準産業用 LoRaWAN® ゲートウェイ

UG65

ユーザーガイド

はじめに

Milesight UG65 LoRaWAN® ゲートウェイをご利用いただきありがとうございます。UG65 は、自動フェイルオーバー/フェイルバック、拡張動作温度、 ハードウェアウォッチドッグ、VPN、ギガビットイーサネットなどのフル機能設計により、 ネットワーク上での粘り強い接続を実現します。

このガイドでは、UG65 LoRaWAN® ゲートウェイの設定方法と動作について説明します。詳細な機能とゲートウェイの構成については、こちらを参照してください。

読者

本ガイドは、主に以下のユーザーを対象としています：

- ネットワークプランナー
- オンサイトのテクニカルサポートおよびメンテナンス担当者
- ネットワークの設定と保守を担当するネットワーク管理者

関連ドキュメント

ドキュメント	製品概要
UG65データシート	UG65 LoRaWAN® ゲートウェイのデータシート。
UG65 クイック・スタート・ガイド	UG65 LoRaWAN® ゲートウェイのクイック・インストール・ガイド。

適合宣言

UG65 は、CE、FCC、RoHS の必須要件およびその他の関連規定に適合しています。

ご不明な点がございましたら、
Milesightテクニカルサポートまで
お問い合わせください：
電子メール iot.support@milesight.com
サポートポータル: support.milesight-iot.com
電話：86-592-5085280
ファックス： 86-592-5023065
住所Building C09, Software Park III,
Xiamen 361024, China

改訂履歴

日付	ドキュメント版	内容
2020年8月31日	V1.0	初期バージョン
2020年12月10日	V2.0	レイアウト差し替え
2021年4月30日	V2.1	1. LoRaWAN® Class Bのサポート 2. Node-RED機能の追加 3. ノイズアナライザ機能の追加 4. マルチキャストグループ機能の追加 5. アプリケーション例の追加
2021年8月24日	V2.2	1. Yeastar Workplaceプラットフォームとの統合をサポート 2. パッケージ転送ステータスページの削除 3. 電話と電子メールウェブページの更新
2021年12月15日	V2.3	1.AS923-3とAS923-4を追加 2. ネットワークサーバーのチャンネルマスクボックスをチャンネルに変更 3. プロファイルにデバイスチャネル設定を追加
2022年2月18日	V2.4	1. バッチバックアップの追加 2. ログインページの更新 3. デフォルトのアンテナタイプを外部アンテナに変更 4. クラスCのACKタイムアウト時間を調整
2022年6月1日	V2.5	1. VLANトランククライアントをサポート 2. SNMPにシステム名を追加 3. L2TP ピア DNS オプションの追加
2022年12月26日	V2.6	1. BACnetサーバー機能の追加 2. ペイロードコーデック機能の追加 3. Node-REDにリセットおよび全フローエクスポート機能を追加 4. Packet Forwardにデータ再送機能を追加
2024年2月21日	V2.7	1. Milesight開発プラットフォームに対応 2. デフォルトのセカンダリICMPおよびDNSサーバーアドレスの更新 3. セルラーIMSおよびカスタムMTU機能の追加 4. 8つのプリセットデバイスプロファイルを追加 5. ビーコン時間オフセット設定の追加
2024年6月7日	V2.8	1. OpenVPN接続用のovpnファイルのインポートをサポート 2. パケットフィルター機能をサポート

		3. デフォルトのWLAN接続パスワードを追加 4. SMTPクライアント設定にユーザー名を追加 5. BACnetオブジェクトタイプの追加、オブジェクトインスタンスのカスタマイズのサポート
2024年10月31日	V 2.9	1. WireGuard機能の追加 2. MQTTデータ再送信および保持オプションの追加； 3. アプリケーションページにメタデータオプションを追加 4. Node-RED SSLアクセスオプションの追加 5. BACnetオブジェクトイベント検出機能の追加 6. ネットワークパケットアナライザー機能の追加 7. DeviceHub 2.0に対応； 8. セルラーサブネットマスクとDNSサーバーのカスタマイズを追加しました。
2025年1月8日	V 2.10	1. ペイロードコーデックページにオブジェクトマッピング機能を追加； 2. アプリケーションページのBACnet/IPオプションを削除しました； 3. BACnetオブジェクトWeb GUIの更新 4. Modbusサーバー機能の追加
2025年4月3日	V 2.11	1. FUOTA機能の追加 2. MQTT Last Will Message機能の追加； 3. デバイス追加時のアプリケーションキーオプションの更新 4. メタデータ・オプションの更新 5. WANデフォルト接続タイプをDHCPに更新； 6. ウェブGUIアクセス手順の更新

目次

目次

第1章 製品はじめに

1.1 概要

UG65 は堅牢な 8 チャンネル屋内 LoRaWAN® ゲートウェイです。SX1302 LoRaチップと高性能クアッドコアCPUを採用し、2000以上のノードとの接続をサポートします。UG65は最大15kmの見通し線を持ち、都市化された環境では約2kmをカバーすることができ、スマートオフィス、スマートビルディング、その他多くの屋内アプリケーションに最適です。

UG65は、イーサネット、Wi-Fi、セルラーによる複数のバックホールバックアップをサポートするだけでなく、主要なネットワークサーバー（The Things Industries、ChirpStackなど）を統合し、ネットワークサーバーを内蔵しているため、導入が容易です。

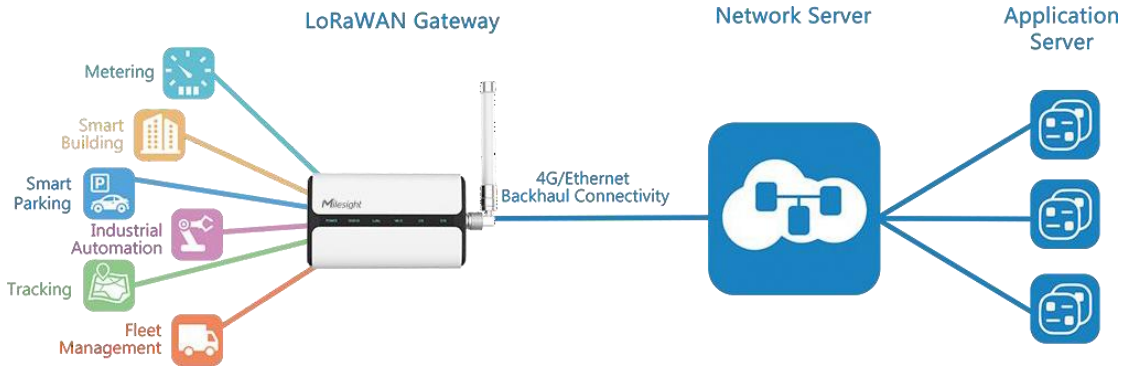


図1-1

1.2 利点

利点

- 産業用CPUと大容量メモリを内蔵
- イーサネット、2.4GHz Wi-Fi、グローバル2G/3G/LTEオプションにより接続が容易
- 組み込みネットワーク・サーバーと複数のサードパーティ製ネットワーク・サーバーとの互換性
- アプリケーション・サーバーへのデータ送信には、MQTT（複数可）またはHTTP（複数可）プロトコルを採用
- 壁やポールへの設置に最適な頑丈な筐体
- 3年保証付き

セキュリティと信頼性

- イーサネットとセルラー間の自動フェイルオーバー/フェイルバック
- IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN/WireGuard などのセキュリティ・フレームワークでユニットを有効化

- 様々なフェイルから自動的に回復し、最高レベルの可用性を保証する内蔵ハードウェア・ウォッチドッグ

容易なメンテナンス

- Milesight DeviceHubとMilesight Development Platformは、簡単なセットアップ、一括設定、リモートデバイスの一元管理を提供します。
- ユーザーフレンドリーなウェブインターフェースデザインと様々なアップグレードオプションにより、管理者はデバイスを簡単に管理することができます。
- ウェブGUIとCLIにより、管理者は大量のデバイスの迅速な設定とシンプルな管理を実現します。
- 業界標準のSNMPを使用して、既存のプラットフォーム上でリモートデバイスを効率的に管理できます。

機能

- 通信技術が常に変化する環境でリモートデバイスをリンク
- 産業用クアッドコア64ビットARM Cortex-A53プロセッサ、低消費電力で最大1.5 GHzの高性能動作、8GB eMMCを搭載し、より多くのアプリケーションをサポート可能
- 40°C～70°C/-40°F～158°Fの幅広い動作温度に対応

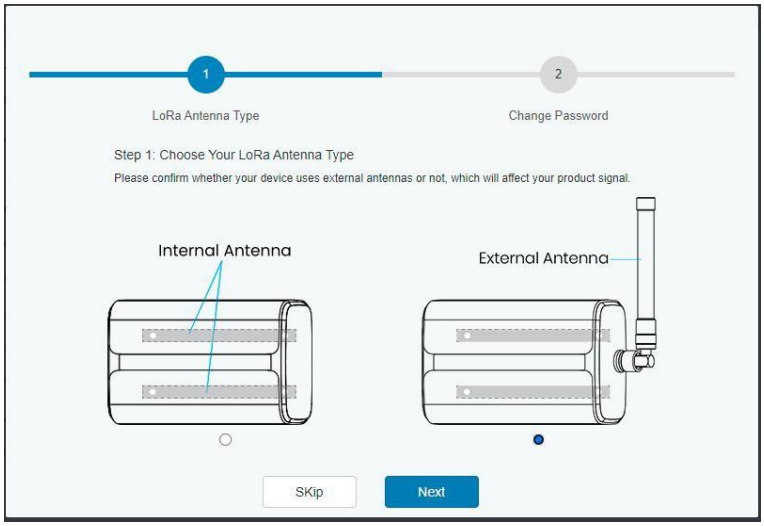
第 2 章 Web GUI へのアクセス

この章では、UG65 の Web GUI へのアクセス方法につ
いて説明します。ユーザー名：**admin**
パスワード：**password**
設定ステップ

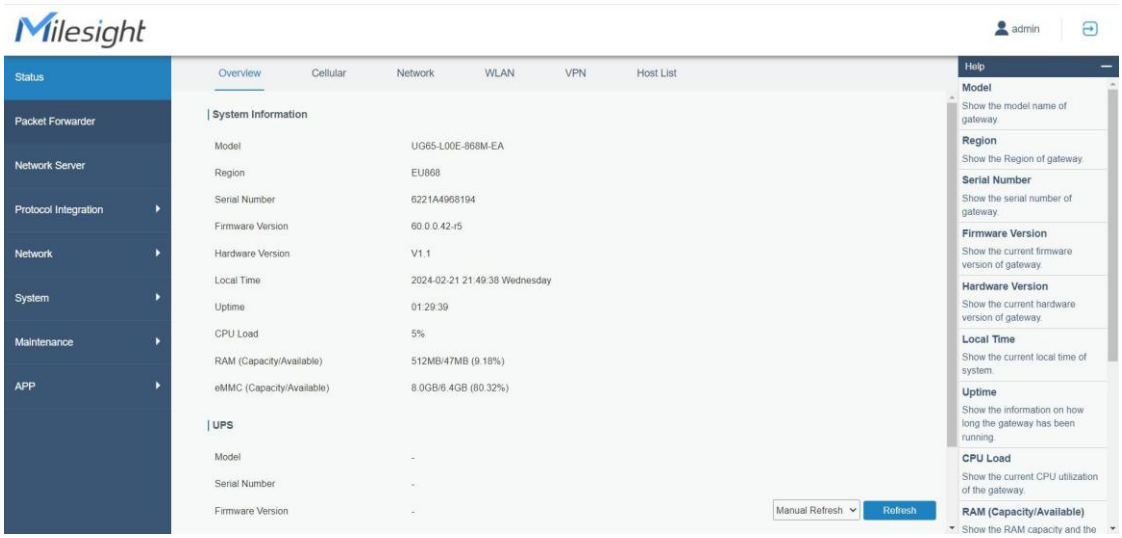
1. コンピュータでワイヤレスネットワーク接続を有効にし、アクセスポイント **Gateway_******** を検索して接続します。
2. パソコンでウェブブラウザ（Chrome推奨）を開き、IPアドレス**192.168.1.1**を入力してウェブGUIにアクセスします。
3. ユーザー名とパスワードを入力し、「Login」をクリックします。

ユーザー名またはパスワードを5回以上間違えると、ログイン画面が10分間ロックされます。

4. Web GUI にログイン後、ガイドに従って基本的な設定を行います。セキュリティのため、パスワードを変更することをお勧めします。



5. システム情報を表示し、ゲートウェイのコンフィギュレーションを実行することができます。

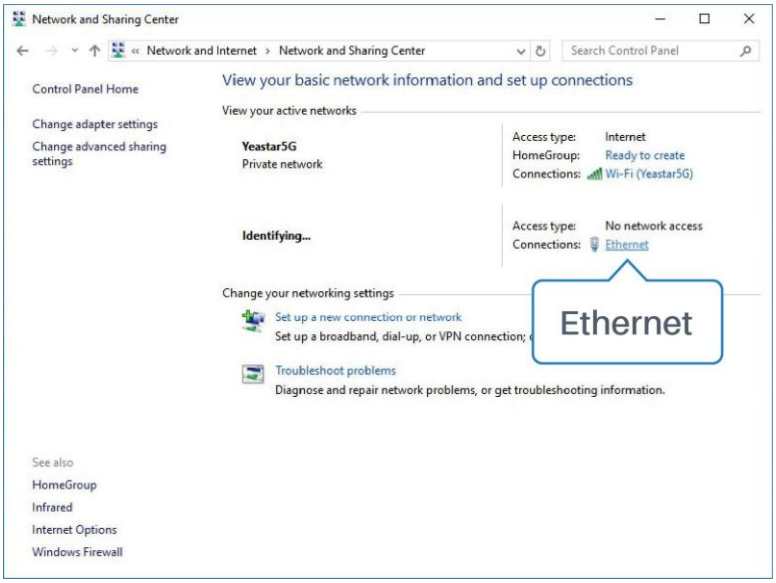


注：イーサネットポートの接続タイプはデフォルトで DHCP です。イーサネットポートの接続タイプを静的 IP として選択し、イーサネットポートに IP アドレスを割り当てる場合、ゲートウェイは有線アクセスもサポートします。

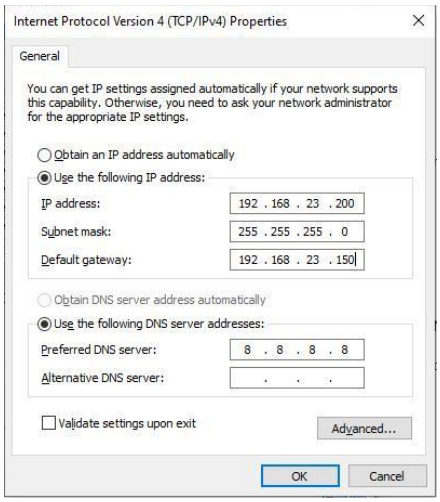
1. **[Network] > [Interface] > [Port]** ページで接続タイプを**静的 IP** に選択し、イーサネット WAN ポートの IP アドレスを設定します。

2. PCをUG65のETHポートに直接、またはPoEインジェクタを介して接続します。

A. コンピュータに IP アドレスを手動で割り当てます。Windows 10システムを例にとると、"コントロールパネル"→ "ネットワークとインターネット"→ "ネットワークと共有センター "に移動し、"イーサネット"（名前が異なる場合があります）をクリックします。



B. プロパティ"→ "インターネットプロトコルバージョン4(TCP/IPv4) "に移動し、"次のIPアドレスを使用する "を選択し、ゲートウェイの同じサブネット内で静的IPを手動で割り当てます。



C. PC でウェブブラウザ（Chrome を推奨）を開き、イーサネットポートの IP アドレスを入力してウェブ GUI にアクセスします。

第 3 章 ウェブ設定

2.1 ステータス

2.1.1 概要

このページでは、ゲートウェイのシステム情報を表示できます。

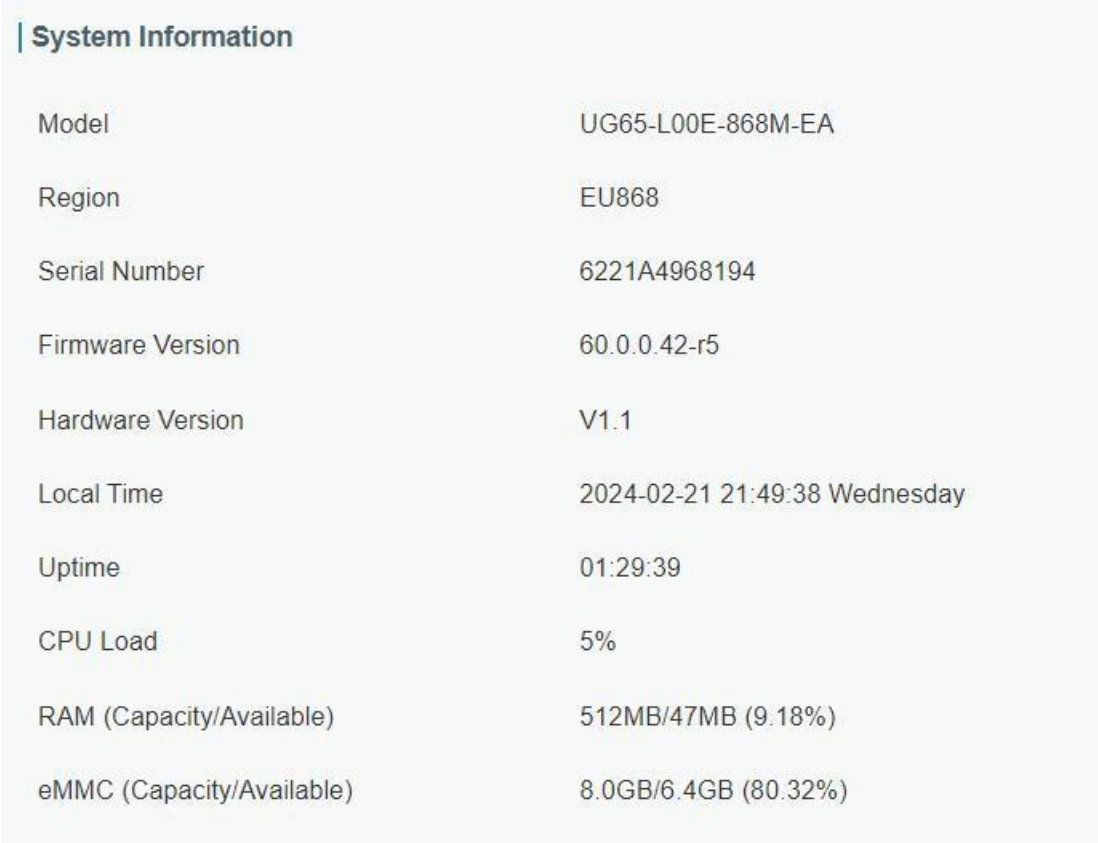


図 3-1-1-1

System Information	
項目	説明
Model	ゲートウェイのモデル名を表示します。
Region	ゲートウェイの LoRaWAN® 使用周波数を表示します。
Serial Number	ゲートウェイのシリアル番号を表示します。
Firmware Version	ゲートウェイの現在のファームウェアバージョンを表示します。
Hardware Version	ゲートウェイの現在のハードウェア・バージョンを表示します。
Local Time	現在のシステムのローカル時間を表示します。
Uptime	ゲートウェイが稼動している時間の情報を表示します。
CPU Load	ゲートウェイの現在の CPU 使用率を表示します。
RAM (Capacity/Available)	RAM 容量と使用可能な RAM メモリを表示します。
eMMC (Capacity/Available)	eMMC の容量と使用可能な eMMC メモリを表示します。

表 3-1-1-1 システム情報

Milesight UPS がデバイスに接続されている場合、UPS の基本情報も Status ページに表示されます。詳細は *Milesight UPS ユーザーガイド*を参照してください。

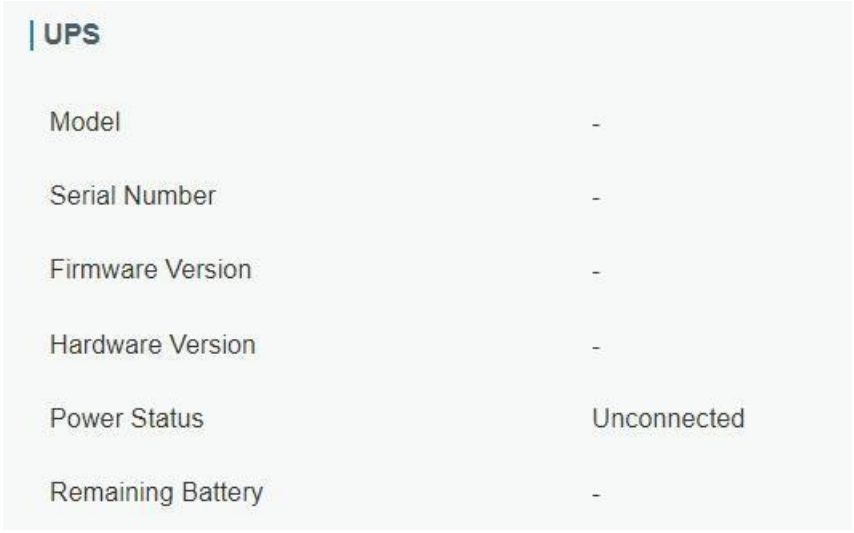


図 3-1-1-2

2.1.2 セルラー

このページではゲートウェイのセルラーネットワークステータスを表示できます。

図 3-1-2-1

Modem Information	
項目	項目 内容
Status	モジュールと SIM カードの対応する検出ステータスを表示します。
Model	セルラーモジュールのモデル名を表示します。
Version	セルラーモジュールのバージョンを表示します。
Signal Level	セルラーの信号レベルを表示します。
Register Status	SIMカードの登録状態を表示します。
IMEI	モジュールのIMEIを表示します。
IMSI	SIM カードの IMSI を表示します。
ICCID	SIMカードのICCIDを表示します。
ISP	SIMカードが登録しているネットワークプロバイダを表示します。
Network Type	LTE、3Gなど、接続されているネットワークの種類を表示します。
PLMN ID	MCC、MNC、LAC、Cell IDなど、現在のPLMN IDを表示します。
LAC	SIM カードの位置エリアコードを表示します。
Cell ID	SIM カードの位置のセル ID を表示します。

表 3-1-2-1 モデム情報

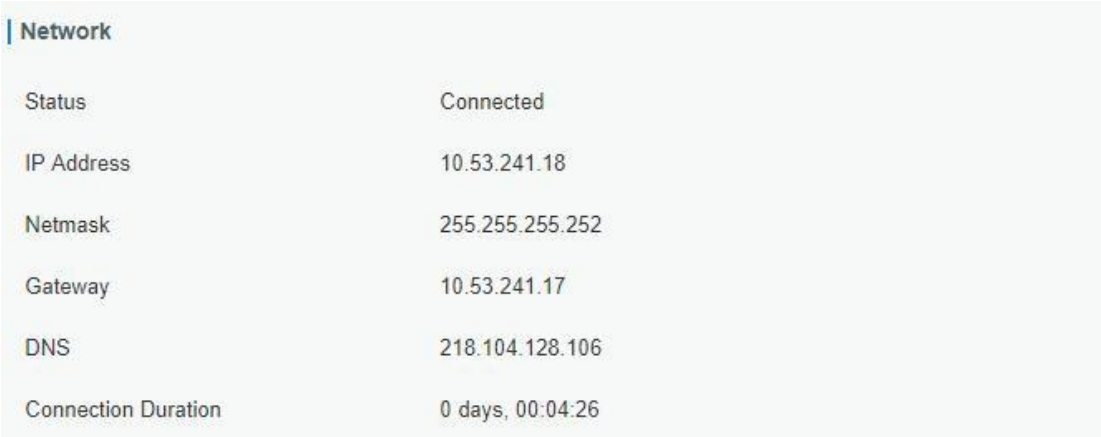


図 3-1-2-2

Network Status	
項目	項目 内容
Status	携帯電話ネットワークの接続状態を表示します。
IP Address	セルラーネットワークのIPアドレスを表示します。
Netmask	セルラーネットワークのネットマスクを表示します。
Gateway	携帯電話ネットワークのゲートウェイを表示します。
DNS	セルラーネットワークのDNSを表示します。
Connection Duration	セルラーネットワークの接続時間を表示します。

表 3-1-2-2 ネットワークステータス

2.1.3 ネットワーク

このページでは、ゲートウェイのイーサネットポートの状態を確認できます。

図 3-1-3-1

Network	
項目	ポート
Port	イーサネットポートの名称を表示します。
Status	イーサネットポートのステータスを表示します。「Up」は、WAN が有効でイーサネットケーブルが接続されている状態を表します。「Down」はイーサネットケーブルが切断されているか、WAN機能が無効になっていることを意味します。
Type	イーサネットポートのダイヤルアップタイプを表示します。
IP Address	イーサネットポートのIPアドレスを表示します。
Netmask	イーサネットポートのネットマスクを表示します。
Gateway	イーサネットポートのゲートウェイを表示します。
DNS	イーサネットポートの DNS を表示します。
Duration	イーサネットポートが有効になっているとき、イーサネットケーブルがイーサネットポートに接続されている時間の情報を表示します。ポートが無効化されるか、イーサネットケーブルが切断されると、継続時間は表示されなくなります。

表 3-1-3-1 WAN ステータス

2.1.4 WLAN

アクセスポイントやクライアントの情報など、Wi-Fi の状態を確認することができます。

図 3-1-4-1

WLAN Status	
項目	内容
Wireless Status	無線ステータスを表示します。
MAC Address	MAC アドレスを表示します。
Interface Type	AP」や「クライアント」など、インターフェースの種類を表示します。
SSID	SSID を表示します。
Channel	ワイヤレスチャンネルを表示します。
Encryption Type	暗号化タイプを表示します。
Status	接続ステータスを表示します。
IP Address	ゲートウェイのIPアドレスを表示します。
Netmask	ゲートウェイの無線 MAC アドレスを表示します。
Gateway	ワイヤレスネットワークのゲートウェイアドレスを表示します。
Connection Duration	Wi-Fi ネットワークの接続時間を表示します。

表 3-1-4-1 WLAN ステータス

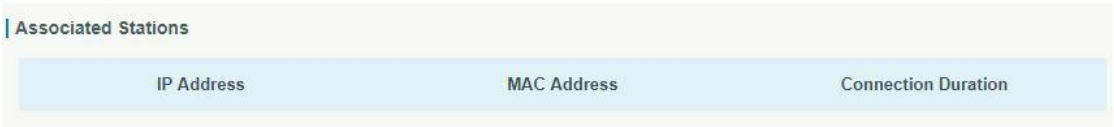


図 3-1-4-2

Associated Stations	
項目	説明
IP Address	アクセスポイントまたはクライアントの IP アドレスを表示します。
MAC Address	アクセスポイントまたはクライアントの MAC アドレスを表示します。
Connection Duration	Wi-Fi ネットワークの接続時間を表示します。

表 3-1-4-2 WLAN ステータス

2.1.5 VPN

このページでは、PPTP、L2TP、IPsec、OpenVPN、DMVPN などの VPN ステータスを確認できます。

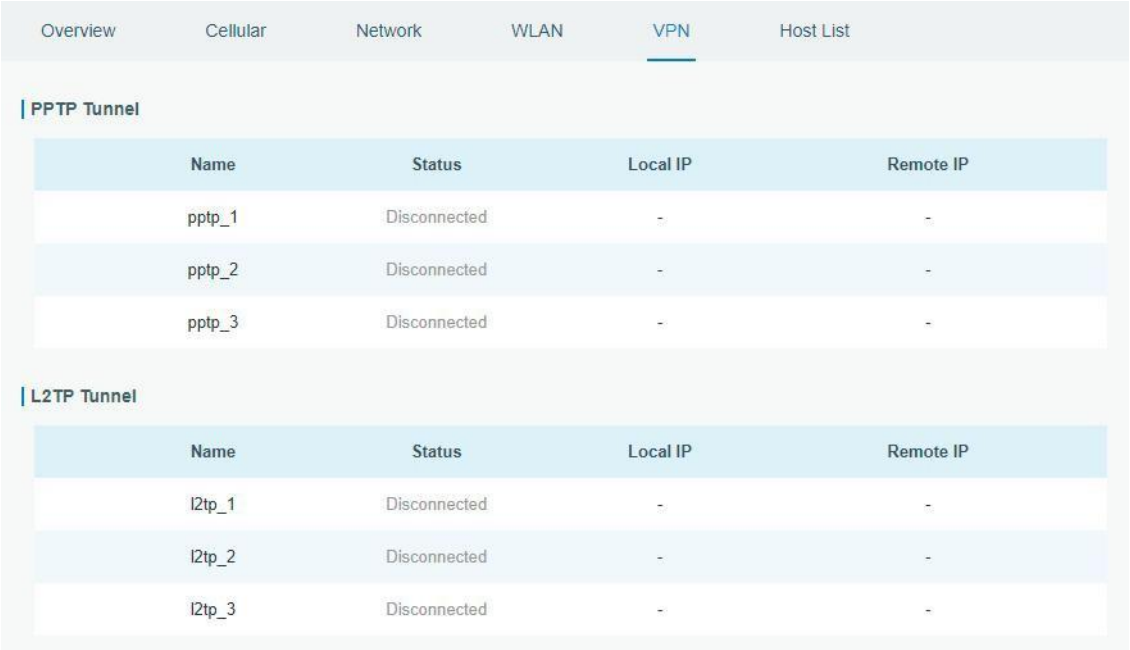


図 3-1-5-1

図 3-1-5-2

図 3-1-5-3

VPN Status	
項目	名称
Name	VPN トンネルの名称を表示します。
Status	VPNトンネルのステータスを表示します。
Local IP	VPNトンネルのローカルトンネルIPを表示します。
Remote IP	VPN トンネルのリモートトンネル IP を表示します。

表 3-1-5-1 VPN ステータス

2.1.6 ホスト一覧

ホスト情報を表示します。

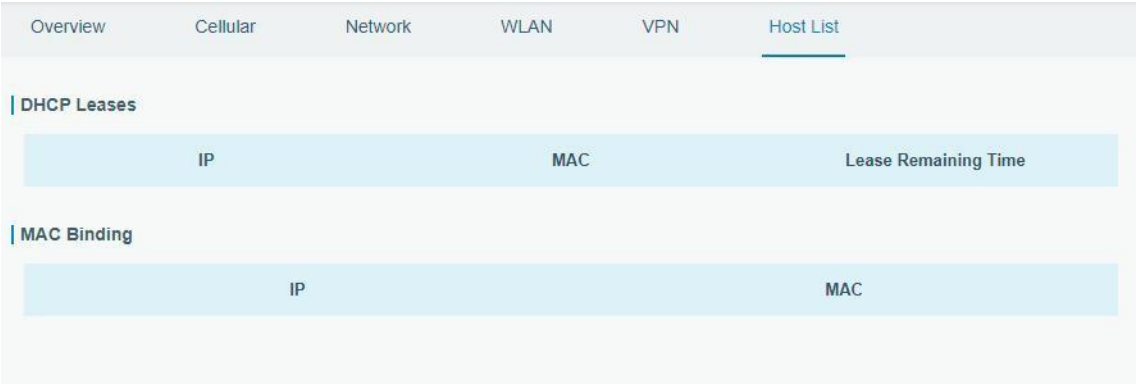
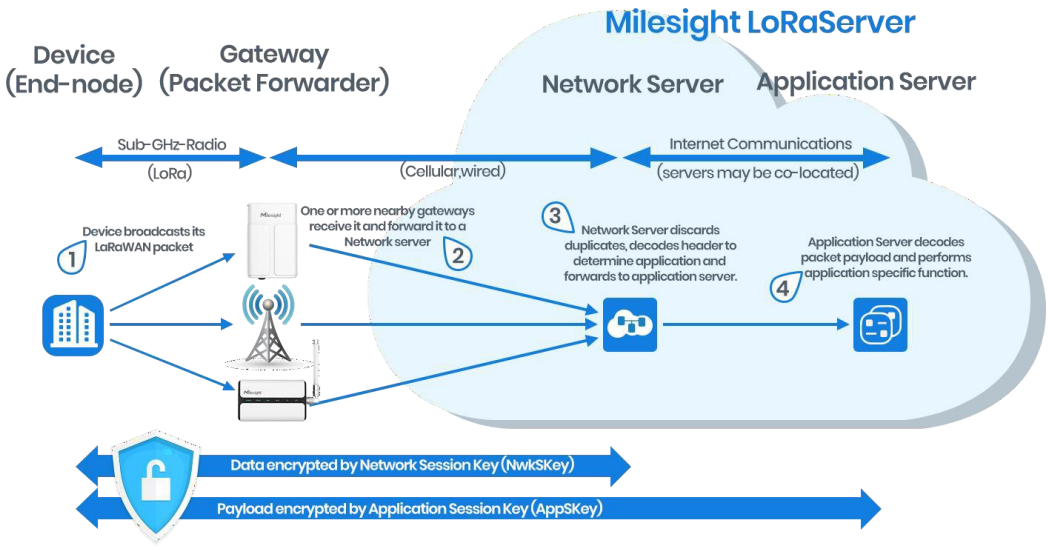


図 3-1-6-1

Host List	
表示項目	説明
DHCP Leases	
IP Address	DHCPクライアントのIPアドレスを表示
MAC Address	DHCPクライアントのMACアドレスを表示
Lease Time Remaining	DHCP クライアントの残りリース時間を表示します。
MAC Binding	
IP & MAC	DHCP サービスの Static IP リストに設定されている IP アドレスと MAC アドレスを表示します。

表 3-1-6-1 ホスト一覧の説明

2.2 LoRaWAN



2.2.1 パケットフォワーダ

2.2.1.1 一般

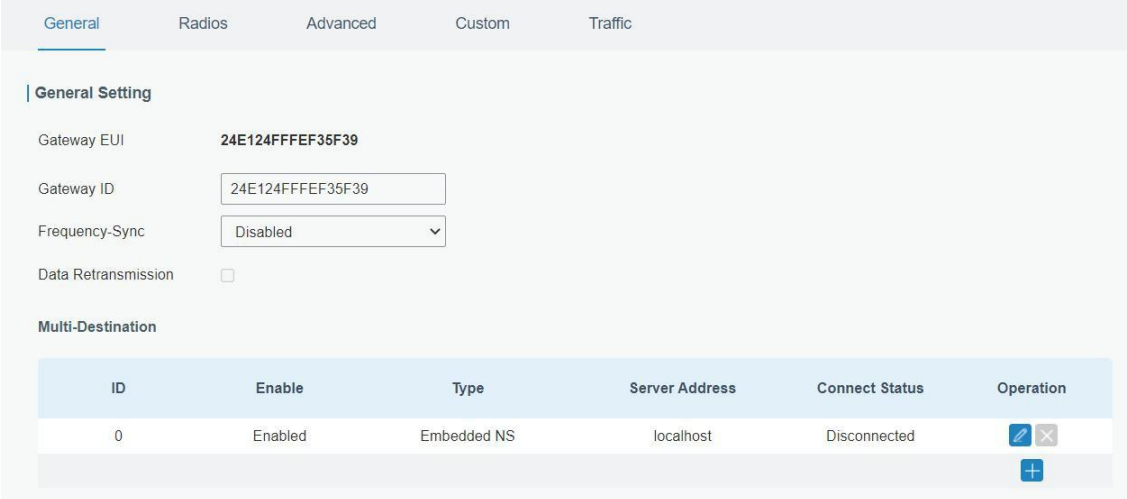


図 3-2-1-1

General Settings	
設定項目	設定項目
Gateway EUI	ゲートウェイの一意の識別子を表示します。
Gateway ID	ゲートウェイをリモートネットワークサーバーに登録する際に使用した、対応する ID を入力します。通常はゲートウェイ EUI と同じで、変更可能です。

Frequency-Sync	対応するマルチデスティネーションIDを選択して、ネットワークサーバーから周波数設定を同期します。
Data Retransmission	ゲートウェイが1台のChirpstack/Semtech/Remote Embedded NS/Basic Stationタイプのパッケージフォワーダに接続する場合、ネットワーク切断時に最大100万件のデータ保存をサポートし、ネットワーク復旧後にデータを再送信します。
Multi-Destination	ゲートウェイは、リストで作成され有効になっているネットワークサーバアドレスにデータを転送します。
Connection Status	パッケージフォワーダの接続状態を表示します。

表 3-2-1-1 一般設定パラメータ

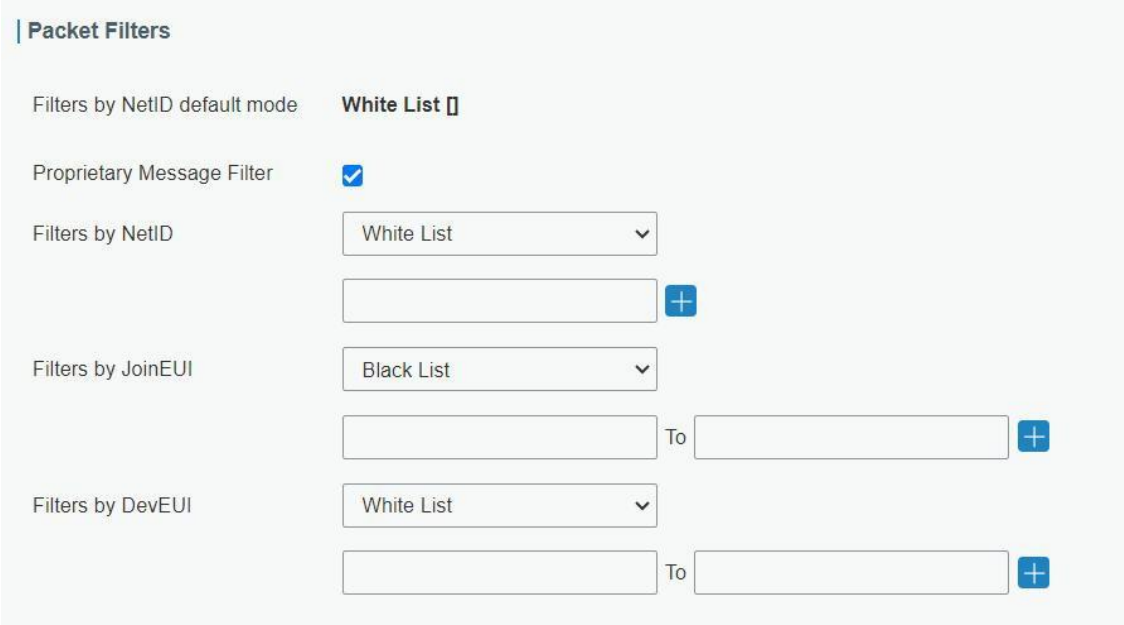


図 3-2-1-2

Packet Filters	
設定項目	説明
Filters by NetID Default Mode	フィルタモードをブラックリストかホワイトリストから選択します。 **White List**：このリストのパケットのみをネットワークサーバーに転送します。 **Black List**：このリスト以外のパケットのみをネットワークサーバーに転送します。
Proprietary Message Filter	独自メッセージパケット（Mtype=111）を転送しないようにします。
Filters by NetID	NetID に一致するアップリンクパケットを転送するかしないかを設定します。
Filters by JoinEUI	JoinEUI 範囲に一致するジョインリクエストパケットをフォワード/フォワードしません。

Filters by DevEUI	DevEUI範囲に一致する参加要求パケットを転送する／転送しません。
List	特定のフィルタリング値または範囲リストを設定します。どの条件でも最大 5 リストまで追加できます。

表 3-2-1-2 パケットフィルタパラメータ

注意

1. join EUI と dev EUI の両方を設定した場合、両方の条件に一致するパケットのみが転送されます。
2. この機能は、パケットフォワーダタイプが Loriot または Everynet の場合はサポートされません。
3. サードパーティーのネットワークサーバーがゲートウェイにフィルター条件を割り当てる場合、ゲートウェイはネットワークサーバーの設定を優先して使用します。

関連設定例

パケットフォワーダーの設定

2.2.1.2 無線機

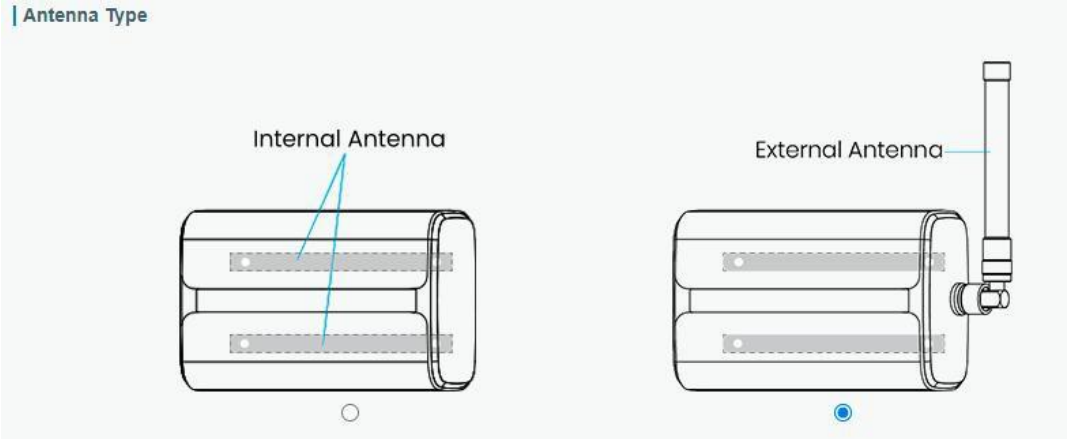


図 3-2-1-3

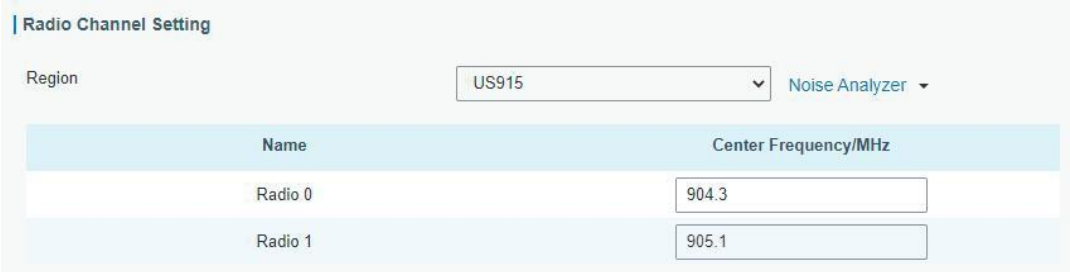


図 3-2-1-4

Radios-Radio Channel Setting	
設定項目	設定項目
Antenna Type	EA 版を使用する場合のアンテナの送信タイプを選択します。

Region	アップストリームとダウンリンクの周波数とデータレートに使用する LoRaWAN® の周波数プランを選択します。利用可能なチャネルプランは、ゲートウェイのモデルによって異なります。
Center Frequency	LoRaWAN® ノードからのパケットを受信する周波数を変更します。

表 3-2-1-3 無線チャネル設定パラメータ

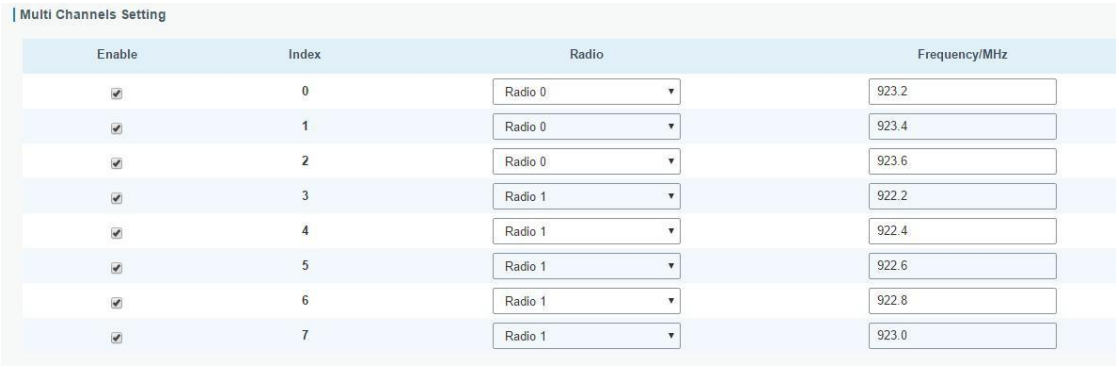


図 3-2-1-5

Radios-Multi Channel Setting	
設定項目	設定項目
Enable	パケットを送信するチャネルを有効にします。
Index	リストの序列を示します。
Radio	中心周波数としてラジオ0またはラジオ1を選択します。
Frequency/MHz	このチャンネルの周波数を入力します。 範囲：中心周波数± 0.4625。

表 3-2-1-4 マルチチャネル設定パラメータ

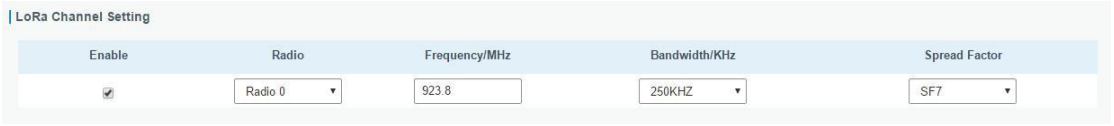


図 3-2-1-6

Radios-LoRa Channel Setting	
設定項目	設定項目
Enable	パケット送信を有効にします。
Radio	中心周波数として Radio 0 または Radio 1 を選択します。
Frequency/MHz	このチャンネルの周波数を入力します。 範囲：中心周波数±0.9。
Bandwidth/MHz	このチャネルの帯域幅を入力します。
Spread Factor	選択可能な拡散係数を選択します。拡散係数が大きいチャネルは低レート、小さいチャネルは高レートに対応します。

表 3-2-1-5 LoRa チャネル設定パラメータ

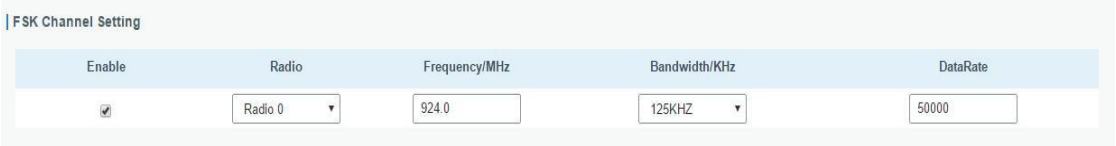


図 3-2-1-7

Radios-FSK Channel Setting	
設定項目	設定項目
Enable	パケット送信を有効にします。
Radio	中心周波数として Radio 0 または Radio 1 を選択します。
Frequency/MHz	このチャンネルの周波数を入力します。 範囲：中心周波数±0.9。
Bandwidth/MHz	このチャンネルの帯域幅を入力します。 推奨値：125KHz、250KHz、500KHz
Data Rate	データレートを入力します。範囲：500～25000

表 3-2-1-6 FSK チャネル設定パラメータ

2.2.1.3 ノイズアナライザ

ノイズアナライザは、各周波数チャネルのノイズをスキャンし、ユーザが環境干渉状 態を分析し、最適な配置を選択するための図を提供するために使用されます。RSSI は各チャンネルの感度を示します。RSSI 値が低いほど、良好な信号です。ダウンリンク伝送に影響するため、パッケージフォワーダーを使用する場合は、この機能を有 効にすることをお勧めしません。

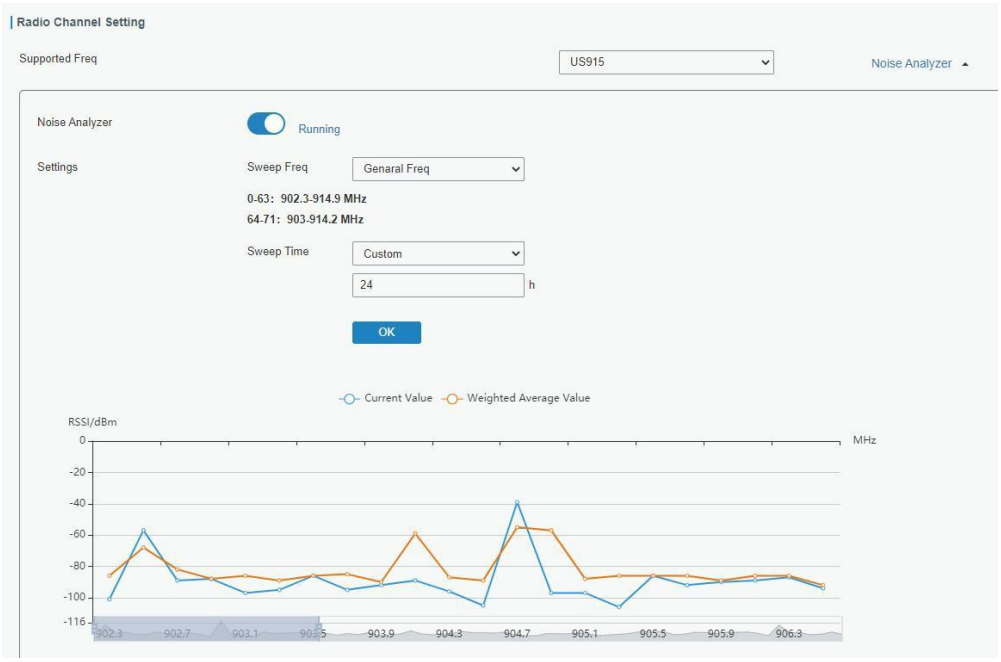


図 3-2-1-8

Noise Analyzer		
項目	項目 内容	デフォルト
Enable	ノイズアナライザ機能を有効にします。	Disabled
Sweep Freq	周波数スイープ範囲を選択します。	General Feq

	General Freq: LoRaWAN® 地域パラメータドキュメントに基づく周波数。 **Custom:** 周波数範囲をカスタマイズします。	
Sweep Time	ノイズアナライザを連続的または一定時間内に有効にします。 Custom を選択した場合、ノイズアナライザは事前に設定した時間後に自動的に停止します。 注：ノイズアナライザ機能は通常のデータ伝送に影響を与えるため、時間をカスタマイズすることをお勧めします。	Custom/24h

表 3-2-1-7 ノイズアナライザ設定パラメータ

2.2.1.4 詳細設定

本節では、ビーコン送信とバリデーションの詳細設定について説明します。

図 3-2-1-9

Advanced-Beacon Setting		
項目	設定項目	初期値
Beacon Period	クラス B デバイスの時間同期のためにゲートウェイがビーコンを送信する間隔。0 は、ゲートウェイがビーコンを送信しないことを意味します。	0
Beacon Freq	ビーコンの周波数。	サポートされている周波数に基づきます。
Beacon Datarate	ビーコンのデータレート。	対応周波数に基づく
Beacon Channel Number	Customを選択した場合、1～8の範囲で設定できます。	1

Beacon Freq Step	ビーコンの周波数間隔。	200000
Beacon Bandwidth	ビーコンの帯域幅。単位：Hz	12500 Hz
Beacon TX Power	ビーコンのTXパワー。	対応周波数に基づく
Beacon Time Offset	このオフセットをシステム時間に追加し、その結果をクラスBデバイスに割り当てます。これにより、複数のクラス B デバイスが近くにある場合の干渉を回避できます。	0

