Milesight

Outdoor LoRaWAN® Gateway

UG67

Benutzerhandbuch

Vorwort

Vielen Dank, dass Sie sich für das Milesight UG67 LoRaWAN® Gateway entschieden haben. Das UG67 bietet eine stabile Netzwerkverbindung mit umfassenden Funktionen wie automatischem Failover/Failback, erweitertem Betriebstemperaturbereich, Hardware-Watchdog, VPN, Gigabit-Ethernet und vielem mehr.

Dieses Handbuch zeigt Ihnen, wie Sie das UG67 LoRaWAN® Gateway konfigurieren und bedienen. Hier finden Sie detaillierte Informationen zu den Funktionen und zur Konfiguration des Gateways.

Leser

Dieses Handbuch richtet sich in erster Linie an folgende Benutzer:

- Netzwerkplaner
- Technisches Support- und Wartungspersonal vor Ort
- Netzwerkadministratoren, die für die Netzwerkkonfiguration und -wartung verantwortlich sind

Verwandte Dokumente

Dokument	Beschreibung
UG67 Datenblatt	Datenblatt für UG67 LoRaWAN® Gateway.
UG67 Schnellstartanleitung	Schnellinstallationsanleitung für UG67 LoRaWAN® Gateway.

Konformitätserklärung

UG67 entspricht den grundlegenden Anforderungen und anderen relevanten Bestimmungen der CE, FCC und RoHS.

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

Revisionsverlauf

Datum	Dokumentversion	Beschreibung
31. Dezember 2020	V1.0	Erstversion
30. April 2021	V1.1	1. Unterstützung von LoRaWAN® Klasse B 2. Node-RED-Funktion hinzufügen 3. Funktion „Rauschanalysator“ hinzufügen 4. Multicast-Gruppen-Funktion hinzufügen 5. Anwendungsbeispiele hinzufügen
24. August 2021	V1.2	1. Unterstützung der Integration der Yeastar Workplace-Plattform 2. Statusseite „Paketweiterleitung“ löschen 3. Aktualisierung der Webseite „Telefon & E-Mail“
15. Dezember 2021	V1.3	1. Hinzufügen von AS923-3 und AS923-4 2. Ändern Sie das Feld „Netzwerkserver-Kanalmaske“ in „Kanal“ 3. Gerätekanaleinstellung im Profil hinzufügen
23. Februar 2022	V1.4	1. Batch-Sicherung hinzufügen 2. Anmeldeseite aktualisieren 3. Standardantennentyp auf externe Antenne ändern 4. Zeit für Class C ACK-Timeout anpassen
1. Juni 2022	V1.5	1. Unterstützung von VLAN-Trunk-Client 2. Systemnamen in SNMP hinzufügen 3. Option „L2TP-Peer-DNS verwenden” hinzufügen
26. Dezember 2022	V1.6	1. BACnet-Server-Funktion hinzufügen 2. Funktion „Payload-Codec“ hinzufügen 3. Funktion „Zurücksetzen“ und „Alle Flows exportieren“ in Node-RED hinzufügen 4. Funktion „Daten-Retransmission” in Packet Forward hinzugefügt
6. März 2023	V1.7	1. Modus „Eingebaute Antenne“ löschen 2. LBT-Funktion hinzufügen
21. Februar 2024	V1.8	1. Kompatibel mit der Milesight-Entwicklungsplattform 2. Standardadresse für sekundären ICMP- und DNS-Server aktualisieren 3. Funktion für Mobilfunk-IMS und benutzerdefinierte MTU hinzufügen 4. 8 voreingestellte Geräteprofile hinzugefügt
7. Juni 2024	V1.9	1. Unterstützung für den Import von OVPN-Dateien für OpenVPN-Verbindungen

		2. Unterstützung der Paketfilterfunktion 3. Hinzufügen eines Standard-WLAN-Verbindungskennworts 4. Hinzufügen eines Benutzernamens in den SMTP-Client-Einstellungen 5. Hinzufügen von BACnet-Objekttypen, Unterstützung der Anpassung von Objektinstanzen
31. Oktober 2024	V 1.10	1. WireGuard-Funktion hinzufügen; 2. MQTT-Daten-Retransmission und Beibehaltungsoption hinzufügen; 3. Metadatenoption auf der Seite „Anwendung" hinzufügen; 4. Node-RED SSL-Zugriffsoption hinzugefügt; 5. BACnet-Objekt-Ereigniserkennungsfunktion hinzugefügt; 6. Netzwerkpaket-Analysator-Funktion hinzufügen; 7. Kompatibel mit DeviceHub 2.0; 8. Fügen Sie die Anpassung der zellularen Subnetzmaske und des DNS-Servers hinzu.
8. Januar 2025	V 1.11	1. Objektzuordnungsfunktion auf der Seite „Payload Codec" hinzufügen. 2. Entfernen der Option „BACnet/IP" auf der Seite „Anwendung"; 3. BACnet-Objekt-Web-GUI aktualisieren; 4. Modbus-Server-Funktion hinzugefügt.
3. April 2025	V 1.12	1. FUOTA-Funktion hinzufügen; 2. MQTT-Last-Will-Message-Funktion hinzufügen; 3. Aktualisieren der Anwendungsschlüsseloptionen beim Hinzufügen eines Geräts; 4. Metadatenoption aktualisieren; 5. Aktualisierung des WAN-Standardverbindungstyps als DHCP; 6. Aktualisierung der Schritte für den Zugriff auf die Web-GUI.
29. Mai 2025	V 1.12.1	1. Zeitüberschreitungsparameter für Geräte hinzufügen; 2. Der BACnet-Server ist standardmäßig aktiviert, aktualisieren Sie die Standard-Geräte-ID. 3. Aktiviertes Element in der Geräteliste in Statuselement ändern; 4. Unterstützung für das Hinzufügen von BACnet-Globalobjekten; 5. Unterstützung für das automatische Hinzufügen von BACnet-Objekten; 6. Erweitern Sie die maximale Anzahl von BACnet- und Modbus-Objekten auf 10.000. 7. Unterstützt das Hinzufügen eines unabhängigen HTTP-API-Kontos.
13. August 2025	V 1.13	1. Hinzufügen eines Datenelements auf der Seite „Packet Forwarder-Traffic" 2. Hinzufügen einer Seitenkonfiguration für die Objektzuordnungsfunktion des benutzerdefinierten Payload-Codecs. 3. ADR-Option im Geräteprofil hinzufügen; 4. Unterstützung für den Export aller Geräteinformationen; 5. Funktion zum Löschen der Download-Warteschlange auf der Seite „Pakete" hinzufügen; 6. BACnet-globale Objekttypen hinzufügen; 7. Modbus-globale Objektfunktion und Server-ID-Typ hinzufügen. 8. Modbus-Objektkopierfunktion hinzufügen.

Inhalt

Kapitel 1 Produktvorstellung

1.1 Übersicht

UG67 ist ein robustes 8-Kanal-LoRaWAN®-Gateway für den Außenbereich. Mit dem SX1302 LoRa-Chip und einer leistungsstarken Quad-Core-CPU unterstützt UG67 die Verbindung mit mehr als 2000 Knoten. UG67 hat eine Sichtverbindung von bis zu 15 km und kann in städtischen Umgebungen eine Reichweite von etwa 2 km abdecken, was es ideal für Smart Offices, Smart Buildings und viele andere Außenanwendungen macht.

UG67 unterstützt nicht nur mehrere Backhaul-Backups mit Ethernet, WLAN und Mobilfunk, sondern verfügt auch über integrierte Mainstream-Netzwerkserver (wie The Things Industries, ChirpStack usw.) sowie einen integrierten Netzwerkserver und die Milesight IoT Cloud für eine einfache Bereitstellung.

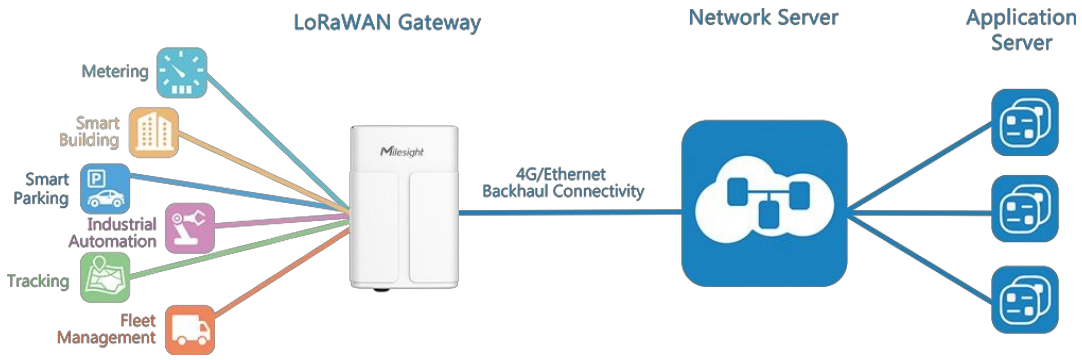


Abbildung 1-1

1.2 Vorteile

Vorteile

- Integrierte industrielle CPU und großer Speicher
- Ethernet, 2,4-GHz-WLAN und globale 2G/3G/LTE-Optionen erleichtern die Verbindung
- Integrierter Netzwerkserver und kompatibel mit mehreren Netzwerkservern von Drittanbietern
- MQTT(s)- oder HTTP(s)-Protokoll für die Datenübertragung zum Anwendungsserver
- Robustes Gehäuse, optimiert für Wand- oder Mastmontage
- 3 Jahre Garantie inklusive

Sicherheit und Zuverlässigkeit

- Automatisches Failover/Failback zwischen Ethernet und Mobilfunk
- Aktivierung des Geräts mit Sicherheitsframeworks wie IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN/WireGuard
- Integrierter Hardware-Watchdog zur automatischen Wiederherstellung nach verschiedenen Ausfällen und zur Gewährleistung höchster Verfügbarkeit

Einfache Wartung

- Milesight DeviceHub und Milesight Development Platform ermöglichen eine einfache Einrichtung, Massenkonfiguration und zentralisierte Verwaltung von Remote-Geräten
- Das benutzerfreundliche Design der Weboberfläche und verschiedene Upgrade-Optionen helfen Administratoren, das Gerät kinderleicht zu verwalten
- WEB-GUI und CLI ermöglichen dem Administrator eine schnelle Konfiguration und einfache Verwaltung einer großen Anzahl von Geräten
- Benutzer können die Remote-Geräte auf der bestehenden Plattform über den Industriestandard SNMP effizient verwalten.

Funktionen

- Verbindung von Remote-Geräten in einer Umgebung, in der sich die Kommunikationstechnologien ständig ändern
- Industrieller Quad-Core-64-Bit-ARM-Cortex-A53-Prozessor, hohe Leistung mit bis zu 1,5 GHz bei geringem Stromverbrauch und 8 GB eMMC zur Unterstützung weiterer Anwendungen
- Unterstützt einen breiten Betriebstemperaturbereich von -40 °C bis 70 °C/-40 °F bis 158 °F

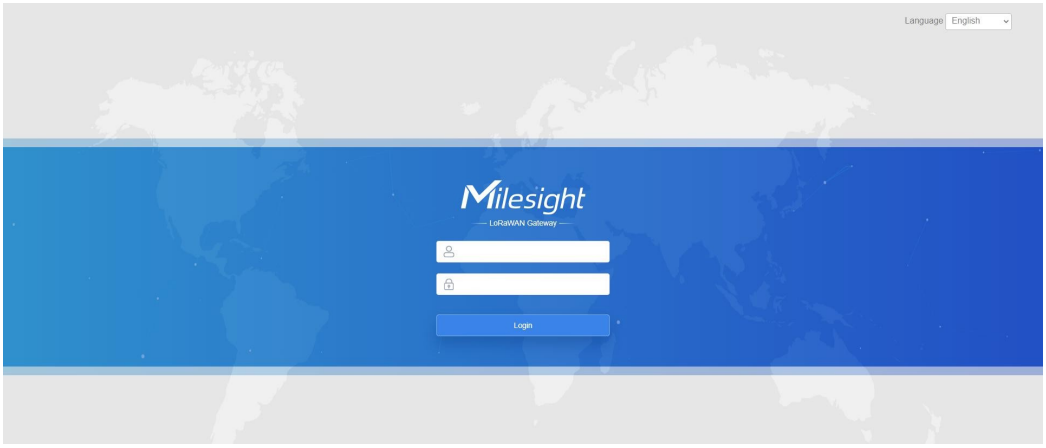
Kapitel 2 Zugriff auf die Web-GUI

In diesem Kapitel wird erläutert, wie Sie auf die Web-GUI des UG67 zugreifen können. Benutzername: **admin**
Passwort: **password**
Konfigurationsschritte:

1. Aktivieren Sie die WLAN-Verbindung auf Ihrem Computer und suchen Sie nach dem Zugangspunkt **Gateway_******, um eine Verbindung herzustellen. Das Standard-WLAN-Passwort lautet **iotpassword**.

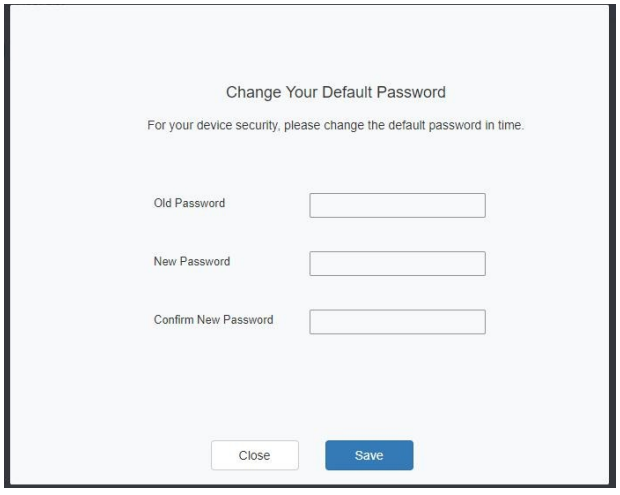
2. Öffnen Sie einen Webbrowser auf Ihrem PC (Chrome wird empfohlen) und geben Sie die IP-Adresse **192.168.1.1** ein, um auf die Web-GUI zuzugreifen.

3. Geben Sie den Benutzernamen und das Passwort ein und klicken Sie auf „Anmelden".

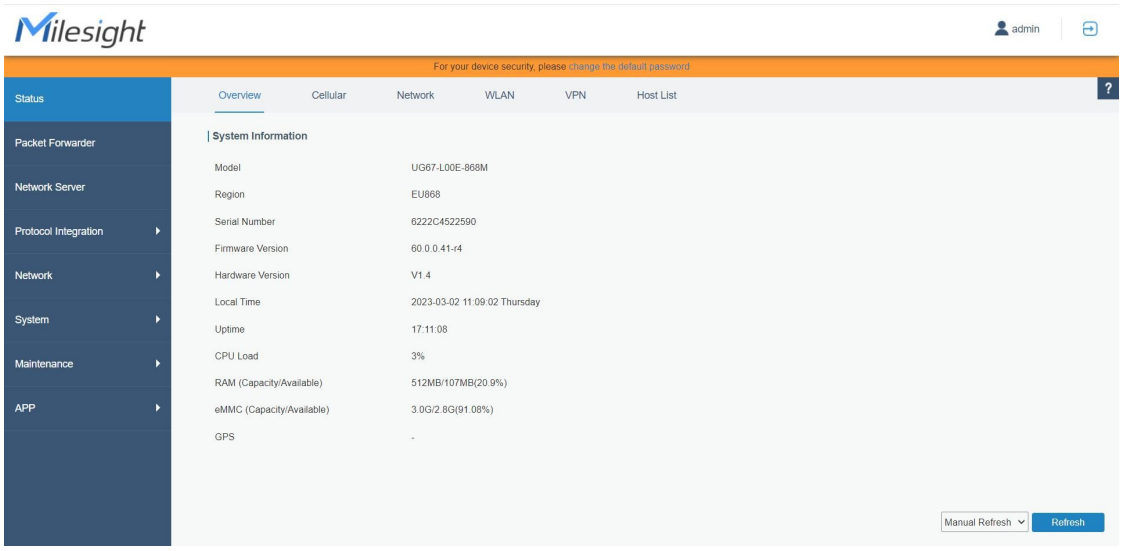


Wenn Sie den Benutzernamen oder das Passwort mehr als 5 Mal falsch eingeben, wird die Anmeldeseite für 10 Minuten gesperrt.

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.

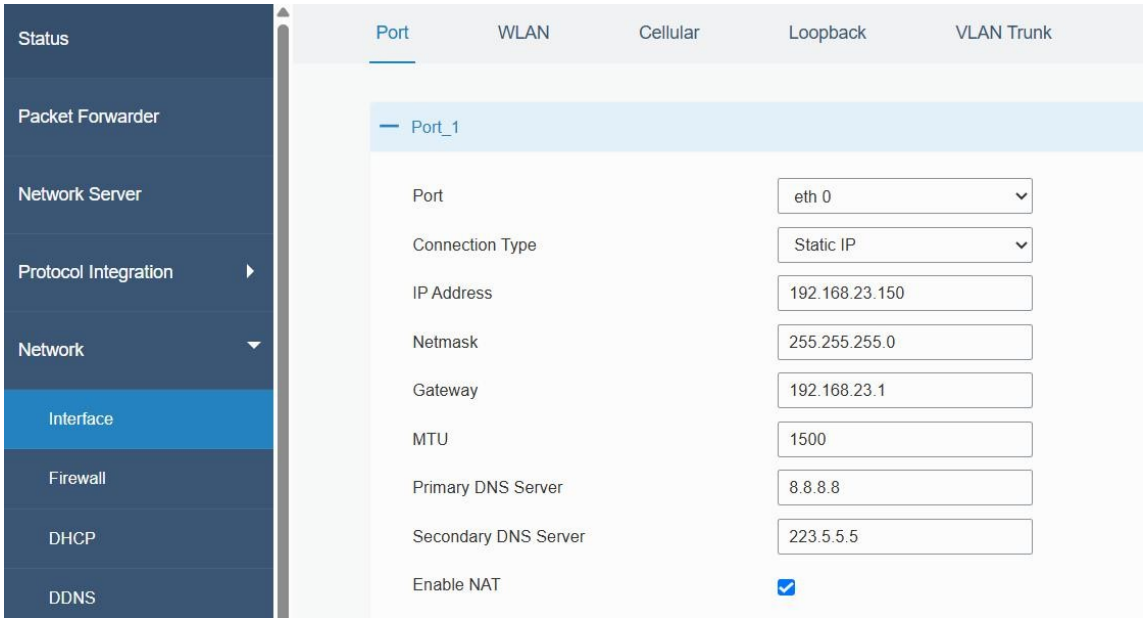


5. Nach der Anmeldung bei der Web-GUI können Sie Systeminformationen anzeigen und die Konfiguration des Gateways vornehmen. Aus Sicherheitsgründen wird empfohlen, das Passwort zu ändern.



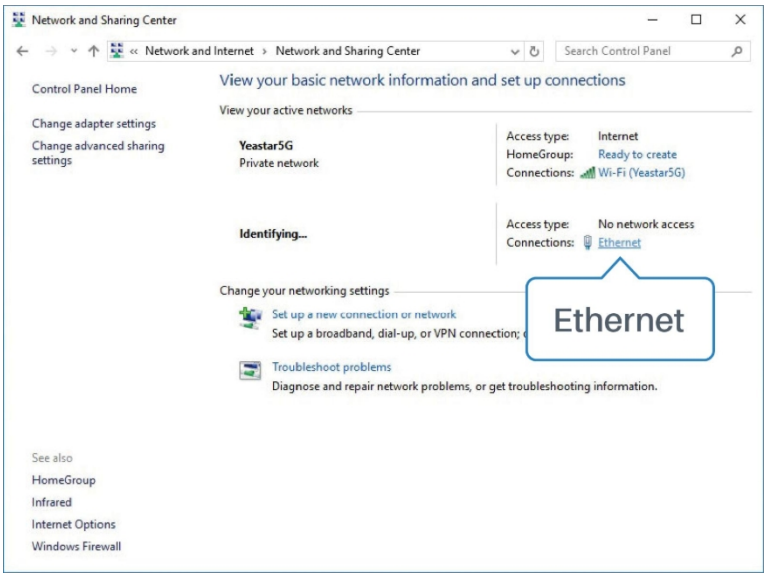
Hinweis: Der Verbindungstyp des Ethernet-Ports ist standardmäßig DHCP. Das Gateway unterstützt auch den kabelgebundenen Zugriff, wenn Sie den Verbindungstyp des Ethernet-Ports als statische IP auswählen und dem Ethernet-Port eine IP-Adresse zuweisen.

1. Gehen Sie zur Seite **„Netzwerk > Schnittstelle > Port“**, um als Verbindungstyp **„Statische IP“** auszuwählen und eine IP-Adresse für den Ethernet-WAN-Port zu konfigurieren.

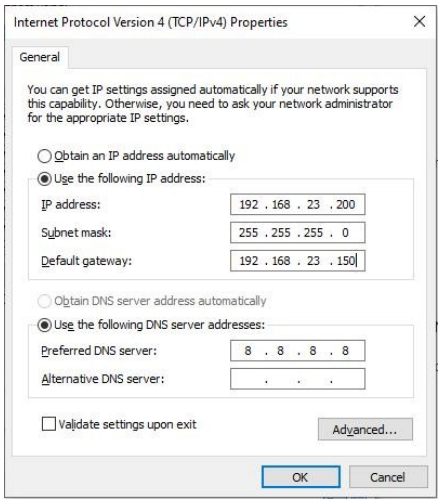


2. Verbinden Sie den PC direkt oder über einen PoE-Injektor mit dem ETH-Port des UG67.
3. Weisen Sie dem Computer die IP-Adresse manuell zu. Nehmen Sie als Beispiel das Windows 10-System:

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



B. Gehen Sie zu „Eigenschaften“ → „Internetprotokoll Version 4 (TCP/IPv4)“ und wählen Sie „Folgende IP-Adresse verwenden“. Weisen Sie dann manuell eine statische IP-Adresse innerhalb desselben Subnetzes zu. Gateway.



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

Kapitel 3 Webkonfiguration

3.1 Status

3.1.1 Übersicht

Auf dieser Seite können Sie die Systeminformationen des Gateways anzeigen.

Abbildung 3-1-1-1

Systeminformationen	
Element	**Beschreibung**
Modell	Zeigt den Modellnamen des Gateways an.
Region	Zeigt die vom Gateway verwendete LoRaWAN®-Frequenz an.
Seriennummer	Zeigt die Seriennummer des Gateways an.
Firmware-Version	Zeigt 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)	Zeigt die RAM-Kapazität und den verfügbaren RAM-Speicher an.
eMMC (Kapazität/verfügbar)	Zeigt die eMMC-Kapazität und den verfügbaren eMMC-Speicher an.
GPS	Zeigt die GPS-Daten des Gateways an.

Tabelle 3-1-1-1 Systeminformationen

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

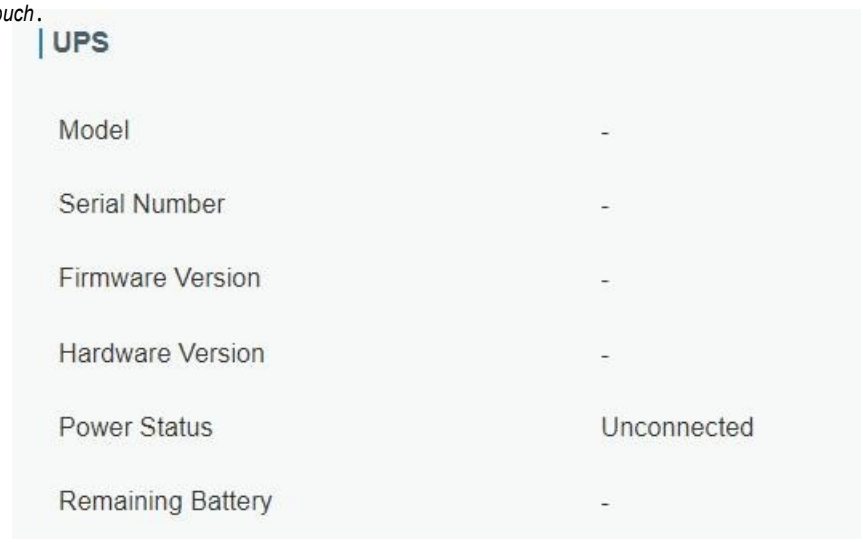


Abbildung 3-1-1-2

3.1.2 Mobilfunk (nur Mobilfunkversion)

Auf dieser Seite können Sie den Mobilfunknetzstatus des Gateways anzeigen.

Abbildung 3-1-2-1

Modem-Informationen	
Element	**Beschreibung**

Status	Zeigt den entsprechenden Erkennungsstatus des Moduls und der SIM-Karte an.
Modell	Zeigen Sie 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	Zeigt den Netzbetreiber an, bei dem die SIM-Karte registriert ist.
Netzwerktyp	Zeigt den verbundenen Netzwerktyp an, z. B. LTE, 3G usw.
PLMN-ID	Zeigt 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.

Tabelle 3-1-2-1 Modem-Informationen

Abbildung 3-1-2-2

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

Tabelle 3-1-2-2 Netzwerkstatus

3.1.3 Netzwerk

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

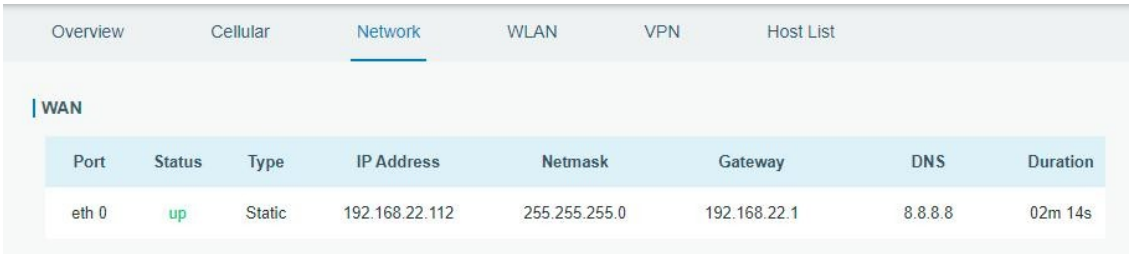


Abbildung 3-1-3-1

Netzwerk	
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 und das Ethernet-Kabel angeschlossen ist. „Down“ bedeutet, dass Ethernet Das Kabel ist nicht angeschlossen oder die WAN-Funktion ist deaktiviert.
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	Zeigt die Informationen darüber an, wie lange das Ethernet-Kabel mit dem Ethernet-Port verbunden ist, wenn der Port aktiviert ist. Sobald der Port ist deaktiviert oder das Ethernet-Kabel ist nicht angeschlossen, wird die Dauer angehalten.

Tabelle 3-1-3-1 WAN-Status

3.1.4 WLAN

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

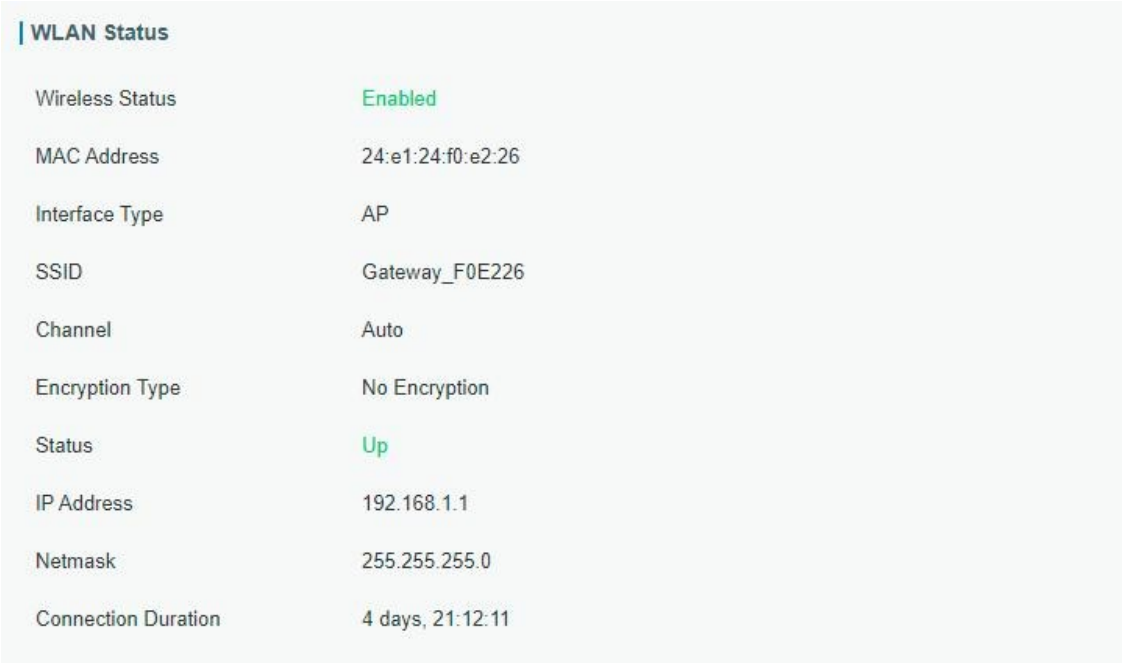


Abbildung 3-1-4-1

WLAN-Status	
Element	**Beschreibung**
WLAN-Status	Zeigt den WLAN-Status an.
MAC-Adresse	Zeigt die MAC-Adresse an.
Schnittstellentyp	Zeigt den Schnittstellentyp an, z. B. „AP“ oder „Client“.
SSID	Zeigt die SSID an.
Kanal	Zeigt den WLAN-Kanal an.
Verschlüsselungstyp	Zeigt den Verschlüsselungstyp an.
Status	Zeige den Verbindungsstatus an.
IP-Adresse	Zeigt die IP-Adresse des Gateways an.
Netzmaske	Zeigt die drahtlose MAC-Adresse des Gateways an.
Gateway	Zeigt die Gateway-Adresse im drahtlosen Netzwerk an.
Verbindungsdauer	Zeigt Informationen darüber an, wie lange das WLAN-Netzwerk verbunden ist.

Tabelle 3-1-4-1 WLAN-Status

Abbildung 3-1-4-2

Verbundene Stationen	
Element	**Beschreibung**
IP-Adresse	Zeigt die IP-Adresse des Zugangspunkts oder Clients an.
MAC-Adresse	Zeigt die MAC-Adresse des Zugangspunkts oder Clients an.
Verbindungsdauer	Zeigen Sie Informationen darüber an, wie lange das WLAN-Netzwerk bereits verbunden ist.

Tabelle 3-1-4-2 WLAN-Status

3.1.5 VPN

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

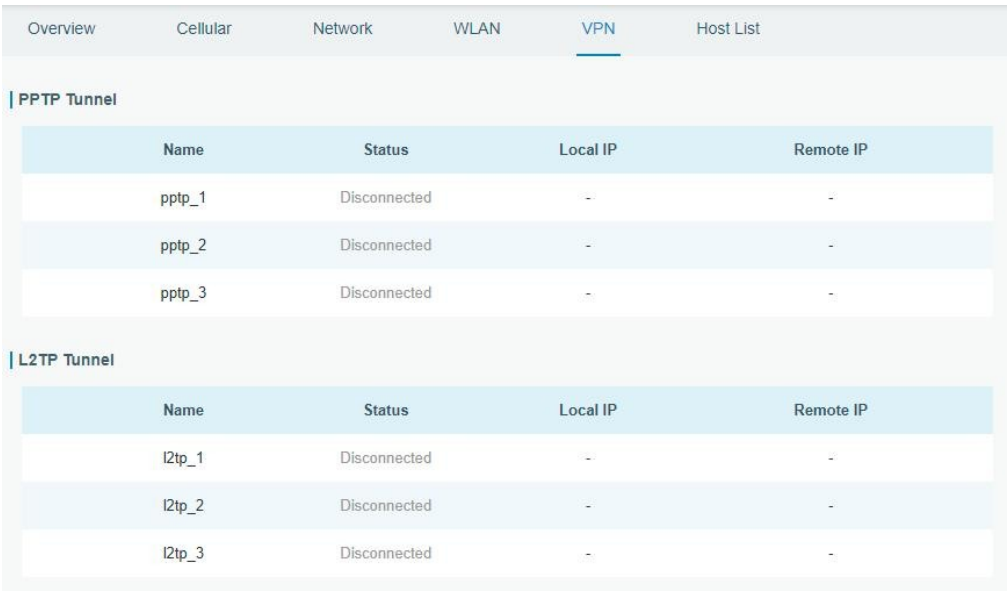


Abbildung 3-1-5-1

Abbildung 3-1-5-2

Abbildung 3-1-5-3

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.

Tabelle 3-1-5-1 VPN-Status

3.1.6 Hostliste

Auf dieser Seite können Sie die Host-Informationen anzeigen.

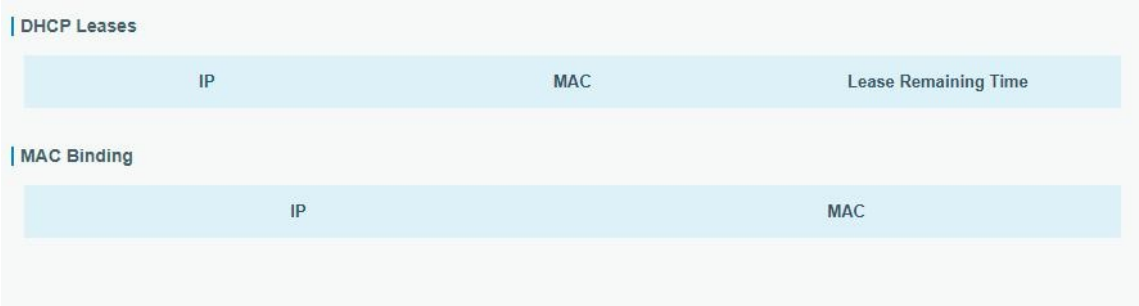
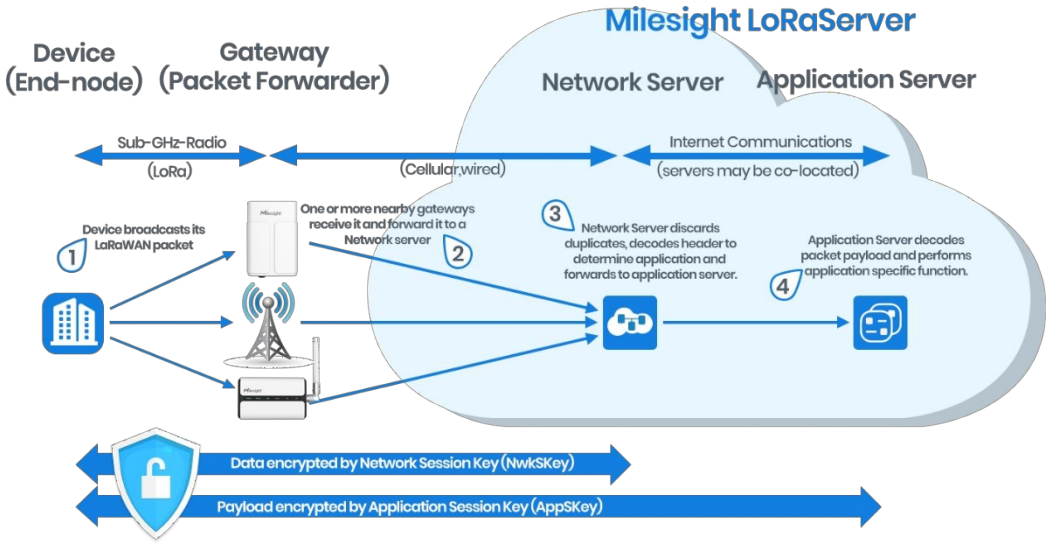


Abbildung 3-1-6-1

Hostliste	
Element	**Beschreibung**
DHCP-Leases	
IP-Adresse	IP-Adresse des DHCP-Clients anzeigen
MAC-Adresse	MAC-Adresse des DHCP-Clients anzeigen
Verbleibende Lease-Zeit	Zeigt die verbleibende Lease-Zeit des DHCP-Clients an.
MAC-Bindung	
IP & MAC	Zeigt die IP-Adresse und MAC-Adresse an, die in der Liste „Static IP“ des DHCP-Dienstes festgelegt sind. des DHCP-Dienstes festgelegten IP-Adresse und MAC-Adresse.

Tabelle 3-1-6-1 Beschreibung der Hostliste

3.2 LoRaWAN



3.2.1 Paketweiterleitung

3.2.1.1 Allgemeines

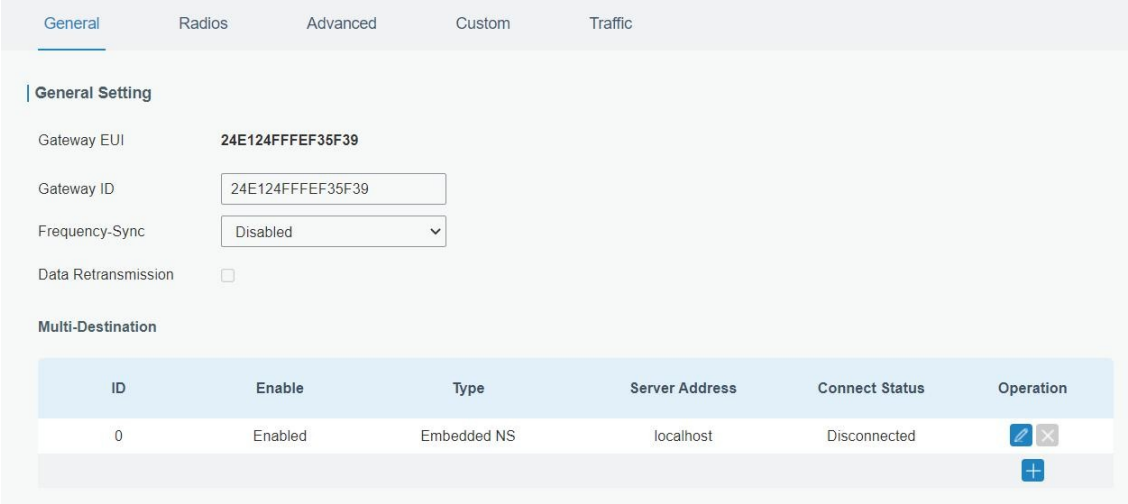


Abbildung 3-2-1-1

Allgemeine Einstellungen	
Element	**Beschreibung**
Gateway-EUI	Zeigt die eindeutige Kennung des Gateways an, die nicht bearbeitet werden kann. Format: „24E124FFFE“ + die letzten 6 Zeichen der Eth-MAC-Adresse
Gateway-ID	Geben Sie die entsprechende ID ein, die Sie für die Registrierung des Gateway beim Remote-Netzwerkserver verwendet haben. Diese entspricht in der Regel der Gateway-EUI und kann geändert werden.
Frequenzsynchronisation	Synchronisieren Sie die Frequenzkonfigurationen vom Netzwerkserver, indem Sie die entsprechende Multi-Destination-ID aus.
Daten	Wenn das Gateway eine Verbindung zu einem einzelnen

Retransmission	Chirpstack/Semtech/Remote Embedded NS/Basic Station-Paketweiterleitungsdienst verbunden ist, unterstützt es die Speicherung von bis zu 1 Million Datenelementen, wenn die Netzwerkverbindung unterbrochen ist, und sendet die Daten nach Wiederherstellung der Netzwerkverbindung erneut.
Mehrfachziel	Das Gateway leitet die Daten an die Netzwerk-Serveradresse weiter, die in der Liste erstellt und aktiviert wurde.
Verbindung Status	Zeigen Sie den Verbindungsstatus des Paketweiterleiters an.

Tabelle 3-2-1-1 Allgemeine Einstellungsparameter

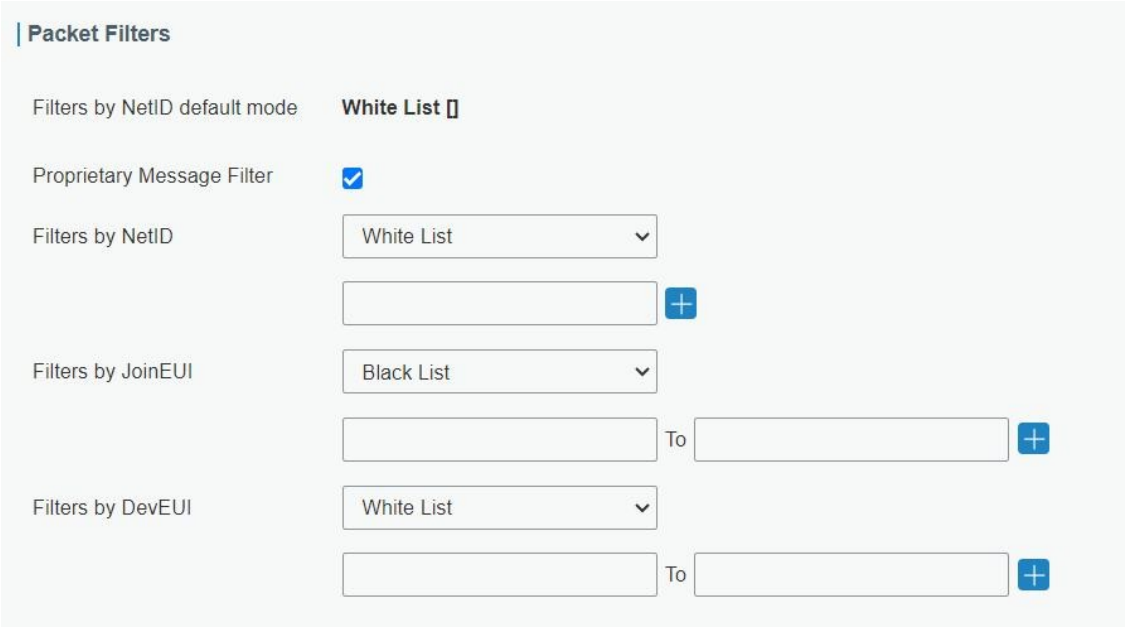


Abbildung 3-2-1-2

Paketfilter	
Parameter	**Beschreibung**
Filter nach NetID Standardmodus	Wählen Sie den Filtermodus als Blacklist oder Whitelist aus. **Whitelist:** Nur die Pakete auf dieser Liste werden an den Netzwerkserver weitergeleitet. **Blacklist:** Leiten Sie nur die Pakete weiter, die nicht auf dieser Liste stehen, an den Netzwerkserver weiter weiterleiten.
Proprietär Nachrichtenfilter	Aktivieren Sie diese Option, um proprietäre Nachrichtenpakete (Mtype=111) nicht weiterzuleiten.
Filter nach NetID	Weiterleiten/Nicht weiterleiten der Uplink-Pakete, die mit der NetID übereinstimmen.
Filter nach JoinEUI	Weiterleiten/Nicht weiterleiten der Join-Anforderungspakete, die mit dem JoinEUI-Bereich entsprechen.
Filterung nach DevEUI	Weiterleiten/Nicht weiterleiten der Join-Anforderungspakete, die mit dem DevEUI-Bereich übereinstimmen entsprechen.
Liste	Legen Sie den spezifischen Filterwert oder die Bereichsliste fest. Jede Bedingung unterstützt

	, um maximal 5 Listen hinzuzufügen.

Tabelle 3-2-1-2 Parameter für Paketfilter

Hinweis:

1. Wenn sowohl EUI als auch dev EUI konfiguriert sind, werden nur Pakete weitergeleitet, die beide Bedingungen erfüllen.
2. Diese Funktion wird nicht unterstützt, wenn der Paketweiterleitungstyp Loriot oder Everynet ist.
3. Wenn ein Netzwerk-Server eines Drittanbieters dem Gateway eine Filterbedingung zuweist, verwendet das Gateway vorrangig die Einstellungen des Netzwerk-Servers.

Beispiel für eine entsprechende Konfiguration

Konfiguration des Paketweiterleiters

3.2.1.2 Funkgeräte

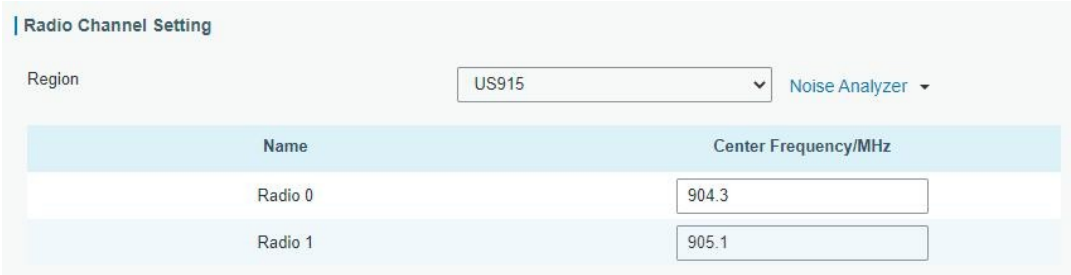


Abbildung 3-2-1-3

Funkgeräte – Funkkanaleinstellung		
Element	**Beschreibung**	**Standard**
Region	Wählen Sie den LoRaWAN®-Frequenzplan für die Upstream- und Downlink-Frequenzen und Datenraten. Die verfügbaren Kanalpläne hängen vom Gateway-Modell ab Modell.	Basierend auf dem Modell des Gateways
Mittenfrequenz	Ändern Sie die Frequenzen, um Pakete von LoRaWAN®-Knoten zu empfangen.	Basierend auf den Angaben in den regionalen LoRaWAN®-Parametern Dokument

Tabelle 3-2-1-3 Einstellparameter für Funkkanäle

Abbildung 3-2-1-4

Funkgeräte – Mehrkanaleinstellung		
Element	**Beschreibung**	**Standard**
Aktivieren	Klicken Sie hier, um diesen Kanal für die Übertragung von Pakete.	Aktiviert
Index	Geben Sie die Ordnungszahl der Liste an.	/
Radio	Wählen Sie Radio 0 oder Radio 1 als Mittenfrequenz Frequenz.	Radio 0
Frequenz/MHz	Geben Sie die Frequenz dieses Kanals ein. Bereich: Mittenfrequenz ±0,4625.	Basierend auf dem LoRaWAN® Regionaldokument

Tabelle 3-2-1-4 Parameter für die Mehrkanaleinstellung

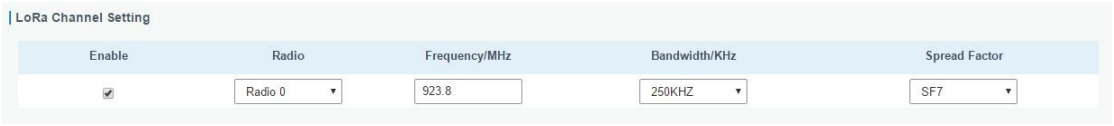


Abbildung 3-2-1-5

Funkgeräte – LoRa-Kanaleinstellung		
Element	**Beschreibung**	**Standard**
Aktivieren	Klicken Sie hier, um diesen Kanal für die Übertragung von Pakete.	Aktiv
Funk	Wählen Sie Radio 0 oder Radio 1 als Mittenfrequenz Frequenz.	Radio 0
Frequenz/MHz	Geben Sie die Frequenz dieses Kanals ein. Bereich: Mittenfrequenz ±0,9.	Basierend auf der unterstützten Frequenz
Bandbreite/MHz	Geben Sie die Bandbreite dieses Kanals ein.	500 kHz
Spreizfaktor	Wählen Sie den auswählbaren Spreizfaktor. Der Kanal mit großem Spreizfaktor entspricht einer niedrigen Rate, während der kleine einem hohen Wert entspricht.	Basierend auf den Angaben in den regionalen LoRaWAN®-Parametern Dokument

Tabelle 3-2-1-5 LoRa-Kanaleinstellungsparameter

Abbildung 3-2-1-6

Funkgeräte-FSK-Kanaleinstellung		
Element	**Beschreibung**	**Standard**
Aktivieren	Klicken Sie hier, um diesen Kanal für die Übertragung von Pakete.	Deaktiviert
Funk	Wählen Sie Radio 0 oder Radio 1 als Mittenfrequenz Frequenz.	Radio 0

Frequenz/MHz	Geben Sie die Frequenz dieses Kanals ein. Bereich: Mittenfrequenz ±0,9.	Basierend auf der unterstützten Frequenz
Bandbreite/MHz	Geben Sie die Bandbreite dieses Kanals ein. Empfohlener Wert: 125 kHz, 250 kHz, 500 kHz	Basierend auf der unterstützten Frequenz
Datenrate	Geben Sie die Datenrate ein. Bereich: 500-25000.	500

Tabelle 3-2-1-6 FSK-Kanaleinstellungsparameter

3.2.1.3 Rauschanalysator

Der Rauschanalysator wird verwendet, um das Rauschen jedes Frequenzkanals zu scannen und ein Diagramm zu erstellen, anhand dessen Benutzer die Umgebungsstörungen analysieren und die beste Konfiguration auswählen können. RSSI gibt die Empfindlichkeit für jeden Kanal an. Je niedriger der RSSI-Wert, desto besser das Signal. Es wird nicht empfohlen, diese Funktion bei Verwendung eines Paketweiterleiters zu aktivieren, da dies die Downlink-Übertragung beeinträchtigt.

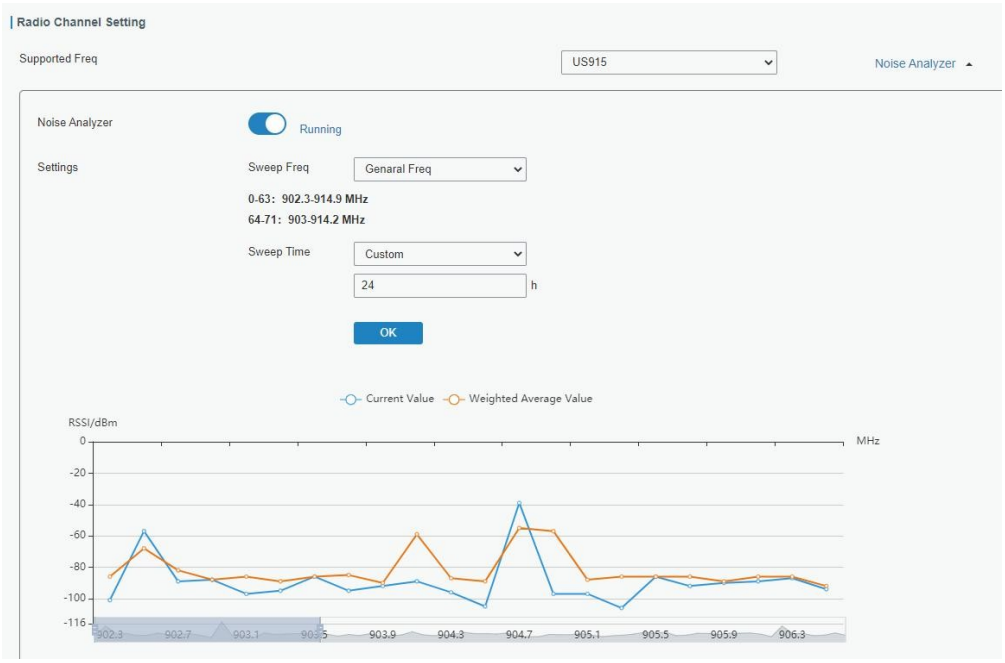


Abbildung 3-2-1-7

Rauschanalysator		
Element	**Beschreibung**	**Standard**
Aktivieren	Klicken Sie hier, um die Rauschanalysator-Funktion zu aktivieren.	Deaktiviert
Frequenzbereich	Wählen Sie den Frequenzbereich für den Sweep aus. **Allgemeine Frequenz:** Frequenzen basierend auf dem LoRaWAN®-Dokument zu regionalen Parametern **Benutzerdefiniert:** Benutzerdefinierter Frequenzbereich	Allgemeine Freq
Sweep-Zeit	Aktivieren Sie den Geräuschanalysator kontinuierlich oder innerhalb eines bestimmten Zeitraums. Wenn „Benutzerdefiniert“ ausgewählt ist, wird der Geräuschanalysator automatisch nach der vorkonfigurierten Zeit.	Benutzerdefiniert/24h

	Hinweis: Es wird empfohlen, die Zeit anzupassen, da die Geräuschanalysefunktion die normale Datenübertragung beeinträchtigt .	

Tabelle 3-2-1-7 Einstellparameter für den Geräuschanalysator

3.2.1.4 Erweitert

Dieser Abschnitt befasst sich mit den detaillierten Einstellungen für die Beacon-Übertragung und -Validierung.

