Wi-Fi HaLow Gateway

HL31

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.
- Stellen Sie das Gerät nicht in der Nähe von Gegenständen mit offener Flamme auf.
- Stellen Sie das Gerät nicht an Orten auf, an denen die Temperatur unterhalb/oberhalb des Betriebsbereichs liegt.
- Schalten Sie das Gerät während der Installation nicht ein und schließen Sie es nicht an andere elektrische Geräte an.
- Überprüfen Sie bei Verwendung im Freien den Blitz- und Wasserschutz.
- Schließen Sie das Gerät nicht mit beschädigten Kabeln an und versorgen Sie es nicht mit Strom.

Konformitätserklärung

HL31 entspricht den grundlegenden Anforderungen und anderen relevanten Bestimmungen der CE, FCC und RoHS.

Wenn Sie Hilfe benötigen, 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
22. Februar 2024	V1.0	Erstversion

Inhalt

Kapitel 1 Produktvorstellung

1.1 Übersicht

HL31 ist ein leichtes Wi-Fi HaLow-Gateway für den Innenbereich. Dank Wi-Fi HaLow-Technologie und einer leistungsstarken Quad-Core-CPU unterstützt HL31 die Einrichtung von mehr als 200 Knoten für die gleichzeitige Übertragung bei geringem Stromverbrauch. HL31 hat eine Sichtverbindung von bis zu 1 km und unterstützt Datenraten von bis zu 32 Mbit/s, was für IoT-Sensoren und Bildkameraanwendungen geeignet ist. HL31 unterstützt nicht nur mehrere Backhaul-Backups mit Ethernet und Mobilfunk, sondern bietet auch mehrere VPN-Lösungen, um die Datenübertragung zu Remote-Servern zu sichern.

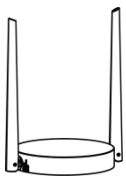
Mit seiner kompakten Größe und verschiedenen Stromversorgungsoptionen ist er eine ideale Ergänzung für große Innenbereiche wie Büros, Parkplätze, Campusgelände usw.

1.2 Wichtigste Merkmale

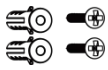
- Industrietaugliche Quad-Core-CPU mit ARM Cortex-A35-Prozessor für hohe Leistung bei der Datenübertragung
- Unterstützt bis zu 200 Endknotenverbindungen
- Geringe Größe für einfachen Transport und Einsatz
- Unterstützt die Montage auf dem Schreibtisch, an der Wand oder an der Decke
- Ausgestattet mit WLAN für die Konfiguration über die Web-GUI
- Multi-Backhaul-Backups mit Ethernet und Mobilfunk (4G)
- Sichere Übertragung mit VPN-Tunneln wie IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN
- Funktioniert gut mit Standard-WLAN-HaLow-Sensoren

Kapitel 2 Hardware-Einführung

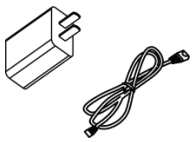
2.1 Packliste



1 × HL31-Gerät



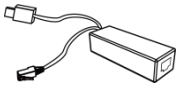
2 × Wandhalterung Kits



1 × Typ-C-Kabel und Netzteil

1 × Kurzanleitung

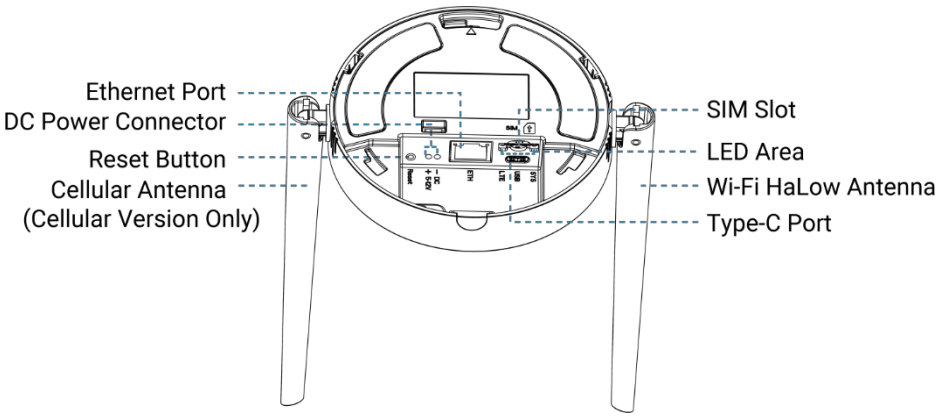
1 × Garantiekarte



1 × PoE-Splitter (optional)

Sollte eines der oben genannten Teile fehlen oder beschädigt sein, wenden Sie sich bitte an Ihren Vertriebsmitarbeiter.

2.2 Hardware-Übersicht



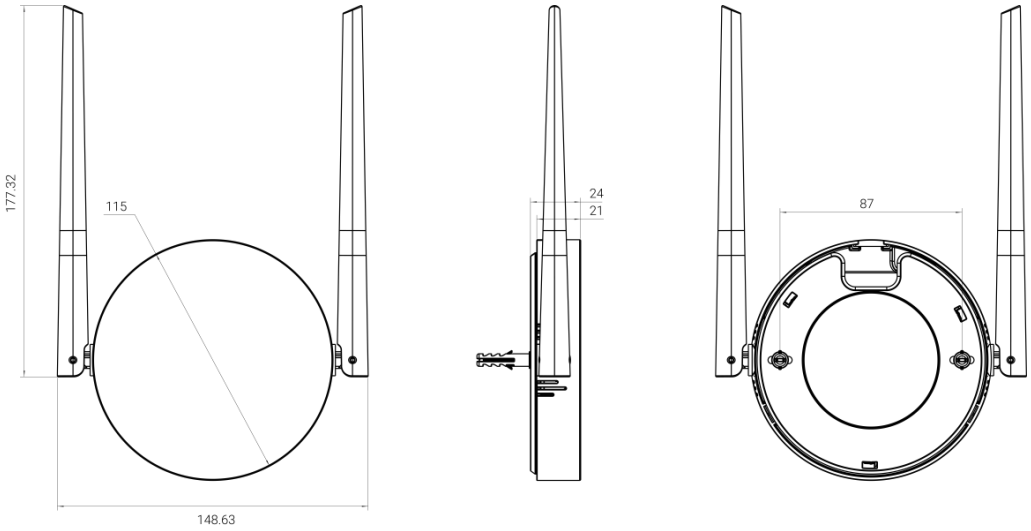
2.3 LED-Anzeige und Reset-Taste LED-Anzeigen

LED	Anzeige	Status	Beschreibung
SYS	Stromversorgung und Systemstatus	Aus	Die Stromversorgung ist ausgeschaltet
		Grünes Licht	Das System läuft ordnungsgemäß
		Rotes Licht	Das System funktioniert nicht richtig
LTE	Mobilfunkstatus	Aus	SIM-Karte wird registriert oder konnte nicht registriert werden (oder es sind keine SIM-Karten eingelegt)
		Grünes Licht	Blinkt langsam: SIM-Karte wurde registriert und ist bereit für die Einwahl
			Blinkt schnell: SIM-Karte wurde registriert und wählt sich gerade ein
			Leuchtet konstant: SIM-Karte wurde registriert und erfolgreich gewählt
Ethernet-Anschluss	Verbindungsanzeige	Aus	Getrennt oder Verbindungsfehler
		Gelb Blinkt	Daten werden übertragen
	Verbindung Anzeige	Aus	Ethernet-Anschluss ist getrennt
		Grünes Licht	Ethernet-Anschluss ist verbunden

Reset-Taste

Funktion	Aktion	LED-Anzeige
Auf Werkseinstellungen zurücksetzen Standard	Halten Sie die Taste länger als 5 Sekunden gedrückt. Sekunden	SYS: blinkt schnell.

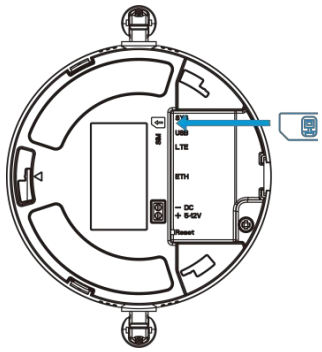
2.4 Abmessungen (mm)



Kapitel 3 Hardware-Installation

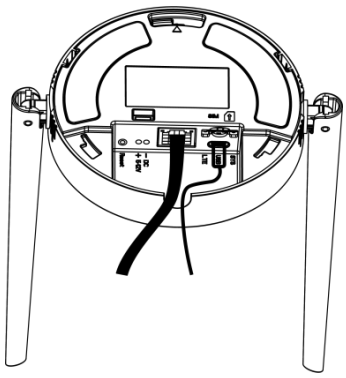
3.1 Installation der SIM-Karte (nur Mobilfunkversion)

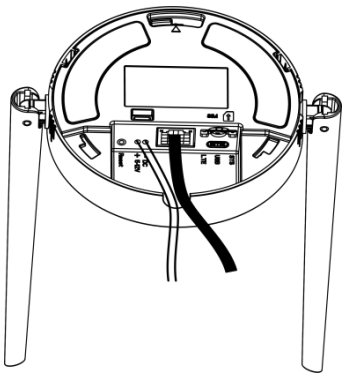
Legen Sie die Micro-SIM-Karte (3FF) wie folgt gemäß den Pfeilen in das Gerät ein. Wenn Sie die SIM-Karte herausnehmen möchten, drücken Sie auf die SIM-Karte, damit sie automatisch herausspringt.



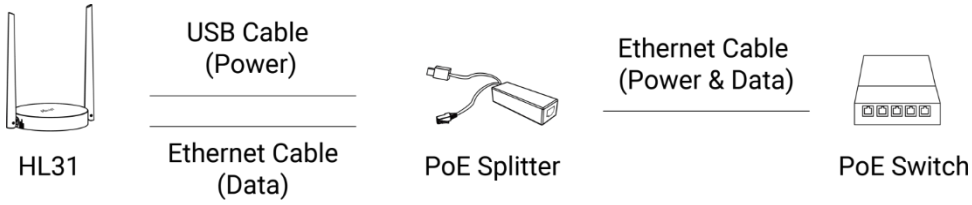
3.2 Stromversorgung

HL31 kann standardmäßig über USB (5 V) oder einen Gleichstromanschluss (5-12 V) mit Strom versorgt werden. Verlegen Sie die Stromkabel zusammen mit den Ethernet-Kabeln durch die Nut.





Zusätzlich kann es auch über einen PoE-Splitter mit einer 802.3af-Standard-PoE-Quelle mit Strom versorgt werden.



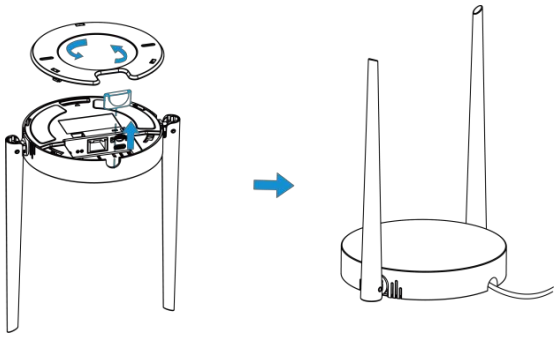
3.3 Gateway-Installation

HL31 unterstützt mehrere Installationsmethoden wie Tischaufstellung, Wandmontage, Deckenmontage usw. Bevor Sie beginnen, vergewissern Sie sich, dass alle Kabel installiert und die Konfigurationen abgeschlossen sind.

Hinweis: Schließen Sie das Gerät während der Installation nicht an die Stromversorgung oder andere Geräte an.

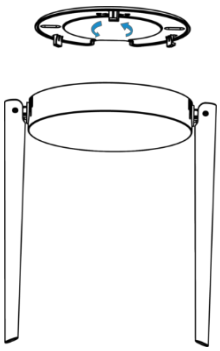
3.3.1 Tisch

Entfernen Sie die Blende und die Montageplatte auf der Rückseite des Geräts, dann können Sie das Gerät auf den Tisch stellen.

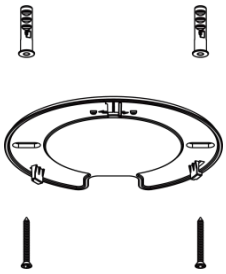


3.3.2 Wand-/Deckenmontage

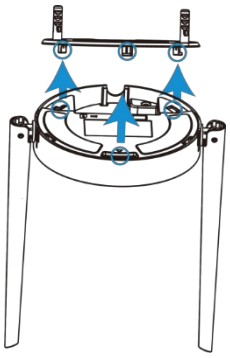
1. Entfernen Sie die Montageplatte auf der Rückseite des Geräts.



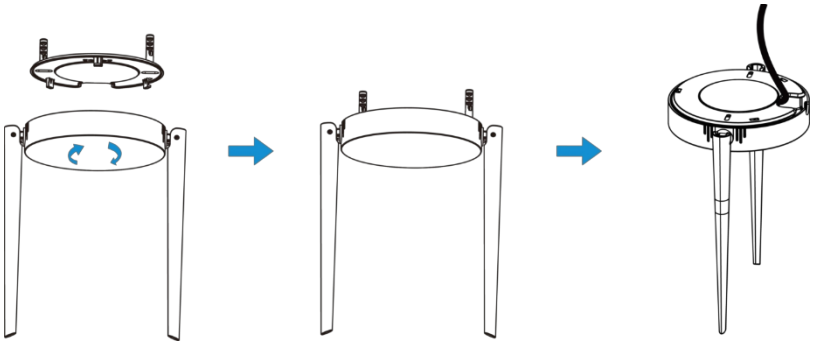
2. Richten Sie die Montageplatte horizontal an der gewünschten Position an der Wand oder Decke aus, um zwei Befestigungslöcher zu markieren, bohren Sie zwei Löcher an diesen Markierungen ein setzen Sie jeweils Dübel in die Löcher ein.



3. Befestigen Sie die Montageplatte mit Schrauben an den Dübeln.



4. Drehen Sie das Gerät im Uhrzeigersinn, um es an der Montageplatte zu arretieren.



Kapitel 4 Zugriff auf die Web-GUI

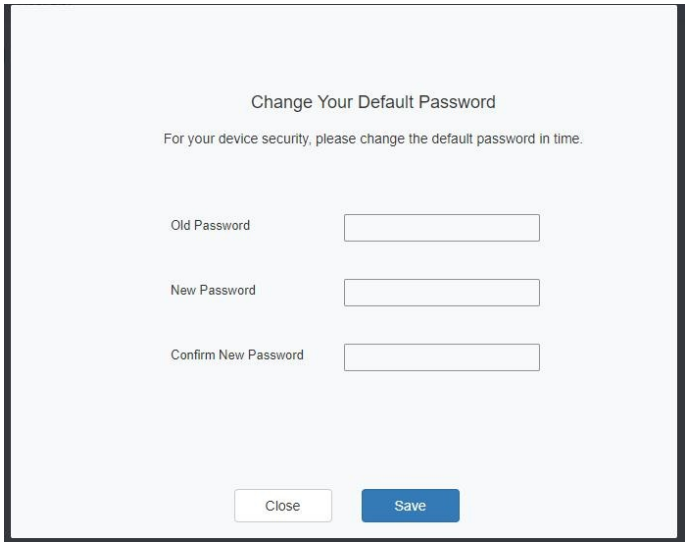
In diesem Kapitel wird erklärt, wie Sie auf die Web-GUI des HL31 zugreifen können. Benutzername: admin
Passwort: password

4.1 Drahtloser Zugriff

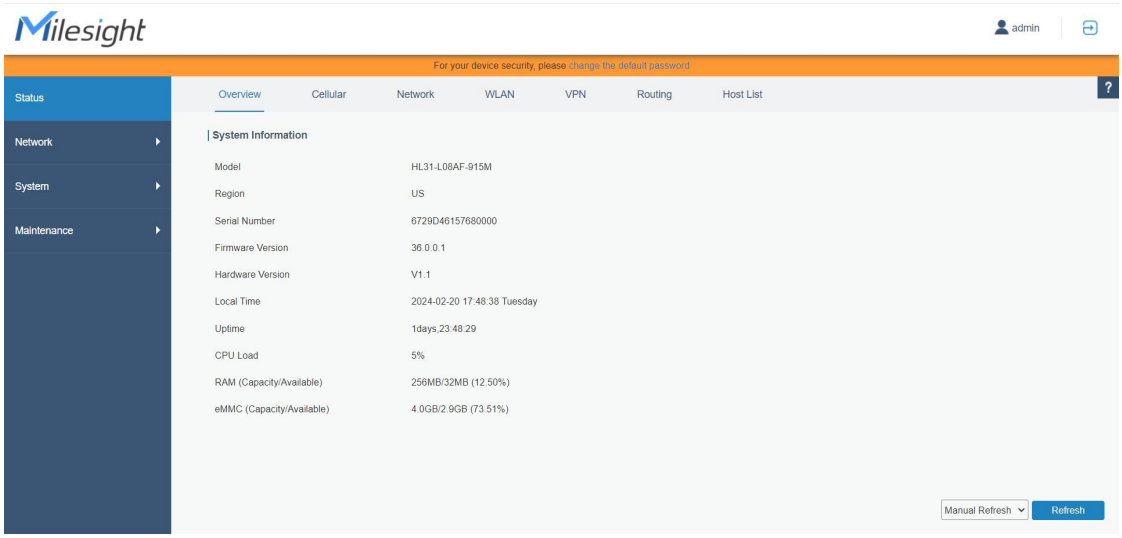
1. Aktivieren Sie die drahtlose Netzwerkverbindung auf Ihrem Computer und suchen Sie nach dem Zugangspunkt Gateway_XXXXXX_2.4G. Geben Sie das Standardpasswort iotpassword ein, um eine Verbindung herzustellen. (XXXXXX = die letzten 6 Ziffern der MAC-Adresse)
2. Öffnen Sie einen Webbrowser auf Ihrem PC (Chrome wird empfohlen) und geben Sie die IP-Adresse 192.168.1.1 ein, um auf die Web-GUI zuzugreifen.
3. Geben Sie den Benutzernamen und das Passwort ein und klicken Sie auf „Anmelden".

Wenn Sie den Benutzernamen oder das Passwort mehr als 5 Mal falsch eingeben, wird die Anmeldeseite für 10 Minuten gesperrt.

4. Nachdem Sie sich bei der Web-GUI angemeldet haben, folgen Sie der Anleitung, um die Grundkonfigurationen abzuschließen. Aus Sicherheitsgründen wird empfohlen, das Passwort zu ändern.



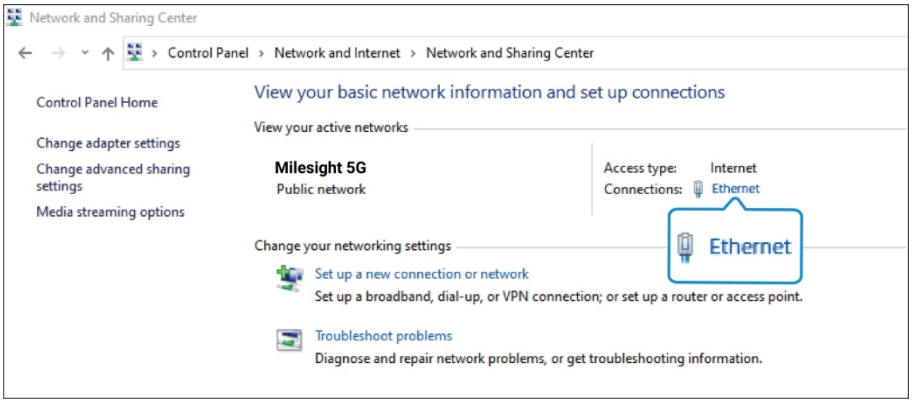
5. Sie können Systeminformationen anzeigen und die Konfiguration des Gateways vornehmen.



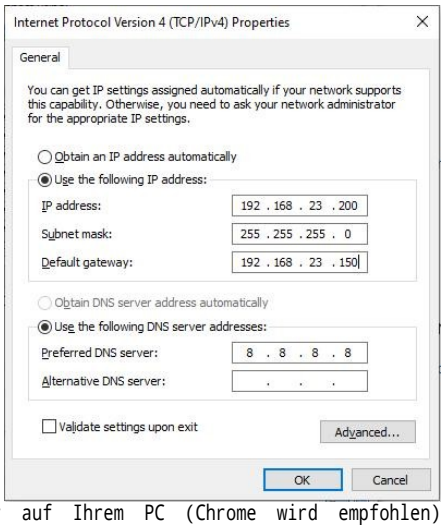
4.2 Kabelgebundener Zugang

Verbinden Sie den PC direkt mit dem HL31 ETH-Port, um auf die Web-GUI des Gateways zuzugreifen. Die folgenden Schritte basieren auf dem Windows 10-System 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)“ und wählen Sie „Folgende IP-Adresse verwenden“ aus. Weisen Sie dann manuell eine statische IP-Adresse innerhalb desselben Subnetzes des Gateways zu.

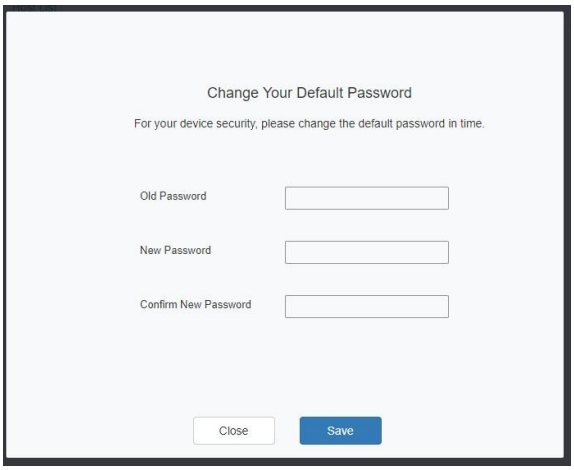


3. Öffnen Sie einen Webbrowser auf Ihrem PC (Chrome wird empfohlen) und geben Sie die IP-Adresse 192.168.23.150 ein, um auf die Web-GUI zuzugreifen.

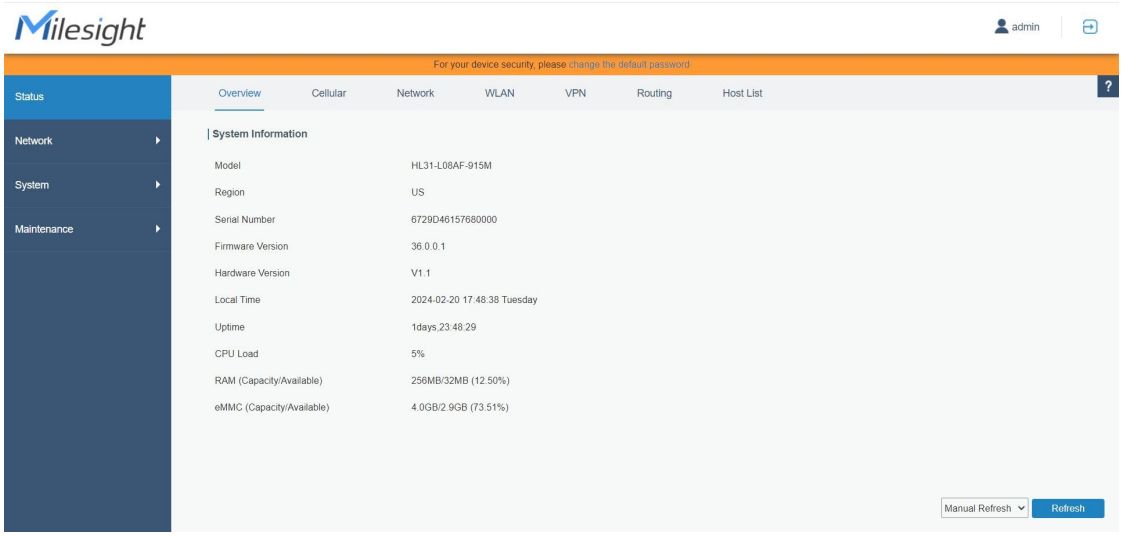
4. Geben Sie den Benutzernamen und das Passwort ein und klicken Sie auf „Anmelden“.

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

5. Nachdem Sie sich bei der Web-GUI angemeldet haben, folgen Sie der Anleitung, um die Grundkonfigurationen abzuschließen. Aus Sicherheitsgründen wird empfohlen, das Passwort zu ändern.



6. Sie können Systeminformationen anzeigen und die Konfiguration des Gateways vornehmen.



Kapitel 5 Anwendungsbeispiele

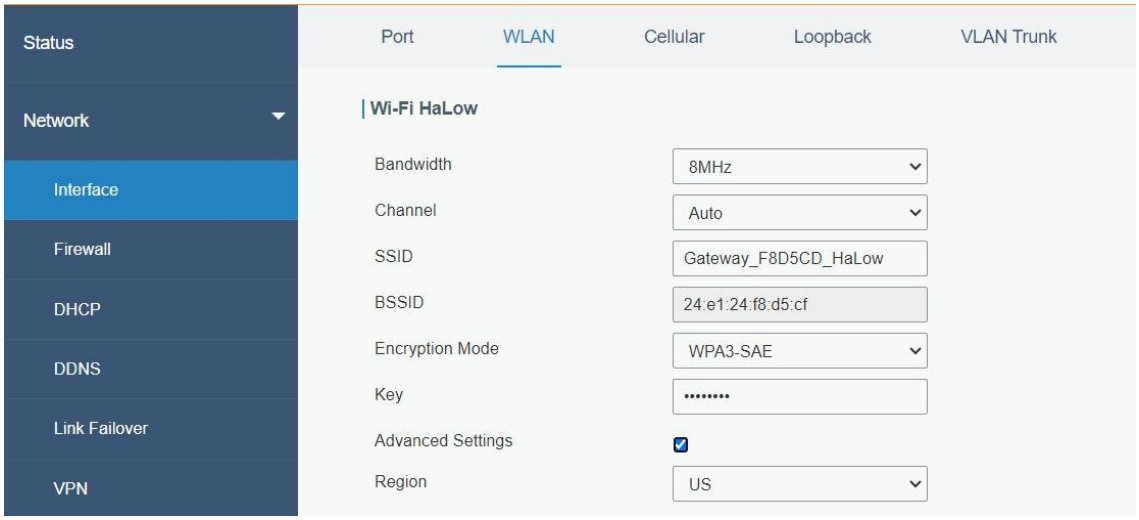
5.1 Wi-Fi HaLow-Zugangspunkt

Anwendungsbeispiel

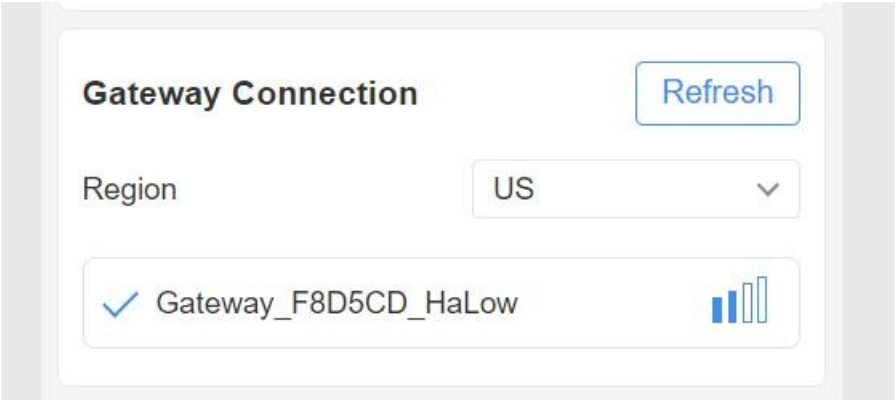
Konfigurieren Sie HL31 als Wi-Fi HaLow AP, um eine Verbindung von X1 Wi-Fi HaLow-Kameras zu ermöglichen.

