Milesight

IoTゲートウェイの構築

EG71

管理者ガイド

目次

第1章：このガイドについて

このガイドでは、ゲートウェイのWeb GUIの設定および動作手順と詳細について説明します。

読者

このガイドは、ビル管理システムの導入準備、設定、および動作を行う必要がある管理者の方を対象としています。ここでは、読者の皆様がネットワークやその他のIT分野に関する知識をお持ちであることを前提としています。

著作権表示

安全上の注意

本操作ガイドは、ユーザーが製品を正しく使用し、危険や財産の損失を回避することを目的としています。Milesightは、本操作ガイドの指示に従わなかったことに起因するいかなる損失や損害についても責任を負いません。

警告：
これらの警告を無視した場合、重傷や死亡事故につながる恐れがあります。

- 本製品の設置は、資格を持つサービス担当者が行う必要があり、地域の電気安全規制を厳守してください。
- 火災や感電の危険を避けるため、設置前は製品を雨や湿気から遠ざけてください。
- 本製品は動作中に底面が非常に高温になります。触れないでください！
- 設置中は、本体の電源を入れたり、他の電気機器に接続したりしないでください。
- 損傷したケーブルを使用して本機を接続したり、電源を入れたりしないでください。
- プラグが電源コンセントにしっかりと差し込まれていることを確認してください。
- 設置の際は、本体がしっかりと固定されていることを確認してください。

注意：

これらの注意事項を無視すると、怪我や機器の損傷を引き起こす恐れがあります。

- 本製品は屋内専用です。
- 本製品は、いかなる方法でも分解または改造しないでください。
- 本製品を、裸火のある物の近くに置かないでください。
- 動作温度範囲を下回る、または上回る場所に本機を置かないでください。
- 本機を落下させたり、物理的な衝撃を与えたりしないでください。
- 熱の蓄積を防ぐため、本機の周囲の空気の流れを妨げないでください。

改訂履歴

Release Date	バージョン	説明
Jan. 16, 2026	V1.0	初期バージョン
March 31, 2026	V1.1	1. 「データ取得」および「Interface」メニュー内の各タブで、LoRaWAN機能のレイアウトと名称を調整してください。 2. ModbusおよびBACnetオブジェクトの最小収集間隔は1秒に設定されています。 3. グローバルオブジェクトをHTTP/MQTTデータ転送ルールの「メタデータ」に統合し、「オブジェクト設定」ページから「デバイス」ページを削除しました。 4. MQTT転送設定ページのレイアウトを更新しました。 5. MQTTアップリンクデータトピックにワイルドカードを追加しました。 6. HTTPS アクセスはデフォルトで有効になっており、HTTP アクセスは無効になっています。 7. Web GUIに初めてログインすると、パスワード変更のメッセージが表示されます。 8. Webパスワードには、少なくとも1文字と1つの数字を含める必要があります。 9. 「HTTPS リダイレクトを強制する」オプションを追加しました。 10. Docker を搭載しています。

第2章 製品紹介

EG71は、スマートビルディング用途向けに設計された、高性能でインテリジェントなエッジIoTゲートウェイです。有線および無線接続の両方に対応するEG71は、さまざまな現場デバイスからのシームレスなデータ集約を可能にし、迅速なプラグアンドプレイ方式のBMS導入を実現します。現場レベルのセンサーやアクチュエータとクラウドプラットフォームやBMSシステムを接続し、コンパクトな筐体で信頼性の高いデータ処理、ローカルオートメーション、およびリモート管理を提供します。

商業ビル、キャンパス、ホテル、および産業施設におけるビルオートメーション、エネルギー管理、空調制御、その他のIoTアプリケーションに最適です。

このゲートウェイには、以下の機能があります：

- 大容量メモリを搭載したクアッドコアの産業用グレードプロセッサにより、大規模なデバイス接続やエッジ処理においても安定したパフォーマンスを確保します
- RS485、KNX、M-BUS（開発中）、LoRaWAN®、Wi-Fi、およびイーサネット機器に対してネイティブに対応する包括的なI/Oインターフェース
- Milesightデバイスを素早く追加できるNFCを搭載
- イーサネット、セルラー（4G）、Wi-Fiなど、複数のバックホールオプションにより、信頼性の高いネットワーク冗長性を実現
- Modbus、BACnet、MQTT、HTTPなどの主要プロトコルに対応しており、サードパーティ製のハードウェアやソフトウェアとのシームレスな統合が可能です
- カスタマイズされたBMSシステムを構築するための二次開発機能（Python SDK、Node-RED、Docker）を提供します
- 複数のVPNトンネルとファイアウォールルールによるセキュアな通信を実現します
- Milesight Development Platformを介して、集中化された簡素なリモートデバイス管理を実現します

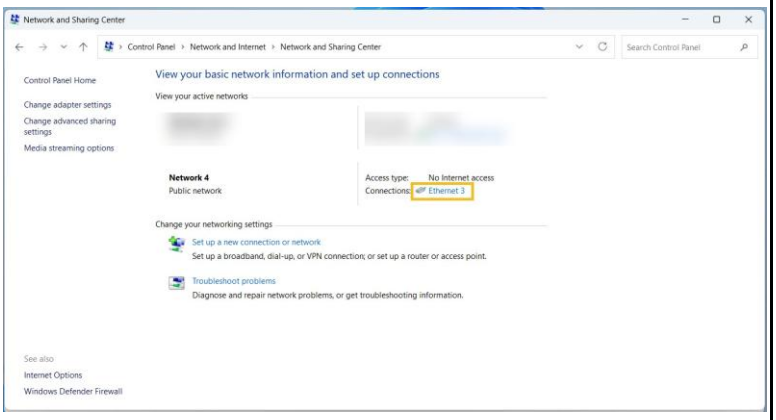
第3章 はじめに

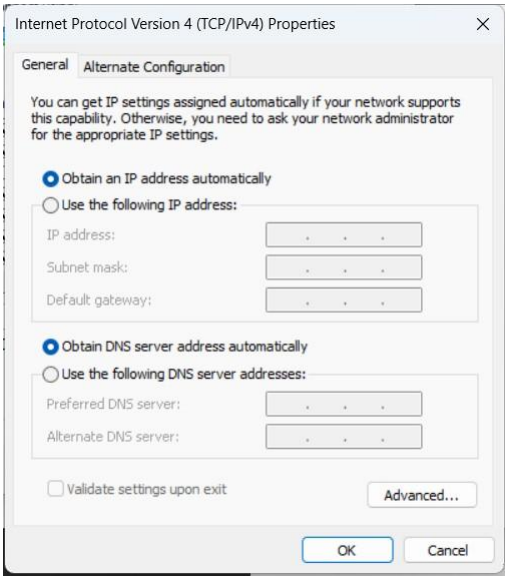
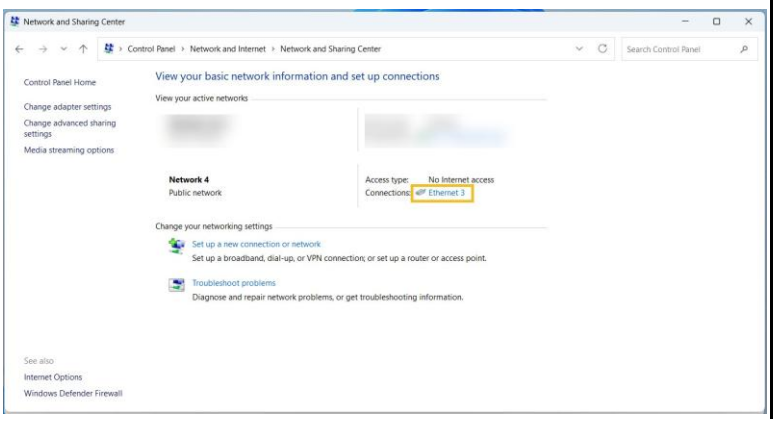
この章では、本ゲートウェイをすぐに使用するための基本的な設定手順について説明します。

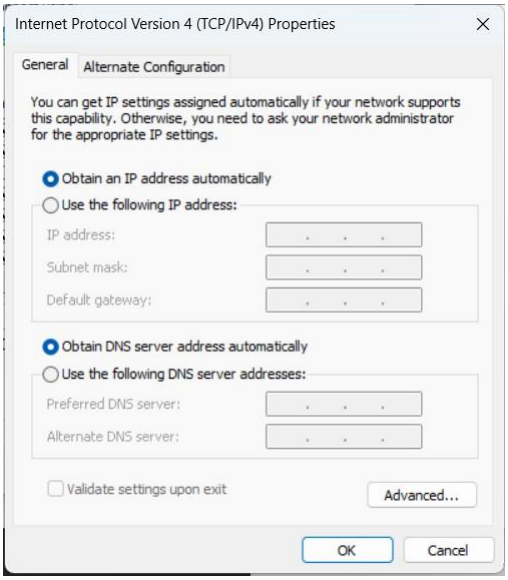
ステップ 1. ゲートウェイの Web GUI にログインする

ゲートウェイには、無線（Wi-Fi）または有線（イーサネットポート）経由でアクセスできます。

1. ゲートウェイに接続してWeb GUIにアクセスするには、以下の方法のいずれかを選択してください。

Method	Step
Access via Wi-Fi	a. お使いのコンピュータでワイヤレスネットワーク接続を有効にし、該当するWi-Fi SSIDを検索して接続してください。デフォルトのWi-Fi認証情報： SSID: **Gateway_XXXXXX**（Wi-Fi MACアドレスの下6桁） パスワード: **iotpassword** ウェブブラウザ（Chromeを推奨）を開き、**https://192.168.2.1** と入力して、Web GUIにアクセスしてください。
Access via a LAN Port	a. ネットワークケーブルを使用して、デバイスの **ETH2** ポートをコンピュータに接続してください。 b. コンピュータのIPアドレスを手動または自動で設定してください。Windows 10を例に挙げます： i. **[ControlPanel] > NetworkandInternet] > [Network andSharingCenter]** の順に移動し、「Ethernet」を選択します（名称が異なる場合があります）。  ii. **> > [ProtocolVersion4 (TCP/IPv4) Properties** に移動し、**[ObtainanIPaddress]** を選択してください

Method	Step
	またはIyUsethefollowingIP、ゲートウェイと同じサブネット内の静的IPアドレスを手動で割り当ててください。  c. Web ブラウザ（Chrome を推奨）を開き、**https://192.168.1.1** と入力して Web GUI にアクセスします。
Access via a WAN Port	a. デバイスの **ETH1** ポートとコンピュータを、DHCP サーバーが有効になっている同じネットワークルーターまたはスイッチに接続します。 b. コンピュータの IP アドレスを自動設定にしてください。Windows 10 を例に挙げます： i. 「**ControlPanel>NetworkandInternet>Network andSharingCenter**」の順に選択し、「Ethernet」を選択してください（名称が異なる場合があります）。 

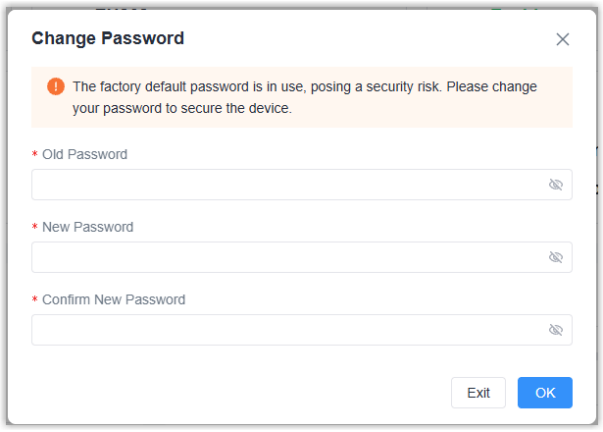
Method	Step
	ii. **[Properties] > [InternetProtocol (TCP/IPv4) 4]** の順に選択し、**[(TCP/IPv4)PropertiesObtainan]** を選択します。  c. 画面に表示されたデバイスの IP アドレスを確認してください。 i. 画面上の任意のボタンを押して、デバイスの画面を起動します。 ii. 「⊞」 ボタンを押して、「Interface Status」メニューに移動します。 iii. 「▶」 ボタンを数回押して、イーサネットステータスページに移動し、ETH1のIPアドレス（**IP**）を確認してください。 d. Webブラウザ（Chromeを推奨）を開き、**https://xx.xx.xx.xx** と入力して Web GUIにアクセスしてください。

2. デフォルトの認証情報を使用してWeb GUIにログインします：

   ユーザー名：**admin**

   パスワード：**password**

3. Web GUIに初めてログインした後、デフォルトのパスワードを変更する必要があります。

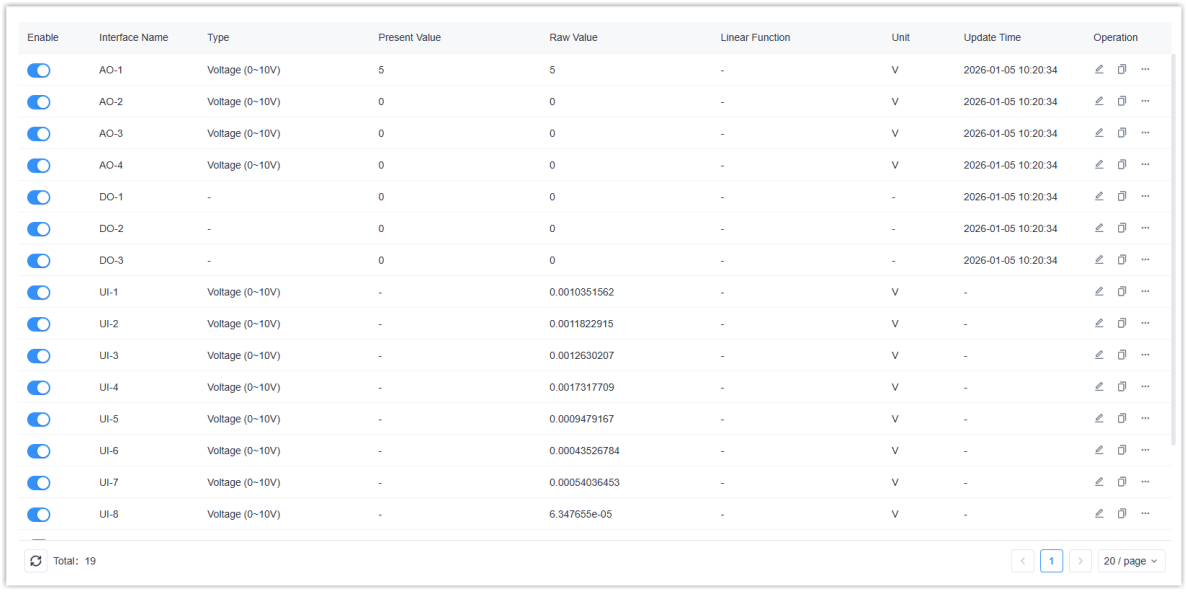


a. 「**Old Password**」を入力してください。
b. **新しいパスワード**を入力してください。パスワードには、少なくとも1文字のアルファベットと1桁の数字を含め、5文字以上31文字以内で入力してください。
c. 「**Confirm New Password**」を入力してください。
d. **[OK]** をクリックしてください。
e. 新しい認証情報を使用して Web GUI にログインします。

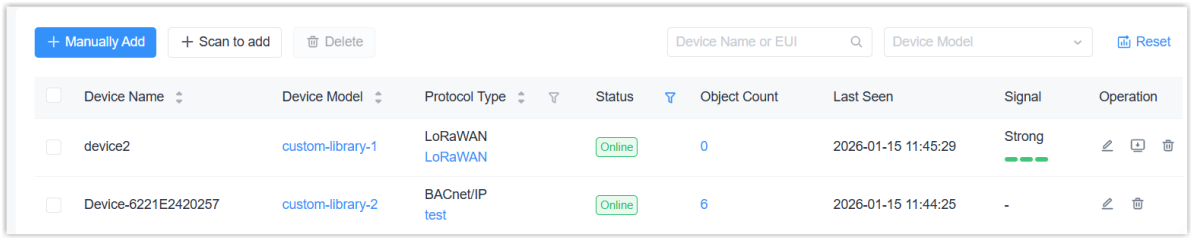
ステップ 2. デバイスの追加

このゲートウェイは、IO インターフェースの有効化やデバイスの追加に対応しています。

IOインターフェースを有効にする：[Data Service] > [Data Acquisition] > [IO Device] ページに移動してIOインターフェースを有効にし、[ ] をクリックして、インターフェースの種類に応じてIOインターフェースのパラメータを設定してください。詳細については、「IO Device」を参照してください。



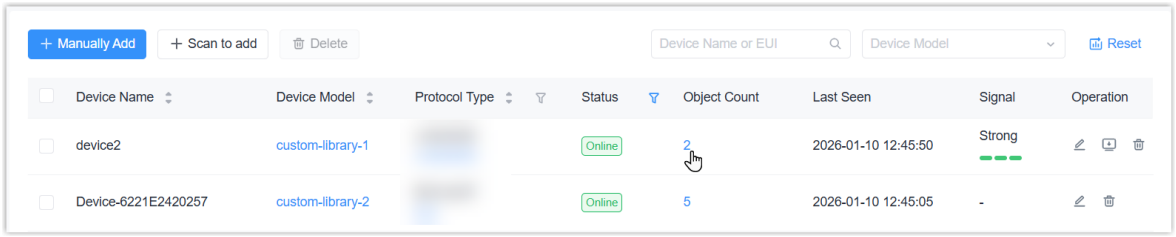
デバイスの追加：[Data Service] > [Data Acquisition] > [Device] ページに移動し、プロトコル種別ごとにデバイスを追加します。詳細については、「Add a Device」を参照してください。



ステップ 3. デバイスオブジェクトの追加

読み取りまたは書き込み動作を行うには、デバイスオブジェクトを追加する必要があります。

1. 「**Data Service**」>「**Data Acquisition**」>「**Device**」ページに移動し、オブジェクト数の値をクリックして「オブジェクト一覧」ページに移動します。

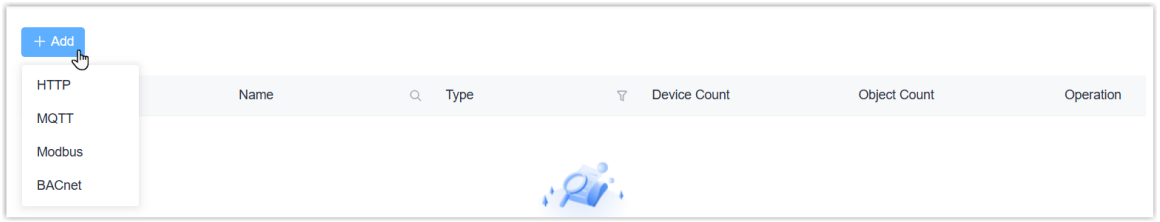


2. デバイスオブジェクトを追加し、必要なオブジェクトを有効にしてください。詳細については、「デバイスオブジェクトの追加」および「デバイスオブジェクトの有効化」を参照してください。

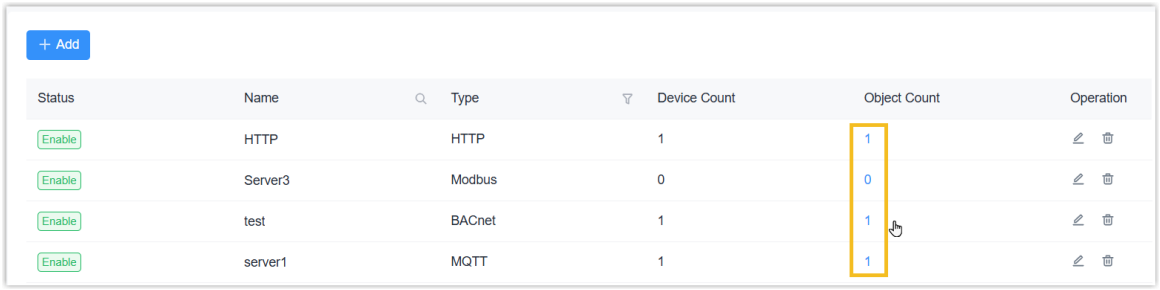
ステップ 4. データ転送先を追加する

データを転送したり、リモート制御を実装したりする必要がある場合は、データ転送ルールを追加する必要があります。

1. 「**Data Service**」>「**Data Forwarding**」ページに移動し、データ転送ルールを追加してください。詳細については、「データ転送ルールの追加」を参照してください。



2. 「**Data Service**」>「**Data Forwarding**」ページに移動し、オブジェクト数の値をクリックして「オブジェクト一覧」ページを開き、転送内容を追加してください。詳細については、「データ転送オブジェクトの追加」を参照してください。

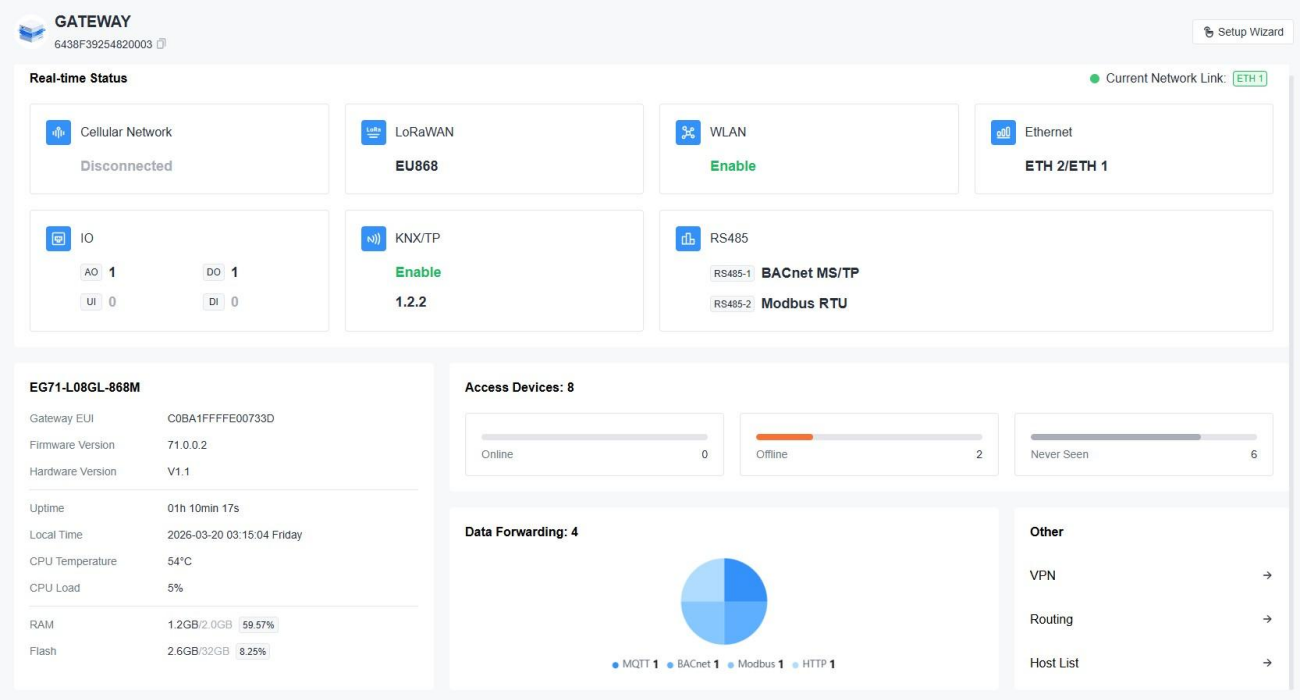


第4章 ステータス

「Status」ページには、デバイスの基本情報と動作状況が表示されます。

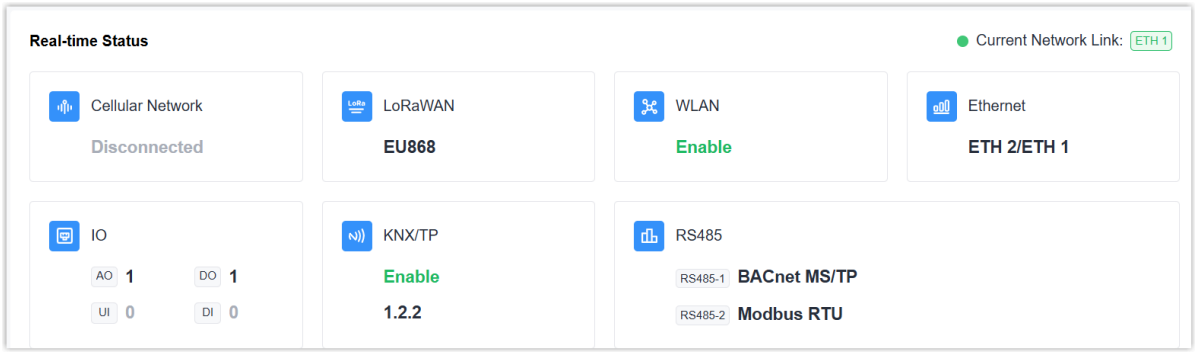
概要

ページの上部には、ホスト名、シリアル番号、およびウィザードポータルが表示されます。詳細については、図中のウィジェットをクリックしてください。



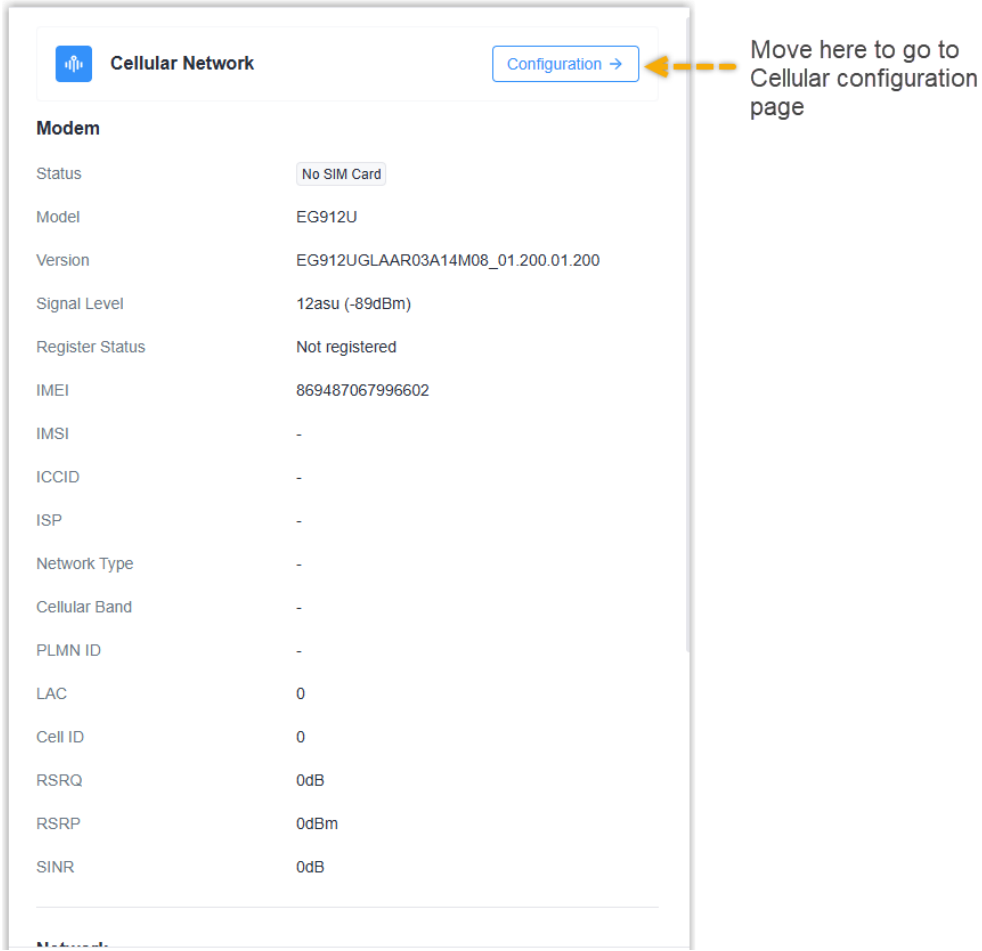
1. リアルタイムステータス
2. 基本情報
3. デバイスへのアクセス
4. データ転送
5. その他

リアルタイムステータス



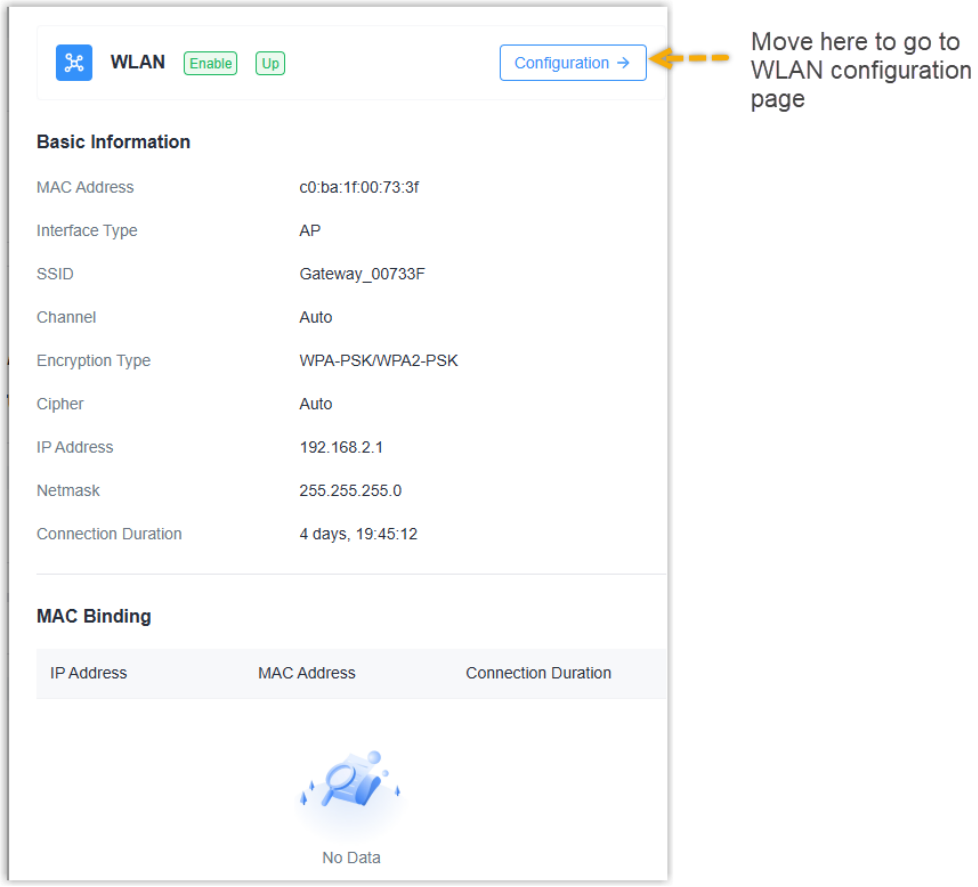
このウィジェットは現在のネットワーク接続状況を表示し、各インターフェースの状態を表示する7つの小さなウィジェットが含まれています。各ウィジェットをクリックすると、状態の詳細を確認できます。

モバイルネットワーク：モバイルモジュールの状態、ネットワーク登録状況、および月間のモバイルデータ使用量を表示します。

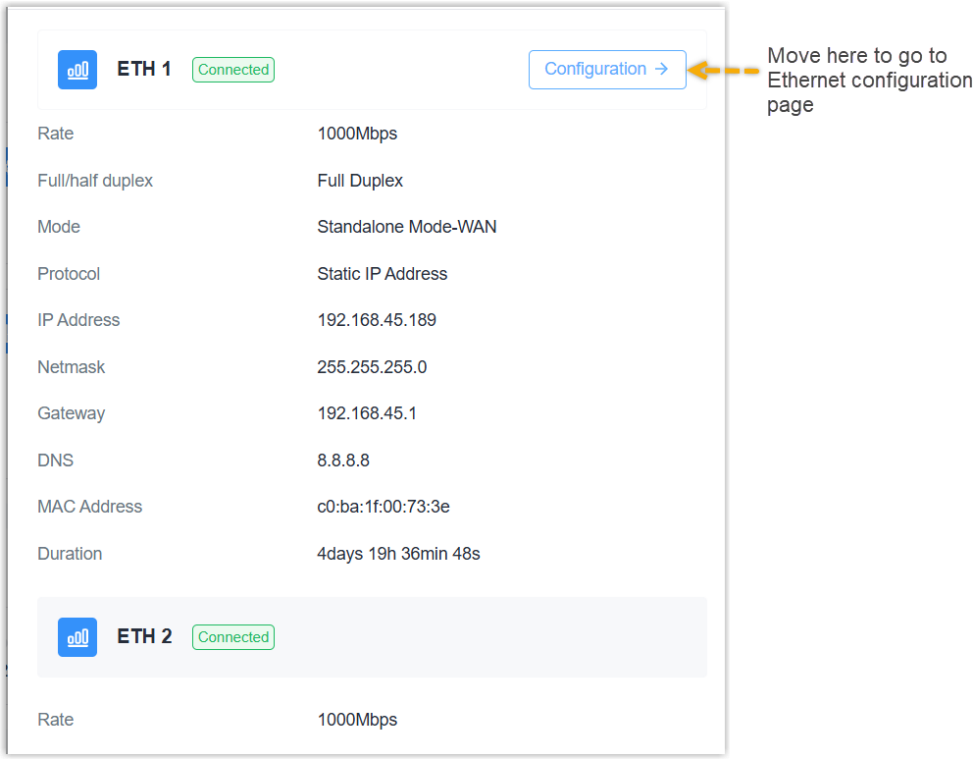


LoRaWAN：チャネルプラン、周波数、および追加されたLoRaWAN®デバイスの数を表示します。

WLAN : WLANの有効状態、接続状態 （接続中／切断中）、および各モードに関する情報を表示します。



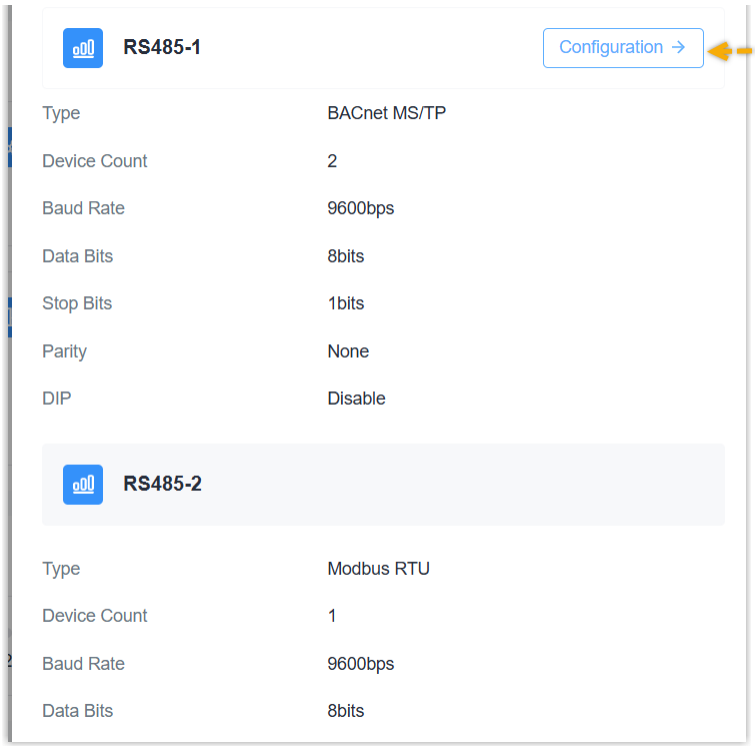
Ethernet : 各イーサネットポートの接続状況と情報を表示します。



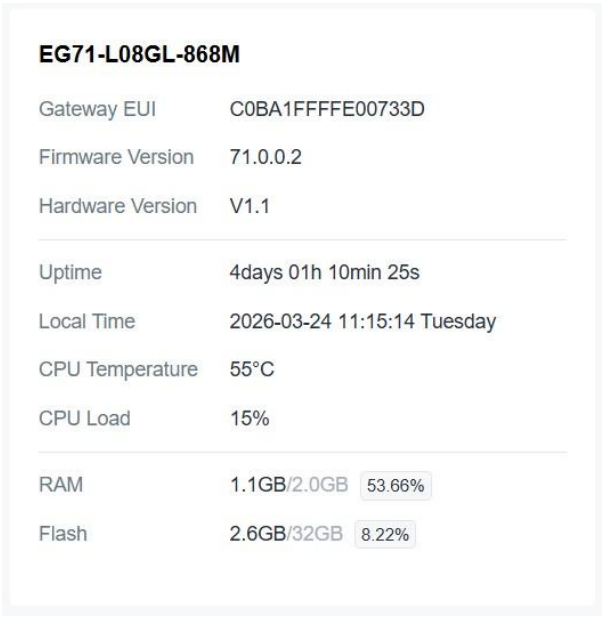
IO：有効になっているIOインターフェースの数、その種類、および現在の値を表示します。

KNX/TP：このインターフェースの物理アドレスと、追加されたKNX/TPデバイスの数を表示します。

RS485：各 RS485 インターフェースの設定および使用されているプロトコルタイプを表示します。

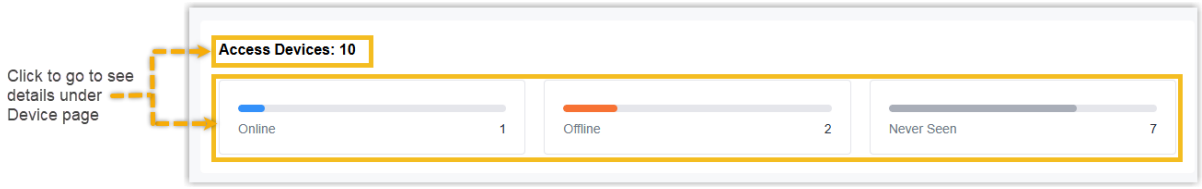


基本情報



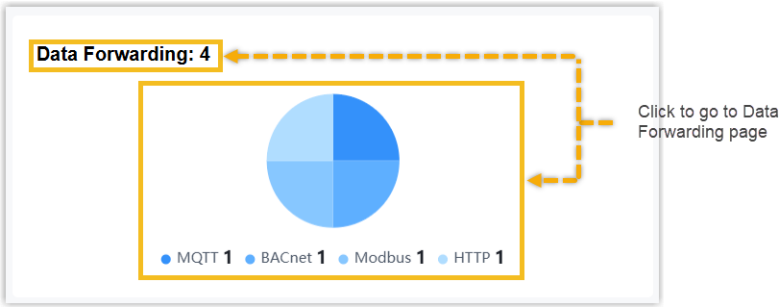
このウィジェットには、基本情報、動作状況、およびストレージの状態が表示されます。

デバイスへのアクセス



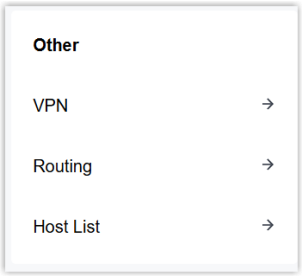
このウィジェットには、追加されたデバイスの総数に加え、各ステータスにあるデバイスの数と割合が表示されます。

データ転送



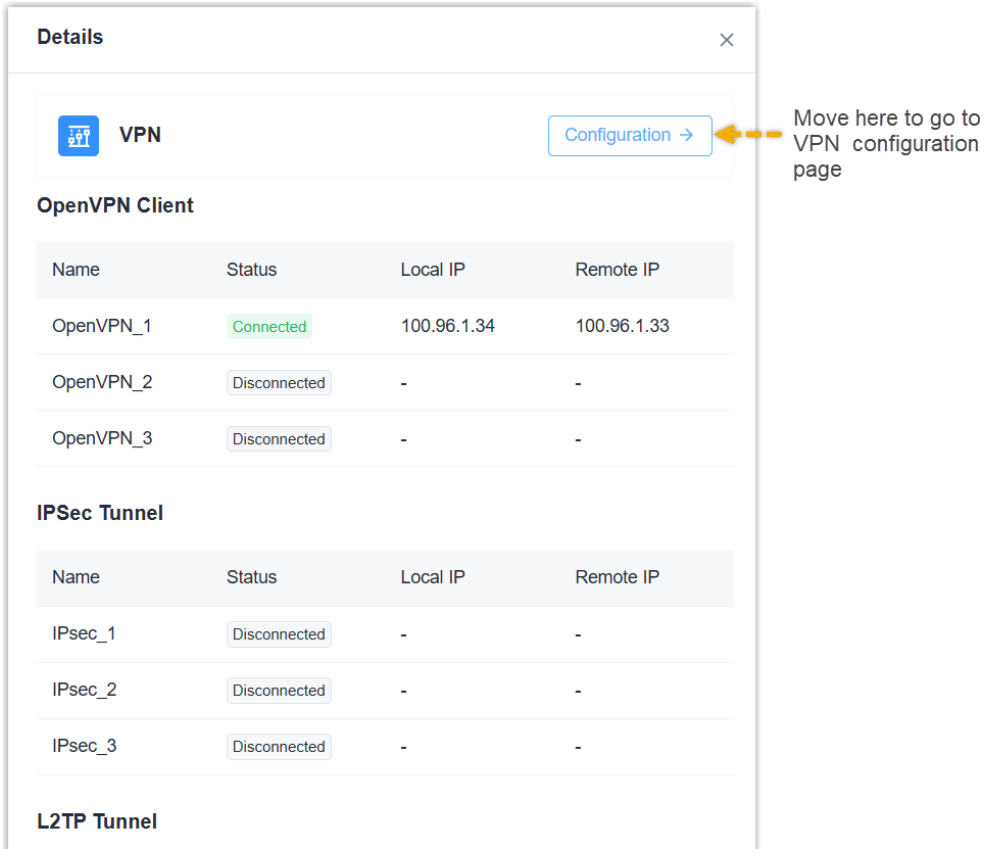
このウィジェットには、追加されたデータ転送ルールの総数に加え、プロトコル種別ごとのルール数と割合が表示されます。

