Milesight

Industrielles LoRaWAN® Gateway

UG56

Benutzerhandbuch

Vorwort

Vielen Dank, dass Sie sich für das Milesight UG56 LoRaWAN® Gateway entschieden haben. Das UG56 bietet eine stabile Netzwerkverbindung mit umfassenden Funktionen wie automatischem Failover/Failback, erweitertem Betriebstemperaturbereich, zwei SIM-Karten, Hardware-Watchdog, VPN, Gigabit-Ethernet und vielem mehr.

Dieses Handbuch zeigt Ihnen, wie Sie das UG56 LoRaWAN® Gateway konfigurieren und bedienen. Hier finden Sie detaillierte Informationen zu den Funktionen und zur Konfiguration des Gateways.

Leser

Diese Anleitung richtet sich in erster Linie an folgende Benutzer:

- Netzwerkplaner
- Technischer Support und Wartungspersonal vor Ort
- Netzwerkadministratoren, die für die Netzwerkkonfiguration und -wartung zuständig sind

Verwandte Dokumente

Dokument	Beschreibung
UG56 Datenblatt	Datenblatt für UG56 LoRaWAN® Gateway.
UG56 Schnellstartanleitung	Schnellinstallationsanleitung für UG56 LoRaWAN® Gateway.

Konformitätserklärung

UG56 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 Tel.: 86-592-5085280
Fax: 86-592-5023065
Adresse: Gebäude C09, Software Park III, Xiamen 361024, China

Revisionsverlauf

Datum	Dokumentversion	Beschreibung
9. August 2022	V1.0	Erstversion

Inhalt

Kapitel 1 Produktvorstellung

1.1 Übersicht

UG56 ist ein robustes 8-Kanal-LoRaWAN®-Gateway für den industriellen Einsatz. Mit dem SX1302 LoRa-Chip und einer leistungsstarken Quad-Core-CPU unterstützt UG56 die Verbindung mit mehr als 2000 Knoten. UG56 hat eine Sichtverbindung von bis zu 15 km und kann in städtischen Gebieten eine Reichweite von etwa 2 km abdecken, was es ideal für intelligente Gebäude, intelligente Industrien und viele andere Innenanwendungen macht.

UG56 unterstützt nicht nur mehrere Backhaul-Backups mit Ethernet, WLAN und Mobilfunk, sondern verfügt auch über integrierte Mainstream-Netzwerkserver (wie TTI, ChirpStack usw.) sowie einen integrierten Netzwerkserver und die Milesight IoT Cloud für eine einfache Bereitstellung.

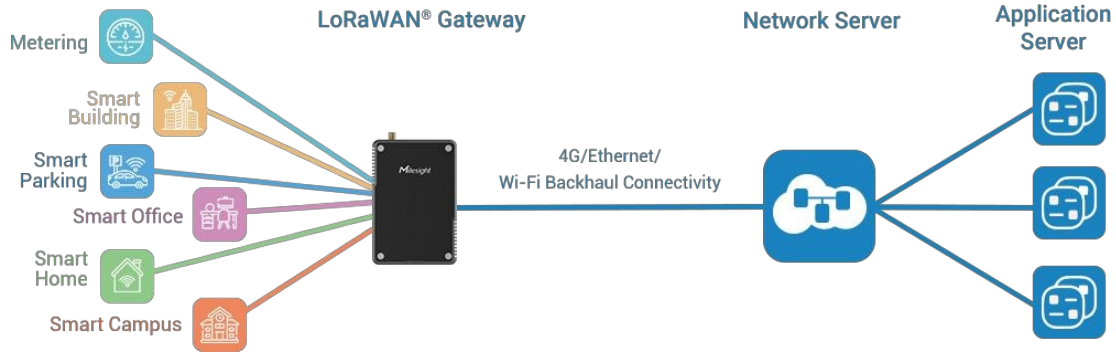


Abbildung 1-1

1.2 Vorteile

Vorteile

- Quad-Core-Industrie-CPU und großer Speicher
- Multi-Backhaul-Konnektivitäts-Backups mit Ethernet, 2,4-GHz-WLAN und globalen 3G/LTE-Optionen erleichtern die Verbindung
- Integrierter Netzwerkserver und kompatibel mit mehreren Netzwerkservern von Drittanbietern
- MQTT, HTTP- oder HTTPS-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
- Integrierter Hardware-Watchdog zur automatischen Wiederherstellung nach verschiedenen Ausfällen und zur Gewährleistung höchster Verfügbarkeit

Einfache Wartung

- Milesight DeviceHub bietet eine einfache Einrichtung, Massenkonfiguration und zentralisierte Verwaltung von Remote-Geräten
- Das benutzerfreundliche Design der Weboberfläche und verschiedene Upgrade-Optionen erleichtern Administratoren die Verwaltung des Geräts erheblich.
- Über die Web-GUI und die CLI kann der Administrator eine schnelle Konfiguration und einfache Verwaltung einer großen Anzahl von Geräten erreichen.
- Benutzer können die Remote-Geräte auf der bestehenden Plattform über den Industriestandard SNMP effizient verwalten.

Funktionen

- Verbinden Sie Remote-Geräte in einer Umgebung, in der sich die Kommunikationstechnologien ständig ändern.
- Industrieller Quad-Core-64-Bit-ARM-Cortex-A35-Prozessor, hohe Leistung mit bis zu 1,3 GHz bei geringem Stromverbrauch und 8 GB eMMC zur Unterstützung weiterer Anwendungen
- Unterstützt einen breiten Betriebstemperaturbereich von -20 °C bis 60 °C/-4 °F bis 140 °F

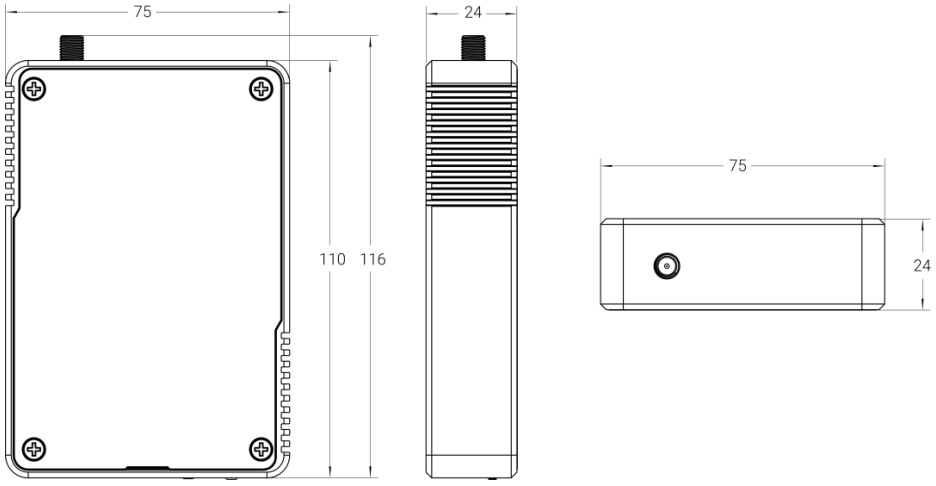
1.3 Technische Daten

Hardware-System	
CPU	Quad-Core 1,3 GHz, 64-Bit ARM Cortex-A35
Speicher	512 MB DDR3 RAM
Flash	8 GB eMMC
Erweiterbarer Speicher	1 × Micro-SD-Steckplatz (intern)
LoRaWAN	
Antennenanschluss	1 × 50 Ω SMA-Anschluss (Mittelstift: SMA-Buchse) Kanal
	8 (Halb-/Vollduplex)
Frequenzband	CN470/IN865/EU868/RU864/US915/AU915/KR920/AS923-1&2&3&4
Empfindlichkeit	-140 dBm Empfindlichkeit bei 292 bps
Ausgangsleistung	27 dBm max.
Protokoll	V1.0 Klasse A/Klasse B/Klasse C und V1.0.2 Klasse A/Klasse B/Klasse C
LBT	Unterstü
Ethernet-Schnittstelle	
Anschluss	1 × RJ45 (PoE PD unterstützt)

Physikalische Schicht	10/100 Base-T (IEEE 802.3)
Datenrate	10/100 Mbit/s (automatische
Erkennung)	
Schnittstelle	Auto MDI/MDIX
Modus	Voll- oder Halbduplex (automatische
WLAN-Schnittstelle	
Antenne	Interne Antenne
Standards	IEEE 802.11b/g/n, 2,4 GHz
Modus	AP- oder Client-Modus
Sicherheit	WPA/WPA2-Authentifizierung, WEP/TKIP/AES-Verschlüsselung
Sendeleistung	802.11b: 18 dBm +/-2,0 dBm (11 Mbit/s) 802.11g: 15 dBm +/-2,0 dBm (6 Mbit/s) 802.11g: 15 dBm +/-2,0 dBm (54 Mbit/s) 802.11n@2.4 GHz: 14 dBm +/-2,0 dBm (MCS0_HT20) 802.11n@2.4-GHz: 14 dBm +/-2,0 dBm (MCS7_HT20) 802.11n@2.4-GHz: 13 dBm +/-2,0 dBm (MCS0_HT40) 802.11n@2.4-GHz: 13 dBm +/-2,0 dBm (MCS7_HT40)
Mobilfunk-Schnittstelle (optional)	
Antenne	Interne Antenne
SIM-	1 (Mini-SIM-2FF)
Sonstiges	
Reset-Taste	1 × RST (intern)
Konsolenanschluss	1 × Typ C
LED-Anzeigen	1 × SYSTEM, 1 × LoRa
Integrier	Watchdog, Timer
Software	
Netzwerkprotokolle	PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, DDNS, HTTP, HTTPS, DNS, ARP, SNTP, Telnet, SSH, MQTT usw.
VPN-Tunnel	OpenVPN/IPsec/PPTP/L2TP/GRE/DMVPN Firewall
	ACL/DMZ/Port-Zuordnung/MAC-Bindung/URL-Filter
Verwaltung	Web, CLI, SMS, On-Demand-Einwahl, DeviceHub, Milesight IoT Cloud
Zuverlässigkeit	WAN-Failover
App	Python SDK, Node-RED
Stromversorgung	
Stromeingang	1. 1 × 802.3 af PoE-Eingang

	2. 5 V, 2 A über Typ-C-Anschluss
Physikalische Eigenschaften	
Schutzart	IP30
Gehäuse und Farbe	Metall, schwarz
Abmessungen	110 x 75 x 24 mm (4,33 x 2,95 x 0,94 Zoll)
Installation	Tischgerät, Wandmontage
Umgebung	
Betriebstemperatur	-20 °C bis +60 °C (-4 °F bis +140 °F)
Lagertemperatur	-40 °C bis +85 °C (-40 °F bis +185 °F)
Ethernet-Isolation	1,5 kV RMS
Relative Luftfeuchtigkeit	0 % bis 95 % (nicht kondensierend) bei 25 °C/77 °F

1.4 Abmessungen (mm)

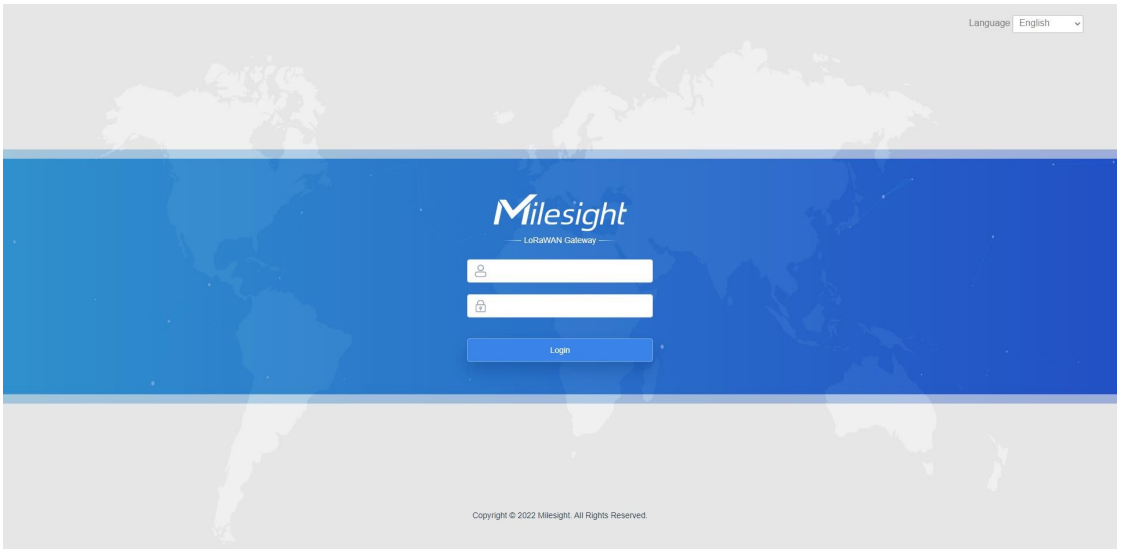


Kapitel 2 Zugriff auf die Web-GUI

In diesem Kapitel wird erläutert, wie Sie auf die Web-GUI des UG56 zugreifen können. Benutzername: **admin**
Passwort: **password**

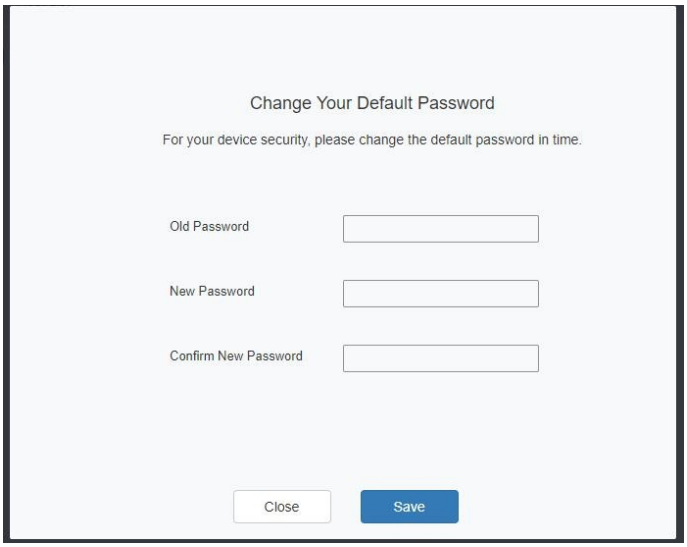
2.1 Drahtloser Zugriff

1. Aktivieren Sie die WLAN-Verbindung auf Ihrem Computer und suchen Sie nach dem Zugangspunkt „Gateway_******“, um eine Verbindung herzustellen.
2. Öffnen Sie einen Webbrowser auf Ihrem PC (Chrome wird empfohlen) und geben Sie die IP-Adresse ein. **192.168.1.1**, um auf die Web-GUI zuzugreifen.
3. Geben Sie den Benutzernamen und das Passwort ein und klicken Sie auf „Anmelden“.

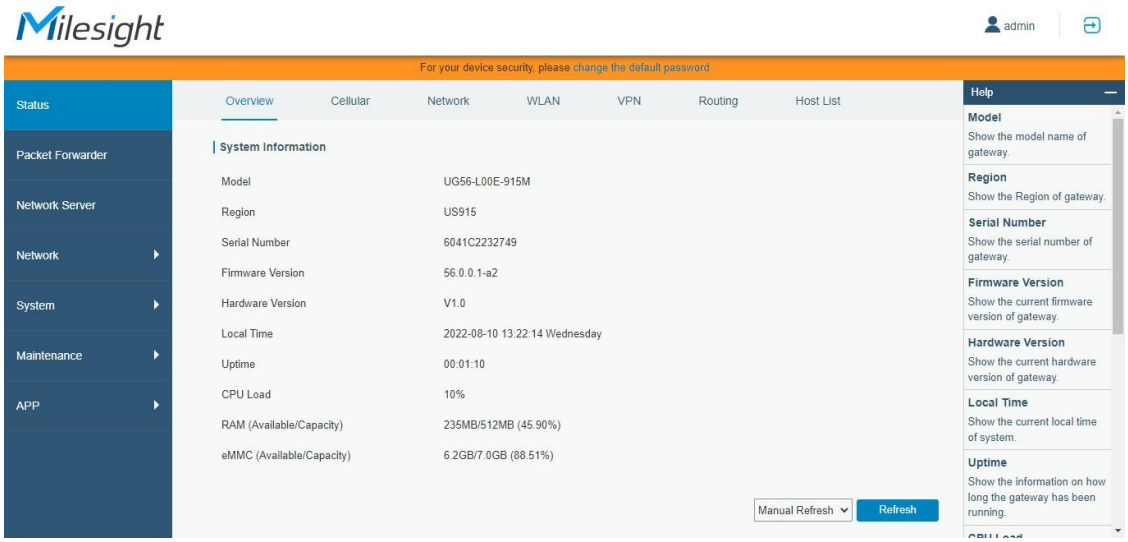


Wenn Sie den Benutzernamen oder das Passwort mehr als fünf Mal falsch eingeben, wird die Anmeldeseite für 10 Minuten gesperrt.

4. Befolgen Sie nach der Anmeldung bei der Web-GUI die Anleitung, um die Grundkonfigurationen abzuschließen. Aus Sicherheitsgründen wird empfohlen, das Passwort zu ändern.



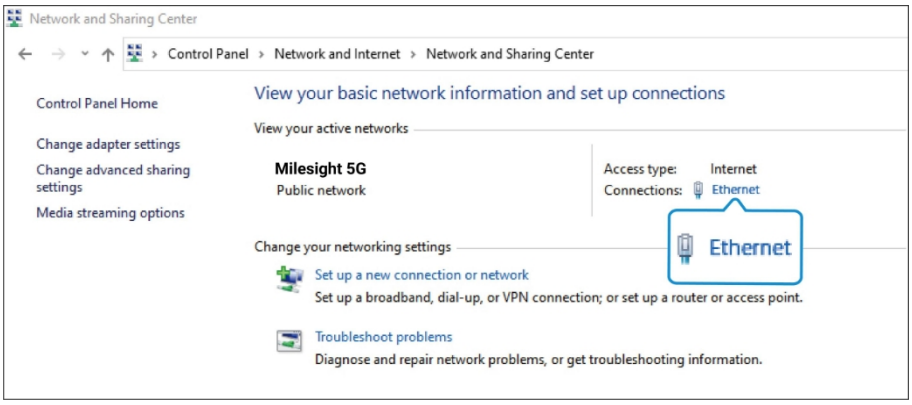
5. Sie können Systeminformationen anzeigen und die Konfiguration des Gateways vornehmen.



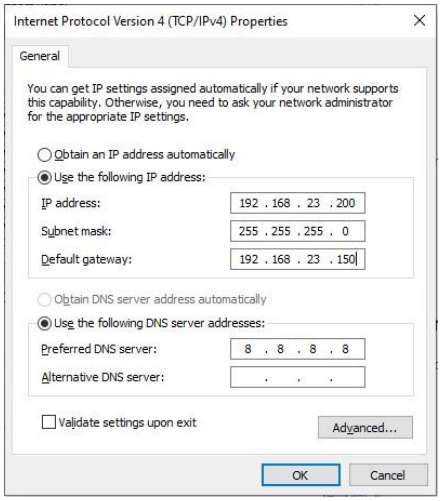
2.2 Kabelgebundener Zugang

Verbinden Sie den PC direkt oder über einen PoE-Injektor mit dem ETH-Port des UG56, um auf die Web-GUI des Gateways zuzugreifen. Die folgenden Schritte basieren auf dem Windows 10-System und dienen als Referenz.

1. Gehen Sie zu „Systemsteuerung“ →„Netzwerk und Internet“ →„Netzwerk- und Freigabecenter“ und klicken Sie dann klicken Sie auf „Ethernet“ (kann auch einen anderen Namen haben).

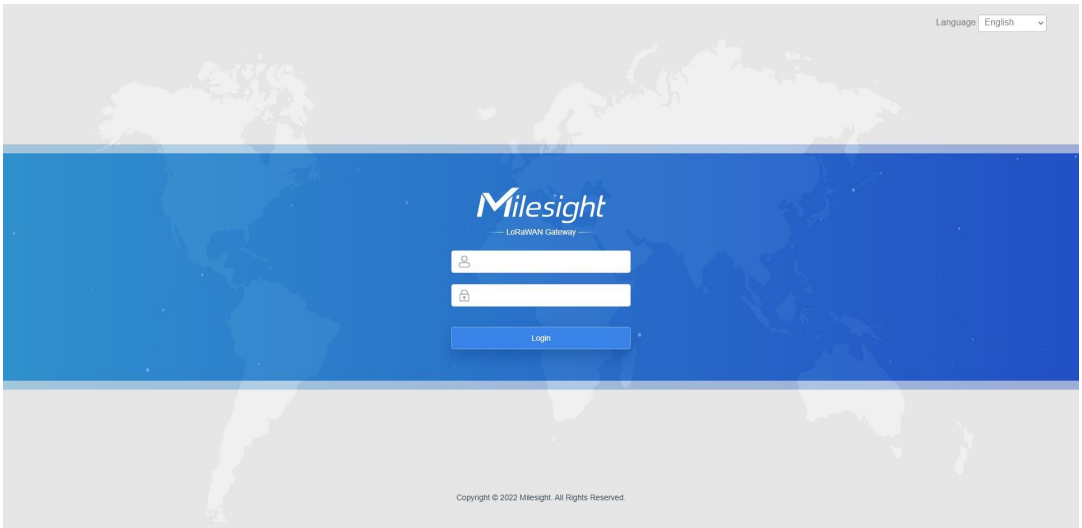


2. Gehen Sie zu „Eigenschaften“ → „Internetprotokoll Version 4 (TCP/IPv4)“ und wählen Sie „Folgende IP-Adresse verwenden“ aus. Weisen Sie dann manuell eine statische IP-Adresse innerhalb desselben Subnetzes des
Gateway.



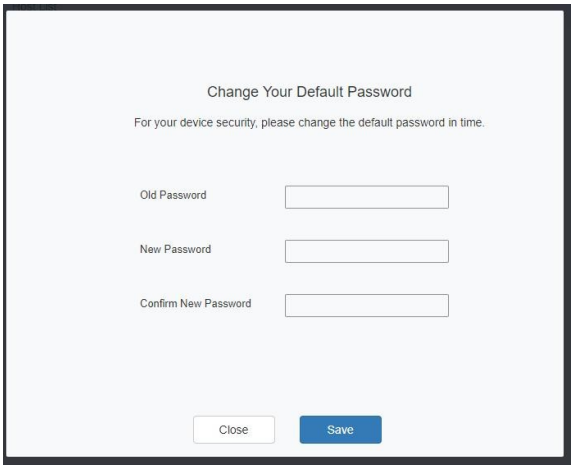
3. Öffnen Sie einen Webbrowser auf Ihrem PC (Chrome wird empfohlen) und geben Sie die IP-Adresse ein. **192.168.23.150**, um auf die Web-GUI zuzugreifen.

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

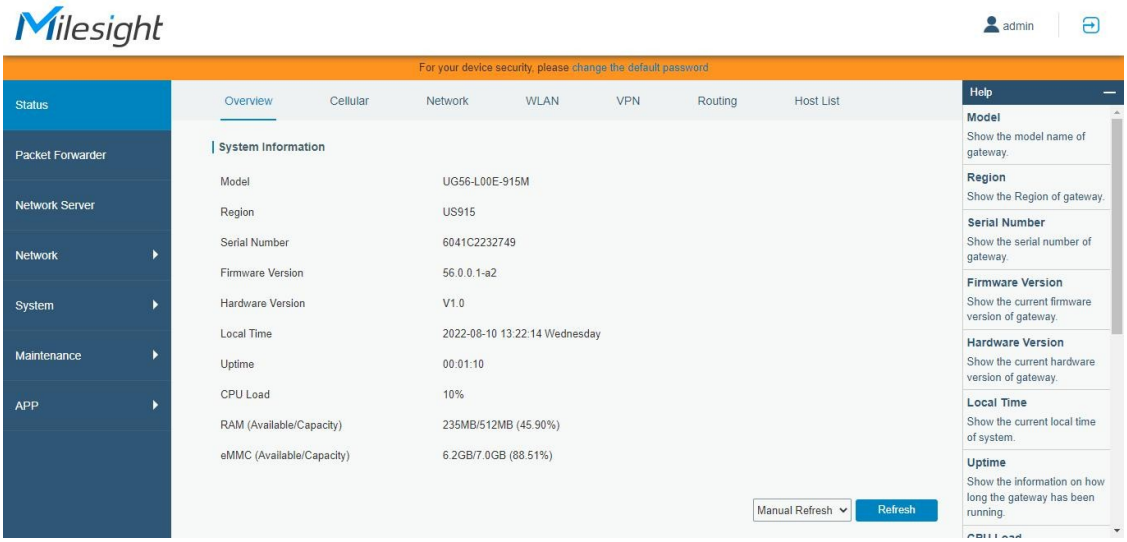


Wenn Sie den Benutzernamen oder das Passwort mehr als fünfmal falsch eingeben, wird die Anmeldeseite für 10 Minuten gesperrt.

5. Befolgen Sie nach der Anmeldung bei der Web-GUI die Anleitung, um die Grundkonfigurationen abzuschließen. Aus Sicherheitsgründen wird empfohlen, das Passwort zu ändern.



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



Kapitel 3 Webkonfiguration

3.1 Status

3.1.1 Übersicht

Auf dieser Seite können Sie die Systeminformationen des Gateways anzeigen.

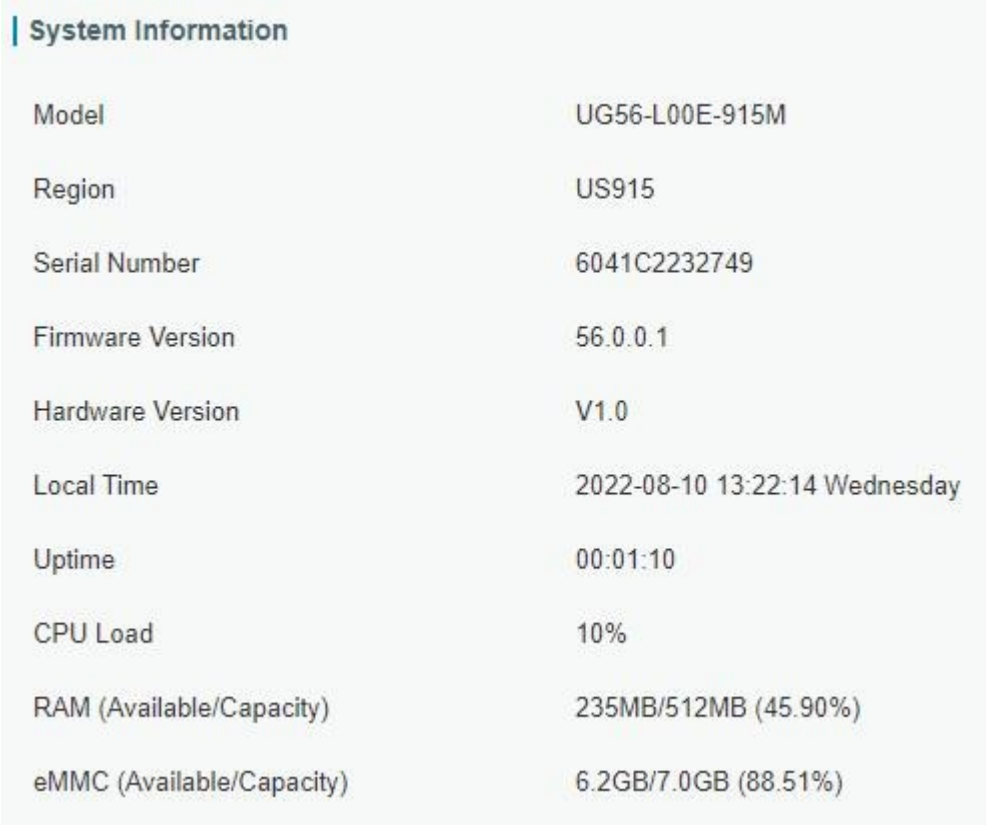


Abbildung 3-1-1-1

Systeminformationen	
Artikel	**Beschreibung**
Modell	Zeigt den Modellnamen des Gateways an.
Region	Zeigt die LoRaWAN®-Frequenzregion des Gateways 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 läuft. in Betrieb ist.
CPU-Auslastung	Zeigt die aktuelle CPU-Auslastung des Gateways an.
RAM (Kapazität/verfügbar)	Zeigen Sie die RAM-Kapazität und den verfügbaren RAM-Speicher an.
eMMC (Kapazität/verfügbar)	Zeigt die eMMC-Kapazität und den verfügbaren eMMC-Speicher an.

Tabelle 3-1-1-1 Systeminformationen

3.1.2 Mobilfunk

Auf dieser Seite können Sie den Mobilfunknetzstatus des Gateways anzeigen.

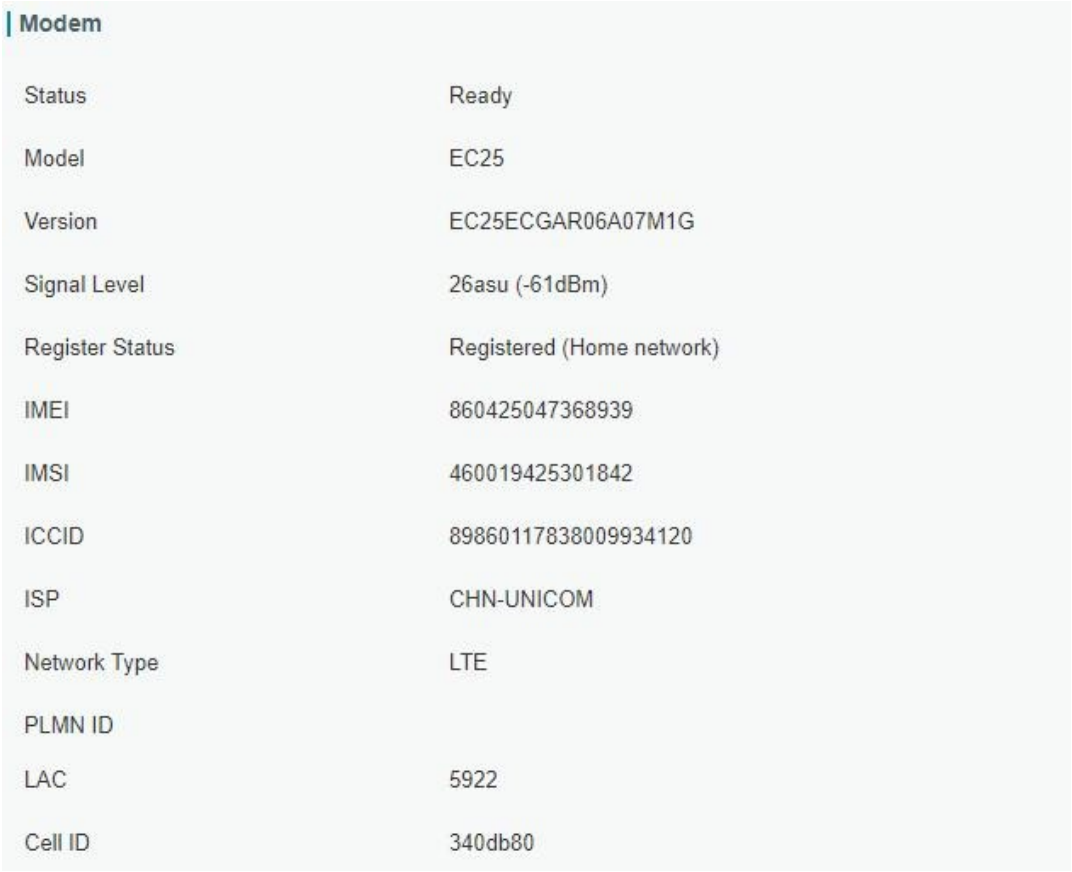


Abbildung 3-1-2-1

Modem-Informationen	
Element	**Beschreibung**
Status	Zeigt den entsprechenden Erkennungsstatus des Moduls und der SIM-Karte an.
Modell	Zeigt den Modellnamen des Mobilfunkmoduls an.
Version	Zeigt die Version des Mobilfunkmoduls an.
Signalpegel	Zeigt die Mobilfunksignalstärke an.
Registrierstatus	Zeigen Sie 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.
Zell-ID	Zeigt die Zell-ID des SIM-Kartenstandorts an.

Tabelle 3-1-2-1 Modem-Informationen

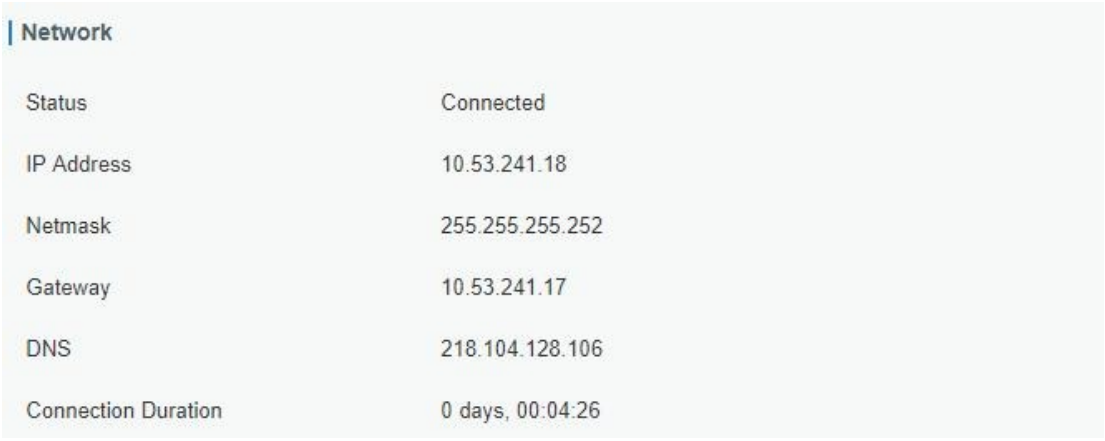


Abbildung 3-1-2-2

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	Zeigt den DNS des Mobilfunknetzes an.
Verbindungsdauer	Zeigt Informationen darüber an, wie lange das Mobilfunknetz verbunden ist.

Tabelle 3-1-2-2 Netzwerkstatus

3.1.3 Netz

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 das Ethernet-Kabel Kabel nicht angeschlossen ist oder die WAN-Funktion deaktiviert ist.
Typ	Zeigt den Einwahl-Typ des Ethernet-Ports an.
IP-Adresse	Zeigen Sie 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 deaktiviert oder das Ethernet-Kabel getrennt wird, wird die Dauer nicht mehr angezeigt.

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.

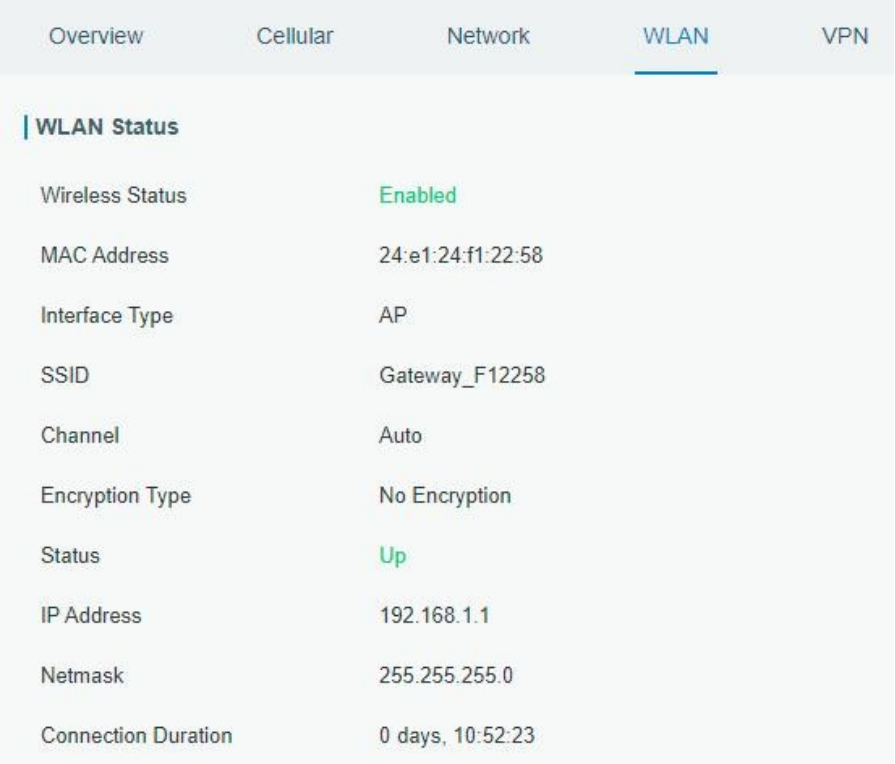


Abbildung 3-1-4-1

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	Zeigt den Verbindungsstatus an.
IP-Adresse	Zeigt die IP-Adresse des Gateways an.
Netzmaske	Zeigen Sie die drahtlose MAC-Adresse des Gateways an.
Gateway	Zeigen Sie die Gateway-Adresse im drahtlosen Netzwerk an.
Verbindungsdauer	Zeigen Sie 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	Zeigt 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.

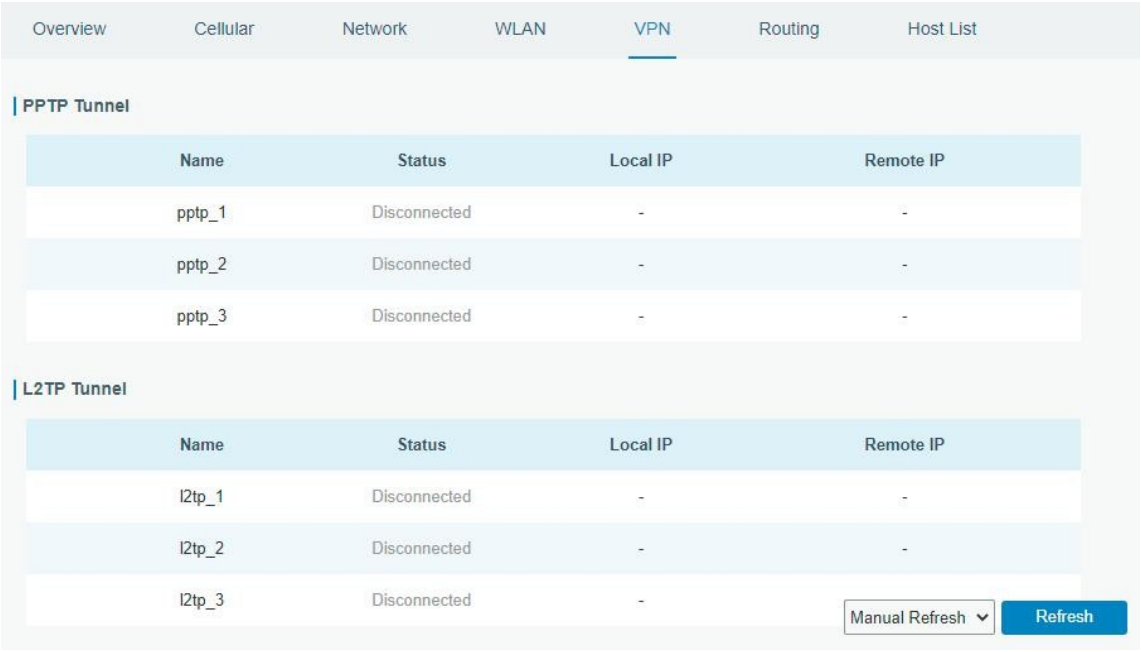


Abbildung 3-1-5-1

IPsec Tunnel

Name	Status	Local IP	Remote IP
ipsec_1	Disconnected	-	-
ipsec_2	Disconnected	-	-
ipsec_3	Disconnected	-	-

OpenVPN Client

Name	Status	Local IP	Remote IP
openvpn_1	Disconnected	-	-
openvpn_2	Disconnected	-	-
openvpn_3	Disconnected	-	-

Abbildung 3-1-5-2

GRE Tunnel

Name	Status	Local IP	Remote IP
gre_1	Disconnected	-	-
gre_2	Disconnected	-	-
gre_3	Disconnected	-	-

DMVPN Tunnel

Name	Status	Local IP	Remote IP
dmvpn	Disconnected	-	-

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 Routing

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

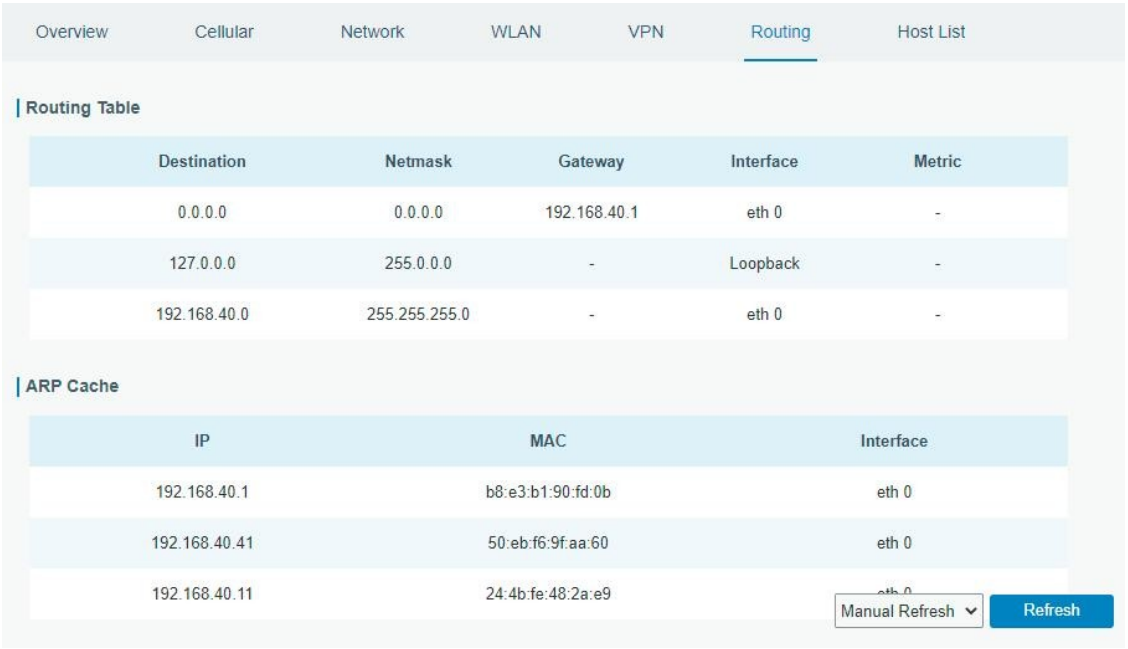


Abbildung 3-1-6-1

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

Tabelle 3-1-6-1 Routing-Informationen

3.1.7 Host-Liste

Auf dieser Seite können Sie die Host-Informationen anzeigen.

