Outdoor LoRaWAN®Gateway

UG67

ユーザーガイド

Preface

Milesight UG67 LoRaWAN® ゲートウェイをお選びいただき、誠にありがとうございます。UG67 は、自動フェイルオーバー/フェイルバック、拡張動作温度範囲、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、充実した機能設計により、ネットワーク上で強固な接続を実現します。

本ガイドでは、UG67 LoRaWAN® ゲートウェイの設定方法および動作方法についてご説明いたします。詳細な機能やゲートウェイの設定については、本ガイドをご参照ください。

Readers

本ガイドは主に以下のユーザーを対象としております：

- ネットワークプランナー
- 現場の技術対応および保守担当者
- ネットワーク構成および保守を担当するネットワーク管理者

Related Documents

Document	Description
UG67 Datasheet	UG67 LoRaWAN® ゲートウェイのデータシートです。
UG67 Quick Start Guide	UG67 LoRaWAN® ゲートウェイのクイックインストールガイドです。

Declaration of Conformity

UG67 は、CE、FCC、RoHS の基本要件およびその他の関連規定に適合しております。

お問い合わせの際は、Milesight テクニカルサポートまでご連絡ください：
メールアドレス：
iot.support@milesight.com
サポートポータル：support.milesight-iot.com
電話：86-592-5085280
FAX：86-592-5023065
住所：Building C09, Software Park III,
Xiamen 361024, China

Revision History

Date	Doc Version	Description
Dec. 31, 2020	V1.0	初期バージョン
Apr. 30, 2021	V1.1	1. LoRaWAN®Class Bの対応 2. Node-RED機能を追加いたしました 3. ノイズアナライザー機能を追加 4. マルチキャストグループ機能を追加 5. アプリケーション例を追加
Aug. 24, 2021	V1.2	1. Yeastar Workplaceプラットフォームの統合に対応いたします 2. パッケージ転送ステータスページの削除 3. 電話とメールのウェブページ更新
Dec. 15, 2021	V1.3	1. AS923-3およびAS923-4の追加 2. ネットワークサーバーのチャンネルマスク欄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
Feb. 23, 2022	V1.4	1. バッチバックアップを追加 2. ログインウェブページを更新しました 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 ACKタイムアウトの時間を調整
Jun. 1, 2022	V1.5	1. VLANトランククライアントの対応 2. SNMPにシステム名を追加 3. L2TPピアDNSオプションの使用を追加
Dec.26, 2022	V1.6	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のエクスポート機能を追加 4. パケット転送にデータ再送信機能を追加
March 6, 2023	V1.7	1. 内蔵アンテナモードを削除 2. LBT機能を追加
Feb. 21, 2024	V1.8	1. Milesight開発プラットフォームとの互換性 2. デフォルトのセカンダリICMPおよびDNSサーバーアドレスを更新 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
June 7, 2024	V1.9	1. OpenVPN接続用のovpnファイルのインポートに対応

		2. パケットフィルタ機能の対応 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に対応
Oct. 31, 2024	V 1.10	1. WireGuard機能を追加； 2. MQTTデータの再送信および保持オプションを追加； 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のSSLアクセスオプションを追加いたします； 5. BACnetオブジェクトイベント検出機能を追加； 6. ネットワークパケットアナライザー機能を追加； 7. DeviceHub 2.0との互換性を実現； 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機能を追加。
Jan. 8, 2025	V 1.11	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内のBACnet/IPオプションを削除； 3. BACnetオブジェクトのWeb GUIを更新しました； 4. Modbusサーバー機能を追加いたしました。
April 3, 2025	V 1.12	1. FUOTA機能を追加； 2. MQTTラストウィルメッセージ機能を追加； 3. デバイス追加時のアプリケーションキーオプションを更新； 4. メタデータオプションを更新しました； 5. WANのデフォルト接続タイプをDHCPに変更； 6. Web GUIへのアクセス手順を更新しました。
May 29, 2025	V 1.12.1	1. デバイスタイムアウトパラメータを追加； 2. BACnetサーバーはデフォルトで有効化されております。デフォルトのデバイスIDを更新してください。 3. デバイスリスト上で「アクティベート済み項目」を「ステータス項目」に変更してください； 4. BACnetグローバルオブジェクトの追加に対応します； 5. BACnetオブジェクトの自動追加に対応します； 6. BACnetおよびModbusオブジェクトの最大数を10,000に拡張しました； 7. 独立したHTTP APIアカウントの追加に対応いたします。
Aug. 13, 2025	V 1.13	1. パケットフォワーダー-トラフィックページにデータ項目を追加 2. カスタムペイロードコーデックのオブジェクトマッピング機能用のページ設定を追加； 3. デバイスプロファイルにADRオプションを追加します。 4. 全デバイス情報のエクスポートに対応； 5. パケットページにダウンロードキュークリア機能を追加； 6. BACnetグローバルオブジェクトタイプを追加しました； 7. Modbusグローバルオブジェクト機能とサーバーIDタイプを追加しました。 8. Modbusオブジェクトコピー機能を追加しました。
Dec. 24, 2025	バージョン 1.14	1. ビーコンによる時刻同期タイプのオプションを追加しました； 2. HTTP経由でのMQTT設定を追加；

		3. MQTT TLS認証用のSSLセキュアオプションを追加； 4. BACnet/SC機能を追加いたしました； 5. Modbusオブジェクトの一括インポートおよび全選択に対応； 6. HTTPプロキシ機能を追加； 7. Webパスワード制限と変更プロンプトを追加； 8. HTTP APIパスワード暗号化機能を追加しました。

Contents

内容

Chapter 1 Product Introduction

1.1 Overview

UG67は、堅牢な8チャンネル屋外用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台以上のノードに対応します。

UG67は、見通し距離最大15km、都市環境で約2kmをカバーでき、スマートオフィス、スマートビルディング、その他多くの屋外アプリケーションに最適です。

UG67は、イーサネット、Wi-Fi、セルラー通信による複数のバックホールバックアップに対応するだけでなく、主流のネットワークサーバー（The Things Industries、ChirpStackなど）との統合機能や、容易な導入を可能にする内蔵ネットワークサーバーを備えております。

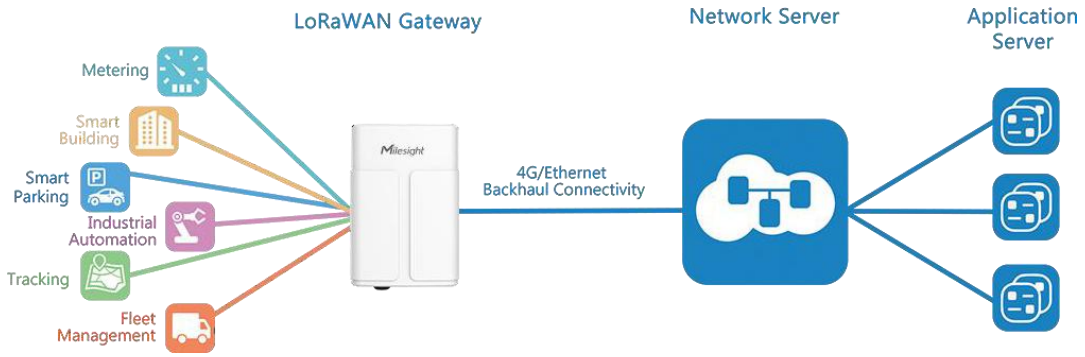


図1-1

1.2 Advantages

Benefits

- 産業用CPUと大容量メモリを内蔵
- イーサネット、2.4GHz Wi-Fi、およびグローバル対応の2G/3G/LTEオプションにより、接続が容易です
- 組み込みネットワークサーバーを搭載し、複数のサードパーティ製ネットワークサーバーに対応しております
- アプリケーションサーバーへのデータ伝送にはMQTT(s)またはHTTP(s)プロトコルを採用しております
- 堅牢な筐体で、壁面またはポールへの取り付けに最適化されています
- 3年間の保証が付帯しております

Security & Reliability

- イーサネットとセルラー間の自動フェイルオーバー/フェイルバック機能
- IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN/WireGuardなどのセキュリティフレームワークに対応
- 組み込みハードウェアウォッチドッグにより、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確保

Easy Maintenance

- Milesight DeviceHub および Milesight Development Platform は、リモートデバイスの簡単なセットアップ、一括設定、集中管理を実現します。
- ユーザーフレンドリーなウェブインターフェース設計と多様なアップグレードオプションにより、管理者は非常に簡単にデバイスを管理できます
- WEB GUIとCLIにより、管理者は大量のデバイス間でも迅速な設定とシンプルな管理を実現できます
- ユーザーは、産業用標準のSNMPを介して、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

Capabilities

- 通信技術が絶えず変化する環境において、リモートデバイスを接続します
- 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 1.5GHz 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に対応
- -40°C～70°C/-40°F～158°Fの広い動作温度範囲に対応

Chapter 2 Access to Web GUI

本章では、UG67のWeb GUIへのアクセス方法について
説明いたします。ユーザー名：**admin**
パスワード：**password**

Configuration Steps:

1. お使いのコンピューター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_XXXXXX**（WLAN MACアドレスの下6桁）を検索して接続してください。デフォルトのWi-Fiパスワードは**iotpassword**です。

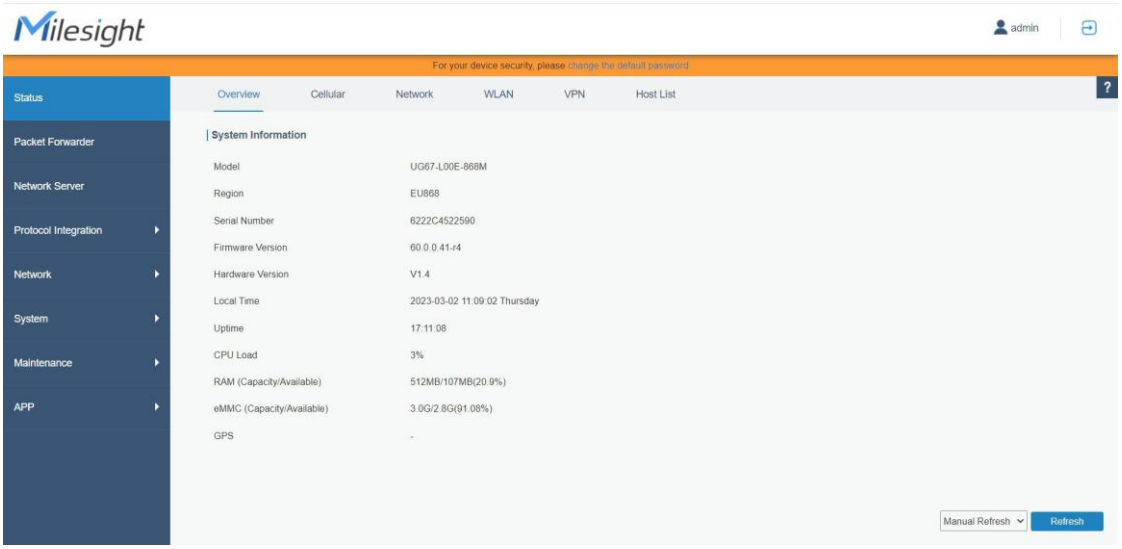
2. お使いのPCでWebブラウザ（Chromeが推奨）を開き、IPアドレス**https://192.168.1.1**を入力してWeb GUIにアクセスしてください。

3. ユーザー名とパスワードを入力し、"Login"をクリックしてください。

If you enter the username or password incorrectly more than 5 times, the login page will be locked for 10 minutes.

4. Web GUIにログイン後、初回にWeb GUIのパスワードを変更する必要があります。パスワードには、少なくとも1文字以上の英字と1文字以上の数字を含める必要があります。

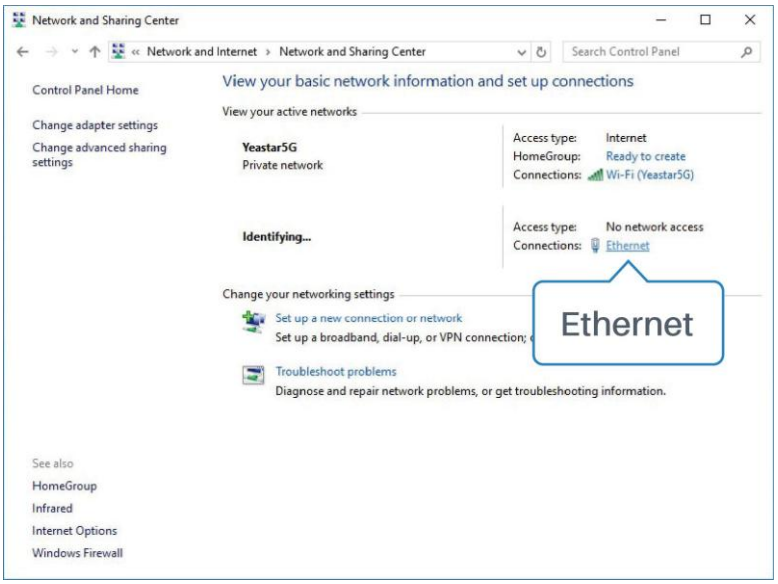
5. 新しいパスワードを使用して、再度ウェブGUIにログインしてください。ウェブGUIにログイン後、システム情報の確認やゲートウェイの設定操作が可能となります。



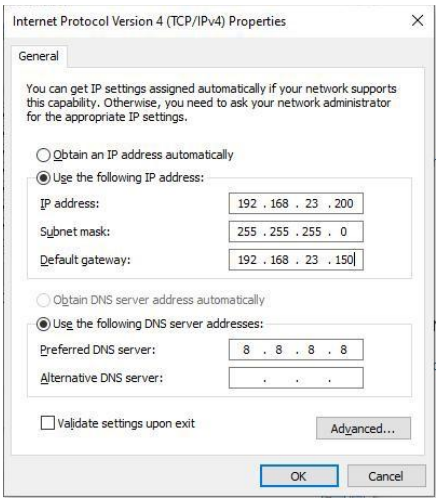
Note: バージョンv60.0.0.46以前の場合、ゲートウェイは有線接続にも対応しております。

1. PCをUG67のETHポートに直接、またはPoEインジェクター経由で接続してください。
2. お使いのコンピュータに手動でIPアドレスを割り当ててください。Windows 10システムを例に説明します。

A. 「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、"Ethernet"（名称が異なる場合があります）をクリックしてください。



B. "Properties"→"Internet Protocol Version 4 (TCP/IPv4)"を選択し、"Use the following IP address"を選択します。その後、ゲートウェイと同じサブネット内で静的 IP アドレスを手動で割り当ててください。



3. お使いのPCでWebブラウザ（Chromeが推奨）を開き、IPアドレス「**192.168.23.150** を入力してWeb GUIにアクセスしてください。

Chapter 3 Web Configuration

3.1 Status

3.1.1 Overview

このページでは、ゲートウェイのシステム情報を確認できます。

図 3-1-1-1

System Information	
Item	**Description**
Model	ゲートウェイのモデル名を表示します。
Region	ゲートウェイが使用するLoRaWAN®の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	システムの現在の現地時間を表示します。
Uptime	ゲートウェイの稼働時間を表示します。
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の容量と利用可能なRAMメモリを表示します。
eMMC (Capacity/Available)	eMMCの容量と空き容量を表示します。
GPS	ゲートウェイのGPSデータを表示します。

表 3-1-1-1 システム情報

Milesight UPSがデバイスに接続されると、UPSの基本情報もステータスページに表示されます。詳細については、*Milesight UPSユーザーガイド*をご参照ください。

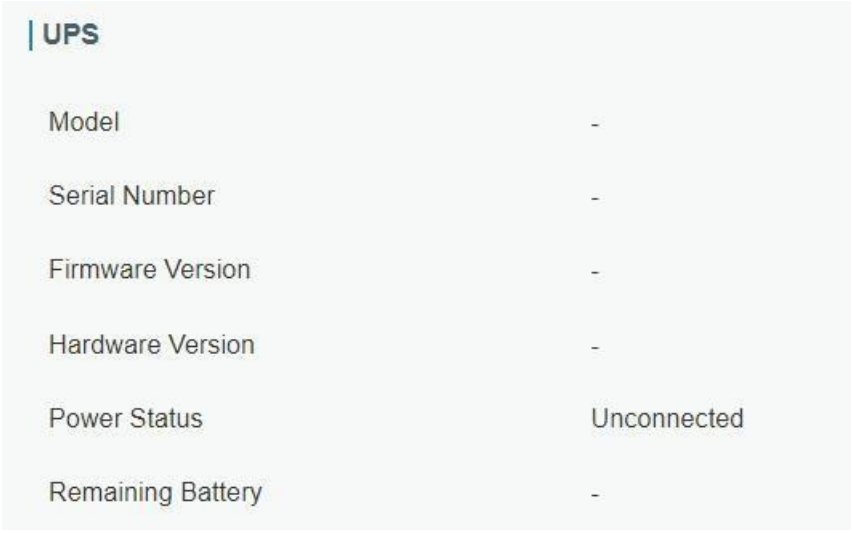


図3-1-1-2

3.1.2 Cellular (Cellular Version Only)

このページでは、ゲートウェイのセルラーネットワークの状態を確認できます。

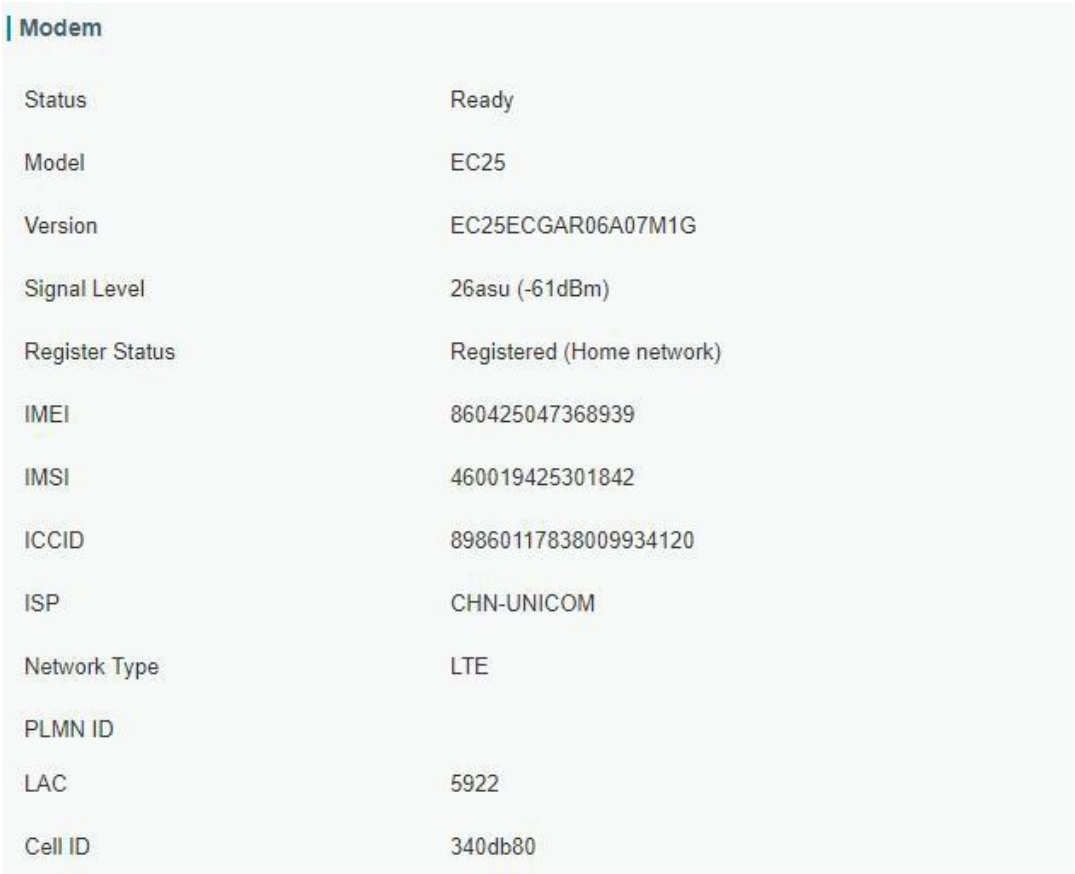


図 3-1-2-1

Modem Information	
Item	**Description**

Status	モジュールおよび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	セルラー信号レベルを表示します。
Register Status	SIMカードの登録ステータスを表示します。
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ーを表示します。
Network Type	接続中のネットワークタイプ（LTE、3Gなど）を表示します。
PLMN ID	現在のPLMN ID（MCC、MNC、LAC、セルIDを含む）を表示します。
LAC	SIMカードのロケーション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

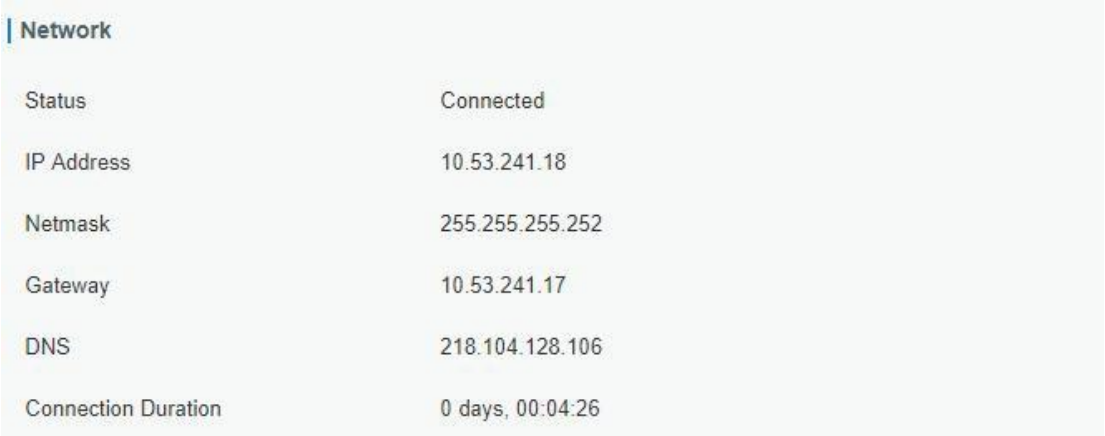


図 3-1-2-2

Network Status	
Item	**Description**
Status	携帯電話ネットワークの接続状態を表示します。
IP Address	携帯電話ネットワークの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	携帯電話ネットワークのDNSを表示します。
Connection Duration	携帯電話ネットワークが接続されている時間の情報を表示します。

表 3-1-2-2 ネットワークステータス

3.1.3 Network

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。

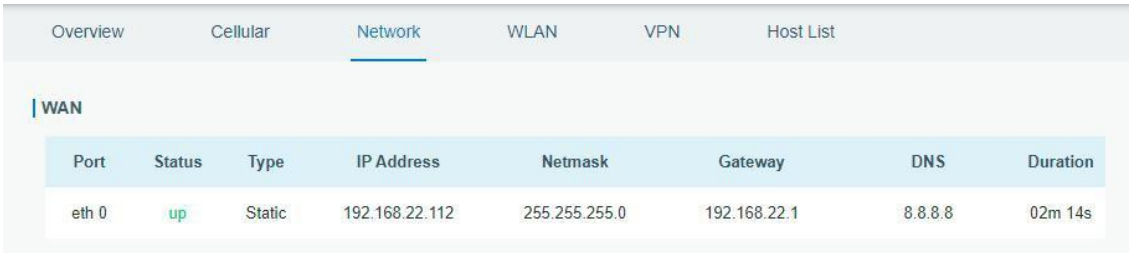


図 3-1-3-1

Network	
Item	**Description**
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状態を表示します。「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指します。「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	ポートが有効な状態で、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からの経過時間を表示します。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、経過時間の計測は停止します。

表 3-1-3-1 WAN ステータス

3.1.4 WLAN

このページでは、アクセスポイントやクライアントの情報を含む Wi-Fi ステータスを確認できます。

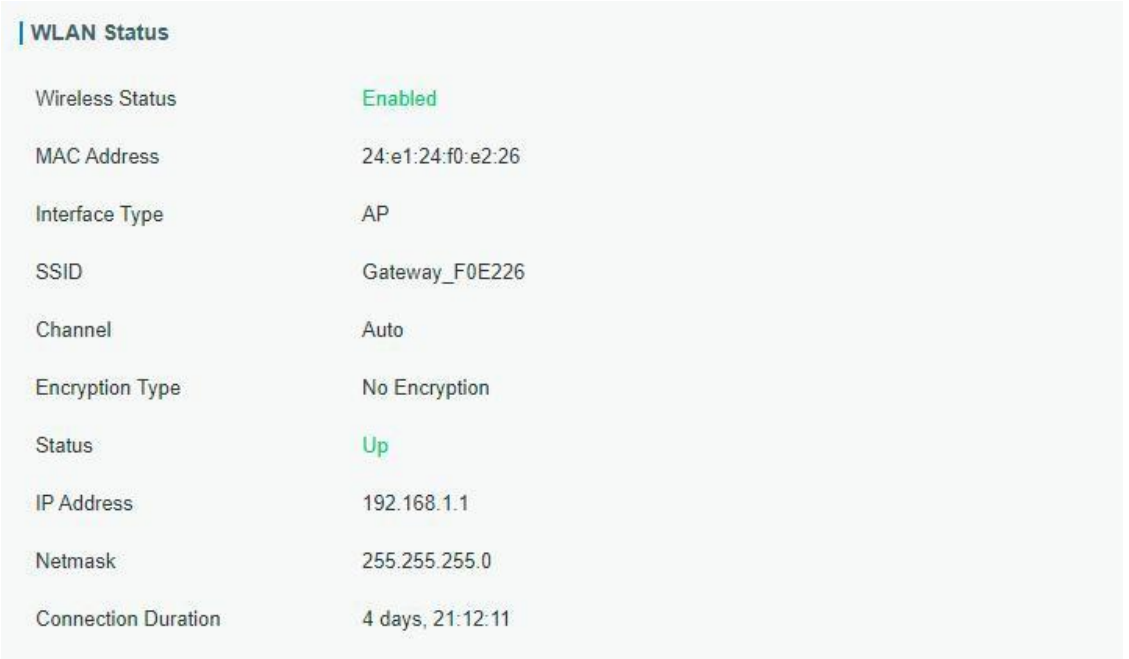


図 3-1-4-1

WLAN Status	
Item	**Description**
Wireless Status	無線の状態を表示します。
MAC Address	MAC アドレスを表示します。
Interface Type	インターフェースの種類（「AP」や"Client"など）を表示します。
SSID	SSIDを表示します。
Channel	無線チャネルを表示します。
Encryption Type	暗号化方式を表示します。
Status	接続状態を表示します。
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	無線ネットワークにおけるゲートウェイのアドレスを表示します。
Connection Duration	Wi-Fi ネットワークが接続されている時間の情報を表示します。

表 3-1-4-1 WLAN ステータス

図 3-1-4-2

Associated Stations	
Item	**Description**
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 ネットワークが接続されている時間の情報を表示します。

表 3-1-4-2 WLAN ステータス

3.1.5 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

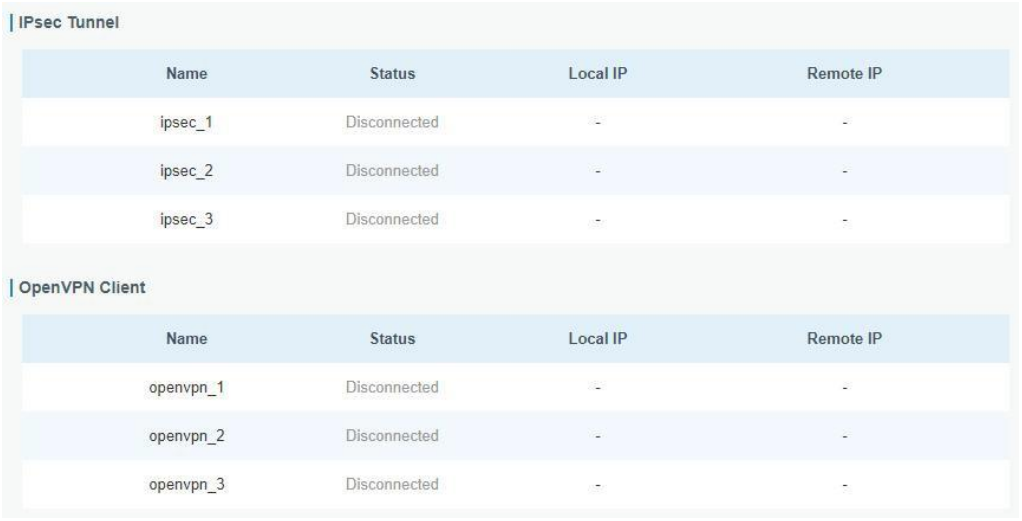


図 3-1-5-2

図 3-1-5-3

VPN Status	
Item	**Description**

Name	VPN トンネルの名称を表示します。
Status	VPN トンネルの状態を表示します。
Local IP	VPN トンネルのローカル IP を表示します。
Remote IP	VPN トンネルのリモート側トンネル IP を表示します。

表 3-1-5-1 VPN ステータス

3.1.6 Host List

このページでは、ホスト情報を確認できます。

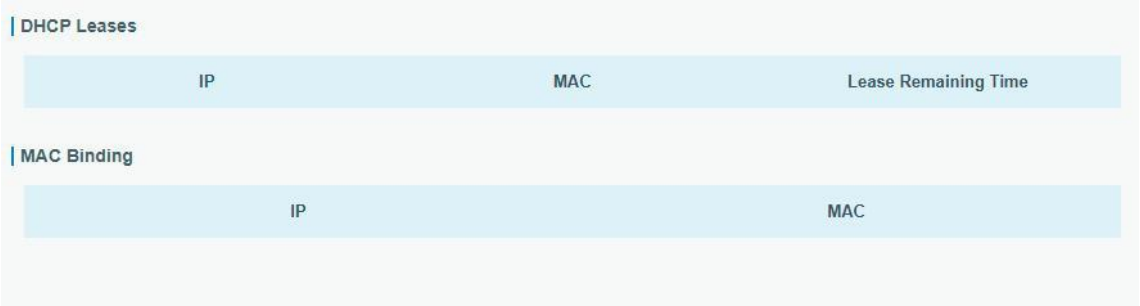
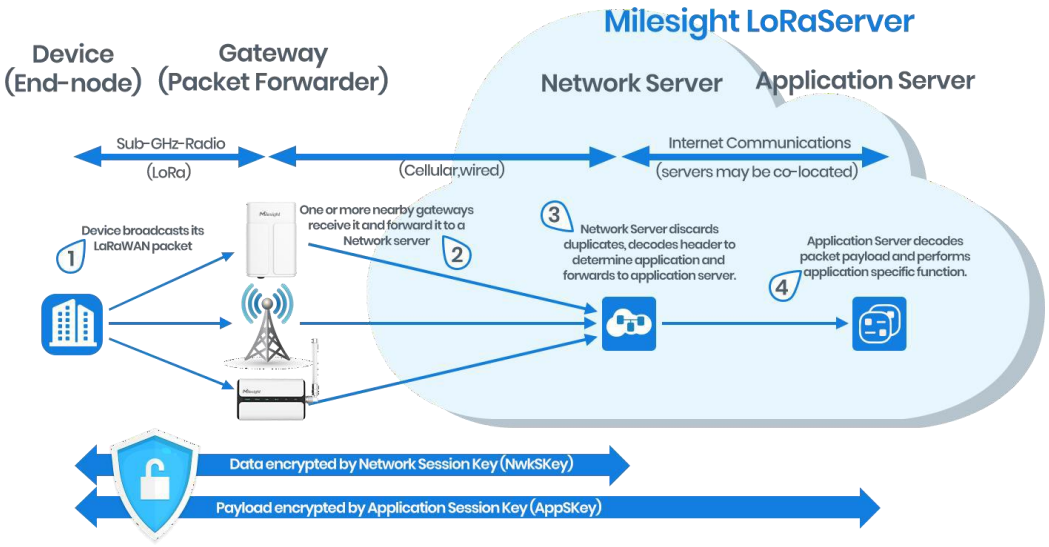


図 3-1-6-1

Host List	
Item	**Description**
DHCP Leases	
IP Address	DHCPクライアントのIPアドレスを表示します
MAC Address	DHCPクライアントのMACアドレスを表示します
Lease Time Remaining	DHCPクライアントのリース残存期間を表示します。
MAC Binding	
IP & MAC	DHCP サービスの静的 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 ホストリストの説明

3.2 LoRaWAN



3.2.1 Packet Forwarder

3.2.1.1 General

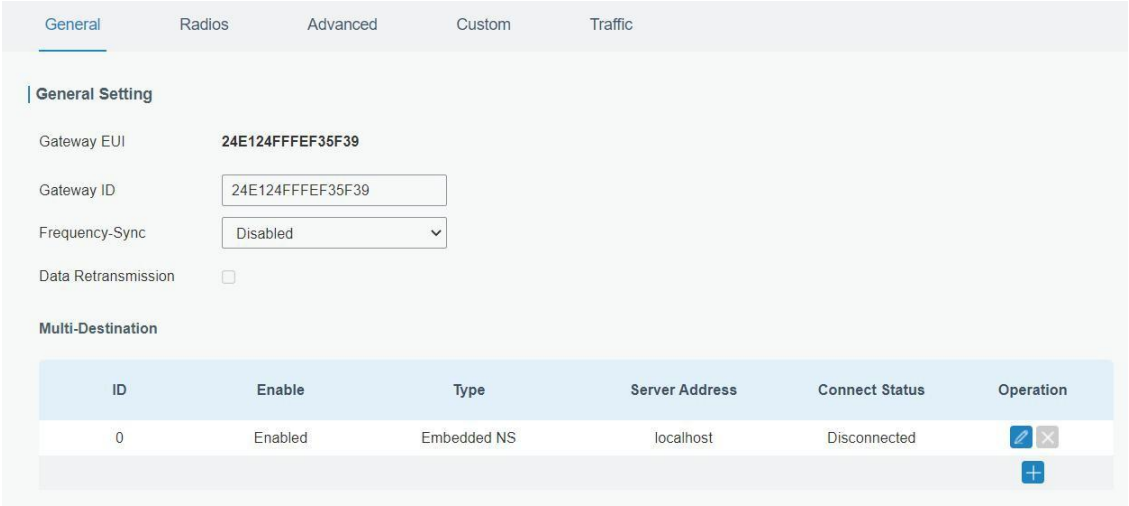


図 3-2-1-1

General Settings	
Item	**Description**
Gateway EUI	ゲートウェイの固有識別子を表示し、編集不可とします。 形式：ETHポートのMACアドレス + 中間に「FFFE」を挿入
Gateway ID	リモートネットワークサーバーへのゲートウェイ登録時に使用した対応するIDをご入力ください。通常はゲートウェイEUIと同じですが、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を選択することで、ネットワークサーバーから周波数設定を同期します。
Data	ゲートウェイが単一の

Retransmission	Chirpstack/Semtech/Remote Embedded NS/Basic Stationタイプのパッケージフォワーダーに接続した場合、ネットワークが切断された際に最大100万件のデータを対応して保存し、ネットワーク回復後にデータを再送信します。
Multi-Destination	ゲートウェイは、リスト内で作成および有効化されたネットワークサーバーアドレスにデータを転送します。
ConnectionStatus	パッケージフォワーダーの接続状態を表示します。

表 3-2-1-1 一般的な設定パラメータ

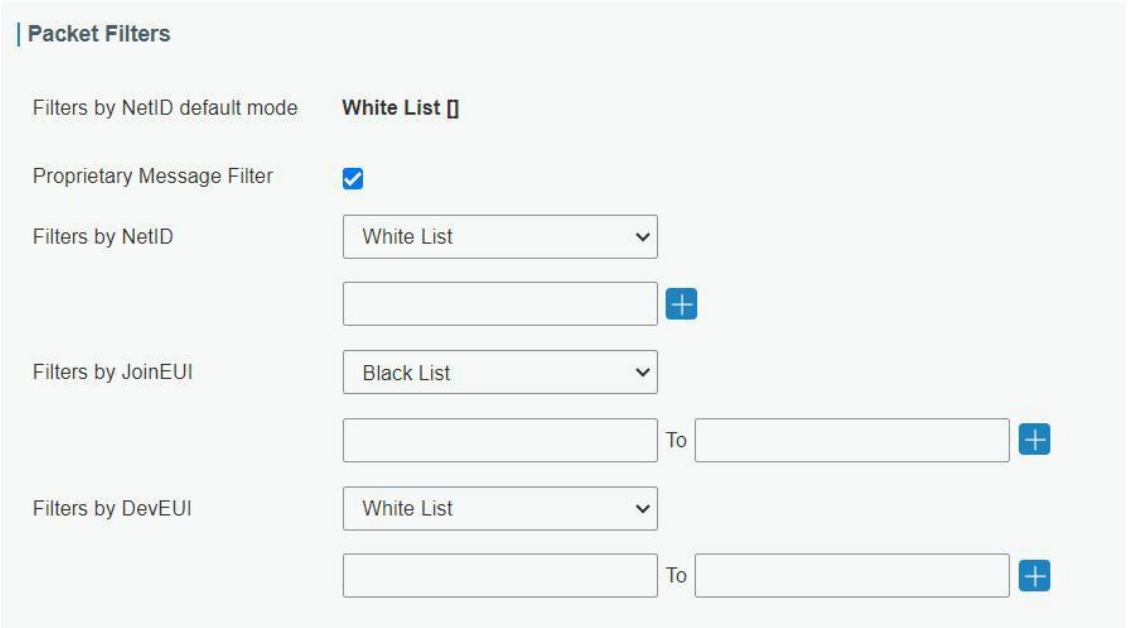


図 3-2-1-2

Packet Filters	
Parameters	**Description**
Filters by NetID Default Mode	フィルタモードをブラックリストまたはホワイトリストから選択します。 **White List:** このリストに記載された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:** このリストにないパケットのみをネットワークサーバーに転送します。
ProprietaryMessage Filter	プロプライエタリメッセージパケット（Mtype=111）を転送しないように有効にします。
Filters by NetID	NetID に一致するアップリンクパケットを転送/非転送します。
Filters by JoinEUI	JoinEUIの範囲に一致するJoinリクエストパケットを転送/転送しない。
Filters by DevEUI	DevEUIの範囲に一致する参加要求パケットを転送するか、転送しないか。
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。各条件で最大5つのリストに対応できます。

表 3-2-1-2 パケットフィルタのパラメータ

Note:

1. Join EUI と Dev EUI の両方が設定されている場合、両方の条件に一致するパケットのみが転送されます。
2. パケット転送タイプが Loriot または Everynet の場合、この機能は対応していません。
3. サードパーティ製ネットワークサーバーがゲートウェイにフィルタ条件を割り当てた場合、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。

Related Configuration Example

パケットフォワーダーの設定

3.2.1.2 Radios

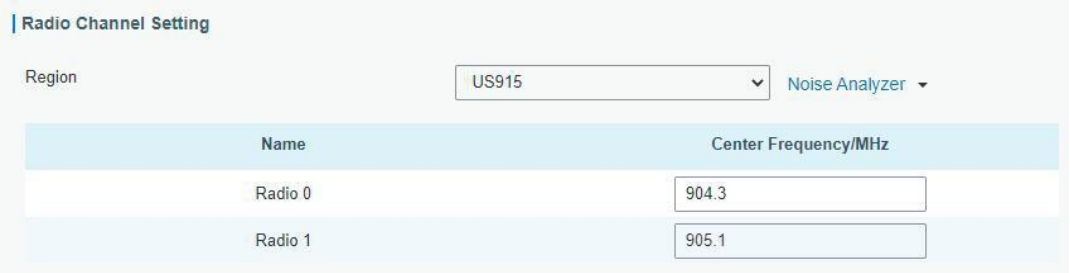


図 3-2-1-3

Radios-Radio Channel Setting		
Item	**Description**	**Default**
Region	上り/下り周波数およびデータレートに使用する LoRaWAN®周波数プランを選択してください。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。	ゲートウェイのモデルに基づきます
Center Frequency	LoRaWAN®ノードからのパケットを受信するための周波数を変更します。	LoRaWAN® 地域パラメータ文書で指定されている内容に基づきます

表 3-2-1-3 無線チャネル設定パラメータ

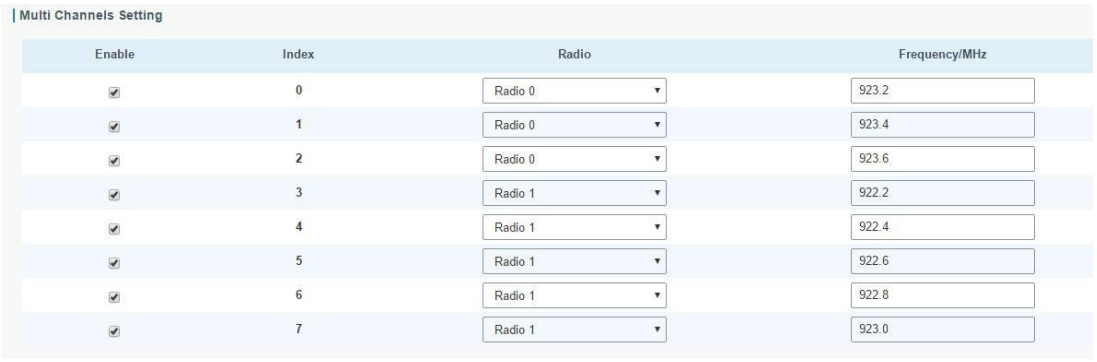


図 3-2-1-4

Radios-Multi Channel Setting		
Item	**Description**	**Default**
Enable	このチャンネルでパケットを送信できるようにするには、クリックしてください。	Enabled
Index	リスト内の順序番号を示します。	/
Radio	中心周波数としてラジオ0またはラジオ1をお選びください。	Radio 0
Frequency/MHz	このチャンネルの周波数を入力してください。範囲：中心周波数±0.4625。	LoRaWAN® 地域別ドキュメントに基づきます

表 3-2-1-4 マルチチャンネル設定パラメータ

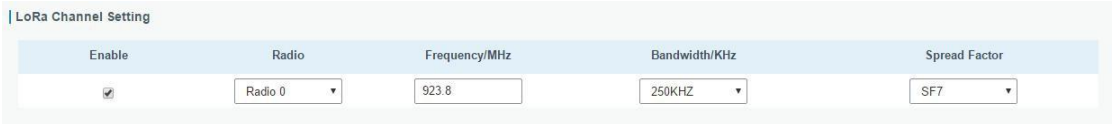


図 3-2-1-5

Radios-LoRa Channel Setting		
Item	**Description**	**Default**
Enable	このチャンネルでパケットを送信できるようにするには、クリックしてください。	Enabled
Radio	中心周波数としてラジオ 0 またはラジオ 1 をお選びください。	Radio 0
Frequency/MHz	このチャンネルの周波数を入力してください。範囲：中心周波数±0.9。	対応周波数に基づきます
Bandwidth/MHz	このチャンネルの帯域幅を入力してください。	500KHz
Spread Factor	選択可能な拡散係数をお選びください。拡散係数の大きいチャンネルは低レートに対応し、小さいチャンネルは高レートに対応します。	LoRaWAN® 地域パラメータ文書で指定されている内容に基づきます

表 3-2-1-5 LoRa チャネル設定パラメータ

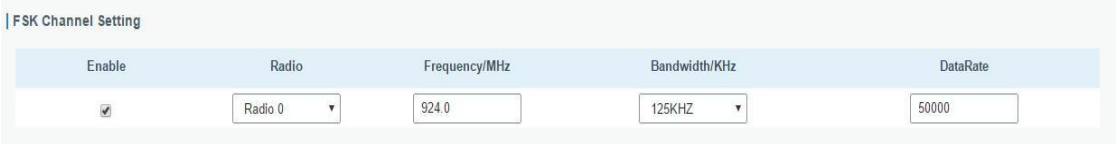


図 3-2-1-6

Radios-FSK Channel Setting		
Item	**Description**	**Default**
Enable	クリックすると、このチャンネルでパケットを送信できるようになります。	Disabled
Radio	中心周波数としてラジオ0またはラジオ1をお選びください。	Radio 0

Frequency/MHz	このチャンネルの周波数を入力してください。範囲：中心周波数±0.9。	対応周波数に基づきます
Bandwidth/MHz	このチャンネルの帯域幅を入力してください。推奨値：125KHz、250KHz、500KHz	対応周波数に基づきます
Data Rate	データレートを入力してください。範囲：500～25000。	500

表 3-2-1-6 FSK チャネル設定パラメータ

3.2.1.3 Noise Analyzer

ノイズアナライザーは、各周波数チャネルのノイズをスキャンし、ユーザー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表を提供するために使用されます。RSSIは各チャネルの感度を示します。RSSI値が低いほど、信号の状態は良好です。パッケージフォワーダーを使用する際には、この機能を有効にすることは推奨されません。ダウンリンク伝送に影響を与える可能性があるためです。

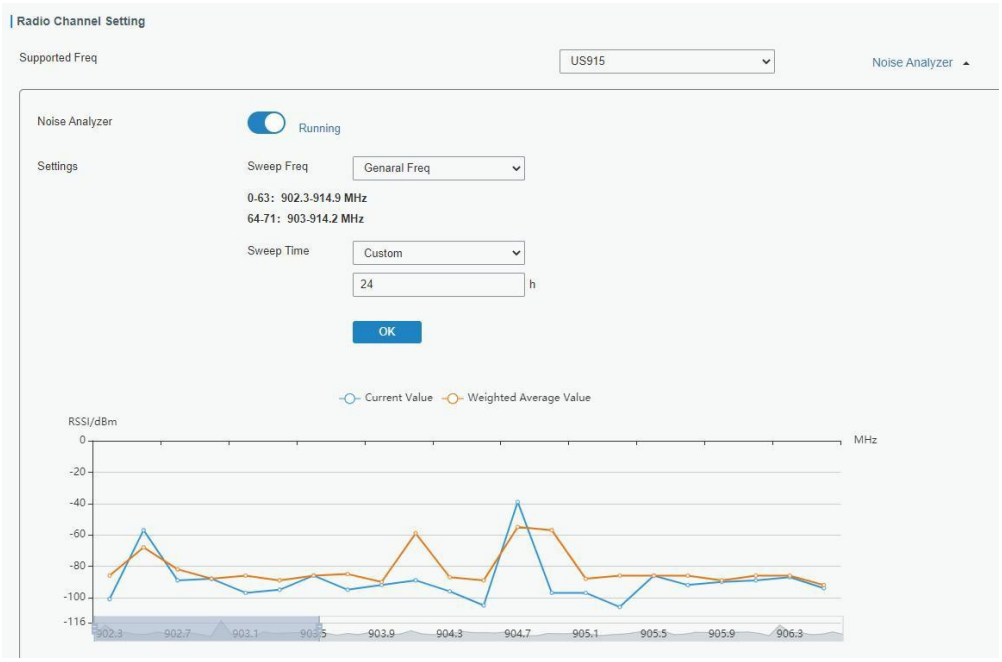


図3-2-1-7

Noise Analyzer		
Item	**Description**	**Default**
Enable	ノイズアナライザー機能を有効にするには、こちらをクリックしてください。	Disabled
Sweep Freq	周波数掃引範囲を選択してください。 **General** LoRaWAN® 地域パラメータ文書に基づく周波数 **Custom:** 周波数範囲をカスタマイズします	General Feq
Sweep Time	ノイズアナライザを連続的に、または一定時間内に有効にします。 カスタムを選択した場合、ノイズアナライザーは事前設定された時間が経過すると自動的に停止します。	Custom/24h

	注記：ノイズアナライザー機能は通常のデータ伝送に影響を与えるため、時間をカスタム設定することをお勧めいたします。	

表 3-2-1-7 ノイズアナライザー設定パラメータ

3.2.1.4 Advanced

このセクションでは、ビーコンの送信および検証に関する詳細な設定について説明します。

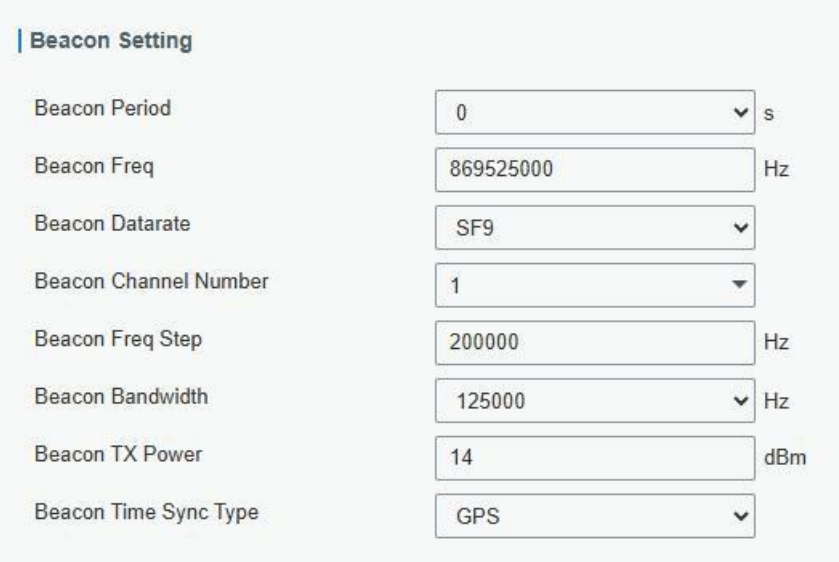


図 3-2-1-8

Advanced-Beacon Setting		
Item	**Description**	**Default**
Beacon Period	クラスBデバイスの時刻同期のためにゲートウェイがビーコンを送信する間隔です。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	ビーコンの周波数です。	対応し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。	対応している周波数に基づきます
Beacon Channel Number	カスタムを選択した場合、ユーザーは1から8までの範囲でカスタマイズすることが可能です。	1
Beacon Freq Step	ビーコンの周波数間隔です。	200000
Beacon Bandwidth	ビーコンの帯域幅です。単位：Hz	12500 Hz
Beacon TX Power	ビーコンの送信電力です。	対応している周波数に基づきます

Beacon Time Sync Type	ビーコンの時間同期タイプをGPSまたはUTCからお選びください。	GPS
Beacon Time Offset	時刻同期タイプが UTC の場合、ゲートウェイはシステム時刻にこのオフセットを加算し、その結果をクラス B デバイスに割り当てます。	0