Konfigurationsschritte

1. Gehen Sie zu Netzwerk > Schnittstelle > WLAN, um die WLAN-Parameter zu konfigurieren und die Einstellungen zu speichern.



2. Wählen Sie den Regionenparameter der X1-Kamera entsprechend dem Gateway aus, suchen Sie den Zugangspunkt von HL31 und stellen Sie eine Verbindung her.



3. Gehen Sie zu Status > WLAN des HL31-Gateways, um die AP-Einstellungen und Informationen des verbundenen Clients/Benutzers zu überprüfen.

Verwandtes Thema

WLAN-Einstellung

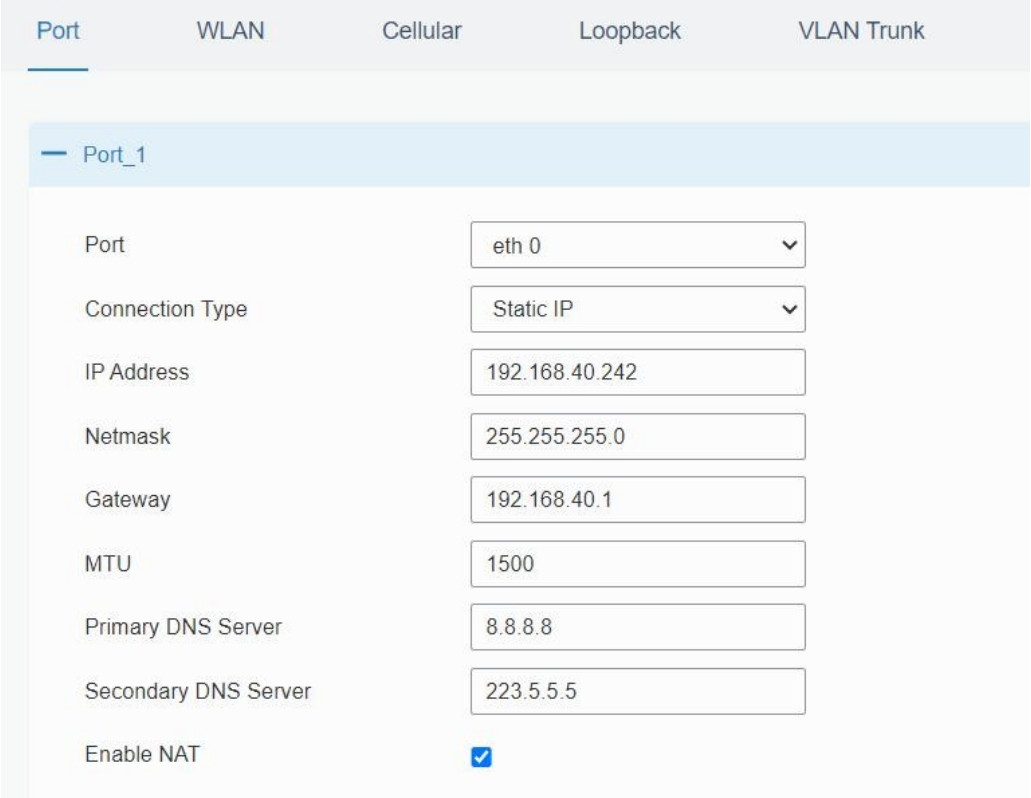
WLAN-Status

5.2 Ethernet-Verbindung

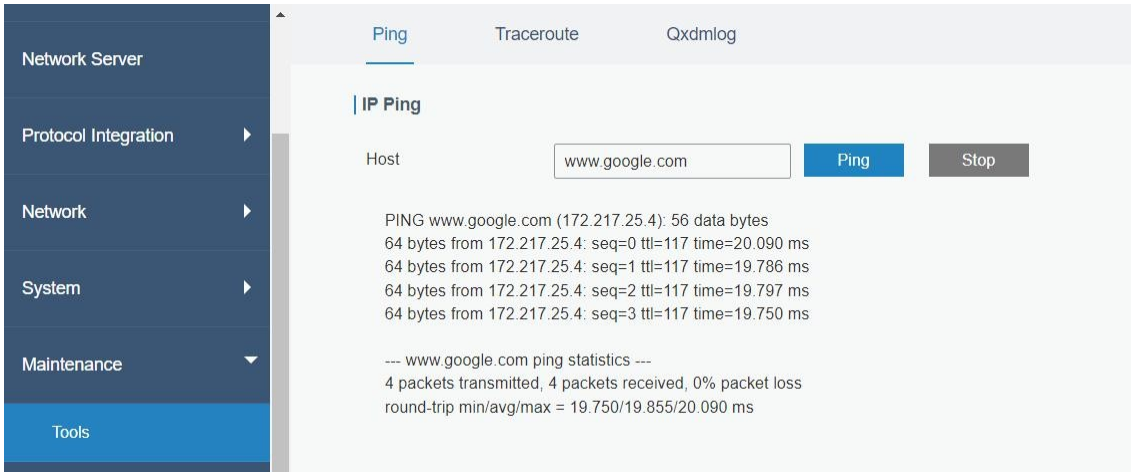
Wir zeigen Ihnen anhand eines Beispiels, wie Sie das Gateway so konfigurieren, dass Sie über den Ethernet-Anschluss Zugang zum Internet erhalten

über den Ethernet-Port zu erhalten.

1. Gehen Sie zur Seite „Netzwerk > Schnittstelle > Port“, um den Verbindungstyp auszuwählen und die Ethernet-Port-Konfiguration zu konfigurieren, und speichern Sie anschließend die Einstellungen.



2. Verbinden Sie den Ethernet-Port des Gateways mit Netzwerkgeräten wie Router oder Modem.
3. Gehen Sie zur Seite „Wartung > Tools > Ping“, um die Netzwerkverbindung zu überprüfen.



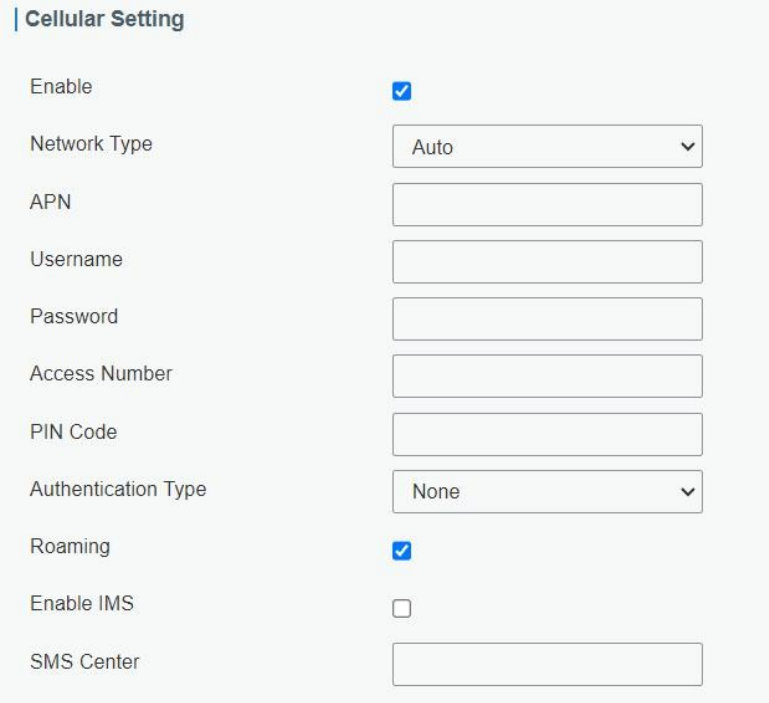
Verwandtes Thema

Port-Einstellung

5.3 Mobilfunkverbindung (nur Mobilfunkversion)

Wir zeigen Ihnen anhand eines Beispiels, wie Sie das Gateway so konfigurieren, dass Sie über Mobilfunk Zugang zum Internet erhalten.

1. Gehen Sie zu Netzwerk > Schnittstelle > Mobilfunk > Mobilfunkeinstellungen und konfigurieren Sie die erforderlichen Informationen der SIM-Karte. Speichern Sie anschließend die Einstellungen.



2. Klicken Sie auf „Status > Mobilfunk“, um den Status der Mobilfunkverbindung anzuzeigen. Wenn „Verbunden“ angezeigt wird, wurde die SIM-Karte erfolgreich gewählt.

Verwandtes Thema

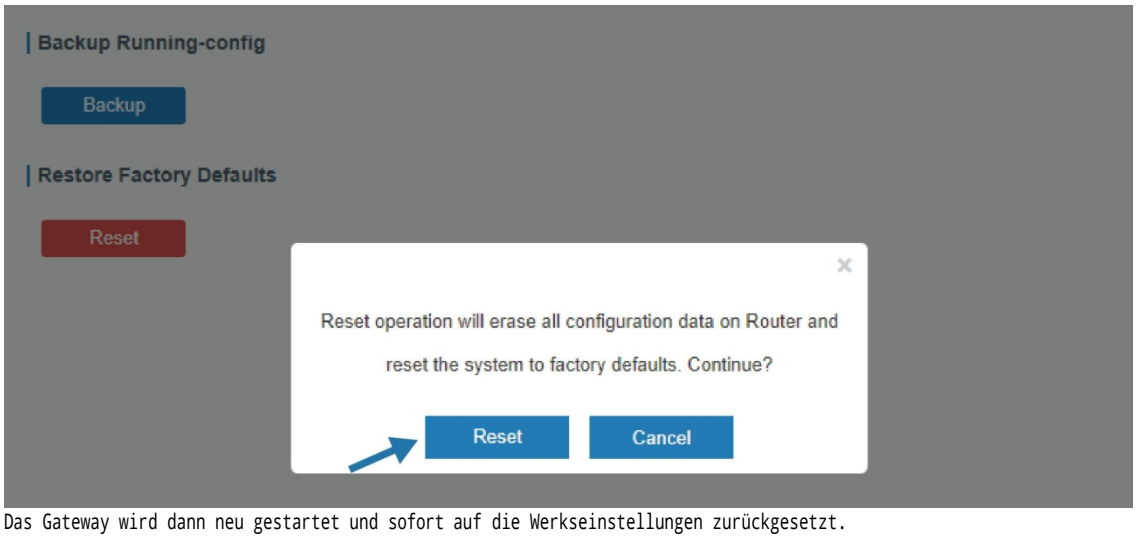
Mobilfunk-Einstellungen

Mobilfunk-Status

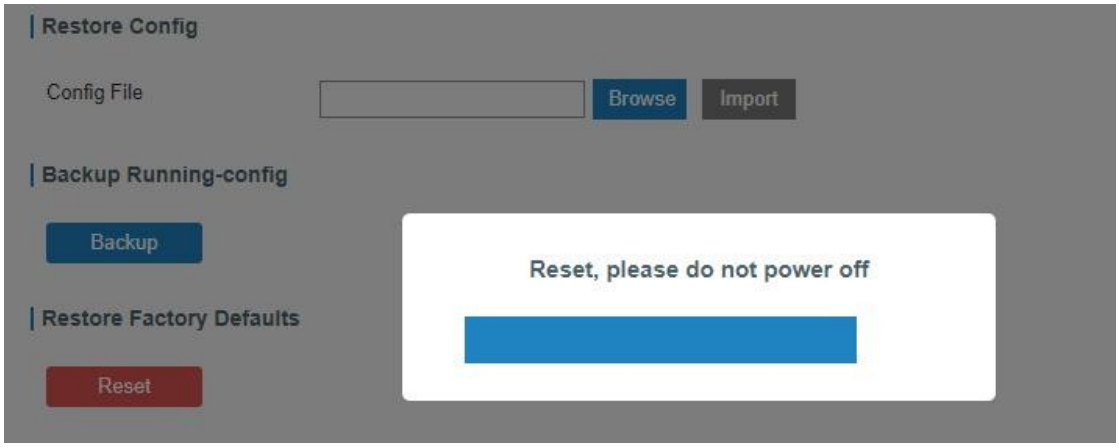
5.4 Werkseinstellungen wiederherstellen

Methode 1:

Melden Sie sich in der Weboberfläche an, gehen Sie zu „Wartung > Sichern und Wiederherstellen“ und klicken Sie auf die Schaltfläche „Zurücksetzen“. Sie werden gefragt, ob Sie das Gerät auf die Werkseinstellungen zurücksetzen möchten. Klicken Sie anschließend auf die Schaltfläche „Zurücksetzen“.



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



Warten Sie, bis die SYS-Anzeige statisch leuchtet und die Anmeldeseite erneut angezeigt wird. Dies bedeutet, dass das Gateway erfolgreich auf die Werkseinstellungen zurückgesetzt wurde.

Verwandtes Thema

Werkseinstellungen wiederherstellen

Methode 2:

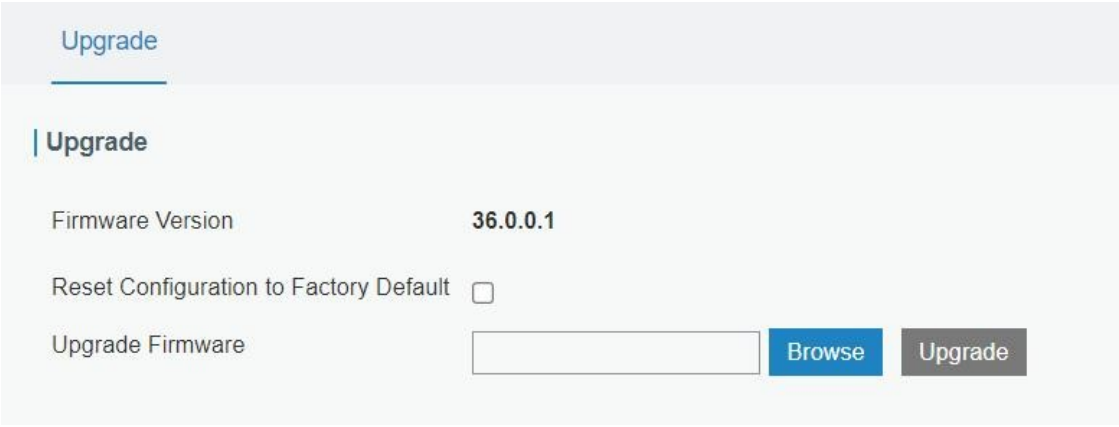
Suchen Sie die Reset-Taste am Gateway, drücken Sie sie und halten Sie sie länger als 5 Sekunden gedrückt, bis die SYS-LED blinkt.

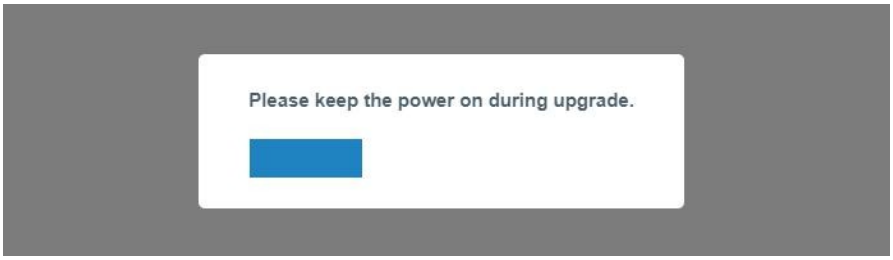
5.5 Firmware-Aktualisierung

Es wird empfohlen, dass Sie sich vor dem Aktualisieren der Gateway-Firmware zunächst an den technischen Support von Milesight wenden. Die Dateiendung der Gateway-Firmware lautet „.bin“.

Nachdem Sie die Firmware-Datei erhalten haben, führen Sie bitte die folgenden Schritte aus, um das Upgrade abzuschließen.

1. Gehen Sie zur Seite „Wartung > Aktualisierung“, klicken Sie auf „Durchsuchen“ und wählen Sie die richtige Firmware-Datei auf dem PC aus.
2. Klicken Sie auf „Upgrade“, und das Gateway überprüft, ob die Firmware-Datei korrekt ist. Wenn dies der Fall ist, wird die Firmware in das Gateway importiert, und das Gateway beginnt mit dem Upgrade.





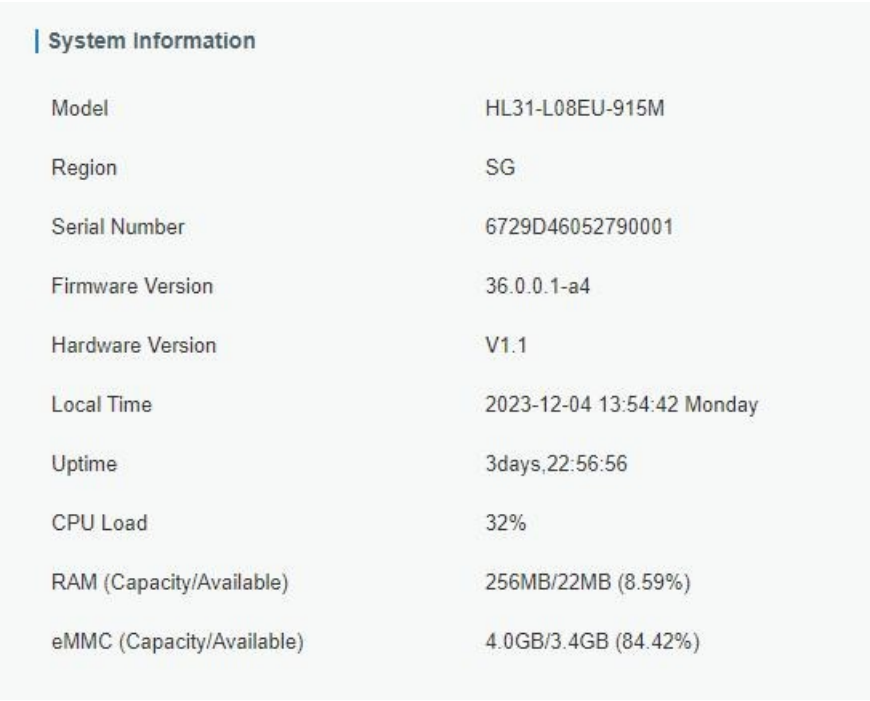
Verwandtes Thema

Upgrade

Kapitel 6 Bedienungsanleitung

6.1 Status

6.1.1 Übersicht

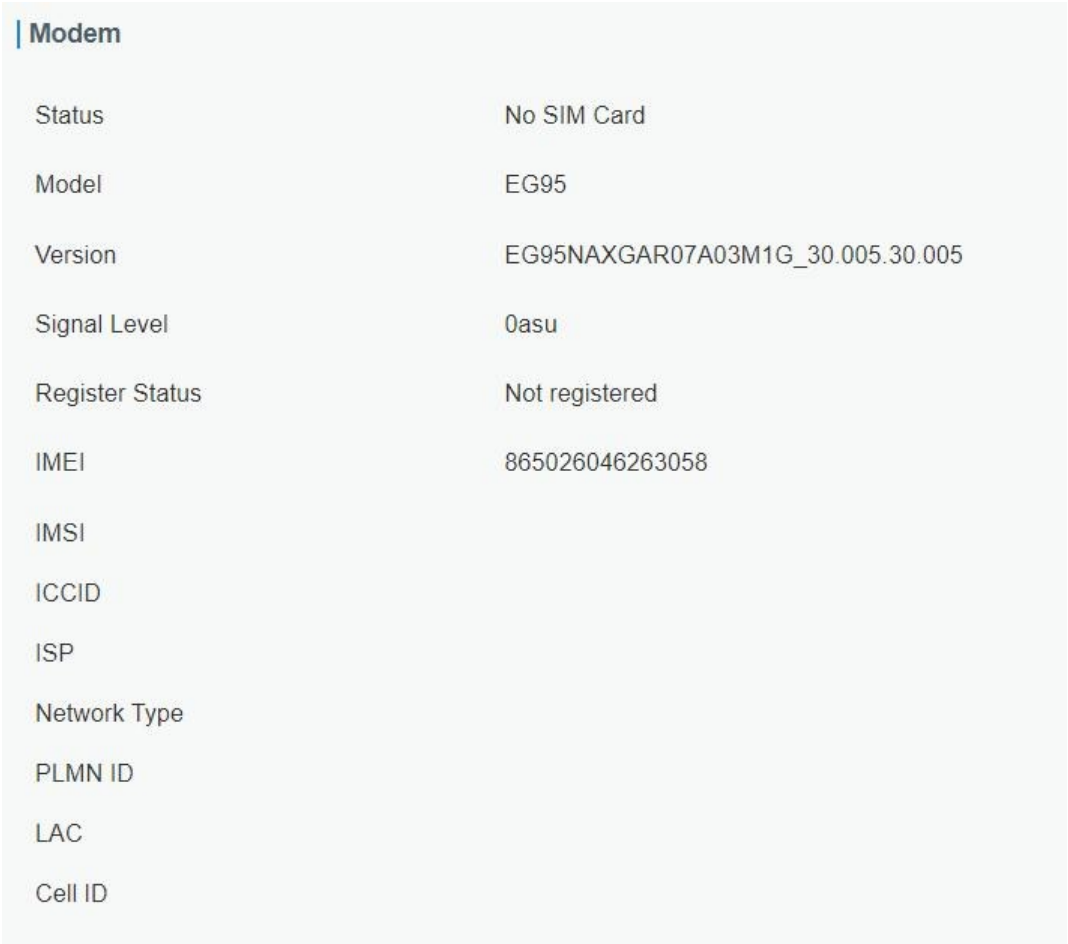


Systeminformationen	
Element	Beschreibung
Modell	Zeigt den Modellnamen des Gateways an.
Region	Zeigt die Wi-Fi HaLow-Frequenzregion des Gateways an.
Seriennummer	Zeigt die Seriennummer des Gateways an.
Firmware-Version	Zeige die aktuelle Firmware-Version des Gateways an.
Hardware-Version	Zeigt die aktuelle Hardwareversion des Gateways an.
Lokale Zeit	Zeigt die aktuelle Ortszeit des Systems an.
Betriebszeit	Zeigt an, wie lange das Gateway bereits in Betrieb ist.

	in Betrieb ist.
CPU-Auslastung	Zeigt die aktuelle CPU-Auslastung des Gateways an.
RAM (Kapazität/verfügbar)	Zeigen Sie die RAM-Kapazität und den verfügbaren RAM-Speicher an.
eMMC (Kapazität/verfügbar)	Zeigt die eMMC-Kapazität und den verfügbaren eMMC-Speicher an.

6.1.2 Mobilfunk (nur Mobilfunkversion)

Auf dieser Seite können Sie den Mobilfunknetzstatus des Gateways anzeigen.



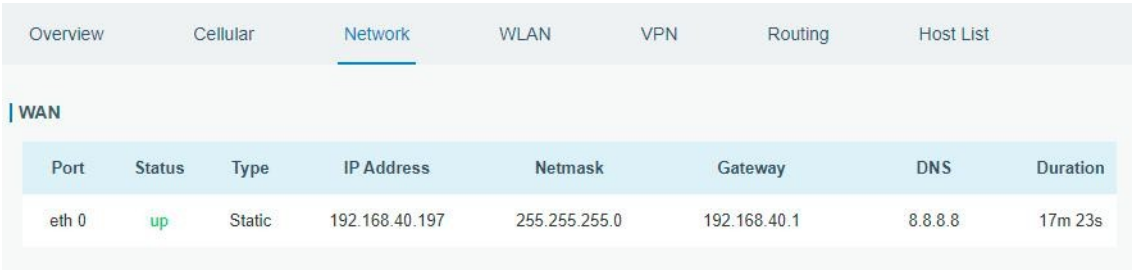
Modem-Informationen	
Element	Beschreibung
Status	Zeigt den entsprechenden Erkennungsstatus des Moduls und der SIM-Karte an.
Modell	Zeigt den Modellnamen des Mobilfunkmoduls an.
Version	Zeigt die Version des Mobilfunkmoduls an.
Signalpegel	Zeigt die Mobilfunksignalstärke an.
Registrierungsstatus	Zeigt den Registrierungsstatus der SIM-Karte an.
IMEI	Zeigt die IMEI des Moduls an.
IMSI	Zeigt die IMSI der SIM-Karte an.
ICCID	Zeigt die ICCID der SIM-Karte an.
ISP	Zeigen Sie den Netzbetreiber an, bei dem die SIM-Karte registriert ist.
Netzwerktyp	Zeigen Sie den verbundenen Netzwerktyp an, z. B. LTE, 3G usw.

PLMN-ID	Zeigen Sie die aktuelle PLMN-ID an, einschließlich MCC,MNC,LAC und Cell-ID.
LAC	Zeigt den Standortbereichscode der SIM-Karte an.
Cell-ID	Zeigt die Cell-ID des Standorts der SIM-Karte an.

Netzwerkstatus	
Element	Beschreibung
Status	Zeigt den Verbindungsstatus des Mobilfunknetzes an.
IP-Adresse	Zeige die IP-Adresse des Mobilfunknetzes an.
Netzmaske	Zeigt die Netzmaske des Mobilfunknetzes an.
Gateway	Zeigt das Gateway des Mobilfunknetzes an.
DNS	Zeigt den DNS des Mobilfunknetzes an.
Verbindungsdauer	Zeigt Informationen darüber an, wie lange das Mobilfunknetz verbunden ist.

6.1.3 Netz

Auf dieser Seite können Sie den Status des Ethernet-Ports des Gateways überprüfen.

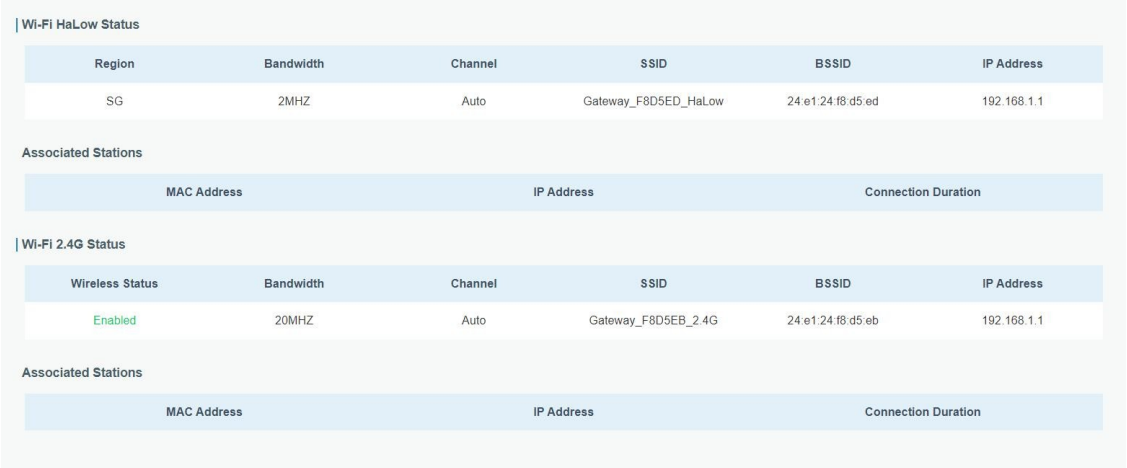


Netz	
Element	Beschreibung
Port	Zeigt den Namen des Ethernet-Ports an.
Status	Zeigt den Status des Ethernet-Ports an. „Up“ bezieht sich auf einen Status, bei dem WAN aktiviert ist und das Ethernet-Kabel angeschlossen ist. „Down“ bedeutet, dass das Ethernet-Kabel nicht angeschlossen ist oder die WAN-Funktion deaktiviert ist.
Typ	Zeigt den Einwahl-Typ des Ethernet-Ports an.
IP-Adresse	Zeigt die IP-Adresse des Ethernet-Ports an.
Netzmaske	Zeigt die Netzmaske des Ethernet-Ports an.
Gateway	Zeigt das Gateway des Ethernet-Ports an.

