robustel | Software Manual

RobustOS Software Manual

robustOS

Guangzhou Robustel Co., Ltd.(広州ロブステル有限公司)

www.robustel.com

このドキュメントについて

このドキュメントでは 、機能の紹介や動作設定など、RobustOS ベースの DTU、ルーター、およびゲートウェイ製品の Web インターフェイス情報について説明します。

関連製品

M1200、M1201
R1500、R1510、R1510 Lite、R1511、R1511P、R1520
R2000、R2000 Dual、R2000 Ent、R2010、R2011、R2110
R3000、R3000 Lite、R3000 Quad、R3000 LG、R3010
R5020、R5020 Lite
R5010 の

商標と許可

robustel &はrobustOS Guangzhou Robustel Co., Ltd.の商標です。 本書に記載されているその他すべての商標および商号は、それぞれの所有者に帰属します。

免責事項

著作権所有者の書面による許可なしに、ドキュメント全体を いかなる形式でも複製することはできません。
このドキュメントの内容は、方法論、設計、および製造の継続的な進歩により、予告なしに変更される場合があります。Robustel は、このドキュメントの誤った使用に起因するいかなる種類のエラーまたは損害についても責任を負わないものとします。

テクニカルサポート

電話番号: +86-20-82321505
電子メール： support@robustel.com
ウェブ： www.robustel.com

ドキュメント 履歴

ドキュメントのバージョン間の更新は累積的です。したがって、最新のドキュメントバージョンには、以前のバージョンに加えられたすべての更新が含まれます。

日付	ドキュメントのバージョン	ファームウェアバージョン	変更の説明
2022 年 8 月 1 日	V1.0.0	V5.0.0 以降	1. 初期リリース
2022 年 10 月 16 日	V1.1.0	V5.1.0 以降	RobustOS V5.1.0 以降に対応しました。
2023 年 10 月 26 日	V5.2.0	V5.2.0 以降	RobustOS V5.2.0 以降に対応しました。

内容

1. 紹介

このソフトウェアマニュアルは、DTU、ルーター、ゲートウェイ製品を含むすべての RobustOS ベースの製品に使用され、Web インターフェイス情報(設定と操作)を提供します。
ハードウェア構成やインターフェイスはモデルによって異なる場合があるため、特定の章を参照してください 。

関連製品	M1200 型	M1201 の	R1510 の	R1510 ライト	R1511 の	R1520 の	R2010 の	R2011 (英語)	R2110 型	R3000 型	R3000 ライト	R3000 クワッド	R3000 LG 電子	R3010 型	R5020 の	R5010 の
SIM カード	2	1	1	1	1	2	2	2	2	2	2	2	2	1	2	2
イーサネット	-	-	2	1	2	5	2	5	4	2	1	4	2	2	4	1
PoE PD	-	-	-	-	-	*	*	*	*	-	-	-	-	-	*	√
PoE PSE	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Wi-Fi 接続	-	-	√	-	√	√	√	√	√	*	-	*	-	-	√	-
BLE の	-	-	-	-	-	-	-	-	*	-	-	-	-	-	-	-
GNSS 測量 (GNSS)	-	-	-	-	-	*	-	-	*	*	-	*	*	-	*	-
DI	2	-	√	-	-	√	√	-	√	2	-	-	2	-	√	-
DO	√	-	√	-	-	√	√	-	√	2	-	-	-	-	√	-
AI	-	-	-	-	-	√	-	-	-	-	-	-	-	-	-	-
RS232	√	*	-	-	*	√	*	-	√	√	√	*	*	√	√	-
RS485	√	*	-	-	*	√	*	-	√	√	√	*	*	√	√	-
USB ホスト	-	-	-	-	-	√	-	-	√	√	√	√	√	√	√	√
RS422	-	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CAN	-	*	-	-	-	-	-	-	-	-	-	-	-	√	-	-
音声(FXS)	-	-	-	-	-	-	-	-	-	-	-	-	-	√	-	-
マイクロ SD	-	-	-	-	-	-	-	-	√	√	-	√	√	-	√	-

注: √ = サポート対象外、 = オプション*

RobustOS について

RobustOS は、Robustel デバイス用に設計された Robustel の自社開発の Linux ベースのオペレーティングシステムです 。RobustOS には、基本的なネットワーク機能とプロトコルが含まれており、優れたユーザーエクスペリエンスを提供します。一方、Robustel は、パートナーや顧客が C および C++を使用して追加のカスタマイズを可能にするソフトウェア開発キット(SDK)を提供しています 。また、細分化された IoT 市場の需要を満たすための豊富なアプリも提供します。

2. 初期設定

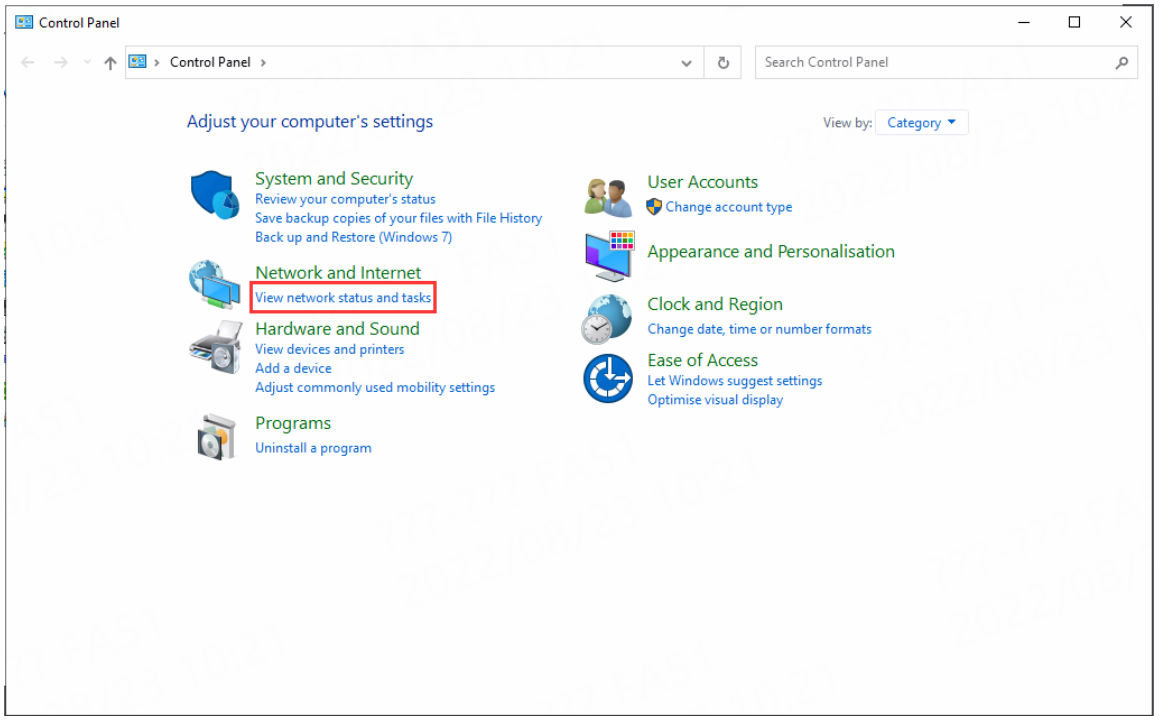
デバイスは、Microsoft Edge、Google Chrome、Firefox などの Web ブラウザーから構成できます。Web ブラウザは、Ubuntu、macOS、Windows7/8/10/11 などのオペレーティングシステムの標準アプリケーションです。設定のための簡単でユーザーフレンドリーなインターフェースを提供します。デバイスを接続するには、外部リピーター/ハブを介して、または PC に直接接続するなど、さまざまな方法があります。ただし、デバイスを接続する前に、PC にイーサネットポートが装備されていることを確認してください。DHCP サーバーを介して IP アドレスを取得するか、デバイスと同じサブネット内にある必要がある固定 IP アドレスを取得するように PC を構成する必要があります。 デバイスの Web インターフェイスへのアクセスで問題が発生した場合は、デバイスの IP アドレスへのアクセスに問題が発生する傾向があるため、PC からファイアウォールプログラムをアンインストールすることをお勧めします。

1) 2.1 PC 設定

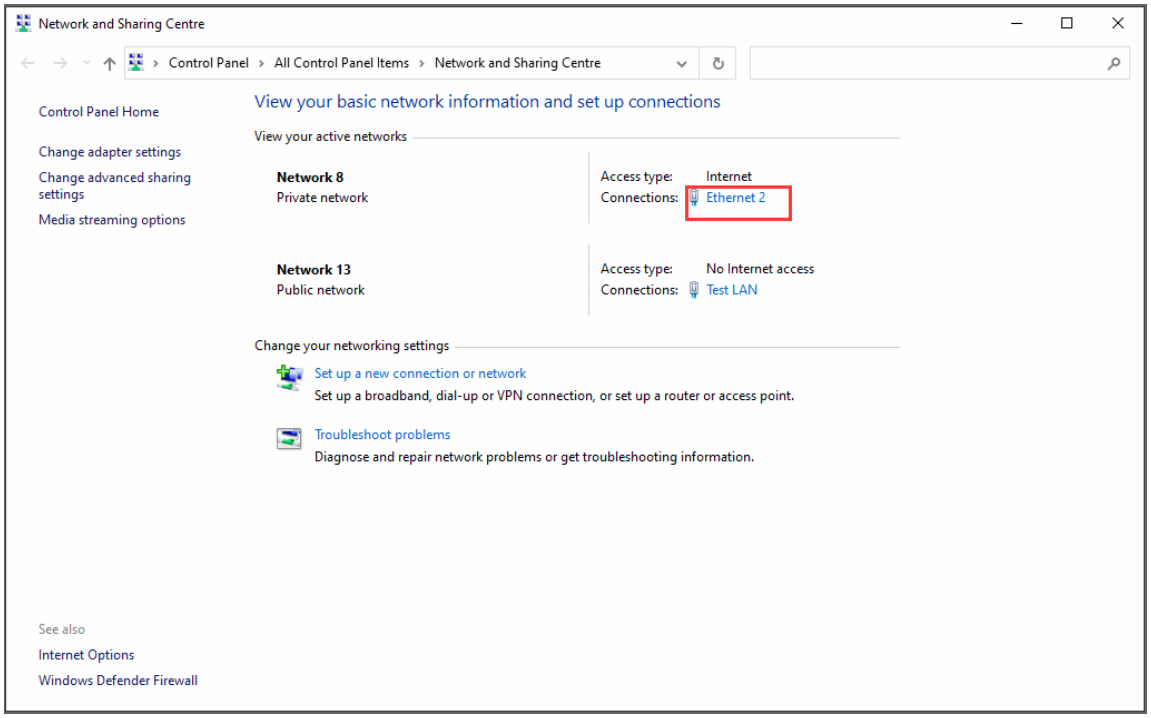
コンピュータの IP アドレスを取得するには、2 つの方法があります。1 つは「ローカルエリア接続」から IP アドレスを自動的に取得する方法で、もう 1 つはデバイスの同じサブネット内で静的 IP アドレスを手動で構成する方法です。以下の手順を参照してください。

ここでは、**例として Windows10** を取り上げます。Windows 7 以降の構成も同様です。

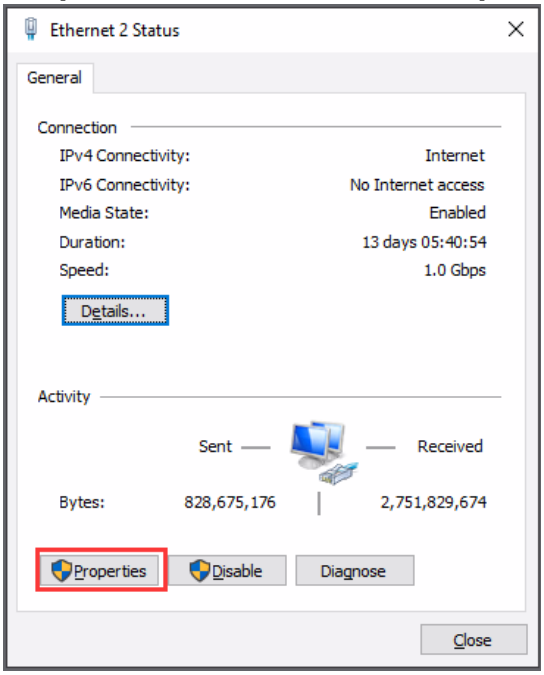
2. キーボードの Windows ロゴ  キー (以下、Win キー)を見つけて **Win + R** を押し、「**Control**」と入力して**コントロールパネル**を実行します。コントロールパネルを開いた後、「**ネットワークステータスとタスクの表示**」を左クリックします。



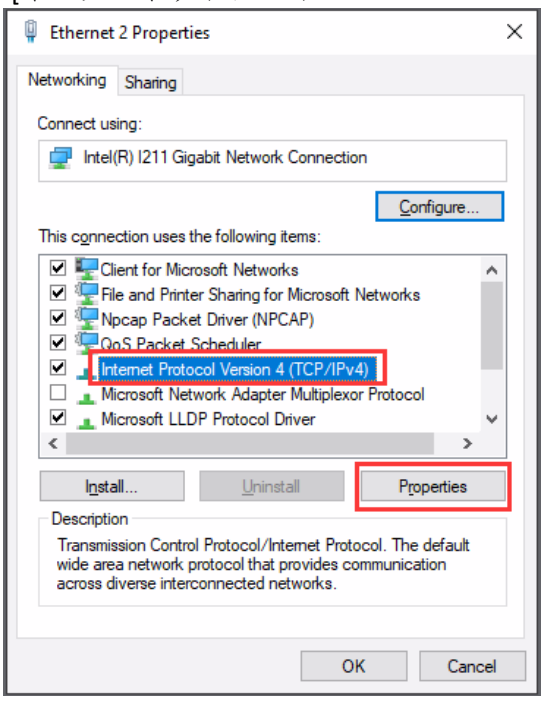
3. 「**ネットワークと共有センター**」に入った後、「**イーサネット**」接続ステータスをクリックします。



4. [ローカルエリア接続**ステータス**]ウィンドウで[**プロパティ**]をクリックします。

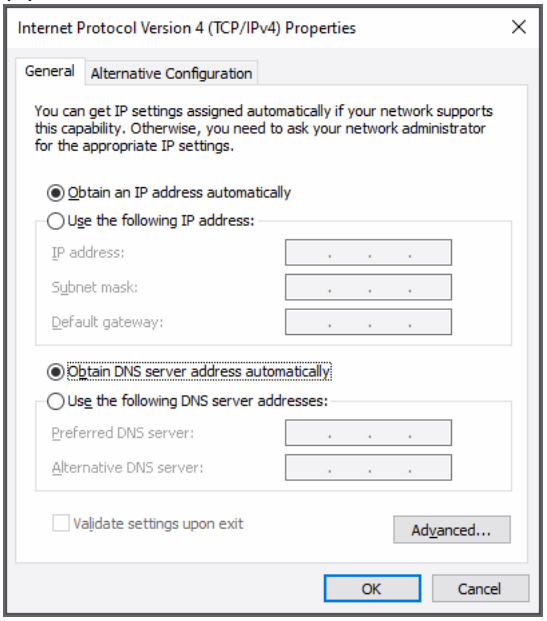


5. [インターネット プロトコル **バージョン 4 (TCP/IPv4)]** を選択し、[プロパティ]をクリックします。

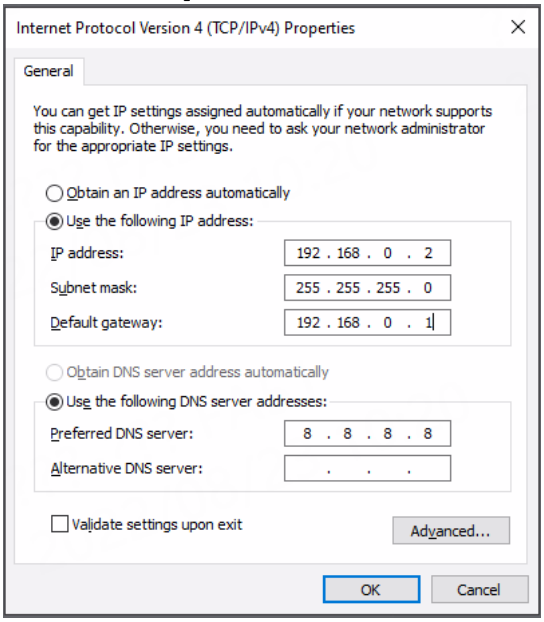


6. コンピュータの IP アドレスを構成する 2 つの方法。

(1) DHCP サーバーから自動取得し、「**IP アドレスを自動的に取得する**」をクリックします。



(2)デバイスアドレスと同じサブネット上の静的 IP アドレスを使用して PC を手動で構成し、**[次の IP アドレスを使用する]をクリックして構成します。**



7. **[OK]**をクリックして構成を終了します。

2.2 工場出荷時のデフォルト設定

デバイスを構成する前に、次のデフォルト設定を知っておく必要があります。

アイテム	説明
ユーザー名	管理者
パスワード	管理者
ETH0	WAN モードまたは 192.168。 0.1/255.255.255.0、LAN モード。
ETH1/2/3/4(※)	192.168.0.1/255.255.255.0、LAN モード。
DHCP サーバ	有効

※ デバイスによって ETH ポート数に違いがあります。詳細については、デバイスの製品仕様を参照してください。

2.3 工場リセット

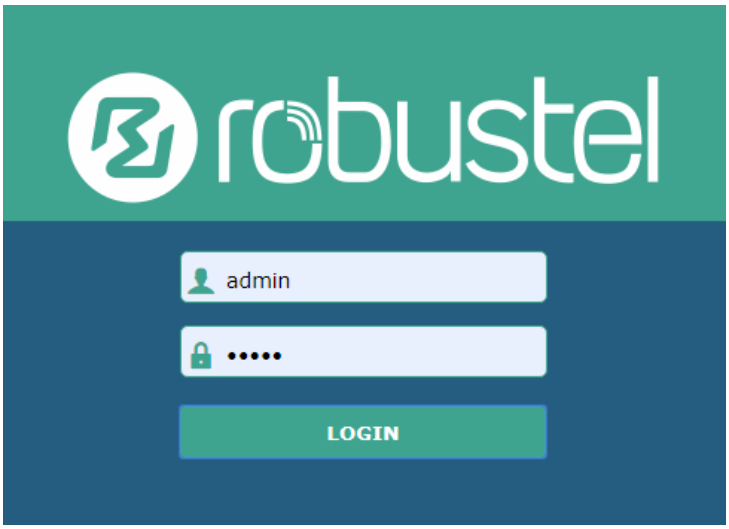
機能	操作
リブート	動作状態で RST ボタンを 2~5 秒間押し続けます。
デフォルトに復元構成	動作状態で RST ボタンを 5~10 秒間押し続けます。実行ライトがすばやく点滅してから RST ボタン を離すと、デバイスはデフォルト構成に戻ります。
工場出荷時の状態に戻す構成	デフォルト設定の復元操作が 1 分以内に 2 回実行されると、デバイスは工場出荷時のデフォルト設定に復元されます。

2.4 デバイスにログインする

管理ページにログインしてデバイスの構成ステータスを表示するには、以下の手順に従ってください。

1. PC でブラウザを起動します。 例:Microsoft Edge、Google Chrome、Firefox など
2. Web ブラウザーから、次のように入力します。 デバイスの IP アドレスをアドレスバーに入力し、Enter キーを押します.デフォルトのデバイスの IP アドレスは http://192.168.0.1/ です。ただし、実際のアドレスは異なる場合があります。
   注:パブリック IP アドレスの SIM カードがデバイスに挿入されている場合は、ブラウザのアドレスバーにこの対応するパブリック IP アドレスを入力して、デバイスにワイヤレスでアクセスします。

3. ログインページで、ユーザー名とパスワードを入力し、言語を選択して、[ログイン]**をクリックします**。 デフォルトのユーザー名とパスワードについては、製品ラベルの情報を確認してください。
   注:間違ったユーザー名またはパスワードを 6 回以上入力すると 、ログイン Web が 5 分間ロックされます。



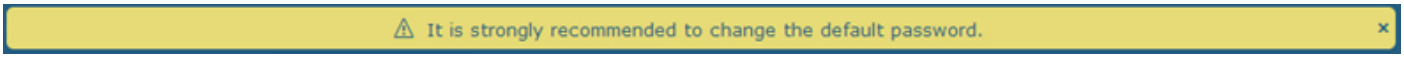
2.5 コントロールパネル

ログイン後、Web インターフェイスのホームページが表示されます。R5020 を例にとってみましょう。

ホームページでは、ユーザーは設定の保存、デバイスの再起動、ログアウトなどの操作を実行できます。

デフォルトのユーザー名とパスワードを使用してデバイスにログイン すると、次のタブにページがポッ

プアップ表示されます



セキュリティ上の理由から、デフォルトのユーザー名やパスワードを変更することを強くお勧めします。

をクリックします。 ボタンをクリックして 通知. ユーザー名やパスワードを変更するには、 3.7.7 システム>ユーザー管理.

コントロールパネル		
アイテム	説明	ボタン
保存 & 適用	クリックすると、現在の設定がデバイスのフラッシュに保存され、すべての設定ページに変更が適用され、変更が有効になります。	Save & Apply
リブート	クリックすると、デバイスが再起動します。[再起動(Reboot)] ボタンが黄色の場合は、完了した設定の一部が再起動後にのみ 有効になることを意味します。	Reboot
ログアウト	クリックすると、現在のユーザーが安全にログアウトされます。ログアウト後、ログインページに切り替わります 。S ログアウトせずに Web ページを直接シャットダウンすると、次の Web ページはタイムアウト前にパスワードなしでこのブラウザで Web にログインできます。	Logout
送信	クリックすると、現在の設定ページで変更が 保存されます。	Submit
キャンセル	クリックすると、現在の設定ページでの変更がキャンセルされます。	Cancel

注: 設定を変更する手順は次のとおりです。

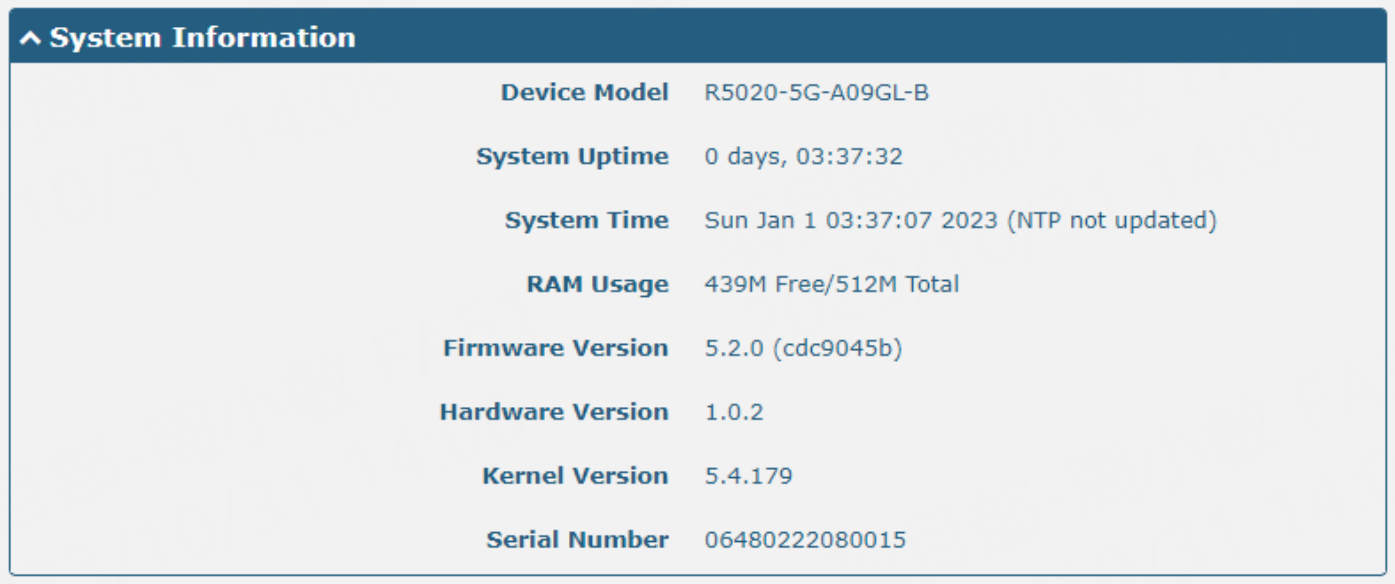
1. 1 ページで変更します。
2. このページの下をクリックし Submit てください。
3. 別のページで変更します。
4. このページの下をクリックし Submit てください。
5. すべての変更を完了します。
6. []をクリックします Save & Apply。

3. WebUI の説明

3.1 ステータス

3.1.1 システム情報

このページでは、デバイスのシステム情報、インターネットステータス、WiFi STA ステータス、および LAN ステータスを表示できます。



システム情報	
アイテム	**説明**
デバイスモデル	デバイスのモデル名を表示します 。
システム稼働時間	デバイスの稼働時間を表示します。
システム時刻	現在のシステム時刻を表示します。
RAM 使用量	空きメモリと合計メモリを表示します。
ファームウェアバージョン	デバイスで実行されているファームウェアのバージョンを表示します。
ハードウェアバージョン	現在のハードウェアバージョンを表示します。
カーネルバージョン	現在のカーネルバージョンを表示します。
シリアル番号	デバイスのシリアル番号を表示します。

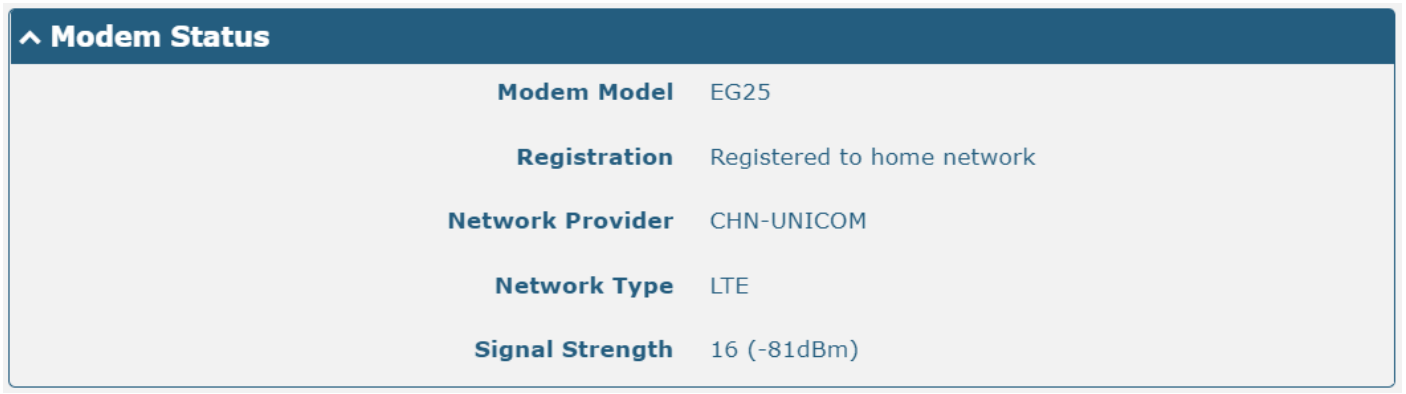
3.1.2 インターネットステータス

このページには、デバイスのインターネットステータス情報が表示されます。

インターネット ステータス	
アイテム	説明
アクティブリンク	現在使用されているリンク(WWAN1、WWAN2、または WAN)を表示します。
アップタイム	リンクが接続されている現在の時間を表示します。
IP アドレス	アクティブリンクの IP アドレスを表示します。
ゲートウェイ	アクティブリンクのゲートウェイアドレスを表示します。
DNS の	現在の DNS サーバーアドレスを表示します。

3.1.3 モデムステータス

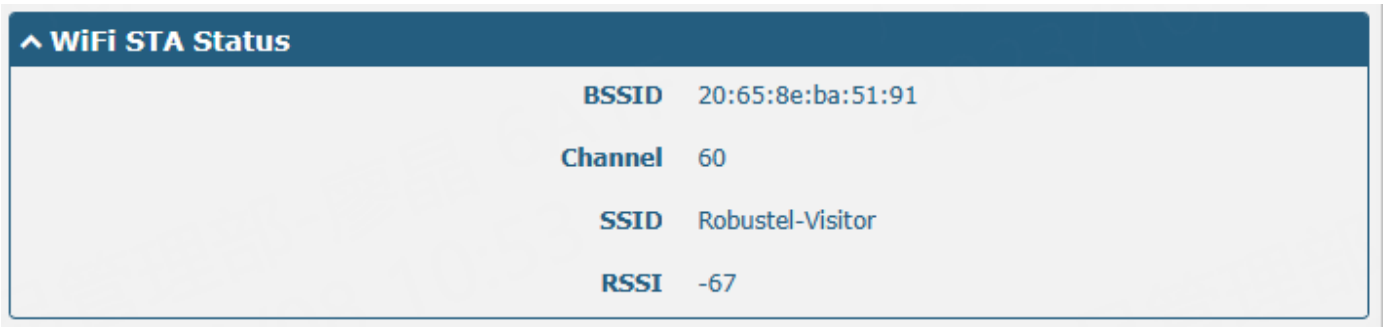
このページには、デバイスの モデム 情報が表示されます。



モデム ステータス	
アイテム	説明
モデムモデル	セルラーモジュールのモデルを表示します。
登録	現在のネットワークステータスを表示します。
ネットワークプロバイダー	ネットワークプロバイダーの名前を表示します。
ネットワークの種類	現在のネットワークサービスの種類を表示します。
信号強度	信号強度の値を表示します。

3.1.4 WiFi STA ステータス

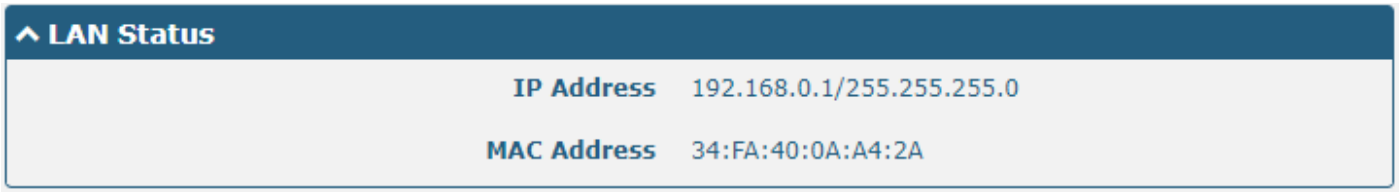
このページは、WiFi ステーションに関する基本的な情報を示しています。



WiFi STA ステータス	
アイテム	説明
BSSID の	デバイスが接続されているワイヤレスアクセスポイントの一意の基本サービス識別子を表示します。
チャンネル	ワイヤレスアクセスポイントに接続されているデバイスの現在のチャネル番号を、ワイヤレスチャネルに対応するものに表示します。
SSID(SSID)	デバイスが接続されているワイヤレスアクセスポイントのサービスセット識別子を表示します。
RSSI の	無線アクセスポイントに接続されている機器の無線信号強度を単位:dBm で表示します。

3.1.5 LAN ステータス

このページには、デバイスの LAN ステータスが表示されます

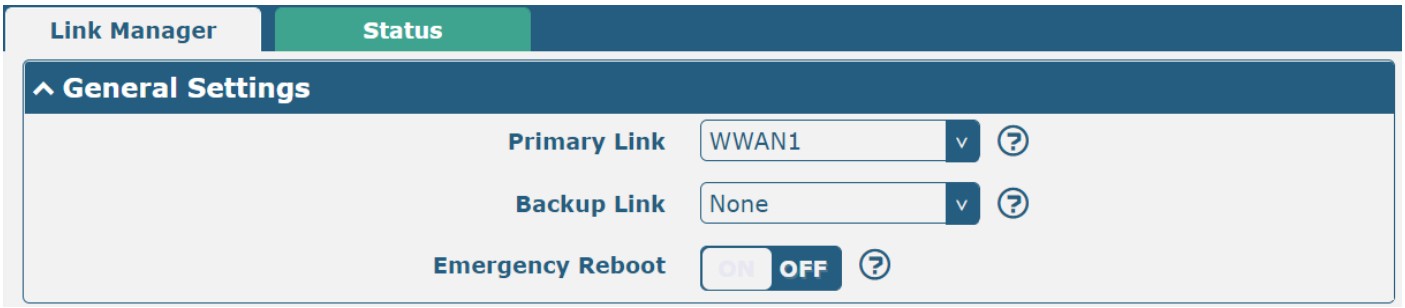


LAN ステータス	
アイテム	説明
IP アドレス	LAN の IP アドレスとネットマスクを表示します。
MAC アドレス	LAN の MAC アドレスを表示します。

3.2 インターフェイス

3.2.1 リンクマネージャ

このページでは、リンク接続を管理できます。リンク管理機能は、シングル/デュアルリンクの選択をサポートしています。同時に、各リンクは、ネットワーク接続を常にオンラインに保つためのリンク検出機能の構成をサポートしています。

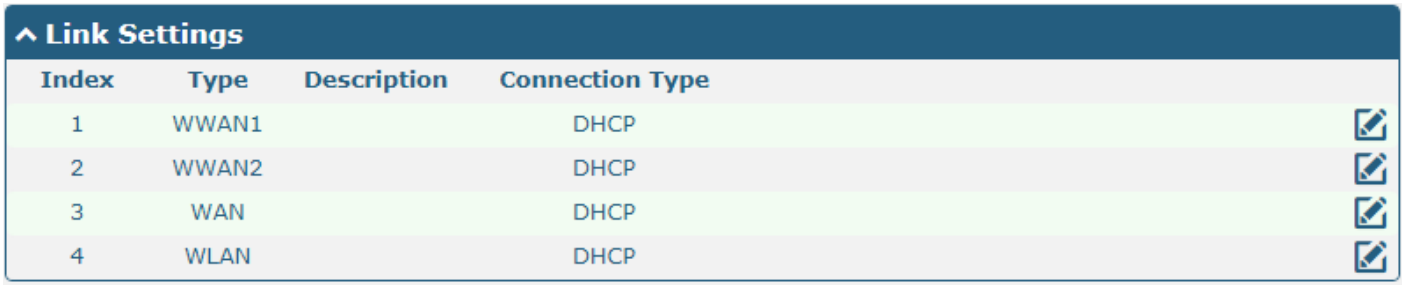


一般設定@ リンクマネージャ		
アイテム	説明	デフォルト
1 次リンク	「WWAN1」、「WWAN2」、「WAN」、または「WLAN」から選択します。 • WWAN1: プライマリ ワイヤレス リンクとして SIM1 を選択します。 • WWAN2: プライマリ ワイヤレス リンクとして SIM2 を選択します。 • WAN:プライマリ有線リンクとして WAN イーサネットポートを選択します。 • WLAN:プライマリワイヤレスリンクとして WLAN を選択します。 *手記： WLAN リンクは、クライアントモードとして Wi-Fi を有効にした場合にのみ使用できます。* ***3.2.5 Wi-Fi 接続***.	WWAN1 の
バックアップ リンク	「 WWAN1」、「WWAN2」、「WAN」、「WLAN」、または「なし」から選択します。 • WWAN1: バックアップ ワイヤレス リンクとして SIM1 を選択します。 • WWAN2: バックアップワイヤレスリンクとして SIM2 を選択します。 • WAN:バックアップ有線リンクとして WAN イーサネットポートを選択します。 • WLAN:バックアップワイヤレスリンクとして WLAN を選択します。 *手記： WLAN リンクは、クライアントモードとして Wi-Fi を有効にした場合にのみ使用できます。* ***3.2.5 Wi-Fi 接続***. • なし: バックアップ リンクはありません。	何一つ
バックアップモード	「コールドバックアップ」、「ウォームバックアップ」、「負荷分散」から選択します。 • コールド バックアップ:非アクティブなリンクはオフラインでスタンバイ状態です。 • ウォーム バックアップ:非アクティブなリンクはスタンバイ状態でオンラインです。 • 負荷分散: 2 つのリンクを同時に使用します。 *注:「バックアップモード」は、「バックアップリンク」が「なし」でない場合にのみ使用できます。*	コールド バックアップ