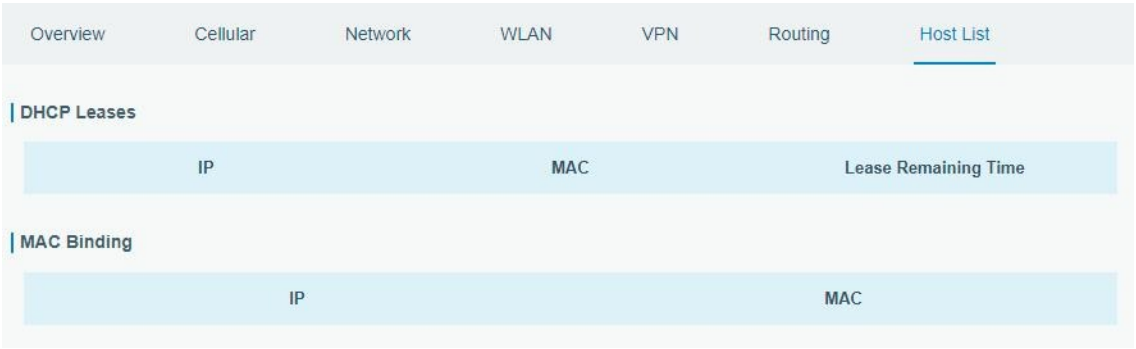


Abbildung 3-1-7-1

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	Zeigen Sie die IP-Adresse und MAC-Adresse an, die in der Liste der statischen IP-Adressen des DHCP-Dienstes festgelegten IP-Adresse und MAC-Adresse an.

Tabelle 3-1-7-1 Beschreibung der Hostliste

3.2 LoRaWAN

3.2.1 Paketweiterleitung

3.2.1.1 Allgemein

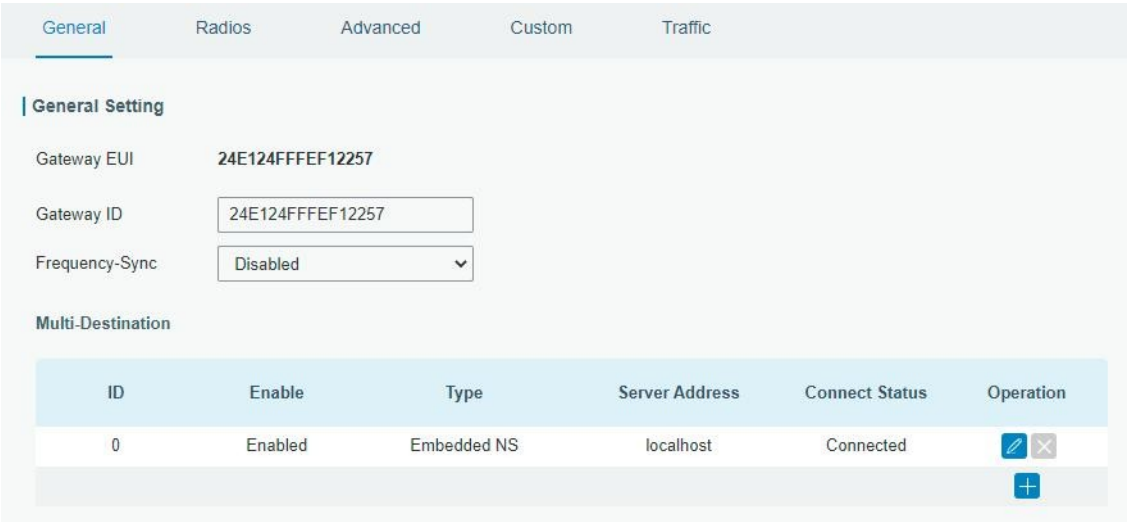


Abbildung 3-2-1-1

Allgemeine Einstellungen		
Element	**Beschreibung**	**Standard**
Gateway-EUI	Zeigt die Kennung des Gateways an.	Wird aus der MAC-Adresse des Gateways generiert und kann nicht nicht geändert werden.
Gateway-ID	Geben Sie die entsprechende ID ein, die Sie für die Registrierung des Gateways auf dem Remote-Netzwerkserver, z. B. TTN, verwendet haben. Diese entspricht in der Regel der Gateway-EUI und kann geändert werden.	Entspricht der Gateway-EUI.
Frequenzsynchronisation	Synchronisieren Sie die Frequenzkonfigurationen vom Netzwerkserver Server durch Auswahl der entsprechenden ID.	Deaktiviert
Multi-Destination	Das Gateway leitet die Daten an den	lokalen Host

	Netzwerkserveradresse weiter, die erstellt und in der Liste aktiviert wurde.	
Verbindung Status	Zeigen Sie den Verbindungsstatus des Paketdienstes an Weiterleiters an.	----

Tabelle 3-2-1-1 Allgemeine Einstellungsparameter

Beispiel für die zugehörige Konfiguration

Konfiguration des Paketweiterleiters

3.2.1.2 Funkgeräte

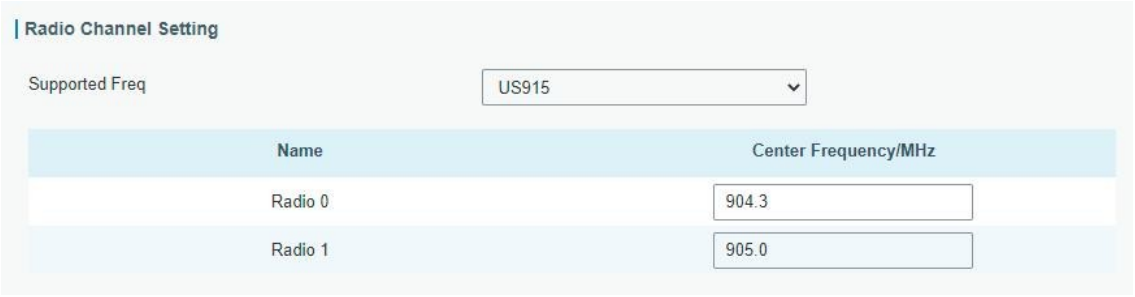


Abbildung 3-2-1-2

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

Tabelle 3-2-1-2 Einstellparameter für Funkkanäle

Abbildung 3-2-1-3

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 3-2-1-3 Parameter für die Mehrkanaleinstellung

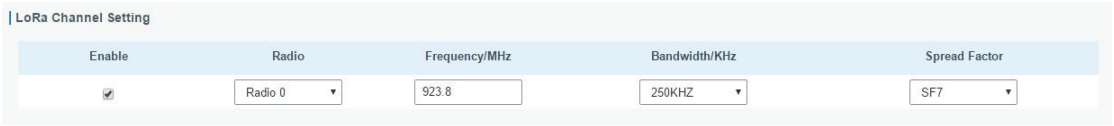


Abbildung 3-2-1-4

Funkgeräte – LoRa-Kanaleinstellung		
Element	**Beschreibung**	**Standard**
Aktivieren	Klicken Sie hier, um diesen Kanal für die Übertragung von Pakete.	Aktiviert
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 3-2-1-4 LoRa-Kanaleinstellungsparameter

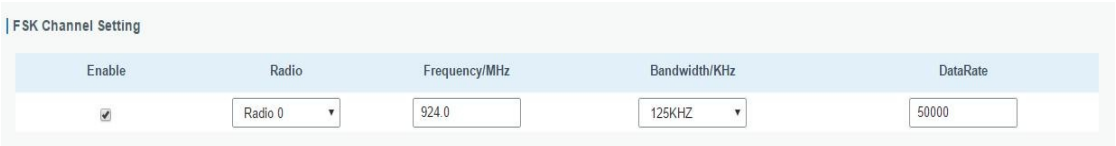


Abbildung 3-2-1-5

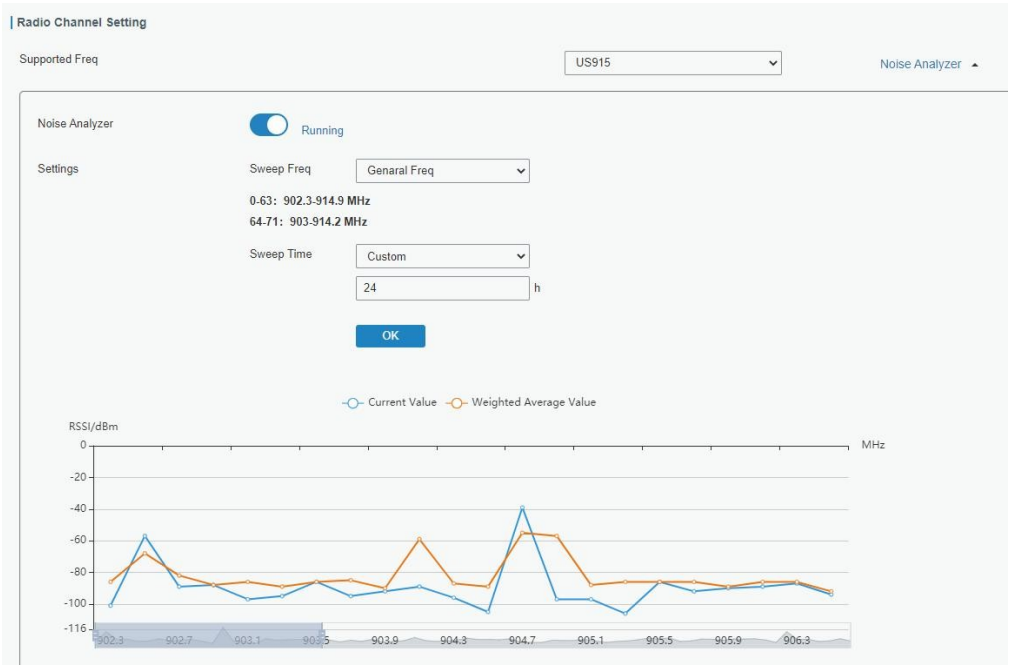
Funkgeräte – FSK-Kanaleinstellung		
Element	**Beschreibung**	**Standard**
Aktivieren	Klicken Sie hier, um diesen Kanal für die Übertragung von Pakete.	Deaktiviert
Funk	Wählen Sie Radio 0 oder Radio 1 als Mittenfrequenz Frequenz.	Radio 0
Frequenz/MHz	Geben Sie die Frequenz dieses Kanals ein.	Basierend auf dem

	Bereich: Mittenfrequenz ±0,9.	Unterstützt 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 3-2-1-5 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.



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 nach der vorkonfigurierten Zeit automatisch beendet. Hinweis: Es wird empfohlen, die Zeit individuell anzupassen, da die die Funktion des Geräuschanalysators die normalen Daten	Benutzerdefiniert/2 4h

	.	

Tabelle 3-2-1-6 Einstellparameter für den Geräuschanalysator

3.2.1.4 Erweitert

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

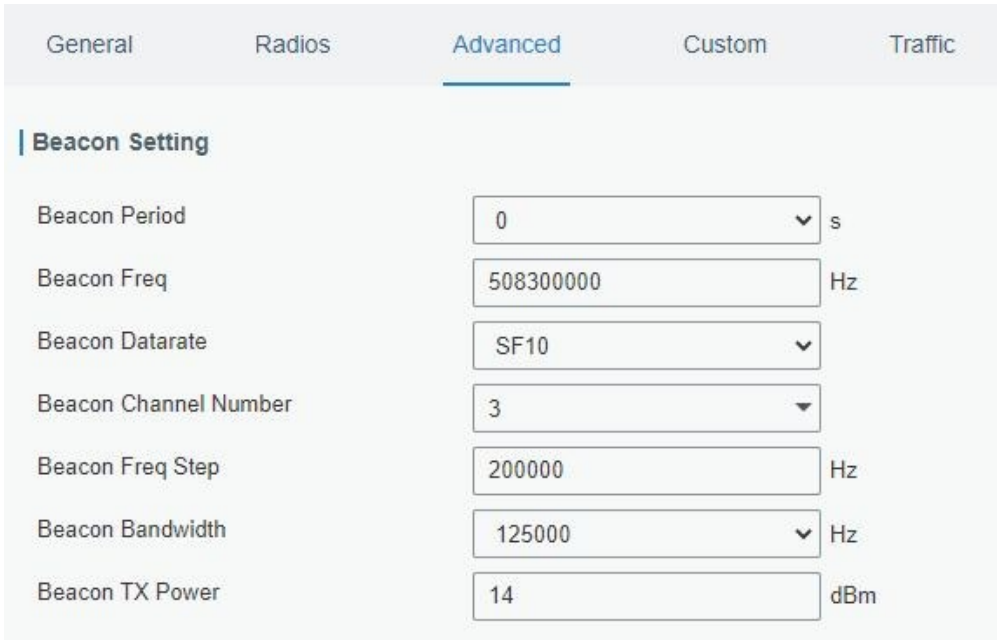


Abbildung 3-2-1-7

Erweitert – Beacon-Einstellung		
Element	**Beschreibung**	**Standard**
Beacon-Periode	Intervall, in dem das Gateway Beacons für die Zeitsynchronisation von Geräten der Klasse B sendet. 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 3-2-1-7 Erweiterte Beacon-Parameter

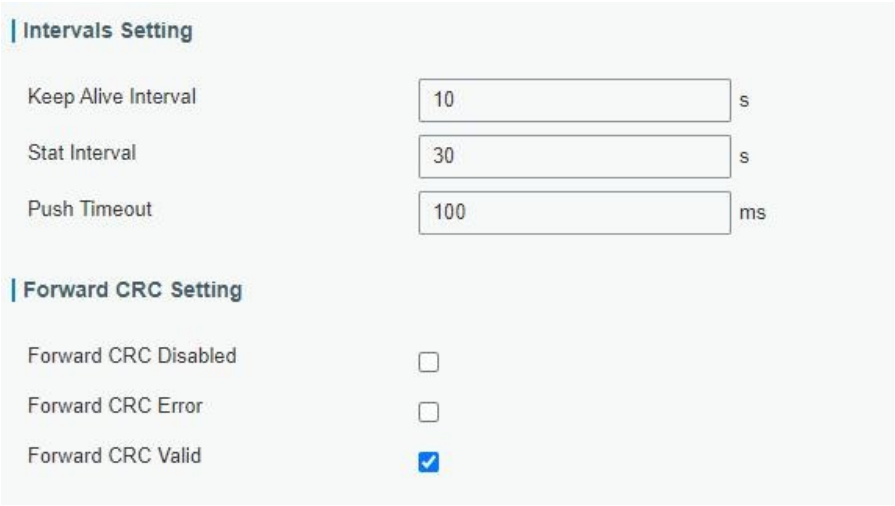


Abbildung 3-2-1-8

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-Zeitlimit	Geben Sie das Zeitlimit ein, um auf die Antwort vom Server zu warten nach dem Senden der Daten des Knotens durch das Gateway. Bereich: 1-1999.	100
CRC weiterleiten Deaktiviert	Aktivieren Sie diese Option, um Pakete, die mit deaktiviertem CRC empfangen wurden, an Netzwerkserver zu senden.	Deaktiviert
CRC weiterleiten Fehler	Aktivieren Sie die Option, 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 3-2-1-8 Erweiterte Parameter

3.2.1.5 Benutzerdefiniert

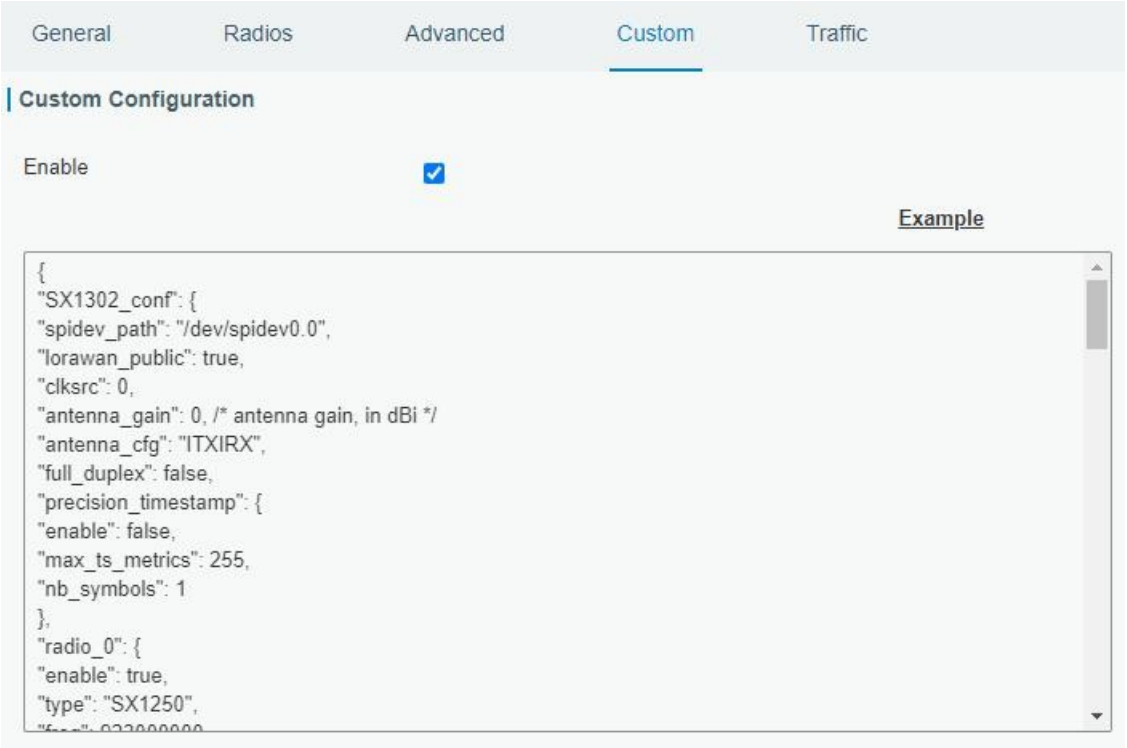
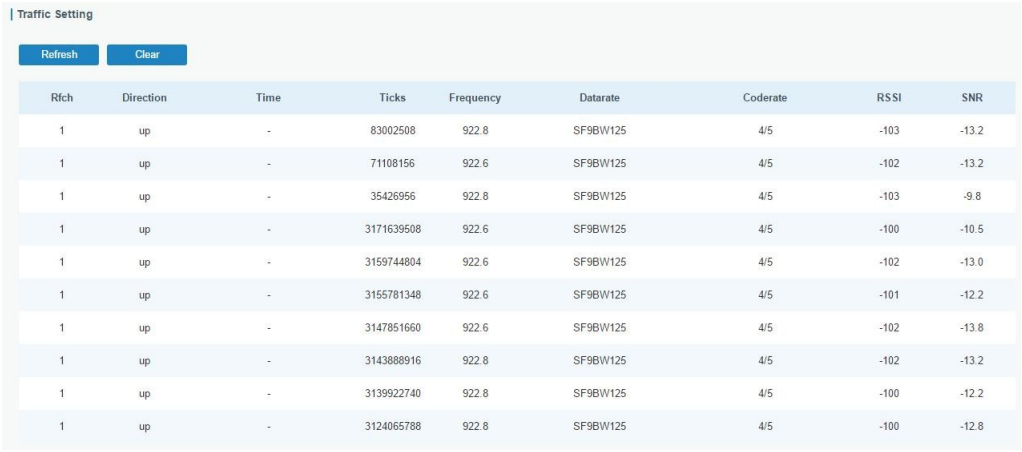


Abbildung 3-2-1-9

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 man eine Konfigurationsdatei schreibt, klicken Sie bitte auf „Beispiel“, um zur Referenzseite zu gelangen.

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“**.



Rfch	Direction	Time	Ticks	Frequency	Datarate	Coderate	RSSI	SNR
1	up	-	83002508	922.8	SF9BW125	4/5	-103	-13.2
1	up	-	71108156	922.6	SF9BW125	4/5	-102	-13.2
1	up	-	35426956	922.8	SF9BW125	4/5	-103	-9.8
1	up	-	3171639508	922.6	SF9BW125	4/5	-100	-10.5
1	up	-	3159744804	922.6	SF9BW125	4/5	-102	-13.0
1	up	-	3155781348	922.6	SF9BW125	4/5	-101	-12.2
1	up	-	3147851660	922.6	SF9BW125	4/5	-102	-13.8
1	up	-	3143888916	922.8	SF9BW125	4/5	-102	-13.2
1	up	-	3139922740	922.8	SF9BW125	4/5	-100	-12.2
1	up	-	3124065788	922.8	SF9BW125	4/5	-100	-12.8

Abbildung 3-2-1-10

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.

Tabelle 3-2-1-9 Verkehrsparameter

3.2.2 Netzwerkserver

3.2.2.1 Allgemein

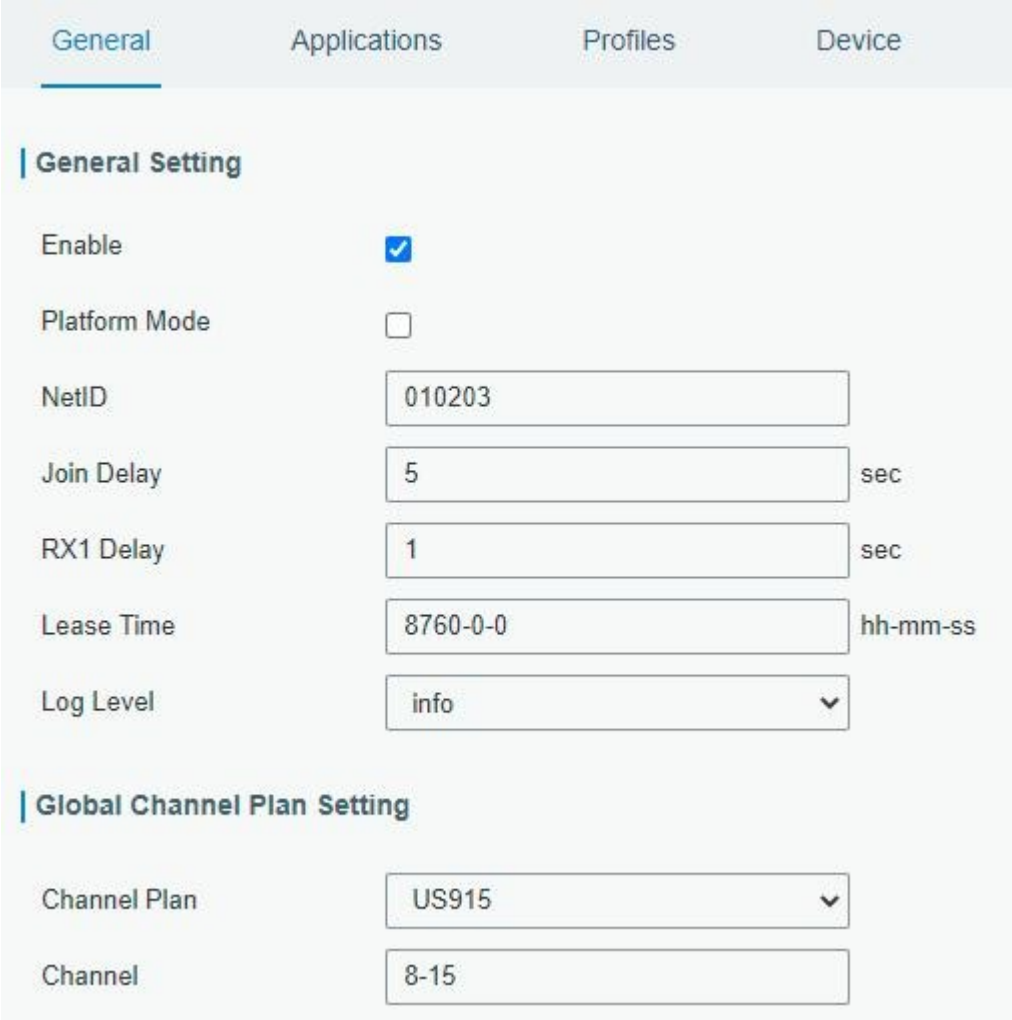


Abbildung 3-2-2-1

Element	Beschreibung	Standard
Allgemeine Einstellung		
Aktivieren	Klicken Sie hier, um den Netzwerkservermodus zu aktivieren.	Aktiv
Plattformmodus	Aktiviert, um das Gateway mit Milesight IoT Cloud oder die Yeastar Workplace-Plattform zu verbinden.	Deaktiviert
NetID	Geben Sie die Netzwerkkennung ein.	010203
Verzögerung beim Beitritt	Geben Sie die Zeitspanne 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 bis zum Ablauf einer erfolgreichen Verbindung ein. Das Format lautet Stunden-Minuten-Sekunden. Wenn der Verbindungstyp OTAA ist, müssen sich die Endgeräte erneut mit dem Netzwerkserver verbinden, wenn die Lease-Zeit überschritten wird. 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 Upstream- und Downlink-Frequenzen und Datenraten verwendet wird. Die verfügbaren Kanalpläne hängen vom Modell des Gateways ab.	Abhängig von der Frequenz des Gateways
Kanal	Die aktivierten Frequenzen werden über die Kanalmaske gesteuert. Wenn Sie das Feld leer lassen, werden alle im LoRaWAN®-Dokument mit regionalen Parametern angegebenen standardmäßigen nutzbaren Kanäle verwendet. Sie können den Index der Kanäle eingeben. **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 Alle: Aktiviert alle Kanäle Null: Zeigt an, dass alle Kanäle deaktiviert sind	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 zusätzlichen Plan verwenden, um zusätzliche Kanäle zu konfigurieren, die nicht durch die LoRaWAN®-Regionalparameter definiert sind

, wie EU868 und KR920, wie in der folgenden Abbildung gezeigt:

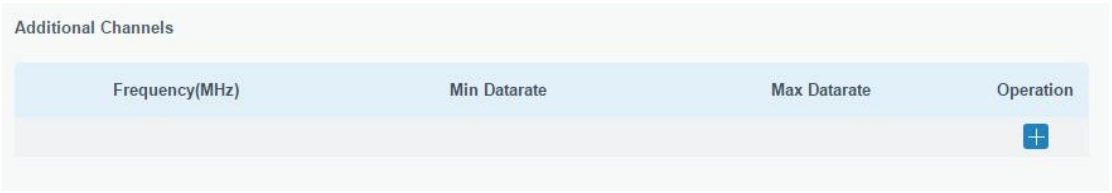


Abbildung 3-2-2-2

Zusätzliche Kanäle		
Element	**Beschreibung**	**Standard**
Frequenz/MHz	Geben Sie die Häufigkeit des zusätzlichen Plans ein.	Null.
Maximale 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. Alle Geräte mit demselben „Payload Codec“ und derselben Datenübertragungsdestination können unter derselben Anwendung hinzugefügt werden.

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

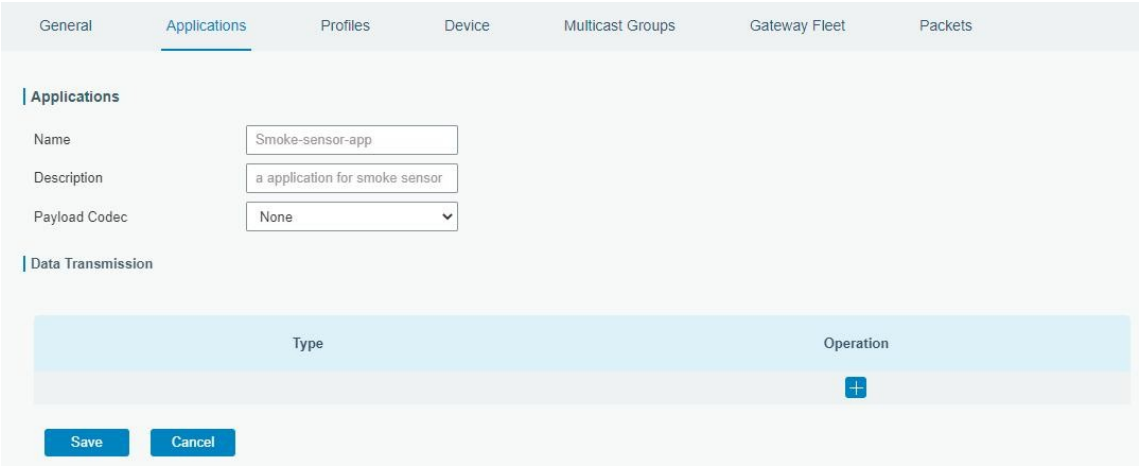


Abbildung 3-2-2-3

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.
Nutzlast-Codec	Wählen Sie aus: „Keine“, „Cayenne LPP“, „Benutzerdefiniert“. Keine: In diesem Modus werden Geräte dazu veranlasst, keine Daten zu verschlüsseln. Cayenne LPP: In diesem Modus können Geräte Daten mit Cayenne Low Power Payload (LPP) verschlüsseln. Benutzerdefiniert: In diesem Modus können Geräte Daten mit der Decoderfunktion und der Encoder-Funktion, für die Sie den Code eingegeben haben.
Daten Die Datenübertragung	Die Daten werden über das MQTT-HTTP- oder HTTPS-Protokoll an Ihren benutzerdefinierten Server gesendet. HTTPS-Protokoll an Ihren benutzerdefinierten Server gesendet.

Tabelle 3-2-2-3 Anwendungsparameter

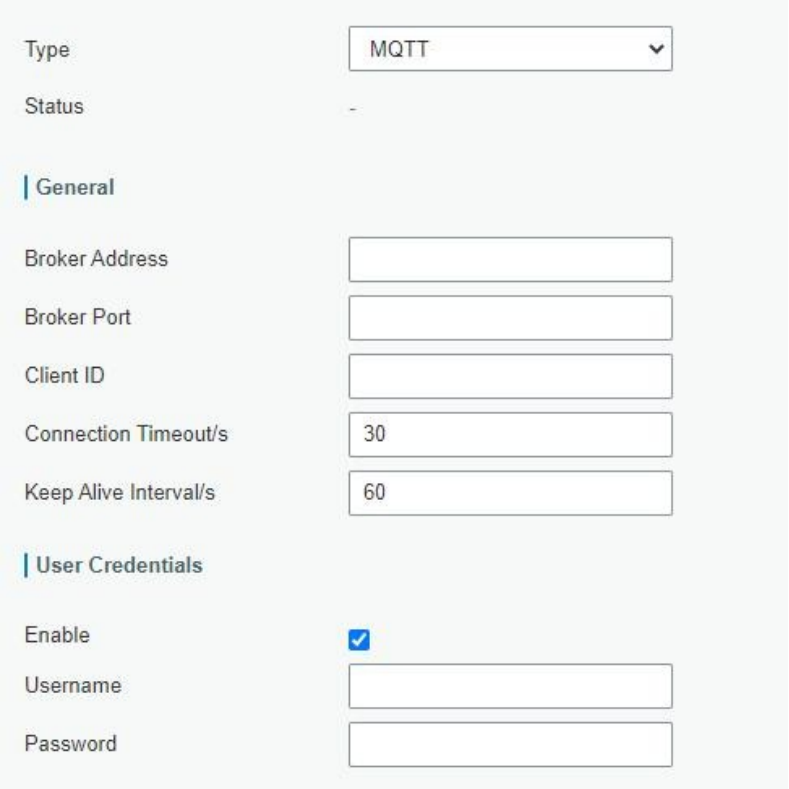


Abbildung 3-2-2-4

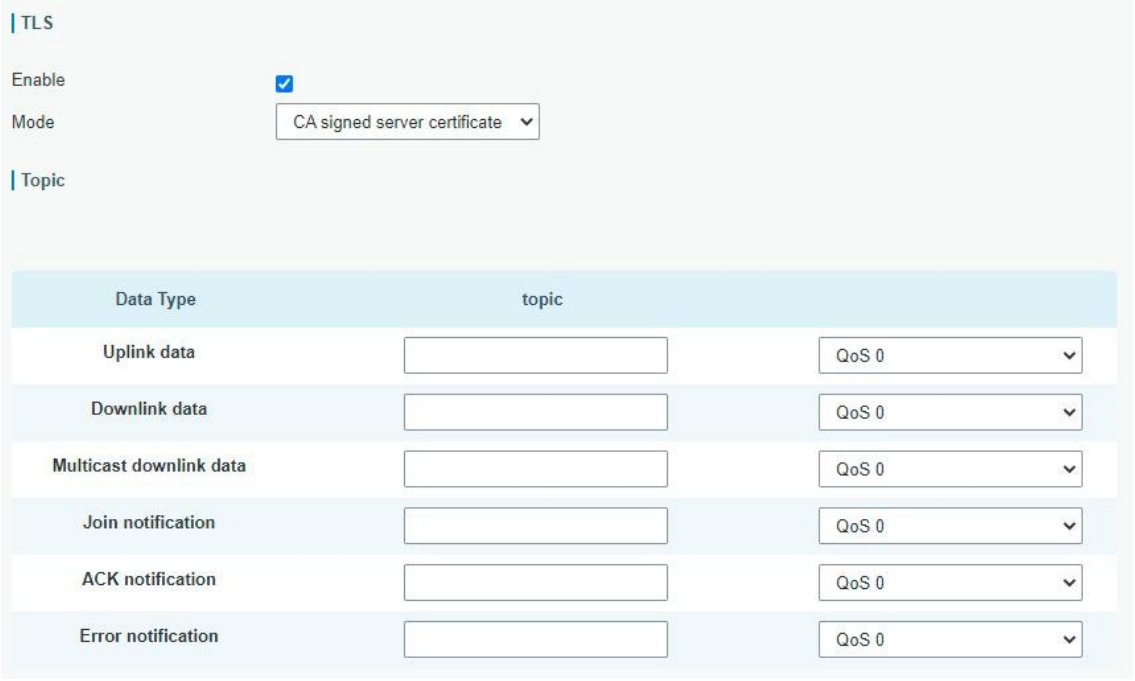


Abbildung 3-2-2-5

MQTT-Einstellungen		
Element	**Beschreibung**	**Standard**
Allgemein		
Broker Adresse	MQTT-Broker-Adresse zum Empfangen 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. Sie muss eindeutig sein, wenn alle Clients mit demselben Server verbunden sind, und ist der Schlüssel zur Verarbeitung von Nachrichten bei QoS 1 und 2.	--
Verbindungszeitlimit (Sekunden)	Wenn der Client nach Ablauf der Verbindungszeitüberschreitung keine Antwort erhält Zeitüberschreitung keine Antwort erhält, wird die Verbindung als unterbrochen betrachtet. Der Bereich: 1-65535	30
Keep-Alive-Intervall/s	Nachdem der Client mit dem Server verbunden ist, sendet der Client regelmäßig ein Heartbeat-Paket an den Server senden, um die Verbindung aufrechtzuerhalten. Bereich: 1-65535	60
Benutzeranmeldedaten		
Aktivieren	Benutzeranmeldedaten aktivieren.	
Benutzername	Der Benutzername, der für die Verbindung mit dem MQTT-Broker verwendet wird.	
Passwort	Das Passwort, das für die Verbindung mit dem MQTT-Broker verwendet wird.	
TLS		
Aktivieren	Aktivieren Sie die TLS-Verschlüsselung in der MQTT-Kommunikation.	
Modus	Wählen Sie zwischen „Selbstsignierte Zertifikate“ und „Von CA signiertes Serverzertifikat“. Von CA signiertes Serverzertifikat: Überprüfen Sie das Zertifikat mit dem Zertifikat, das von der Zertifizierungsstelle (CA) ausgestellt und auf dem Gerät vorinstalliert wurde. Selbstsignierte Zertifikate: Laden Sie die benutzerdefinierten CA-Zertifikate, Client-Zertifikate und geheimen Schlüssel zur Überprüfung hoch.	

Thema	
Datentyp	An den MQTT-Broker gesendeter Datentyp.
Thema	Themenname des Datentyps, der für die Veröffentlichung verwendet wird.
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

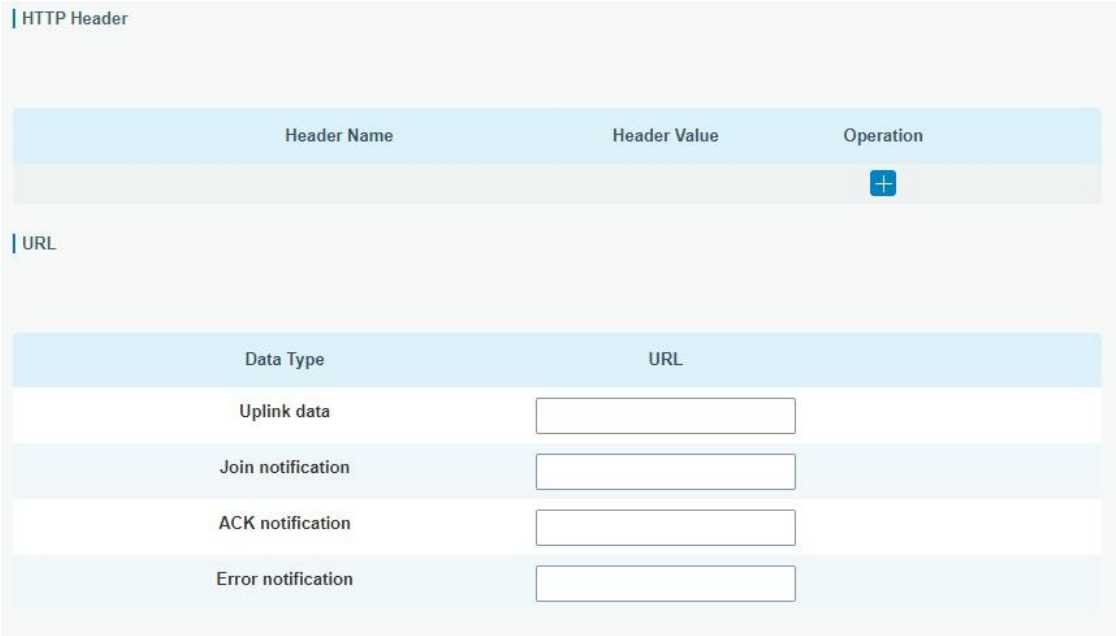


Abbildung 3-2-2-6

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.
Thema	Themenname des Datentyps, der für die Veröffentlichung verwendet wird.
URL	HTTP/HTTPS-Server-URL zum Empfangen von Daten.

