# Industrieller Router Ultra-Serie UR75

Benutzerhandbuch



## Sicherheitshinweise

Milesight übernimmt keine Verantwortung für Verluste oder Schäden, die durch Nichtbeachtung der Anweisungen in dieser Bedienungsanleitung entstehen.

- Das Gerät darf in keiner Weise zerlegt oder umgebaut werden.
- Um die Gefahr von Bränden und Stromschlägen zu vermeiden, halten Sie das Produkt vor der Installation von Regen und Feuchtigkeit fern.
- Stellen Sie das Gerät nicht an Orten auf, an denen die Temperatur oder Luftfeuchtigkeit unterhalb/oberhalb des Betriebsbereichs liegt.
- Das Gerät darf niemals Stürzen, Stößen oder Schlägen ausgesetzt werden.
- Stellen Sie sicher, dass das Gerät bei der Installation fest sitzt.
- Stellen Sie sicher, dass der Stecker fest in die Steckdose eingesteckt ist.
- Ziehen Sie nicht an der Antenne oder dem Netzkabel, sondern ziehen Sie diese an den Anschlüssen heraus.



## Konformitätserklärung

UR75 entspricht den grundlegenden Anforderungen und anderen relevanten Bestimmungen der CE- und RoHS-Richtlinien.



Für Unterstützung wenden Sie sich bitte an den technischen Support von Milesight:
E-Mail:iot.support@milesight.com Support-Portal: support.milesight-iot.com Tel.: 86-592-5085280
Fax: 86-592-5023065
Adresse: Gebäude C09, Software Park III, Xiamen 361024, China

**Revisionsverlauf**

| Datum | Dokumentversion | Beschreibung |
|---|---|---|
| 25. November 2022 | V 3.0 | Erstversion basierend auf Hardware 3.x |
| 17. Januar 2023 | V 3.1 | 1. Änderung des Web-GUI-Designs<br>2. LT2P- und PPTP-VPN-Client-Funktion hinzufügen<br>3. VLAN-Funktion hinzufügen<br>4. HTTPS-Zertifikat-Importfunktion hinzufügen |
| 20. April 2024 | V 3.2 | 1. Node-RED-, DDNS-, IP-Passthrough-, SMS- und SNMP-Funktion hinzufügen<br>2. Umbenennung von Modbus Master in Modbus Client<br>3. Unterstützung für benutzerdefinierte Mobilfunk-MTU, IMS und SMS-Zentralnummer<br>4. Hinzufügen der NAT-Option auf WAN- und Mobilfunk-Schnittstellen<br>5. Unterstützung für die Anpassung des AT-Debug-Befehls<br>6. Unterstützung für Hard-Reset |
| 20. September 2024 | V3.3 | 1. Hinzufügen des WLAN-Client-Modus und Unterstützung für die Konfiguration des WLAN-Ländercodes;<br>2. WLAN-Statusseite hinzufügen;<br>3. Funktion zum Zurücksetzen der Verbindung mit hoher Priorität bei zwei Karten hinzufügen;<br>4. MQTT Ereignisalarm und Multi-User-Funktion hinzufügen;<br>5. Anpassen des Systemmenüs. |

# Inhalt

# Kapitel 1 Produktvorstellung

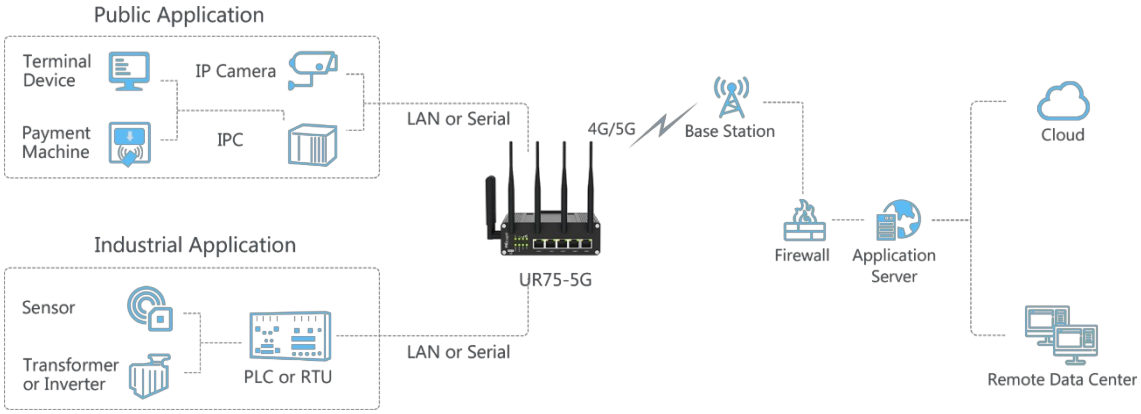
## 1.1 Übersicht

Der UR75 ist ein industrieller Mobilfunkrouter mit integrierten intelligenten Softwarefunktionen, der für vielfältige M2M/IoT-Anwendungen entwickelt wurde. Der UR75 wurde auf die neueste Mobilfunktechnologie - 5G - aufgerüstet und ermöglicht so einen ultraschnellen Breitbandzugang über ein 5G-Mobilfunknetz.

Dank der Verwendung einer leistungsstarken und stromsparenden CPU in Industriequalität sowie eines drahtlosen Moduls bietet der UR75 ein Netzwerk mit Wire-Speed bei geringem Stromverbrauch und einer extrem kompakten Bauweise, um eine äußerst sichere und zuverlässige Verbindung zum drahtlosen Netzwerk zu gewährleisten.

Gleichzeitig unterstützt der UR75 auch Gigabit-Ethernet-Ports, serielle Ports (RS232/RS485) und I/O (Input/Output), wodurch Sie M2M-Anwendungen durch die Kombination von Daten und Videos in begrenzter Zeit und mit begrenztem Budget skalieren können.

Der UR75 eignet sich besonders für intelligente Stromnetze, digitale Medieninstallationen, industrielle Automatisierung, Telemetriegeräte, medizinische Geräte, digitale Fabriken, Finanzwesen, Zahlungsgeräte, Umweltschutz, Wasserwirtschaft und vieles mehr.




## 1.2 Vorteile

**Ultraschnelle Konnektivität**

- Industrietaugliche Quad-Core-CPU ARM Cortex-A55 mit großem Speicher,die eine hohe Leistung für die Datenübertragung bietet
- Globales 5G (NSA/SA)/4G LTE-Netzwerk mit zwei SIM-Karten für die Sicherung zwischen mehreren Mobilfunknetzen
- Dual Carrier Aggregation (2CC CA) wird im 5G Sub-6GHz unterstützt und ermöglicht eine größere Signalabdeckung mit einer hervorragenden Download-Geschwindigkeit von bis zu 4,67 Gbps
- Plug&Play, blitzschnelle Übertragung über Gigabit-Ethernet-Ports oder USB-Typ-C-Schnittstelle

- Unterstützt Wi-Fi 6 und ermöglicht gleichzeitige 2,4G- und 5G-Dualband-Verbindungen mit einer Download-Geschwindigkeit von bis zu 1,8 Gbit/s

**Sicherheit und Zuverlässigkeit**

- Automatische Failover-/Failback-Sicherung über Ethernet, Mobilfunk (Dual-SIM) und WLAN
- Sichere Übertragung mit VPN-Tunneln wie IPsec/OpenVPN/L2TP/PPTP
- Integrierte Hardware-Überwachung zur automatischen Wiederherstellung nach verschiedenen Ausfällen, wodurch ein Höchstmaß an Verfügbarkeit gewährleistet wird
- Ausgestattet mit mehreren Sicherheitsmaßnahmen wie ACL, DMZ,SYN-Flood-Schutz und Datenfilterung, um die Sicherheit des Netzwerks zu gewährleisten
- Unterstützt Policy Routing und NAT für einen sichereren Intranetzugang

**Einfache Wartung**

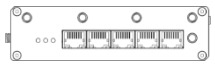
- Milesight DeviceHub ermöglicht eine einfache Einrichtung, Massenkonfiguration und zentralisierte Verwaltung von Remote-Geräten
- Das benutzerfreundliche Design der Weboberfläche und mehrere Upgrade-Optionen helfen Administratoren bei der einfachen Verwaltung der Geräte
- Unterstützt mehrstufige Benutzerberechtigungen für die Sicherheitsverwaltung
- Schnelle und benutzerfreundliche Programmierung mit dem Entwicklungswerkzeug Node-RED

**Industrielles Design**

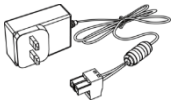
- Breiter Betriebstemperaturbereich von -30 °C bis 60 °C und industrielles Design für raue Umgebungen
- Robustes Gehäuse mit Schutzart IP30, optimiert für die Montage auf DIN-Schienen oder in Regalen.
- Ausgestattet mit E/A, serieller Schnittstelle und GPS für industrielle Übertragungsanwendungen
- 3 Jahre Garantie inklusive

# Kapitel 2 Hardware-Einführung

## 2.1 Packliste

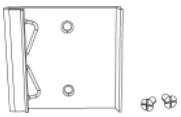


1 × UR75-Gerät



1 × Netzteil

1 × 8-poliger steckbarer Anschluss

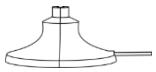


1 × DIN-Schienen-Kit

4× kurze Mobilfunkantennen

4 × Stubby-WLAN-Antennen

1 × GPS-Antenne



Magnetische Antennenhalterungen (optional)

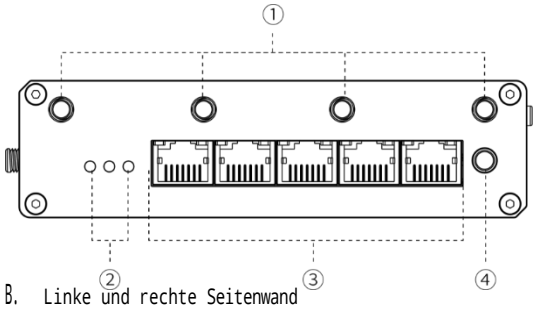
1 × Kurzanleitung


1 × Garantiekarte

**Wenn eines der oben genannten Teile fehlt oder beschädigt ist, wenden Sie sich bitte an Ihren Vertriebsmitarbeiter.**

## 2.2 Übersicht über die Hardware

A. Frontblende

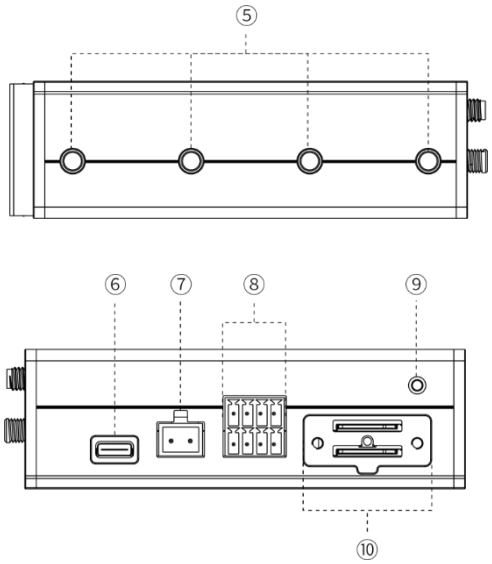



① Wi-Fi-Antennenanschlüsse (nur Wi-Fi-Version) LED-Anzeigefeld

② SYSTEM: Strom- und Statusanzeige SIM 1 und SIM 2: SIM-Statusanzeige Ethernet-Anschlüsse und Anzeigen

③④ GPS-Antennenanschluss

B. Linke und rechte Seitenwand




⑤ Mobilfunkantennenanschlüsse

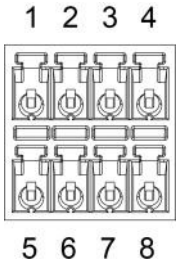
⑥ USB-Typ-C-Anschluss

⑦ Stromanschluss Serielle Anschlüsse und E/A-Anschlüsse

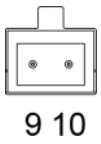
⑧ Erdungsbolzen

⑨⑩ SIM-Steckplätze und Reset-Taste

## 2.3 Serielle & IO- & Stromversorgungs-Pinbelegungen




| PIN | RS232 | RS485 | DI | DO | Beschreibung |
|---|---|---|---|---|---|
| 1 | --- | --- | IN | --- | Digitaler Eingang |
| 2 | GND | --- | GND | --- | Masse |
| 3 | --- | B | --- | --- | Daten - |
| 4 | TXD | --- | --- | --- | Daten übertragen |
| 5 | --- | --- | --- | COM | Gemeinsame Grundlage |
| 6 | --- | --- | --- | OUT | Digitalausgang |
| 7 | --- | A | --- | --- | Daten + |
| 8 | RXD | --- | --- | --- | Daten empfangen |

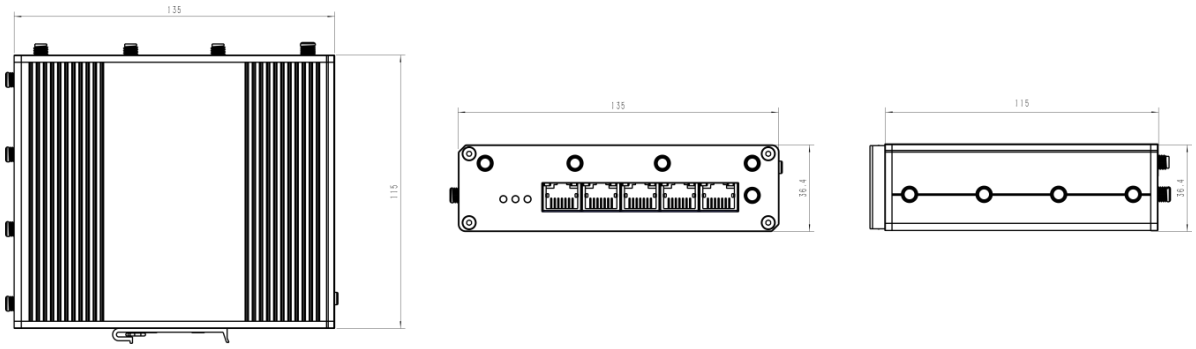



| PIN | Beschreibung | Drahtfarbe |
|---|---|---|
| 9 | Positiv | Rot |
| 10 | Negativ | Schwarz |

## 2.4 LED-Anzeigen

| LED | Anzeige | Status | Beschreibung |
|---|---|---|---|
| SYSTEM | Stromversorgung und Systemstatus | Aus | Der Strom ist ausgeschaltet |
| | | Orange | Statisch: Das System wird gestartet |
| | | Grün | Statisch: Das System läuft ordnungsgemäß |
| | | Rot | Statisch: Das System funktioniert nicht richtig |
| SIM1/SIM2 | Mobilfunk- und Signalstatus | Aus | SIM-Karte wird registriert oder kann nicht registriert werden (oder es sind keine SIM-Karten eingelegt) |
| | | Grün | Blinkt schnell: SIM-Karte wurde registriert und wählt sich gerade ein |
| | | | Leuchtet konstant: SIM-Karte wurde registriert und wählt sich mit dem 5G-Netzwerk verbunden |
| | | Orange | Statisch: SIM-Karte wurde registriert und wählt sich ein zum 4G-Netzwerk |
| Ethernet-Anschluss | Verbindungsanzeige (orange) | Aus | Getrennt oder Verbindungsfehler |
| | | Ein | Verbunden |
| | | Blinkt | Daten werden übertragen |
| | Geschwindigkeitsanzeige (Grün) | Aus | 100-Mbps-Modus |
| | | Ein | 1000-Mbps-Modus |

## 2.5 Abmessungen (mm)



## 2.6 Reset-Taste

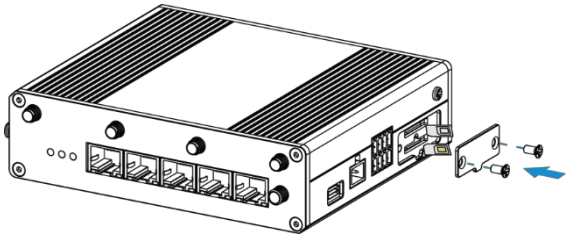
Die Reset-Taste befindet sich neben den SIM-Steckplätzen.

| Funktion | Beschreibung | |
|---|---|---|
| | LED-Anzeige | Aktion |
| Soft-Reset | Statisch | Halten Sie beim Einschalten des Geräts die Reset-Taste<br>Taste länger als 5 Sekunden gedrückt. |
| | Statisch →Alle blinken | Lassen Sie die Taste los und warten Sie. |
| | Aus →SYSTEM Statisch Grün | Das Gerät wird auf die Werkseinstellungen zurückgesetzt. |
| Hard-Reset | Aus | Wenn das Gerät ausgeschaltet ist, halten Sie die Reset-Taste gedrückt<br>Taste gedrückt. |
| | Statisch →Alle blinken | Schalten Sie das Gerät ein, während Sie die Reset-Taste<br>mehr als 5 Sekunden gedrückt halten und dann loslassen. |
| | Aus →SYSTEM Statisch Grün | Das Gerät wird auf die Werkseinstellungen zurückgesetzt. |

# Kapitel 3 Hardware-Installation

## 3.1 SIM-Installation

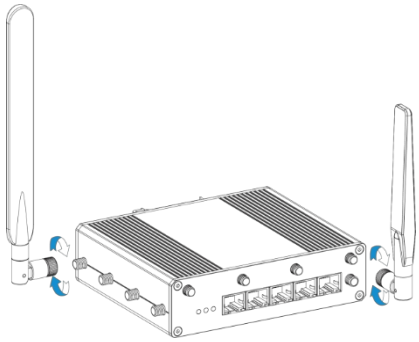
Schrauben Sie die Halterung der SIM-Karte ab, legen Sie die SIM-Karte gemäß dem Richtungssymbol auf dem Gerät in den Steckplatz ein und befestigen Sie die Halterung wieder mit Schrauben am Gerät.



## 3.2 Antenneninstallation

Drehen Sie die Antenne entsprechend in den Antennenanschluss. Antennen sollten vertikal installiert werden und sich immer an einem Standort mit gutem Empfang befinden.

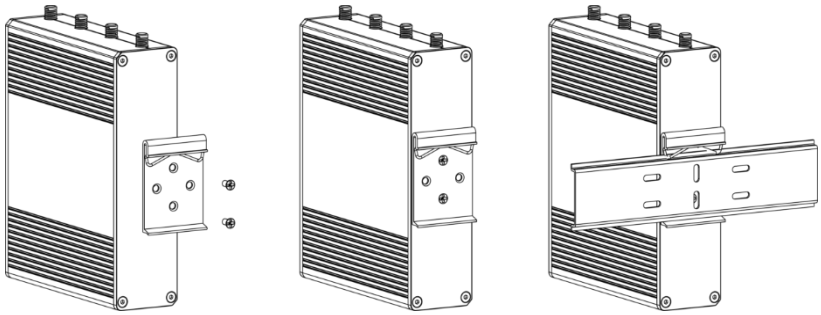
Hinweis: Die Mobilfunkantennen 1, 2 und 3 sind Hauptantennen, Antenne 4 ist eine Diversity-Antenne.



## 3.3 Geräteinstallation

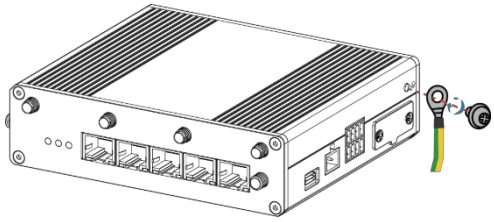
Das UR75-Gerät kann auf einem Tisch aufgestellt oder auf einer DIN-Schiene montiert werden. Verwenden Sie für die Montage auf einer DIN-Schiene zwei M3 × 6-Flachkopf-Kreuzschlitzschrauben, um die Halteklammer am Gerät zu befestigen, und hängen Sie das Gerät dann an die DIN-Schiene. Die Breite der DIN-Schiene beträgt 3,5 cm.

**Das empfohlene Drehmoment für die Befestigung beträgt 1,0 N·m, das maximal zulässige Drehmoment 1,2 N·m.**



## 3.4 Installation der Schutzerdung

Verbinden Sie den Erdungsring des Erdungskabels des Gehäuses mit dem Erdungsbolzen und schrauben Sie die Erdungsmutter fest.



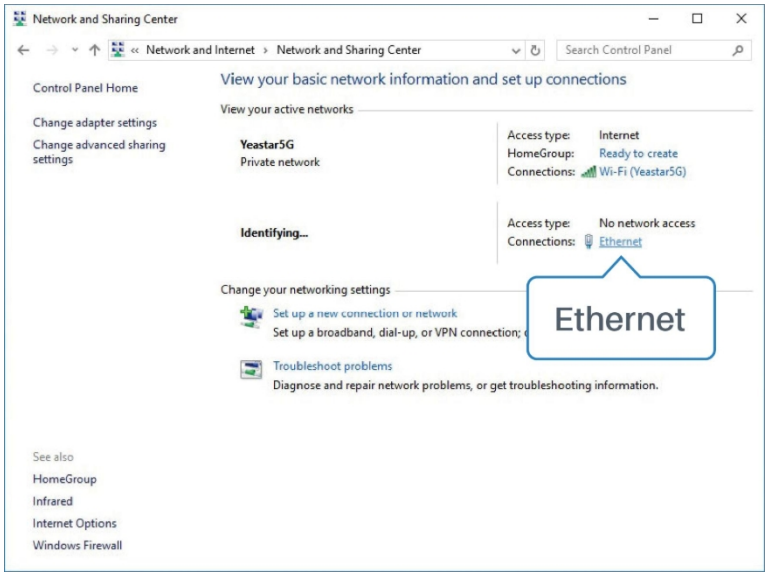
# Kapitel 4 Zugriff auf die Web-GUI

Der UR75 bietet eine benutzerfreundliche Web-GUI für die Konfiguration, auf die Benutzer über den LAN-Port zugreifen können. In diesem Kapitel wird erläutert, wie Sie auf die Web-GUI des UR75-Routers zugreifen können.

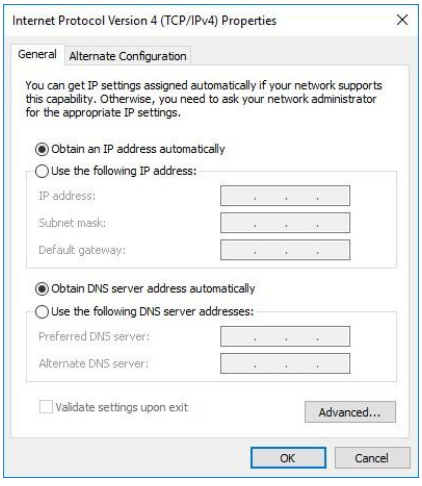
Benutzername: **admin**
Passwort: **password**
IP-Adresse: **192.168.1.1**

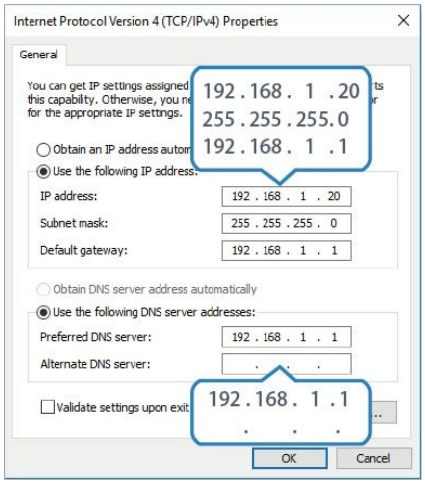
Verbinden Sie den PC direkt mit dem LAN-Port oder USB-Port des UR75-Routers. Die folgenden Schritte basieren auf dem Betriebssystem Windows 10 und dienen als Referenz.

1. Gehen Sie zu **Systemsteuerung → Netzwerk und Internet → Netzwerk- und Freigabecenter** und klicken Sie dann auf **Ethernet** (kann auch anders heißen).

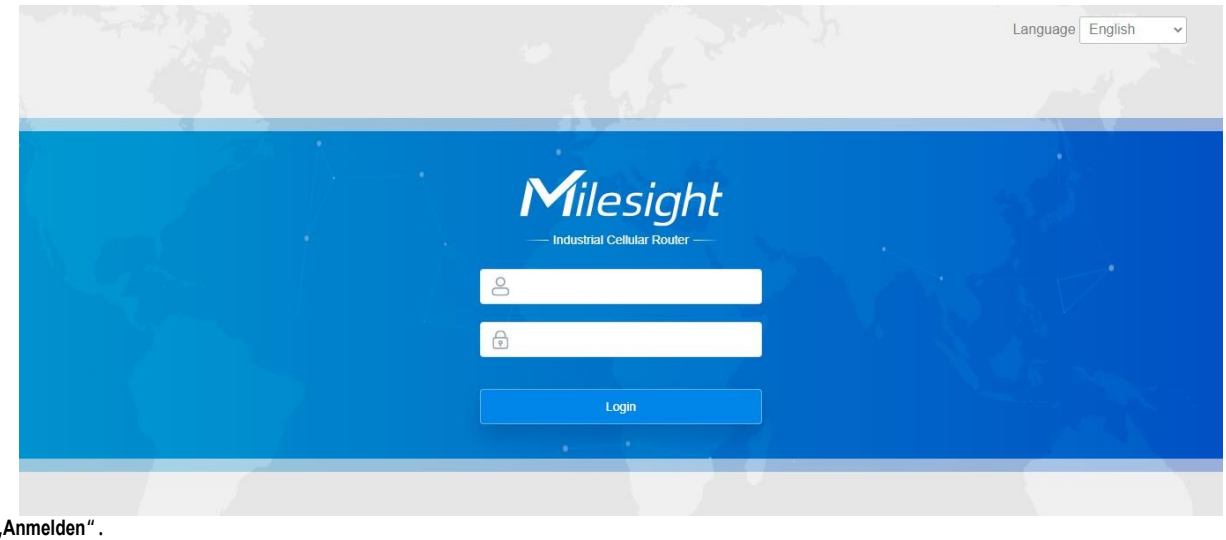



2. Gehen Sie zu **Eigenschaften → Internetprotokoll Version 4 (TCP/IPv4)**, wählen Sie **„IP-Adresse automatisch beziehen“** oder **„Folgende IP-Adresse verwenden“** und weisen Sie dann manuell eine statische IP-Adresse innerhalb desselben Subnetzes des Geräts zu.



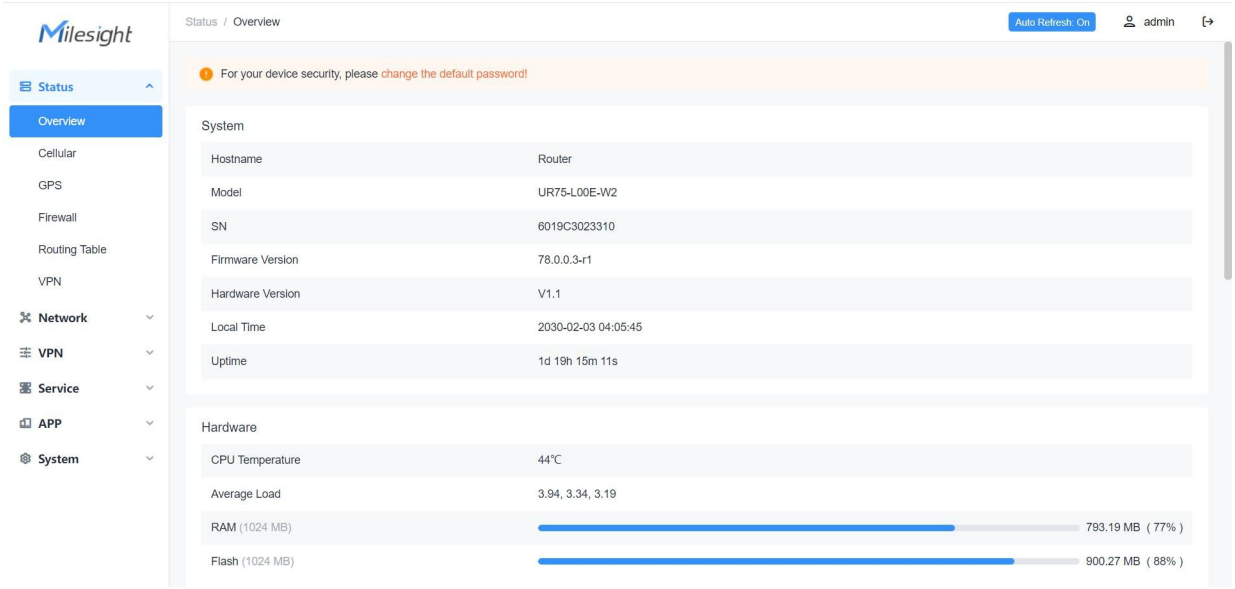
3. Öffnen Sie einen Webbrowser auf Ihrem PC (Chrome wird empfohlen), geben Sie die IP-Adresse 192.168.1.1 ein, um auf die Web-GUI zuzugreifen, geben Sie dann den Standardbenutzernamen und das Standardkennwort ein und klicken Sie auf




**„Anmelden“.**

**Wenn Sie den Benutzernamen oder das Passwort mehr als fünfmal falsch eingeben, wird die Anmeldeseite für 10 Minuten gesperrt.**

4. Nachdem Sie sich bei der Web-GUI angemeldet haben, können Sie Systeminformationen anzeigen und Konfigurationen am Router vornehmen.



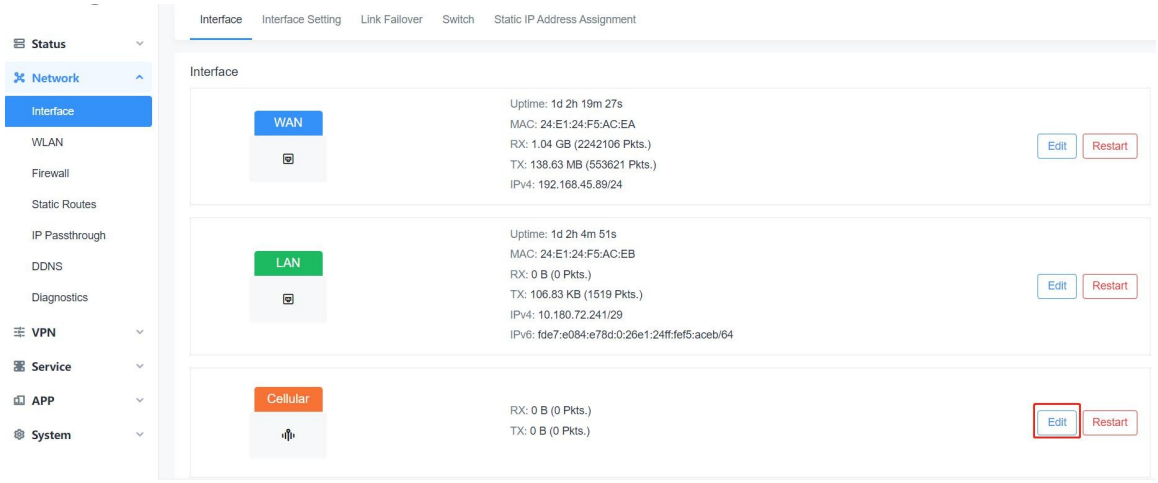
# Kapitel 5 Anwendungsbeispiele

## 5.1 Mobilfunkverbindung konfigurieren

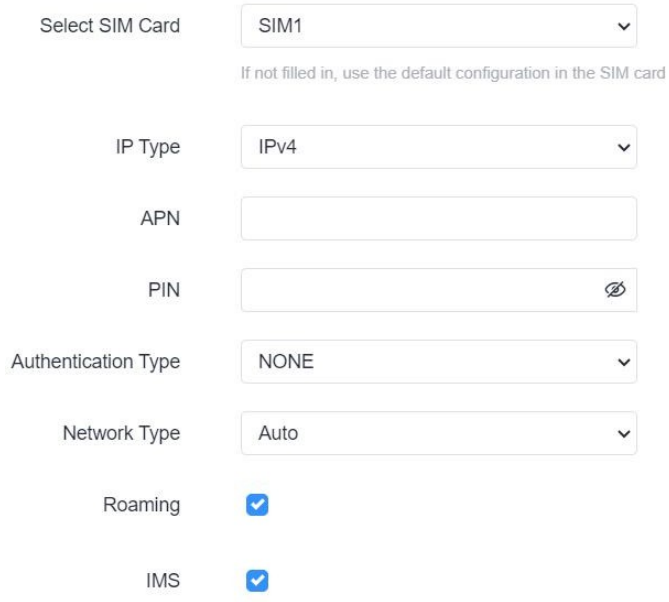
UR75-Router verfügen über zwei Mobilfunk-Schnittstellen: SIM1 und SIM2. Es ist jeweils nur eine Mobilfunk-Schnittstelle aktiv. Wir zeigen Ihnen anhand eines Beispiels, wie Sie eine SIM-Karte in den SIM1-Steckplatz des UR75 einlegen und den Router so konfigurieren, dass Sie über Mobilfunk Zugang zum Internet erhalten.

**Konfigurationsschritte**

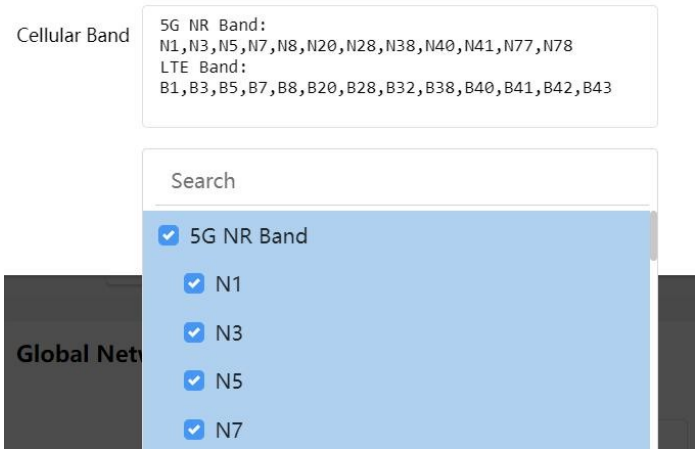
1. Stellen Sie sicher, dass die SIM-Karte richtig eingelegt ist und alle Mobilfunkantennen an den richtigen Anschlüssen angeschlossen sind.
2. Gehen Sie zu **Netzwerk > Schnittstelle >** Schnittstellenseite, suchen Sie die Mobilfunkschnittstelle und klicken Sie auf die Schaltfläche **Bearbeiten**.



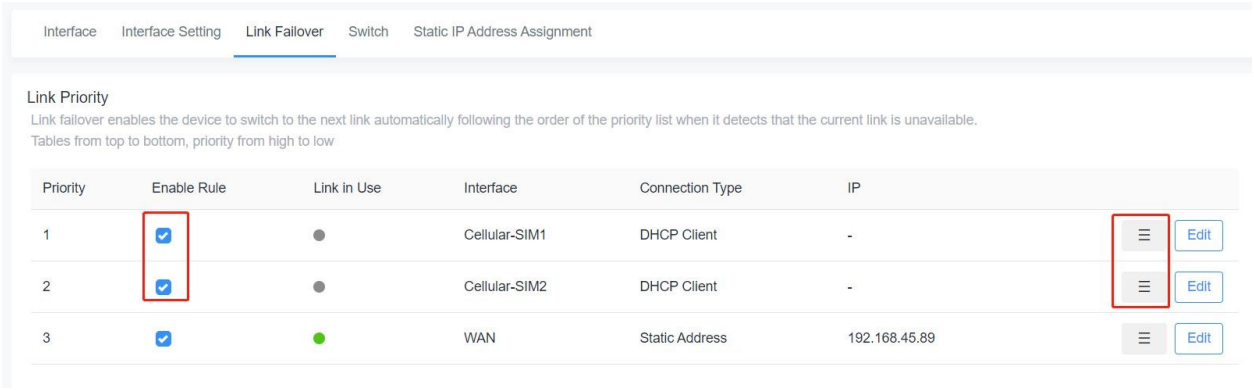

3. Wählen Sie die SIM-Karte aus, die Sie konfigurieren möchten, geben Sie die erforderlichen Informationen zur SIM-Karte ein und speichern Sie alle Einstellungen.




Für eine 5G-Verbindung können Sie bestimmte Frequenzbänder auswählen, um eine hohe Netzwerkgeschwindigkeit zu gewährleisten.

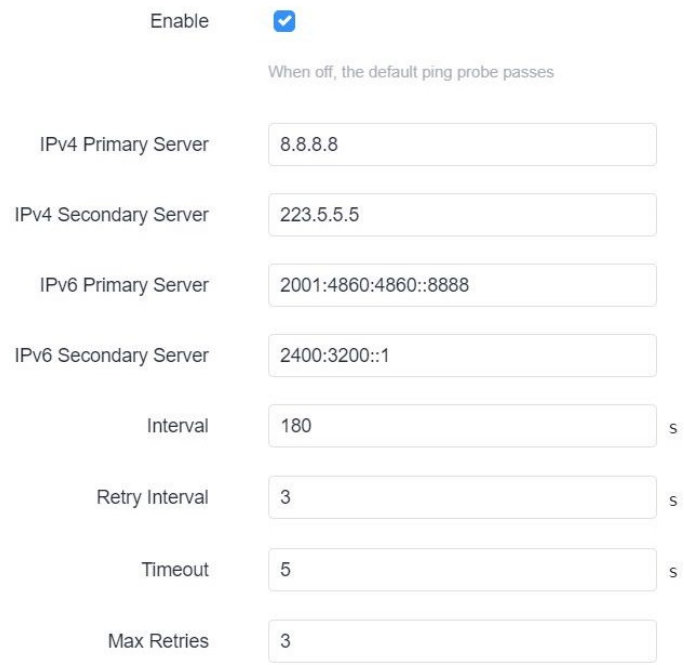



4. Gehen Sie zu **Netzwerk > Schnittstelle > Link-Failover,** um die entsprechende SIM-Karte zu aktivieren, und ziehen Sie die Schaltflächen, um die Link-Priorität zu ändern.

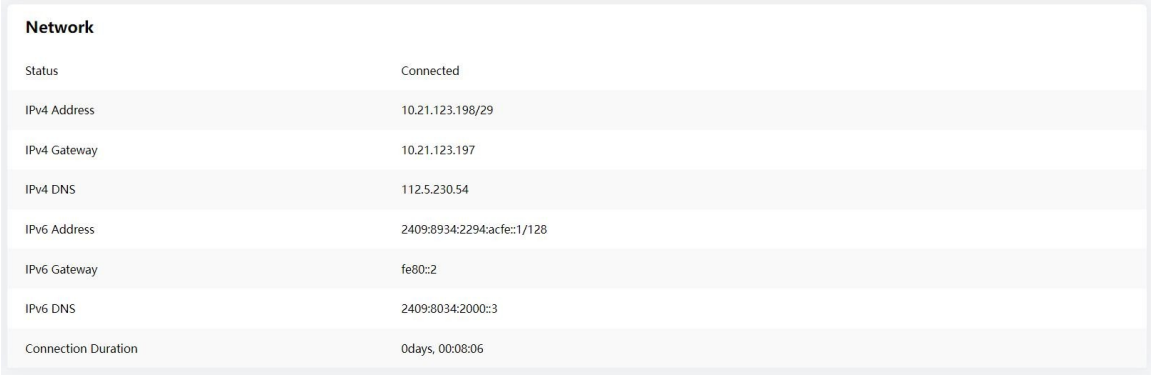



5. Klicken Sie auf **„Bearbeiten“** eines Links, um die ICMP-Ping-Erkennungsinformationen zu konfigurieren. Wenn die Ping-Prüfung aktiviert ist, sendet der Router ICMP-Pakete an den Erkennungsserver, um zu überprüfen, ob dieser Link gültig ist. Wenn keine Antwort erfolgt und die maximale Anzahl an Wiederholungsversuchen überschritten wird, wechselt er zu dem Link mit niedrigerer Priorität.

**Hinweis:** Wenn Sie eine private SIM-Karte verwenden, ändern Sie bitte die Adresse des privaten Servers oder deaktivieren Sie die Ping-Prüfung.



6. Gehen Sie zu **„Status“ > „Mobilfunk“**, um den Status der Mobilfunkverbindung zu überprüfen. Wenn der Modemstatus „Bereit“ und der Netzwerkstatus **„Verbunden“** lautet, wurde die SIM-Karte erfolgreich gewählt.




**Verwandtes Thema**

Mobilfunk-Einstellungen

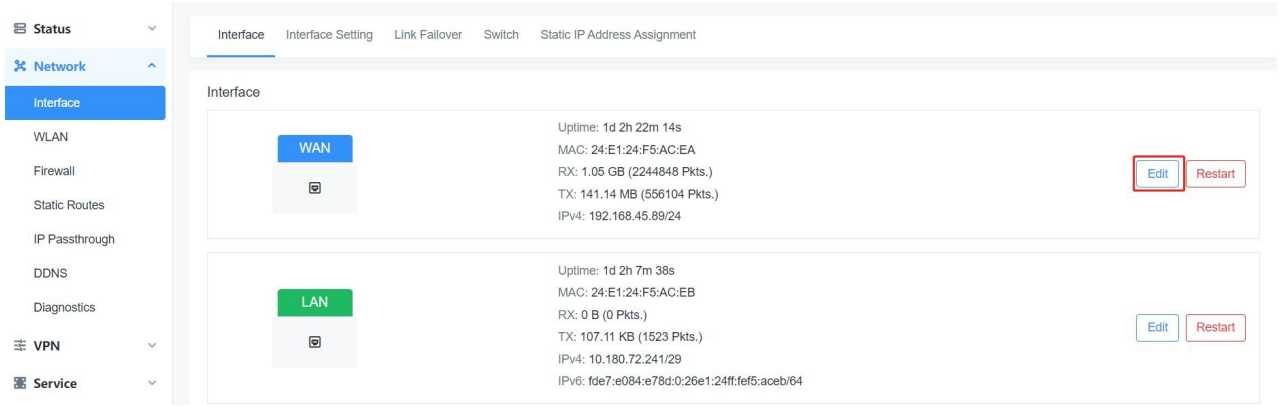
Mobilfunk-Status

## 5.2 Ethernet-Verbindung konfigurieren

UR75-Router unterstützen den Netzwerkzugang über den WAN-Port.

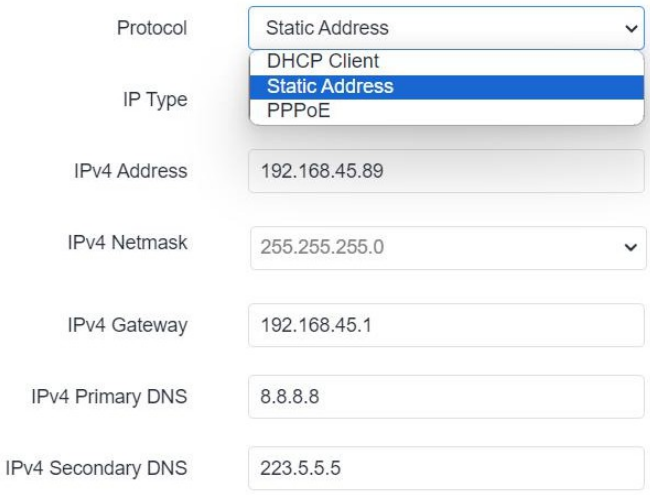
**Konfigurationsschritte**

1. Gehen Sie zu **Netzwerk > Schnittstelle >** Schnittstellenseite, suchen Sie die WAN-Schnittstelle und klicken Sie auf die Schaltfläche **Bearbeiten**.

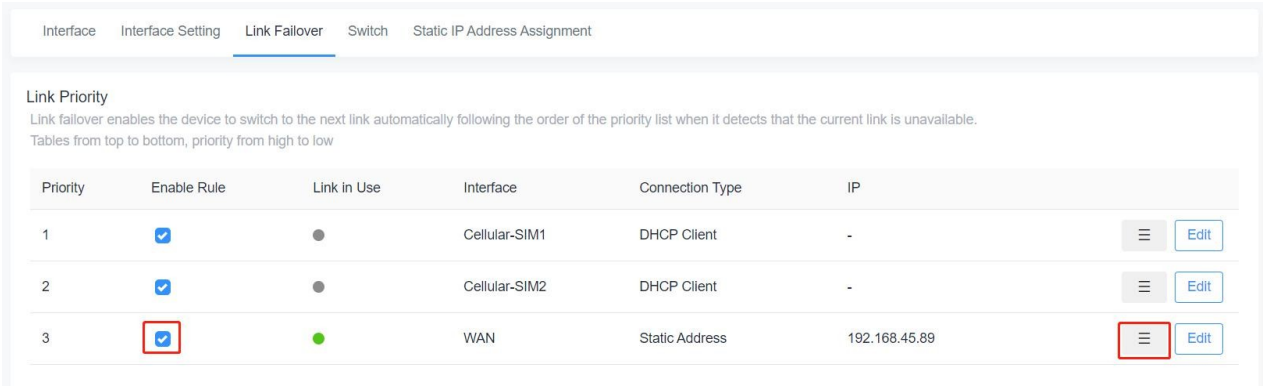



2. Wählen Sie das Protokoll entsprechend Ihrem Netzwerkrouter-Modus oder Netzwerkanbieter-Typ aus, konfigurieren Sie die entsprechenden Parameter und speichern Sie anschließend alle Einstellungen.

- **DHCP:** Der übergeordnete Netzwerkrouter weist dem WAN-Port des UR75 eine IP-Adresse zu. Dies ist die einfachste Methode und erfordert, dass der übergeordnete Router den DHCP-Server aktiviert.
- **Statusadresse:** Weisen Sie eine statische IP-Adresse mit demselben Subnetz wie das LAN-Subnetz des oberen Netzwerkrouters zu. Außerdem muss mindestens ein DNS-Server konfiguriert werden.
- **PPPoE:** Geben Sie den Benutzernamen und das Passwort Ihres PPPoE-Kontos ein. Wenden Sie sich dazu an Ihren Netzwerkanbieter.

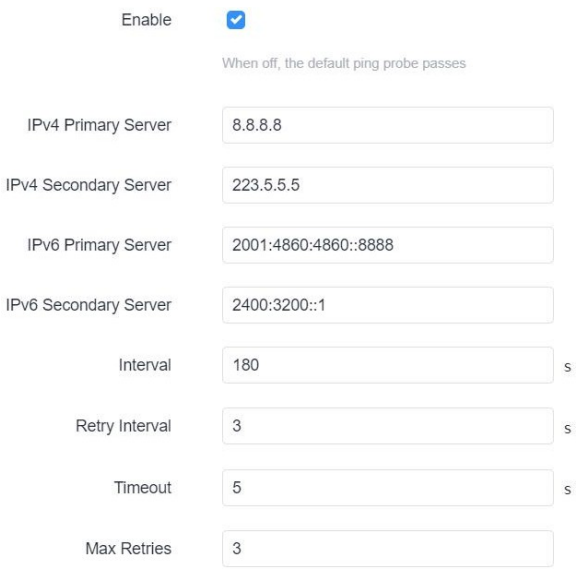



3. Gehen Sie zu **Netzwerk > Schnittstelle > Link-Failover,** um WAN zu aktivieren, und ziehen Sie die Schaltfläche, um die Link-Priorität zu ändern.

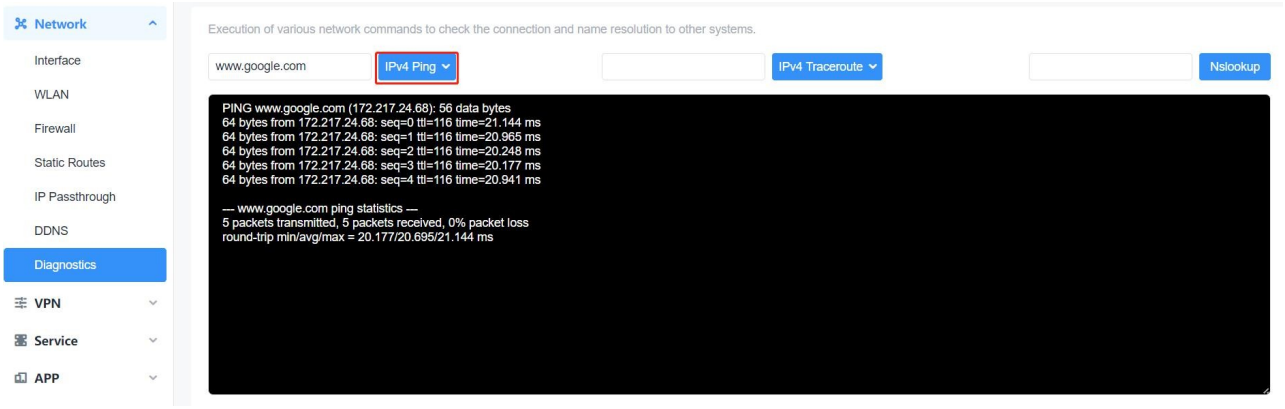



4. Klicken Sie auf **„Bearbeiten"** eines Links, um die ICMP-Ping-Erkennungsinformationen zu konfigurieren. Wenn die Ping-Prüfung aktiviert ist, sendet der Router ICMP-Pakete an den Erkennungsserver, um zu überprüfen, ob dieser Link gültig ist. Wenn keine Antwort erfolgt und die maximale Anzahl an Wiederholungsversuchen überschritten wird, wechselt er zu dem Link mit niedrigerer Priorität.

