendet werden.
  - 1:1NAT: verwendet eine Eins-zu-Eins-IP-Adressübersetzung.
- Source Network (verfügbar, wenn die Aktion auf SNAT oder DNAT eingestellt ist):
  - Inside: übersetzt private IP-Adressen.
  - Outside: übersetzt die öffentlichen IP-Adressen.
- Übersetzungstyp (Translation Type), der sein kann:
  - IP zu IP
  - IP zu INTERFACE
  - IP PORT zu IP PORT
  - ACL zu INTERFACE
  - ACL zu IP
- Zugriffskontrollliste (nicht verfügbar für 1:1 NAT): gibt die ACL-Regel an, die verwendet wird, um die Pakete abzugleichen, deren IP-Adressen übersetzt werden.
- Übersetzte Adresse (nicht verfügbar für 1:1 NAT): gibt die IP-Adresse oder Schnittstelle an, die von der Source-Adresse übersetzt wird.
- Beschreibung: gibt die Beschreibung der NAT-Regel an.

3.6 Edge Computing

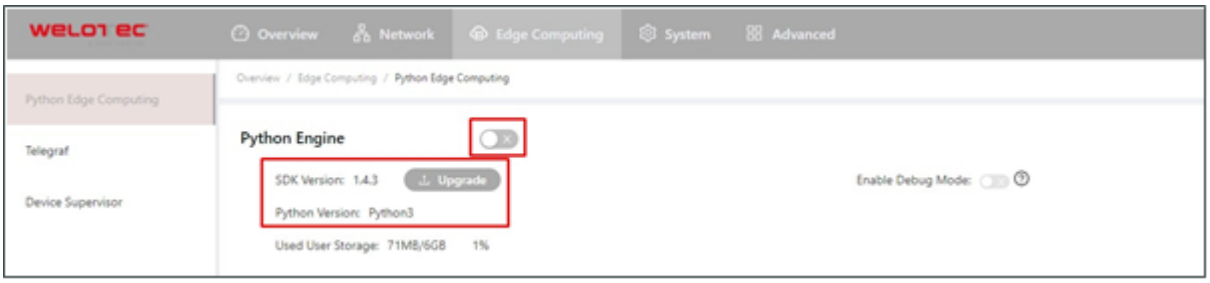
3.6.1 Python Edge Computing

Python-App installieren und ausführen

Um die Python App auf dem TK600 zu installieren und auszuführen, gehen Sie bitte wie folgt vor, wobei dieses Dokument den Device Supervisor als Beispiel nimmt (wenn Sie eine eigene Funktionalität wünschen, wenden Sie sich bitte an Ihren Welotec Vertrieb):

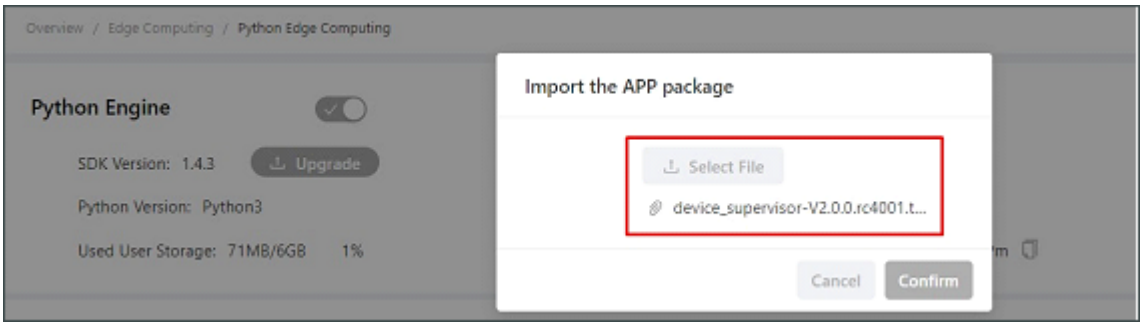
- **Schritt 1:** Installieren Sie die App

Vor der Installation der App müssen Sie sicherstellen, dass die Python Edge Computing Engine aktiviert und das Python SDK installiert ist, wie in der folgenden Abbildung dargestellt:

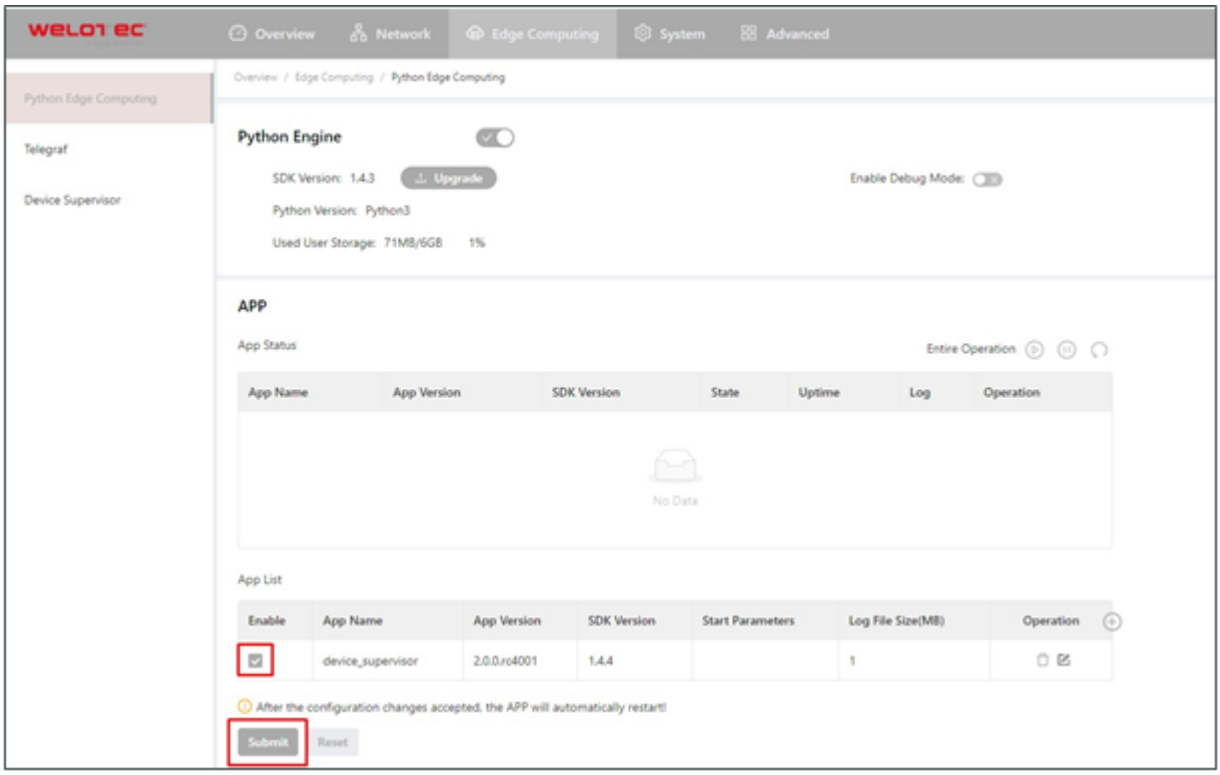


Wählen Sie **Edge Computing** > **Python Edge Computing**. Klicken Sie auf die Schaltfläche Hinzufügen und wählen Sie die zu installierende App-Paketdatei aus, dann klicken Sie auf Submit