表 3-2-1-8 高度なビーコンパラメータ

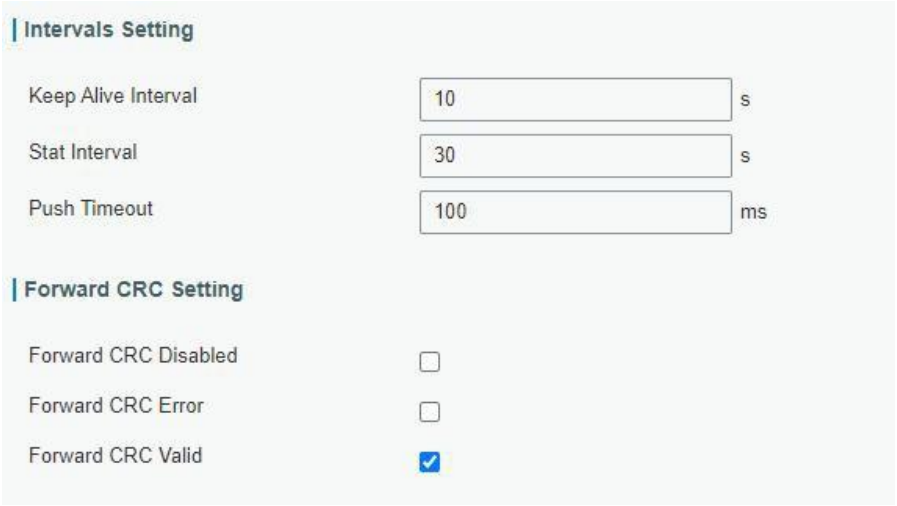


図 3-2-1-9

Item	Description	Default
Keep Alive Interval	ゲートウェイからネットワークサーバーへ送信されるキープアライブパケットの間隔を入力してください。これにより接続が安定し、維持されます。 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てください。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機するタイムアウトを入力してください。範囲：1～1999。	100
Forward CRC Disabled	CRCを無効にした状態で受信したパケットをネットワークサーバーへ送信できるようにします。	Disabled
Forward CRC Error	有効にすると、CRCエラーのある受信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	有効にすると、CRCが有効な状態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

図 3-2-1-10

Item	Description	Default
Enable	LBT機能の有効化または無効化を行います。LBT（Listen Before Talk）は、ダウンリンクチャネルがアイドル状態であるかどうかを検知し、チャネルアクセス競合を回避するために使用されます。 注記：AU915 および US915 は LBT 機能に対応しておりません。	Disabled
RSSI Target	空き状態のチャネルの基準値を入力してください。チャネルの実際のRSSIが基準値/目標値未満の場合、そのチャネルは空き状態と見なされます。範囲：-120～0	-80

表 3-2-1-10 高度な LBT パラメータ

3.2.1.5 Custom

カスタム設定モードを有効にした場合、編集ボックスに独自のパケットフォワーダー設定ファイルを記述してパケットフォワーダーを設定できます。"Save"をクリックするとカスタム設定ファイルの内容が保存され、"Apply"をクリックすると設定が有効になります。"Clear"をクリックすると編集ボックスの内容がすべて消去されます。設定ファイルの記述方法がわからない場合は、"Example"をクリックして参照ページに移動してください。

Note: カスタム設定はWeb GUIのパケット転送設定を上書きします。

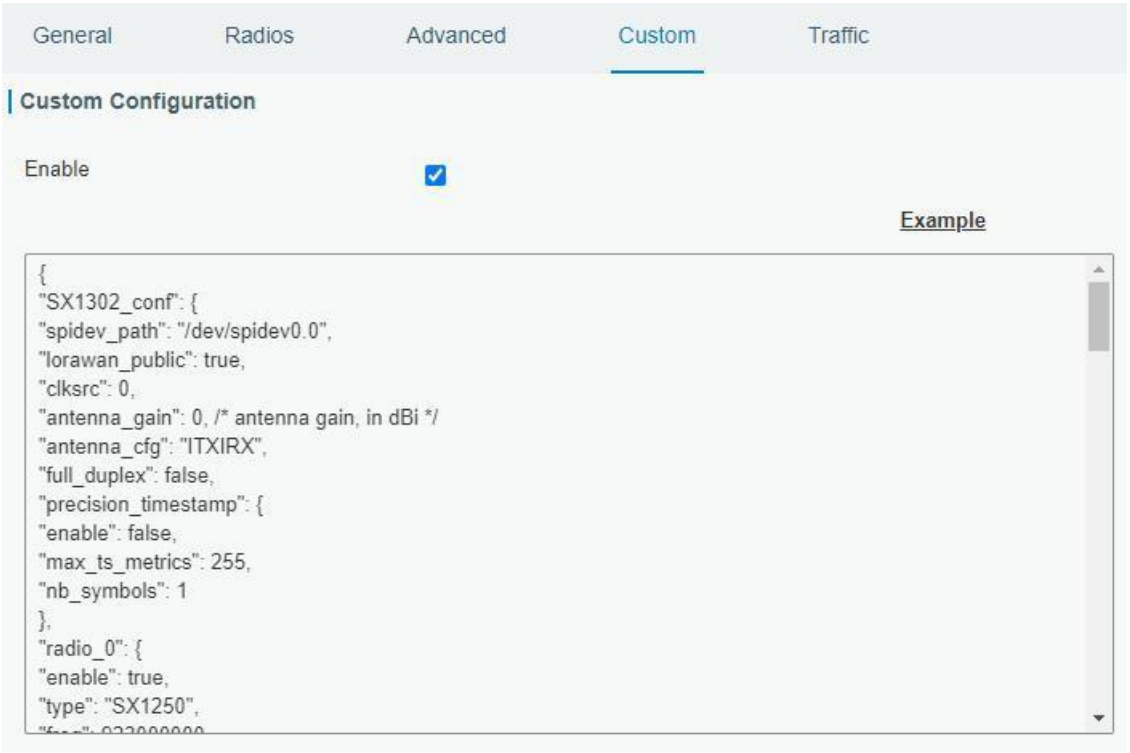


図 3-2-1-11

3.2.1.6 Traffic

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直近のトラフィックが表示されます。ライブトラフィックを監視するには、「**Refresh**をクリックしてください。

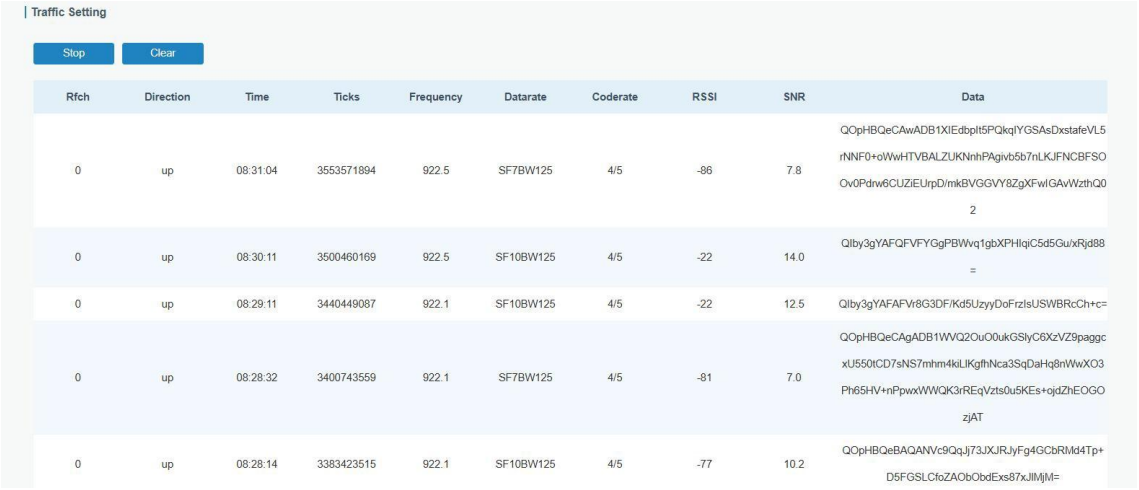


図 3-2-1-12

Item	Description
Refresh	最新のデータを入手するには、こちらをクリックしてください。
Clear	すべてのデータを消去するにはクリックしてください。
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	このパケットの符号化率を表示します。
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。
Data	このパケットのペイロード（Base64）を表示します。 **Note**：Loriot および Actility パケットフォワーダーでは機能しません。

表 3-2-1-11 トラフィックパラメータ

3.2.2 Network Server

3.2.2.1 General

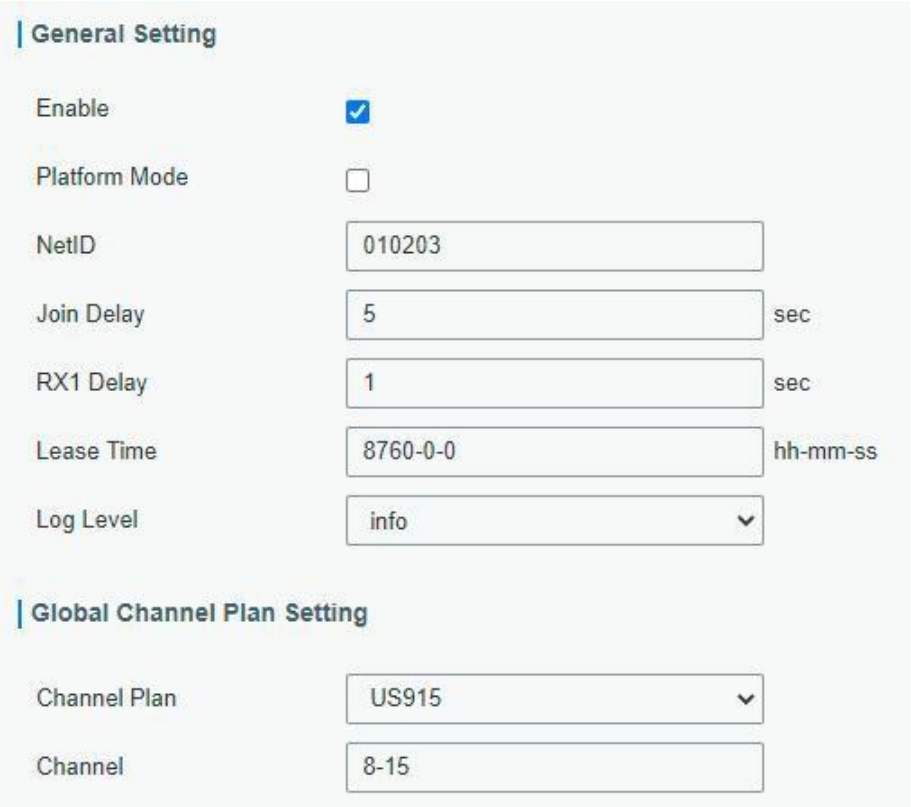


図 3-2-2-1

Item	Description	Default
General Setting		
Enable	クリックするとネットワークサーバーモードが有効になります。	Enabled
Platform Mode	有効にすると、ゲートウェイを Milesight IoT クラウドまたはYeastar Workplaceプラットフォームに接続します。	Disabled
NetID	ネットワーク識別子を入力してください。	010203
Join Delay	エンドデバイスがネットワークサーバーに Join_request_message を送信してから、エンドデバイスがネットワークサーバーから送信される Join_accept_messageを受信するためにRX1を開く準備が整うまでの間隔時間を入力してください。	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、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てください。	1
Lease Time	成功した参加が期限切れになるまでの時間を入力してください。形式は時間-分-秒です。参加タイプが OTAA の場合、リース時間が経過すると、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てください。	情報
Channel Plan Setting		
Channel Plan	上りリンクおよび下りリンクの周波数とデータレートに使用するLoRaWAN®チャネルプランをお選びください。ご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依存します

Channel	エンドデバイスが特定の周波数チャネルで通信できるようにします。 空白のままにすると、LoRaWAN®の地域パラメータ文書で指定されているデフォルトの標準使用可能チャネルすべてを使用します。チャネルのインデックスを入力することができます。**Examples:** 1, 40: チャネル1とチャネル40を有効化 1-40: チャネル1からチャネル40を有効化 1-40, 60: チャネル1からチャネル40およびチャネル60を有効化	ゲートウェイの周波数に依存します

表 3-2-2-1 基本パラメータ

Note: 一部の地域バリエーションでは、ご利用の 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 のように LoRaWAN® 地域パラメータで定義されていない追加チャンネルを設定することができます。以下の図をご参照ください：

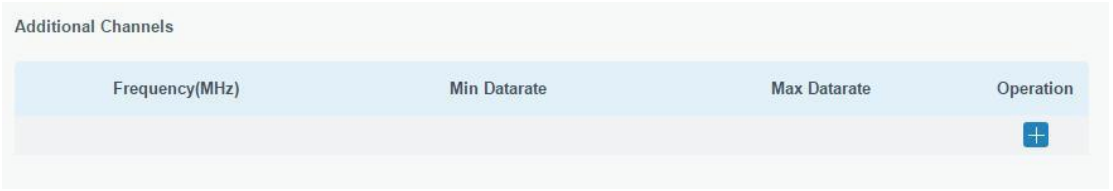


図 3-2-2-2

Additional Channels		
Item	**Description**	**Default**
Frequency/MHz	追加プランの周波数を入力してください。	Null
Max Datarate	エンドデバイスの最大データレートを入力してください。範囲は、LoRaWAN® 地域パラメータ文書で規定されている内容に基づいています。	DR0（SF12、125kHz）
Min Datarate	エンドデバイスの最小データレートを入力してください。範囲はLoRaWAN®地域パラメータ文書で規定されている内容に基づきます。	DR3(SF9,125kHz)

表 3-2-2-2 追加プランパラメータ

3.2.2.2 Application

アプリケーションとは、同じ目的または同じタイプのデバイスの集合体です。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。

アプリケーションは、クリックして編集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したり、 をクリックすることで作成できます。

図 3-2-2-3

Application	
Item	**Description**
Name	アプリケーションプロファイルの名前を入力してください。 例：smoker-sensor-app
Description	このアプリケーションの説明を入力してください。 例：煙感知器用アプリケーション。
Metadata	デバイスがペイロードコーデックを追加した際に、アップリンクパケットで自動的に報告する詳細情報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、お客様の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では、MQTT伝送とHTTP（HTTPS）伝送をそれぞれ1つずつ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 Integration

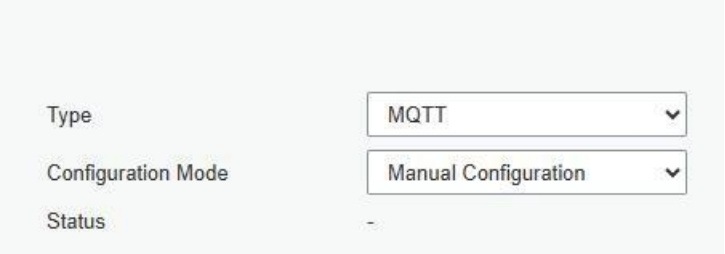


図 3-2-2-4

MQTT Settings	
Item	**Description**
Type	タイプを MQTT として選択してください。
Configuration Mode	設定モードを選択してください。 **Manual Configuration:** ウェブページ経由でパラメータを設定します。 **Get via HTTP:** プラットフォームにHTTPリクエストを送信し、MQTT設定パラメータを取得します。
Status	MQTT接続状態を表示します。
Get via HTTP	

Platform URL	HTTPリクエストを送信するプラットフォームURLを選択してください。
Custom Format	プラットフォームに送信する HTTP リクエストの内容をカスタマイズします。

表 3-2-2-4 MQTT 設定パラメータ

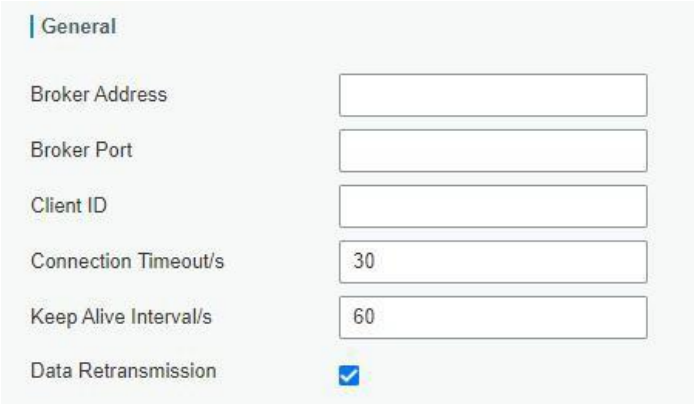


図 3-2-2-5

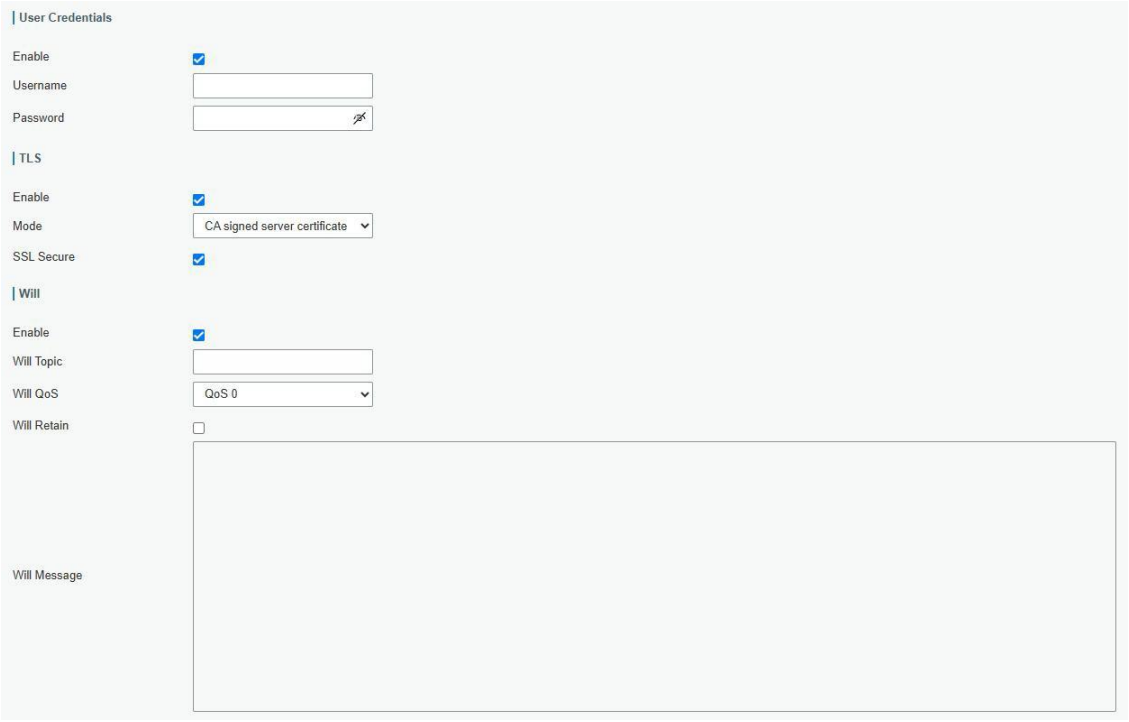


図 3-2-2-6

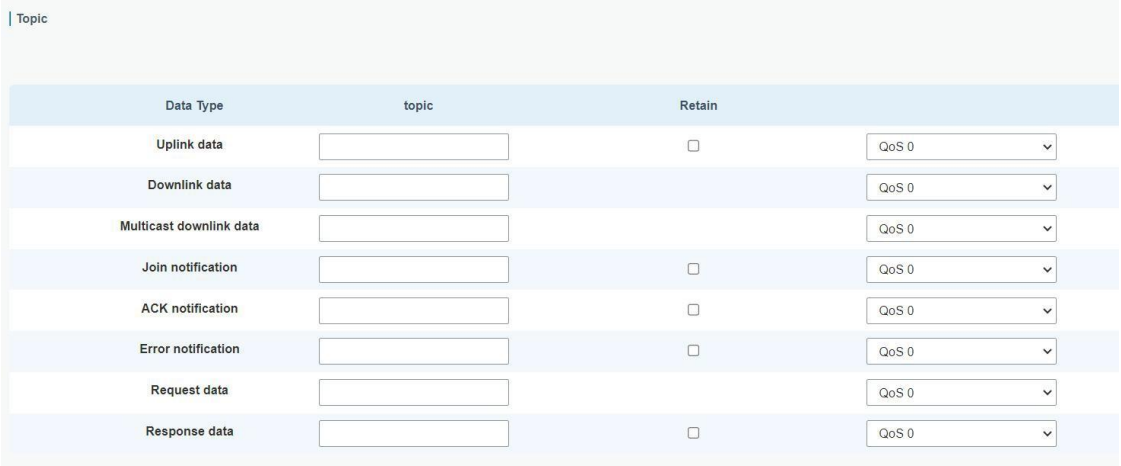


図 3-2-2-7

MQTT Settings - Manual Configuration	
Item	**Description**
General	
BrokerAddress	データを受信するためのMQTTブローカーのアドレス。
Broker Port	データを受信するためのMQTTブローカーのポート番号です。
Client ID	クライアントIDは、サーバーに対するクライアントの固有の識別子です。複数のクライアントが同じサーバーに接続している場合、これは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に不可欠です。
ConnectionTimeout/s	クライアントが接続タイムアウト後に応答を得られない場合、接続は切断されたものとみなされます。範囲：1～65535
Keep AliveInterval/s	クライアントがサーバーに接続した後、クライアントは定期的にハートビートパケットをサーバーに送信し、接続を維持します。範囲：1～65535
Data Restransmission	有効化後、ネットワークが切断された場合に最大 10,000 件のデータを対応し、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です。
Password	MQTTブローカーへの接続に使用するパスワードです。
TLS	
Enable	MQTT通信におけるTLS暗号化を有効にします。 **Note:** MQTTブローカーの種類がHiveMQの場合、**TLS** 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	「自己署名証明書」または「CA署名サーバー証明書」からお選びください。**CA signed server certificate:** デバイスにプリロードされている認証局（CA）発行の証明書で検証します。 **Self signed certificates:** 検証用のカスタム CA 証明書（.crt または .pem）、クライアント証明書（.crt）、および秘密鍵（.key）をアップロードします。
SSL Secure	有効化後、ゲートウェイは証明書の有効性を検証します。

Will	
Enable	MQTTクライアントが異常切断された場合、ラストウィルメッセージが自動的に送信されます。通常、デバイスの状態情報を送信したり、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状態を通知するために使用されます。
Will Topic	ラストウィルメッセージを受信するためのトピックをカスタマイズします。
Will QoS	QoS0、QoS1、QoS2は任意で設定可能です。
Will Retain	有効にすると、最終意志メッセージを保持メッセージとして設定します。
Will Message	最終状態メッセージの内容をカスタマイズします。
Topic	
Data Type	MQTTブローカーとの通信に使用するデータ型： **Uplink Data:** デバイスからのアップリンクパケットを受信します。 **Downlink**デバイスへのダウンリンクコマンド送信。単一デバイスへのダウンリンクコマンド送信が必要な場合は、このトピックにワイルドカード「$deveui」を追加し、トピック購読時に実際のデバイスの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:** ゲートウェイが参加許可パケットを送信し、デバイスがネットワークに参加することを許可した場合、参加通知を受信します。 **ACK**ダウンリンクコマンド送信時にデバイスからACKパケットを受信します。 **Error Notification:** デバイスからのエラーパケットを受信します。 **Request data:** ゲートウェイのNS（ネットワークサービス）を照会・設定するためのリクエストを送信します。 **Response data:** リクエストに対する応答を受信します。
Topic	パブリッシュに使用されるデータ型のトピック名。
Retain	有効にすると、このトピックの最新メッセージをリテインメッセージとして設定します。
QoS	QoS 0 – 1回のみ配信 これは最も高速な方法であり、メッセージは1回のみ送信されます。ただし、信頼性が最も低いモードとなります。 QoS 1 – 少なくとも一度 このレベルでは、メッセージが少なくとも1回は確実に配信されますが、複数回配信される可能性もあります。 QoS 2 – 厳密に1回 QoS 2 は MQTT における最高レベルのサービスです。このレベルでは、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が保証されます。QoS 2 は最も安全で、最も遅いサービス品質レベルです。

表 3-2-2-5 MQTT 設定 - 手動構成パラメータ

HTTP/HTTPS Integration

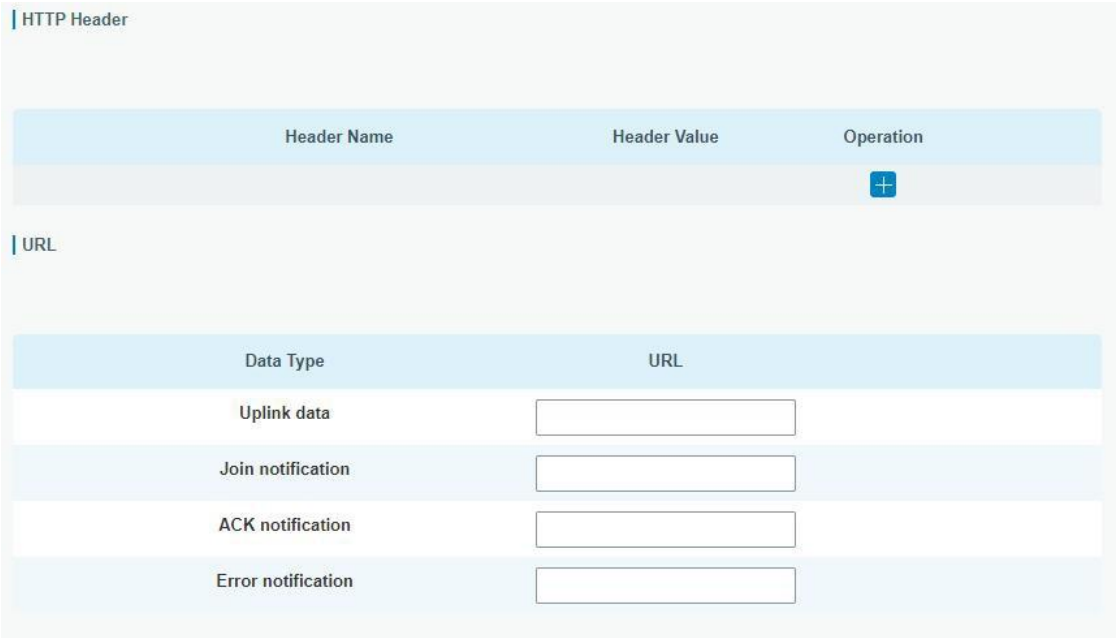


図 3-2-2-8

HTTP/HTTPS Settings	
Item	**Description**
HTTP Header	
Header Name	HTTP ヘッダーにおける主要なフィールド群です。
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:** デバイスからのアップリンクパケットを受信します **Join Notification:** ゲートウェイが参加許可パケットを送信し、デバイスがネットワークに参加できるようにした場合、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パケットを受信します **Error Notification:** デバイスからのエラーパケットを受信します
Topic	公開に使用されるデータ型のトピック名。
URL	データを受信するためのHTTP/HTTPSサーバーのURLです。

表 3-2-2-6 HTTP/HTTPS 設定パラメータ

Related Configuration Example

アプリケーション設定

3.2.2.3 Payload Codec

ペイロードコーデックは、Milesight LoRaWAN® デバイスに組み込まれたペイロードコーデックライブラリを提供し、データのデコードおよびエンコードを容易に行います。ユーザーは、他ブランド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、要件に応じてアップリンクおよびダウンリンクのコンテンツを調整したりすることも可能です。

Inbuilt Payload Codec Library

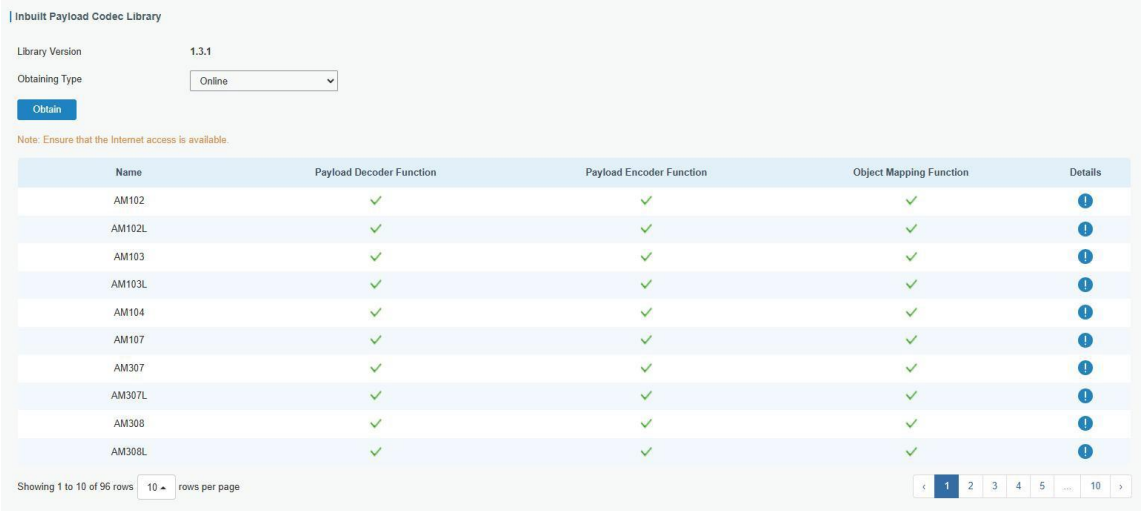


図 3-2-2-9

Inbuilt Payload Codec Library	
Item	**Description**
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てください。**Online:** ゲートウェイの電源投入時およびインターネット接続時に、バージョン更新を検出した場合、自動的に更新されます。 ユーザー様は"Fetch"ボタンをクリックして、更新状況を手動で確認することも可能です。**Obtain** 「**Local**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、 をクリックするとライブラリが更新されます。Milesightペイロードコーデックパッケージについては、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に対応する 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かどうかを表示します。
Payload Encoder Function	エンコーダーが存在するか表示します。
Object Mapping Function	オブジェクトマッピング関数が存在するかどうかを表示します。
Details	デコーダおよびエンコーダの詳細を表示します。ご要件に合わない場合は、ペイロードコーデックをカスタマイズしてください。

表 3-2-2-7 内蔵ペイロードコーデックライブラリパラメータ

Custom Payload Codec

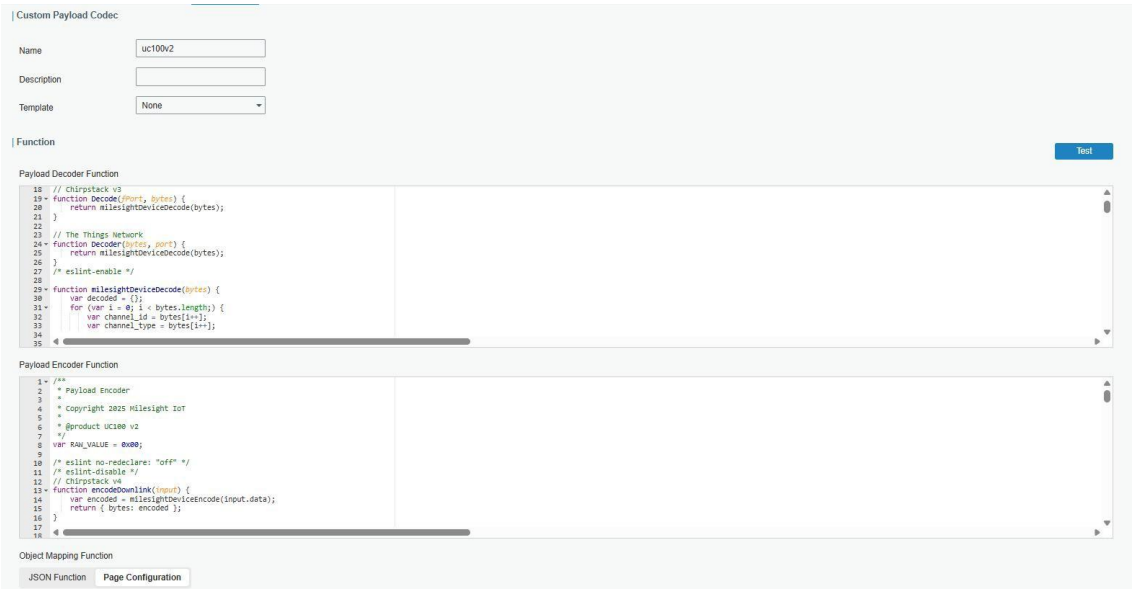


図 3-2-2-10

Custom Payload Codec	
Item	**Description**
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てください。
Description	このペイロードコーデックの説明を入力してください。
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てください。
Payload Decoder Function	デバイスのペイロードデコーダーをカスタマイズし、16進形式のデータをJSON形式に変換します。 なお、関数のヘッダーはblanks上の例と同じである必要があります。
Payload Encoder Function	デバイスのペイロードエンコーダをカスタマイズし、JSON形式のメッセージを16進形式のコマンドに変換します。関数ヘッダーは、空白欄の例と同じであることにご注意ください。
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関数をカスタマイズしてください。以下の2つの追加方法を提供します： **JSON Function**：関数をJSON形式で追加します。 **Page Configuration**：ページ経由で関数を追加します。
Test	ペイロードコーデックテストの有効化または無効化。 **Input**：空白を含まない16進形式の生のデータ、またはJSON形式のコマンドを入力してください。 **fPort**：LoRaWAN®デバイスのアプリケーションポートです。Milesightデバイスではデフォルトで85となります。 **Decoder** ：16進形式の生のデータをJSON形式の結果に変換します。 **TestEn**：JSON形式のコマンドを16進形式のコマンドに変換します。 **Decoder/Encoder Test Result**：デコードまたはエンコードされた結果を表示します。 **Object Mapping Test Result**：エンコーダーまたはデコーダーにおけるオブジェクトの有効性を確認します。

表 3-2-2-8 カスタムペイロードコーデックパラメータ

Note:

1. ペイロードデコーダーおよびエンコーダーで対応しているJavaScriptのバージョンはES2020です。
2. 同一ペイロードコーデックのデコーダーおよび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、同一である必要があります。

Object Mapping Function -JSON Function Example:

```
{
  "object": [
    {
      "id": "ipso_version",
      "name": "IPSO Version",
      "value": "",
      "unit": "",
      "access_mode": "R",
      "data_type": "TEXT",
      "value_type": "STRING",
      "max_length": 6,
      "bacnet_type": "character_string_value_object",
      "bacnet_unit_type_id": 95,
      "bacnet_unit_type": "UNITS_NO_UNITS"
    },
        {
      "id": "temperature_unit",
      "name": "Temperature Unit",
      "value": "",
      "unit": "",
      "access_mode": "RW",
      "data_type": "ENUM",
      "value_type": "UINT8",
      "values": [
        { "value": 0, "name": "celsius" },
        { "value": 1, "name": "fahrenheit" }
      ],
      "bacnet_type": "multistate_value_object",
      "bacnet_unit_type_id": 95,
      "bacnet_unit_type": "UNITS_NO_UNITS",
      "reference": ["temperature_control_mode", "temperature_target"]
    }
```

```
    ]
}
```

<table>
<tr><th colspan="2">Object Mapping Function-JSON Configuration</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>id</td><td>この値は、デコーダーおよびエンコーダーの変数名と一致している必要があります。</td></tr>
<tr><td>name</td><td>必要に応じて空白のままにするか、内容をカスタマイズしてください。</td></tr>
<tr><td>value</td><td>未使用です。空欄のままにしてください。</td></tr>
<tr><td>unit</td><td>空欄のままにするか、必要に応じて単位を入力してください。</td></tr>
<tr><td>access_mode</td><td>このオブジェクトのアクセスモードを設定します。対応するModbusレジスタタイプは以下の通りです：
<table>
<tr><th>Option</th><th>Description</th><th>Modbus Register Type</th></tr>
<tr><td>R</td><td>読み取り専用</td><td>ディスクリート入力、入力レジスタ</td></tr>
<tr><td>W</td><td>書き込み専用</td><td>コイル、保持レジスタ</td></tr>
<tr><td>RW</td><td>読み書き</td><td>コイル、保持レジスタ</td></tr>
</table></td></tr>
<tr><td>data_type</td><td>この変数の値のタイプを定義します。対応するオプション：
<table>
<tr><th>Option</th><th>Description</th><th>Modbus Register Type</th></tr>
<tr><td>TEXT</td><td>文字列型のデータ、例：シリアル番号</td><td>入力レジスタ、保持レジスタ</td></tr>
<tr><td>NUMBER</td><td>数値型データ（整数および浮動小数点を含む）、例：温度</td><td>入力レジスタ、保持レジスタ</td></tr>
<tr><td>BOOL</td><td>0とIのみのステータス、例：ボタンの状態</td><td>離散入力、コイル</td></tr>
<tr><td>ENUM</td><td>複数値</td><td>入力レジスタ、保持レジスタ</td></tr>
</table>
Note:データ型がENUMで、参照パラメータが空白でない場合、Modbusレジスタタイプを"Input Register"または"Holding Register"に設定することをお勧めいたします。</td></tr>
<tr><td>value_type</td><td>対応するオプション：UINT8、INT8、UINT16、INT16、UINT32、INT32、FLOAT、STRING。</td></tr>
<tr><td>values</td><td>この変数の値の範囲を設定します。</td></tr>
<tr><td>max_length</td><td>値のタイプが STRING の場合、文字列の最大長または Modbus レジスタの最大長を設定します。</td></tr>
<tr><td>bacnet_type</td><td>対応しているオプション：
アナログ値オブジェクト、アナログ入力オブジェクト、アナログ出力オブジェクト、バイナリ値オブジェクト、バイナリ入力オブジェクト、バイナリ出力オブジェクト、マルチステート値オブジェクト、マルチステート入力オブジェクト、マルチステート出力オブジェクト</td></tr>
<tr><td>bacnet_unit_type_id</td><td>こちらのページで確認できるBACnetユニットIDを入力してください。</td></tr>
<tr><td>bacnet_unit_type</td><td>こちらの説明に記載されているBACnetユニットタイプを入力してください。</td></tr>
</table>

reference	この変数を他の変数と併せて記述する場合は、ここに変数配列を追加してください。

表 3-2-2-9 オブジェクトマッピング関数 - JSON 関数パラメータ

図 3-2-2-11

Object Mapping Function-Page Configuration	
Item	**Description**
Add	新しいオブジェクトを追加します。
Object Name	オブジェクト名を表示します。
Data Type	このオブジェクトのデータ型を表示します。
Numeric Type	データ型が NUMBER の場合、数値型を表示します。
Access Mode	このオブジェクトのアクセスモードを表示します。
Unit	このオブジェクトの単位を表示します。
Reference	このオブジェクトに関連するオブジェクトを表示します。
Operation	: オブジェクトを編集します。 : このオブジェクトを他のオブジェクトに関連付けます。関連付け後は、これらのオブジェクトは一緒に記述される必要があります。 : オブジェクトを削除します。

表 3-2-2-10 オブジェクトマッピング機能 - ページ構成パラメータ

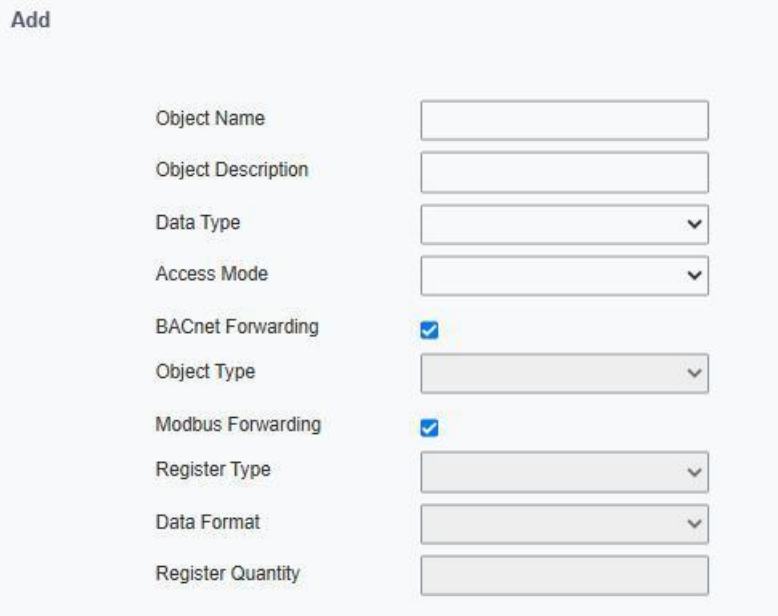


図 3-2-2-12

Object Mapping Function-Add an Object	
Item	**Description**
Object Name	名前はデコーダーまたはエンコーダーの変数名と同一である必要があります。
Object Description	オブジェクトの説明です。
Data Type	このオブジェクトのデータ型です。
Value 0/1	データ型がBOOLの場合、0と1のステータス値を設定します。
EnumerationNumber	データ型が ENUM の場合、対応するオプションの数量を設定します。
Numeric Type	データ型が数値型の場合、数値の型を設定します。
Unit	データ型が NUMBER の場合、オブジェクトの単位を設定します。
Maximum Length	データ型がTEXTの場合、テキストの最大長を設定します。
Access Mode	このオブジェクトのアクセスモードです。
BACnet Forwarding	BACnet オブジェクトパラメータの詳細を表示するには有効にしてください。これらのパラメータは、データ型とアクセスモードに応じて自動的に入力されます。
Modbus Forwarding	Modbus オブジェクトパラメータの詳細を表示するために有効にします。これらのパラメータは、データ型とアクセスモードに応じて自動的に入力されます。

表 3-2-2-11 オブジェクトマッピング機能 - オブジェクトパラメータの追加

3.2.2.4 Profiles

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ネットワークサーバーが必要とするデバイスの機能と起動パラメータを定義します。これらの情報要素は、エンドデバイスメーカーによって提供される必要があります。UG67 には 8 つのデバイスファイルが事前設定されており、ユーザー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。

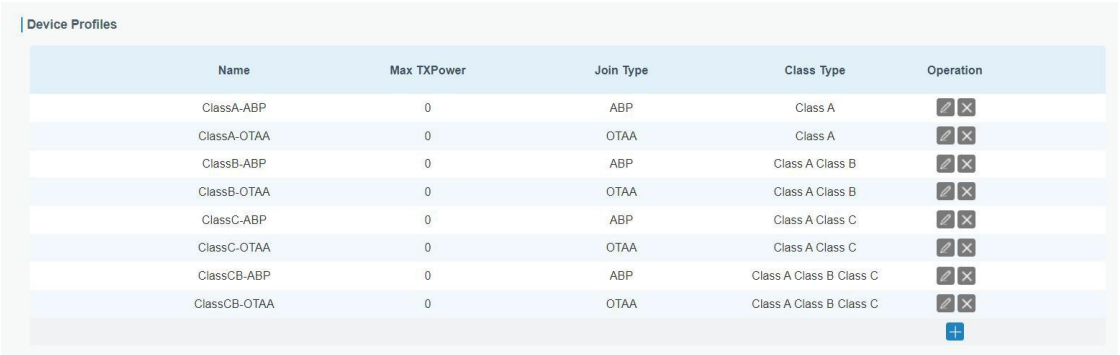


図 3-2-2-13

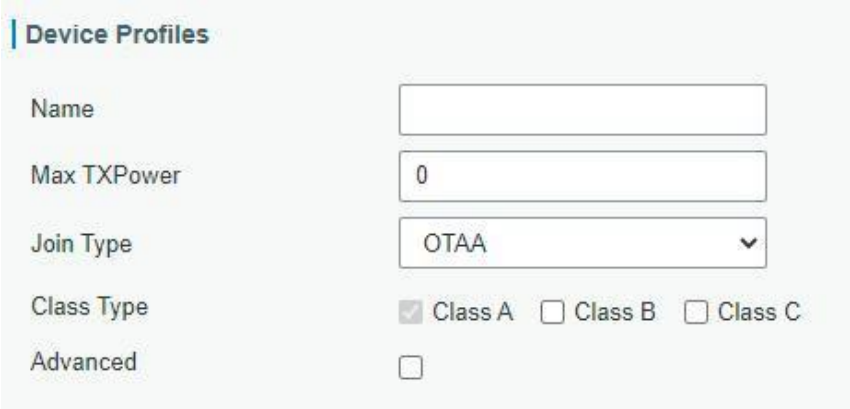


図 3-2-2-14

Device Profiles Settings	
Item	**Description**
Name	デバイスプロファイルの名前を入力してください。
Max TXPower	最大送信電力を入力してください。 TXPowerは、端末機器の最大EIRPレベルに対する電力レベルを示します。0は最大EIRPを使用していることを意味します。EIRPとは等方放射等価電力（Equivalent Isotropically Radiated Power）を指します。
Join Type	「OTAA」および「ABP」から選択してください。
Class Type	クラスAは有効に固定されています。クラスBまたはクラスCのチェックボックスを選択することで、クラスタイプを追加できます。 注記：クラスBを使用する場合**Packet Forwarder > Advanced**においてビーコン周期をゼロ以外の値に設定する必要があります。

表 3-2-2-12 デバイスプロファイル設定パラメータ

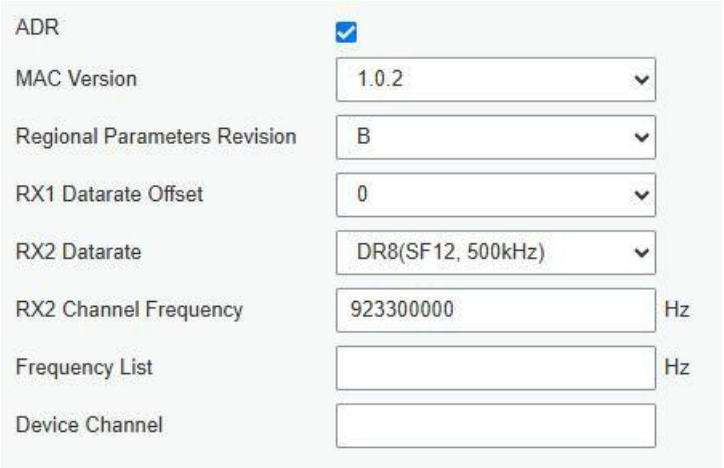


図 3-2-2-15

Device Profile Advanced Settings		
Item	**Description**	**Default**
ADR	エンドデバイスのデータレートを調整するためのゲートウェイネットワークサーバーを有効または無効にします。	Enable
MAC Version	エンドデバイスが対応するLoRaWAN®のバージョンを選択します。	1.0.2
Regional Parameter Revision	エンドデバイスが対応する地域パラメータ文書の改訂版。	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です。	LoRaWAN® 地域パラメータ文書で規定されている内容に基づきます。
RX2 Datarate	RX2 受信ウィンドウに使用される RX2 データレートを入力してください。	
RX2 Channel Frequency	RX2受信ウィンドウに使用されるRX2チャンネル周波数。	
Frequency List	工場出荷時設定の周波数リストです。範囲はLoRaWAN®地域パラメータ文書で規定されている内容に基づいています。	Null
Device Channel	チャンネルインデックスを入力して、このデバイスの周波数チャンネルを変更してください。設定すると、グローバルチャンネルよりも優先されます。この設定は、CN470/US915/AU915 ゲートウェイでのみ有効です。	Null
PingSlot Period	PingSlot を開く期間です。	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。	対応している周波数に基づきます
PingSlot Freq	ダウンリンクを受信するノードの周波数。	対応している周波数に基づきます
ACK Timeout	ダウンリンク送信の承認にかかる時間です。 このオプションはクラス B およびクラス C にのみ適用されます。	Class B: 10 Class C: 10

表 3-2-2-13 デバイスプロファイルの詳細設定パラメータ

3.2.2.5 Device

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を指します。

図 3-2-2-16

Item	Description
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。 **Note:**テンプレートファイルの表の見出し行は削除しないでください。各行には各デバイスの情報が含まれています。
Delete All	リスト内のすべてのデバイスを削除します。
Export All	すべてのデバイス情報をCSVファイルとしてエクスポートします。
Device Name	デバイスの名称を表示します。
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	デバイスの使用済みペイロードコーデックを表示します。詳細を確認するにはクリックしてください。
Application	デバイスのアプリケーション名を表示します。
Last Seen	最後に受信したパケットの時刻を表示します。
Status	デバイスのステータスを表示します。 **Never activated:** デバイスがネットワークに参加したことがなく、パケットを送信したこともありません。 **Offline:** デバイスはタイムアウト時間内にパケットを送信しませんでした。 **Online:** デバイスはタイムアウト時間内にパケットを送信しました。
Operation	デバイスの編集または削除を行います。

表 3-2-2-14 デバイスパラメータ

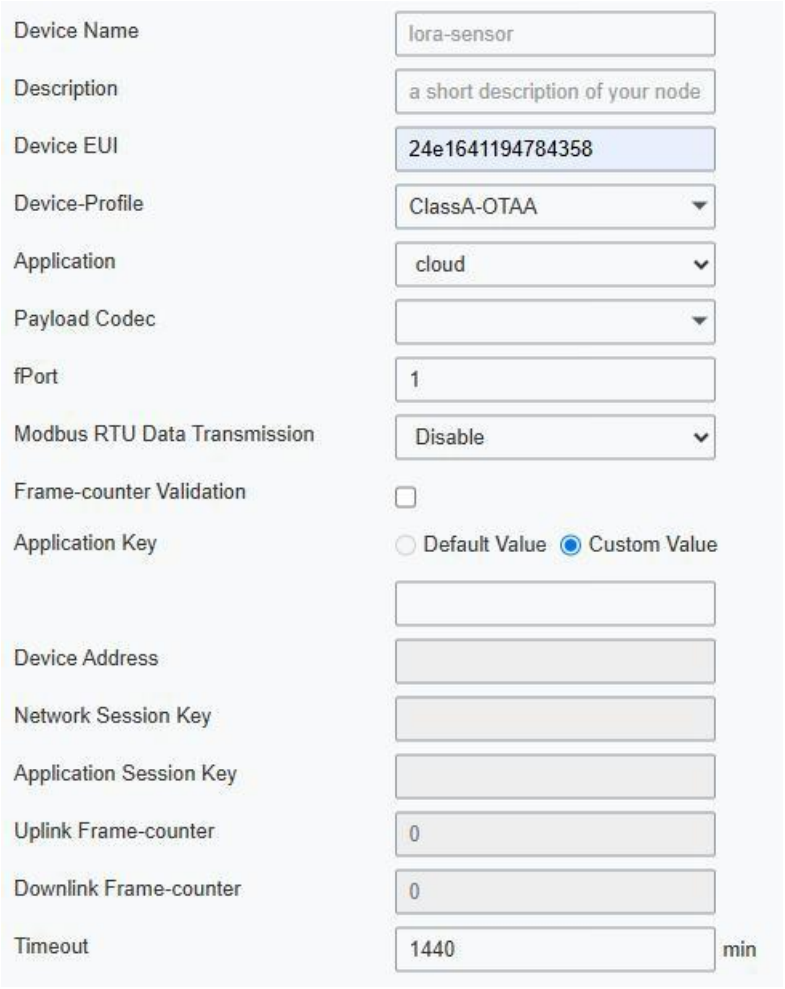


図 3-2-2-17

Device Configuration	
Item	**Description**
Device Name	このデバイスの名前を入力してください。
Description	こちらのデバイスの説明を入力してください。
Device EUI	こちらのデバイスのEUIを入力してください。
Device-Profile	デバイスプロファイルをお選びください。
Application	アプリケーションプロファイルをお選びください。
Payload Codec	ペイロードコーデックページに存在する**Payload Codec** コーデックをお選びください。
fPort	デバイスのダウンリンクポートを入力してください。Milesight デバイスではデフォルトで 85 です。
Modbus RTU Data Transmission	以下のいずれかを選択してください："Disabled"、"Modbus RTU to TCP"、"Modbus RTU over TCP"。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クライアントがModbus TCPコマンドを送信し、コントローラのModbusデータを要求できます。 **Modbus RTU over** TCPクライアントがModbus RTUコマンドを送信し、コントローラのModbusデータを要求できます。
Modbus RTU Fport	Milesight LoRaWAN® コントローラーとUG67間の透過伝送用に、LoRaWAN® フレームポートを入力してください。範囲：2～84、86～223。