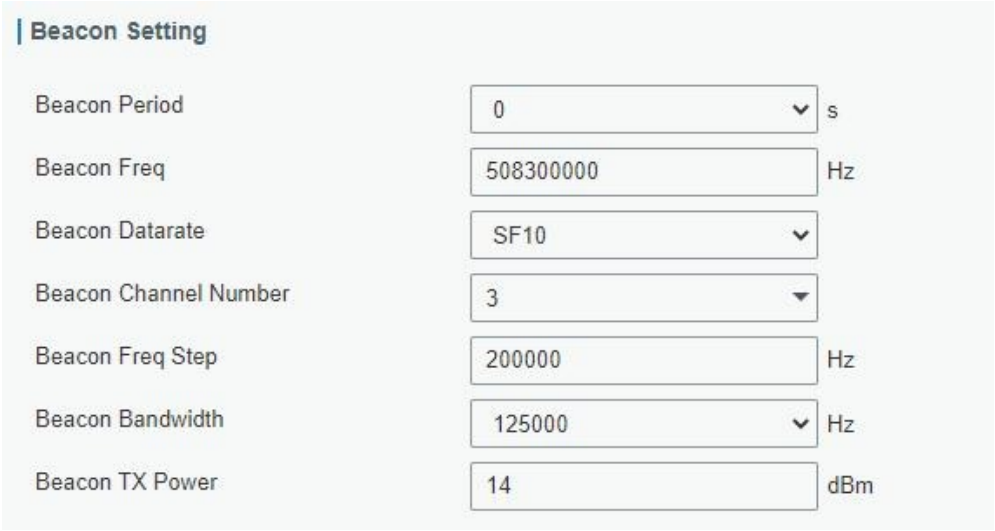


Abbildung 3-2-1-8

Erweitert – Beacon-Einstellung		
Element	**Beschreibung**	**Standard**
Beacon-Periode	Intervall, in dem das Gateway Beacons für die Zeit synchronisierung der Klasse B sendet. Gerätezeitsynchronisation. 0 bedeutet, dass das Gateway keine Beacons sendet.	0
Beacon-Frequenz	Die Frequenz der Beacons.	Basierend auf der unterstützten Frequenz
Beacon-Datenrate	Die Datenrate der Beacons.	Basierend auf der unterstützten Frequenz
Beacon-Kanal Anzahl	Bei Auswahl von „Benutzerdefiniert“ können Benutzer Bereich von 1 bis 8 anpassen.	1
Beacon-Frequenz Schritt	Frequenzintervall der Beacons.	200000
Beacon Bandbreite	Die Bandbreite der Beacons. Einheit: Hz	12500 Hz
Beacon-Sendeleistung	Die Sendeleistung der Beacons.	Basierend auf der unterstützten

		Frequenz

Tabelle 3-2-1-8 Erweiterte Beacon-Parameter

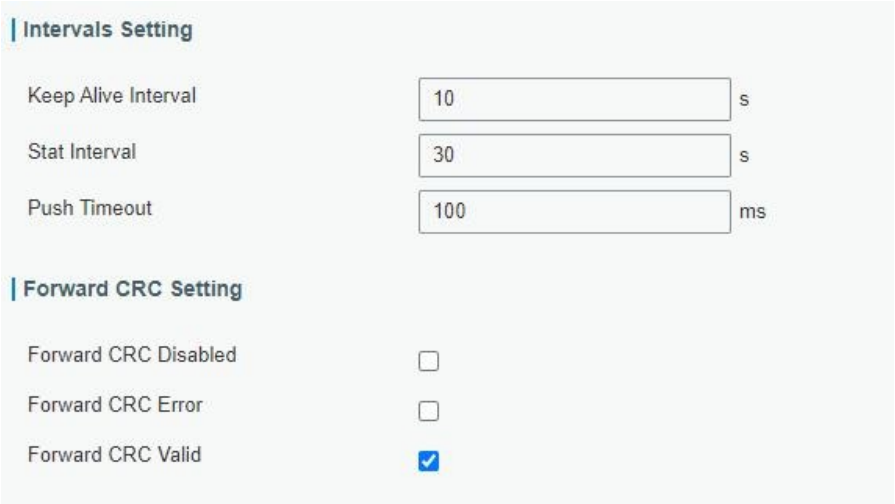


Abbildung 3-2-1-9

Element	Beschreibung	Standard
Keep-Alive-Intervall	Geben Sie das Intervall für Keepalive-Pakete ein, die vom Gateway an den Netzwerkserver gesendet werden, um die Verbindung stabil und aktiv zu halten. Bereich: 1–3600.	10
Stat-Intervall	Geben Sie das Intervall ein, in dem der Netzwerkserver mit Gateway-Statistiken aktualisiert wird. Bereich: 1–3600.	30
Push-Timeout	Geben Sie das Zeitlimit ein, nach dem auf die Antwort vom Server gewartet wird, nachdem das Gateway Daten des Knotens gesendet hat. Bereich: 1–1999.	10
CRC weiterleiten Deaktiviert	Aktivieren Sie diese Option, um Pakete, die mit deaktiviertem CRC empfangen wurden, an der Netzwerkserver.	Deaktiviert
Vorwärts-CRC Fehler	Aktivieren, um Pakete, die mit CRC-Fehlern empfangen wurden, an den Netzwerkserver zu senden.	Deaktiviert
CRC weiterleiten Gültig	Aktivieren, um Pakete, die mit gültigem CRC empfangen wurden, an den Netzwerkserver zu senden.	Aktiviert

Tabelle 3-2-1-9 Erweiterte Parameter

Abbildung 3-2-1-10

Element	Beschreibung	Standard
Aktivieren	Aktivieren oder deaktivieren Sie die LBT-Funktion. Listen before talk (LBT) wird wird verwendet, um zu erkennen, ob der Downlink-Kanal frei ist, und	Deaktiviert

	Vermeidung von Kanalzugriffskonflikten. Hinweis: AU915 und US915 unterstützen die LBT-Funktion nicht.	
RSSI-Ziel	Geben Sie die Kriterien für einen inaktiven Kanal ein. Wenn der tatsächliche RSSI-Wert eines Kanals unter dem Kriterium/Zielwert liegt, wird der Kanal als frei betrachtet. Bereich: -120 bis 0	-80

Tabelle 3-2-1-10 Erweiterte LBT-Parameter

3.2.1.5 Benutzerdefiniert

Wenn der benutzerdefinierte Konfigurationsmodus aktiviert ist, können Sie Ihre eigene Konfigurationsdatei für den Paketweiterleiter in das Bearbeitungsfeld schreiben, um den Paketweiterleiter zu konfigurieren. Klicken Sie auf „Speichern“, um den Inhalt Ihrer benutzerdefinierten Konfigurationsdatei zu speichern, und klicken Sie auf „Übernehmen“, um die Änderungen zu übernehmen. Sie können auf „Löschen“ klicken, um den gesamten Inhalt des Bearbeitungsfeldes zu löschen. Wenn Sie nicht wissen, wie Sie eine Konfigurationsdatei schreiben, klicken Sie bitte auf „Beispiel“, um zur Referenzseite zu gelangen.

Hinweis: Die benutzerdefinierte Konfiguration überschreibt die Paketweiterleitungskonfigurationen der Web-GUI.

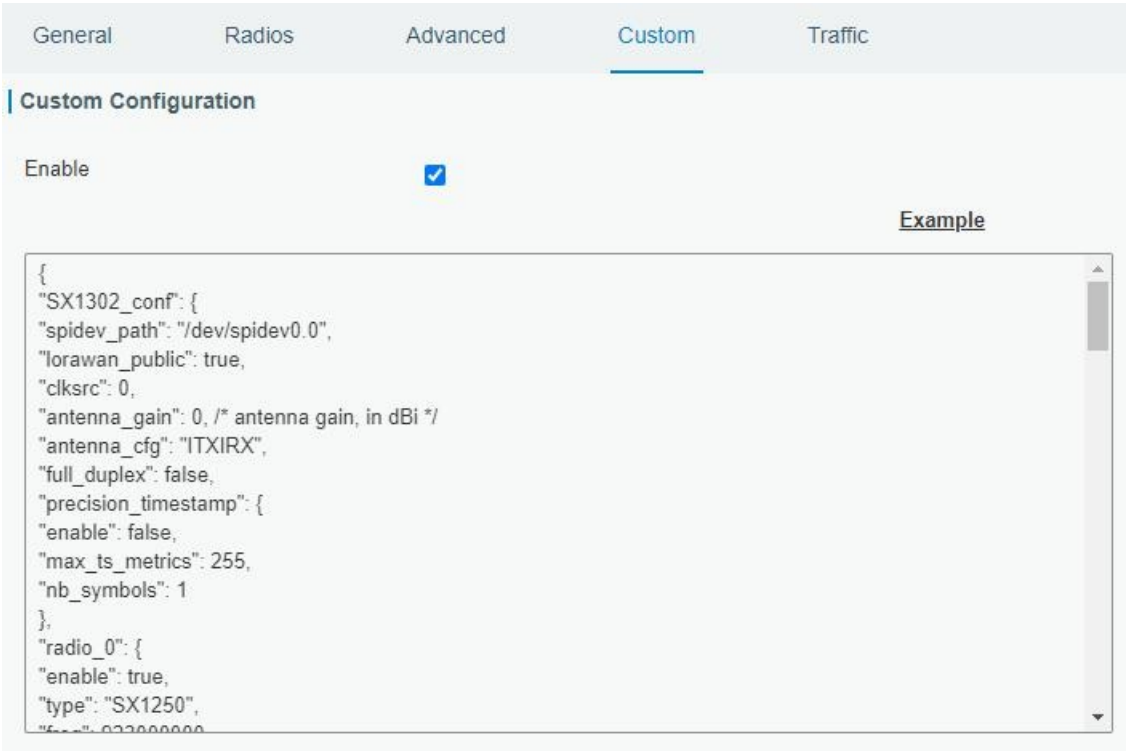


Abbildung 3-2-1-11

3.2.1.6 Datenverkehr

Wenn Sie zur Verkehrsseite navigieren, werden alle aktuellen Verkehrsdaten angezeigt, die vom Gateway empfangen wurden. Um den Live-Verkehr zu verfolgen, klicken Sie auf **„Aktualisieren“**.

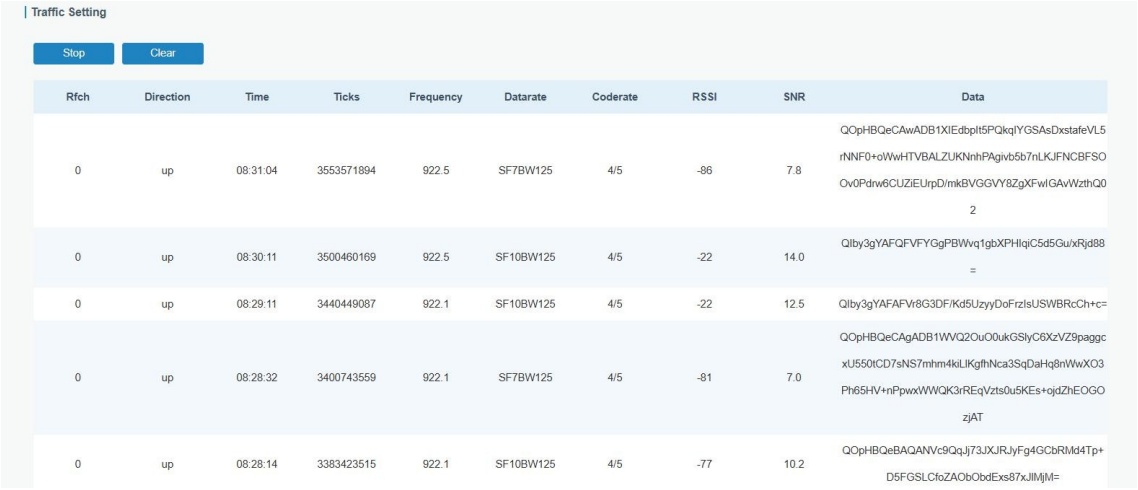


Abbildung 3-2-1-12

Element	Beschreibung
Aktualisieren	Klicken Sie hier, um die neuesten Daten abzurufen.
Löschen	Klicken Sie hier, um alle Daten zu löschen.
Rfch	Zeigt den Kanal dieses Pakets an.
Richtung	Zeigt die Richtung dieses Pakets an.
Zeit	Zeigt die Empfangszeit dieses Pakets an.
Ticks	Zeigt die Ticks dieses Pakets an.
Frequenz	Zeigt die Frequenz des Kanals an.
Datenrate	Zeige die Datenrate des Kanals an.
Codierrate	Zeigt die Codierrate dieses Pakets an.
RSSI	Zeigt die empfangene Signalstärke an.
SNR	Zeigt das Signal-Rausch-Verhältnis dieses Pakets an.
Daten	Zeigt die Nutzlast (base64) dieses Pakets an. **Hinweis**: Dies funktioniert nicht mit Loriot- und Actility-Paketweiterleitern.

Tabelle 3-2-1-11 Verkehrsparameter

3.2.2 Netzwerkserver

3.2.2.1 Allgemein

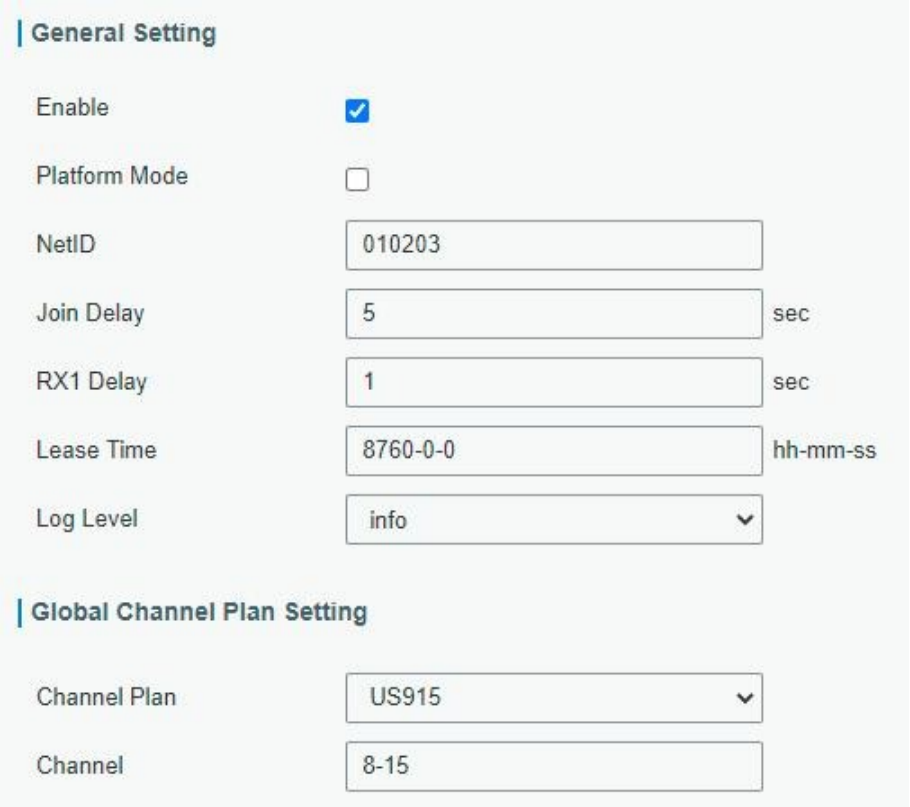


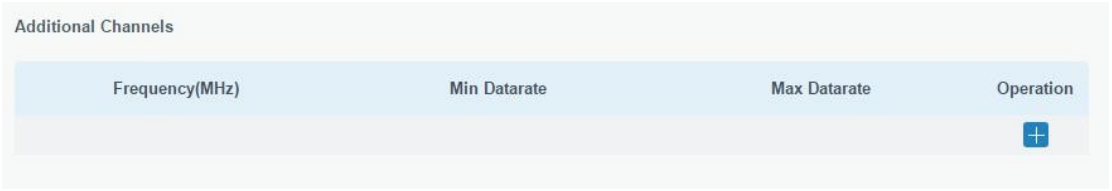
Abbildung 3-2-2-1

Element	Beschreibung	Standard
Allgemeine Einstellung		
Aktivieren	Klicken Sie hier, um den Netzwerkservermodus zu aktivieren.	Aktiv
Plattformmodus	Aktiviert, um Gateway mit Milesight IoT oder die Yeastar Workplace-Plattform.	Deaktiviert
NetID	Geben Sie die Netzwerkkennung ein.	010203
Verzögerung beim Beitritt	Geben Sie das Zeitintervall zwischen dem Senden einer Join_request_message durch das Endgerät an den Netzwerkserver und dem Vorbereiten des Endgeräts zum Öffnen von RX1 zum Empfangen der Join_accept_message vom Netzwerkserver gesendet wird.	5
RX1-Verzögerung	Geben Sie die Zeitspanne zwischen dem Zeitpunkt ein, zu dem das Endgerät Uplink-Pakete sendet und dem Zeitpunkt, zu dem das Endgerät sich darauf vorbereitet, RX1 zu öffnen, um das Downlink-Paket zu empfangen.	1
Lease-Zeit	Geben Sie die Zeitdauer ein, nach der eine erfolgreiche Verbindung abläuft. Das Format lautet Stunden-Minuten-Sekunden. Wenn der Verbindungstyp OTAA ist, müssen die Endgeräte erneut eine Verbindung zum Netzwerkserver herstellen, wenn die die Lease-Zeit überschritten ist.	876000-00-00
Protokollstufe	Wählen Sie die Protokollstufe aus.	Info
Einstellung des Kanalplans		
Kanalplan	Wählen Sie den LoRaWAN®-Kanalplan, der für die	Abhängig von den

	Upstream- und Downlink-Frequenzen und Datenraten. Die verfügbaren Kanalpläne hängen vom Modell des Gateways ab.	Frequenz des Gateways
Kanal	Ermöglicht Endgeräten die Kommunikation mit bestimmten Frequenzkanälen. Leer lassen bedeutet, dass alle im LoRaWAN®-Dokument zu regionalen Parametern angegebenen standardmäßigen nutzbaren Kanäle verwendet werden. Hier kann der Index der Kanäle eingegeben werden. **Beispiele:** 1, 40: Aktivierung von Kanal 1 und Kanal 40 1-40: Aktivierung von Kanal 1 bis Kanal 40 1-40, 60: Aktivierung von Kanal 1 bis Kanal 40 und Kanal 60	Abhängig von der Frequenz des Gateways

Tabelle 3-2-2-1 Allgemeine Parameter

Hinweis: Bei einigen regionalen Varianten können Sie, sofern dies von Ihrer LoRaWAN®-Region zugelassen wird, den Zusatzplan verwenden, um zusätzliche Kanäle zu konfigurieren, die nicht in den LoRaWAN®-Regionalparametern definiert sind, wie z. B. EU868 und KR920, wie in der folgenden Abbildung



dargestellt:

Abbildung 3-2-2-2

Zusätzliche Kanäle		
Element	**Beschreibung**	**Standard**
Frequenz/MHz	Geben Sie die Frequenz des zusätzlichen Plans ein.	Null.
Max. Datenrate	Geben Sie die maximale Datenrate für das Endgerät ein. Der Bereich basiert auf den Angaben in den regionalen LoRaWAN®-Parametern .	DR0(SF12,125 kHz)
Minimale Datenrate	Geben Sie die minimale Datenrate für das Endgerät ein. Der Bereich basiert auf den Angaben im Dokument „ LoRaWAN® regional parameters“ Dokument.	DR3(SF9,125kHz)

Tabelle 3-2-2-2 Zusätzliche Planparameter

3.2.2.2 Anwendung

Eine Anwendung ist eine Sammlung von Geräten mit demselben Zweck/desselben Typs. Benutzer können eine Reihe von Geräten zu derselben Anwendung hinzufügen, die an denselben Server senden müssen.

Sie können die Anwendung bearbeiten, indem Sie auf „ “ (Anwendung bearbeiten) klicken, oder eine neue Anwendung erstellen, indem Sie auf „ “ (Neue Anwendung erstellen) klicken.

Abbildung 3-2-2-3

Anwendung	
Element	**Beschreibung**
Name	Geben Sie den Namen des Anwendungsprofils ein. Z. B. „smoker-sensor-app”.
Beschreibung	Geben Sie die Beschreibung dieser Anwendung ein. Z. B. eine Anwendung für einen Rauchmelder.
Metadaten	Aktivieren Sie diese Option, um die Details auszuwählen, die mit Uplink-Paketen , wenn das Gerät den Payload-Codec hinzufügt.
Datenübertragung	Die Daten werden über das MQTT-HTTP- oder HTTPS-Protokoll an Ihren benutzerdefinierten Server gesendet. Eine Anwendung kann nur einen MQTT hinzufügen. Übertragung und eine HTTP-Übertragung (HTTPS).

Tabelle 3-2-2-3 Anwendungsparameter

MQTT-Integration

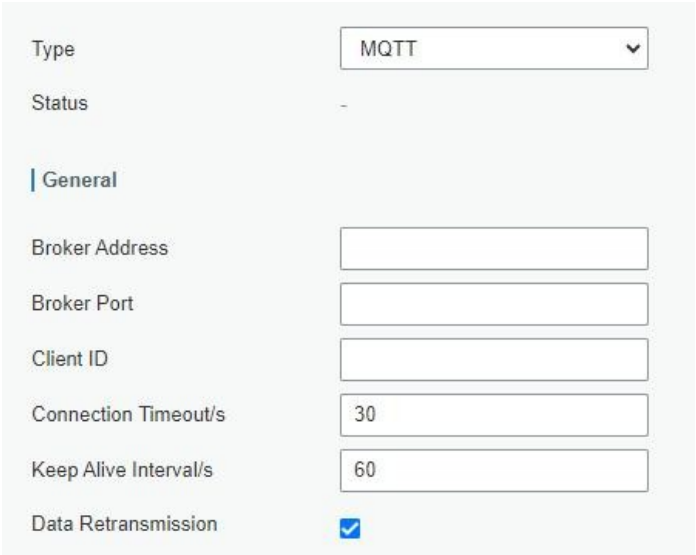


Abbildung 3-2-2-4

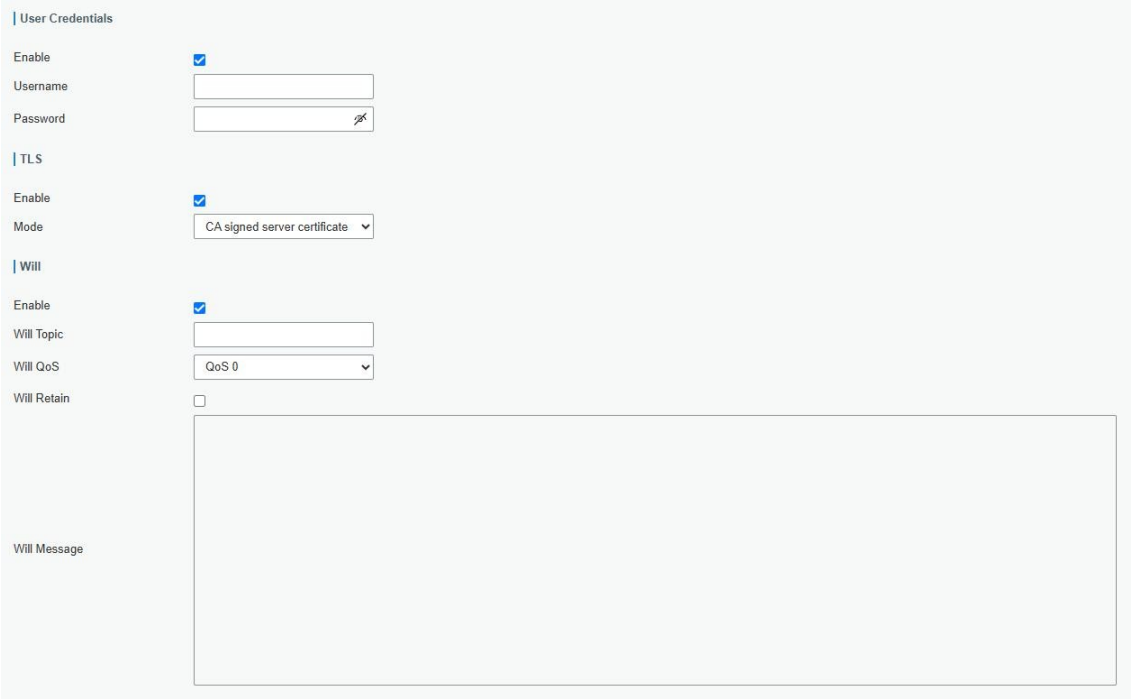


Abbildung 3-2-2-5

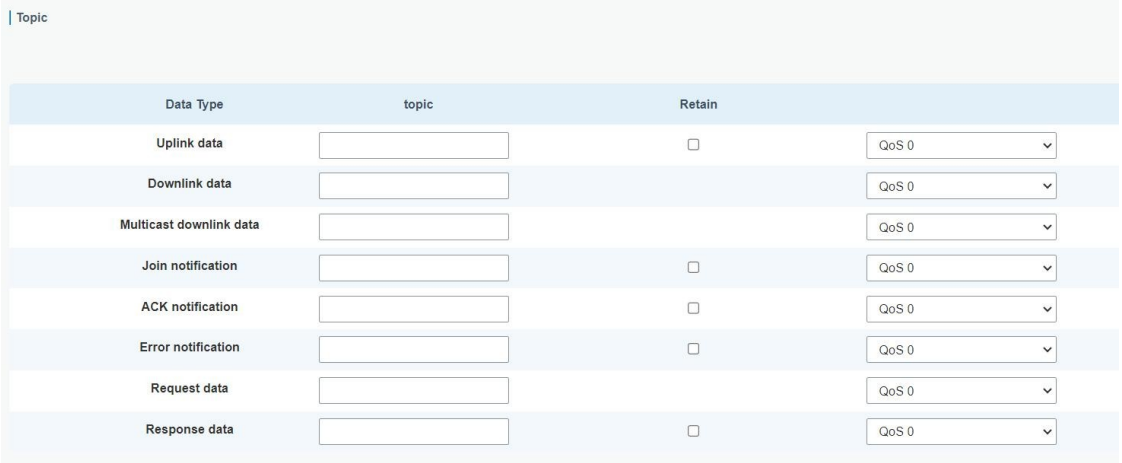


Abbildung 3-2-2-6

MQTT-Einstellungen	
Element	**Beschreibung**
Allgemein	
Broker Adresse	MQTT-Broker-Adresse zum Empfang von Daten.
Broker-Port	MQTT-Broker-Port zum Empfang von Daten.
Client-ID	Die Client-ID ist die eindeutige Identität des Clients gegenüber dem Server. Es muss eindeutig sein, wenn alle Clients mit demselben Server verbunden sind, und es ist der Schlüssel zur Verarbeitung von Nachrichten mit QoS 1 und 2.
Verbindung Zeitüberschreitung/s	Wenn der Client nach Ablauf des Verbindungszeitlimits keine Antwort erhält, Verbindung als unterbrochen betrachtet. Der Bereich: 1-65535
Keep Alive Intervall/s	Nachdem der Client mit dem Server verbunden ist, sendet der Client einen Heartbeat. Paket regelmäßig an den Server senden, um die Verbindung aufrechtzuerhalten. Bereich: 1-65535

Datenwiederholungsratession	Nach der Aktivierung unterstützt es die Datenspeicherung von bis zu 10.000 Datenelementen, wenn die Netzwerkverbindung unterbrochen wird, und überträgt die Daten nach der Wiederherstellung der Netzwerkverbindung erneut übertragen.
Benutzeranmeldedaten	
Aktivieren	Benutzeranmeldedaten aktivieren.
Benutzername	Der Benutzername, der für die Verbindung mit dem MQTT-Broker verwendet wird.
Passwort	Das Passwort, das für die Verbindung mit dem MQTT-Broker verwendet wird.
TLS	
Aktivieren	Aktivieren Sie die TLS-Verschlüsselung in der MQTT-Kommunikation. Hinweis: Wenn der MQTT-Broker vom Typ HiveMQ ist, aktivieren Sie bitte **TLS** und legen Sie die Option als **CA-signiertes Serverzertifikat** fest.
Modus	Wählen Sie zwischen „Selbstsignierte Zertifikate“ und „CA-signiertes Serverzertifikat“. **CA-signiertes Serverzertifikat:** Überprüfen Sie dies mit dem Zertifikat, das von der Zertifizierungsstelle (CA) ausgestellt und auf dem Gerät vorinstalliert ist. **Selbstsignierte Zertifikate:** Laden Sie die benutzerdefinierten CA-Zertifikate (.crt oder .pem), Client-Zertifikate (.crt) und den geheimen Schlüssel (.key) zur Überprüfung hoch.
Wird	
Aktivieren	Die Last-Will-Nachricht wird automatisch gesendet, wenn die Verbindung zum MQTT-Client abnormal getrennt wird. Sie wird in der Regel verwendet, um Geräte-Statusinformationen zu senden oder andere Geräte oder Proxy-Server über den Offline-Status zu informieren.
Will Topic	Passen Sie das Thema an, um Last-Will-Nachrichten zu empfangen.
Will QoS	QoS0, QoS1 oder QoS2 sind optional.
Will Retain	Aktivieren Sie diese Option, um die letzte Willensnachricht als beibehaltene Nachricht festzulegen.
Will Nachricht	Passen Sie den Inhalt der letzten Willensnachricht an.
Thema	
Datentyp	Datentyp für die Kommunikation mit dem MQTT-Broker: **Uplink-Daten:** Empfang von Uplink-Paketen des Geräts. **Downlink-Daten:** Senden von Downlink-Befehlen an Geräte. Wenn Sie einen Downlink-Befehl an ein einzelnes Gerät senden möchten, fügen Sie bitte den Platzhalter „$deveui“ zu diesem Thema hinzu und ersetzen Sie diesen beim Abonnieren dieses Themas durch die tatsächliche EUI des Geräts. **Multicast-Downlink-Daten:** Senden von Downlink-Befehlen an eine Multicast-Gruppe **Beitrittsbenachrichtigung:** Empfangen von Beitrittsbenachrichtigungen, wenn das Gateway Beitrittsakzeptanzpakete sendet, um den Geräten den Beitritt zum Netzwerk zu ermöglichen. **ACK-Benachrichtigung:** Empfang von ACK-Paketen von Geräten beim Senden von Downlink-Befehlen. **Fehlerbenachrichtigung:** Empfang von Fehlerpaketen von Geräten. **Anforderungsdaten:** Senden von Anfragen zur Abfrage und Konfiguration des Gateway-NS. **Antwortdaten:** Empfang der Antworten auf die Anfragen.
Thema	Themenname des für die Veröffentlichung verwendeten Datentyps.
Beibehalten	Aktivieren Sie diese Option, um die neueste Nachricht dieses Themas als Retain-Nachricht festzulegen.
QoS	QoS 0 – Nur einmal

	Dies ist die schnellste Methode und erfordert nur eine Nachricht. Es ist auch der unzuverlässigste Übertragungsmodus. QoS 1 – Mindestens einmal Diese Stufe garantiert, dass die Nachricht mindestens einmal zugestellt wird, jedoch möglicherweise mehr als einmal. QoS 2 – Genau einmal QoS 2 ist die höchste Servicestufe in MQTT. Diese Stufe garantiert, dass jede Nachricht nur einmal von den vorgesehenen Empfängern empfangen wird. QoS 2 ist die sicherste und langsamste Servicestufe.

Tabelle 3-2-2-4 MQTT-Einstellungsparameter

HTTP/HTTPS-Integration

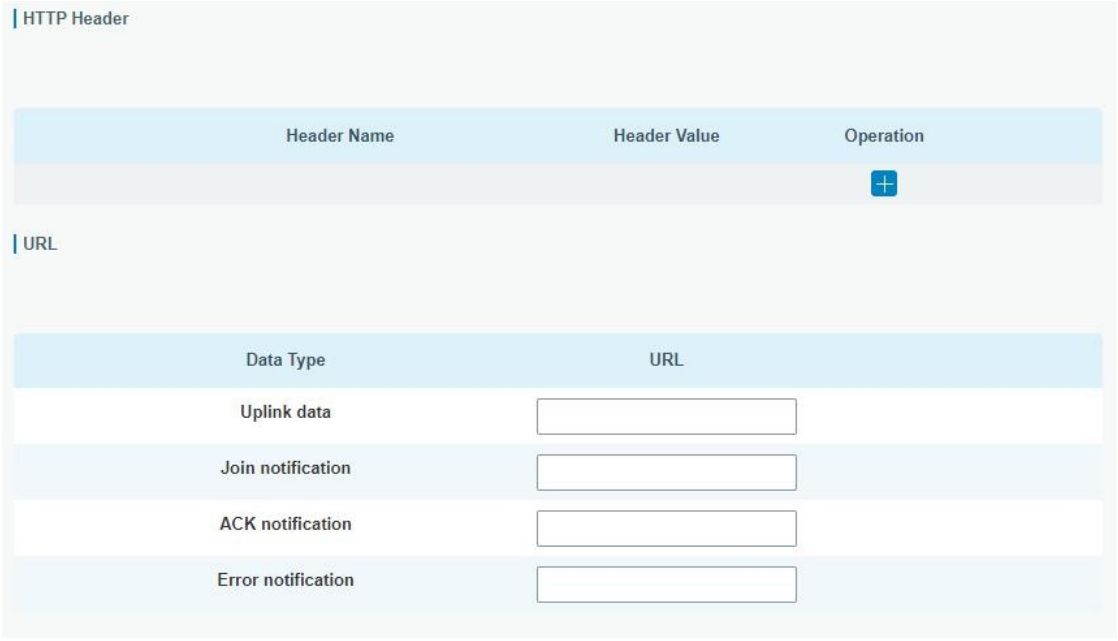


Abbildung 3-2-2-7

HTTP/HTTPS-Einstellungen	
Element	**Beschreibung**
HTTP-Header	
Header-Name	Eine Reihe von Kernfeldern im HTTP-Header.
Header-Wert	Wert des HTTP-Headers.
URL	
Datentyp	An den HTTP/HTTPS-Server gesendeter Datentyp. **Uplink-Daten:** Empfang von Uplink-Paketen des Geräts **Join-Benachrichtigung:** Empfang von Join-Benachrichtigungen, wenn das Gateway Join-Accept-Pakete sendet, um den Geräten den Beitritt zum Netzwerk zu ermöglichen **ACK-Benachrichtigung:** Empfang von ACK-Paketen von Geräten beim Senden von Downlink-Befehlen **Fehlerbenachrichtigung:** Empfang von Fehlerpaketen von Geräten

Thema	Themenname des für die Veröffentlichung verwendeten Datentyps.
URL	HTTP/HTTPS-Server-URL zum Empfangen von Daten.

Tabelle 3-2-2-5 HTTP/HTTPS-Einstellungsparameter

Beispiel für eine zugehörige Konfiguration

Anwendungskonfiguration

3.2.2.3 Nutzlast-Codec

Der Payload-Codec stellt die integrierte Payload-Codec-Bibliothek von Milesight LoRaWAN®-Geräten zur Verfügung, um die Daten einfach zu decodieren und zu codieren. Benutzer können auch den Payload-Codec von Geräten anderer Marken anpassen oder die Uplink- und Downlink-Inhalte nach Bedarf anpassen.

Integrierte Payload-Codec-Bibliothek

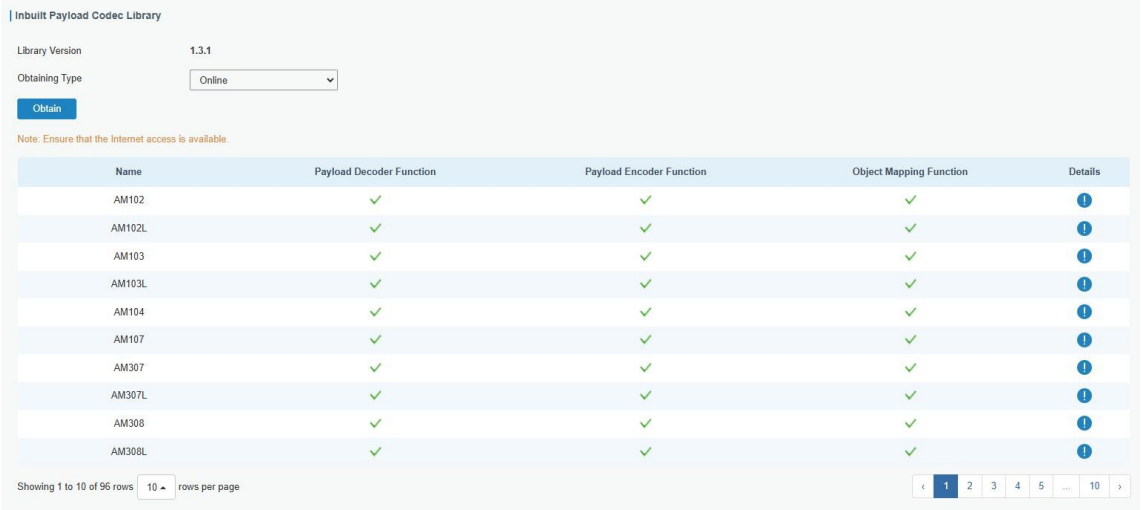


Abbildung 3-2-2-8

Integrierte Payload-Codec-Bibliothek	
Element	**Beschreibung**
Bibliotheksversion	Zeigen Sie die Version der Milesight-Geräte-Payload-Codec-Bibliothek an.
Typ abrufen	Wählen Sie den Typ aus, um die Payload-Codec-Bibliothek der Milesight-Geräte zu aktualisieren. **Online:** Automatische Aktualisierung, wenn das Gateway bei jedem Einschalten und beim Zugriff auf das Internet eine Versionsaktualisierung feststellt. Benutzer können auch auf die Schaltfläche **„Abrufen“** klicken, um den Aktualisierungsstatus manuell zu überprüfen. **Lokales Hochladen:** Klicken Sie auf **„Durchsuchen“**, um das Payload-Codec-Paket im ZIP-Format hochzuladen, und klicken Sie auf **„Importieren“**, um die Bibliothek zu aktualisieren. Für Milesight-Payload Codec-Paket, bitte hier herunterladen.
Name	Zeigen Sie das entsprechende Milesight-Produktmodell der Nutzlast an. Codec.
Nutzlast-Decoder Funktion	Zeigt an, ob Decoder vorhanden sind.

Nutzlast-Encoder Funktion	Zeigt an, ob Encoder vorhanden sind.
Objektzuordnung Funktion	Zeigt an, ob Objektzuordnungsfunktionen vorhanden sind.
Details	Zeigen Sie die Details des Decoders und Encoders an. Wenn dies nicht Ihren Anforderungen entspricht, passen Sie bitte Ihren Payload-Codec an.

Tabelle 3-2-2-6 Parameter der integrierten Payload-Codec-Bibliothek

Benutzerdefinierter Payload-Codec

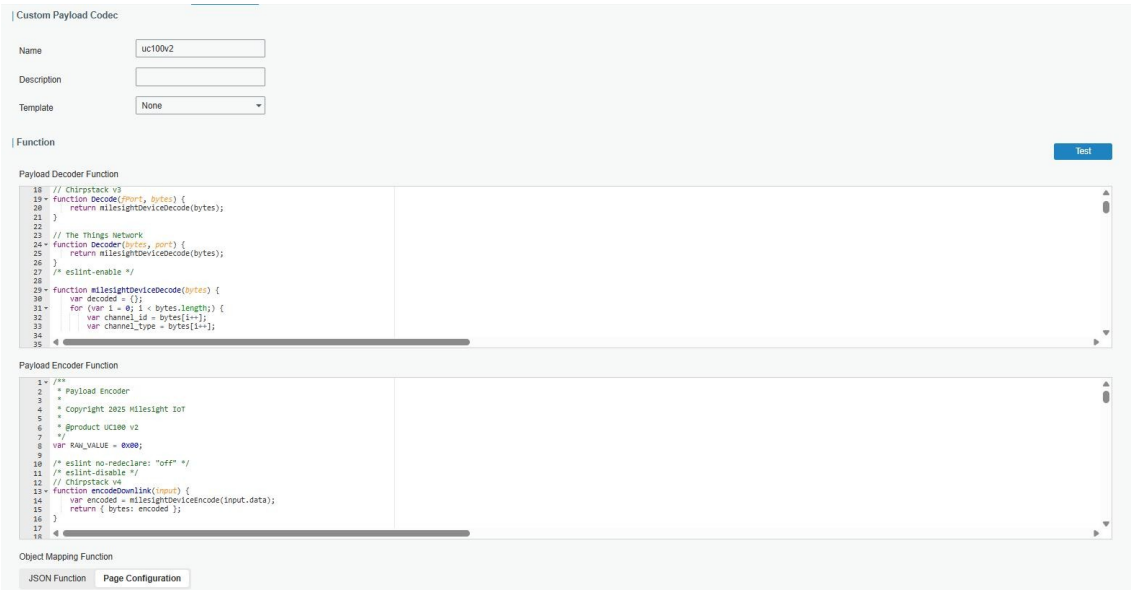


Abbildung 3-2-2-9

Benutzerdefinierter Payload-Codec	
Element	**Beschreibung**
Name	Geben Sie den eindeutigen Namen des benutzerdefinierten Payload-Codecs ein.
Beschreibung	Geben Sie die Beschreibung dieses Payload-Codecs ein.
Vorlage	Wählen Sie einen vorhandenen integrierten Payload-Codec als Vorlage aus.
Payload-Decoder-Funktion	Passen Sie den Payload-Decoder des Geräts an, um Daten im Hexadezimalformat in das JSON-Format zu konvertieren. Beachten Sie, dass der Funktionsheader derselbe sein sollte wie im Beispiel auf den Feldern sein sollte.
Nutzlast-Encoder-Funktion	Passen Sie den Payload-Encoder des Geräts an, um Daten im JSON-Format zu konvertieren. Befehl zum Konvertieren von Nachrichten in das Hexadezimalformat. Beachten Sie, dass der Funktionsheader mit dem Beispiel in den Leerzeichen übereinstimmen sollte.
Objekt-Zuordnungsfunktion	Passen Sie die Mapping-Funktion an, um LoRaWAN®-Nachrichten in BACnet- oder Modbus-Objekte zu konvertieren. Es stehen zwei Hinzufügungsmethoden zur Verfügung: **JSON-Funktion**: Fügen Sie die Funktion im JSON-Format hinzu. **Seitenkonfiguration**: Fügen Sie die Funktion über die Seite hinzu.
Test	Aktivieren oder deaktivieren Sie den Payload-Codec-Test. **Eingabe**: Geben Sie die Rohdaten im Hex-Format ohne Leerzeichen oder als JSON ein.

	Formatierungsbefehl. **fPort**: Anwendungsport von LoRaWAN®-Geräten. Bei Milesight-Geräten ist der Standardwert 85. **Decodertest**: Konvertiert Rohdaten im Hexadezimalformat in Ergebnisse im JSON-Format. **Encodertest**: Konvertiert Befehle im JSON-Format in Befehle im Hexadezimalformat. **Decoder-/Encoder-Testergebnis**: Zeigt das decodierte oder codierte Ergebnis an. **Ergebnis des Objektzuordnungstests**: Überprüfen Sie die Objektgültigkeit im Encoder oder Decoder.

Tabelle 3-2-2-7 Benutzerdefinierte Payload-Codec-Parameter

Hinweis:

1. Die unterstützte JavaScript-Version des Payload-Decoders und -Encoders ist ES2020.
2. Die in Decodern und Encodern eines Payload-Codecs verwendeten Variablennamen müssen identisch sein, wenn sie auf dieselben Elemente verweisen.

Objektzuordnungsfunktion – JSON-Funktionsbeispiel:

```
{
  „object ": [
    {
      „id ": „ipso_version ", „name ":
      „IPSO-Version ", „value ": „ ",
      „unit ": „ ",
      „access_mode ": „R ",
      „Datentyp ": „TEXT ",
      „Werttyp ": „STRING ",
      „Maximale Länge ": 6,
      „bacnet_type ": „character_string_value_object ",
      „bacnet_unit_type_id ": 95,
      „bacnet_unit_type ": „UNITS_NO_UNITS "
    },
      {
      „id ": „temperature_unit ", „name ":
      „Temperatureinheit ", „value ": „ ",
      „unit ": „ ",
      „access_mode ": „RW ",
      „datentyp ": „ENUM ",
      „wertetyp ": „UINT8 ",
```

```
        „Werte“: [
            { „Wert“: 0, „Name“: „Celsius“ },
            { „Wert“: 1, „Name“: „Fahrenheit“ }
        ],
        „bacnet_type“: „multistate_value_object“,
        „bacnet_unit_type_id“: 95, „bacnet_unit_type“:
        „UNITS_NO_UNITS“,
        „reference“: [„temperature_control_mode“, „temperature_target“]
    }
    ]
}
```

Objektzuordnungsfunktion – JSON-Konfiguration

Element	Beschreibung
id	Dieser Wert muss mit den Variablennamen der Decoder und Codern übereinstimmen.
name	Lassen Sie das Feld leer oder passen Sie den Inhalt nach Bedarf an.
Wert	Nicht verwendet. Leer lassen.
Einheit	Leer lassen oder Einheit nach Bedarf eingeben.
Zugriffsmodus	Legen Sie den Zugriffsmodus dieses Objekts fest. Unterstützte Optionen und entsprechende Modbus-Registertypen:
datentyp	Definieren Sie den Wertetyp dieser Variablen. Unterstützte Optionen:
value_type	Unterstützte Optionen: UINT8, INT8, UINT16, INT16, UINT32, INT32, FLOAT, STRING.

Zugriffsmodus:

Option	Beschreibung	Modbus-Registertyp
R	Nur Lesen	Diskreter Eingang, Eingangsregister
W	Nur-Schreiben	Spule, Halte-Register
RW	Lesen/Schreiben	Spule, Halteregister

datentyp:

Option	Beschreibung	Modbus-Registertyp
TEXT	Zeichenkettendaten, Beispiel: Seriennummer	Eingangsregister, Halteregister
NUMBER	Zahldaten, einschließlich Ganzzahlen und Gleitkommazahlen, Beispiel: Temperatur	Eingangsregister, Halte-Register
BOOL	Nur Status 0 und 1, Beispiel: Status der Taste	Diskreter Eingang, Spule
ENUM	Mehrere Werte	Eingangsregister, Halteregister

Hinweis: Wenn der Datentyp ENUM ist und der Referenzparameter nicht leer ist, wird empfohlen, den Modbus-Registertyp als Eingangsregister oder Halteregister festzulegen.

Werte	Legen Sie den Wertebereich dieser Variablen fest.
max_length	Wenn der Wertetyp STRING ist, legen Sie die maximale Länge der Zeichenfolgen oder maximale Länge der Modbus-Register fest.
bacnet_type	Unterstützte Optionen: analog_value_object, analog_input_object, analog_output_object, binary_value_object, binary_input_object, binary_output_object, multistate_value_object, multistate_input_object, multistate_output_object
bacnet_unit_type_id	Geben Sie die BACnet-Geräte-ID ein, die Sie hier finden.
bacnet_unit_type	Geben Sie den BACnet-Gerätetyp ein, den Sie hier finden (siehe Beschreibung).
reference	Wenn diese Variable zusammen mit anderen Variablen geschrieben werden soll, fügen Sie hier das Variablen-Array hier hinzu.

Tabelle 3-2-2-8 Objektzuordnungsfunktion – JSON-Funktionsparameter

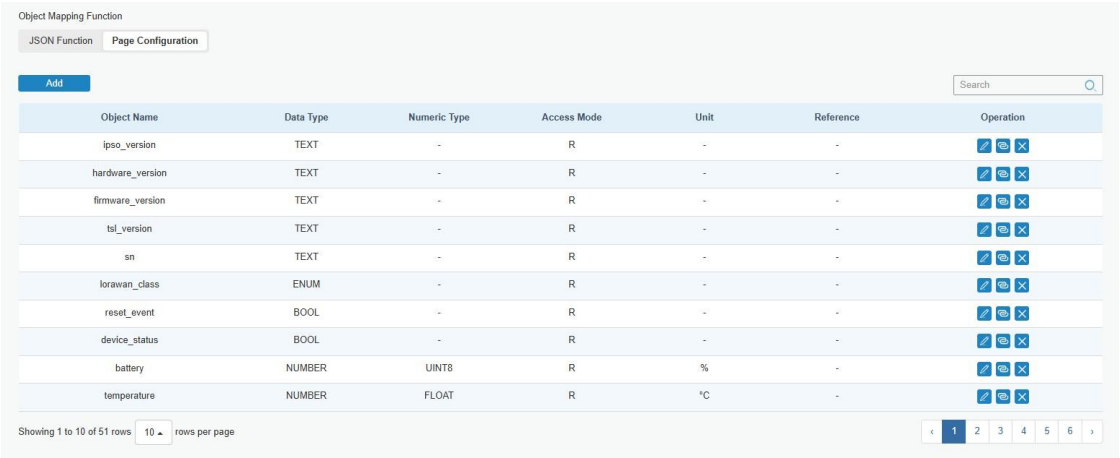


Abbildung 3-2-2-10

Objektzuordnungsfunktion – Seitenkonfiguration	
Element	**Beschreibung**
Hinzufügen	Neues Objekt hinzufügen.
Objektname	Zeigt den Objektnamen an.
Datentyp	Zeigt den Datentyp dieses Objekts an.
Numerischer Typ	Zeigt den numerischen Typ an, wenn der Datentyp NUMBER ist.
Zugriffsmodus	Zeigt den Zugriffsmodus dieses Objekts an.
Einheit	Zeigt die Einheit dieses Objekts an.
Referenz	Zeigt die zugehörigen Objekte dieses Objekts an.
Operation	: Bearbeiten Sie das Objekt. : Verknüpfen Sie dieses Objekt mit anderen Objekten. Nach der Verknüpfung sollten diese Objekte zusammen geschrieben werden. : Löschen Sie das Objekt.

Tabelle 3-2-2-9 Objektzuordnungsfunktion – Seitenkonfigurationsparameter

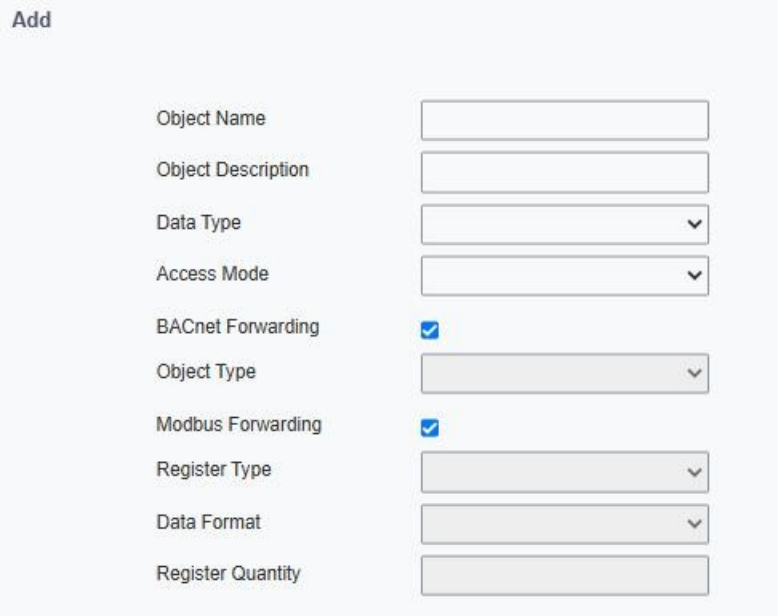


Abbildung 3-2-2-11

Objektzuordnungsfunktion – Objekt hinzufügen	
Element	**Beschreibung**
Objektname	Der Name muss mit dem Variablennamen des Decoders oder Encoders übereinstimmen.
Objekt Beschreibung	Die Beschreibung des Objekts.
Datentyp	Der Datentyp dieses Objekts.
Wert 0/1	Wenn der Datentyp BOOL ist, legen Sie den Wert auf 0 und 1 fest.
Aufzählung Zahl	Wenn der Datentyp ENUM ist,legen Sie die unterstützte Optionsmenge fest.
Numerischer Typ	Wenn der Datentyp numerisch ist, legen Sie den Zahlentyp fest.
Einheit	Wenn der Datentyp NUMBER ist,legen Sie die Einheit des Objekts fest.
Maximal Länge	Wenn der Datentyp TEXT ist, legen Sie die maximale Länge des Textes fest.
Zugriffsmodus	Der Zugriffsmodus dieses Objekts.
BACnet Weiterleitung	Aktivieren Sie diese Option, um die Details der BACnet-Objektparameter anzuzeigen. Diese Parameter werden automatisch entsprechend dem Datentyp und dem Zugriffsmodus eingegeben.
Modbus-Weiterleitung	Aktivieren Sie diese Option, um die Details der Modbus-Objektparameter anzuzeigen. Diese Parameter werden automatisch entsprechend dem Datentyp und dem Zugriffsmodus automatisch eingegeben.

Tabelle 3-2-2-10 Objektzuordnungsfunktion – Objektparameter hinzufügen

3.2.2.4 Profile

Ein Profil definiert die Gerätefunktionen und Boot-Parameter, die der Netzwerkserver für die Einrichtung des LoRaWAN®-Funkzugangsdienstes benötigt. Diese Informationen müssen vom Hersteller des Endgeräts bereitgestellt werden. UG67 verfügt über 8 vorkonfigurierte Gerätedateien und

Benutzer können auch ein neues Geräteprofil erstellen.

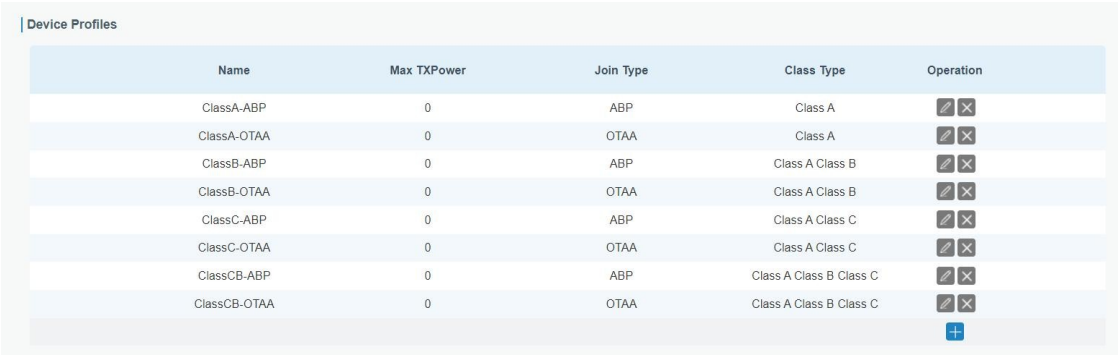


Abbildung 3-2-2-12

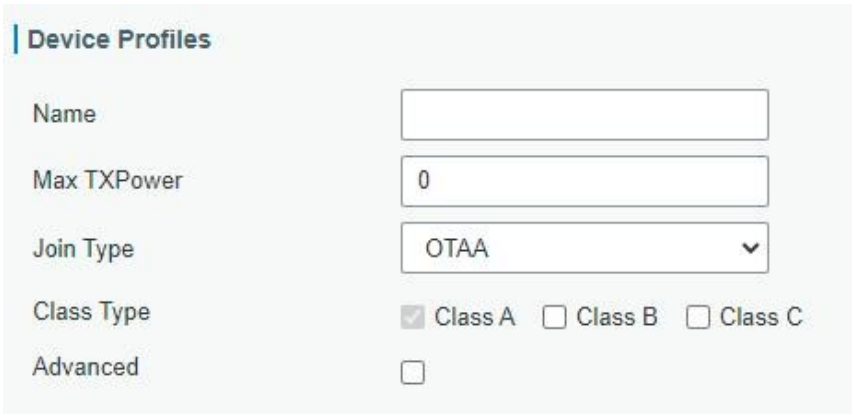


Abbildung 3-2-2-13

Geräteprofileinstellungen	
Element	**Beschreibung**
Name	Geben Sie den Namen des Geräteprofils ein.
Max. Sendeleistung	Geben Sie die maximale Sendeleistung ein. Die TXPower gibt die Leistungsstufen relativ zum maximalen EIRP-Pegel des Endgeräts an. 0 bedeutet, dass die maximale EIRP verwendet wird. EIRP bezieht sich auf die äquivalente isotrope Strahlungsleistung.
Verbindungstyp	Wählen Sie zwischen „OTAA“ und „ABP“.
Klassentyp	Klasse A ist standardmäßig aktiviert. Benutzer können das Kontrollkästchen für Klasse B oder Klasse C aktivieren, um den Klassentyp hinzuzufügen. Hinweis: Der Beacon-Zeitraum sollte in **„Packet Forwarder > Advanced** auf einen Wert ungleich Null gesetzt werden.