表 3-2-1-8 ビーコン詳細パラメータ

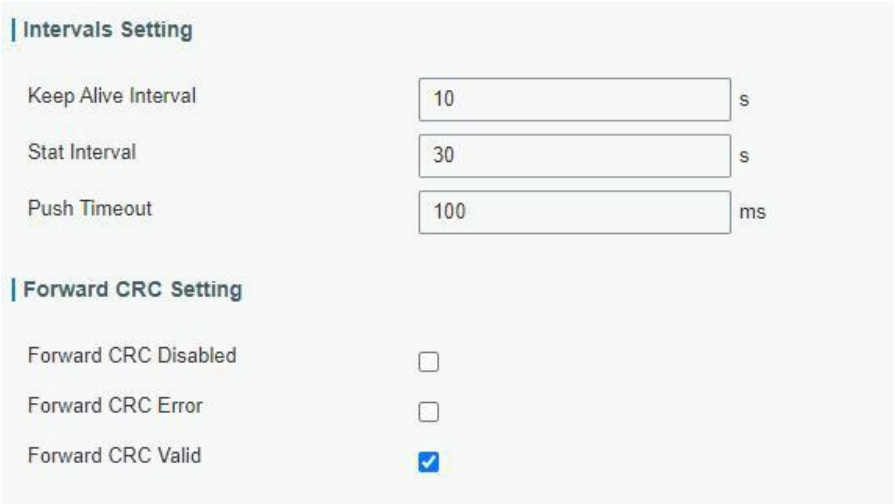


図 3-2-1-10

項目	項目 内容	デフォルト
Keep Alive Interval	ゲートウェイからネットワークサーバーに送信されるキープアライブパケットの間隔を入力します。 範囲1-3600.	10
Stat Interval	ゲートウェイの統計情報をネットワークサーバーに更新する間隔を入力します。範囲：1-3600.	30
Push Timeout	ゲートウェイがノードのデータを送信した後、サーバーからの応答を待つタイムアウトを入力します。範囲：1-19991-1999.	100
Forward CRC Disabled	CRC を無効にして受信したパケットをネットワークサーバーに送信するかどうかを設定します。	Disabled
Forward CRC Error	CRC エラーで受信したパケットをネットワークサーバーに送信します。	Disabled
Forward CRC Valid	CRC が有効で受信したパケットをネットワークサーバーに送信します。	Enabled

表 3-2-1-9 詳細パラメータ

2.2.1.5 カスタム

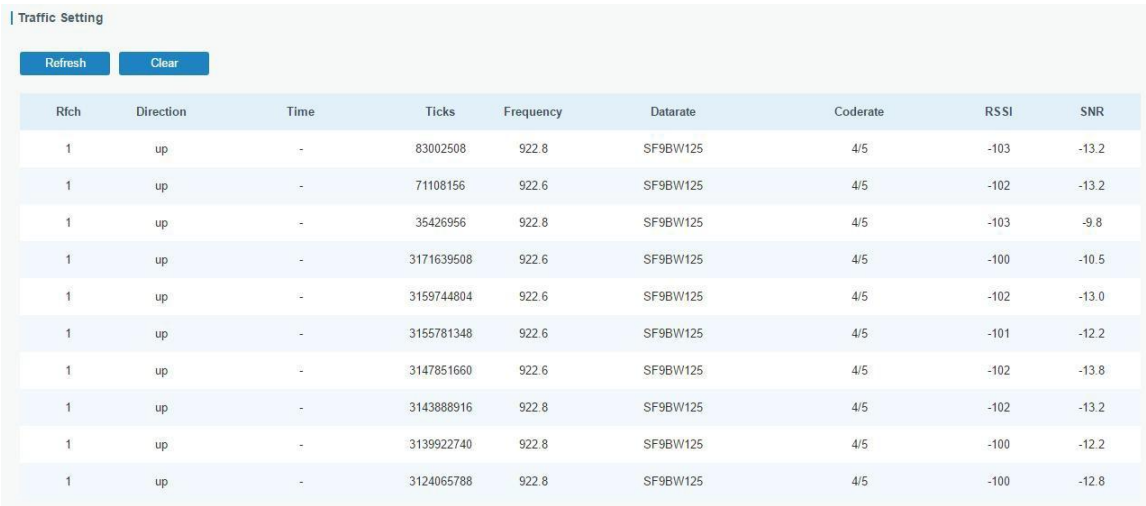
Custom Configuration モードを有効にすると、エディットボックスに独自のパケットフォワー ダ設定ファイルを記述し、パケットフォワーダの設定を行うことができます。Save" をクリックすると、カスタムコンフィグレーションファイルの内容が保存され、"Apply" をクリックすると反映されます。Clear "をクリックすると、エディットボックスの内容がすべて消去されます。設定ファイルの書き方がわからない場合は、「Example」をクリックしてリファレンスページを参照してください。

注：カスタマイズされた設定は、Web GUI のパケットフォワード設定を上書きします。

図 3-2-1-11

2.2.1.6 トラフィック

トラフィックページに移動すると、ゲートウェイが受信した最新のトラフィックが表示されます。ライブトラフィックを表示するには、「**Refresh**」をクリックします。



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

図 3-2-1-12

項目	表示内容
Refresh	最新のデータを取得します。
Clear	全てのデータをクリアします。
Rfch	このパケットのチャンネルを表示します。
Direction	このパケットの方向を表示します。
Time	このパケットの受信時刻を表示します。
Ticks	このパケットのティックを表示します。
Frequency	チャネルの周波数を表示します。
Datarate	チャネルのデータレートを表示します。
Coderate	このパケットのコーデレートを表示します。
RSSI	受信信号強度を表示します。
SNR	このパケットの信号対雑音比を表示します。

表 3-2-1-10 トラフィックパラメータ

2.2.2 ネットワーク サーバー

2.2.2.1 一般

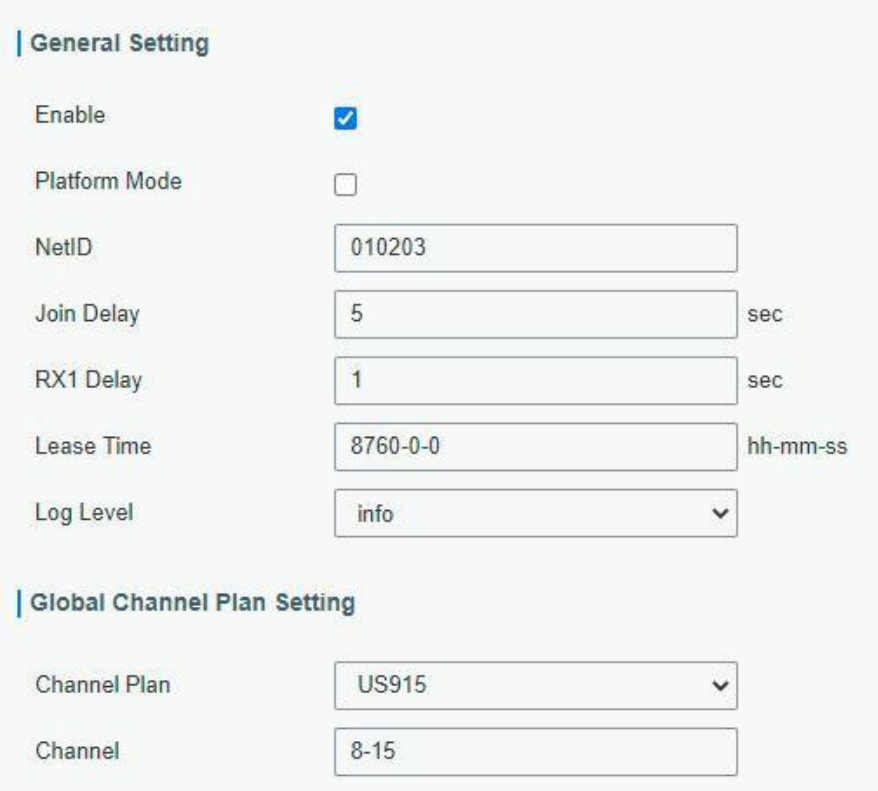


図 3-2-2-1

項目	説明	デフォルト
General Setting		
Enable	ネットワークサーバーモードを有効にします。	Enabled
Platform Mode	ゲートウェイをMilesight IoTに接続するために有効にします。	Disabled

	クラウドまたはYeastar Workplaceプラットフォーム.	
NetID	ネットワーク識別子を入力します。	010203
Join Delay	エンドデバイス が に Join_request_message をネットワークサーバーに送信してから、エンドデバイスがネットワークサーバーから送信された Join_accept_message を受信するために RX1 を開く準備をするまでの間隔時間を入力します。	5
RX1 Delay	エンドデバイスがアップリンクパケットを送信してから、エンドデバイスがダウンリンクパケットを受信するためにRX1を開く準備をするまでの間隔時間を入力します。	1
Lease Time	結合が成功した場合の有効期限までの時間を入力します。フォーマットは時-分-秒です。参加タイプが OTAA の場合、リース時間を超えると、エンドデバイスはネットワークサーバーに再度参加する必要があります。	876000-00-00
Log level	ログレベルを選択します。	Info
Channel Plan Setting		
Channel Plan	アップストリームとダウンリンクの周波数とデータレートに使用されるLoRaWAN® チャネルプランを選択します。利用可能なチャネルプランはゲートウェイのモデルによって異なります。	ゲートウェイの周波数による
Channel	エンドデバイスが特定の周波数チャネルと通信できるようにします。 空白のままでは、LoRaWAN® 地域パラメータ・ドキュメントで指定されたデフォルトの標準使用可能チャネルをすべて使用することを意味します。チャネルのインデックスを入力できます。 例 1, 40: チャンネル 1 とチャンネル 40 を有効にします。 1-40:チャネル 1 からチャネル 40 まで有効 1-40、60：チャンネル1をチャンネル40とチャンネル60に有効化	ゲートウェイの周波数による

表 3-2-2-1 一般パラメータ

注：LoRaWAN® 地域で許可されている場合、追加プランを使用して、EU868 や KR920 のような LoRaWAN® 地域パラメータで定義されていない追加チャネルを設定することができます：

図 3-2-2-2

Additional Channels	
項目	項目
Frequency/MHz	追加プランの周波数を入力します。
Max Datarate	エンドデバイスの最大データレートを入力します。範囲は、LoRaWAN® 地域パラメータ・ドキュメントで指定されているものに基づきます。
Min Datarate	エンドデバイスの最小データレートを入力します。範囲は、LoRaWAN® 地域パラメータ文書で指定されたものに基づきます。

表 3-2-2-2 追加プランパラメータ

2.2.2.2 アプリケーション

アプリケーションは、同じ目的/同じタイプのデバイスの集まりです。ユーザーは、同じサーバーに送信する必要がある一連のデバイスを同じアプリケーションに追加することができます。

 をクリックしてアプリケーションを編集するか、  をクリックして新しいアプリケーションを作成することができます。

図 3-2-2-3

Application	
項目	名称
Name	アプリケーションプロファイルの名前を入力します。 例：smoker-sensor-app。
Description	このアプリケーションの説明を入力します。 例：喫煙者センサーのアプリケーション。
Metadata	デバイスがペイロードコーデックを追加したときに、自動的にアップリンクパケットで報告する詳細を選択できるようにします。
Data Transmission	データはMQTT、HTTPまたはHTTPSプロトコルを使用してカスタムサーバーに送信されます。1つのアプリケーションは、1つのMQTT送信と1つのHTTP（HTTPS）送信しか追加できません。

表 3-2-2-3 アプリケーションパラメータ

MQTT 連携

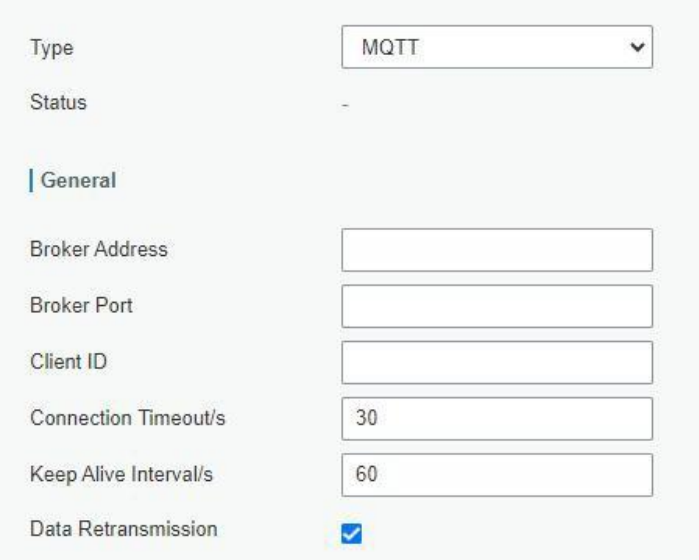

Type
MQTT
Status
-
General
Broker Address
Broker Port
Client ID
Connection Timeout/s
30
Keep Alive Interval/s
60
Data Retransmission

図 3-2-2-4

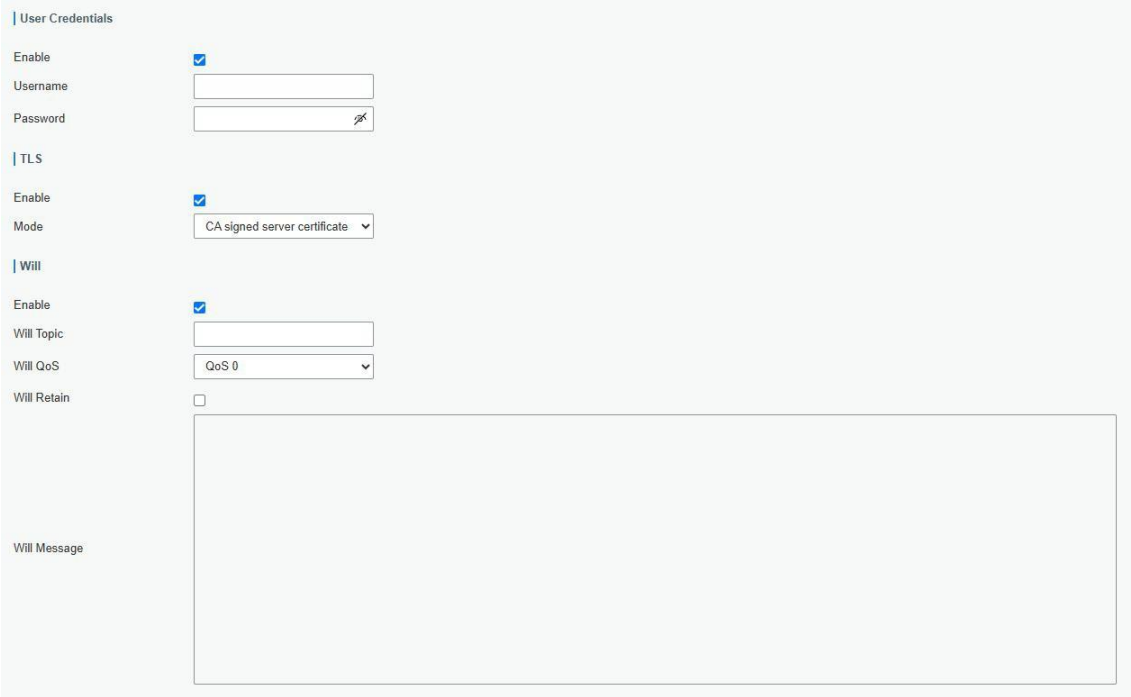

User Credentials
Enable
Username
Password
TLS
Enable
Mode
CA signed server certificate
Will
Enable
Will Topic
Will QoS
QoS 0
Will Retain
Will Message

図 3-2-2-5

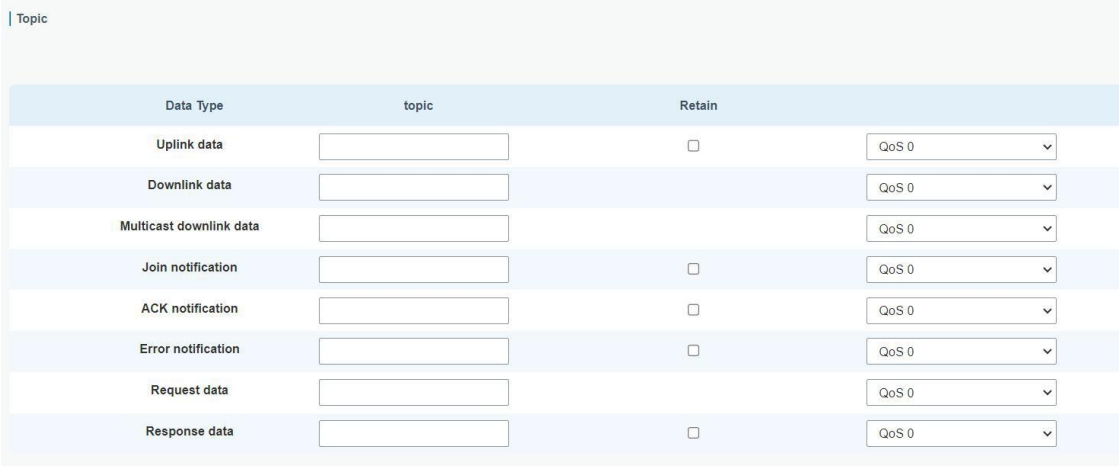


図 3-2-2-6

MQTT Settings	
設定項目	設定項目
General	
Broker Address	データを受信するMQTTブローカーのアドレス。
Broker Port	データを受信するMQTTブローカーポート。
Client ID	クライアントIDは、サーバに対するクライアントの一意なIDです。すべてのクライアントが同じサーバーに接続されている場合に一意である必要があり、QoS 1および2でメッセージを処理するための鍵となります。
Connection Timeout/s	接続タイムアウトの後、クライアントからの応答がない場合、接続は切断されたとみなされます。範囲は1-65535.
Keep Alive Interval/s	クライアントがサーバーに接続された後、クライアントは定期的にサーバーにハートビートパケットを送信し、キープアライブします。範囲は1-65535.
Data Restransmission	有効化後、ネットワーク切断時に最大 10,000 個のデータ保存をサポートし、ネットワーク回復後にデータを再送信します。
User Credentials	
Enable	ユーザー認証情報を有効にします。
Username	MQTT ブローカーへの接続に使用するユーザー名。
Password	MQTT ブローカーへの接続に使用するパスワード。
TLS	
Enable	MQTT通信のTLS暗号化を有効にします。 注: MQTT ブローカのタイプが HiveMQ の場合、**TLS** を有効にし、オプションを **CA signed server certificate** として設定してください。
Mode	Self signed certificates、CA signed server certificateから選択します。 **CA signed server certificate**：デバイスにあらかじめ搭載されている認証局（CA）が発行した証明書で検証します。 **Self signed certificates**：認証局のカスタム証明書(.crt または .pem)、クライアント証明書(.crt)、秘密鍵(.key)をアップロードして検証します。
Will	

Enable	最終willメッセージは、MQTTクライアントが異常切断されたときに自動的に送信されます。通常、デバイスのステータス情報を送信したり、他のデバイスやプロキシサーバーにデバイスのオフラインステータスを通知するために使用されます。
Will Topic	最後のwillメッセージを受信するトピックをカスタマイズします。
Will QoS	QoS0、QoS1またはQoS2はオプションです。
Will Retain	willメッセージを保持メッセージとして設定します。
Will Message	willメッセージの内容をカスタマイズします。
Topic	
Data Type	MQTTブローカーと通信するためのデータ型： **Uplink Data**：デバイスのアップリンクパケットを受信します。 **Downlink Data**：デバイスにダウンリンクコマンドを送信します。単一のデバイスにダウンリンクコマンドを送信する必要がある場合は、このトピックにワイルドカード **"$deveui"** を追加し、このトピックを購読する際にこれを実際のデバイス **EUI** に置き換えてください。 **Multicast Downlink Data**：マルチキャストグループにダウンリンクコマンドを送信します。 **Join Notification**：ゲートウェイがデバイスのネットワーク参加を許可する参加アクセプトパケットを送信した場合、参加通知を受信します。 **ACK Notification**：ダウンリンクコマンド送信時にデバイスからACKパケットを受信 **Error Notification**：機器からエラーパケットを受信 **Request data**：ゲートウェイ NS を照会および設定するためのリクエストを送信します。 **Response data**：リクエスト・レスポンスを受信
Topic	パブリッシングに使用されるデータタイプのトピック名。
Retain	このトピックの最新メッセージを保持メッセージとして設定します。
QoS	QoS 0 - 一度だけ これは最も高速な方法で、必要なメッセージは 1 回だけです。また、最も信頼性の低い転送モードです。 QoS 1 - 最低一回 このレベルは、メッセージが少なくとも一度は配信されることを保証しますが、複数回配信されることもあります。 QoS 2 - 一度だけ QoS 2 は、MQTT の最高レベルのサービスです。このレベルは、各メッセージが意図された受信者によって一度だけ受信されることを保証します。QoS 2 は、最も安全で最も遅いサービス品質レベルです。

表 3-2-2-4 MQTT 設定パラメータ

HTTP/HTTPS 統合

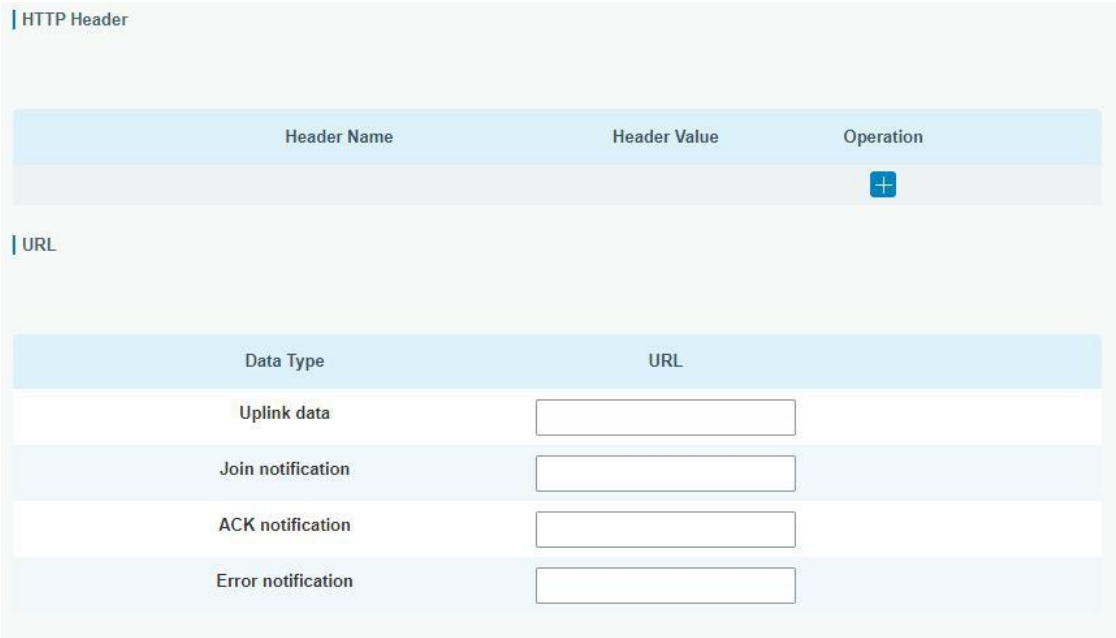


図 3-2-2-7

HTTP/HTTPS Settings	
設定項目	設定項目
HTTP Header	
Header Name	HTTPヘッダーの中核となるフィールド・セット。
Header Value	HTTPヘッダーの値。
URL	
Data Type	HTTP/HTTPS サーバーに送信されるデータ型。 **Uplink Data**：デバイスのアップリンクパケットを受信します。 **Join Notification（参加通知）**：ゲートウェイがデバイスのネットワーク参加を許可する参加アクセプト・パケットを送信した場合に、参加通知を受信します。 **ACK Notification**：ダウンリンクコマンド送信時にデバイスからACKパケットを受信 **Error Notification**：デバイスからエラーパケットを受信
Topic	パブリッシングに使用されるデータタイプのトピック名。
URL	データを受信する HTTP/HTTPS サーバの URL。

表 3-2-2-5 HTTP/HTTPS 設定パラメータ

関連設定例

アプリケーション設定

2.2.2.3 ペイロードコーデック

ペイロードコーデックは、Milesight LoRaWAN® デバイスの内蔵ペイロードコーデックライブラリを提供し、データを簡単にデコードおよびエンコードします。また、ユーザは他メーカーのデバイスのペイロードコーデックをカスタマイズしたり、 アップリンクとダウンリンクのコンテンツを要件に応じて調整することもできます。

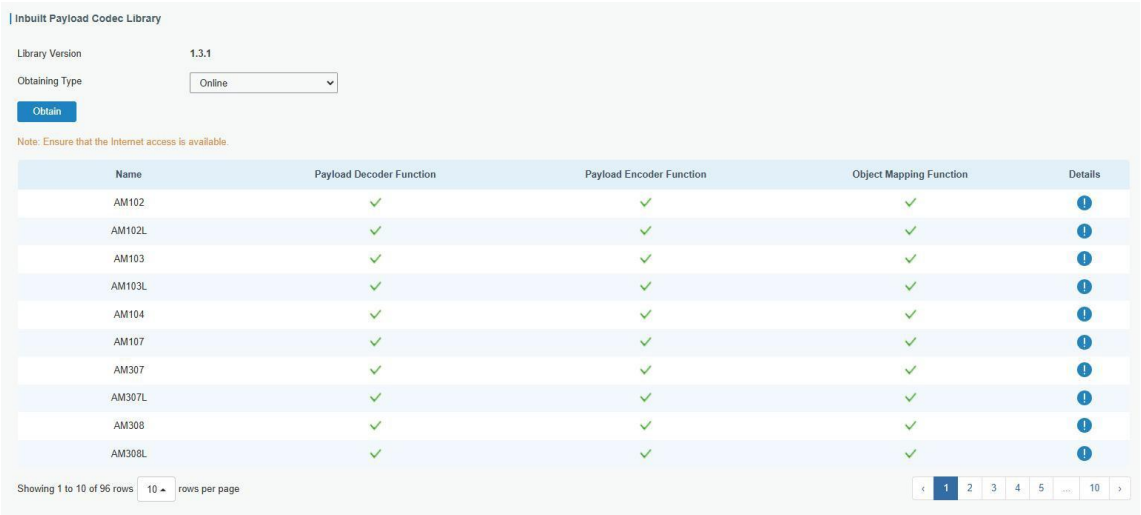


図 3-2-2-8

Inbuilt Payload Codec Library	
項目	説明
Library Version	Milesight デバイスのペイロードコーデックライブラリのバージョンを表示します。
Obtaining Type	Milesightデバイスのペイロードコーデックライブラリを更新するタイプを選択します。 **Online**：ゲートウェイの電源が入ってインターネットにアクセスするたびに、ゲートウェイがバージョン更新を検出すると自動的に更新されます。また、**[Obtain]**ボタンをクリックして手動でアップデート状況を確認することもできます。 **Local Upload**：「**Browse**」をクリックしてzip形式のペイロードコーデックパッケージをアップロードし、「**Import**」をクリックしてライブラリを更新します。Milesightペイロードコーデックパッケージは、こちらからダウンロードしてください。
Name	ペイロードコーデックの対応するMilesight製品モデルを表示します。
Payload Decoder Function	デコーダーが存在する場合に表示します。
Payload Encoder Function	エンコーダーが存在するかどうかを表示します。
Object Mapping Function	オブジェクトマッピング機能が存在するかどうかを表示します。
Details	デコーダとエンコーダの詳細を表示します。もしこれがペイロードコーデックをカスタマイズしてください。

表 3-2-2-6 内蔵ペイロードコーデックライブラリのパラメータ

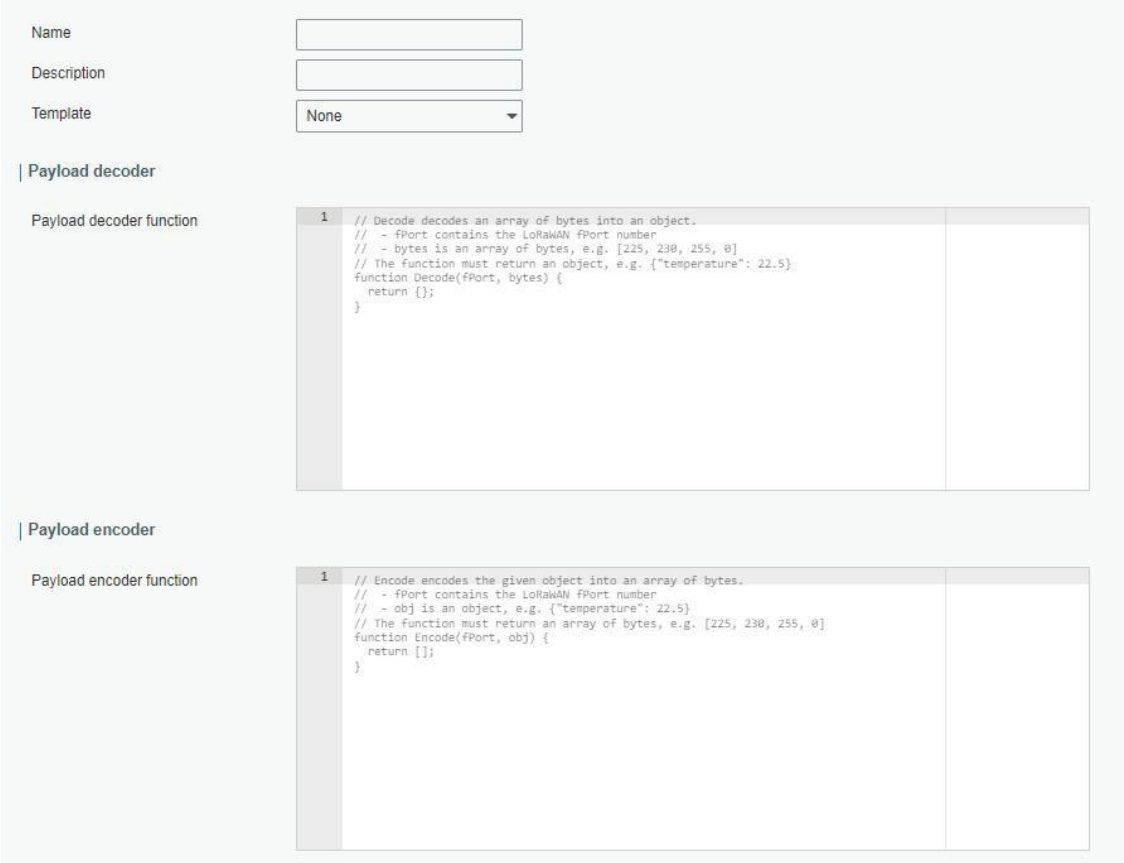

Name
Description
Template
None
Payload decoder
Payload decoder function
// Decode decodes an array of bytes into an object.
// - fPort contains the LoRaWAN fPort number
// - bytes is an array of bytes, e.g. [225, 230, 255, 0]
// The function must return an object, e.g. {"temperature": 22.5}
function Decode(fPort, bytes) {
return {};
}
Payload encoder
Payload encoder function
// Encode encodes the given object into an array of bytes.
// - fPort contains the LoRaWAN fPort number
// - obj is an object, e.g. {"temperature": 22.5}
// The function must return an array of bytes, e.g. [225, 230, 255, 0]
function Encode(fPort, obj) {
return [];
}

図 3-2-2-9

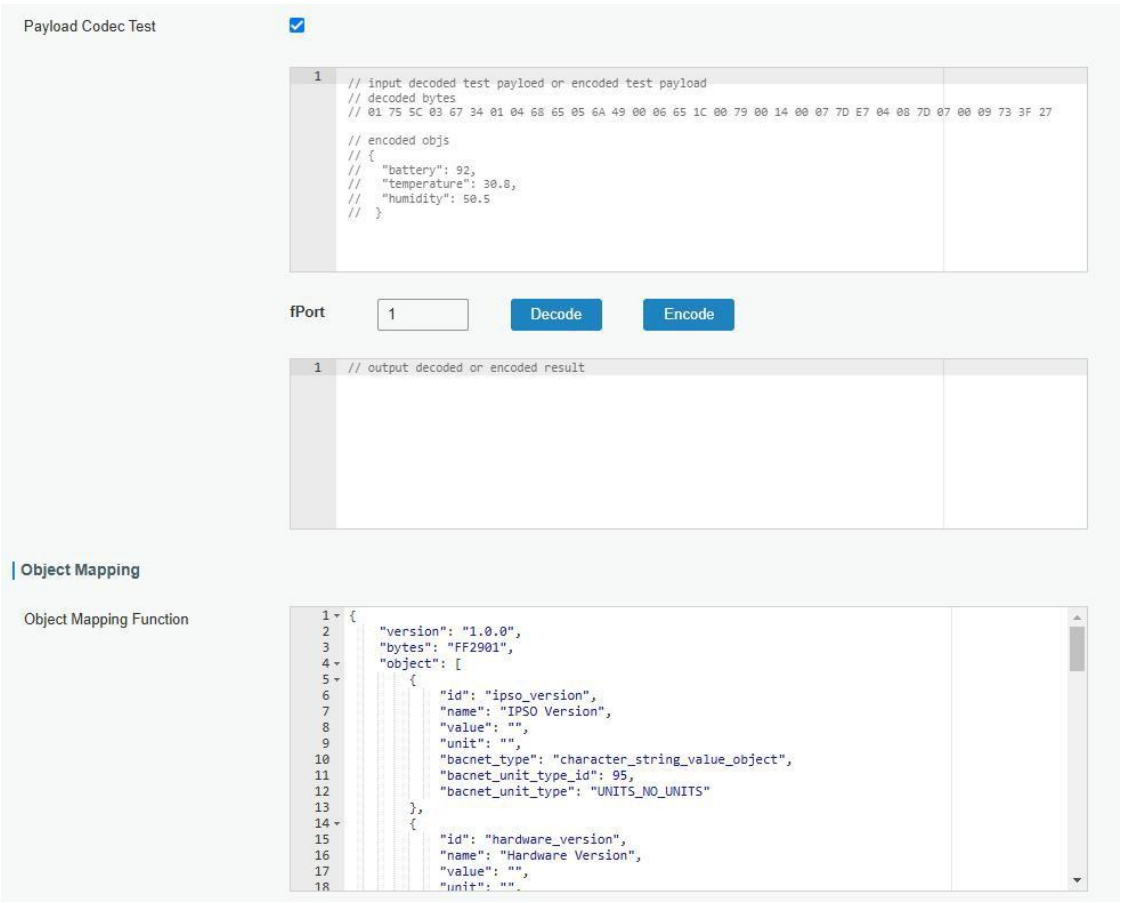

Payload Codec Test
// input decoded test payloed or encoded test payload
// decoded bytes
// 01 75 5C 03 67 34 01 04 68 65 05 6A 49 00 06 65 1C 00 79 00 14 00 07 7D E7 04 08 7D 07 00 09 73 3F 27
// encoded objs
// {
// "battery": 92,
// "temperature": 30.8,
// "humidity": 50.5
// }
fPort
1
Decode
Encode
// output decoded or encoded result
Object Mapping
Object Mapping Function
{
"version": "1.0.0",
"bytes": "FF2901",
"object": [
{
"id": "ipso_version",
"name": "IPSO Version",
"value": "",
"unit": "",
"bacnet_type": "character_string_value_object",
"bacnet_unit_type_id": 95,
"bacnet_unit_type": "UNITS_NO_UNITS"
},
{
"id": "hardware_version",
"name": "Hardware Version",
"value": "",

図 3-2-2-10

Custom Payload Codec	
項目	名称
Name	カスタムペイロードコーデックの固有の名前を入力します。
Description	このペイロードコーデックの説明を入力します。
Template	既存の内蔵ペイロードコーデックをテンプレートとして選択します。
Payload Decoder Function	16進数形式のデータをJSON形式に変換するために、デバイスのペイロードデコーダをカスタマイズします。関数ヘッダーは、空欄の例と同じでなければならないことに注意してください。
Payload Encoder Function	JSON形式のメッセージをhex形式のコマンドに変換するために、デバイスのペイロードエンコーダをカスタマイズします。関数ヘッダは、空欄の例と同じでなければならないことに注意してください。
Payload Codec Test	ペイロード・コーデック・テストを無効または有効にします。 fPortLoRaWAN® デバイスのアプリケーションポート。Milesight LoRaWAN® デバイスのデフォルトは85です。 **デコード**：16進数形式の生データを空白なしで入力し、**Decode**をクリックして結果を確認します。 **エンコードします**：JSON形式のコマンドを入力し、**Encode**をクリックして結果を確認します。 結果を確認します。
Object Mapping Function	LoRaWAN® メッセージを BACnet または Modbus オブジェクトに変換するマッピングをカスタマイズします。 またはModbusオブジェクトに変換するマッピングをカスタマイズします。詳細はこちらをご覧ください。

表 3-2-2-7 カスタムペイロードコーデックのパラメータ

注記

1. ペイロードデコーダとエンコーダのサポートするJavaScriptのバージョンはES5です。
2. 1つのペイロードコーデックのデコーダーとエンコーダーで使用される変数名は、同じ項目を指す場合、同じでなければなりません。

2.2.2.4 プロファイル

プロファイルは、LoRaWAN® 無線アクセスサービスを設定するために Netwo rk Server が必要とするデバイス能力とブートパラメータを定義するもの。これらの情報要素は、エンドデバイス製造者が提供するもの。UG65 にはあらかじめ 8 つのデバイスファイルが設定されており、ユーザは新しいデバイスプロファイルを作成することもできます。

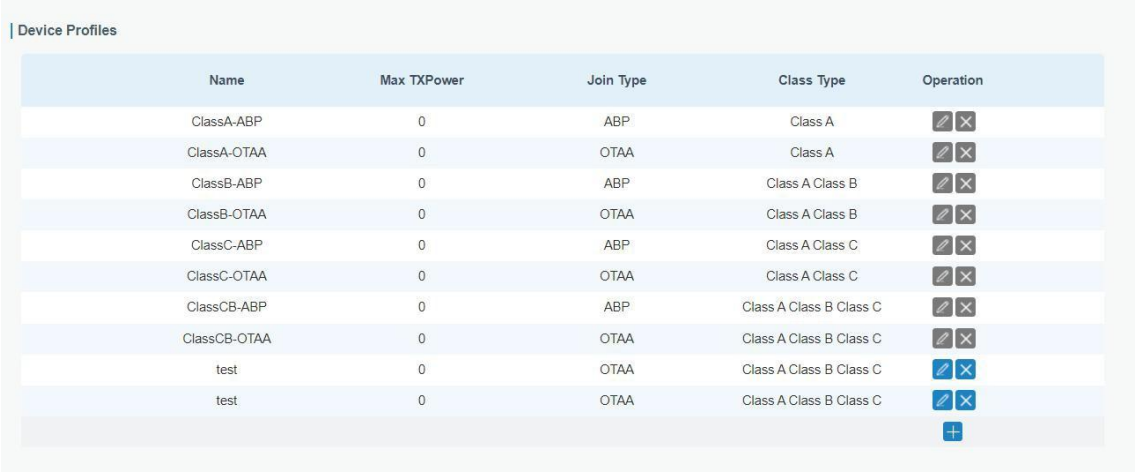


図 3-2-2-11

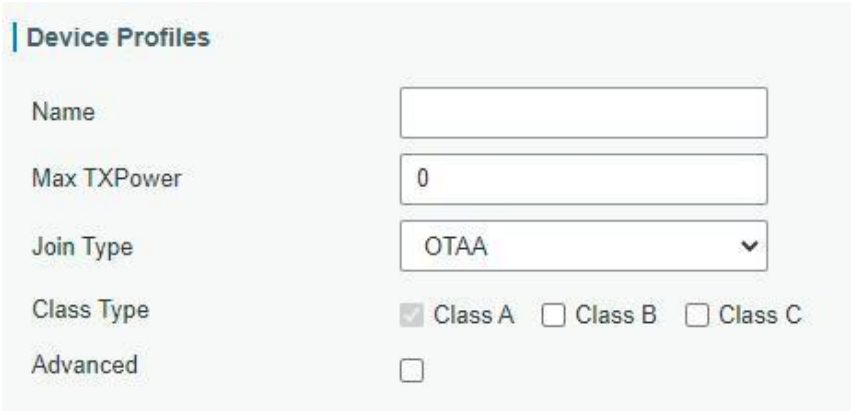


図 3-2-2-12

Device Profiles Settings	
設定項目	設定項目
Name	デバイスプロファイルの名前を入力します。
Max TXPower	最大送信電力を入力します。 TXPowerは、エンドデバイスのMax EIRPレベルに対するパワーレベルを示します。0 は最大 EIRP を使用することを意味します。EIRPとは、等方放射電力（Equivalent Isotropically Radiated Power）のことです。
Join Type	「OTAA」と「ABP」から選択します。
Class Type	クラスAは有効固定です。クラス B、クラス C にチェックを入れることで、クラスタイプを追加することができます。 注：クラス A を使用する場合は、**[Packet Forwarder] >** [Advanced] の [Beacon Period] でビーコン周期を 0 以外の値に設定する必要があります。 **Forwarder > Advancedでビーコン周期を 0 以外に設定する**必要があります。

表 3-2-2-8 デバイスプロファイル設定パラメータ

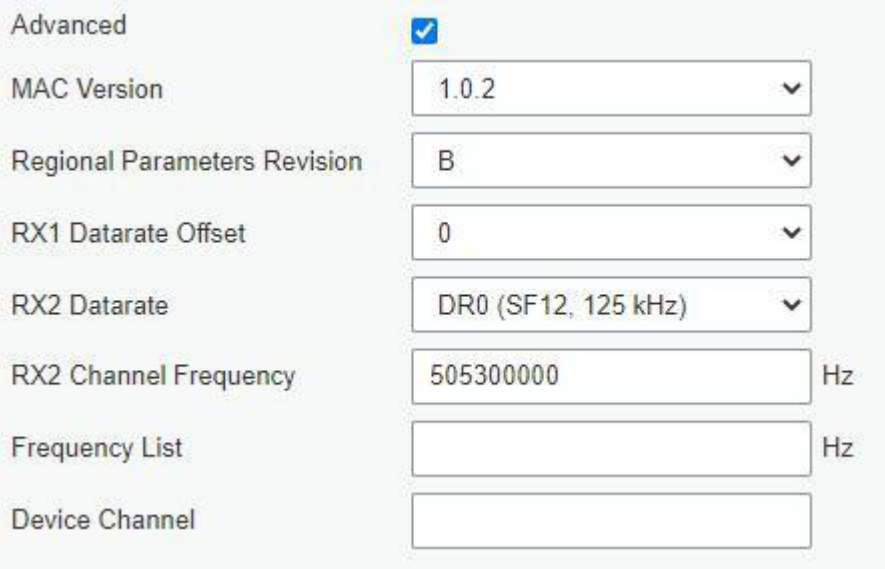


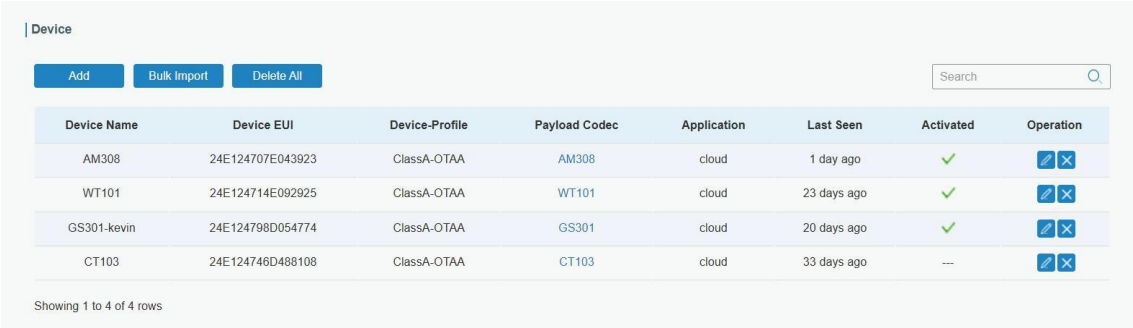
図 3-2-2-13

Device Profile Advanced Settings		
設定項目	設定項目	デフォルト
MAC Version	エンドデバイスがサポートする LoRaWAN® のバージョンを選択します。	1.0.2
Regional Parameter Revision	エンドデバイスがサポートする Regional Parameters 文書のリビジョン。	B
RX1 Datarate Offset	アップリンクデータレートに基づいて RX1 データレートを計算するために使用されるオフセット。	LoRaWAN® リージョナル・パラメータ・ドキュメントで指定されているものに基づきます。
RX2 Datarate	RX2 受信ウィンドウで使用する RX2 データレートを入力します。	
RX2 Channel Frequency	RX2 受信ウィンドウで使用する RX2 チャネル周波数を入力します。	
Frequency List	工場出荷時にプリセットされている周波数のリスト。範囲は、LoRaWAN® regional parameters document で指定されているものに基づきます。	Null
Device Channel	チャネルインデックスを入力して、このデバイス周波数チャネルを変更します。設定すると、グローバルチャネルより優先されます。この設定は CN470/US915/AU915 でのみ有効です。	Null
PingSlot Period	ピングスロットを開放する周期。	毎秒
PingSlot DataRate	ダウンリンクを受信するノードのデータレート。	サポートされている周波数に基づく
PingSlot Freq	ダウンリンクを受信するノードの周波数。	対応周波数に基づく
ACK Timeout	ダウンリンク送信の確認時間。 このオプションはクラス B とクラス C にのみ適用されます。	クラス B：10 クラス C：10

表 3-2-2-9 デバイスプロファイル詳細設定パラメータ

2.2.2.5 デバイス

デバイスとは、LoRaWAN® ネットワークに接続し、通信を行うエンドデバイスのこ



とです。

図 3-2-2-14

項目	説明
Add	デバイスを追加します。
Bulk Import	テンプレートをダウンロードし、複数のデバイスをインポートします。
Delete All	リスト内のすべてのデバイスを削除します。
Device Name	デバイス名を表示します。
Device EUI	デバイスの EUI を表示します。
Device-Profile	デバイスのデバイスプロファイル名を表示します。
Payload Codec	デバイスの使用ペイロードコーデックを表示します。クリックすると、このペイロードコーデックの詳細を確認できます。
Application	デバイスのアプリケーション名を表示します。
Last Seen	最後にパケットを受信した時刻を表示します。
Activated	デバイスのステータスを表示します。 は、デバイスがアクティブになったことを意味します。
Operation	デバイスの編集、削除を行います。

表 3-2-2-10 デバイスパラメータ

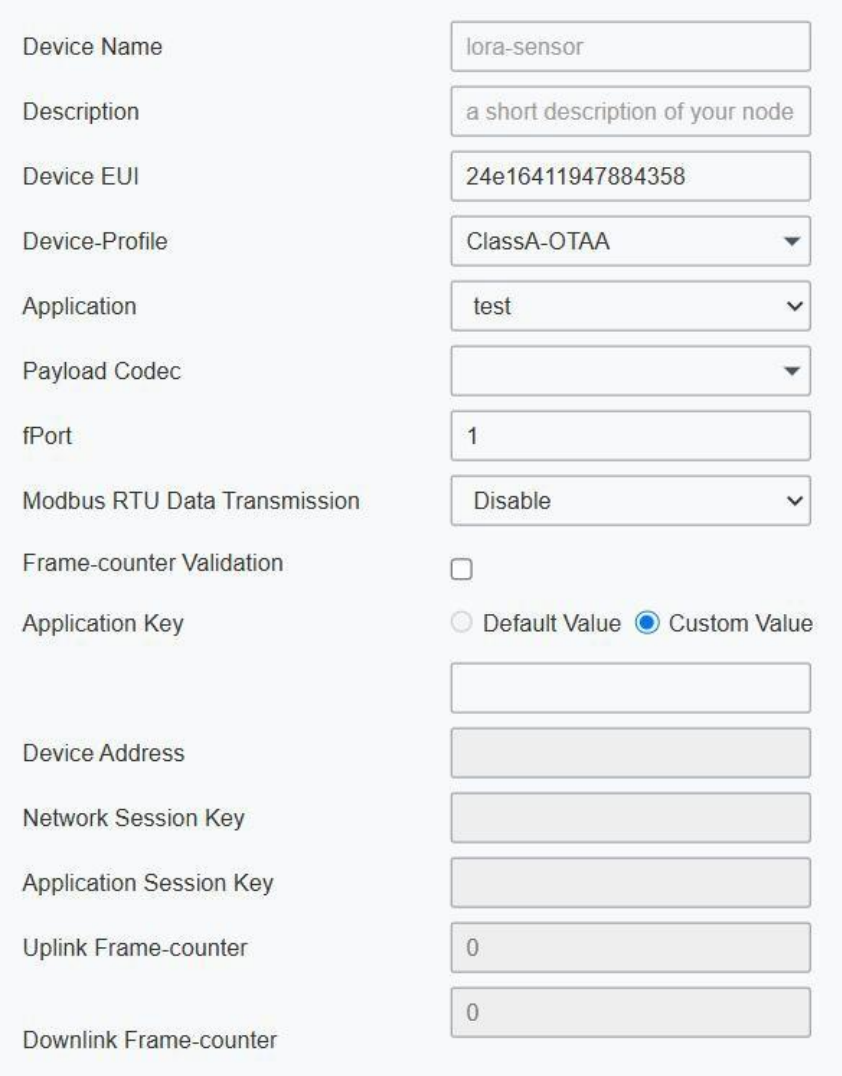


図 3-2-2-15

Device Configuration	
項目	名称
Device Name	このデバイスの名前を入力します。
Description	このデバイスの説明を入力します。
Device EUI	このデバイスの EUI を入力します。
Device-Profile	デバイスプロファイルを選択します。
Application	アプリケーション・プロファイルを選択します。
Payload Codec	ペイロードコーデックページに存在するペイロードコーデックを選択します。
fPort	デバイスのダウンリンクポートを入力します。Milesightデバイスのデフォルトは85です。
Modbus RTU Data Transmission	Disable", "Modbus RTU to TCP", "Modbus RTU over TCP" から選択します。この機能はMilesight LoRaWAN® コントローラ（UC501/UC300など）にのみ適用されます。 **Modbus RTU to TCP:** TCPクライアントはコントローラのModbusデータを要求するためにModbus TCPコマンドを送信できます。 **Modbus RTU over TCP:** TCP クライアントがコントローラの Modbus データを要求するために Modbus RTU コマンドを送信できます。

Modbus RTU Fport	Milesight LoRaWAN® コントローラと UG65 間のトランスペアレント伝送用の LoRaWAN® フレームポートを入力します。 範囲：2-84、86-223。 注意：この値はMilesight LoRaWAN® コントローラのfPortと同じである必要があります。
TCP Port	TCPクライアントとUG65（TCPサーバーとして）間のデータ伝送用のTCPポートを入力します：1-65535.
Frame-Counter Validation	フレームカウンタ検証を無効にすると、リプレイアタックが可能になるため、セキュリティが損なわれます。
Application Key	エンドデバイスが無線アクティベーションによってネットワークに参加するたびに、アプリケーション・キーがアプリケーション・セッション・キーの導出に使用されます。 **デフォルト値：**Milesightエンドデバイスのデフォルト値は5572404C696E6B4C6F5261323031 3823です。 **カスタム値：**エンドデバイスに応じてappkeyを定義します。
Device Address	デバイス・アドレスは現在のネットワーク内のエンドデバイスを識別します。
Network Session Key	エンド・デバイス固有のネットワーク・セッション・キー。エンド・デバイスがすべてのアップリンク・データ・メッセージの MIC または MIC の一部（メッセージ整合性コード）を計算し、データの整合性を確保するために使用します。
Application Session Key	AppSKey は、エンド・デバイス固有のアプリケーション・セッション・キーです。アプリケーション・サーバーとエンド・デバイスの両方が、アプリケーション固有のデータ・メッセージのペイロード・フィールドを暗号化および復号化するために使用します。
Uplink Frame-counter	ネットワーク・サーバーにアップリンク送信されたデータ・フレームの数。 エンド・デバイスによってインクリメントされ、エンド・デバイスによって受信されます。 エンド・デバイスのフレーム・カウンターとネットワーク・サーバーのフレーム・カウンターは0にリセットされます。
Downlink Frame-counter	エンド・デバイスがネットワーク・サーバーからダウンリンクで受信したデータ・フレームの数。ネットワーク・サーバーによってインクリメントされます。 エンドデバイスのフレームカウンタとネットワークサーバーのフレームカウンタは0にリセットされます。