**Hinweis:** Wenn Sie ein privates Netzwerk verwenden, ändern Sie bitte die Adresse des privaten Servers oder deaktivieren Sie die Ping-Prüfung.



5. Klicken Sie auf **„Netzwerk > Diagnose“**, um die Netzwerkverbindung zu überprüfen.




**Verwandtes Thema**

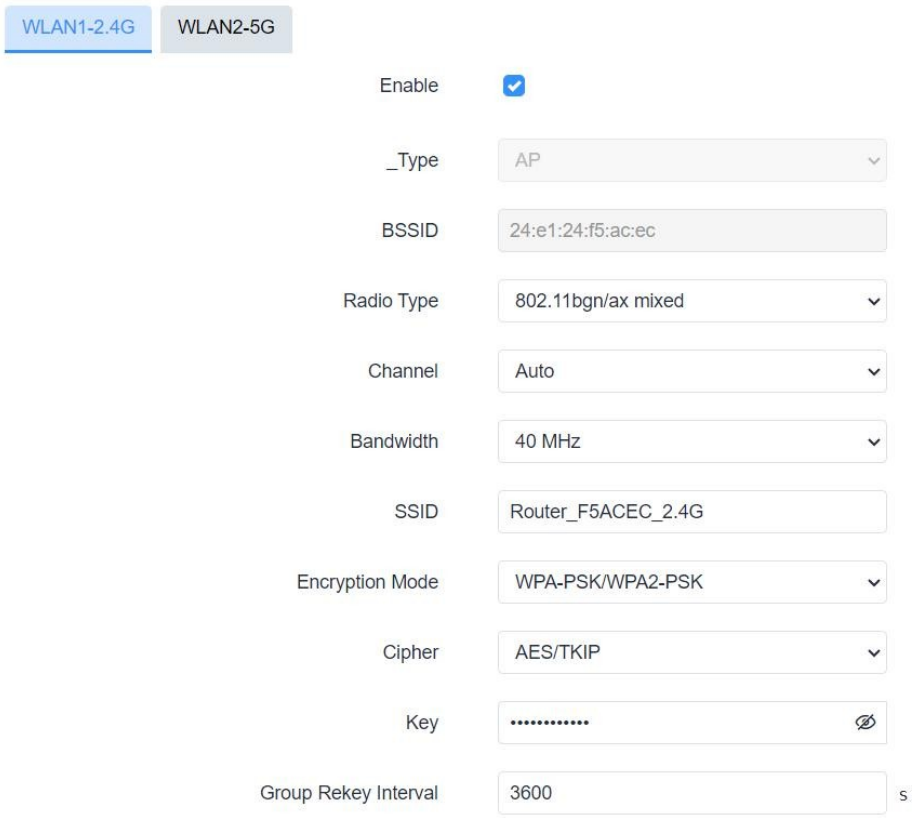
WAN-Einstellungen

## 5.3 WLAN-Zugangspunkt konfigurieren

UR75-Router unterstützen sowohl 2,4-GHz- als auch 5-GHz-WLAN und können als Zugangspunkte fungieren, um gleichzeitig anderen Geräten Netzwerkzugang zu gewähren. Wir werden nun ein Beispiel für die Konfiguration eines 2,4-GHz-WLAN-Zugangspunkts betrachten.

**Konfigurationsschritte**

1. Stellen Sie sicher, dass der Router WLAN unterstützt und die WLAN-Antennen an die richtigen Anschlüsse angeschlossen sind.
2. Gehen Sie zur Seite **„Netzwerk > WLAN“**, um den 2,4-GHz-WLAN-Modus zu aktivieren. Anschließend können Benutzer den Funktyp, die SSID und andere Parameter ändern. Aus Sicherheitsgründen wird empfohlen, einen Verschlüsselungsmodus auszuwählen und einen Schlüssel für Geräte festzulegen, die eine Verbindung zum WLAN herstellen sollen.




3. Verwenden Sie ein Smartphone, um eine Verbindung zum Zugangspunkt des UR75 herzustellen. Sie können die Informationen zum verbundenen Client/Benutzer auf der Seite **„Status > Übersicht"** überprüfen.


**Verwandtes Thema**

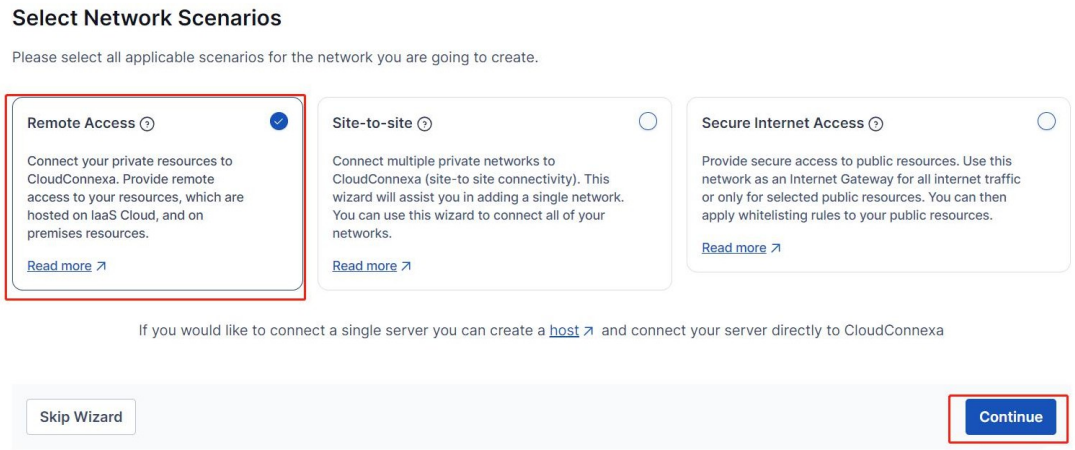
WLAN-Einstellungen

## 5.4 OpenVPN-Client konfigurieren

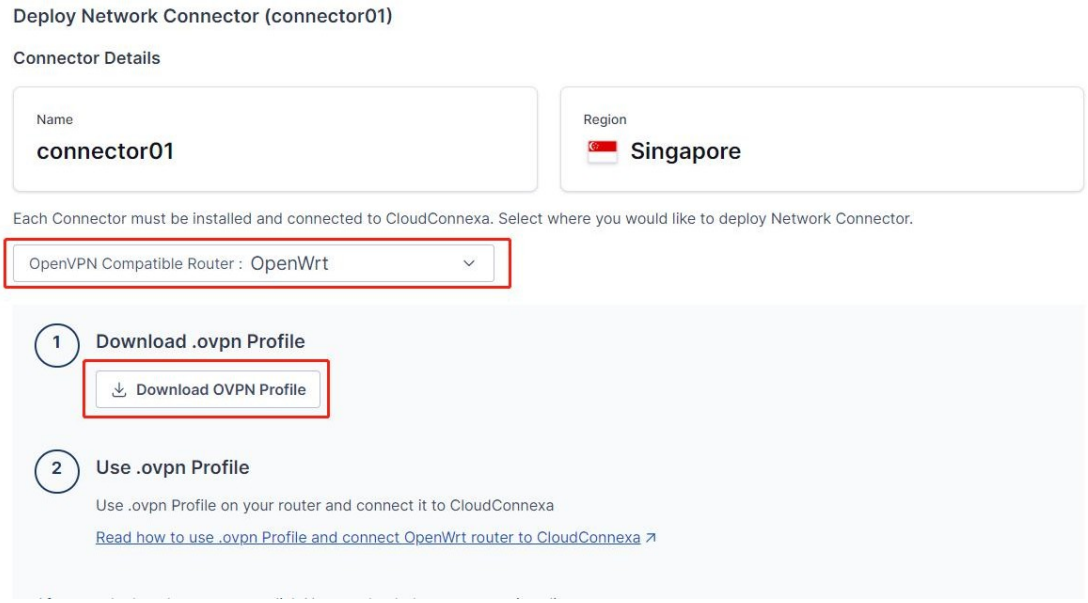
UR75-Router können als OpenVPN-Clients oder OpenVPN-Server fungieren. Wir zeigen Ihnen anhand eines Beispiels, wie Sie den OpenVPN-Client für die Verbindung mit CloudConnexa konfigurieren.

**Konfigurationsschritte**

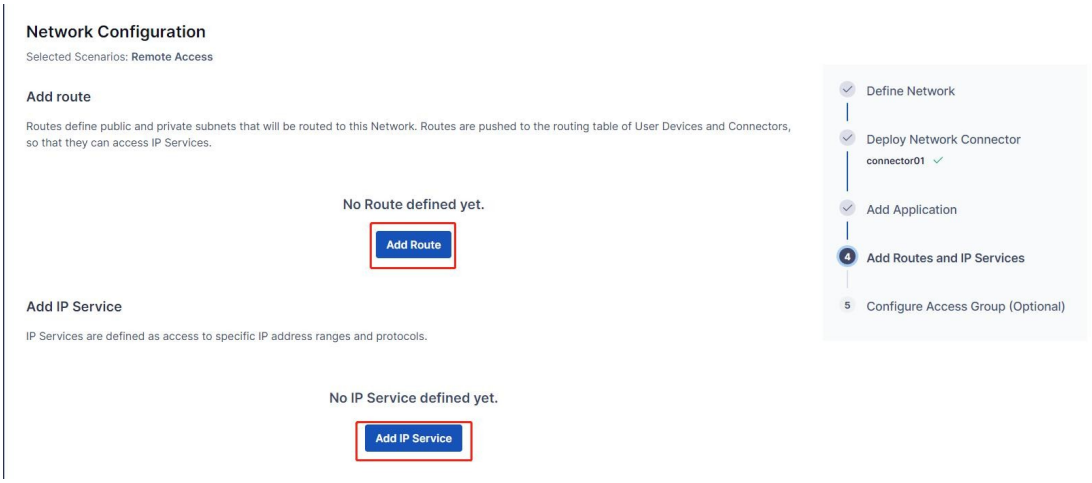
1. Stellen Sie sicher, dass der UR75 Zugang zum Internet hat.
2. Melden Sie sich bei Ihrem CloudConnexa-Konto an, wählen Sie den Abschnitt „Netzwerk" und wählen Sie den gewünschten Dienst entsprechend Ihren Anforderungen aus. Folgen Sie dann den Anweisungen des Assistenten, um mit den Einstellungen fortzufahren.



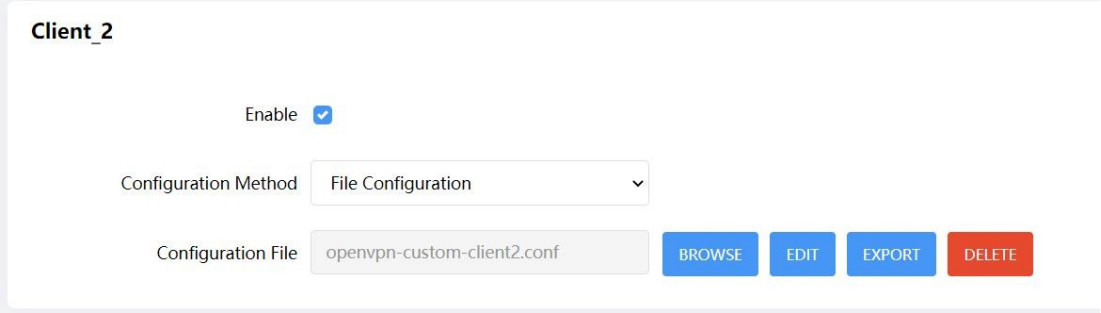

3. Wählen Sie als Anbietertyp „OpenWrt“ aus und laden Sie die OVPN-Datei herunter.



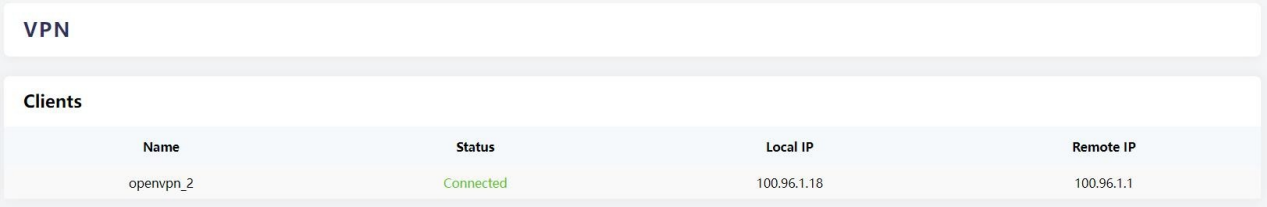

4. Wenn Sie auf die Endgeräte im Subnetz zugreifen müssen, müssen Sie die Route und den IP-Dienst als LAN-Subnetz des Routers hinzufügen.



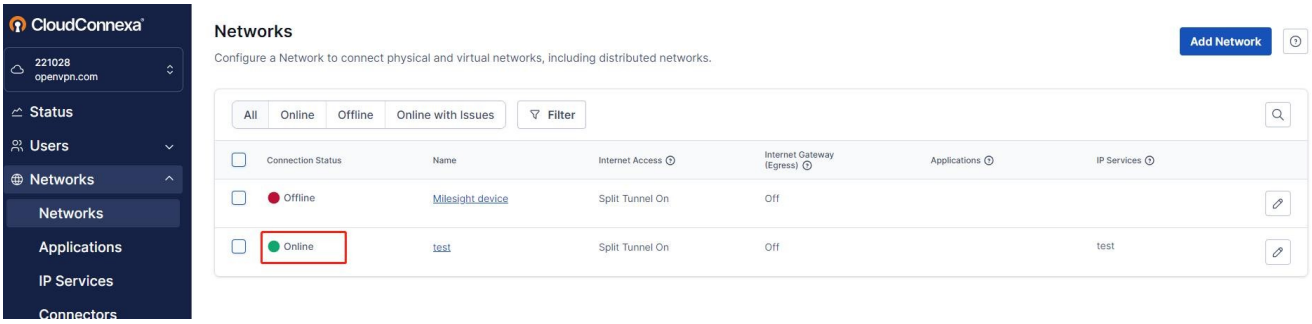
5. Gehen Sie auf der UR75 zur Seite **„VPN > OpenVPN > OpenVPN-Client“**, wählen Sie als Konfigurationsmethode „Dateikonfiguration“ aus und importieren Sie dann die OVPN-Datei.




6. Gehen Sie zur Seite **„Status > VPN“**, um zu überprüfen, ob der Client verbunden ist.




Sie können den Verbindungsstatus auch auf CloudConnexa überprüfen.



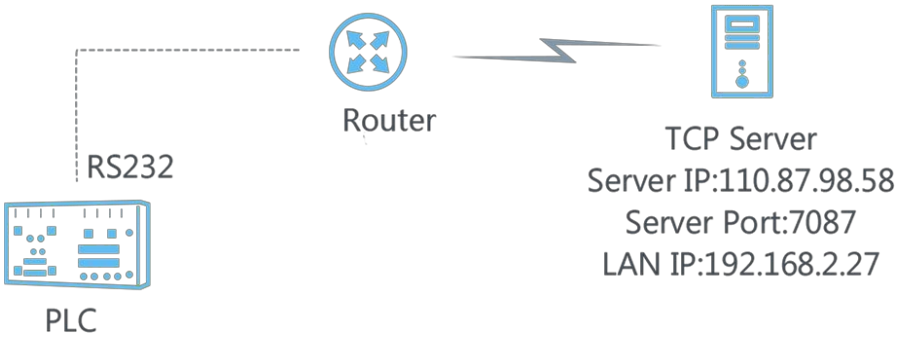

**Verwandtes Thema**

OpenVPN-Client

## 5.6 Serielle DTU-Verbindung konfigurieren

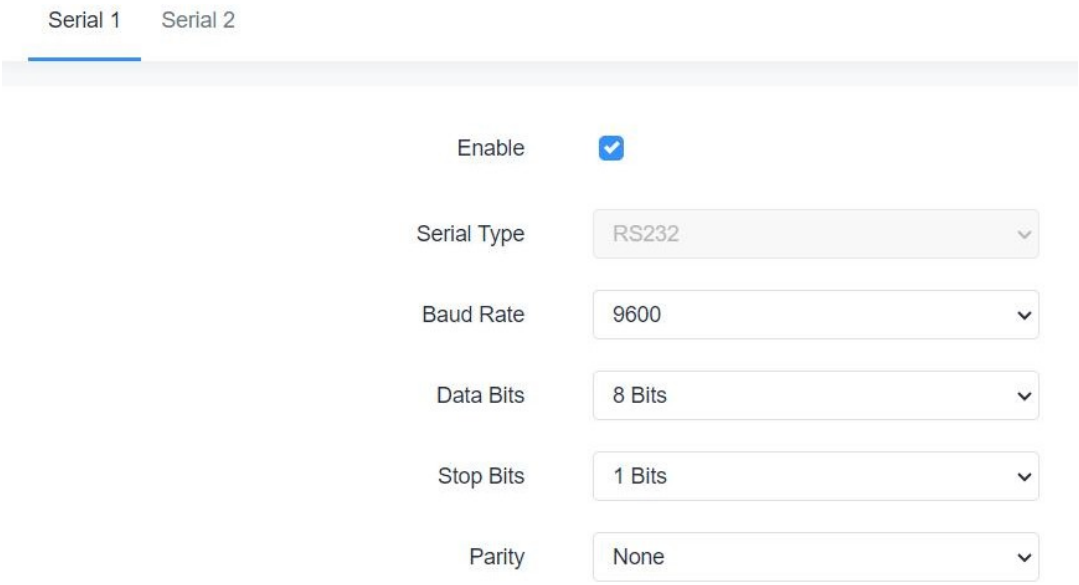
**Beispiel**

Eine SPS ist über RS232 mit dem UR75 verbunden und muss die Daten transparent an einen Remote-TCP-Server übertragen.

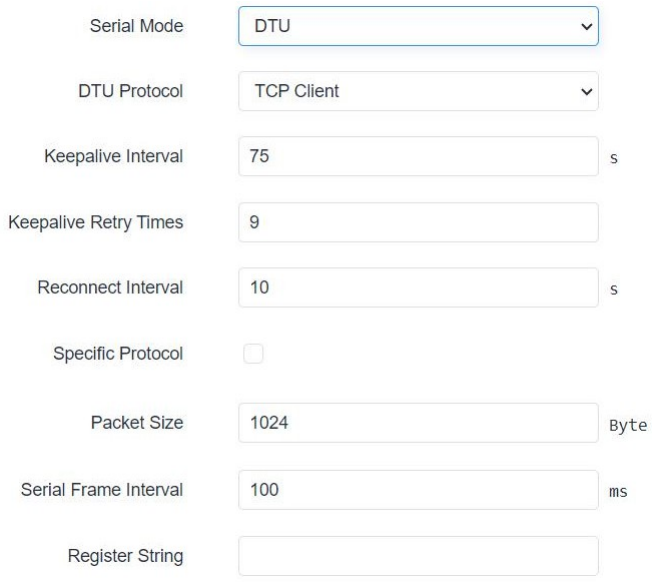



**Konfigurationsschritte**

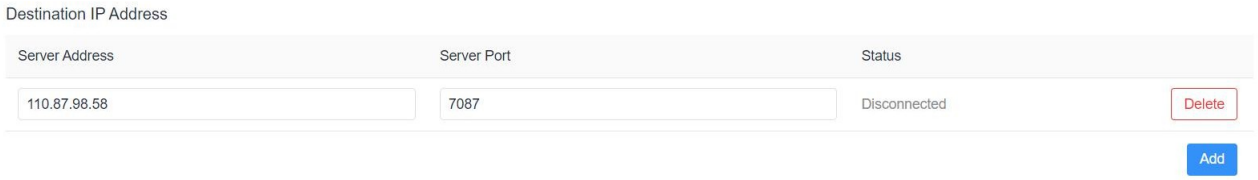
1. Gehen Sie zu **„Service" > „Serielle Schnittstelle"**, aktivieren Sie „Seriell 1" und konfigurieren Sie die Parameter der seriellen Schnittstelle. Die Parameter der seriellen Schnittstelle müssen mit denen der SPS übereinstimmen, wie in der Abbildung unten gezeigt.



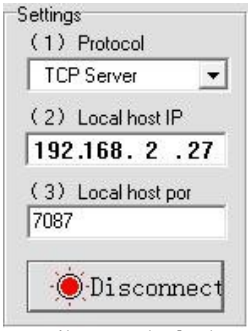

2. Konfigurieren Sie den seriellen Modus als **DTU-Modus** und das Protokoll als **TCP-Client**.



3. Konfigurieren Sie die IP-Adresse und den Port des TCP-Servers.



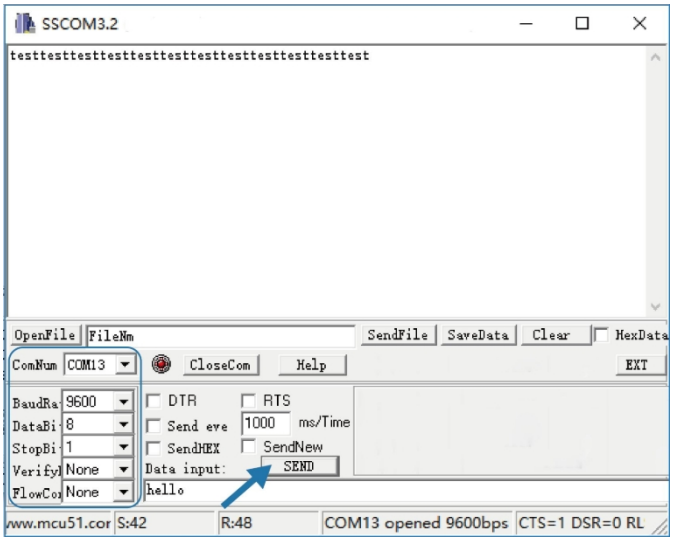

4. Starten Sie den TCP-Server auf dem PC. Nehmen Sie als Beispiel die Testsoftware **Netassist**. Stellen Sie sicher, dass die Portzuordnung vorgenommen wurde.



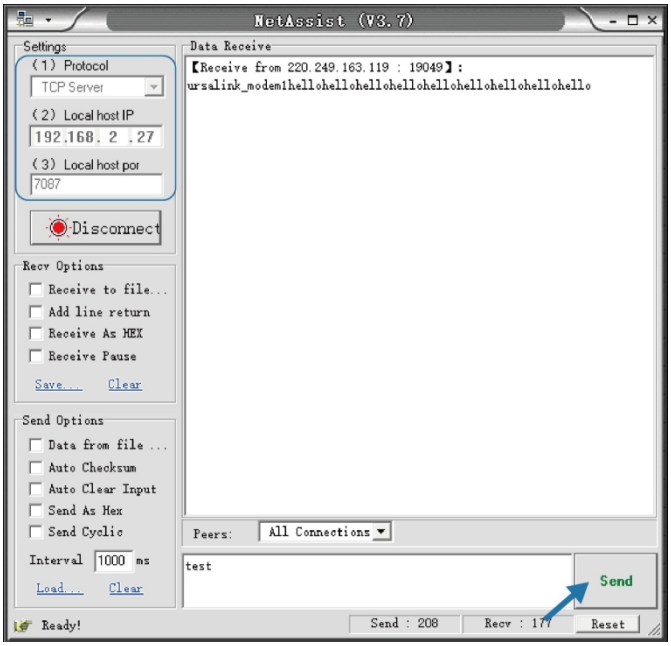

5. Verbinden Sie den UR75 über RS232 mit dem PC, um die SPS-Simulation durchzuführen. Starten Sie anschließend die sscom-Software auf dem PC, um die Kommunikation über die serielle Schnittstelle zu testen.


6. Nachdem die Verbindung zwischen dem UR75 und dem TCP-Server hergestellt wurde, können Sie Daten zwischen sscom und Netassit senden.

**PC-Seite**




**TCP-Serverseite**




7. Nachdem der Test der seriellen Kommunikation abgeschlossen ist, können Sie die SPS zum Testen an den RS232-Anschluss des UR75 anschließen.

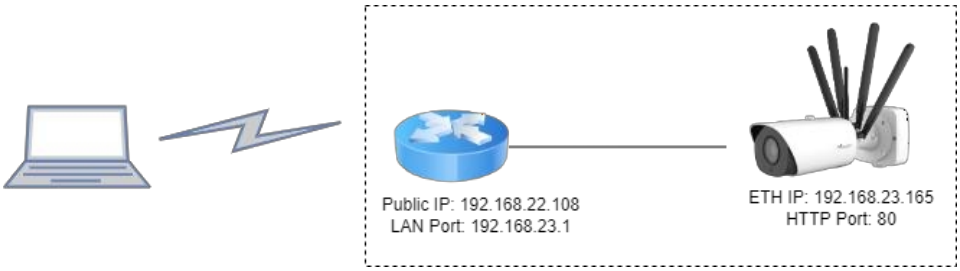
**Verwandtes Thema**

Serieller Port

## 5.5 NAT-Regel konfigurieren

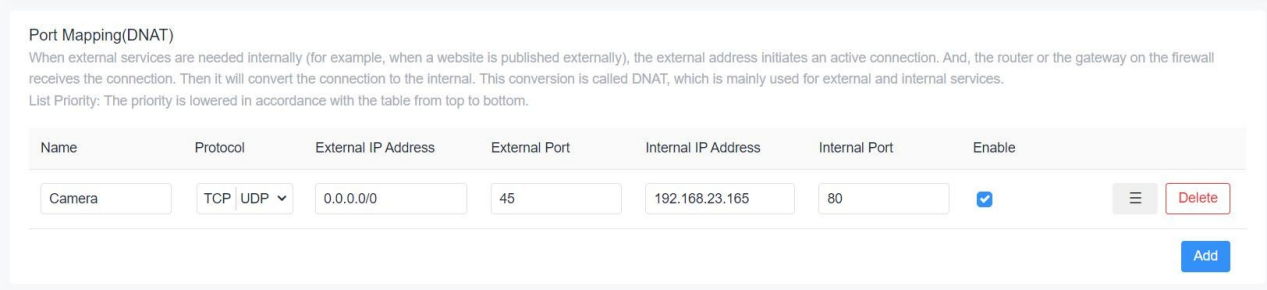
**Beispiel**

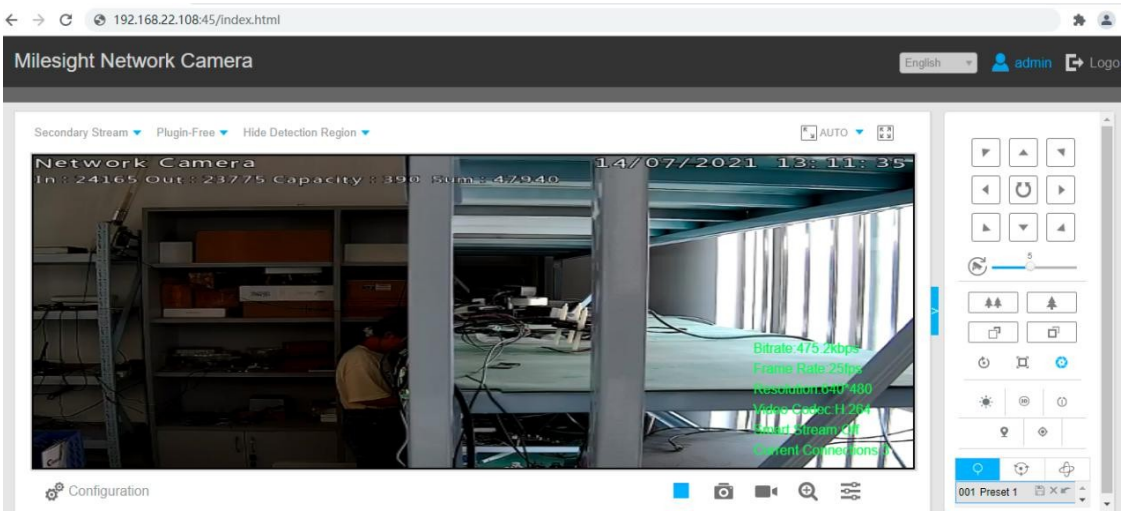
Ein UR75-Router kann über Mobilfunk auf das Internet zugreifen und eine öffentliche IP-Adresse erhalten. Der LAN-Port ist mit einer IP-Kamera verbunden, deren IP-Adresse 192.168.23.165 lautet und deren HTTP-Port 80 ist. Auf diese IP-Kamera kann über die folgenden Port-Mapping-Einstellungen mit der öffentlichen IP-Adresse zugegriffen werden.




**Konfigurationsschritte**

Gehen Sie zu **Netzwerk > Firewall > Portzuordnung** und konfigurieren Sie die Portzuordnungsparameter wie unten angegeben. Die externe IP-Adresse 0.0.0.0/0 bedeutet, dass alle externen Adressen Zugriff haben. Danach können Benutzer die öffentliche IP-Adresse: externen Port verwenden, um auf die IP-Kamera zuzugreifen.




**Verwandtes Thema**

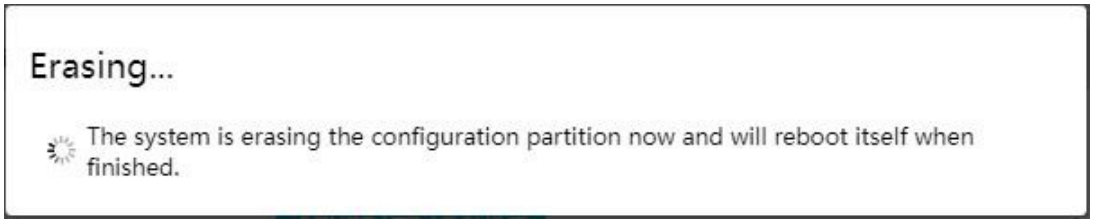
Portzuordnung

## 5.7 Werkseinstellungen wiederherstellen

**Methode 1:**

Gehen Sie zur Seite **„System > Wartung > Sicherung/Upgrade“**, klicken Sie auf die Schaltfläche **„Zurücksetzen“** und bestätigen Sie, dass Sie das Gerät auf die Werkseinstellungen zurücksetzen möchten. Klicken Sie anschließend auf die Schaltfläche **„OK“**.


Das Gerät wird dann neu gestartet und sofort auf die Werkseinstellungen zurückgesetzt.



Bitte warten Sie, bis die SYSTEM-LED grün leuchtet. Dies bedeutet, dass das Gerät erfolgreich auf die Werkseinstellungen zurückgesetzt wurde.

**Verwandtes Thema**

Sicherung/Flash-Firmware

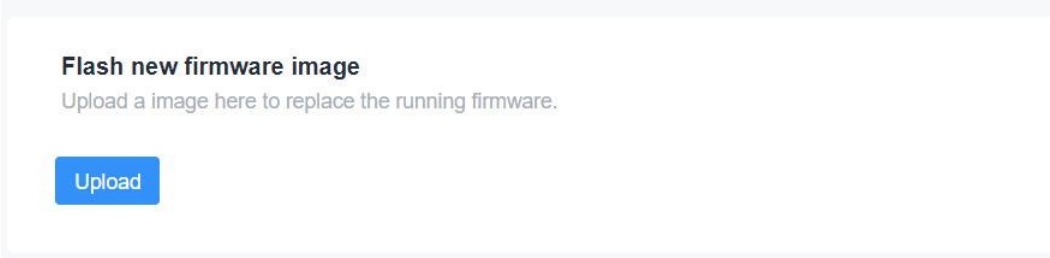
**Methode 2:**

Suchen Sie die Reset-Taste am Router, drücken Sie sie und halten Sie sie länger als 5 Sekunden gedrückt, bis die LED blinkt.

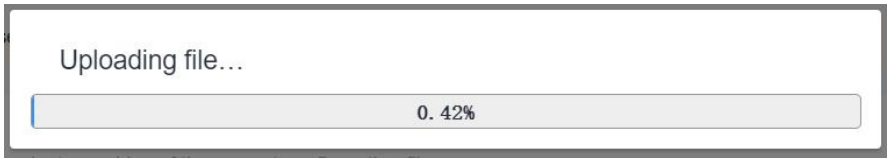
## 5.8 Firmware-Upgrade

Es wird empfohlen, vor dem Upgrade des Geräts zunächst den technischen Support von Milesight zu kontaktieren. Nachdem Sie die Bilddatei erhalten haben, führen Sie bitte die folgenden Schritte aus, um das Upgrade abzuschließen.

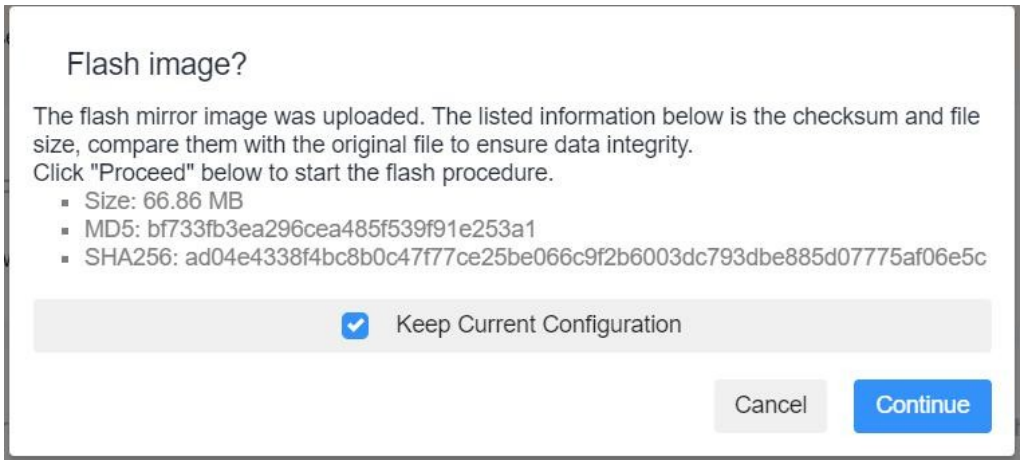
1. Gehen Sie zur Seite **„System > Wartung > Sicherung/Aktualisierung“** und klicken Sie auf **„Hochladen“.**




2. Suchen Sie die richtige Firmware-Datei auf dem PC, klicken Sie auf **„Hochladen“** und das Gerät überprüft, ob die Firmware-Datei korrekt ist. Wenn sie korrekt ist, wird die Firmware auf das Gerät importiert.


3. Klicken Sie nach dem Hochladen **auf „Weiter“**, um das Gerät zu aktualisieren. Wenn die SYS-LED von orange auf grün wechselt und statisch leuchtet, ist die Aktualisierung abgeschlossen. Führen Sie während der Aktualisierung keine Vorgänge durch und trennen Sie das Gerät nicht vom Stromnetz.





**Verwandtes Thema**

Sichern/Flashen der Firmware

# Kapitel 6 Webkonfiguration

## 6.1 Status

### 6.1.1 Übersicht

Die Registerkarte „System“ enthält die grundlegenden Informationen zum Router auf dieser Seite.

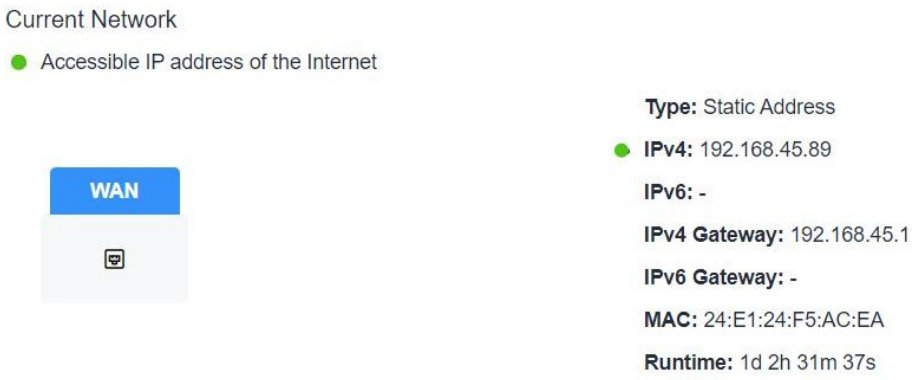
System

| | |
|---|---|
| Hostname | Router |
| Model | UR75-L00E-W2 |
| SN | 6019C3023310 |
| Firmware Version | 78.0.0.3-r1 |
| Hardware Version | V1.1 |
| Local Time | 2030-02-03 04:18:01 |
| Uptime | 1d 19h 27m 27s |

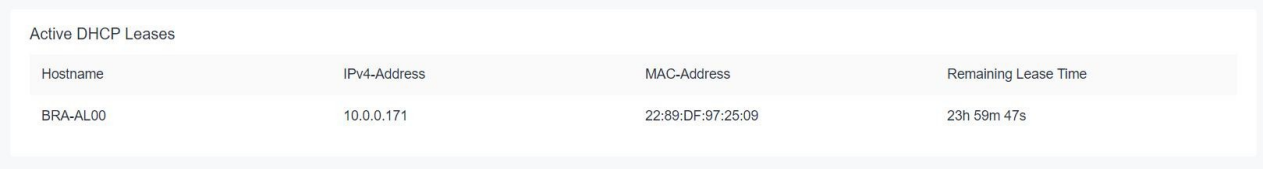
| System | |
|---|---|
| **Artikel** | **Beschreibung** |
| Hostname | Der Hostname des Geräts kann unter **„System > Verwaltung > Systemeinstellungen geändert werden.** |
| Modell | Der Modellname des Geräts. |
| SN | Die Seriennummer des Geräts. |
| Firmware-Version | Die aktuelle Firmware-Version des Geräts. |
| Hardware-Version | Die aktuelle Hardwareversion des Geräts. |
| Lokale Zeit | Die aktuelle Systemzeit des Geräts kann unter **System > Verwaltung > Systemeinstellungen geändert werden.** |
| Betriebszeit | Die Zeit, seitdem das Gerät eingeschaltet ist und läuft. |


| Hardware | |
|---|---|
| **Element** | **Beschreibung** |
| CPU-Temperatur | Die Temperatur der CPU. |
| Durchschnittliche Auslastung | Durchschnittswerte über zunehmend längere Zeiträume (1, 5 und 15 Minuten), je kleiner die Zahlen, desto besser. |
| RAM | Die RAM-Kapazität und der verfügbare RAM-Speicher. |
| Flash | Die Flash-Kapazität und der verfügbare Flash-Speicher. |

Die Registerkarte **„Aktuelles Netzwerk“** zeigt die grundlegenden Informationen zur verwendeten Verbindung an. Klicken Sie für weitere Details auf das Kapitel „Schnittstelle“.




Die Registerkarte „Aktive DHCP-Leases“ zeigt die grundlegenden Informationen der verbundenen Geräte an.


Active DHCP Leases

| Hostname | IPv4-Address | MAC-Address | Remaining Lease Time |
|---|---|---|---|
| BRA-AL00 | 10.0.0.171 | 22:89:DF:97:25:09 | 23h 59m 47s |

| Aktive DHCP-Leases | |
|---|---|
| **Element** | **Beschreibung** |
| Hostname | Der Hostname des verbundenen Geräts. |
| IPv4-Adresse | Die IPv4-Adresse des verbundenen Geräts. |
| MAC-Adresse | Die MAC-Adresse des verbundenen Geräts. |
| Verbleibende Leasingdauer Zeit | Die verbleibende Zeit für diese Lease. |

Wenn Milesight UPS mit dem Gerät verbunden ist, werden die grundlegenden Informationen zur USV ebenfalls auf der Statusseite angezeigt. Weitere Informationen finden Sie im *Milesight UPS-Benutzerhandbuch*.


UPS

| | |
|---|---|
| Model | - |
| SN | - |
| Firmware Version | - |
| Hardware Version | - |
| Power Status | Disconnected_ups |
| Battery | - |
| Battery Temperature | - |

### 6.1.2 Mobilfunk

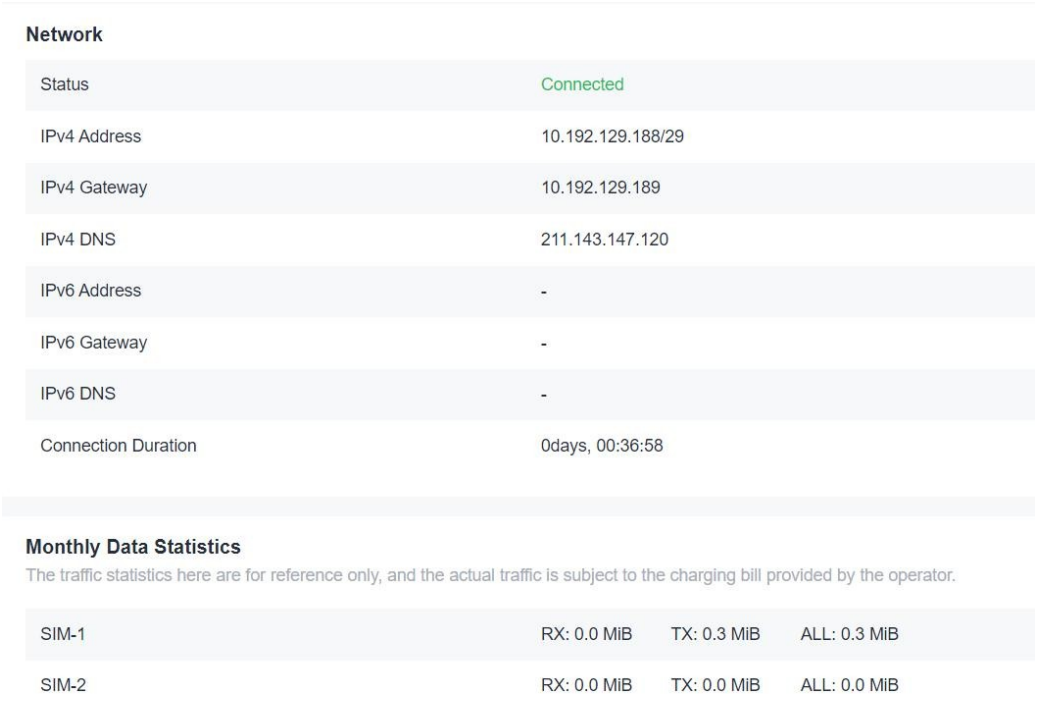
Auf dieser Seite können Sie den Mobilfunknetzstatus des Routers anzeigen.

**Cellular Status**

| | |
|---|---|
| SIM Status | Ready |
| Module Model | RG500L-EU |
| Version | RG500LEUACR04A01M8G_OCPU_20.001.20.001 |
| Current SIM | SIM1 |
| Cellular Band | N41 |
| Signal Strength | -72dBm |
| Register Status | Registered(Home network) |
| IMEI | 869263050069693 |
| IMSI | 460005970144201 |
| ICCID | 898600511318F2001680 |
| ISP | CHINA MOBILE |
| Network Type | 5G SA |
| PLMN ID | 46000 |
| LAC | 3259E7 |
| Cell ID | 203959107 |
| CQI | - |
| DL Bandwidth | 100MHz |
| UL Bandwidth | 100MHz |
| SINR | 26dB |
| PCI | 23F |
| RSRP | -71dBm |
| RSRQ | -11dB |
| EARFCN | 7B49E |

| Modem-Informationen | |
|---|---|
| **Element** | **Beschreibung** |
| Status | Entsprechender Erkennungsstatus von Modul und SIM-Karte.<br>● Keine SIM-Karte: Die SIM-Karte ist nicht eingelegt.<br>● PIN-Fehler: Der PIN-Code ist fehlerhaft<br>● PIN erforderlich: Für die SIM-Karte muss ein PIN-Code eingegeben werden<br>● PUK erforderlich: Die SIM-Karte muss mit dem PUK-Code entsperrt werden<br>● Kein Signal: kein Mobilfunksignal<br>● Bereit: Die SIM-Karte ist eingelegt |

| | |
|---|---|
| | ● Aus: Die SIM-Karte ist deaktiviert oder das Datenvolumen ist überschritten |
| Modulmodell | Der Modellname des Mobilfunkmoduls. |
| Version | Die Firmware-Version des Mobilfunkmoduls. |
| Aktuelle SIM | Die aktuell verwendete SIM-Karte. |
| Mobilfunkband | Das Mobilfunkband, über das sich der Router beim Netzwerk angemeldet hat. |
| Signalstärke | Der RSSI-Wert (Received Signal Indicator) des registrierten Mobilfunknetzes. |
| Registrierungsstatus | Der Registrierungsstatus der SIM-Karte. |
| IMEI | Die IMEI des Mobilfunkmoduls. |
| IMSI | Die IMSI der SIM-Karte. |
| ICCID | Die ICCID der SIM-Karte. |
| ISP | Der Netzbetreiber, bei dem die SIM-Karte registriert ist. |
| Netzwerktyp | Der verbundene Netzwerktyp, z. B. LTE, 3G usw. |
| PLMN-ID | Die aktuelle PLMN-ID, einschließlich MCC,MNC,LAC und Cell ID. |
| LAC | Der Standortbereichscode der SIM-Karte. |
| Cell-ID | Die Zell-ID des Standorts der SIM-Karte. |
| CQI | Der Kanalqualitätsindikator des Mobilfunknetzes. |
| DL-Bandbreite | Die DL-Bandbreite des Mobilfunknetzes. |
| UL-Bandbreite | Die UL-Bandbreite des Mobilfunknetzes. |
| SINR | Das Signal-Interferenz-Rausch-Verhältnis des Mobilfunknetzes. |
| PCI | Die physikalische Zellenkennung des Mobilfunknetzes. |
| RSRP | Die Referenzsignalempfangsleistung des Mobilfunknetzes. |
| RSRQ | Die Referenzempfangsqualität des Mobilfunknetzes. |
| EARFCN | Die absolute Funkkanalnummer von E-UTRA. |

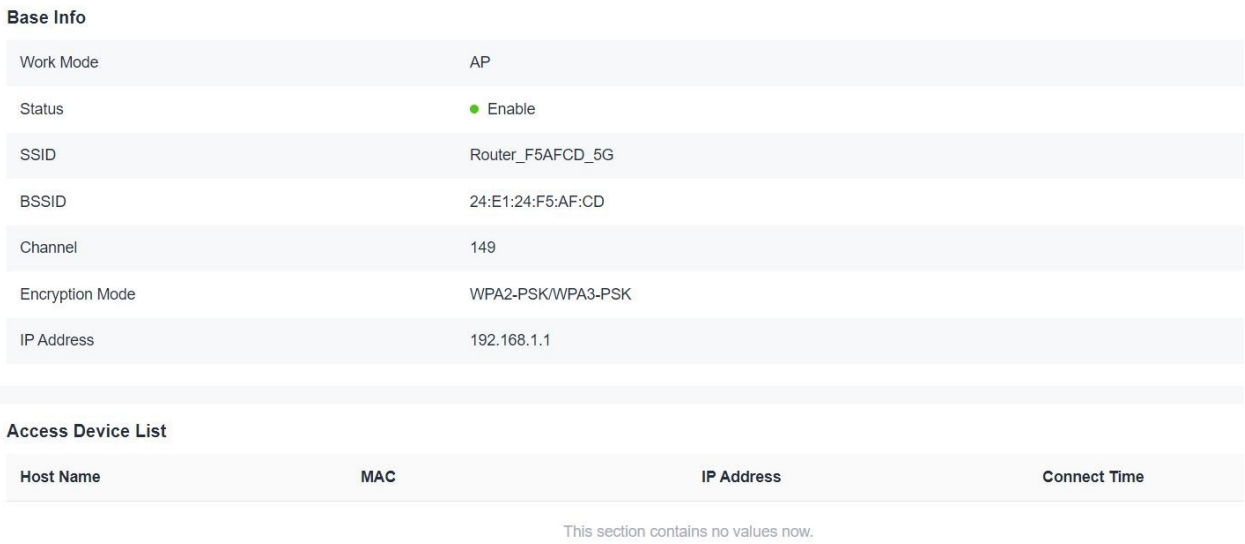



**Netzwerk**

| Element | Beschreibung |
|---|---|
| Status | Der Verbindungsstatus des Mobilfunknetzes. |
| IPv4/IPv6-Adresse | Die IPv4/IPv6-Adresse und Netzmaske des Mobilfunknetzes. |
| IPv4/IPv6-Gateway | Das IPv4/IPv6-Gateway und die Netzmaske des Mobilfunknetzes. |
| IPv4/IPv6-DNS | Der DNS-Server des Mobilfunknetzes. |
| Verbindungsdauer | Die Information darüber, wie lange das Mobilfunknetz verbunden war verbunden ist. |
| RX | Das Datenvolumen und die empfangenen Pakete dieses Monats. |
| TX | Das Datenvolumen und die übertragenen Pakete dieses Monats. |
| ALL | Gesamtdatenvolumen und Pakete dieses Monats. |

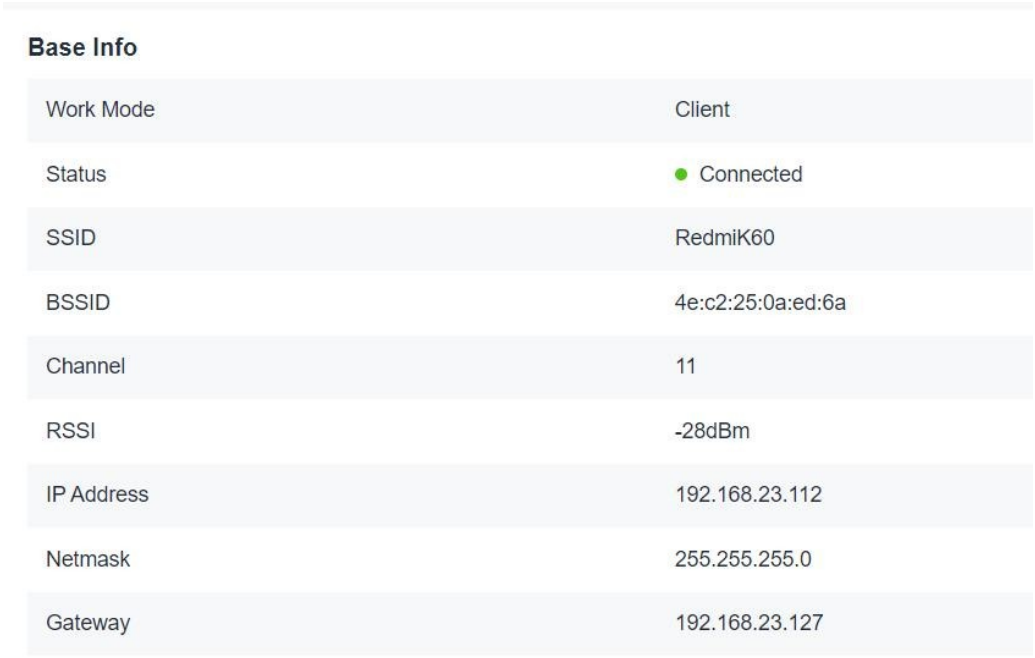
### 6.1.3 WLAN

Auf dieser Seite können Sie den WLAN-Status überprüfen, einschließlich der Informationen zum Zugangspunkt und zum Client.




| WLAN-Status – AP-Modus | |
|---|---|
| **Element** | **Beschreibung** |
| **Grundlegende Informationen** | |
| Arbeitsmodus | Zeigt den Arbeitsmodus dieser WLAN-Schnittstelle an. |
| Status | Zeigt den Aktivierungsstatus dieser WLAN-Schnittstelle an. |
| Typ | Zeigt den Typ der WLAN-Schnittstelle an. |
| SSID | Zeigt die SSID dieses Geräts an. |
| Kanal | Zeigen Sie den verwendeten Kanal dieser WLAN-Schnittstelle an. |
| Verschlüsselungsmodus | Zeigt den Verschlüsselungsmodus dieser WLAN-Schnittstelle an. |
| IP-Adresse | Zeigt die IP-Adresse dieses Geräts an. |
| **Liste der zugehörigen Geräte** | |
| Hostname | Zeigt den Hostnamen des Clients an, der mit diesem Gerät verbunden ist. |
| MAC-Adresse | Zeigen Sie die MAC-Adresse des Clients an, der mit diesem Gerät verbunden hat. |
| IP-Adresse | Zeigt die IP-Adresse des Clients an, der mit diesem Gerät verbunden ist. |
| Verbindungszeit | Zeigen Sie die Verbindungsdauer zwischen dem Client-Gerät und diesem |

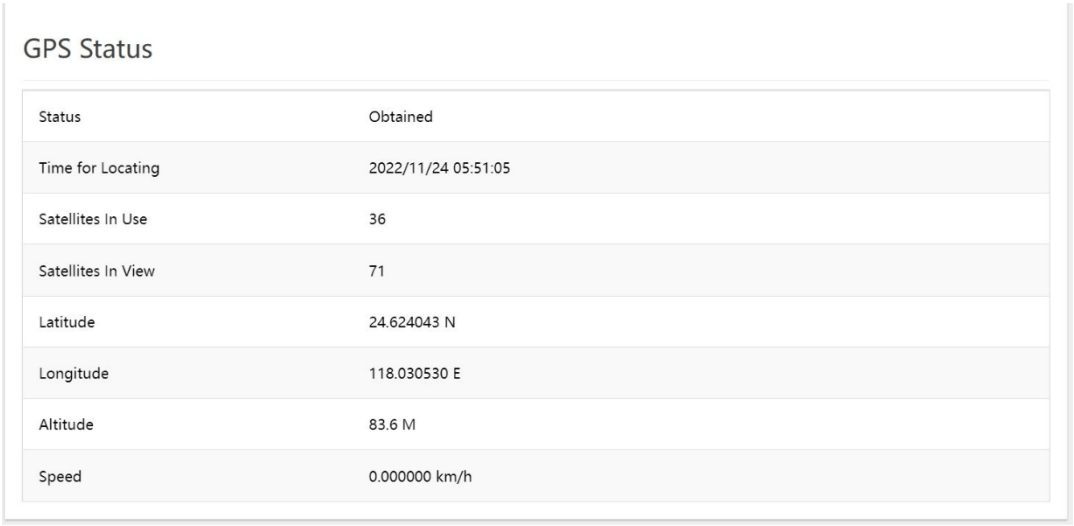
| | |
|---|---|
| | Gerät an. |




| WLAN-Status – Client-Modus | |
|---|---|
| **Element** | **Beschreibung** |
| **Grundlegende Informationen** | |
| Arbeitsmodus | Zeigt den Arbeitsmodus dieser WLAN-Schnittstelle an. |
| Status | Zeigt den Verbindungsstatus mit dem WLAN-Zugangspunkt an. |
| SSID | Zeigt die SSID des AP an, mit dem das Gerät verbunden ist. |
| BSSID | Zeigt die MAC-Adresse des AP an, mit dem das Gerät verbunden ist. |
| Kanal | Zeigt den verwendeten Kanal dieser WLAN-Schnittstelle an. |
| RSSI | Zeigt das Signal dieser WLAN-Schnittstelle an. |
| IP | Zeigen Sie die IP-Adresse dieses Geräts an, die vom WLAN-AP zugewiesen wurde. |
| Netzmaske | Zeigt die vom WLAN-AP zugewiesene Netzmaske dieses Geräts an. |
| Gateway | Zeigt die IP-Adresse des WLAN-AP an. |

### 6.1.4 GPS

Wenn die GPS-Funktion aktiviert ist und die GPS-Informationen erfolgreich abgerufen wurden, können Sie auf dieser Seite die aktuellen GPS-Informationen einschließlich GPS-Zeit, Breitengrad, Längengrad und Geschwindigkeit anzeigen.