その他

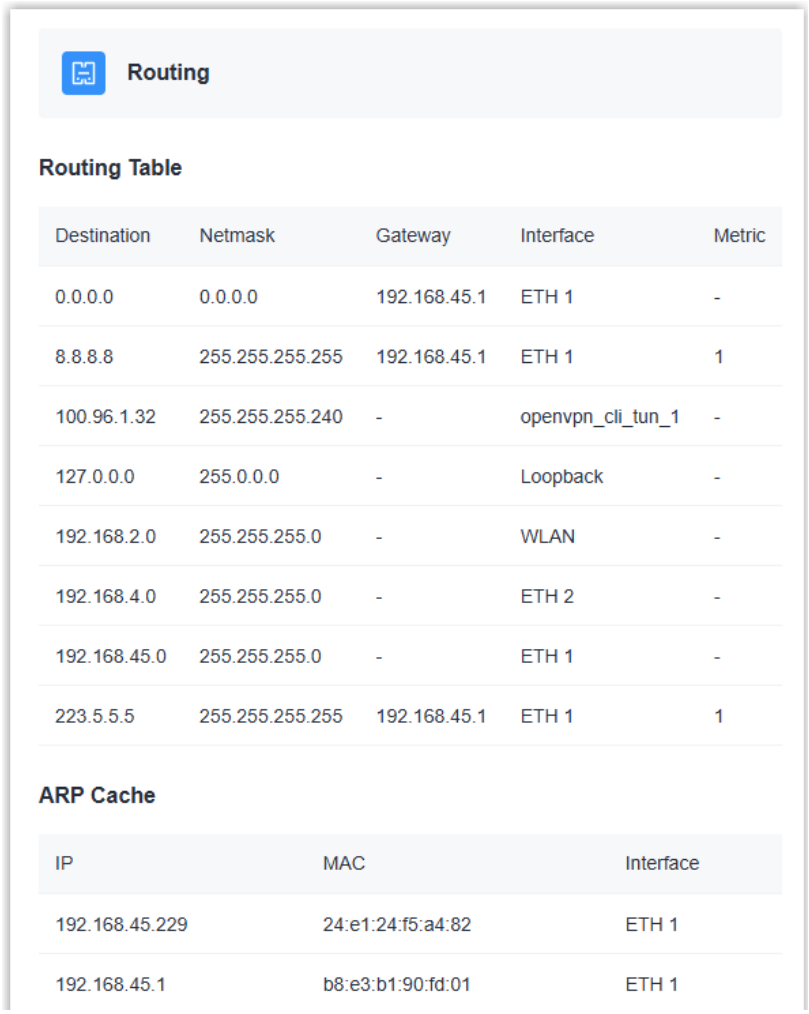


このウィジェットには、次の3つのメニューが表示されます：

VPN：OpenVPNクライアント、IPsecトンネル、L2TPトンネル、およびPPTPトンネルの接続状態を表示します。



Routing：ルーティングテーブルとARPキャッシュを表示します。



Routing

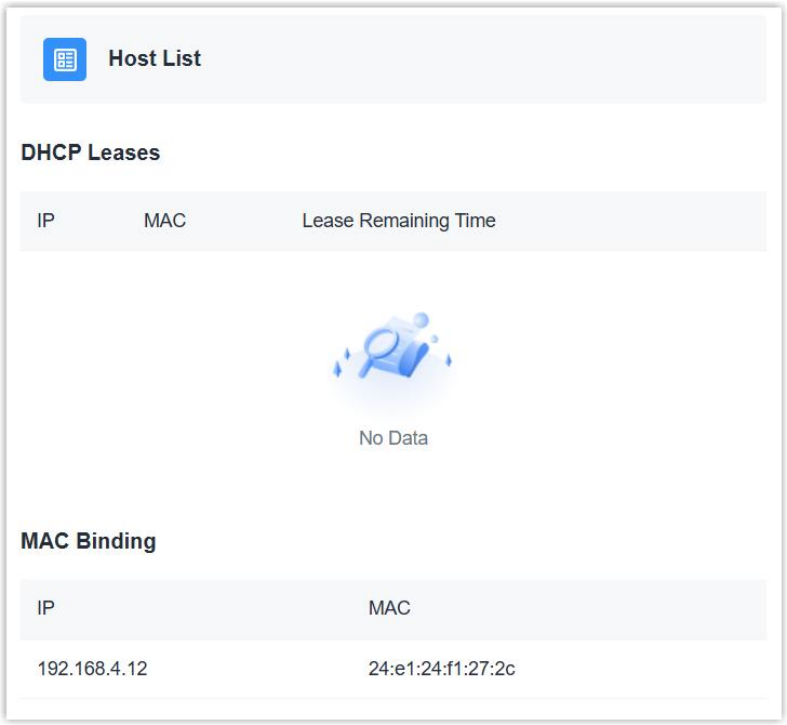
Routing Table

Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.45.1	ETH 1	-
8.8.8.8	255.255.255.255	192.168.45.1	ETH 1	1
100.96.1.32	255.255.255.240	-	openvpn_cli_tun_1	-
127.0.0.0	255.0.0.0	-	Loopback	-
192.168.2.0	255.255.255.0	-	WLAN	-
192.168.4.0	255.255.255.0	-	ETH 2	-
192.168.45.0	255.255.255.0	-	ETH 1	-
223.5.5.5	255.255.255.255	192.168.45.1	ETH 1	1

ARP Cache

IP	MAC	Interface
192.168.45.229	24:e1:24:f5:a4:82	ETH 1
192.168.45.1	b8:e3:b1:90:fd:01	ETH 1

Host Leases：DHCP サーバーの DHCP リース一覧と MAC バインディング一覧を表示します。


Host List
DHCP Leases
IP
MAC
Lease Remaining Time
No Data
MAC Binding
IP
MAC
192.168.4.12
24:e1:24:f1:27:2c

第5章 データサービス

データ取得

デバイス

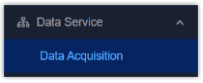
この章では、デバイスの追加および管理方法について説明します。

デバイスの追加

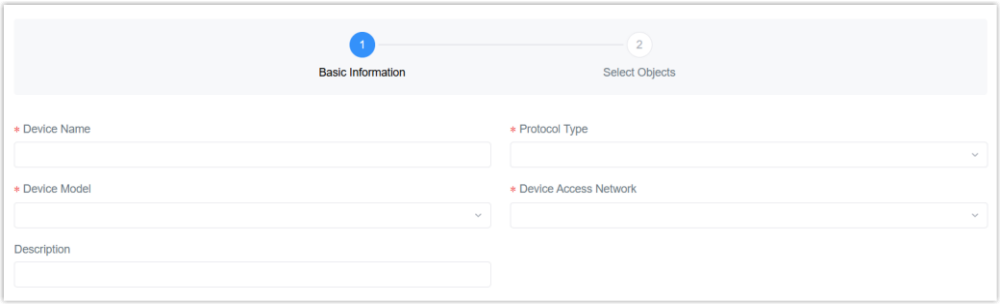
ゲートウェイは、さまざまな方法に対応し、最大2000台のデバイスを追加できます。デバイスを追加するには、いずれかの方法を選択してください。

デバイスの手動追加

1. 左側のバーで、「**Data Service**」＞「**Data Acquisition**」ページを選択してください。



2. 上部のバーで、「**Device**」タブを選択します。
3. 「**+Manually Add**」をクリックして、新しいデバイスを追加します。
4. デバイスの基本情報を設定します。



Parameter	説明
Device Name	デバイスに固有の名前を定義します。
Protocol Type	端末機器に応じて、プロトコルタイプを選択してください：LoRaWAN、BACnet/IP、BACnet MS/TP、Modbus RTU、Modbus TCP、Modbus RTU over TCP、KNX/TP。
Device Model	デバイスライブラリからデバイスモデルを選択してください。デバイスに互換性のあるモデルがない場合、またはカスタム設定が必要な場合は、**None**を選択してください。

Parameter	説明
	Tip： デバイスモデルが選択されている場合のみ、次のステップでデバイスがオブジェクトを選択できます。
Device Access Network	「デバイスアクセスネットワーク」から追加されたデバイスアクセスネットワークを選択してください。
Description	このデバイスを記録するためです。
Protocol Type is LoRaWAN	
Device EUI	デバイスの固有の 16 桁の 16 進数 EUI です。
Device-Profile	「デバイスプロファイル」から追加したデバイスプロファイルを選択してください。 **注：** デバイスタイプがクラスBの場合は、クラスB設定が有効になっていることを確認してください。
fPort	fPort（フレームポート）は、MACペイロード内の1バイトフィールドであり、データのタイプまたは宛先を識別するものです。これは、エンドデバイス上の異なるサービスやアプリケーションに対するポート番号のように機能します。
Modbus RTU Data Transmission	以下のいずれかを選択してください：無効、Modbus RTU to TCP、Modbus RTU over TCP。これはMilesight LoRaWAN®コントローラ（UC501/UC300など）にのみ適用されます。**Modbus RTU to TCP**：TCPクライアントは、Modbus TCPコマンドを送信して、コントローラからModbusデータを要求することができます。 **Modbus RTU over TCP**：TCPクライアントは、Modbus RTUコマンドを送信して、コントローラからModbusデータを要求できます。
Application Key	接続タイプがOTAAの場合、32桁の16進数のAppKey値を設定してください。 Milesightデバイスでは、ユーザーは「Default」を選択してMilesightのデフォルトAppKeyを使用するか、「Custom」を選択してAppKeyをカスタマイズすることができます。

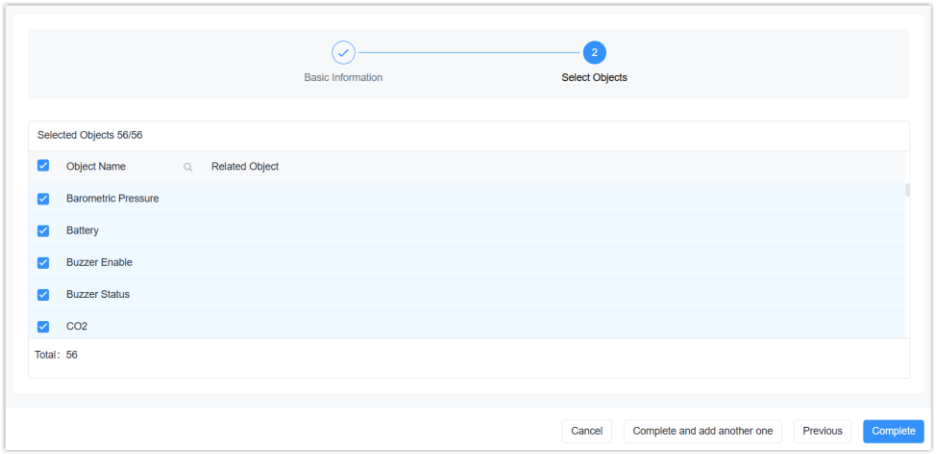
Parameter	説明
Device Address	参加タイプが ABP の場合、8 桁の 16 進数の DevAddr を設定します。
Application Session Key	結合タイプがABPの場合、32桁の16進数であるNwkSKeyの値を設定してください。
Network Session Key	参加タイプが ABP の場合、32 桁の英数字の AppSKey 値を設定してください。
Uplink Frame-counter	結合タイプがABPの場合、アップリンクのフレームカウンタを設定してください。
Downlink Frame-counter	参加タイプが ABP の場合、ダウンリンクのフレームカウンタを設定します。
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
Frame-counter Validation	リプレイ攻撃を防ぐために、この機能を有効にしてください。
Protocol Type is BACnet/IP or BACnet MS/TP	
Device Instance Nr	BACnet ネットワーク内でのデバイスの一意の識別子を設定します。
Protocol Type is Modbus TCP or Modbus RTU over TCP	
IP Address	Modbus サーバー（スレーブ）デバイスの IP アドレスを設定します。
Server ID	Modbus デバイスのベンダーから提供された一意のサーバー ID（スレーブ ID）を設定します。
Port	Modbus サーバー（スレーブ）デバイスのポートを設定します。
Protocol Type is Modbus RTU	
Server ID	Modbus RTU デバイスベンダーから提供された一意のサーバー ID（スレーブ ID）を設定してください。
Protocol Type is KNX/TP	
Physical Address	KNX バスネットワーク内でのデバイスの固有の物理アドレスを設定してください。

5. 「**Next Step**」をクリックして、このデバイスに割り当てるオブジェクトを選択してください。

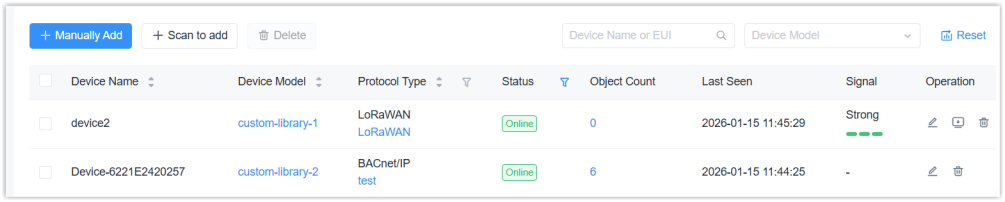
デバイスモデルが選択されていない場合、選択可能なオブジェクトは存在せず、デバイスは自動的に作成されます。

前の手順でデバイスモデルを選択した場合は、そのデバイスに追加する必要なオブジェクトを選択してください。

a. 「**Finished**」をクリックしてデバイスの追加を終了するか、「**Finished**」をクリックして**別のデバイスを追加し**、新しいデバイスを追加してください。



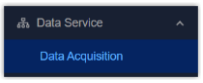
6. 追加後、デバイス一覧でデバイスのステータスを確認してください。



デバイスがまだオンラインになっていない場合は、「**Data Service**」>「**Data Stream**」ページに移動し、デバイスとゲートウェイ間の通信を確認してください。

スキャンによる BACnet デバイスの追加

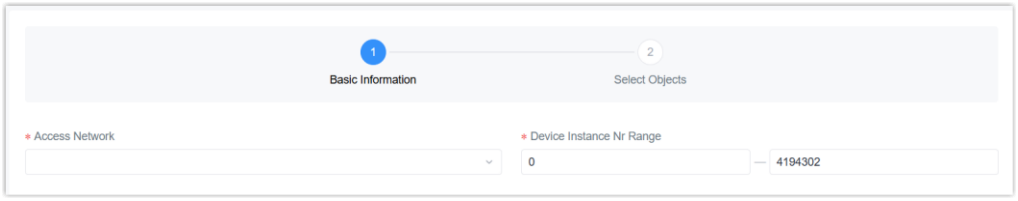
1. 左側のバーで、「**Data Service**」>「**Data Acquisition**」ページを選択してください。



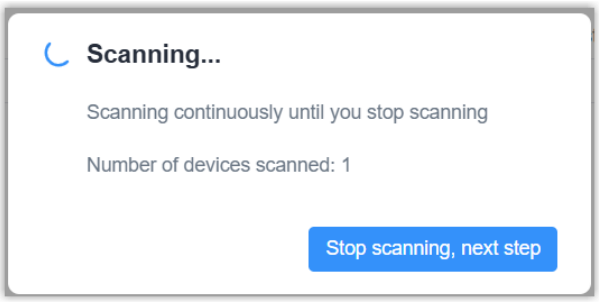
2. 上部のバーで、「**Device**」タブを選択します。
3. 「**+Scan to Add**」をクリックして新しいデバイスを追加し、「**Scan BACnet/IP**」または「**Scan BACnet MS/TP**」を選択してください。
4. アクセスネットワークを選択し、スキャンするデバイスのインスタンス番号の範囲を設定してください。

注：

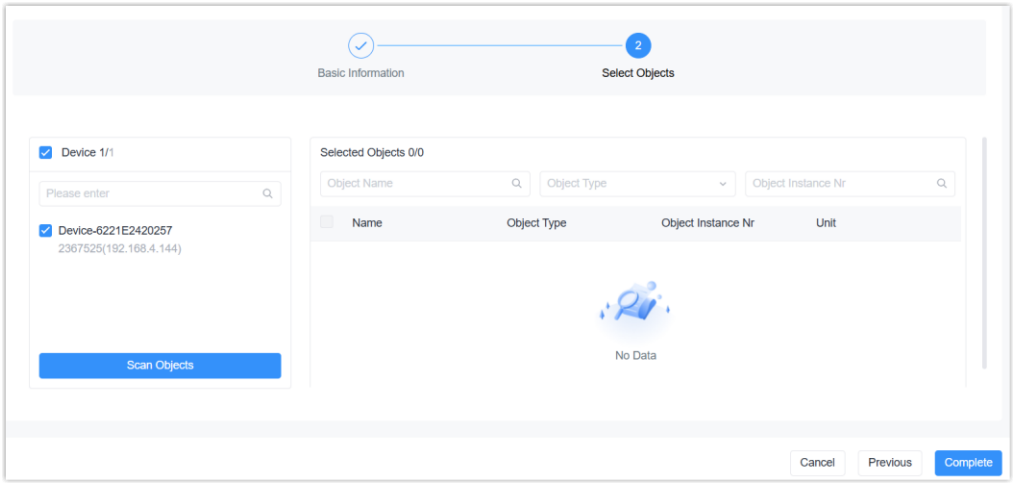
このアクセスネットワークの物理インターフェースまたはネットワークインターフェースが、BACnetデバイスに到達できることを確認してください。



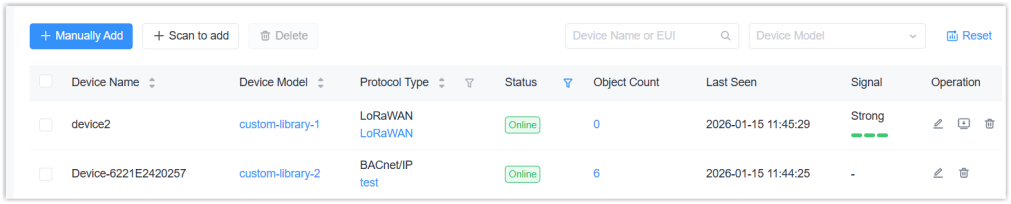
5. **[Next Step]** をクリックして、ネットワーク内の到達可能な BACnet デバイスのスキャンを開始します。
6. スキャン可能なデバイスがある場合は、「**Stop scanning**」をクリックし、**次の手順に進んでください**。



7. デバイス一覧からデバイスを選択し、「**Finished**」をクリックして追加を完了するか、「**Scan Objects**」をクリックして、そのデバイス用のオブジェクトを検索して追加してください。



8. 追加後、デバイス一覧でデバイスのステータスを確認してください。



デバイスがまだオンラインになっていない場合は、「**Data Service**」＞「**Data Stream**」ページに移動し、デバイスとゲートウェイ間の通信を確認してください。

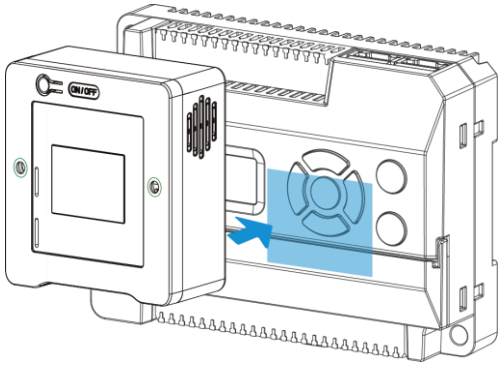
NFC による Milesight LoRaWAN® デバイスの追加 前提条

件：

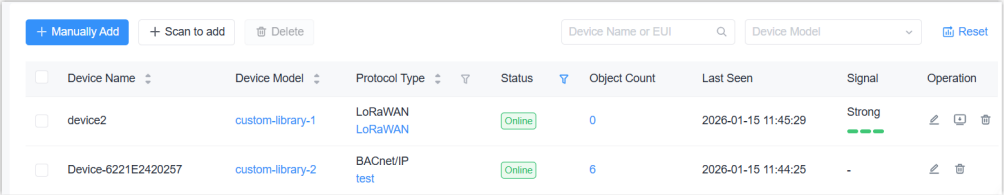
- エンドデバイスがNFC設定に対応していること。
- エンドデバイスとゲートウェイが、同じ LoRaWAN® チャネルプランに対応していること。

手順：

1. 端末の電源を入れてください。
2. ゲートウェイの画面上の任意のボタンを押して、ゲートウェイの画面を表示してください。
3. 端末のNFCエリアをゲートウェイに数秒間かざしてください。画面に追加の進行状況が表示されます。追加に成功すると、デバイス一覧にそのデバイスが表示されます。



4. 追加されたデバイスの「 」をクリックして、デバイスモデルを選択してください。
5. 追加後、デバイス一覧でデバイスのステータスを確認してください。



デバイスがまだオンラインになっていない場合は、**Data Service > Data Stream**ページに移動し、デバイスとゲートウェイ間の通信を確認してください。

デバイスオブジェクトの追加

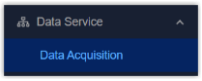
各デバイスでは、読み取りまたは書き込み動作を行うためのオブジェクトの追加に対応しています。通常、オブジェクトはデバイスを追加する際に追加できます。この手順をスキップした場合は、以下の手順に従って、そのデバイス用のオブジェクトを追加してください。

デバイスライブラリからオブジェクトを追加する

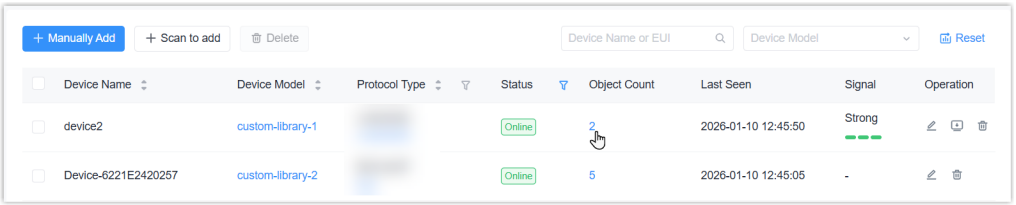
前提条件：デバイスに対してデバイスモデルが選択されていること。

手順：

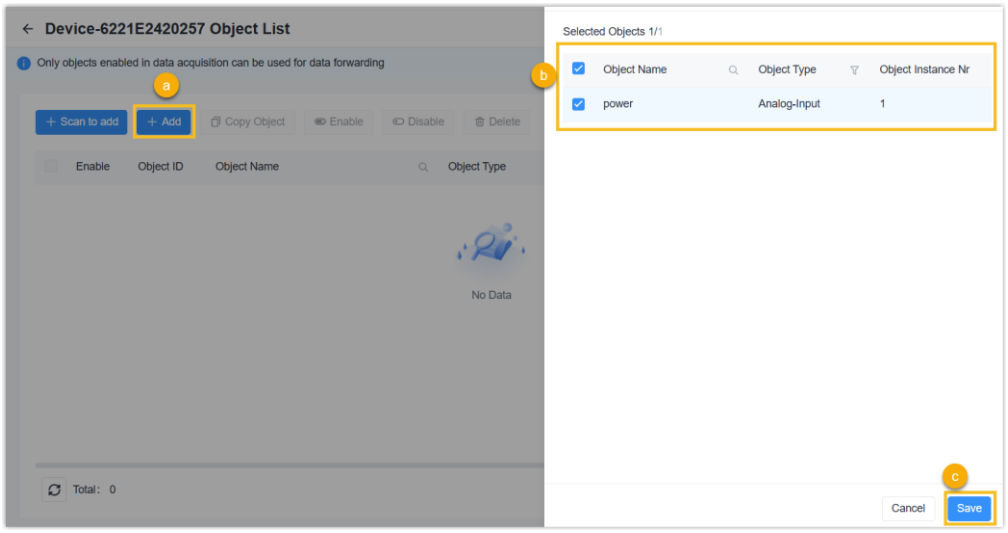
1. 左側のバーで、**Data Service > Data Acquisition**ページを選択してください。



2. 上部のバーで、「**Device**」タブを選択します。
3. 目的のデバイスを選択し、オブジェクト数の値をクリックして「オブジェクトリスト」ページに移動します。



4. 「**+Add**」をクリックし、「**Device Library**」を選択します。
5. ポップアップリストからオブジェクトを選択し、「**Save**」をクリックします。



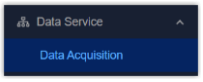
6. オブジェクトリストで「 」の編集をクリックし、必要に応じてオブジェクトのパラメータ（収集間隔、線形関数など）を設定してください。

オブジェクトを手動で追加する

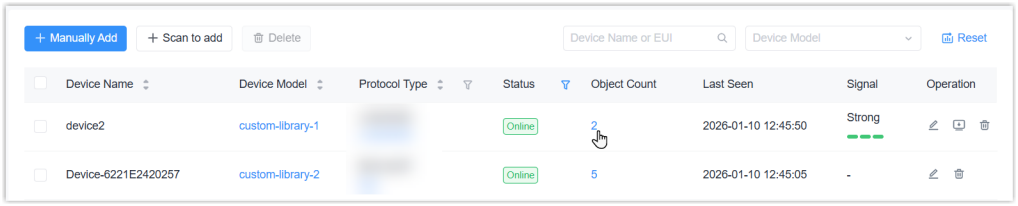
カスタムオブジェクトを追加する必要がある場合は、以下の手順に従ってください。

> **注：**
> LoRaWAN® デバイスはこの機能に対応していません。

1. 左側のバーで、「**Data Service**」>「**Data Acquisition**」ページを選択してください。



2. 上部バーで、「**Device**」タブを選択します。
3. 目的のデバイスを選択し、オブジェクト数の値をクリックして「オブジェクト一覧」ページに移動します。



4. 「**+Add**」をクリックし、「**Custom Objects**」を選択します。
5. プロトコルの種類に応じて、オブジェクト情報を設定してください。

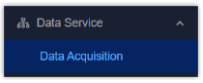
Parameter	説明
Object Name	このオブジェクトに一意の名前を定義します。
Object Description	このオブジェクトに関する注記用です。
BACnet/IP or BACnet MS/TP	
Object Type	BACnet オブジェクトタイプを選択してください。
Object Instance Nr	一意のオブジェクトインスタンス番号を設定します。
Collection Interval	オブジェクトデータを収集する間隔です。範囲：1～86400秒。
Unit	オブジェクトタイプがアナログタイプの場合、値の単位を選択します。
Linear Function	有効にすると、収集された値は表示される前に関数式に代入されます。 式：y=a*x+b（y：現在の値、x：生データ/実際の収集値）
COV Sub scription	この機能を有効にすると、アナログ型の値が変化した際にゲートウェイから通知が送信されます。
Modbus RTU/TCP or Modbus RTU over TCP	
Register Type	Modbus レジスタタイプを選択してください。 **Discrete Input**：オン/オフの値を読み取ります。**Coil**：オン/オフの値を読み書きします。**Input Register**：測定値とステータスを読み取ります。**Holding Register**：設定値を読み書きします。
Data Format	レジスタタイプが「入力レジスタ」または「保持レジスタ」の場合、データタイプを選択します。
Register Address	レジスタ内のこのオブジェクトの値を読み書きするための開始アドレスを設定します。
Register Quantity	データ形式に基づいて数量を表示します。

Parameter	説明
Collection Interval	オブジェクトデータを収集する間隔です。範囲：1～86400秒。
Unit	レジスタタイプが「入力レジスタ」または「ホールドレジスタ」の場合、この値の単位を選択します。
Linear Function	有効にすると、収集された値は表示される前に関数の式に代入されます。式：`y=a*x+b`（y：現在値、x：生データ／実際の収集値）
KNX	
Group Address	このオブジェクトのグループアドレスを定義します。
Datapoint Type	値を定義するために、KNX データポイントタイプ (DPT) を選択してください。タイプが 「カスタム」 の場合は、データ長を定義する必要があります。
Access Mode	このオブジェクトのアクセスモードを選択してください。
Collection Interval	オブジェクトデータを収集する間隔です。範囲：300～86400秒。
Unit	データポイントの種類を選択した後、データ単位が表示されます。

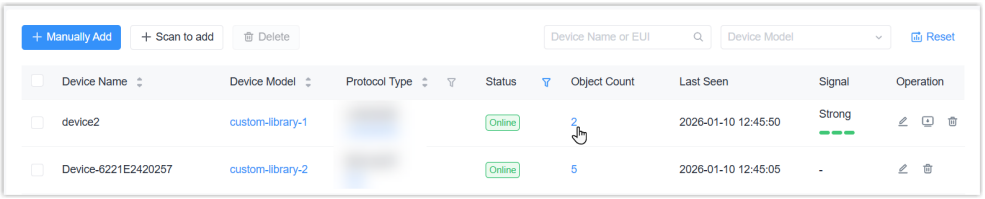
6. **[Save]** をクリックして設定を保存します。

スキャンによるBACnetオブジェクトの追加

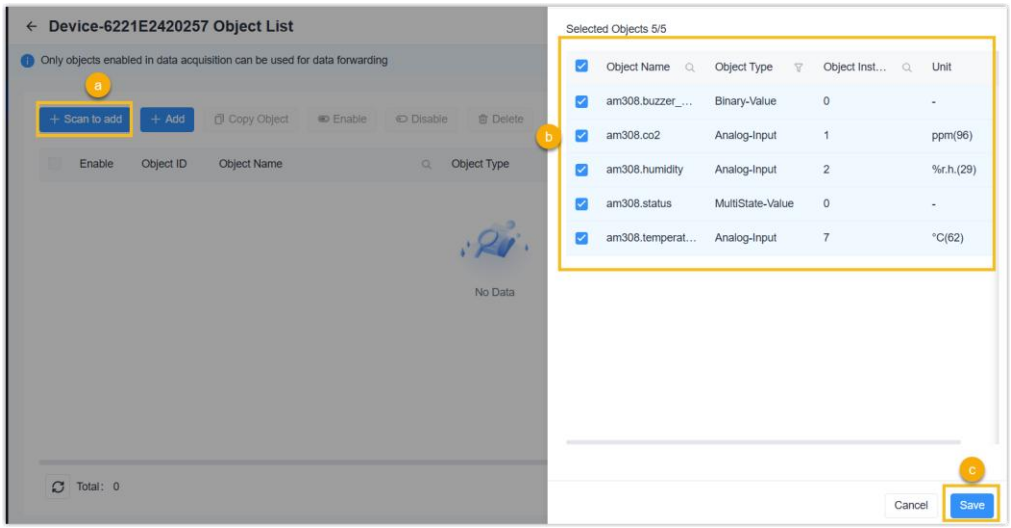
1. 左側のバーで、「**Data Service**」＞「**Data Acquisition**」ページを選択してください。



2. 上部のバーで、「**Device**」タブを選択します。
3. 目的のデバイスを選択し、オブジェクト数の値をクリックして「オブジェクトリスト」ページに移動します。



4. 「**+Scan to add**」をクリックして、このBACnetデバイスのオブジェクトのスキャン対象に**追加**します。
5. ポップアップリストから目的のオブジェクトを選択し、「**Save**」をクリックしてください。

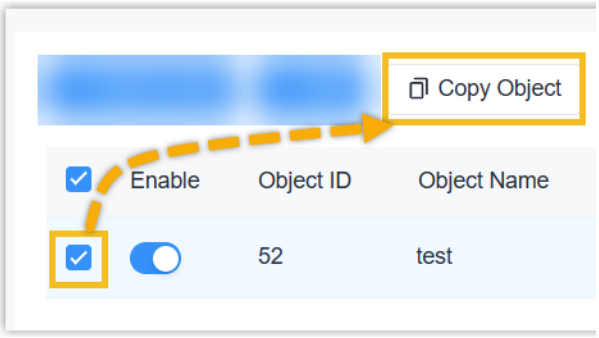


コピーによるオブジェクトの追加

同じモデルのデバイスを複数追加する場合は、以下の手順に従ってコピーしてオブジェクトを追加してください。

> **注：**
> KNXデバイスはこの機能に対応していません。

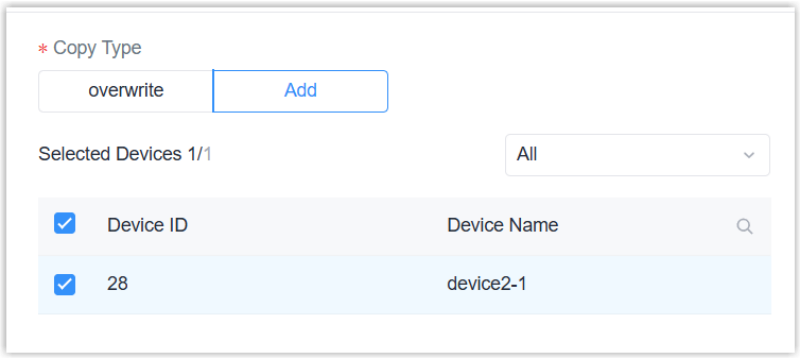
1. 上記の手順に従って、いずれかのデバイスにオブジェクトを追加してください。
2. デバイス一覧からオブジェクトが追加されたデバイスを選択し、オブジェクト数の値をクリックして「オブジェクト一覧」ページに移動してください。
3. 対象のオブジェクトのチェックボックスを選択し、「**Copy Object**」をクリックしてください。



4. ポップアップウィンドウで、コピータイプとデバイスを選択してください。

上書き：選択したデバイスのオブジェクトが上書きされます。

追加：選択したデバイスのオブジェクトは上書きされません。

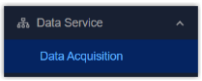


5. **[Save]** をクリックして、オブジェクトを選択したデバイスにコピーします。

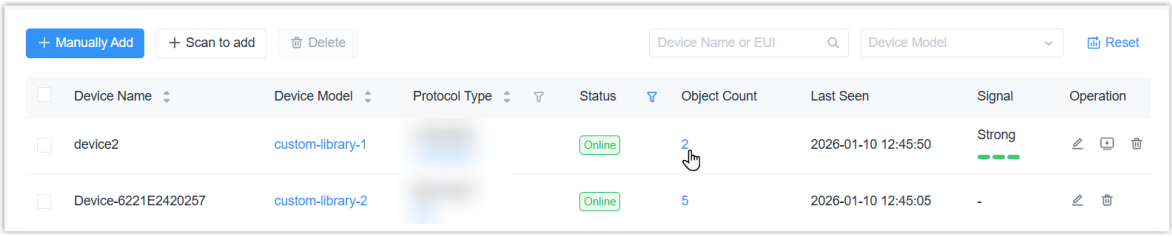
オブジェクトの有効化または無効化

デバイスにオブジェクトを追加した後、必要に応じてそのオブジェクトを有効または無効にすることができます。

1. 左側のバーで、「**Data Service**」＞「**Data Acquisition**」ページを選択します。

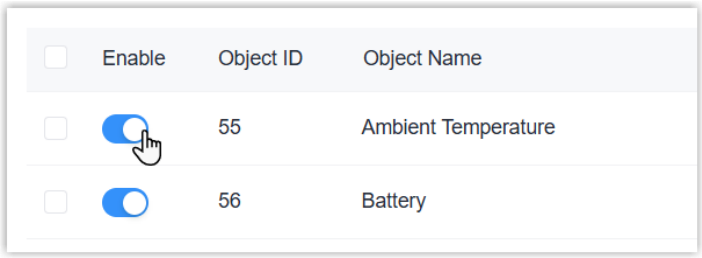


2. 上部のバーで、「**Device**」タブを選択します。
3. 目的のデバイスを選択し、オブジェクト数の値をクリックして「オブジェクト一覧」ページに移動します。



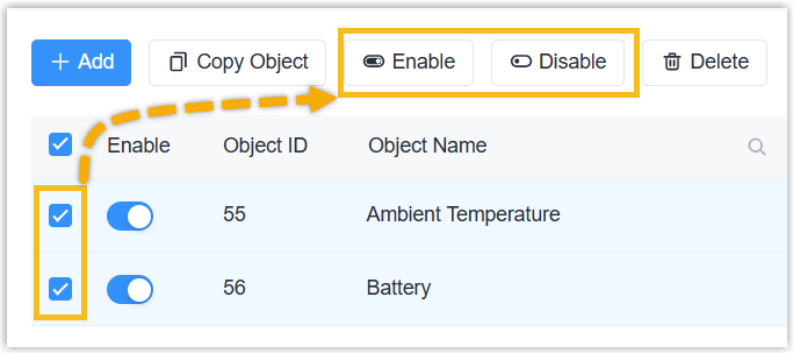
4. オブジェクトを有効または無効にします。有効にすると、そのオブジェクトを使用してデータの転送や読み取り/書き込み動作を行うことができます。

   単一のオブジェクトを有効または無効にする：対象のオブジェクトの **[Enable]** ボタンをタップします。



オブジェクトを一括で有効または無効にするには: 対象のオブジェクトのチェックボックスを選択し、「**Enable**」または

Disable」ボタンをクリックしてください。



デバイスの読み取り/書き込み

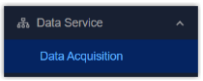
ゲートウェイは、デバイスデータの読み取りや、デバイスへの直接的なコマンド送信に対応しています。

前提条件：

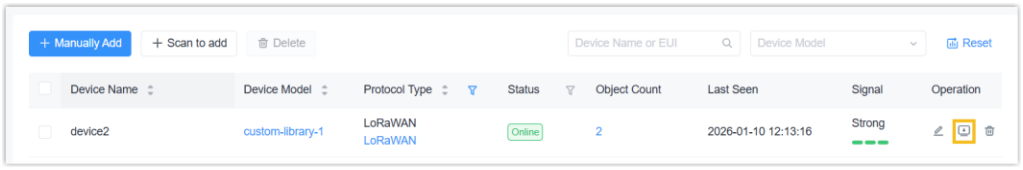
- デバイスがオンライン状態であること。
- 対象のデバイスオブジェクトが書き込み可能であること。
- LoRaWAN® デバイスがクラス B タイプの場合は、クラス B 設定が有効になっていることを確認してください。

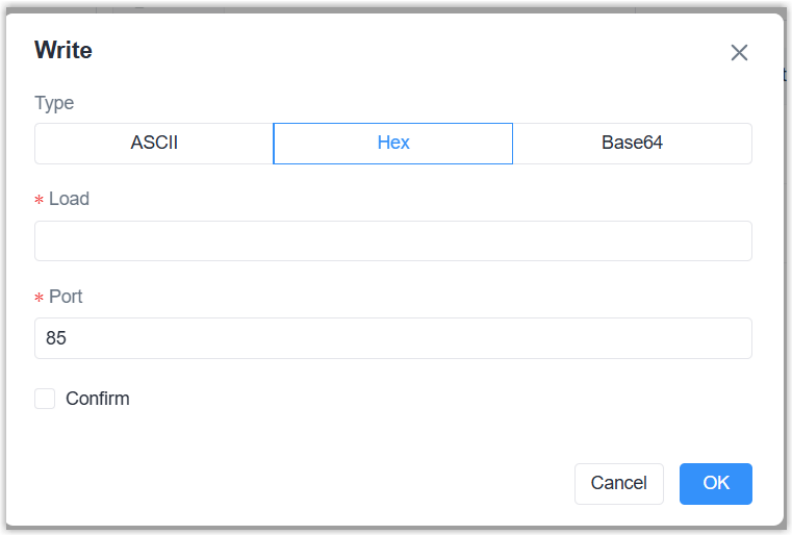
LoRaWAN® デバイスへのコマンド送信

1. 左側のバーで、**[Data Service] > [Data Acquisition]** ページを選択します。



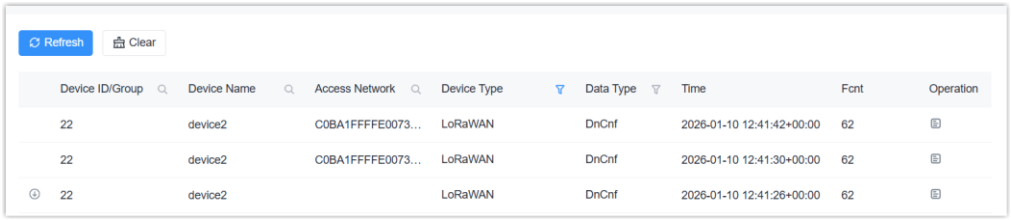
2. 上部のバーで、**[Device]** タブを選択します。
3. 目的のデバイスを選択し、[ ] をクリックしてダウンリンクペイロードを設定します。





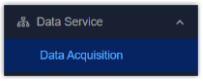
Parameter	説明
Type	ダウンリンクペイロードのタイプを選択します。
Load	対応するタイプに基づいて、ダウンリンクペイロードを定義します。
Port	このデバイスのアプリケーションポートを定義します。
Confirm	このダウンリンクペイロードを受信した後、デバイスが応答するように有効にするか、無効にします。

4. **[OK]** をクリックして、ダウンリンクペイロードを送信します。
5. 「**Data Service**」＞「**Data Stream**」に移動し、ダウンリンクの送信状況を確認してください。

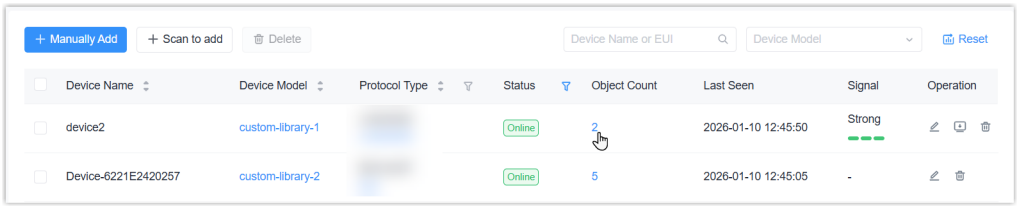


その他のデバイスの読み取り/書き込み

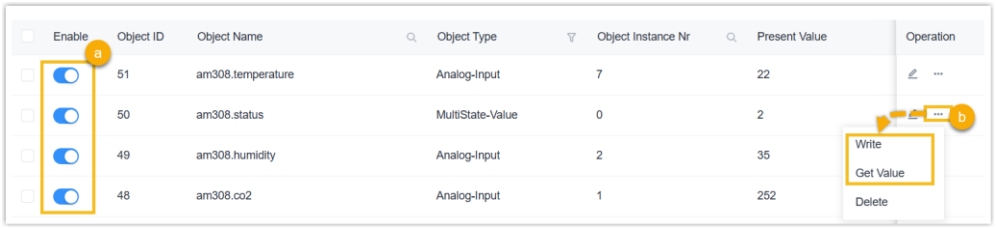
1. 左側のバーで、「**Data Service**」＞「**Data Acquisition**」ページを選択してください。



2. 上部のバーで、「**Device**」タブを選択します。
3. 対象のデバイスを選択し、オブジェクト数の値をクリックして「オブジェクト一覧」ページに移動します。



4. 上記の手順に従って、オブジェクトを追加し、有効にしてください。
5. [Operation] 列で、目的のオブジェクトの　　動作列にある目的のオブジェクトの [有効化] をクリックします。
6. 「**Get Value**」を選択して最新の値を読み取るか、「**Write**」をクリックしてこの値を書き込んでください。読み取り／書き込みの権限は、データ型またはアクセスモードによって異なります。



I/O デバイス

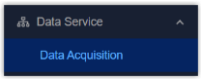
この章では、端末デバイス接続のための IO インターフェースの設定方法について説明します。

前提条件

- 「配線図」を参照し、IO デバイスがゲートウェイと互換性があることを確認してください。
- 「端末デバイスの配線」の手順に従って、IO デバイスを正しいインターフェースに接続してください。