DNS	Zeigt den DNS des Ethernet-Ports an.
Dauer	Zeigen Sie die Informationen darüber an, wie lange das Ethernet-Kabel mit dem Ethernet-Port verbunden ist, wenn der Port aktiviert ist. Sobald der Port deaktiviert oder das Ethernet-Kabel getrennt wird, wird die Dauer nicht mehr angezeigt.

6.1.4 WLAN

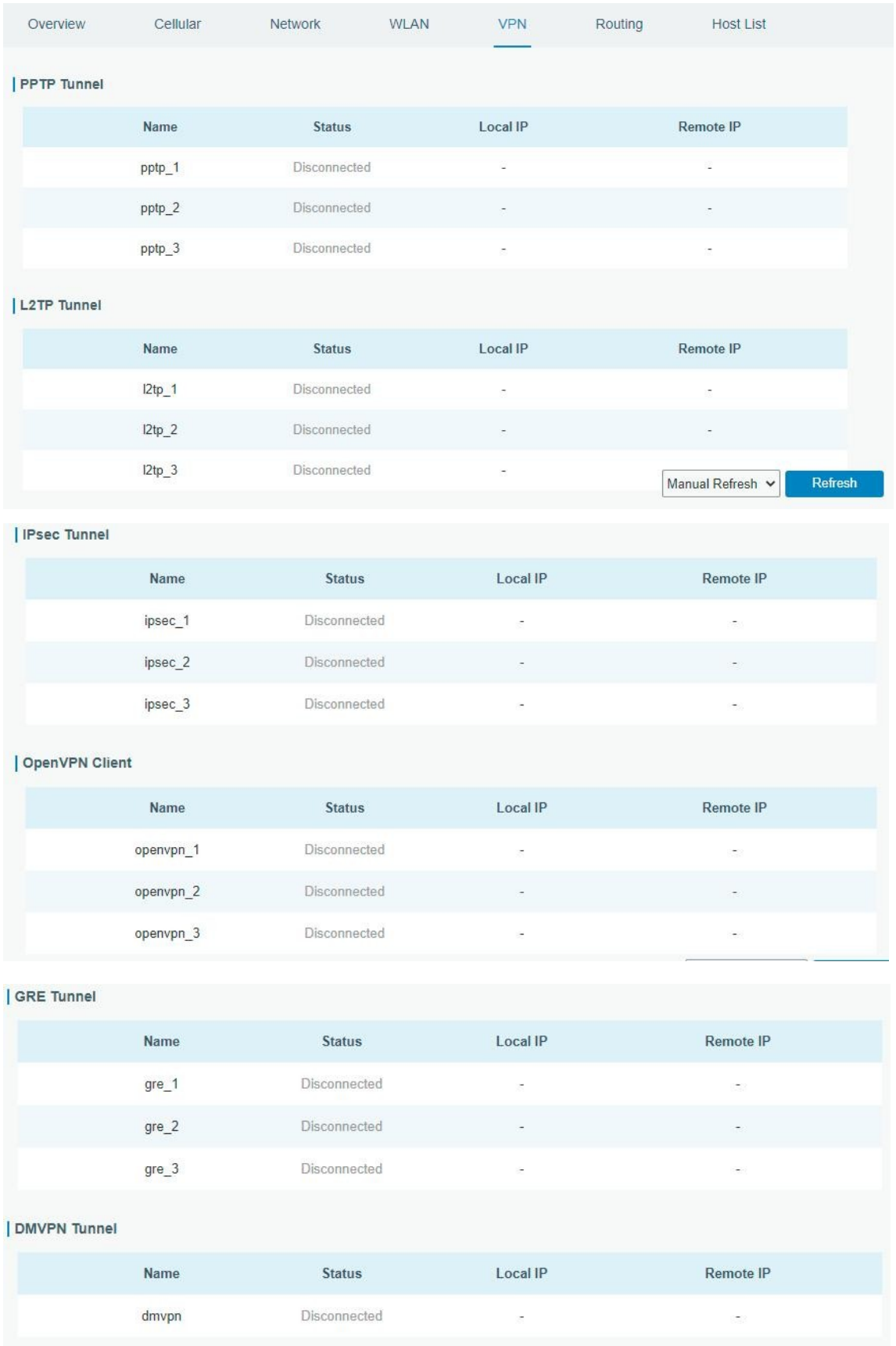
Auf dieser Seite können Sie den WLAN-Status überprüfen, einschließlich der Informationen zum Zugangspunkt und zum Client.



WLAN-Status	
Element	Beschreibung
WLAN HaLow/WLAN 2,4G-Status	
Region	Zeigt die Region an, in der Wi-Fi HaLow verwendet wird.
Drahtlosstatus	Zeigen Sie den Status des 2,4-GHz-WLANs an.
Bandbreite	Zeigt die verfügbare Bandbreite an.
Kanal	Zeigt den WLAN-Kanal an.
SSID	Zeigt die SSID an.
BSSID	Zeigt die BSSID an.
IP-Adresse	Zeigt die IP-Adresse des Gateways an.
Status	Zeigt den Verbindungsstatus an.
Zugehörige Stationen	
MAC-Adresse	Zeigt die MAC-Adresse des Clients an.
IP-Adresse	Zeigt die IP-Adresse des Clients an.
Verbindungsdauer	Zeigt Informationen darüber an, wie lange die Verbindung zum WLAN-Netzwerk besteht.

6.1.5 VPN

Auf dieser Seite können Sie den VPN-Status überprüfen, einschließlich PPTP, L2TP, IPsec, OpenVPN und DMVPN.



VPN-Status	
Element	Beschreibung

Name	Zeigt den Namen des VPN-Tunnels an.
Status	Zeigt den Status des VPN-Tunnels an.
Lokale IP	Zeigt die lokale Tunnel-IP des VPN-Tunnels an.
Remote-IP	Zeigt die Remote-Tunnel-IP des VPN-Tunnels an.

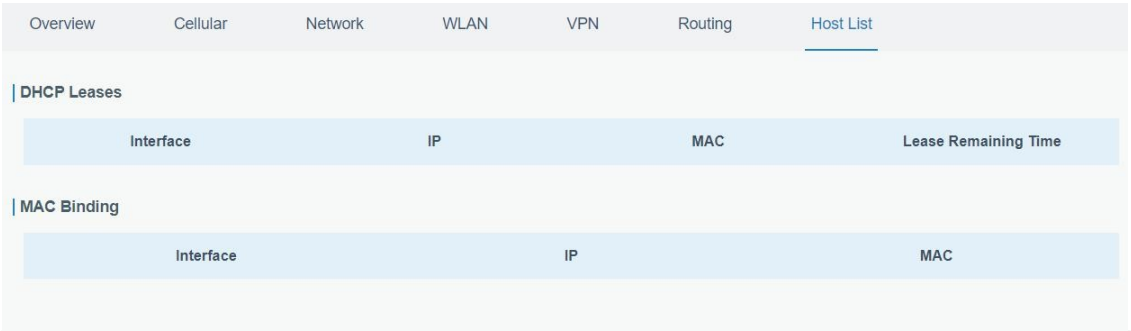
6.1.6 Routing

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

Element	Beschreibung
Routing-Tabelle	
Ziel	Zeigen Sie die IP-Adresse des Zielhosts oder des Zielnetzwerks an.
Netzmaske/Präfix Länge	Zeigt die Netzmaske oder Präfixlänge des Zielhosts oder Zielnetzwerks an.
Gateway	Zeigt die IP-Adresse des Gateways an.
Schnittstelle	Zeigt die ausgehende Schnittstelle der Route an.
Metrik	Zeigt die Metrik der Route an.
ARP-Cache	
IP	Zeigt die IP-Adresse des ARP-Pools an.
MAC	Zeigt die der IP-Adresse entsprechende MAC-Adresse an.
Schnittstelle	Zeigt die Bindungsschnittstelle von ARP an.

6.1.7 Host-Liste

Auf dieser Seite können Sie die Host-Informationen einsehen.



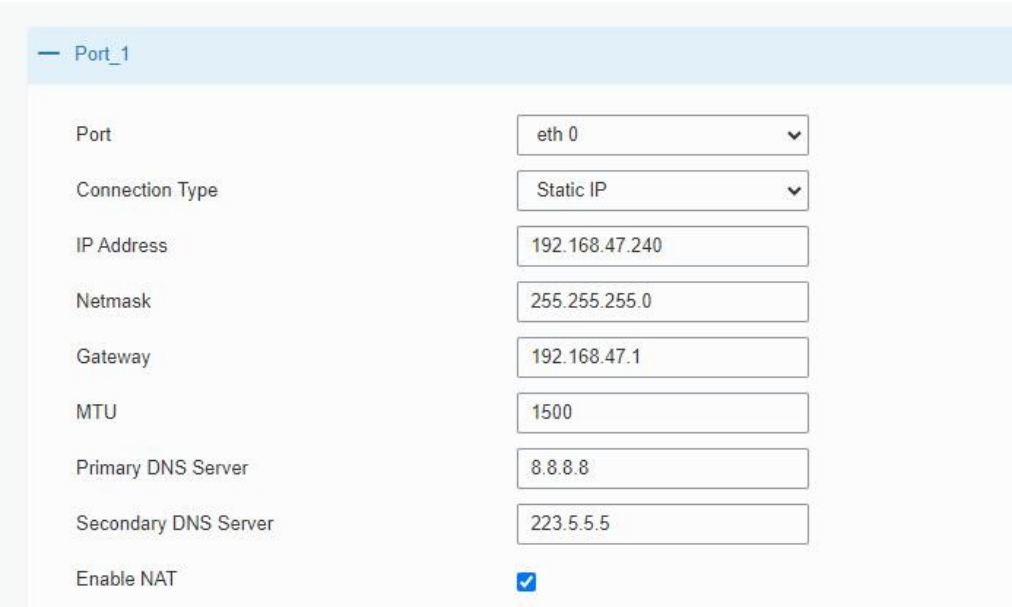
Host-Liste	
Element	Beschreibung
DHCP-Leases	
Schnittstelle	Zeigt die Schnittstelle an: Wi-Fi HaLow oder Wi-Fi 2,4G.
IP	IP-Adresse des DHCP-Clients anzeigen
MAC-Adresse	MAC-Adresse des DHCP-Clients anzeigen
Verbleibende Leasingdauer	Anzeige der verbleibenden Lease-Zeit des DHCP-Clients.
MAC-Bindung	
Schnittstelle	Schnittstelle anzeigen: Wi-Fi HaLow oder Wi-Fi 2,4G.
IP & MAC	Zeigen Sie die IP-Adresse und MAC-Adresse an, die in der Liste „Statische IP“ festgelegt sind. des DHCP-Dienstes.

6.2 Netzwerk

6.2.1 Schnittstelle

6.2.1.1 Anschluss

Der Ethernet-Port kann mit einem Ethernet-Kabel verbunden werden, um einen Internetzugang zu erhalten.



Port-Einstellung

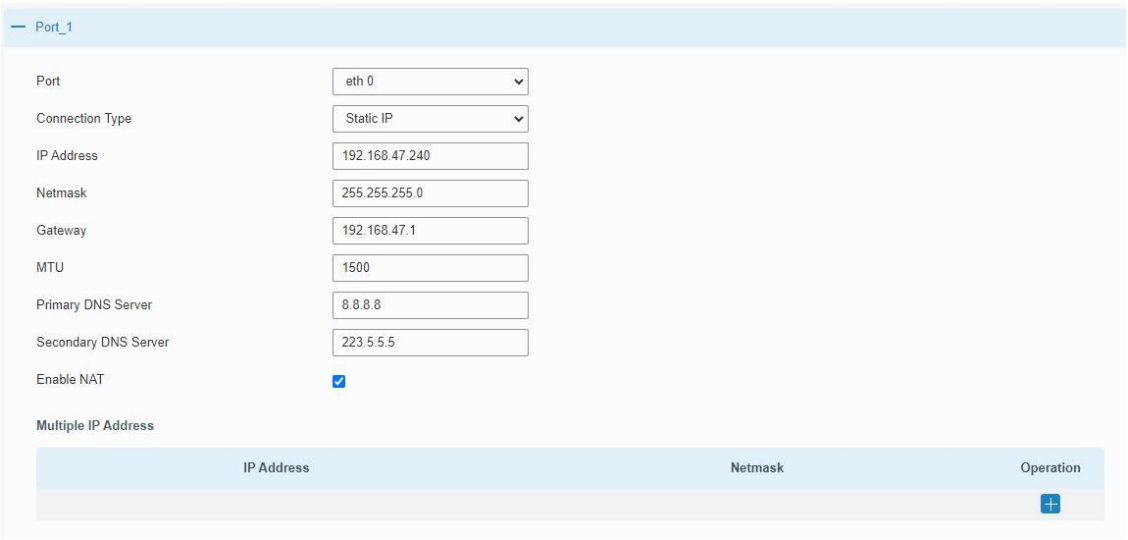
Element	Beschreibung	Standard
Port	Der Port, der als eth0-Port festgelegt und aktiviert ist.	eth 0
Verbindungstyp	Wählen Sie zwischen „Statische IP“, „DHCP-Client“ und „PPPoE“. Statische IP: Konfigurieren Sie die IP-Adresse, die Netzmaske und das Gateway für die Ethernet-WAN-Schnittstelle. DHCP-Client: Konfigurieren Sie die Ethernet-WAN-Schnittstelle als DHCP-Client, um die IP-Adresse automatisch zu beziehen. PPPoE: Ethernet-WAN-Schnittstelle als PPPoE-Client konfigurieren.	Statische IP
MTU	Legen Sie die maximale Übertragungseinheit fest.	1500
Primärer DNS Server	Legen Sie den primären DNS fest.	8.8.8.8
Sekundärer DNS Server	Sekundären DNS festlegen.	223.5.5.5
NAT aktivieren	Aktivieren oder deaktivieren Sie die NAT-Funktion. Wenn diese Funktion aktiviert ist, kann eine private IP-Adresse in eine öffentliche IP-Adresse übersetzt werden.	Aktivieren

Beispiel für eine zugehörige Konfiguration

Ethernet-Verbindung

1. Statische IP-Konfiguration

Wenn das externe Netzwerk dem Ethernet-Port eine feste IP zuweist, kann der Benutzer diesen Modus auswählen.



Statische IP		
Artikel	Beschreibung	Standard
IP-Adresse	Legen Sie die IP-Adresse fest, die auf das Internet zugreifen kann.	192.168.23.150
Netzmaske	Legen Sie die Netzmaske für den Ethernet-Port fest.	255.255.255.0
Gateway	Legen Sie die IP-Adresse des Gateways für den Ethernet-Port fest.	192.168.23.1
Mehrere IP-Adressen Adresse	Legen Sie die mehreren IP-Adressen für den Ethernet-Port fest.	Null

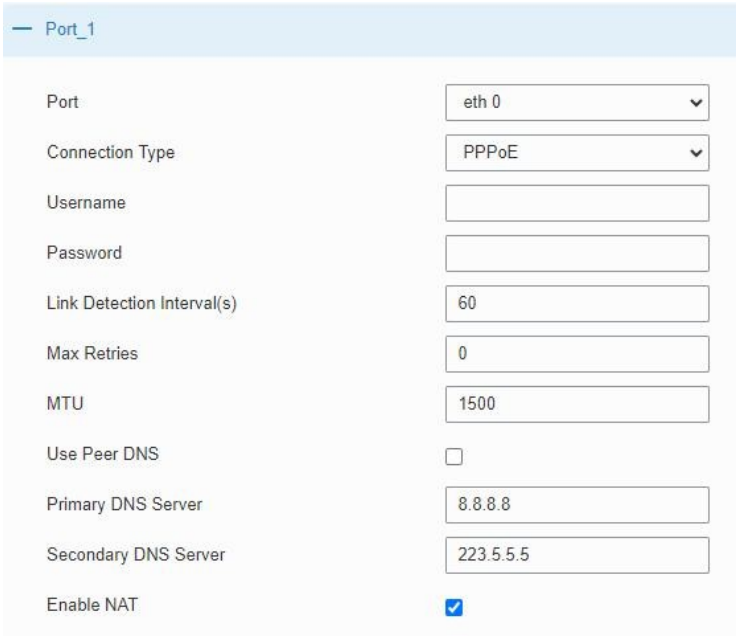
2. DHCP-Client

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	
Element	Beschreibung
Peer-DNS verwenden	Peer-DNS automatisch während des PPP-Wählvorgangs abrufen. DNS ist erforderlich, wenn der Benutzer einen Domänennamen aufruft.

3. PPPoE

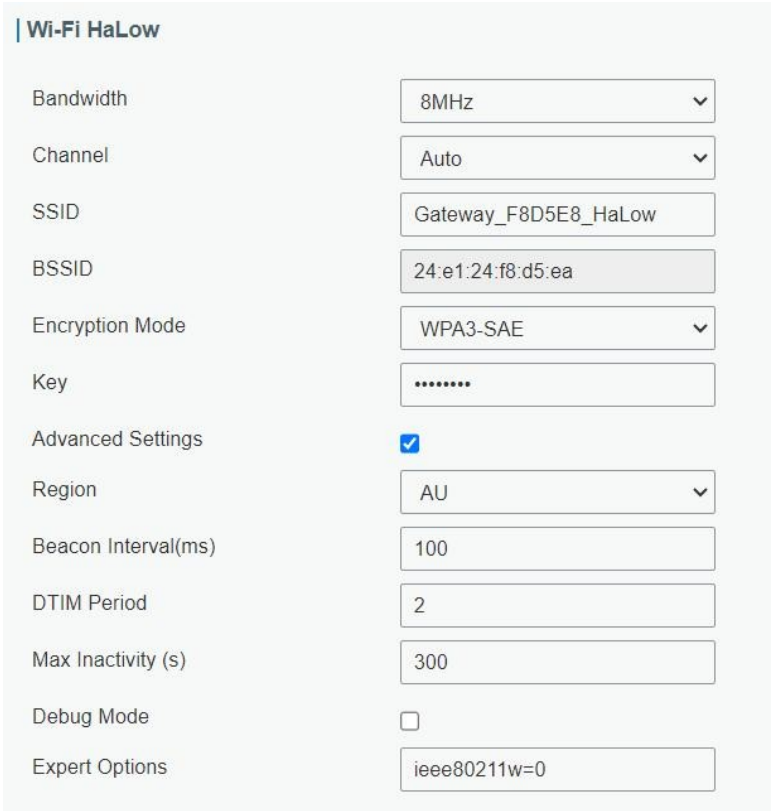
PPPoE steht für „Point-to-Point Protocol over Ethernet". Der Benutzer muss einen PPPoE-Client auf der Grundlage der ursprünglichen Verbindungsart installieren. Mit PPPoE können Fernzugriffsgeräte die Kontrolle über jeden Benutzer übernehmen.



PPPoE	
Element	Beschreibung
Benutzername	Geben Sie den Benutzernamen ein, den Sie von Ihrem Internetdienstanbieter (ISP) erhalten haben.
Passwort	Geben Sie das Passwort ein, das Sie von Ihrem Internetdienstanbieter (ISP) erhalten haben.
Link-Erkennung Intervall (s)	Legen Sie das Heartbeat-Intervall für die Verbindungserkennung fest. Bereich: 1-600.
Maximale Wiederholungsversuche	Legen Sie die maximale Anzahl der Wiederholungsversuche nach einem fehlgeschlagenen Verbindungsaufbau fest. Bereich: 0-9.
Peer-DNS verwenden	Peer-DNS während des PPP-Wählvorgangs automatisch abrufen. DNS ist erforderlich , wenn der Benutzer einen Domänennamen aufruft.

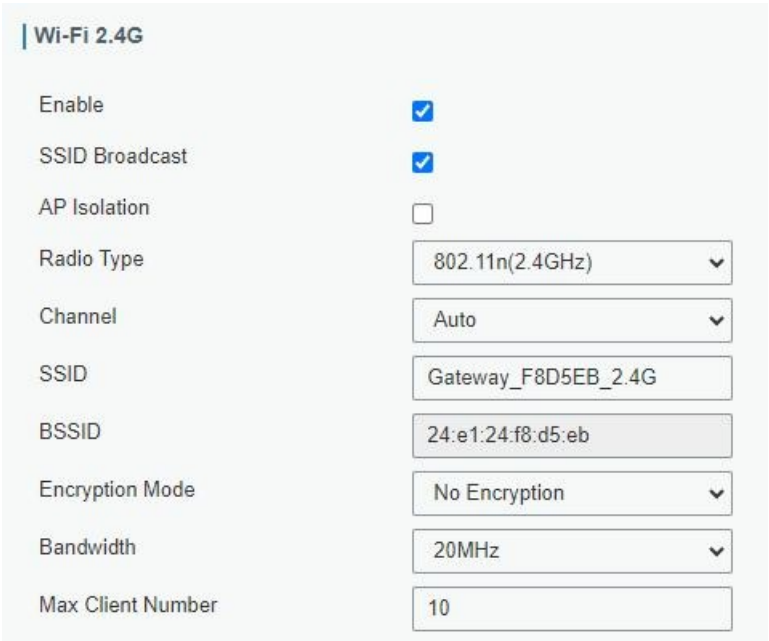
6.2.1.2 WLAN

In diesem Abschnitt wird erläutert, wie Sie die entsprechenden Parameter für Wi-Fi 2.4G- und Wi-Fi HaLow-Netzwerke einstellen. HL31 kann als Wi-Fi 2.4G- oder Wi-Fi HaLow-Zugangspunkt fungieren, um Verbindungen zu ermöglichen.



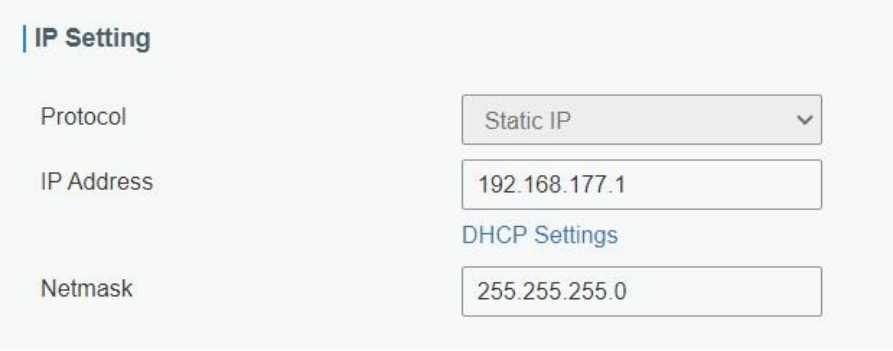
Wi-Fi HaLow-Einstellungen	
Element	Beschreibung
Bandbreite	Wählen Sie die Arbeitsbandbreite aus. Die Optionen unterscheiden sich je nach Region. Eine höhere Bandbreite erhöht die Datenrate, die Übertragungsentfernung wird kürzer.
Kanal	Wählen Sie den WLAN-Kanal aus. Die Optionen variieren je nach Region.
SSID	Geben Sie die SSID des Zugangspunkts ein. Standard: Gateway_XXXXXX_HaLow (XXXXXX = letzte 6 Ziffern der MAC-Adresse)
BSSID	Die MAC-Adresse des Zugangspunkts. Entweder die SSID oder die BSSID kann eingegeben werden, um sich mit dem Netzwerk zu verbinden.

Verschlüsselungsmodus	Wählen Sie den Verschlüsselungsmodus aus. Die Optionen sind „Keine Verschlüsselung“ und „WPA3-SAE“.
Schlüssel	Geben Sie den vorab geteilten Schlüssel der WPA3-Verschlüsselung ein.
Erweiterte Einstellungen	
Region	Die Region der Frequenz. Dieser Parameter sollte mit dem von Wi-Fi HaLow-Clients übereinstimmen.
Beacon-Intervall (ms)	Das Intervall für die Übertragung der Beacons an Wi-Fi HaLow-Clients.
DTIM-Periode	Der Zeitraum, in dem DTIM-Nachrichten an Wi-Fi HaLow-Clients gesendet werden. DTIM ist ein Nachricht, die mit Beacons gesendet wird, um Wi-Fi HaLow-Clients aus dem Ruhezustand zu „wecken“.
Maximale Inaktivität (s)	Wenn ein Client innerhalb dieses Intervalls nichts sendet, sendet das Gateway einen Frame an den Client, um die Verbindung zu überprüfen. Wenn keine Antwort erfolgt, trennt das trennt das Gateway die Verbindung zu diesem Client.
Debug-Modus	Nach der Aktivierung werden in den Gateway-Protokolldateien Debug-Protokollinformationen ausgegeben.
Expertenoptionen	Geben Sie einige andere PPP-Initialisierungszeichenfolgen ein, um erweiterte Einstellungen zu erzielen Einstellungen zu erzielen.