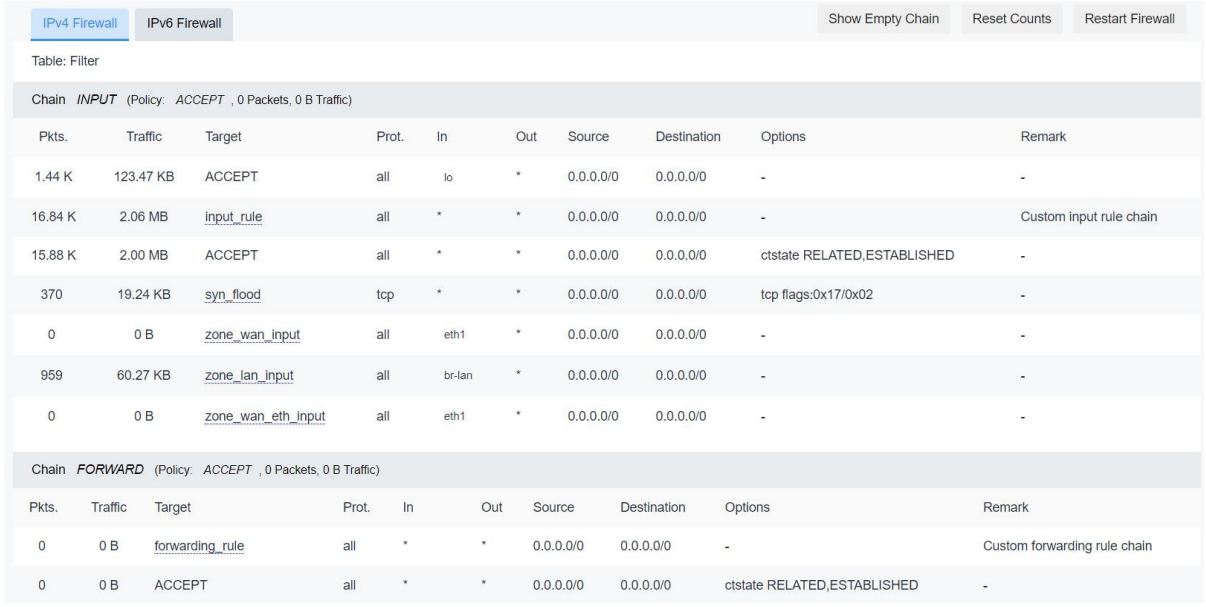
GPS Status

| | |
|---|---|
| Status | Obtained |
| Time for Locating | 2022/11/24 05:51:05 |
| Satellites In Use | 36 |
| Satellites In View | 71 |
| Latitude | 24.624043 N |
| Longitude | 118.030530 E |
| Altitude | 83.6 M |
| Speed | 0.000000 km/h |

| GPS-Status | |
|---|---|
| **Element** | **Beschreibung** |
| Status | Der Status der GPS-Erfassung. |
| Zeit für die Ortung | Die Zeit für die Ortung. |
| Verwendete Satelliten | Die Anzahl der eingesetzten Satelliten. |
| Sichtbare Satelliten | Die Anzahl der sichtbaren Satelliten. |
| Breitengrad | Der Breitengrad des Standorts. |
| Längengrad | Der Längengrad des Standorts. |
| Höhe | Die Höhe des Standorts. |
| Geschwindigkeit | Die Bewegungsgeschwindigkeit. |

### 6.1.5 Firewall

Auf dieser Seite können Sie alle IPv4/IPv6-Ketten von iptables überprüfen. Benutzer können auf die Ziele mit gestrichelten Linien klicken, um zu den entsprechenden Ketten zu springen.



IPv4 Firewall | IPv6 Firewall — Show Empty Chain | Reset Counts | Restart Firewall

Table: Filter

Chain *INPUT* (Policy: *ACCEPT*, 0 Packets, 0 B Traffic)

| Pkts. | Traffic | Target | Prot. | In | Out | Source | Destination | Options | Remark |
|---|---|---|---|---|---|---|---|---|---|
| 1.44 K | 123.47 KB | ACCEPT | all | lo | * | 0.0.0.0/0 | 0.0.0.0/0 | - | - |
| 16.84 K | 2.06 MB | input_rule | all | * | * | 0.0.0.0/0 | 0.0.0.0/0 | - | Custom input rule chain |
| 15.88 K | 2.00 MB | ACCEPT | all | * | * | 0.0.0.0/0 | 0.0.0.0/0 | ctstate RELATED,ESTABLISHED | - |
| 370 | 19.24 KB | syn_flood | tcp | * | * | 0.0.0.0/0 | 0.0.0.0/0 | tcp flags:0x17/0x02 | - |
| 0 | 0 B | zone_wan_input | all | eth1 | * | 0.0.0.0/0 | 0.0.0.0/0 | - | - |
| 959 | 60.27 KB | zone_lan_input | all | br-lan | * | 0.0.0.0/0 | 0.0.0.0/0 | - | - |
| 0 | 0 B | zone_wan_eth_input | all | eth1 | * | 0.0.0.0/0 | 0.0.0.0/0 | - | - |

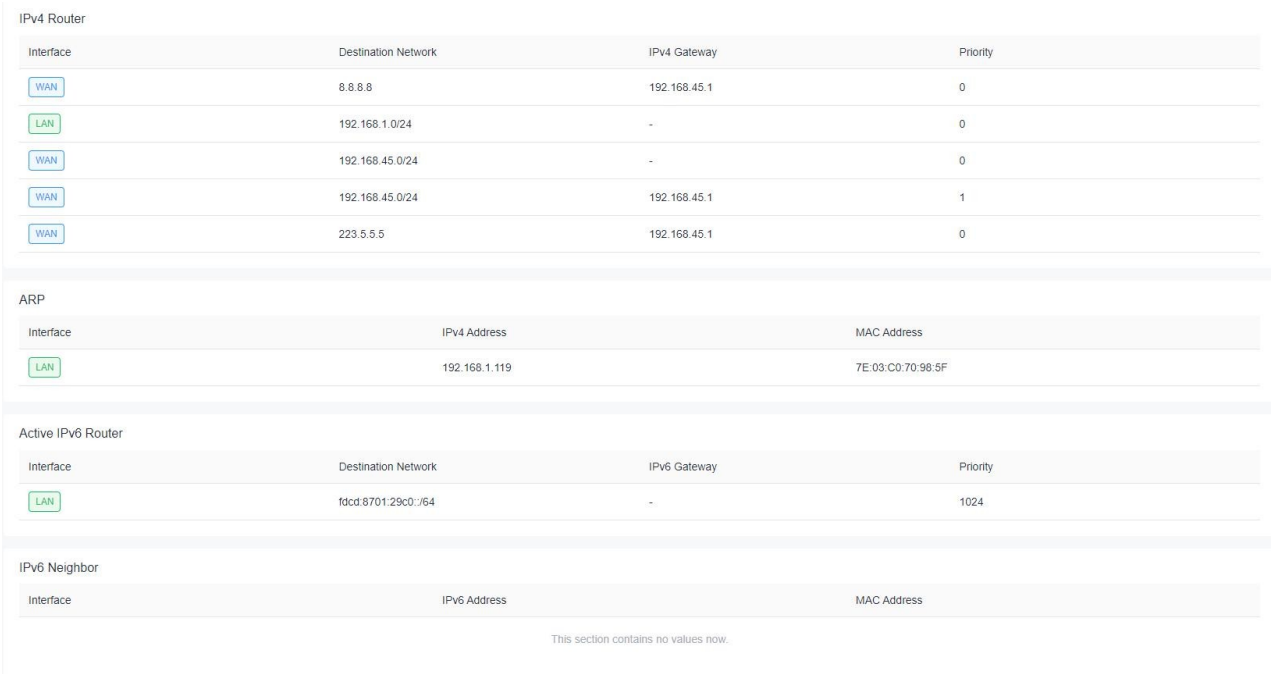
Chain *FORWARD* (Policy: *ACCEPT*, 0 Packets, 0 B Traffic)

| Pkts. | Traffic | Target | Prot. | In | Out | Source | Destination | Options | Remark |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 B | forwarding_rule | all | * | * | 0.0.0.0/0 | 0.0.0.0/0 | - | Custom forwarding rule chain |
| 0 | 0 B | ACCEPT | all | * | * | 0.0.0.0/0 | 0.0.0.0/0 | ctstate RELATED,ESTABLISHED | - |

| Firewall-Status | |
|---|---|
| **Element** | **Beschreibung** |
| Tabelle: Filter | Die Standardtabelle für die Verarbeitung von Netzwerkpaketen. |
| Tabelle: NAT | Wird verwendet, um Pakete zu ändern, die eine neue Verbindung herstellen, und<br>für die Netzwerkadressübersetzung (NAT) verwendet. |
| Tabelle: Mangle | Wird für bestimmte Arten der Paketänderung verwendet. |
| Leere Kette anzeigen/ausblenden | Zeigt/verbirgt die Kette ohne Regeln. |
| Zähler zurücksetzen | Setzt die Verkehrszählungen aller Ketten zurück. |
| Firewall neu starten | Den gesamten Firewall-Prozess neu starten. |

### 6.1.6 Routing-Tabelle

Auf dieser Seite können Sie den Routing-Status überprüfen, einschließlich der Routing-Tabelle und des ARP-Caches.

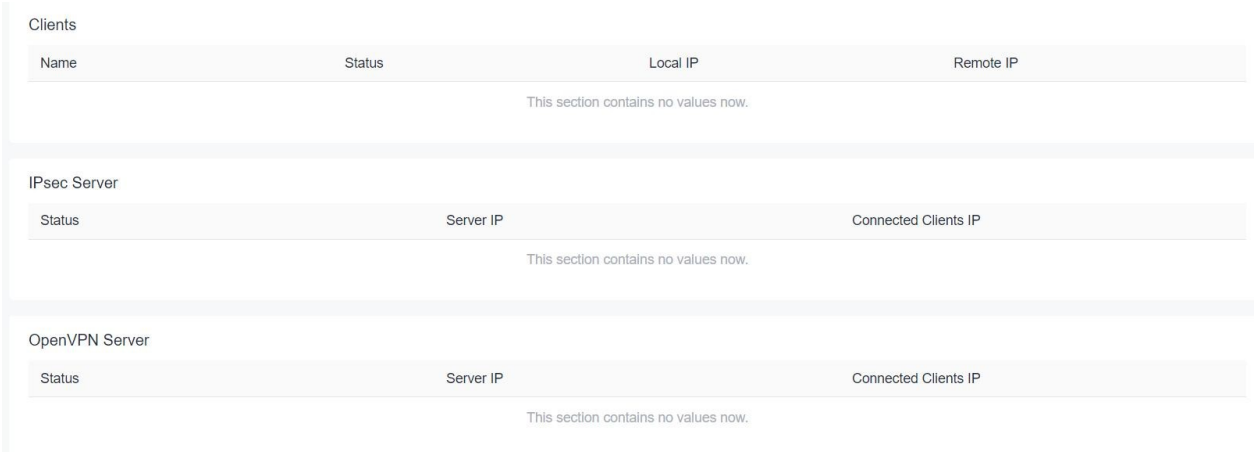



| Artikel | Beschreibung |
|---|---|
| **Aktiver IPv4/IPv6-Router** | |
| Schnittstelle | Die ausgehende Schnittstelle der Route. |
| Ziel Netzwerk | Die IP-Adresse und Netzmaske des Zielhosts oder des Zielnetzwerks Netzwerks. |
| IPv4/IPv6 Gateway | Die IP-Adresse des Gateways, von dem aus Pakete gesendet werden sollen. |
| Priorität | Die Metriknummer, die die Priorität der Schnittstelle angibt. |
| **ARP-Cache** | |
| Schnittstelle | Die Bindungsschnittstelle von ARP. |
| IPv4-Adresse | Die IP-Adresse des ARP-Pools. |
| MAC-Adresse | Die der IP-Adresse zugeordnete MAC-Adresse. |

| IPv6-Nachbar | |
|---|---|
| Schnittstelle | Die Bindungsschnittstelle des Nachbarn. |
| IPv6-Adresse | Die IP-Adresse des Nachbarn. |
| MAC-Adresse | Die der IP-Adresse entsprechende MAC-Adresse. |

### 6.1.7 VPN

Auf dieser Seite können Sie den VPN-Status überprüfen.

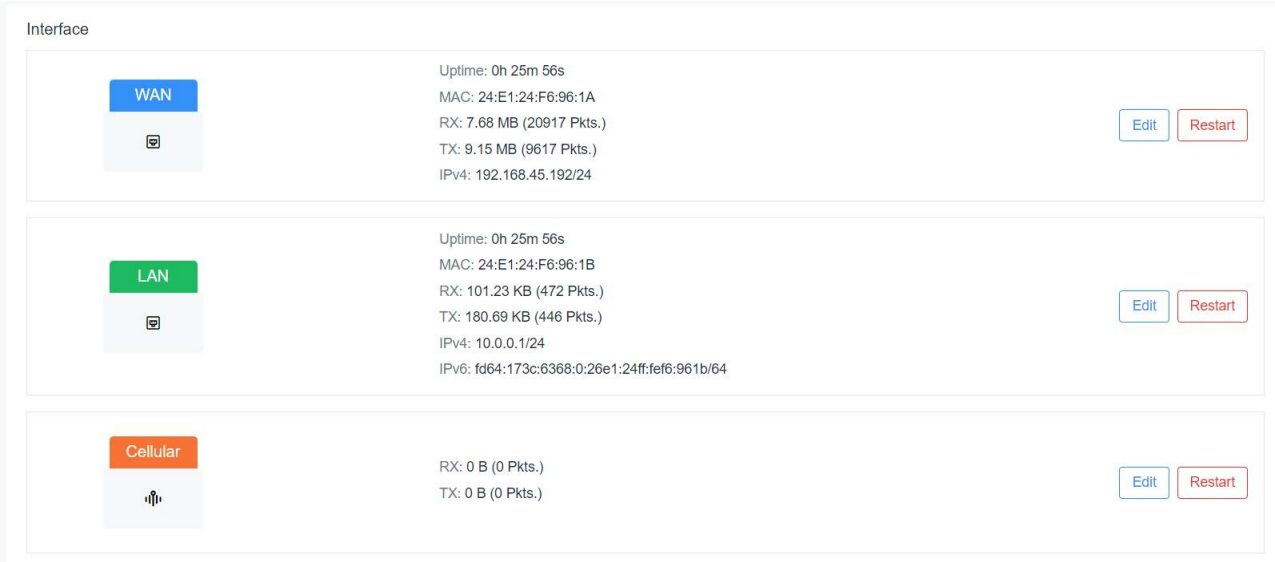



| VPN-Status | |
|---|---|
| **Element** | **Beschreibung** |
| **Clients** | |
| Name | Der Name der aktivierten VPN-Clients. |
| Status | Der Verbindungsstatus des Clients. |
| Lokale IP | Die lokale IP-Adresse und das Subnetz des VPN-Tunnels. |
| Remote-IP | Die tatsächliche Remote-IP-Adresse und das Subnetz des VPN-Tunnels. |
| **IPsec/OpenVPN-Server** | |
| Status | Der Status des Servers. |
| Server-IP | Die Server-IP-Adresse und das Subnetz des VPN-Tunnels. |
| IP-Adresse der verbundenen Clients | Die IP-Adresse des Clients, der mit dem Server verbunden ist. |

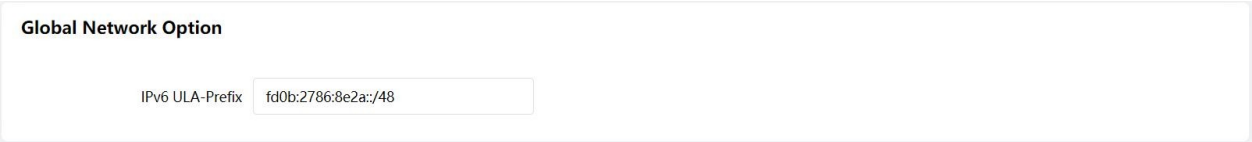
## 6.2 Netzwerk

### 6.2.1 Schnittstellen

In diesem Menü können Sie die Grundeinstellungen für Mobilfunk-, WAN- und LAN-Schnittstellen konfigurieren.




| Schnittstellen | |
|---|---|
| **Element** | **Beschreibung** |
| Neustart | Klicken Sie hier, um diese Netzwerkschnittstelle neu zu starten. |
| Bearbeiten | Klicken Sie hier, um die allgemeinen Einstellungen dieser Netzwerkschnittstelle zu bearbeiten. |

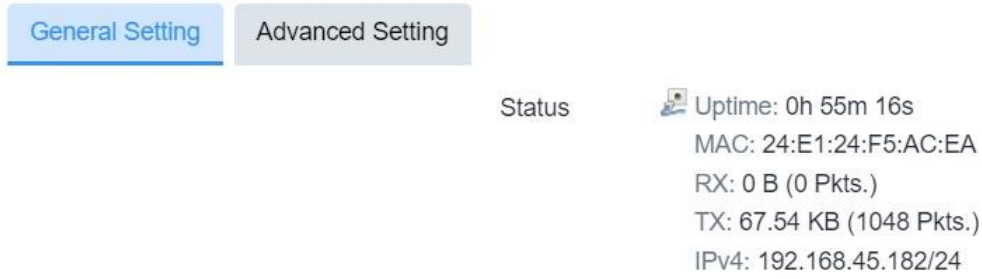



| Globale Netzwerkoptionen | |
|---|---|
| **Element** | **Beschreibung** |
| IPv6-ULA-Präfix | Das IPv6-Präfix für die eindeutige lokale Adresse (ULA) dieses Geräts. |

### 6.2.1.1 WAN

Der WAN-Port kann über ein Ethernet-Kabel mit dem Internet verbunden werden. Er unterstützt drei Verbindungstypen, die sowohl mit IPv4 als auch mit IPv6 funktionieren.

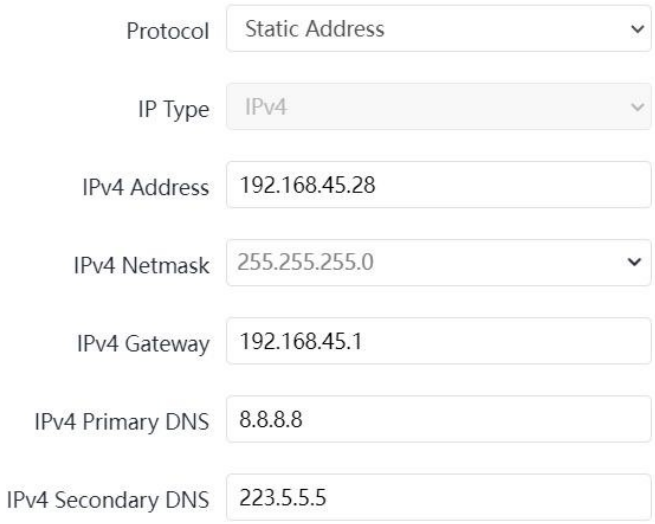
- **Statische IP**: Konfigurieren Sie die IPv4-Adresse, die Netzmaske und das Gateway für die Ethernet-WAN-Schnittstelle.
- **DHCP-Client**: Konfigurieren Sie die Ethernet-WAN-Schnittstelle als DHCP-Client, um automatisch eine IPv4-Adresse zu erhalten.
- **PPPoE**: Konfigurieren Sie die Ethernet-WAN-Schnittstelle als PPPoE- oder PPPoEv6-Client.



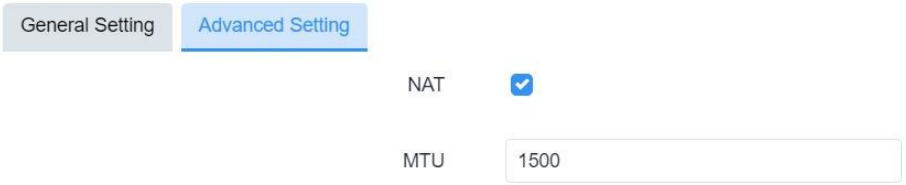
| WAN – Status | |
|---|---|
| **Element** | **Beschreibung** |
| Betriebszeit | Wie lange ist das Gerät bereits in Betrieb? |
| MAC | MAC-Adresse der WAN-Schnittstelle. |
| RX | RX: Das Datenvolumen und die Pakete, die über diese Schnittstelle empfangen wurden. |
| TX | TX: Das Datenvolumen und die Pakete, die von dieser Schnittstelle übertragen wurden. |
| IPv4 | IPv4-Adresse der WAN-Schnittstelle. |

### 1. Statische IP-Konfiguration

Wenn das externe Netzwerk der WAN-Schnittstelle eine feste IP-Adresse zuweist, wählen Sie bitte diesen Modus.




| Statische Adresse – Allgemeine Einstellungen | | |
|---|---|---|
| **Element** | **Beschreibung** | **Standard** |
| IP-Typ | Ist fest auf IPv4 eingestellt. | IPv4 |
| IPv4-Adresse | Legen Sie die IPv4-Adresse des WAN-Ports fest. | -- |
| IPv4-Netzmaske | Legen Sie die Netzmaske für den WAN-Port fest. | 255.255.255.0 |
| IPv4-Gateway | Legen Sie das Gateway für die IPv4-Adresse des WAN-Ports fest. | -- |
| Primärer IPv4-DNS | Legen Sie den primären IPv4-DNS-Server fest. | 8.8.8.8 |
| Sekundärer IPv4 DNS | Legen Sie den sekundären IPv4-DNS-Server fest. | 223.5.5.5 |

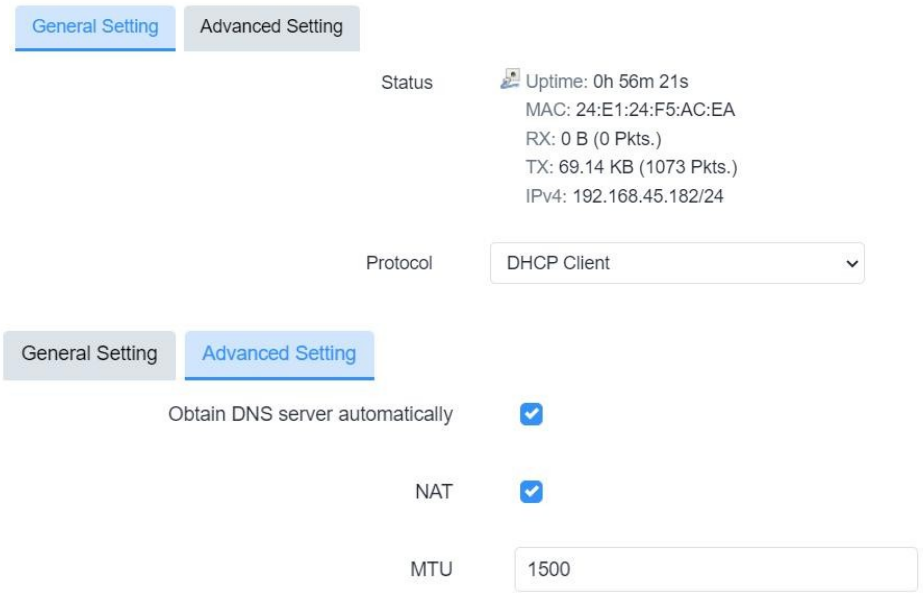



| Statische Adresse – Erweiterte Einstellungen | |
|---|---|
| **Element** | **Beschreibung** |

| | |
|---|---|
| NAT | Aktivieren oder deaktivieren Sie die NAT-Funktion. Wenn diese Funktion aktiviert ist, kann eine private IP-Adresse in eine öffentliche IP übersetzt werden. |
| MTU | Legen Sie die maximale Übertragungseinheit fest. Bereich: 68-1500. |

## 2. DHCP-Client

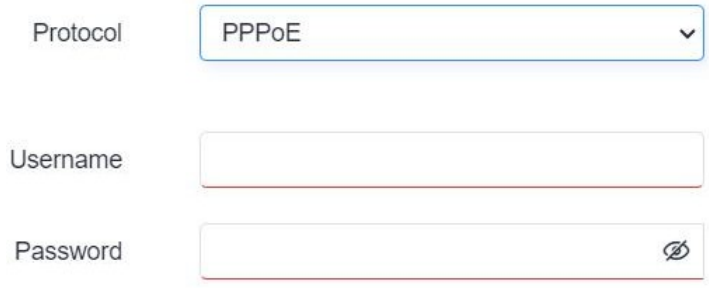
Wenn im externen Netzwerk ein DHCP-Server aktiviert ist und der Ethernet-WAN-Schnittstelle IP-Adressen zugewiesen wurden, wählen Sie diesen Modus, um die IP-Adresse automatisch zu beziehen.



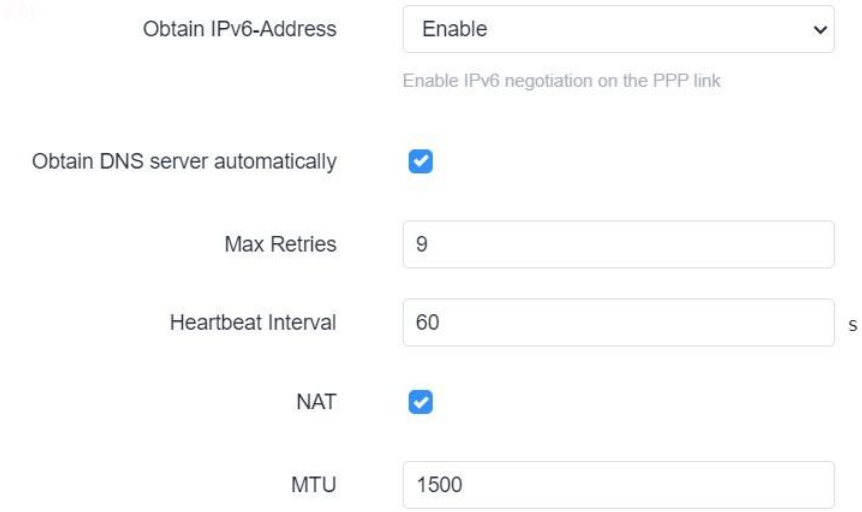

| DHCP-Client – Erweiterte Einstellungen | |
|---|---|
| **Element** | **Beschreibung** |
| DNS-Server abrufen automatisch | Peer-DNS automatisch beziehen. DNS ist erforderlich, wenn Sie eine Domänenname. |
| NAT | Aktivieren oder deaktivieren Sie die NAT-Funktion. Wenn sie aktiviert ist, kann eine private IP-Adresse in eine öffentliche IP übersetzt werden. |
| MTU | Legen Sie die maximale Übertragungseinheit fest. Bereich: 68-1500. |

## 3. PPPoE/PPPoEv6

PPPoE bezieht sich auf ein Punkt-zu-Punkt-Protokoll über Ethernet. Wenn die IPv6-Aushandlung aktiviert ist, kann der Router sowohl IPv4- als auch IPv6-Adressen erhalten.



| PPPoE – Allgemeine Einstellungen | |
|---|---|
| **Element** | **Beschreibung** |
| PAP/CHAP-Benutzername | Geben Sie den von Ihrem Internetdienstanbieter (ISP) bereitgestellten Benutzernamen ein. |
| PAP/CHAP-Passwort | Geben Sie das von Ihrem Internetdienstanbieter (ISP) bereitgestellte Passwort ein. |

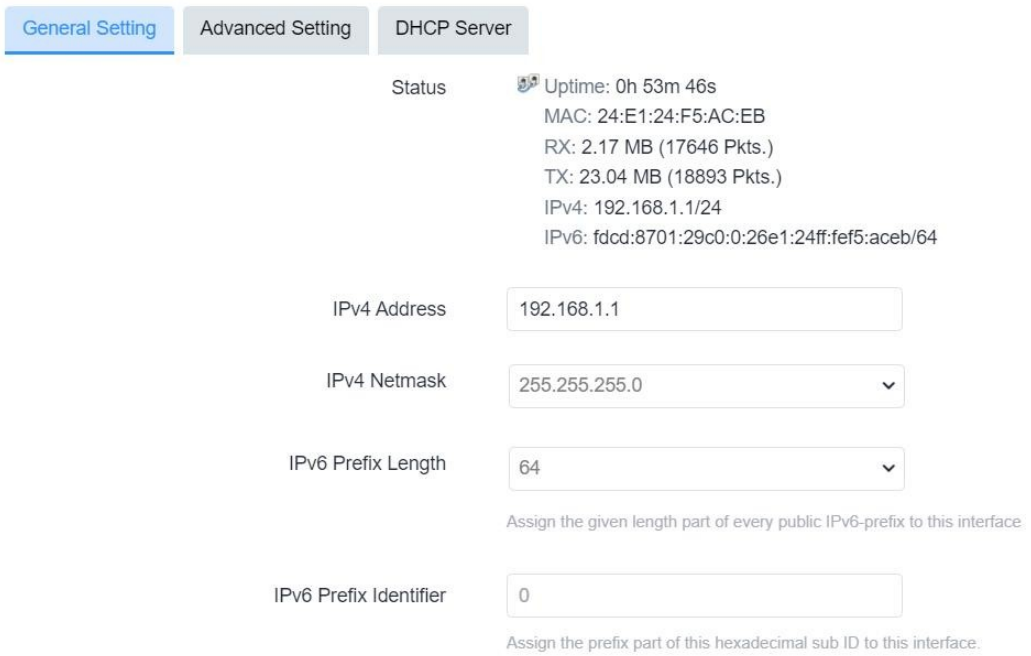



| PPPoE – Erweiterte Einstellungen | |
|---|---|
| **Element** | **Beschreibung** |
| IPv6-Adresse beziehen | Aktivieren Sie die IPv6-Aushandlung auf der PPP-Verbindung. |
| DNS-Server abrufen automatisch | Peer-DNS automatisch während des PPP-Wählvorgangs abrufen. DNS ist erforderlich beim Aufrufen von Domainnamen. |
| Maximale Wiederholungsversuche | Legen Sie die maximale Anzahl der Wiederholungsversuche nach einem fehlgeschlagenen Verbindungsaufbau fest. Bereich: 0-9. |
| Heartbeat-Intervall (s) | Legen Sie das Heartbeat-Intervall für die Verbindungserkennung fest. Bereich: 1-600. |
| NAT | Aktivieren oder deaktivieren Sie die NAT-Funktion. Wenn diese Funktion aktiviert ist, kann eine private IP-Adresse in eine öffentliche IP übersetzt werden. |
| MTU | Legen Sie die maximale Übertragungseinheit fest. Bereich: 68-1500. |

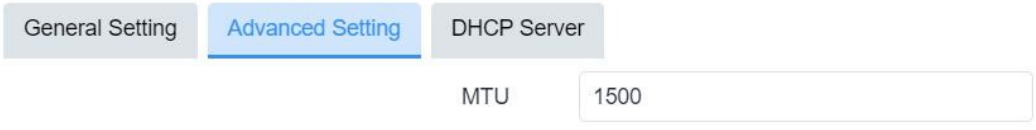
**Beispiel für eine zugehörige Konfiguration**

Ethernet-WAN-Verbindung

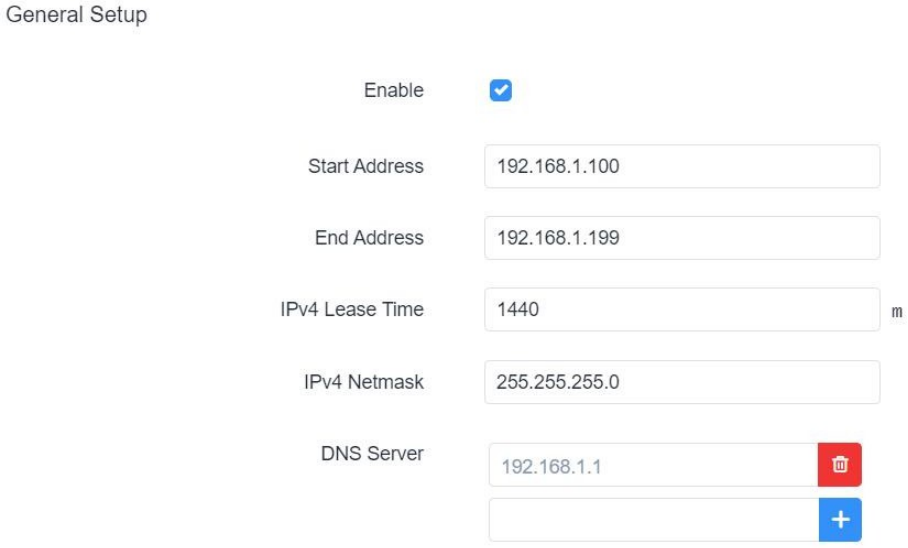
### 6.2.1.2 LAN/DHCP-Server



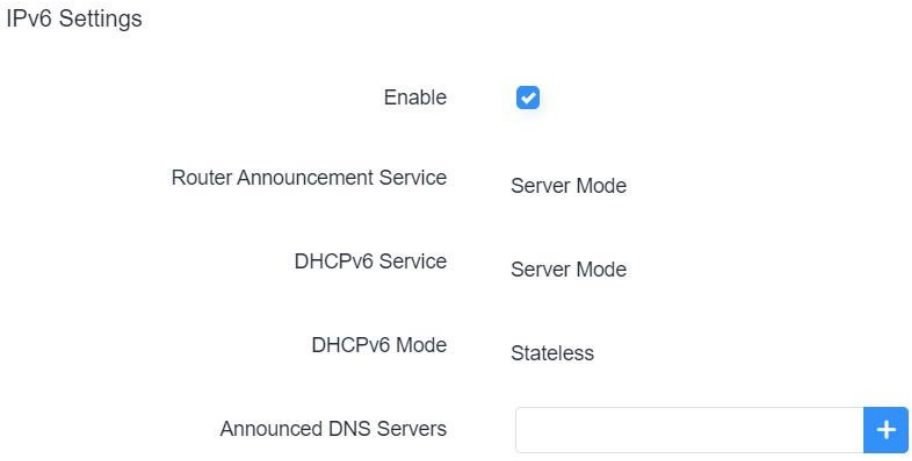

| LAN – Allgemeine Einstellungen | |
|---|---|
| **Element** | **Beschreibung** |
| Status | **Betriebszeit:** Wie lange ist das Gerät bereits in Betrieb? |
| | **MAC:** MAC-Adresse der LAN-Schnittstellen. |
| | **RX:** Das Datenvolumen und die Pakete, die über diese Schnittstelle empfangen wurden. |
| | **TX:** Das Datenvolumen und die Pakete, die von dieser Schnittstelle übertragen wurden. |
| | **IPv4/IPv6:** IPv4/IPv6-Adresse der LAN-Schnittstellen. |
| IPv4-Adresse | Legen Sie die IPv4-Adresse der LAN-Schnittstelle fest. |
| IPv4-Netzmaske | Legen Sie die Netzmaske für die LAN-Schnittstelle fest. |
| IPv6-Präfixlänge | Weisen Sie dieser Schnittstelle einen Teil der angegebenen Länge jedes öffentlichen IPv6-Präfixes zu. |
| IPv6-Präfix Kennung | Weisen Sie dieser Schnittstelle Präfixteile unter Verwendung dieser hexadezimalen Subpräfix-ID zu. |




| LAN – Erweiterte Einstellungen | |
|---|---|
| **Element** | **Beschreibung** |
| MTU | Legen Sie die maximale Übertragungseinheit fest. Bereich: 68-1500. |



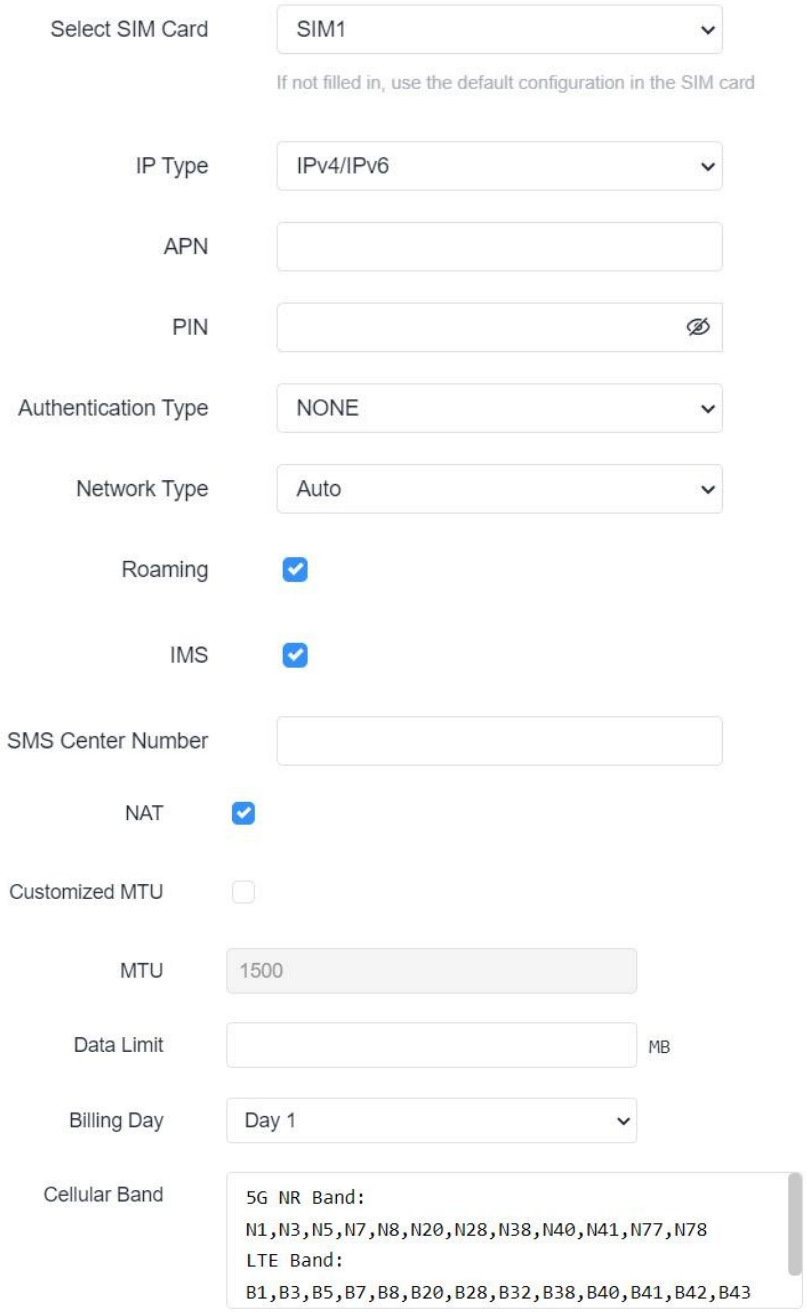

| DHCP-Server – Allgemeine Einrichtung | |
|---|---|
| **Element** | **Beschreibung** |
| Aktivieren | Aktivieren Sie diese Option, um DHCP für diese Schnittstelle zu deaktivieren. |
| Startadresse | Definieren Sie den Anfang des Pools von IP-Adressen, die an DHCP-Clients vergeben werden. |
| Endadresse | Legen Sie das Ende des Pools von IP-Adressen fest, die an DHCP-Clients vermietet werden. |
| IPv4-Lease-Zeit | Legen Sie die Ablaufzeit der vermieteten Adressen fest, das Minimum beträgt 2 Minuten (2m). |
| IPv4-Netzmaske | Legen Sie diese fest, um die an Clients gesendete Netzmaske zu überschreiben. Normalerweise ist sie berechnet aus dem bedienten Subnetz. |
| DNS-Server | Legen Sie die DNS-Serverliste für Clients fest. |




| DHCP-Server-IPv6-Einstellungen | |
|---|---|
| **Element** | **Beschreibung** |
| Aktivieren | Wählen Sie diese Option, um den DHCPv6-Server bei Verwendung von Mobilfunk IPv6 oder PPPoE v6 verwenden. |
| Router-Advertisement-Dienst | Er ist als Servermodus festgelegt. |
| DHCPv6-Dienst | Er ist als Servermodus festgelegt. |

| | |
|---|---|
| DHCPv6-Modus | Er ist als zustandsloser Modus festgelegt. |
| Angekündigte DNS-Server | Legen Sie die DNS-Serverliste für Clients fest. |

### 6.2.1.3 Mobilfunk




| Mobilfunk | |
|---|---|
| **Element** | **Beschreibung** |
| SIM auswählen Karte | Wählen Sie die SIM-Karte aus, für die Sie die Einstellungen konfigurieren möchten. |
| IP-Typ | Zeigen Sie den für diese Schnittstelle zu verwendenden Internetprotokolltyp an.<br>Option: IPv4, IPv6 und IPv4/IPv6. |
| APN | Geben Sie den Zugangspunktnamen für die Mobilfunk-Einwahlverbindung ein, der von |

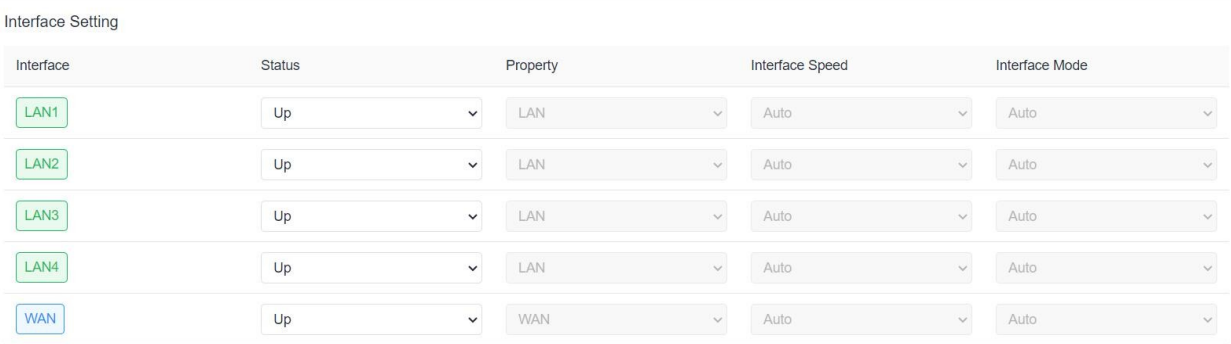
| | |
|---|---|
| | lokalen Internetdienstanbieters bereitgestellt wird. |
| PIN | Geben Sie einen 4-8-stelligen PIN-Code ein, um die SIM-Karte zu entsperren. |
| Authentifizierung Typ | Wählen Sie zwischen KEINE, PAP, CHAP und PAP/CHAP. |
| Netzwerktyp | Wählen Sie zwischen Auto, Nur 5G, Nur 4G und Nur 3G.<br>Auto: Automatische Verbindung zum Netzwerk mit dem stärksten Signal. Nur 5G: Verbindung nur zum 5G-Netzwerk.<br>Und so weiter. |
| Roaming | Roaming aktivieren oder deaktivieren. |
| IMS | IMS-Funktion aktivieren oder deaktivieren. |
| SMS-Zentrale Nummer | Geben Sie die Nummer des lokalen SMS-Centers ein, um SMS-Nachrichten zu speichern, weiterzuleiten, zu konvertieren und<br>Zustellung von SMS-Nachrichten. |
| NAT | Aktivieren oder deaktivieren Sie die NAT-Funktion. |
| Angepasst MTU | Aktivieren oder deaktivieren Sie diese Option, um die maximalen Übertragungseinheiten anzupassen. Wenn<br>deaktiviert, verwendet das Gerät die MTU-Einstellungen des Betreibers. |
| MTU | Legen Sie die maximalen Übertragungseinheiten fest. Bereich: 68-1500. |
| Datenlimit | Legen Sie das Datenlimit für diesen Monat fest. Wenn der Datenverkehr das Limit überschreitet, wird die SIM-Karte<br>in diesem Monat gesperrt. Die Standardeinstellung ist leer (keine Begrenzung). |
| Abrechnungstag | Löschen Sie die monatlichen Datenstatistiken, wenn der Abrechnungstag dieses Monats erreicht ist<br>Monats erreicht ist. |
| Mobilfunkband | Wählen Sie die 5G NR- und 4G LTE-Bänder aus, die zur Registrierung im Mobilfunknetz verwendet werden. Es<br>kann zur Optimierung der Mobilfunkgeschwindigkeit durch Auswahl bestimmter Frequenzbänder verwendet werden. |

**Verwandte Anwendung**

Mobilfunk-Anwendung

### 6.2.1.4 Schnittstelleneinstellungen

Der Mobilfunkrouter UR75 unterstützt 5 Gigabit-Ethernet-Ports. Auf dieser Seite werden die Eigenschaften aller Ethernet-Ports angezeigt und Sie können den Status dieser Ports steuern.