Tabelle 3-2-2-11 Einstellparameter für Geräteprofile

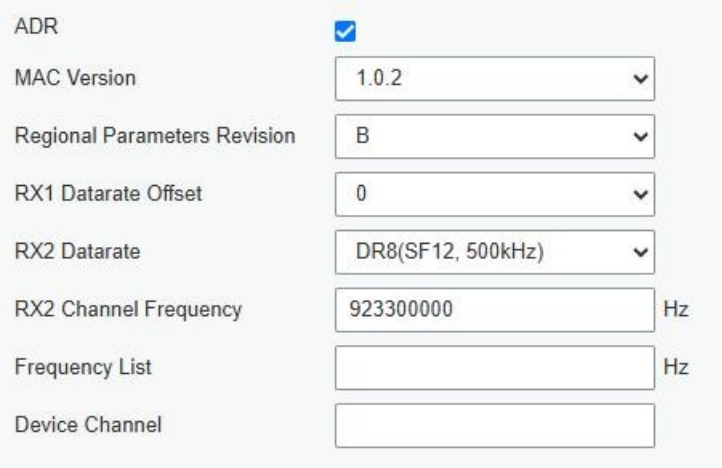


Abbildung 3-2-2-14

Erweiterte Einstellungen für Geräteprofile		
Element	**Beschreibung**	**Standard**
ADR	Aktivieren oder deaktivieren Sie den Gateway-Netzwerkserver, um die Datenrate der Endgeräte anzupassen.	Aktivieren
MAC-Version	Wählen Sie die vom Endgerät unterstützte Version von LoRaWAN® vom Endgerät unterstützte Version von LoRaWAN(®)	1.0.2
Regionaler Parameter Revision	Revision des vom Endgerät unterstützten Dokuments „Regionale Parameter".	B
RX1 Datenrate Offset	Der Offset, der zur Berechnung der RX1 Datenrate verwendet wird, basierend auf der Uplink-Datenrate.	Basierend auf den Angaben in den regionalen LoRaWAN®-Parametern Dokument
RX2-Datenrate	Geben Sie die RX2-Datenrate ein, die für das RX2 Empfangsfenster verwendet wird.	
RX2-Kanal Frequenz	RX2-Kanalfrequenz, die für das RX2 Empfangsfenster verwendet wird.	
Frequenzliste	Liste der werkseitig voreingestellten Frequenzen. Der Bereich basiert auf den Angaben im LoRaWAN® .	Null
Gerätekanal	Ändern Sie diesen Gerätefrequenzkanal, indem Sie die Kanalindizes eingeben. Nach der Konfiguration hat er Vorrang vor dem globalen Kanal. Diese Einstellung funktioniert nur für CN470/US915/AU915-Gateways.	Null
PingSlot-Periode	Zeitraum, in dem der Ping-Slot geöffnet ist.	Jede Sekunde
PingSlot-Datenrate	Datenrate des Knotens, der Downlinks empfängt.	Basierend auf der unterstützten Frequenz
PingSlot-Frequenz	Frequenz des Knotens, der Downlinks empfängt.	Basierend auf der unterstützten Frequenz
ACK-Zeitlimit	Die Zeit für bestätigte Downlink-Übertragungen. Diese Option gilt nur für Klasse B und Klasse	Klasse B: 10 Klasse C: 10

	C.	

Tabelle 3-2-2-12 Geräteprofile – Erweiterte Einstellungsparameter

3.2.2.5 Gerät

Ein Gerät ist das Endgerät, das mit dem LoRaWAN®-Netzwerk verbunden ist und über dieses kommuniziert.

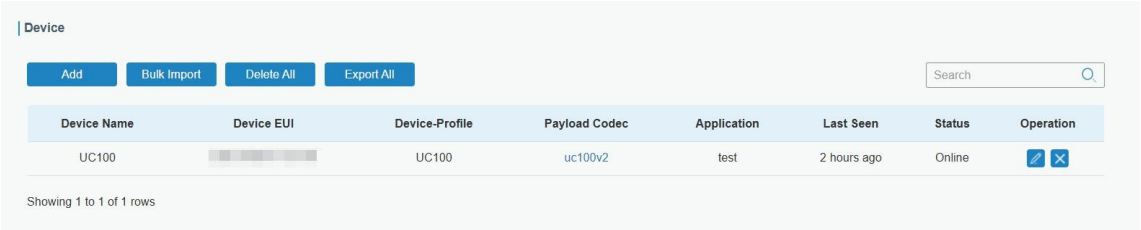


Abbildung 3-2-2-15

Element	Beschreibung
Hinzufügen	Ein Gerät hinzufügen.
Massenimport	Vorlage herunterladen und mehrere Geräte importieren.
Alle löschen	Löschen Sie alle Geräte in der Liste.
Alle exportieren	Exportieren Sie alle Geräteinformationen als CSV-Datei.
Gerätename	Zeigen Sie den Namen des Geräts an.
Geräte-EUI	Zeigen Sie die EUI des Geräts an.
Geräteprofil	Zeigen Sie den Namen des Geräteprofils des Geräts an.
Nutzlast-Codec	Zeigt den verwendeten Nutzdaten-Codec des Geräts an. Klicken Sie hier, um die Details dieses Nutzdaten-Codecs anzuzeigen.
Anwendung	Zeigt den Namen der Anwendung des Geräts an.
Zuletzt gesehen	Zeigt den Zeitpunkt des zuletzt empfangenen Pakets an.
Status	Zeigt den Status des Geräts an. **Nie aktiviert:** Das Gerät hat sich nie mit dem Netzwerk verbunden oder Pakete gesendet. **Offline:** Das Gerät hat innerhalb der Zeitüberschreitung keine Pakete gesendet. **Online:** Das Gerät hat innerhalb der Zeitüberschreitung Pakete gesendet.
Vorgang	Bearbeiten oder löschen Sie das Gerät.

Tabelle 3-2-2-13 Geräteparameter

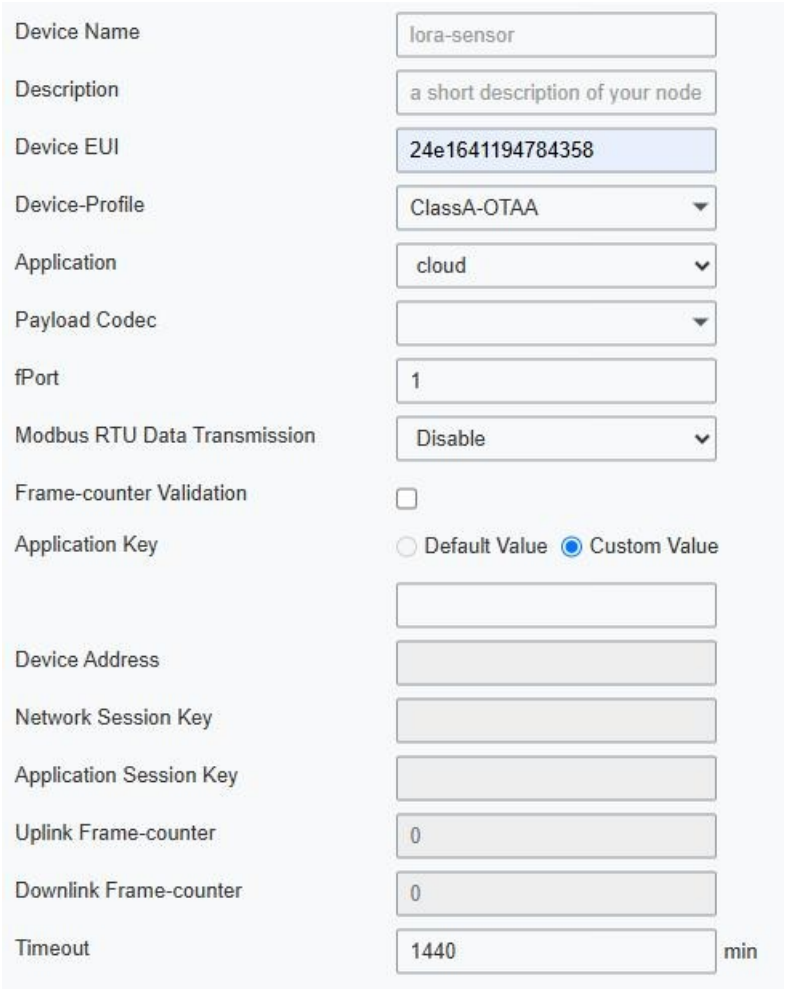


Abbildung 3-2-2-16

Gerätekonfiguration	
Element	**Beschreibung**
Gerätename	Geben Sie den Namen dieses Geräts ein.
Beschreibung	Geben Sie die Beschreibung dieses Geräts ein.
Geräte-EUI	Geben Sie die EUI dieses Geräts ein.
Geräteprofil	Wählen Sie das Geräteprofil aus.
Anwendung	Wählen Sie das Anwendungsprofil aus.
Nutzlast-Codec	Wählen Sie den Payload-Codec aus, der auf der Seite **„Payload-Codec“** vorhanden ist.
fPort	Geben Sie den Downlink-Port des Geräts ein. Bei Milesight-Geräten ist dies standardmäßig 85. .
Modbus RTU-Datenübertragung	Wählen Sie aus: „Deaktivieren“, „Modbus RTU zu TCP“, „Modbus RTU über TCP“. Diese Funktion ist nur für Milesight LoRaWAN®-Controller verfügbar (UC501/UC300 usw.). **Modbus RTU zu TCP:** Der TCP-Client kann Modbus-TCP-Befehle senden, um Modbus-Daten vom Controller anzufordern. **Modbus RTU über TCP:** Der TCP-Client kann Modbus-RTU-Befehle senden , um Modbus-Daten vom Controller anzufordern.
Modbus RTU Fport	Geben Sie den LoRaWAN®-Frame-Port für die transparente Übertragung zwischen Milesight LoRaWAN® Controllern und UG67.

	Bereich: 2-84, 86-223. Hinweis: Dieser Wert muss mit dem Fport des Milesight LoRaWAN®-Controllers übereinstimmen.
TCP-Port	Geben Sie den TCP-Port für die Datenübertragung zwischen dem TCP-Client und UG67 (als TCP-Server) ein. Bereich: 1-65535.
Frame-Zähler Validierung	Wenn die Frame-Zähler-Validierung deaktiviert wird, gefährdet dies die Sicherheit, da Replay-Angriffe ermöglicht.
Anwendungsschlüssel	Wenn ein Endgerät über eine Over-the-Air-Aktivierung mit einem Netzwerk verbunden wird, wird der Anwendungsschlüssel verwendet, um den Anwendungssitzungsschlüssel abzuleiten. **Standardwert:** Der Standardwert für Milesight-Endgeräte lautet 5572404C696E6B4C6F52613230313823. **Benutzerdefinierter Wert:** Definieren Sie den App-Schlüssel entsprechend den Endgeräten.
Geräteadresse	Die Geräteadresse identifiziert das Endgerät innerhalb dem aktuellen Netzwerk.
Netzwerksitzungsschlüssel	Der Netzwerksitzungsschlüssel ist spezifisch für das Endgerät. Er wird vom Endgerät verwendet, um den MIC oder einen Teil des MIC (Message Integrity Code) aller Uplink-Datenmeldungen, um die Datenintegrität sicherzustellen.
Anwendungssitzungsschlüssel	Der AppSKey ist ein für das Endgerät spezifischer Anwendungssitzungsschlüssel. Er wird sowohl vom Anwendungsserver als auch vom Endgerät verwendet, um udentschlüsseln.
Uplink Frame-Zähler	Die Anzahl der Datenframes, die zum Netzwerkserver hochgeladen wurden. Sie wird vom Endgerät erhöht und vom Endgerät empfangen. Benutzer können ein personalisiertes Endgerät manuell zurücksetzen, woraufhin die Frame-Zähler auf dem Endgerät und die Frame-Zähler auf dem Netzwerkserver für dieses Endgerät auf 0 zurückgesetzt.
Downlink-Rahmenzähler	Die Anzahl der Datenframes, die vom Netzwerk-Server über die Downlink-Verbindung vom Endgerät empfangen wurden. Sie wird vom Netzwerk-Server erhöht. Benutzer können ein personalisiertes Endgerät manuell zurücksetzen, woraufhin die Frame-Zähler auf dem Endgerät und die Frame-Zähler auf dem Netzwerk-Server für dieses Endgerät auf 0 zurückgesetzt.
Zeitlimit	Die Zeit, um den Online-/Offline-Status des Geräts zu beurteilen. Bereich: 1-4320 Minuten

Tabelle 3-2-2-14 Geräteeinstellungsparameter

Beispiel für die zugehörige Konfiguration

Gerätekonfiguration

3.2.2.6 FUOTA

Firmware Update Over the Air (FUOTA) ist ein Standard für die Verteilung von Firmware-Updates an Endgeräte über Unicast oder Multicast. **Bevor Sie diese Funktion nutzen, stellen Sie sicher, dass das Endgerät das Standard-LoRaWAN®FUOTA-Protokoll unterstützt.**

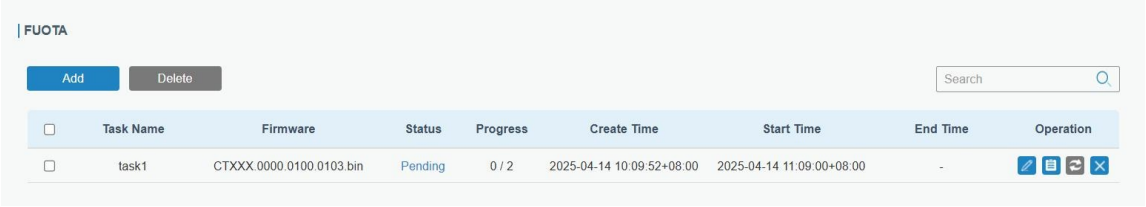


Abbildung 3-2-2-17

FUOTA	
Element	**Beschreibung**
Hinzufügen	Klicken Sie hier, um eine Aufgabe hinzuzufügen.
Löschen	Aktivieren Sie die Kontrollkästchen der Aufgabenliste und klicken Sie auf , um diese Aufgaben zu löschen.
Aufgabenname	Der Name der Aufgabe.
Firmware	Die Firmware, die in dieser Aufgabe aktualisiert werden soll.
Status	Der Status der Aufgabe. **Ausstehend:** Warten Sie auf den geplanten Zeitpunkt für die Bearbeitung der Aufgabe. **Warten:** Bereiten Sie die Erstellung der Sitzung für ein Upgrade vor. **Ausführung:** Mindestens ein Gerät antwortet auf das Upgrade-Ergebnis. **Fertig:** Alle Geräte antworten auf die Upgrade-Ergebnisse, einschließlich Erfolg und Fehlschlag.
Fortschritt	Die Anzahl der Geräte, die erfolgreich aktualisiert wurden/für eine Aktualisierung vorgesehen sind .
Erstellungszeit	Erstellungszeitpunkt dieser Aufgabe.
Startzeit	Der Zeitpunkt, zu dem diese Aufgabe gestartet wird.
Endzeit	Die Zeit, zu der diese Aufgabe abgeschlossen sein soll.
Vorgang	: Bearbeiten Sie diese Aufgabe, wenn der Aufgabenstatus „Ausstehend“ lautet. : Überprüfen Sie die Aufgabendetails, einschließlich des Erfolgs- und Fehlerstatus jedes Geräts. Wiederholen Sie die Aufgabe für Geräte, bei denen das Upgrade fehlgeschlagen ist, wenn der Aufgabenstatus „Abgeschlossen“ ist. : Löschen Sie diese Aufgabe, wenn der Aufgabenstatus „Ausstehend“ oder „Abgeschlossen“ lautet.

Tabelle 3-2-2-15 FUOTA-Parameter

FUOTA-Aufgaben hinzufügen

1. Klicken Sie auf die Schaltfläche **„Hinzufügen“**, um eine FUOTA-Aufgabe hinzuzufügen.
2. Konfigurieren Sie die Aufgabeneinstellungen.

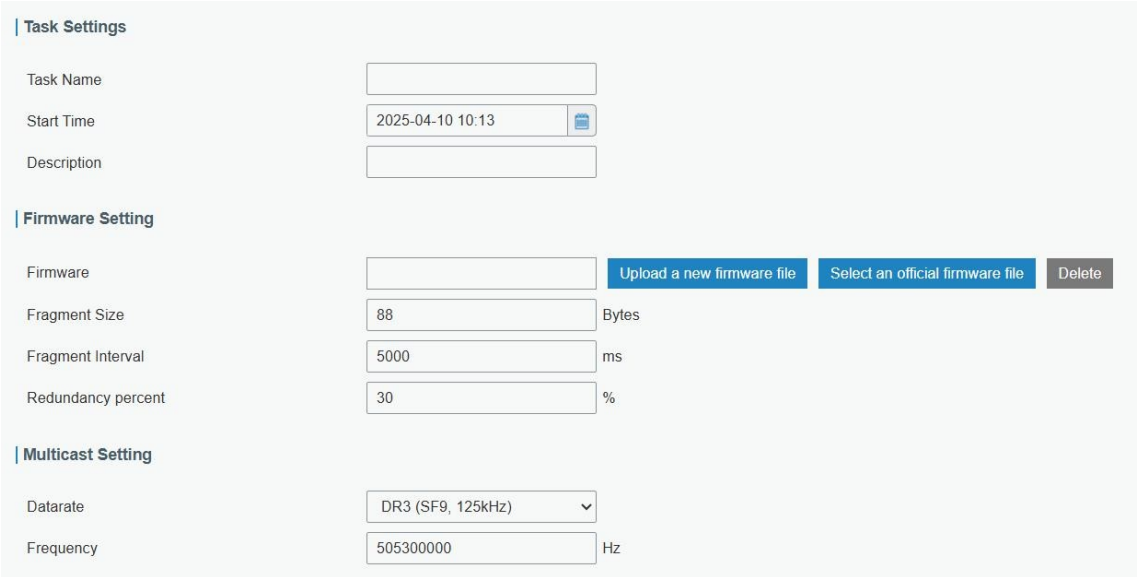
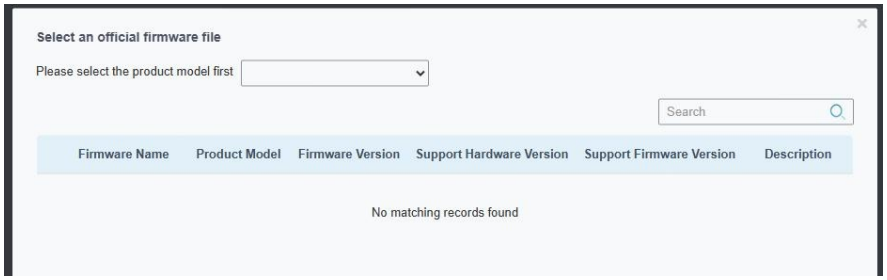


Abbildung 3-2-2-18

Aufgabeneinstellungen hinzufügen	
Element	**Beschreibung**
Grundlegende Informationen	
Aufgabenname	Passen Sie einen Aufgabennamen an.
Startzeit	Legen Sie die Startzeit für diese Aufgabe fest.
Beschreibung	Geben Sie die Beschreibung für diese Aufgabe ein.
Firmware-Einstellungen	
Firmware	Importieren Sie die zu aktualisierende Firmware. **Neue Firmware-Datei hochladen:** Importieren Sie eine Firmware lokal. **Offizielle Firmware-Datei auswählen:** Wählen Sie zunächst das Produktmodell aus und wählen Sie dann die Firmware zum Herunterladen von der offiziellen Website aus. Dazu muss das Gateway Zugang zum Internet haben. 
Fragmentgröße	Die Firmware-Datei wird in diese Größe aufgeteilt, um sie Geräten zuzuweisen. In der Regel sollten Sie diesen Wert als Standard beibehalten. Bei einer komplexen oder schlechten Netzwerkumgebung wird empfohlen, diesen Wert auf 64 oder weniger zu reduzieren. Bei einer guten Netzwerkumgebung kann dieser Wert erhöht werden, um die Übertragungsgeschwindigkeit zu verbessern .
Fragmentintervall	Das Intervall, in dem Firmware-Fragmente den Geräten zugewiesen werden. In der Regel sollte dieser Wert auf dem Standardwert belassen werden. Bei einer komplexen oder schlechten Netzwerkumgebung wird empfohlen, diesen Wert auf 7-10s oder einen höheren Wert zu erhöhen; wenn die Netzwerkumgebung

	gute Netzwerkumgebung vorliegt, kann dieser Wert verringert werden, um die Übertragungsgeschwindigkeit zu verbessern.
Redundanzprozentsatz	Das Gerät sendet 30 % Redundanzpakete zur Korrektur von Firmware-Dateipaketen. In der Regel sollte dieser Wert auf dem Standardwert belassen werden. Wenn die Netzwerkumgebung komplex oder schlecht ist, wird empfohlen, diesen Wert auf 40 % bis 50 % oder einen höheren Wert zu erhöhen, um die Übertragungserfolgsrate zu verbessern. Wenn die Netzwerkumgebung gut ist, kann dieser Wert verringert werden.
Multicast-Einstellungen	
Datenrate	Datenrate für die Zuweisung der Firmware-Fragmente zu den Geräten.
Frequenz	Downlink-Frequenz, um die Firmware-Fragmente den Geräten zuzuweisen.

Tabelle 3-2-2-16 Aufgabenparameter

3. Wählen Sie die Geräte aus, auf denen diese Aufgabe ausgeführt werden soll. Bitte wählen Sie Geräte desselben Modells aus.

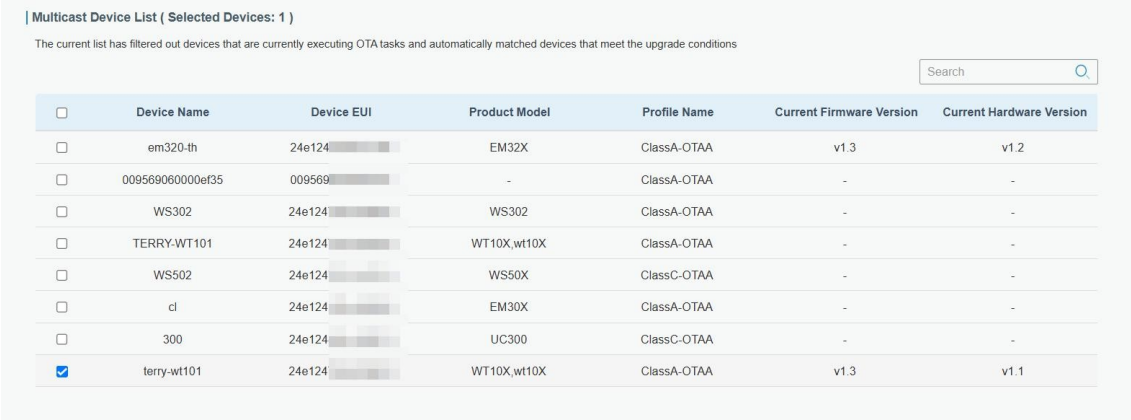
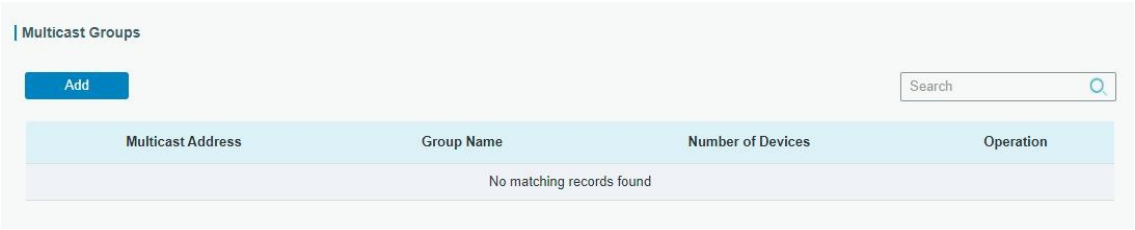


Abbildung 3-2-2-19

4. Klicken Sie auf **„Speichern“**, um diese Aufgabeneinstellungen zu speichern.

3.2.2.7 Multicast-Gruppen

Milesight-Gateways unterstützen die Erstellung von Multicast-Gruppen der Klasse B oder C, um Downlink-Nachrichten an eine Gruppe von Endgeräten zu senden. Eine Multicast-Gruppe ist ein virtuelles ABP-Gerät (d. h. gemeinsam genutzte Sitzungsschlüssel) und unterstützt weder Uplink noch bestätigte Downlink- oder



MAC-Befehle.

Abbildung 3-2-2-20

Element	Beschreibung
Hinzufügen	Eine Multicast-Gruppe hinzufügen.

Gruppenname	Zeigt den Namen der Gruppe an.
Anzahl der Geräte	Zeigt die Anzahl der Geräte in der Gruppe an.
Vorgang	Bearbeiten oder löschen Sie die Multicast-Gruppe.

Tabelle 3-2-2-17 Multicast-Gruppenparameter

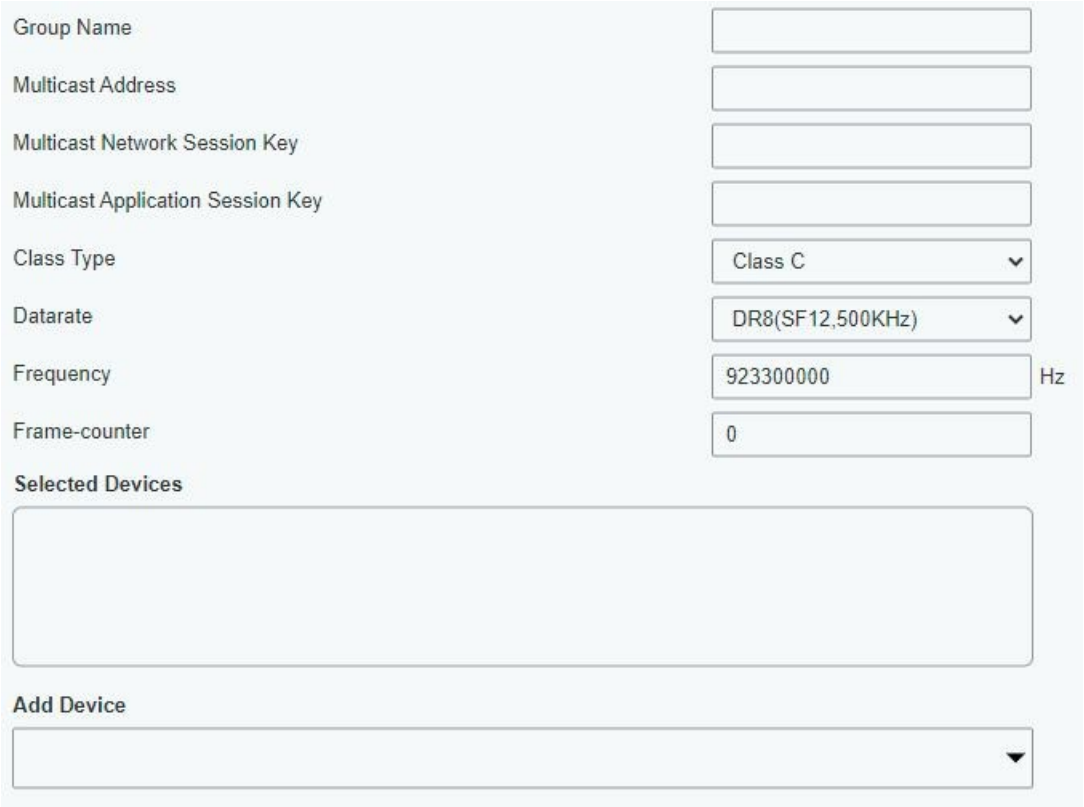


Abbildung 3-2-2-21

Konfiguration der Multicast-Gruppe	
Element	**Beschreibung**
Gruppenname	Geben Sie den Namen dieser Multicast-Gruppe ein.
Multicast-Adresse	Geräteadresse (Dev Addr) aller Geräte in dieser Gruppe.
Multicast-Netzwerk Sitzungsschlüssel	Der Netzwerksitzungsschlüssel (Netwks Key) aller Geräte in dieser Gruppe.
Multicast-Anwendung Sitzungsschlüssel	Der Anwendungssitzungsschlüssel (AppSKey) aller Geräte in dieser Gruppe.
Klassentyp	Klasse B und Klasse C sind optional.
Datenrate	Datenrate des Knotens, der Downlinks empfängt
Frequenz	Downlink-Frequenz aller Geräte in dieser Gruppe.
Frame-Zähler	Die Anzahl der Datenframes, die vom Endgerät empfangen wurden Downlink vom Netzwerkserver empfangen hat. Er wird vom Netzwerkserver erhöht.
Ping-Slot Periodizität	Zeitraum, in dem der Ping-Slot geöffnet ist. Dies gilt nur für Endgeräte der Klasse B Endgeräten.
Ausgewählte Geräte	Alle Gerätenamen in dieser Gruppe anzeigen.

Gerät hinzufügen	Geräte in der Pulldown-Liste hinzufügen.

Tabelle 3-2-2-18 Parameter für die Multicast-Gruppeneinstellung

3.2.2.8 Gateway-Flotte

Milesight-Gateways können eine Verbindung zum Gateway-Netzwerkserver herstellen. Ein Gateway unterstützt maximal 100 Gateways.

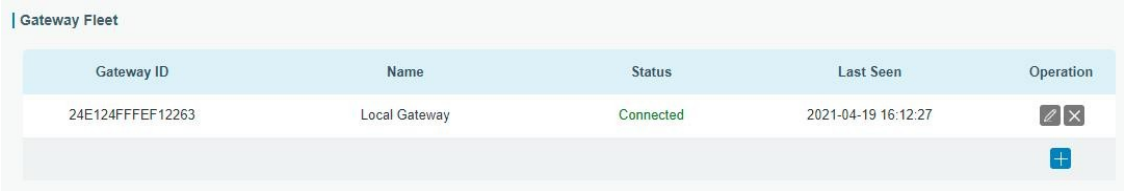


Abbildung 3-2-2-22

Element	Beschreibung
Gateway-ID	Zeigt die Gateway-ID an.
Name	Zeigt den Namen des Gateways an.
Status	Zeigt den Verbindungsstatus des Gateways an.
Zuletzt gesehen	Zeigt den Zeitpunkt des letzten empfangenen Pakets an.
Vorgang	Bearbeiten oder löschen Sie das Gateway.

Tabelle 3-2-2-19 Gateway-Flottenparameter

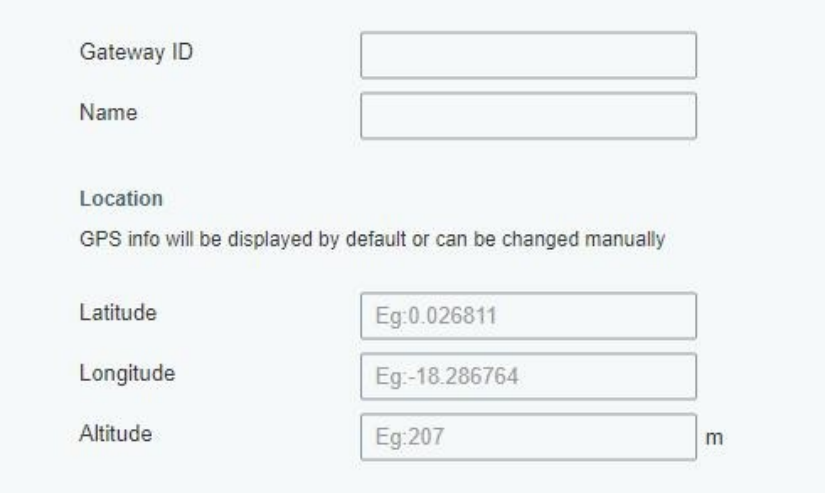


Abbildung 3-2-2-23

Element	Beschreibung
Gateway-ID	Geben Sie die eindeutige Gateway-ID ein, um das Gateway zu erkennen.
Name	Geben Sie den Namen dieses Gateways ein.
Standort	Die GPS-Daten des Gateways können hier bearbeitet werden. Wenn das Gateway GPS-Daten sendet Daten sendet, werden Ihre benutzerdefinierten Daten ersetzt.

Tabelle 3-2-2-20 Gateway-Einstellungsparameter

3.2.2.9 Pakete

Das Gateway unterstützt die Anzeige der letzten 1000 Pakete und das Senden von Befehlen an Geräte.

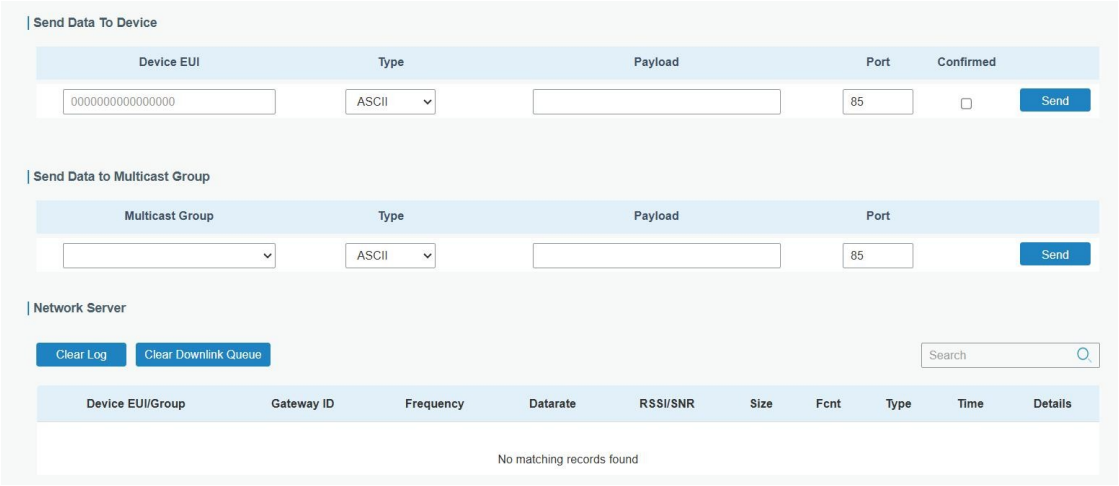


Abbildung 3-2-2-24

Daten an Gerät/Multicast-Gruppe senden	
Element	**Beschreibung**
Geräte-EUI	Geben Sie die EUI des Geräts ein, das die Nutzlast empfangen soll die Nutzlast empfangen soll.
Multicast Gruppe	Wählen Sie die Multicast-Gruppe aus, um Downlinks zu senden. Multicast-Gruppen können unter der Registerkarte **„Multicast-Gruppen"** hinzugefügt werden.
Typ	Wählen Sie den Nutzlasttyp aus, der in das Eingabefeld „Nutzlast" eingegeben werden soll: ASCII, Hex, Base64.
Nutzlast	Geben Sie die Nachricht ein, die an dieses Gerät gesendet werden soll.
Port	Geben Sie den LoRaWAN®Frame-Port für die Paketübertragung zwischen Gerät und Netzwerkserver ein.
Bestätigt	Nach der Aktivierung empfängt das Endgerät ein Downlink-Paket und sollte dem Netzwerkserver mit „bestätigt" antworten. Die Multicast-Funktion unterstützt keine bestätigten Downlinks.

Tabelle 3-2-2-21 Parameter für das Senden von Daten an das Gerät

Netzwerkserver	
Element	**Beschreibung**
Protokoll löschen	Löschen Sie die an den Netzwerkserver gesendeten Paketprotokolle.
Downlink-Warteschlange löschen	Löschen Sie die Downlink-Warteschlange, die nicht an das Gerät gesendet wird.
Geräte-EUI/Gruppe	Zeigt die EUI des Geräts oder der Multicast-Gruppe an.
Frequenz	Zeigt die verwendete Frequenz zum Senden von Paketen an.
Datenrate	Zeigt die verwendete Datenrate für die Übertragung von Paketen an.
SNR	Zeigt das Signal-Rausch-Verhältnis an.
RSSI	Zeigt den Empfangssignalstärkeindikator an.
Größe	Zeigt die Größe der Nutzlast an.
Fcnt	Zeigt den Frame-Zähler an.
Typ	Zeigt den Typ des Pakets an: JnAcc – Join Accept Packet (Paket zum Akzeptieren des Beitritts) JnReq – Join Request Packet (Paket zum Anfordern des Beitritts) UpUnc – Unbestätigtes Uplink-Paket

	UpCnf – Bestätigtes Uplink-Paket – ACK-Antwort vom Netzwerk angefordert DnUnc – Unbestätigtes Downlink-Paket DnCnf – Downlink Confirmed Packet – ACK-Antwort vom Endgerät angefordert
Zeit	Zeigt die Zeit an, zu der das Paket gesendet oder empfangen wurde.

Tabelle 3-2-2-22 Paketparameter

Klicken Sie auf „ “, um weitere Details zum Paket anzuzeigen. Wie gezeigt:

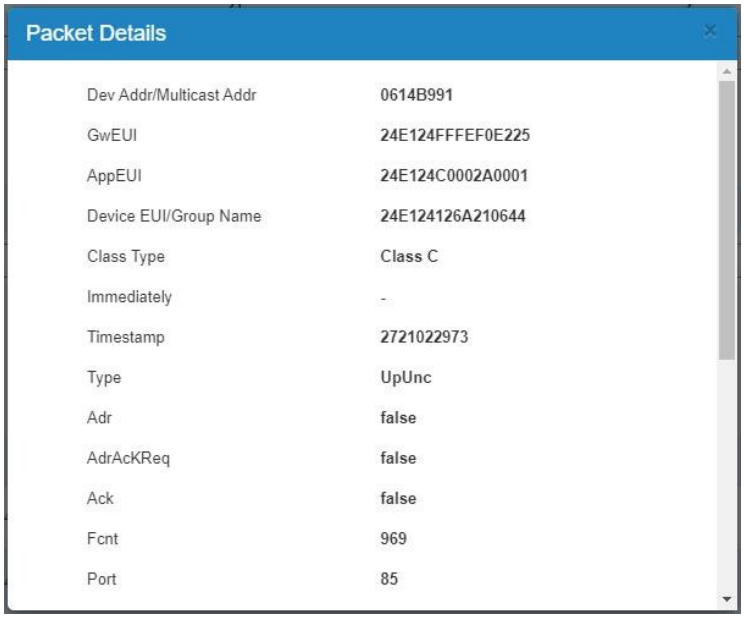


Abbildung 3-2-2-25

Element	Beschreibung
Dev Adresse/Multicast-Adresse	Zeigt die Adresse des Geräts/der Multicast-Gruppe an.
GwEUI	Zeigt die EUI des Gateways an.
AppEUI	Zeigt die App-EUI des Endgeräts an.
DevEUI/Gruppe Name	Zeigt die EUI des Geräts/Multicast-Gruppennamens an.
Klassentyp	Zeigt den Klassentyp des Geräts oder der Multicast-Gruppe an.
Sofort	Ob dieses Downlink-Paket sofort gesendet werden soll.
Zeitstempel	Zeigt die Zeit an, zu der dieses Paket nach dem Start des Paketweiterleiters empfangen wird . Einheit: ms
Typ	Zeigt den Typ des Pakets an: JnAcc – Join-Akzeptanzpaket JnReq – Join-Anforderungspaket UpUnc – Unbestätigtes Uplink-Paket UpCnf – Bestätigtes Uplink-Paket – ACK-Antwort vom angeforderten Netzwerk

	DnUnc – Unbestätigtes Downlink-Paket DnCnf – Downlink Confirmed Packet – ACK-Antwort vom Endgerät angefordert
Adr	True: Der Endknoten hat ADR aktiviert. Falsch: Der Endknoten hat ADR nicht aktiviert.
AdrAckReq	Um zu überprüfen, ob das Netzwerk die Uplink-Nachrichten empfängt, senden die Knoten regelmäßig eine ADRACKReq-Nachricht. Diese ist 1 Bit lang. True: Das Netzwerk sollte innerhalb der Zeit ADR_ACK_DELAY antworten, um zu bestätigen, dass es die Uplink-Nachrichten empfängt. Falsch: ADR ist deaktiviert oder das Netzwerk antwortet nicht in ADR_ACK_DELAY.
Bestätigt	Wahr: Dieser Frame ist ACK. Falsch: Dieser Frame ist kein ACK.
Fcnt	Zeigt den Frame-Zähler dieses Pakets an. Der Netzwerkserver verfolgt den Uplink-Frame-Zähler und generiert den Downlink-Zähler für jedes Endgerät einen Downlink-Zähler.
FPort	Der FPort zum Senden dieses Pakets. Wenn es sich bei diesem Paket um einen MAC-Befehl handelt, ist der Port 0; wenn dieses Paket Anwendungsdaten enthält, ist der Port nicht 0 (1-233).
Modulation	LoRa bedeutet, dass die physikalische Schicht die LoRa-Modulation verwendet.
Bandbreite	Zeigt die Bandbreite dieses Kanals an.
SpreadFactor	Zeigt den SpreadFactor dieses Kanals an.
Bitrate	Zeigt die Bitrate dieses Kanals an.
Codierrate	Zeigt die Codierrate dieses Kanals an.
SNR	Zeigt das SNR dieses Kanals an.
RSSI	Zeige den RSSI dieses Kanals an.
Leistung	Zeige die Sendeleistung des Geräts an.
Nutzlast (b64)	Zeige die Anwendungsnutzlast dieses Pakets an.
Nutzlast (hex)	Zeigt die Anwendungsnutzlast dieses Pakets an.
Json	Zeigt die Daten nach der Dekodierung an.
MIC	Zeigt den MIC dieses Pakets an. MIC ist ein kryptografischer Nachrichtenintegritätscode, der über die Felder MHDR,FHDR, FPort und den verschlüsselten FRMPayload berechnet wird.

Tabelle 3-2-2-23 Paketdetails-Parameter

Verwandtes Thema

Daten an Gerät senden

3.3 Protokollintegration

3.3.1 BACnet-Server

UG67 kann als LoRaWAN®-zu-BACnet-Gateway fungieren, um eine einfache Integration in das BMS-System zu ermöglichen. Bevor Sie diese Funktion nutzen, stellen Sie sicher, dass die Version der integrierten Payload-Codec-Bibliothek auf dem neuesten Stand ist und

die entsprechenden LoRaWAN®-Geräte den richtigen Payload-Codec hinzugefügt haben.

3.3.1.1 Server

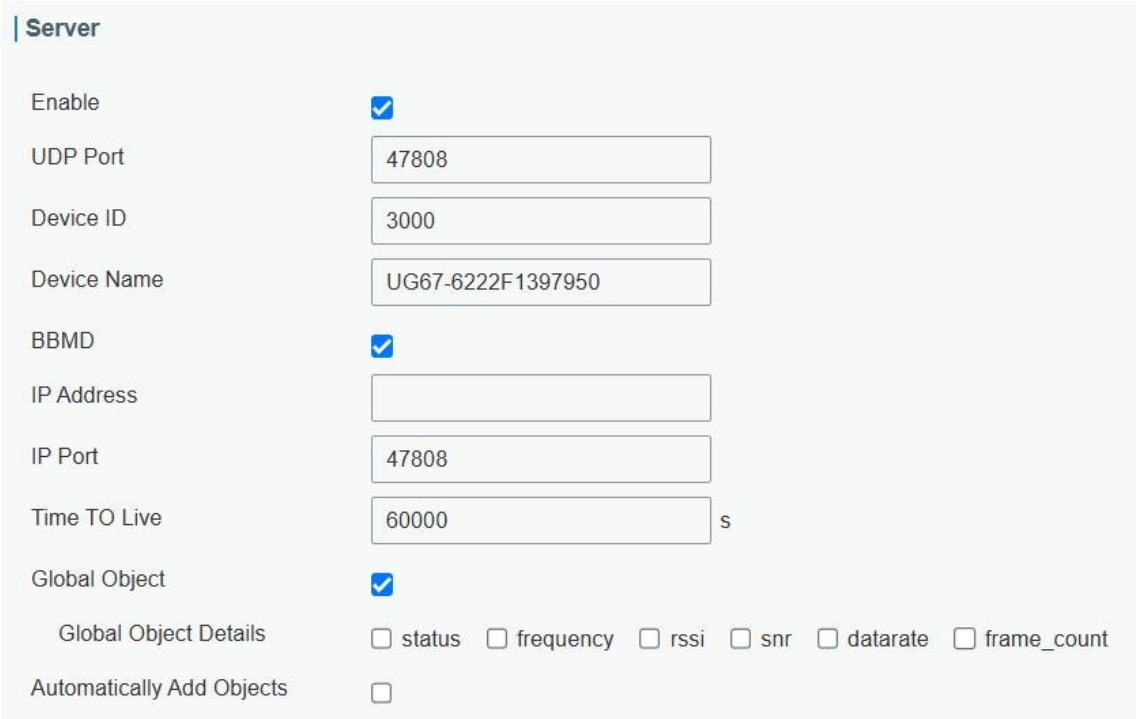


Abbildung 3-3-1-1

Servereinstellungen	
Element	**Beschreibung**
Aktivieren	Aktivieren oder deaktivieren Sie die BACnet-Serverfunktion.
UDP-Port	Kommunikationsport von BACnet/IP einstellen. Bereich: 1-65535. Der Standardport ist 47808.
Geräte-ID	Die eindeutige BACnet-Gerätekennung, die Konflikte mit anderen Geräten vermieden werden muss. Der Standardwert sind die Zeichen 6 bis 11 der SN.
Gerätename	Der Name, der das Gerät repräsentiert.
BBMD	Aktivieren Sie BBMD (BACnet/IP Broadcast Management Device), wenn BACnet-Geräte aus verschiedenen Netzwerk-Subnetzen zusammenarbeiten sollen. **IP-Adresse**: Geben Sie die IP-Adresse des BBMD-Geräts oder des externen Geräte-Registrars ein. **IP-Port**: Geben Sie den UDP/IP-Port für die Registrierung externer Geräte ein. **Time TO Live**: Anzahl der Sekunden, die für die Registrierung externer Geräte verwendet werden.
Globales Objekt	Nach der Aktivierung fügt das Gateway automatisch globale Objekte für jedes Gerät hinzu. Diese globalen Objekte dürfen nicht gelöscht werden, es sei denn, diese Option ist deaktiviert. **Status:** Online-/Offline-Status des Geräts **Frequenz**: Uplink-Frequenz des Geräts **Rssi**: Uplink-RSSI des Geräts **Snr**: SNR des Geräts im Uplink

	Datarate: Datenrate des Geräts im Uplink **Frame_count**: Anzahl der Uplink-Frames des Geräts (FCNT)
Automatisch Objekte hinzufügen	Nach der Aktivierung fügt das Gateway Objekte entsprechend dem Payload-Codec automatisch Objekte hinzu, wenn Geräte zum Netzwerkserver hinzugefügt werden.

Tabelle 3-3-1-1 Serverparameter

3.3.1.2 BACnet-Objekt

Abbildung 3-3-1-2

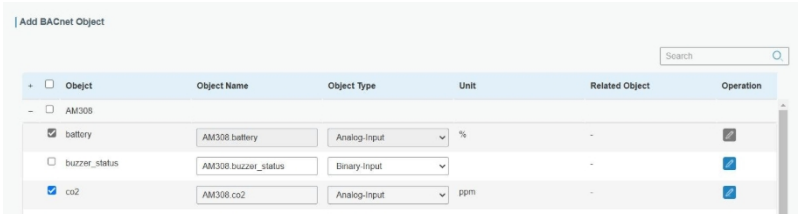
Element	Beschreibung
Objekt hinzufügen	Klicken Sie hier, um die gewünschten Objekte auszuwählen, die zu diesem Server hinzugefügt werden sollen. Das Gateway unterstützt das Hinzufügen von maximal 10.000 Objekten. **Hinweis:** Stellen Sie sicher, dass der Inhalt des Payload-Codecs korrekt ist und das Gerät den richtigen Payload-Codec auswählt. 
NC-Objekt hinzufügen	Fügen Sie ein Objekt vom Typ „Notification-Class“ hinzu, um die Empfänger von Alarmen festzulegen. Das Gateway unterstützt das Hinzufügen von maximal 200 NC-Objekten .
Massenimport	Laden Sie eine Vorlage herunter, um mehrere BACnet-Objekte zu importieren.
Massen-Export	Wählen Sie die gewünschten Objekte aus, um sie als Datei im .xlsx-Format zu exportieren.
Löschen	Wählen Sie die gewünschten Objekte zum Löschen aus.
Objektname	Zeigen Sie den Namen des BACnet-Objekts an.
Objekttyp	Zeigen Sie den Typ dieses Objekts an.
Objektinstanz-Nr.	Zeigt die Instanznummer dieses Objekts an.
Aktueller Wert	Zeige den aktuellen Wert des Objekts an.
Einheiten	Zeigt die Einheit dieses Objektwerts an.
Aktualisierungen	Zeigt die Aktualisierungszeiten dieses Objektwerts an.
Aktualisierungszeit	Zeigt den Zeitpunkt an, zu dem dieses Objekt die Daten abgerufen und aktualisiert hat.
COV	Zeigt an, ob COV (Wertänderung) aktiviert ist.
Operation	Bearbeiten oder löschen Sie das Objekt.

Tabelle 3-3-1-2 BACnet-Objektlistenparameter

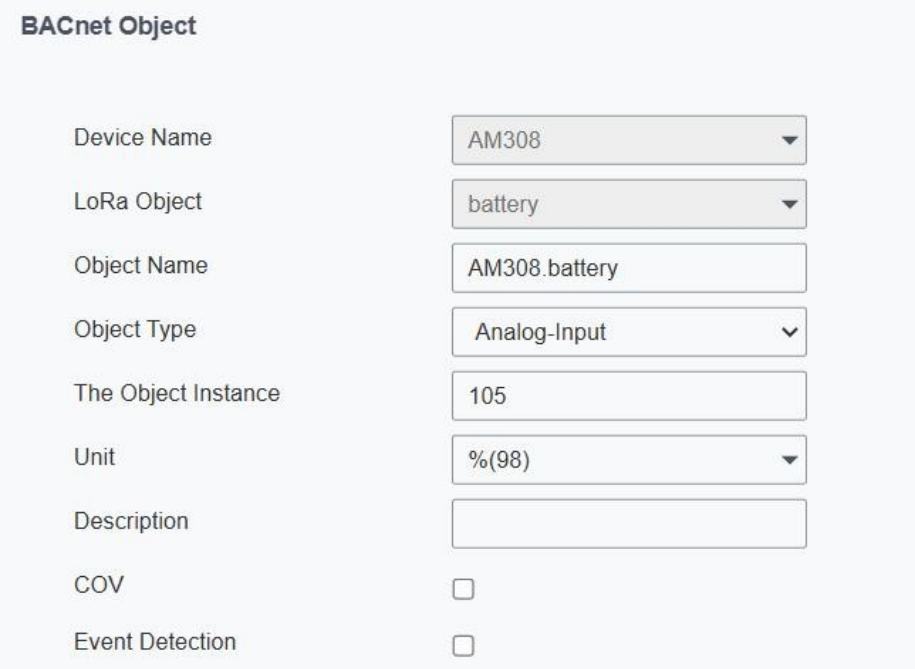


Abbildung 3-3-1-3

BACnet-Objektkonfiguration	
Element	**Beschreibung**
Gerätename	Zeigt den Namen der Geräte an.
LoRa-Objekt	Zeigen Sie den entsprechenden Namen des LoRa-Objekts an.
Objektname	Passen Sie einen eindeutigen Namen für dieses Objekt an.
Objekttyp	Wählen Sie den Objekttyp als Binäreingabe/-ausgabe/-wert, Analogeingabe/-ausgabe/-wert, MultiState-Eingabe/-Ausgabe/-wert und Zeichenfolgenwert.
Das Objekt Instanz	Passen Sie die Objektinstanz an.
Beschreibung	Geben Sie die Beschreibung dieses Objekts ein.
Ereigniserkennung	Aktivieren Sie diese Option, um den Alarm für diesen Wert zu melden. Dazu muss mindestens ein Benachrichtigungsklassenobjekt definiert werden.
Analoge Ein-/Ausgänge/Werte	
Einheiten	Wählen Sie die Einheit für den Wert dieses Objekts aus.
COV	Wenn sich der Objektwert ändert, sendet der BACnet-Server (Gateway) eine Benachrichtigung über den neuen Wert an den BACnet-Client. Dies gilt nur für Objekte vom Typ „Analog".
COV-Inkrement	Nur wenn der Objektwert diesen Inkrementwert erreicht oder überschreitet, sendet der BACnet-Server (Gateway) die Benachrichtigung.
Verzicht Standard	Wenn kein Befehl vorliegt wird der Analogausgang auf diesen Standardwert zurückgesetzt.
Binäreingabe/-ausgabe/-wert	
Polarität	Definieren Sie den Status der binären Ein-/Ausgänge als „Normal" oder „Umgekehrt".
Aktiver Text	Charakterisieren Sie die beabsichtigte Wirkung des aktiven Zustands des Objekts vom Typ „Binärwert".