WLAN-2,4G-Einstellungen	
Element	**Beschreibung**
Aktivieren	Aktivieren/Deaktivieren von WLAN 2,4G.
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.
AP-Isolation	Wenn die AP-Isolation aktiviert ist, sind alle Benutzer, die auf den AP zugreifen, isoliert, ohne miteinander kommunizieren zu können.
Funkmodus	Wählen Sie den Funkstandard aus. Die Optionen sind „802.11b (2,4 GHz)“, „802.11g

	(2,4 GHz)“, „802.11n (2,4 GHz)“.
Kanal	Wählen Sie den WLAN-Kanal aus. Die Optionen sind „Auto“, „1“, „2“.....„13“.
BSSID	Die MAC-Adresse des Zugangspunkts. Entweder die SSID oder die BSSID kann eingegeben werden, um sich mit dem Netzwerk zu verbinden.
SSID	Geben Sie die SSID des Zugangspunkts ein. Standard: Gateway_XXXXXX_2.4G (XXXXXX=die letzten 6 Ziffern der MAC-Adresse)
Verschlüsselungsmodus	Wählen Sie den Verschlüsselungsmodus aus. Die Optionen sind „Keine Verschlüsselung“, „WEP Open System“, „WEP Shared Key“, „WPA-PSK“, „WPA2-PSK“ und „WPA-PSK/WPA2-PSK“.
Verschlüsselung	Wählen Sie die Verschlüsselung aus. Die Optionen sind „Auto“, „AES“, „TKIP“ und „AES/TKIP“.
Schlüssel	Geben Sie den vorab geteilten Schlüssel der WEP/WPA-Verschlüsselung ein. Standard: iotpassword
Bandbreite	Wählen Sie die Bandbreite aus. Die Optionen sind „20 MHz“ und „40 MHz“.
Maximale Client-Anzahl	Legen Sie die maximale Anzahl von Clients fest, die sich mit diesem Zugangspunkt verbinden können. Bereich: 1-15



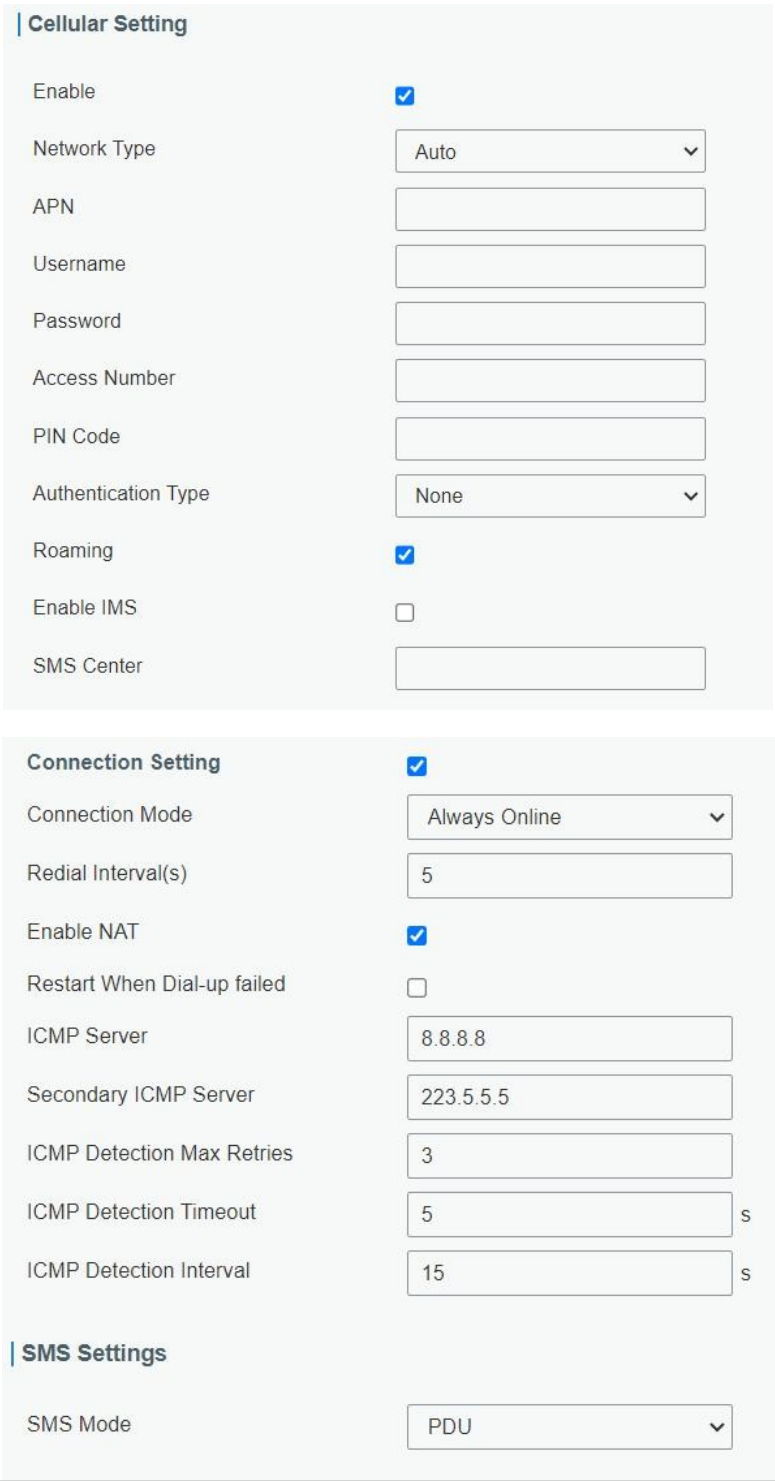
IP-Einstellung	
Element	Beschreibung
Protokoll	Es ist als statische IP festgelegt.
IP-Adresse	Legen Sie die WLAN-IP-Adresse dieses Geräts fest. Wi-Fi HaLow und Wi-Fi 2,4 GHz verwenden dieselbe IP-Adresse.
Netzmaske	Legen Sie die Netzmaske der IP-Adresse fest.

Verwandtes Thema

Beispiel für eine WLAN-Anwendung

6.2.1.3 Mobilfunk (nur Mobilfunkversion)

In diesem Abschnitt wird erläutert, wie Sie die entsprechenden Parameter für das Mobilfunknetz einstellen.



Allgemeine Einstellungen	
Element	Beschreibung
Aktivieren	Aktivieren oder deaktivieren Sie die Registrierung des Geräts im Mobilfunknetz.
Netzwerktyp	Wählen Sie zwischen „Auto“, „Auto 3G/4G“, „Nur 4G“ und „Nur 3G“. Auto: Verbindet sich automatisch mit dem Netzwerk mit dem stärksten Signal. Nur 4G: Verbindet sich nur mit dem 4G-Netzwerk. Und so weiter.
APN	Geben Sie den Zugangspunktnamen für die Mobilfunk-Einwahlverbindung ein, der

	Ihrem lokalen Internetdienstanbieter bereitgestellt wird.
Benutzername	Geben Sie den Benutzernamen für die vom lokalen ISP bereitgestellte Mobilfunk-Einwahlverbindung ein Internetdienstanbieters bereitgestellt wird.
Passwort	Geben Sie das Passwort für die Mobilfunk-Einwahlverbindung ein, das Ihnen von Ihrem lokalen Internetdienstanbieter bereitgestellt wurde.
Zugangsnummer	Geben Sie die Nummer des Einwahlzentrums ein. Für mobile Einwahlverbindungen, die vom lokalen ISP bereitgestellt wird.
PIN-Code	Geben Sie einen 4-8-stelligen PIN-Code ein, um die SIM-Karte zu entsperren.
Authentifizierung Typ	Wählen Sie zwischen KEINE, PAP und CHAP.
Roaming	Roaming aktivieren oder deaktivieren.
IMS aktivieren	IMS-Funktion aktivieren oder deaktivieren.
SMS-Zentrale	Geben Sie die Nummer des lokalen SMS-Centers ein, um SMS-Nachrichten zu speichern, weiterzuleiten, zu konvertieren und Zustellung von SMS-Nachrichten.
NAT aktivieren	NAT-Funktion aktivieren oder deaktivieren.
Neustart bei Einwahl fehlgeschlagen	Wenn diese Funktion aktiviert ist, startet das Gateway automatisch neu , wenn die Einwahl mehrmals fehlschlägt.
ICMP-Server	Legen Sie die IP-Adresse des ICMP-Erkennungsservers fest.
Sekundärer ICMP Server	Legen Sie die IP-Adresse des sekundären ICMP-Erkennungsservers fest.
ICMP-Erkennung Maximale Wiederholungsversuche	Legen Sie die maximale Anzahl von Wiederholungsversuchen fest, wenn die ICMP-Erkennung fehlschlägt.
ICMP-Erkennung Zeitlimit	Legen Sie das Zeitlimit für die ICMP-Erkennung fest.
ICMP-Erkennung Intervall	Intervall für die ICMP-Erkennung einstellen.
SMS-Modus	Wählen Sie den SMS-Modus aus TEXT und PDU aus.

Element	Beschreibung
Verbindungsmodus	
Verbindungsmodus	Wählen Sie zwischen „Immer online“ und „Bei Bedarf verbinden“.
Wiederwahlintervall(e)	Legen Sie das Zeitintervall zwischen den Wahlwiederholungen fest. Bereich: 0-3600.
Maximale Leerlaufzeit	Legen Sie die maximale Dauer fest, während der das Gateway im Leerlaufzustand bleibt, wenn die aktuelle Verbindung im Leerlaufstatus ist. Bereich: 10-3600.

Durch Anruf ausgelöst	Das Gateway wechselt automatisch vom Offline-Modus in den Mobilfunknetzmodus, wenn es einen Anruf von der angegebenen Telefonnummer erhält.
Anrufgruppe	Wählen Sie eine Anrufgruppe für den Anrufauslöser aus. Gehen Sie zu System > Allgemein Einstellungen > Telefon, um die Telefongruppe einzurichten.
Ausgelöst durch SMS	Das Gateway wechselt automatisch vom Offline-Modus in den Mobilfunkmodus , wenn es eine bestimmte SMS von einem bestimmten Mobiltelefon empfängt.
SMS-Gruppe	Wählen Sie eine SMS-Gruppe für die Auslösung aus. Gehen Sie zu System > Allgemeine Einstellungen > Telefon, um die SMS-Gruppe einzurichten.
SMS-Text	Geben Sie den SMS-Inhalt für den Auslöser ein.

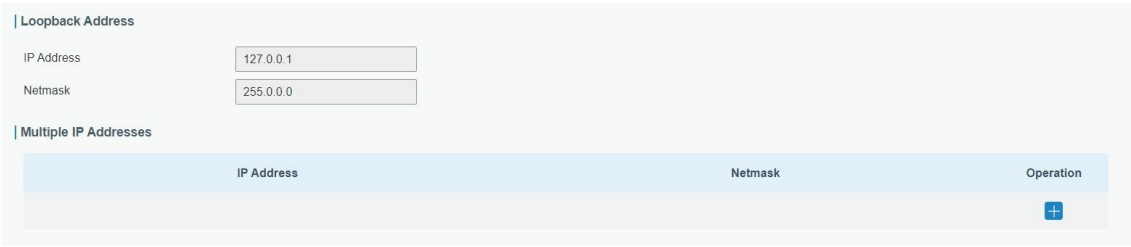
Verwandte Themen

Anwendungsbeispiel für Mobilfunkverbindung

Telefongruppe

6.2.1.4 Loopback

Die Loopback-Schnittstelle wird zum Ersetzen der Gateway-ID verwendet, solange sie aktiviert ist. Wenn die Schnittstelle DOWN istmuss die ID des Gateways erneut ausgewählt werden, was zu einer langen Konvergenzzeit von OSPF führt. Daher wird die Loopback-Schnittstelle im Allgemeinen als ID des Gateways empfohlen.
Die Loopback-Schnittstelle ist eine logische und virtuelle Schnittstelle auf dem Gateway. Unter Standardbedingungen gibt es keine Loopback-Schnittstelle auf dem Gateway, sie kann jedoch bei Bedarf erstellt werden.



Loopback		
Element	Beschreibung	Standard
IP-Adresse	Unveränderlich	127.0.0.1
Netzmaske	Unveränderlich	255.0.0.0
Mehrere IP-Adressen Adressen	Abgesehen von der oben genannten IP-Adresse kann der Benutzer weitere IP-Adressen konfigurieren. Adressen	Null

6.2.1.5 VLAN-Trunk

Der HL31-Gateway unterstützt den Ethernet-Port als VLAN-Trunk-Client und kann eine VLAN-ID zugewiesen bekommen, was die Klassifizierung des Datenverkehrs erleichtert. Wenn die VLAN-ID festgelegt ist, kann der Port unter „Netzwerk > Schnittstelle > Port“ als eth0.x ausgewählt werden, wobei x für die VLAN-ID steht. Die VLAN-Einstellung ist standardmäßig leer

. Sie können eine neue VLAN-Kennzeichnung zu einer bestimmten Schnittstelle hinzufügen, indem Sie auf „  “ klicken.

VLAN-Trunk	
Element	Beschreibung
Schnittstelle	Wählen Sie die VLAN-Schnittstelle aus, sie ist als eth0 festgelegt.
VID	Legen Sie die Label-ID des VLAN fest. Bereich: 1-4094.

6.2.2 Firewall

In diesem Abschnitt wird beschrieben, wie Sie die Firewall-Parameter einstellen, darunter Website-Blockierung, ACL, DMZ, Port-Zuordnung und MAC-Bindung.
Die Firewall implementiert eine entsprechende Kontrolle des Datenflusses in Eingangsrichtung (vom Internet zum lokalen Netzwerk) und Ausgangsrichtung (vom lokalen Netzwerk zum Internet) entsprechend den Inhaltsmerkmalen der Pakete, wie z. B. Protokollstil, Quell-/Ziel-IP-Adresse usw. Sie stellt sicher, dass das Gateway in einer sicheren Umgebung und der Host im lokalen Netzwerk betrieben werden.

6.2.2.1 Sicherheit

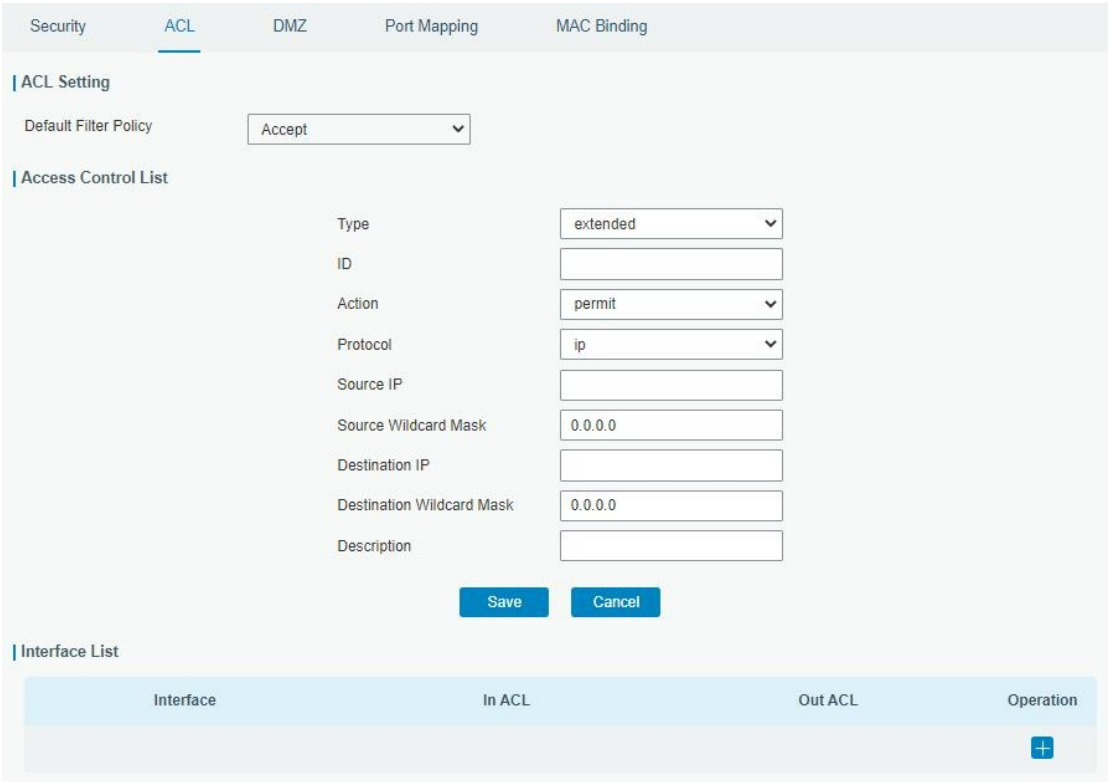
Website-Sperrung	
URL-Adresse	Geben Sie die HTTP-Adresse ein, die Sie sperren möchten.
Stichwort	Sie können bestimmte Websites blockieren, indem Sie ein Schlüsselwort eingeben. Die maximal zulässige Zeichenanzahl beträgt 64.

6.2.2.2 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 Netzwerkverkehr zu filtern. Wenn das Gateway ein Paket empfängt,

Das Feld wird gemäß der ACL-Regel analysiert, die auf die aktuelle Schnittstelle angewendet wird. Nachdem das spezielle Paket identifiziert wurde, wird die Berechtigung oder Sperrung des entsprechenden Pakets gemäß der voreingestellten Strategie umgesetzt.

Die von ACL definierten Regeln für die Datenpaketzuordnung können auch von anderen Funktionen verwendet werden, die eine Unterscheidung des Datenflusses erfordern.



Element	Beschreibung
ACL-Einstellung	
Standardfilterrichtlinie	Wählen Sie zwischen „Akzeptieren“ und „Ablehnen“. Die Pakete, die nicht in der Zugriffskontrollliste enthalten sind, werden gemäß der Standardfilterrichtlinie verarbeitet.
Zugriffskontrollliste	
Typ	Wählen Sie den Typ aus „Erweitert“ und „Standard“.
ID	Benutzerdefinierte ACL-Nummer. Bereich: 1-199.
Aktion	Wählen Sie zwischen „Zulassen“ und „Verweigern“.
Protokoll	Wählen Sie das Protokoll aus „ip“, „icmp“, „tcp“, „udp“ und „1-255“ aus.
Quell-IP	Quellnetzwerkadresse (wenn Sie das Feld leer lassen, bedeutet dies „alle“).
Quell-Wildcard Maske	Platzhaltermaske der Quellnetzwerkadresse.
Ziel-IP	Zielnetzwerkadresse (0.0.0.0 bedeutet alle).
Ziel-Wildcard Maske	Wildcard-Maske der Zieladresse.
Beschreibung	Geben Sie eine Beschreibung für die Gruppen mit derselben ID ein.
ICMP-Typ	Geben Sie den Typ des ICMP-Pakets ein. Bereich: 0-255.
ICMP-Code	Geben Sie den Code des ICMP-Pakets ein. Bereich: 0-255.
Quellporttyp	Wählen Sie den Quellporttyp aus, z. B. angegebener Port, Portbereich usw.

Quellport	Legen Sie die Quellportnummer fest. Bereich: 1-65535.
Start-Quellport	Legen Sie die Startnummer des Quellports fest. Bereich: 1-65535.
Endpunkt des Quellports	Legen Sie die Nummer des Endquellports fest. Bereich: 1-65535.
Zielport Typ	Wählen Sie den Typ des Zielports aus, z. B. angegebener Port, Portbereich, usw.
Zielport	Zielportnummer festlegen. Bereich: 1-65535.
Startziel Port	Startzielportnummer festlegen. Bereich: 1-65535.
Endzielport	Legen Sie die Endzielportnummer fest. Bereich: 1-65535.
Weitere Details	Informationen zum Port anzeigen.
Schnittstellenliste	
Schnittstelle	Wählen Sie die Netzwerkschnittstelle für die Zugriffskontrolle aus.
In ACL	Wählen Sie eine Regel für eingehenden Datenverkehr aus der ACL-ID aus.
Ausgehende ACL	Wählen Sie eine Regel für ausgehenden Datenverkehr aus der ACL-ID aus.

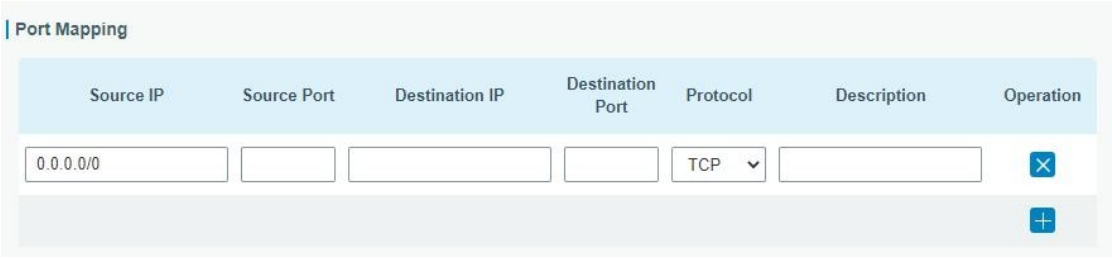
6.2.2.3 DMZ

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.
Quelladresse	Legen Sie die Quell-IP-Adresse fest, die auf den DMZ-Host zugreifen kann. „0.0.0.0/0“ bedeutet „beliebige Adresse“.

6.2.2.4 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 und wandelt sie in eine interne Verbindung um. Diese Umwandlung wird als DNAT bezeichnet und wird hauptsächlich für externe und interne Dienste verwendet.



Port-Zuordnung	
Element	Beschreibung
Quell-IP	Geben Sie den Host oder das Netzwerk an, das auf die lokale IP-Adresse zugreifen kann. 0.0.0.0/0 bedeutet alle.
Quellport	Geben Sie den TCP- oder UDP-Port ein, von dem aus eingehende Pakete empfangen werden sollen. weitergeleitet. Bereich: 1-65535.
Ziel-IP	Geben Sie die IP-Adresse ein, an die Pakete nach dem Empfang weitergeleitet werden von der eingehenden Schnittstelle empfangen wurden.
Zielport	Geben Sie den TCP- oder UDP-Port ein, an den Pakete weitergeleitet werden, nachdem vom eingehenden Port (den eingehenden Ports) empfangen wurden. Bereich: 1-65535.
Protokoll	Wählen Sie TCP oder UDP entsprechend den Anforderungen Ihrer Anwendung.
Beschreibung	Die Beschreibung dieser Regel.

Beispiel für eine zugehörige Konfiguration

NAT-Anwendungsbeispiel

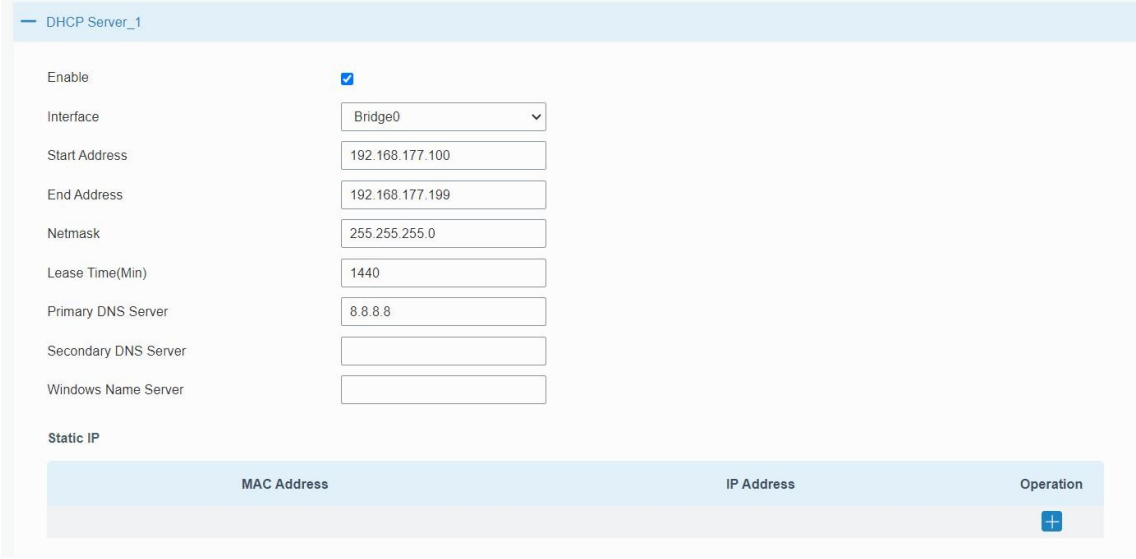
6.2.2.5 MAC-Bindung

MAC-Bindung wird verwendet, um Hosts durch Abgleich von MAC-Adressen und IP-Adressen zu spezifizieren, die in der Liste der zugelassenen externen Netzwerkzugriffe enthalten sind.

MAC-Bindungsliste	
Element	Beschreibung
MAC-Adresse	Legen Sie die zugeordnete MAC-Adresse fest.
IP-Adresse	Legen Sie die zugeordnete IP-Adresse fest.
Beschreibung	Geben Sie eine Beschreibung ein, um die Bedeutung der Bindungsregel für jedes MAC-IP-Paar zu dokumentieren.

6.2.3 DHCP

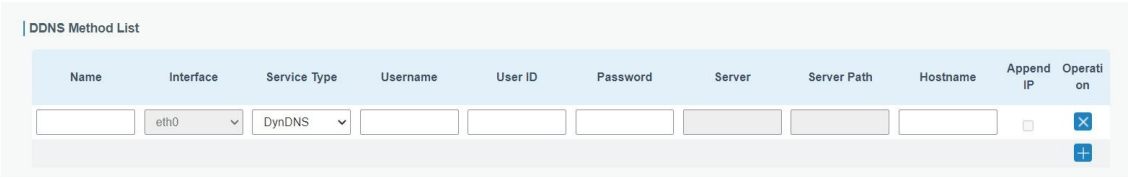
HL31 kann als DHCP-Server eingerichtet werden, um IP-Adressen an WLAN-Clients zu verteilen. Wi-Fi HaLow und Wi-Fi 2,4 GHz verwenden denselben DHCP-IP-Adressbereich.



DHCP-Server		
Element	Beschreibung	Standard
Aktivieren	DHCP-Server aktivieren oder deaktivieren.	Aktiv
Schnittstelle	Die Schnittstelle, über die IP-Adressen zugewiesen werden sollen.	Bridge0
Start Adresse	Definieren Sie den Anfang des Pools von IP-Adressen , die an DHCP-Clients vergeben werden sollen.	192.168.1.100
Endadresse	Legen Sie das Ende des Pools von IP-Adressen fest, die an DHCP-Clients vermietet werden.	192.168.1.199
Netzmaske	Definieren Sie die Subnetzmaske der IP-Adresse, die von DHCP-Clients vom DHCP-Server erhalten wurde.	255.255.255.0
Lease-Zeit (Min)	Legen Sie die Lease-Zeit fest, während der der Client die vom DHCP-Server erhaltene IP-Adresse verwenden kann vom DHCP-Server erhaltene IP-Adresse nutzen kann. Bereich: 1-10080.	1440
Primärer DNS-Server	Legen Sie den primären DNS-Server fest.	8.8.8.8
Sekundär DNS-Server	Sekundären DNS-Server festlegen.	Null
Windows-Name Server	Definieren Sie den Windows Internet Naming Service, den DHCP-Clients vom DHCP-Server erhalten. Im Allgemeinen können Sie dieses Feld leer lassen.	Null
Statische IP		
MAC Adresse	Legen Sie eine statische und spezifische MAC-Adresse für den DHCP-Client fest (sie sollte sich von anderen MAC-Adressen unterscheiden, um Konflikte zu vermeiden).	Null
IP-Adresse	Legen Sie eine statische und spezifische IP-Adresse für den DHCP (sie sollte außerhalb des DHCP-Bereichs liegen).	Null

6.2.4 DDNS

Dynamic DNS (DDNS) ist eine Methode, die einen Nameserver im Domain Name System automatisch aktualisiert, wodurch Benutzer eine dynamische IP-Adresse mit einem statischen Domainnamen verknüpfen 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
Name	Geben Sie dem DDNS einen aussagekräftigen Namen.
Schnittstelle	Legen Sie die mit dem DDNS gebündelte Schnittstelle fest.
Diensttyp	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.
Hostname	Geben Sie den Hostnamen für DDNS ein.
IP anhängen	Fügen Sie Ihre aktuelle IP-Adresse zum Aktualisierungspfad des DDNS-Servers hinzu.