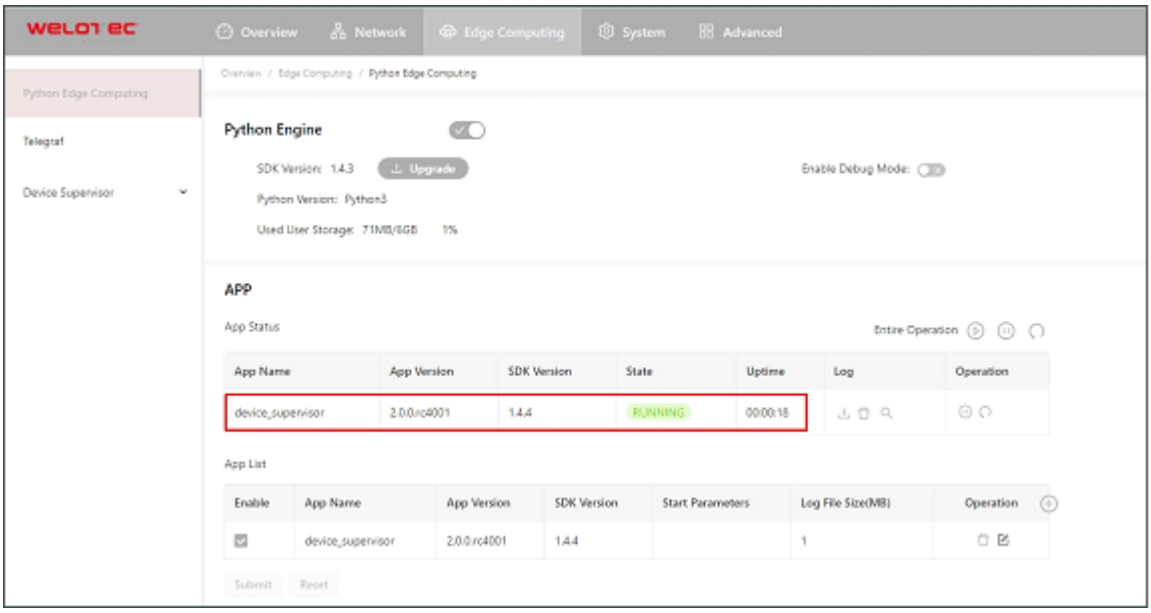
Nach dem Import können Sie die importierten Apps anzeigen, wie in der folgenden Abbildung dargestellt:



- **Schritt 2:** Führen Sie die App aus Wählen Sie „App aktivieren“ und klicken Sie auf „Senden“.

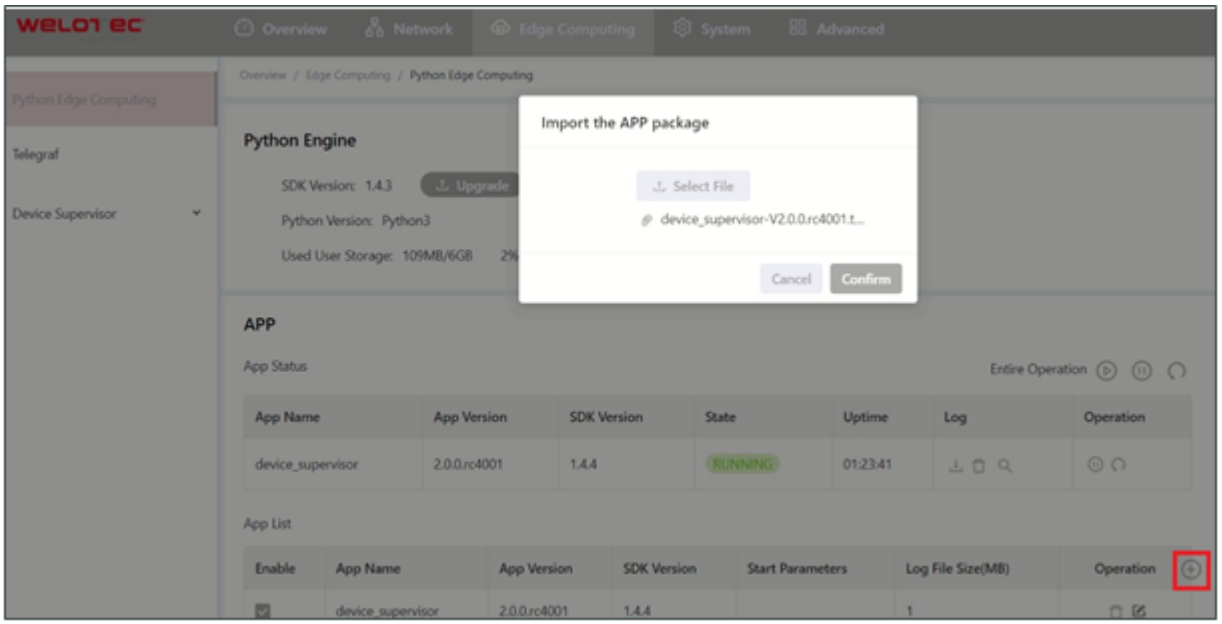


Nach der Aktivierung wird die App automatisch gestartet und läuft jedes Mal, wenn der TK600 gestartet wird.