	. **Beispiel:** Wenn eine Taste gedrückt wird und der Binäreingang 1 ist, kann der aktive Text als „Gedrückt“ definiert werden.
Inaktiver Text	Charakterisieren Sie die beabsichtigte Wirkung des inaktiven Zustands des Binärtyps Objektwert. **Beispiel:** Bei einer Schaltfläche kann der inaktive Text als „Nicht gedrückt“ definiert werden.
Aufgeben Standard	Wenn kein Befehl vorhanden istwird die Binär-Ausgabe wie folgt festgelegt Standardwert festgelegt.
MultiState-Eingabe/Ausgabe/Wert	
Anzahl der Zustände	Legen Sie die Anzahl der Zustände fest und definieren Sie den Namen jedes Zustands.
Verzicht Standard	Wenn kein Befehl vorhanden istwird die Mehrzustandsausgabe auf diesen Standardwert festgelegt.
Ereigniserkennung	
Benachrichtigung Klasse	Wählen Sie die Benachrichtigungsklasse aus, um die Empfänger dieses Alarms.
Ereignis	Wählen Sie den zu meldenden Ereignistyp aus.
Ereignis einschränken	Wenn es sich um einen analogen Objekttyp handelt, wählen Sie aus, ob das Ereignis gemeldet werden soll, wenn die obere oder untere Grenze erreicht wird.
Totzone	Bei „To Offnormal Status“ (Bei abnormem Zustand) generiert das Gerät ein „To Normal“-Ereignis, wenn der aktuelle Wert während der Verzögerungszeit auf den Wert (Obergrenze – Totzone) oder (Untergrenze + Totzone) zurückkehrt. Nur analoge Typen verfügen über diese Option.
Zeitverzögerung	Nur wenn der aktuelle Wert die Schwellenwertbedingung erfüllt oder diesmal außerhalb des Schwellenwerts liegt, meldet das Gerät das entsprechende Ereignis.
Alarmwert	Meldet das Ereignis „To Offnormal“, wenn der aktuelle Wert während der Verzögerungszeit dem Alarmwert entspricht; meldet das Ereignis „To Normal“, wenn der aktuelle Wert während der Verzögerungszeit nicht dem Alarmwert entspricht. Nur Binäreingang, Binärwert Wert, Mehrfachzustandseingang oder Mehrfachzustandswert.
Fehlerwert	Melden Sie das Ereignis „To Fault“, wenn der aktuelle Wert dem Fehlerwert entspricht. Nur „Multi-State Input“ (Mehrzustands-Eingang) oder „Multi-State Value“ (Mehrzustandswert) verfügen über diese Option.
Rückmeldungswert	Melden Sie das Ereignis „To Offnormal“, wenn der aktuelle Wert während der Verzögerungszeit dem Rückmeldungswert entspricht; melden Sie das Ereignis „To Normal“, wenn der aktuelle Wert während der Verzögerungszeit nicht dem Rückmeldungswert entspricht. Nur Mehrzustands-Eingänge oder binäre Ausgänge über diese Option.
Benachrichtigung Typ	Wählen Sie den Benachrichtigungstyp als „Alarm“ oder „Ereignis“ aus.

Tabelle 3-3-1-3 BACnet-Objektkonfigurationsparameter

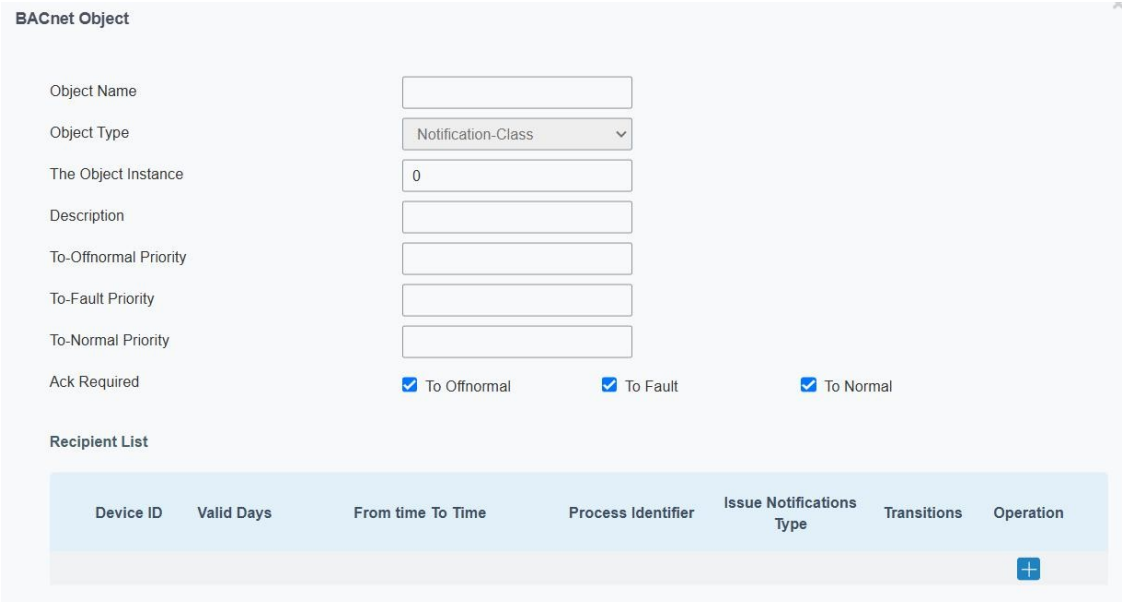


Abbildung 3-3-1-4

Benachrichtigungsklasse BACnet-Objektkonfiguration	
Element	**Beschreibung**
Objektname	Legen Sie einen eindeutigen Namen für dieses Objekt fest.
Objekttyp	Er ist als Benachrichtigungsklasse festgelegt.
Das Objekt Instanz	Passen Sie die Objektinstanz an.
Beschreibung	Geben Sie die Beschreibung dieses Objekts ein.
To-Offnormal Priorität	Legen Sie die Prioritätsnummer fest, anhand derer Empfänger die Ereignisbenachrichtigungen sortieren. Bereich: 0-255 (0 ist am wichtigsten, 255 am wenigsten wichtig)
Priorität bei Störungen	
Normal Priorität	
Bestätigung erforderlich	Geben Sie an, ob der Empfänger bei diesem Ereignis eine Bestätigungsalarmmeldung an das Gateway zurücksenden muss.
Empfängerliste	Wenn die Ereigniserkennung aktiviert und diese Benachrichtigungsklasse ausgewählt ist, wird die Ereignisbenachrichtigung an die Empfänger in dieser Liste gesendet. In einer Liste können maximal 10 Empfänger hinzugefügt werden. **Geräte-ID:** Die Geräte-ID des Zielempfängers. **Gültige Tage**: Gültige Tage für den Versand von Benachrichtigungen. **Von Zeit zu Zeit:** Gültige Zeit für das Senden von Benachrichtigungen. **Prozesskennung:** Die Kennung, die angibt, für welchen Prozess der Alarm bestimmt ist. Beispielsweise könnte die Prozesskennung 1 für Wartungsalarme, 2 für kritische Alarme und 3 für Lebensrettungsalarme stehen usw. **Art der Benachrichtigungen:** Wählen Sie die Art der Benachrichtigung als bestätigt oder unbestätigt aus. Wenn das Gateway keine Antwort auf die bestätigte Benachrichtigung erhält, sendet es die Benachrichtigung erneut. **Übergänge:** Wählen Sie die gemeldeten Ereignistypen aus.

Tabelle 3-3-1-4 Benachrichtigungsklasse BACnet-Objektkonfigurationsparameter

3.3.2 Modbus-Server

Das Gateway kann als Modbus-Server (Slave) fungieren, um Modbus-RTU- oder Modbus-TCP-Befehle von SPS-/BMS-Systemen zu empfangen und LoRaWAN®-Geräte zu lesen oder zu beschreiben. Bevor Sie diese Funktion nutzen, stellen Sie sicher, dass die Version der integrierten Payload-Codec-Bibliothek aktuell ist und die entsprechenden LoRaWAN®-Geräte den richtigen Payload-Codec hinzugefügt haben.

3.3.2.1 Server

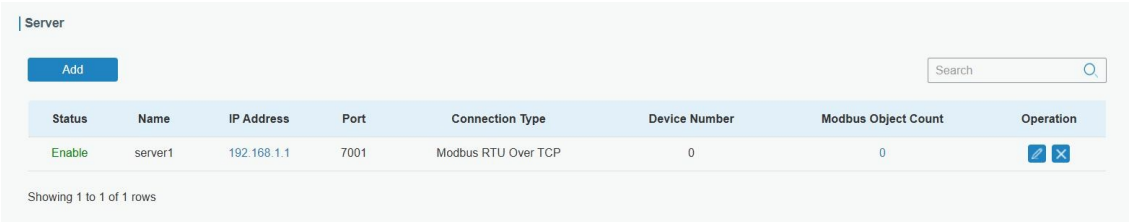


Abbildung 3-3-2-1

Element	Beschreibung
Hinzufügen	Fügen Sie einen Modbus-Server (Slave) hinzu. Ein Gateway unterstützt maximal 15 Server hinzu.
Status	Zeigt den Aktivierungsstatus dieses Servers an.
Name	Zeigt den Namen des Servers an.
IP-Adresse	Zeigt die IP-Adresse dieses Servers an. Klicken Sie darauf, um die Details anzuzeigen.
Port	Zeigt den Kommunikationsport dieses Servers an.
Verbindungstyp	Zeigen Sie den Verbindungstyp dieses Servers an.
Gerätenummer	Zeigt die Gerätenummer dieses Servers an.
Modbus-Objekt Anzahl	Zeigen Sie die Modbus-Objektanzahl dieses Servers an und klicken Sie auf die Nummer, um die Details zu überprüfen.
Bearbeiten	Bearbeiten oder löschen Sie diesen Server.

Tabelle 3-3-2-1 Serverparameter

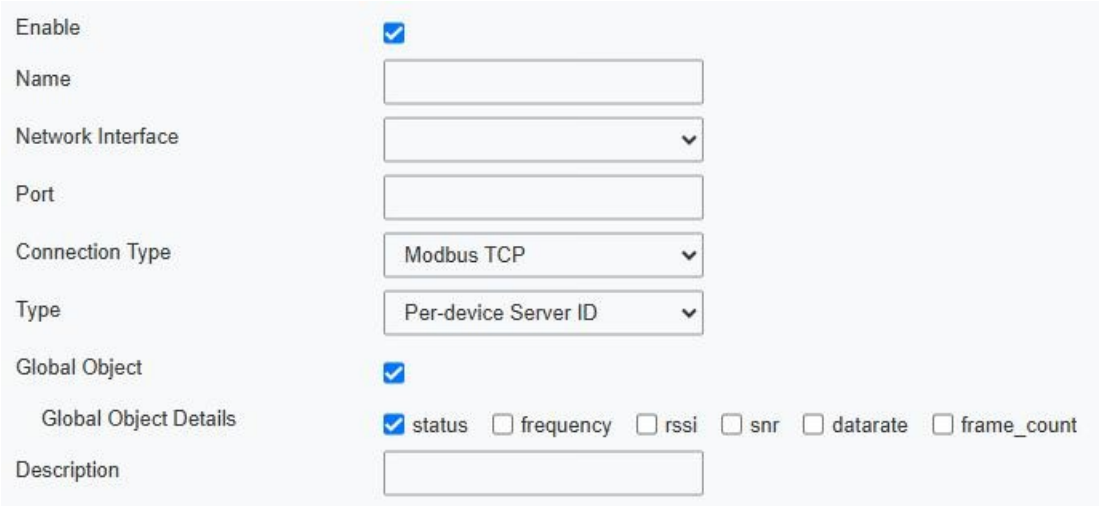


Abbildung 3-3-2-2

Servereinstellungen	
Element	**Beschreibung**
Aktivieren	Aktivieren oder deaktivieren Sie diesen Modbus-Server.
Name	Legen Sie einen eindeutigen Namen fest, um diesen Server zu identifizieren.
Netzwerkschnittstelle	Wählen Sie die Netzwerkschnittstelle aus, über die dieser Server mit Modbus-Clients (Master) kommunizieren soll. Das Gerät unterstützt die Verwendung verschiedener Netzwerkschnittstellen für die Kommunikation mit verschiedenen Remote-Plattformen .
Port	Kommunikationsport dieses Servers einstellen. Bereich: 1-65535.
Verbindungstyp	Wählen Sie den Verbindungstyp dieses Servers aus. **Modbus TCP:** Der Modbus-Client sendet Befehle im Modbus-TCP-Format an diesen Modbus-Server. **Modbus RTU über TCP:** Der Modbus-Client sendet Befehle im Modbus-RTU-Format Befehle an diesen Modbus-Server.
Typ	Legen Sie den Server-ID-Typ dieses Modbus-Servers fest. Dieser wird vom Modbus-Client verwendet, um jeden Server zu identifizieren. **Keine Server-ID**: Alle Geräte verwenden eine beliebige Server-ID. **Gerätespezifische Server-ID**: Unterstützung für die Konfiguration einer Server-ID pro Gerät.
Globales Objekt	Nach der Aktivierung fügt das Gateway automatisch globale Objekte für jedes Gerät hinzu. Diese globalen Objekte dürfen nicht gelöscht werden, es sei denn, diese Option ist deaktiviert. **Status:** Online-/Offline-Status des Geräts **Frequenz**: Uplink-Frequenz des Geräts **Rssi**: Uplink-RSSI des Geräts **Snr**: SNR der Geräte-Uplink **Datarate**: Datenrate des Geräts im Uplink **Frame_count**: Anzahl der Uplink-Frames des Geräts (FCNT)
Beschreibung	Fügen Sie eine Beschreibung für diesen Server hinzu.

Tabelle 3-3-2-2 Server-Einstellungsparameter

3.3.2.2 Modbus-Objekt

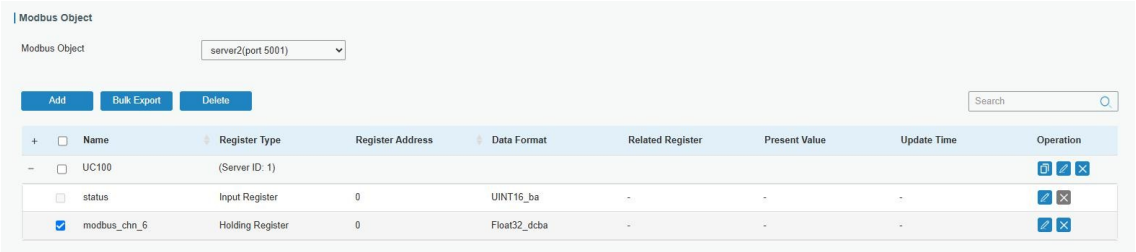


Abbildung 3-3-2-3

Element	Beschreibung
Modbus-Objekt	Wählen Sie den Modbus-Server aus, um die Objekte hinzuzufügen und zu bearbeiten.
Hinzufügen	Klicken Sie auf die gewünschten Objekte, um sie zu diesem Server hinzuzufügen. Das Gateway unterstützt das Hinzufügen von maximal 10.000 Objekten. **Hinweis:** Stellen Sie sicher, dass der Inhalt des Payload-Codecs korrekt ist und das

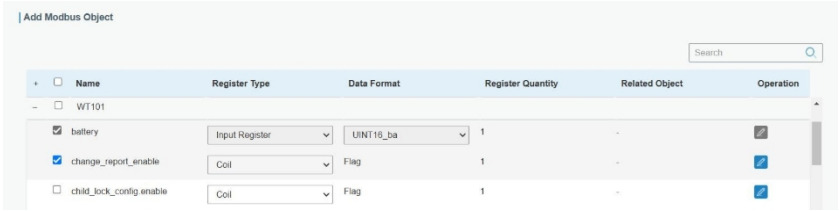
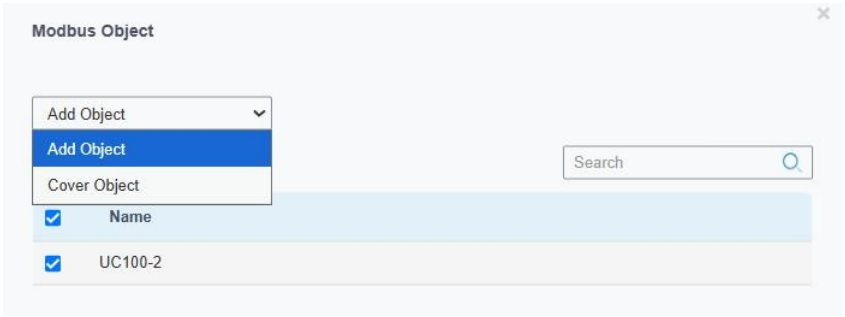
	Gerät den richtigen Payload-Codec auswählt. 
Massen-Export	Wählen Sie die gewünschten Objekte aus, die Sie als Datei im Format .xlsx exportieren möchten.
Löschen	Wählen Sie die Objekte aus, die Sie löschen möchten.
Name	Zeigen Sie den Namen dieses Objekts an.
Registrierungstyp	Zeigen Sie den Registrierungstyp dieses Objekts an.
Registeradresse	Zeigt die Registeradresse dieses Objekts an.
Datenformat	Zeigt das Datenformat dieses Objekts an.
Verwandtes Objekt	Zeigt die zugehörigen Objekte an.
Aktueller Wert	Zeigt den aktuellen Wert des Objekts an.
Aktualisierungszeit	Zeigen Sie die Zeit an, die dieses Objekt benötigt, um die Daten abzurufen und zu aktualisieren.
Vorgang	: Bearbeiten Sie das Objekt. : Löschen Sie das Objekt. : Wählen Sie die Objekte aus, die kopiert werden sollen, und klicken Sie auf dieses Symbol, um die Objekte zu anderen Geräten desselben Modells hinzuzufügen oder zu übertragen. **Objekt hinzufügen**: Fügen Sie die Objekte zu ausgewählten Geräten hinzu. **Objekt übertragen:** Übertragen Sie die Objekte auf ausgewählte Geräte. Die ursprünglichen Objekteinstellungen der ausgewählten Geräte werden dabei gelöscht. 

Tabelle 3-3-2-3 Modbus-Objektliste Parameter

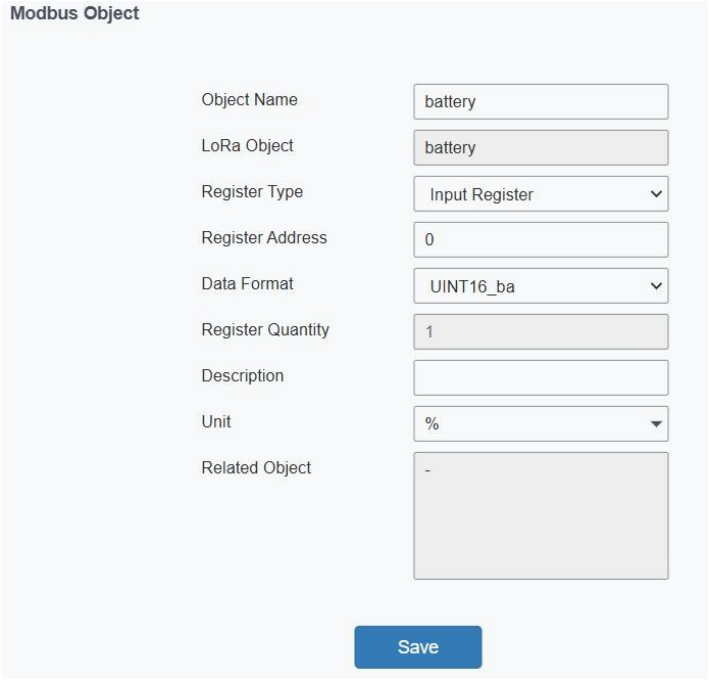


Abbildung 3-3-2-4

Modbus-Objektkonfiguration	
Element	**Beschreibung**
Objektname	Legen Sie einen eindeutigen Namen für dieses Objekt fest.
LoRa-Objekt	Zeigen Sie den entsprechenden Namen des LoRa-Objekts an.
Objektname	Legen Sie einen eindeutigen Namen für dieses Objekt fest.
Registrierungstyp	Wählen Sie den Modbus-Registertyp aus. **Diskreter Eingang:** schreibgeschützt, nur mit Status 0 und 1. **Spule:** lesbar und beschreibbar, nur mit Status 0 und 1. **Halte-Register:** lesbar und beschreibbar, einschließlich Analogwerten, Zeichenfolgen usw. **Eingangsregister:** schreibgeschützt, einschließlich Analogwerten, Zeichenfolgen usw.
Registeradresse	Beim Hinzufügen eines Objekts wird diese Adresse automatisch generiert. Diese Adresse kann geändert werden. Bereich: 0-65535 **Hinweis** 1) Die Adressen desselben Registertyps müssen in einem Modbus-Server unterschiedlich sein. 2) Die Adresse hängt von der Registeranzahl ab. Wenn die Adresse dieses Objekts 0 und die Registeranzahl 2 beträgt, muss die Adresse des nächsten Objekts 2 (0+2) oder höher sein.
Datenformat	Zeigen Sie das Datenformat dieses Objekts an oder wählen Sie es aus.
Registermenge	Zeigen Sie die belegte Menge dieses Objekts im Register an.
Beschreibung	Geben Sie die Beschreibung dieses Objekts ein.
Einheit	Wählen Sie die Einheit dieses Objekts aus.
Zugehöriges Register	Zeigen Sie die zugehörigen Register an. Beim Schreiben dieses Objekts sollten die zugehörigen Register zusammen geschrieben werden. Andernfalls kann dieses Objekt nicht geändert werden nicht geändert werden.

Tabelle 3-3-2-4 Modbus-Objekt-Konfigurationsparameter

3.4 Netzwerk

3.4.1 Schnittstelle

3.4.1.1 Port

Der Ethernet-Anschluss kann mit einem Ethernet-Kabel verbunden werden, um einen Internetzugang zu erhalten. Er unterstützt 3 Verbindungstypen.

- **Statische IP**: Konfigurieren Sie IP-Adresse, Netzmaske und 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**: Konfigurieren Sie die Ethernet-WAN-Schnittstelle als PPPoE-Client.

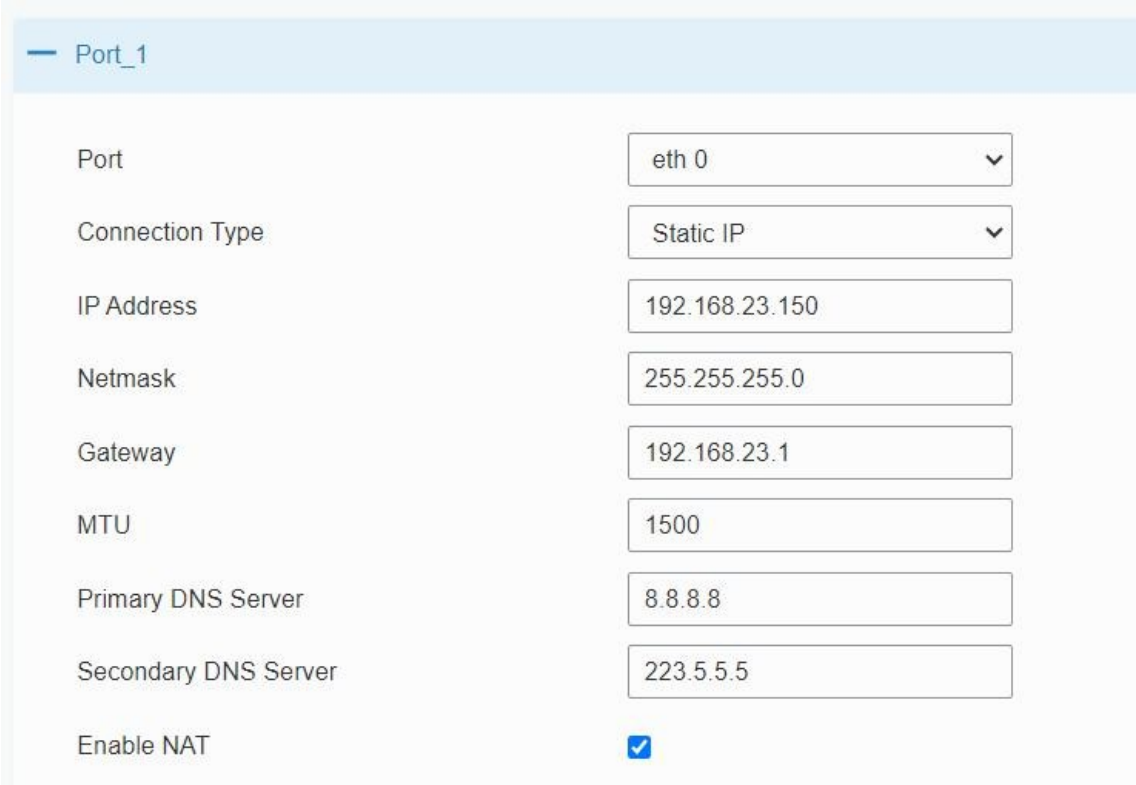


Abbildung 3-4-1-1

Port-Einstellung		
Element	**Beschreibung**	**Standard**
Port	Der Port, der als eth0-Port festgelegt und aktiviert ist.	eth 0
Verbindung Typ	Wählen Sie zwischen „Statische IP“, „DHCP-Client“ und „PPPoE“.	DHCP
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

Tabelle 3-4-1-1 Port-Parameter

Beispiel für die zugehörige Konfiguration

Ethernet-Verbindung

1. Statische IP-Konfiguration

Wenn das externe Netzwerk dem Ethernet-Port eine feste IP-Adresse zuweist, kann der Benutzer den Modus „Statische IP“ auswählen.

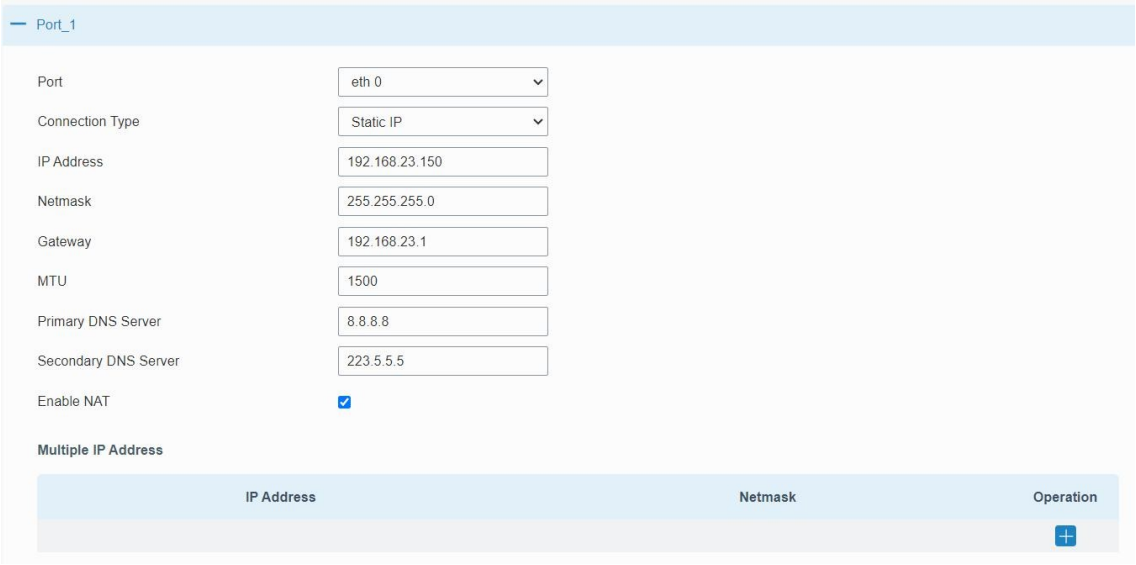


Abbildung 3-4-1-2

Statische IP		
Element	**Beschreibung**	**Standard**
IP-Adresse	Legen Sie die IP-Adresse fest, über die auf das Internet zugegriffen werden 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

Tabelle 3-4-1-2 Statische IP-Parameter

2. DHCP-Client

Wenn im externen Netzwerk ein DHCP-Server aktiviert ist und der Ethernet-WAN-Schnittstelle IP-Adressen zugewiesen wurden, kann der Benutzer den Modus „DHCP-Client“ auswählen, um die IP-Adresse automatisch zu beziehen.

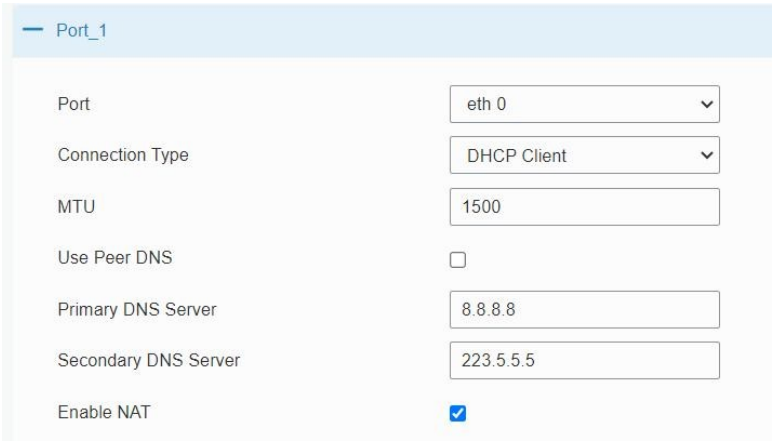


Abbildung 3-4-1-3

DHCP-Client	
Element	**Beschreibung**
Peer-DNS verwenden	Peer-DNS automatisch während der PPP-Einwahl beziehen. DNS ist erforderlich, wenn der Benutzer einen Domänennamen aufruft.

Tabelle 3-4-1-3 DHCP-Client-Parameter

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.

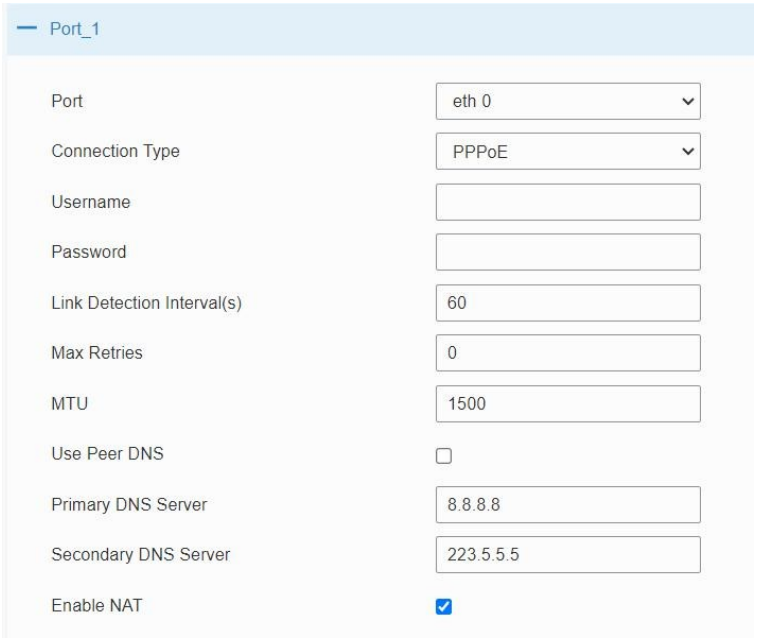


Abbildung 3-4-1-4

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	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.

Tabelle 3-4-1-4 PPPOE-Parameter

3.4.1.2 WLAN

In diesem Abschnitt wird erläutert, wie Sie die entsprechenden Parameter für das WLAN-Netzwerk einstellen. UG67 unterstützt 802.11 b/g/n im AP- oder Client-Modus.

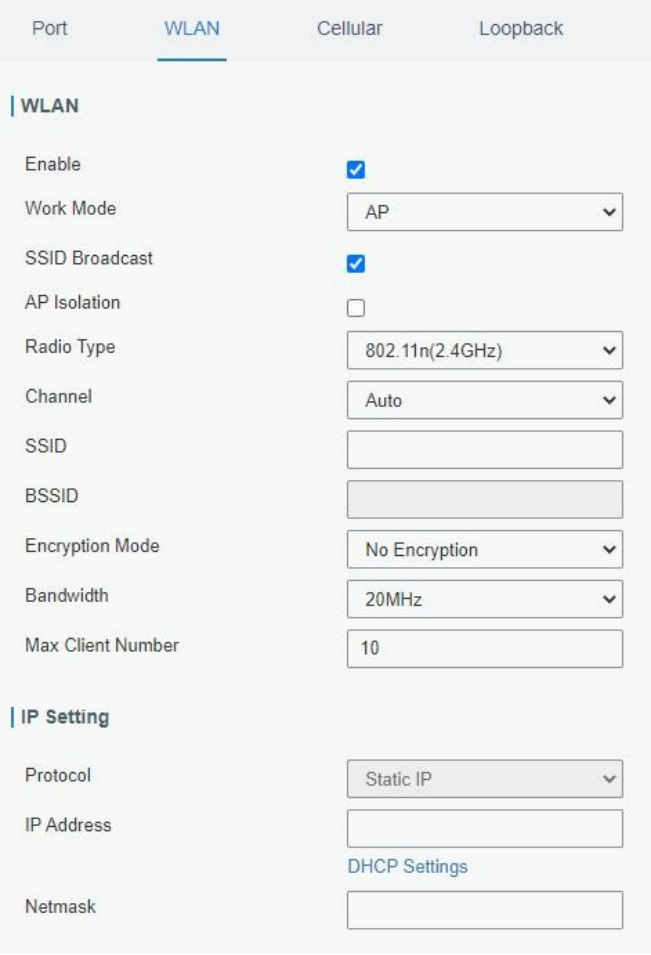


Abbildung 3-4-1-5

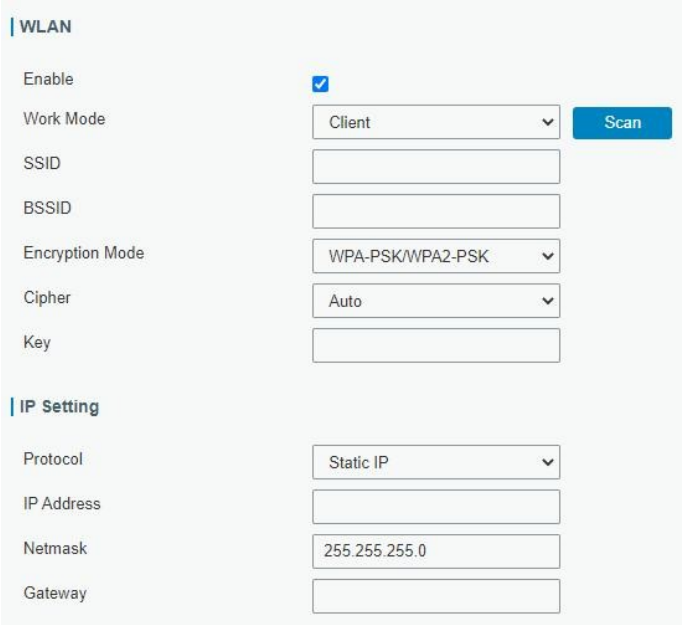


Abbildung 3-4-1-6

WLAN-Einstellungen	
Element	**Beschreibung**
Aktivieren	WLAN aktivieren/deaktivieren.
Arbeitsmodus	Wählen Sie den Arbeitsmodus des Gateways aus. Die Optionen sind „Client“ oder „AP“.
BSSID	Geben Sie die MAC-Adresse des Zugangspunkts ein. Entweder SSID oder BSSID eingegeben werden, um sich mit dem Netzwerk zu verbinden.
SSID	Geben Sie die SSID des Zugangspunkts ein.
Client-Modus	
Scannen	Klicken Sie auf die Schaltfläche „Scannen“, um nach einem Zugangspunkt in der Nähe zu suchen.
Verschlüsselungsmodus	Wählen Sie den Verschlüsselungsmodus aus. Die Optionen sind „Keine Verschlüsselung“, „WEP Open System“, „WEP Shared Key“, „WPA-PSK“, „WPA2-PSK“, „WPA-PSK/WPA2-PSK“, „WPA-Enterprise“, „WPA2-Enterprise“ und „WPA-Enterprise/WPA2-Enterprise“.
Verschlüsselung	Wählen Sie eine Verschlüsselung aus. Die Optionen sind „Auto“, „AES“, „TKIP“ und „AES/TKIP“.
Schlüssel	Geben Sie den vorab geteilten Schlüssel der WEP/WPA-Verschlüsselung ein.
XSupplicant-Typ	Wählen Sie zwischen „Peap“, „Leap“, „TLS“ und „TTLS“.
Benutzer	Geben Sie den Benutzer von WPA/WPA2-Enterprise ein.
Anonym Identität	Geben Sie die anonyme Identität von WPA/WPA2-Enterprise ein.
Phase2	Füllen Sie die Phase 2 von WPA/WPA2-Enterprise aus.
Öffentlicher Server Zertifikat	Das öffentliche Serverzertifikat, das für die Überprüfung mit dem WPA/WPA2-Enterprise-Zugangspunkt verwendet wird.
AP-Modus	
SSID-Übertragung	Wenn die SSID-Übertragung deaktiviert ist, können andere drahtlose Geräte nicht die SSID finden, und Benutzer müssen die SSID manuell eingeben, um

	auf das drahtlose Netzwerk zugreifen zu können.
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 Funktyp aus. Die Optionen sind „802.11b (2,4 GHz)“, „802.11g (2,4 GHz)”, „802.11n (2,4 GHz)””.
Kanal	Wählen Sie den Funkkanal aus. Die Optionen sind „Auto“, „1“, „2“ .....„11”.
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 WPA-Verschlüsselung ein. Das Standardpasswort lautet **„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 auf das Gateway zugreifen können, wenn als AP konfiguriert ist.
IP-Einstellung	
Protokoll	Legen Sie das Protokoll im drahtlosen Netzwerk fest.
IP-Adresse	Legen Sie die IP-Adresse im drahtlosen Netzwerk fest.
Netzmaske	Legen Sie die Netzmaske im drahtlosen Netzwerk fest.
Gateway	Legen Sie das Gateway im drahtlosen Netzwerk fest.

Tabelle 3-4-1-5 WLAN-Parameter

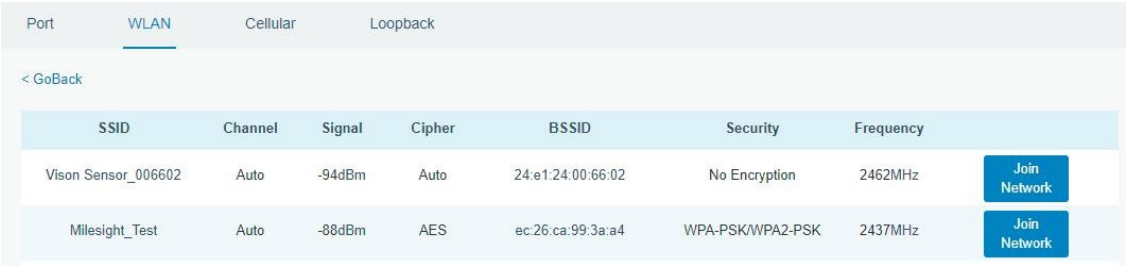


Abbildung 3-4-1-7

Client-Modus-Scan	
SSID	SSID anzeigen.
Kanal	Drahtlosen Kanal anzeigen.
Signal	Drahtloses Signal anzeigen.
BSSID	Zeigt die MAC-Adresse des Zugangspunkts an.
Sicherheit	Zeigt den Verschlüsselungsmodus an.
Frequenz	Zeigt die Funkfrequenz an.
Mit Netzwerk verbinden	Klicken Sie auf die Schaltfläche, um sich mit dem drahtlosen Netzwerk zu verbinden.

Tabelle 3-4-1-6 WLAN-Scan-Parameter

Verwandtes Thema

Beispiel für eine WLAN-Anwendung

3.4.1.3 Mobilfunk (nur Mobilfunkversion)

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

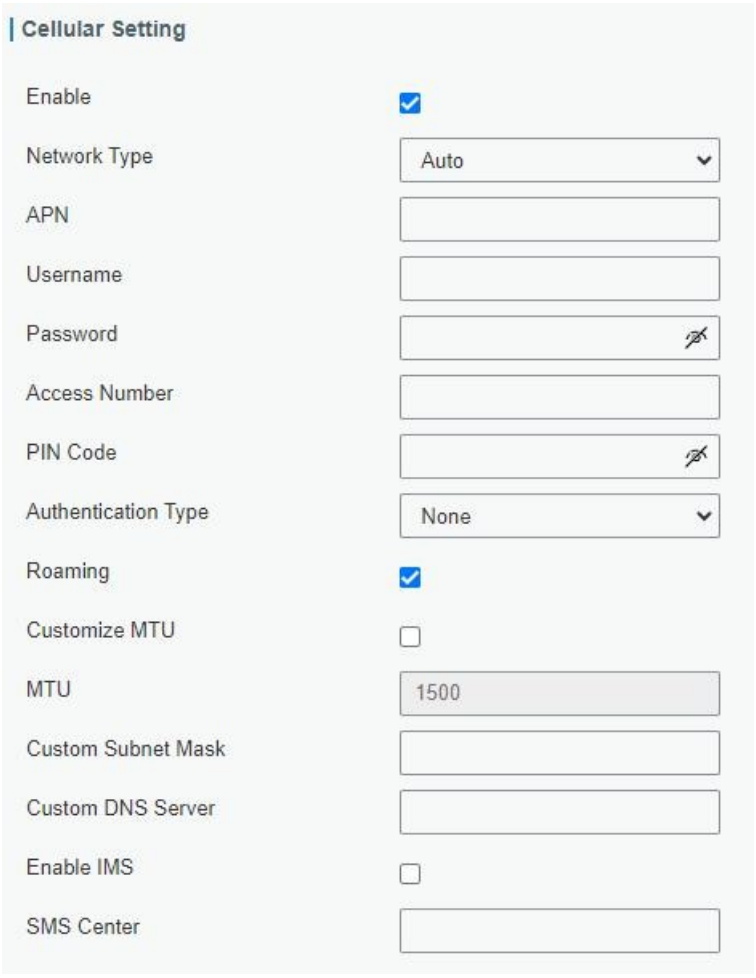


Abbildung 3-4-1-8

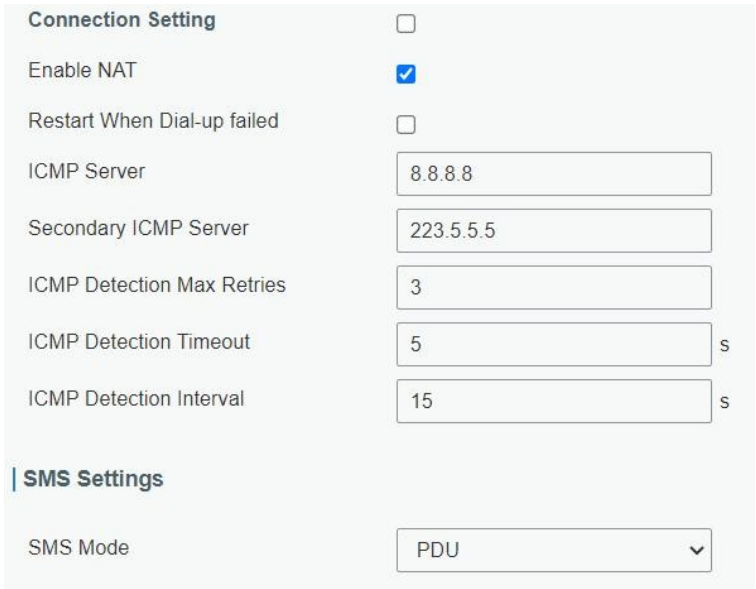


Abbildung 3-4-1-9

Allgemeine Einstellungen	
Element	**Beschreibung**
Aktivieren	Aktivieren Sie diese Option, um die Mobilfunkfunktion zu aktivieren.
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 von lokalen Internetdienstanbieters bereitgestellt wird.
Benutzername	Geben Sie den Benutzernamen für die Mobilfunk-Einwahlverbindung ein, die von Ihrem lokalen Internetdienstanbieter bereitgestellt wird.
Passwort	Geben Sie das Passwort für die Mobilfunk-Einwahlverbindung ein, das von Ihrem lokalen Internetdienstanbieter bereitgestellt wird.
Zugangsnummer	Geben Sie die Nummer der Einwahlzentrale für die Mobilfunk-Einwahlverbindung ein, die von lokalen Internetdienstanbieters.
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	Aktivieren oder deaktivieren Sie Roaming.
Angepasst MTU	Aktivieren oder deaktivieren Sie diese Option, um die maximalen Übertragungseinheiten anzupassen. Wenn deaktiviert, verwendet das Gerät die MTU-Einstellungen des Betreibers.
MTU	Legen Sie die maximalen Übertragungseinheiten fest. Bereich: 68-1500.
Benutzerdefinierte Subnetzmaske	Passen Sie die Subnetzmaske für Mobilfunk an. Wenn dieses Feld leer ist, verwendet das Gerät die von der Mobilfunkbasisstation bereitgestellte Subnetzmaske. **Hinweis:** Diese Funktion wird nur von bestimmten Mobilfunkmodulen unterstützt.
Benutzerdefiniertes DNS Server	Passen Sie den Mobilfunk-DNS-Server an. Wenn das Feld leer ist, verwendet das Gerät den DNS-Server des Mobilfunkanbieters.
IMS aktivieren	Aktivieren oder deaktivieren Sie die IMS-Funktion.
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, wird das Gateway automatisch neu gestartet, wenn die die Einwahl mehrmals fehlschlägt.
ICMP-Server	Legen Sie die IP-Adresse des ICMP-Erkennungsservers fest. **Hinweis:** Bitte wenden Sie sich an Ihren Internetdienstanbieter, um zu erfahren, ob die Ping-Erkennung zulässig ist, und um die richtigen ICMP-Serveradressen zu erhalten. Wenn die Ping-Erkennung nicht zulässig ist, lassen Sie dieses Feld leer.
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 festlegen.

SMS-Modus	Wählen Sie den SMS-Modus aus „TEXT“ und „PDU“ aus.

Tabelle 3-4-1-7 Mobilfunkparameter

Abbildung 3-4-1-10

Element	Beschreibung
Verbindungsmodus	
Verbindungsmodus	Wählen Sie zwischen „Immer online“ und „Bei Bedarf verbinden“.
Wiederwahlintervall(e)	Legen Sie das Zeitintervall zwischen den Wiederwahlversuchen 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.
Ausgelöst durch Anruf	Das Gateway wechselt automatisch vom Offline-Modus in den Mobilfunkmodus, wenn es einen Anruf von der angegebenen Telefonnummer erhält.
Anrufgruppe	Wählen Sie eine Anrufgruppe für die Anrufauslösung aus. Gehen Sie zu **„System“ > „Allgemeine 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 als Auslöser aus. Gehen Sie zu **System > Allgemein Einstellungen > Telefon**, um die SMS-Gruppe einzurichten.
SMS-Text	Geben Sie den SMS-Inhalt für den Auslöser ein.

Tabelle 3-4-1-8 Mobilfunkparameter

Verwandte Themen

Anwendungsbeispiel für Mobilfunkverbindung

Telefongruppe

3.4.1.4 Loopback

Die Loopback-Schnittstelle wird zum Ersetzen der Gateway-ID verwendet, solange sie aktiviert ist. Wenn die Schnittstelle „t “ auf „DOWN“ steht muss 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.

Abbildung 3-4-1-11

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

Tabelle 3-4-1-9 Loopback-Parameter

3.4.1.5 VLAN-Trunk

UG67-Gateway unterstützt den Ethernet-Port, der als VLAN-Trunk-Client fungiert und eine VLAN-ID zugewiesen bekommt, 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 leer, wenn

Standardmäßig können Sie einer bestimmten Schnittstelle ein neues VLAN-Label hinzufügen, indem Sie auf „  “ klicken.

Abbildung 3-4-1-12

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

Tabelle 3-4-1-10 VLAN-Trunk-Parameter

3.4.2 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 (von

Internet zum lokalen Netzwerk) und Ausgangsrichtung (vom lokalen Netzwerk zum Internet) entsprechend den Inhaltsmerkmalen der Pakete, wie Protokolltyp, Quell-/Ziel-IP-Adresse usw. Dadurch wird sichergestellt, dass das Gateway in einer sicheren Umgebung und der Host im lokalen Netzwerk betrieben werden.

3.4.2.1 Sicherheit

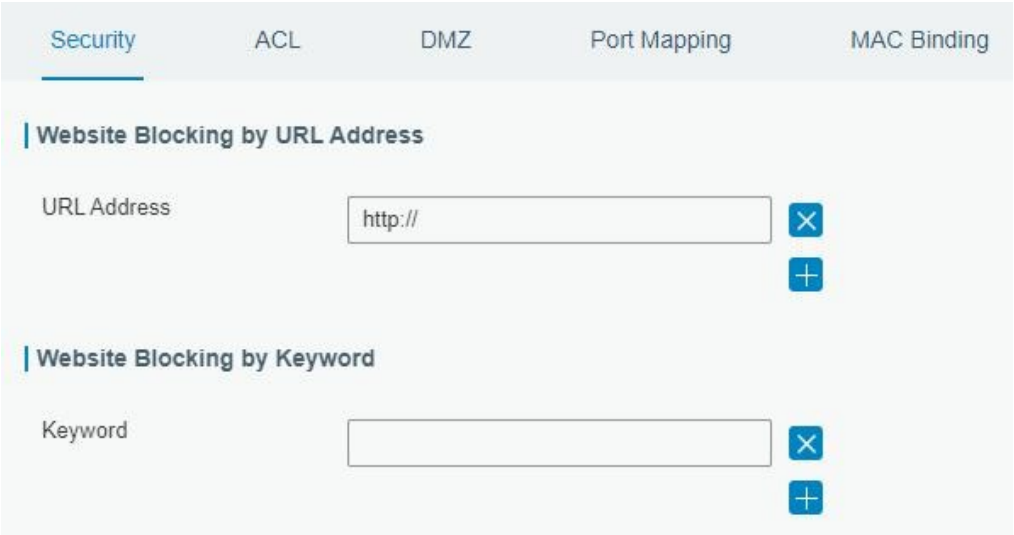


Abbildung 3-4-2-1

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

Tabelle 3-2-2-1 Sicherheitsparameter

3.4.2.2 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, wird das Feld gemäß der für die aktuelle Schnittstelle geltenden ACL-Regel analysiert. Nachdem das spezielle Paket identifiziert wurde, wird die Erlaubnis oder Verweigerung des entsprechenden Pakets gemäß der voreingestellten Strategie umgesetzt.
Die von ACL definierten Regeln für die Datenpaketzuordnung können auch von anderen Funktionen verwendet werden, die eine Unterscheidung des Datenflusses erfordern.

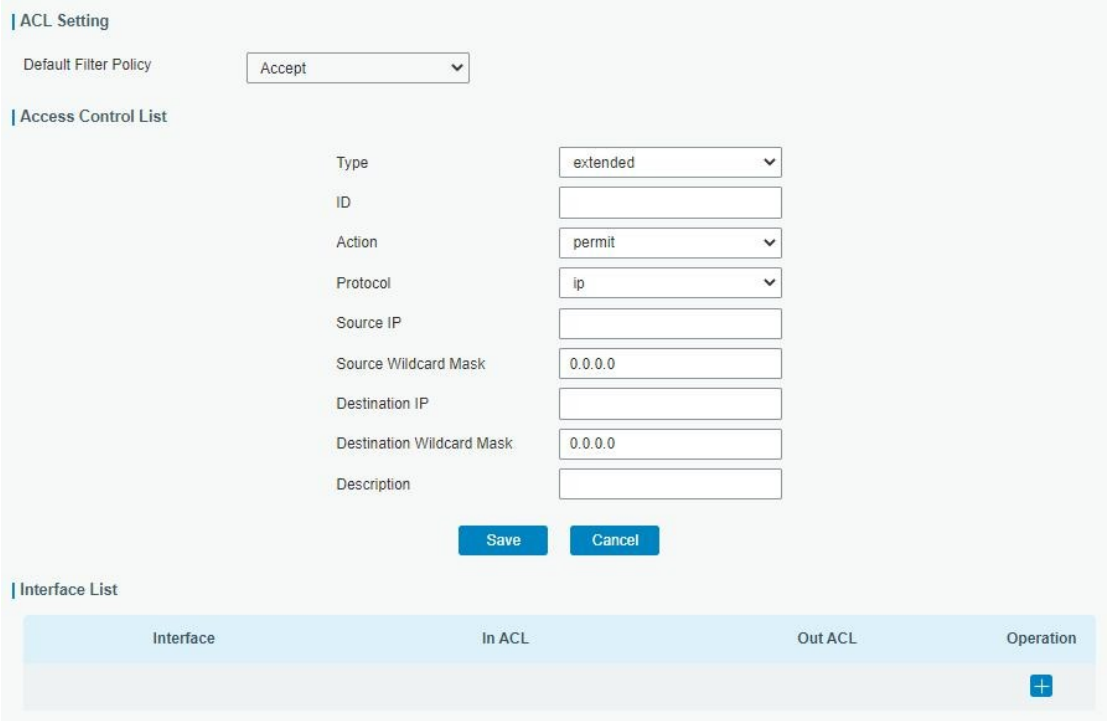


Abbildung 3-4-2-2

Element	Beschreibung
ACL-Einstellung	
Standardfilterrichtlinie	Wählen Sie zwischen „Akzeptieren“ und „Ablehnen“. 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, werden alle berücksichtigt).
Quell-Platzhalter 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. einen bestimmten Port, einen 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	Wählen Sie den Zielporttyp aus, z. B. angegebener Port, Portbereich,

Typ	usw.
Zielport	Legen Sie die Zielportnummer fest. Bereich: 1-65535.
Startziel Port	Legen Sie die Startnummer des Zielports fest. Bereich: 1-65535.
Endzielport	Endziel-Portnummer festlegen. 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.

Tabelle 3-4-2-2 ACL-Parameter

3.4.2.3 DMZ

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

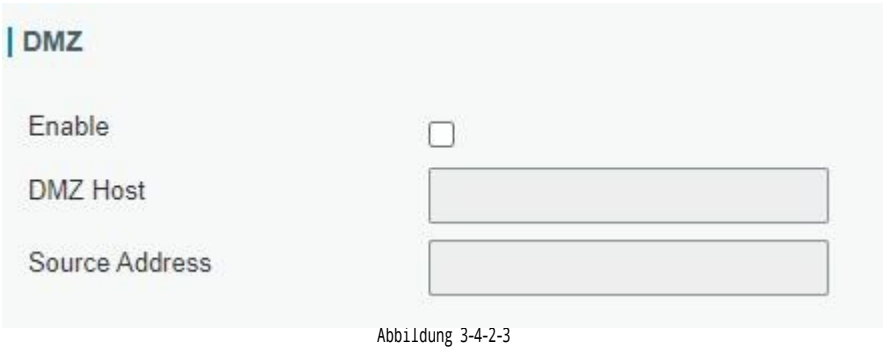


Abbildung 3-4-2-3

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“.

Tabelle 3-4-2-3 DMZ-Parameter

3.4.2.4 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. Anschließend wandelt er die Verbindung in eine interne Verbindung um. Diese Umwandlung wird als DNAT bezeichnet und wird hauptsächlich für externe und Intervalldienste verwendet.