表 3-2-2-11 デバイス設定パラメータ

関連設定例

機器設定

2.2.2.6 FUOTA

FUOTA（Firmware Update Over the Air）は、ユニキャストまたはマルチキャストを使用して、ファームウェアの更新をエンドデバイスに配信するための規格です。**この機能を使用する前に、エンドデバイスが標準 LoRaWAN® FUOTA プロトコルをサポートしていることを確認してください。**

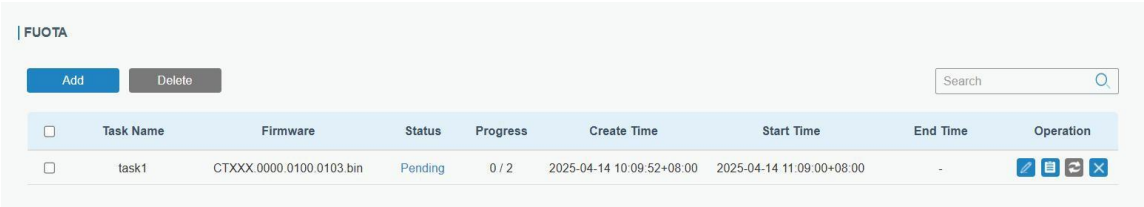


図 3-2-2-16

FUOTA	
項目	項目 説明
Add	タスクを追加します。
Delete	タスクリストのボックスにチェックを入れ、クリックするとタスクが削除されます。
Task Name	タスクの名前。
Firmware	このタスクでアップグレードするファームウェア。
Status	タスクのステータス。 **Pending**：タスクの処理予定時間を待ちます。 **Waiting**：アップグレードのためのセッション作成の準備。 **Executing**：少なくとも 1 台のデバイスがアップグレード結果に返信しています。 **Finished**：全機器がアップグレード結果を返信（成功・フェイルを含む）。
Progress	アップグレードに成功した/アップグレードを予定している機器の台数。
Create Time	このタスクを作成した時間。
Start Time	このタスクを開始した時間。
End Time	このタスクが完了する時間。
Operation	:タスクステータスが「保留」の場合、このタスクを編集します。 :タスクの詳細を確認します。 タスクがフェイルの場合、アップグレードに失敗した機器にタスクを再試行します。 :タスクステータスが "Pending "または "Finished "の場合、タスクを削除します。

表 3-2-2-12 FUOTA パラメータ

FUOTA タスクの追加

1. **Add** ボタンをクリックし、FUOTA タスクを追加します。

2. タスクの設定を行います。

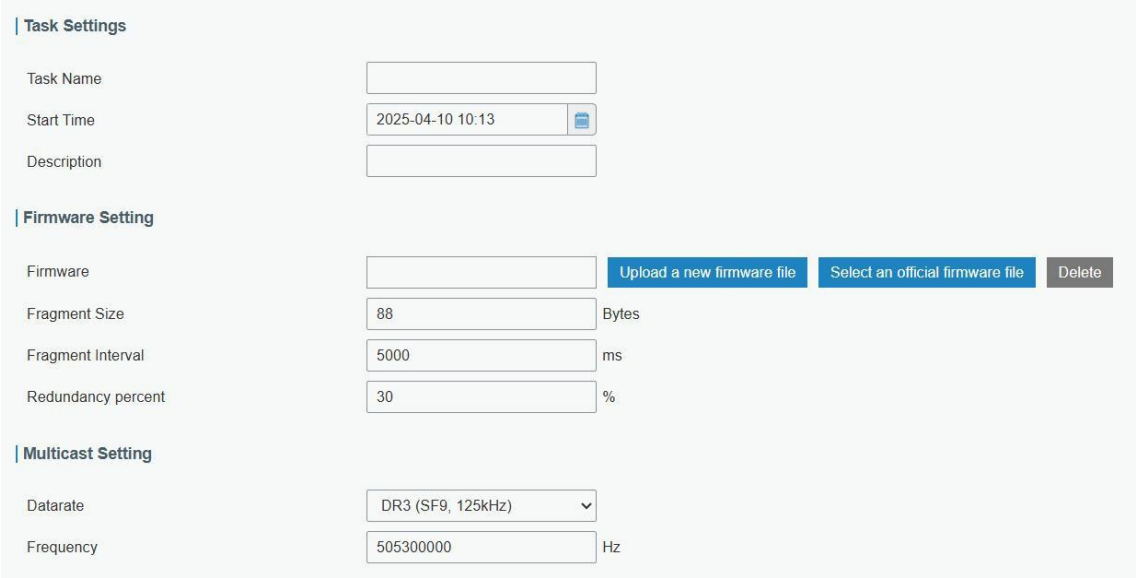
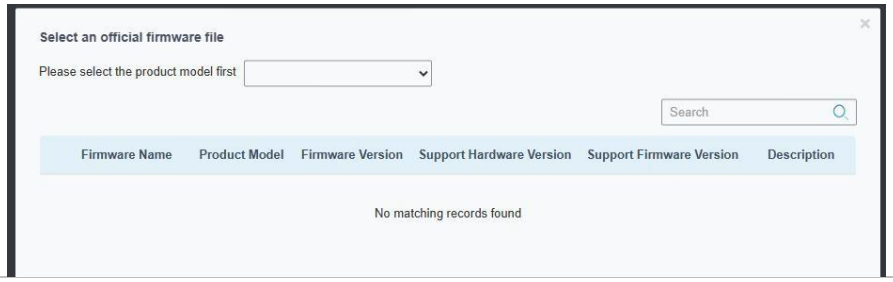


図 3-2-2-17

Add Task Settings	
項目	内容
Basic Information	
Task Name	タスク名をカスタマイズします。
Start Time	タスクの開始時間を設定します。
Description	このタスクの説明を入力します。
Firmware Settings	
Firmware	アップグレードするファームウェアをインポートします。 **Upload a new firmware file**：ローカルにファームウェアをインポートします。 **Select an Official Firmware file**：最初に製品モデルを選択し、公式ウェブサイトからダウンロードするファームウェアを選択します。ゲートウェイがインターネットにアクセスできる必要があります。 
Fragment Size	ファームウェアファイルはこのサイズで分割され、デバイスに割り当てられます。通常はこの値をデフォルトとしてください。 ネットワーク環境が複雑または悪い場合は、この値を**64**またはそれ以下にすることをお勧めします。
Fragment Interval	ファームウェアのフラグメントをデバイスに割り当てる間隔。通常はこの値をデフォルトのままにしてください。 ネットワーク環境が複雑または悪い場合は、この値を**3**以下にすることをお勧めします。ネットワーク環境が良い場合は、この値を増やして伝送速度を向上させることができます。

Redundancy Percent	ファームウェアファイルのパケット補正のために、デバイスは30%の冗長パケットを送信します。通常はこの値をデフォルトとしてください。 ネットワーク環境が複雑または悪い場合は、この値を20%またはそれより低い値に下げることをお勧めします。
Multicast Settings	
Datarate	ファームウェアのフラグメントをデバイスに割り当てるDatarate。
Frequency	ファームウェア・フラグメントをデバイスに割り当てるダウンリンク周波数。

表 3-2-2-13 タスクパラメータ

3. 本タスクを実行する機器を選択します。同一機種の機器を選択してください。

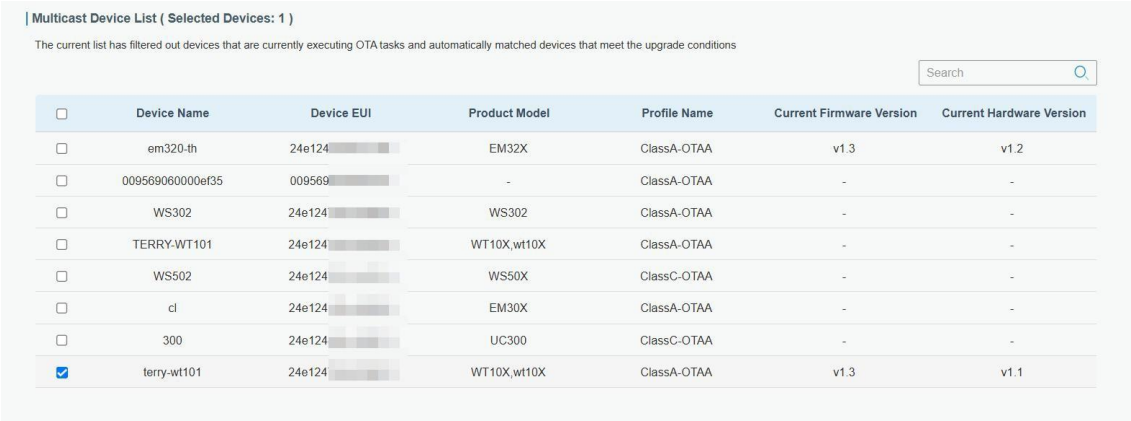
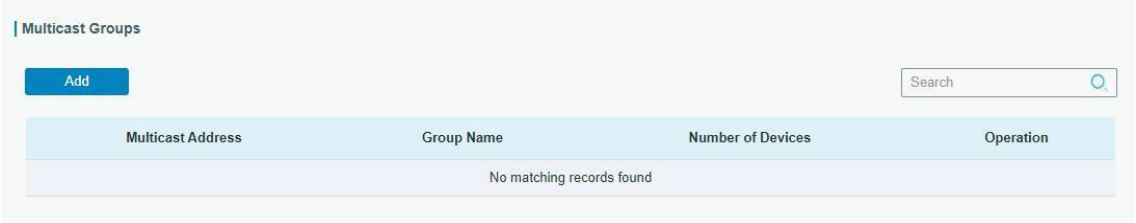


図 3-2-2-18

4. **Save** をクリックし、タスクの設定を保存します。

2.2.2.7 マルチキャストグループ

Milesight ゲートウェイは、クラス B またはクラス C マルチキャストグループを作成し、エンドデバイ スのグループにダウンリンクメッセージを送信することがで



きます。マルチキャストグループは仮想ABPデバイス（すなわち共有セッションキー）であり、アップリンク、確認済みダウンリンク、およびMACコマンドをサポートしません。

図 3-2-2-19

項目	説明
Add	マルチキャストグループを追加します。

Group Name	グループ名を表示します。
Number of Devices	グループのデバイス番号を表示します。
Operation	マルチキャストグループの編集、削除を行います。

表 3-2-2-14 マルチキャストグループパラメータ

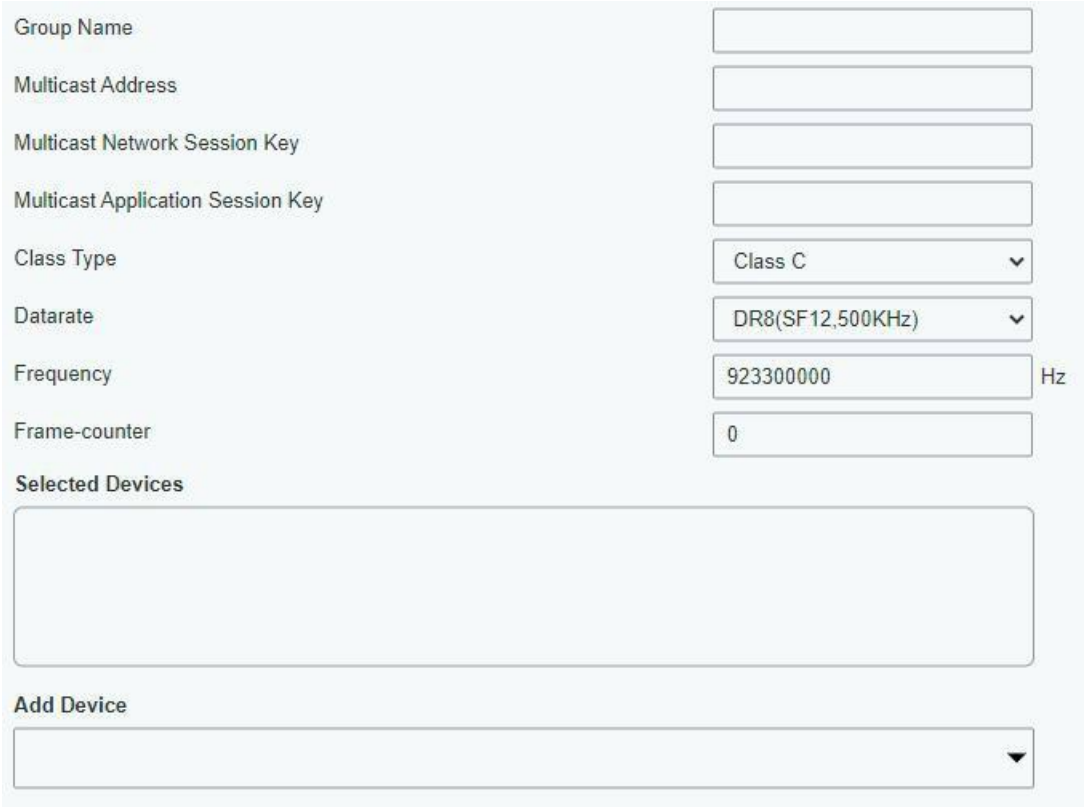


図 3-2-2-20

Multicast Group Configuration	
設定項目	設定項目
Group Name	このマルチキャストグループの名前を入力します。
Multicast Address	このグループ内のすべてのデバイスのデバイスアドレス（Dev Addr）。
Multicast Network Session Key	このグループ内のすべてのデバイスのネットワークセッションキー（Netwks Key）。
Multicast Application Session Key	このグループ内のすべてのデバイスのアプリケーションセッションキー（AppSKey）。
Class Type	クラスBとクラスCはオプションです。
Datarate	ダウンリンクを受信するノードのDatarate。
Frequency	このグループ内の全デバイスのダウンリンク周波数。
Frame-counter	ネットワーク・サーバーからダウンリンクしたエンド・デバイスが受信したデータ・フレームの数。ネットワーク・サーバーによってインクリメントされます。
Ping Slot Periodicity	ピングスロットを開く周期。これはクラス B エンド・デバイスにのみ適用されます。
Selected Devices	このグループ内のすべてのデバイス名を表示します。

Add Device	プルダウンリストからデバイスを追加します。

表 3-2-2-15 マルチキャストグループ設定パラメータ

2.2.2.8 ゲートウェイ群

Milesight ゲートウェイは UG65 ネットワークサーバーに接続することができます。ゲートウェイは最大 100 台まで追加可能です。

図 3-2-2-21

設定項目	ゲートウェイID
Gateway ID	ゲートウェイ ID を表示します。
Name	ゲートウェイの名前を表示します。
Status	ゲートウェイの接続ステータスを表示します。
Last Seen	最後にパケットを受信した時刻を表示します。
Operation	ゲートウェイの編集または削除を行います。

表 3-2-2-16 ゲートウェイフリートパラメータ

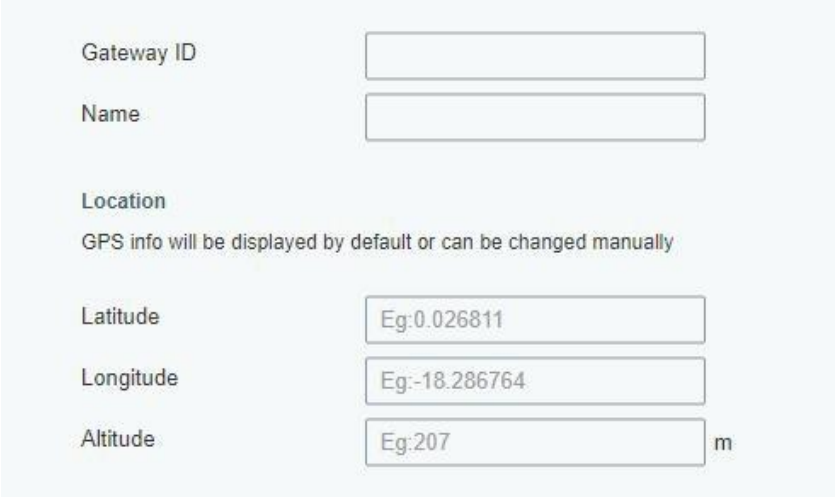


図 3-2-2-22

項目	項目
Gateway ID	ゲートウェイを認識するための固有のゲートウェイ ID を入力します。
Name	このゲートウェイの名前を入力します。
Location	ゲートウェイのGPSデータを編集できます。ゲートウェイがGPSデータを送信する場合、カスタマイズしたデータに置き換わります。

表 3-2-2-17 ゲートウェイ設定パラメータ

2.2.2.9 パケット

ゲートウェイは、最新 1000 個のパケットを表示し、機器にコマンドを送信します。

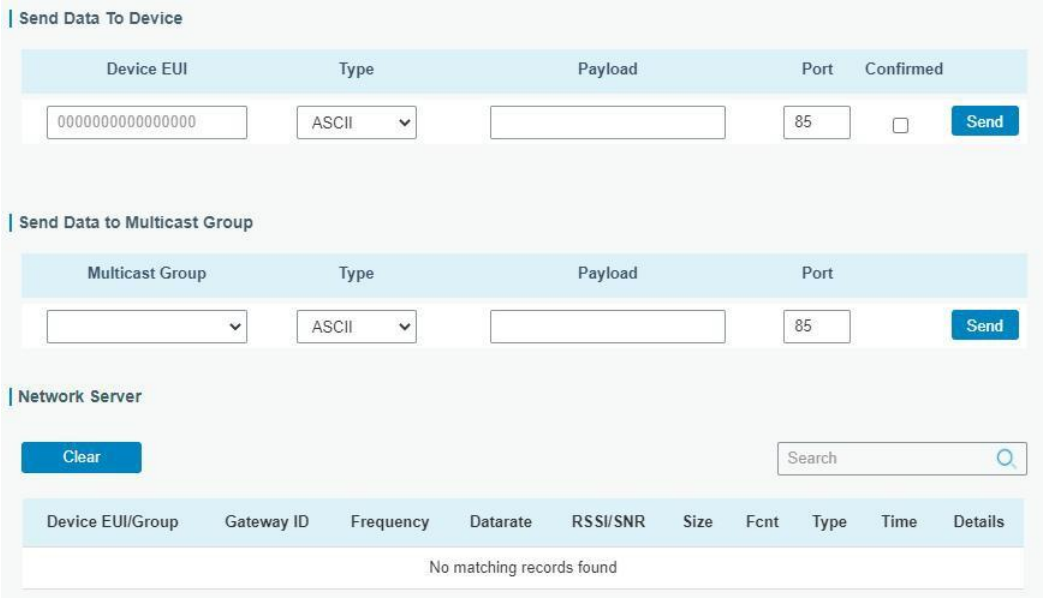


図 3-2-2-23

Send Data To Device/Multicast Group	
設定項目	項目 内容
Device EUI	ペイロードを受信するデバイスの EUI を入力します。
Multicast Group	ダウンリンクを送信するマルチキャストグループを選択します。マルチキャストグループは「**Multicast Groups**」タブで追加できます。
Type	ペイロード入力ボックスに入力するペイロードのタイプを選択します：ASCII、Hex、base64。
Payload	このデバイスに送信するメッセージを入力します。
Port	デバイスとネットワークサーバー間のパケット伝送に使用する LoRaWAN® フレームポートを入力します。
Confirmed	有効化後、エンドデバイスはダウンリンクパケットを受信し、ネットワークサーバーに "confirmed "と応答する必要があります。マルチキャスト機能は確認済みダウンリンクに対応していません。

表 3-2-2-18 デバイスへのデータ送信パラメータ

Network Server	
項目	説明
Device EUI/Group	デバイスまたはマルチキャストグループの EUI を表示します。
Frequency	パケット送信に使用する周波数を表示します。
Datarate	パケット送信に使用するデータレートを表示します。
SNR	SN比を表示します。
RSSI	受信信号強度インジケータを表示します。
Size	ペイロードのサイズを表示します。
Fcnt	フレームカウンタを表示します。
Type	パケットのタイプを表示します： JnAcc - Join Accept パケット。

	JnReq - 参加要求パケット UpUnc - アップリンク未確認パケット UpCnf - アップリンク確認済みパケット - ネットワークからの ACK 応答が要求されました。 DnUnc - ダウンリンク未確認パケット DnCnf - ダウンリンク確認済みパケット-要求されたエンドデバイスからのACK応答
Time	パケットの送受信時刻を表示します。

表 3-2-2-19 パケットパラメータ

をクリックすると、パケットの詳細が表示されます。

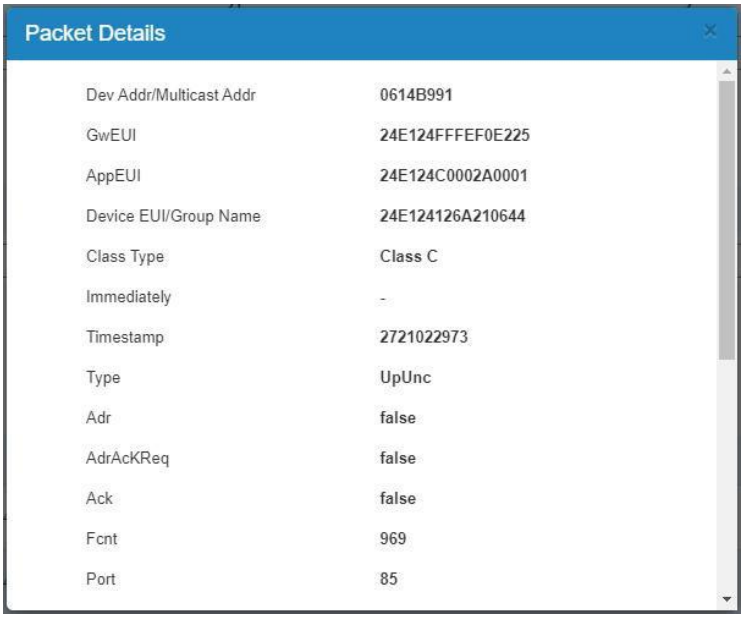


図 3-2-2-24

項目	説明
Dev Addr/Multicast Addr	デバイス／マルチキャストグループのアドレスを表示します。
GwEUI	ゲートウェイの EUI を表示します。
AppEUI	エンドデバイスの App EUI を表示します。
DevEUI/Group Name	デバイス/マルチキャストグループ名の EUI を表示します。
Class Type	デバイスまたはマルチキャストグループのクラスタイプを表示します。
Immediately	このダウンリンクパケットをすぐに送信するかどうか。
Timestamp	パケットフォワーダ起動後、このパケットを受信するまでの時間を表示します。単位：ms
Type	パケットのタイプを表示します： JnAcc - 参加受付パケット JnReq - 参加要求パケット UpUnc - アップリンク未確認パケット

	UpCnf - アップリンク確認済みパケット - ネットワークからの ACK 応答が要求されました。 DnUnc - ダウンリンク未確認パケット DnCnf - ダウンリンク確認済みパケット - 要求されたエンドデバイスからの ACK 応答
Adr	True: エンドノードが ADR を有効にしました。 偽：エンドノードは ADR を有効にしていません。
AdrAcKReq	ネットワークがアップリンク・メッセージを受信していることを検証するために、ノードは ADRACKReq メッセージを定期的に送信します。これは 1 ビット長です。True: アップリンク・メッセージを受信していることを確認するために、ネットワークは ADR_ACK_DELAY 時間内に応答する必要があります。 False：ADR が無効であるか、ネットワークが ADR_ACK_DELAY 時間内に応答しない場合。
Ack	True：このフレームは ACK です。 False: このフレームは ACK です：このフレームは ACK ではありません。
Fcnt	ネットワークサーバーはアップリンクフレームカウンターを追跡し、各エンドデバイスのダウンリンクカウンターを生成します。
FPort	このパケットを送信する FPort。このパケットがMACコマンドである場合、ポートは0です。このパケットがアプリケーション・データを含む場合、ポートは0ではありません（1-233）。
Modulation	物理層がLoRa変調を使用することを意味します。
Bandwidth	このチャネルの帯域幅を表示します。
SpreadFactor	このチャネルのSpreadFactorを表示します。
Bitrate	このチャンネルのビットレートを表示します。
CodeRate	このチャンネルのコードレートを表示します。
SNR	このチャンネルの SNR を表示します。
RSSI	このチャンネルの RSSI を表示します。
Power	デバイスの送信電力を表示します。
Payload (b64)	このパケットのアプリケーションペイロードを表示します。
Payload (hex)	このパケットのアプリケーションペイロードを表示します。
Json	デコード後のデータを表示します。
MIC	このパケットのMICを表示します。MICは暗号化されたメッセージ整合性コードで、MHDR、FHDR、FPort、および暗号化されたFRMPayloadのフィールド上で計算されます。

表 3-2-2-20 パケット詳細パラメータ

関連トピック

デバイスへのデータ送信

2.3 プロトコル統合

2.3.1 BACnetサーバー

UG65はLoRaWAN to BACnetゲートウェイとして動作し、BMSシステムと簡単に統合することができます。

この機能を使用する前に、内蔵ペイロードコーデックライブラリのバージョンが最新であり、対応するLoRaWAN® デバイスに正しいペイロードコーデックが追加されていることを確認してください。

2.3.1.1 サーバ

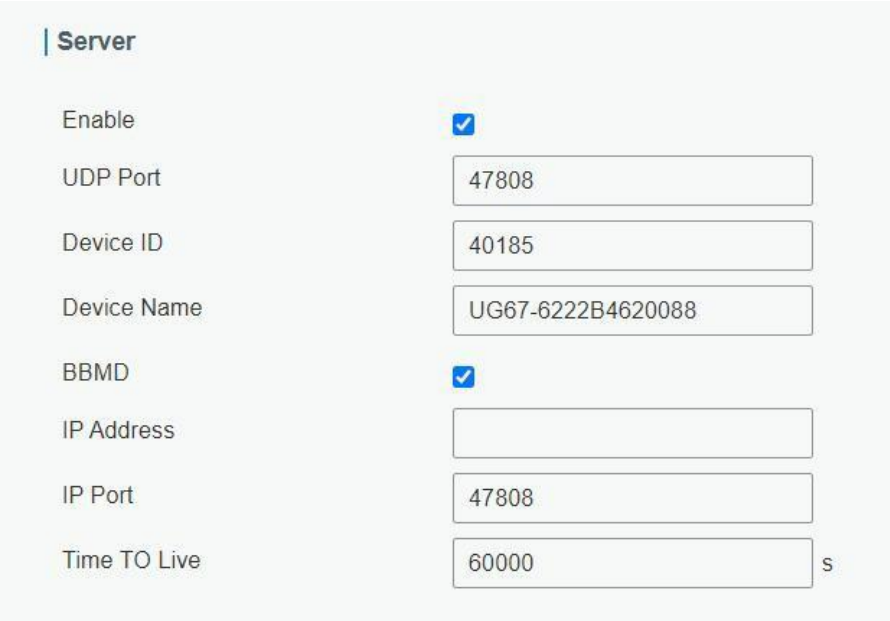


図 3-3-1-1

Server Settings	
設定項目	設定項目
Enable	BACnet サーバー機能を有効または無効にします。
UDP Port	BACnet/IP の通信ポートを設定します。範囲：1-65535.デフォルトは47808です。
Device ID	他の機器との競合を避ける必要がある、固有のBACnet機器識別子。
Device Name	デバイスを表すデバイス名。
BBMD	異なるネットワークサブネットのBACnetデバイスが一緒に動作する必要がある場合、BBMD(BACnet/IP Broadcast Management Device)を有効にします。
IP Address	BBMDデバイスまたは外部デバイス登録機関のIPアドレスを入力します。
IP Port	外部機器登録用のUDP/IPポートを入力します。
Time TO Live	外部機器登録で使用する秒数です。

表 3-3-1-1 サーバーパラメーター

2.3.1.2 BACnet オブジェクト

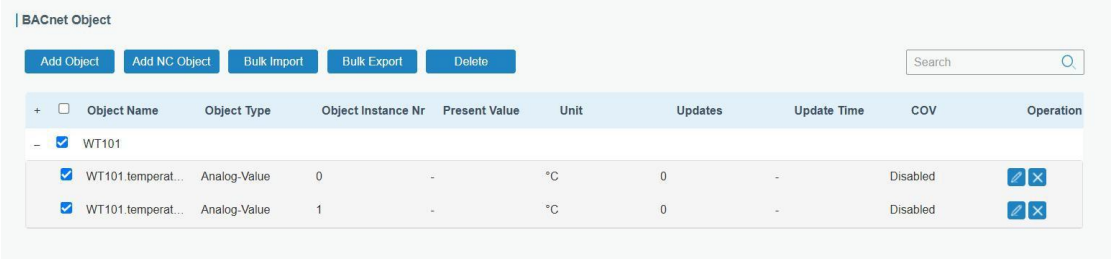


図 3-3-1-2

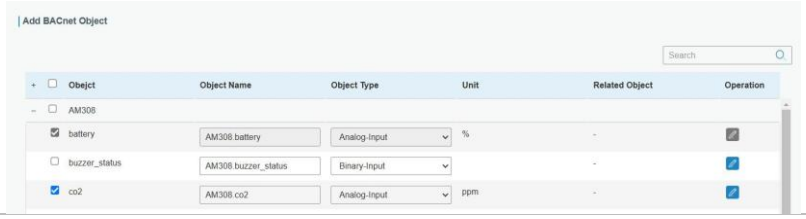
項目	説明
Add Object	このサーバーに追加するオブジェクトを選択します。ゲートウェイは最大 2000 オブジェクトの追加をサポートします。 注：ペイロードコーデックの内容が正しく、デバイスが正しいペイロードコーデックを選択していることを確認してください。 
Add NC Object	アラームの受信者を決定する Notification-Class タイプのオブジェクトを追加します。ゲートウェイは最大 200 の NC オブジェクトの追加をサポートします。
Bulk Import	複数のBACnetオブジェクトをインポートするためのテンプレートをダウンロードします。
Bulk Export	.xlsx形式のファイルとしてエクスポートするオブジェクトを選択します。
Delete	削除したいオブジェクトを選択します。
Object Name	BACnetオブジェクトの名前を表示します。
Object Type	オブジェクトのタイプを表示します。
Object Instance Nr	このオブジェクトのインスタンス番号を表示します。
Present Value	オブジェクトの最新値を表示します。
Units	このオブジェクトの値の単位を表示します。
Updates	このオブジェクトの値の更新時間を表示します。
Update time	このオブジェクトがデータを取得して更新するまでの時間を表示します。
COV	COV（値の変更）が有効かどうかを表示します。
Operation	オブジェクトの編集、削除を行います。

表 3-3-1-2 BACnet オブジェクトリストパラメータ

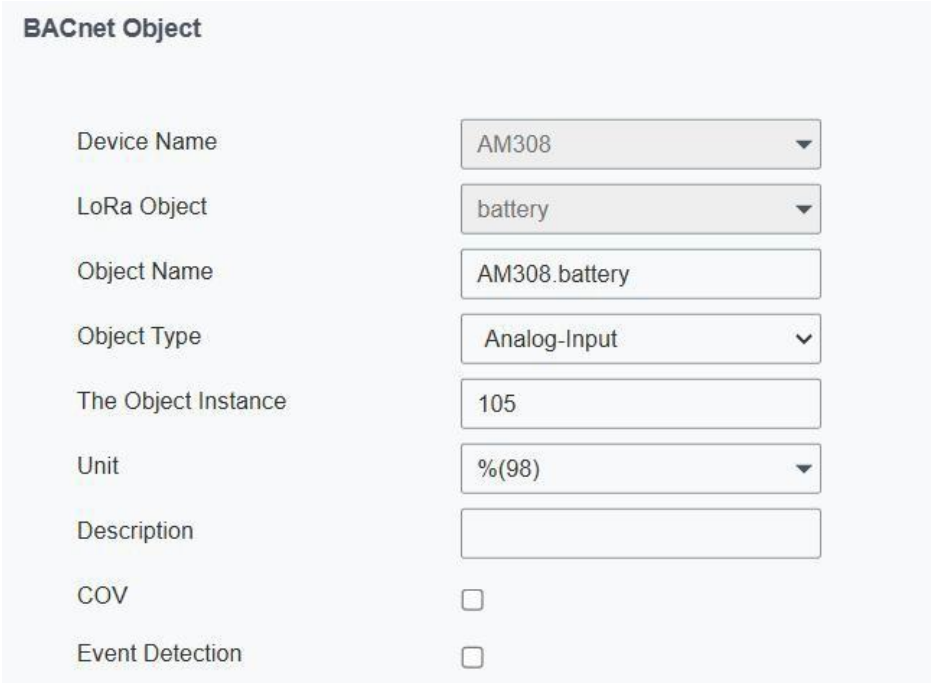


図 3-3-1-3

BACnet Object Configuration	
項目	説明
Device Name	デバイス名を表示します。
LoRa Object	LoRa オブジェクトの対応する名前を表示します。
Object Name	このオブジェクトの固有の名前をカスタマイズします。
Object Type	オブジェクトのタイプをバイナリ入出力値、アナログ入出力値、マルチステート入出力値、文字列値から選択します。
The Object Instance	オブジェクト・インスタンスをカスタマイズします。
Description	このオブジェクトの説明を入力します。
Event Detection	この値のアラーム報告を有効にします。少なくとも通知クラスオブジェクトを定義する必要があります。
Analog Input/Output/Value	
Units	このオブジェクトの値の単位を選択します。
COV	オブジェクトの値が変更されると、BACnetサーバー（ゲートウェイ）は新しい値の通知をBACnetクライアントに送信します。アナログタイプのオブジェクトにのみ適用されます。
COV Increment	オブジェクト値がこの増分値以上になったときのみ、BACnetサーバー（ゲートウェイ）は通知を送信します。
Relinquish Default	コマンドがない場合、アナログ出力はこのデフォルト値として設定されます。
Binary Input/Output/Value	
Polarity	バイナリ入出力の状態をノーマルまたはリバースとして定義します。
Active Text	バイナリ型オブジェクト値のアクティブ状態の効果を指定します。

	例：ボタンが押され、バイナリ入力が1の場合、アクティブテキストは "Pressed "と定義できます。
Inactive Text	バイナリ型オブジェクト値の非アクティブ状態の意図された効果を表します。**例：**ボタンの場合、非アクティブテキストは "Unpressed "と定義できます。
Relinquish Default	コマンドがない場合、バイナリ出力はこの放棄デフォルト値として設定されます。
MultiState Input/Output/Value	
Number of States	ステートの数を設定し、各ステートの名前を定義します。
Relinquish Default	コマンドがない場合、マルチステート出力はこの放棄デフォルト値として設定されます。
Event Detection	
Notification Class	このアラームの受信者を決定する通知クラスを選択します。
Event	通知するイベントタイプを選択します。
Limit Event	オブジェクトタイプがアナログタイプの場合、上限または下限に達したときにイベントを報告するかどうかを選択します。
Deadband	To Offnormalステータスの下で、電流値が（上限-デッドバンド）値または（下限＋デッドバンド）値に遅延時間内に戻ったとき、デバイスはTo Normalイベントを生成します。アナログタイプのみこのオプションがあります。
Time Delay	電流値がしきい値と一致した時、またはしきい値から外れた時にのみ、デバイスは対応するイベントを報告します。
Alarm Value	現在値が遅延時間のアラーム値と等しい場合、To Offnormalイベントを報告し、現在値が遅延時間のアラーム値と等しくない場合、To Normalイベントを報告します。バイナリ入力、バイナリ値、マルチステート入力、マルチステート値のみこのオプションがあります。
Fault Value	現在値がフォルト値と等しい場合に、To Faultイベントを報告します。マルチステート入力またはマルチステート値のみこのオプションがあります。
Feedback Value	現在の値が遅延時間のフィードバック値と等しいときはOffnormal イベントを報告し、現在の値が遅延時間のフィードバック値と等しくないときは Normal イベントを報告します。マルチステート出力またはバイナリ出力にのみこのオプションがあります。
Notification Type	通知タイプを Alarm または Event から選択します。

表 3-3-1-3 BACnet オブジェクト設定パラメータ

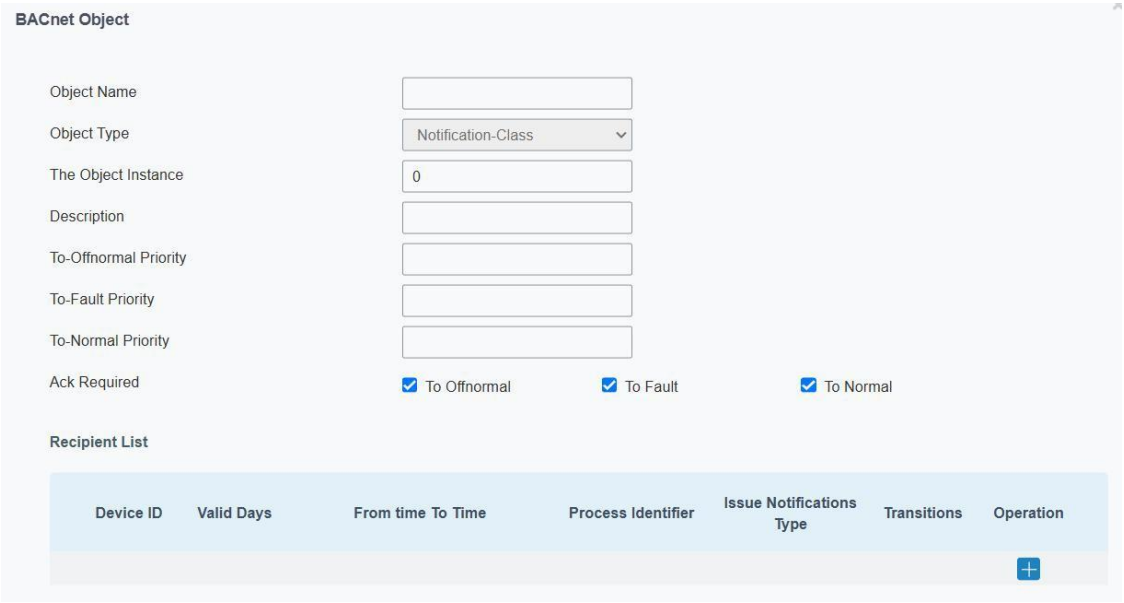


図 3-3-1-4

Notification Class BACnet Object Configuration	
項目	説明
Object Name	このオブジェクトの固有の名前をカスタマイズします。
Object Type	Notification-Classとして固定です。
The Object Instance	オブジェクトのインスタンスをカスタマイズします。
Description	このオブジェクトの説明を入力します。
To-Offnormal Priority	受信者がイベント通知をソートするために使用する優先順位の番号を設定します。範囲：0～255（0は最も重要、255は最も重要でない）。
To-Fault Priority	
To-Normal Priority	
Ack Required	このイベントで受信者がゲートウェイに確認アラームメッセージを返送する必要があるかどうかを指定します。
Recipient List	イベント検出が有効で、この通知クラスが選択されている場合、イベント通知はこのリストの受信者に送信されます。1つのリストには最大10人の受信者を追加できます。 **Device ID:** ターゲットの受信者のデバイスID。 **Valid Days**：通知を送信する有効日。 **From time to time**：通知を送信するのに有効な時間。 **Process Identifier**：アラームがどのプロセスを対象としているかを示す識別子。例えば、プロセス識別子1はメンテナンスアラーム、2は重要アラーム、3は生命安全アラームなどを意味します。 **Issue Notifications Type**：通知タイプを確認済みまたは未確認から選択します。ゲートウェイが確認済み通知の応答を受信しない場合、再度通知を送信します。 **Transitions**： 報告されるイベントタイプを選択します。

表 3-3-1-4 通知クラス BACnet オブジェクト設定パラメータ

2.3.2 Modbus サーバー

ゲートウェイは Modbus サーバー（スレーブ）として動作し、PLC/BMS システムから Modbus RTU または Modbus TCP コマンドを受信し、LoRaWAN® デバイスを読み書きできます。この機能を使用する前に、内蔵ペイロードコーデックライブラリのバージョンが最新であり、対応する LoRaWAN® デバイスに正しいペイロードコーデックが追加されていることを確認してください。

2.3.2.1 サーバ

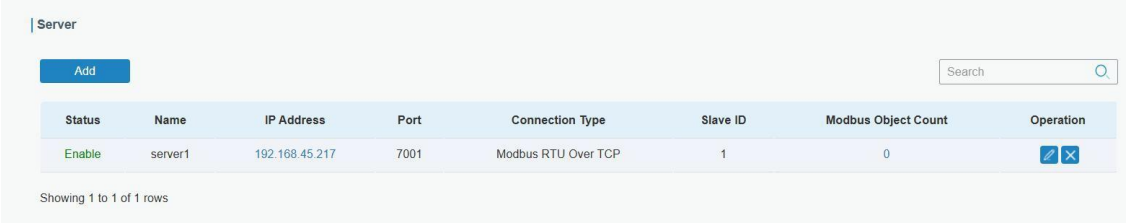


図 3-3-2-1

項目	説明
Add	Modbus サーバ（スレーブ）を追加します。つのゲートウェイで最大 15 台のサーバを追加できます。
Status	このサーバーの有効ステータスを表示します。
Name	サーバー名を表示します。
IP Address	IPアドレスを表示します。
Port	このサーバーの通信ポートを表示します。
Connection Type	接続タイプを表示します。
Sever ID	このサーバーのサーバー ID を表示します。
Modbus Object Count	このサーバーの Modbus オブジェクト数を表示します。
Operation	このサーバーの編集、削除を行います。

表 3-3-2-1 サーバーパラメータ

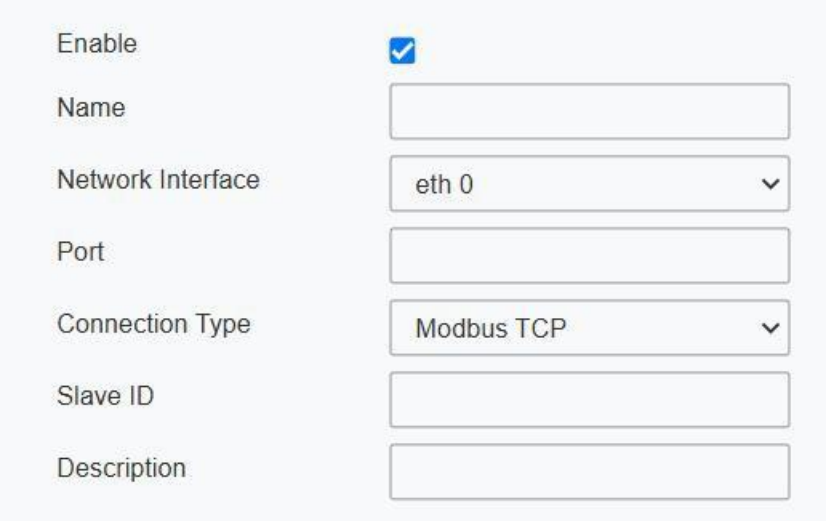


図 3-3-2-2

Server Settings	
項目	設定項目
Enable	この Modbus サーバーを有効または無効にします。
Name	このサーバーを識別するための固有の名前をカスタマイズします。
Network Interface	このサーバーが Modbus クライアント（マスター）と通信するためのネットワーク・インターフェイスを選択します。デバイスは、異なるリモート・プラットフォームと通信するために異なるネットワーク・インターフェイスを使用することをサポートしています。
Port	このサーバーの通信ポートを設定します。範囲：1-65535.
Connection Type	接続タイプを選択します。 **Modbus TCP**： Modbus クライアントが Modbus TCP フォーマットのコマンドをこの Modbus サーバーに送信します。 **Modbus RTU over TCP**： Modbus クライアントが Modbus RTU フォーマットのコマンドをこの Modbus サーバーに送信します。
Server ID	この Modbus サーバーのサーバー ID を設定します。Modbus クライアントが各サーバを識別するために使用します。
Description	このサーバーの説明を追加します。

表 3-3-2-2 サーバー設定パラメータ

2.3.2.2 Modbus Object

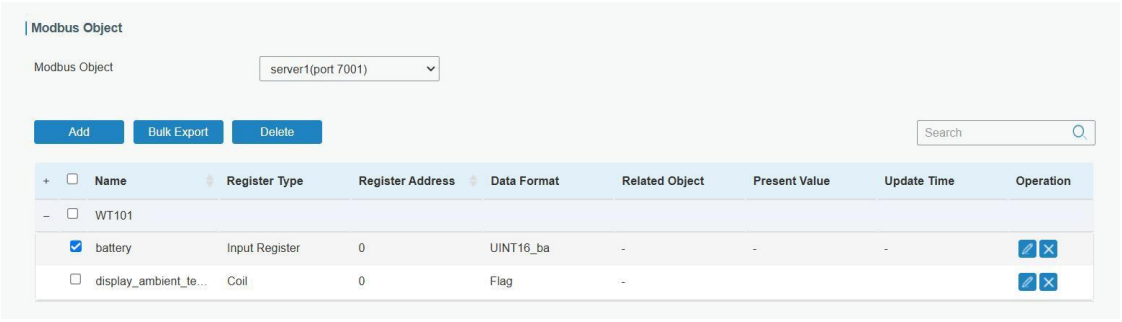
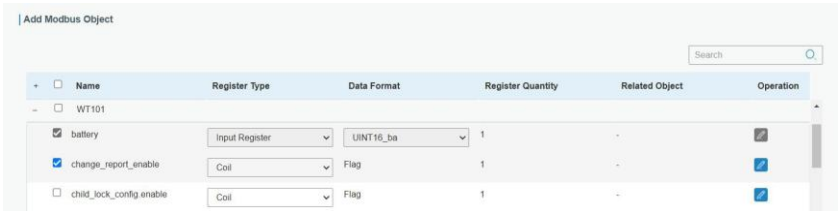


図 3-3-2-3

項目	説明
Modbus Object	オブジェクトを追加・編集する Modbus サーバーを選択します。
Add	このサーバに追加するオブジェクトをクリックして選択します。ゲートウェイは最大 2000 オブジェクトの追加をサポートします。 注意：ペイロードコーデックの内容が正しく、デバイスが正しいペイロードコーデックを選択していることを確認してください。 
Bulk Export	.xlsx 形式のファイルとしてエクスポートするオブジェクトを選択します。
Delete	削除したいオブジェクトを選択します。
Name	このオブジェクトの名前を表示します。

Register Type	このオブジェクトのレジスタ・タイプを表示します。
Register Address	このオブジェクトのレジスタ・アドレスを表示します。
Data Format	このオブジェクトのデータ・フォーマットを表示します。
Related Object	関連オブジェクトを表示します。
Present value	オブジェクトの最新値を表示します。
Update time	このオブジェクトがデータを取得・更新するまでの時間を表示します。
Operation	オブジェクトの編集、削除を行います。

表 3-3-2-3 Modbus オブジェクトリストパラメータ

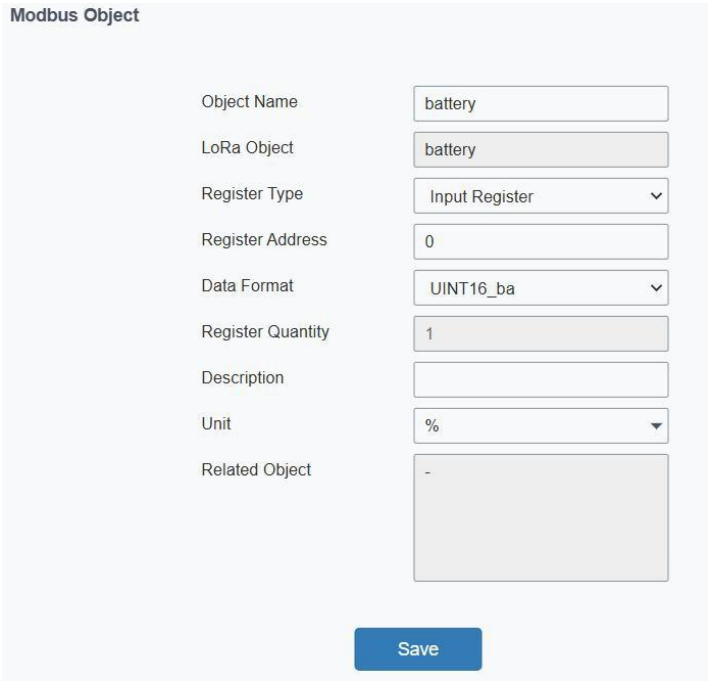


図 3-3-2-4

Modbus Object Configuration	
項目	オブジェクト名
Object Name	このオブジェクトの固有の名前をカスタマイズします。
LoRa Object	LoRaオブジェクトの対応する名前を表示します。
Object Name	このオブジェクトの固有の名前をカスタマイズします。
Register Type	Modbus レジスタ・タイプを選択します。 **Discrete Input**：リードオンリー、0とIのステータスのみ。 **コイル**：リードライト、0 と I ステータスのみ。 **ホールディング・レジスタ**：リード・ライト、アナログ値、文字列など。 **入力レジスタ**：読み出し専用、アナログ値、文字列などを含む
Register Address	オブジェクトを追加すると、このアドレスが自動的に生成されます。また、このアドレスは変更可能です。範囲**0-65535** 注意 1) 同じレジスタ・タイプのアドレスは、I つの Modbus サーバで異なる必要があります。 アドレスはレジスタ量に関連しています。このオブジェクトのアドレスが 0 でレジスタ量が 2 の場合、次のオブジェクトのアドレスは **2(0+2)**かそれ以上の値でなければなりません。

Data Format	このオブジェクトのデータフォーマットを表示または選択します。
Register Quantity	このオブジェクトのレジスタ占有量を表示します。
Description	このオブジェクトの説明を入力します。
Unit	このオブジェクトの単位を選択します。
Related Register	関連するレジスタを表示します。このオブジェクトを書き込むときは、関連するレジスタを一緒に書き込む必要があります。さもないと、このオブジェクトの変更はフェイルされます。

表 3-3-2-4 Modbus オブジェクト・コンフィグレーション・パラメータ

2.4 ネットワーク

2.4.1 インターフェース

2.4.1.1 ポート

イーサネット・ポートはインターネット・アクセスを得るためにイーサネット・ケーブルで接続することができます。3 つの接続タイプをサポートしています。

- **Static IP**：イーサネットWANインターフェースのIPアドレス、ネットマスク、ゲートウェイを設定します。
- **DHCPクライアント**：イーサネットWANインターフェースをDHCPクライアントとして設定し、IPアドレスを自動的に取得します。
- **PPPoE**: イーサネット WAN インターフェイスを PPPoE クライアントとして設定します。