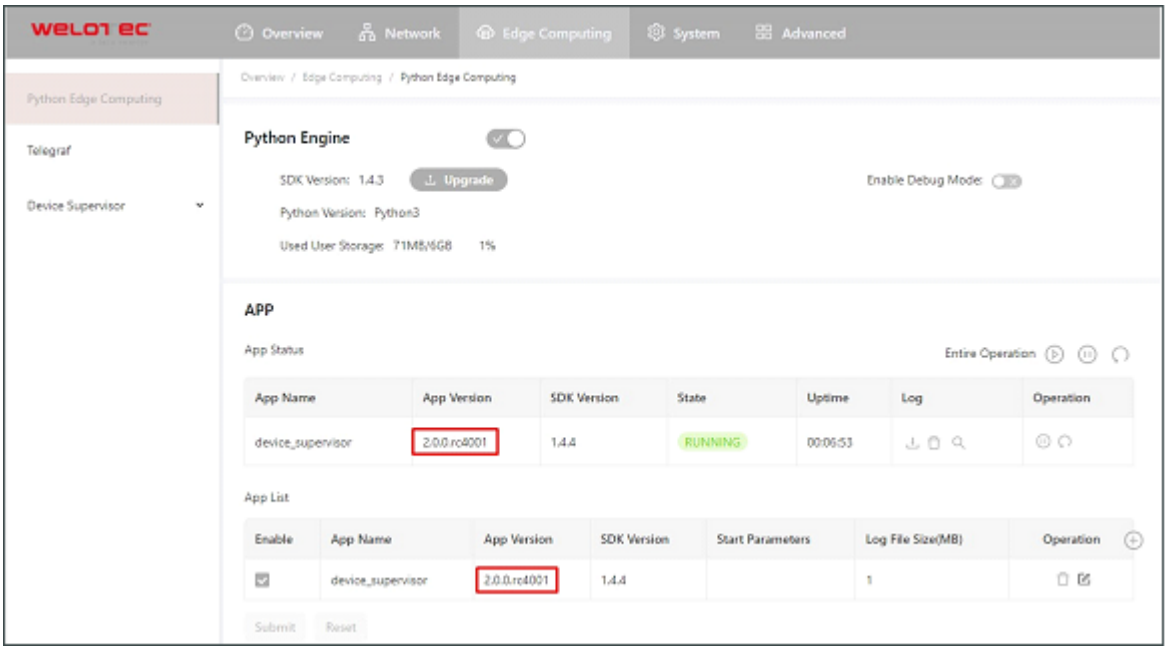


Python-App-Version aktualisieren

Wenn Sie die Version der Python-App aktualisieren müssen, brauchen Sie im Allgemeinen nur die neue Version der App auf der Seite **Edge Computing** > **Python Edge Computing** zu importieren.

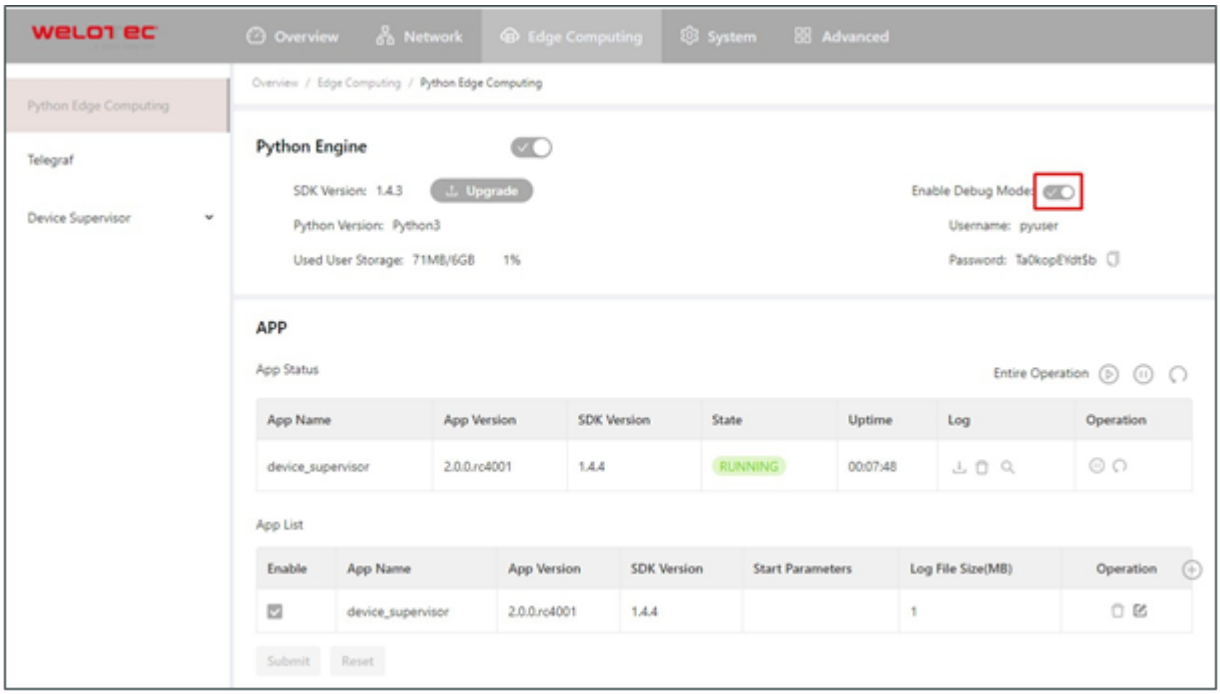


Nachdem die Aktualisierung abgeschlossen ist, wie unten abgebildet



Debug-Modus aktivieren

Um Python-Code auf dem TK600 auszuführen und zu debuggen, müssen Sie den Debug-Modus vom TK600 aktivieren. Wählen Sie **Edge Computing** > **Python Edge Computing** und wählen Sie **Enable Debug Mode**.



Nachdem der Debugging-Modus aktiviert ist, startet der TK600 einen SSH-Server, der den Port 222 des LAN abhört (Standard-IP-Adresse 192.168.2.1). Der Benutzername und das Passwort des SSH-Servers werden auf der vorherigen Webseite angezeigt. Ein zufälliges Passwort wird jedes Mal generiert, wenn der Debugging-Modus aktiviert oder der TK600 neu gestartet wird, um die Sicherheit zu gewährleisten.