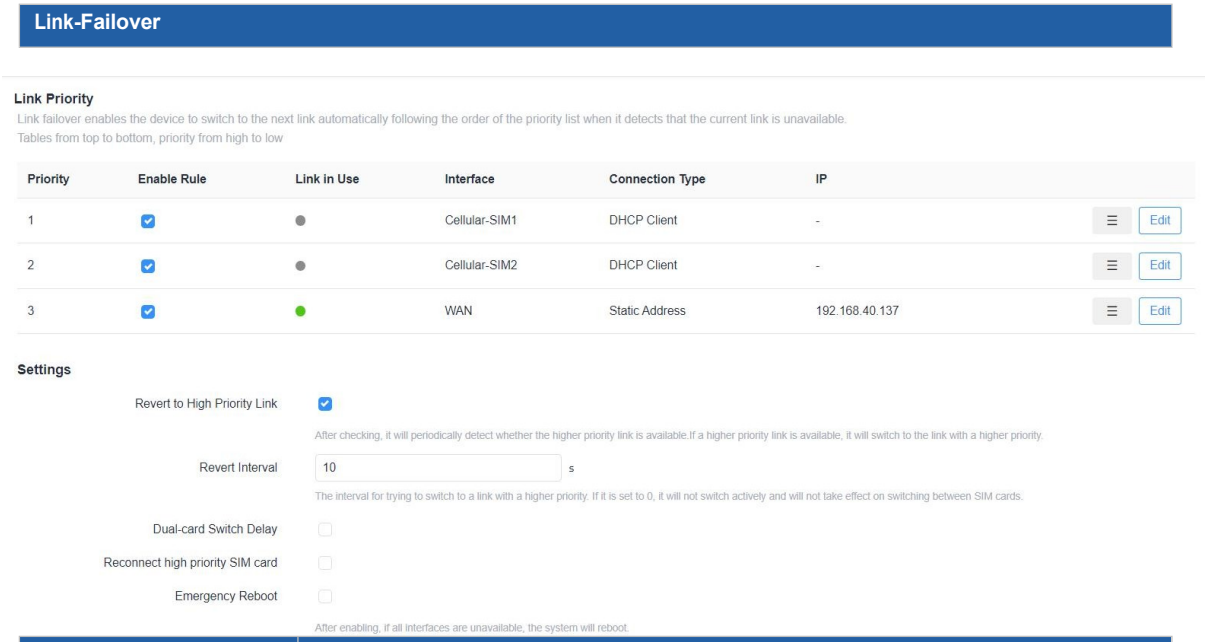



| Schnittstelleneinstellung | |
|---|---|
| **Element** | **Beschreibung** |
| Schnittstelle | Benutzer können die Ethernet-Ports entsprechend ihren Anforderungen definieren. |
| Status | Legen Sie den Status des Ethernet-Ports fest. Wählen Sie **„Up"**, um ihn zu aktivieren, und **„Down"**, um ihn zu |

| | |
|---|---|
| | zu deaktivieren. |
| Eigenschaft | Der Typ des Ethernet-Ports, festgelegt als WAN-Port oder LAN-Port. |
| Schnittstellengeschwindigkeit | Die Geschwindigkeit des Ethernet-Ports ist auf „Auto“ festgelegt. |
| Schnittstellenmodus | Der Modus des Ethernet-Ports ist auf „Auto“ festgelegt. |

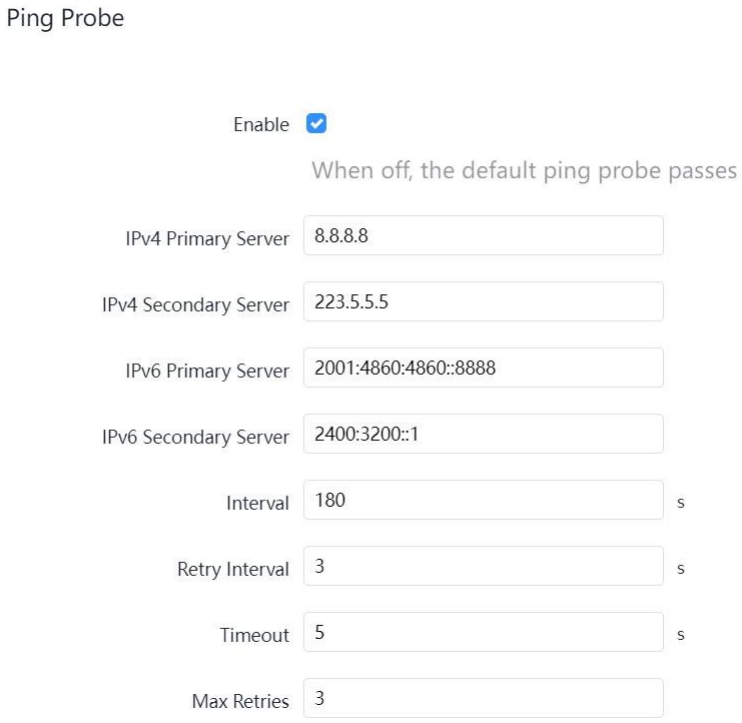
### 6.2.1.5 Link-Failover

In diesem Abschnitt wird beschrieben, wie Sie Link-Failover-Strategien, deren Priorität und die Ping-Einstellungen konfigurieren. Jede Regel verfügt standardmäßig über eigene Ping-Regeln. Der Router wählt gemäß der Priorität die nächste verfügbare Schnittstelle für den Internetzugang aus. Stellen Sie sicher, dass Sie hier die gesamte Schnittstelle aktiviert haben, die Sie verwenden möchten. Wenn Priorität 1 nur IPv4 verwenden kann, wählt UR75 einen zweiten Link aus, in dem IPv6 als primärer IPv6-Link fungiert, und umgekehrt.




| Element | Beschreibung |
|---|---|
| **Verbindungspriorität** | |
| Priorität | Zeigen Sie die Priorität jeder Schnittstelle an. Sie können sie mit der **Aufwärts-** und Ab**wärts**-Schaltflächen der Operation ändern. |
| Regel aktivieren | Wenn diese Option aktiviert ist, wählt der Router diese Schnittstelle für seine Switching-Regel aus. Wenn die Mobilfunk-Schnittstelle hier nicht aktiviert ist, wird die Schnittstelle ebenfalls deaktiviert. |
| Verbindung in Gebrauch | Markieren Sie mit grüner Farbe, ob diese Schnittstelle verwendet wird. |
| Schnittstelle | Zeigen Sie den Namen der Schnittstelle an. |
| Verbindungstyp | Zeigen Sie an, wie die IP-Adresse in dieser Schnittstelle abgerufen werden kann, z. B. statische IP oder DHCP. Bei Mobilfunk-Schnittstellen wird nur DHCP-Client unterstützt. |
| IP | Zeigen Sie die IP-Adresse der Schnittstelle an. |
| ☰ | Ziehen Sie diese Schaltfläche, um die Priorität der Netzwerkverbindungen anzupassen. Der oberste Eintrag der Liste hat die höchste Priorität. |
| Bearbeiten | Klicken Sie hier, um die Ping-Probe-Einstellungen jeder Netzwerkverbindung zu bearbeiten. |
| **Einstellungen** | |
| Auf „Hoch“ zurücksetzen | Wenn diese Option aktiviert ist, wird regelmäßig überprüft, ob die Verbindung mit hoher Priorität |

| | |
|---|---|
| Prioritätsverbindung | pingt werden, und wenn ja, die Verbindung mit einer höheren Priorität umschalten. |
| Rückstellintervall | Geben Sie die Anzahl der Sekunden an, die Sie warten sollten, bevor Sie zu die Verbindung mit höherer Priorität zu wechseln. 0 bedeutet, dass nicht aktiv gewechselt wird. |
| Dual-Karten-Umschaltung Verzögerung | Aktivieren oder deaktivieren Sie diese Option, um die Verzögerungszeit für den Wechsel zur Karte mit niedrigerer Karte zu wechseln, wenn die Mobilfunkverbindung mit hoher Priorität fehlschlägt. |
| Hochprioritäre SIM-Karte erneut verbinden | Aktivieren oder deaktivieren Sie diese Option, um das Intervall für die Erkennung einer Mobilfunkverbindung mit hoher Priorität zu konfigurieren. Wenn die Verbindung wiederhergestellt ist, wird wieder auf die Mobilfunkverbindung mit hoher Priorität zurück. |
| Notfall-Neustart | Aktivieren Sie diese Option, um das Gerät neu zu starten, wenn keine Verbindung verfügbar ist. |

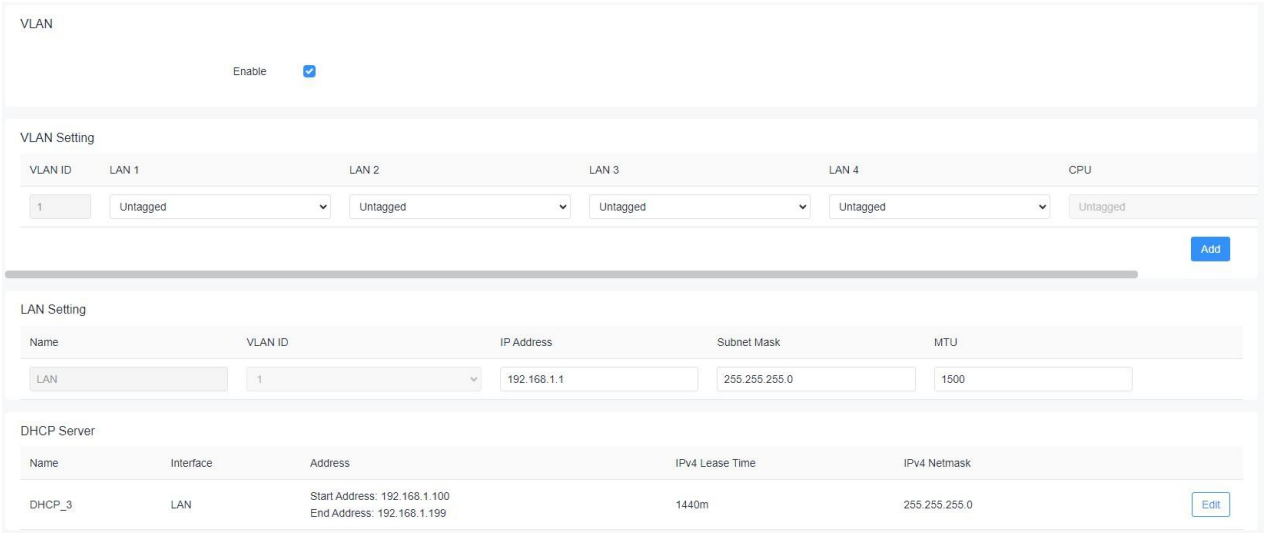



| Ping-Prüfung | |
|---|---|
| **Element** | **Beschreibung** |
| Aktivieren | Wenn diese Option aktiviert ist, überprüft der Router regelmäßig den Verbindungsstatus des Links durch Senden von ICMP-Paketen. |
| IPv4/IPv6-Primärserver | Der Router sendet ein ICMP-Paket an die IPv4/IPv6-Adresse, um festzustellen, ob die Netzwerkverbindung noch verfügbar ist oder nicht. |
| IPv4/IPv6-Sekundär Server | Der Router versucht, die alternative Serveradresse anzupingen, wenn Primärserver nicht verfügbar ist. |
| Intervall | Zeitintervall (in Sekunden) zwischen zwei Pings. |
| Wiederholungsintervall | Legen Sie das Intervall für Ping-Wiederholungen fest. Wenn der Ping fehlgeschlagen ist, sendet der Router erneut in jedem Wiederholungsintervall. |
| Zeitlimit | Die maximale Zeit, die der Router auf eine Antwort auf eine Ping-Anfrage wartet. Wenn er innerhalb der in diesem Feld vordefinierten Zeit keine Antwort erhält, wird die Ping-Anfrage als fehlgeschlagen betrachtet. |

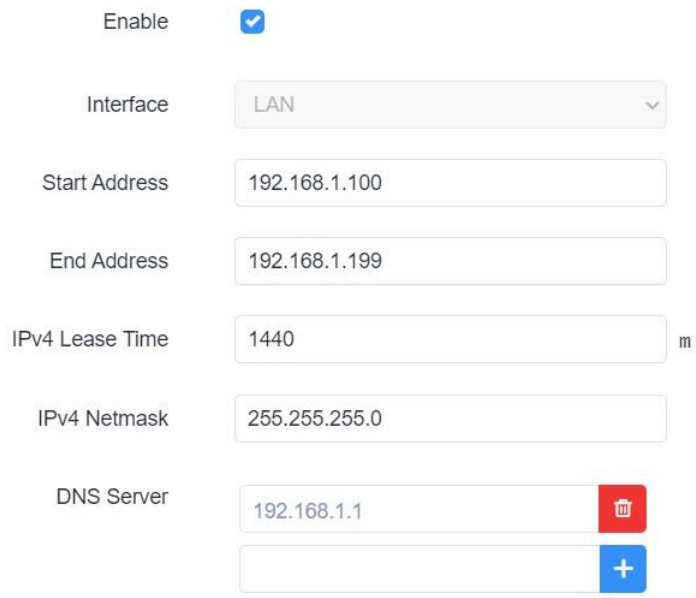
| | |
|---|---|
| Maximale Wiederholungsversuche | Die Anzahl der Wiederholungsversuche, die der Router beim Senden von Ping-Anfragen unternimmt, bis feststellt, dass die Verbindung fehlgeschlagen ist. |

### 6.2.1.6 Switch (VLAN)

VLAN ist eine neue Datenaustauschtechnologie, die virtuelle Arbeitsgruppen realisiert, indem sie die LAN-Geräte logisch in Netzwerksegmente unterteilt.



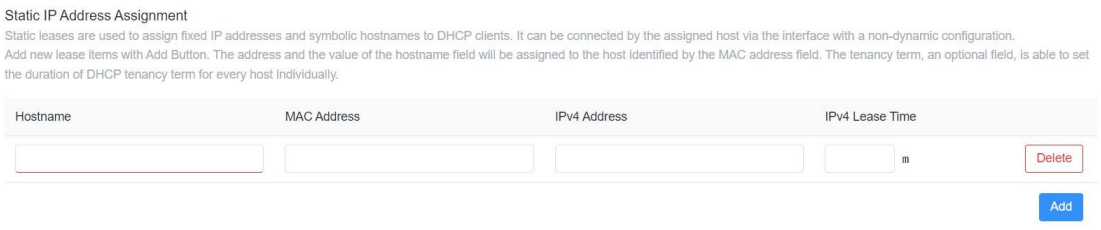

| Switch | |
|---|---|
| **Element** | **Beschreibung** |
| VLAN | Aktivieren oder deaktivieren Sie die VLAN-Funktion. |
| **VLAN-Einstellungen** | |
| VLAN-ID | Legen Sie die Label-ID des VLAN fest. Bereich: 3-4094. |
| LAN 1/2/3/4 | Binden Sie das VLAN an die entsprechenden Ports und wählen Sie den Status aus „Getaggt“, „Nicht getaggt“ und „Schließen für Ethernet-Frame auf Trunk-Verbindung“ aus. |
| CPU | Steuern Sie die Kommunikation zwischen VLAN und anderen Netzwerken. |
| **LAN-Einstellungen** | |
| Name | Legen Sie den Schnittstellennamen des VLAN fest. |
| VLAN-ID | Wählen Sie die VLAN-ID der Schnittstelle aus. |
| IP-Adresse | Legen Sie die IP-Adresse des LAN-Ports fest, die sich von WANLAN und andere VLANs. |
| Subnetzmaske | Legen Sie die Netzmaske des LAN-Ports fest. |
| MTU | Legen Sie die maximale Übertragungseinheit des LAN-Ports fest. Bereich: 68-1500. |




| Switch – DHCP-Server | |
|---|---|
| **Element** | **Beschreibung** |
| Aktivieren | Aktivieren Sie diese Option, um DHCP für diese VLAN-Schnittstelle zu deaktivieren. Der DHCP-Server kann nur gelöscht werden, wenn Sie die entsprechenden LAN-Einstellungen gelöscht haben. |
| Schnittstelle | Zeigt den VLAN-Schnittstellennamen des DHCP-Servers an. |
| Startadresse | Definieren Sie den Anfang des Pools von IP-Adressen, die an DHCP-Clients vergeben werden . |
| Endadresse | Definieren Sie das Ende des Pools von IP-Adressen, die an DHCP-Clients vermietet werden. |
| IPv4-Lease-Zeit | Legen Sie die Ablaufzeit der vermieteten Adressen fest, das Minimum beträgt 2 Minuten (2m). |
| IPv4-Netzmaske | Legen Sie diese fest, um die an Clients gesendete Netzmaske zu überschreiben. Normalerweise wird sie aus dem bedienten Subnetz berechnet. |
| DNS-Server | Legen Sie die DNS-Serverliste für Clients fest. |

### 6.2.1.7 Zuweisung statischer IP-Adressen

Wenn die LAN/VLAN-Schnittstelle als DHCP-Server fungiert, können Benutzer Geräten mit festen MAC-Adressen feste IP-Adressen und symbolische Hostnamen zuweisen.



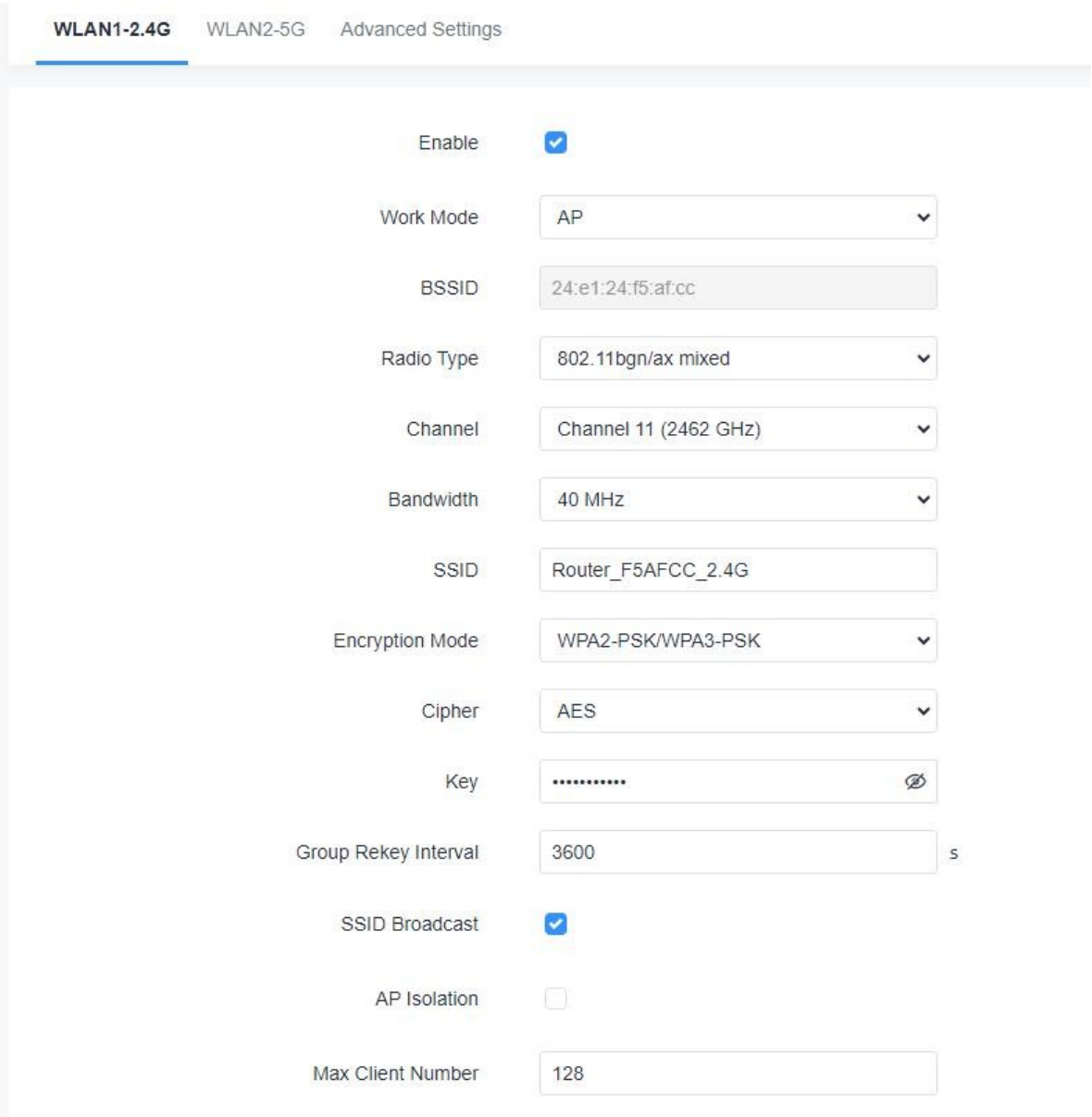

| Zuweisung statischer IP-Adressen | |
|---|---|
| **Element** | **Beschreibung** |
| Hostname | Der Hostname statischer Leases. |

| | |
|---|---|
| MAC-Adresse | Die MAC-Adresse des DHCP-Clients. |
| IPv4-Adresse | Die dem Client zugewiesene IPv4-Adresse. |
| IPv4-Lease-Zeit | Verbleibende Zeit für den Client. |

## 6.2.2 WLAN

### 6.2.2.1 WLAN

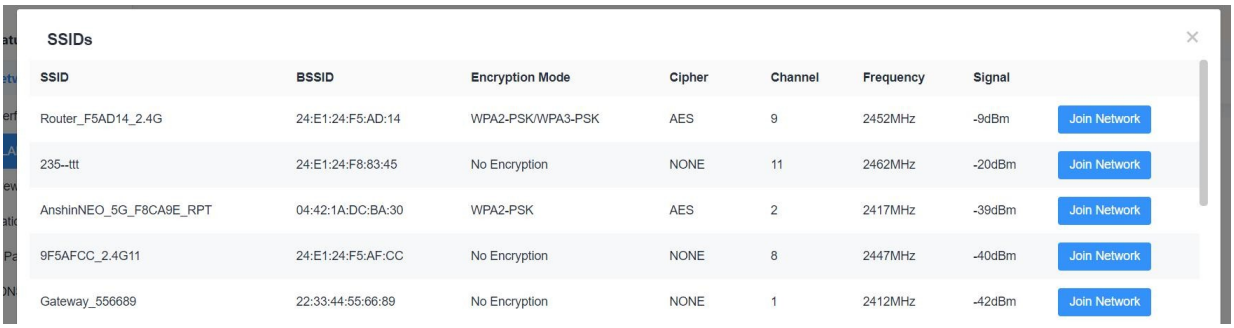
In diesem Abschnitt wird erläutert, wie Sie die entsprechenden Parameter für ein WLAN-Netzwerk einstellen. Der UR75 unterstützt sowohl 2,4-GHz- als auch 5-GHz-WLAN, die gleichzeitig betrieben werden können.




| WLAN | |
|---|---|
| **Element** | **Beschreibung** |
| Aktivieren | WLAN aktivieren/deaktivieren. |

| | |
|---|---|
| Arbeitsmodus | Wählen Sie den Arbeitsmodus des Routers aus. Die Optionen sind „Client“ oder „AP“. |
| **AP-Modus** | |
| BSSID | Zeigt die MAC-Adresse dieser WLAN-Schnittstelle an. |
| Funkmodus | Wählen Sie den Funktyp aus. |
| Kanal | Wählen Sie einen Funkkanal zwischen 1 und 13 oder wählen Sie „Auto“. |
| Bandbreite | Wählen Sie die Bandbreite aus. Die Optionen sind 20 MHz und 40 MHz. |
| SSID | Geben Sie die SSID des Zugangspunkts ein. |
| Verschlüsselungsmodus | Wählen Sie den Verschlüsselungsmodus aus. Die Optionen sind Keine Verschlüsselung, WEP Open System , WEP Auto, WEP Shared Key, WPA-PSK, WPA2-PSK, WPA3-PSK, WPA-PSK/WPA2-PSK und WPA2-PSK/WPA3-PSK. |
| Verschlüsselung | Wählen Sie die Verschlüsselung aus, wenn Sie den PSK-Verschlüsselungsmodus verwenden. Die Optionen sind AES, TKIP und AES/TKIP. |
| Schlüssel | Geben Sie den Schlüssel ein, um eine Verbindung zu diesem Zugangspunkt herzustellen. Der Standardschlüssel lautet **„iotpassword“**. |
| Gruppen-Schlüsselaktualisierung Intervall | Das Intervall für die Änderung des Verschlüsselungsschlüssels. |
| SSID Übertragung | Wenn die SSID-Übertragung deaktiviert ist, können andere drahtlose Geräte die SSID nicht finden, und Benutzer müssen die SSID manuell eingeben, um auf das drahtlose Netzwerk zugreifen zu können . |
| AP-Isolation | Wenn die AP-Isolation aktiviert ist, werden alle Benutzer, die auf den AP zugreifen, isoliert und können nicht miteinander kommunizieren. |
| Max. Client Anzahl | Legen Sie die maximale Anzahl von Clients fest, die zugreifen können, wenn der Router als AP konfiguriert ist. |
| MAC-Filterung | Aktivieren Sie diese Option, um die Clients zu filtern, die sich mit diesem Zugangspunkt verbinden dürfen. |
| Typ | Wählen Sie den Filtertyp für Geräte, die mit dem WLAN-Zugangspunkt dieses Routers verbunden sind.<br>**Whitelist:** Nur die aufgeführten MAC-Adressen dürfen eine Verbindung zum WLAN-Zugangspunkt des Routers herstellen.<br>**Blacklist:** Die aufgeführten MAC-Adressen dürfen keine Verbindung zum WLAN-Zugangspunkt des Routers verbinden. |
| MAC Adresse | Die MAC-Adressen der Geräte, die blockiert oder zugelassen werden sollen. |
| Beschreibung | Die Beschreibung dieser MAC-Adresse. |
| **Client-Modus** | |
| Scannen | Klicken Sie hier, um die Zugangspunkte in der Umgebung dieses Geräts zu scannen. |
| SSID | Geben Sie die SSID des Zugangspunkts ein. |
| BSSID | Geben Sie die MAC-Adresse des Zugangspunkts ein. Entweder die SSID oder die BSSID kann eingegeben werden , um sich mit dem Netzwerk zu verbinden. |
| Kanal | Wählen Sie einen WLAN-Kanal von 1 bis 13 oder wählen Sie „Auto“. |
| Verschlüsselung Modus | Wählen Sie den Verschlüsselungsmodus aus. Die Optionen sind „Keine Verschlüsselung“, „WPA-PSK“, WPA2-PSK, WPA3-PSK, WPA-PSK/WPA2-PSK und WPA2-PSK/WPA3-PSK. |
| Verschlüsselung | Wählen Sie die Verschlüsselungsmethode für die WPA-Verschlüsselung aus. Die Optionen sind „AES“, „TKIP“ und „AES/TKIP”. |
| Schlüssel | Geben Sie den Schlüssel ein, um eine Verbindung zu diesem Zugangspunkt herzustellen. |

| IP-Einstellung | |
|---|---|
| Protokoll | Legen Sie das Protokoll fest, um die WLAN-IP-Adresse zu erhalten. |
| IPv4-Adresse | Legen Sie die IP-Adresse im drahtlosen Netzwerk fest, wenn das Protokoll „Statische IP“ lautet. Beachten Sie, dass das Subnetz dieser IP-Adresse sich vom WAN-Port unterscheiden sollte. |
| Netzmaske | Stellen Sie die Netzmaske im drahtlosen Netzwerk ein, wenn das Protokoll „Statische IP“ lautet. |
| Gateway | Stellen Sie das Gateway im drahtlosen Netzwerk ein, wenn das Protokoll „Statische IP“ lautet. |
| Bevorzugt DNS | Legen Sie den primären IPv4-DNS-Server fest. |
| Alternativ DNS | Legen Sie den sekundären IPv4-DNS-Server fest. |



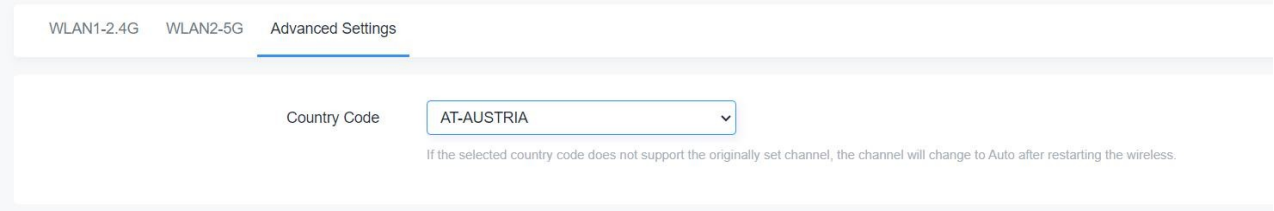

| WLAN-Scan | |
|---|---|
| **Element** | **Beschreibung** |
| SSID | SSID anzeigen. |
| BSSID | Zeigt die MAC-Adresse des Zugangspunkts an. |
| Verschlüsselungsmodus | Verschlüsselungsmodus anzeigen. |
| Verschlüsselung | Zeigt die Verschlüsselung des Zugangspunkts an. |
| Kanal | Drahtlosen Kanal anzeigen. |
| Frequenz | Zeigt die Frequenz des Funkgeräts an. |
| Signal | Drahtloses Signal anzeigen. |
| Mit Netzwerk verbinden | Klicken Sie auf die Schaltfläche, um sich mit dem WLAN-Netzwerk zu verbinden. |

**Verwandtes Thema**

Beispiel für eine WLAN-Anwendung

### 6.2.2.2 Erweiterte Einstellungen

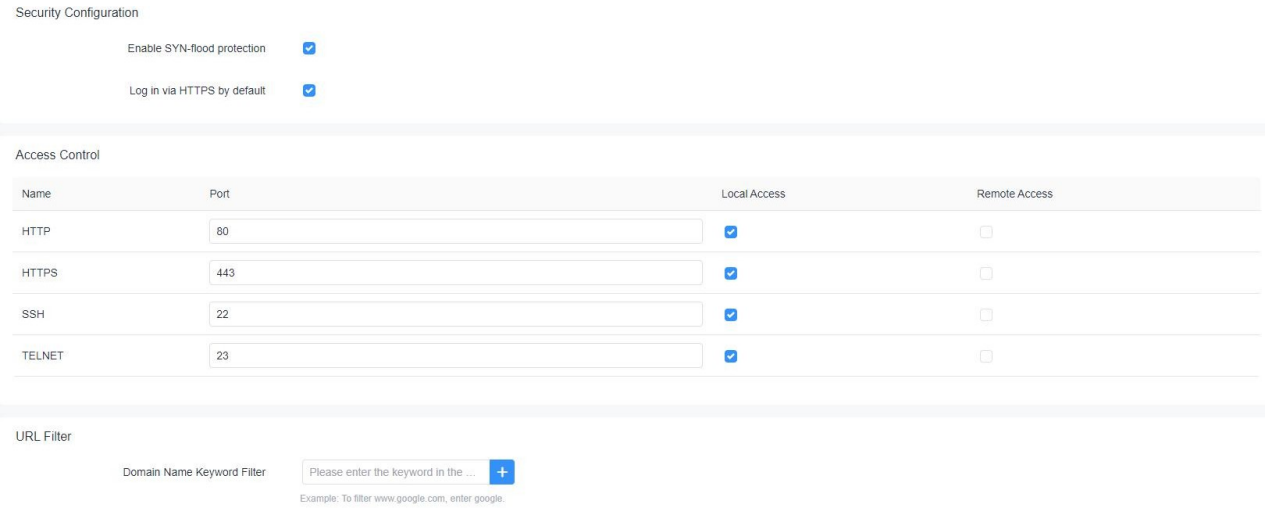
Das Gerät unterstützt die Auswahl des Ländercodes zur Anpassung des Kanals und der Sendeleistung.




### 6.2.3 Firewall

In diesem Abschnitt wird beschrieben, wie Sie die Firewall-Parameter einstellen, darunter Sicherheit, ACL, DMZ Port-Zuordnung und benutzerdefinierte iptables-Regeln. Nach der Einstellung können Sie unter **„Status > Firewall“** überprüfen, ob die Firewall-Einstellungen funktionieren.

#### 6.2.3.1 Allgemeine Einstellungen

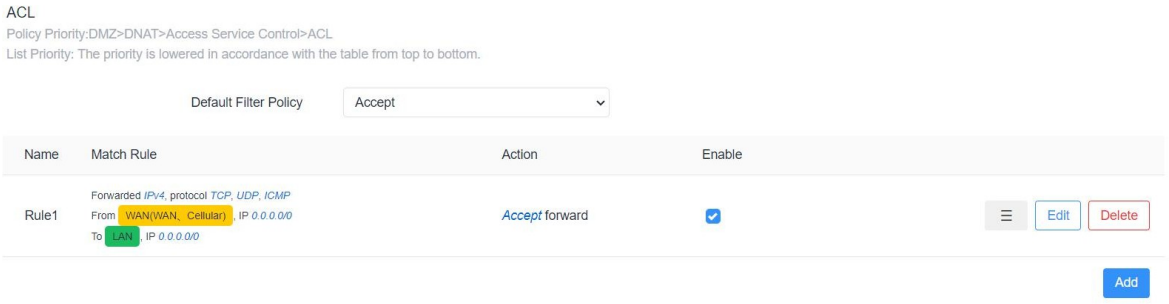



| Allgemeine Einstellungen | | |
|---|---|---|
| **Element** | **Beschreibung** | **Standard** |
| **Sicherheitskonfiguration** | | |
| SYN-Flood-Schutz aktivieren | Aktivieren/Deaktivieren Sie den SYN-Flood-Schutz. Der SYN-Flood-Schutz schützt vor DDoS-Angriffen, die einen Teil des normalen TCP-Drei-Wege-Handshakes ausnutzen, um Ressourcen auf dem Zielserver zu verbrauchen und ihn unbrauchbar zu machen. | Aktivieren |
| Standardmäßig über HTTPS anmelden standardmäßig | Standardmäßig über HTTPS in die Web-GUI des Geräts einloggen. | Aktivieren |
| **Zugriffskontrolle** | | |
| Port | Legen Sie die Portnummer der Dienste fest. Bereich: 1-65535. | -- |
| Lokaler Zugriff | Greifen Sie lokal auf den Router zu. | Aktivieren |
| Fernzugriff | Greifen Sie remote auf den Router zu. | Deaktivieren |
| HTTP | Benutzer können sich lokal über HTTP beim Gerät anmelden, um und es über das Web steuern, nachdem die Option | 80 |

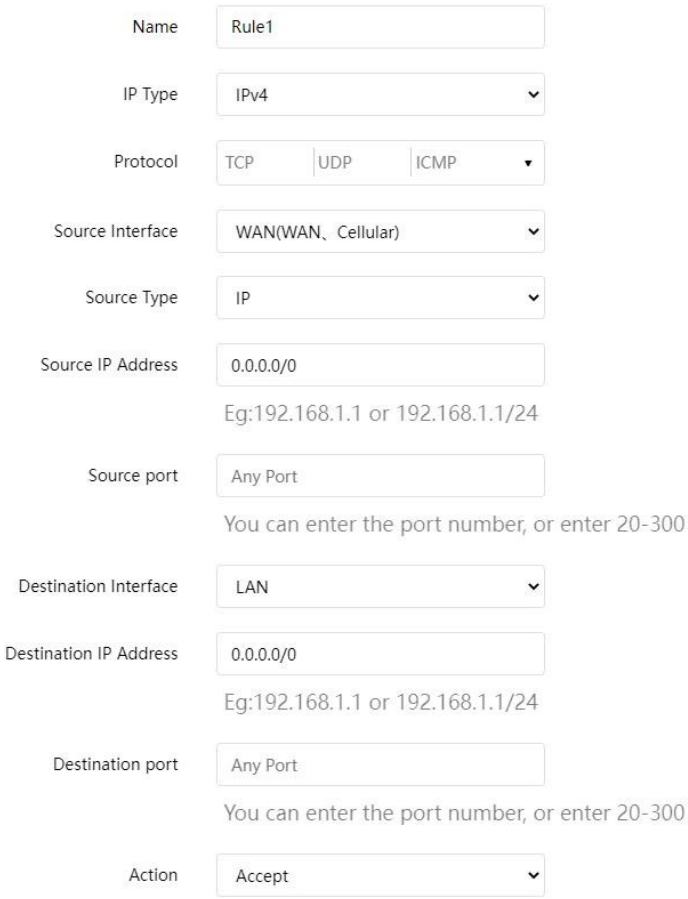
| | | |
|---|---|---|
| | aktiviert ist. | |
| HTTPS | Benutzer können sich lokal und remote über HTTPS beim Gerät anmelden, um über das Web darauf zuzugreifen und es zu steuern<br>, nachdem die Option aktiviert wurde. | 443 |
| TELNET | Benutzer können sich lokal und remote über Telnet beim Gerät anmelden<br>über Telnet anmelden, nachdem die Option aktiviert wurde. | 23 |
| SSH | Benutzer können sich lokal und remote<br>über SSH, nachdem die Option aktiviert wurde. | 22 |
| **URL-Filter** | | |
| Domainname-Stichwortfilter | Sie können bestimmte Websites blockieren, indem Sie ein Schlüsselwort aus einem Domainnamen eingeben. Nach dem Filtern können die Geräte unter den LAN-Ports nicht mehr auf die entsprechenden Websites zugreifen. Die maximal zulässige Anzahl von<br>Zulässige Zeichenanzahl: 64. | |

### 6.2.3.2 ACL

Die Zugriffskontrollliste, auch ACL genannt, implementiert die Erlaubnis oder Verweigerung des Zugriffs für bestimmten Netzwerkverkehr (z. B. die Quell-IP-Adresse), indem sie eine Reihe von Übereinstimmungsregeln konfiguriert, um den Netzwerk-Schnittstellenverkehr zu filtern. Wenn ein Router ein Paket empfängt, wird das Feld gemäß der für die aktuelle Schnittstelle geltenden ACL-Regel analysiert. Nachdem das spezielle Paket identifiziert wurde, wird die Erlaubnis oder Verweigerung des entsprechenden Pakets gemäß der voreingestellten Strategie implementiert. Die von der ACL definierten Datenpaket-Übereinstimmungsregeln können auch von anderen Funktionen verwendet werden, die eine Unterscheidung des Datenflusses erfordern.




| ACL | |
|---|---|
| **Element** | **Beschreibung** |
| Standardfilterrichtlinie | Pakete, die nicht in der Zugriffskontrollliste enthalten sind, werden gemäß der Standardfilterrichtlinie verarbeitet.<br>**Akzeptieren:** Erlaubt den gesamten Datenverkehr aus Geräten unter LAN-Ports.<br>**Verwerfen:** Verweigern Sie den gesamten Datenverkehr aus Geräten unter LAN-Ports. |
| Aktivieren | Aktivieren Sie diese ACL-Regel. |
| ☰ | Ziehen Sie diese Schaltfläche, um die Priorität der ACL-Regeln anzupassen. Der Anfang der<br>Liste hat die höchste Priorität. |
| Bearbeiten | Klicken Sie hier, um die Details dieser ACL-Regel zu bearbeiten. |
| Löschen | Diese ACL-Regel löschen. |




| ACL – Hinzufügen/Bearbeiten | |
|---|---|
| Name | Legen Sie einen eindeutigen Namen für diese ACL-Regel fest. |
| Typ | Wählen Sie den Typ IPv4 oder IPv6 aus. |
| Protokoll | Wählen Sie das Protokoll aus TCP, UDP und ICMP aus. |
| Quellschnittstelle | Wählen Sie den Quellschnittstellentyp aus „Geräteausgang“, „LAN“, „VLAN“ oder „WAN“ (WAN,Mobilfunk, WLAN). „Geräteausgang“ bedeutet, dass die Pakete vom Router selbst kommen. |
| Quelltyp | Bei Verwendung des IPv4-Typs wählen Sie den Adresstyp als IP, MAC oder IP+MAC aus. |
| Quell-IP/MAC Adresse | Quellnetzwerkadresse entsprechend dem Adresstyp festlegen. (0.0.0.0/0 bedeutet alle). |
| Quellport | Legen Sie eine bestimmte Quellportnummer oder einen Portbereich fest, Beispiel: 20-300. |
| Zielschnittstelle | Wählen Sie den Zielschnittstellentyp aus LAN, WAN (WAN,Mobilfunk, WLAN),VLAN oder Geräteeingang. Geräteeingang bedeutet, dass die Pakete an den Router selbst gesendet werden. |
| Ziel-IP Adresse | Legen Sie die Zielnetzwerkadresse fest (0.0.0.0/0 bedeutet alle). |
| Zielport | Legen Sie eine bestimmte Quellportnummer oder einen Portbereich fest, Beispiel: 20-300. |
| Aktion | Wählen Sie die Aktion „Akzeptieren“ oder „Ablehnen“. |

### 6.2.3.3 Portzuordnung (DNAT)

Wenn externe Dienste intern benötigt werden (z. B wenn eine Website extern veröffentlicht wird), initiiert die externe Adresse eine aktive Verbindung. Der Router oder das Gateway der Firewall empfängt die Verbindung. Anschließend wird die Verbindung in eine interne Verbindung umgewandelt. Diese Umwandlung wird als DNAT bezeichnet und wird hauptsächlich für externe und interne Dienste verwendet.


| Portzuordnung (DNAT) | |
|---|---|
| **Artikel** | **Beschreibung** |
| Name | Legen Sie einen eindeutigen Namen für die Portzuordnungsregel fest. |
| Protokoll | Wählen Sie TCP oder UDP entsprechend den Anforderungen Ihrer Anwendung aus. |
| Externe IP-Adresse | Geben Sie den Host oder das Netzwerk an, das auf die lokale IP-Adresse zugreifen kann.<br>0.0.0.0/0 bedeutet alle. |
| Externer Port | Legen Sie den Port oder Portbereich fest, von dem aus eingehende Pakete weitergeleitet werden, Beispiel: 20-300. |
| Interne IP-Adresse | Geben Sie die IP-Adresse ein, an die Pakete weitergeleitet werden, nachdem Empfang über die eingehende Schnittstelle weitergeleitet werden. |
| Interner Port | Geben Sie den Port oder Portbereich ein, an den Pakete nach dem Empfang vom eingehenden Port weitergeleitet werden. Bei der Einstellung des Portbereichs sollte der<br>Wert mit dem externen Portbereich übereinstimmen. |
| Aktivieren | Aktivieren oder deaktivieren Sie diese Portzuordnungsregel. |
| ☰ | Ziehen Sie diese Schaltfläche, um die Priorität der Portzuordnungsregeln anzupassen. Die<br>oberste Eintrag in der Liste hat die höchste Priorität. |
| Löschen | Löschen Sie diese Regel. |

**Beispiel für eine zugehörige Konfiguration**

NAT-Anwendungsbeispiel

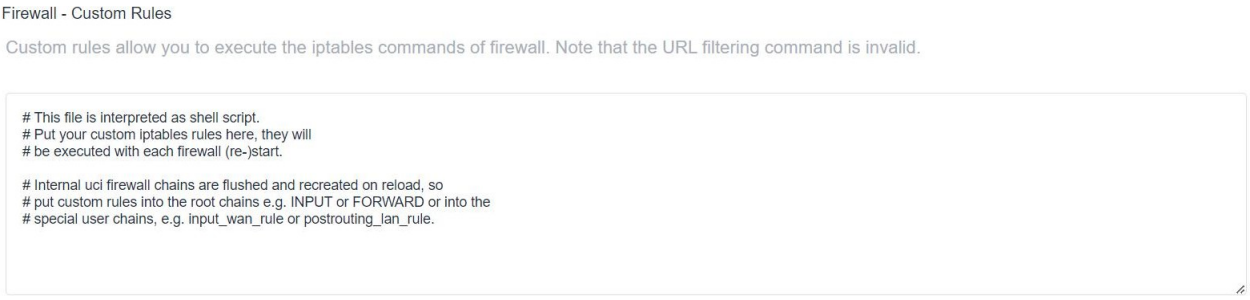
### 6.2.3.4 DMZ

DMZ ist ein Host innerhalb des internen Netzwerks, bei dem alle Ports offen sind, mit Ausnahme der in der Portzuordnung weitergeleiteten Ports.


| DMZ | |
|---|---|
| **Element** | **Beschreibung** |
| Aktivieren | DMZ aktivieren oder deaktivieren. |
| DMZ-Host | Geben Sie die IP-Adresse des DMZ-Hosts im internen Netzwerk ein. |
| Quell-IP-Adresse | Legen Sie die Quell-IP-Adresse fest, die auf den DMZ-Host zugreifen kann.<br>„0.0.0.0/0“ bedeutet „beliebige Adresse“. |

### 6.2.3.5 Benutzerdefinierte Regeln

Auf dieser Seite können Sie Ihre eigenen benutzerdefinierten Firewall-iptables-Regeln eingeben, die als Linux-Shell-Skript ausgeführt werden.

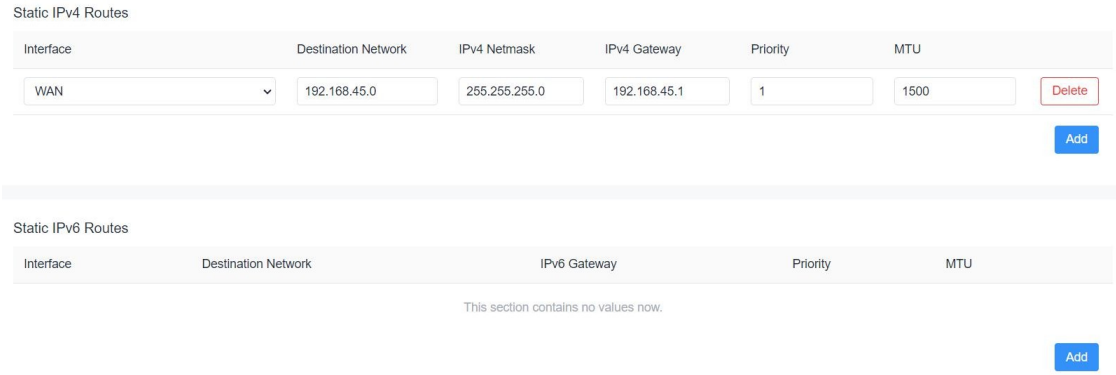



### 6.2.3.6 Zertifikate

Auf dieser Seite können Sie die HTTPS-Zertifikate für den sicheren Zugriff auf die Web-GUI des Routers importieren.


## 6.2.4 Statische Routen

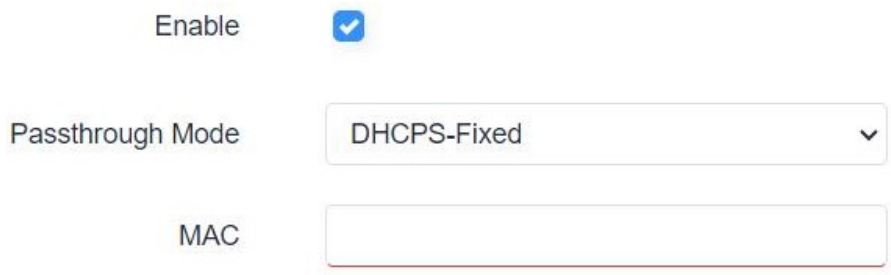
Eine statische Route ist ein manuell konfigurierter Routing-Eintrag. Die Informationen zum Routing werden manuell eingegeben und nicht aus dem dynamischen Routing-Verkehr abgerufen. Nach der Einrichtung der statischen Route wird das Paket für das angegebene Ziel an den vom Benutzer festgelegten Pfad weitergeleitet.




| Statische Routen | |
|---|---|
| **Element** | **Beschreibung** |
| Schnittstelle | Über die Schnittstelle gelangen die Daten zur Zieladresse. |
| Ziel Netzwerk | Geben Sie die Ziel-IPv4/IPv6-Adresse ein. |
| IPv4-Netzmaske | Geben Sie die Subnetzmaske der IPv4-Zieladresse ein. |
| IPv4/IPv6 Gateway | IPv4/IPv6-Adresse des nächsten Routers, der passiert wird, bevor die Eingangsdaten die Zieladresse erreichen. |
| Priorität | Ein kleinerer Wert bedeutet eine höhere Priorität. Bereich: 1-255. |
| MTU | Legen Sie die maximale Übertragungseinheit fest. Bereich: 68-1500. |

### 6.2.5 IP-Passthrough

Der IP-Passthrough-Modus teilt die vom Internetanbieter zugewiesene IP-Adresse mit einem einzelnen LAN-Clientgerät, das mit dem Router verbunden ist, oder „leitet“ sie weiter.