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

Beispiel für zugehörige Konfiguration

Anwendungskonfiguration

3.2.2.3 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.

Sie können das Geräteprofil bearbeiten, indem Sie auf „  “ klicken, oder ein neues Geräteprofil erstellen, indem Sie auf  .

Abbildung 3-2-2-7

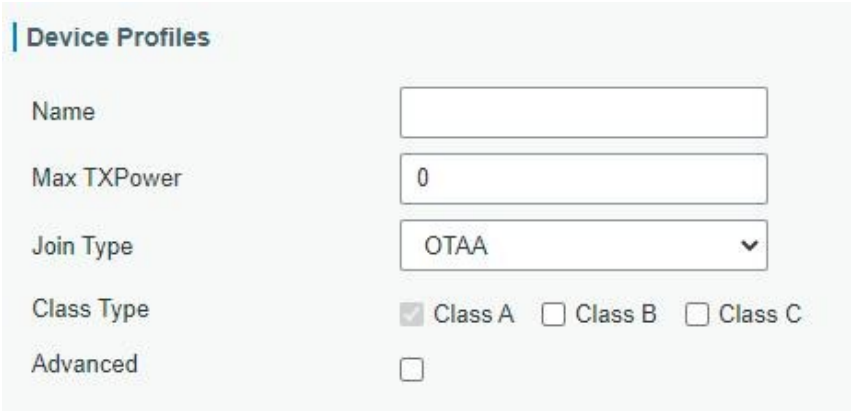


Abbildung 3-2-2-8

Einstellungen für Geräteprofile		
Element	**Beschreibung**	**Standard**
Name	Geben Sie den Namen des Geräteprofils ein. Z. B. Smoker-Sensor-App.	Null
Max TXPower	Geben Sie die maximale Sendeleistung ein. Der TXPower gibt die Leistungspegel relativ zum maximalen EIRP-Pegel des Endgeräts an. 0 bedeutet, dass die maximale EIRP verwendet wird. EIRP bezieht sich auf die äquivalente isotrope Strahlungsleistung.	0
Verbindungstyp	Wählen Sie zwischen „OTAA“ und „ABP“. OTAA: Over-the-Air-Aktivierung.	OTAA

	Für die Over-the-Air-Aktivierung müssen Endgeräte vor der Teilnahme am Datenaustausch mit dem Netzwerkserver teilnehmen können. Ein Endgerät muss jedes Mal ein neues Beitrittsverfahren durchlaufen durchlaufen, da es die Sitzungskontextinformationen verloren hat. ABP: Aktivierung durch Personalisierung. Unter bestimmten Umständen können Endgeräte durch Personalisierung aktiviert werden. Die Aktivierung durch Personalisierung verbindet ein Endgerät direkt mit einem bestimmten Netzwerk und umgeht dabei das Verfahren der Beitrittsanfrage und Beitrittsannahme.	
Klassentyp	Der Gerätetyp ist standardmäßig Klasse A. 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 3-2-2-6 Geräteprofile Einstellparameter

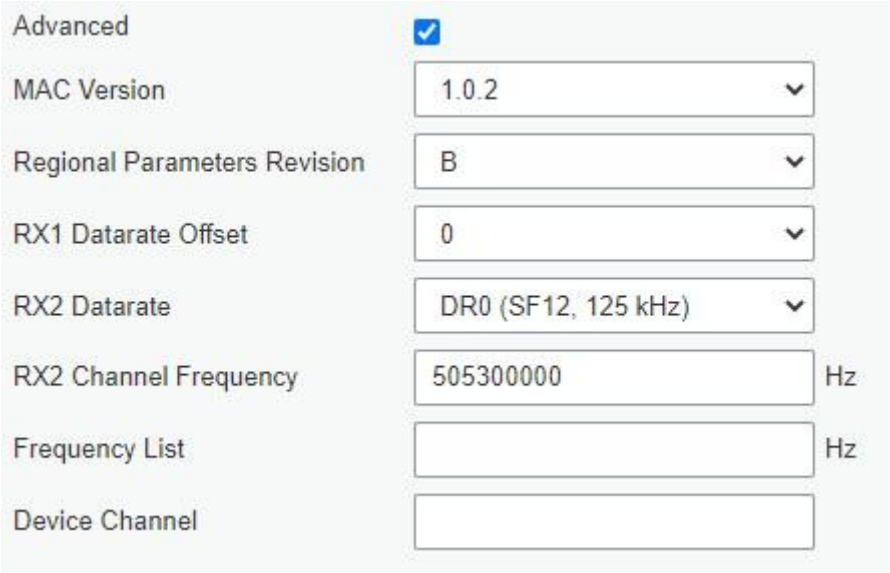


Abbildung 3-2-2-9

Erweiterte Einstellungen für Geräteprofile		
Element	**Beschreibung**	**Standard**
MAC-Version	Wählen Sie die Version von LoRaWAN® vom Endgerät unterstützten LoRaWAN(®)-Version aus.	1.0.2
Regional Parameter Revision	Überarbeitung des Dokuments „Regionale Parameter”, das vom Endgerät unterstützt wird.	B
RX1 Datenrate Offset	Der Offset, der zur Berechnung der RX1 Datenrate verwendet wird, basierend auf der Uplink-Datenrate.	Basierend auf dem, was in der LoRaWAN®
RX2-Datenrate	Geben Sie die RX2-Datenrate ein, die für den RX2 verwendet wird.	

	Empfangsfenster.	regionale Parameter Dokument
RX2-Kanal Frequenz	RX2-Kanalfrequenz, die für den RX2 verwendet wird Empfangsfenster verwendet wird.	
Frequenzliste	Liste der werkseitig voreingestellten Frequenzen. Der Bereich basiert auf den Angaben im LoRaWAN® Dokument mit regionalen Parametern.	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 C.	Klasse B: 10 Klasse C: 10

Tabelle 3-2-2-7 Geräteprofile - Erweiterte Einstellungsparameter

3.2.2.4 Gerät

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

Abbildung 3-2-2-10

Element	Beschreibung
Hinzufügen	Ein Gerät hinzufügen.
Massenimport	Vorlage herunterladen und mehrere Geräte importieren.
Alle löschen	Alle Geräte in der Liste löschen.
Gerätename	Zeigt den Namen des Geräts an.
Geräte-EUI	Zeigt die EUI des Geräts an.
Geräteprofil	Zeigt den Namen des Geräteprofils des Geräts an.
Anwendung	Zeigt den Namen der Anwendung des Geräts an.
Zuletzt gesehen	Zeigt den Zeitpunkt des letzten empfangenen Pakets an.

Aktiviert	Zeigt den Status des Geräts an. „ ✓ " bedeutet, dass das Gerät aktiviert wurde.
Operation	Bearbeiten oder löschen Sie das Gerät.

Tabelle 3-2-2-8 Geräteparameter

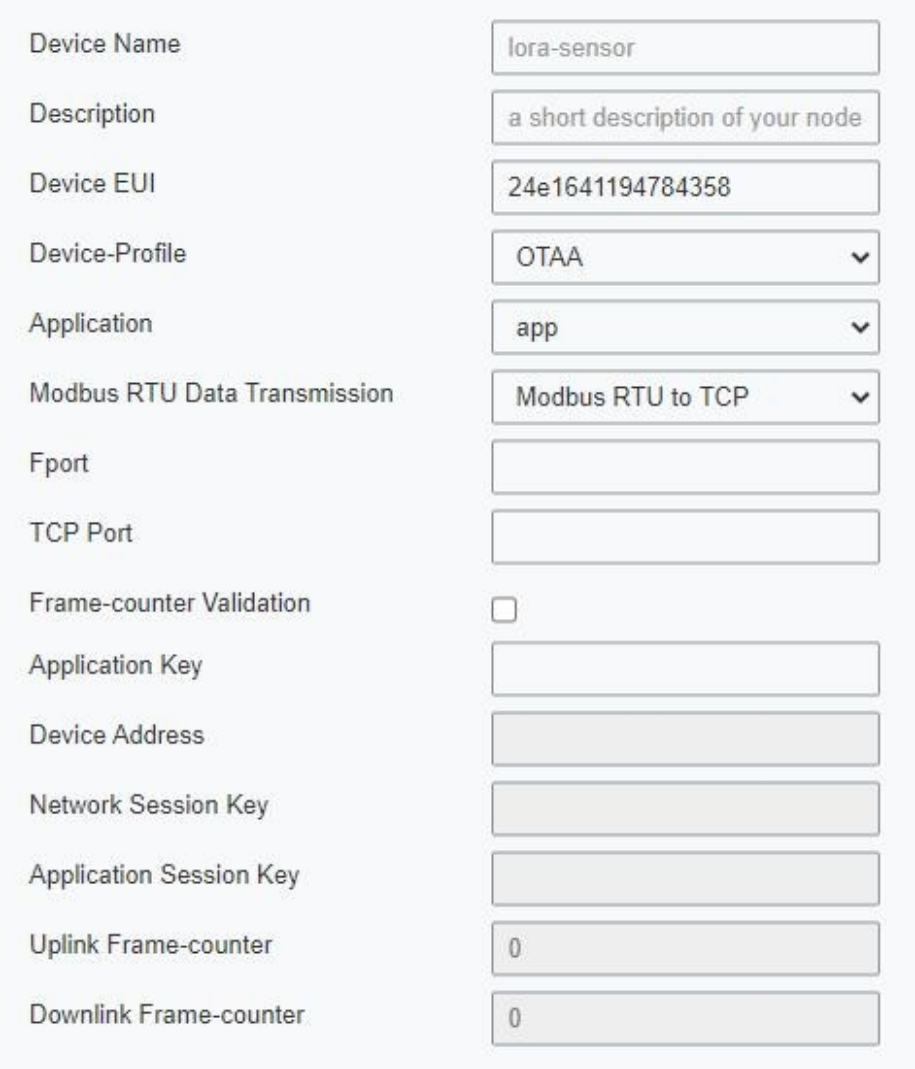


Abbildung 3-2-2-11

Gerätekonfiguration		
Element	**Beschreibung**	**Standard**
Gerätename	Geben Sie den Namen dieses Geräts ein.	Null
Beschreibung	Geben Sie die Beschreibung dieses Geräts ein.	Null
Geräte-EUI	Geben Sie die EUI dieses Geräts ein.	Null
Geräteprofil	Wählen Sie das Geräteprofil aus.	Null
Anwendung	Wählen Sie das Anwendungsprofil aus.	Null
Modbus RTU-Datenübertragung	Wählen Sie aus: „Deaktivieren", „Modbus RTU zu TCP", „Modbus RTU über TCP". Diese Funktion gilt nur für Milesight-Controller **der Klasse C** vom Typ LoRaWAN® (UC501/UC300 usw.)	Deaktivieren

	-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.	
Fport	Geben Sie den LoRaWAN®-Frame-Port für die transparente Übertragung zwischen Milesight LoRaWAN®-Controllern und UG56 ein. Bereich: 2-84, 86-223. Hinweis: Dieser Wert muss mit dem Fport des Milesight LoRaWAN®-Controllers übereinstimmen.	Null
TCP-Port	Geben Sie den TCP-Port für die Datenübertragung zwischen dem TCP-Client und UG56 (als TCP-Server) ein. Bereich: 1-65535.	Null
Frame-Zähler-Validierung	Wenn Sie die Frame-Zähler-Validierung deaktivieren, wird die Sicherheit beeinträchtigt, da dies die Durchführung von Replay-Angriffe durchführen können.	Aktiviert
Anwendungsschlüssel	Wenn ein Endgerät über eine Over-the-Air-Aktivierung mit einem Netzwerk verbunden wird, wird der Anwendungsschlüssel verwendet, um Ableitung des Anwendungssitzungsschlüssels verwendet.	Null
Geräteadresse	Die Geräteadresse identifiziert das Endgerät innerhalb dem aktuellen Netzwerk.	Null
Netzwerksitzungsschlüssel	Der für das Endgerät spezifische Netzwerksitzungsschlüssel. Er wird vom Endgerät verwendet, um den MIC oder einen Teil des MIC (Message Integrity Code) aller Uplink-Daten , um die Datenintegrität sicherzustellen.	Null
Anwendungssitzungsschlüssel	Der AppSKey ist ein für das Endgerät spezifischer Anwendungssitzungsschlüssel. Er wird sowohl vom Anwendungsserver als auch vom Endgerät zum Ver- und Entschlüsseln des Nutzdatenfeld anwendungsspezifischer Datenmeldungen zu verschlüsseln und zu entschlüsseln.	Null
Uplink Frame-Zähler	Die Anzahl der Datenrahmen, die zum Netzwerkserver hochgeladen wurden. Sie wird vom Endgerät erhöht und vom Endgerät empfangen. Benutzer können ein personalisiertes Endgerät manuell zurücksetzen. Dadurch werden die Frame-Zähler auf dem Endgerät und die Frame-Zähler auf dem Netzwerkserver für dieses Endgerät auf 0 zurückgesetzt.	Null
Downlink-Rahmenzähler	Die Anzahl der Datenframes, die vom Endgerät über die Downlink-Verbindung vom Netzwerkserver empfangen wurden. Sie wird vom Netzwerkserver erhöht. 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.	Null

Tabelle 3-2-2-9 Geräteeinstellungsparameter

Beispiel für die zugehörige Konfiguration

Gerätekonfiguration

3.2.2.5 Multicast-Gruppen

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

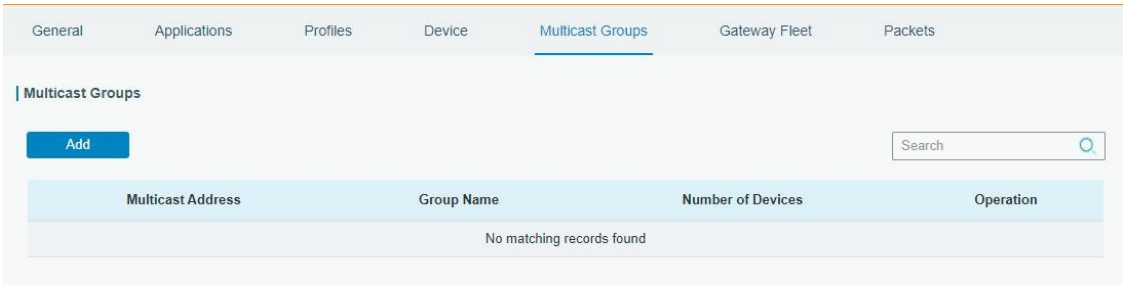


Abbildung 3-2-2-12

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 3-2-2-10 Multicast-Gruppenparameter

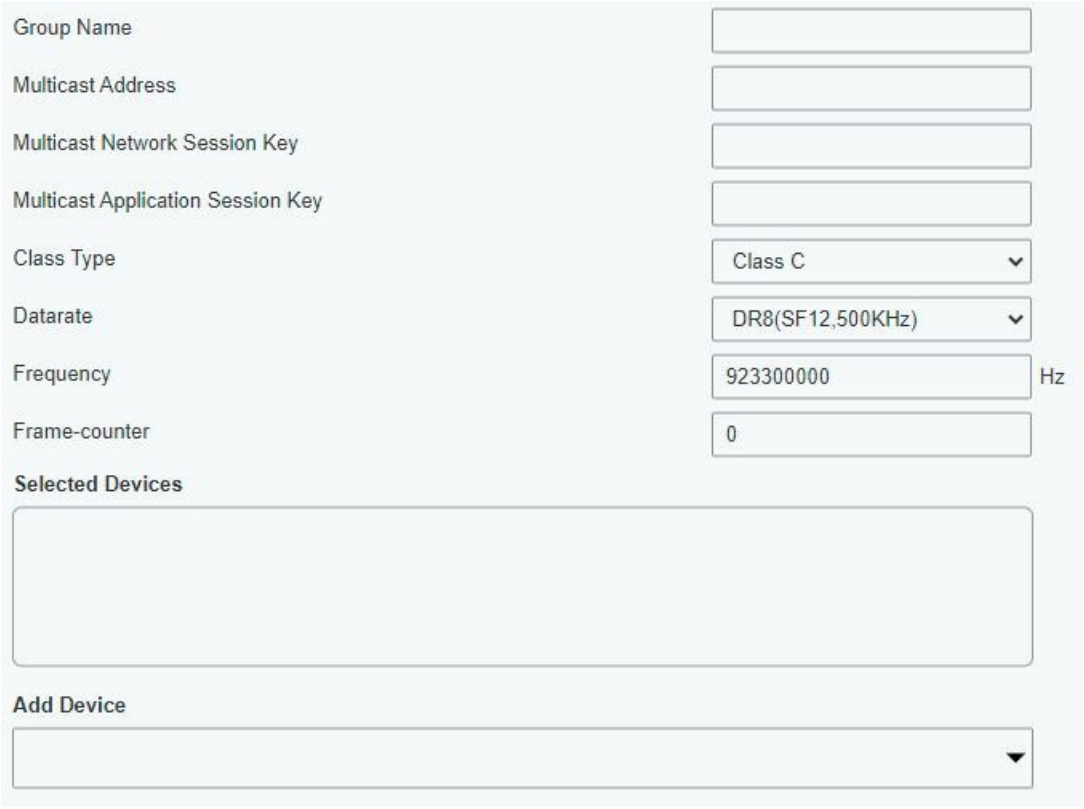


Abbildung 3-2-2-13

Multicast-Gruppenkonfiguration		
Element	**Beschreibung**	**Standard**
Gruppenname	Geben Sie den Namen dieser Multicast-Gruppe ein.	Null
Multicast Adresse	Geräteadresse (Dev Addr) aller Geräte in dieser Gruppe.	Null
Multicast-Netzwerk Sitzungsschlüssel	Der Netzwerksitzungsschlüssel (Netwks Key) aller Geräte in dieser Gruppe.	Null
Multicast Anwendungssitzungsschlüssel	Der Anwendungssitzungsschlüssel (AppSKey) aller Geräte in dieser Gruppe.	Null
Klassentyp	Klasse B und Klasse C sind optional.	Klasse C
Datenrate	Datenrate des Knotens, der Downlinks empfängt	Basierend auf der unterstützten Frequenz
Frequenz	Downlink-Frequenz aller Geräte in dieser Gruppe.	Basierend auf der unterstützten Frequenz
Frame-Zähler	Die Anzahl der Datenframes, die vom Endgerät über die Downlink-Verbindung vom Netzwerkserver empfangen wurden. Sie wird vom Netzwerkserver erhöht.	0
Ping-Slot Periodizität	Zeitraum, in dem der Ping-Slot geöffnet ist. Dies gilt nur für Endgeräten der Klasse B.	Jedes 4 Sekunde
Ausgewählte Geräte	Alle Gerätenamen in dieser Gruppe anzeigen.	Null
Gerät hinzufügen	Geräte in der Pulldown-Liste hinzufügen.	Null

Tabelle 3-2-2-11 Parameter für die Multicast-Gruppeneinstellung

3.2.2.6 Gateway-Flotte

Milesight-Gateways können eine Verbindung zum UG56-Netzwerkserver herstellen. Es wird empfohlen, maximal 5 Gateways hinzuzufügen.

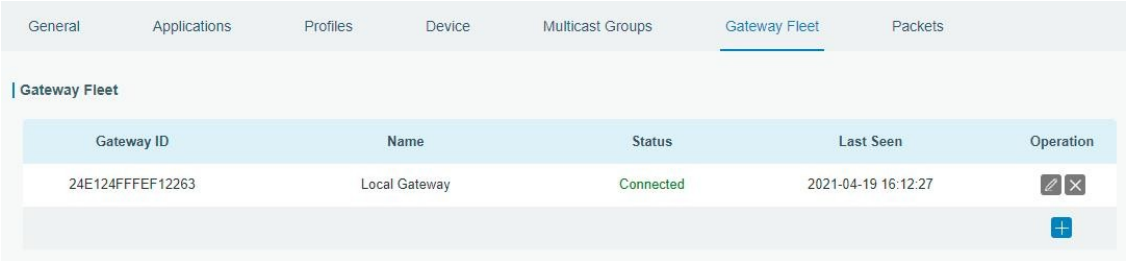


Abbildung 3-2-2-14

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 3-2-2-12 Gateway-Flottenparameter

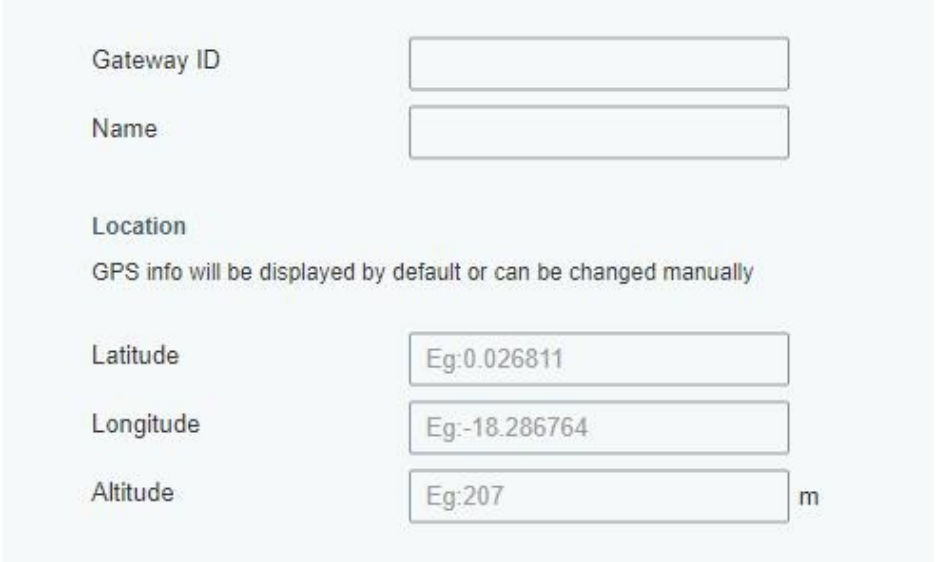


Abbildung 3-2-2-15

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 3-2-2-13 Gateway-Einstellungsparameter

3.2.2.7 Pakete

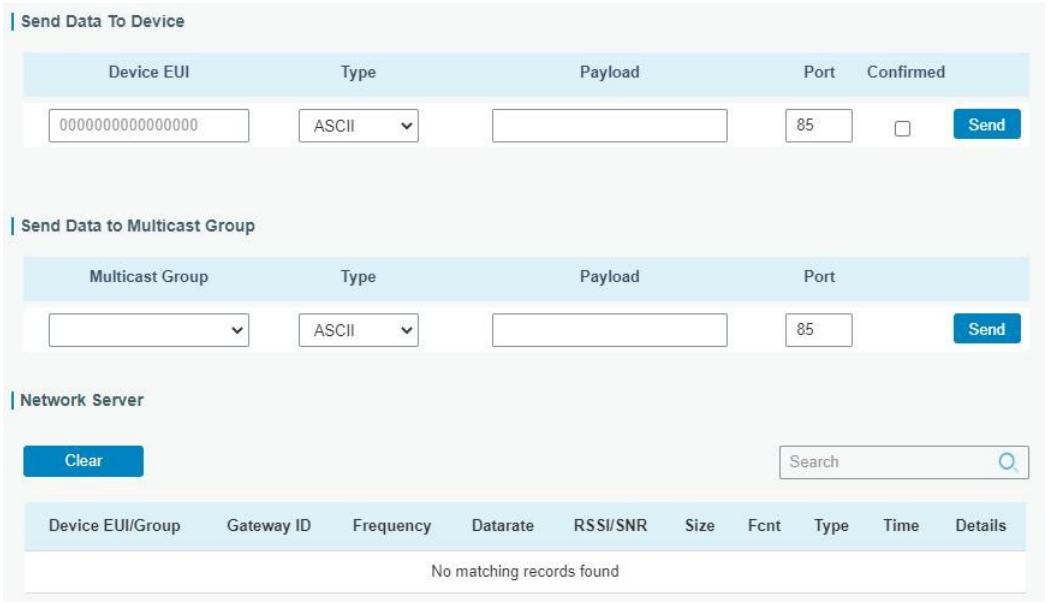


Abbildung 3-2-2-16

Daten an Gerät/Multicast-Gruppe senden		
Element	**Beschreibung**	**Standard**
Geräte-EUI	Geben Sie die EUI des Geräts ein, das die die Nutzlast empfangen soll.	Null
Multicast Gruppe	Wählen Sie die Multicast-Gruppe aus, um Downlinks zu senden. Multicast Gruppen können unter der Registerkarte „Multicast-Gruppen“ hinzugefügt werden.	Null
Typ	Wählen Sie aus: „ASCII“, „hex“, „base64“. Wählen Sie den Nutzlasttyp aus, der in das Eingabefeld „Nutzlast“ eingegeben werden soll.	ASCII
Nutzlast	Geben Sie die Nachricht ein, die an dieses Gerät gesendet werden soll.	Null
Port	Geben Sie den LoRaWAN®-Frame-Port für die Paketübertragung zwischen Gerät und Netzwerkserver ein.	Null
Bestätigt	Nach der Aktivierung empfängt das Endgerät ein Downlink-Paket und sollte dem Netzwerkserver mit „bestätigt” antworten. Die Multicast-Funktion unterstützt keine bestätigte Downlink-Verbindung.	Deaktiviert

Tabelle 3-2-2-14 Parameter für das Senden von Daten an das Gerät

Netzwerkserver	
Element	**Beschreibung**
Geräte-EUI/Gruppe	Zeigt die EUI des Geräts oder der Multicast-Gruppe an.
Frequenz	Zeigt die verwendete Frequenz zur Übertragung 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-Paket JnReq – Join Request-Paket UpUnc – Unbestätigtes Uplink-Paket UpCnf – Bestätigtes Uplink-Paket – ACK-Antwort vom Netzwerk angefordert DnUnc – Unbestätigtes Downlink-Paket DnCnf – Bestätigtes Downlink-Paket – ACK-Antwort vom Endgerät angefordert
Zeit	Zeigt die Zeit an, zu der das Paket gesendet oder empfangen wurde.

Tabelle 3-2-2-15 Paketparameter

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

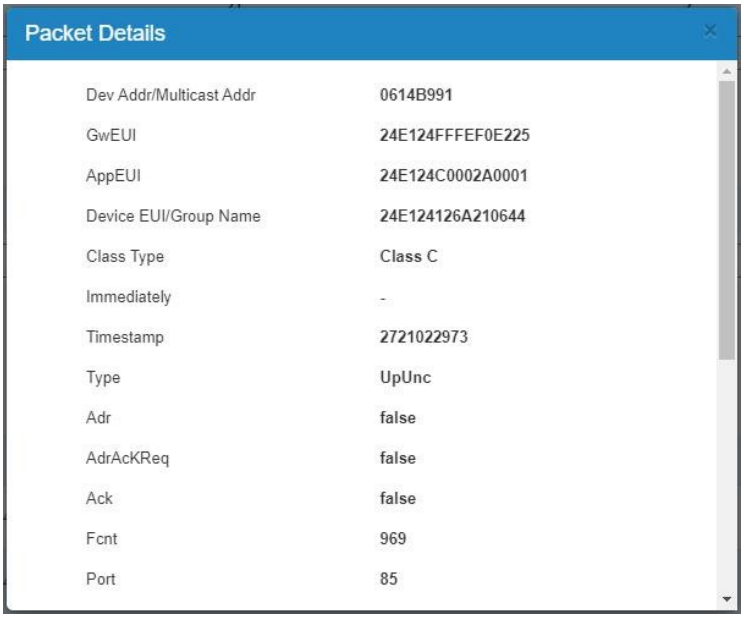


Abbildung 3-2-2-17

Element	Beschreibung
Geräteadresse/Multicast Adresse	Zeige die Adresse des Geräts/der Multicast-Gruppe an.
GwEUI	Zeigt die EUI des Gateways an.
AppEUI	Zeigt die EUI der Anwendung an.
DevEUI/Gruppe Name	Zeigt die EUI des Geräts/Multicast-Gruppennamens an.
Klassentyp	Zeigen Sie den Klassentyp des Geräts oder der Multicast-Gruppe an.
Sofort	Wahr: Das Gerät kann unmittelbar nach dem Empfang einer Datenmeldung, die eine Bestätigung erfordert, eine explizite (möglicherweise leere) Bestätigungsdatenmeldung senden. Datenmeldung, die eine Bestätigung erfordert.
Zeitstempel	Zeigt den Zeitstempel dieses Pakets an.
Typ	Zeige den Typ des Pakets an: JnAcc - Join-Akzeptanzpaket JnReq - Join-Anforderungspaket UpUnc - Unbestätigtes Uplink-Paket UpCnf - Bestätigtes Uplink-Paket - ACK-Antwort vom Netzwerk angefordert DnUnc - Unbestätigtes Downlink-Paket DnCnf - Bestätigtes Downlink-Paket - 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 ADRACKReq-Nachrichten. Diese sind 1 Bit lang. True: Das Netzwerk sollte innerhalb der ADR_ACK_DELAY-Zeit antworten, um zu bestätigen, dass es die Uplink-Nachrichten empfängt.

	Falsch: ADR ist deaktiviert oder das Netzwerk antwortet nicht innerhalb von ADR_ACK_DELAY antwortet.
Bestätigt	Wahr: Dieser Frame ist ein ACK. Falsch: Dieser Frame ist kein ACK.
Fcnt	Zeigen Sie den Frame-Zähler dieses Pakets an. Der Netzwerkserver verfolgt den Uplink-Frame-Zähler und generiert den Downlink-Zähler für jedes Endgerät.
FPort	FPort ist ein Multiplexing-Portfeld. Wenn das Frame-Nutzdatenfeld nicht leer ist, muss das Portfeld vorhanden sein. Wenn vorhanden, bedeutet ein FPort 16-Wert von 0, dass die FRMPayload MAC-Befehle enthält. Nur. In diesem Fall muss das Feld FOptsLen den Wert Null haben. FOptsLen ist die Länge des Feldes FOpts in Byte.
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	Zeigt den RSSI dieses Kanals an.
Leistung	Zeige die Sendeleistung des Geräts an.
Nutzlast (b64)	Zeigt die Anwendungsnutzlast dieses Pakets an.
Nutzlast (hex)	Zeigt die Anwendungsnutzlast dieses Pakets 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 3-2-2-16 Paketdetails-Parameter

Verwandtes Thema

Daten an Gerät senden

3.3 Netzwerk

3.3.1 Schnittstelle

3.3.1.1 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.

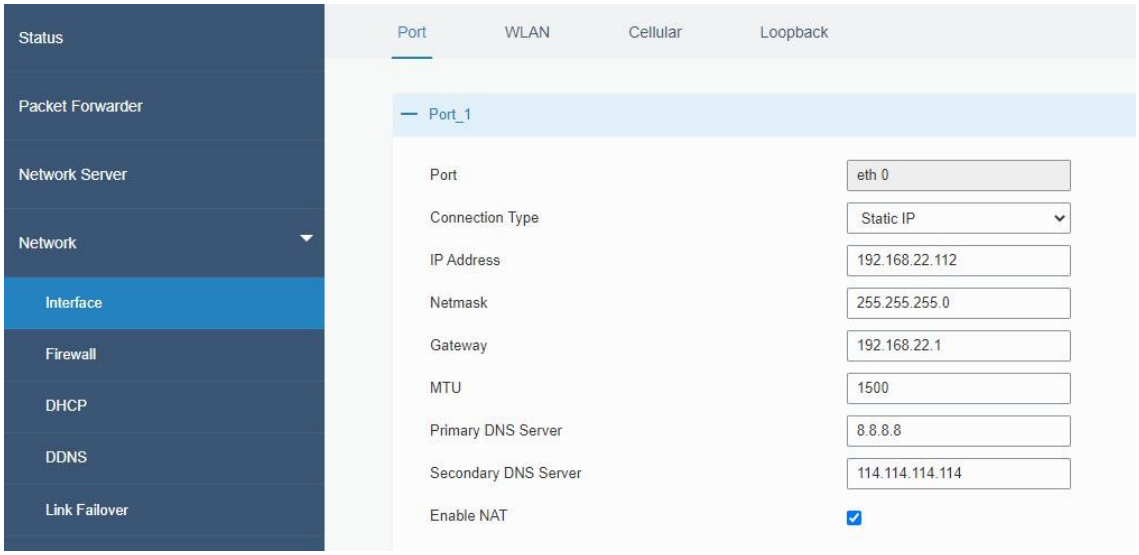


Abbildung 3-3-1-1

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“.	Statische IP
MTU	Legen Sie die maximale Übertragungseinheit fest.	1500
Primärer DNS Server	Legen Sie den primären DNS fest.	8.8.8.8
Sekundärer DNS Server	Sekundären DNS festlegen.	114.114.114.114
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 3-3-1-1 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.

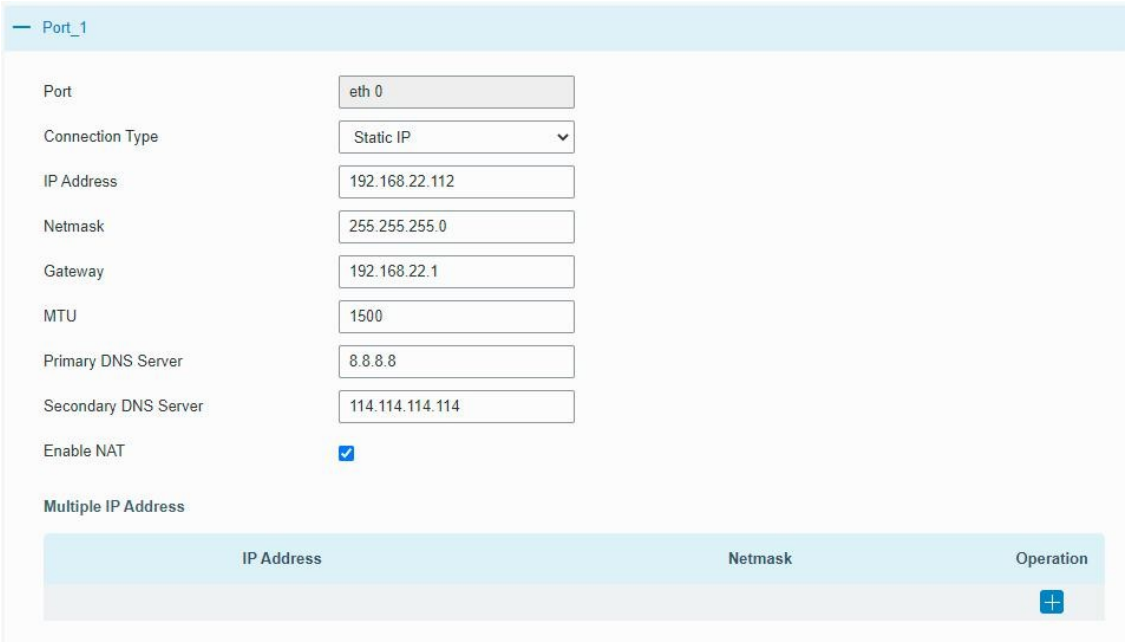


Abbildung 3-3-1-2

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 3-3-1-2 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.

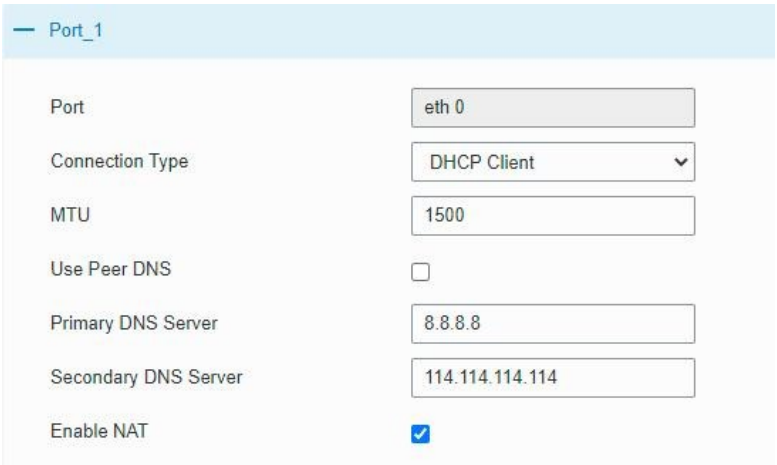


Abbildung 3-3-1-3

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

Tabelle 3-3-1-3 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.

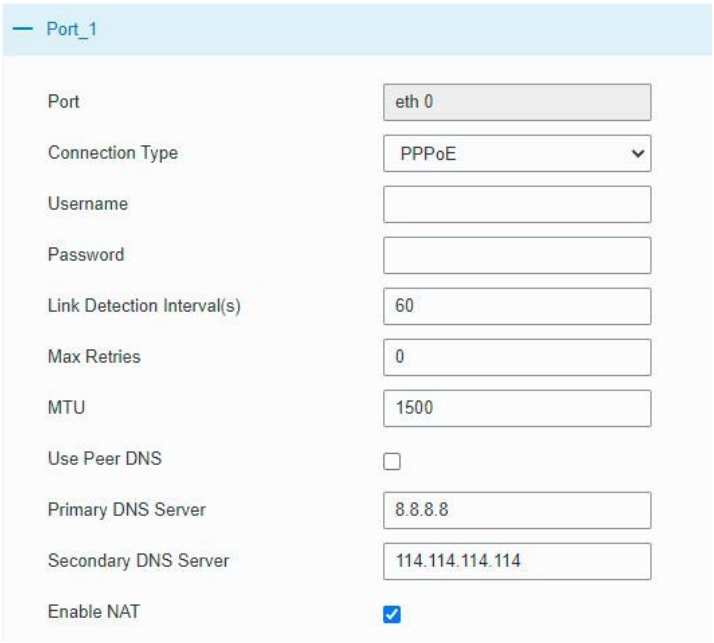


Abbildung 3-3-1-4

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 3-3-1-4 PPOE-Parameter

3.3.1.2 WLAN

In diesem Abschnitt wird erläutert, wie Sie die entsprechenden Parameter für das WLAN-Netzwerk einstellen. UG56 unterstützt 802.11 b/g/n im AP- oder Client-Modus.