3.7 System

3.7.1 Systemzeit

Damit der TK600 ordnungsgemäß mit anderen Geräten zusammenarbeiten kann, müssen Sie eventuell eine genaue Systemzeit für ihn einstellen. Stellen Sie zu diesem Zweck die Systemzeit auf der Seite **Systemzeit** ein und aktivieren Sie das NTP-Protokoll, um die Uhrensynchronisation zwischen allen Geräten im Netzwerk zu implementieren, die diese Funktion unterstützen. Auf diese Weise behalten alle Geräte die gleiche Uhr bei, um Anwendungen auf der Grundlage einer einheitlichen Zeit bereitzustellen. Gehen Sie folgendermaßen vor, um die Systemzeit einzustellen:

Methode 1: Wählen Sie eine Zeitzone aus.

1. Wählen Sie **System > System Time**, um die Seite **System Time** anzuzeigen.
2. Wählen Sie die Zeitzone, in der sich der TK600 befindet, aus der Dropdown-Liste **Time Zone** aus.
3. Klicken Sie auf **Apply**

Methode 2: Stellen Sie die Systemzeit manuell ein.

1. Wählen Sie **System > System Time**, um die Seite **System Time** anzuzeigen.
2. Stellen Sie im Feld Zeit einstellen eine bestimmte Uhrzeit ein.
3. Klicken Sie auf **Apply**

Methode 3: Verwenden Sie die lokale Uhrzeit des PCs.

1. Wählen Sie **System > System Time**, um die Seite **System Time** anzuzeigen.
2. Der TK600 kann die Uhrzeit des PCs als Ortszeit beziehen.
3. Klicken Sie neben dem Feld Gerätezeit auf Sync.

Methode 4: Aktivieren Sie SNTP-Clients.

1. Wählen Sie **System > System Time**, um die Seite **System Time** anzuzeigen.
2. Wählen Sie **Enable SNTP Clients**.
3. Stellen Sie die Parameter ein.
4. Klicken Sie auf **Submit**, um die Konfiguration zu übernehmen.

3.7.2 System Logs

Wählen Sie **System > Log**, um die Seite **Log** anzuzeigen. Diese Seite zeigt eine große Anzahl von Informationen über das Netzwerk und den TK600 an, wie z.B. den Betriebsstatus und Konfigurationsänderungen. Auf der Seite **Configure** können Sie einen Remote Log Server einstellen. Dann synchronisiert der TK600 alle Systemprotokolle mit dem entfernten Protokollserver. Der als Remote-Log-Server verwendete Host muss ein Remote-Log-Programm ausführen.

3.7.3 Konfigurationsverwaltung

Wählen Sie **System > Configuration Management**, um die Seite **Configuration Management** anzuzeigen. Auf dieser Seite können Sie die Konfigurationsparameter sichern, Parametereinstellungen importieren und die Werkseinstellungen des TK600 wiederherstellen. Diese Funktionen werden im Folgenden beschrieben:

- Configuration Management
  - Auto Save: aktiviert oder deaktiviert das automatische Speichern der geänderten Konfiguration in der Startkonfigurationsdatei.
  - Encrypted: aktiviert oder deaktiviert die Passwortverschlüsselung. Wenn diese Option ausgewählt ist, werden alle auf dem TK600 Web-System konfigurierten Passwörter in verschlüsseltem Text angezeigt. Diese Funktion verbessert die Sicherheit der Passwörter.
- Configuration Files Operations
  - Import Startup Config: ermöglicht den Import einer Konfigurationsdatei als Startup-Konfiguration des TK600. Der TK600 wird die importierte Konfigurationsdatei bei einem Neustart laden. Achte auf die Gültigkeit und die richtige Reihenfolge der Befehle in der importierten Konfigurationsdatei. Der TK600 filtert ungültige Befehle in der importierten Konfigurationsdatei heraus und speichert dann die gültigen Befehle als Startup-Konfiguration. Das System führt diese Befehle nach einem Neustart sequentiell aus. Wenn die Befehle in der importierten Konfigurationsdatei nicht in einer gültigen Reihenfolge aufgeführt sind, kann das System nach einem Neustart nicht in den erwarteten Zustand übergehen.
  - Export Startup Config: Ermöglicht das Sichern der Startup-Konfiguration auf einem Host. Die Startup-Konfiguration ist die Konfiguration, die der TK600 nach dem Start lädt.
  - Export Running Config: ermöglicht das Sichern der laufenden Konfiguration auf einem Host. Die laufende Konfiguration ist die Konfiguration, die auf dem TK600 läuft.
  - Restore Factory Configuration: ermöglicht die Wiederherstellung der Werkseinstellungen des TK600. Dieser Vorgang setzt alle Parameter des TK600 auf die Standardeinstellungen zurück. Die Werkseinstellungen werden nach einem Neustart des TK600 wiederhergestellt.

3.7.4 Firmware Upgrade

Folgen Sie diesen Schritten, um die Firmware-Version zu aktualisieren:

1. Wählen Sie **System > Firmware Upgrade**, um die Seite **Firmware Upgrade** anzuzeigen.
2. Klicken Sie auf **Select File**, um eine Firmware-Datei für den TK600 auszuwählen.
3. Klicken Sie auf **Starting Upgrade** und **OK**, um das Firmware-Upgrade zu starten.
4. Warten Sie, bis das Upgrade erfolgreich durchgeführt wurde, und klicken Sie dann auf **Reboot**, um den TK600 neu zu starten.

3.7.5 Zugriffswerkzeuge

Um die Verwaltung und Konfiguration des TK600 zu erleichtern, können Sie die Verwaltungs- und Zugriffsmethoden des TK600 auf der Seite **Access Tools** konfigurieren. Folgen Sie diesen Schritten, um die Konfiguration abzuschließen:

- HTTPS konfigurieren

1. Wählen Sie **System > Access Tools**, um die Seite **Access Tools** anzuzeigen.
2. Wählen Sie **Enable HTTPS** und legen Sie die Parameter fest.
3. Klicken Sie auf **Submit**, um die Konfiguration zu übernehmen.

- Telnet konfigurieren

1. Wählen Sie **System > Access Tools**, um die Seite **Access Toos** anzuzeigen.
2. Wählen Sie **Enable TELNET** und stellen Sie die Parameter ein.
3. Klicken Sie auf **Submit**, um die Konfiguration zu übernehmen.

- SSH konfigurieren

1. Wählen Sie **System > Access Tools**, um die Seite **Access Tools** anzuzeigen.
2. Wählen Sie **Enable SSH** und legen Sie die Parameter fest.
3. Klicken Sie auf **Submit**, um die Konfiguration zu übernehmen.

Die folgende Abbildung zeigt die Konfiguration der HTTPS-basierten Verwaltung.