	注記：この値は、Milesight LoRaWAN® コントローラの Fport と同一である必要があります。
TCP Port	TCP クライアントと UG67（TCP サーバーとして）間のデータ伝送用の TCP ポートを入力してください。範囲：1～65535。
Frame-Counter Validation	フレームカウンタの検証を無効にすると、リプレイ攻撃が可能になるため、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によるアクティベーションでネットワークに参加する際、アプリケーションキーを使用してアプリケーションセッションキーが導出されます。 **Default Value:** Milesight エンドデバイスのデフォルト値は 5572404C696E6B4C6F52613230313823 です。 **Custom Value:** エンドデバイスに応じてアプリキーを定義してください。
Device Address	デバイスアドレスは、現在のネットワーク内でエンドデバイスを識別します。
Network Session Key	ネットワークセッションキーは端末固有のものです。端末はこれを使用して、すべてのアップリンクデータメッセージのMIC（メッセージ整合性コード）またはその一部を計算し、データの完全性を確保します。
Application Session Key	AppSKeyは、端末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端末の両方で使用され、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の暗号化および復号化を行います。
Uplink Frame-counter	ネットワークサーバーへアップリンクで送信されたデータフレームの数を示します。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。ユーザーは、個人用エンドデバイスを手動でリセットすることが可能です。その場合、当該エンドデバイス上のフレームカウンタおよび当該エンドデバイスに対応するネットワークサーバー上のフレームカウンタは、0にリセットされます。
Downlink Frame-counter	ネットワークサーバーからエンドデバイスのダウンリンクで受信したデータフレームの数です。ネットワークサーバーによって増加します。ユーザーは個人用エンドデバイスを手動でリセットすることができ、その場合、当該エンドデバイス上のフレームカウンタと、そのエンドデバイスに対応するネットワークサーバー上のフレームカウンタは共に0にリセットされます。
Timeout	デバイスのオンライン/オフライン状態を判定する時間。範囲：1～4320 分

表 3-2-2-15 デバイス設定パラメータ

Related Configuration Example

デバイス設定

3.2.2.6 FUOTA

Firmware Update Over the Air（FUOTA）は、ユニキャストまたはマルチキャストを使用してエンドデバイスにファームウェアの更新を配布するための規格です。

Before using this feature, ensure the end device supports the standard LoRaWANLoRaWAN®FUOTA protocol.対応していることをご確認ください。

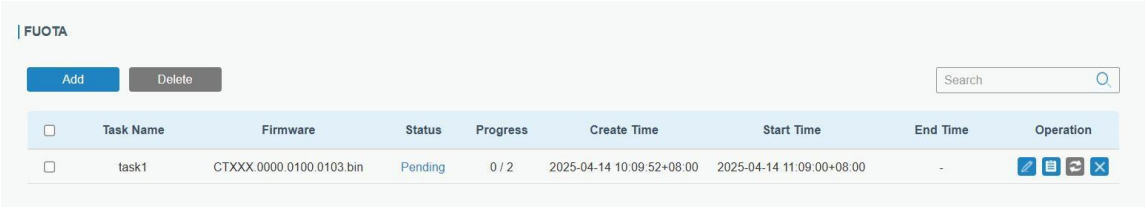


図 3-2-2-18

FUOTA	
Item	**Description**
Add	タスクを追加するにはクリックしてください。
Delete	タスクリストのチェックボックスにチェックを入れ、クリックするとこれらのタスクを削除できます。
Task Name	タスク名です。
Firmware	このタスクでアップグレードするファームウェアです。
Status	タスクの状態。 **Pending:** タスクを処理する予定の時刻をお待ちください。 **Waiting:** アップグレードセッションの作成準備中です。 **Executing:** 少なくとも1台のデバイスがアップグレード結果を返信しています。**Finished:** すべてのデバイスが成功またはフェイルを含むアップグレード結果を返信しました。
Progress	正常にアップグレードされた／アップグレードが予定されているデバイスの数。
Create Time	このタスクを作成した時刻。
Start Time	このタスクを開始する時刻です。
End Time	このタスクを完了する時間です。
Operation	タスクのステータスが保留中の場合に、このタスクを編集してください。 : タスクの詳細を確認してください。各デバイスの成功・フェイルステータスを含みます。 タスクステータスが完了の場合、アップグレードでフェイルしたデバイスに対してタスクを再実行してください。 : タスクステータスが保留中または完了中の場合、このタスクを削除してください。

表 3-2-2-16 FUOTA パラメータ

Add FUOTA Tasks

1. **Add**ボタンをクリックして、FUOTA タスクを追加します。
2. タスク設定を構成します。

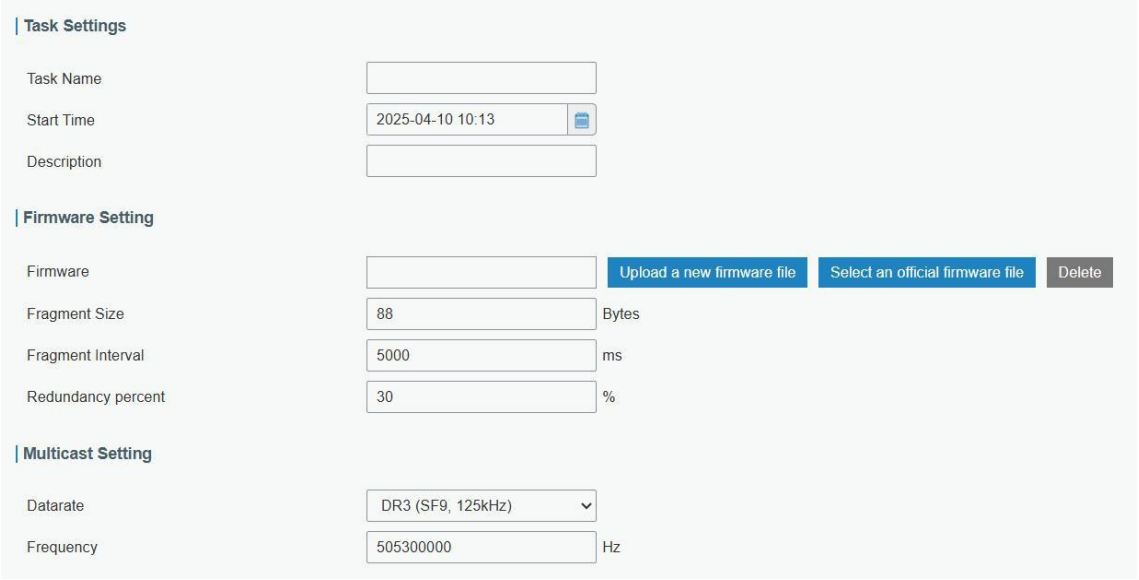
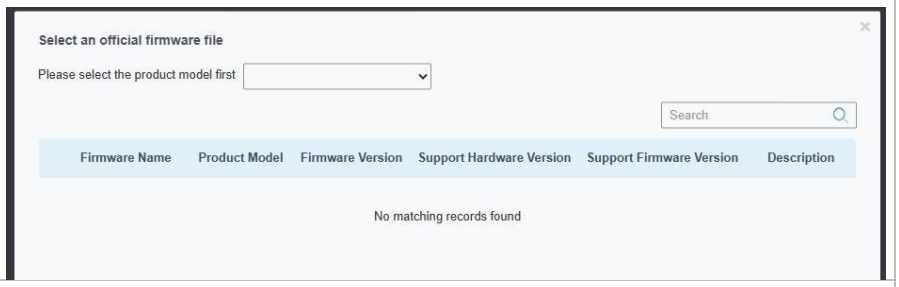


図 3-2-2-19

Add Task Settings	
Item	**Description**
Basic Information	
Task Name	タスク名をカスタマイズします。
Start Time	このタスクを開始する時刻を設定します。
Description	このタスクの説明を入力してください。
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てください。 **Upload a new firmware file:** ローカルからファームウェアをインポートします。 **Select an**まず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お選びください。インターネットにアクセスするにはゲートウェイが必要です 
Fragment Size	ファームウェアファイルはこのサイズに分割され、各デバイスに割り当てられます。通常はデフォルト値のままにしておいてください。 ネットワーク環境が複雑または不安定な場合は、この値を**64**またはそれ以下に減らすことをお勧めいたします。ネットワーク環境が良好な場合は、この値を増やして転送速度を向上させることが可能です。
Fragment Interval	デバイスにファームウェアの断片を割り当てる間隔です。通常はデフォルト値のままにしておいてください。 ネットワーク環境が複雑または不安定な場合、この値を**7**～**10**秒以上に増やすことをお勧めいたします。ネットワーク環境が良好な場合、この値を減らすことで伝送速度を向上させることが可能です。

Redundancy Percent	デバイスはファームウェアファイルのパケット補正のために30%の冗長パケットを送信します。通常はデフォルト値のままにしておいてください。ネットワーク環境が複雑または不良な場合、伝送成功率を向上させるため、この値を40～50%以上に増やすことをお勧めします。ネットワーク環境が良好な場合、この値を減らすことができます。
Multicast Settings	
Datarate	デバイスに割り当てるファームウェアフラグメントのデータレートです。
Frequency	デバイスにファームウェアフラグメントを割り当てるダウンリンクの周波数です。

表 3-2-2-17 タスクパラメータ

3. このタスクを実行するデバイスを選択してください。同じモデルのデバイスを選択してください。

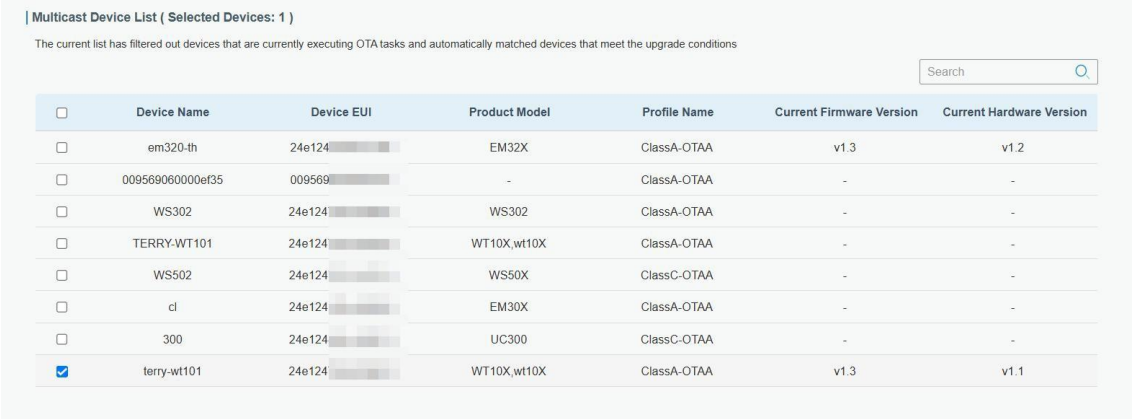
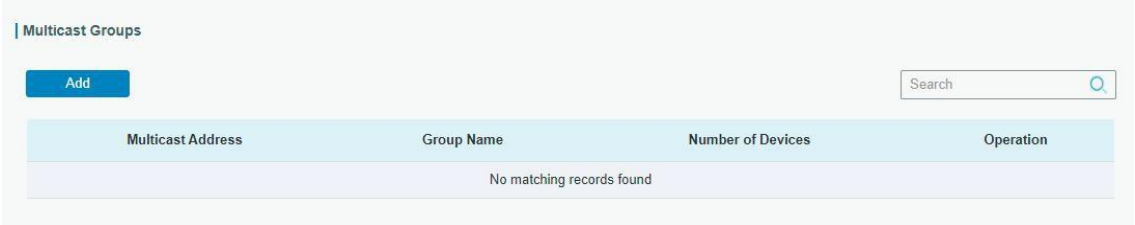


図 3-2-2-20

4. **Save**をクリックして、これらのタスク設定を保存してください。

3.2.2.7 Multicast Groups

Milesightゲートウェイは、エンドデバイス群へダウンリンクメッセージを送信するためのクラスBまたはクラスCマルチキャストグループの作成に対応しております。



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、確認付きダウンリンク、MACコマンドは対応しておりません。

図 3-2-2-21

Item	Description
Add	マルチキャストグループを追加します。

Group Name	グループの名称を表示します。
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を編集または削除します。

表 3-2-2-18 マルチキャストグループパラメータ

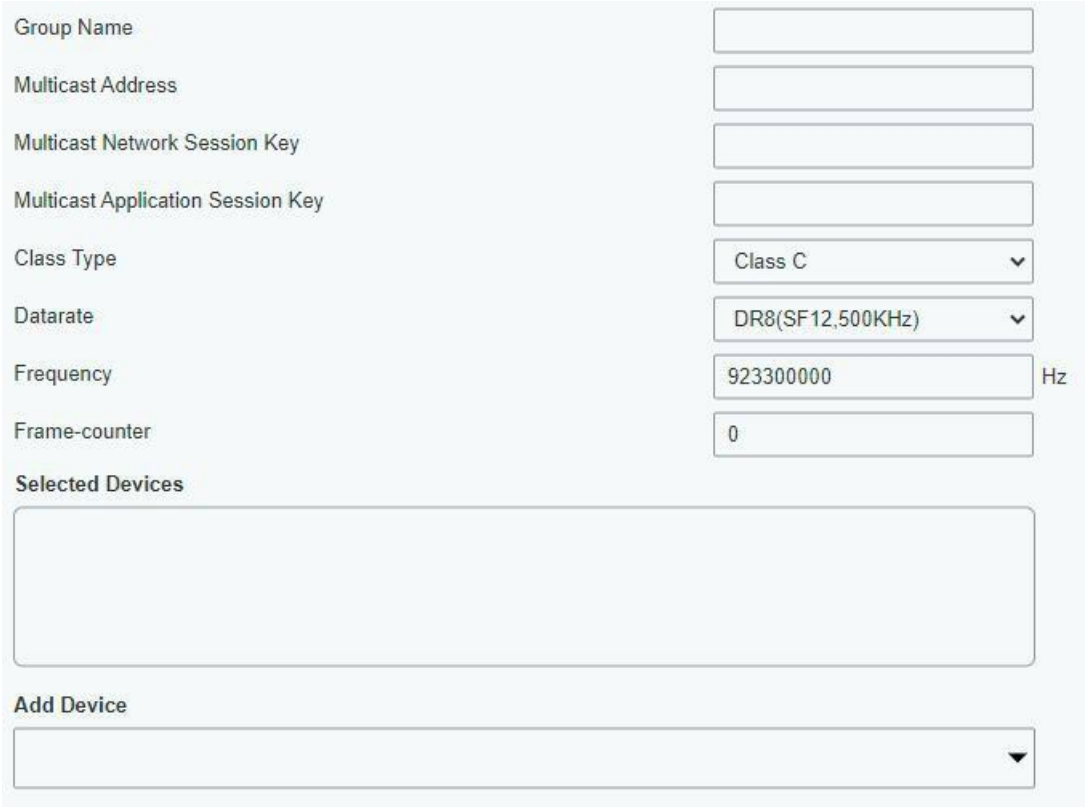


図 3-2-2-22

Multicast Group Configuration	
Item	**Description**
Group Name	このマルチキャストグループの名前を入力してください。
Multicast Address	このグループ内の全デバイスのデバイスアドレス（Dev Addr）です。
Multicast NetworkSession Key	このグループ内の全デバイスのネットワークセッションキー（Netwks Key）です。
Multicast ApplicationSession Key	このグループ内の全デバイスにおけるアプリケーションセッションキー（AppSKey）です。
Class Type	クラス B およびクラス 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データレート
Frequency	このグループ内の全デバイスのダウンリンク周波数です。
Frame-counter	ネットワークサーバーからエンドデバイスのダウンリンクが受信したデータフレームの数です。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です。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 3-2-2-19 マルチキャストグループ設定パラメータ

3.2.2.8 Gateway Fleet

Milesightゲートウェイは、ゲートウェイネットワークサーバーに接続できます。1つのゲートウェイは最大100台のゲートウェイに対応できます。

図 3-2-2-23

Item	Description
Gateway ID	ゲートウェイIDを表示します。
Name	ゲートウェイの名称を表示します。
Status	ゲートウェイの接続状態を表示します。
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 3-2-2-20 ゲートウェイフリートパラメータ

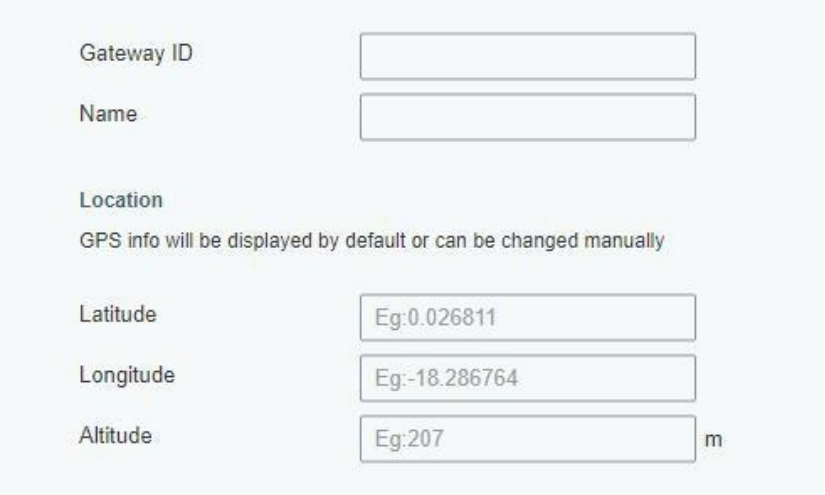


図 3-2-2-24

Item	Description
Gateway ID	ゲートウェイを識別するための一意のゲートウェイIDを入力してください。
Name	このゲートウェイの名前を入力してください。
Location	ゲートウェイのGPSデータはここで編集できます。ゲートウェイがGPSデータを送信した場合、カスタマイズしたデータは上書きされます。

表 3-2-2-21 ゲートウェイ設定パラメータ

3.2.2.9 Packets

ゲートウェイは、最新の 1000 個のパケットを表示し、デバイスにコマンドを送信する機能を対応しております。

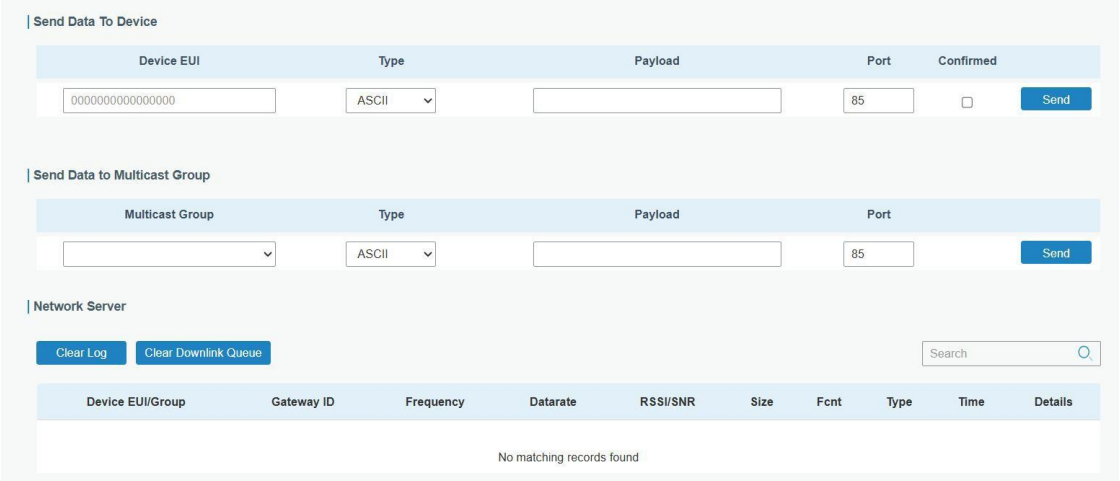


図 3-2-2-25

Send Data To Device/Multicast Group	
Item	**Description**
Device EUI	ペイロードを受信するデバイスの EUI を入力してください。
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てください。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種類をお選びください：ASCII、Hex、base64。
Payload	このデバイスに送信するメッセージを入力してください。
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てください。
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対して"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 3-2-2-22 デバイスへのデータ送信パラメータ

Network Server	
Item	**Description**
Clear Log	ネットワークサーバーに送信されたパケットログをクリアします。
Clear Downlink Queue	デバイスに送信されていないダウンリンクキューをクリアします。
Device EUI/Group	デバイスの EUI 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されている周波数を表示します。
Datarate	パケット送信に使用されているデータレートを表示します。
SNR	信号対雑音比を表示します。
RSSI	受信信号強度インジケーターを表示します。
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 - 参加承諾パケット 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 - 要求ネットワークからの ACK 応答 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 - エンドデバイスから のACK応答を要求
Time	パケットが送信または受信された時刻を表示します。

表 3-2-2-23 パケットパラメータ

をクリックすると、パケットの詳細情報を取得できます。以下に示す通りです：

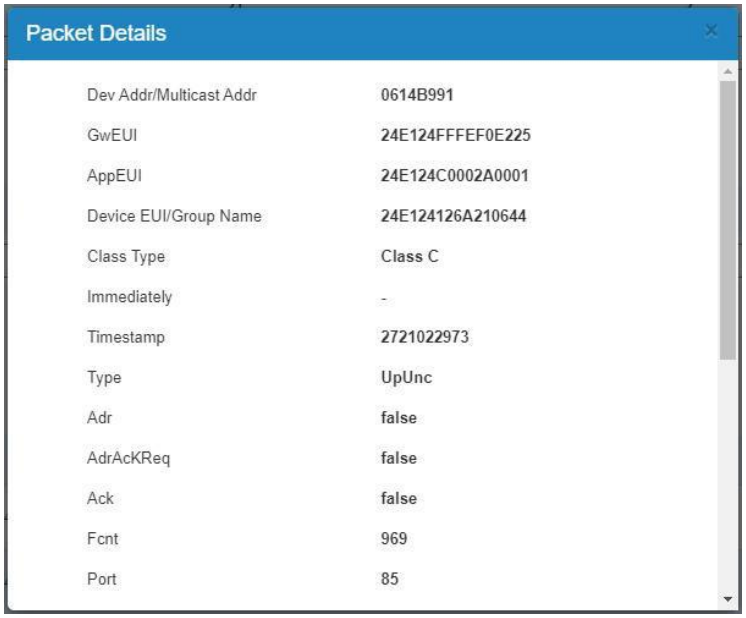


図 3-2-2-26

Item	Description
Dev Addr/Multicast Addr	デバイスのアドレス/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	エンドデバイスのアプリケーション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直ちに送信するかどうか。
Timestamp	パケットフォワーダーの起動後、このパケットを受信するまでの時間を表示します。単位：ミリ秒
Type	パケットの種類を表示します： JnAcc - 参加承諾パケットJnReq - 参加要求パケット UpUnc - 上りリンク未確認パケット UpCnf - 上りリンク確認済みパケット - 要求ネットワークからのACK応答

	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 - エンドデバイスからのACK応答を要求
Adr	True: エンドノードが ADR を有効にしています。 False：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確認するため、ノードは定期的に ADRACKReq メッセージを送信します。これは 1 ビットの長さです。True: ネットワークは、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、ADR_ACK_DELAY 時間で応答する必要があります。 False: ADRが無効になっているか、ネットワークがADR_ACK_DELAY時間内に応答しません。
Ack	True: このフレームは ACK です。 偽：このフレームは ACK ではありません。
Fcnt	このパケットのフレームカウンタを表示します。ネットワークサーバーは、アップリンクのフレームカウンタを追跡し、各エンドデバイスに対してダウンリンクのカウンタを生成します。
FPort	このパケットを送信するFPortです。このパケットがMACコマンドの場合、ポートは0となります。このパケットにアプリケーションデータが含まれる場合、ポートは0以外（1～233）となります。
Modulation	LoRaとは、物理層がLoRa変調方式を採用していることを意味します。
Bandwidth	このチャネルの帯域幅を示します。
SpreadFactor	このチャネルのスプレッドファクターを表示します。
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	このチャンネルの受信感度（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とは、暗号メッセージ整合性コードのことで、MHDR、FHDR、FPort、および暗号化されたFRMPayloadのフィールドに対して計算されます。

表 3-2-2-24 パケットの詳細パラメータ

Related Topic

デバイスへのデータ送信

3.3 Protocol Integration

3.3.1 BACnet Server

UG67はLoRaWAN®からBACnetへのゲートウェイとして機能し、BMSシステムとの容易な統合を可能にします。この機能をご利用になる前に、内蔵ペイロードコーデックライブラリのバージョンが

最新版であることを確認し、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ご確認ください。

3.3.1.1 Server

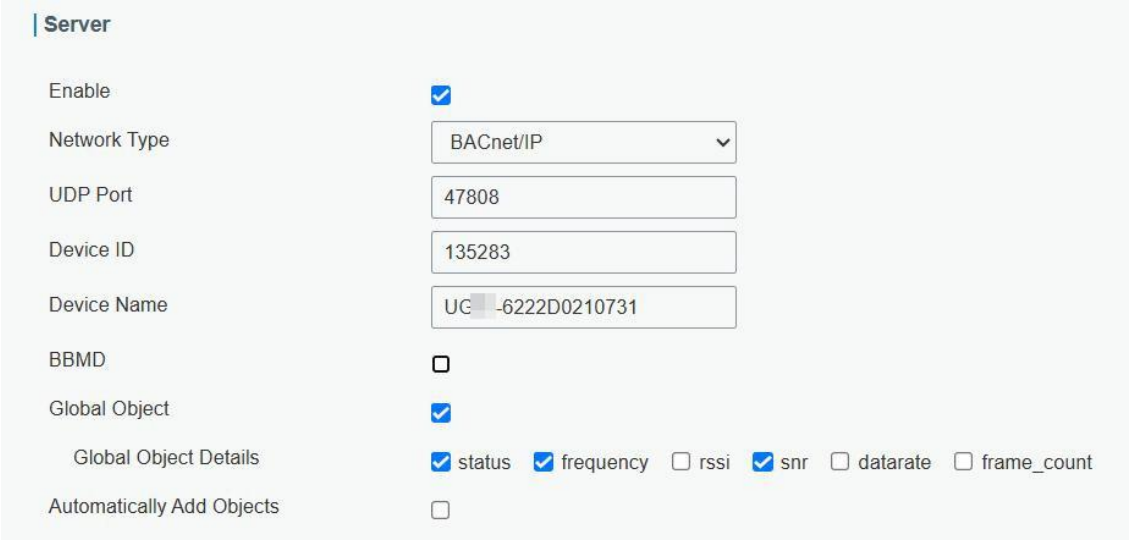


図 3-3-1-1

Server Settings	
Item	**Description**
Enable	BACnet サーバー機能を有効または無効にします。
Network Type	ネットワークタイプをBACnet/IPまたはBACnet/SCから選択してください。
Device ID	このゲートウェイのBACnetデバイスIDです。BACnetネットワーク上で一意である必要があります。
Device Name	BACnetネットワーク内でデバイスを表す固有の名前です。
Global Object	有効化後、ゲートウェイは各デバイスに対して自動的にグローバルオブジェクトを追加します。このオプションが無効化されていない限り、これらのグローバルオブジェクトを削除することはできません。 **Status:** デバイスのオンライン/オフライン **Frequency**：デバイスのアップリンク周波数 RSSI：デバイスのアップリンク受信感度 **SNR**: デバイスのアップリンクSNR **Datarate**：デバイスのアップリンクデータレート **Frame_count**: デバイス上りリンクフレームカウント (FCNT)
AutomaticallyAdd Objects	有効化後、ゲートウェイはネットワークサーバーにデバイスを追加する際に、ペイロードコーデックに基づいて自動的にオブジェクトを追加します。

表 3-3-1-1 サーバーパラメータ

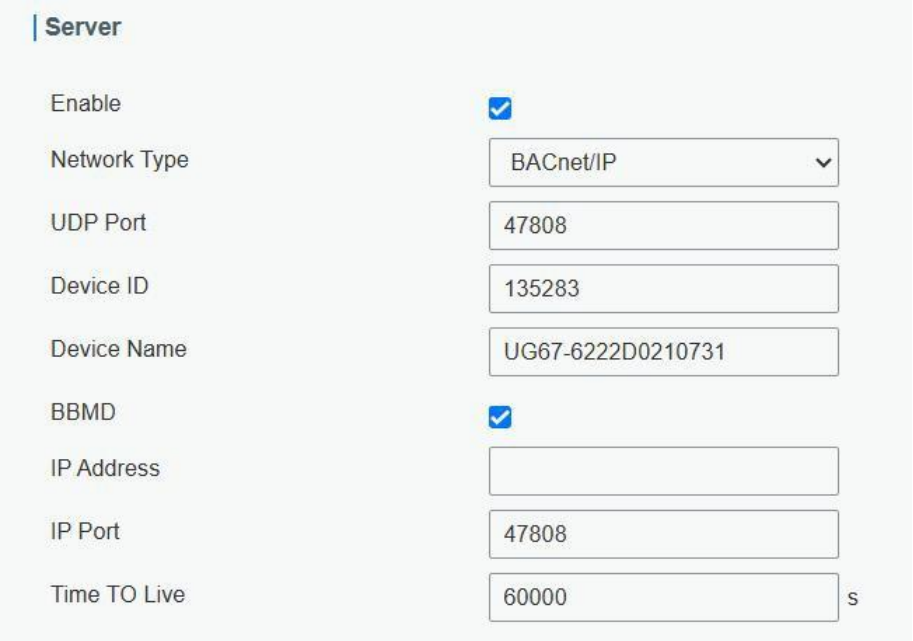


図 3-3-1-2

Server-BACnet/IP Settings	
Item	**Description**
UDP Port	BACnet/IP の通信ポートを設定します。範囲：1～65535。 デフォルトのポートは 47808 です。
BBMD	異なるネットワークサブネットの BACnet デバイスを連携させる必要がある場合、BBMD（BACnet/IP ブロードキャスト管理デバイス）を有効にしてください。 **IP** ：BBMD デバイスまたは外部デバイスレジストラの IP アドレスを入力してください。 **IP Port**：外部デバイス登録用の UDP/IP ポートを入力してください。 **Time TO Live**：外部デバイス登録に使用される秒数です。

表 3-3-1-2 サーバー-BACnet/IP パラメータ

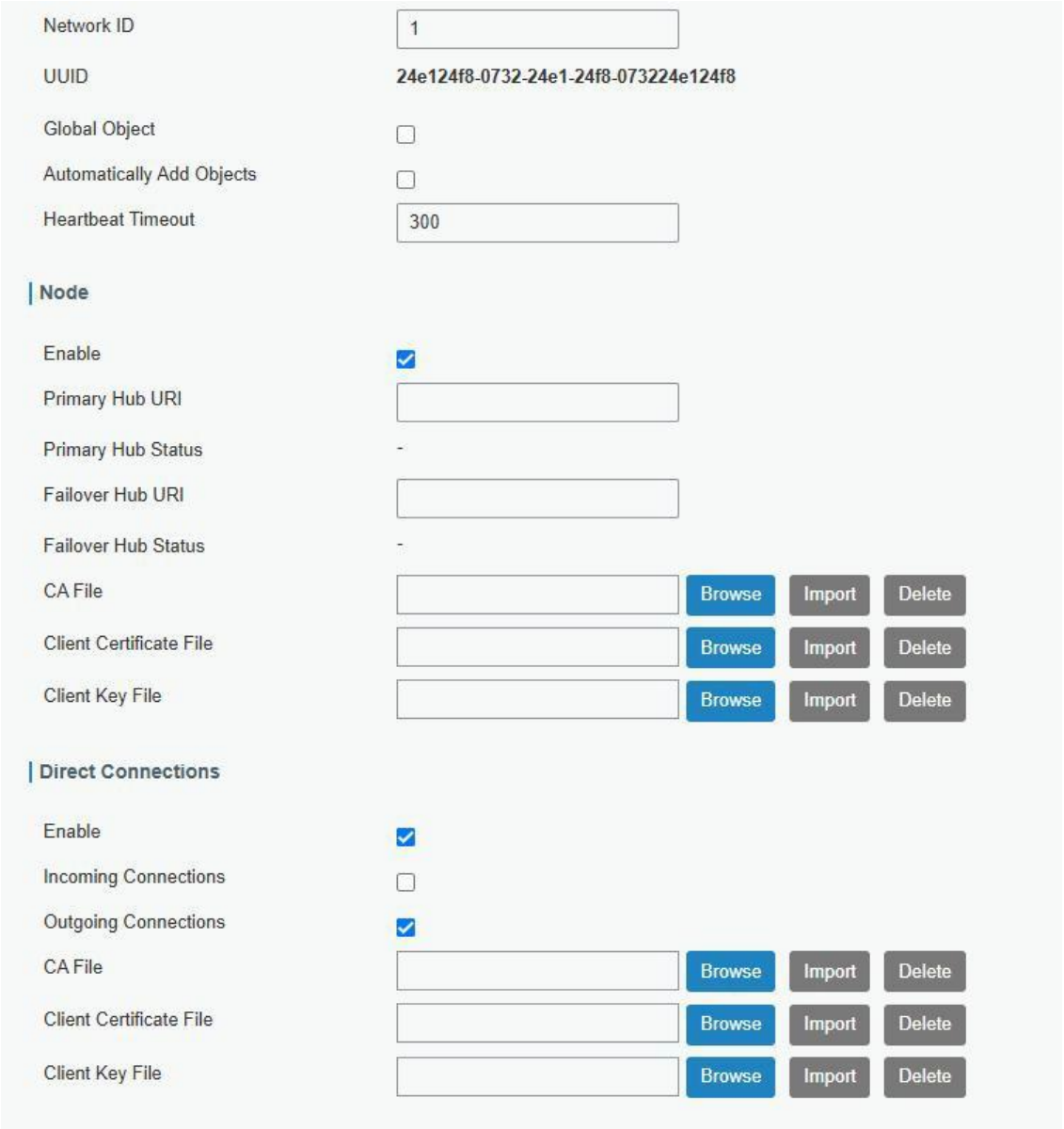


図 3-3-1-3

Server-BACnet/SC Settings	
Item	**Description**
Network ID	ネットワークを識別するためのネットワークIDを設定してください。同じネットワークIDを持つデバイス間のみが、ルーティングなしで相互に通信できます。
UUID	BACnet/SC ネットワークにおけるゲートウェイの UUID を表示します。
HeartbeatTimeout	ハブまたはノードにハートビートパケットを送信する間隔を設定します。
Node	
Enable	ノードとして動作するかどうかを設定します。
Primary Hub URI	プライマリハブのURIを設定します。URI形式（アドレスはIPまたはドメイン名）：*wss://アドレス:ポート*
Primary HubStatus	ノードとプライマリハブ間の接続状態を表示します。
Failover Hub URI	ノードがプライマリハブへの接続にフェイルした場合のフェイルオーバーハブのURIを設定します。

Failover Hub Status	ノードとフェイルオーバーハブ間の接続状態を表示します。URI 形式（アドレスは IP またはドメイン名）：*wss://アドレス:ポート*
CA File Client Certificate File Client Key File	「**Browse** をクリックしてローカルパスからファイルを選択し、「**Import** をクリックしてファイルをアップロードしてください。
Direct Connections	
Enable	他のノードとの直接接続を設定するには、有効または無効に設定してください。
Incoming Connections	他のノードからの接続を有効または無効にします。最大10ノードまでこのゲートウェイに接続できます。 **Port Number:** 接続を許可するポート番号を設定してください。 **CA File/Server Certificate File/Server Key File: Browse** をクリックし、ローカルパスからファイルを選択した後、**Import** をクリックしてファイルをアップロードしてください。**Device ID:** ゲートウェイに接続するノードデバイスIDを表示します。 **UUID:** ゲートウェイに接続するノードデバイスのUUIDを表示します。 **VMAC:** ゲートウェイに接続するノードデバイスのVMACを表示します。 **Status:** ゲートウェイとノード間の接続状態を表示します。
Outgoing Connections	他のノードへの接続を有効または無効にします。ゲートウェイは最大10台のノードに接続できます。 **CA File/Client Certificate File/Client Key File: Browse** をクリックしてローカルパスからファイルを選択し、**Import** をクリックしてファイルをアップロードします。 **Name:** 接続するノードの名前を設定します。 **URI:** 接続するノードのURIを設定します。URI形式（アドレスはIPまたはドメイン名）：*wss://アドレス:ポート* **Status:** ゲートウェイとノード間の接続状態を表示します。

表 3-3-1-3 サーバー-BACnet/SC パラメータ

3.3.1.2 BACnet Object

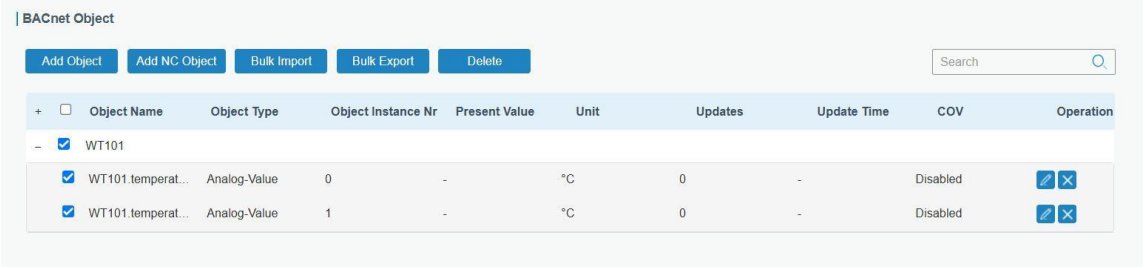


図 3-3-1-2

Item	Description
Add Object	このサーバーに追加する対象オブジェクトを選択するには、クリックしてください。ゲートウェイは最大10,000個のオブジェクト追加に対応しております。

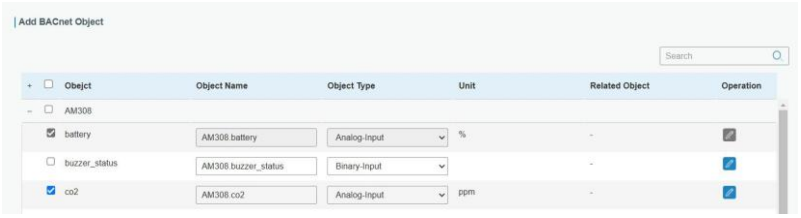
	注ペイロードコーデックの内容が正しいことを確認し、デバイスが正しいペイロードコーデックを選択していることをご確認ください。 
Add NC Object	アラームの受信者を決定するための通知クラス（NC）タイプのオブジェクトを追加します。ゲートウェイは最大200個のNCオブジェクトの追加に対応しています。
Bulk Import	複数のBACnetオブジェクトをインポートするためのテンプレートをダウンロードします。
Bulk Export	ご希望のオブジェクトを選択し、.xlsx形式のファイルとしてエクスポートいたします。
Delete	削除したいオブジェクトを選択してください。
Object Name	BACnet オブジェクトの名称を表示します。
Object Type	この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刻を表示します。
Update time	このオブジェクトがデータを取得および更新した時刻を表示します。
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または削除を行います。

表 3-3-1-2 BACnet オブジェクトリストパラメータ

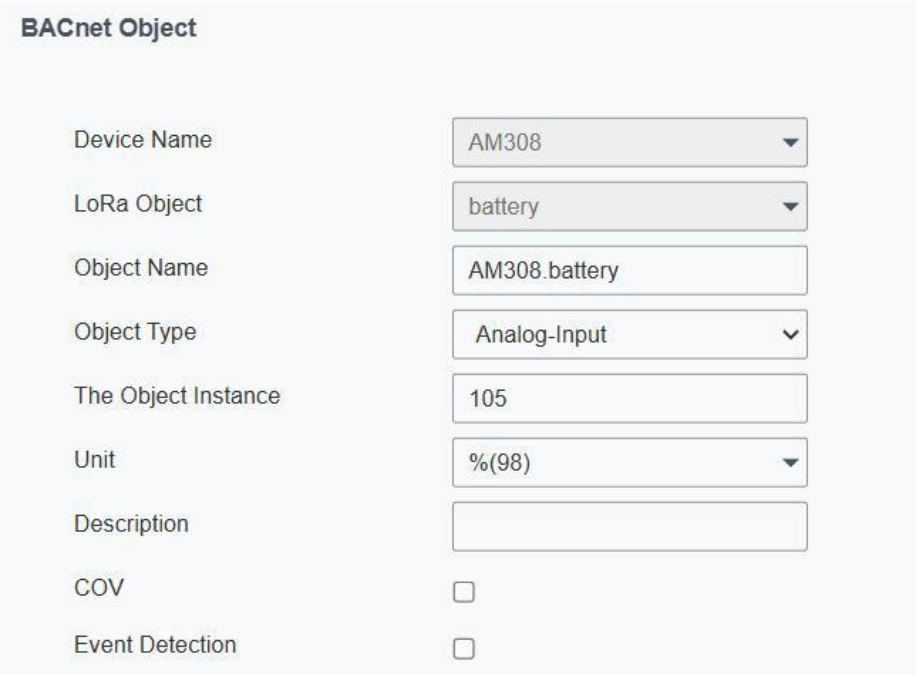


図 3-3-1-3

BACnet Object Configuration

I	Description
Device Name	デバイスの名称を表示します。
LoRa Object	対応するLoRaオブジェクトの名前を表示します。
Object Name	このオブジェクトに固有の名前をカスタマイズします。
Object Type	オブジェクトタイプを、バイナリ入力/出力/値、アナログ入力/出力/値、マルチステート入力/出力/値、および文字列値から選択してください。
The Object Instance	オブジェクトインスタンスをカスタマイズしてください。
Description	このオブジェクトの説明を入力してください。
Event Detection	この値のアラームを報告するには有効にしてください。まず、少なくとも1つの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てください。
COV	オブジェクトの値が変更された場合、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。これは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に達した、または超えた場合にのみ、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リリークデフォルト値に設定されます。
Binary Input/Output/Value	
Polarity	バイナリ入出力のステータスを"Normal"または"Reverse"として定義します。
Active Text	バイナリ型オブジェクトの値のアクティブ状態における意図された効果を特徴付けます。**Example:**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の値の非アクティブ状態における意図された効果を特徴付けます。**Example:**ボタンの場合、非アクティブテキストは"Not Pressed"と定義できます。
Relinquish Default	コマンドが存在しない場合、バイナリ出力はこの放棄デフォルト値に設定されます。
MultiState Input/Output/Value	
Number of States	状態数を設定し、各状態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てください。
Event	報告するイベントの種類を選択してください。
Limit Event	オブジェクトタイプがアナログタイプの場合、上限値または下限値に達した際にイベントを報告するかを選択してください。
Deadband	異常状態下において、現在の値が（上限値－デッドバンド）値または（下限値＋デッドバンド）値に遅延時間持続して戻った場合、装置は正常復帰イベントを生成します。このオプションはアナログタイプのみに適用されます。

Time Delay	現在の値が閾値条件に一致する場合、または今回のみ閾値を超えた場合に限り、デバイスは対応するイベントを報告いたします。
Alarm Value	遅延時間内に現在の値が警報値と等しい場合、「異常」イベントを報告します。遅延時間内に現在の値が警報値と等しくない場合、「正常」イベントを報告します。このオプションは、バイナリ入力、バイナリ値、マルチステート入力、またはマルチステート値のみに適用されます。
Fault Value	現在の値が故障値と等しい場合、"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がこのオプションを有します。
Feedback Value	遅延時間内に現在の値がフィードバック値と等しい場合、異常状態イベントを報告します。遅延時間内に現在の値がフィードバック値と等しくない場合、正常状態イベントを報告します。このオプションはマルチステート出力またはバイナリ出力のみが利用可能です。
Notification Type	通知タイプをアラームまたはイベントから選択してください。

表 3-3-1-3 BACnet オブジェクト設定パラメータ

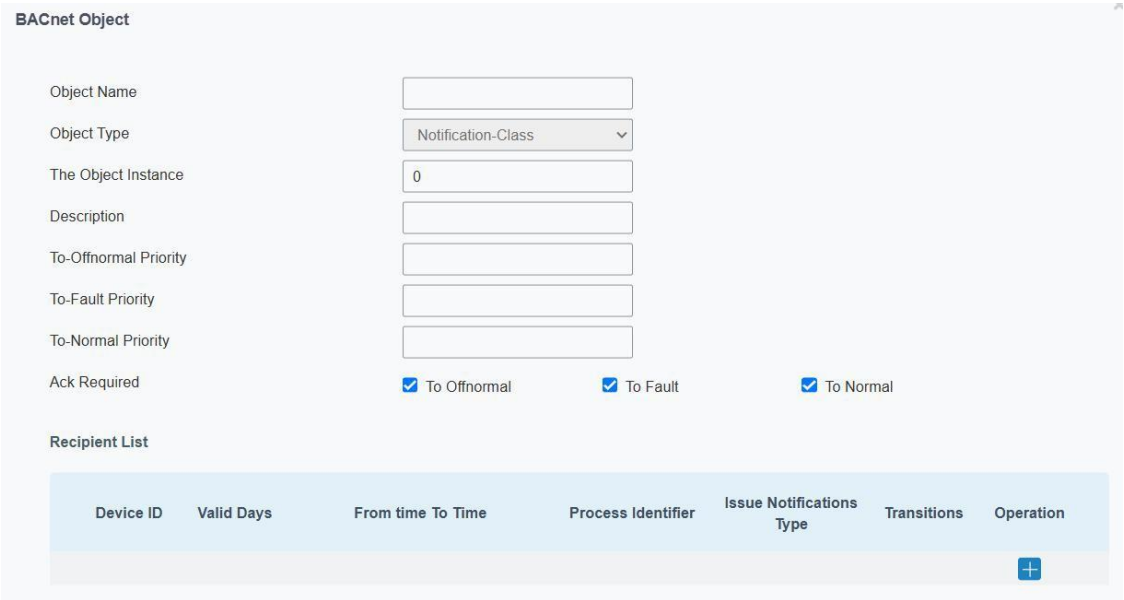


図 3-3-1-4

Notification Class BACnet Object Configuration	
Item	**Description**
Object Name	このオブジェクトに固有の名前をカスタマイズしてください。
Object Type	通知クラスとして固定されています。
The Object Instance	オブジェクトインスタンスをカスタマイズしてください。
Description	このオブジェクトの説明を入力してください。
To-Offnormal	受信者がイベント通知を並べ替える際に使用する優先度番号を設定します。範囲：0～255（0が最も重要、255が最も重要でない）

Priority To-Fault Priority To-NormalPriority	
Ack Required	このイベントにおいて、受信者が確認応答アラームメッセージをゲートウェイに返信する必要があるかどうかを指定してください。
Recipient List	イベント検出が有効化され、この通知クラスが選択された場合、イベント通知は本リストに記載された受信者宛に送信されます。1つのリストは最大10名の受信者を対応できます。 **Device ID:** 通知の受信対象となるデバイスのIDです。 **Valid Days**：通知を送信する有効な期間です。 **From time to time:** 通知を送信する有効な時間帯。 **Process**アラームの対象となるプロセスを示す識別子です。例えば、プロセス識別子1は保守アラーム、2は重大アラーム、3は生命安全アラームなどを意味する場合があります。 **Issue** 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の種類を選択します。

表 3-3-1-4 通知クラス BACnet オブジェクト設定パラメータ

3.3.2 Modbus Server

ゲートウェイはModbusサーバー（スレーブ）として動作し、PLC/BMSシステムからのModbus RTUまたはModbus TCPコマンドを受信し、LoRaWAN®デバイスへの読み書きを行うことが可能です。本機能をご利用になる前に、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版であることを確認し、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ご確認ください。

3.3.2.1 Server

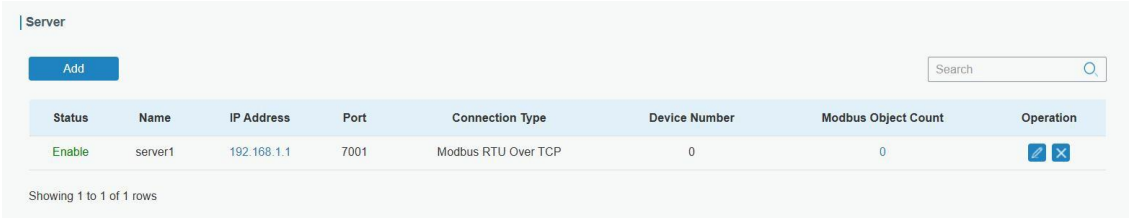


図 3-3-2-1

Item	Description
Add	Modbusサーバー（スレーブ）を追加します。1台のゲートウェイで最大15台のサーバーに対応できます。
Status	このサーバーの有効状態を表示します。
Name	サーバーの名前を表示します。
IP Address	このサーバーのIPアドレスを表示し、クリックすると詳細を確認できます。
Port	このサーバーの通信ポートを表示します。

Connection Type	このサーバーの接続タイプを表示します。
Device Number	このサーバーのデバイス番号を表示します。
Modbus Object Count	このサーバーのModbusオブジェクトの数を表示し、その数をクリックすると詳細を確認できます。
Operation	このサーバーを編集または削除します。