Klicken Sie auf „ + “ , um neue Port-Mapping-Regeln hinzuzufügen.

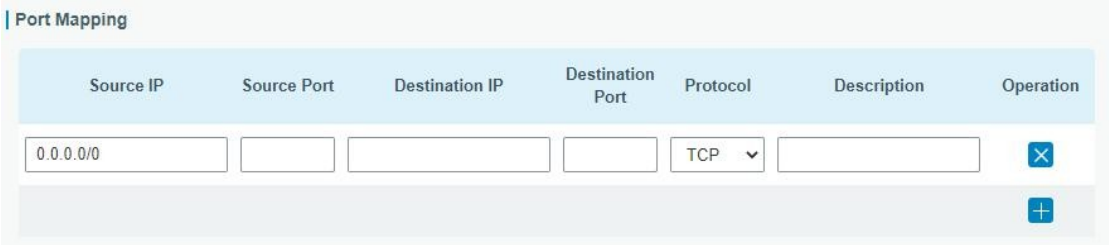


Abbildung 3-4-2-4

Portzuordnung	
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 weitergeleitet werden. Bereich: 1-65535.
Ziel-IP	Geben Sie die IP-Adresse ein, an die Pakete weitergeleitet werden, nachdem sie auf der eingehenden Schnittstelle empfangen wurden.
Zielport	Geben Sie den TCP- oder UDP-Port ein, an den Pakete weitergeleitet werden, nachdem Empfang an den eingehenden Ports weitergeleitet werden. Bereich: 1-65535.
Protokoll	Wählen Sie je nach Anforderung Ihrer Anwendung zwischen „TCP" und „UDP".
Beschreibung	Die Beschreibung dieser Regel.

Tabelle 3-4-2-4 Port-Mapping-Parameter

Beispiel für eine zugehörige Konfiguration

Beispiel für NAT-Anwendung

3.4.2.5 MAC-Bindung

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

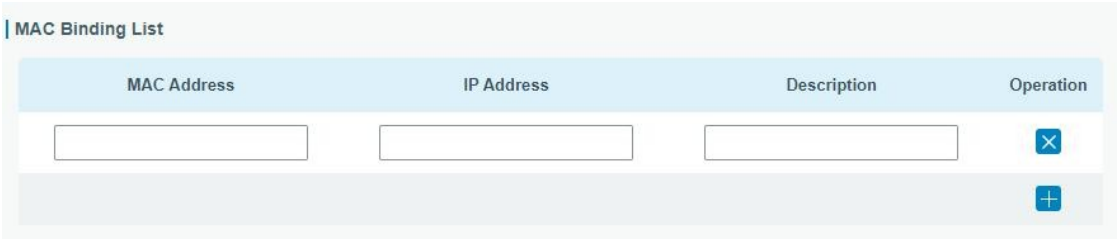


Abbildung 3-4-2-5

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-Element zu dokumentieren.

Tabelle 3-4-2-5 MAC-Bindungsparameter

3.4.3 DHCP

UG67 kann als DHCP-Server eingerichtet werden, um IP-Adressen zu verteilen, wenn Wi-Fi im AP-Modus arbeitet.

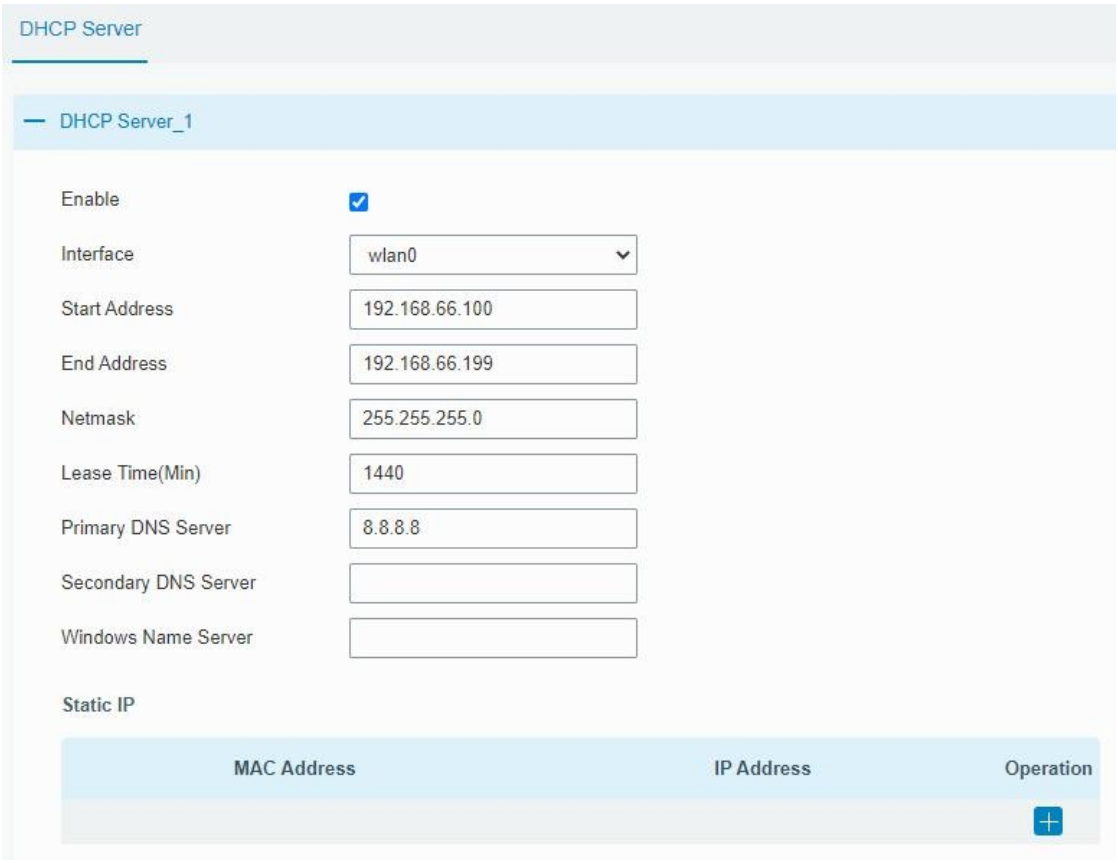


Abbildung 3-4-3-1

DHCP-Server		
Element	**Beschreibung**	**Standard**
Aktivieren	DHCP-Server aktivieren oder deaktivieren.	Aktiv
Schnittstelle	Nur die WLAN-Schnittstelle darf IP-Adressen verteilen zu verteilen.	wlan0
Start Adresse	Definieren Sie den Anfang des Pools von IP-Adressen , die an DHCP-Clients vergeben werden sollen.	192.168.1.100
Endadresse	Definieren Sie das Ende des Pools von IP-Adressen, 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 haben.	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	Sekundärer DNS-Server einstellen.	Null
Windows	Definieren Sie den erhaltenen Windows-Internetnamensdienst.	Null

Name Server	von DHCP-Clients vom DHCP-Server. Im Allgemeinen können Sie dieses Feld leer lassen.	
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 fest. Client (dieser sollte außerhalb des DHCP-Bereichs liegen).	Null

Tabelle 3-4-3-1 DHCP-Server-Parameter

3.4.4 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 einer Website eines geeigneten Domainnamenanbieters registrieren und einen Domainnamen beantragen.

Abbildung 3-4-4-1

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.

Tabelle 3-4-4-1 DDNS-Parameter

3.4.5 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-Vorgangs zu verfolgen.

3. Definieren Sie Anwendungen, die mit Track-Objekten verbunden sind, wie VRRP oder statisches Routing.

3.4.5.1 SLA

Die SLA-Einstellung wird zum Konfigurieren der Link-Probe-Methode verwendet. Der Standard-Probe-Typ ist ICMP.

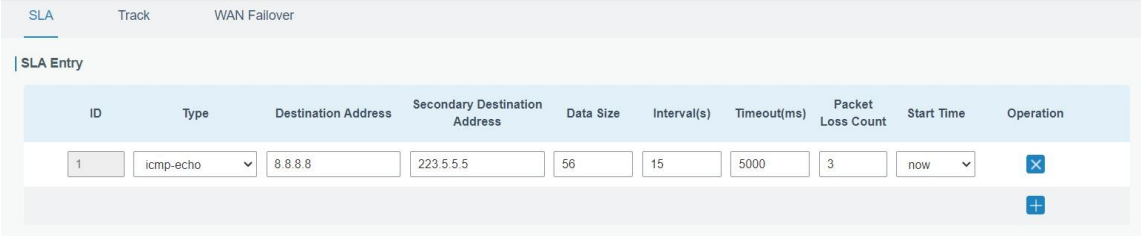


Abbildung 3-4-5-1

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	Startzeit der Erkennung; wählen Sie zwischen „Jetzt“ und einem Leerzeichen. Ein Leerzeichen bedeutet, dass die SLA-Erkennung Erkennung nicht gestartet wird.	Jetzt

Tabelle 3-4-5-1 SLA-Parameter

3.4.5.2 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 dient zur Erkennung des Verbindungsstatus, der Netzwerkleistung und zur Benachrichtigung des Track-Moduls. Die Erkennungsergebnisse helfen dabei, den Status

rechtzeitig zu verfolgen.

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

Verknüpfung 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 es eine sofortige Benachrichtigung an das Anwendungsmodul sendet, kann die Kommunikation unter bestimmten Umständen aufgrund von Routing-Fehlern wie zeitlicher 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 Track-Elements ändert.

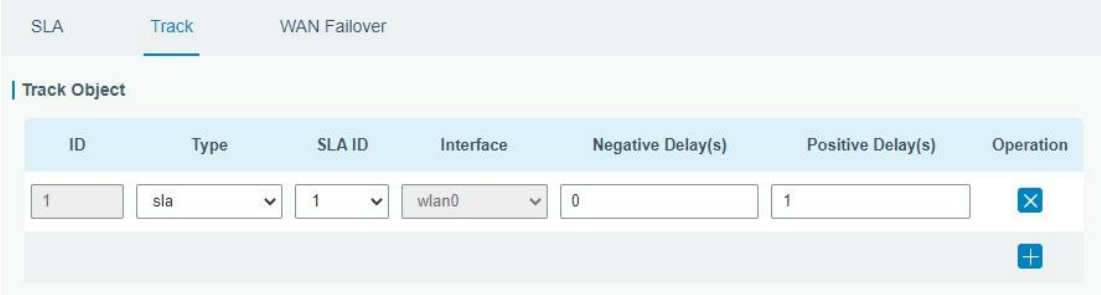


Abbildung 3-4-5-2

Element	Beschreibung	Standard
Index	Track-Index. Es können bis zu 10 Track-Einstellungen 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.	cellular0
Negative Verzögerung (s)	Wenn die Schnittstelle ausgefallen ist oder die SLA-Prüfung fehlschlägt, wird entsprechend der hier eingestellten Zeit gewartet, bevor der Status tatsächlich auf „Ausgefallen” geändert wird. Bereich: 0-180 (0 bezieht sich auf sofortige Umschaltung).	0
Positive Verzögerung (s)	Bei einer Fehlerbehebung wird entsprechend der hier eingestellten Zeit gewartet, bevor der Status tatsächlich auf „Up“ (Aktiv) geändert wird. Bereich: 0-180 (0 bedeutet sofortiges Umschalten).	1

Tabelle 3-4-5-2 Track-Parameter

3.4.5.3 WAN-Failover

WAN-Failover bezieht sich auf das Failover zwischen der Ethernet-WAN-Schnittstelle und der Mobilfunkschnittstelle. Wenn die Dienstübertragung aufgrund einer Fehlfunktion einer bestimmten

Schnittstelle oder mangelnde Bandbreite kann die Übertragungsrate schnell auf die Backup-Schnittstelle umgeschaltet werden. Dann übernimmt die Backup-Schnittstelle die Übertragung der Dienste und teilt sich den Netzwerkfluss, um die Zuverlässigkeit der Kommunikation der Datenausrüstung zu verbessern.

Wenn der Verbindungsstatus der Hauptschnittstelle von „up" auf „down" 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 „down" ist, schaltet das System auf die Verbindung der Backup-Schnittstelle um. Andernfalls bleibt das System unverändert.

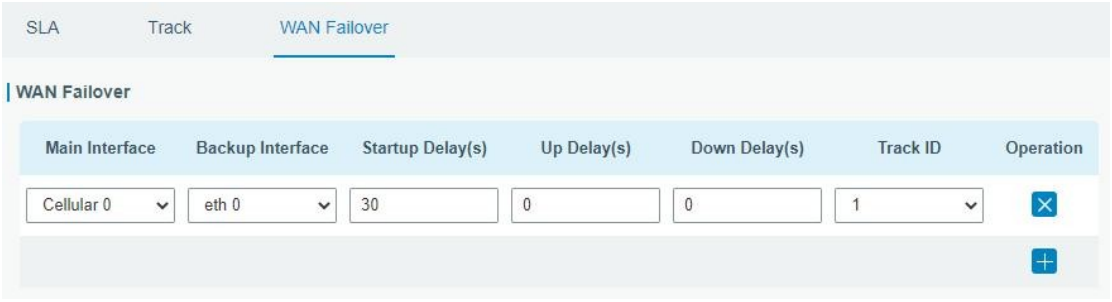


Abbildung 3-4-5-3

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.	--

Tabelle 3-4-5-3 WAN-Failover-Parameter

3.4.6 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.

UG67 unterstützt DMVPNIPsec, GRE, L2TP, PPTP, OpenVPN sowie GRE über IPsec und L2TP über IPsec.

3.4.6.1 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.

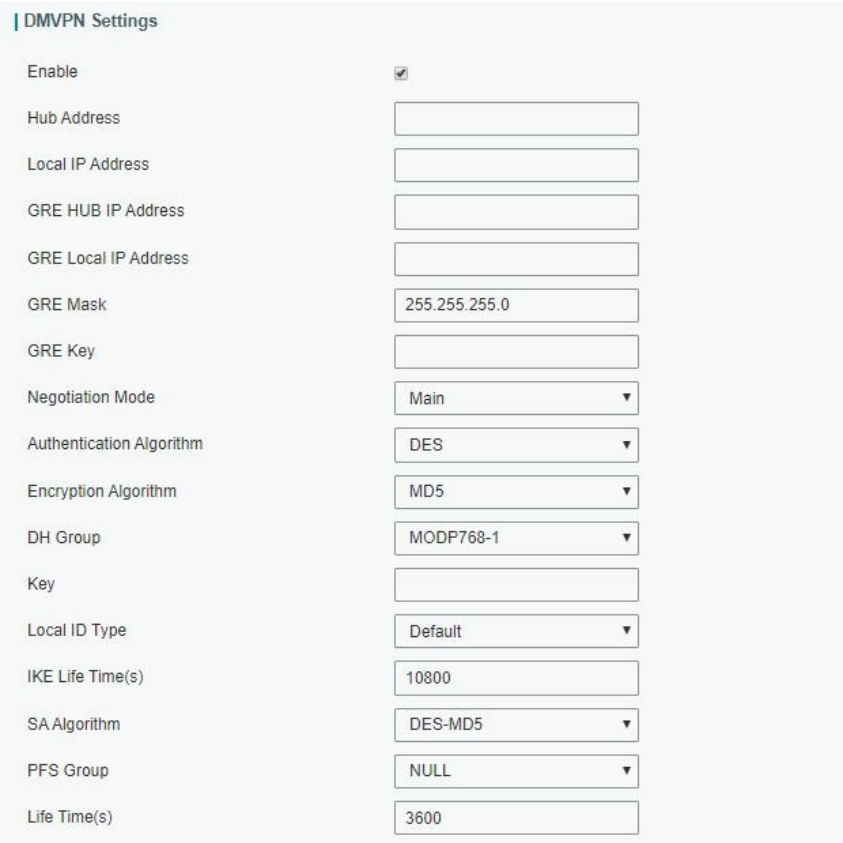


Abbildung 3-4-6-1

Abbildung 3-4-6-2

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	GRE-lokale Tunnel-Netzmaske.
GRE-Schlüssel	GRE-Tunnelschlüssel.
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 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)	DPD-Intervallzeit einstellen
DPD-Zeitüberschreitung (s)	DPD-Zeitüberschreitung festlegen.
Cisco-Geheimnis	Cisco Nhrp-Schlüssel.
NHRP-Haltezeit (s)	Die Haltezeit des Nhrp-Protokolls.

Tabelle 3-4-6-1 DMVPN-Parameter

3.4.6.2 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 Sicherheitsdienste zur Auswahl: 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.

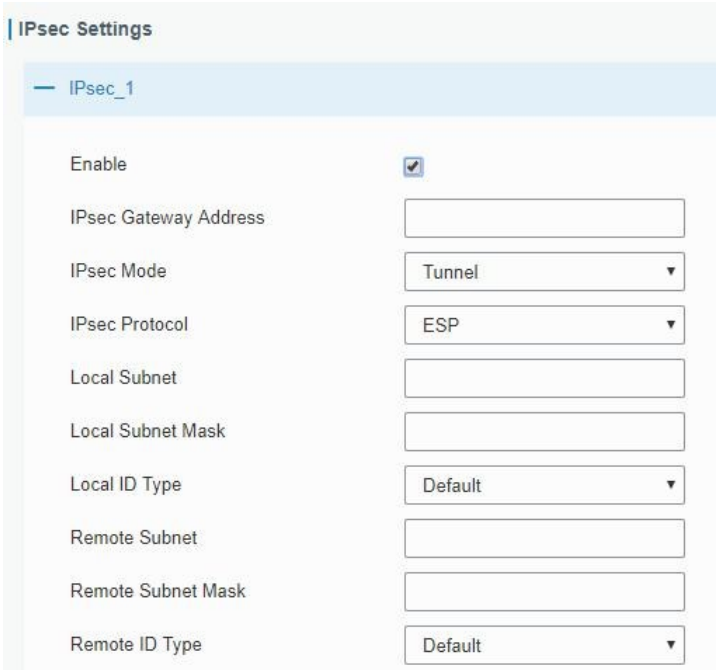


Abbildung 3-4-6-3

IPsec

Element	Beschreibung
Aktivieren	IPsec-Tunnel aktivieren. Es sind maximal 3 Tunnel zulässig.
IPsec-Gateway-Adresse	Geben Sie die IP-Adresse oder den Domänennamen des Remote-IPsec-Servers ein. .
IPsec-Modus	Wählen Sie zwischen „Tunnel“ und „Transport“.
IPsec-Protokoll	Wählen Sie zwischen „ESP“ und „AH“.
Lokales Subnetz	Geben Sie die IP-Adresse des lokalen Subnetzes ein, das durch IPsec geschützt wird.
Lokale Subnetz-Netzmaske	Geben Sie die lokale Netzmaske ein, die durch IPsec geschützt wird.
Lokaler ID-Typ	Wählen Sie zwischen „Standard“, „ID“, „FQDN“ und „Benutzer-FQDN“.
Remote-Subnetz	Geben Sie die IP-Adresse des Remote-Subnetzes ein, das durch IPsec geschützt ist.
Remote-Subnetzmaske	Geben Sie die Remote-Netzmaske ein, die durch IPsec geschützt wird.
Remote-ID-Typ	Wählen Sie zwischen „Standard“, „ID“, „FQDN“ und „Benutzer-FQDN“.

Tabelle 3-4-6-2 IPsec-Parameter

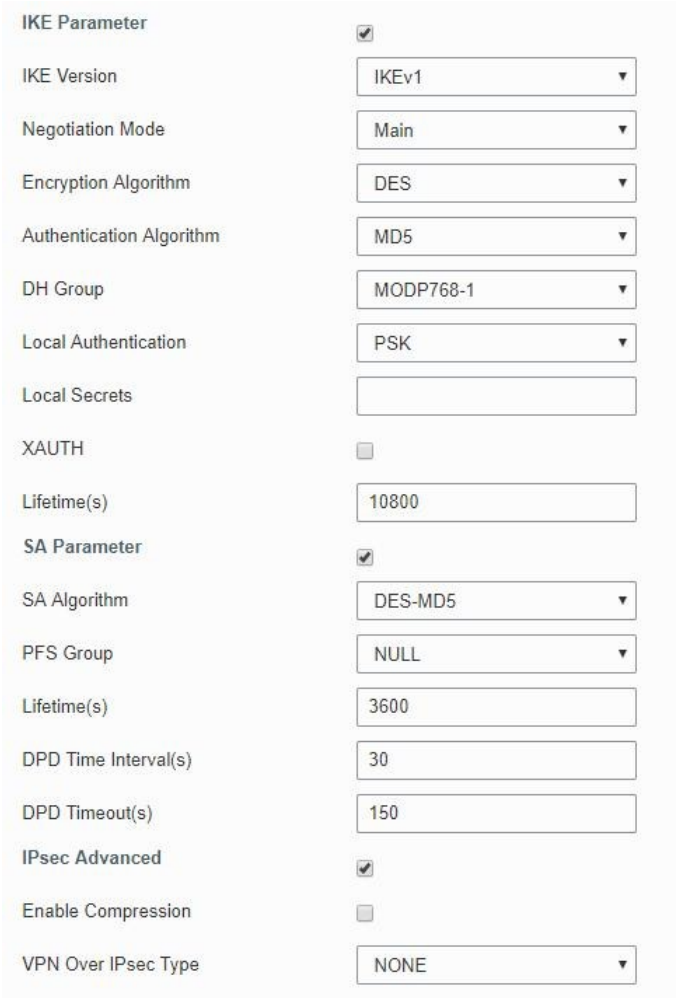


Abbildung 3-4-6-4

IKE-Parameter	
Element	**Beschreibung**
IKE-Version	Wählen Sie zwischen „IKEv1“ und „IKEv2“.
Verhandlungsmodus	Wählen Sie zwischen „Main“ und „Aggressive“.
Verschlüsselungsalgorithmus	Wählen Sie zwischen „DES“, „3DES“, „AES128“, „AES192“ und „AES256“.

Authentifizierung Algorithmus	Wählen Sie zwischen „MD5“ und „SHA1“.
DH-Gruppe	Wählen Sie zwischen „MODP768_1”, „MODP1024_2” und „MODP1536_5”.
Lokale Authentifizierung	Wählen Sie zwischen „PSK“ und „CA“.
Lokale Geheimnisse	Geben Sie den vorab geteilten Schlüssel ein.
XAUTH	Geben Sie den XAUTH-Benutzernamen und das Passwort ein, 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(en)	Legen Sie die DPD-Intervallzeit fest, um zu erkennen, ob die Gegenstelle ausfällt.
DPD-Zeitüberschreitung(en)	Legen Sie das DPD-Zeitlimit fest. 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 VPN über IPsec-Funktion zu aktivieren.

Tabelle 3-4-6-3 IPsec-Parameter

3.4.6.3 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 die Verschlüsselung von Multicast nicht realisieren.
- Ein bestimmtes Protokoll kann nicht geroutet werden.
- Ein Netzwerk mit unterschiedlichen IP-Adressen ist erforderlich, um zwei andere ähnliche Netzwerke miteinander zu verbinden.

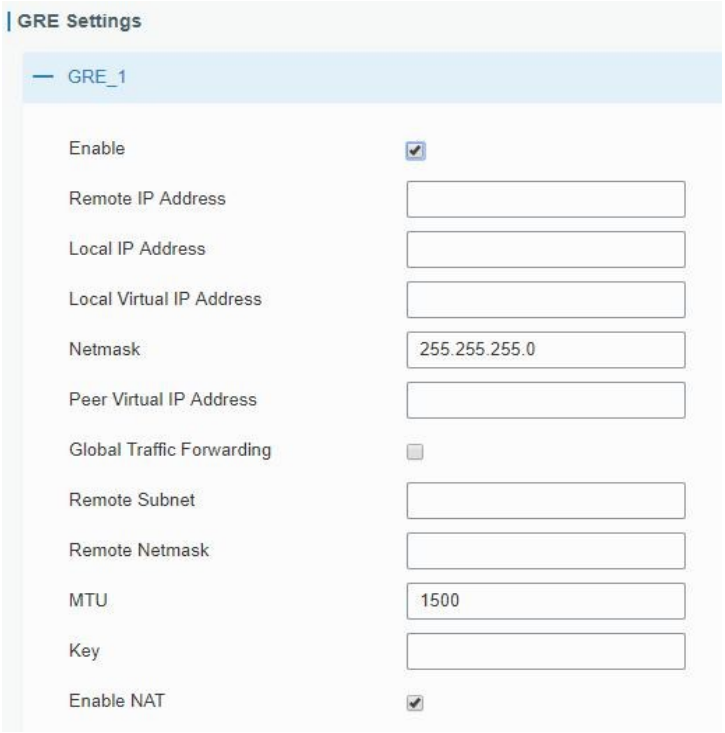


Abbildung 3-4-6-5

GRE	
Element	**Beschreibung**
Aktivieren	Aktivieren Sie diese Option, um die GRE-Funktion zu aktivieren.
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 einen GRE-Tunnel gesendet, wenn diese Funktion aktiviert ist.
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.

Tabelle 3-4-6-4 GRE-Parameter

3.4.6.4 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.

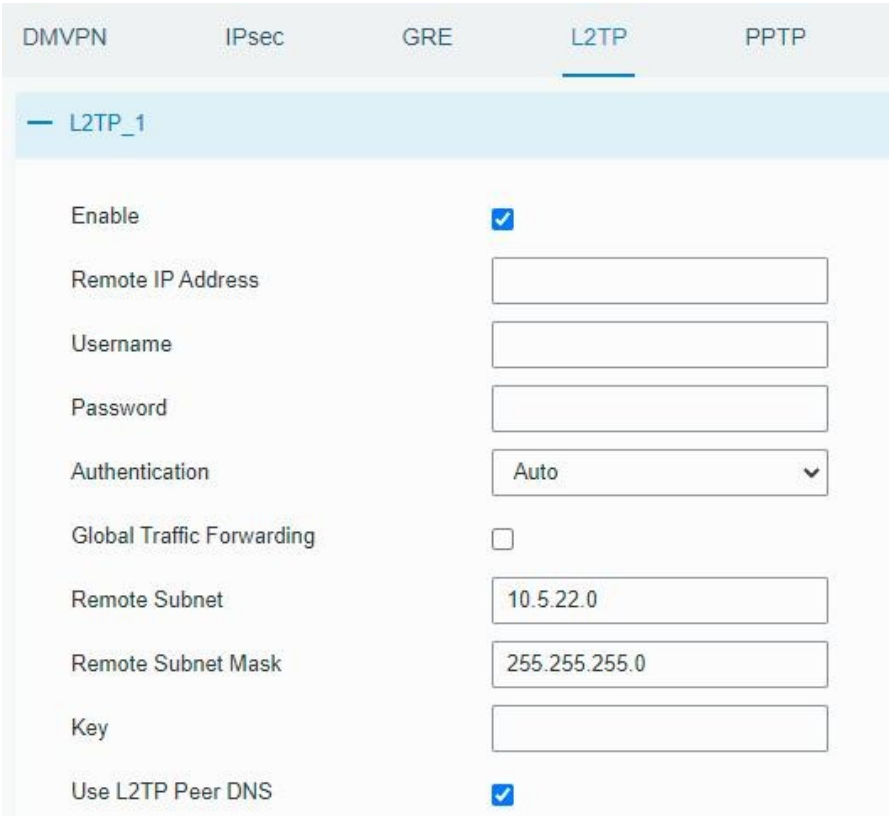


Abbildung 3-4-6-6

L2TP	
Element	**Beschreibung**
Aktivieren	Aktivieren Sie diese Option, um die L2TP-Funktion zu aktivieren.
Remote-IP-Adresse	Geben Sie die öffentliche IP-Adresse oder den Domänennamen des 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 zwischen „Auto“, „PAP“, „CHAP“, „MS-CHAPv1“ und „MS-CHAPv2“ aus.
Globaler Datenverkehr Weiterleitung	Der gesamte Datenverkehr wird über einen L2TP-Tunnel gesendet, sobald diese Funktion aktiviert ist.
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.

Tabelle 3-4-6-5 L2TP-Parameter

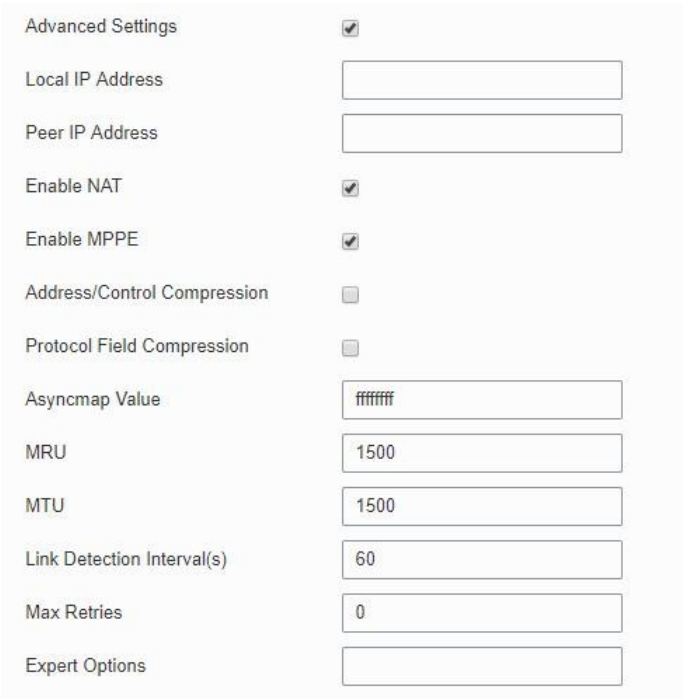


Abbildung 3-4-6-7

Erweiterte Einstellungen	
Element	**Beschreibung**
Lokale IP-Adresse	Tunnel-IP-Adresse des L2TP-Clients festlegen. Der Client erhält die Tunnel-IP-Adresse automatisch vom Server, wenn sie null ist.
Peer-IP-Adresse	Geben Sie die Tunnel-IP-Adresse des L2TP-Servers ein.
NAT aktivieren	Aktivieren Sie die NAT-Traversal-Funktion.
MPPE aktivieren	MPPE-Verschlüsselung aktivieren.
Adresse/Steuerung Komprimierung	Für die PPP-Initialisierung. Der Benutzer kann die Standardoption beibehalten.
Protokollfeld Komprimierung	Für die PPP-Initialisierung. Der Benutzer kann die Standardoption beibehalten.
Asyncmap-Wert	Eine der PPP-Protokoll-Initialisierungszeichenfolgen. Der Benutzer kann Der Standardwert. Bereich: 0-ffffffff.
MRU	Legt die maximale Empfangseinheit fest. Bereich: 64-1500.
MTU	Legt die maximale Übertragungseinheit fest. Bereich: 128-1500
Link-Erkennungsintervall (s)	Legen Sie das Verbindungserkennungsintervall fest, um die Tunnelverbindung sicherzustellen Verbindung. Bereich: 0-600.
Maximale Wiederholungsversuche	Legen Sie die maximale Anzahl von Wiederholungsversuchen fest, um den L2TP-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.

Tabelle 3-4-6-6 L2TP-Parameter

3.4.6.5 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.

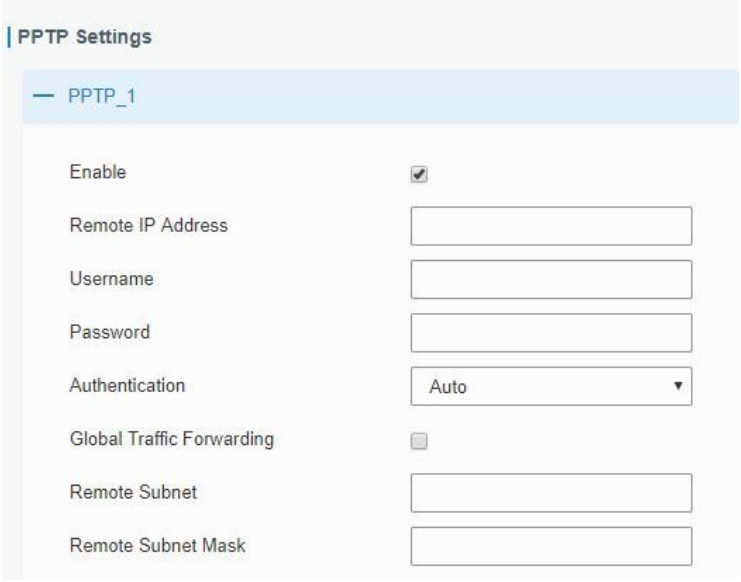


Abbildung 3-4-6-8

PPTP	
Element	**Beschreibung**
Aktivieren	PPTP-Client aktivieren. Es sind maximal 3 Tunnel zulässig.
Remote-IP-Adresse	Geben Sie die öffentliche IP-Adresse oder den Domänennamen des 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 zwischen „Auto", „PAP", „CHAP", „MS-CHAPv1" und „MS-CHAPv2" aus.
Globaler Datenverkehr Weiterleitung	Der gesamte Datenverkehr wird über den PPTP-Tunnel gesendet, sobald Sie diese Funktion aktivieren.
Remote-Subnetz	Legen Sie das Peer-Subnetz von PPTP fest.
Remote-Subnetz Maske	Legen Sie die Netzmaske des Peer-PPTP-Servers fest.

Tabelle 3-4-6-7 PPTP-Parameter

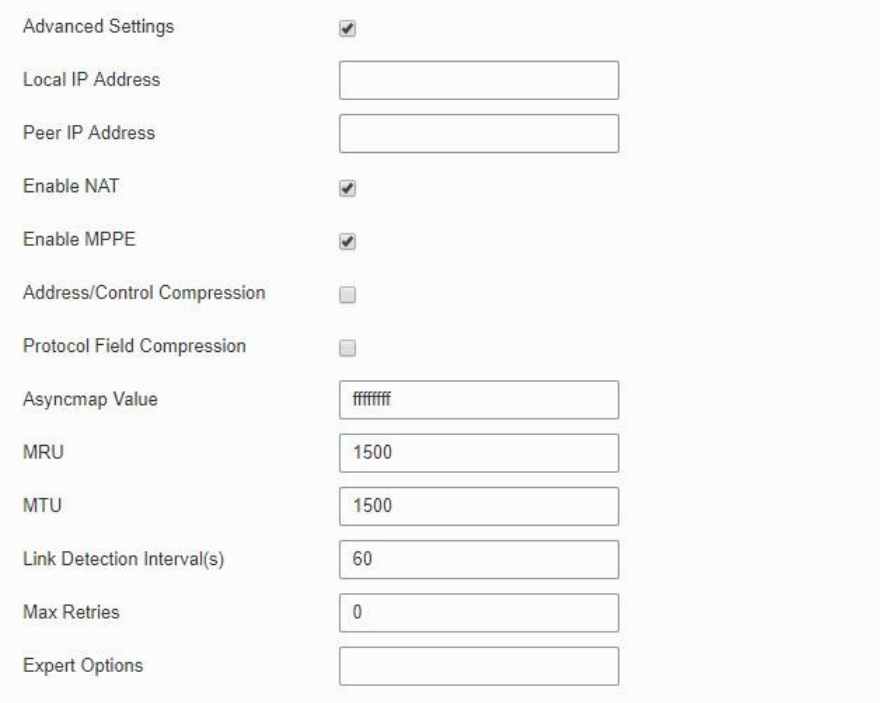


Abbildung 3-4-6-9

Erweiterte PPTP-Einstellungen	
Element	**Beschreibung**
Lokale IP-Adresse	Legen Sie die IP-Adresse des PPTP-Clients fest.
Peer-IP-Adresse	Geben Sie die Tunnel-IP-Adresse des PPTP-Servers ein.
NAT aktivieren	Aktivieren Sie die NAT-Funktion von PPTP.
MPPE aktivieren	MPPE-Verschlüsselung aktivieren.
Adresse/Steuerung Komprimierung	Für die PPP-Initialisierung. Der Benutzer kann die Standardoption beibehalten.
Protokollfeld Komprimierung	Für die PPP-Initialisierung. Der Benutzer kann die Standardoption beibehalten.
Asyncmap-Wert	Eine der Initialisierungszeichenfolgen für das PPP-Protokoll. Der Benutzer kann den Standardwert beibehalten. Bereich: 0-ffffffff.
MRU	Geben Sie die maximale Empfangseinheit ein. Bereich: 64-1500.
MTU	Geben Sie die maximale Übertragungseinheit ein. Bereich: 128-1500.
Link-Erkennungsintervall (s)	Stellen Sie das Link-Erkennungsintervall ein, um die Tunnelverbindung sicherzustellen Verbindung. Bereich: 0-600.
Maximale 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.

Tabelle 3-4-6-8 PPTP-Parameter

3.4.6.6 OpenVPN-Client

OpenVPN ist ein Open-Source-Produkt für virtuelle private Netzwerke (VPN), das ein vereinfachtes Sicherheitsframework, ein modulares Netzwerkdesign und plattformübergreifende Portabilität bietet. UG67

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

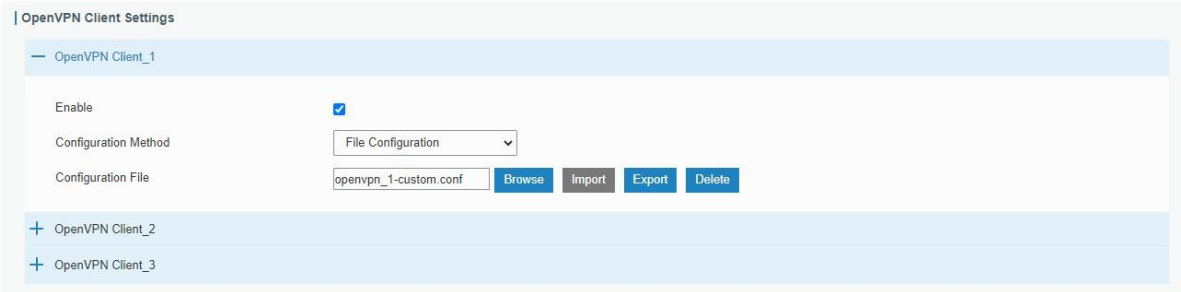


Abbildung 3-4-6-10

OpenVPN-Client – Dateikonfiguration	
Element	**Beschreibung**
Durchsuchen	Klicken Sie hier, um die Client-Konfigurationsdatei im OVPN-Format einschließlich der Einstellungen und Zertifikatsinhalte zu durchsuchen. Bitte beachten Sie die Client-Konfigurationsdatei gemäß dem Beispiel: client.conf
Bearbeiten	Klicken Sie hier, um die importierte Datei zu bearbeiten.
Export	Exportieren Sie die Serverkonfigurationsdatei.
Löschen	Klicken Sie hier, um die Konfigurationsdatei zu löschen.

Tabelle 3-4-6-9 OpenVPN-Client-Parameter

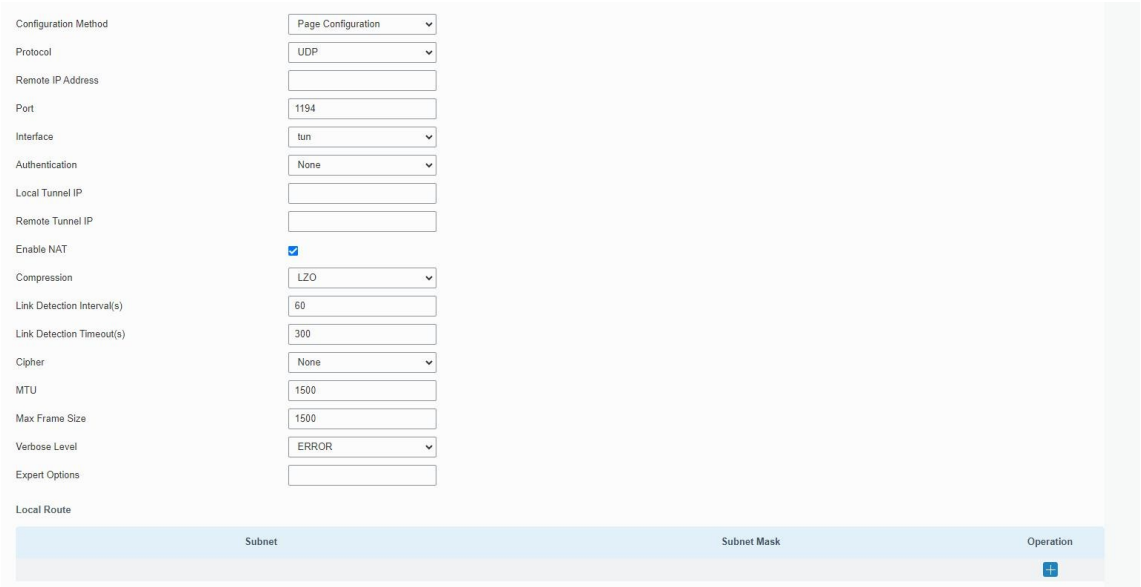


Abbildung 3-4-6-11

OpenVPN-Client – Seitenkonfiguration	
Element	**Beschreibung**
Protokoll	Wählen Sie ein Transportprotokoll aus, das durch die Verbindung von UDP und TCP verwendet wird.
Remote-IP-Adresse	Geben Sie die IP-Adresse oder den Domänennamen des Remote-OpenVPN-Servers ein.
Port	Geben Sie die TCP/UCP-Servicenummer des Remote-OpenVPN-Servers ein. Bereich: 1-65535
Schnittstelle	Wählen Sie den Typ der virtuellen VPN-Netzwerkschnittstelle aus TUN und TAP aus. TUN-Geräte

	Geräte kapseln IPv4 oder IPv6 (OSI-Schicht 3), während TAP-Geräte Ethernet 802.3 (OSI-Schicht 2) kapseln.
Authentifizierungstyp	Wählen Sie den Authentifizierungstyp aus, der zur Sicherung von Datensitzungen verwendet wird. **Vorab geteilt:** Verwenden Sie denselben geheimen Schlüssel wie der Server, um die Authentifizierung abzuschließen. Gehen Sie nach der Auswahl zur Seite **„Netzwerk > VPN > Zertifizierungen“**, um eine statische Datei in das Feld **„PSK“** 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 > Zertifikate“**, 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 X.509-Zertifikat als Authentifizierungstyp.
Lokale virtuelle IP	Legen Sie die lokale Tunneladresse fest, wenn der Authentifizierungstyp **„Keine“** oder **„Vorab geteilt“** ist.
Virtuelle Remote-IP	Remote-Tunneladresse festlegen, wenn der Authentifizierungstyp **„Keine“** oder **„Pre-shared“ 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“ lautet. 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 diesen Formatstring in der Expertenoption hinzu: tls-crypt /etc/openvpn/openvpn-client1-ta.key
Komprimierung	Wählen Sie diese Option, um LZO zur Komprimierung von Daten zu aktivieren oder zu deaktivieren.
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 festgelegt ist, überschreibt der vom Server übermittelte 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 und dem Client festgelegt ist, überschreibt der vom Server übertragene 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:** ncp-ciphers AES-128-GCM,Schlüsselrichtung 1
Lokale Route	
Subnetz	Legen Sie die IP-Adresse der lokalen Route fest.
Subnetzmaske	Legen Sie die Netzmaske der lokalen Route fest.

Tabelle 3-4-6-10 OpenVPN-Client-Parameter

3.4.6.7 OpenVPN-Server

UG67 unterstützt OpenVPN-Server zum Erstellen sicherer Punkt-zu-Punkt- oder Standort-zu-Standort-Verbindungen in gerouteten oder gebrückten Konfigurationen und Fernzugriffsfunktionen. Sie können die ovpn-Datei direkt importieren oder die Parameter auf dieser Seite konfigurieren, um diesen Server einzurichten.

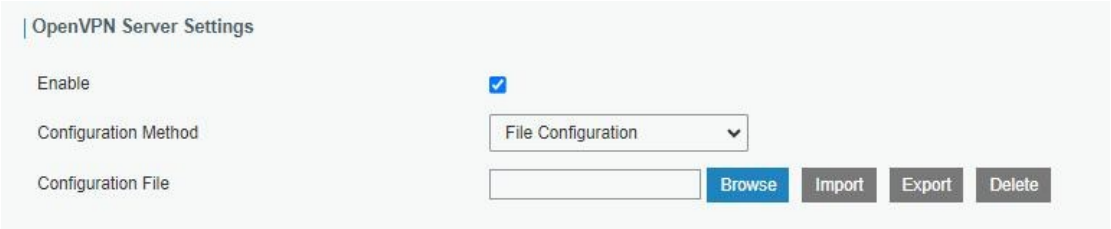


Abbildung 3-4-6-12

OpenVPN-Server – Dateikonfiguration	
Element	**Beschreibung**
Durchsuchen	Klicken Sie hier, um die Serverkonfigurationsdatei im OVPN-Format einschließlich der Einstellungen und Zertifikatsinhalte. Bitte beachten Sie die Serverkonfigurationsdatei gemäß dem Beispiel: server.conf
Bearbeiten	Klicken Sie hier, um die importierte Datei zu bearbeiten.
Export	Exportieren Sie die Serverkonfigurationsdatei.
Löschen	Klicken Sie hier, um die Konfigurationsdatei zu löschen.

Tabelle 3-4-6-11 OpenVPN-Serverparameter

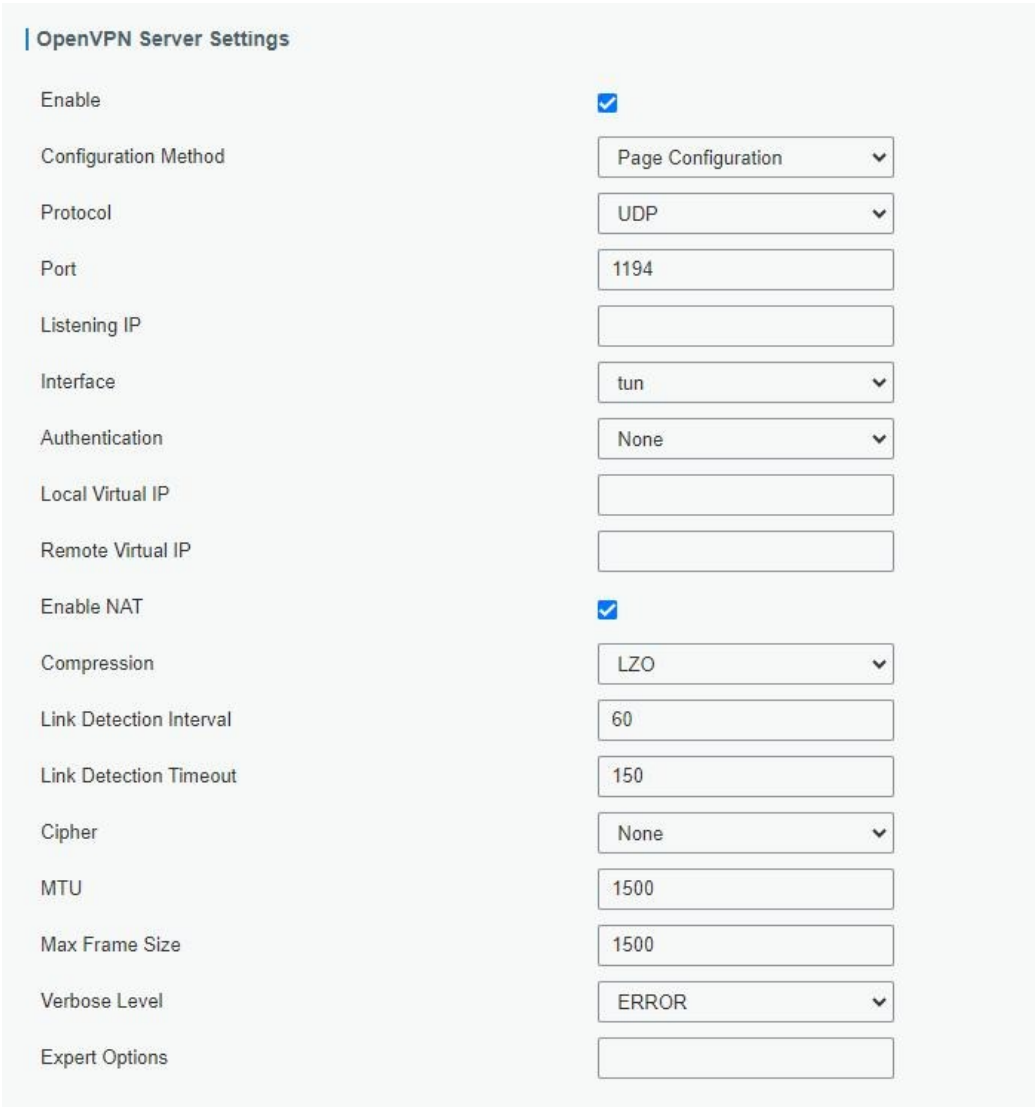


Abbildung 3-4-6-13

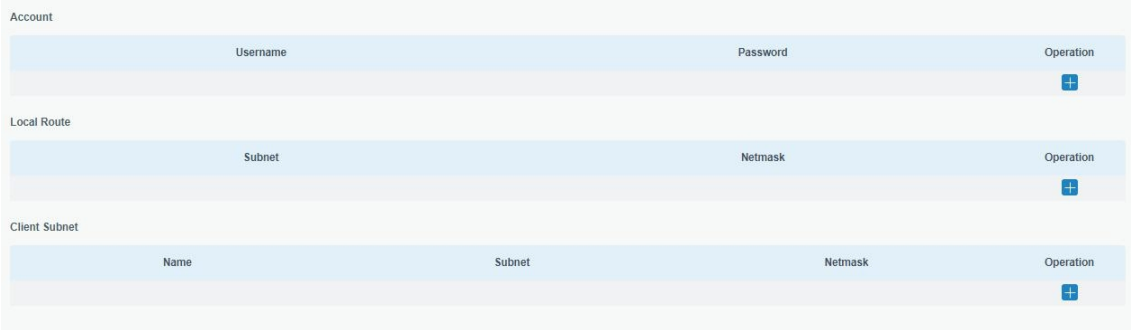


Abbildung 3-4-6-14

OpenVPN-Server – Seitenkonfiguration	
Element	**Beschreibung**
Protokoll	Wählen Sie ein Transportprotokoll aus, das von der Verbindung verwendet wird: UDP oder TCP.
Zuhörende IP	Geben Sie den lokalen Hostnamen oder die IP-Adresse für die Bindung ein. Wenn das Feld leer bleibt, bindet sich der OpenVPN Server mit allen Schnittstellen verbunden.
Port	Geben Sie die TCP/UCP-Servicenummer für die OpenVPN-Clientverbindung ein. Bereich: 1-65535.

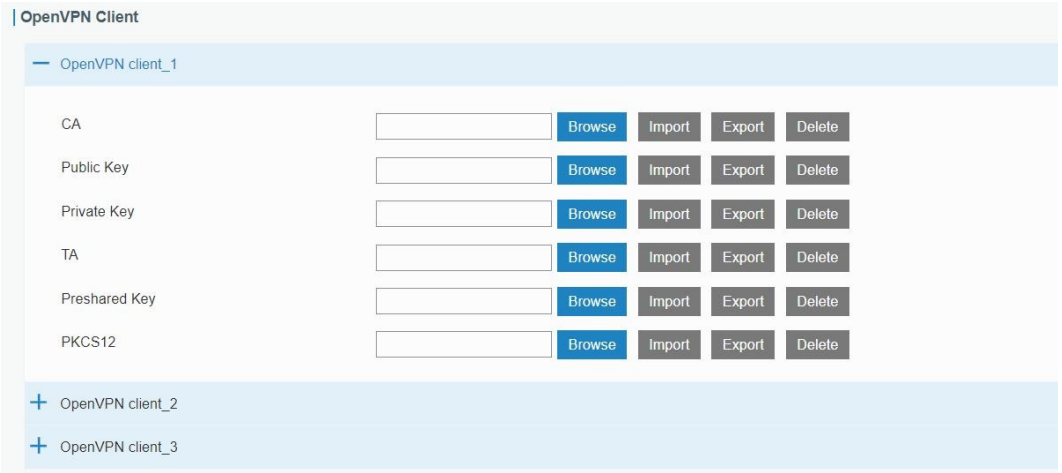
Schnittstelle	Wählen Sie den Typ der virtuellen VPN-Netzwerkschnittstelle aus TUN und TAP aus. TUN-Geräte kapseln IPv4 oder IPv6 (OSI-Schicht 3), während TAP-Geräte Ethernet 802.3 (OSI-Schicht 2) kapseln.
Authentifizierungstyp	Wählen Sie den Authentifizierungstyp aus, der zur Sicherung von Datensitzungen 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 zur Seite **Netzwerk > VPN > Zertifikate**, 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 X.509-Zertifikat als Authentifizierungstyp.
Lokale virtuelle IP	Legen Sie die lokale Tunneladresse fest, wenn der Authentifizierungstyp **„Keine“** oder **„Vorab geteilt“** ist.
Virtuelle Remote-IP	Legen Sie die Remote-Tunneladresse fest, wenn der Authentifizierungstyp **„Keine“** oder „Vorab geteilt“ lautet. **„Vorab geteilt“ ist.**
Client-Subnetz	Definieren Sie einen IP-Adresspool für den OpenVPN-Client.
Client-Netzmaske	Legen Sie die Subnetzmaske des Clients fest, um den IP-Adressbereich zu begrenzen.
Neuverhandlungsintervall	Verhandeln Sie den Datenkanalschlüssel nach diesem Intervall neu. 0 bedeutet deaktivieren.
Maximale Anzahl von Clients	Begrenzen Sie den Server auf eine maximale Anzahl gleichzeitiger Clients, Bereich: 1-20. **Hinweis:** Bitte stellen Sie die Protokollierungsstufe auf „Info” ein, wenn Sie viele Clients verbinden müssen.
CRL aktivieren	CRL-Überprüfung aktivieren oder deaktivieren.
Client-zu-Client aktivieren	Wenn diese Option aktiviert ist, können OpenVPN-Clients miteinander kommunizieren.
Dup-Client aktivieren	Ermöglicht mehreren Clients, sich mit demselben gemeinsamen Namen oder derselben gemeinsamen Zertifizierung zu verbinden. Zertifizierung verbinden.
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 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
Komprimierung	Wählen Sie diese Option, um LZO zum Komprimieren von Daten zu aktivieren oder zu deaktivieren.
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 festgelegt 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 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. Werte. 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 Frame-Größe fest. Bereich: 64–1500.