Die HTTPS-Parameter werden im Folgenden beschrieben:

1. Listen IP Address: gibt die zu überwachende IP-Adresse an. Zu den Optionen gehören Any, 127.0.0.1 und andere IP-Adressen.

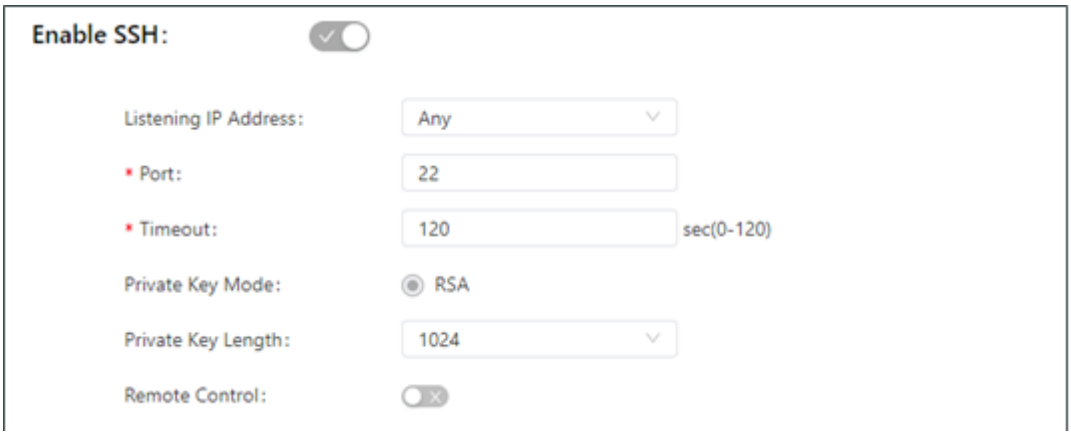
2. Port: gibt die Nummer des HTTPS-Ports an.
3. Web Login Timeout: gibt die Zeitüberschreitung für die Anmeldung auf der Webseite an. Der gültige Wertebereich ist 0-3600.
4. Remote Control: aktiviert oder deaktiviert den Fernzugriff auf den TK600 über HTTPS. Wenn kein Fernsteuerungsnetzwerk angegeben wird, kann der TK600 über jedes Netzwerk ferngesteuert werden.

Die folgende Abbildung zeigt die Konfiguration der Telnet-basierten Verwaltung.

Die Telnet-Parameter werden im Folgenden beschrieben:

1. Listen IP Address: gibt die zu überwachende IP-Adresse an. Zu den Optionen gehören Any, 127.0.0.1 und andere IP-Adressen.
2. Port: gibt die Nummer des Ports für Telnet an.
3. Remote Control: aktiviert oder deaktiviert den Fernzugriff auf den TK600 über Telnet. Wenn kein Fernsteuerungsnetzwerk angegeben wird, kann der TK600 über jedes Netzwerk ferngesteuert werden.

Die folgende Abbildung zeigt die Konfiguration der SSH-basierten Verwaltung.



Die SSH-Parameter werden im Folgenden beschrieben:

1. Listen IP Address: gibt die zu überwachende IP-Adresse an. Zu den Optionen gehören Any, 127.0.0.1 und andere IP-Adressen.
2. Port: gibt die Nummer des Ports für SSH an.
3. Timeout: gibt die SSH-Timeout-Zeit an. Der gültige Wertebereich ist 0-120.
4. Schlüsselmodus: fest auf RSA eingestellt.
5. Schlüssellänge: gibt die Länge des verwendeten Schlüssels an. Die Optionen sind 512, 1024, 2048 und 4096.
6. Fernsteuerung: aktiviert oder deaktiviert den Fernzugriff auf den TK600 über Telnet. Wenn kein Fernsteuerungsnetzwerk angegeben wird, kann der TK600 über jedes Netzwerk ferngesteuert werden.

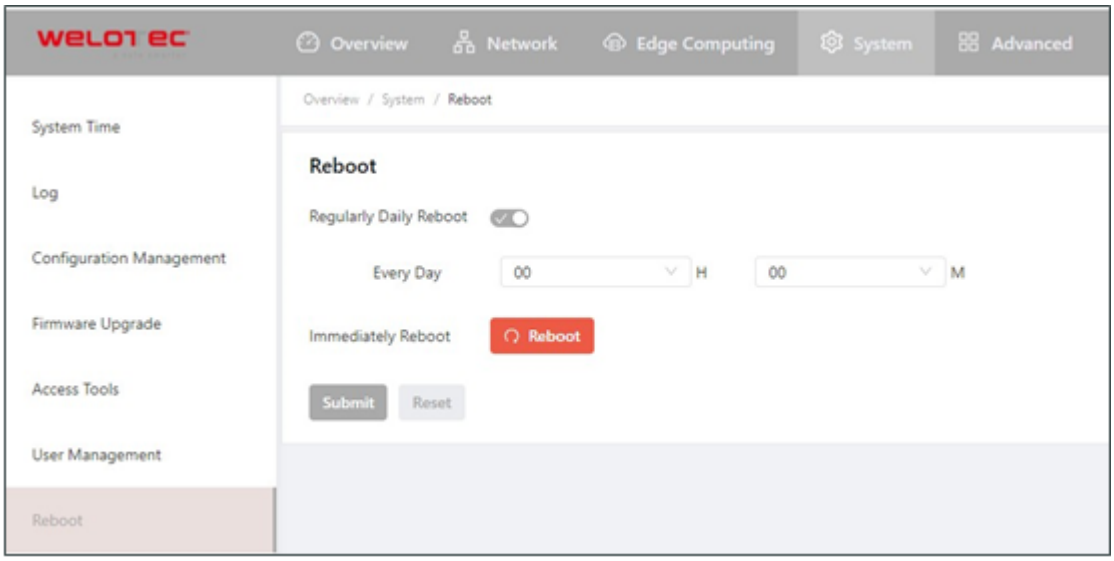
3.7.6 Benutzerverwaltung

Auf der Seite **User Management** können Sie Benutzerkonten hinzufügen und das Passwort und die Zugriffsrechte für jedes Konto verwalten. Diese Konten ermöglichen es mehreren Benutzern, auf den TK600 zuzugreifen und ihn zu verwalten. Gehen Sie wie folgt vor, um einen Benutzer hinzuzufügen:

1. Wählen Sie **System > User Management**, um die Seite **User Management** anzuzeigen.
2. Klicken Sie auf das Symbol **Add**, um einen Benutzer hinzuzufügen.
3. Stellen Sie die Parameter ein.
4. Klicken Sie auf **OK**, um die Konfiguration zu speichern.