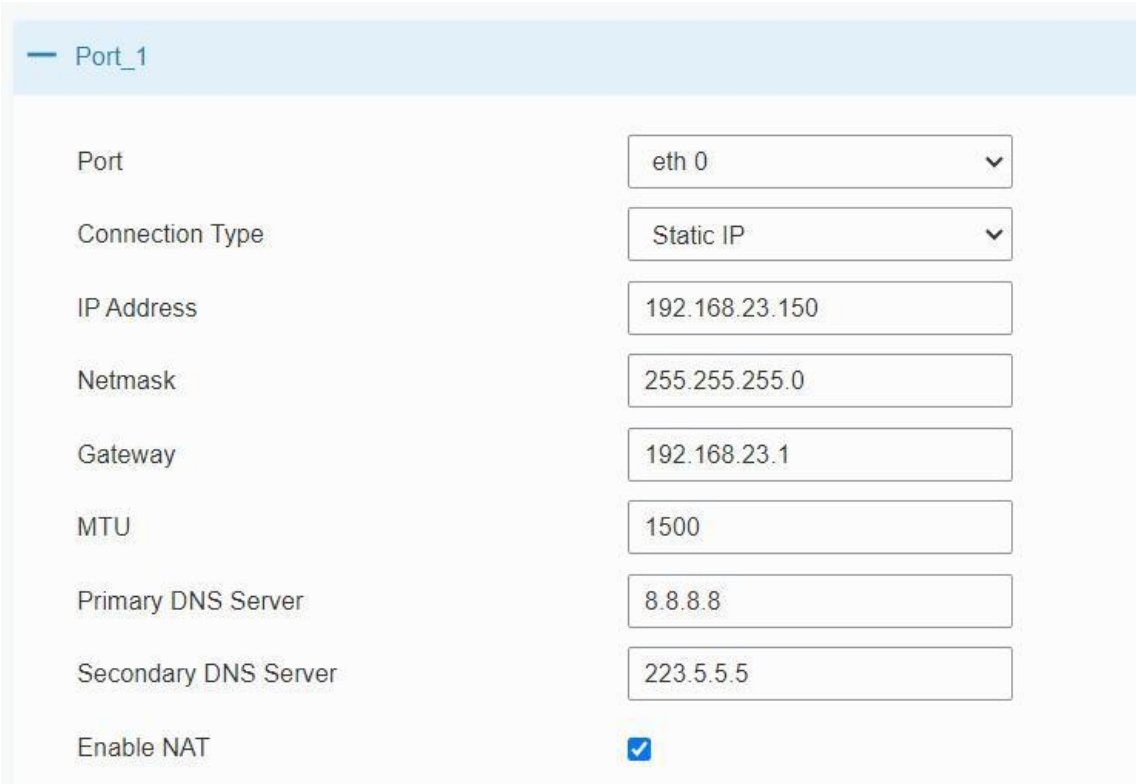


図 3-4-1-1

Port Setting

設定項目	設定項目	デフォルト
Port	eth0 ポートとして固定され、有効になっているポート。	eth 0
Connection Type	Static IP」、「DHCP Client」、「PPPoE」から選択します。	DHCP
MTU	最大伝送単位を設定します。	1500
Primary DNS Server	プライマリ DNS を設定します。	8.8.8.8
Secondary DNS Server	セカンダリDNSを設定します。	223.5.5.5
Enable NAT	NAT 機能を有効または無効にします。有効にすると、プライベートIPをパブリックIPに変換できます。	有効

表 3-4-1-1 ポートパラメータ

関連設定例

イーサネット接続

1. 固定IP設定

外部ネットワークがイーサネットポートに固定IPを割り当てる場合、ユーザーは "Static IP "モードを選択することができます。

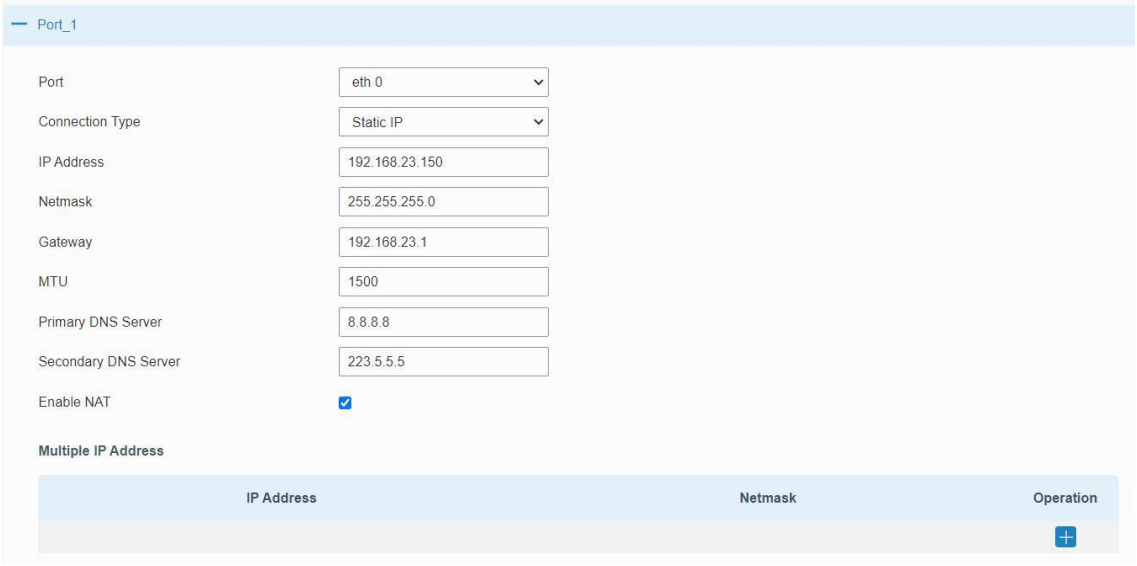


図 3-4-1-2

Static IP		
設定項目	設定内容	デフォルト
IP Address	インターネットにアクセスできるIPアドレスを設定します。	192.168.23.150
Netmask	イーサネットポートのネットマスクを設定します。	255.255.255.0
Gateway	イーサネットポートのゲートウェイのIPアドレスを設定します。	192.168.23.1
Multiple IP Address	イーサネットポートのIPアドレスを複数設定します。	Null

表 3-4-1-2 スタティック IP パラメータ

2. DHCP クライアント

外部ネットワークで DHCP サーバーが有効になっており、イーサネット WAN インターフェースに IP アドレスが割り当てられている場合、ユーザーは「DHCP クライアント」モードを選択して IP アドレスを自動的に取得することができます。

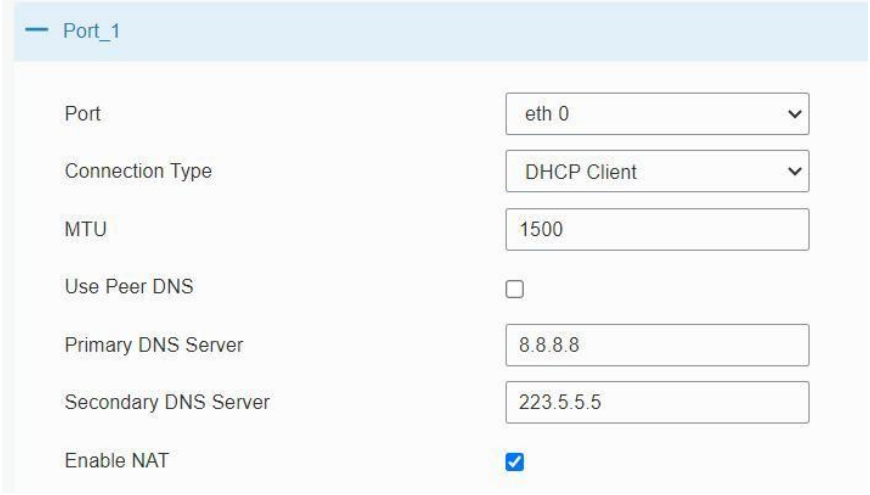


図 3-4-1-3

DHCP Client	
項目	設定内容
Use Peer DNS	PPP ダイヤル時にピア DNS を自動的に取得します。DNS は、ユーザがドメイン名を訪問するときに必要です。

表 3-4-1-3 DHCP クライアントパラメータ

3. PPPoE

PPPoE は、イーサネット上のポイントツーポイントプロトコルです。PPPoE はイーサネット上のポイントツーポイントプロトコルです。PPPoE を使用すると、リモートアクセス機器は各ユーザーを制御することができます。

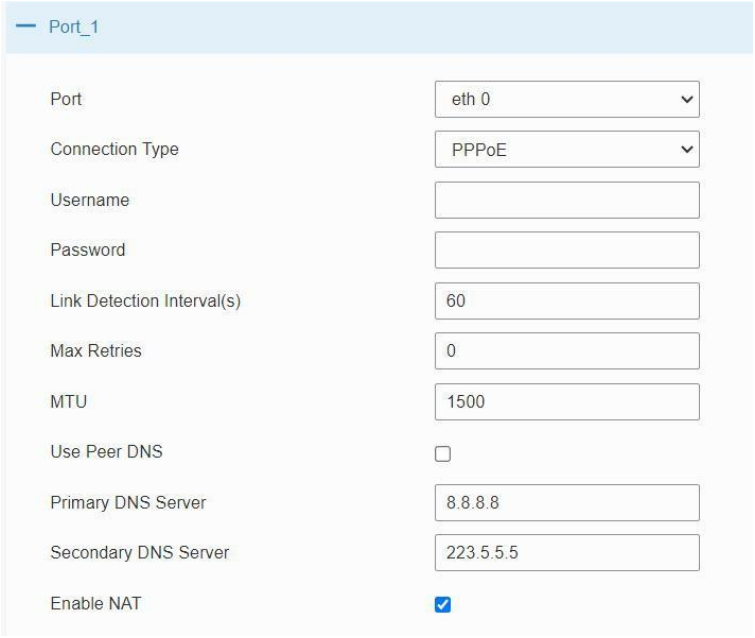


図3-4-1-4

PPPoE	
項目	項目
Username	インターネットサービスプロバイダー（ISP）から提供されたユーザー名を入力します。
Password	インターネットサービスプロバイダー（ISP）から提供されたパスワードを入力します。
Link Detection Interval (s)	リンク検出のハートビート間隔を設定します。範囲：1-600.
Max Retries	ダイヤルアップ失敗後の最大リトライ回数を設定します。範囲：0-9.
Use Peer DNS	PPPダイヤル時にピアDNSを自動的に取得します。DNSは、ユーザーがドメイン名を訪問するときに必要です。

表 3-4-1-4 PPOE パラメータ

2.4.1.2 WLAN

ここでは、Wi-Fi ネットワークの関連パラメータの設定方法を説明します。UG65 は、AP またはクライアントモードとして 802.11 b/g/n をサポートします。

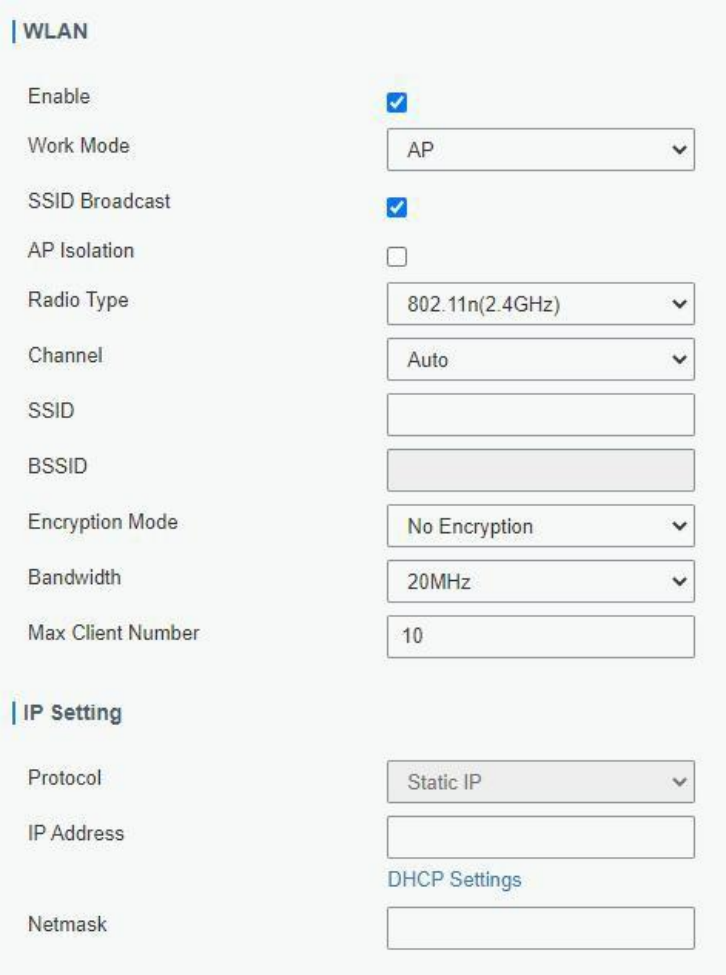


図 3-4-1-5

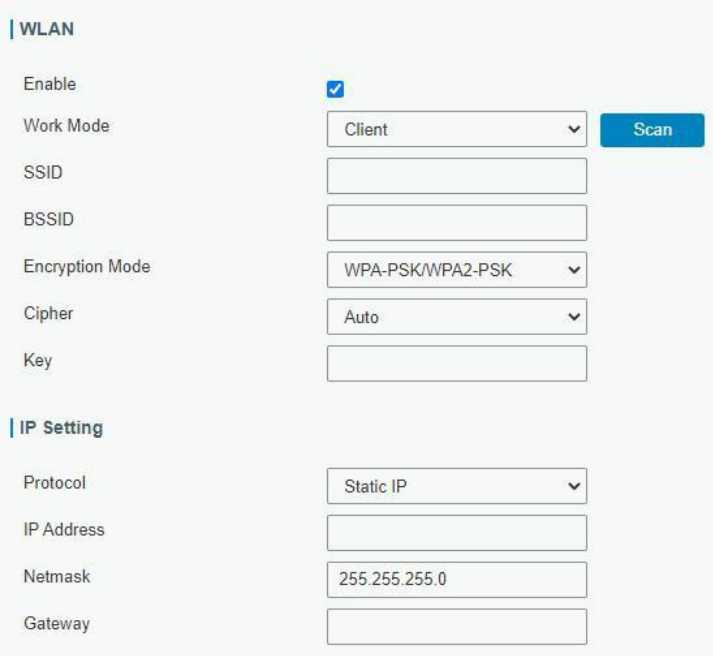


図 3-4-1-6

WLAN	
項目	説明

Enable	WLAN の有効／無効を設定します。
Work Mode	作業モードを選択します。オプションは "Client" または "AP" です。
AP Mode	
BSSID	この WLAN インターフェースの MAC アドレスを表示します。
Radio Type	無線タイプを選択します。オプションは、「802.11b（2.4GHz）」、「802.11g（2.4GHz）」、「802.11n（2.4GHz）」です、 「802.11n（2.4GHz）」です。
Channel	ワイヤレスチャンネルを選択します。オプションは、"Auto"、"1"、"2"　"11".
Bandwidth	帯域幅を選択します。20MHz」と「40MHz」から選択できます。
SSID	アクセスポイントのSSIDを入力します。
Encryption Mode	暗号化モードを選択します。暗号化なし」、「WEP Open System」、「WEP Shared Key」、「WPA-PSK」、「WPA2-PSK」、「WPA-PSK/WPA2-PSK」から選択できます。
Cipher	WPA暗号化の暗号を選択します。Auto」、「AES」、「TKIP」、「AES/TKIP」から選択できます。
Key	このアクセスポイントに接続するためのキーを入力します。デフォルトのキーは **iotpassword** です。
Max Client Number	アクセスするクライアントの最大数を設定します。
IP設定	
Protocol	Static IP固定です。
IP Address	無線LANのIPアドレスを設定します。
Netmask	無線LANのネットマスクを設定します。
Client Mode	
Scan	本機周辺のアクセスポイントをスキャンします。
SSID	アクセスポイントのSSIDを入力します。
BSSID	アクセスポイントのMACアドレスを入力します。SSIDまたはBSSIDのどちらかを入力すると、ネットワークに参加できます。 を入力します。
Encryption Mode	暗号化モードを選択します。暗号化なし」、「WEP Open System」、「WEP Shared Key」、「WPA-PSK」、「WPA2-PSK」、「WPA-PSK/WPA2-PSK」、「WPA-Enterprise」、「WPA2-Enterprise」、「WPA-Enterprise/WPA2-Enterprise」から選択できます。
Cipher	WPA暗号化の暗号を選択します。Auto」、「AES」、「TKIP」、「AES/TKIP」から選択できます。
Key	このアクセスポイントに接続するためのキーを入力します。
Xsupplicant Type	Peap」、「Leap」、「TLS」、「TTLS」から選択します。
User	WPA/WPA2-Enterprise のユーザー名を入力します。
Anonymous Identity	WPA/WPA2-Enterpriseの匿名IDを入力します。
Phase 2	WPA/WPA2-Enterpriseのフェーズを入力します。
Public Server Certificate	WPA/WPA2-Enterpriseアクセスポイントとの認証に使用する公開サーバー証明書を入力します。
IP設定	

Protocol	WLAN IPアドレスを取得するプロトコルを設定します。

IP Address	プロトコルが静的IPの場合、無線LANのIPアドレスを設定します。
Netmask	プロトコルがスタティックIPの場合、ワイヤレスネットワークのネットマスクを設定します。
Gateway	プロトコルがStatic IPの場合、ワイヤレスネットワークのゲートウェイを設定します。
Primary DNS Server	プライマリIPv4 DNSサーバーを設定します。
Secondary DNS Server	セカンダリ IPv4 DNS サーバーを設定します。

表 3-4-1-5 WLAN パラメーター

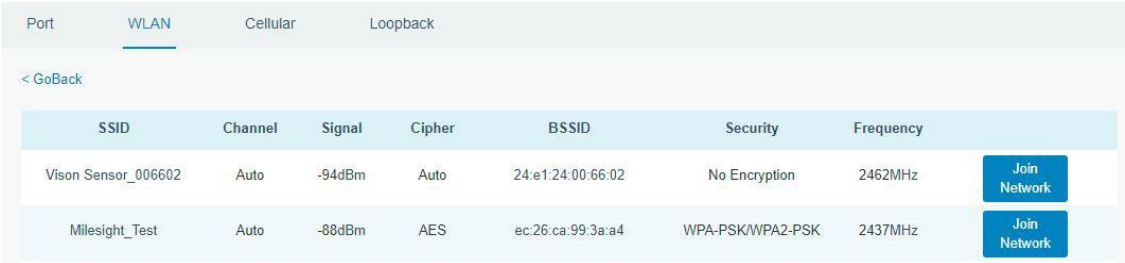


図 3-4-1-7

Client Mode-Scan	
SSID	SSID を表示します。
Channel	無線チャンネルを表示します。
Signal	無線信号を表示します。
BSSID	アクセスポイントの MAC アドレスを表示します。
Security	暗号化モードを表示します。
Frequency	無線の周波数を表示します。
Join Network	ワイヤレスネットワークに参加するボタンをクリックします。

表 3-4-1-6 WLAN スキャンパラメータ

関連トピック

Wi-Fi アプリケーションの例

2.4.1.3 セルラー（セルラー版のみ）

ここでは、セルラーネットワークの関連パラメーターの設定方法を説明します。

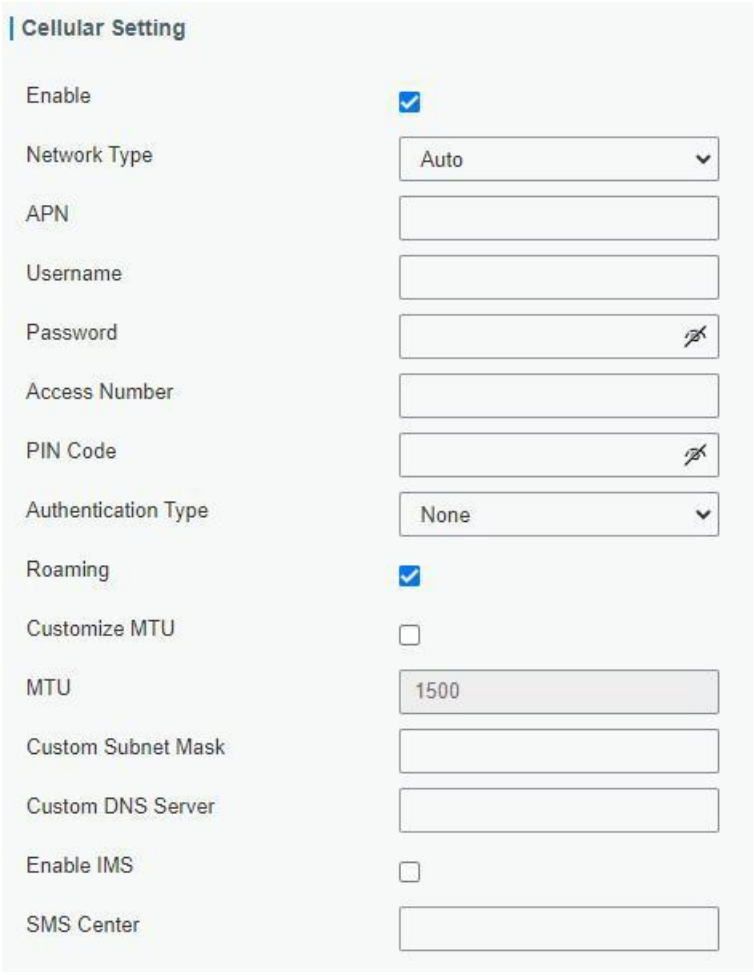


図 3-4-1-8

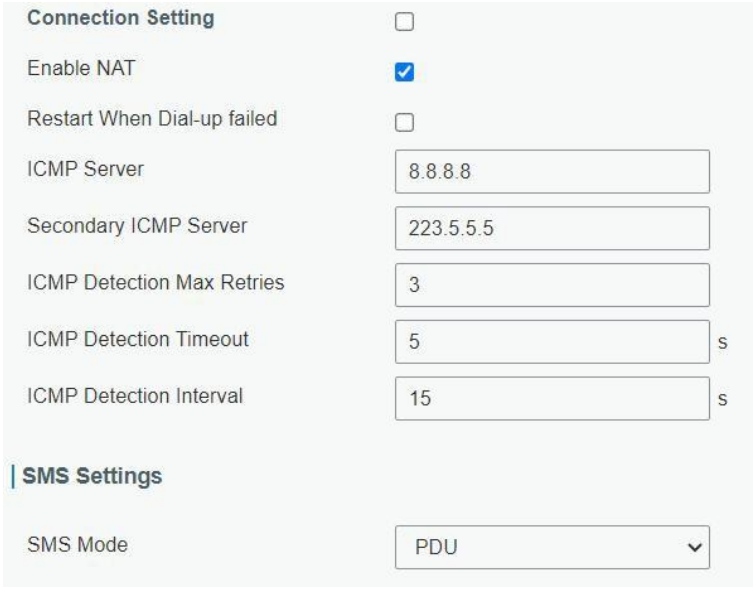


図3-4-1-9

General Settings	
設定項目	説明
Enable	セルラー機能を有効にするオプションをチェックします。

Network Type	Auto」、「Auto 3G/4G」、「4G Only」、「3G Only」から選択します。 自動：最も電波の強いネットワークに自動的に接続します。4Gのみ：4Gネットワークのみに接続します。など。
APN	ローカルISPが提供する携帯電話ダイヤルアップ接続のアクセスポイント名を入力します。
Username	ローカル ISP が提供する携帯電話ダイヤルアップ接続のユーザー名を入力します。
Password	ローカル ISP が提供するセルラーダイヤルアップ接続のパスワードを入力します。
Access Number	ダイヤルアップセンター番号を入力します。ローカル ISP が提供するセルラーダイヤルアップ接続の場合。
PIN Code	SIMロックを解除するための4～8文字のPINコードを入力します。
Authentication Type	なし」、「PAP」、「CHAP」から選択します。
Roaming	ローミングを有効または無効にします。
Customized MTU	最大伝送単位をカスタマイズするために有効または無効にします。無効の場合、デバイスはオペレーターの MTU 設定を使用します。
MTU	最大伝送単位を設定します。範囲：68-1500.
Custom Subnet Mask	セルラーサブネットマスクをカスタマイズします。空白の場合、デバイスはセルラー基地局が提供するサブネットマスクを使用します。 注：この機能はセルラーモジュールの一部でのみサポートされています。
Custom DNS Server	セルラーDNSサーバーをカスタマイズします。空白の場合、デバイスはセルラー・プロバイダーが提供するDNSサーバーを使用します。
Enable IMS	IMS機能を有効または無効にします。
SMS Center	SMSメッセージの保存、転送、変換、配信を行うローカルSMSセンターの番号を入力します。
Enable NAT	NAT機能を有効または無効にします。
Restart When Dial-up failed	この機能を有効にすると、ダイヤルアップに数回失敗した場合、ゲートウェイは自動的に再起動します。
ICMP Server	ICMP 検出サーバーの IP アドレスを設定します。 注：ISP に問い合わせて、ping 検出が許可されているかどうかを確認し、正しい ICMP サーバーアドレスを取得してください。ping 検出が許可されていない場合、このサーバーアドレスは空白のままにしてください。
Secondary ICMP Server	セカンダリ ICMP 検出サーバーの IP アドレスを設定します。
ICMP Detection Max Retries	ICMP検出フェイル時の最大リトライ回数を設定します。
ICMP Detection Timeout	ICMP 検出のタイムアウト時間を設定します。
ICMP Detection Interval	ICMP 検出の間隔を設定します。

SMS Mode	SMS モードを "TEXT"、"PDU "から選択します。

表 3-4-1-7 セルラーパラメータ

図 3-4-1-10

項目	項目 内容
Connection Mode	
Connection Mode	常時接続」と「オンデマンド接続」から選択します。
Redial Interval(s)	リダイヤル間隔を設定します。範囲0-3600.
Max Idle Time(s)	現在のリンクがアイドル状態のときのゲートウェイの最大時間を設定します。範囲：10-3600.
Triggered by Call	ゲートウェイは、仕様の電話番号からコールを受信すると、オフライン・モードからセルラー・ネットワーク・モードに自動的に切り替わります。
Call Group	コールトリガー用のコールグループを選択します。**System > General Settings > Phone**で電話グループを設定します。
Triggered by SMS	特定の携帯電話から特定の SMS を受信すると、ゲートウェイは自動的にオフラインモードからセルラーネットワークモードに切り替わります。
SMS Group	トリガーするSMSグループを選択します。**System > General Settings > Phone** でSMSグループを設定します。
SMS Text	トリガーするSMSの内容を入力します。

表 3-4-1-8 セルラー パラメータ

関連トピック

セルラー接続アプリケーションの例

電話グループ

2.4.1.4 ループバック

ループバック・インターフェースは、ゲートウェイの ID を置き換えるために使用されます。 インタフェースがダウンすると、ゲートウェイの ID を再選択する必要があり、OSPF の収束時間が長くなります。そのため、一般的にはループバックインタフェースをゲートウェイのIDとして推奨します。

ループバックインタフェースはゲートウェイ上の論理的かつ仮想的なインタフェースです。デフォルトではゲートウェイにループバックインタフェースはありませんが、必要に応じて作成することができます。

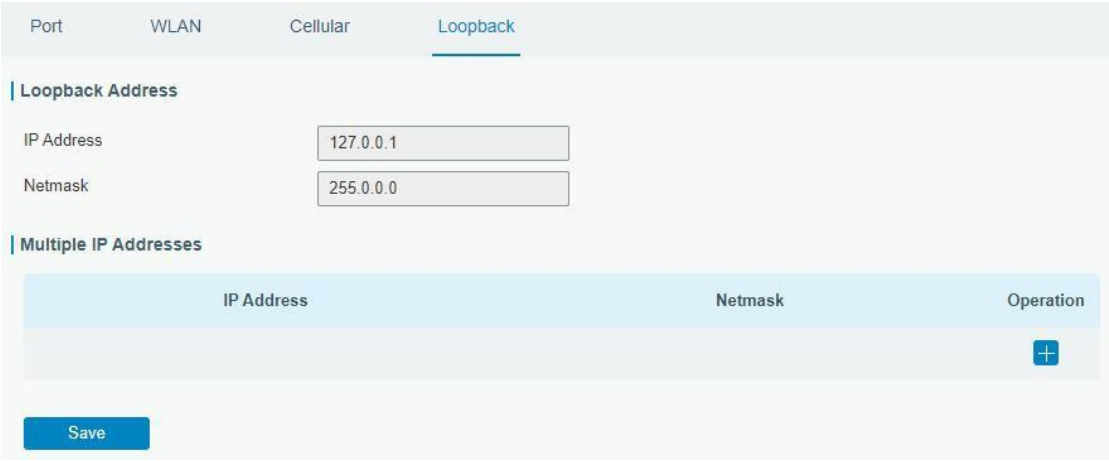


図 3-4-1-11

Loopback		
項目	説明	デフォルト
IP Address	変更不可	127.0.0.1
Netmask	変更不可	255.0.0.0
Multiple IP Addresses	上記のIPアドレスとは別に、他のIPアドレスを設定することができます。	Null

表 3-4-1-9 ループバックパラメータ

2.4.1.5 VLAN トランク

UG65 ゲートウェイは、VLAN トランククライアントとして動作するイーサネットポートをサポートし、トラフィックの分類が容易な VLAN ID を割り当てます。VLAN ID が設定されている場合、**"Network" > "Interface" > "Port"** でポートを eth0.x として選択できます。VLAN設定は空白

デフォルトでは空白になっていますが、 をクリックすることで、特定のインターフェイスに新しい VLAN ラベルを追加することができます。

図 3-4-1-12

VLAN トランク	
項目	項目
Interface	VLAN インタフェースを選択します。
VID	VLAN のラベル ID を設定します。範囲は1-4094.

表 3-4-1-10 VLAN トランクパラメータ

2.4.2 ファイアウォール

このセクションでは、ウェブサイトブロック、ACL、DMZ、ポートマッピング、MAC バインディングを含むファイアウォール パラメータの設定方法について説明します。

ファイアウォールは、プロトコルスタイル、ソース/宛先 IP アドレスなどのパケットのコンテンツ機能に従って、入口方向(インターネットからローカルエリアネットワークへ)と出口方向(ローカルエリアネットワークからインターネットへ)のデータフローに対応する制御を実行します。これにより、ゲートウェイはローカルエリアネットワーク内のホストと安全な環境で動作することができます。

2.4.2.1 セキュリティ

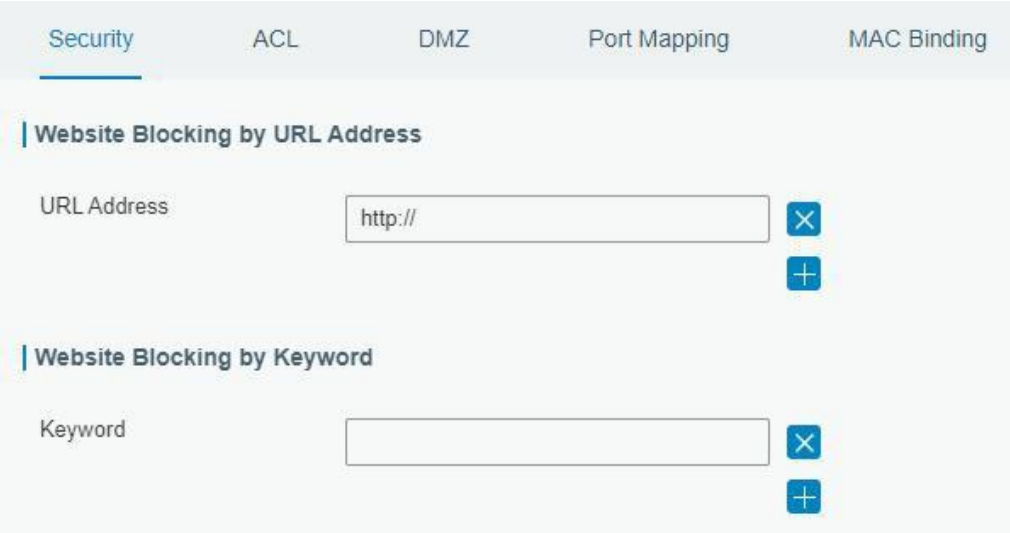


図3-4-2-1

Website Blocking	
URL Address	ブロックしたい HTTP アドレスを入力します。
Keyword	キーワードを入力することで、特定の Web サイトをブロックすることができます。最大文字数は 64 文字です。

表 3-2-2-1 セキュリティパラメータ

2.4.2.2 ACL

ACL（Access Control List）とは、ネットワークインタフェースのトラフィックをフィルタリングするために、一連のマッチングルールを設定することで、指定されたネットワークトラフィック（送信元IPアドレスなど）に対するアクセスの許可または禁止を実装するものです。ゲートウェイがパケットを受信すると、現在のインターフェイスに適用されている ACL ルールに従ってフィールドが解析されます。特別なパケットが識別された後、対応するパケットの許可または禁止は、事前に設定された戦略に従って実行されます。

ACL によって定義されたデータパッケージのマッチングルールは、フローの区別を必要とする他の機能によって使用することもできます。

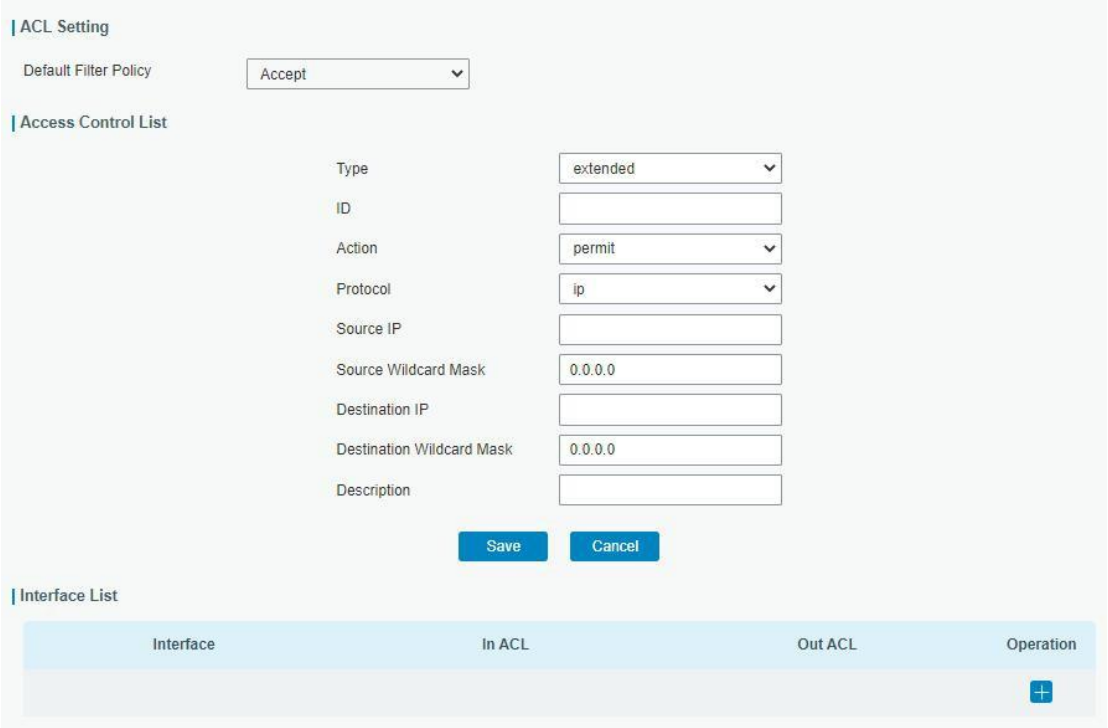


図 3-4-2-2

項目	内容
ACL Setting	
Default Filter Policy	Accept」と「Deny」から選択します。 アクセス制御リストに含まれないパケットは、デフォルトフィルタポリシーで処理されます。
Access Control List	
Type	拡張」「標準」から選択します。
ID	ユーザー定義の ACL 番号。範囲：1-199.
Action	「Permit」と「Deny」から選択します。
Protocol	プロトコルを「ip」「icmp」「tcp」「udp」「1-255」から選択します。
Source IP	送信元のネットワークアドレス（空白の場合はすべて）。
Source Wildcard Mask	送信元ネットワークアドレスのワイルドカードマスク。
Destination IP	宛先ネットワークアドレス（0.0.0.0はすべてを意味します）。
Destination Wildcard Mask	宛先アドレスのワイルドカードマスク。
Description	同じ ID を持つグループの説明を入力します。
ICMP Type	ICMPパケットのタイプを入力します。範囲：0-255.
ICMP Code	ICMPパケットのコードを入力します。範囲：0～2550-255.
Source Port Type	指定ポート、ポート範囲など、送信元ポートの種類を選択します。
Source Port	送信元ポート番号を設定します。範囲：1-65535.
Start Source Port	開始ソースポート番号を設定します。範囲：1-65535：1-65535.
End Source Port	終了ソースポート番号を設定します。範囲：1-65535.

Destination Port Type	指定ポート、ポート範囲など、宛先ポートの種類を選択します。
Destination Port	宛先ポート番号を設定します。範囲を指定します：1-65535.
Start Destination Port	開始宛先ポート番号を設定します。範囲：1-65535：1-65535.
End Destination Port	終了宛先ポート番号を設定します。範囲：1-65535：1-65535.
More Details	ポートの情報を表示します。
Interface List	
Interface	アクセス制御を行うネットワークインタフェースを選択します。
In ACL	ACL ID から受信トラフィックのルールを選択します。
Out ACL	ACL ID から送信トラフィックのルールを選択します。

表 3-4-2-2 ACL パラメータ

3.4.2.4 ポートマッピング (DNAT)

外部サービスが内部で必要な場合（Web サイトを外部公開する場合など）、外部アドレスがアクティブな接続を開始します。そして、ファイアウォール上のルータまたはゲートウェイがその接続を受信します。そして、その接続を内部接続に変換します。この変換はDNATと呼ばれ、主に外部およびインターバルサービスに使用されます。

をクリックし、新しいポートマッピングルールを追加します。

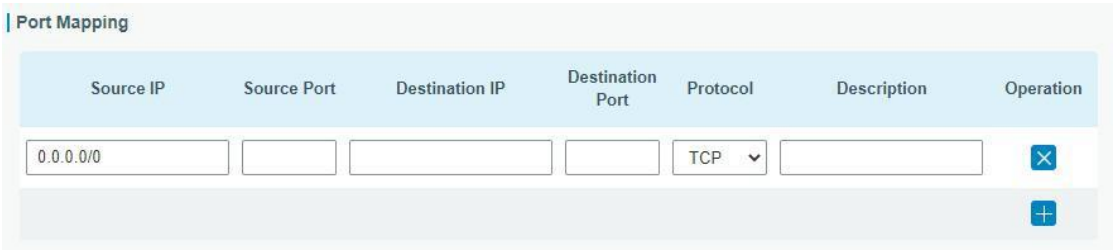


図 3-4-2-4

Port Mapping	
項目	説明
Source IP	ローカル IP アドレスにアクセスできるホストまたはネットワークを指定します。0.0.0.0/0はすべてです。
Source Port	受信パケットを転送するTCPまたはUDPポートを入力します。範囲：1-65535.
Destination IP	受信インターフェイスで受信した後、パケットが転送される IP アドレスを入力します。
Destination Port	受信ポートで受信後、パケットが転送されるTCPまたはUDPポートを入力します。範囲：1-65535.
Protocol	TCP」、「UDP」の中から用途に応じて選択します。
Description	このルールの説明です。

表 3-4-2-4 ポートマッピングパラメータ

関連設定例

NAT アプリケーションの例

3.4.2.3 DMZ

DMZ は、ポートマッピングで転送されるポートを除く、すべてのポートが公開される内部ネッ トワーク内のホストです。

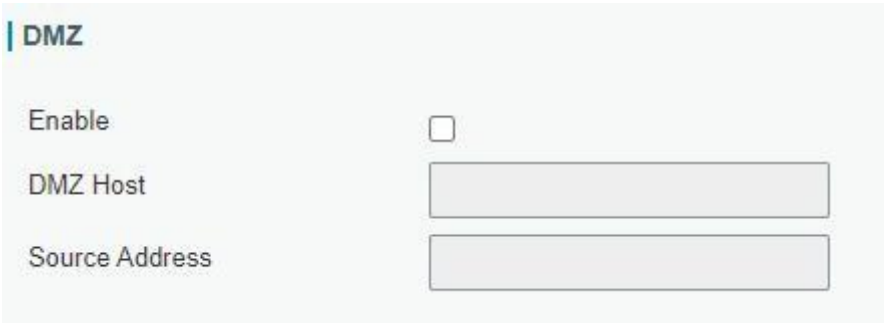


図 3-4-2-3

DMZ	
項目	説明
Enable	DMZ を有効または無効にします。
DMZ Host	内部ネットワーク上のDMZホストのIPアドレスを入力します。
Source Address	DMZホストにアクセスできるソースIPアドレスを設定します。「0.0.0.0/0」は任意のアドレスを意味します。

表 3-4-2-3 DMZ パラメータ

3.4.2.5 MACバインド

MAC Binding は、外部ネットワークアクセス許可リストにある MAC アドレスと IP アドレスを照合してホストを指定します。

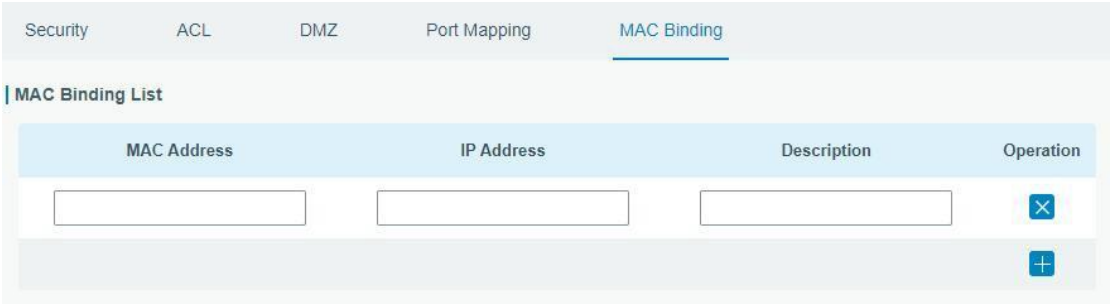


図 3-4-2-5

MAC Binding List	
項目	項目 内容
MAC Address	バインドする MAC アドレスを設定します。
IP Address	バインドするIPアドレスを設定します。
Description	バインディングルールの意味を MAC-IP ごとに記述します。

表 3-4-2-5 MAC バインディングパラメータ

2.4.3 DHCP

UG65 は、Wi-Fi を AP モードで動作させる際に、IP アドレスを配布する DHCP サーバーとして設定することができます。

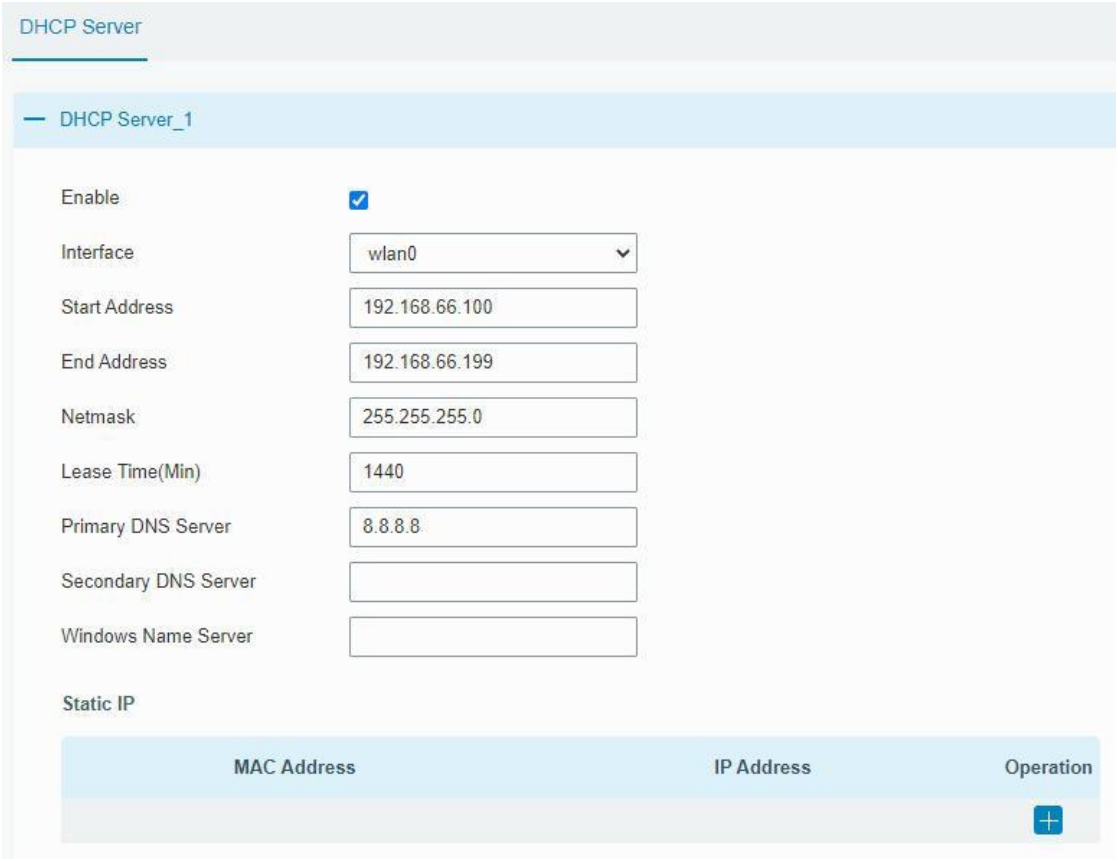
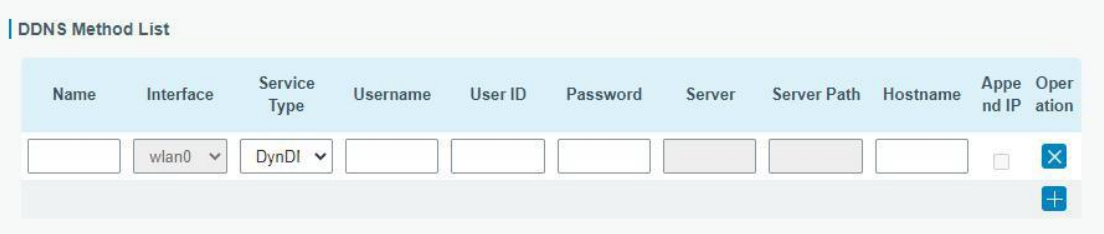


図 3-4-3-1

DHCP Server		
設定項目	設定内容	デフォルト
Enable	DHCP サーバーを有効または無効にします。	Enable
Interface	wlan インターフェースだけが IP アドレスを配布できます。	wlan0
Start Address	DHCP クライアントにリースする IP アドレスプールの開始アドレスを定義します。	192.168.1.100
End Address	DHCP クライアントにリースされる IP アドレスのプールの終端を定義します。	192.168.1.199
Netmask	DHCPクライアントがDHCPサーバーから取得するIPアドレスのサブネットマスクを定義します。	255.255.255.0
Lease Time (Min)	クライアントがDHCPサーバーから取得したIPアドレスを使用できるリース時間を設定します。範囲：1-10080.	1440
Primary DNS Server	プライマリ DNS サーバーを設定します。	8.8.8.8
Secondary DNS Server	セカンダリDNSサーバーを設定します。	Null
Windows Name Server	DHCPクライアントがDHCPサーバから取得するWindowsインターネットネーミングサービスを定義します。通常は空白のままでかまいません。	Null

Static IP		
MAC Address	DHCPクライアントの静的で仕様の異なるMACアドレスを設定します（競合を避けるため、他のMACアドレスとは異なる必要があります）。	Null
IP Address	DHCP クライアントに静的で特定の IP アドレスを設定します（DHCP 範囲外である必要があります）。	Null

表 3-4-3-1 DHCP サーバーパラメーター



2.4.4 DDNS

ダイナミックDNS（DDNS）は、ドメインネームシステムのネームサーバーを自動的に更新する方法で、ユーザーが動的IPアドレスを静的ドメイン名にエイリアスすることを可能にします。

DDNSはクライアントツールとして機能し、DDNSサーバーと調整する必要があります。設定を開始する前に、ユーザは適切なドメイン名プロバイダのウェブサイトに登録し、ドメイン名を申請する必要があります。

図3-4-4-1

DDNS	
項目	説明
Name	DDNS にわかりやすい名前を付けます。
Interface	DDNSにバンドルされているインターフェイスを設定します。
Service Type	DDNSサービスプロバイダを選択します。
Username	DDNS登録用のユーザー名を入力します。
User ID	カスタムDDNSサーバーのユーザーIDを入力します。
Password	DDNS登録用のパスワードを入力します。
Server	DDNSサーバー名を入力します。
Hostname	DDNSのホスト名を入力します。
Append IP	現在のIPをDDNSサーバーの更新パスに追加します。

表 3-4-4-1 DDNS パラメータ

2.4.5 リンクフェイルオーバー

VRRP などのリンクフェイルオーバーの設定方法について説明します。

設定手順

1. 1つ以上のSLA動作（ICMPプローブ）を定義します。
2. SLA動作のステータスを追跡するために、1つ以上のtrackオブジェクトを定義します。
3. VRRPやスタティックルーティングなど、トラックオブジェクトに関連するアプリケーションを定義します。

2.4.5.1 SLA

SLA 設定は、リンクプローブ方法の設定に使用します。デフォルトのプローブタイプは ICMP です。

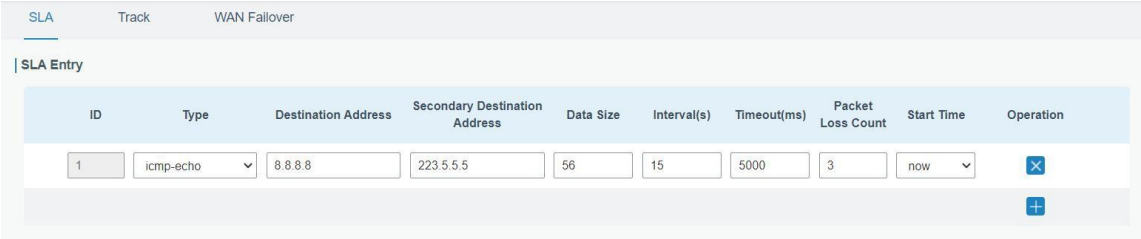


図 3-4-5-1

SLA		
設定項目	設定項目	デフォルト
ID	SLAのインデックス。最大10個のSLA設定を追加できます。 範囲：1-10.	1
Type	リンクが生きているかどうかを検出するためのデフォルトのタイプはICMP-ECHOです。	icmp エコー
Destination Address	検出された IP アドレス。	8.8.8.8
Secondary Destination Address	検出されたセカンダリIPアドレス。	223.5.5.5
Data Size	ユーザー定義のデータサイズ。範囲：0-1000.	56
Interval (s)	ユーザー定義の検出間隔。範囲：1-608400.	30
Timeout (ms)	ユーザー定義のICMP検出フェイル判定応答タイムアウト。範囲：1-300000.	5000
Packet Loss Count	各 SLA プローブにおけるパケットロス数を設定します。設定したパケットロス数を超えるとSLAプローブがフェイルします。	5
Start Time	検出開始時刻を "Now "と空白文字から選択します。空白文字はSLA検知を開始しないことを意味します。	今

表 3-4-5-1 SLA パラメータ

2.4.5.2 トラック

SLAモジュール、Trackモジュール、Applicationモジュールの連携を実現するための設定です。Track設定はアプリケーションモジュールとSLAモジュールの間に位置し、各種SLAモジュールの違いを遮蔽し、アプリケーションモジュールに統一されたインターフェースを提供することを主な機能としています。