一般設定@ リンクマネージャ		
アイテム	説明	デフォルト
Revert Interval	バックアップ・リンクがコールド・バックアップ・モードで使用されている場合に、プライマリ・リンクがチェックされるまでの経過時間を分単位で指定します。0 はチェックを無効にすることを意味します。 *注: 復元インターバルは、コールドバックアップモードでのみ使用できます。*	0
緊急再起動	切り替えボタンをクリックして、このオプションを有効/無効にします。使用可能なリンクがない場合にシステム全体を再起動できるようにします。	オフ

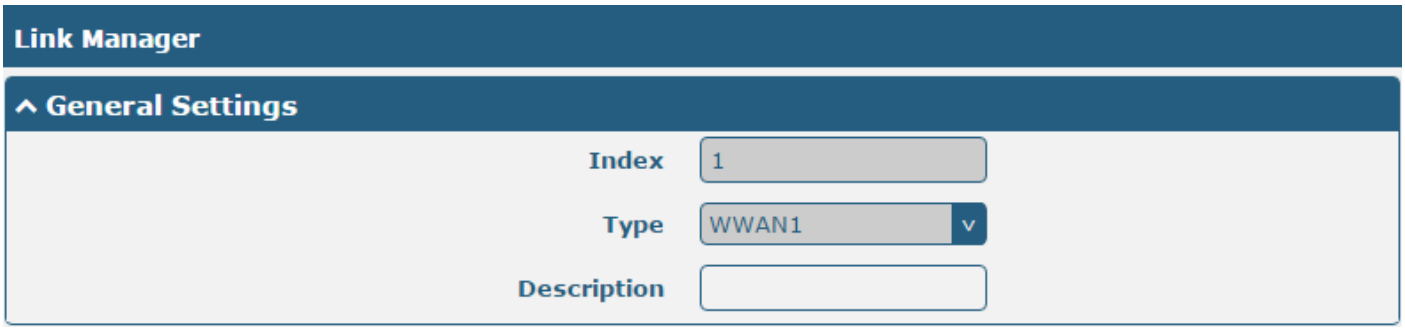
注: クリック ⓘ *するとヘルプが表示されます。*

Link Settings(リンク設定)では、WWAN1/WWAN2、WAN、WLAN などのリンク接続のパラメータを設定できます。 デバイスを常にオンラインに保つために 、Ping 検出を有効にすることをお勧めします。Ping 検出により、信頼性が向上し、データトラフィックも節約されます。

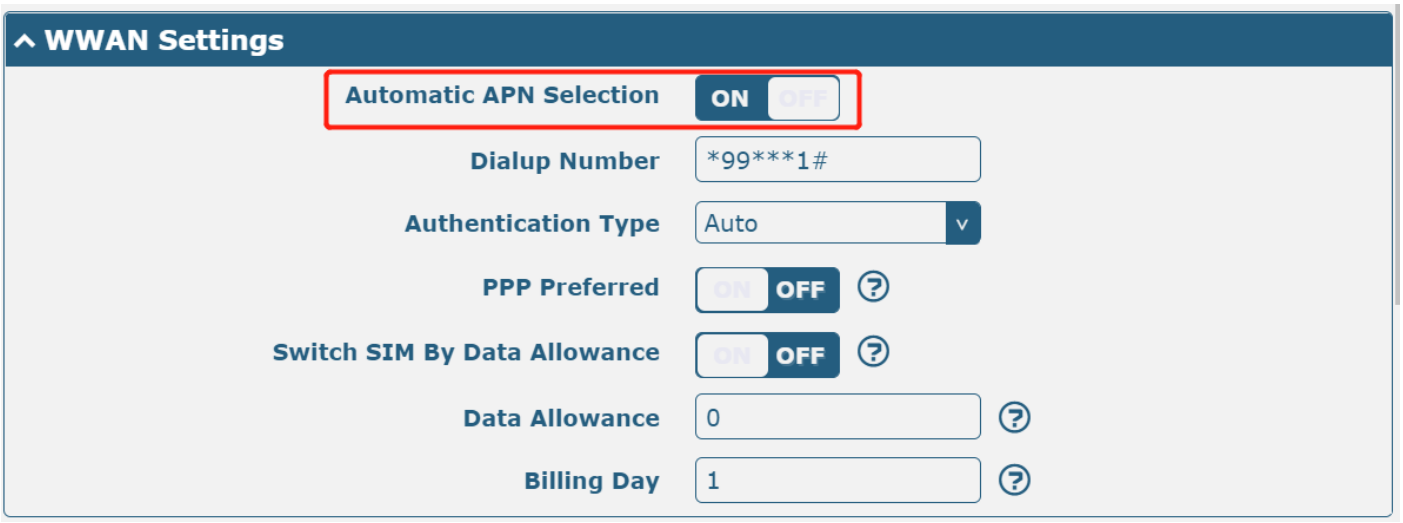


WWAN1/WWAN2 の右端をクリックして、設定ウィンドウに入ります。

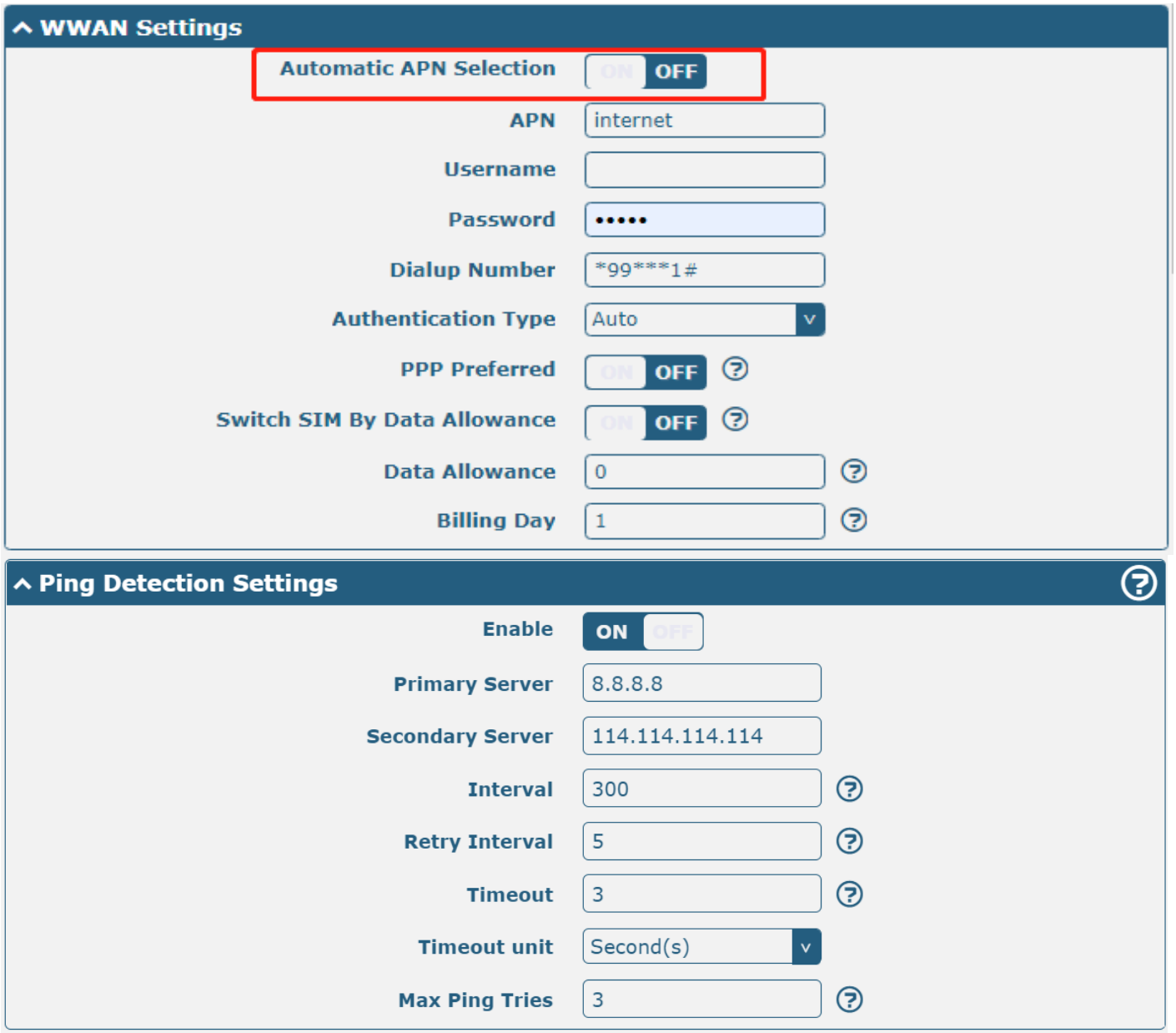
1) WWAN1/WWAN2

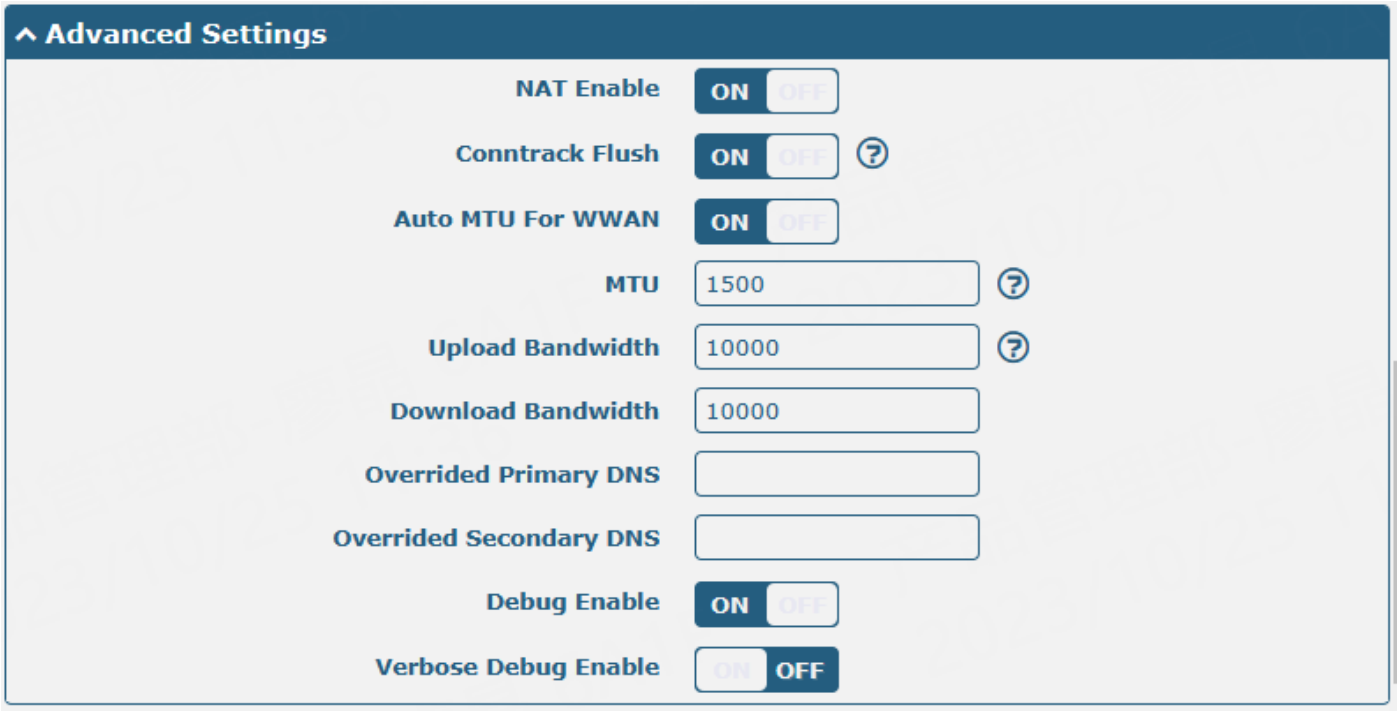


「自動 APN 選択」オプションを有効にすると、ウィンドウが下に表示されます。


WWAN Settings
Automatic APN Selection
ON
OFF
Dialup Number
*99***1#
Authentication Type
Auto
PPP Preferred
ON
OFF
Switch SIM By Data Allowance
ON
OFF
Data Allowance
0
Billing Day
1

「自動 APN 選択」オプションを無効にすると、ウィンドウが下に表示されます。





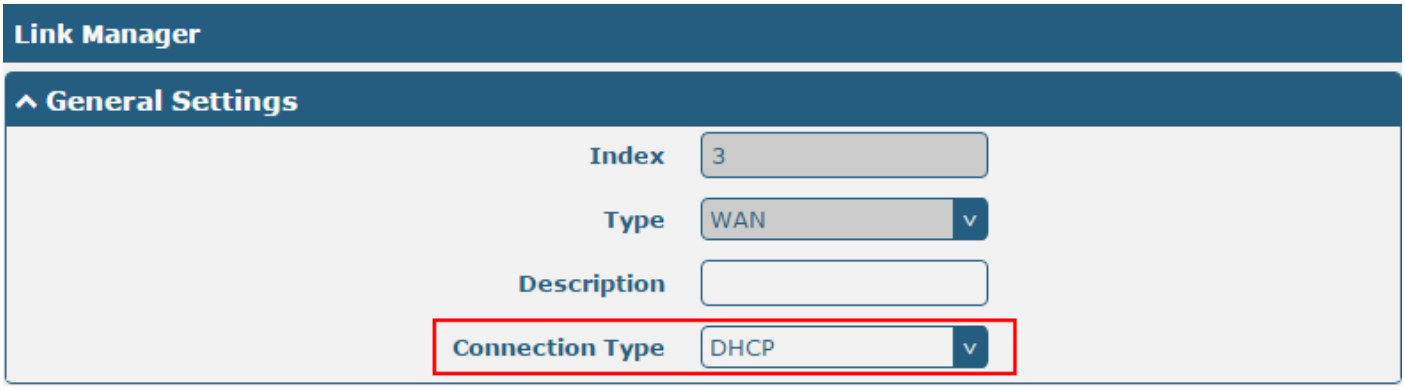
リンク設定(WWAN)		
アイテム	説明	デフォルト
一般設定		
インデックス	リストの序数を示します。	--
種類	リンクの種類を表示します。	WWAN1
説明	このリンクの説明を入力します。	Null
WWAN 設定		
APN の自動選択	トグルボタンをクリックして、「自動 APN 選択」オプションを有効/無効にします。有効にすると、デバイスは APN(アクセスポイント名)を自動的に認識します。または、このオプションを無効にして、APN(アクセスポイント名)を手動で追加することもできます。	オン
APN	ローカル ISP から提供されたセルラーダイヤルアップ接続の APN(アクセスポイント名)を入力します。	インターネット
ユーザー名	ローカル ISP から提供されたセルラーダイヤルアップ接続のユーザー名を入力します。	Null
パスワード	ローカル ISP から提供されたセルラーダイヤルアップ接続のパスワードを入力します。	Null
ダイヤルアップ番号	ローカル ISP から提供された携帯ネットワークダイヤルアップ接続のダイヤルアップ番号を入力します。	*99***1#
認証の種類	必要なローカル ISP として「Auto」、「PAP」、または「CHAP」から選択します。	自動
PPP 優先	PPP ダイヤルアップ方式が推奨されます。	オフ
データ許容量による SIM の切り替え	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、データ制限に達すると別の SIM に切り替わります。 *注:デュアル SIM バックアップにのみ使用されます。*	オフ

リンク設定(WWAN)		
アイテム	説明	デフォルト
データ許容量	毎月のデータトラフィック制限を設定します。データは、データ トラフィック制限 (MiB) が指定されている場合、データ トラフィック統計を記録します。 トラフィック レコードは、**インターフェイス > リンク マネージャーの [ステータス] > [WWAN データ使用統計] >に表示されます。** 0 は、データ トラフィック レコードを無効にすることを意味します。	0
請求日	毎月の請求日を指定します。データトラフィックの統計は、その日から再計算されます。	1
Ping 検出設定		
エネーブル	トグルボタンをクリックして、デバイスのキープアライブポリシーである ping 検出メカニズムを有効/無効にします。	オン
プライマリ サーバ	デバイスは、このプライマリアドレス/ドメイン名に ping を実行して、現在の IPv4 接続がアクティブかどうかを確認します。	8.8.8.8
セカンダリ サーバ	デバイスは、このセカンダリ アドレス/ドメイン名に ping を実行して、現在の IPv4 接続がアクティブかどうかを確認します。	114.114.114.114
インターバル	ping インターバルを設定します。	300
再試行インターバル	ping の再試行インターバルを設定します。 ping が失敗すると、デバイスは再試行インターバルごとに再度 ping を実行します。	5
タイムアウト	ping タイムアウトを設定します。	3
タイムアウト 単位	ping タイムアウト単位を設定します。秒またはミリ秒(ms)。	秒
最大 ping 試行回数 (Max Ping Trys)	ping の最大試行回数を設定します。 別のリンクに切り替えるか、最大連続 ping 試行回数に達した場合は緊急アクションを実行します。	3
詳細設定		
NAT 有効(NAT Enable)	トグルボタンをクリックして、ネットワークアドレス変換を有効/無効にします。	オン
Conntrack フラッシュ	トグルボタンをクリックして、リンクが確立されたときに conntrack テーブル内の接続トラッキング情報をクリアすることを有効または無効にします。 注:このオプションは、「NAT を有効にする」がオンの場合にのみ使用できます。	オン
WWAN 自動 MTU	トグルボタンをクリックして、 WWAN の自動 MTU 機能を有効または無効にします。	オン
MTU (英語)	最大伝送単位を設定します。 ***注: MTU は、「WWAN の自動 MTU」がオフになっている場合にのみ使用できます。***	1500
アップロード帯域幅	QoS に使用するアップロード帯域幅を kbps 単位で設定します。	10000
ダウンロード帯域幅	QoS に使用するダウンロード帯域幅を kbps 単位で設定します。	10000
プライマリ DNS 指定	リンクで使用するプライマリ IPv4 DNS サーバ アドレスを定義します。	Null
セカンダリ DNS 指定	リンクで使用するセカンダリ IPv4 DNS サーバ アドレスを定義します。	Null
デバッグ有効(Debug Enable)	切り替えボタンをクリックして、このオプションを有効/無効にします。デバッグ情報の出力を有効にします。	オン

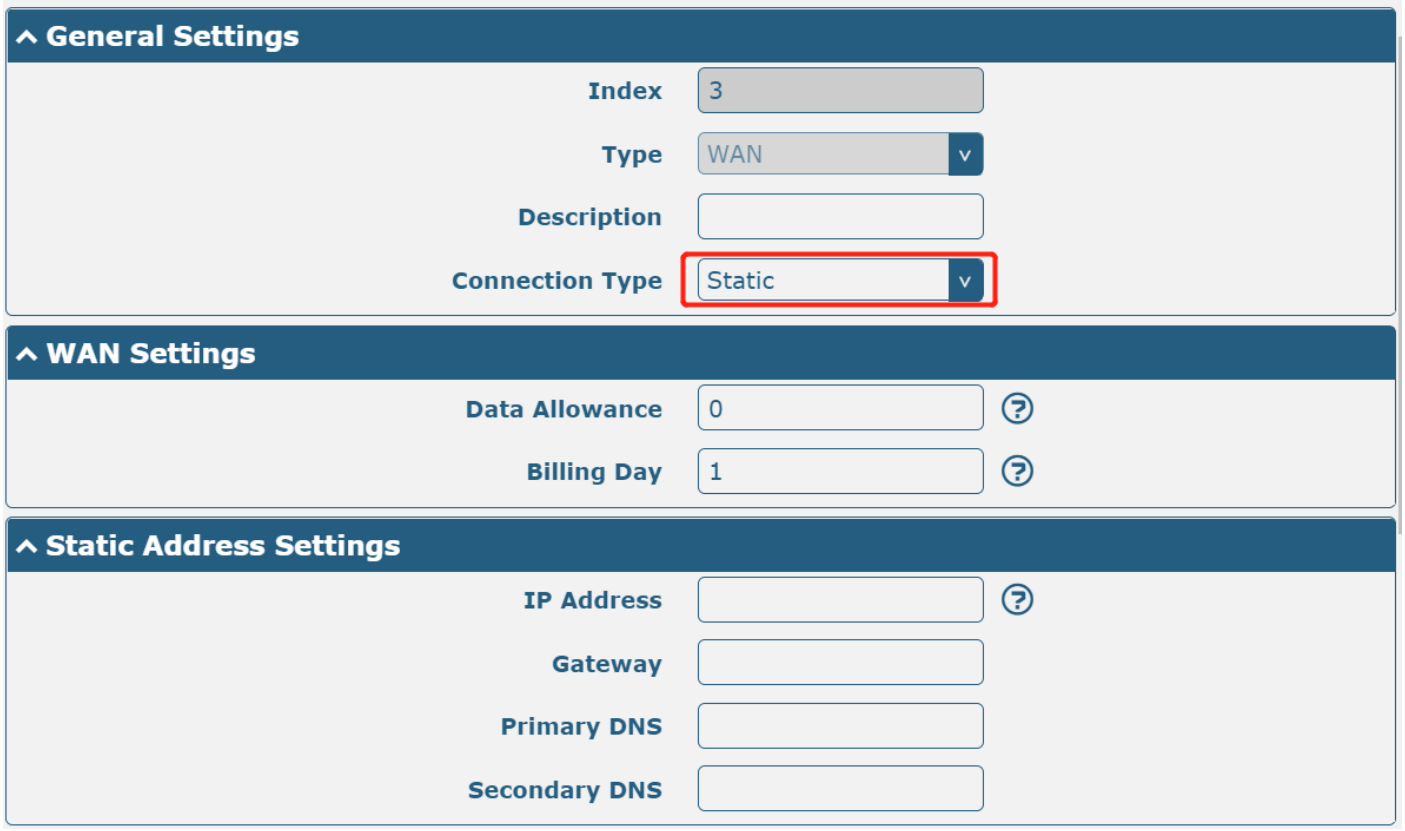
リンク設定(WWAN)		
アイテム	説明	デフォルト
詳細デバッグ有効 (Verbose Debug Enable)	切り替えボタンをクリックして、このオプションを有効/無効にします。詳細なデバッグ情報の出力を有効にします。	オフ

2) WAN

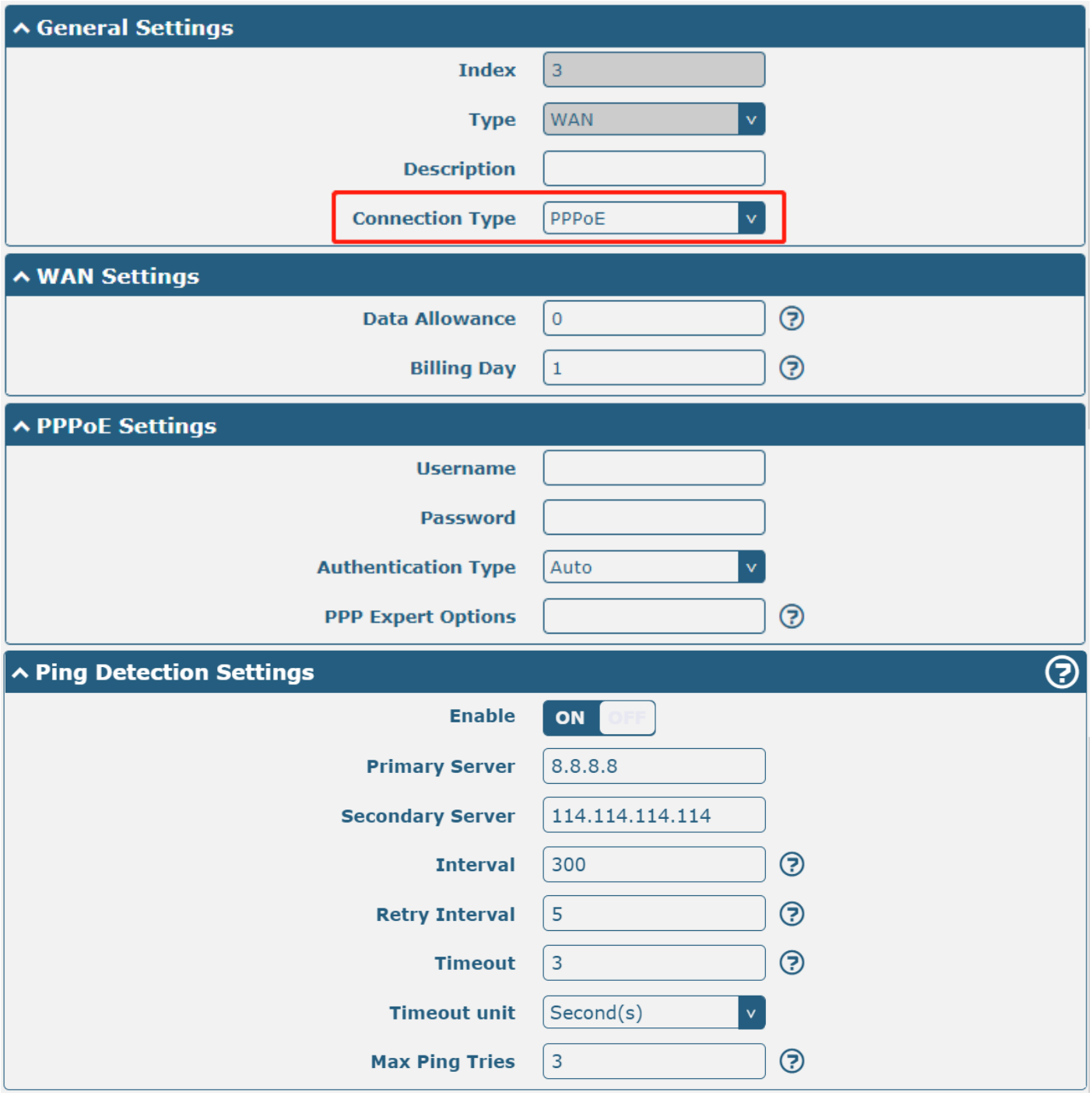
デバイスは、「DHCP」を適用すると、DHCP サーバーから IP を自動的に取得します。

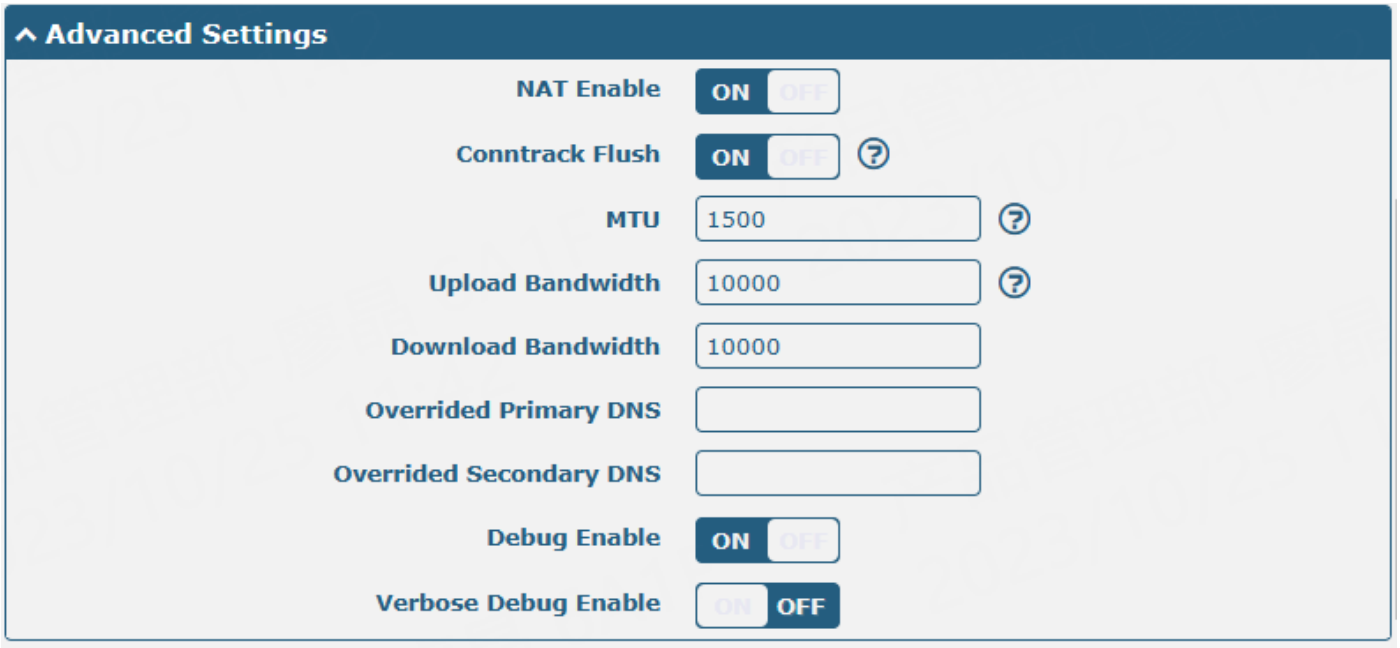


接続タイプとして「静的」を選択すると、ウィンドウが下に表示されます。



接続タイプとして「PPPoE」を選択すると、以下のウィンドウが表示されます。



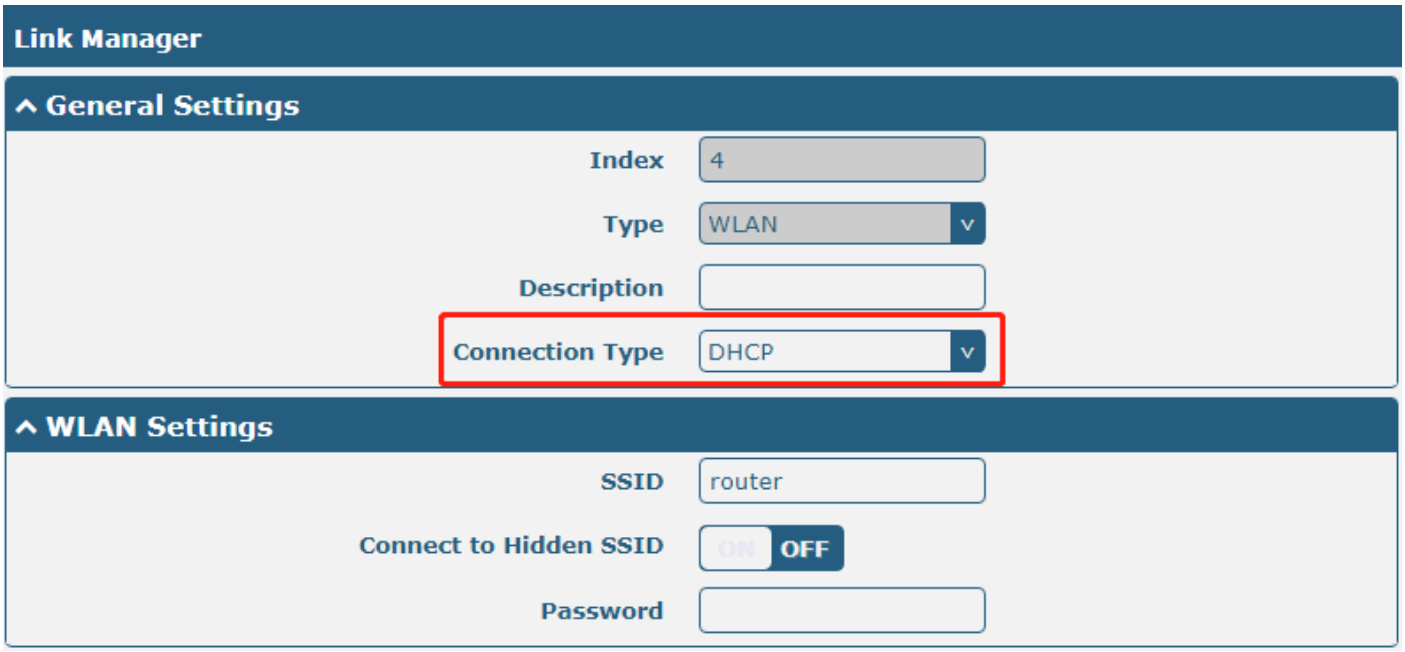


リンク設定(WAN)		
アイテム	説明	デフォルト
一般設定		
インデックス	リストの序数を示します。	--
種類	リンクの種類を表示します。	WAN (英語)
説明	このリンクの説明を入力します。	Null
接続タイプ	「DHCP」、「静的」、または「PPPoE」を選択します。	DHCP
静的アドレス設定		
IP アドレス	インターネットにアクセスできるネットマスクで IP アドレスを設定します。 ネットマスク付きの IP アドレス(例:192.168.1.1/24)	Null
ゲートウェイ	WAN ポートのゲートウェイアドレスを設定します。	Null
プライマリ DNS	プライマリ DNS アドレスを設定します。	Null
セカンダリ DNS	セカンダリ DNS アドレスを設定します。	Null
PPPoE 設定		
ユーザー名	インターネットサービスプロバイダーから提供されたユーザー名を入力します。	Null
パスワード	インターネットサービスプロバイダから提供されたパスワードを入力します。	Null
認証の種類	ローカル ISP の要求に応じて、「Auto」、「PAP」、または「CHAP」から選択します。	自動
PPP エキスパート オプション	PPPoE ダイヤルアップに使用する PPP Expert オプションを入力します。このフィールドには、他の PPP ダイヤル文字列を入力できます。各文字列はセミコロンで区切ることができます。	Null
WAN 設定		