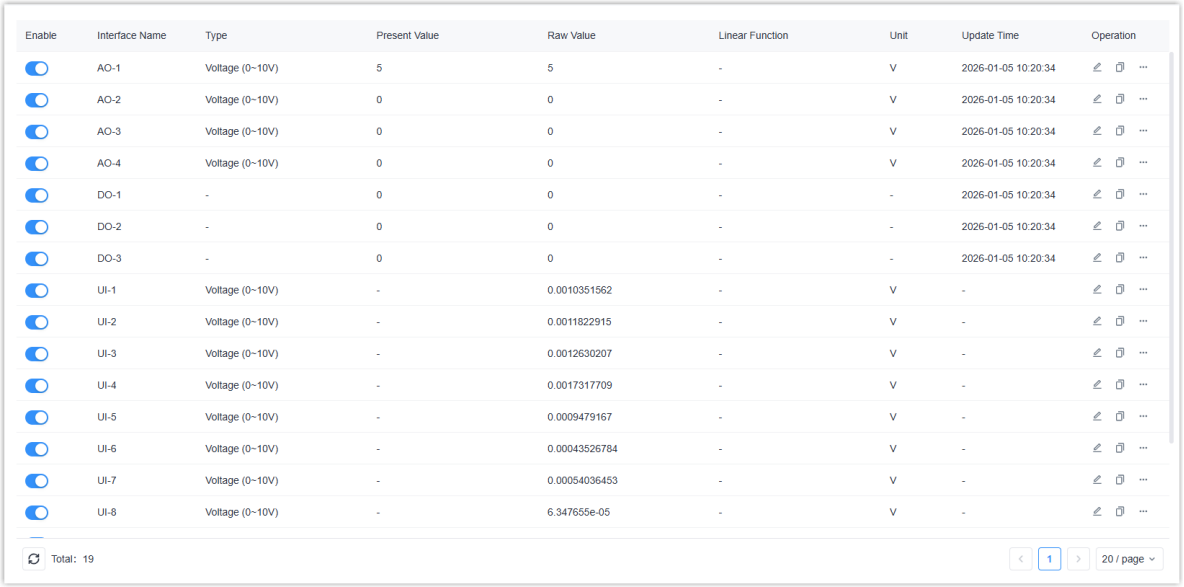
手順

1. 左側のバーで、**[Data Service] > [Data Acquisition]** ページを選択します。



2. 上部のバーで、「**IO Device**」タブを選択してください。

3. 必要な IO インターフェースを有効にし、その情報を確認してください。



Enable	Interface Name	Type	Present Value	Raw Value	Linear Function	Unit	Update Time	Operation
	AO-1	Voltage (0~10V)	5	5	-	V	2026-01-05 10:20:34	
	AO-2	Voltage (0~10V)	0	0	-	V	2026-01-05 10:20:34	
	AO-3	Voltage (0~10V)	0	0	-	V	2026-01-05 10:20:34	
	AO-4	Voltage (0~10V)	0	0	-	V	2026-01-05 10:20:34	
	DO-1	-	0	0	-	-	2026-01-05 10:20:34	
	DO-2	-	0	0	-	-	2026-01-05 10:20:34	
	DO-3	-	0	0	-	-	2026-01-05 10:20:34	
	UI-1	Voltage (0~10V)	-	0.0010351562	-	V	-	
	UI-2	Voltage (0~10V)	-	0.0011822915	-	V	-	
	UI-3	Voltage (0~10V)	-	0.0012630207	-	V	-	
	UI-4	Voltage (0~10V)	-	0.0017317709	-	V	-	
	UI-5	Voltage (0~10V)	-	0.0009479167	-	V	-	
	UI-6	Voltage (0~10V)	-	0.00043526784	-	V	-	
	UI-7	Voltage (0~10V)	-	0.00054036453	-	V	-	
	UI-8	Voltage (0~10V)	-	6.347655e-05	-	V	-	

Total: 19 1 20 / page

Parameter	説明
Enable	インターフェースを有効または無効にします。
Interface Name	インターフェースの種類を表示します。
Type	インターフェースの設定タイプを表示します。
Present Value	入力タイプの場合、線形関数または極性反転による処理後の値が表示されます。出力タイプの場合、ユーザーから送信された値が表示されます。
Raw Value	入力タイプの場合、収集された生の値が表示されます。出力タイプの場合、線形関数または極性反転による処理後の値が表示されます。
Linear Function	タイプがDI、Counter、またはDOでない場合、線形関数の式が表示されます。
Unit	タイプがDI、Counter、またはDOでない場合、値の単位が表示されます。
Update Time	値が出力された、または入力値が取得された最新の時刻を表示します。
Operation	操作 ：現在のインターフェースのパラメータを、同じタイプの他のインターフェースにコピーします。

Parameter	説明
	••• : クリックして、さまざまなインターフェースタイプに基づいたテストアクションを実行します。

4. 「  」をクリックして、インターフェースの種類に応じてIOインターフェースのパラメータを設定します。

アナログ出力 (AO) の場合

Parameter	説明
Enable	このインターフェースを有効または無効にします。
Output Type	出力タイプとして「電流 (4～20mA)」または「電圧 (0～10V)」を選択します。 **注意：** 接続されたデバイスとタイプが一致していることを確認してください。一致していない場合、ゲートウェイまたは接続されたデバイスが損傷する恐れがあります。
Unit	出力値の値の単位を選択してください。
Output After Reboot	再起動後の出力値を選択してください。 **KeepLast**」：再起動後も最後の生値を出力します。 **Raw**：出力するカスタム生データ値を定義します。
Description	このインターフェースに関する注意事項。
Linear Function	有効にすると、設定された出力値は、出力される前に関数式に代入されます。 式：y=a*x+b (y：現在値/設定値、x：生値/実際の出力値)

デジタル出力（DO）用

Parameter	説明
Enable	このインターフェースを有効または無効にします。

Parameter	説明
Polarity Inversion	極性反転の状態を選択します。 **Normal**：開 = 0、閉 = 1 **Reverse**：閉 = 0、開 = 1
Output After Reboot	再起動後の出力値を選択してください。 **Keep Last Value**：再起動前の最後の値を出力します。 **Closed/Open**：出力したい値を選択してください。
Description	このインターフェースに関する注意事項です。

デジタル入力（DI）用

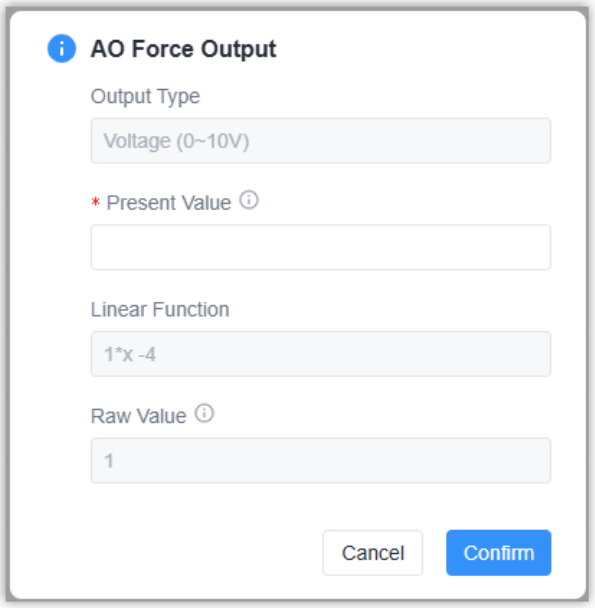
Parameter	説明
Enable	このインターフェースを有効または無効にします。
Input Type	入力タイプとして「レベルステータス」または「カウンタ」を選択します。
Description	このインターフェースに関する注記です。
Input Type is Level Status	
Filter Time	この値は、変更されたレベルステータスがこの時間より長く続いた場合にのみ更新されます。
Polarity Inversion	極性反転の状態を選択してください。 **Normal**：ローレベル = 0、ハイレベル = 1 **Reverse**：ハイレベル = 0、ローレベル = 1
Input Type is Counter	
Trigger Condition	カウント値をインクリメントするためのトリガー条件を選択してください。
Filter Time	カウント値は、レベルの状態の変化がこの時間より長く続いた場合にのみ、1 ずつ増加します。
Trigger Count	カウント値がこの値に達すると、MQTTブローカーにパケットが送信されます。

ユニバーサル入力 (UI) の場合

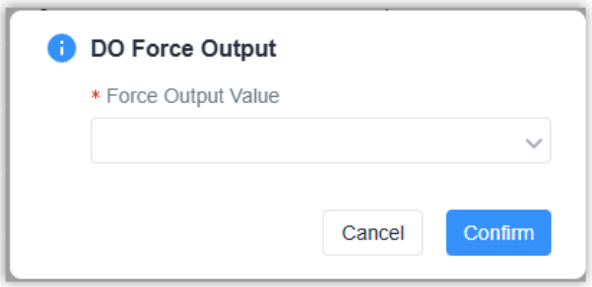
Parameter	説明
Enable	このインターフェースを有効または無効にします。
Input Type	以下のオプションから入力タイプを選択してください：電圧（0～10V）、電流（4～20mA）、抵抗 1000Ω、抵抗 2000Ω、NTC 10K Type2、NTC 10K Type3、NTC 20K、Pt1000、Ni1000、DI。 **注意：** 接続するデバイスとタイプが一致していることを確認してください。一致していない場合、ゲートウェイが破損する恐れがあります。
Collection Interval	端末デバイスからデータを収集する間隔を定義します。 範囲：1～86400秒。
Description	このインターフェースを識別するためです。
Input Type is DI	
High-Level Threshold	外部電圧がこのしきい値を超えると、DIはハイレベルであると判断されます。範囲：2～24V。
Low-Level Threshold	外部電圧がこのしきい値を下回ると、DIはローレベルであると判定されます。範囲：0～2V。
Polarity Inversion	極性反転の状態を選択してください。 **Normal**：ローレベル = 0、ハイレベル = 1 **Reverse**：ハイレベル = 0、ローレベル = 1
Input Type is not DI	
Unit	入力値の値の単位を選択してください。
Linear Function	有効にすると、収集された値は、表示される前に関数式に代入されます。 式：y=a*x+b (y：現在値、x：生データ/実際の収集値)
Single Lead Resistance	Pt1000またはNi1000センサーの場合、リード線の値を入力することで、リード線が精度に影響を与えるのを防ぐことができます。

5. 「**Save**」をクリックして、上記の設定を保存してください。

6. ••• をクリックして、IOインターフェースをテストするための操作を行ってください。
   - AO タイプの場合は、「**Force Output**」をクリックして、出力する値を定義します。



   - DO タイプの場合は、「**Force Output**」をクリックして、出力ステータスを「閉」または「開」



   に設定します。

   - UI タイプの場合は、「**Get Value**」をクリックして、その値を即座に読み取ります。
   - DI-Count タイプの場合は、「**Reset**」をクリックしてカウント値をリセットします。

デバイスアクセスネットワーク

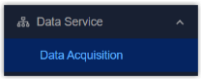
この章では、端末デバイスからデータを収集するためのネットワークの設定方法について説明します。

LoRaWAN® ネットワークの設定

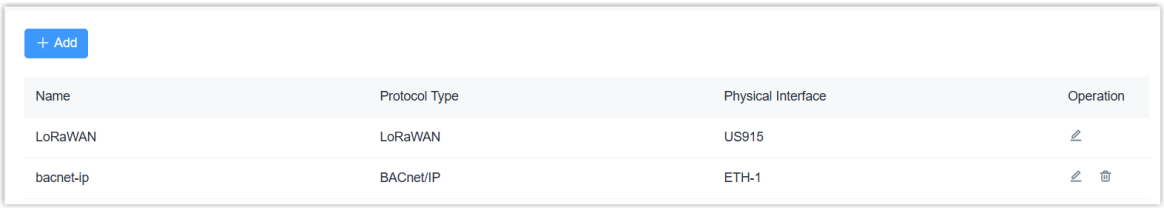
LoRaWAN® ネットワークはデフォルトでプリロードされており、削除することはできません。

手順：

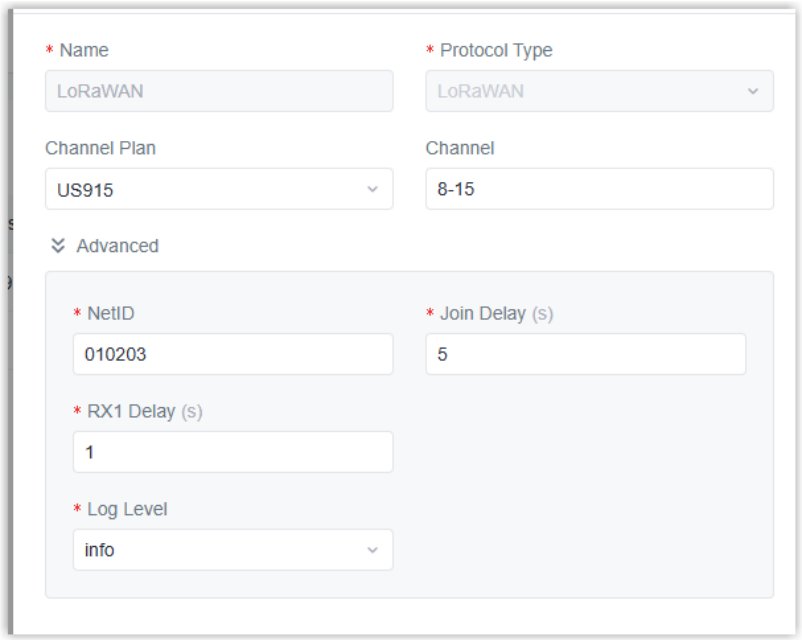
1. 左側のバーで、「**Data Service**」＞「**Data Acquisition**」ページを選択してください。



2. 上部のバーで、「**Device Access Network**」タブを選択します。



3. 「 」をクリックして、チャネルプランを選択します。その他のパラメータは、デフォルト値のままにするか、必要に応じてカスタマイズできます。



Parameter	説明
Channel Plan	ネットワークのチャネルプランを選択します。オプションはモデルによって異なります： -868M: EU868、IN865、RU864 -915M: AU915、US915、KR920、AS923-1/2/3/4 -470M: CN470
Channel	チャネルインデックスを入力することで、エンドデバイスが特定の周波数チャネルを介して通信できるようにします。例：

Parameter	説明
	1,40：チャンネル 1 および 40 を有効にします。 1-40：チャンネル 1～40 を有効にします。 1-40, 60：チャンネル 1～40 および 60 を有効にします。 Null：すべてのチャンネルを有効にします。
Additional Channels	**Add** をクリックして、LoRaWAN® 地域パラメータで定義されていないチャネルを追加します。この機能は、US915/ AU915/CN470 以外のチャネルプランでのみ動作します。
Advanced	
NetID	エンドデバイスがネットワークサーバーを識別するために使用する一意の識別子です。
Join Delay	エンドデバイスが Join Request を送信した後、Join Accept メッセージを待機する間隔を定義します。
RX1 Delay	エンドデバイスが最初の受信ウィンドウ（RX1）が開くのを待機する遅延時間を定義します。
Log Level	ログ記録のレベルを選択します。

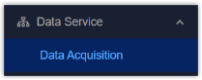
4. 「**Save**」をクリックして設定を保存してください。

デバイスのネットワークアクセスを追加

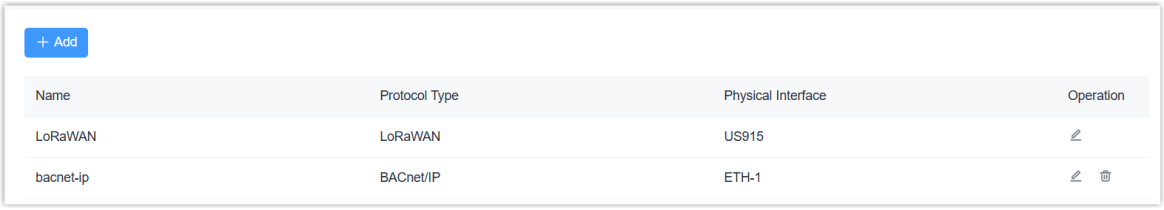
このデバイスでは、さまざまな種類のネットワークに対応しています。

手順：

1. 左側のバーで、「**Data Service**」>「**Data Acquisition**」ページを選択します。



2. 上部バーで、「**Device Access Network**」タブを選択します。



3. 「**+Add**」をクリックして新しいネットワークを追加し、基本パラメータを設定します。

Parameter	説明
Name	ネットワークに固有の名前を定義します。
Protocol Type	端末機器に応じて、プロトコルタイプを選択してください：BACnet/IP、BACnet MS/TP、Modbus RTU、Modbus TCP、Modbus RTU over TCP、KNX/TP。

4. プロトコルの種類に応じて、ネットワークパラメータを設定してください。

BACnet/IP

Parameter	説明
Network Interface	他の BACnet/IP 端末デバイス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。
Advanced	
Device Instance Nr	BACnet/IP ネットワークにおけるゲートウェイの一意の識別子を定義します。
UDP Port	通信ポートを設定します。
Timeout	コマンド送信後、端末デバイスからの応答を待つ時間を設定します。
Retry times	応答がない場合、端末デバイスへのコマンド送信の再試行回数を定義します。
Keep Alive Interval	端末機器のオンライン／オフライン状態を確認するために、ハートビートパケットを送信する間隔を指定してください。3回試行しても応答がない場合、その端末機器はオフラインとみなされます。

BACnet MS/TP

Parameter	説明
Physical Interface	BACnet MS/TP 端末機器に接続するための RS485 インターフェースを選択します。
Baud Rate	シリアルデータ転送速度を選択します。
Data Bits	各文字のデータビット数です。8 ビットに固定されています。
Stop Bits	各データフレームの終了を示すもので、受信側がフレームが完了しているかどうかを判断できるようにします。オプション：1、2

Parameter	説明
Parity	これは、送信中のエラーを検出するために使用されます。オプション：なし、奇数、偶数。
DIP	この設定を有効または無効にすることで、端子AとB間に120Ωの終端抵抗を追加し、ケーブル端からの信号反射を防止します。
Advanced	
Device Instance Nr	BACnet MS/TP ネットワーク内でのゲートウェイの一意の識別子を定義します。
MAC Address	BACnet MS/TP ネットワーク内でのゲートウェイの一意の MAC アドレスを定義します。範囲：0～127
Max Master	ネットワーク上で他のマスターを検索する際、デバイスが検索する最大のMACアドレスを定義します。
Max Info Frames	デバイスがネットワーク上の別のデバイスにトークンをパスする前に送信できるデータフレームの最大数を設定します。
Timeout	コマンドを送信するたびに、端末デバイスからの応答を待つ時間を設定します。
Retry times	応答がない場合、端末デバイスへのコマンド送信の再試行回数を設定します。
Keep Alive Interval	端末機器のオンライン／オフライン状態を確認するために、ハートビートパケットを送信する間隔を指定します。3回試行しても応答がない場合、その端末機器はオフラインとみなされます。

Modbus TCP または TCP 経由の Modbus RTU

Parameter	説明
Timeout	コマンド送信後、端末デバイスからの応答を待つ時間を設定します。
Retry times	応答がない場合、端末デバイスへのコマンド送信を再試行する回数を定義します。

Parameter	説明
Keep Alive Interval	端末機器のオンライン／オフライン状態を確認するために、ハートビートパケットを送信する間隔を指定します。3回試行しても応答がない場合、その端末機器はオフラインとみなされます。

Modbus RTU

Parameter	説明
Physical Interface	Modbus サーバー（スレーブ）デバイスに接続するための RS485 インターフェースを選択します。
Baud Rate	シリアルデータ転送速度を選択します。
Data Bits	各文字のデータビット数です。8ビットに固定されています。
Stop Bits	各データフレームの終了を示すもので、受信側がフレームが完了したかどうかを判断できるようにします。オプション：1、2
Parity	これは、送信中のエラーを検出するために使用されます。オプション：なし、奇数、偶数。
DIP	この設定を有効または無効にすることで、端子AとB間に120Ωの終端抵抗を追加し、ケーブル端からの信号反射を防止します。
Advanced	
Timeout	コマンド送信後、端末デバイスが応答するまで待機する時間を定義します。
Retry times	応答がない場合、端末デバイスへのコマンド送信の再試行回数を定義します。
Keep Alive Interval	端末機器のオンライン／オフライン状態を確認するために、ハートビートパケットを送信する間隔を指定します。3回試行しても応答がない場合、その端末機器はオフラインとみなされます。
Interframe Delay	2つの連続するModbus RTUコマンド間の遅延時間を設定します。

KNX/TP

Parameter	説明
Physical Address	KNX バスネットワーク内でのゲートウェイの一意の物理アドレスを定義します。
Advanced	
Timeout	コマンド送信後、端末機器からの応答を待つ時間を設定します。
Retry times	端末デバイスへの送信コマンドに対して応答がない場合の再試行回数を設定します。
Keep Alive Interval	端末装置のオンライン/オフライン状態を確認するために、ハートビートパケットを送信する間隔を定義します。3回試行しても応答がない場合、その端末装置はオフラインとみなされます。

5. **[Save]** をクリックして設定を保存します。
6. ネットワークパラメータを編集するには「 」をクリックし、必要に応じてネットワークを削除するには「 」をクリックしてください。

LoRaWAN

ゲートウェイ・フリート

この章では、このデバイスにエージェントゲートウェイを追加する方法について説明します。

概要

Milesight LoRaWAN® ゲートウェイは、Gateway Fleet機能を使用してマルチゲートウェイアーキテクチャを構築することができ、これにより、異なるゲートウェイ同士が相互にフェイルオーバーを提供し、信号のカバレッジを拡大し、単一のセンサーが複数のゲートウェイ間をローミングできるようにします。1つのゲートウェイ（コントローラー・ゲートウェイと呼ばれる）がネットワークサーバーとして機能し、他のゲートウェイ（エージェント・ゲートウェイと呼ばれる）はパケット転送専用として機能し、すべてのデータパケットをコントローラー・ゲートウェイに送信します。

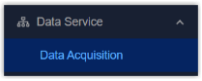
EG71は、コントローラーゲートウェイとして機能し、他のMilesight LoRaWAN®ゲートウェイからデータを受信することができます。

前提条件

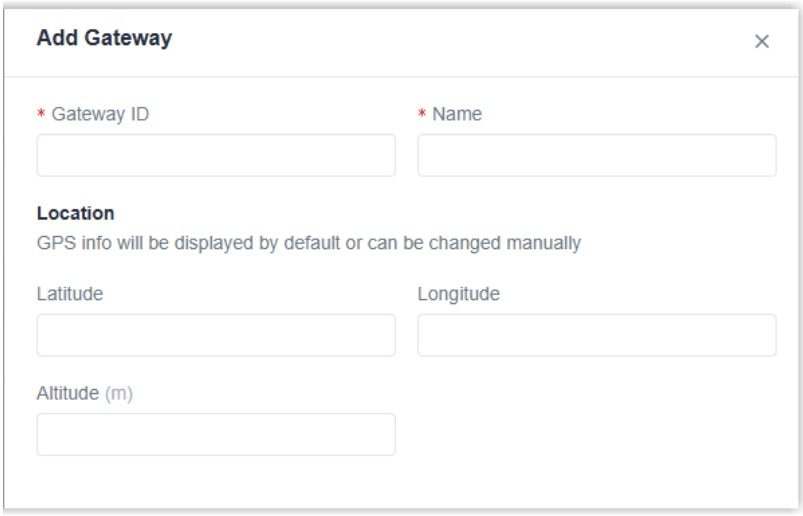
- エージェントゲートウェイ：EG71以外の任意のMilesight LoRaWAN®ゲートウェイ
- EG71 ゲートウェイにはパブリック IP アドレスが割り当てられているか、他のゲートウェイから到達可能である必要があります。

エージェントゲートウェイの追加

1. 左側のバーで、「**Data Service**」>「**Data Acquisition**」ページを選択します。

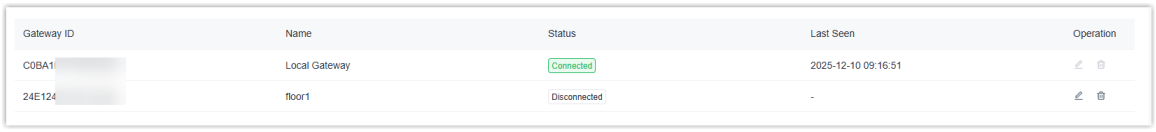


2. 上部バーで **[LoRaWAN]** タブを選択し、次に **[Gateway Fleet]** タブを選択します。
3. 「**+Add**」をクリックして、エージェントゲートウェイを追加します。
4. エージェントゲートウェイのパラメータを設定し、「**Save**」をクリックしてください。



Parameter	説明
Gateway ID	これは、エージェントゲートウェイの「パケット転送」設定ページで確認できます。
Name	エージェントゲートウェイの識別可能な名前を定義します。
Location	ゲートウェイの緯度、経度、高度を入力してください。エージェントゲートウェイがGPSに対応している場合、位置情報はここで自動的に更新されます。

5. エージェントゲートウェイのパケット転送タイプを「**Remote Embedded NS**」に設定し、サーバーアドレスをEG71ゲートウェイのアドレスに設定してください。詳細については、各ゲートウェイのユーザーガイドをご参照ください。
6. エージェントゲートウェイの接続状態を確認してください。



7. クリックして をクリックしてゲートウェイ情報を編集するか、 をクリックして、必要に応じてゲートウェイを削除してください。

デバイスプロファイル

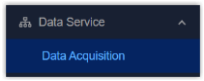
デバイスプロファイルは、LoRaWAN® エンドデバイスの機能およびネットワークへの参加パラメータを定義します。ゲートウェイは、ほとんどのデバイス向けに8種類のプロファイルを提供しています。これらのプロファイルがお使いのデバイスと互換性がない場合は、この章を参照して、カスタムデバイスプロファイルを追加および管理してください。

前提条件

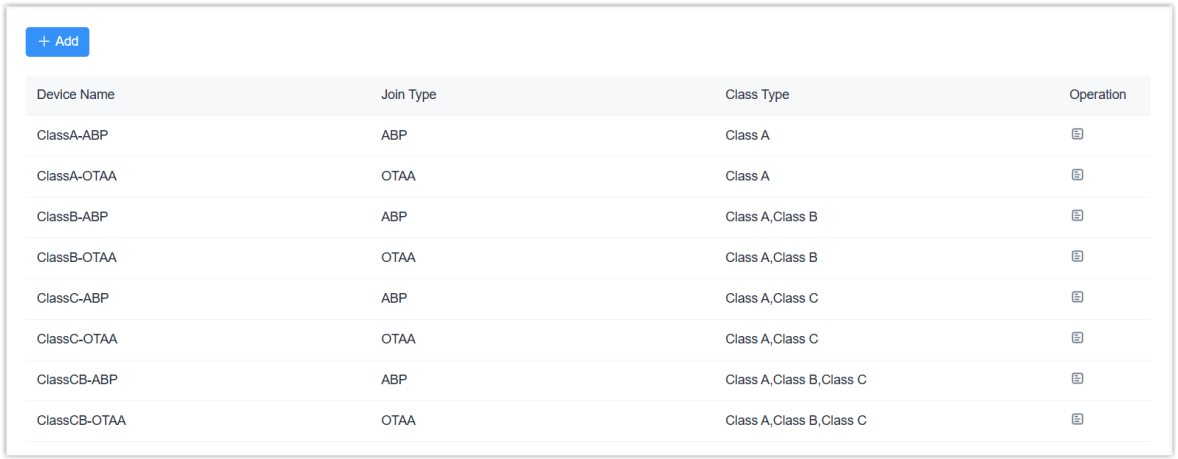
エンドデバイスベンダーからプロファイルパラメータを入手してください。

手順

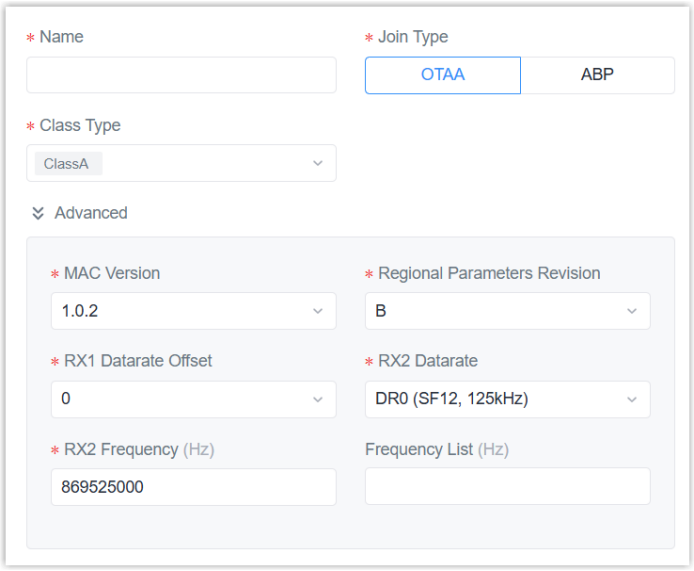
1. 左側のバーで、「**Data Service**」＞「**Data Acquisition**」ページを選択してください。



2. 上部のバーで、「**LoRaWAN**」タブを選択し、次に「**Device Profiles**」タブを選択します。
3. 「 」をクリックして、デフォルトプロファイルの詳細を確認します。



お使いのデバイスに該当するものがない場合は、「**+Add**」をクリックして新しいプロファイルを追加し、パラメータを設定してください。



Parameter	説明
Name	一意のデバイスプロファイル名を定義します。
Join Type	「OTAA」または「ABP」を選択してください。
Class Type	クラス B またはクラス C を選択してください。クラス A は常に有効になっています。
Advanced	
MAC Version	エンドデバイスのMACバージョンを選択してください。
Regional Parameters Revision	このプロファイルの地域パラメータのバージョン識別子を選択してください。
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。
RX2 Datarate	RX2ウィンドウのデータレートです。
RX2 Frequency	RX2ウィンドウの周波数です。
Frequency List	デバイスベンダーから提供された工場出荷時の周波数値を、カンマ区切りのリストとして入力してください。
Device Channel	チャンネルインデックスを入力することで、エンドデバイスが特定の周波数チャンネルを介して通信できるようにします。この機能は、CN470/US915/AU915のチャンネルプランでのみ動作します。例： 1,40：チャンネル 1 および 40 を有効にします。 1-40：チャンネル 1～40 を有効にします。

Parameter	説明
	1-40, 60：チャンネル1～40および60を有効にします Null：すべてのチャンネルを有効にします **Tip：** Milesightエンドデバイスのデフォルト設定を使用する場合は、この値を8～15に設定してください。
Ping Slot Periodicity	クラスBエンドデバイスがメッセージを受信するためにPingスロットを開く期間です。
Ping Slot Data Rate	クラス B デバイス向けのダウンリンクを受信するためのデータレートです。
Ping Slot Frequency	クラスBデバイスのダウンリンクを受信するための周波数です。
Class B ACK Timeout	クラスBデバイスからのダウンリンク応答を待機する時間です。この時間内に応答が受信されない場合、ゲートウェイはダウンリンクコマンドを再送信します。
Class C ACK Timeout	クラスCデバイスからのダウンリンク応答を待機する時間です。この時間内に応答が受信されない場合、ゲートウェイはダウンリンクコマンドを再送信します。

4. **[Save]** をクリックしてプロファイルを保存します。
5. 「 」をクリックしてカスタムプロファイルを編集するか、「 」をクリックしてカスタムプロファイルを削除します。

マルチキャスト

マルチキャストグループを作成することで、同じマルチキャストアドレス、セッションキー、およびフレームカウンタを共有するデバイスのグループに対して、単一のダウンリンクペイロードを送信することができます。この章では、マルチキャストグループの追加方法と使用方法について説明します。

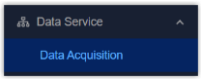
前提条件

同じグループ内のすべての LoRaWAN® エンドデバイスが、以下の条件を満たしていることを確認してください：

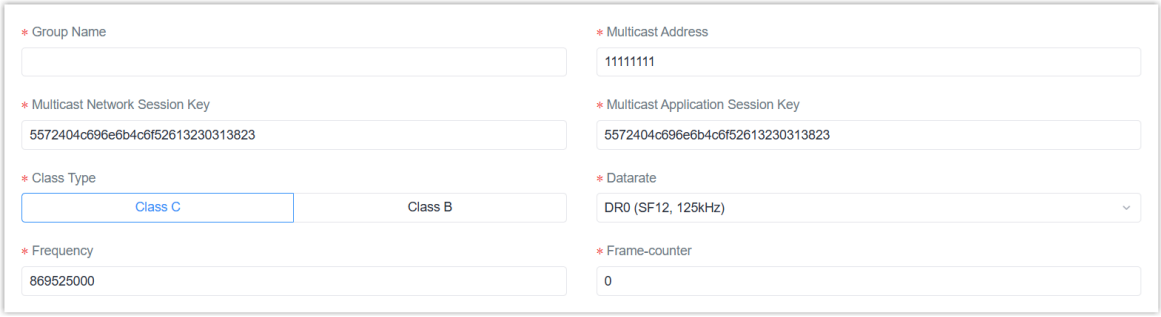
- マルチキャスト機能を対応していること。
- 以下のパラメータを同じ設定にしてください：クラス種別（クラスBまたはクラスC）、マルチキャストアドレス、マルチキャストMcNetSkey、マルチキャストMcAppSkey、RX2データレート、RX2周波数、およびアプリケーションポート。
- このゲートウェイに追加されました。

手順

1. 左側のバーで、「**Data Service**」>「**Data Acquisition**」ページを選択します。

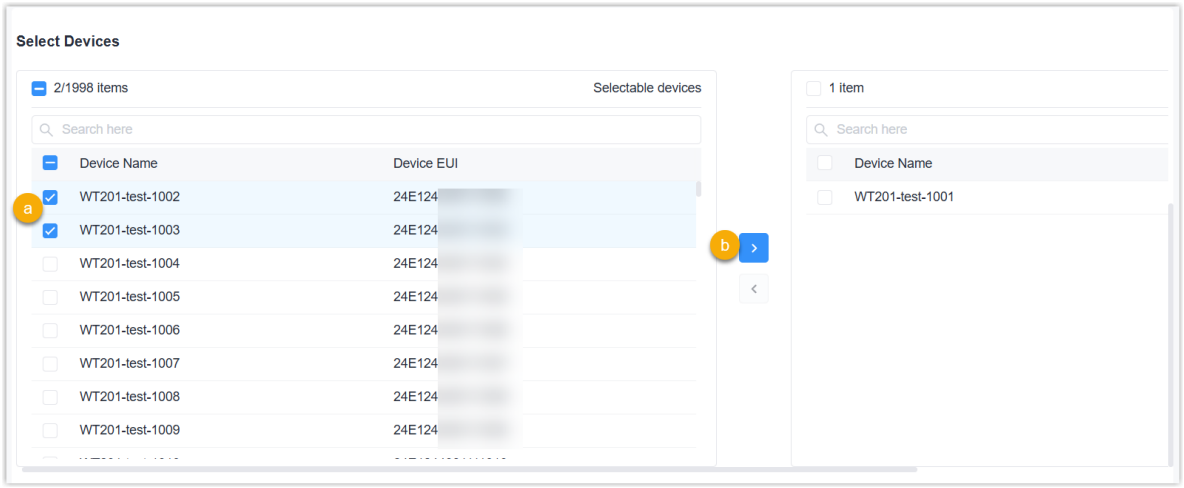


2. 上部バーで「**LoRaWAN**」タブを選択し、次に「**Multicast**」タブを選択します。
3. 「**+Add**」をクリックしてグループを追加し、関連するパラメータを設定します。



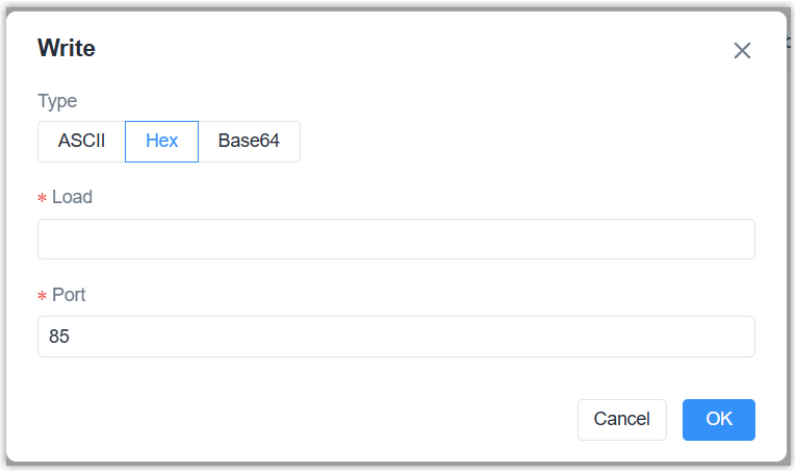
Parameter	説明
Group Name	マルチキャストグループに固有の名前を定義します。
Multicast Address	異なるマルチキャストグループを区別するために使用される、一意の 8 桁のアドレスを定義します。
Multicast Network Session Key	このグループ内のすべてのデバイスに対するネットワーク セッション キー（Netwks Key）です。
Multicast Application Session Key	このグループ内のすべてのデバイスに対するアプリケーション・セッション・キー（AppSKey）です。
Class Type	クラス B またはクラス C はオプションです。
Datarate	エンドデバイスがダウンリンクのペイロードを受信する際に使用するRX2データレートです。
Frequency	エンドデバイスがダウンリンクペイロードを受信するために使用するRX2周波数。
Frame-Counter	ダウンリンクパケットを介して受信されたデータフレームの数です。ゲートウェイによって自動的にインクリメントされます。
Ping Slot Periodicity	エンドデバイスがクラスBデバイス向けのメッセージを受信するためにPingスロットを開く周期です。

4. このマルチキャストグループに追加するデバイスを選択してください。通常は、同じモデルのデバイス



を選択します。

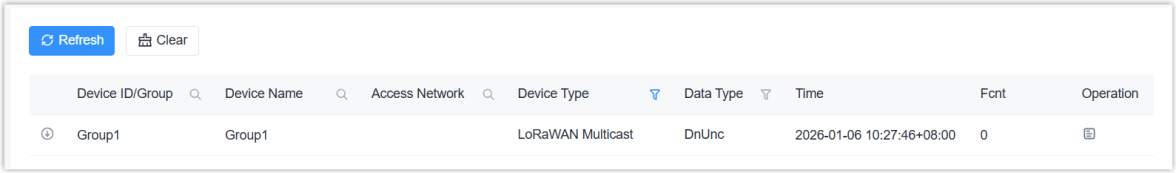
5. 「**Apply**」をクリックして設定を保存してください。
6. グループ一覧からグループを選択し、「 」をクリックしてダウンリンクペイロードを設定します。



Parameter	説明
Type	ダウンリンクペイロードのタイプを選択します。
Load	対応するタイプに基づいて、ダウンリンクペイロードを定義します。
Port	エンドデバイス用のアプリケーションポートを定義します。

7. 「**OK**」をクリックして、ダウンリンクペイロードを送信します。

8. **[Data Service] > [Data Stream]** に移動し、ダウンリンクの送信状況を確認します。



FUOTA

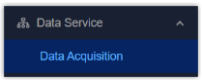
Firmware Update Over the Air（FUOTA）は、ユニキャストまたはマルチキャストを使用してLoRaWAN®エンドデバイスにファームウェアの更新を配信するための規格です。この章では、エンドデバイスのアップグレード方法について説明します。

前提条件

- エンドデバイスが標準のFUOTAプロトコルに対応しているか、またはFUOTAに対応するように更新されていること。
- エンドデバイスがゲートウェイに追加されていること。

手順

1. 左側のバーで、**[Data Service] > [Data Acquisition]** ページを選択します。

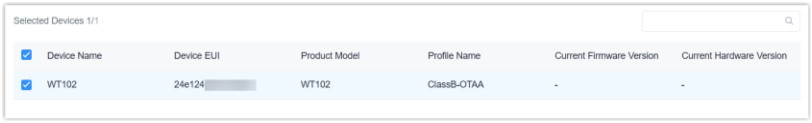


2. 上部のバーで「**LoRaWAN**」タブを選択し、次に「**FUOTA**」タブを選択してください。
3. 「**+Add**」をクリックしてFUOTAタスクを追加し、関連するパラメータを設定します。

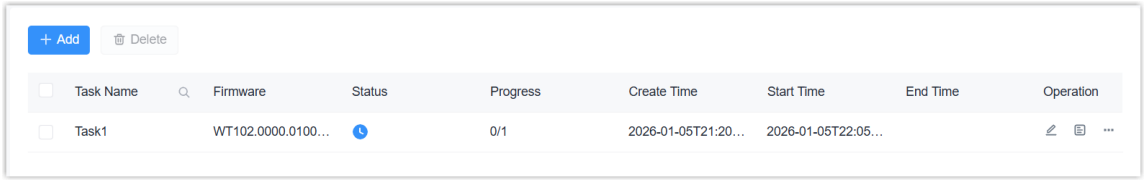
Parameter	説明
Task Settings	
Task Name	FUOTA タスクに一意の名前を指定します。
Start Time	このタスクを開始する時刻を選択してください。
Description	このタスクに関するメモです。
Firmware Setting	
Firmware	アップグレードするファームウェアをインポートします。 **Upload**：クリックしてローカルパスからファームウェアを選択します。 **Selectanofficialfile**：公式ウェブサイトからダウンロードするファームウェアを選択します。これには、ゲートウェイがインターネットに接続されている必要があります。

Parameter	説明
Fragment Size	ファームウェアファイルは、デバイスへの配布のためにこのサイズごとに分割されます。通常は、デフォルト値のままにしておいてください。 ネットワーク環境が複雑または不安定な場合は、この値を 64 またはそれ以下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のフラグメントを割り当てる間隔です。通常は、デフォルト値のままにしておいてください。 ネットワーク環境が複雑または不安定な場合は、この値を7～10秒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	本デバイスは、ファームウェアパケットの訂正のために、30%の冗長パケットを送信します。通常は、デフォルト値のままにしておいてください。 ネットワーク環境が複雑または劣悪な場合は、送信成功率を向上させるために、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、この値を下げることができます。
Multicast Setting	
Datarate	ファームウェアのフラグメントをデバイスに割り当てるためのデータレート。
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ためのダウンリンク周波数。

4. 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。



5. **[Apply]** をクリックして設定を保存します。
6. リストでタスクのステータスを確認してください。



Parameter	説明
Task Name	タスク名が表示されます。
Firmware	このタスクでアップグレードするファームウェアを表示します。
Status	タスクのステータスを表示します。 **Pending：**タスクを処理するために、スケジュールされた時刻を待っています。 **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を返信しています。 **Finished：**すべてのデバイスから、成功またはフェイルを含むアップグレード結果の応答がありました。
Progress	アップグレード済みまたは計画中のデバイスの数を表示します。
Create Time	このタスクの作成日時を表示します。
Start Time	このタスクの開始時刻を表示します。
End Time	このタスクの完了時刻を表示します。
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ます。  ：すべてのデバイスの成功・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「完了」の場合、アップグレードにフェイルしたデバイスに対してタスクを再試行するには「**Update**をクリックし、タスクのステータスが「Pending」または「Finished」の場合、このタスクを削除するには**Delete**をクリックします。

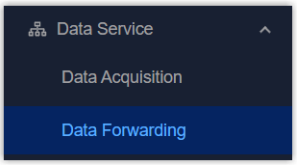
データの転送

この章では、外部サーバー（クライアント）へのデータの転送方法について説明します。

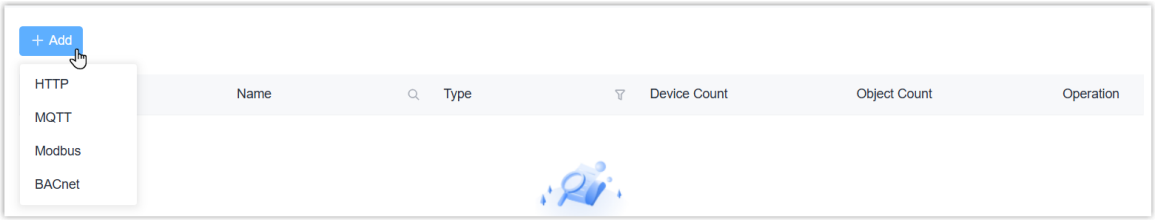
データ転送ルールの追加

ゲートウェイは、HTTP/MQTT サーバーへの接続、または BACnet/Modbus サーバーとして動作し、データの転送やダウンリンク制御コマンドの受信に対応しています。

1. 左側のバーで、「**Data Service**」＞「**Data Forwarding**」ページを選択してください。



2. 「**+Add**」をクリックし、HTTP、MQTT、Modbus、BACnet からプロトコルを選択します。



3. プロトコルに応じて、関連するパラメータを設定してください。

HTTP

Parameter	説明
Enable	HTTP(s) サーバーへのデータ転送を有効または無効にします。
Name	このデータ転送ルールに一意の名前を指定します。
Description	このデータ転送ルールに関するメモです。
Metadata	有効化後、ゲートウェイは選択された項目をアップリンクデータの転送コンテンツに追加します。
HTTP Header	**Add**をクリックして、HTTPヘッダーの名前と値を追加してください。
URL	さまざまな種類のデータを送信するには、URLを`http://`または`https://`で始まるように設定してください。詳細については、『MQTT&HTTPアプリケーションガイド』をご参照ください。 **Data Up**：通常のデータアップリンクです。 **ACK Notification**：LoRaWAN® デバイスへのダウンリンクコマンドの送信確認後の ACK 通知。 **Error Notification**：デバイスのエラー通知。**Online** **Notification**：デバイスのオンライン通知。**Offline** **Notification**：デバイスのオフライン通知。