TrackモジュールとSLAモジュールの連携

設定を完了すると、TrackモジュールとSLAモジュールの連携関係が確立されます。SLAモジュールは、リンク・ステータスの検出、ネットワーク・パフォーマンスの検出、Trackモジュールへの通知に使用されます。検出結果は、トラック・ステータスをタイムリーに変更するのに役立ちます。

- 検出が成功した場合、対応するトラック・アイテムはPositiveになります。
- フェイル検出の場合、対応するトラック項目はネガティブになります。

Trackモジュールとアプリケーションモジュールの連携

設定後、Trackモジュールと Applicationモジュール間のリンク関係が確立されます。トラック・アイテムに何らかの変更が発生すると、対応する処理が必要な通知がアプリケーション・モジュールに送信されます。

現在、VRRPやスタティック・ルーティングなどのアプリケーション・モジュールは、Trackモジュールと連携することができます。

アプリケーションモジュールに即座に通知を送信する場合、ルーティングのフェイルによるタイムリーな復旧などにより、通信が中断される場合があります。そのため、トラックアイテムの状態が変化したときに、アプリケーションモジュールへの通知を遅延させる期間を設定することができます。

図 3-4-5-2

項目	説明	デフォルト
Index	トラックインデックス。最大10トラックまで設定可能。範囲：1-10.	1
Type	オプションは「sla」と「interface」です。	SLA
SLA ID	定義されたSLA ID。	1
Interface	状態を検出するインタフェースを選択します。	セルラー0
Negative Delay (s)	インターフェイスがダウンまたはSLAプローブに失敗した場合、ここで設定した時間だけ待ってから、実際にステータスをDownに変更します。範囲：0～180（0は即時切り替え）。	0
Positive Delay (s)	フェイルリカバリーが発生した場合、ここで設定した時間だけ待ってから、実際にステータスをUpに変更します。範囲0～180（0は即時切替）。	1

表 3-4-5-2 トラックパラメータ

2.4.5.3 WAN フェイルオーバー

WAN フェイルオーバーとは、イーサネット WAN インターフェースとセルラー インターフェース間のフェイルオーバーを指します。特定のインタフェースの故障や帯域幅の不足により、サービス伝送が正常に行われない場合、フロー速度をバックアップインタフェースに迅速に切り替えることができます。バックアップインターフェースはサービス伝送を行い、ネットワークフローを共有し、データ設備の通信信頼性を向上させます。

主要なインターフェイスのリンク状態がアップからダウンに転換されるとき、システムにバックアップ インターフェイスのリンクにすぐに転換する代りに前もって調整された遅れの仕事があります。主インターフェイスの状態が遅れの後でまだダウンしていれば、システムはバックアップ インターフェイスのリンクに転換します。それ以外の場合、システムは変更されません。

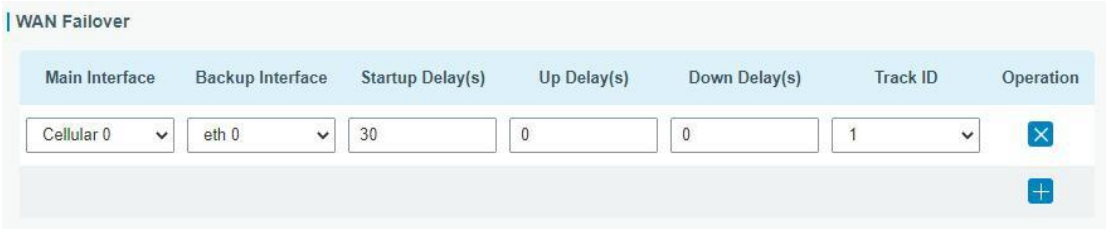


図 3-4-5-3

WAN Failover		
パラメータ	説明	デフォルト
Main Interface	メイン・リンクとしてリンク・インタフェースを選択します。	--
Backup Interface	バックアップリンクとしてリンクインタフェースを選択します。	--
Startup Delay (s)	起動トラッキング検出ポリシーが有効になるまでの待機時間を設定します。範囲：0-300.	30
Up Delay (s)	プライマリインタフェースがフェイル検出から検出成功に切り替わるとき、設定した時間に基づいて切り替えを遅延させることができます。範囲：0～180（0は即時切り替え）	0
Down Delay (s)	プライマリインタフェースが検出成功からフェイルに切り替わるとき、設定した時間だけ切り替えを遅らせることができます。範囲0～180（0は即時切換え）。	0
Track ID	トラック検出で、定義されたトラック ID を選択します。	--

表 3-4-5-3 WAN フェイルオーバーパラメータ

2.4.6 VPN

仮想プライベートネットワークは、VPN とも呼ばれ、2 つのプライベートネットワークを安全に接続するために使用されます。

UG65 は DMVPN、IPsec、GRE、L2TP、PPTP、OpenVPN、および GRE over IPsec と L2TP over IPsec をサポートしています。

2.4.6.1 DMVPN

mGREとIPsecを組み合わせた動的マルチポイント仮想プライベートネットワーク（DMVPN）は、組織の本部のVPNサーバーまたはゲートウェイを経由せずにサイト間でデータを交換する安全なネットワークです。

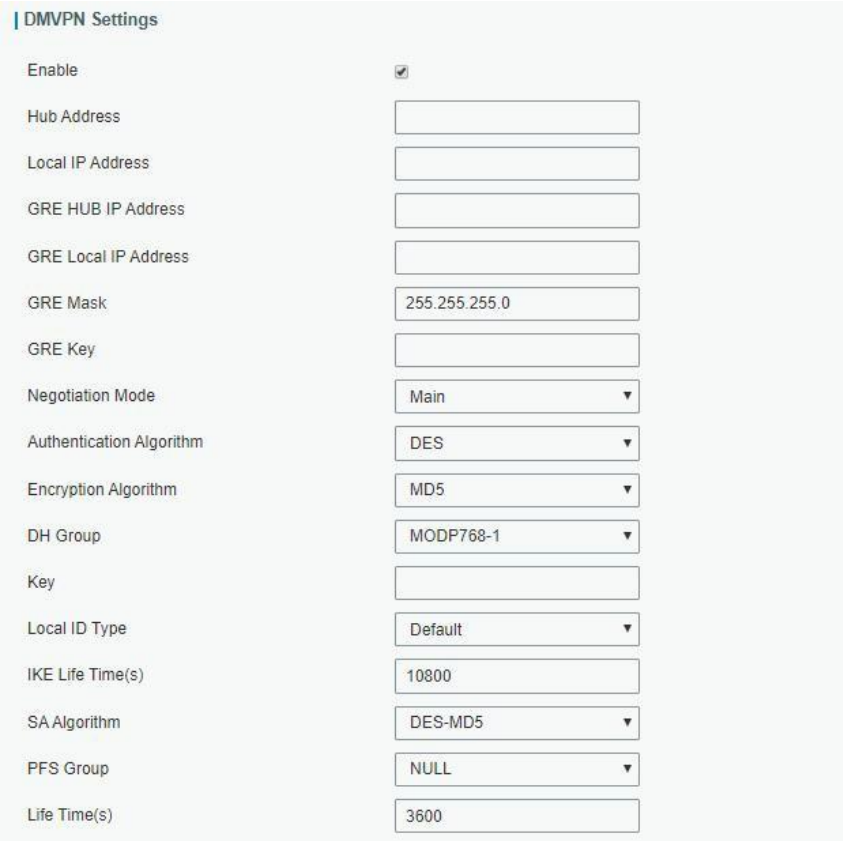


図 3-4-6-1

図 3-4-6-2

DMVPN	
項目	説明
Enable	DMVPN を有効または無効にします。
Hub Address	DMVPN ハブの IP アドレスまたはドメイン名。
Local IP address	DMVPN ローカルトンネルの IP アドレス。
GRE Hub IP Address	GRE ハブのトンネル IP アドレス。
GRE Local IP Address	GRE ローカルトンネル IP アドレス。
GRE Netmask	GRE ローカルトンネルのネットマスク。
GRE Key	GRE トンネルキー。
Negotiation Mode	Main」と「Aggressive」から選択します。
Authentication Algorithm	DES」、「3DES」、「AES128」、「AES192」、「AES256」から選択します。
Encryption Algorithm	MD5」「SHA1」から選択します。
DH Group	MODP768_1」「MODP1024_2」「MODP1536_5」から選択します。
Key	共有キーを入力します。

Local ID Type	"Default"、"ID"、"FQDN"、"User FQDN "から選択します。
IKE Life Time (s)	IKE ネゴシエーションの有効期間を設定します。範囲：60-86400.
SA Algorithm	DES_MD5」、「DES_SHA1」、「3DES_MD5」、「3DES_SHA1」、「AES128_MD5」、「AES128_SHA1」、「AES192_MD5」、「AES192_SHA1」、「AES256_MD5」、「AES256_SHA1」から選択します。
PFS Group	NULL」、「MODP768_1」、「MODP1024_2」、「MODP1536-5」から選択。
Life Time (s)	IPsec SA の有効期間を設定します。範囲：60-86400.
DPD Interval Time (s)	DPD 間隔時間を設定します。
DPD Timeout (s)	DPD タイムアウトを設定します。
Cisco Secret	Cisco Nhrp キー。
NHRP Holdtime (s)	Nhrp プロトコルのホールドタイム。

表 3-4-6-1 DMVPN パラメータ

2.4.6.2 IPSec

IPsec は、仮想プライベートネットワークの実装や、プライベートネットワークへのダイヤルアップ接続によるリモートユーザーアクセスに特に便利です。IPsec の大きな利点は、個々のユーザーコンピュータに変更を加えることなく、セキュリティの取り決めを処理できることです。

IPsec は 3 種類のセキュリティサービスを提供します：認証ヘッダー(AH)、カプセル化セキュリティペイロード(ESP)、インターネット鍵交換(IKE)。AHは基本的に送信者のデータの認証を可能にします。ESPは送信者の認証とデータの暗号化の両方をサポートします。IKEは暗号コードの交換に使用されます。これらはすべて、ホスト間、ホストとゲートウェイ間、およびゲートウェイ間の1つ以上のデータフローを保護することができます。

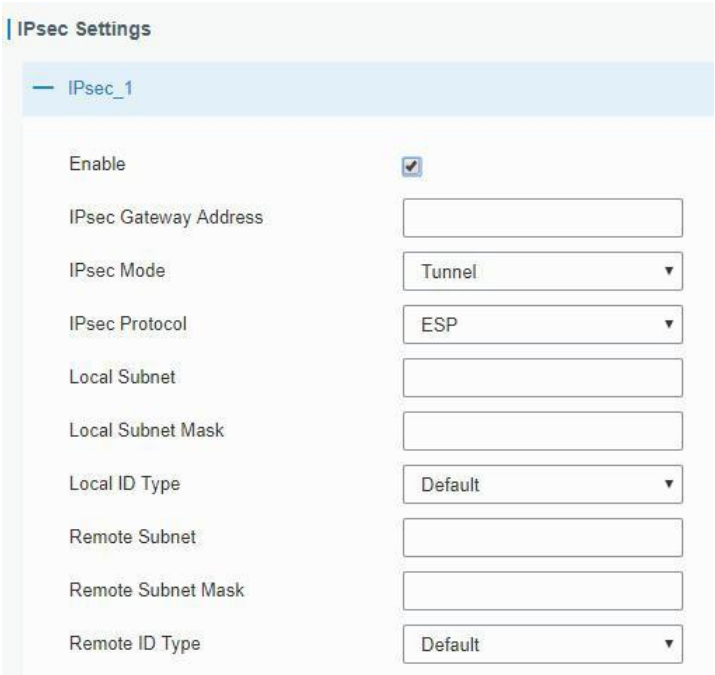


図 3-4-6-3

IPsec	
項目	説明
Enable	IPsec トンネルを有効にします。最大 3 つのトンネルが許可されます。
IPsec Gateway Address	リモート IPsec サーバーの IP アドレスまたはドメイン名を入力します。
IPsec Mode	Tunnel」と「Transport」から選択します。
IPsec Protocol	ESP」「AH」から選択します。
Local Subnet	IPsecが保護するローカルサブネットのIPアドレスを入力します。
Local Subnet Netmask	IPsec が保護するローカルネットマスクを入力します。
Local ID Type	Default」、「ID」、「FQDN」、「User FQDN」から選択します。
Remote Subnet	IPsecが保護するリモートサブネットのIPアドレスを入力します。
Remote Subnet Mask	IPsecが保護するリモートネットマスクを入力します。
Remote ID type	Default」、「ID」、「FQDN」、「User FQDN」から選択します。

表 3-4-6-2 IPsec パラメータ

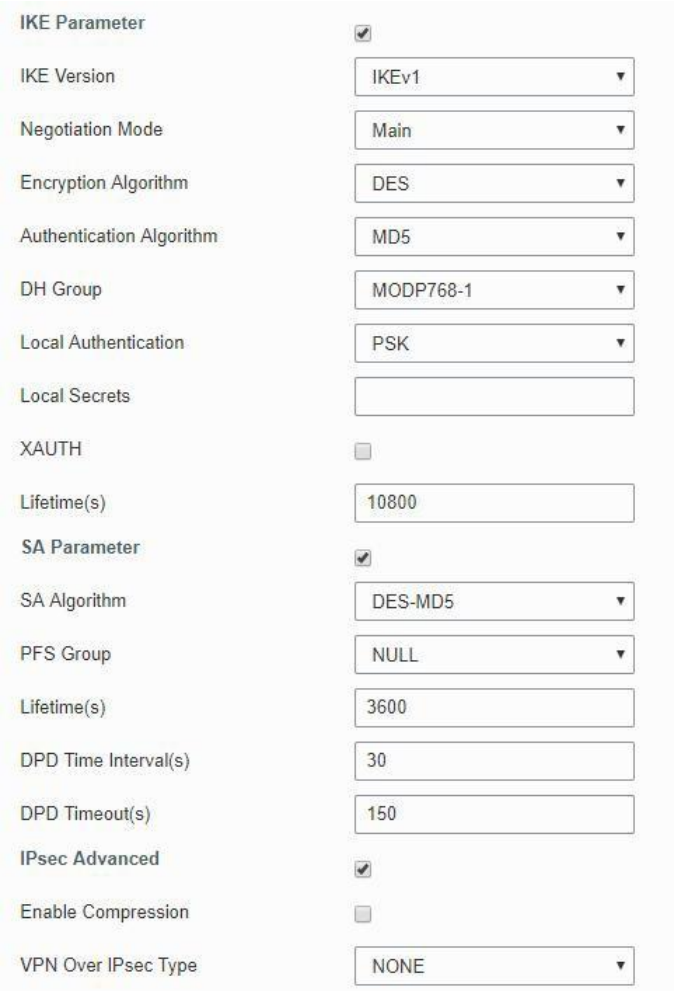


図 3-4-6-4

IKE Parameter	
項目	説明
IKE Version	IKEv1」と「IKEv2」から選択します。
Negotiation Mode	Main」「Aggressive」から選択します。

Encryption Algorithm	DES」、「3DES」、「AES128」、「AES192」、「AES256」から選択します。
Authentication Algorithm	MD5」「SHA1」から選択します。
DH Group	MODP768_1」「MODP1024_2」「MODP1536_5」から選択。
Local Authentication	PSK」「CA」から選択します。
Local Secrets	共有鍵を入力します。
XAUTH	XAUTHを有効にした後のXAUTHユーザー名とパスワードを入力します。
Lifetime (s)	IKE ネゴシエーションの有効期間を設定します。範囲：60-86400.
SA Parameter	
SA Algorithm	DES_MD5」、「DES_SHA1」、「3DES_MD5」、「3DES_SHA1」、「AES128_MD5」、「AES128_SHA1」、「AES192_MD5」、「AES192_SHA1」、「AES256_MD5」、「AES256_SHA1」から選択します。
PFS Group	NULL」、「MODP768_1」、「MODP1024_2」、「MODP1536_5」から選択。
Lifetime (s)	IPsec SA の有効期間を設定します。範囲：60-86400.
DPD IntervalTime(s)	リモート側のフェイルを検出するための DPD 間隔時間を設定します。
DPD Timeout(s)	DPDタイムアウトを設定。範囲：10-3600.
IPsec Advanced	
Enable Compression	有効化後にIPパケットの先頭を圧縮します。
VPN Over IPsec Type	VPN over IPsec 機能を有効にする場合、"NONE"、"GRE"、"L2TP "から選択します。

表 3-4-6-3 IPsec パラメータ

2.4.6.3 GRE

GRE（Generic Routing Encapsulation）は、IP ネットワーク上で他のプロトコルをルーティングするためにパケットをカプセル化するプロトコルです。これは、カプセル化されたデータメッセージが伝送されるチャネルを提供し、両端でカプセル化とカプセル化を解除することができるトンネリング技術です。

次のような場合にGREトンネル伝送が適用できます：

- GRE トンネルは、あたかも真のネットワークインターフェースのようにマルチキャストデータパケットを伝送できます。IPSecの単独使用では、マルチキャストの暗号化を実現できません。
- 採用された特定のプロトコルをルーティングできないこと。
- 異なるIPアドレスのネットワーク同 士 を 接続する必要があります。

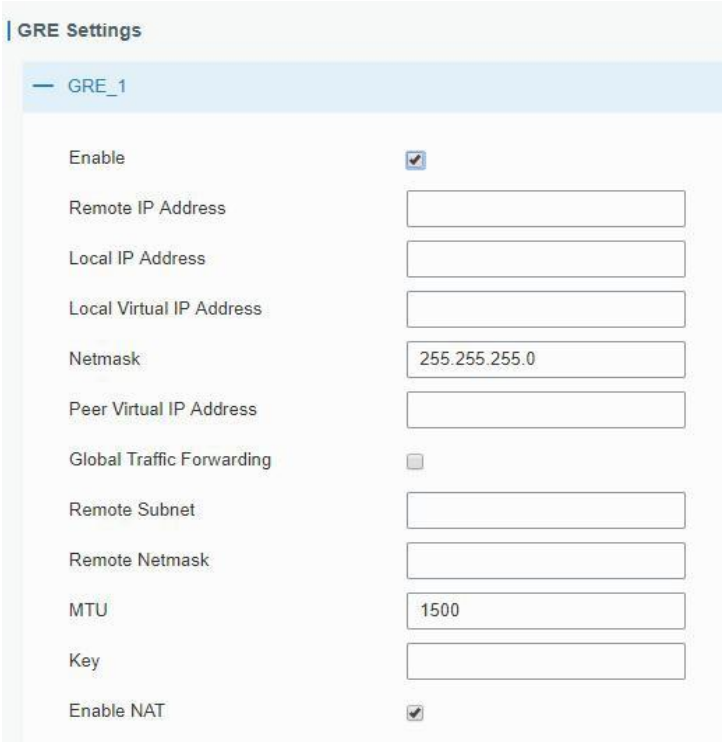


図 3-4-6-5

GRE	
項 目	説明
Enable	GRE 機能を有効にします。
Remote IP Address	GRE トンネルの実際のリモート IP アドレスを入力します。
Local IP Address	ローカル IP アドレスを設定します。
Local Virtual IP Address	GRE トンネルのローカルトンネル IP アドレスを設定します。
Netmask	ローカルのネットマスクを設定します。
Peer Virtual IP Address	GRE トンネルのリモートトンネル IP アドレスを入力します。
Global Traffic Forwarding	この機能を有効にすると、すべてのデータトラフィックが GRE トンネル経由で送信されます。
Remote Subnet	GRE トンネルのリモートサブネット IP アドレスを入力します。
Remote Netmask	GRE トンネルのリモートネットマスクを入力します。
MTU	最大伝送単位を入力します。範囲：64-1500.
Key	GREトンネルのキーを設定します。
Enable NAT	NAT トラバーサル機能を有効にします。

表 3-4-6-4 GRE パラメータ

2.4.6.4 L2TP

L2TP (Layer Two Tunneling Protocol) は、インターネットサービスプロバイダ (ISP) がインターネット上の仮想プライベートネットワーク (VPN) の動作を可能にするために使用する PPTP (Point-to-Point Tunneling Protocol) の拡張です。

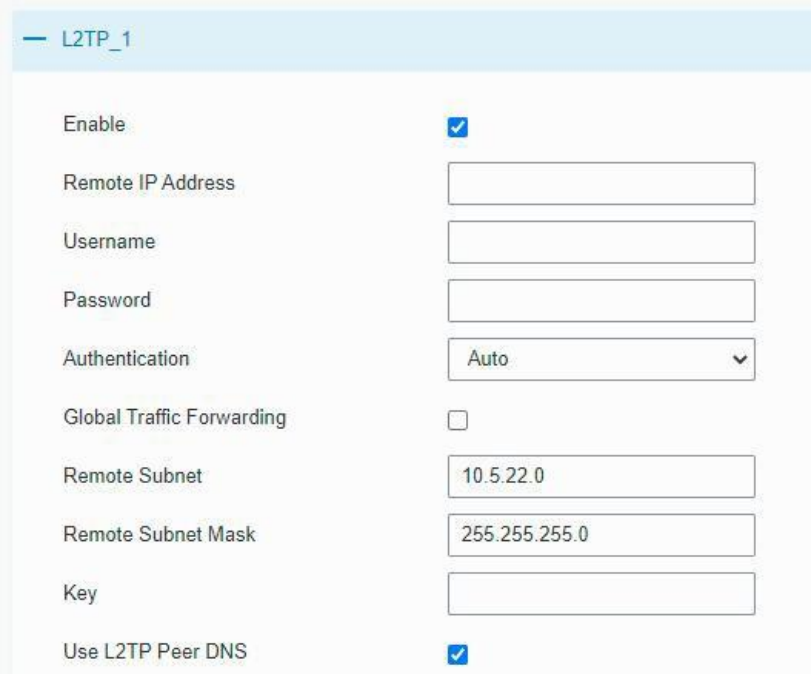


図 3-4-6-6

L2TP	
項目	項目 説明
Enable	L2TP 機能を有効にします。
Remote IP Address	L2TPサーバーのパブリックIPアドレスまたはドメイン名を入力します。
Username	L2TPサーバーが提供するユーザー名を入力します。
Password	L2TPサーバーが提供するパスワードを入力します。
Authentication	「Auto」、「PAP」、「CHAP」、「MS-CHAPv1」、「MS-CHAPv2」から選択します。
Global Traffic Forwarding	この機能を有効にすると、すべてのデータトラフィックが L2TP トンネル経由で送信されます。
Remote Subnet	L2TP が保護するリモート IP アドレスを入力します。
Remote Subnet Mask	L2TPが保護するリモートネットマスクを入力します。
Key	L2TP トンネルのパスワードを入力します。
UseL2TP Peer DNS	ピア L2TP サーバーの DNS アドレスを使用します。

表 3-4-6-5 L2TP パラメータ

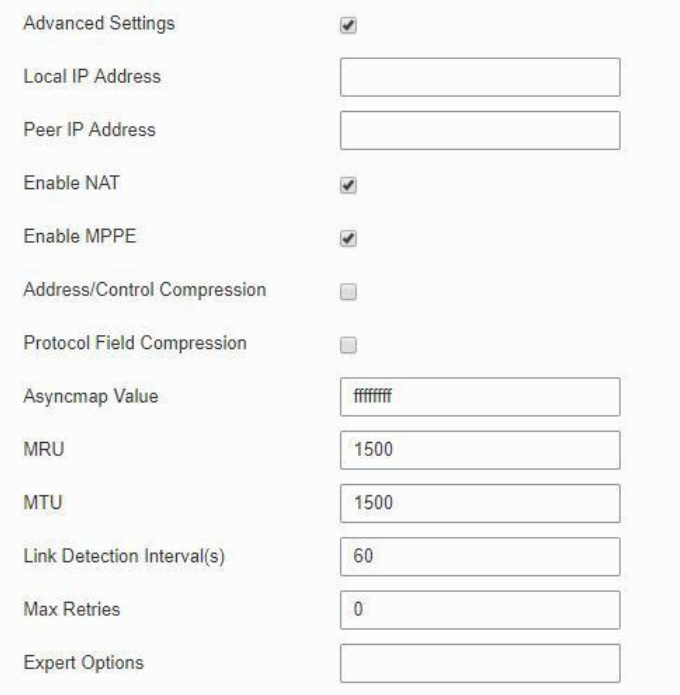


図 3-4-6-7

Advanced Settings	
項目	設定項目
Local IP Address	L2TP クライアントのトンネル IP アドレスを設定します。L2TPクライアントがNULLの場合、クライアントはサーバーから自動的にトンネルIPアドレスを取得します。
Peer IP Address	L2TPサーバーのトンネルIPアドレスを入力します。
Enable NAT	NAT トラバーサル機能を有効にします。
Enable MPPE	MPPE 暗号化を有効にします。
Address/Control Compression	PPP 初期化用。デフォルトのままでもかまいません。
Protocol Field Compression	PPP 初期化用。ユーザはデフォルトのオプションを維持できます。
Asyncmap Value	PPP プロトコル初期化文字列の 1 つ。ユーザはデフォルト値を維持できます。範囲：0-ffffffff。
MRU	最大受信単位を設定します。範囲：64-1500.
MTU	最大送信単位を設定します。範囲：128-1500128-1500
Link Detection Interval (s)	トンネル接続を確保するためのリンク検出間隔時間を設定します。範囲：0-6000-600.
Max Retries	L2TP 接続のフェイルを検出するための最大リトライ回数を設定します。範囲：0-10.
Expert Options	ユーザーは、このフィールドに他の PPP 初期化文字列を空白で区切って入力できます。

表 3-4-6-6 L2TP パラメータ

2.4.6.5 PPTP

ポイントツーポイントトンネリングプロトコル（PPTP）は、企業がパブリックインターネット上のプライベート「トンネル」を介して独自の企業ネットワークを拡張できるようにするプロトコルです。事実上、企業は広域ネットワークを 1 つの大きなローカ

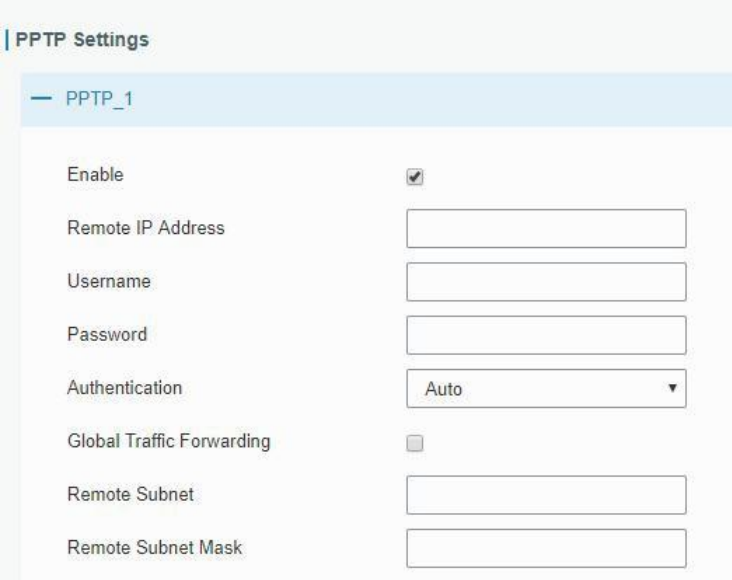


図 3-4-6-8

PPTP	
項目	説明
Enable	PPTP クライアントを有効にします。最大 3 つのトンネルが許可されます。
Remote IP Address	PPTPサーバーのパブリックIPアドレスまたはドメイン名を入力します。
Username	PPTPサーバーが提供するユーザー名を入力します。
Password	PPTPサーバーが提供するパスワードを入力します。
Authentication	Auto」、「PAP」、「CHAP」、「MS-CHAPv1」、「MS-CHAPv2」から選択します。
Global Traffic Forwarding	この機能を有効にすると、すべてのデータトラフィックが PPTP トンネル経由で送信されます。
Remote Subnet	PPTP のピアサブネットを設定します。
Remote Subnet Mask	PPTP サーバーのネットマスクを設定します。

表 3-4-6-7 PPTP パラメータ

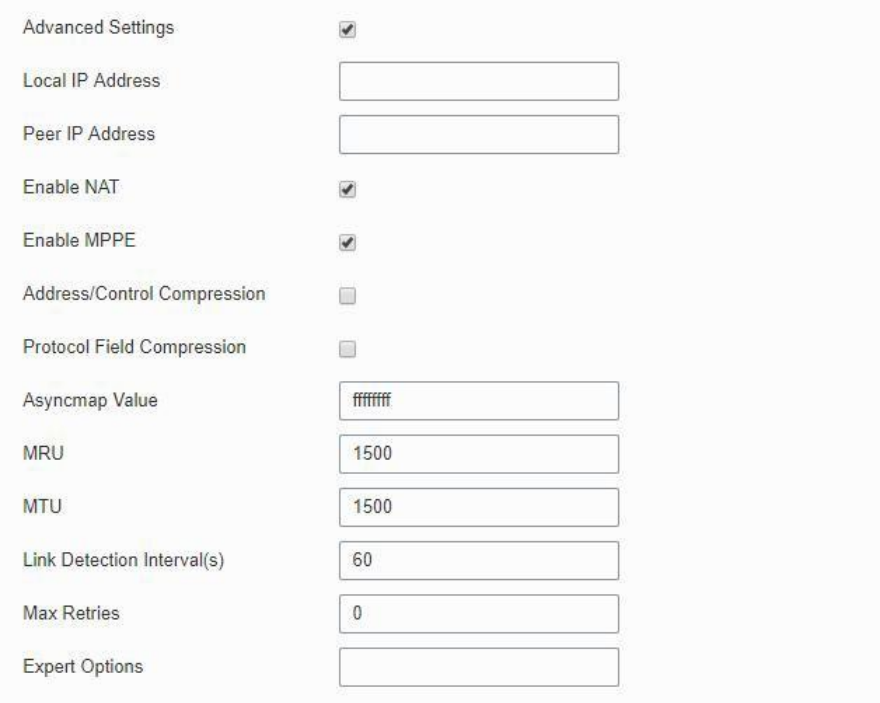


図 3-4-6-9

PPTP Advanced Settings	
項目	説明
Local IP Address	PPTP クライアントの IP アドレスを設定します。
Peer IP Address	PPTP サーバーのトンネル IP アドレスを入力します。
Enable NAT	PPTP の NAT 機能を有効にします。
Enable MPPE	MPPE 暗号化を有効にします。
Address/Control Compression	PPP 初期化用。デフォルトのままでもかまいません。
Protocol Field Compression	PPP 初期化用。ユーザはデフォルトのオプションを維持できます。
Asyncmap Value	PPP プロトコル初期化文字列の 1 つ。ユーザはデフォルト値を維持できます。範囲：0-ffffffff。
MRU	最大受信単位を入力します。範囲：64-1500.
MTU	最大送信単位を入力します。範囲：128-1500：128-1500.
Link Detection Interval (s)	トンネル接続を確保するためのリンク検出間隔時間を設定します。範囲：0-600.
Max Retries	PPTP 接続フェイルを検出するための最大リトライ回数を設定します。範囲：0-10.
Expert Options	ユーザーはこのフィールドに他の PPP 初期化文字列を空白で区切って入力できます。

表 3-4-6-8 PPTP パラメータ

2.4.6.6 OpenVPN クライアント

OpenVPN はオープンソースの仮想プライベートネットワーク (VPN) 製品で、簡素化されたセキュリティフレームワーク、モジュラーネットワーク設計、およびクロスプラットフォームの移植性を提供します。UG65は、同時に最大3つのOpenVPNクライアントの実行をサポートしています。

ovpn ファイルを直接インポートするか、このページのパラメータを設定してクライアントを設定することができます。

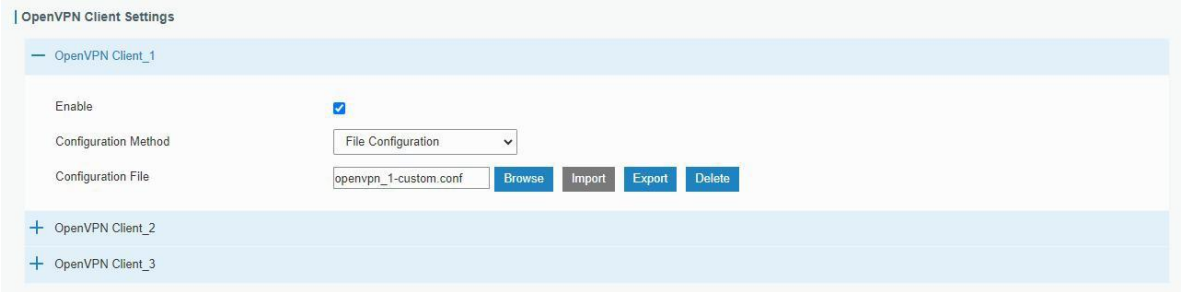


図 3-4-6-10

OpenVPN Client - File Configuration	
項目	説明
Browse	クライアント設定ファイル（ovpn 形式）を参照します。クライアント設定ファイルは、client.confを参考にしてください。
Edit	インポートしたファイルを編集します。
Export	サーバー設定ファイルをエクスポートします。
Delete	設定ファイルを削除します。

表 3-4-6-9 OpenVPN クライアントパラメータ

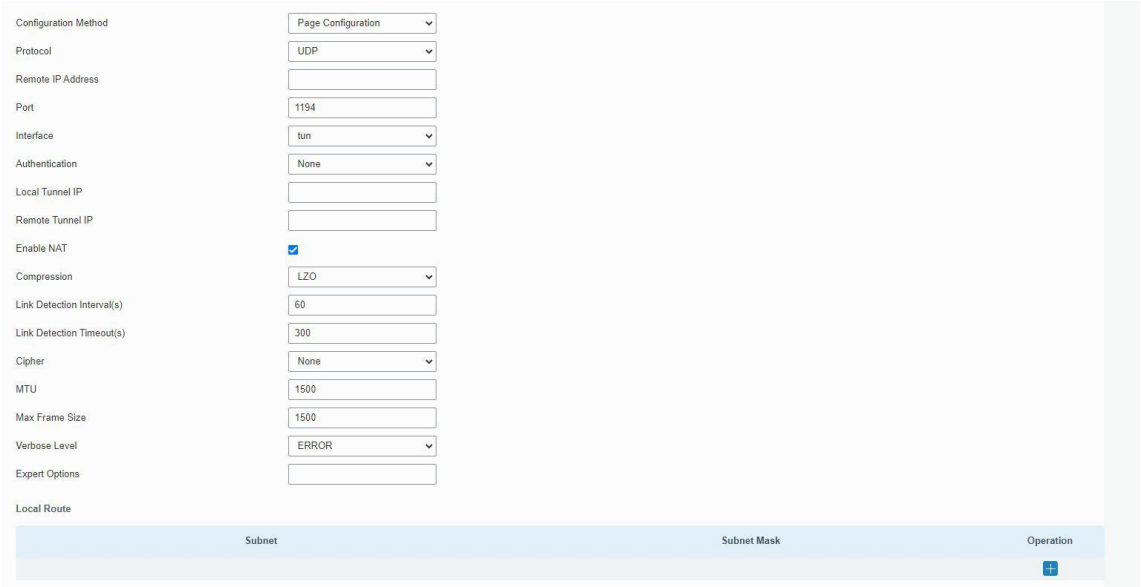


図 3-4-6-11

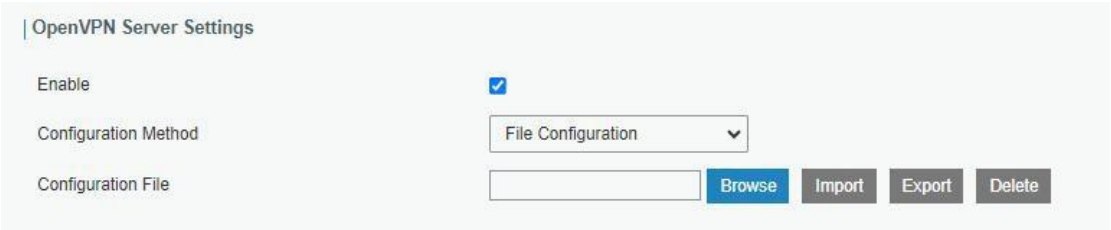
OpenVPN Client - Page Configuration	
項目	設定項目
Protocol	UDP および TCP 接続で使用するトランスポートプロトコルを選択します。
Remote IP Address	リモートOpenVPNサーバーのIPアドレスまたはドメイン名を入力します。
Port	リモート OpenVPN サーバーの TCP/UCP サービス番号を入力します。範囲：1-65535.
Interface	仮想 VPN ネットワークインターフェースのタイプを TUN および TAP から選択します。TUNデバイスはIPv4またはIPv6（OSIレイヤー3）をカプセル化し、TAPデバイスはイーサネット802.3（OSIレイヤー2）をカプセル化します。

Authentication Type	データセッションを保護するために使用する認証タイプを選択します。 **Pre-shared**：サーバーと同じ秘密鍵を使用して認証を完了します。選択後、**Network> VPN> Certifications**ページに進み、静的.keyを**PSK**フィールドにインポートします。 **Username/Password:** サーバー側でプリセットされているユーザー名/パスワードを使用して認証を完了します。 **X.509 cert**： X.509タイプの証明書を使用して認証を完了します。選択後、**[ネットワーク] > [VPN] > [証明書]**ページで、CA証明書、クライアント証明書、クライアント秘密鍵を対応するフィールドにインポートします。 **X.509 cert + user**：ユーザー名/パスワードとX.509証明書認証タイプの両方を使用します。
Local Virtual IP	認証タイプが「**None**」または「**Pre-shared**」の場合に、ローカルトンネルアドレスを設定します。
Remote Virtual IP	認証タイプが「**None**」または「**Pre-shared**」の場合に、リモートトンネルアドレスを設定します。
Global Traffic Forwarding	この機能を有効にすると、すべてのデータトラフィックが OpenVPN トンネル経由で送信されます。
Enable TLS Authentication	認証タイプが X.509 証明書の場合、TLS 認証を無効または有効にします。有効にした後、**Network> VPN> Certifications** ページで、**TA** フィールドに ta.key をインポートします。 **注意:** このオプションは、tls-auth にのみ対応しています。tls-crypt の場合は、エキスパートオプションに次のフォーマット文字列を追加してください: tls-crypt /etc/openvpn/openvpn-client1-ta.key
Compression	データを圧縮する LZO の有効/無効を選択します。
Link Detection Interval (s)	トンネル接続を確保するためのリンク検出間隔時間を設定します。サーバーとクライアントの両方で設定した場合、サーバーからプッシュされた値がクライアントのローカル値を上書きします。範囲：10-1800 s.
Link Detection Timeout (s)	タイムアウト後に OpenVPN を再確立します。サーバーとクライアントの両方で設定した場合、サーバーからプッシュされた値がクライアントのローカル値より優先されます。範囲：60-3600 s.
Cipher	NONE、BF-CBC、DES-CBC、DES-EDE3-CBC、AES-128-CBC、AES-192-CBC、AES-256-CBC から選択します。
MTU	最大伝送単位を入力します。範囲：128-1500.
Max Frame Size	最大フレームサイズを設定します。範囲：128-1500：128-1500.
Verbose Level	ERROR、WARING、NOTICE、DEBUG から選択します。
Expert Options	ユーザはこのフィールドにいくつかの初期化文字列を入力し、文字列をセミコロンで区切ることができます。 **例:** ncp-ciphers AES-128-GCM; キー方向 1
ローカルルート	
Subnet	ローカルルートの IP アドレスを設定します。
Subnet Mask	ローカルルートのネットマスクを設定します。

表 3-4-6-10 OpenVPN クライアントパラメータ

2.4.6.7 OpenVPN サーバー

UG65 は、ルーティングまたはブリッジ構成およびリモートアクセス設備で安全なポイント-ツー-ポイントまたはサイト-ツー-サイト接続を作成するための OpenVPN



サーバーをサポートしています。ovpnファイルを直接インポートするか、このページのパラメータを設定して、このサーバーを設定することができます。

図 3-4-6-12

OpenVPN Server - File Configuration	
項目	説明
Browse	サーバー設定ファイル（ovpn 形式）を参照します。サーバ設定ファイルは、server.confを参考にしてください。
Edit	インポートしたファイルを編集します。
Export	サーバー設定ファイルをエクスポートします。
Delete	設定ファイルを削除します。

表 3-4-6-11 OpenVPN サーバーパラメータ

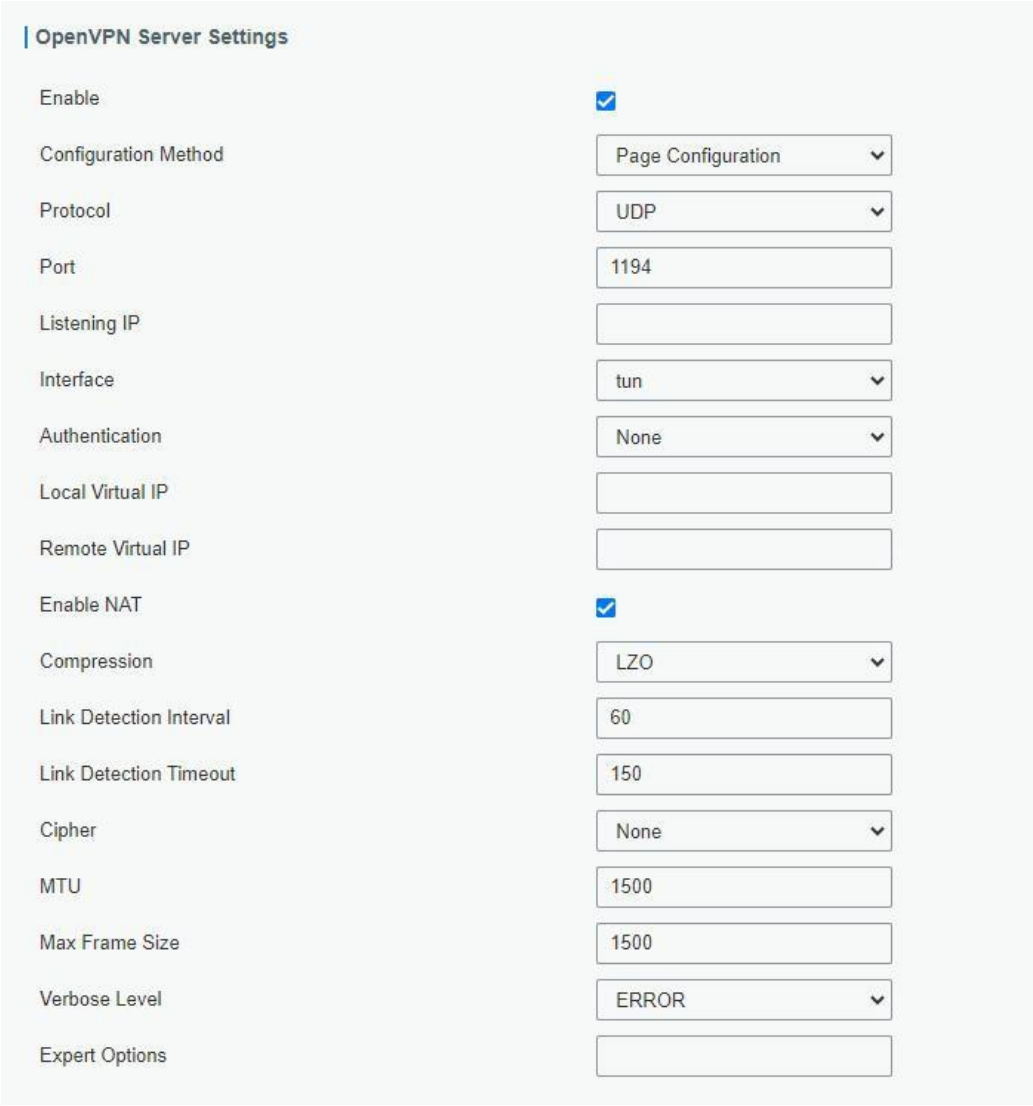


図 3-4-6-13

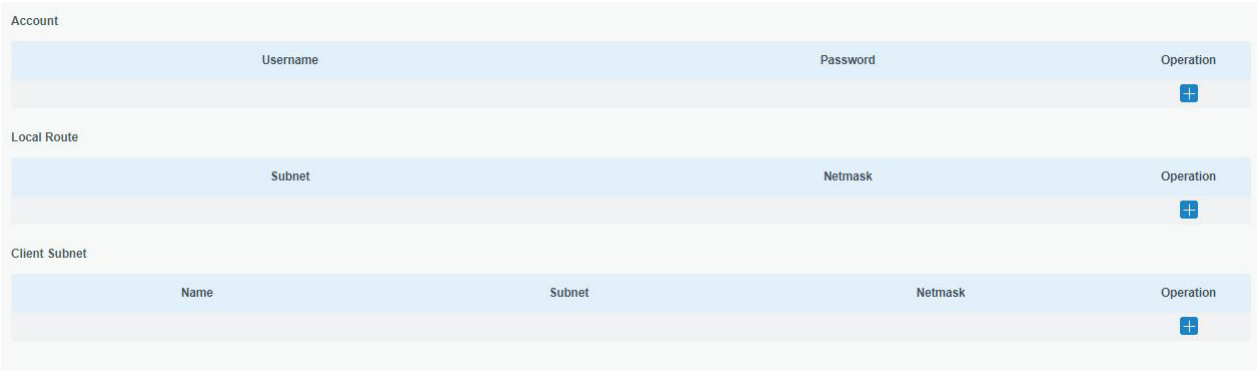


図 3-4-6-14

OpenVPN Server - Page Configuration	
項目	設定項目
Protocol	接続に使用するトランスポートプロトコルを UDP と TCP から選択します。
Listening IP	バインドするローカルホスト名またはIPアドレスを入力します。空白の場合、OpenVPNサーバはすべてのインタフェースにバインドします。
Port	OpenVPN クライアント接続用の TCP/UCP サービス番号を入力します。範囲：1-65535.

Interface	仮想 VPN ネットワークインターフェースのタイプを TUN および TAP から選択します。TUNデバイスはIPv4またはIPv6（OSIレイヤー3）をカプセル化し、TAPデバイスはイーサネット802.3（OSIレイヤー2）をカプセル化します。
Authentication Type	データセッションを保護するために使用する認証タイプを選択します。 **Pre-shared**：サーバーと同じ秘密鍵を使用して認証を完了します。選択後、**Network> VPN> Certifications**ページに進み、静的.keyを**PSK**フィールドにインポートします。 **ユーザー名/パスワード:** サーバー側でプリセットされているユーザー名/パスワードを使用して認証を完了します。 **X.509証明書:** X.509タイプの証明書を使用して認証を完了します。選択後、**Network > VPN > Certifications**ページで、CA証明書、クライアント証明書、クライアント秘密鍵を対応するフィールドにインポートします。 **X.509証明書+ユーザー**：ユーザー名/パスワードとX.509証明書の両方の認証タイプを使用します。
Local Virtual IP	認証タイプが「**None**」または「**Pre-shared**」の場合に、ローカルトンネルアドレスを設定します。
Remote Virtual IP	認証タイプが「**None**」または「**Pre-shared**」の場合に、リモートトンネルアドレスを設定します。
Client Subnet	openVPNクライアントのIPアドレスプールを定義します。
Client Netmask	IPアドレスの範囲を制限するために、クライアントサブネットのネットマスクを設定します。
Renegotiation Interval	この間隔の後にデータチャネルキーを再ネゴシエートします。0 は無効を意味します。
Max Clients	サーバを最大同時クライアント数に制限します：1-20. **注：**多数のクライアントを接続する必要がある場合は、ログの重要度を「情報」に調整してください。
Enable CRL	CRLの検証を有効または無効にします。
Enable Client to Client	有効にすると、openVPN クライアント間で通信できます。
Enable Dup Client	複数のクライアントが同じコモンネームまたは証明書で接続できるようにします。
Enable TLS Authentication	認証タイプが X.509 証明書の場合、TLS 認証を無効または有効にします。有効にした後、**Network> VPN> Certifications** ページで、**TA** フィールドに ta.key をインポートします。 **注意:** このオプションは、tls-auth にのみ対応しています。tls-crypt の場合は、エキスパートオプションに以下のフォーマット文字列を追加してください。 /etc/openvpn/openvpn-client1-ta.key。
Compression	データを圧縮する LZO の有効/無効を選択します。
Link Detection Interval (s)	トンネル接続を確保するためのリンク検出間隔時間を設定します。サーバーとクライアントの両方で設定した場合、サーバーからプッシュされた値がクライアントのローカル値を上書きします。範囲：10-1800 s.
Link Detection Timeout (s)	タイムアウト後に OpenVPN を再確立します。サーバーとクライアントの両方で設定した場合、サーバーからプッシュされた値がクライアントのローカル値より優先されます。範囲：60-3600 s.
Cipher	NONE、BF-CBC、DES-CBC、DES-EDE3-CBC、AES-128-CBC、AES-192-CBC、AES-256-CBC から選択します。
MTU	最大伝送単位を入力します。範囲：64-1500.