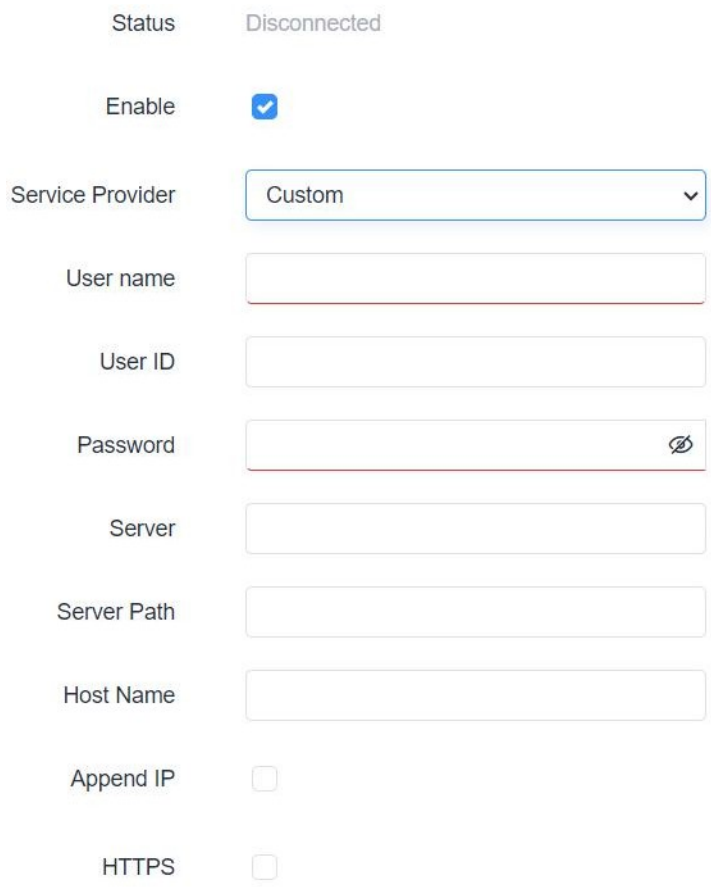



| IP-Passthrough | |
|---|---|
| **Element** | **Beschreibung** |
| Aktivieren | IP-Passthrough aktivieren oder deaktivieren. |
| Passthrough-Modus | Wählen Sie den Passthrough-Modus aus „DHCPS-Fixed” und „DHCPS-Dynamic“ aus. |
| MAC | Legen Sie die MAC-Adresse fest, wenn der Passthrough-Modus „DHCPS-Fixed“ ist. |

### 6.2.6 DDNS

Dynamic DNS (DDNS) ist eine Methode, die einen Nameserver in der Domain Name

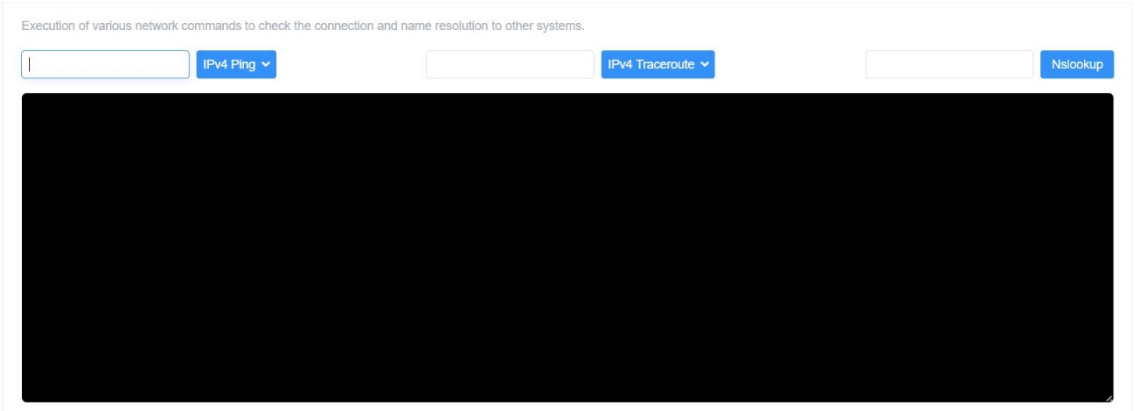
System, mit dem Benutzer eine dynamische IP-Adresse einem statischen Domainnamen zuordnen können.
DDNS dient als Client-Tool und muss mit dem DDNS-Server koordiniert werden. Vor Beginn der Konfiguration muss sich der Benutzer auf der Website eines geeigneten Domainnamenanbieters registrieren und einen Domainnamen beantragen.




| DDNS | |
|---|---|
| **Element** | **Beschreibung** |
| Status | Zeigt den Verbindungsstatus von DDNS an. |
| Aktiv | DDNS aktivieren/deaktivieren. |
| Dienstanbieter | Wählen Sie den DDNS-Dienstanbieter aus. |
| Benutzername | Geben Sie den Benutzernamen für die DDNS-Registrierung ein. |
| Benutzer-ID | Geben Sie die Benutzer-ID des benutzerdefinierten DDNS-Servers ein. |
| Passwort | Geben Sie das Passwort für die DDNS-Registrierung ein. |
| Server | Geben Sie den Namen des DDNS-Servers ein. |
| Serverpfad | Standardmäßig wird der Hostname an den Pfad angehängt. |
| Hostname | Geben Sie den Hostnamen für DDNS ein. |
| IP anhängen | Fügen Sie Ihre aktuelle IP zum DDNS-Server-Update-Pfad hinzu. |
| HTTPS | Aktivieren Sie HTTPS für einige DDNS-Anbieter. |

### 6.2.7 Diagnose

Netzwerkdienstprogramme umfassen IPv4/IPv6-Ping, IPv4/IPv6-Traceroute und das Befehlszeilentool nslookup.




| Netzwerkdienstprogramme | |
|---|---|
| **Element** | **Beschreibung** |
| IPv4-Ping | Klicken Sie hier, um vom Gerät in IPv4 aus das externe Netzwerk anzupingen. |
| IPv6-Ping | Klicken Sie hier, um das externe Netzwerk vom Gerät in IPv6 aus anzupingen. |
| IPv4-Traceroute | Adresse des Zielhosts, der in IPv4 erkannt werden soll. |
| IPv6-Traceroute | Adresse des Zielhosts, der in IPv6 erkannt werden soll. |
| Nslookup | Klicken Sie hier, um die Zuordnung zwischen Domänenname und IP-Adresse oder andere DNS-Einträge anzuzeigen. |

## 6.3 VPN

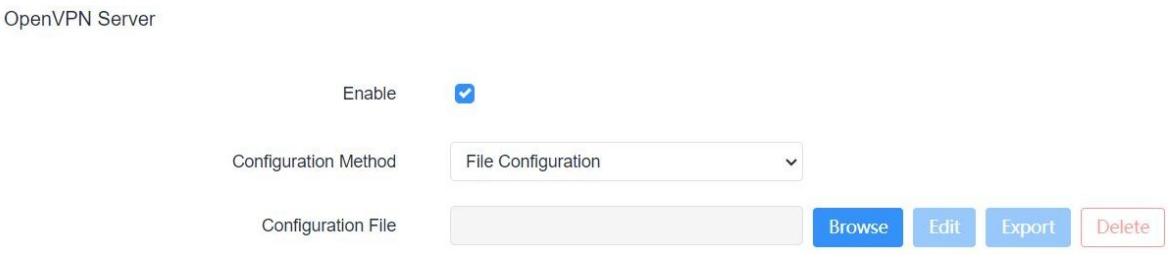
Virtuelle private Netzwerke, auch VPNs genannt, werden verwendet, um zwei private Netzwerke sicher miteinander zu verbinden, sodass Geräte über sichere Kanäle von einem Netzwerk zum anderen Netzwerk verbunden werden können.

### 6.3.1 OpenVPN

OpenVPN ist ein Open-Source-Produkt für virtuelle private Netzwerke (VPN), das ein vereinfachtes Sicherheitsframework, ein modulares Netzwerkdesign und plattformübergreifende Portabilität bietet. Die Standardversion von OpenVPN für UR75 ist 2.5.3.

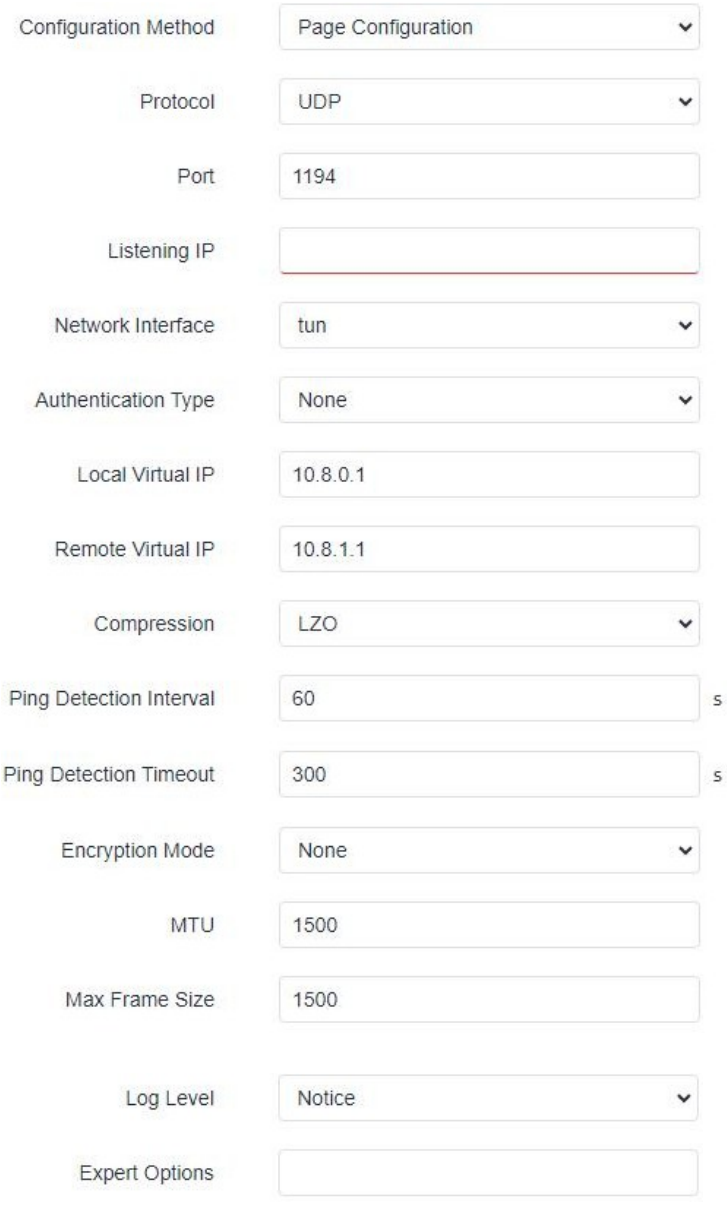
#### 6.3.1.1 OpenVPN-Server

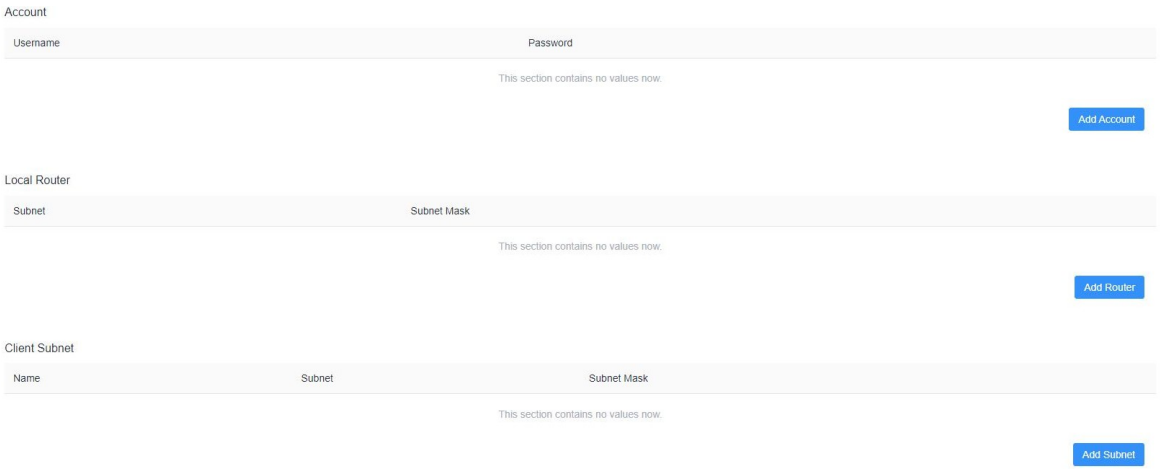
UR75 unterstützt OpenVPN-Server, um sichere Punkt-zu-Punkt- oder Standort-zu-Standort-Verbindungen in gerouteten oder gebrückten Konfigurationen und Fernzugriffsfunktionen zu erstellen. Sie können die ovpn-Datei direkt importieren oder die Parameter auf dieser Seite konfigurieren, um diesen Server einzurichten.




**OpenVPN-Server – Dateikonfiguration**

| Element | Beschreibung |
|---|---|
| Durchsuchen | Klicken Sie hier, um die OVPN-Konfigurationsdatei des Servers mit den Einstellungen und Zertifikatsinhalten anzuzeigen. Bitte beachten Sie die Serverkonfigurationsdatei gemäß dem Beispiel: server.conf |
| Bearbeiten | Klicken Sie hier, um die importierte Datei zu bearbeiten. |
| Export | Exportieren Sie die Serverkonfigurationsdatei. |
| Löschen | Klicken Sie hier, um die Konfigurationsdatei zu löschen. |






| OpenVPN-Server – Seitenkonfiguration | |
|---|---|
| **Element** | **Beschreibung** |
| Protokoll | Wählen Sie ein Transportprotokoll für die Verbindung aus UDP und TCP aus. |
| Zuhörende IP | Geben Sie den lokalen Hostnamen oder die IP-Adresse für die Bindung ein. Wenn das Feld leer bleibt, verbindet sich der OpenVPN-Server<br>Server an alle Schnittstellen gebunden. |
| Port | Geben Sie die TCP/UCP-Servicenummer für die OpenVPN-Clientverbindung ein.<br>Bereich: 1-65535. |
| Netzwerkschnittstelle | Wählen Sie den Typ der virtuellen VPN-Netzwerkschnittstelle aus TUN und TAP aus. TUN-Geräte kapseln IPv4 oder IPv6 (OSI-Schicht 3), während TAP-Geräte<br>Ethernet 802.3 (OSI-Schicht 2) kapseln. |
| Authentifizierungstyp | Wählen Sie den Authentifizierungstyp aus, der zur Sicherung von Datensitzungen verwendet wird.<br>**Vorab geteilt:** Verwenden Sie denselben geheimen Schlüssel wie der Server, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite **VPN > OpenVPN > Zertifikate**, um eine statische Datei (static.key) in das Feld **PSK** zu importieren.<br>**Benutzername/Passwort:** Verwenden Sie den auf der Serverseite voreingestellten Benutzernamen/das Passwort, um die Authentifizierung abzuschließen.<br>**X.509-Zertifikat:** Verwenden Sie ein Zertifikat vom Typ X.509, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite **VPN > OpenVPN > Zertifizierungen**, um das CA-Zertifikat, das Client-Zertifikat und den privaten Client-Schlüssel in die entsprechenden Felder zu importieren.<br>**X.509-Zertifikat + Benutzer:** Verwenden Sie sowohl Benutzername/Passwort als auch X.509-Zertifikat<br>als Authentifizierungstyp verwenden. |
| Lokale virtuelle IP | Legen Sie die lokale Tunneladresse fest, wenn der Authentifizierungstyp **„Keine“** oder **„Vorab geteilt“** ist. |
| Virtuelle Remote-IP | Legen Sie die Remote-Tunneladresse fest, wenn der Authentifizierungstyp **„Keine“** oder „Vorab geteilt“ lautet.<br>**„Vorab geteilt“ ist.** |
| Client-Subnetz | Definieren Sie einen IP-Adresspool für den OpenVPN-Client. |
| Client-Netzmaske | Legen Sie die Netzmaske des Client-Subnetzes fest, um den IP-Adressbereich zu begrenzen. |
| Neuverhandlungsintervall | Verhandeln Sie den Datenkanalschlüssel nach diesem Intervall neu. 0 bedeutet deaktivieren. |
| Maximale Anzahl von Clients | Begrenzen Sie den Server auf eine maximale Anzahl gleichzeitiger Clients, Bereich: 1-128.<br>**Hinweis:** Bitte stellen Sie die Protokollierungsstufe auf „Info“ ein, wenn Sie viele Clients verbinden müssen. |
| CRL aktivieren | CRL-Überprüfung aktivieren oder deaktivieren. |
| Client-zu-Client aktivieren | Wenn diese Option aktiviert ist, können OpenVPN-Clients miteinander kommunizieren. |

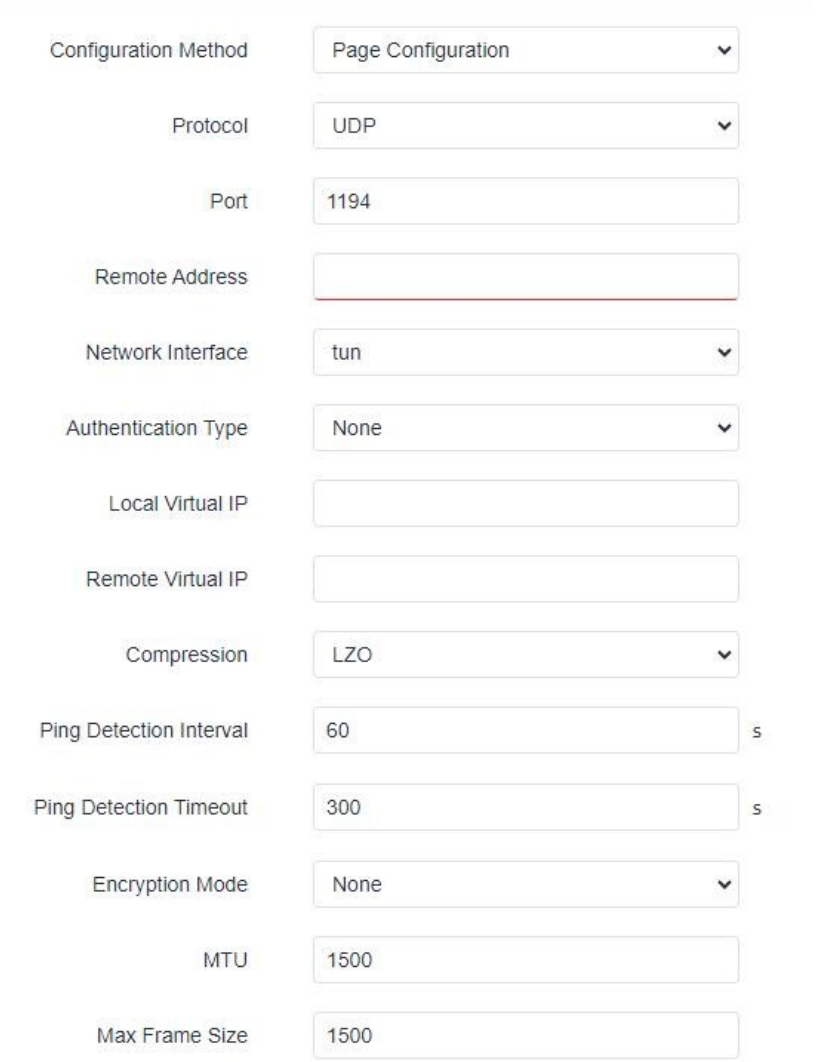
| | |
|---|---|
| Dup-Client aktivieren | Ermöglicht mehreren Clients, sich mit demselben gemeinsamen Namen oder derselben gemeinsamen Zertifizierung zu verbinden.<br>Zertifizierung. |
| TLS-Authentifizierung aktivieren | Deaktivieren oder aktivieren Sie die TLS-Authentifizierung, wenn der Authentifizierungstyp „X.509-Zertifikat“ ist. Nach der Aktivierung gehen Sie zur Seite **„VPN > OpenVPN > Zertifikate“**, um eine ta.key-Datei in das Feld **„TA“** zu importieren.<br>**Hinweis:** Diese Option unterstützt nur tls-auth. Für tls-crypt fügen Sie bitte diese Formatzeichenfolge in der Expertenoption hinzu: tls-crypt<br>/etc/openvpn/openvpn-client1-ta.key |
| Komprimierung | Wählen Sie diese Option, um LZO zur Komprimierung von Daten zu aktivieren oder zu deaktivieren. |
| Ping-Erkennungsintervall | Legen Sie das Intervall für die Verbindungserkennung fest, um die Tunnelverbindung sicherzustellen. Wenn dies festgelegt ist<br>Sowohl auf dem Server als auch auf dem Client überschreibt der vom Server übertragene Wert die lokalen Werte des Clients. Bereich: 10–1800 s. |
| Zeitlimit für Ping-Erkennung | OpenVPN wird nach Ablauf des Zeitlimits neu aufgebaut. Wenn dies sowohl auf dem Server und dem Client festgelegt ist, überschreibt der vom Server übermittelte Wert die lokalen Werte des Clients. Bereich: 60–3600 s. |
| Verschlüsselungsmodus | Wählen Sie zwischen NONE, BF-CBC, DES-CBC, DES-EDE3-CBC, AES-128-CBC, AES-192-CBC und AES-256-CBC. |
| MTU | Geben Sie die maximale Übertragungseinheit ein. Bereich: 68–1500. |
| Maximale Frame-Größe | Legen Sie die maximale Frame-Größe fest. Bereich: 64-1500. |
| Ausführlichkeitsstufe | Wählen Sie zwischen ERROR, WARING,NOTICE und DEBUG. |
| Expertenoptionen | Der Benutzer kann in diesem Feld einige Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Semikolons trennen.<br>**Beispiel:** auth SHA256; key direction 1 |
| **Konto** | |
| Benutzername und Passwort | Legen Sie den Benutzernamen und das Passwort für den OpenVPN-Client fest, wenn der Authentifizierungstyp<br>„Benutzername/Passwort“ ist. |
| **Lokaler Router** | |
| Subnetz | Legen Sie die IP-Adresse der lokalen Route fest. |
| Subnetzmaske | Legen Sie die Netzmaske der lokalen Route fest. |
| **Client-Subnetz** | |
| Name | Legen Sie den Namen als allgemeinen Namen des OpenVPN-Client-Zertifikats fest. |
| Subnetz | Legen Sie das Subnetz des OpenVPN-Clients fest. |
| Subnetzmaske | Legen Sie die Subnetzmaske des OpenVPN-Clients fest. |

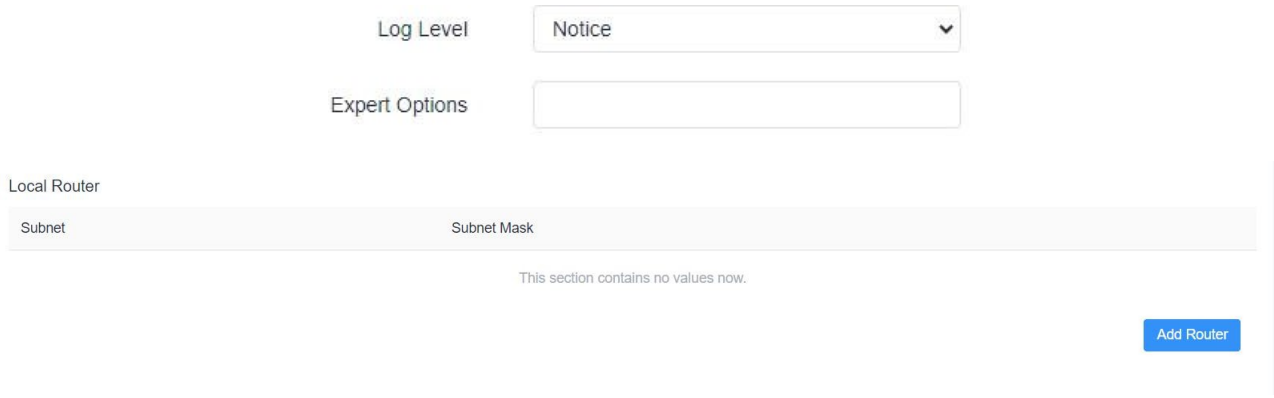
#### 6.3.1.2 OpenVPN-Client

UR75 unterstützt die gleichzeitige Ausführung von maximal 3 OpenVPN-Clients. Sie können die ovpn-Datei direkt importieren oder die Parameter auf dieser Seite konfigurieren, um Clients einzurichten.

Client_1


| OpenVPN-Client – Dateikonfiguration | |
|---|---|
| **Element** | **Beschreibung** |
| Durchsuchen | Klicken Sie hier, um die OVPN-Konfigurationsdatei des Clients mit den Einstellungen und Zertifikatsinhalte. Bitte beachten Sie die Client-Konfigurationsdatei gemäß dem Beispiel: client.conf |
| Bearbeiten | Klicken Sie hier, um die importierte Datei zu bearbeiten. |
| Export | Exportieren Sie die Serverkonfigurationsdatei. |
| Löschen | Klicken Sie hier, um die Konfigurationsdatei zu löschen. |






| OpenVPN-Client – Seitenkonfiguration | |
|---|---|
| **Element** | **Beschreibung** |
| Protokoll | Wählen Sie ein Transportprotokoll aus, das durch die Verbindung von UDP und TCP verwendet wird. |
| Remote-IP-Adresse | Geben Sie die IP-Adresse oder den Domänennamen des Remote-OpenVPN-Servers ein. |
| Port | Geben Sie die TCP/UCP-Servicenummer des Remote-OpenVPN-Servers ein. Bereich: 1-65535. |
| Netzwerkschnittstelle | Wählen Sie den Typ der virtuellen VPN-Netzwerkschnittstelle aus TUN und TAP aus. TUN-Geräte kapseln IPv4 oder IPv6 (OSI-Schicht 3), während TAP-Geräte Ethernet 802.3 (OSI-Schicht 2) kapseln. |
| Authentifizierungstyp | Wählen Sie den Authentifizierungstyp aus, der zur Sicherung von Datensitzungen verwendet wird.<br>**Vorab geteilt:** Verwenden Sie denselben geheimen Schlüssel wie der Server, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite **VPN > OpenVPN > Zertifikate**, um eine statische Datei (static.key) in das Feld **PSK** zu importieren.<br>**Benutzername/Passwort:** Verwenden Sie den auf der Serverseite voreingestellten Benutzernamen/das Passwort, um die Authentifizierung abzuschließen.<br>**X.509-Zertifikat:** Verwenden Sie ein Zertifikat vom Typ X.509, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite **VPN > OpenVPN > Zertifizierungen**, um das CA-Zertifikat, das Client-Zertifikat und den privaten Client-Schlüssel in die entsprechenden Felder zu importieren.<br>**X.509-Zertifikat + Benutzer:** Verwenden Sie sowohl Benutzername/Passwort als auch X.509-Zertifikat als Authentifizierungstyp verwenden. |
| Lokale virtuelle IP | Legen Sie die lokale Tunneladresse fest, wenn der Authentifizierungstyp **„Keine"** oder **„Vorab geteilt"** ist. |
| Virtuelle Remote-IP | Legen Sie die Remote-Tunneladresse fest, wenn der Authentifizierungstyp **„Keine"** oder „Vorab geteilt" lautet.<br>**„Vorab geteilt" ist.** |
| Globaler Datenverkehr Weiterleitung | Der gesamte Datenverkehr wird über den OpenVPN-Tunnel gesendet, wenn diese Funktion aktiviert ist. |
| TLS-Authentifizierung aktivieren | Deaktivieren oder aktivieren Sie die TLS-Authentifizierung, wenn der Authentifizierungstyp „X.509-Zertifikat" ist. Nach der Aktivierung gehen Sie zur Seite **„VPN > OpenVPN > Zertifikate"**, um eine ta.key-Datei in das Feld **„TA"** zu importieren.<br>**Hinweis:** Diese Option unterstützt nur tls-auth. Für tls-crypt fügen Sie bitte diese Formatzeichenfolge in der Expertenoption hinzu: tls-crypt /etc/openvpn/openvpn-client1-ta.key |
| Komprimierung | Wählen Sie diese Option, um LZO zur Komprimierung von Daten zu aktivieren oder zu deaktivieren. |
| Ping-Erkennungsintervall | Legen Sie das Intervall für die Verbindungserkennung fest, um die Tunnelverbindung sicherzustellen. Wenn dies festgelegt ist Sowohl auf dem Server als auch auf dem Client überschreibt der vom Server übertragene Wert die |

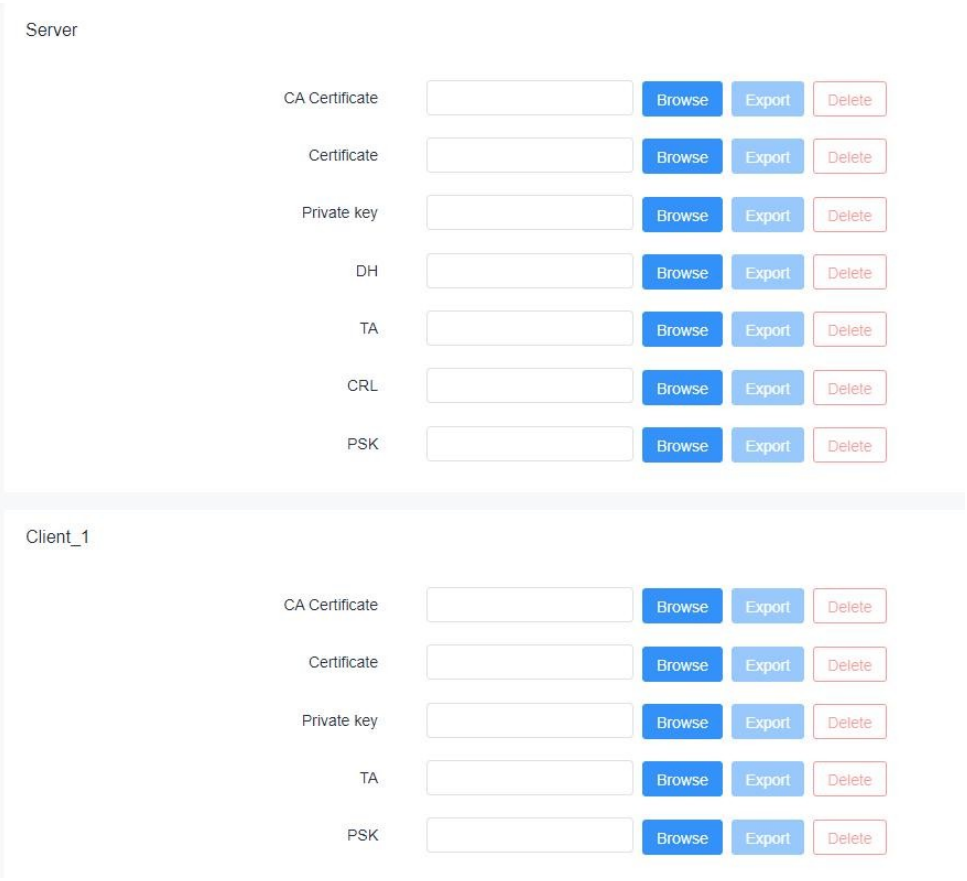
| | |
|---|---|
| | lokalen Werte des Clients. Bereich: 10-1800 s. |
| Zeitlimit für Ping-Erkennung | OpenVPN wird nach Ablauf des Zeitlimits neu aufgebaut. Wenn dies sowohl auf dem Server als auch auf dem Client eingestellt ist, überschreibt der vom Server übermittelte Wert die lokalen Werte des Clients<br>. Bereich: 60-3600 s. |
| Verschlüsselungsmodus | Wählen Sie zwischen NONE, BF-CBC, DES-CBC, DES-EDE3-CBC, AES-128-CBC, AES-192-CBC und AES-256-CBC. |
| MTU | Geben Sie die maximale Übertragungseinheit ein. Bereich: 128-1500. |
| Maximale Frame-Größe | Legen Sie die maximale Bildgröße fest. Bereich: 128-1500. |
| Ausführlichkeitsstufe | Wählen Sie zwischen ERROR, WARING,NOTICE und DEBUG. |
| Expertenoptionen | Der Benutzer kann in diesem Feld einige Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Semikolons trennen.<br>**Beispiel:** auth SHA256; key direction 1 |
| **Lokale Route** | |
| Subnetz | Legen Sie die IP-Adresse der lokalen Route fest. |
| Subnetzmaske | Legen Sie die Netzmaske der lokalen Route fest. |

**Beispiel für eine zugehörige Konfiguration**

Beispiel für eine OpenVPN-Client-Anwendung

### 6.3.1.3 Zertifikat

Bei Verwendung der Seitenkonfiguration des OpenVPN-Servers oder -Clients kann der Benutzer die erforderlichen Zertifikats- und Schlüsseldateien entsprechend den Authentifizierungstypen auf diese Seite importieren/exportieren.

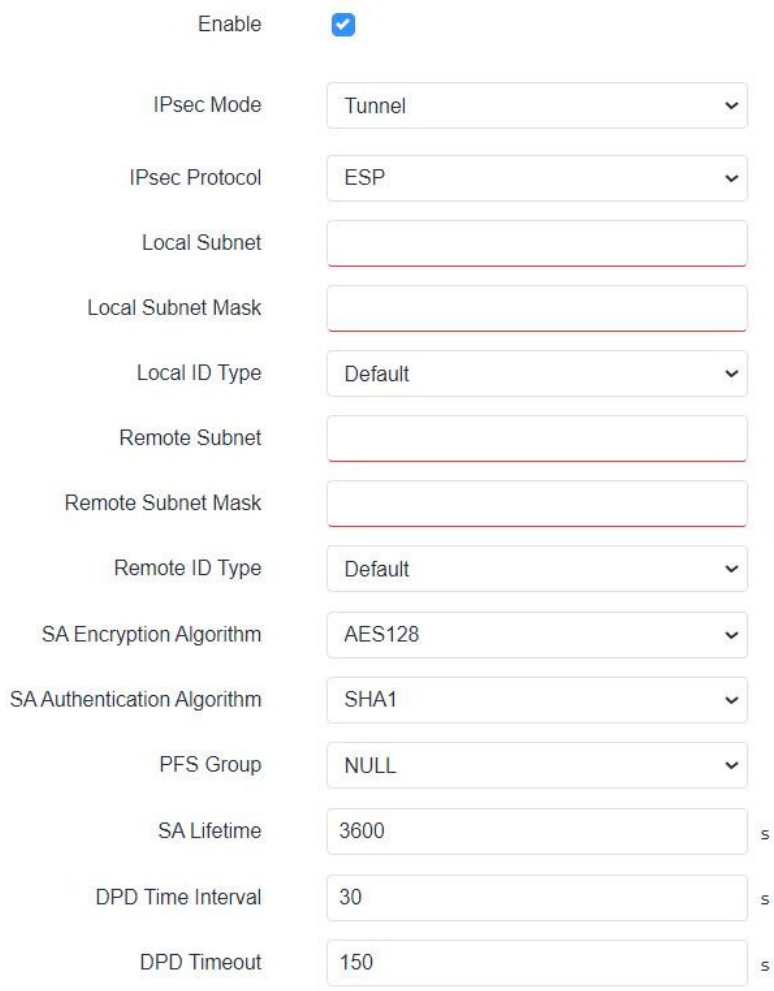



### 6.3.2 IPsecVPN

IPsec ist besonders nützlich für die Implementierung virtueller privater Netzwerke und für den Fernzugriff von Benutzern über eine Einwahlverbindung zu privaten Netzwerken. Ein großer Vorteil von IPsec besteht darin, dass Sicherheitsvorkehrungen getroffen werden können, ohne dass Änderungen an einzelnen Computern erforderlich sind.

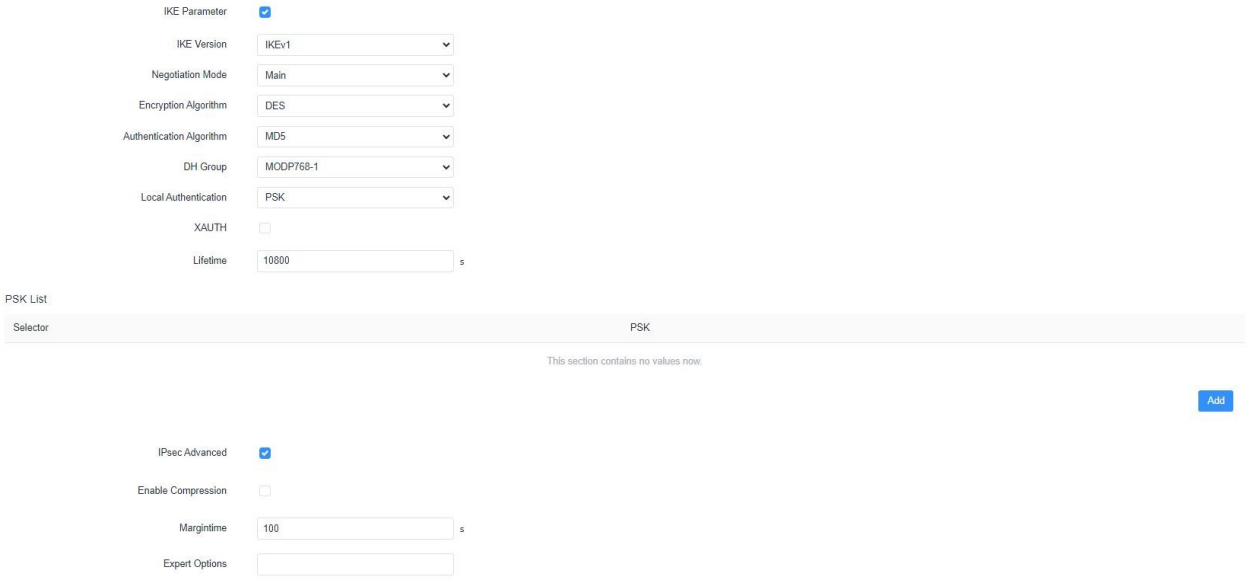
IPsec bietet drei Optionen für Sicherheitsdienste: Authentication Header (AH), Encapsulating Security Payload (ESP) und Internet Key Exchange (IKE). AH ermöglicht im Wesentlichen die Authentifizierung der Daten des Absenders. ESP unterstützt sowohl die Authentifizierung des Absenders als auch die Datenverschlüsselung. IKE wird für den Austausch von Verschlüsselungscodes verwendet. Alle drei Dienste können einen oder mehrere Datenflüsse zwischen Hosts, zwischen Host und Gateway sowie zwischen Gateways schützen.

#### 6.3.2.1 IPSec-Server




| IPsec-Server | |
|---|---|
| **Element** | **Beschreibung** |
| Aktivieren | Aktivieren oder deaktivieren Sie den IPsec-Servermodus. |
| IPsec-Modus | Wählen Sie „Tunnel“ oder „Transport“. |
| IPsec-Protokoll | Wählen Sie zwischen ESP und AH. |
| Lokales Subnetz | Geben Sie die IP-Adresse des lokalen LAN-Subnetzes im IPsec-Tunnel ein. |
| Lokale Subnetzmaske | Geben Sie die lokale LAN-Netzmaske für den IPsec-Tunnel ein. |
| Lokaler ID-Typ | Wählen Sie den Identifizierungstyp aus und senden Sie ihn an den Remote-Peer.<br>**Standard:** Keine<br>**ID:** Verwenden Sie die IP-Adresse des lokalen Subnetzes als ID.<br>**FQDN:** Vollständig qualifizierter Domänenname, Beispiel: test.user.com<br>**Benutzer-FQDN:** Vollständig qualifizierte Benutzername-Zeichenfolge im E-Mail-Adressformat, Beispiel: test@user.com |
| Remote-Subnetz | Legen Sie das Remote-LAN-Subnetz für den IPsec-Tunnel fest. |
| Remote-Subnetzmaske | Geben Sie die Remote-LAN-Netzmaske im IPsec-Tunnel ein. |
| Remote-ID-Typ | Wählen Sie den Identifizierungstyp aus, der mit der lokalen ID des Remote-Peers übereinstimmt.<br>**Standard:** Keine<br>**ID:** Remote-Subnetz-IP-Adresse als ID verwenden |

| | |
|---|---|
| | **FQDN:** Vollständig qualifizierter Domänenname, Beispiel: test.user.com<br>**Benutzer-FQDN:** Vollständig qualifizierte Benutzername-Zeichenfolge im E-Mail-Adressformat, Beispiel: test@user.com |
| SA-Verschlüsselungsalgorithmus | Wählen Sie AES128, AES192 oder AES256. |
| SA-Authentifizierung Algorithmus | Wählen Sie SHA1 oder SHA2-256. |
| PFS-Gruppe | Wählen Sie NULL, MODP768_1, MODP1024_2 oder MODP1536_5. |
| SA-Lebensdauer | Legen Sie die Lebensdauer der IPsec-SA fest. Bereich: 60-86400 s. |
| DPD-Intervallzeit | Legen Sie das DPD-Wiederholungsintervall für das Senden von DPD-Anfragen fest. Bereich: 2-60 s |
| DPD-Zeitlimit | Bei Verwendung von IKE V1 legen Sie das DPD-Zeitlimit fest, um den Ausfall der Gegenstelle zu erkennen<br>. Bereich: 10-3600 s. |

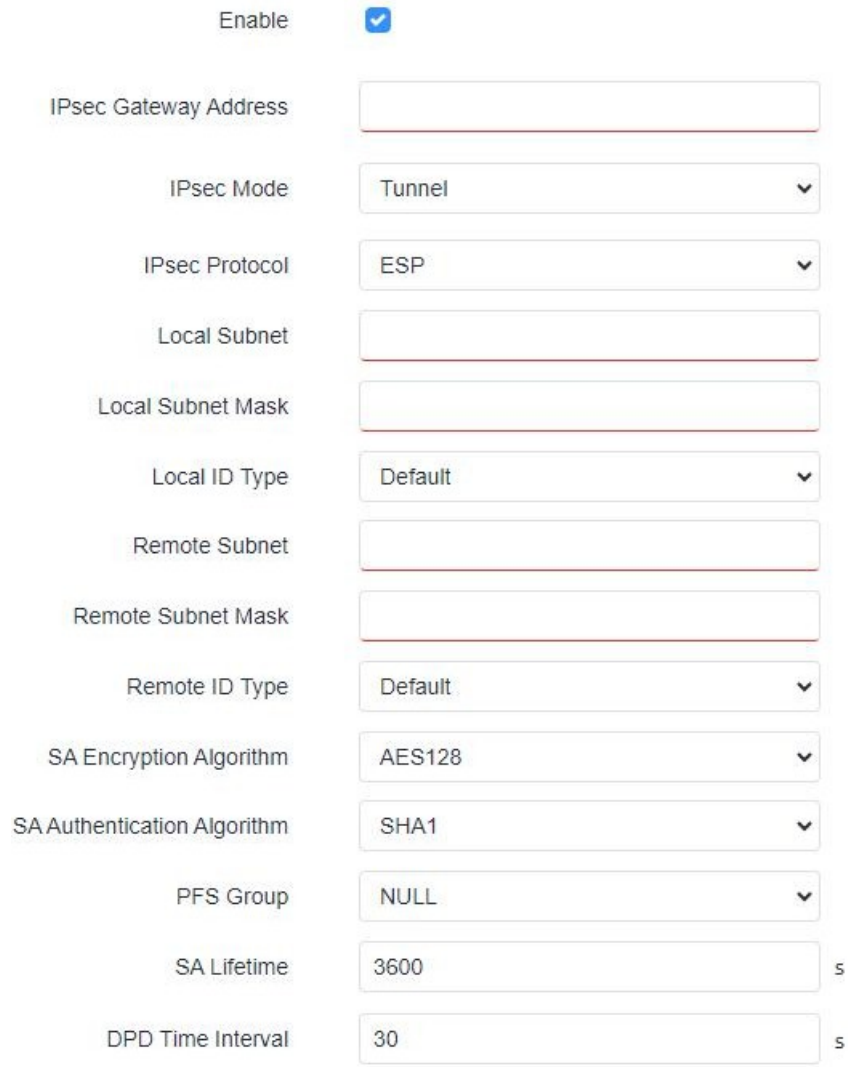



| IKE-Parameter | |
|---|---|
| **Element** | **Beschreibung** |
| IKE-Version | Wählen Sie die Methode für den Schlüsselaustausch aus IKEv1 und IKEv2 aus. |
| Verhandlungsmodus | Bei Verwendung von IKEv1 wählen Sie „Main“ oder „Aggressive“. |
| Verschlüsselungsalgorithmus | Wählen Sie DES, 3DES, AES128, AES192 oder AES256. |
| Authentifizierungsalgorithmus | Wählen Sie MD5, SHA1 oder SHA2-256. |
| DH-Gruppe | Wählen Sie MODP768_1, MODP1024_2 oder MODP1536_5. |
| Lokale Authentifizierung | Wählen Sie PSK oder CA.<br>**PSK:** Verwenden Sie einen vorab geteilten Schlüssel, um die Authentifizierung abzuschließen.<br>**CA:** Verwenden Sie ein Zertifikat, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite **VPN > IPsec > Zertifizierungen**, um das CA-Zertifikat, das lokale Zertifikat und den privaten Schlüssel in die entsprechenden Felder zu importieren. |
| Remote-Authentifizierung | Bei Verwendung von IKEv2 wählen Sie PSK oder CA.<br>**PSK:** Verwenden Sie einen vorab geteilten Schlüssel, um die Authentifizierung abzuschließen.<br>**CA:** Verwenden Sie ein Zertifikat, um die Authentifizierung abzuschließen. |

| | |
|---|---|
| XAUTH | Bei Verwendung von IKEv1 definieren Sie den XAUTH-Benutzernamen und das Passwort nach<br>XAUTH aktiviert ist. |
| Lebensdauer | Legen Sie die Lebensdauer in der IKE-Verhandlung fest. Bereich: 60-86400 s. |
| **XAUTH-Liste** | |
| Benutzername | Legen Sie den Benutzernamen fest, der für die Client-Xauth-Authentifizierung verwendet wird. |
| Passwort | Legen Sie das Passwort fest, das für die Client-Xauth-Authentifizierung verwendet wird. |
| **PSK-Liste** | |
| Selektor | Stellen Sie den Selektor als IP-Adresse oder lokale ID des IPsec-Clients ein. Wenn er leer bleibt<br>leer gelassen wird, können alle Clients diesen PSK zur Authentifizierung verwenden. |
| PSK | Definieren Sie den vorab geteilten Schlüssel. |
| **IPsec erweitert** | |
| Komprimierung aktivieren | Der Kopf des IP-Pakets wird nach der Aktivierung komprimiert. |
| Margintime | Legen Sie eine erweiterte Zeit vor Ablauf der Lebensdauer fest, um die<br>Neuverhandlung zu beginnen. |
| Expertenoptionen | Der Benutzer kann in diesem Feld einige andere Initialisierungszeichenfolgen eingeben, um zusätzliche<br>Einstellungen und trennen Sie die Zeichenfolgen durch Semikolons. |

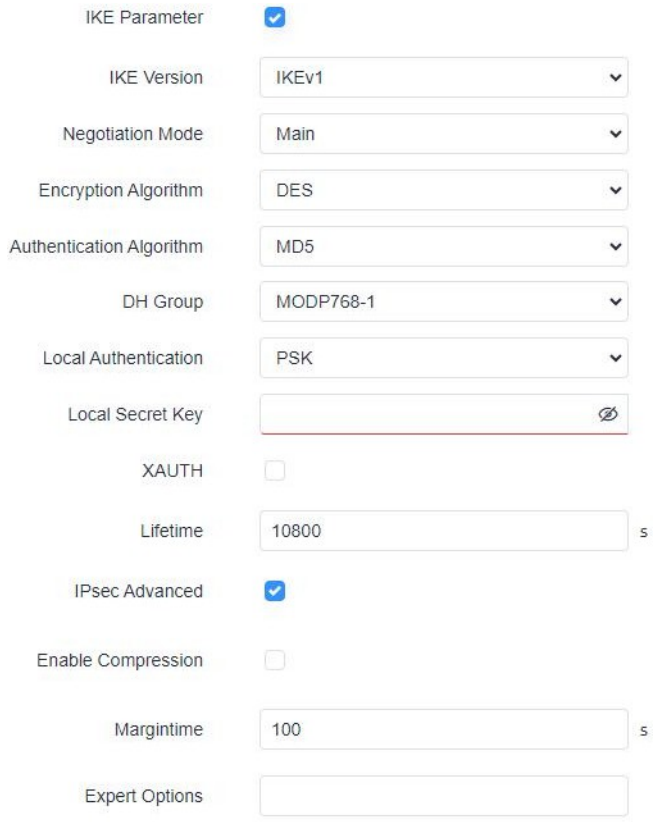
#### 6.3.2.2 IPSec-Client

UR75 unterstützt die gleichzeitige Ausführung von maximal 3 IPSec-Clients.