MQTT

Parameter	説明
Enable	MQTT ブローカーとの通信を設定するために、有効または無効にしてください。
General	
Name	このデータ転送ルールに一意の名前を定義します。
Description	このデータ転送ルールのメモ用です。
Broker Address	MQTTブローカーのIPアドレスまたはドメイン名です。
Broker Port	MQTTブローカーのサービスポートです。
Client ID	ゲートウェイの一意の識別子です。
Connection Timeout	接続タイムアウト後もゲートウェイに応答がない場合、その接続は切断されたものとみなされます。
Keep Alive Interval	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する間隔です。
User Credentials	ユーザー名とパスワードによる認証を有効または無効にします。 **Username：**認証に使用するユーザー名です。 **Password：**認証用のパスワードです。
TLS	TLS認証を有効または無効にします。 **SSL Security：**有効にすると、ゲートウェイは証明書の有効性を確認します。 **Mode：**プリロードされた証明書を使用する場合は「**CASignedServer**を、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）、およびクライアントキー（.key）をインポートする場合は「**Certificate**を選択してください。
Data Retransmission	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、ネットワークが復旧した後にそのデータを再送信します。
Data	
Data Format	アップリンクオブジェクトデータのレポート形式を選択します。

Parameter	説明
	Combined：すべてのオブジェクトデータを 1 つのメッセージで報告します。 **Per Object**：各オブジェクトのデータを個別に報告します。
Metadata	有効にすると、ゲートウェイは選択された項目をアップリンクデータの転送コンテンツに追加します。
Topic	
Data Type	MQTTブローカーと通信するためのデータ型です。詳細については、『MQTT&HTTPアプリケーションガイド』をご参照ください。 **Data**：デバイスのアップリンクパケットを受信します。受信する内容を制限する必要がある場合は、このトピックにワイルドカード「$gatewaySN」、「$device Name」、「devEUI」、「deveui」、「objectID」、「objectName」を追加し、このトピックを購読する際に実際の値に置き換えてください。 **Downlink Data**：デバイスにダウンリンクコマンドを送信します。特定のデバイスまたはオブジェクト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「gatewaySN」、「$devEUI」、「devui」、「$deviceID」、または「$objectID」を追加し、このトピックを購読する際に実際の値に置き換えてください。 **UplinkMulticastData**：LoRaWAN® 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。 **Online Notification**：デバイスのオンライン通知を受信します。 **Offline Notification**：デバイスのオフライン通知を受信します。 **ACK Notification**：LoRaWAN® デバイスにダウンリンクコマンドを送信し、確認された後に ACK 通知を受信します。 **Error Notification**：デバイスのエラー通知を受信します。 **ACKRequest**：このデータ転送ルールに追加されたデバイスおよびオブジェクト情報を照会するために、空白のパケットを送信します。 **ManagementResponse**：Management Request トピックにリクエストを送信した後、このデータ転送ルールに追加されたデバイスおよびオブジェクトの情報（数、名前、ID を含む）を受け取ります。
Topic	パブリッシュに使用されるデータ型のトピック名。
QoS	QoS0、QoS1、または QoS2 はオプションです。

Parameter	説明
Retain	有効または無効にして、このトピックの最新のメッセージをリテインメッセージとして設定します。
Will	
Will	「最終メッセージ」の送信を有効または無効にします。MQTTクライアントが異常終了した際、最後のメッセージが自動的に送信されます。これは通常、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トピックです。
Will QoS	QoS0、QoS1、QoS2はオプションです。
Will Retain	有効または無効にして、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します。
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。

Modbus

Parameter	説明
Enable	この Modbus サーバー（スレーブ）を有効または無効にします。
Name	このデータ転送ルールに一意の名前を定義します。
Port	このサーバーの通信ポートです。
Connection Type	リモートModbusクライアント（マスター）と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。
Network Interface	このサーバーが Modbus クライアント（マスター）と通信するためのネットワークインターフェースを選択してください。設定を保存すると、このインターフェースの IP アドレスが表示されます。
Server ID	このサーバーを識別するための一意の ID を定義します。
Description	このデータ転送ルールを記録するためのものです。

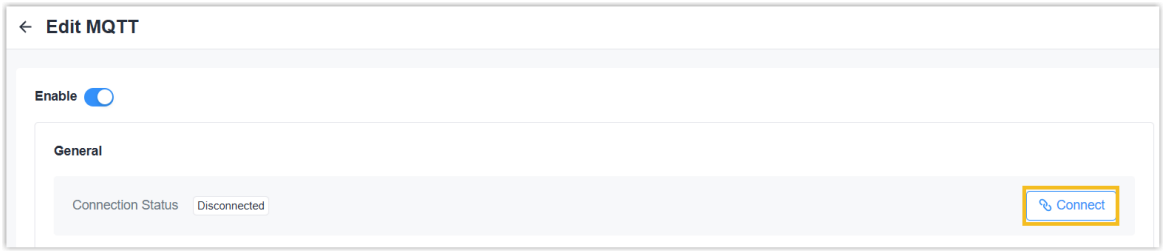
Parameter	説明
Global Object	有効にすると、デバイスオブジェクトを追加する際に、選択されたグローバルオブジェクトが転送オブジェクトに自動的に追加されます。

BACnet

Parameter	説明
Enable	この BACnet/IP サーバーを有効または無効にします。
Name	このデータ転送ルールに一意の名前を定義します。
UDP Port	このサーバーの通信ポートです。
Network Interface	このサーバーが BACnet クライアントと通信するためのネットワークインターフェースを選択してください。
Device Instance Nr	BACnet ネットワーク内でこのサーバーを識別するための一意の ID を定義します。
Device Name	BACnetネットワーク内でこのサーバーを識別するための一意の名前を指定してください。
Description	このデータ転送ルールを記録するためのものです。
Global Object	有効にすると、デバイスオブジェクトを追加する際に、選択されたグローバルオブジェクトが転送オブジェクトに自動的に追加されます。
BBMD	
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。
BBMD Type	BBMD タイプを選択してください。 **BBMD:** 異なるネットワークサブネットにメッセージをブロードキャストするデバイスとして機能します。 **ForeignDeviceRegistration：**BBMDに登録して、ブロードキャストメッセージを受信します。
Broadcast Distribution Table	**Add**をクリックして、メッセージを転送するためのBBMDまたは外部デバイスの情報（**IP**アドレス、ポート、サブネットマスクなど）を追加してください。追加できるデバイスは最大10台までです。

Parameter	説明
IP Address	BBMDのタイプが「外部デバイス登録」の場合、BBMDのIPアドレスを設定します。
IP Port	BBMD タイプが「外部デバイス登録」の場合、BBMD の UDP/IP ポートを設定します。
Registration Interval	BBMDタイプが「外部デバイス登録」の場合、登録間隔を設定してください。

4. **[Apply]** をクリックして設定を保存してください。
5. （MQTTのみ）データ転送リストで、 をクリックしてMQTTデータ転送ルールの編集ページに移動し、「**Connect**」をクリックしてMQTTブローカーとの接続を設定します。



データ転送オブジェクトの追加

本ゲートウェイは、外部サーバー（クライアント）への転送内容を定義する機能に対応しています。

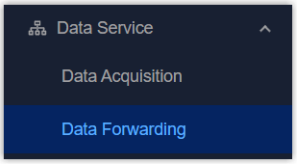
デバイスオブジェクトの追加

デバイスオブジェクトを追加すると、そのオブジェクトデータは、HTTP/MQTTサーバーへの転送や、Modbus/BACnetクライアントによる読み取りに対応します。

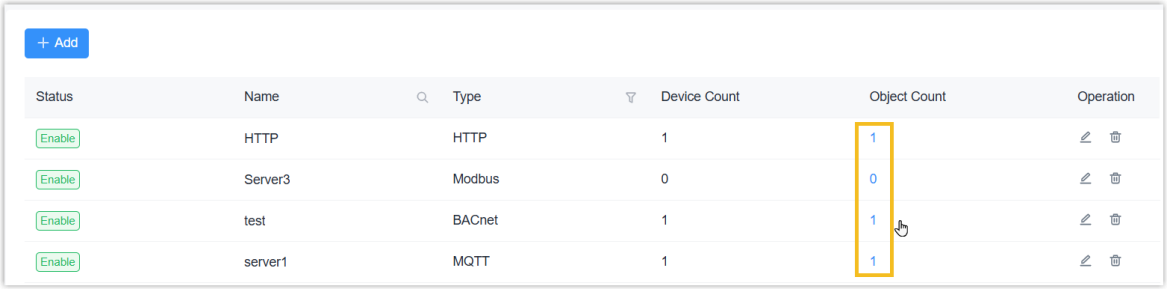
前提条件：IOインターフェースを有効にするか、必要なデバイスオブジェクトを有効にしてください。

手順：

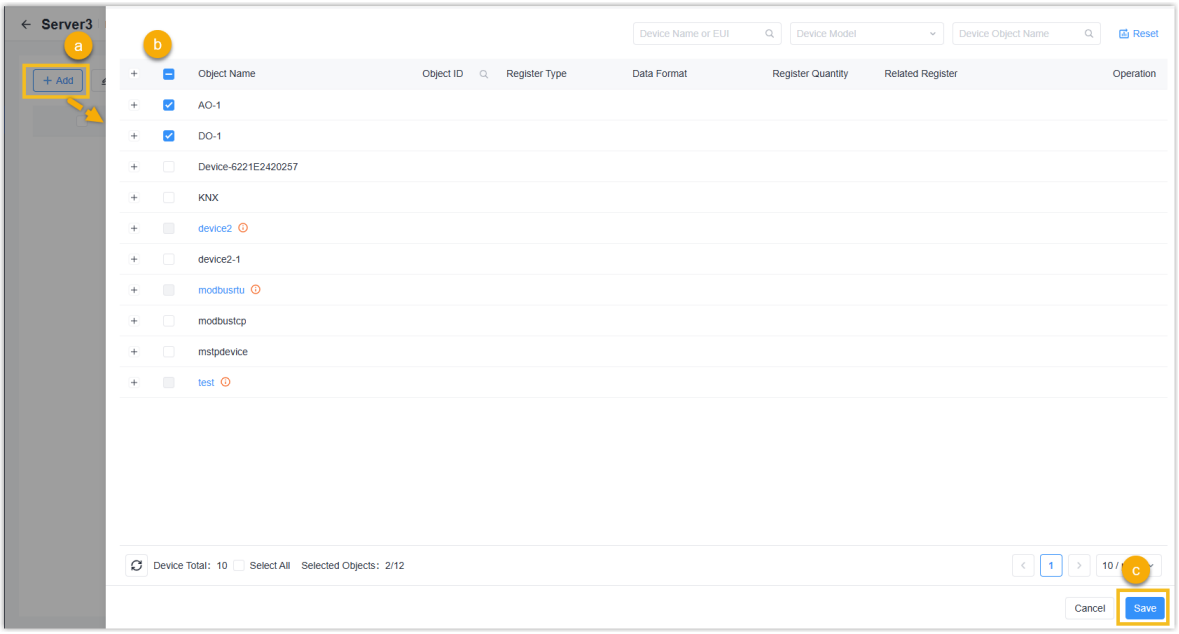
1. 左側のバーで、**[Data Service] > [Data Forwarding]** ページを選択します。



2. 目的のデータ転送ルールを選択し、オブジェクト数の値をクリックして「**Device Object**」ページに移動します。



3. 「**+Add**」をクリックして追加するオブジェクトを選択し、「**Save**」をクリックします。
   HTTP/MQTTタイプの場合、デバイスオブジェクトが追加されていない場合でも、LoRaWAN®デバ

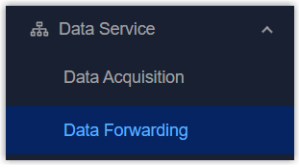


イスを直接選択するのに対応しています。

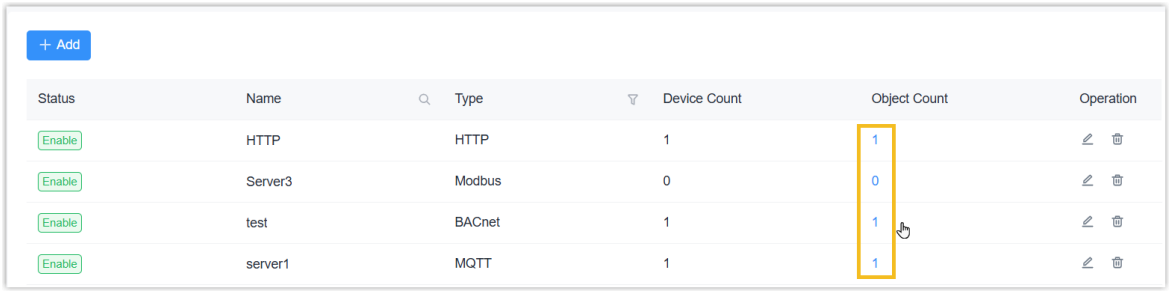
BACnetクライアント用のNCオブジェクトを追加する

ゲートウェイは、BACnetクライアントにアラームを送信するための通知クラスオブジェクトの追加に対応しています。

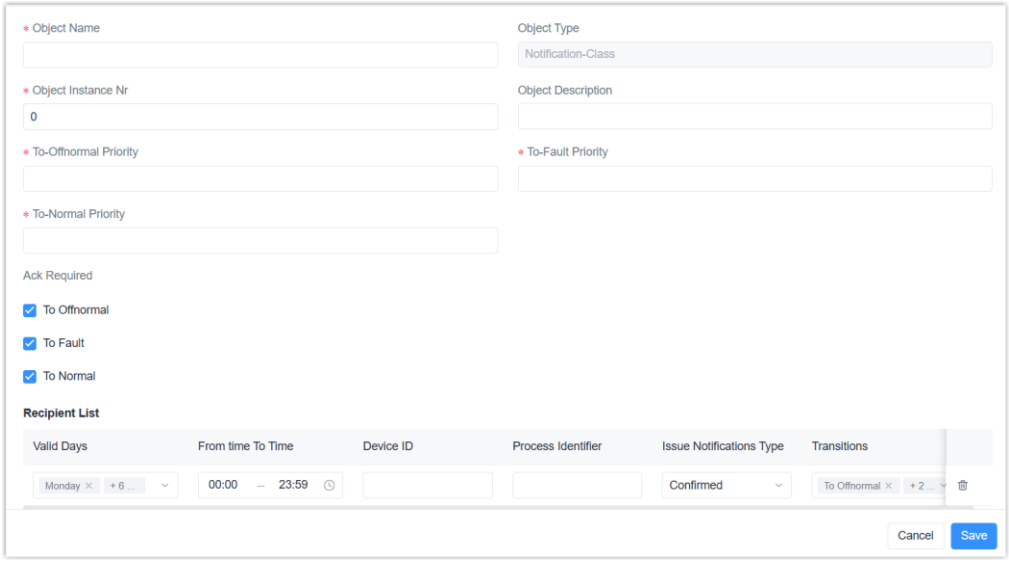
1. 左側のバーで、「**Data Service**」>「**Data Forwarding**」ページを選択します。



2. 目的のBACnetデータ転送ルールを選択し、オブジェクト数の値をクリックして「**Device Object**」ページに移動します。



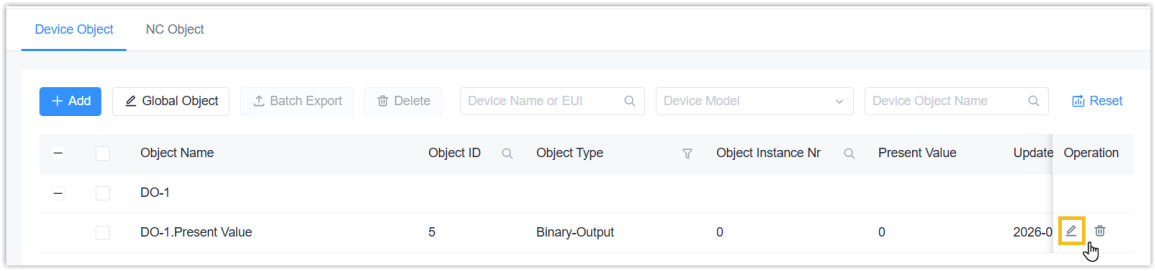
3. 上部のバーから、「**NC Object**」ページを選択します。
4. 「+Add」をクリックして新しい通知クラスオブジェクトを追加し、アラームパラメータを設定します。



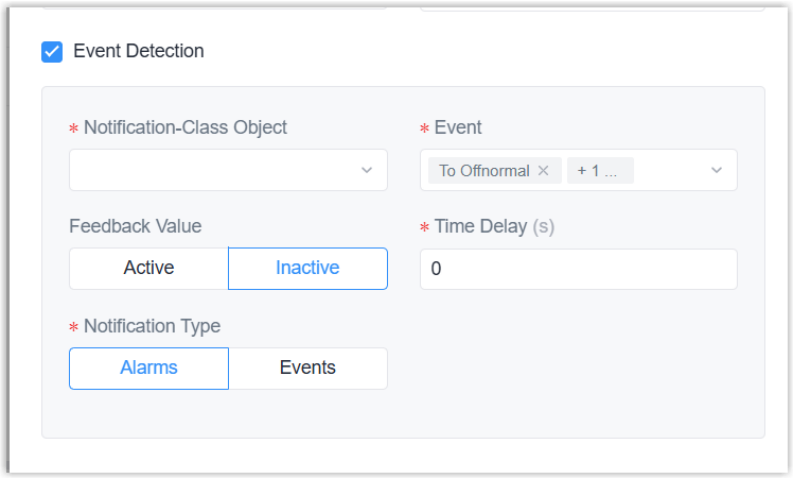
Parameter	説明
Object Name	このオブジェクトに一意の名前を定義します。
Object Type	Notification-Class に固定されています。
Object Instance Nr	一意のオブジェクトインスタンス番号を設定してください。
Object Description	このオブジェクトに関する注記用です。
To-Offnormal Priority	受信者がイベント通知を並べ替える際に使用する優先度番号を設定します。範囲：0～255（0が最も重要、255が最も重要度が低い）
To-Fault Priority	
To-Normal Priority	
Ack 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てください。

Parameter	説明
Recipient List	イベントがトリガーされると、このリストの受信者にイベント通知が送信されます。1 つのリストは、最大 10 人の受信者を対応できます。 **Valid Days**：通知を送信する有効な日。 **From time to time**： 通知を送信する有効な時間帯です。 **Device ID**：対象となる受信者のデバイスIDです。 **Identifier**：アラームの対象となるプロセスを示す識別子です。例えば、プロセス識別子「1」は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「Confirmed」または「未確認」を選択してください。ゲートウェイが「Confirmed」通知に対する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。

5. **[Save]** をクリックして、NCオブジェクトの設定を保存します。
6. 上部のバーから、「**Device Object**」ページを選択します。
7. 目的のオブジェクトを選択し、「 」をクリックして、このオブジェクトを編集します。



8. **Event Detection**を有効にし、関連するパラメータを設定してください。この機能は、文字列値を除くすべてのオブジェクトタイプに対応しています。



Parameter	説明
Notification-Class Object	通知クラスを選択して、受信者やその他のアラーム設定を決定します。
Event	報告するイベントの種類を選択します。
Time Delay	現在の値がしきい値条件に一致する場合、またはこの時間内にしきい値の範囲外になった場合にのみ、デバイスは対応するイベントを報告します。
Notification Type	通知タイプとして「アラーム」または「Event」を選択してください。
Object Type is Analog Input/Output/Value	
Limit Event	上限または下限に達したときにイベントを報告する場合は、これを選択してください。
High Limit	上限のしきい値の値を定義します。
Low Limit	下限の値を定義します。
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。
Object Type is Binary Input/Output/Value	
Alarm/Feedback Value	現在の値がこの値と一致している状態が指定された遅延時間続いた場合、「異常」イベントを通知します。また、現在の値がこの値と一致していない状態が指定された遅延時間続いた場合、「正常」イベントを通知します。
Object Type is Multi-State Input/Output/Value	

Parameter	説明
Alarm Value	「複数状態入力/値」の場合、現在の値がアラーム値と一致している間は「異常状態」イベントを報告し、一致していない間は「正常状態」イベントを報告します。
Fault Value	「複数状態入力/値」の場合、現在の値が故障値と等しいときは「故障」イベントを報告します。
Feedback Value	マルチステート出力の場合、現在の値がフィードバック値と等しい場合は、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は、遅延時間後に「To Normal」イベントを報告します。

9. 「**Save**」をクリックして、オブジェクトの設定を保存してください。

デバイスライブラリ

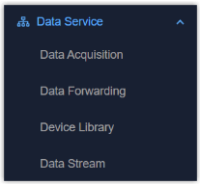
本デバイスは、端末デバイスのデータをオブジェクトに変換し、迅速かつ容易に統合することを対応しています。この章では、組み込みデバイスリポジトリまたはカスタムデバイスリポジトリを更新する方法について説明します。

組み込みデバイスリポジトリの更新

本デバイスには、Milesight LoRaWAN® エンドデバイスのリポジトリが組み込まれています。

手順：

1. 左側のバーで、「**Data Service**」>「**Data Library**」ページを選択します。



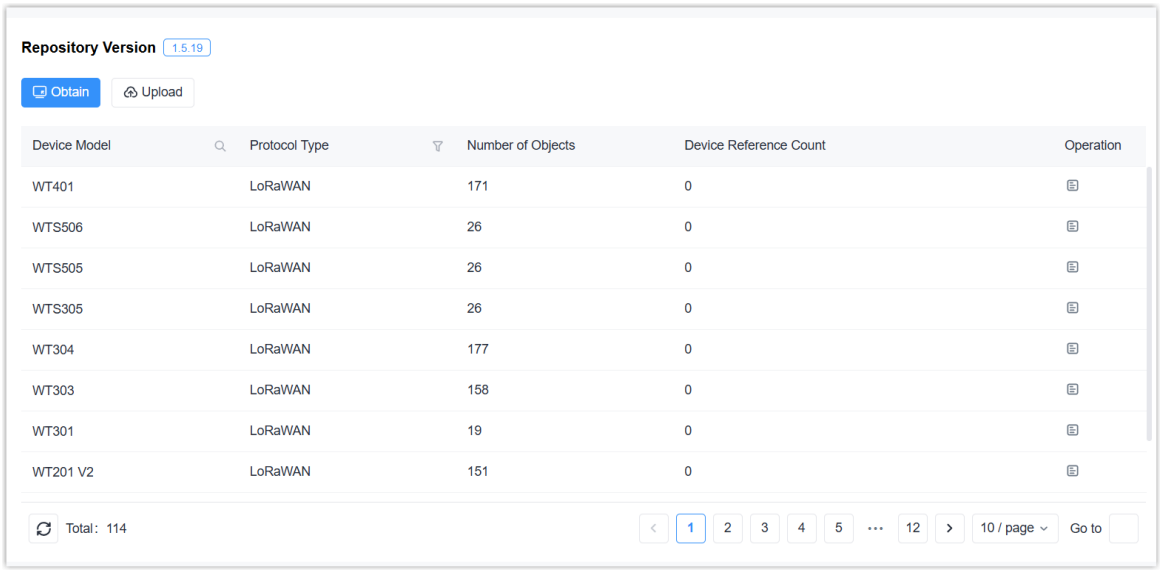
2. 上部バーで、「**Inbuilt Device Repository**」タブを選択します。
3. 以下の方法でデバイスリポジトリを更新します：

   Update Online：[Obtain] をクリックして、デバイスのリポジトリを更新します。これを行うには、デバイスがインターネットに接続されている必要があります。

   Update Locally：[Upload] をクリックし、ローカルパスからリポジトリファイルを選択してください。Milesight製品の最新リポジトリファイルは、こちらからダウンロードできます。

注：

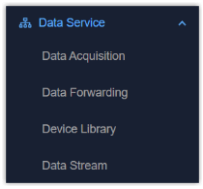
現在のバージョンより新しいバージョンのインポートのみ対応しています。



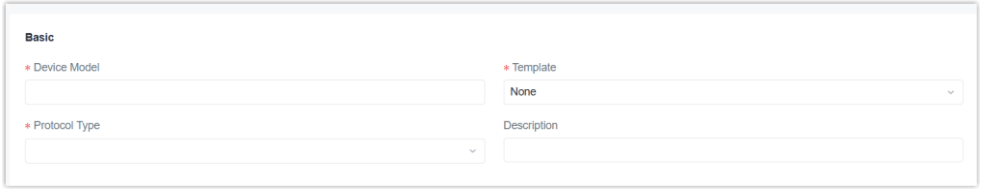
カスタムデバイスリポジトリ

本デバイスでは、サードパーティ製デバイス用のカスタムデバイスリポジトリを追加したり、カスタマイズされたコンテンツを追加したりすることができます。**前提条件：**デバイスの通信プロトコル、またはエンコーダー／デコーダーをデバイスベンダーから入手してください。**デバイスモデルを個別に追加する**

1. 左側のバーで、「**Data Service**」>「**Data Library**」ページを選択します。



2. 上部のバーで、「**Custom Device Repository**」タブを選択してください。
3. 「**+Add**」をクリックしてデバイスリポジトリを追加し、基本パラメータを設定します。



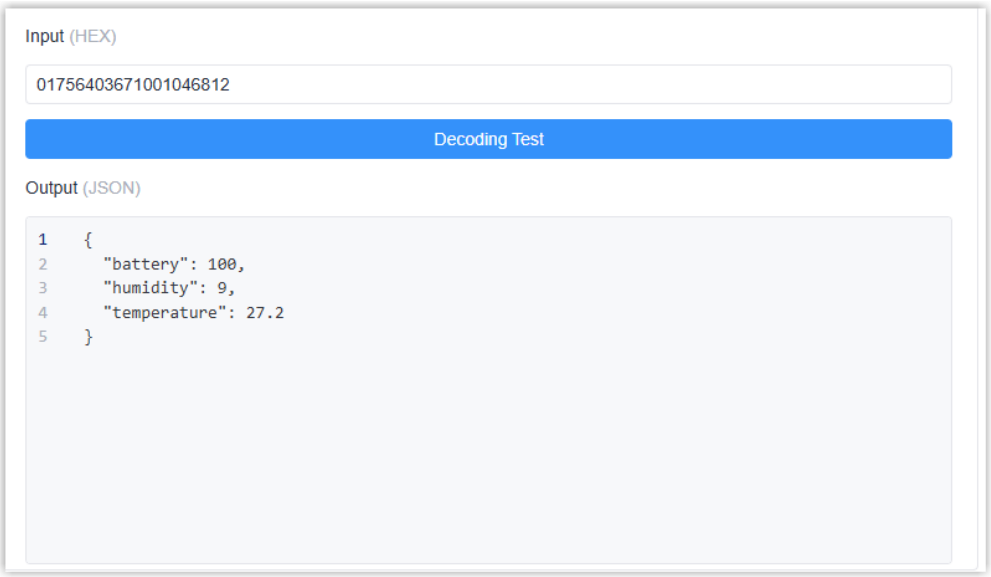
Parameter	説明
Device Model	デバイスモデル名を設定します。
Template	組み込みのデバイスリポジトリからテンプレートを選択してください。これは、Milesight LoRaWAN® デバイスモデルに合わせてカスタムコンテンツを調整する場合に適しています。サードパーティ製デバイスやその他のプロトコルタイプの場合は、「None」を選択してください。
Protocol Type	デバイスモデルのプロトコルタイプを選択してください。
Description	このデバイスモデルに関する説明です。
Protocol type is LoRaWAN®	
DevEUI Prefix (9 chars)	デバイス EUI の最初の 9 文字を設定します。
Device-Profile	このモデルのデバイスプロファイルを選択してください。

4. LoRaWAN® 対応デバイス用のペイロードデコーダーおよびエンコーダーを追加してください。
その他のプロトコルタイプの場合は、この手順をスキップしてください。

   a. デコーダーを追加して、16進形式の生データをJSON形式の結果にデコードするか、エンコーダーを追加して、JSON形式のコマンドを16進形式の生コマンドにエンコードします。対応言語はJavaScript ES2020です。

   注：
   デコーダーとエンコーダーの両方に変数が含まれる場合、使用する変数名は同一でなければなりません。

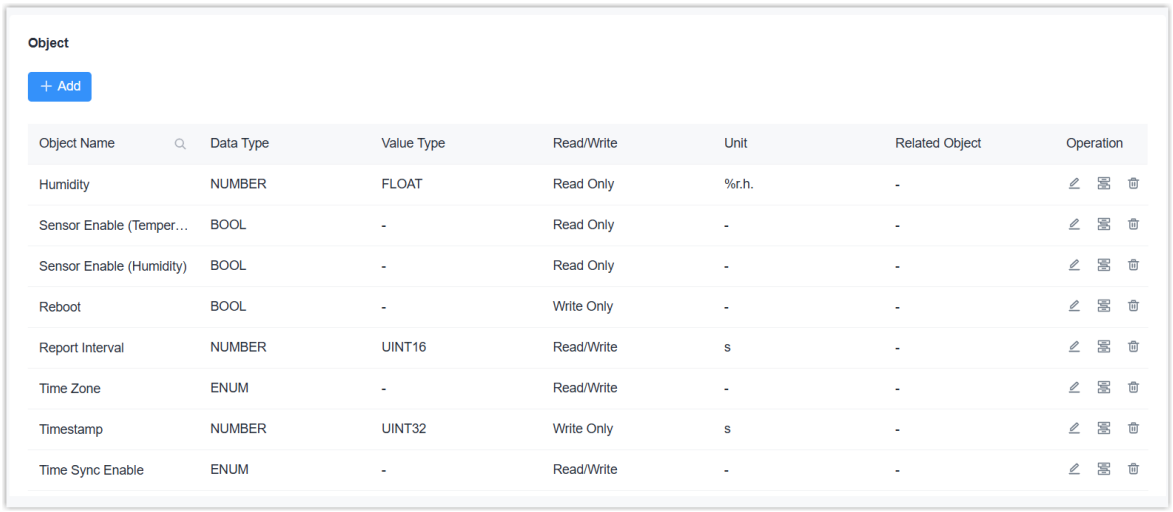
   b. HEX形式の生データを入力し、「**Decoding Test**」をクリックして、デコーダーが正常に動作するか確認してください。



c. JSON形式のコンテンツを入力し、「**Encoding Test**」をクリックして、エンコーダーが正常に動

作するか確認してください。

5. 「**+Add**」をクリックしてオブジェクトを追加します。また、オブジェクトリスト内の「 」をクリックして、オブジェクトリスト内のオブジェクトパラメータを調整することもできます。



6. プロトコルタイプに応じてオブジェクト情報を設定してください。

LoRaWAN

Parameter	説明
Object Name	このオブジェクトの一意の名前を定義します。
Object Description	このオブジェクトに関するメモです。
Data Type	このオブジェクトのデータ型を選択し、関連するパラメータを設定してください。 **BOOL**：0 または 1 の状態の値を設定します。 **ENUM**：列挙数の数と各列挙値を設定します。 **NUMBER**：データ値の型を選択します。 **TEXT:** 文字列の最大長を設定します。
Read/Write	このオブジェクトのアクセスモードを選択します。
BACnet Forward	
BACnet Forward	有効または無効にして、このオブジェクトを BACnet オブジェクトに変換します。
Object Type	BACnet オブジェクトタイプを選択します。データタイプおよび読み取り/書き込みオプションを選択すると、デバイスはオブジェクトタイプおよび BACnet パラメータの一部を自動的に照合します。
Polarity	バイナリ入力/出力/値の状態を「Normal」または「Reverse」から選択します。

Parameter	説明
Active Text	バイナリ入力／出力／値型のアクティブ状態を示すテキストを追加してください。これは「値 1」と同じです。
Inactive Text	バイナリ入力/出力/値タイプのアクティブ状態を示すテキストを追加します。これは値 0 と同じです。
Number of States	オブジェクトタイプが MultiState タイプの場合、状態の数を設定します。これは列挙番号と同じです。 **StateText：**各状態を示すテキストを追加します。これは「列挙値」と同じです。
Relinquish Default	アナログ出力、バイナリ出力、またはマルチステート出力タイプのデフォルトの値を設定します。
Modbus Forward	
Modbus Forward	このオブジェクトを Modbus オブジェクトに変換するかどうかを有効または無効にします。
Register Type	データ型および読み取り/書き込みオプションに応じて、Modbus レジスタタイプを選択します。 **Discrete Input：**BOOL タイプおよび読み取り専用アクセスを選択する場合に選択してください**Coil：**BOOL タイプを選択する場合に選択してください **InputRegister：**ENUM、NUMBER、または TEXT タイプおよび読み取り専用を選択する場合に選択してください **Holding Register：**ENUM、NUMBER、または TEXT タイプを選択する場合に選択してください。
Data Format	レジスタタイプが「入力レジスタ」または「保持レジスタ」の場合、データタイプを選択します。
Register Quantity	データ形式に基づいて数量が表示されます。

BACnet/IP または BACnet MS/TP

Parameter	説明
Object Name	このオブジェクトの一意の名前を定義します。
Object Description	このオブジェクトに関するメモです。

Parameter	説明
Data Type	オブジェクトタイプを選択してください。
Object Instance Nr	一意のオブジェクトインスタンス番号を設定します。

Modbus TCP/RTU または TCP 経由の Modbus RTU

Parameter	説明
Object Name	このオブジェクトに一意の名前を定義します。
Register Type	Modbus レジスタタイプを選択してください。 **Discrete Input**：オン／オフの値を読み取ります。 **Coil**：オン／オフの値を読み書きします。 **Input Register**：測定値とステータスを読み取ります。 **Holding Register**：設定値を読み書きします。
Data Format	レジスタタイプが「入力レジスタ」または「保持レジスタ」の場合、データ型を選択してください。
Register Quantity	データ形式に基づいて数量を表示します。
Register Address	レジスタ内のこのオブジェクトの値を読み書きするための開始アドレスを設定します。
Unit	レジスタタイプが「入力レジスタ」または「ホールドレジスタ」の場合、この値の単位を選択します。
Object Description	このオブジェクトに関する注記用です。
BACnet Forward	
BACnet Forward	このオブジェクトを BACnet オブジェクトに変換するかどうかを有効または無効にします。
Object Type	BACnet オブジェクトタイプを選択します。レジスタタイプを選択すると、デバイスは自動的にオブジェクトタイプに一致します。
Polarity	バイナリ入出力／値の状態を「通常」または「反転」から選択してください。
Active Text	バイナリ入力/出力/値タイプのアクティブ状態を示すテキストを追加します。

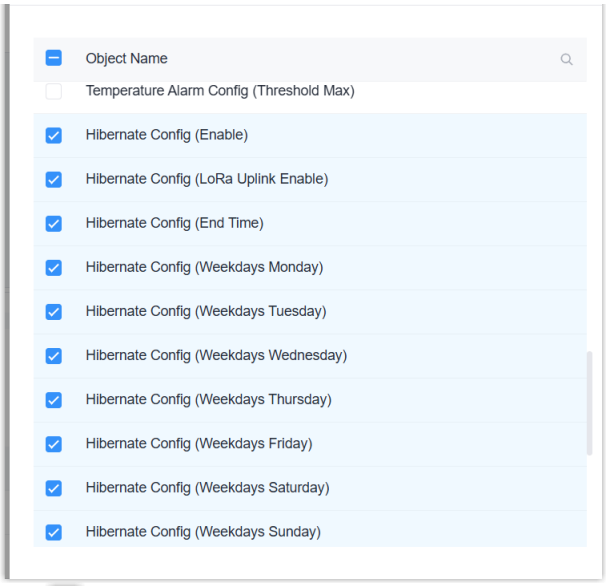
Parameter	説明
Inactive Text	バイナリ入力/出力/値タイプの非アクティブ状態を示すテキストを追加します。
Number of States	オブジェクトタイプが MultiState タイプの場合、状態の数を設定します。
State Text	オブジェクトタイプが MultiState タイプの場合、各ステータスを示すテキストを追加します。
Relinquish Default	アナログ出力、バイナリ出力、またはマルチステート出力タイプの場合、デフォルトの値を設定します。

KNX/TP

Parameter	説明
Object Name	このオブジェクトの一意の名前を定義します。
Object Description	このオブジェクトに関するメモです。
Datapoint Type	値を定義するには、KNXデータポイントタイプ（DPT）を選択してください。「カスタム」タイプの場合は、データ長を定義する必要があります。
Unit	データポイントタイプを選択した後、データの単位が表示されます。
Access Mode	このオブジェクトのアクセスモードを選択します。
BACnet Forward	
BACnet Forward	このオブジェクトを BACnet オブジェクトに変換するかどうかを有効または無効にします。
Object Type	BACnet オブジェクトタイプを選択してください。データポイントタイプを選択すると、デバイスは自動的にオブジェクトタイプに一致します。
Polarity	バイナリ入力/出力/値の状態を「Normal」または「Reverse」から選択します。
Active Text	バイナリ入力／出力／値型のアクティブ状態を示すテキストを追加してください。
Inactive Text	バイナリ入力/出力/値タイプの非アクティブ状態を示すテキストを追加します。
Number of States	オブジェクトタイプが MultiState タイプの場合、ステータスの数を設定します。

Parameter	説明
State Text	オブジェクトタイプが MultiState タイプの場合、各ステータスを示すテキストを追加します。
Relinquish Default	アナログ出力、バイナリ出力、またはマルチステート出力タイプのデフォルトの値を設定します。
Modbus Forward	
Modbus Forward	このオブジェクトを Modbus オブジェクトに変換するかどうかを有効または無効にします。
Register Type	Modbus レジスタタイプを選択します。データポイントタイプを選択すると、デバイスは自動的にレジスタタイプに一致します。
Data Format	レジスタの種類が「入力レジスタ」または「ホールドレジスタ」の場合、データ型を選択してください。
Register Quantity	データ形式に基づいて数量を表示します。

7. **[Save]** をクリックして、このオブジェクトを保存します。
8. オブジェクトを他のオブジェクトと同時に書き込む必要がある場合は、オブジェクトリスト

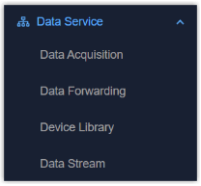


で [] をクリックして、関連するオブジェクトを追加してください。

9. **[Apply]** をクリックして、このカスタム デバイス モデルを保存します。

デバイスモデルを一括で追加する

1. 左側のバーで、**[Data Service] > [Data Library]** ページを選択します。



2. 上部のバーで、**[Custom Device Repository]** タブを選択します。
3. カスタムデバイスリポジトリが少なくとも1つある場合は、すべてを選択し、「**Batch Export**」をクリックして.ZIPファイルをエクスポートしてください。

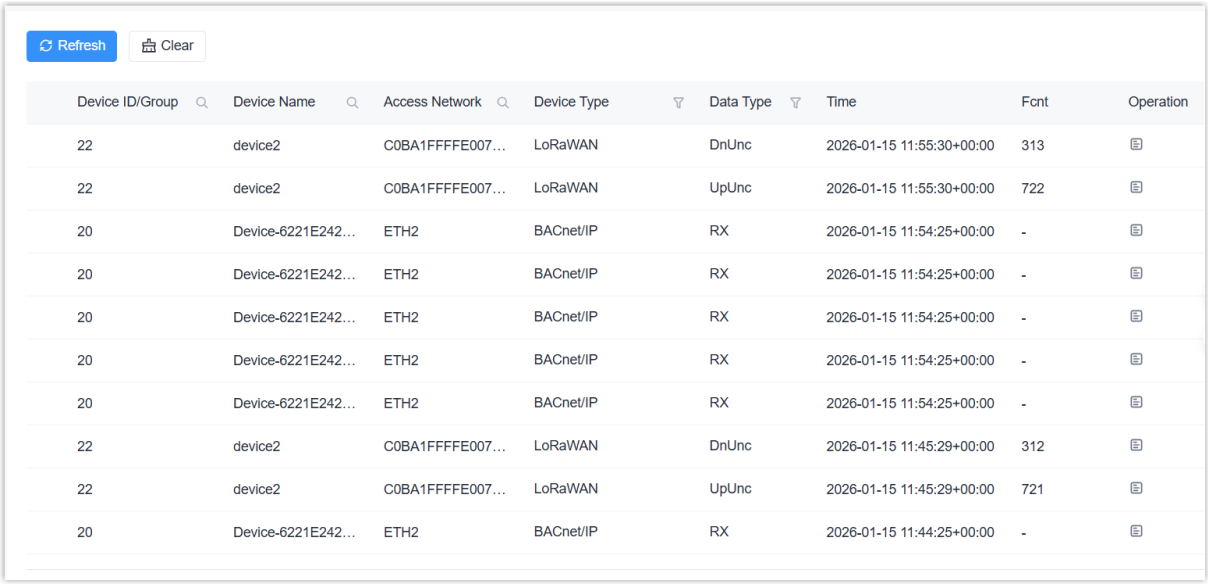
> **ヒント：**
> 1つ以上のデバイスを手動で追加してからファイルをエクスポートし、フォーマットを確認することをお勧めします。

4. エクスポートしたファイルを変更して、新しいデバイスモデルを追加してください。
5. 「**Import**」をクリックし、ローカルパスからデバイスリポジトリの.ZIPファイルを選択してください。インポート完了後、デバイスのインポート結果が表示されます。

> **注：**
> ファイルをインポートする際、デバイスはリポジトリに追加するのではなく、上書きします。

データストリーム

このページは、接続されたデバイスとゲートウェイ間の通信パケットを表示するために使用されます。



Parameter	説明
Refresh	クリックすると、最新のデータストリームレコードが更新されます。
Clear	クリックすると、すべてのデータストリームレコードがクリアされます。
Device ID/Group	デバイスIDまたはマルチキャストグループ名を表示します。
Device Name	デバイス名またはマルチキャストグループ名を表示します。
Access Network	LoRaWAN® デバイスの EUI または使用されているインターフェース名を表示します。
Device Type	デバイスのプロトコルタイプを表示します。
Data Type	データタイプを表示します。LoRaWAN® デバイスでは、JnAcc (Join Accept)、JnReq (Join Request)、UpUnc (Uplink Unconfirmed)、UpCnf (Uplink Confirmed)、DnUnc (Downlink Unconfirmed)、または DnCnf (Downlink Confirmed) が表示され、その他のデバイスでは TX または RX が表示されます。
Time	このデータパケットを受信または送信した時刻を表示します。
Fcnt	LoRaWAN® パケットの Fcnt を表示します。
Operation	をクリックして、データ内容を含むパケットの詳細を確認してください。

第6章 ネットワーク

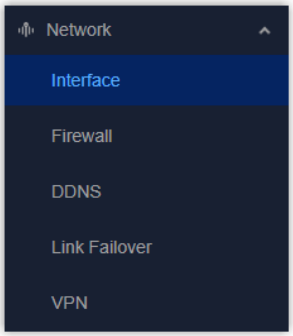
インターフェース

イーサネット

このデバイスには 2 つのイーサネットポートがあります。この章では、これらのイーサネットポートの設定方法について説明します。

手順

1. 左側のバーで、「**Network**」>「**Interface**」ページを選択します。



2. 上部のバーで、「**Ethernet**」タブを選択します。
3. ポートモードとして、「Standalone Mode」または「Bridge Mode」を選択します。