Max Frame Size	最大フレームサイズを設定します。範囲：64-1500.
Verbose Level	ERROR、WARING、NOTICE、DEBUGから選択します。
Expert Options	ユーザはこのフィールドにいくつかの初期化文字列を入力し、文字列をセミコロンで区切ることができます。 例: ncp-ciphers AES-128-GCM; キー方向 1
アカウント	
Username & Password	認証タイプがユーザー名/パスワードの場合、OpenVPN クライアントのユーザー名とパスワードを設定します。
ローカルルート	
Subnet	ローカルルートのIPアドレスを設定します。
Subnet Mask	ローカルルートのネットマスクを設定します。
クライアントサブネット	
Name	OpenVPN クライアント証明書のコモンネームとして設定します。
Subnet	OpenVPN クライアントのサブネットを設定します。
Subnet Mask	OpenVPN クライアントのサブネットネットマスクを設定します。

表 3-4-6-12 OpenVPN サーバーパラメーター

2.4.6.8 認証

OpenVPN サーバー、OpenVPN クライアント、または IPsec サーバーとして動作する場合、ユーザーは認証タイプに応じて必要な証明書と鍵ファイルをこのページにインポート/エクスポートすることができます。

図 3-4-6-15

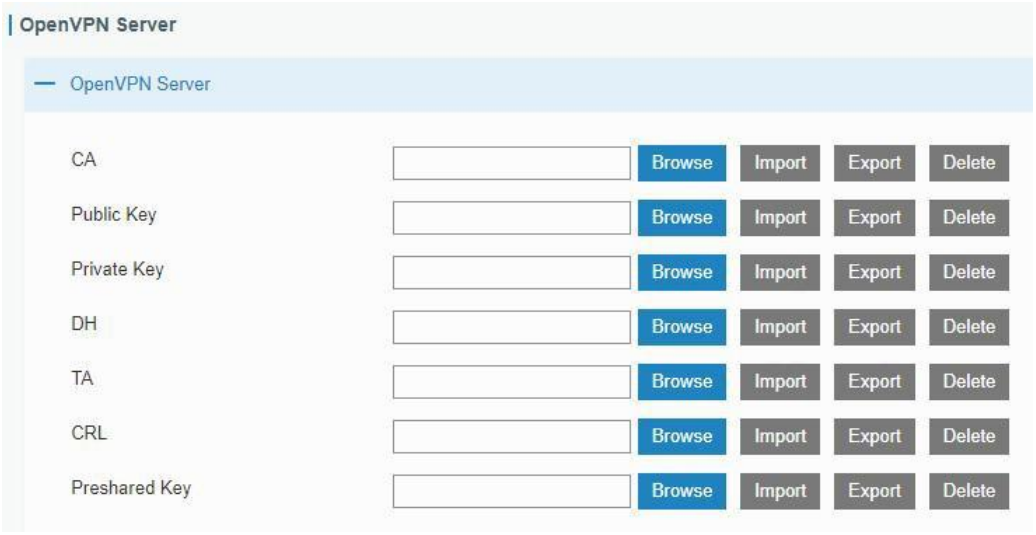


図 3-4-6-16

図 3-4-6-17

2.4.6.9 ワイヤガード

WireGuard は、最先端の暗号化技術を利用した非常にシンプルかつ高速な最新の VPN です。WireGuard は UDP プロトコルでトラフィックをパスします。

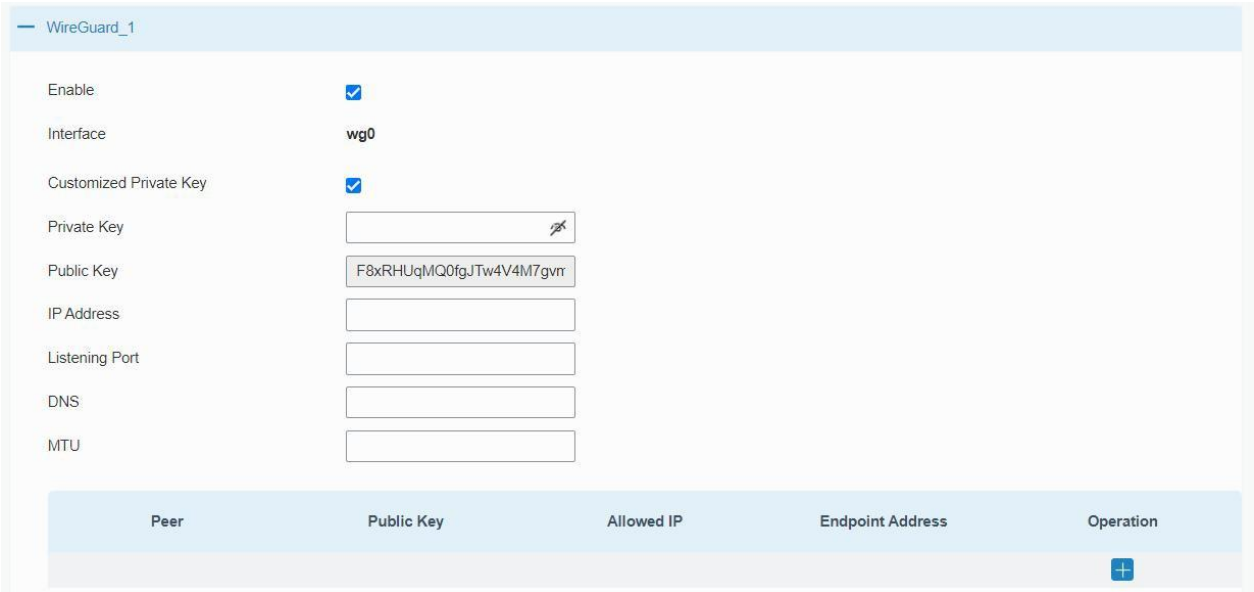


図3-4-6-18

WireGuard	
項目	説明
Enable	WireGuard インタフェースを有効にします。最大3つのWireGuardインタフェースを使用できます。
Interface	WireGuard インタフェース名を表示します。
Customized Private Key	このWireGuardインタフェースの秘密鍵をカスタマイズするために有効または無効にします。無効の場合、クライアントはこのルータが生成した秘密鍵を使用します。
Public Key	秘密鍵によって生成された公開鍵を表示します。
IP Address	ローカル仮想 IP アドレスとネットマスクを設定します。例：10.8.0.2/24
Listening Port	WireGuardパケットを送受信するポートを設定します。異なるWireGuardインターフェースのポート番号は異なる必要があります。
DNS	このWireGuardインターフェースのDNSサーバーアドレスを設定します。空白のままにすると、ルーターは一般的なネットワークインターフェイス (WAN、携帯電話など) の DNS サーバーアドレスを使用します。
MTU	このWireGuardインタフェースの最大伝送単位を設定します。空白のままにすると、ルーターは共通ネットワークインターフェイス (WAN、携帯電話など) の MTU を使用します。
Peer Table	をクリックすると、このWireGuardインターフェイスのWireGuardピアが追加されます。 1つのWireGuardインターフェースは最大20のピアを追加できます。

表 3-4-6-13 WireGuard パラメータ

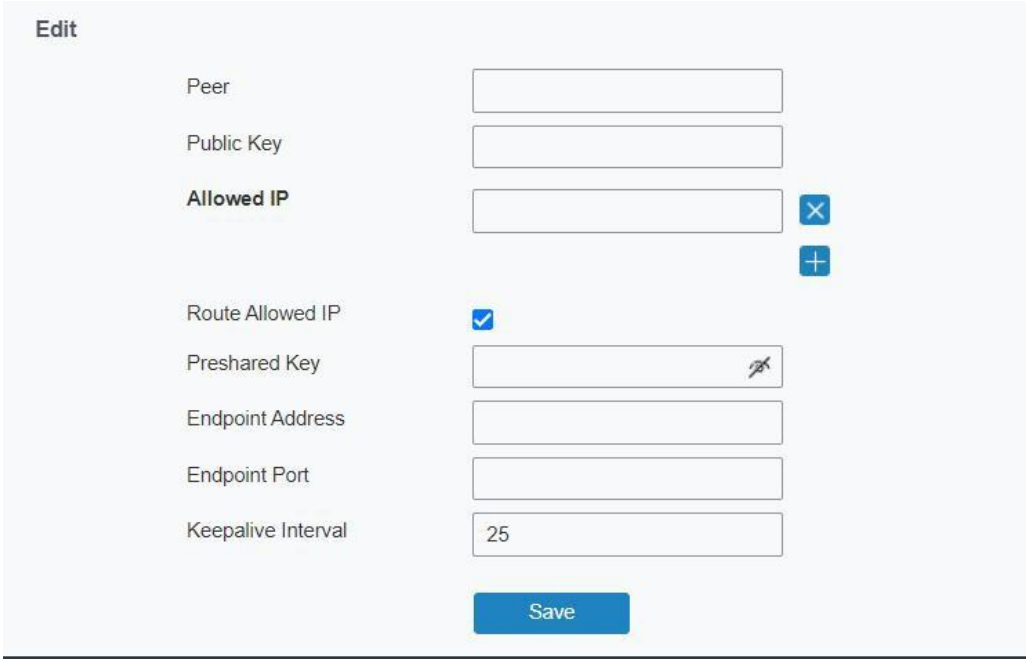


図 3-4-6-19

WireGuard-Peer	
項目	項目
Peer	WireGuard ピア名を設定します。この名前は、この WireGuardクライアント内で一意である必要があります。

Public Key	WireGuard ピアサーバ/クライアントの公開鍵を設定します。
Allowed IP	WireGuardピアのLANネットワークの実際のIPアドレスとネットマスクを設定します。例: 192.168.1.0/24 1つのWireGuardピアで8つの許可IPアドレスを追加できます。
Route Allowed IP	許可された IP アドレスの静的ルーティングを追加するかどうかを設定します。
Preshared Key	事前共有キーを設定し、このインタフェースとピアインタフェースの両方で同じキー値を設定する必要があります。
Endpoint Address	WireGuardピアサーバー/クライアントのIPアドレスまたはドメイン名を設定します。
Endpoint Port	WireGuard ピアサーバー/クライアントの宛先ポートを設定します。
Keepalive Interval	接続が確立されると、このWireGuardインターフェースは定期的にハートビート・パケットを送信して、接続を維持します。0 は無効を意味します。

表 3-4-6-13 WireGuard-Peer パラメータ

3.5 システム

このセクションでは、管理アカウント、アクセスサービス、システム時間、共通ユーザー管理、SNMP、イベントアラームなどの一般設定の構成方法について説明します。

3.5.1 一般設定

3.5.1.1 一般設定

一般設定には、システム情報、アクセスサービス、HTTPS 証明書が含まれます。

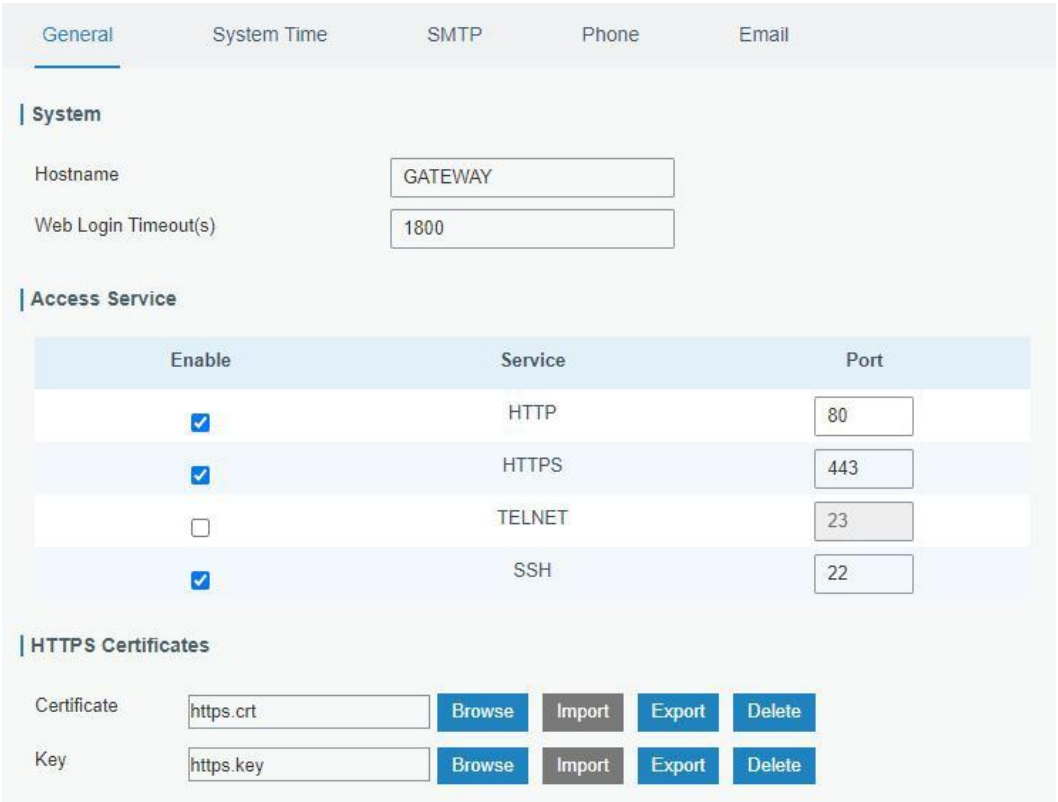


図 3-5-1-1

General		
設定項目	設定内容	デフォルト
System		
Hostname	ユーザー定義のゲートウェイ名。	GATEWAY
Web Login Timeout (s)	タイムアウトした場合、再度ログインする必要があります。範囲：100-3600.	1800
Access Service		
Port	サービスのポート番号を設定します。範囲：1-65535.	--
HTTP	このオプションをオンにすると、ユーザーはHTTP経由でデバイスにローカルにログインし、Web経由でデバイスにアクセスして制御できます。	80
HTTPS	オプションをオンにすると、ユーザーは HTTPS 経由でデバイスにローカルおよびリモートでログインし、Web 経由でアクセスおよび制御できます。	443
TELNET	ユーザーは、TELNET 経由でデバイスにローカルおよびリモートでログインし、オプショ ンをオンにした後に Web 経由でアクセスおよび制御できます。	23
SSH	オプションにチェックを入れると、ユーザーは SSH 経由でデバイスにローカルおよびリモートでログインできます。	22
HTTPS Certificates		
Certificate	Browse"（参照）ボタンをクリックし、PC 上の証明書ファイルを選択し、"Import"（イン ポート）ボタンをクリックしてファイルをゲートウェイにアップロードします。Export "ボタンをクリックすると、ファイルが PC にエクスポートされます。削除」ボタンをクリックすると、ファイルを削除します。	--
Key	Browse "ボタンをクリックし、PC上のキーファイルを選択し、"Import "ボタンをクリックし、ファイルをゲートウェイにアップロードします。Export "ボタンをクリックすると、ファイルをPCにエクスポートします。 Delete "ボタンをクリックするとファイルが削除されます。	--

表 3-5-1-1 一般設定パラメータ

3.5.1.2 システム時刻

このセクションでは、タイムゾーンと時刻同期タイプを含むシステム時刻の設定方法について説明します。

注：ゲートウェイが正しい時刻で動作するように、ゲートウェイを設定する際にシステム時刻を設定することを推奨します。

図 3-5-1-2

システム時間	
項目	説明
Current Time	現在のシステム時刻を表示します。
Time Zone	ドロップダウンリストをクリックして、タイムゾーンを選択します。
Sync Type	ドロップダウンリストをクリックして、時刻同期のタイプを選択します。 **ブラウザと同期**：ブラウザと時刻を同期します。 **NTPサーバーと同期**：NTPサーバーと時刻を同期します。 **手動で設定**：手動で時刻を設定します。
NTPサーバーと同期	
NTP Server Address	NTPサーバーのアドレス（ドメイン名/IP）を設定します。
Enable NTP Server	チェックを入れると、ネットワーク上の NTP クライアントがゲートウェイと時刻同期を行うことができます。

表 3-5-1-2 システム時刻パラメータ

3.5.1.3 SMTP

SMTP は Simple Mail Transfer Protocol の略で、電子メールの送受信に使用される TCP/IP プロトコルです。ここでは、電子メールの設定方法について説明します。

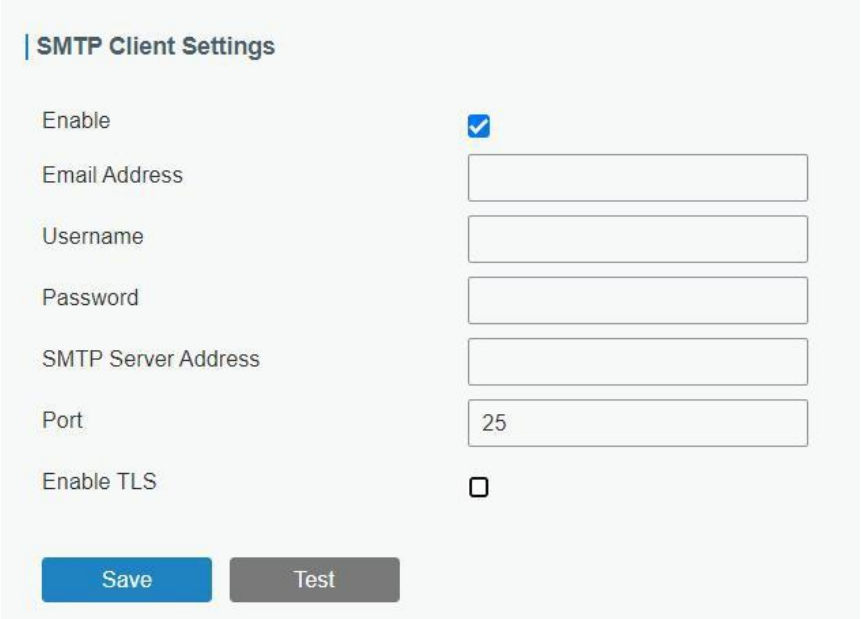


図 3-5-1-3

SMTP	
項目	説明
SMTP Client Settings	
Enable	SMTPクライアント機能の有効/無効を設定します。
Email Address	送信者のメールアドレスを入力します。
Username	送信者のユーザー名を入力します。
Password	送信者のメールパスワードを入力します。

SMTP Server Address	SMTPサーバーのドメイン名を入力します。
Port	SMTPサーバーのポートを入力します。範囲：1-65535.
Enable TLS	TLS 暗号化を有効または無効にします。

表 3-5-1-3 SMTP 設定

関連項目

イベント設定

3.5.1.4 電話

電話の設定は、イベントのコール/SMS トリガーと SMS アラームに関係します。これは、セルラー機能を持つゲートウェイにのみ適用されます。

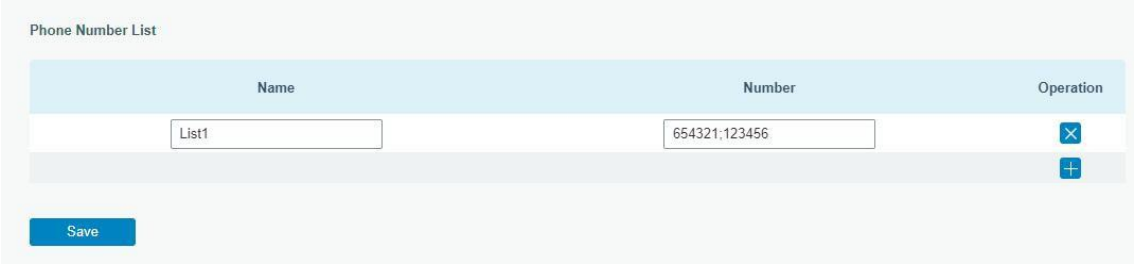


図 3-5-1-4

Phone	
項目	説明
Phone Number List	
Name	電話グループ名を設定します。
Number	電話番号を入力します。桁、"+"、"-"が使用できます。複数の番号を「;」で分割できます。

表3-5-1-4 電話設定

関連項目

オンデマンド接続

3.5.1.5 電子メール

電子メールの設定は、イベントに対する電子メールアラームに関係します。

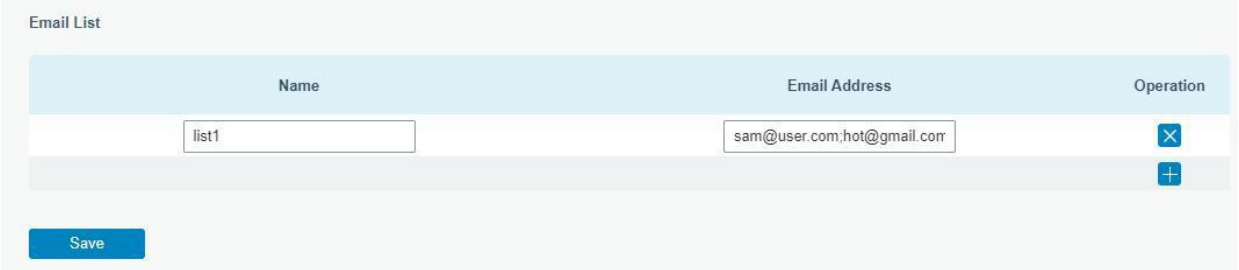


図 3-5-1-5

Email	
項目	メール項目
Email List	
Name	メールグループ名を設定します。
Email Address	メールアドレスを入力します。複数のメールアドレスを"; "で区切ることができます。

表 3-5-1-5 メール設定

3.5.2 ユーザー管理

3.5.2.1 アカウント

ここでは、管理者のログインユーザー名とパスワードを変更できます。

注意：セキュリティのため、変更することを強くお勧めします。

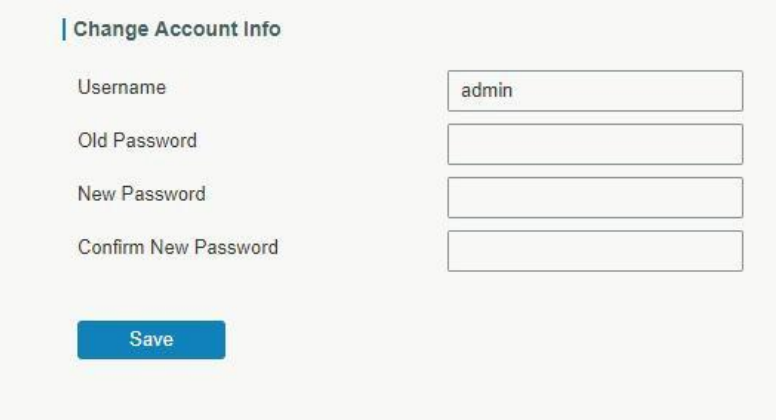


図 3-5-2-1

Account	
項目	項目
Username	新しいユーザー名を入力します。a-z、0-9、"_"、"-"などの文字を使用できます。最初の文字は数字にすることはできません。
Old Password	古いパスワードを入力します。
New Password	新しいパスワードを入力します。空白以外の ASCII 文字を使用できます。
Confirm New Password	新しいパスワードをもう一度入力します。

表 3-5-2-1 アカウント情報

3.5.2.2 ユーザー管理

共通ユーザーアカウントの作成方法について説明します。

共通ユーザー権限には、「Read-Only」と「Read-Write」があります。

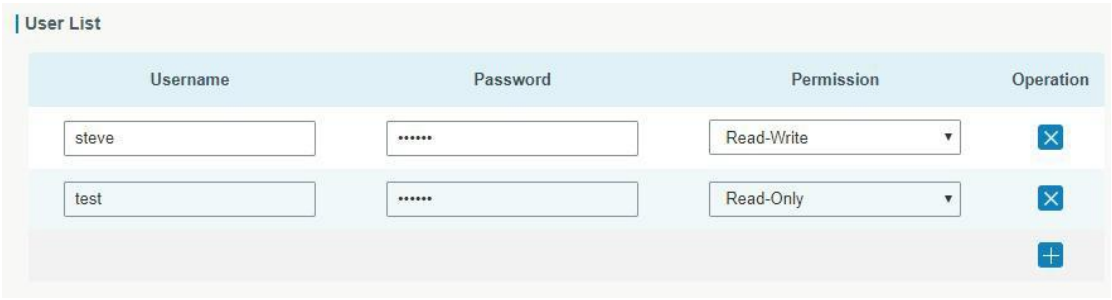


図 3-5-2-2

User Management	
項目	ユーザー名
Username	新しいユーザー名を入力します。a-z、0-9、"_"、"-"などの文字を使用できます。最初の文字は数字にすることはできません。
Password	パスワードを設定します。空白以外のASCII文字が使用できます。
Permission	Read-Only "と "Read-Write "からユーザの権限を選択します。 - Read-Only：ユーザはこのレベルのゲートウェイのコンフィギュレーションを閲覧することしかできません。 - Read-Write：ユーザはこのレベルでゲートウェイのコンフィグレーションの表示と設定ができます。

表 3-5-2-2 ユーザー管理

3.5.3 SNMP

SNMP は、ネットワーク監視のためにネットワーク管理で広く使用されています。SNMP は、管理されるシステム内の変数形式で管理データを公開します。SNMP は、管理対象システム内の変数で管理データを公開します。 これらの変数は、管理アプリケーションからリモートで照会できます。

ネットワーク、NMS、およびSNMPの管理プログラムでのSNMPの設定は、マネージャで設定する必要があります。

NMS からのクエリを実現するための設定手順を以下に示します：

1. SNMPの設定を有効にします。
2. MIBファイルをダウンロードし、NMSにロードします。
3. MIBビューを設定します。
4. VCAMを設定します。

3.5.3.1 SNMP

UG65はSNMPv1、SNMPv2c、SNMPv3をサポートしています。SNMPv1とSNMPv2cはコミュニティ名認証を採用しています。SNMPv3 は、ユーザー名とパスワードによる認証暗号化を採用しています。

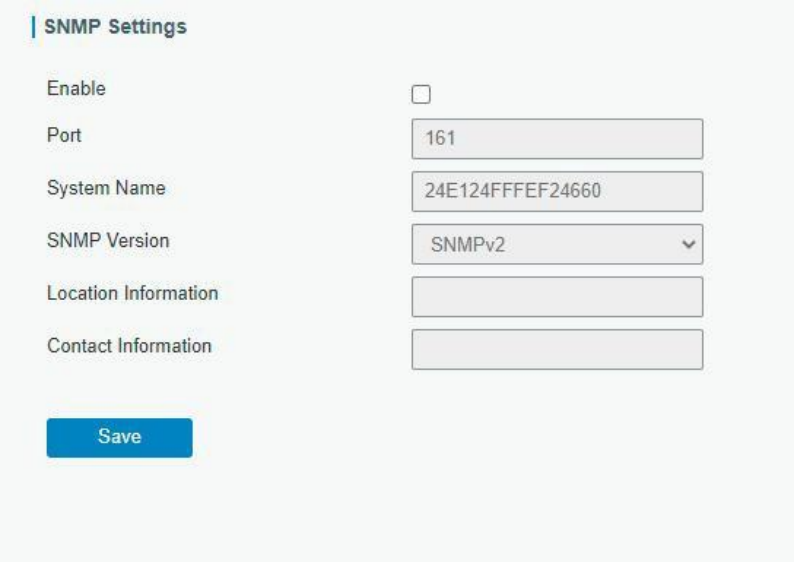


図 3-5-3-1

SNMP Settings	
設定項目	設定項目
Enable	SNMP 機能を有効または無効にします。
Port	SNMPをリッスンするポートを設定します。範囲：1-65535. デフォルトは161です。
System Name	ゲートウェイを表すシステム名を入力します。
SNMP Version	SNMP v1/v2c/v3をサポートします。
Location Information	所在地情報を入力します。
Contact Information	連絡先情報を入力します。

表 3-5-3-1 SNMP パラメータ

3.5.3.2 MIBビュー

オブジェクトの MIB ビューの設定方法を説明します。

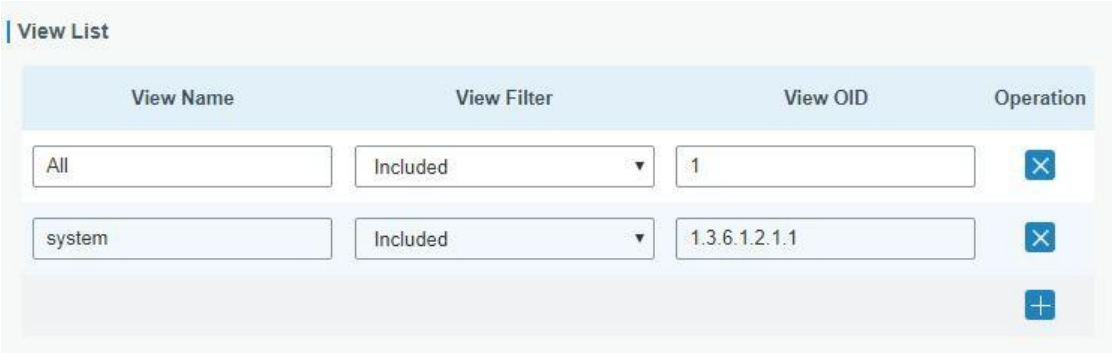


図 3-5-3-2 MIB ビュー

MIB View	
表示項目	ビュー名
View Name	MIB ビューの名称を設定します。
View Filter	含む」「含まない」から選択します。

View OID	OID番号を入力します。
Included	指定したMIBノード内のすべてのノードを照会できます。
Excluded	指定した MIB ノード以外のすべてのノードを照会できます。

表 3-5-3-2 MIB View パラメータ

3.5.3.3 VACM

VCAM パラメータの設定方法を説明します。

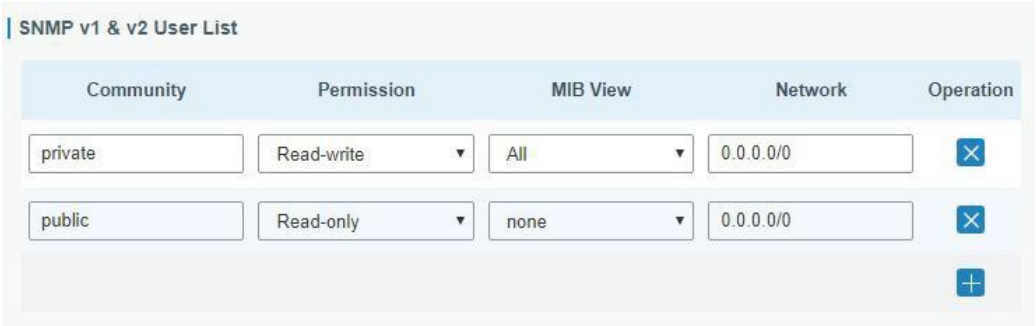


図 3-5-3-3

VACM	
項目	設定項目
SNMP v1 & v2 User List	
Community	コミュニティ名を設定します。
Permission	Read-Only」と「Read-Write」から選択します。
MIB View	MIBビュー一覧からパーミッションを設定するMIBビューを選択します。
Network	MIBビューにアクセスする外部ネットワークのIPアドレスとビットを指定します。
Read-Write	指定したMIBノードの読み書き権限です。
Read-Only	指定されたMIBノードの権限は読み取り専用です。
SNMP v3 User List	
Group Name	SNMPv3のグループ名を設定します。
Security Level	NoAuth/NoPriv」、「Auth/NoPriv」、「Auth/Priv」から選択します。
Read-Only View	MIBビュー一覧から、権限を「読み取り専用」に設定するMIBビューを選択します。
Read-Write View	MIBビューの一覧から、権限を「Read-write」に設定するMIBビューを選択します。
Inform View	MIB ビュー一覧から、権限を「Inform」に設定する MIB ビューを選択します。

表 3-5-3-3 VACM パラメータ

3.5.3.4 トラップ

SNMP トラップによるネットワーク監視を有効にする方法を説明します。

図 3-5-3-4

SNMP Trap	
項目	内容
Enable	SNMP トラップ機能を有効または無効にします。
SNMP Version	SNMP v1/v2c/v3をサポートします。
Server Address	NMSのIPアドレスまたはドメイン名を入力します。
Port	UDPポートを入力します。ポート範囲は1～65535です。デフォルトのポートは162です。
Name	SNMP v1/v2cを使用する場合はグループ名を、SNMP v3を使用する場合はユーザー名を入力します。
Auth/Priv Mode	NoAuth & NoPriv」、「Auth & NoPriv」、「Auth & Priv」から選択します。

表 3-5-3-4 トラップパラメータ

3.5.3.5 MIB

MIB ファイルのダウンロード方法について説明します。

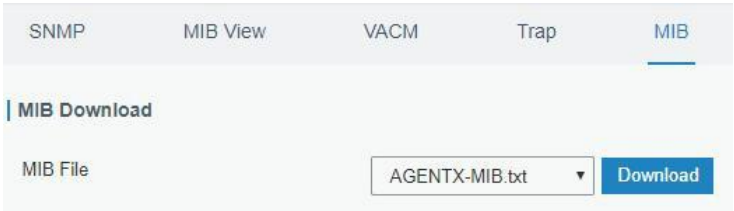


図 3-5-3-5

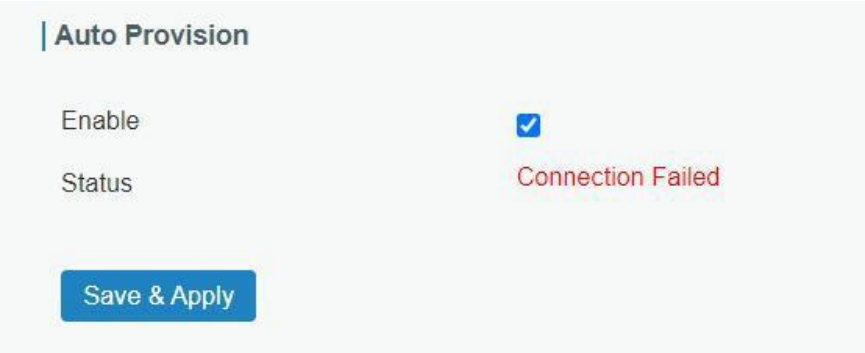
MIB	
項目	説明
MIB File	必要な MIB ファイルを選択します。
Download	Downloadボタンをクリックすると、MIB ファイルを PC にダウンロードします。

表 3-5-3-5 MIB ダウンロード

3.5.4 機器管理

3.5.4.1 自動設定

ユーザはMilesight Development Platformからコンフィギュレーション・プロファイルをカスタマイズして選択することができます。オートプロビジョニングが有効で、デバイスがインターネットに接続されている場合、デバイスは初期設定を行うためのプロファイルを受信します。この機能は、デバイスがMilesight Development Platformに接続していない場合でも機能します。



3.5.4.2 管理プラットフォーム

このページでデバイスをDeviceHubまたはMilesight Development Platformに接続し、ゲートウェイを一元的かつリモートで管理することができます。

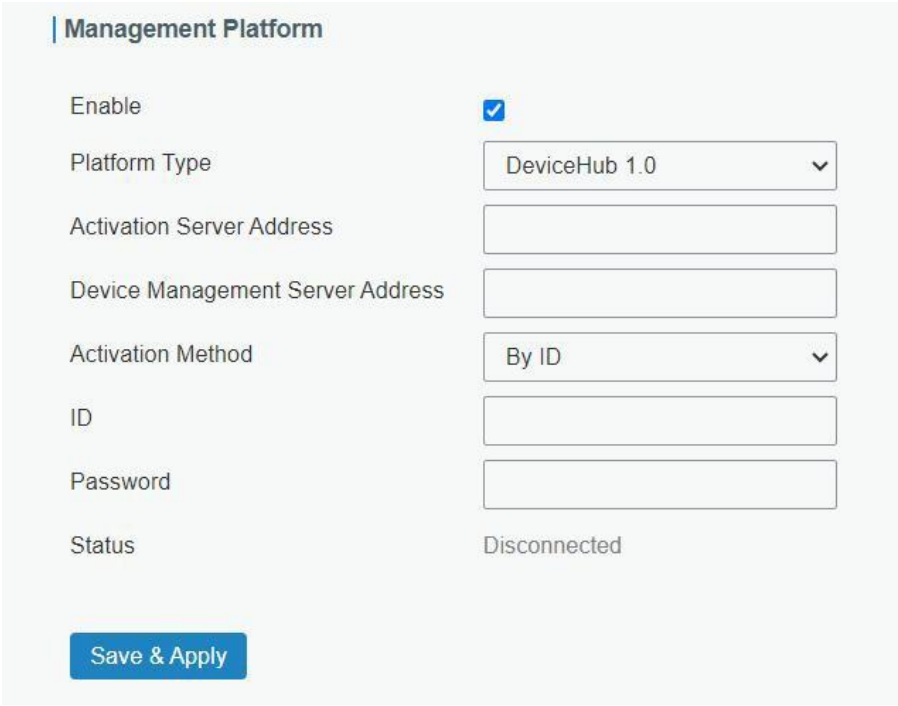


図 3-5-4-1

Management Platform	
項目	説明
Enable	ゲートウェイを管理プラットフォームに接続するかどうかを設定します。
Platform Type	Milesight DeviceHub 1.0、Milesight DeviceHub 2.0またはMilesight Development Platformはオプションです。
Status	ゲートウェイと管理プラットフォームの接続状態を表示します。
DeviceHub 1.0	
Activation Server Address	DeviceHubのIPアドレスまたはドメイン。

DeviceHub Management Address	デバイスがDeviceHubに接続するためのURLアドレス（例：http://220.82.63.79:8080/acs）。
Activation Method	ゲートウェイをDeviceHubサーバーに接続する認証方法を選択します。オプションは "認証IDによる "と "IDによる "です。
Authentication Code	DeviceHubから生成された認証コードを入力します。
ID	登録したDeviceHubアカウント（Eメール）とパスワードを入力します。
Password	
DeviceHub 2.0	
Server Address	DeviceHubのIPアドレスまたはドメイン。

表3-5-4-1

3.5.5 イベント

イベント機能は、特定のシステムイベント発生時に電子メールでアラートを送信する機能です。

3.5.5.1 イベント

このページではアラームメッセージを見ることができます。

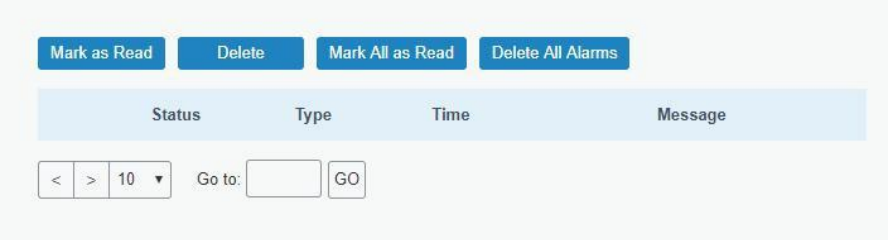


図 3-5-5-1

Events	
項目	説明
Mark as Read	選択したイベントアラームを既読にします。
Delete	選択したイベントアラームを削除します。
Mark All as Read	すべてのイベントアラームを既読にします。
Delete All Alarms	すべてのイベントアラームを削除します。
Status	イベントアラームの読み取りステータスを表示します。
Type	アラームするイベントタイプを表示します。
Time	アラーム時刻を表示します。
Message	アラーム内容を表示します。

表 3-5-5-1 イベントパラメータ

3.5.5.2 イベント設定

このセクションでは、記録するイベントと、変化が発生したときに電子メールと SMS 通知を受信するかどうかを決定できます。

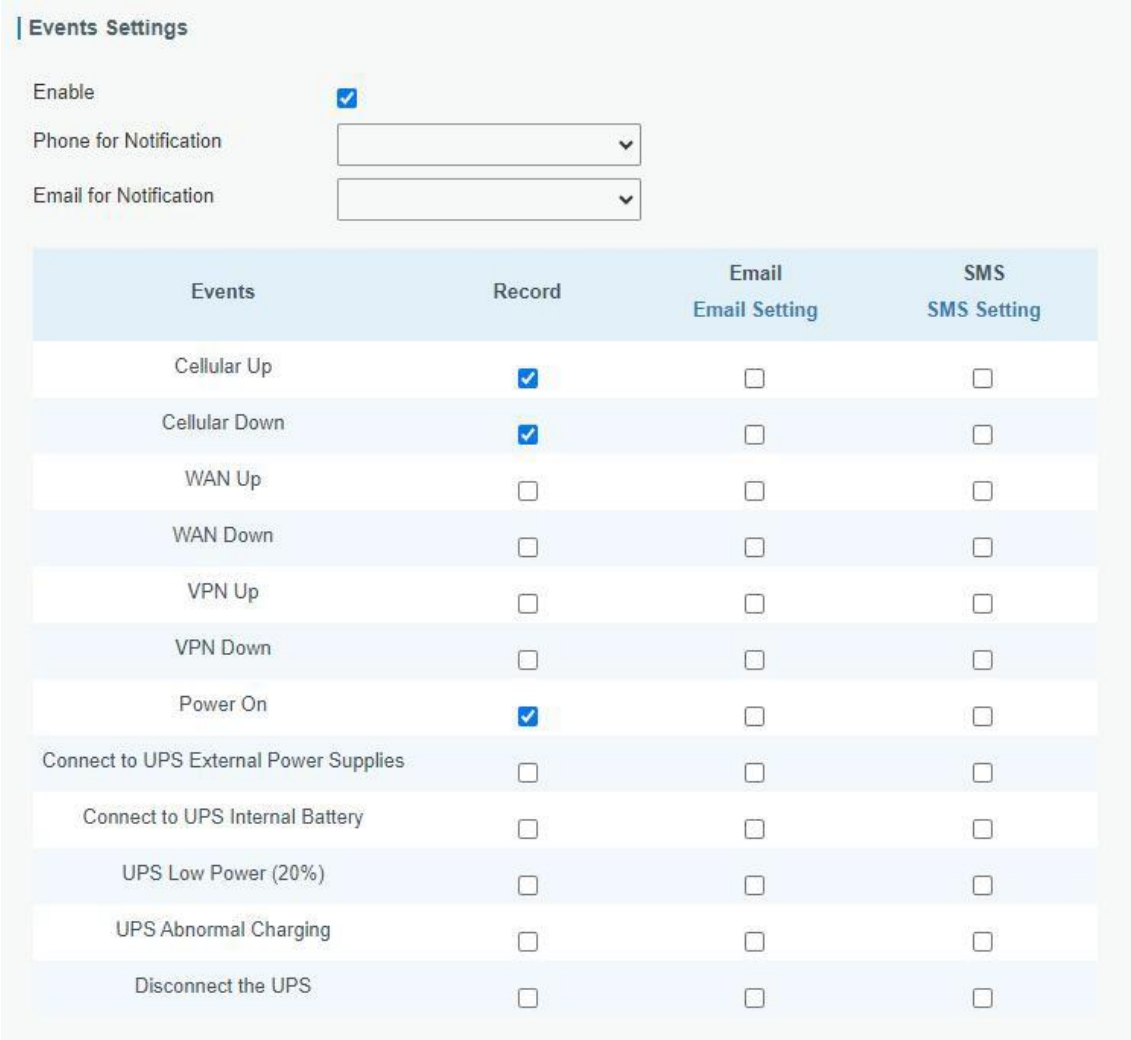


図 3-5-5-2

Event Settings	
設定項目	設定項目
Enable	イベント設定」を有効にします。
Phone for Notification	SMSアラームを受信する電話グループを選択します。
Email for Notification	Eメールアラームを受信するEメールグループを選択します。
Events	ゲートウェイが記録するイベントタイプ。
Record	このオプションをチェックすると、イベントアラームの関連内容が "イベント "ページに記録されます。
Email	このオプションをチェックすると、イベントアラームの関連内容が電子メールで送信されます。
Email Setting	クリックすると、「Eメール」ページに移動し、Eメールグループを設定できます。
SMS	このオプションをオンにすると、イベントアラームの関連内容がSMSで送信されます。
SMS Setting	クリックすると「電話」のページに移動し、電話グループリストを設定します。

Phone Group List	SMSアラームを受信する電話グループを選択します。
Email Group List	メールアラームを受信するメールグループを選択します。

表 3-5-5-2 イベントパラメータ

関連項目 メール設定 電話設定

3.6 メンテナンス

ここでは、システムのメンテナンスツールおよび管理について説明します。

3.6.1 ツール

トラブルシューティングツールには、ping と traceroute があります。

3.6.1.1 Ping

Ping ツールは、外部ネットワークに Ping を送信するためのツールです。

図 3-6-1-1

PING	
項目	名称
Host	ゲートウェイから外部ネットワークを Ping します。

表 3-6-1-1 IP Ping パラメータ

3.6.1.2 トレースルート

Traceroute ツールは、ネットワークルーティングのトラブルシューティングに使用します。

図 3-6-1-2

Traceroute	
項目	項目
Host	検出する宛先ホストのアドレス。

表 3-6-1-2 トレースルートのパラメータ

3.6.1.3 パケットアナライザ

パケットアナライザは、異なるインタフェースのパケットをキャプチャするために使用します。

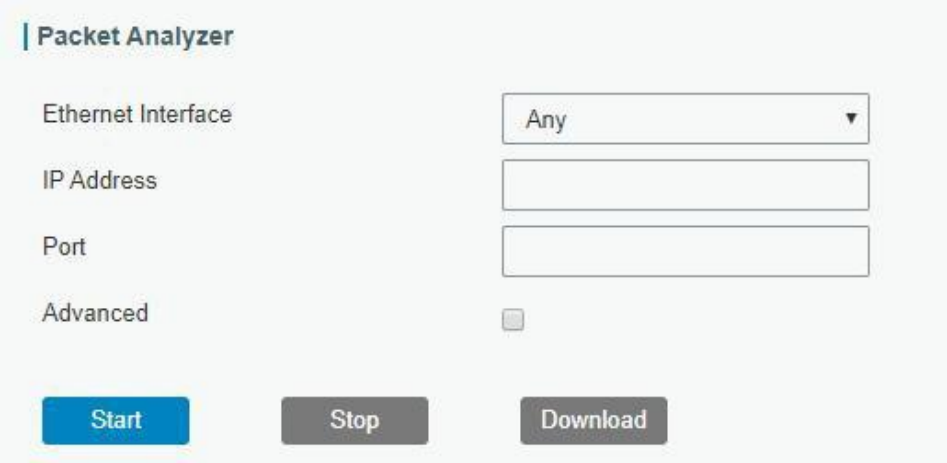


図 3-6-1-3

Packet Analyzer	
項目	説明
Ethernet Interface	パッケージをキャプチャするインターフェイスを選択します。
IP Address	ルーターがキャプチャするIPアドレスを設定します。
Port	ルーターがキャプチャするポートを設定します。
Advanced	スニッファのルールを設定します。フォーマットは tcpdump です。

表 3-6-1-3 パケットアナライザパラメータ

3.6.1.4 Qxdmlog

このセクションでは、QXDM ツールを使用してセルラーモジュールの診断ログを収集します。

図 3-6-1-4

3.6.2 スケジュール

このセクションでは、ゲートウェイ上でスケジュールされたリブートを設定する方法を説 明します。

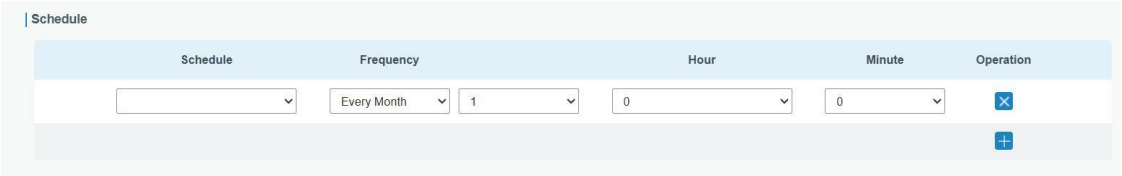


図 3-6-2-1

Schedule	
項目	説明

Schedule	スケジュールイベントを選択します： 再起動ゲートウェイを定期的に再起動します。
Frequency	スケジュールを実行する周波数を選択します。

表 3-6-2-1 スケジュールパラメータ

3.6.3 ログ

システムログには、システムの処理方法を示す情報、エラー、警告イベントの記録が含まれます。ログに含まれるデータを確認することで、システムのトラブルシューティングを行う管理者またはユーザーは、問題の原因またはシステムプロセスが正常にロードされているかどうかを特定することができます。リモートログサーバーは実現可能で、ゲートウェイはすべてのシステムログを Syslog Watcher などのリモートログサーバーにアップロードします。

3.6.3.1 システムログ

このセクションでは、ログファイルをダウンロードし、最近のログをウェブで表示する方法について説明します。

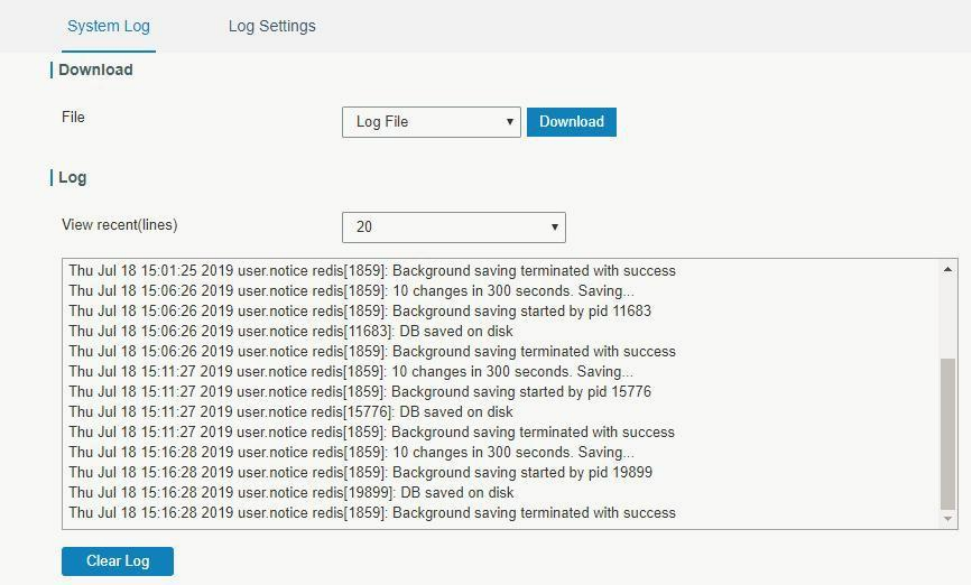


図 3-6-3-1

System Log	
項目	説明
Download	ログファイルをダウンロードします。
View recent (lines)	指定した行のシステムログを表示します。
Clear Log	現在のシステムログをクリアします。

表 3-6-3-1 システムログパラメータ

3.6.3.2 ログ設定

本節では、リモートログサーバーおよびローカルログの設定方法について説明します。

図 3-6-3-2

Log Settings	
設定項目	設定項目
Remote Log Server	
Enable	Remote Log Server "を有効にすると、ゲートウェイはすべてのシステムログをリモートサーバーに送信します。
Syslog Server Address	リモートシステムログサーバーのアドレス（IP/ドメイン名）を入力します。
Port	リモートシステムログサーバのポートを入力します。
Local Log File	
Storage	ログファイルをメモリ上に保存できます。
Size	保存するログファイルのサイズを設定します。
Log Severity	重要度のリストは syslog プロトコルに従います。

表 3-6-3-2 システムログパラメータ

3.6.4 アップグレード

本節では、Web 経由でゲートウェイのファームウェア e をアップグレードする方法を説明します。通常、ファームウェアのアップグレードを行う必要はありません。

注意：ファームウェアアップグレード中は、Web ページ上での動作は禁止されています。

図 3-6-4-1

Upgrade

項目	ファームウェアバージョン
Firmware Version	現在のファームウェアバージョンを表示します。
Reset Configuration to Factory Default	このオプションをチェックすると、ゲートウェイはアップグレード後に工場出荷時のデフォルトにリセットされます。
Upgrade Firmware	Browse "ボタンをクリックして新しいファームウェアファイルを選択し、"Upgrade "ボタンをクリック してファームウェアをアップグレードします。

表 3-6-4-1 アップグレードパラメータ

関連設定例

ファームウェアのアップグレード

3.6.5 バックアップとリストア

ここでは、システム全体のコンフィグレーションのバックアップをファイルに作成する方法、バッ チバックアップのために重要なコンフィグレーションの一部のみを複製する方法、コンフィグ ファイルをゲートウェイにリストアする方法、工場出荷時のデフォルトにリセットする方法を説 明します。

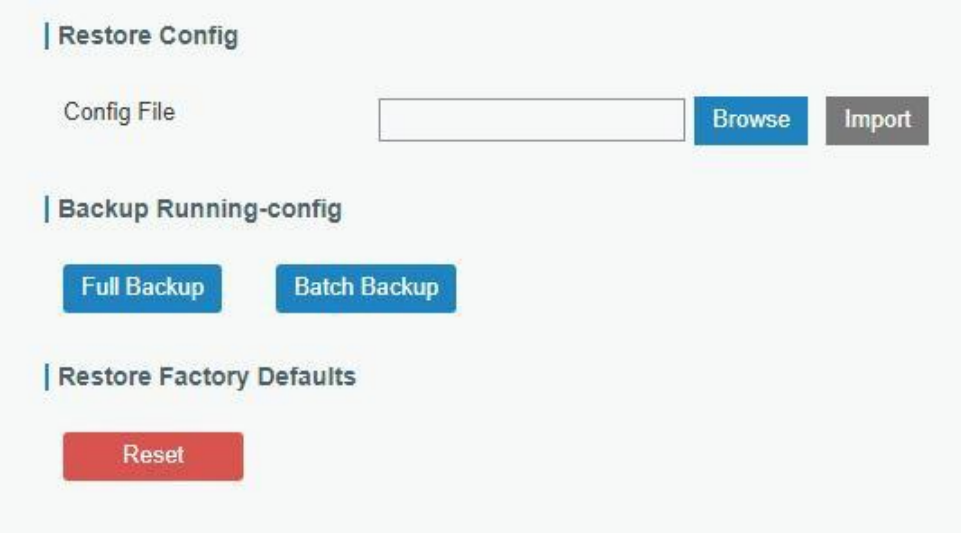


図 3-6-5-1

Backup and Restore	
項目	説明
Config File	Browse "ボタンをクリックしてコンフィギュレーション・ファイルを選択し、"Import "ボタンをクリックしてコンフィギュレーション・ファイルをゲートウェイにアップロードします。
Full Backup	Full Backup "ボタンをクリックすると、現在の設定ファイルをPCにエクスポートします。
Batch Backup	バッチバックアップ]をクリックすると、パケット転送装置のゲートウェイID、すべての組み込みNS設定、WANの固定IPアドレス、WLAN設定、ユーザー管理設定、DeviceHub認証コード、すべてのAPP設定を除く現在の設定がエクスポートされます。
Reset	リセット "ボタンをクリックすると、工場出荷時のデフォルト設定がリセットされます。