表 3-3-2-1 サーバーパラメータ

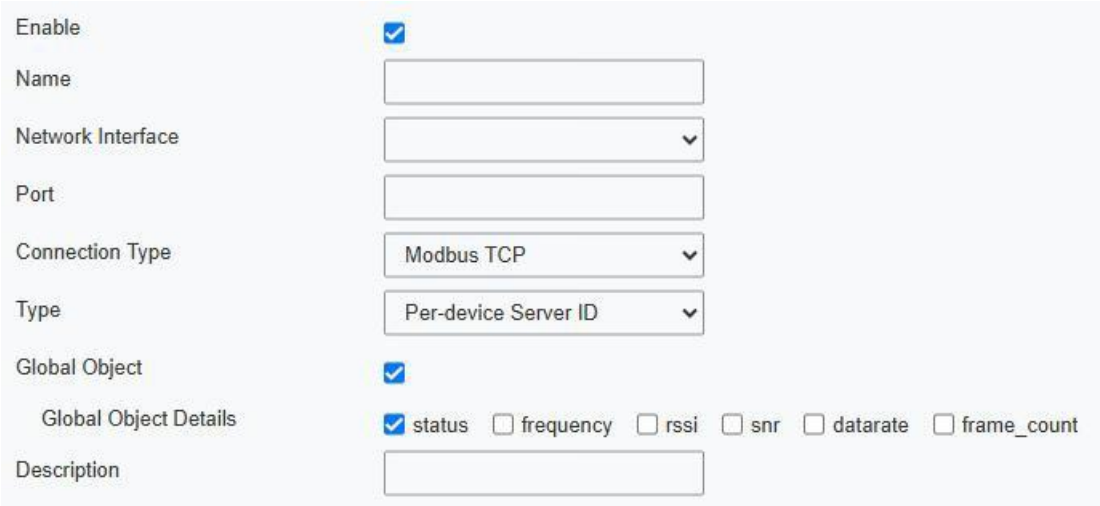


図 3-3-2-2

Server Settings	
Item	**Description**
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一意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ースを選択してください。本デバイスは、異なるリモートプラットフォームとの通信に異なるネットワークインターフェースに対応しております。
Port	本サーバーの通信ポートを設定します。範囲：1～65535。
Connection Type	このサーバーの接続タイプを選択してください。 **Modbus** Modbusクライアントが**Modbus TCP**形式のコマンドをこのModbusサーバーに送信します。 **Modbus RTU over TCP:** Modbusクライアントは、このModbusサーバーに**Modbus RTU**形式のコマンドを送信します。
Type	このModbusサーバーのサーバーIDタイプを設定します。これは、Modbusクライアントが各サーバーを識別するために使用されます。 **No server ID**：すべてのデバイスが任意のサーバーIDを使用します。 **Per-device server ID**：デバイスごとにサーバーIDを設定することを対応します。
Global Object	有効化後、ゲートウェイはすべてのデバイスに対してグローバルオブジェクトを自動的に追加します。このオプションが無効化されない限り、これらのグローバルオブジェクトは削除できません。 **Status:** デバイスのオンライン/オフライン状態 **Frequency**：デバイスのアップリンク周波数

	RSSI: デバイスのアップリンクRSSI **SNR**：デバイスのアップリンクSNR **Datarate**：デバイスのアップリンクデータレート **Frame_count**: デバイスアップリンクフレームカウント (FCNT)
Description	このサーバーの説明を追加してください。

表 3-3-2-2 サーバー設定パラメータ

3.3.2.2 ModbusObject

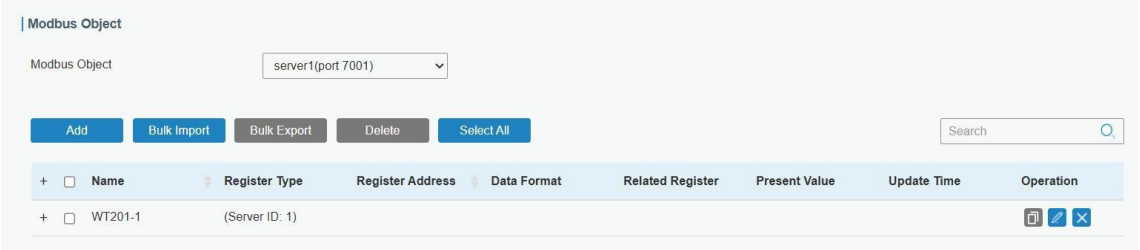
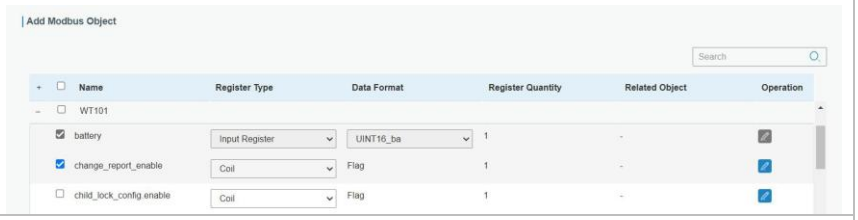


図 3-3-2-3

Item	Description
Modbus Object	オブジェクトを追加および編集する Modbus サーバーを選択します。
Add	このサーバーに追加する対象オブジェクトを選択するには、こちらをクリックしてください。ゲートウェイは最大10,000個のオブジェクト追加に対応しております。 **Note:**ペイロードコーデックの内容が正しいことを確認し、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ご確認ください。 
Bulk Import	複数の Modbus 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	エクスポートしたいオブジェクトを選択し、.xlsx形式のファイルとしてエクスポートしてください。
Delete	削除したいオブジェクトを選択してください。
Select All/DeslectAll	すべてのオブジェクトを選択/選択解除します。
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形式を表示します。
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および更新した時刻を表示します。
Operation	：オブジェクトを編集します。 ：オブジェクトを削除します。 ：コピーが必要なオブジェクトを選択し、このアイコンをクリックすると、他の同一モデルデバイスにオブジェクトを追加または適用します。

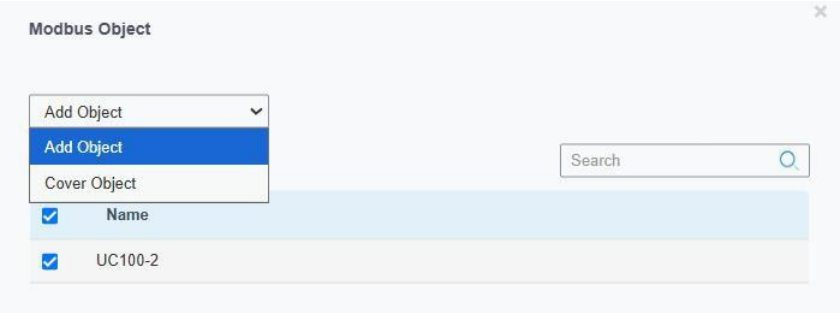
	Add Object：選択したデバイスにオブジェクトを追加します。 **Cover**選択されたデバイスに対してオブジェクトを適用し、選択されたデバイスの元のオブジェクト設定はクリアされます。 

表 3-3-2-3 Modbus オブジェクトリストのパラメータ

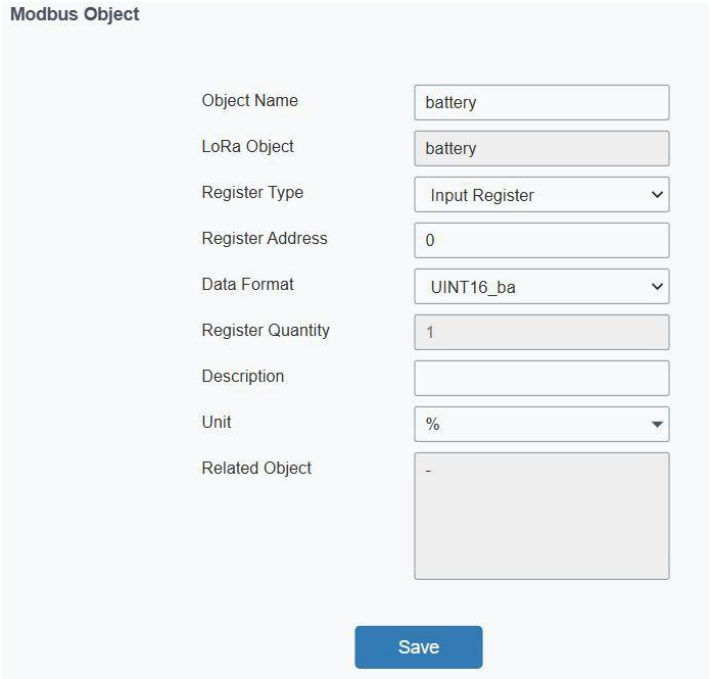


図 3-3-2-4

Modbus Object Configuration	
Item	**Description**
Object Name	このオブジェクトに固有の名前をカスタマイズしてください。
LoRa Object	対応するLoRaオブジェクトの名前を表示します。
Object Name	このオブジェクトに固有の名前をカスタマイズしてください。
Register Type	Modbus レジスタタイプを選択します。 **Discrete Input:** 読み取り専用、0 および I の状態のみを含みます。 **Coil:** 読み書き可能、0とIの状態のみを含みます。 **Holding Register:** 読み書き可能、アナログ値、文字列などを含む。 **Input Register:** 読み取り専用、アナログ値、文字列などを含みます。
Register Address	オブジェクトを追加する際、このアドレスは自動的に生成されます。また、このアドレスは変更に対応しています。範囲：0～65535

	注 1) 同一レジスタタイプのアドレスは、1つのModbusサーバー内で異なる必要があります。 2) アドレスはレジスタ数に関連します。このオブジェクトのアドレスが0でレジスタ数が2の場合、次のオブジェクトのアドレスは2（0+2）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形式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数を表示します。
Description	このオブジェクトの説明を入力してください。
Unit	このオブジェクトの単位を選択してください。
Related Register	関連レジスタを表示します。このオブジェクトを書き込む際には、関連レジスタも同時に書き込む必要があります。そうしない場合、このオブジェクトの変更はフェイルします。

表 3-3-2-4 Modbus オブジェクト構成パラメータ

3.4 Network

3.4.1 Interface

3.4.1.1 Port

イーサネットポートはイーサネットケーブルで接続し、インターネットアクセスが可能です。3種類の接続タイプに対応しています。

- **StaticIP**：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** ：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、自動的にIPアドレスを取得します。
- **PPPoE**：イーサネットWANインターフェースをPPPoEクライアントとして設定します。

図 3-4-1-1

Port Setting		
Item	**Description**	**Default**
Port	eth0 ポートとして固定され、有効化されているポートです。	eth 0
ConnectionType	「Static IP」、「DHCP Client」、「PPPoE」から選択してください。	DHCP
MTU	最大伝送単位を設定してください。	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

Related Configuration Example

イーサネット接続

1. Static IP Configuration

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"モードを選択できます。

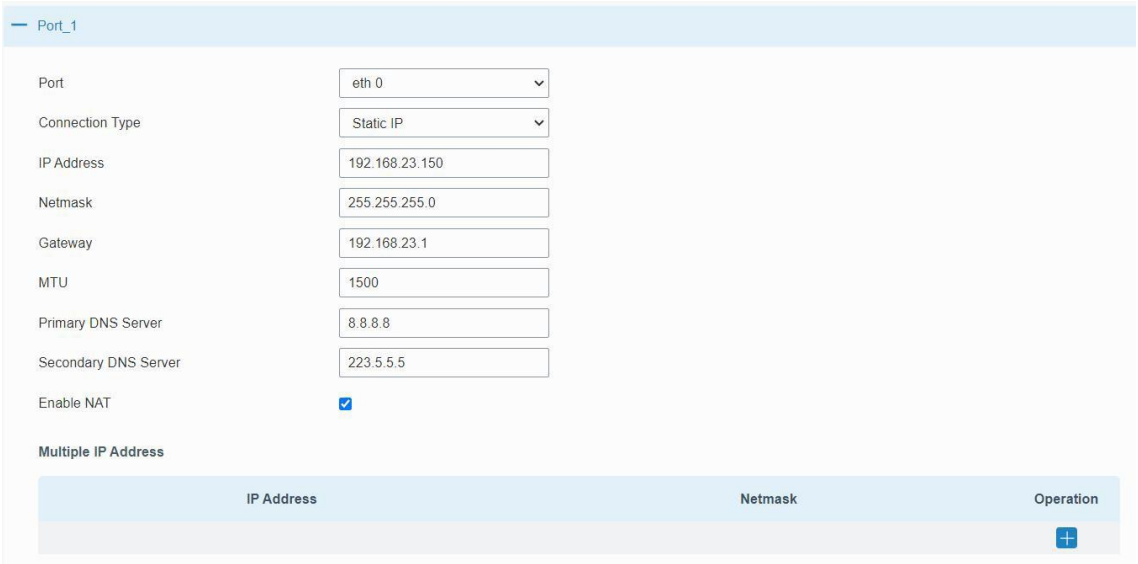


図 3-4-1-2

Static IP		
Item	**Description**	**Default**
IP Address	インターネットにアクセス可能な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複数IPアドレスを設定します。	なし

表 3-4-1-2 固定 IP パラメータ

2. DHCP Client

外部ネットワークで DHCP サーバーが有効化されており、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 Client"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。

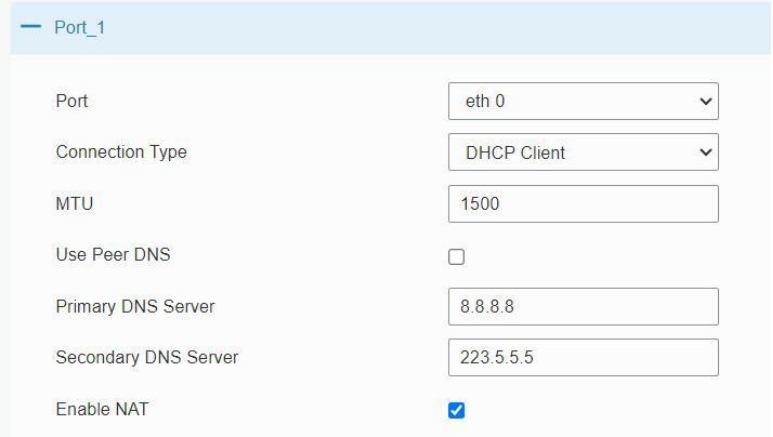


図 3-4-1-3

DHCP Client	
Item	**Description**
Use Peer DNS	PPP接続中にピアDNSを自動的に取得します。ユーザーがドメイン名を訪問する際にはDNSが必要です。

表 3-4-1-3 DHCP クライアントパラメータ

3. PPPoE

PPPoEとは、イーサネット上のポイントツーポイントプロトコルを指します。ユーザーは、元の接続方式に基づいてPPPoEクライアントをインストールする必要があります。PPPoEを利用することで、リモートアクセスデバイスは各ユーザーを管理することが可能となります。

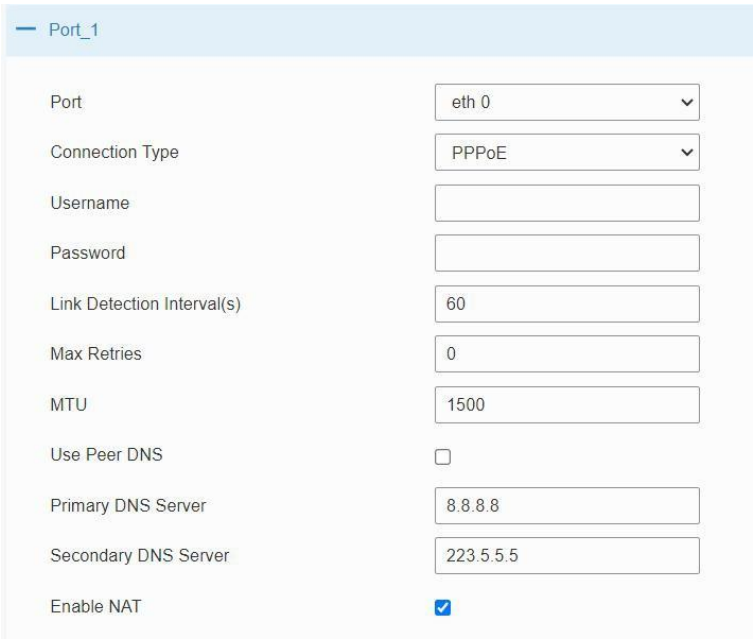


図3-4-1-4

PPPoE	
Item	**Description**
Username	インターネットサービスプロバイダ（ISP）から提供されたユーザー名を入力してください。
Password	ご利用のインターネットサービスプロバイダ（ISP）から提供されたパスワードを入力してください。
Link Detection Interval (s)	リンク検出のためのハートビート間隔を設定してください。範囲：1～600。
Max Retries	ダイヤルアップにフェイルした後の最大再試行回数を設定してください。範囲：0～9。
Use Peer DNS	PPP接続中にピアDNSを自動的に取得します。ユーザーがドメイン名を訪問する際にはDNSが必要です。

表 3-4-1-4 PPPOE パラメータ

3.4.1.2 WLAN

このセクションでは、Wi-Fi ネットワークに関連するパラメータの設定方法について説明します。UG67 は対応しています。

802.11 b/g/n を、AP モードまたはクライアントモードでサポートしております。

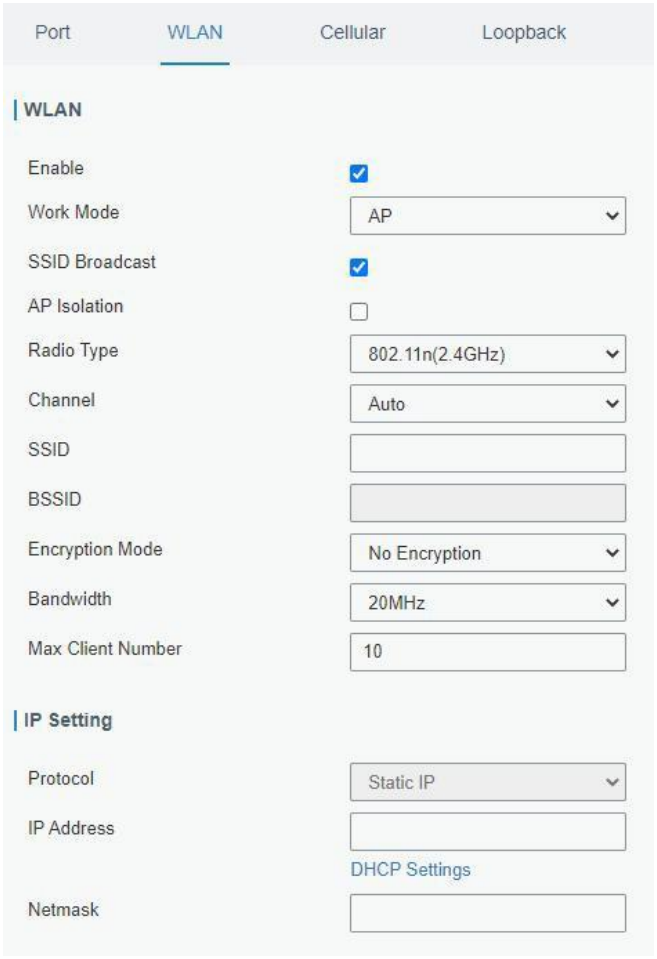


図 3-4-1-5

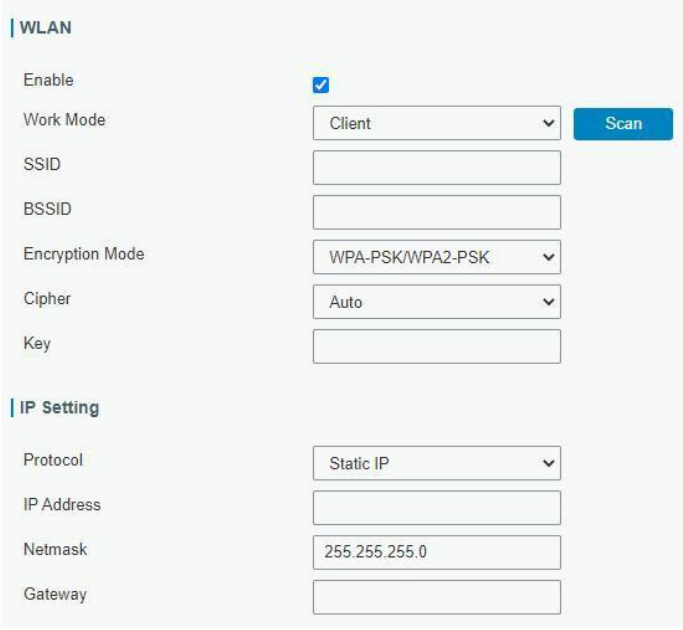


図 3-4-1-6

WLAN Settings	
Item	**Description**
Enable	WLAN を有効/無効にします。

Work Mode	ゲートウェイの動作モードを選択します。オプションは"Client"または「AP」です。
BSSID	アクセスポイントのMACアドレスを入力してください。ネットワークに接続するには、SSIDまたはBSSIDのいずれかを入力できます。
SSID	アクセスポイントのSSIDを入力してください。
Client Mode	
Scan	"Scan"ボタンをクリックして、近くのアクセスポイントを検索してください。
Encryption Mode	暗号化モードを選択してください。オプションは"No Encryption"、"WEP Open System"、"WEP Shared Key"、「WPA-PSK」、「WPA2-PSK」、「WPA-PSK/WPA2-PSK」、"WPA-Enterprise"、"WPA2-Enterprise"、"WPA-Enterprise/WPA2-Enterprise"です。
Cipher	暗号化方式を選択します。オプションは"Auto"、「AES」、「TKIP」、「AES/TKIP」です。
Key	WEP/WPA 暗号化の前もって共有された鍵を入力してください。
XSupplicant Type	「Peap」、「Leap」、「TLS」、「TTLS」から選択してください。
User	WPA/WPA2-Enterprise のユーザーを入力してください。
AnonymousIdentity	WPA/WPA2-Enterprise の匿名識別情報を入力してください。
Phase2	WPA/WPA2-Enterprise のフェーズ2 を入力してください。
Public ServerCertificate	WPA/WPA2-Enterprise アクセスポイントとの認証に使用されるパブリックサーバー証明書です。
AP Mode	
SSID Broadcast	SSIDのブロードキャストが無効化されている場合、他の無線機器はSSIDを検出できません。そのため、ユーザーは無線ネットワークにアクセスするために手動でSSIDを入力する必要があります。
AP Isolation	AP分離が有効になっている場合、APにアクセスするすべてのユーザーは、相互に通信できない状態で分離されます。
Radio Type	無線タイプを選択してください。オプションは「802.11b (2.4 GHz)」、「802.11g (2.4 GHz)」、および「802.11n (2.4 GHz)」です。
Channel	無線チャネルを選択します。オプションは"Auto"、「1」、「2」……「11」です。
Encryption Mode	暗号化モードを選択します。オプションは"No Encryption"、「WEP オープンシステム」、「WEP 共有キー」、「WPA-PSK」、「WPA2-PSK」、「WPA-PSK/WPA2-PSK」です。
Cipher	暗号化方式を選択してください。選択肢は"Auto"、「AES」、「TKIP」、「AES/TKIP」です。
Key	WPA暗号化用の事前共有キーを入力してください。デフォルトのパスワードは「**iotpassword**です。
Bandwidth	帯域幅を選択してください。選択肢は「20MHz」と「40MHz」です。
Max Client Number	ゲートウェイをアクセスポイントとして設定した場合にアクセス可能なクライアントの最大数を設定します。
IP Setting	
Protocol	無線ネットワークにおけるプロトコルを設定します。
IP Address	無線ネットワークにおけるIPアドレスを設定します。
Netmask	無線ネットワークでネットマスクを設定します。

Gateway	無線ネットワークのゲートウェイを設定します。

表 3-4-1-5 WLAN パラメータ

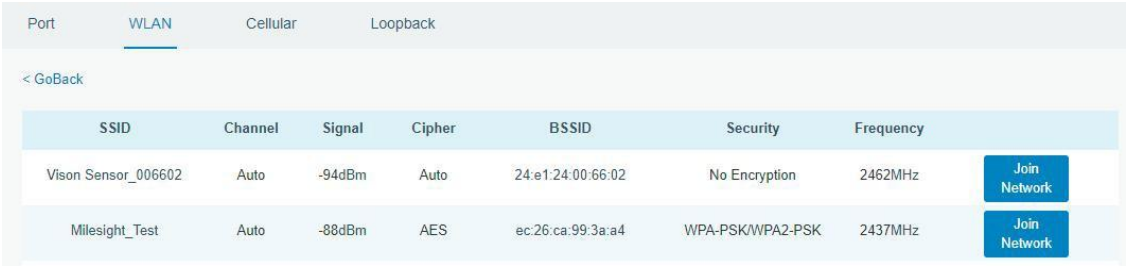


図 3-4-1-7

Client Mode-Scan	
SSID	SSID を表示します。
Channel	無線チャネルを表示します。
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	ボタンをクリックして、無線ネットワークに接続してください。

表 3-4-1-6 WLAN スキャンパラメータ

Related Topic

Wi-Fi アプリケーションの例

3.4.1.3 Cellular (Cellular Version Only)

このセクションでは、セルラーネットワークに関連するパラメータの設定方法について説明します。

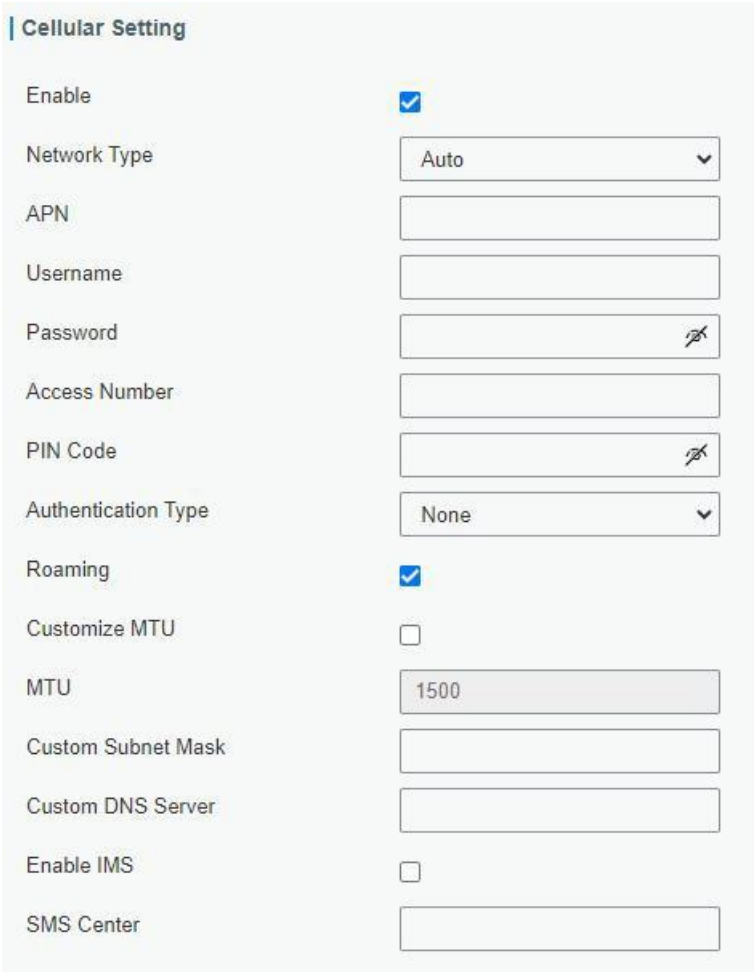


図 3-4-1-8

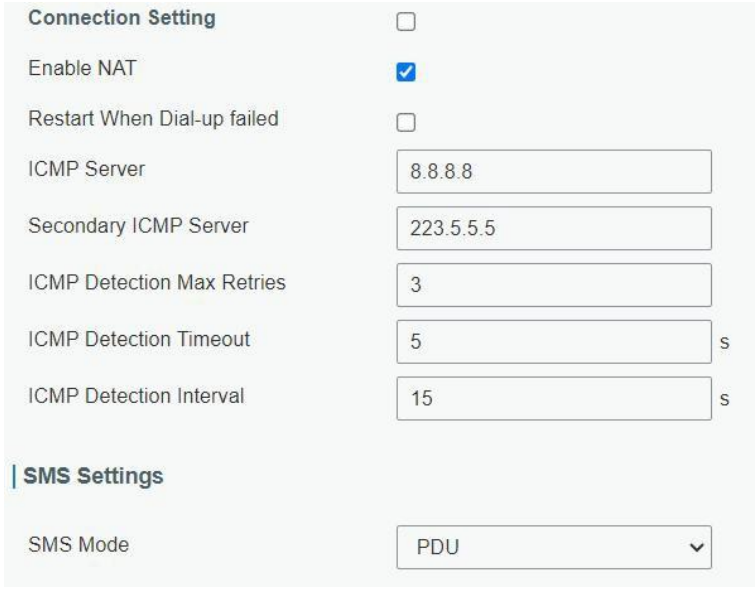


図 3-4-1-9

General Settings	
Item	**Description**
Enable	このオプションをチェックすると、セルラー機能が有効になります。

Network Type	"Auto"、"Auto 3G/4G"、"4G Only"、"3G Only"から選択してください。 自動：最も強い信号の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	お住まいの地域のインターネットサービスプロバイダ（ISP）が提供する、携帯電話ダイヤルアップ接続用のアクセスポイント名（APN）を入力してください。
Username	お住まいの地域のインターネットサービスプロバイダ（ISP）から提供された、携帯電話ダイヤルアップ接続用のユーザー名を入力してください。
Password	お住まいの地域のインターネットサービスプロバイダー（ISP）が提供する、携帯電話ダイヤルアップ接続用のパスワードを入力してください。
Access Number	お使いの地域ISPが提供する携帯電話ダイヤルアップ接続用のダイヤルアップセンター番号を入力してください。
PIN Code	SIMロックを解除するための4～8桁のPINコードを入力してください。
Authentication Type	"None"、「PAP」、「CHAP」から選択してください。
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（MTU）をカスタマイズする機能を有効または無効にします。無効の場合、デバイスは通信事業者の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	セルラー用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。 **Note:** この機能は一部のセルラーモジュールでのみ対応しています。
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てください。
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、ダイヤルアップが数回フェイルした場合、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。 **Note:** ping 検出が許可されているかどうか、また正しい ICMP サーバーのアドレスについては、ISP にお問い合わせください。ping 検出が許可されていない場合は、このサーバーの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検出がフェイルした場合の最大再試行回数を設定します。
ICMP Detection Timeout	ICMP検出のタイムアウトを設定します。
ICMP Detection Interval	ICMP検出の間隔を設定します。
SMS Mode	SMSモードを「TEXT」と「PDU」から選択してください。

表 3-4-1-7 携帯電話パラメータ

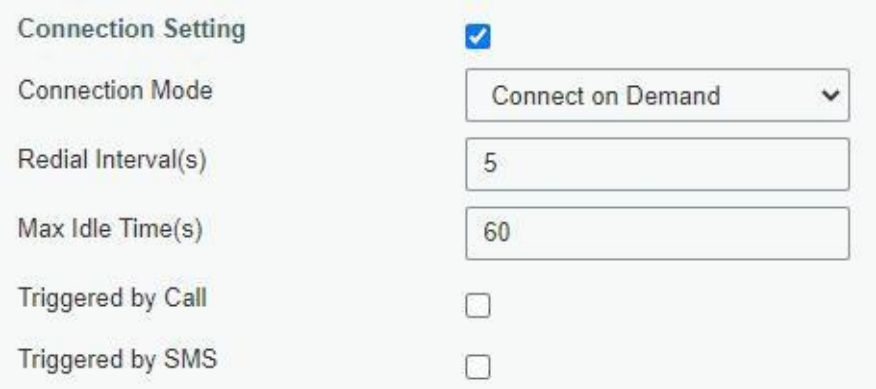


図 3-4-1-10

Item	Description
Connection Mode	
Connection Mode	"Always Online"と"Connect on Demand"から選択してください。
Redial Interval(s)	再ダイヤル間の時間間隔を設定します。範囲：0～3600。
Max Idle Time(s)	現在のリンクがアイドル状態にある場合のゲートウェイの最大継続時間を設定します。範囲：10～3600。
Triggered by Call	特定の電話番号からの着信を受信した場合、ゲートウェイは自動的にオフラインモードから携帯電話ネットワークモードに切り替わります。
Call Group	通話トリガー用の通話グループを選択してください。**System > General Settings > Phone** で電話グループを設定してください。
Triggered by SMS	特定の携帯電話から特定の SMS を受信すると、ゲートウェイはオフラインモードから携帯電話ネットワークモードに自動的に切り替わります。
SMS Group	トリガー用のSMSグループを選択してください。**System > General**＞電話設定に移動し、SMSグループを設定してください。 **Settings > Phone** を設定してください。
SMS Text	トリガーとなるSMSの内容を入力してください。

表 3-4-1-8 携帯電話パラメータ

Related Topics

携帯電話接続アプリケーションの例

電話グループ

3.4.1.4 Loopback

ループバックインターフェースは、アクティブ化されている限り、ゲートウェイの ID を置き換えるために使用されます。インターフェースがダウンしている場合、ゲートウェイの ID を再度選択する必要があり、その結果、OSPF の収束時間が長くなります。したがって、ゲートウェイの ID としてループバックインターフェースを使用することをお勧めいたします。

ループバックインターフェースは、ゲートウェイ上の論理的かつ仮想的なインターフェースです。デフォルトの状態では、ゲートウェイ上にループバックインターフェースは存在しませんが、必要に応じて作成することができます。

図 3-4-1-11

Loopback		
Item	**Description**	**Default**
IP Address	変更不可	127.0.0.1
Netmask	変更不可	255.0.0.0
Multiple IPAddresses	上記のIPアドレスとは別に、ユーザーは他の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

3.4.1.5 VLAN Trunk

UG67ゲートウェイは、イーサネットポートがVLANトランククライアントとして

動作し、VLAN IDを割り当てられることを対応しております。これにより、トラフィックの分類が容易になります。VLAN IDを設定した場合、**[Network] > [Interface] > [Port]** のポートは、eth0.x（xはVLAN ID）として選択可能です。VLAN設定は、のデフォルトでは空白となっております。特定のインターフェースに新しいVLANラベルを追加するには、[ ]をクリックしてください。

図 3-4-1-12

VLAN Trunk	
Item	**Description**
Interface	VLAN インターフェースを選択してください。デフォルトでは eth0 に固定されています。
VID	VLAN のラベル ID を設定します。範囲：1～4094。

表 3-4-1-10 VLAN トランクパラメータ

3.4.2 Firewall

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バインディングなどの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、パケットの内容特性（プロトコルスタイル、送信元/宛先 IP アドレスなど）に基づいて、

インターネットからローカルエリアネットワークへ）および退出方向（ローカルエリアネットワークからインターネットへ）において、プロトコルスタイル、送信元/宛先IPアドレスなどのパケットの内容特性に基づいて対応する制御を実行します。これにより、ゲートウェイが安全な環境で動作し、ローカルエリアネットワーク内のホストが保護されることを保証します。

3.4.2.1 Security

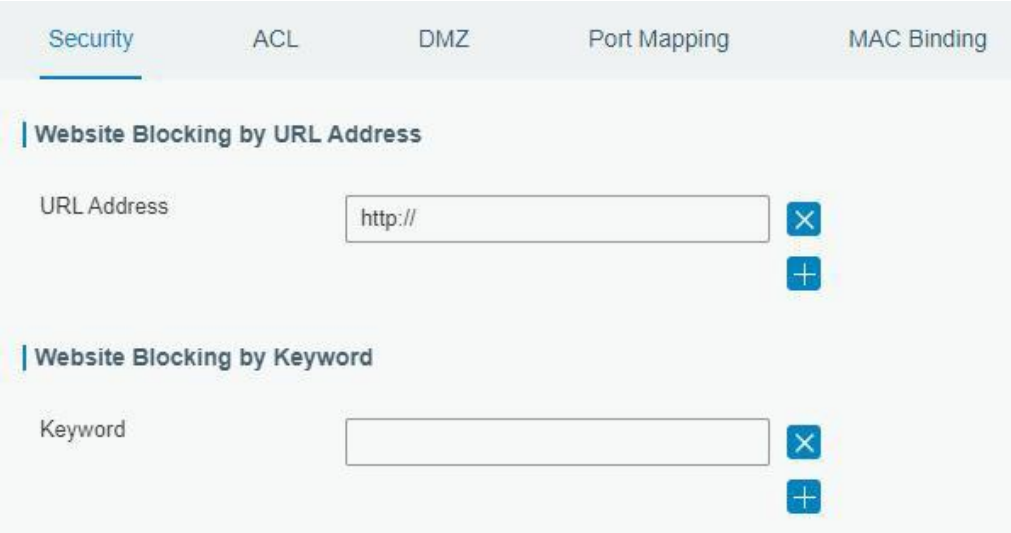


図3-4-2-1

Website Blocking	
URL Address	ブロックしたいHTTPアドレスを入力してください。
Keyword	キーワードを入力することで特定のウェブサイトをブロックできます。最大入力文字数は64文字です。

表 3-2-2-1 セキュリティパラメータ

3.4.2.2 ACL

アクセス制御リスト（ACL）は、一連のマッチングルールを設定することで、ネットワークインターフェースのトラフィックをフィルタリングし、特定のネットワークトラフィック（送信元IPアドレスなど）へのアクセス許可または禁止を実装します。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ースに適用されるACLルールに従ってフィールドが分析されます。特定のパケットが識別された後、事前設定された戦略に従って、対応するパケットへのアクセス許可または禁止が実施されます。

ACLによって定義されたデータパケットのマッチングルールは、フローの識別を必要とする他の機能でも使用することができます。

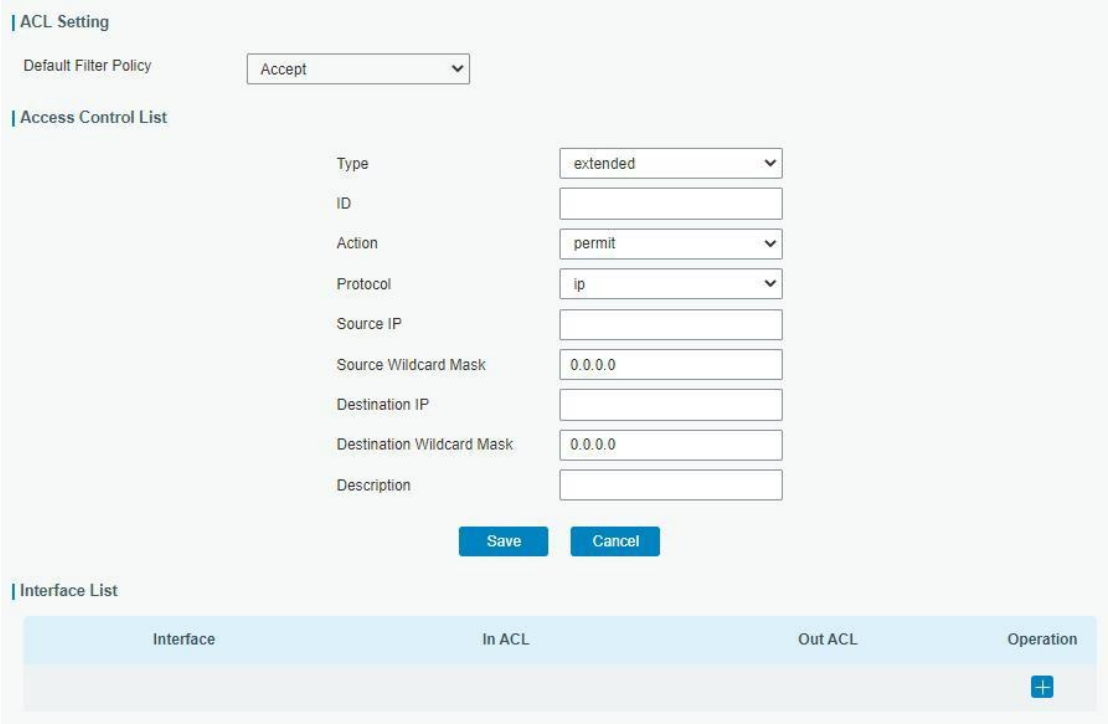


図3-4-2-2

Item	Description
ACL Setting	
Default Filter Policy	"Accept"と"Deny"から選択してください。 アクセス制御リストに含まれていないパケットは、デフォルトのフィルタポリシーによって処理されます。
Access Control List	
Type	"Extended"および"Standard"からタイプを選択してください。
ID	ユーザー定義の ACL 番号です。範囲：1～199。
Action	"Accept"と"Deny"から選択してください。
Protocol	「ip」、「icmp」、「tcp」、「udp」、および「1-255」からプロトコルを選択してください。
Source IP	送信元ネットワークアドレス（空白のままにするとすべてを意味します）。
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です。
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です。
Description	同一IDを持つグループの説明を入力してください。
ICMP Type	ICMPパケットのタイプを入力してください。範囲：0～255。
ICMP Code	ICMPパケットのコードを入力してください。範囲：0～255。
Source Port Type	送信元ポートの種類を選択してください。例：指定ポート、ポート範囲など。
Source Port	送信元ポート番号を設定します。範囲：1～65535。
Start Source Port	開始送信元ポート番号を設定します。範囲：1～65535。
End Source Port	送信元ポートの終了番号を設定します。範囲：1～65535。
Destination Port	宛先ポートの種類を選択してください。例えば、特定のポート、ポート範囲、

Type	など
Destination Port	宛先ポート番号を設定します。範囲：1～65535。
Start Destination Port	開始宛先ポート番号を設定します。範囲：1～65535。
End Destination Port	終了宛先ポート番号を設定します。範囲：1～65535。
More Details	ポートの情報を表示します。
Interface List	
Interface	アクセス制御用のネットワークインターフェースを選択します。
In ACL	ACL ID から着信トラフィック用のルールを選択してください。
Out ACL	送信トラフィック用のルールをACL IDから選択してください。

表 3-4-2-2 ACL パラメータ

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き、すべてのポートが公開されている内部ネットワーク内のホストです。

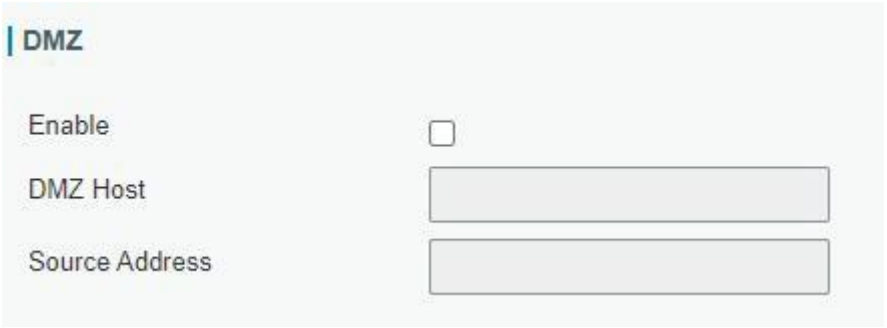


図 3-4-2-3

DMZ	
Item	**Description**
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アドレスを入力してください。
Source Address	DMZ ホストにアクセスできる送信元 IP アドレスを設定してください。 「0.0.0.0/0」は、すべてのアドレスを意味します。

表 3-4-2-3 DMZ パラメータ

3.4.2.4 Port Mapping (DNAT)

外部サービスが内部で必要となる場合（例えば、ウェブサイトが外部に公開されている場合など）、外部アドレスからアクティブな接続が開始されます。そして、ルーターまたはファイアウォールのゲートウェイがその接続を受信します。その後、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、主に外部サービスと内部サービス間で使用されます。

新しいポートマッピングルールを追加するには、[ ]をクリックしてください。

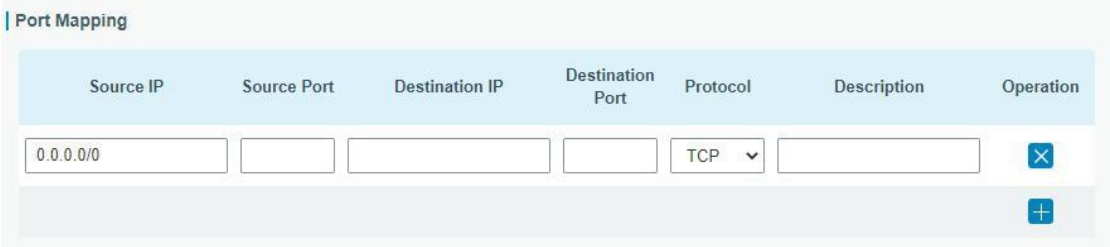


図 3-4-2-4

Port Mapping	
Item	**Description**
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 はすべてを意味します。
Source Port	着信パケットを転送する TCP または UDP ポートを入力してください。範囲：1～65535。
Destination IP	受信インターフェースで受信したパケットが転送される宛先 IP アドレスを入力してください。
Destination Port	受信ポートで受信したパケットが転送されるTCPまたはUDPポートを入力してください。範囲：1～65535。
Protocol	アプリケーションの要件に応じて、「TCP」または「UDP」から選択してください。
Description	このルールの説明です。

表 3-4-2-4 ポートマッピングのパラメータ

Related Configuration Example

NAT アプリケーションの例

3.4.2.5 MAC Binding

MAC バインディングは、許可された外部ネットワークアクセスリストにある MAC アドレスと IP アドレスを照合してホストを指定するために使用されます。

図 3-4-2-5

MAC Binding List	
Item	**Description**
MAC Address	バインディング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	各MAC-IPペアのバインディングルールの意味を記録しやすくするため、説明欄にご記入ください。

表 3-4-2-5 MAC バインディングパラメータ

3.4.3 DHCP

UG67 は、Wi-Fi が AP モードで動作する場合、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。

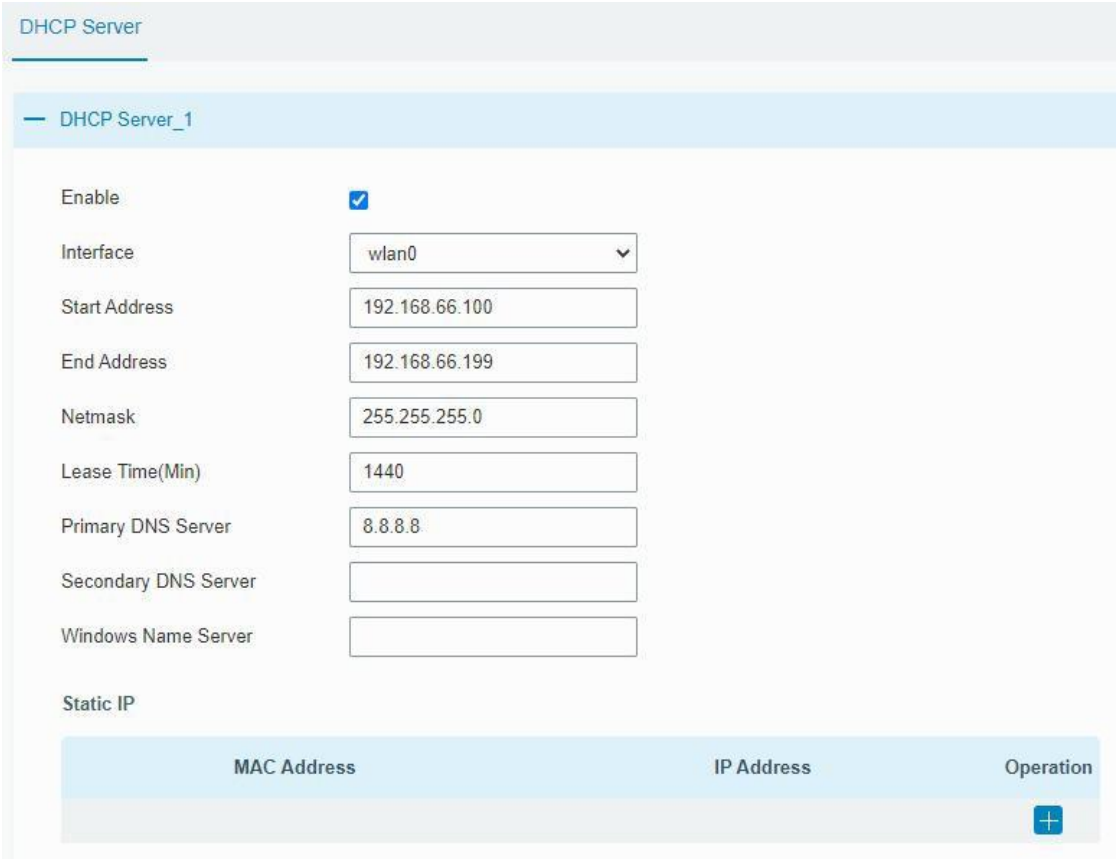


図 3-4-3-1

DHCP Server		
Item	**Description**	**Default**
Enable	DHCPサーバーを有効または無効にします。	有効
Interface	wlan インターフェースのみが IP アドレスを配布することを許可します。	wlan0
StartAddress	DHCPクライアントにリースされるIPアドレスプールの開始点を定義します。	192.168.1.100
End Address	DHCPクライアントに割り当てられるIPアドレスプールの終了点を定義します。	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	取得した Windows インターネット ネーミング サービスを定義します。	Null

NameServer	DHCPクライアントがDHCPサーバーから取得するWindowsインターネットネーミングサービスです。通常は空欄のままにしておいてください。	
Static IP		
MACAddress	DHCPクライアントに静的で特定のMACアドレスを設定します（他のMACアドレスと異なるものにしてください。衝突を避けるためです）。	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 サーバーのパラメータ

3.4.4 DDNS

ダイナミックDNS（DDNS）とは、ドメインネームシステム（DNS）内のネームサーバーを自動的に更新する方式であり、これによりユーザーは動的IPアドレスを静的ドメイン名にエイリアス設定することが可能となります。
DDNSはクライアントツールとして機能し、DDNSサーバーとの連携が必要です。設定を開始する前に、ユーザーは適切なドメイン名プロバイダー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。

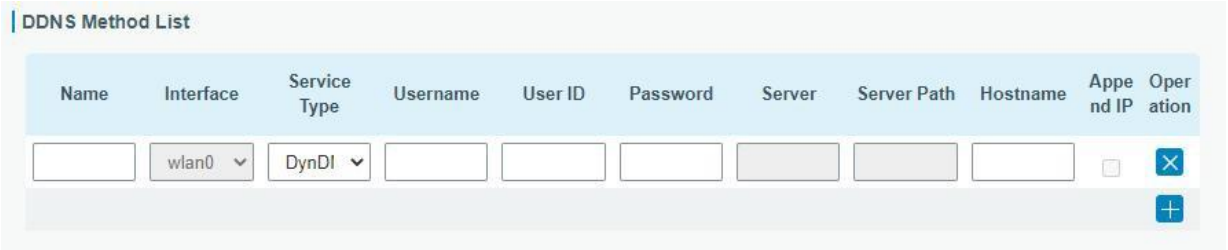


図 3-4-4-1

DDNS	
Item	**Description**
Name	DDNSにわかりやすい名前を付けてください。
Interface	DDNSと組み合わせて使用するインターフェースを設定してください。
Service Type	DDNSサービスプロバイダーを選択してください。
Username	DDNS登録用のユーザー名を入力してください。
User ID	カスタム DDNS サーバーのユーザー ID を入力してください。
Password	DDNS登録用のパスワードを入力してください。
Server	DDNSサーバーの名前を入力してください。
Hostname	DDNS用のホスト名を入力してください。
Append IP	現在のIPアドレスを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