6.2.5 Link-Failover

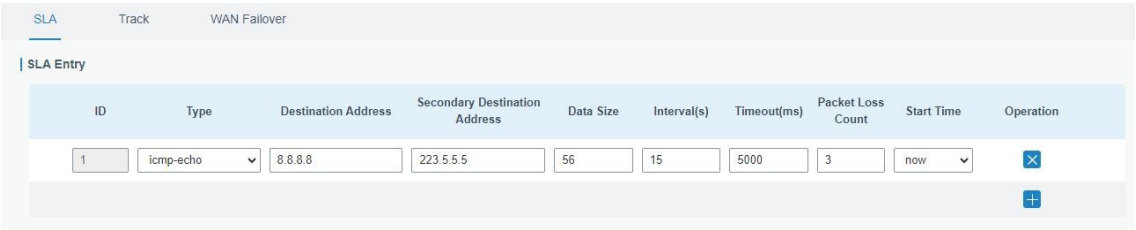
In diesem Abschnitt wird beschrieben, wie Sie Link-Failover-Strategien, z. B. VRRP-Strategien, konfigurieren.

Konfigurationsschritte

1. Definieren Sie einen oder mehrere SLA-Vorgänge (ICMP-Prüfung).
2. Definieren Sie ein oder mehrere Track-Objekte, um den Status des SLA-Betriebs zu verfolgen.
3. Definieren Sie Anwendungen, die mit Track-Objekten verbunden sind, wie VRRP oder statisches Routing.

6.2.5.1 SLA

Die SLA-Einstellung wird zur Konfiguration der Link-Prüfmethode verwendet. Der Standard-Prüftyp ist ICMP.



SLA		
Element	Beschreibung	Standard
ID	SLA-Index. Es können bis zu 10 SLA-Einstellungen hinzugefügt werden. Bereich: 1-10.	1

Typ	ICMP-ECHO ist der Standardtyp, um zu erkennen, ob die Verbindung aktiv ist.	icmp-echo
Zieladresse	Die erkannte IP-Adresse.	8.8.8.8
Sekundär Zieladresse	Die sekundäre erkannte IP-Adresse.	223.5.5.5
Datengröße	Benutzerdefinierte Datengröße. Bereich: 0-1000.	56
Intervall (s)	Benutzerdefiniertes Erkennungsintervall. Bereich: 1-608400.	30
Zeitlimit (ms)	Benutzerdefiniertes Zeitlimit für die Antwort zur Bestimmung ICMP-Erkennungsfehler. Bereich: 1-300000.	500
Anzahl der Paketverluste	Definieren Sie die Anzahl der Paketverluste in jeder SLA-Prüfung. Die SLA-Prüfung schlägt fehl, wenn die voreingestellte Anzahl der Paketverluste überschritten wird.	5
Startzeit	Startzeitpunkt der Erkennung; wählen Sie zwischen „Jetzt“ und einem Leerzeichen. Ein Leerzeichen bedeutet, dass die Erkennung dieser SLA Erkennung nicht startet.	Jetzt

6.2.5.2 Track

Die Track-Einstellung dient dazu, eine Verbindung zwischen dem SLA-Modul, dem Track-Modul und dem Anwendungsmodul herzustellen. Die Track-Einstellung befindet sich zwischen dem Anwendungsmodul und dem SLA-Modul und hat die Hauptaufgabe, die Unterschiede zwischen den verschiedenen SLA-Modulen abzuschirmen und einheitliche Schnittstellen für das Anwendungsmodul bereitzustellen.

Verknüpfung zwischen Track-Modul und SLA-Modul

Sobald Sie die Konfiguration abgeschlossen haben, wird die Verknüpfung zwischen dem Track-Modul und dem SLA-Modul hergestellt. Das SLA-Modul wird zur Erkennung des Verbindungsstatus, der Netzwerkleistung und zur Benachrichtigung des Track-Moduls verwendet. Die Erkennungsergebnisse helfen dabei, Statusänderungen zeitnah zu verfolgen.

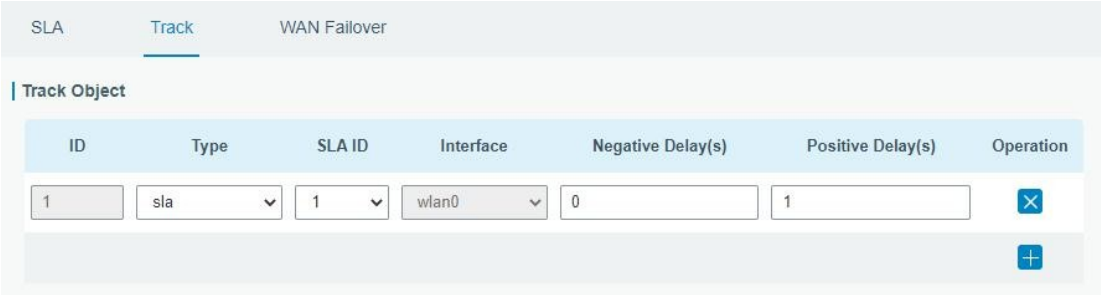
- Bei erfolgreicher Erkennung ist das entsprechende Track-Element positiv.
- Bei fehlgeschlagener Erkennung wird das entsprechende Track-Element als „Negativ“ gekennzeichnet.

Verbindung zwischen Track-Modul und Anwendungsmodul

Nach der Konfiguration wird die Verknüpfung zwischen dem Track-Modul und dem Anwendungsmodul hergestellt. Bei jeder Änderung eines Track-Elements wird eine Benachrichtigung, die eine entsprechende Maßnahme erfordert, an das Anwendungsmodul gesendet.

Derzeit können Anwendungsmodule wie VRRP und statisches Routing mit dem Track-Modul verknüpft werden.

Wenn eine sofortige Benachrichtigung an das Anwendungsmodul gesendet wird, kann die Kommunikation unter bestimmten Umständen aufgrund von Routing-Fehlern wie einer zeitnahen Wiederherstellung oder anderen Gründen unterbrochen werden. Daher kann der Benutzer einen Zeitraum festlegen, um die Benachrichtigung des Anwendungsmoduls zu verzögern, wenn sich der Status des verfolgten Elements ändert.

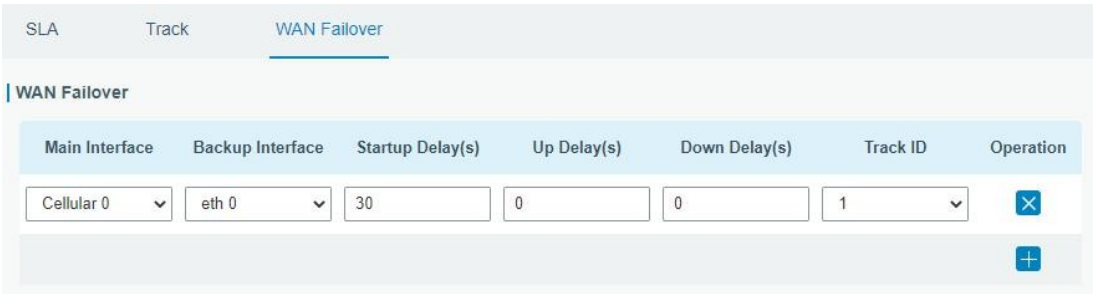


Element	Beschreibung	Standard
Index	Track-Index. Es können bis zu 10 Track-Einstellungen konfiguriert werden konfiguriert werden. Bereich: 1-10.	1
Typ	Die Optionen sind „sla" und „interface".	SLA
SLA-ID	Definierte SLA-ID.	1
Schnittstelle	Wählen Sie die Schnittstelle aus, deren Status ermittelt werden soll.	----
Negative Verzögerung (s)	Wenn die Schnittstelle ausgefallen ist oder die SLA-Prüfung fehlschlägt, wartet sie entsprechend der hier eingestellten Zeit, bevor sie ihren Status tatsächlich auf „Ausgefallen" ändert. Bereich: 0-180 (0 auf sofortige Umschaltung).	0
Positive Verzögerung (s)	Wenn eine Fehlerbehebung erfolgt, wartet das Gerät entsprechend der hier eingestellten Zeit, bevor es seinen Status tatsächlich auf „Up" (Aktiv) ändert. Bereich: 0-180 (0 bedeutet sofortige Umschalten).	1

6.2.5.3 WAN-Failover

WAN-Failover bezieht sich auf das Failover zwischen Ethernet-WAN-Schnittstelle und Mobilfunkschnittstelle. Wenn die Dienstübertragung aufgrund einer Fehlfunktion einer bestimmten Schnittstelle oder mangelnder Bandbreite nicht normal durchgeführt werden kann, kann die Datenrate schnell auf die Backup-Schnittstelle umgeschaltet werden. Dann übernimmt die Backup-Schnittstelle die Dienstübertragung und teilt sich den Netzwerkdatenverkehr, um die Zuverlässigkeit der Kommunikation der Datenausrüstung zu verbessern.

Wenn der Verbindungsstatus der Hauptschnittstelle von „aktiv" auf „inaktiv" wechselt, wird die voreingestellte Verzögerung aktiviert, anstatt sofort auf die Verbindung der Backup-Schnittstelle umzuschalten. Nur wenn der Status der Hauptschnittstelle nach Ablauf der Verzögerung weiterhin „inaktiv" ist, schaltet das System auf die Verbindung der Backup-Schnittstelle um. Andernfalls bleibt das System unverändert.



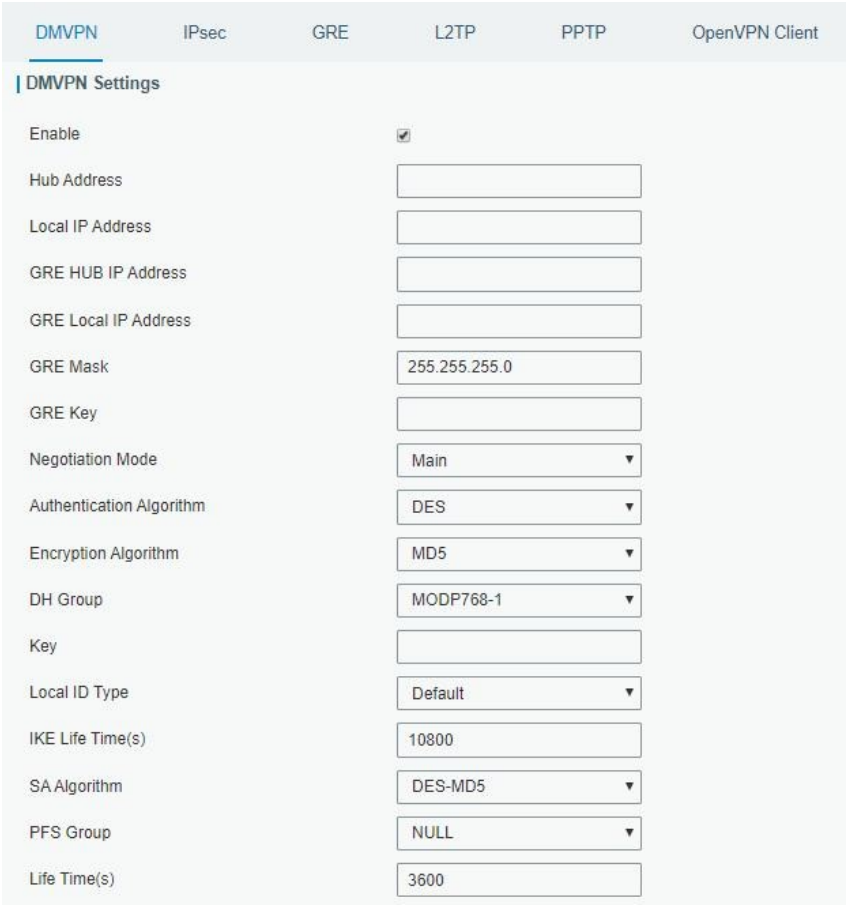
WAN-Failover		
Parameter	Beschreibung	Standard
Hauptschnittstelle	Wählen Sie eine Verbindungsschnittstelle als Hauptverbindung aus.	--
Sicherungs-Schnittstelle	Wählen Sie eine Verbindungsschnittstelle als Backup-Verbindung aus.	--
Startverzögerung (s)	Legen Sie fest, wie lange gewartet werden soll, bis die Richtlinie zur Startverfolgungserkennung in Kraft tritt. Bereich: 0-300.	30
Verzögerung beim Hochfahren (s)	Wenn die primäre Schnittstelle von einer fehlgeschlagenen Erkennung zu einer erfolgreichen Erkennung wechselt, kann der Wechsel basierend auf der eingestellten Zeit verzögert werden. Bereich: 0-180 (0 bezieht sich auf einen sofortigen Wechsel)	0
Verzögerung beim Herunterfahren (s)	Wenn die primäre Schnittstelle von einer erfolgreichen Erkennung zu einer fehlgeschlagenen Erkennung wechselt, kann der Wechsel basierend auf der eingestellten Zeit verzögert werden. Bereich: 0-180 (0 bedeutet sofortiges Umschalten).	0
Spur-ID	Spurerkennung, wählen Sie die definierte Spur-ID aus.	--

6.2.6 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. HL31 unterstützt DMVPN IPsec, GRE, L2TP, PPTP, OpenVPN sowie GRE über IPsec und L2TP über IPsec.

6.2.6.1 DMVPN

Ein dynamisches Multi-Point Virtual Private Network (DMVPN), das mGRE und IPsec kombiniert, ist ein sicheres Netzwerk, das Daten zwischen Standorten austauscht, ohne den Datenverkehr über den VPN-Server oder das Gateway der Unternehmenszentrale zu leiten.



DMVPN	
Element	Beschreibung
Aktivieren	DMVPN aktivieren oder deaktivieren.
Hub-Adresse	Die IP-Adresse oder der Domänenname des DMVPN-Hubs.
Lokale IP-Adresse	Lokale Tunnel-IP-Adresse von DMVPN.
GRE-Hub-IP-Adresse	IP-Adresse des GRE-Hub-Tunnels.
Lokale GRE-IP-Adresse	Lokale GRE-Tunnel-IP-Adresse.
GRE-Netzmaske	Lokale GRE-Tunnel-Netzmaske.
GRE-Schlüssel	GRE-Tunnels-Schlüssel.
Verhandlungsmodus	Wählen Sie zwischen „Main“ und „Aggressive“.
Authentifizierung Algorithmus	Wählen Sie zwischen „DES“, „3DES“, „AES128“, „AES192“ und „AES256“.
Verschlüsselungsalgorithmus	Wählen Sie zwischen „MD5“ und „SHA1“.
DH-Gruppe	Wählen Sie zwischen „MODP768_1“, „MODP1024_2“ und „MODP1536_5“.

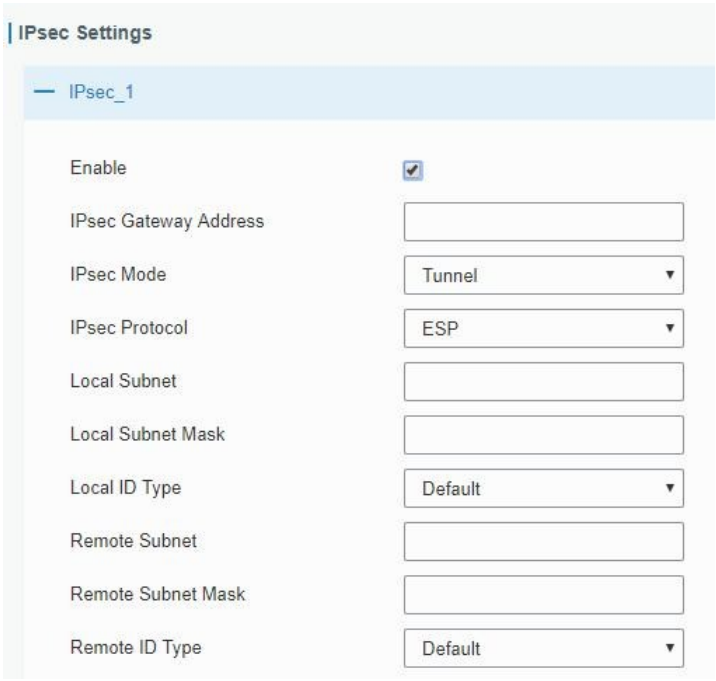
Schlüssel	Geben Sie den vorab vereinbarten Schlüssel ein.
Lokale ID-Art	Wählen Sie zwischen „Standard“, „ID“, „FQDN“ und „Benutzer-FQDN“
IKE-Lebensdauer (s)	Legen Sie die Lebensdauer in der IKE-Verhandlung fest. Bereich: 60-86400.
SA-Algorithmus	Wählen Sie zwischen „DES_MD5“, „DES_SHA1“, „3DES_MD5“, „3DES_SHA1“, „AES128_MD5“, „AES128_SHA1“, „AES192_MD5“, „AES192_SHA1“, „AES256_MD5“ und „AES256_SHA1”.
PFS-Gruppe	Wählen Sie aus „NULL“, „MODP768_1“, „MODP1024_2“ und „MODP1536-5“.
Lebensdauer (s)	Legen Sie die Lebensdauer von IPsec SA fest. Bereich: 60-86400.
DPD-Intervallzeit (s)	DPD-Intervallzeit festlegen
DPD-Zeitlimit (s)	DPD-Zeitüberschreitung festlegen.
Cisco-Geheimnis	Cisco Nhrp-Schlüssel.
NHRP-Haltezeit (s)	Die Haltezeit des Nhrp-Protokolls.

6.2.6.2 IPSec

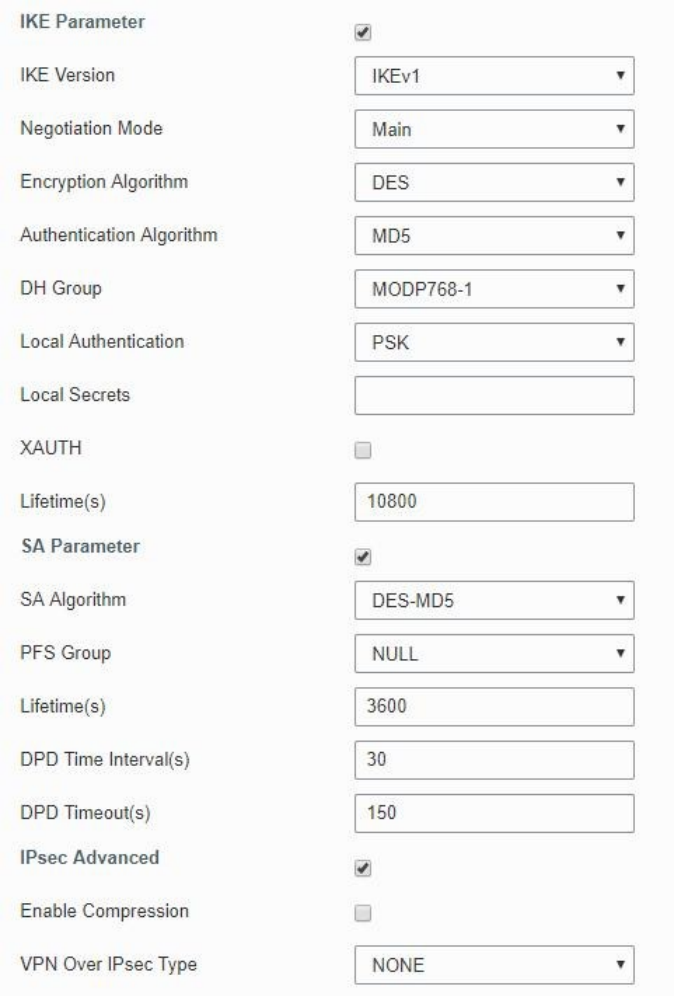
IPsec ist besonders nützlich für die Implementierung virtueller privater Netzwerke und für den Fernzugriff von Benutzern über eine Einwahlverbindung zu privaten Netzwerken. Ein großer Vorteil von IPsec besteht darin, dass Sicherheitsvorkehrungen getroffen werden können, ohne dass Änderungen an den einzelnen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

HL31 unterstützt die gleichzeitige Ausführung von maximal 3 IPsec-Clients.



IPsec	
Element	Beschreibung
Aktivieren	IPsec-Tunnel aktivieren oder deaktivieren. Es sind maximal 3 Tunnel .
IPsec-Gateway-Adresse	Geben Sie die IP-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.
Lokale Subnetz-Netzmaske	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. Standard: Keine ID: Lokale Subnetz-IP-Adresse als ID verwenden FQDN: vollqualifizierter Domänenname,Beispiel: test.user.com Benutzer-FQDN: vollqualifizierter Benutzername im E-Mail-Format, example:test@user.com
Remote-Subnetz	Legen Sie das Remote-LAN-Subnetz fest, das sich auf dem 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. Standard: Keine ID: Remote-Subnetz-IP-Adresse als ID verwenden FQDN: Vollständig qualifizierter Domänenname,Beispiel: test.user.com Benutzer-FQDN: Vollständig qualifizierte Benutzernamenzeichenfolge im E-Mail-Adressformat, Beispiel: test@user.com



IKE-Parameter	
Element	Beschreibung
IKE-Version	Wählen Sie die Methode für den Schlüsselaustausch von IKEv1 oder IKEv2 aus.
Verhandlungsmodus	Wählen Sie zwischen „Main“ und „Aggressive“.
Verschlüsselungsalgorithmus	Wählen Sie zwischen DES, 3DES, AES128, AES192 oder AES256.
Authentifizierung Algorithmus	Wählen Sie zwischen MD5 und SHA1.
DH-Gruppe	Wählen Sie MODP768_1,MODP1024_2 oder MODP1536_5.
Lokale Authentifizierung	Wählen Sie zwischen PSK und CA. PSK: Verwenden Sie einen vorab geteilten Schlüssel, um die Authentifizierung abzuschließen. CA: Verwenden Sie ein Zertifikat, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite „Netzwerk > VPN > Zertifikate“, um das CA-Zertifikat, das lokale Zertifikat und den privaten Schlüssel in die entsprechenden Felder zu importieren.
Lokale Geheimnisse	Geben Sie den vorab geteilten Schlüssel ein.
Remote Authentifizierung	Geben Sie den vorab geteilten Schlüssel ein, der auf der Serverseite definiert ist.
Remote-Geheimnisse	Wählen Sie PSK oder CA. PSK: Verwenden Sie den vorab geteilten Schlüssel, um die Authentifizierung abzuschließen. CA: Verwenden Sie das Zertifikat, um die Authentifizierung abzuschließen.

XAUTH	Bei Verwendung von IKEv1 müssen Sie den XAUTH-Benutzernamen und das Passwort , nachdem XAUTH aktiviert wurde.
Lebensdauer (s)	Legen Sie die Lebensdauer in der IKE-Verhandlung fest. Bereich: 60-86400.
SA-Parameter	
SA-Algorithmus	Wählen Sie aus DES_MD5, DES_SHA1, 3DES_MD5, 3DES_SHA1, AES128_MD5, AES128_SHA1, AES192_MD5, AES192_SHA1, AES256_MD5 und AES256_SHA1.
PFS-Gruppe	Wählen Sie aus NULL, MODP768_1 , MODP1024_2 und MODP1536_5.
Lebensdauer (s)	Legen Sie die Lebensdauer von IPsec SA fest. Bereich: 60-86400.
DPD-Intervallzeit (s)	Legen Sie das DPD-Intervall fest, um zu erkennen, ob die Gegenstelle ausfällt.
DPD-Zeitüberschreitung(en)	DPD-Zeitlimit festlegen. Bereich: 10-3600.
IPsec erweitert	
Komprimierung aktivieren	Der Kopf des IP-Pakets wird nach der Aktivierung komprimiert.
VPN über IPsec-Typ	Wählen Sie zwischen NONE, GRE und L2TP, um die VPN-über-IPsec-Funktion zu aktivieren. .

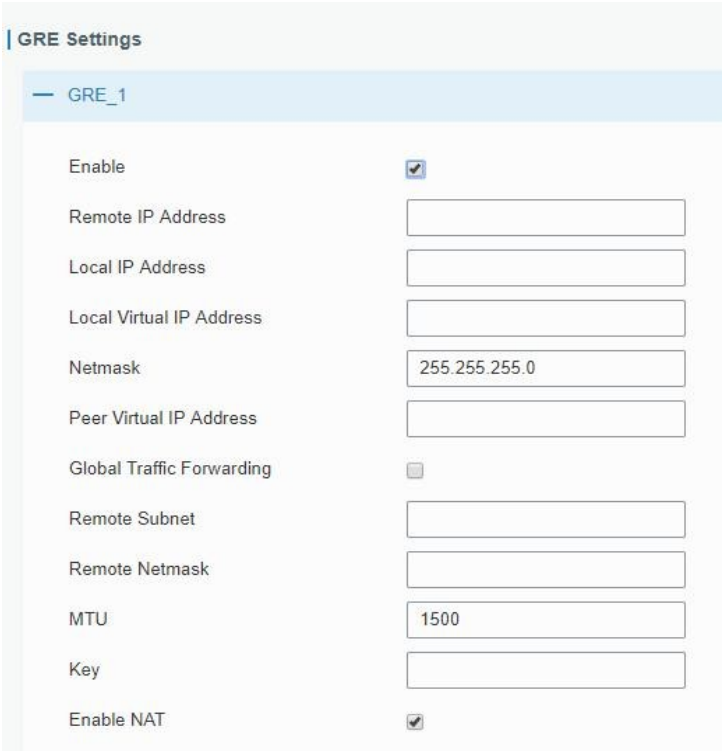
6.2.6.3 GRE

Generic Routing Encapsulation (GRE) ist ein Protokoll, das Pakete kapselt, um andere Protokolle über IP-Netzwerke zu routen. Es handelt sich um eine Tunneling-Technologie, die einen Kanal bereitstellt, über den gekapselte Datennachrichten übertragen und an beiden Enden gekapselt und entkapselt werden können.

Unter den folgenden Umständen kann die GRE-Tunnelübertragung angewendet werden:

- Der GRE-Tunnel kann Multicast-Datenpakete übertragen, als wäre er eine echte Netzwerkschnittstelle. Mit IPSec allein lässt sich keine Verschlüsselung von Multicast erreichen.
- Ein bestimmtes Protokoll kann nicht geroutet werden.
- Ein Netzwerk mit unterschiedlichen IP-Adressen ist erforderlich, um zwei andere ähnliche Netzwerke zu verbinden.