表 3-6-5-1 バックアップとリストアパラメータ

関連設定例

工場出荷時のデフォルトに戻す

3.6.6 再起動

このページでは、ゲートウェイを再起動してログインページに戻ることができます。新しいコンフィギュレーションが失われないように、ゲートウェイを再起動する前に "Save" ボタンをクリックすることを強くお勧めします。

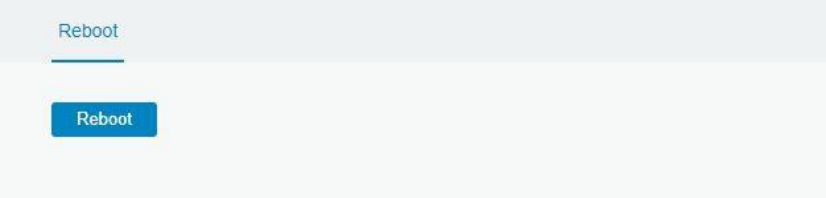


図 3-6-6-1

3.7 APP

3.7.1 Python

Python はオブジェクト指向プログラミング言語であり、その明確な構文と読みやすさで人気を博し ています。
インタプリタ型言語である Python には、コードの読みやすさを重視する設計思想があり、特に、中括弧やキーワードではなく空白インデントを使用してコードブロックを区切り、プログラマが C++ や Java などの他の言語で使用されるよりも少ないコード行数で概念を表現できる構文が採用されています。Pythonは、小規模なものから大規模なものまで、明確なプログラムを書くための構成要素と意図を提供します。
ユーザはPythonを使って、プログラムの最終的なインタフェースとなるプログラムのプロトタイプを素早く生成し、より適切な言語で書き直し、Pythonが呼び出せる拡張クラスライブラリをカプセル化することができます。
このセクションでは、App-manager、SDKバージョン、拡張ストレージなど、関連する実行ステータスを表示する方法について説明します。また、App-managerの設定を変更したり、Python Appパッケージをインポートすることもできます。

3.7.1.1 Python

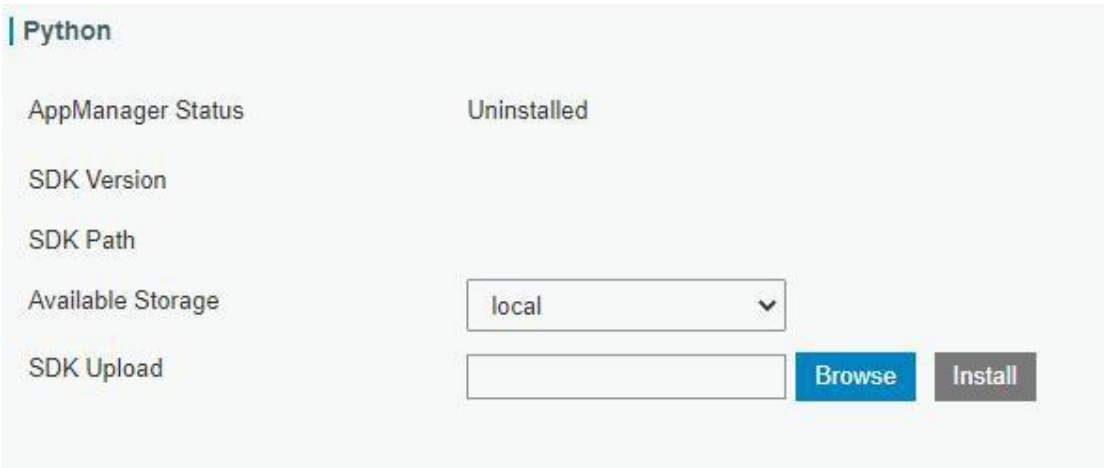


図 3-7-1-1

Python	
項目	説明
AppManager Status	AppManagerの実行状態（「Uninstalled」、「Running」、「Stopped」など）を表示します。
SDK Version	インストールされているSDKのバージョンを表示します。
SDK Path	SDKのインストールパスを表示します。
Available Storage	SDKをインストールするストレージを選択します。
SDK Upload	SDK for Pythonをアップロードしてインストールします。
Uninstall	SDKをアンインストールします。
View	AppManager で管理しているアプリケーションの状態を表示します。

表 3-7-1-1 Python パラメータ

3.7.1.2 App Manager の設定

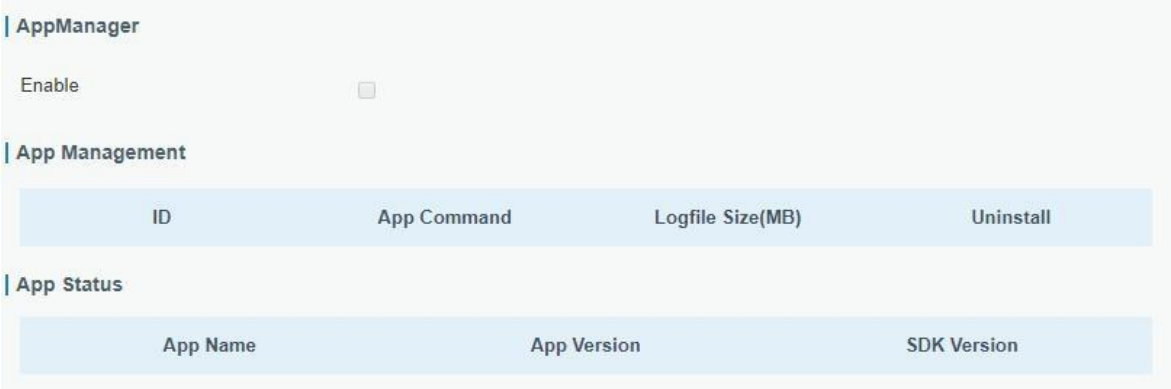


図 3-7-1-2

AppManager Configuration	
項目	説明
Enable	Python AppManager を有効にした後、"Python "ウェブページの "View "ボタンをクリックすると、 AppManager が管理しているアプリケーションのステータスが表示されます。
App Management	
ID	インポートしたアプリのIDを表示します。
App Command	インポートしたアプリの名前を表示します。
Logfile Size(MB)	ユーザー定義のログファイルサイズ。範囲：1-50.
Uninstall	APPをアンインストールします。
App Status	
App Name	インポートしたアプリの名前を表示します。
App Version	インポートしたアプリのバージョンを表示します。
SDK Version	インポートされた App が基づいている SDK バージョンを表示します。

表 3-7-1-2 APP Manager パラメータ

3.7.1.3 Python アプリ

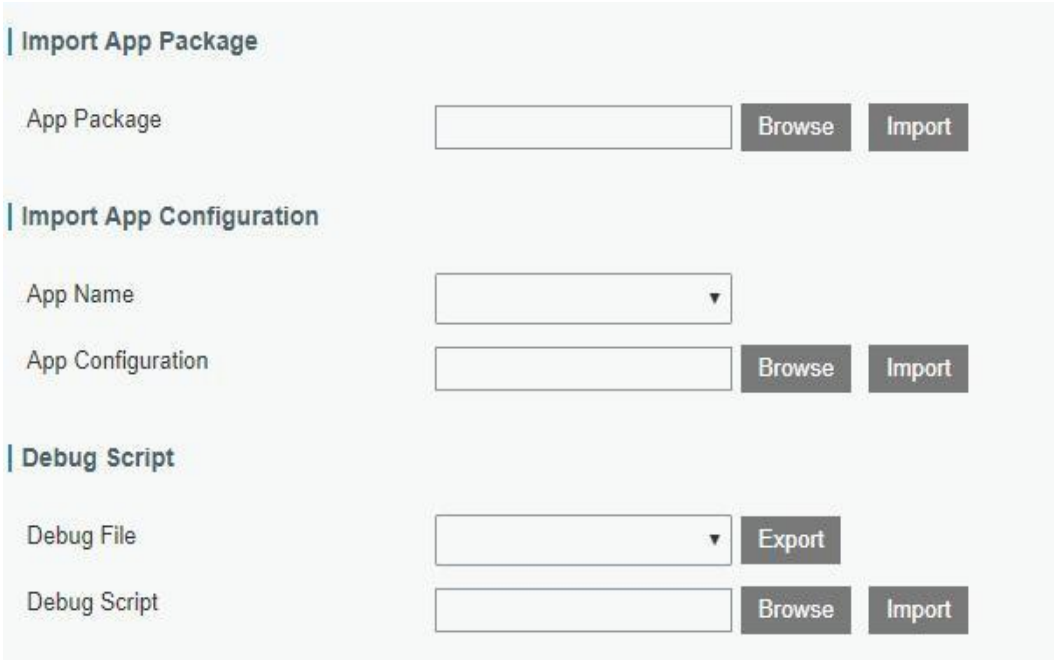


図 3-7-1-3

Python APP	
項目	説明
App Package	Appパッケージとインポートを選択します。
App Name	設定をインポートするアプリを選択します。
App Configuration	設定ファイルを選択してインポートします。
Debug File	スクリプトファイルをエクスポートします。
Debug Script	デバッグする Python スクリプトを選択し、インポートします。

表 3-7-1-3 APP パラメータ

3.7.2 Node-RED

Node-REDは、モノのインターネットの一部として、ハードウェアデバイス、API、オンラインサービスを視覚的にプログラミングし、配線するためのフローベースの開発ツールです。Node-REDはウェブブラウザベースのフローエディタを提供し、パレットの幅広いノードを使用してフローを簡単に配線することができます。より詳しいガイダンスやドキュメントについては、Node-RED公式ウェブサイトを参照してください。

3.7.2.1 Node-RED

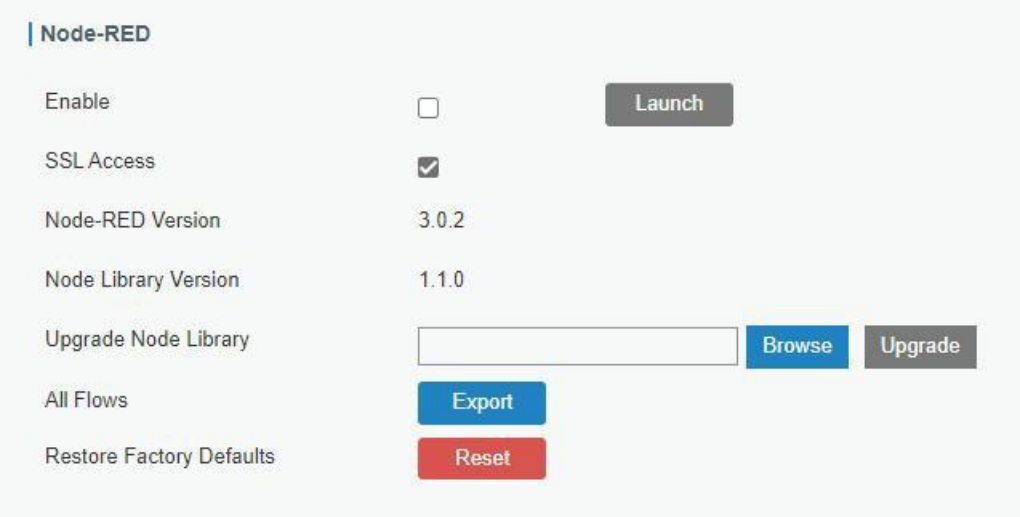


図 3-7-2-1

Node-RED	
項目	説明
Enable	Node-RED を有効にします。
Launch	Node-REDのWeb GUIを起動します。
SSL Access	Node-REDのウェブGUIにHTTPSサービスのみでアクセスする場合に有効にします。
Node-RED Version	Node-RED のバージョンを表示します。Node-RED のバージョンはゲートウェイをアップグレードしたときにのみアップグレードできます。
Node Library Version	ノードライブラリのバージョンを表示します。
Upgrade Node Library	ライブラリパッケージをインポートして、ノードライブラリをアップグレードします。
All Flows Export	すべてのフローをJSON形式のファイルとしてエクスポートします。
Restore Factory Default	Node-RED の全フローデータを消去します。

表 3-7-2-1 Node-RED パラメータ

Milesight は、ゲートウェイのインターフェースを使用するためにカスタマイズされたノードライブラリを提供します。

図 3-7-2-2

Node Library	
ノード	説明
LoRa Input	ゲートウェイから LoRaWAN® パケットを受信します。ネットワークサーバーが有効な場合のみ動作。
LoRa Output	LoRaWAN® ノードにダウンリンクコマンドを送信します。
Device Filter	デバイス EUI を介して、1 つ以上の特定の LoRaWAN® ノードのデータをフィルタリングします。
GW Info	ゲートウェイのイベントを監視します。これは、**General> Events> Events Settings**でイベント検出が有効になっていることを確認する必要があります。
Email Output	電子メールを送信します。STMPオプションを "Same as the gateway "として選択した場合、**System > General Settings > SMTP**ページでSMTPクライアント設定を行う必要があります。
SMS Input	SMSメッセージを受信します。携帯電話接続時のみ有効です。
SMS Output	SMSメッセージを送信します。セルラーが接続されている時のみ機能します。

表 3-7-2-2 ノードライブラリパラメータ

関連設定例

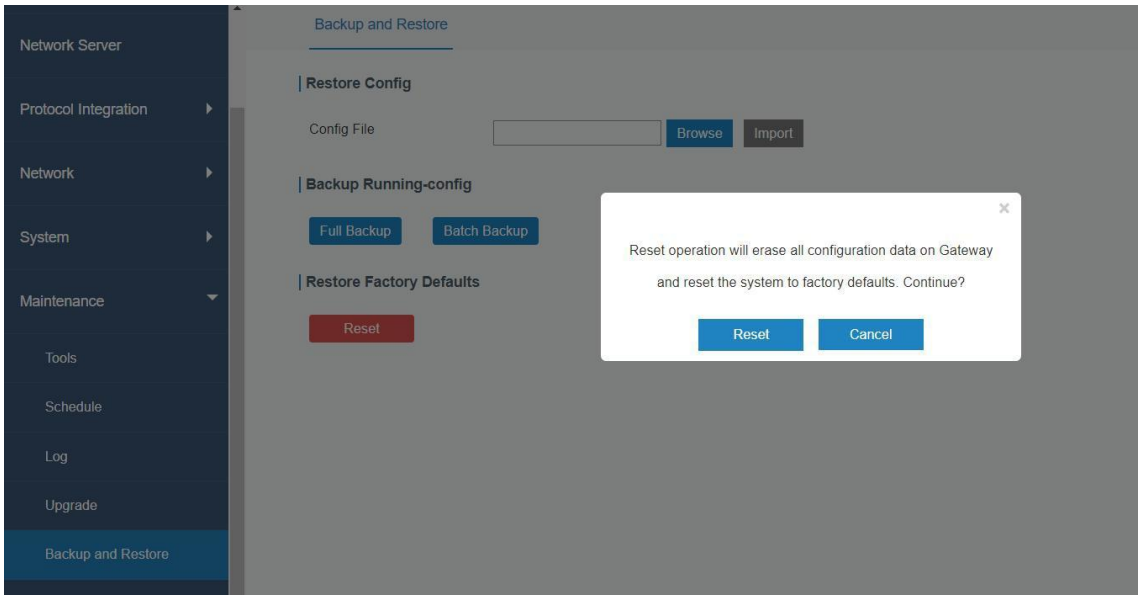
Node-RED

第 4 章 アプリケーション例

4.1 工場出荷時のデフォルトに戻す

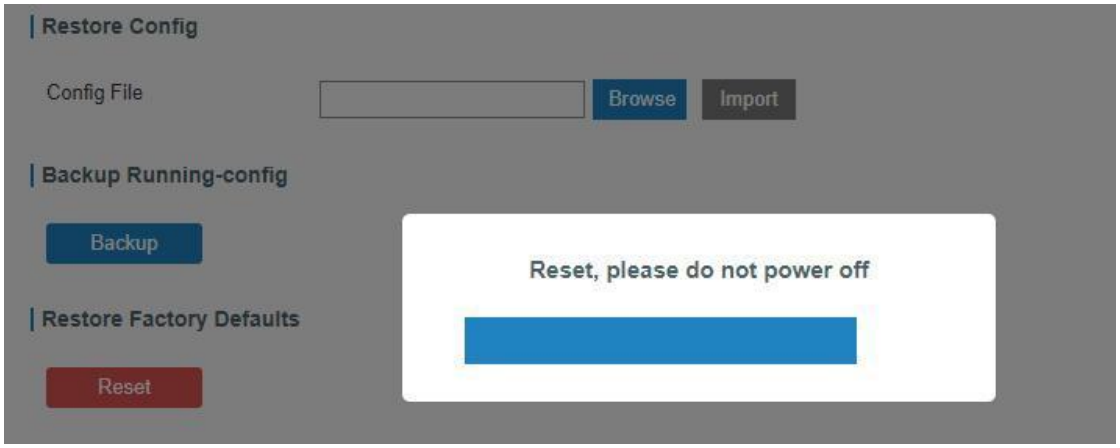
方法 1：

Web インターフェースにログインし、**「Maintenance（メンテナンス）」> 「Backup and Restore（バックアップと復元）」**に進み、**「Reset（リセット）」**ボタンをクリ



ックします。**リセット**ボタンをクリックします。

すると、ゲートウェイは直ちに再起動し、工場出荷時の設定に復元します。



STATUSランプが静止し、ログインページが再びポップアップするまでお待ちください。

関連トピック

工場出荷時の戻すデフォルトに

方法 2：

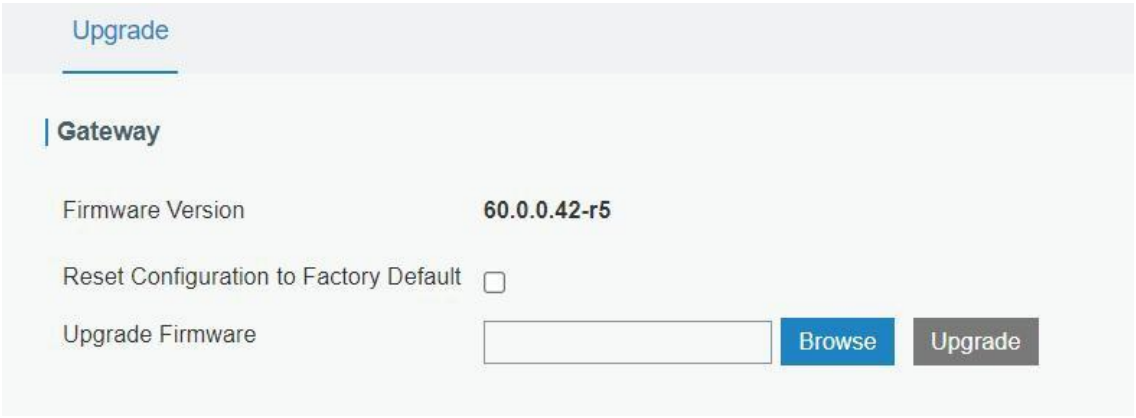
ゲートウェイのリセットボタンを探し、STATUS LEDが点滅するまでリセットボタンを5秒以上押し続けます。

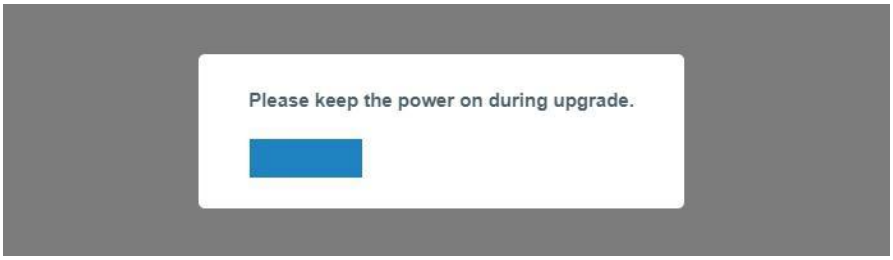
4.2 ファームウェアのアップグレード

ゲートウェイのファームウェアをアップグレードする前に、まずMilesightテクニカルサポートに連絡することをお勧めします。ゲートウェイのファームウェアファイルの接尾辞は".bin "です。

ファームウェアファイルを入手した後、以下のステップを参照してアップグレードを完了してください。

1. メンテナンス > アップグレード "に進みます。
2. Browse "をクリックし、PCから正しいファームウェアファイルを選択します。
3. アップグレード "をクリックすると、ゲートウェイはファームウェアファイルが正しいかどうかをチェックします。正しい場合、ファームウェアはゲートウェイにインポートされ、ゲートウェイはアップグレードを開始します。
4. アップグレード後、ブラウザ経由でゲートウェイのウェブ GUI を開き、アップグレードが成功したかどうかを確認します。
   開く前に、ブラウザのキャッシュを削除することをお勧めします。





関連トピック

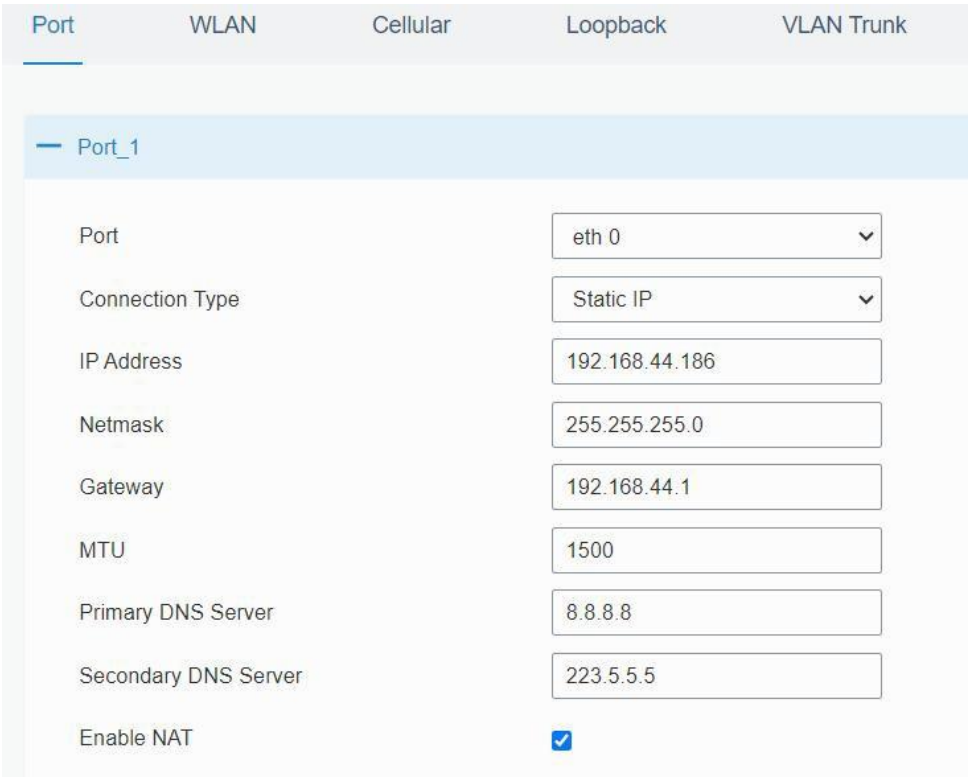
アップグレード

4.3 ネットワーク接続

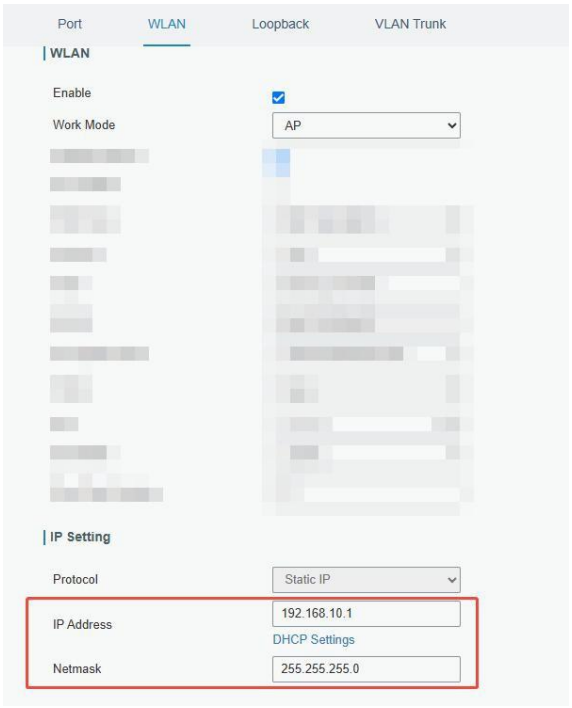
ゲートウェイは、ネットワーク接続を設定する複数の方法をサポートしています。

4.3.1 イーサネット接続

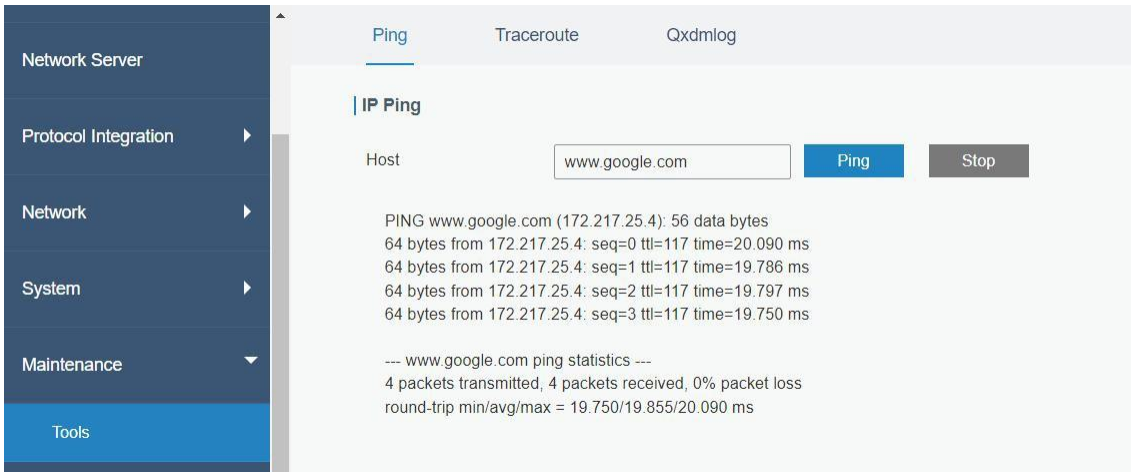
1. Network > Interface > Portページで接続タイプを選択し、イーサネットポートの設定を行います。



注意：イーサネットポートの**IP**アドレスを変更する際、**IP**が競合する場合は、まず**WLAN**のサブネットを変更してください。



2. ゲートウェイのイーサネットポートをルーターやモデムなどのデバイスに接続します。
3. **Maintenance > Tools > Ping**でネットワークの接続性を確認します。

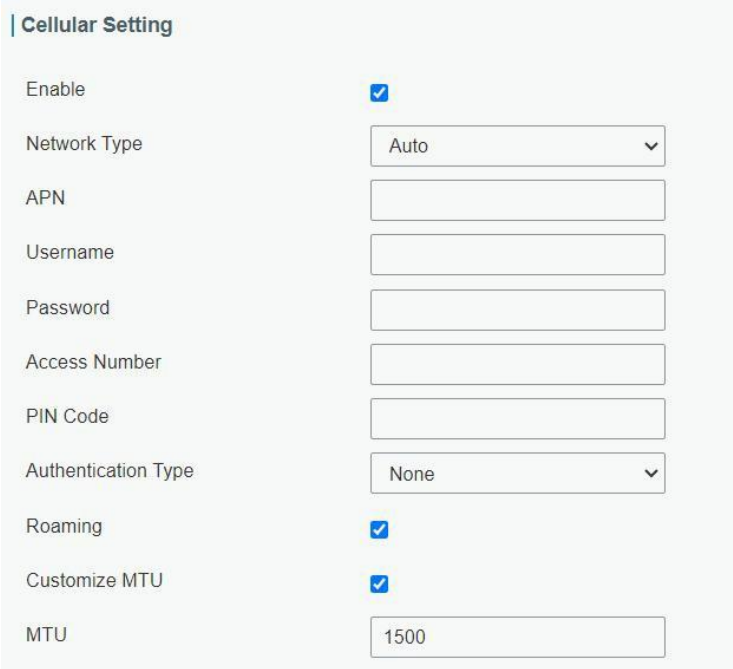


関連トピック

ポート設定

4.3.2 セルラー接続（セルラー版のみ）

1. Network > Interface > Cellular > Cellular Setting"（ネットワーク > インターフェース > セルラー > セルラー設定）でSIMカードの必要なセルラー情報を設定し、



"Save"（保存）と "Apply"（適用）をクリックして設定を有効にします。

2. Status > Cellularでセルラー接続のステータスを表示します。'Connected'と表示されていれば、SIMは正常にダイヤルアップしています。

関連トピック セルラー設定 ステータス

4.4 Wi-Fiアプリケーションの例

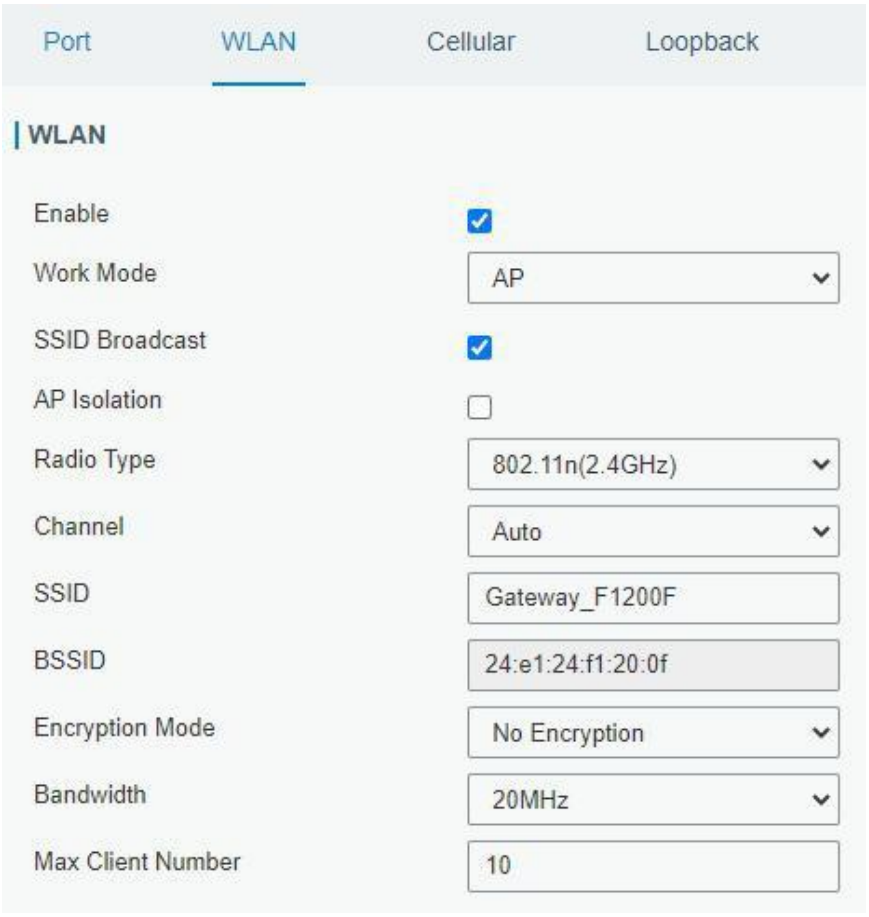
4.4.1 APモードアプ

リケーションの例

UG65をAPとして設定し、ユーザーまたはデバイスからの接続を許可します。

設定手順

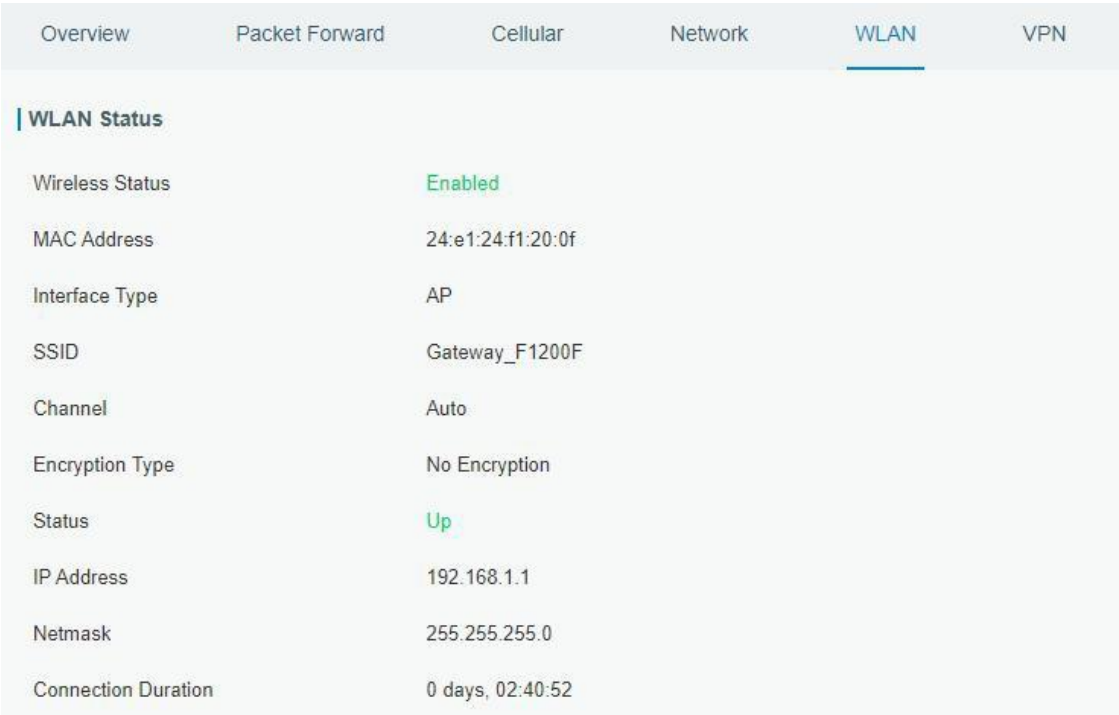
1. Network> Interface> WLANにアクセスし、ワイヤレスパラメータを以下のように設定します。



すべての設定が完了したら、「**Save**」と「**Apply**」ボタンをクリックします。

2. スマートフォンを使用してゲートウェイのアクセスポイントに接続します。

Status > WLANに移動し、**AP** 設定と接続されたクライアント/ユーザーの情報を確認できます。



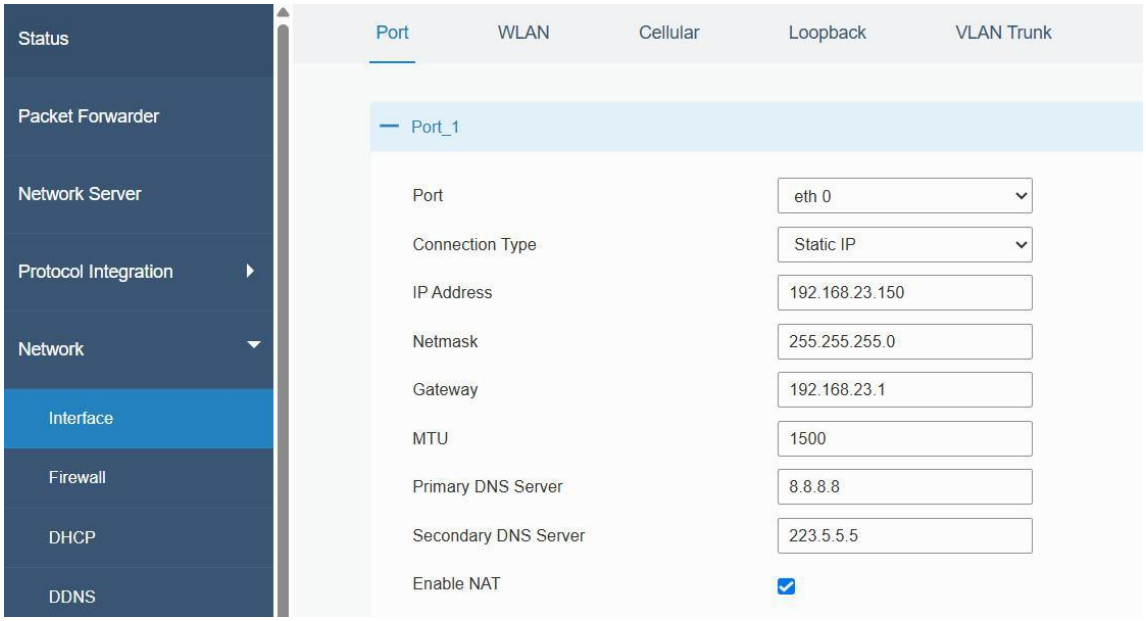
4.4.2 クライアント

モードの使用例

UG65をWi-Fiクライアントとして設定し、アクセスポイントに接続してインターネットに接続します。

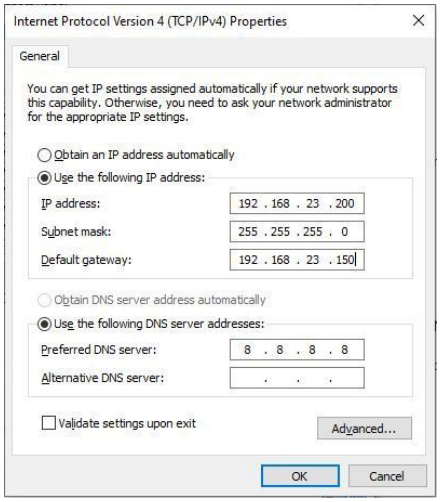
設定手順

1. **Network > Interface > Port**ページで接続タイプを**Static IP**に選択し、イーサネット

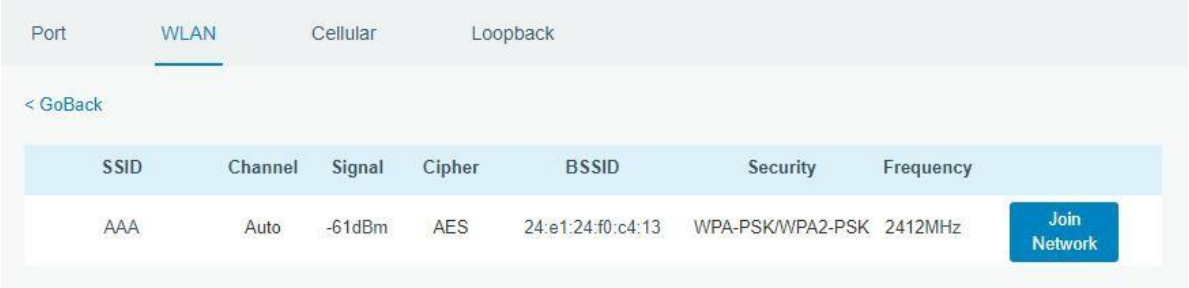


WANポートのIPアドレスを設定します。

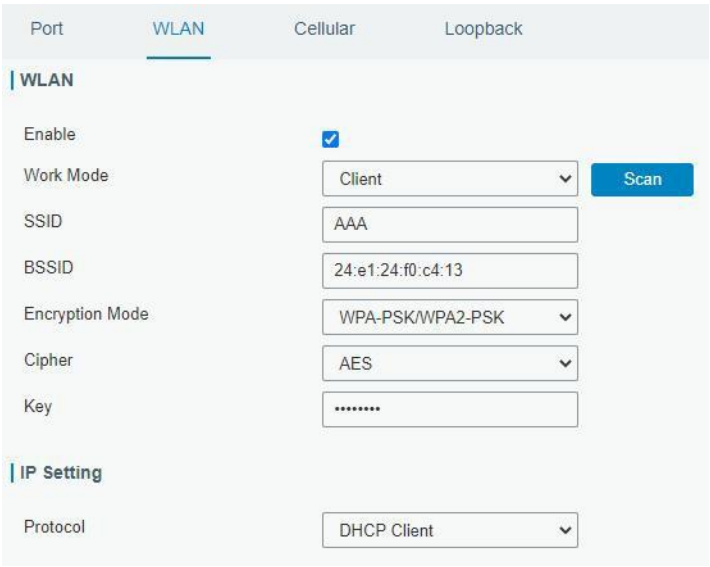
2. PCをUG65のETHポートに直接、またはPoEインジェクタを介して接続します。
3. コンピュータに IP アドレスを手動で割り当てます。Windows 10システムを例にします：



4. ウェブブラウザを開き、イーサネットポートの IP アドレスを入力して、ウェブ GUI にアクセスします。
5. **Network> Interface> WLAN**にアクセスし、**Scan**をクリックしてWiFiアクセスポイントを検索します。

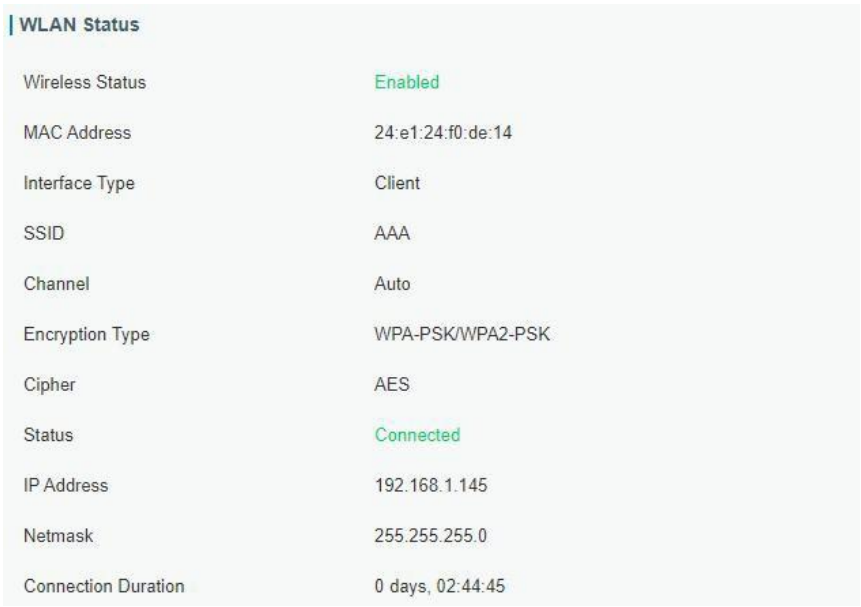


6. アクセスポイントを1つ選択し、**[Join Network（ネットワークに参加）]**をクリックして、アクセスポイントのパスワードを入力します。

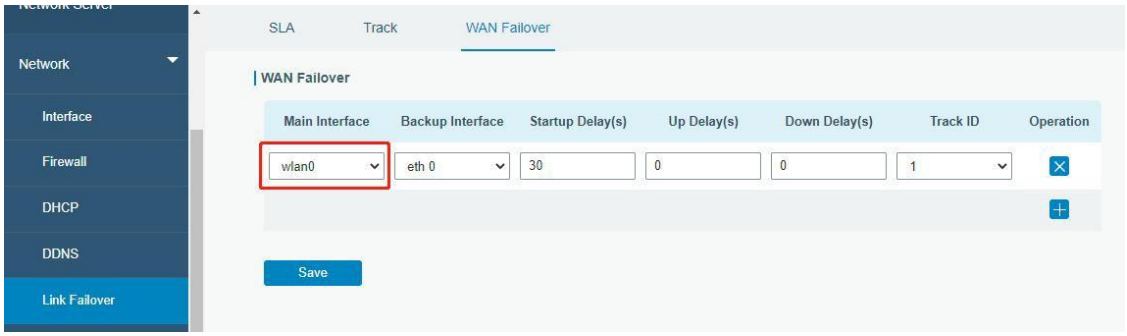


すべての設定が完了したら、**[Save]** と **[Apply]** ボタンをクリックします。

7. **Status > WLAN** にアクセスして、クライアントの接続ステータスを確認します。



8. **Network > Failover > WAN Failover**に進み、wlan0 をメインインターフェイスとして切り替え、ゲートウェイが Wi-Fi を使用してネットワークにアクセスできるようにします。



関連トピック

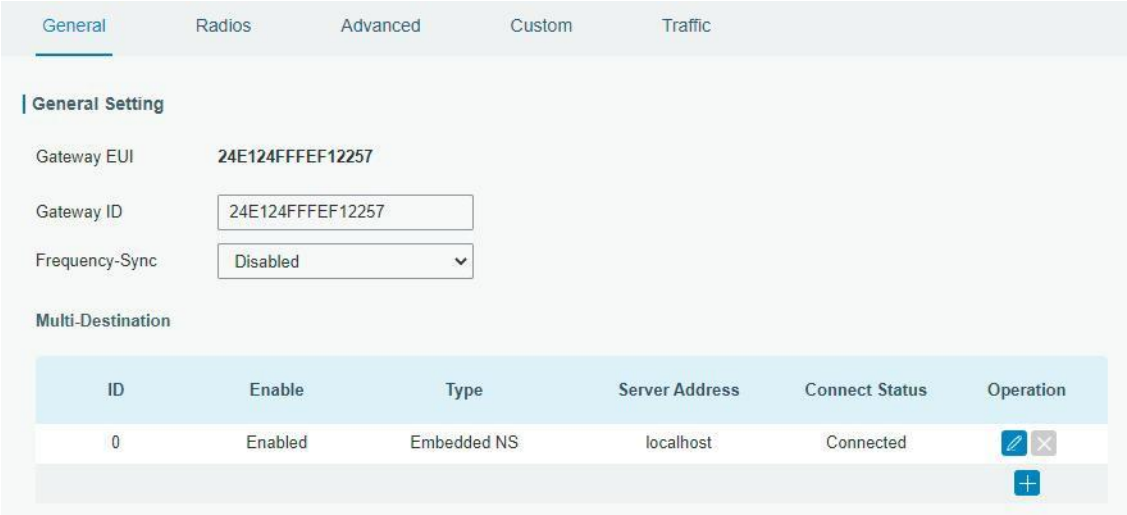
WLAN 設定

WLANステータス

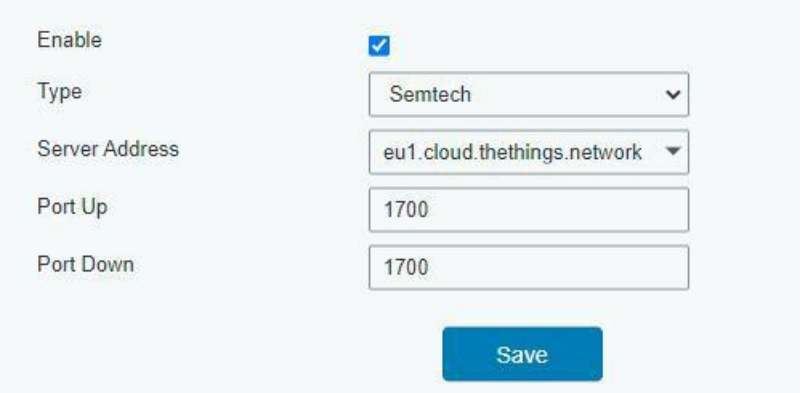
4.5 パケットフォワーダーの設定

UG65 ゲートウェイには、Semtech、Basic station、Chirpstack など複数のパケットフォワーダーがインストールされています。接続する前に、ゲートウェイがネットワークに接続されていることを確認してください。

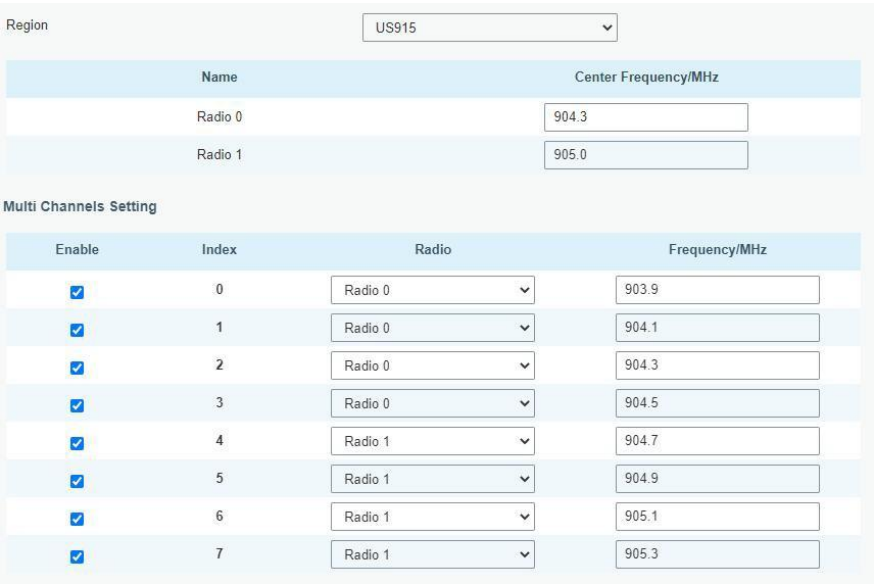
1. **Packet Forwarder > General**に進みます。



2.  をクリックして新しいネットワークサーバを追加します。ネットワークサーバー情報を入力し、このサーバーを有効にします。



3. **[Packet Forwarder] > [Radio]** ページで中心周波数とチャンネルを設定します。ゲートウェイとネットワークサーバーのチャンネルは同じにする必要があります。



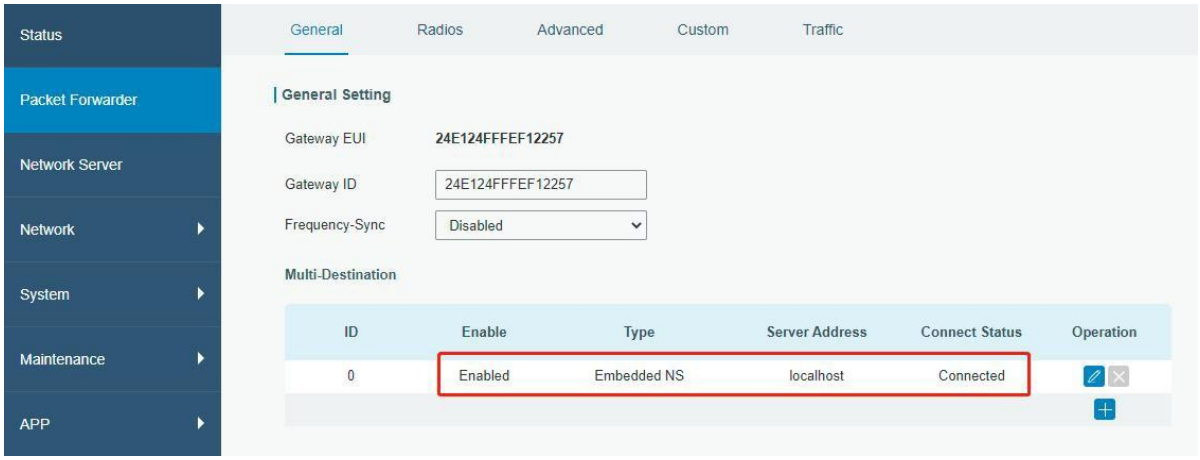
4. ネットワークサーバーのページにゲートウェイを追加します。ネットワークサーバー接続の詳細については、Milesight IoTサポートポータルをご参照ください。