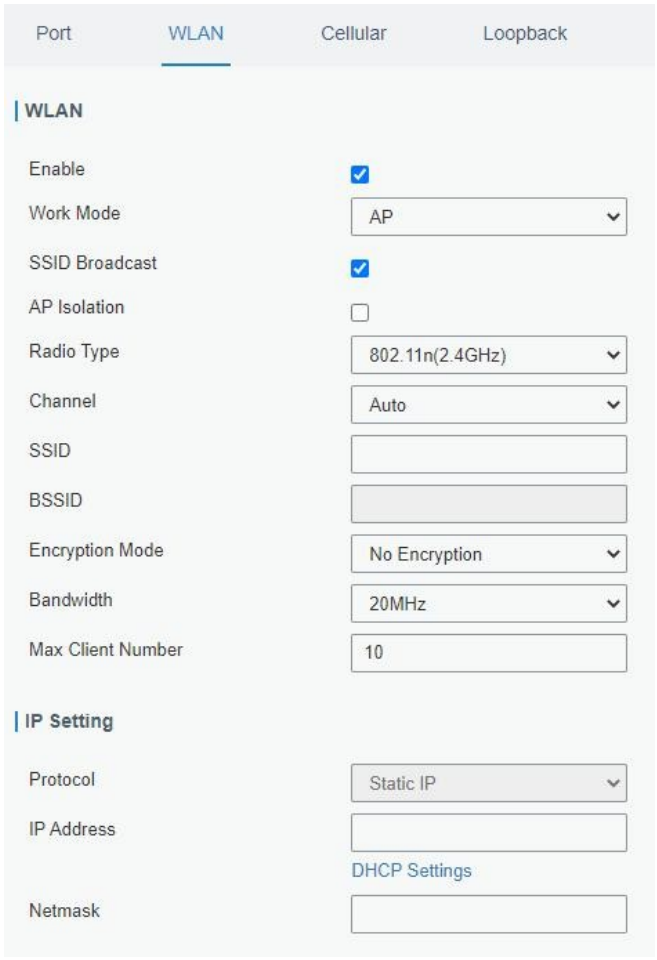


Abbildung 3-3-1-5

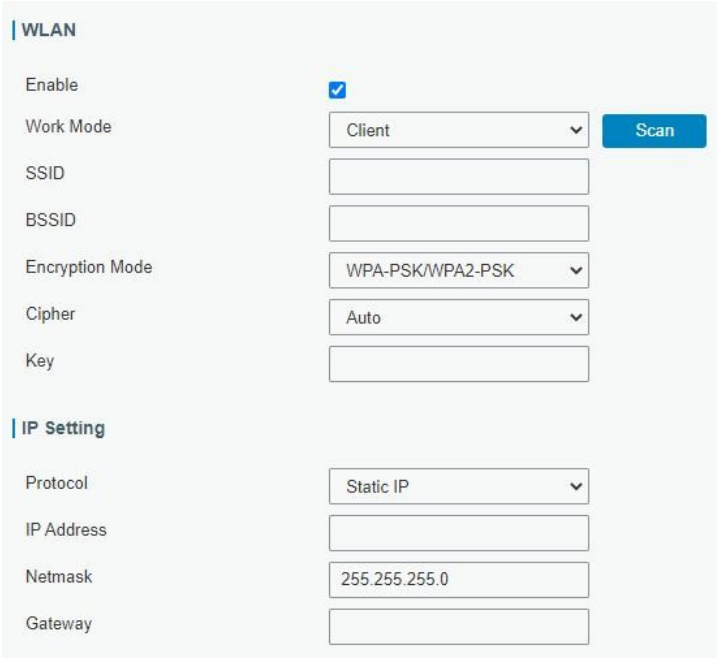


Abbildung 3-3-1-6

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 die SSID nicht finden, und Benutzer müssen die SSID manuell eingeben, um auf das drahtlose Netzwerk zugreifen.
AP-Isolation	Wenn die AP-Isolation aktiviert ist, sind alle Benutzer, die auf den AP zugreifen isoliert, ohne miteinander kommunizieren zu können.
Funkmodus	Wählen Sie den 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.
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 3-3-1-5 WLAN-Parameter

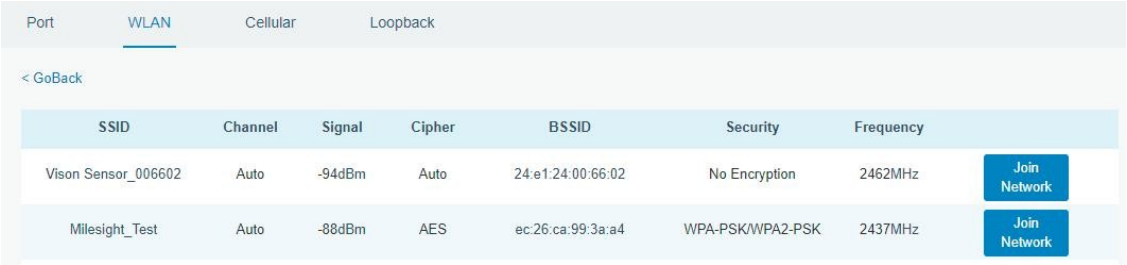


Abbildung 3-3-1-7

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 3-3-1-6 WLAN-Scan-Parameter

Verwandtes Thema

Beispiel für eine WLAN-Anwendung

3.3.1.3 Mobilfunk

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

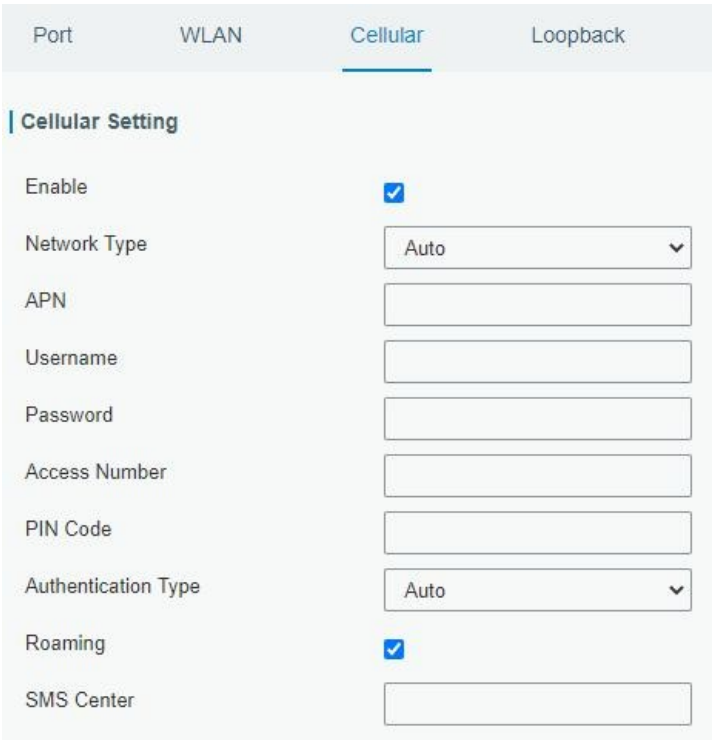


Abbildung 3-3-1-8

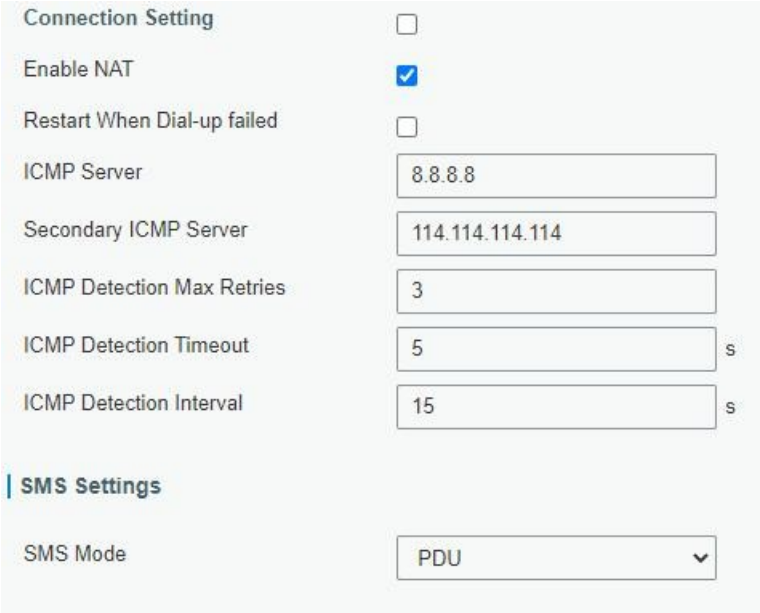


Abbildung 3-3-1-9

Allgemeine Einstellungen		
Element	**Beschreibung**	**Standard**
Aktivieren	Aktivieren Sie diese Option, um die entsprechende SIM-Karte zu aktivieren zu aktivieren.	Aktivieren
Netzwerktyp	Wählen Sie zwischen „Auto", „Auto 3G/4G", „Nur 4G" und „Nur 3G". Auto: Stellt automatisch eine Verbindung zum Netzwerk mit dem stärksten Signal her. Nur 4G: Verbindet sich nur mit dem 4G-Netzwerk. Und so weiter.	Auto
APN	Geben Sie den Namen des Zugangspunkts für die Mobilfunk-Einwahlverbindung , die von Ihrem lokalen Internetdienstanbieter bereitgestellt wird.	Null
Benutzername	Geben Sie den Benutzernamen für die Mobilfunk-Einwahlverbindung , die von Ihrem lokalen Internetdienstanbieter bereitgestellt wird.	Null
Passwort	Geben Sie das Passwort für die Mobilfunk-Einwahlverbindung , das von Ihrem lokalen Internetdienstanbieter bereitgestellt wird.	Null
Zugangsnummer	Geben Sie die Nummer der Einwahlzentrale für die Mobilfunk-Einwahlverbindung Verbindung, die von Ihrem lokalen Internetdienstanbieter bereitgestellt wird.	Null
PIN-Code	Geben Sie einen 4-8-stelligen PIN-Code ein, um die SIM-Karte zu entsperren.	Null
Authentifizierung Typ	Wählen Sie zwischen „Auto", „PAP", „CHAP", „MS-CHAP" und „MS-CHAPv2".	Auto
Roaming	Roaming aktivieren oder deaktivieren.	Aktivieren
SMS-Zentrale	Geben Sie die lokale SMS-Center-Nummer für die Speicherung, Weiterleitung, Konvertierung und Zustellung von SMS-Nachrichten.	Null
NAT aktivieren	Aktivieren oder deaktivieren Sie die NAT-Funktion.	Aktiviert
Neustart Wenn	Wenn diese Funktion aktiviert ist, wird das Gateway neu gestartet.	Deaktiviert

Einwahl fehlgeschlagen	automatisch, wenn die Einwahl mehrmals fehlschlägt.	
ICMP-Server	Legen Sie die IP-Adresse des ICMP-Erkennungsservers fest.	8.8.8.8
Sekundärer ICMP Server	Legen Sie die IP-Adresse des sekundären ICMP-Erkennungsservers fest.	114.114.114.114
ICMP-Erkennung Maximale Wiederholungsversuche	Legen Sie die maximale Anzahl von Wiederholungsversuchen fest, wenn die ICMP-Erkennung fehlschlägt.	3
ICMP-Erkennung Zeitlimit	Zeitlimit für die ICMP-Erkennung festlegen.	5
ICMP-Erkennung Intervall	Intervall für die ICMP-Erkennung festlegen.	15
SMS-Modus	Wählen Sie den SMS-Modus aus „TEXT“ und „PDU“ aus.	PDU

Tabelle 3-3-1-7 Mobilfunkparameter

Abbildung 3-3-1-10

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(en)	Legen Sie die maximale Dauer des Gateways fest, wenn die aktuelle Verbindung im Leerlaufstatus ist. Bereich: 10-3600.
Durch Anruf ausgelöst	Das Gateway wechselt automatisch vom Offline-Modus in den Mobilfunknetzmodus, wenn es einen Anruf von der angegebenen Telefonnummer erhält.
Anrufgruppe	Wählen Sie eine Anrufgruppe für 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 dem bestimmten Mobiltelefon erhält.
SMS-Gruppe	Wählen Sie eine SMS-Gruppe als Auslöser aus. Gehen Sie zu „System > Allgemeine Einstellungen > Telefon“, um die SMS-Gruppe einzurichten.
SMS-Text	Geben Sie den SMS-Inhalt für die Auslösung ein.

Tabelle 3-3-1-8 Mobilfunkparameter

Verwandte Themen

Anwendungsbeispiel für Mobilfunkverbindung

Telefongruppe

3.3.1.4 Loopback

Die Loopback-Schnittstelle wird zum Ersetzen der Gateway-ID verwendet, solange sie aktiviert ist. Wenn die Schnittstelle DOWN ist 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.

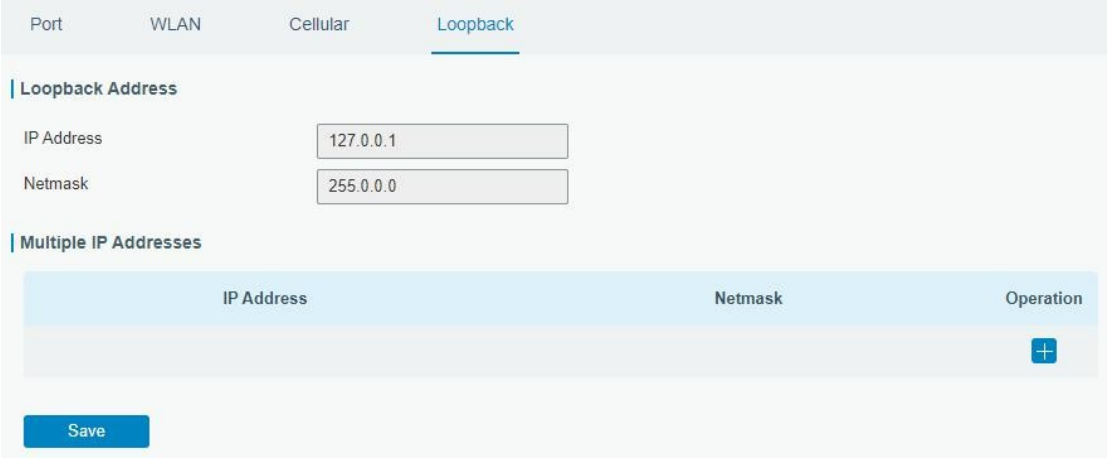


Abbildung 3-3-1-11

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

Tabelle 3-3-1-9 Loopback-Parameter

3.3.1.5 VLAN-Trunk

Das UG56-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 die VLAN-ID ist. Die VLAN-Einstellung ist standardmäßig leer

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

Abbildung 3-3-1-12

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

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

3.3.2 Firewall

In diesem Abschnitt wird beschrieben, wie Sie die Firewall-Parameter einstellen, darunter Website-Blockierung, ACL, DMZ, Port-Zuordnung und MAC-Bindung.

Die Firewall implementiert eine entsprechende Kontrolle des Datenflusses in Eingangsrichtung (vom Internet zum lokalen Netzwerk) und Ausgangsrichtung (vom lokalen Netzwerk zum Internet) entsprechend den Inhaltsmerkmalen der Pakete, wie z. B. Protokolltyp, Quell-/Ziel-IP-Adresse usw. Sie stellt sicher, dass das Gateway in einer sicheren Umgebung und der Host im lokalen Netzwerk betrieben werden.

3.3.2.1 Sicherheit

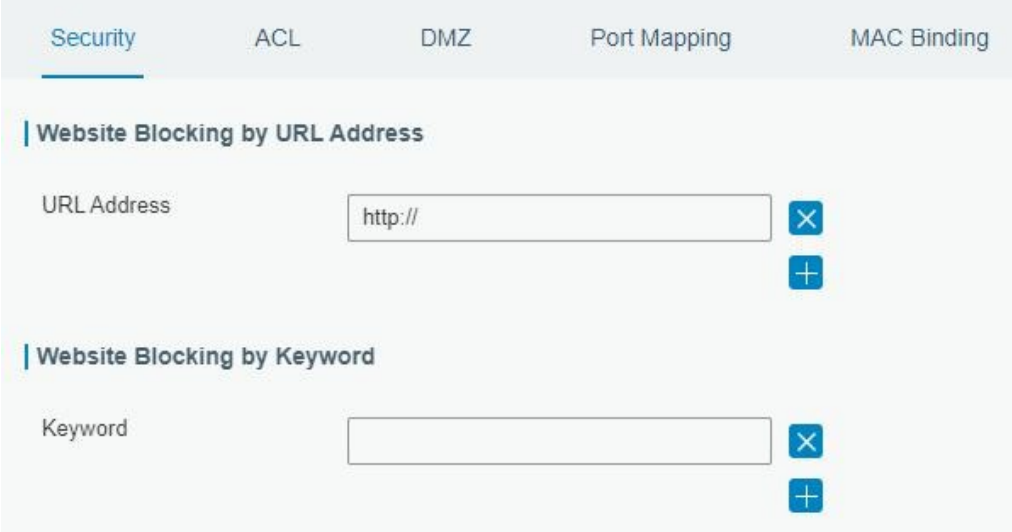


Abbildung 3-3-2-1

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

3.3.2.2 ACL

Die Zugriffskontrollliste, auch ACL genannt, implementiert die Erlaubnis oder das Verbot 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 Berechtigung oder Sperrung des entsprechenden Pakets gemäß der voreingestellten Strategie umgesetzt.
Die von ACL definierten Regeln für die Datenpaketzuordnung können auch von anderen Funktionen verwendet werden, die eine Unterscheidung des Datenflusses erfordern.

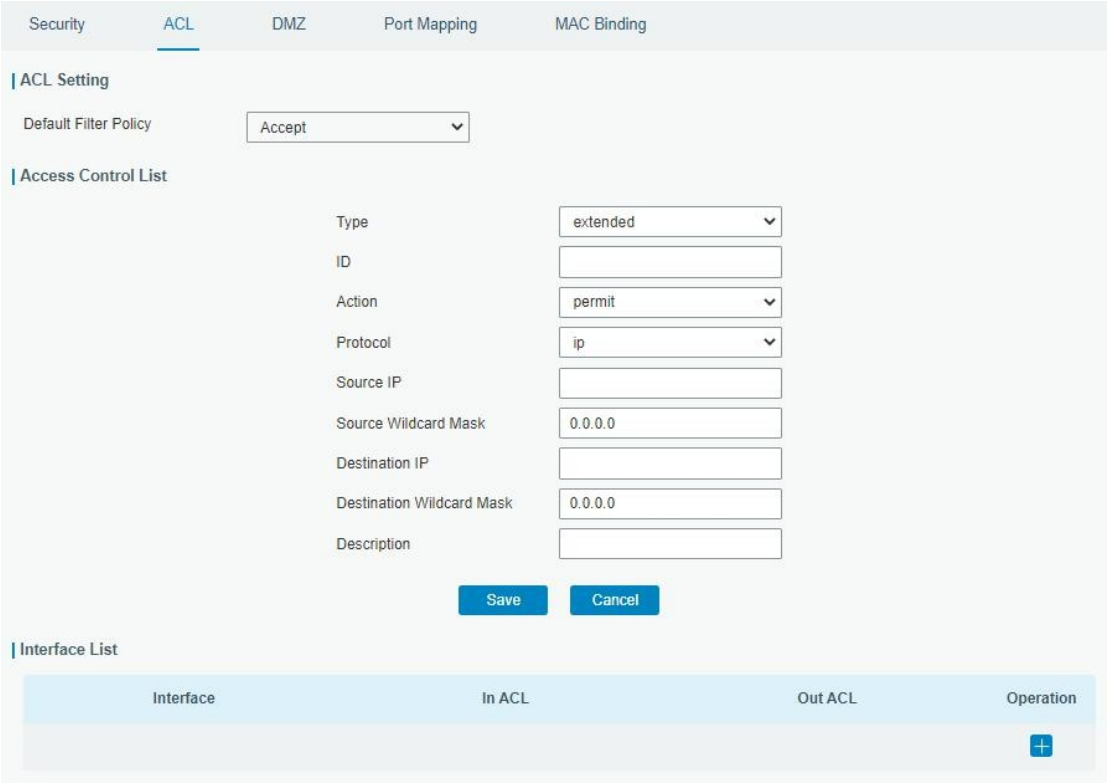


Abbildung 3-3-2-2

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 Typ	Wählen Sie den Typ des Zielports aus, z. B. angegebener Port, Portbereich, 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 3-3-2-2 ACL-Parameter

3.3.2.3 DMZ

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

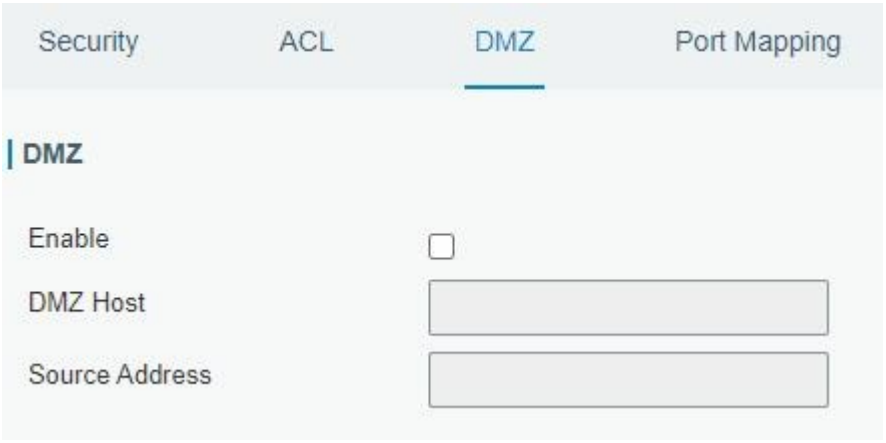


Abbildung 3-3-2-3

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 3-3-2-3 DMZ-Parameter

3.3.2.4 Portzuordnung

Port-Mapping ist eine Anwendung der Netzwerkadressübersetzung (NAT), die eine Kommunikationsanfrage von der Kombination aus Adresse und Portnummer zu einer anderen umleitet, während die Pakete ein Netzwerk-Gateway wie einen Gateway oder eine Firewall durchlaufen.

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

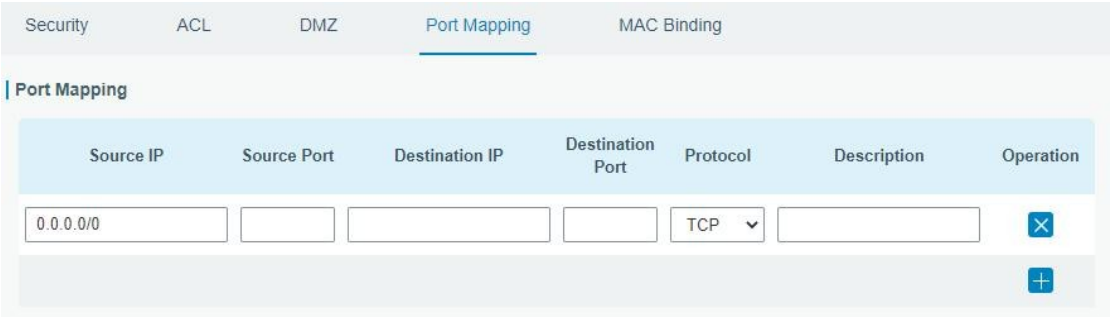


Abbildung 3-3-2-4

Portzuordnung	
Element	**Beschreibung**
Quell-IP	Geben Sie den Host oder das Netzwerk an, der/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 die am/an den eingehenden Port(s) empfangen werden. Bereich: 1-65535.
Protokoll	Wählen Sie je nach Anforderung Ihrer Anwendung zwischen „TCP” und „UDP”.
Beschreibung	Die Beschreibung dieser Regel.

Tabelle 3-3-2-4 Parameter für die Portzuordnung

Beispiel für eine zugehörige Konfiguration

Beispiel für NAT-Anwendung

3.3.2.5 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.

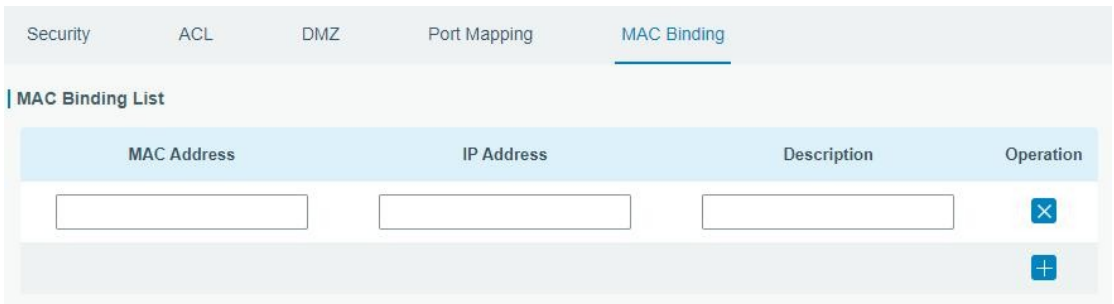


Abbildung 3-3-2-5

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-Paar leichter zu dokumentieren. Bindungsregel für jedes MAC-IP-Paar zu dokumentieren.

Tabelle 3-3-2-5 MAC-Bindungsparameter

3.3.3 DHCP

UG56 kann als DHCP-Server eingerichtet werden, um IP-Adressen zu verteilen, wenn Wi-Fi im AP-Modus arbeitet.

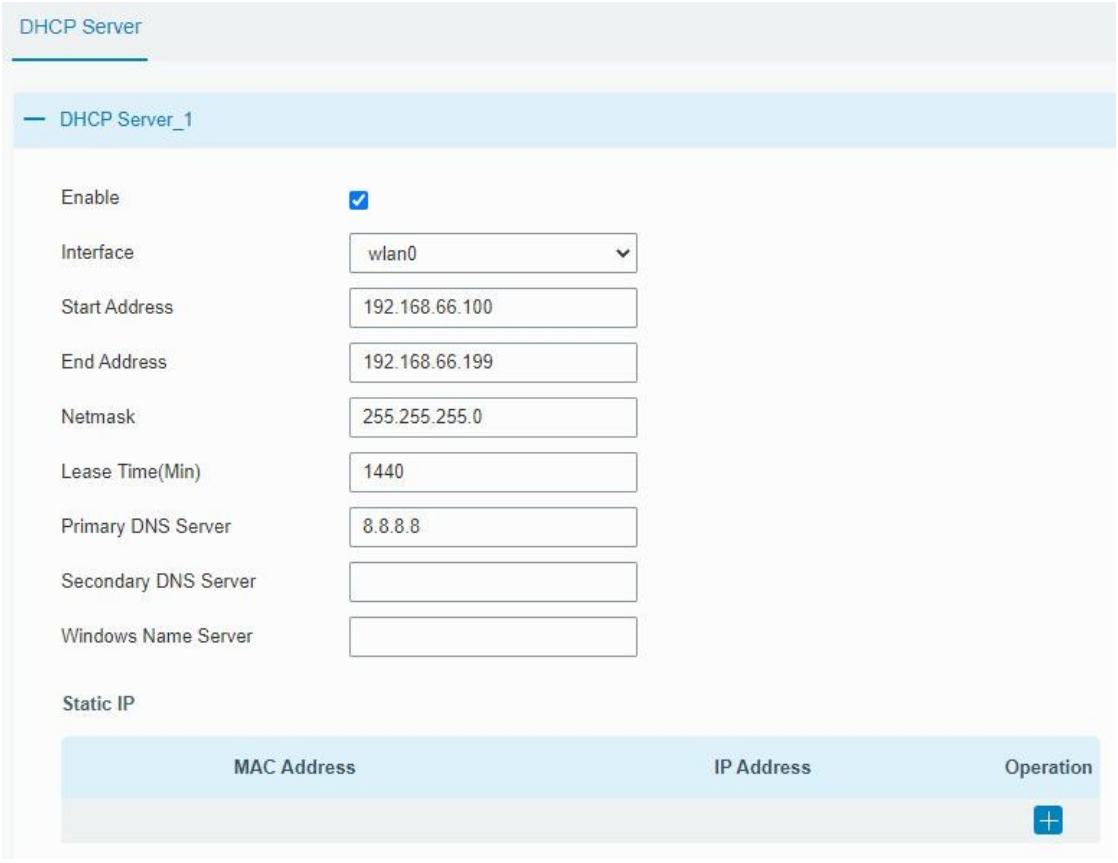


Abbildung 3-3-3-1

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	Legen Sie das Ende des Pools von IP-Adressen fest, die an DHCP-Clients vermietet werden.	192.168.1.199
Netzmaske	Definieren Sie die Subnetzmaske der IP-Adresse, die von DHCP-Clients vom DHCP-Server erhalten 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 erhalten hat. Bereich: 1-10080.	1440
Primär DNS-Server	Legen Sie den primären DNS-Server fest.	114.114.114.114
Sekundär DNS-Server	Sekundären DNS-Server festlegen.	Null
Windows-Name Server	Definieren Sie den Windows-Internetnamensdienst, den DHCP-Clients vom DHCP-Server erhalten. Im Allgemeinen können Sie dieses Feld leer lassen.	Null
Statische IP		
MAC Adresse	Legen Sie eine statische und spezifische MAC-Adresse für den DHCP-Client fest (sie sollte sich von anderen MAC-Adressen unterscheiden, um Konflikte zu vermeiden).	Null
IP-Adresse	Legen Sie eine statische und spezifische IP-Adresse für den DHCP fest. Client (dieser sollte außerhalb des DHCP-Bereichs liegen).	Null

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

3.3.4 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.

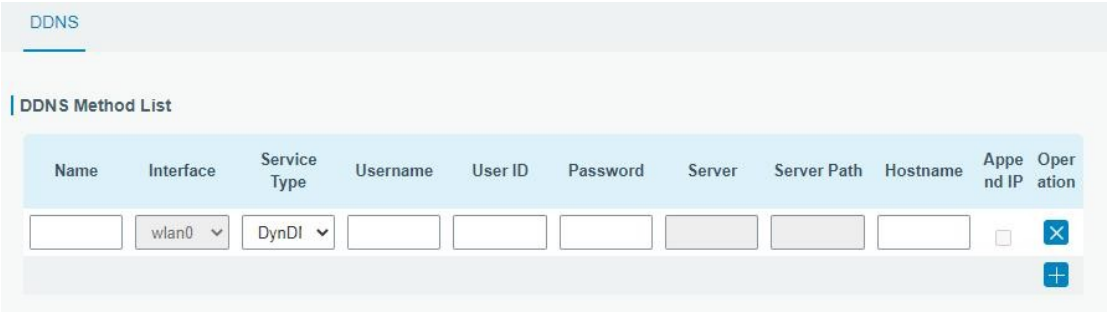


Abbildung 3-3-4-1

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 3-3-4-1 DDNS-Parameter

3.3.5 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.

3.3.5.1 SLA

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

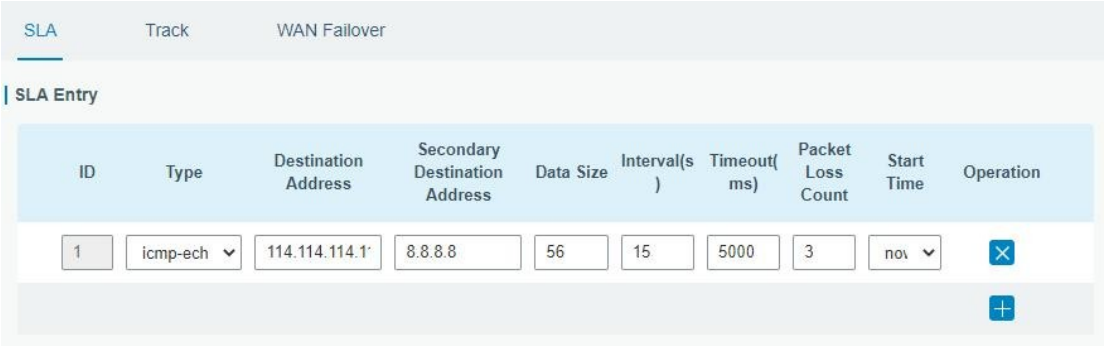


Abbildung 3-3-5-1

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.	114.114.114.114
Sekundär Zieladresse	Die sekundäre erkannte IP-Adresse.	8.8.8.8
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 3-3-5-1 SLA-Parameter

3.3.5.2 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, Statusänderungen zeitnah zu verfolgen.

- Bei erfolgreicher Erkennung ist das entsprechende Track-Element positiv.
- Bei einer fehlgeschlagenen 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.

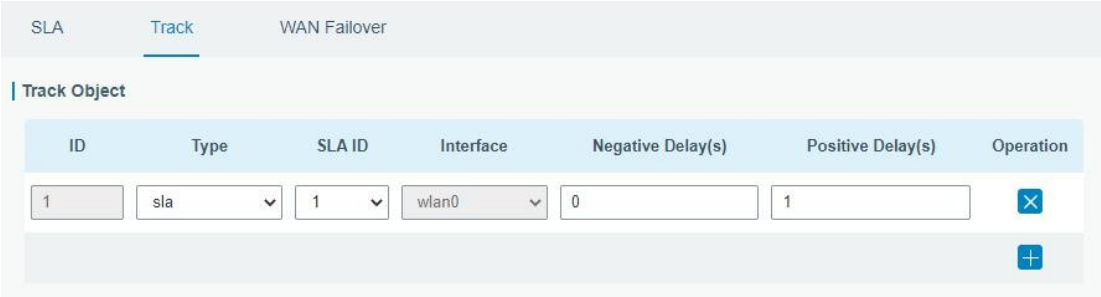


Abbildung 3-3-5-2

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 3-3-5-2 Track-Parameter

3.3.5.3 WAN-Failover

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

Wenn der Verbindungsstatus der Hauptschnittstelle von „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.

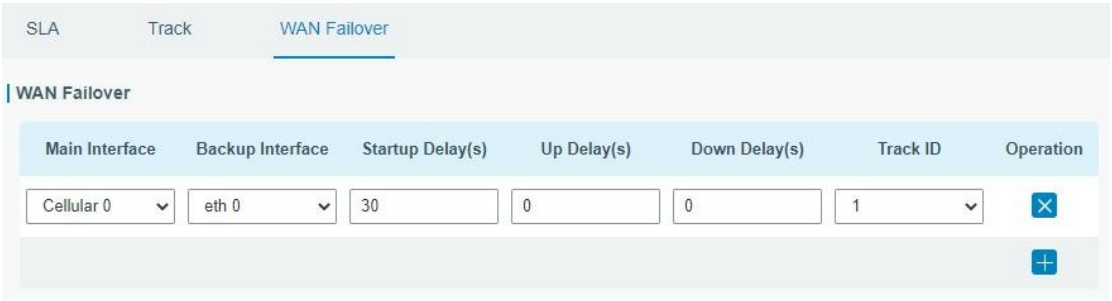


Abbildung 3-3-5-3

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 Startverfolgung 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 erfolgreicher	0

	Bei einer fehlerhaften Erkennung kann die Umschaltung basierend auf der eingestellten Zeit verzögert werden. Bereich: 0-180 (0 bedeutet sofortige Umschaltung).	
Spur-ID	Spurerkennung, wählen Sie die definierte Spur-ID aus.	--

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

3.3.6 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.
UG56 unterstützt DMVPNIPsec, GRE, L2TP, PPTP, OpenVPN sowie GRE über IPsec und L2TP über IPsec.

3.3.6.1 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.

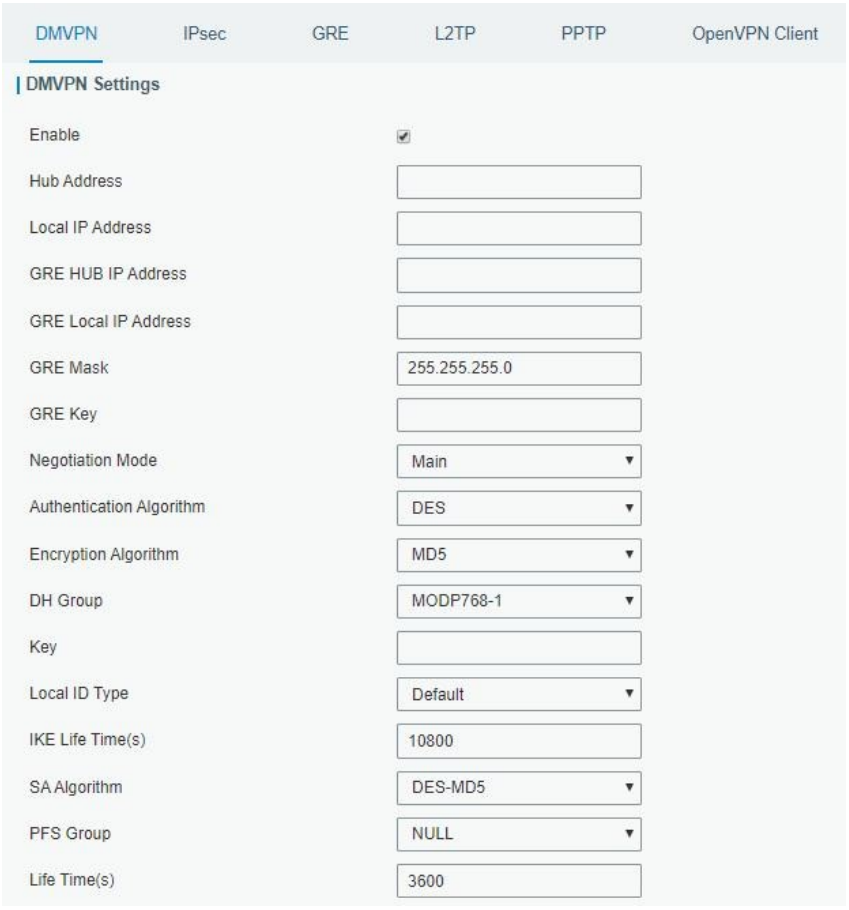


Abbildung 3-3-6-1

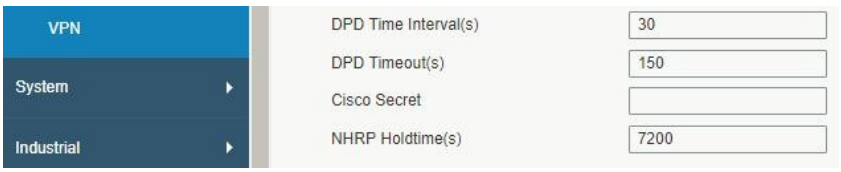


Abbildung 3-3-6-2

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	Lokale GRE-Tunnel-Netzmaske.
GRE-Schlüssel	GRE-Tunnels-Schlüssel.
Verhandlungsmodus	Wählen Sie zwischen „Main“ und „Aggressive“.
Authentifizierung Algorithmus	Wählen Sie zwischen „DES“, „3DES“, „AES128“, „AES192“ und „AES256“ aus.
Verschlüsselungsalgorithmus	Wählen Sie zwischen „MD5“ und „SHA1“.
DH-Gruppe	Wählen Sie zwischen „MODP768_1“, „MODP1024_2“ und „MODP1536_5“.
Schlüssel	Geben Sie den vorab vereinbarten Schlüssel ein.
Lokale ID-Art	Wählen Sie zwischen „Standard“, „ID“, „FQDN“ und „Benutzer-FQDN“
IKE-Lebensdauer (s)	Legen Sie die Lebensdauer in der IKE-Verhandlung fest. Bereich: 60-86400.
SA-Algorithmus	Wählen Sie zwischen „DES_MD5“, „DES_SHA1“, „3DES_MD5“, „3DES_SHA1“, „AES128_MD5“, „AES128_SHA1“, „AES192_MD5“, „AES192_SHA1“, „AES256_MD5“ und „AES256_SHA1”.
PFS-Gruppe	Wählen Sie zwischen „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 3-3-6-1 DMVPN-Parameter

3.3.6.2 IPSec

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

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

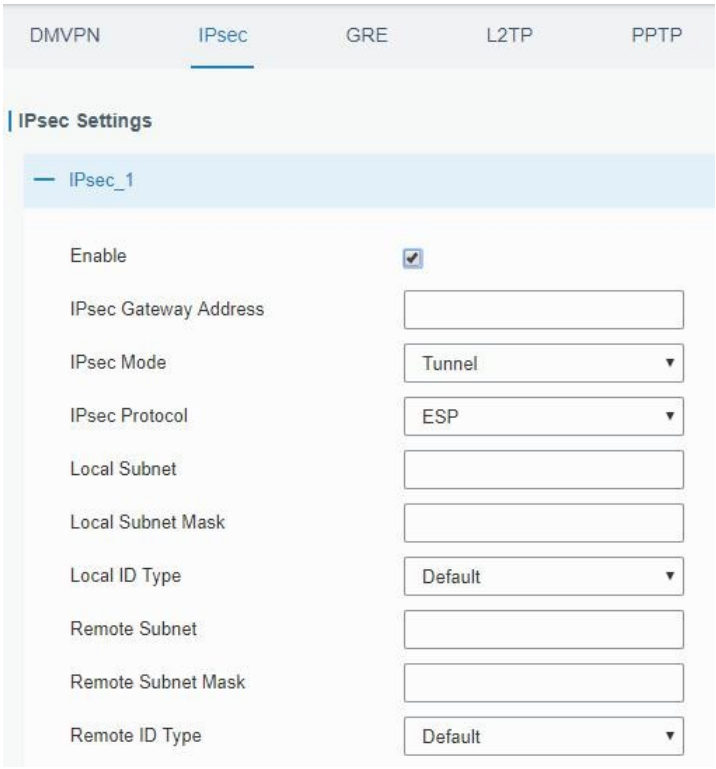


Abbildung 3-3-6-3

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 .
Wählen Sie zwischen „Tunnel“ und „Transport“.	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 wird.
Remote-Subnetzmaske	Geben Sie die Remote-Netzmaske ein, die IPsec schützt.
Remote-ID-Typ	Wählen Sie zwischen „Standard“, „ID“, „FQDN“ und „Benutzer-FQDN“.