   スタンドアロンモード：各イーサネットポートは、WANポートまたはLANポートとして機能します。

   ブリッジモード：2つのイーサネットポートがブリッジ接続され、透過転送が行われます。

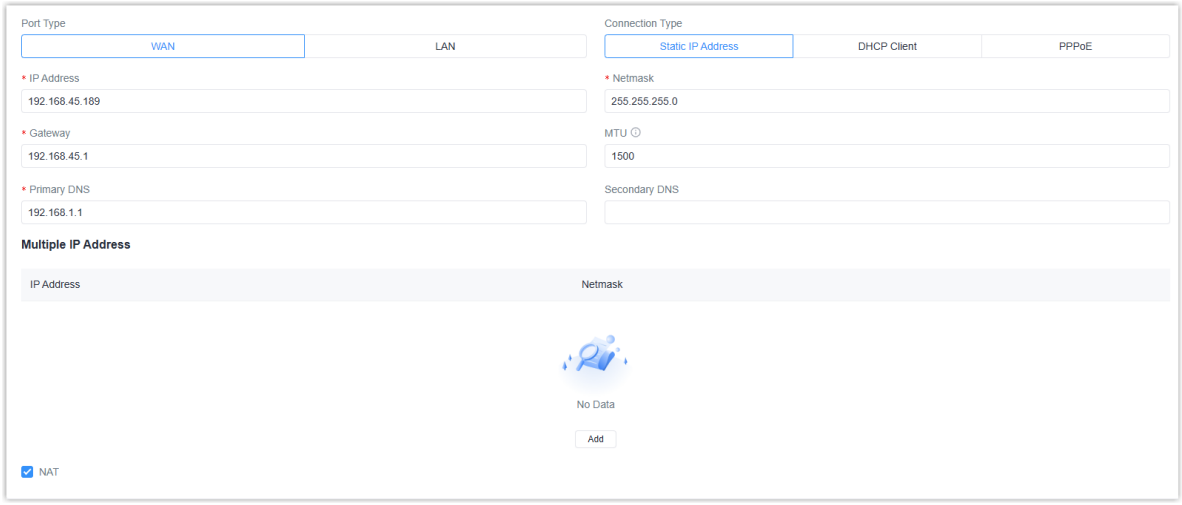
4. ポートモードに応じて、イーサネットパラメータを設定してください。
   - スタンドアロン-WAN 設定
   - スタンドアロン-LAN 設定
   - ブリッジモードの設定
5. 「インターフェース設定」でイーサネットポートを有効または無効にします。
6. 「**Apply**」をクリックして設定を保存してください。
7. イーサネットポートをデバイスに接続した後、画面を確認するか、**[ステータス]** ページに移動して、イーサネットポートの接続状態を確認してください。
8. リンクフェイルオーバー設定を構成し、ETHインターフェースまたはブリッジインターフェースをネットワークリンクとして有効にします。

スタンドアロンモード - WAN設定

イーサネットポートがWANポートとして機能し、外部ネットワーク（インターネット）に接続する場合、以下の3種類の接続方式に対応しています：

1. 固定IPアドレス

このWANポートに手動で静的IPアドレスを割り当てます。



Parameter	説明
IP Address	このインターフェースの IPv4 アドレスです。このアドレスは、ゲートウェイアドレスと同じサブネットに属している必要があります。
Netmask	このインターフェースのIPv4ネットマスクです。
Gateway	このWANポートのIPv4ゲートウェイアドレスです。
MTU	このインターフェースを通過するパケットの最大伝送単位です。
Primary DNS	プライマリ DNS サーバーのアドレスです。
Secondary DNS	プライマリ DNS サーバーが機能しない場合のセカンダリ DNS サーバーのアドレスです。
Multiple IP Address	**Add**] をクリックして、このインターフェースに IP アドレスとネットマスクを追加します。
NAT	このインターフェースのNATを有効または無効にします。

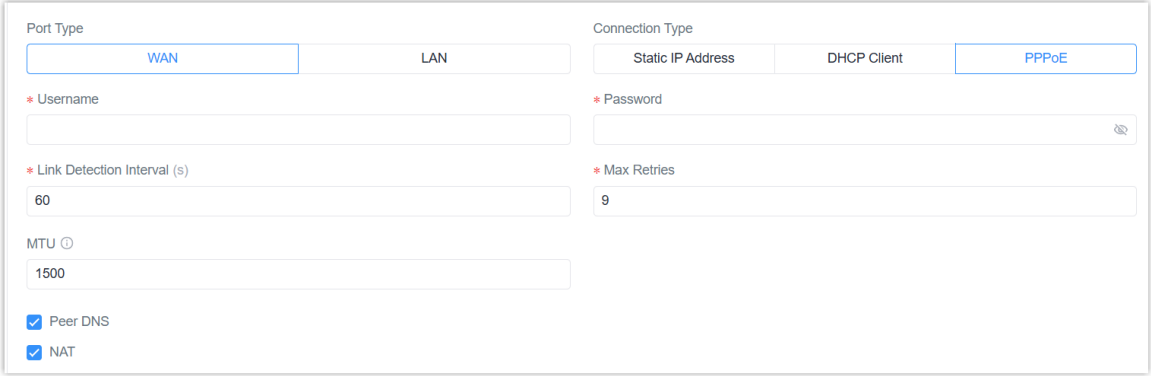
2. DHCPクライアント

DHCP サーバーから IPv4 アドレスを自動的に取得します。

Parameter	説明
MTU	このインターフェースを通過するパケットの最大伝送単位です。
Peer DNS	相手先のDNSサーバーのアドレスを使用します。無効にしている場合は、プライマリDNSサーバーとセカンダリDNSサーバーを手動で設定する必要があります。
NAT	このインターフェースのNATを有効または無効にします。

3. PPPoE

イーサネットポート経由で PPP (Point-to-Point Protocol) 接続を設定し、IP アドレスを取得します。

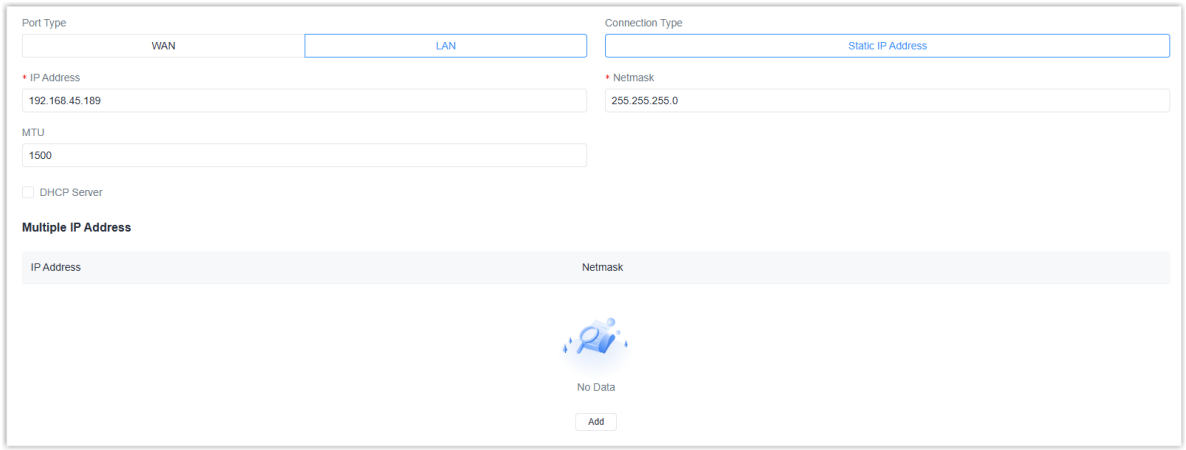


Parameter	説明
Username	PAP/CHAP 認証用のユーザー名です。
Password	PAP/CHAP 認証用のパスワードです。
Link Detection Interval	リンクの状態を検出するためにハートビートパケットを送信する間隔です。
Max Retries	ダイヤルがフェイルした場合の最大再試行回数です。
MTU	このインターフェースを通過するパケットの最大伝送単位です。実際のMTU値は、設定値から8を引いた値となります。

Parameter	説明
Peer DNS	相手先のDNSサーバーのアドレスを使用します。無効にしている場合は、プライマリDNSサーバーとセカンダリDNSサーバーを手動で設定する必要があります。
NAT	このインターフェースのNATを有効または無効にします。

スタンドアロンモード - LAN設定

イーサネットポートが、ローカル相互接続およびデータ共有のために内部デバイスを接続する LAN ポートとして機能する場合。



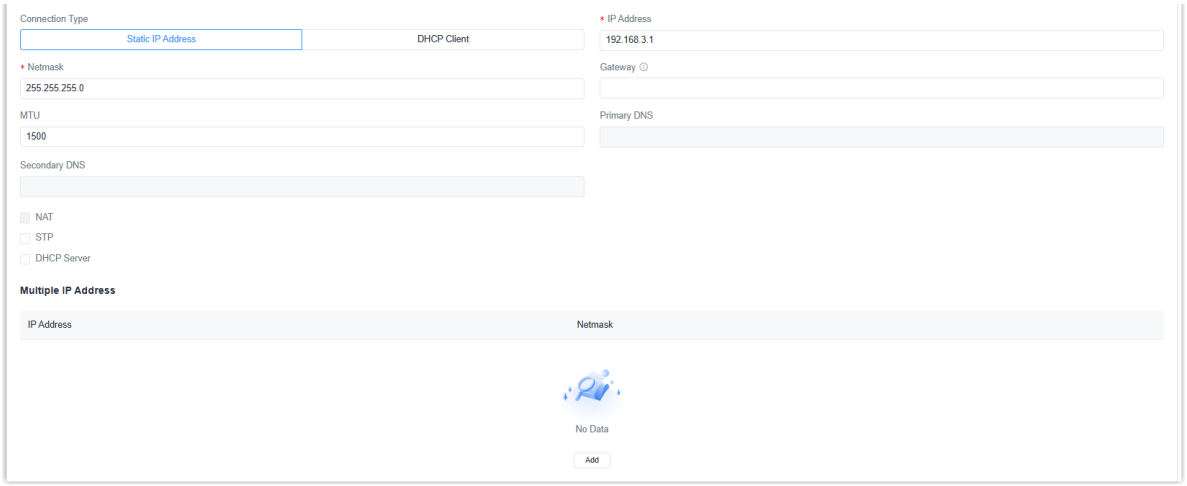
Parameter	説明
IP Address	このインターフェースの IPv4 アドレスです。
Netmask	このインターフェースのIPv4ネットマスクです。
MTU	このインターフェースを通過するパケットの最大伝送単位です。
Multiple IP Address	**Add**] をクリックして、このインターフェースに IP アドレスとネットマスクを追加します。
DHCP Server	
DHCP Server	DHCP サーバーを有効にすると、接続されたクライアントデバイスに IP アドレスが自動的に割り当てられます。無効の場合、クライアントデバイスは各自で IP アドレスを設定する必要があります。
Start Address	IP アドレスを割り当てる IP 範囲の開始 IP アドレスを設定します。
End Address	IP アドレスを割り当てる IP 範囲の終了 IP アドレスを設定します。
Lease Time	クライアントがDHCPサーバーから割り当てられたIPアドレスを使用できるリース期間を設定します。この期間が終了すると、クライアントは新しいリースを要求する必要があります。

Parameter	説明
Primary DNS	プライマリ DNS サーバーのアドレスです。
Secondary DNS	プライマリ DNS サーバーが機能しない場合のセカンダリ DNS サーバーのアドレスです。
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指定します。通常は空欄のままにしておいてください。
MAC Binding	**Add** をクリックして、クライアントの MAC アドレスごとに特定の IP アドレスを特定のクライアントに紐付けます。

ブリッジモード設定

両方のイーサネットポートは同じ設定を共有し、2 種類の接続タイプに対応しています：

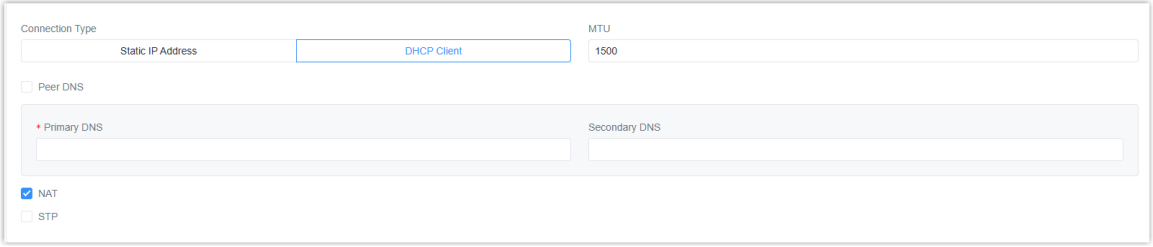
1. 静的IPアドレス



Parameter	説明
IP Address	このインターフェースのIPv4アドレスです。外部ネットワークに接続する必要がある場合、このアドレスはゲートウェイアドレスと同じサブネットに属している必要があります。
Netmask	このインターフェースのIPv4ネットマスクです。
Gateway	外部ネットワークに接続する必要がある場合、このインターフェースの IPv4 ゲートウェイアドレスを入力してください。
MTU	このインターフェースを通過するパケットの最大伝送単位です。
Primary DNS	ゲートウェイアドレスを入力した場合は、プライマリDNSサーバーのアドレスを設定してください。
Secondary DNS	ゲートウェイアドレスを入力する場合、セカンダリDNSサーバーのアドレスを設定します。

Parameter	説明
NAT	ゲートウェイアドレスを入力した際、このインターフェースのNATを有効または無効にします。
STP	このインターフェースの STP を無効または有効にします。
Multiple IP Address	**Add]** をクリックして、このインターフェースに IP アドレスとネットマスクを追加します。
DHCP Server	
DHCP Server	DHCPサーバーを有効にすると、接続されたクライアントデバイスにIPアドレスが自動的に割り当てられます。無効にしている場合、クライアントデバイスは各自でIPアドレスを設定する必要があります。
Start Address	IPアドレスを割り当てるIP範囲の開始IPアドレスを設定します。
End Address	IP アドレスを割り当てる IP 範囲の終了 IP アドレスを設定します。
Lease Time	クライアントがDHCPサーバーから割り当てられたIPアドレスを使用できるリース期間を設定します。この期間が終了すると、クライアントは新しいリースを要求する必要があります。
Primary DNS	プライマリDNSサーバーのアドレスです。
Secondary DNS	プライマリDNSサーバーが機能しない場合のセカンダリDNSサーバーのアドレスです。
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指定します。通常は空欄のままにしておいてください。
MAC Binding	**Add** をクリックして、クライアントの MAC アドレスごとに特定の IP アドレスを特定のクライアントに紐付けます。

2. DHCP クライアント

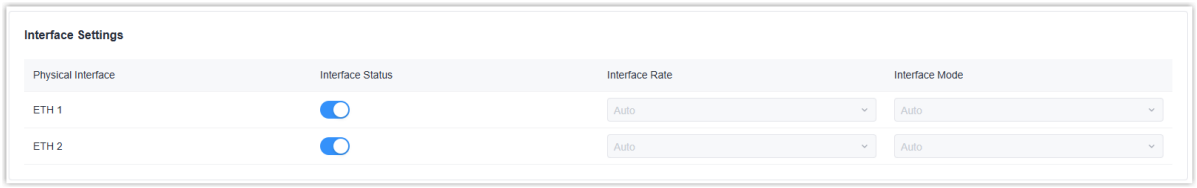


Parameter	説明
MTU	このインターフェースを通過するパケットの最大伝送単位です。
Peer DNS	相手先のDNSサーバーのアドレスを使用します。無効にしている場合は、プライマリDNSサーバーとセカンダリDNSサーバーを手動で設定する必要があります。

Parameter	説明
NAT	このインターフェースのNATを有効または無効にします。
STP	このインターフェースの STP を無効または有効にします。

インターフェース設定

必要に応じて、ETHインターフェースを有効または無効にします。



Cellular

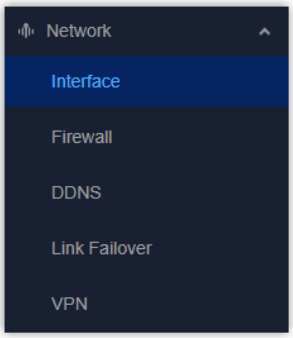
この章では、セルラーネットワークに登録するための設定方法について説明します。

前提条件

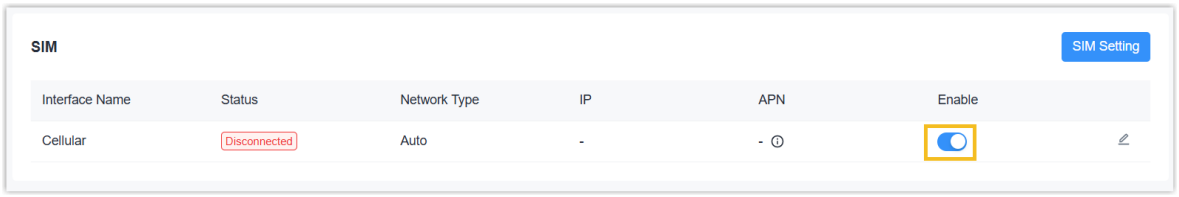
- SIMカードの対応周波数が、デバイスのモデルと一致していること。
- SIMカードの残高が十分にあること、および他の端末で正常に動作することを確認してください。
- 端末にSIMカードと携帯電話用アンテナが正しく取り付けられていることを確認してください。
- 携帯電話事業者からSIMカードの情報を入手してください。

手順

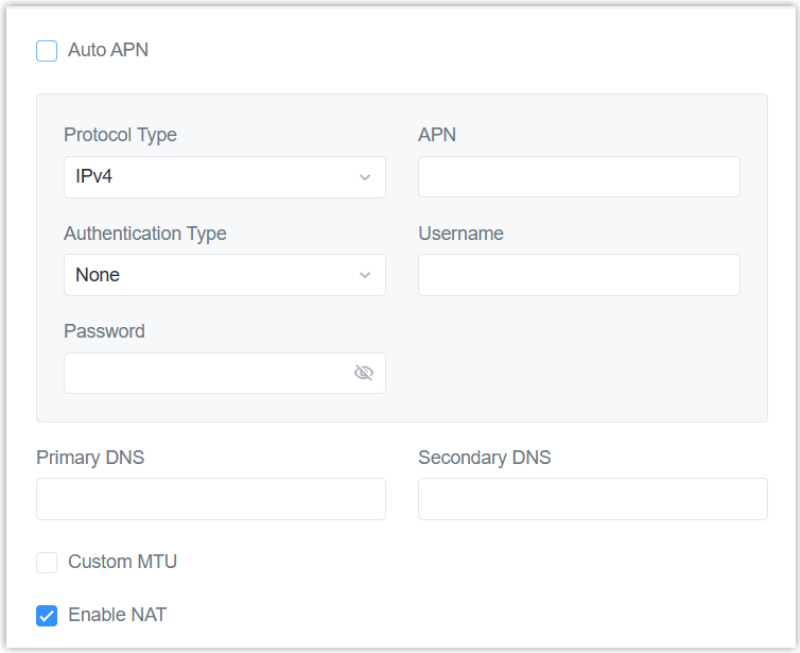
1. 左側のバーで、**[Network] > [Interface]** ページを選択します。



2. 上部のバーで、「**Cellular**」タブを選択します。
3. セルラーインターフェースを有効にしてください。



4. クリックして　をクリックして、このSIMカードの設定を行います。必要がない場合は、この手順をス

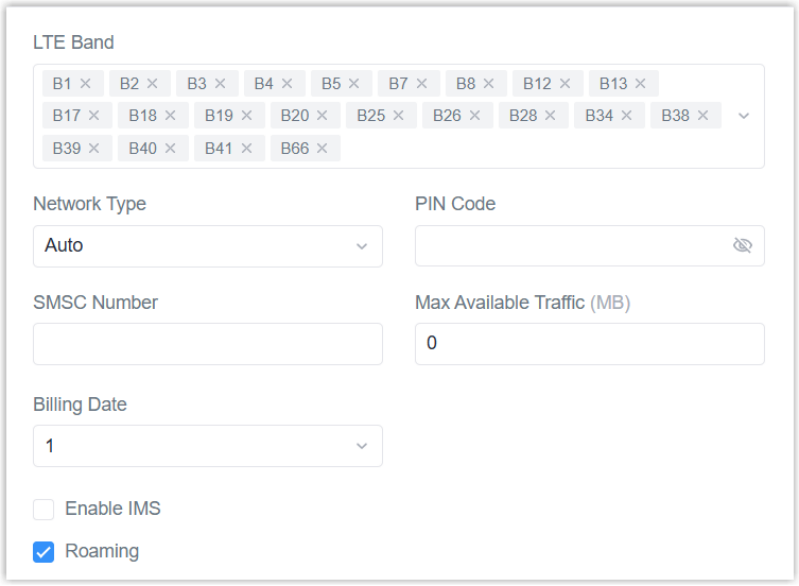


キップしてください。

Parameter	説明
Auto APN	有効にすると、デバイスは内部のAPNデータベースをスキャンし、SIMカードの通信事業者および国に基づいてAPNを選択します。最初に自動的に選択されたAPNが機能しない場合、内部データベースから次のAPNを使用しようとします。 無効にしている場合は、以下のパラメータを設定してカスタムAPN情報を指定してください： **Protocol Type**：タイプを「IPv4」または「IPv4/IPv6」に設定してください。 **APN**：携帯電話の登録および接続する外部ネットワークを指定するためのアクセスポイント名を設定します。使用できるのは英字、数字、ハイフン（-）、ピリオド（.）のみです。また、先頭文字はアンダーバー（_）またはピリオド（.）にしてはいけません。最大文字数は63文字です。 **Authentication**：通信事業者のネットワーク上で新しい接続を認証する方法を設定します。

Parameter	説明
	Username：携帯電話の登録に使用するユーザー名を設定します。 **Password**：セルラー登録用のパスワードを設定します。
Primary DNS	セルラーのプライマリ DNS サーバーをカスタマイズします。空白のままにすると、デバイスは通信事業者の設定を使用します。
Secondary DNS	セルラーのセカンダリ DNS サーバーをカスタマイズします。空白のままにすると、デバイスは通信事業者の設定を使用します。
Custom MTU	最大送信単位（MTU）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、デバイスは通信事業者のMTU設定を使用します。
Enable NAT	NATを有効または無効にします。

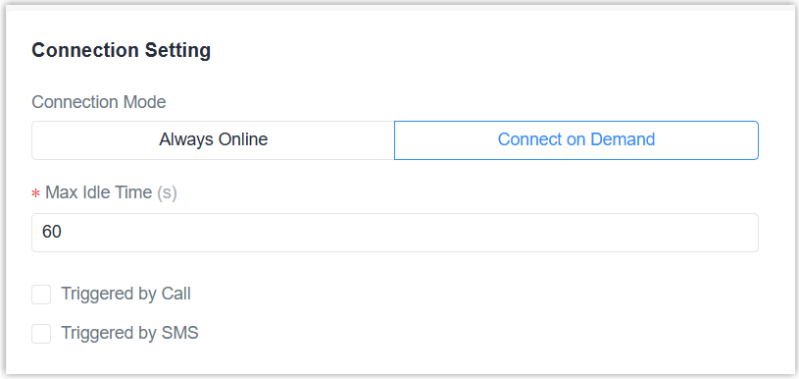
5. 「**SIM Setting**」をクリックして、すべてのインターフェースのSIMパラメータを設定します。必要がない場合は、この手順をスキップしてください。



Parameter	説明
LTE Band	モバイルネットワークの登録に使用する周波数帯を選択してください。特定の周波数帯を選択することで、モバイル通信の速度を最適化することができます。
Network Type	「Auto」、「4Gのみ」などから選択してください（オプションは機種によって異なります）。
PIN Code	SIMのロックを解除するための4～8文字のPINコードを設定してください。
SMSC Number	SMSメッセージの保存、ルーティング、または配信を行うハブ番号を設定します。この機能は、-L08GLモデルのみで利用可能です。

Parameter	説明
Max Available Traffic	この制限に達すると、請求日までSIMカードは使用できなくなります。0は制限なしを意味します。
Billing Date	利用可能なトラフィックデータをリセットする月の日付を選択してください。
IPv4 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。空欄のままにすると、デバイスは通信事業者の設定を使用します。この機能は-L09NAモデルのみ利用可能です。
Enable IMS	IMS機能を有効または無効にします。この機能は-L08GLモデルのみで利用可能です。
Roaming	ローミングを有効または無効にします。

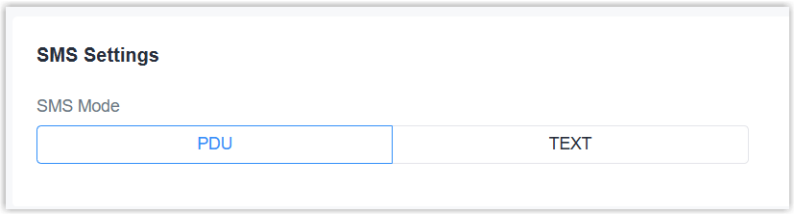
6. 必要に応じて接続モードを選択します。この機能は-L08GLモデルのみ利用可能です。



「**Connect on Demand**」が選択されている場合は、以下のパラメータを設定してください：

Parameter	説明
Max Idle Time	この時間内にセルラーデータ通信がない場合、セルラー接続を切断します。
Triggered by Call	有効にすると、選択した通話グループのいずれかの番号から着信があった後、デバイスはモバイルネットワークへの登録を試みます。
Triggered by SMS	有効にすると、本デバイスは、選択したSMSグループ内の任意の番号から特定のSMSメッセージを受信した後、携帯電話ネットワークへの登録を試みます。

7. 必要に応じて、SMSモードをPDUまたはTEXTから選択してください。この機能は-L08GLモデルのみで利用可能です。



8. **[Apply]** をクリックして設定を保存してください。
9. セルラーのステータスが「Connected」になっているか確認してください。
10. リンクフェイルオーバー設定を構成し、セルラーインターフェースをネットワークリンクとして有効にしてください。

関連情報

ステータス

リンクフェ

イルオーバ

ーサービス

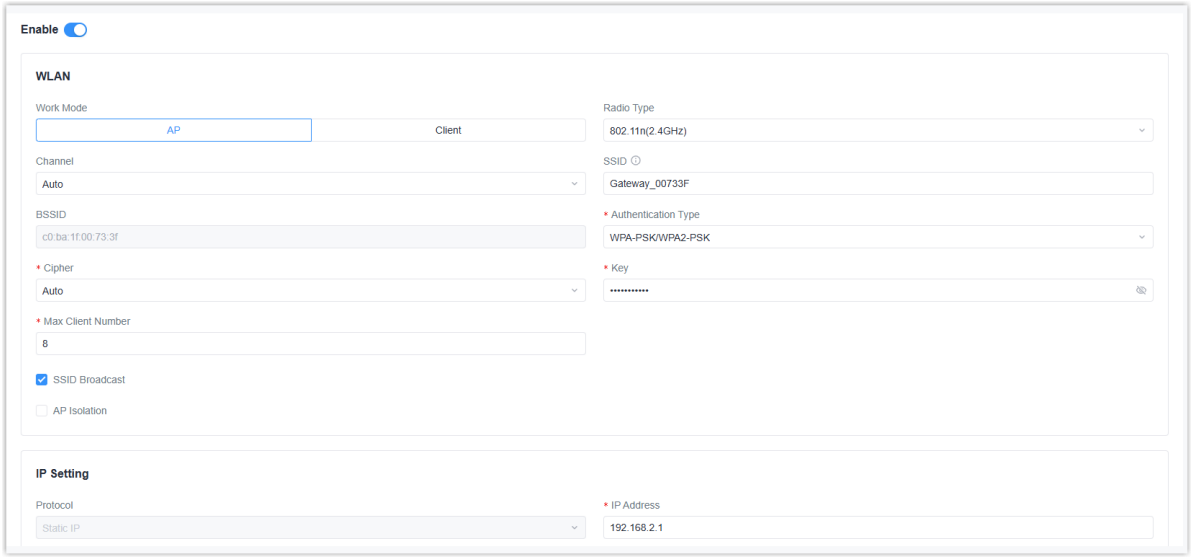
ツール

WLAN

この章では、Wi-Fi 設定の構成方法について説明します。

APモードの設定

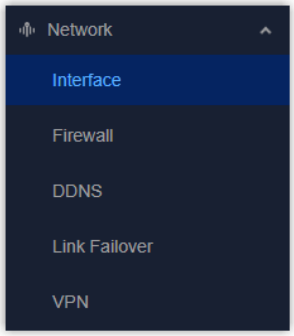
このデバイスは、デバイスのWebアクセスやWi-Fiセンサーの接続用として、アクセスポイントとして機能させ



ることができます。

手順：

1. 左側のバーで、「**Network**」＞「**Interface**」ページを選択してください。



2. 上部のバーで、「**WLAN**」タブを選択します。
3. WLAN機能を有効にしてください。
4. 動作モードとして「AP」を選択し、関連するパラメータを設定します。

Parameter	説明
Radio Type	無線タイプを 802.11b（2.4GHz）、802.11g（2.4GHz）、802.11n（2.4GHz）から選択します。
Channel	データを送信する周波数チャネルを選択してください。 **Tip：** 設置予定場所のチャンネル使用状況を確認するには、Wi-Fiアナライザーツールを使用することをお勧めします。干渉を避け、ネットワーク速度を向上させ、安定性を高めるために、最も混雑していないチャンネルを選択してください。
SSID	このアクセスポイントを識別するために、サービスセット識別子（SSID）を設定してください。デフォルト値は **Gateway_XXXXXX** （＝WLAN MACアドレスの下6桁）です。
BSSID	WLANインターフェースのMACアドレスを表示します。
Authentication Type	接続に使用する認証方式を選択してください。オプション：「暗号化なし」、「WEP」、「WPA-PSK」、「WPA2-PSK」、「WPA-PSK/WPA2-PSK」です。 **Cipher：**暗号化モードが「No Encryption」でない場合、使用する暗号化方式を選択してください。 **Key：**このアクセスポイントに接続するためのキーを設定します。スペースを含まないASCII文字のみ使用可能です。デフォルト値は「**iotpassword**です。

Parameter	説明
Max. Client Number	このアクセスポイントに接続できるクライアントの最大数を設定します。範囲：1～8。
SSID Broadcast	無効にすると、SSIDを直接検索することはできなくなります。ユーザーは、アクセスポイントに接続するためにSSIDを手動で入力する必要があります。
AP Isolation	有効にすると、接続されているすべてのクライアントは互いに通信できなくなります。

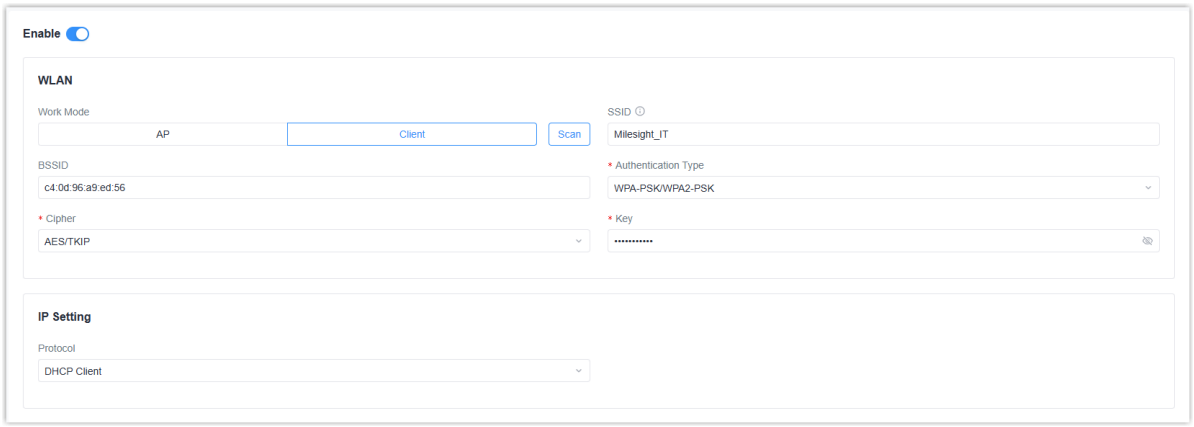
5. 必要に応じて、クライアントデバイスのIP設定を行ってください。

Parameter	説明
Protocol	固定 IP として設定されています。
IP Address	この WLAN インターフェースの IP アドレスを設定します。デフォルト値は **192.168.2.1** です。
Subnet Mask	このWLANインターフェースのサブネットマスクを設定します。
DHCP Server	
DHCP Server	DHCPサーバーを有効にすると、接続されたクライアントデバイスにIPアドレスが自動的に割り当てられます。無効にしている場合、クライアントデバイスは各自でIPアドレスを設定する必要があります。
Start Address	IPアドレスを割り当てるIP範囲の開始IPアドレスを設定します。
End Address	IPアドレスを割り当てるIP範囲の終了IPアドレスを設定します。
Netmask	IP アドレスを割り当てる IP 範囲のネットマスクを設定します。
Lease Time	クライアントがDHCPサーバーから割り当てられたIPアドレスを使用できるリース期間を設定します。この期間が終了すると、クライアントは新しいリースを要求する必要があります。
Primary DNS Server	プライマリ DNS サーバーのアドレスを設定します。
Secondary DNS Server	プライマリ DNS サーバーが機能しない場合に備えて、セカンダリ DNS サーバーのアドレスを設定します。
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。
MAC Binding	**Add**をクリックして、特定のIPアドレスをクライアントのMACアドレスに基づいて特定のクライアントに紐付けます。

6. 「**Apply**」をクリックして設定を保存します。
7. スマートフォンまたはWi-Fiクライアントデバイスをアクセスポイントに接続します。これには、アクセスポイントと同じパラメータが必要です。
8. 接続後、「**Status**」ページに移動し、クライアント情報が表示されているか確認してください。

クライアントモードの設定

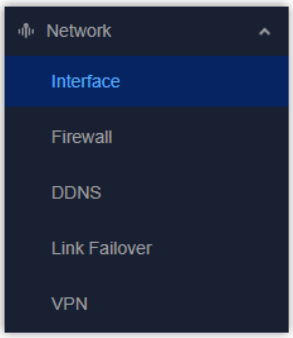
このデバイスは、インターネット接続やWi-Fiセンサーとの接続のために、別のアクセスポイントに接続するクライアントとして機能します。



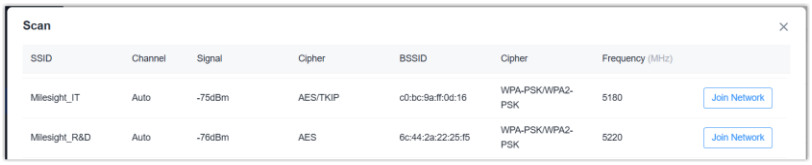
注：
WLANインターフェースをクライアントモードとして設定する必要がある場合は、無線経由でWeb GUIにアクセスしないでください！

手順：

1. 左側のバーで、「**Network**」>「**Interface**」ページを選択します。



2. 上部バーで、「**WLAN**」タブを選択します。
3. WLAN機能を有効にします。
4. 動作モードを「クライアント」に設定し、「**Scan**」をクリックして、デバイス周辺のアクセスポイントを検索します。



5. 利用可能なアクセスポイントを選択し、「**Join Network**」をクリックしてください。
6. 選択すると、アクセスポイントの基本情報が自動的に入力されます。一部のアクセスポイントでは、キー（Wi-Fiパスワード）の入力が必要となります。
7. 必要に応じて、クライアントデバイスのIP設定を行ってください。

Parameter	説明
Protocol	WLAN IP アドレスを受信するモードを選択します。 **DHCP Client**：アクセスポイントから IP アドレスを取得します。 **Static IP**：IP アドレスを手動で割り当てます。
Static IP Setting	
IP Address	アクセスポイントと同じサブネットの WLAN インターフェース IP アドレスを設定します。
Subnet Mask	WLAN インターフェースの IP アドレスのサブネットマスクを設定します。
Gateway	接続先のゲートウェイの IP アドレスを設定します。
Primary DNS Server	プライマリ DNS サーバーのアドレスを設定します。
Secondary DNS Server	プライマリ DNS サーバーが機能しない場合に備えて、セカンダリ DNS サーバーのアドレスを設定します。

8. 「**Apply**」をクリックして設定を保存します。
9. 接続後、「**Status**」ページに移動し、ステータスが「Connected」になっているか確認してください。
10. リンクフェイルオーバー設定を構成し、WLAN インターフェースをネットワークリンクとして有効にしてください。

関連情報

リンクフェイルオーバー

LoRa

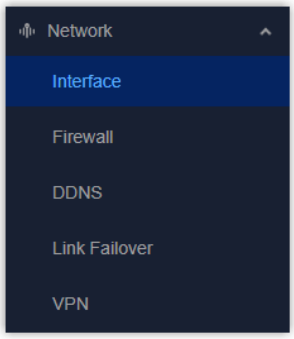
この章では、LoRaWAN® 通信の周波数設定について説明します。

基本設定

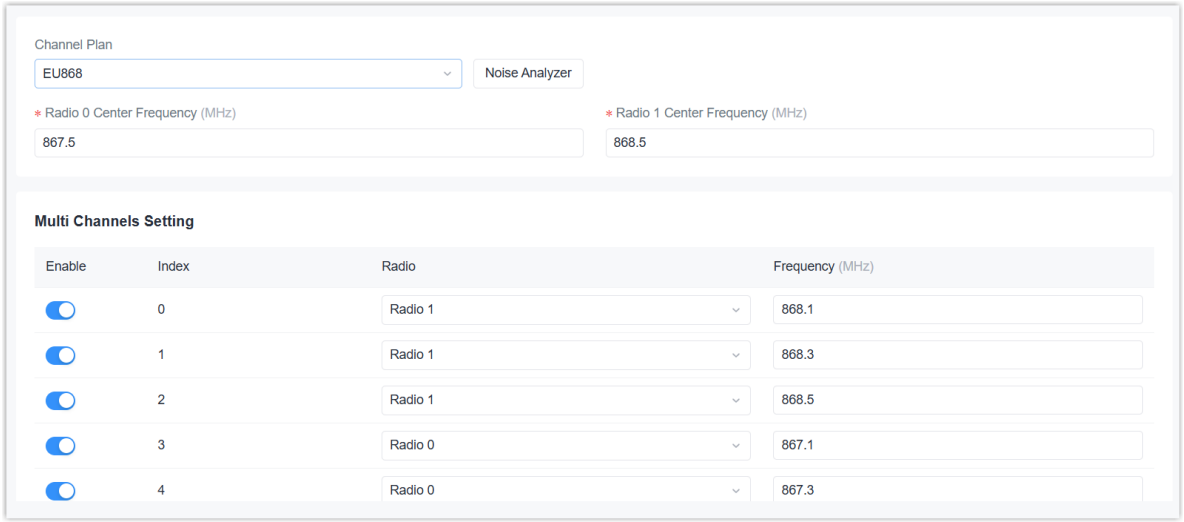
このセクションは、LoRaWAN® デバイスの通信の大部分に使用されます。

手順：

1. 左側のバーで、**[Network] > [Interface]** ページを選択します。



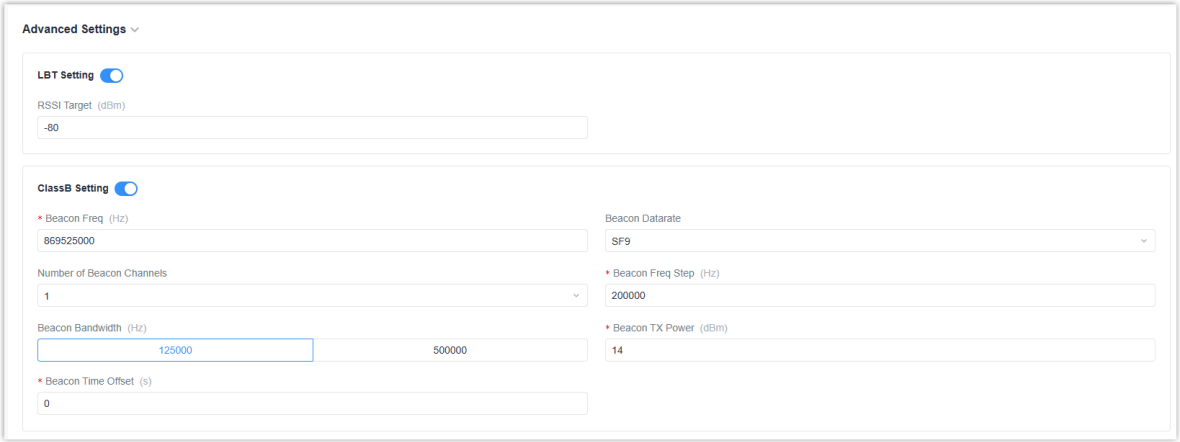
2. 上部バーで、「**LoRa**」タブを選択します。
3. LoRaWAN® エンドデバイスと同じチャネルプランを選択します。
4. 必要に応じて周波数パラメータを設定してください。デフォルト設定のままにすることも可能です。



Parameter	説明
Channel Plan	ネットワークのチャネルプランを選択してください。オプションはモデルによって異なります： -868M: EU868、IN865、RU864 -915M: AU915、US915、KR920、AS923-1/2/3/4 -470M: CN470
Noise Analyzer	詳細はこちらをクリックしてください。

Parameter	説明
Center Frequency	各モジュールの中心周波数を設定します。
Multi Channels Setting	
Enable	パケットを送信するチャンネルを有効または無効にします。
Radio	中心周波数として「Radio 0」または「Radio 1」を選択してください。
Frequency	各チャンネルの周波数を設定します。
LoRa/FSK Channel Setting	
Enable	LoRa/FSK チャンネルを有効または無効にします。
Radio	中心周波数として、Radio 0 または Radio 1 を選択します。
Frequency	LoRa/FSKチャネルの周波数を設定します。
Bandwidth	LoRa/FSKチャネルの帯域幅を設定します。
Data Rate	LoRa/FSKチャネルのデータレートを設定します。

5. 必要に応じて詳細設定を行います。



Parameter	説明
LBT Setting	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はこの機能に対応していません。

Parameter	説明
	RSSI Target：アイドル状態のチャネルの基準を入力します。チャネルの実際の RSSI が基準値/ターゲット値より低い場合、そのチャネルはアイドル状態とみなされます。
Class B Setting	クラスBのエンドデバイスと通信するためにビーコンを送信するかどうかを設定します。 **Beacon Freq**：ビーコンを送信する周波数です。 **Beacon Datarate**：ビーコンを送信するデータレートです。 **Number of Beacon Channels**：使用するビーコンチャネルの数です。 **Beacon Freq Step**：ビーコンを送信する際の周波数ステップです。 **Beacon Bandwidth**：ビーコンの帯域幅です。 **Beacon Tx Power**：ビーコンの送信電力です。 **BeaconTimeOffset**：このオフセットをシステム時刻に加算し、その結果をクラスBデバイスに割り当てます。これにより、複数のクラスBデバイスが近接している場合の干渉を回避できます。

