産業用LoRaWAN®
ゲートウェイ

UG56

ユーザーガイド

はじめに

Milesight UG56 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。UG56は、自動フェイルオーバー/フェイルバック、広範囲な動作温度、ハードウェアウォッチドッグ、VPN、ギガビットイーサネットなどの充実した機能を備え、ネットワーク上で堅牢な接続を実現します。

本ガイドでは、UG56 LoRaWAN® ゲートウェイの設定および動作方法について説明します。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。

対象読者

本ガイドは、主に以下のユーザーを対象としています：

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

関連ドキュメント

ドキュメント	説明
UG56 データシート	UG56 LoRaWAN® ゲートウェイのデータシート。
UG56 クイックスタートガイド	UG56 LoRaWAN® ゲートウェイのクイックインストールガイド。

適合宣言

UG56は、CE、FCC、およびRoHSの必須要件およびその他の関連規定に適合しています。

ご不明な点がございましたら、
Milesight テクニカルサポートに問い合わせてください：
Eメール：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

改訂履歴

日付	ドキュメント版	説明
2022年8月9日	V1.0	初期版
2023年4月21日	V 1.1	1. BACnetサーバー機能を追加 2. ペイロードコーデック機能を追加 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. Packet Forwardにデータ再送信機能を追加 5. ビーコンの時間オフセットを追加 6. 「プロファイル」ページに8つのプロファイルが事前設定されています
2024年8月2日	V 1.2	1. セルラー回線のMTUカスタマイズおよびIMS機能を追加しました。 2. OpenVPN接続用のovpnファイルのインポートに対応しました； 3. パケットフィルタ機能を対応； 4. デフォルトのWi-Fi接続パスワードを追加しました； 5. SMTPクライアント設定にユーザー名を追加しました； 6. BACnetオブジェクトタイプを追加し、オブジェクトインスタンスのカスタマイズに対応しました。
2025年1月8日	V 1.3	1. MQTTデータの再送信および保持オプションを追加しました； 2. 「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し、BACnet/IPオプションを削除しました； 3. 「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しました； 4. BACnetオブジェクトのイベント検出機能およびNotificationクラスオブジェクトタイプを追加します； 5. Modbusサーバー機能を追加します； 6. WireGuard機能を追加； 7. セルラーサブネットマスクおよびDNSサーバーのカスタマイズ機能を追加； 8. DeviceHub 2.0 に対応しました； 9. Node-REDのSSLアクセスオプションを追加しました。 10. ネットワークパケットアナライザ機能を追加します。
2025年4月3日	V 1.4	1. FUOTA機能を追加； 2. MQTT Last Willメッセージ機能を追加； 3. デバイスを追加する際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に更新しました； 6. Web GUIへのアクセス手順を更新しました。

2025年5月29日	V 1.4.1	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、デフォルトのデバイスIDを更新しました； 3. デバイス一覧において、「アクティブ項目」を「ステータス項目」に変更します； 4. BACnetグローバルオブジェクトの追加に対応しました； 5. BACnetオブジェクトの自動追加に対応しました； 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しました。
2025年8月13日	V 1.5	1. 「Packet Forwarder-Traffic」ページにデータ項目を追加しました 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した； 4. すべてのデバイス情報のエクスポートに対応しました； 5. 「Packets」ページにダウンロードキューのクリア機能を追加しました； 6. BACnetグローバルオブジェクトタイプを追加； 7. Modbusグローバルオブジェクト機能およびサーバーIDタイプを追加しました。 8. Modbusオブジェクトのコピー機能を追加します。
2025年12月24日	V 1.6	1. HTTP経由でのMQTT設定を追加； 2. MQTT TLS認証用のSSLセキュアオプションを追加してください； 3. BACnet/SC機能を追加； 4. Modbusオブジェクトの一括インポートおよび全オブジェクトの選択に対応； 5. HTTPプロキシ機能を追加； 6. Webパスワードの制限および変更プロンプトを追加； 7. HTTP APIのパスワード暗号化機能を追加しました。

目次

目次

第1章 製品紹介

1.1 概要

UG56は、堅牢な8チャネル産業用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を採用したUG56は、2000台以上のノードとの接続に対応しています。UG56は、見通し距離が最大15km、都市部では約2kmの通信範囲をカバーでき、スマートビルディング、スマート産業、その他多くの屋内用途に最適です。

UG56は、イーサネット、Wi-Fi、セルラーによる複数のバックホールバックアップに対応しているだけでなく、主要なネットワークサーバー（The Things Industries、ChirpStackなど）との連携や、組み込みのネットワークサーバーを備えており、容易な導入が可能です。

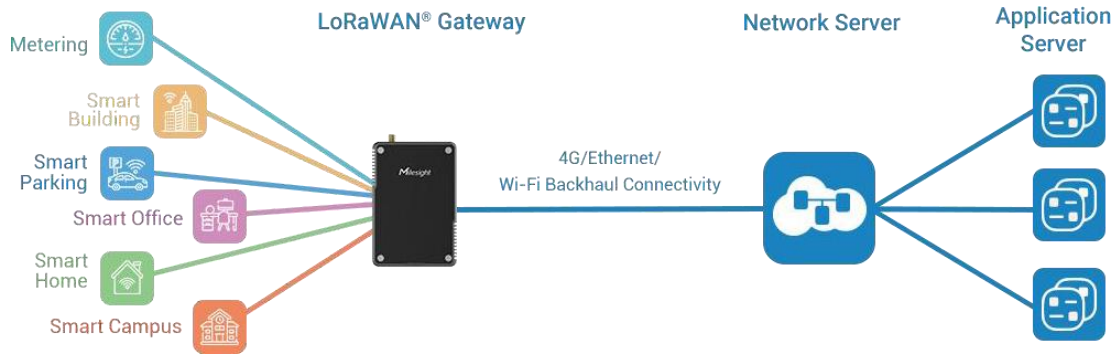


図1-1

1.2 特長

メリット

- クアッドコア産業用CPUと大容量メモリ
- イーサネット、2.4GHz Wi-Fi、および世界対応の3G/4G LTEオプションによるマルチバックホール接続のバックアップにより、簡単に接続できます
- 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います
- アプリケーションサーバーへのデータ転送には、MQTT、HTTP、またはHTTPSプロトコルに対応
- 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年間の保証付き

セキュリティと信頼性

- イーサネットとセルラー間の自動フェイルオーバー／フェイルバック
- IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN/WireGuardなどのセキュリティフレームワークに対応

- ハードウェアウォッチドッグを内蔵し、様々なフェイルから自動的に復旧し、最高レベルの可用性を確保します

メンテナンスが容易

- 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、および一元管理を実現します
- ユーザーフレンドリーなWebインターフェースのデザインと、さまざま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、管理者は多数のデバイスに対して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、業界標準のSNMPを通じて、既存のプラットフォーム上でリモートデバイスを効率的に管理できます

機能

- 通信技術が絶えず変化する環境において、リモートデバイスを連携させます
- 産業用クアッドコア 64 ビット ARM Cortex-A35 プロセッサ、最大 1.3 GHz の高性能かつ低消費電力、さらに 8GB eMMC を搭載し、より多くのアプリケーションに対応
- -20°C～60°C/-4°F～140°F の幅広い動作温度に対応

第2章 Web GUIへのアクセス

この章では、UG56のWeb GUIにアクセスする方法について説明します。

ユーザー名：**admin**

パスワード：**password**

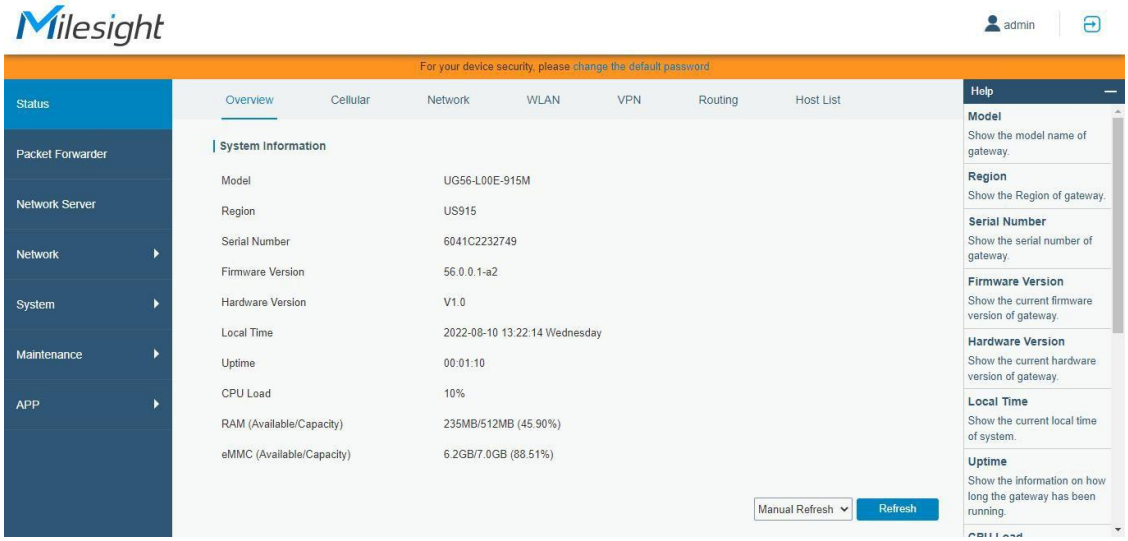
設定手順：

1. お使いのコンピュータで無線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. PCでWebブラウザ（Chromeを推奨）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。

ユーザー名またはパスワードを5回以上間違えて入力すると、ログインページが10分間ロックされます。

4. Web GUIにログインした後、初回は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文字のアルファベットと1桁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、Web GUIに再度ログインしてください。Web GUIにログインすると、システム情報の確認やゲートウェイの設定を行うことができます。

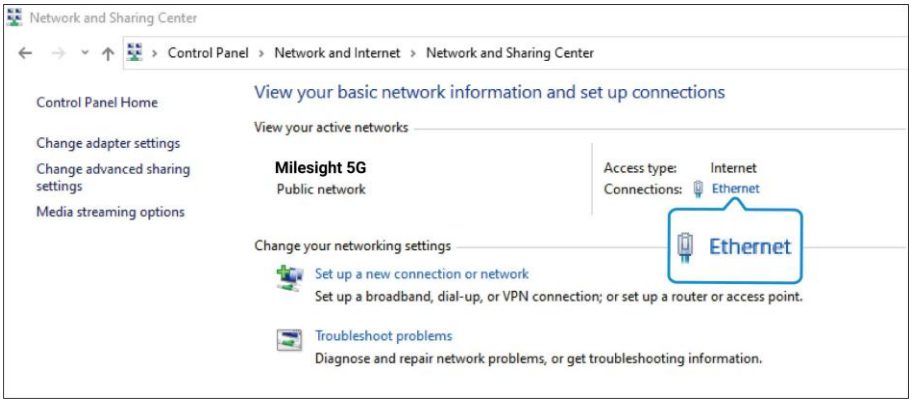


注：v56.0.0.6 以前のバージョンでは、ゲートウェイは有線接続にも対応しています。

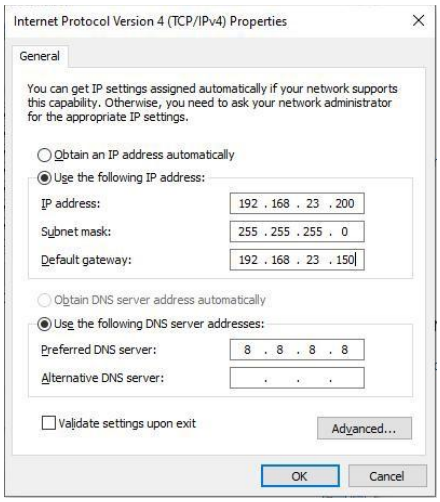
1. PCをUG56のETHポートに直接、またはPoEインジェクタを介して接続してください。

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システムを例に挙げると、

「Control Panel」→「Network and Internet」→「Network and Sharing Center」の順に選択し、「Ethernet」をクリックしてください（名称が異なる場合があります）。



A. 「Properties」→「Internet Protocol Version 4(TCP/IPv4)」の順に選択し、「Use the following IP address」を選択した後、ゲートウェイと同じサブネット内で手動で静的IPアドレスを割り当ててください。



3. PCでWebブラウザ（Chromeを推奨）を開き、IPアドレス **192.168.23.150** を入力して、Web GUI にアクセスします。

第 3 章 Web 設定

3.1 Status

3.1.1 概要

このページでは、ゲートウェイのシステム情報を確認できます。

図 3-1-1-1

System Information	
項目	説明
Model	ゲートウェイのモデル名を表示します。
Region	ゲートウェイで使用されている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	システムの現在のローカル時刻を表示します。
Uptime	ゲートウェイが稼働している期間に関する情報を表示します。
CPU Load	ゲートウェイの現在のCPU使用率を表示します。
RAM (Capacity/Available)	RAMの容量と使用可能なRAMメモリを表示します。
eMMC (Capacity/Available)	eMMC の容量と使用可能な eMMC メモリを表示します。

表 3-1-1-1 システム情報

3.1.2 Cellular

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。

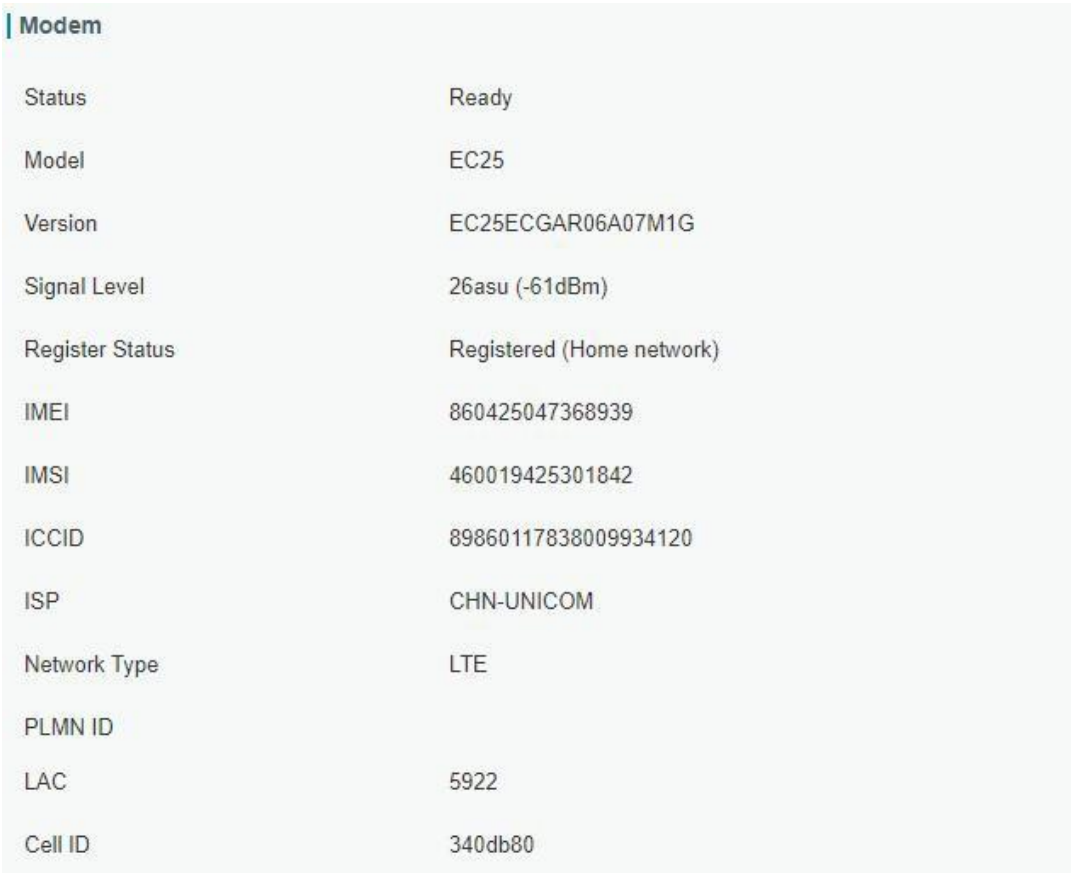


図 3-1-2-1

Modem Information	
項目	説明
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カードの登録状況を表示します。
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カードが登録されている通信事業者を表示します。
Network Type	接続されているネットワークの種類（LTE、3Gなど）を表示します。
PLMN ID	現在のPLMN ID（MCC、MNC、LAC、Cell 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 カードの所在地のセル ID を表示します。

表 3-1-2-1 モデム情報

図 3-1-2-2

Network Status	
項目	説明
Status	携帯電話ネットワークの接続状況を表示します。
IP Address	モバイルネットワークのIPアドレスを表示します。
Netmask	モバイル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からどのくらいの時間が経過しているかに関する情報を表示します。

表 3-1-2-2 ネットワークの状態

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	
項目	説明
Port	イーサネットポートの名前を表示します。
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接続されていないか、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	ポートが有効な場合、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経過した時間を表示します。ポートが無効になったり、イーサネットケーブルが外されたりすると、経過時間の表示は停止します。

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め、Wi-Fi のステータスを確認できます。

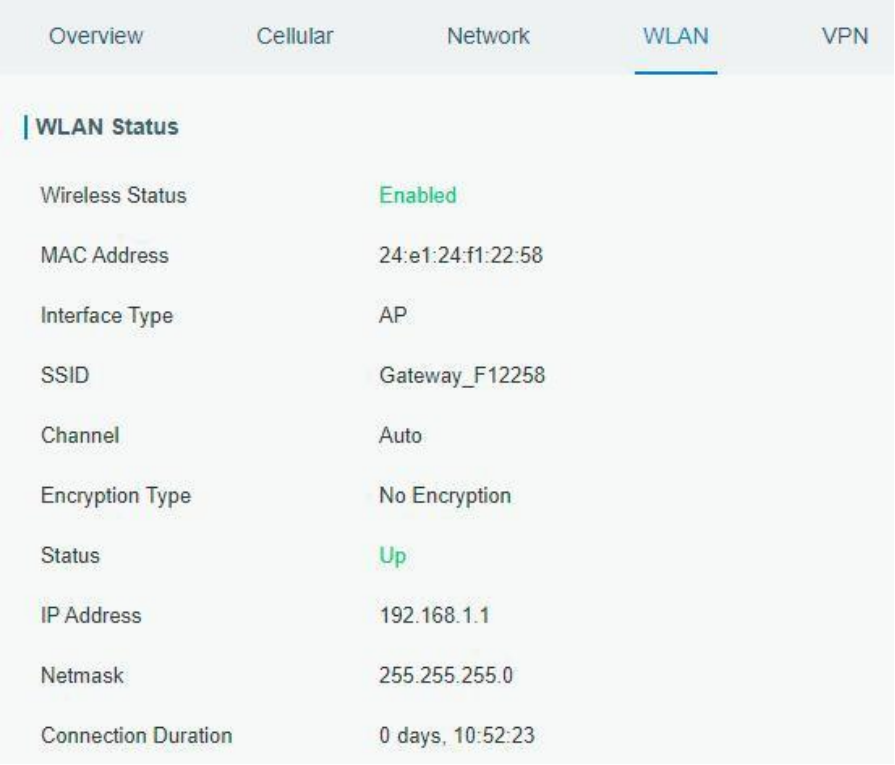


図 3-1-4-1

WLAN Status	
項目	説明
Wireless Status	ワイヤレスのステータスを表示します。
MAC Address	MACアドレスを表示します。
Interface Type	「AP」や「クライアント」などのインターフェースの種類を表示します。
SSID	SSIDを表示します。
Channel	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	接続ステータスを表示します。
IP Address	ゲートウェイのIPアドレスを表示します。
Netmask	ゲートウェイのワイヤレスMACアドレスを表示します。
Gateway	ワイヤレスネットワークのゲートウェイアドレスを表示します。
Connection Duration	Wi-Fi ネットワークへの接続時間がどれくらいか、そ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	
項目	説明
IP Address	アクセスポイントまたはクライアントの IP アドレスを表示します。
MAC Address	アクセスポイントまたはクライアントのMACアドレスを表示します。
Connection Duration	Wi-Fi ネットワークへの接続時間が表示されます。

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

表 3-1-5-1 VPN ステータス

3.1.6 Routing

このページでは、ルーティングテーブルや ARP キャッシュなど、ルーティングの状態を確認できます。

図 3-1-6-1

項目	説明
Routing Table	
Destination	宛先ホストまたは宛先ネットワークの IP アドレスを表示します。
Netmask/Prefix Length	宛先ホストまたは宛先ネットワークのネットマスクまたはプレフィックス長を表示します。
Gateway	ゲートウェイの IP アドレスを表示します。
Interface	ルートの送信元インターフェースを表示します。
Metric	ルートのメトリックを表示します。
ARP Cache	
IP	ARPプールのIPアドレスを表示します。
MAC	IP アドレスに対応する MAC アドレスを表示します。
Interface	ARPのバインディングインターフェースを表示します。

表 3-1-6-1 ルーティング情報

3.1.7 Host List

このページでは、ホスト情報を表示できます。

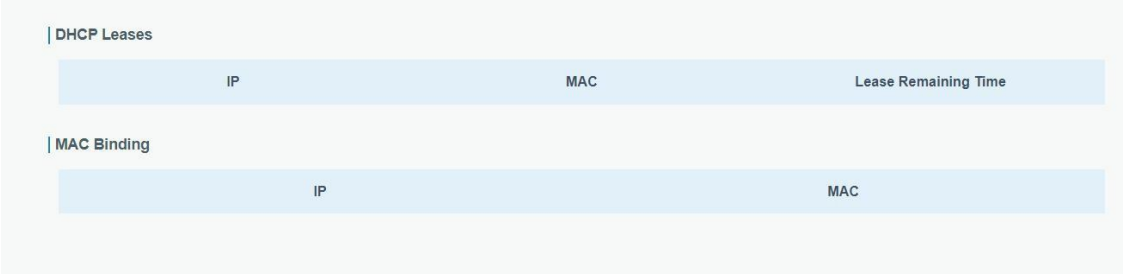


図 3-1-7-1

Host List	
項目	説明
DHCP Leases	

IP Address	DHCPクライアントのIPアドレスを表示
MAC Address	DHCPクライアントのMACアドレスを表示
Lease Time Remaining	DHCPクライアントのリース残り時間を表示します。
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 3-1-7-1 ホストリストの説明

3.2 LoRaWAN

3.2.1 Packet Forwarder

3.2.1.1 General

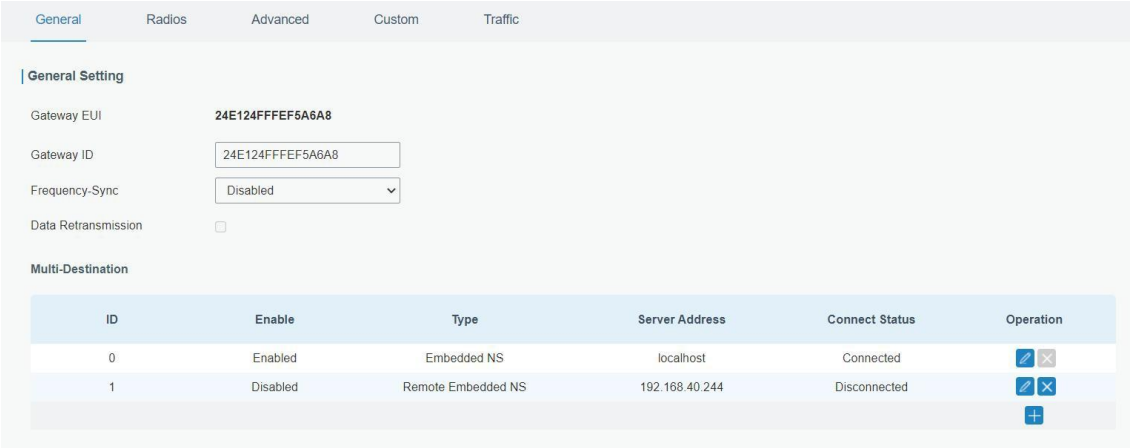


図 3-2-1-1

General Settings	
項目	説明
Gateway EUI	ゲートウェイの識別子を表示します。これは編集できません。 形式：ETHポートのMACアドレス + 中央に「FFFE」
Gateway ID	TTNなどのリモートネットワークサーバーでゲートウェイを登録する際に使用した、対応するIDを入力してください。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 Retransmission	ゲートウェイが単一のChirpstack/Semtech/Basic Station/Remote Embedded NSタイプのパッケージフォワーダーに接続している場合、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、ネットワークが復旧した後にデータを再送信します。
Multi-Destination	ゲートウェイは、リスト内で作成され、有効化されたネットワークサーバーのアドレスにデータを転送します。
Connection Status	パッケージフォワーダーの接続ステータスを表示します。

表 3-2-1-1 一般設定パラメータ

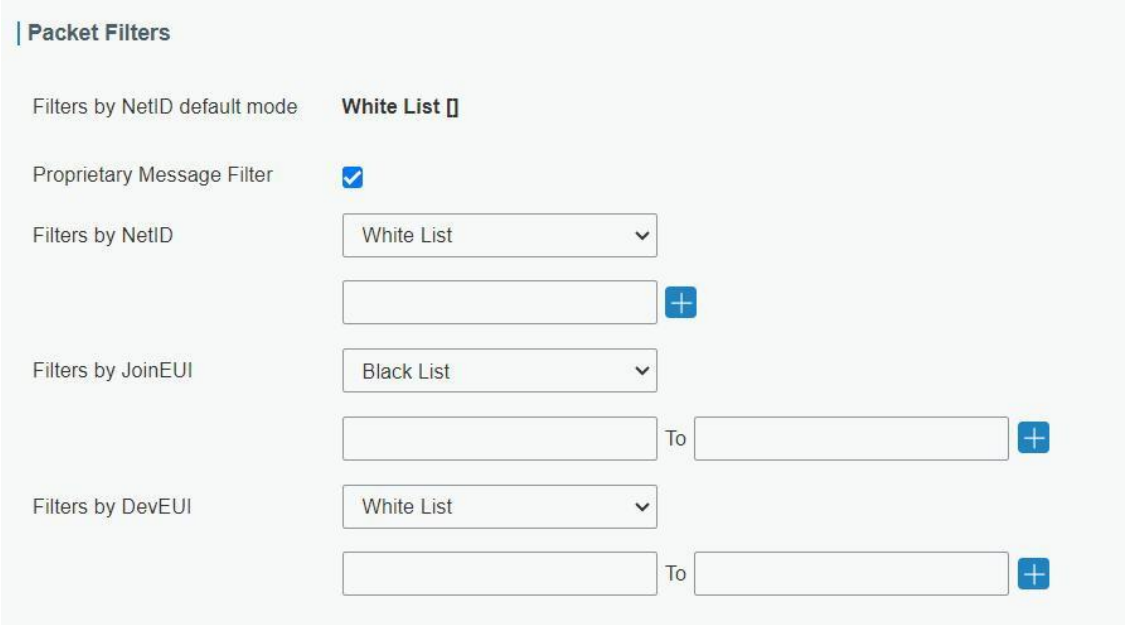


図 3-2-1-2

Packet Filters	
パラメータ	説明
Filters by NetID Default Mode	フィルタモードとして、ブラックリストまたはホワイトリストを選択してください。 **White List**：このリストにある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**：このリストに含まれるパケット以外のパケットのみをネットワークサーバーに転送します。
Proprietary Message Filter	有効にすると、独自メッセージパケット（Mtype=111）を転送しなくなります。
Filters by NetID	指定されたNetIDに一致するアップリンクパケットを転送するか、転送しないかを設定します。
Filters by JoinEUI	指定されたJoinEUIの範囲に一致する参加要求パケットを転送するか、転送しないかを設定します。
Filters by DevEUI	指定されたDevEUIの範囲に一致する参加要求パケットを転送する／転送しない。
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

注：

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. パケットフォワーダーのタイプが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。

関連する設定例

パケットフォワーダーの設定

3.2.1.2 Radios

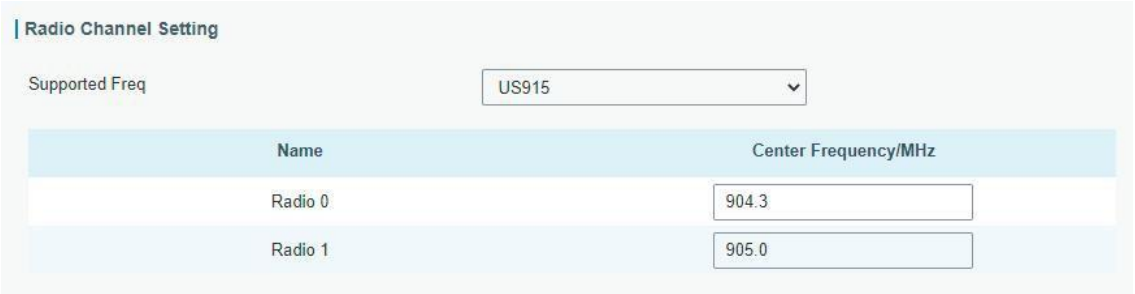


図 3-2-1-2

Radios-Radio Channel Setting	
項目	説明
Region	アップストリームおよびダウンリンクの周波数と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。
Center Frequency	LoRaWAN® ノードからパケットを受信するための周波数を変更します。

表 3-2-1-2 無線チャネルの設定パラメータ

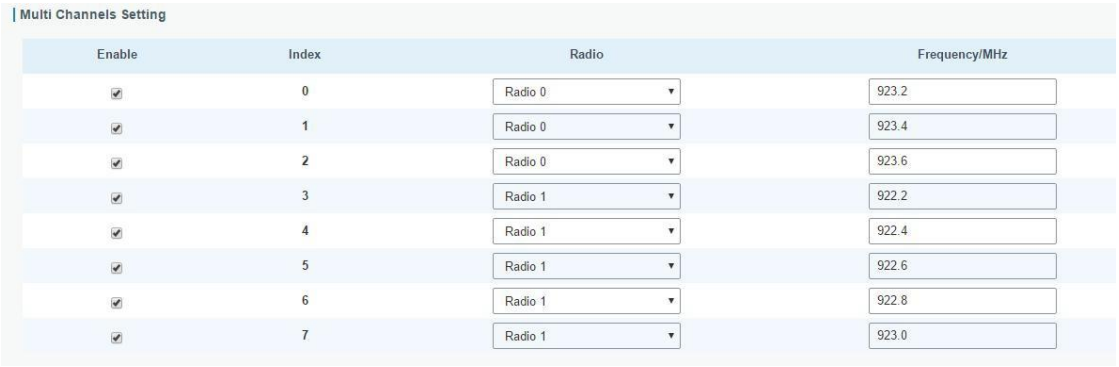


図 3-2-1-3

Radios-Multi Channel Setting		
項目	説明	デフォルト
Enable	クリックして、このチャンネルでパケットを送信できるようにします。	Enabled
Index	リスト内の順序を示します。	/
Radio	中心周波数として「Radio 0」または「Radio 1」を選択してください。	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く

表 3-2-1-3 マルチチャンネル設定パラメータ

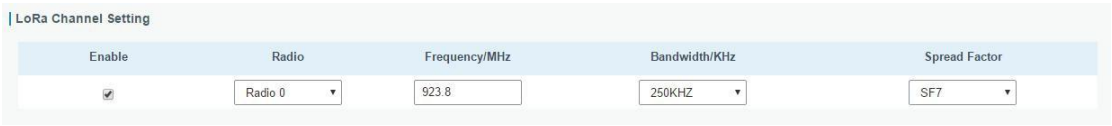


図 3-2-1-4

Radios-LoRa Channel Setting		
項目	説明	デフォルト
Enable	このチャンネルでパケットを送信するには、ここをクリックして有効にしてください。	Enabled
Radio	中心周波数として、Radio 0 または Radio 1 を選択してください。	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。	対応している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選択してください。拡散係数が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に規定されている内容に基づきます

表 3-2-1-4 LoRa チャネル設定パラメータ

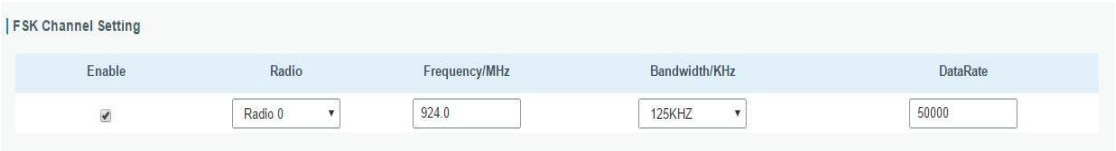


図 3-2-1-5

Radios-FSK Channel Setting		
項目	説明	デフォルト
Enable	このチャンネルでパケットを送信するには、ここをクリックして有効にしてください。	Disabled
Radio	中心周波数として、Radio 0 または Radio 1 を選択してください。	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。	対応している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	対応している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 3-2-1-5 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、ユーザーが環境の干渉状況を分析して最適な配置を選択できるよう、図表を表示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**の値が低いほど、信号の状態は良好です。この機能はダウンリンクの送信に影響を与えるため、パケットフォワーダーを使用する際は有効にしないことをお勧めします。

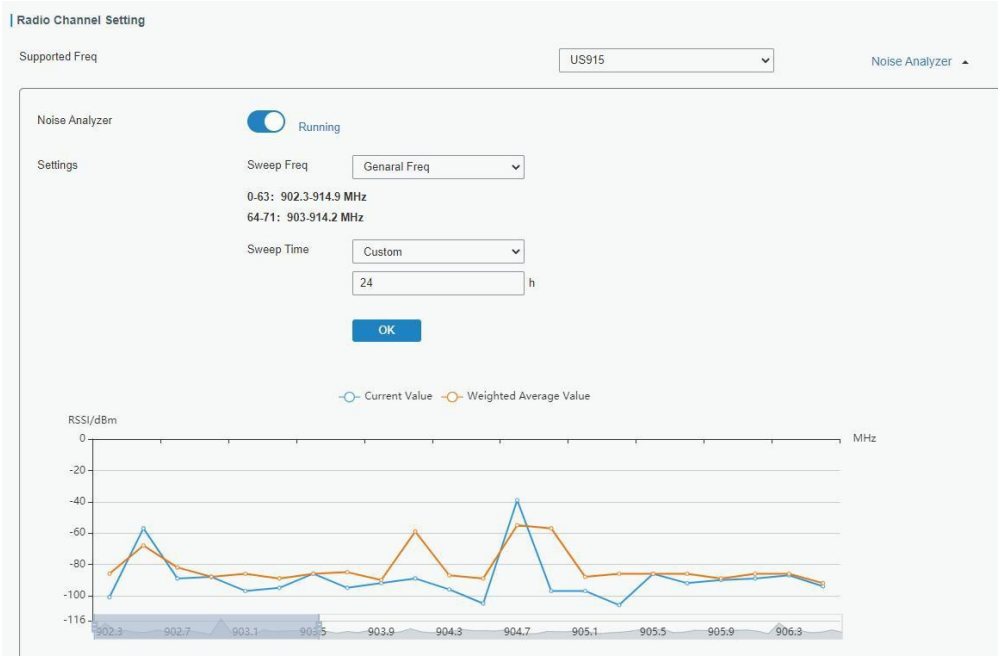


図 3-2-1-6

Noise Analyzer		
項目	説明	デフォルト
Enable	クリックしてノイズアナライザー機能を有効にしてください。	Disabled
Sweep Freq	周波数スイープ範囲を選択してください。 **一般周波数：**LoRaWAN® 地域パラメータ文書に基づく周波数 **カスタム：**周波数範囲をカスタマイズ	一般周波数
Sweep Time	ノイズアナライザを継続的に、または一定期間有効にします。「カスタム」を選択した場合、ノイズアナライザは事前に設定された時間が経過すると自動的に停止します。 注：ノイズアナライザ機能は通常のデータ送信に影響を与えるため、時間をカスタマイズすることをお勧めします。	カスタム/24時間

表 3-2-1-6 ノイズアナライザの設定パラメータ

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。

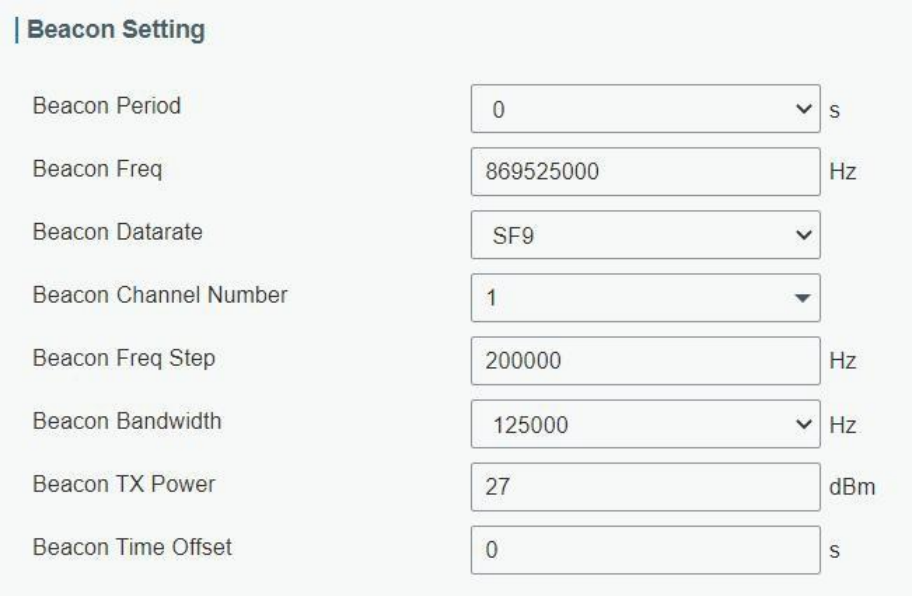


図 3-2-1-7

Advanced-Beacon Setting		
項目	説明	デフォルト
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の場合、ゲートウェイはビーコンを送信しません。	0
Beacon Freq	ビーコンの送信周波数です。	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です。	対応している周波数に基づきます
Beacon Channel Number	「カスタム」を選択すると、1 から 8 までの範囲でユーザー自身が設定できます。	1
Beacon Freq Step	ビーコンの周波数間隔。	200000
Beacon Bandwidth	ビーコンの帯域幅です。単位：Hz	12500 Hz
Beacon TX Power	ビーコンの送信出力です。	対応している周波数に基づきます
Beacon Time Offset	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 3-2-1-7 高度なビーコンパラメータ

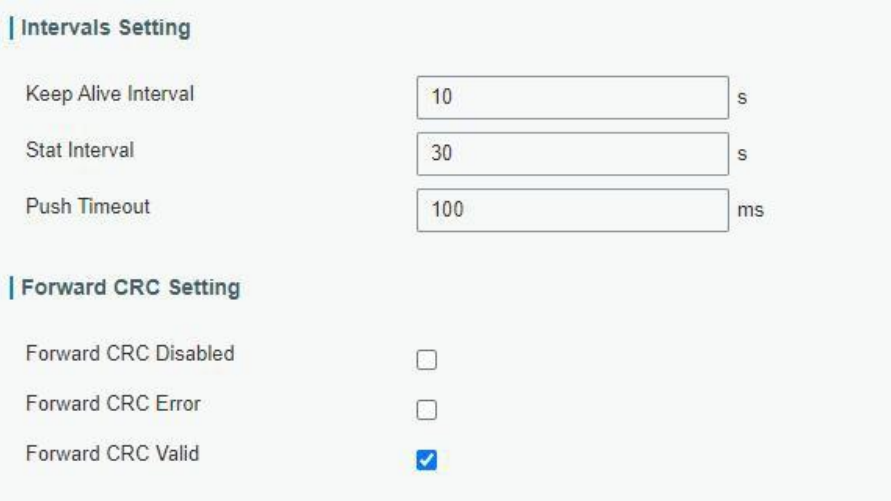


図 3-2-1-8

項目	説明	デフォルト
Keep Alive Interval	接続を安定させ、維持するために、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。 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つタイムアウト時間を入力してください。範囲：1～1999。	100
Forward CRC Disabled	CRCが無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するように有効にします。	Disabled
Forward CRC Error	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するには、有効にしてください。	Disabled
Forward CRC Valid	CRC が有効な受信パケットをネットワークサーバーに送信するには、これを有効にしてください。	Enabled

表 3-2-1-8 詳細パラメータ

図 3-2-1-9

項目	説明	デフォルト
Enable	LBT 機能を有効または無効にします。Listen before talk (LBT) 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出し、チャネルアクセスの競合を回避するために使用されます。 注：AU915およびUS915はLBT機能に対応していません。	Disabled
RSSI Target	アイドル状態のチャネルの基準を入力してください。実際のRSSIが	-80

	チャンネルの実際のRSSIが基準値/目標値より小さい場合、そのチャンネルはアイドル状態とみなされます。範囲：-120～0	

表 3-2-1-9 Advanced-LBT パラメータ

3.2.1.5 Custom

カスタム設定モードが有効になっている場合、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入力して、パケットフォワーダーを設定することができます。「Save」をクリックしてカスタム設定ファイルの内容を保存し、「Apply」をクリックして有効にしてください。「Clear」をクリックすると、編集ボックス内のすべての内容が消去されます。設定ファイルの書き方がわからない場合は、「Example」をクリックして参照ページに移動してください。

注：カスタム設定は、Web GUIのパケットフォワーダー設定を上書きします。

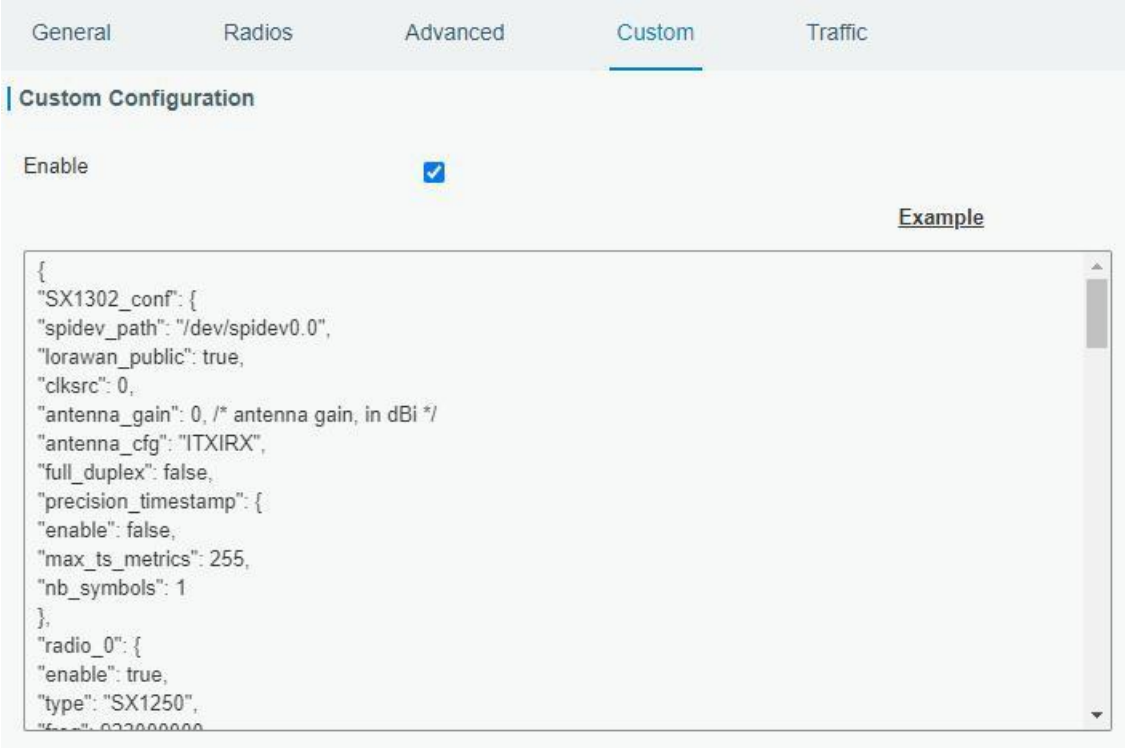


図 3-2-1-10

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。リアルタイムのトラフィックを確認するには、「**Refresh**」をクリックしてください。

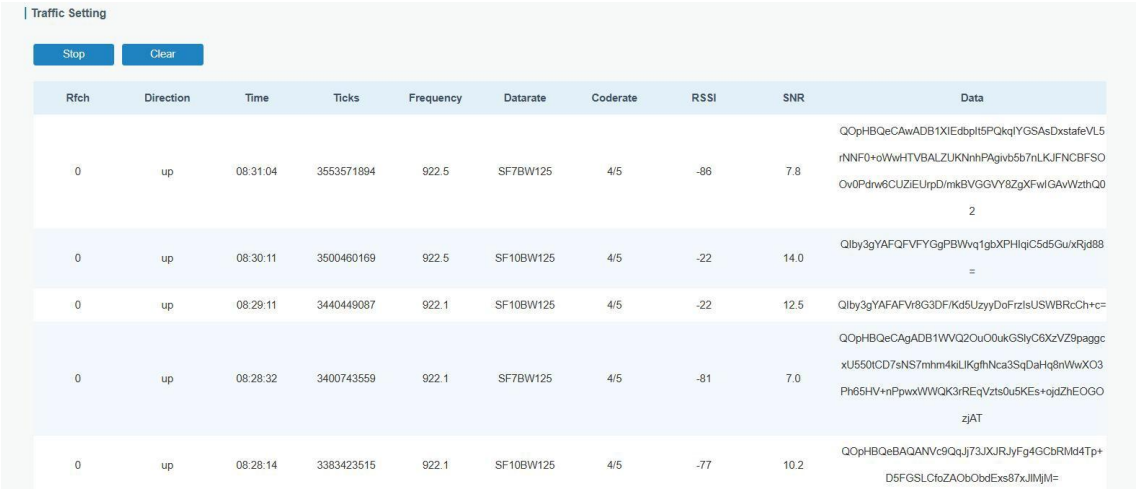


図 3-2-1-11

項目	説明
Refresh	クリックすると、最新のデータが取得されます。
Clear	クリックしてすべてのデータをクリアしてください。
Rfch	このパケットのチャネルを表示します。
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数を表示します。
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レートを表示します。
RSSI	受信信号強度を表示します。
SNR	このパケットの信号対雑音比を表示します。
Data	このパケットのペイロード（Base64）を表示します。 注：これは Actility パケットフォワーダーでは機能しません。

表 3-2-1-10 トラフィックパラメータ

3.2.2 Network Server

3.2.2.1 General

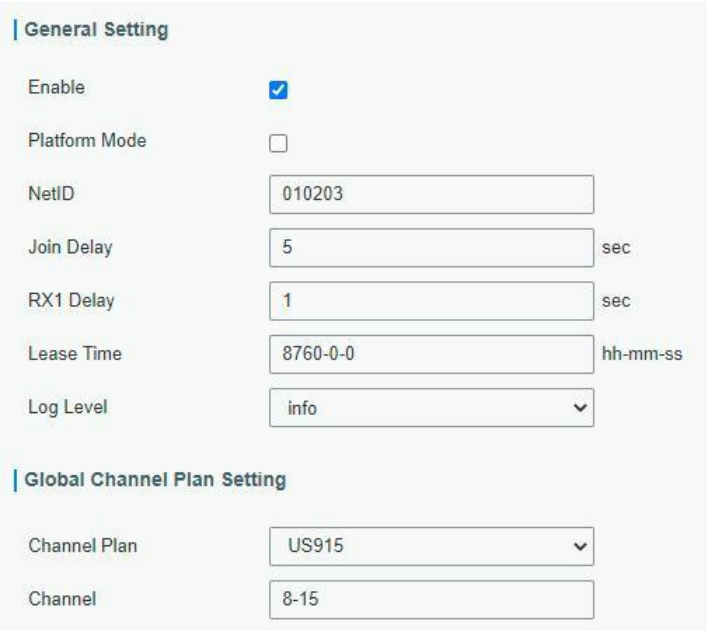


図 3-2-2-1

項目	説明	デフォルト
General Setting		
Enable	クリックしてネットワークサーバーモードを有効にしてください。	Enabled
Platform Mode	Milesight IoT Cloud にゲートウェイを接続するには、有効にしてください。	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対して Join_request_message を送信してから、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を開く準備をする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	正常な参加が失効す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、リース時間を超えると、エンドデバイスはネットワークサーバーに再度参加する必要があります。	876000-00-00
Log level	ログレベルを選択してください。	Info
Channel Plan Setting		
Channel Plan	アップストリームおよびダウン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。	ゲートウェイの周波数に依存します
Channel	有効な周波数は、チャネルを使用して制御されます	チャンネルマスクによって異なります