Tabelle 3-3-6-2 IPsec-Parameter

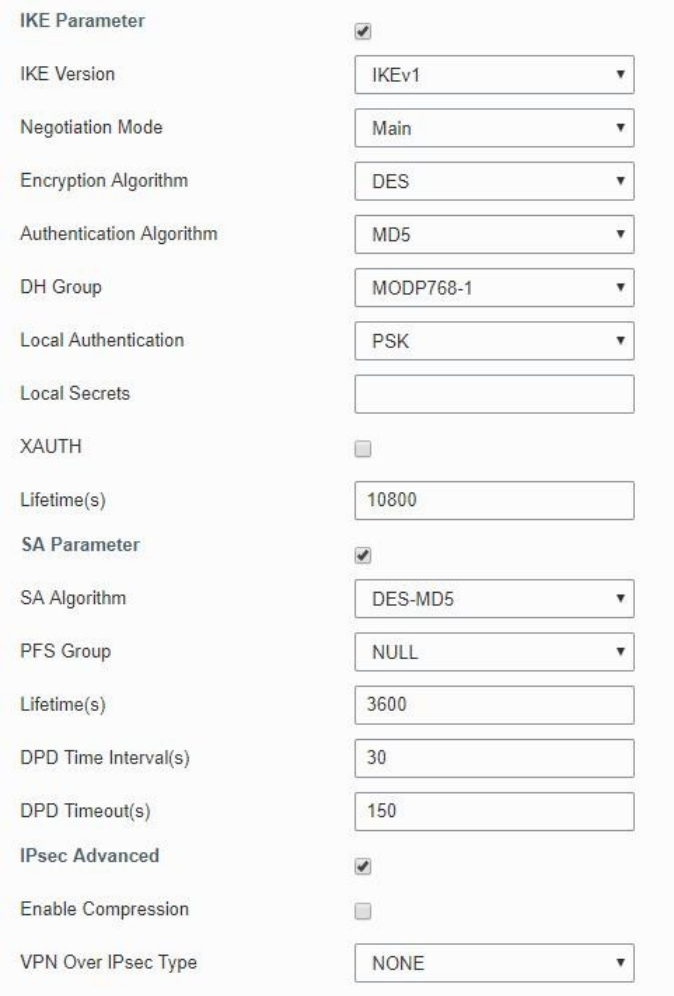


Abbildung 3-3-6-4

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 (s)	Legen Sie das DPD-Intervall fest, um zu erkennen, ob die Gegenstelle ausgefallen ist.
DPD-Zeitüberschreitung(en)	DPD-Zeitlimit festlegen. Bereich: 10-3600.
IPsec erweitert	
Komprimierung aktivieren	Der Kopf des IP-Pakets wird nach der Aktivierung komprimiert.
VPN über IPsec-Typ	Wählen Sie zwischen „NONE", „GRE" und „L2TP", um VPN über IPsec-Funktion zu aktivieren.

Tabelle 3-3-6-3 IPsec-Parameter

3.3.6.3 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.

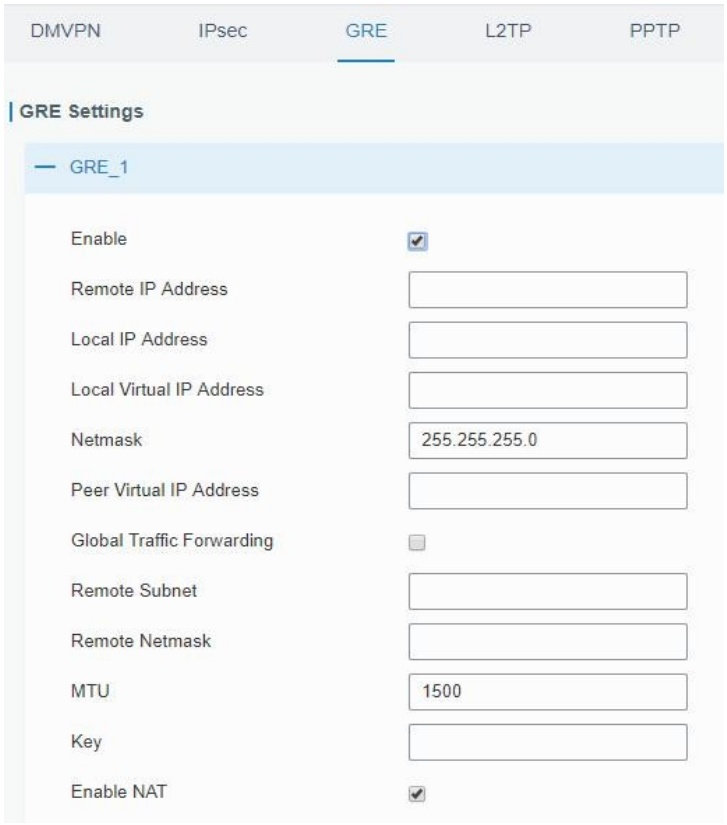


Abbildung 3-3-6-5

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 3-3-6-4 GRE-Parameter

3.3.6.4 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.

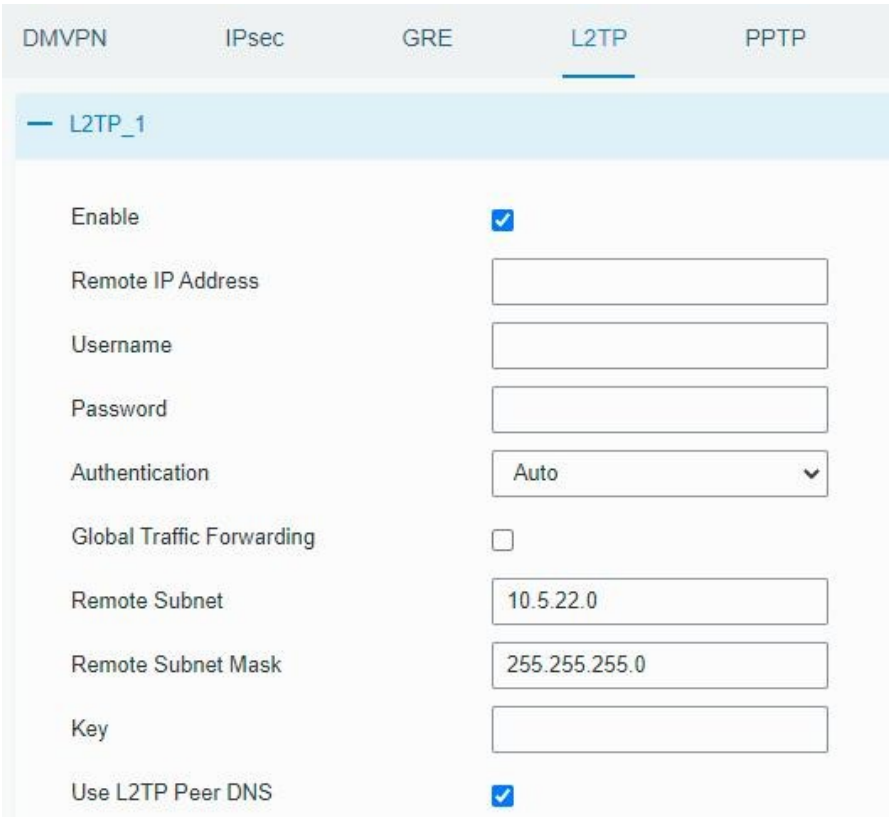


Abbildung 3-3-6-6

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 3-3-6-5 L2TP-Parameter

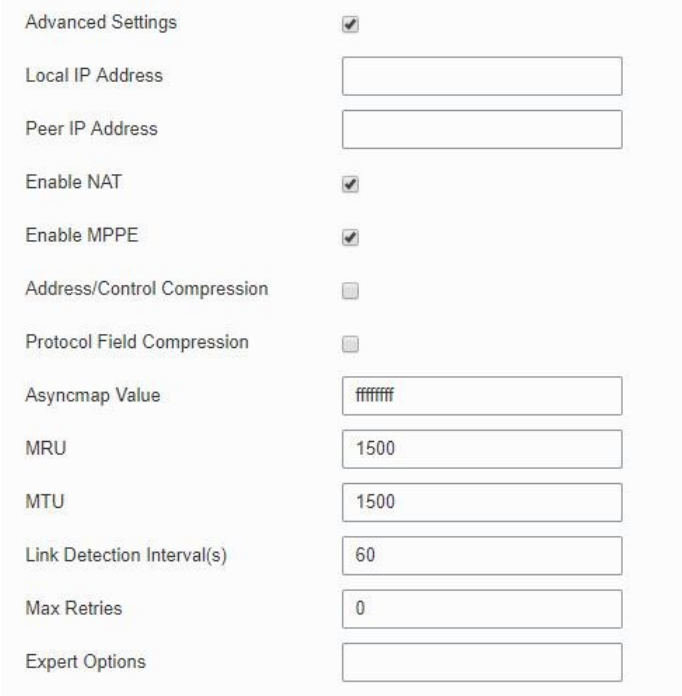


Abbildung 3-3-6-7

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.
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: 64-1500
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 3-3-6-6 L2TP-Parameter

3.3.6.5 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.

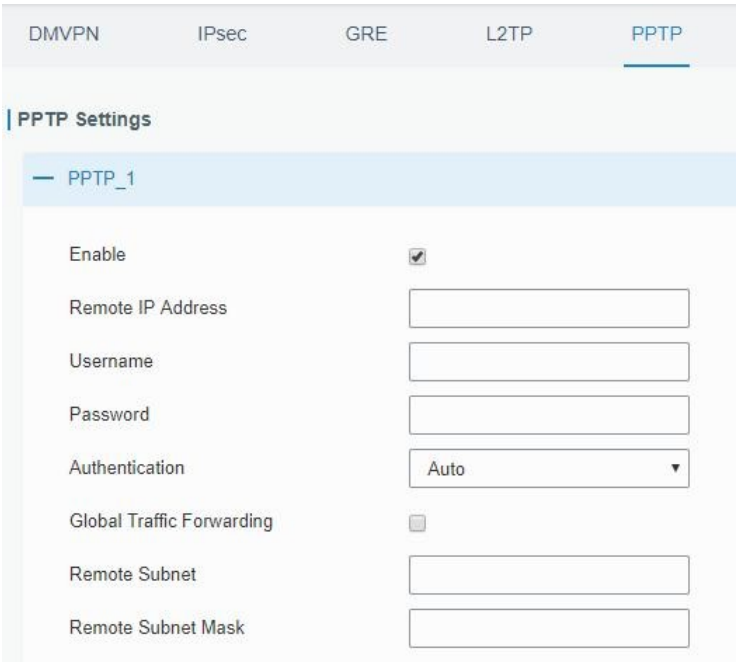


Abbildung 3-3-6-8

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. 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 3-3-6-7 PPTP-Parameter

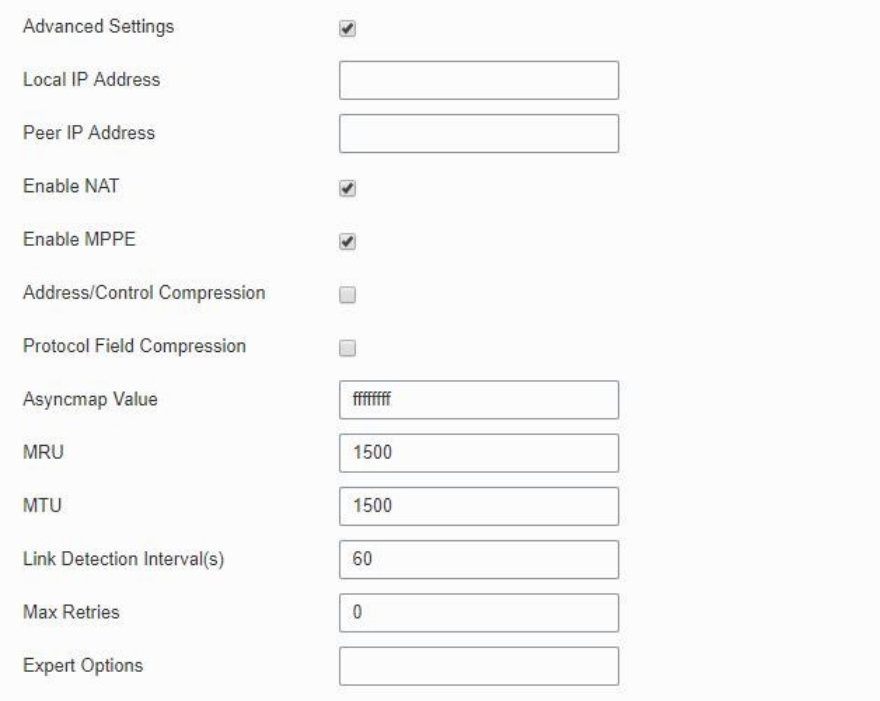


Abbildung 3-3-6-9

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: 0-1500.
MTU	Geben Sie die maximale Übertragungseinheit ein. Bereich: 0-1500.
Link-Erkennungsintervall (s)	Stellen Sie das Link-Erkennungsintervall ein, um die Tunnelverbindung sicherzustellen Verbindung. Bereich: 0-600.
Maximale Wiederholungsversuche	Legen Sie die maximale Anzahl von Wiederholungsversuchen 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 3-3-6-8 PPTP-Parameter

3.3.6.6 OpenVPN-Client

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

Zu den Vorteilen von OpenVPN gehören:

- Sicherheitsvorkehrungen, die sowohl gegen aktive als auch passive Angriffe wirken.
- Kompatibilität mit allen gängigen Betriebssystemen.
- Hohe Geschwindigkeit (in der Regel 1,4 Megabyte pro Sekunde).
- Möglichkeit, mehrere Server so zu konfigurieren, dass sie zahlreiche Verbindungen gleichzeitig verarbeiten können.
- Alle Verschlüsselungs- und Authentifizierungsfunktionen der OpenSSL-Bibliothek.
- Erweitertes Bandbreitenmanagement.
- Eine Vielzahl von Tunneling-Optionen.
- Kompatibilität mit Smartcards, die die Windows Crypt-Anwendungsprogrammierschnittstelle (API) unterstützen.

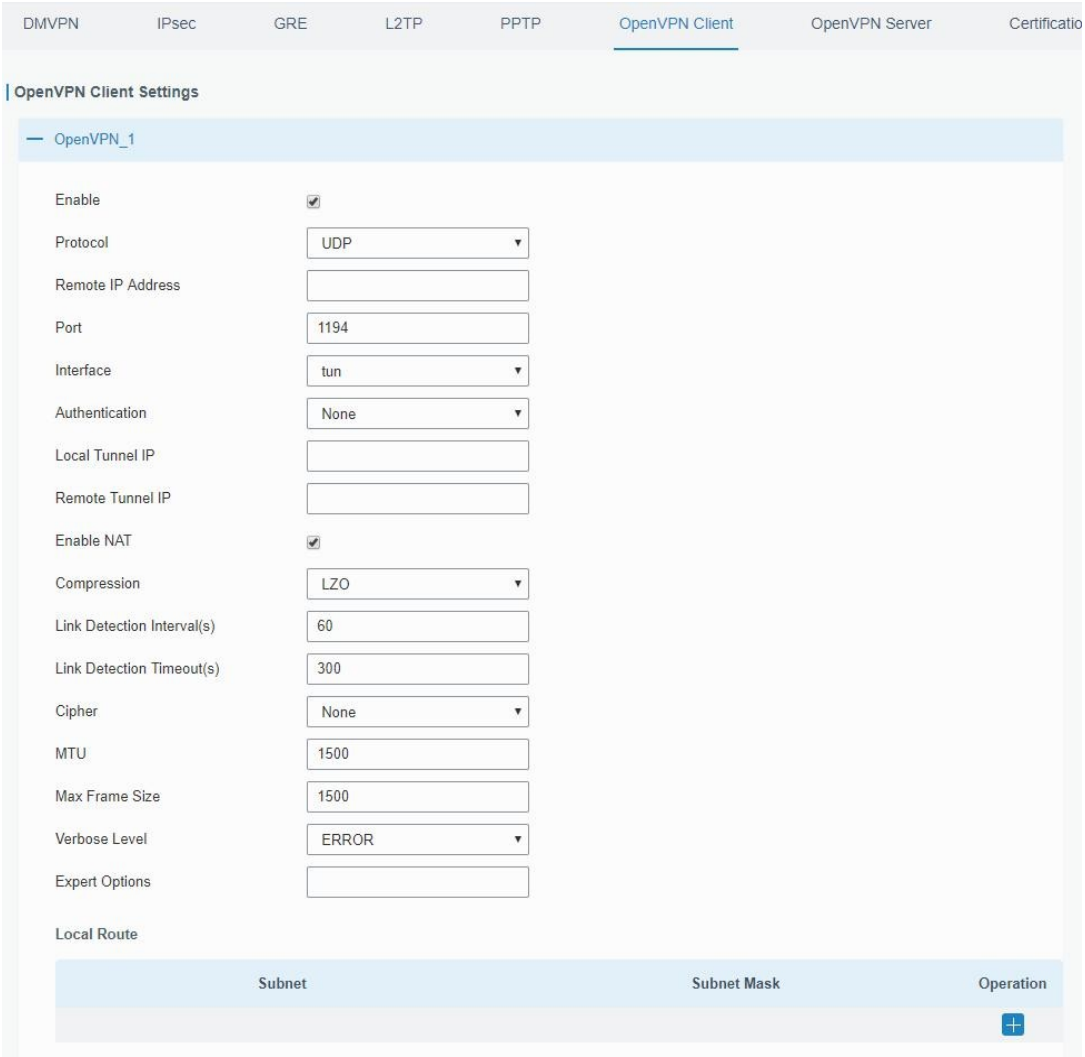


Abbildung 3-3-6-10

OpenVPN-Client	
Element	**Beschreibung**
Aktivieren	OpenVPN-Client aktivieren. Es sind maximal 3 Tunnel zulässig.

Protokoll	Wählen Sie zwischen „UDP" und „TCP".
Remote-IP-Adresse	Geben Sie die IP-Adresse oder den Domänennamen des Remote-OpenVPN-Servers ein.
Port	Geben Sie die Portnummer des Remote-OpenVPN-Servers ein. Bereich: 1-65535.
Schnittstelle	Wählen Sie zwischen „tun" und „tap".
Authentifizierung	Wählen Sie zwischen „Keine", „Vorab geteilt", „Benutzername/Passwort", „X.509-Zertifikat" und „X.509-Zertifikat+Benutzer".
Lokale Tunnel-IP	Legen Sie die lokale Tunneladresse fest.
Remote-Tunnel-IP	Geben Sie die Remote-Tunneladresse ein.
Globaler Datenverkehr Weiterleitung	Der gesamte Datenverkehr wird über den OpenVPN-Tunnel gesendet, wenn diese Funktion aktiviert ist.
TLS-Authentifizierung aktivieren Authentifizierung	Aktivieren Sie diese Option, um die TLS-Authentifizierung zu aktivieren.
Benutzername	Geben Sie den vom OpenVPN-Server bereitgestellten Benutzernamen ein.
Passwort	Geben Sie das vom OpenVPN-Server bereitgestellte Passwort ein.
NAT aktivieren	NAT-Traversal-Funktion aktivieren.
Komprimierung	Wählen Sie LZO, um Daten zu komprimieren.
Link-Erkennungsintervall (s)	Legen Sie das Verbindungserkennungsintervall fest, um die Tunnelverbindung sicherzustellen. Bereich: 10-1800.
Zeitlimit für die Verbindungserkennung (s)	Legen Sie das Zeitlimit für die Verbindungserkennung fest. OpenVPN wird nach Ablauf des Zeitlimits. Bereich: 60-3600.
Verschlüsselung	Wählen Sie zwischen „NONE", „BF-CBC", „DE-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 andere Initialisierungszeichenfolgen eingeben und die Zeichenfolgen durch Semikolons trennen.
Lokale Route	
Subnetz	Legen Sie die IP-Adresse der lokalen Route fest.
Subnetzmaske	Legen Sie die Netzmaske der lokalen Route fest.

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

3.3.6.7 OpenVPN-Server

UG56 unterstützt OpenVPN-Server zum Erstellen sicherer Punkt-zu-Punkt- oder Standort-zu-Standort-Verbindungen in gerouteten oder gebrückten Konfigurationen und Fernzugriffsfunktionen.

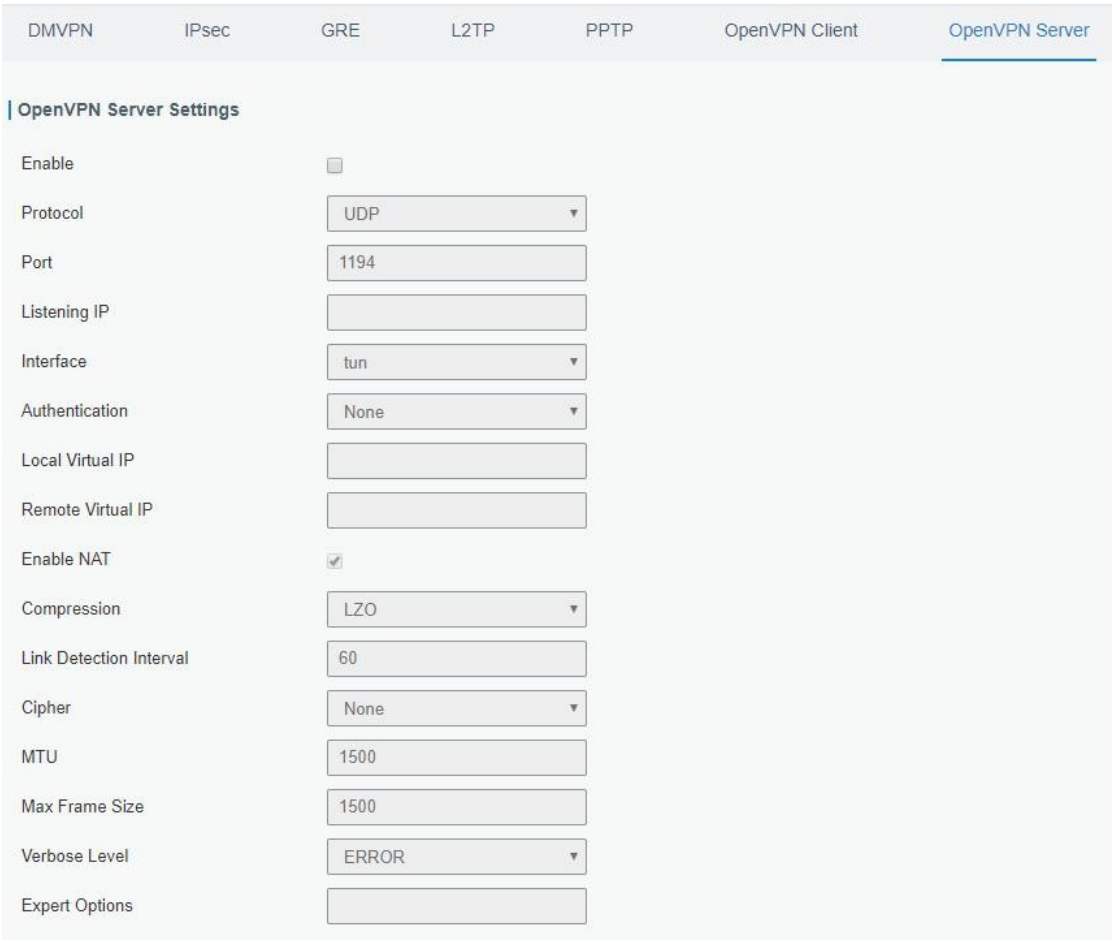


Abbildung 3-3-6-11

Abbildung 3-3-6-12

OpenVPN-Server	
Element	**Beschreibung**
Aktivieren	OpenVPN-Server aktivieren/deaktivieren.
Protokoll	Wählen Sie zwischen TCP und UDP.
Port	Geben Sie die Nummer des Listening-Ports ein. Bereich: 1-65535.
IP-Adresse für den Listening-Port	Geben Sie die WAN-IP-Adresse oder die LAN-IP-Adresse ein. Wenn Sie das Feld leer lassen bezieht sich auf alle aktiven WAN-IP- und LAN-IP-Adressen.
Schnittstelle	Wählen Sie zwischen „ tun" und „tap".
Authentifizierung	Wählen Sie zwischen „Keine", „Vorab geteilt", „Benutzername/Passwort", „X.509-Zertifikat" und „X.509-Zertifikat + Benutzer".
Lokale virtuelle IP	Die lokale Tunneladresse des OpenVPN-Tunnels.

Virtuelle Remote-IP	Die Remote-Tunneladresse des OpenVPN-Tunnels.
Client-Subnetz	Lokale Subnetz-IP-Adresse des OpenVPN-Clients.
Client-Netzmaske	Lokale Netzmaske des OpenVPN-Clients.
Neuverhandlungsintervall(e)	Intervall für Neuverhandlungen festlegen. Bereich: 0-86400.
Maximale Anzahl Clients	Maximale Anzahl von OpenVPN-Clients. Bereich: 1-128.
CRL aktivieren	CRL aktivieren
Client-zu-Client aktivieren	Zugriff zwischen verschiedenen OpenVPN-Clients zulassen.
Dup-Client aktivieren	Ermöglicht mehreren Benutzern die Verwendung derselben Zertifizierung.
NAT aktivieren	Aktivieren Sie diese Option, um die NAT-Traversal-Funktion zu aktivieren.
Komprimierung	Wählen Sie „LZO“, um Daten zu komprimieren.
Link-Erkennungsintervall	Legen Sie das Intervall für die Verbindungserkennung fest, um die Tunnelverbindung sicherzustellen. Bereich: 10-1800.
Verschlüsselung	Wählen Sie zwischen „NONE“, „BF-CBC“, „DES-CBC“, „DES-EDE3-CBC“, „AES-128-CBC“, „AES-192-CBC“ und „AES-256-CBC“.
MTU	Geben Sie die maximale Übertragungseinheit ein. Bereich: 64-1500.
Maximale Frame-Größe	Legen Sie die maximale Rahmengröße fest. Bereich: 64-1500.
Ausführlichkeitsstufe	Wählen Sie zwischen „ERROR“, „WARING“, „NOTICE“ und „DEBUG“.
Expertenoptionen	Der Benutzer kann in diesem Feld einige andere Initialisierungszeichenfolgen eingeben. und trennen Sie die Zeichenfolgen durch Semikolons.
Lokale Route	
Subnetz	Die tatsächliche lokale IP-Adresse des OpenVPN-Clients.
Netzmaske	Die tatsächliche lokale Netzmaske des OpenVPN-Clients.
Konto	
Benutzername und Passwort	Legen Sie Benutzername und Passwort für den OpenVPN-Client fest.

Tabelle 3-3-6-10 OpenVPN-Serverparameter

3.3.6.8 Zertifikate

Auf dieser Seite kann der Benutzer Zertifikats- und Schlüsseldateien für OpenVPN und IPsec importieren/exportieren.

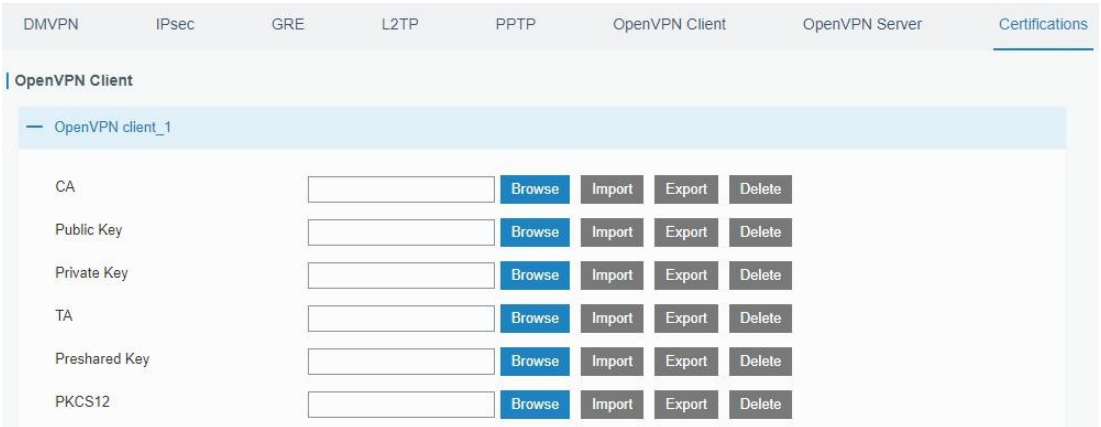


Abbildung 3-3-6-13

OpenVPN-Client	
Element	**Beschreibung**
CA	CA-Zertifikatsdatei importieren/exportieren.

Öffentlicher Schlüssel	Öffentliche Schlüsseldatei importieren/exportieren.
Privater Schlüssel	Private Schlüssel-Datei importieren/exportieren.
TA	Importieren/Exportieren der TA-Schlüsseldatei.
Vorab geteilter Schlüssel	Importieren/Exportieren einer statischen Schlüsseldatei.
PKCS12	PKCS12-Zertifikatsdatei importieren/exportieren.

Tabelle 3-3-6-11 OpenVPN-Client-Zertifizierungsparameter

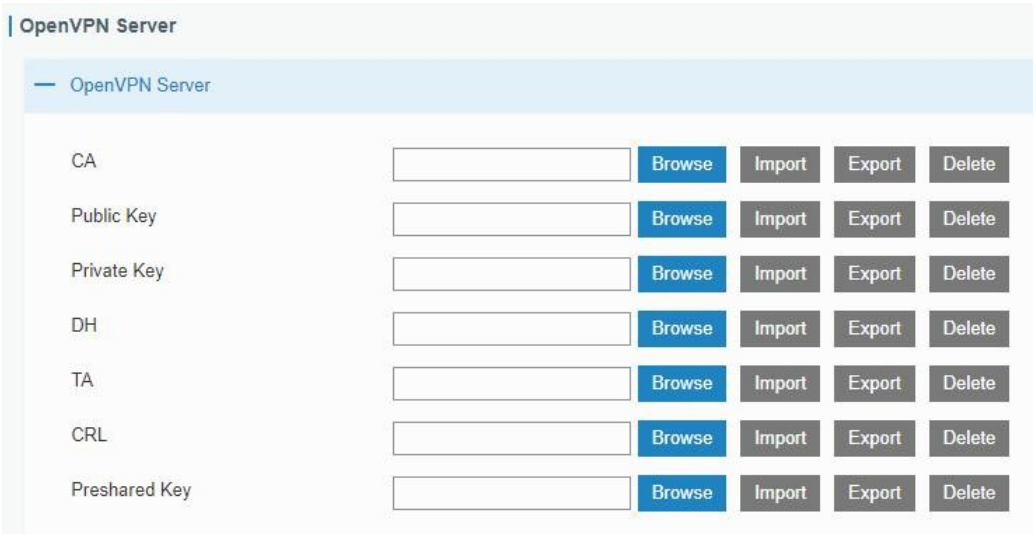


Abbildung 3-3-6-14

OpenVPN-Server	
Element	**Beschreibung**
CA	CA-Zertifikatsdatei importieren/exportieren.
Öffentlicher Schlüssel	Öffentliche Schlüsseldatei importieren/exportieren.
Privater Schlüssel	Importieren/Exportieren der Datei mit dem privaten Schlüssel.
DH	DH-Schlüsseldatei importieren/exportieren.
TA	Importieren/Exportieren einer TA-Schlüsseldatei.
CRL	CRL importieren/exportieren.
Vorab geteilter Schlüssel	Importieren/Exportieren der statischen Schlüsseldatei.

Tabelle 3-3-6-12 OpenVPN-Serverparameter

Abbildung 3-3-6-15

IPsec	
Element	**Beschreibung**
CA	CA-Zertifikat importieren/exportieren.
Client-Schlüssel	Client-Schlüssel importieren/exportieren.
Serverschlüssel	Importieren/Exportieren Sie den Serverschlüssel.
Privater Schlüssel	Privaten Schlüssel importieren/exportieren.
CRL	Importieren/Exportieren der Zertifikatswiederherstellungsliste.

Tabelle 3-3-6-13 IPsec-Parameter

3.4 System

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

3.4.1 Allgemeine Einstellungen

3.4.1.1 Allgemein

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

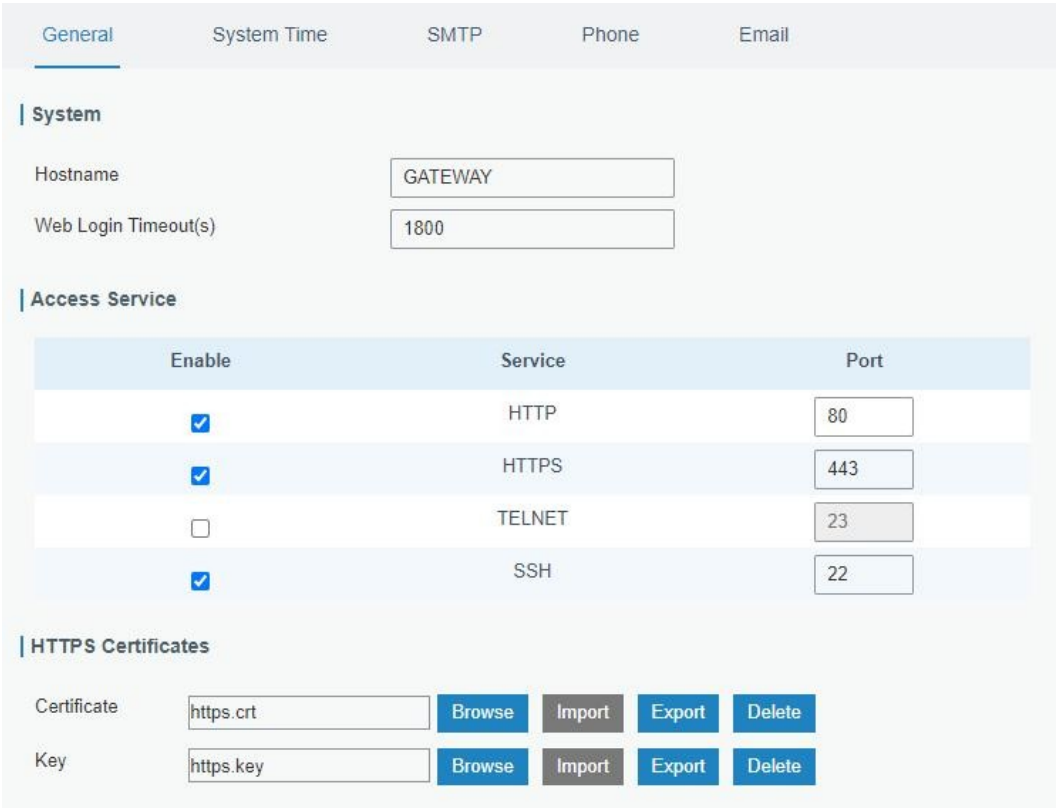


Abbildung 3-4-1-1

Allgemein		
Element	**Beschreibung**	**Standard**
System		
Hostname	Benutzerdefinierter Gateway-Name, muss mit einem Buchstaben beginnen.	GATEWAY

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

Tabelle 3-4-1-1 Allgemeine Einstellungsparameter

3.4.1.2 Systemzeit

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

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

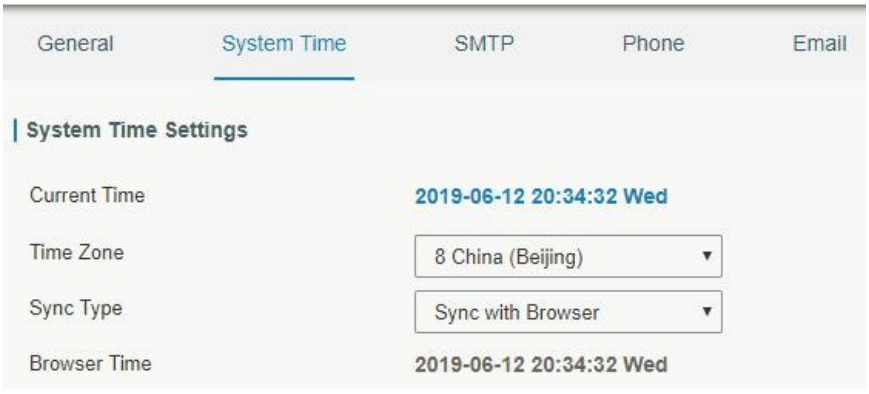


Abbildung 3-4-1-2

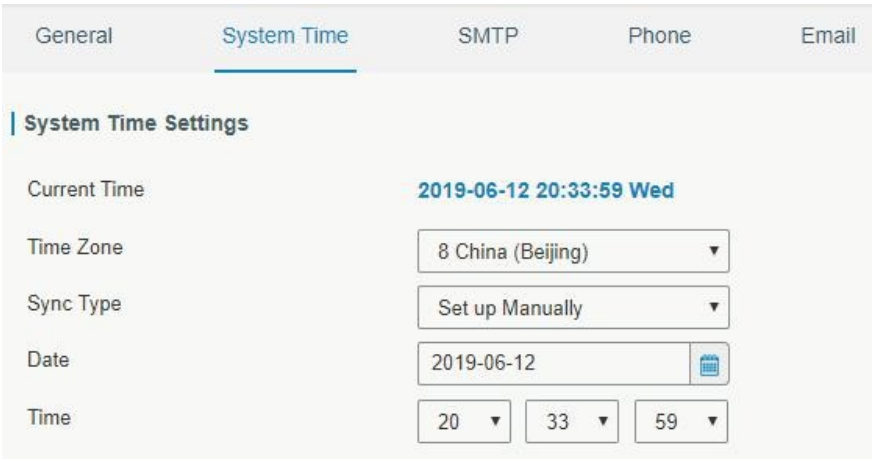


Abbildung 3-4-1-3

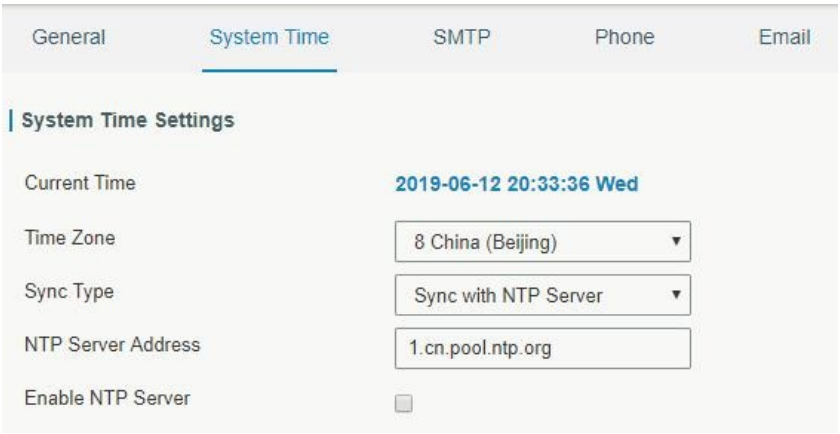


Abbildung 3-4-1-4

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 Zeitsynchronisationstyp auszuwählen .
Mit Browser synchronisieren	Synchronisieren Sie die Zeit mit dem Browser.
Browser-Zeit	Zeigt die aktuelle Zeit des Browsers an.
Manuell einrichten	Konfigurieren Sie die Systemzeit manuell.
Mit NTP-Server synchronisieren	Synchronisieren Sie die Zeit mit dem NTP-Server, um eine Zeitsynchronisation Synchronisierung aller mit einer Uhr ausgestatteten Geräte im Netzwerk zu erreichen.
Mit NTP-Server synchronisieren	
NTP-Serveradresse	Legen Sie die NTP-Serveradresse (Domänenname/IP) fest.
NTP-Server aktivieren	Der NTP-Client im Netzwerk kann die Zeitsynchronisation mit dem Gateway durchführen, nachdem die Option „NTP-Server aktivieren" aktiviert wurde.

Tabelle 3-4-1-2 Systemzeitparameter

3.4.1.3 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.