3.4.5 Link Failover

このセクションでは、VRRP 戦略などのリンクフェイルオーバー戦略の設定方法について説明します。

Configuration Steps

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の 1 つ以上の追跡オブジェクトを定義します。

3. トラックオブジェクトに関連付けられたアプリケーション（VRRPや静的ルーティングなど）を定義します。

3.4.5.1 SLA

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

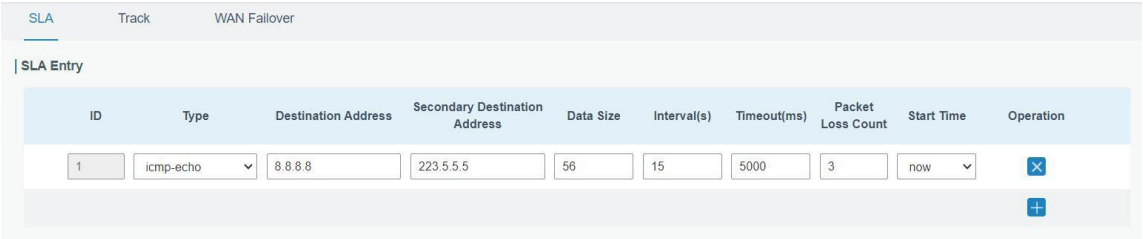


図 3-4-5-1

SLA		
Item	**Description**	**Default**
ID	SLA 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	ICMP-ECHO は、リンクが稼働しているかどうかを検出するためのデフォルトのタイプです。	icmp-echo
Destination Address	検出されたIPアドレスです。	8.8.8.8
SecondaryDestination 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)	ICMP検出フェイルを判定するための応答に対するユーザー定義のタイムアウト。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定義します。設定済みのパケットロス数を超過した場合、SLAプローブはフェイルとなります。	5
Start Time	検出開始時刻。"Now"と空白文字から選択してください。空白文字は、このSLA検出を開始しないことを意味します。	now

表 3-4-5-1 SLA パラメータ

3.4.5.2 Track

トラック設定は、SLAモジュール、トラックモジュール、アプリケーションモジュール間の連携を実現するために設計されています。トラック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、主な機能として各種SLAモジュールの差異を隠蔽し、アプリケーションモジュールに対して統一されたインターフェースを提供します。

Linkage between Track Module and SLA module

設定を完了すると、トラックモジュールとSLAモジュール間の連携関係が確立されます。SLAモジュールは、リンク状態やネットワークパフォーマンスの検出、およびトラックモジュールへの通知に使用されます。検出結果は、トラックの状態変化をタイムリーに追跡するのに役立ちます。

- 正常に検出された場合、対応するトラック項目は「正常」となります。
- 検出がフェイルした場合、対応する追跡項目は「Negative」となります。

Linkage between Track Module and Application Module

設定後、トラックモジュールとアプリケーションモジュール間の連携関係が確立されます。トラック項目に変更が生じた際には、対応が必要な通知がアプリケーションモジュールへ送信されます。

現在、VRRPや静的ルーティングなどのアプリケーションモジュールは、トラックモジュールとの連携が可能です。

アプリケーションモジュールへ即時通知を行う場合、ルーティングのフェイルや復旧の遅れなどの理由により、通信が中断される可能性があります。そのため、トラック項目の状態が変化した際にアプリケーションモジュールへ通知するタイミングを、ユーザーが設定可能な遅延時間を設定できます。

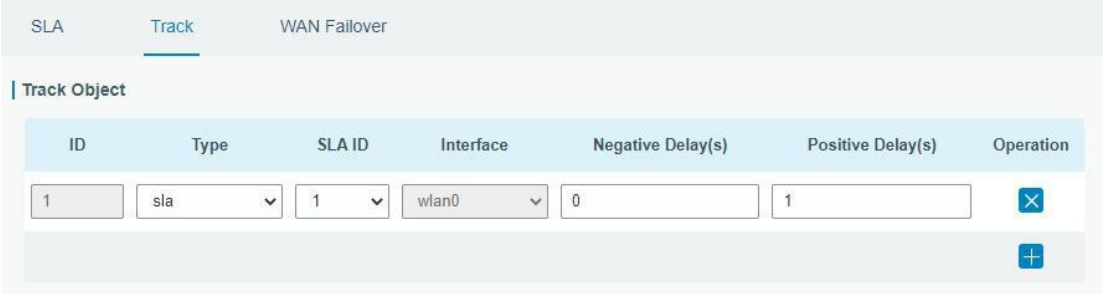


図 3-4-5-2

Item	Description	Default
Index	トラックインデックス。最大10個のトラック設定が可能です。範囲：1～10。	1
Type	オプションは「sla」と「interface」です。	SLA
SLA ID	定義済み SLA ID。	1
Interface	ステータスを検出するインターフェースを選択してください。	cellular0
Negative Delay (s)	インターフェースがダウン状態になった場合、またはSLAプローブがフェイルした場合、実際にダウン状態に変更される前に、ここで設定された時間待機します。範囲：0～180（0は即時切り替えを意味します）。	0
Positive Delay (s)	障害復旧が発生した場合、実際にステータスを「アップ」に変更する前に、ここで設定された時間待機します。範囲：0～180（0は即時切り替えを意味します）。	1

表 3-4-5-2 トラックパラメータ

3.4.5.3 WAN Failover

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。特定のインターフェースの故障や帯域幅不足によりサービス伝送が正常に行えない場合、フローレートを迅速にバックアップインターフェースへ切り替えることが可能です。

これにより、バックアップインターフェースがサービス伝送を引き継ぎ、ネットワークフローを分担することで、データ機器の通信信頼性が向上します。

メインインターフェースのリンク状態がアップからダウンに切り替わった場合、システムはバックアップインターフェースのリンクに即時切替を行うのではなく、あらかじめ設定された遅延時間を適用いたします。遅延時間経過後もメインインターフェースの状態がダウンのままの場合に限り、システムはバックアップインターフェースのリンクへ切替を行います。それ以外の場合は、システムは変更されません。

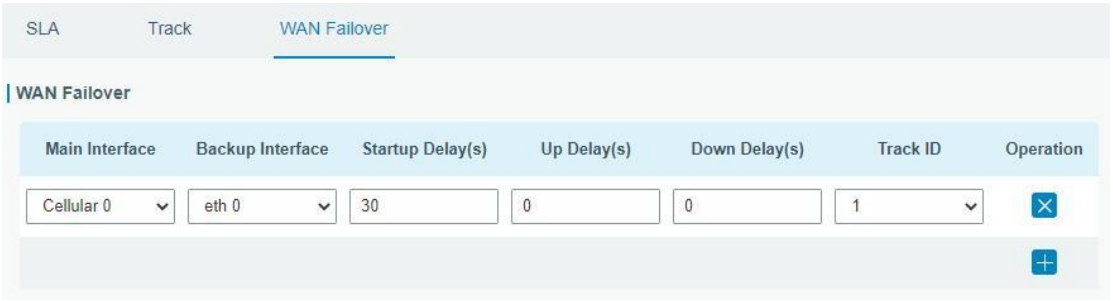


図3-4-5-3

WAN Failover		
Parameters	**Description**	**Default**
Main Interface	リンクインターフェースをメインリンクとして選択してください。	--
Backup Interface	リンクインターフェースをバックアップリンクとして選択してください。	--
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)	プライマリインターフェースが"Fail Detection"から"Success Detection"に切り替わる際、設定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は即時切り替えを意味します）	0
Down Delay (s)	プライマリインターフェースが正常検出からフェイル検出に切り替わる際、設定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は即時切り替えを意味します）。	0
Track ID	トラック検出時、定義済みのトラック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

3.4.6 VPN

仮想プライベートネットワーク（VPN）は、二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、デバイスが安全なチャネルを介して一方のネットワークから他方のネットワークへ接続できるようにします。

UG67は、DMVPN、IPsec、GRE、L2TP、PPTP、OpenVPNに加え、IPsec上のGREおよびIPsec上のL2TPに対応しております。

3.4.6.1 DMVPN

ダイナミック・マルチポイント仮想プライベートネットワーク（DMVPN）は、mGREとIPsecを組み合わせたもので、組織の本社VPNサーバーやゲートウェイを経

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。

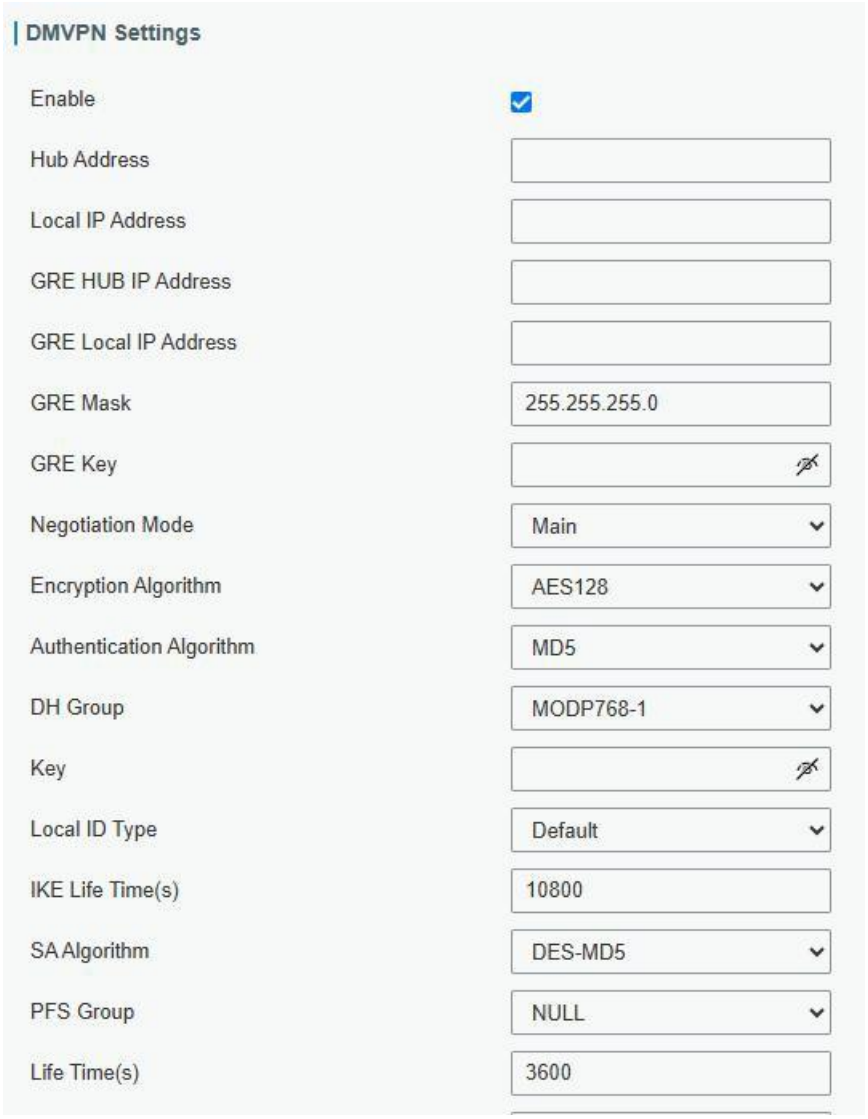


図 3-4-6-1

図 3-4-6-2

DMVPN	
Item	**Description**
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です。
Local IP address	DMVPNローカルトンネルのIPアドレスです。
GRE Hub IP Address	GREハブのトンネルIPアドレスです。
GRE Local IP Address	GREローカルトンネルのIPアドレスです。
GRE Netmask	GREローカルトンネルのネットマスクです。

GRE Key	GRE トンネルキー。
Negotiation Mode	"Main"と"Aggressive"からお選びください。
Encryption Algorithm	「DES」、「3DES」、「AES128」、「AES192」、「AES256」から選択してください。
AuthenticationAlgorithm	「MD5」と「SHA1」からお選びください。
DH Group	「MODP768_1」、「MODP1024_2」、および「MODP1536_5」から選択してください。
Key	事前共有鍵を入力してください。
Local ID Type	"Default"、「ID」、「FQDN」、"User FQDN"から選択してください。
IKE Life Time (s)	IKEネゴシエーションにおける有効期間を設定します。範囲：60～86400。
SA Algorithm	「DES_MD5」、「DES_SHA1」、「3DES_SHA1」、「AES128_MD5」、「AES128_SHA1」、「AES192_MD5」、「AES192_SHA1」、「AES256_MD5」、「AES256_SHA1」から選択してください。
PFS Group	「NULL」、「MODP768_1」、「MODP1024_2」、および「MODP1536-5」から選択してください。
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です。

表 3-4-6-1 DMVPN パラメータ

3.4.6.2 IPSec

IPsec は、仮想プライベートネットワークの実装や、ダイヤルアップ接続によるプライベートネットワークへのリモートユーザーアクセスに特に有用です。IPsec の大きな利点は、個々のユーザーのコンピュータに変更を加えることなく、セキュリティ対策を実施できることです。

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)、およびインターネットキー交換 (IKE) です。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暗号化の両方に対応します。IKE は暗号コード交換に使用されます。これらすべては、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。

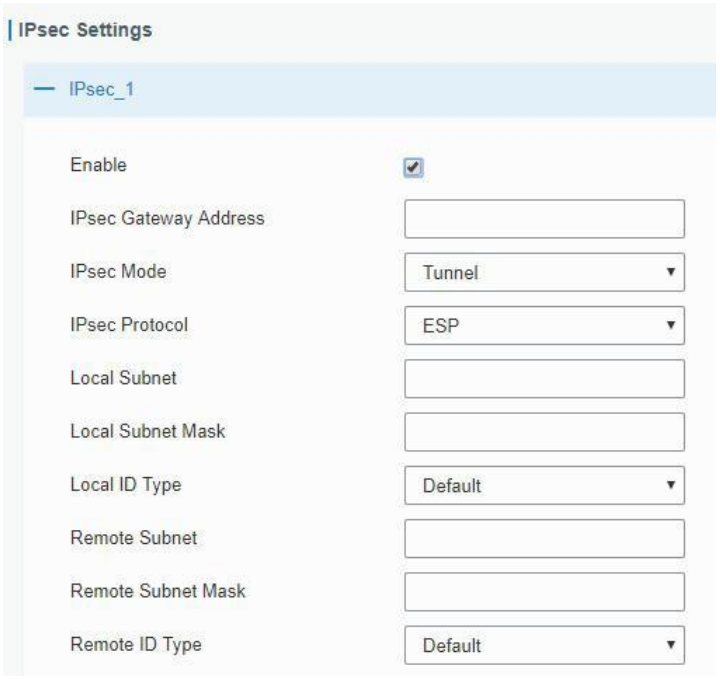


図 3-4-6-3

IPsec	
Item	**Description**
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てください。
IPsec Mode	"Tunnel"と"Transport"から選択してください。
IPsec Protocol	「ESP」と「AH」から選択してください。
Local Subnet	IPsec が保護するローカルサブネットの IP アドレスを入力してください。
Local Subnet Netmask	IPsec が保護するローカルのネットマスクを入力してください。
Local ID Type	"Default"、「ID」、「FQDN」、"User FQDN"から選択してください。
Remote Subnet	IPsec が保護するリモートサブネットの IP アドレスを入力してください。
Remote Subnet Mask	IPsec が保護するリモートネットマスクを入力してください。
Remote ID type	"Default"、「ID」、「FQDN」、"User FQDN"から選択してください。

表 3-4-6-2 IPsec パラメータ

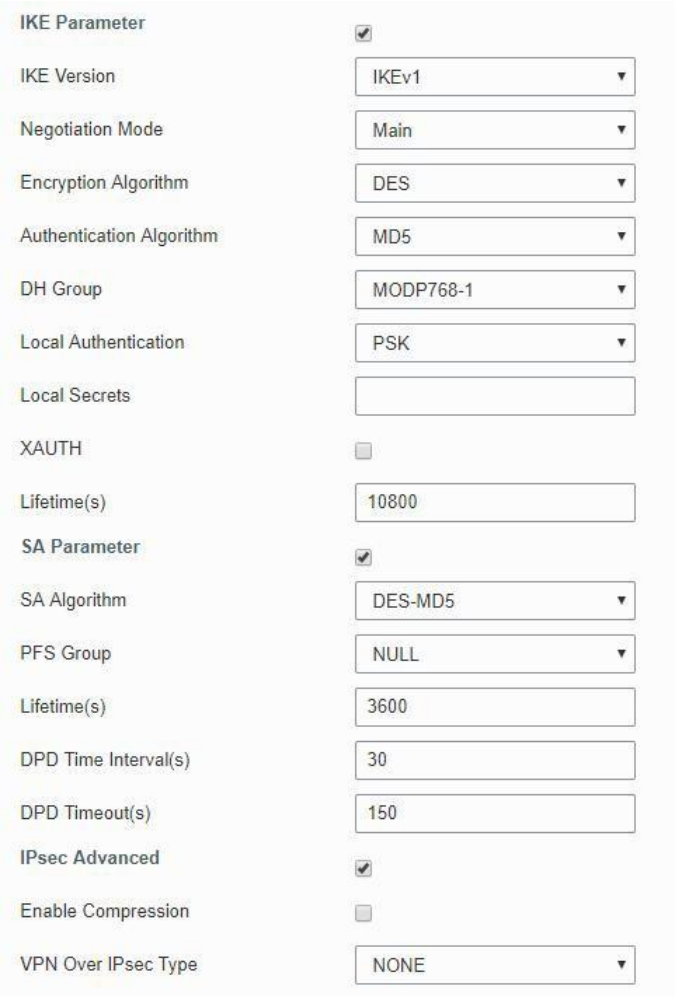


図 3-4-6-4

IKE Parameter	
Item	**Description**
IKE Version	「IKEv1」および「IKEv2」から選択してください。
Negotiation Mode	"Standard"と"Aggressive"からお選びください。
Encryption Algorithm	「DES」、「3DES」、「AES128」、「AES192」、「AES256」からお選びください。
AuthenticationAlgorithm	「MD5」および「SHA1」からお選びください。
DH Group	「MODP768_1」、「MODP1024_2」、および「MODP1536_5」から選択してください。
Local Authentication	「PSK」および「CA」から選択してください。
Local Secrets	事前共有鍵を入力してください。
XAUTH	XAUTHを有効にした後、XAUTHユーザー名とパスワードを入力してください。
Lifetime (s)	IKEネゴシエーションにおける有効期間を設定します。範囲：60～86400。
SA Parameter	
SA Algorithm	「DES_MD5」、「DES_SHA1」、「3DES_SHA1」、「AES128_MD5」、「AES128_SHA1」、「AES192_MD5」、「AES192_SHA1」、「AES256_MD5」、「AES256_SHA1」から選択してください。
PFS Group	「NULL」、「MODP768_1」、「MODP1024_2」、および「MODP1536_5」から選択してください。
Lifetime (s)	IPsec SA の有効期間を設定します。範囲：60～86400。

DPD Interval Time(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します。範囲：10～3600。
IPsec Advanced	
Enable Compression	有効にすると、IP パケットのヘッダーが圧縮されます。
VPN Over IPsec Type	「NONE」、「GRE」、「L2TP」から選択し、VPN over IPsec 機能を有効にしてください。

表 3-4-6-3 IPsec パラメータ

3.4.6.3 GRE

汎用ルーティングカプセル化（GRE）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を伝送し、両端でカプセル化およびカプセル解除を実現できるチャネルを提供するトンネリング技術です。

以下の状況において、GRE トンネル伝送を適用することができます：

- 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であるか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単体ではマルチキャストの暗号化を実現できません。
- 特定のプロトコルはルーティングできません。
- 異なるIPアドレスを持つネットワークを接続するには、他の2つの同様のネットワークが必要となります。

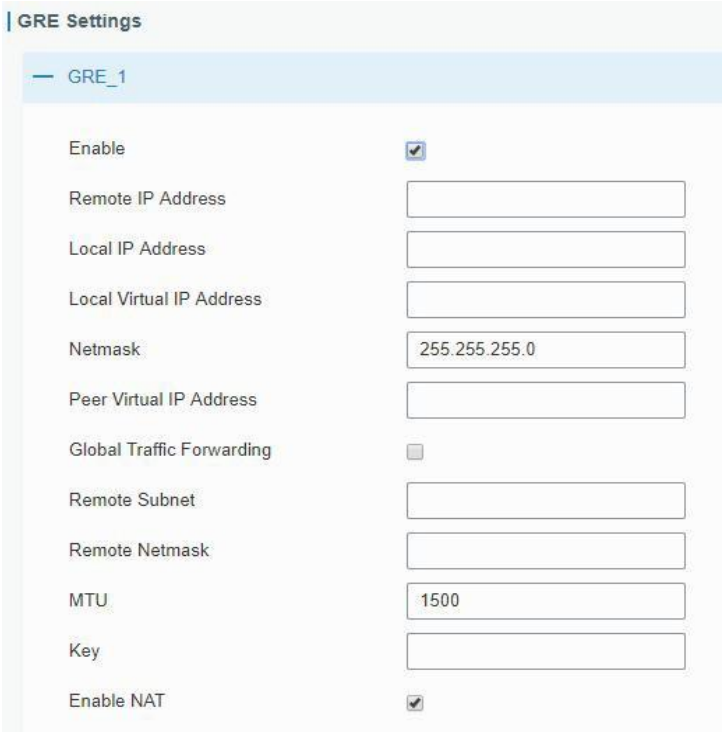


図 3-4-6-5

GRE	
Item	**Description**
Enable	GRE機能を有効にするにはチェックを入れてください。
Remote IP Address	GRE トンネルの実際のリモート IP アドレスを入力してください。

Local IP Address	ローカル IP アドレスを設定します。
Local Virtual IPAddress	GRE トンネルのローカル トンネル IP アドレスを設定してください。
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 アドレスを入力してください。
Global TrafficForwarding	この機能を有効にすると、すべてのデータトラフィックは 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 アドレスを入力してください。
Remote Netmask	GREトンネルのリモートネットマスクを入力してください。
MTU	最大伝送単位を入力してください。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

3.4.6.4 L2TP

レイヤ 2 トンネリングプロトコル (L2TP) 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で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、ポイントツーポイントトンネリングプロトコル (PPTP) の拡張機能です。

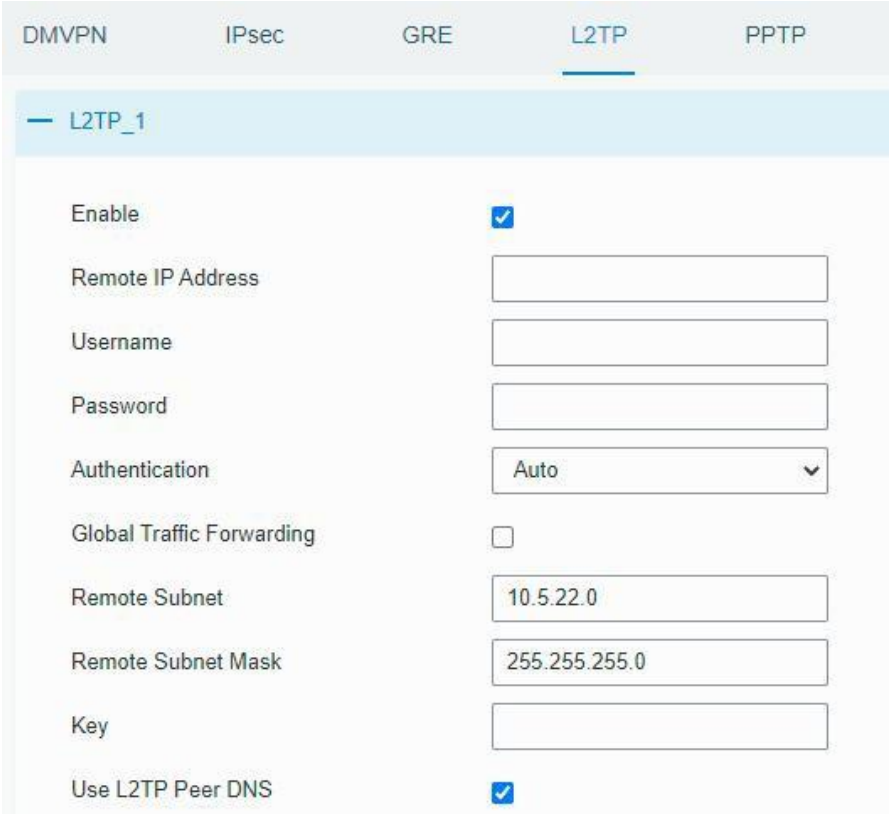


図 3-4-6-6

L2TP	
Item	**Description**
Enable	L2TP機能を有効にするには、チェックを入れてください。
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てください。
Username	L2TPサーバーが提供するユーザー名を入力してください。

Password	L2TPサーバーが提供するパスワードを入力してください。
Authentication	"Auto"、「PAP」、「CHAP」、「MS-CHAPv1」、「MS-CHAPv2」から選択してください。
Global TrafficForwarding	この機能を有効にすると、すべてのデータトラフィックは 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 アドレスを入力してください。
Remote Subnet Mask	L2TP が保護するリモートネットマスクを入力してください。
Key	L2TP トンネルのパスワードを入力してください。
Use L2TP Peer DNS	有効にすると、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

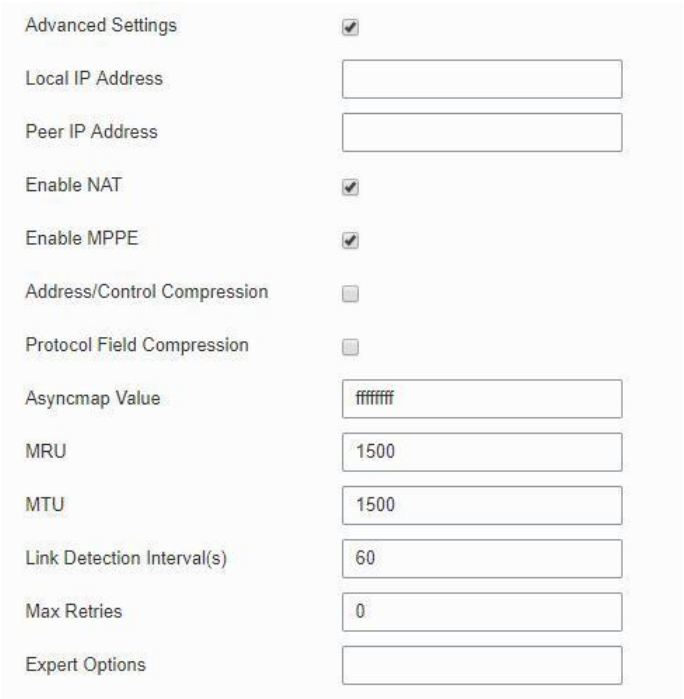


図 3-4-6-7

Advanced Settings	
Item	**Description**
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。空欄の場合、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アドレスを入力してください。
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/ControlCompression	PPP初期化用です。ユーザーはデフォルト設定のままにしておくことができます。
Protocol FieldCompression	PPPの初期化用です。ユーザーはデフォルト設定のままにしておくことができます。
Asyncmap Value	PPPプロトコル初期化文字列のいずれかです。ユーザー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：128～1500
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	L2TP接続のフェイルを検出するための最大再試行回数を設定します。範囲：0～10。
Expert Options	このフィールドには、その他の PPP 初期化文字列を入力できます。文字列は空白で区切ってください。

表 3-4-6-6 L2TP パラメータ

3.4.6.5 PPTP

ポイントツーポイントトンネリングプロトコル（PPTP）は、企業が自社の企業ネットワークを、公衆インターネット上のプライベートな"tunnels"を通じて拡張することを可能にするプロトコルです。これにより、企業は広域ネットワークを単一の大きなローカルエリアネットワークとして効果的に利用できます。

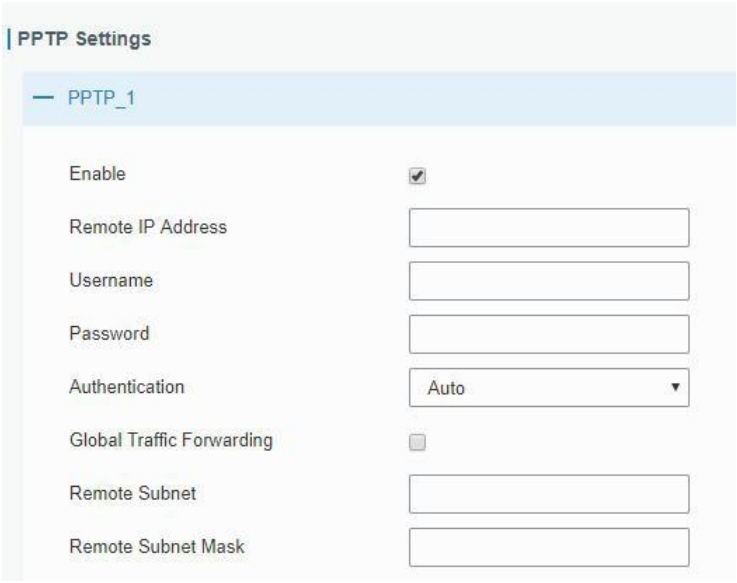


図 3-4-6-8

PPTP	
Item	**Description**
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てください。
Username	PPTPサーバーが提供するユーザー名を入力してください。
Password	PPTPサーバーが提供するパスワードを入力してください。
Authentication	"Auto"、「PAP」、「CHAP」、「MS-CHAPv1」、「MS-CHAPv2」から選択してください。
Global TrafficForwarding	この機能を有効にすると、すべてのデータトラフィックは 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 SubnetMask	対向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

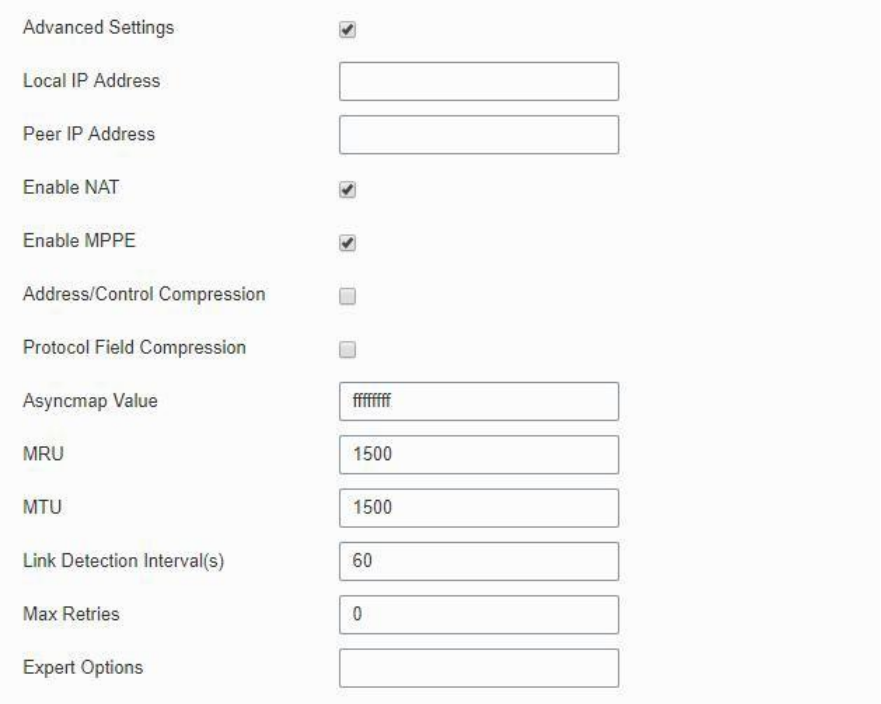


図 3-4-6-9

PPTP Advanced Settings	
Item	**Description**
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アドレスを入力してください。
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/ControlCompression	PPPの初期化用です。ユーザーはデフォルト設定のままにしておくことができます。
Protocol FieldCompression	PPPの初期化用です。ユーザーはデフォルト設定のままにすることができます。
Asyncmap Value	PPPプロトコル初期化文字列のいずれかです。ユーザーはデフォルト値のままにすることができます。範囲：0～ffffffff。
MRU	最大受信単位を入力してください。範囲：64～1500。
MTU	最大送信単位を入力してください。範囲：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てください。範囲：0～600。
Max Retries	PPTP接続のフェイルを検出するための最大再試行回数を設定してください。範囲：0～10。
Expert Options	このフィールドには、その他の PPP 初期化文字列を入力できます。文字列は空白で区切ってください。

表 3-4-6-8 PPTP パラメータ

3.4.6.6 OpenVPN Client

OpenVPN は、簡素化されたセキュリティフレームワーク、モジュール式のネットワーク設計、およびクロスプラットフォームの移植性を提供するオープンソースの仮想プライベートネットワーク（VPN）製品です。UG67 は、最大 3 つの OpenVPN クライアントを同時に実行すること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

セキュリティフレームワーク、モジュール式のネットワーク設計、およびクロスプラットフォームの移植性を提供します。UG67 は、最大 3 台の OpenVPN クライアントを同時に実行することを対応しています。ovpn ファイルを直接インポートするか、このページで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。

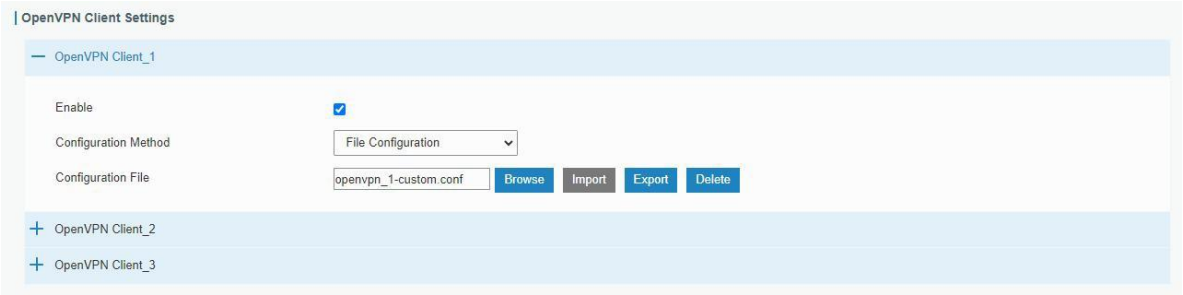


図 3-4-6-10

OpenVPN Client - File Configuration	
Item	**Description**
Browse	クライアント設定のovpn形式ファイル（設定内容および証明書の内容を含む）を参照するには、こちらをクリックしてください。サンプルに基づいてクライアント設定ファイルをご参照ください：
Edit	クリックすると、インポートされたファイルを編集できます。
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するにはクリックしてください。

表 3-4-6-9 OpenVPN クライアントのパラメータ

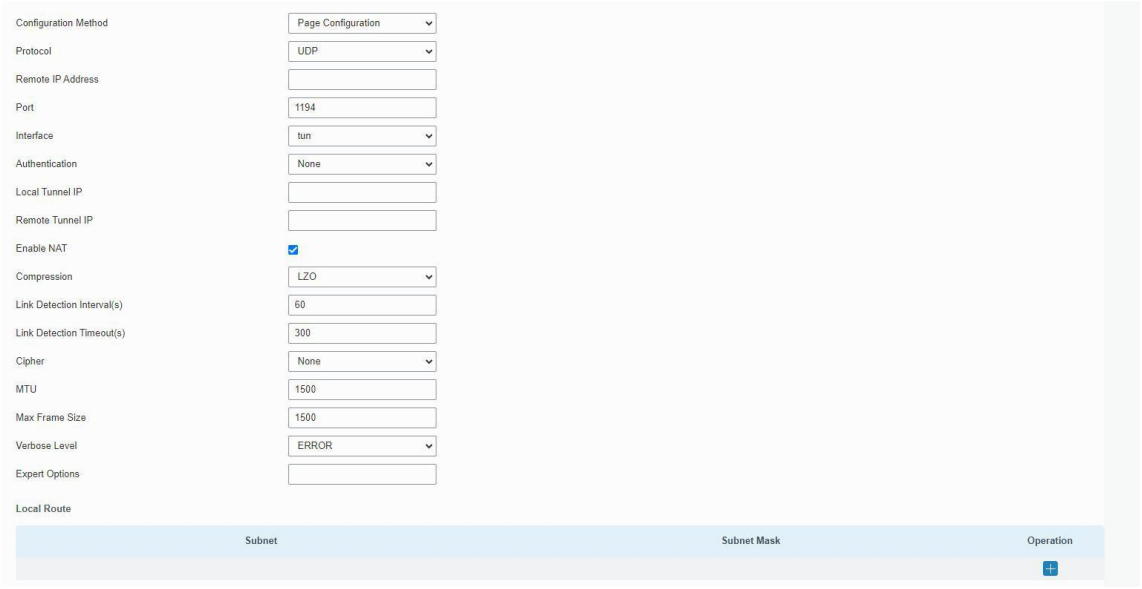


図 3-4-6-11

OpenVPN Client - Page Configuration	
Item	**Description**
Protocol	接続に使用するトランスポートプロトコル（UDP または TCP）を選択してください。
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てください。
Port	リモート OpenVPN サーバーの TCP/UCP サービス番号を入力してください。範囲：1～65535。

Interface	仮想VPNネットワークインターフェースの種類として、TUNまたはTAPをお選びください。TUNデバイスはIPv4またはIPv6（OSIレイヤ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2）をカプセル化します。
Authentication Type	データセッションのセキュリティを確保するために使用する認証タイプを選択してください。 **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] > VPN** ページに移動し、static.key を **PSK** フィールドにインポートしてください。 **Username/Password:**サーバー側で事前設定されたユーザー名/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、**Network > VPN > Certifications** ページに移動し、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てください。 **X.509 cert + user:** ユーザー名/パスワード認証と X.509 証明書認証の両方を使用します。
Local Virtual IP	認証タイプが「**None**または「 の場合、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 TrafficForwarding	この機能を有効にすると、すべてのデータ通信は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。有効にした後は、**Network> VPN >VPN**ページに移動し、ta.keyを**TA**フィールドにインポートしてください。 **Note:**このオプションは tls-auth のみに対応しています。tls-crypt をご利用の場合は、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：tls-crypt /etc/openvpn/openvpn-client1-ta.key
Compression	LZOによるデータ圧縮を有効または無効にするために選択してください。
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されている場合、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秒。
Link Detection Timeout (s)	OpenVPNはタイムアウト後に再確立されます。サーバーとクライアントの両方で設定されている場合、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設定を上書きします。範囲：60～3600秒。
Cipher	NONE、BF-CBC、DES-CBC、DES-EDE3-CBC、AES-128-CBC、AES-192-CBC、AES-256-CBC から選択してください。
MTU	最大伝送単位を入力してください。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。
Verbose Level	ERROR、WARNING、NOTICE、DEBUG から選択してください。
Expert Options	このフィールドに初期化文字列を入力できます。各文字列はセミコロンで区切ってください。 **Example:** ncp-ciphers AES-128-GCM; キー方向 1
Local Route	
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 クライアントのパラメータ

3.4.6.7 OpenVPN Server

UG67 は、ルーティングまたはブリッジ構成での安全なポイントツーポイントまたはサイト間接続、およびリモートアクセス機能に対応した OpenVPN サーバーに対応しています。ovpn ファイルを直接インポートするか、このページで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。

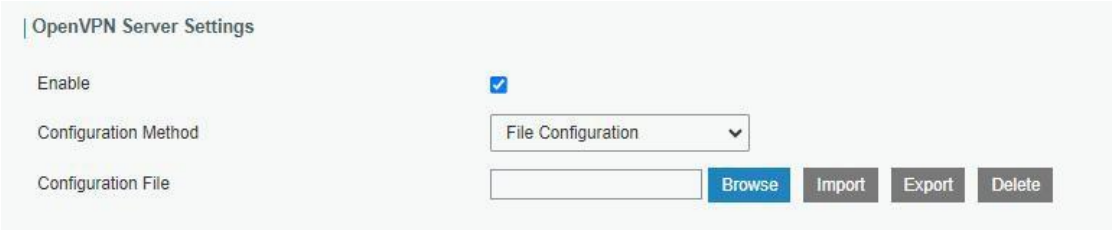


図 3-4-6-12

OpenVPN Server - File Configuration	
Item	**Description**
Browse	サーバー設定のOVPN形式ファイル（設定内容および証明書の内容を含む）を閲覧するには、こちらをクリックしてください。サンプルに基づいてサーバー設定ファイルをご参照ください：
Edit	クリックすると、インポートされたファイルを編集できます。
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するにはクリックしてください。

表 3-4-6-11 OpenVPN サーバーパラメータ

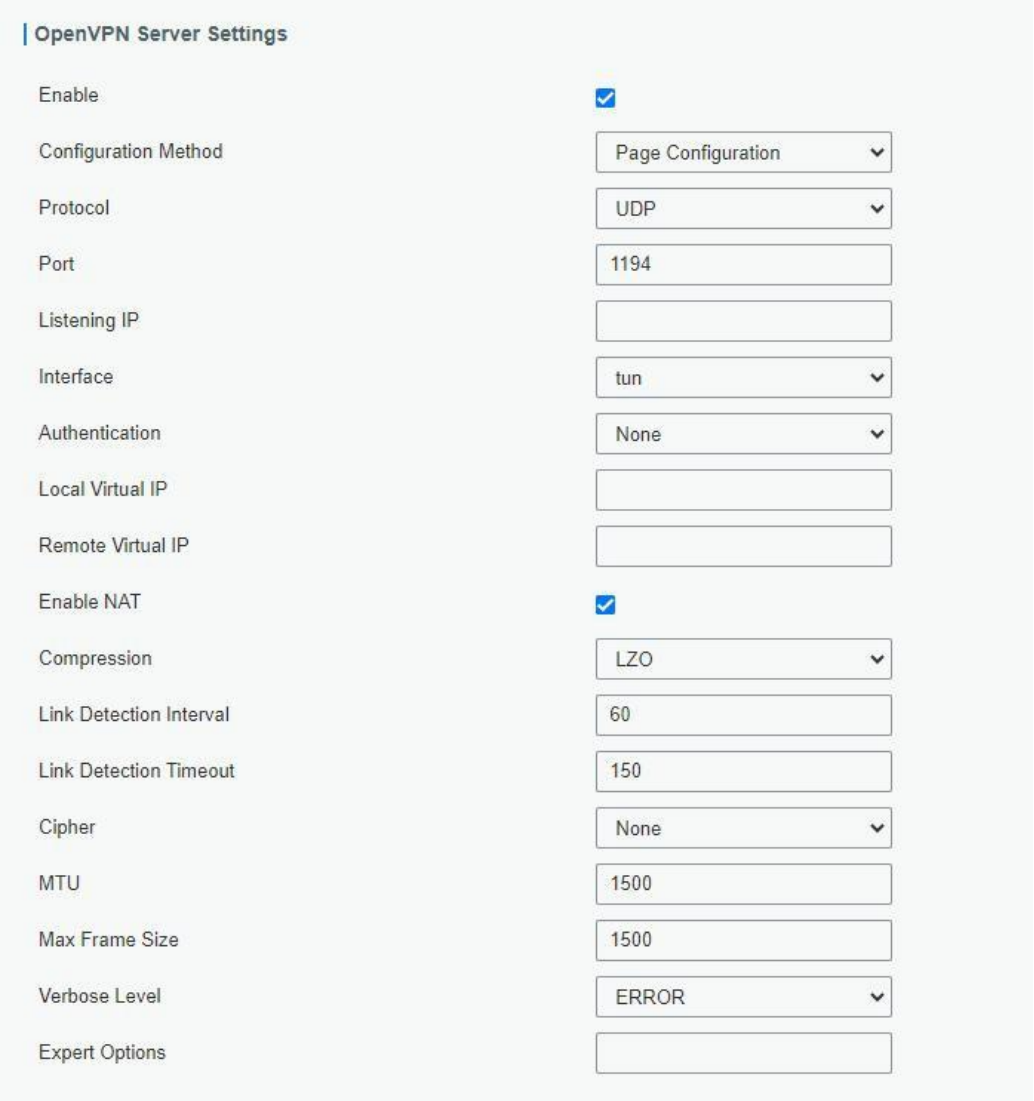


図 3-4-6-13

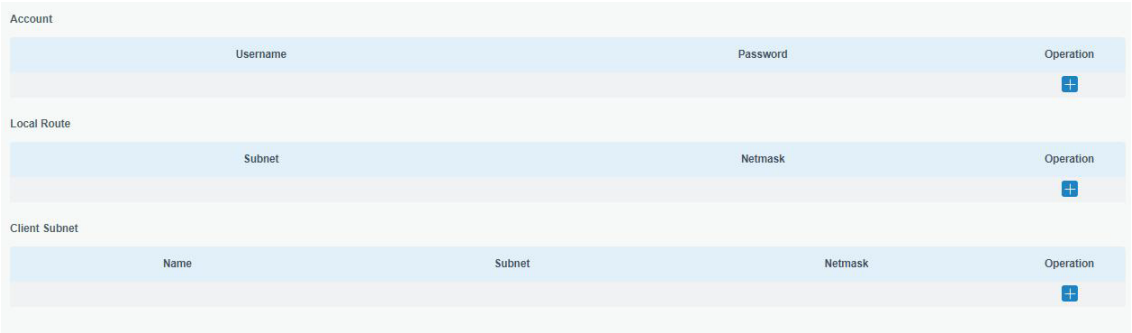


図 3-4-6-14

OpenVPN Server - Page Configuration	
Item	**Description**
Protocol	接続に使用するトランスポートプロトコルを UDP または TCP から選択してください。
Listening IP	バインドするローカルホスト名またはIPアドレスを入力してください。空白のままにすると、OpenVPNサーバーはすべてのインター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/UDPサービス番号を入力してください。 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 または TAP から選択してください。TUN デバイスは IPv4 または IPv6 (OSI レイヤ 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 2) をカプセル化します。
Authentication Type	データセッションのセキュリティ確保に使用する認証タイプを選択してください。 **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] > VPN** ページに移動し、static.key を **PSK** フィールドにインポートしてください。 **Username/Password:**サーバー側で事前設定されたユーザー名/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、**[Network > VPN > Certifications** ページに移動し、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てください。 **X.509 cert + user:** ユーザー名/パスワードとX.509証明書認証の両方を使用します。
Local Virtual IP	認証タイプが「**None**または「 の場合、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クライアント用のIPアドレスプールを定義します。
Client Netmask	クライアントサブネットのネットマスクを設定し、IPアドレスの範囲を制限します。
Renegotiation Interval	この間隔後にデータチャネルキーを再ネゴシエーションします。0は非アクティブ化を意味します。
Max Clients	サーバーが同時に接続できるクライアント数を最大値で制限します。範囲：1～20。 **Note:**多数のクライアントを接続する必要がある場合は、ログの深刻度を「情報」に調整してください。
Enable CRL	CRL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クライアント同士が相互に通信できるようになります。
Enable Dup Client	同一の共通名または証明書で複数のクライアントが接続することを許可します。
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。有効にした後は、**Network VPN VPN**ページに移動し、ta.keyを**TA**フィールドにインポートしてください。 **Note:**このオプションはTLS認証のみに対応しております。TLS暗号化をご利用の場合は、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：tls-crypt /etc/openvpn/openvpn-client1-ta.key
Compression	LZOによるデータ圧縮を有効または無効にするには、こちらを選択してください。
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されている場合、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秒。
Link Detection Timeout (s)	タイムアウト後にOpenVPNが再確立されます。サーバーとクライアントの両方で設定されている場合、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：60～3600秒。
Cipher	NONE、BF-CBC、DES-CBC、DES-EDE3-CBC、AES-128-CBC、AES-192-CBC、AES-256-CBC から選択してください。
MTU	最大伝送単位を入力してください。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	エラー、警告、通知、デバッグから選択してください。
Expert Options	このフィールドには初期化文字列を入力でき、各文字列はセミコロンで区切ります。 **Example:** ncp-ciphers AES-128-GCM; キー方向 1
Account	
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。
Local Route	
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。
Client Subnet	
Name	名前を OpenVPN クライアント証明書の共通名として設定します。
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てください。

表 3-4-6-12 OpenVPN サーバーのパラメータ

3.4.6.8 Certifications

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、認証タイプに応じて、このページで必要な証明書およびキーファイルをインポート/エクスポートすることができます。

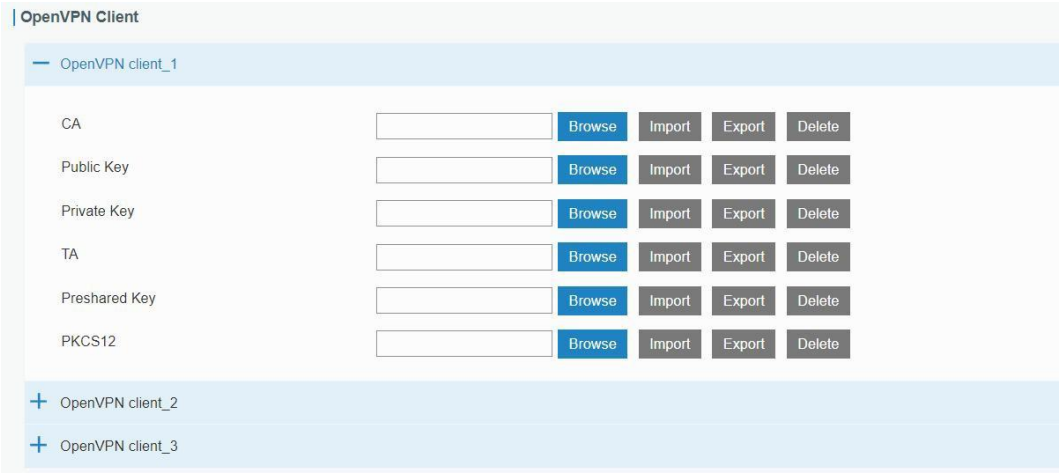


図 3-4-6-15

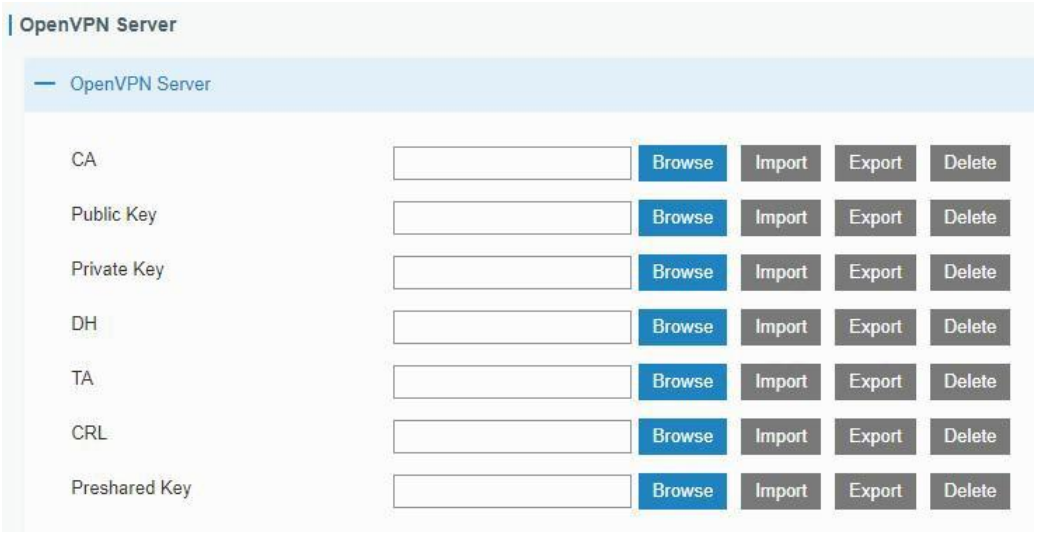


図 3-4-6-16

図 3-4-6-17

3.4.6.9 WireGuard

WireGuardは、非常にシンプルでありながら高速で現代的なVPNであり、最先端の暗号技術を活用しています。WireGuardはUDPプロトコルを介してトラフィックを伝送します。