| IPSec-Client | |
|---|---|
| **Element** | **Beschreibung** |
| Aktivieren | Aktivieren oder deaktivieren Sie den IPsec-Client-Modus. Es sind maximal 3 Tunnel sind zulässig. |
| IP-Gateway-Adresse | Geben Sie die Adresse des Remote-IPsec-Servers ein. |
| IPsec-Modus | Wählen Sie „Tunnel“ oder „Transport“. |
| IPsec-Protokoll | Wählen Sie „ESP“ oder „AH“. |
| Lokales Subnetz | Geben Sie die IP-Adresse des lokalen LAN-Subnetzes im IPsec-Tunnel ein. |
| Netzmaske des lokalen Subnetzes | Geben Sie die lokale LAN-Netzmaske im IPsec-Tunnel ein. |
| Lokaler ID-Typ | Wählen Sie den Identifizierungstyp aus, der an den Remote-Peer gesendet werden soll.<br>**Standard:** Keine<br>**ID:** Verwenden Sie die lokale Subnetz-IP-Adresse als ID<br>**FQDN:** Vollständig qualifizierter Domänenname,Beispiel: test.user.com<br>**Benutzer-FQDN:** Vollständig qualifizierte Benutzername-Zeichenfolge im E-Mail-Adressformat, example:test@user.com |
| Remote-Subnetz | Legen Sie das Remote-LAN-Subnetz fest, das sich im IPsec-Tunnel befindet. |
| Remote-Subnetzmaske | Geben Sie die Remote-LAN-Netzmaske für den IPsec-Tunnel ein. |

| | |
|---|---|
| Remote-ID-Typ | Wählen Sie den Identifizierungstyp aus, der mit der lokalen ID des Remote-Peers übereinstimmt.<br>**Standard:** Keine<br>**ID:** Remote-Subnetz-IP-Adresse als ID verwenden<br>**FQDN:** Vollständig qualifizierter Domänenname, Beispiel: test.user.com<br>**Benutzer-FQDN:** Vollständig qualifizierte Benutzername-Zeichenfolge im E-Mail-Adressformat, Beispiel: test@user.com |
| SA-Verschlüsselungsalgorithmus | Wählen Sie AES128, AES192 oder AES256. |
| SA-Authentifizierung Algorithmus | Wählen Sie SHA1 oder SHA2-256. |
| PFS-Gruppe | Wählen Sie NULL, MODP768_1, MODP1024_2 oder MODP1536_5. |
| SA-Lebensdauer | Legen Sie die Lebensdauer von IPsec SA fest. Bereich: 60-86400 s. |
| DPD-Intervallzeit | Legen Sie das DPD-Wiederholungsintervall für das Senden von DPD-Anfragen fest. Bereich: 2-60 s |
| DPD-Zeitlimit | Bei Verwendung von IKEv1 legen Sie das DPD-Zeitlimit fest, um den Ausfall der Gegenstelle zu erkennen<br>. Bereich: 10-3600 s. |

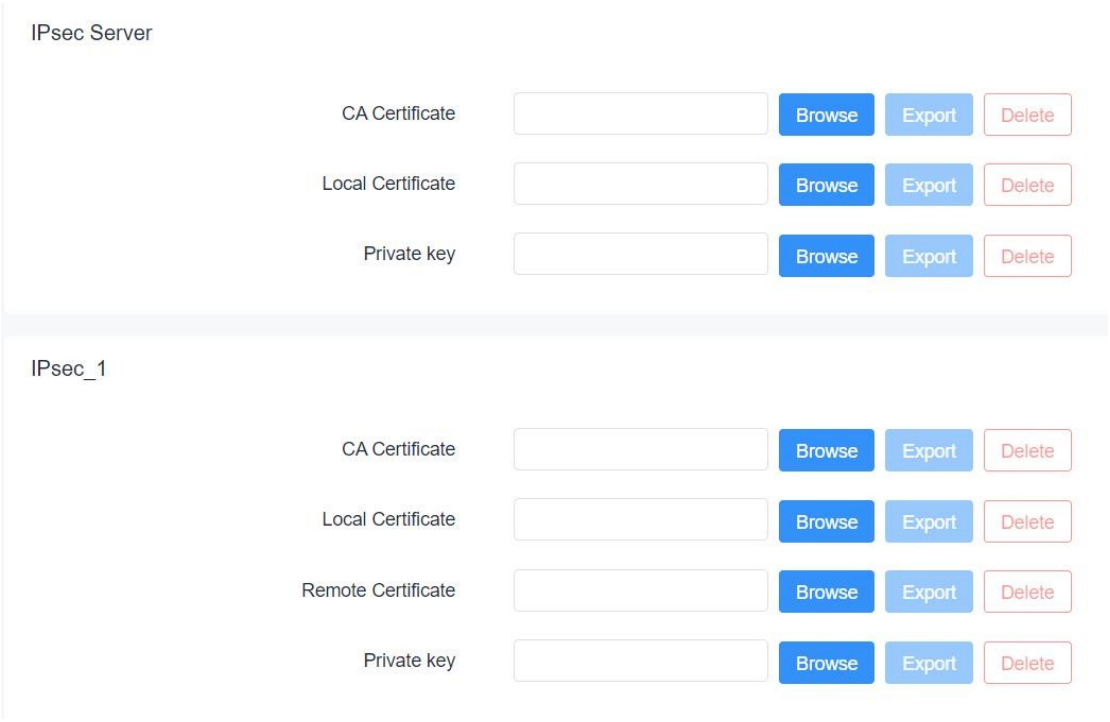



| IKE-Parameter | |
|---|---|
| **Element** | **Beschreibung** |
| IKE-Version | Wählen Sie die Methode für den Schlüsselaustausch von IKEv1 oder IKEv2. |
| Verhandlungsmodus | Bei Verwendung von IKEv1 wählen Sie „Main“ oder „Aggressive“. |
| Verschlüsselungsalgorithmus | Wählen Sie „DES“, „3DES“, „AES128“, „AES192“ oder „AES256“. |
| Authentifizierungsalgorithmus | Wählen Sie MD5, SHA1 oder SHA2-256. |

| | |
|---|---|
| DH-Gruppe | Wählen Sie MODP768_1, MODP1024_2 oder MODP1536_5. |
| Lokale Authentifizierung | Wählen Sie PSK oder CA.<br>**PSK:** Verwenden Sie einen vorab geteilten Schlüssel, um die Authentifizierung abzuschließen.<br>**CA:** Verwenden Sie ein Zertifikat, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite **„VPN > IPsec > Zertifizierungen“**, um das CA-Zertifikat, das lokale Zertifikat und den privaten Schlüssel in die entsprechenden Felder zu importieren. |
| Lokaler geheimer Schlüssel | Geben Sie den vorab geteilten Schlüssel ein, der auf der Serverseite definiert ist. |
| Remote-Authentifizierung | Wählen Sie PSK oder CA.<br>**PSK:** Verwenden Sie einen vorab geteilten Schlüssel, um die Authentifizierung abzuschließen.<br>**CA:** Verwenden Sie ein Zertifikat, um die Authentifizierung abzuschließen. |
| Remote-Schlüssel | Geben Sie den vorab geteilten Schlüssel ein, der auf der Serverseite definiert ist. |
| XAUTH | Bei Verwendung von IKEv1 definieren Sie den XAUTH-Benutzernamen und das Passwort nach<br>XAUTH aktiviert ist. |
| Lebensdauer | Legen Sie die Lebensdauer in der IKE-Verhandlung fest. Bereich: 60-86400 s. |
| **IPsec Advanced** | |
| Komprimierung aktivieren | Der Kopf des IP-Pakets wird nach der Aktivierung komprimiert. |
| Marginalzeit | Legen Sie eine erweiterte Zeit vor Ablauf der Lebensdauer fest, um den Vorgang zu starten.<br>Neuverhandlung. |
| Expertenoptionen | Der Benutzer kann in diesem Feld einige andere Initialisierungszeichenfolgen eingeben, um zusätzliche<br>Einstellungen hinzuzufügen. Die Zeichenfolgen müssen durch Semikolons getrennt werden. |

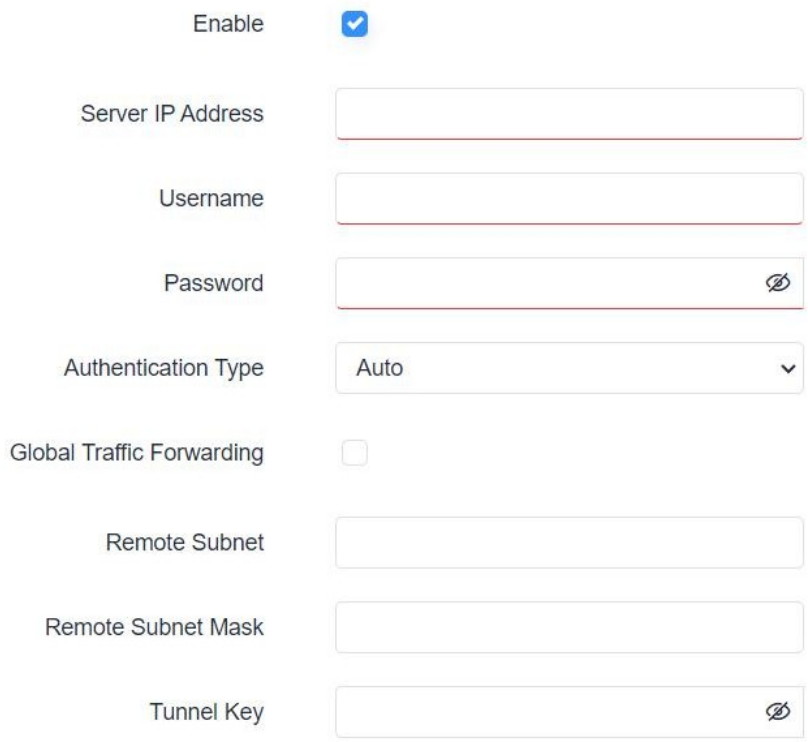
#### 6.3.2.3 Zertifikat

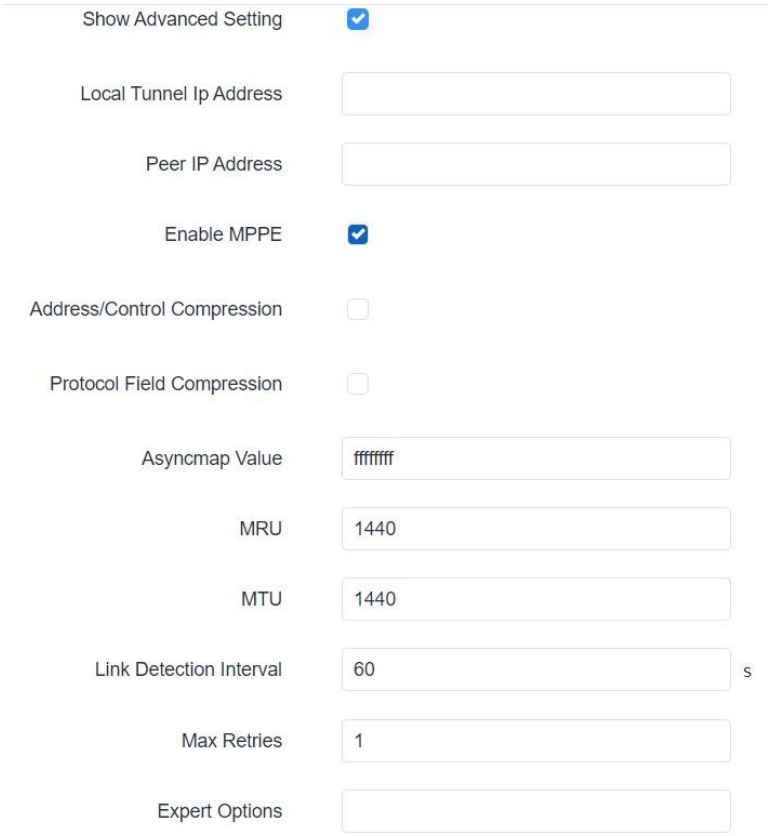
Bei Verwendung der lokalen Authentifizierung des IPsec-Servers oder -Clients als CA kann der Benutzer die erforderlichen Zertifikats- und Schlüsseldateien auf dieser Seite importieren/exportieren.




### 6.3.3 L2TP

Das Layer Two Tunneling Protocol (L2TP) ist eine Erweiterung des Point-to-Point Tunneling Protocol (PPTP), das von Internetdienstanbietern (ISP) verwendet wird, um den Betrieb eines virtuellen privaten Netzwerks (VPN) über das Internet zu ermöglichen.



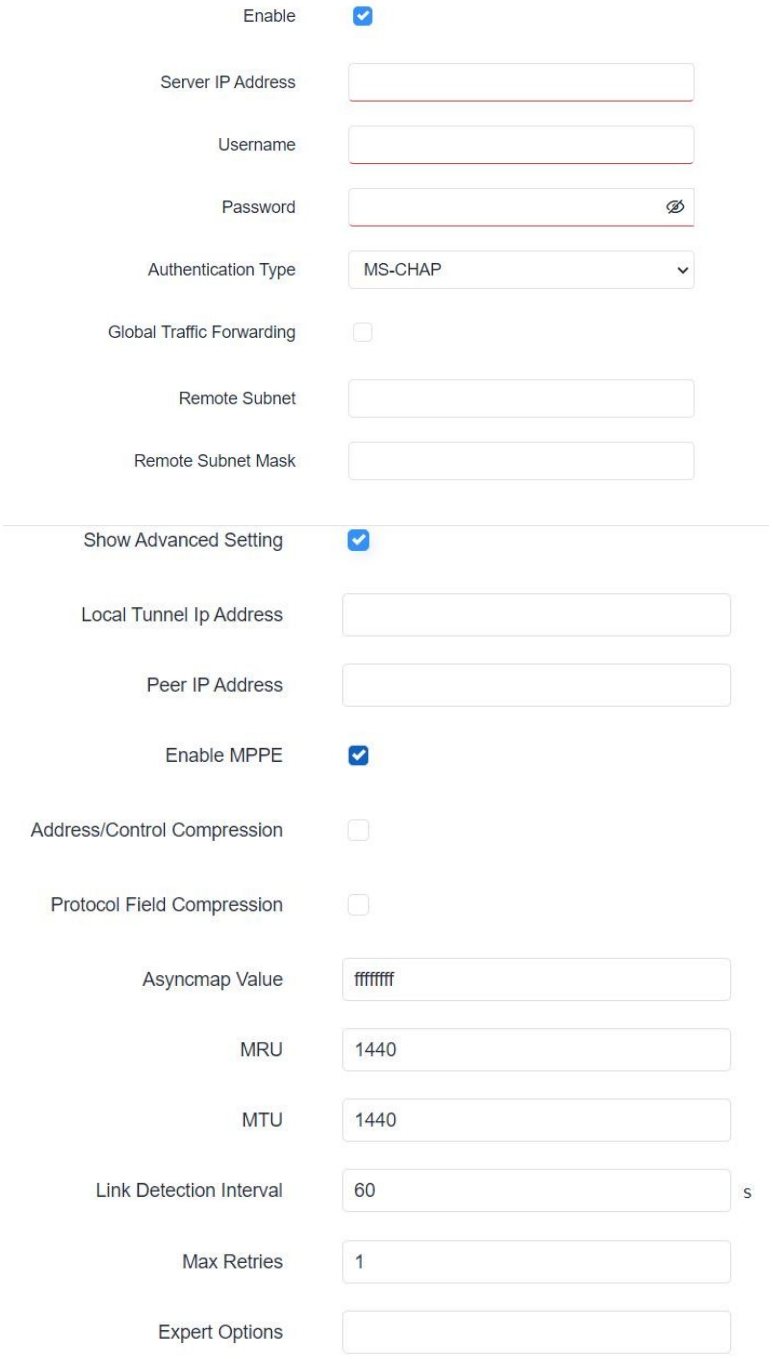



| L2TP | |
|---|---|
| **Element** | **Beschreibung** |
| Aktivieren | L2TP-Client aktivieren oder deaktivieren. |
| Server-IP-Adresse | Geben Sie die IP-Adresse oder den Domänennamen des Remote-L2TP-Servers ein. |
| Benutzername | Geben Sie den Benutzernamen ein, den der L2TP-Server bereitstellt. |
| Passwort | Geben Sie das vom L2TP-Server bereitgestellte Passwort ein. |
| Authentifizierungstyp | Wählen Sie den Authentifizierungstyp aus, der zur Sicherung von Datensitzungen verwendet wird. |
| Globaler Datenverkehr Weiterleitung | Der gesamte Datenverkehr wird über den L2TP-VPN-Tunnel gesendet, wenn diese Funktion aktiviert ist. |
| Remote-Subnetz | Geben Sie das Remote-Subnetz des L2TP-VPN-Servers ein. |
| Remote-Subnetzmaske | Geben Sie die Remote-Netzmaske des L2TP-VPN-Servers ein. |
| Tunnelschlüssel | Geben Sie das Passwort für den L2TP-Tunnel ein. |
| Lokale Tunnel-IP Adresse | Legen Sie die Tunnel-IP-Adresse des L2TP-Clients fest. Der Client erhält die Tunnel-IP-Adresse automatisch vom Server, wenn sie null ist. |
| Peer-IP-Adresse | Geben Sie die Tunnel-IP-Adresse des L2TP-Servers ein. |
| MPPE aktivieren | MPPE (Microsoft Point to Point Encryption) aktivieren oder deaktivieren. |
| Adresse/Steuerung Komprimierung | Für die PPP-Initialisierung. Der Benutzer kann die Standardoption beibehalten. |
| Protokollfeld Komprimierung | Für die PPP-Initialisierung. Der Benutzer kann die Standardoption beibehalten. |
| Asyncmap-Wert | Eine der L2TP-Initialisierungszeichenfolgen. Der Benutzer kann den Standardwert beibehalten. Bereich: 0-ffffffff. |
| MRU | Legt die maximale Empfangseinheit fest. Bereich: 64-1500. |

| | |
|---|---|
| MTU | Legen Sie die maximale Übertragungseinheit fest. Bereich: 68-1500. |
| Link-Erkennungsintervall | Legen Sie das Intervall für die Verbindungserkennung fest, um die Tunnelverbindung sicherzustellen. Bereich:<br>0–600. |
| Expertenoptionen | Der Benutzer kann in diesem Feld einige Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Semikolons trennen. |

### 6.3.4 PPTP

Das Point-to-Point Tunneling Protocol (PPTP) ist ein Protokoll, das einen TCP-Steuerkanal und einen Generic Routing Encapsulation-Tunnel verwendet, um PPP-Pakete zu kapseln.

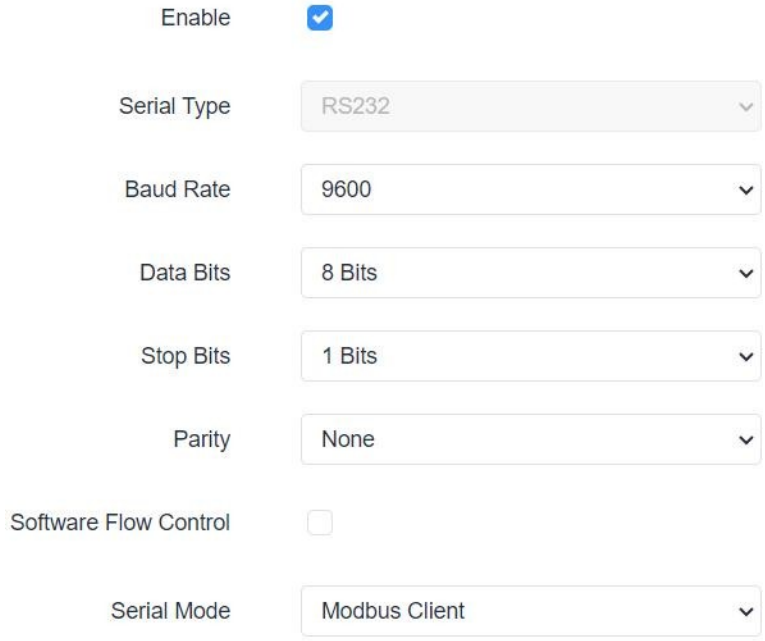


| PPTP | |
|---|---|
| **Element** | **Beschreibung** |
| Aktivieren | Aktivieren oder deaktivieren Sie den PPTP-Client. |
| Server-IP-Adresse | Geben Sie die IP-Adresse oder den Domänennamen des Remote-PPTP-Servers ein. |
| Benutzername | Geben Sie den Benutzernamen ein, den der PPTP-Server bereitstellt. |
| Passwort | Geben Sie das vom PPTP-Server bereitgestellte Passwort ein. |
| Authentifizierungstyp | Wählen Sie den Authentifizierungstyp aus, der zur Sicherung von Datensitzungen verwendet wird. |
| Globaler Datenverkehr Weiterleitung | Der gesamte Datenverkehr wird über einen PPTP-VPN-Tunnel gesendet, wenn diese Funktion aktiviert ist. |
| Remote-Subnetz | Geben Sie das Remote-Subnetz des PPTP-VPN-Servers ein. |
| Remote-Subnetzmaske | Geben Sie die Remote-Netzmaske des PPTP-VPN-Servers ein. |
| Lokale Tunnel-IP Adresse | Legen Sie die Tunnel-IP-Adresse des PPTP-Clients fest. Der Client erhält die Tunnel-IP-Adresse automatisch vom Server, wenn sie null ist. |
| Peer-IP-Adresse | Geben Sie die Tunnel-IP-Adresse des PPTP-Servers ein. |
| MPPE aktivieren | MPPE (Microsoft Point-to-Point-Verschlüsselung) aktivieren. |
| Adresse/Steuerung Komprimierung | Für die PPP-Initialisierung. Der Benutzer kann die Standardoption beibehalten. |
| Protokollfeld Komprimierung | Für die PPP-Initialisierung. Der Benutzer kann die Standardoption beibehalten. |
| Asyncmap-Wert | Eine der PPTP-Initialisierungszeichenfolgen. Der Benutzer kann den Standardwert beibehalten. Bereich: 0-ffffffff. |
| MRU | Legen Sie die maximale Empfangseinheit fest. Bereich: 64-1440. |
| MTU | Legen Sie die maximale Übertragungseinheit fest. Bereich: 68-1440. |
| Link-Erkennungsintervall | Legen Sie das Intervall für die Verbindungserkennung fest, um die Tunnelverbindung sicherzustellen. Bereich: 0–600. |
| Maximale Wiederholungsversuche | Legen Sie die maximale Anzahl der Wiederholungsversuche fest, um den Ausfall der PPTP-Verbindung zu erkennen. Bereich: 0-10. |
| Expertenoptionen | Der Benutzer kann in diesem Feld einige Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Semikolons trennen. |

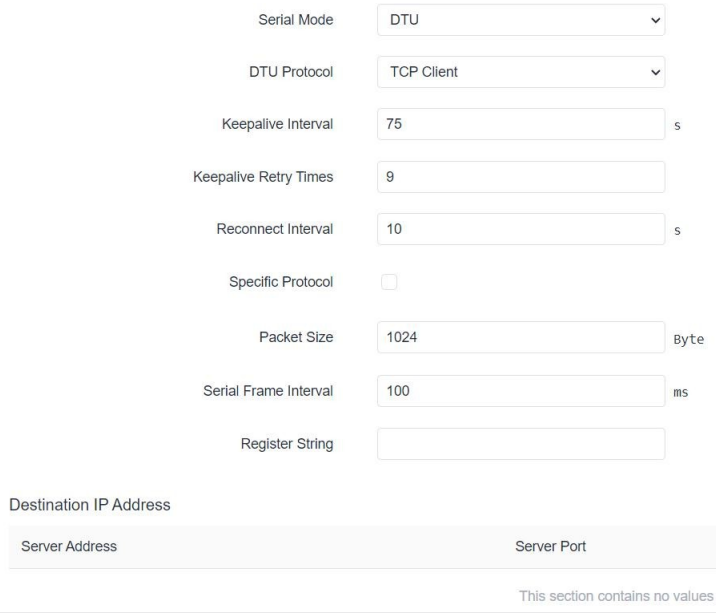
## 6.4 Dienst

### 6.4.1 Serielle Schnittstelle

In diesem Abschnitt wird erläutert, wie Sie die Parameter der seriellen Schnittstelle konfigurieren, um die Kommunikation mit seriellen Terminals herzustellen, und wie Sie den Arbeitsmodus konfigurieren, um die Kommunikation mit den Remote-Rechenzentren herzustellen, sodass eine bidirektionale Kommunikation zwischen seriellen Terminals und Remote-Rechenzentren möglich ist.




| Serielle Einstellung | | |
|---|---|---|
| **Element** | **Beschreibung** | **Standard** |
| Aktivieren | Serielle Schnittstelle aktivieren oder deaktivieren. | Deaktivieren |
| Serieller Typ | Der serielle Anschluss 1 ist ein RS232-Anschluss und der serielle Anschluss 2 ist ein RS485-Anschluss. | -- |
| Baudrate | Der Bereich liegt zwischen 300 und 230400. Entspricht der Baudrate des angeschlossenen Endgerätes. | 9600 |
| Datenbits | 8 Bit oder 7 Bit optional. Entspricht den Datenbits des angeschlossenen Endgerät. | 8 |
| Stoppbits | 1 Bit oder 2 Bit optional. Gleich wie bei den Stoppbits des angeschlossenen Endgerät. | 1 |
| Parität | Die Optionen sind „Keine“, „Ungerade“ und „Gerade“. Das Gleiche gilt für die Parität des angeschlossenen Endgeräts. | Keine |
| Software-Ablauf Steuerung | Aktivieren oder deaktivieren Sie die Software-Flusskontrolle. | Deaktivieren |
| Serieller Modus | Wählen Sie den Arbeitsmodus der seriellen Schnittstelle aus.<br>**DTU-Modus:** Im DTU-Modus kann die serielle Schnittstelle eine Kommunikation mit dem Remote-Server/Client herstellen.<br>**GPS:** Im GPS-Modus gehen Sie zu **„Service“ > „GPS“ > „GPS Serial Forwarding“**, um die grundlegenden Parameter für die Übertragung von GPS-Daten an die serielle Schnittstelle zu konfigurieren.<br>**Modbus-Client:** Im Modbus-Client-Modus gehen Sie zu **„Service“ > „Modbus-Client“**, um grundlegende Parameter und Kanäle zu konfigurieren. | Deaktivieren |




| DTU-Modus | | |
|---|---|---|
| **Element** | **Beschreibung** | **Standard** |
| DTU-Protokoll | Wählen Sie aus den folgenden Protokollen aus:<br>**TCP-Client:** Der Router wird als TCP-Client verwendet und überträgt Daten transparent an den TCP-Server.<br>**UDP-Client:** Der Router wird als UDP-Client verwendet und überträgt Daten transparent an den UDP-Server.<br>**TCP-Server:** Der Router wird als TCP-Server verwendet, um auf Abfragedaten zu warten.<br>**UDP-Server:** Der Router wird als UDP-Server verwendet, um auf Abfragedaten zu warten.<br>**Modbus:** Der Router wird als Modbus-Gateway verwendet, das die Konvertierung zwischen Modbus RTU und Modbus TCP ermöglicht.<br>**Node-RED:** Der Router leitet die Daten an den seriellen Eingangs-Knoten weiter, wenn Node-RED installiert ist.<br>**MQTT:** Der Router wird als MQTT-Client verwendet, um Daten an den MQTT-Broker weiterzuleiten oder den Downlink an den seriellen Port weiterzuleiten. | -- |
| **TCP/UDP-Server** | | |
| Lokaler Port | Legen Sie den lokalen Port dieses TCP/UDP-Servers fest. Bereich: 1-65535. | 502 |
| Keepalive Intervall | Nachdem die TCP-Verbindung hergestellt wurde, sendet der Client regelmäßig Heartbeat-Pakete, um die Verbindung aufrechtzuerhalten. Der Intervallbereich liegt zwischen 1 und 3600 Sekunden. | 75 |
| Maximale Wiederholungsversuche | Wenn der TCP-Heartbeat-Zeitüberschreitung erreicht ist, sendet der Router den Heartbeat erneut. Nachdem die voreingestellte Anzahl an Wiederholungsversuchen erreicht ist, wird die TCP-Verbindung neu aufgebaut. Der Bereich für die Wiederholungsversuche liegt zwischen 1 und 16. | 9 |
| Paketgröße | Legen Sie die Größe des seriellen Datenrahmens fest. Das Paket wird gesendet, wenn die voreingestellte Rahmengröße die Grenze erreicht. Der Größenbereich liegt zwischen 1 und 1024 Byte. | 1024 |
| Serielles Rahmenintervall | Das Intervall, in dem der Router die im Pufferbereich gespeicherten realen seriellen Daten an das öffentliche Netzwerk sendet. Der Bereich liegt zwischen 10 und 65535 ms.<br>**Hinweis:** Die Daten werden an das öffentliche Netzwerk gesendet, wenn die Größe der tatsächlichen seriellen Daten die voreingestellte Paketgröße erreicht, auch wenn sie innerhalb der seriellen | 100 |

| | | |
|---|---|---|
| | -Rahmenintervall liegen. | |
| **TCP/UDP-Client** | | |
| Keepalive-Intervall | Nachdem der TCP-Client mit dem TCP-Server verbunden ist, sendet der Client regelmäßig Heartbeat-Pakete über TCP, um die Verbindung aufrechtzuerhalten. Der Intervallbereich liegt zwischen<br>1–3600 s. | 75 |
| Keepalive-Wiederholungszeiten | Wenn die TCP-Heartbeat-Zeiten abgelaufen sind, sendet der Router den Heartbeat erneut. Nachdem die voreingestellten Wiederholungsversuche erreicht sind, stellt der Router die Verbindung zum TCP-Server wieder her<br>. Der Bereich liegt zwischen 1 und 16. | 9 |
| Wiederverbindungsintervall<br>Intervall | Wenn die Verbindung fehlschlägt, stellt der Router die Verbindung zum Server erneut her, und zwar im<br>Voreingestelltes Intervall. Der Bereich liegt zwischen 10 und 60 Sekunden. | 10 |
| Spezifisches Protokoll | Mit dem spezifischen Protokoll kann der Router eine Verbindung zur<br>TCP2COM-Software verbinden. | Deaktivieren |
| Heartbeat Intervall | Mit einem bestimmten Protokoll sendet der Router regelmäßig Heartbeat-Pakete an den Server, um die Verbindung aufrechtzuerhalten. Der Intervallbereich liegt zwischen 1 und 3600 Sekunden. | 30 |
| ID | Definieren Sie eine eindeutige ID für jeden Router. Diese darf nicht länger als 63 Zeichen sein und<br>enthalten keine Leerzeichen. | -- |
| Paketgröße | Legen Sie die Größe des seriellen Datenrahmens fest. Das Paket wird gesendet, wenn die voreingestellte Rahmengröße erreicht ist. Der Bereich liegt zwischen 1 und 1024 Byte. | 1024 |
| Serielles Frame-Intervall | Das Intervall, in dem der Router die im Pufferbereich gespeicherten realen seriellen Daten an das öffentliche Netzwerk sendet. Der Bereich liegt zwischen 10 und 65535 ms.<br>**Hinweis:** Die Daten werden an das öffentliche Netzwerk gesendet, wenn die Größe der tatsächlichen seriellen Daten die voreingestellte Paketgröße erreicht, auch wenn sie innerhalb des seriellen Bereichs liegt.<br>Rahmenintervall. | 100 |
| Registerzeichenfolge | Bei der Einrichtung des UDP-Clients definieren Sie die Registrierungszeichenfolge für die Verbindung mit dem<br>Server. | Null |
| Serveradresse | Geben Sie die TCP- oder UDP-Serveradresse (IP/Domänenname) ein. | Null |
| Server-Port | Geben Sie den TCP- oder UDP-Serverport ein. Bereich: 1-65535. | Null |
| Status | Zeigt den Verbindungsstatus zwischen dem Router und dem Server an. | -- |
| **Modbus** | | |
| Lokaler Port | Legen Sie den Listening-Port des Routers fest. Bereich: 1-65535. | 502 |
| Max. TCP-Clients | Geben Sie die maximale Anzahl von TCP-Clients an, die eine Verbindung zum R<br>, der als TCP-Server fungiert. | 32 |
| Verbindungszeitlimit<br>Zeitüberschreitung | Wenn der TCP-Server innerhalb der Verbindungszeitüberschreitung keine Daten vom Slave-Gerät empfängt<br>innerhalb der Verbindungszeitüberschreitung keine Daten vom Slave-Gerät, wird die TCP-Verbindung unterbrochen. | 60 |
| Leseintervall | Legen Sie das Intervall für das Auslesen der Fernkanäle fest. Wenn ein Lesezyklus endet, beginnt der neue Lesezyklus, bis dieses Intervall abgelaufen ist. Wenn es auf 0 gesetzt ist, startet das Gerät den neuen Lesezyklus neu, nachdem alle Kanäle ausgelesen wurden.<br>. | 100 |
| Zeitüberschreitung bei der Antwort | Legen Sie die maximale Antwortzeit fest, die der Router auf die Antwort auf den Befehl wartet. Wenn das Gerät nach Ablauf der maximalen Antwortzeit keine Antwort erhält, wird davon ausgegangen, dass die Zeit für den Befehl abgelaufen ist<br>. | 3000 |
| Maximale Wiederholungsversuche | Legen Sie die maximale Anzahl von Wiederholungsversuchen fest, nachdem das Lesen fehlgeschlagen ist. | 3 |
| **Node-RED** | | |

| | | |
|---|---|---|
| Paketgröße | Legen Sie die Größe des seriellen Datenrahmens fest. Das Paket wird gesendet, wenn Die voreingestellte Rahmengröße ist erreicht. Der Bereich liegt zwischen 1 und 1024 Byte. | 1024 |
| Serielles Rahmenintervall | Das Intervall, in dem der Router die im Pufferbereich gespeicherten realen seriellen Daten an das öffentliche Netzwerk sendet. Der Bereich liegt zwischen 10 und 65535 ms. **Hinweis:** Die Daten werden an das öffentliche Netzwerk gesendet, wenn die Größe der tatsächlichen seriellen Daten die voreingestellte Paketgröße erreicht, auch wenn sie innerhalb des seriellen Rahmenintervall liegen. | 100 |
| **MQTT** | | |
| Paketgröße | Legen Sie die Größe des seriellen Datenrahmens fest. Das Paket wird gesendet, wenn die voreingestellte Rahmengröße erreicht ist. Der Bereich liegt zwischen 1 und 1024 Byte. | 1024 |
| Serielles Rahmenintervall | Das Intervall, in dem der Router die im Pufferbereich gespeicherten realen seriellen Daten an das öffentliche Netzwerk sendet. Der Bereich liegt zwischen 10 und 65535 ms. **Hinweis:** Die Daten werden an das öffentliche Netzwerk gesendet, wenn die Größe der tatsächlichen seriellen Daten erreicht die voreingestellte Paketgröße, obwohl sie innerhalb des seriellen Rahmenintervalls liegt. | 100 |
| MQTT Verbindung | Wählen Sie die MQTT-Verbindung zum Senden von Daten über die serielle Schnittstelle aus. Diese ist auf der Seite **„Service > MQTT“ eingerichtet.** | Null |
| Typ | Wählen Sie für diese transparente Verbindung „Uplink“ oder „Downlink“. Jeder Typ unterstützt maximal 10 Verbindungen hinzugefügt werden. | Null |
| Thema | Themenname, der für die Veröffentlichung von Daten der seriellen Schnittstelle verwendet wird. | Null |
| Beibehalten | Aktivieren Sie diese Option, um die neueste Nachricht dieses Themas als beibehaltene Nachricht festzulegen. | Null |
| QoS | QoS0, QoS1 oder QoS2 sind optional. | Null |

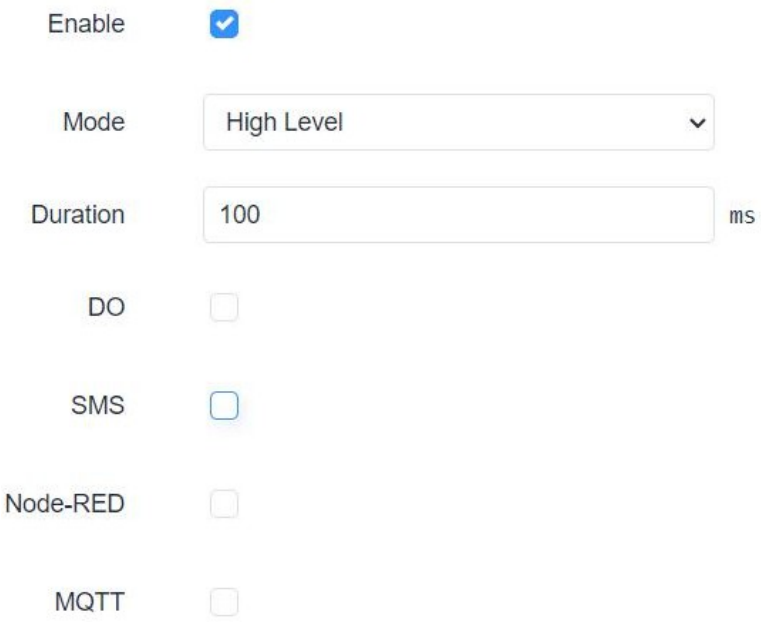
**Beispiel für eine zugehörige Konfiguration**

DTU-Anwendungsbeispiel

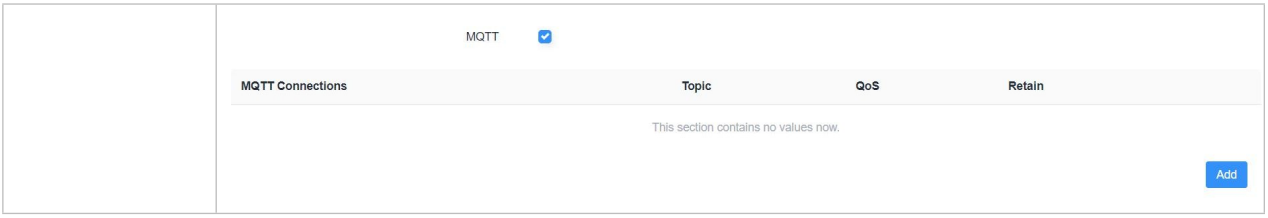
## 6.4.2 E/A

### 6.4.2.1 DI

In diesem Abschnitt wird erläutert, wie Sie Überwachungsbedingungen für digitale Eingänge konfigurieren und bestimmte Aktionen ausführen können, sobald die Bedingungen erfüllt sind.

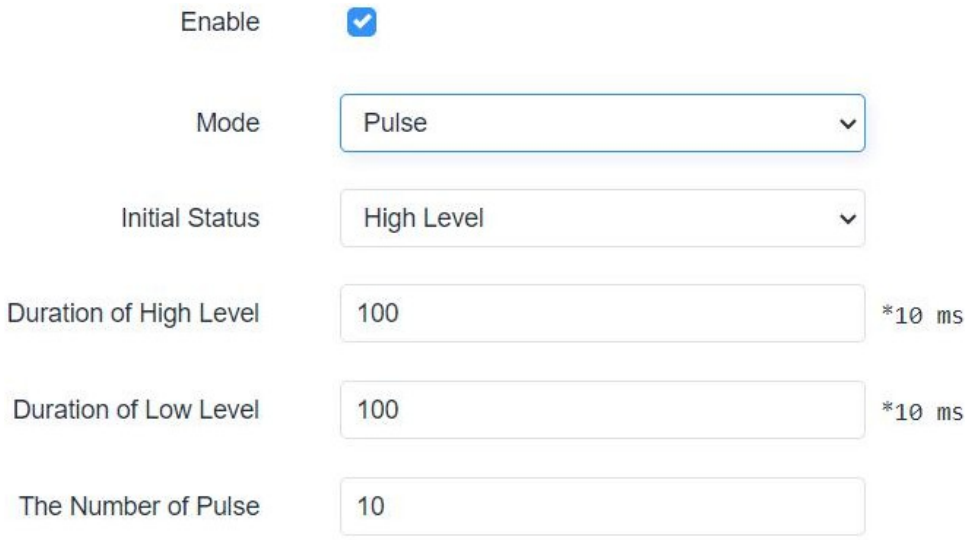



| DI | |
|---|---|
| **Element** | **Beschreibung** |
| Aktivieren | DI aktivieren oder deaktivieren. |
| Modus | Wählen Sie den Arbeitsmodus von DI aus.<br>**Hoher Pegel:** Wenn ein hoher Pegel erkannt wird, wird die Aktion ausgelöst.<br>**Niedriger Pegel:** Wenn ein niedriger Pegel erkannt wird, wird die Aktion ausgelöst.<br>**Zähler:** Wenn ein Impuls erkannt wird, erhöht sich der Zählerwert um 1. |
| Dauer (ms) | Wenn der Modus auf High/Low-Pegel eingestellt ist, legen Sie die Dauer des High/Low-Pegels fest. Bereich: 1-10000. |
| Auslösebedingung | Wenn der Modus auf Zähler eingestellt ist, wählen Sie die Zähler-Auslösebedingung aus.<br>**Niedrig->Hoch:** Der Zählerwert erhöht sich um 1, wenn sich der Status des digitalen Eingangs von niedrigem auf hohen Pegel ändert.<br>**Hoch->Niedrig:** Der Zählerwert erhöht sich um 1, wenn sich der Status des digitalen Eingangs ändert. von hohem Niveau zu niedrigem Niveau. |
| Auslöser Zähler | Das System ergreift entsprechende Maßnahmen, wenn der Zählerwert den voreingestellten Wert erreicht erreicht hat, und setzt dann den Zählerwert auf 0 zurück. Bereich: 1-100. |
| Aktion | Wählen Sie die entsprechenden Maßnahmen aus, die das System ergreifen soll, wenn der digitale Eingangsmodus die voreingestellte Bedingung oder Dauer erfüllt.<br>**DO:** Steuerung des Ausgangsstatus von DO.<br>**SMS:** Wählen Sie die Telefongruppe aus, an die SMS-Alarme gesendet werden sollen.<br>**Node-RED:** Senden Sie den DI-Status an den Knoten „Digital Input“, wenn Node-RED installiert ist.<br>**MQTT**: Aktivieren Sie diese Option, um Nachrichten an den MQTT-Broker zu senden. Die MQTT-Verbindung wird auf der Seite **„Service > MQTT“** eingerichtet. |




### 6.4.2.2 DO

In diesem Abschnitt wird beschrieben, wie Sie den digitalen Ausgabemodus konfigurieren.



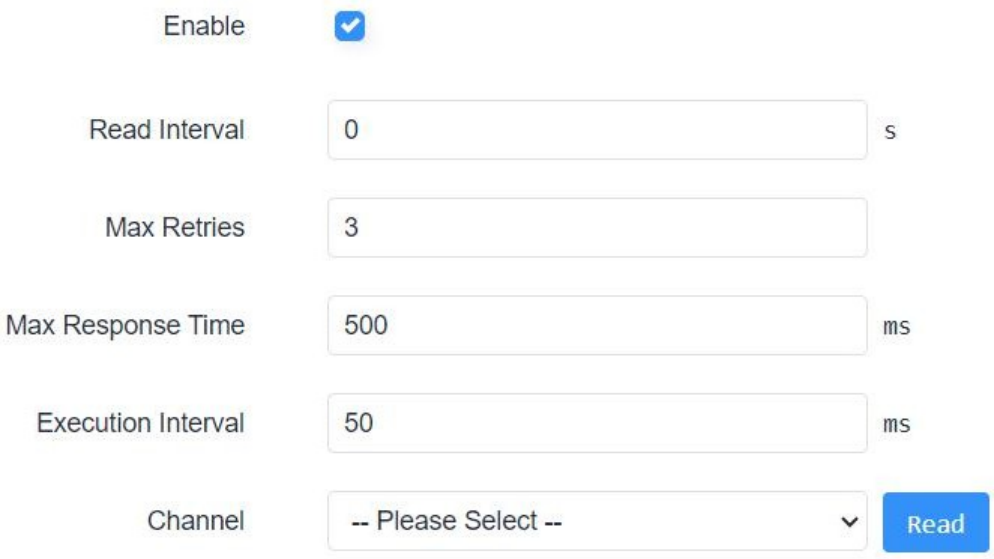

| DO | |
|---|---|
| **Element** | **Beschreibung** |
| Aktivieren | DO aktivieren oder deaktivieren. |
| Modus | Wählen Sie den Arbeitsmodus von DO aus.<br>**High Level:** Löst den DO aus, um ein High-Level-Signal zu senden. **Low Level:** Löst den DO aus, um ein Low-Level-Signal zu senden. **Zähler:** Löst den DO aus, um Impulse zu senden. |
| Anfangszustand | Wählen Sie High Level oder Low Level als Anfangszustand des Impulses. |
| Dauer des hohen Pegels (*10 ms) | Legen Sie die Dauer des hohen Pegels des Impulses fest. Bereich: 1-10000. |
| Dauer des niedrigen Pegels (*10 ms) | Stellen Sie die Dauer des niedrigen Pegels des Impulses ein. Bereich: 1-10000. |
| Anzahl der Impulse | Stellen Sie die Impulsanzahl ein. Bereich: 1-100. |

## 6.4.3 Modbus-Client (Master)

Der UR75-Router kann als Modbus RTU/TCP-Client konfiguriert werden, um den Remote-Modbus-Server abzufragen und Daten an den TCP-Server zu senden.

### 6.4.3.1 Modbus-Client

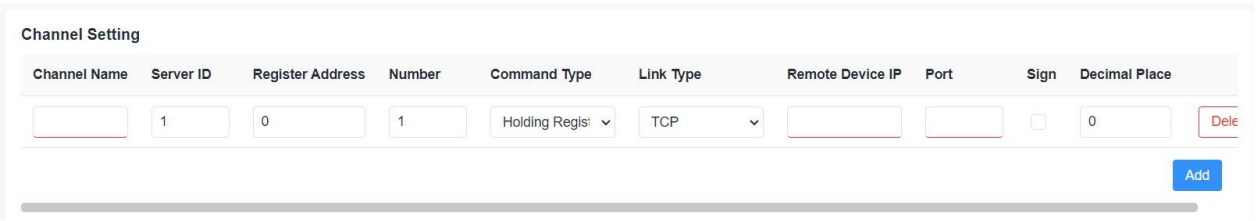
Auf dieser Seite können Sie die Parameter des Modbus-Clients konfigurieren.