	マスクを使用して制御されます。 空欄のままにすると、LoRaWAN® 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ンネルすべてが使用されます。チャンネルのインデックスを入力することができます。 **例：** 1, 40: チャンネル1とチャンネル40を有効化 1-40：チャンネル1からチャンネル40までを有効化 1-40, 60: チャンネル1から40およびチャンネル60を有効化 All：すべてのチャンネルを有効にします Null：すべてのチャンネルが無効であることを示します	ゲートウェイの周波数

表 3-2-2-1 一般的なパラメータ

注：一部の地域バリエーションでは、お使いの LoRaWAN® 地域で許可されている場合、次の図に示すように、[Additional Plan] を使用して、EU868 や KR920 など、LoRaWAN® 地域パラメータで定義されていない追加のチャンネルを設定することができます。

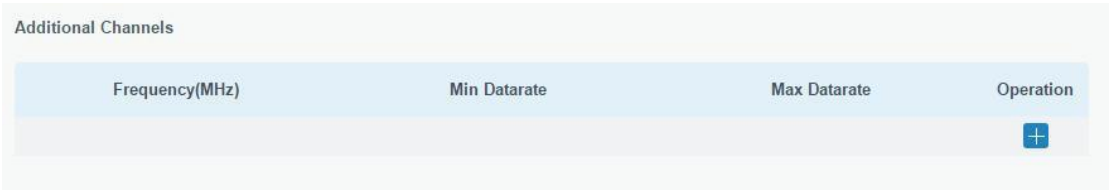


図 3-2-2-2

Additional Channels		
項目	説明	デフォルト
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。この範囲は、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に規定されている内容に基づいています。	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、 をクリックして新しいアプリケーションを作成したりできます。

図 3-2-2-3

Application	
項目	説明
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：喫煙者センサー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に追加できる MQTT 送信と HTTP (HTTPS) 送信は、それぞれ 1 つだけです。

表 3-2-2-3 アプリケーションパラメータ

MQTT Integration

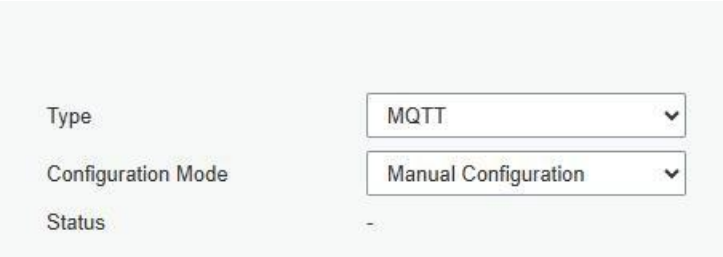


図 3-2-2-4

MQTT Settings	
項目	説明
Type	タイプとして「MQTT」を選択してください。
Configuration Mode	設定モードを選択してください。 **Manual Configuration**：Webページから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の接続ステータスを表示します。
Get via HTTP	
Platform URL	HTTPリクエストを送信するプラットフォームのURLを選択します。
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

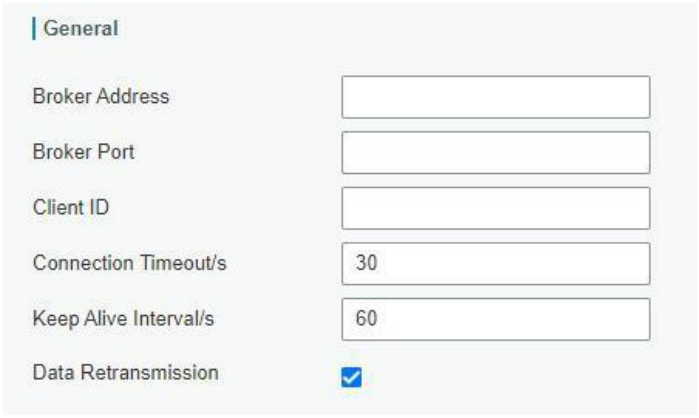


図 3-2-2-5

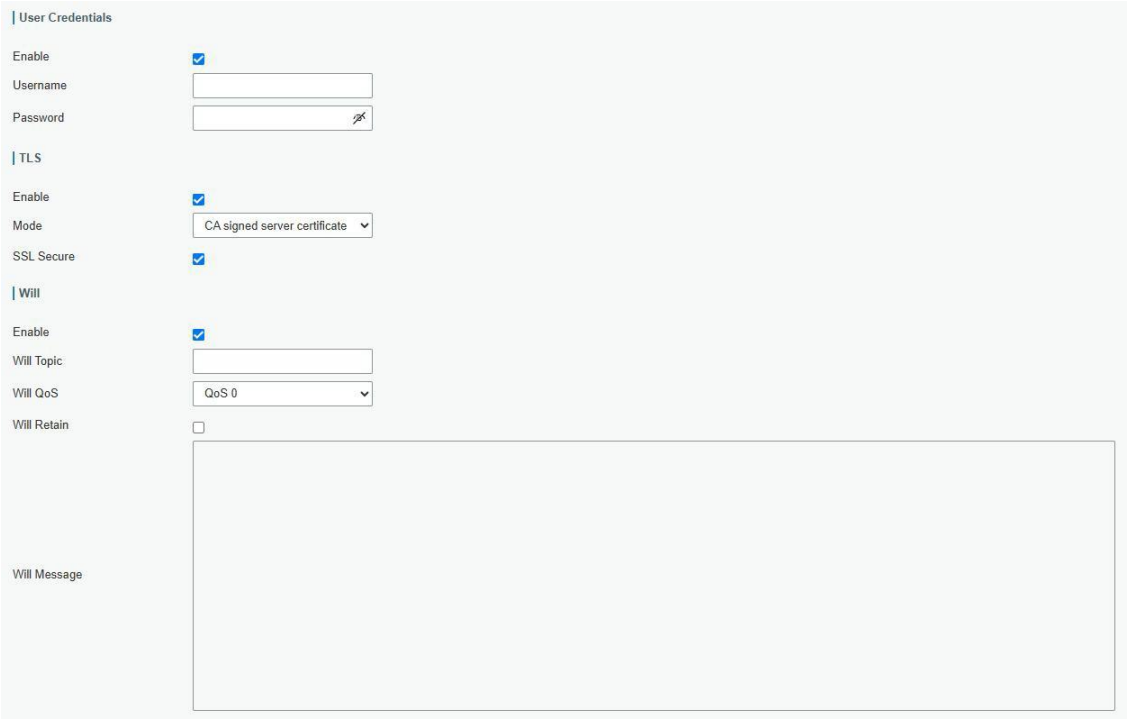


図3-2-2-6

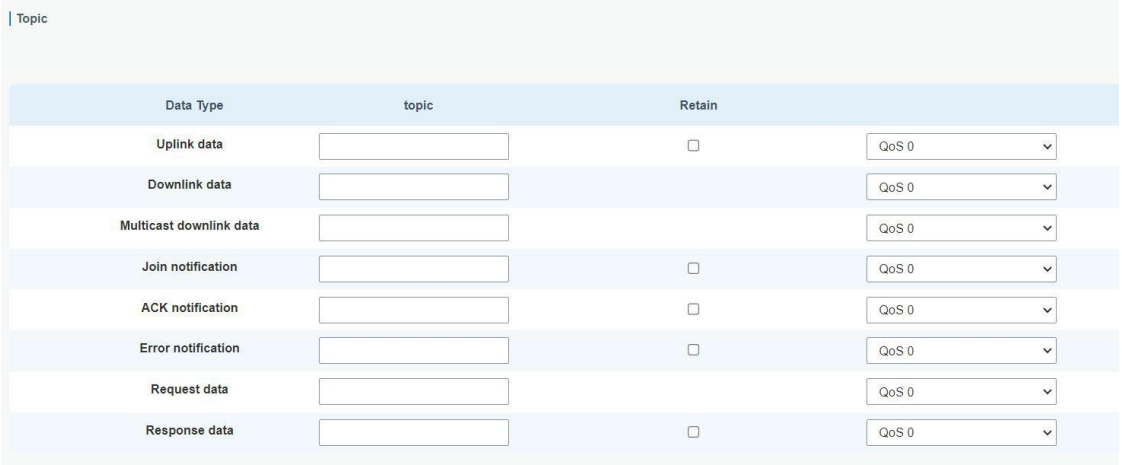


図 3-2-2-7

MQTT Settings - Manual Configuration	
項目	説明
General	
Broker Address	データを受信するMQTTブローカーのアドレスです。
Broker Port	データを受信するMQTTブローカーのポートです。
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一意の識別子です。 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は一意である 必要があり、QoS 1 および 2 でのメッセージ処理に不可欠です。
Connection Timeout/s	接続タイムアウト後にクライアントが応答を受け取らない場合、接続は切断されたものとみなされます。範囲：1～65535
Keep Alive Interval/s	クライアントがサーバーに接続した後、クライアントは接続を維持するために定期的にサーバーにハートビートパケットを送信します。範囲：1～65535
Data Restransmission	有効にすると、ネットワークが切断された際に最大10,000件のデータを対応し、ネットワークが回復した後にデータを再送信します。
User Credentials	
Enable	ユーザー認証情報を有効にします。 注：MQTT ブローカーのタイプが HiveMQ の場合、**TLS を**有効にし、オプションを「**CA signed server certificate**」に設定してください。
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通信でTLS暗号化を有効にします。
Mode	「Self-signed certificates」または「CA signed server certificate」から選択してください。**CA signed server certificate**：デバイスにプリロードされている認証局（CA）が発行した証明書で検証してください。 **Self-signed certificates**：検証用に、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）をアップロードしてください。
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終了した際、ラストウィルメッセージが自動的に送信されます。通常、デバイスのステータス情報を送信したり、他のデバイスやプロキシサーバーにデバイスのオフライン状態を通知したり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、またはQoS2から選択できます。
Will Retain	有効にすると、ラストウィルメッセージをリテインメッセージとして設定できます。
Will Message	ラストウィル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**：デバイスのアップリンクパケットを受信します。

	Downlink Data：デバイスへのダウンリンクコマンドを送信します。単一のデバイスにダウンリンクコマンドを送信する必要がある場合は、このトピックにワイルドカード「$deveui」を追加し、このトピックを購読する際に実際のデバイスの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**：ゲートウェイがデバイスのネットワーク参加を許可するために参加承認パケットを送信した場合、その参加通知を受信します。 **ACK Notification**：ダウンリンクコマンドを送信する際、デバイスからACKパケットを受信します。 **Error Notification**：デバイスからエラーパケットを受信します。 **Request data**：ゲートウェイのNSを照会および設定するためのリクエストを送信します。 **Response data**：リクエストに対する応答を受信します。
Topic	パブリッシュに使用す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のメッセージを保持メッセージとして設定します。
QoS	QoS 0 – 1回のみ これは最も高速な方法であり、メッセージは 1 つだけで済みます。ただし、信頼性は最も低くなります。 QoS 1 – 少なくとも1回 このレベルでは、メッセージが少なくとも1回は配信されることが保証されますが、複数回配信される可能性もあります。 QoS 2 – 正確に1回 QoS 2は、MQTTにおける最高レベルのサービス品質です。このレベルでは、各メッセージが宛先によって1回だけ受信されることが保証されます。 QoS 2は、最も安全ですが、最も遅いサービス品質レベルです。

表 3-2-2-5 MQTT 設定 - 手動設定パラメータ

HTTP/HTTPS 統合

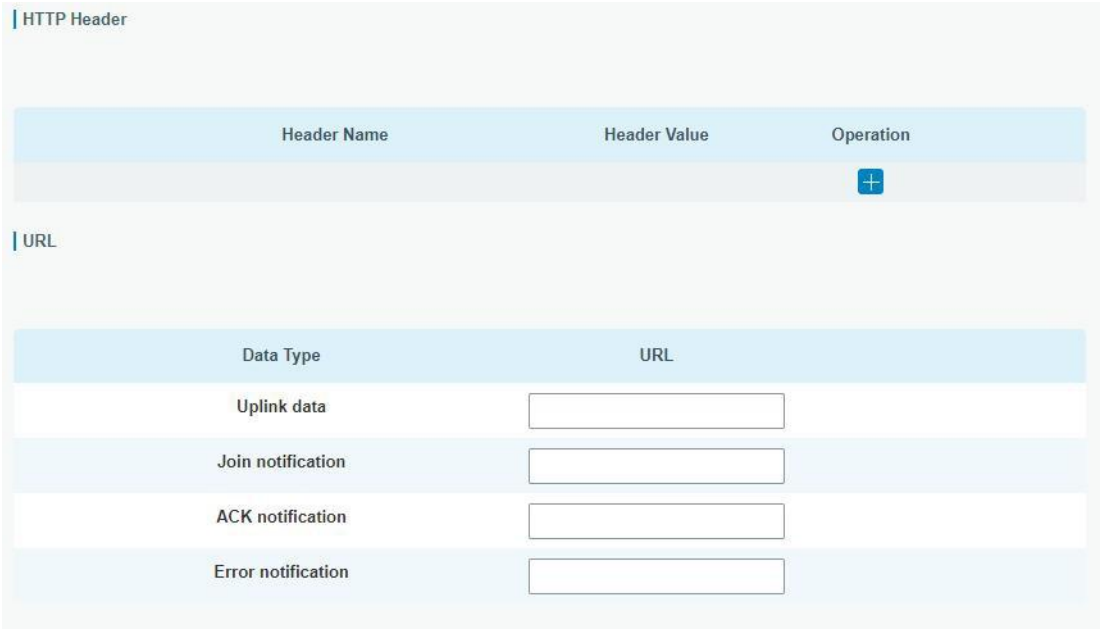


図 3-2-2-8

HTTP/HTTPS Settings	
項目	説明
HTTP Header	
Header Name	HTTPヘッダーの主要なフィールド群です。
Header Value	HTTPヘッダーの値です。
URL	
Data Type	HTTP/HTTPSサーバーに送信されるデータ型。 **Uplink Data**：デバイスのアップリンクパケットを受信します **Join Notification**：ゲートウェイがデバイスのネットワーク参加を許可するために参加承認パケットを送信した場合、参加通知を受信します **ACK Notification**：ダウンリンクコマンドを送信する際、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	パブリッシュに使用するデータ型のトピック名。
URL	データを受信する HTTP/HTTPS サーバーの URL。

表 3-2-2-6 HTTP/HTTPS 設定パラメータ

関連する設定例

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えます。また、ユーザーは他社製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内容を調整したりすることも可能です。

Inbuilt Payload Codec Library

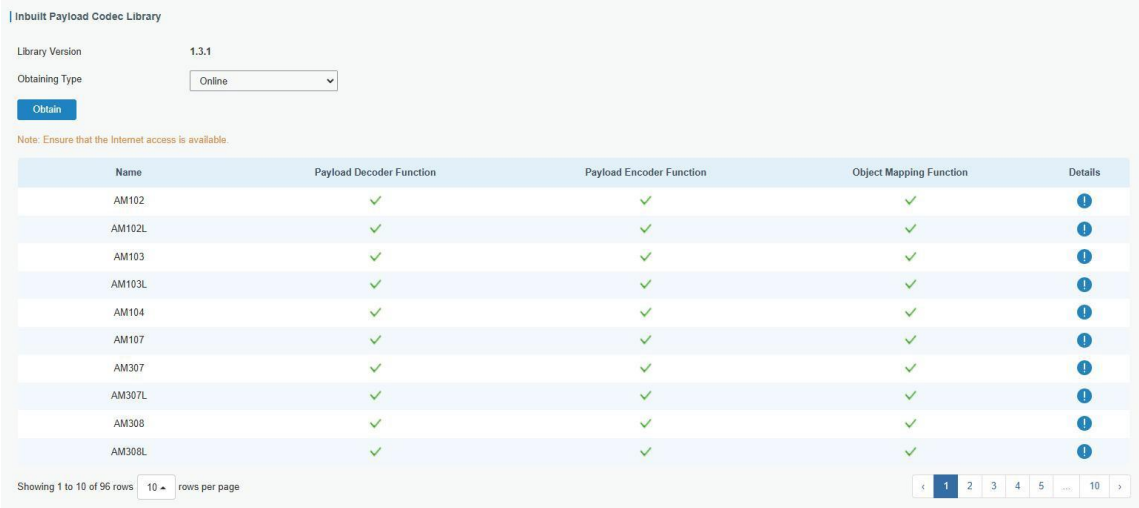


図 3-2-2-9

Inbuilt Payload Codec Library	
項目	説明
Library Version	Milesight デバイスのペイロードコーデックライブラリのバージョンを表示します。

Obtaining Type	Milesightデバイスのペイロードコーデックライブラリを更新するタイプを選択してください。**Online**：ゲートウェイが電源投入時にインターネットに接続し、バージョン更新があることを検出した場合、自動的に更新されます。また、ユーザーは「**Obtain**」ボタンをクリックして、手動で更新状況を確認することもできます。 **Local Upload**：「**Browse**」をクリックしてZIP形式のペイロードコーデックパッケージをアップロードし、「**Import**」をクリックしてライブラリを更新します。Milesightペイロードコーデックパッケージについては、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場合に表示されます。
Payload Encoder Function	エンコーダが存在するかどうかを表示します。
Object Mapping Function	オブジェクトマッピング関数が存在する場合に表示します。
Details	デコーダおよびエンコーダの詳細を表示します。これでは要件を満たさない場合は、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 組み込みペイロードコーデックライブラリのパラメータ

Custom Payload Codec

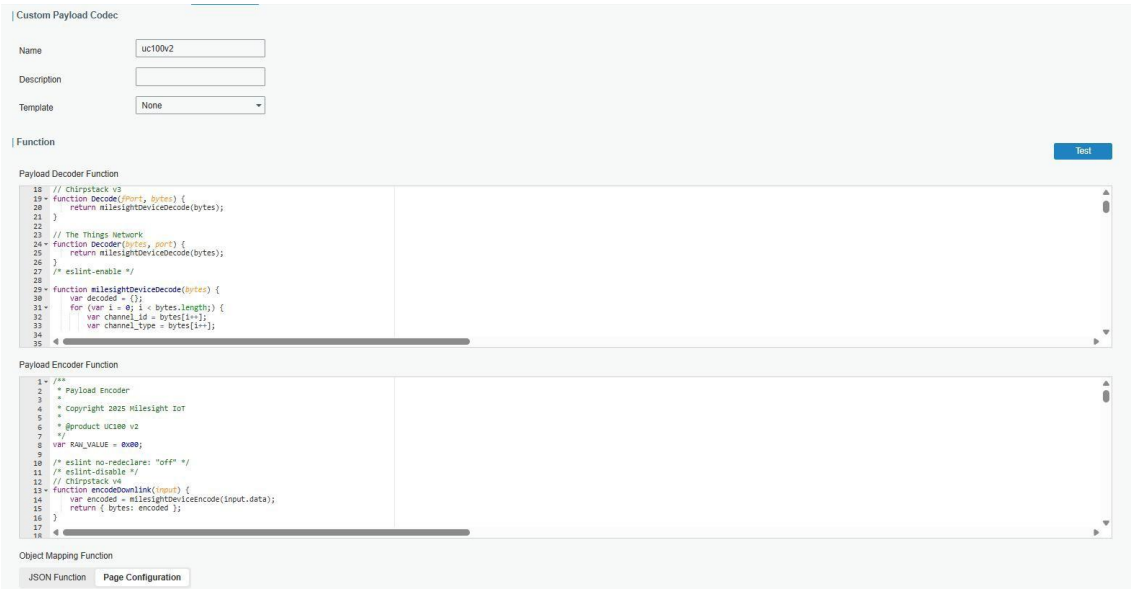


図3-2-2-10

Custom Payload Codec	
項目	説明
Name	カスタムペイロードコーデックの一意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	既存の組み込み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をカスタマイズし、16進数形式のデータをJSON形式に変換します。関数のヘッダーは、空白欄の例と同じである必要がありますのでご注意ください。
Payload Encoder	デバイスのペイロードエンコーダーをカスタマイズして、JSON形式に変換するように設定します

Function	メッセージを16進数形式に変換するコマンド。なお、関数のヘッダーは、空白欄の例と同じである必要があります。
Object Mapping Function	LoRaWAN® メッセージを BACnet または Modbus オブジェクトに変換するマッピング関数をカスタマイズします。追加方法は 2 通りあります： **JSON Function**：JSON 形式で関数を追加します。 **Page Configuration**：ページ経由で機能を追加します。
Test	ペイロードコーデックのテストを有効または無効にします。 **入力**：空白を含まない16進形式の生データ、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 です。 **Decoder Test**：16進形式の生データをJSON形式の結果に変換します。 **Encoder Test**：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

注：

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. 1つのペイロードコーデックのデコーダおよびエンコーダで使用される変数名は、同じ項目を指す場合、同一でなければなりません。