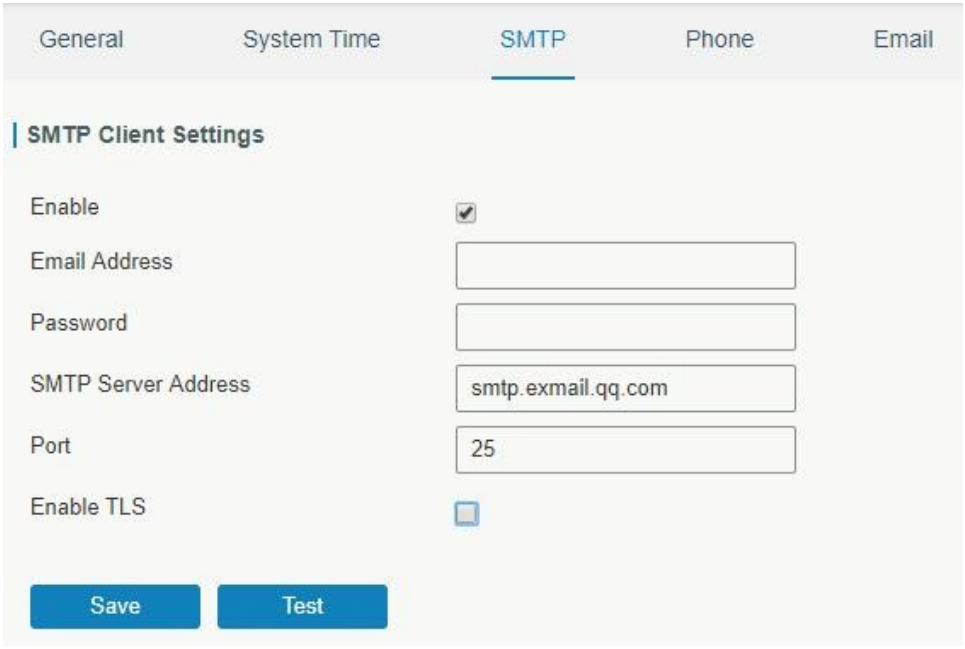


Abbildung 3-4-1-5

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

Tabelle 3-4-1-3 SMTP-Einstellungen

Verwandte Themen

Ereigniseinstellungen

3.4.1.4 Telefon

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

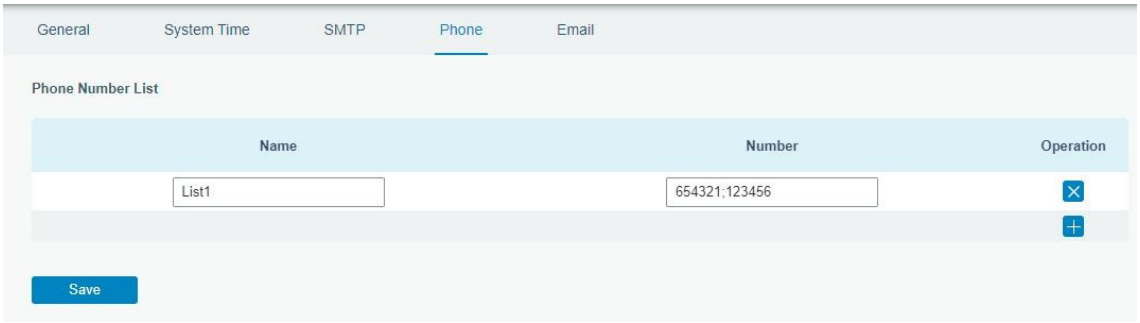


Abbildung 3-4-1-6

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 3-4-1-4 Telefoneinstellungen

Verwandtes Thema

Verbindung bei Bedarf

3.4.1.5 E-Mail

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

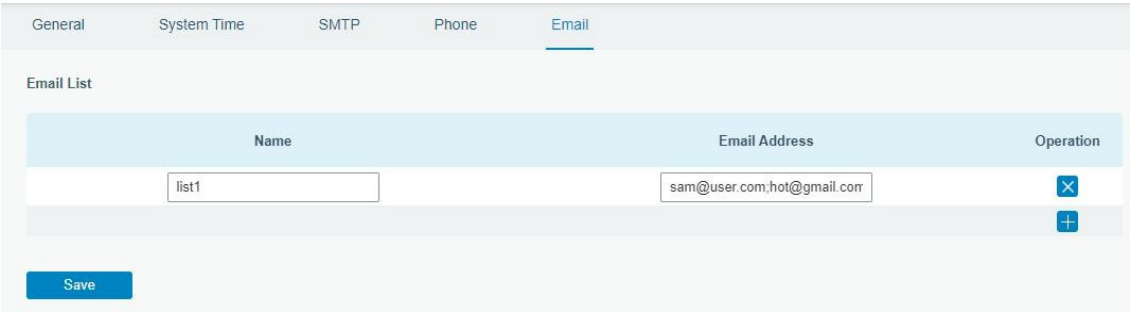


Abbildung 3-4-1-7

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 3-4-1-5 E-Mail-Einstellungen

3.4.2 Benutzerverwaltung

3.4.2.1 Konto

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

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

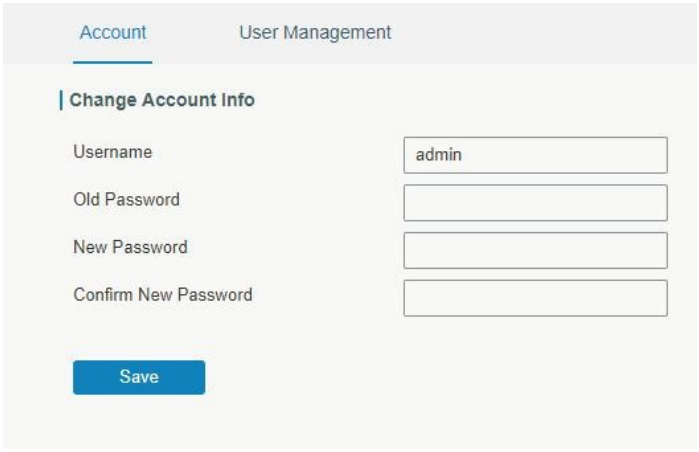


Abbildung 3-4-2-1

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.
Neues Passwort bestätigen	Geben Sie das neue Passwort erneut ein.

Tabelle 3-4-2-1 Kontoinformationen

3.4.2.2 Benutzerverwaltung

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

Abbildung 3-4-2-2

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.

Berechtigung	Wählen Sie die Benutzerberechtigung aus „Nur lesen“ und „Lesen-Schreiben“ aus. - Nur Lesen: Benutzer können auf dieser Ebene nur die Konfiguration des Gateways anzeigen. - Lesen/Schreiben: Benutzer können die Konfiguration des Gateways in dieser Ebene anzeigen und festlegen. Gateways anzeigen und festlegen.

Tabelle 3-4-2-2 Benutzerverwaltung

3.4.3 SNMP

SNMP wird häufig in der Netzwerkverwaltung für die Netzwerküberwachung eingesetzt. SNMP stellt Verwaltungsdaten in Form von Variablen im verwalteten System bereit. Das System ist in einer Verwaltungsinformationsbasis (MIB) organisiert, die den Systemstatus und die Konfiguration beschreibt. Diese Variablen können von Verwaltungsanwendungen aus ferngesteuert abgefragt werden.
Die Konfiguration von SNMP im Netzwerk, NMS und einem Verwaltungsprogramm von SNMP sollte auf dem Manager eingerichtet werden.

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

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

3.4.3.1 SNMP

UG56 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.

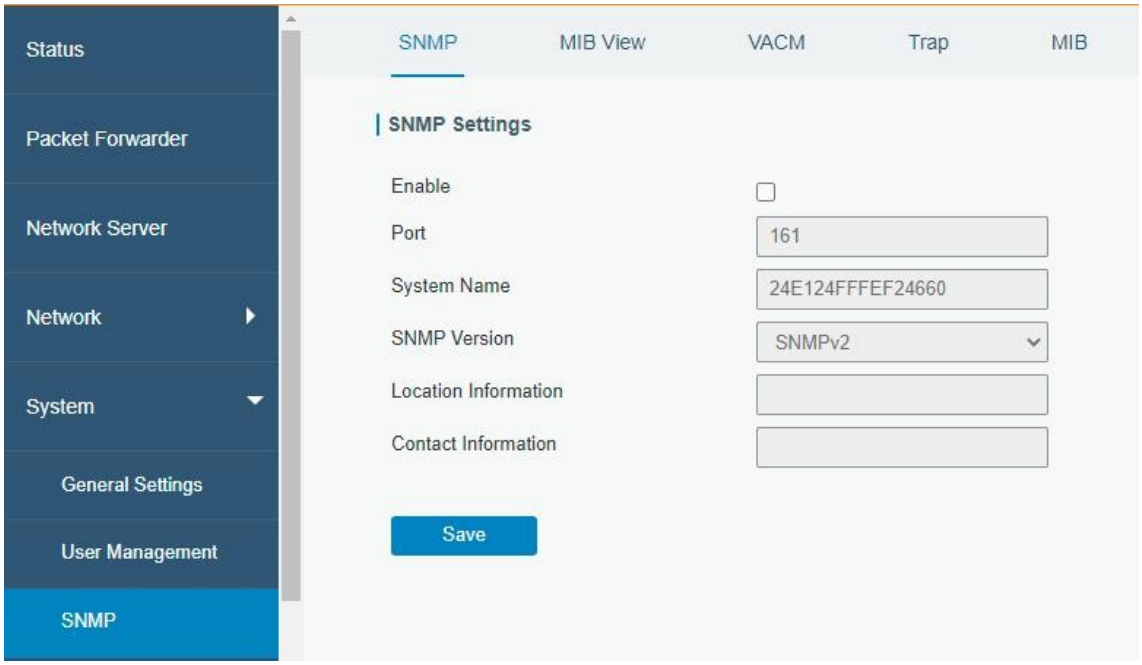


Abbildung 3-4-3-1

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.
Kontakt	Geben Sie die Kontaktinformationen ein.

Tabelle 3-4-3-1 SNMP-Parameter

3.4.3.2 MIB-Ansicht

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

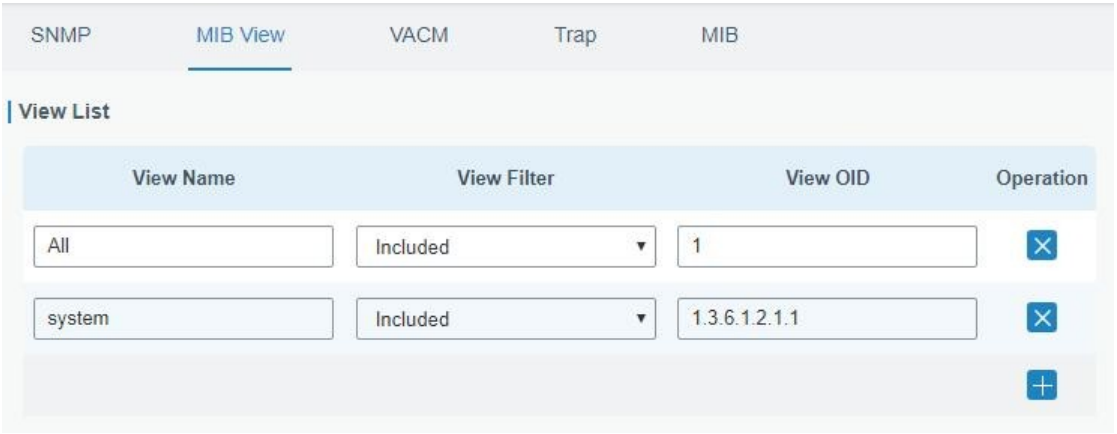


Abbildung 3-4-3-2

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 3-4-3-2 MIB-Ansichtsparameter

3.4.3.3 VACM

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

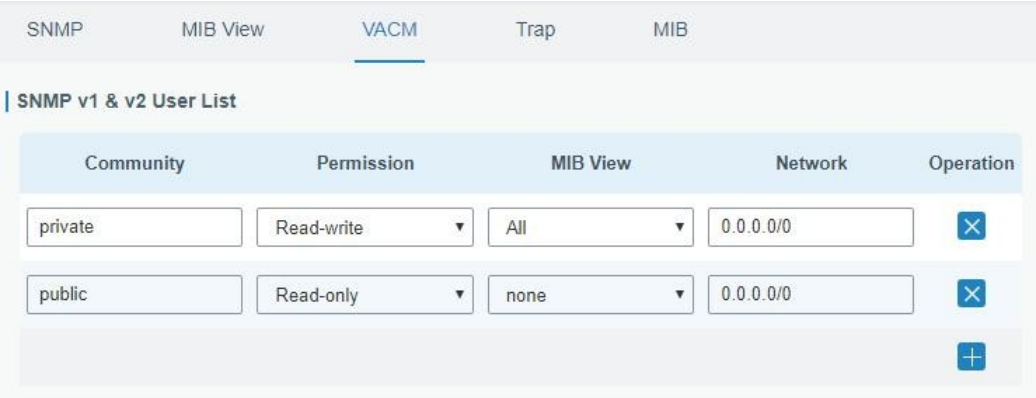


Abbildung 3-4-3-3

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 „Lesen-Schreiben" in der Liste der MIB-Ansichten festzulegen .
Inform-Ansicht	Wählen Sie eine MIB-Ansicht aus, um die Berechtigung als „Informieren" aus der MIB-Ansichtsliste festzulegen.

Tabelle 3-4-3-3 VACM-Parameter

3.4.3.4 Trap

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

Abbildung 3-4-3-4

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 von NMS ein.
Port	Geben Sie den UDP-Port ein. Der Portbereich liegt zwischen 1 und 65535. Der Standardport ist 162.
Name	Geben Sie den Gruppennamen ein, wenn Sie SNMP v1/v2c verwenden; 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 3-4-3-4 Trap-Parameter

3.4.3.5 MIB

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

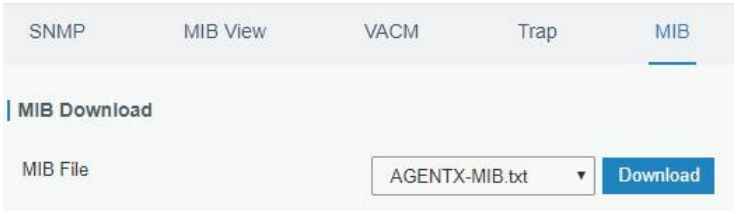


Abbildung 3-4-3-5

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

Tabelle 3-4-3-5 MIB-Download

3.4.4 Geräteverwaltung

Sie können das Gerät auf dieser Seite mit dem DeviceHub verbinden, um das Gateway zentral und remote zu verwalten. Weitere Informationen finden Sie im DeviceHub-Benutzerhandbuch.

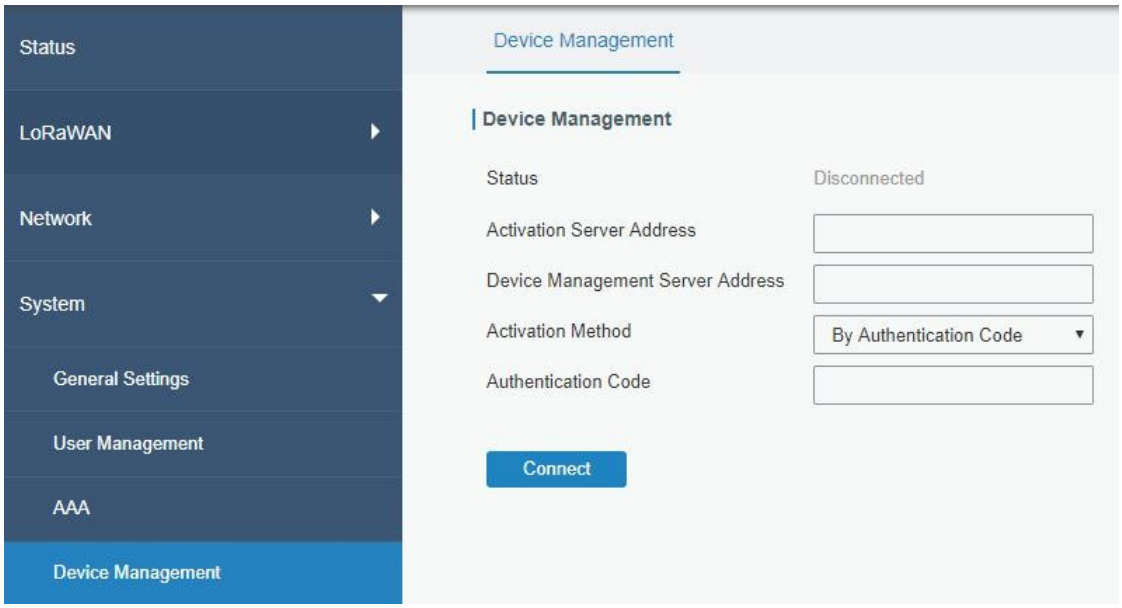


Abbildung 3-4-5-1

DeviceHub	
Element	**Beschreibung**
Status	Zeigt den Verbindungsstatus zwischen dem Gateway und dem DeviceHub anzeigen.
Getrennt	Klicken Sie auf diese Schaltfläche, um die Verbindung zwischen dem Gateway und dem DeviceHub zu trennen.
Aktivierungsserver Adresse	IP-Adresse oder Domäne des DeviceHub.
DeviceHub-Server 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 zu verbinden. Die 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	

Tabelle 3-4-5-1

3.4.5 Ereignisse

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

3.4.5.1 Ereignisse

Auf dieser Seite können Sie Alarmmeldungen anzeigen.

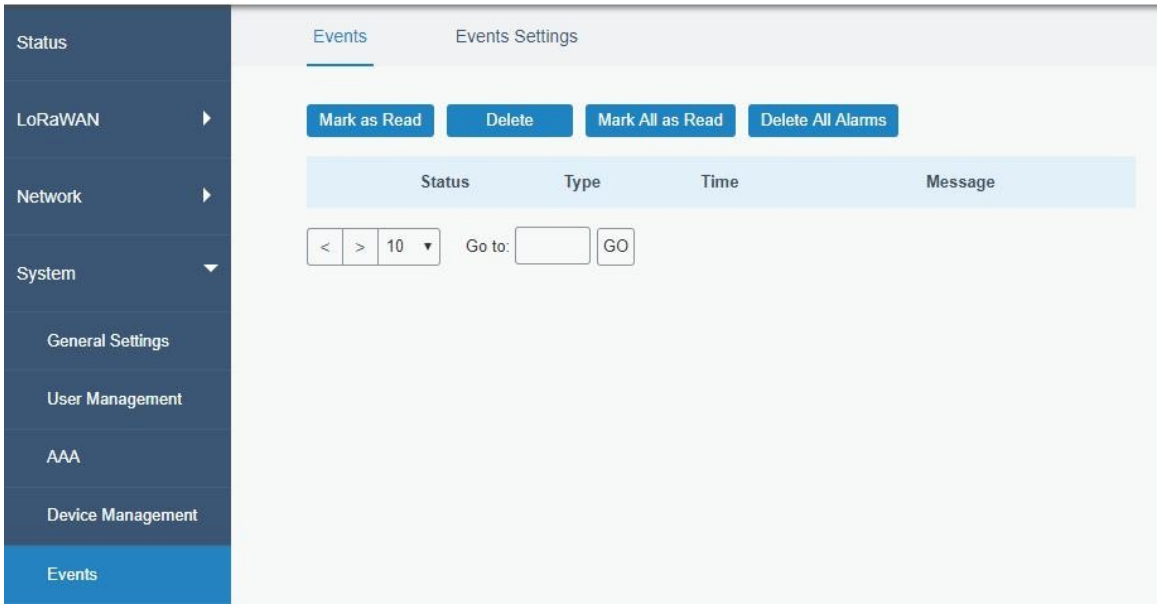


Abbildung 3-4-6-1

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, z. B. „Gelesen“ und „Ungelesen“.
Typ	Zeigt den Ereignistyp an, der alarmiert werden soll.
Zeit	Zeigen Sie die Alarmzeit an.
Meldung	Zeigt den Inhalt des Alarms an.

Tabelle 3-4-6-1 Ereignisparameter

3.4.5.2 Ereigniseinstellungen

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

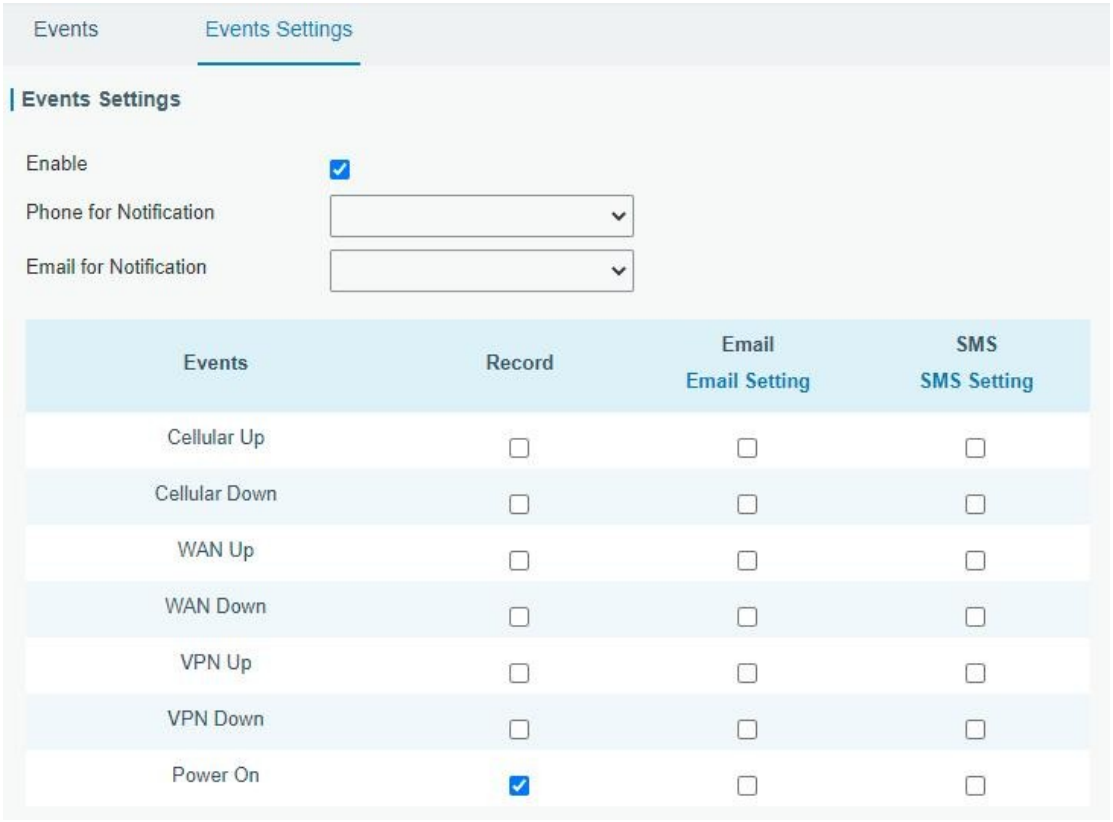


Abbildung 3-4-6-2

Ereigniseinstellungen	
Element	**Beschreibung**
Aktivieren	Aktivieren Sie diese Option, um die „Ereigniseinstellungen“ zu aktivieren.
Mobilfunkverbindung	Das Mobilfunknetz ist verbunden.
Mobilfunknetz ausgefallen	Mobilfunknetz ist getrennt.
WAN aktiv	Ethernet-Kabel ist mit dem WAN-Port verbunden.
WAN-Verbindung unterbrochen	Das Ethernet-Kabel ist nicht mit dem WAN-Port verbunden.
VPN aktiv	VPN ist verbunden.
VPN-Verbindung unterbrochen	VPN ist getrennt.
Strom eingeschaltet	Das Gateway wurde eingeschaltet.
Aufzeichnung	Der relevante Inhalt des Ereignisalarms wird auf der Seite „Ereignis“ aufgezeichnet aufgezeichnet, wenn diese Option aktiviert ist.
E-Mail	Der relevante Inhalt des Ereignisalarms wird per E-Mail versendet, wenn Diese Option ist aktiviert.
E-Mail-Einstellungen	Klicken Sie darauf, um zur Seite „E-Mail“ weitergeleitet zu werden, wo Sie 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 die Telefon-Gruppenliste konfigurieren können.
Telefon-Gruppenliste	Wählen Sie die Telefongruppe aus, die den SMS-Alarm empfangen soll.
E-Mail-Gruppenliste	Wählen Sie eine E-Mail-Gruppe aus, die E-Mail-Alarme empfangen soll.

Tabelle 3-4-6-2 Ereignisparameter

Verwandte Themen E-Mail-Einstellungen Telefoneinstellungen

3.5 Wartung

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

3.5.1 Tools

Zu den Tools zur Fehlerbehebung gehören Ping und Traceroute.

3.5.1.1 Ping

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

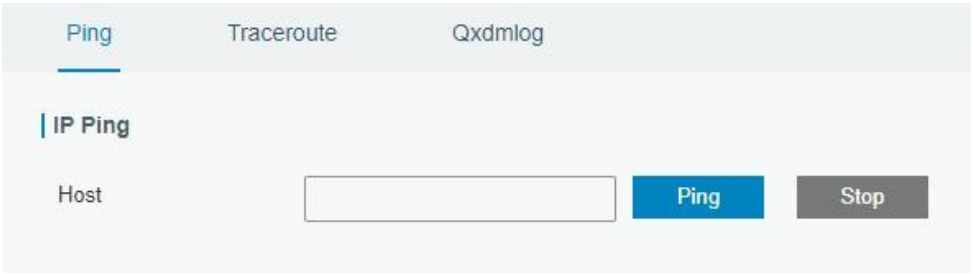


Abbildung 3-5-1-1

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

Tabelle 3-5-1-1 IP-Ping-Parameter

3.5.1.2 Traceroute

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

Abbildung 3-5-1-2

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

Tabelle 3-5-1-2 Traceroute-Parameter

3.5.1.3 Qxdmlog

In diesem Abschnitt können Diagnoseprotokolle über das QXDM-Tool erfasst werden.

Abbildung 3-5-1-3

3.5.2 Zeitplan

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

Abbildung 3-5-2-1

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

Tabelle 3-5-2-1 Zeitplanparameter

3.5.3 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.

3.5.3.1 Systemprotokoll

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

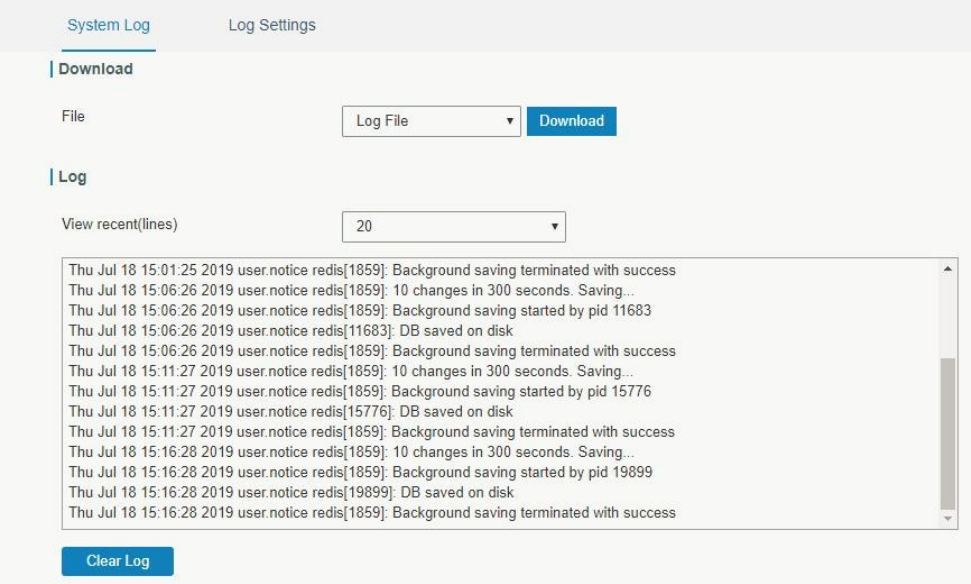


Abbildung 3-5-3-1

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 3-5-3-1 Systemprotokollparameter

3.5.3.2 Protokolleinstellungen

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

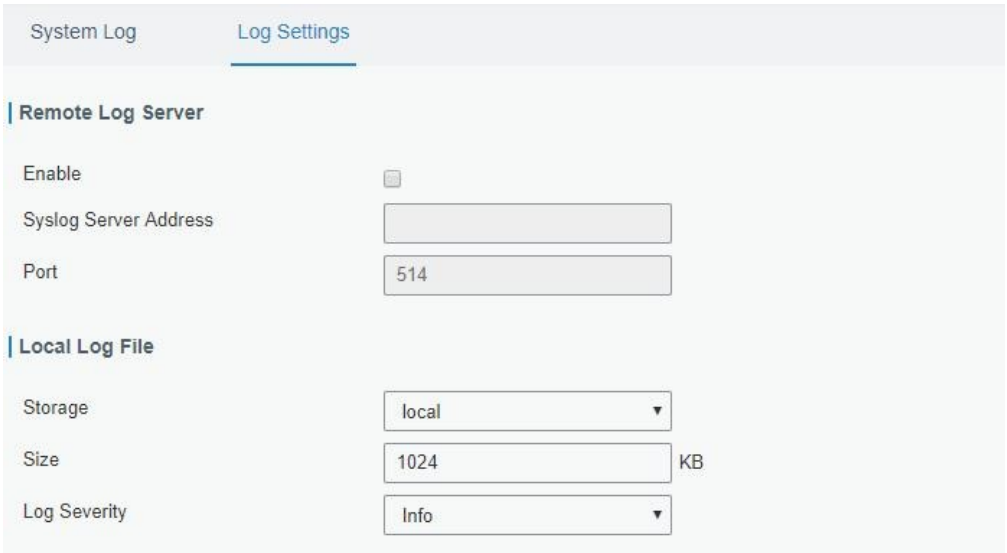


Abbildung 3-5-3-2

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 oder auf einer TF-Karte speichern.
Größe	Legen Sie die Größe der zu speichernden Protokolldatei fest.
Protokollschweregrad	Die Liste der Schweregrade entspricht dem Syslog-Protokoll.

Tabelle 3-5-3-2 Systemprotokollparameter

3.5.4 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 der Firmware-Aktualisierung sind keine Vorgänge auf der Webseite zulässig, da dies zu einer Unterbrechung der Aktualisierung oder sogar zu einem Ausfall des Geräts führen kann.

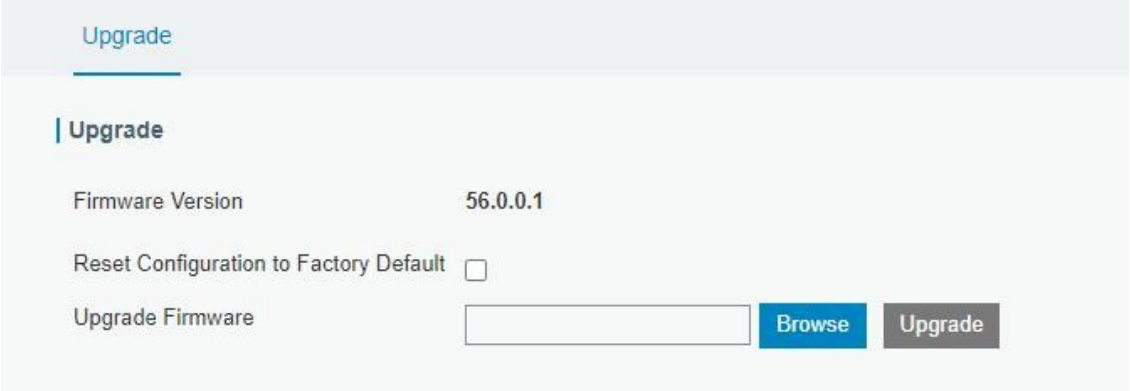


Abbildung 3-5-4-1

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 „Aktualisieren“, um die Firmware zu aktualisieren.

Tabelle 3-5-4-1 Upgrade-Parameter

Beispiel für die entsprechende Konfiguration

Firmware-Aktualisierung

3.5.5 Sichern und Wiederherstellen

In diesem Abschnitt wird erläutert, wie Sie eine 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.

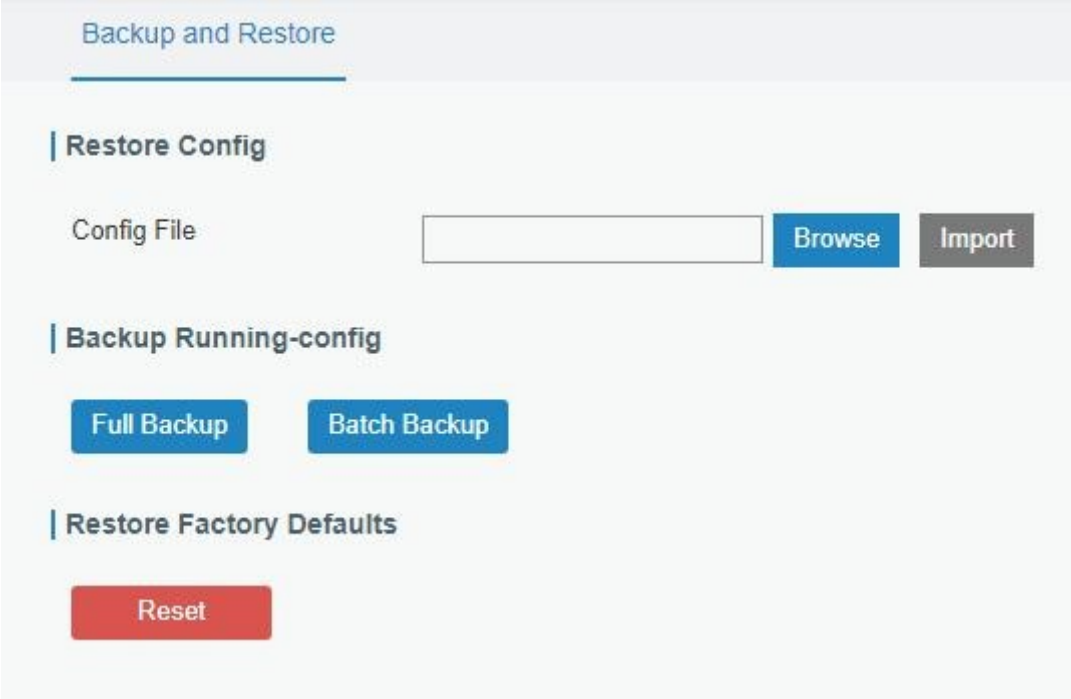


Abbildung 3-5-5-1

Sichern und Wiederherstellen	
Element	**Beschreibung**
Konfigurationsdatei	Klicken Sie auf die Schaltfläche „Durchsuchen“, um die Konfigurationsdatei auszuwählen, und klicken Sie dann auf „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 und des DeviceHub zu exportieren. 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 3-5-5-1 Parameter für Sicherung und Wiederherstellung

Beispiel für die entsprechende Konfiguration

Werkseinstellungen wiederherstellen

3.5.6 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.

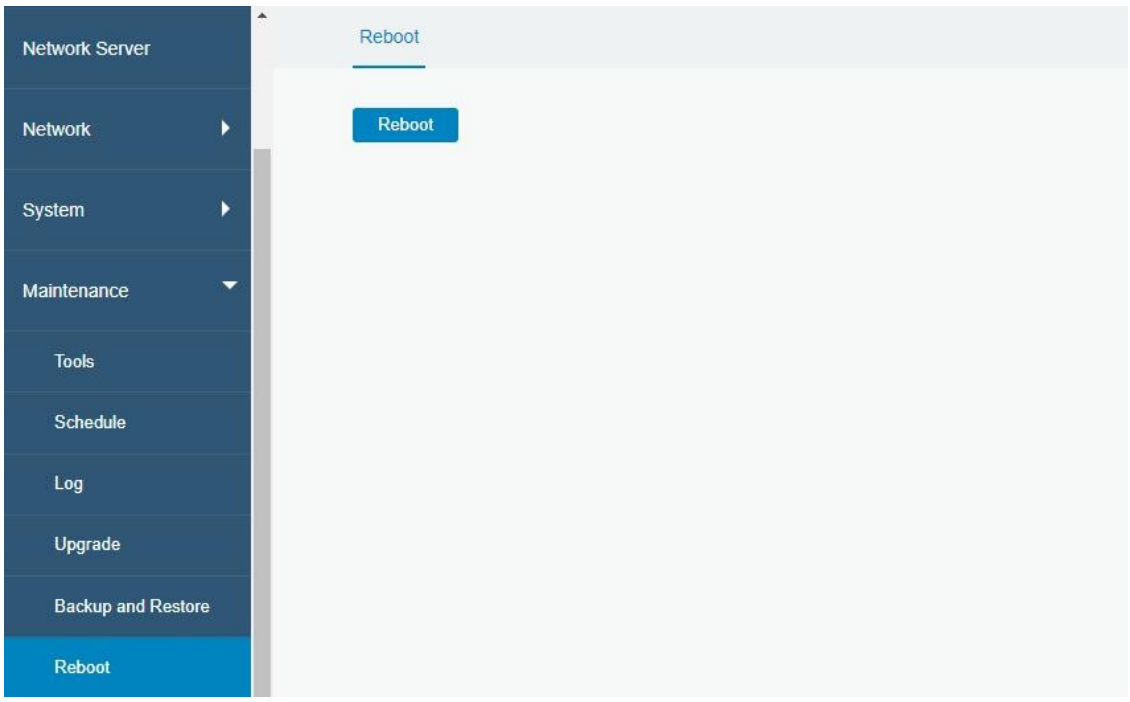


Abbildung 3-5-6-1

3.6 APP

3.6.1 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. Dazu werden insbesondere Leerzeichen zur Einrückung verwendet, um Codeblöcke abzugrenzen, anstatt geschweifte Klammern oder Schlüsselwörter. Die Syntax ermöglicht es Programmierern, 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 darstellen kann, diesen mit einer geeigneteren Sprache umschreiben und dann die erweiterte Klassenbibliothek kapseln, 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.