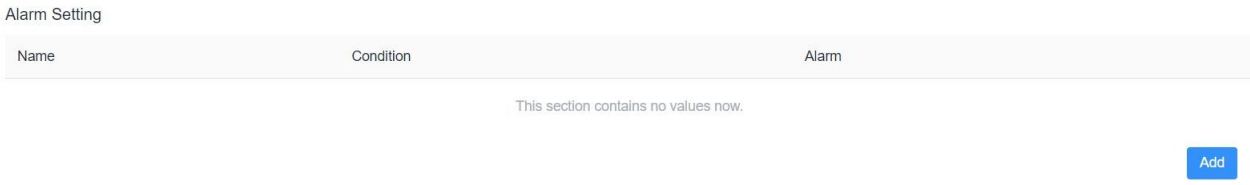

| Modbus-Client | | |
|---|---|---|
| **Element** | **Beschreibung** | **Standard** |
| Aktivieren | Modbus-Master aktivieren/deaktivieren. | -- |
| Leseintervall | Legen Sie das Intervall für das Lesen von Remote-Kanälen fest. Wenn der Lesezyklus endet, werden die Befehle, die nicht gesendet wurden, verworfen und der neue Lesezyklus beginnt. Wenn der Wert auf 0 gesetzt ist, startet das Gerät den neuen Lesezyklus, nachdem alle Kanäle gelesen wurden. Bereich: 0-600 s. | 0 |
| Maximale Wiederholungsversuche | Legen Sie die maximale Anzahl der Wiederholungsversuche fest, wenn das Lesen fehlschlägt, Bereich: 0-5. | 3 |
| Maximale Antwortzeit | Legen Sie die maximale Antwortzeit fest, die der Router auf die Antwort auf den Befehl wartet. Wenn das Gerät nach Ablauf der maximalen Antwortzeit keine Antwort erhält, wird davon ausgegangen , dass die Zeit für den Befehl abgelaufen ist. Bereich: 10-1000 ms. | 500 |
| Ausführungs Intervall | Das Ausführungsintervall zwischen den einzelnen Befehlen. Bereich: 10-1000 ms. | 50 |
| Kanal | Wählen Sie einen lesbaren Kanal aus **„Service > Channel > Kanal.** | -- |

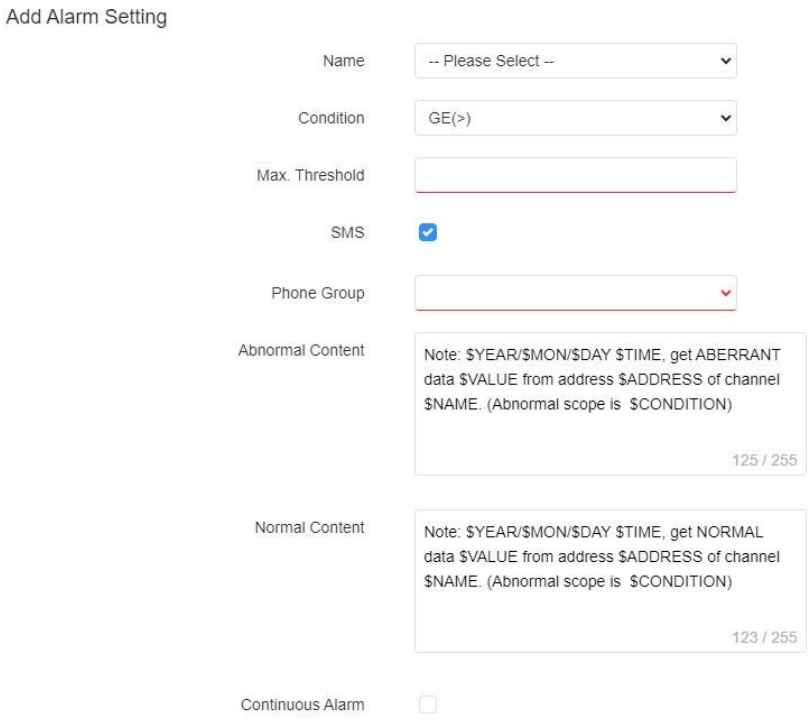
### 6.4.3.2 Kanal

Auf dieser Seite können Sie die Kanäle hinzufügen und die Alarmeinstellungen konfigurieren, um den Router mit dem Remote-Modbus-Server zu verbinden, die Adresse auf dieser Seite abzufragen und Alarme vom Router unter verschiedenen Bedingungen zu empfangen.

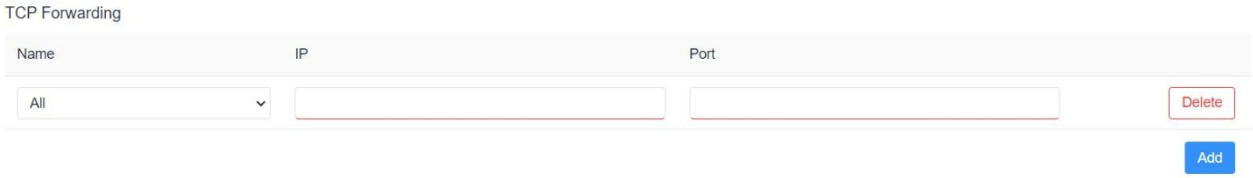


| Kanaleinstellungen | |
|---|---|
| **Element** | **Beschreibung** |
| Kanal Name | Legen Sie den Namen fest, um den Remote-Kanal zu identifizieren. Er darf nicht leer sein. |
| Server-ID | Legen Sie die Modbus-Server-ID fest. |
| Register Adresse | Die Startadresse für das Lesen von Modbus. |
| Nummer | Die Lesemenge ab der Startadresse. |
| Befehl Typ | Lesebefehl-Datentyp, Optionen sind Spule, Diskret, Halteregister (INT16), Eingangsregister (INT16), Halteregister (INT32) und Halteregister (Float). |
| Verbindungstyp | Wählen Sie die serielle Schnittstelle oder die TCP-Verbindung aus.<br>**Serielle Schnittstelle:** Der Router kommuniziert mit Geräten über das Modbus-RTU-Protokoll.<br>**TCP:** Der Router kommuniziert mit Geräten über das Modbus-TCP-Protokoll. |
| Remote Geräte-IP | Wenn die Verbindung TCP ist, geben Sie die IP-Adresse des Remote-Modbus-TCP-Geräts ein. |
| Port | Wenn es sich um eine TCP-Verbindung handelt, geben Sie den Port des entfernten Modbus-TCP-Geräts ein. |
| Zeichen | Wenn der Befehlsdaten-Typ ein Halte-Register oder Eingangsregister ist, aktivieren oder deaktivieren Sie diese Option, um festzulegen, ob dieser Kanal vorzeichenbehaftet ist. |
| Dezimalstelle | Wenn der Befehlsdaten-Typ ein Halte-Register oder Eingangsregister ist, geben Sie einen Punkt im Lesen Sie die Position des Kanals ein. Beispiel: Der gelesene Kanalwert ist 1234 und die Dezimalstelle ist gleich 2, dann ist der tatsächliche Wert 12,34. |

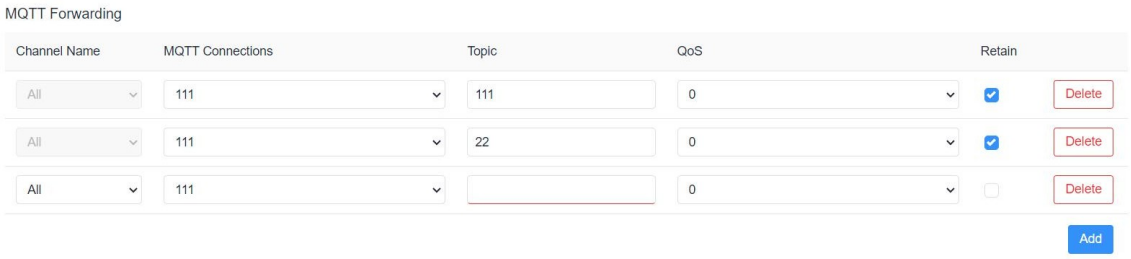





| Alarmeinstellung | |
|---|---|
| **Element** | **Beschreibung** |
| Kanal Name | Wählen Sie den Modbus-Kanal aus. |
| Bedingung | Die Bedingung, die den Alarm auslöst. |
| Min. Schwellenwert | Legen Sie den Mindestwert fest, bei dem der Alarm ausgelöst wird. Wenn der tatsächliche Wert unter diesem Wert liegt, wird der Alarm ausgelöst. |
| Max. Schwellenwert | Stellen Sie den Maximalwert ein, bei dem der Alarm ausgelöst werden soll. Wenn der tatsächliche Wert diesen Wert überschreitet diesem Wert liegt, wird der Alarm ausgelöst. |
| SMS | Aktivieren oder deaktivieren Sie den SMS-Alarm, wenn der Modbus-Kanal die Bedingung erfüllt. |
| Telefon Gruppe | Wählen Sie die Telefongruppe aus, die die Alarm-SMS erhalten soll. Die Telefongruppe kann auf **der Seite „Service > Telefon & SMS > Telefon“** hinzugefügt werden. |
| Anormaler Inhalt | Wenn der tatsächliche Wert die voreingestellte Bedingung erfüllt, löst der Router automatisch den Alarm aus und sendet den voreingestellten abnormalen Inhalt an die angegebene Telefongruppe. |
| Normaler Inhalt | Wenn der tatsächliche Wert nach Überschreiten des Schwellenwert wieder auf den Normalwert zurückkehrt, hebt der Router automatisch den Alarm wegen einer Anomalie auf und sendet den voreingestellten normalen Inhalt an die angegebene Telefongruppe. |
| Kontinuierlich Alarm | Einmal aktiviert, wird derselbe Alarm kontinuierlich gemeldet. Andernfalls Der gleiche Alarm wird nur einmal gemeldet. |



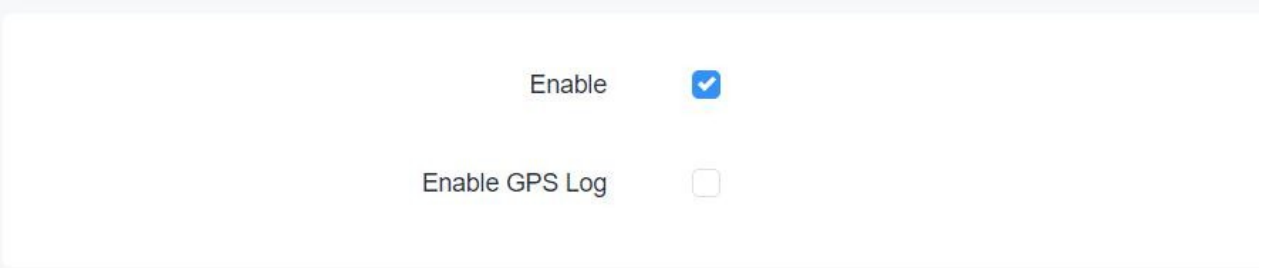

| TCP-Weiterleitung | |
|---|---|
| **Element** | **Beschreibung** |
| Name | Der Name des Kanals des Modbus-Clients. |
| IP | Die IP-Adresse des Servers, an den die Pakete weitergeleitet werden. |
| Port | Der Port des Servers, an den die Pakete weitergeleitet werden. |




| MQTT-Weiterleitung | |
|---|---|
| **Element** | **Beschreibung** |
| Kanal Name | Der Name des Kanals des Modbus-Clients. |
| MQTT Verbindungen | Wählen Sie die MQTT-Verbindung zum Senden von Modbus-Kanaldaten aus. Diese wird auf der Seite **„Service > MQTT“**. |
| Thema | Themenname, der für die Veröffentlichung von Modbus-Kanaldaten verwendet wird. |
| Beibehalten | Aktivieren Sie diese Option, um die neueste Nachricht dieses Themas als beibehaltene Nachricht festzulegen. |
| QoS | QoS0, QoS1 oder QoS2 sind optional. |

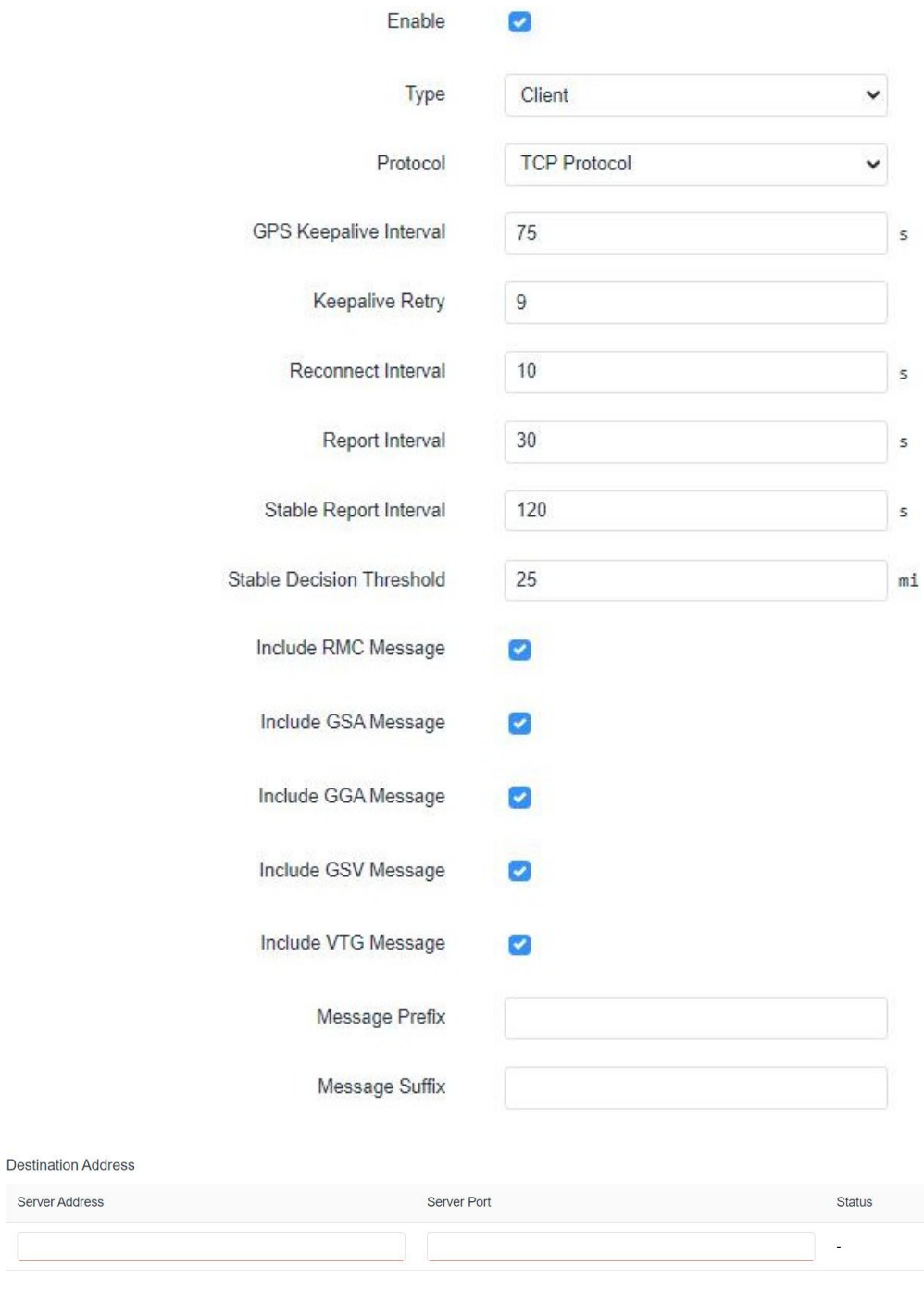
### 6.4.4 GPS

Benutzer können hier die GPS-Funktion aktivieren. Für weitere Debug-Informationen aktivieren Sie bitte auch das GPS-Protokoll.



### 6.4.4.1 GPS-IP-Weiterleitung

GPS-IP-Weiterleitung bedeutet, dass GPS-Daten über das Internet weitergeleitet werden können.

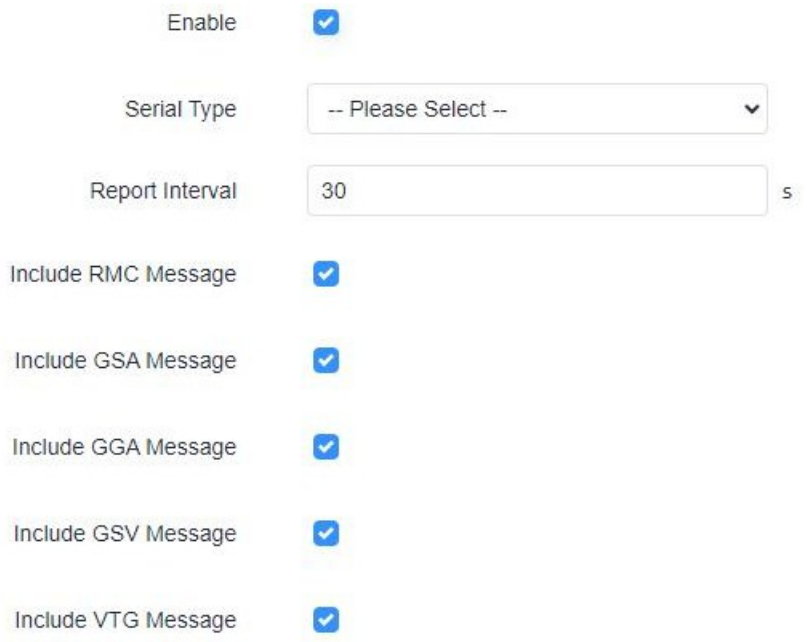



| GPS-IP-Weiterleitung | | |
|---|---|---|
| **Element** | **Beschreibung** | **Standard** |
| Aktivieren | Leiten Sie die GPS-Daten an den Client oder Server weiter. | Deaktivieren |
| Typ | Wählen Sie den Verbindungstyp des Routers als Client oder Server aus. | Client |
| Protokoll | Wählen Sie das Protokoll für die Datenübertragung als TCP oder UDP. | TCP |

| | | |
|---|---|---|
| GPS-Keepalive-Intervall | Wenn das Gerät mit dem Server/Client verbunden ist, sendet es regelmäßig ein Heartbeat-Paket an den Server/Client, um die Verbindung aufrechtzuerhalten. Der Intervallbereich liegt zwischen 1 und 3600 Sekunden. | 75 |
| Keepalive-Wiederholungsversuche | Wenn die TCP-Heartbeat-Zeiten abgelaufen sind, sendet der Router den Heartbeat erneut. Nachdem die voreingestellten Wiederholungszeiten erreicht sind, stellt der Router die Verbindung zum TCP-Server wieder her . Der Bereich liegt zwischen 1 und 16. | 9 |
| Lokaler Port | Legen Sie den Listening-Port des Routers fest, wenn Sie ihn als Server verwenden. Bereich: 1-65535. | |
| Wiederverbinden Intervall | Wenn die Verbindung fehlschlägt, stellt der Router die Verbindung zum Server nach dem voreingestellten Intervall erneut mit dem Server. Der Bereich liegt zwischen 10 und 60 Sekunden. | 10 |
| Meldeintervall | Das Gerät sendet GPS-Daten entsprechend diesem Intervall an den Server/Client, wenn es den stabilen Entscheidungsschwellenwert erreicht. Der Bereich liegt zwischen 1–65535 s. | 30 |
| Stabiles Berichtsintervall | Das Gerät sendet GPS-Daten entsprechend diesem Intervall an den Server/Client, wenn es den stabilen Entscheidungsschwellenwert nicht erreicht. Der Bereich 1–65535 s. | 120 |
| Stabile Entscheidung Schwellenwert | Die GPS-Standortabweichung innerhalb dieser Entfernung kann als unverändert angesehen werden. Der Bereich liegt zwischen 1 und 65535 m. | 25 |
| RMC einbeziehen Nachricht | RMC umfasst Daten zu Uhrzeit, Datum, Position, Kurs und Geschwindigkeit. | Aktivieren |
| GSA einbeziehen Nachricht | GSA enthält den Betriebsmodus des GPS-Empfängers, die für die Positionsbestimmung verwendeten Satelliten und die DOP-Werte. | Aktivieren |
| GGA einschließen Nachricht | GGA umfasst Zeit-, Positions- und Fix-Typ-Daten. | Aktivieren |
| GSV einbeziehen Nachricht | GSV enthält die Anzahl, Höhe und Azimut der GPS-Satelliten sowie SNR-Werte. | Aktivieren |
| VTG einbeziehen Meldung | VTG enthält Kurs- und Geschwindigkeitsinformationen relativ zum Boden. | Aktivieren |
| Meldung Präfix | Fügen Sie den GPS-Daten ein Präfix hinzu. | Null |
| Nachricht Suffix | Fügen Sie den GPS-Daten ein Suffix hinzu. | Null |
| **Zieladresse** | | |
| Server Adresse | Geben Sie die Serveradresse ein, um GPS-Daten zu empfangen (IP/Domänenname). | -- |
| Server-Port | Geben Sie den Server-Port ein, um GPS-Daten zu empfangen. Bereich: 1-65535. | -- |
| Status | Zeigt den Verbindungsstatus zwischen dem Router und dem Server an. | -- |

### 6.4.4.2 GPS-Serienweiterleitung

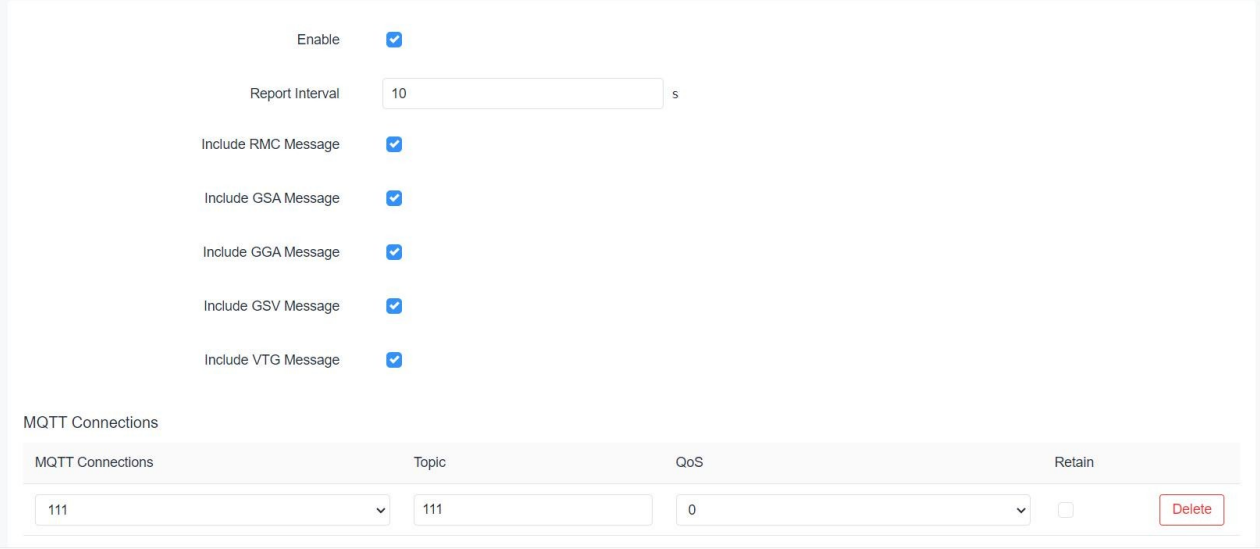
GPS-Serienweiterleitung bedeutet, dass GPS-Daten an den seriellen Anschluss weitergeleitet werden können.




| Serielle GPS-Weiterleitung | | |
|---|---|---|
| **Element** | **Beschreibung** | **Standard** |
| Aktiv | Leitet die GPS-Daten an den voreingestellten seriellen Anschluss weiter. | Deaktivieren |
| Serieller Typ | Wählen Sie den seriellen Anschluss aus, der die GPS-Daten empfangen soll. Stellen Sie sicher, dass der serieller Anschluss unter **„Service > Serieller Anschluss“** aktiviert ist. | -- |
| Berichtsintervall | Das Gerät leitet die GPS-Daten entsprechend diesem Intervall an den seriellen Anschluss weiter gemäß diesem Intervall an den seriellen Anschluss weiter. Der Bereich liegt zwischen 1 und 65535 Sekunden. | 30 |
| RMC einbeziehen Nachricht | RMC umfasst Daten zu Uhrzeit, Datum, Position, Kurs und Geschwindigkeit. | Aktivieren |
| GSA einbeziehen Nachricht | GSA umfasst den Betriebsmodus des GPS-Empfängers,die verwendeten Satelliten in der Positionsbestimmung verwendeten Satelliten und DOP-Werte. | Aktivieren |
| GGA einschließen Nachricht | GGA enthält Zeit-, Positions- und Fix-Typ-Daten. | Aktivieren |
| GSV einbeziehen Nachricht | GSV enthält die Anzahl, Höhe und Azimut der GPS-Satelliten und SNR-Werte. | Aktivieren |
| VTG einbeziehen Nachricht | VTG enthält Kurs- und Geschwindigkeitsinformationen relativ zum Boden. | Aktivieren |

### 6.4.4.3 GPS-MQTT-Weiterleitung

GPS-MQTT-Weiterleitung bedeutet, dass GPS-Rohdaten automatisch an den MQTT-Broker weitergeleitet werden können.

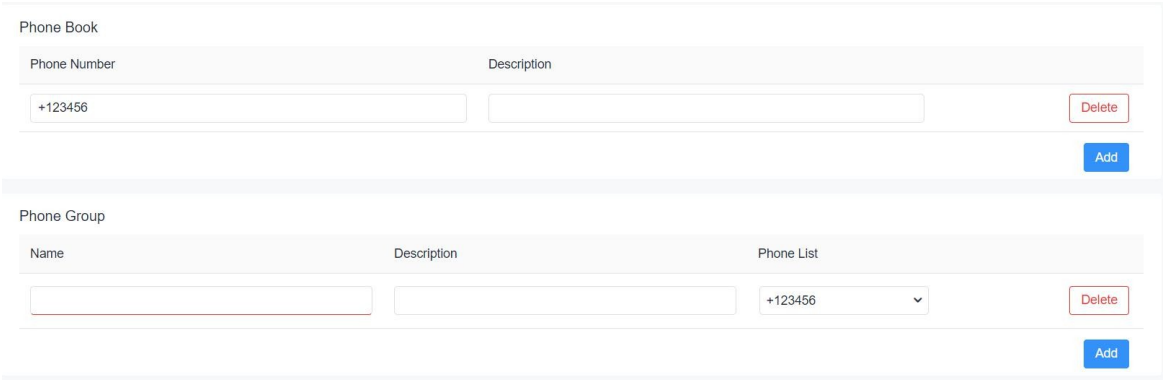



| GPS-MQTT-Weiterleitung | | |
|---|---|---|
| **Element** | **Beschreibung** | **Standard** |
| Aktivieren | Leitet die GPS-Daten automatisch an den MTT-Broker weiter. | Deaktivieren |
| Berichtsintervall | Das Intervall, in dem die GPS-Daten ermittelt und an den MQTT-Broker. Der Bereich liegt zwischen 1 und 60 Sekunden. | 30 |
| RMC einschließen Nachricht | RMC enthält Daten zu Uhrzeit, Datum, Position, Kurs und Geschwindigkeit. | Aktivieren |
| GSA einbeziehen Nachricht | GSA umfasst den Betriebsmodus des GPS-Empfängers,die verwendeten Satelliten für die Positionsbestimmung und die DOP-Werte. | Aktivieren |
| GGA einschließen Nachricht | GGA enthält Zeit-, Positions- und Fix-Typ-Daten. | Aktivieren |
| GSV einbeziehen Nachricht | GSV enthält die Anzahl, Höhe und Azimut der GPS-Satelliten und SNR-Werte. | Aktivieren |
| VTG einbeziehen Nachricht | VTG enthält Kurs- und Geschwindigkeitsinformationen relativ zum Boden. | Aktivieren |
| **MQTT-Verbindungen** | | |
| MQTT Verbindungen | Wählen Sie die MQTT-Verbindung zum Senden von GPS-Daten aus. Diese ist unter **„Service“ > MQTT**-Seite. | |
| Thema | Themenname für die Veröffentlichung von GPS-Rohdaten. | |
| Beibehalten | Aktivieren Sie diese Option, um die neueste Nachricht dieses Themas als Retain-Nachricht festzulegen. | |
| QoS | QoS0, QoS1 oder QoS2 sind optional. | |

## 6.4.5 Telefon & SMS

### 6.4.5.1 Telefon

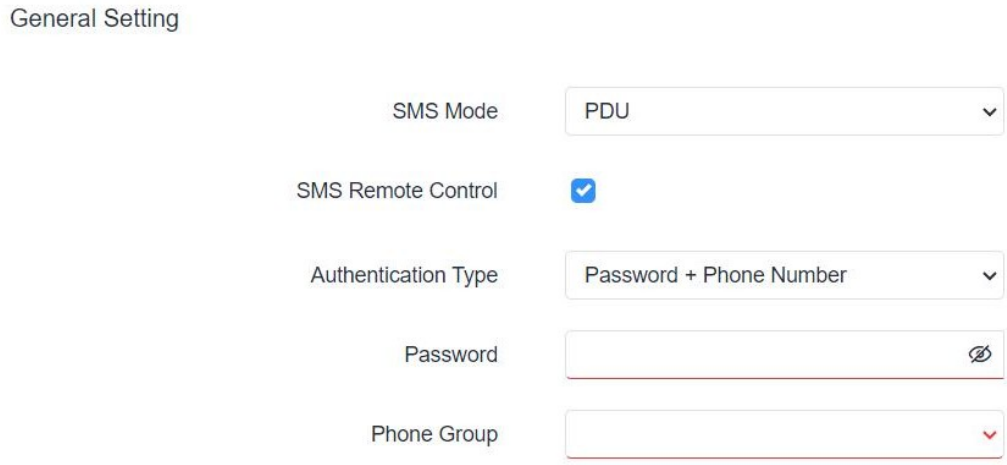
Die Telefoneinstellungen umfassen Anruf-/SMS-Auslöser, SMS-Steuerung und SMS-Alarm für Ereignisse.




| Element | Beschreibung |
|---|---|
| **Telefonbuch** | |
| Telefonnummer | Geben Sie die Telefonnummer ein. Ziffern, „+“ und „-“ sind zulässig. |
| Beschreibung | Die Beschreibung der Telefonnummer. |
| **Telefon-Gruppenliste** | |
| Gruppenname | Name für Telefongruppe festlegen. |
| Beschreibung | Die Beschreibung der Telefongruppe. |
| Telefonliste | Wählen Sie die Telefonnummern für die Liste aus. |

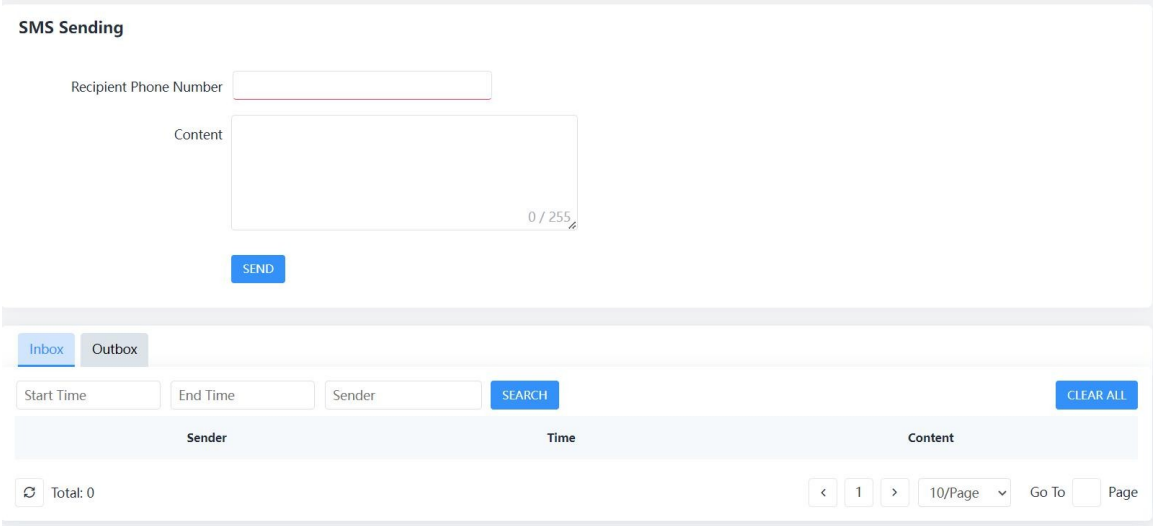
### 6.4.5.2 SMS

Die SMS-Einstellungen umfassen die Fernsteuerung per SMS, das Senden von SMS sowie den Status des SMS-Empfangs und -Versands.




| SMS | |
|---|---|
| **Element** | **Beschreibung** |
| SMS-Modus | Wählen Sie den SMS-Modus:<br>**Text:** Reiner Textmodus, der hauptsächlich in Europa und Amerika verwendet wird. Technisch gesehen kann er auch zum Versenden von Kurznachrichten in chinesischer Sprache verwendet werden.<br>**PDU:** Dies ist der Standard-Kodierungsmodus für Mobiltelefone, der mit dem SMS-Format aller Mobiltelefone kompatibel ist und beliebige Zeichen verwenden kann.<br>mit dem SMS-Format aller Mobiltelefone übereinstimmt und alle Zeichen verwenden kann. |
| SMS-Fernbedienung<br>Steuerung | Aktivieren/Deaktivieren der SMS-Fernsteuerung. Klicken Sie hier, um die SMS-Steuerbefehle zu überprüfen<br>Steuerungsbefehle zu überprüfen. |
| Authentifizierung Typ | Wählen Sie den Authentifizierungstyp, um zu überprüfen, ob die SMS von einem gültigen Controllers stammt. |

| | |
|---|---|
| | **Telefonnummer:** Nur die Telefonnummern in Telefongruppen unterstützen die Fernsteuerung.<br>**Passwort + Telefonnummer:** Nur die Telefonnummern in der Telefongruppe Gruppen unterstützen die Fernsteuerung; außerdem sollte die Steuerungs-SMS im Format „Passwort+";+Befehlsinhalt" gesendet werden. |
| Passwort | Legen Sie ein Passwort für die Authentifizierung fest. |
| Telefongruppe | Wählen Sie die Telefongruppe aus, die für die Fernsteuerung verwendet werden soll. |




| SMS | |
|---|---|
| **Element** | **Beschreibung** |
| **SMS-Versand** | |
| Empfänger-Telefon Nummer | Geben Sie die Nummer ein, an die die SMS gesendet werden soll. |
| Inhalt | Inhalt der SMS. |
| **Posteingang/Postausgang** | |
| Suche | Suche nach SMS-Datensatz. |
| Alle löschen | Löschen Sie die SMS-Eingangs-/Ausgangsbox-Datensätze. |

### 6.4.6 SNMP

SNMP wird häufig im Netzwerkmanagement für die Netzwerküberwachung eingesetzt. SNMP stellt Verwaltungsdaten mit Variablenform im verwalteten System bereit. Das System ist in einer Verwaltungsinformationsbasis (MIB) organisiert, die den Systemstatus und die Konfiguration beschreibt. Diese Variablen können von Verwaltungsanwendungen aus ferngesteuert abgefragt werden.

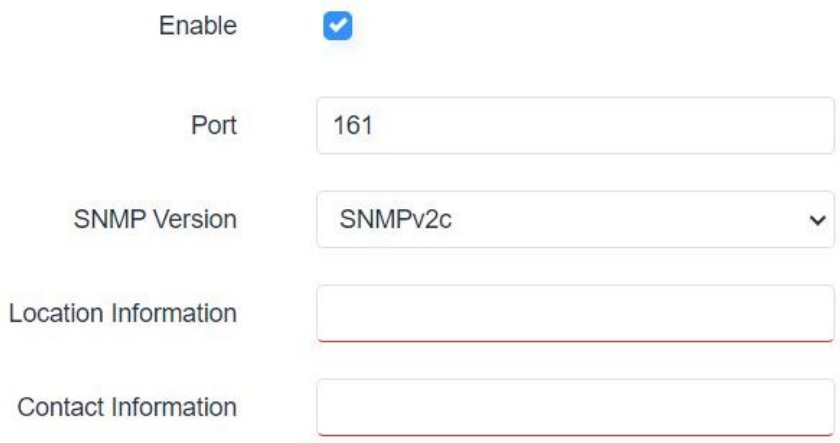
Die Konfiguration von SNMP im Netzwerk, NMS und einem Verwaltungsprogramm von SNMP sollte auf dem Manager eingerichtet werden.

Die Konfigurationsschritte für die Abfrage aus NMS sind nachfolgend aufgeführt:

1. Aktivieren Sie die SNMP-Einstellung.
2. Laden Sie die MIB-Datei herunter und laden Sie sie in NMS.
3. Konfigurieren Sie die MIB-Ansicht.
4. VCAM konfigurieren.

### 6.4.6.1 SNMP

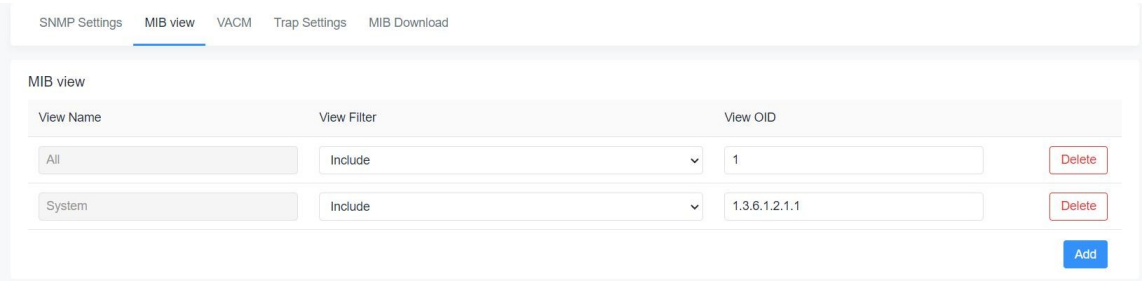
UR75 unterstützt die Versionen SNMPv1, SNMPv2c und SNMPv3. SNMPv3 verwendet eine Authentifizierungsverschlüsselung mit Benutzername und Passwort.




| SNMP-Einstellungen | |
|---|---|
| **Element** | **Beschreibung** |
| Aktivieren | Aktivieren oder deaktivieren Sie die SNMP-Funktion. |
| Port | Legen Sie den SNMP-Port fest. Bereich: 1-65535.<br>Der Standardport ist 161. |
| SNMP-Version | Ist fest auf SNMP v3 eingestellt. |
| Standortinformationen | Geben Sie die Standortinformationen ein. |
| Kontakt | Geben Sie die Kontaktinformationen ein. |

### 6.4.6.2 MIB-Ansicht

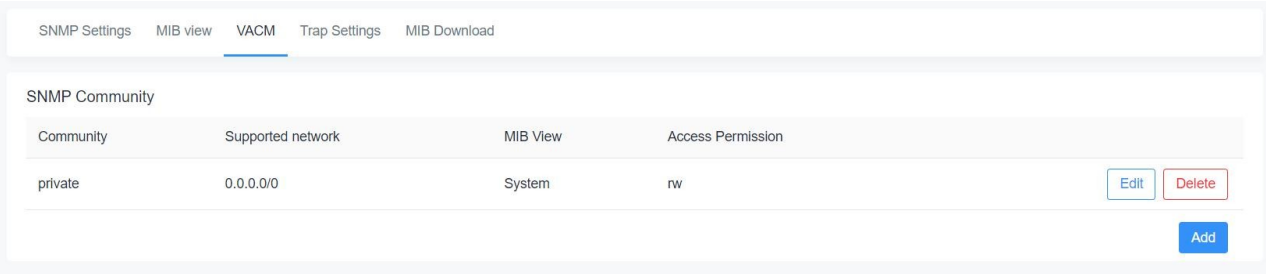
In diesem Abschnitt wird erläutert, wie Sie die MIB-Ansicht für die Objekte konfigurieren.




| MIB-Ansicht | |
|---|---|
| **Artikel** | **Beschreibung** |
| Ansichtsname | Legen Sie den Namen der MIB-Ansicht fest. |
| Ansichtsfilter | Wählen Sie zwischen „Eingeschlossen" und „Ausgeschlossen".<br>Eingeschlossen: Alle Knoten innerhalb des angegebenen MIB-Knotens abfragen.<br>Ausgeschlossen: Alle Knoten außer dem angegebenen MIB-Knoten abfragen. |
| Ansicht-OID | Geben Sie die OID-Nummer ein. |
| Hinzufügen/Löschen | Klicken Sie hier, um eine MIB-Ansicht hinzuzufügen oder zu löschen. |

### 6.4.6.3 VACM

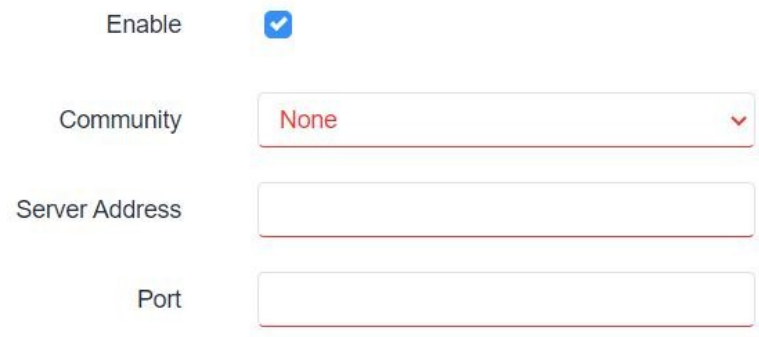
In diesem Abschnitt wird beschrieben, wie Sie VCAM-Parameter konfigurieren.




| VACM | |
|---|---|
| **Element** | **Beschreibung** |
| **SNMP v1 & v2c Unterstütztes Netzwerk** | |
| Community | Legen Sie den Community-Namen fest. |
| IP Adresse/Netzmaske | Der externe IP-Adressbereich für den Zugriff auf diese MIB-Ansicht. |
| MIB-Ansicht | Wählen Sie eine MIB-Ansicht aus der MIB-Ansichtsliste aus, um Berechtigungen festzulegen. |
| Zugriffsberechtigung | Wählen Sie zwischen „Nur Lesen“ und „Lesen/Schreiben“. |
| **SNMP v3-Benutzer** | |
| Benutzername | Legen Sie den Namen des SNMPv3-Benutzers fest. |
| Sicherheitsstufe | Wählen Sie zwischen „Keine“, „Auth/NoPriv“ und „Auth/Priv“. |
| Authentifizierung Algorithmus | Wählen Sie „MD5“ oder „SHA“, wenn „Auth“ ausgewählt ist. |
| Authentifizierung Passwort | Das Passwort muss eingegeben werden. |
| Verschlüsselung Algorithmus | Wählen Sie zwischen „AES” und „DES”, wenn „Auth/Priv” ausgewählt ist. |
| Verschlüsselung Passwort | Das Passwort muss eingegeben werden. |
| Nur-Lesen-Ansicht | Wählen Sie eine MIB-Ansicht aus, um die Berechtigung als „Nur Lesen“ in der MIB-Ansicht festzulegen. . |
| Lese-/Schreibansicht | Wählen Sie eine MIB-Ansicht aus, um die Berechtigung als „Lesen-Schreiben“ aus der MIB-Ansicht . |
| Benachrichtigungsansicht | Wählen Sie eine MIB-Ansicht aus, um die Berechtigung als „Benachrichtigen“ aus der MIB-Ansichtsliste festzulegen. |

### 6.4.6.4 Trap-Einstellungen

In diesem Abschnitt wird erläutert, wie Sie die Netzwerküberwachung durch SNMP-Traps aktivieren können.




| SNMP-Trap | |
|---|---|
| **Element** | **Beschreibung** |
| Aktivieren | Aktivieren oder deaktivieren Sie die SNMP-Trap-Funktion. |
| Community | Wählen Sie die Community von SNMP v1/v2c aus. |
| Benutzer | Wählen Sie den Benutzer von SNMPv3 aus. |
| Serveradresse | Geben Sie die IP-Adresse oder den Domänennamen des NMS ein. |
| Port | Geben Sie den UDP-Port ein. Der Portbereich liegt zwischen 1 und 65535. |

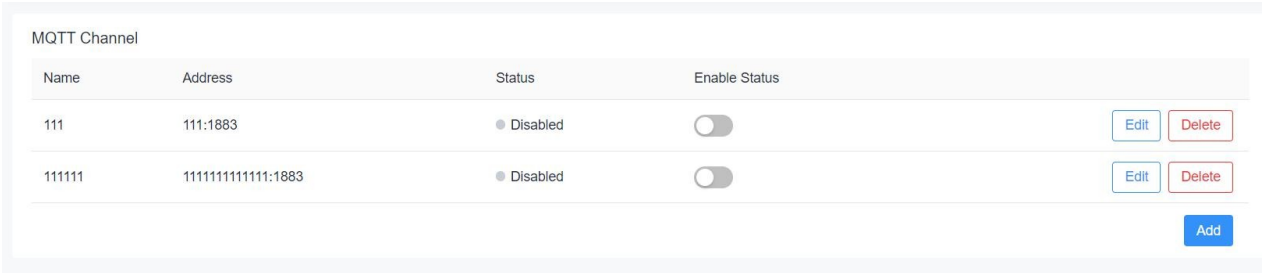
#### 6.4.6.5 MIB-Download

In diesem Abschnitt wird beschrieben, wie Sie MIB-Dateien herunterladen können.