オブジェクトマッピング関数 - JSON関数の例：

```
{
  "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>項目</th><th>説明</th></tr>
<tr><td>id</td><td>この値は、デコーダおよびエンコーダの変数名と同じである必要があります。</td></tr>
<tr><td>name</td><td>空白のままにするか、必要に応じて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。空白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：
<table>
<tr><th>オプション</th><th>説明</th><th>Modbus レジスタタイプ</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>この変数の値の型を定義します。対応するオプション：
<table>
<tr><th>オプション</th><th>説明</th><th>Modbusレジスタタイプ</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>整数および浮動小数点数を含む数値データ、例：温度</td><td>入力レジスタ、保持レジスタ</td></tr>
</table>
</td></tr>
</table>

	<table><tr><td>BOOL</td><td>0または1の状態のみ。 例：ボタンの状態</td><td>離散入力、コイル</td></tr><tr><td>ENUM</td><td>複数の値</td><td>入力レジスタ、保持レジスタ</td></tr></table> 注：データ型が ENUM で、参照パラメータが空白でない場合は、Modbus レジスタタイプを「入力レジスタ」または「保持レジスタ」に設定することをお勧めします。
value_type	対応しているオプション：UINT8、INT8、UINT16、INT16、UINT32、INT32、FLOAT、STRING。
values	この変数の値の範囲を設定します。
max_length	値の型が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。
bacnet_type	対応しているオプション： analog_value_object 、 analog_input_object 、 analog_output_object 、 binary_value_object 、 binary_input_object 、 binary_output_object 、 multistate_value_object、multistate_input_object、multistate_output_object
bacnet_unit_type_id	BACnet ユニット ID を入力してください。こちらで確認できます。
bacnet_unit_type	BACnet ユニットタイプを入力してください。こちらで確認できます（「説明」を参照）。
reference	この変数を他の変数と一緒に書き込む必要がある場合は、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 関数のパラメータ

図 3-2-2-11

Object Mapping Function-Page Configuration	
項目	説明
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	このオブジェクトの関連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。関連付けられた後、これらのオブジェクトはまとめて表示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関数 - ページ構成パラメータ

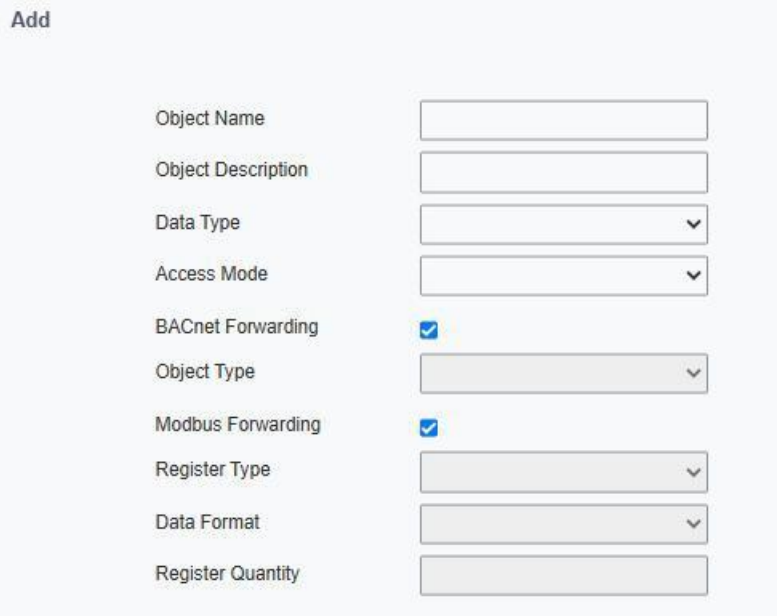


図3-2-2-12

Object Mapping Function-Add an Object	
項目	説明
Object Name	名前は、デコーダまたはエンコーダの変数名と同じ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 および 1 のステータスに値を設定します。
Enumeration Number	データ型が ENUM の場合、対応するオプションの数を設定します。
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	有効にすると、BACnetオブジェクトのパラメータの詳細が表示されます。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。
Modbus Forwarding	Modbus オブジェクトのパラメータ詳細を表示するには、これを有効にしてください。これらのパラメータは、データ型およびアクセスモードに従っ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、デバイスの機能およびブートパラメータを定義します。これらの情報要素は、エンドデバイスの製造元によって提供される必要があります。UG56 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。

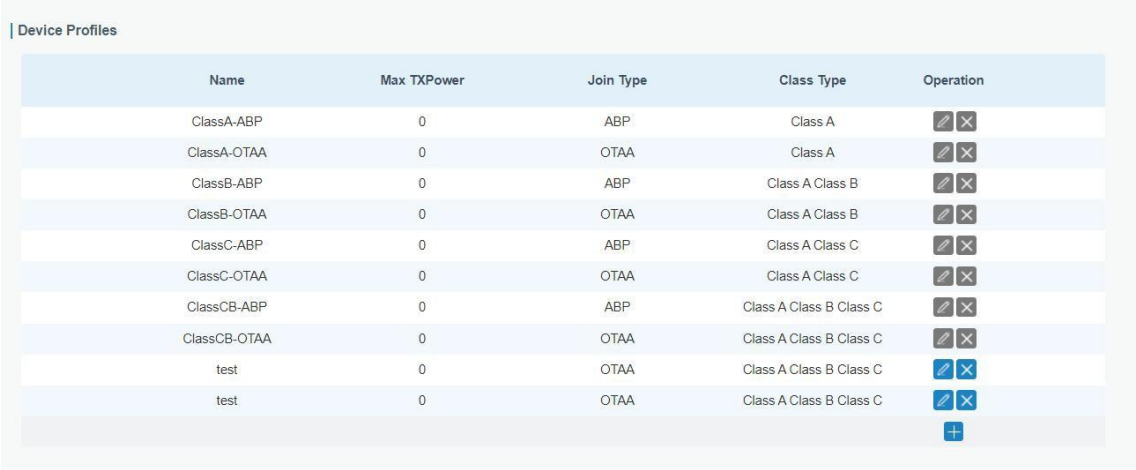


図 3-2-2-13

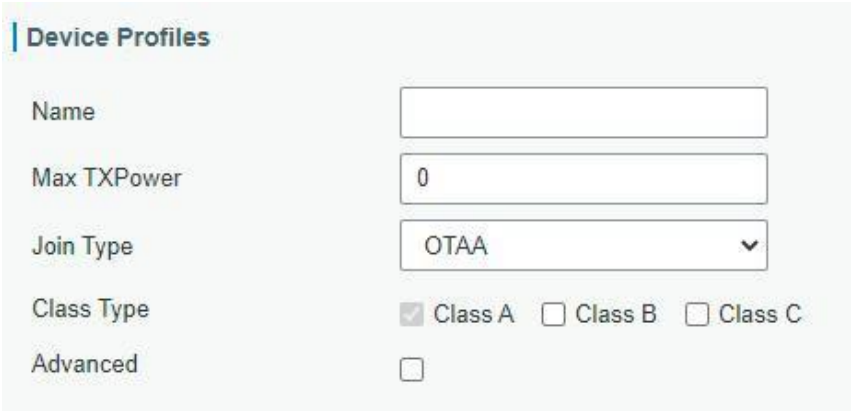


図 3-2-2-14

Device Profiles Settings	
項目	説明
Name	デバイスプロファイルの名前を入力してください。 例：Smoker-sensor-app
Max TXPower	最大送信電力を入力してください。 TXPowerは、エンドデバイスの最大EIRPレベルに対する電力レベルを示します。0は最大EIRPを使用することを意味します。EIRPとは、等方性放射等価電力のことです。
Join Type	「OTAA」または「ABP」から選択してください。
Class Type	デフォルトでは、デバイスタイプはクラス A です。ユーザーは、クラス B またはクラス C のチェックボックスをオンにして、クラスタイプを追加できます。

	注：クラスBを使用する場合は、**[Packet Forwarder> Advance**の値が非ゼロである必要があります。

表 3-2-2-12 デバイスプロファイルの設定パラメータ

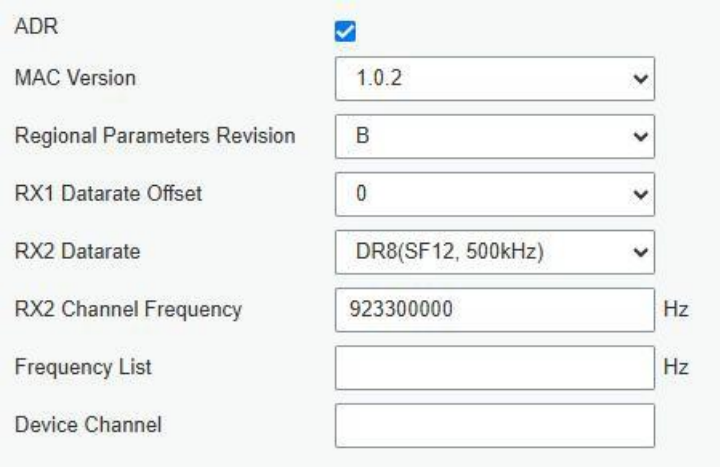


図 3-2-2-15

Device Profile Advanced Settings		
項目	説明	デフォルト
ADR	エンドデバイスのデータ転送速度を調整するために、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に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チャネル周波数です。	
Frequency List	工場出荷時のプリセット周波数のリストです。範囲は、LoRaWAN® 地域パラメータ文書で指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ます。設定された場合、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の開放間隔です。	1秒ごと
PingSlot DataRate	ダウンリンクを受信するノードのデータレート。	対応周波数に基づいて

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いて
ACK Timeout	ダウンリンク送信の確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。	クラス B：10 クラス 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です。

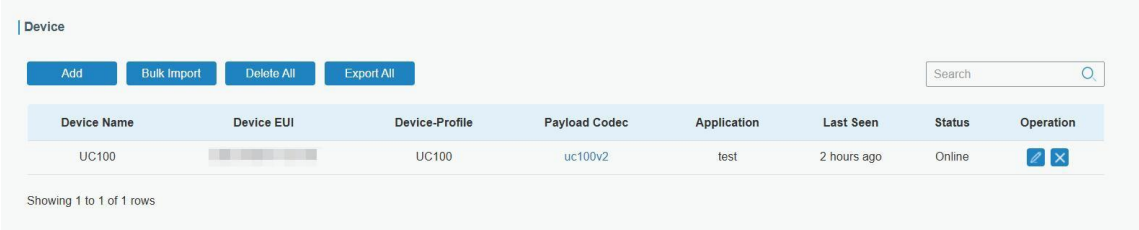


図 3-2-2-16

項目	説明
Add	デバイスを追加します。
Bulk Import	テンプレートをダウンロードし、複数のデバイスをインポートします。 注：テンプレートファイルの表ヘッダー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	デバイスの名前を表示します。
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	デバイスの使用されているペイロードコーデックを表示します。クリックすると、このペイロードコーデックの詳細を確認できます。
Application	デバイスのアプリケーション名を表示します。
Last Seen	最後にパケットを受信した時刻を表示します。
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いか、パケットを送信したことがないことを示します。 **Offline**：タイムアウト期間内にデバイスがパケットを送信しませんでした。 **Online**：デバイスがタイムアウト時間内にパケットを送信しました。
Operation	デバイスを編集または削除します。

表 3-2-2-14 デバイスパラメータ

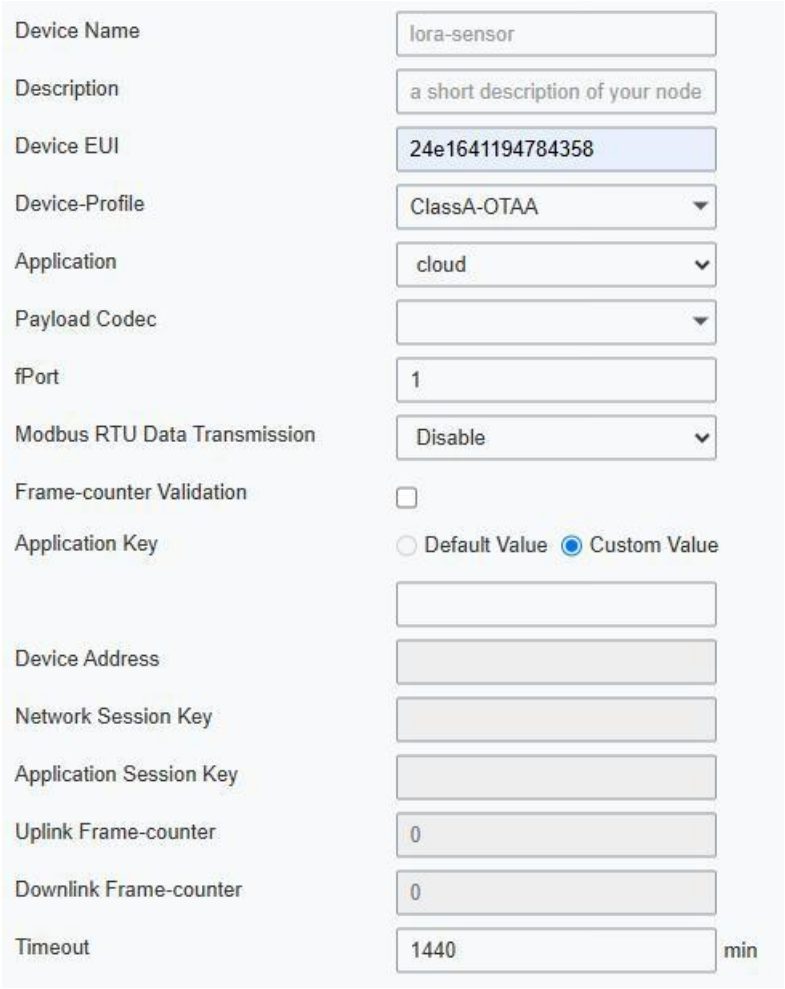


図 3-2-2-17

Device Configuration	
項目	説明
Device Name	このデバイスの名前を入力してください。
Description	このデバイスの説明を入力してください。
Device EUI	このデバイスの EUI を入力してください。
Device-Profile	デバイスプロファイルを選択してください。
Application	アプリケーションプロファイルを選択してください。
Payload Codec	「**Payload Codec**」ページにある**ペイロードコーデック**を選択してください。
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	「無効」、「Modbus RTU to TCP」、「Modbus RTU over TCP」から選択してください。この機能は、Milesight LoRaWAN® コントローラー（UC501/UC300 など）にのみ適用されます。 **Modbus RTU to TCP**：TCP クライアントは、Modbus TCP コマンドを送信して、コントローラの Modbus データを要求できます。 **Modbus RTU over TCP**：TCPクライアントは、Modbus RTUコマンドを送信して、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 UG56 間の透過的な伝送を行うための LoRaWAN® フレームポートを入力してください。 Milesight LoRaWAN® コントローラーと UG56。

	範囲：2～84、86～223。 注：この値は、Milesight LoRaWAN® コントローラーの Fport と同じである必要があります。
TCP Port	TCP クライアントと UG56（TCP サーバーとして）間のデータ転送に使用する 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を介してネットワークに参加するたびに、アプリケーションキーが使用され、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 または Device EUI+Device EUI です。 **Custom Value**：エンドデバイスに応じてアプリキーを定義します。
Device Address	デバイスアドレスは、現在のネットワーク内における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、エンドデバイスごとに固有のものです。エンドデバイスは、データの完全性を確保するために、すべてのアップリンク・データ・メッセージのMIC（メッセージ完全性コード）またはその一部を計算する際に、このキーを使用します。
Application Session Key	AppSKeyは、エンドデバイス固有のアプリケーションセッションキーです。アプリケーションサーバーとエンドデバイスの双方が、アプリケーション固有のデータメッセージのペイロードフィールドを暗号化および復号化するために使用します。
Uplink Frame-counter	ネットワークサーバーへアップリンクで送信されたデータフレームの数です。これは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。ユーザーはパーソナライズされた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、エンドデバイス上のフレームカウンタおよびそのエンドデバイスに対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端末のダウンリンクで受信したデータフレームの数です。これは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。ユーザーは、個別の端末を手動でリセットすることができ、その場合、端末側のフレームカウンターおよびその端末に対応するネットワークサーバー側のフレームカウンターは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です。範囲：1～4320分

表 3-2-2-15 デバイス設定パラメータ

関連する設定例

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。**この機能を使用する前に、エンドデバイスが標準の LoRaWAN® FUOTA プロトコルに対応していることを確認してください。**

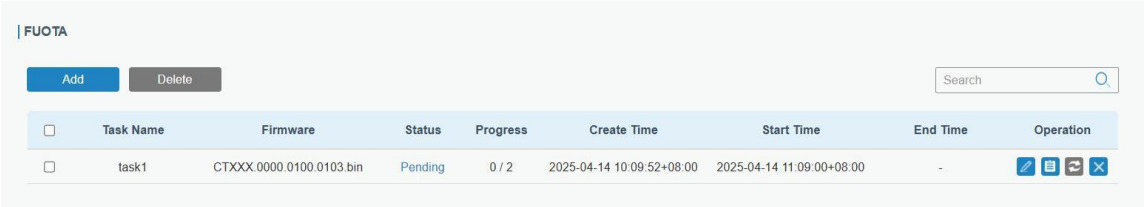


図 3-2-2-18

FUOTA	
項目	説明
Add	クリックしてタスクを追加してください。
Delete	タスクリストのチェックボックスにチェックを入れ、クリックしてこれらのタスクを削除してください。
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	タスクのステータスです。 **Pending**：タスクを処理する予定時刻を待機しています。 **Waiting**：アップグレード用のセッション作成の準備中です。 **Executing**：少なくとも 1 台のデバイスがアップグレード結果に応答しています。 **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に応答しました。
Progress	アップグレードに成功した、または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日時です。
Start Time	このタスクの開始時刻です。
End Time	このタスクを完了する時刻です。
Operation	: タスクのステータスが「**Pending**」のときに、このタスクを編集してください。 : すべてのデバイスの成功およびフェイルステータスを含む、タスクの詳細を確認します。 タスクのステータスが「**Finished**」になった場合、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ます。 : タスクのステータスが「**Pending**」または「**Finished**」のときに、このタスクを削除します。

表 3-2-2-16　FUOTA パラメータ

FUOTA タスクの追加

1. **[Add]** ボタンをクリックして、FUOTA タスクを追加します。
2. タスク設定を行います。

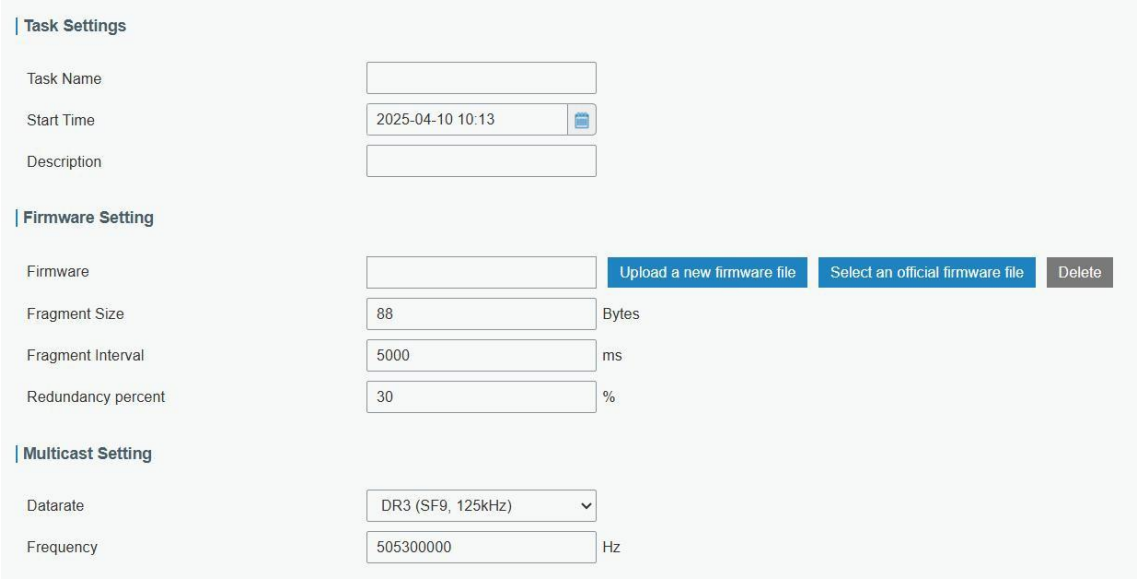
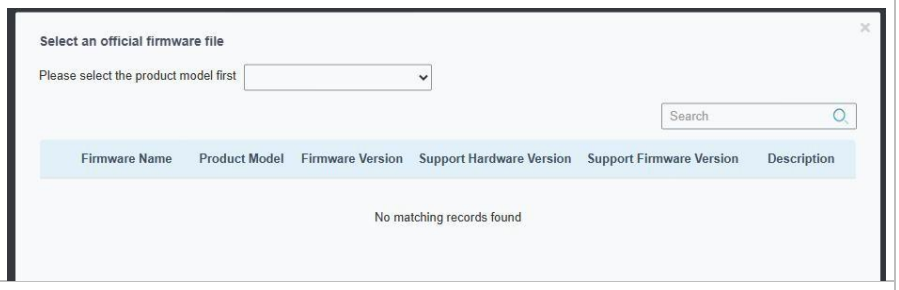


図 3-2-2-19

Add Task Settings	
項目	説明
Basic Information	
Task Name	タスク名をカスタマイズします。
Start Time	このタスクの開始時間を設定します。
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ます。 **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 Official Firmware file**：まず製品モデルを選択し、公式サイトからダウンロードするファームウェアを選択してください。この操作には、ゲートウェイがインターネットに接続されている必要があります。 
Fragment Size	ファームウェアファイルはこのサイズに分割され、各デバイスに割り当てられます。通常は、この値をデフォルト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**またはそれ以下の値に下げることをお勧めします。ネットワーク環境が良好な場合は、この値を大きくすることで転送速度を向上させることができます。
Fragment Interval	デバイスにファームウェアフラグメントを割り当てる間隔です。通常は、この値をデフォルト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**7**～**10**秒、あるいはそれ以上に増やすことをお勧めします。ネットワーク

	良好な場合は、この値を小さくすることで転送速度を向上させることができます。
Redundancy Percent	デバイスは、ファームウェアファイルのパケット修正のために、**30%**の冗長パケットを送信します。通常は、この値をデフォルト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悪い場合は、送信成功率を高めるために、この値を **40%～50%** またはそれ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は、この値を減らすことができます。
Multicast Settings	
Datarate	デバイスにファームウェアのフラグメントを割り当てるデータレートです。
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周波数。

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。

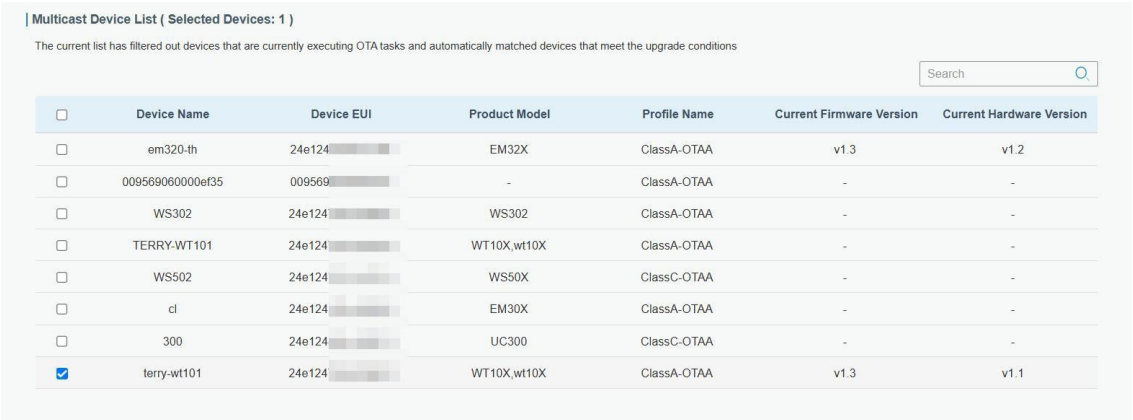


図 3-2-2-20

4. **[Save]** をクリックして、これらのタスク設定を保存します。

3.2.2.7 Multicast Groups

Milesightゲートウェイは、エンドデバイス群にダウンリンクメッセージを送信するために、クラスBまたはクラスCのマルチキャストグループを作成する機能を対応しています。マルチキャストグループは仮想のABPデバイス（つまり、セッションキーが共有される）であり、アップリンク、確認付きダウンリンク、およびMACコマンドは対応していません。

図 3-2-2-21

項目	項目
Add	マルチキャストグループを追加します。

Group Name	グループ名を表示します。
Number of Devices	グループのデバイス数を表示します。
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のパラメータ

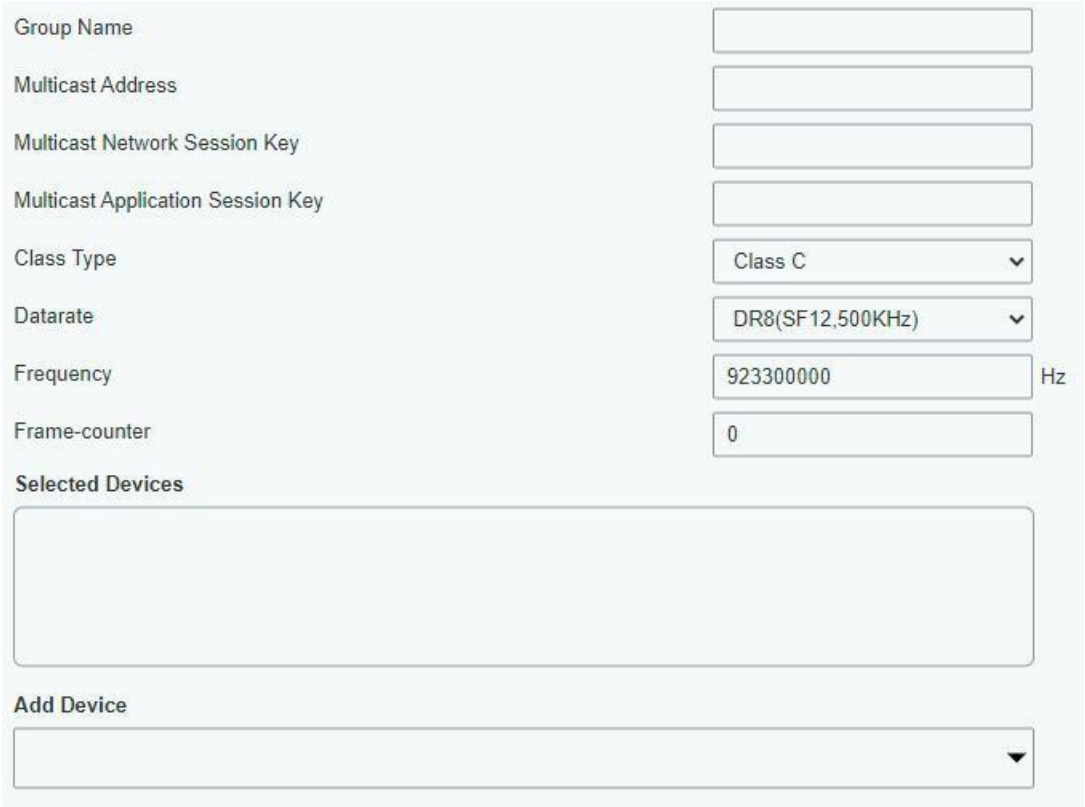


図 3-2-2-22

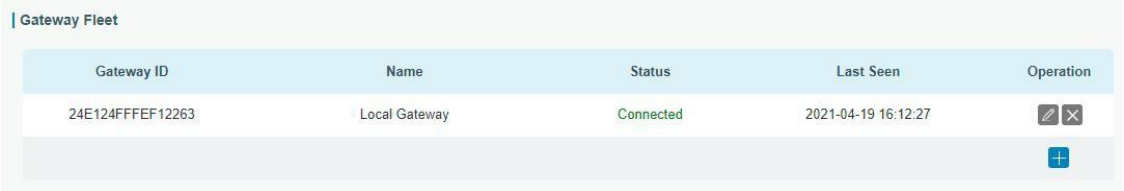
Multicast Group Configuration	
項目	説明
Group Name	このマルチキャストグループの名前を入力してください。
Multicast Address	このグループ内のすべてのデバイスのデバイスアドレス（Dev Addr）です。
Multicast Network Session Key	このグループ内のすべてのデバイスのネットワークセッションキー（Netwks Key）です。
Multicast Application Session Key	このグループ内のすべてのデバイスのアプリケーション・セッション・キー（AppSKey）です。
Class Type	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	このグループ内のすべてのデバイスのダウンリンク周波数。
Frame-count er	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。これは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	Pingスロットが開く周期です。これはクラスBの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



のゲートウェイにつき、最大100台のゲートウェイに対応できます。

図 3-2-2-23

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

表 3-2-2-20 ゲートウェイ・フリートのパラメータ

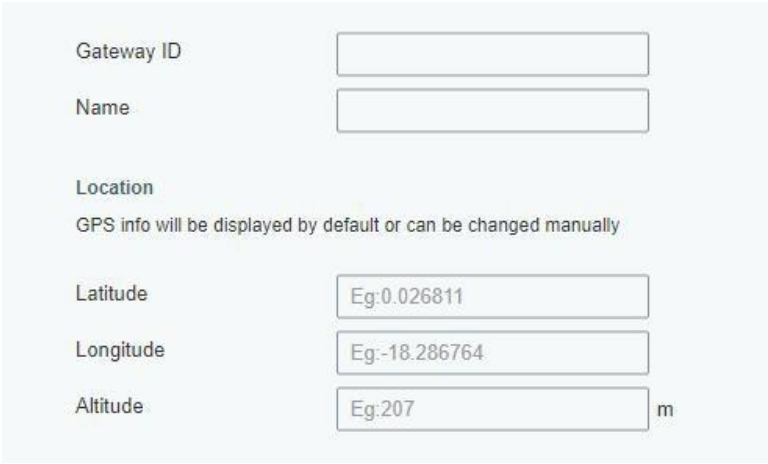


図 3-2-2-24

項目	説明
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	ここでゲートウェイのGPSデータを編集できます。ゲートウェイがGPSデータを送信する場合、そのデータがカスタマイズしたデータに上書きされます。

表 3-2-2-21 ゲートウェイ設定パラメータ

3.2.2.9 Packets

このゲートウェイは、最新の 1000 個のパケットに対応し、コマンドを送信します。

デバイスへのコマンド送信をサポートしています。

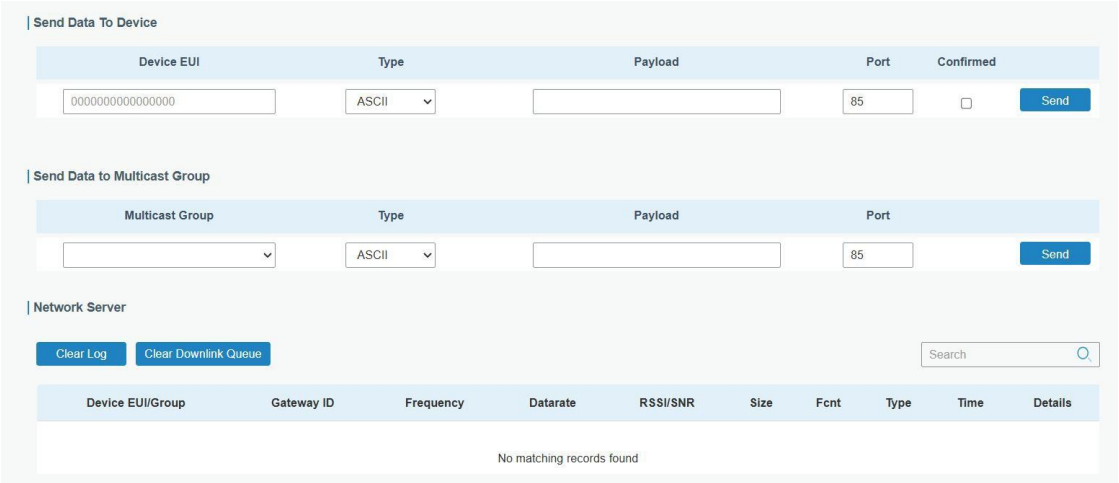


図 3-2-2-25

Send Data To Device/Multicast Group	
項目	説明
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、「マルチキャストグループ」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選択してください：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送信に使用する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「確認済み」と応答する必要があります。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	
項目	説明
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消去します。
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を表示します。
Frequency	パケットの送信に使用されている周波数を表示します。
Datarate	パケットの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	パケットの種類を表示します：JnAcc - 参加承認パケット JnReq - 参加要求パケット

	UpUnc - アップリンク未確認パケット UpCnf - アップリンク確認済みパケット - ネットワークから要求された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、パケットの詳細を確認できます。図に示すように：

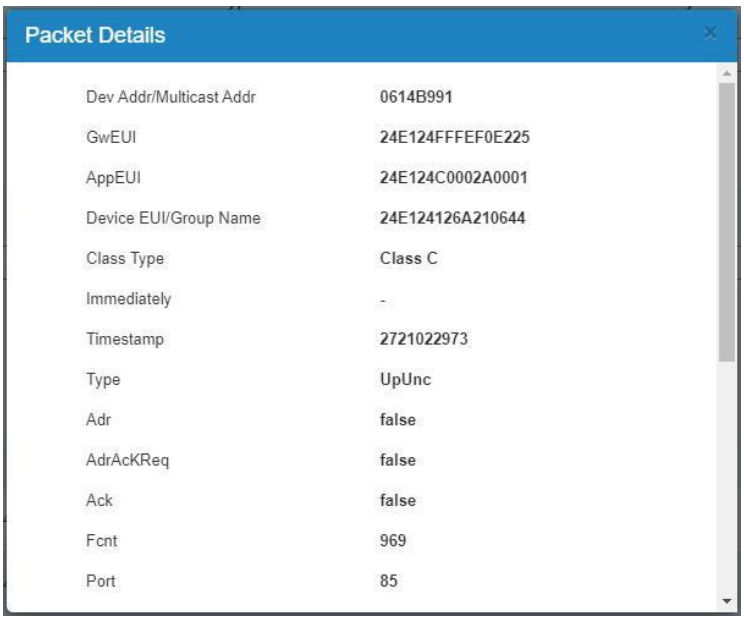


図 3-2-2-26

項目	説明
Dev Addr/Multicast Addr	デバイスまたはマルチキャストグループのアドレスを表示します。
GwEUI	ゲートウェイのEUIを表示します。
AppEUI	エンドデバイスのApp EUIを表示します。
DevEUI/Group Name	デバイスまたは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実行開始後、このパケットを受信するまでの時間を表示します。単位：ms
Type	パケットのタイプを表示します： JnAcc - 参加承認パケットJnReq - 参加要求パケット UpUnc - アップリンク未確認パケット UpCnf - アップリンク確認済みパケット - ネットワークからのACK応答要求

	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
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に、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に、ADR_ACK_DELAY 時間内に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 内に応答しません。
Ack	True：このフレームは ACK です。 False：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Fポートです。このパケットがMACコマンドの場合、ポートは0になります。このパケットにアプリケーションデータが含まれている場合、ポートは0以外（1～233）になります。
Modulation	LoRaとは、物理層でLoRa変調を使用することを意味します。
Bandwidth	このチャネルの帯域幅を表示します。