3.6.1.1 Python

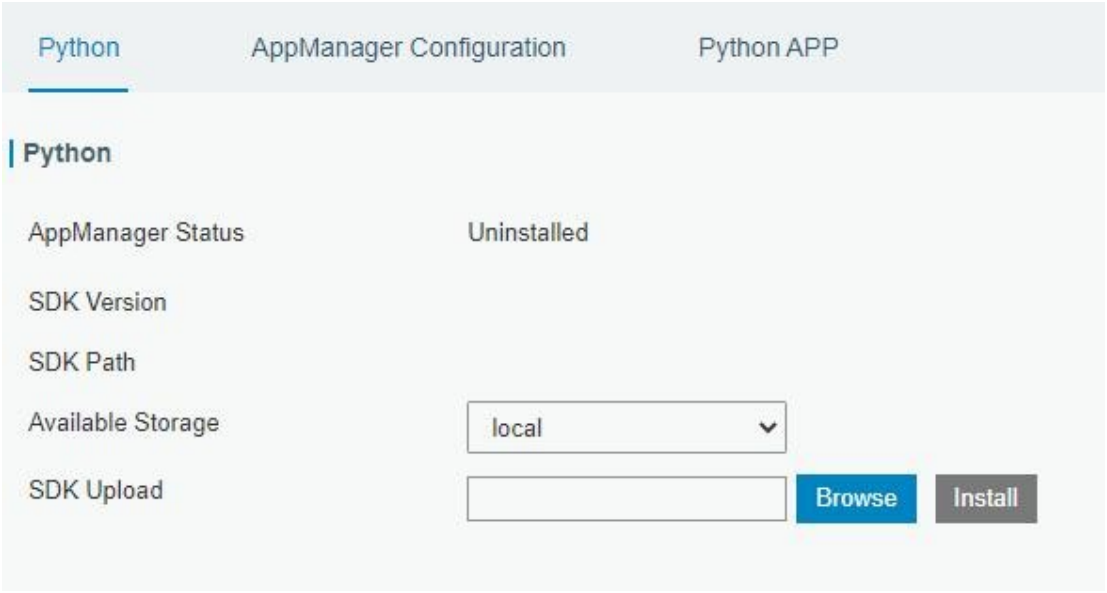


Abbildung 3-6-1-1

Python	
Element	**Beschreibung**
AppManager-Status	Zeigt den Ausführungsstatus von AppManager an, z. B. „Deinstalliert“, „Läuft“ oder „Beendet“.
SDK-Version	Zeige die Version des installierten SDK an.
SDK-Pfad	Zeigen Sie den Installationspfad des SDK an.
Verfügbarer Speicher	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 3-6-1-1 Python-Parameter

3.6.1.2 App Manager-Konfiguration

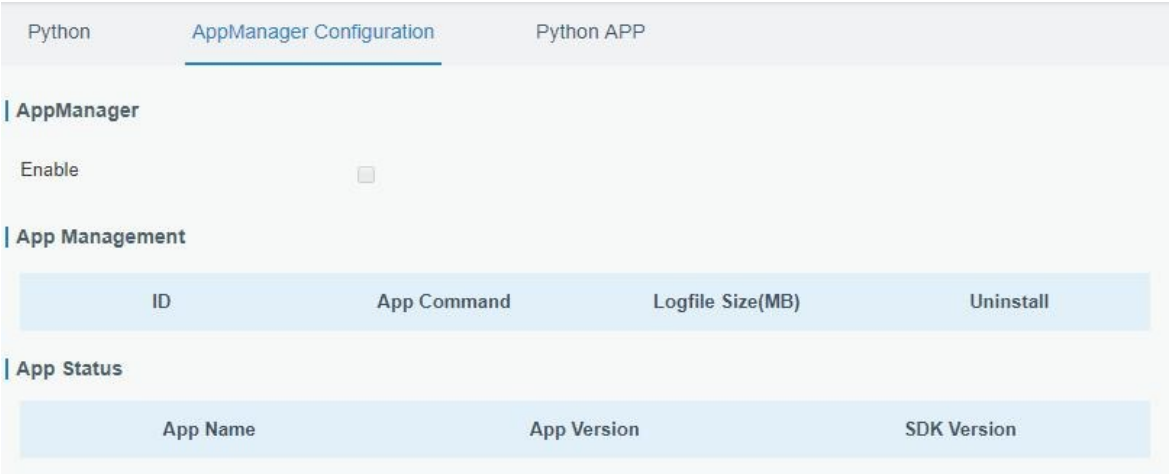


Abbildung 3-6-1-2

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	
ID	Zeigt die ID der importierten App an.
App-Befehl	Zeigt 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	Zeigen Sie die SDK-Version an, auf der die importierte App basiert.

Tabelle 3-6-1-2 APP-Manager-Parameter

3.6.1.3 Python-App

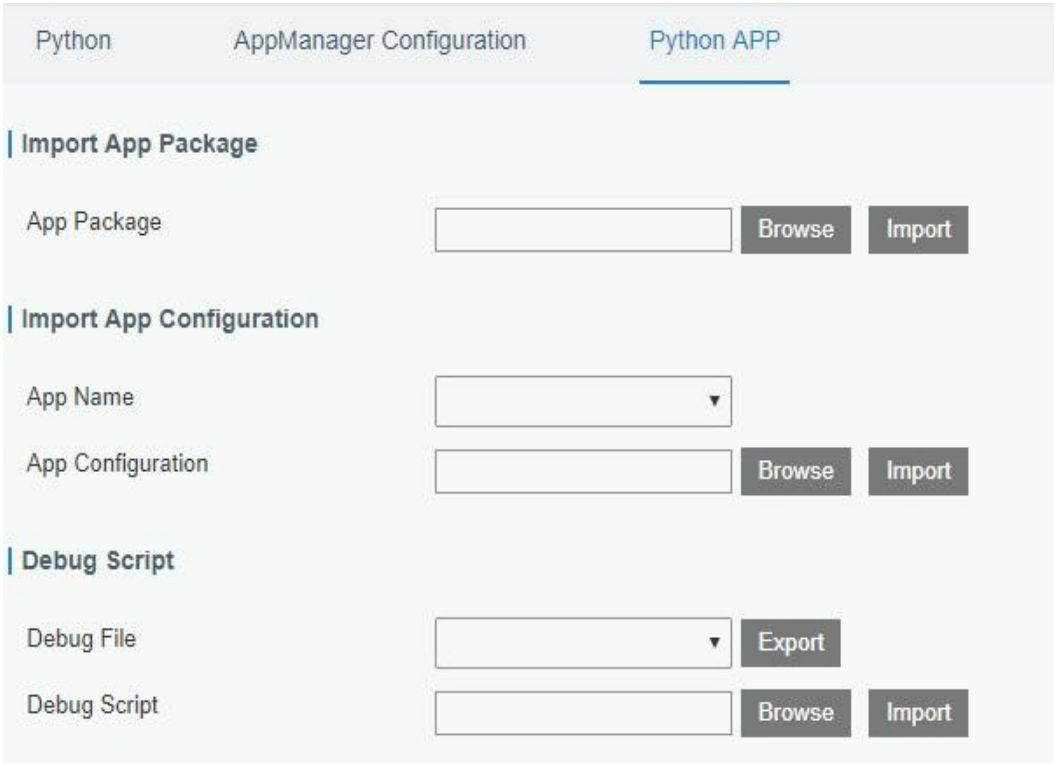


Abbildung 3-6-1-3

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 3-6-1-3 APP-Parameter

3.6.2 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. Neben den grundlegenden Knoten bieten Milesight-Gateways folgende benutzerdefinierte Knoten:

- LoRa-Eingang: Empfängt die LoRa-Daten. Bitte stellen Sie sicher, dass der Netzwerkservermodus aktiviert ist. , bevor Sie diesen Knoten verwenden
- LoRa-Ausgang: Senden Sie Downlinks an LoRaWAN®-Knoten
- Gerätefilter: Filtert die Daten eines oder mehrerer spezifischer LoRaWAN®-Knoten heraus
- Decoder: Dekodiert die Daten der Milesight LoRaWAN®Endknoten
- GW-Info: Überwachen Sie die Alarmmeldungen des Gateways. Stellen Sie sicher, dass die Ereigniserkennung unter „Allgemein -> Ereignisse -> Ereigniseinstellungen" aktiviert ist.
- E-Mail-Ausgabe: Senden von LoRa-Daten oder Gateway-Alarmen per E-Mail
- SMS-Eingabe: Empfang von SMS-Nachrichten. Dies funktioniert nur, wenn eine Mobilfunkverbindung besteht
- SMS-Ausgabe: SMS-Nachrichten senden. Dies funktioniert nur, wenn eine Mobilfunkverbindung besteht

3.6.2.1 Node-RED

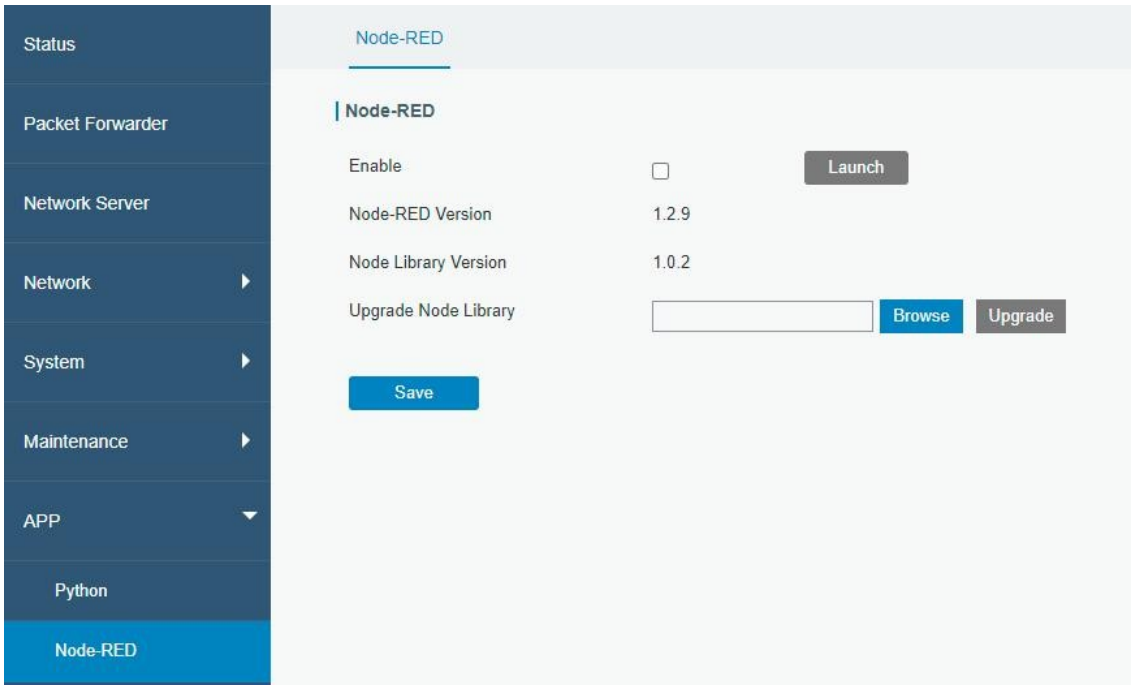


Abbildung 3-6-2-1

Node-RED	
Element	**Beschreibung**
Aktivieren	Aktivieren Sie Node-RED.
Starten	Klicken Sie hier, um die Web-GUI von Node-RED zu starten.
Node-RED-Version	Zeigen Sie 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.

Tabelle 3-6-2-1 Node-RED-Parameter

Beispiel für zugehörige Konfiguration

Node-RED

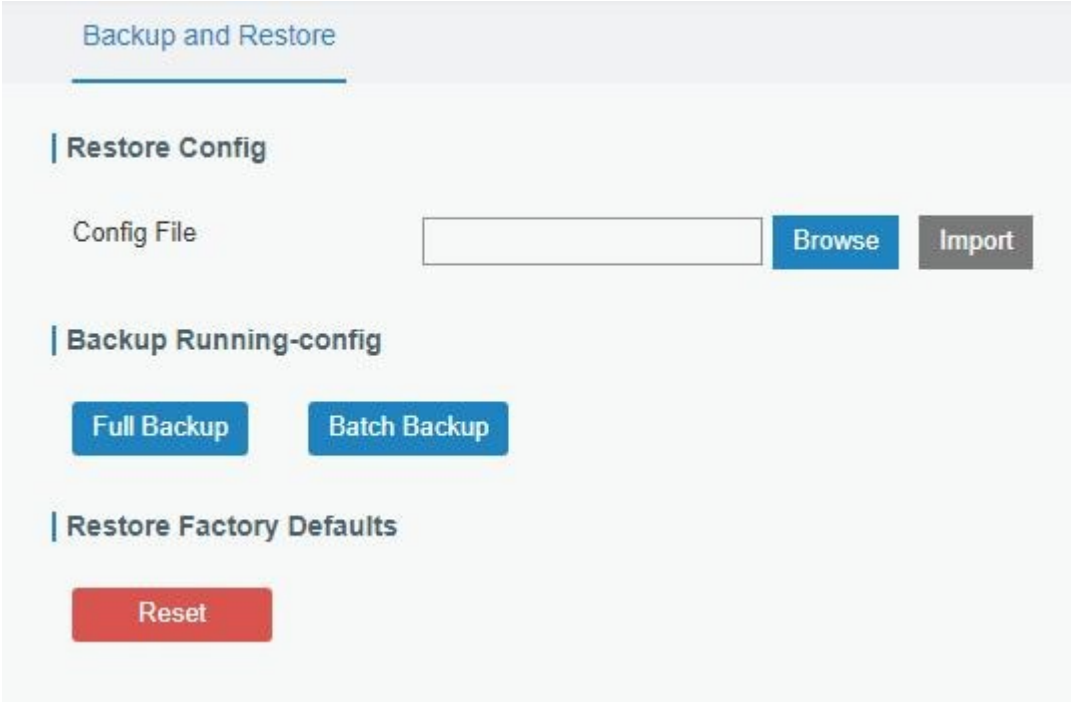
Kapitel 4 Anwendungsbeispiele

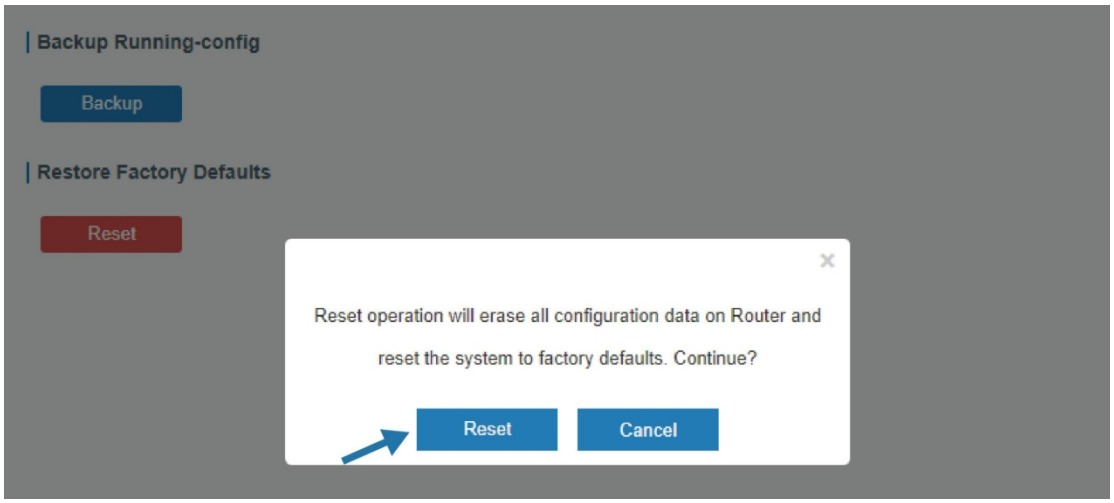
4.1 Werkseinstellungen wiederherstellen

4.1.1 Über die Webschnittstelle

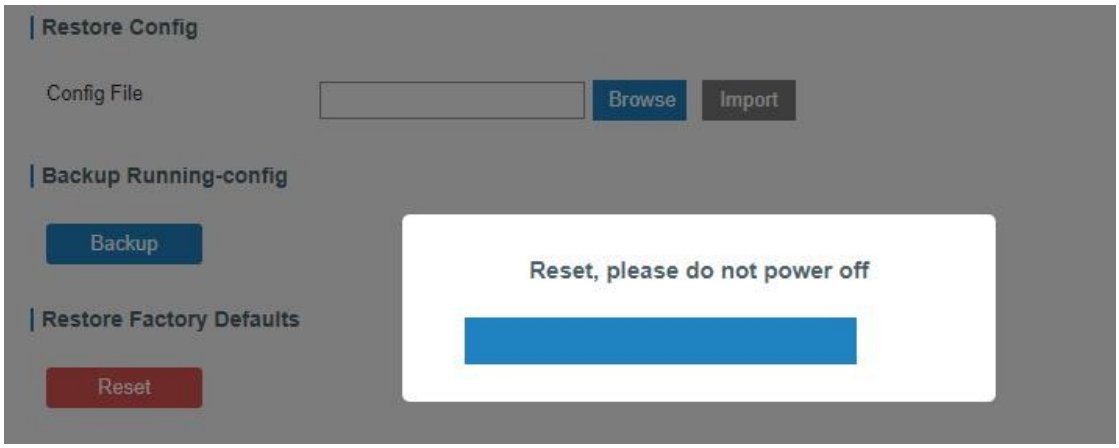
1. Melden Sie sich bei der Weboberfläche an und gehen Sie zu „Wartung > Sichern und Wiederherstellen".
2. Klicken Sie unter „Werkseinstellungen wiederherstellen" auf die Schaltfläche „Zurücksetzen".

Sie werden gefragt, ob Sie das Gerät auf die Werkseinstellungen zurücksetzen möchten. Klicken Sie dann auf die Schaltfläche „Zurücksetzen".





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



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

Verwandtes Thema

Werkseinstellungen wiederherstellen

4.1.2 Über die Hardware

Suchen Sie die Reset-Taste am Gateway und führen Sie je nach Status der STATUS-LED die entsprechenden Maßnahmen durch.

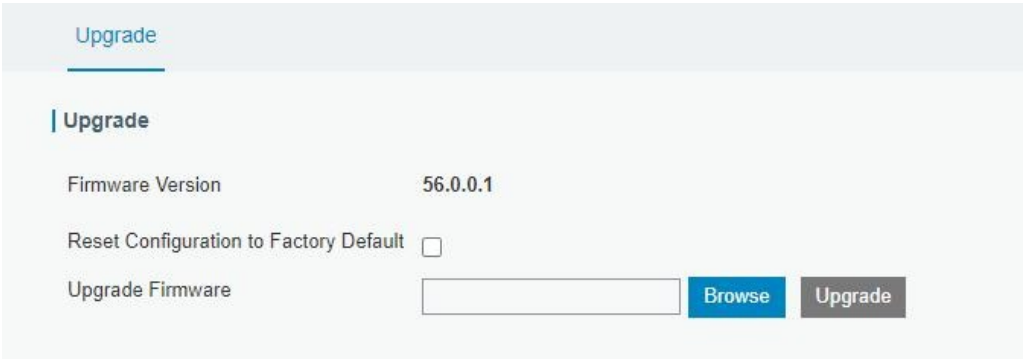
STATUS-LED	Aktion
Statisch grün	Halten Sie die Reset-Taste länger als 5 Sekunden gedrückt.
Statisch grün → Schnell blinkend	Lassen Sie die Taste los und warten Sie.
Aus → Statisch grün	Das Gateway wurde nun auf die Werkseinstellungen zurückgesetzt.

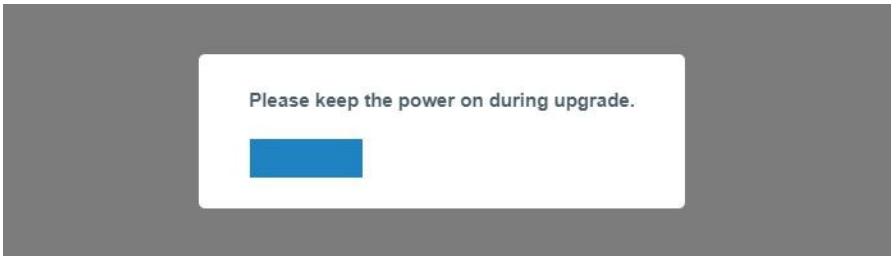
4.2 Firmware-Upgrade

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

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

1. Gehen Sie 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.



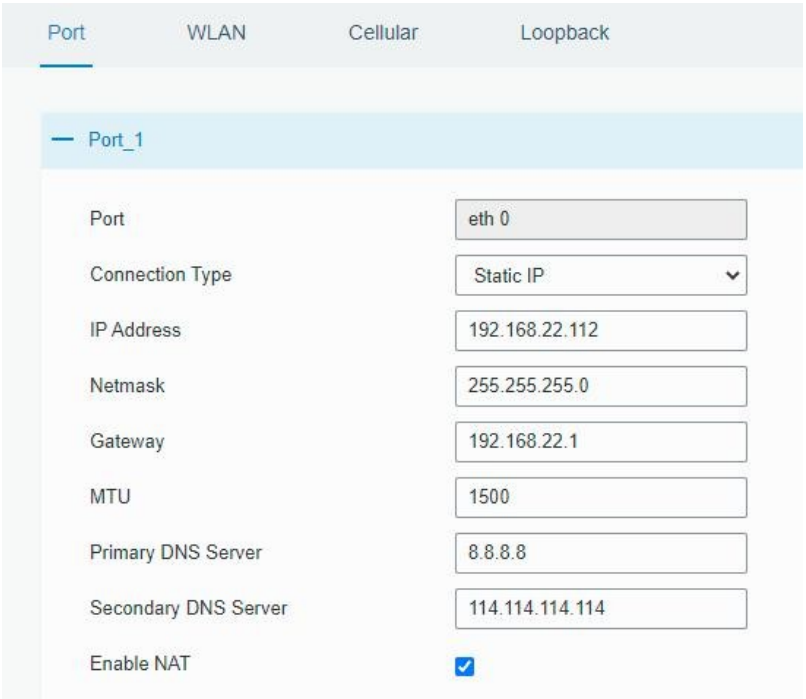


Verwandtes Thema

Upgrade

4.3 Ethernet-Verbindung

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



3. Verbinden Sie den Ethernet-Anschluss des Gateways mit Geräten wie Router oder Modem.
4. Melden Sie sich über die neu zugewiesene IP-Adresse bei der Web-GUI an und gehen Sie zu „Status -> Netzwerk“, um

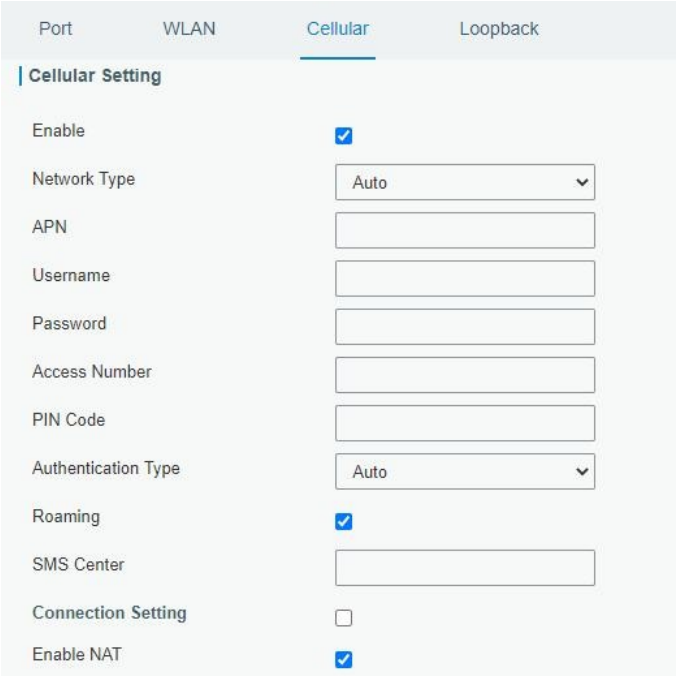
den Status des Ethernet-Anschlusses zu überprüfen.

Verwandtes Thema

Port-Einstellung

4.4 Mobilfunkverbindung

1. Gehen Sie zu „Netzwerk > Schnittstelle > Mobilfunk > Mobilfunkeinstellungen“ und konfigurieren Sie die Mobilfunkdaten.
2. Wählen Sie den entsprechenden Netzwerktyp aus.



Klicken Sie auf „Speichern“ und „Übernehmen“, damit die Konfiguration wirksam wird.

3. Überprüfen Sie den Status der Mobilfunkverbindung über die WEB-GUI des Gateways.

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

4. Überprüfen Sie mit dem Browser Ihres PCs, ob das Netzwerk ordnungsgemäß funktioniert.

Öffnen Sie Ihren bevorzugten Browser auf dem PC, geben Sie eine beliebige verfügbare Webadresse in die Adressleiste ein und prüfen Sie, ob Sie über das UG56 auf das Internet zugreifen können.

Verwandtes Thema

Mobilfunk-Einstellungen

Mobilfunk-Status

4.5 Beispiel für eine WLAN-Anwendung

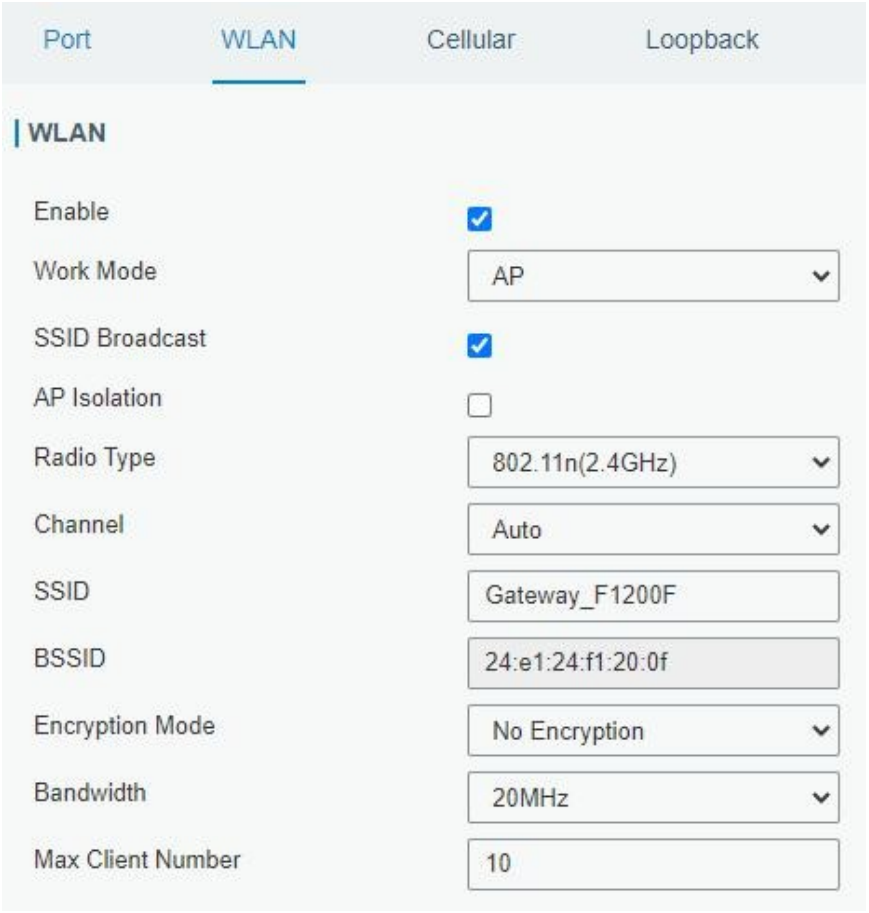
4.5.1 AP-Modus

Anwendungsbeispiel

Konfigurieren Sie das UG56 als AP, um Verbindungen von Benutzern oder Geräten zu ermöglichen.

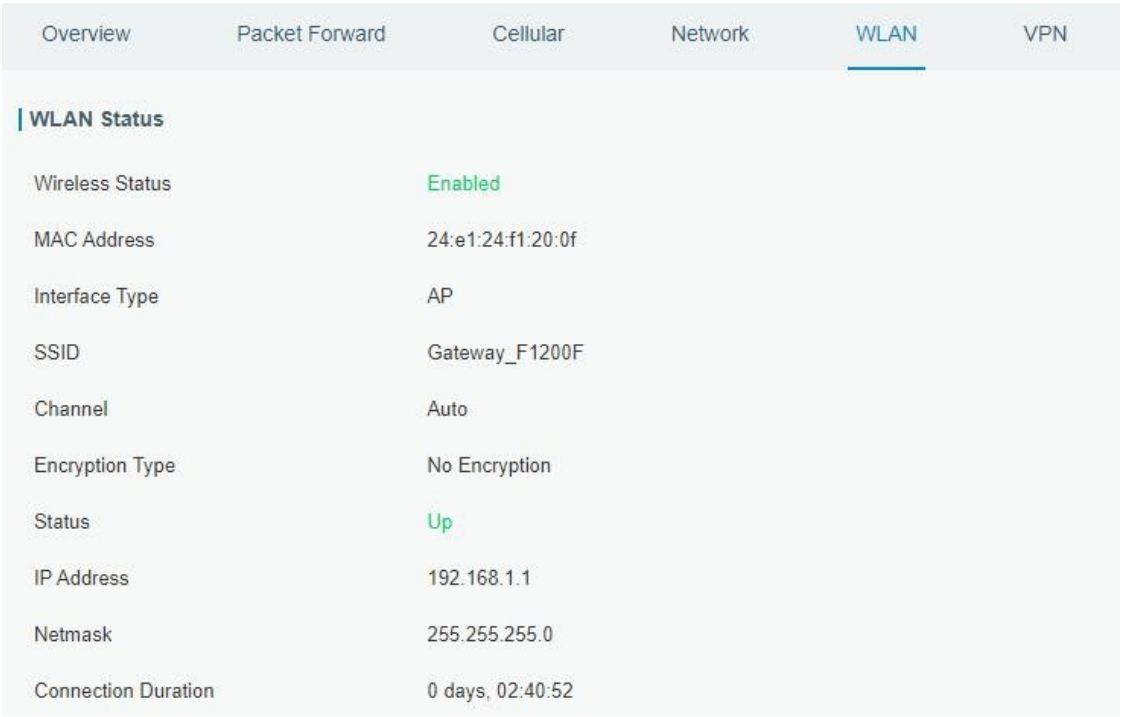
Konfigurationsschritte

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.

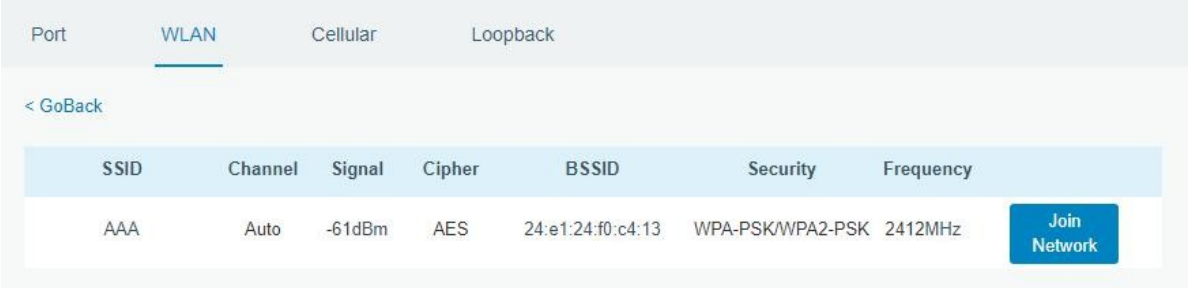


4.5.2 Anwendungsbeispiel für den Client-Modus

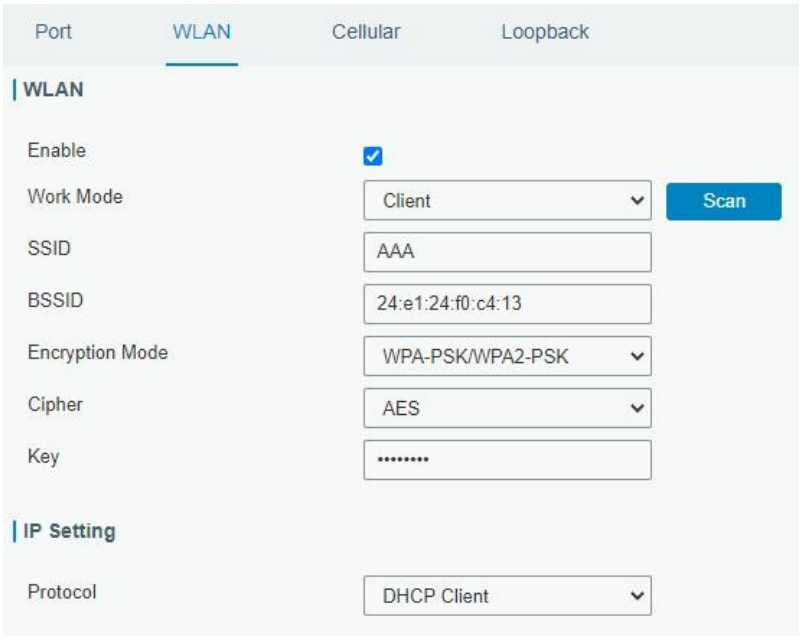
Konfigurieren Sie UG56 als WLAN-Client, um eine Verbindung zu einem Zugangspunkt herzustellen und Internetzugang zu erhalten.

Konfigurationsschritte

1. Gehen Sie zu „Netzwerk > Schnittstelle > WLAN“ und klicken Sie auf „Scannen“, um nach einem WLAN-Zugangspunkt zu suchen.

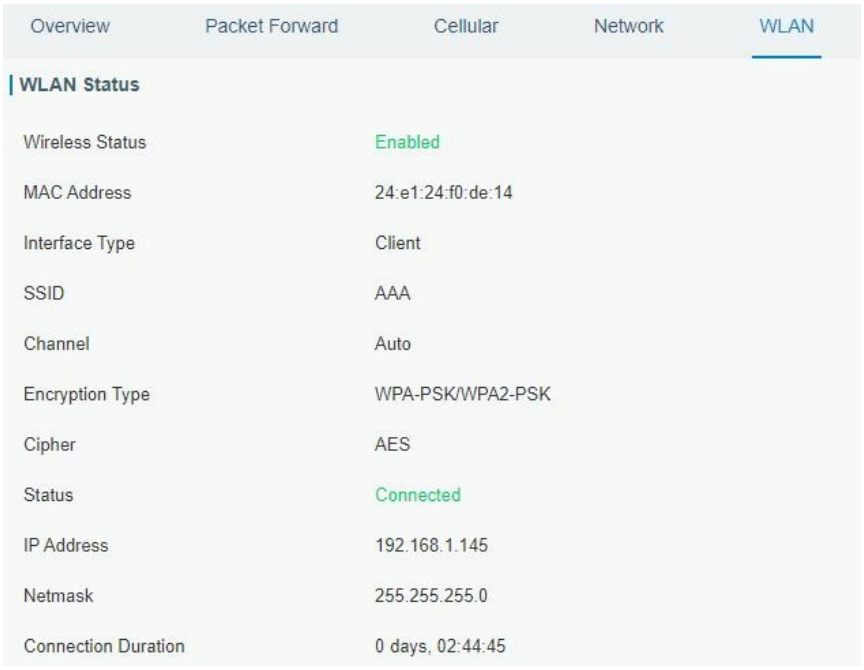


2. Wählen Sie einen Zugangspunkt aus und klicken Sie auf „Mit Netzwerk verbinden“. Geben Sie dann das Passwort des Zugangspunkts ein.



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

3. Gehen Sie zu „Status > WLAN“, um den Verbindungsstatus des Clients zu überprüfen.



Verwandtes

Thema WLAN-

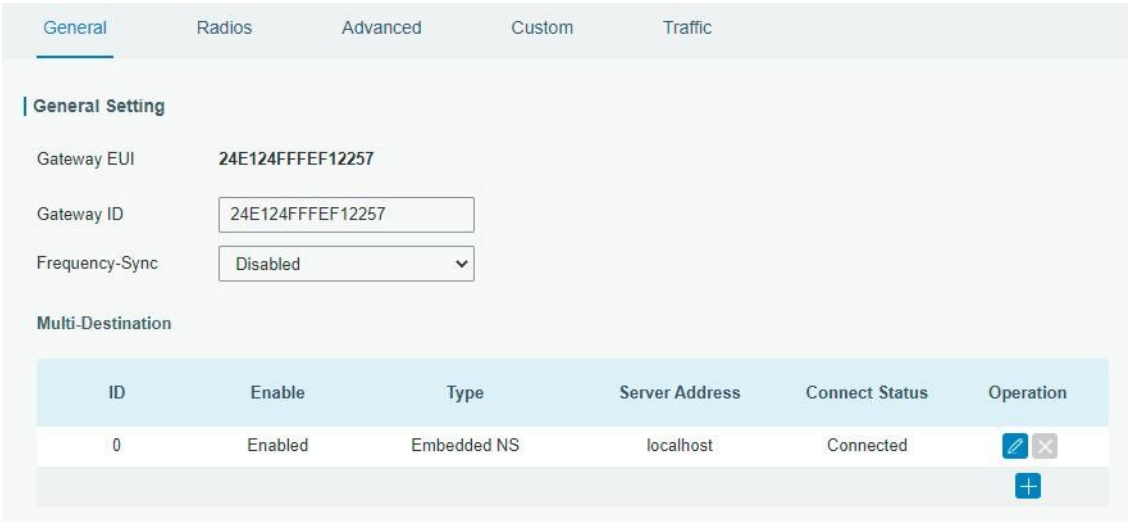
Einstellungen

WLAN-Status

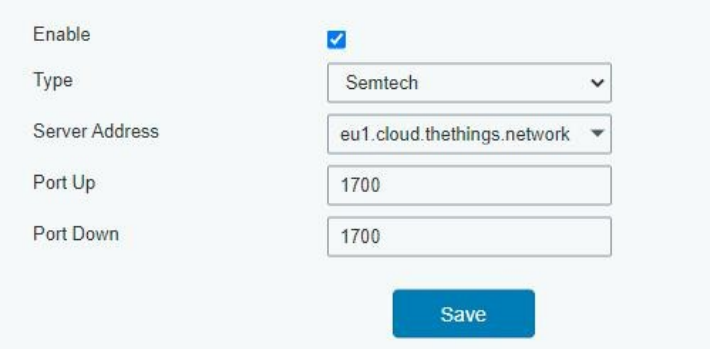
4.6 Konfiguration des Paketweiterleiters

Das UG56-Gateway verfügt über mehrere Paketweiterleiter, darunter Semtech Basic Station, Chirpstack-Generic MQTT Broker usw. Vergewissern Sie sich vor dem Herstellen einer Verbindung, dass das Gateway mit dem Netzwerk verbunden ist.

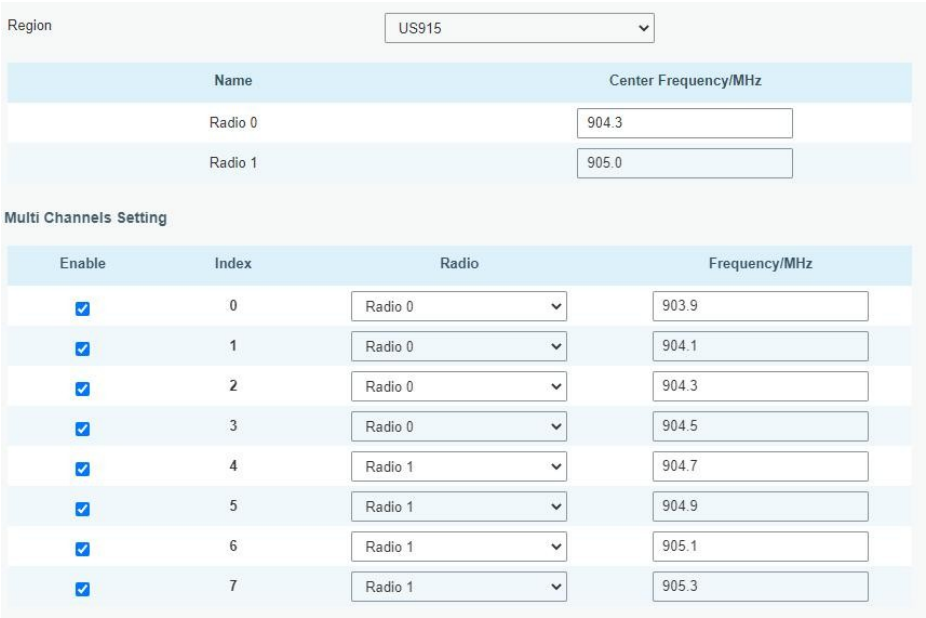
1. Gehen Sie zu „Packet Forwarder“ > „General“.



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

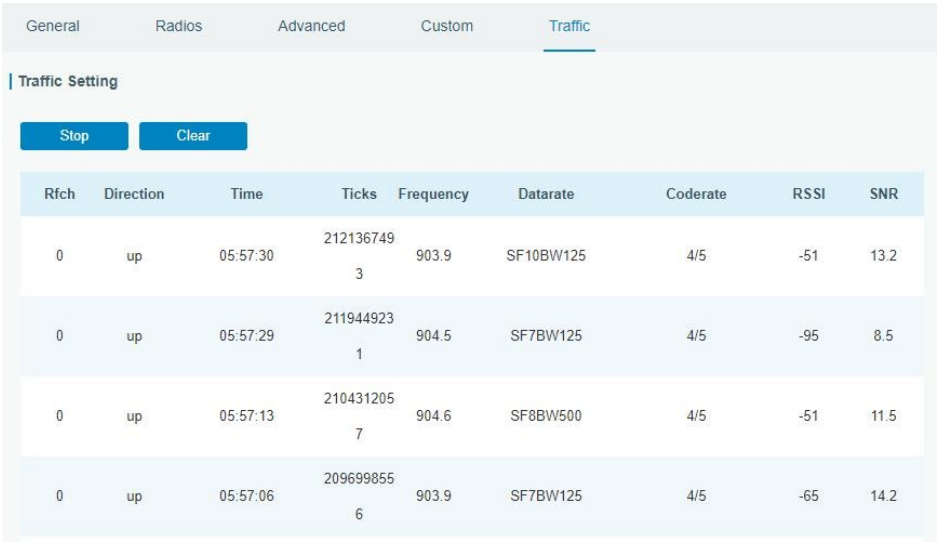


3. Gehen Sie zur Seite „Packet Forwarder -> Radio“, um den Antennentyp, die Mittenfrequenz und die Kanäle zu konfigurieren. Die Kanäle des Gateways und des Netzwerkservers müssen identisch sein.