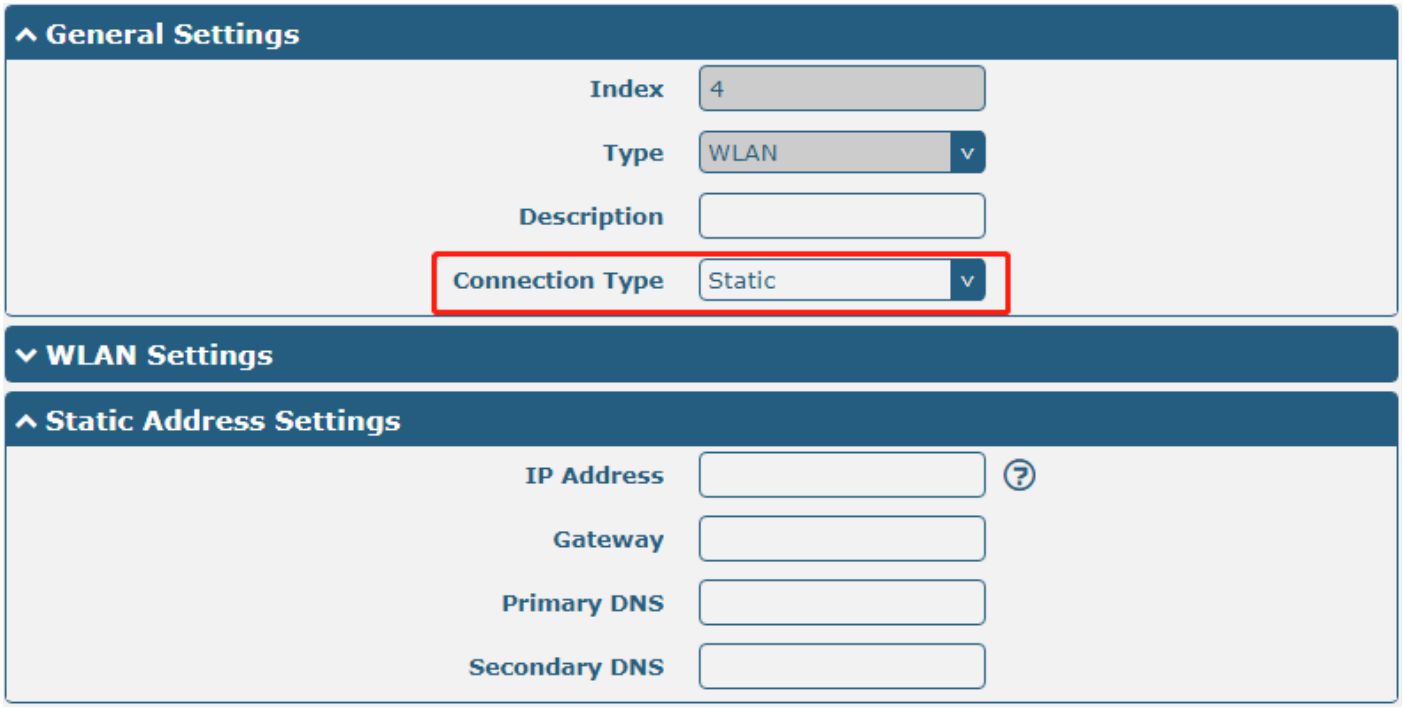
データ許容量	毎月のデータトラフィック制限を設定します。システムは、データトラフィック制限 (MB) が指定されている場合、データ トラフィック統計を記録します。 トラフィックレコードは、**インターフェイス>リンクマネージャの [ステータス] > > [WAN データ使用統計] に表示されます。** 0 は、データ トラフィック レコードを無効にすることを意味します。	0
請求日	毎月の請求日を指定します。データトラフィックの統計は、その日から再計算されます。	1
Ping 検出設定		
エネーブル	トグルボタンをクリックして、デバイスのキープアライブポリシーである ping 検出メカニズムを有効または無効にします。	オン
プライマリ サーバ	デバイスは、このプライマリアドレス/ドメイン名に ping を実行して、現在の接続がアクティブかどうかを確認します。	8.8.8.8
セカンダリ サーバ	デバイスは、このセカンダリアドレス/ドメイン名に ping を実行して、現在の接続がアクティブかどうかを確認します。	114.114.114.114
間	ping インターバルを設定します。	300
再試行インターバル	ping の再試行インターバルを設定します。ping が失敗すると、デバイスは再試行インターバルごとに再度 ping を実行します。	5
タイムアウト	ping タイムアウトを設定します。	3
タイムアウト 単位	ping タイムアウト単位を設定します。秒またはミリ秒	秒
最大 ping 試行回数 (Max Ping Trys)	ping の最大試行回数を設定します。 別のリンクに切り替えるか、最大連続 ping 試行回数に達した場合は緊急アクションを実行します。	3
詳細設定		
NAT 有効(NAT Enable)	トグルボタンをクリックして、ネットワークアドレス変換オプションを有効/無効にします。	オン
Conntrack フラッシュ	トグルボタンをクリックして、リンクがアップしているときに conntrack テーブル内の接続トラッキング情報をクリアすることを有効または無効にします。 注:このオプションは、「NAT を有効にする」がオンの場合にのみ使用できます。	オン
MTU (英語)	「Maximum Transmission Unit」と入力します。	1500
アップロード帯域幅	QoS のアップロード帯域幅 (kbps 単位)を入力します。	10000
ダウンロード帯域幅	QoS に使用するダウンロード帯域幅を kbps 単位で入力します。	10000
プライマリ DNS 指定	リンクで使用するプライマリ IPv4 DNS サーバ アドレスを定義します。	Null
セカンダリ DNS 指定	リンクのセカンダリ IPv4 DNS サーバ アドレスを定義します。	Null
デバッグ有効(Debug Enable)	切り替えボタンをクリックして、このオプションを有効/無効にします。デバッグ情報の出力を有効にします。	オン
詳細デバッグ有効 (Verbose Debug Enable)	切り替えボタンをクリックして、このオプションを有効/無効にします。詳細なデバッグ情報の出力を有効にします。	オフ

3) 無線 LAN

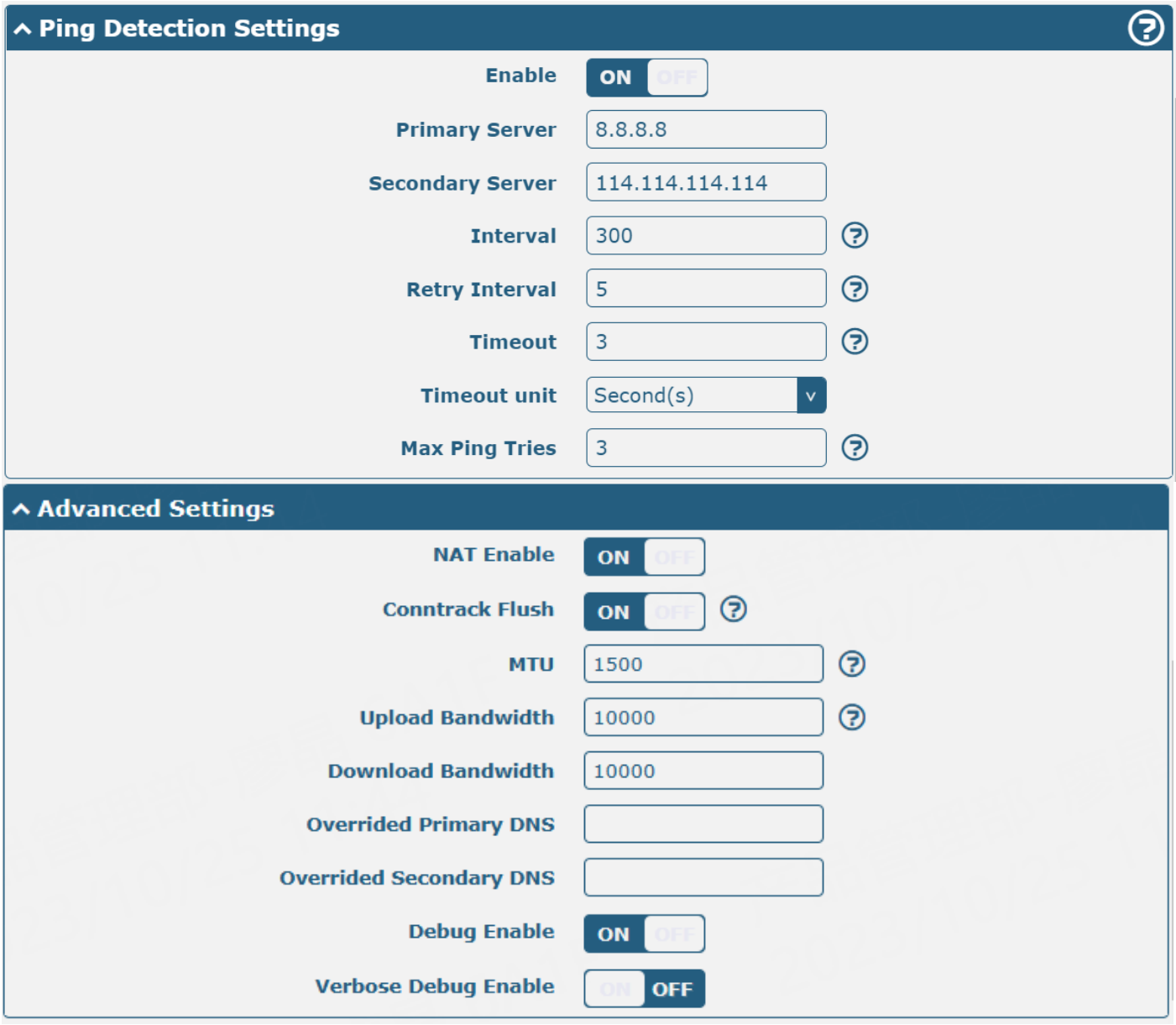
デバイスは、接続タイプとして「DHCP」を適用すると、WLAN AP から IP アドレスを自動的に取得します。SSID の具体的なパラメータ設定を以下に示します。



接続タイプとして「静的」を選択すると、ウィンドウが下に表示されます。



注:WLAN 接続タイプは「PPPoE」をサポートしていません。

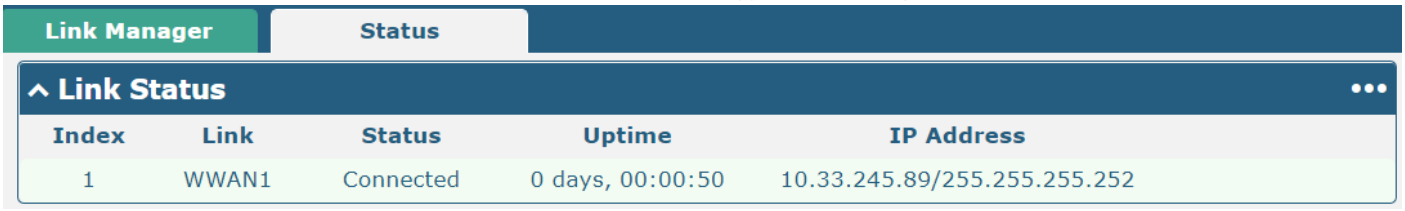


リンク設定(WLAN)		
アイテム	説明	デフォルト
一般設定		
インデックス	リストの序数を示します。	--
種類	リンクの種類を表示します。	無線 LAN
説明	このリンクの説明を入力します。	Null
接続タイプ	「DHCP」または「静的」から選択します。	DHCP
WLAN 設定		
SSID(SSID)	デバイスが接続する 1～32 文字の SSID を入力します。SSID(Service Set Identifier)は、ワイヤレスネットワークの名前です。	デバイス
非表示の SSID に接続する	切り替えボタンをクリックして、このオプションを有効/無効にします。デバイスがクライアントモードで動作し、SSID が非表示のアクセスポイントに接続する必要がある場合は、このオプションを有効にする必要があります。	オフ

パスワード	デバイスが接続するアクセスポイントの 8〜63 文字のパスワードを入力します 。	Null
静的アドレス設定		
IP アドレス	インターネットにアクセスできるネットマスク付きの IP アドレスを入力し、 たとえば、192.168.1.1/24 です。	Null
ゲートウェイ	Wi-Fi AP の IP アドレスを入力します。	Null
プライマリ DNS	プライマリ DNS アドレスを設定します。	Null
セカンダリ DNS	セカンダリ DNS アドレスを設定します。	Null
Ping 検出設定		
エネーブル	トグルボタンをクリックして、デバイスのキープアライブポリシーである ping 検出メカニズムを有効または無効にします。	オン
プライマリ サーバ	デバイスは、このプライマリアドレス/ドメイン名に ping を実行して、現在の接続がアクティブかどうかを確認します。	8.8.8.8
セカンダリ サーバ	デバイスは、このセカンダリアドレス/ドメイン名に ping を実行して、現在の接続がアクティブかどうかを確認します。	114.114.114.114
インターバル	ping インターバルを設定します。	300
再試行インターバル	ping の再試行インターバルを設定します。 ping が失敗すると、デバイスは再試行インターバルごとに再度 ping を実行します。	5
タイムアウト	ping タイムアウトを設定します。	3
タイムアウト 単位	ping タイムアウト単位を設定します。秒またはミリ秒	秒
最大 ping 試行回数 (Max Ping Trys)	ping の最大試行回数を設定します。別のリンクに切り替えるか、最大連続 ping 試行回数に達した場合は緊急アクションを実行します。	3
詳細設定		
NAT 有効(NAT Enable)	トグルボタンをクリックして、ネットワークアドレス変換オプションを有効/無効にします。	オン
Conntrack フラッシュ	トグルボタンをクリックして、リンクがアップしているときに conntrack テーブル内の接続トラッキング情報をクリアすることを有効または無効にします。 注:このオプションは、「NAT を有効にする」がオンの場合にのみ使用できます。	オン
MTU (英語)	「Maximum Transmission Unit」と入力します。	1500
アップロード帯域幅	QoS に使用するアップロード帯域幅を kbps 単位で入力します。	10000
ダウンロード帯域幅	QoS に使用するダウンロード帯域幅を kbps 単位で入力します。	10000
プライマリ DNS の指定	リンクで使用するプライマリ DNS サーバ アドレスを定義します。	Null
セカンダリ DNS の指定	リンクのセカンダリ DNS サーバ アドレスを定義します。	Null
デバッグ有効(Debug Enable)	切り替えボタンをクリックして、このオプションを有効/無効にします。デバッグ情報の出力を有効にします。	オン
詳細デバッグ有効 (Verbose Debug Enable)	切り替えボタンをクリックして、このオプションを有効/無効にします。詳細なデバッグ情報の出力を有効にします。	オフ

4) ステータス

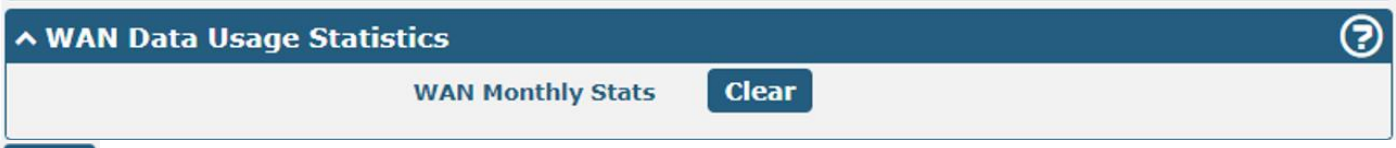
このページでは 、リンク接続のステータスを表示し、毎月のデータ使用量の統計をクリアできます。



右端のボタンをクリックして、現在のリンクの接続状態を選択します。

リンクの行をクリックすると、その行の下に現在のリンク接続の 詳細情報が表示されます。

Clear ボタンをクリックして、 SIM1 または SIM2 の月間データ 使用量統計を消去します。データ統計は、Interface > Link Manager > Link Settings> WWAN Settings>Data Allowance で Data Allowance **機能を有効にした場合にのみ表示されます。**



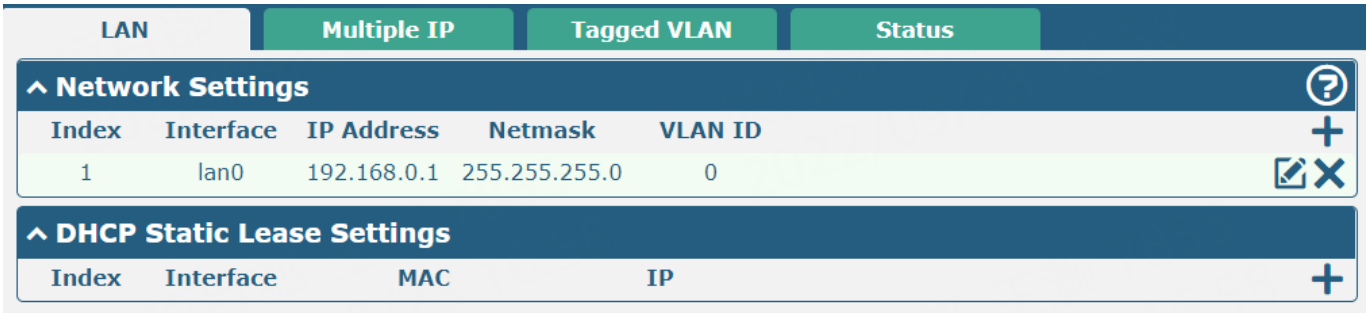
Clear ボタンをクリックして、WAN の月次データトラフィック使用量統計をクリアします。データ統計は、インターフェイス>リンクマネージャー>リンク設定>WAN 設定>データ許容量**でデータ許容量機能を有効にした場合にのみ表示されます。**

3.2.2 LAN

このセクションでは、LAN ポートに関連するパラメータを設定できます。デバイスには複数のイーサネットポートがある場合があり、少なくとも 1 つの LAN ポート をデフォルトの IP 192.168.0.1/255.255.255.0 の lan0 として割り当てる必要があります。

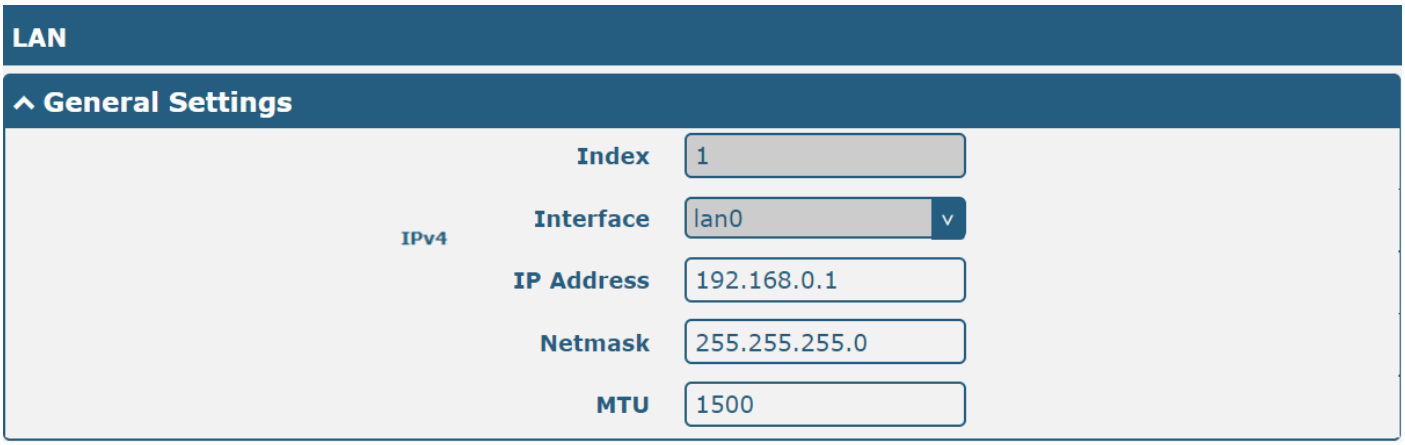
手記:
1) R3000 Lite にはイーサネットポートが 1 つしかなく、LAN としてのみ割り当てることができます。
2) R2000 Lite にはイーサネットポートが 1 つしかなく、LAN としてのみ割り当てることができます。
3) R1510 Lite にはイーサネットポートが 1 つしかなく、LAN としてのみ割り当てることができます。

1) LAN



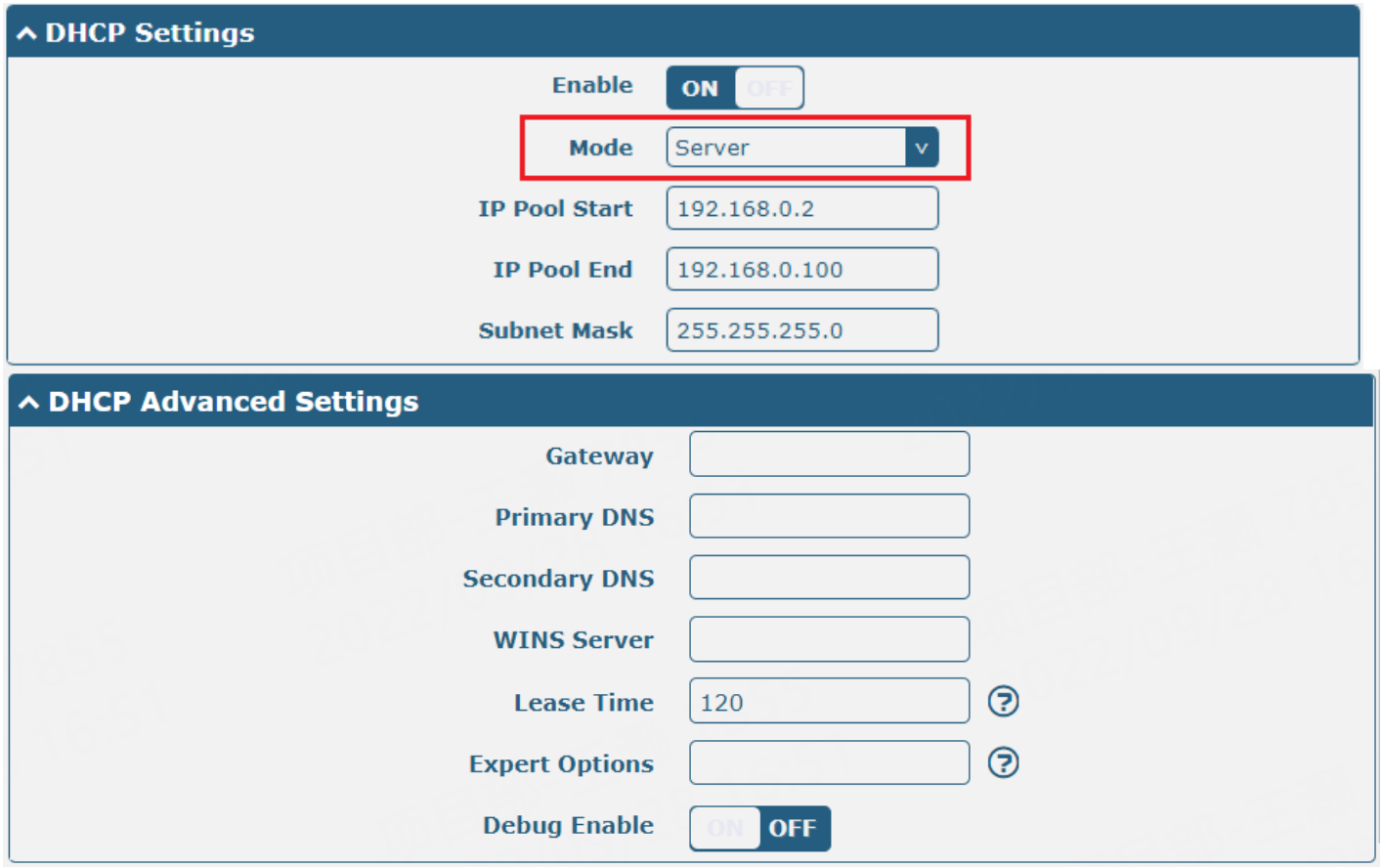
注: lan0 は削除できません。

クリックして＋新しい LAN ポートを追加するか、クリックして現在の LAN ポート✕を削除できます。次に、クリック✎して LAN ポートの構成を編集します。

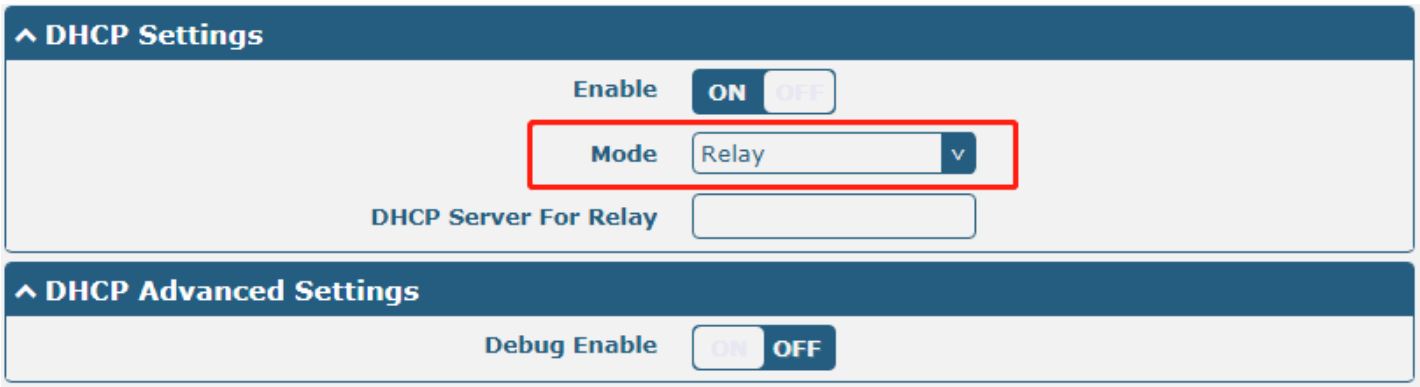


一般設定@ LAN		
アイテム	説明	デフォルト
インデックス	リストの序数を示します。	--
インターフェイス	編集ポートを表示します。 lan1 は、イーサネット > ポート > ポート設定 の **ETH0~ETHn のいずれかで選択された場合にのみ使用できます。**	lan0 (ラン 0)
IPv4 アドレス	LAN ポートの IP アドレスを設定します。	192.168.0.1
ネットマスク	LAN ポートのネットマスクを設定します。	255.255.255.0
MTU (英語)	「Maximum Transmission Unit」と入力します。	1500

モードとして「サーバー」を選択すると、ウィンドウが下に表示されます。

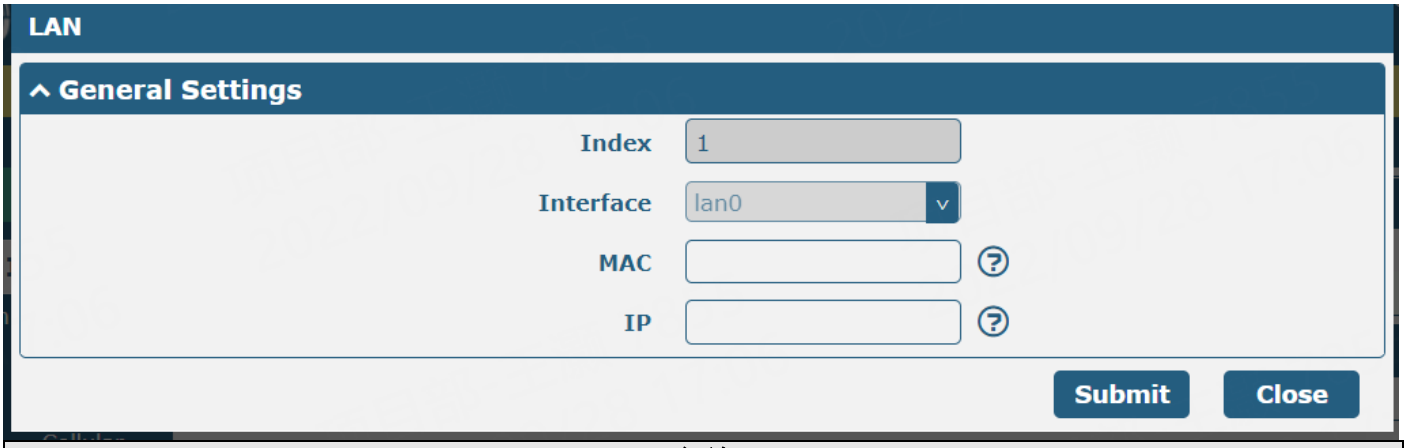


モードとして「リレー」を選択すると、ウィンドウが下に表示されます。



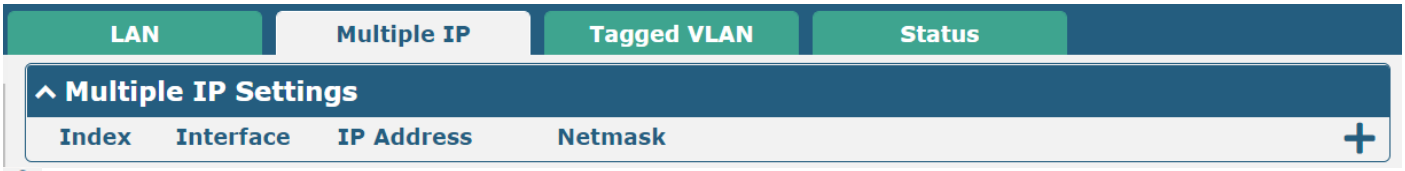
LAN(無線 LAN		
アイテム	説明	デフォルト
DHCP 設定		
エネーブル	トグルボタンをクリックして、DHCP 機能を有効/無効にします。	オン
モード	「サーバー」または「リレー」を選択します。 • サーバ:LAN ポートに接続した DHCP クライアントに IP アドレスをリースします • リレー:デバイスは DHCP リレーにすることができ 、DHCP クライアントと DHCP サーバーが同じサブネットにないという問題を解決するためのリレートンネルを提供します	サーバー
IPv4 プールの開始	DHCP クライアントにリースされる IP アドレスのプールの先頭を定義します。	192.168.0.2
IPv4 パーティの終了	DHCP クライアントにリースされる IP アドレスのプールの末尾を定義します。	192.168.0.100
サブネットマスク	DHCP クライアントが DHCP サーバから取得した IP アドレス のサブネットマスクを定義します。	255.255.255.0
リレー用の DHCP サーバ	DHCP リレー サーバの IP アドレスを入力します。	Null
DHCP の詳細設定		
ゲートウェイ	DHCP サーバがクライアントに割り当てるゲートウェイアドレスを定義します。ゲートウェイアドレスは、DHCP アドレスプールと同じネットワークセグメント上にある必要があります 。	Null
プライマリ DNS	DHCP サーバがクライアントに割り当てる プライマリ DNS サーバアドレスを定義します。	Null
セカンダリ DNS	DHCP サーバがクライアントに割り当てるセカンダリ DNS サーバアドレスを定義します。	Null
WINS サーバ	DHCP クライアントが DHCP サーバーから取得した Windows インターネットネームサービスを定義します。	Null
リース 期間	クライアントが DHCP サーバーから取得した IP アドレスを使用できるリース期間を秒単位で設定します。	120
エキスパートオプション	このフィールドには、DHCP サーバーの他のオプションを入力します。 フォーマット:config-desc;設定-desc、例えば.log-DHCP;クワイエット-DHCP	Null
デバッグ有効(Debug Enable)	切り替えボタンをクリックして、このオプションを有効/無効にします。 DHCP 情報出力を有効にします。	オフ

[DHCP Static Lease Settings] のポップアップ ウィンドウから ＋ クリックして新しい MAC と IP を追加できます。

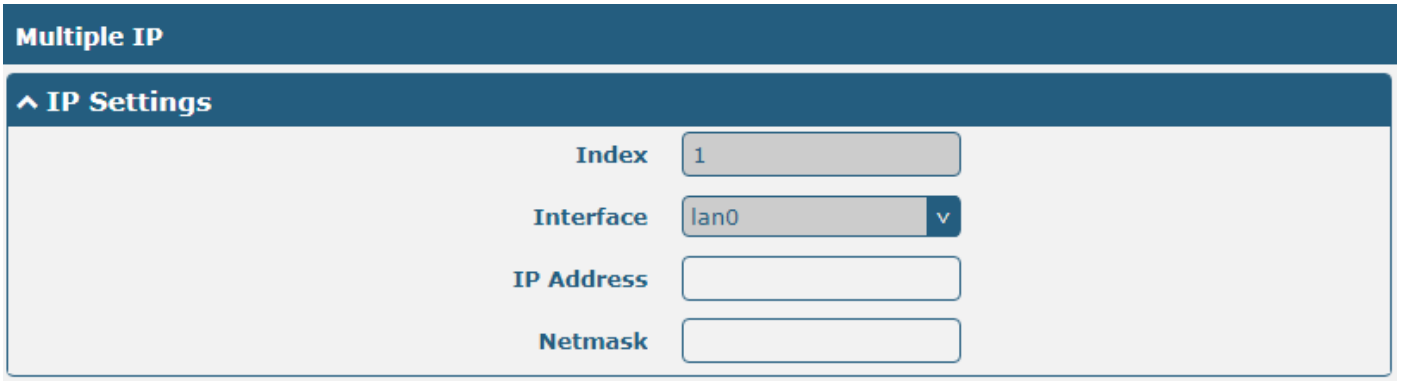


LAN(無線 LAN		
アイテム	説明	デフォルト
一般 設定		
マック	スタティックリースの MAC アドレスを入力します。	Null
IP アドレス	スタティックリースの IP アドレスを入力します。	Null

2) マルチプル IP

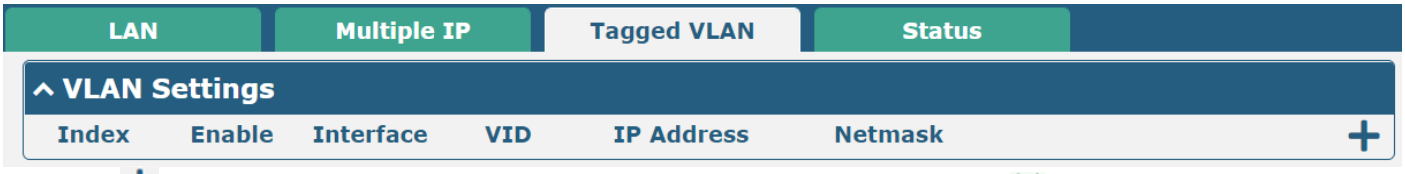


＋クリックして LAN ポートに複数の IP を追加したり、クリックして LAN ポート✕の複数の IP を削除したりできます。次に、クリック して LAN ポートの複数の IP を編集します。