SpreadFactor	このチャネルの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	このチャンネルの符号化率を表示します。
SNR	このチャンネルのSNRを表示します。
RSSI	このチャンネルのRSSIを表示します。
Power	デバイスの送信電力を表示します。
Payload (b64)	このパケットのアプリケーションペイロードを表示します。
Payload (hex)	このパケットのアプリケーションペイロードを表示します。
Json	デコード後のデータを表示します。
MIC	このパケットのMICを表示します。MICは暗号化メッセージ整合性コードであり、MHDR、FHDR、FPort、および暗号化されたFRMPayloadの各フィールドに基づいて計算されます。

表 3-2-2-24 パケット詳細パラメータ

関連トピック

デバイスへのデータ送信

3.3 Protocol Integration

3.3.1 BACnet Server

UG56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

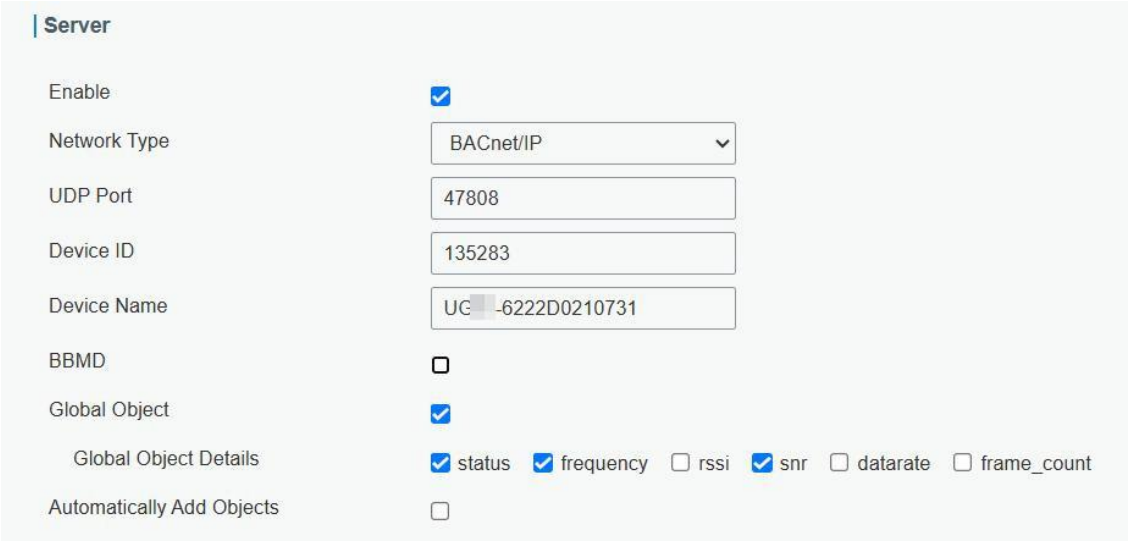


図 3-3-1-1

Server Settings	
項目	説明
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として、BACnet/IP または BACnet/SC を選択します。
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 ネットワーク上でデバイスを識別するための一意の名前です。
Global Object	有効にすると、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にされていない限り、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**：デバイスのアップリンクフレーム数 (FCNT)
Automatically Add Objects	有効にすると、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従ってオブジェクトを自動的に追加します。

表 3-3-1-1 サーバーパラメータ

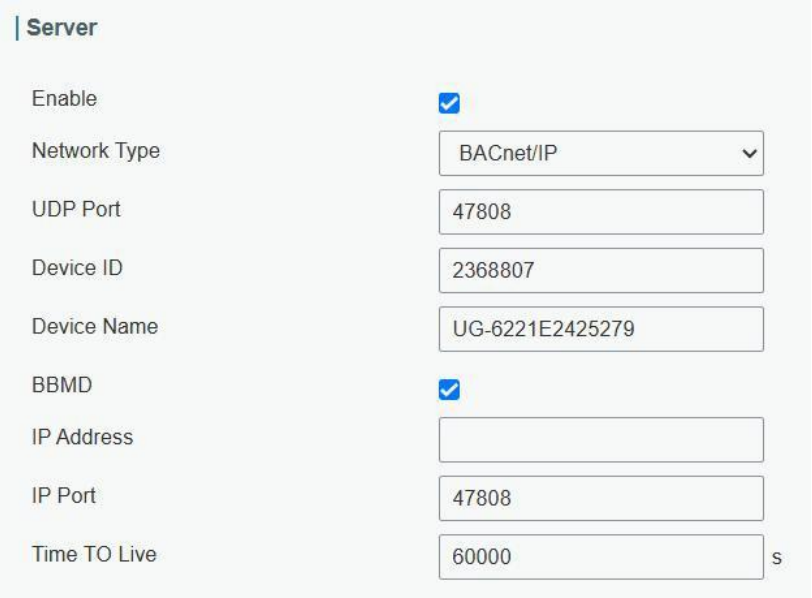


図 3-3-1-2

Server-BACnet/IP Settings	
項目	説明
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上の BACnet デバイスを連携させる場合は、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 Address**：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**：外部デバイスの登録に使用する UDP/IP ポートを入力してください。 **Time TO Live**：外部デバイスの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

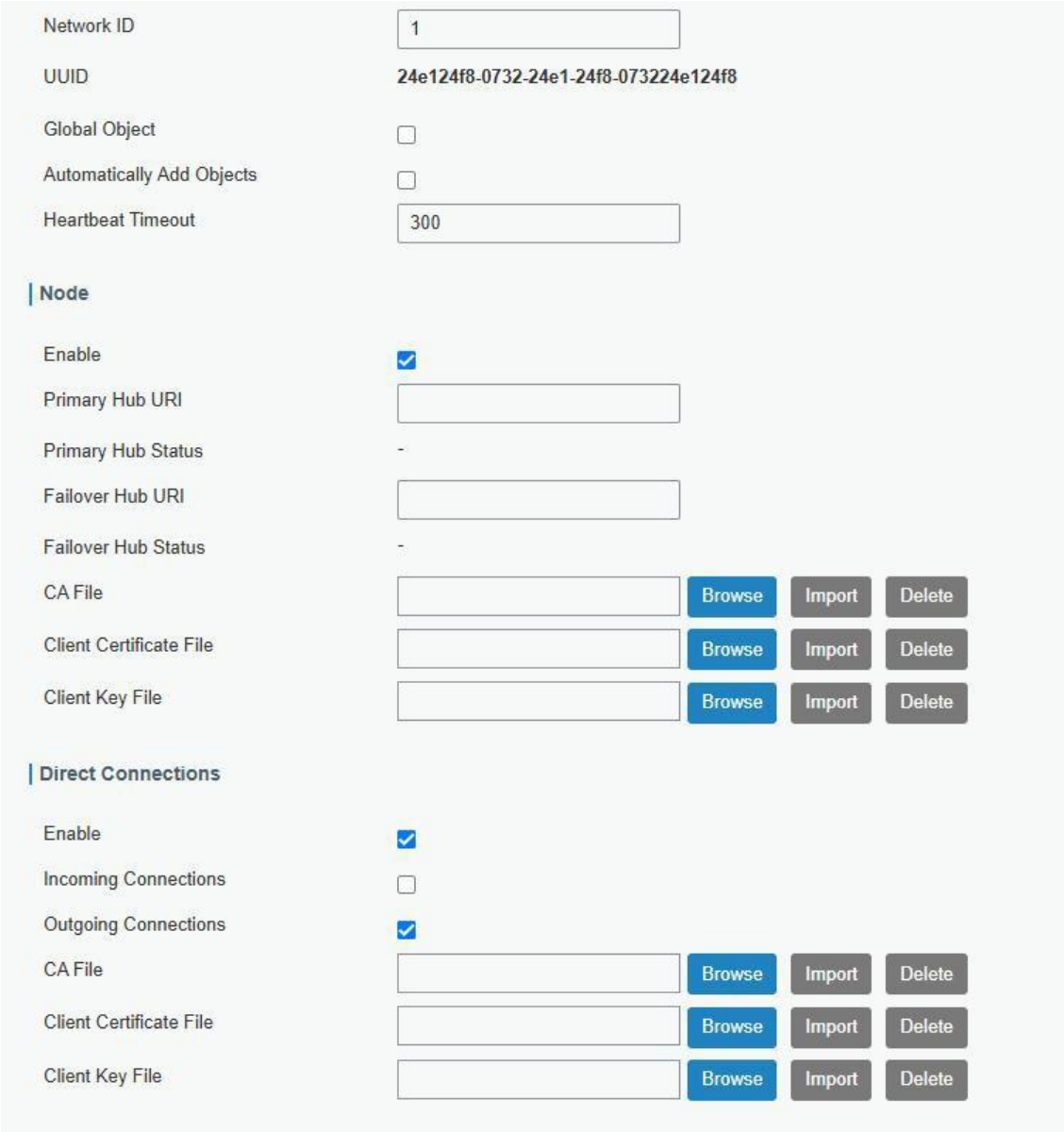


図 3-3-1-3

Server-BACnet/SC Settings	
項目	説明
Network ID	ネットワークを識別するためのネットワーク ID を設定します。同じネットワーク ID を持つデバイス同士のみ、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。
Heartbeat Timeout	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	ノードとして機能させるかどうかの設定
Primary Hub URI	プライマリハブのURIを設定します。URIの形式（アドレスはIPまたはドメイン名）：*wss://アドレス:ポート*
Primary Hub Status	ノードとプライマリハブ間の接続ステータスを表示します。
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。

	プライマリハブへの接続に失敗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ステータスを表示します。 URI 形式（アドレスは IP またはドメイン名です）： *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ます。
Direct Connections	
Enable	有効または無効にして、他のノードとの直接接続を設定します。
Incoming Connections	他のノードからの接続を有効または無効にします。このゲートウェイには最大10ノードまで接続できます。 **Port Number**：接続を許可するポート番号を設定します。 **CA File/Server Certificate File/Server 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。 **Device ID**：ゲートウェイに接続するノードのデバイス 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ステータスを表示します。
Outgoing Connections	他のノードに接続するには、有効または無効に設定してください。1 つのゲートウェイは、最大 10 個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。**名前**：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の形式（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ステータスを表示します。

表 3-3-1-3 Server-BACnet/SC パラメータ

3.3.1.2 BACnet オブジェクト

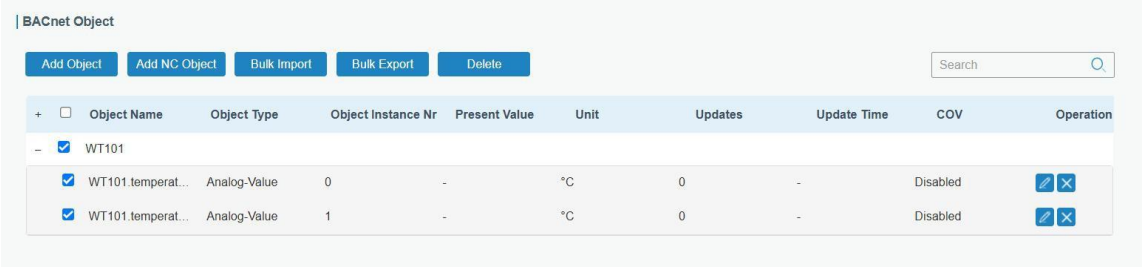


図 3-3-1-4

項目	説明
Add Object	クリックして、このサーバーに追加したいオブジェクトを選択してください。ゲートウェイは、最大 10,000 個のオブジェクトの追加に対応しています。

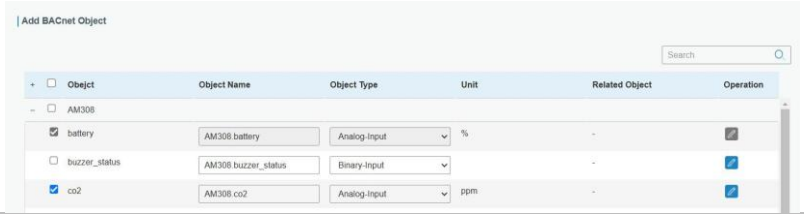
	注：ペイロードコーデックの内容が正しいことを確認し、デバイスが正しいペイロードコーデックを選択していることを確認してください。 
Add NC Object	アラームの受信者を決定するために、Notification-Class タイプのオブジェクトを追加します。ゲートウェイは、最大 200 個の NC オブジェクトの追加に対応しています。
Bulk Import	テンプレートをダウンロードして、複数のBACnetオブジェクトをインポートします。
Bulk Export	エクスポートしたいオブジェクトを選択し、.xlsx形式のファイルとしてエクスポートします。
Delete	削除したいオブジェクトを選択してください。
Object Name	BACnetオブジェクトの名前を表示します。
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の値を表示します。
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日時を表示します。
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	オブジェクトを編集または削除します。

表 3-3-1-4 BACnet オブジェクトリストのパラメータ

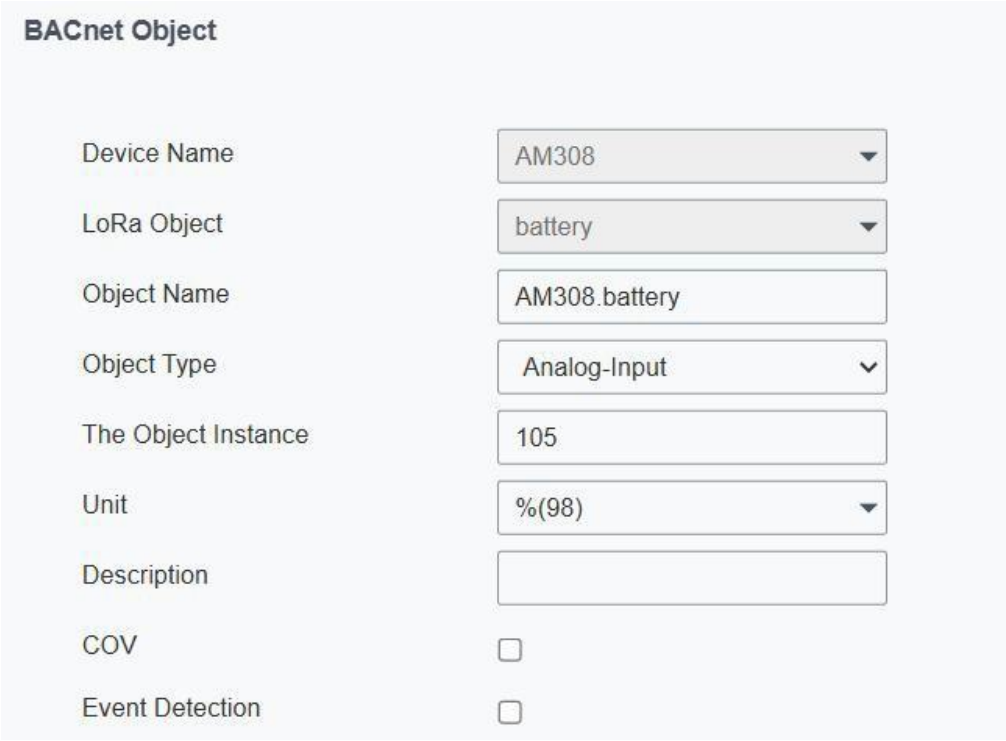


図 3-3-1-5

BACnet Object Configuration	
項目	説明
Device Name	デバイスの名前を表示します。
LoRa Object	対応するLoRaオブジェクトの名前を表示します。
Object Name	このオブジェクトの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として、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、および文字列値を選択します。
The Object Instance	オブジェクトのインスタンスをカスタマイズします。
Description	このオブジェクトの説明を入力してください。
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I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	このオブジェクト値の単位を選択してください。
COV	オブジェクトの値が変化すると、BACnet サーバー（ゲートウェイ）は新しい値の通知を BACnet クライアントに送信します。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するか、それを超えた場合にのみ、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よる意図された効果を特徴づけます。**例：**ボタンが押され、バイナリ入力が 1 の場合、アクティブテキストは「押下」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記述します。**例：**ボタンの場合、非アクティブテキストは「押されていない」と定義できます。
Relinquish Default	コマンドがない場合、バイナリ出力はこのリリンキッシュの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デフォルト値に設定されます。
Event Detection	
Notification Class	このアラームの受信者を決定するために、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、上限または下限に達した際にイベントを報告するかどうかを選択してください。

Deadband	「To Offnormal」ステータスにおいて、現在の値が（上限値－デッドバンド）または（下限値＋デッドバンド）の値に戻り、かつその状態がディレイ時間継続した場合、デバイスは「To Normal」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が利用可能です。
Time Delay	現在の値がしきい値条件に一致した場合、またはこの時間しきい値外にある場合にのみ、デバイスは対応するイベントを報告します。
Alarm Value	現在の値がアラーム値と一致している場合、遅延時間後に「To Offnormal」イベントを報告します。現在の値がアラーム値と一致していない場合、遅延時間後に「To Normal」イベントを報告します。このオプションは、「Binary Input」、「Binary Value」、「Multi-State Input」、または「Multi-State Value」にのみ適用されます。
Fault Value	現在の値がフォールト値と等しい場合、「To Fault」イベントを報告します。 このオプションは、マルチステート入力またはマルチステート値にのみ利用可能です。
Feedback Value	現在の値がフィードバック値と等しい場合、遅延時間後に「To Offnormal」イベントを報告します。現在の値がフィードバック値と等しくない場合、遅延時間後に「To Normal」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にのみあります。
Notification Type	通知タイプとして「Alarm」または「Event」を選択します。

表 3-3-1-5 BACnet オブジェクト設定パラメータ

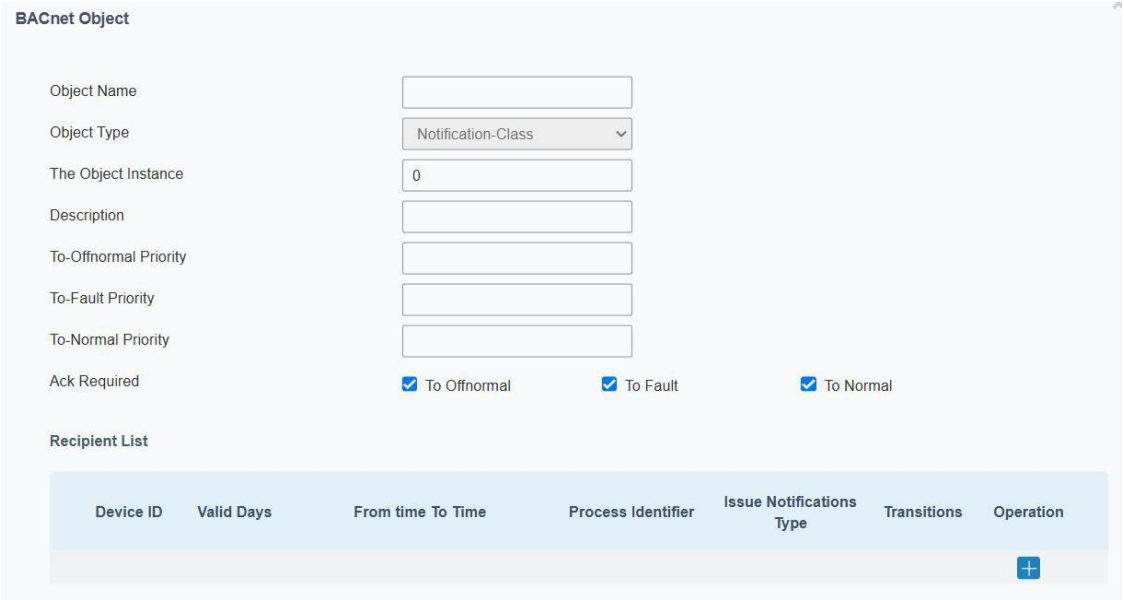


図 3-3-1-6

Notification Class BACnet Object Configuration	
項目	説明
Object Name	このオブジェクトの固有の名前をカスタマイズしてください。
Object Type	「Notification-Class」に固定されています。
The Object Instance	オブジェクトのインスタンスをカスタマイズします。

Description	このオブジェクトの説明を入力してください。
To-Offnormal Priority To-Fault Priority To-Normal Priority	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を設定します。 範囲：0～255（0が最も重要、255が最も重要度が低い）
Ack Required	このイベントにおいて、受信者が 確認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ます。
Recipient List	イベント検出が有効になっており、この通知クラスが選択されている場合、イベント通知はこのリストにある受信者に送信されます。1つのリストは、最大10人の受信者を対応できます。 **Device ID**：対象となる受信者のデバイス ID です。 **Valid Days**：通知を送信する有効期間。 **From time to time**：通知を送信する有効な時間帯です。 **Process Identifier**：アラームがどのプロセスを対象としているかを示す識別子です。例えば、プロセス識別子1はメンテナンスアラーム、2は重大アラーム、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 Notifications Type**：通知タイプとして「確認済み」または「未確認」を選択してください。ゲートウェイが「確認済み」通知の応答を受信しなかった場合、通知を再度送信します。 **Transitions**：報告されるイベントの種類を選択します。

表 3-3-1-6 通知クラス BACnet オブジェクト設定パラメータ

3.3.2 Modbus Server

UG56 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 コマンドを受信して、LoRaWAN® デバイスへの読み書きを行うことができます。この機能を使用する前に、内蔵ペイロードコーデックライブラリのバージョンが最新であることを確認し、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確認してください。

3.3.2.1 Server

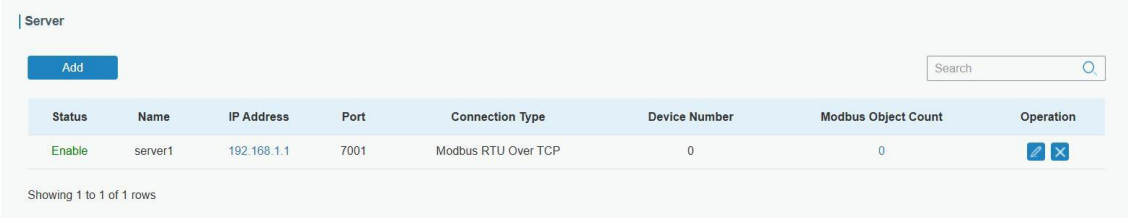


図 3-3-2-1

項目	説明
Add	Modbus サーバー（スレーブ）を追加します。1 つのゲートウェイで、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、クリックして詳細を確認します。
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オブジェクト数を表示します。詳細を確認するには、その数字をクリックしてください。
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

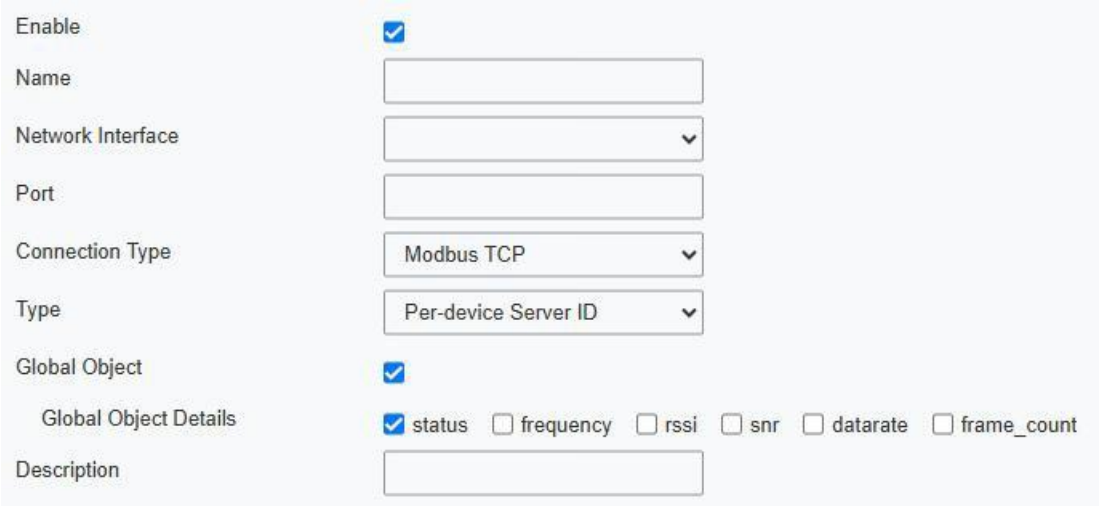


図3-3-2-2

Server Settings	
項目	説明
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指定します。
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ます。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を使用することを対応しています。
Port	このサーバーの通信ポートを設定してください。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 TCP**：Modbus クライアントは、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、Modbus RTU 形式のコマンドをこの Modbus サーバーに送信します。
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 を設定する対応があります。
Global Object	有効にすると、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にされていない限り、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**：デバイスの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 Modbus Object

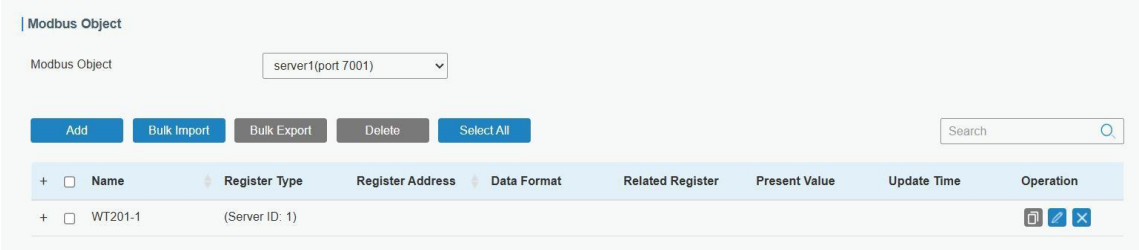
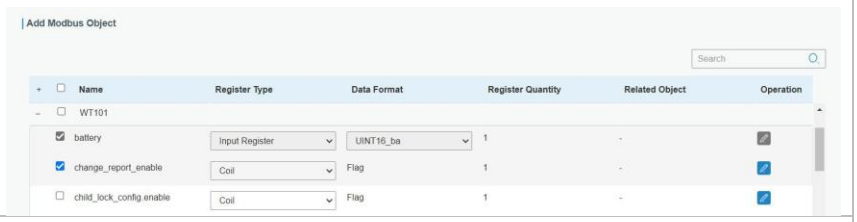


図 3-3-2-3

項目	説明
Modbus Object	オブジェクトを追加および編集する Modbus サーバーを選択してください。
Add	クリックして、このサーバーに追加したいオブジェクトを選択してください。ゲートウェイは最大10,000個のオブジェクトの追加に対応しています。 注：ペイロードコーデックの内容が正しく、デバイスが正しいペイロードコーデックを選択していることを確認してください。 
Bulk Import	テンプレートをダウンロードして、複数の Modbus オブジェクトをインポートします。
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ます。
Delete	削除したいオブジェクトを選択してください。
Select All/Deslect All	すべてのオブジェクトを選択または選択解除します。
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の値を表示します。
Update time	このオブジェクトがデータを取得および更新した日時を表示します。
Operation	：オブジェクトを編集します。

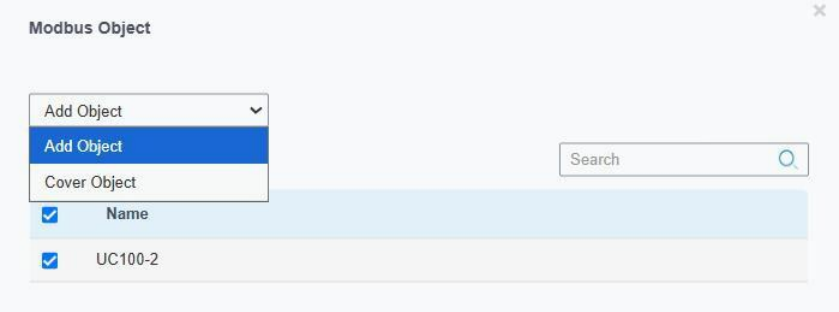
	: オブジェクトを削除します。 : コピーが必要なオブジェクトを選択し、このアイコンをクリックして、他の同じモデルのデバイスにオブジェクトを追加または適用します。 **Add Object**：選択したデバイスにオブジェクトを追加します。 **Cover Object**：選択したデバイスにオブジェクトをコピーします。選択したデバイスの元のオブジェクト設定は消去されます。 

表 3-3-2-3 Modbus オブジェクトリストのパラメータ

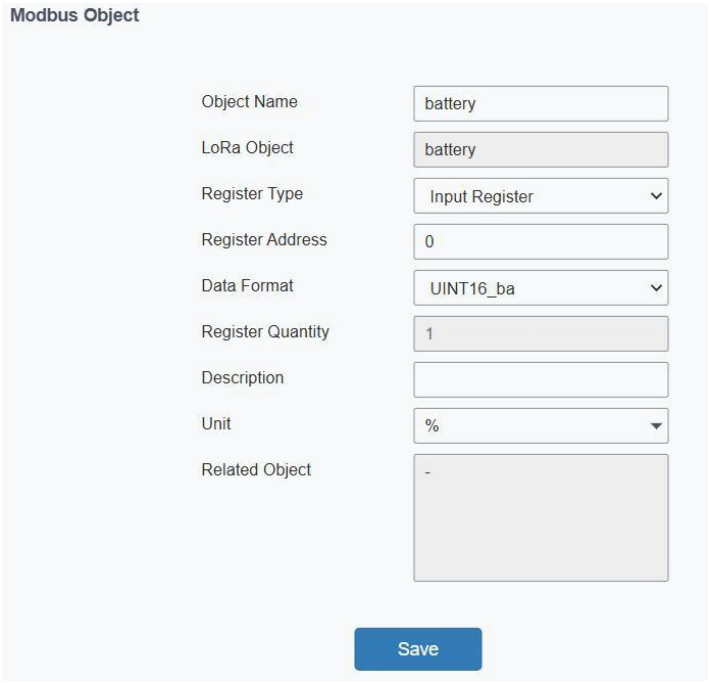


図 3-3-2-4

Modbus Object Configuration	
項目	説明
Object Name	このオブジェクトの固有の名前をカスタマイズします。
LoRa Object	対応するLoRaオブジェクトの名前を表示します。
Object Name	このオブジェクトの一意の名前をカスタマイズします。
Register Type	Modbus レジスタタイプを選択してください。 **Discrete Input**：読み取り専用で、0 および I のステータスのみを含みます。 **Coil**：読み書き可能、0 および I のステータスのみを含みます。 **Holding Register**：読み書き可能、アナログ値、文字列などを含みます。

	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、このアドレスには変更に対応しています。範囲：0～65535 注： 1) 1つのModbusサーバー内では、同じレジスタタイプのアドレスは異なるものでなければなりません。 2) アドレスはレジスタ数に関連しています。このオブジェクトのアドレスが0で、レジスタ数が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	このオブジェクトが占有するレジスタ数を表示します。
Description	このオブジェクトの説明を入力します。
Unit	このオブジェクトの単位を選択してください。
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は、関連レジスタも一緒に書き込む必要があります。そうしないと、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 オブジェクト設定パラメータ

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を接続することでインターネットにアクセスできます。3種類の接続方式に対応しています。

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

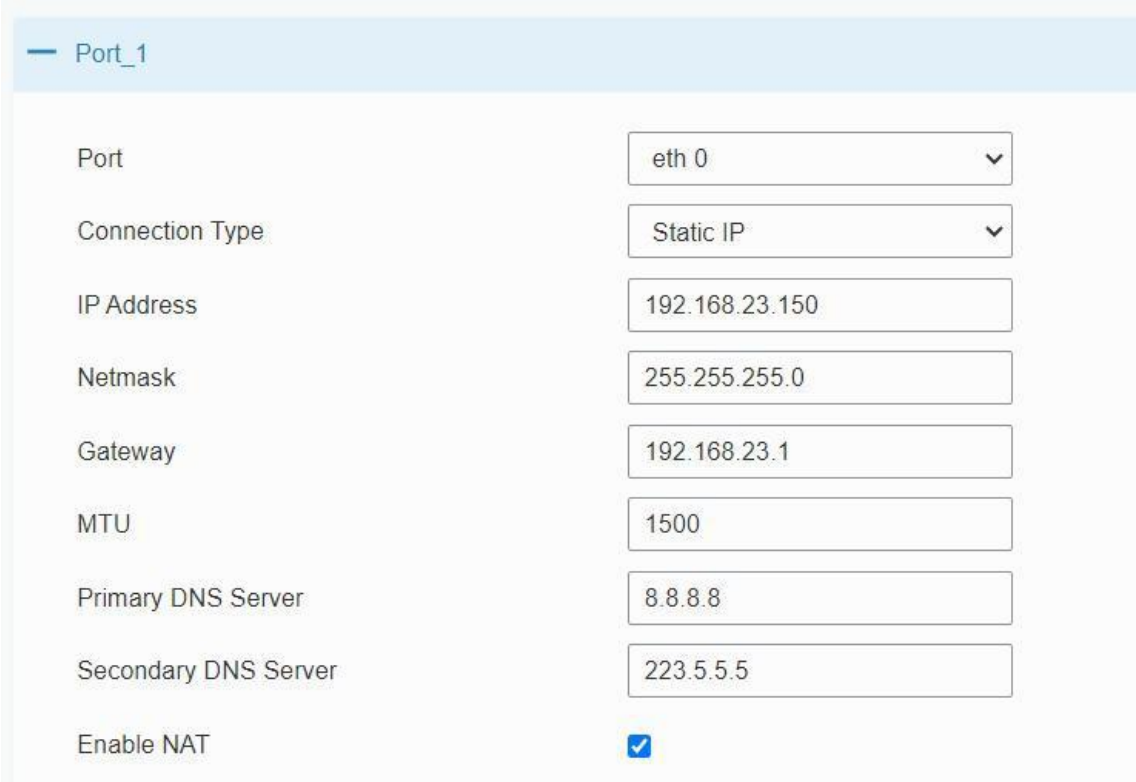


図 3-4-1-1

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

表 3-4-1-1 ポートパラメータ

関連する設定例

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。

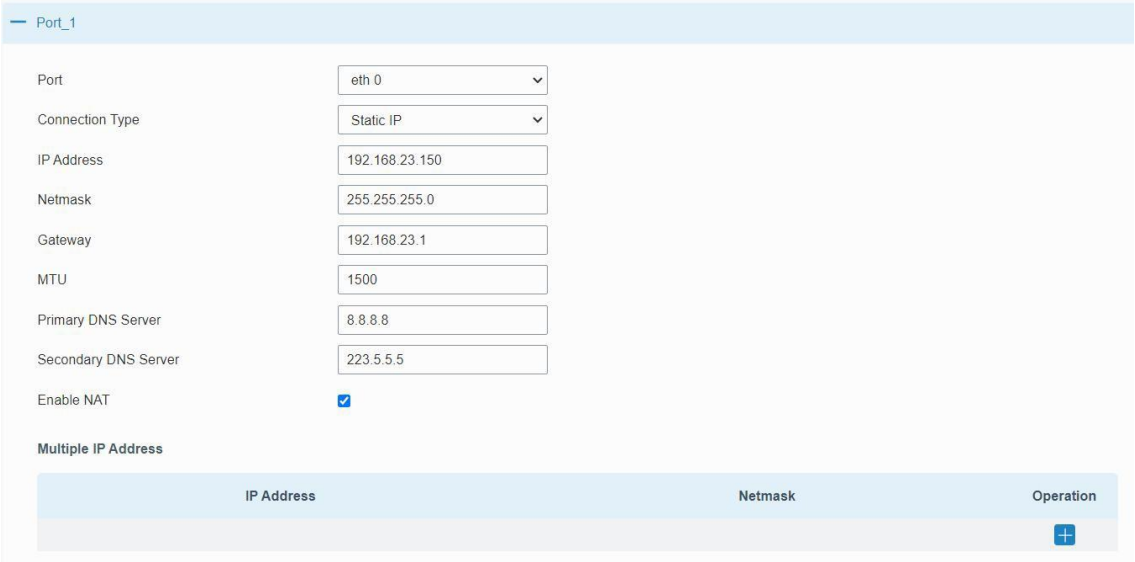


図 3-4-1-2

Static IP		
項目	説明	デフォルト
IP Address	インターネットにアクセスできるIPアドレスを設定してください。	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の IP アドレスを設定します。	Null

表 3-4-1-2 静的 IP パラメータ

2. DHCP Client

外部ネットワークで DHCP サーバーが有効になっており、イーサネット WAN インターフェースに IP アドレスが割り当てられている場合、ユーザーは「DHCP 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。

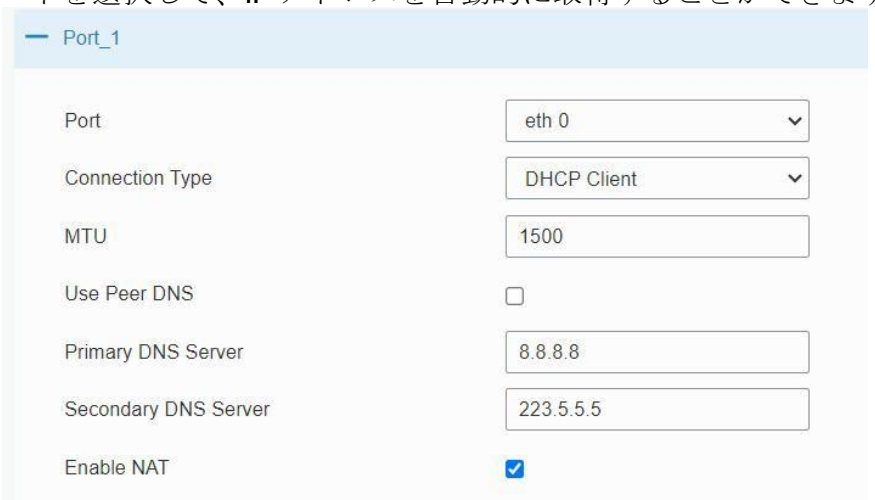


図 3-4-1-3

DHCP Client

項目	説明
Use Peer DNS	PPP ダイヤル中にピア DNS を自動的に取得します。ユーザーがドメイン名にアクセスする際には、DNS が必要です。

表 3-4-1-3 DHCP クライアントのパラメータ

3. PPPoE

PPPoEとは、イーサネット上のポイント・ツー・ポイント・プロトコルのことです。ユーザーは、元の接続方法に基づいてPPPoEクライアントをインストールする必要があります。PPPoEを使用すると、リモートアクセスデバイスが各ユーザーを管理できるようになります。

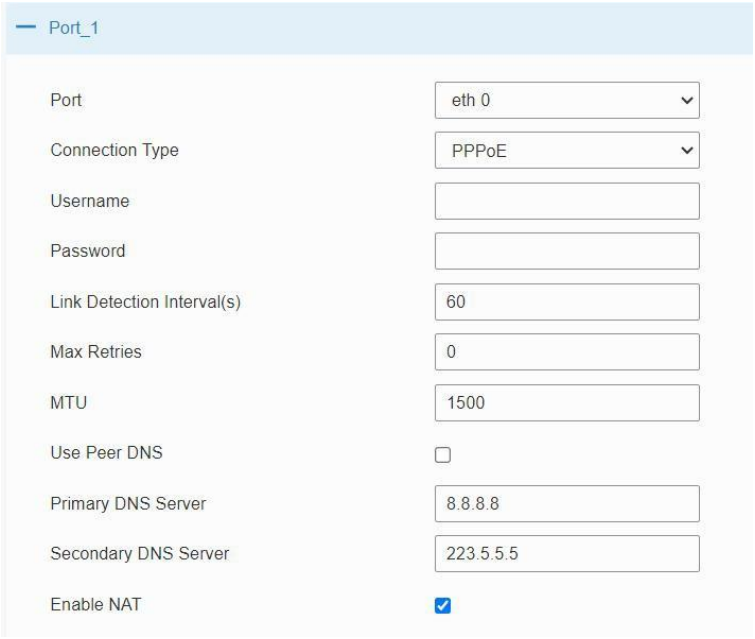


図 3-4-1-4

PPPoE	
項目	説明
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	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	ダイヤルアップがフェイルした後の最大再試行回数を設定します。範囲：0～9。
Use Peer DNS	PPP ダイヤル中にピアの DNS を自動的に取得します。ユーザーがドメイン名にアクセスする際、DNS が必要です。

表 3-4-1-4 PPOE 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。UG56 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います。

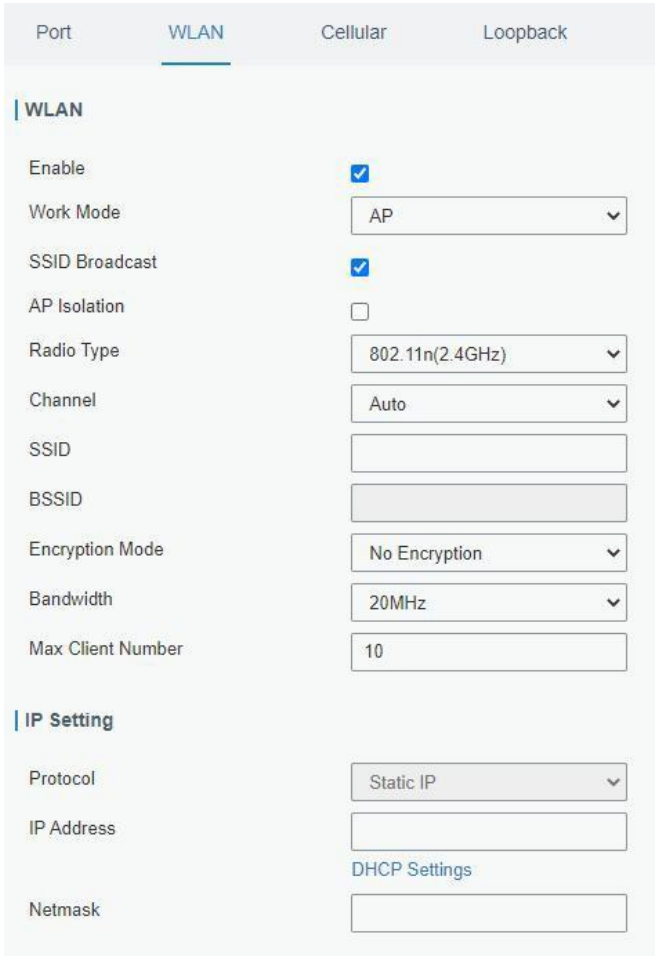


図 3-4-1-5

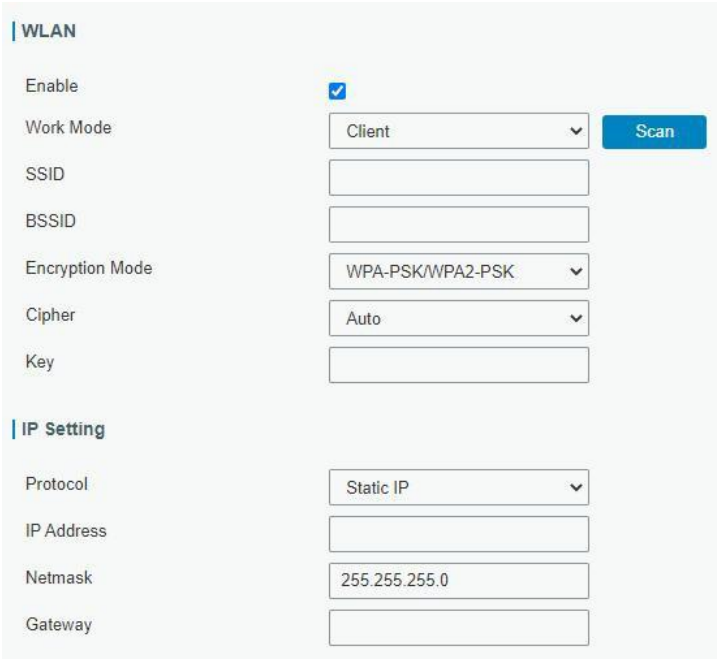


図 3-4-1-6

WLAN	
項目	説明
Enable	WLAN を有効または無効にします。

Work Mode	有効WLANを有効または無効にします。
AP Mode	
BSSID	この WLAN インターフェースの MAC アドレスを表示します。
Radio Type	無線タイプを選択してください。オプションは「802.11b (2.4 GHz)」、「802.11g (2.4 GHz)」、「802.11n (2.4 GHz)」です。
Channel	無線チャネルを選択します。選択肢は「Auto」、「1」、「2」「11」です。
Bandwidth	帯域幅を選択してください。選択肢は「20MHz」と「40MHz」です。
SSID	アクセスポイントの SSID を入力してください。
Encryption Mode	暗号化モードを選択してください。選択肢は、「No Encryption」、「WEP Open System」、「WEP Shared Key」、「WPA-PSK」、「WPA2-PSK」、および「WPA-PSK/WPA2-PSK」です。
Cipher	WPA 暗号化の暗号方式を選択してください。選択肢は、「Auto」、「AES」、「TKIP」、および「AES/TKIP」です。
Key	このアクセスポイントに接続するためのキーを入力してください。デフォルトのキーは「**iotpassword**」です。
Max Client Number	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	固定IPアドレスに設定されています。
IP Address	無線ネットワークのIPアドレスを設定します。