4.6 ネットワークサーバーの設定

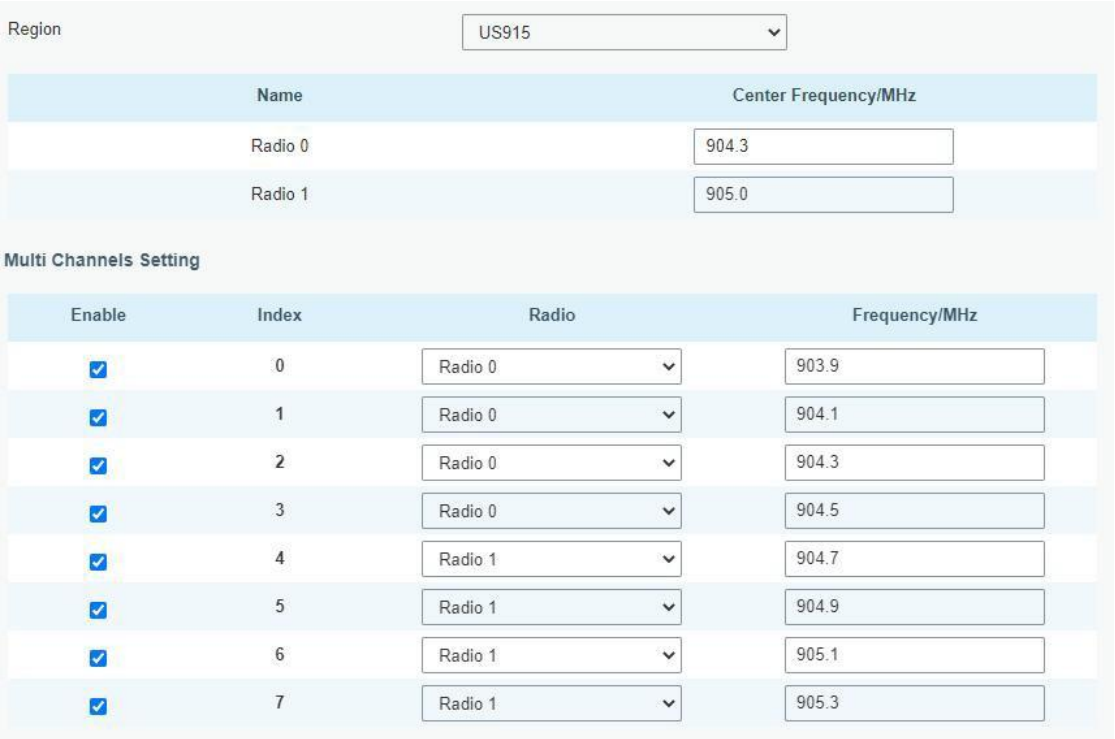
ゲートウェイはLoRaWAN® ネットワークサーバーとして動作し、LoRaWAN® エンドデバイスのデータを受信、分析し、異なるシステムとの柔軟な統合を実現します。

4.6.1 Milesight IoTクラウドへの接続

1. **Packet Forwarder> General**ページにアクセスし、組み込みネットワークサーバーを有効にします。

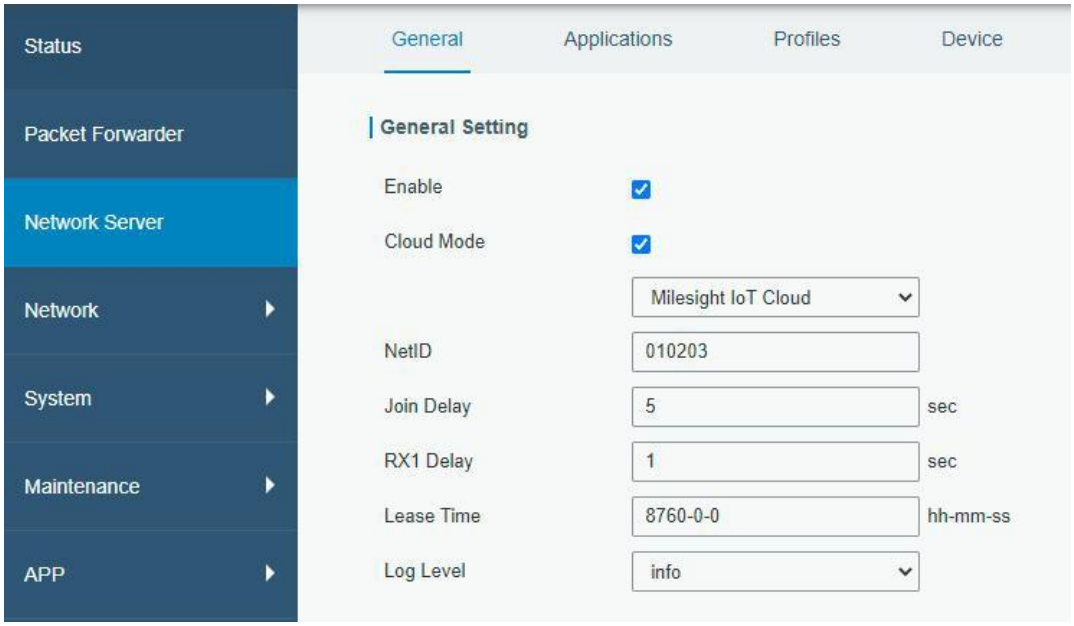


2. **Packet Forwarder > Radio** ページでアンテナタイプを選択し、中心周波数とチャンネルを設定します。ゲートウェイと　端末のチャンネルは　同じにする必要がありま

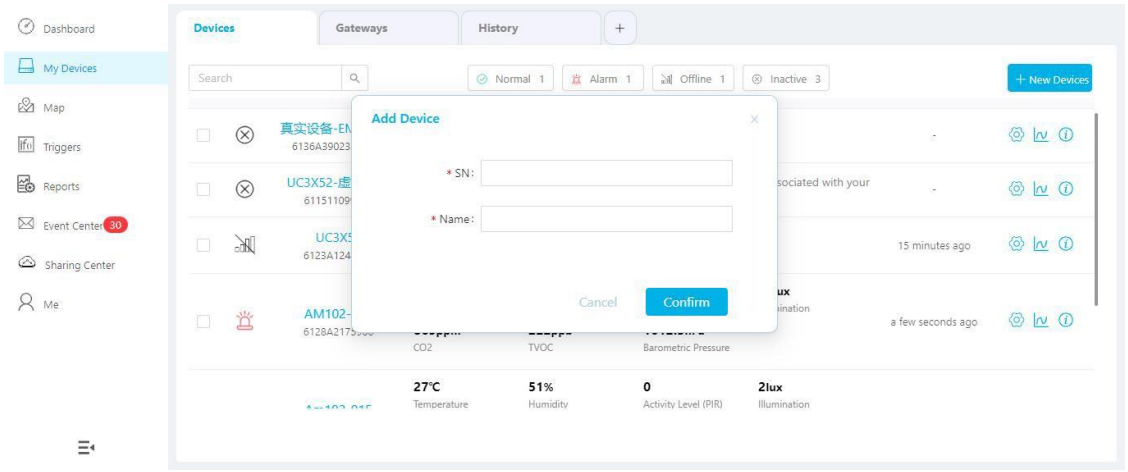


す。

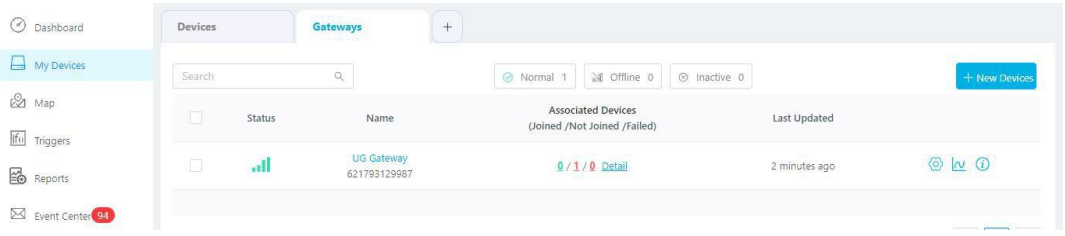
3. **Network Server > General**ページでネットワークサーバーと "Cloud mode "を有効にし、"Milesight IoT Cloud "モードを選択します。



4. Milesight IoT Cloudにログインします。次に**My Devices**ページで "+New Devices " をクリックし、SN経由でMilesight IoT Cloudにゲートウェイを追加します。ゲートウェイは "**Gateways** "メニューに追加されます。

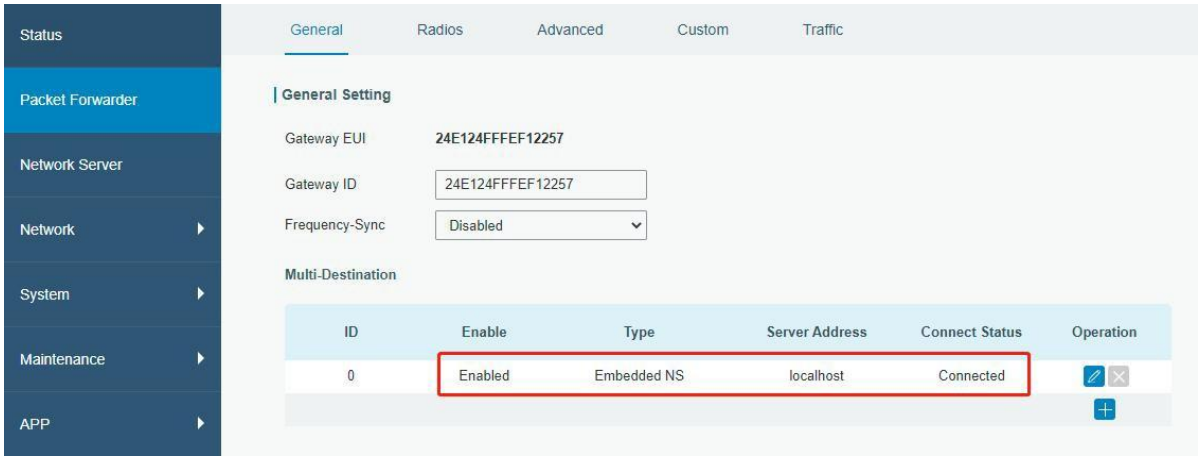


5. ゲートウェイはMilesight IoT Cloud上でオンラインになります。

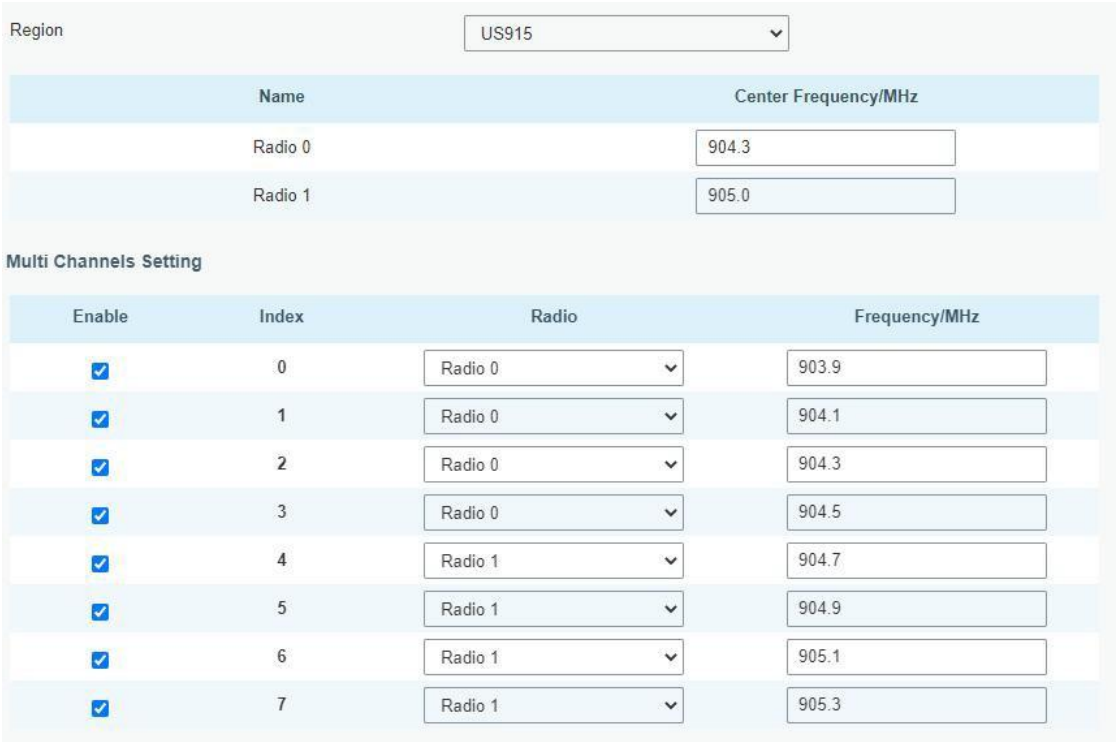


4.6.2 エンドデバイスの追加

1. **Packet Forwarder> General**ページにアクセスし、組み込みNSを有効にします。

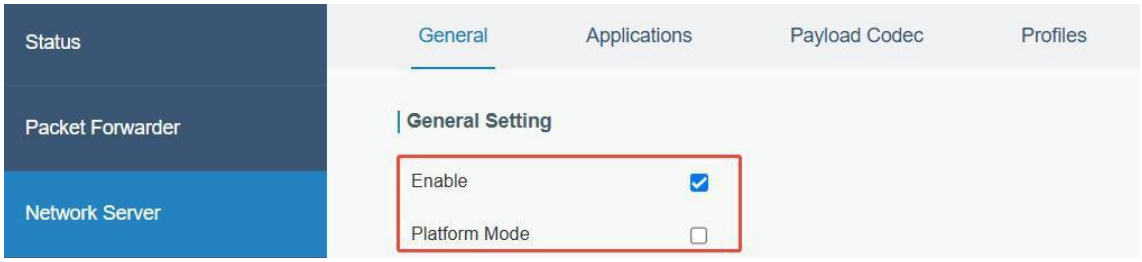


2. **Packet Forwarder > Radio** ページで中心周波数とチャンネルを設定します。ゲート

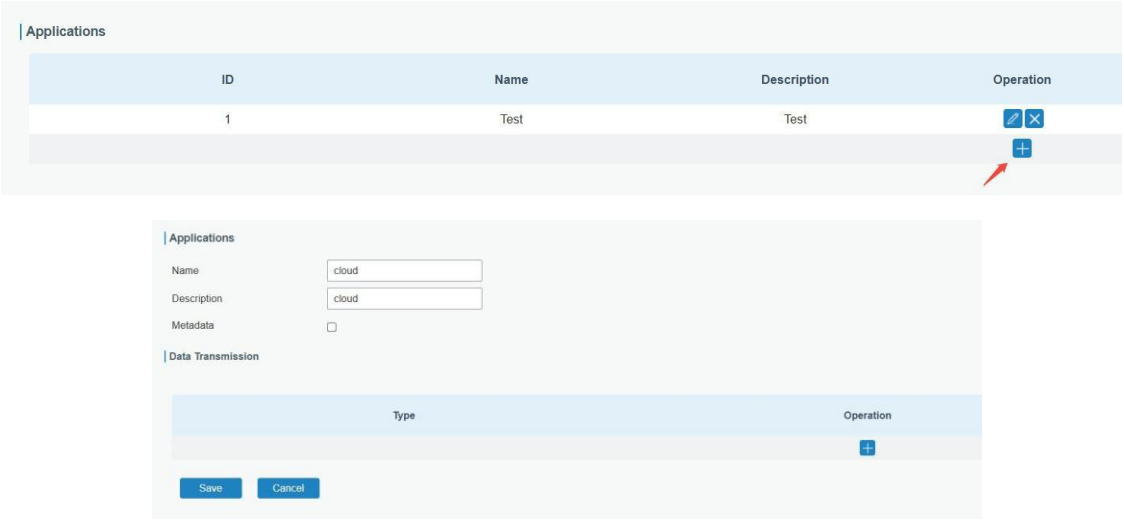


ウェイとエンドデバイスのチャンネルは同じにする必要があります。

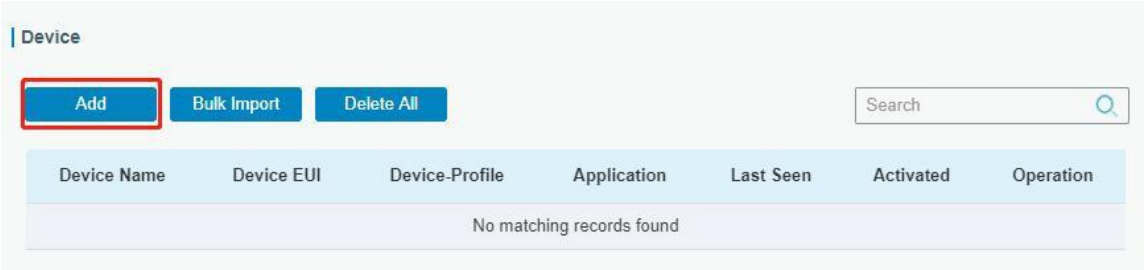
3. **Network Server> [General]** ページでネットワークサーバーを有効にします。



4. **Network Server> [Applications]**ページでアプリケーションを追加します。



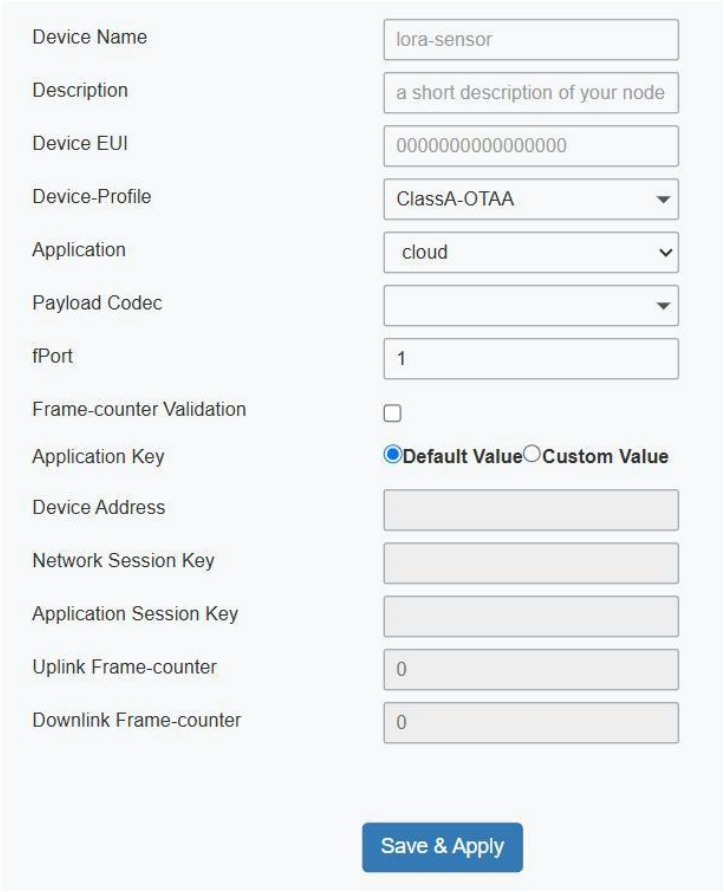
5. **Network Server > Device** ページに移動し、**Add** をクリックして LoRaWAN® ノードデバイスを追加します。**一括インポートを**クリックすると、テンプレートを使って一



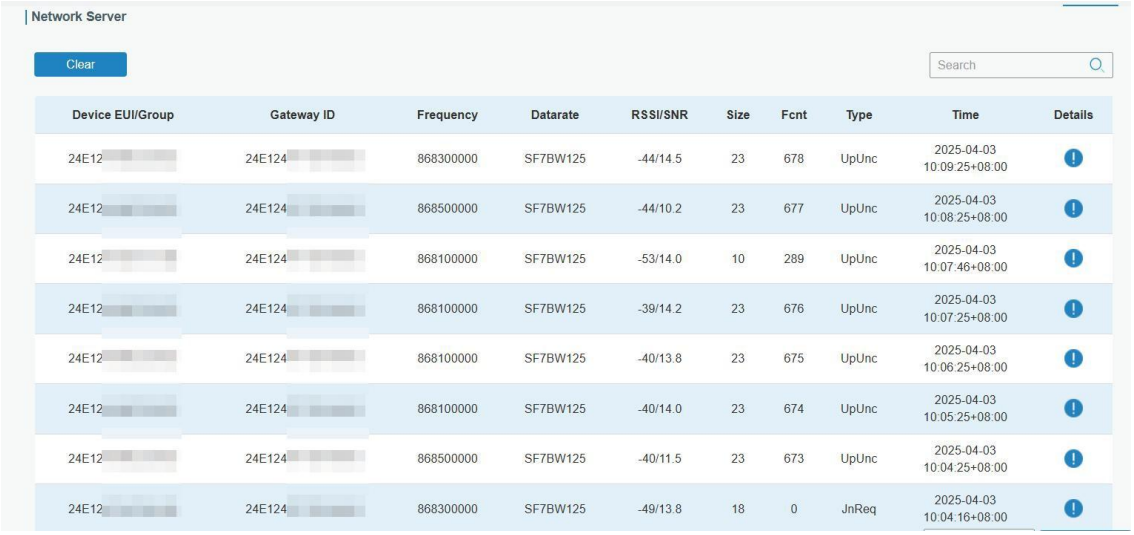
度に大量のデバイスを追加することもできます。

6. エンドデバイスの情報を入力し、**Save&Apply**をクリックします。情報はエンドデバイスの設定ページまたはメーカーのマニュアルで確認できます。以下は Milesightエンドデバイスのデフォルト設定です：

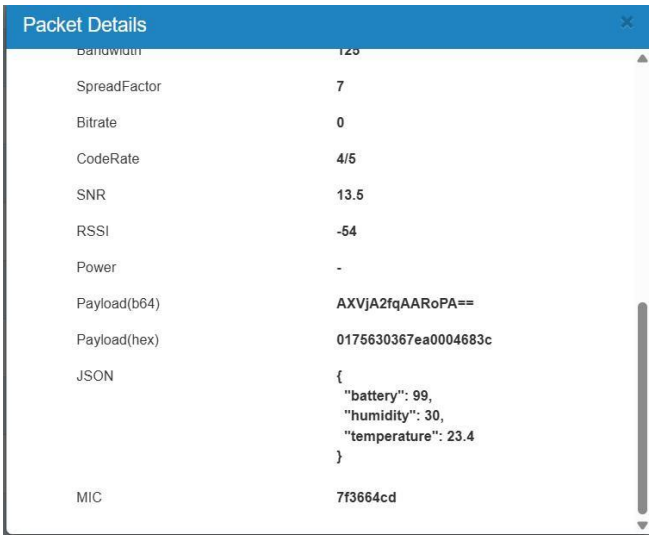
- Device EUI：デバイスに記載されています。
- Device-Profile：OTAAタイプファイル
- Payload Codec： モデルを選択
- fPort： 85
- Application Key: Default Valueを選択してください。ランダムキーを使用する場合は、カスタム値を選択してください。



7. **Network Server> Packets**ページに移動して、このデバイスからのアップリンクの有無を確認します。

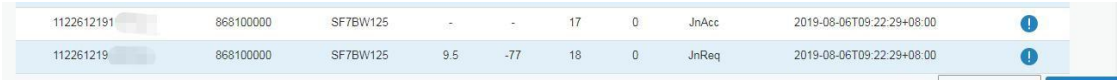


Detailsをクリックして、パケットの詳細とデコード結果を確認します。



4.6.3 デバイスへのデータ送信

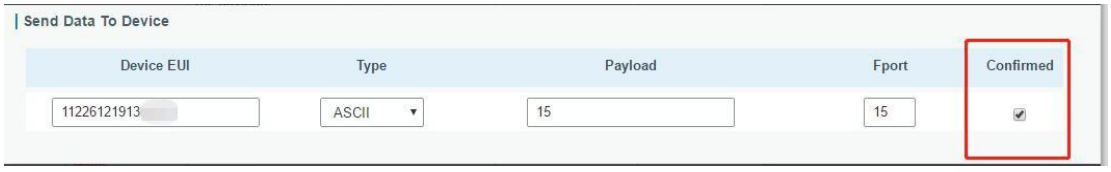
1. **Network Server > Packets**に進み、ネットワークサーバーリストのパケットをチェックして、デバイスがネットワークに正常に参加していることを確認します。



2. デバイスの**EUI**を入力するか、ダウンリンクを送信するマルチキャストグループを選択します。次に、ダウンリンクコマンド、ポートを入力します。

3. **Send**をクリックします。

4. ネットワークサーバーリストでパケットを確認し、デバイスがこのメッセージを正常に受信したことを確認します。確認済み」を有効にすることをお勧めします。マルチキャスト機能は確認済みダウンリンクをサポートしていません。

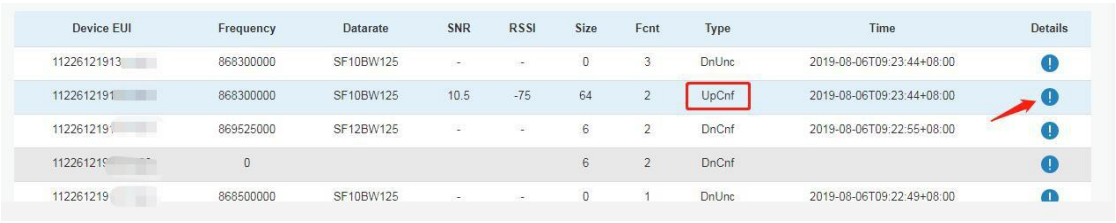


更新」をクリックしてリストを更新するか、リストの自動更新頻度を設定できます。デバイスのクラスタイプがクラス C の場合、デバイスは常にパケットを受信します。

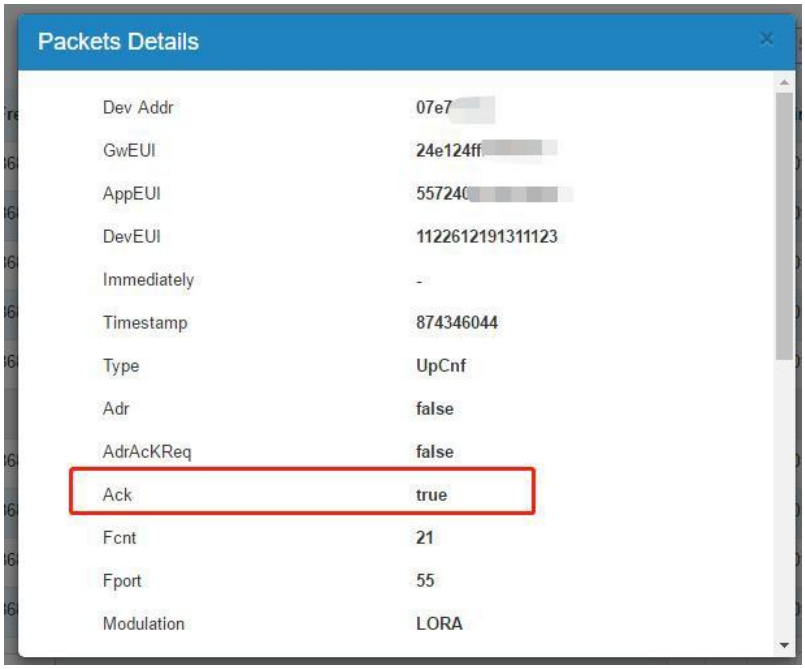
このパケットのタイプは DnCnf (Downlink Confirmed Packet) で、パケットの色がグレーの場合は、少なくとも 1 つのメッセージがキューに入っているため、そのパケットを今送信できないことを意味します。パケットのレコードの色が白なら、パケットは正常に配信されたことを意味します。

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

デバイスがこのダウンリンク確認済みパケットを受信した場合、デバイスは次に配信するときに "ACK "を返信します。

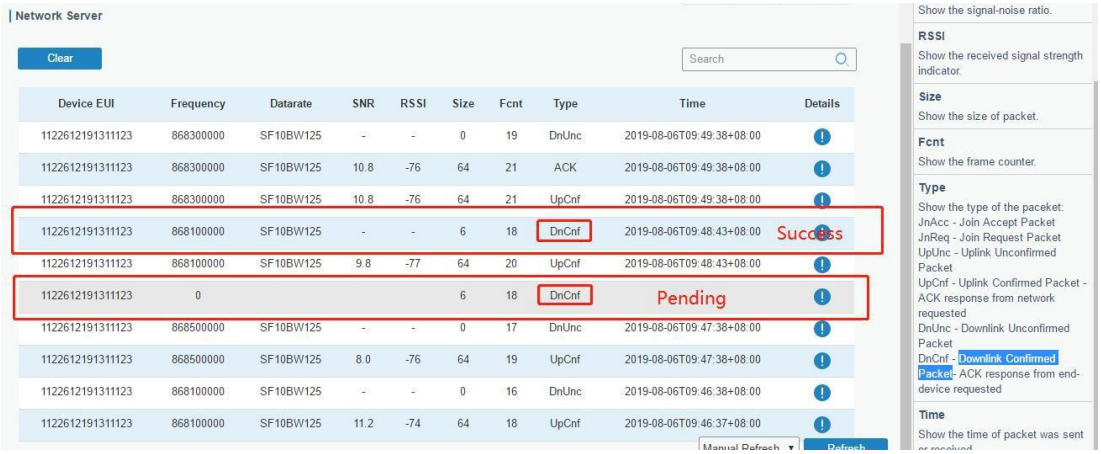


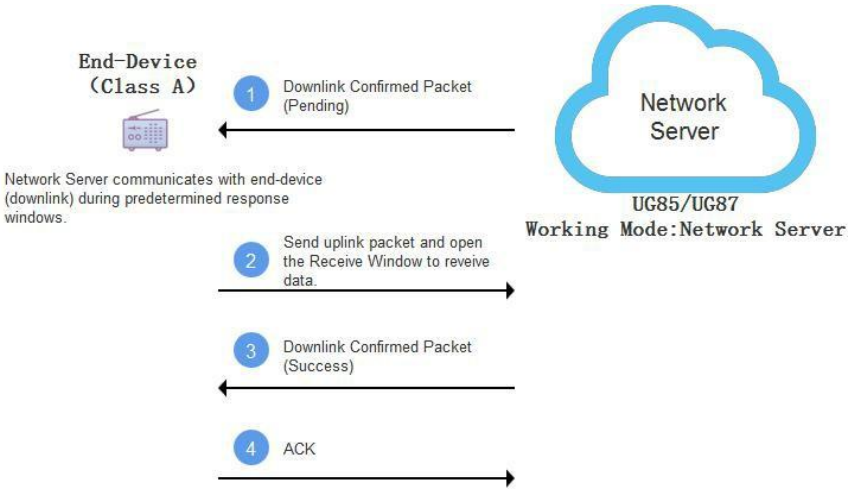
Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Type	Time	Details
11226121913	868300000	SF10BW125	-	-	0	3	DnUnc	2019-08-06T09:23:44+08:00	
1122612191	868300000	SF10BW125	10.5	-75	64	2	UpCnf	2019-08-06T09:23:44+08:00	
112261219	869525000	SF12BW125	-	-	6	2	DnCnf	2019-08-06T09:22:55+08:00	
112261219	0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

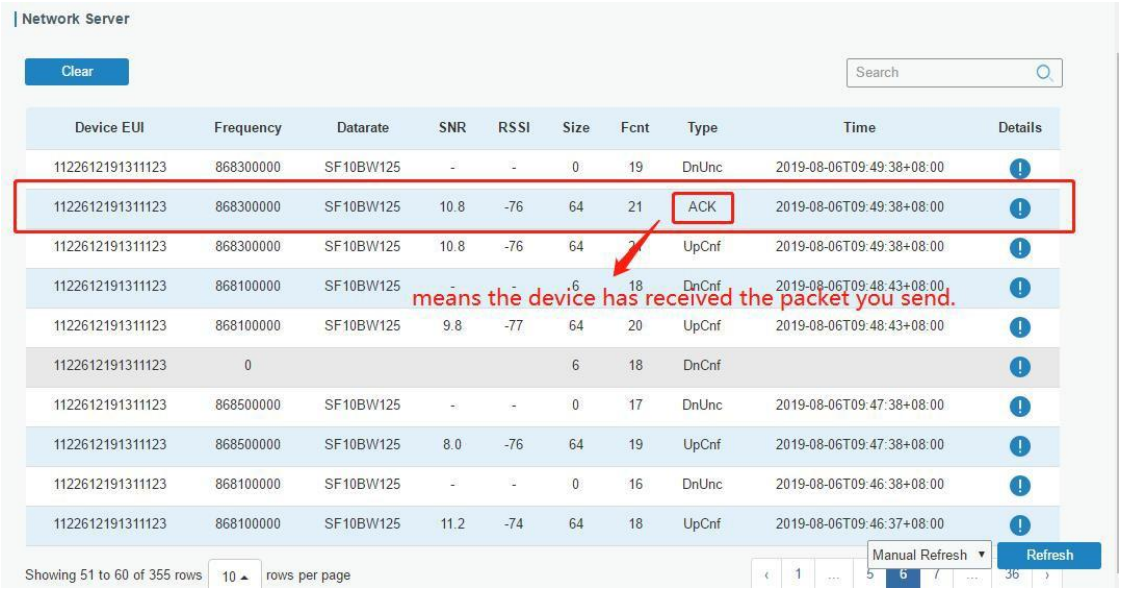


Ackが "true "であれば、このパケットを受信したことを意味します。

デバイスのクラスタイプがクラス A の場合、デバイスがアップリンクパケットを送信した後にのみ、ネットワークサーバーはデバイスにデータを送信します。







関連トピック

パケット

4.6.4 HTTP/MQTT サーバーへの接続

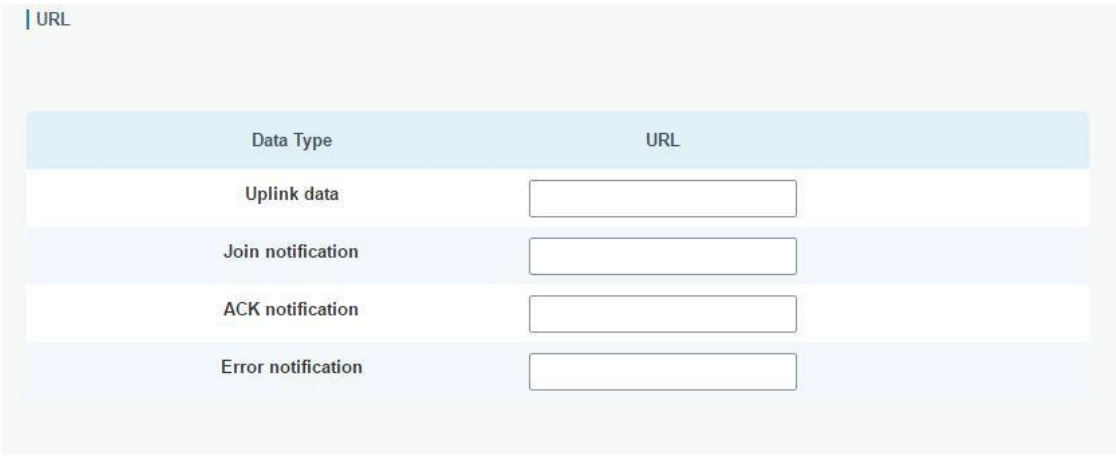
ゲートウェイは、MQTT、HTTP、または HTTPS プロトコルを使用して別のサーバー・アドレスにデータを送信するために、データ・トランスポート・プロトコルの選択をサポートします。

1. **Network Server（ネットワークサーバー）]> [Application（アプリケーション）]**に移動して、編集するアプリケーションを選択します。
2.  をクリックして、データ転送タイプを追加します。

HTTP または HTTPS

ステップ 1：送信プロトコルとして HTTP または HTTPS を選択します。

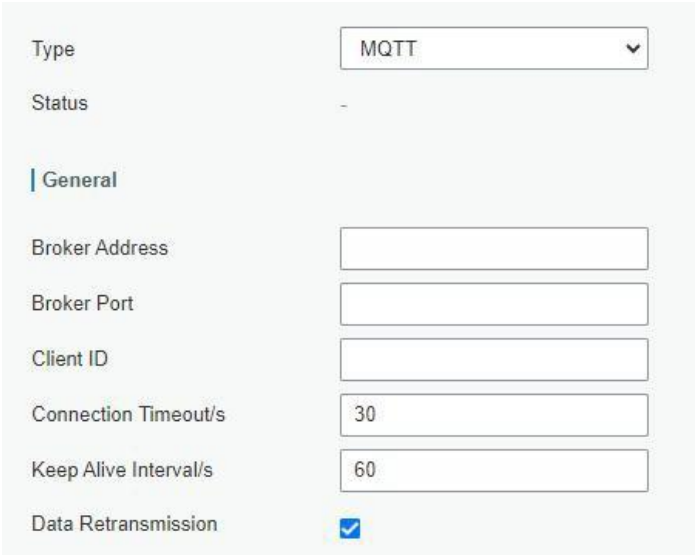
ステップ2：送信先URLを入力します。異なるタイプのデータを異なる URL に送信できます。



HTTP(s)サーバーにアクセスする際にユーザー認証情報がある場合は、ヘッダー名とヘッダー値を入力します。

MQTT

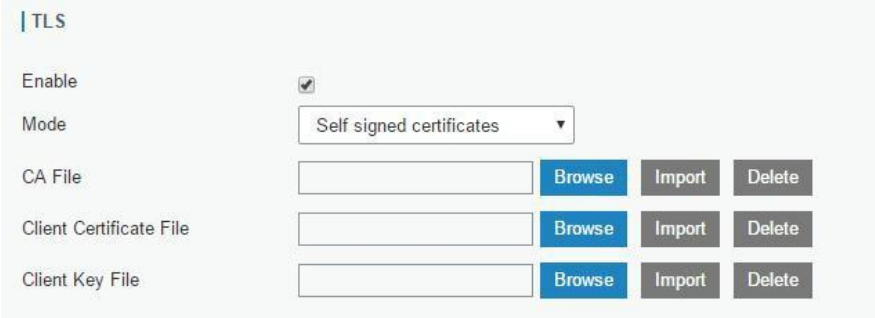
ステップ1：送信プロトコルをMQTTに選択します。ステップ2： MQTTブローカーの一般設定を入力します。



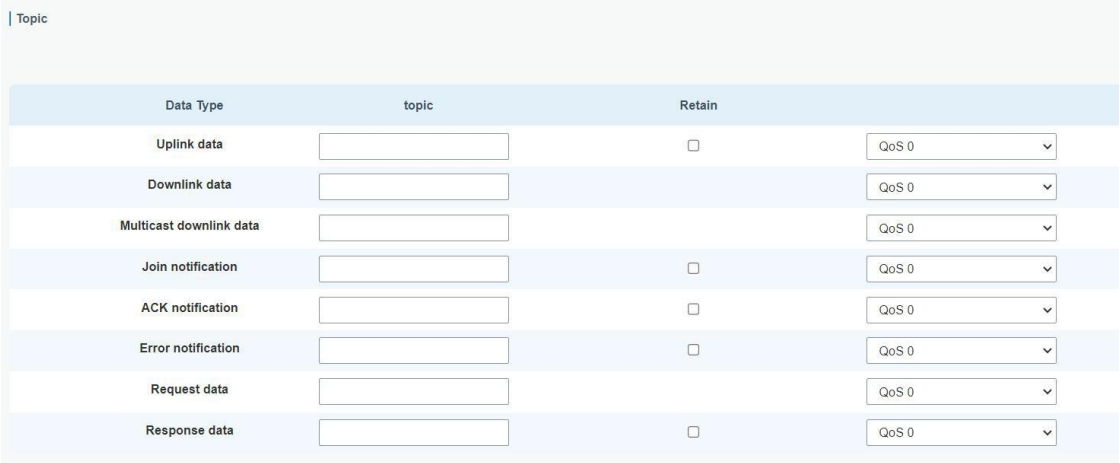
ステップ3：サーバーが必要とする認証方法を選択します。

認証にユーザー認証情報を選択した場合、認証にユーザー名とパスワードを入力する必要があります。

認証に証明書が必要な場合は、モードを選択し、認証用のCA証明書、クライアント証明書、クライアント鍵ファイルをインポートしてください。



ステップ4：データ受信またはダウンリンク送信のトピックを入力し、QoSを選択します。

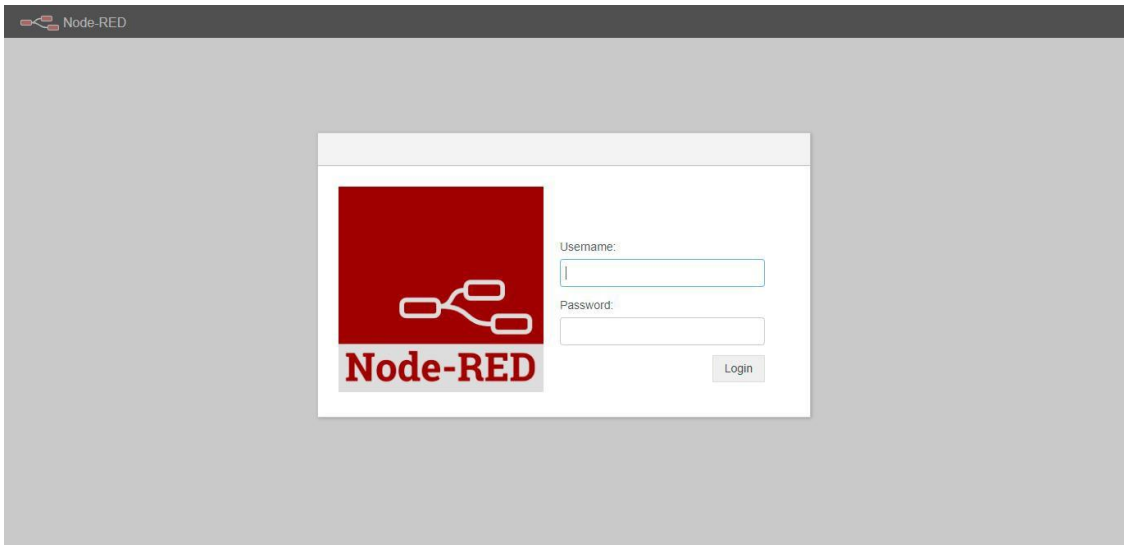


4.7 Node-RED

4.7.1 Node-REDの起動

1. App> Node-RED」にアクセスし、Node-RED機能を有効にします。

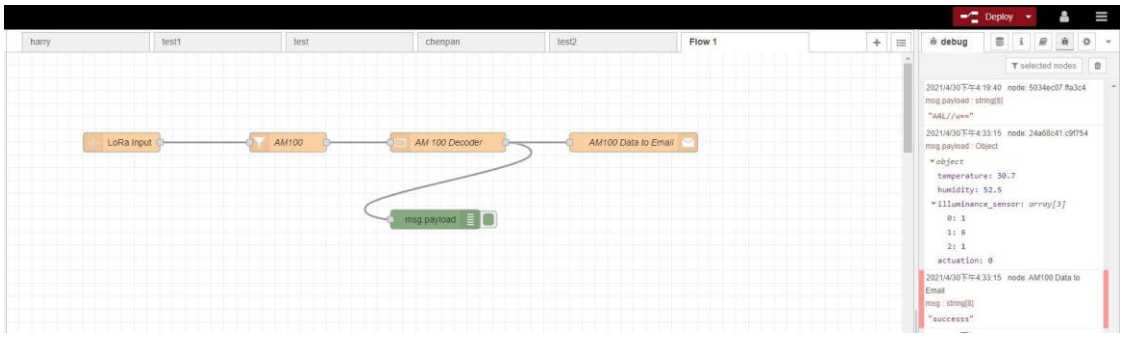
2. 有効化後、"Launch "をクリックして Node-RED のウェブ GUI にアクセスし、ゲートウェイと同じユーザー名とパスワードでログインします。



4.7.2 電子メールによるデータ送信

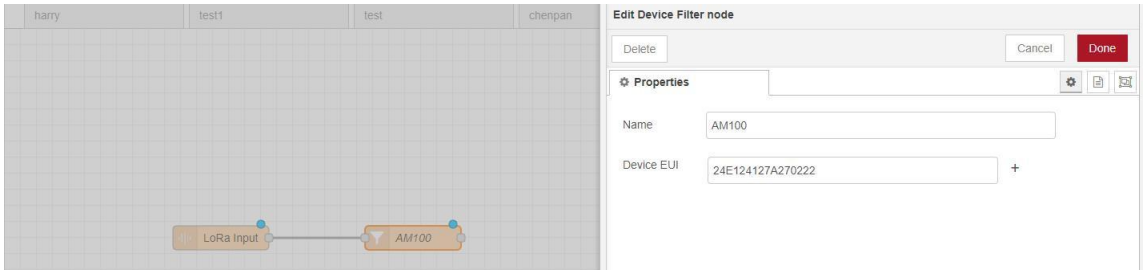
アプリケーションの例

AM102デバイスのデータを電子メールで送信します。

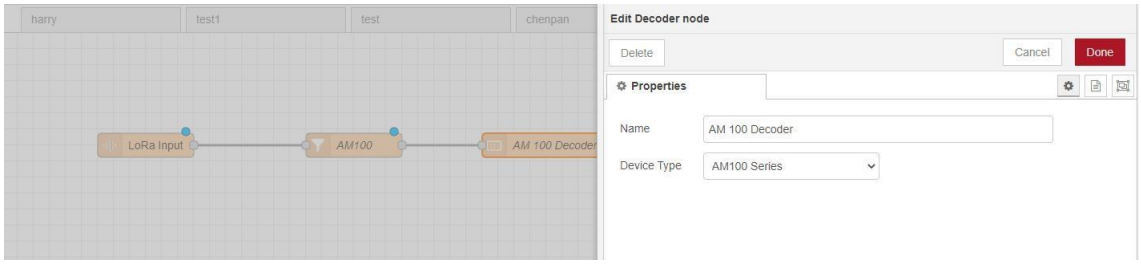


設定ステップ

1. LoRa Input" ノードを追加します。追加する前に、ネットワークサーバーモードが有効になっていることと、LoRaWANデバイスがネットワークに参加していることを確認してください。
2. 多数のデバイスを追加し、1つのデバイスデータしか必要ない場合は、"Device Filter " ノードを "LoRa Input "の後ろに追加し、デバイスのEUIを入力します。



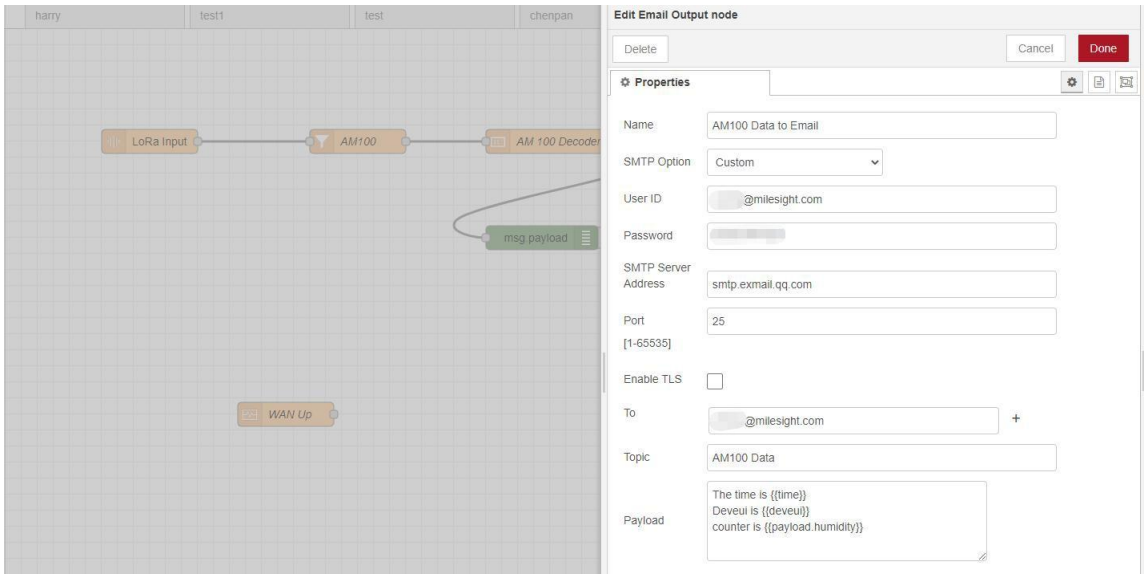
3. Milesightセンサーデータをデコードするために "Decoder "ノードを追加します。



4. Email Output "ノードを追加し、SMTPクライアントの設定、送信先メールアドレス、内容を入力します。

例

The time is{{time}}
Deveui is{{deveui}}
Humidity is {{payload.humidity}}



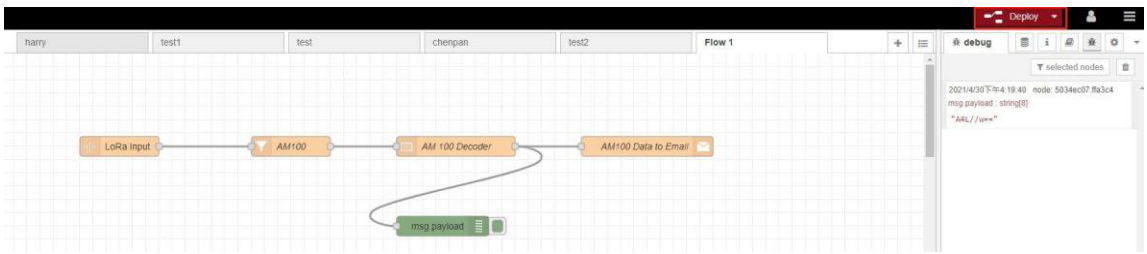
注意

1) SMTPオプションを "Same as Gateway "に選択した場合、"System -> General Settings-> SMTP "でSMTPクライアントの設定を行います。

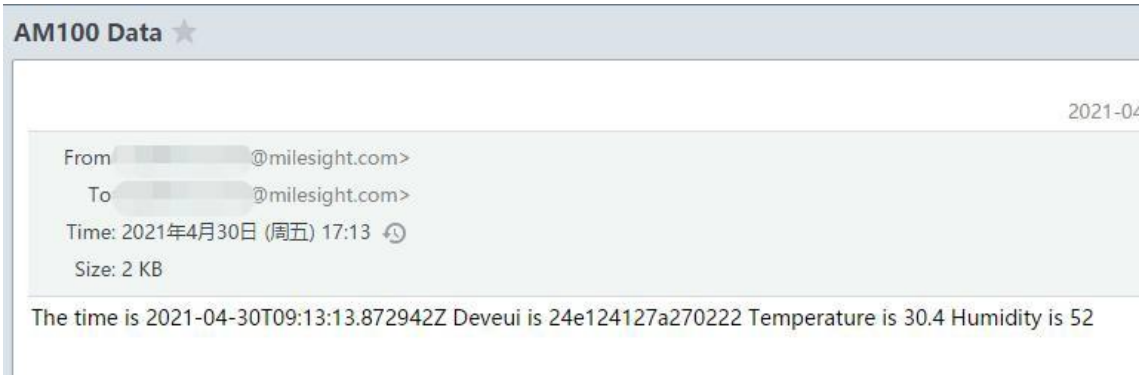
2) LoRaWANノードデータを呼び出す基本フォーマットは*{{プロパティ名}}*です。

3) 各ノードの出力内容を確認する必要がある場合は、デバッグノードを追加してください。

5. 設定が完了したら、"Deploy "をクリックして全ての設定を保存します。



6. AM102がゲートウェイにデータを送信すると、ゲートウェイはそのデータをEメールに転送します。



関連トピック

Node-RED

以上