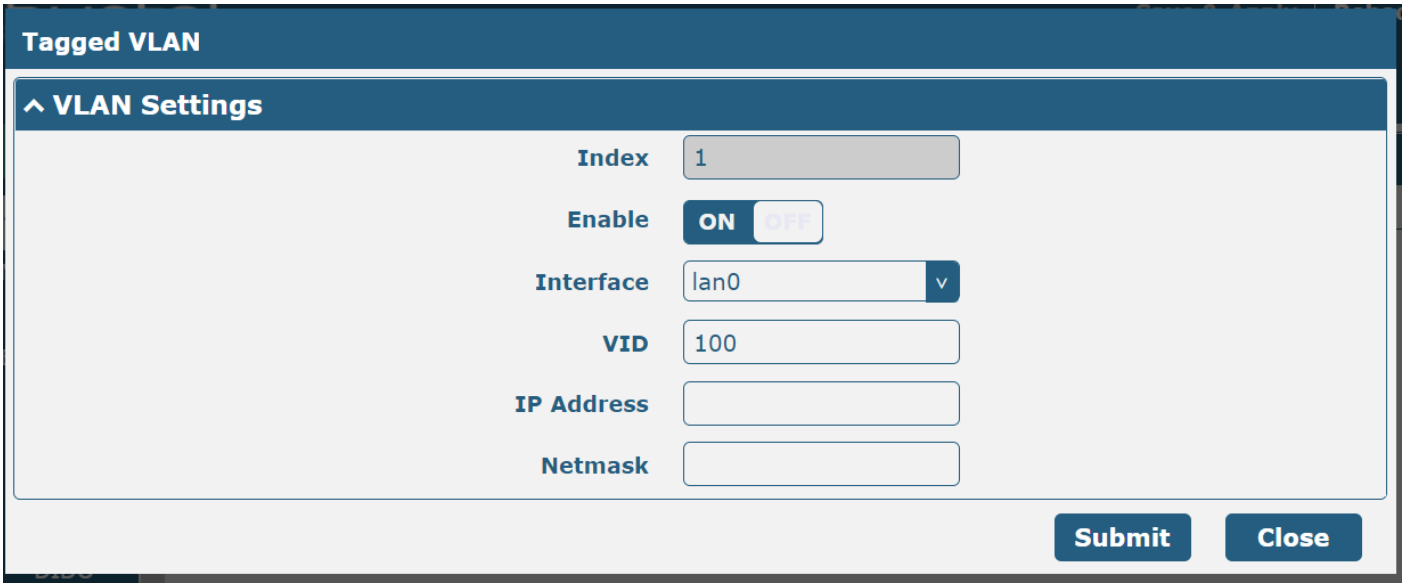


IP 設定		
アイテム	説明	デフォルト
インデックス	インデックス一覧を表示します。	--
インターフェイス	編集ポートを表示します。	--
IP アドレス	LAN ポートの IP アドレスを設定します。	Null
ネットマスク	LAN ポートのネットマスクを設定します。	Null

3) タグ付き VLAN



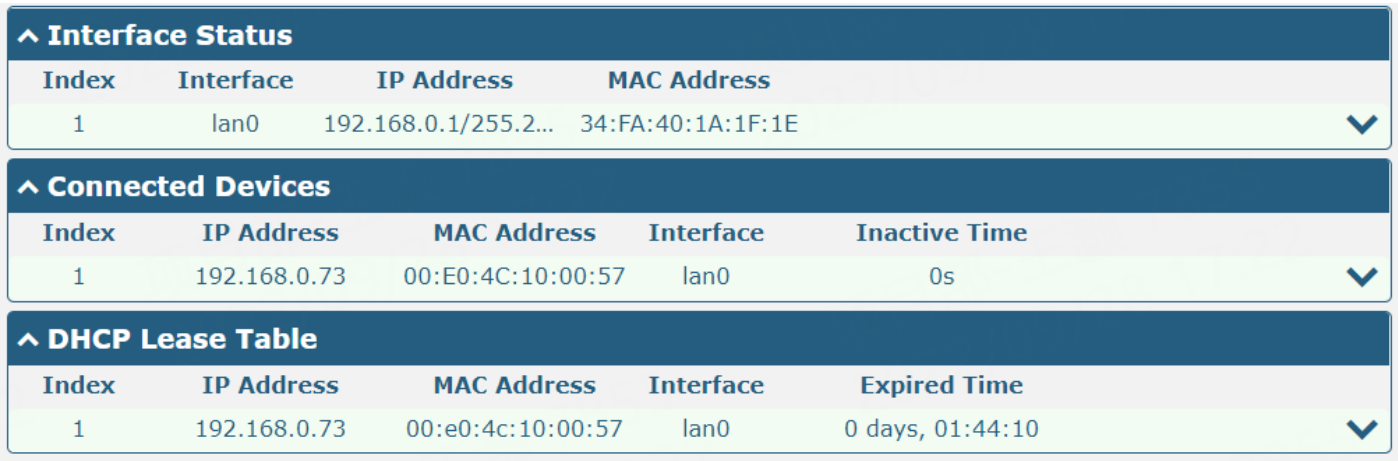
クリック＋して LAN ポートに VLAN を追加したり、クリックして LAN ポート✕の VLAN を削除したりできます。次に、クリック✎して LAN ポートの VLAN を編集します。



VLAN 設定		
アイテム	説明	デフォルト
インデックス	インデックス一覧を表示します。	--
エネーブル	トグルボタンをクリックして、タグ VLAN 機能を有効/無効にします。	オン
インターフェイス	編集ポートを表示します。	--
VID の	LAN ポートの VLAN ID を設定します 。値の範囲は 1 から 4094 です	100
IP アドレス	VLAN の IP アドレスを設定します。	Null
ネットマスク	VLAN のネットマスクを設定します。	Null

4) ステータス

このセクションでは、 LAN 接続のステータスを表示できます。



ステータスの行をクリックすると、その行の下に詳細なステータス情報が表示されます。

DHCP Lease Table

Index	IP Address	MAC Address	Interface	Expired Time
1	192.168.0.73	00:e0:4c:10:00:57	lan0	0 days, 01:44:10

Index	1
IP Address	192.168.0.73
MAC Address	00:e0:4c:10:00:57
Interface	lan0
Expired Time	0 days, 01:44:10

3.2.3 イーサネット

このセクションでは、イーサネットに関連するパラメータを設定できます。デバイスにマルチイーサネットポート がある場合があります。 デバイスの ETH0 は WAN ポートまたは LAN ポートとして設定できますが、他のイーサネットポートは LAN ポートとしてのみ設定できます。 すべてのイーサネットポートのデフォルト設定は lan0 で、デフォルトの IP は 192.168.0.1/255.255.255.0 です。

手記:

1) R2000 Dual は、ETH1~ETH4(ポート設定で POE を有効にする)を介して背後のデバイスに電力を供給できます。

2) R3000 Lite にはイーサネットポートが1 つしかなく、LAN としてのみ設定可能です。

3) R2000 Lite にはイーサネットポートが1 つしかなく、LAN としてのみ設定可能です。

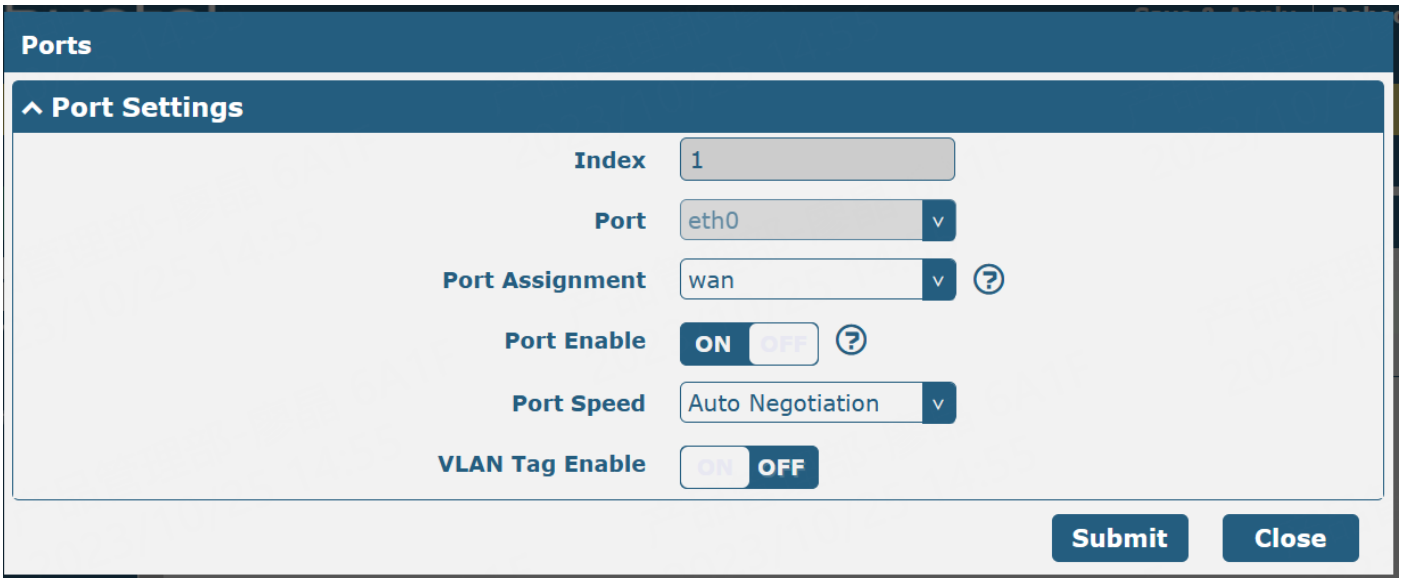
4) R1510 Lite にはイーサネットポートが1 つしかなく、LAN としてのみ設定可能です。

Ports | Status

Port Settings

Index	Port	Port Assignment	Port Enable
1	eth0	lan0	true
2	eth1	lan0	true
3	eth2	lan0	true
4	eth3	lan0	true

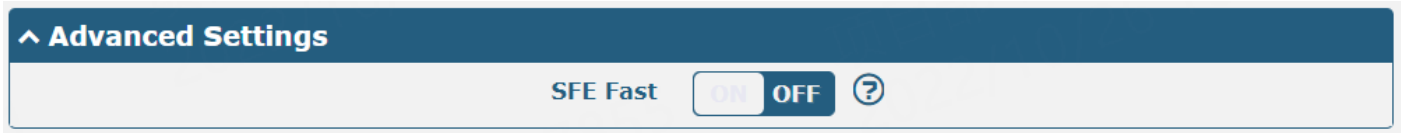
eth0 のボタンをクリックしてパラメータを設定し、ポップアップウィンドウで eth0 のポート割り当てパラメータを変更します。



手記:

(1) R3000 シリーズ/R3000LG/R2110/R5020/R5020Lite のみ対応しています。

ポート設定		
アイテム	説明	デフォルト
インデックス	リストの序数を示します。	--
ポート	編集ポートを表示、読み取り専用。	--
ポート割り当て	WAN ポートや LAN ポートなどのイーサネット ポート タイプを選択します。ポートを LAN ポートとして設定する場合は、ドロップダウンリストをクリックして「lan0」または「lan1」を選択できます。	lan0
ポート有効(Port Enable)	ポートを有効または無効にします。	オン
ポート速度(オプション)	ポート速度を指定します。	オート ネゴシエーション
PoE 対応(PoE Enable)(オプション)	クリックすると、PoE 機能を有効または無効にできます。 PoE 機能を有効にすると、PoE 電圧が接続されます。	オン
VLAN タグの有効化(VLAN Tag Enable)	ボタンをクリックして、VLAN ID のオンとオフを切り替えます。これは、ポート割り当てが wan に設定されている場合にのみ使用できます。	オフ



詳細設定		
アイテム	説明	デフォルト
SFE ファスト	トグルボタンをクリックして、この機能を有効/無効にします。 SFE Fast はイーサネット ポート レートを上げることができますが、QoS に影響します。	オフ

注: R5020 のみが「SFE Fast」をサポートしています。

1) ステータス

このセクションでは、 イーサネット接続のステータスを表示できます。

Port Status

Index	Port	Link
1	eth0	Down
2	eth1	Down
3	eth2	Down
4	eth3	Down
5	eth4	Down

ステータスの行をクリックすると、その行の下に詳細なステータス情報が表示されます。以下のスクリーンショットを参照してください。

Port Status

Index	Port	Link
1	eth0	Down
2	eth1	Down
3	eth2	Down
4	eth3	Down
5	eth4	Down

Index 5
Port eth4
Link Down

3.2.4 セルラー

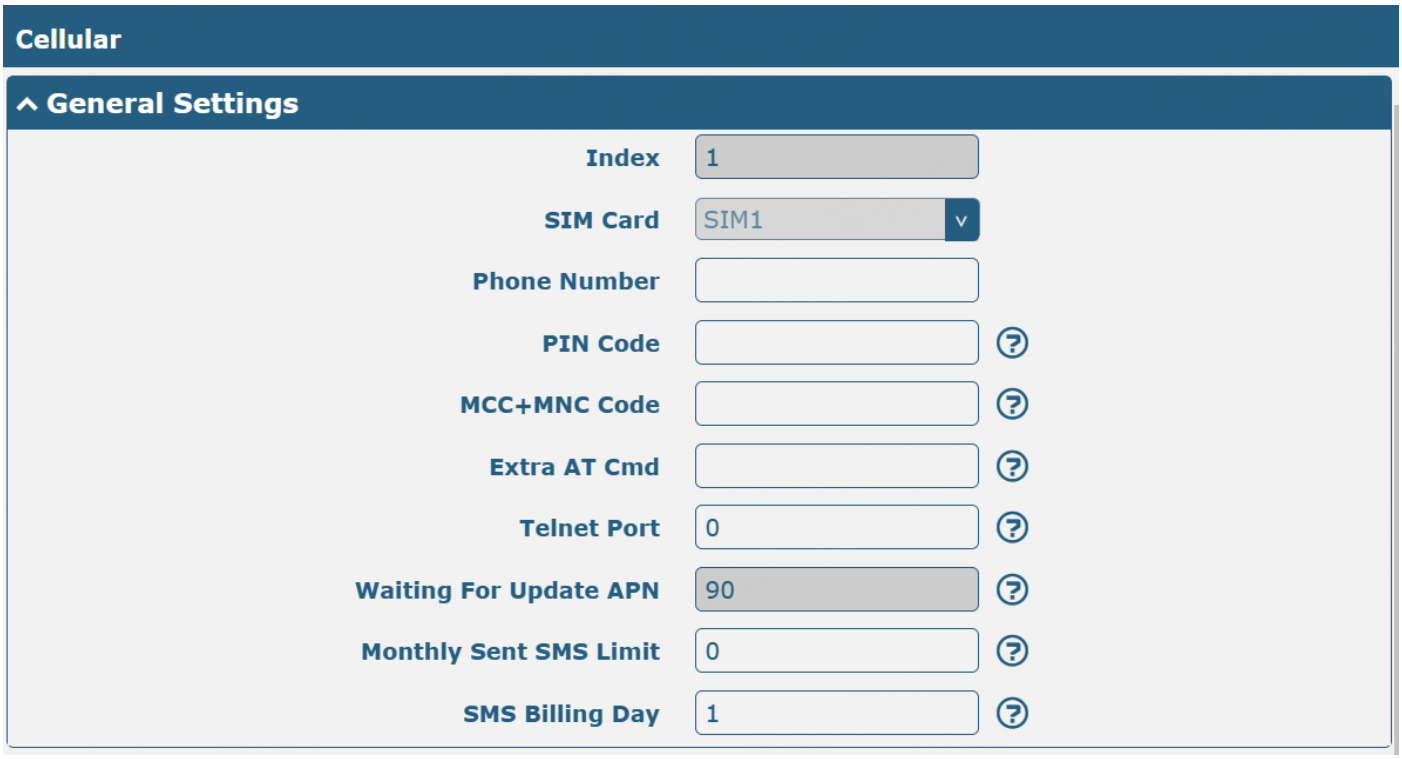
このセクションでは、セルラーの関連パラメータ を設定できます。 デバイスには 1 つまたは 2 つの SIM カードスロットがあります。

Cellular | Status | AT Debug

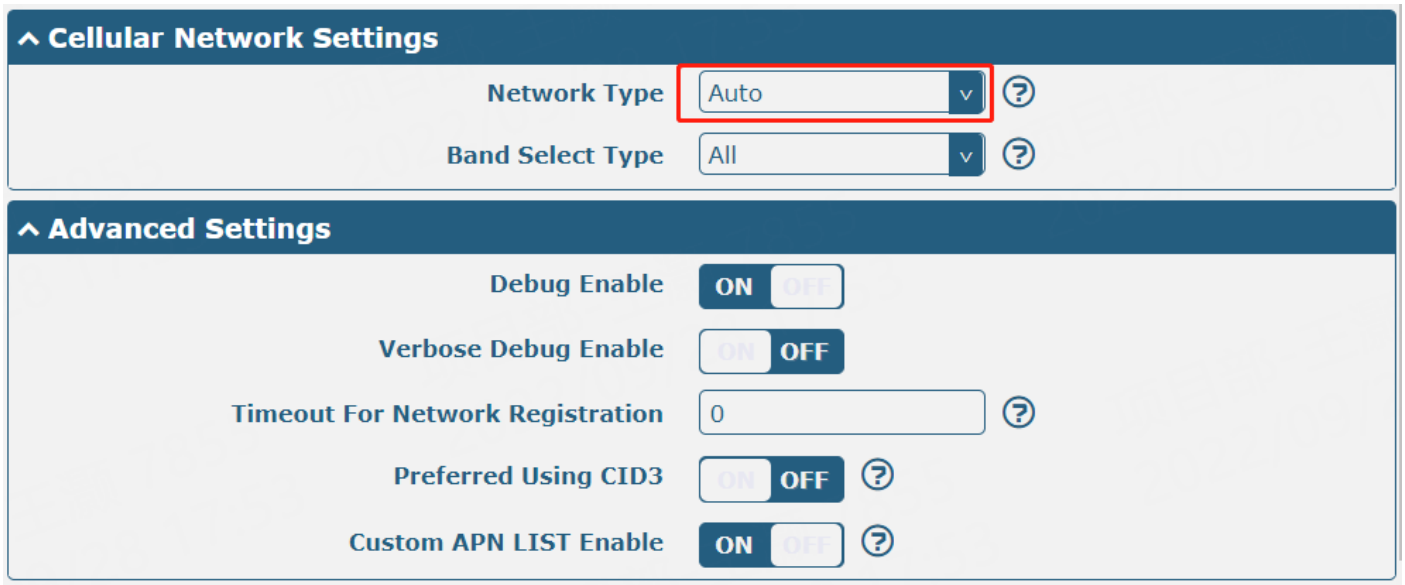
Advanced Cellular Settings

Index	SIM Card	Phone Number	Network Type	Band Select Type
1	SIM1		Auto	All
2	SIM2		Auto	All

SIM 1 の右端をクリックして、パラメーターを編集します。



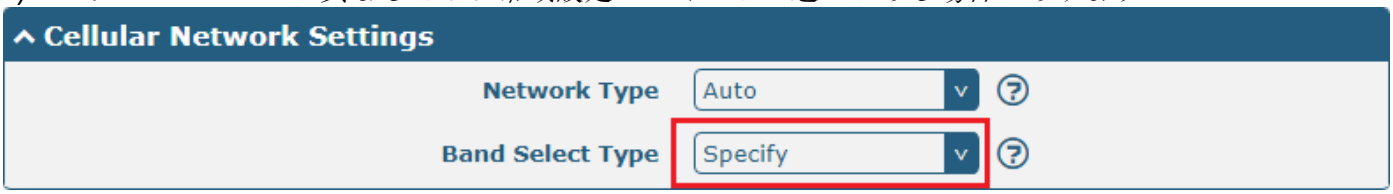
ネットワークタイプ**として「自動**」を選択すると、ウィンドウが下に表示されます。

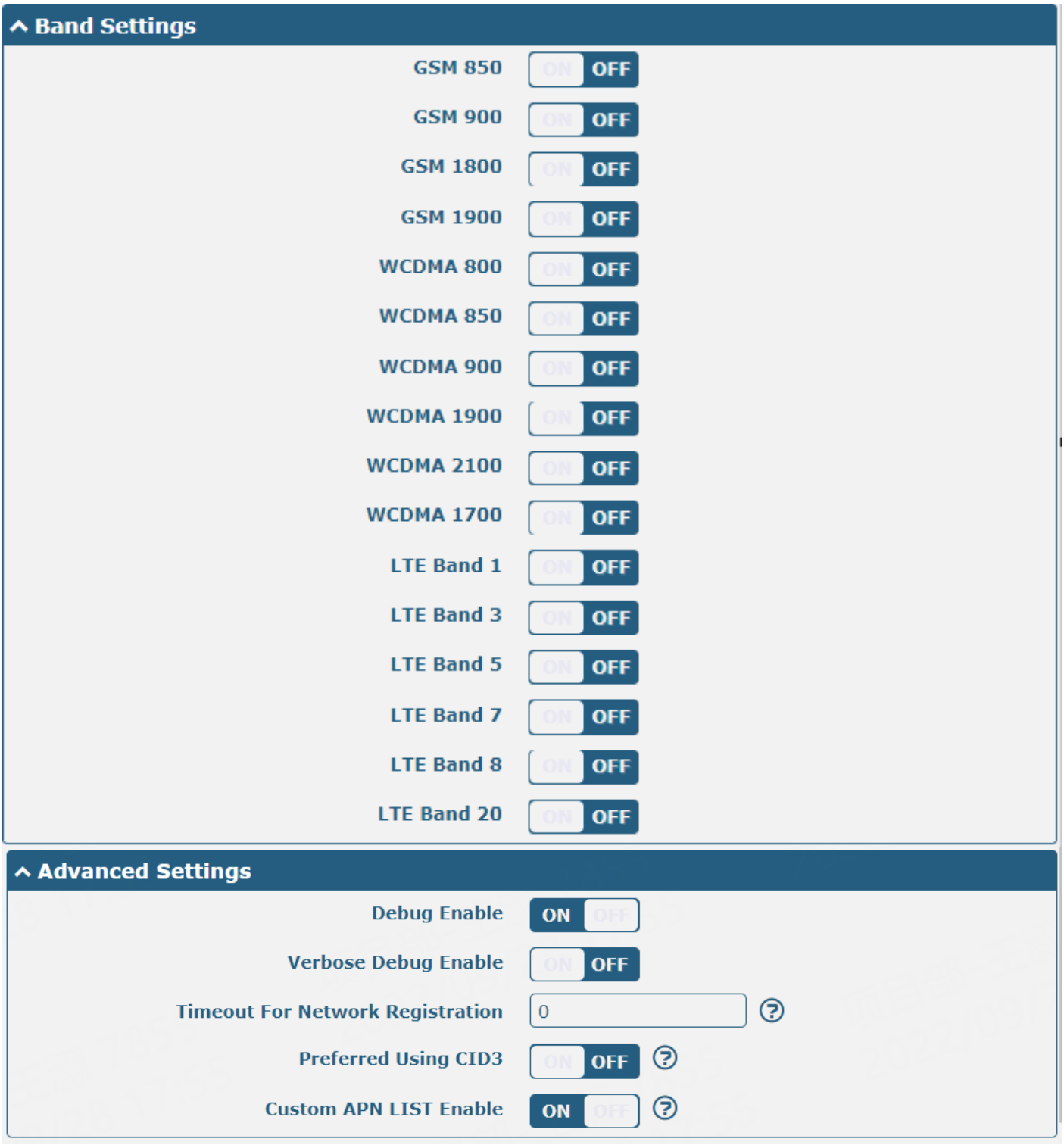


帯域選択**タイプ**を「指定」を選択すると、以下のウィンドウが表示されます。

手記:

1) セルラーモジュールが異なるため、帯域設定にいくつかの違いがある場合があります。





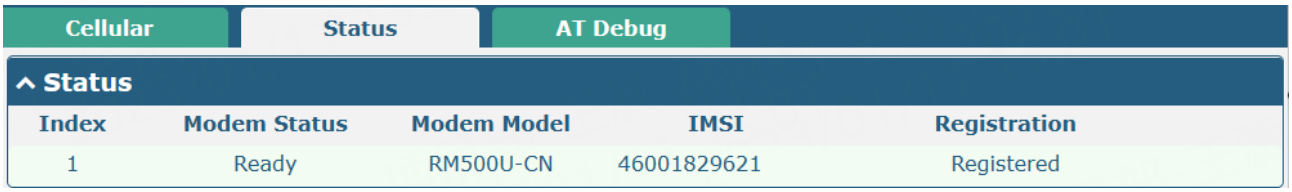
携帯		
アイテム	説明	デフォルト
一般設定		
インデックス	リストの序数を示します。	--
SIM カード	現在編集中の SIM カードを表示します。	SIM1
電話番号	SIM カードの電話番号を入力します。	Null
PIN コード	SIM のロック解除に使用する 4~8 文字の PIN コードを入力します。	Null

携帯		
アイテム	説明	デフォルト
MCC + MNC コード	5～6 桁の数字を入力し、セミコロンの末尾を使用する必要があります。 デバイスをロックするために使用され、指定されたキャリア SIM カードのみを使用できます。	Null
追加の AT コマンド	セルラーの初期化に使用する AT コマンドを入力します。	Null
Telnet ポート	Telnet 経由の AT に使用する telnet サービスのポートリスニングを指定します。	0
APN の更新待ち	ネットワークに接続した後、APN を自動的に更新する時間インターバル。 単位:秒 モデムは自動更新 APN 機能をサポートしている必要があります。 例:HL7618RD	90
月間送信 SMS 制限	月に送信できる SMS の最大数を入力し 、0 は制限がないことを意味します。	0
SMS 請求日	毎月の日付を入力して、SMS カウントをゼロにリセットします。	1
セルラーネットワーク設定		
ネットワークの種類	携帯ネットワークの種類 (ネットワーク アクセス順序) を選択します。「オート」、「2G のみ」、「2G ファースト」、「3G のみ」、「3G ファースト」、「4G のみ」、「4G ファースト」から 選択します。 • 自動:最適な信号ネットワークに自動的に接続します。 • 2G のみ:2G ネットワークのみが接続されます。 • 2G ファースト:2G ネットワークに優先的に接続します。 • 3G のみ:3G ネットワークのみが接続されます。 • 3G ファースト:3G ネットワークに優先的に接続します。 • 4G のみ:4G ネットワークのみが接続されます。 • 4G ファースト:4G ネットワークに優先的に接続します。 *手記:* *1) セルラーモジュールが異なるため、オプションのネットワークタイプが異なる場合があります。* *2) クリック」?" 詳細を確認するためのヘルプのメニューの文字。*	自動
バンド選択タイプ	「すべて」または「指定」 から選択します。「指定」を選択すると、特定のバンドを選択できます。	すべての
詳細設定		
デバッグ有効 (Debug Enable)	切り替えボタンをクリックして、このオプションを有効/無効にします。 デバッグ情報の出力を有効にします。	オン
詳細デバッグ有効(Verbose Debug Enable)	切り替えボタンをクリックして、このオプションを有効/無効にします。 詳細なデバッグ情報の出力を有効にします。	オフ
ネットワーク登録のタイムアウト	タイムアウトは、モジュールがネットワークに登録するために必要です。 単位は秒です。0 は、既定の設定が使用されることを意味します。	0
CID3 の使用を推奨	切り替えボタンをクリックして、このオプションを有効/無効にします。 APN3 を使用してインターネットにアクセスできるようにします。一部のオペレーターは、Verizon と同様に、APN3 を使用してインターネットに通常どおりアクセスする必要があり、必要に応じてオンにすることができます	オフ

携帯		
アイテム	説明	デフォルト
カスタム APN リスト有効	切り替えボタンをクリックして、このオプションを有効/無効にします。 カスタム APN LIST 機能を有効にする	オン

1) ステータス

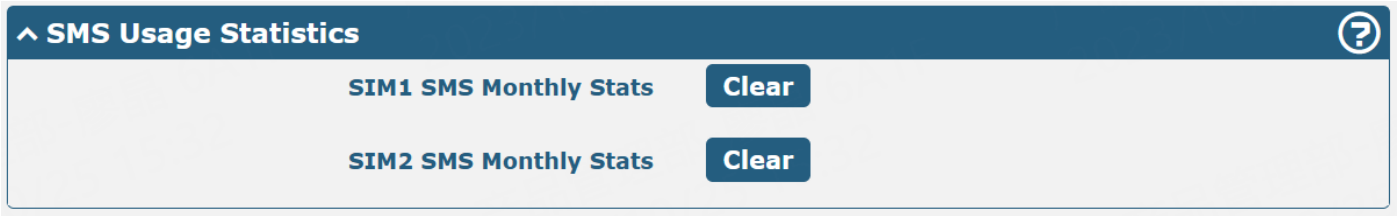
このセクションでは、セルラー接続のステータスを表示できます。



ステータスの行をクリックすると、その行の下に詳細が表示されます。

ステータス	
アイテム	説明
インデックス	リストの序数を示します。
モデム ステータス	無線モジュールのステータスを表示します。
モデムモデル	無線モジュールのモデルを表示します。
現在の SIM	端末が使用している SIM カードを表示します。

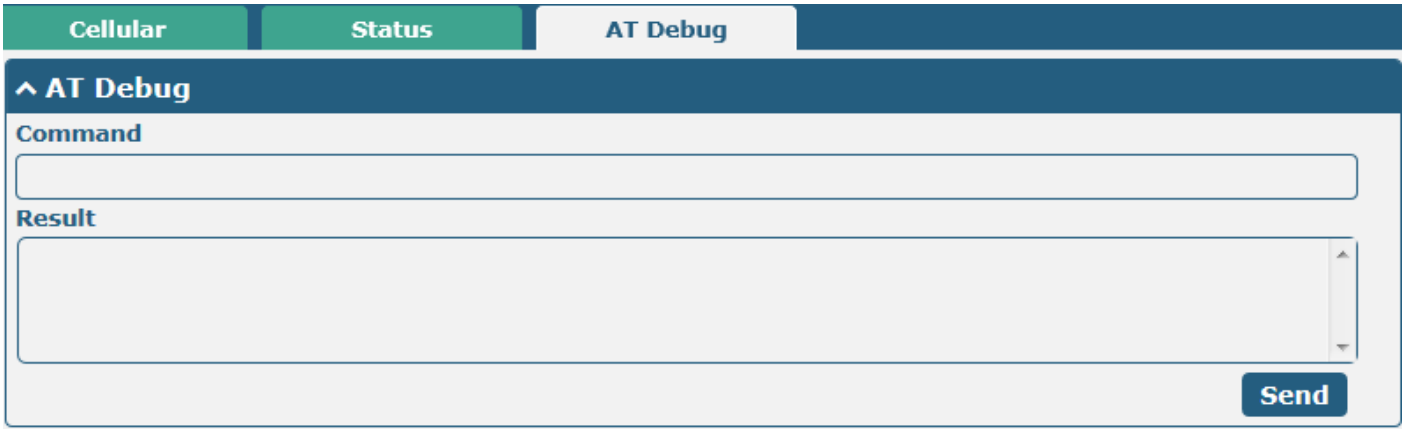
ステータス	
アイテム	説明
電話番号	現在の SIM の電話番号を表示します。 *注:このオプションは、[携帯電話>SIM1 / SIM2]>[一般設定]>[電話番号]に 手動で入力した場合に表示されます。*
IMSI の	現在の SIM の IMSI 番号を表示します。
ICCID(英語)	現在の SIM の ICCID 番号を表示します。
登録	現在のネットワークステータスを表示します。
ネットワークプロバイダー	ネットワークプロバイダーの名前を表示します。
ネットワークの種類	現在のネットワークサービスの種類(GPRS など)を表示します。
ENDC ステータス	現在の ENDC 状況を表示します。
5G アーキテクチャ	現在の 5G タイプを表示します。SA または NSA。このオプションは、5G 製品でのみ表示されます。
バンド	現在のネットワークの帯域を表示します。
信号強度	信号強度を表示します。(2/3/4G ネットワークでのみ有効、5G ネットワークの RSRP を参照してください)
RSRP	[Show Reference Signal Received Power] の値を表示します。 (4G または 5G ネットワークでのみ有効)
RSRQ の	参照信号の受信品質値を表示します。 (4G または 5G ネットワークでのみ有効)
PLMN ID	現在の PLMN ID を表示します。
市外局番	さまざまなエリアを識別するために使用される現在のローカルエリアコードを表示します 。
セル ID	デバイスの検索に使用されている現在のセル ID を表示します。
IMEI の	無線モジュールの IMEI(International Mobile Equipment Identity)番号を表示します。
ファームウェアバージョン	セルラーモジュールの現在のファームウェアバージョンを表示します。
SINR の	信号と干渉の対雑音比を表示します。(4G ネットワークまたは 5G ネットワークのみ)
物理セル ID	物理セル ID を表示します。



SMS 使用統計	
アイテム	説明
SIM1 SMS 月次統計	ボタンをクリックすると、Clear SIM1 を使用して送信された SMS の累積数を手動でクリアできます。
SIM2 SMS 月次統計	ボタンをクリックして、Clear SIM2 を使用して送信された SMS の累積数を手動でクリアします。

2) AT デバッグ

このセクションでは、AT デバッグを実行できます。



AT デバッグ		
アイテム	説明	デフォルト
コマンド	セルラーモジュールに送信する AT コマンド をこのテキストボックスに入力します。	Null
リザルト	セルラーモジュールが 応答した AT コマンドをこのテキストボックスに表示します。	Null
Send	ボタンをクリックして AT コマンドを送信します。	--

3.2.5 Wi-Fi 接続

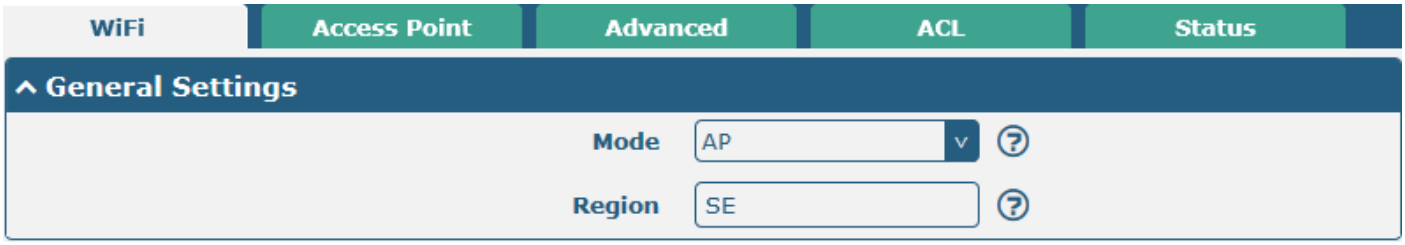
このセクションでは、2 つの Wi-Fi モードのパラメータを設定できます。 デバイスは、Wi-Fi AP モードとクライアントモードの両方をサポートし、デフォルトは AP です。

1) Wi-Fi AP

デバイスを Wi-Fi AP として構成する

「**Wi-Fi>Wi-Fi>インターフェイス**」**をクリックし**、モードとして「AP」を選択して、「送信」をクリックします。

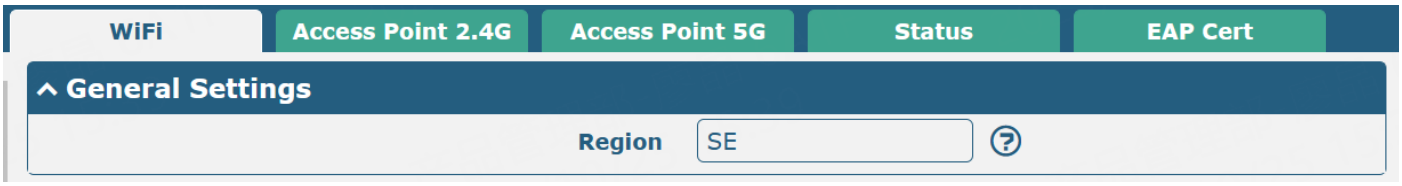
2.4GHz WI-FI のみ



手記:

(1) R3000 シリーズのみがモードオプションをサポートしています。

2.4GHz および 5GHz の Wi-Fi

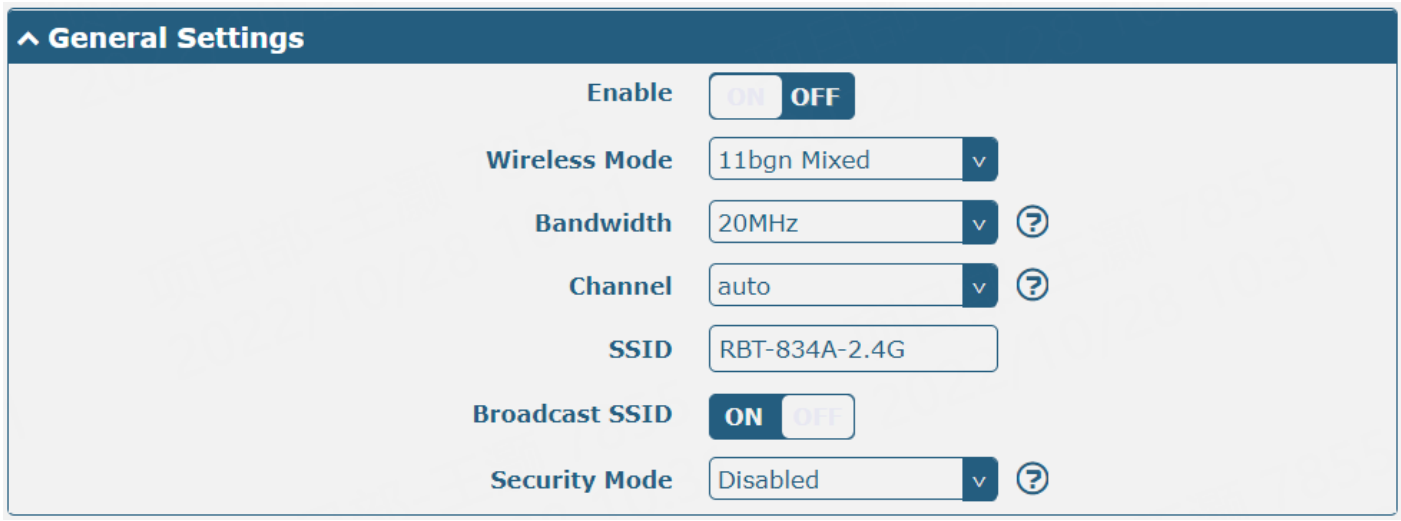


手記:

1) 設定が終わったら、**Save & Apply > Reboot** をクリックすると、変更が有効になります。
2) R2110 と R5020 のみが 2.4GHz と 5GHz の両方に対応しています。
3) R2110/R5020 シリーズ/R151 シリーズ/520/R201X シリーズにおいて、WiFi AP モードと WiFi クライアントモードの同時実行に対応しました。WLAN インターフェイスはリンク管理にデフォルトで追加されており、ここで動作モードを選択する必要はありません。

2) アクセスポイント 2.4G

[**Access Point 2.4G**] 列をクリックして、Wi-Fi AP のパラメータを設定します。デフォルトでは、セキュリティモードは「無効」に設定されています。



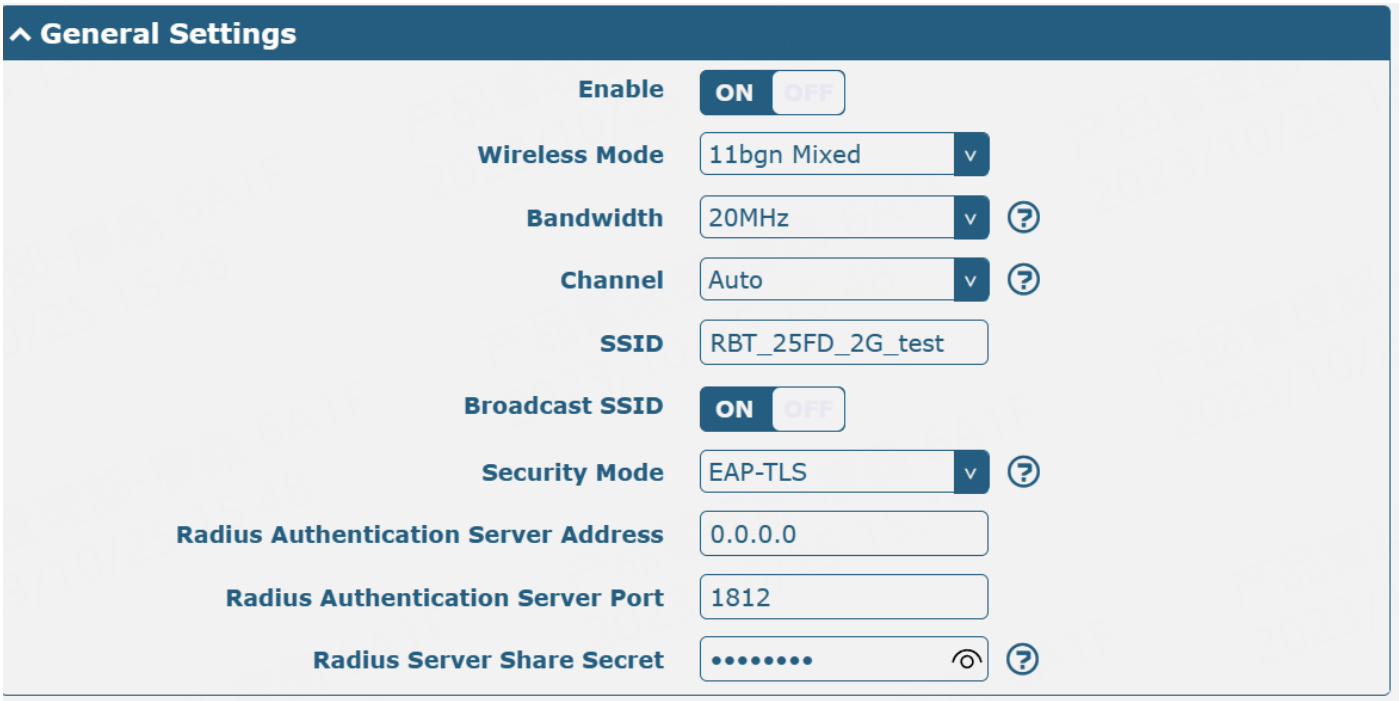
セキュリティモードを「WPA-Personal」に設定した場合、以下のウィンドウが表示されます。

セキュリティモードを「WEP」に設定している間、ウィンドウが下に表示されます。

セキュリティモードを「EAP-TLS」に設定している間、以下のウィンドウが表示されます。

手記:

(1) R2110/R5020/R5020Lite のみ、セキュリティモード「EAP-TLS」に対応しています。

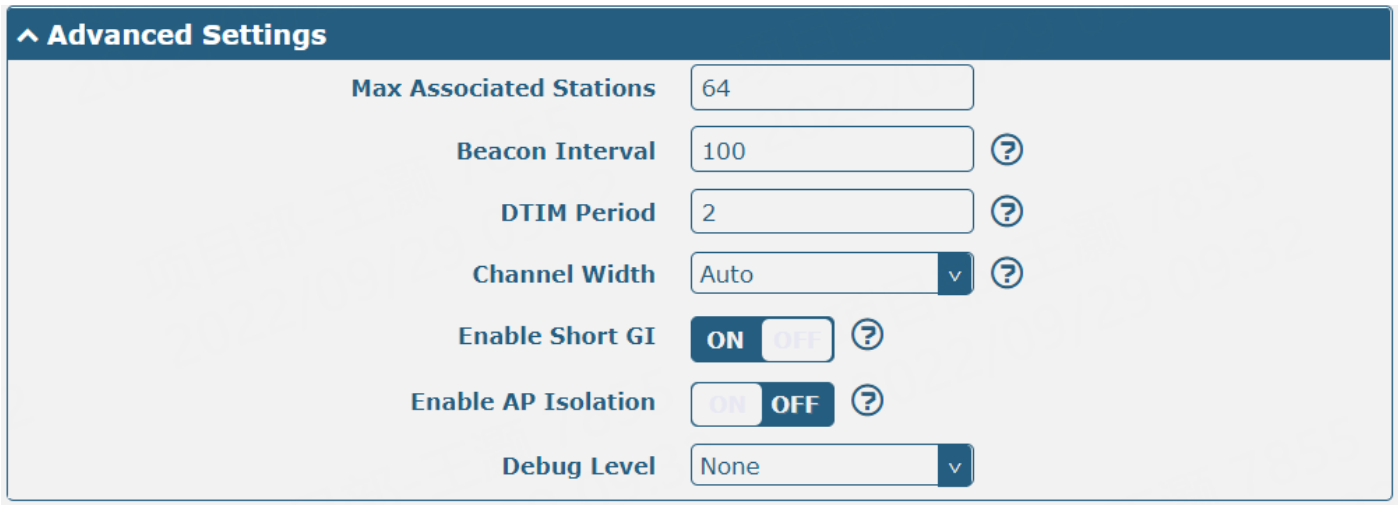


一般設定@アクセスポイント 2.4G		
アイテム	説明	デフォルト
エネーブル	トグルボタンをクリックして、Wi-Fi アクセスポイントオプションを有効/無効にします。	オフ
ワイヤレスモード	「11bgn Mixed」「11b のみ」「11g のみ」「11n のみ」から選択します。 • 11bgn Mixed: 下位互換性のために 3 つのプロトコルを混在させる • 11b のみ: IEEE 802.11b、11 Mbps • 11g のみ: IEEE 802.11g、54 Mbps • 11n:IEEE 802.11n、450 Mbps	11bgn 混合
チャンネル	異なる帯域幅が選択できるチャネルは次のとおりです。 • 自動:デバイスは、最適な周波数チャンネルが見つかるまですべての周波数チャンネルをスキャンします。 • 20MHz 帯域幅の利用できるチャネルの 1~13 チャネルの頻度: 1～2412 MHz 2～2417 MHz 3～2422 MHz 4～2427 MHz の 5～2432 MHz 6～2437 MHz 7～2442 MHz 8～2447 MHz	自動

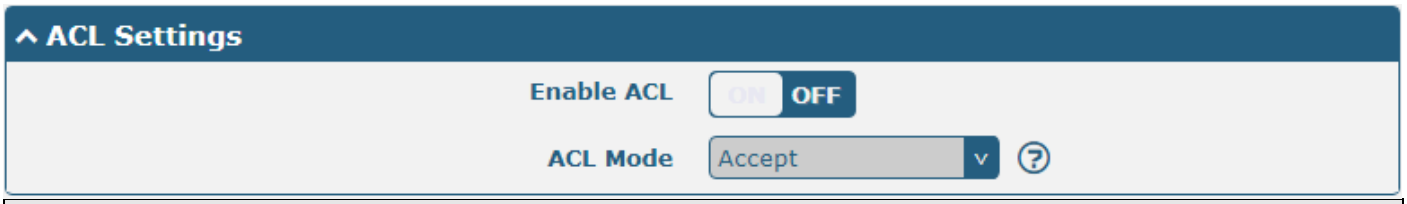
一般設定@アクセスポイント 2.4G		
アイテム	説明	デフォルト
	9〜2452 MHz 10〜2457 MHz 11〜2462 MHz の 12〜2467 MHz の 13〜2472 MHz の • 40MHz 帯域幅の利用できるチャネルの 1~13 チャネルの頻度: 1〜2412 MHz 2〜2417 MHz 3〜2422 MHz 4〜2427 MHz の 5〜2432 MHz 6〜2437 MHz 7〜2442 MHz 8〜2447 MHz 9〜2452 MHz 10〜2457 MHz 11〜2462 MHz の 12〜2467 MHz の 13〜2472 MHz の	
SSID(SSID)	ワイヤレスネットワークの名前である SSID(Service Set Identifier)を入力します。 クライアントと AP が相互に通信するには、クライアントの SSID と AP の SSID が同一である必要があります。1 から 32 文字まで入力します。	RBT-XXXX-2.4G
ブロードキャスト SSID	トグルボタンをクリックして、ブロードキャストされている SSID を有効/無効にします。有効にすると、クライアントは SSID をスキャンできます。無効にすると、クライアントは SSID をスキャンできません。デバイス AP に接続する場合は、Wi-Fi クライアント側でデバイス AP の SSID を手動で入力する必要があります。	オン

一般設定@アクセスポイント 2.4G		
アイテム	説明	デフォルト
セキュリティモード	「無効」、「WPA-パーソナル」、「WPA-エンタープライズ」、「WEP」、「EAP-TLS」を選択します。 • 無効: ユーザーはパスワードなしで Wi-Fi にアクセスできます *注:セキュリティ上の理由から、この種のモードを選択しないことを強くお勧めします。* • WPA-パーソナル:Wi-Fi アクセス保護。ID 認証には 1 つのパスワードのみが提供されます • WEP:Wired Equivalent Privacy は、ワイヤレスデバイスのデータ送信を暗号化します • WPA エンタープライズ: ネットワークに接続する各ユーザーは、個人のユーザー名とパスワード、デジタル証明書、または認証用のその他の資格情報を提供する必要があります。 *注:このオプションは、一部のモデル、R3000 で使用できます* • EAP-TLS:Transport Layer Security(TLS)プロトコルに基づく強力な認証とセキュリティのための高度な認証プロトコル。 *注:R2110 / R5020 / R5020Lite のみが WiFi EAP-TLS 認証方式をサポートしています。*	無効
WPA バージョン	「WPA/WPA2」、「WPA」、「WPA2」、「WPA3」から選択します。 • WPA / WPA2:デバイスは最適な WPA バージョンを自動的に選択します • WPA:初期の Wi-Fi セキュリティ規格は、TKIP(Temporal Key Integrity Protocol)暗号化プロトコルを使用してデータ転送を保護し、ある程度のデータ保護を提供します。 • WPA2:WPA2 は WPA のアップグレードバージョンであり、より強力な暗号化プロトコル AES(Advanced Encryption Standard)を使用し、より高度なデータ保護を提供します。 • WPA3:WPA3 は WPA2 をさらに改善したもので、より強力なパスワードクラッキング保護を使用し、公衆無線ネットワークのセキュリティを強化し、パスワードの選択方法を改善します。 *※R2110/R5020 シリーズ/R151X シリーズ/R1520/R201X シリーズは WPA3 対応*	WPA/WPA2 (英語)

一般設定@アクセスポイント 2.4G		
アイテム	説明	デフォルト
暗号化	「TKIP」または「AES」から選択します。 • TKIP: Temporal Key Integrity Protocol(TKIP)暗号化は、ワイヤレス接続を使用します。TKIP 暗号化は、WPA-PSK および WPA 802.1x 認証に使用できます • AES: AES 暗号化はワイヤレス接続を使用します。AES は、CCMP、WPA-PSK、および WPA 802.1x 認証に使用できます。AES は TKIP よりも強力な暗号化アルゴリズムです ***注意:*** *セキュリティモードはワイヤレス通信速度に影響します。ワイヤレスモードが異なれば、サポートする暗号化モードも異なります。たとえば、802.11n は WEP セキュリティ モードも TKIP アルゴリズムもサポートしていません 。使用すると、無線通信速度は 54Mbps(802.11g モード)に低下します。802.11n モードで AES を選択することをお勧めします。*	自動
PSK パスワード	事前共有キーのパスワードを入力します。8 文字から 63 文字まで入力します。	Null
RADIUS 認証サーバ アドレス	RADIUS 認証サーバのアドレスを入力します。	0.0.0.0
RADIUS 認証サーバ ポート(Radius Authentication Server Port)	Radius 認証サーバのポートを入力します。	1812
Radius サーバ共有シークレット	Radius サーバ共有パスワードを 8 ～ 128 文字に制限して入力します。	Null
グループ キーの更新インターバル	グループキーの更新時刻を入力します。	3600
WEP キー	WEP キーを入力します。キーの長さは、使用する WEP キーに応じて 10 桁または 26 桁の 16 進数(64 桁または 128 桁)にする必要があります。	Null

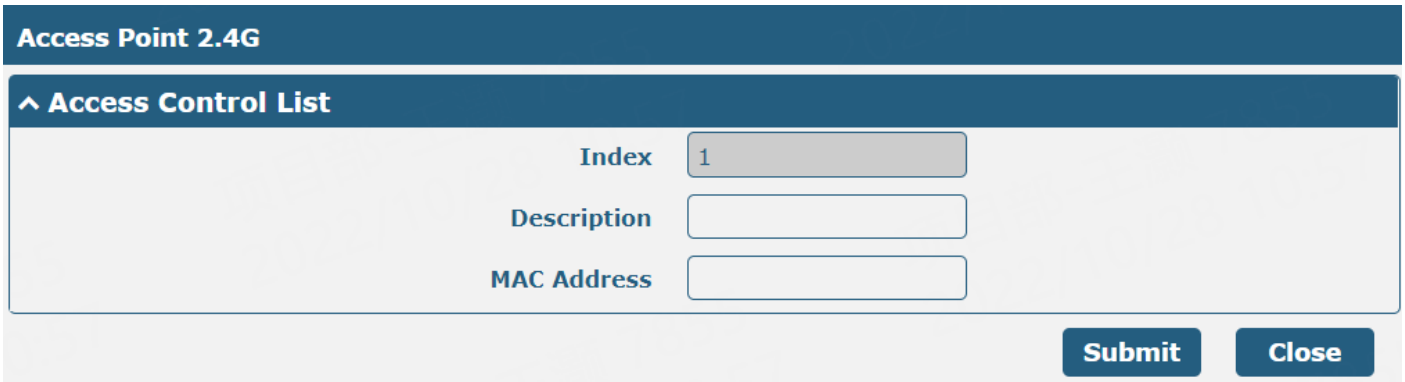


詳細設定@アクセスポイント 2.4G		
アイテム	説明	デフォルト
最大関連ステーション数	デバイスの AP にアクセスできるクライアントの最大数を設定します(値 0 は制限なしを意味します)。	0
ビーコンインターバル (Beacon Interval)	デバイス AP がワイヤレスネットワーク認証に使用されるビーコンをブロードキャストする時間インターバルを設定します。	100
DTIM 期間	配信トラフィック表示メッセージ期間を設定すると、デバイス AP はこの期間に従ってデータをマルチキャストします。	2
チャネル幅(Channel Width)	デバイスのチャネル幅を「20 MHz」または「40 MHz」 から選択します。 *注: 40MHz のチャネル幅は 2 倍のデータレートを提供します 単一の 20MHz チャネルで利用可能。データ転送速度 80MHz の帯域幅は、単一の帯域幅の 4 倍です。 20Mhz の帯域幅。*	自動
ショート GI を有効にする	トグルボタンをクリックして、[Short Guard Interval]オプションを有効/無効にします。 ショート GI は、2 つのシンボル間のブランク時間であり、信号遅延のバッファ時間が長くなります。ショート GI を使用すると、データ レートが 11% 向上しますが、パケット エラー レートも高くなります。	オン
AP 分離の有効化(Enable AP Isolation)	トグルボタンをクリックして、AP 分離オプションを有効/無効にします。有効にすると、デバイスは接続されているすべてのワイヤレスデバイスを分離します。 ワイヤレス デバイスは相互にアクセスできません。	オフ
デバッグレベル	「verbose」「debug」「info」「notice」「warning」「none」から選択します。	何一つ



ACL 設定@アクセスポイント 2.4G		
アイテム	説明	デフォルト
ACL の有効化	切り替えボタンをクリックして、このオプションを有効/無効にします。	オフ
ACL モード(ACL Mode)	「同意する」または「拒否」を選択します。 • Accept:「アクセス制御リスト」のエンティティに適合するパケットのみを許可できます • 拒否:「アクセス制御リスト」のエンティティに適合するすべてのパケットが拒否されます *注:デバイスは、「アクセス制御リスト」に含まれるデバイスのみを一度に許可または拒否できます。*	受け入れる

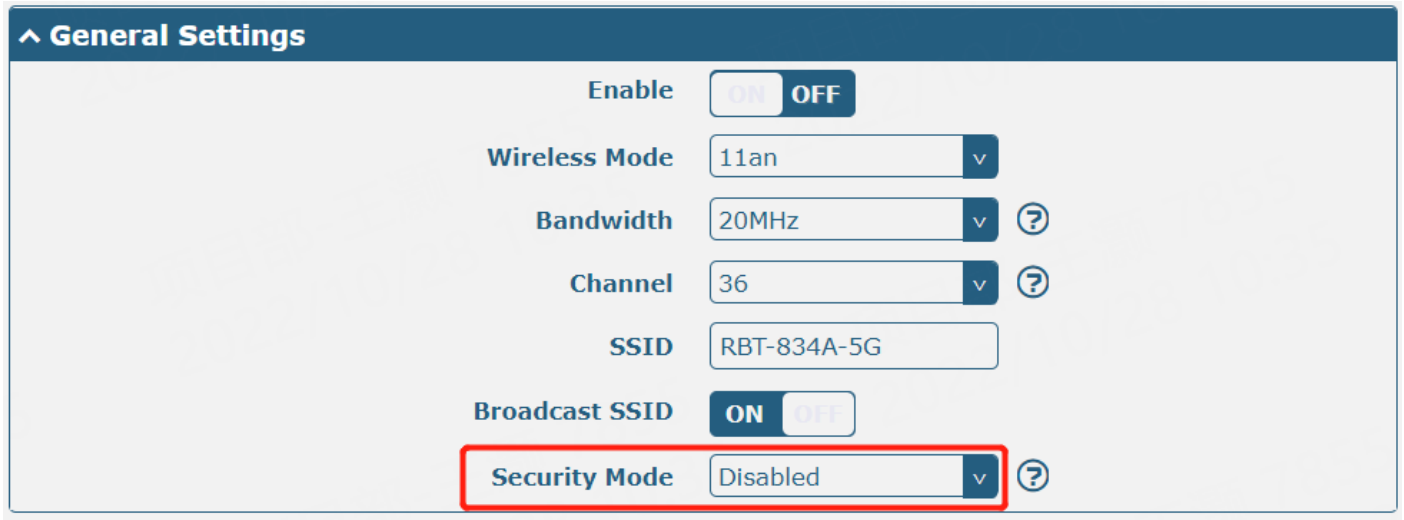
クリック + すると、MAC アドレスが [Access Control List] に追加されます。 MAC アドレスの最大数は **64** です。



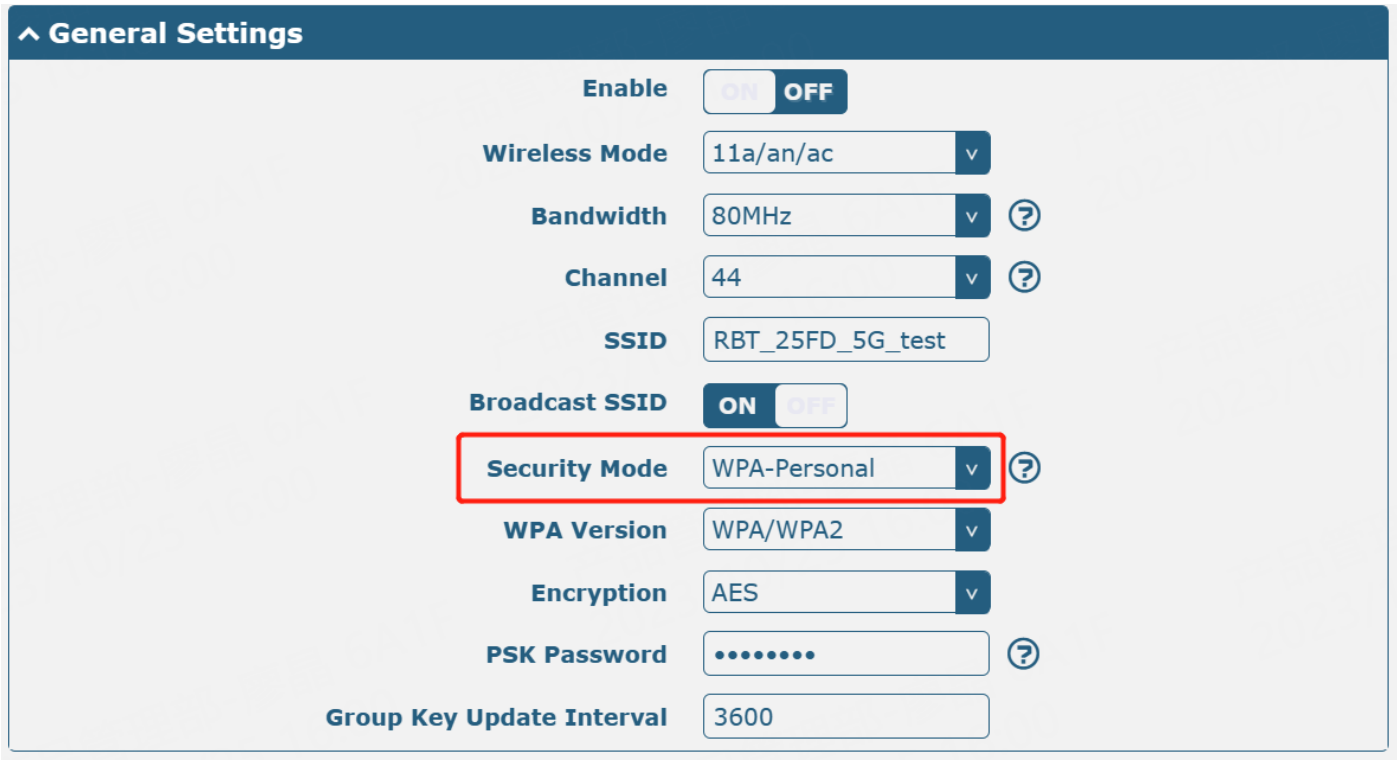
アクセス制御リスト@アクセスポイント 2.4G		
インデックス	リストの序数を示します。	--
説明	このアクセス制御リストの説明を入力します。	Null
MAC アドレス	ここに MAC アドレスを追加します。	Null

3) アクセスポイント 5G

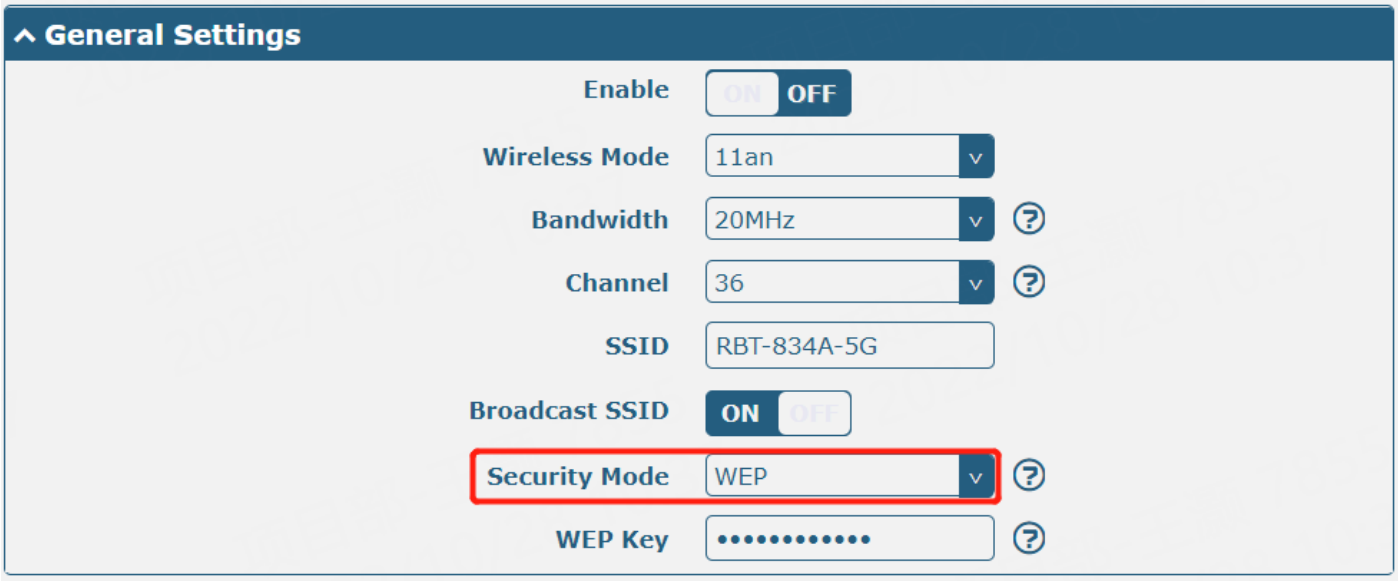
[**アクセスポイントの 5G**]列をクリックして、Wi-Fi AP のパラメータを設定します。デフォルトでは、セキュリティモードは「無効」に設定されています。



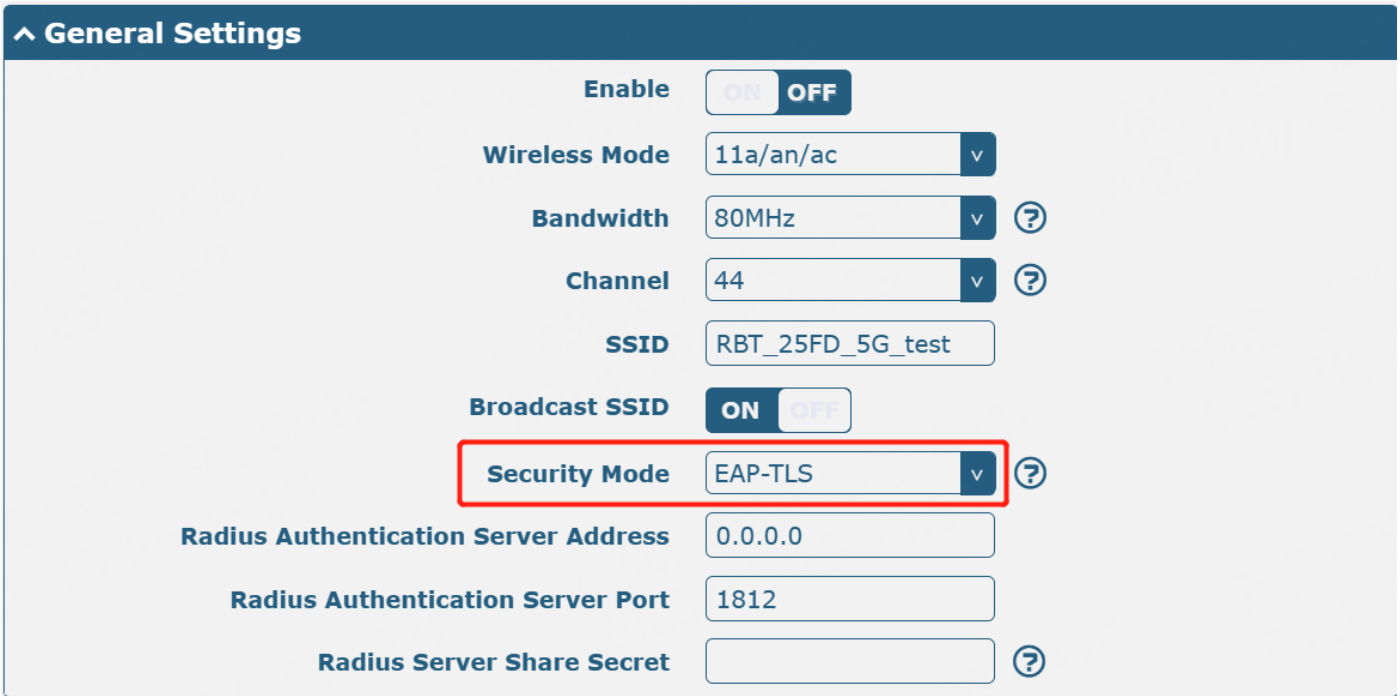
セキュリティモードを「WPA-Personal」に設定した場合、以下のウィンドウが表示されます。



セキュリティモードを「WEP」に設定すると、以下のウィンドウが表示されます。



セキュリティモードを「EAP-TLS」に設定している間、以下のウィンドウが表示されます。
手記:
(1) R2110/R5020/R5020Lite のみ、セキュリティモード「EAP-TLS」に対応しています。

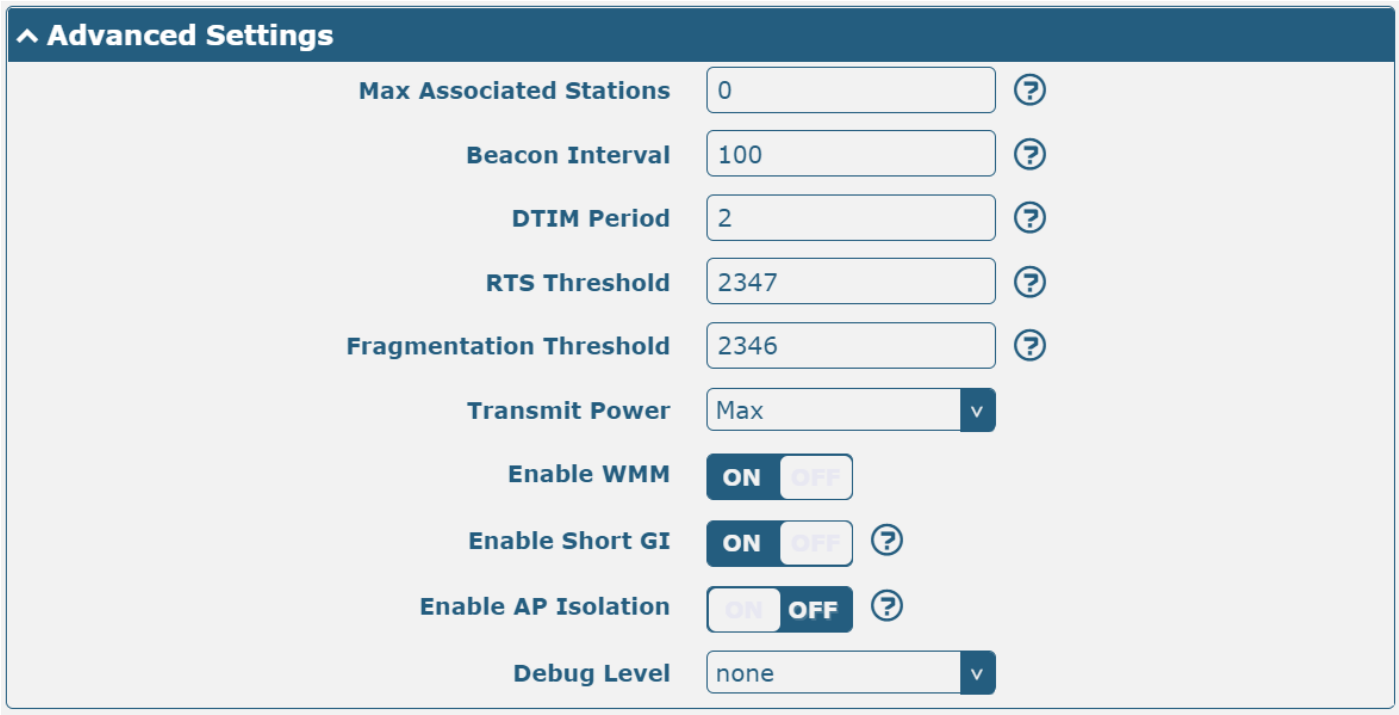


一般設定 @ Access Point 5G		
アイテム	説明	デフォルト
エネーブル	トグルボタンをクリックして、Wi-Fi アクセスポイントオプションを有効/無効にします。	オフ
ワイヤレスモード	「11an」または「11a/an/ac」から選択します。 • 11an:IEEE 802.11a、54Mbps および IEEE 802.11n、300Mbps に対応 • 11a/an/ac:IEEE 802.11a、54Mbps、IEEE802.11n 300Mbps および 802.11ac、867Mbps に対応	平成 11 年
帯域幅	「20MHz」「40MHz」「80MHz」から選択します。 *注:40 MHz のチャネル幅は、1 つの 20 MHz チャネルで使用可能なデータレートの 2 倍を提供します。80 MHz 帯域幅のデータ転送速度は、単一の 20 MHz 帯域幅のデータ転送速度の 4 倍です。*	20MHz の
チャンネル	帯域幅のオプションチャネルは次のとおりです。 • 20MHz 帯域幅の利用できるチャネルの 36~165 チャネルの頻度: 36～5180 MHz の 40～5200 MHz の 44～5220 MHz の 48～5240 MHz の 149 - 5745 MHz の 153 - 5765 MHz 157～5785 MHz 161 - 5805 MHz	36