Netmask	ワイヤレスネットワークのネットマスクを設定します。
Client Mode	
Scan	クリックすると、このデバイスの周辺にあるアクセスポイントをスキャンします。
SSID	アクセスポイントのSSIDを入力してください。
BSSID	アクセスポイントのMACアドレスを入力してください。ネットワークに参加するには、SSIDまたはBSSIDのいずれかを入力すれば可能です。
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」、および「WPA-Enterprise/WPA2-Enterprise」です。
Cipher	WPA 暗号化の暗号を選択します。オプションは、「Auto」、「AES」、「TKIP」、および「AES/TKIP」です。
Key	このアクセスポイントに接続するためのキーを入力してください。
Xsupplicant Type	「Peap」、「Leap」、「TLS」、および「TTLS」から選択してください。
User	WPA/WPA2-Enterpriseのユーザー名を入力してください。
Anonymous Identity	WPA/WPA2-Enterpriseの匿名IDを入力してください。
Phase 2	WPA/WPA2-Enterpriseのフェーズを入力してください。
Public Server Certificate	WPA/WPA2-Enterprise アクセスポイントとの認証に使用される公開サーバー証明書です。
IP Setting	
Protocol	WLANのIPアドレスを取得するためのプロトコルを設定します。
IP Address	プロトコルが「静的IP」の場合、ワイヤレスネットワークのIPアドレスを設定します。

Netmask	プロトコルが「Static IP」の場合、ワイヤレスネットワークのネットマスクを設定します。
Gateway	プロトコルが「Static IP」の場合、ワイヤレスネットワークのゲートウェイを設定します。
Primary DNS Server	プライマリ IPv4 DNS サーバーを設定します。
Secondary DNS Server	セカンダリ IPv4 DNS サーバーを設定します。

表 3-4-1-5 WLAN パラメータ

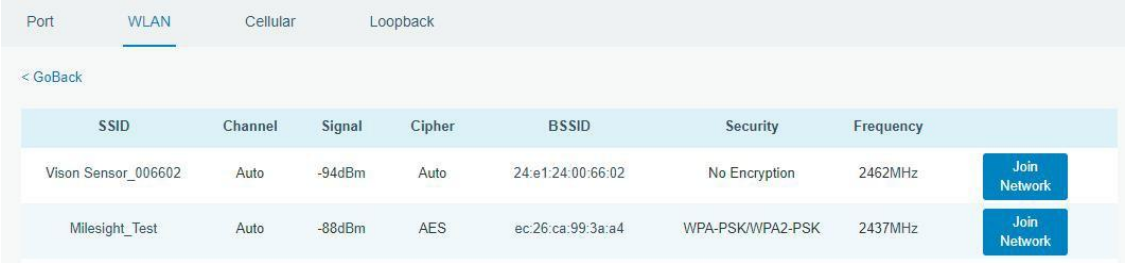


図 3-4-1-7

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	無線周波数を表示します。
Join Network	このボタンをクリックして、ワイヤレスネットワークに参加します。

表 3-4-1-6 WLAN スキャンパラメータ

関連トピック

Wi-Fi の使用例

3.4.1.3 Cellular

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。

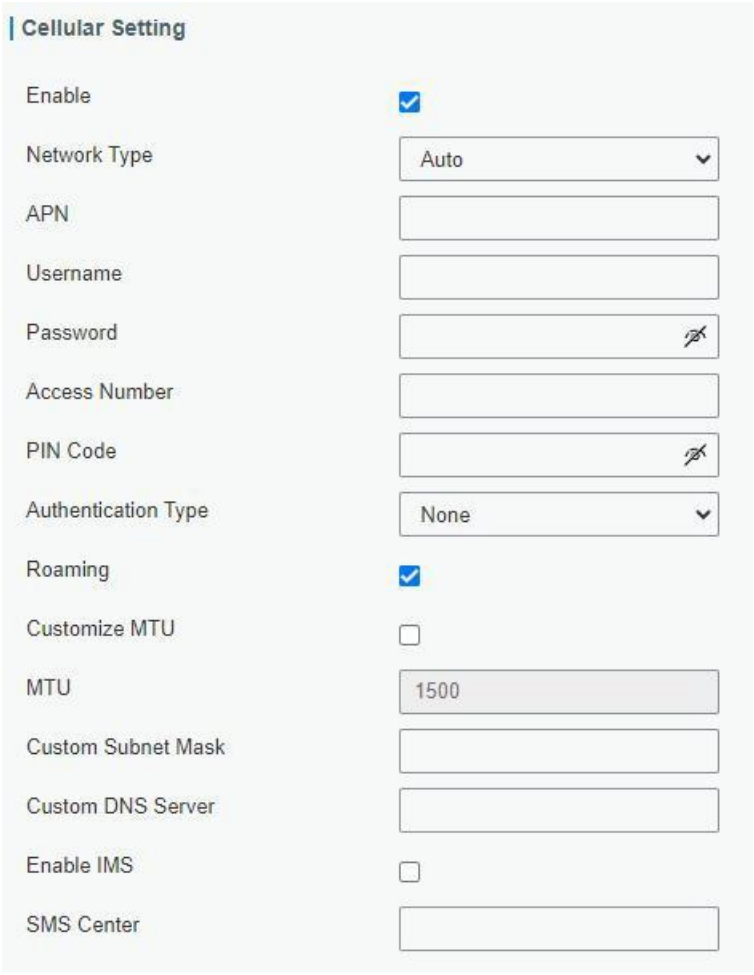


図 3-4-1-8

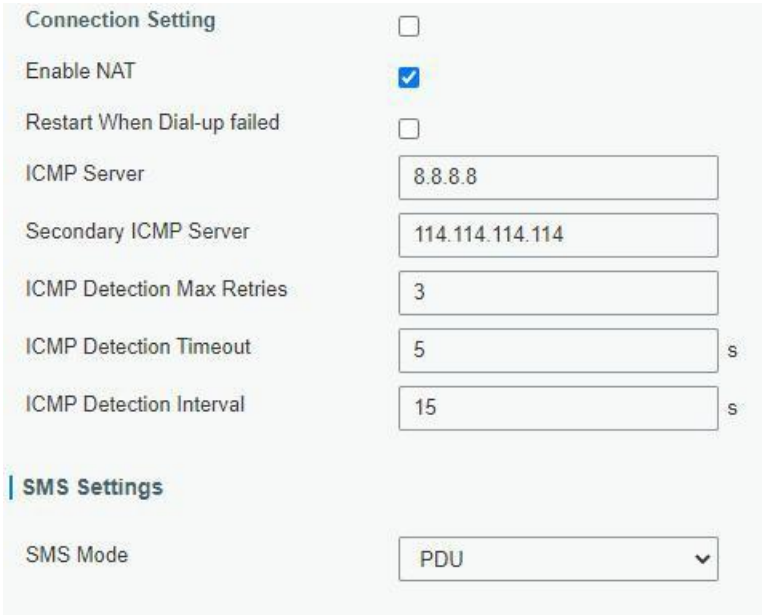


図 3-4-1-9

General Settings	
項目	説明
Enable	対応する SIM カードを有効にするには、このオプションにチェックを入れてください。

Network Type	「Auto」、「Auto 3G/4G」、「4G Only」、「3G Only」から選択してください。 Auto：信号が最も強いネットワークに自動的に接続します。 4G Only：4Gネットワークにのみ接続します。 など。
APN	お住まいの地域のISPが提供する携帯電話のダイヤルアップ接続用のアクセスポイント名を入力してください。
Username	お住まいの地域の ISP が提供する携帯電話の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ISPが提供する携帯電話ダイヤルアップ接続のパスワードを入力してください。
Access Number	お住まいの地域の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のロックを解除するための4～8文字の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	最大伝送単位をカスタマイズするために、有効または無効に設定します。 無効にすると、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	セルラーの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から提供されたサブネットマスクを使用します。 注：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。空欄の場合、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、および配信を行うためのローカルSMSセンター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。 注：ping 検出が許可されているかどうかを確認し、正しい ICMP サーバーのアドレスを取得するには、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を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際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	「TEXT」と「PDU」から SMS モードを選択します。

表 3-4-1-7 携帯電話パラメータ

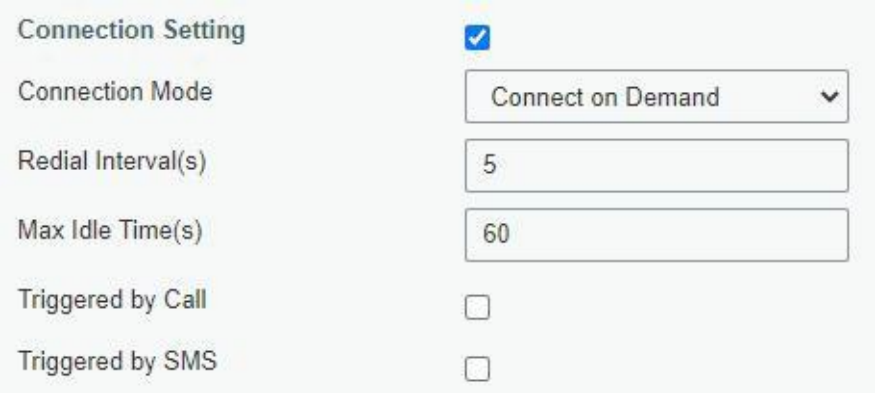


図 3-4-1-10

項目	説明
Connection Mode	
Connection Mode	「Always Online」または「Connect on Demand」から選択してください。
Redial Interval(s)	再ダイヤルの間隔を設定します。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アイドル時間を設定します。範囲：10～3600。
Triggered by Call	特定の電話番号から着信があった場合、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ます。電話グループの設定は、「System > General Settings > Phone」で行ってください。
Triggered by SMS	ゲートウェイは、特定の携帯電話から特定のSMSを受信すると、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。
SMS Group	トリガーとして使用するSMSグループを選択してください。SMSグループの設定は、「System > General Settings > Phone」で行ってください。
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 携帯電話のパラメータ

関連トピック

携帯電話接続のアプリケーション例

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、有効化されている限り、ゲートウェイのIDの代わりとして使用されます。 eインターフェースがDOWNになると、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。そのため、ゲートウェイのIDとしては、一般的にループバックインターフェースの使用が推奨されます。

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。

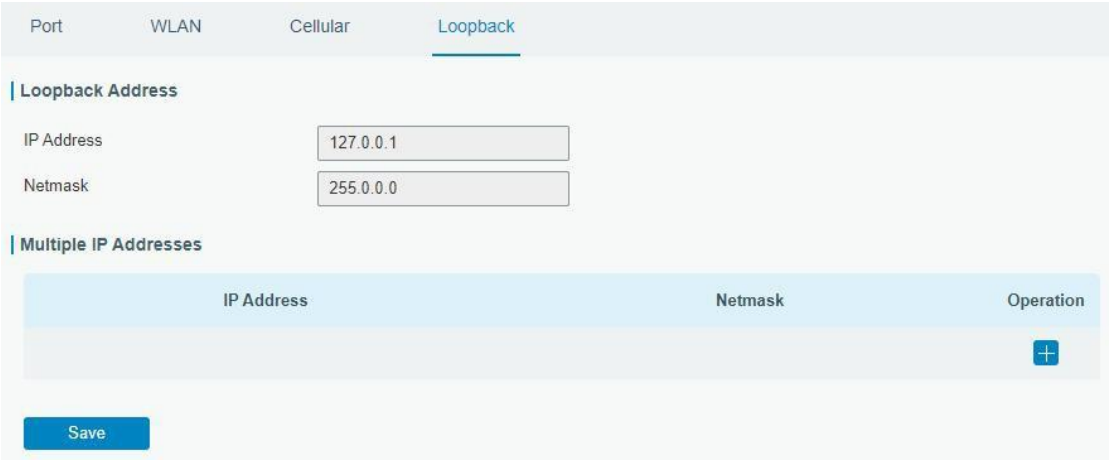


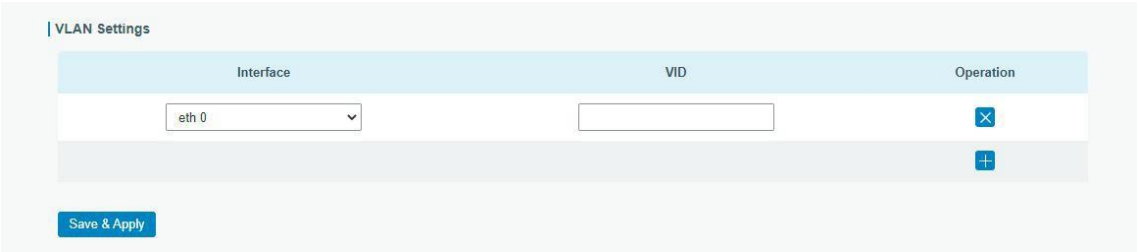
図 3-4-1-11

Loopback		
項目	説明	デフォルト
IP Address	変更不可	127.0.0.1
Netmask	変更不可	255.0.0.0
Multiple IP Addresses	上記のIPアドレスとは別に、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

UG56 ゲートウェイは、VLAN トランククライアントとして機能するイーサネットポー



トに対応しており、VLAN ID を割り当てることができるため、トラフィックの分類が容易になります。VLAN ID が設定されている場合、**「Network」 > 「Interface」 > 「Port」**のポートは、x を VLAN ID とした eth0.x として選択できます。VLAN 設定はデフォルトで空欄（ ）になっていますが、「 」をクリックすることで、特定のインターフェースに新しい VLAN ラベルを追加することができます。

図 3-4-1-12

VLAN Trunk	
項目	説明
Interface	VLAN インターフェースを選択してください。これは 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、Web サイトのブロック、ACL、DMZ、ポートマッピング、MAC バインディングなど、ファイアウォールのパラメータの設定方法について説明します。

ファイアウォールは、プロトコル形式、送信元/宛先 IP アドレスなどのパケットの内容特性に応じて、流入方向（インターネットからローカルエリアネットワークへ）および流出方向（ローカルエリアネットワークからインターネットへ）のデータフローを適切に制御します。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

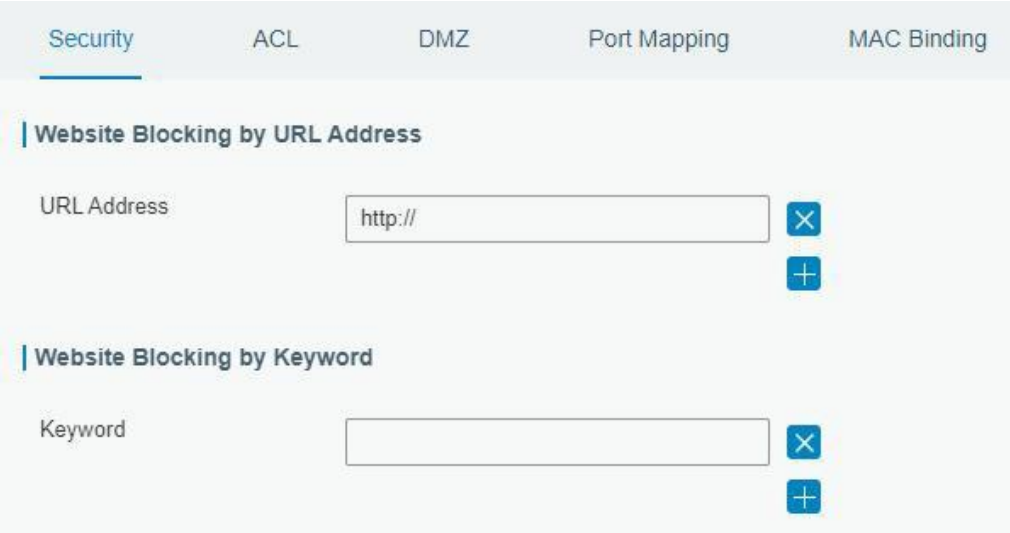


図3-4-2-1

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 Web サイトをブロックすることができます。入力できる文字数は最大 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

ACL とも呼ばれるアクセス制御リストは、一連のマッチングルールを設定して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することにより、指定されたネットワークトラフィック（送信元 IP アドレスなど）へのアクセスを許可または禁止します。ゲートウェイがパケットを受信すると、そのフィールドは現在のインターフェースに適用されている ACL ルールに従って分析されます。特定のパケットが識別されると、あらかじめ設定されたポリシーに従って、そのパケットの許可または禁止が実行されます。

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、フローの区別を必要とする他の機能でも利用できます。

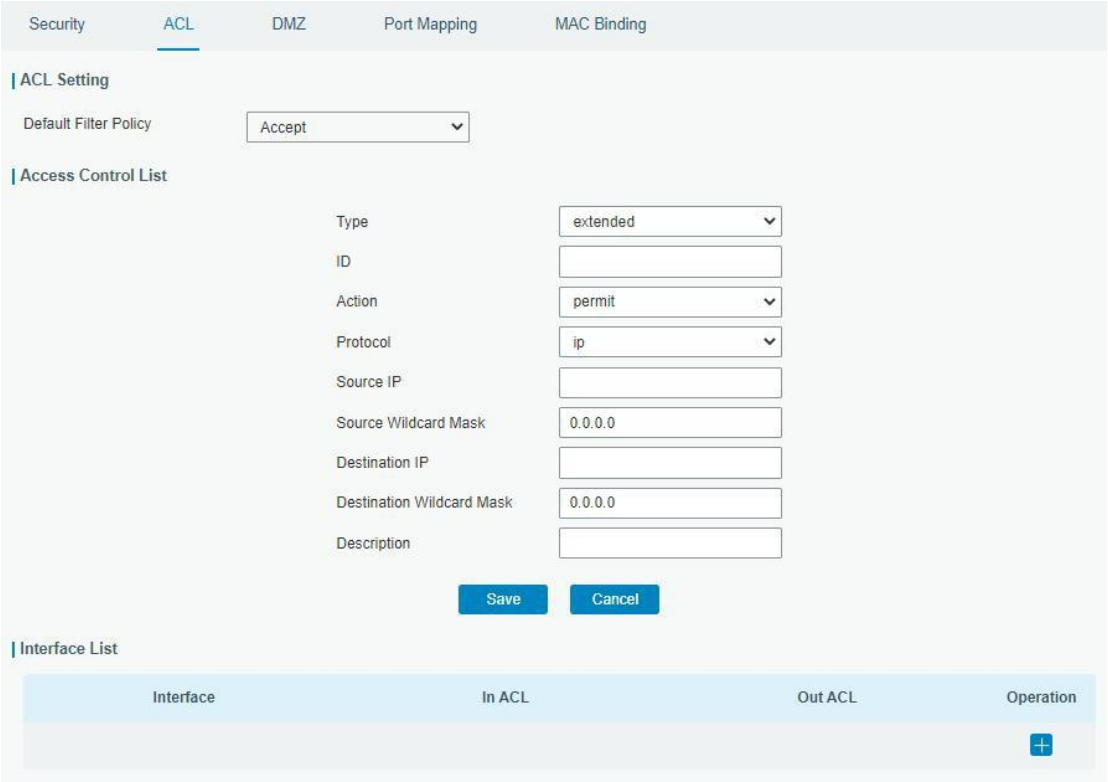


図 3-4-2-2

項目	説明
ACL Setting	
Default Filter Policy	「Accept」または「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」または「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。範囲：1～199。
Action	「Permit」または「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となります）。
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	同じ 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（指定ポート、ポート範囲など）を選択してください。
Source Port	送信元ポート番号を設定してください。範囲：1～65535。
Start Source Port	送信元ポートの開始番号を設定します。範囲：1～65535。
End Source Port	送信元ポート番号を設定します。範囲：1～65535。

Destination Port Type	宛先ポートの種類（指定ポート、ポート範囲など）を選択してください。
Destination Port	宛先ポート番号を設定します。範囲：1～65535。
Start Destination Port	宛先ポートの開始番号を設定します。範囲：1～65535。
End Destination Port	宛先ポートの終了番号を設定します。範囲：1～65535。
More Details	ポートの情報を表示します。
Interface List	
Interface	アクセス制御を行う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ます。
Out ACL	送信トラフィック用のルールをACL IDから選択します。

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。

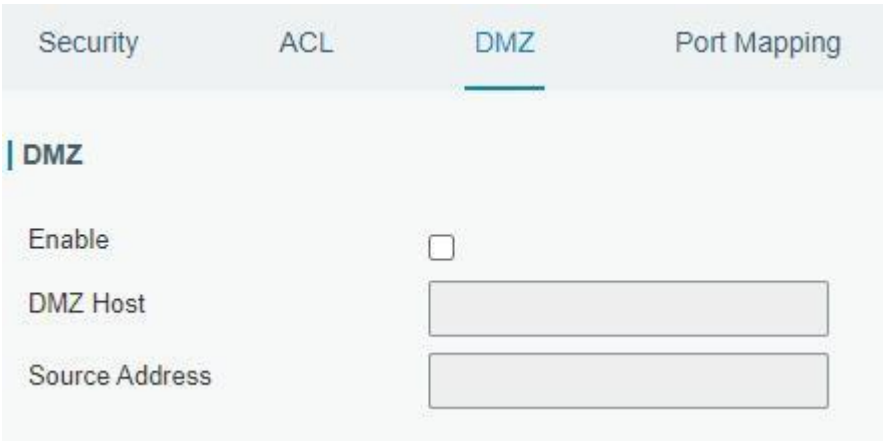


図 3-4-2-3

DMZ	
項目	説明
Enable	DMZ を有効または無効にします。
DMZ Host	内部ネットワーク上のDMZホストのIPアドレスを入力してください。
Source Address	DMZホストにアクセスできる送信元IPアドレスを設定します。 「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)

社内で外部サービスを利用する必要がある場合（例えば、Webサイトを外部に公開する場合など）、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け取ります。その後、その接続は内部接続に変換されます。この変換はDNATと呼ばれ、主に外部サービスやインターネットサービスに使用されます。

「 」をクリックして、新しいポートマッピングルールを追加します。

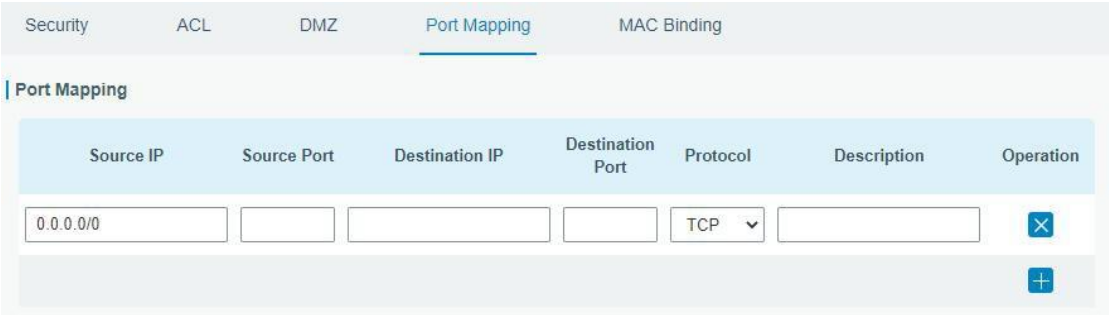


図 3-4-2-4

Port Mapping	
項目	説明
Source IP	ローカル IP アドレスにアクセスできるホストまたはネットワークを指定します。 0.0.0.0/0 はすべてを意味します。
Source Port	着信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。
Destination IP	着信インターフェースで受信されたパケットが転送される IP アドレスを入力してください。
Destination Port	着信ポートで受信された後、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」を選択してください。
Description	このルールの説明です。

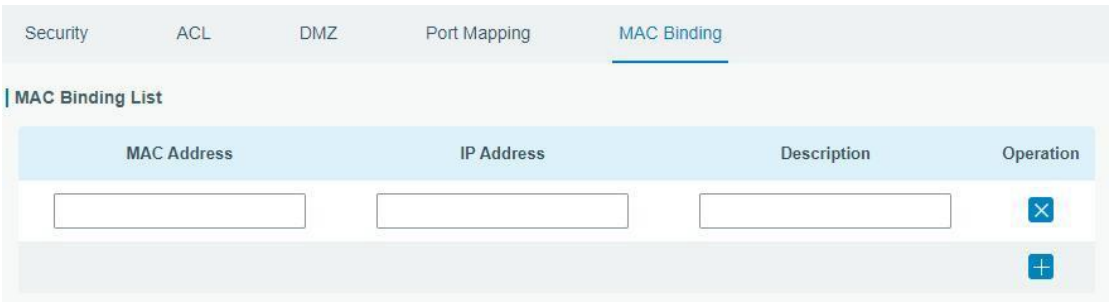
表 3-4-2-4 ポートマッピングのパラメータ

関連する設定例

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、外部ネットワークへのアクセスを許可するリストにあ



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	
項目	説明

MAC Address	バインディングMACアドレスを設定します。
IP Address	バインディング IP アドレスを設定します。
Description	各MAC-IP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に、説明を入力してください。

表 3-4-2-5 MAC バインディングのパラメータ

3.4.3 DHCP

UG56 は、Wi-Fi が AP モードで動作しているときに、IP アドレスを配布する DHCP サーバーとして設定できます。

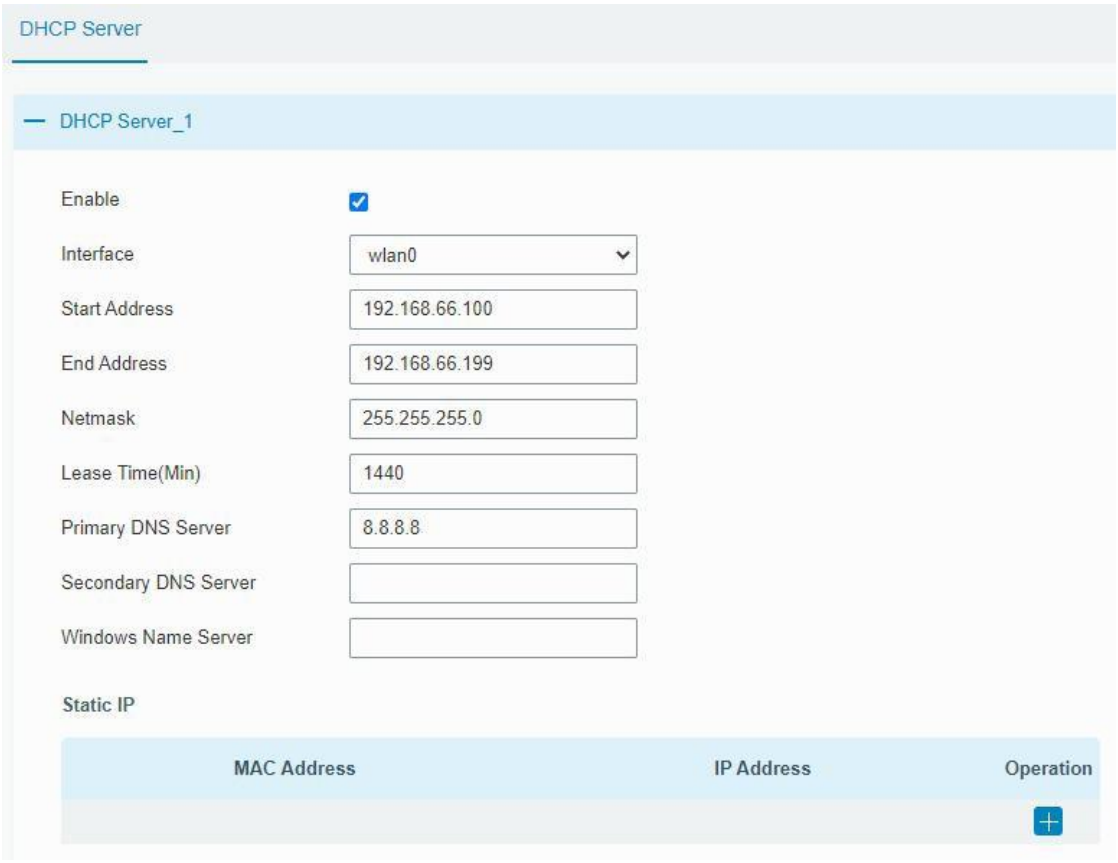


図 3-4-3-1

DHCP Server		
項目	説明	デフォルト
Enable	DHCP サーバーを有効または無効にします。	Enable
Interface	IPアドレスの割り当ては、wlanインターフェースのみが許可されます。	wlan0
Start Address	DHCPクライアントに割り当てられるIPアドレスプールの開始アドレスを定義します。	192.168.1.100
End Address	DHCP クライアントにリースされる IP アドレスプールの終了アドレスを定義します。	192.168.1.199
Netmask	DHCPクライアントがDHCPサーバーから取得するIPアドレスのサブネットマスクを定義します。	255.255.255.0
Lease Time (Min)	クライアントが DHCP サーバーから取得した IP アドレスを使用できるリース時間を設定します。範囲：1～10080。	1440

Primary DNS Server	プライマリ DNS サーバーを設定します。	8.8.8.8
Secondary DNS Server	セカンダリ DNS サーバーを設定します。	Null
Windows Name Server	DHCPクライアントがDHCPサーバーから取得するWindows インターネットネーミングサービスを定義します。通常は空欄のままにしておいてください。	Null
Static IP		
MAC Address	DHCP クライアントに特定の静的 MAC アドレスを設定します（競合を避けるため、他の MAC アドレスとは異なるものにしてください）。	Null
IP Address	DHCPクライアントに特定の静的IPアドレスを設定します（DHCPの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）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なIPアドレスを静的なドメイン名に紐付けることができます。

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。

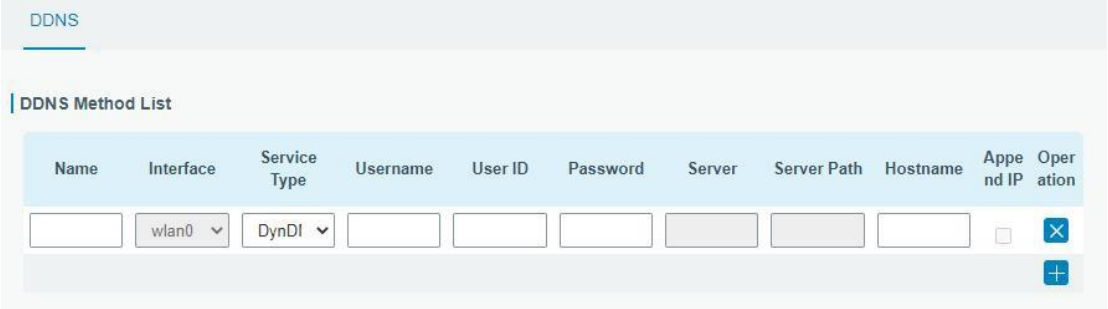


図 3-4-4-1

DDNS	
項目	説明
Name	DDNSにわかりやすい名前を付けてください。
Interface	DDNSに紐付けるインターフェースを設定します。
Service Type	DDNSサービスプロバイダ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。

設定手順

1. 1 つ以上の SLA 動作（ICMP プローブ）を定義します。
2. SLA 動作のステータスを追跡するために、1 つ以上の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、リンクプローブ方式を設定するために使用されます。デフォルトのプローブタイプはICMPです。

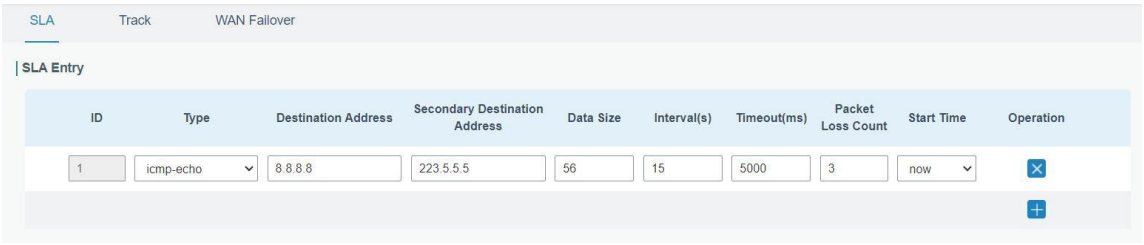


図 3-4-5-1

SLA		
項目	説明	デフォルト
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、リンクが有効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
Secondary Destination Address	検出されたセカンダリ IP アドレスです。	223.5.5.5
Data Size	ユーザー定義のデータサイズです。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検出の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です。範囲：1～300000。	5000
Packet Loss Count	各SLAプローブでパケット損失数を設定します。設定されたパケット損失数を超えると、SLAプローブはフェイルとなります。	5
Start Time	検知開始時刻。「現在」または空白文字から選択してください。 空白文字を選択した場合、このSLA検知は開始されません。	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、および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、主な機能は、さまざまな SLA モジュール間の違いを吸収し、アプリケーションモジュールに統一されたインターフェースを提供することです。

TrackモジュールとSLAモジュールの連携

設定が完了すると、Track 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、Track モジュールのリンク状態、ネットワークパフォーマンスの検出、および通知に使用されます。検出結果により、状態の変化をタイムリーに追跡することができます。

- 検出に成功した場合、対応するトラック項目は「Positive」となります。
- 検出がフェイルした場合、対応するトラック項目は「Negative」となります。

Trackモジュールとアプリケーションモジュールの連携

設定後、Trackモジュールと Applicationモジュール間の連携関係が確立されます。Track項目に変更が生じた場合、対応が必要な通知がApplicationモジュールに送信されます。

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、Trackモジュールと連携することができます。

アプリケーションモジュールに即時通知を送信する場合、復旧のタイミングやその他の理由によるルーティングのフェイルなどにより、状況によっては通信が中断される可能性があります。そのため、ユーザーは、追跡項目のステータスが変更された際に、アプリケーションモジュールへの通知を遅らせる時間を設定することができます。

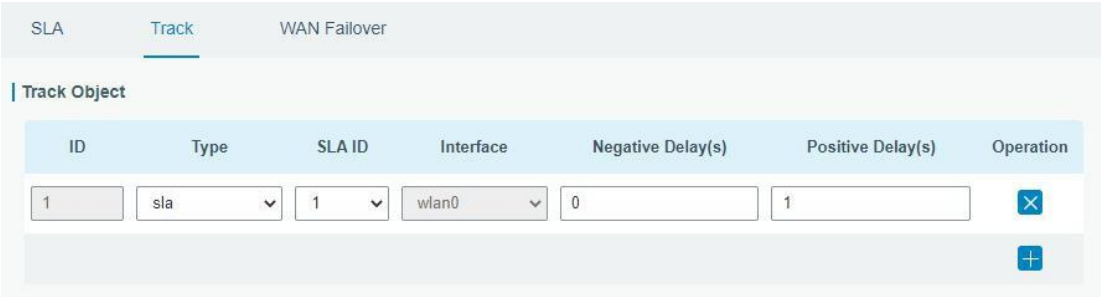


図 3-4-5-2

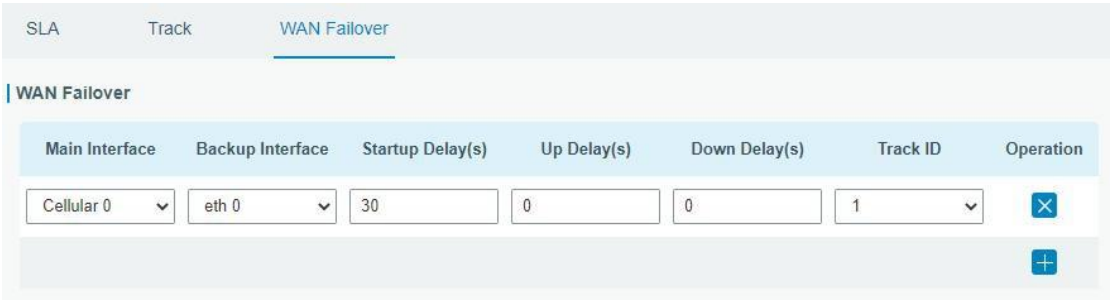
項目	説明	デフォルト
Index	トラックインデックス。最大10個のトラック設定を構成できます。範囲：1～10。	1
Type	オプションは「sla」と「interface」です。	SLA
SLA ID	定義されたSLA ID。	1
Interface	ステータスを検出するインターフェースを選択してください。	cellular0
Negative Delay (s)	インターフェースがダウン状態にある場合、またはSLAプローブがフェイルした場合、ここで設定された時間だけ待機してから、実際にステータスを「Down」に変更します。範囲：0～180（0は即時切り替えを意味します）。	0
Positive Delay (s)	フェイルからの復旧が発生した場合、ここで設定された時間だけ待機してから、実際にステータスを「Up」に変更します。範囲：0～180（0は即時切り替えを意味します）。	1

表 3-4-5-2 トラッキングパラメータ

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の不足によりサービスの送信が正常に行えない場合、トラフィックをバックアップインターフェースに迅速に切り替えることができます。その後、バックアップインターフェースがサービスの送信を行い、ネットワークトラフィックを分担することで、データ機器の通信信頼性を向上させます。
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、システムは直ちにバックアップインターフェースのリンクに切り替えるのではなく、あらかじめ設定された遅延時間を適用します。遅延時間が経過した後もメインインターフェースの状態が「ダウン」のままである場合にのみ、システムはバックアップインターフェースのリンクに切り替わります。それ以外の場合は、システムの状態は変更されません。

図 3-4-5-3



WAN Failover		
パラメータ	説明	デフォルト
Main Interface	リンクインターフェースをメインリンクとして選択します。	--
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ます。	--
Startup Delay (s)	起動追跡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「検出フェイル」から「検出成功」に切り替わった際、設定された時間に基づいて切り替えを遅延させることができます。範囲：0～180（0は即時切り替えを意味します）	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った際、設定された時間に基づいて切り替えを遅延させることができます。範囲：0～180（0は即時切り替えを意味します）。	0
Track ID	トラック検出、定義されたトラックIDを選択します。	--

表 3-4-5-3 WAN フェイルオーバーパラメータ

3.4.6 VPN

仮想プライベートネットワーク（VPN）は、2つのプライベートネットワークを安全に接続するために使用されます

ネットワークを相互に接続し、デバイスが安全な通信経路を介して一方のネットワークからもう一方のネットワークへ接続できるようにします。

UG56は、DMVPN、IPsec、GRE、L2TP、PPTP、OpenVPNに加え、GRE over IPsecおよびL2TP over IPsecにも対応しています。

3.4.6.1 DMVPN

mGRE と IPsec を組み合わせたダイナミック・マルチポイント・仮想プライベート・ネットワーク（DMVPN）は、組織の本社にある 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。