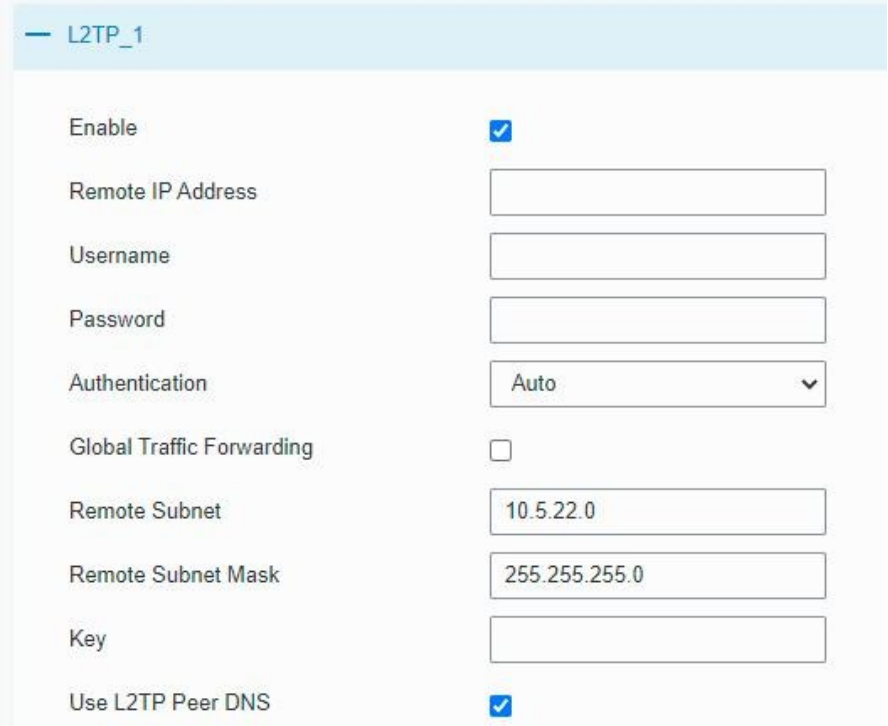
HL31 unterstützt die gleichzeitige Ausführung von maximal 3 GRE-Clients.



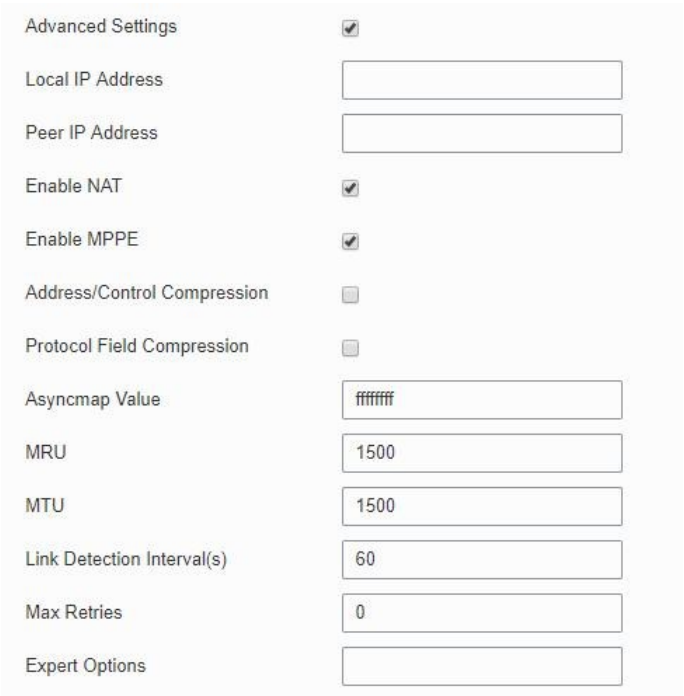
GRE	
Element	Beschreibung
Aktivieren	Aktivieren Sie die GRE-Funktion. Es sind maximal 3 Tunnel .
Remote-IP-Adresse	Geben Sie die tatsächliche Remote-IP-Adresse des GRE-Tunnels ein.
Lokale IP-Adresse	Legen Sie die lokale IP-Adresse fest.
Lokale virtuelle IP Adresse	Legen Sie die lokale Tunnel-IP-Adresse des GRE-Tunnels fest.
Netzmaske	Legen Sie die lokale Netzmaske fest.
Virtuelle IP-Adresse des Peers	Geben Sie die Remote-Tunnel-IP-Adresse des GRE-Tunnels ein.
Globaler Datenverkehr Weiterleitung	Der gesamte Datenverkehr wird über den GRE-Tunnel gesendet, wenn dies Die Funktion ist aktiviert.
Remote-Subnetz	Geben Sie die IP-Adresse des Remote-Subnetzes des GRE-Tunnels ein.
Remote-Netzmaske	Geben Sie die Remote-Netzmaske des GRE-Tunnels ein.
MTU	Geben Sie die maximale Übertragungseinheit ein. Bereich: 64–1500.
Schlüssel	Legen Sie den GRE-Tunnelschlüssel fest.
NAT aktivieren	Aktivieren Sie die NAT-Traversal-Funktion.

6.2.6.4 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.



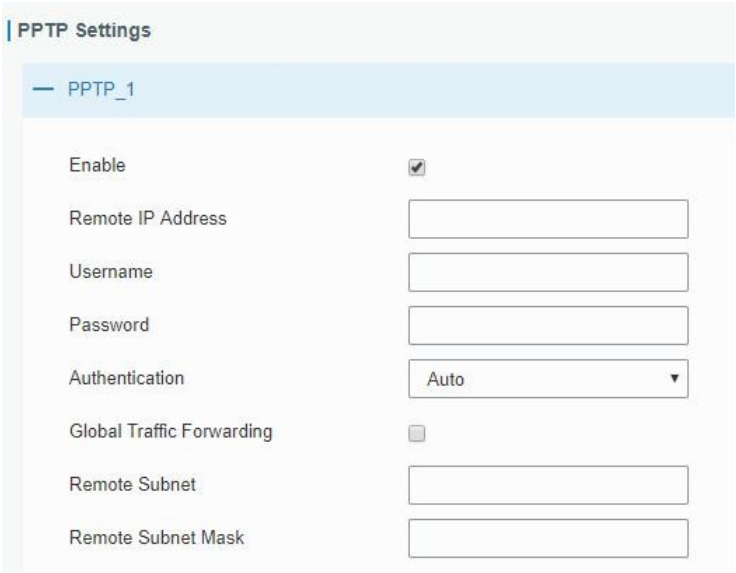
L2TP	
Element	Beschreibung
Aktivieren	L2TP-Client aktivieren oder deaktivieren. Es sind maximal 3 Tunnel möglich. erlaubt.
Remote-IP-Adresse	Geben Sie die IP-Adresse oder den Domänennamen des Remote-L2TP-Servers ein.
Benutzername	Geben Sie den Benutzernamen ein, den der L2TP-Server bereitstellt.
Passwort	Geben Sie das vom L2TP-Server bereitgestellte Passwort ein.
Authentifizierung	Wählen Sie den Authentifizierungstyp aus, der zur Sicherung der Datensitzungen verwendet wird.
Globaler Datenverkehr Weiterleitung	Der gesamte Datenverkehr wird über den L2TP-Tunnel gesendet, nachdem Aktivierung dieser Funktion über einen L2TP-Tunnel gesendet.
Remote-Subnetz	Geben Sie die Remote-IP-Adresse ein, die L2TP schützt.
Remote-Subnetzmaske	Geben Sie die Remote-Netzmaske ein, die L2TP schützt.
Schlüssel	Geben Sie das Passwort für den L2TP-Tunnel ein.
L2TP-Peer-DNS verwenden	Aktivieren Sie diese Option, um die DNS-Adresse des Peer-L2TP-Servers zu verwenden.



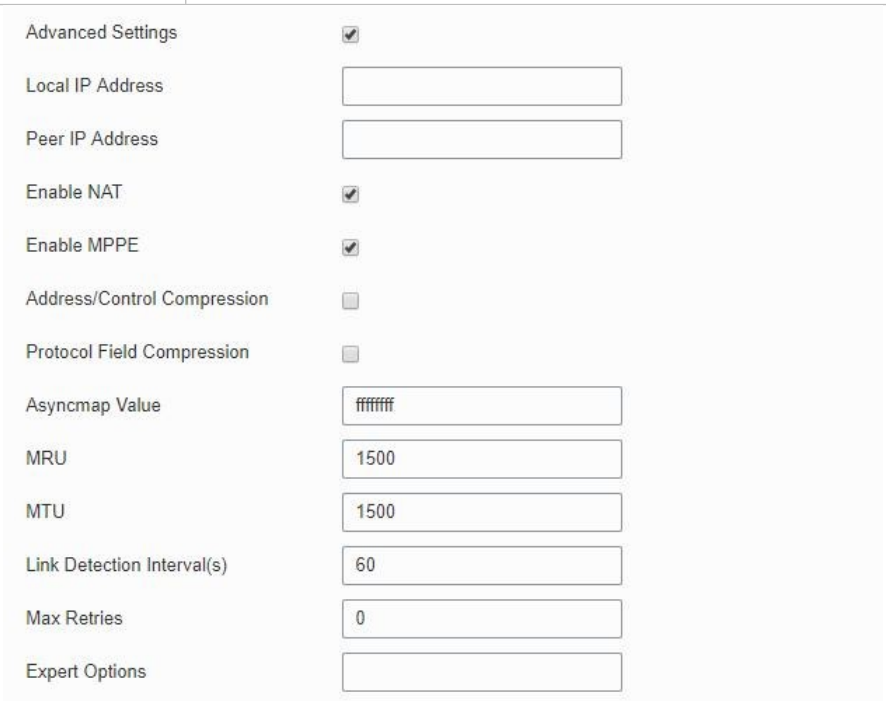
Erweiterte Einstellungen	
Element	**Beschreibung**
Lokale IP-Adresse	Legen Sie die Tunnel-IP-Adresse des L2TP-Clients fest. Der Client erhält die Tunnel-IP-Adresse automatisch vom Server, wenn sie null ist. IP-Adresse automatisch vom Server, wenn sie null ist.
Peer-IP-Adresse	Geben Sie die Tunnel-IP-Adresse des L2TP-Servers ein.
NAT aktivieren	Aktivieren Sie die NAT-Traversal-Funktion.
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 Initialisierungszeichenfolgen für das PPP-Protokoll. Der Benutzer kann den Standardwert beibehalten. Bereich: 0-ffffffff.
MRU	Legt die maximale Empfangseinheit fest. Bereich: 64-1500.
MTU	Legt die maximale Übertragungseinheit fest. Bereich: 64-1500
Link-Erkennungsintervall (s)	Legen Sie das Verbindungserkennungsintervall fest, um die Tunnelverbindung sicherzustellen Verbindung. Bereich: 0-600.
Max. Wiederholungsversuche	Legen Sie die maximale Anzahl der Wiederholungsversuche fest, um den L2TP-Verbindungsfehler zu erkennen Verbindungsfehler zu erkennen. Bereich: 0-10.
Expertenoptionen	Der Benutzer kann in diesem Feld einige andere PPP-Initialisierungszeichenfolgen eingeben Feld einige andere PPP-Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Leerzeichen trennen.

6.2.6.5 PPTP

Das Point-to-Point Tunneling Protocol (PPTP) ist ein Protokoll, mit dem Unternehmen ihr eigenes Unternehmensnetzwerk über private „Tunnel" über das öffentliche Internet erweitern können. Im Endeffekt nutzt ein Unternehmen ein Weitverkehrsnetzwerk als ein einziges großes lokales Netzwerk.



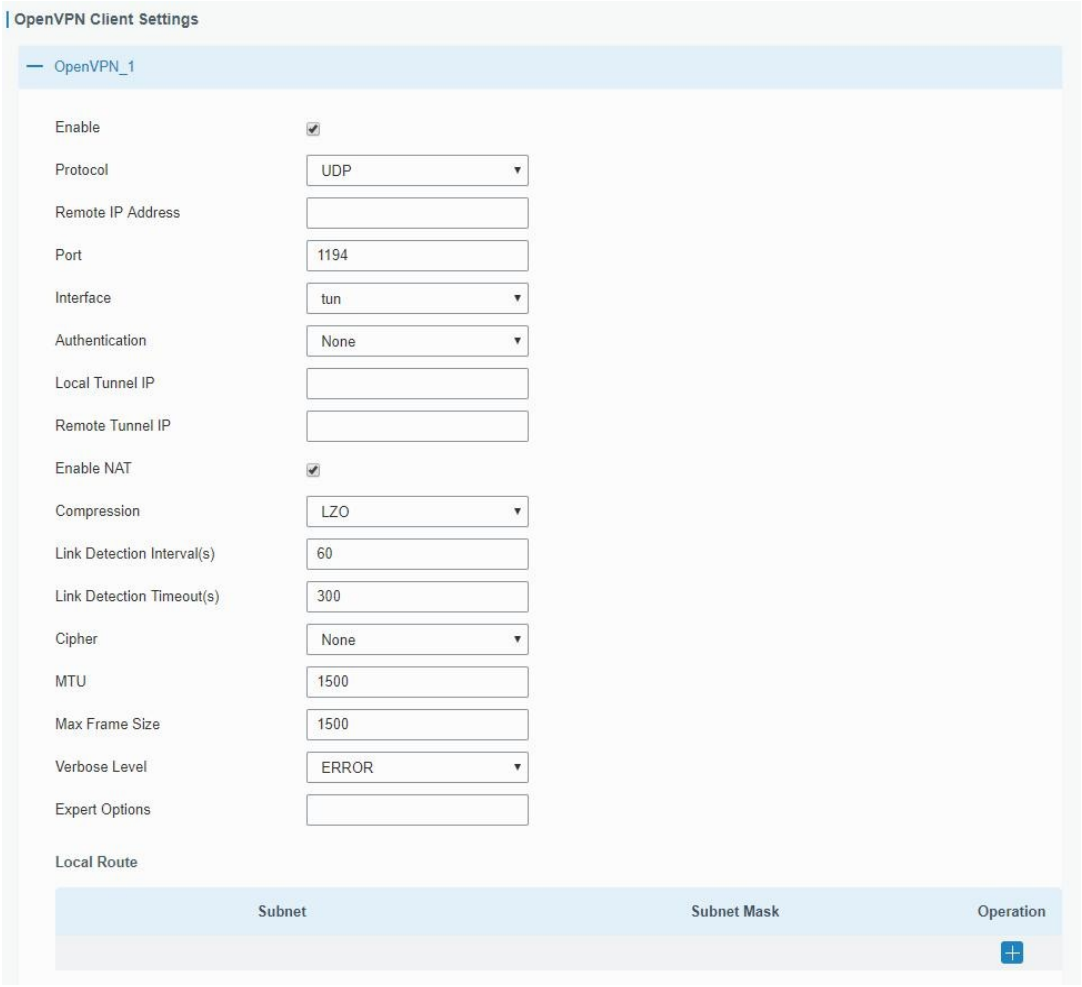
PPTP	
Element	Beschreibung
Aktivieren	PPTP-Client aktivieren oder deaktivieren. Es sind maximal 3 Tunnel .
Remote-IP-Adresse	Geben Sie die IP-Adresse oder den Domänennamen des Remote-PPTP-Servers ein.
Benutzername	Geben Sie den Benutzernamen ein, den der PPTP-Server bereitstellt.
Passwort	Geben Sie das vom PPTP-Server bereitgestellte Passwort ein.
Authentifizierung	Wählen Sie den Authentifizierungstyp aus, der zur Sicherung der Datensitzungen verwendet wird.
Globaler Datenverkehr Weiterleitung	Der gesamte Datenverkehr wird über den PPTP-Tunnel gesendet, sobald diese Funktion aktiviert ist.
Remote-Subnetz	Geben Sie das Remote-Subnetz des PPTP-VPN-Servers ein.
Remote-Subnetz Maske	Geben Sie die Remote-Netzmaske des PPTP-VPN-Servers ein.



Erweiterte PPTP-Einstellungen	
Element	Beschreibung
Lokale 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.
Peer-IP-Adresse	Geben Sie die Tunnel-IP-Adresse des PPTP-Servers ein.
NAT aktivieren	Aktivieren Sie die NAT-Funktion von PPTP.
MPPE aktivieren	Aktivieren Sie MPPE (Microsoft Point to Point Encryption).
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 Initialisierungszeichenfolgen für das PPP-Protokoll. Der Benutzer kann den Standardwert beibehalten. Bereich: 0-ffffffff.
MRU	Geben Sie die maximale Empfangseinheit ein. Bereich: 0-1500.
MTU	Geben Sie die maximale Übertragungseinheit ein. Bereich: 0-1500.
Link-Erkennungsintervall (s)	Legen Sie das Verbindungserkennungsintervall fest, um die Tunnelverbindung sicherzustellen Verbindung. Bereich: 0-600.
Max. Wiederholungsversuche	Legen Sie die maximale Anzahl der Wiederholungsversuche fest, um den PPTP-Verbindungsfehler zu erkennen Verbindungsfehler. Bereich: 0-10.
Expertenoptionen	Der Benutzer kann in diesem Feld einige andere PPP-Initialisierungszeichenfolgen eingeben Feld einige andere PPP-Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Leerzeichen trennen.

6.2.6.6 OpenVPN-Client

OpenVPN ist ein Open-Source-Produkt für virtuelle private Netzwerke (VPN), das ein vereinfachtes Sicherheitsframework, ein modulares Netzwerkdesign und plattformübergreifende Portabilität bietet. HL31 unterstützt die gleichzeitige Ausführung von maximal 3 OpenVPN-Clients.

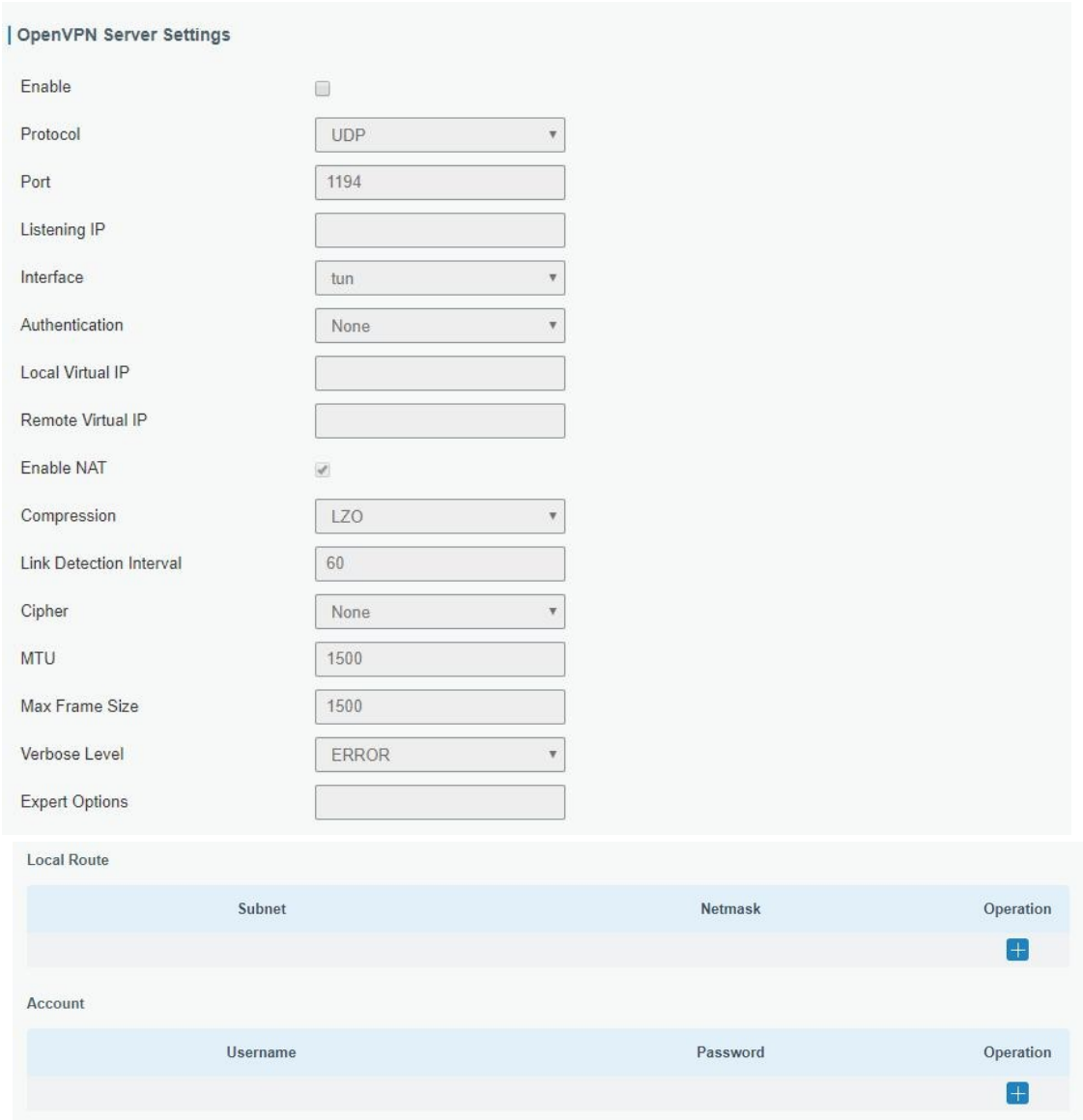


OpenVPN-Client	
Element	Beschreibung
Aktivieren	OpenVPN-Client aktivieren. Es sind maximal 3 Tunnel zulässig.
Protokoll	Wählen Sie ein Transportprotokoll aus, das durch die Verbindung von UDP und TCP.
Remote-IP-Adresse	Geben Sie die IP-Adresse oder den Domänennamen des Remote-OpenVPN-Servers ein.
Port	Geben Sie die TCP/UCP-Servicenummer des Remote-OpenVPN-Servers ein . Bereich: 1-65535.
Schnittstelle	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.
Authentifizierung	Wählen Sie den Authentifizierungstyp aus, der zur Sicherung von Datensitzungen verwendet wird. Vorab geteilt: Verwenden Sie denselben geheimen Schlüssel wie der Server, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite „Netzwerk > VPN > Zertifizierungen“, um eine statische Datei („static.key“) in das Feld „PSK“ zu importieren. Benutzername/Passwort: Verwenden Sie den auf der Serverseite voreingestellten Benutzernamen/das Passwort, um die Authentifizierung abzuschließen. X.509-Zertifikat: Verwenden Sie ein Zertifikat vom Typ X.509, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zu Netzwerk > VPN > Zertifikate, um das CA-Zertifikat und das Client-Zertifikat zu importieren.

	und den privaten Schlüssel des Kunden in die entsprechenden Felder ein. X.509-Zertifikat + Benutzer: Verwenden Sie sowohl die Authentifizierungsart „Benutzername/Passwort“ als auch „X.509-Zertifikat“.
Lokale Tunnel-IP	Legen Sie die lokale Tunneladresse fest, wenn der Authentifizierungstyp „Keine“ oder „Vorab geteilt“ ist.
Remote-Tunnel-IP	Legen Sie die Remote-Tunneladresse fest, wenn der Authentifizierungstyp „Keine“ oder „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 „Netzwerk > VPN > Zertifikate“, um eine ta.key-Datei in das Feld „TA“ zu importieren. 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
NAT aktivieren	Aktivieren Sie die NAT-Traversal-Funktion.
Komprimierung	Wählen Sie LZO, um Daten zu komprimieren.
Link-Erkennungsintervall (s)	Legen Sie das Intervall für die Verbindungserkennung fest, um die Tunnelverbindung sicherzustellen. Wenn dies sowohl auf dem Server als auch auf dem Client eingestellt ist, überschreibt der vom Server übertragene Wert die lokalen Werte des Clients. Server die lokalen Werte des Clients. Bereich: 10-1800 s.
Zeitlimit für die Verbindungserkennung (s)	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. Bereich: 60-3600 s.
Verschlüsselung	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 Rahmengröße 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. 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.

6.2.6.7 OpenVPN-Server

HL31 unterstützt OpenVPN-Server, um sichere Punkt-zu-Punkt- oder Standort-zu-Standort-Verbindungen in gerouteten oder gebrückten Konfigurationen und Fernzugriffsfunktionen herzustellen.