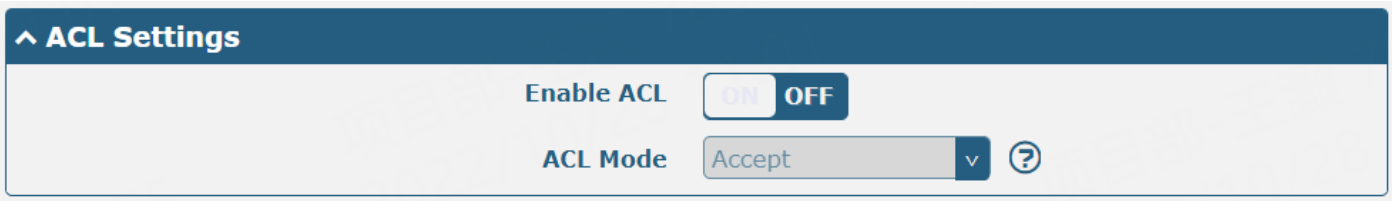
一般設定 @ Access Point 5G		
アイテム	説明	デフォルト
	165〜5825 MHz • 40MHz 帯域幅の利用できるチャネルの 36~165 チャネルの頻度: 36〜5180 MHz の 40〜5200 MHz の 44〜5220 MHz の 48〜5240 MHz の 149 - 5745 MHz の 153 - 5765 MHz 157〜5785 MHz 161 - 5805 MHz 165〜5825 MHz • 80MHz 帯域幅の 36~165 チャネルの周波数は、チャネルを利用できます。 36〜5180 MHz の 40〜5200 MHz の 44〜5220 MHz の 48〜5240 MHz の 149 - 5745 MHz の 153 - 5765 MHz 157〜5785 MHz 161 - 5805 MHz 165〜5825 MHz ***注:*** *異なる帯域幅で 5GHzWi-Fi の利用可能なすべてのチャネルは上記のとおりです。Web パラメータは、国や地域によって利用可能なチャネルが異なるため、設定する必要があります。*	
SSID(SSID)	ワイヤレスネットワークの名前である SSID(Service Set Identifier)を入力します。 クライアントと AP が相互に通信するには、クライアントの SSID と AP の SSID が同一である必要があります。1 から 32 文字まで入力します。	RBT-XXXX-5G
ブロードキャスト SSID	トグルボタンをクリックして、ブロードキャストされている SSID を有効/無効にします。有効にすると、クライアントは SSID をスキャンできます。無効にすると、クライアントは SSID をスキャンできません。デバイス AP に接続する場合は、Wi-Fi クライアント側でデバイス AP の SSID を手動で入力する必要があります。	オン

一般設定 @ Access Point 5G		
アイテム	説明	デフォルト
セキュリティモード	「無効」、「WPA-パーソナル」、「WPA-エンタープライズ」、「WEP」、「EAP-TLS」を選択します。 • 無効: ユーザーはパスワードなしで Wi-Fi にアクセスできます *注:セキュリティ上の理由から、この種のモードを選択しないことを強くお勧めします。* • WPA-パーソナル:Wi-Fi アクセス保護。ID 認証には 1 つのパスワードのみが提供されます • WEP:Wired Equivalent Privacy は、ワイヤレスデバイスのデータ送信を暗号化します • WPA エンタープライズ: ネットワークに接続する各ユーザーは、個人のユーザー名とパスワード、デジタル証明書、または認証用のその他の資格情報を提供する必要があります。 *注:このオプションは、一部のモデル、R3000 で使用できます* • EAP-TLS:Transport Layer Security(TLS)プロトコルに基づく強力な認証とセキュリティのための高度な認証プロトコル。 • *注:R2110 / R5020 / R5020Lite のみが WiFi EAP-TLS 認証方式をサポートしています。*	無効
WPA バージョン	「WPA/WPA2」、「WPA」、「WPA2」、「WPA3」から選択します。 • WPA / WPA2:デバイスは最適な WPA バージョンを自動的に選択します • WPA:初期の Wi-Fi セキュリティ規格は、TKIP(Temporal Key Integrity Protocol)暗号化プロトコルを使用してデータ転送を保護し、ある程度のデータ保護を提供します。 • WPA2:WPA2 は WPA のアップグレードバージョンであり、より強力な暗号化プロトコル AES(Advanced Encryption Standard)を使用し、より高度なデータ保護を提供します。 • WPA3:WPA3 は WPA2 をさらに改善したもので、より強力なパスワードクラッキング保護を使用し、公衆無線ネットワークのセキュリティを強化し、パスワードの選択方法を改善します。 • *注:R2110/R5020 シリーズ/R151X シリーズ /R1520/R201X シリーズは WAP3 をサポートします*	WPA/WPA2 (英語)

一般設定 @ Access Point 5G		
アイテム	説明	デフォルト
暗号化	「TKIP」または「AES」から選択します。 • TKIP: Temporal Key Integrity Protocol(TKIP)暗号化は、ワイヤレス接続を使用します。TKIP 暗号化は、WPA-PSK および WPA 802.1x 認証に使用できます • AES: AES 暗号化はワイヤレス接続を使用します。AES は、CCMP、WPA-PSK、および WPA 802.1x 認証に使用できます。AES は TKIP よりも強力な暗号化アルゴリズムです ***注意:*** *セキュリティモードはワイヤレス通信速度に影響します。ワイヤレスモードが異なれば、サポートする暗号化モードも異なります。たとえば、802.11n は WEP セキュリティ モードも TKIP アルゴリズムもサポートしていません 。使用すると、無線通信速度は 54Mbps(802.11g モード)に低下します。802.11n モードで AES を選択することをお勧めします。*	AES の
PSK パスワード	事前共有キーのパスワードを入力します。8 文字から 63 文字まで入力します。	Null
RADIUS 認証サーバ アドレス	RADIUS 認証サーバのアドレスを入力します。	0.0.0.0
RADIUS 認証サーバ ポート(Radius Authentication Server Port)	Radius 認証サーバのポートを入力します。	1812
Radius サーバ共有シークレット	Radius サーバ共有パスワードを 8 ~ 128 文字に制限して入力します。	Null
グループ キーの更新インターバル	グループキーの更新時刻を入力します。	3600
WEP キー	WEP キーを入力します。キーの長さは、使用する WEP キーに応じて 10 桁または 26 桁の 16 進数(64 桁または 128 桁)にする必要があります。	Null

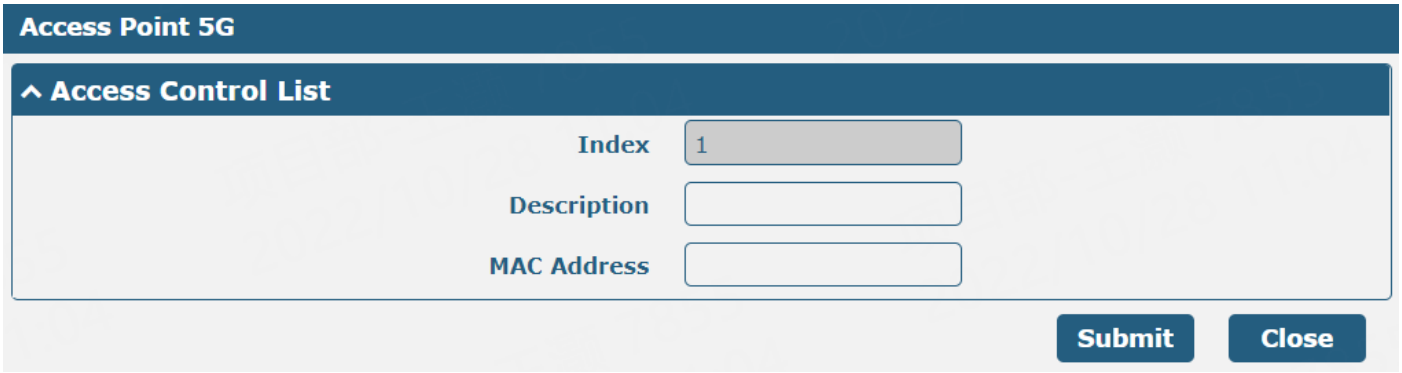


詳細設定@アクセスポイント 5G		
アイテム	説明	デフォルト
最大関連ステーション数	デバイスの AP にアクセスできるクライアントの最大数を設定します(値 0 は制限なしを意味します)。	0
ビーコンインターバル (Beacon Interval)	デバイス AP がワイヤレスネットワーク認証に使用されるビーコンをブロードキャストする時間インターバルを設定します。	100
DTIM 期間	配信トラフィック表示メッセージ期間を設定すると、デバイス AP はこの期間に従ってデータをマルチキャストします。	2
RTS しきい値	「送信要求」のしきい値を設定します。しきい値が 2347 に設定されている場合、デバイス AP はデータを送信する前に検出信号を送信しません。また、しきい値が 0 に設定されている場合、デバイス AP はデータを送信する前に検出信号を送信します。	2347
フラグメンテーションしきい値(Fragmentation Threshold)	Wi-Fi AP のフラグメンテーションしきい値を設定します。デフォルト値の 2346 を使用することをお勧めします。	2346
送信電力	「Max」、「High」、「Medium」、「Low」から選択します。	マックス
WMM を有効にする	トグルボタンをクリックして、WMM オプションを有効/無効にします。	オン
ショート GI を有効にする	トグルボタンをクリックして、[Short Guard Interval]オプションを有効/無効にします。 ショート GI は、2 つのシンボル間のブランク時間であり、信号遅延のバッファ時間が長くなります。ショート GI を使用すると、データレートが 11% 向上しますが、パケットエラーレートも高くなります。	オン
AP 分離の有効化(Enable AP Isolation)	トグルボタンをクリックして、AP 分離オプションを有効/無効にします。有効にすると、デバイスは接続されているすべてのワイヤレスデバイスを分離します。ワイヤレスデバイスは 相互にアクセスできません。	オフ
デバッグレベル	「verbose」「debug」「info」「notice」「warning」「none」から選択します。	何一つ



ACL 設定 @ Access Point 5G		
アイテム	説明	デフォルト
ACL の有効化	切り替えボタンをクリックして、このオプションを有効/無効にします。	オフ
ACL モード(ACL Mode)	「同意する」または「拒否する」から選択します。 • Accept:「アクセス制御リスト」のエンティティに適合するパケットのみを許可できます • 拒否:「アクセス制御リスト」のエンティティに適合するすべてのパケットが拒否されます *注:デバイスは、「アクセス制御リスト」に含まれるデバイスのみを一度に許可または拒否できます。*	受け入れる

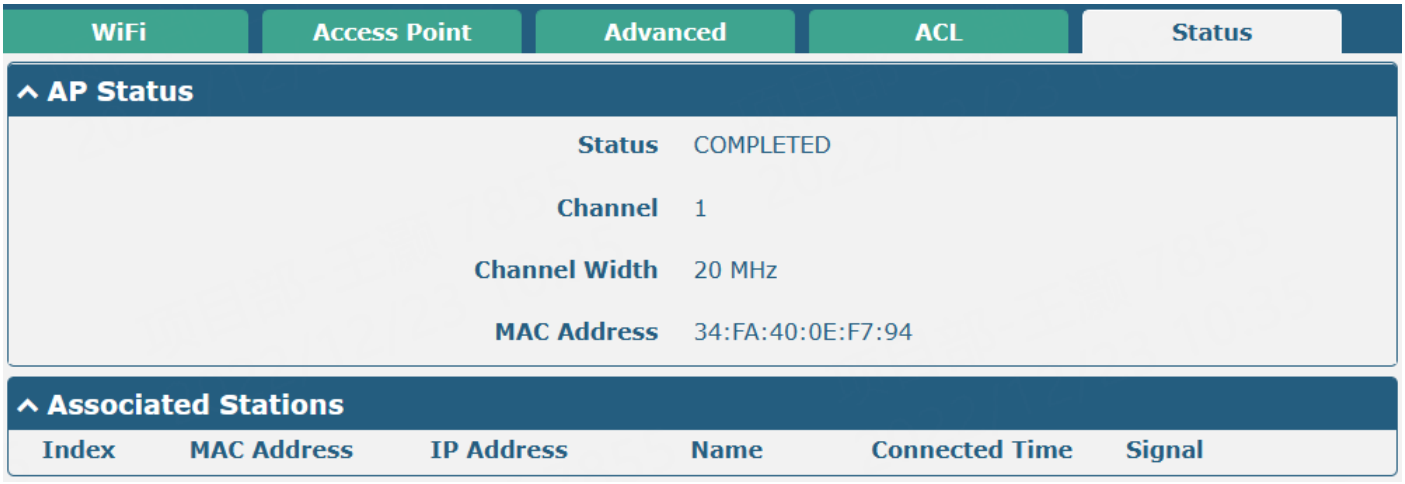
クリック + すると、MAC アドレスが [Access Control List] に追加されます。 MAC アドレスの最大数は **64** です。



アクセス制御リスト@アクセスポイント 5G		
インデックス	リストの序数を示します。	--
説明	このアクセス制御リストの説明を入力します。	Null
MAC アドレス	ここに MAC アドレスを追加します。	Null

4) ステータス

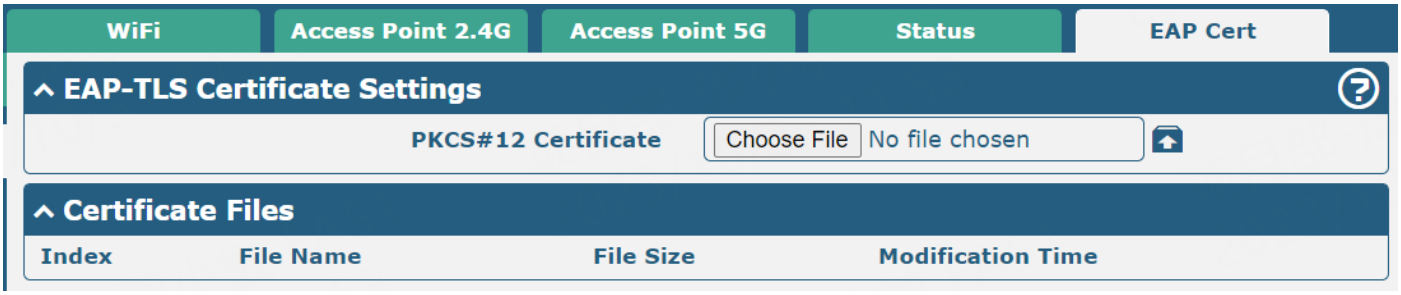
このセクションでは、AP のステータスを表示できます。



注: Wi-Fi はデフォルトでオフになっています。以下の手順に従って有効にし、デバイスを Wi-Fi クライアントとして設定します。

5) EAP 証明書

このセクションでは、EAP 証明書の設定と証明書ファイル情報の表示について説明します。



EAP 証明書		
インデックス	リストの序数を示します。	--
PKCS#12 証明書	Choose File ボタンをクリックしてローカル PKCS#12 証明書ファイルを選択し、ボタンをクリックして証明書 ファイルをインポートします。	

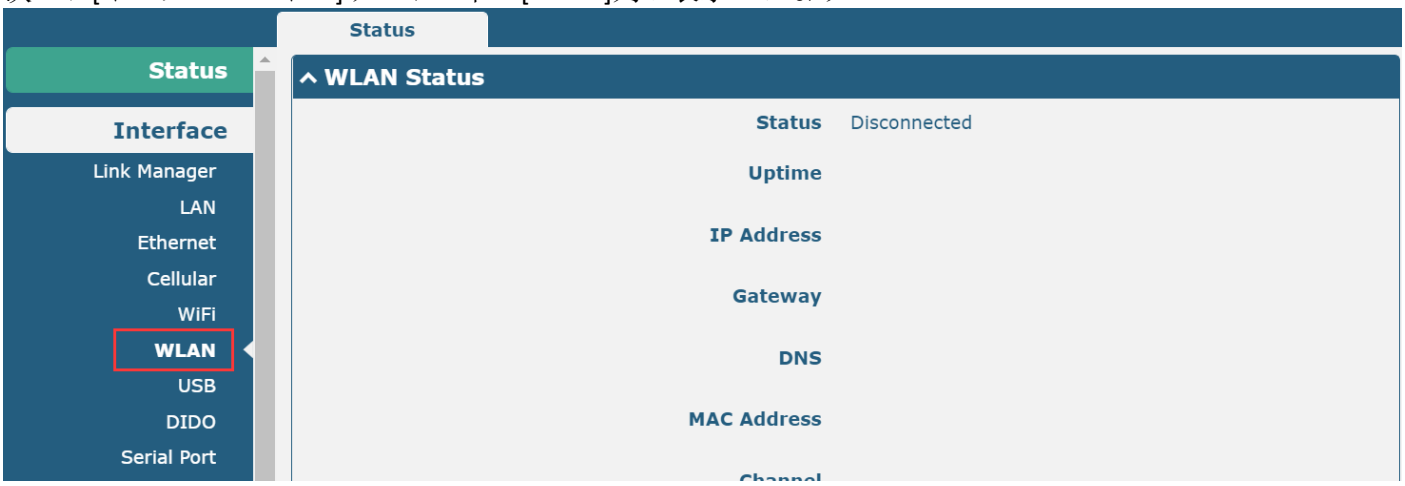
6) Wi-Fi クライアント

注:この部分は R3000 シリーズにのみ適用されます。

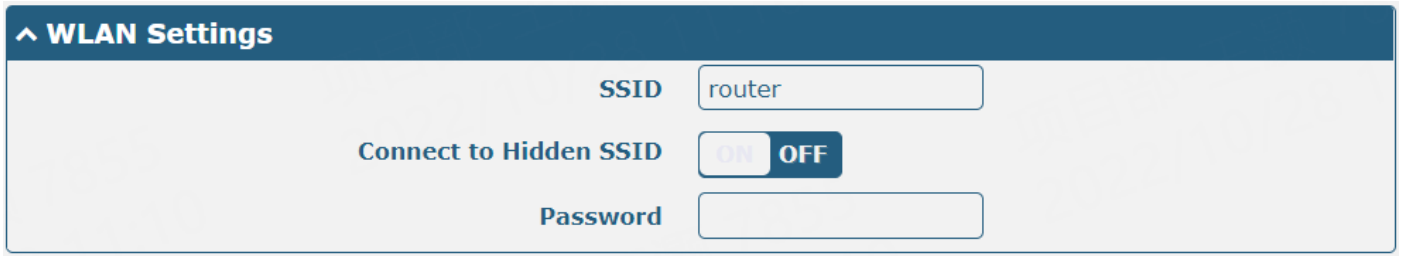
デバイスを Wi-Fi クライアントとして構成する

[**Interface** > WiFi] > [WiFi] をクリックし、モードとして [Client] を選択し、AP タイプに関して関連するクライアント バンドを選択して [Submit] をクリックします。

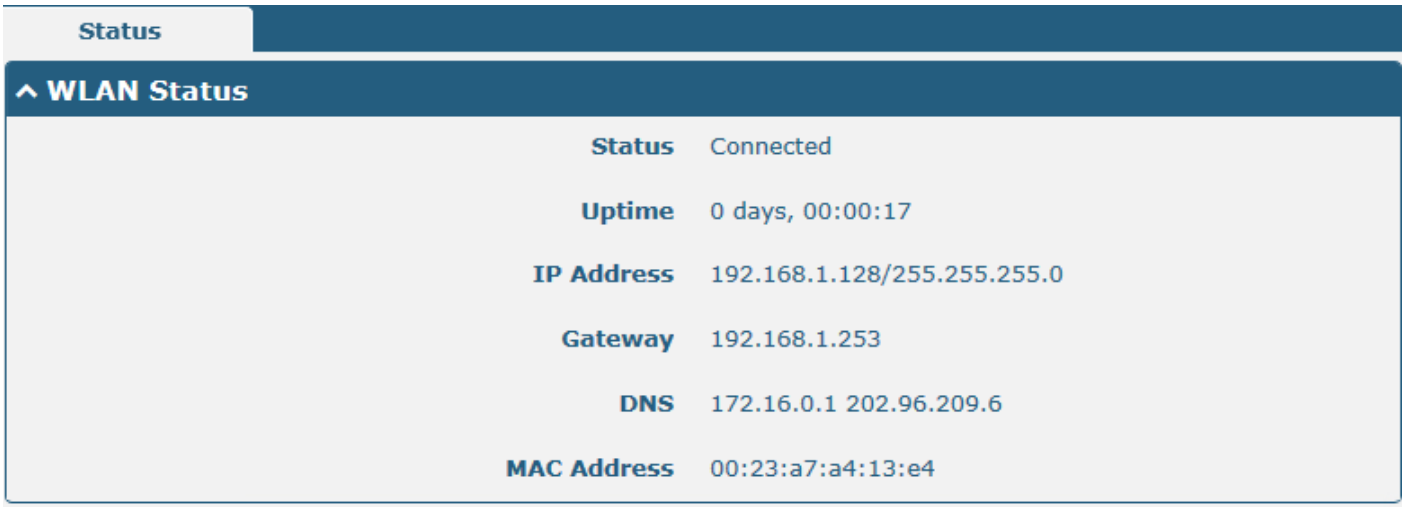
次に、[インターフェイス]リストの下に[WLAN]列が表示されます。



[**Interface > Link Manager] > [Link Settings] をクリックし**、WLAN の編集ボタンをクリックして、関連するパラメータを設定します。

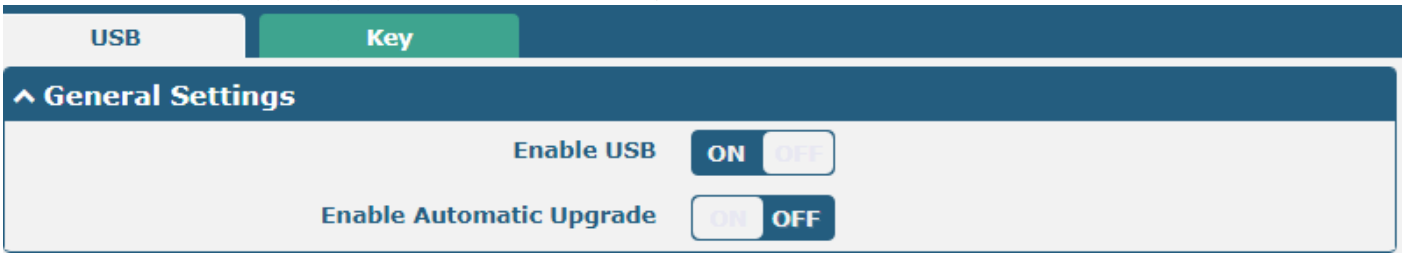


モードをクライアントに設定した後、Wi-Fi クライアントのパラメータを設定するには、**WLAN>インターフェイス**をクリックします。 **設定が終わったら、忘れずに** Save & Apply > Reboot をクリックして、設定を有効にしてください。



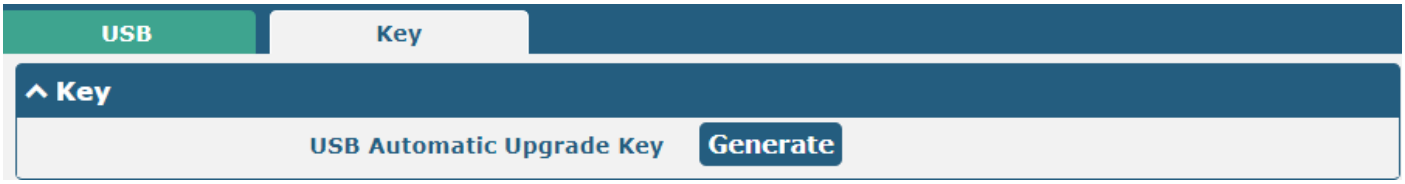
3.2.6 USB 接続

このセクションでは、USB パラメータを設定できます。デバイスの USB インターフェイスは、ファームウェアのアップグレードと構成のアップグレードに使用できます。



1) キー

このセクションでは、USB のキーを生成できます。



一般設定 @ USB		
アイテム	説明	デフォルト
USB を有効にする	トグルボタンをクリックして、USB オプションを有効/無効にします。	オン
自動アップグレードの有効化	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、デバイスのファームウェアを備えた USB ストレージデバイスを挿入すると、デバイスのファームウェアが自動的に更新されます。	オフ
鍵		
アイテム	説明	デフォルト

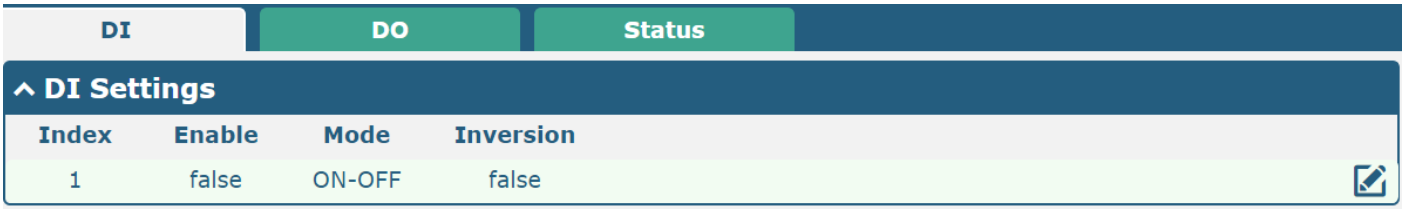
USB 自動更新キー	Generate クリックしてキーを生成し、クリックしてキー Download をダウンロードします。	--

注意: USB 自動アップグレードの過程で、USB 自動アップグレード機能を使用しているときにランニングライトが表示される場合は、アップグレードが進行中であることを意味します。ランニングライトが停止し、USR ライトが点灯すると、アップグレードが完了したことを意味します。アップグレード後、デバイスは自動的に再起動しません。ランニングライト効果がない場合は、異常があることを意味し、自動アップグレードプロセスには入りません。

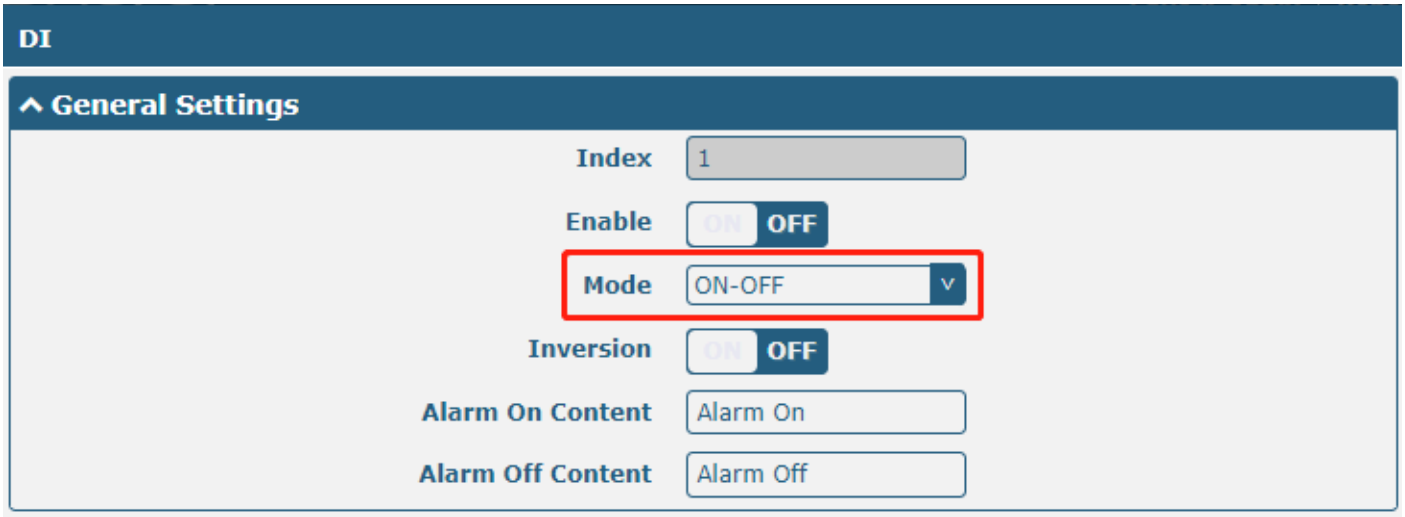
3.2.7 DI/DO

このセクションでは、DI/DO パラメータを設定できます。 DI インターフェースはアラームのトリガーに使用でき、DO はスレーブデバイスの制御に使用してリアルタイム監視を実現できます。

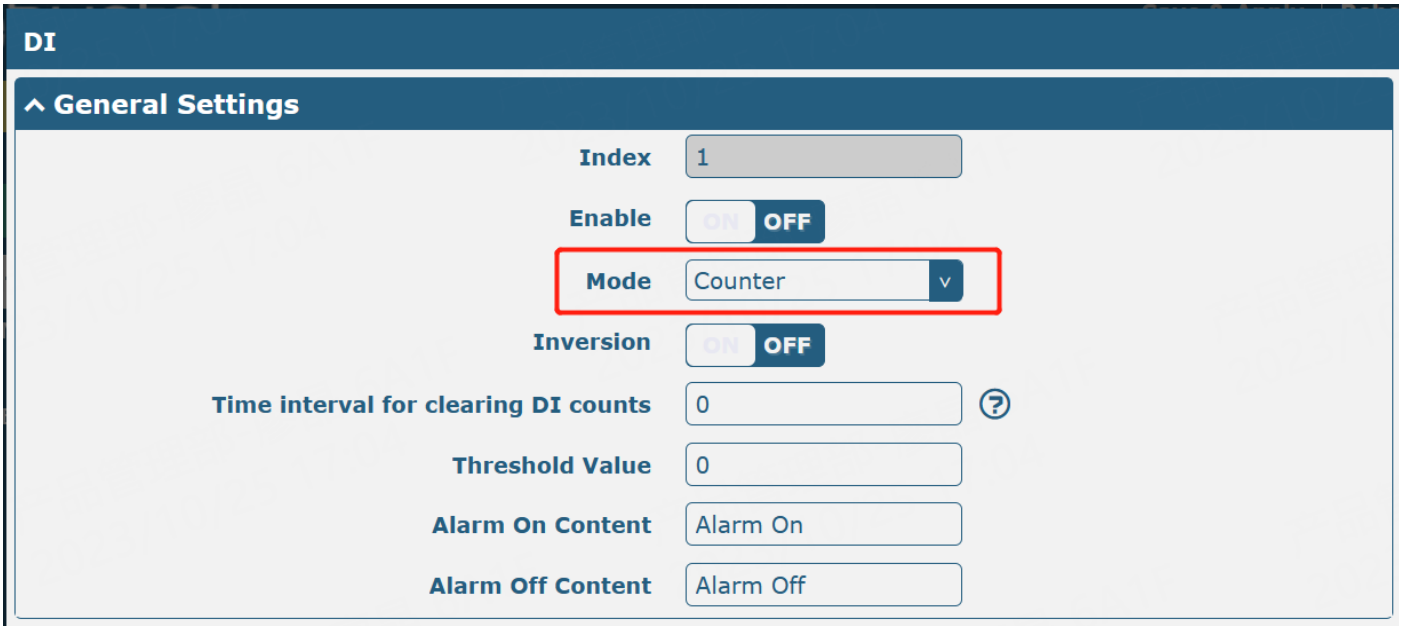
1) DI



DI インデックス 1 の 右端のボタンは下図のようです。 デフォルトモードが「ON-OFF」の場合、ウィンドウが下に表示されます。



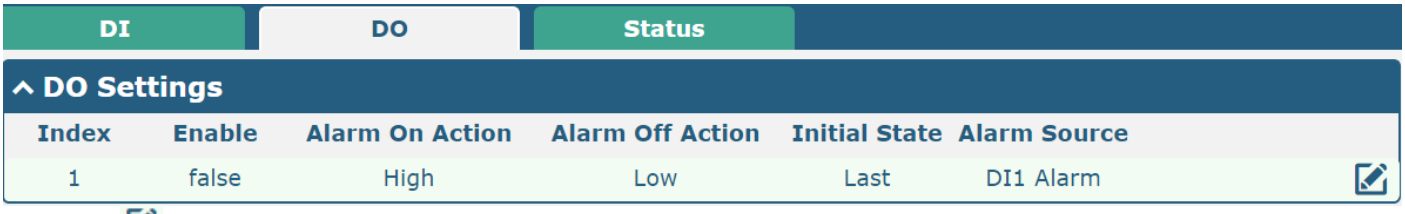
モードとして「カウンター」を選択すると、ウィンドウが下に表示されます。



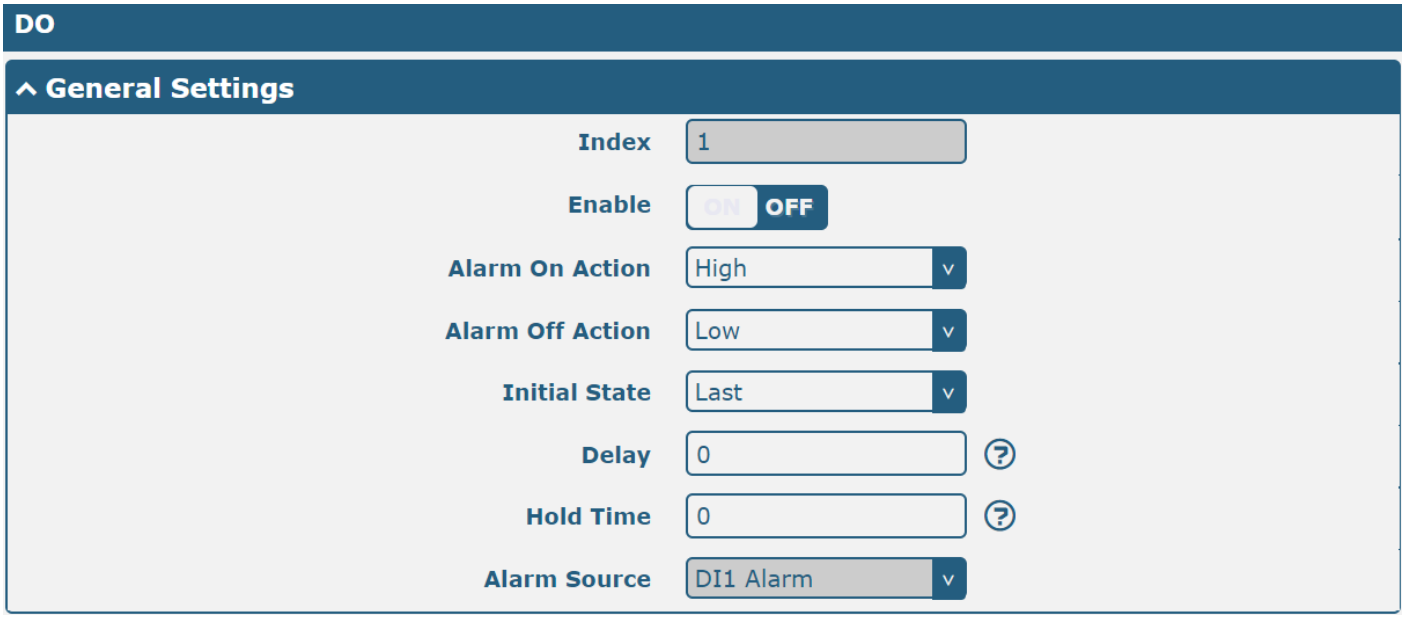
一般設定 @ DI		
アイテム	説明	デフォルト
インデックス	リストの序数を示します。	--
エネーブル	トグルボタンをクリックして、デジタル入力機能を有効/無効にします。	オフ
モード	「ON-OFF」または「カウンター」を選択します。 • ON-OFF:DI アクセス ON-OFF 時にアラームモードをトリガーできます。 • カウンター: イベント カウンター モード。	オンオフ
倒置	カウントは、レベルの立ち上がりエッジ カウントまたは立ち下がりエッジ カウントに分割されます。現在の立ち上がりエッジがカウントの場合、逆エッジは立ち下がりエッジカウントです。	オフ
DI カウントをクリアする時間インターバル	DI カウントクリアタイマーを設定するための入力です。可能な値の範囲は 0~2880 で、単位は分です。0 は、この関数を使用しないことを意味します。	0
しきい値	しきい値は、モードがカウントされるときに一意のパラメーターです。カウント値がしきい値に達したときに DI アラームをトリガーするようにしきい値を設定します。	0
コンテンツのアラーム	アラームがオンのときにコンテンツを表示します。	アラームオン
アラームオフコンテンツ	アラームがオフのときにコンテンツを表示します。	アラームオフ