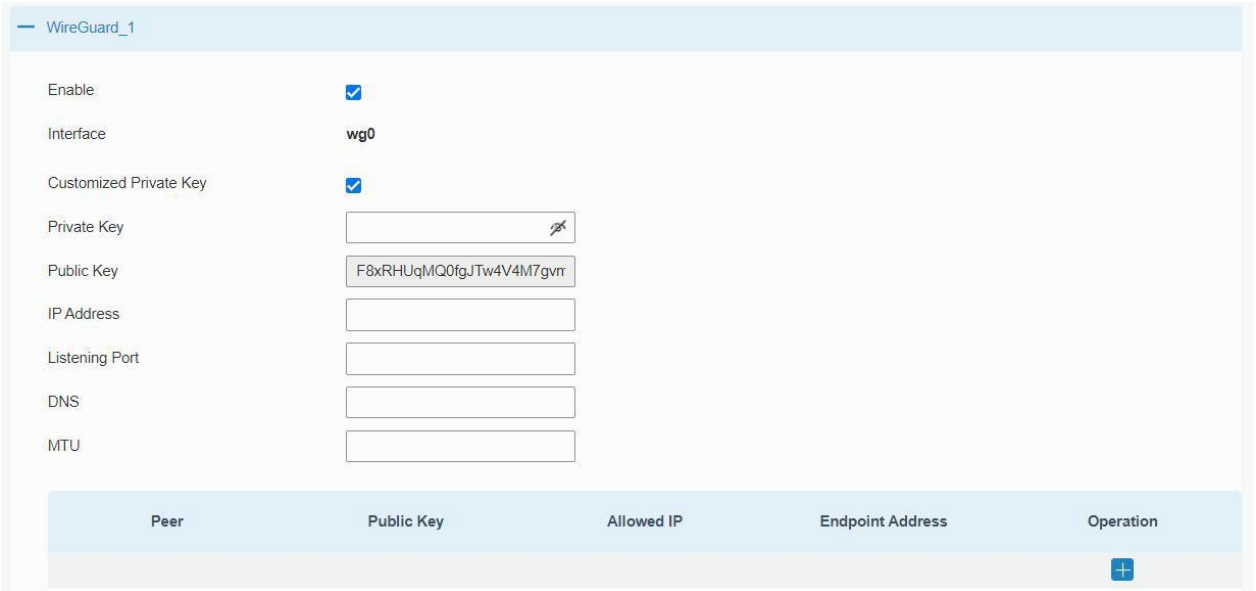


図3-4-6-18

WireGuard	
Item	**Description**
Enable	WireGuard インターフェースを有効にします。最大 3 つの WireGuard インターフェースが許可されます。
Interface	WireGuardインターフェース名を表示します。
Customized Private Key	このWireGuardインターフェースの秘密鍵をカスタマイズするかどうかを設定します。無効にした場合、クライアントはこのルーター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パケットの送受信に使用するポートを設定します。異なるWireGuardインターフェースではポート番号を区別する必要があります。
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。空欄のままにすると、ルーターは共通ネットワークインターフェース（WAN、セルラーなど）のDNSサーバーアドレスを使用します。
MTU	このWireGuardインターフェースの最大伝送単位（MTU）を設定します。空欄のままにすると、ルーターは共通ネットワークインターフェース（WAN、セルラーなど）のMTUを使用します。
Peer Table	「+」をクリックすると、このWireGuardインターフェースのWireGuardピアを追加できます。1つのWireGuardインターフェースには最大20個のピアを追加できます。

表 3-4-6-13 WireGuard パラメータ

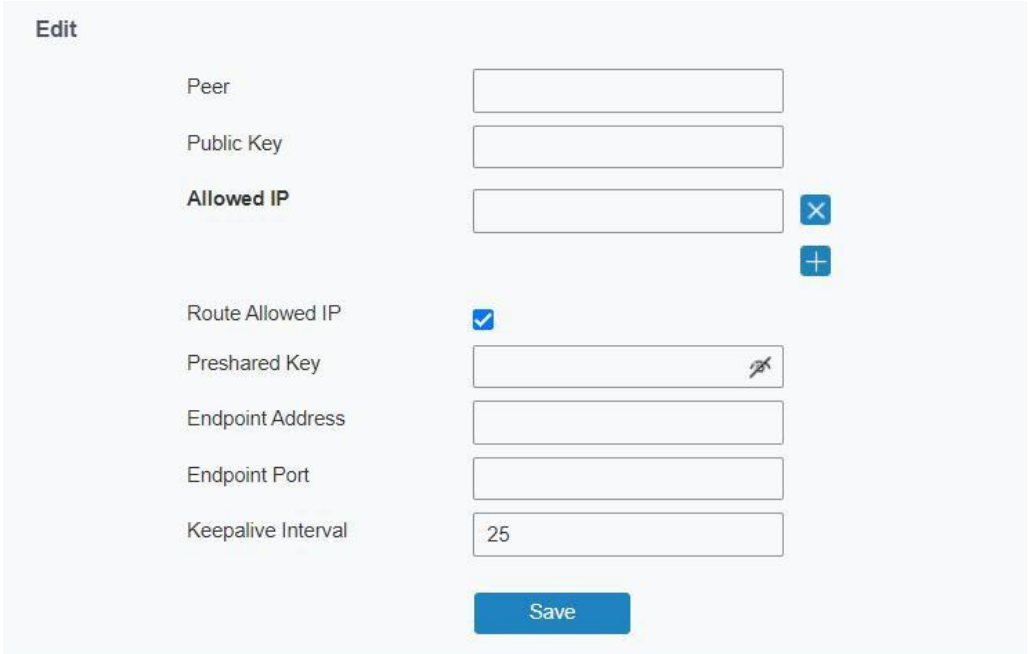


図 3-4-6-19

WireGuard-Peer	
Item	**Description**
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 ピアサーバー/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 ピアに対して、最大 8 つの許可 IP アドレスに対応できます。
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機能を有効または無効にします。
Preshared Key	事前共有鍵を設定します。このインターフェースとピアインターフェースの両方に同じ鍵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	接続が確立された後、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、接続を維持します。0は非有効化を意味します。

表 3-4-6-13 WireGuard-Peer パラメータ

3.4.7 HTTP Proxy

ゲートウェイは、セキュリティ上の目的で実際の IP アドレスを隠しながら、HTTP プロキシサーバーに接続して対象のインターネットサイトと通信することができます。

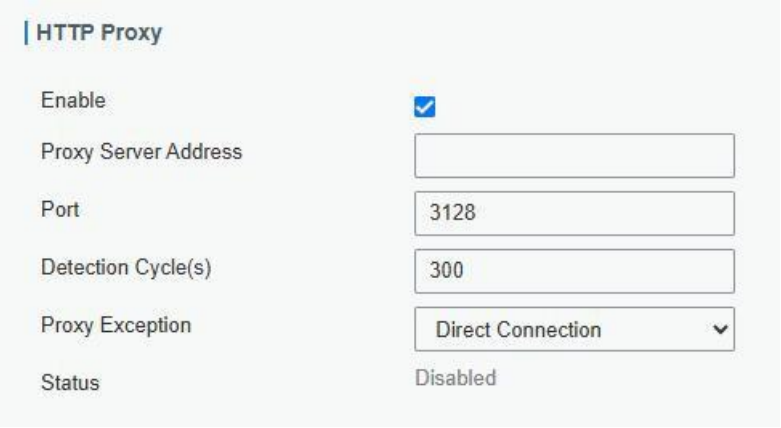


図 3-4-7-1

HTTP Proxy	
Item	**Description**
Enable	HTTP プロキシ機能を有効または無効にします。
Proxy Sever Address	リクエストを送信するプロキシサーバーのアドレス（IP/ドメイン名）を設定します。
Port	リクエストを送信するプロキシサーバーのポートを設定します。
Detection Cycle	HTTP プロキシサーバーへの接続がフェイルした場合の再試行間隔を設定します。
Proxy Exception	プロキシサーバーへの接続がフェイルした場合のトラフィックモードを選択してください： **Direct Connection:** プロキシを経由せず、対象サーバーへ直接トラフィックを送信します。 **Traffic Interception:** プロキシサーバーとの接続が復旧するまでトラフィックをインターセプトします。
Status	ゲートウェイとプロキシサーバー間の接続状態を表示します。

表 3-4-7-1 HTTP プロキシパラメータ

3.5 System

このセクションでは、管理アカウント、アクセスサービス、システム時刻、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 General Settings

3.5.1.1 General

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

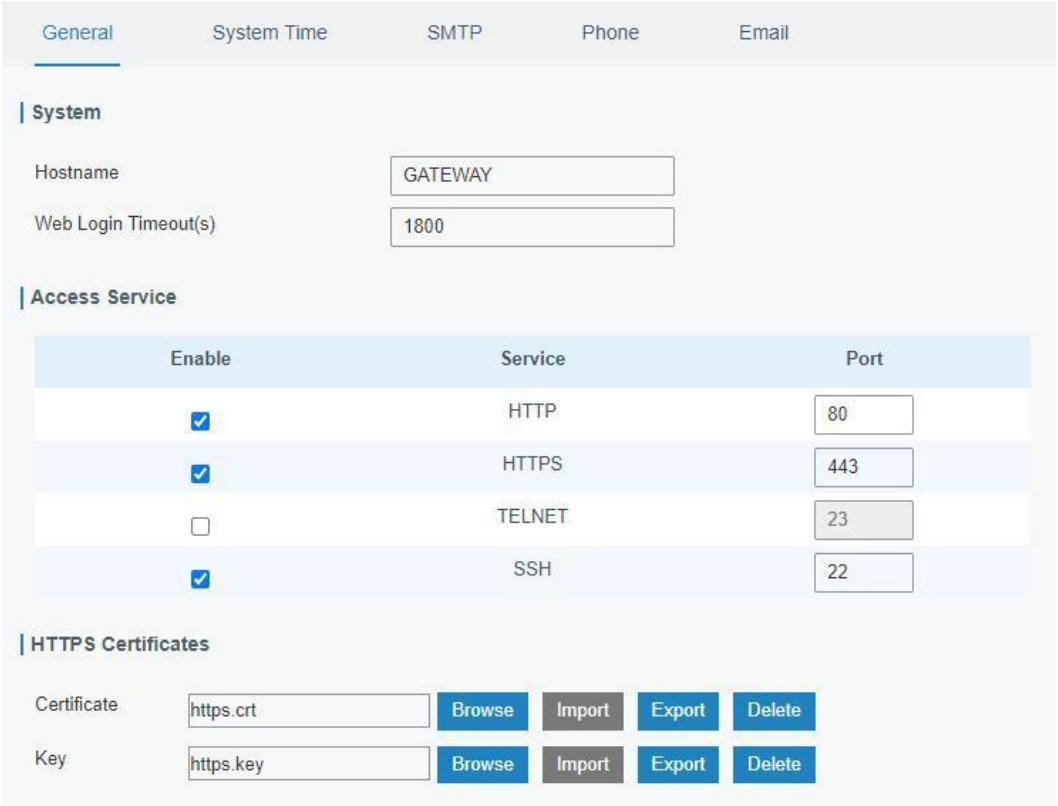


図 3-5-1-1

General		
Item	**Description**	**Default**
System		
Hostname	ユーザー定義のゲートウェイ名。最初の文字はアルファベットで始まる必要があります。	GATEWAY
Web LoginTimeout (s)	タイムアウトが発生した場合、再度ログインが必要となります。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	このオプションを有効にすると、ユーザーはHTTP経由でデバイスにローカルログインし、Webを通じてアクセスおよび制御が可能となります。	80
HTTPS	このオプションを選択すると、ユーザーはHTTPS経由でローカルおよびリモートからデバイスにログインし、Web経由でアクセスおよび制御することが可能となります。	443
TELNET	ユーザーは、ローカルおよびリモートからデバイスにログインし、	23

	TELNET を使用してローカルおよびリモートからログインし、オプションを選択後、Web 経由でアクセスおよび制御することができます。	
SSH	このオプションを選択すると、ユーザー様はSSH経由でデバイスにローカルおよびリモートからログインすることが可能となります。	22
HTTPS Certificates		
Certificate	"Browse"ボタンをクリックし、PC上の証明書ファイルを選択した後、"Import"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。"Delete"ボタンをクリックすると、ファイルが削除されます。	--
Key	"Browse"ボタンをクリックし、PC上のキーファイルを選択した後、"Import"ボタンをクリックすると、ファイルがゲートウェイにアップロードされます。"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。 "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 基本設定パラメータ

3.5.1.2 System Time

このセクションでは、タイムゾーンや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。

Note: to ensure that the gateway runs with the correct time, it's recommended that you set the system time when configuring the gateway.

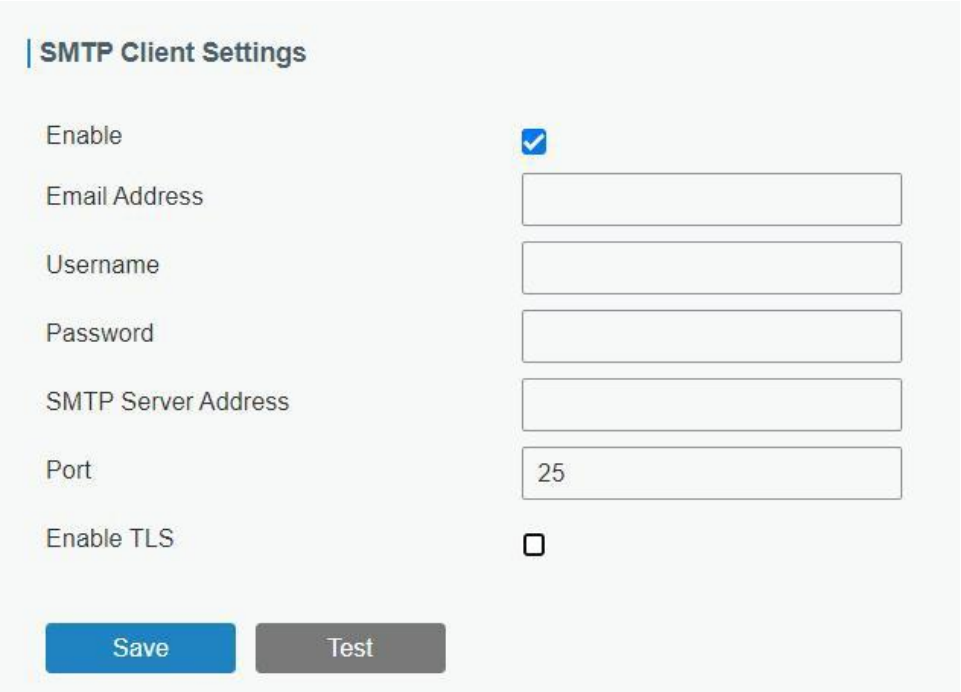
図 3-5-1-2

System Time	
Item	**Description**
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、ご自身のタイムゾーンを選択してください。
Sync Type	ドロップダウンリストをクリックして、時刻同期の種類をお選びください。 **Sync with Browser:** ブラウザと時刻を同期します。 **Sync with NTP Server:** NTPサーバーと時刻を同期します。 **Set up Manually:** 手動で時刻を設定します。
Sync with NTP Server	
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	チェック後、ネットワーク上の NTP クライアントはゲートウェイとの時刻同期を実現できます。

表 3-5-1-2 システム時刻パラメータ

3.5.1.3 SMTP

SMTP（Simple Mail Transfer Protocol）は、電子メールの送受信に使用される



TCP/IP プロトコルです。このセクションでは、電子メール設定の構成方法について説明します。

図 3-5-1-3

SMTP	
Item	**Description**
SMTP Client Settings	
Enable	SMTPクライアント機能を有効または無効にします。
Email Address	送信者のメールアドレスを入力してください。
Username	送信者のメールユーザー名を入力してください。
Password	送信者のメールパスワードを入力してください。
SMTP Server Address	SMTPサーバーのドメイン名を入力してください。
Port	SMTP サーバーのポート番号を入力してください。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

Related Topics

イベント設定

3.5.1.4 Phone

電話の設定は、通話/SMS トリガーおよびイベントの SMS アラームに関連します。これは、携帯電話機能を備えたゲートウェイにのみ適用されます。

図 3-5-1-4

Phone	
Item	**Description**
Phone Number List	
Name	電話グループ名を設定します。
Number	電話番号を入力してください。数字、および「+」と「-」の使用が可能です。複数の番号は「;」で区切ることができます。

表 3-5-1-4 電話設定

Related Topic

オンデマンド接続

3.5.1.5 Email

メール設定には、イベントのメールアラートが含まれます。

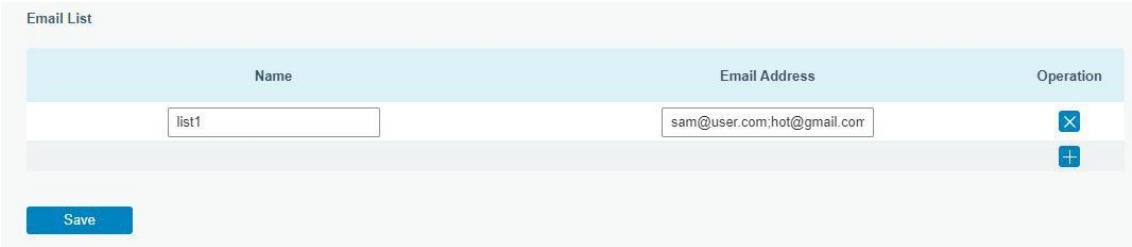


図 3-5-1-5

Email	
Item	**Description**
Email List	
Name	メールグループの名前を設定してください。
Email Address	メールアドレスを入力してください。複数のメールアドレスは「;」で区切ることができます。

表 3-5-1-5 メール設定

3.5.2 User Management

3.5.2.1 Account

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。

Note: it is strongly recommended that you modify them for the sake of security.

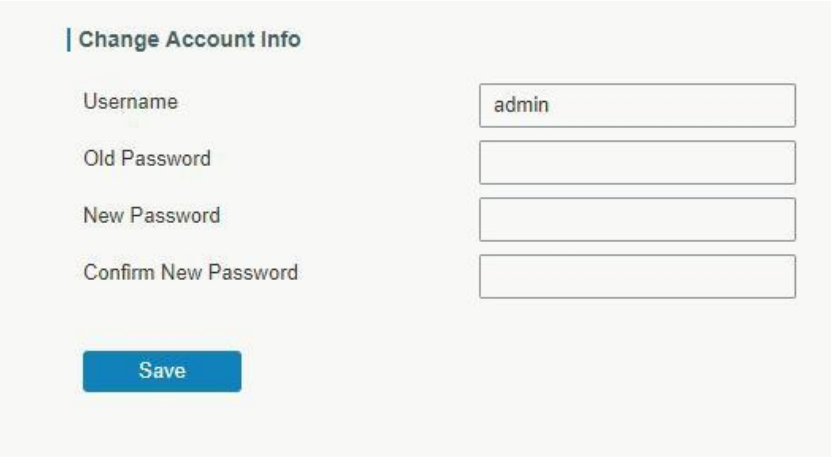


図 3-5-2-1

Account	
Item	**Description**
Username	新しいユーザー名を入力してください。a-z、0-9、"_"、"-" などの文字を使用できます。最初の文字は数字ではいけません。
Old Password	現在のパスワードを入力してください。
New Password	空白以外の任意のASCII文字を含む新しいパスワードを入力してください。パスワードは少なくとも1文字以上の英字と1文字以上の数字を含み、5～31文字の長さである必要があります。
Confirm New Password	新しいパスワードを再度入力してください。

表 3-5-2-1 アカウント情報

3.5.2.2 User Management

このセクションでは、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。共通ユーザーの権限には、読み取り専用と読み取り/書き込みが含まれます。

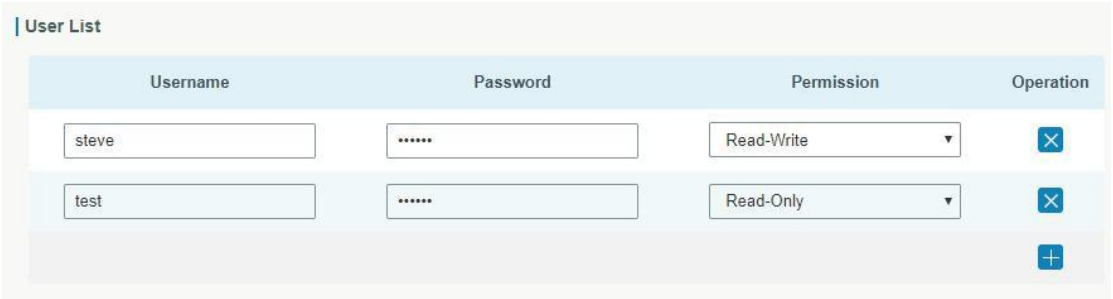


図 3-5-2-2

User Management	
Item	**Description**
Username	新しいユーザー名を入力してください。a-z、0-9、"_"、"-" などの文字を使用できます。最初の文字は数字ではいけません。
Password	パスワードは、空白を除く任意のASCII文字で設定してください。パスワードには少なくとも1文字と1つの数字を含め、5～31文字の長さである必要があります。
Permission	ユーザー権限を"Read-Only"または"Read-write"からお選びください。

	- 読み取り専用：このレベルのユーザーは、ゲートウェイの設定を表示するのみ可能です。 - 読み書き: このレベルでは、ユーザーはゲートウェイの設定を表示および設定できます。

表 3-5-2-2 ユーザー管理

3.5.2.3 HTTP API Management

このセクションでは、HTTP API アカウント情報の設定方法について説明します。

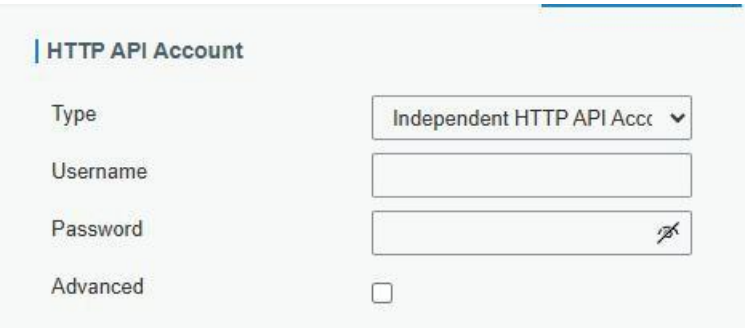


図 3-5-2-3

User Management	
Item	**Description**
Type	Web GUI アカウントと同じ HTTP API アカウント情報を選択するか、独立したアカウントを使用してください。
Username	他のアカウント情報と異なる新しいユーザー名をご入力ください。a-z、0-9、"_"、"-" などの文字を使用できます。最初の文字は数字ではできません。
Password	パスワードは、空白を除く任意のASCII文字を含めて設定してください。
Advanced	
Password	現在のパスワードを入力し、「**Transform** をクリックすると、HTTP API ログイン認証情報用の暗号化されたパスワードが表示されます。

表 3-5-2-3 HTTP API 管理

3.5.3 SNMP

SNMP は、ネットワーク監視のためのネットワーク管理で広く使用されています。SNMP は、管理対象システム内の変数形式で管理データを公開します。システムは、システムの状態と構成を記述する管理情報ベース (MIB) で構成されています。これらの変数は、管理アプリケーションによってリモートで照会することができます。ネットワーク環境におけるSNMPの設定では、NMSおよびSNMP管理プログラムをマネージャー側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は下記の通りです：

1. SNMP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

UG67はSNMPv1、SNMPv2c、SNMPv3バージョンを対応しております。SNMPv1およびSNMPv2cはコミュニティ名認証を採用しております。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おります。

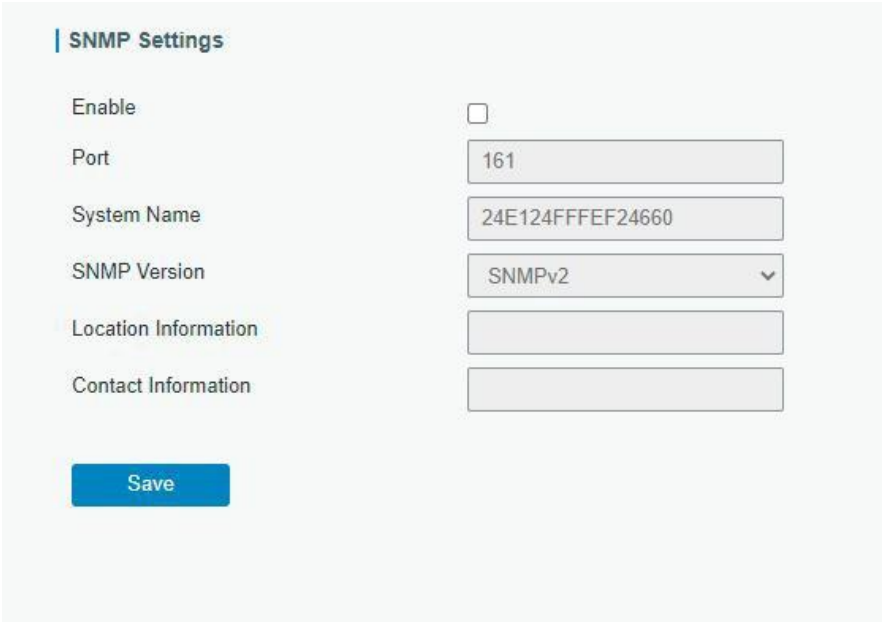


図 3-5-3-1

SNMP Settings	
Item	**Description**
Enable	SNMP機能を有効または無効にします。
Port	SNMPのリスニングポートを設定します。範囲：1～65535。 デフォルトのポートは 161 です。
System Name	ゲートウェイを表すシステム名をご入力ください。
SNMP Version	SNMP バージョンを選択してください。SNMP v1/v2c/v3 に対応しています。
Location Information	場所情報を入力してください。
Contact Information	連絡先情報を入力してください。

表 3-5-3-1 SNMP パラメータ

3.5.3.2 MIB View

このセクションでは、オブジェクトの MIB ビューの設定方法について説明します。

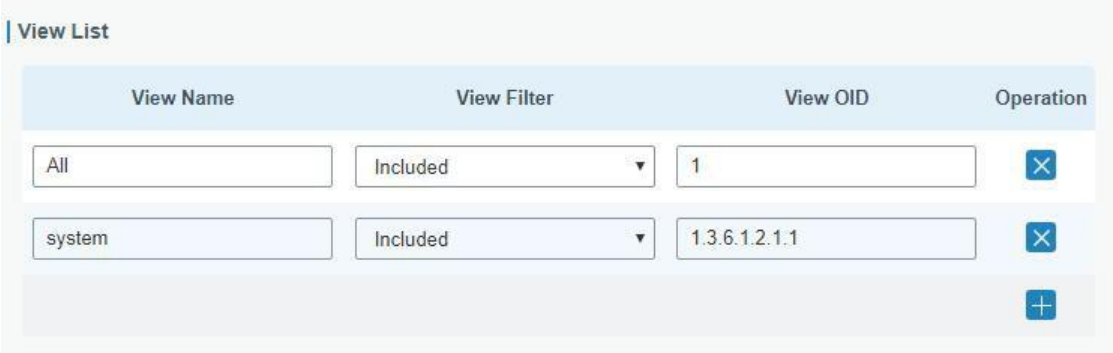


図 3-5-3-2

MIB View	
Item	**Description**
View Name	MIB ビューの名前を設定します。
View Filter	"Included"と"Excluded"から選択してください。
View OID	OID 番号を入力してください。
Included	指定されたMIBノード内のすべてのノードをクエリできます。
Excluded	指定された MIB ノードを除くすべてのノードをクエリできます。

表 3-5-3-2 MIB ビューのパラメータ

3.5.3.3 VACM

このセクションでは、VCAM パラメータの設定方法について説明します。

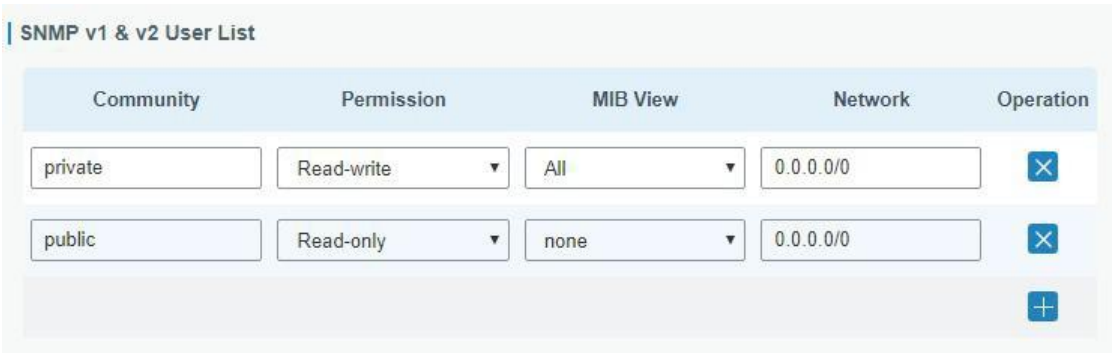


図 3-5-3-3

VACM	
Item	**Description**
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"から選択してください。
MIB View	MIB ビューリストから、権限を設定する MIB ビューを選択してください。
Network	MIB ビューにアクセスする外部ネットワークの IP アドレスおよびビット数。
Read-Write	指定された MIB ノードの権限は、読み取りと書き込みです。
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 グループの名前を設定します。

Security Level	「認証なし/非暗号化」、「認証あり/非暗号化」、" Auth/Priv"から選択してください。
Read-Only View	MIB ビューリストから、権限を"Read-Only"に設定する MIB ビューを選択してください。
Read-Write View	MIB ビューリストから、権限を"Read-write"に設定する MIB ビューを選択してください。
Inform View	MIB ビューリストから、権限を"Inform"に設定する MIB ビューを選択してください。

表 3-5-3-3 VACM パラメータ

3.5.3.4 Trap

このセクションでは、SNMP トラップによるネットワーク監視を有効にする方法について説明しま

す。

図 3-5-3-4

SNMP Trap	
Item	**Description**
Enable	SNMPトラップ機能を有効または無効にします。
SNMP Version	SNMPのバージョンを選択します。SNMP v1/v2c/v3に対応しております。
Server Address	NMS の IP アドレスまたはドメイン名をご入力ください。
Port	UDPポートを入力してください。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 をご利用の場合はグループ名をご入力ください。SNMP v3 をご利用の場合はユーザー名をご入力ください。
Auth/Priv Mode	"NoAuth & No Priv"、「認証あり・非暗号化」、"Auth & Priv"から選択してください。

表 3-5-3-4 トラップパラメータ

3.5.3.5 MIB

このセクションでは、MIB ファイルのダウンロード方法について説明します。

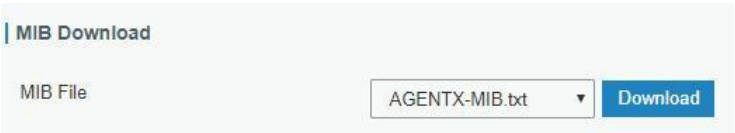


図 3-5-3-5

MIB	
Item	**Description**

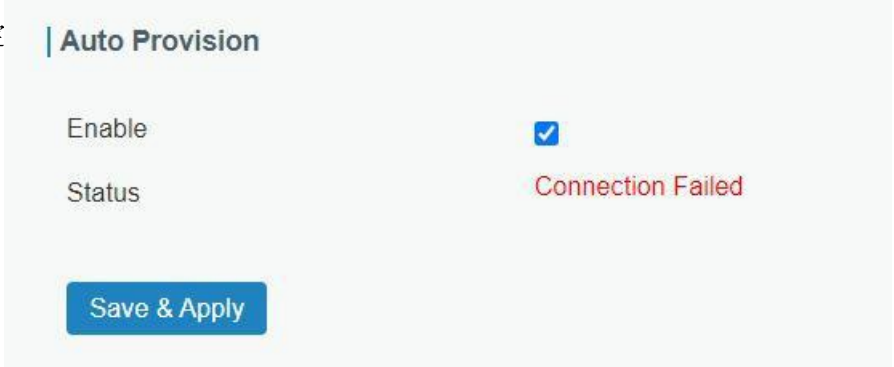
MIB File	必要なMIBファイルをお選びください。
Download	"Download"ボタンをクリックして、MIBファイルをPCにダウンロードしてください。

表 3-5-3-5 MIB ダウンロード

3.5.4 Device Management

3.5.4.1 Auto

ユーザー様は、Milesight開発プラットフォームから設定プロファイルをカスタマイズし、選択することができます。自動プロビジョニングが有効化され、デバイスがインターネットに接続されている場合、デバイスはプロファイルを受信し、初期設定を行います。この機能は、デバイスがMilesight開発プラットフォームへの接続を設定



3.5.4.2 Management Platform

このページでは、デバイスをDeviceHubまたはMilesight開発プラットフォームに接続し、ゲートウェイを集中的に遠隔管理することが可能です。

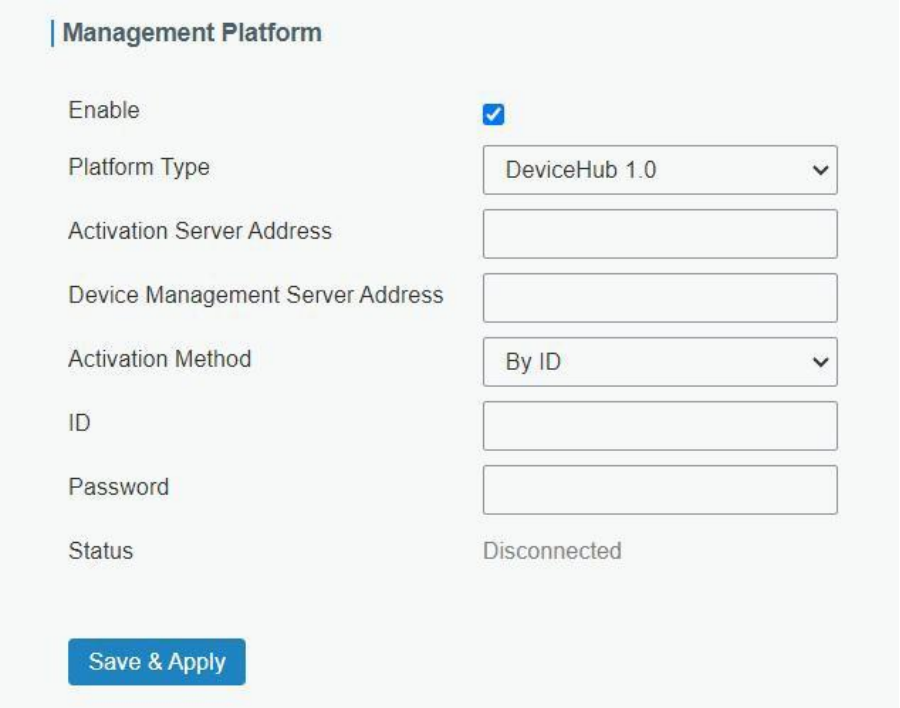


図 3-5-5-1

Management Platform	
Item	**Description**
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 はオプションとなります。
Status	ゲートウェイと管理プラットフォーム間の接続状態を表示します。
DeviceHub 1.0	
Activation ServerAddress	DeviceHub の IP アドレスまたはドメイン。
DeviceHubManagement Address	デバイスがデバイスハブに接続するためのURLアドレスです。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ためのアクティベーション方法を選択してください。オプションは"By Authentication ID"と"By ID"です。
Authentication Code	DeviceHubから生成された認証コードを入力してください。
ID	登録済みのDeviceHubアカウント（メールアドレス）とパスワードを入力してください。
Password	
DeviceHub 2.0	
Server Address	DeviceHub の IP アドレスまたはドメイン名。

表 3-5-5-1

3.5.5 Events

イベント機能は、特定のシステムイベントが発生した際に、Eメールでアラートを送信することが可能です。

3.5.5.1 Events

このページでは、アラームメッセージを確認することができます。

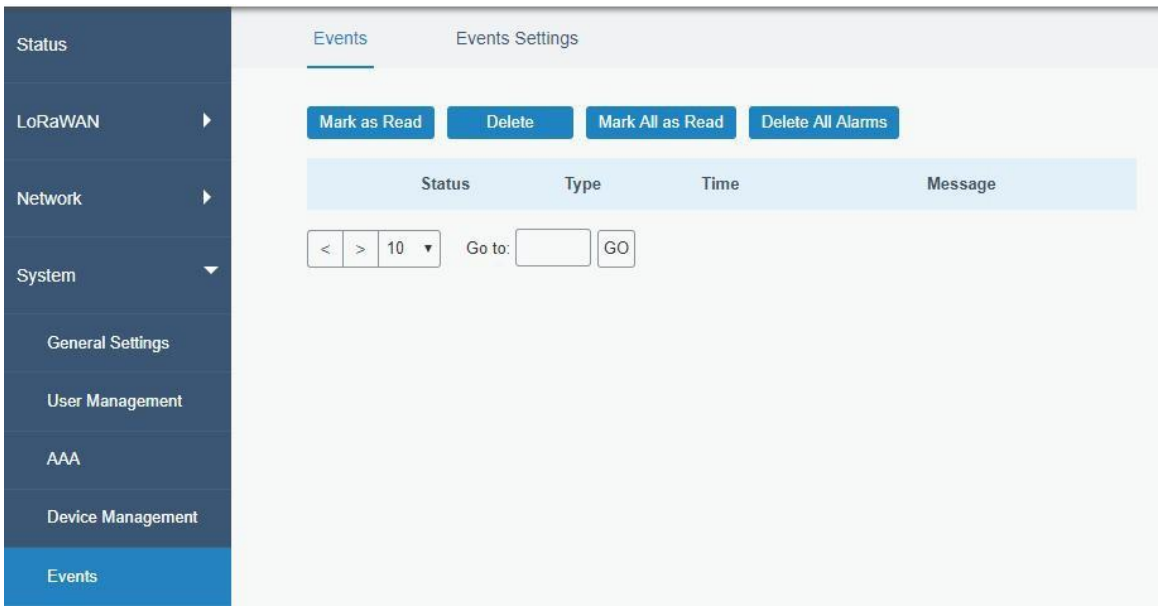


図 3-5-6-1

Events

Item	Description
Mark as Read	選択したイベントアラームを既読としてマークします。
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としてマークします。
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	アラーム対象となるイベントの種類を表示します。
Time	アラーム発生時刻を表示します。
Message	アラームの内容を表示します。

表 3-5-6-1 イベントパラメータ

3.5.5.2 Events Settings

このセクションでは、記録するイベントの種類と、変更が発生した際にメールおよびSMS通知を受け取るかどうかを決定できます。

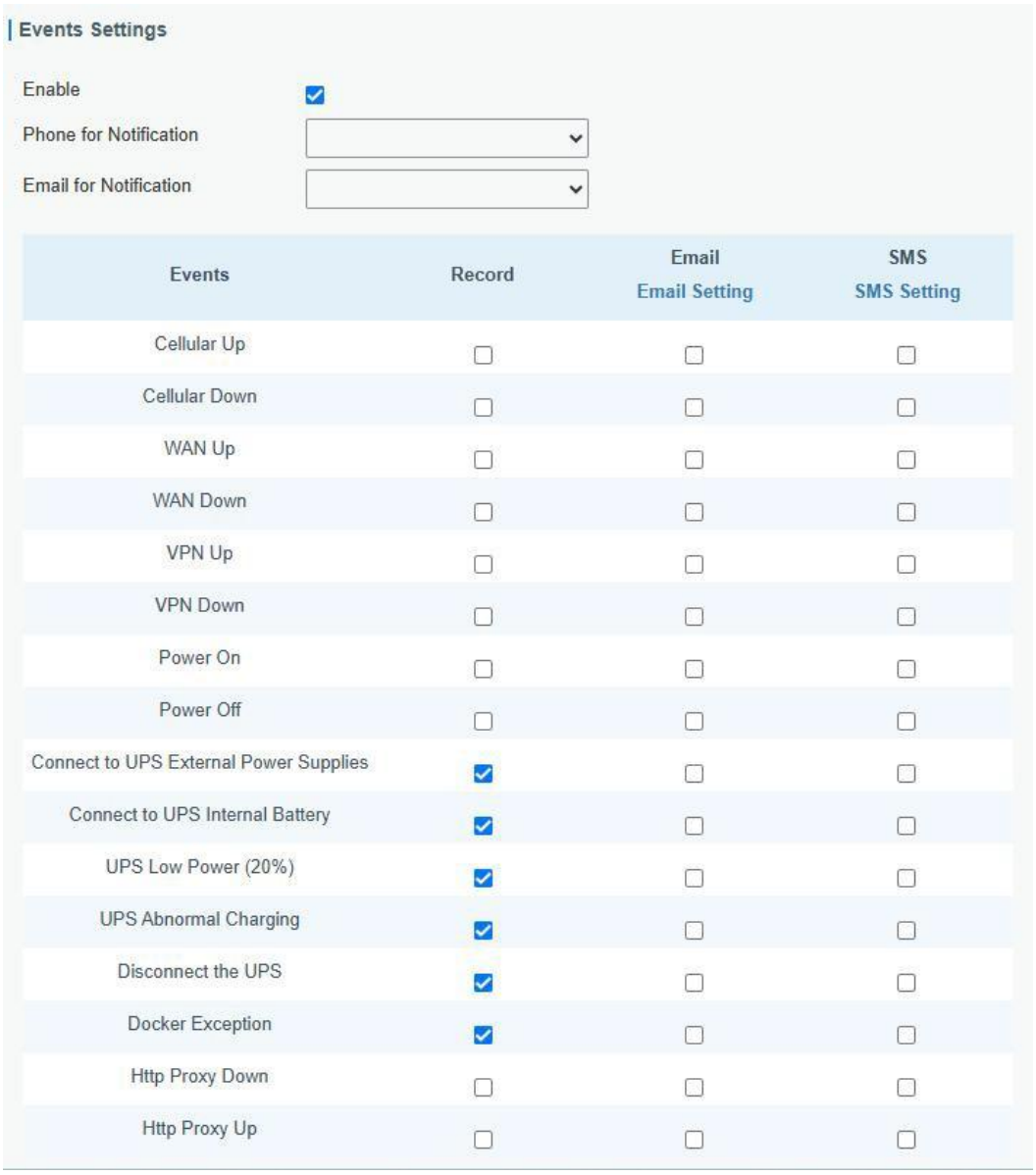


図 3-5-6-2

Event Settings	
Item	**Description**
Enable	"Events Settings"を有効にするには、チェックを入れてください。
Phone for Notification	SMSアラームを受信する電話グループを選択してください。
Email for Notification	メールアラームを受信するメールグループを選択してください。
Events	ゲートウェイが対応しているイベントの種類です。
Record	このオプションにチェックを入れると、イベントアラームの関連内容が"Event"ページに記録されます。
Email	このオプションにチェックを入れると、イベントアラームの関連内容がメールで送信されます。
Email Setting	クリックすると、"Email"ページにリダイレクトされ、メールグループを設定できます。
SMS	このオプションにチェックを入れると、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、"Phone"ページに移動し、電話グループリストを設定できます。

表 3-5-6-2 イベントパラメータ

Related Topics

メール設定

電話設定

3.6 Maintenance

このセクションでは、システムのメンテナンスツールと管理について説明します。

3.6.1 Tools

トラブルシューティングツールには、ping および traceroute が含まれます。

3.6.1.1 Ping

Pingツールは、外部ネットワークへのpingを実行するために設計されています。

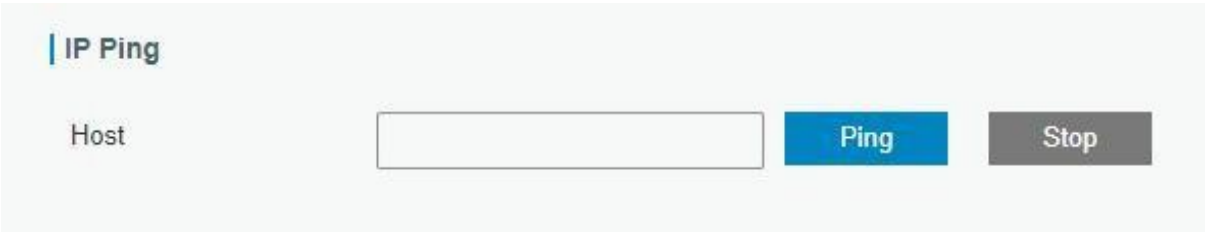


図 3-6-1-1

PING	
Item	**Description**
Host	ゲートウェイから外部ネットワークへPingを送信します。

表 3-6-1-1 IP Ping パラメータ

3.6.1.2 Traceroute

トレースルートツールは、ネットワークルーティングフェイルのトラブルシューティングに使

用されます。

図 3-6-1-2

Traceroute	
Item	**Description**
Host	検出対象となる宛先ホストのアドレスです。

表 3-6-1-2 トレースルートパラメータ

3.6.1.3 Packet Analyzer

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

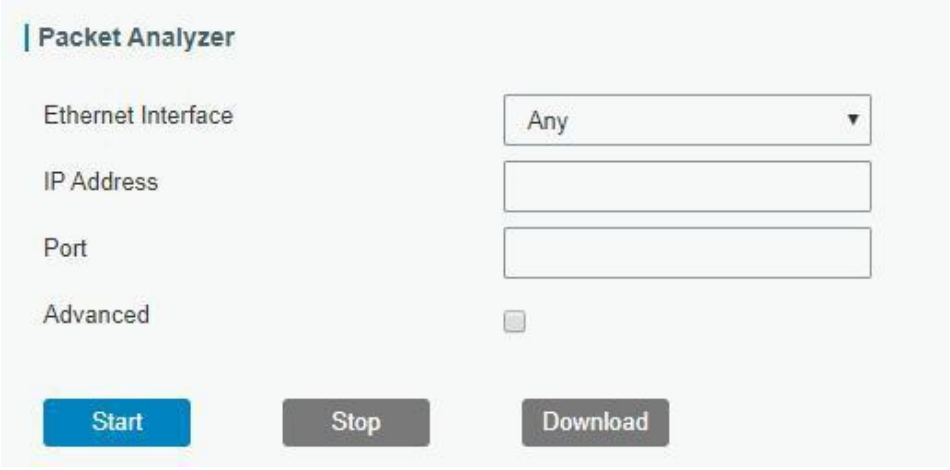


図3-6-1-3

Packet Analyzer	
Item	**Description**
Ethernet Interface	パケットをキャプチャするインターフェースを選択してください。
IP Address	ルーターがキャプチャするIPアドレスを設定してください。
Port	ルーターがキャプチャするポートを設定してください。
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のパラメータ

3.6.1.4 Qxdmlog

このセクションでは、QXDM ツールを介してセルラーモジュールの診断ログを収集することができます。

図 3-6-1-4

3.6.2 Schedule

このセクションでは、ゲートウェイでの定期的な再起動の設定方法について説明します。

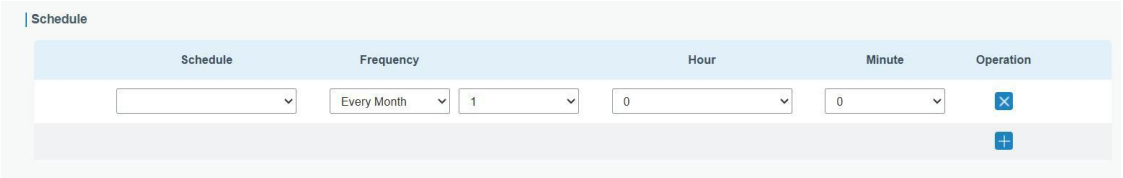


図 3-6-2-1

Schedule	
Item	**Description**
Schedule	スケジュールイベントの選択: 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てください。

表 3-6-2-1 スケジュールパラメータ

3.6.3 Log

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ています。ログに含まれるデータを確認することで、システムをトラブルシューティングする管理者やユーザーは、問題の原因や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の利用が可能であり、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 System Log

このセクションでは、ログファイルのダウンロード方法と、Web 上で最近のログを表示する方法について説明します。

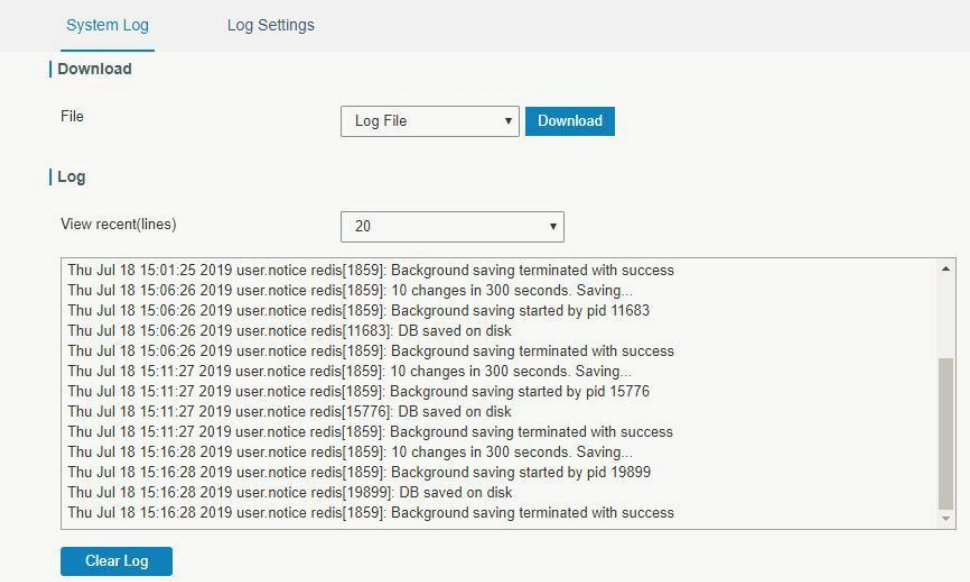


図 3-6-3-1

System Log	
Item	**Description**
Download	ログファイルをダウンロードします。
View recent (lines)	システムログの指定行を表示します。
Clear Log	現在のシステムログをクリアします。