3.7.7 Reboot

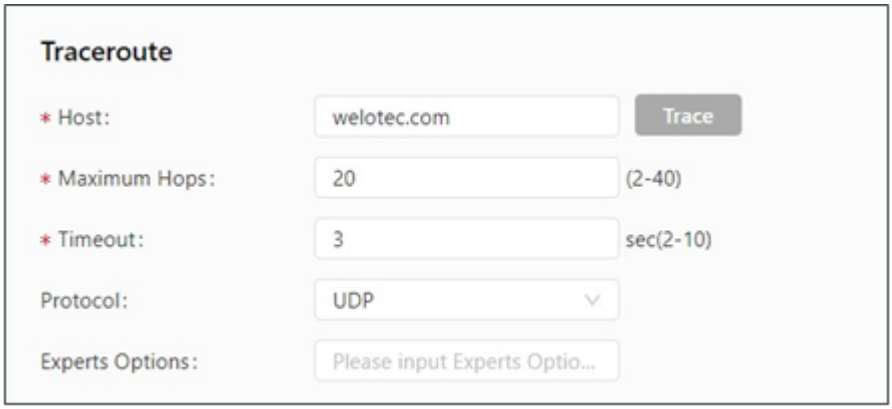
Wählen Sie **System >Reboot**, um die Seite **Reboot** anzuzeigen, und starten Sie dann den TK600 neu oder legen Sie einen geplanten Neustartplan für ihn fest. Wie in der folgenden Abbildung dargestellt, ist der TK600 so konfiguriert, dass er jeden Tag um 0:00 Uhr neu gestartet wird.



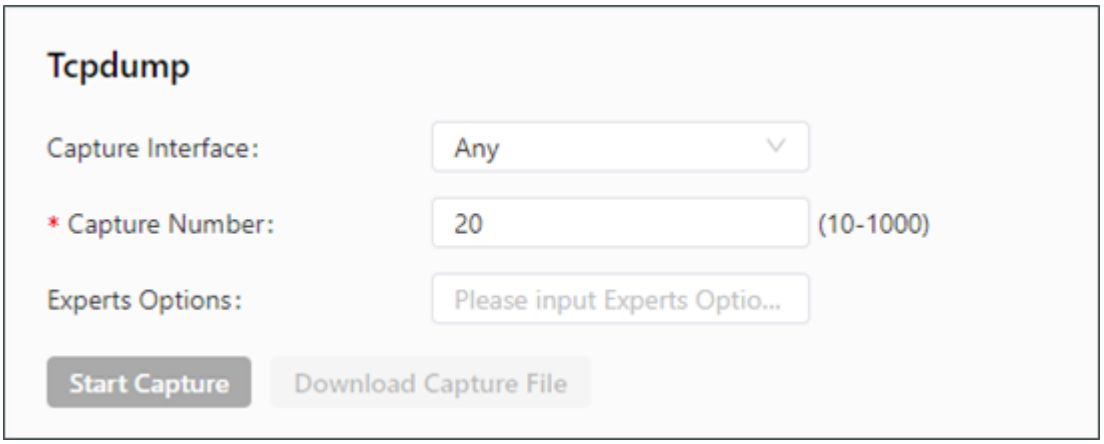
3.7.8 Netzwerk-Tools

Wählen Sie **System > Network Tools**, um die Seite **Network Tools** anzuzeigen. Auf dieser Seite können Sie Netzwerkprobleme des TK600 diagnostizieren. Sie können einige Erweiterungsoptionen in den Bereich Expertenoptionen eingeben. Zum Beispiel ermöglicht die Expertenoption -t für das Ping-Tool, dass der TK600 einen bestimmten Host kontinuierlich anpingt, bis Sie den Ping stoppen. Das Ping-Tool kann verwendet werden, um zu prüfen, ob ein Netzwerk erreichbar ist. Die folgende Abbildung zeigt die Konfiguration eines Ping-Tests.

Mit dem Tool Traceroute kann die Route ermittelt werden, über die IP-Datagramme zu einem Ziel übertragen werden. Die folgende Abbildung zeigt die Konfiguration eines Traceroute-Tests.



Das Tool Tcpdump kann verwendet werden, um Pakete zu erfassen, die über eine bestimmte Schnittstelle übertragen werden. Die folgende Abbildung zeigt die Tcpdump-Konfiguration.



3.7.9 3rd Party Benachrichtigung

Wählen Sie **System > 3rd Party Notification**, um die Seite **3rd Party Notification** anzuzeigen. Sie können die Erklärung über die für den TK600 verwendete Software von Drittanbietern anzeigen.

3.8 Advanced

Einige Funktionen sind noch nicht vollständig von der TK800 Serie zur TK600 Serie migriert. Für erweiterte Funktionen können Sie immer noch das TK800 Webinterface verwenden.

3.8.1 Administration

Auf dieser Seite können Sie den Systemstatus und den Netzwerkstatus (einschließlich Firmware-Version, MAC-Adresse, Systemzeit und Betriebszeit des Routers) anzeigen.

3.8.2 VPN

OpenVPN

Wenn in der OpenVPN-Architektur ein Benutzer auf eine entfernte virtuelle Adresse zugreift (eine Adresse einer virtuellen Netzwerkkarte, keine reale Adresse), verwendet das Betriebssystem den Routing-Mechanismus, um die Datagramme (TUN-Modus) oder Datenrahmen (TAP-Modus) an die virtuelle Netzwerkkarte zu senden. Wenn das Dienstprogramm die Daten empfängt, verarbeitet es sie und sendet sie über den Socket an das externe Netz. Wenn das entfernte Dienstprogramm die Daten aus dem externen Netz über seinen Socket empfängt, verarbeitet es die Daten und sendet sie an die virtuelle NIC. Die Anwendungssoftware empfängt dann die Daten. Zu diesem Zeitpunkt ist ein unidirektionaler Übertragungsprozess abgeschlossen. Der umgekehrte Übertragungsprozess ist ähnlich.