Ausführlichkeitsstufe	Wählen Sie zwischen ERROR, WARING,NOTICE und DEBUG.
Expertenoptionen	Der Benutzer kann in diesem Feld einige Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Semikolons trennen. **Beispiel:** ncp-ciphers AES-128-GCM;Schlüsselrichtung 1
Konto	
Benutzername und Passwort	Benutzername und Passwort für OpenVPN-Client festlegen, wenn der Authentifizierungstyp „Benutzername/Passwort“ ist.
Lokale Route	
Subnetz	Legen Sie die IP-Adresse der lokalen Route fest.
Subnetzmaske	Legen Sie die Netzmaske der lokalen Route fest.
Client-Subnetz	
Name	Legen Sie den Namen als allgemeinen Namen des OpenVPN-Client-Zertifikats fest.
Subnetz	Legen Sie das Subnetz des OpenVPN-Clients fest.
Subnetzmaske	Legen Sie die Subnetzmaske des OpenVPN-Clients fest.

Tabelle 3-4-6-12 OpenVPN-Serverparameter

3.4.6.8 Zertifizierungen

Bei der Arbeit als OpenVPN-Server, OpenVPN-Client oder IPsec-Server kann der Benutzer die erforderlichen Zertifikats- und Schlüsseldateien entsprechend den Authentifizierungstypen auf diese Seite



importieren/exportieren.

Abbildung 3-4-6-15

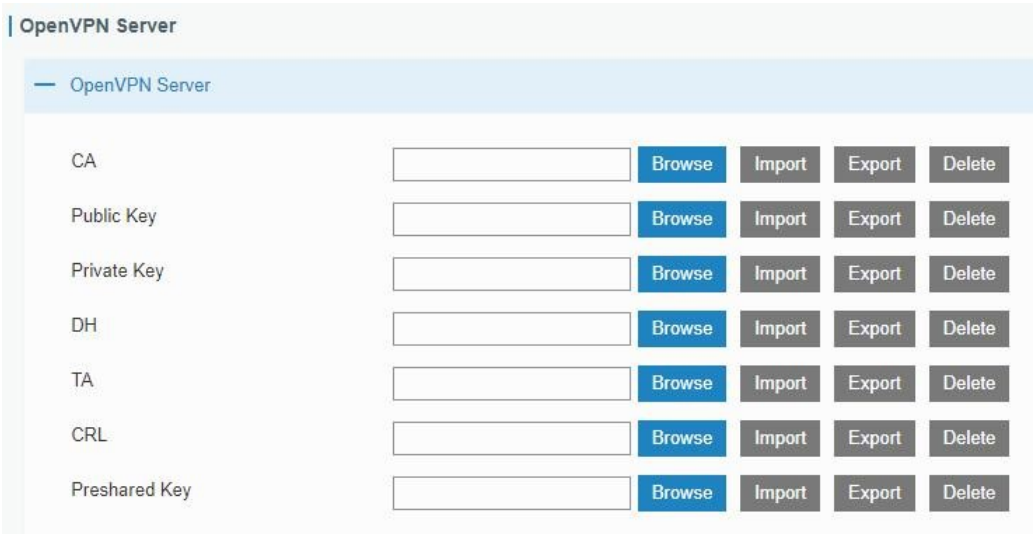


Abbildung 3-4-6-16

Abbildung 3-4-6-17

3.4.6.9 WireGuard

WireGuard ist ein extrem einfaches, aber schnelles und modernes VPN, das modernste Kryptografie nutzt. WireGuard leitet den Datenverkehr über das UDP-Protokoll weiter.

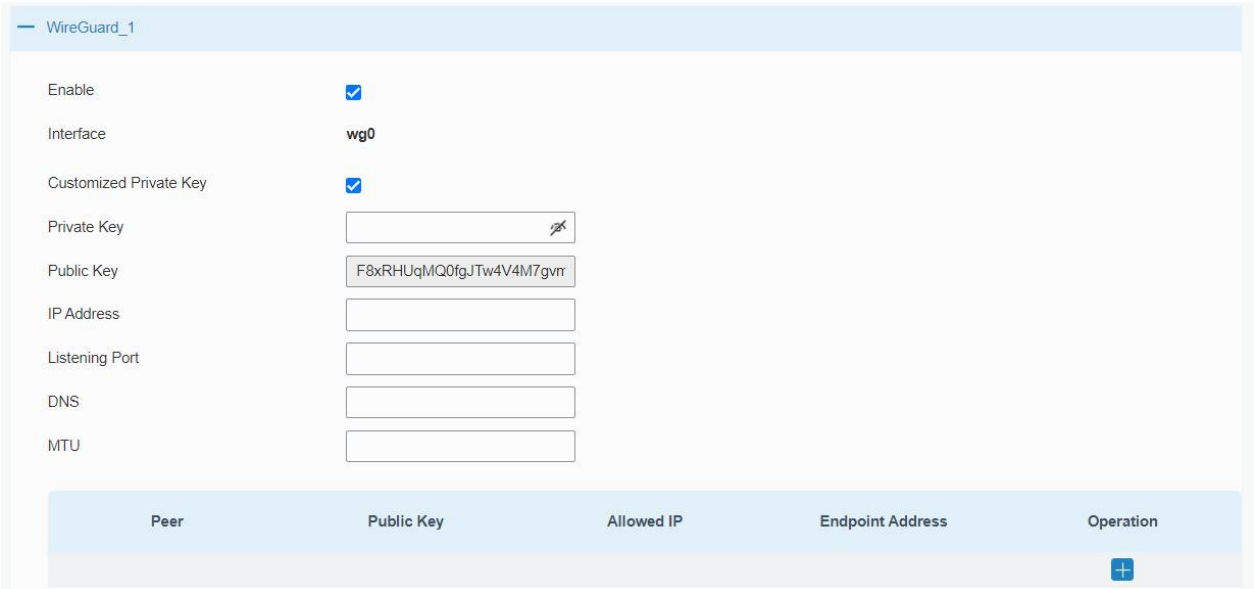


Abbildung 3-4-6-18

WireGuard	
Element	**Beschreibung**
Aktivieren	Aktivieren Sie die WireGuard-Schnittstelle. Es sind maximal 3 WireGuard-Schnittstellen sind zulässig.
Schnittstelle	Zeige den Namen der WireGuard-Schnittstelle an.
Benutzerdefinierter privater Schlüssel	Aktivieren oder deaktivieren Sie diese Option, um den privaten Schlüssel dieser WireGuard-Schnittstelle anzupassen Schnittstelle anzupassen. Wenn diese Option deaktiviert ist, verwendet der Client den von diesem Router generierten privaten Schlüssel.
Öffentlicher Schlüssel	Zeigt den vom privaten Schlüssel generierten öffentlichen Schlüssel an.
IP-Adresse	Legen Sie die lokale virtuelle IP-Adresse und die Netzmaske fest. Beispiel: 10.8.0.2/24
Empfangsport	Legen Sie den Port zum Senden oder Empfangen von WireGuard-Paketen fest. Der Port Die Nummern der verschiedenen WireGuard-Schnittstellen sollten unterschiedlich sein.
DNS	Legen Sie die DNS-Serveradresse dieser WireGuard-Schnittstelle fest. Wenn das Feld leer bleibt, verwendet der Router die DNS-Serveradresse der gemeinsamen Netzwerkschnittstellen (WAN Mobilfunk usw.).
MTU	Legen Sie die maximale Übertragungseinheit dieser WireGuard-Schnittstelle fest. Wenn dieses Feld leer bleibt, verwendet der Router die MTU der gängigen Netzwerkschnittstellen (WAN Mobilfunk usw.).
Peer-Tabelle	Klicken Sie auf „+“, um WireGuard-Peers dieser WireGuard-Schnittstelle hinzuzufügen. Eine WireGuard-Schnittstelle kann maximal 20 Peers hinzufügen.

Tabelle 3-4-6-13 WireGuard-Parameter

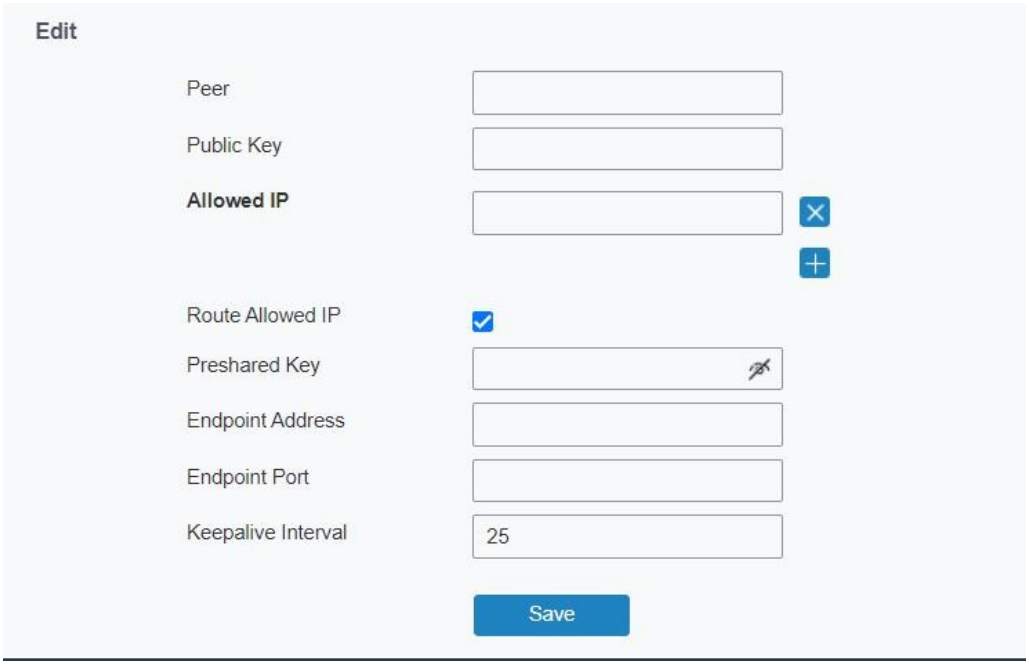


Abbildung 3-4-6-19

WireGuard-Peer	
Element	**Beschreibung**
Peer	Legen Sie einen WireGuard-Peer-Namen fest. Dieser Name sollte in diesem

	WireGuard-Client eindeutig sein.
Öffentlicher Schlüssel	Legen Sie den öffentlichen Schlüssel des WireGuard-Peer-Servers/Clients fest.
Zulässige IP	Legen Sie die tatsächliche IP-Adresse und Netzmaske des LAN-Netzwerks des WireGuard-Peers fest. Beispiel: 192.168.1.0/24 Ein WireGuard-Peer unterstützt das Hinzufügen von 8 zulässigen IP-Adressen.
Zulässige IP-Adresse weiterleiten	Aktivieren oder deaktivieren Sie diese Option, um statische Routings von zugelassenen IP-Adressen hinzuzufügen.
Vorab geteilter Schlüssel	Legen Sie den vorab geteilten Schlüssel fest, und sowohl diese Schnittstelle als auch die Peer-Schnittstelle sollten denselben Schlüsselwert haben.
Endpunktadresse	Legen Sie die IP-Adresse oder den Domänennamen des WireGuard-Peer-Servers/Clients fest.
Endpunkt-Port	Legen Sie den Zielport des WireGuard-Peer-Servers/Clients fest.
Keepalive-Intervall	Nachdem die Verbindung hergestellt wurde, wird diese WireGuard-Schnittstelle Sende regelmäßig Heartbeat-Pakete, um die Verbindung aufrechtzuerhalten. 0 bedeutet deaktiviert.

Tabelle 3-4-6-13 WireGuard-Peer-Parameter

3.5 System

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

3.5.1 Allgemeine Einstellungen

3.5.1.1 Allgemein

Zu den allgemeinen Einstellungen gehören Systeminformationen, Zugriffsservice und HTTPS-Zertifikate.

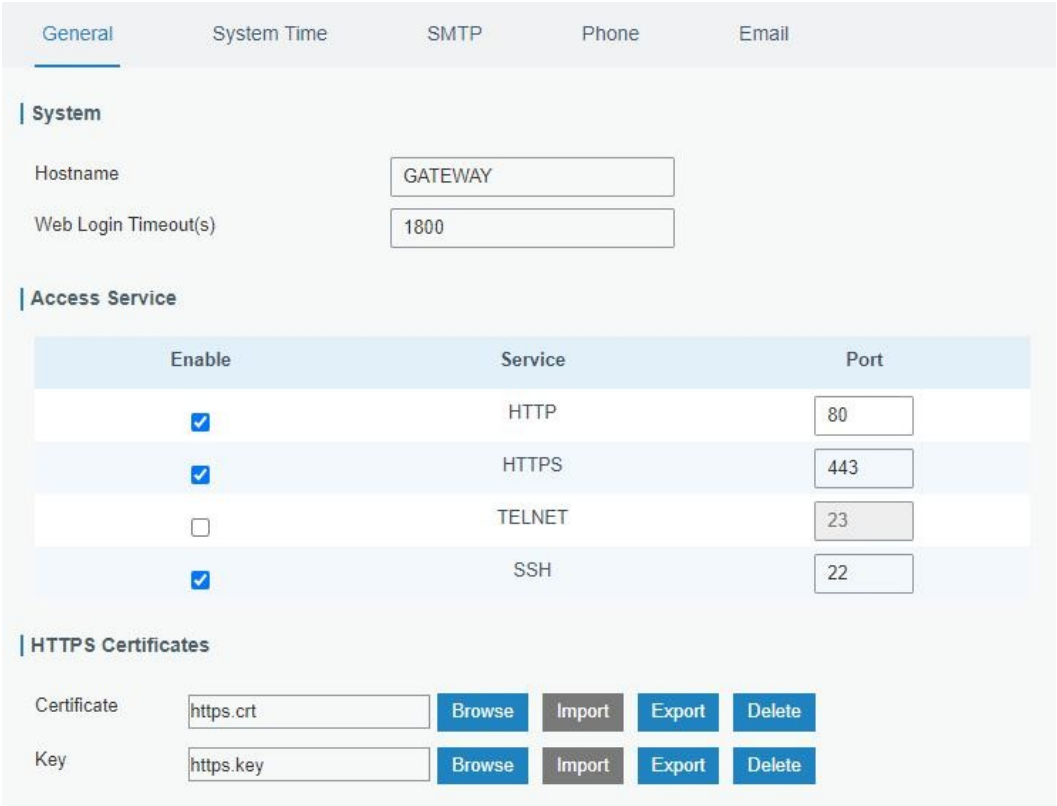


Abbildung 3-5-1-1

Allgemein		
Element	**Beschreibung**	**Standard**
System		
Hostname	Benutzerdefinierter Gateway-Name,muss mit einem Buchstaben beginnen.	GATEWAY
Web-Anmeldung Zeitüberschreitung (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 es über das Web steuern, nachdem die Option aktiviert wurde.	80
HTTPS	Benutzer können sich lokal und remote über HTTPS lokal oder remote beim 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 am Gerät anmelden, um über das Web darauf zuzugreifen und es zu steuern, nachdem 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 in das PC. 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. Klicken Sie auf die Schaltfläche „Löschen“, um die Datei zu löschen.	--

Tabelle 3-5-1-1 Allgemeine Einstellungsparameter

3.5.1.2 Systemzeit

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

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

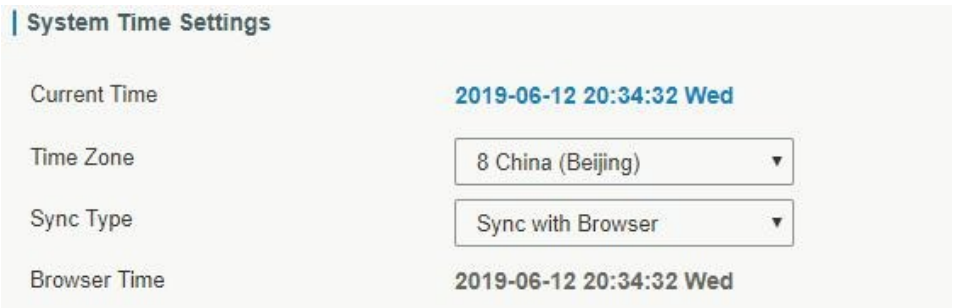


Abbildung 3-5-1-2

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 Synchronisierungstyp auszuwählen. **Mit Browser synchronisieren:** Synchronisieren Sie die Zeit mit dem Browser. **Mit NTP-Server synchronisieren:** Zeit mit NTP-Server synchronisieren. **Manuell einrichten:** Konfigurieren Sie die Zeit manuell.
Mit NTP-Server synchronisieren	
NTP-Serveradresse	NTP-Serveradresse (Domänenname/IP) festlegen.
NTP-Server aktivieren	Nach dem Aktivieren kann der NTP-Client im Netzwerk die Zeitsynchronisation mit dem Gateway synchronisieren.

Tabelle 3-5-1-2 Systemzeitparameter

3.5.1.3 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 die E-Mail-Einstellungen konfigurieren.

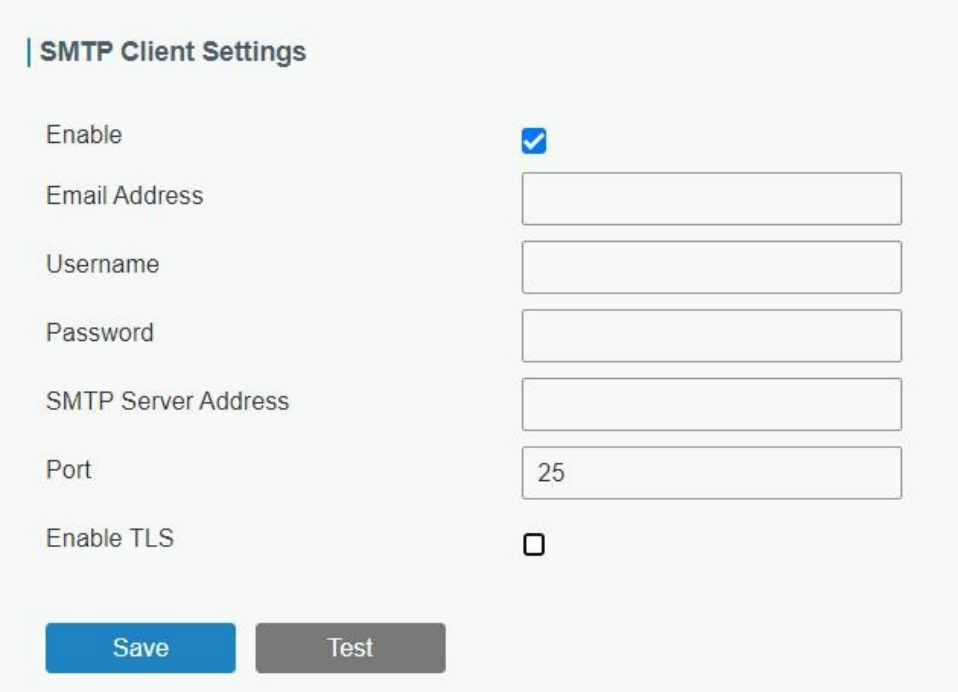


Abbildung 3-5-1-3

SMTP	
Element	**Beschreibung**
SMTP-Client-Einstellungen	
Aktivieren	SMTP-Client-Funktion aktivieren oder deaktivieren.
E-Mail-Adresse	Geben Sie die E-Mail-Adresse des Absenders ein.

Benutzername	Geben Sie den E-Mail-Benutzernamen 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.

Tabelle 3-5-1-3 SMTP-Einstellung

Verwandte Themen

Ereigniseinstellungen

3.5.1.4 Telefon

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

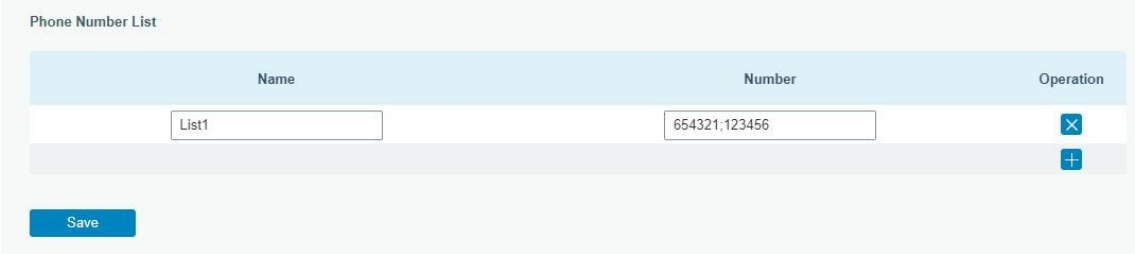


Abbildung 3-5-1-4

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.

Tabelle 3-5-1-4 Telefoneinstellungen

Verwandtes Thema

Verbindung bei Bedarf

3.5.1.5 E-Mail

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

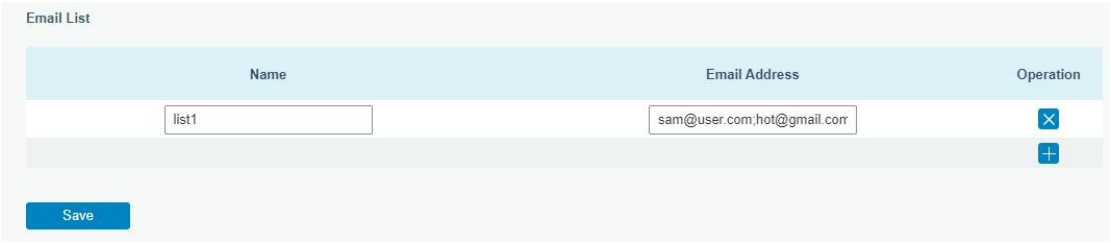


Abbildung 3-5-1-5

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.

Tabelle 3-5-1-5 E-Mail-Einstellungen

3.5.2 Benutzerverwaltung

3.5.2.1 Konto

Hier können Sie den Benutzernamen und das Passwort des Administrators ändern.

Hinweis: Aus Sicherheitsgründen wird dringend empfohlen, diese zu ändern.

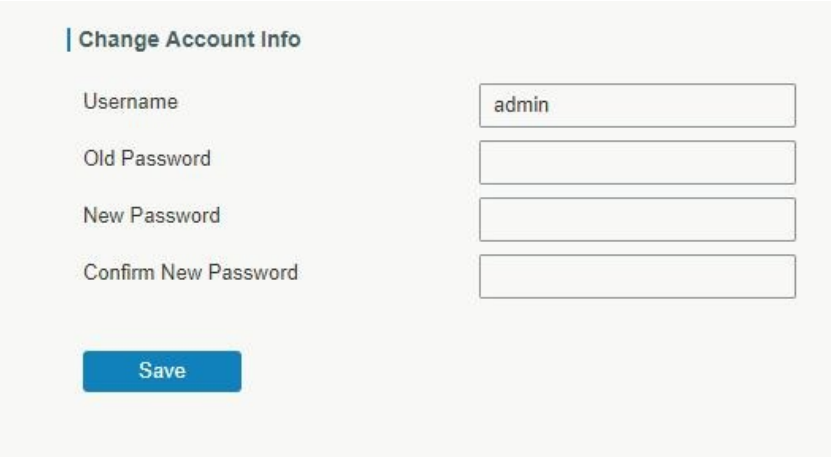


Abbildung 3-5-2-1

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. Sie können alle ASCII-Zeichen verwenden außer Leerzeichen verwenden.
Neues Passwort bestätigen	Geben Sie das neue Passwort erneut ein.

Tabelle 3-5-2-1 Kontoinformationen

3.5.2.2 Benutzerverwaltung

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

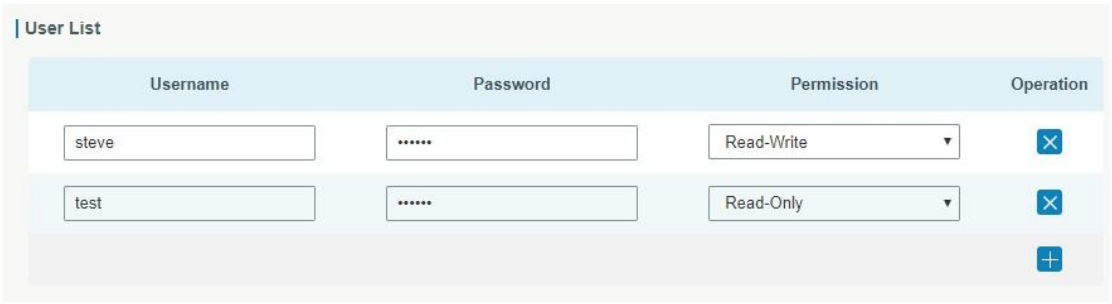


Abbildung 3-5-2-2

Benutzerverwaltung	
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.
Passwort	Legen Sie ein Passwort fest. Sie können alle ASCII-Zeichen außer Leerzeichen.
Berechtigung	Wählen Sie die Benutzerberechtigung aus „Nur Lesen“ und „Lesen-Schreiben“. - Nur Lesen: Benutzer können auf dieser Ebene nur die Konfiguration des Gateways anzeigen. - Lesen/Schreiben: Benutzer können die Konfiguration des Gateway auf dieser Ebene anzeigen und festlegen.

Tabelle 3-5-2-2 Benutzerverwaltung

3.5.2.3 HTTP-API-Verwaltung

In diesem Abschnitt wird beschrieben, wie Sie die HTTP-API-Kontoinformationen konfigurieren.

Abbildung 3-5-2-3

Benutzerverwaltung	
Element	**Beschreibung**
Typ	Wählen Sie die HTTP-API-Kontoinformationen aus, die mit denen des Web-GUI-Kontos übereinstimmen oder verwenden Sie ein unabhängiges Konto.
Benutzername	Geben Sie einen neuen Benutzernamen ein, der sich von allen anderen Kontoinformationen unterscheidet. Sie können Zeichen wie a-z, 0-9, „_“ und „-“ verwenden. Das erste Zeichen darf keine Ziffer sein.
Passwort	Passwort festlegen. Sie können alle ASCII-Zeichen außer Leerzeichen verwenden.

Tabelle 3-5-2-3 HTTP-API-Verwaltung

3.5.3 SNMP

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

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

Die Konfigurationsschritte für die Abfrage aus NMS sind nachfolgend aufgeführt:

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

3.5.3.1 SNMP

UG67 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.

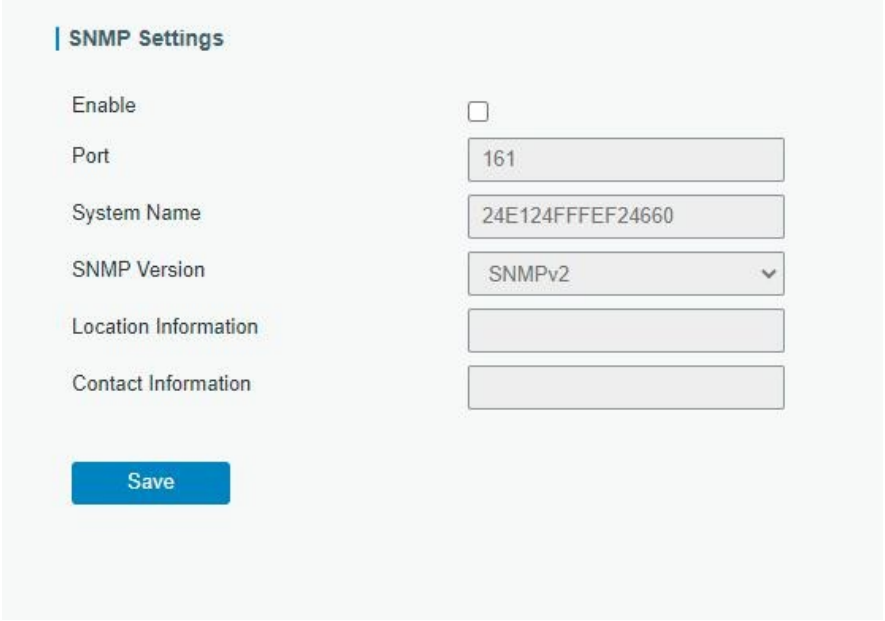


Abbildung 3-5-3-1

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.
Kontaktdaten	Geben Sie die Kontaktinformationen ein.

Tabelle 3-5-3-1 SNMP-Parameter

3.5.3.2 MIB-Ansicht

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

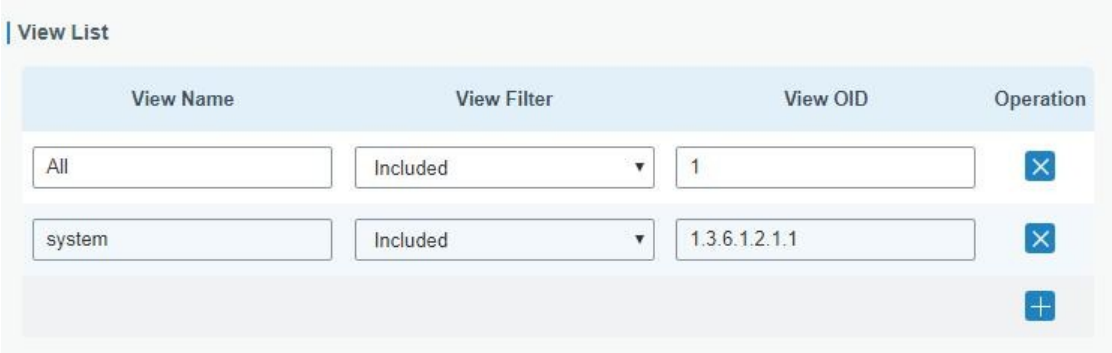


Abbildung 3-5-3-2

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.

Tabelle 3-5-3-2 MIB-Ansichtsparameter

3.5.3.3 VACM

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

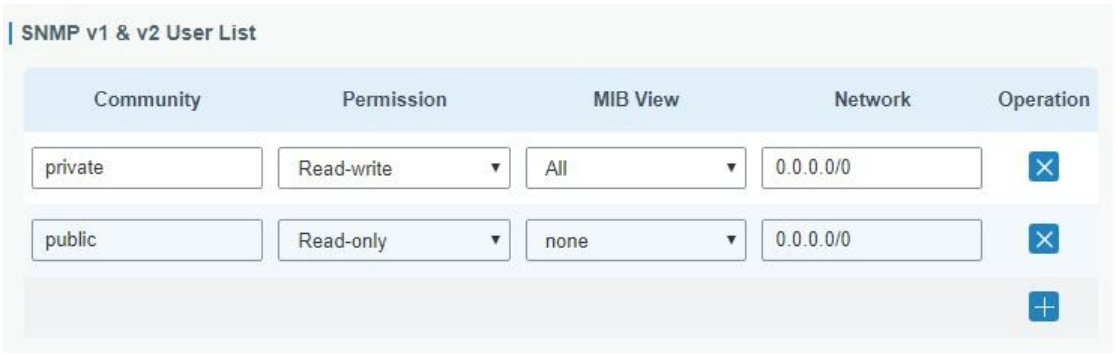


Abbildung 3-5-3-3

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 als „Lesen-Schreiben" aus der MIB-Ansichtsliste festzulegen .
Informieren Ansicht	Wählen Sie eine MIB-Ansicht aus der MIB-Ansichtsliste aus, um die Berechtigung auf „Informieren" zu setzen.

Tabelle 3-5-3-3 VACM-Parameter

3.5.3.4 Trap

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

Abbildung 3-5-3-4

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 ist 1-65535. Der Standardport ist 162.
Name	Geben Sie bei Verwendung von SNMP v1/v2c den Gruppennamen ein; geben Sie den Benutzernamen ein, wenn Sie SNMP v3 verwenden.
Auth/Priv-Modus	Wählen Sie zwischen „NoAuth & No Priv", „Auth & NoPriv" und „Auth & Priv".

Tabelle 3-5-3-4 Trap-Parameter

3.5.3.5 MIB

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

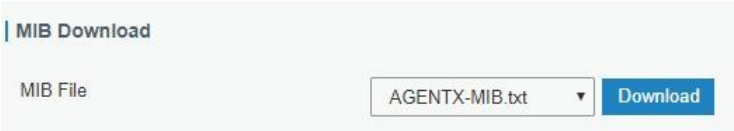


Abbildung 3-5-3-5

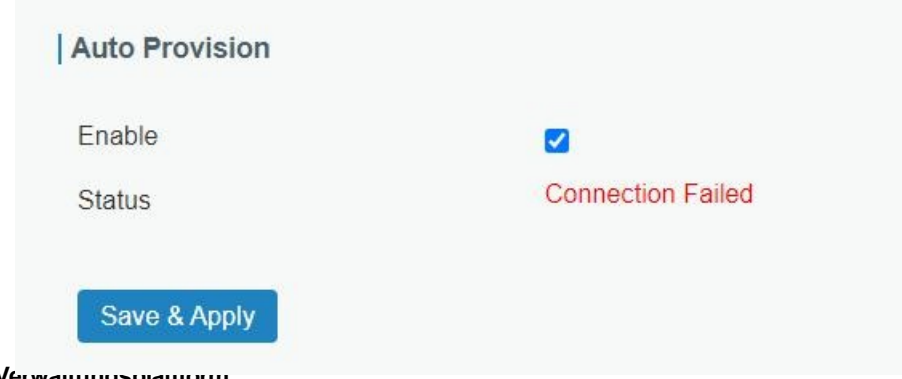
MIB	
Element	**Beschreibung**
MIB-Datei	Wählen Sie die gewünschte MIB-Datei aus.
Herunterladen	Klicken Sie auf die Schaltfläche „Herunterladen“, um die MIB-Datei auf den PC herunterzuladen.

Tabelle 3-5-3-5 MIB-Download

3.5.4 Geräteverwaltung

3.5.4.1 Automatische Bereitstellung

Benutzer können das Konfigurationsprofil in der Milesight Development Platform anpassen und auswählen. Wenn die automatische Bereitstellung aktiviert ist und das Gerät mit dem Internet verbunden ist, empfängt das Gerät das Profil, um die Erstkonfiguration durchzuführen. Diese Funktion ist auch dann verfügbar, wenn das Gerät nicht für die Verbindung mit der Milesight Development Platform konfiguriert ist.



3.5.4.2 Verwaltungsplattform

Auf dieser Seite können Sie das Gerät mit dem DeviceHub oder der Milesight-Entwicklungsplattform verbinden, um das Gateway zentral und remote zu verwalten.

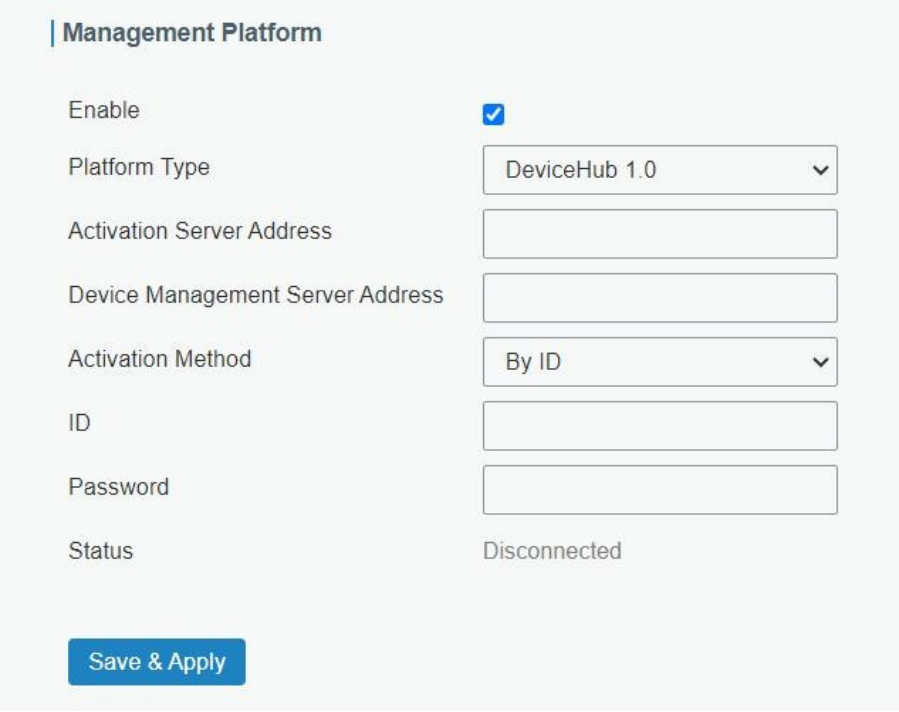


Abbildung 3-5-5-1

Verwaltungsplattform	
Element	**Beschreibung**
Aktivieren	Aktivieren oder deaktivieren Sie diese Option, um das Gateway mit der Verwaltungsplattform zu verbinden.
Plattformtyp	Milesight DeviceHub 1.0, Milesight DeviceHub 2.0 oder Milesight Entwicklungsplattform ist optional.
Status	Zeigt den Verbindungsstatus zwischen dem Gateway und der Verwaltungsplattform anzeigen.
DeviceHub 1.0	
Aktivierungsserver Adresse	IP-Adresse oder Domäne des DeviceHub.
DeviceHub-Verwaltung Adresse	Die URL-Adresse, über die das Gerät eine Verbindung zum DeviceHub herstellt, z. B. http://220.82.63.79:8080/acs.
Aktivierungsmethode	Wählen Sie die Aktivierungsmethode, um das Gateway mit dem DeviceHub-Server, Optionen sind „Nach Authentifizierungs-ID“ und „Nach ID“.
Authentifizierungscode	Geben Sie den vom DeviceHub generierten Authentifizierungscode ein.
ID	Geben Sie das registrierte DeviceHub-Konto (E-Mail) und das Passwort ein.
Passwort	
DeviceHub 2.0	
Serveradresse	IP-Adresse oder Domain des DeviceHub.

Tabelle 3-5-5-1

3.5.5 Ereignisse

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

3.5.5.1 Ereignisse

Auf dieser Seite können Sie Alarmmeldungen anzeigen.

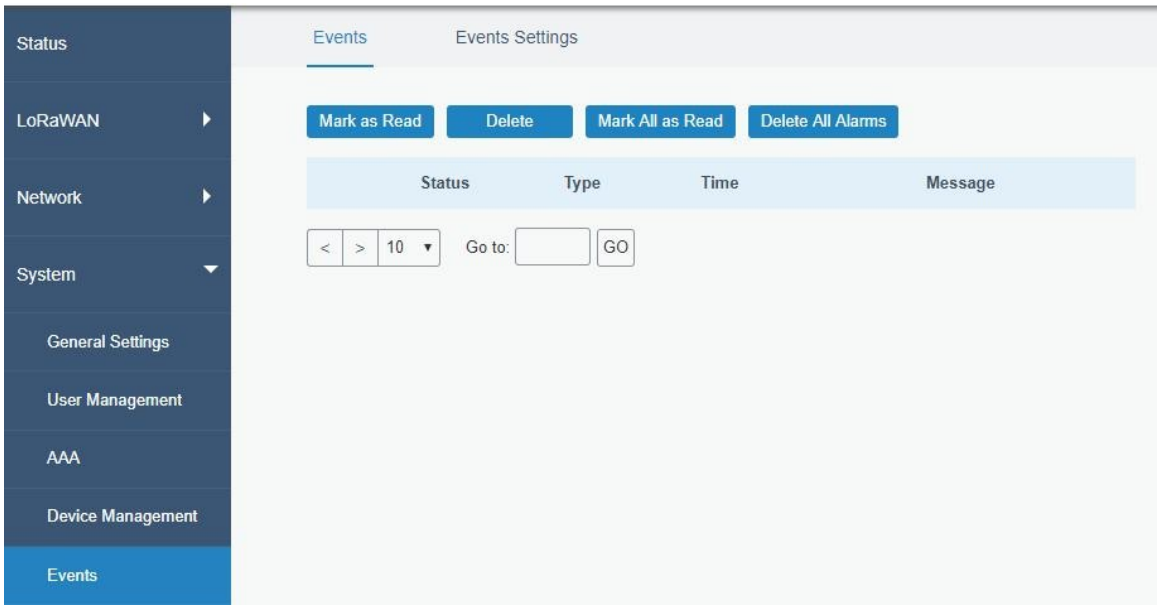


Abbildung 3-5-6-1

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.
Typ	Zeigt den Ereignistyp an, der alarmiert werden soll.
Zeit	Zeigt die Alarmzeit an.
Meldung	Zeigt den Inhalt des Alarms an.

Tabelle 3-5-6-1 Ereignisparameter

3.5.5.2 Ereigniseinstellungen

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

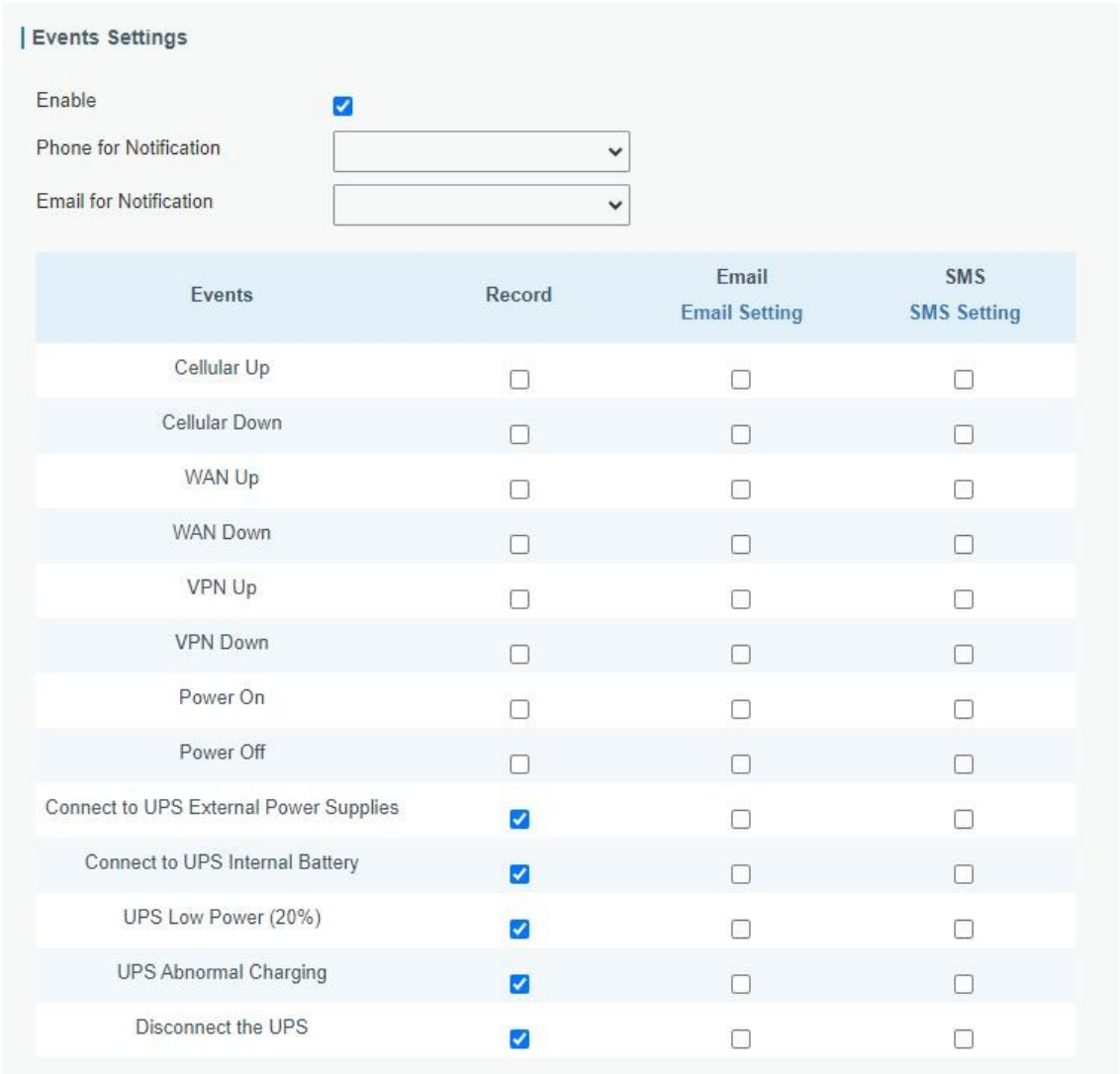


Abbildung 3-5-6-2

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	Ereignistyp, den das Gateway zur Aufzeichnung unterstützt.
Aufzeichnung	Der relevante Inhalt des Ereignisalarms wird unter „Ereignis“ aufgezeichnet. Seite, wenn diese Option aktiviert ist.
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“ zu gelangen und die E-Mail-Gruppe konfigurieren können.
SMS	Der relevante Inhalt des Ereignisalarms wird per SMS versendet, wenn diese Option aktiviert ist.

SMS-Einstellungen	Klicken Sie auf und Sie werden zur Seite „Telefon“ weitergeleitet, um Telefon-Gruppenliste konfigurieren.

Tabelle 3-5-6-2 Ereignisparameter

Verwandte Themen E-Mail-Einstellungen Telefoneinstellungen

3.6 Wartung

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

3.6.1 Tools

Zu den Tools zur Fehlerbehebung gehören Ping und Traceroute.

3.6.1.1 Ping

Das Ping-Tool wurde entwickelt, um externe Netzwerke anzupingen.

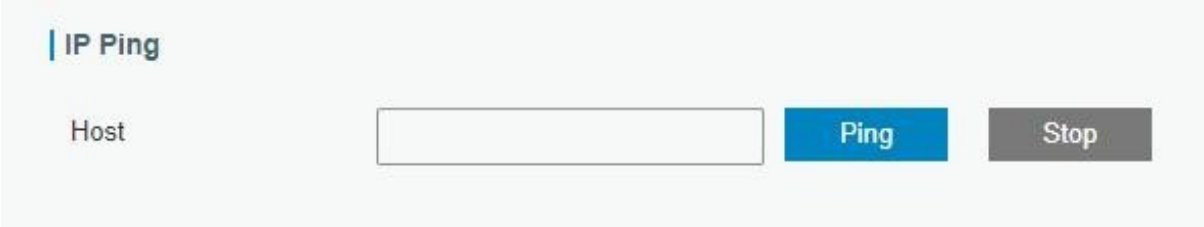


Abbildung 3-6-1-1

PING	
Element	**Beschreibung**
Host	Ping-Befehl für das externe Netzwerk vom Gateway aus.

Tabelle 3-6-1-1 IP-Ping-Parameter

3.6.1.2 Traceroute

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

Abbildung 3-6-1-2

Traceroute	
Element	**Beschreibung**
Host	Adresse des zu ermittelnden Zielhosts.

Tabelle 3-6-1-2 Traceroute-Parameter

3.6.1.3 Paketanalysator

Der Paketanalysator wird zum Erfassen der Pakete verschiedener Schnittstellen verwendet.

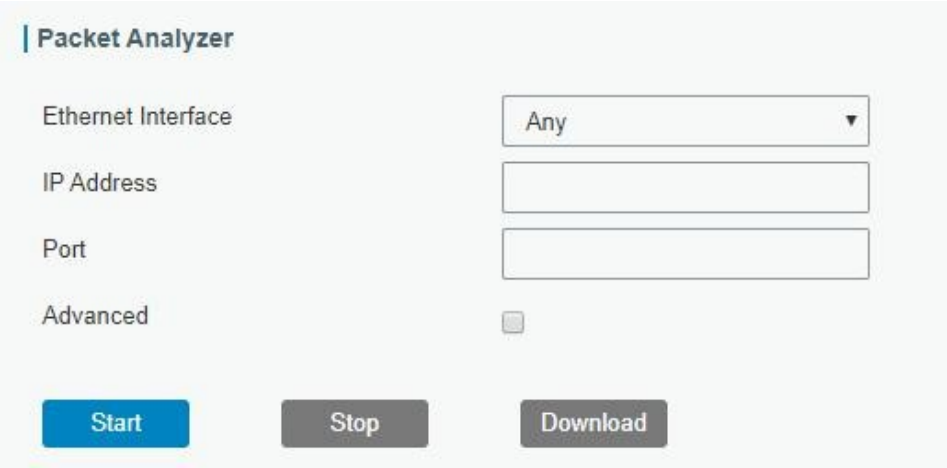


Abbildung 3-6-1-3

Paketanalysator	
Element	**Beschreibung**
Ethernet-Schnittstelle	Wählen Sie die Schnittstelle aus, über die Pakete erfasst werden sollen.
IP-Adresse	Legen Sie die IP-Adresse fest, die der Router erfassen soll.
Port	Legen Sie den Port fest, den der Router erfassen soll.
Erweitert	Legen Sie die Regeln für den Sniffer fest. Das Format lautet tcpdump.

Tabelle 3-6-1-3 Parameter des Paketanalysators

3.6.1.4 Qxdmlog

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

Abbildung 3-6-1-4

3.6.2 Zeitplan

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

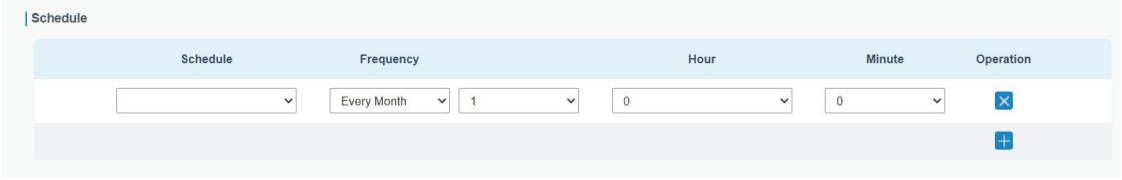


Abbildung 3-6-2-1

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.

Tabelle 3-6-2-1 Zeitplanparameter

3.6.3 Protokoll

Das Systemprotokoll enthält eine Aufzeichnung von Informations-, Fehler- und Warnereignissen, die Aufschluss über die Systemprozesse 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. Ein Remote-Protokollserver ist möglich, und das Gateway lädt alle Systemprotokolle auf einen Remote-Protokollserver wie Syslog Watcher hoch.

3.6.3.1 Systemprotokoll

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

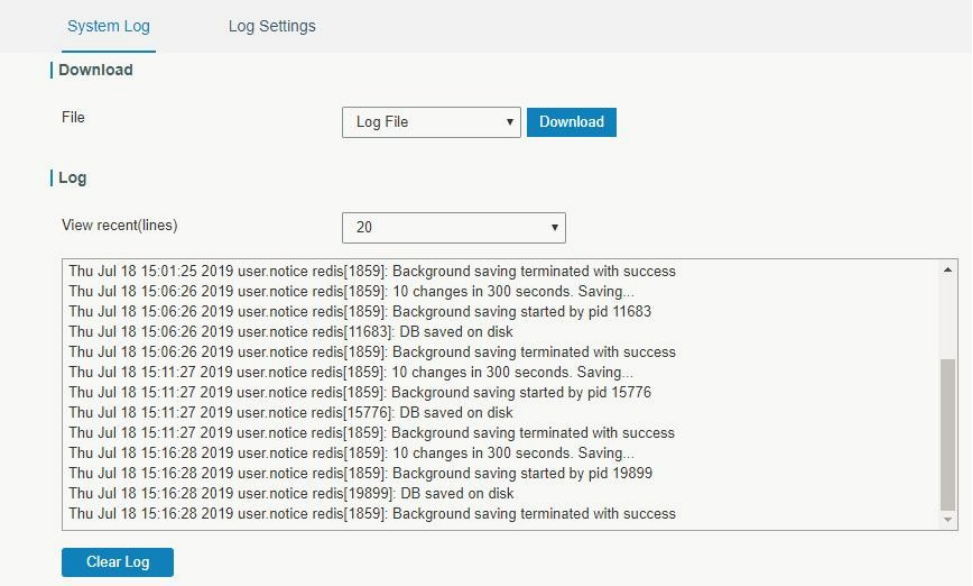


Abbildung 3-6-3-1

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

Tabelle 3-6-3-1 Systemprotokollparameter

3.6.3.2 Protokolleinstellungen

In diesem Abschnitt wird erläutert, wie Sie die Einstellungen für den Remote-Protokollserver und das lokale Protokoll aktivieren.

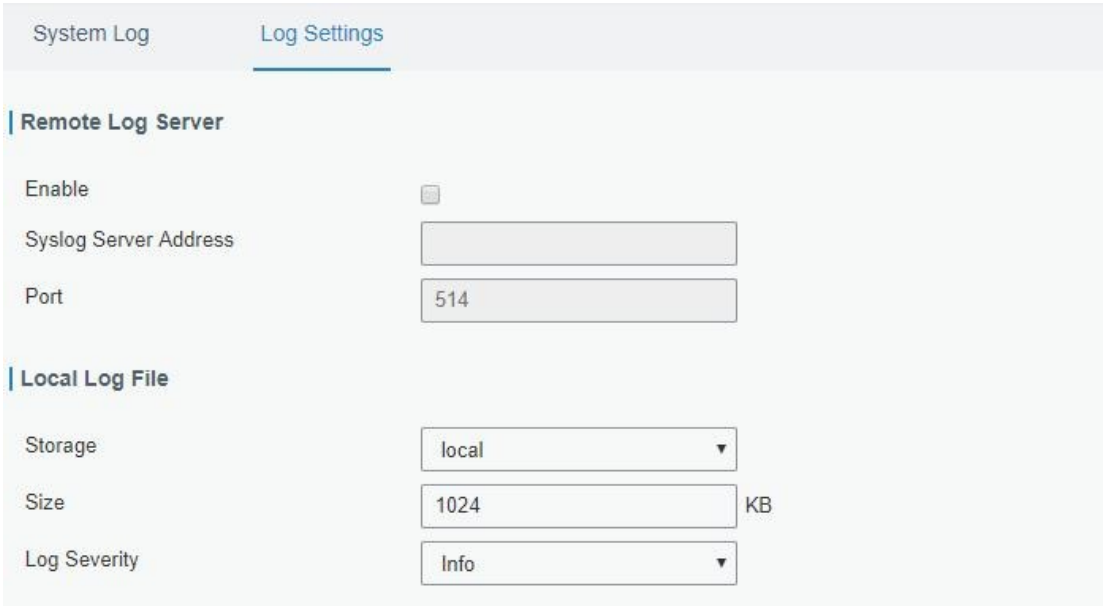


Abbildung 3-6-3-2

Protokolleinstellungen	
Element	**Beschreibung**
Remote-Protokollserver	
Aktivieren	Wenn „Remote-Protokollserver“ aktiviert ist, sendet das Gateway alle Systemprotokolle an den Remote-Server.
Syslog-Server-Adresse	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 ablegen.
Größe	Legen Sie die Größe der zu speichernden Protokolldatei fest.
Protokollschweregrad	Die Liste der Schweregrade entspricht dem Syslog-Protokoll.