注:「反転」ボタンを有効にした後、低アラームに切り替わると、デフォルトで高アラームになります。

2) DO

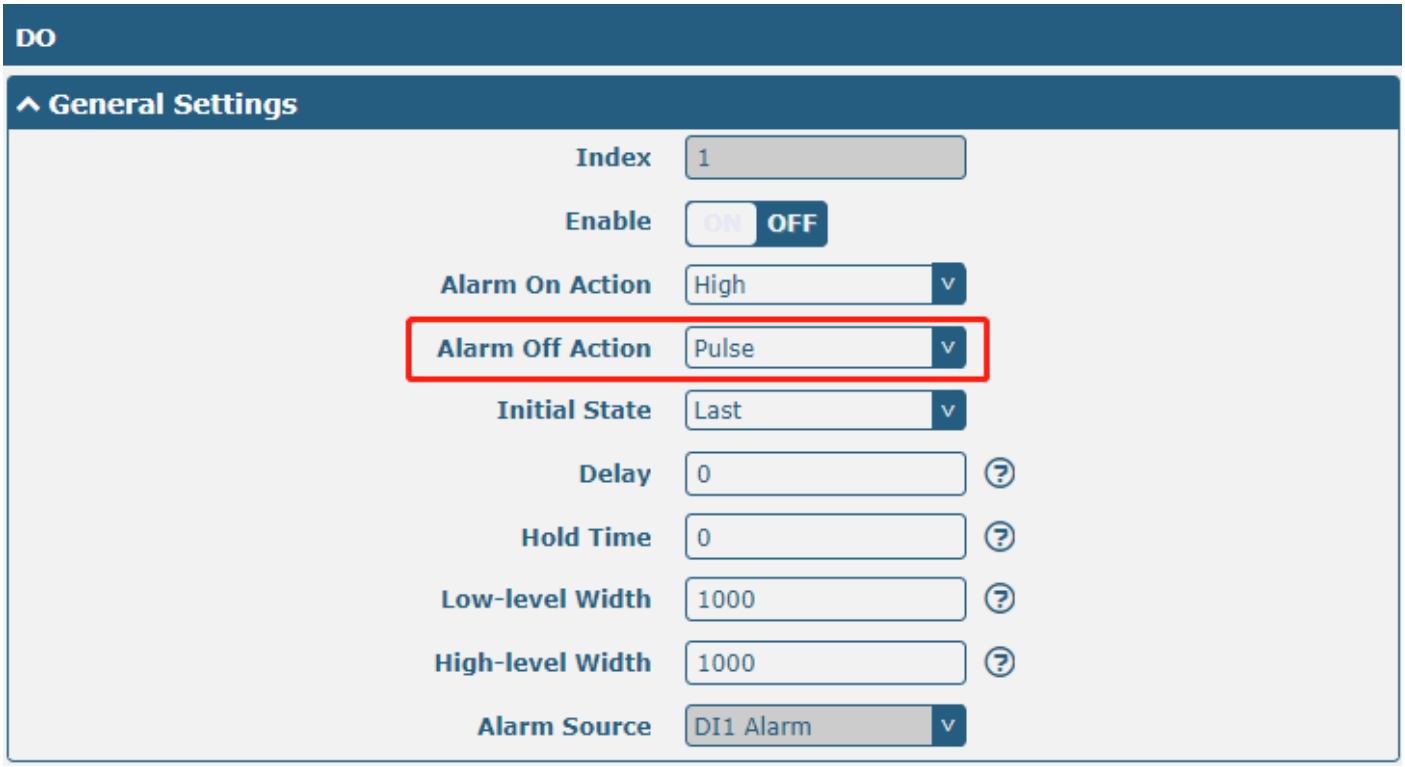


クリック して DO インデックス 1 を入力すると、設定ウィンドウが下に表示されます。



アクションのアラーム として「パルス」を選択すると、ウィンドウが下に表示されます。

アラームオフアクションとして「パルス」を選択すると、ウィンドウが下に表示されます。



一般設定@ DO		
アイテム	説明	デフォルト
インデックス	リストの序数を示します。	--
エネーブル	トグルボタンをクリックして、この DO を有効/無効にします。	オフ
アラーム オン アクション	デジタル出力は、アラームが発生すると開始されます。「High」「Low」「Pulse」から選択します。 • 高:高電気レベル出力。 • 低: 低 電気レベル 出力。 • パルス:トリガー時にパルスモードパラメータで指定された矩形波を生成します。	高い
アラーム オフ アクション	アラームが解除されると、デジタル出力が開始されます。「High」「Low」「Pulse」から選択します。 • 高:高電気レベル出力。 • 低: 低 電気レベル 出力。 • パルス:トリガー時にパルスモードパラメータで指定された矩形波を生成します。	低い
初期状態	電源投入時のデジタル出力状態を指定します。「Last」「High」「Low」から選択します。 • 最後: DO のステータスは、最後の電源オフのステータスで構成されます。 • 高:DO インターフェースは高い電気レベルにあります。 • 低: DO インターフェースは 電気レベルが低いです。	Last
遅延 (単位:100ms)	DO アラーム起動の遅延時間を設定します。 最初のパルスは「遅延」の後に生成されます。 0 から 3000 まで入力します (0 = 遅延なしでパルスを生成します)。	0
ホールドタイム (単位:秒)	DO ステータスのホールド時間(アラームオンアクション/アラームオフアクション)を設定します。アクション時間がこの指定された時間に達すると、DO はアクションを停止します。 0 から 3000 秒の範囲で入力します。	0

一般設定@ DO		
アイテム	説明	デフォルト
	(0: 次のアクションまで継続)	
低レベル幅 (単位:ms)	低レベルの幅を設定します。 Pulse を「Alarm On Action/Alarm Off Action」として有効にした場合に使用できます 。パルス出力モードでは、選択したデジタル出力チャンネルは、パルスモードパラメータで指定された矩形波を生成します。ここでは、低レベルの幅を指定します。 1000 から 3000 まで 入力します。	1000
大まかな幅 (単位:ms)	大まかな幅を設定します。 Pulse を「Alarm On Action/Alarm Off Action」として有効にした場合に使用できます 。パルス出力モードでは、選択したデジタル出力チャンネルは、パルスモードパラメータで指定された矩形波を生成します。大まかな幅はここで指定します。1000 から 3000 まで 入力します。	1000
アラーム源	デジタル出力の起動は、このアラームによってアクティブにすることができます。	None

3) ステータス

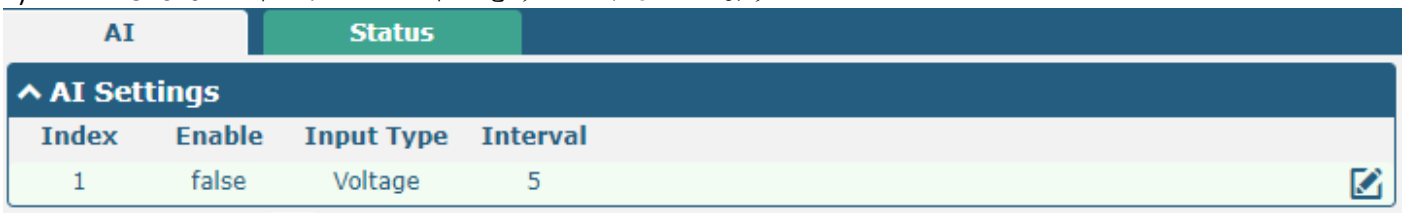
このウィンドウでは、 DI/DO インタフェースのステータスを表示することができます。また、ここで DI のカウンターアラームをクリアすることもできます。 Clear ボタンをクリックして、カウンターアラームの DI1 または DI2 の月次使用統計情報をクリアします。

3.2.8 AI

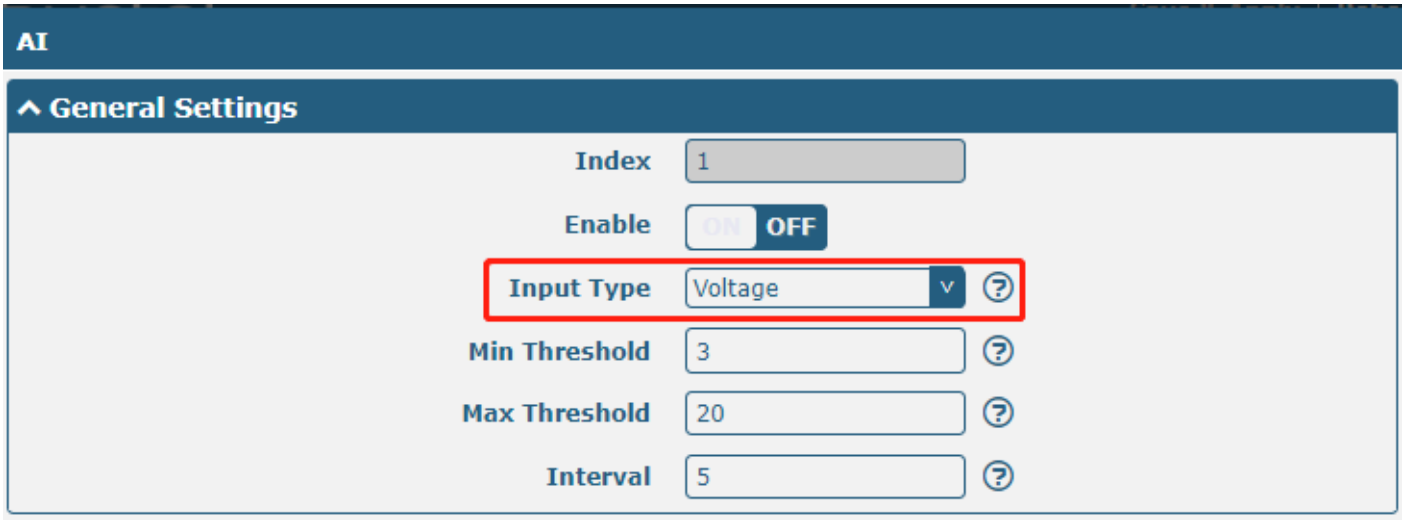
アナログ入力(AI)のパラメータを設定するセクションです。アナログ入力は、特定の範囲内のアナログ信号を収集するために使用され、センサーの電圧、電流、温度、圧力などの連続的に変化する値を収集するためによく使用されます。アナログ入力に使用される ADC ビットの精度が高いほど、アナログ量子化が細かくなり、結果の精度が高くなります。

手記：

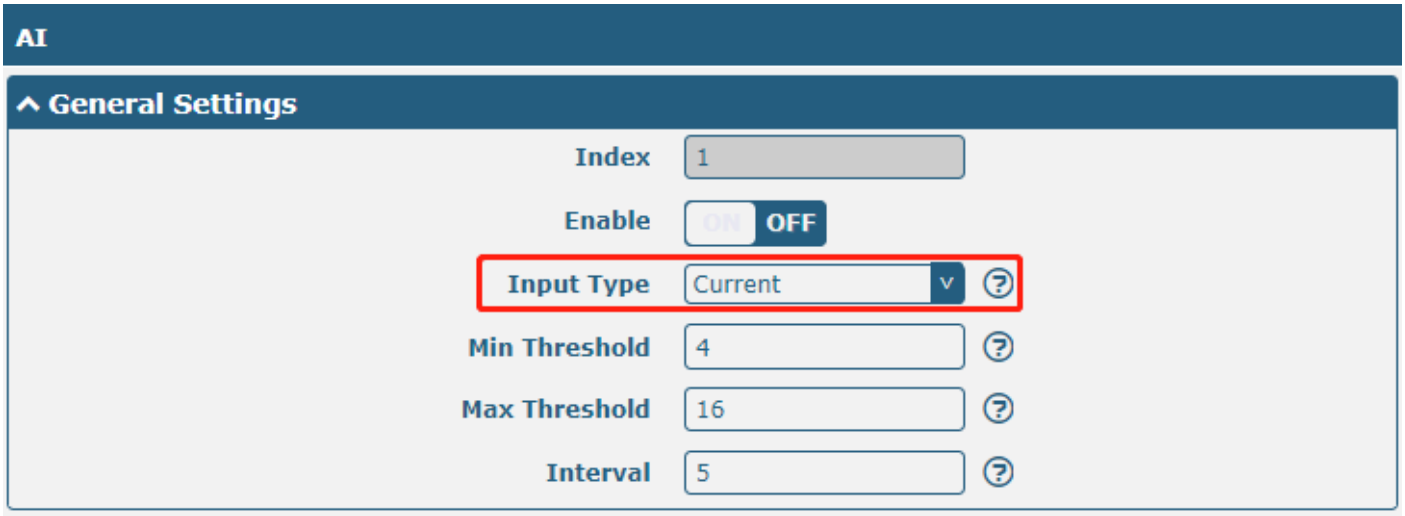
1) R1520 は AI インターフェイスをサポートしています。



DI インデックス 1 の 右端のボタンは下図のようです。「入力タイプ」が「電圧」の場合、以下のようにウィンドウが表示されます。



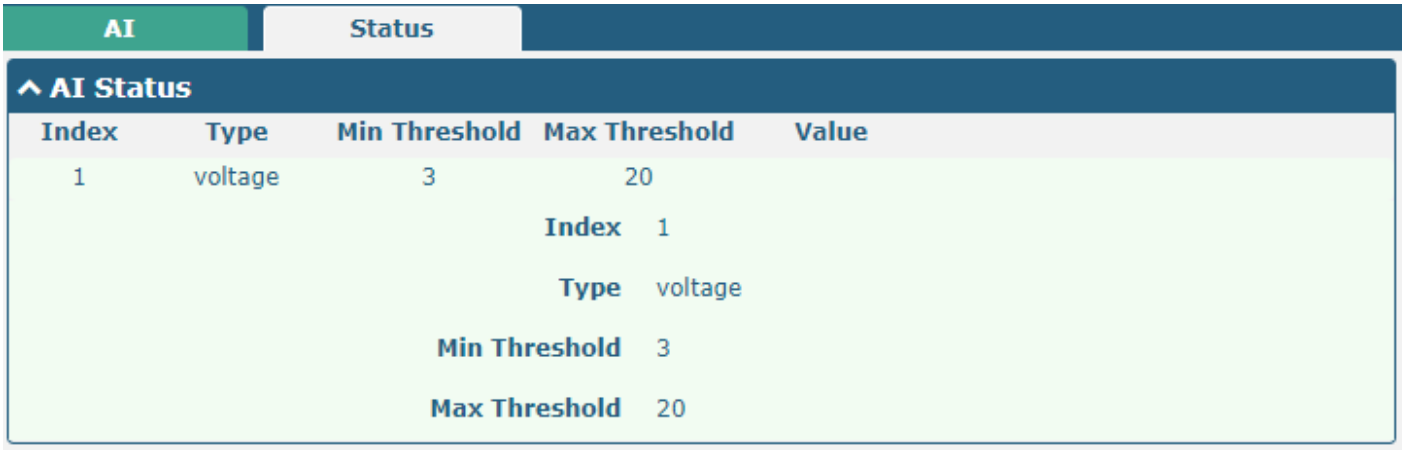
「 入力タイプ」が「Current」の場合、ウィンドウが下に表示されます。



AI(アナログ入力)		
アイテム	説明	デフォルト
インデックス	リストの序数を示します。	--
エネーブル	スイッチボタンを「ON」にすると、アナログ入力機能がオンになります。	オフ
入力タイプ	「電圧」または「電流」を選択します。 • 電圧:収集されるデータは電圧です。 • 現在: 収集されるデータは最新です。	電圧
最小しきい値 (Min Threshold) @Voltage	最小電圧閾値を設定します。AI インターフェースによって収集された電圧が最小電圧しきい値を下回ると、イベント通知がトリガーされます。単位:V。	3
最大しきい値 (Max Threshold) @Voltage	最大電圧閾値を設定します。AI インターフェースによって収集された電圧が最小電圧しきい値を超えると、イベント通知がトリガーされます。単位:V。	20
最小しきい値 (Min Threshold) @Current	最小電流しきい値を設定します。AI インターフェースによって収集された電流が最小電圧しきい値を下回ると、イベント通知がトリガーされます。単位:mA。	4
最小しきい値 (Min Threshold) @Current	最大電流閾値を設定します。AI インターフェースによって収集された電流が最小電圧しきい値を超えると、イベント通知がトリガーされます。単位:mA。	16
間	数秒ごとに最新のデータを収集します。	5

1) ステータス

「ステータス」列をクリックすると、AI のステータスが表示されます。

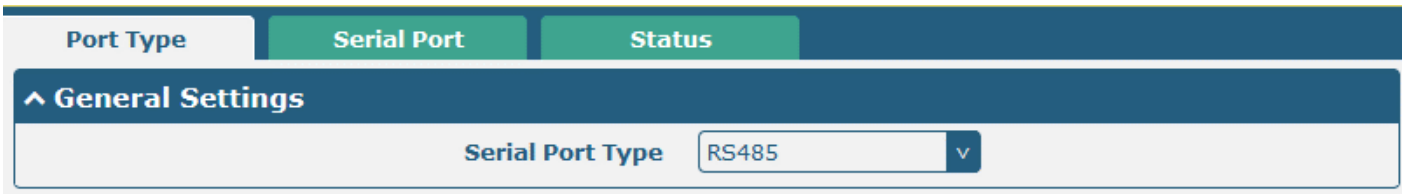


3.2.9 シリアルポート

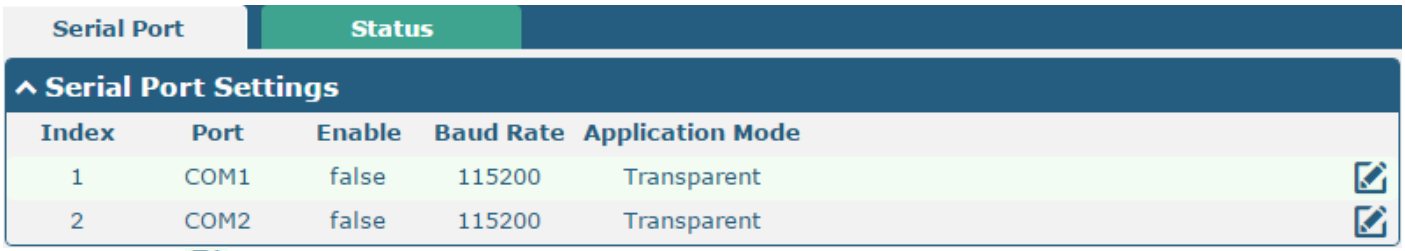
このセクションでは、シリアルポートのパラメータを設定できます。デバイスは COM1 と COM2 の 2 つのシリアル ポートをサポートする場合があり、要件に応じて 2 つの COM1 または 2 つの COM2 として構成できます。シリアルデータは IP データに変換したり、IP データを介してシリアルデータに変換したり、有線または無線ネットワークを介して送信したりして、透過的なデータ伝送機能を実現できます。

手記:

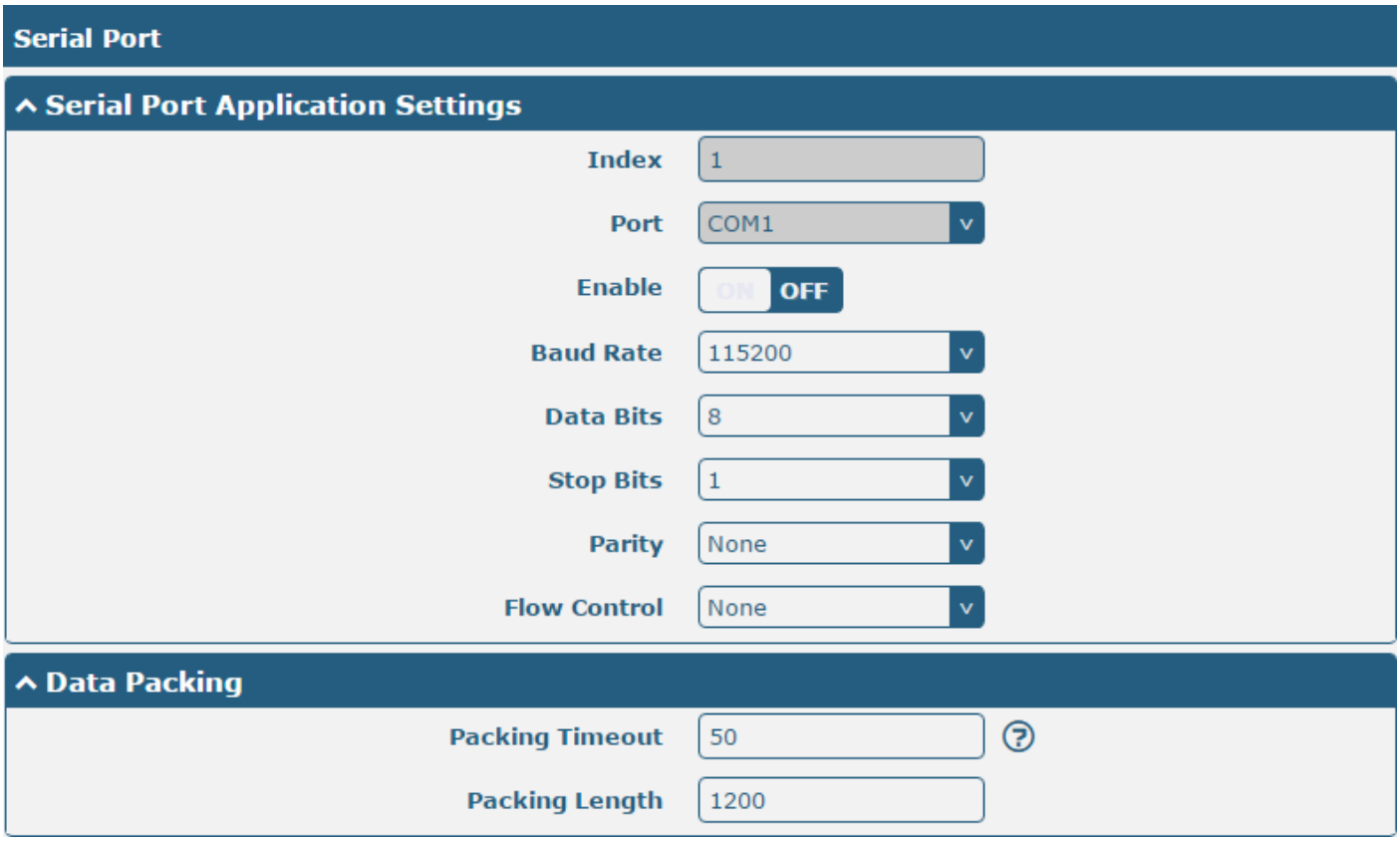
*1) R2010 および R3000-Quad のシリアルポートは、*RS232 または RS485 として構成できます。



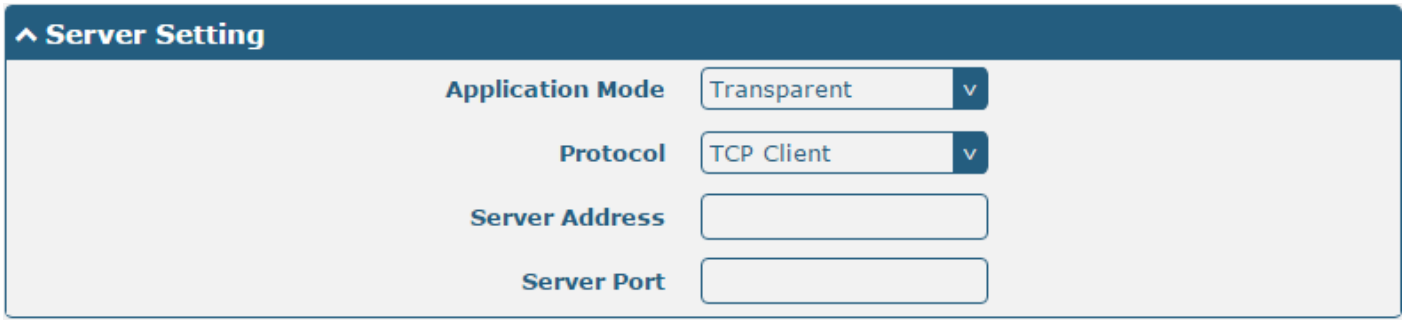
シリアルポート		
アイテム	説明	デフォルト
シリアルポートタイプ	RS485 または RS232 をサポート	RS485



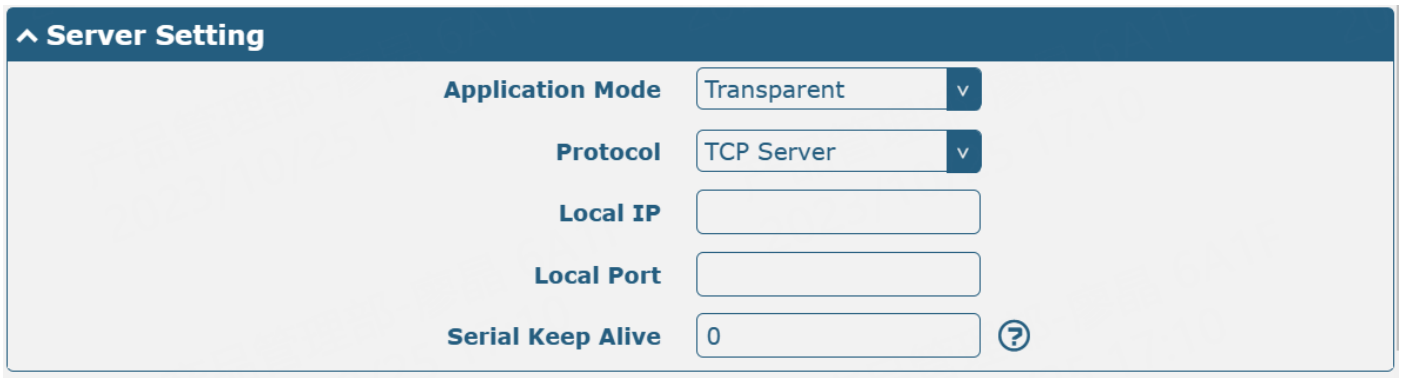
以下のように COM1 の右端のボタンをクリックします。



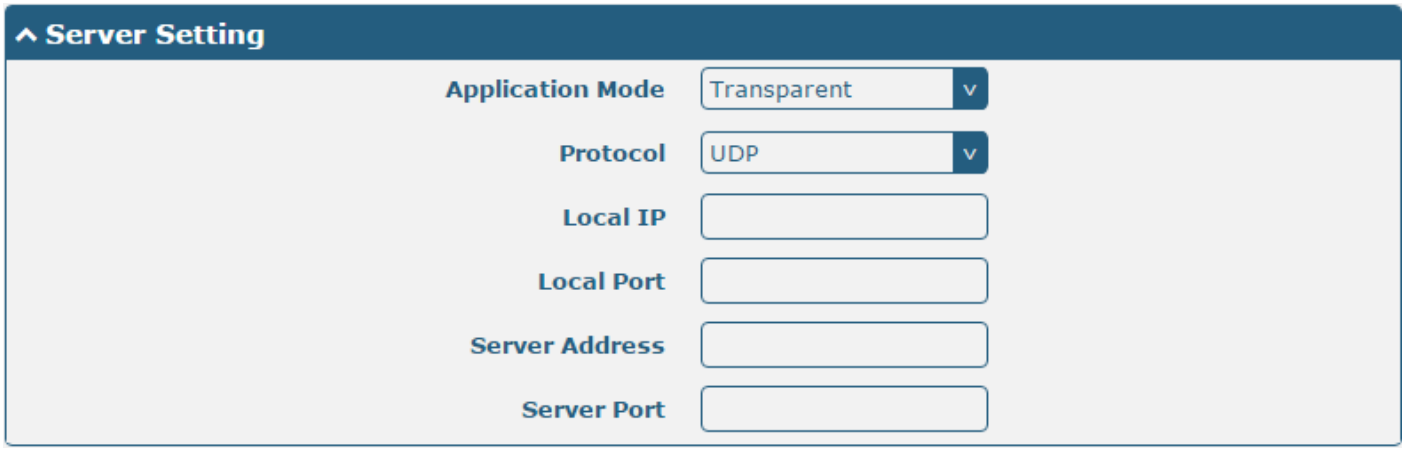
「サーバー設定」欄で、アプリケーションモードを「透過的」、プロトコルを「TCP クライアント」にすると、以下のようなウィンドウが表示されます。



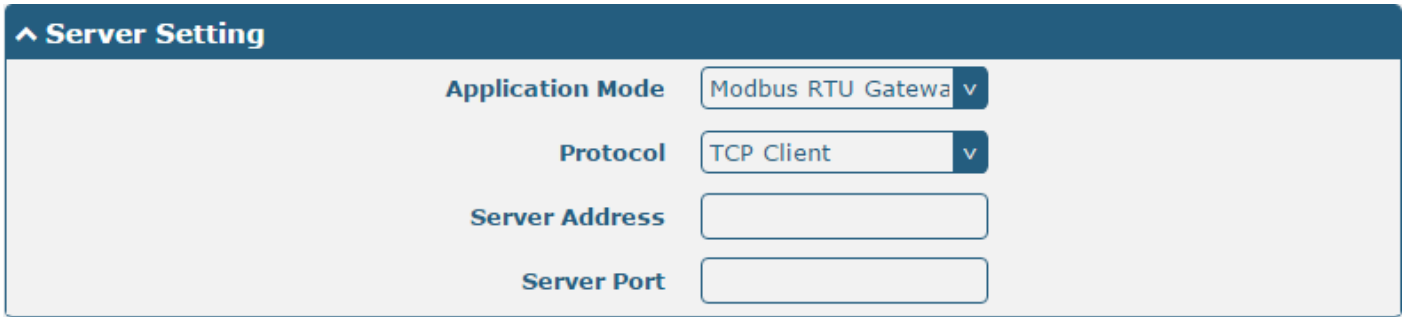
アプリケーションモードを「透過的」、プロトコルを「TCP サーバー」に設定した場合、ウィンドウは次のようになります。



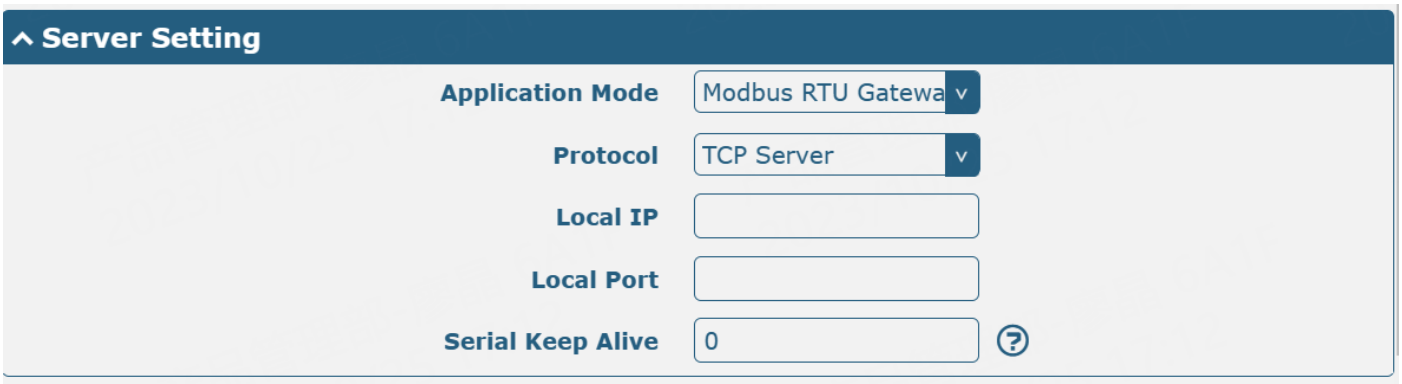
アプリケーションモードを「透過」、プロトコルを「UDP」に設定した場合、ウィンドウは次のようになります。



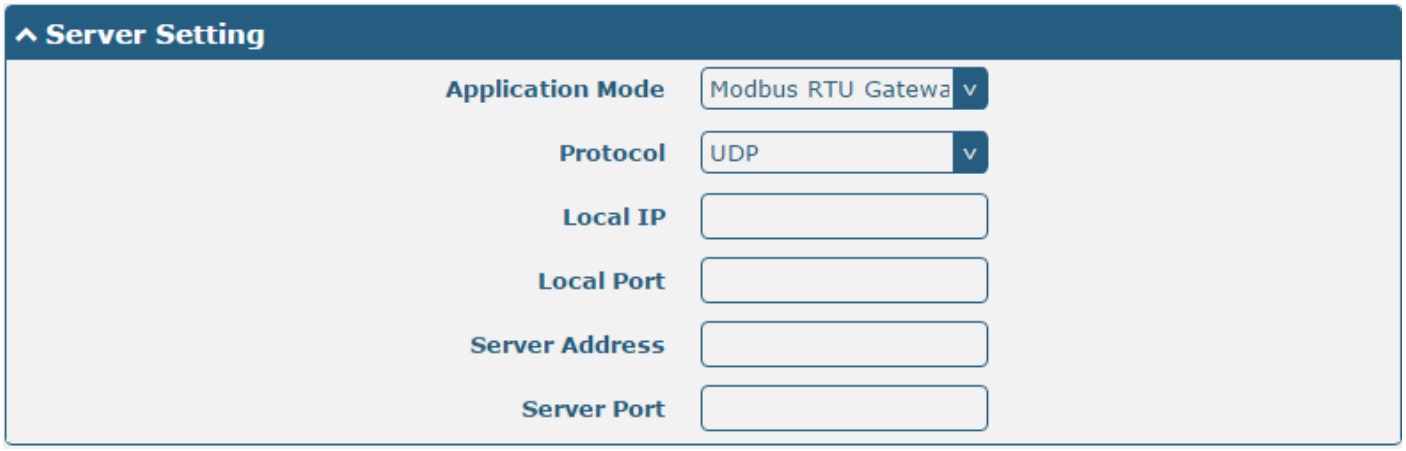
アプリケーションモードとして「Modbus RTU Gateway」を選択し、プロトコルとして「TCP Client」を選択した場合、ウィンドウは次のようになります。