表 3-6-3-1 システムログのパラメータ

3.6.3.2 Log Settings

このセクションでは、リモートログサーバーとローカルログの設定を有効にする方法について説明します。

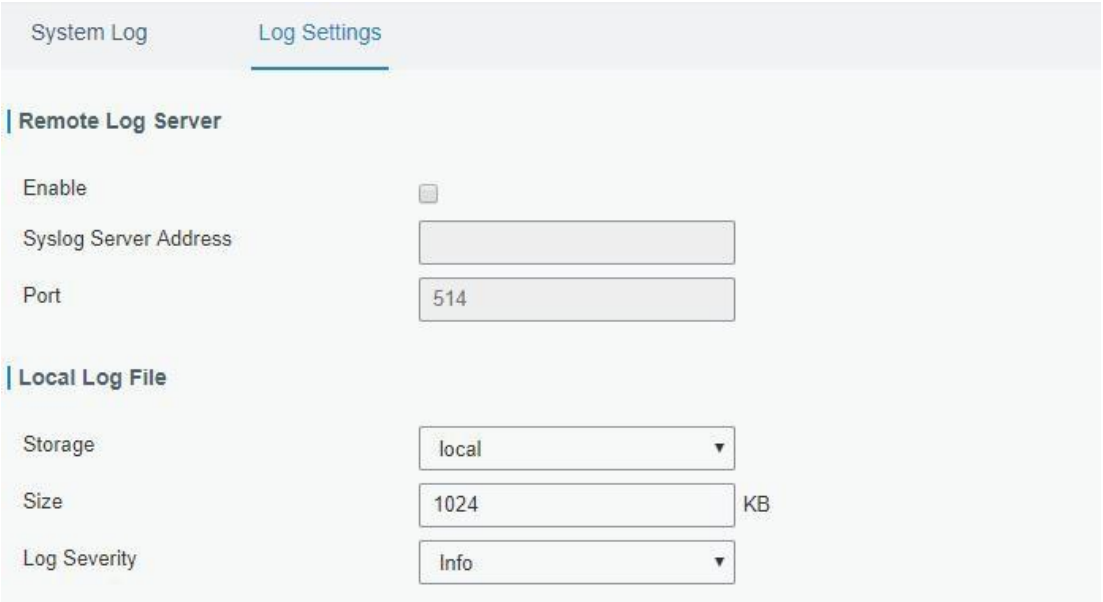


図3-6-3-2

Log Settings	
Item	**Description**

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）をご入力ください。
Port	リモートシステムログサーバーのポートを入力してください。
Local Log File	
Storage	ユーザーはログファイルをメモリに保存することができます。
Size	保存するログファイルのサイズを設定してください。
Log Severity	重大度のリストは、syslog プロトコルに準拠しています。

表 3-6-3-2 システムログのパラメータ

3.6.4 Upgrade

このセクションでは、Web 経由でゲートウェイのファームウェアをアップグレードする方法について説明します。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。

ご注意：ファームウェアのアップグレード中は、ウェブページ上での動作は一切お控えください。動作を行うとアップグレードが中断されるか、場合によっては機器が故障する可能性があります。

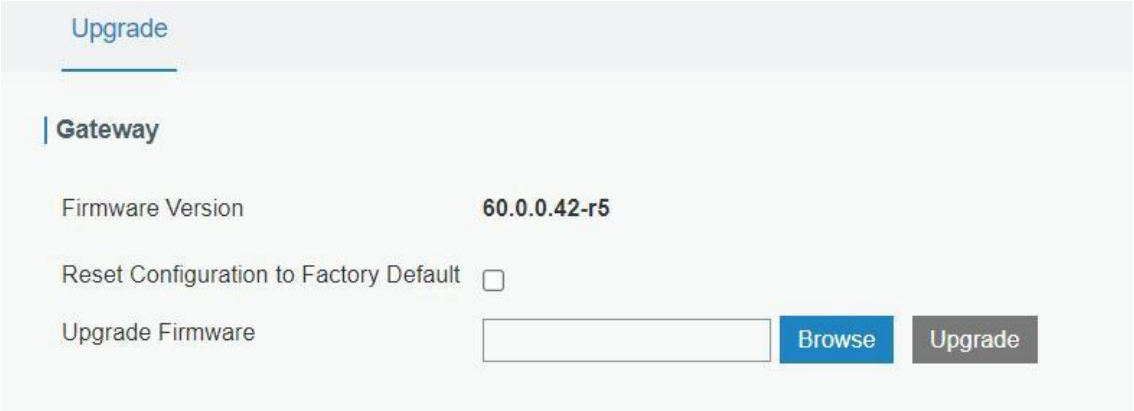


図 3-6-4-1

Upgrade	
Item	**Description**
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	このオプションを選択すると、アップグレード後にゲートウェイは工場出荷時のデフォルト設定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"をクリックするとファームウェアがアップグレードされます。

表 3-6-4-1 アップグレードパラメータ

Related Configuration Example

ファームウェアのアップグレード

3.6.5 Backup and Restore

このセクションでは、システム設定全体の完全な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設定の一部のみを複製する方法、設定ファイルをゲートウェイに復元する方法、および工場出荷時のデフォルトにリセットする方法について説明します。

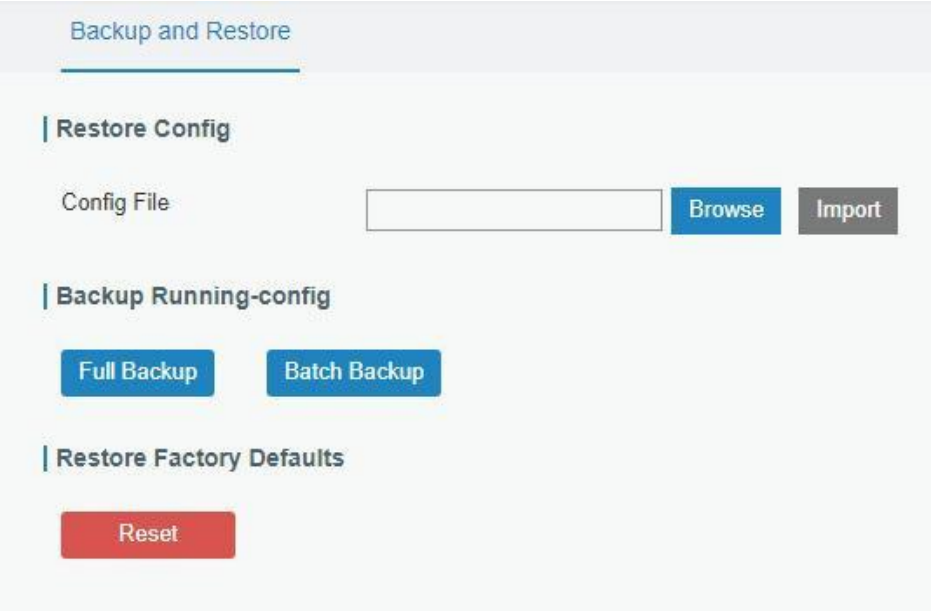


図 3-6-5-1

Backup and Restore	
Item	**Description**
Config File	"Browse"ボタンをクリックして設定ファイルを選択し、その後"Import"ボタンをクリックして設定ファイルをゲートウェイにアップロードしてください。
Full Backup	「フルバックアップ」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、パケットフォワーダーのゲートウェイ ID、すべての組み込み NS 設定、WAN の静的 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、現在の設定をエクスポートします。
Reset	"Reset"ボタンをクリックすると、工場出荷時のデフォルト設定にリセットされます。リセット処理が完了すると、ゲートウェイは再起動します。

表 3-6-5-1 バックアップおよび復元パラメータ

Related Configuration Example

工場出荷時のデフォルト設定への復元

3.6.6 Reboot

このページでは、ゲートウェイを再起動し、ログインページに戻ることができます。新しい設定が失われることを避けるため、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いたします。

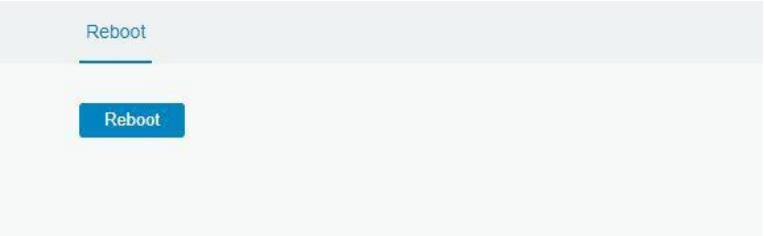


図 3-6-6-1

3.7 APP

3.7.1 Python

Python は、その明確な構文と可読性により人気を博しているオブジェクト指向プログラミング言語です。

Pythonはインタプリタ型言語として、コードの可読性を重視する設計思想を有しております。特に、コードブロックの区切りには中括弧やキーワードではなく空白のインデントを用いる点が特徴的で、C++やJavaなどの他言語と比較して、より少ない行数で概念を表現できる構文を備えております。この言語は、小規模から大規模まで、明瞭なプログラム記述を可能とする構文を提供し、その実現を目指しております。

ユーザーはPythonを用いてプログラムのプロトタイプを迅速に生成し、それをプログラムの最終インターフェースとして使用したり、より適切な言語で書き直したり、拡張されたクラスライブラリをカプセル化してPythonから呼び出せるようにすることができます。

本セクションでは、App-manager、SDKバージョン、拡張ストレージなどの関連する稼働状況を確認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アプリパッケージをここからインポートしたりすることも可能です。

3.7.1.1 Python

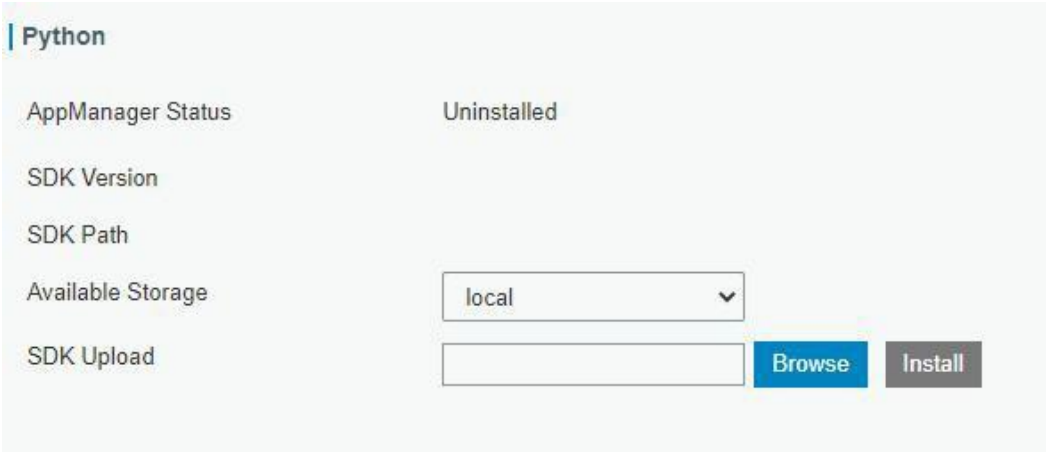


図 3-7-1-1

Python	
Item	**Description**
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 のインストール先パスを表示します。
Available Storage	SDKをインストールするための利用可能なストレージを選択してください。
SDK Upload	Python用SDK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 で管理されているアプリケーションのステータスを表示します。

表 3-7-1-1 Python パラメータ

3.7.1.2 App Manager Configuration

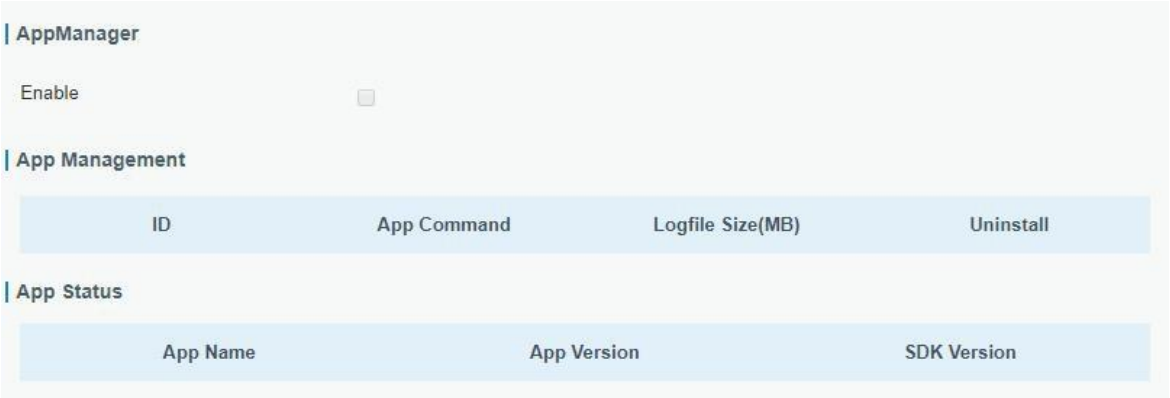


図 3-7-1-2

AppManager Configuration	
Item	**Description**
Enable	Python AppManagerを有効にした後、ユーザーは「Python」ウェブページ上の"Python"ボタンをクリックすることで、AppManagerによって管理されているアプリケーションの状態を確認できます。
App Management	
ID	インポートされたアプリのIDを表示します。
App Command	インポートされたアプリケーションの名称を表示します。
Logfile Size(MB)	ユーザー定義のログファイルサイズ。範囲：1～50。
Uninstall	アプリをアンインストールします。
App Status	
App Name	インポートされたアプリの名前を表示します。
App Version	インポートされたアプリのバージョンを表示します。
SDK Version	インポートされたアプリが基づいているSDKのバージョンを表示します。

表 3-7-1-2 APP マネージャーのパラメータ

3.7.1.3 Python App

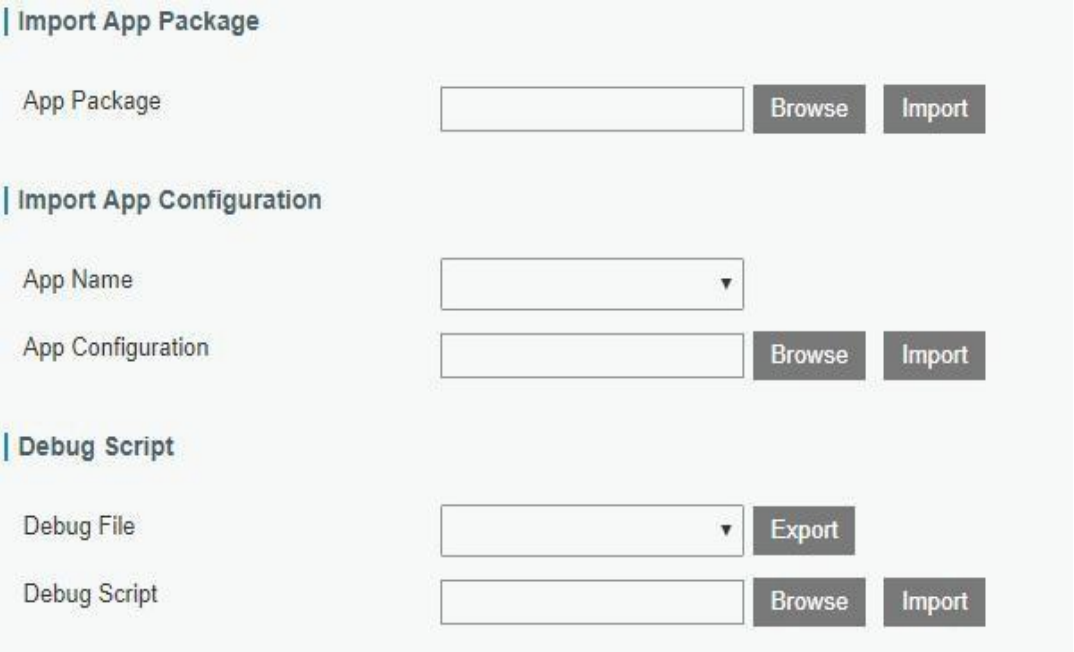


図 3-7-1-3

Python APP	
Item	**Description**
App Package	アプリパッケージを選択し、インポートしてください。
App Name	設定をインポートするアプリを選択してください。
App Configuration	設定ファイルを選択し、インポートしてください。
Debug File	スクリプトファイルをエクスポートします。
Debug Script	デバッグ対象のPythonスクリプトを選択し、インポートしてください。

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（IoT）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および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ており、パレット内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。詳細なガイダンスおよびドキュメントについては、Node-RED 公式ウェブサイトをご参照ください。

3.7.2.1 Node-RED

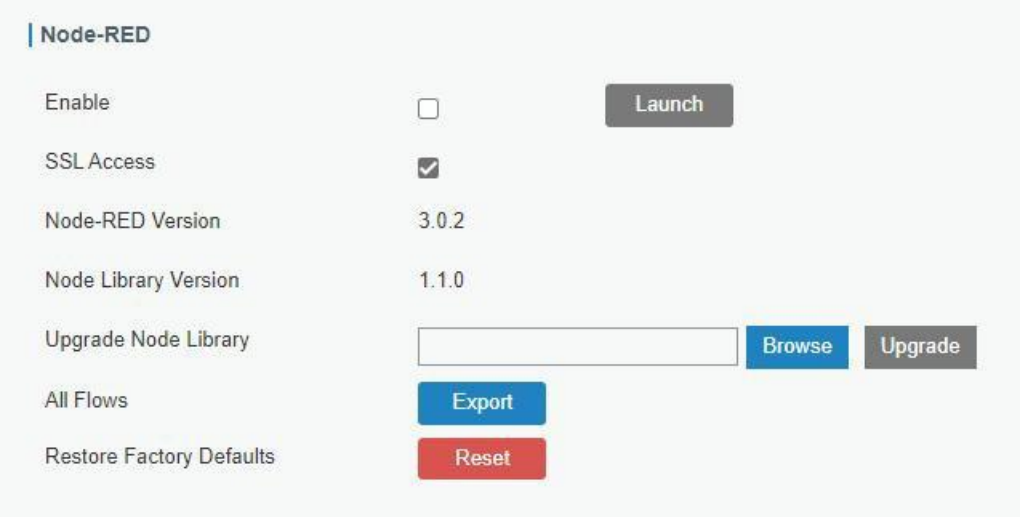


図 3-7-2-1

Node-RED	
Item	**Description**
Enable	Node-RED を有効にします。
Launch	クリックすると、Node-RED の Web GUI を起動します。
SSL Access	HTTPSサービス経由でのみNode-REDのWeb GUIにアクセスできるようにします。
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場合にのみ更新可能です。
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 FactoryDefault	Node-RED のすべての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のカスタマイズされたノードライブラリを提供しております。

図 3-7-2-2

Node Library	
Node	**Description**
LoRa Input	ゲートウェイから LoRaWAN® パケットを受信します。これは、ネットワークサーバーが有効になっている場合にのみ機能します。
LoRa Output	LoRaWAN®ノードへダウンリンクコマンドを送信します。
Device Filter	デバイス EUI により、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。これには、**[General> >] > [** 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	メールを送信します。STMPオプションを「ゲートウェイと同じ」に選択された場合、**System > General Settings > SMTP** 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。これは携帯電話が接続されている場合のみ機能します。
SMS Output	SMSメッセージを送信します。これは、セルラーが接続されている場合にのみ機能します。

表 3-7-2-2 ノードライブラリパラメータ

Related Configuration Example

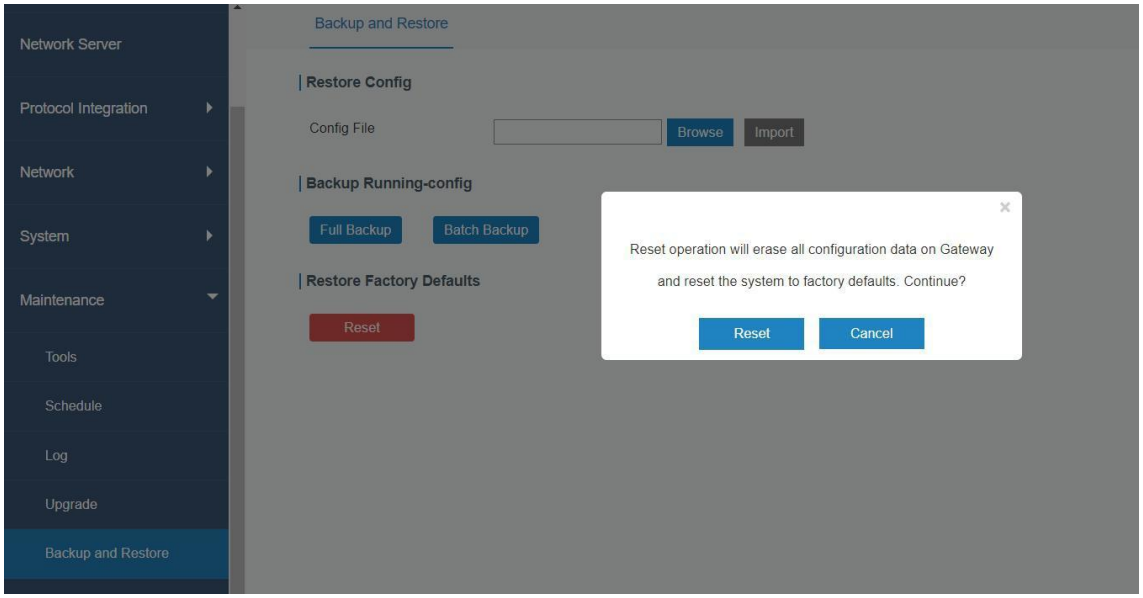
Node-RED

Chapter 4 Application Examples

4.1 Restore Factory Defaults

Method 1:

ウェブインターフェースにログインし、**Maintenance >**」に進みます。「 」ボタンをクリックすると、工場出荷時のデフォルト設定にリセットするかどうかを確認するメッセージが表示されます。その後、**Backup**ボタンをクリックしてください。



その後、ゲートウェイは再起動し、直ちに工場出荷時の設定に復元されます。

SYSランプが点灯したままの状態になり、ログインページが再度表示されるまでお待ちください。これにより、ゲートウェイが正常に工場出荷時設定にリセットされたことを確認できます。

Related Topic

工場出荷時設定への復元

Method 2:

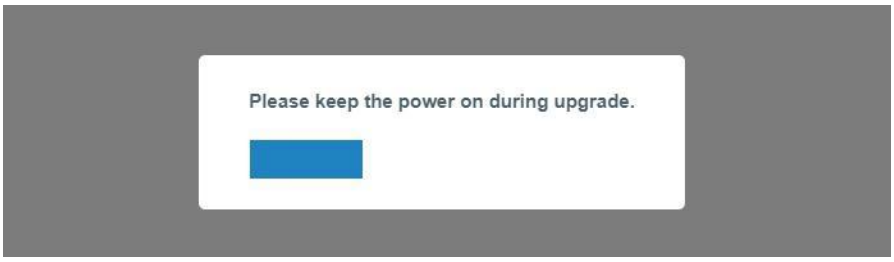
ゲートウェイのリセットボタンを見つけ、SYS LED が点滅するまで 5 秒以上リセットボタンを押し続けてください。

4.2 Firmware Upgrade

ゲートウェイのファームウェアをアップグレードされる前に、まずMilesightテクニカルサポートまでご連絡いただくことをお勧めいたします。ゲートウェイのファームウェアファイルの拡張子は「.bin」です。
ファームウェアファイルを入手後、以下の手順に従っ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」に移動します。
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てください。
3. "Upgrade"をクリックすると、ゲートウェイがファームウェアファイルの正しさを確認します。問題がなければ、ファームウェアがゲートウェイにインポートされ、アップグレードが開始されます。
4. アップグレード後、ブラウザからゲートウェイのWeb GUIを開き、アップグレードが正常に完了したかどうかをご確認ください。

Before opening, it is suggested to clean the caches of browser.



Related Topic

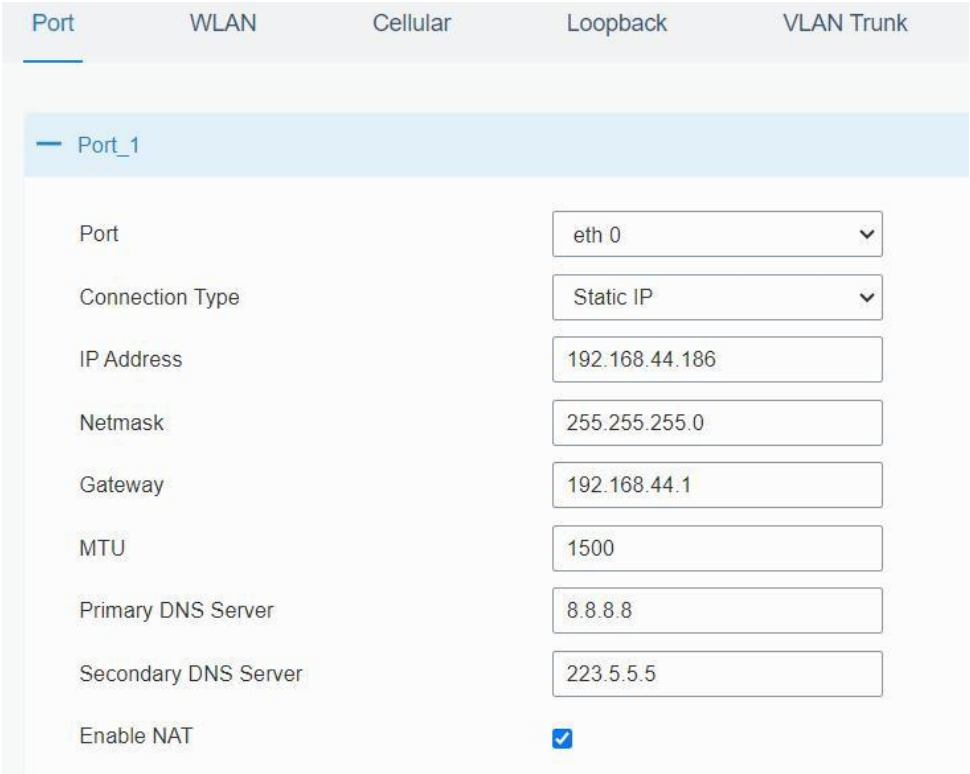
アップグレード

4.3 Network Connection

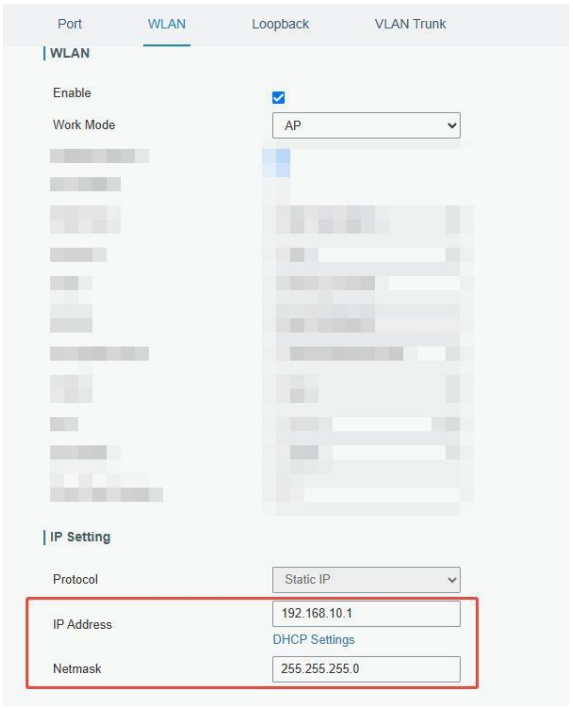
ゲートウェイは、ネットワーク接続を設定するための複数の方法を対応しています。

4.3.1 Ethernet Connection

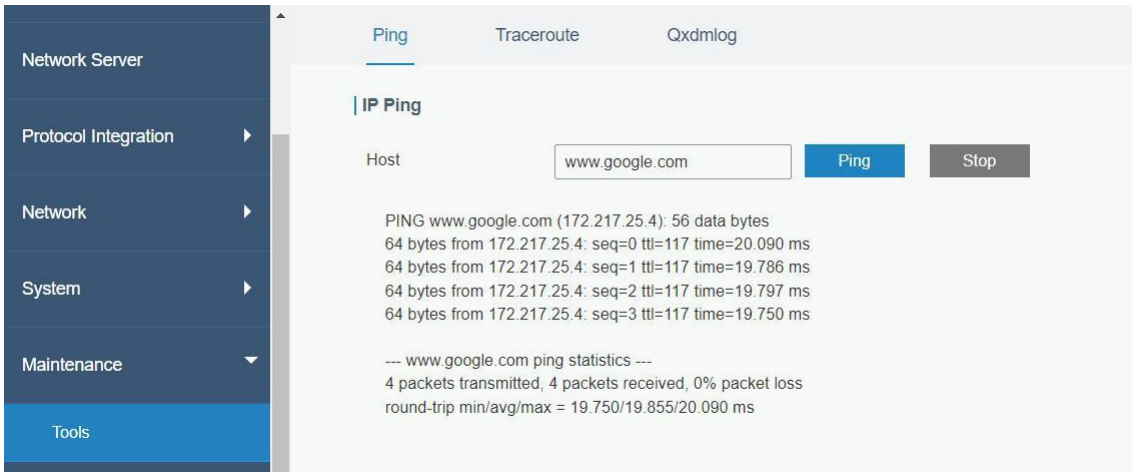
1. "Network > Interface > Port"ページに移動し、接続タイプを選択してイーサネットポートの設定を行ってください。"Save & Apply"をクリックすると設定が有効になります。



Note: イーサネットポートのIPアドレス変更時にIP衝突が発生した場合は、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機器に接続してください。
3. "Maintenance > Tools > Ping"に移動し、ネットワーク接続を確認してください。

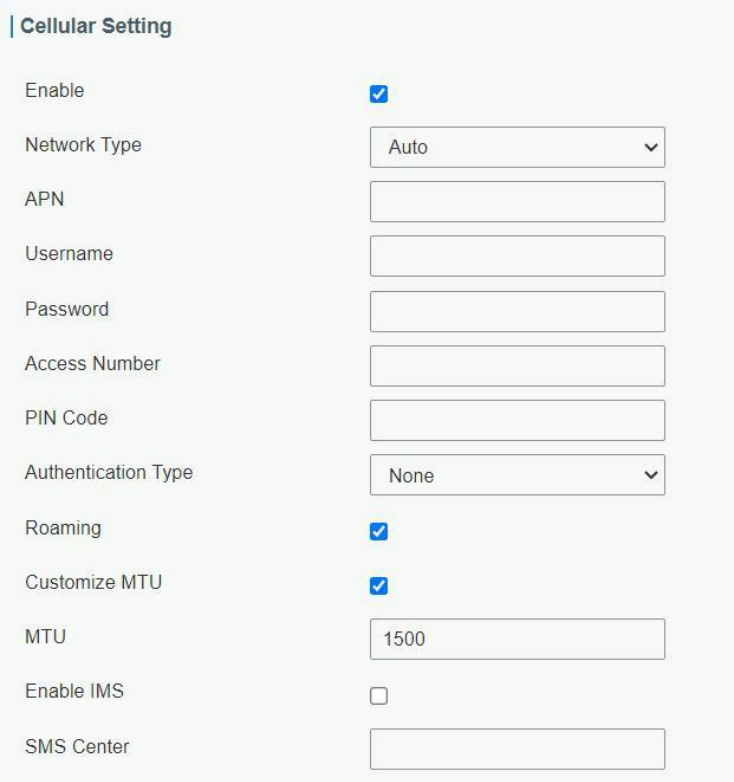


Related Topic

ポート設定

4.3.2 Cellular Connection (Cellular Version Only)

1. "Network > Interface > Cellular > Cellular Setting"に移動し、SIM カードの必要なセルラー情報を設定してください。"Save"および"Apply"をクリックすると設定が有効になります。



2. "Status > Cellular"に移動し、携帯電話接続の状態を確認してください。"Connected"と表示されている場合、SIM カードのダイヤルアップは正常に完了しています。

Related Topic

携帯電話の設定

携帯電話の状態

4.4 Wi-Fi Application Example

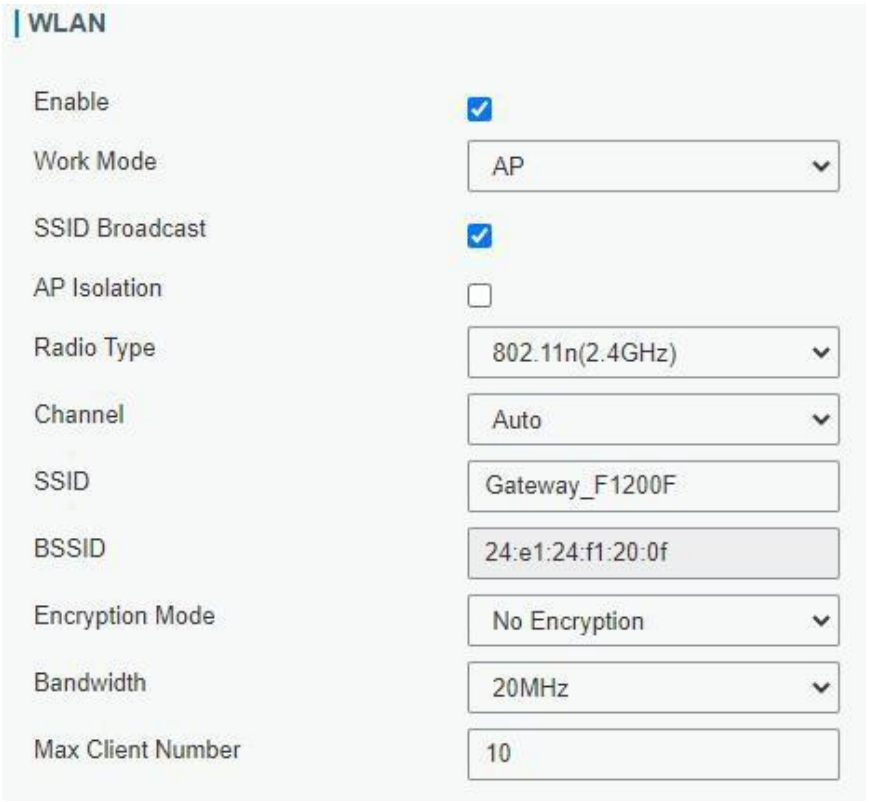
4.4.1 AP Mode

Application Example

UG67をAPとして設定し、ユーザーやデバイスからの接続を許可します。

Configuration Steps

1. 「ネットワーク ＞ インターフェース ＞ WLAN」に移動し、以下の通り無線パラメータを設定してください。



すべての設定が完了しましたら、"Save"ボタンと"Apply"ボタンをクリックしてください。

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てください。

「Status > WLAN」に移動すると、APの設定および接続中のクライアント/ユーザー情報を確認できます。

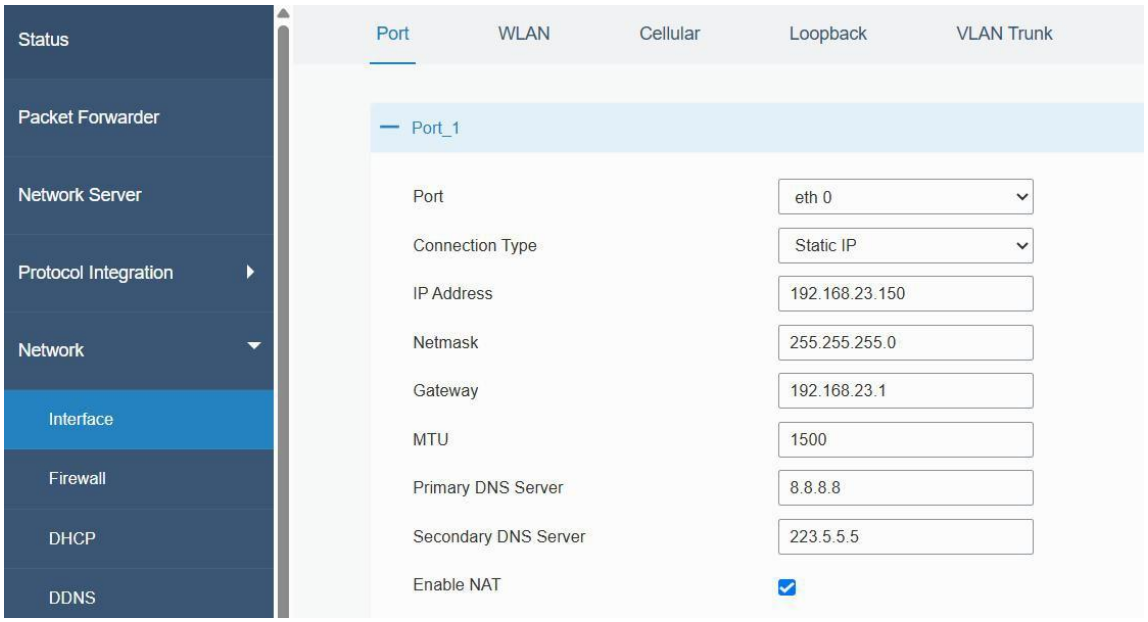
4.4.2 Client Mode

Application Example

UG67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アクセスします。

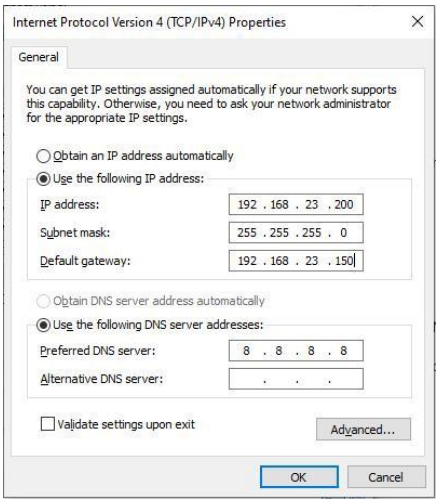
Configuration Steps

1. **Network > Interface > Port** ポートページに移動し、接続タイプを「**Static IP** 」に

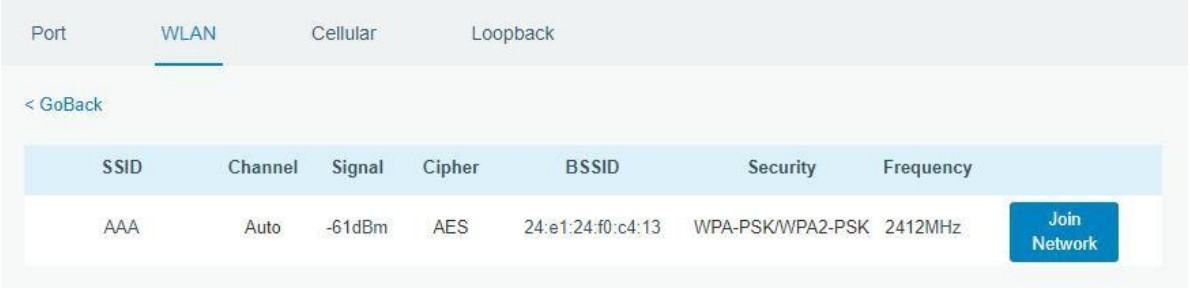


選択し、イーサネットWANポートのIPアドレスを設定してください。

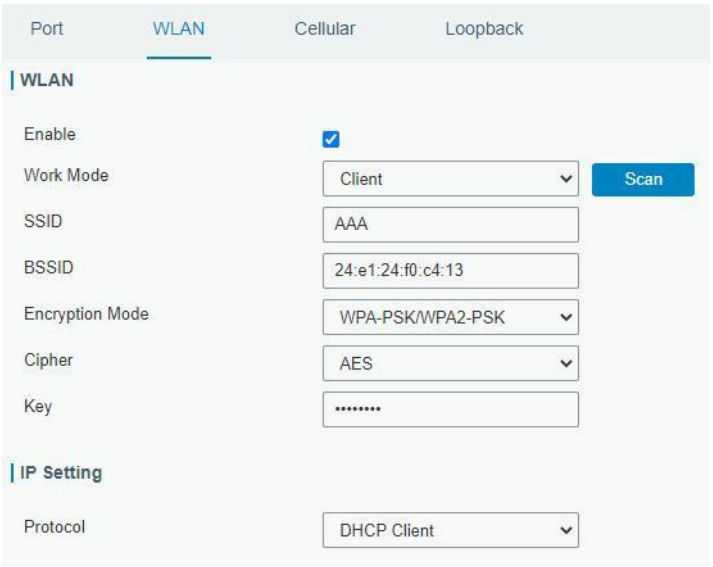
2. PCをUG67のETHポートに直接、またはPoEインジェクター経由で接続してください。
3. コンピューターにIPアドレスを手動で割り当てます。Windows 10システムを例に説明いたします：



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にアクセスしてください。
5. **Network > WLAN** に移動し、「 をクリックしてWiFiアクセスポイントを検索します。

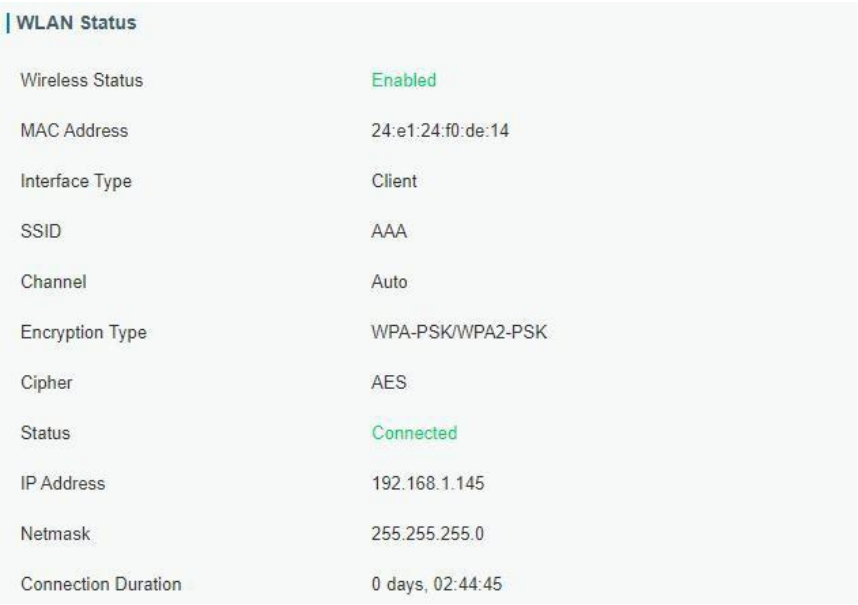


6. アクセスポイントを選択し、「**Join Network**」をクリックした後、アクセスポイントのパスワードを入力してください。

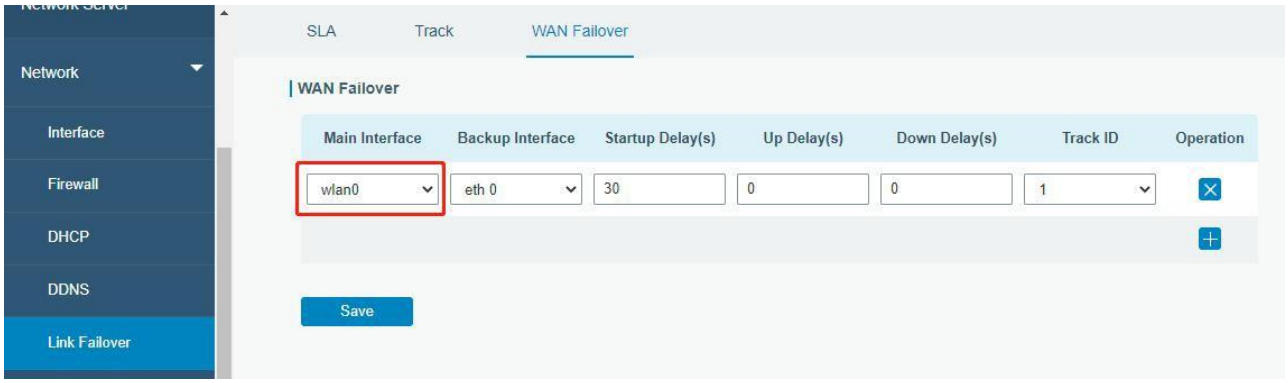


すべての設定が完了しましたら、「**Save** および「**Apply** ボタンをクリックしてください。

7. **Status> WLAN** に移動し、クライアントの接続状況をご確認ください。



8. **Network > WAN** に移動し、wlan0 をメインインターフェースに切り替えてください。そうすることで、ゲートウェイが Wi-Fi 経由でネットワークにアクセスできるようになります。



Related Topic

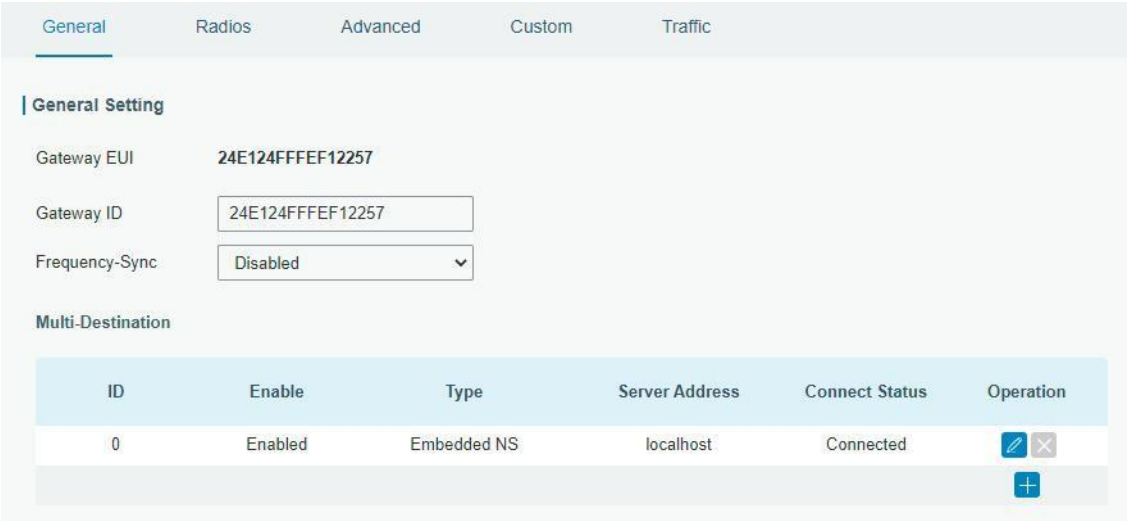
WLAN設定

WLANステータス

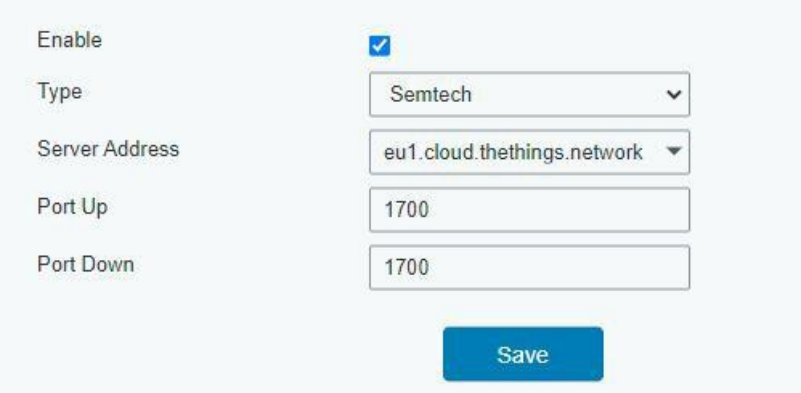
4.5 Packet Forwarder Configuration

UG67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ご確認ください。

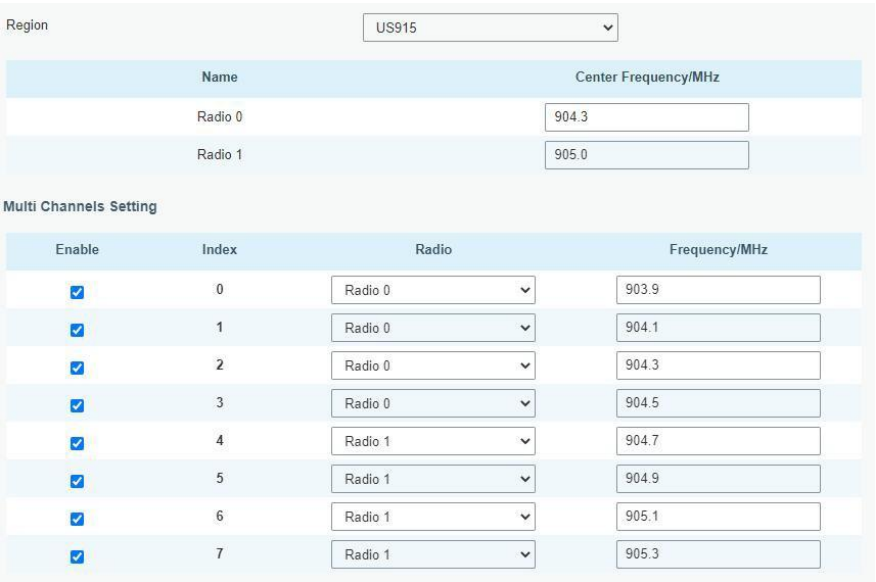
1. **Packet Forwarder >** に移動してください。



2. 「  」をクリックし、新しいネットワークサーバーを追加します。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てください。



3. **Packet Forwarder > Radio** 無線ページに移動し、中心周波数とチャネルを設定します。ゲートウェイとネットワークサーバーのチャネルは同一である必要があります。



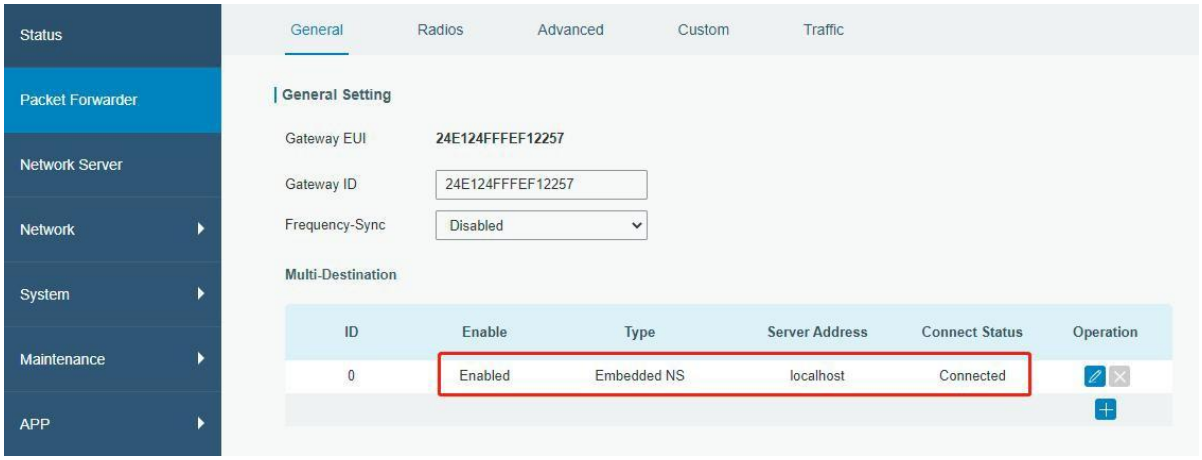
4. ネットワークサーバーページでゲートウェイを追加してください。ネットワークサーバー接続の詳細については、Milesight IoT対応ポータルをご参照ください。