Tabelle 3-6-3-2 Systemprotokollparameter

3.6.4 Upgrade

In diesem Abschnitt wird beschrieben, wie Sie die Gateway-Firmware über das Web aktualisieren können. In der Regel ist eine Aktualisierung der Firmware nicht erforderlich.

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

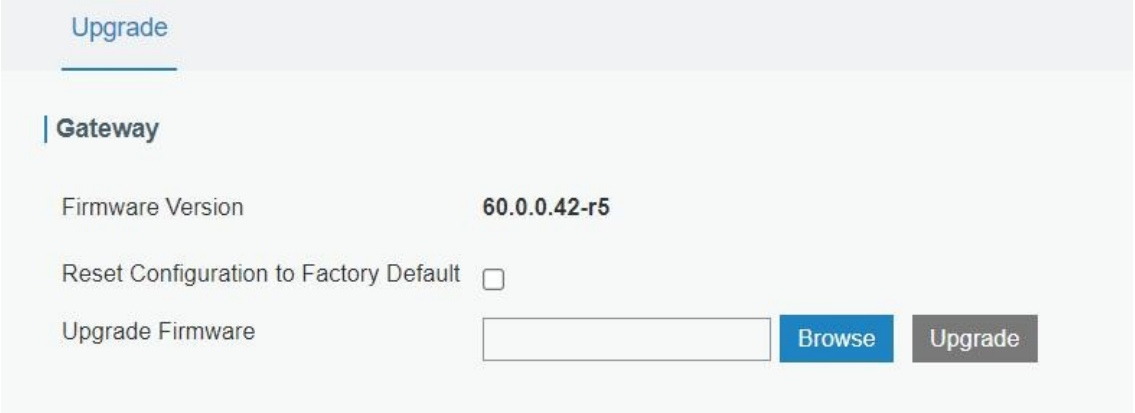


Abbildung 3-6-4-1

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

Tabelle 3-6-4-1 Upgrade-Parameter

Beispiel für die entsprechende Konfiguration

Firmware-Aktualisierung

3.6.5 Sichern und Wiederherstellen

In diesem Abschnitt wird erläutert, wie Sie eine vollständige Sicherung der gesamten Systemkonfigurationen in einer Datei erstellen, nur wichtige Teile der Konfiguration für die Batch-Sicherung replizieren, die Konfigurationsdatei auf dem Gateway wiederherstellen und die Werkseinstellungen zurücksetzen.

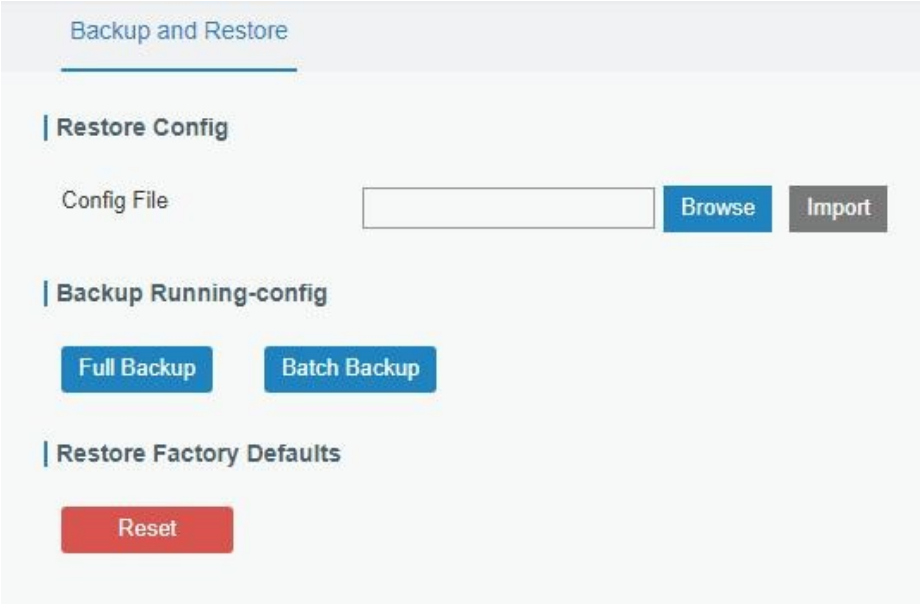


Abbildung 3-6-5-1

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.
Batch-Sicherung	Klicken Sie auf „Batch-Sicherung“, um die aktuelle Konfiguration mit Ausnahme der Gateway-ID des Paketweiterleiters, aller eingebetteten NS-Einstellungen, der statischen IP-Adresse des WAN der WLAN-Einstellungen, der Benutzerverwaltungseinstellungen, des DeviceHub Authentifizierungscode, alle APP-Einstellungen.
Zurücksetzen	Klicken Sie auf die Schaltfläche „Zurücksetzen“, um die Werkseinstellungen wiederherzustellen. Das Gateway wird nach Abschluss des Zurücksetzens neu gestartet.

Tabelle 3-6-5-1 Parameter für Sicherung und Wiederherstellung

Beispiel für die entsprechende Konfiguration

Werkseinstellungen wiederherstellen

3.6.6 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 den Verlust der neuen Konfiguration zu vermeiden.

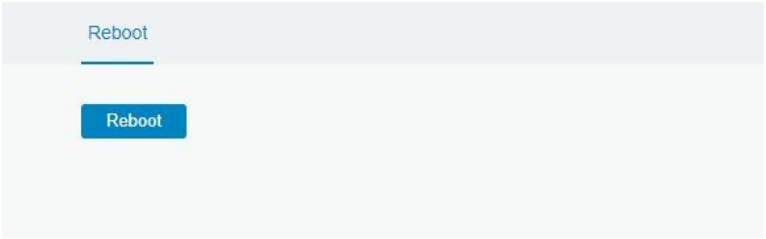


Abbildung 3-6-6-1

3.7 APP

3.7.1 Python

Python ist eine objektorientierte Programmiersprache, die aufgrund ihrer klaren Syntax und Lesbarkeit an Beliebtheit gewonnen hat.

Als interpretierte Sprache verfolgt Python eine Designphilosophie, die Wert auf die Lesbarkeit des Codes legt, insbesondere durch die Verwendung von Einrückungen zur Abgrenzung von Codeblöcken anstelle von geschweiften Klammern oder Schlüsselwörtern, sowie eine Syntax, die es Programmierern ermöglicht, Konzepte in weniger Codezeilen auszudrücken als in anderen Sprachen wie C++ oder Java. Die Sprache bietet Konstrukte und soll das Schreiben klarer Programme sowohl im kleinen als auch im großen Maßstab ermöglichen.

Benutzer können Python verwenden, um schnell einen Prototyp des Programms zu erstellen, der die endgültige Schnittstelle des Programms sein kann, ihn mit einer geeigneteren Sprache umschreiben und dann

Kapseln Sie die erweiterte Klassenbibliothek, die Python aufrufen kann.
In diesem Abschnitt wird beschrieben, wie Sie den relevanten Ausführungsstatus wie App-Manager, SDK-Version, erweiterter Speicher usw. anzeigen können. Außerdem können Sie hier die App-Manager-Konfiguration ändern und das Python-App-Paket importieren.

3.7.1.1 Python

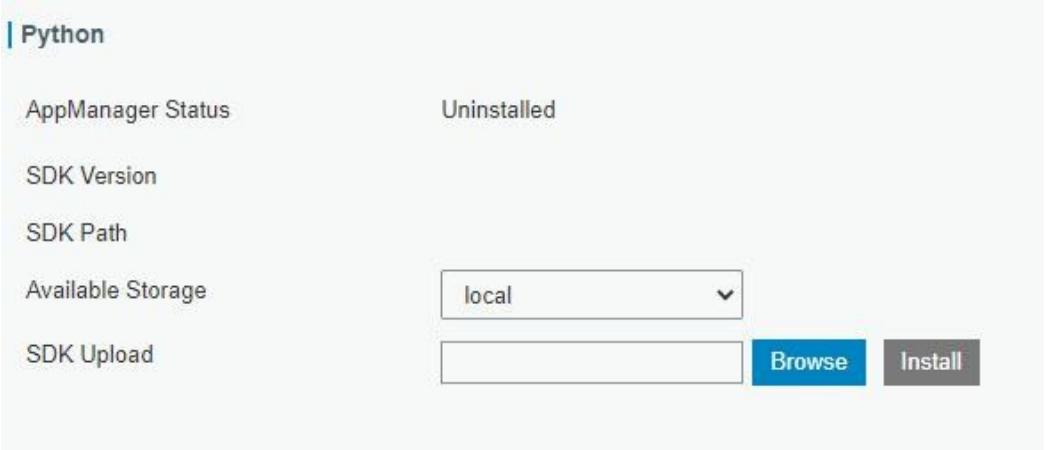


Abbildung 3-7-1-1

Python	
Element	**Beschreibung**
AppManager-Status	Zeigt den Ausführungsstatus von AppManager an, z. B. „Deinstalliert“, „Läuft“ oder „Beendet“.
SDK-Version	Zeigt die Version des installierten SDK an.
SDK-Pfad	Zeigt den Installationspfad des SDK an.
Verfügbarer Speicherplatz	Wählen Sie den verfügbaren Speicherplatz für die Installation des SDK aus.
SDK hochladen	Laden Sie das SDK für Python hoch und installieren Sie es.
Deinstallieren	Deinstallieren Sie das SDK.
Anzeigen	Anwendungsstatus anzeigen, der von AppManager verwaltet wird.

Tabelle 3-7-1-1 Python-Parameter

3.7.1.2 App Manager-Konfiguration

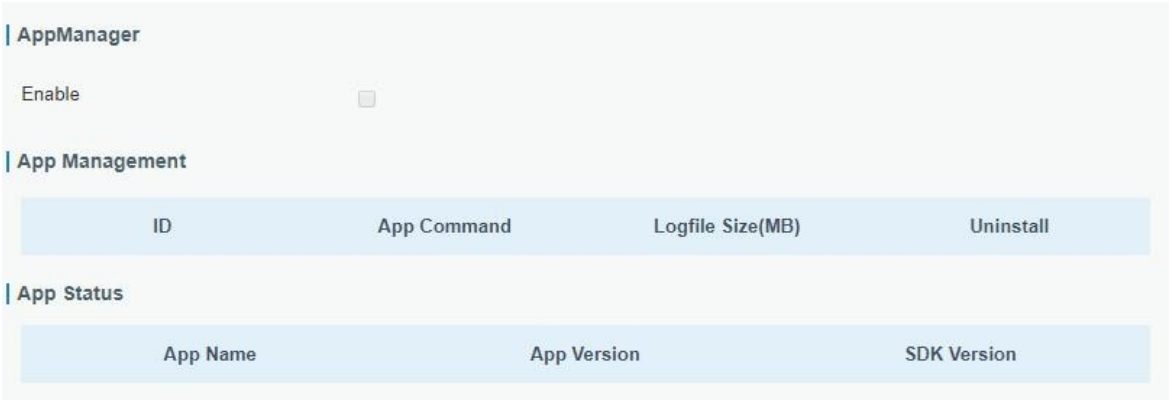


Abbildung 3-7-1-2

AppManager-Konfiguration	
Element	**Beschreibung**
Aktivieren	Nach der Aktivierung von Python AppManager kann der Benutzer auf der Webseite „Python“ auf die Schaltfläche „Anzeigen“ klicken, um den von AppManager verwaltet werden.
Anwendungsverwaltung	
Anzeige	Zeigt die ID der importierten App an.
App-Befehl	Zeige den Namen der importierten App an.
Logdateigröße (MB)	Benutzerdefinierte Logdateigröße. Bereich: 1-50.
Deinstallieren	App deinstallieren.
App-Status	
App-Name	Zeigt den Namen der importierten App an.
App-Version	Zeigt die Version der importierten App an.
SDK-Version	Zeigt die SDK-Version an, auf der die importierte App basiert.

Tabelle 3-7-1-2 APP-Manager-Parameter

3.7.1.3 Python-App

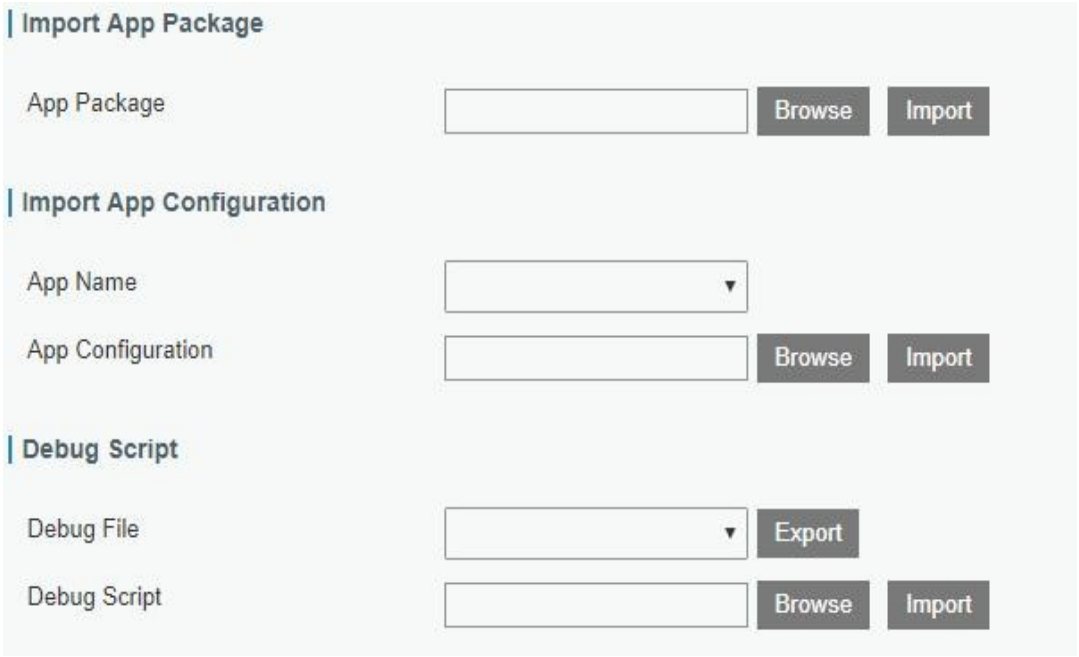


Abbildung 3-7-1-3

Python-App	
Element	**Beschreibung**
App-Paket	Wählen Sie das App-Paket aus und importieren Sie es.
App-Name	Wählen Sie die App aus, um die Konfiguration zu importieren.
App-Konfiguration	Wählen Sie die Konfigurationsdatei aus und importieren Sie sie.
Debug-Datei	Skriptdatei exportieren.
Skript debuggen	Wählen Sie das zu debuggende Python-Skript aus und importieren Sie es.

Tabelle 3-7-1-3 APP-Parameter

3.7.2 Node-RED

Node-RED ist ein flussbasiertes Entwicklungstool für die visuelle Programmierung und Verknüpfung von Hardwaregeräten, APIs und Online-Diensten als Teil des Internets der Dinge. Node-RED bietet einen webbrowserbasierten Flusseditor, mit dem sich Flüsse mithilfe der zahlreichen Knoten in der Palette einfach miteinander verknüpfen lassen. Weitere Anleitungen und Dokumentationen finden Sie auf der offiziellen Website von Node-RED.

3.7.2.1 Node-RED

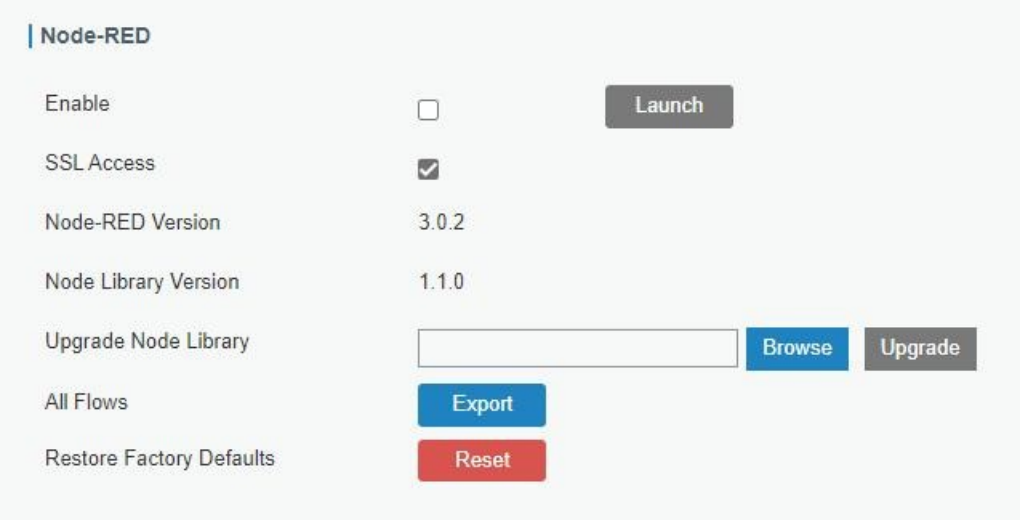


Abbildung 3-7-2-1

Node-RED	
Element	**Beschreibung**
Aktivieren	Aktivieren Sie Node-RED.
Starten	Klicken Sie hier, um die Web-GUI von Node-RED zu starten.
SSL-Zugriff	Aktivieren Sie diese Option, um über den HTTPS-Dienst auf die Node-RED-Web-GUI zuzugreifen .
Node-RED-Version	Zeigt die Version von Node-RED an. Die Node-RED-Version kann nur aktualisiert werden, wenn Sie das Gateway aktualisieren.
Node-Bibliotheksversion	Zeigt die Version der Node-Bibliothek an.
Node-Bibliothek aktualisieren	Aktualisieren Sie die Node-Bibliothek, indem Sie das Bibliothekspaket importieren.
Alle Flows exportieren	Alle Flows als JSON-Datei exportieren.
Werkseinstellungen wiederherstellen Standard	Löschen Sie alle Flussdaten von Node-RED.

Tabelle 3-7-2-1 Node-RED-Parameter

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

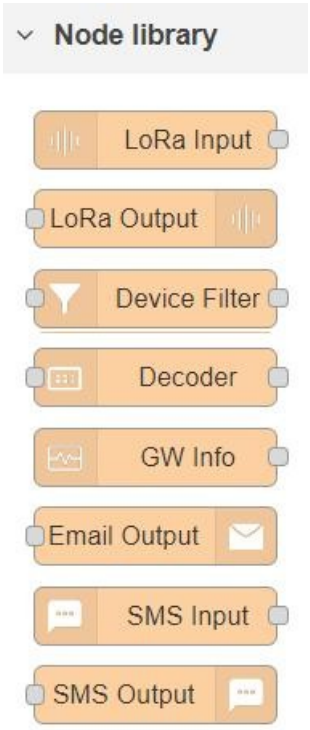


Abbildung 3-7-2-2

Knotenbibliothek	
Knoten	**Beschreibung**
LoRa-Eingang	Empfängt LoRaWAN®-Pakete vom Gateway. Dies funktioniert nur, wenn der Netzwerkserver aktiviert ist.
LoRa-Ausgang	Senden Sie Downlink-Befehle an LoRaWAN®-Knoten.
Gerätefilter	Filtern Sie die Daten eines oder mehrerer spezifischer LoRaWAN®-Knoten über Geräte-EUIs heraus.
GW-Info	Überwachen Sie Ereignisse des Gateways. Dazu muss die Ereigniserkennung unter **„Allgemein > Ereignisse > Ereigniseinstellungen“** aktiviert sein.
E-Mail-Ausgabe	Senden Sie eine E-Mail. Wenn Sie die STMP-Option „Wie das Gateway“ auswählen, müssen Sie zur Seite **„System > Allgemeine Einstellungen > SMTP“** gehen, um die SMTP-Client-Einstellungen zu konfigurieren.
SMS-Eingabe	SMS-Nachricht empfangen. Dies funktioniert nur, wenn das Mobilfunknetz verbunden ist.
SMS-Ausgabe	Eine SMS-Nachricht senden. Dies funktioniert nur, wenn das Mobiltelefon verbunden ist.

Tabelle 3-7-2-2 Parameter der Knotenbibliothek

Beispiel für die zugehörige Konfiguration

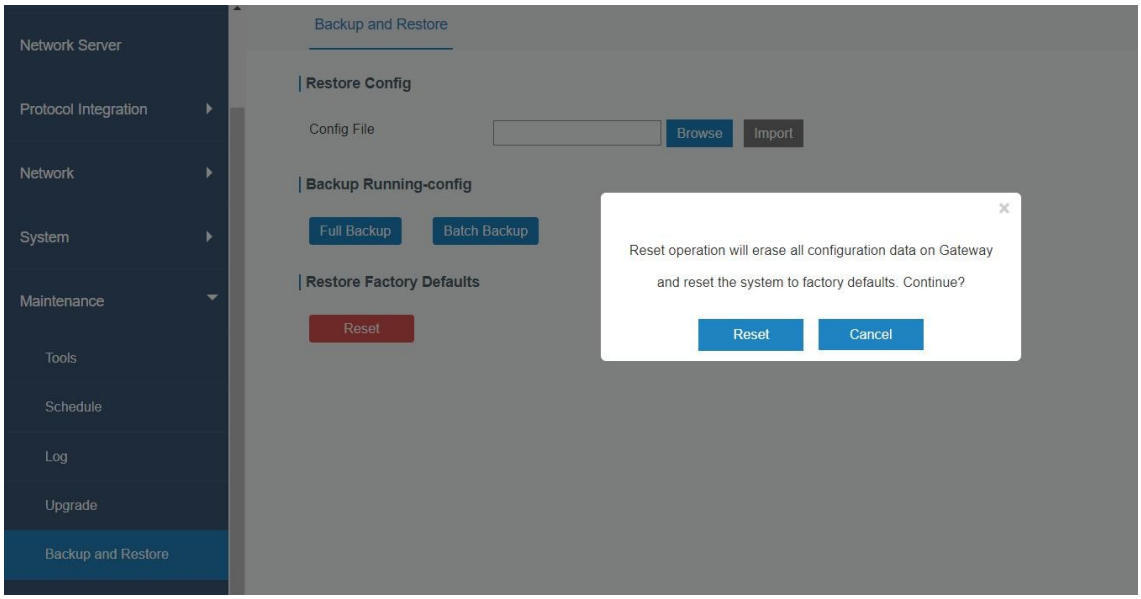
Node-RED

Kapitel 4 Anwendungsbeispiele

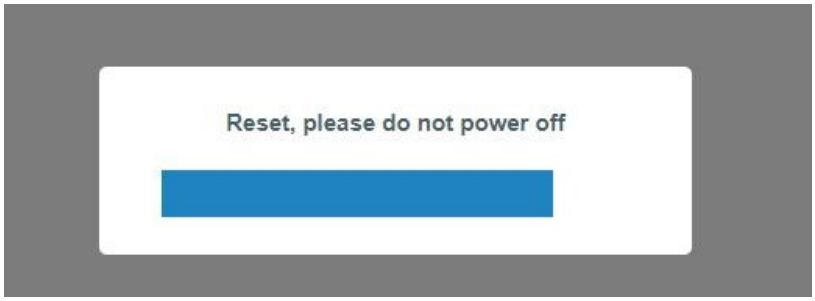
4.1 Werkseinstellungen wiederherstellen

Methode 1:

Melden Sie sich bei der Webschnittstelle an, gehen Sie zu **„Wartung > Sichern und Wiederherstellen“** und klicken Sie auf die Schaltfläche **„Zurücksetzen“**. Sie werden gefragt, ob Sie die Werkseinstellungen wiederherstellen möchten. Klicken Sie anschließend auf die Schaltfläche **„Zurücksetzen“**.



Anschließend wird das Gateway neu gestartet und sofort auf die Werkseinstellungen zurückgesetzt.



Bitte 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

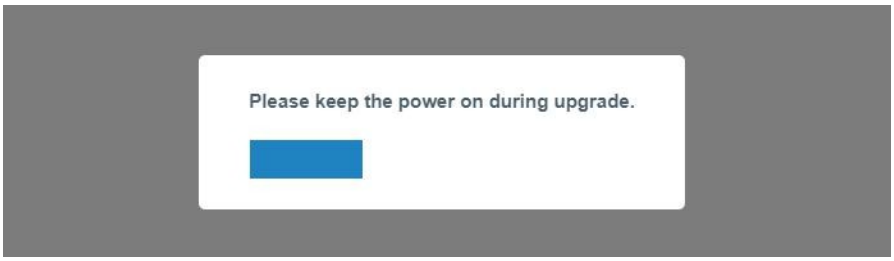
Suchen Sie die Reset-Taste am Gateway und halten Sie sie länger als 5 Sekunden gedrückt, bis die SYS-LED blinkt.

4.2 Firmware-Upgrade

Es wird empfohlen, sich vor dem Aktualisieren der Gateway-Firmware zunächst an den technischen Support von Milesight zu 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 zu „Wartung > Upgrade“.
2. Klicken Sie auf „Durchsuchen“ und wählen Sie die richtige Firmware-Datei auf Ihrem PC aus.
3. 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.
4. Öffnen Sie nach dem Upgrade die Gateway-Web-GUI über den Browser, um zu überprüfen, ob das Upgrade erfolgreich war.
   Vor dem Öffnen wird empfohlen, den Cache des Browsers zu leeren.



Verwandtes Thema

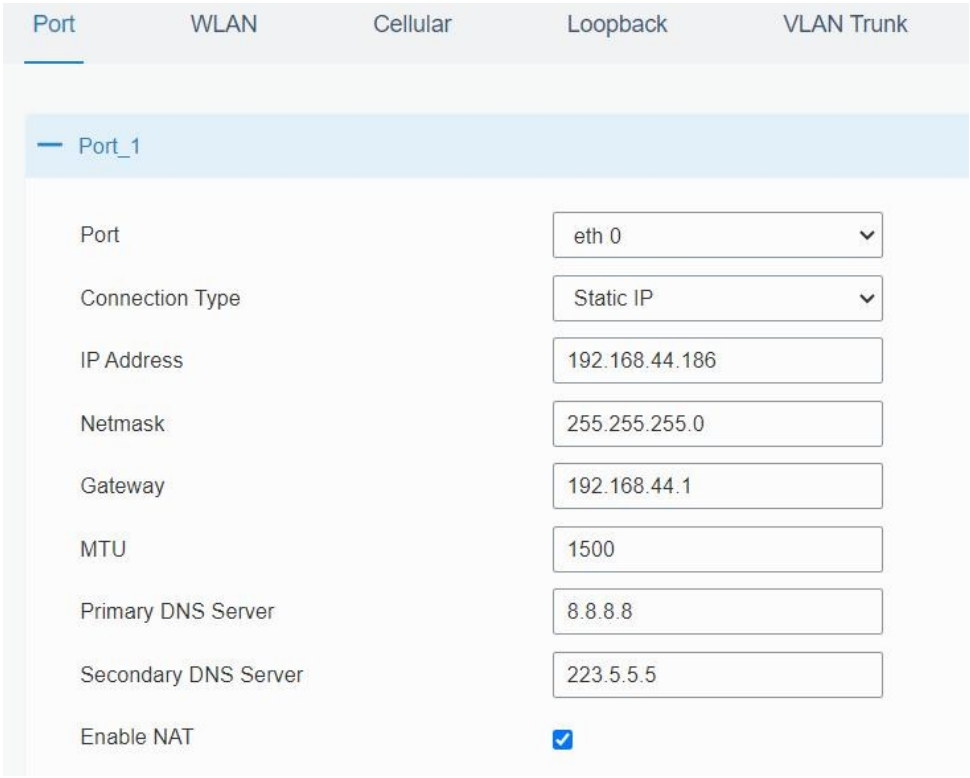
Upgrade

4.3 Netzwerkverbindung

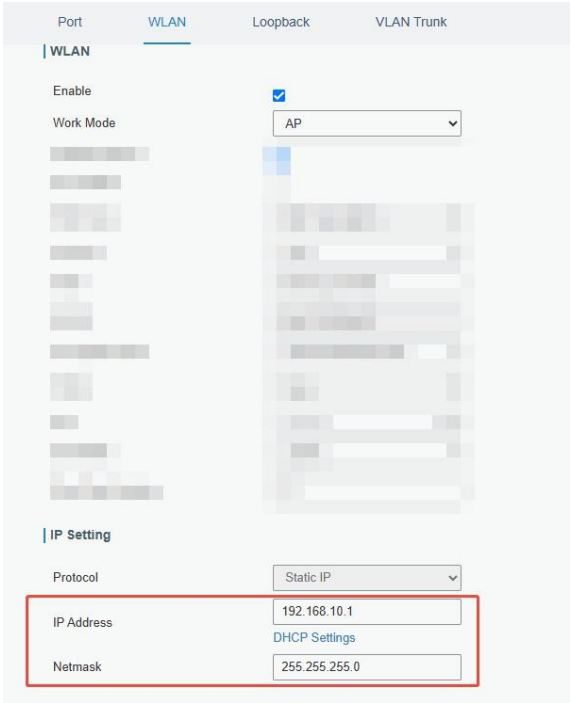
Das Gateway unterstützt mehrere Methoden zum Einrichten von Netzwerkverbindungen.

4.3.1 Ethernet-Verbindung

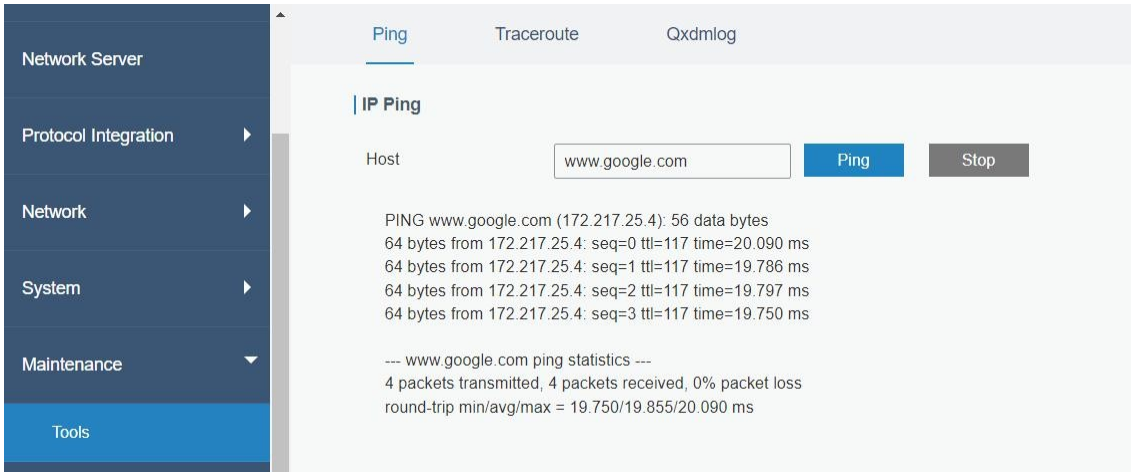
1. Gehen Sie zur Seite „Netzwerk > Schnittstelle > Port“, um den Verbindungstyp auszuwählen und die Ethernet-Port-Konfiguration zu konfigurieren. Klicken Sie auf „Speichern & Anwenden“, damit die Konfiguration wirksam wird.



Hinweis: Wenn beim Ändern der IP-Adresse des Ethernet-Ports ein IP-Konflikt auftritt, ändern Sie bitte zuerst das Subnetz des WLANs.



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

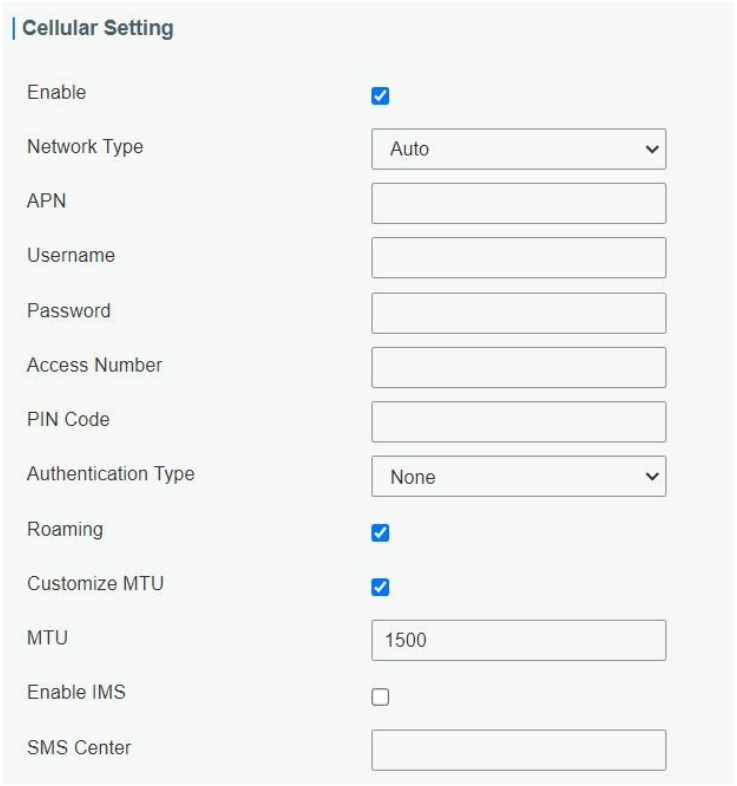


Verwandtes Thema

Port-Einstellung

4.3.2 Mobilfunkverbindung (nur Mobilfunkversion)

1. Gehen Sie zu „Netzwerk > Schnittstelle > Mobilfunk > Mobilfunkeinstellungen“ und konfigurieren Sie die erforderlichen Mobilfunkdaten der SIM-Karte. Klicken Sie auf „Speichern“ und „Übernehmen“, damit die Konfiguration wirksam wird.



2. Gehen Sie zu „Status > Mobilfunk“, um den Status der Mobilfunkverbindung anzuzeigen. Wenn „Verbunden“ angezeigt wird, hat die SIM-Karte erfolgreich eine Verbindung hergestellt.

Verwandtes Thema

Mobilfunk-Einstellungen

Mobilfunk-Status

4.4 Beispiel für die Wi-Fi-Anwendung

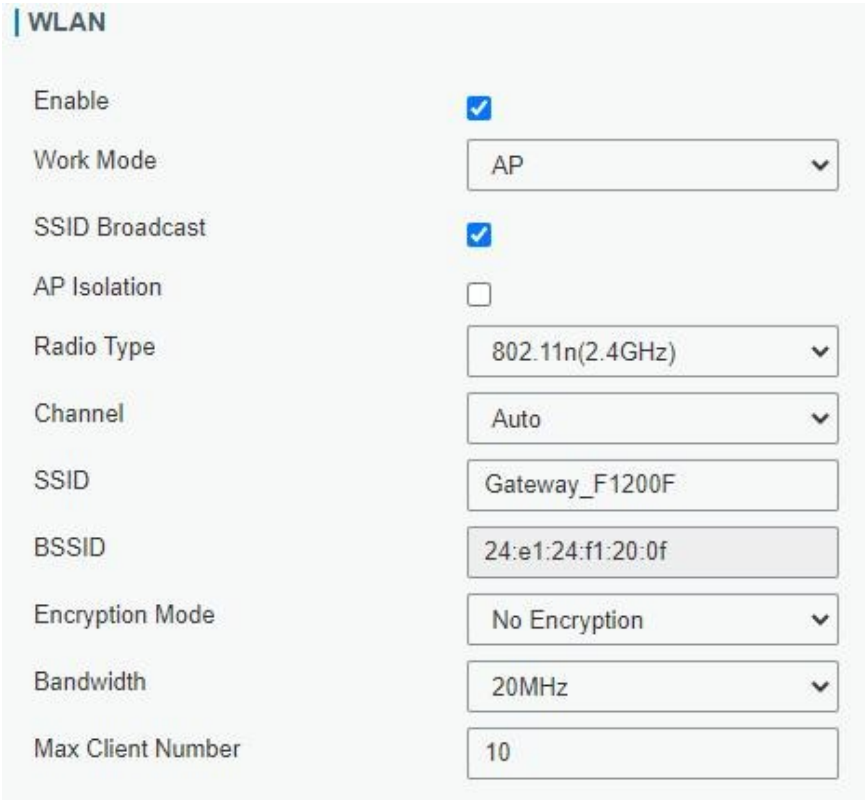
4.4.1 AP-Modus

Anwendungsbeispiel

Konfigurieren Sie UG67 als AP, um Verbindungen von Benutzern oder Geräten zuzulassen.

Konfigurationsschritte

1. Gehen Sie zu „Netzwerk > Schnittstelle > WLAN“, um die WLAN-Parameter wie unten beschrieben zu konfigurieren.



Klicken Sie nach Abschluss aller Konfigurationen auf die Schaltflächen „Speichern“ und „Übernehmen“.

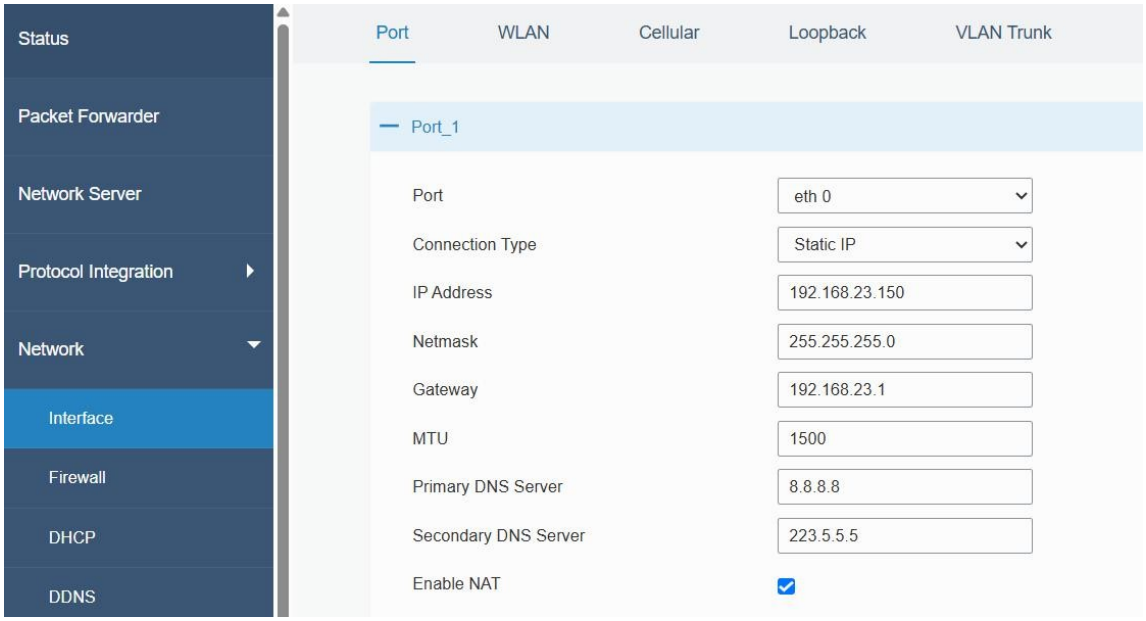
2. Verwenden Sie ein Smartphone, um eine Verbindung zum Zugangspunkt des Gateways herzustellen. Gehen Sie zu „Status > WLAN“,um die AP-Einstellungen und Informationen zu den verbundenen Clients/Benutzern zu überprüfen.

4.4.2 Anwendungsbeispiel für den Client-Modus

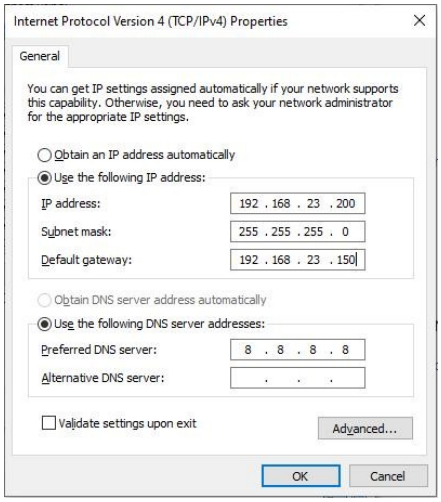
Konfigurieren Sie UG67 als WLAN-Client, um eine Verbindung zu einem Zugangspunkt herzustellen und Internetzugang zu erhalten.

Konfigurationsschritte

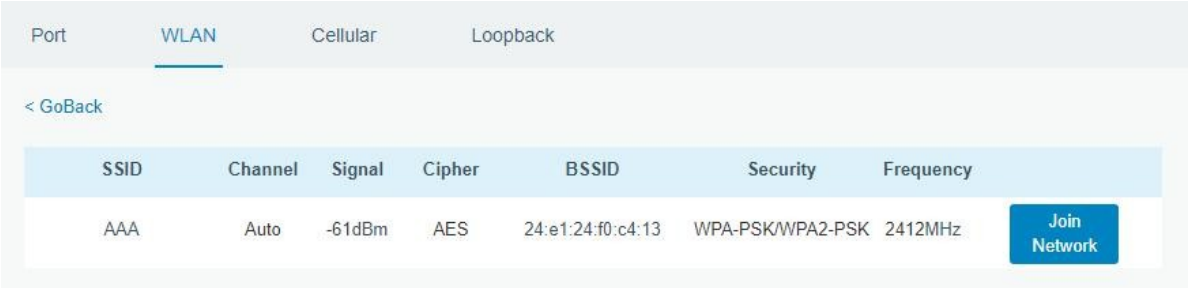
1. Gehen Sie zur Seite **„Netzwerk > Schnittstelle > Port“**, wählen Sie als Verbindungstyp **„Statische IP“** aus und konfigurieren Sie eine IP-Adresse für den Ethernet-WAN-Port.



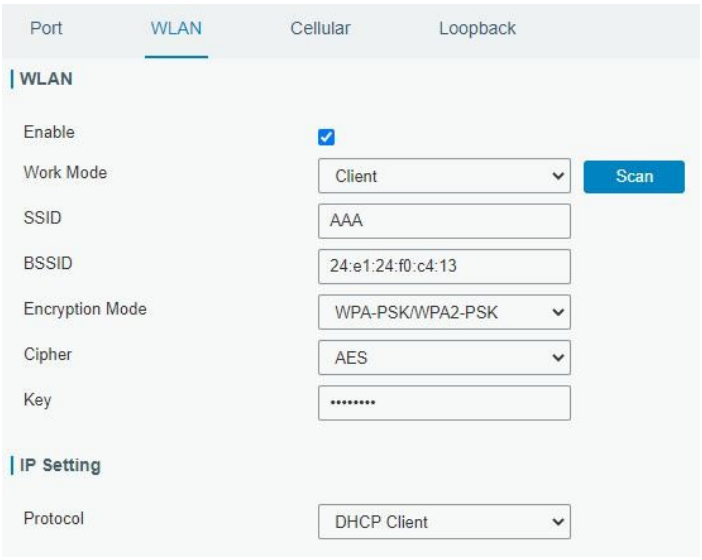
2. Verbinden Sie den PC direkt oder über einen PoE-Injektor mit dem ETH-Port des UG67.
3. Weisen Sie dem Computer die IP-Adresse manuell zu. Nehmen Sie als Beispiel das Windows 10-System:



4. Öffnen Sie einen Webbrowser und geben Sie die IP-Adresse des Ethernet-Ports ein, um auf die Web-GUI zuzugreifen.
5. Gehen Sie zu **Netzwerk > Schnittstelle > WLAN** und klicken Sie auf **Scannen,** um nach einem WLAN-Zugangspunkt zu suchen.

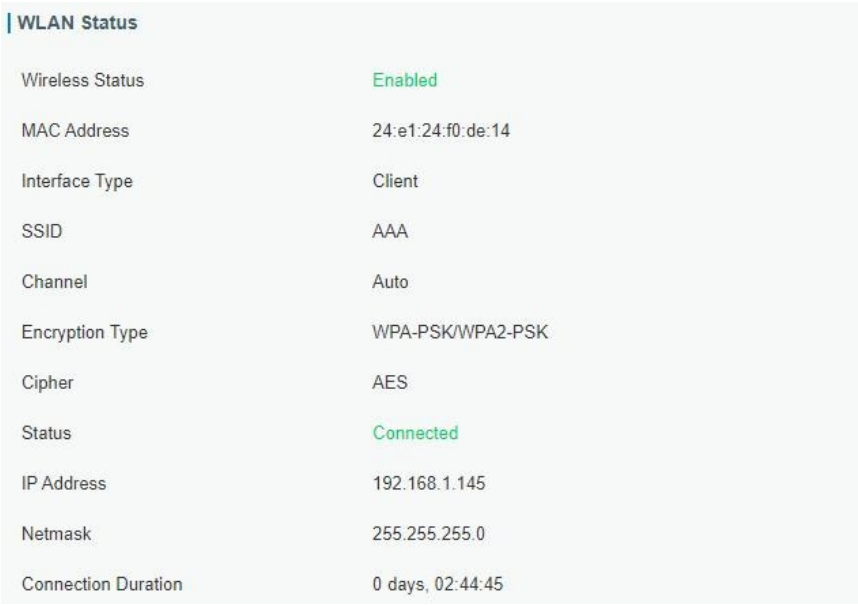


6. Wählen Sie einen Zugangspunkt aus und klicken Sie auf **„Mit Netzwerk verbinden“**, geben Sie dann das Passwort des Zugangspunkts ein.

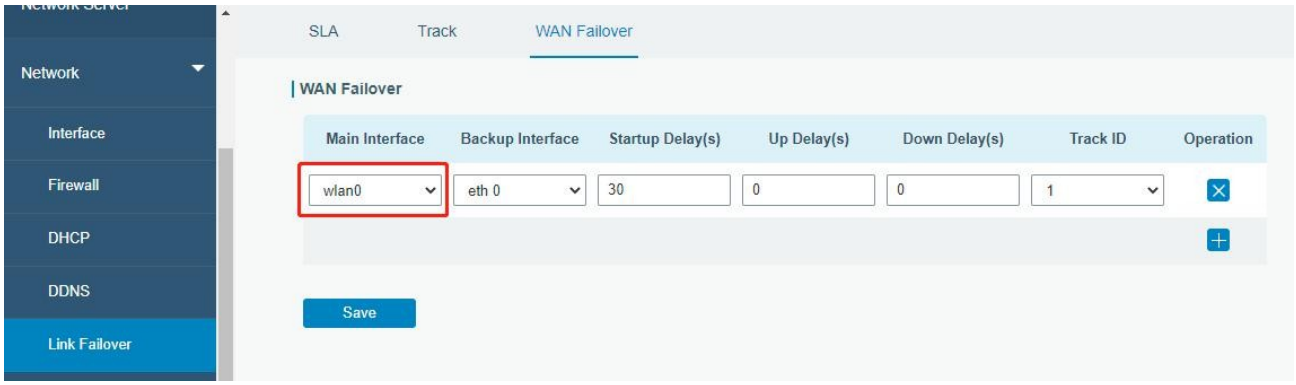


Klicken Sie nach Abschluss aller Konfigurationen auf die Schaltflächen **„Speichern“** und **„Übernehmen“**.

7. Gehen Sie zu **Status > WLAN,** um den Verbindungsstatus des Clients zu überprüfen.



8. Gehen Sie zu **Netzwerk > Failover > WAN-Failover**, um wlan0 als Hauptschnittstelle zu aktivieren, damit das Gateway über WLAN auf das Netzwerk zugreifen kann.



Verwandtes

Thema WLAN-

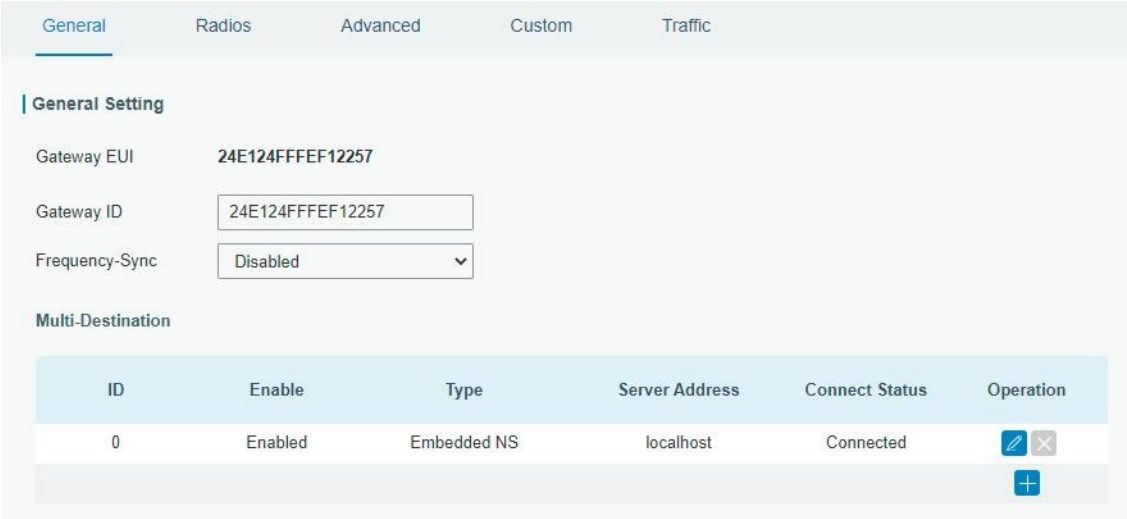
Einstellungen

WLAN-Status

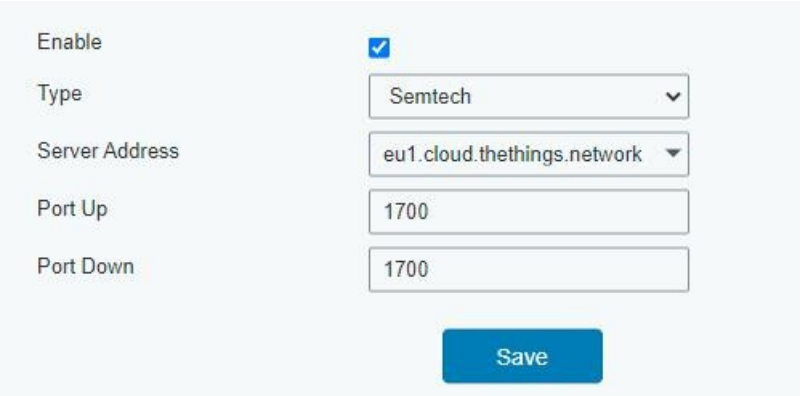
4.5 Konfiguration des Paketweiterleiters

Das UG67-Gateway verfügt über mehrere installierte Paketweiterleiter, darunter Semtech,Basic Station, Chirpstack usw. Vergewissern Sie sich vor dem Herstellen der Verbindung, dass das Gateway mit dem Netzwerk verbunden ist.

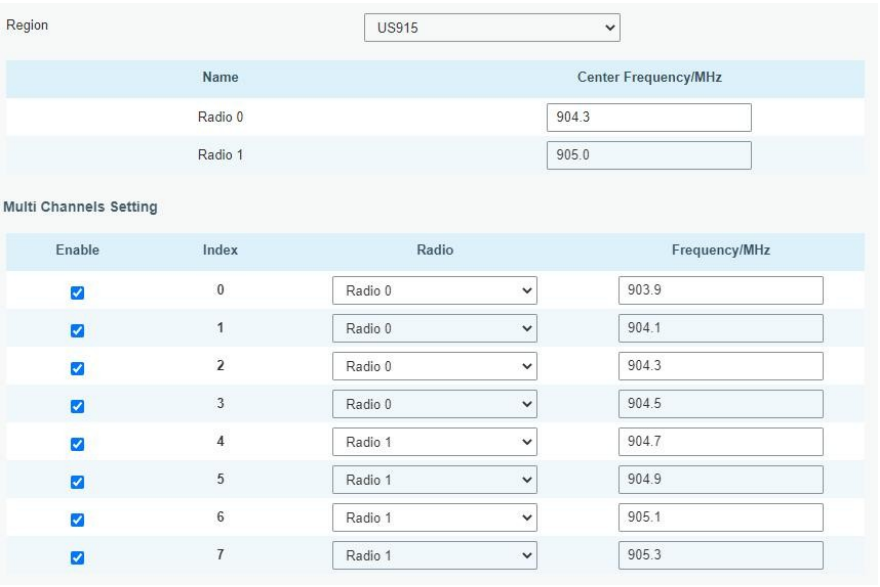
1. Gehen Sie zu **„Paketweiterleitung > Allgemein“**.



2. Klicken Sie auf „  “, um einen neuen Netzwerkserver hinzuzufügen. Geben Sie die Netzwerkserverinformationen ein und aktivieren Sie diesen Server.



3. Gehen Sie zur Seite **„Packet Forwarder > Radio“**, um die Mittenfrequenz und die Kanäle zu konfigurieren. Die Kanäle des Gateways und des Netzwerkservers müssen identisch sein.



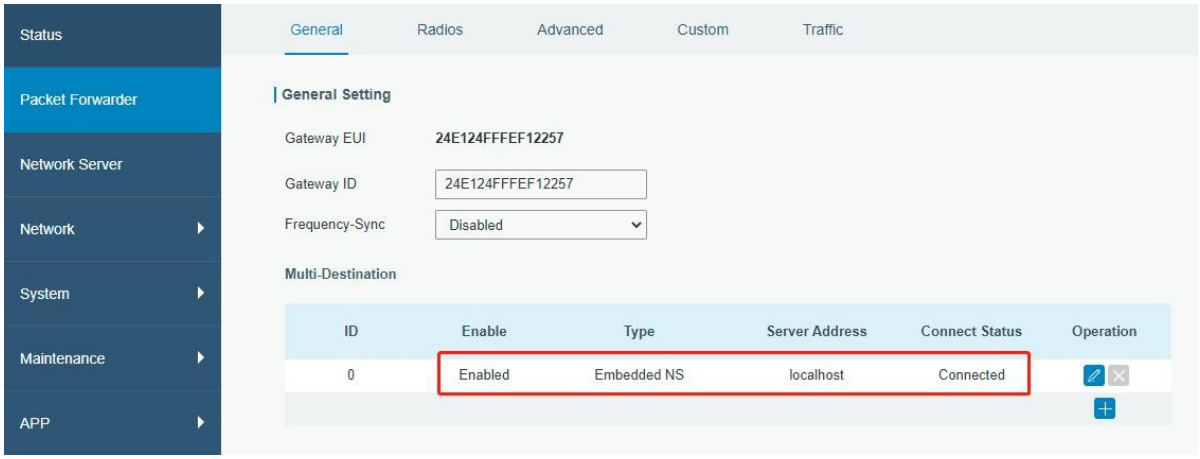
4. Fügen Sie das Gateway auf der Netzwerk-Server-Seite hinzu. Weitere Informationen zur Netzwerk-Server-Verbindung finden Sie im Milesight IoT Support-Portal.