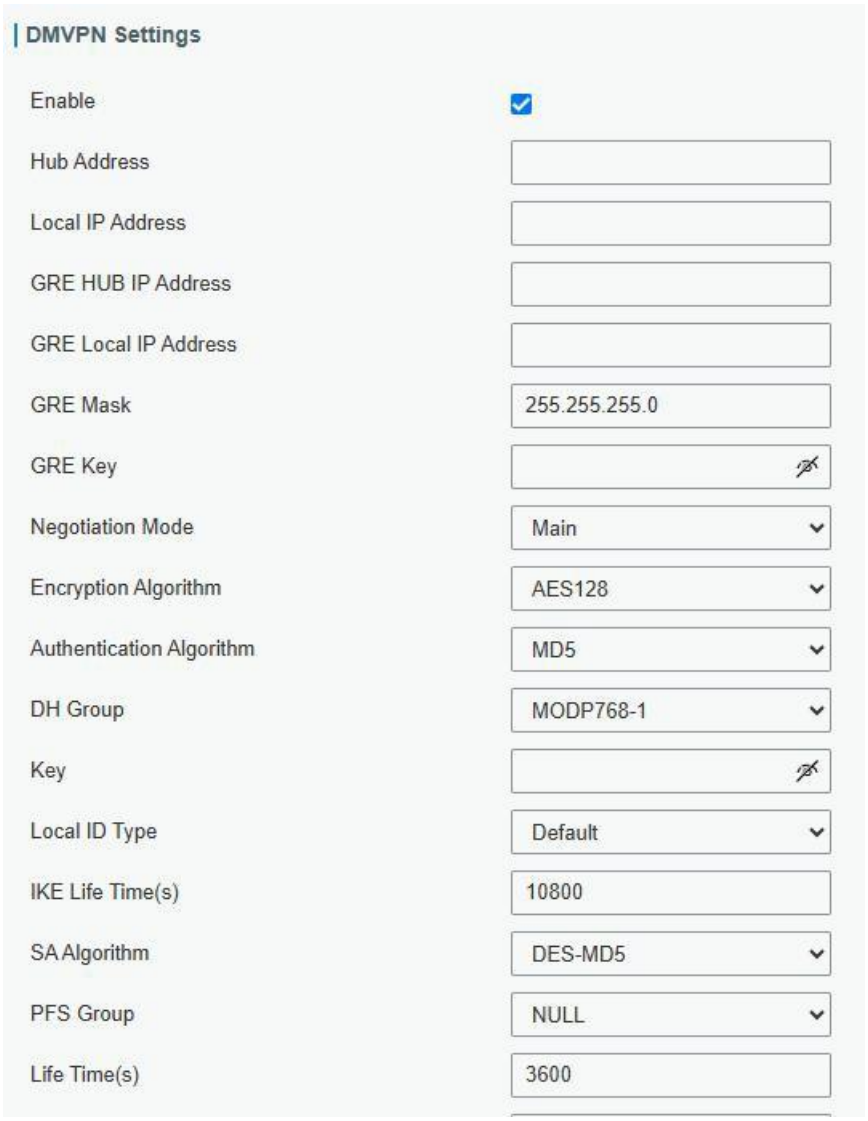


図 3-4-6-1

図 3-4-6-2

DMVPN	
項目	説明
Enable	有効化または無効化します。
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。
GRE Netmask	GRE ローカルトンネルのネットマスク。
GRE Key	GRE トンネルキー。
Negotiation Mode	「Main」または「Aggressive」から選択してください。
Encryption Algorithm	「DES」、「3DES」、「AES128」、「AES192」、および「AES256」から選択してください。
Authentication Algorithm	「MD5」または「SHA1」から選択してください。
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」、および「User FQDN」から選択してください
IKE Life Time (s)	IKEネゴシエーションの有効期間を設定します。範囲：60～86400。
SA Algorithm	「DES_MD5」、「DES_SHA1」、「3DES_MD5」、「3DES_SHA1」、「AES128_MD5」、「AES128_SHA1」、「AES192_MD5」、「AES192_SHA1」、「AES256_MD5」、および「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 インターバル時間を設定します
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を介した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、セキュリティ設定を処理できることです。

IPsec には、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) の 3 種類のセキュリティサービスがあります。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の暗号化の両方に対応します。IKE は、暗号鍵の交換に使用されます。これらはいずれも、ホスト間、ホストとゲートウェイ間、およびゲートウェイ間の 1 つ以上のデータフローを保護することができます。

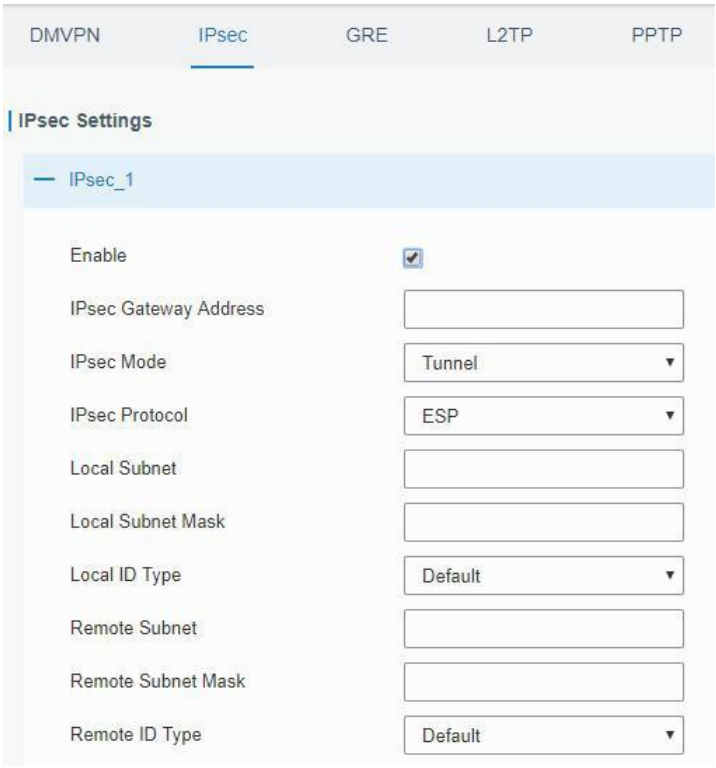


図 3-4-6-3

IPsec	
項目	説明
Enable	有効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」または「Transport」から選択してください。
IPsec Protocol	「ESP」または「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 サブネット マスクを入力してください。
Remote ID type	「Default」、「ID」、「FQDN」、および「User FQDN」から選択してください。

表 3-4-6-2 IPsec パラメータ

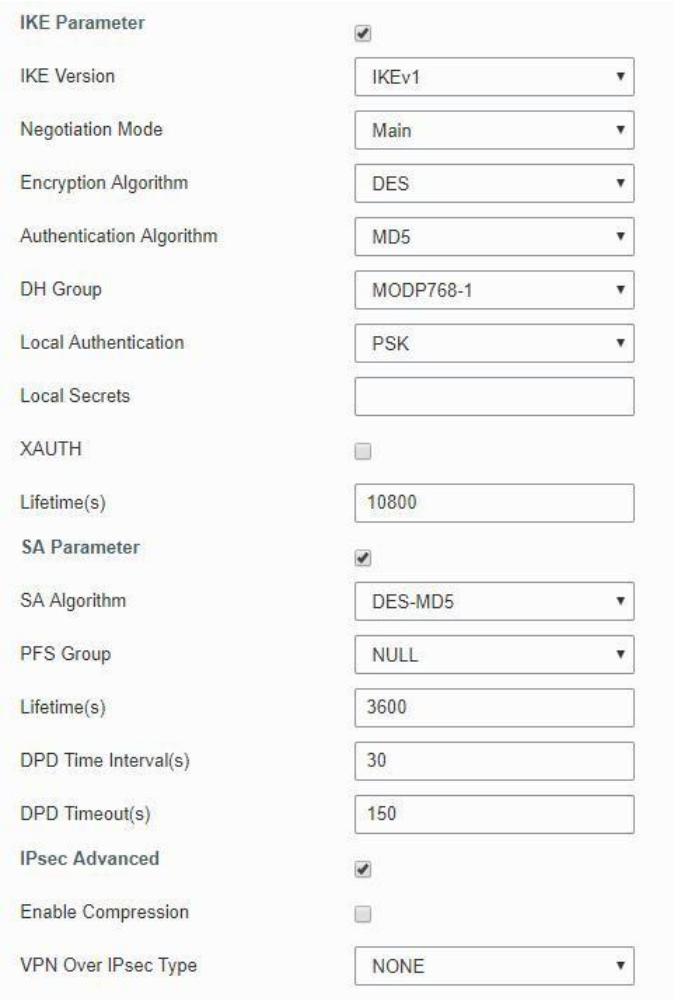


図 3-4-6-4

IKE Parameter	
項目	説明
IKE Version	「IKEv1」または「IKEv2」から選択してください。
Negotiation Mode	「Main」または「Aggressive」から選択してください。
Encryption Algorithm	「DES」、「3DES」、「AES128」、「AES192」、および「AES256」から選択してください。
Authentication Algorithm	「MD5」または「SHA1」から選択してください。
DH Group	「MODP768_1」、「MODP1024_2」、および「MODP1536_5」から選択してください。
Local Authentication	「PSK」または「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のユーザー名とパスワードを入力してください。
Lifetime (s)	IKEネゴシエーションでの有効期間を設定します。範囲：60～86400。
SA Parameter	
SA Algorithm	「DES_MD5」、「DES_SHA1」、「3DES_MD5」、「3DES_SHA1」、「AES128_MD5」、「AES128_SHA1」、「AES192_MD5」、「AES192_SHA1」、「AES256_MD5」、および「AES256_SHA1」から選択します。
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 IntervalTime(s)	リモート側のフェイルを検出するための DPD 間隔時間を設定します。
DPD Timeout(s)	DPDタイムアウトを設定します。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」、および「L2TP」から選択して、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

Generic Routing Encapsulation (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送信できるチャネルを提供し、両端でカプセル化とデカプセル化を実現できるトンネリング技術です。

以下の状況では、GRE トンネル伝送を適用できます。

- GREトンネルは、あたかも本物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送信できます。IPsecのみを使用しても、マルチキャストの暗号化は実現できません。
- 採用された特定のプロトコルはルーティングできません。
- 他の2つの同様のネットワークを接続するには、異なるIPアドレスを持つネットワークが必要となります。

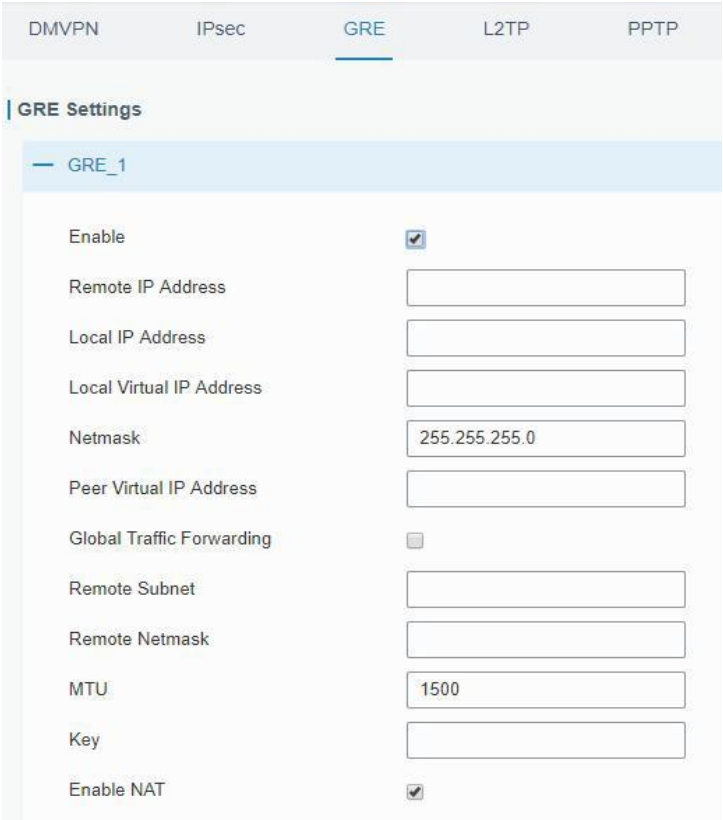


図3-4-6-5

GRE	
項目	説明
Enable	GRE 機能を有効にするには、ここに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 アドレスを設定してください。
Local Virtual IP Address	GRE トンネルのローカル IP アドレスを設定してください。
Netmask	ローカル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 IP アドレスを入力してください。
Global Traffic Forwarding	この機能を有効にすると、すべてのデータトラフィックは 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) の動作を実現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。

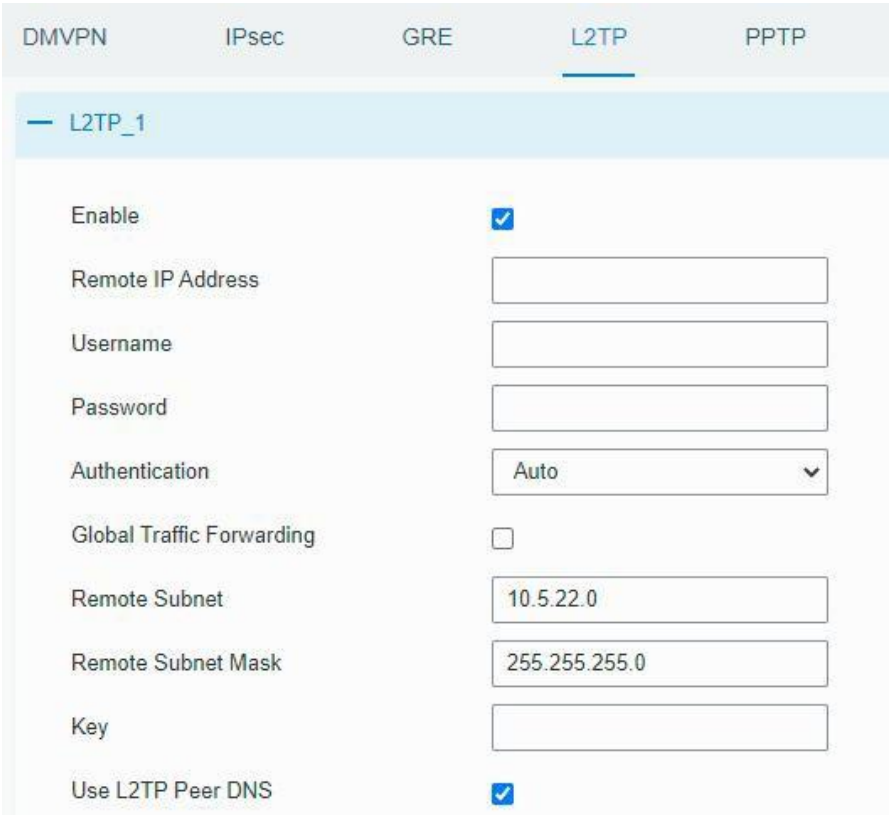


図 3-4-6-6

L2TP	
項目	説明
Enable	L2TP 機能を有効にするには、ここに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サーバーから提供されたユーザー名を入力してください。
Password	L2TP サーバーから提供されたパスワードを入力してください。
Authentication	「Auto」、「PAP」、「CHAP」、「MS-CHAPv1」、および「MS-CHAPv2」から選択してください。
Global Traffic Forwarding	この機能を有効にすると、すべてのデータトラフィックが L2TP トンネル経由で送信されます。
Remote Subnet	L2TP が保護するリモート IP アドレスを入力してください。
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。
UseL2TP Peer DNS	有効にすると、L2TP ピアサーバーの DNS アドレスが使用されます。

表 3-4-6-5 L2TP パラメータ

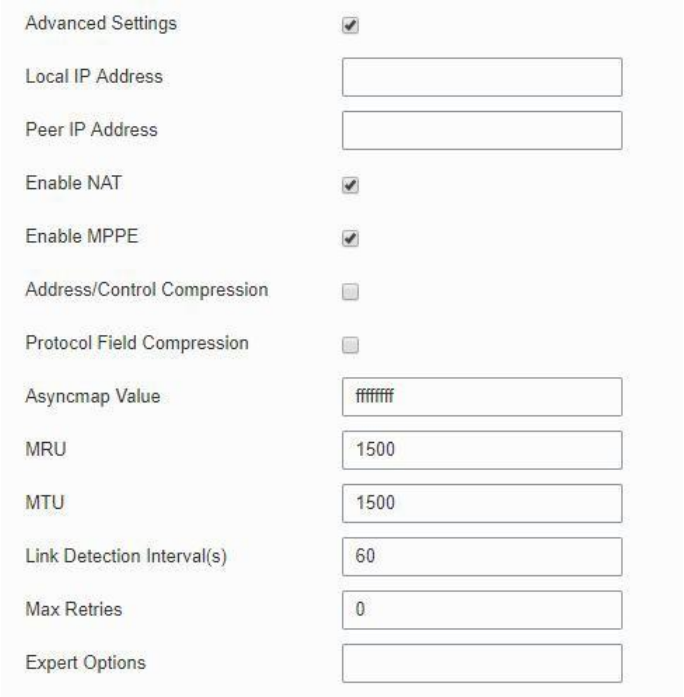


図 3-4-6-7

Advanced Settings	
項目	説明
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。この項目が空の場合、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/Control Compression	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 Field Compression	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プロトコルの初期化文字列の一つです。デフォルト値のままにしておくことができます。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再試行の最大回数を設定します。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、文字列間は空白で区切ります。

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、企業がパブリック インターネット上のプライベートな「トンネル」を通じて、自社の企業ネットワークを拡張できるようにするプロトコルです。事実上、企業は広域ネットワークを 1 つの大きなローカル エリア ネットワークとして利用することになります。

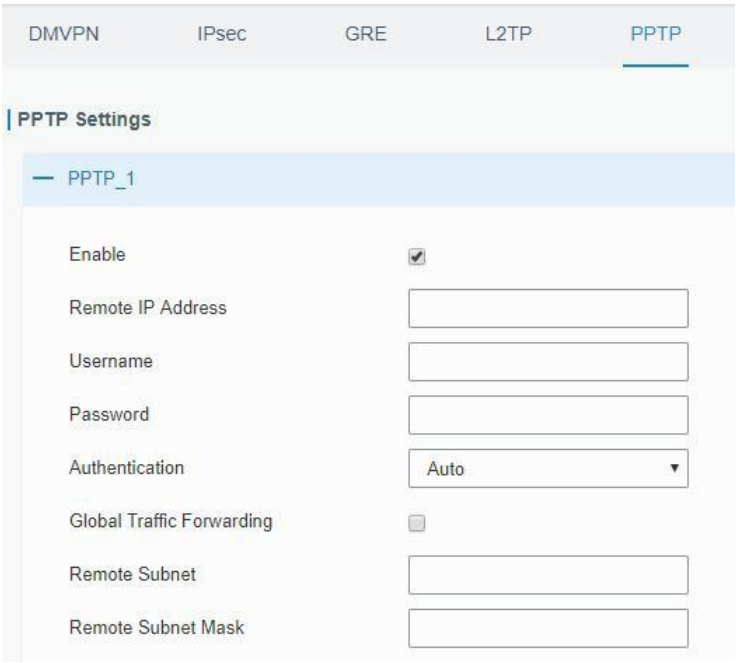


図 3-4-6-8

PPTP	
項目	説明
Enable	有効化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サーバーから提供されたユーザー名を入力してください。
Password	PPTP サーバーから提供されたパスワードを入力してください。
Authentication	「Auto」、「PAP」、「CHAP」、「MS-CHAPv1」、および「MS-CHAPv2」から選択してください。
Global Traffic Forwarding	この機能を有効にすると、すべてのデータ通信は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 Subnet Mask	ピア PPTP サーバーのネットマスクを設定します。

表 3-4-6-7 PPTP パラメータ

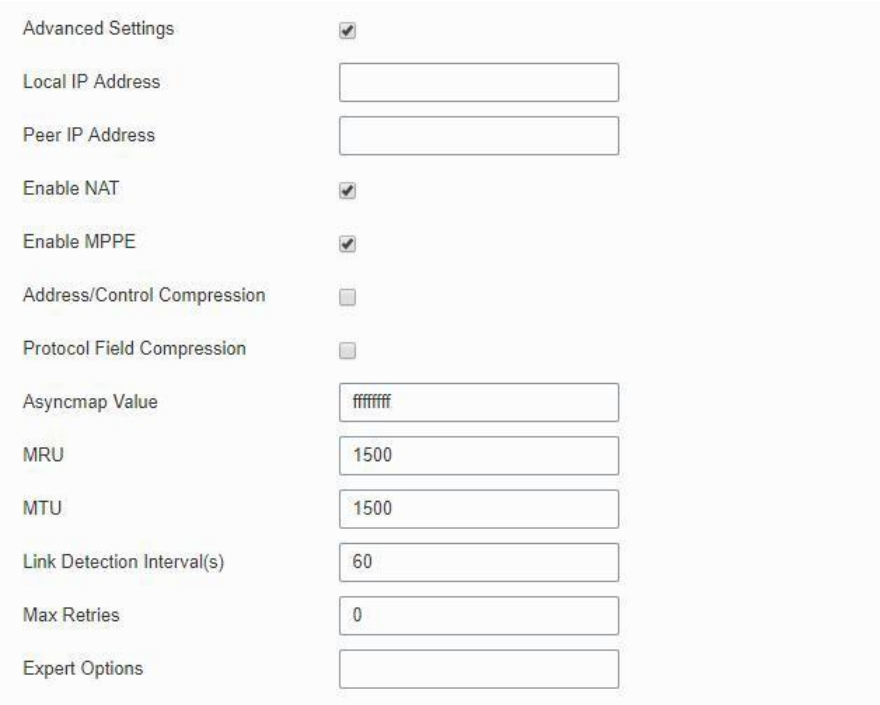


図 3-4-6-9

PPTP Advanced Settings	
項目	説明
Local IP Address	PPTP クライアントの IP アドレスを設定します。
Peer IP Address	PPTP サーバーのトンネル IP アドレスを入力してください。
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/Control Compression	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 Field Compression	PPPの初期化用です。デフォルト設定のままにしておいてください。
Asyncmap Value	PPPプロトコルの初期化文字列の一つです。デフォルト値のままにしておくことができます。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に、リンク検出間隔を設定します。範囲：0～600。
Max Retries	PPTP接続のフェイルを検出するための再試行の最大回数を設定します。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、文字列間は空白で区切ります。

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での移植性を備えた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。UG56では、最大3つのOpenVPNクライアントを同時に実行できます。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構成することができます。

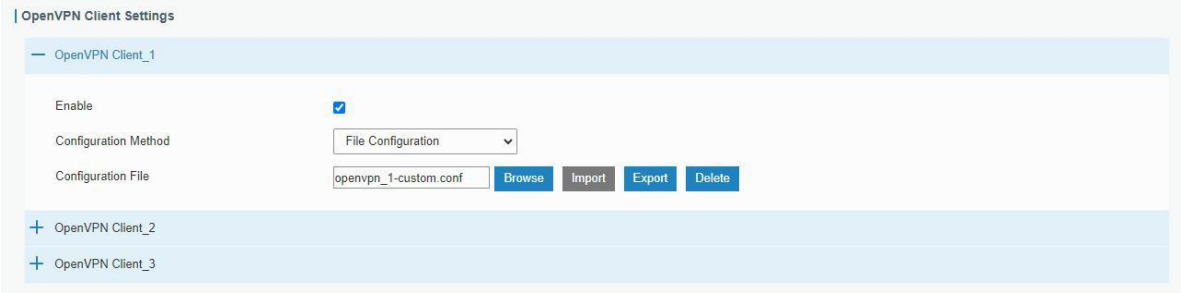


図 3-4-6-10

OpenVPN Client - File Configuration	
項目	説明
Browse	クリックすると、設定や証明書の内容を含む、ovpn 形式のクライアント設定ファイルを参照できます。以下のサンプルを参照して、クライアント設定ファイルをご確認ください：client.conf
Edit	インポートされたファイルを編集するには、ここをクリックしてください。
Export	サーバー設定ファイルをエクスポートします。
Delete	クリックして設定ファイルを削除します。

表 3-4-6-9 OpenVPN クライアントのパラメータ

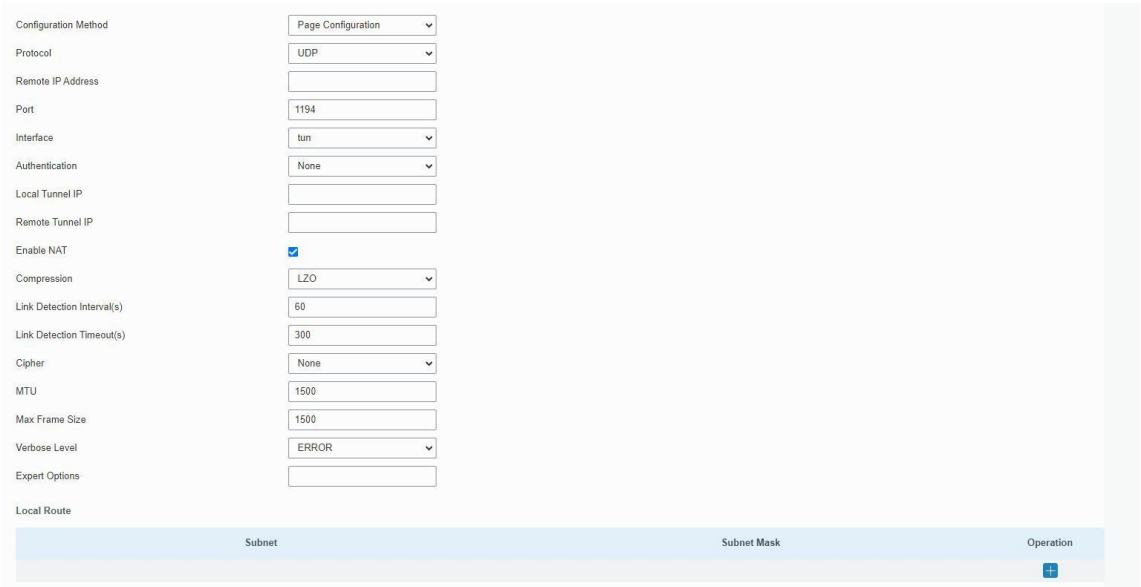


図 3-4-6-11

OpenVPN Client - Page Configuration	
項目	説明
Protocol	UDP および TCP 接続で使用されるトランスポートプロトコルを選択します。
Remote IP Address	リモート OpenVPN サーバーの IP アドレスまたはドメイン名を入力してください。

Port	リモート OpenVPN サーバーの TCP/UDP ポート番号を入力してください。範囲：1～65535。
Interface	TUN および TAP から仮想 VPN ネットワークインターフェースの種類を選択してください。TUN デバイスは IPv4 または IPv6 (OSI レイヤー 3) をカプセル化し、TAP デバイスはイーサネット 802.3 (OSI レイヤー 2) をカプセル化します。
Authentication Type	データセッション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」>「Certifications」**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ているユーザー名とパスワードを使用して、認証を完了してください。 **X.509 cert**：X.509形式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、およびクライアント秘密鍵をそれぞれのフィールドにインポートしてください。 **X.509 cert + user**：ユーザー名とパスワード、および X.509 証明書の両方の認証タイプを使用します。
Local Virtual IP	認証タイプが「**None**」または「**Pre-shared**」の場合、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、リモートトンネルアドレスを設定します。
Global Traffic Forwarding	この機能を有効にすると、すべてのデータトラフィックがOpenVPNトンネル経由で送信されます。
Enable TLS Authentication	認証タイプが「X.509 cert」の場合、TLS 認証を無効または有効にします。有効にした後、**「Network」>「VPN」>「Certifications」**ページに移動し、**TA** フィールドに ta.key をインポートしてください。 注：このオプションは tls-auth のみに対応しています。tls-crypt を使用する場合は、expert オプションに次の形式の文字列を追加してください：tls-crypt /etc/openvpn/openvpn-client1-ta.key
Compression	データの圧縮にLZOを使用するかどうかを選択します。
Link Detection Interval (s)	トンネル接続を確保するために、リンク検出間隔を設定してください。サーバーとクライアントの両方でこの設定が行われている場合、サーバーから送信された値がクライアントのローカル設定値よりも優先されます。範囲：10～1800秒。
Link Detection Timeout (s)	タイムアウト後、OpenVPN接続が再確立されます。サーバーとクライアントの両方で設定されている場合、サーバーから送信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てください。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し、セミコロンで区切ることができます。 **例**：ncp-ciphers AES-128-GCM; key direction 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

UG56は、ルーティング構成またはブリッジ構成における安全なポイントツーポイント接続やサイト間接続、およびリモートアクセス機能に対応し、OpenVPNサーバーをサポートしています。このサーバーを設定するには、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ください。

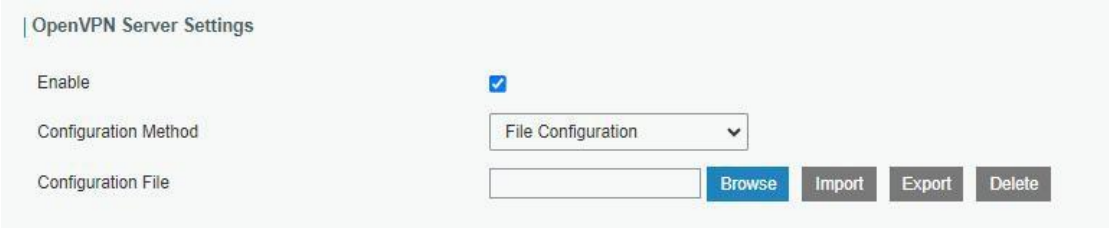


図 3-4-6-12

OpenVPN Server - File Configuration	
項目	説明
Browse	クリックすると、設定や証明書の内容を含むサーバー設定のovpn形式ファイルを参照できます。以下のサンプルを参照して、サーバー設定ファイルをご確認ください：
Edit	インポートされたファイルを編集するには、ここをクリックしてください。
Export	サーバー設定ファイルをエクスポートします。
Delete	クリックして設定ファイルを削除します。

表 3-4-6-11 OpenVPN サーバーのパラメータ

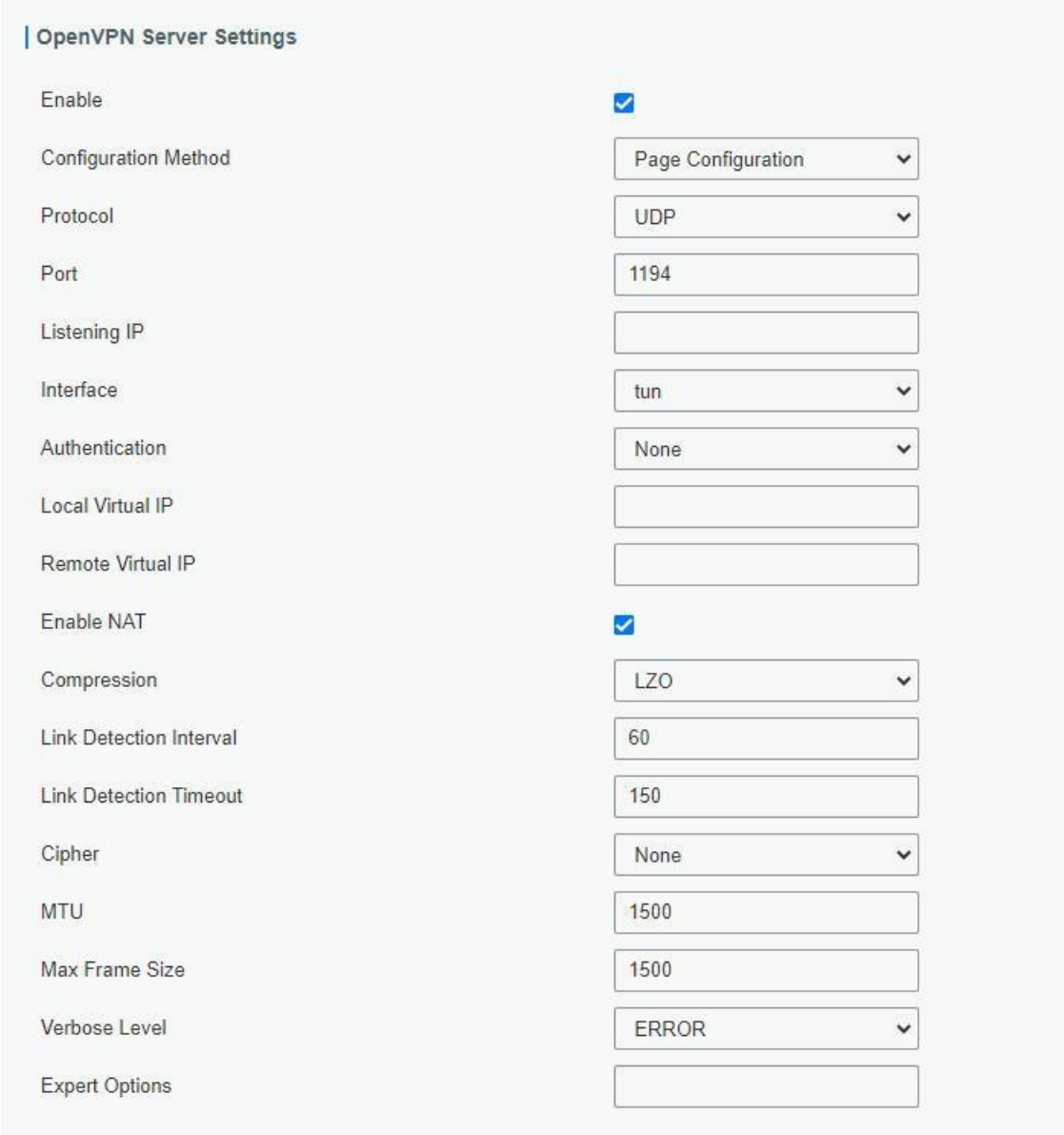


図 3-4-6-13

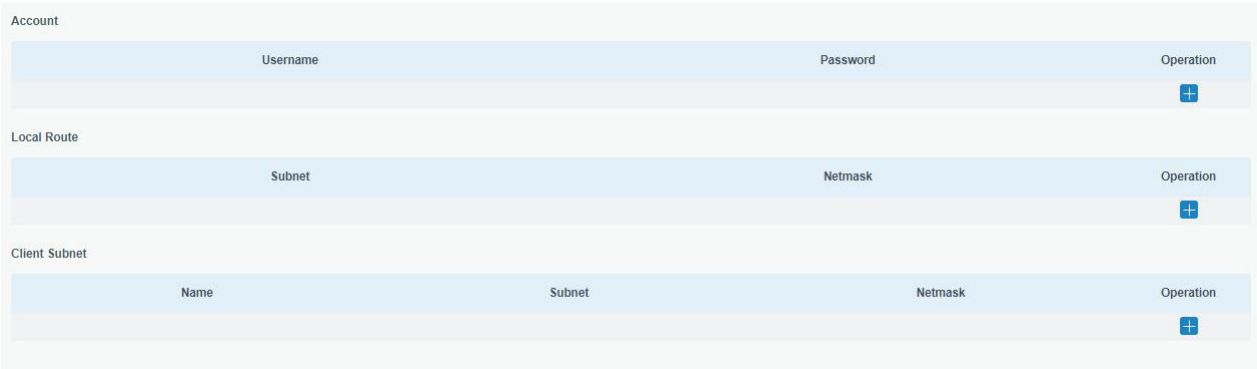


図 3-4-6-14

OpenVPN Server - Page Configuration	
項目	説明
Protocol	UDP および TCP から、接続に使用するトランスポートプロトコルを選択します。
Listening IP	バインド先の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。空欄のままにすると、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	TUN および TAP から仮想 VPN ネットワークインターフェースの種類を選択してください。TUN デバイスは IPv4 または IPv6 (OSI レイヤー 3) をカプセル化し、TAP デバイスはイーサネット 802.3 (OSI レイヤー 2) をカプセル化します。
Authentication Type	データセッション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**：認証を完了するために、サーバーと同じ秘密鍵を使用します。選択後、「**Network**」>「**VPN**」>「**Certifications**」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ているユーザー名とパスワードを使用して、認証を完了してください。 **X.509 cert**：X.509形式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、およびクライアント秘密鍵をそれぞれの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 証明書の両方の認証タイプを使用します。
Local Virtual IP	認証タイプが「**None**」または「**Pre-shared**」の場合、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、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	IPアドレスの範囲を制限するために、クライアントサブネットのネットマスクを設定します。
Renegotiation Interval	この間隔ごとにデータチャネルキーを再ネゴシエーションします。0は無効を意味します。
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に制限します。範囲：1～20。 **注**：多数のクライアントを接続する必要がある場合は、ログの重大度を「Info」に設定してください。
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通信できるようになります。
Enable Dup Client	同じ共通名または証明書を使用して、複数のクライアントが接続できるようにします。
Enable TLS Authentication	認証タイプが X.509 証明書の場合、TLS 認証を無効または有効にします。有効にした後、「**Network**」>「**VPN**」>「**Certifications**」ページに移動し、**TA** フィールドに ta.key をインポートしてください。 注：このオプションは tls-auth のみに対応しています。tls-crypt を使用する場合は、expert オプションに次の形式の文字列を追加してください：tls-crypt /etc/openvpn/openvpn-client1-ta.key
Compression	データの圧縮に LZO を使用するかどうかを選択します。
Link Detection Interval (s)	トンネル接続を確保するために、リンク検出間隔を設定します。サーバーとクライアントの両方で設定されている場合、サーバーから送信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：10～1800秒。
Link Detection Timeout (s)	タイムアウト後、OpenVPNは再接続されます。サーバーとクライアントの両方でこの設定がされている場合、サーバーから送信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、および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てください。範囲：64～1500。
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し、セミコロンで区切ることができます。 **例：**ncp-ciphers AES-128-GCM; key direction 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	OpenVPN クライアント証明書の共通名として名前を設定します。
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マスクを設定します。

表 3-3-6-12 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、ユーザーは認証の種類に応じて、必要な証明書および鍵ファイルをこのページにインポートまたはエクスポートすることができます。

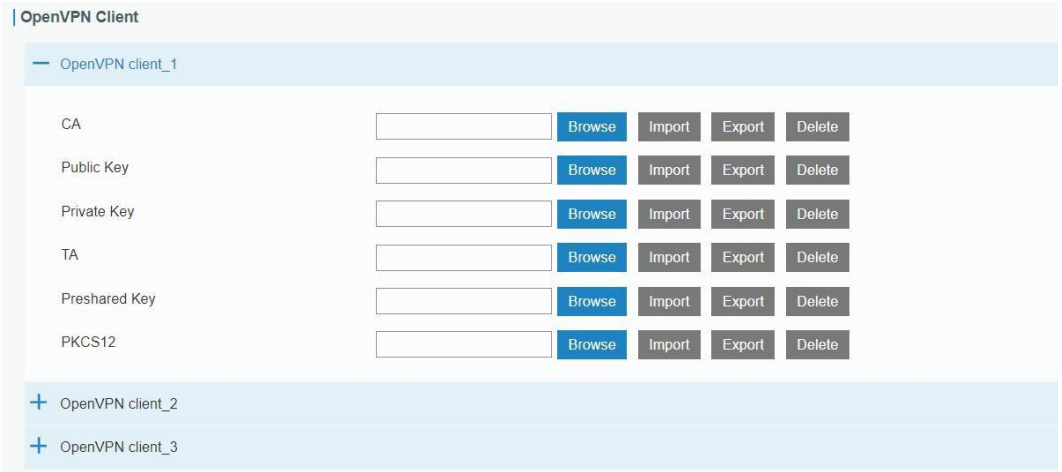


図 3-4-6-15

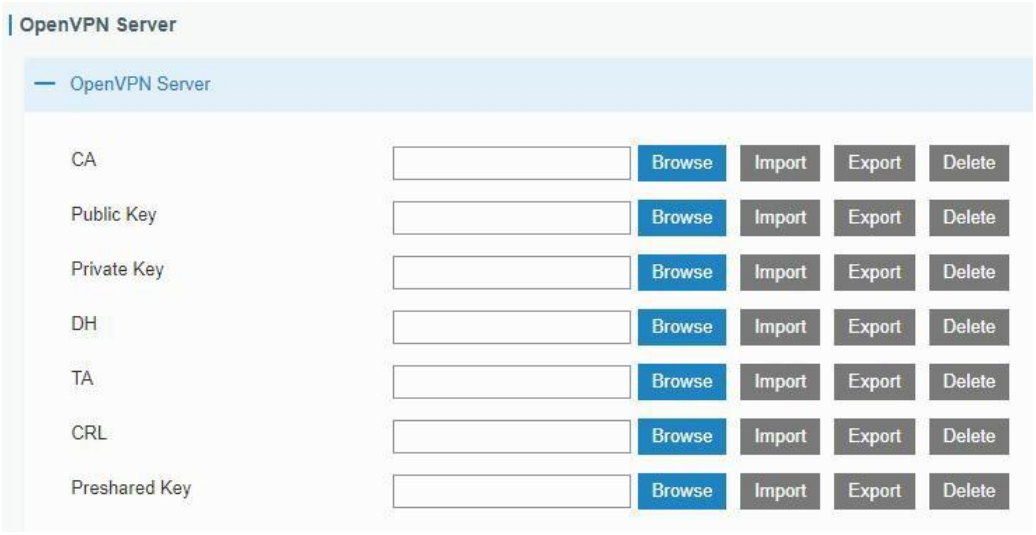


図 3-4-6-16

図 3-4-6-17

3.4.6.9 WireGuard

WireGuard は、最先端の暗号技術を採用した、非常にシンプルでありながら高速で最新の VPN です。WireGuard は、UDP プロトコルを介してトラフィックを送信します。

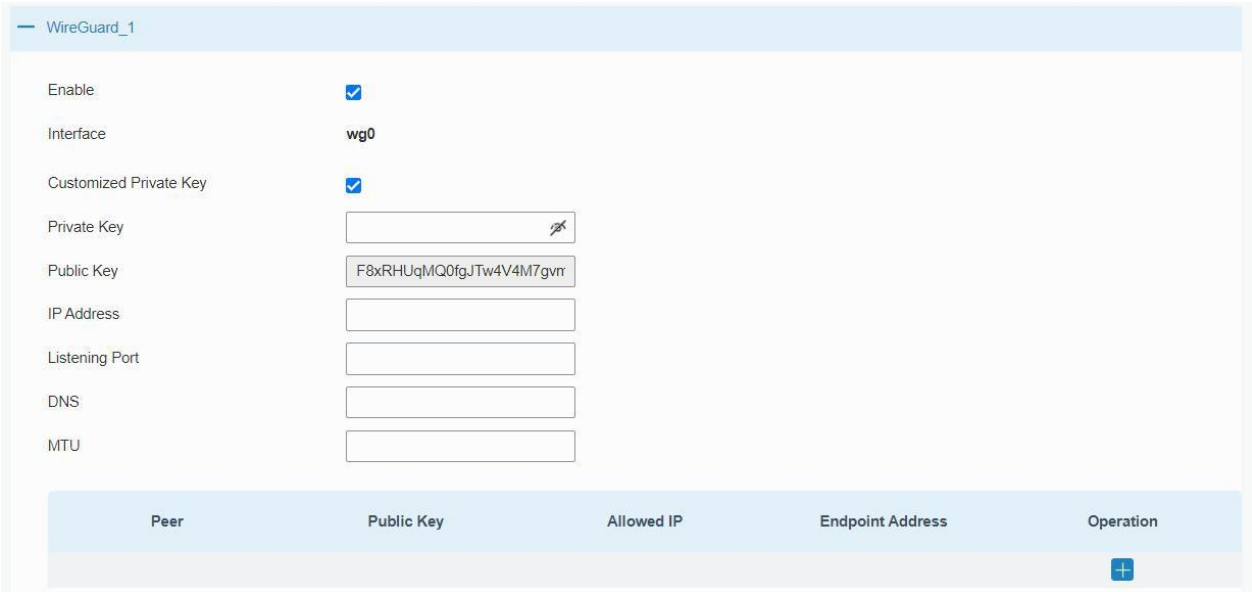


図 3-4-6-18

WireGuard	
項目	説明
Enable	有効化WireGuard インターフェースを有効にします。WireGuard インターフェースは最大 3 つまで許可されます。
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には、有効または無効に設定してください。無効にした場合、クライアントはこのルーターによって生成され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	ローカルの仮想IPアドレスとネットマスクを設定してください。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インターフェースのポート番号は、それぞれ異なるものにしてください。
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、ルーターは一般的なネットワークインターフェース（WAN、モバイル回線など）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、ルーターは一般的なネットワークインターフェース（WAN、モバイル回線など）のMTUを使用します。
Peer Table	「+」をクリックして、このWireGuardインターフェースのWireGuardピアを追加します。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

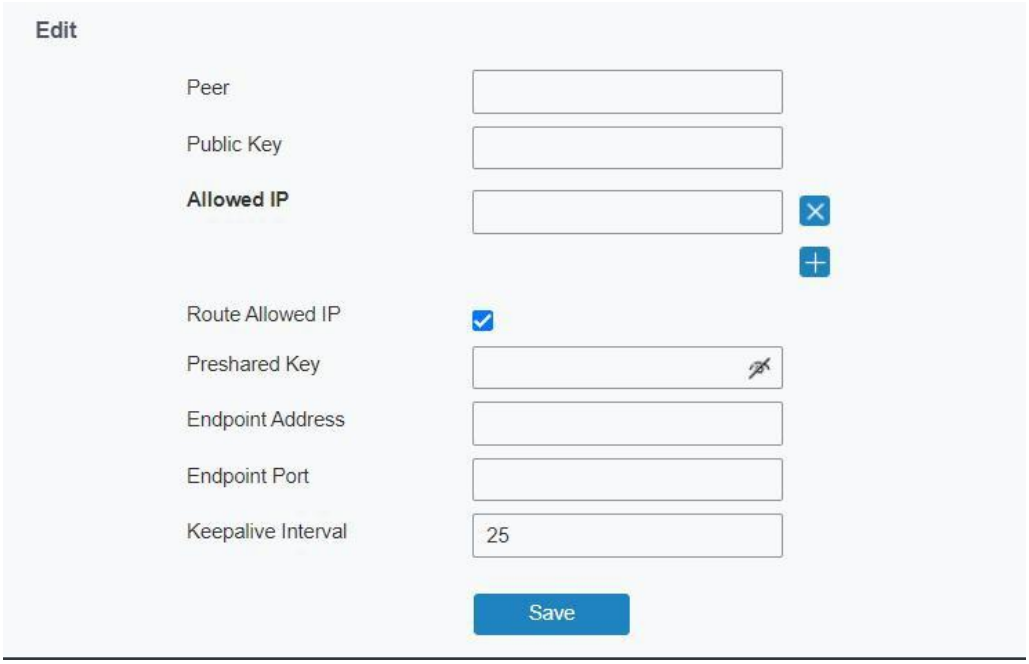


図 3-4-6-19

WireGuard-Peer	
項目	説明