6. **[Apply]** をクリックして設定を保存します。

ノイズアナライザ

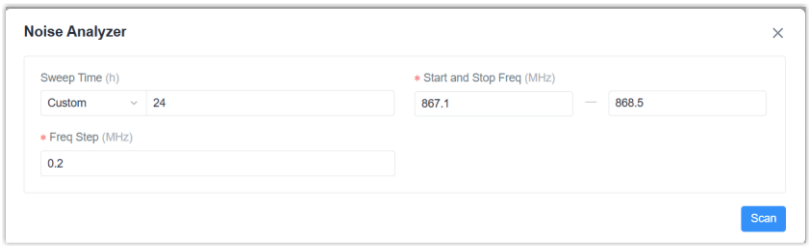
ノイズアナライザは、各周波数チャネルのノイズをスキャンし、ユーザーが環境干渉の状態を分析して最適な配置を選択できるよう、図表を作成するために使用されます。

前提条件

- 本装置は対象場所に設置してください。設置場所を変更する場合は、ノイズアナライザーを再設置してください。
- この機能はLoRaWAN®のダウンリンク通信に影響を与えるため、スウィープ中はデバイスにダウンリンクコマンドを送信しないでください。

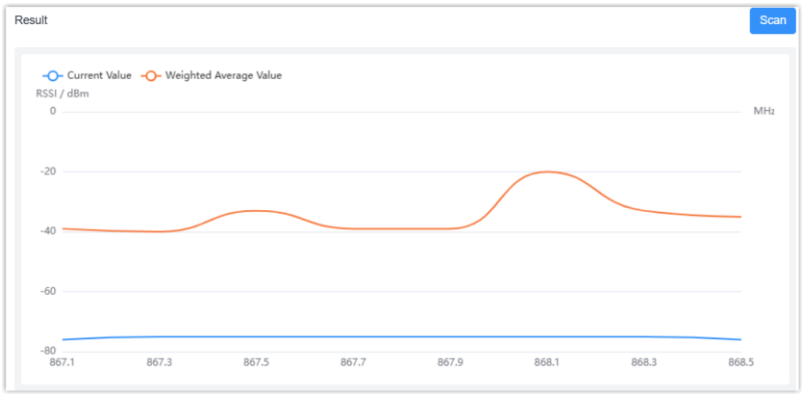
手順：

1. 「**Noise Analyzer**」をクリックします。
2. ポップアップウィンドウで、周波数範囲と時間を設定します。



Parameter	説明
Sweep Time	周波数範囲をスイープする時間を設定します。 **Continuous**：周波数を連続的にスイープします。 **Custom**：周波数をスイープする時間をカスタマイズします。 **Tip**： 正確な結果を得るためには、スイープ時間を24時間に設定することをお勧めします。
Start and Stop Freq	スキャンする周波数範囲を設定してください。
Freq Step	スキャンする各周波数チャネルのステップを設定します。

3. 「**Scan**」をクリックして、周波数のスイープを開始します。
4. 設定した時間が経過すると、デバイスはスキャンを停止します。または、「**Stop Scanning**」をクリックしてください。
5. 分析結果を確認してください。RSSI 値が低いほど、信号の状態は良好です。



6. 「マルチチャンネル設定」で、必要に応じて周波数を調整してください。

RS485

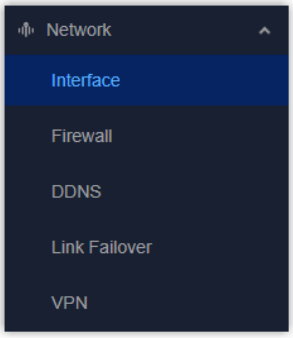
この章では、RS485の基本パラメータの設定方法について説明します。

前提条件

端末デバイスのユーザーガイドまたはメーカーから、RS485 の基本パラメータを収集してください。

手順

1. 左側のバーで、**[Network] > [Interface]** ページを選択します。



2. 上部のバーで、**[RS485]** タブを選択します。
3. 該当する RS485 インターフェースの基本パラメータを設定します。**通常、これらは端末機器の設定と同じである必要があります。**

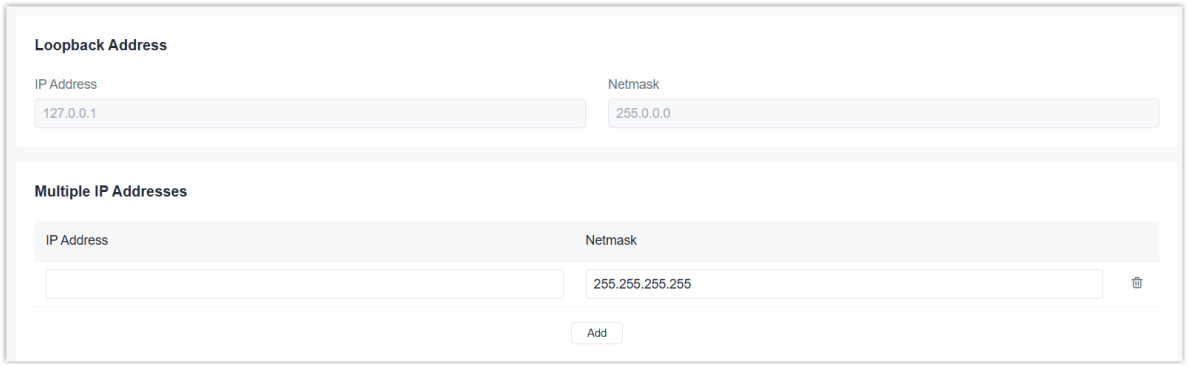
Parameter	説明
Baud Rate	シリアルデータ伝送速度を選択します。
Data Bits	各文字のデータビット数です。8 ビットに固定されています。
Stop Bits	各データフレームの終了を示すもので、受信側がフレームが完了しているかどうかを判断できるようにします。オプション：1、2
Parity	これは、送信中のエラーを検出するために使用されます。オプション：なし、奇数、偶数。
DIP	この設定を有効または無効にすることで、端子AとB間に120Ωの終端抵抗を追加し、ケーブル端からの信号反射を防止します。

4. **[Apply]** をクリックして設定を保存します。

ループバック

ループバックアドレスとは、内部テスト、開発、トラブルシューティングのために、物理的なネットワークを経由せずにデバイスが自身にデータを送信できるようにする、特別に予約されたIPアドレスのことです。これは「localhost」とも呼ばれ、アプリケーションが内部で通信するための仮想インターフェースを構築し、実際のトラフィックに影響を与えることなくネットワークソフトウェアが正常に動作することを確認します。

このページにはデフォルトのループバックアドレスが表示され、必要に応じて追加のループバックアドレスに対応することができます。

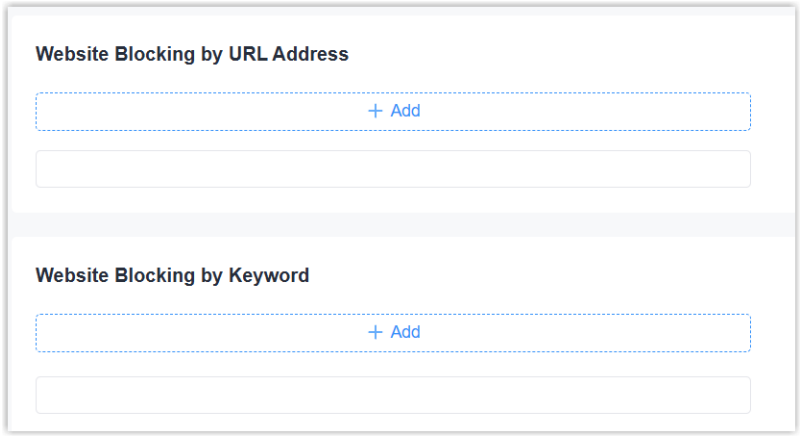


ファイアウォール

この章では、デバイスのセキュリティに関するファイアウォールの設定について説明します。

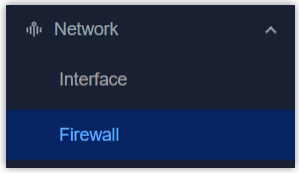
セキュリティ

このページは、LAN ポートに接続されたデバイスが特定の Web サイトにアクセスできないように、URL アドレスまたはキーワードを追加するために使用します。



手順：

1. 左側のバーで、「**Network**」>「**Firewall**」ページを選択します。

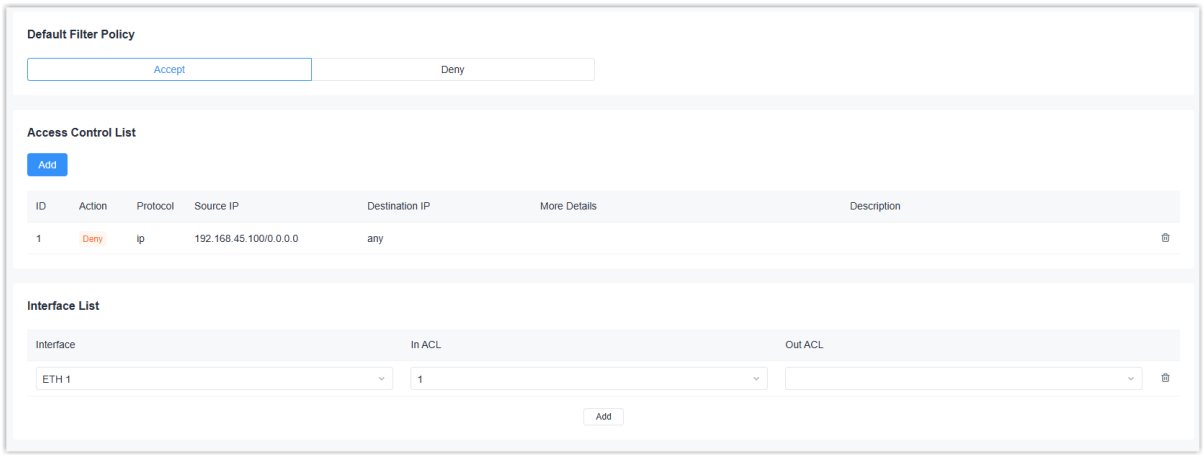


2. 上部のバーで、「**Security**」タブを選択します。

3. 「**+Add**」をクリックして、ブロックするURLアドレスまたはキーワードを追加します。
4. 「**Apply**」をクリックして設定を保存します。

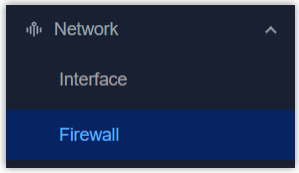
ACL

このページは、ACL ルールの追加および管理に使用します。

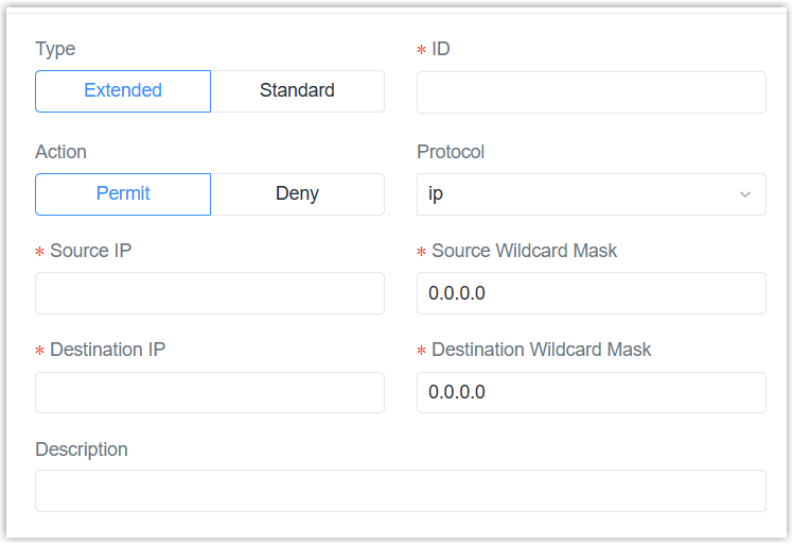


手順：

1. 左側のバーで、「**Network**」>「**Firewall**」ページを選択します。



2. 上部のバーで、「**Security**」タブを選択します。
3. デフォルトのフィルタポリシーとして「Permit」または「Deny」を選択してください。ACLルールに含まれていないパケットは、このポリシーによって処理されます。
4. **[Add]** をクリックして ACL ルールを追加し、関連するパラメータを設定します。



Parameter	説明
Type	ACL タイプを選択します。 **Standard**：送信元IPアドレスのみに基づいてトラフィックをフィルタリングします。 **Extended**：送信元IP、宛先IP、プロトコル、およびポート番号に基づいてトラフィックをフィルタリングし、きめ細かな制御を行います。
ID	このルールに一意の ID を定義します。
Action	パケットがこのルールに一致した場合に実行するアクションを選択します。
Source IP	フィルタリング対象のパケットの送信元IPv4アドレスです。
Source Wildcard Mask	送信元 IP アドレスのワイルドカードマスクです。
Description	このACLルールを注記するためのものです。
Extended Type ACL	
Protocol	フィルタリングするパケットのプロトコルタイプを選択します。
Destination IP	フィルタリングするパケットの宛先 IPv4 アドレスです。
Destination Wildcard Mask	宛先 IP アドレスのワイルドカードマスクです。
ICMP Type	プロトコルがICMPの場合は、フィルタリング対象としてICMPメッセージタイプIDを設定してください。
ICMP Code	プロトコルが ICMP の場合、ICMP メッセージコード ID をフィルタに設定します。
Source Port Type	プロトコルがUDPまたはTCPの場合、送信元ポートの条件を設定してください。

Parameter	説明
	SourcePort：タイプが「None」でない場合は、フィルタリングする特定の送信元ポート番号またはポート範囲を設定します。
Destination Port Type	プロトコルがUDPまたはTCPの場合、宛先ポートの条件を設定してください。 **DestinationPort：**タイプが「None」でない場合は、フィルタリングする特定の宛先ポート番号またはポート範囲を設定してください。

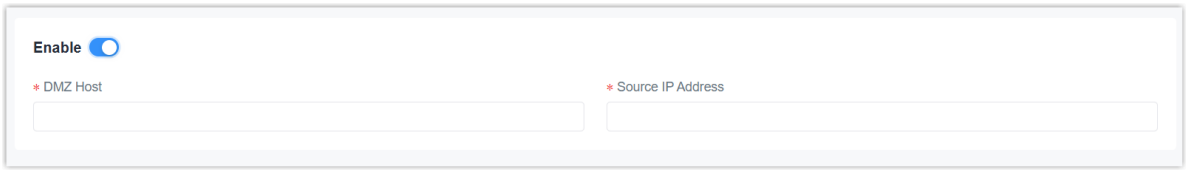
5. ACL ルールを実行するインターフェースと方向を選択してください。

   ACL 内：このインターフェースに受信されるパケットを
   フィルタリングします。ACL 外：このインターフェース
   から送信されるパケットをフィルタリングします。

6. 「**Apply**」をクリックして設定を保存してください。

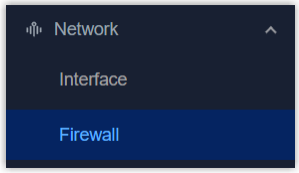
DMZ

このページでは、DMZの設定を行います。DMZ（非武装地帯）は、ファイアウォールが設定されている場合でも、外部ネットワークのユーザーが内部ネットワークのサーバーにアクセスできるようにする機能です。DMZを有効にすると、ユーザーはインターネットから直接DMZホスト（例:お使いのコンピュータ）にアクセスできるようになります。



手順：

1. 左側のバーで、「**Network**」>「**Firewall**」ページを選択します。



2. 上部のバーで、「**DMZ**」タブを選択してください。
3. DMZを有効にし、関連するパラメータを設定します。

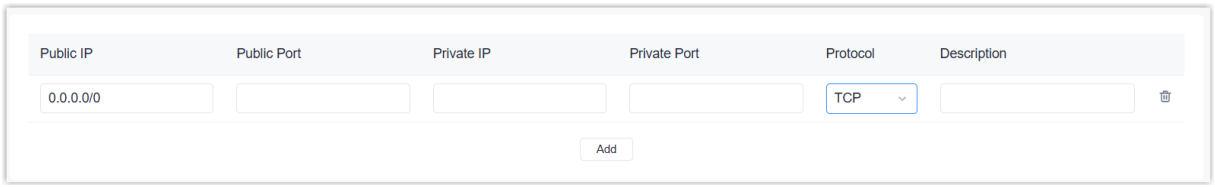
Parameter	説明
Enable	DMZ 機能を有効または無効にします。

Parameter	説明
DMZ Host	内部ホストの IP アドレス。
Source IP Address	DMZ ホストにアクセスできる IP アドレスまたは IP アドレス/マスクです。0.0.0.0/0 はすべてを意味します。

4. **[Apply]** をクリックして設定を保存します。

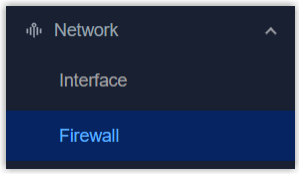
ポートマッピング (DNAT)

このページは、ポートマッピングルールを追加するために使用します。ポートマッピング（ポートフォワーディングまたはDNATとも呼ばれます）は、着信パケットの宛先IPアドレスを変更し、パブリックネットワークまたは外部ネットワークから内部ネットワークのサービスにアクセスできるようにするネットワーク技術です。



手順：

1. 左側のバーで、「**Network**」＞「**Firewall**」ページを選択してください。



2. 上部のバーで、「**Port Mapping**」タブを選択します。
3. **[Add]** をクリックしてポートマッピングルールを追加し、関連するパラメータを設定します。

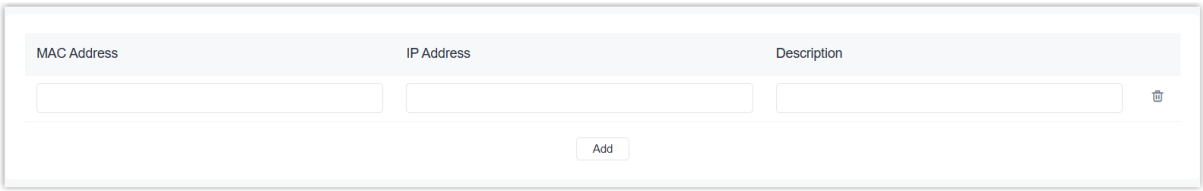
Parameter	説明
Public IP	内部サービスにアクセスできる IP アドレス/マスクです。0.0.0.0/0 はすべてを意味します。
Public Port	ポート番号またはポート範囲
Private IP	着信パケットがリダイレクトされるIPアドレス、またはIPアドレスとマスクです。
Private Port	着信パケットがリダイレクトされるポート番号またはポート範囲です。
Protocol	TCP、UDP、または「両方」からプロトコルを選択してください。

Parameter	説明
Description	このポートマッピングルールをメモします。
	このポートマッピングルールを削除します。

4. **[Apply]** をクリックして設定を保存します。

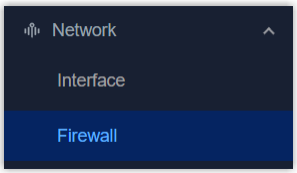
MAC バインディング

このページでは、MACバインディングの設定を行います。MACバインディングルールが追加されている場合、このリストにあるデバイスだけが外部ネットワークにアクセスできます。



手順：

1. 左側のバーで、「**Network**」>「**Firewall**」ページを選択します。



2. 上部のバーで、「**MAC Binding**」タブを選択してください。
3. **[Add]** をクリックして MAC バインディングルールを追加し、関連するパラメータを設定します。

Parameter	説明
MAC Address	ホストの MAC アドレスです。
IP Address	ホストの IPv4 アドレスです。
Description	このMACバインディングルールを記録するためです。
	このMACバインディングルールを削除します。

4. **[Apply]** をクリックして設定を保存します。

DDNS

この章では、DDNS の設定について説明します。

概要

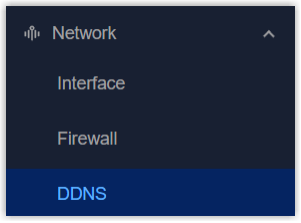
ダイナミックDNS（DDNS）とは、ドメインネームシステム（DNS）内のネームサーバーを自動的に更新する方式であり、これによりユーザーは動的IPアドレスを静的なドメイン名に紐付けることができます。DDNSはクライアントツールとして機能し、DDNSサーバーとの連携が必要です。

前提条件

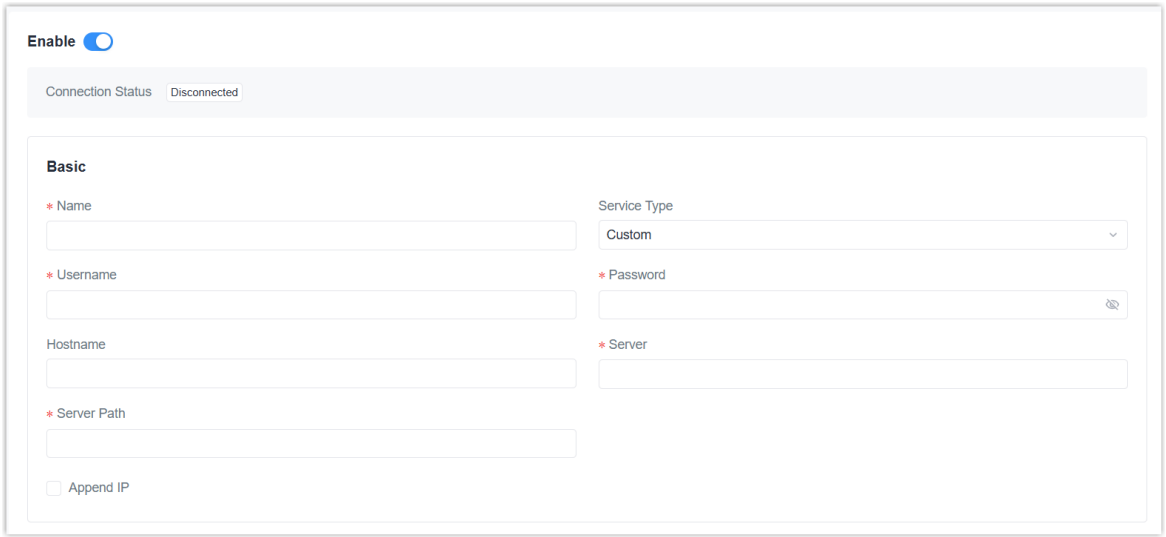
- 適切なDNSサービスプロバイダのウェブサイトに登録し、ドメイン名を申請してください。
- 必要に応じて、デバイスのリモートアクセスサービスを有効にしてください。

手順

1. 左側のバーで、「**Network**」>「**DDNS**」ページを選択します。



2. DDNS サービスを有効にし、基本設定を行います。



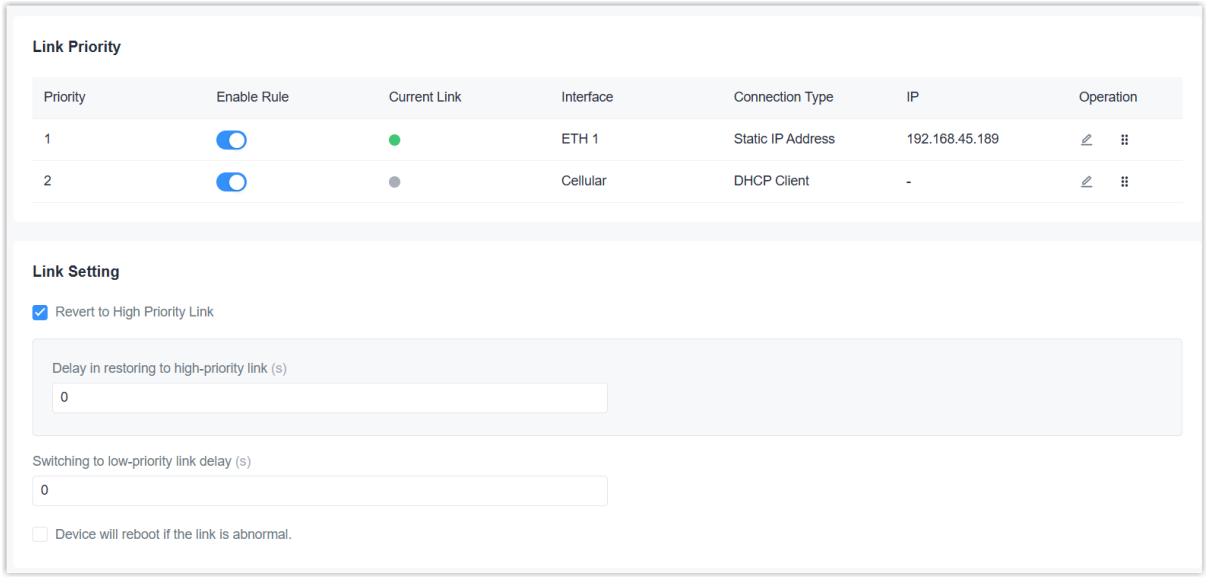
Parameter	説明
Name	この DDNS サービスの名前を定義します。
Service Type	DNS サービスプロバイダを選択してください。これらのオプションにない場合は、「カスタム」を選択してください。
Username	DNSサービスプロバイダのアカウントにログインし、更新を行うためのユーザー名です。
User ID	一部のDNSサービスプロバイダーでは、分類を行うためにこのIDが必要となります。
Password	DNSサービスプロバイダーのアカウントにログインし、更新を行うためのパスワードです。
Hostname	このデバイスのIPアドレスに関連付けるドメイン名です。
If service type is Custom	
Server	カスタム DNS サービスプロバイダのサーバーアドレス。
Server Path	DNS サービスプロバイダに IP 更新リクエストを送信するための URL です。
Append IP	現在のデバイスのIPアドレスをサーバーパスに追加する機能を有効または無効にします。

3. **[Apply]** をクリックして設定を保存します。
4. 接続ステータスが「Connected」になっているか確認してください。
5. ドメイン名を使用してデバイスにアクセスし、DDNS設定が有効になっているか確認してください。

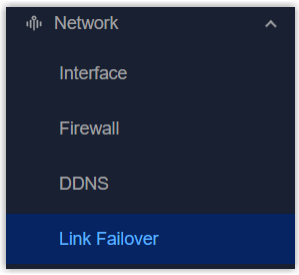
リンクのフェイルオーバー

この章では、リンクフェイルオーバー設定の構成方法について説明します。

手順



1. 左側のバーで、**[Network] > [Failover]** ページを選択します。



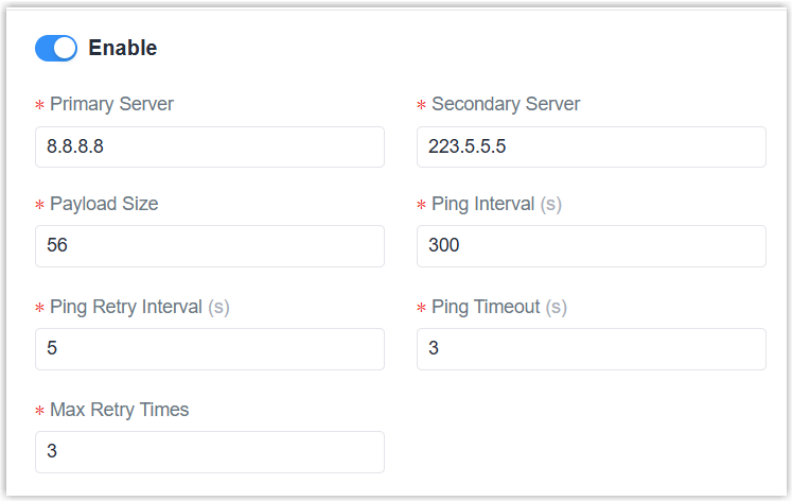
2. 「**Enable Rule**」ボタンをタップして、これらのインターフェースを本デバイスのネットワークリンクとして有効にし、次に「 」をドラッグして、これらのネットワークリンクの優先順位を調整してください。

Parameter	説明
Priority	このリンクの優先度を表示します。1 が最優先となります。
Enable Rule	このインターフェースをネットワークリンクとして使用するかどうかの設定です。
Current Link	現在のネットワークリンクを緑色で表示します。
Interface	ネットワークリンクとして使用可能なインターフェースを表示します。
Connection Type	このインターフェースの接続タイプを表示します。セルラーインターフェースの場合、DHCPクライアントに固定されています。
IP	このインターフェースのIPアドレスを表示します。

Parameter	説明
Operation	: クリックして、ping 検出設定を編集します。 : ドラッグしてリンクの優先順位を調整します。

3. クリックして　必要に応じて、選択したリンクのping検出を有効にし、関連するパラメータを設定してください。

注：
デバイスがプライベートネットワークに登録されている場合は、ping検出を無効にするか、サーバーアドレスをプライベートネットワークから到達可能なアドレスに設定するこ



Parameter	説明
Enable	有効にすると、デバイスはICMPパケットを送信して、リンクの接続状態を定期的に検出します。
Primary Server	ICMP パケットを送信するプライマリサーバーのアドレスです。
Secondary Server	プライマリサーバーからの応答を受信しなかった場合に、ICMP パケットを送信するセカンダリサーバーのアドレスです。
Payload Size	ICMP パケットのペイロードサイズです。
Ping Interval	2回のPing検出の間隔です。

Parameter	説明
Ping Retry Interval	前回のpingがタイムアウトに達し、かつ最大再試行回数に達していない場合の、再試行間隔です。
Ping Timeout	デバイスがpingリクエストへの応答を待機する最大時間です。このフィールドで事前定義された時間内に応答を受信しない場合、pingリクエストはフェイルとみなされます。
Max Retry Times	接続がフェイルしたと判断されるまで、pingリクエストを送信するデバイスの再試行回数です。

4. 必要に応じて、リンク設定パラメータを構成してください。

Parameter	説明
Revert to High Priority Link	有効にすると、優先度の高いリンクが回復した場合に、そのリンクに戻ります。 **Delayinrestoringtohigh-prioritylink：**高優先度リンクに切り替えるまでの遅延時間です。0 は即時を意味します。
Switch to low-priority link delay	低優先度リンクに切り替えるまでの遅延時間です。0 は即時を意味します。
Device will reboot if the link is abnormal	すべてのリンクが利用できない場合は、このデバイスを再起動してください。3回再起動してもリンクが回復しない場合、それ以上の再起動は行われません。

5. **[Apply]** をクリックして設定を保存してください。

関連情報

セルラー

WLAN

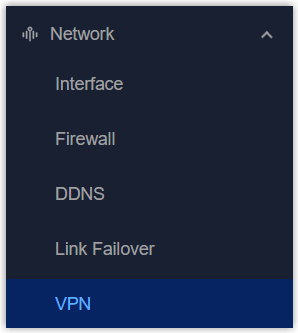
VPN

この章では、安全な通信を確保するための VPN 機能について紹介します。

概要

仮想プライベートネットワーク（VPN）とは、データの安全な送信を確保し、2つのプライベートネットワーク間の通信を可能にするために、暗号化されたトンネルを構築する機能です。基本的な手順は以下の通りです：

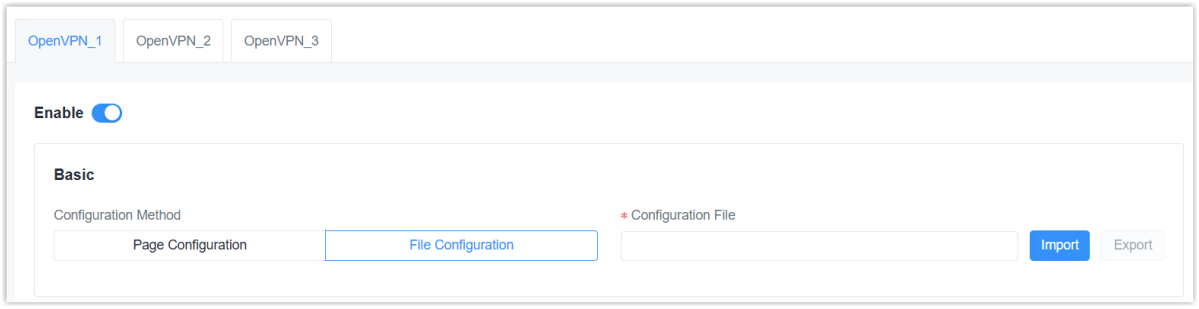
1. 左側のバーで、「**Network**」＞「**VPN**」ページを選択してください。



2. 上部のバーで、該当するVPNページを選択し、VPNパラメータを設定してください。パラメータは相手側と一致している必要があります。
   - OpenVPN クライアント設定
   - OpenVPN サーバー設定
   - IPsecの設定
   - WireGuardの設定
   - L2TPクライアント設定
   - PPTP クライアント設定
3. 「**Apply**」をクリックして設定を保存してください。
4. 「**Status**」ページに移動し、「その他」モジュールから「**VPN**」を選択して、VPN接続の状態を確認してください。

OpenVPN クライアント

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。

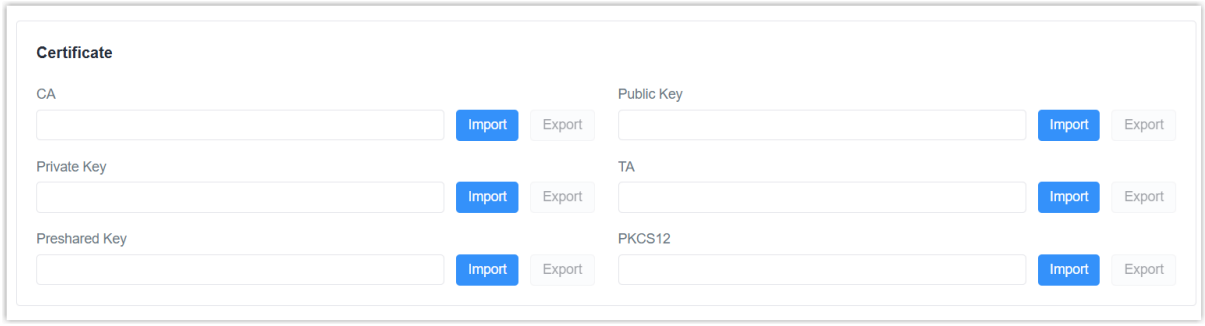


Parameter	説明
Enable	この OpenVPN クライアントを有効または無効にします。ゲートウェイは最大 3 つのクライアントに対応しています。
Configuration Method	設定方法を選択します。

Parameter	説明
	Page Configuration：Webページから設定します。 **Configuration**：パラメータや証明書の内容を含む設定ファイルをインポートして設定します。
File Configuration	
Configuration File	**Import** をクリックして、.ovpn 設定ファイルをアップロードします。サンプルである client.conf を参照して、クライアント設定ファイルを作成してください。
Page Configuration	
Protocol	リモートサーバーと通信するために、UDP または TCP からプロトコルを選択してください。
Remote IP Address	OpenVPN サーバーの IP アドレスまたはドメイン名です。
Port	OpenVPNサービスのポート番号です。このポートがファイアウォールで開放されていることを確認してください。
Interface	TapおよびTunから仮想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）をカプセル化しますが、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	VPN ネットワークを認証する方式を選択してください。 **None**：認証は不要です。 **Pre-shared**：静的キーファイルを使用します。 **Username/Password**：サーバー側で事前設定されたユーザー名/パスワードを使用します。 **X.509 cert**：証明書を使用します。 **X.509 cert + user**：ユーザー名/パスワードと証明書の両方を使用します。
Local IP	認証タイプが「None」または「Pre-shared」の場合、ローカルの仮想IPアドレスを設定してください。
Remote IP	認証タイプが None または Pre-shared で、インターフェースが Tun の場合、リモート側の仮想 IP アドレスを設定します。
Local Subnet Mask	認証タイプが None または Pre-shared で、インターフェースが Tap の場合、ローカルサブネットマスクを設定します。
Global Traffic Forwarding	認証タイプにX.509証明書が含まれている場合、有効化後はすべてのデータ通信がこのOpenVPNトンネル経由で送信されます。
TLS Authentication	認証タイプにX.509証明書が含まれる場合、TLS認証を無効または有効にします。有効にした後は、TAキーファイルをインポートする必要があります。

Parameter	説明
	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、次のようにオプション文字列を export オプションに追加してください：tls-crypt /etc/openvpn/openvpn_1-ta.key
NAT	このインターフェースのNATを有効または無効にします。
Compression	LZO 圧縮アルゴリズムを有効または無効にします。
Ping Interval	接続が有効かどうかを確認するためにハートビートパケットを送信する間隔です。この値が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値よりも優先されます。
Ping Retry	この時間内にサーバーからパケットが受信されない場合、ゲートウェイは接続を再試行します。この値が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側の値よりも優先されます。
Cipher	データパケットを暗号化するための暗号方式を、「None」、「AES-128-CBC」、「AES-192-CBC」、および「AES-256-CBC」から選択してください。
MTU	この Tun/Tap 仮想インターフェースを通過するパケットの最大伝送単位です。
Max Frame Size	UDPデータパケットがこのサイズを超える場合、フラグメント化されます。
Verbose Level	ログ出力の詳細レベルを、「エラー (0)」、「警告 (4)」、「通知 (5)」、「デバッグ (6)」から選択してください。
Expert Options	設定オプションの文字列を追加し、セミコロンで区切ってください。対応しているオプションについては、こちらをご覧ください。 **例：** auth SHA256; key direction 1
Local Route	**Add** をクリックして、ローカルホストのサブネットとネットマスクを追加してください。

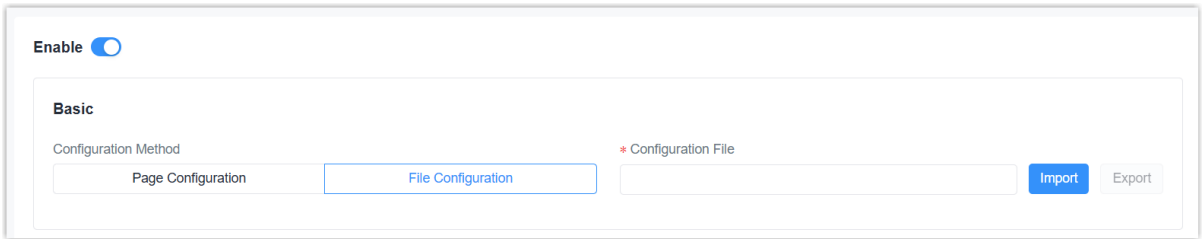
ページ設定を使用する場合、または設定ファイルに証明書の内容が含まれていない場合は、証明書をインポートする必要があります。サンプルキーファイルを入手するには、ここをクリックしてください。



Certificate Type	Description
CA	認証タイプにX.509証明書が含まれる場合は、ルートCA証明書ファイル（.crt）をインポートしてください。これはサーバーと一致している必要があります。
Public Key	認証タイプに X.509 証明書が含まれる場合は、クライアント証明書ファイル (.crt) をインポートします。
Private Key	認証タイプに X.509 証明書が含まれる場合、ローカルのクライアント秘密鍵ファイル (.key) をインポートします。
TA	認証タイプに X.509 証明書が含まれ、TLS 認証が有効になっている場合、TA キーファイル (.key) をインポートします。
Preshared Key	認証タイプが「事前共有」の場合、静的キーファイル (.key) をインポートします。これはサーバーと一致している必要があります。
PKCS12	CA、公開鍵、および秘密鍵を含むPCKS（.p12）ファイルをインポートします。これにより、ファイルの管理やインポートの手順を簡略化できます。

OpenVPN サーバー

このゲートウェイは、OpenVPNクライアントからの接続を許可するOpenVPNサーバーとして対応します。これには、すべてのクライアントからゲートウェイに到達可能なアドレスが必要です。



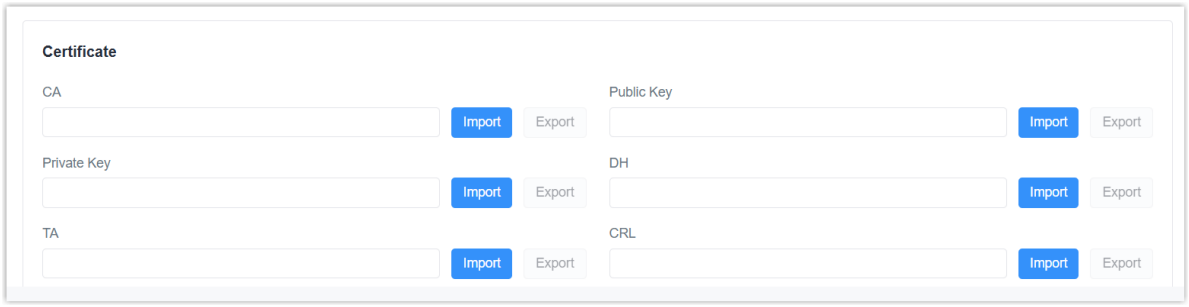
Parameter	説明
Enable	この OpenVPN サーバーを有効または無効にします。
Configuration Method	設定方法を選択します。

Parameter	説明
	Page Configuration：Webページから設定します。 **Configuration**：パラメータや証明書の内容を含む設定ファイルをインポートして設定します。
File Configuration	
Configuration File	**Import**をクリックして、.ovpn設定ファイルをアップロードしてください。サンプル（server.conf）に従って、クライアント設定ファイルをご参照ください。
Page Configuration	
Protocol	リモートクライアントと通信するために、UDP または TCP からプロトコルを選択してください。
Port	OpenVPN サービスのポート番号です。このポートがファイアウォールで開放されていることを確認してください。
Listen 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されます。
Interface	Tap および Tun から仮想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	VPN ネットワークを認証する方式を選択してください。 **None**：認証は不要です。 **Pre-shared**：静的キーファイルを使用します。 **Username/Password**：ユーザー名とパスワードを使用します。 **X.509 cert**：証明書を使用します。 **X.509 cert + user**： ユーザー名/パスワードと証明書の両方を使用します。
Local IP	認証タイプが「None」または「事前共有」の場合、ローカルの仮想 IP アドレスを設定します。
Remote IP	認証タイプが「None」または「事前共有」で、インターフェースが「Tun」の場合、リモート側の仮想 IP アドレスを設定します。
Local Subnet Mask	認証タイプが「None」または「Pre-shared」で、インターフェースが「Tap」の場合、ローカルサブネットマスクを設定してください。
Client Subnet	認証タイプにユーザー名/パスワードまたは x.509 証明書が含まれる場合は、OpenVPN クライアント用の IP アドレスプールを定義してください。
Client Submask	クライアントサブネットのサブ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トします。0 は無効を意味します。

Parameter	説明
Max Clients	許可されるクライアント接続の最大数です。範囲：1〜128
Enable TLS Authentication	認証タイプに X.509 証明書が含まれる場合、TLS 認証を無効または有効にします。有効にした後は、TA キーファイルをインポートする必要があります。 **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、次のようにオプション文字列を export オプションに追加してください：tls-crypt /etc/openvpn/openvpn_1-ta.key
Enable CRL	認証タイプにユーザー名/パスワードまたは X.509 証明書が含まれる場合、CRL 検証を有効または無効にします。
Enable Client to Client	認証タイプにユーザー名/パスワードまたは X.509 証明書が含まれる場合、クライアント間の通信を有効または無効にします。
Enable Dup Client	認証タイプにユーザー名/パスワードまたはX.509証明書が含まれる場合、クライアントがこのサーバーに接続する際に、同じ証明書またはユーザー名/パスワードを使用できるようにするか、または使用できないようにするかを選択します。
NAT	このインターフェースのNATを有効または無効にします。
Compression	LZO 圧縮アルゴリズムを有効または無効にします。
Ping Interval	接続が有効かどうかを確認するためにハートビートパケットを送信する間隔です。この値が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値よりも優先されます。
Ping Retry	この時間内にサーバーからパケットが受信されない場合、ゲートウェイは接続を再起動します。この値がサーバーとクライアントの両方で設定されている場合、サーバーからプッシュされた値がクライアントの値よりも優先されます。
Cipher	データパケットを暗号化するための暗号方式を、「None」、「AES-128-CBC」、「AES-192-CBC」、および「AES-256-CBC」から選択してください。
MTU	この Tun/Tap 仮想インターフェースを通過するパケットの最大伝送単位です。
Max Frame Size	UDPデータパケットがこのサイズを超える場合、フラグメント化されます。
Verbose Level	ログ出力の詳細レベルを、「エラー (0)」、「警告 (4)」、「通知 (5)」、「デバッグ (6)」から選択してください。
Expert Options	設定オプションの文字列を追加し、セミコロンで区切ってください。対応しているオプションについては、こちらをご覧ください。