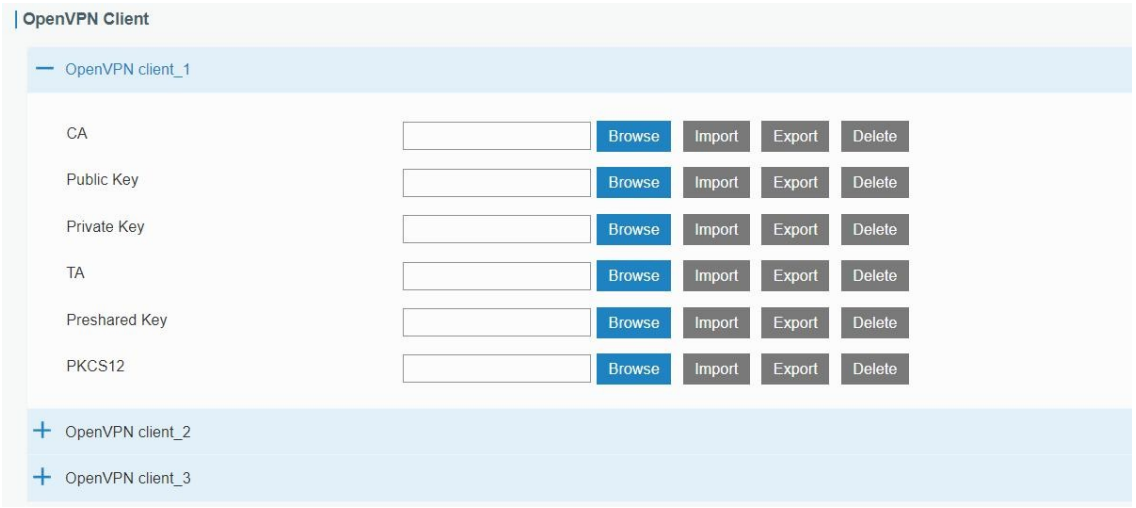
OpenVPN-Server	
Artikel	**Beschreibung**
Aktivieren	OpenVPN-Server aktivieren/deaktivieren.
Protokoll	Wählen Sie ein Transportprotokoll für die Verbindung aus UDP und TCP.
Port	Geben Sie die TCP/UCP-Servicenummer für die OpenVPN-Clientverbindung ein Verbindung ein. Bereich: 1-65535.
Zuhörende IP	Geben Sie den lokalen Hostnamen oder die IP-Adresse für die Bindung ein. Wenn das Feld leer bleibt leer gelassen, bindet sich der OpenVPN-Server an alle Schnittstellen.
Schnittstelle	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).
Authentifizierung	Wählen Sie den Authentifizierungstyp aus, der zur Sicherung von Datensitzungen verwendet wird. Vorab geteilt: Verwenden Sie denselben geheimen Schlüssel wie der Server, um die . Nach der Auswahl gehen Sie zu Netzwerk > VPN >

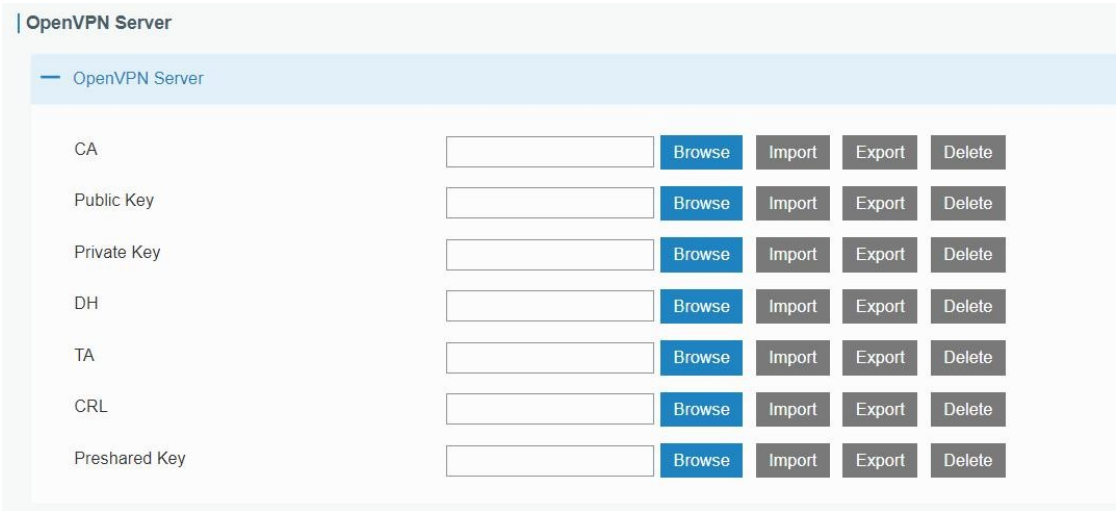
	Zertifizierungsseite, um eine statische Datei („static.key“) in das PSK-Feld zu importieren. Benutzername/Passwort: Verwenden Sie den auf der Serverseite voreingestellten Benutzernamen/das voreingestellte Passwort, um die Authentifizierung abzuschließen. X.509-Zertifikat: Verwenden Sie ein Zertifikat vom Typ X.509, um die Authentifizierung abzuschließen. Nach der Auswahl gehen Sie zur Seite „Netzwerk > VPN > Zertifizierungen“, um das CA-Zertifikat, das Client-Zertifikat und den privaten Client-Schlüssel in die entsprechenden Felder zu importieren. X.509-Zertifikat + Benutzer: Verwenden Sie sowohl Benutzername/Passwort als auch den Authentifizierungstyp X.509 Zertifikat.
Lokale virtuelle IP	Lokale Tunneladresse festlegen, wenn der Authentifizierungstyp „Keine“ oder „Vorab geteilt“ ist.
Virtuelle Remote-IP	Remote-Tunneladresse festlegen, wenn der Authentifizierungstyp „Keine“ oder „Vorab geteilt“.
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(e)	Verhandeln Sie den Datenkanalschlüssel nach diesem Intervall neu. 0 bedeutet Deaktivieren. Bereich: 0–86400.
Maximale Anzahl von Clients	Maximale Anzahl von OpenVPN-Clients. Bereich: 1–128.
TLS-Authentifizierung aktivieren	Deaktivieren oder aktivieren Sie die TLS-Authentifizierung, wenn der Authentifizierungstyp „X.509-Zertifikat“ ist. Nach der Aktivierung gehen Sie zur Seite „Netzwerk > VPN > Zertifikate“, um eine ta.key-Datei in das Feld „TA“ zu importieren. 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
CRL aktivieren	CRL-Überprüfung aktivieren oder deaktivieren.
Client-zu-Client aktivieren	Wenn diese Option aktiviert ist, können OpenVPN-Clients miteinander kommunizieren miteinander.
Dup-Client aktivieren	Ermöglichen Sie mehreren Kunden, sich mit demselben gemeinsamen Namen oder Zertifizierung verbinden.
NAT aktivieren	Aktivieren Sie diese Option, um die NAT-Traversal-Funktion zu aktivieren.
Komprimierung	Wählen Sie LZO, um Daten zu komprimieren.
Link-Erkennungsintervall (s)	Legen Sie das Verbindungserkennungsintervall fest, um die Tunnelverbindung sicherzustellen. Wenn dies sowohl auf dem Server als auch auf dem Client eingestellt ist, überschreibt der vom Server übertragene Wert die lokalen Werte des Clients. Bereich: 10–1800 s.
Zeitlimit für die Verbindungserkennung (s)	OpenVPN wird nach Ablauf der Zeitüberschreitung wiederhergestellt. Wenn dies sowohl auf dem Server als auch auf dem Client eingestellt ist, überschreibt der vom Server übertragene Wert die lokalen Werte des Clients überschreiben. Bereich: 60–3600 s.
Verschlüsselung	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: 64–1500.
Maximale Frame-Größe	Legen Sie die maximale Rahmengröße fest. Bereich: 64–1500.
Ausführlichkeitsstufe	Wählen Sie zwischen ERROR, WARING NOTICE und DEBUG.
Expertenoptionen	Der Benutzer kann in diesem Feld einige Initialisierungszeichenfolgen eingeben und

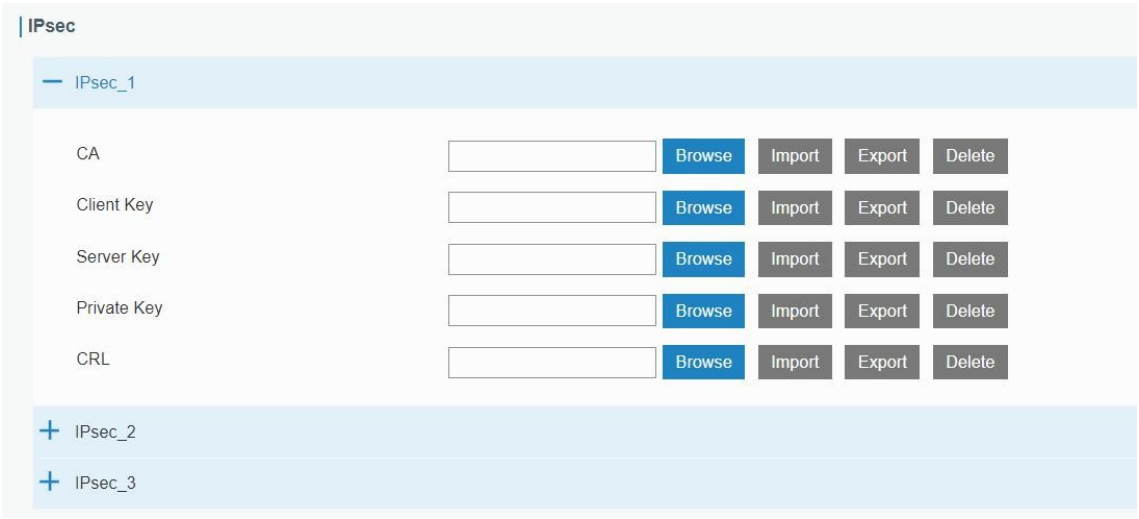
	die Zeichenfolgen durch Semikolons trennen. Beispiel: auth SHA256; key direction 1
Lokale Route	
Subnetz	Die tatsächliche lokale IP-Adresse des OpenVPN-Clients.
Netzmaske	Die tatsächliche lokale Netzmaske des OpenVPN-Clients.
Konto	
Benutzername und Passwort	Legen Sie Benutzername und Passwort für den OpenVPN-Client fest, wenn der Authentifizierungstyp „Benutzername/Passwort" ist.
Client-Subnetz	
Name	Legen Sie den Namen als allgemeinen Namen für das OpenVPN-Client-Zertifikat fest.
Subnetz	Legen Sie das Subnetz des OpenVPN-Clients fest.
Subnetzmaske	Legen Sie die Subnetzmaske des OpenVPN-Clients fest.

6.2.6.8 Zertifizierungen

Bei der Arbeit als OpenVPN-Server, OpenVPN-Client oder IPsec-Server kann der Benutzer die erforderlichen Zertifikats- und Schlüsseldateien entsprechend den Authentifizierungstypen auf dieser Seite importieren/exportieren.







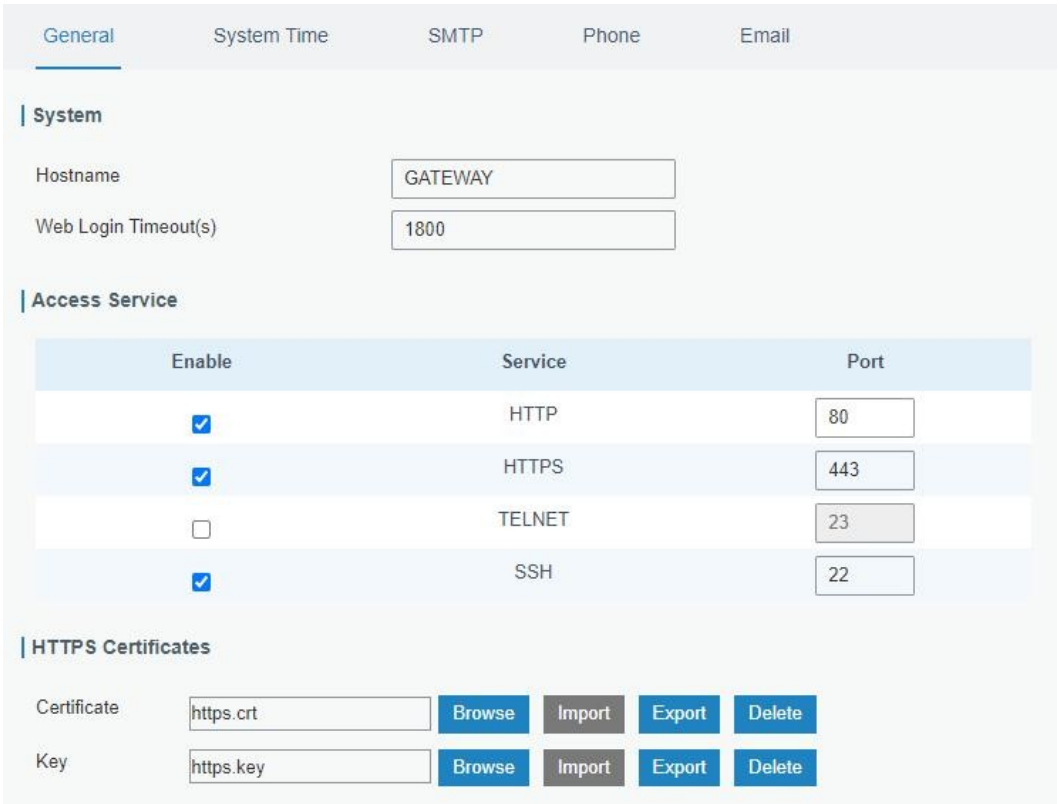
6.3 System

In diesem Abschnitt wird beschrieben, wie allgemeine Einstellungen wie Administratorkonto, Zugriffsservice, Systemzeit, allgemeine Benutzerverwaltung, SNMP, Ereignisalarme usw. konfiguriert werden.

6.3.1 Allgemeine Einstellungen

6.3.1.1 Allgemein

Die allgemeinen Einstellungen umfassen Systeminformationen, Zugriffsdienste und HTTPS-Zertifikate.

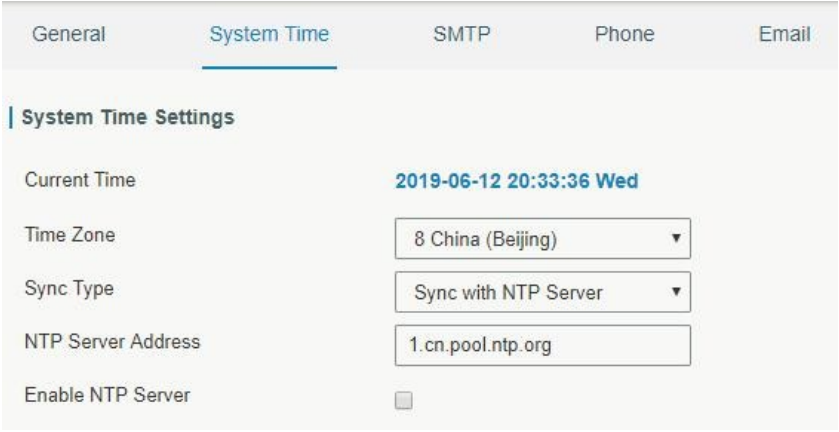


Allgemein		
Element	Beschreibung	Standard
System		
Hostname	Benutzerdefinierter Gateway-Name,muss mit einem Buchstaben beginnen.	GATEWAY
Web-Anmeldung Zeitlimit (s)	Bei Ablauf der Zeit müssen Sie sich erneut anmelden. Bereich: 100-3600.	1800
Zugriffsservice		
Port	Legen Sie die Portnummer der Dienste fest. Bereich: 1-65535.	--
HTTP	Benutzer können sich lokal über HTTP beim Gerät anmelden, um darauf zuzugreifen. und steuern Sie es über das Web, nachdem die Option aktiviert wurde.	80
HTTPS	Benutzer können sich lokal und remote über HTTPS lokal und remote auf dem Gerät anmelden, um nach Aktivierung der Option über das Web darauf zuzugreifen und es zu steuern.	443
TELNET	Benutzer können sich lokal und remote über TELNET beim Gerät anmelden, um nach Aktivieren der Option über das Web darauf zuzugreifen und es zu steuern. die Option aktiviert ist.	23
SSH	Benutzer können sich lokal und remote über SSH beim Gerät anmelden , nachdem die Option aktiviert wurde.	22
HTTPS-Zertifikate		
Zertifikat	Klicken Sie auf die Schaltfläche „Durchsuchen“, wählen Sie die Zertifikatsdatei auf dem PC aus und klicken Sie dann auf die Schaltfläche „Importieren“, um die Datei in das Gateway hochzuladen. Durch Klicken auf die Schaltfläche „Exportieren“ wird die Datei auf den PC exportiert. Durch Klicken auf die Schaltfläche „Löschen“ wird die Datei gelöscht.	--
Schlüssel	Klicken Sie auf die Schaltfläche „Durchsuchen“, wählen Sie die Schlüsseldatei auf dem PC aus und klicken Sie dann auf die Schaltfläche „Importieren“, um die Datei in das Gateway hochzuladen. Durch Klicken auf die Schaltfläche „Exportieren“ wird die Datei auf den PC exportiert. Durch Klicken auf die Schaltfläche „Löschen“ wird die Datei gelöscht.	--

6.3.1.2 Systemzeit

In diesem Abschnitt wird erläutert, wie Sie die Systemzeit einschließlich Zeitzone und Zeitsynchronisationstyp einstellen.

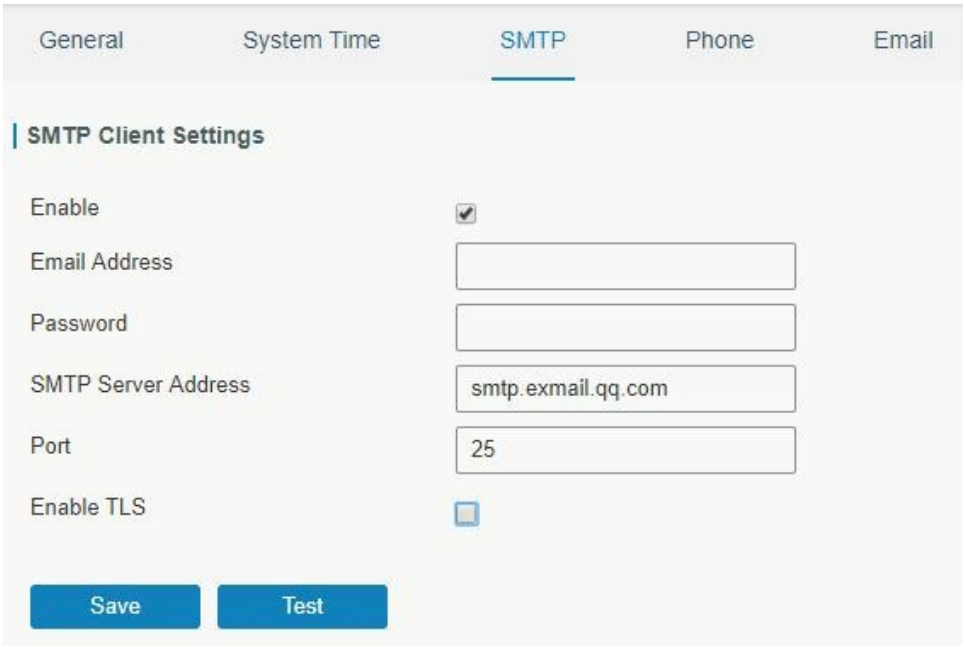
Hinweis: Um sicherzustellen, dass das Gateway mit der richtigen Zeit läuft, wird empfohlen, die Systemzeit bei der Konfiguration des Gateways einzustellen.



Systemzeit	
Element	Beschreibung
Aktuelle Uhrzeit	Zeigt die aktuelle Systemzeit an.
Zeitzone	Klicken Sie auf die Dropdown-Liste, um die Zeitzone auszuwählen, in der Sie sich befinden.
Synchronisierungstyp	Klicken Sie auf die Dropdown-Liste, um den Typ der Zeitsynchronisierung auszuwählen. Mit Browser synchronisieren: Synchronisieren Sie die Zeit mit dem Browser. Mit NTP-Server synchronisieren: Synchronisieren Sie die Zeit mit dem NTP-Server. Manuell einrichten: Konfigurieren Sie die Zeit manuell.
Mit NTP-Server synchronisieren	
NTP-Serveradresse	Legen Sie die NTP-Serveradresse (Domänenname/IP) fest.
NTP-Server aktivieren	Nach dem Aktivieren können NTP-Clients im Netzwerk die Zeit abrufen. Synchronisierung mit Gateway.

6.3.1.3 SMTP

SMTP kurz für Simple Mail Transfer Protocol, ist ein TCP/IP-Protokoll, das zum Senden und Empfangen von E-Mails verwendet wird. In diesem Abschnitt wird beschrieben, wie Sie das Gateway als SMTP-Client zum Senden von E-Mails konfigurieren.



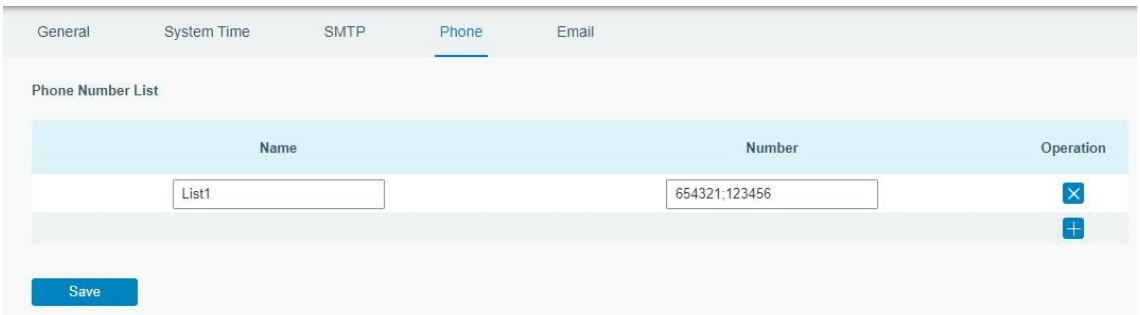
SMTP	
Element	Beschreibung
SMTP-Client-Einstellungen	
Aktivieren	SMTP-Client-Funktion aktivieren oder deaktivieren.
E-Mail-Adresse	Geben Sie das E-Mail-Konto des Absenders ein.
Passwort	Geben Sie das E-Mail-Passwort des Absenders ein.
SMTP-Serveradresse	Geben Sie den Domainnamen des SMTP-Servers ein.
Port	Geben Sie den Port des SMTP-Servers ein. Bereich: 1-65535.
TLS aktivieren	Aktivieren oder deaktivieren Sie die TLS-Verschlüsselung.

Verwandte Themen

Ereigniseinstellungen

6.3.1.4 Telefon

Die Telefoneinstellungen umfassen Anruf-/SMS-Auslöser und SMS-Alarme für Ereignisse. Dies gilt nur für Gateways mit Mobilfunkfunktion.



Telefon	
Element	Beschreibung

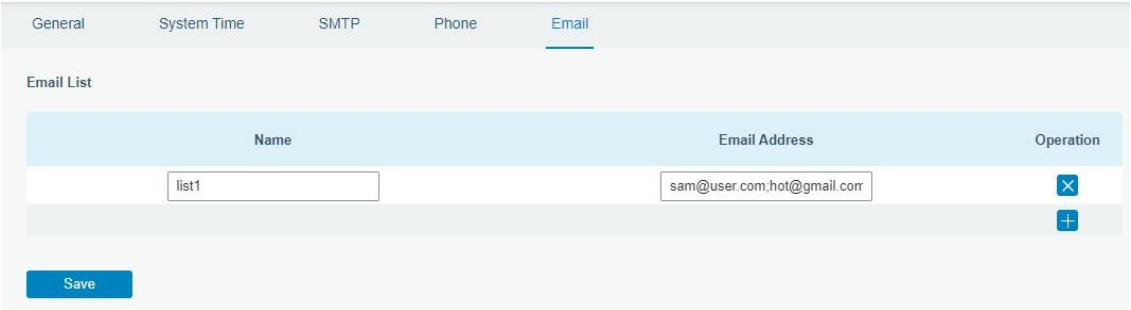
Telefonnummernliste	
Name	Legen Sie den Namen der Telefongruppe fest.
Nummer	Geben Sie die Telefonnummer ein. Ziffern, „+“ und „-“ sind zulässig. Sie können mehrere Nummern durch „;“ trennen.

Verwandtes Thema

Verbindung auf Abruf

6.3.1.5 E-Mail

Die E-Mail-Einstellungen umfassen E-Mail-Benachrichtigungen für Ereignisse.

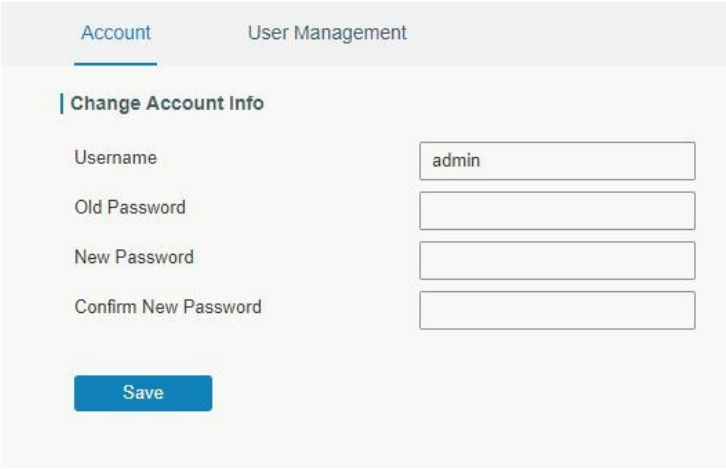


E-Mail	
Element	Beschreibung
E-Mail-Liste	
Name	E-Mail-Gruppennamen festlegen.
E-Mail-Adresse	Geben Sie die E-Mail-Adresse ein. Sie können mehrere E-Mail-Adressen durch „;“ trennen.

6.3.2 Benutzerverwaltung

6.3.2.1 Konto

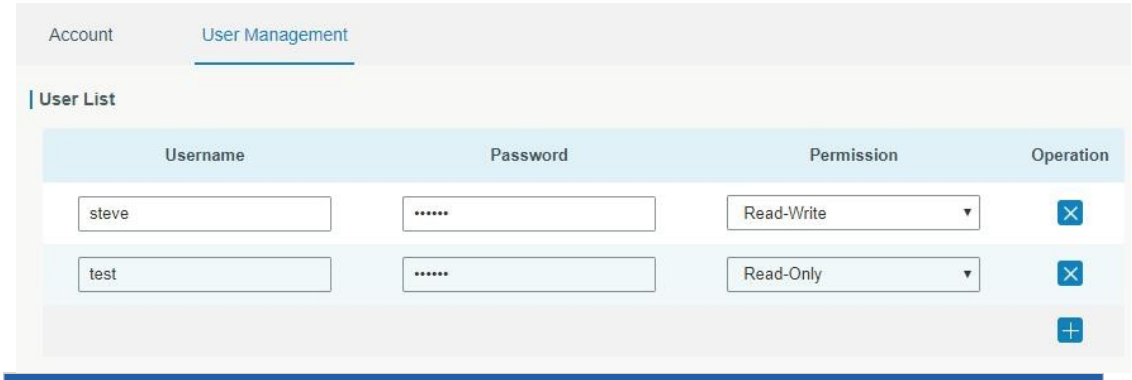
Hier können Sie den Benutzernamen und das Passwort des Administrators ändern. Hinweis: Aus Sicherheitsgründen wird dringend empfohlen, diese zu ändern.



Konto	
Element	Beschreibung
Benutzername	Geben Sie einen neuen Benutzernamen ein. Sie können Zeichen wie a-z, 0-9, „_“, „-“ und „$“ verwenden. Das erste Zeichen darf keine Ziffer sein.
Altes Passwort	Geben Sie das alte Passwort ein.
Neues Passwort	Geben Sie ein neues Passwort ein.
Neues Passwort bestätigen	Geben Sie das neue Passwort erneut ein.

6.3.2.2 Benutzerverwaltung

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



Benutzerverwaltung	
Element	Beschreibung
Benutzername	Geben Sie einen neuen Benutzernamen ein. Sie können Zeichen wie a-z, 0-9, „_“, „-“ verwenden. Das erste Zeichen darf keine Ziffer sein.
Passwort	Legen Sie ein Passwort fest.
Berechtigung	Wählen Sie die Benutzerberechtigung aus „Nur lesen“ und „Lesen-Schreiben“ aus. - Nur Lesen: Benutzer können auf dieser Ebene nur die Konfiguration des Gateways anzeigen. - Lesen/Schreiben: Benutzer können die Konfiguration des Gateways in dieser Ebene anzeigen und festlegen. Gateways anzeigen und festlegen.

6.3.3 SNMP

SNMP wird häufig in der Netzwerkverwaltung für die Netzwerküberwachung eingesetzt. SNMP stellt Verwaltungsdaten in Form von Variablen 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.

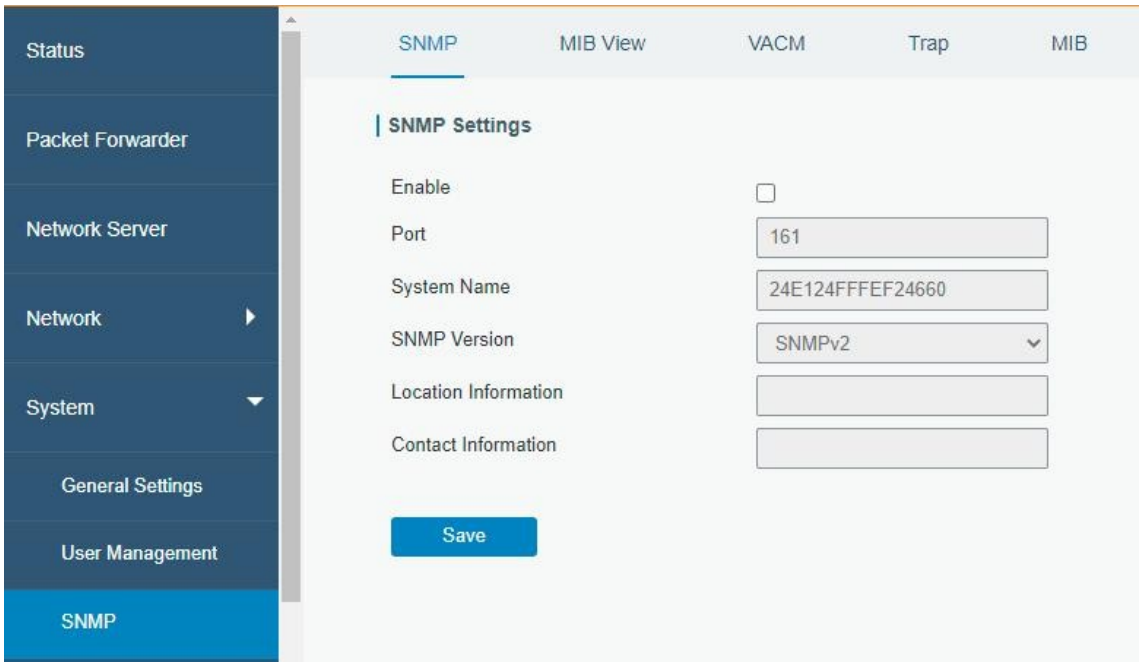
Die folgenden Konfigurationsschritte sind erforderlich, um eine Abfrage von NMS durchzuführen:

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. Konfigurieren Sie VCAM.