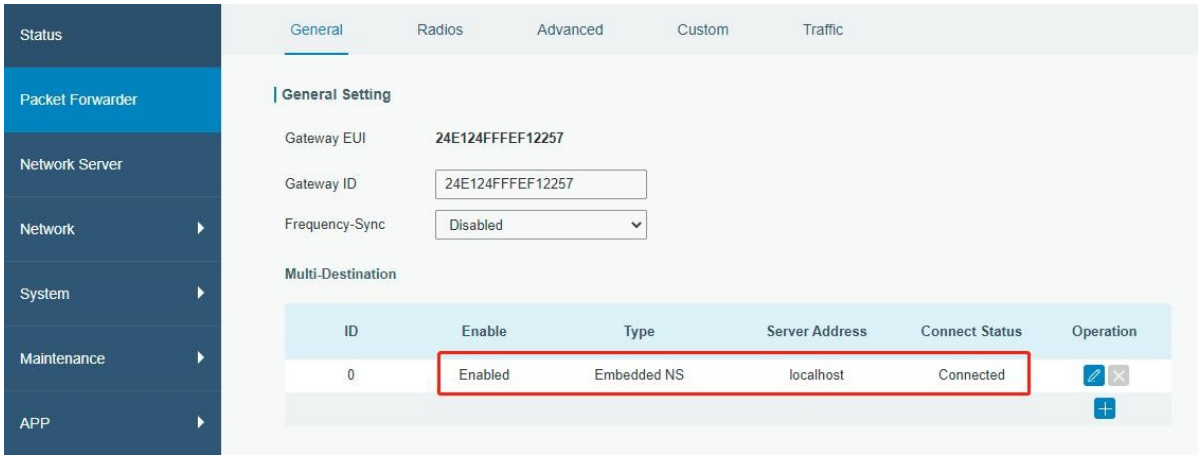
4. Fügen Sie das Gateway auf der Netzwerk-Server-Seite hinzu. Weitere Informationen zur Netzwerk-Server-Verbindung finden Sie im Milesight IoT Support-Portal.

5. Gehen Sie zur Seite „Traffic“, um die Datenkommunikation des UG56 anzuzeigen.

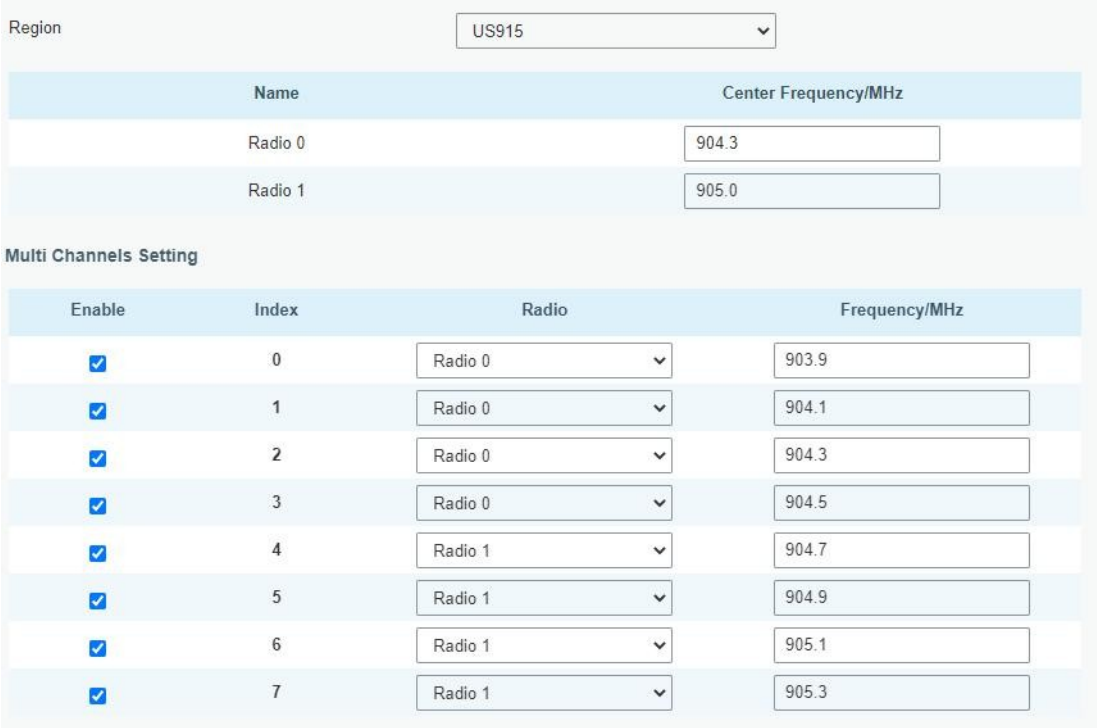


4.7 Verbinden Sie sich mit der Milesight IoT Cloud.

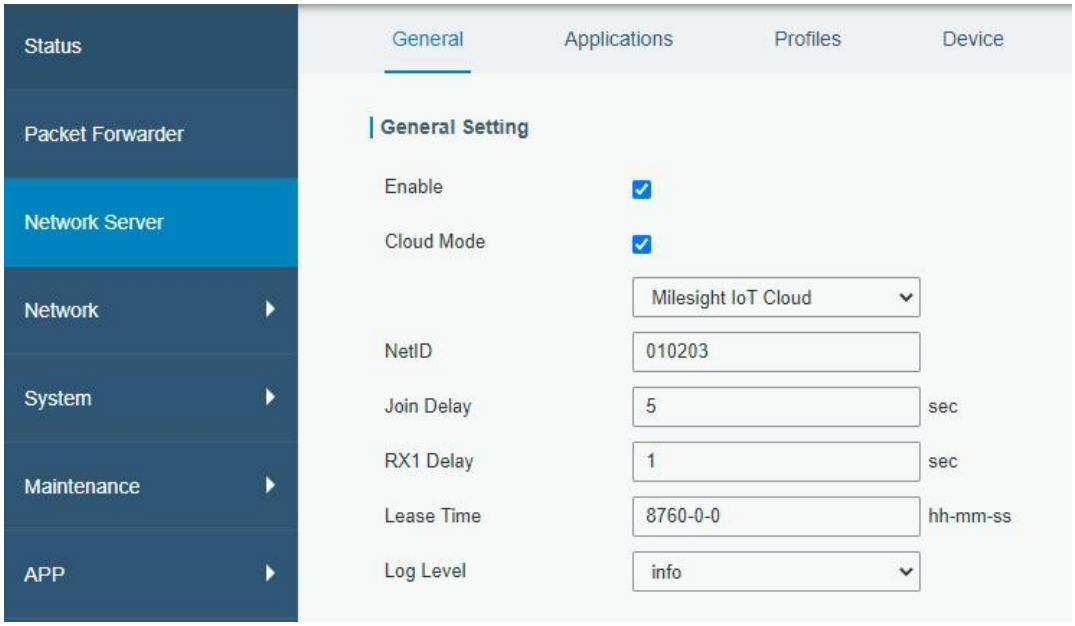
1. Gehen Sie zur Seite „Packet Forwarder->General“, um den eingebetteten Netzwerkserver zu aktivieren.



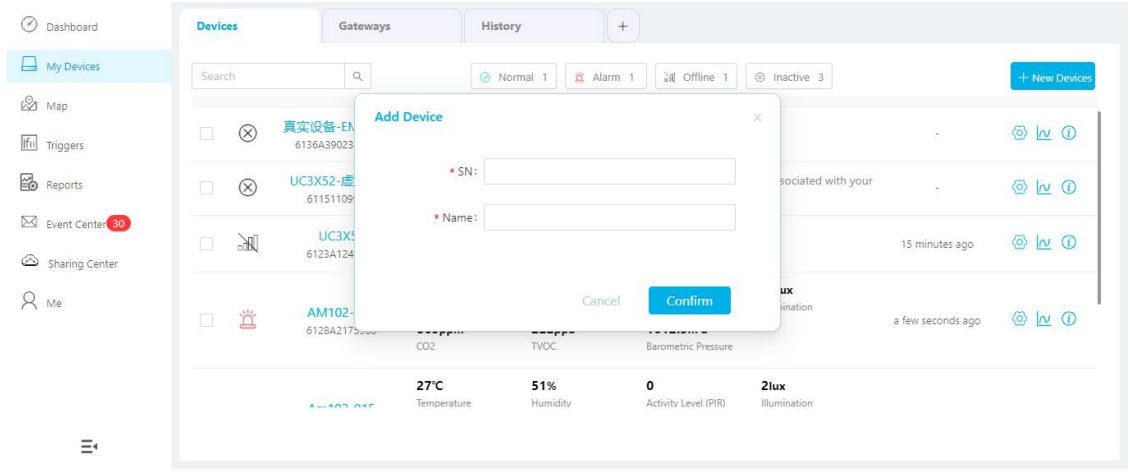
2. Gehen Sie zur Seite „Packet Forwarder->Radio“, um den Antennentyp, die Mittenfrequenz und die Kanäle auszuwählen. Die Kanäle des Gateways und der Knoten müssen identisch sein.



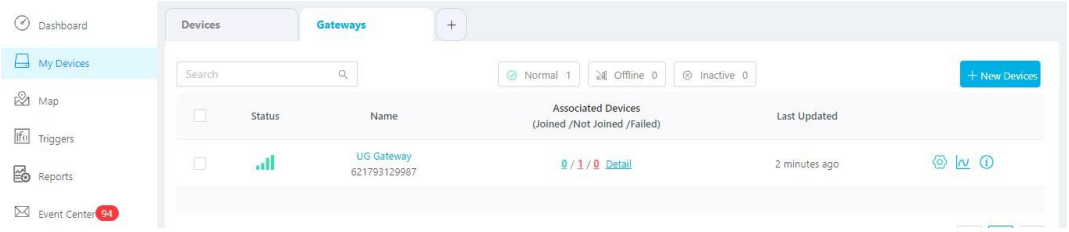
3. Gehen Sie zur Seite „Netzwerkserver“ → „Allgemein“, um den Netzwerkserver und den „Cloud-Modus“ zu aktivieren, und wählen Sie dann „Milesight IoT Cloud“.



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 Menü „Gateways“ hinzugefügt.



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

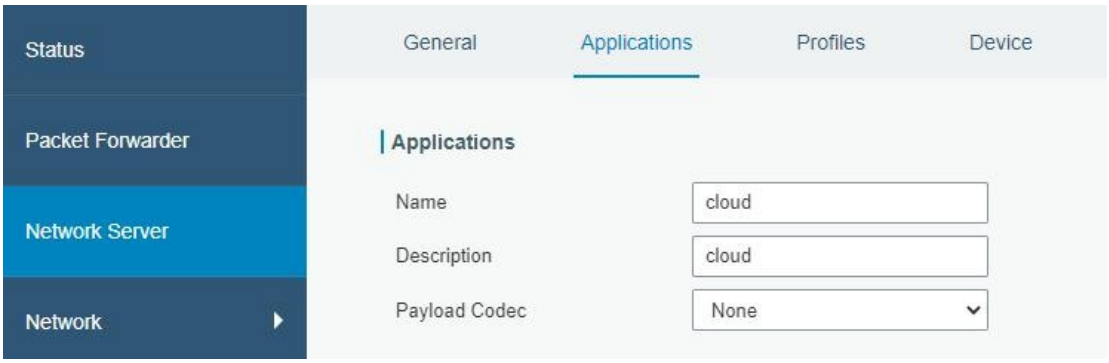


4.8 Anwendungskonfiguration

Auf dieser Seite können Sie eine neue Anwendung erstellen, die hauptsächlich dazu dient, die Methode zur Dekodierung der vom Endgerät gesendeten Daten zu definieren und das Datenübertragungsprotokoll für die Übertragung der Daten an eine andere Serveradresse auszuwählen. Die Daten werden unter Verwendung des MQTT-, HTTP- oder HTTPS-Protokolls an Ihre benutzerdefinierte Serveradresse gesendet.

1. Gehen Sie zu „Netzwerkserver“ > „Anwendung“.

2. Klicken Sie auf „  “ , um die Konfigurationsseite aufzurufen, die wie in der folgenden Abbildung dargestellt angezeigt wird:

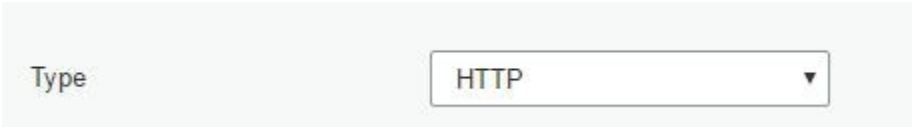


3. Klicken Sie auf „Save“, um diese Anwendung zu erstellen.

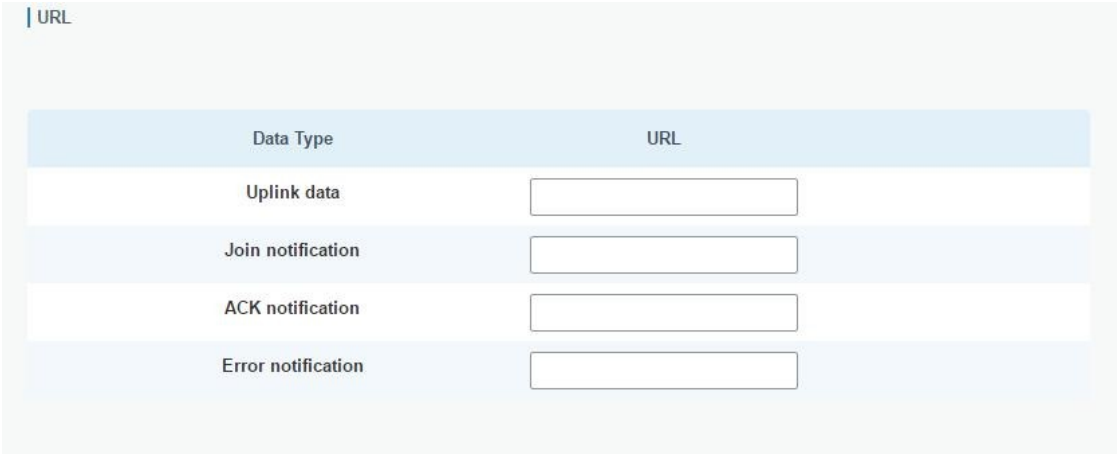
4. Klicken Sie auf „  “ , um einen Datentransmissionstyp hinzuzufügen.

HTTP oder HTTPS:

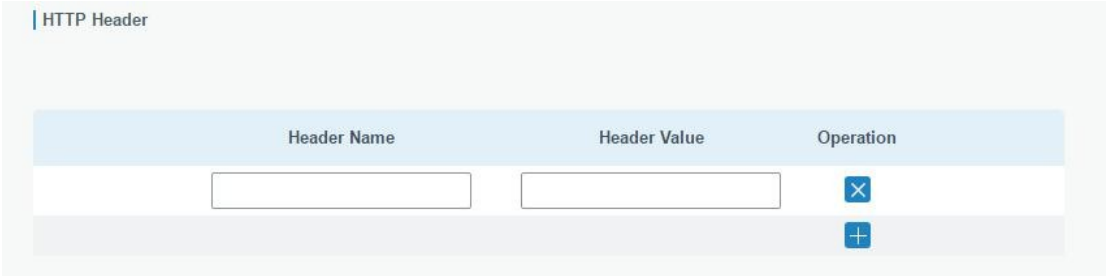
Schritt 1: Wählen Sie HTTP oder HTTPS als Übertragungsprotokoll aus.



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



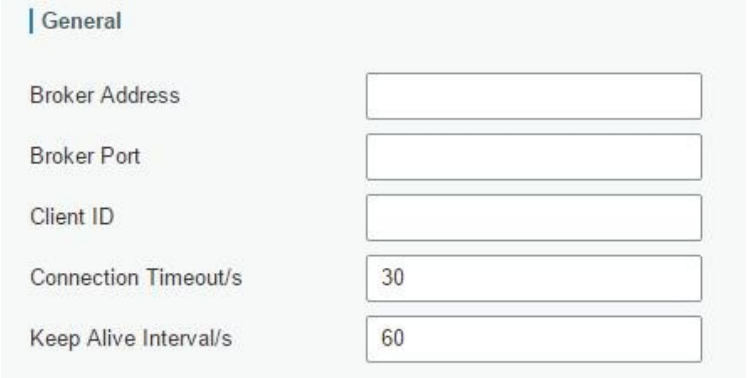
Geben Sie den Headernamen und den Headerwert ein, wenn beim Zugriff auf den HTTP(s)-Server Benutzeranmeldedaten erforderlich sind.



MQTT：

Schritt 1: Wählen Sie als Übertragungsprotokoll MQTT aus.

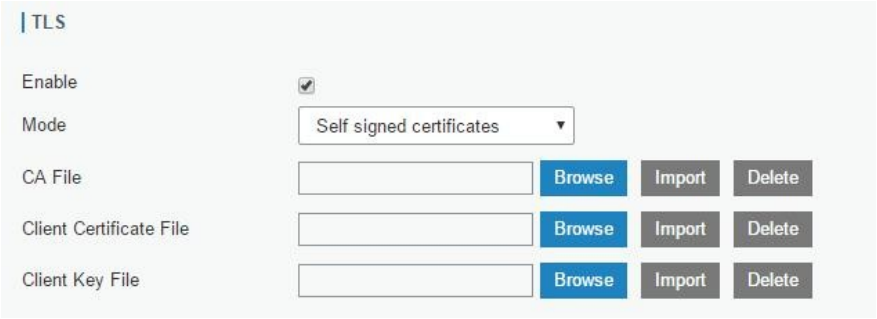
Schritt 2: Geben Sie die allgemeinen Einstellungen für den MQTT-Broker ein.



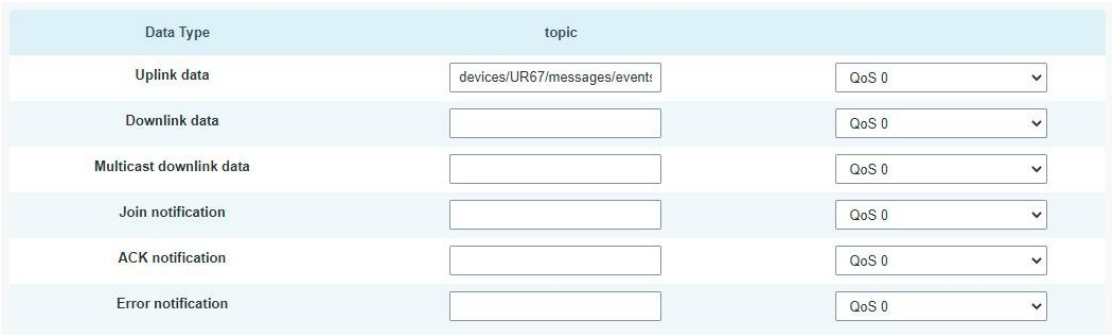
Schritt 3: Wählen Sie die vom Server geforderte Authentifizierungsmethode aus.

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

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

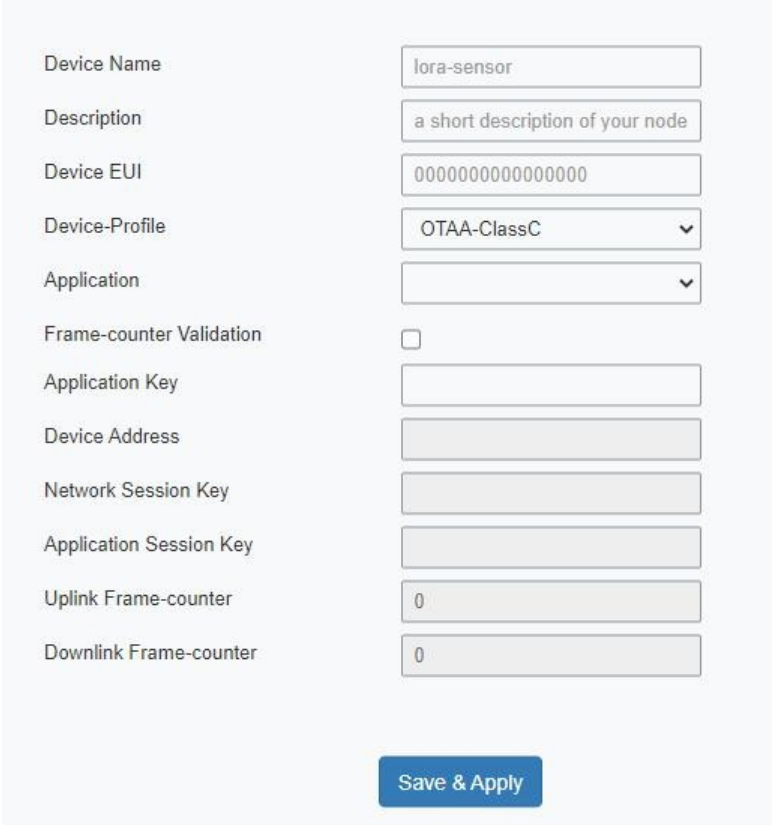


Schritt 4: Geben Sie das Thema für den Datenempfang ein und wählen Sie die QoS aus.



4.9 Gerätekonfiguration

Gehen Sie zur Seite „Gerät“ und klicken Sie auf „Hinzufügen“, um LoRaWAN®-Knotengeräte hinzuzufügen. Wählen Sie bitte das richtige Geräteprofil entsprechend dem Gerätetyp aus.



Sie können auch auf „Bulk Import“ klicken, wenn Sie viele Knoten auf einmal hinzufügen möchten.

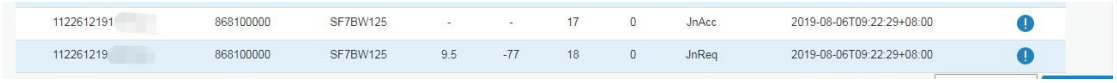
Klicken Sie auf „Vorlage herunterladen“, um die Vorlagendatei herunterzuladen und Geräteinformationen zu dieser Datei hinzuzufügen. Die Anwendung und das Geräteprofil sollten mit denen übereinstimmen, die Sie auf der Webseite erstellt haben.

	A	B	C	D	E	F	G	H	I
1	name	description	deveui	application	deviceprofile	appkey	devaddr	appskey	nwkskey
2	24e1242191323266		24e1242191323266	cloud	ClassC-OTAA	112233445566778899aa112233445566			
3									
4									
5									

Importieren Sie diese Datei, um mehrere Geräte gleichzeitig hinzuzufügen.

4.10 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 wurde.



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.

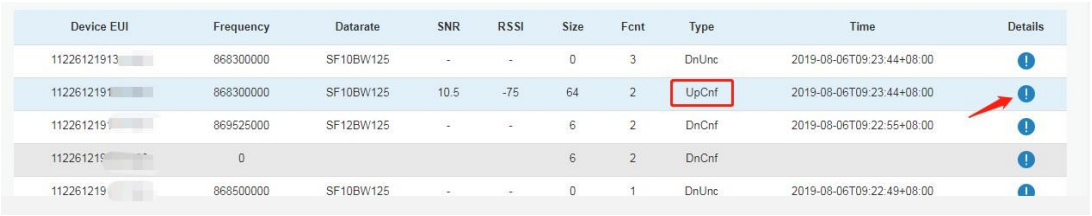
3. Klicken Sie auf „Senden“.

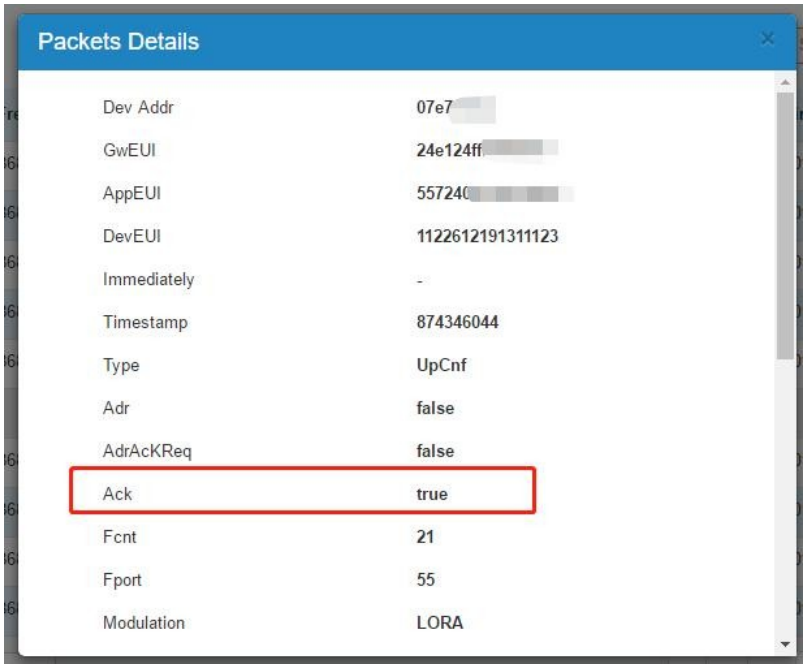
4. Überprüfen Sie das Paket in der Netzwerkserverliste, um sicherzustellen, dass das Gerät diese Nachricht erfolgreich empfangen hat. Es wird empfohlen, „Bestätigt“ zu aktivieren. Die Multicast-Funktion unterstützt keine bestätigten Downlinks.

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) und wenn die Farbe des Pakets grau ist, bedeutet dies, dass das Paket derzeit nicht übertragen werden kann, da sich mindestens eine Nachricht in der Warteschlange befindet. Wenn der Paketeintrag weiß ist, bedeutet dies, dass das Paket erfolgreich zugestellt wurde.

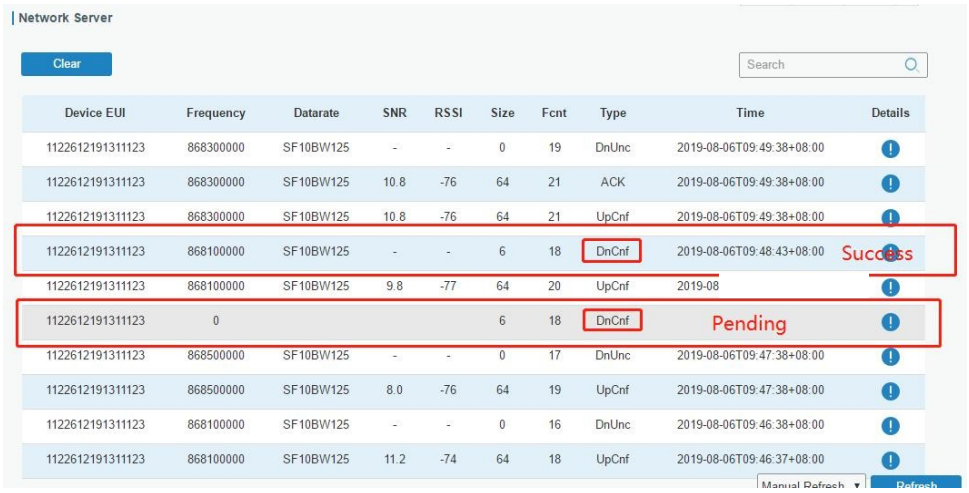
Wenn das Gerät dieses bestätigte Downlink-Paket empfängt, antwortet es bei der nächsten Zustellung mit „ACK“.

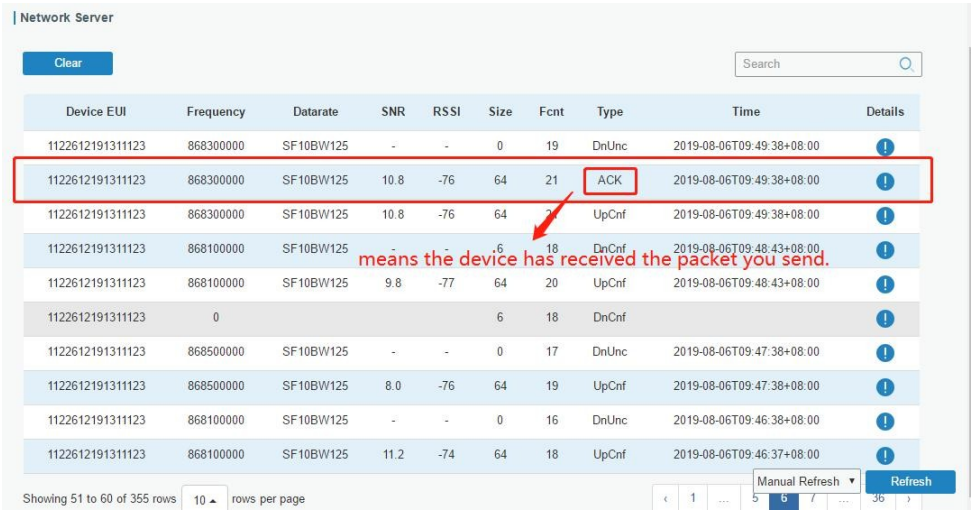




„Ack“ bedeutet „wahr“, d. h., das Gerät hat dieses Paket empfangen.

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

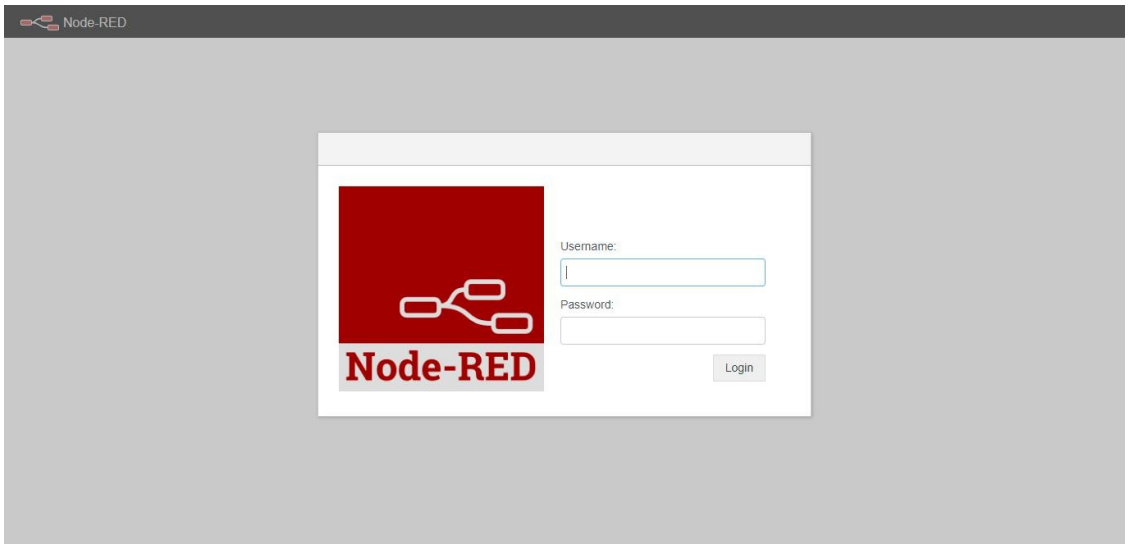
Pakete

4.11 Node-RED

4.11.1 Starten Sie Node-RED

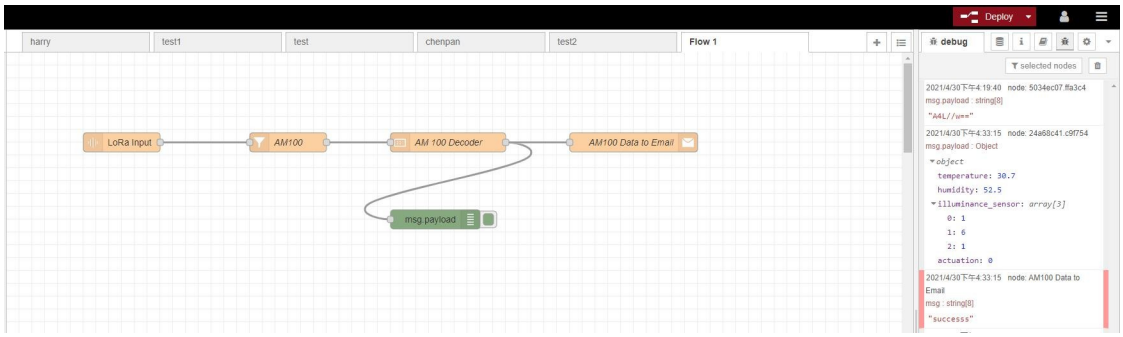
1. Gehen Sie zu „App > Node-RED“, um die Node-RED-Funktion zu aktivieren.

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



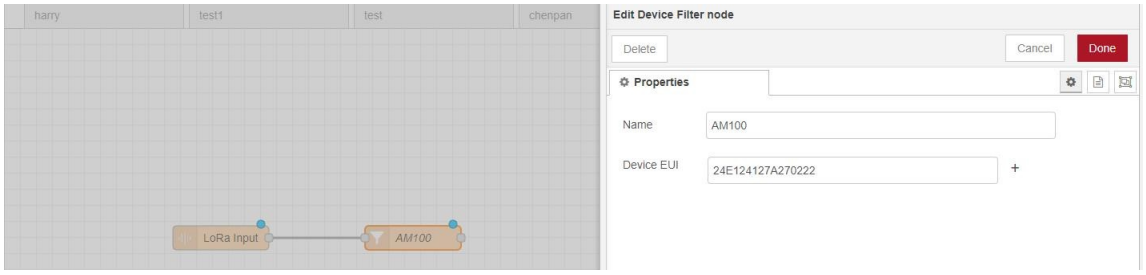
4.11.2 Beispiel für die Anwendung „Daten per E-Mail senden“

Senden Sie AM104-Gerätedaten per E-Mail.

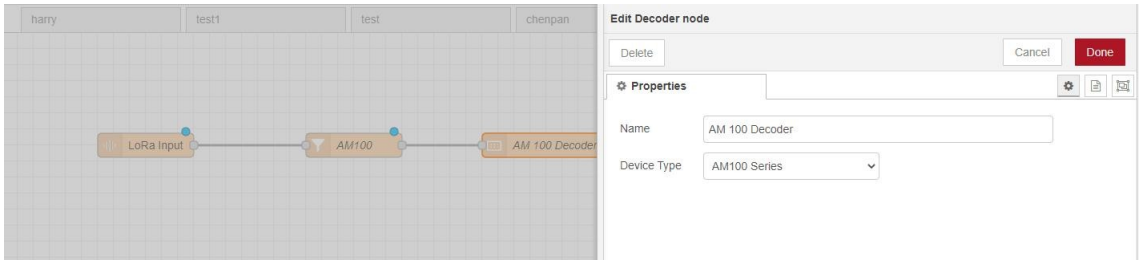


Konfigurationsschritte

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 Input“-Knoten einen „Device Filter“-Knoten hinzu und geben Sie die EUI des Geräts ein.



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

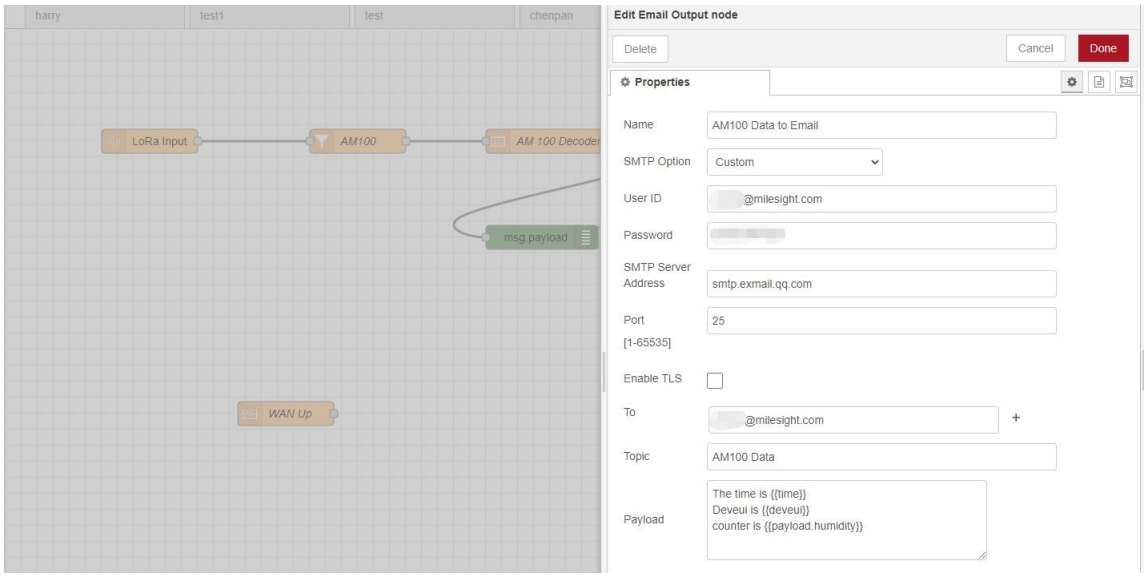


4. Fügen Sie einen „E-Mail-Ausgang" hinzu und geben Sie die SMTP-Client-Einstellungen, die Ziel-E-Mail-Adresse und den Inhalt ein. Beispielinhalt:

Die Uhrzeit ist {{time}} Deveui

ist {{deveui}}

Die Luftfeuchtigkeit beträgt {{payload.humidity}}



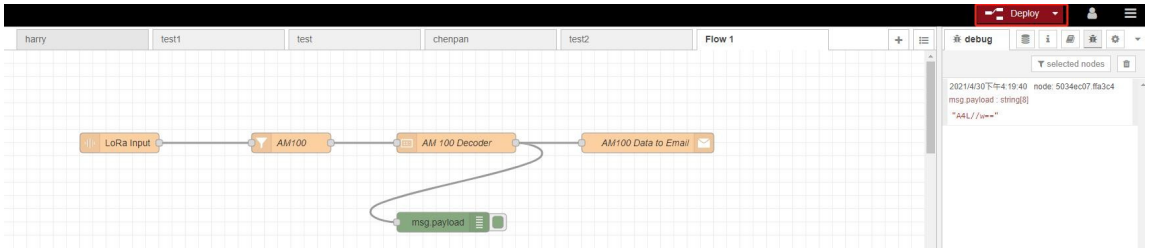
Hinweis:

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

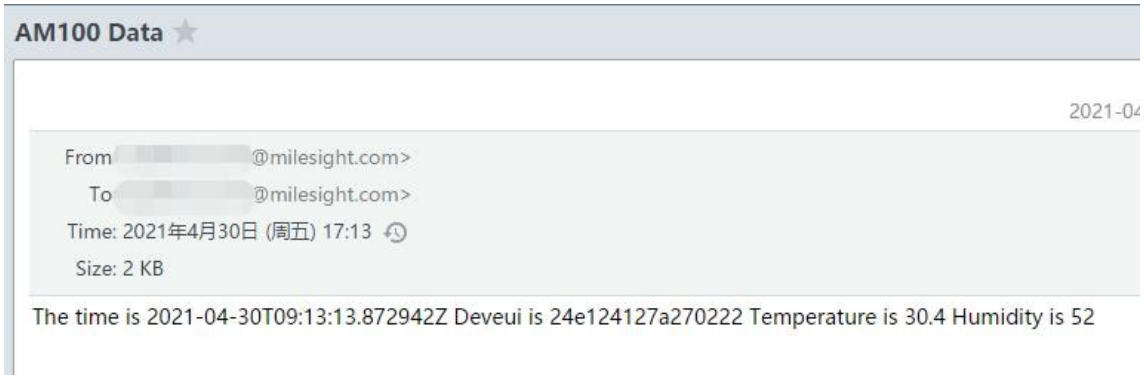
2) Das Grundformat zum Abrufen von LoRaWAN-Knotendaten lautet *{{Eigenschaftsname}}*. Weitere Informationen zum E-Mail- oder SMS-Nutzdatenformat finden Sie auf der Seite „Hilfe".

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

5. Klicken Sie nach Abschluss der Konfiguration auf „Bereitstellen", um alle Ihre Konfigurationen zu speichern.



6. Wenn AM104 Daten an das Gateway sendet, überträgt das Gateway die Daten an die E-Mail.



Verwandtes Thema

Node-RED

[ENDE]