4.6 Konfiguration des Netzwerkservers

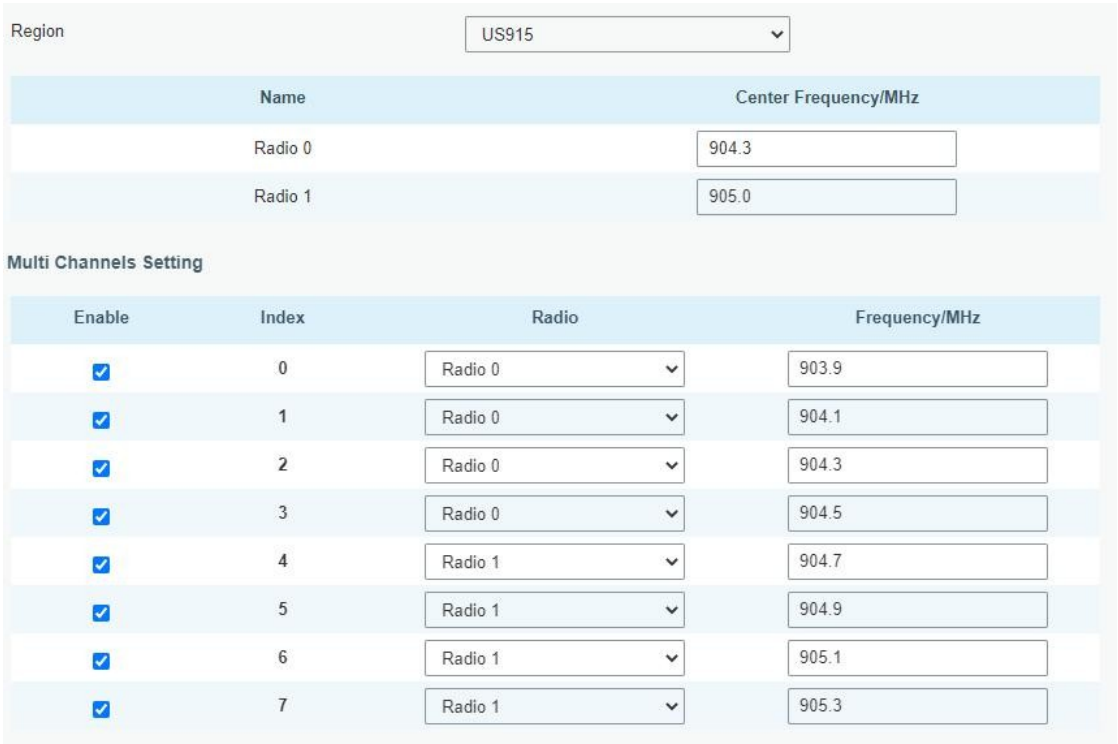
Das Gateway kann als LoRaWAN®-Netzwerkserver fungieren, um die Daten von LoRaWAN®-Endgeräten zu empfangen und zu analysieren und anschließend eine flexible Integration mit verschiedenen Systemen zu erreichen.

4.6.1 Verbindung zur Milesight IoT Cloud

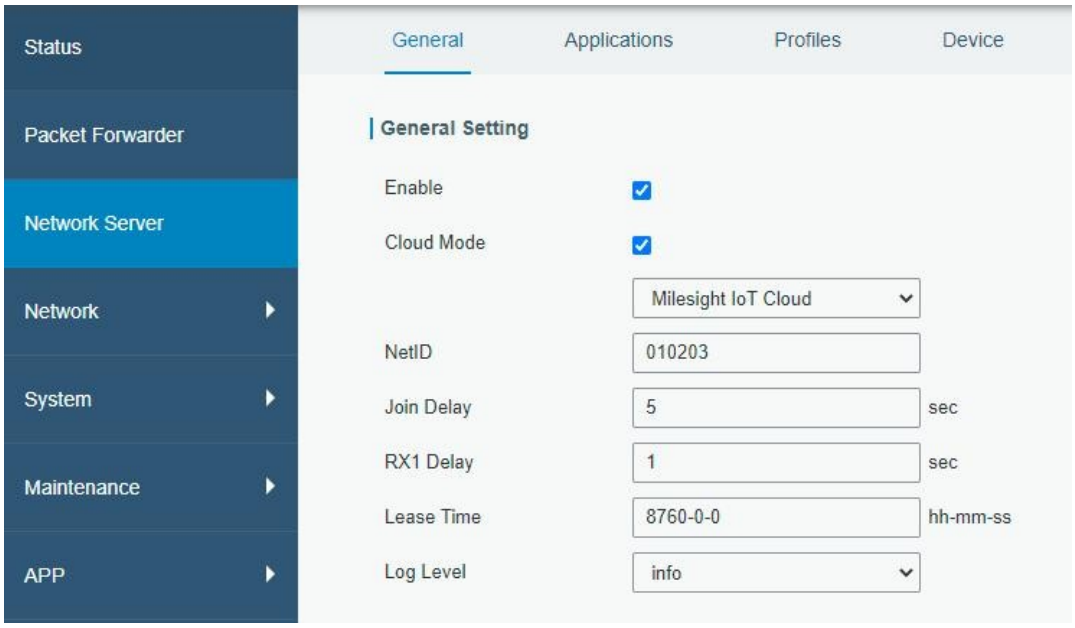
1. Gehen Sie zur Seite **„Packet Forwarder > General“**, um den integrierten Netzwerkserver zu aktivieren.



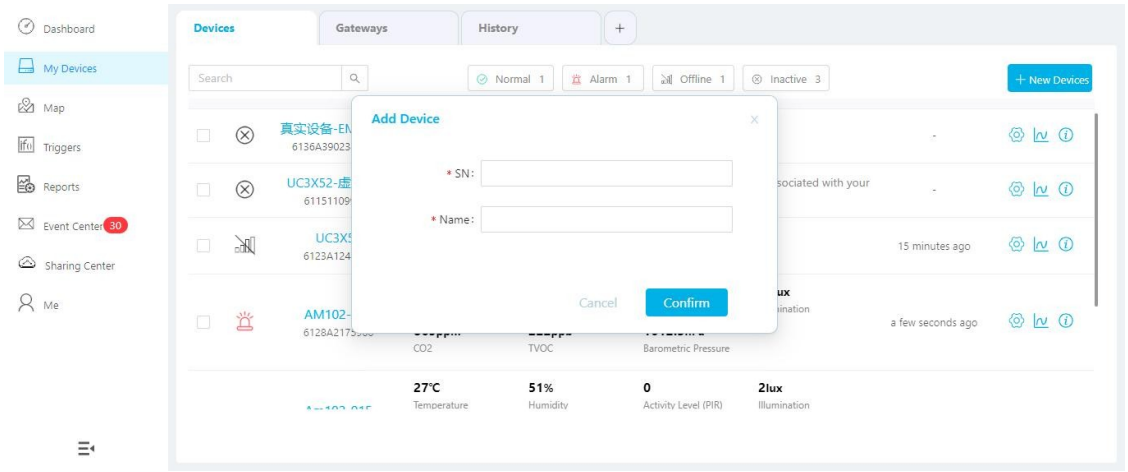
2. Gehen Sie zur Seite **„Packet Forwarder > Radio“**, um die Mittenfrequenz und die Kanäle zu konfigurieren. Die Kanäle des Gateways und der Endgeräte müssen identisch sein.



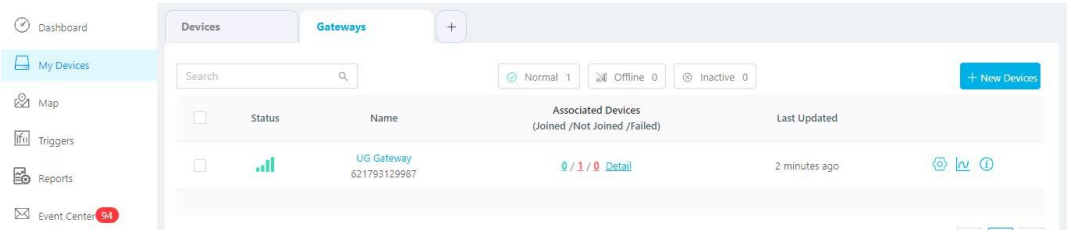
3. Gehen Sie zur Seite **„Netzwerkserver > Allgemein“**, um den Netzwerkserver und den „Cloud-Modus“ zu aktivieren, und wählen Sie dann den Modus „Milesight IoT Cloud“.



4. Melden Sie sich bei der Milesight IoT Cloud an. Gehen Sie dann zur Seite **„Meine Geräte“** und klicken Sie auf „+Neue Geräte“, um das Gateway über SN zur Milesight IoT Cloud hinzuzufügen. Das Gateway wird unter dem Menüpunkt „Gateways“ hinzugefügt.

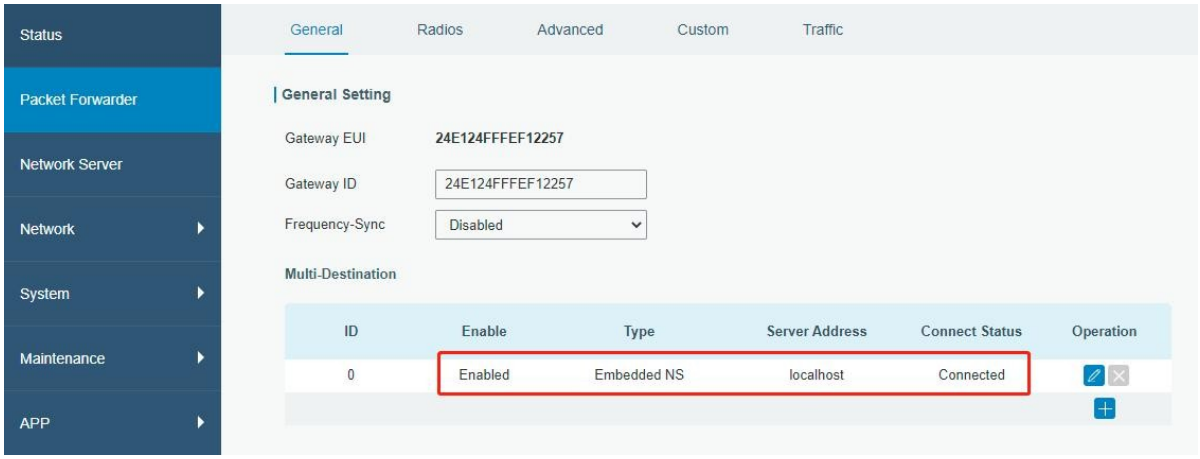


5. Das Gateway ist nun in der Milesight IoT Cloud online.

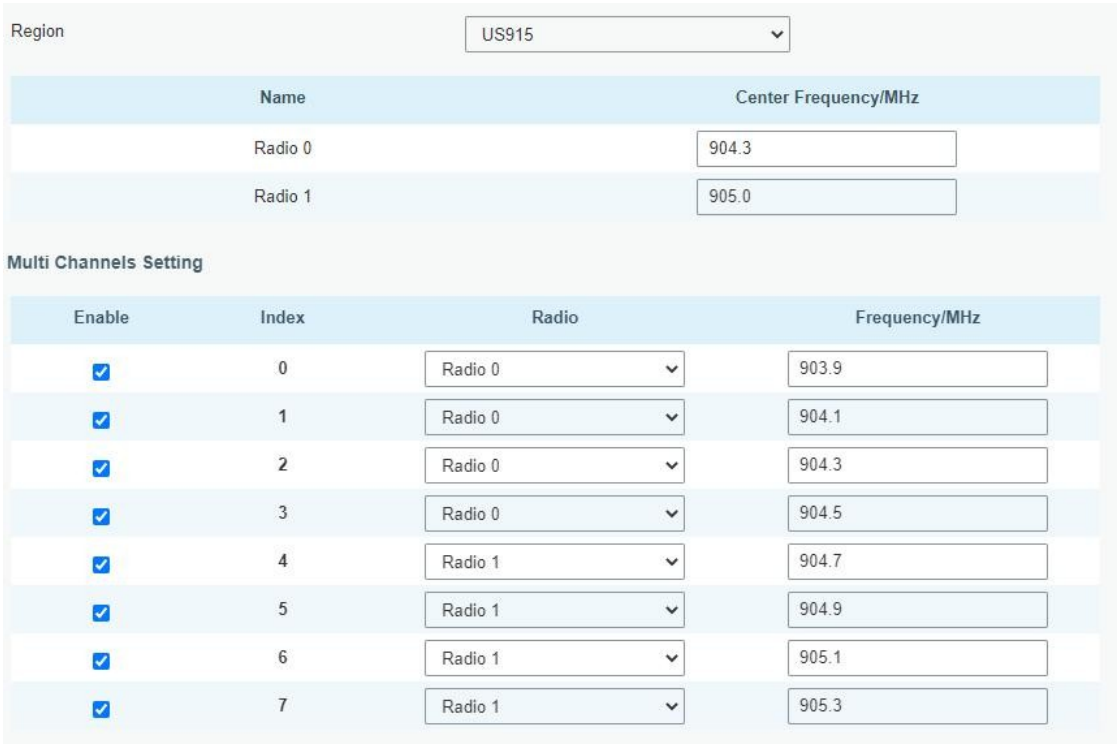


4.6.2 Endgeräte hinzufügen

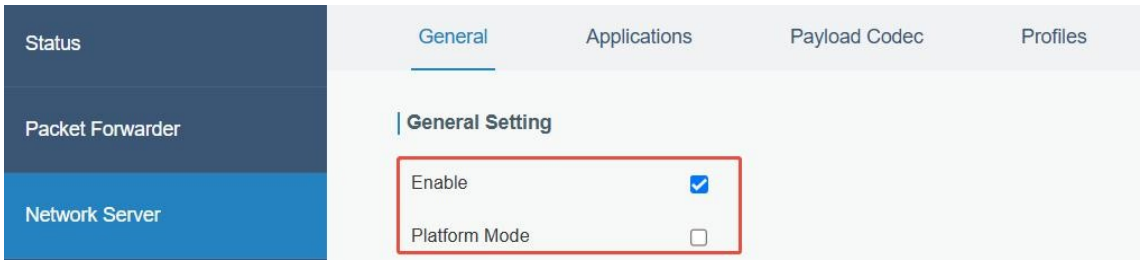
1. Gehen Sie zur Seite **„Paketweiterleitung > Allgemein“**, um das integrierte NS zu aktivieren.



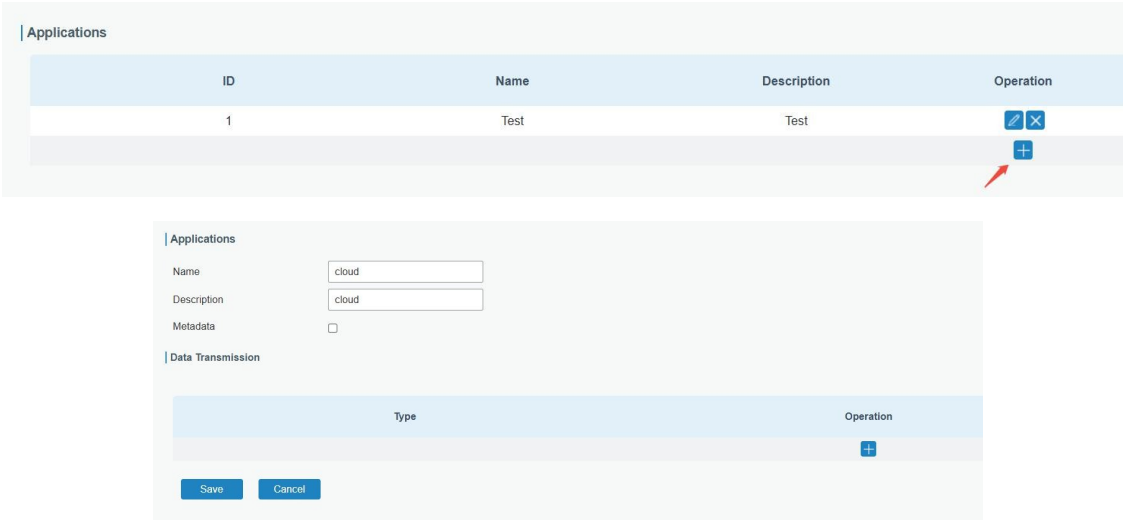
2. Gehen Sie zu **„Packet Forwarder" >** „Radio", um die Mittenfrequenz und die Kanäle zu konfigurieren. Die Kanäle des Gateways und der Endgeräte müssen identisch sein.



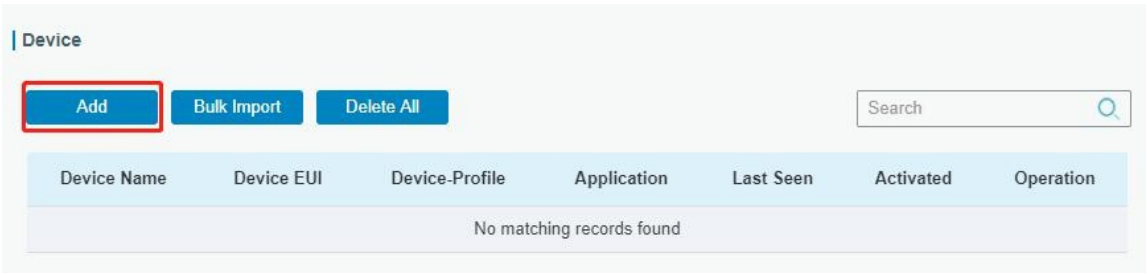
3. Gehen Sie zur Seite **„Netzwerkserver > Allgemein"**, um den Netzwerkserver zu aktivieren.



4. Gehen Sie zur Seite **„Netzwerkserver > Anwendungen"**, um eine Anwendung hinzuzufügen.



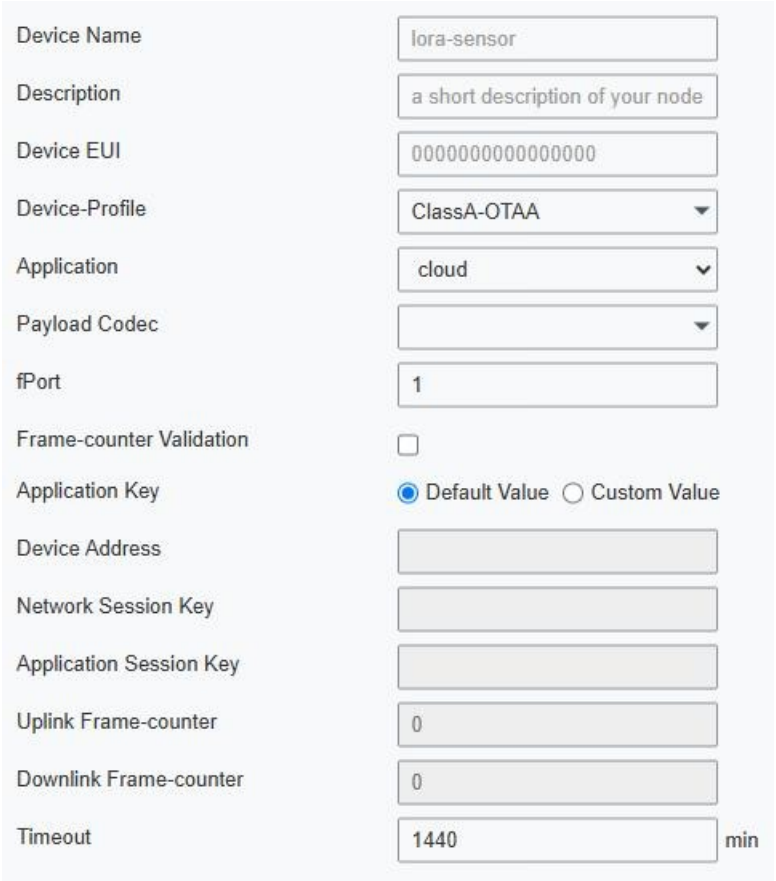
5. Gehen Sie zu **Netzwerk-Server >** Geräteseite und klicken Sie auf **Hinzufügen,** um ein LoRaWAN®-Knotengerät hinzuzufügen. Sie können auch auf **Massenimport** klicken, um mithilfe einer Vorlage



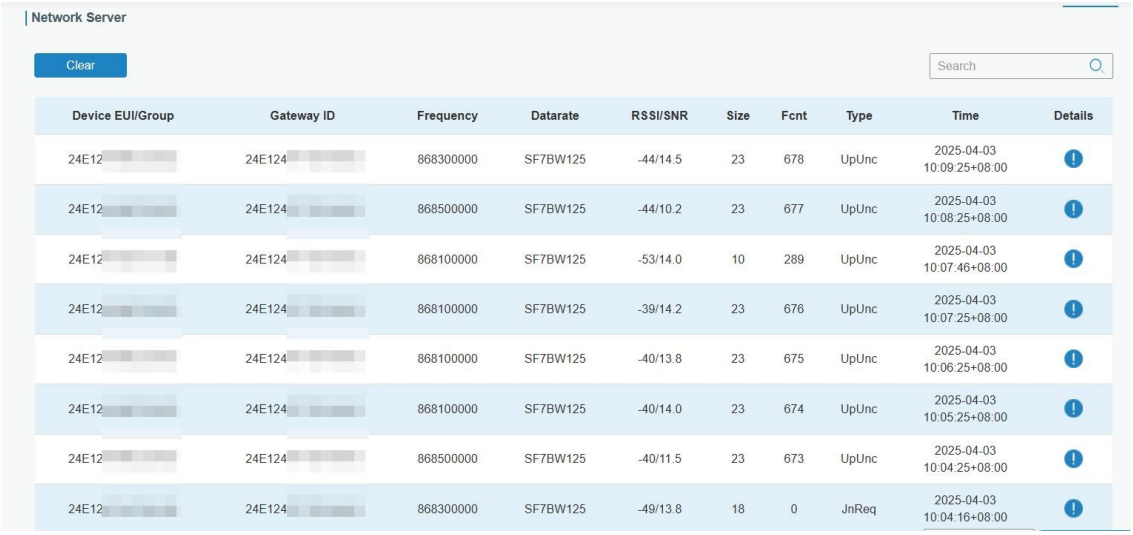
mehrere Geräte gleichzeitig hinzuzufügen.

6. Geben Sie die Informationen zum Endgerät ein und klicken Sie auf „**Speichern und anwenden**“. Die Informationen finden Sie auf der Konfigurationsseite des Endgeräts oder in den Handbüchern des Herstellers. Hier sind die Standardeinstellungen der Milesight-Endgeräte:

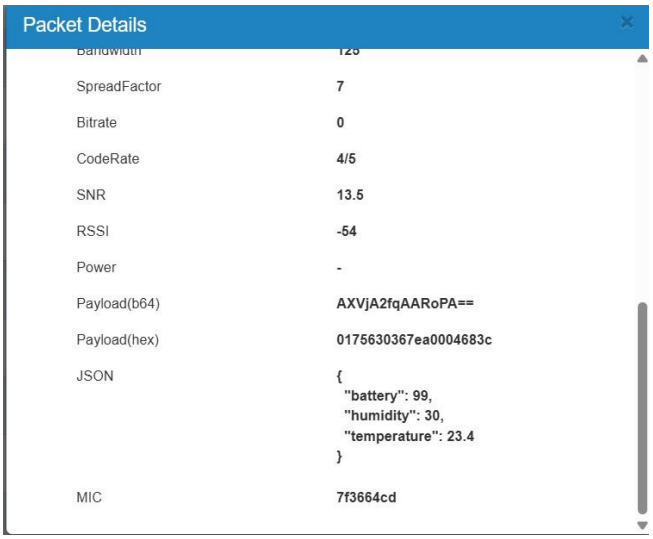
- Geräte-EUI: Diese finden Sie auf dem Gerät.
- Geräteprofil: OTAA-Dateien
- Nutzlast-Codec: Wählen Sie das Modell aus
- fPort: 85
- Anwendungsschlüssel: Wählen Sie „Standardwert“. Wenn Sie zufällige Schlüssel verwenden, wählen Sie bitte „Benutzerdefinierter Wert“.
- Zeitlimit: Die Zeit, nach der der Online-/Offline-Status des Geräts beurteilt wird.



7. Gehen Sie zur Seite **„Netzwerkserver > Pakete“**, um zu überprüfen, ob von diesem Gerät Uplinks vorhanden sind.

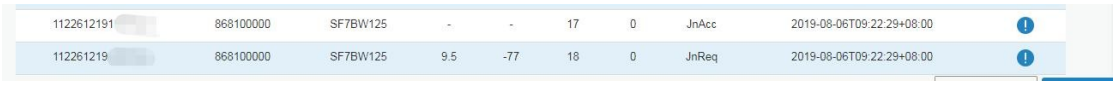


Klicken Sie auf **„Details“**, um die Paketdetails und die decodierten Ergebnisse zu überprüfen.



4.6.3 Daten an Gerät senden

1. Gehen Sie zu **Netzwerkserver > Pakete** und überprüfen Sie das Paket in der Netzwerkserverliste, um sicherzustellen, dass das Gerät erfolgreich mit dem Netzwerk verbunden ist.



2. Geben Sie die EUI des Geräts ein oder wählen Sie die Multicast-Gruppe aus, an die Sie Downlinks senden möchten. Geben Sie dann die Downlink-Befehle ⅈPorts ein.

3. Klicken Sie auf „Senden“.

4. Überprüfen Sie das Paket in der Netzwerkserverliste, um sicherzustellen, dass das Gerät diese Nachricht erfolgreich empfangen hat. Es wird empfohlen, „Bestätigt“ zu aktivieren. Die Multicast-Funktion unterstützt keine bestätigten Downlinks.

Sie können auf „Aktualisieren“ klicken, um die Liste zu aktualisieren, oder eine automatische Aktualisierungsfrequenz für die Liste festlegen. Wenn der Gerätetyp Klasse C ist, empfängt das Gerät ständig Pakete.

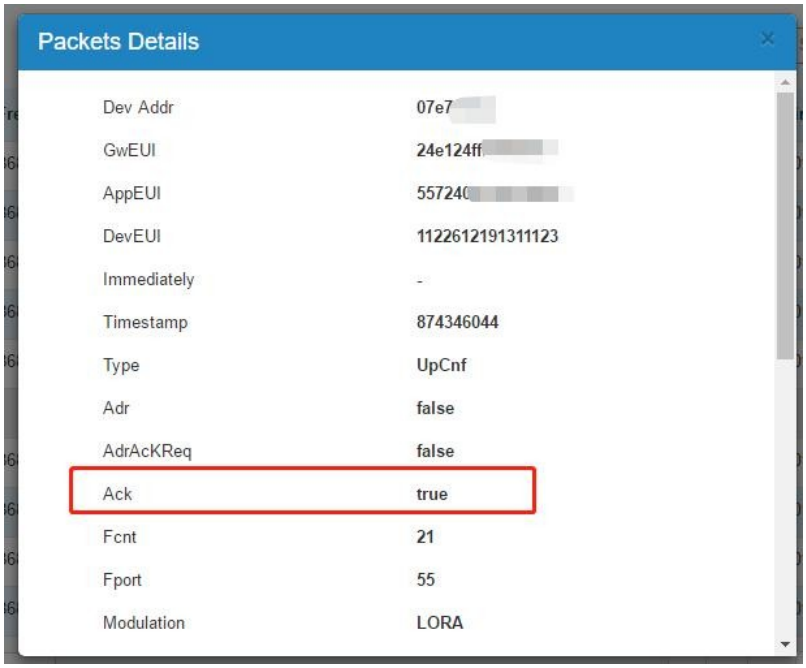
Der Typ dieses Pakets ist DnCnf (Downlink Confirmed Packet). Wenn das Paket grau ist, bedeutet dies, dass das Paket derzeit nicht übertragen werden kann, da sich mindestens eine Nachricht

in der Warteschlange steht. Wenn der Paketeintrag weiß ist, bedeutet dies, dass das Paket erfolgreich zugestellt wurde.

1122612191311123	869525000	SF12BW125	-	-	6	2	DnCnf	2019-08-06T09:22:55+08:00	Success
1122612191311123	0				6	2	DnCnf		Pending

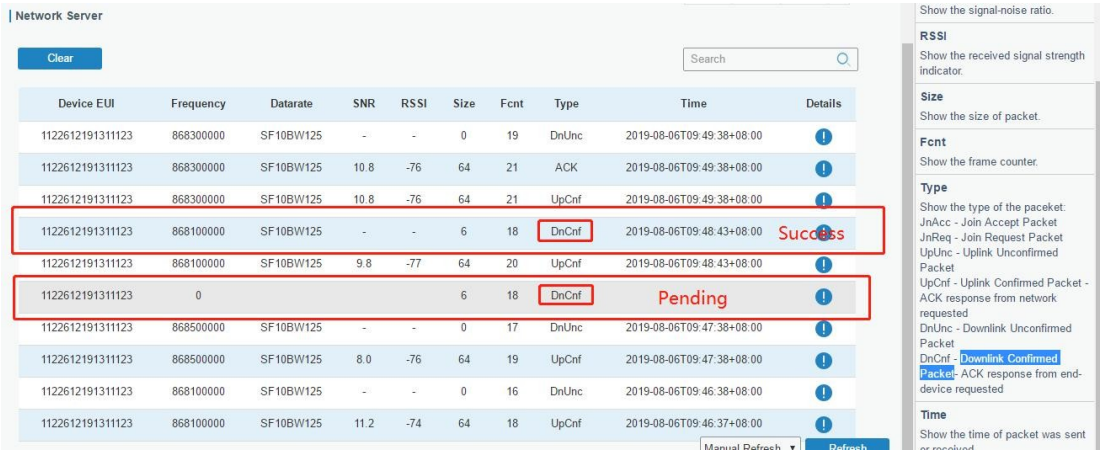
Wenn das Gerät dieses bestätigte Downlink-Paket empfängt, antwortet es bei der nächsten Übertragung mit „ACK“.

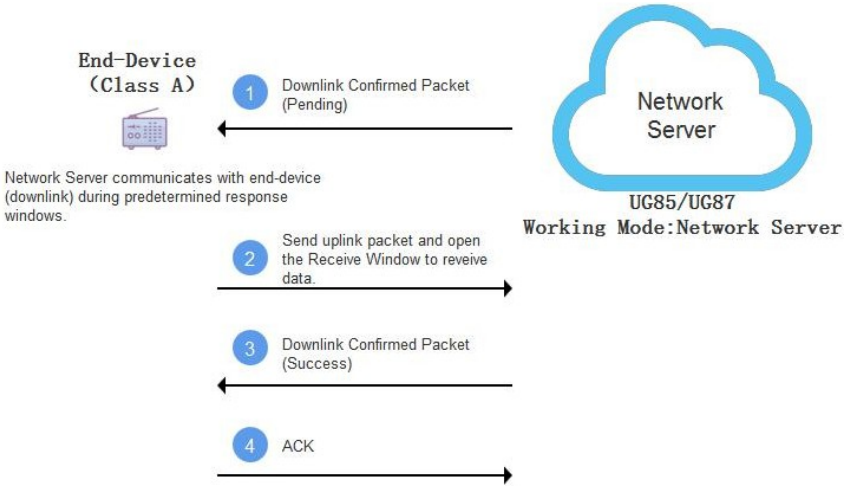
Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Type	Time	Details
11226121913	868300000	SF10BW125	-	-	0	3	DnUnc	2019-08-06T09:23:44+08:00	
1122612191	868300000	SF10BW125	10.5	-75	64	2	UpCnf	2019-08-06T09:23:44+08:00	
112261219	869525000	SF12BW125	-	-	6	2	DnCnf	2019-08-06T09:22:55+08:00	
112261219	0				6	2	DnCnf		
112261219	868500000	SF10BW125	-	-	0	1	DnUnc	2019-08-06T09:22:49+08:00	

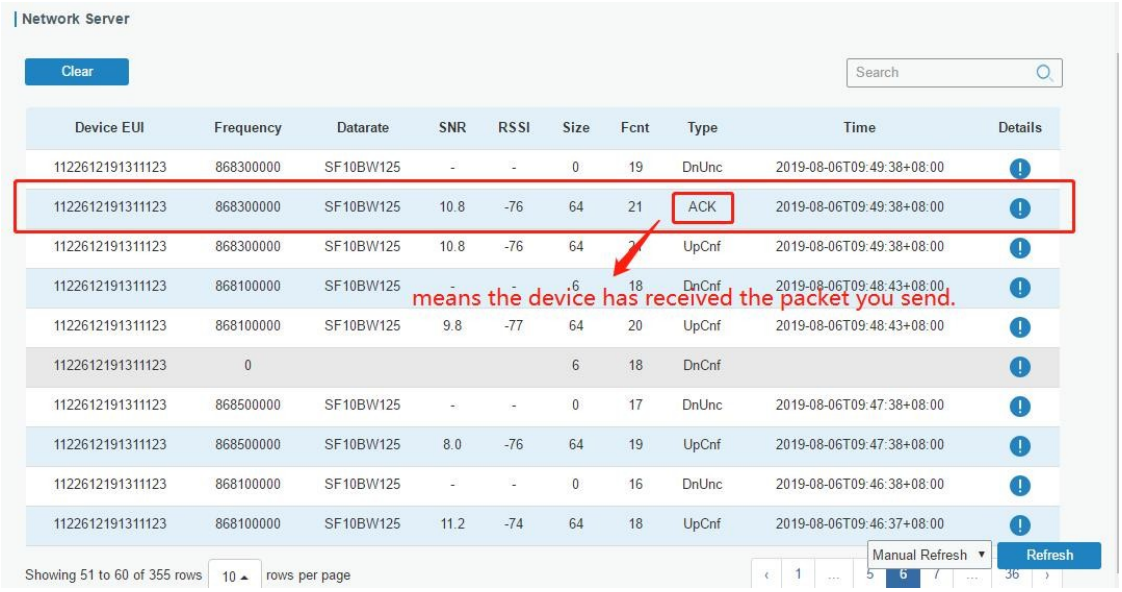


„ACK“ bedeutet, dass das Gerät dieses Paket empfangen hat.

Wenn der Gerätetyp Klasse A ist, sendet der Netzwerkserver erst dann Daten an das Gerät, nachdem das Gerät ein Uplink-Paket gesendet hat.







Verwandtes Thema

Pakete

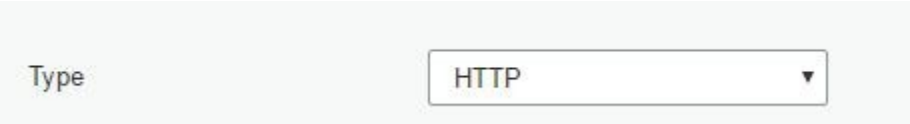
4.6.4 Verbindung zum HTTP/MQTT-Server herstellen

Das Gateway unterstützt die Auswahl des Datenübertragungsprotokolls, um Daten unter Verwendung des MQTT-,HTTP- oder HTTPS-Protokolls an eine andere Serveradresse zu senden.

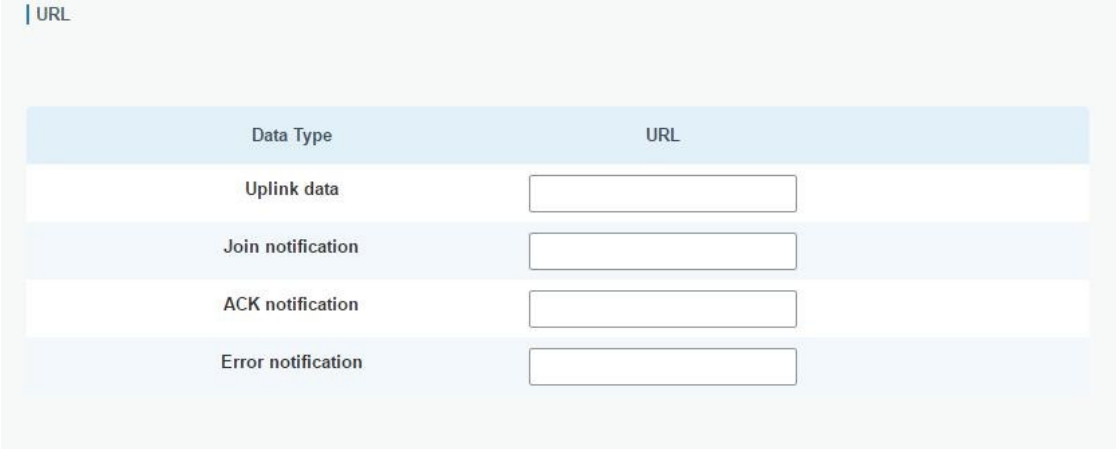
1. Gehen Sie zu **„Netzwerkserver > Anwendung“**, um die zu bearbeitende Anwendung auszuwählen.
2. Klicken Sie auf „ “ , um einen Datentransmissionstyp hinzuzufügen.

HTTP oder HTTPS:

Schritt 1: Wählen Sie HTTP oder HTTPS als Übertragungsprotokoll aus.



Schritt 2: Geben Sie die Ziel-URL ein. Verschiedene Datentypen können an verschiedene URLs gesendet werden.

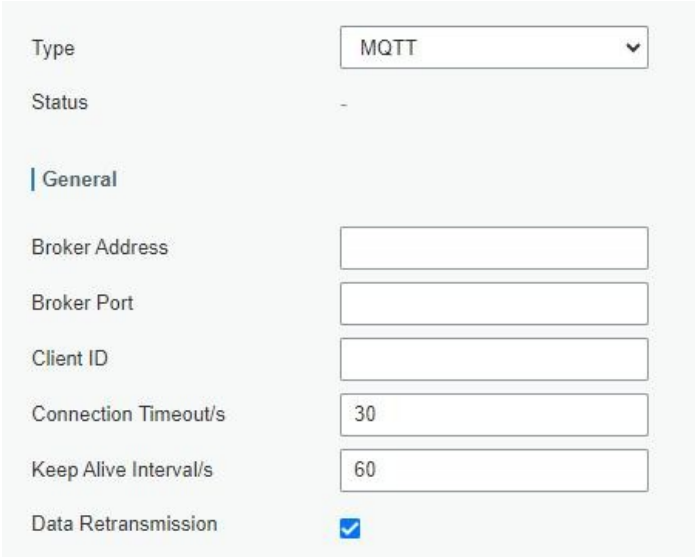


Geben Sie den Headernamen und den Headerwert ein, wenn beim Zugriff auf den HTTP(s)-Server Benutzeranmeldedaten erforderlich sind.

MQTT：

Schritt 1: Wählen Sie als Übertragungsprotokoll MQTT aus.

Schritt 2: Geben Sie die allgemeinen Einstellungen für den

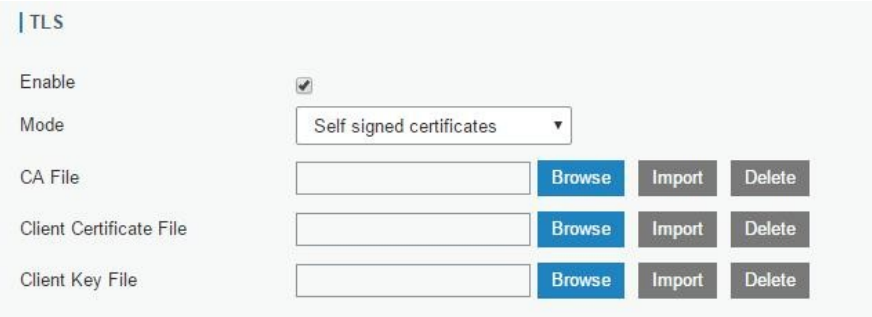


MQTT-Broker ein.

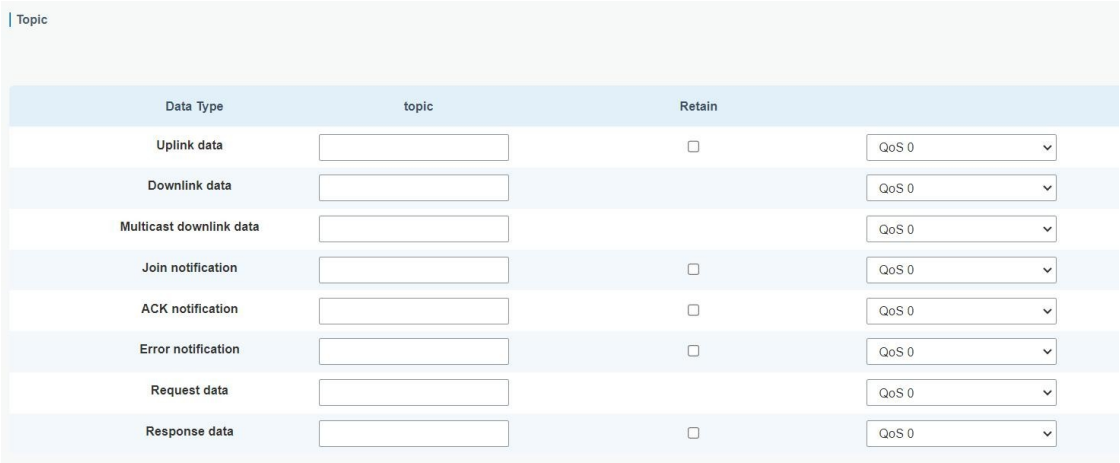
Schritt 3: Wählen Sie die vom Server geforderte Authentifizierungsmethode aus.

Wenn Sie für die Authentifizierung Benutzeranmeldedaten auswählen, müssen Sie den Benutzernamen und das Passwort für die Authentifizierung eingeben.

Wenn für die Überprüfung ein Zertifikat erforderlich ist, wählen Sie den Modus aus und importieren Sie das CA-Zertifikat, das Client-Zertifikat und die Client-Schlüsseldatei für die Authentifizierung.



Schritt 4: Geben Sie das Thema ein, um Daten zu empfangen oder Downlinks zu senden, und wählen Sie die QoS aus.

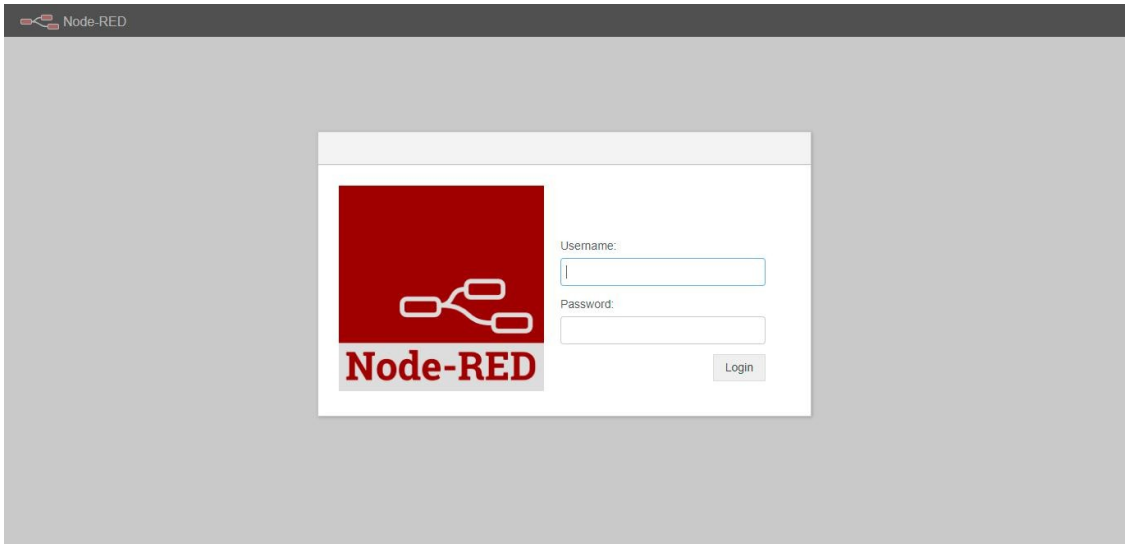


4.7 Node-RED

4.7.1 Starten Sie Node-RED

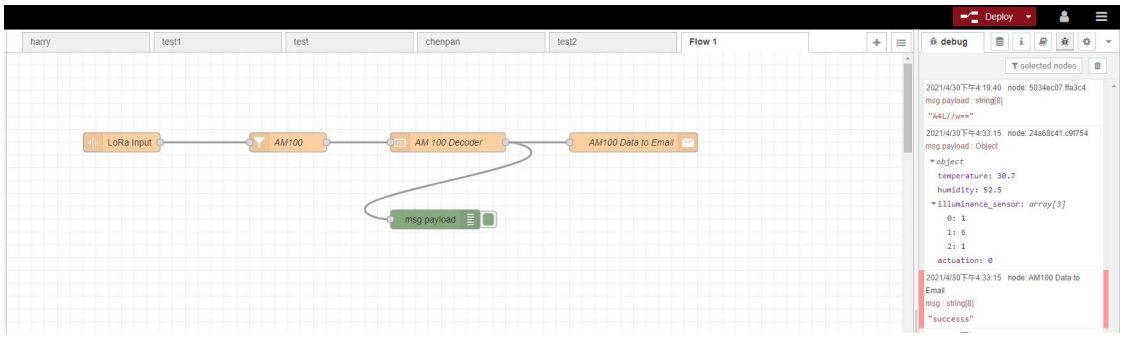
1. Gehen Sie zu „App > Node-RED“, um die Node-RED-Funktion zu aktivieren.

2. Klicken Sie nach der Aktivierung auf „Starten“, um zur Node-RED-Web-GUI zu gelangen und sich mit dem gleichen Benutzernamen und Passwort wie beim Gateway anzumelden.



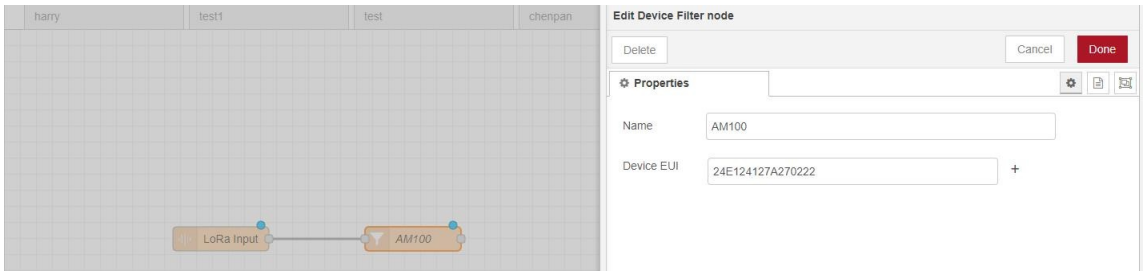
4.7.2 Beispiel für die Anwendung „Daten per E-Mail senden“

Senden Sie AM102-Gerätedaten per E-Mail.

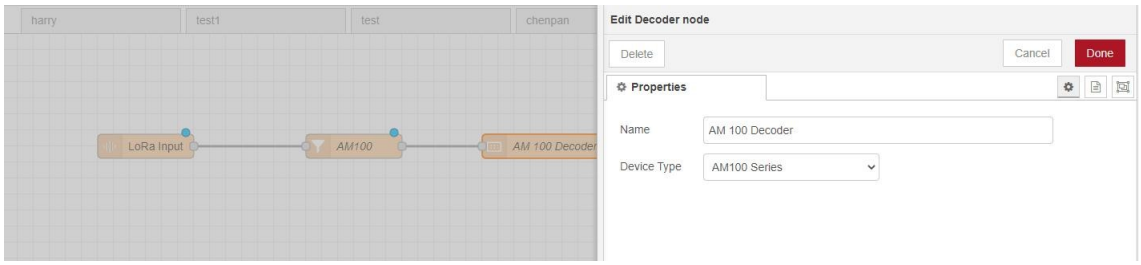


Konfigurationsschritte

1. Fügen Sie einen „LoRa Input”-Knoten hinzu. Bevor Sie diesen hinzufügen, stellen Sie bitte sicher, dass der Netzwerkservermodus aktiviert ist und die LoRaWAN-Geräte mit dem Netzwerk verbunden sind.
2. Wenn Sie viele Geräte hinzufügen und nur die Daten eines Geräts benötigen, fügen Sie hinter dem „LoRa-Eingabe“-Knoten einen „Gerätefilter“-Knoten hinzu und geben Sie die EUI des Geräts ein.



3. Fügen Sie einen „Decoder“-Knoten hinzu, um die Milesight-Sensordaten zu decodieren.

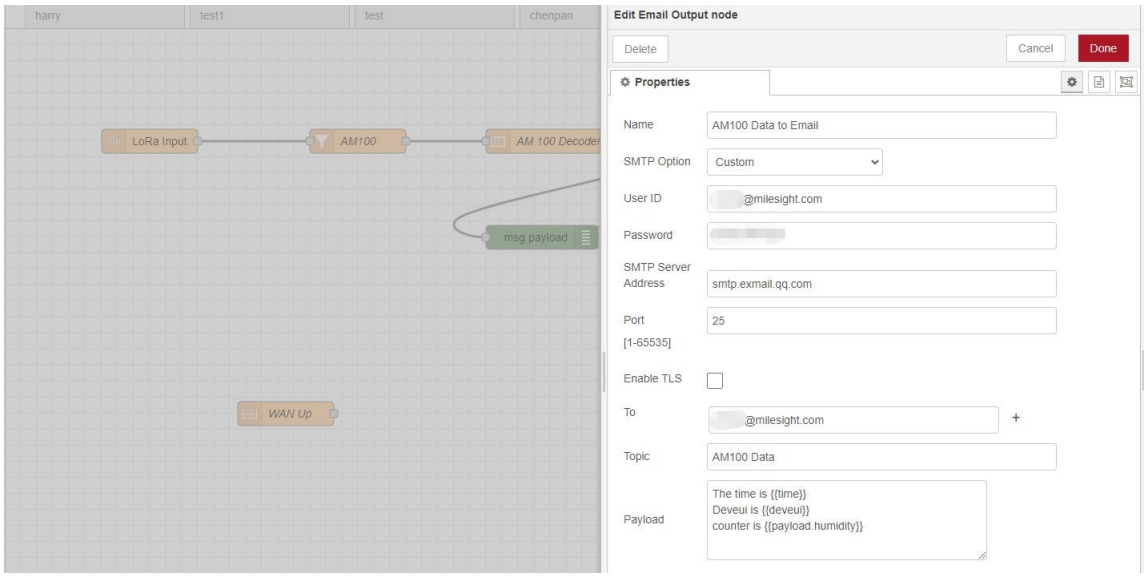


4. Fügen Sie einen „Email Output“ hinzu und geben Sie die SMTP-Client-Einstellungen, die Ziel-E-Mail-Adresse und den Inhalt ein. Beispielinhalt:

Die Uhrzeit ist {{time}} Deveui

ist {{deveui}}

Die Luftfeuchtigkeit beträgt {{payload.humidity}}



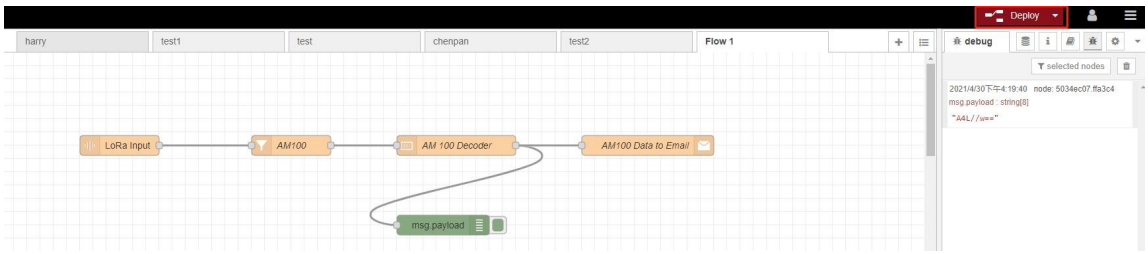
Hinweis:

1) Wenn Sie die SMTP-Option „Wie Gateway“ auswählen, gehen Sie zu „System -> Allgemeine Einstellungen -> SMTP“, um die SMTP-Clients zu konfigurieren.

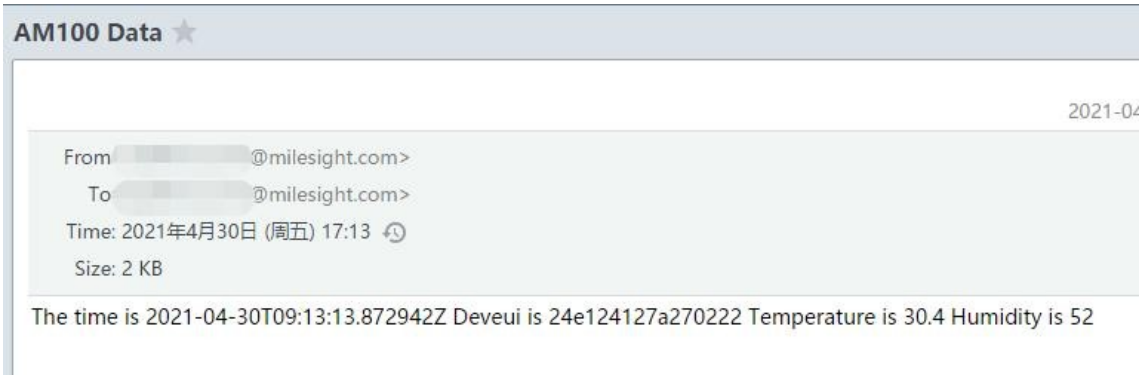
2) Das Grundformat zum Aufrufen von LoRaWAN-Knotendaten lautet *{{property name}}*. Weitere Informationen zum E-Mail- oder SMS-Nutzdatenformat finden Sie auf der Seite „Hilfe“.

3) Wenn Sie den Ausgabeeinhalt in jedem Knoten überprüfen müssen, fügen Sie bitte einen Debug-Knoten hinzu.

5. Nach Abschluss der Konfiguration klicken Sie auf „Bereitstellen“, um alle Ihre Einstellungen zu speichern.



6. Wenn AM102 Daten an das Gateway sendet, überträgt das Gateway die Daten an die E-Mail.



Verwandtes Thema

Node-RED

[ENDE]