6.3.3.1 SNMP

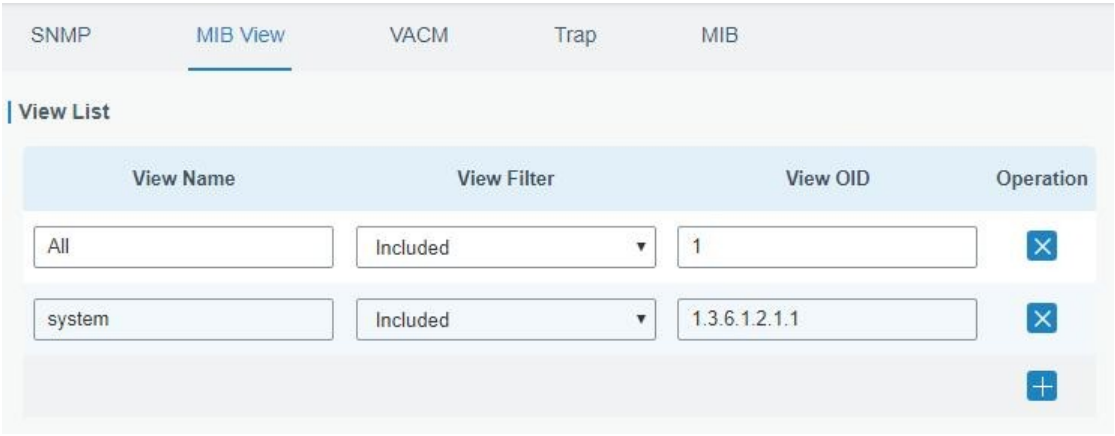
HL31 unterstützt die Versionen SNMPv1, SNMPv2c und SNMPv3. SNMPv1 und SNMPv2c verwenden die Authentifizierung über einen Community-Namen. SNMPv3 verwendet die Authentifizierung durch Verschlüsselung mit Benutzername und Passwort.



SNMP-Einstellungen	
Element	**Beschreibung**
Aktivieren	Aktivieren oder deaktivieren Sie die SNMP-Funktion.
Port	Legen Sie den SNMP-Port fest. Bereich: 1-65535. Der Standardport ist 161.
Systemname	Geben Sie den Systemnamen ein, der das Gateway repräsentiert.
SNMP-Version	Wählen Sie die SNMP-Version aus; unterstützt werden SNMP v1/v2c/v3.
Standortinformationen	Geben Sie die Standortinformationen ein.
Kontakt	Geben Sie die Kontaktinformationen ein.

6.3.3.2 MIB-Ansicht

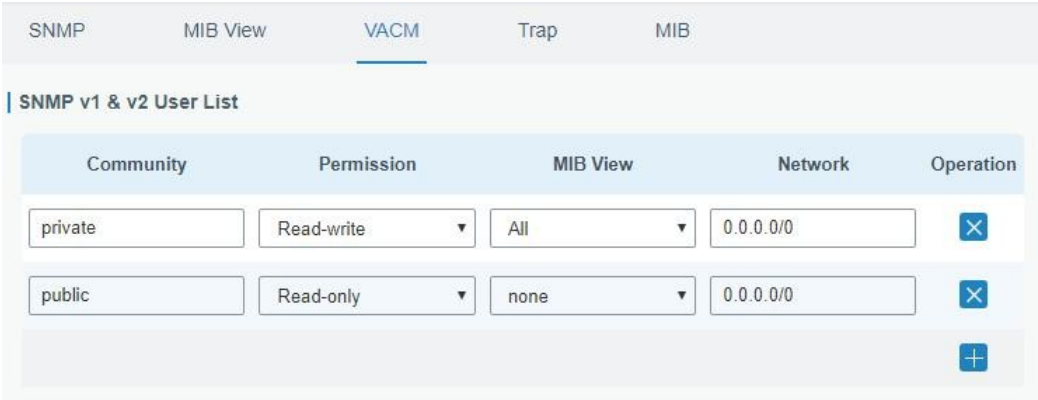
In diesem Abschnitt wird erläutert, wie Sie die MIB-Ansicht für die Objekte konfigurieren.



MIB-Ansicht	
Element	Beschreibung
Ansichtsname	Legen Sie den Namen der MIB-Ansicht fest.
Ansichtsfilter	Wählen Sie zwischen „Enthalten" und „Ausgeschlossen".
Ansicht-OID	Geben Sie die OID-Nummer ein.
Enthalten	Sie können alle Knoten innerhalb des angegebenen MIB-Knotens abfragen.
Ausgeschlossen	Sie können alle Knoten außer dem angegebenen MIB-Knoten abfragen.

6.3.3.3 VACM

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



VACM	
Element	Beschreibung
SNMP v1 & v2 Benutzerliste	
Community	Legen Sie den Community-Namen fest.
Berechtigung	Wählen Sie zwischen „Nur Lesen" und „Lesen/Schreiben".
MIB-Ansicht	Wählen Sie eine MIB-Ansicht aus der MIB-Ansichtsliste aus, um Berechtigungen festzulegen.
Netzwerk	Die IP-Adresse und die Bits des externen Netzwerks, das auf die MIB-Ansicht zugreift.
Lesen/Schreiben	Die Berechtigung für den angegebenen MIB-Knoten ist Lesen und Schreiben.
Nur Lesen	Die Berechtigung für den angegebenen MIB-Knoten ist schreibgeschützt.
SNMP v3-Benutzerliste	
Gruppenname	Legen Sie den Namen der SNMPv3-Gruppe fest.
Sicherheitsstufe	Wählen Sie zwischen „NoAuth/NoPriv", „Auth/NoPriv" und „Auth/Priv".

Schreibgeschützte Ansicht	Wählen Sie eine MIB-Ansicht aus, um die Berechtigung als „Nur Lesen“ aus der MIB-Ansichtsliste festzulegen. .
Lese-/Schreibansicht	Wählen Sie eine MIB-Ansicht aus, um die Berechtigung „Lesen-Schreiben” in der Liste der MIB-Ansichten festzulegen .
Inform-Ansicht	Wählen Sie eine MIB-Ansicht aus, um die Berechtigung als „Informieren“ aus der MIB-Ansichtsliste festzulegen.

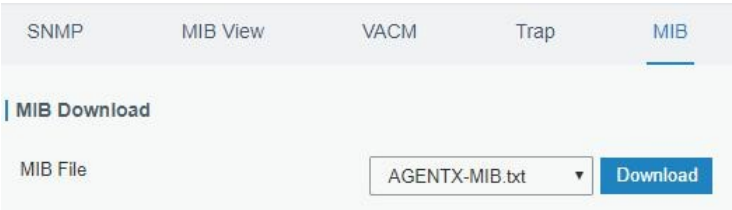
6.3.3.4 Trap

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

SNMP-Trap	
Element	Beschreibung
Aktivieren	Aktivieren oder deaktivieren Sie die SNMP-Trap-Funktion.
SNMP-Version	Wählen Sie die SNMP-Version aus; unterstützt SNMP v1/v2c/v3.
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. Der Standardport ist 162.
Name	Geben Sie bei Verwendung von SNMP v1/v2c den Gruppennamen ein; geben Sie bei Verwendung von SNMP v3 den Benutzernamen ein, wenn Sie SNMP v3 verwenden.
Auth/Priv-Modus	Wählen Sie zwischen „NoAuth & No Priv”, „Auth & NoPriv” und „Auth & Priv”.

6.3.6.3 MIB

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



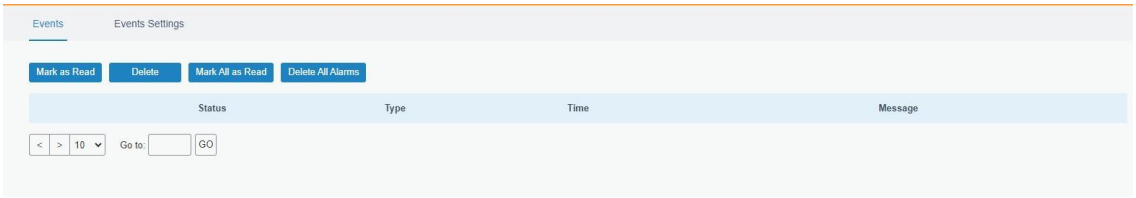
MIB	
Element	Beschreibung
MIB-Datei	Wählen Sie die gewünschte MIB-Datei aus.
Herunterladen	Laden Sie die MIB-Datei auf Ihren PC herunter.

6.3.5 Ereignisse

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

6.3.5.1 Ereignisse

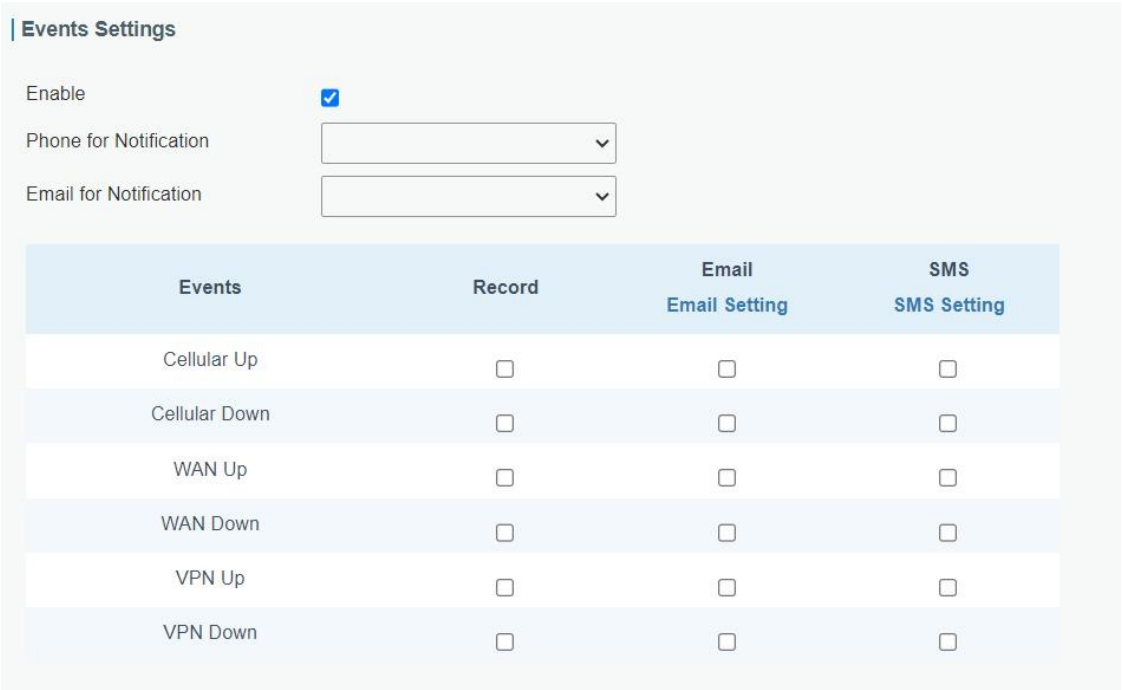
Auf dieser Seite können Sie Alarmmeldungen anzeigen.



Ereignisse	
Element	**Beschreibung**
Als gelesen markieren	Markieren Sie den ausgewählten Ereignisalarm als gelesen.
Löschen	Löschen Sie den ausgewählten Ereignisalarm.
Alle als gelesen markieren	Markieren Sie alle Ereignisalarme als gelesen.
Alle Alarme löschen	Löschen Sie alle Ereignisalarme.
Status	Zeigt den Lesestatus der Ereignisalarme an, z. B. „Gelesen“ und „Ungelesen“.
Typ	Zeigen Sie den Ereignistyp an, der alarmiert werden soll.
Zeit	Zeigen Sie die Alarmzeit an.
Meldung	Zeigen Sie den Alarminhalt an.

6.3.5.2 Ereigniseinstellungen

In diesem Abschnitt können Sie festlegen, welche Ereignisse aufgezeichnet werden sollen und ob Sie bei Änderungen E-Mail- und SMS-Benachrichtigungen erhalten möchten.



Ereigniseinstellungen	
Element	Beschreibung
Aktivieren	Aktivieren Sie diese Option, um die Ereigniseinstellungen zu aktivieren.
Telefon für Benachrichtigung	Wählen Sie die Telefongruppe aus, die SMS-Alarme empfangen soll.
E-Mail für Benachrichtigung	Wählen Sie eine E-Mail-Gruppe aus, die E-Mail-Alarme empfangen soll.
Ereignisse	Vom Gateway unterstützte Ereignistypen für die Aufzeichnung.
Aufzeichnung	Der relevante Inhalt des Ereignisalarms wird auf der Seite „Ereignis“ aufgezeichnet aufgezeichnet.
E-Mail	Der relevante Inhalt des Ereignisalarms wird per E-Mail versendet, wenn diese Option aktiviert ist.
E-Mail-Einstellungen	Klicken Sie auf „E-Mail“, um zur Seite „E-Mail“ weitergeleitet zu werden, auf der Sie die E-Mail-Gruppe konfigurieren.
SMS	Der relevante Inhalt des Ereignisalarms wird per SMS versendet, wenn diese Option aktiviert ist. Option ist aktiviert.
SMS-Einstellungen	Klicken Sie auf und Sie werden zur Seite „Telefon“ weitergeleitet, um die Telefon-Gruppenliste zu konfigurieren.

Verwandte Themen E-Mail-Einstellungen Telefoneinstellungen

6.4 Wartung

In diesem Abschnitt werden die Tools und die Verwaltung für die Systemwartung beschrieben.

6.4.1 Tools

Zu den Tools zur Fehlerbehebung gehören Ping und Traceroute.

6.4.1.1 Ping

Das Ping-Tool dient dazu, die IP-Adresse oder den Domänennamen eines externen Netzwerks anzupingen.

6.4.1.2 Traceroute

Das Traceroute-Tool wird zur Fehlerbehebung bei Netzwerk-Routing-Fehlern verwendet.

6.4.1.3 Qxdmlog

In diesem Abschnitt können Sie Diagnoseprotokolle des Mobilfunkmoduls über das QXDM-Tool erfassen.

6.4.2 Zeitplan

In diesem Abschnitt wird erläutert, wie Sie einen geplanten Neustart auf dem Gateway konfigurieren.

Zeitplan	
Element	Beschreibung
Zeitplan	Zeitplanereignis auswählen: Neustart: Starten Sie das Gateway regelmäßig neu.
Häufigkeit	Wählen Sie die Häufigkeit aus, mit der der Zeitplan ausgeführt werden soll.
Stunde und Minute	Wählen Sie die Uhrzeit für die Ausführung des Zeitplans.

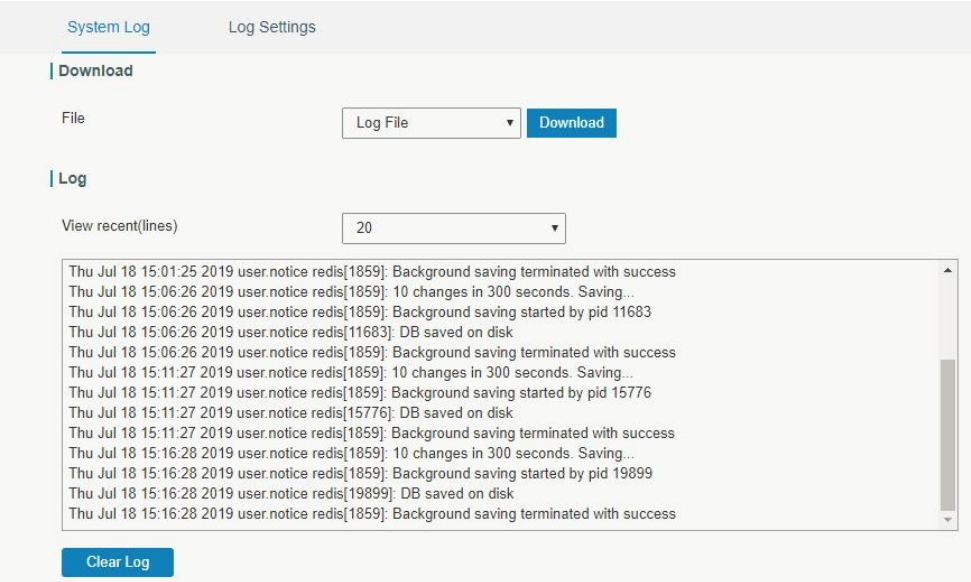
6.4.3 Protokoll

Das Systemprotokoll enthält eine Aufzeichnung von Informations-, Fehler- und Warnereignissen, die Aufschluss über die Funktionsweise des Systems geben. Durch Überprüfen der im Protokoll enthaltenen Daten kann ein Administrator oder Benutzer, der Fehlerbehebungen am System vornimmt, die Ursache eines Problems identifizieren oder feststellen, ob die Systemprozesse erfolgreich geladen werden.

Prozesse erfolgreich geladen werden. Ein Remote-Protokollserver ist möglich, und das Gateway lädt alle Systemprotokolle auf einen Remote-Protokollserver wie Syslog Watcher hoch.

6.4.3.1 Systemprotokoll

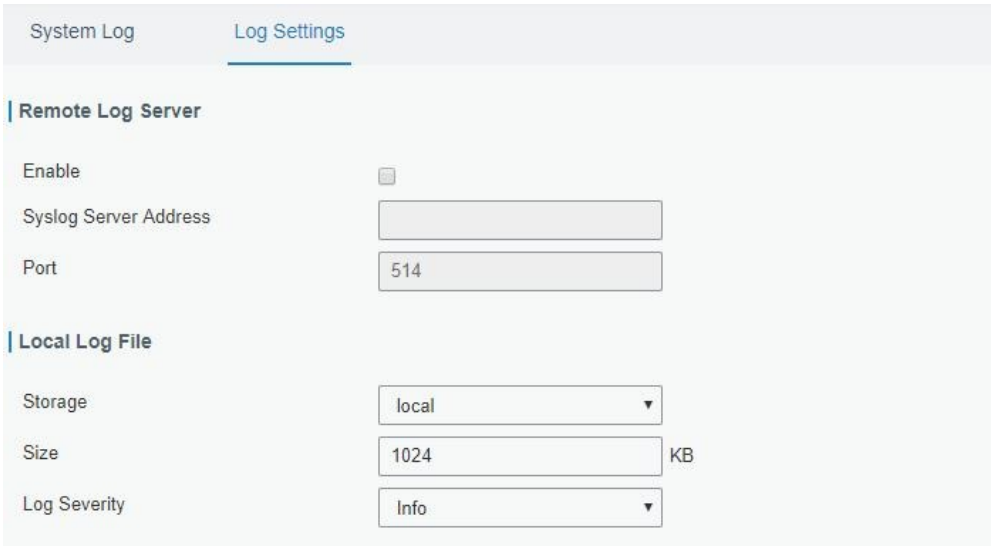
In diesem Abschnitt wird beschrieben, wie Sie die Protokolldatei herunterladen und das aktuelle Protokoll im Web anzeigen können.



Systemprotokoll	
Element	Beschreibung
Herunterladen	Protokoll-Datei herunterladen.
Letzte (Zeilen) anzeigen	Zeige die angegebenen Zeilen des Systemprotokolls an.
Protokoll löschen	Löschen Sie das aktuelle Systemprotokoll.

6.4.3.2 Protokolleinstellungen

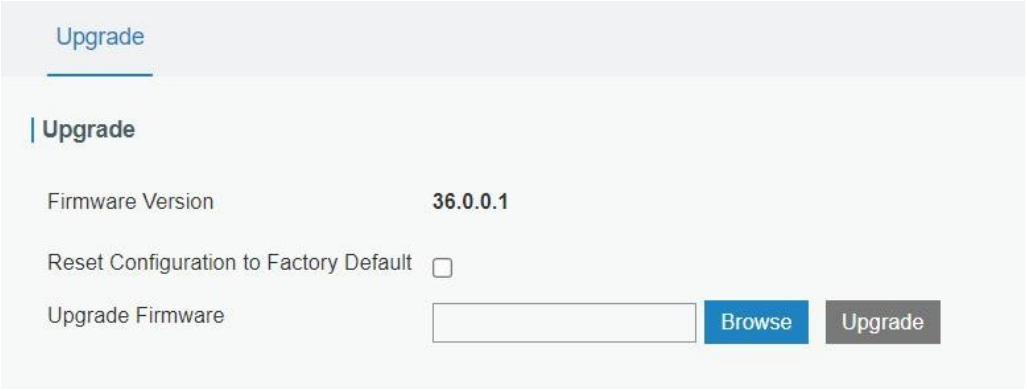
In diesem Abschnitt wird erläutert, wie Sie den Remote-Protokollserver und die lokalen Protokolleinstellungen aktivieren.



Protokolleinstellungen	
Element	Beschreibung
Remote-Protokollserver	
Aktivieren	Wenn „Remote-Protokollserver“ aktiviert ist, sendet das Gateway alle Systemprotokolle an den Remote-Server.
Syslog-Serveradresse	Geben Sie die Adresse des Remote-Systemprotokoll-Servers ein (IP/Domänenname).
Port	Geben Sie den Port des Remote-Systemprotokoll-Servers ein.
Lokale Protokolldatei	
Speicher	Der Benutzer kann die Protokolldatei im Speicher oder auf einer TF-Karte speichern.
Größe	Legen Sie die Größe der zu speichernden Protokolldatei fest.
Protokollschweregrad	Die Liste der Schweregrade entspricht dem Syslog-Protokoll.

6.4.4 Upgrade

In diesem Abschnitt wird beschrieben, wie Sie die Firmware des G- ateways über das Internet aktualisieren können. In der Regel ist eine Aktualisierung der Firmware nicht erforderlich.
Hinweis: Während des Firmware-Upgrades dürfen keine Vorgänge auf der Webseite durchgeführt werden, da sonst das Upgrade unterbrochen wird oder sogar das Gerät beschädigt werden kann.



Aktualisieren	
Element	Beschreibung
Firmware-Version	Zeigt die aktuelle Firmware-Version an.
Konfiguration zurücksetzen auf Werkseinstellungen zurücksetzen	Wenn diese Option aktiviert ist, wird das Gateway nach dem Upgrade auf die Werkseinstellungen zurückgesetzt.
Firmware aktualisieren	Klicken Sie auf die Schaltfläche „Durchsuchen“, um die neue Firmware-Datei auszuwählen, und klicken Sie auf „Aktualisieren“, um die Firmware zu aktualisieren.

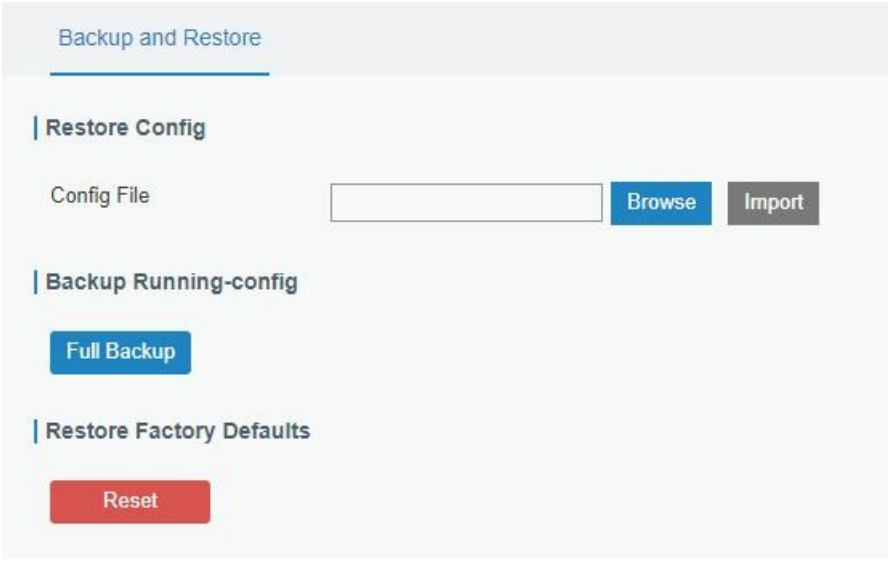
Beispiel für eine zugehörige Konfiguration

Firmware-Aktualisierung

6.4.5 Sichern und Wiederherstellen

In diesem Abschnitt wird erläutert, wie Sie eine Sicherung der gesamten Systemkonfigurationen in einer Datei erstellen,

wie Sie Teile wichtiger Konfigurationen nur für die Batch-Sicherung replizieren, die Konfigurationsdatei auf dem Gateway wiederherstellen und die Werkseinstellungen zurücksetzen können.



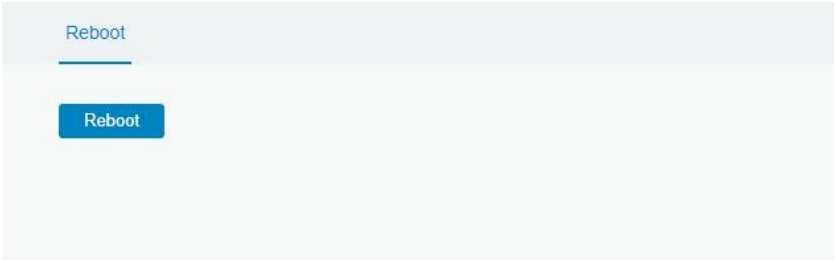
Sichern und Wiederherstellen	
Element	Beschreibung
Konfigurationsdatei	Klicken Sie auf die Schaltfläche „Durchsuchen“, um die Konfigurationsdatei auszuwählen, und klicken Sie dann auf die Schaltfläche „Importieren“ , um die Konfigurationsdatei auf das Gateway hochzuladen.
Vollständige Sicherung	Klicken Sie auf „Vollständige Sicherung“, um die aktuelle Konfigurationsdatei auf den PC zu exportieren.
Zurücksetzen	Klicken Sie auf die Schaltfläche „Zurücksetzen“, um die Werkseinstellungen wiederherzustellen. Das Gateway wird nach Abschluss des Zurücksetzens neu gestartet.

Beispiel für eine zugehörige Konfiguration

Werkseinstellungen wiederherstellen

6.4.6 Neustart

Auf dieser Seite können Sie das Gateway neu starten und zur Anmeldeseite zurückkehren. Wir empfehlen dringend, vor dem Neustart des Gateways auf die Schaltfläche „Speichern“ zu klicken, um zu vermeiden, dass die neue Konfiguration verloren geht.



[ENDE]