Parameter	説明
	例： auth SHA256; key direction 1
Account	認証タイプにユーザー名とパスワードが含まれる場合、**Add** をクリックして OpenVPN クライアントのユーザー名とパスワードを追加します。
Local Route	**Add** をクリックして、ローカルホストのサブネットとネットマスクを追加します。
Client Subnet	**Add**をクリックして、OpenVPNクライアントのサブネットを追加します。サブネット名は、OpenVPNクライアント証明書の共通名である必要があります。

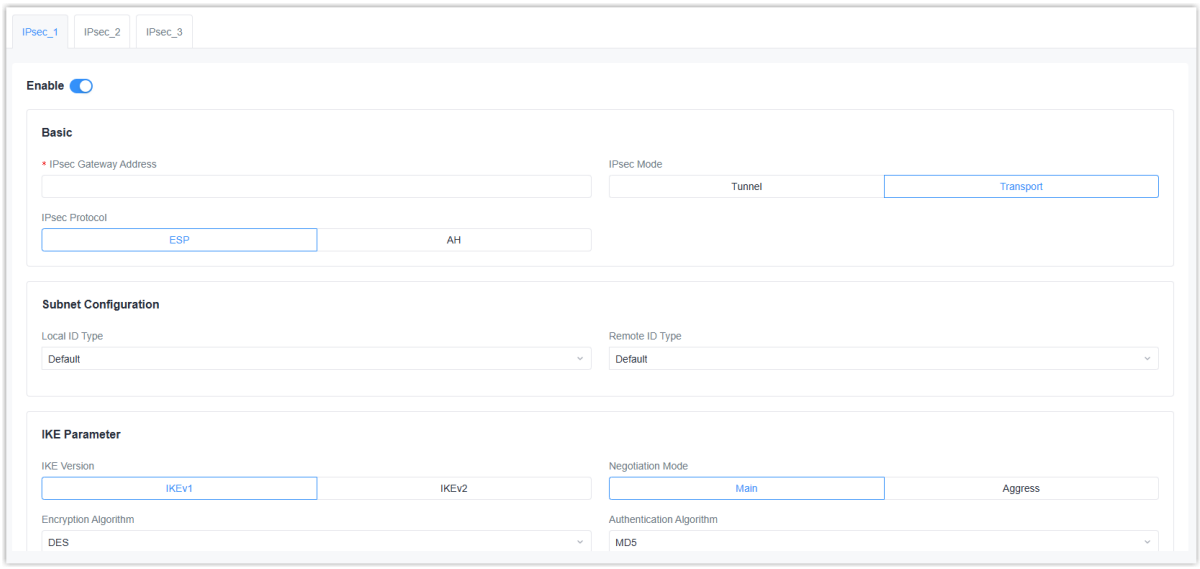
ページ設定を使用する場合、または設定ファイルに証明書の内容が含まれていない場合は、証明書をインポートする必要があります。サンプルキーファイルを入手するには、こちらをクリックしてください。



Certificate Type	Description
CA	認証タイプに X.509 証明書が含まれる場合は、ルート CA 証明書ファイル (.crt) をインポートしてください。
Public Key	認証タイプに X.509 証明書が含まれる場合、サーバー証明書ファイル (.crt) をインポートします。
Private Key	認証タイプに X.509 証明書が含まれている場合、サーバーの秘密鍵ファイル (.key) をインポートします。
DH	DHグループファイル（.pem）をインポートします。
TA	TLS 認証が有効になっている場合、TA キーファイル (.key) をインポートします。
CRL	CRL検証が有効になっている場合、CRLファイル（.pem）をインポートします。
Preshared Key	認証タイプが「事前共有」の場合、静的キーファイル（.key）をインポートします。

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役立ちます。ゲートウェイは、最大3つのクライアントに対応しています。



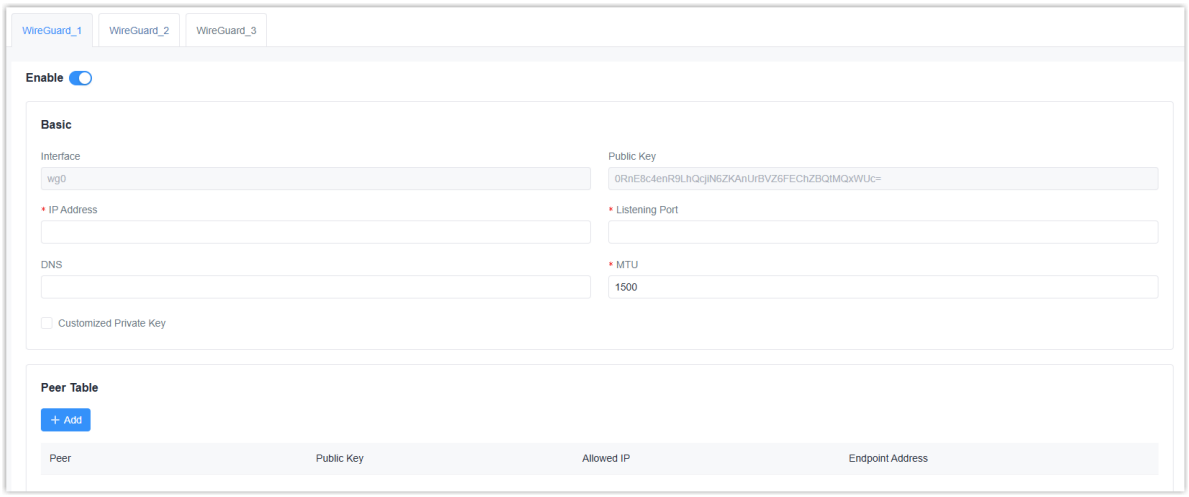
Parameter	説明
Enable	IPsec トンネルを有効または無効にします。最大 3 つの IPsec トンネルが許可されます。
IPsec Gateway Address	相手側のIPアドレスまたはドメイン名です。
IPsec Mode	「Tunnel」または「Transport」を選択します。 **Tunnel：**これは、中間にある信頼できないネットワーク（インターネットなど）によって隔てられた2つの異なるネットワーク間で、安全な接続が必要な構成において最も一般的に使用されます。 **Transport：**クライアントとサーバー間の通信（ワークステーションとゲートウェイ間、またはホスト間）など、高速かつ安全なエンドツーエンドの通信が必要な場合に一般的に使用されます。
IPsec Protocol	ESP または AH を選択します。
Subnet Configuration	
Local ID Type	リモート・ピアに送信する識別子のタイプを選択します。 **Default：**なし **ID：**ローカルサブネットのIPアドレスをIDとして使用 **FQDN：**完全修飾ドメイン名、例：test.user.com **FQDN：**メールアドレス形式の完全修飾ユーザー名文字列、例：
Remote ID Type	リモート・ピアのローカル ID と同じ識別子タイプを選択してください。

Parameter	説明
	Default：なし **ID：**リモートサブネットの IP アドレスを ID として使用 **FQDN：**完全修飾ドメイン名、例：test.user.com **User FQDN：**電子メールアドレス形式の完全修飾ユーザー名文字列、例：
Local Subnet	IPsec モードが「Tunnel」の場合、ローカル LAN サブネットを設定します。
Local Subnet Mask	IPsec モードが「Tunnel」の場合、ローカル LAN サブネットマスクを設定します。
Remote Subnet	IPsec モードが「Tunnel」の場合、リモート LAN サブネットを設定します。
Remote Subnet Mask	IPsec モードが「Tunnel」の場合、リモート LAN サブネットマスクを設定します。
IKE Parameter	
IKE Version	IKEv1 または IKEv2 を選択してください。
Negotiation Mode	IKEv1 を使用する場合は、「Main」または「Aggressive」を選択してください。
Encryption Algorithm	AES128、AES192、AES256から選択してください。
Authentication Algorithm	MD5 または SHA1 を選択してください。
DH Group	MODP768-1、MODP1024-2、または MODP1536-5 から選択してください。
Local Authentication Type	PSK または CA を選択してください。 **PSK：**事前共有鍵を使用して認証を完了します。これには、相手側と同じローカル秘密鍵値の入力が必要です。 **CA：**認証を完了するために証明書を使用します。選択後、CA証明書、クライアント証明書、および秘密鍵をそれぞれのフィールドにインポートする必要があります。
Remote Authentication Type	IKEv2を使用する場合は、PSKまたはCAを選択してください。 **PSK：**事前共有鍵を使用して認証を完了します。リモート秘密鍵の値を入力する必要があります。 **CA：**証明書を使用して認証を完了します。選択後、対応するフィールドにサーバー証明書をインポートする必要があります。
Lifetime	IKEの再ネゴシエーションが行われるまでの残り時間です。

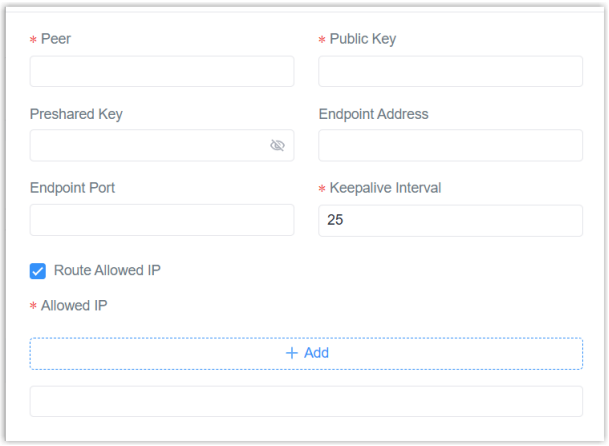
Parameter	説明
XAUTH	IKEv1を使用する場合、XAUTHを有効にした後、XAUTHリクエストに応答するためにXAUTHのユーザー名とパスワードを定義してください。
SA Parameter	
SA Algorithm	AES128-SHA1、AES128-MD5、AES192-SHA1、AES192-MD5、AES256-SHA1、およびAES256-MD5 から選択してください。
PFS Group	NULL、MODP768-1、MODP1024-2、またはMODP1536-5から選択してください。
DPD Time Interval	DPDリクエストを送信する再試行間隔です。
DPD Timeout	IKEv1 を使用する場合、リモート側のフェイルを検出するために DPD タイムアウトを設定します。
Lifetime	SAの再ネゴシエーションが行われるまでの最後の時間です。
IPsec Advanced	
VPN Over IPsec Type	L2TP over IPsec を有効にするかどうかを選択してください。L2TP を選択した場合は、L2TP トンネルを選択する必要があります。
Enable Compression	IPパケットのヘッダーを圧縮するかどうかを設定します。
Certificate	
CA	ローカル認証タイプが CA の場合、ルート CA 証明書ファイル (.crt) をインポートします。
Client Certificate	ローカル認証タイプが CA の場合、クライアント証明書ファイル (.crt) をインポートします。
Server Certificate	リモート認証タイプが CA の場合、サーバー証明書ファイル (.crt) をインポートします。
Private Key	ローカル認証タイプが CA の場合、ローカルのクライアント秘密鍵ファイル (.key) をインポートします。
CRL	必要に応じて、証明書失効リスト（CRL）をインポートします。

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モダンなVPNです。WireGuardはUDPプロトコル経由でトラフィックを送信します。

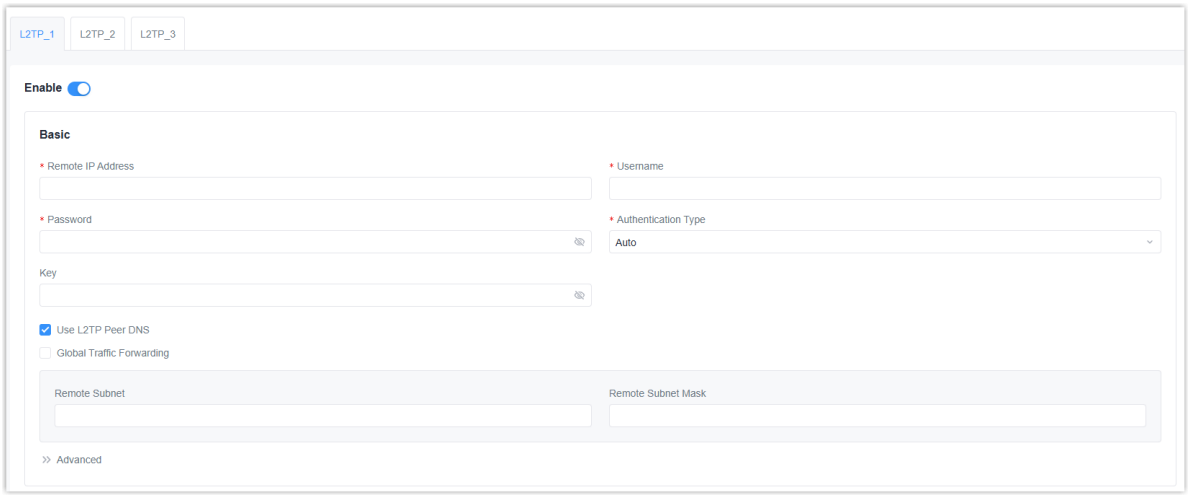


Parameter	説明
Enable	WireGuardインターフェースを有効または無効にします。WireGuardインターフェースは最大3つまで許可されます。
Interface	WireGuardインターフェース名を表示します。
Public Key	秘密鍵によって生成された公開鍵を表示します。
IP Address	ローカルの仮想IPアドレスとネットマスクです。例：10.8.0.2/24
Listening Port	WireGuardパケットの送受信を行うポートです。異なるWireGuardインターフェースのポート番号は、それぞれ異なる必要があります。
DNS	このWireGuardインターフェースのDNSサーバーアドレスです。空欄のままにすると、デバイス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です。
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デバイスで生成された秘密鍵を使用します。
Peer Table	**+Add]** 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。

Parameter	説明
	 **Peer：**一意のピア名です。 **Public Key：** ピアの公開鍵です。 **PresharedKey：**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、同じキー値を使用する必要があります。 **Endpoint Address：**ピアの IP アドレスまたはドメイン名です。 **Endpoint Port：**ピアの宛先ポートです。 **KeepaliveInterval：**接続後、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する間隔です。0 は無効を意味します。 **RouteAllowedAlloweIP：**許可されたIPアドレスの静的ルーティングを追加するには、この機能を有効または無効にしてください。 **dIP：**WireGuardピアのLANネットワークの実際のIPアドレスとネットマスクです。1つのWireGuardピアで最大8つの許可されたIPアドレスに対応できます。例：192.168.1.0/24

L2TP

レイヤー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。

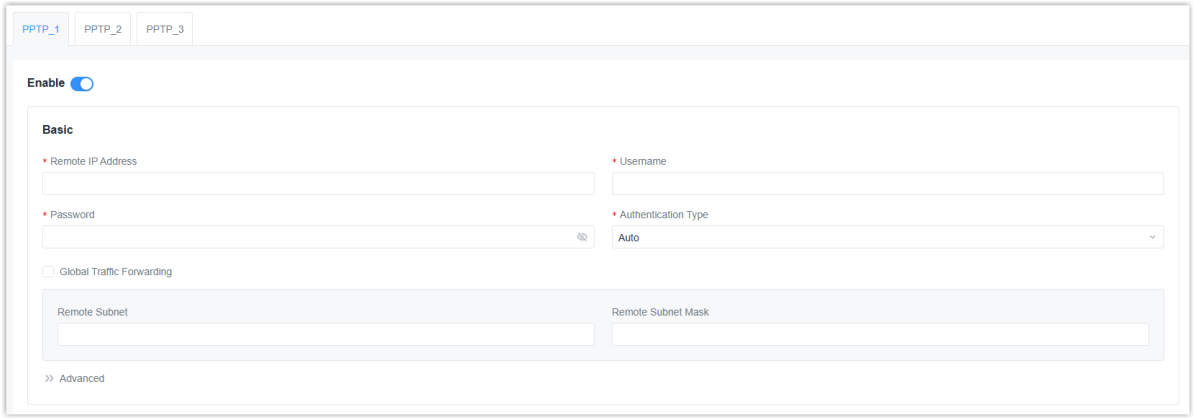


Parameter	説明
Enable	L2TPクライアントを有効または無効にします。L2TPクライアントは最大3台まで許可されます。
Remote IP Address	L2TPサーバーのIPアドレスまたはドメイン名です。
Username	L2TP サーバーへの認証に使用するユーザー名です。
Password	L2TP サーバーへの認証に使用するパスワードです。
Authentication Type	「Auto」、「PAP」、「CHAP」、「MS-CHAPv1」、および「MS-CHAPv2」から選択してください。
Key	L2TP トンネル認証に使用されるキーです。
Use L2TP Peer DNS	ピア L2TP サーバーの DNS アドレスを使用する場合は有効にし、使用しない場合は無効にしてください。
Global Traffic Forwarding	有効にすると、すべてのデータトラフィックがこのVPNトンネル経由で送信されます。無効にした場合は、リモートサブネットとマスクを設定する必要があります。
Advanced	
Local IP Address	このクライアントのローカルトンネルIPアドレスです。空欄のままにすると、クライアントはサーバーからトンネルIPアドレスを取得します。
Peer IP Address	ピアのトンネルIPアドレスです。
Asyncmap Value	非同期リンク上でエスケープすべきASCII制御文字を定義します。範囲：0～ffffffff。
MRU	この L2TP インターフェースを通過するパケットの最大受信単位です。
MTU	この L2TP インターフェースを通過するパケットの最大送信単位です。
Link Detection Interval	接続が有効かどうかを確認するためにハートビートパケットを送信する間隔です。

Parameter	説明
Max Retries Times	この時間内にサーバーからパケットが受信されない場合、ゲートウェイは接続を再起動します。
Expert Options	設定オプションの文字列を追加し、セミコロンで区切ってください。
Enable NAT	このインターフェースの NAT を有効または無効にします。
Enable MPPE	MPPE 暗号化を有効または無効にします。
Address/Control Compression	アドレスおよび制御フィールド圧縮（ACFC）を有効または無効にします。
Protocol Field Compression	プロトコルフィールド圧縮（PFC）を有効または無効にします。

PPTP

ポイント・ツー・ポイント・トンネリング・プロトコル（PPTP）は、TCP制御チャネルと汎用ルーティングカプセル化（GRE）トンネルを使用して、PPPパケットをカプセル化するプロトコルです。



Parameter	説明
Enable	PPTP クライアントを有効または無効にします。**PPTP** クライアントは最大 3 つまで許可されます。
Remote IP Address	PPTP サーバーの IP アドレスまたはドメイン名です。
Username	PPTP サーバーへの認証に使用するユーザー名です。
Password	PPTP サーバーへの認証に使用するパスワードです。
Authentication Type	[自動]、[PAP]、[CHAP]、[MS-CHAPv1]、[MS-CHAPv2] から選択してください。

Parameter	説明
Global Traffic Forwarding	有効にすると、すべてのデータ通信はこのVPNトンネルを経由して送信されます。無効にする場合は、リモートサブネットとサブネットマスクを設定する必要があります。
Advanced	
Local IP Address	このクライアントのローカルトンネルIPアドレスです。空欄のままにすると、クライアントはサーバーからトンネルIPアドレスを取得します。
Peer IP Address	ピアのトンネルIPアドレスです。
Asyncmap Value	非同期リンク上でエスケープすべきASCII制御文字を定義します。範囲：0～ffffffff。
MRU	このPPTPインターフェースを通過するパケットの最大受信単位です。
MTU	この PPTP インターフェースを通過するパケットの最大送信単位です。
Link Detection Interval	接続が有効かどうかを確認するためにハートビートパケットを送信する間隔です。
Max Retries Times	この時間内にサーバーからパケットが受信されない場合、ゲートウェイは接続を再確立します。
Expert Options	設定オプションの文字列を追加し、セミコロンで区切ってください。
Enable NAT	このインターフェースの NAT を有効または無効にします。
Enable MPPE	MPPE 暗号化を有効または無効にします。
Address/Control Compression	アドレスおよび制御フィールド圧縮（ACFC）を有効または無効にします。
Protocol Field Compression	プロトコルフィールド圧縮（PFC）を有効または無効にします。

第7章 プラットフォーム管理

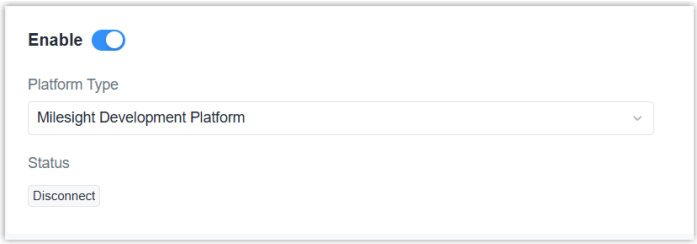
この章では、デバイスをMilesightリモート管理プラットフォームに接続する方法について説明します。

前提条件

- デバイスがインターネットネットワークに接続されていること。
- Milesight Development Platformのアカウントとエンタープライズが作成されており、デバイスの追加に対応していること。

手順

1. 左側のバーから、「**Platform Management**」ページを選択します。
2. デバイスがプラットフォームに接続できるようにします。



3. **[Apply]** をクリックして設定を保存します。
4. デバイスをプラットフォームに追加してください。詳細については、「デバイスの接続」を参照してください。
5. プラットフォームとデバイス上で、接続状態が「Connected」に変わっているか確認してください。

第8章 システム

一般

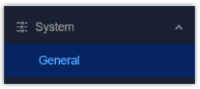
この章では、一般的なアクセス設定と時刻設定について説明します。

一般

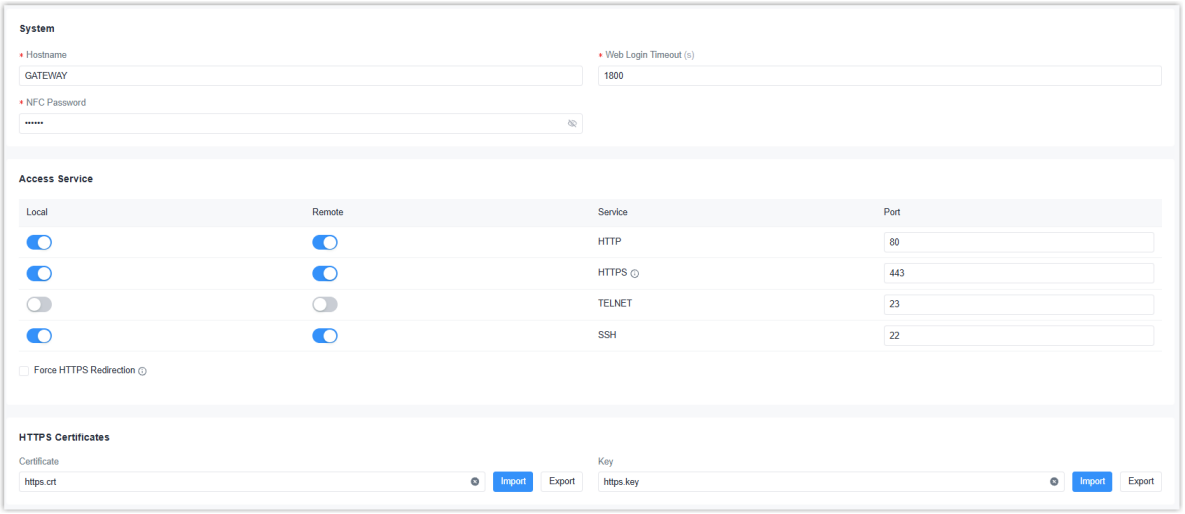
このページでは、いくつかの基本パラメータおよびアクセスパラメータを設定します。

手順：

1. 左側のバーで、**[System] > [General]** ページを選択します。



2. 上部のバーで、「**General**」タブを選択してください。
3. 必要に応じて一般パラメータを設定してください。



Parameter	説明
System	
Hostname	このデバイスを識別するための一意の名前を定義します。
Web Login Timeout	このタイムアウト時間が経過すると、Web GUI は自動的にログアウトします。範囲：100～3600 秒。
NFC Password	Milesight LoRaWAN® エンドデバイスに設定を書き込むためのパスワードを定義します。

Parameter	説明
Access Service	
Local	デバイスへのローカルアクセスを有効または無効にします。
Remote	デバイスにリモートでアクセスするためのサービスを有効または無効にします。
Service	このデバイスは、HTTP/HTTPS 経由の Web アクセス、または SSH/TELNET 経由の CLI アクセスを対応しています。
Port	サービスのポート番号を設定します。各サービスは一意のポートを使用する必要があります。
Force HTTPS Redirection	この機能を有効にすると、HTTPSアクセスサービスが有効な場合、HTTPアクセスは自動的にHTTPSにリダイレクトされます。
HTTPS Certificates	
Certificate	ゲートウェイには、HTTPS アクセス用の証明書および鍵ファイルがプリロードされています。 **Import**：クリックして、カスタマイズしたファイルをインポートします。 **Export**：クリックしてファイルをエクスポートします。
Key	

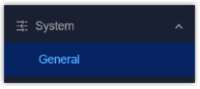
4. **[Apply]** をクリックして設定を保存します。

システム時刻

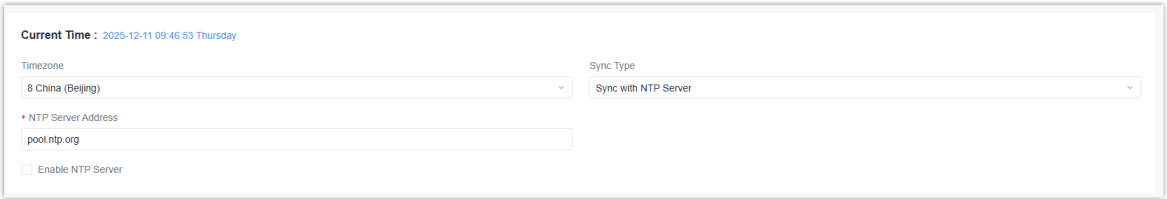
このページは、デバイスのシステム時刻パラメータを設定するために使用します。

手順：

1. 左側のバーで、「**System**」＞「**General**」ページを選択してください。



2. 上部のバーで、「**System Time**」タブを選択します。
3. 必要に応じて、一般パラメータを設定してください。



Parameter	説明
Current Time	現在のデバイスの時刻を表示します。
Timezone	デバイスのタイムゾーンを選択します。
Sync Type	「ブラウザと同期」、「NTP サーバーと同期」、または「Manual Configuration」の中から、時刻同期のソースを選択します。
Sync with NTP Server	
NTP Server Address	時刻を同期させるために、NTPサーバーのアドレス（ドメイン名またはIPアドレス）を設定してください。これを行うには、ゲートウェイがこのサーバーにアクセスできる必要があります。
Enable NTP Server	有効にすると、このデバイスはNTPサーバーとして機能し、接続された他のデバイスに時刻を提供できるようになります。

4. **[Apply]** をクリックして設定を保存します。

ユーザー

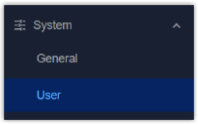
この章では、アカウント情報の変更方法とサブユーザーの追加方法について説明します。

アカウント

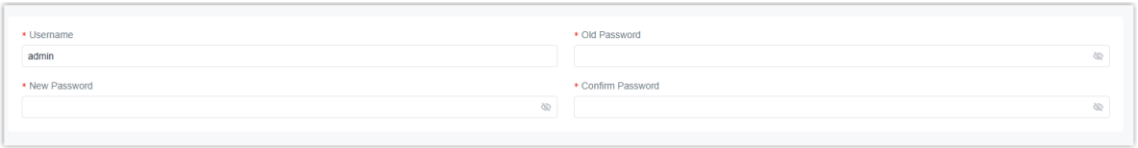
このセクションでは、現在のアカウント情報を変更します。

手順：

1. 左側のバーで、「**System**」＞「**Users**」ページを選択します。



2. 上部のバーで、「**Account**」タブを選択します。
3. 必要に応じて、現在のアカウント情報を変更してください。



Parameter	説明
Username	新しいユーザー名を入力してください。小文字、数字、「-」、「_」のみ使用可能で、最初の文字は英字または「_」でなければなりません。文字数の制限：1～31文字。
Old Password	現在のパスワードを入力してください。
New Password	新しいパスワードを入力してください。スペースを除き、ASCII文字のみ使用可能です。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、5文字以上31文字以内で入力してください。
Confirm Password	新しいパスワードをもう一度入力してください。

4. **[Apply]** をクリックして設定を保存してください。

ユーザー管理

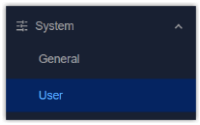
このセクションでは、デバイスのサブアカウントを追加および管理します。

前提条件

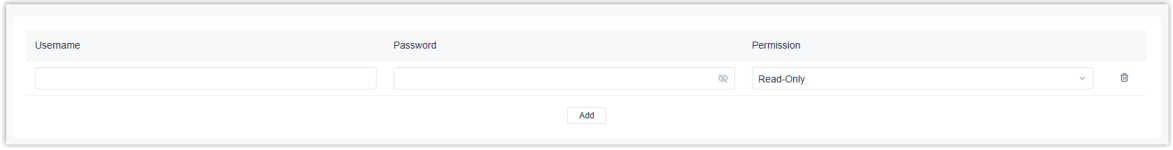
現在のアカウントは管理者アカウントです。

手順：

1. 左側のバーで、**[System] > [User]** ページを選択します。



2. 上部バーで、「**User Management**」タブを選択します。
3. 「**Add**」をクリックしてサブアカウントを追加し、アカウント情報を設定します。



Parameter	説明
Username	新しいユーザー名を入力してください。小文字、数字、「-」および「_」のみ使用可能で、最初の文字は英字または「_」でなければなりません。文字数制限：1～31文字。

Parameter	説明
Password	パスワードを入力してください。スペースを除き、ASCII文字のみ使用可能です。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、5文字以上31文字以内で入力してください。
Permission	このサブアカウントの権限を選択してください。 **Read-Write**：ユーザーがすべての設定を読み書きできるようにします。 **Read-Only**：ユーザーがすべての設定を読み取り、以下の設定を行うことができます： ◦ **[System] > [Maintenance] > Tools]** ページにあるユーザーデバッグツール。 ◦ **>LogSystem**ページにあるログのダウンロード。 ◦ **>UserUsers**」ページにある現在のアカウント情報の変更。
	このサブアカウントを削除します。

4. 「**Apply**」をクリックして設定を保存してください。

サービス

この章では、メール設定と電話設定の構成方法について説明します。

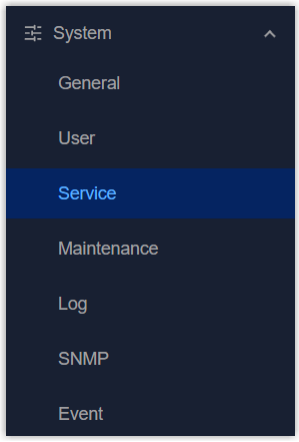
SMTP

このデバイスは、メールの送受信を行う SMTP クライアントとして対応します。

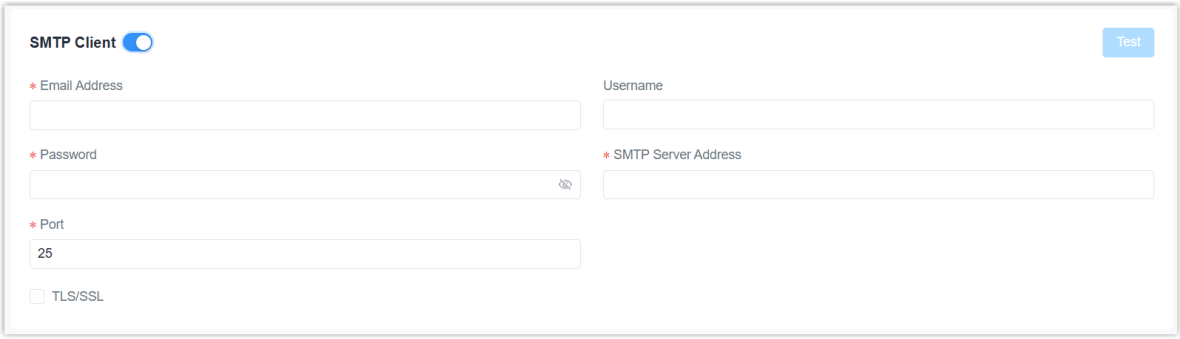
前提条件：有効なメールアドレスの情報があり、そのメールアドレスがサードパーティ製アプリへのアクセスを許可していることを確認してください。

手順：

1. 左側のバーで、「**System**」>「**Service**」ページを選択します。



2. 上部バーで、「**SMTP**」タブを選択します。
3. SMTPクライアントを有効にし、関連するパラメータを設定します。



Parameter	説明
SMTP Client	SMTP クライアントを有効または無効にします。
Email Address	メール送信に使用するアドレスです。形式： xxx@xxx.xx
Username	SMTPサーバーでの認証に使用するユーザー名です。
Password	SMTPサーバーでの認証に使用するパスワードです。
SMTP Server Address	メールサービスプロバイダの SMTP サーバーのアドレスです。
Port	メールサービスプロバイダの SMTP サーバーのポート番号です。
TLS/SSL	TLS/SSL 認証を有効または無効にします。

4. **[Apply]** をクリックして設定を保存します。
5. 右上の「**Test**」ボタンをクリックして、設定が反映されているか確認してください。

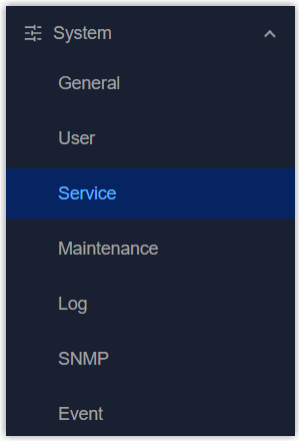
メール

このページでは、メールアラームを送信するためのメールグループを設定します。

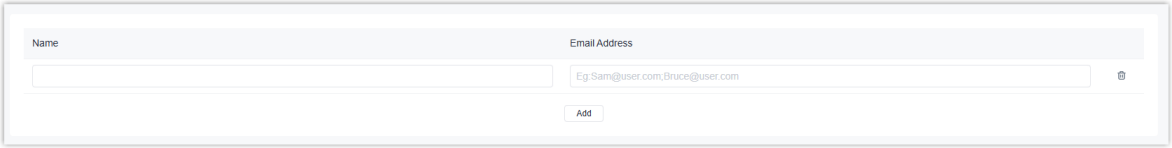
前提条件：SMTP クライアントの設定が有効になっていること。

手順：

1. 左側のバーで、「**System**」>「**Service**」ページを選択します。



2. 上部バーで、「**Email**」タブを選択します。
3. **[Add]** をクリックしてメールグループを追加し、関連するパラメータを設定します。



Parameter	説明
Name	このメールグループを識別するための一意の名前を設定します。
Email Address	メールグループにメールアドレスを入力し、各アドレスをセミコロンで区切ってください。
	このメールグループを削除してください。

4. **[Apply]** をクリックして設定を保存します。

電話

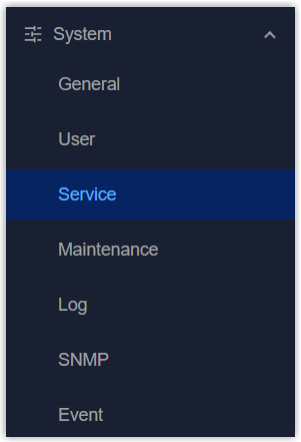
このページは、アラームを送信する電話グループを設定するために使用します。

前提条件：

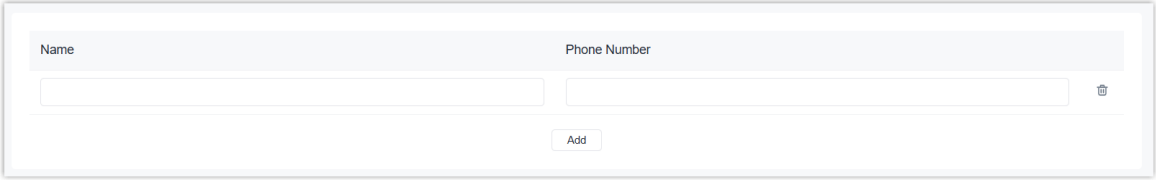
- この機能は、-L08GL モデルでのみご利用いただけます。
- 使用するSIMカードがSMSサービスに対応していることを確認してください。
- SMSセンター番号が正しく設定されていることを確認してください。

手順：

1. 左側のバーで、「**System**」＞「**Service**」ページを選択してください。



2. 上部のバーで、「**Phone**」タブを選択します。
3. **[Add]** をクリックして電話グループを追加し、関連するパラメータを設定します。



Parameter	説明
Name	この電話グループを識別するための一意の名前を設定します。
Phone Number	電話番号を電話グループに入力し、各番号をセミコロンで区切ります。
	この電話グループを削除します。

4. 「**Apply**」をクリックして設定を保存してください。

関連情報

イベント

メンテナンス

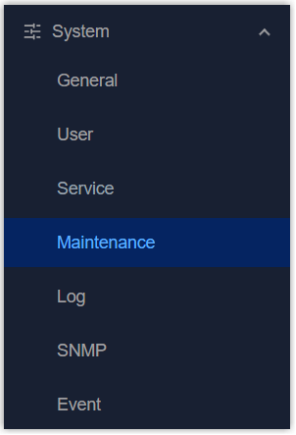
この章では、メンテナンスツールと機能について説明します。

ツール

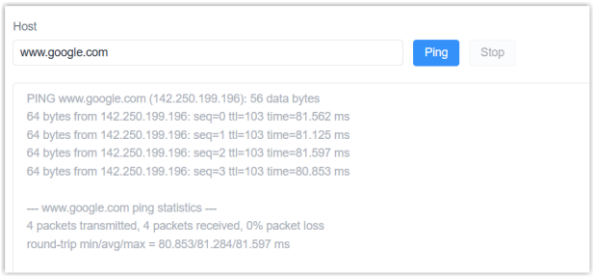
このセクションでは、さまざまなツールを使用してネットワーク接続を確認します。

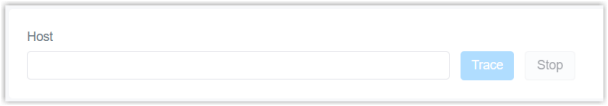
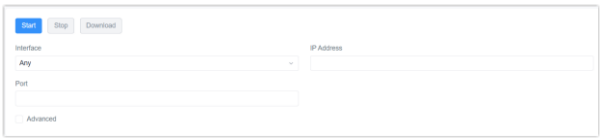
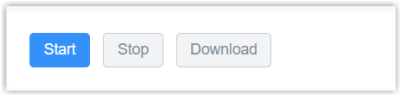
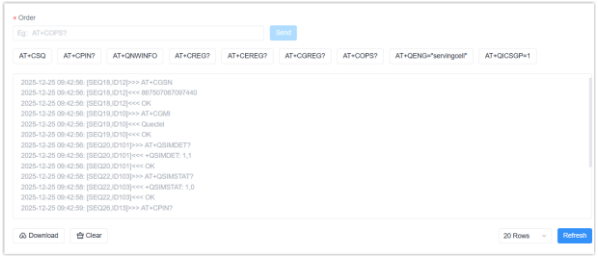
手順：

1. 左側のバーで、**[System] > [Maintenance]** ページを選択します。



2. 上部バーで、「**Tools**」タブを選択します。
3. 本デバイスには、デバッグ用のツールが5つ用意されています。問題に応じて選択してください。

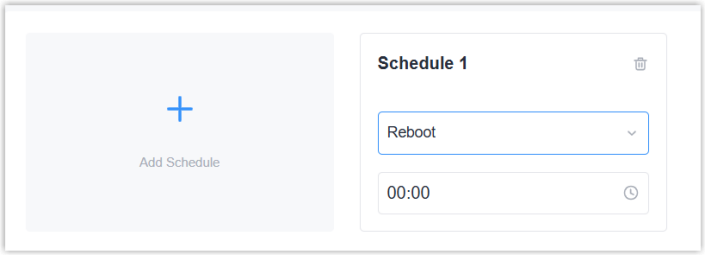
Tool	Feature	Steps
Ping	本デバイスとターゲットホスト間のネットワーク接続および遅延をテストします。	 a. IPアドレスまたはドメイン名を入力します。 b. **[Ping]** をクリックします。

Tool	Feature	Steps
Traceroute	デバイスからターゲットホストまでのパケットの経路を追跡します。	 a. IPアドレスまたはドメイン名を入力します。 b. **Trace** をクリックします。
Packet Analyzer	TCPDUMPを使用して、デバイスのネットワークインターフェースを通過するネットワークパケットをキャプチャします。	 a. インターフェース、IPアドレス、ポートなどのパケットキャプチャ条件を設定します。より複雑な要件がある場合は、**Advanced**有効にし、TCPDUMPコマンドを入力してください。 b. **Start**をクリックし、しばらくお待ちください。 c. **Stop**をクリックしてキャプチャを停止します。 d. **Download**をクリックして、.pcapファイルをダウンロードします。 e. ツールを使用してファイルを分析するか、Milesightのテクニカルサポートに送信してください。
Qxdmlog	セルラーモジュールから診断ログを収集します。	 a. **Start**をクリックし、2分以上待ちます。 b. **Stop**をクリックして収集を停止します。 c. **Download**をクリックしてログをダウンロードし、Milesightのテクニカルサポートに連絡してください。
Cellular AT Debug	ATコマンドを送信して、セルラーモジュールからデバッグ情報を取得したり、モジュールを設定したりします。	

Tool	Feature	Steps
		a. ATコマンドを入力し、「**Sen**をクリックします。または、プリセットされたコマンドボタンをクリックして直接送信します。 b. ボックス上のセルラーログを確認し、「**d**をクリックして、必要に応じてログファイルをダウンロードします。 c. そのファイルをMilesightのテクニカルサポートに送信してください。

スケジュール

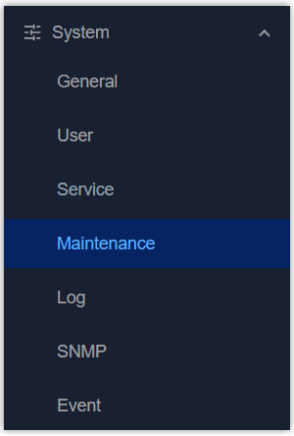
このセクションは、再起動のスケジュール設定を追加するために使用します。



前提条件：デバイスの時刻が正しいことを確認してください。

手順：

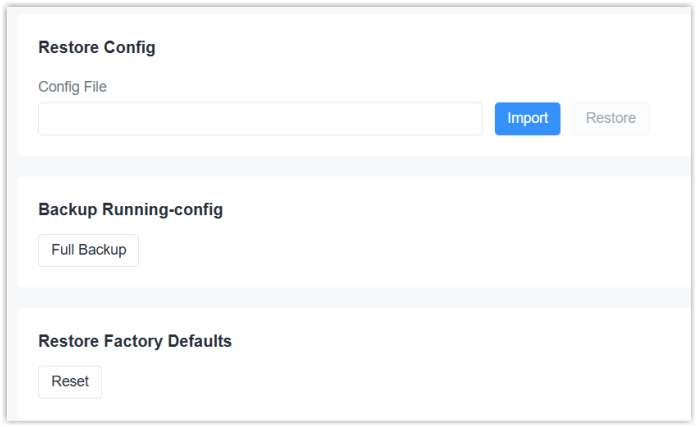
1. 左側のバーで、「**System**」＞「**Maintenance**」ページを選択してください。