### 6.4.7 MQTT

Das Gerät unterstützt die Funktion als MQTT-Client, um Daten und Router-Informationen auf zwei Arten an den MQTT-Broker weiterzuleiten:

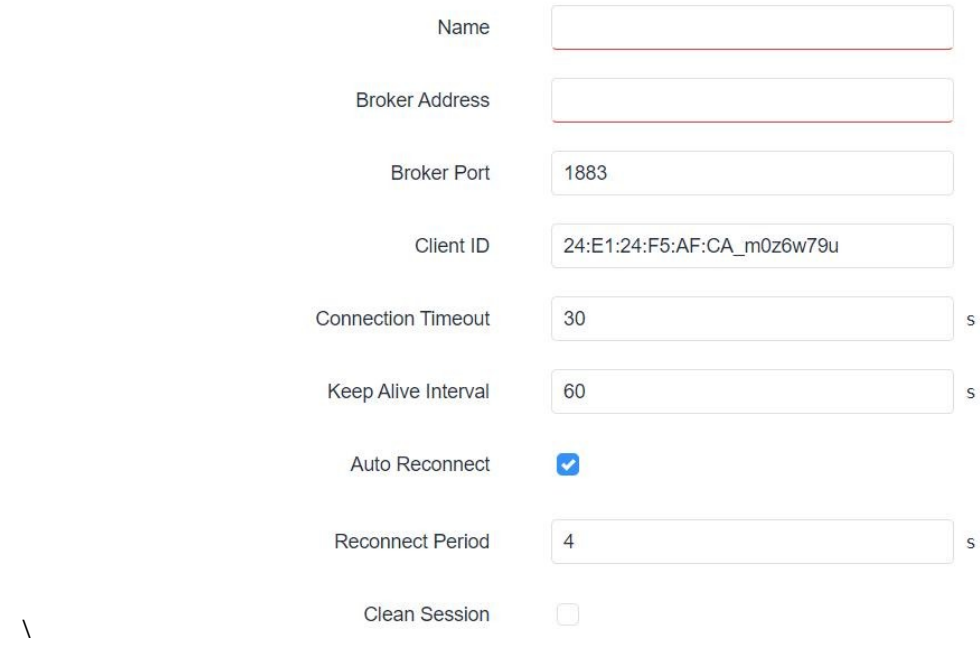
1. Benutzer senden Anfragen an den Router, um die Routerinformationen abzufragen.
2. Der Router veröffentlicht die Daten automatisch.




| MQTT-Kanal | |
|---|---|
| **Element** | **Beschreibung** |
| Name | Der eindeutige Name des MQTT-Kanals. |
| Adresse | Adresse und Port des MQTT-Brokers zum Empfang von Daten. |
| Status | Zeigt den Verbindungsstatus zwischen Router und MQTT-Broker an. |
| Status aktivieren | Aktivieren oder deaktivieren Sie diesen MQTT-Kanal. |
| Bearbeiten | Diesen MQTT-Kanal bearbeiten. |

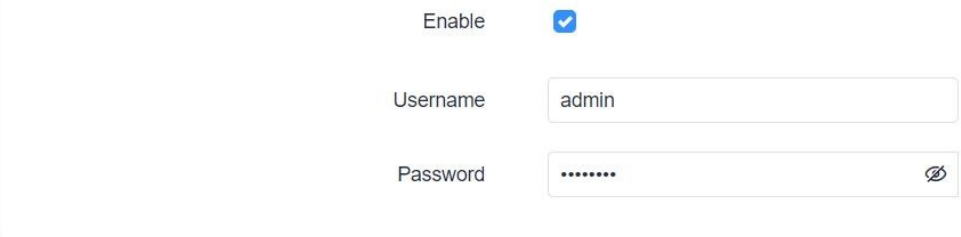
| | |
|---|---|
| Löschen | Löschen Sie diesen MQTT-Kanal. |
| Hinzufügen | Einen neuen MQTT-Kanal hinzufügen. |

**General**

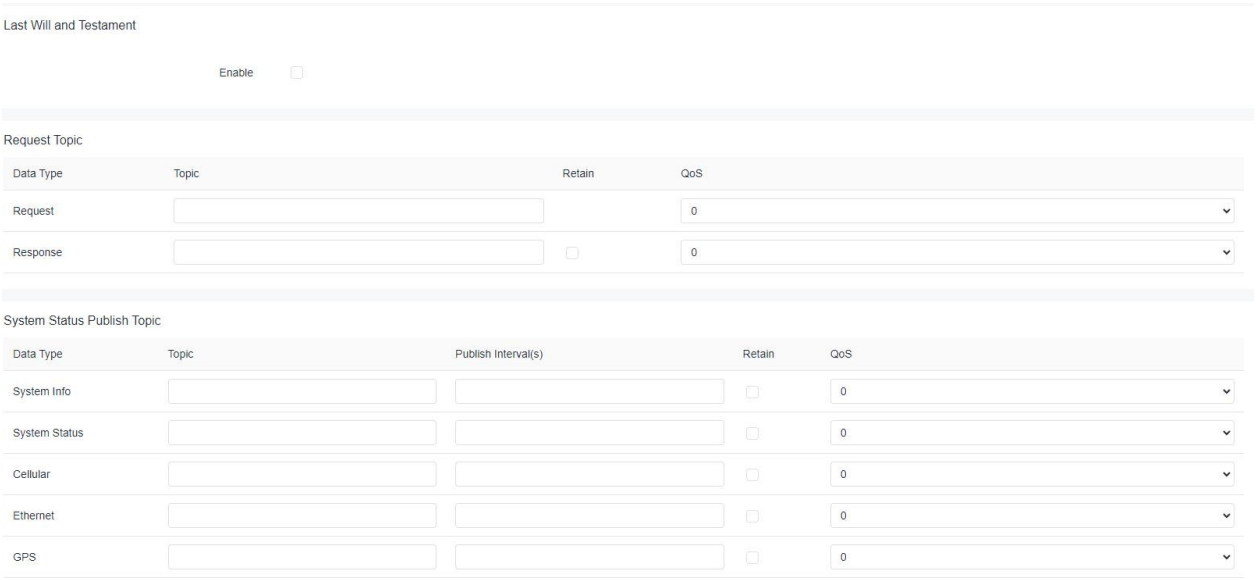



\

**User Credentials**




**TLS**




| MQTT-Einstellungen | |
|---|---|
| **Element** | **Beschreibung** |
| **Allgemein** | |
| Name | Passen Sie einen eindeutigen Verbindungsnamen an. |
| Broker-Adresse | MQTT-Broker-Adresse zum Empfangen von Daten. |
| Broker-Port | MQTT-Broker-Port zum Empfangen von Daten. |
| Client-ID | Die Client-ID ist die eindeutige Identität des Clients gegenüber dem Server. Sie muss eindeutig sein.<br>wenn alle Clients mit demselben Server verbunden sind, und es ist der Schlüssel zur<br>Verarbeitung von Nachrichten mit QoS 1 und 2. |
| Verbindung Zeitüberschreitung/s | Wenn der Client nach Ablauf des Verbindungszeitlimits keine Antwort erhält,<br>Verbindung als unterbrochen betrachtet. Der Bereich: 1-65535. |
| Keep Alive Intervall/s | Nachdem der Client mit dem Server verbunden ist, sendet der Client regelmäßig Heartbeat-Pakete<br>Paket an den Server, um die Verbindung aufrechtzuerhalten. Bereich: 1-65535. |
| Auto Wiederverbinden | Wenn die Verbindung unterbrochen wird, versuchen Sie, die Verbindung zum Server automatisch wiederherzustellen. |
| Wiederverbinden Zeitraum | Wenn die Verbindung unterbrochen wird, wird der Zeitraum für die erneute Verbindung mit dem Server<br>. |
| Sitzung bereinigen | Wenn diese Option aktiviert ist, erstellt die Verbindung eine temporäre Sitzung, und alle Informationen gehen verloren, wenn die Verbindung des Clients zum Broker unterbrochen wird.<br>Wenn diese Option deaktiviert ist, erstellt die Verbindung eine dauerhafte Sitzung, die bestehen bleibt<br>und speichert Offline-Nachrichten, bis die Sitzung nach Ablauf der Zeit abgemeldet wird. |
| **Benutzeranmeldedaten** | |
| Aktivieren | Benutzeranmeldedaten aktivieren. |
| Benutzername | Der Benutzername, der für die Verbindung mit dem MQTT-Broker verwendet wird. |
| Passwort | Das Passwort, das für die Verbindung mit dem MQTT-Broker verwendet wird. |
| **TLS** | |
| Aktivieren | Aktivieren Sie die TLS-Verschlüsselung in der MQTT-Kommunikation. |
| Modus | Wählen Sie zwischen selbstsignierten Zertifikaten und CA-signierten Serverzertifikaten.<br>**Von einer Zertifizierungsstelle signiertes Serverzertifikat:** Überprüfen Sie das vom Gerät vorinstallierte Zertifikat der |

| | |
|---|---|
| | Zertifizierungsstelle (CA) überprüfen, das auf dem Gerät vorinstalliert ist.<br>**Selbstsignierte Zertifikate:** Laden Sie die benutzerdefinierten CA-Zertifikate, Client-Zertifikate und den geheimen Schlüssel zur Überprüfung hoch. |
| **Letzter Wille und Testament** | |
| Aktivieren | Die Last-Will-Nachricht wird automatisch gesendet, wenn die Verbindung zum MQTT-Client abnormal getrennt wird. Sie wird in der Regel verwendet, um Geräte-Statusinformationen zu senden oder andere Geräte oder Proxy-Server über den Offline-Status des Geräts zu informieren . |
| Last-Will-Thema | Passen Sie das Thema an, um Last-Will-Nachrichten zu empfangen. |
| Last-Will-QoS | QoS0, QoS1 oder QoS2 sind optional. |
| Last-Will-Beibehaltung | Aktivieren Sie diese Option, um die Last-Will-Nachricht als Retain-Nachricht festzulegen. |
| Letzter Wille Nutzlast | Passen Sie den Inhalt der Last-Will-Nachricht an. |
| **Anfrage- und Antwortthema** | |
| Thema | Der Router unterstützt das Senden von Anfragen zur Abfrage von Router-Informationen.<br>**Anfrage:** Benutzer können Anfragen an dieses Thema senden, um Router-Informationen abzufragen.<br>Anfrageformat:<br>*{*<br>*"id":"1",*<br>*"status":"systeminfo", „sn":*<br>"64E1213132456",<br>„need_response":1 //1 bedeutet, dass eine Antwort erforderlich ist<br>*}*<br>Die ID ist ein Zufallswert, und der Status kann auf fünf Arten festgelegt werden: systeminfo, systemstatus, cellular, ethernet, gps.<br>**Antwort:** Benutzer können dieses Thema abonnieren, um die Antworten zu erhalten. |
| Beibehalten | Aktivieren Sie diese Option, um die neueste Nachricht dieses Themas als gespeicherte Nachricht festzulegen. |
| QoS | QoS0, QoS1 oder QoS2 sind optional. |
| **Systemstatus-Veröffentlichungsthema** | |
| Datentyp | Datentyp, der automatisch an den MQTT-Broker gesendet wird. Beachten Sie, dass es sich bei den GPS-Daten auf dieser<br>Seite keine Rohdaten, sondern dekodierte Standortdaten sind. |
| Thema | Themenname des für die Veröffentlichung verwendeten Datentyps. |
| Veröffentlichungsintervall (s) | Das Intervall, in dem Daten automatisch an den MQTT-Broker veröffentlicht werden. |
| Beibehalten | Aktivieren Sie diese Option, um die neueste Nachricht dieses Themas als gespeicherte Nachricht festzulegen. |
| QoS | QoS0, QoS1 oder QoS2 sind optional. |

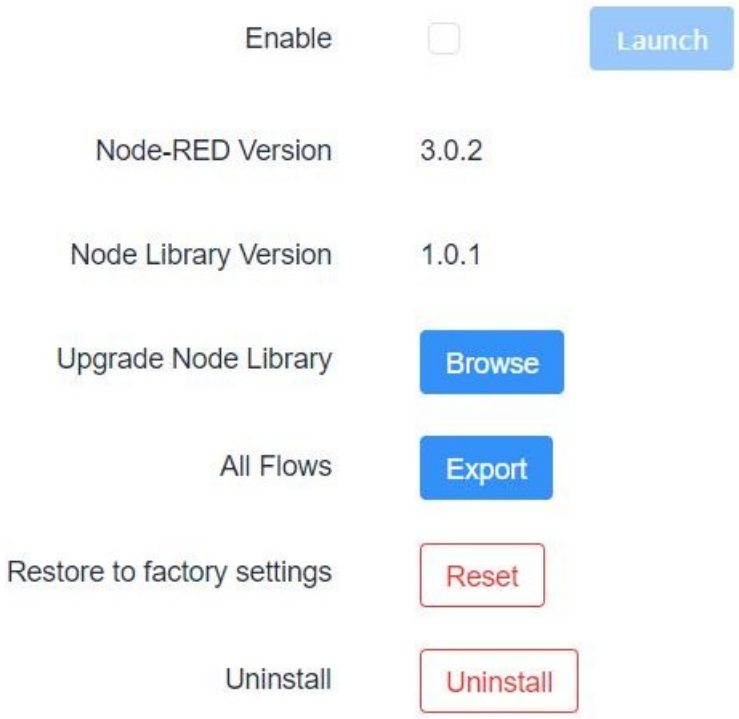
## 6.5 App

### 6.5.1 Node-RED

Node-RED ist ein flussbasiertes Entwicklungstool für die visuelle Programmierung und Verknüpfung von Hardwaregeräten, APIs und Online-Diensten als Teil des Internets der Dinge. Node-RED bietet einen

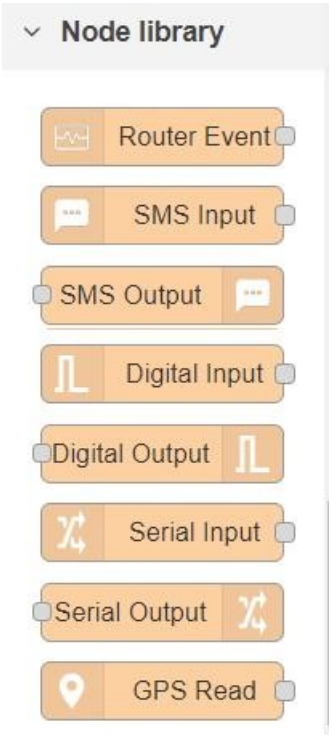
webbrowserbasierten Flusseditor, mit dem sich Flüsse mithilfe der zahlreichen Knoten in der Palette einfach miteinander verbinden lassen. Weitere Anleitungen und Dokumentationen finden Sie auf der offiziellen Website von Node-RED.
Wenn Node-RED nicht installiert ist, laden Sie bitte die Node-RED-App von der Milesight-Website herunter und installieren Sie sie auf dem Gerät.


Nach der Installation wird der folgende Status angezeigt.




| Node-RED | |
|---|---|
| **Element** | **Beschreibung** |
| Aktivieren | Aktivieren Sie Node-RED. |
| Starten | Klicken Sie hier, um die Web-GUI von Node-RED zu starten. Die Anmeldeberechtigung für die Web-GUI von Node RED entspricht der des Admin-Kontos der Web-GUI. |
| Node-RED-Version | Zeigen Sie die Version von Node-RED an. |
| Node-Bibliotheksversion | Zeigt die Version der von Milesight bereitgestellten Node-Bibliothek an. |
| Node-Bibliothek aktualisieren | Aktualisieren Sie die Node-Bibliothek, indem Sie das Bibliothekspaket importieren. |
| Alle Flows exportieren | Alle Flows als JSON-Datei exportieren. |
| Auf Werkseinstellungen zurücksetzen Einstellungen | Löschen Sie alle Flows-Daten von Node-RED. |
| Deinstallieren | Deinstallieren Sie die Node-RED-App von diesem Gerät. |

Milesight bietet eine angepasste Knotenbibliothek zur Verwendung der Schnittstellen des Routers.



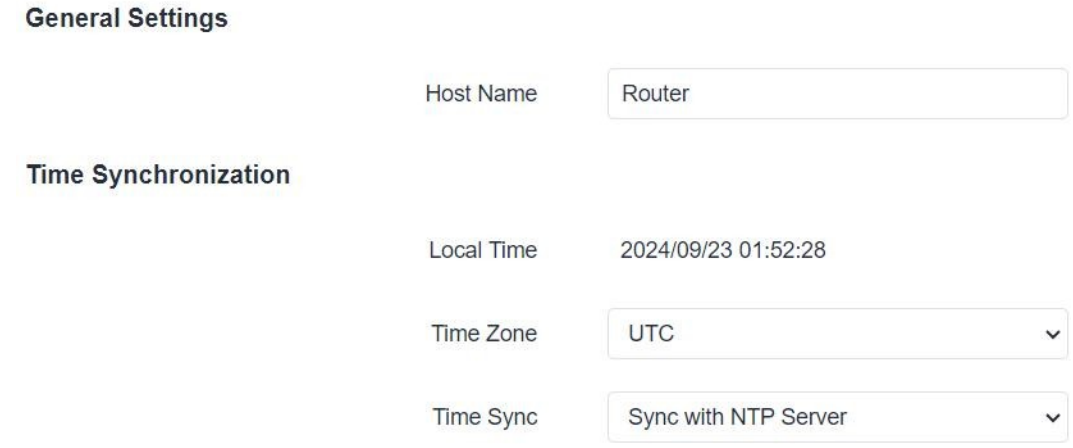

| Knotenbibliothek | |
|---|---|
| **Knoten** | **Beschreibung** |
| Router-Ereignis | Überwachen Sie Alarmereignisse des Geräts. |
| SMS-Eingabe | Empfangen von SMS-Nachrichten. Dies funktioniert nur, wenn das Mobilfunknetz verbunden ist. |
| SMS-Ausgabe | Eine SMS-Nachricht senden. Dies funktioniert nur, wenn das Mobiltelefon verbunden ist. |
| Digitaler Eingang | DI-Status empfangen. Dies funktioniert nur, wenn DI aktiviert ist und die Aktion Node-RED unter **Service > I/O > DI**-Web-GUI. |
| Digitaler Ausgang | DO-Status auslösen. Dies funktioniert nur, wenn DO unter **„Service > I/O > DO** Web-GUI aktiviert ist. |
| Serieller Eingang | Serielle Schnittstellendaten empfangen. Dies funktioniert nur, wenn die serielle Schnittstelle aktiviert ist, der serielle Modus DTU ist und das DTU-Protokoll Node-RED auf **Service > Serieller Anschluss > Serieller Anschluss** Web-GUI. |
| Serielle Ausgabe | Befehl an die serielle Schnittstelle senden. Dies funktioniert nur, wenn die serielle Schnittstelle aktiviert ist, der serielle Modus DTU ist und das DTU-Protokoll Node-RED unter **Service > Serieller Anschluss > Serieller Anschluss** Web-GUI. |
| GPS lesen | GPS-Daten empfangen. Dies funktioniert nur, wenn GPS unter **„Service" > GPS >** GPS-Web-GUI aktiviert ist. |

## 6.6 System

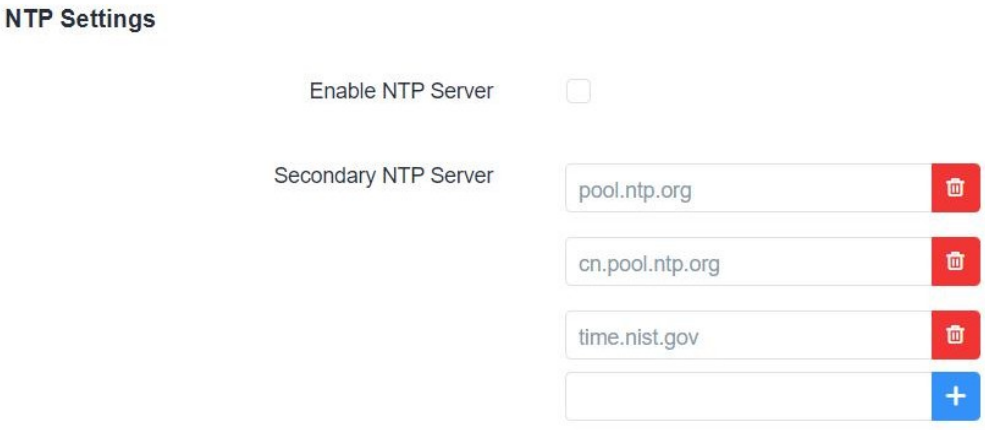
In diesem Abschnitt wird beschrieben, wie Sie allgemeine Einstellungen und Debugging-Funktionen konfigurieren, z. B. Administratorkonto, Systemzeit, allgemeine Benutzerverwaltung, Geräteverwaltung, Download-Protokolle usw.

## 6.6.1 Verwaltung

### 6.6.1.1 Systemeinstellungen



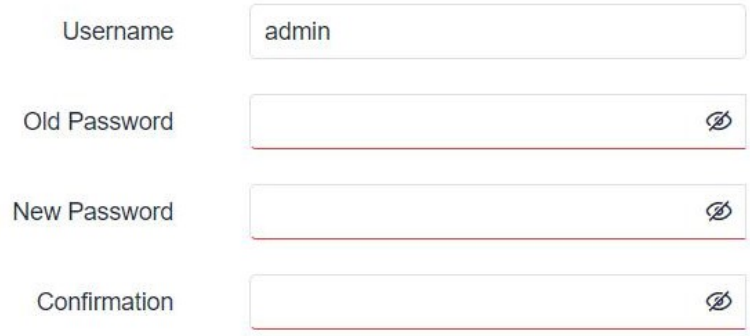

| System – Allgemeine Einstellungen | |
|---|---|
| **Element** | **Beschreibung** |
| Hostname | Legen Sie den Gerätenamen fest, der mit einem Buchstaben beginnen muss. |
| Ortszeit | Zeigt die aktuelle Systemzeit an. |
| Zeitzone | Klicken Sie auf die Dropdown-Liste, um die Zeitzone auszuwählen, in der Sie sich befinden. |
| Zeitsynchronisation | Wählen Sie den Modus für die Zeitsynchronisierung aus.<br>**Browserzeit synchronisieren:** Zeit mit dem Browser synchronisieren.<br>**Mit NTP-Server synchronisieren:** Synchronisieren Sie die Zeit mit dem NTP-Server.<br>**GPS-Zeitsynchronisierung:** Synchronisieren Sie die Zeit stündlich mit GPS. Stellen Sie sicher, dass GPS unter **„Service > GPS > GPS“** aktiviert ist.<br>**Manuell:** Konfigurieren Sie die Zeit manuell. |




| System – NTP-Einstellung | |
|---|---|
| **Element** | **Beschreibung** |
| NTP-Server aktivieren | Aktivieren Sie diese Option, um einen NTP-Server für verbundene Geräte bereitzustellen. |
| NTP-Server-Kandidaten | Geben Sie die IP-Adresse oder den Domänennamen des NTP-Servers ein, um die Zeit zu synchronisieren. Es können maximal 5 Server hinzugefügt werden. |

### 6.6.1.2 Benutzereinstellungen

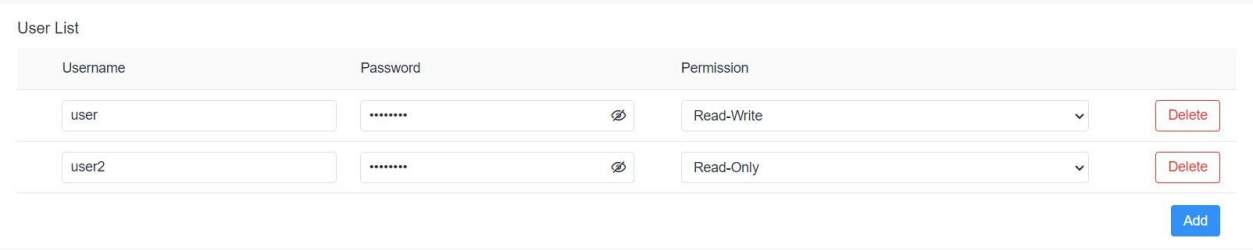
Sie können den Benutzernamen oder das Passwort des Administrators für den Zugriff auf das Gerät ändern.




| Kontoinformationen ändern | |
|---|---|
| **Element** | **Beschreibung** |
| Benutzername | Geben Sie den Benutzernamen des Administratorkontos ein. |
| Altes Passwort | Geben Sie das alte Passwort ein, um die Berechtigung zu überprüfen. |
| Neues Passwort | Geben Sie ein neues Passwort ein. Sie können alle ASCII-Zeichen außer Leerzeichen. |
| Bestätigung | Geben Sie das neue Passwort erneut ein. |

### 6.6.1.3 Verwaltung mehrerer Benutzer

In diesem Abschnitt wird beschrieben, wie Sie allgemeine Benutzerkonten erstellen. Die allgemeinen Benutzerberechtigungen umfassen „Nur Lesen“ und „Lesen/Schreiben“.

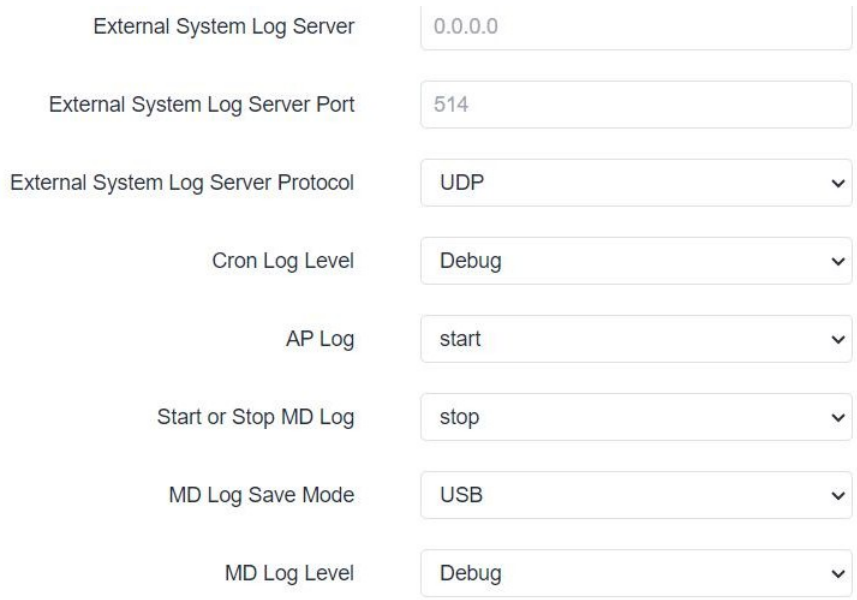



| Benutzerliste | |
|---|---|
| **Element** | **Beschreibung** |
| Benutzername | Geben Sie einen neuen Benutzernamen ein. Sie können Zeichen wie a-z, 0-9, „_“ und „-“ verwenden. Das erste Zeichen muss ein Buchstabe oder „_“ sein. |
| Passwort | Legen Sie ein Passwort fest. Sie können alle ASCII-Zeichen außer Leerzeichen verwenden. |
| Berechtigung | Wählen Sie die Benutzerberechtigung aus „Nur Lesen“ und „Lesen-Schreiben“ aus.<br>**Nur Lesen:** Benutzer können auf dieser Ebene nur die Konfiguration des Routers anzeigen.<br>**Lesen/Schreiben:** Benutzer können auf dieser Ebene die Konfiguration des Routers anzeigen und festlegen. |

### 6.6.2 Wartung

#### 6.6.2.1 Protokoll

Benutzer können Protokolle herunterladen, die Aufzeichnungen über Informations-, Fehler- und Warnereignisse enthalten, die Aufschluss über die Systemprozesse geben. Durch Überprüfen der Daten im Protokoll kann ein Administrator oder Benutzer, der Fehlerbehebungen am System vornimmt, die Ursache eines Problems identifizieren oder feststellen, ob die Systemprozesse erfolgreich geladen werden. Ein Remote-Protokollserver ist möglich, und das Gerät lädt alle Systemprotokolle auf einen Remote-Protokollserver wie Syslog Watcher hoch.



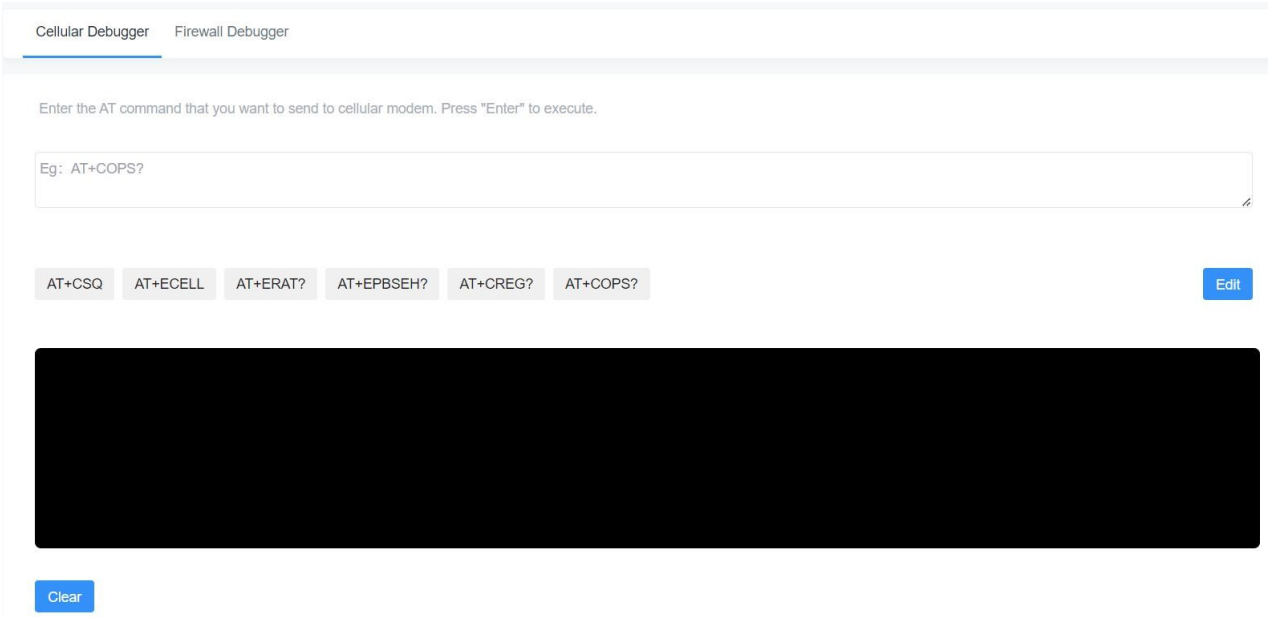

| Protokoll – Allgemeine Einstellungen | |
|---|---|
| **Element** | **Beschreibung** |
| Externes Systemprotokoll Server | Geben Sie die Adresse des Remote-Protokoll-Servers (IP/Domänenname) ein, an den der Router sendet. |
| Externes Systemprotokoll Server-Port | Geben Sie den Port des Remote-Protokoll-Servers ein, an den der Router sendet. |
| Externes Systemprotokoll Serverprotokoll | Wählen Sie aus der Dropdown-Liste „UDP“ oder „TCP“ aus, um die Protokolldatei im entsprechenden Protokoll zu übertragen. |
| Cron-Protokollstufe | Die Schweregrade zum Drucken des AP-Protokolls: Normal, Warnung, Debug. |
| AP-Protokoll | Wählen Sie diese Option, um die Aufzeichnung des Systemprotokolls zu starten oder zu beenden. |
| MD starten oder stoppen Protokoll | Wählen Sie diese Option, um die Aufzeichnung des Mobilfunkmodulprotokolls zu starten oder zu stoppen. |
| MD-Protokoll-Speichermodus | Wählen Sie den Speicher- und Ausgabemodus des MD-Protokolls aus. |
| MD-Protokollstufe | Die Schweregrade zum Drucken des MD-Protokolls: Info, Hinweis, Warnung, Fehler, Kritisch, Alarm, Notfall,Debug. |


| Protokoll – Erweiterte Einstellungen | |
|---|---|
| **Element** | **Beschreibung** |
| **AP-Protokoll** | |
| Herunterladen | Klicken Sie hier, um das zuletzt aufgezeichnete AP-Protokoll herunterzuladen. |
| **Tcpdump-Protokoll** | |
| Start | Klicken Sie hier, um die Aufzeichnung des Tcpdump-Protokolls zu starten. |
| Stopp | Klicken Sie hier, um die Aufzeichnung des tcpdump-Protokolls zu beenden. |
| Herunterladen | Klicken Sie hier, um das zuletzt aufgezeichnete tcpdump-Protokoll herunterzuladen. |

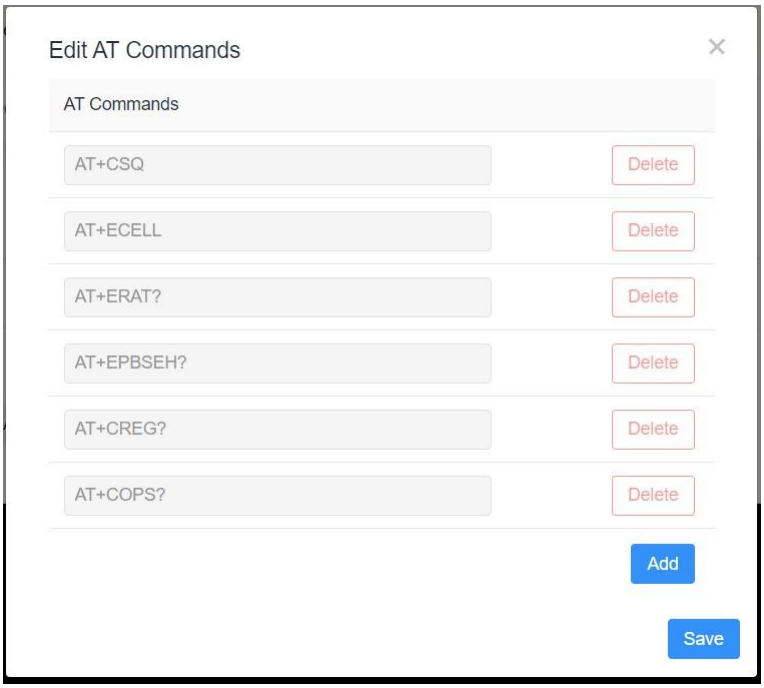


### 6.6.2.2 Mobilfunk-Debugger

Mit diesem Tool können Sie AT-Befehle eingeben, indem Sie den AT-Befehl eingeben und **die Eingabetaste** drücken, um ihn auszuführen und die Debug-Informationen des Mobilfunknetzes zu überprüfen.




Klicken Sie außerdem auf **„EDIT“**, um die gängigen AT-Befehle anzupassen, drücken Sie dann direkt auf die Schaltflächen oben im schwarzen Rahmen, um gängige Befehle direkt auszuführen.




**Beschreibung der gängigen Befehle:**

AT+CSQ? ---------Mobilfunknetzsignal abrufen

AT+ECELL?----------Aktuelle Zellinformationen abrufen

AT+ERAT?---------RAT-Status und Netzwerktyp abrufen

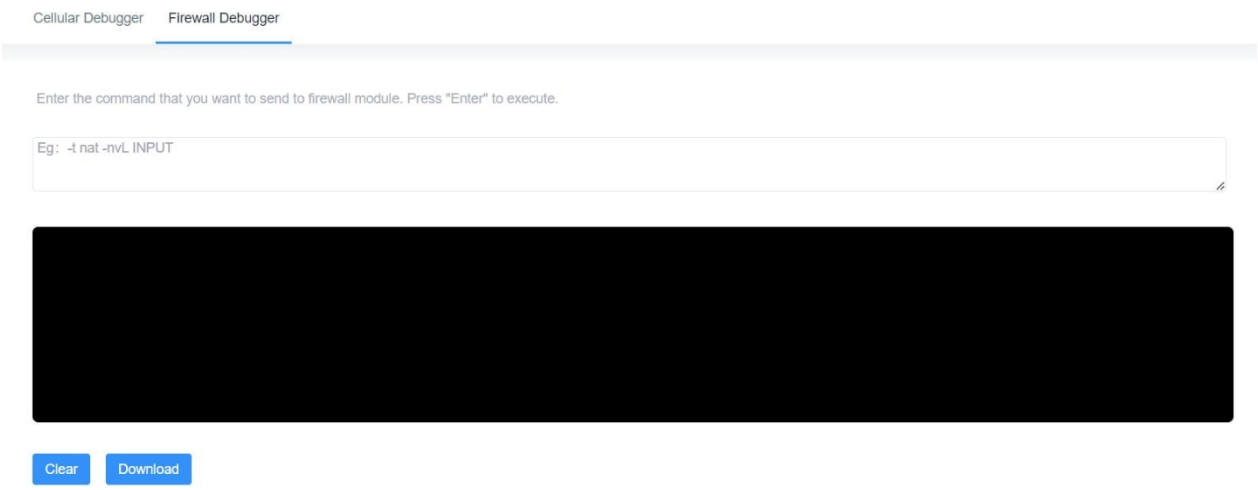
AT+EPBSEH?----------Verwendete Frequenzbänder abrufen

AT+CREG? ---------Netzwerkregistrierungsstatus abrufen

AT+COPS?----------Informationen zum Betreiber und zur Zugangstechnologie abrufen

### 6.6.2.3 Firewall-Debugger

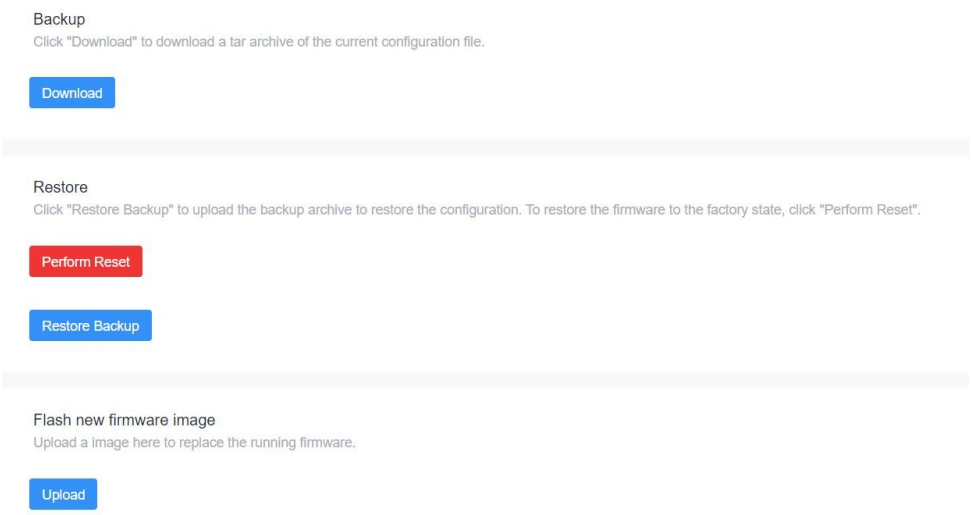
Mit diesem Tool können Sie iptables-Befehle verwenden, um Firewall-Informationen zu überprüfen und Ergebnisse herunterzuladen.



### 6.6.2.4 Sicherung/Upgrade

In diesem Abschnitt wird beschrieben, wie Sie eine vollständige Sicherung der Systemkonfigurationen in einer Datei erstellen, die Werkseinstellungen wiederherstellen, die Konfigurationsdatei auf dem Gerät wiederherstellen und das Flash-Image über das Internet aktualisieren können. In der Regel ist ein Firmware-Upgrade nicht erforderlich.

**Hinweis:** Während des Firmware-Upgrades sind keine Vorgänge auf der Webseite zulässig, da sonst das Upgrade unterbrochen wird oder das Gerät sogar ausfällt.




| Sicherung/Aktualisierung | |
|---|---|
| **Element** | **Beschreibung** |
| Sicherung erstellen | Klicken Sie hier, um ein Tar-Archiv der aktuellen Konfigurationsdatei herunterzuladen. |
| Zurücksetzen | Klicken Sie hier, um das Gerät auf die Werkseinstellungen zurückzusetzen. |
| Sicherung wiederherstellen | Um Konfigurationsdateien wiederherzustellen, können Sie hier ein zuvor erstelltes Sicherungsarchiv hochladen. Benutzerdefinierte Dateien (Zertifikate, Skripte) können auf dem System verbleiben. Um dies zu verhindern, können Sie zunächst einen Werksreset durchführen. |
| Hochladen | Laden Sie hier ein Image hoch, um die laufende Firmware zu ersetzen. |

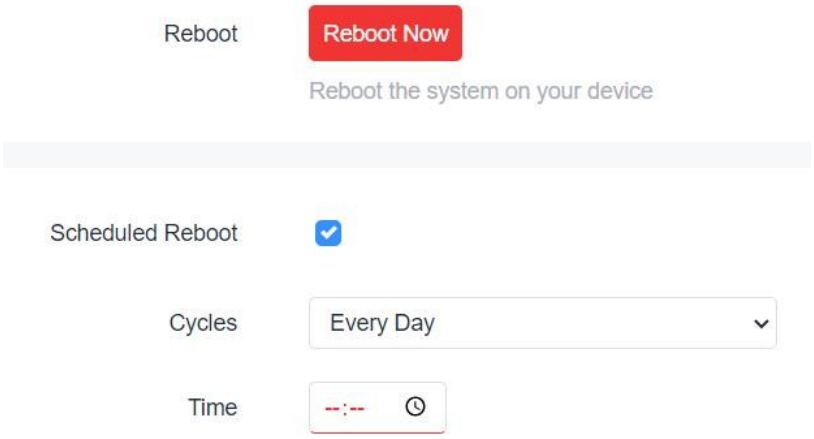
**Verwandtes Konfigurationsbeispiel**

Firmware-Upgrade

Werkseinstellungen wiederherstellen

### 6.6.2.5 Neustart

Auf dieser Seite können Sie das Gerät sofort oder regelmäßig neu starten.



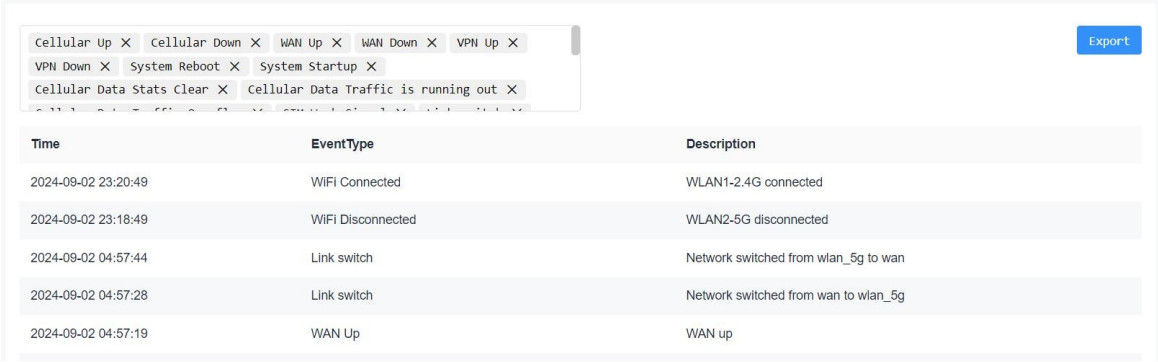

| Neustart | |
|---|---|
| **Element** | **Beschreibung** |
| Jetzt neu starten | Das Gerät sofort neu starten. |
| **Zeitplan** | |
| Aktivieren | Klicken Sie hier, um den Neustart-Zeitplan zu aktivieren. |
| Zyklen | Starten Sie das Gerät in einem festgelegten Zeitabstand neu. |
| Zeit | Wählen Sie die Uhrzeit für die Ausführung des Zeitplans aus. |

### 6.6.3 Ereignisalarm

Die Ereignisfunktion kann bei bestimmten Systemereignissen Warnmeldungen per E-Mail versenden.

#### 6.6.3.1 Ereignisalarm

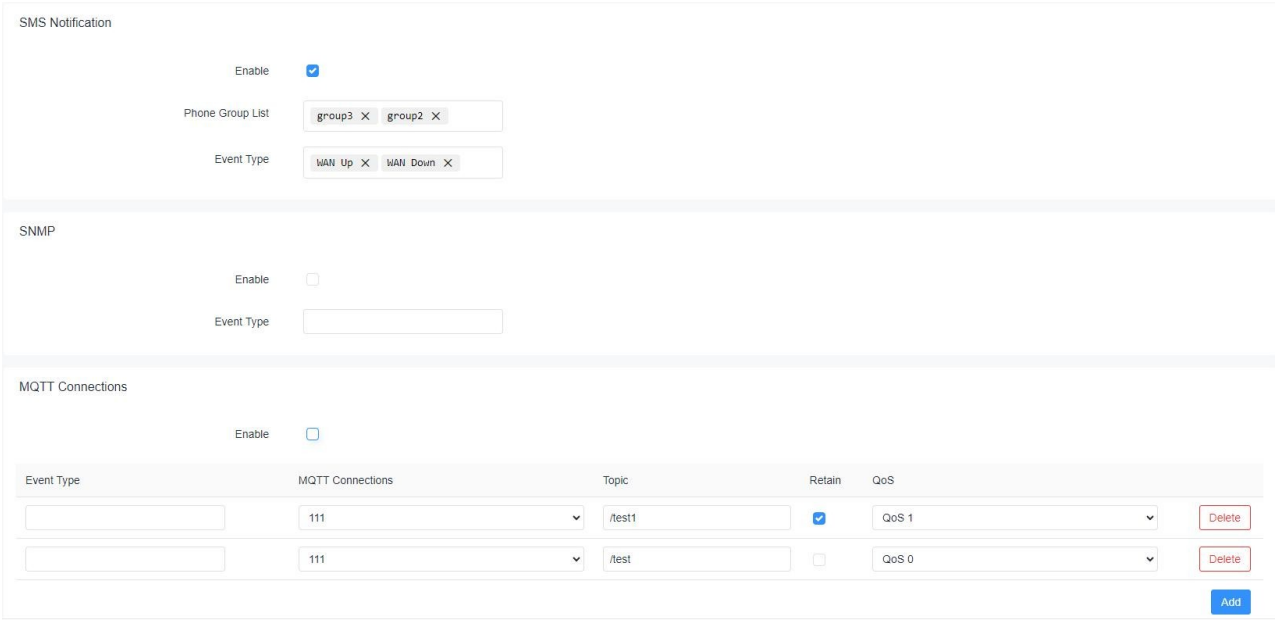
Auf dieser Seite können Sie Alarmmeldungen anzeigen.




| Ereignisalarm | |
|---|---|
| **Element** | **Beschreibung** |
| Suche | Wählen Sie den Ereignisalarm aus, den Sie in dieser Liste anzeigen möchten. |
| Export | Exportieren Sie die Ereignisalarmliste in eine CSV-Datei. |
| Zeit | Zeigen Sie die Alarmzeit an. |
| Ereignistyp | Zeigen Sie den Typ der Ereignisalarme an. |
| Beschreibung | Zeigt die Details der Ereignisalarme an. |

#### 6.6.3.2 Ereigniseinstellungen

In diesem Abschnitt können Sie festlegen, ob Sie bei Änderungen Benachrichtigungen per SMS, SNMP oder MQTT erhalten möchten.

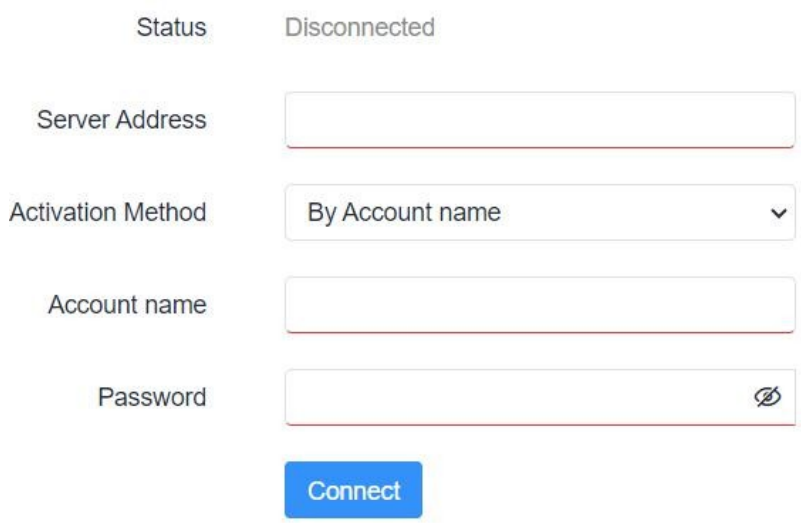



| Ereigniseinstellungen | |
|---|---|
| **Element** | **Beschreibung** |
| **SMS-Benachrichtigung** | |
| Aktivieren | Aktivieren Sie die SMS-Benachrichtigung, wenn ein Ereignis ausgelöst wird. |
| Telefon-Gruppenliste | Wählen Sie die Telefongruppe aus, die SMS-Benachrichtigungen erhalten soll. |
| Ereignistyp | Wählen Sie den Ereignistyp aus, für den SMS-Benachrichtigungen gesendet werden sollen. |
| **SNMP** | |
| Aktivieren | Aktivieren Sie diese Option, um SNMP-Benachrichtigungen zu aktivieren, wenn ein Ereignis ausgelöst wird. |
| Ereignistyp | Wählen Sie den Ereignistyp aus, der über SNMP aufgezeichnet werden soll. |
| **MQTT-Verbindungen** | |
| Aktivieren | Aktivieren Sie diese Option, um MQTT-Benachrichtigungen zu aktivieren, wenn ein Ereignis ausgelöst wird. |
| Ereignistyp | Wählen Sie den Ereignistyp aus, der MQTT senden soll.<br>Benachrichtigungen. |
| MQTT-Verbindung | Wählen Sie die MQTT-Verbindung zum Senden von Benachrichtigungen aus. Diese ist auf der Seite **„Service > MQTT“**. |
| Thema | Themenname, der für die Veröffentlichung von Daten aus der seriellen Schnittstelle verwendet wird. |
| Beibehalten | Aktivieren Sie diese Option, um die neueste Nachricht dieses Themas als Retain-Nachricht festzulegen<br>Nachricht festzulegen. |
| QoS | QoS0, QoS1 oder QoS2 sind optional. |

## 6.6.4 Geräteverwaltung

### 6.6.4.1 Geräteverwaltung

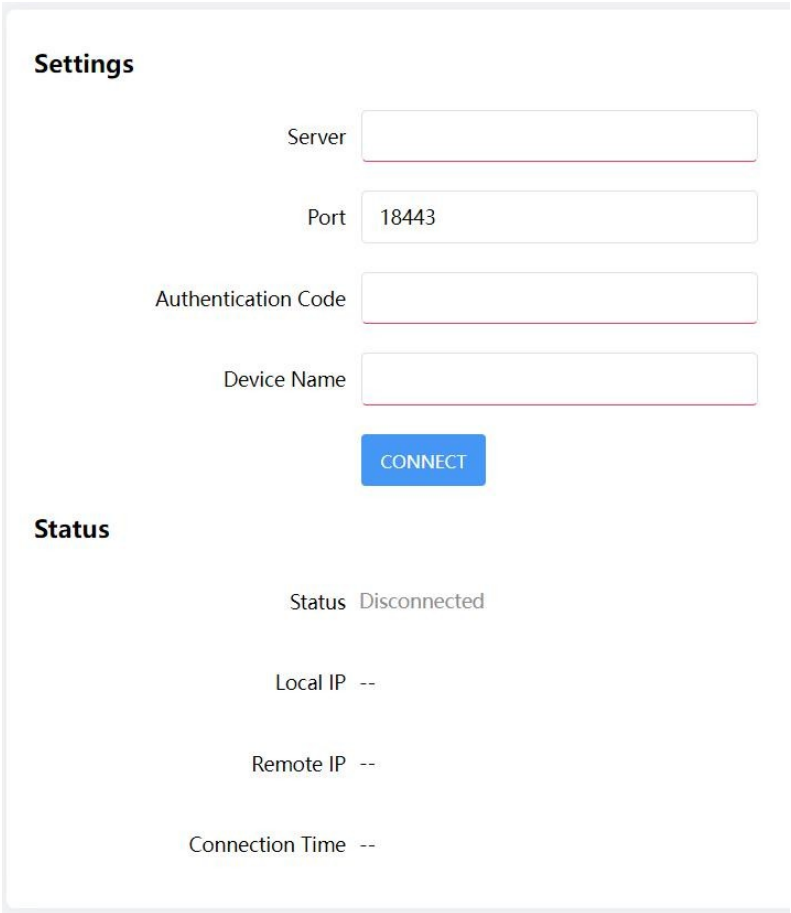
Sie können das Gerät auf dieser Seite mit der Milesight DeviceHub-Verwaltungsplattform verbinden, um das Gerät zentral und aus der Ferne zu verwalten. Weitere Informationen finden Sie im *DeviceHub-Benutzerhandbuch*.




| Geräteverwaltung | |
|---|---|
| **Element** | **Beschreibung** |
| Status | Zeigt den Verbindungsstatus zwischen dem Gerät und dem DeviceHub. |
| Serveradresse | IP-Adresse oder Domäne des DeviceHub-Verwaltungsservers. |
| Aktivierungsmethode | Wählen Sie die Aktivierungsmethode, um das Gerät mit dem DeviceHub-Server zu verbinden. Die Optionen sind **„Per Authentifizierungscode“** und **„Per Kontoname“**. |
| Authentifizierungscode | Geben Sie den vom DeviceHub generierten Authentifizierungscode ein. |
| Kontoname | Geben Sie den registrierten DeviceHub-Kontonamen (E-Mail-Adresse) und das Passwort ein. |
| Passwort | |
| Verbinden/Trennen | Klicken Sie auf diese Schaltfläche, um das Gerät mit dem DeviceHub zu verbinden/die Verbindung zum DeviceHub zu trennen.<br>DeviceHub zu verbinden/zu trennen. |

### 6.6.4.2 Cloud-VPN

Sie können das Gerät auf dieser Seite mit MilesightVPN verbinden, um den Router und die angeschlossenen Geräte zentral und aus der Ferne zu verwalten. Weitere Informationen finden Sie im *MilesightVPN-Benutzerhandbuch*.




| Cloud-VPN | |
|---|---|
| **Element** | **Beschreibung** |
| **Einstellungen** | |
| Server | Geben Sie die IP-Adresse oder den Domänennamen von MilesightVPN ein. |
| Port | Geben Sie die HTTPS-Portnummer ein. |
| Autorisierungscode | Geben Sie den von MilesightVPN generierten Autorisierungscode ein. |
| Gerätename | Geben Sie den Namen des Geräts ein. |
| **Status** | |
| Status | Zeigen Sie die Verbindungsinformationen darüber an, ob der Router mit MilesightVPN verbunden ist. |
| Lokale IP | Zeigt die virtuelle IP-Adresse des Routers an. |
| Remote-IP | Zeigt die virtuelle IP des Milesight VPN-Servers an. |
| Verbindungszeit | Zeigt an, wie lange der Router bereits mit dem Milesight VPN verbunden ist. |

**[ENDE]**