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のピアサーバー／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、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かどうかを有効または無効にします。
Preshared Key	事前共有キーを設定します。このインターフェースとピアのインターフェースの両方で、同じキー値を設定する必要があります。
Endpoint Address	WireGuardピアサーバー/クライアントのIPアドレスまたはドメイン名を設定します。
Endpoint Port	WireGuardのピアサーバーまたはクライアントの宛先ポートを設定してください。
Keepalive Interval	接続が確立された後、この WireGuard インターフェースは、接続を維持するために定期的にハートビートパケットを送信します。0 は無効を意味します。

表 3-4-6-13 WireGuard-Peer パラメータ

3.4.7 HTTP Proxy

ゲートウェイは、セキュリティ上の理由から実際の IP アドレスを隠しながら、ターゲットのインターネットサイトと通信するために HTTP プロキシサーバーに接続することができます。

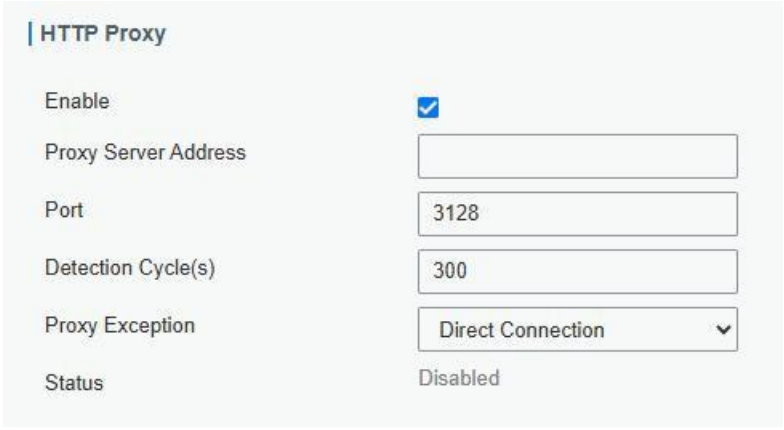


図 3-4-7-1

HTTP Proxy	
項目	説明
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アドレスまたはドメイン名）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ます： **Direct Connection**：プロキシを経由せずにターゲットへ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回復するまで、トラフィックを遮断します。
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、一般的なユーザー管理、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、およびHTTPS証明書が含まれます。

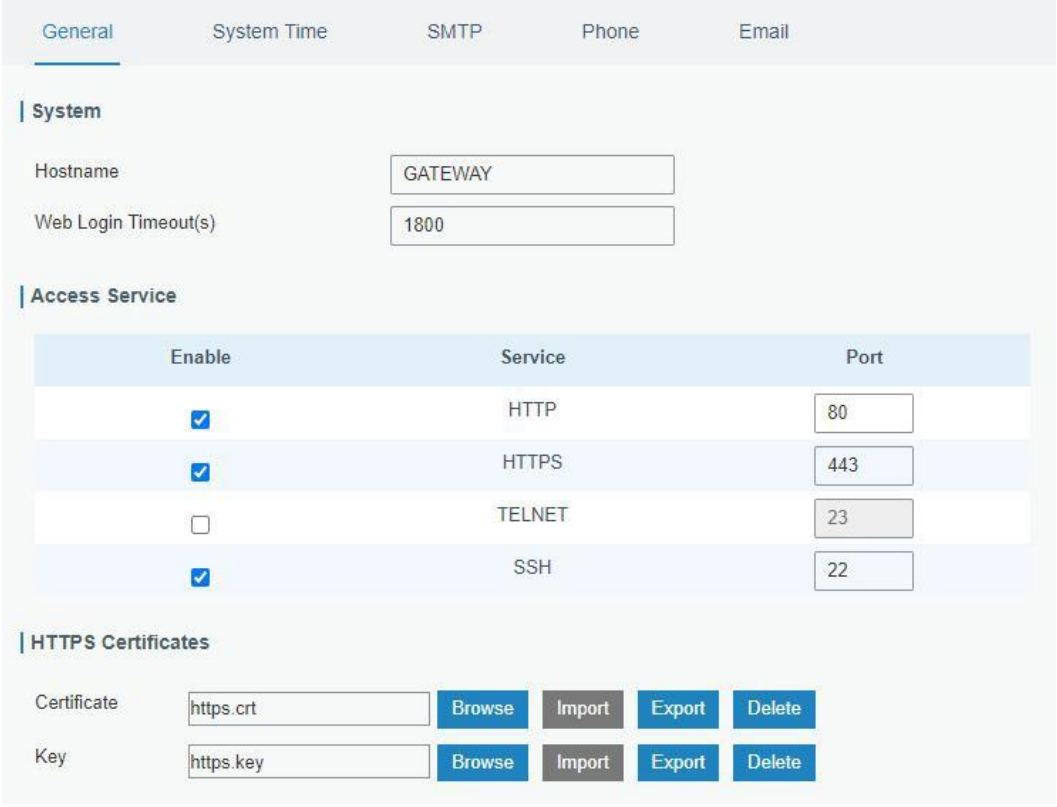


図 3-5-1-1

General		
項目	説明	デフォルト
System		
Hostname	ユーザー定義のゲートウェイ名。先頭は英字でなければなりません。	GATEWAY
Web Login Timeout (s)	タイムアウトした場合は、再度ログインする必要があります。範囲：100～3600。	1800
アクセスサービス		
Port	サービスのポート番号を設定します。範囲：1～65535。	--
HTTP	このオプションにチェックを入れると、ユーザーはHTTP経由でデバイスにローカルログインし、Webを通じてデバイスにアクセスして制御できるようになります。	80
HTTPS	このオプションにチェックを入れると、ユーザーはHTTPS経由でデバイスにローカルおよびリモートからログインし、Webを通じてデバイスにアクセスして制御できるようになります。	443
TELNET	TELNETこのオプションにチェックを入れると、ユーザーはTELNET経由でデバイスにローカルおよびリモートからログインし、Webを通じてデバイスにアクセスして制御できるようになります。	23

SSH	このオプションにチェックを入れると、ユーザーはSSH経由でデバイスにローカルおよびリモートからログインできます。	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てから、「Import」ボタンをクリックして、そのファイルをゲートウェイにアップロードしてください。「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てから、「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。	--

表 3-5-1-1 一般設定パラメータ

3.5.1.2 システム時刻

このセクションでは、タイムゾーンや時刻同期方式を含むシステム時刻の設定方法について説明します。

注：ゲートウェイが正しい時刻で動作するようにするため、ゲートウェイの設定時にシステム時刻を設定することをお勧めします。

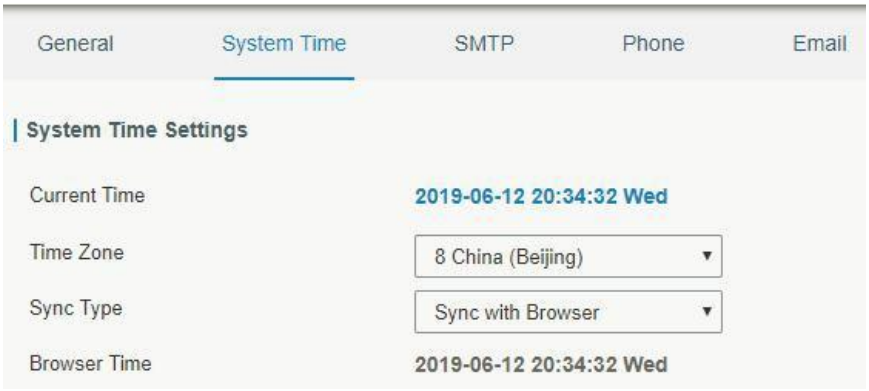


図 3-5-1-2

System Time	
項目	**説明**
Current Time	現在のシステム時刻を表示します。
Time Zone	ドロップダウンリストをクリックして、現在お住まい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、時刻の同期タイプを選択してください。 **Sync with Browser**：時間をブラウザと同期します。 **Sync with NTP Server**：NTP サーバーと時刻を同期します。 **Set up Manually**：時刻を手動で設定します。
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	「Enable NTP Server」オプションにチェックを入れると、ネットワーク上の NTP クライアントはゲートウェイと時刻を同期できるようになります。

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。

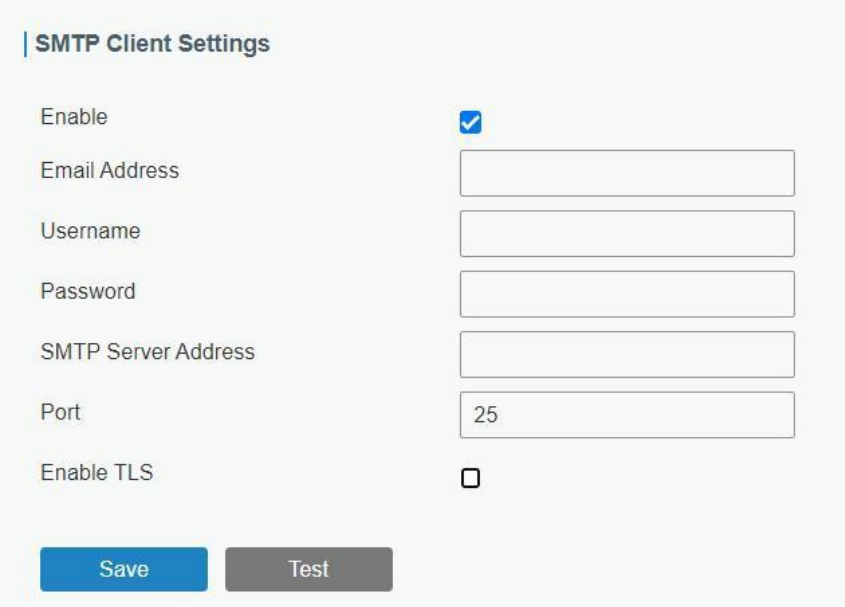


図 3-5-1-3

SMTP	
項目	説明
SMTP クライアント設定	
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	送信者のメールアカウント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

関連トピック

イベント設定

3.5.1.4 Phone

電話の設定には、イベントに対する通話/SMS トリガーおよび SMS アラームが含まれます。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。

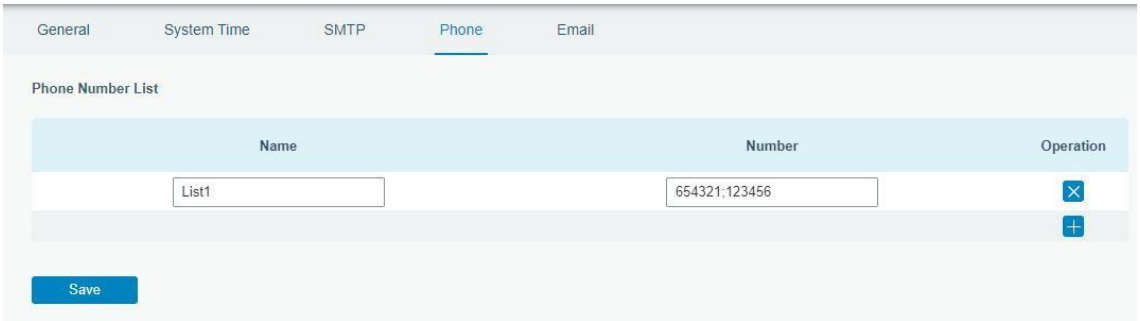


図 3-5-1-4

Phone	
項目	説明
Phone Number List	
Name	電話グループ名を設定します。
Number	電話番号を入力してください。数字、"+"、および "-" を使用できます。 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

関連トピック

オンデマンド接続

3.5.1.5 Email

E メール設定には、イベントの E メールアラームが含まれます。

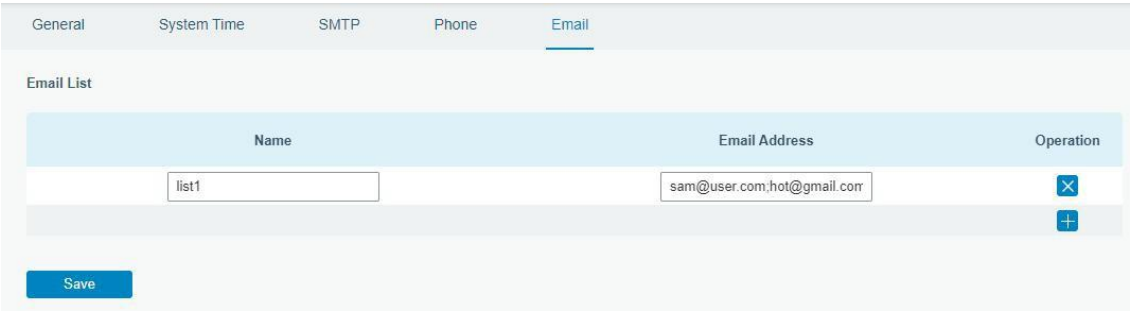


図 3-5-1-5

Email	
項目	説明
Email List	
Name	メールグループ名を設定します。
Email Address	メールアドレスを入力してください。複数のメールアドレスは「;」で区切ってください。

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。

注：セキュリティ上の理由から、これらを変更することを強くお勧めします。

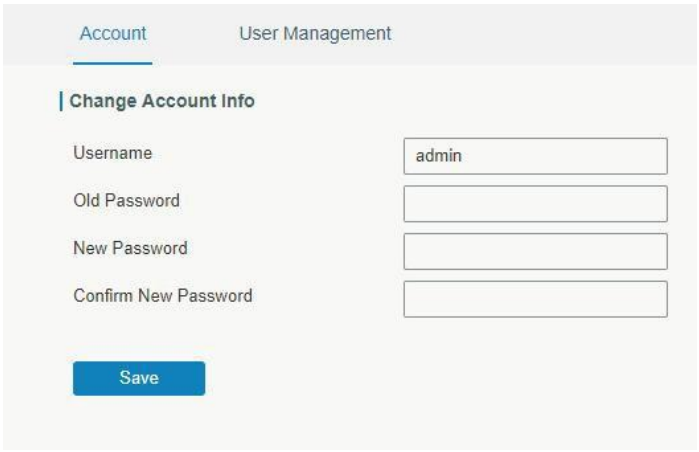


図 3-5-2-1

Account	
項目	説明
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。最初の文字は数字にすることはできません。
Old Password	現在のパスワードを入力してください。
New Password	スペース以外のASCII文字を含む新しいパスワードを入力してください。パスワードには、少なくとも1文字のアルファベットと1桁の数字を含める必要があり、文字数は5～31文字でなければなりません。
Confirm New Password	新しいパスワードをもう一度入力してください。

表 3-5-2-1 アカウント情報

3.5.1.1 User Management

3.5.1.2

このセクションでは、一般ユーザーアカウントの作成方法について説明します。一般ユーザーの権限には、「読み取り専用」と「読み書き」があります。

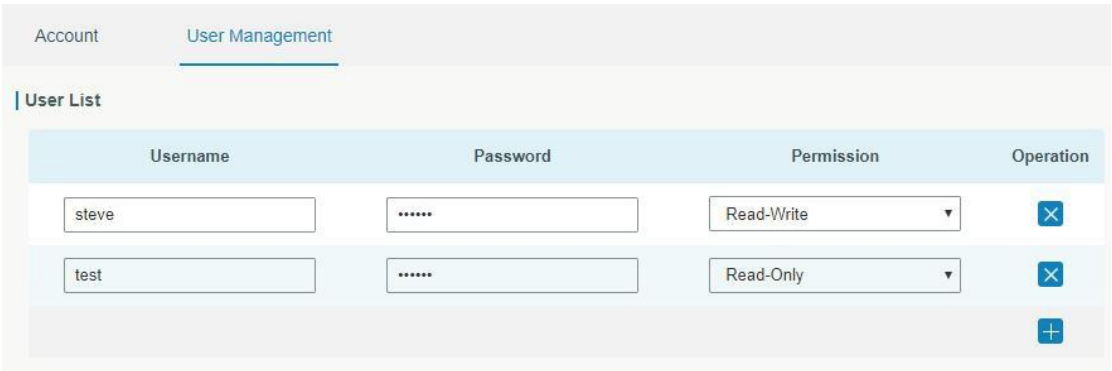


図 3-5-2-2

User Management	
項目	説明
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。

	最初の文字は数字にすることはできません。
Password	パスワードには、スペース以外の ASCII 文字を使用してください。パスワードには、少なくとも 1 文字のアルファベットと 1 桁の数字を含め、5～31 文字で設定してください。
Permission	ユーザー権限を「Read-Only」または「Read-Write」から選択してください。 - Read-Only：このレベルでは、ユーザーはゲートウェイの設定を表示することしかできません。 - Read-Write：この権限レベルでは、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

3.5.1.3 HTTP API 管理

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。

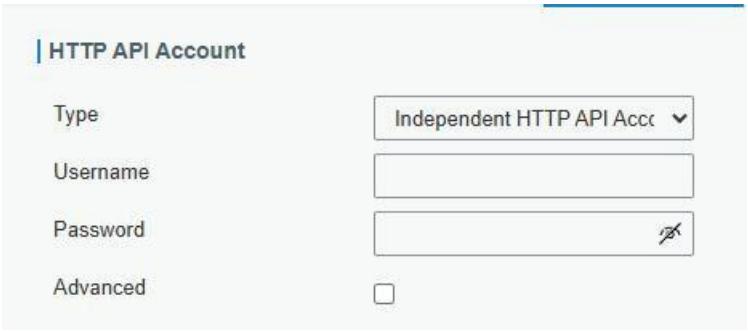


図 3-5-2-3

User Management	
項目	説明
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は異なる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。最初の文字は数字にすることはできません。
Password	パスワードには、スペースを除く任意の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

3.5.2 SNMP

SNMPは、ネットワーク監視のためのネットワーク管理において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、システムの状態や構成を記述する管理情報ベース（MIB）として構成されています。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、NMS、およびSNMP管理プログラムでSNMPを設定するには、Managerで設定を行う必要があります。

NMSからのクエリを実現するための設定手順は以下の通りです：

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に読み込んでください。
3. MIBビューを設定します。
4. VCAMを設定します。

3.5.2.1 SNMP

UG56は、SNMPv1、SNMPv2c、およびSNMPv3の各バージョンを対応しています。SNMPv1およびSNMPv2cでは、コミュニティ名による認証が使用されます。SNMPv3では、ユーザー名とパスワードによる認証と暗号化が使用されます。

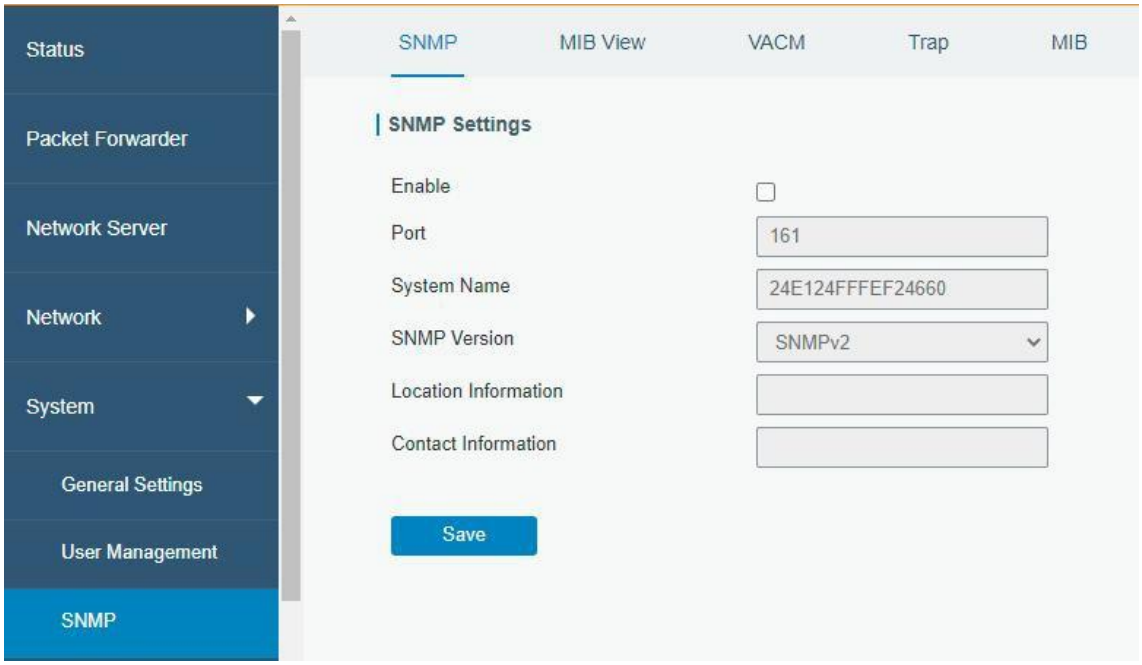


図 3-5-3-1

SNMP Settings	
項目	説明
Enable	有効にするか無効にするかを選択します。
Port	設定SNMPの受信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入力してください。
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

3.5.2.2 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。

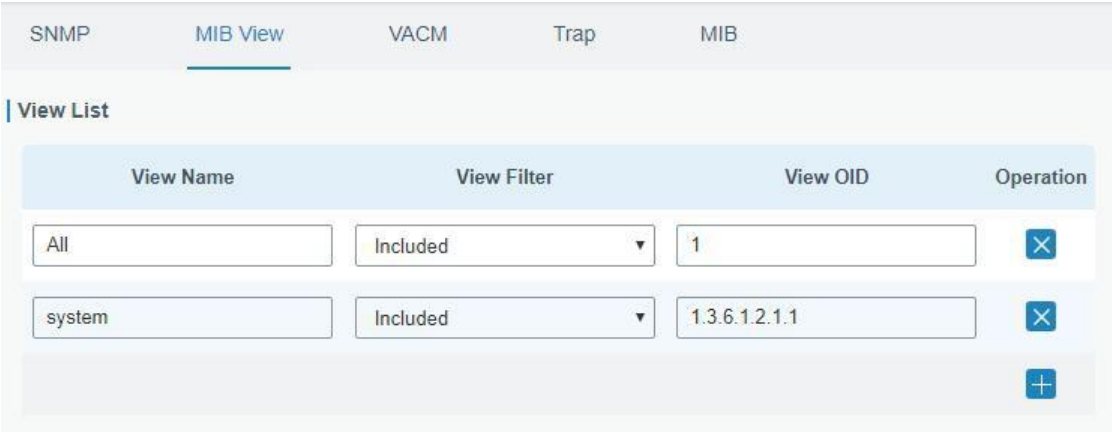


図 3-5-3-2

MIB View	
項目	説明
View Name	MIB ビューの名前を設定します。
View Filter	「Included」または「Excluded」から選択します。
View OID	OID 番号を入力してください。
Included	指定したMIBノード内のすべてのノードを照会できます。
Excluded	指定した MIB ノードを除くすべてのノードを照会できます。

表 3-5-3-2 MIB ビューのパラメータ

3.5.2.3 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。

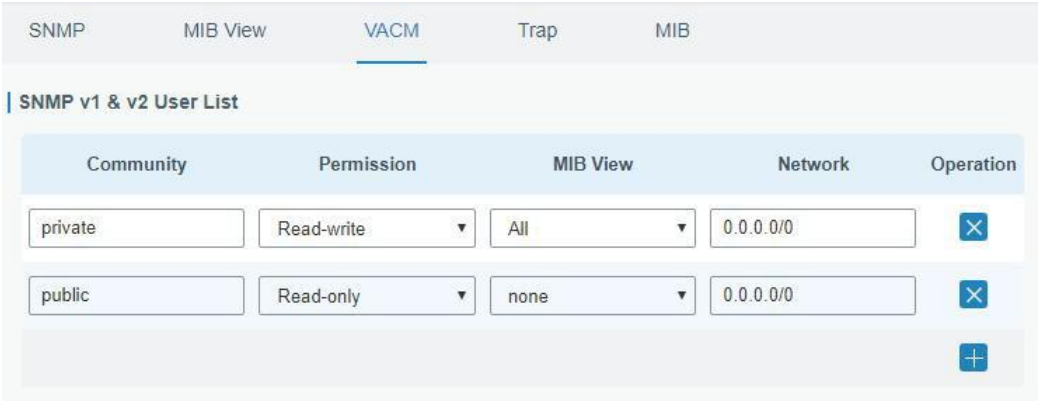


図 3-5-3-3

VACM	
項目	説明
SNMP v1 & v2 User List	
Community	コミュニティ名を設定します。
Permission	「Read-Only」または「Read-Write」から選択します。
MIB View	MIB ビュー一覧から、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アドレスとビットです。
Read-Write	指定された MIB ノードの権限は、読み取りおよび書き込みです。

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	「NoAuth/NoPriv」、「Auth/NoPriv」、および「Auth/Priv」から選択してください。
Read-Only View	MIB ビュー一覧から、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 ビュー一覧から、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 ビュー一覧から、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

3.5.2.4 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。

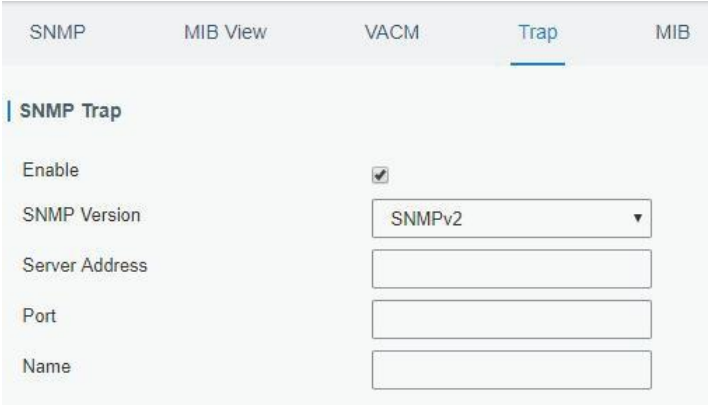


図 3-5-3-4

SNMP Trap	
項目	説明
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に対応しています。
Server Address	NMSのIPアドレスまたはドメイン名を入力してください。
Port	UDPポートを入力してください。ポートの範囲は1～65535です。デフォルトのポートは162です。
Name	SNMP v1/v2c を使用する場合はグループ名を入力し、SNMP v3 を使用する場合はユーザー名を入力してください。
Auth/Priv Mode	「NoAuth & No Priv」、「Auth & NoPriv」、および「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

3.5.2.5 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。

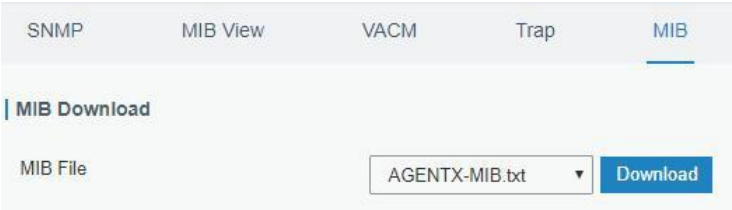


図 3-5-3-5

MIB	
項目	説明
MIB File	必要な MIB ファイルを選択してください。
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

3.5.3 Device Management

3.5.3.1 Auto Provision

ユーザーは、Milesight Development Platform から設定プロファイルをカスタマイズして割り当てることができます。自動プロビジョニングが有効になっており、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て初期設定を行います。この機能は、デバイスが Milesight Development Platform に接続するように設定されていなくても動作します。

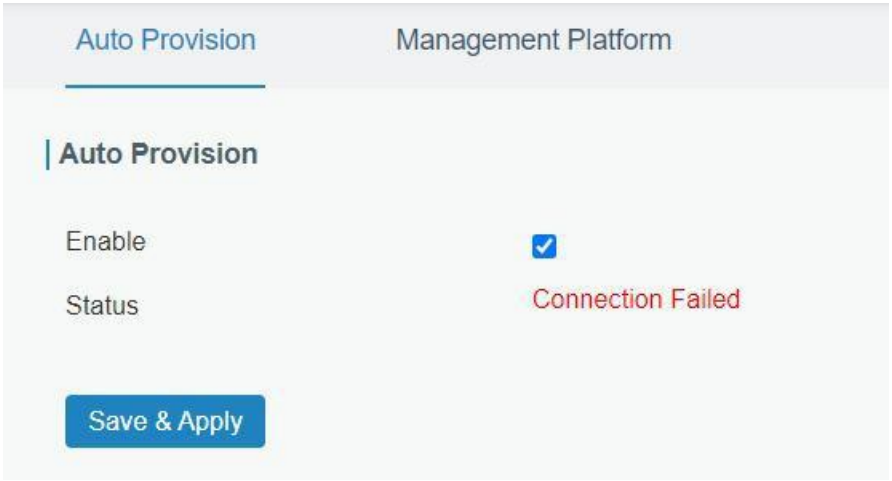


図 3-5-4-1

3.5.3.2 Management Platform

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

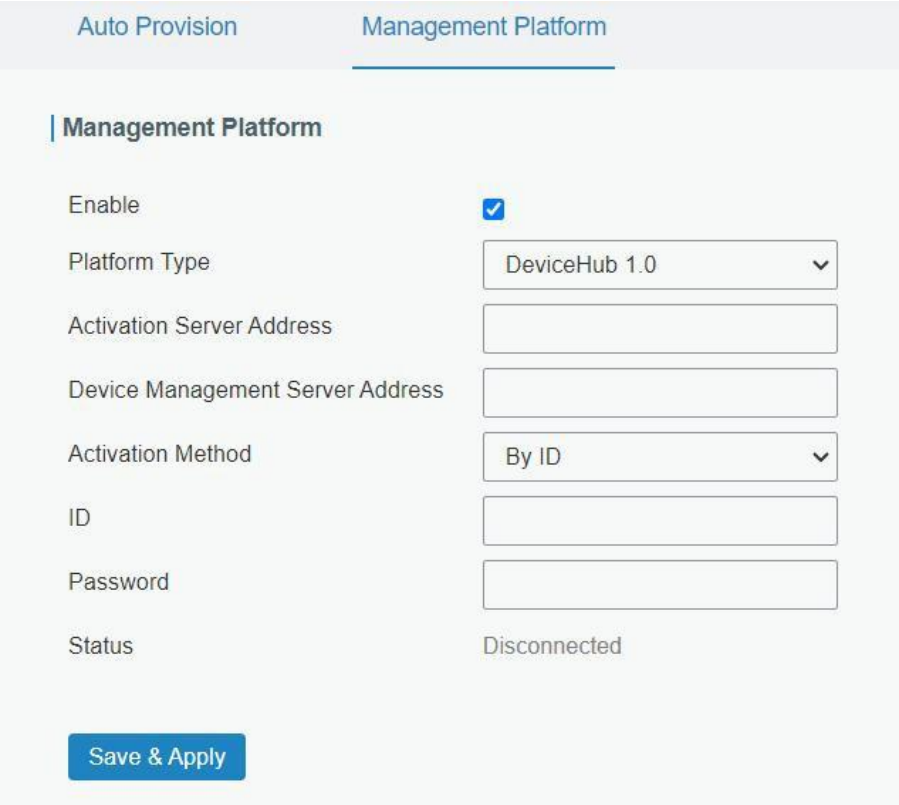


図 3-5-4-2

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

表 3-5-4-1

3.5.4 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できます。

3.5.4.1 Events

このページでは、アラームメッセージを表示できます。

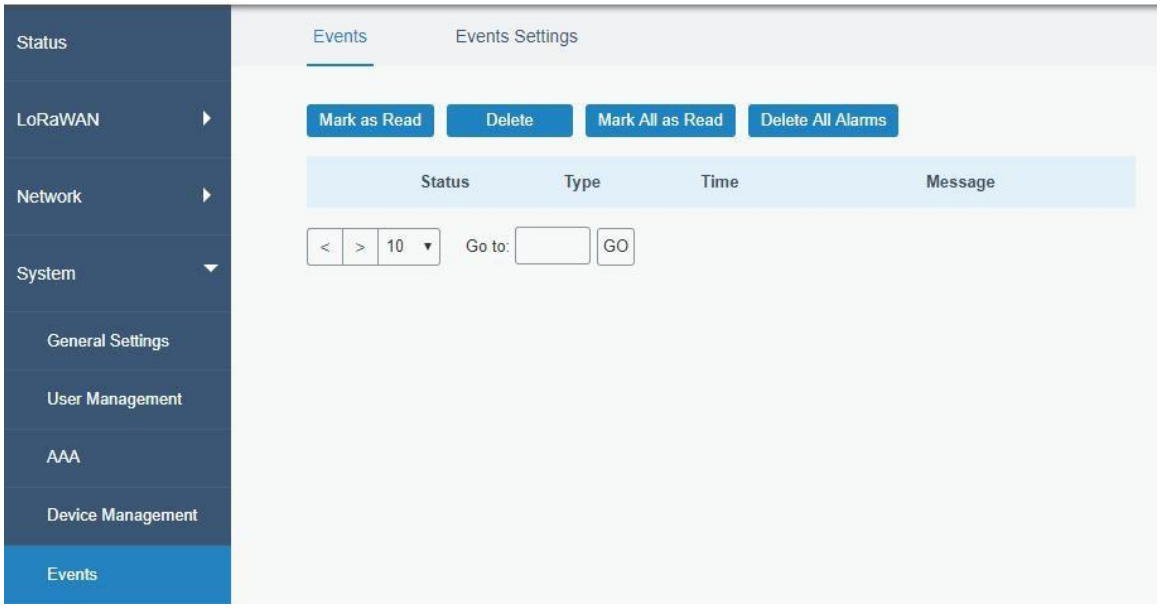


図 3-5-5-1

Events	
項目	説明
Mark as Read	選択したイベントアラームを既読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にします。
Delete All Alarms	すべてのイベントアラームを削除します。
Status	イベントアラームの既読ステータス（「既読」や「未読」など）を表示します。
Type	アラームの対象となるイベントの種類を表示します。
Time	アラームの時刻を表示します。
Message	アラームの内容を表示します。

表 3-5-5-1 イベントパラメータ

3.5.4.2 Events Settings

このセクションでは、記録するイベントを決定し、変更が発生した際に E メールや SMS による通知を受け取るかどうかを設定できます。

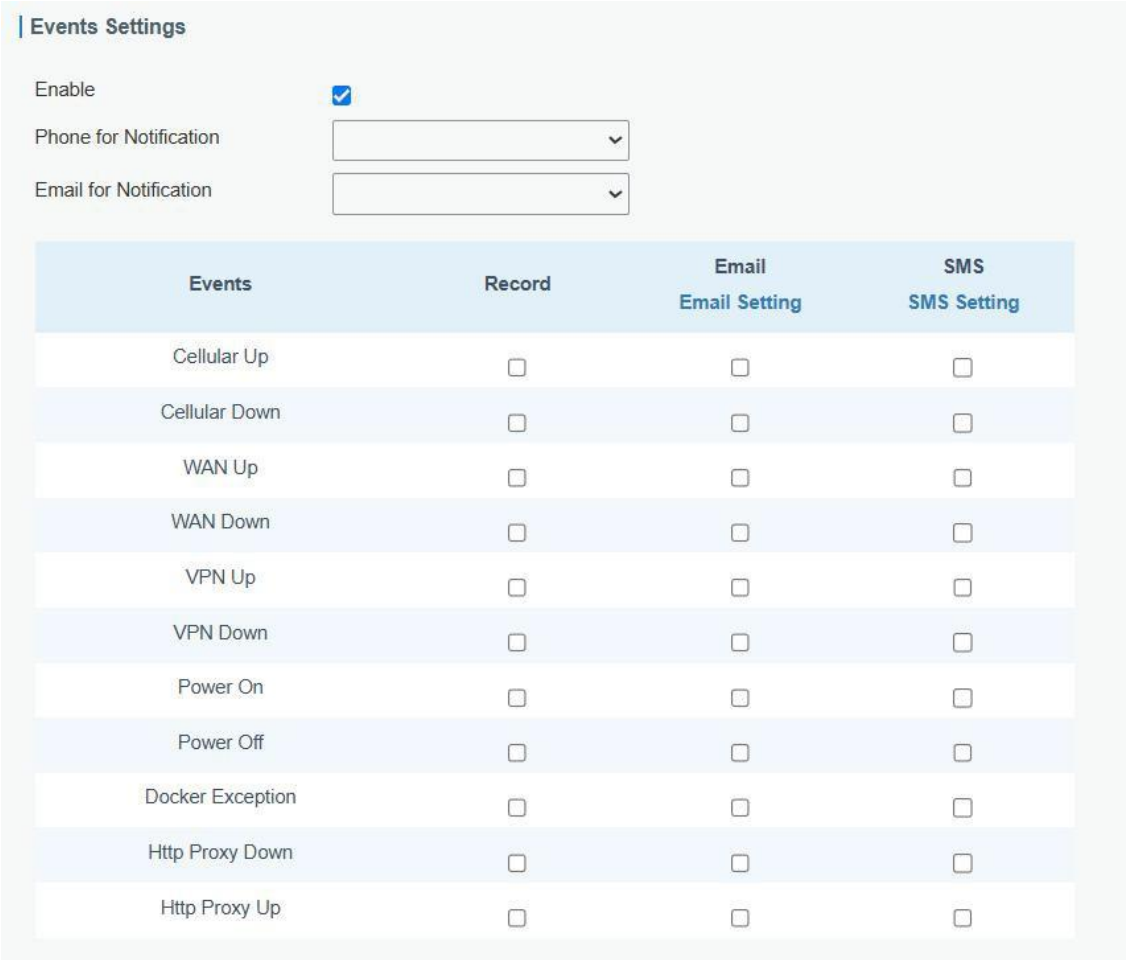


図 3-5-5-2

Event Settings	
項目	説明
Enable	「Events Settings」を有効にするには、ここに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	Eメールアラームを受信するEメールグループを選択してください。
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」ページに遷移し、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」ページに遷移し、電話グループリストを設定できます。
Phone Group List	SMSアラームを受信する電話グループを選択してください。

Email Group List	Eメールアラームを受信するEメールグループを選択してください。

表 3-5-5-2 イベントパラメータ

関連トピックE

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を行うために設計されています。

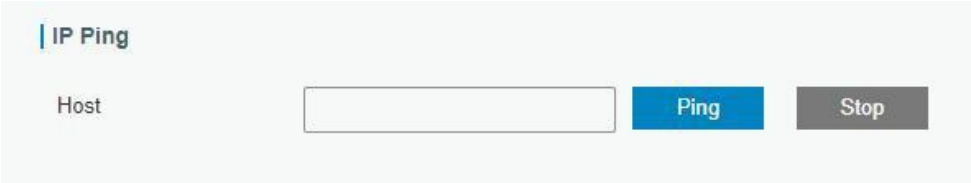


図 3-6-1-1

PING	
項目	説明
Host	ゲートウェイから外部ネットワークへのPing。

表 3-6-1-1 IP Ping パラメータ

3.6.1.2 Traceroute

Traceroute ツールは、ネットワークの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	
項目	説明
Host	検出対象の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。

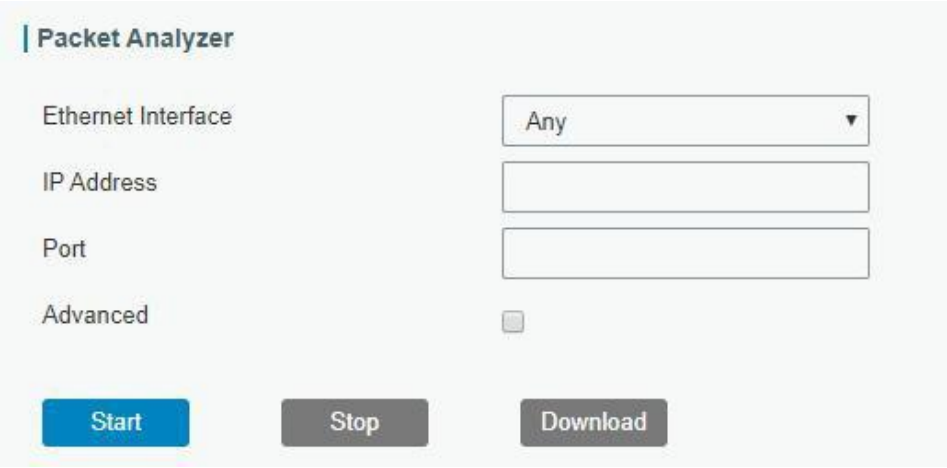


図 3-6-1-3

Packet Analyzer	
項目	説明
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ます。
IP Address	ルーターがキャプチャするIPアドレスを設定します。
Port	ルーターがパケットをキャプチャするポートを設定してください。
Advanced	スニファーのルールを設定します。形式は 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 ツールを使用して診断ログを収集できます。

図 3-6-1-4

3.6.2 Schedule

このセクションでは、ゲートウェイでの再起動のスケジュール設定方法について説明します。

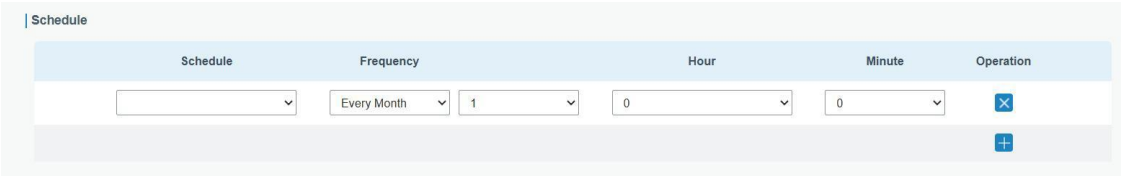


図 3-6-2-1

Schedule	
項目	説明
Schedule	スケジュールイベントの選択： 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、システムの処理状況を示す情報、エラー、および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、システムのトラブルシューティングを行う管理者やユーザーは、問題の原因を特定したり、システムの処理が正常に実行されているかどうかを確認したり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。

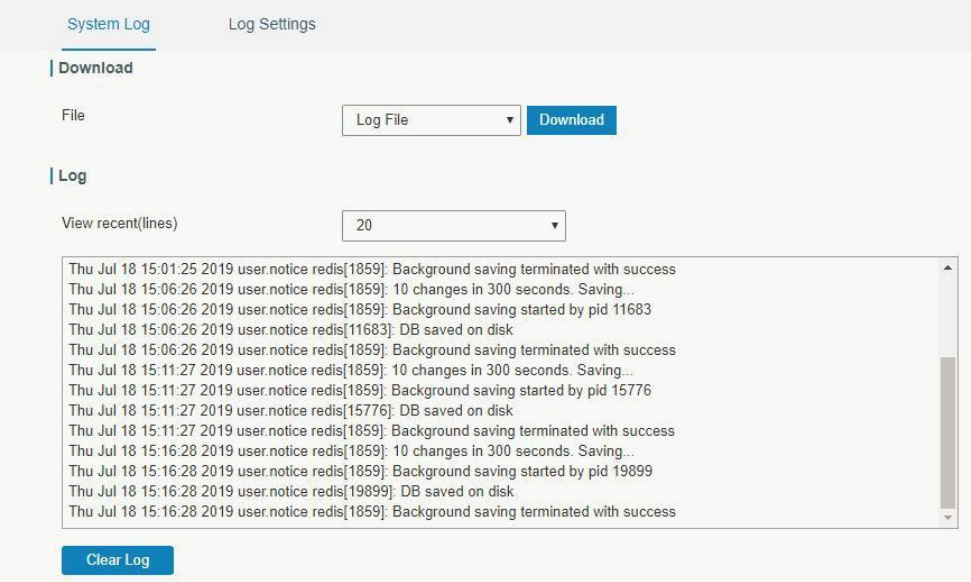


図 3-6-3-1

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

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。

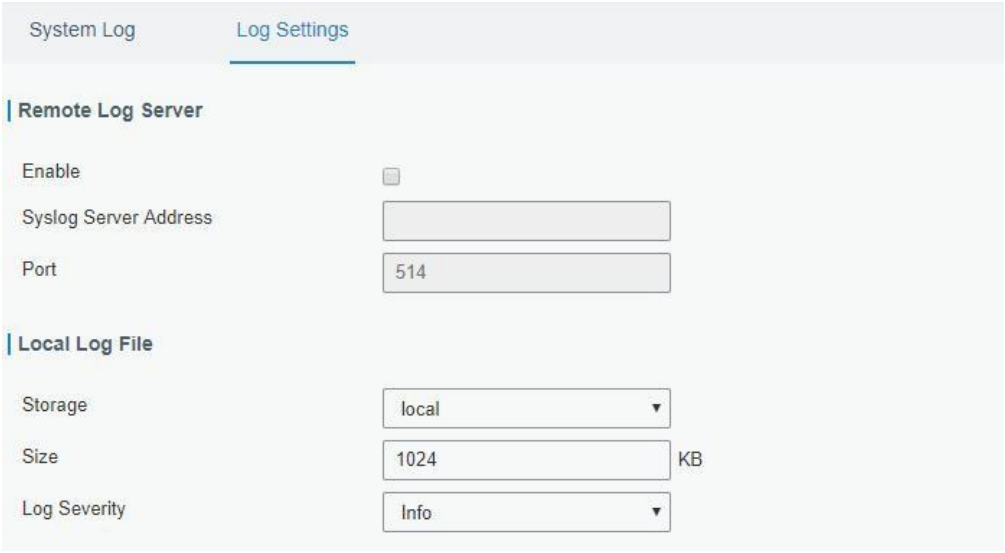


図 3-6-3-2

Log Settings	
項目	説明
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 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	ログファイルは、メモリまたはTFカードに保存できます。
Size	保存するログファイルのサイズを設定してください。
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。

注：ファームウェアのアップグレード中は、Web ページでの動作は一切行わないでください。動作を行うと、アップグレードが中断されたり、デバイスが故障したりする恐れがあります。

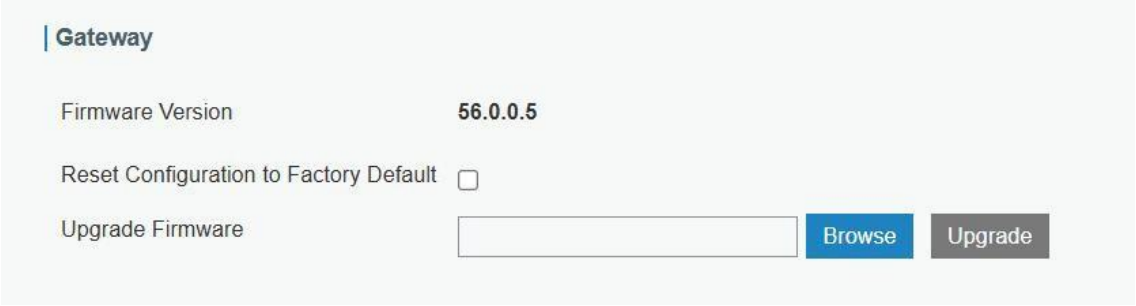


図 3-6-4-1

Upgrade	
項目	説明
Firmware Version	現在のファームウェアのバージョンを表示します。
Reset Configuration to Factory Default	このオプションにチェックを入れると、アップグレード後にゲートウェイが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」をクリックしてファームウェアをアップグレードします。

表 3-6-4-1 アップグレードパラメータ

関連する設定例

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、システム全体の設定をファイルにバックアップする方法、重要な設定の一部のみをバッチバックアップ用に複製する方法、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設定にリセットする方法について説明します。

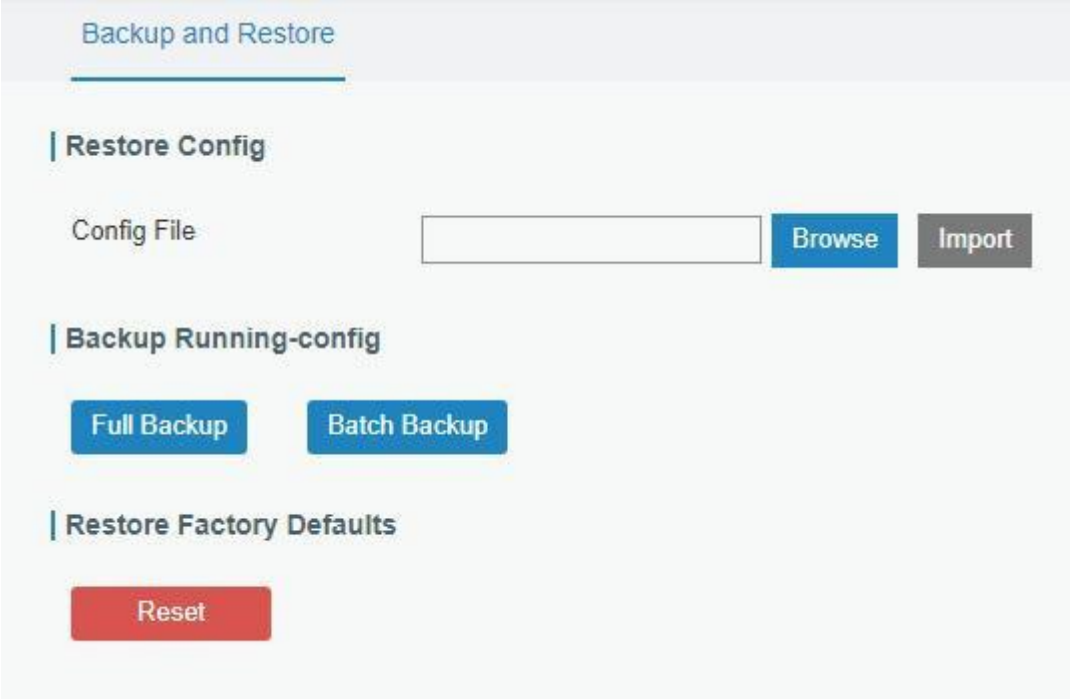


図 3-6-5-1

Backup and Restore	
項目	説明
Config File	「Browse」ボタンをクリックして設定ファイルを選択し、「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ます。
Full Backup	「Full Backup」をクリックして、現在の設定ファイルをPCにエクスポートします。

Batch Backup	「Batch Backup」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、およびすべての APP 設定を除く、現在の設定がエクスポートされます。
Reset	「Reset」ボタンをクリックして、工場出荷時の設定に戻してください。リセット処理が完了すると、ゲートウェイが再起動します。

表 3-6-5-1 バックアップおよび復元パラメータ

関連する設定例

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ないように、ゲートウェイを再起動する前に「Save」ボタンをクリックすることを強くお勧めします。

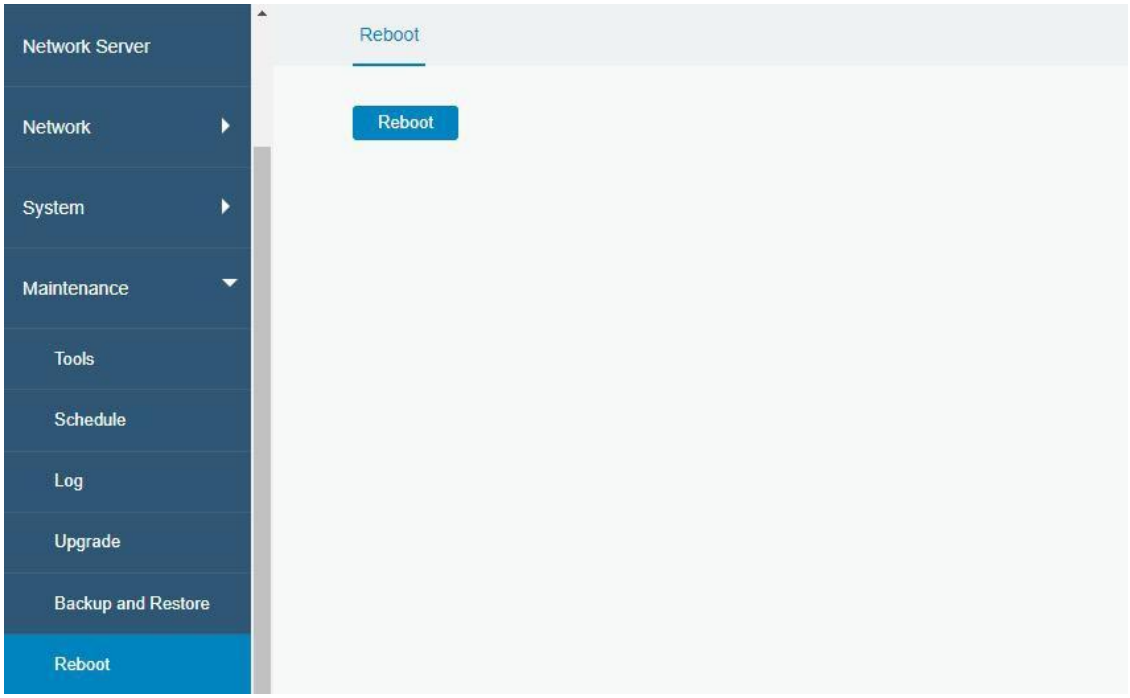


図 3-6-6-1

3.7 APP

3.7.1 Python

Python は、その明確な構文と可読性の高さから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。

インタプリタ型言語であるPythonは、コードの可読性を重視する設計思想を持っています。特に、中括弧やキーワードではなく、空白によるインデントでコードブロックを区切る点や、C++やJavaなどの他の言語に比べて少ない行数で概念を表現できる構文が特徴です。この言語は、小規模から大規模まで、明確なプログラムを作成できるようにするための構文を提供しています。
ユーザーはPythonを使用してプログラムのプロトタイプを迅速に生成し、それを最終的なプログラムインターフェースとして活用したり、より適切な言語で書き直したり、Pythonから呼び出せる拡張クラスライブラリとしてカプセル化したりすることができます。