2. 上部のバーで、「**Schedule**」タブを選択します。
3. 「**Add Schedule**」をクリックして、新しいスケジュールを追加します。
4. 再起動イベントを選択し、再起動の時間を選択します。
5. 「**Apply**」をクリックして設定を保存します。

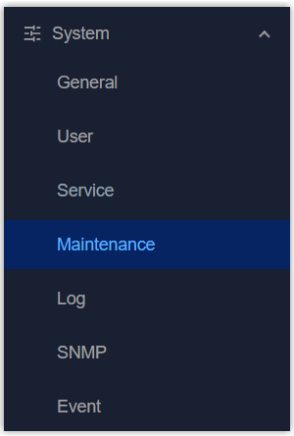
バックアップと復元

このセクションは、設定のバックアップと復元に使用します。



バックアップと復元の手順：

1. 左側のバーで、「**System**」>「**Maintenance**」ページを選択します。



2. 上部のバーで、「**Backup and Restore**」タブを選択します。
3. 「**Full Backup**」をクリックして、現在のデバイスの設定ファイルをダウンロードします。
4. 新しいデバイスのWeb GUIを開き、「**Import**」をクリックして、ローカルパスから設定ファイルを選択してください。
5. 「**Restore**」をクリックして、設定を新しいデバイスにインポートします。

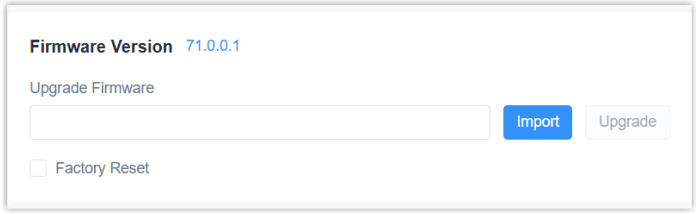
工場出荷時設定へのリセット手順：

1. 「**Reset**」をクリックして、工場出荷時のデフォルト設定にリセットします。

> **注：**
>
> Web GUI にログインできない場合は、リセットボタンを使用してデバイスをリセットしてください。

アップグレード

このセクションは、デバイスのアップグレードに使用します。

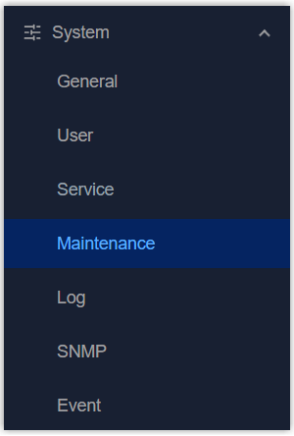


前提条件：

- Milesightの公式ウェブサイトから、お使いのデバイスに適したファームウェアファイルをダウンロードしてください。安全かつ確実にアップグレードを行うため、アップグレード前にテクニカルサポートにご相談されることをお勧めします。
- アップグレードを行うには、ネットワーク接続が十分に安定していることを確認してください。

手順：

1. 左側のバーから、「**System**」＞「**Maintenance**」ページを選択してください。



2. 上部バーから「**Upgrade**」タブを選択します。
3. 「**Import**」をクリックし、ローカルパスからファームウェアファイルを選択してください。
4. 必要に応じて「**Factory Reset**」を有効にしてください。有効にすると、アップグレード後にデバイスが工場出荷時の設定にリセットされます。
5. 「**Upgrade**」をクリックして、デバイスをアップグレードしてください。

> **注意：**
> ファームウェアのアップグレード中は、ウェブページでのいかなる動作も行ってはいけません。そうしないと、アップグレードが中断されたり、デバイスが動作しなくなったりする恐れ

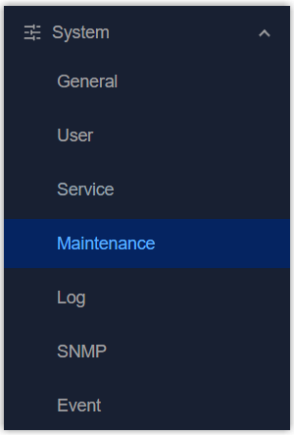
6. デバイスのSYS LEDが緑色に点灯したら、Web GUIにログインして、アップグレードが正常に完了したことを確認してください。

再起動

このセクションでは、デバイスの再起動を行います。

手順：

1. 左側のバーで、**[System] > [Maintenance]** ページを選択します。



2. 上部のバーで、「**Reboot**」タブを選択します。
3. 「**Reboot**」をクリックして、このデバイスを再起動します。

ログ

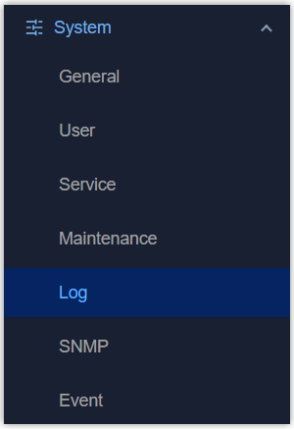
この章では、デバッグに使用するデバイスのログを取得する方法について説明します。

前提条件

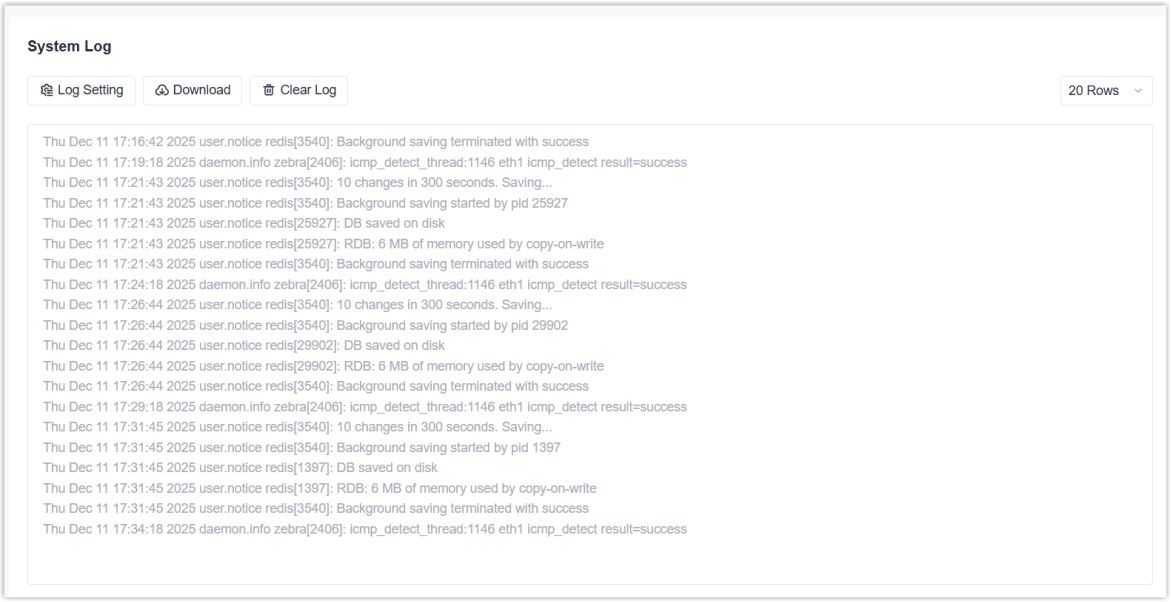
デバイスのシステム時刻が正しいことを確認してください。

手順

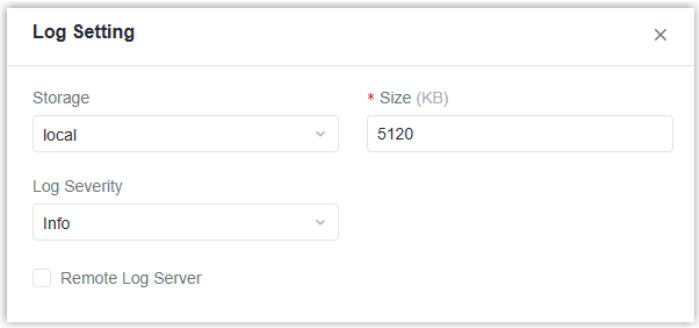
1. 左側のバーで、**[System] > [Log]** ページを選択します。



2. ビューにシステムログが表示されます。ビューのログを更新する必要がある場合は、他のページに切り替えてから、このページに戻ってください。



3. 「**Log Setting**」をクリックして関連するパラメータを設定し、「**Save**」をクリックしてください。



Parameter	説明
Storage	ログの保存場所を選択してください。
Size	保存するログファイルのサイズを設定します。
Log Severity	ログを表示する重大度を選択してください。テクニカル対応にログを送信する場合は、ログの重大度を「デバッグ」に設定することをお勧めします。 **注：** ログの重大度を変更した後、問題が再現されるか確認し、ログに詳細が記録されていることをご確認ください。
Remote Log Server	すべてのログファイルをリモートサーバーに送信するかどうかを有効または無効にします。 **Syslog Address：**リモートログサーバーのアドレス（IP アドレスまたはドメイン名）を設定します。 **Port：**リモートログサーバーのポートを設定します。

4. 必要に応じて、「**Download**」をクリックしてすべてのログファイルをダウンロードしてください。ログファイルを解凍して直接確認することも、Milesightのテクニカルサポートにすべて送信することも可能です。

SNMP

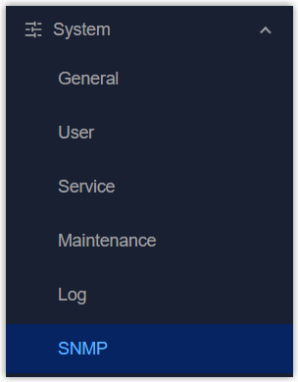
この章では、本デバイスのSNMP機能の概要について説明します。

概要

Simple Network Management Protocol (SNMP) は、情報の収集やネットワークデバイスの設定に使用されるネットワーク管理プロトコルです。

手順：

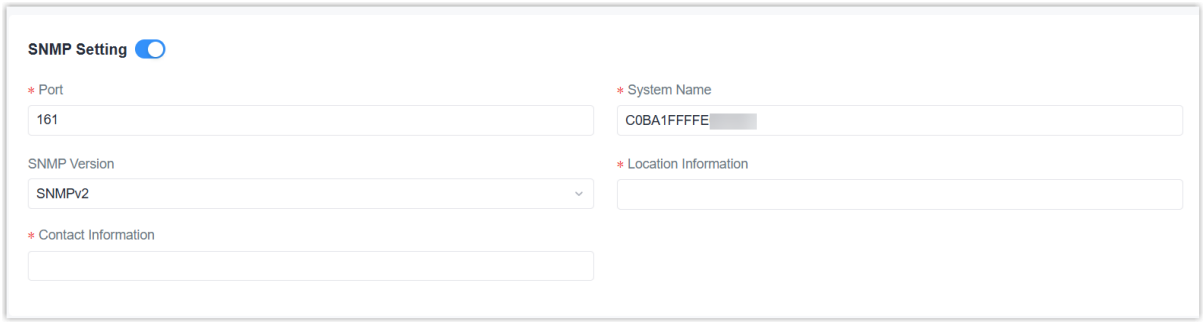
1. 左側のバーで、**[System] > [SNMP]** ページを選択します。



2. **SNMP**タブを選択してSNMP機能を有効にし、一般的なSNMP情報を設定した後、**[Apply]** をクリックして設定を保存します。
3. （任意）**[MIB ビュー]** タブを選択して、異なるアクセス範囲を定義するための MIB ビューを追加し、**[Apply]** をクリックして設定を保存します。
4. （任意）**[VACM]** タブを選択して、アクセス権限を管理するコミュニティやユーザーを追加し、**[Apply]** をクリックして設定を保存してください。
5. （任意）**[Trap]** タブを選択して SNMP トラップ機能を有効にし、SNMP トラップを受信するための情報を設定してから、**[Apply]** をクリックして設定を保存してください。
6. 「**MIB**」タブを選択してMIBファイルをダウンロードし、そのファイルを任意のSNMP MIBブラウザツールにインポートして、デバイスのステータスや設定変数を確認してください。

SNMP設定

このページは、一般的な SNMP 情報を設定するために使用します。

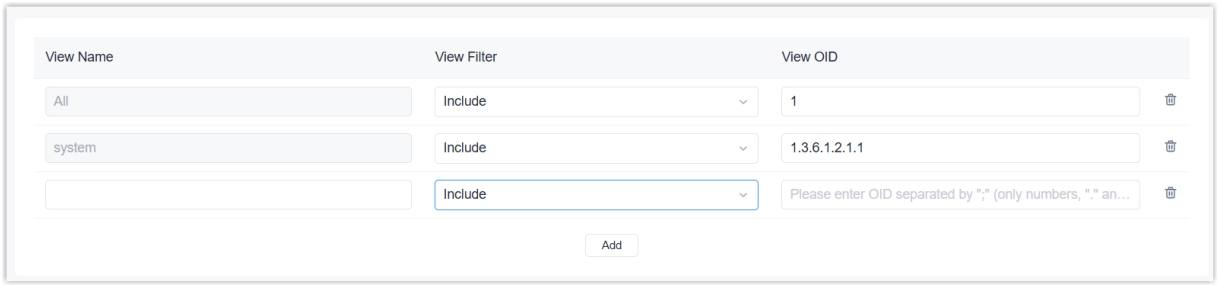


Parameter	説明
SNMP Setting	デバイスを SNMP エージェントとして動作させるかどうかの設定を行います。
Port	SNMP サービスのポートです。

Parameter	説明
System Name	このデバイスシステムを表す名前です。
SNMP Version	SNMPv1、SNMPv2、SNMPv3の中からバージョンを選択してください。
Location Information	システムの設置場所。
Contact Information	システムの連絡先情報です。

MIB ビュー

このページは、アクセス範囲を定義するためのMIBビューを追加・管理するために使用します。

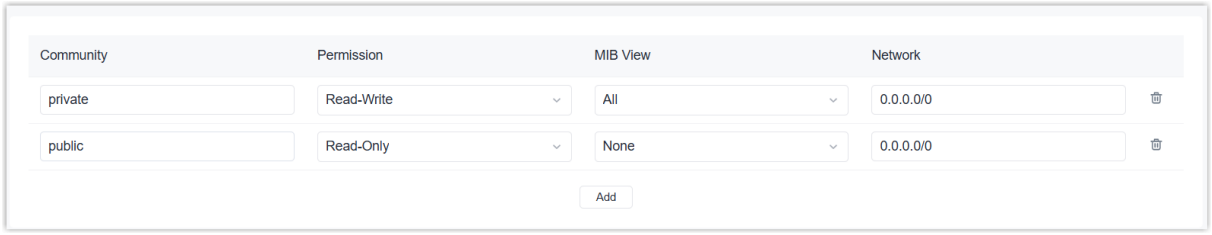


Parameter	説明
Add	MIB ビューを追加します。
View Name	一意の MIB ビュー名を定義します。
View Filter	この MIB ビューの OID 範囲を定義するフィルタオプションを選択してください。 **Include:** MIB 内のリストされた OID へのアクセスのみを対応します。 **Excluded :** リストされた OID 以外の MIB へのアクセスを対応します。
View OID	アクセス対象の OID または除外する OID をセミコロンで区切って入力してください。
	この MIB ビューを削除します。

VACM

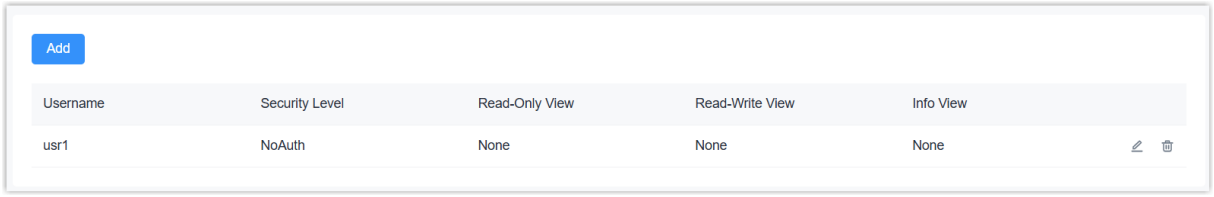
このページは、コミュニティ/ユーザーのアクセス権限を追加および管理するために使用します。

SNMP バージョンが SNMPv1/SNMPv2 の場合



Parameter	説明
Add	コミュニティを追加します。
Community	追加コミュニティを追加します。
Permission	このコミュニティのアクセス権限を選択してください。
MIB View	このコミュニティでアクセス可能なMIBビューを選択してください。
Network	このMIBビューへのアクセスを許可する外部IPアドレス/サブネットを入力してください。 0.0.0.0/0はすべて許可することを意味します。
	このコミュニティを削除します。

SNMPバージョンがSNMPv3の場合

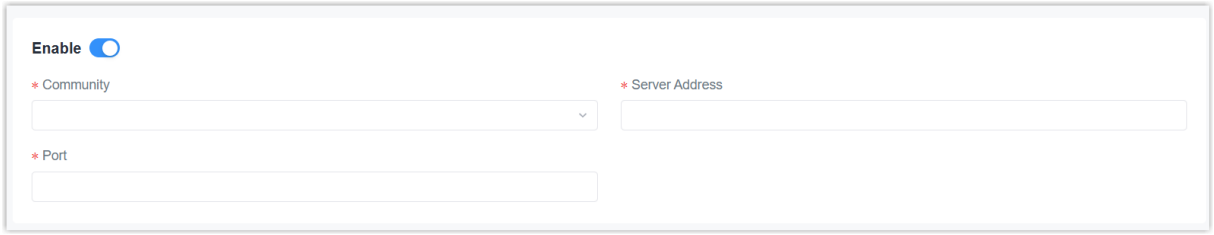


Parameter	説明
Add	SNMPv3 ユーザーを追加します。
Username	一意のユーザー名を定義します。
Security Level	このユーザーの認証方式を選択してください。 **NoAuth**：認証なし、プライバシーなし。 **Auth/NoPriv**：認証あり、プライバシーなし。 **Auth/Priv**：認証あり、プライバシーあり。 「Auth/NoPriv」または「Auth/Priv」が選択されている場合は、認証アルゴリズムとパスワードを設定する必要があります。「Auth/Priv」が有効になっている場合は、暗号化アルゴリズムとパスワードを設定する必要があります。

Parameter	説明
Read-Only View	この権限を割り当てるMIBビューを選択してください。
Read-Write View	
Notify View	
	このユーザーを編集します。
	このユーザーを削除します。

トラップ

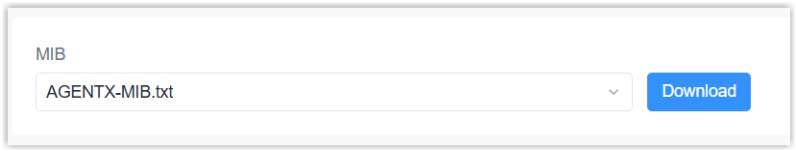
このページは、SNMPトラップの設定を行うために使用されます。SNMPトラップは、重要なイベントが発生した際に、SNMPマネージャーに対してリアルタイムかつ自発的なアラートメッセージを送信するために使用されます。これにより、マネージャーが更新情報をポーリングするのを待つことなく、即座に通知を行うことができます。



Parameter	説明
Enable	SNMPトラップ機能を有効または無効にします。
Community/User	SNMPトラップを送信するコミュニティ/ユーザーを選択します。
Server Address	SNMPトラップを送信するIPアドレスまたはドメイン名です。
Port	SNMPトラップを送信するサーバーのポートです。

MIB

このページは、MIBファイルをダウンロードするために使用します。これらのファイルはMIBブラウザにインポートすることで、このデバイスのステータスおよび設定変数にアクセスできます。



イベント

この章では、デバイス関連のイベントを記録するためのイベント設定について説明します。

イベント一覧

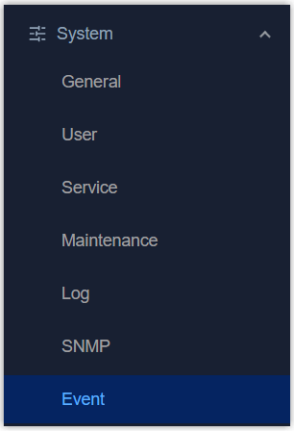
このセクションでは、デバイスに関連するイベントを一覧表示します。

Time	Type	Message
2025-12-11 13:49:07	Power On	Power On
2025-12-11 13:49:02	Ethernet up	ETH1 WAN up
2025-12-11 11:59:01	Ethernet up	ETH1 WAN up
2025-12-11 11:58:58	Ethernet down	ETH1 WAN down
2025-12-11 11:49:37	Power On	Power On
2025-12-11 11:49:32	Ethernet up	ETH1 WAN up
2025-12-11 09:05:49	Power On	Power On
2025-12-10 01:00:58	Power On	Power On
2025-12-09 02:55:58	Power On	Power On
2025-11-28 01:03:41	Power On	Power On

前提条件：デバイスのシステム時刻が正しいこと。

手順：

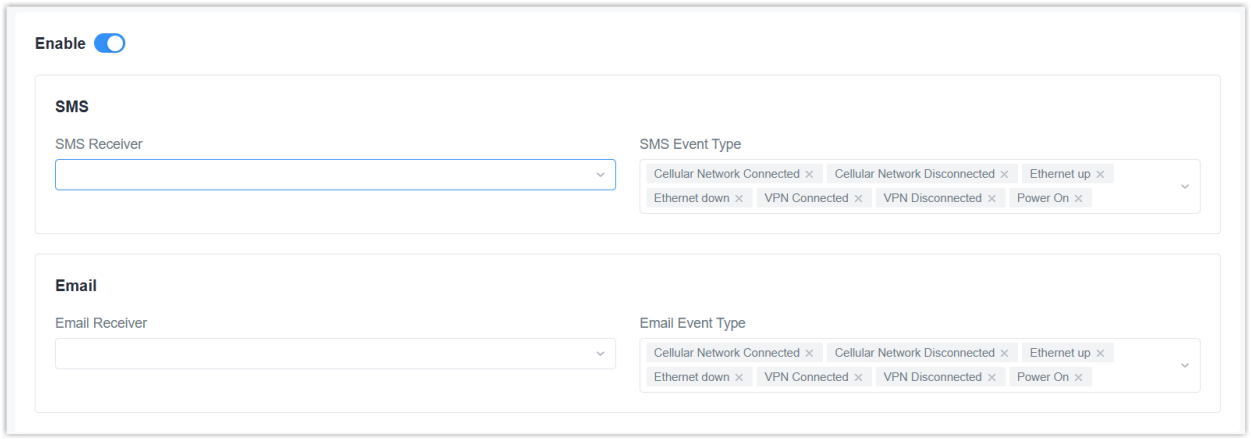
1. 左側のバーで、**[System] > [Event]** ページを選択します。



2. 上部バーで、「**Event List**」タブを選択します。一覧には、デバイスに関連するイベントが表示されます。

イベント通知

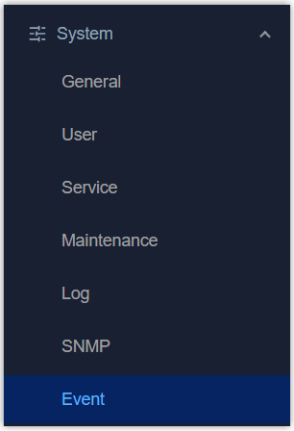
このセクションでは、イベントアラームを受信するためのメールまたは電話の受信先を設定します。



前提条件：メールグループまたは電話グループが追加されていること。

手順：

1. 左側のバーで、「**System**」>「**Event**」ページを選択します。



2. 上部のバーで、「**Event Notification**」タブを選択してください。
3. イベント通知を有効にしてください。
4. 必要に応じて、イベントメールを送信するメールグループとイベントの種類を選択してください。
5. 必要に応じて、イベントSMSを送信する電話グループとイベントタイプを選択してください。
6. 「**Apply**」をクリックして設定を保存します。

第9章. アプリ

Python

この章では、デバイス上で Python アプリを実行する手順について説明します。

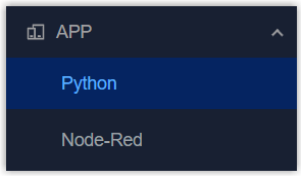
前提条件

- Pythonアプリをインポートするのに十分なデバイス容量があることを確認してください。
- Milesightの公式ウェブサイトからPython SDKをダウンロードしてください。
- Pythonアプリを開発し、ZIPファイルにパッケージ化してください。

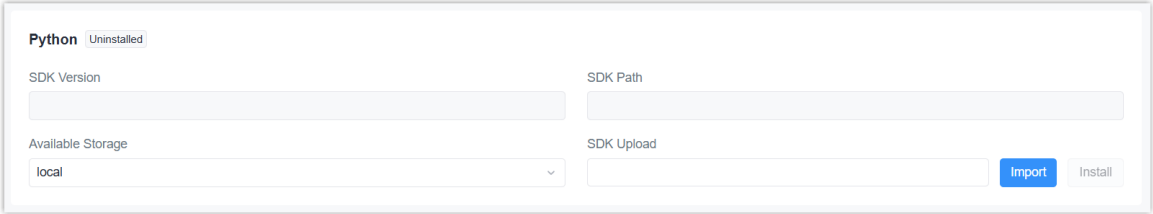
手順

Python SDKのインストール

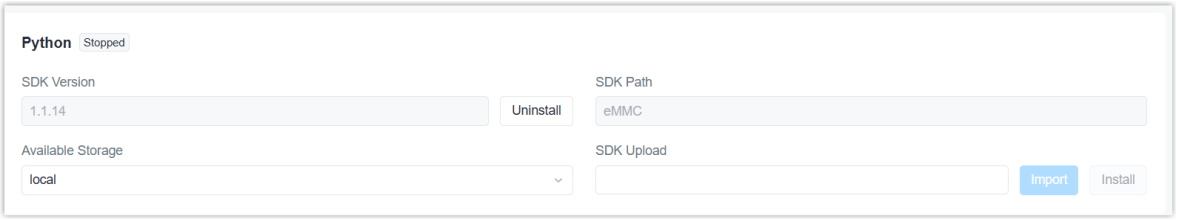
1. 左側のバーで、**[APP] > [Python]** ページを選択します。



2. 上部のバーで、「**Python**」タブを選択します。
3. **[Import]** をクリックし、ローカルパスから Python SDK ファイルを選択します。



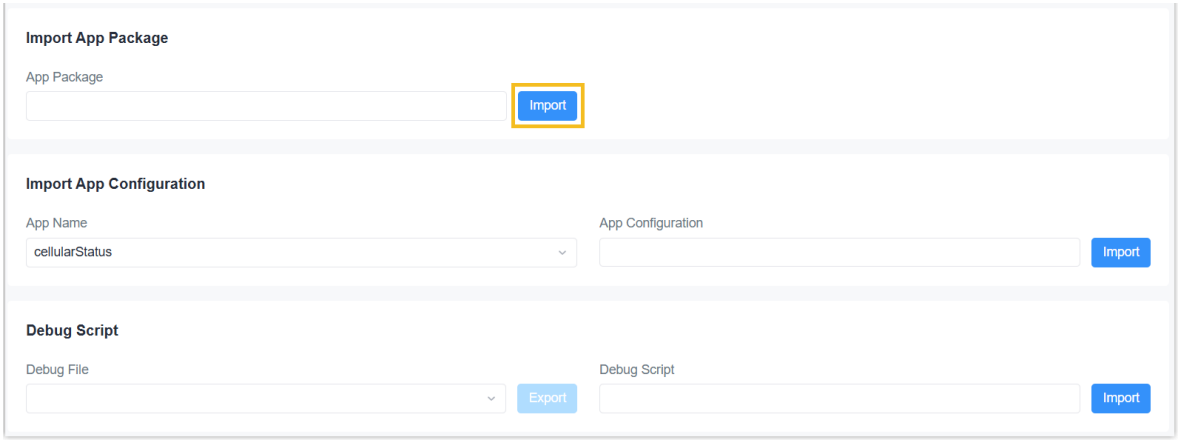
4. 「**Install**」をクリックして、Python SDKをインストールしてください。インストールが完了すると、SDKの



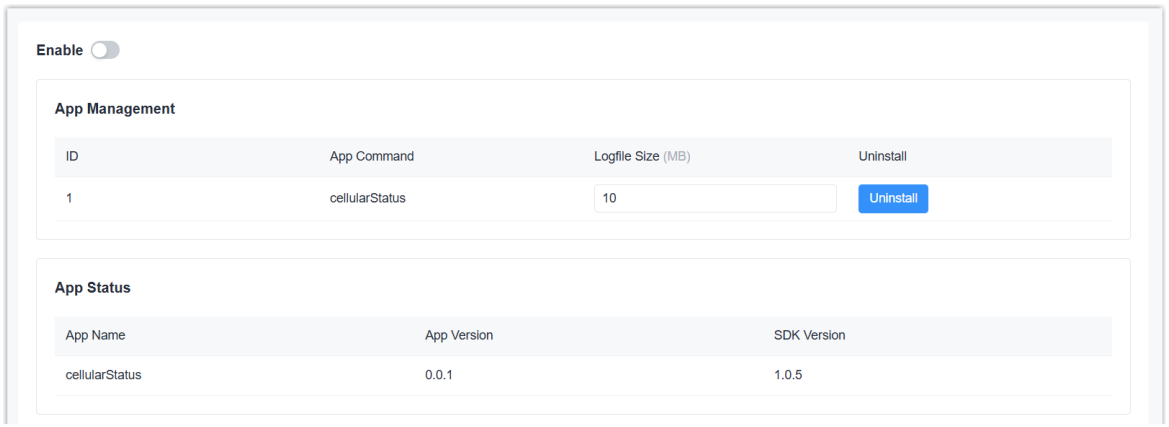
バージョンとパスが表示されます。

Pythonアプリのインストールとアンインストール

1. 上部バーの「**Python APP**」タブを選択してください。
2. 「**Import**」をクリックし、ローカルパスからアプリファイルを選択してアプリをインポートします。

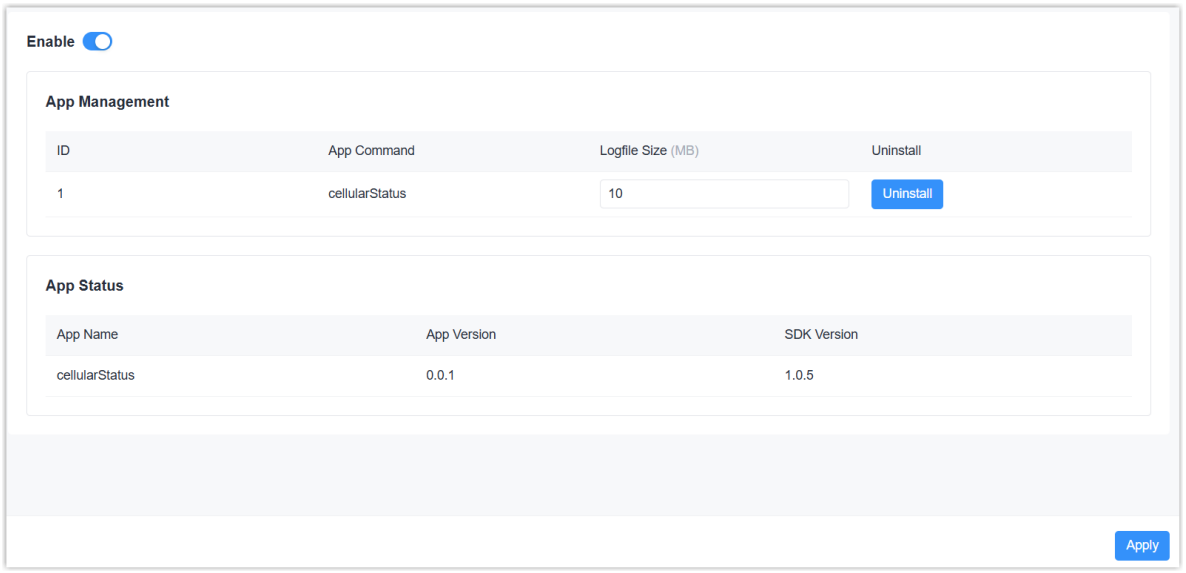


アプリが正常にインポートされると、**AppManagerの「設定」**ページに表示されます。必要に応じて必要に応じて「**Uninstall」をクリックしてください。**

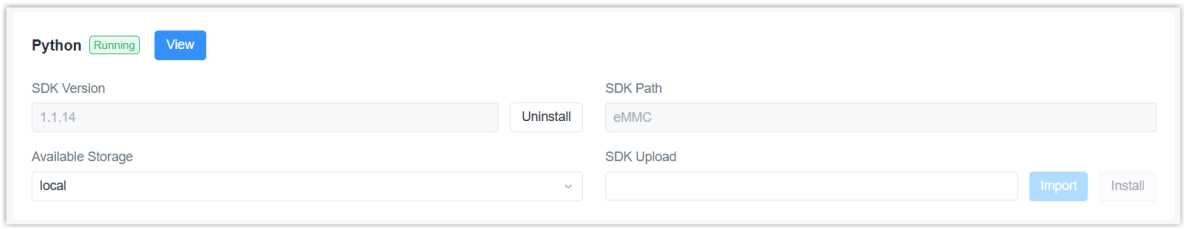


Pythonアプリを実行する

1. 上部のバーで、「**AppManager Configuration**」タブを選択してください。
2. 「App Management」機能を有効にし、「**Apply**」をクリックして設定を保存します。



3. 上部のバーで、「**Python**」タブを選択します。
4. Pythonのステータスが「**Running**」と表示されます。「**View**」をクリックして、アプリの実行状況とログを確認してください。



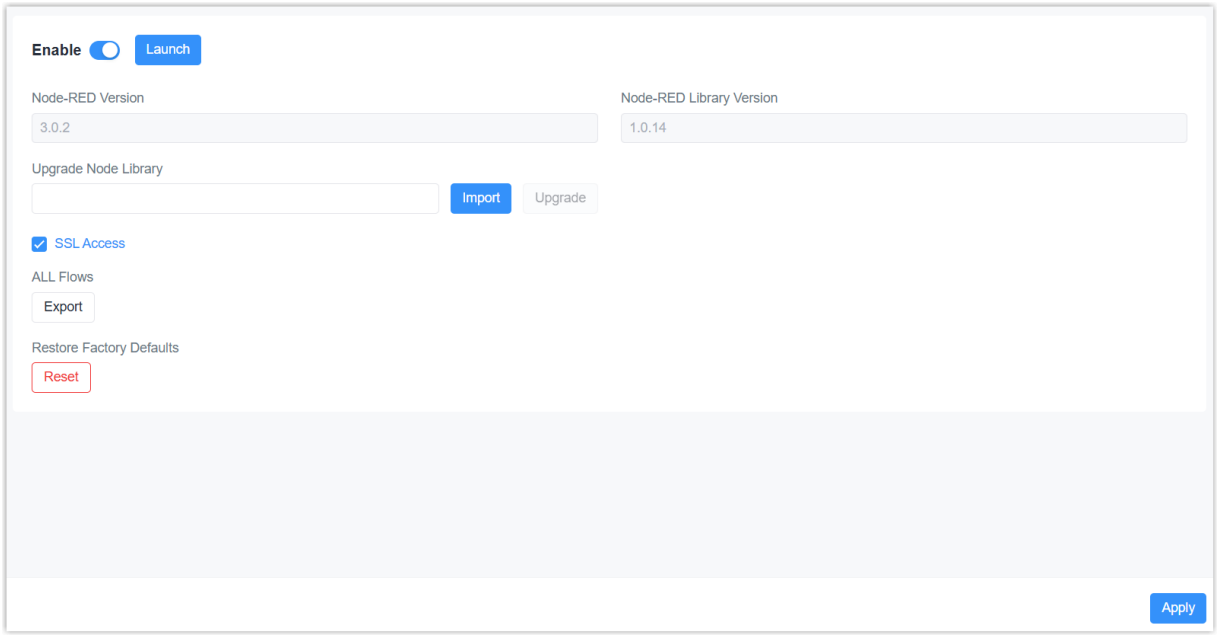
Node-RED

本ゲートウェイには、Node-REDツールが組み込まれています。この章では、本ゲートウェイのNode-REDソフトウェアについて紹介します。

概要

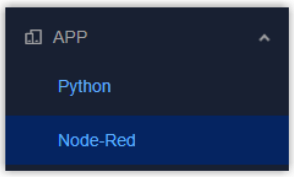
Node-REDは、IoT（モノのインターネット）の一環として、ハードウェアデバイス、API、オンラインサービスを視覚的にプログラミングし、相互に接続するためのフローベースの開発ツールです。Node-REDはWebブラウザベースのフローエディタを提供しており、パレットにある多種多様なノードを使用して、フローを簡単に接続することができます。詳細については、Node-REDの公式ウェブサイトをご覧ください。

Node-RED を起動します



手順：

1. 左側のバーで、**[APP] > [Node-RED]** ページを選択します。



2. Node-REDを有効にします。
3. HTTPS経由でNode-REDにWebアクセスする必要がある場合は、「**SSL Access**」オプションを有効にしてください。HTTP経由でNode-REDにWebアクセスする必要がある場合は、「**SSL Access**」オプションを無効にしてください。
4. 「**Apply**」をクリックして設定を保存し、Node-REDを起動してください。
5. 「**Launch**」をクリックして、Node-REDのWeb GUIを開きます。
6. ゲートウェイのWeb GUIと同じ認証情報を使用して、Node-REDのWeb GUIにログインしてください。

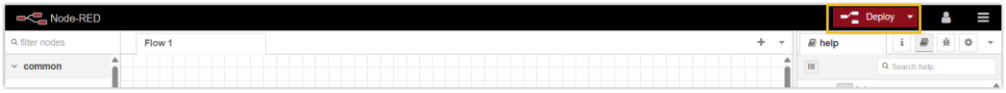
新しいNode-REDフローを作成します

以下は、Node-REDフローを作成するための基本的な手順です。詳細については、Node-REDユーザーガイドをご参照ください。

手順：

1. 「+」をクリックして、新しいフローを追加します。
2. 任意のノードをワークスペースにドラッグ＆ドロップします。

3. 必要に応じて、一部のノードのパラメータを設定します。
4. ノード同士を接続してフローを作成します。
5. 右上の「**Deploy**」をクリックして設定を保存します。



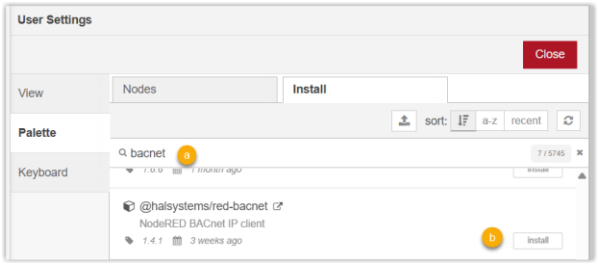
6. フローを起動し、結果を確認してください。

Node-RED ライブラリの更新

ノードは、フローを作成するための基本的な構成要素です。本デバイスには、Node-RED公式ライブラリの基本ノードと、Milesightのカスタムノードがプリロードされています。

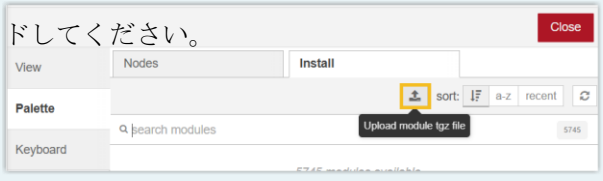
Node-RED 公式ライブラリモジュールのインストール

1. 「**Launch**」をクリックして Node-RED Web GUI を開き、ログインしてください。
2. 右上隅の「 」をクリックし、「**Manage palette**」を選択します。
3. 「**Install**」タブを選択し、モジュール名を検索して、インストールしたいモジュールを選択してください。これを行うには、デバイスがインターネットに接続されている必要があります。



注：

デバイスがインターネットに接続できない場合は、Node-RED公式ライブラリからnode-redモジュールパッケージを検索してダウンロードし、そのファイルをデバイスにアップロードしてください。



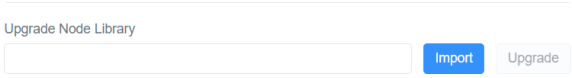
カスタム Node-RED ライブラリの更新

デバイスには、デバイスのプログラムやアプリケーションに関連するカスタムノードがプリロードされています：

Node	Description
LoRa Input	LoRaWAN® ネットワークから受信したすべての LoRaWAN® パケットを入力します。
LoRa Output	特定の LoRaWAN® エンドデバイスにダウンリンクコマンドを送信します。
Device Filter	デバイス EUI に基づいて、入力された LoRaWAN® パケットをフィルタリングします。
GW Info	デバイスのイベントを監視します。これを行うには、まずイベント通知を有効にする必要があります。
Email Output	カスタムメールを送信します。「SMTP オプション」が**Sameasgateway**に設定されている場合は、まず 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。この機能は-L08GLモデルのみで利用可能であり、セルラー接続が有効であることを確認してください。
SMS Output	SMSメッセージを送信します。この機能は-L08GLモデルのみ利用可能で、セルラー接続が有効になっていることを確認してください。

このカスタムライブラリを更新するには、以下の手順に従ってください：

1. Milesightからカスタムノードライブラリパッケージを受け取ります。
2. 「**Import**」をクリックしてローカルパスからライブラリパッケージを選択し、次に「**Upgrade**」をクリックします。



Docker

本ゲートウェイにはDockerが組み込まれています。本章では、本ゲートウェイのDocker機能について説明します。

前提条件

- 利用可能なRAMは1GB以上、利用可能なフラッシュメモリは6GB以上を確保することをお勧めします。
- SSH または TELNET アクセスサービスは、[General settings] で有効になっています。
- SSH/TELNETツール（Puttyなど）

基本的な手順

1. SSH/TELNET ツールを開き、ゲートウェイの IP アドレスを入力して CLI にアクセスします。
2. ユーザー名「**admin**」と、Web GUIと同じパスワードを使用してCLIにログインしてください。

3. Docker の情報を確認し、必要に応じて動作を行うためのコマンドを入力してください。詳細については、Docker のドキュメントをご参照ください。

第10章 サービス

Milesightは、お客様に迅速かつ包括的なテクニカルサポートサービスを提供しています。エンドユーザー様は、お近くの販売代理店に連絡してテクニカルサポートを受けることができます。販売代理店および再販業者様は、Milesightに直接連絡してテクニカルサポートを受けることができます。

テクニカルサポートのメールアドレス：

iot.support@milesight.com オンラインサポートポータル：

https://support.milesight-iot.com

リソースダウンロードセンター：https://www.milesight.com/iot/resources/download-center/

Milesight CHINA

TEL：+86-592-5085280

FAX：+86-592-5023065

Add: Building C09, Software Park Phase III, Xiamen 361024, Fujian, China

ウェーブクレスト株式会社
https://www.wavecrestkk.co.jp/ms/