OpenVPN Client

Die Parameter eines OpenVPN-Clients werden im Folgenden beschrieben:

- Aktivieren: aktiviert oder deaktiviert den OpenVPN-Client.
- Index: gibt eine Tunnel-ID an.
- OpenVPN-Server: gibt die IP-Adresse oder den Domänennamen eines OpenVPN-Servers an.
- Port: gibt die Portnummer an, die zum Aufbau eines OpenVPN-Tunnels verwendet wird.
- Protokolltyp: gibt das für die Datenübertragung verwendete Protokoll an. Die Optionen sind UDP und TCP.
- Authentifizierungstyp: Wählen Sie eine Authentifizierungsart und legen Sie die Parameter für die Authentifizierungsart fest.
- Beschreibung: gibt die Beschreibung des OpenVPN-Tunnels an.
- Erweiterte Optionen anzeigen
  - Source Schnittstelle: gibt die Schnittstelle an, die für den Aufbau des OpenVPN-Tunnels verwendet wird.
  - Schnittstellentyp: gibt die Art der Daten an, die von der Schnittstelle gesendet werden.
    * Tun: meist für IP-basierte Kommunikation verwendet.
    * Tap: Ermöglicht den Durchgang kompletter Ethernet-Frames durch den OpenVPN-Tunnel und bietet Unterstützung für Nicht-IP-Protokolle.
  - Netzwerktyp: Die Optionen sind net30, p2p und subnet.

    * net30: Es werden vier IP-Adressen mit einer 30-Bit-Maske aus dem IP-Adresspool ausgewählt. Die größere der beiden dazwischen liegenden IP-Adressen wird als IP-Adresse der virtuellen NIC des Clients verwendet, die kleinere als Peer-IP-Adresse.
    * p2p: Eine IP-Adresse wird aus dem IP-Adresspool als IP-Adresse der virtuellen Netzwerkkarte des Clients ausgewählt, und die tatsächliche IP-Adresse der virtuellen Netzwerkkarte wird als Peer-IP-Adresse verwendet.

- Subnet: Eine IP-Adresse wird aus dem IP-Adresspool als IP-Adresse der virtuellen Netzwerkkarte des Clients ausgewählt, und die Subnetzmaske der virtuellen Netzwerkkarte wird als Peer-IP-Adresse verwendet.
- Cipher: gibt das Protokoll an, das zur Verschlüsselung der über den OpenVPN-Tunnel übertragenen Daten verwendet wird. Die Einstellung muss auf dem Client und dem Server identisch sein.
- HMAC: gibt die Authentifizierungsmethode an, die für die über den OpenVPN-Tunnel übertragenen Daten verwendet wird. Die Daten können nicht übertragen werden, wenn die Authentifizierung fehlschlägt. Die Einstellung muss auf dem Client und dem Server identisch sein.
- Compression LZO: gibt das Komprimierungsformat der über den OpenVPN-Tunnel übertragenen Daten an.
- Redirect-Gateway: ermöglicht, dass die OpenVPN-Schnittstelle als Standard-Gateway für den Client fungiert, so dass der gesamte Datenverkehr des Clients über die OpenVPN-Schnittstelle weitergeleitet wird.
- Remote Float: Ermöglicht es dem entfernten Gerät, seine IP-Adresse oder seinen Port zu ändern.
- Link Detection Interval: gibt das Intervall für das Senden von Link-Detection-Paketen nach dem Aufbau eines OpenVPN-Tunnels an. Der gültige Wertebereich ist 10-1800, und die Einheit ist Sekunde.
- Link Detection Timeout: Legt die Zeitüberschreitung bei der OpenVPN-Verbindungserkennung fest. Wenn die Anzahl der Fehler bei der Verbindungserkennung den Maximalwert erreicht, initiiert das lokale Gerät eine neue L2TP-Verbindung. Der gültige Wertebereich ist 60-3600.
- MTU: gibt die maximale Übertragungseinheit (maximum transmit unit) auf der OpenVPN-Schnittstelle an, die in Bytes ausgedrückt wird.
- Enable Debug: Aktiviert oder deaktiviert die Debugging-Protokolle.
- Expert Configuration: legt die Parameter der OpenVPN-Erweiterung fest.
- Import Configuration: Wählen Sie die OpenVPN-Konfigurationsdatei aus, die Sie importieren möchten.

OpenVPN Server

Die Parameter eines OpenVPN-Servers werden im Folgenden beschrieben:

- Enable: aktiviert oder deaktiviert den OpenVPN-Server.
- Config Mode: Gibt an, ob die Konfiguration manuell durchgeführt oder eine Konfigurationsdatei importiert werden soll.
    - Manual Config (Manuelle Konfiguration)
    - Authentication Type (Authentifizierungstyp): gibt die verwendete Authentifizierungsmethode an.
    - Local IP Address: gibt die virtuelle IP-Adresse der OpenVPN-Server-Schnittstelle an.
    - Remote IP Address: gibt die virtuelle IP-Adresse des OpenVPN-Clients an.
    - Description: gibt die Beschreibung des OpenVPN-Tunnels an.

Show Advanced Options: aktiviert oder deaktiviert die Anzeige der erweiterten Optionen.

- Source Interface: gibt die Schnittstelle an, die für den Aufbau des OpenVPN-Tunnels verwendet wird.
- Interface Type: gibt die Art der Daten an, die von der Schnittstelle gesendet werden.
  - Tun: meist für IP-basierte Kommunikation verwendet.
  - Tap: Ermöglicht den Durchgang kompletter Ethernet-Frames durch den OpenVPN-Tunnel und bietet Unterstützung für Nicht-IP-Protokolle.
    - Netzwerktyp: Die Optionen sind net30, p2p und subnet.
    - Protokolltyp: gibt das zwischen Client und Server verwendete Kommunikationsprotokoll an. Die Einstellung muss auf dem Client und dem Server identisch sein.
    - Port: gibt die Portnummer des OpenVPN-Dienstes an.
    - Cipher: gibt das Protokoll an, das zur Verschlüsselung der über den OpenVPN-Tunnel übertragenen Daten verwendet wird. Die Einstellung muss auf dem Client und dem Server identisch sein.
    - HMAC: gibt die Authentifizierungsmethode an, die für die über den OpenVPN-Tunnel übertragenen Daten verwendet wird. Die Daten können nicht übertragen werden, wenn die Authentifizierung fehlschlägt. Die Einstellung muss auf dem Client und dem Server identisch sein.
    - Compression LZO: Legt das Komprimierungsformat der über den OpenVPN-Tunnel übertragenen Daten fest. Die Einstellung muss mit der auf dem Client identisch sein.
    - Link Detection Interval: gibt das Intervall für das Senden von Link-Detection-Paketen nach dem Aufbau eines OpenVPN-Tunnels an. Der gültige Wertebereich ist 10-1800, und die Einheit ist Sekunde.
    - Link Detection Timeout: gibt die Zeitspanne für die OpenVPN-Link-Erkennung an. Wenn das lokale Gerät innerhalb dieses Zeitraums keine Antwort auf das Link-Erkennungspaket erhält, schlägt die Link-Erkennung fehl. Der gültige Wertebereich ist 60-3600.
    - MTU: gibt die maximale Übertragungseinheit auf der OpenVPN-Schnittstelle an, die in Bytes ausgedrückt wird.
    - Enable Debug: Aktiviert oder deaktiviert die Debugging-Protokolle.
    - Expert Configuration: legt die Parameter der OpenVPN-Erweiterung fest.
    - Username/Password: gibt den Benutzernamen und das Kennwort für den Serverzugang an, wenn die Kennwortauthentifizierung verwendet wird.