このセクションでは、App-manager、SDKバージョン、拡張ストレージなどの関連する実行状況を確認する方法について説明します。また、ここからApp-managerの設定を変更したり、Pythonアプリパッケージをインポートしたりすることもできます。

3.7.1.1 Python

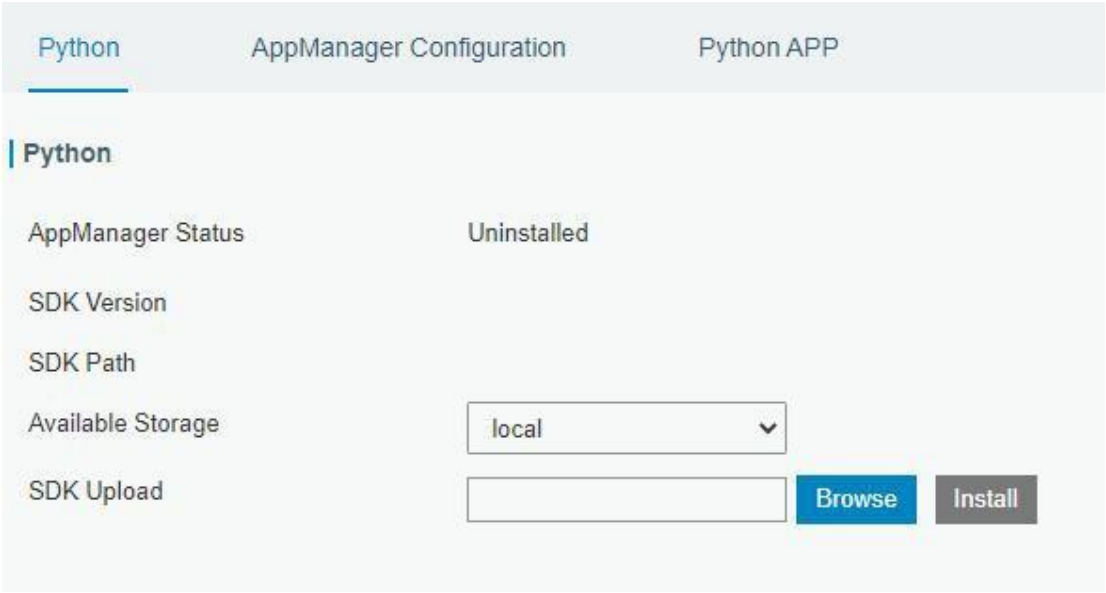


図 3-7-1-1

Python	
項目	説明
AppManager Status	AppManager の実行ステータス（「Uninstalled」、「Running」、「Stopped」など）を表示します。
SDK Version	インストールされている SDK のバージョンを表示します。
SDK Path	SDKのインストールパスを表示します。
Available Storage	SDKをインストールする空き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

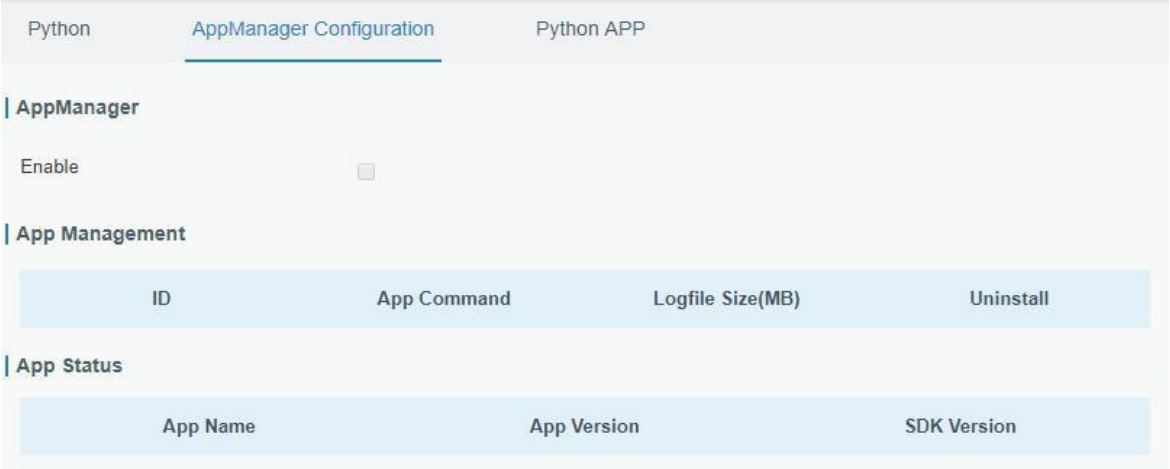


図 3-7-1-2

AppManager Configuration	
項目	説明
Enable	Python AppManager を有効にすると、ユーザーは「Python」ウェブページの「View」ボタンをクリックして、AppManager によって管理されているアプリケーションのステータスを確認できます。
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の名前を表示します。
Logfile Size(MB)	ユーザー定義のログファイルサイズ。範囲：1～50。
Uninstall	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 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

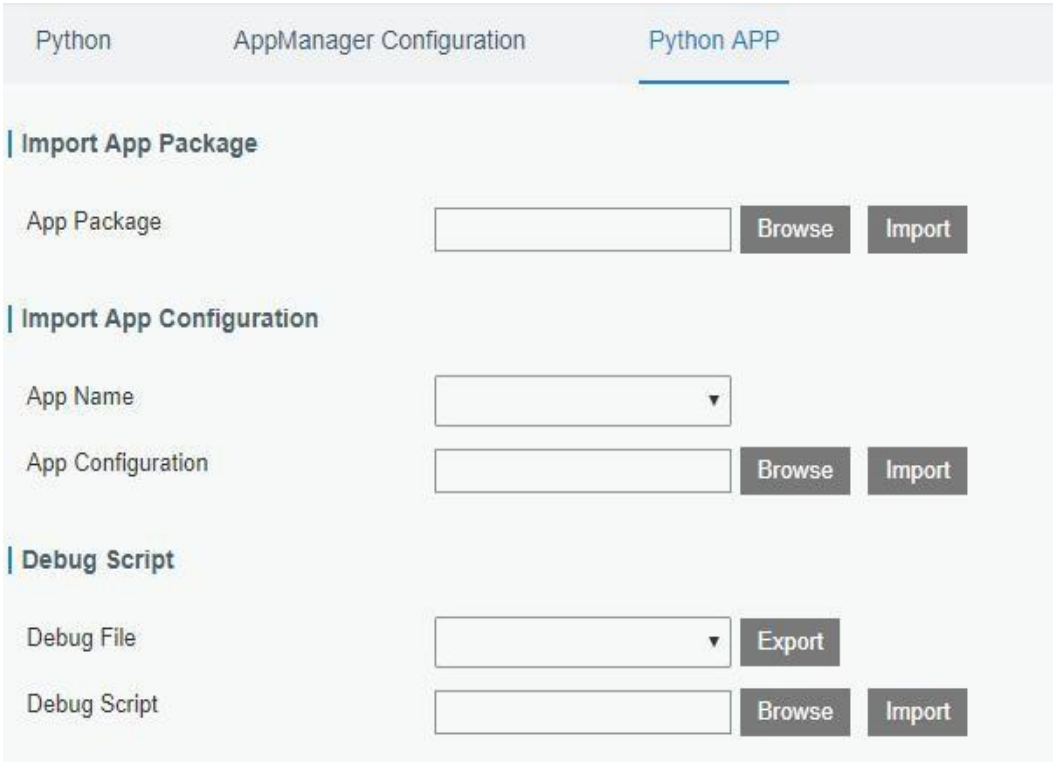


図 3-7-1-3

Python APP	
項目	説明
App Package	アプリパッケージを選択し、インポートします。
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てインポートします。
Debug File	スクリプトファイルをエクスポートします。
Debug Script	デバッグ対象の Python スクリプトを選択し、インポートします。

表 3-7-1-3 APP パラメータ

3.7.2 Node-RED

Node-RED は、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し、相互に接続するためのフローベースの開発ツールです。Node-RED は、Web 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、フローを簡単に接続することができます。詳細なガイダンスやドキュメントについては、Node-RED 公式ウェブサイトをご覧ください。

3.7.2.1 Node-RED

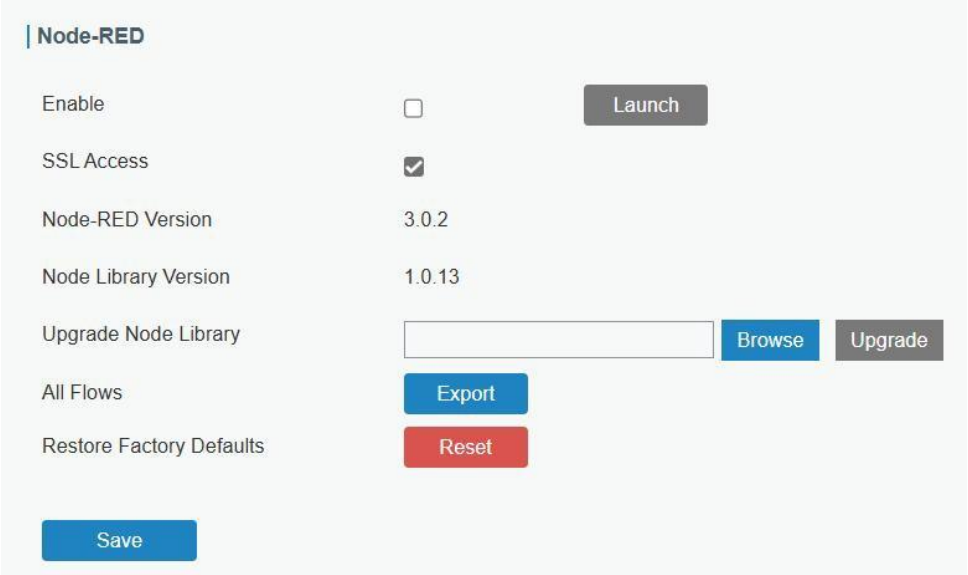


図 3-7-2-1

Node-RED	
項目	説明
Enable	Node-RED を有効にします。
Launch	クリックして、Node-REDのWeb GUIを起動します。
SSL Access	Node-REDのWeb GUIへのアクセスをHTTPSサービス経由のみに制限します。
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できます。
Node Library Version	ノードライブラリのバージョンを表示します。
Upgrade Node Library	ライブラリパッケージをインポートして、ノードライブラリをアップグレードします。
All Flows Export	すべてのフローをJSON形式のファイルとしてエクスポートします。
Restore Factory Default	Node-REDの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います。

図 3-7-2-2

Node Library	
Node	**説明**
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® ノードにダウンリンクコマンドを送信します。
Device Filter	デバイス EUI を使用して、1 つまたは複数の特定の 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。これを行うには、「**General**」>「**Events**」>「**Events Settings**」でイベント検出が有効になっている必要があります。
Email Output	メールを送信します。「SMTP」オプションで「ゲートウェイと同じ」を選択した場合は、「**System**」>「**General Settings**」>「**SMTP**」ページに移動し、SMTPクライアントの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、携帯電話回線が接続されている場合にのみ機能します。
SMS Output	SMSメッセージを送信します。これは、セルラー接続が確立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

関連する設定例

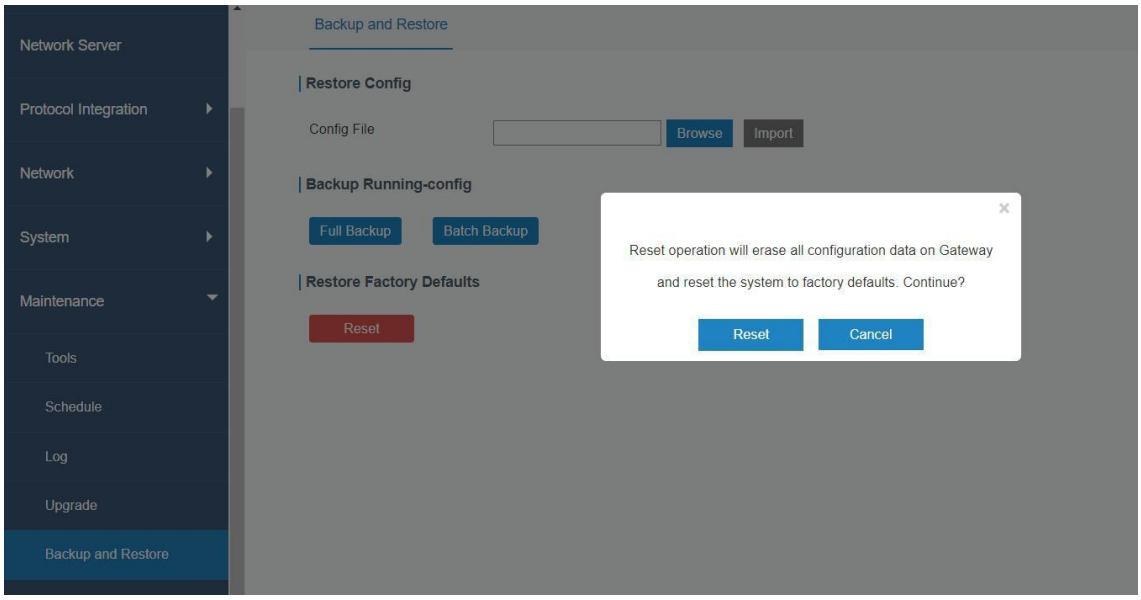
Node-RED

第4章 アプリケーション例

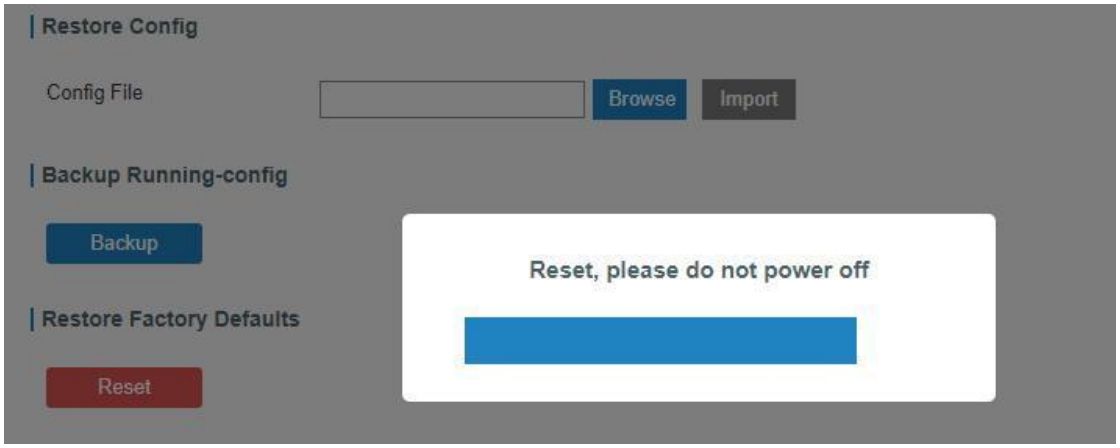
4.1 工場出荷時の設定に復元

方法 1：

Webインターフェースにログインし、「**Maintenance**」＞「**Backup and Restore**」に移動して、「**Reset**」ボタンをクリックします。工場出荷時の設定にリセットするかどうか確認のメッセージが表示されますので、確認後、「**Reset**」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になり、ログインページが再び表示されるまでお待ちください。これで、ゲートウェイが工場出荷時の設定に正常にリセットされたことを意味します。

関連トピック

工場出荷時の設定に復元する

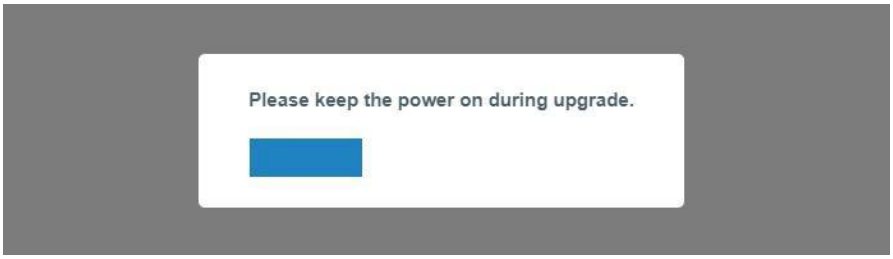
方法 2：

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秒以上長押ししてください。

4.2 ファームウェアのアップグレード

ゲートウェイのファームウェアをアップグレードする前に、まずMilesightのテクニカルサポートにご連絡いただくことをお勧めします。ゲートウェイのファームウェアファイルの拡張子は「.bin」です。
ファームウェアファイルを入手したら、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. 「Maintenance > Upgrade」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が正しいかどうかを確認します。正しい場合、ファームウェアがゲートウェイにインポートされ、その後、ゲートウェイのアップグレードが開始されます。
4. アップグレード完了後、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ご確認ください。
   開く前に、ブラウザのキャッシュを消去することをお勧めします。



関連トピック

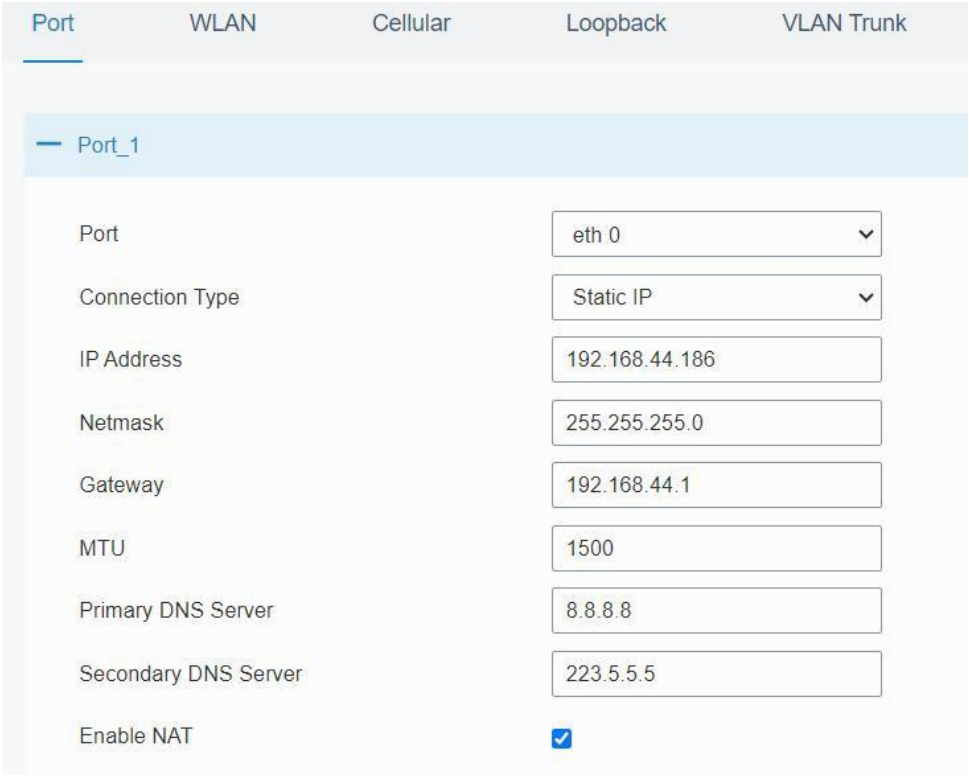
アップグレード

4.3 ネットワーク接続

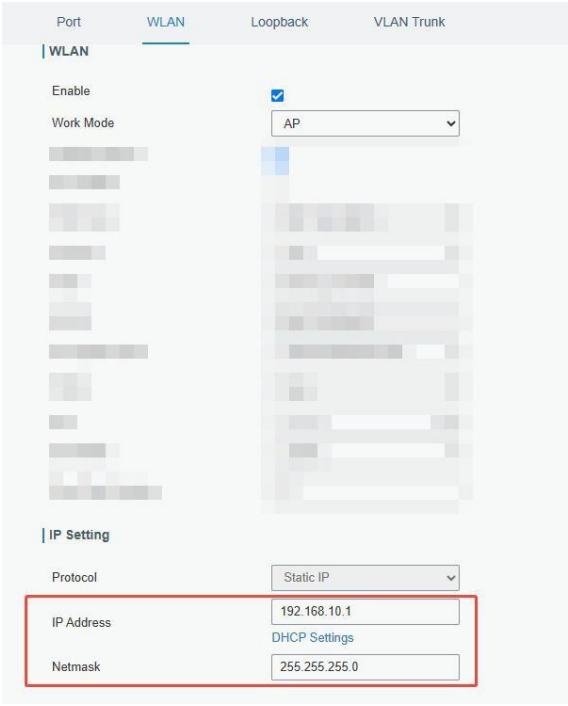
ゲートウェイは、ネットワーク接続を設定するための複数の方法を対応しています。

4.3.1 イーサネット接続

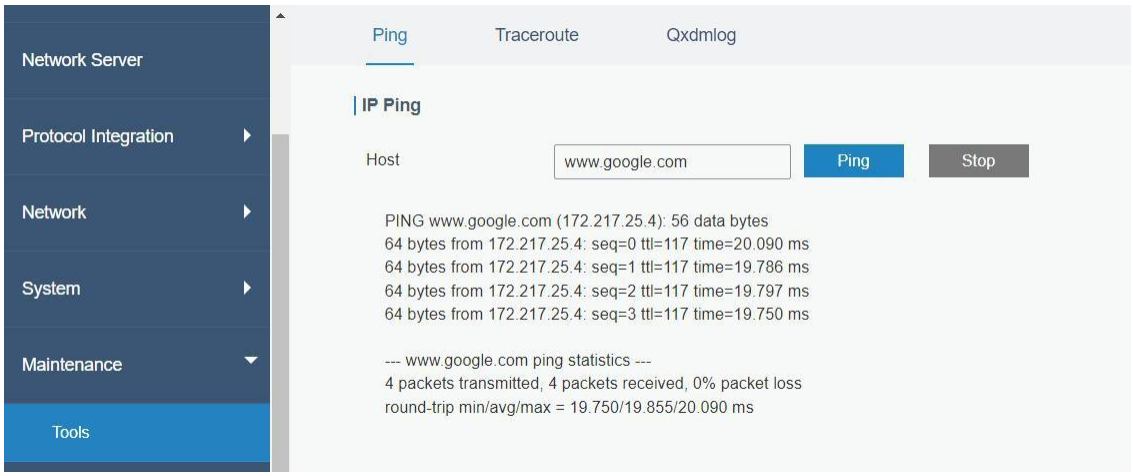
1. 「Network > Interface > Port」ページに移動し、接続タイプを選択してイーサネットポートの設定を行います。「Save & Apply」をクリックすると、設定が有効になります。



注：イーサネットポートのIPアドレスを変更する際にIPアドレスの競合が発生した場合は、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。

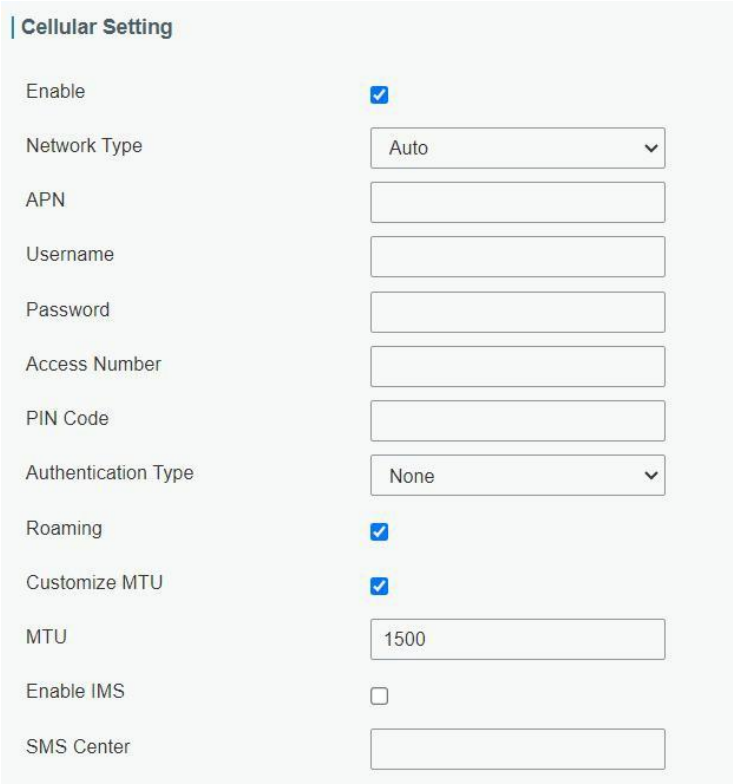


関連トピック

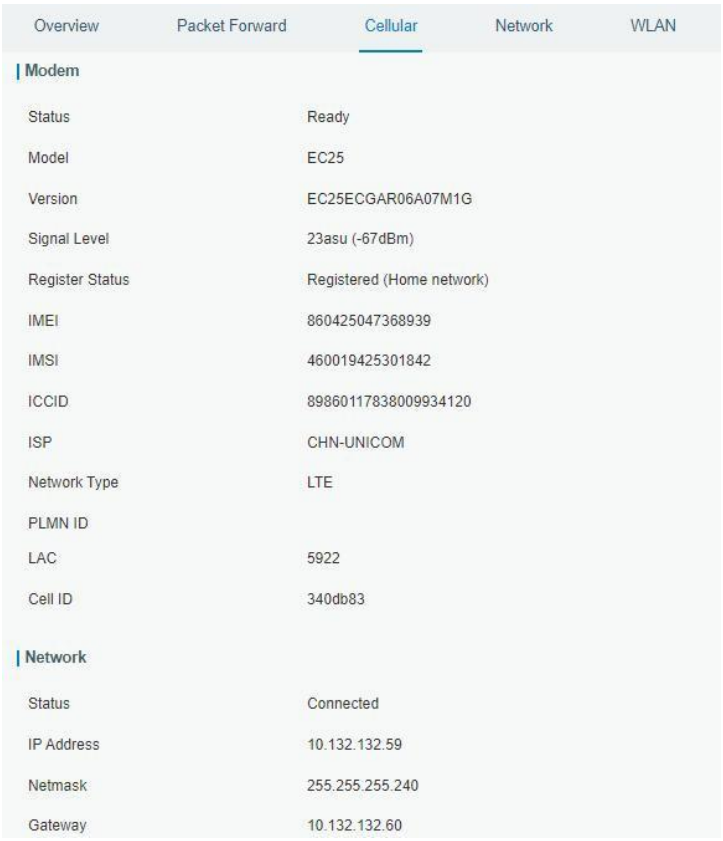
ポート設定

4.3.2 モバイル接続（モバイル版のみ）

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ます。「Save」および「Apply」をクリックして、設定を有効にしてください。



2. 「Status」＞「Cellular」をクリックして、モバイル通信のステータスを確認してください。「Connected」と表示されていれば、SIMカードの接続は正常に確立されています。



関連トピック：

モバイル設定、

モバイルステータス

4.4 Wi-Fiの応用例

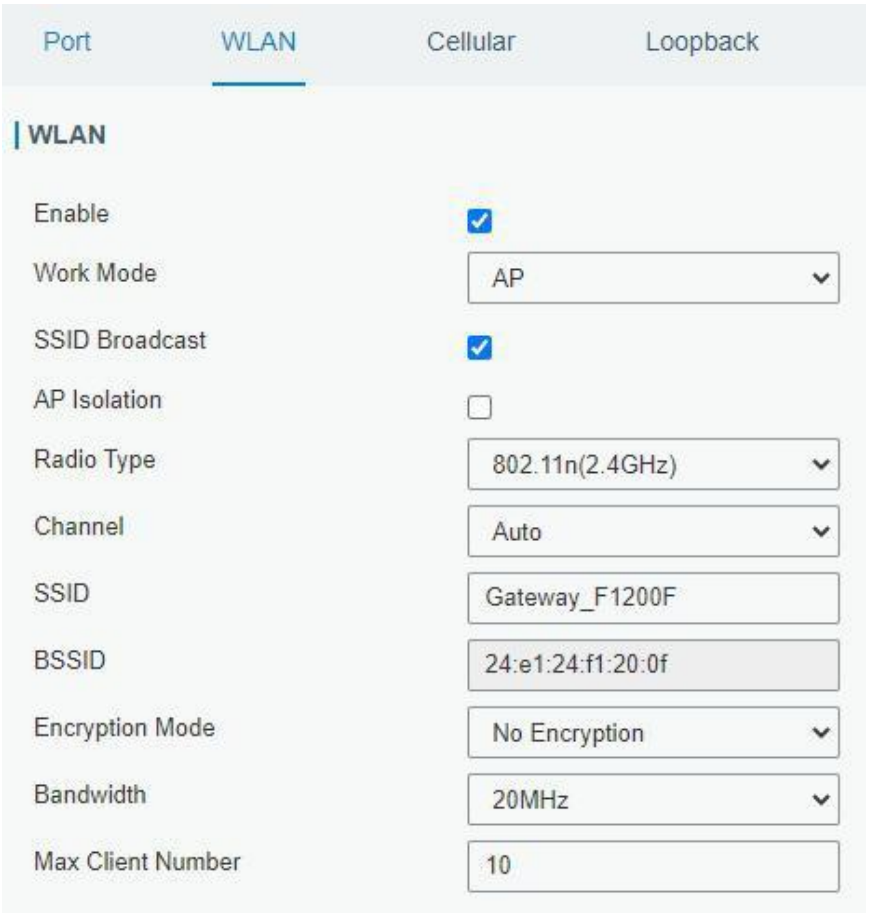
4.4.1 APモードの適

用例

UG56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。

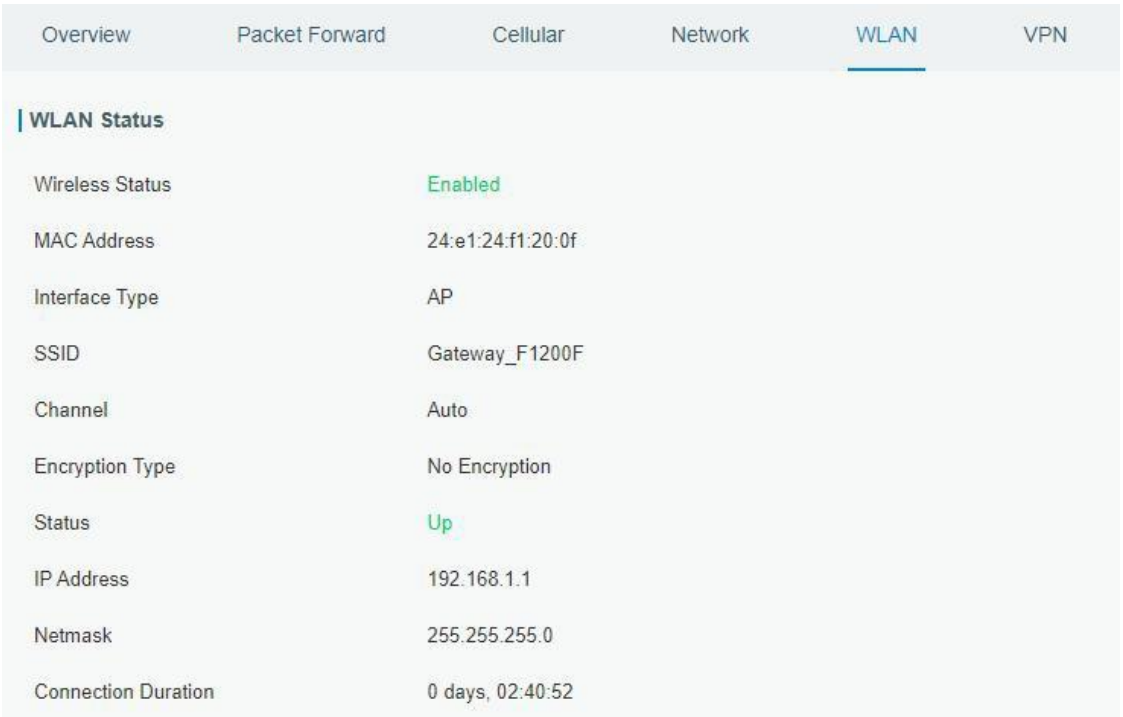
設定手順

1. 「Network > Interface > WLAN」に移動し、以下の通り無線パラメータを設定します。



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

2. スマートフォンを使用して、ゲートウェイのアクセスポイントに接続します。「Status > WLAN」に移動すると、APの設定および接続されたクライアント/ユーザーの情報を確認できます。



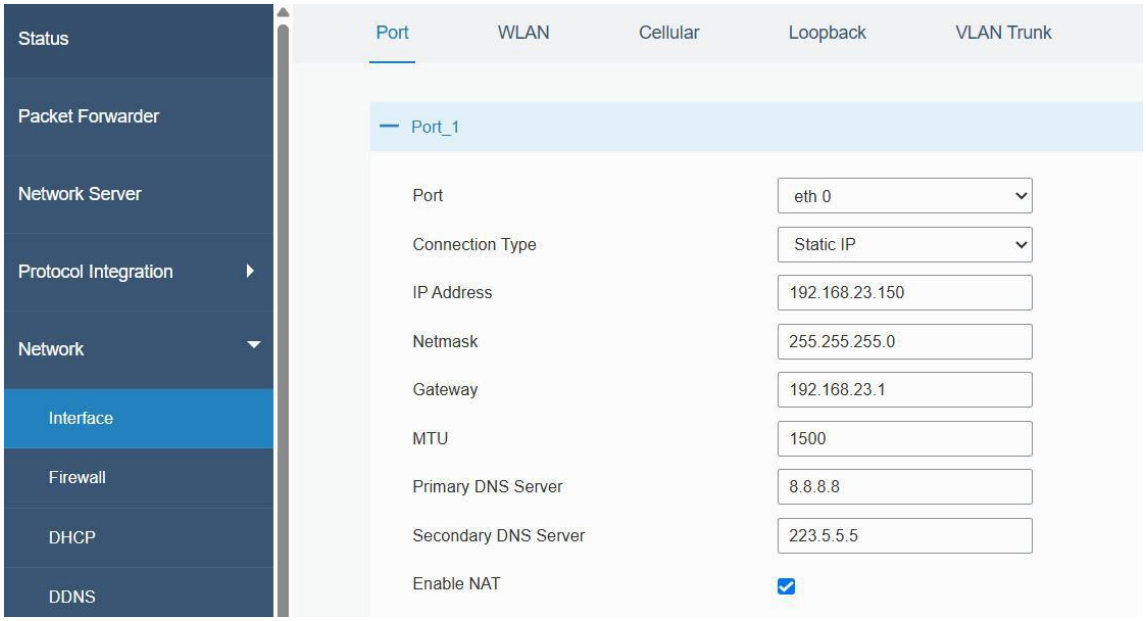
4.4.2 クライアント

モードの適用例

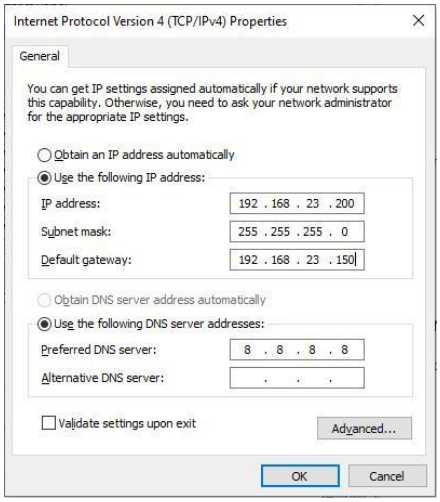
UG56をWi-Fiクライアントとして設定し、アクセスポイントに接続してインターネットにアクセスします。

設定手順

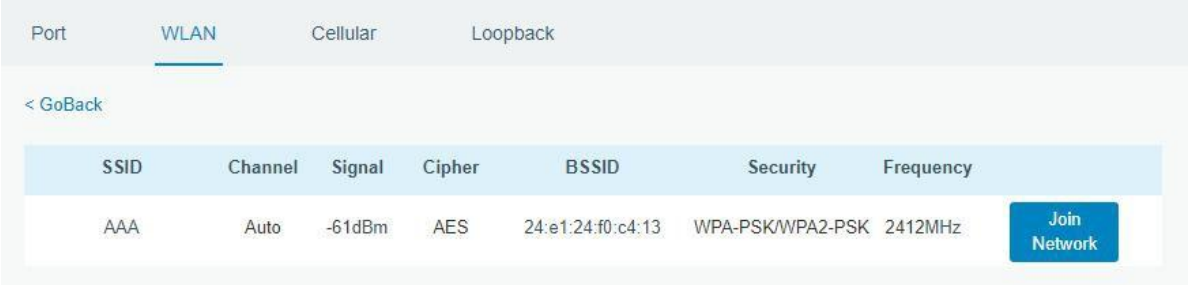
1. 「**Network**」>「**Interface**」>「**Port**」ページに移動し、接続タイプを「**Static IP**」に設定して、イーサネットWANポートのIPアドレスを設定してください。



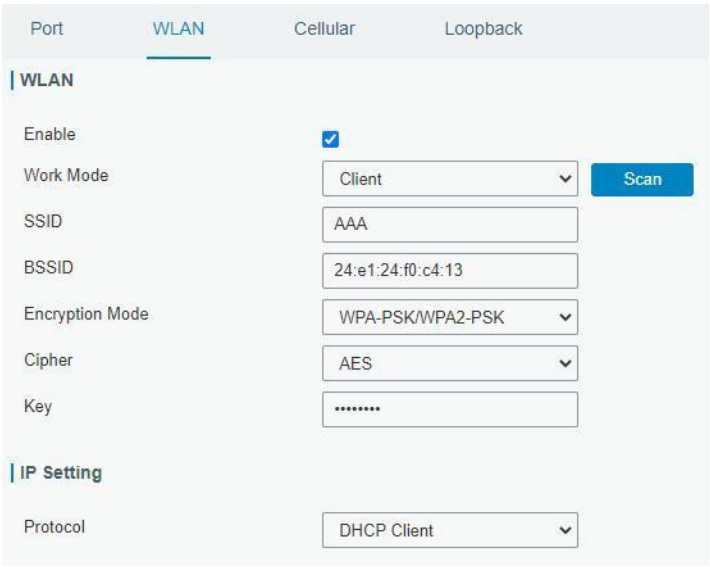
2. PCをUG56のETHポートに直接、またはPoEインジェクタを介して接続してください。
3. コンピュータに手動でIPアドレスを割り当ててください。Windows 10システムを例に挙げます：



4. Web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Web GUIにアクセスします。
5. 「**Network**」>「**Interface**」>「**WLAN**」に移動し、「**Scan**」をクリックしてWi-Fiアクセスポイントを検索します。

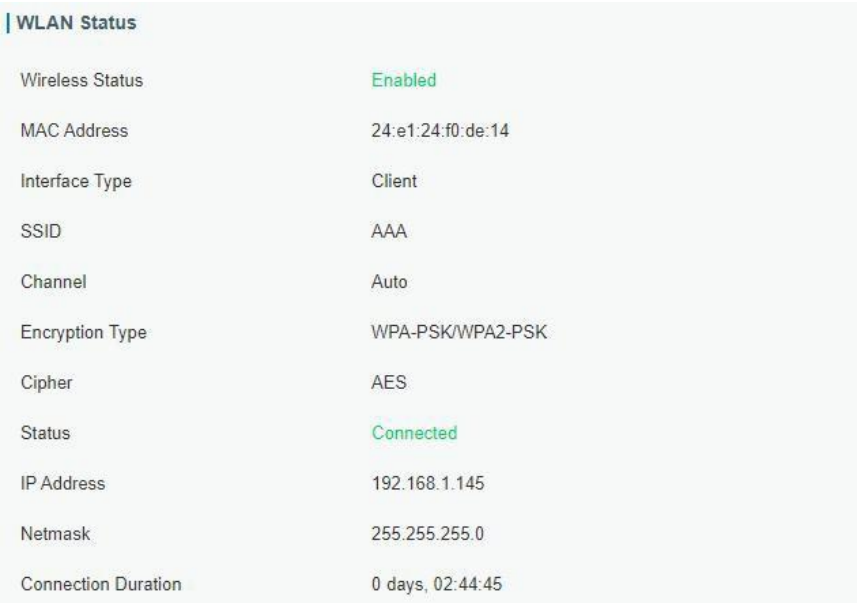


6. 1つのアクセスポイントを選択し、「**Join Network**」をクリックしてから、そのアクセスポイントのパスワードを入力します。

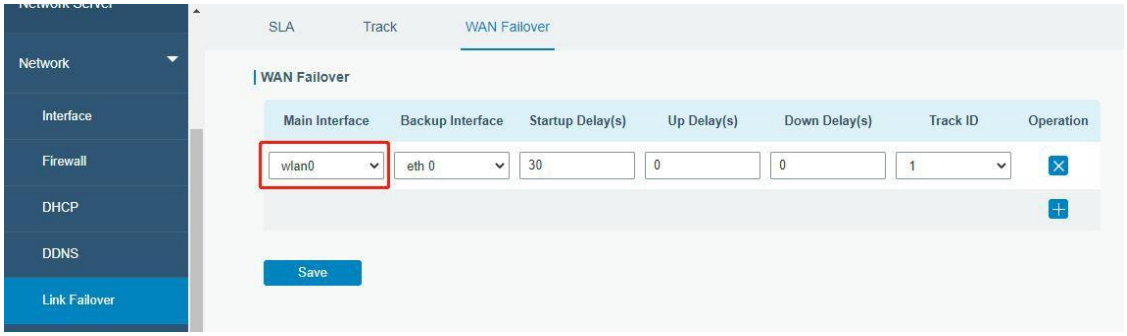


すべての設定が完了したら、「**Save**」および「**Apply**」ボタンをクリックしてください。

7. 「**Status**」＞「**WLAN**」に移動し、クライアントの接続状態を確認してください。



8. 「**Network**」＞「**Failover**」＞「**WAN フェイルオーバー**」に移動し、wlan0 をメインインターフェースに切り替えると、ゲートウェイは Wi-Fi を使用してネットワークにアクセスできるようになります。



関連トピック

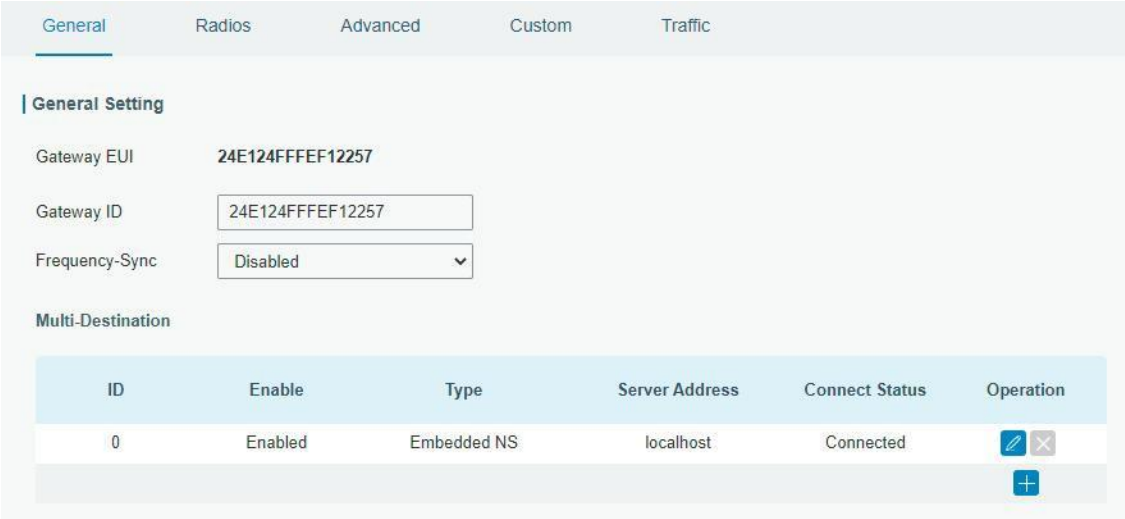
WLANの設定

WLANのステータス

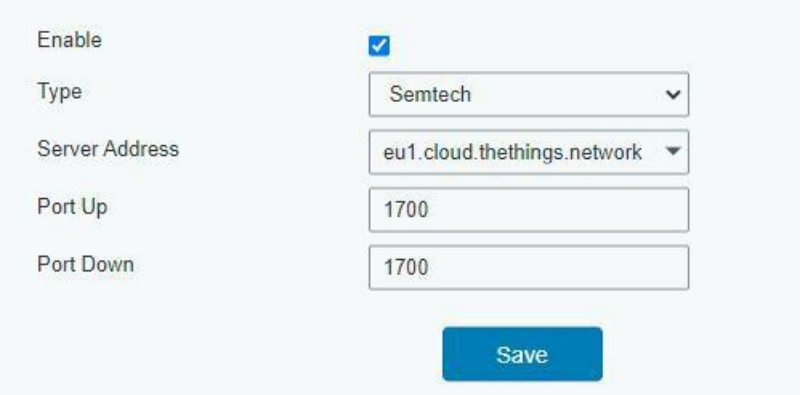
4.5 パケットフォワーダーの設定

UG56 ゲートウェイには、Semtech、Basic station、Chirpstack など、複数のパケットフォワーダーがインストールされています。接続する前に、ゲートウェイがネットワークに接続されていることを確認してください。

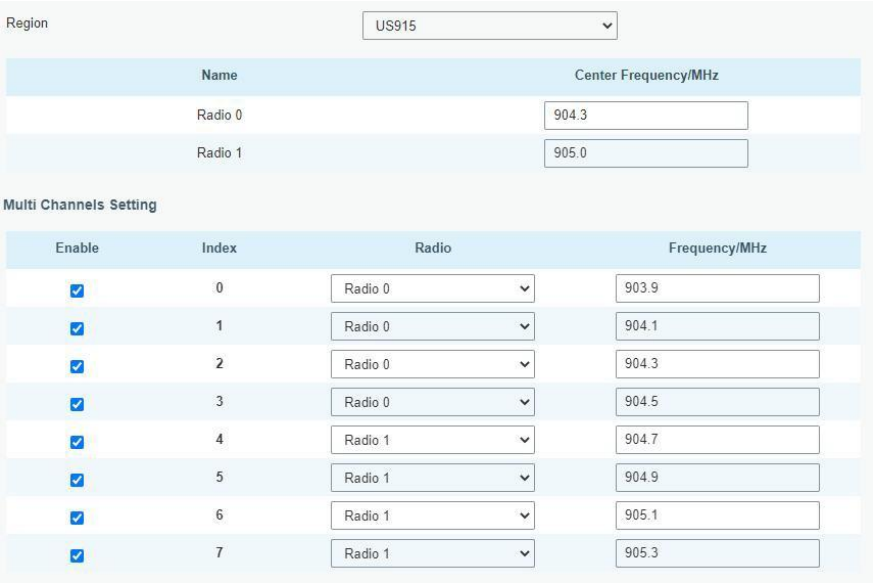
1. 「**Packet Forwarder**」>「**General**」に移動します。



2. 「  」をクリックして、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ます。



3. 「**Packet Forwarder**」＞「**Radio**」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。ゲートウェイとネットワークサーバーのチャンネルは同じである必要があります。



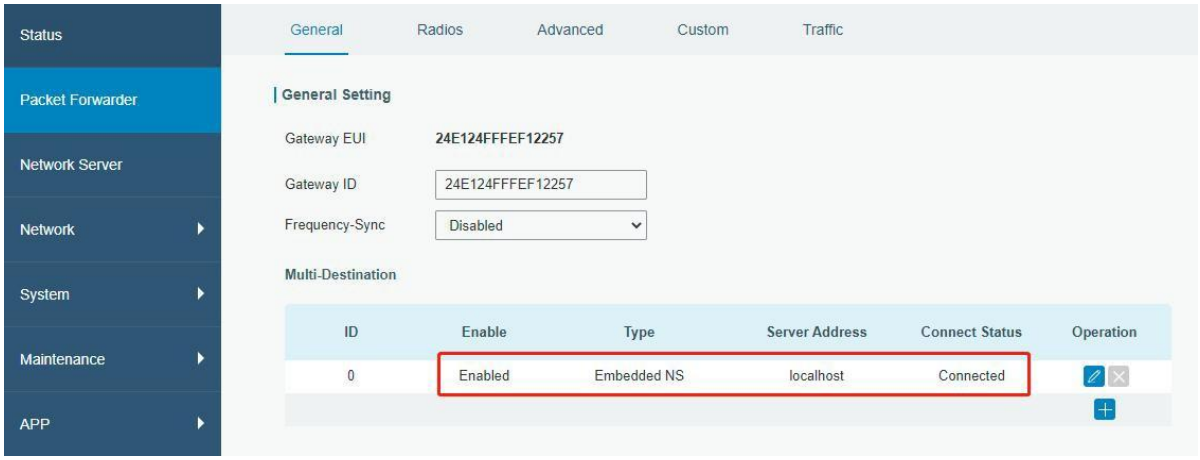
4. ネットワークサーバーページでゲートウェイを追加してください。ネットワークサーバー接続の詳細については、Milesight IoT対応ポータルをご参照ください。

4.6 ネットワークサーバーの設定

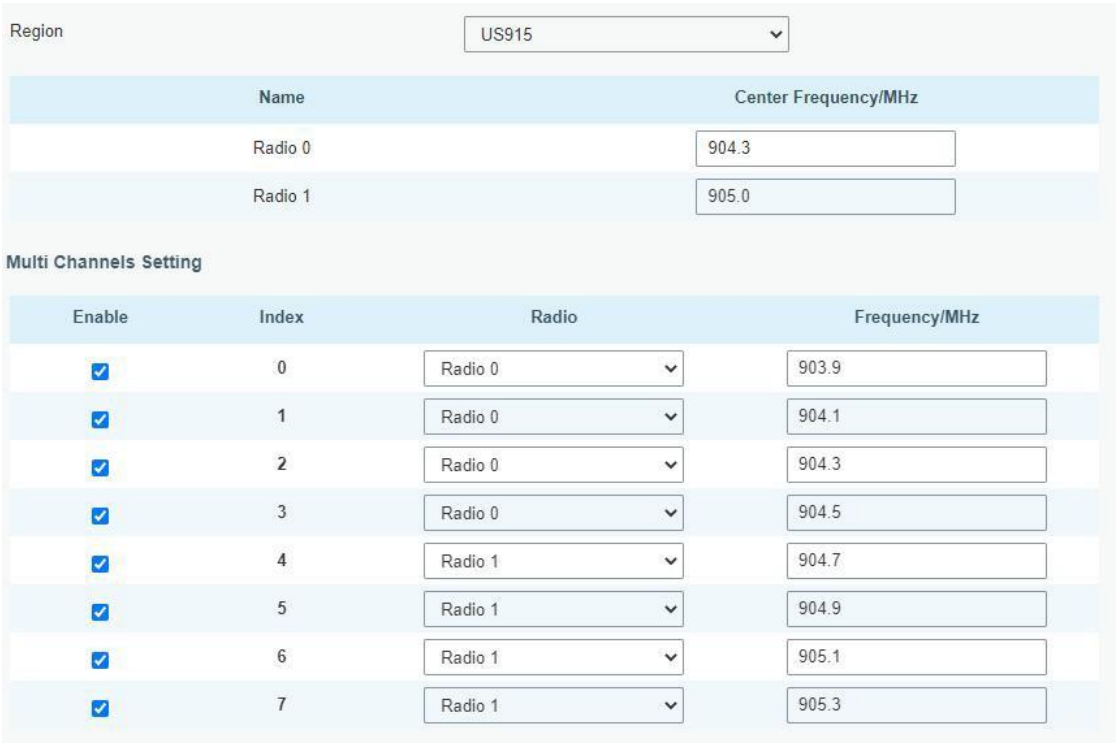
このゲートウェイは、LoRaWAN® ネットワークサーバーとして機能し、LoRaWAN® エンドデバイスのデータを受信・分析することで、さまざまなシステムとの柔軟な連携を実現します。

4.6.1 Milesight IoT Cloudに接続する

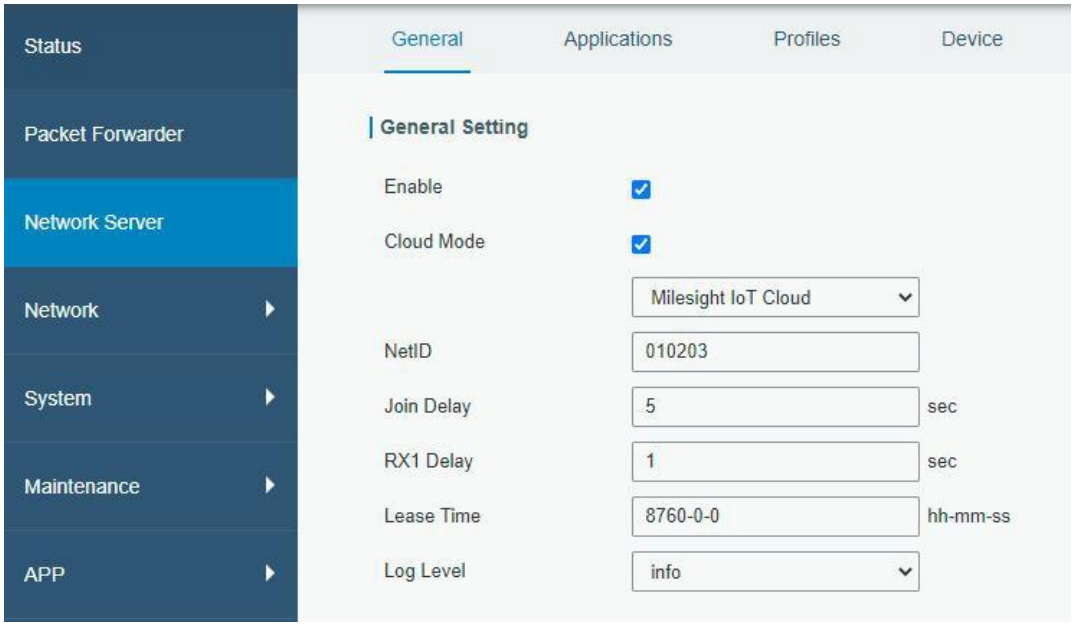
1. 「**Packet Forwarder**」＞「**General**」ページに移動し、組み込みネットワークサーバーを有効にしてください。



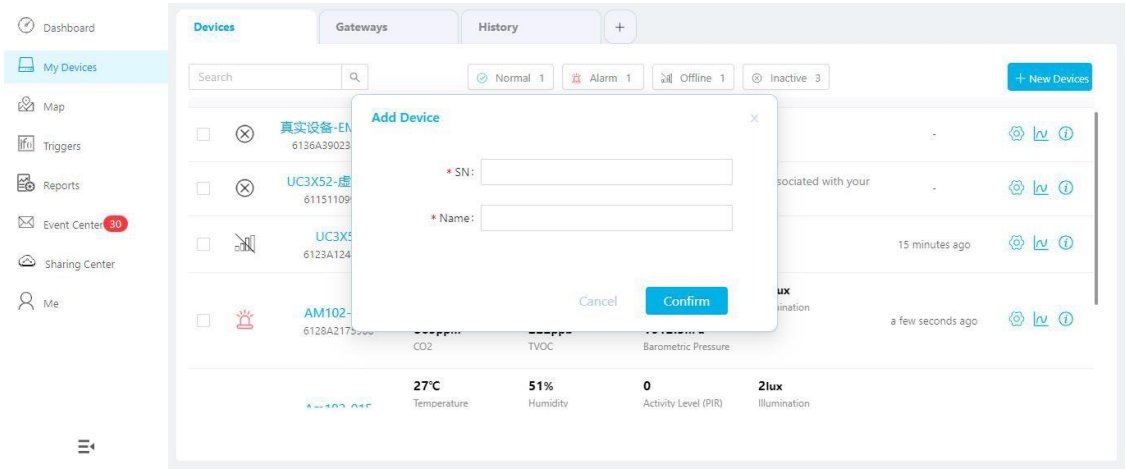
2. 「**Packet Forwarder**」＞「**Radio**」ページに移動し、中心周波数とチャンネルを設定します。ゲートウェイとエンドデバイスのチャンネルは同一である必要があります。



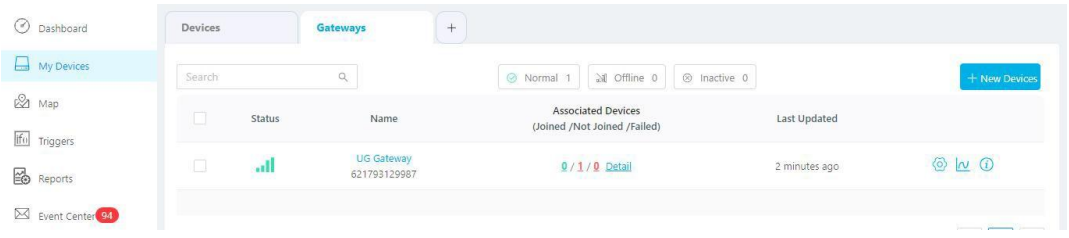
3. 「**Network Server**」＞「**General**」ページに移動し、ネットワークサーバーと「Cloud mode」を有効にしてから、「Milesight IoT Cloud」モードを選択してください。



4. Milesight IoT Cloudにログインします。次に、「**My Devices**」ページに移動し、「+New Devices」をクリックして、SN経由でMilesight IoT Cloudにゲートウェイを追加します。ゲートウェイは「**Gateways**」メニューの下に追加されます。

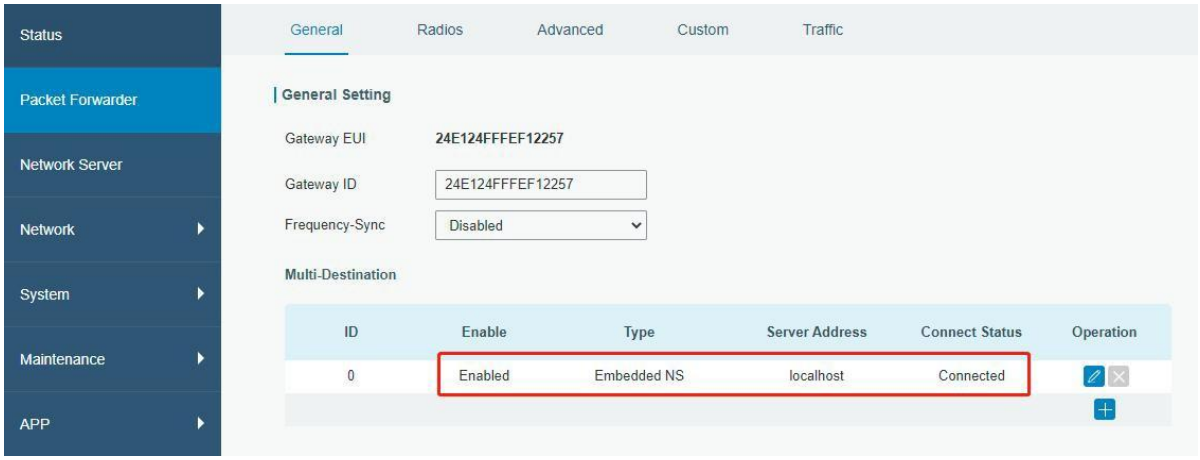


5. Milesight IoT Cloud上でゲートウェイがオンライン状態になります。

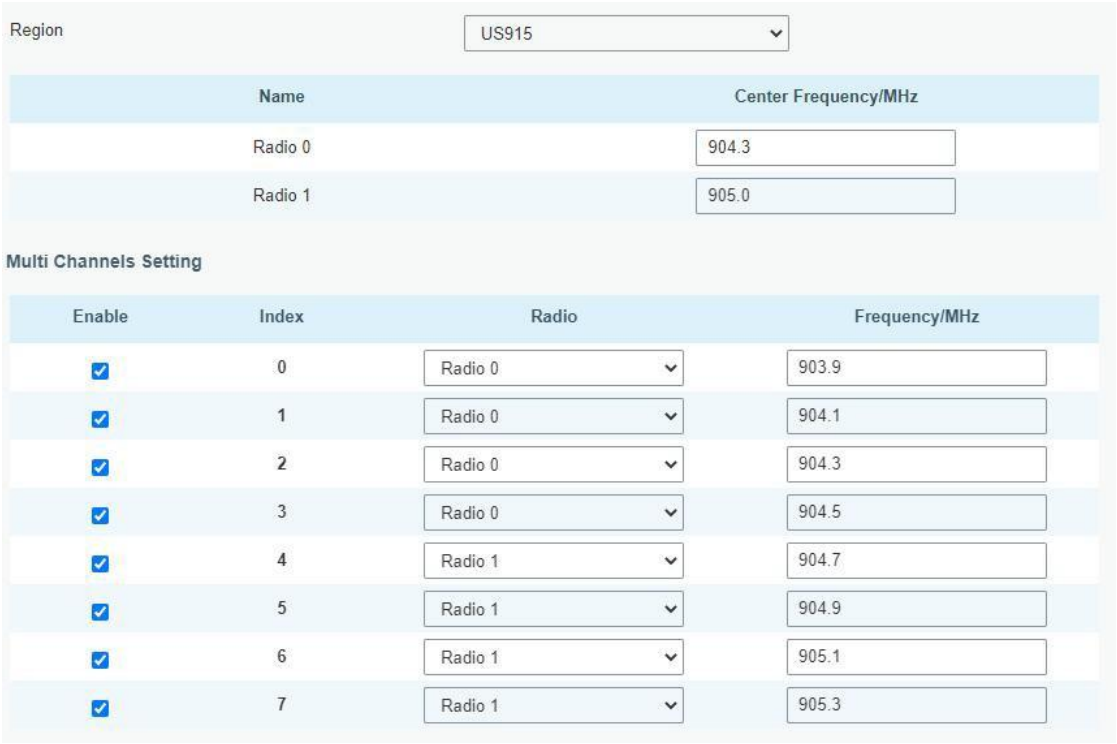


4.6.2 エンドデバイスを追加する

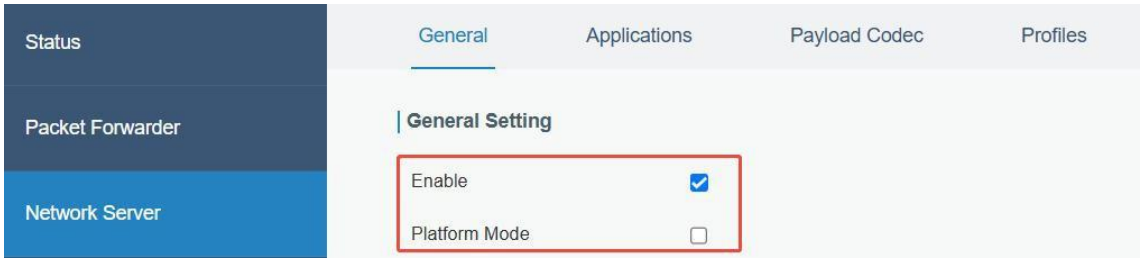
1. 「**Packet Forwarder**」＞「**General**」ページに移動し、組み込みNSを有効にしてください。



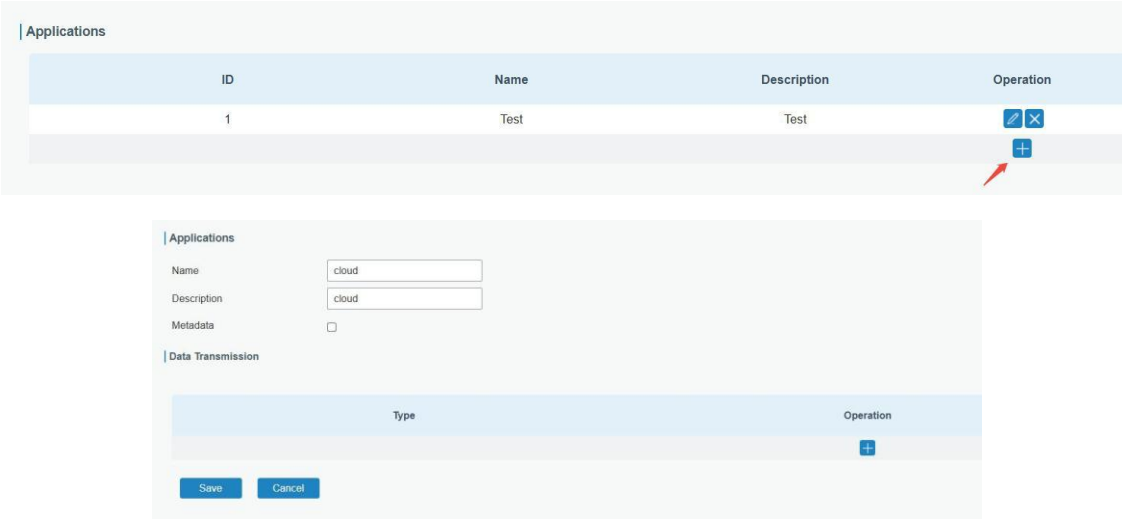
2. 「**Packet Forwarder**」＞「**Radio**」ページに移動し、中心周波数とチャンネルを設定します。ゲートウェイとエンドデバイスのチャンネルは同じである必要があります。



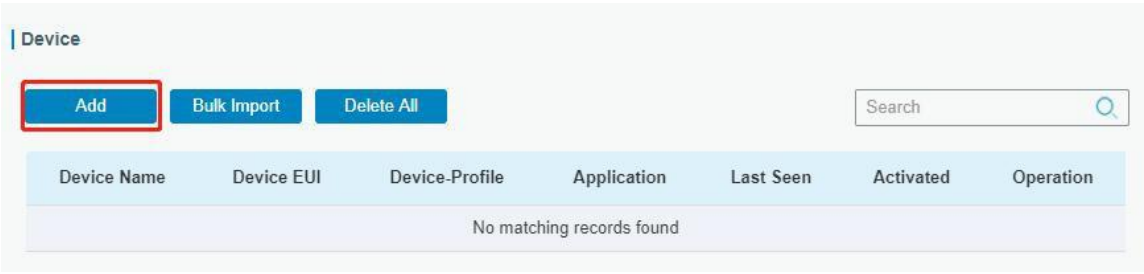
3. 「**Network Server**」＞「**General**」ページに移動し、ネットワークサーバーを有効にしてください。



4. 「**Network Server**」>「**Applications**」ページに移動し、アプリケーションを追加します。

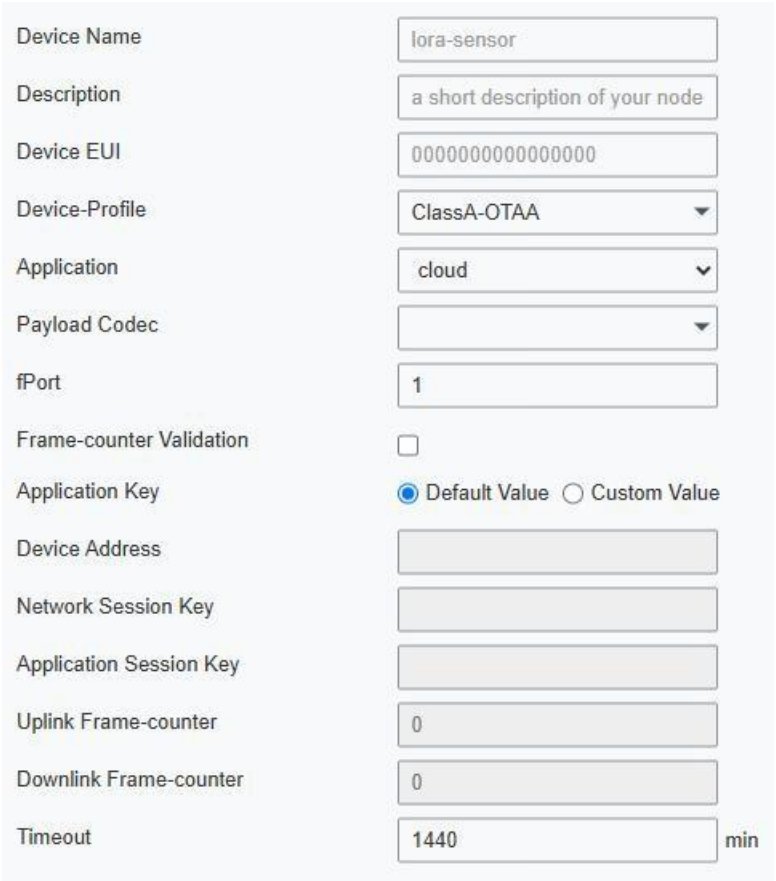


5. 「**Network Server**」＞「**Device**」ページに移動し、「**Add**」をクリックしてLoRaWAN® ノードデバイスを追加します。「**Bulk Import**」をクリックしてテンプレートを使用し、デバイスを一括で追加することもできます。

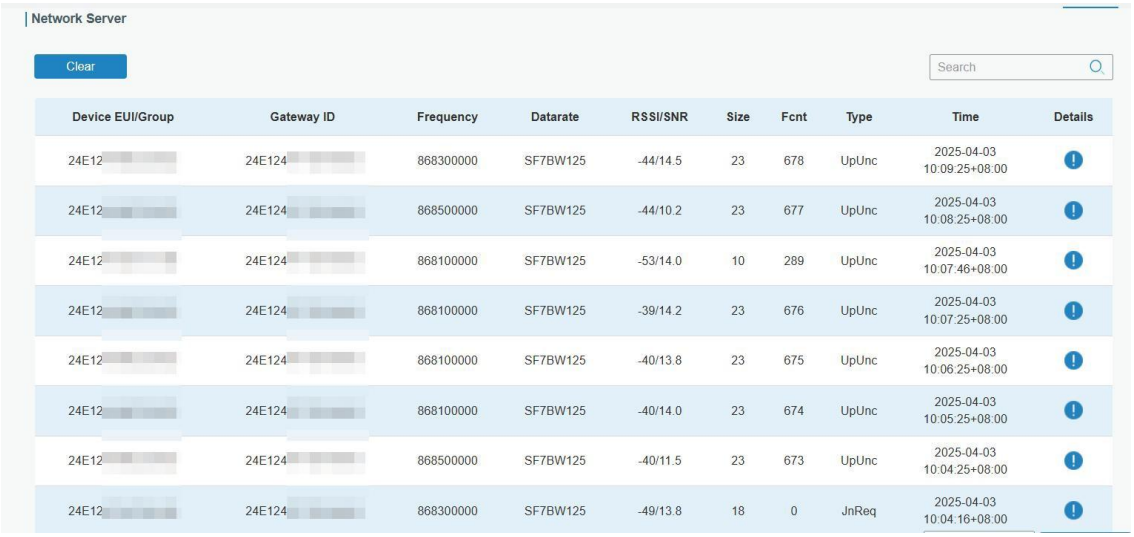


6. エンドデバイスの情報を入力し、「**Save&Apply**」をクリックしてください。この情報は、エンドデバイスの設定ページまたはメーカーのマニュアルで確認できます。Milesight製エンドデバイスのデフォルト設定は以下の通りです：

- 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 タイプのファイル
- ペイロードコーデック：モデルを選択してください。fPort：85
- アプリケーションキー：「Default Value」を選択してください。ランダムなキーを使用する場合は、「Custom Value.」を選択してください。
- タイムアウト：デバイスのオンライン／オフライン状態を判定する時間です。



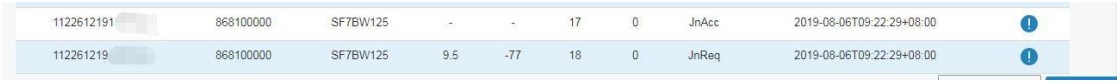
7. 「**Network Server**」＞「**Packets**」ページに移動し、このデバイスからのアップリンクがあるかどうかを確認してください。



[Details] をクリックして、パケットの詳細とデコード結果を確認してください。

4.6.3 デバイスへのデータ送信

1. 「**Network Server**」>「**Packets**」に移動し、ネットワークサーバーリストで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確認してください。



2. デバイスの EUI を入力するか、ダウンリンクを送信する必要があるマルチキャストグループを選択してください。次に、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」をクリックします。

4. ネットワークサーバーのリストでパケットを確認し、デバイスがこのメッセージを正常に受信したことを確認してください。「Confirmed」を有効にすることをお勧めします。マルチキャスト機能では、確認済みのダウンリンクには対応していません。

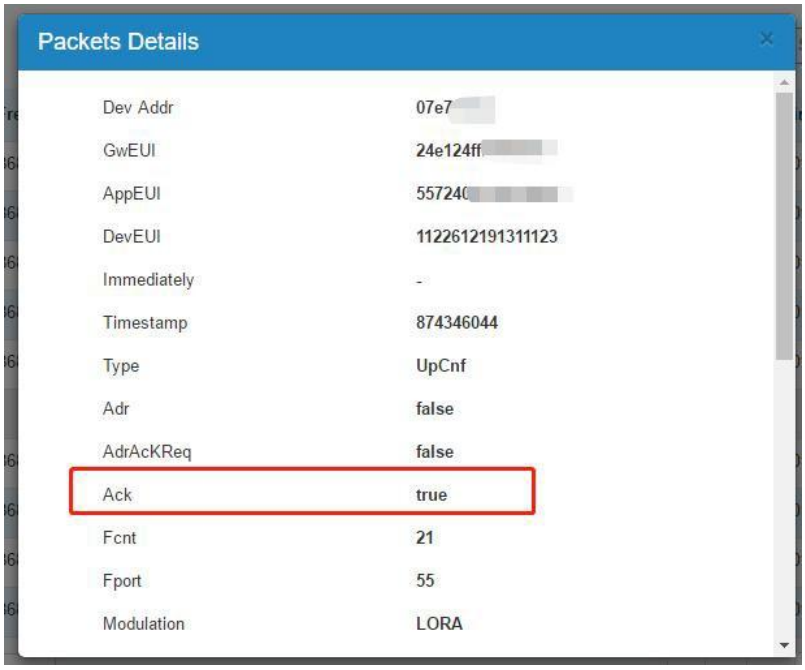
「Refresh」をクリックしてリストを更新するか、リストの自動更新周波数を設定することができます。デバイスのクラスタイプがClass Cの場合、そのデバイスは常にパケットを受信し続けます。

このパケットのタイプは DnCnf（ダウンリンク確認パケット）です。パケットの色が灰色の場合、キューに少なくとも1つのメッセージが残っているため、現在その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意味します

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

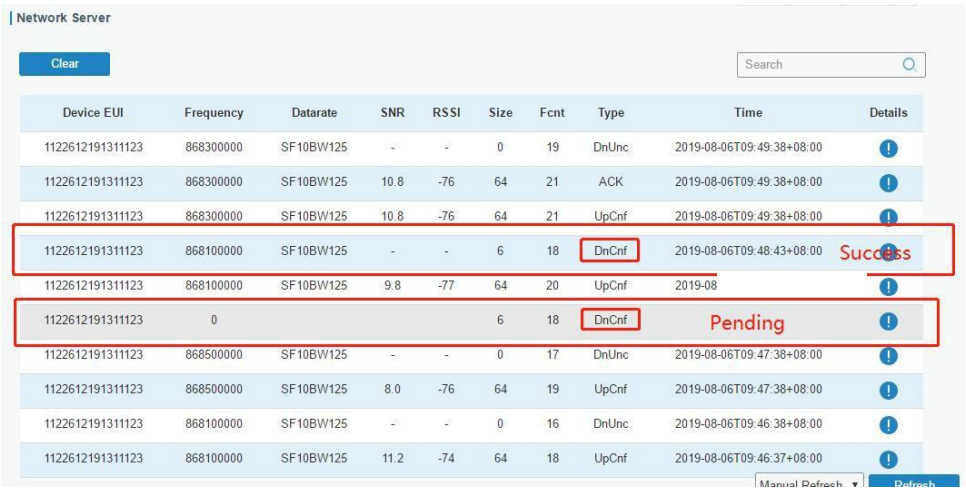
デバイスがこのダウンリンク確認パケットを受信した場合、デバイスは次のパケットを送信する際に「**ACK**」を返信します。

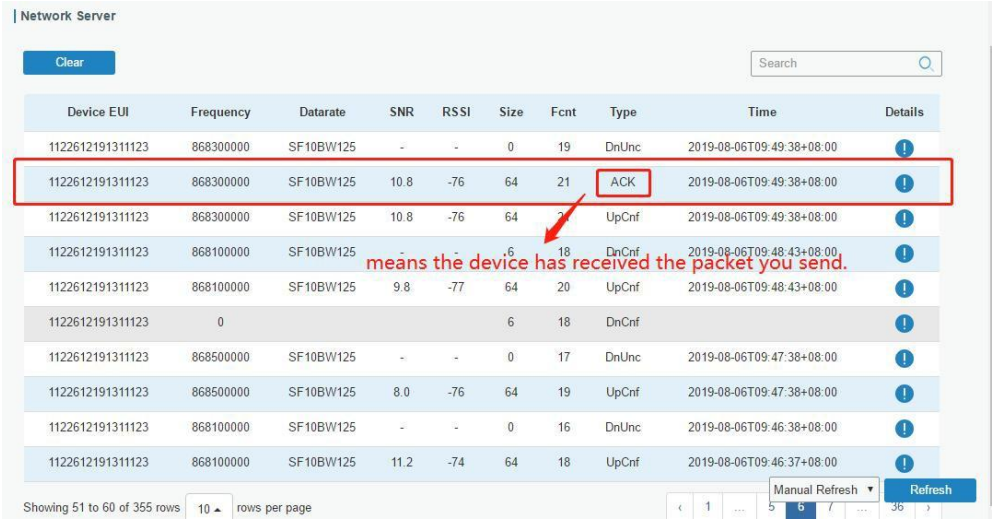
Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Type	Time	Details
11226121913	868300000	SF10BW125	-	-	0	3	DnUnc	2019-08-06T09:23:44+08:00	
1122612191	868300000	SF10BW125	10.5	-75	64	2	UpCnf	2019-08-06T09:23:44+08:00	
112261219	869525000	SF12BW125	-	-	6	2	DnCnf	2019-08-06T09:22:55+08:00	
112261219	0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



Ackが「**true**」であるということは、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て初めて、ネットワークサーバーはデバイスにデータを送信します。





関連トピック

パケット

4.6.4 HTTP/MQTT サーバーへの接続

ゲートウェイは、MQTT、HTTP、または HTTPS プロトコルを使用して別のサーバーアドレスにデータを送信するためのデータ転送プロトコルの選択に対応しています。

1. **[Network Server] > [Application]** に移動し、編集するアプリケーションを選択します。
2. 「  」をクリックして、データ送信タイプを追加します。

HTTP または HTTPS：

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

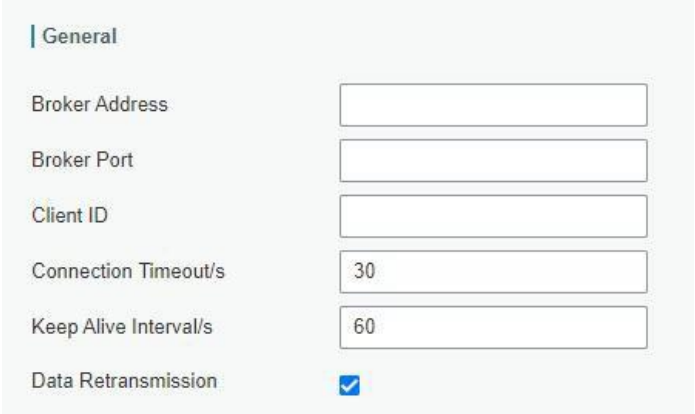
ステップ2：宛先URLを入力します。異なる種類のデータを異なるURLに送信することができます。

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：

手順 1：伝送プロトコルとして MQTT を、設定モードとして「Manual Configuration」を選択します。

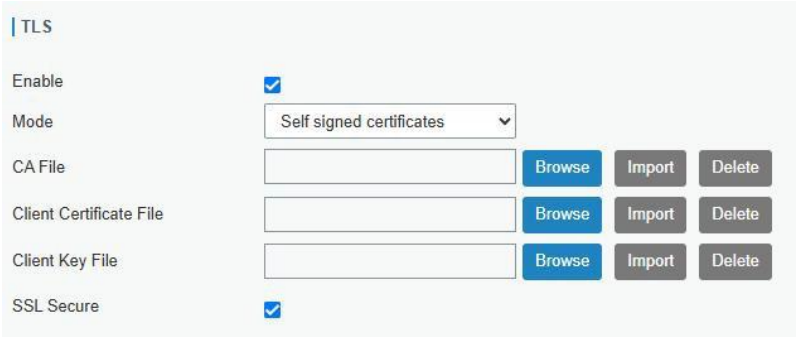
ステップ 2：MQTT ブローカーの基本設定を入力します。



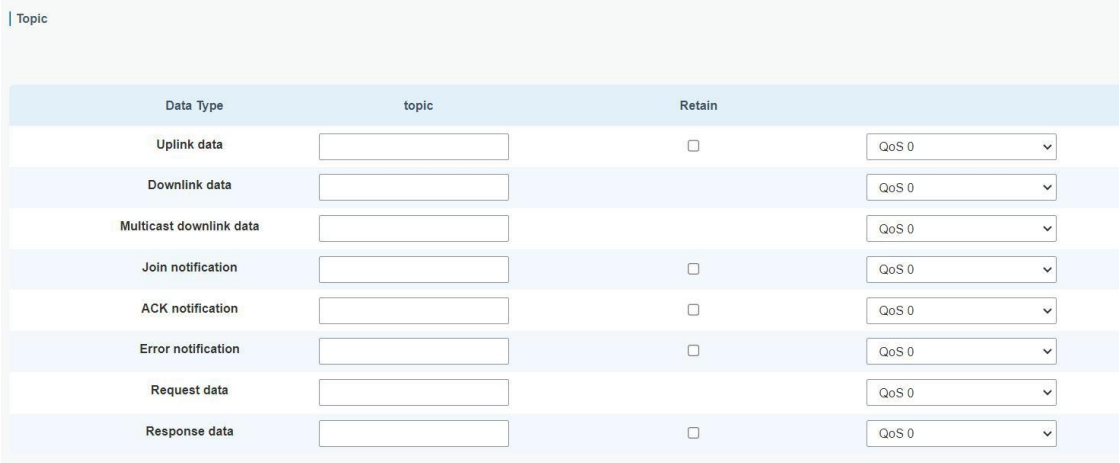
ステップ3：サーバーで要求される認証方法を選択します。

認証にユーザー認証情報を選択する場合は、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、およびクライアントキーファイルをインポートしてください。



ステップ 4：データを受信したりダウンリンクを送信したりするためのトピックを入力し、QoS を選択します。

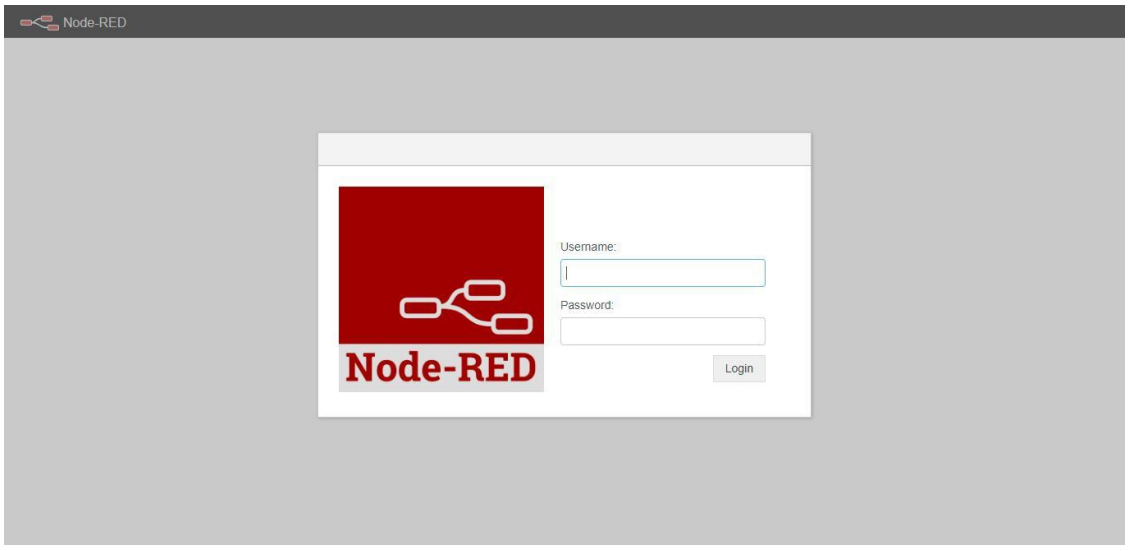


4.7 Node-RED

4.7.1 Node-RED を起動します

1. 「App > 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、「Launch」をクリックして Node-RED の Web GUI に移動し、gateway 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。



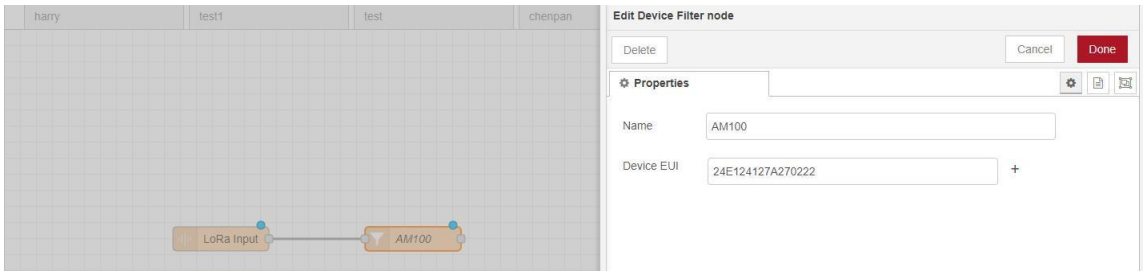
4.7.2 メールによるデータ送信

アプリケーション例

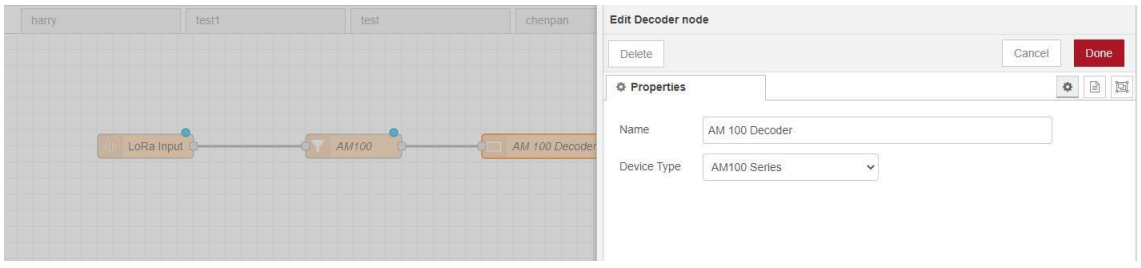
AM102デバイスのデータをメールで送信します。

設定手順

1. 「LoRa Input」ノードを追加します。追加する前に、ネットワークサーバーモードが有効になっており、LoRaWAN デバイスがネットワークに参加していることを確認してください。
2. 多くのデバイスを追加し、特定の1つ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「Device Filter」ノードを追加し、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に、「Decoder」ノードを追加してください。

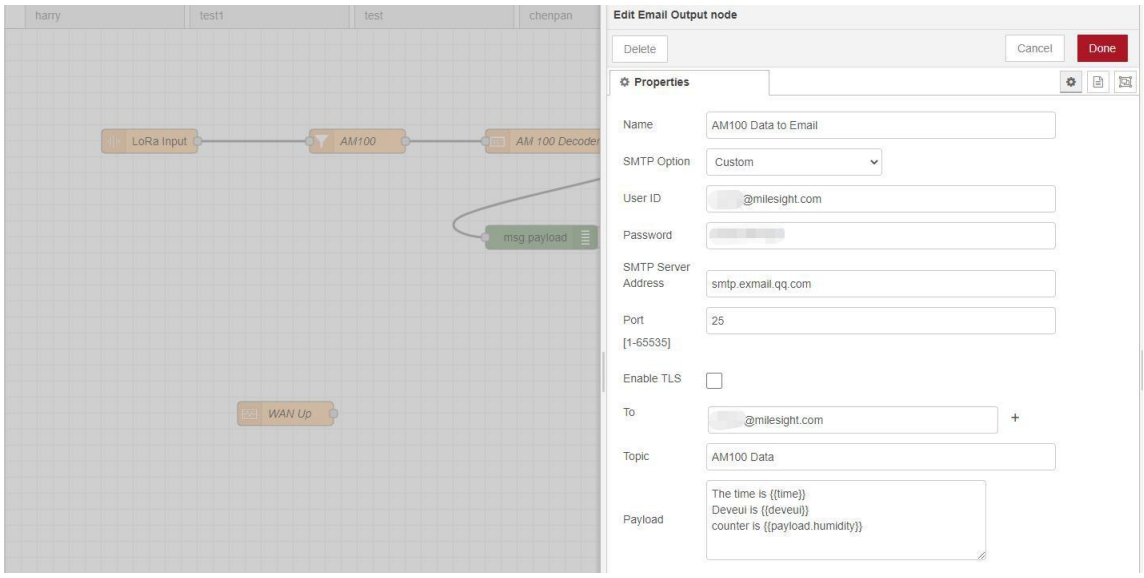


4. 「Email Output」を追加し、SMTPクライアントの設定、宛先メールアドレス、および本文を入力してください。本文の例：

時刻は {{time}} です。

デバイスIDは {{deveui}} です。

湿度は {{payload.humidity}} です



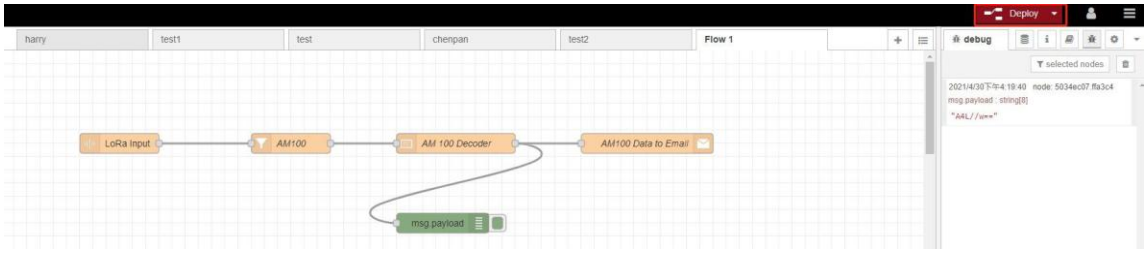
注：

1) SMTPオプションを「ゲートウェイと同じ」に設定する場合は、**[System] > [General Settings] > [SMTP]** に移動し、SMTPクライアントを設定してください。

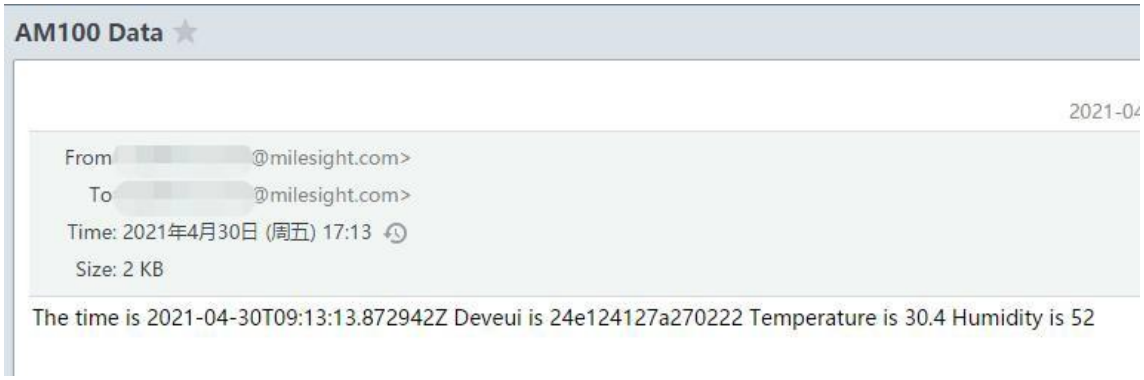
2) LoRaWANノードのデータを呼び出す際の基本的な形式は *{{property name}}* です。EメールやSMSのペイロード形式に関する詳細については、「Help」ページをクリックしてください。

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、ゲートウェイはそのデータをメールに転送します。



関連トピック

Node-RED

[以上]