4.6 Network Server Configuration

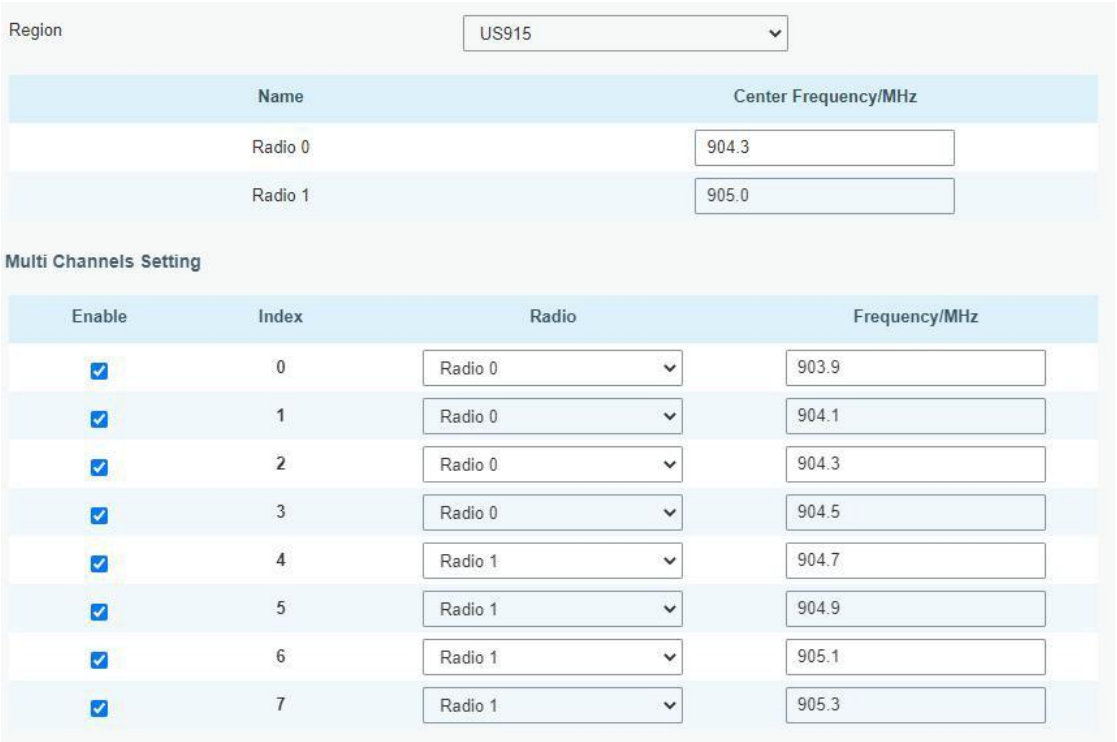
ゲートウェイはLoRaWAN®ネットワークサーバーとして機能し、LoRaWAN®エンドデバイスのデータを受信・分析し、様々なシステムとの柔軟な連携を実現します。

4.6.1 Connect to Milesight IoT Cloud

1. **Packet Forwarder**設定ページに移動し、組み込みネットワークサーバーを有効にしてください。

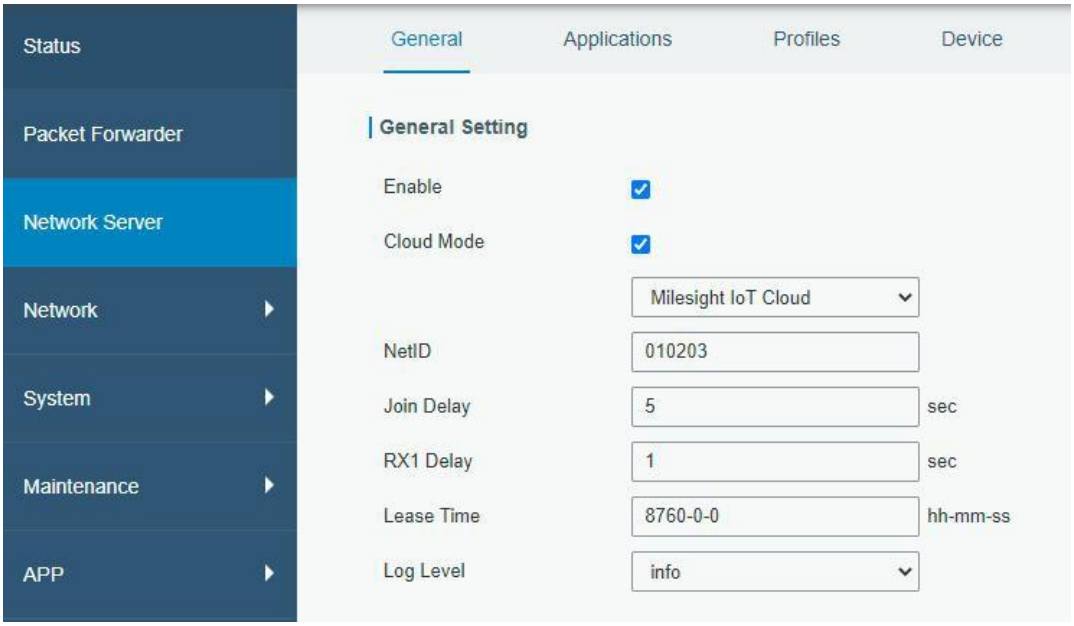


2. **Packet Forwarder > Radio** ＞無線ページに移動し、中心周波数とチャンネルを設定

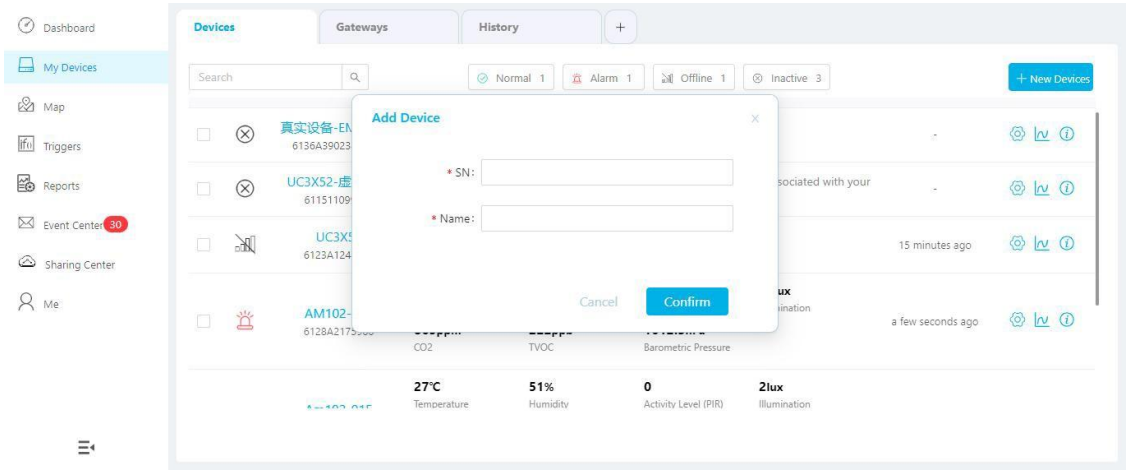


してください。ゲートウェイとエンドデバイスのチャンネルは同一である必要があります。

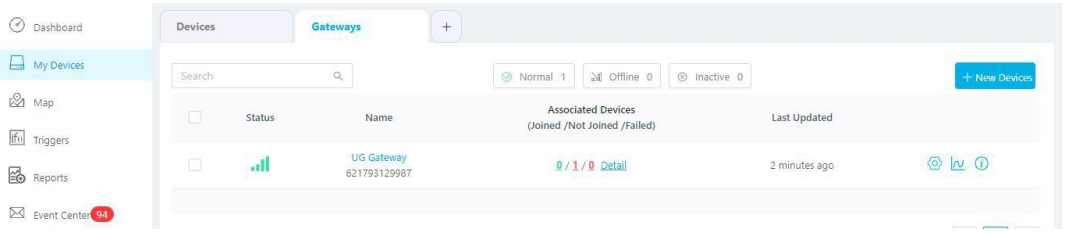
3. **Network Server > General** ページに移動し、ネットワークサーバーと"Cloud Mode"を有効にした後、「Milesight IoT Cloud」モードを選択してください。



4. Milesight IoT Cloudにログインしてください。その後、「**My** ページに移動し、「+新規デバイス」をクリックして、SN経由でゲートウェイをMilesight IoT Cloudに追加してください。ゲートウェイは"Gateway"メニュー下に追加されます。

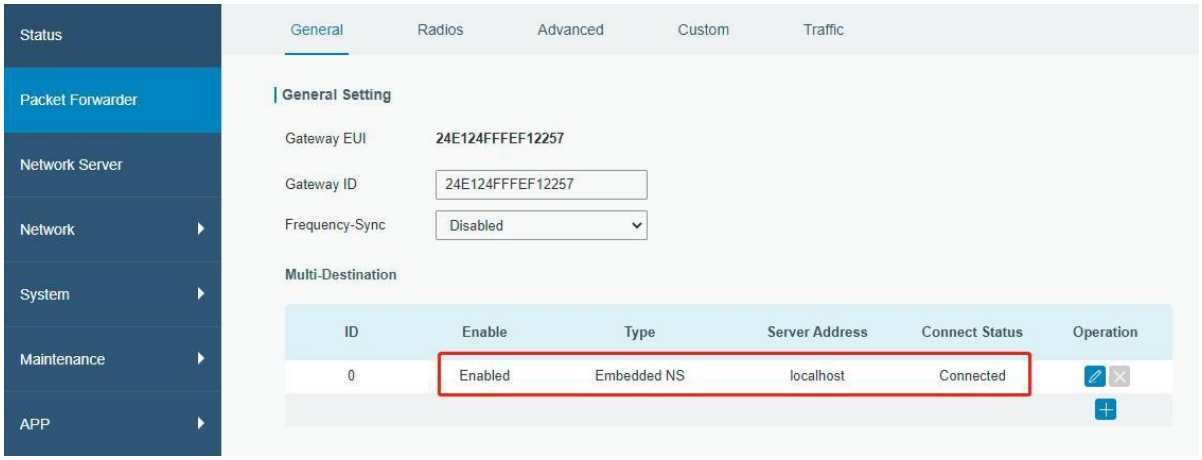


5. ゲートウェイはMilesight IoT Cloud上でオンライン状態となります。

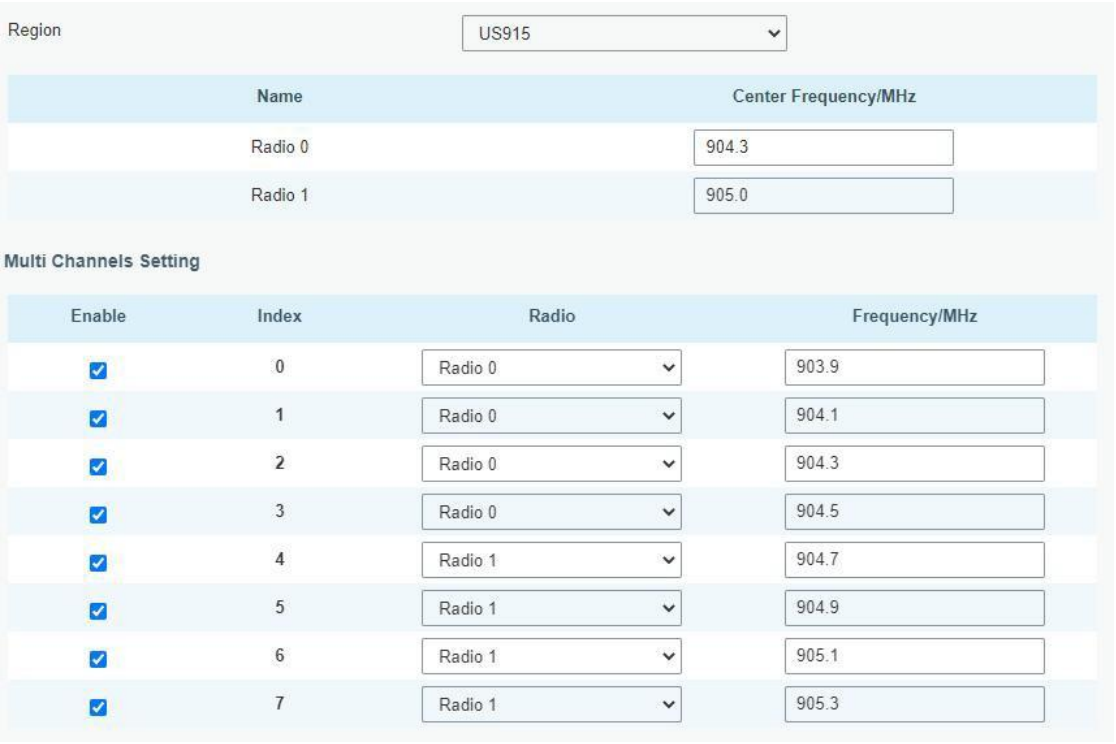


4.6.2 Add End Devices

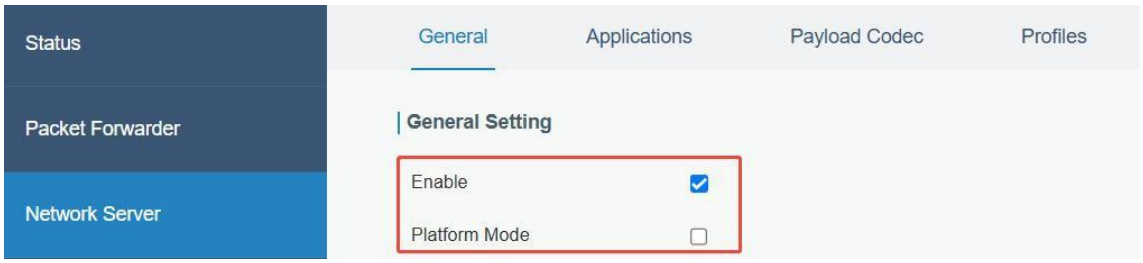
1. **Packet Forwarder > General**設定ページに移動し、組み込みNSを有効にしてください。



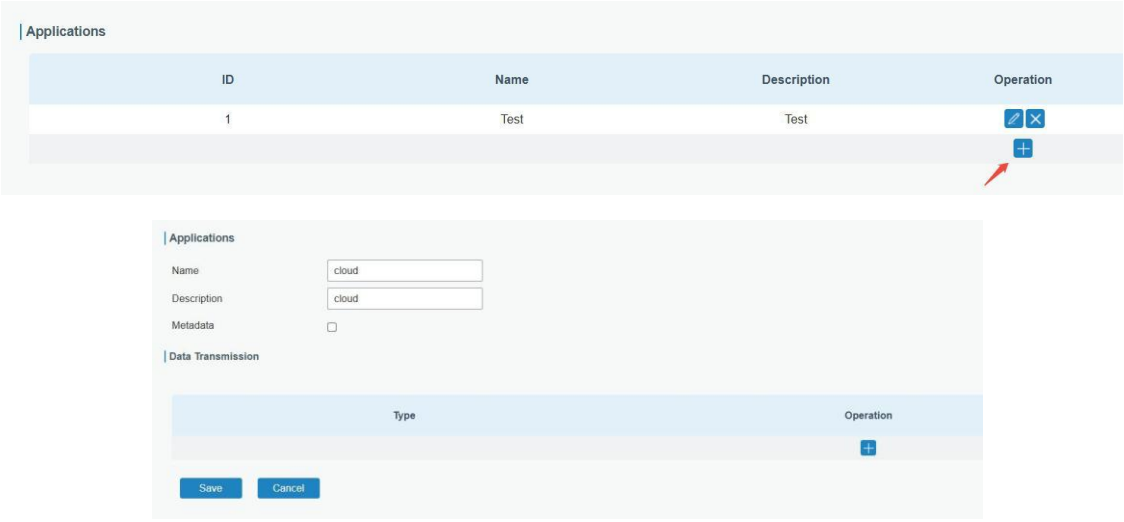
2. **Packet Forwarder > Radio** ＞無線ページに移動し、中心周波数とチャンネルを設定してください。ゲートウェイとエンドデバイスのチャンネルは同一である必要があります。



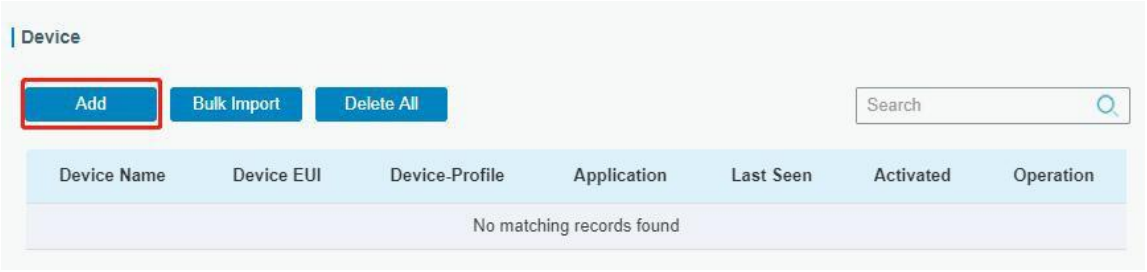
3. **Network >** ページに移動し、ネットワークサーバーを有効にしてください。



4. **Network Server** ページに移動し、アプリケーションを追加してください。



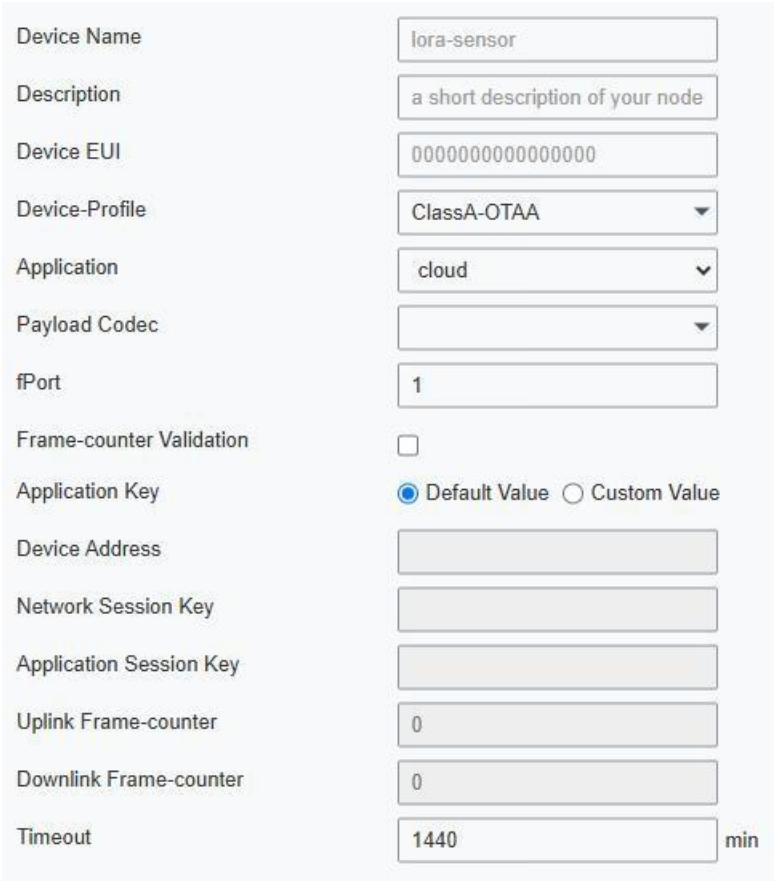
5. **Network Server > Device** デバイスページに移動し、「**Add** をクリックして LoRaWAN®ノードデバイスを追加してください。また、**Bulk Import** をクリックすると、



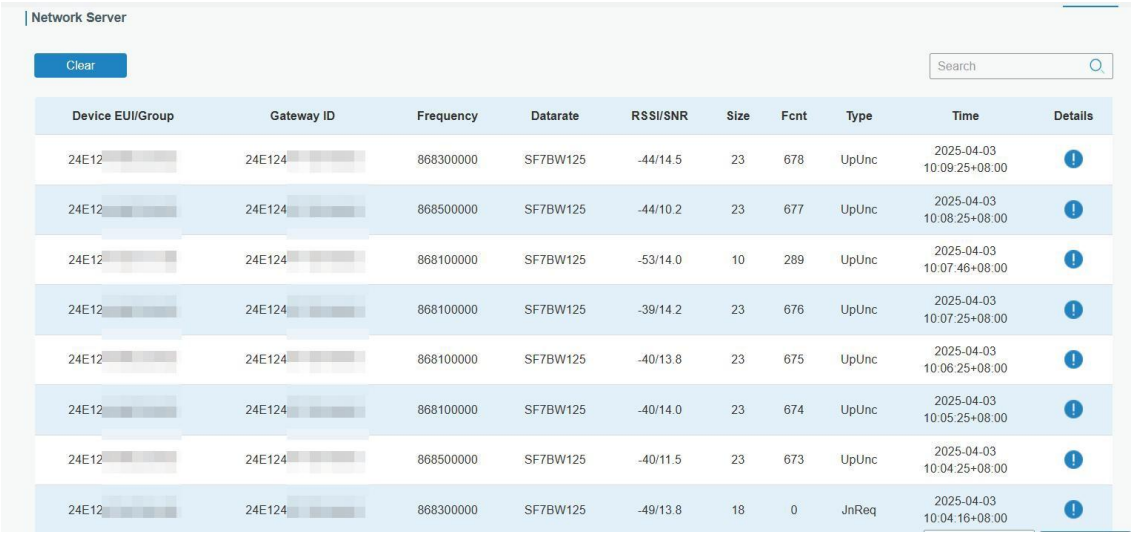
テンプレートを使用してデバイスを一括で追加することも可能です。

6. エンドデバイスの情報を入力し、**Save&Apply**をクリックしてください。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ご確認いただけます。Milesightエンドデバイスのデフォルト設定は以下の通りです：

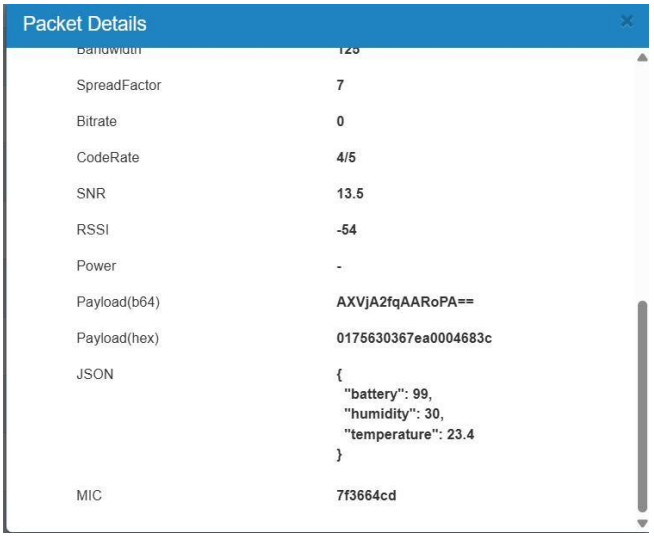
- デバイス EUI：デバイス本体に記載されています。
- デバイスプロファイル： OTAA タイプファイル
- ペイロードコーデック：モデルを選択してくださいポート：85
- アプリケーションキー：デフォルト値を選択してください。ランダムキーを使用する場合は、カスタム値を選択してください。
- タイムアウト：デバイスがオンライン/オフラインの状態を判断するまでの時間です。



7. **Network Server >** ページに移動し、このデバイスからのアップリンクがあるかどうかをご確認ください。



Details をクリックすると、パケットの詳細とデコード結果を確認できます。



4.6.3 Send Data to Device

1. **Network Server > Packets**に移動し、ネットワークサーバーリスト内のパケットを確認して、デバイスがネットワークに正常に参加していることをご確認ください。

2. デバイス EUI を入力するか、ダウンリンク送信に必要なマルチキャストグループを選択してください。その後、ダウンリンクコマンドとポートを入力してください。

3. "Send"をクリックしてください。

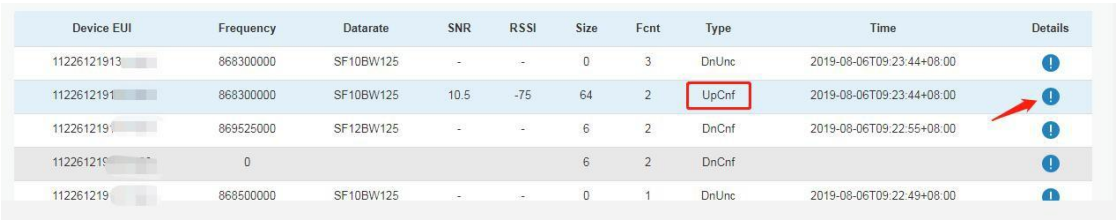
4. ネットワークサーバーリスト内のパケットを確認し、デバイスがメッセージを正常に受信したことをご確認ください。"Confirmed"を有効にすることをお勧めいたします。マルチキャスト機能は確認付きダウンリンクに対応しておりません。

リストを更新するには"Refresh"をクリックするか、リストの自動更新周波数を設定することができます。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。

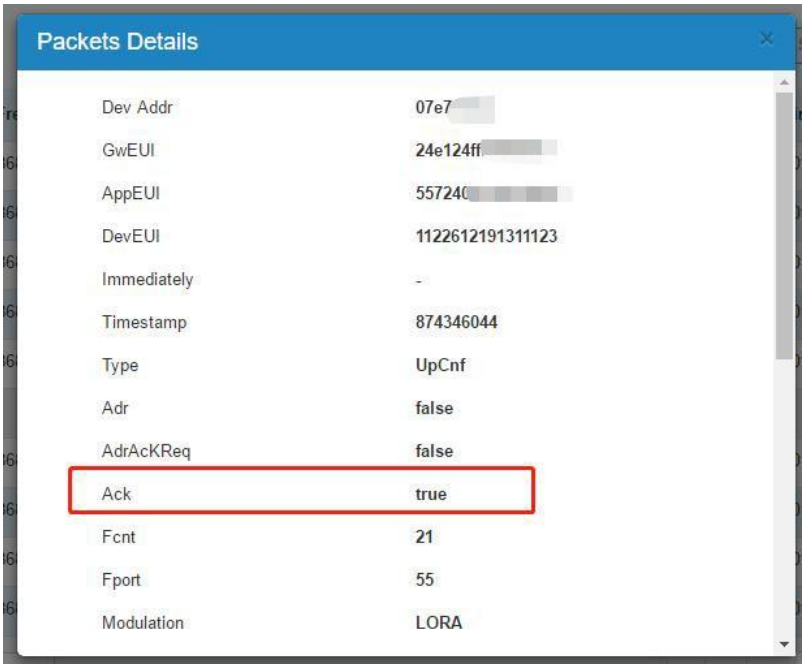
このパケットのタイプはDnCnf（ダウンリンク確認済みパケット）であり、パケットの色が灰色の場合、少なくとも1つのメッセージがキューに存在するため、現在パケットを送信できないことを意味します。パケットの記録が白色の場合は、パケットが正常に配信されたことを示します。

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パケットを受信した場合、次回配信時に「**ACK**」を返信します。

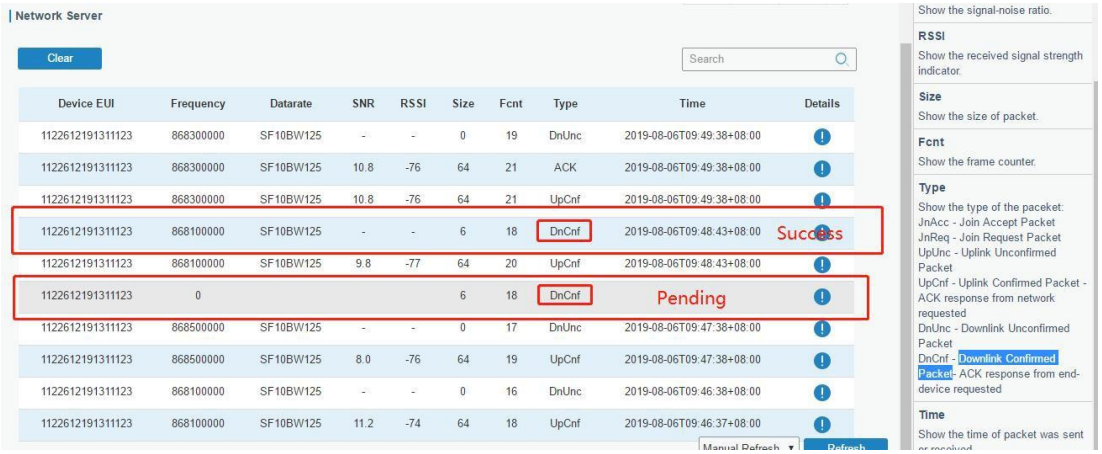


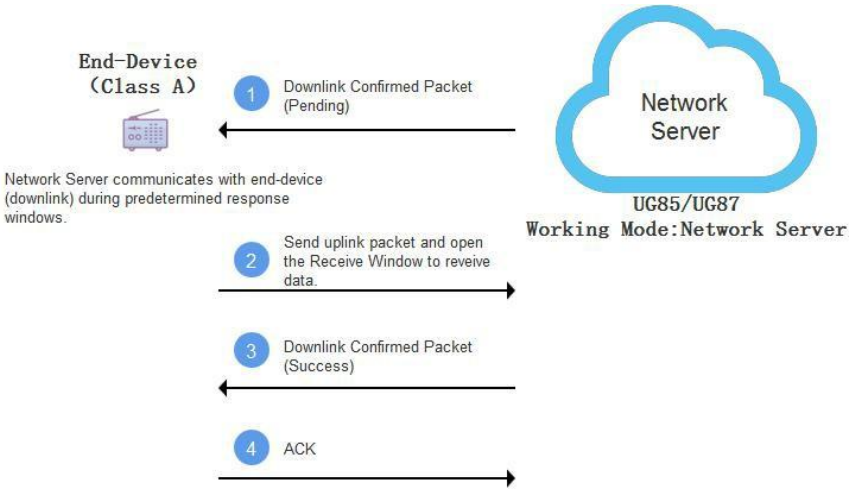
Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Type	Time	Details
11226121913	868300000	SF10BW125	-	-	0	3	DnUnc	2019-08-06T09:23:44+08:00	
1122612191	868300000	SF10BW125	10.5	-75	64	2	UpCnf	2019-08-06T09:23:44+08:00	
112261219	869525000	SF12BW125	-	-	6	2	DnCnf	2019-08-06T09:22:55+08:00	
112261219	0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

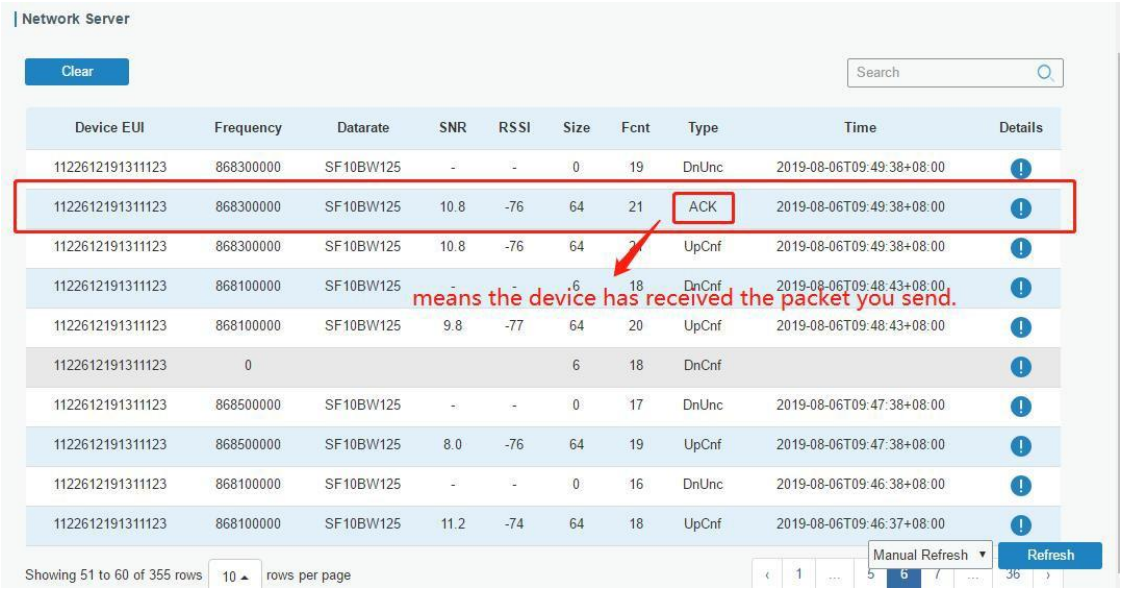


ACKが「**true**」である場合、デバイスがこのパケットを受信したことを意味します。

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で初めて、ネットワークサーバーがデバイスにデータを送信します。







Related Topic

パケット

4.6.4 HTTP/MQTT Server

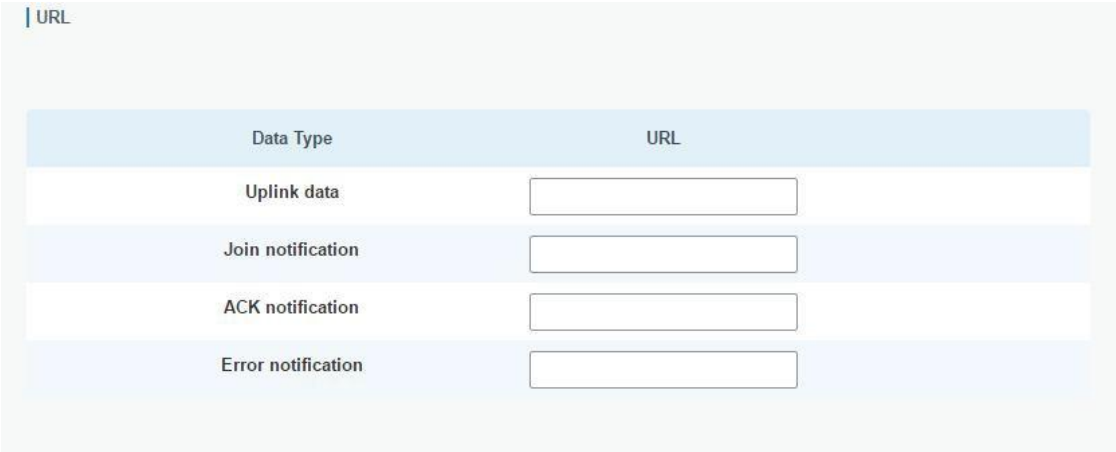
本ゲートウェイでは、MQTT、HTTP、またはHTTPSプロトコルに対応し、別のサーバーアドレスへデータを送信するためのデータ転送プロトコルを選択することが可能です。

1. 編集するアプリケーションを選択するには、**Network >** に移動してください。
2. 「  」をクリックし、データ転送タイプを追加してください。

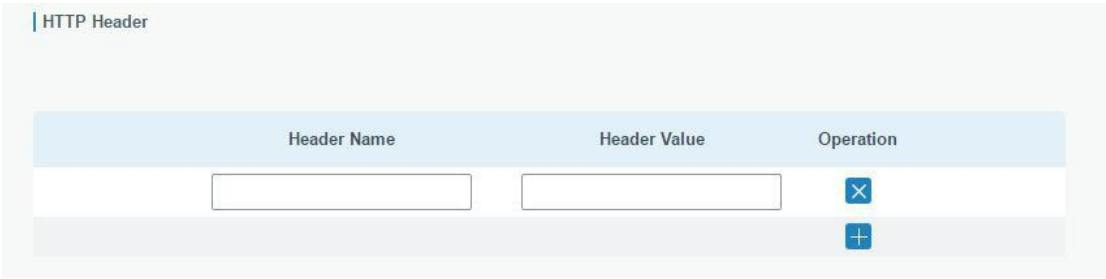
HTTP or HTTPS：

ステップ1：伝送プロトコルとしてHTTPまたはHTTPSを選択してください。

ステップ2：送信先のURLを入力します。異なる種類のデータを異なるURLに送信することが可能です。



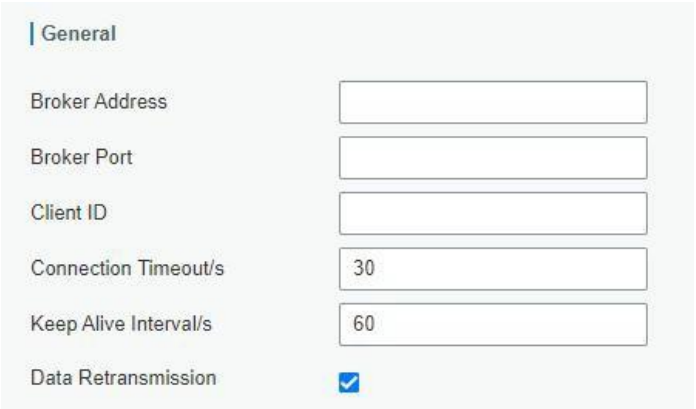
HTTP(s)サーバーへのアクセス時にユーザー認証情報が必要な場合は、ヘッダー名とヘッダー値を入力してください。



MQTT：

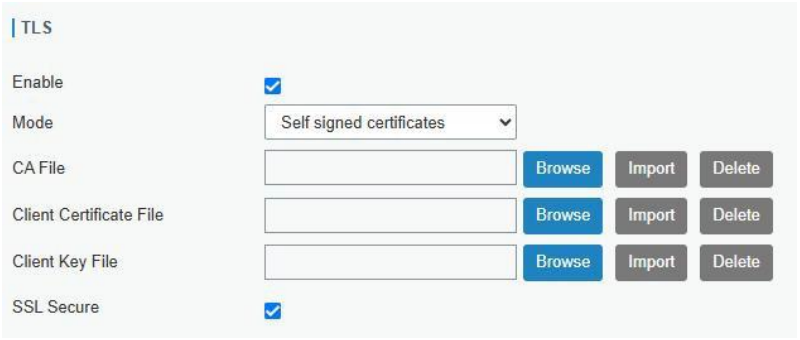
ステップ1：伝送プロトコルとしてMQTTを選択し、設定モードを「手動設定」に設定してください。

ステップ2：MQTTブローカーの基本設定を入力してください。

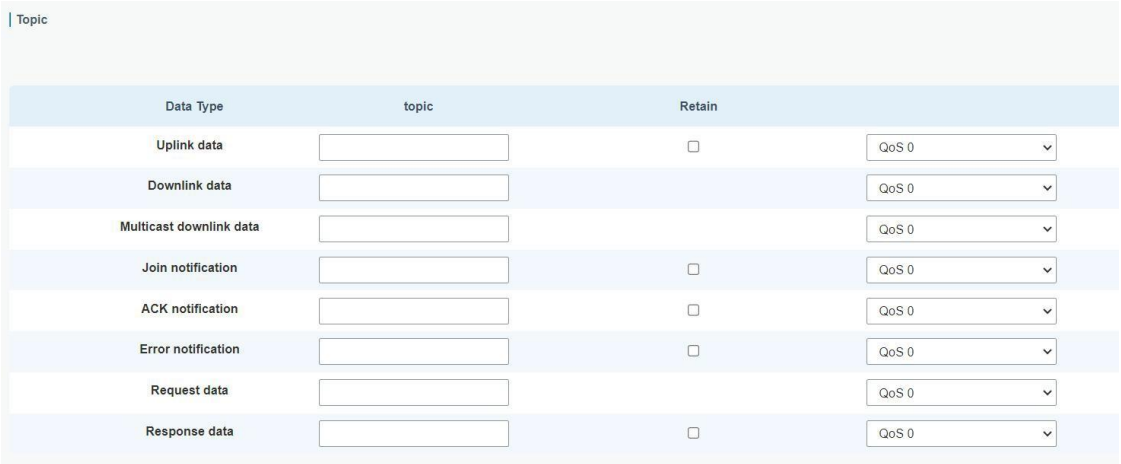


ステップ3：サーバーが要求する認証方法を選択してください。
認証方法としてユーザー認証を選択された場合、認証用のユーザー名とパスワードを入力する必要があります。

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用のトピックを入力し、QoSを選択してください。

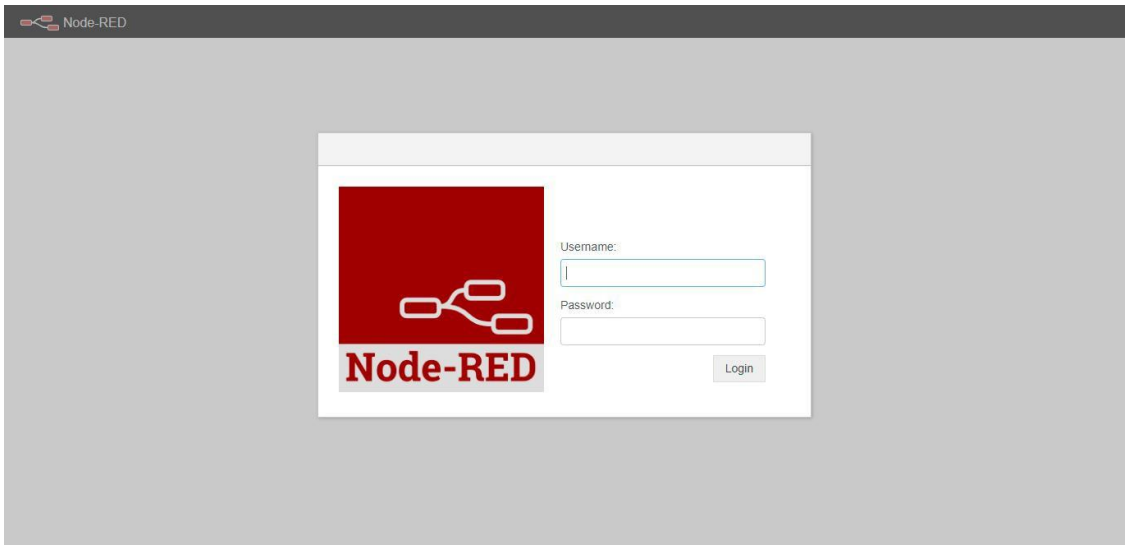


4.7 Node-RED

4.7.1 Start the Node-RED

1. 「アプリ > Node-RED」に移動し、Node-RED 機能を有効にしてください。

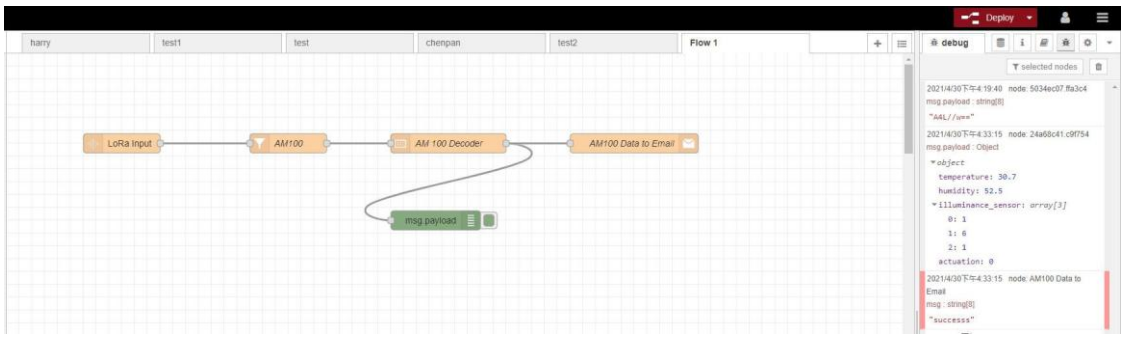
2. 有効化後、"Start"をクリックしてNode-REDのWeb GUIに移動し、ゲートウェイと同じユーザー名とパスワードでログインしてください。



4.7.2 Send Data by Email

Application Example

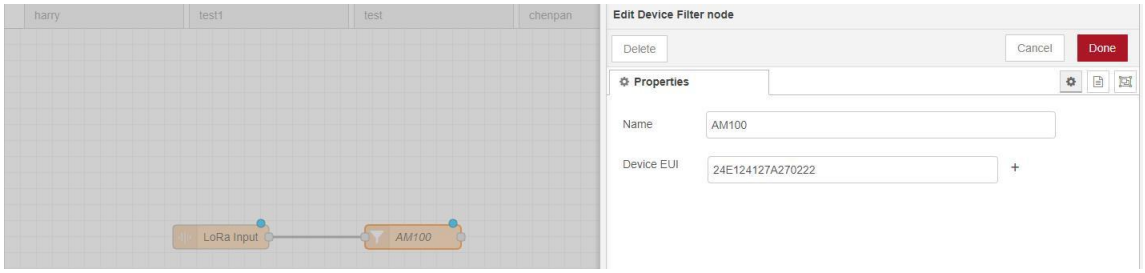
AM102デバイスのデータをメールで送信します。



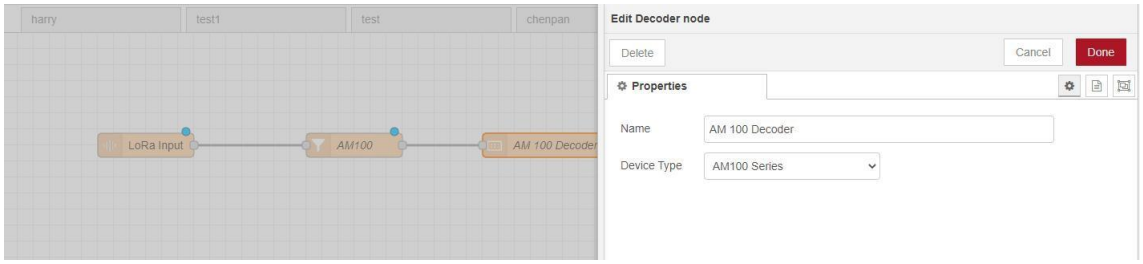
Configuration Steps

1. 「LoRa Input」ノードを追加します。追加前に、ネットワークサーバーモードが有効化されており、LoRaWANデバイスがネットワークに参加していることをご確認ください。

2. 複数のデバイスを追加し、特定のデバイスのデータのみが必要な場合は、「LoRa Input」ノードの後ろに「デバイスフィルター」ノードを追加し、対象デバイスのEUIを入力してください。



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

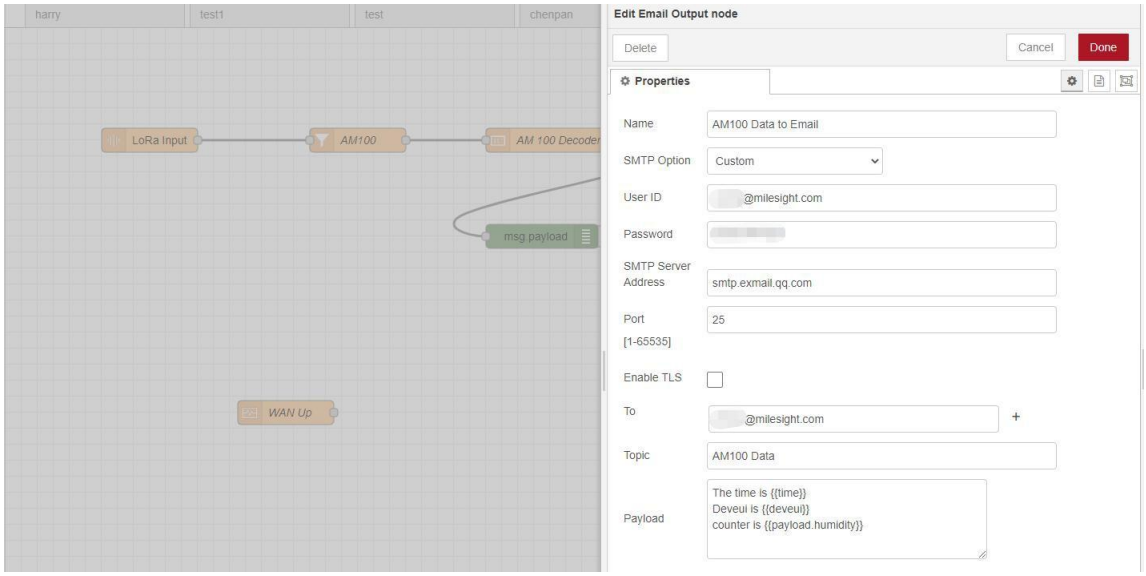


4. 「メール出力」を追加し、SMTPクライアントの設定、宛先メールアドレス、および内容を記入してください。例：

The time is {{time}}

Deveui is {{deveui}}

Humidity is {{payload.humidity}}



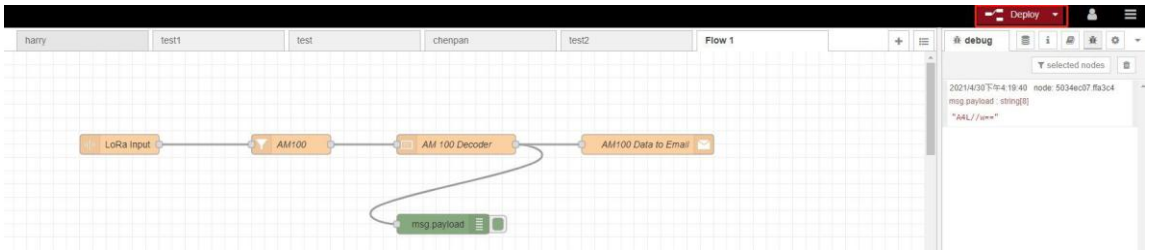
ご注意：

1) SMTPオプションを「Same as Gateway」に設定される場合は、「System -> General Settings-> SMTP」に移動し、SMTPクライアントを設定してください。

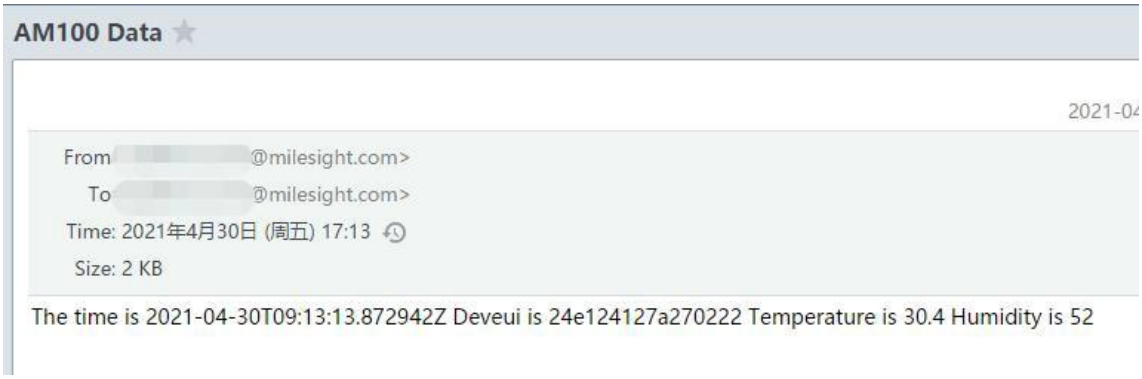
2) LoRaWANノードデータを呼び出す基本形式は*{{property name}}*となります。メールまたはSMSのペイロード形式に関する詳細は、"Help"ページをクリックしてご確認ください。

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. 設定が完了しましたら、"Deploy"をクリックしてすべての設定を保存してください。



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



Related Topic

Node-RED

[END]