Zertifikatsverwaltung

Das Simple Certificate Enrollment Protocol (SCEP) ist ein gemeinsam von Cisco und Verisign formuliertes Protokoll zur Zertifikatsverwaltung. Dieses Protokoll kombiniert die Standards PKCS#7 und PKCS#10 und unterstützt umfangreiche Clients und Zertifizierungsstellen („Certification Authorities“, CAs).Die Parameter der Zertifikatsverwaltung werden im Folgenden beschrieben:

- Enable SCEP: aktiviert oder deaktiviert das Simple Certificate Enrollment Protocol.
- Force to re-enroll: startet den Zertifikatsregistrierungsdienst jedes Mal neu, ohne den Status des aktuellen Zertifikats zu überprüfen.
- Status: Zeigt den aktuellen Status der Zertifikatsregistrierung auf dem Gerät an, d. h. Initiierung, Registrierung, erneute Registrierung oder Abschluss.
- Protect Key: gibt den Schlüssel an, der bei der Zertifikatsregistrierung für die Verschlüsselung des digitalen Zertifikats festgelegt wurde. Sie können ein Zertifikat nur importieren oder exportieren, wenn Sie den bei der Zertifikatsregistrierung festgelegten Schutzschlüssel eingegeben haben.
- Protect Key Confirm: Geben Sie den Schutzschlüssel erneut ein, um den Schlüssel zu bestätigen.

- Strict CA: legt die ID einer vertrauenswürdigen CA fest. Das Zertifikat eines Geräts wird von einer vertrauenswürdigen CA registriert und ausgestellt. Daher müssen Sie die ID einer vertrauenswürdigen CA angeben, um das Gerät an die CA zu binden. Anschließend führt das Gerät die Beantragung, den Erwerb, den Widerruf und die Abfrage von Zertifikaten über diese CA durch.
- Server-URL: gibt die URL des CA-Servers an. Sie müssen zuvor eine CA-Server-URL angeben, damit das Gerät über SCEP ein Zertifikat bei diesem Server beantragen kann, z. B. http://100.17.145.158:8080/certsrv/mscep/mscep.dll.
- Common Name: gibt den allgemeinen Namen des erforderlichen Zertifikats an.
- FQDN: gibt den vollständig qualifizierten Domänennamen („Fully Qualified Domain Name“, FQDN) des Zertifikats an. Der FQDN ist die eindeutige Kennung einer Einheit in einem Netzwerk und setzt sich aus einem Hostnamen und einem Domänennamen zusammen. Er kann in eine IP-Adresse aufgelöst werden. Zum Beispiel bilden der Hostname www und der Domänenname whatever.com einen FQDN [www.whatever.com.]
- Unit 1: gibt den Namen der ersten Organisation des Zertifikats an.
- Unit 2: gibt den Namen der zweiten Organisation des Zertifikats an.
- Domain: gibt den qualifizierten Domainnamen des Zertifikats an.
- Serial Number: gibt die Seriennummer des Zertifikats an.
- Challenge: gibt den Challenge-Code des Zertifikats an, der für den Widerruf des Zertifikats erforderlich ist (optional).
- Challenge Confirm: Geben Sie den Sicherheitscode erneut ein, um die Einstellung zu bestätigen.
- Unstructured address: gibt die IP-Adresse des Zertifikats an.
- RSA Key Length: gibt die Länge des RSA-Schlüssels an. Der gültige Wertebereich ist 128-2048, und die Einheit ist Bit.
- Poll Interval: gibt das Intervall an, in dem das Gerät den aktuellen Zertifikatsstatus vom Server abfragt. Der gültige Wertebereich ist 30-3600, die Einheit ist Sekunde.
- Poll Timeout: gibt die maximale Dauer für die Abfrage des Zertifikatsstatus an. Das Gerät geht davon aus, dass der Zertifikatsantrag fehlgeschlagen ist, wenn die Timeout-Zeit abgelaufen ist. Der gültige Wertebereich ist 30-86400, und die Einheit ist Sekunde.
- Revocation: Aktiviert oder deaktiviert den Zertifikatswiderruf.
  - CRL URL: gibt die URL der Verteilungsstelle für die Zertifikatswiderrufsliste (CRL) an.
  - OCSP URL: gibt die URL des Online Certificate Status Protocol (OCSP) Servers an. In der Regel ist dies die gleiche URL wie die des CA-Servers.

Hinweis: Wenn Sie ein Zertifikat verwenden, stellen Sie sicher, dass die Systemzeit mit der tatsächlichen Zeit übereinstimmt.

4 FAQ

4.1 Wie kann ich die Werkseinstellungen über die Hardware wiederherstellen?

Folgen Sie diesen Schritten

1. Drücken Sie die RESET-Taste, während Sie die TK600 einschalten.
2. Sobald die LED ERROR aufleuchtet (ca. 10 Sekunden nach dem Einschalten), lassen Sie die RESET-Taste los.
3. Nach ein paar Sekunden leuchtet die ERROR-LED nicht mehr auf. Drücken Sie nun erneut die RESET-Taste, bis die Error-LED blinkt, und lassen Sie dann die Taste los.
4. Jetzt blinken die LED-Leuchten ERROR und STATUS, was bedeutet, dass das Zurücksetzen auf die Standardeinstellung erfolgreich war.

Standard-Werkseinstellungen	
IP WAN:	192.168.1.1
IP LAN:	192.168.2.1
Net mask:	255.255.255.0
Username:	adm
Password:	123456
Serial Port RS-485:	115200-N-8-1
Serial Port RS-232:	9600-N-8-1