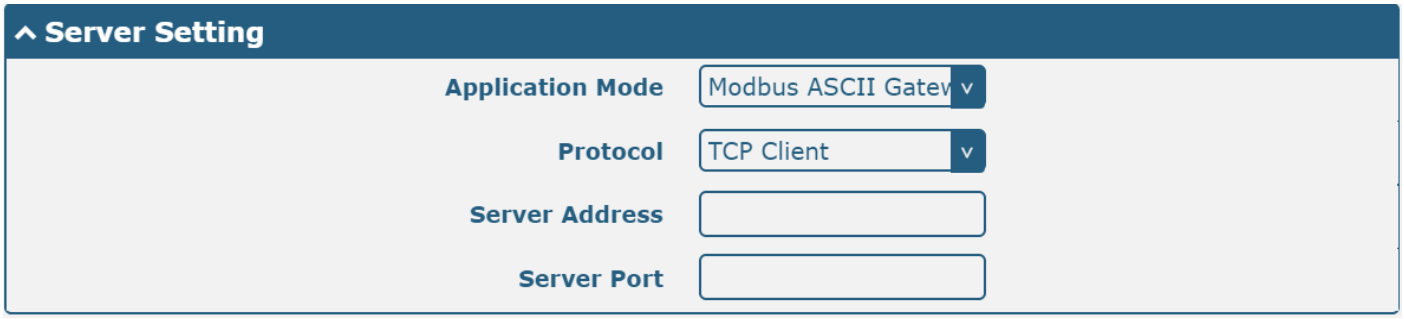
アプリケーションモードとして「Modbus RTU ゲートウェイ」を選択し、プロトコルとして「TCP サーバー」を選択した場合、ウィンドウは次のようになります。



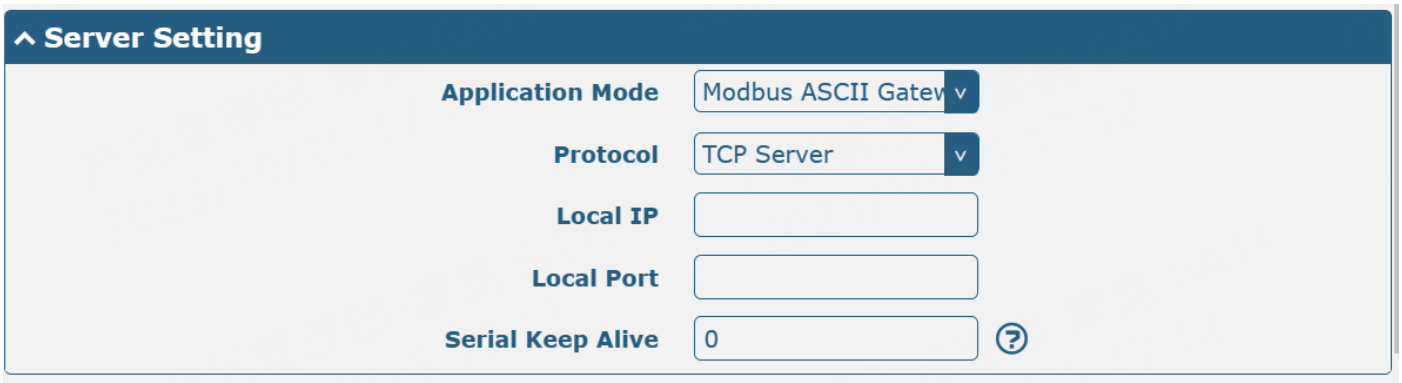
アプリケーションモードとして「Modbus RTU Gateway」を選択し、プロトコルとして「UDP」を選択した場合、ウィンドウは次のようになります。



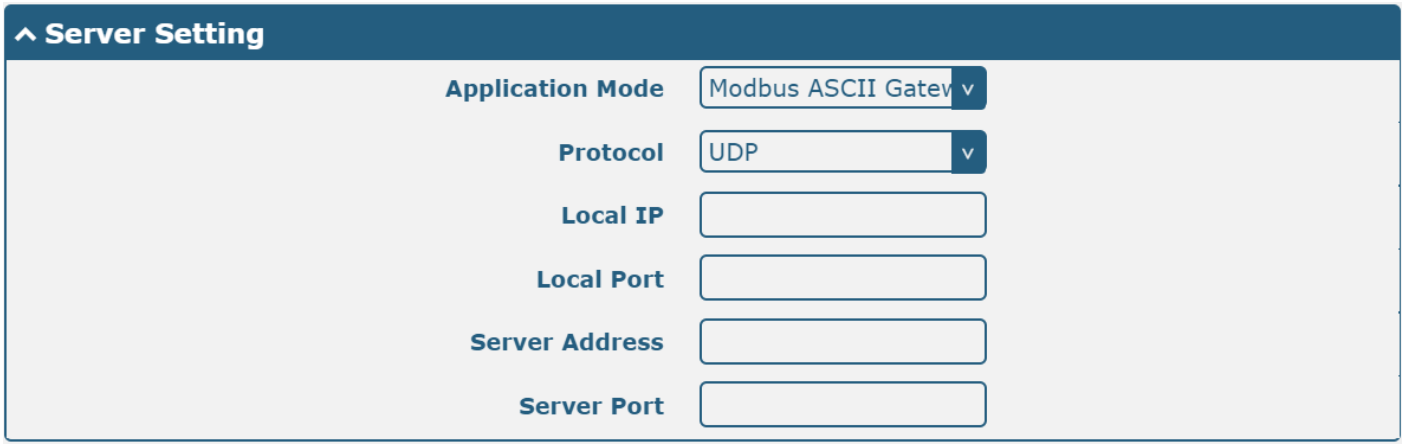
アプリケーションモードに「Modbus ASCII Gateway」、プロトコルに「TCP Client」を選択した場合、ウィンドウは次のようになります。



アプリケーションモードとして「Modbus ASCII ゲートウェイ」を選択し、プロトコルとして「TCP サーバー」を選択した場合、ウィンドウは次のようになります。



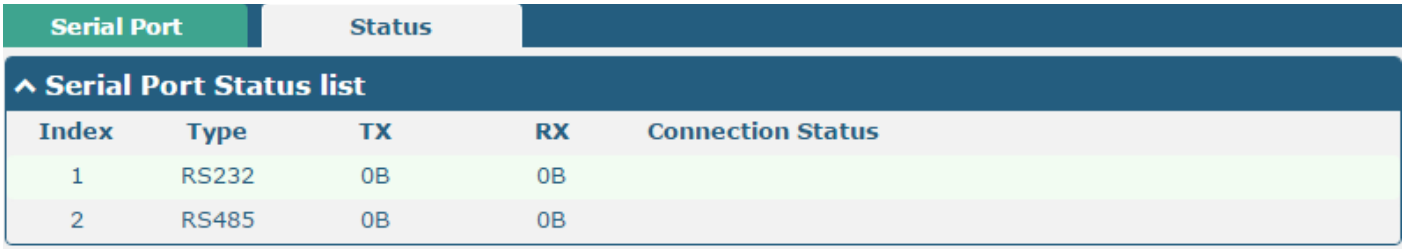
アプリケーションモードとして「Modbus ASCII ゲートウェイ」を選択し、プロトコルとして「UDP」を選択した場合、ウィンドウは次のようになります。



シリアルポート		
アイテム	説明	デフォルト
シリアルポートのアプリケーション設定		
インデックス	リストの序数を示します。	--
港	現在のシリアル名を読み取り専用で表示します。	COM1
エネーブル	トグルボタンをクリックして、このシリアルポートを有効/無効にします。ステータスが OFF の場合、シリアルポートは 使用できません。	オフ
ボー レート	「300」、「600」、「1200」、「2400」、「4800」、「9600」、「19200」、「38400」、「57600」、「115200」から選択します 。	115200
データ ビット	「7」または「8」から選択します。	8
ストップ ビット	「1」または「2」から選択します。	1
パリティ	「なし」、「奇数」、「 偶数」から選択します。	None
フロー制御	「なし」、「ソフトウェア」、「 ハードウェア」から選択します。	None
データパッキング		
パッキング タイムアウト	パッキング タイムアウトを設定します。 シリアルポートはバッファ内のデータをキューに入れ、フィールドのインターバルタイムアウトに達すると、セルラーWAN/イーサネット WAN/WLAN にデータを送信します。単位はミリ秒です。 *注:データは、データがフィールドのインターバルタイムアウトに達していない場合でも、パケット長で指定されたとおりに送信されます。*	50
パケット長	パケット長を設定します。 パケット長の設定は、送信前にシリアルポートバ	1200

シリアルポート		
アイテム	説明	デフォルト
	ッファに蓄積できるデータの最大量を指します。1 から 3000 バイトのパケット長を指定すると、バッファー内のデータは、指定された長さに達するとすぐに送信されます。	
サーバー設定		
アイテム	説明	デフォルト
アプリケーション モード	「トランスペアレント」、「Modbus RTU ゲートウェイ」、「Modbus ASCII ゲートウェイ」から選択します。 • トランスペアレント:デバイスはシリアルデータをトランスペアレントに送信します。 • Modbus RTU ゲートウェイ:デバイスは Modbus RTU データを Modbus TCP データに変換して送信し、その逆も同様です。 • Modbus ASCII ゲートウェイ:デバイスは Modbus ASCII データを Modbus TCP データに変換して送信し、その逆も同様です。	透明
プロトコル	「TCP クライアント」、「TCP サーバー」、または「UDP」を選択します。 • TCP クライアント:デバイスは TCP クライアントとして機能し、TCP サーバーへの TCP 接続を開始します。サーバーアドレスは、IP とドメイン名の両方をサポートします。 • TCP サーバ:デバイスは TCP サーバとして機能し、TCP クライアントからの接続要求をリッスンします。 • UDP:デバイスは UDP クライアントとして機能します。	TCP クライアント
サーバーアドレス	デバイスのシリアルポートから送信されたデータを受信するサーバーの アドレスを入力します 。IP アドレスまたはドメイン名が利用可能になります。	Null
サーバ ポート	シリアルデータの受信に使用するサーバーの指定ポートを入力します。	Null
シリアルキープアライブ	キープアライブ時間を入力し、値の範囲は 0~18000、単位:秒です。設定された時間内にシリアルポートまたは TCP データが検出されない場合、すべての TCP クライアント接続がアクティブに切断されます。0 は、この機能が有効になっていないことを意味します。	0
ローカル IP @ トランスペアレント	デバイスのインターネットポートに転送する デバイスの LAN IP を入力します。	Null
ローカル ポート @ トランスペアレント	デバイスの LAN IP のポートを入力します。	Null
ローカル IP @ Modbus	Modbus モードでローカル IP を入力します。	Null
ローカルポート@Modbus	Modbus モードでローカルポートに入ります。	Null

「ステータス」列をクリックして、現在のシリアルポートのステータスを表示します。

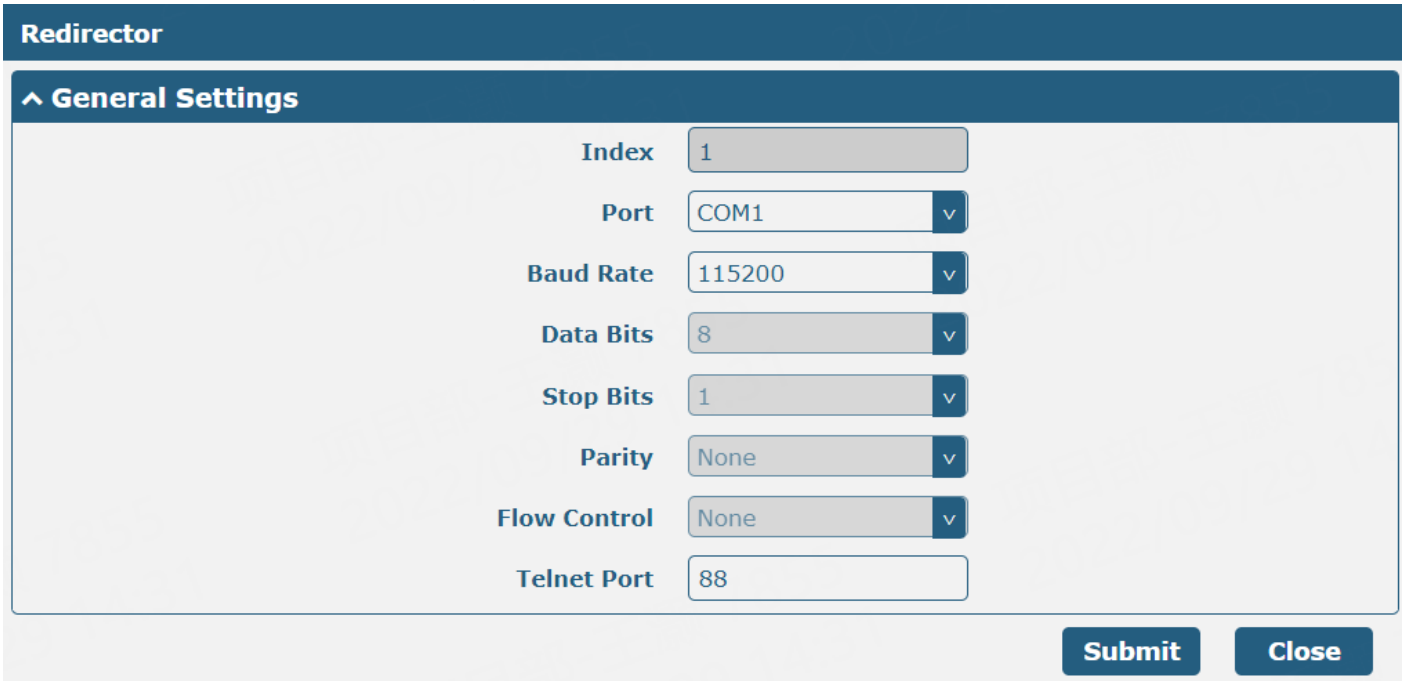


ステータス	
アイテム	**説明**
テキサス州	シリアルポートにデータを送信します。
RX の	シリアルポートからデータを受信しました。

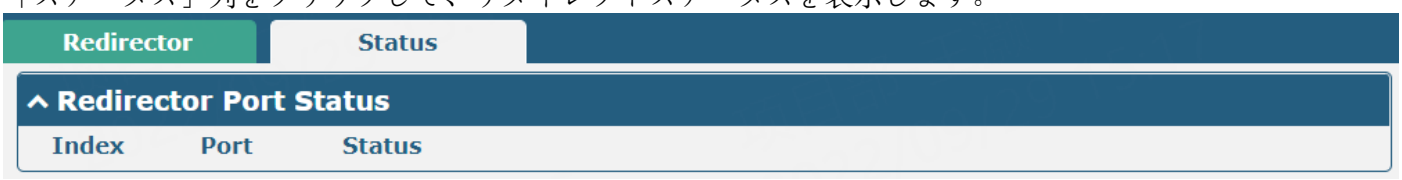
3.2.10 シリアル・リダイレクタ

このセクションでは、シリアルポートを Telnet にリダイレクトできます。 R1520 専用です。

「リダイレクタ」列をクリックして、シリアルリダイレクタを設定します。
+シリアルポートのデバイスに対応するシリアルポートとボーレートをクリックして選択し、リダイレクトする正しい Telnet ポートまたは入力します。



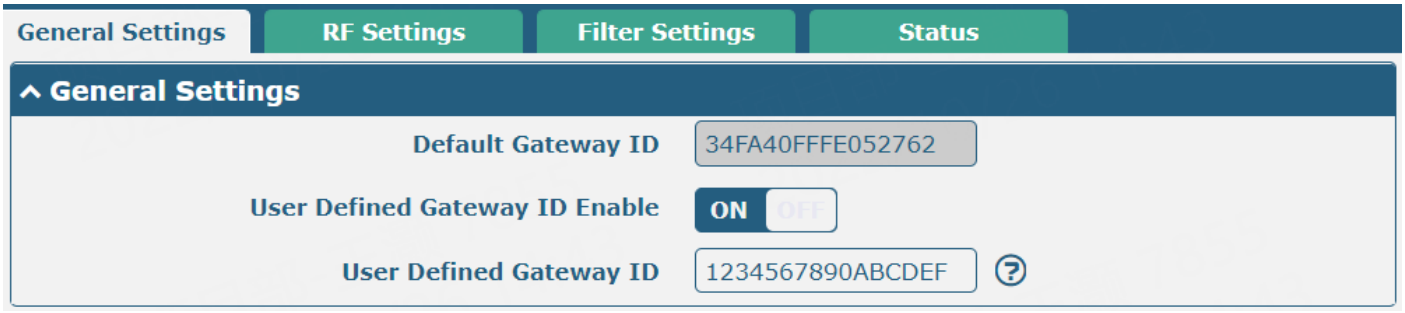
「ステータス」列をクリックして、リダイレクトステータスを表示します。



3.2.11 LoRa

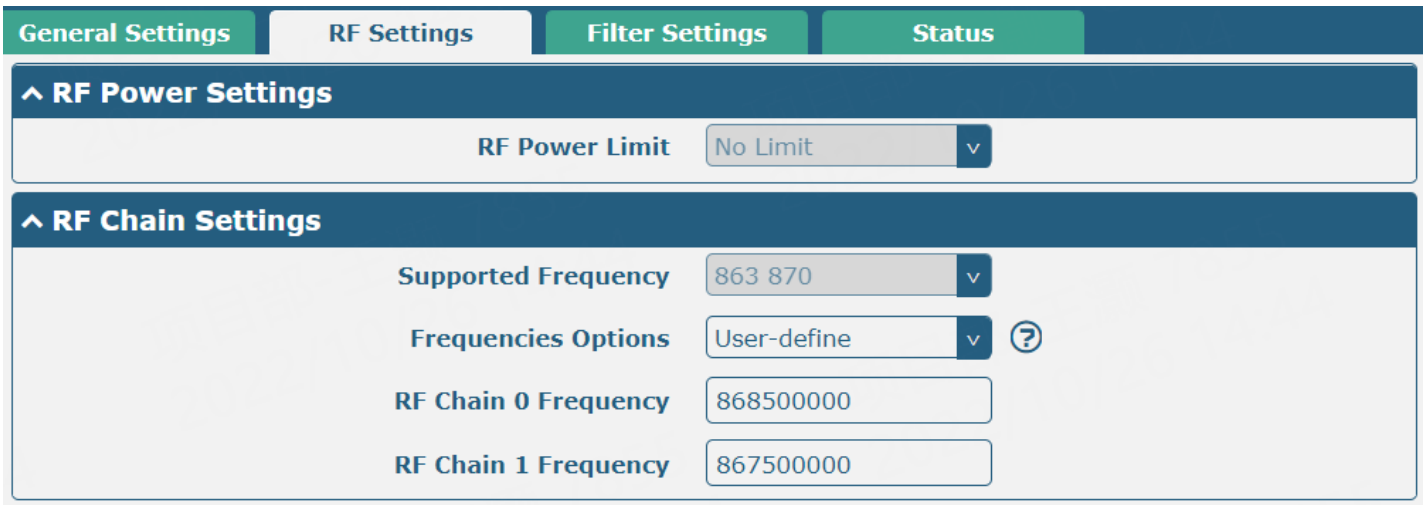
このセクションでは、 LoRaWAN パラメータを設定できます。 R3000-LG 専用です。

「一般設定」をクリックして、ゲートウェイ ID を設定します。 以下はその例です。



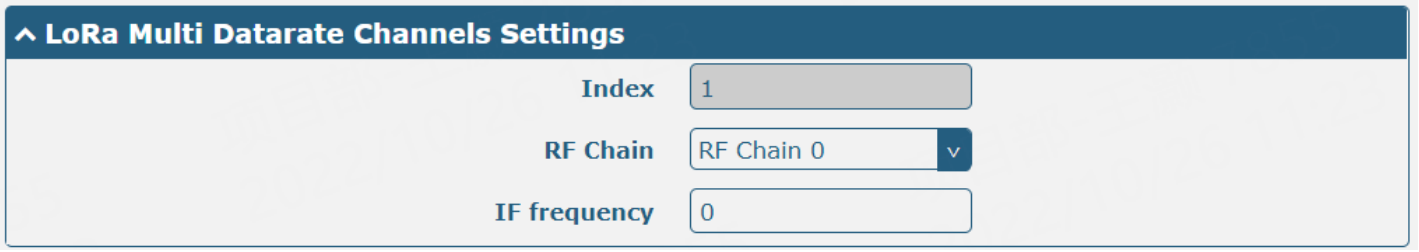
一般設定		
アイテム	説明	デフォルト
デフォルトゲートウェイ ID	デフォルトゲートウェイ ID を設定するか、一意の 64 ビットシーケンスでゲートウェイ ID を自分で定義できます。	Null
ユーザー定義ゲートウェイ ID の有効化 (User Defined Gateway ID Enable)	切り替えボタンをクリックして、このオプションを有効/無効にします。	オフ
ユーザー定義のゲートウェイ ID	ゲートウェイ ID を入力します。	Null

1) RF 設定

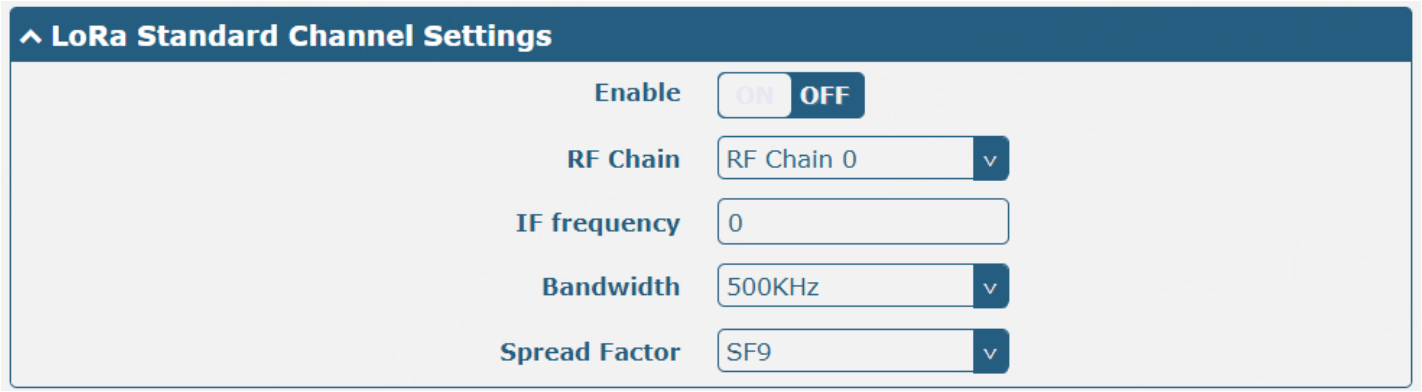


RF 設定		
アイテム	説明	デフォルト
RF 電力設定		
RF 電力制限	RF 電力制限を表示します。	制限なし
RF チェーン設定		
サポート頻度	サポート周波数を表示します。	863 870
周波数オプション	リンク周波数を設定します。 EU868: 868.1,868.3,868.5,867.1,867.3,867.5,867.7,867.9, STD 868.3 および FSK 868.8; RU868: RF チェーン 0:869000000、RF チェーン 1:864500000、 868.9,869.1,869.3,864.1,864.3,864.5,864.7,864.9; KZ868: RF チェーン 0:865300000、RF チェーン 1:867500000、 865.1,865.3,865.5,867.1,867.3,867.5,867.7,867.9.	ユーザー定義
RF チェーン 0 周波数	RF リンクの周波数を 0 に設定します。	868500000
RF チェーン 1 周波数	RF リンク 1 の周波数を設定します。	867500000

クリック+して、LoRa マルチ データレート チャネル設定を追加します。



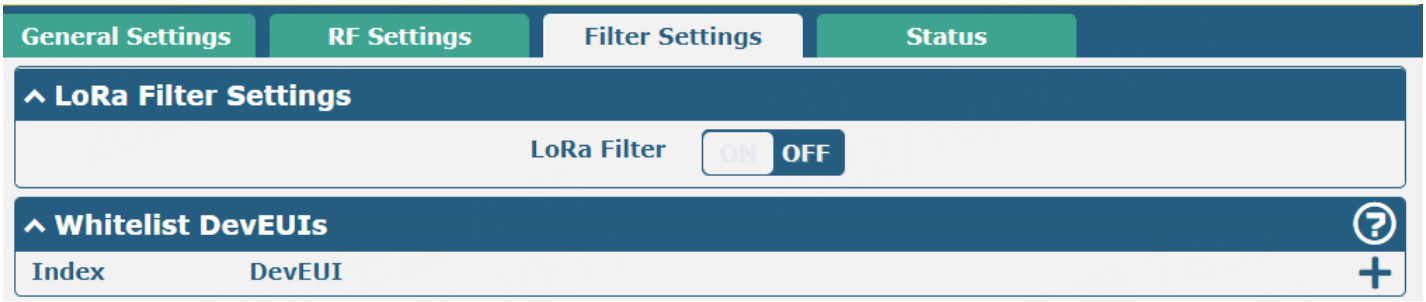
LoRa マルチ データレート チャンネル Settings@RF 設定		
アイテム	説明	デフォルト
インデックス	リストの序数を示します。	1
RF チェーン	[RF Chain] を選択します。	RF チェーン 0
IF 周波数	中心周波数を -500000-500000 の範囲で Hz 単位で入力します。特定のチャネルの中心周波数と RF リンク 0/1 の中心周波数との間のオフセット。	0



LoRa 標準チャンネル Settings@RF 設定		
アイテム	説明	デフォルト
エネーブル	切り替えボタンをクリックして、このオプションを有効/無効にします。	オフ
RF チェーン	[RF Chain] を選択します。	RF チェーン 0
IF 周波数	中心周波数を -500000-500000 の範囲で Hz 単位で入力します。特定のチャネルの中心周波数と RF リンク 0/1 の中心周波数との間のオフセット。	0
帯域幅	オプションの帯域幅を KHz 単位で選択します。	500KHz の
スプレッドファクター	オプションの拡散係数を入力します。拡散係数が高いと低いレートに相当し、拡散係数が低いと高いレートに対応します。	SF9 の

2) フィルタ設定

このセクションは、LoRa フィルター設定を変更するために使用されます。



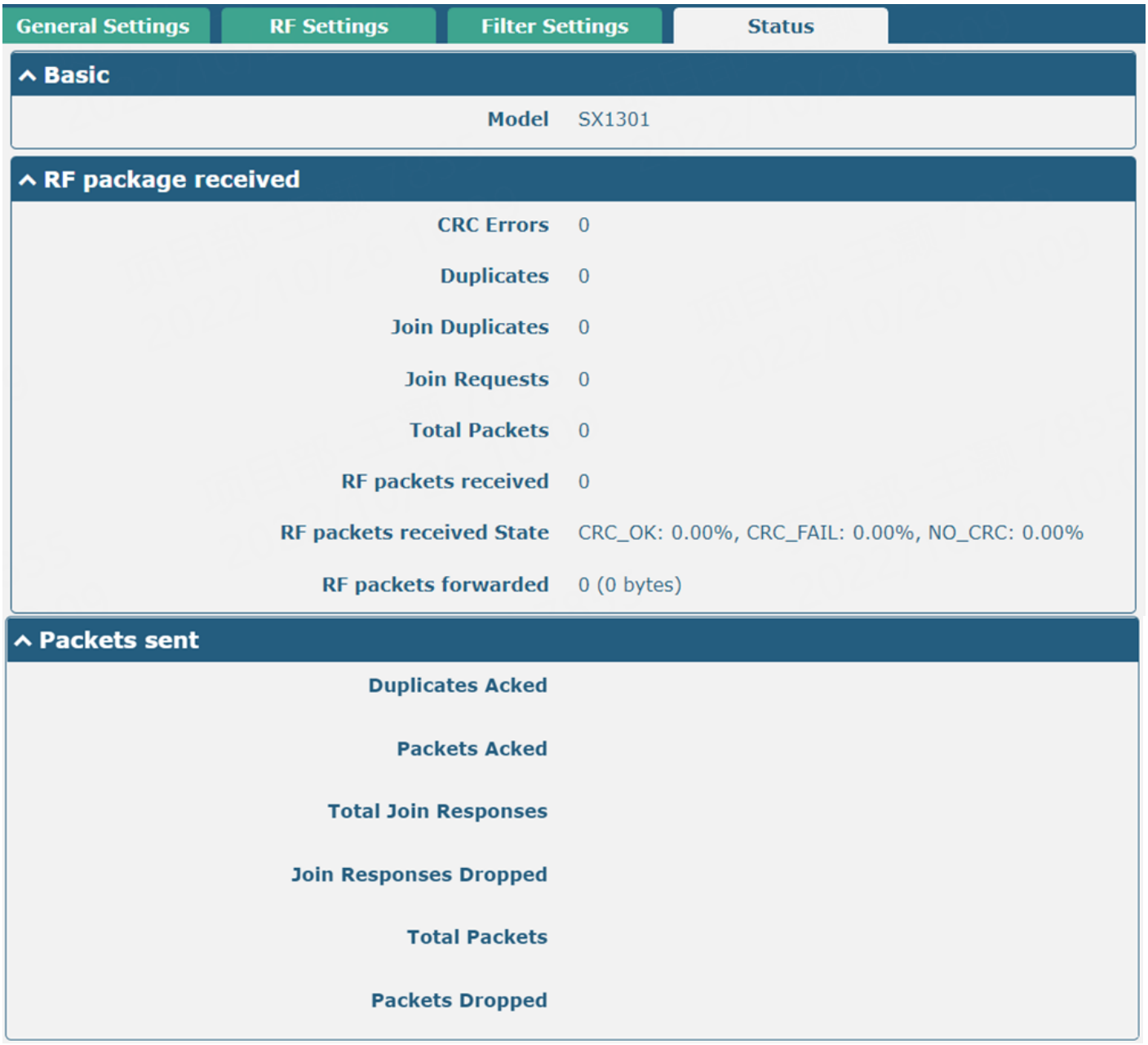
フィルタ設定		
アイテム	説明	デフォルト
LoRa フィルター	切り替えボタンをクリックして、このオプションを有効/無効にします。	オフ

クリック＋すると、ホワイトリストルールが追加されます。

ホワイトリスト Rules@Filter 設定		
アイテム	説明	デフォルト
インデックス	テーブル番号を表示します。	1
DevEUI の	デバイスに「DevEUI」と入力します。	Null

3) ステータス

このセクションでは、LoRa インターフェースのステータスを確認できます。



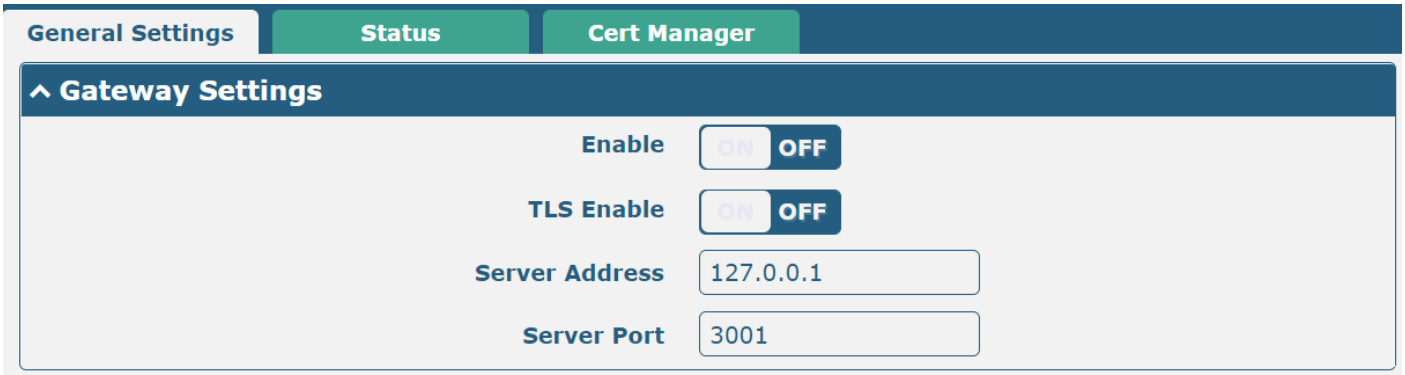
ステータス	
アイテム	説明
基本的な	
モデル	LoRa モジュールモデルを表示します。
受信パケット	
CRC エラー	エラーで受信した RF パケットの値を表示します。
重複	受信した重複 RF パケットの値を表示します 。
重複の結合	受信した重複した RF 参加要求パケットの値を表示します。
参加リクエスト	受信した RF 参加要求パケットの値を表示します。
合計パケット数	受信した RF パケットの値を表示します。
受信した RF パケット(RF Packets Received)	ノードからゲートウェイへのデータパケットの数を表示します。
RF パケット受信状態(RF Packets Received State)	RF パケットの受信状態を表示します。 • CRC_OK:CRC 検証の割合 • CRC_Fail:CRC 検証の失敗率 • NO_CRC:CRC のない異常パケットの割合
送信されたパケット	
質問された重複	送信された重複 RF 応答パケットの値を表示します。

ステータス	
アイテム	**説明**
要求されたパケット(Packets Asked)	送信された RF 応答パケットの値を表示します。
合計結合応答数	送信された重複 RF 結合応答パケットの値を表示します。
Join Responses Dropped	失敗した RF join 応答パケットの値を表示します。
合計パケット数	送信された RF パケットの値を表示します。
ドロップされたパケット(Packets Dropped)	RF ドロップされたパケットの値を表示します。
中心周波数	
RF チェーン 0 周波数	LoRa チャンネル 0 の中心周波数
RF チェーン 1 周波数	LoRa チャンネル 1 の中心周波数
LoRa マルチデータレートチャンネル	
RF チェーン	LoRa チャンネルのインデックス。
IF 周波数	LoRa チャネルの IF 周波数
LoRa 標準チャンネル	
RF チェーン	LoRa 標準チャンネルのインデックス。
IF 周波数	LoRa 標準チャンネルの IF 周波数
帯域幅	LoRa 標準チャネルの帯域幅。
スプレッドファクター	LoRa 標準チャネルのスプレッドファクター。
FSK 標準チャンネル	
RF チェーン	FSK 標準チャンネルのインデックス。
IF 周波数	FSK 標準チャンネルの IF 周波数
帯域幅	FSK 標準チャネルの帯域幅。
データレート	FSK 標準チャンネルのデータレート

3.3 パケットフォワーダ

3.3.1 ジェネラルステーション

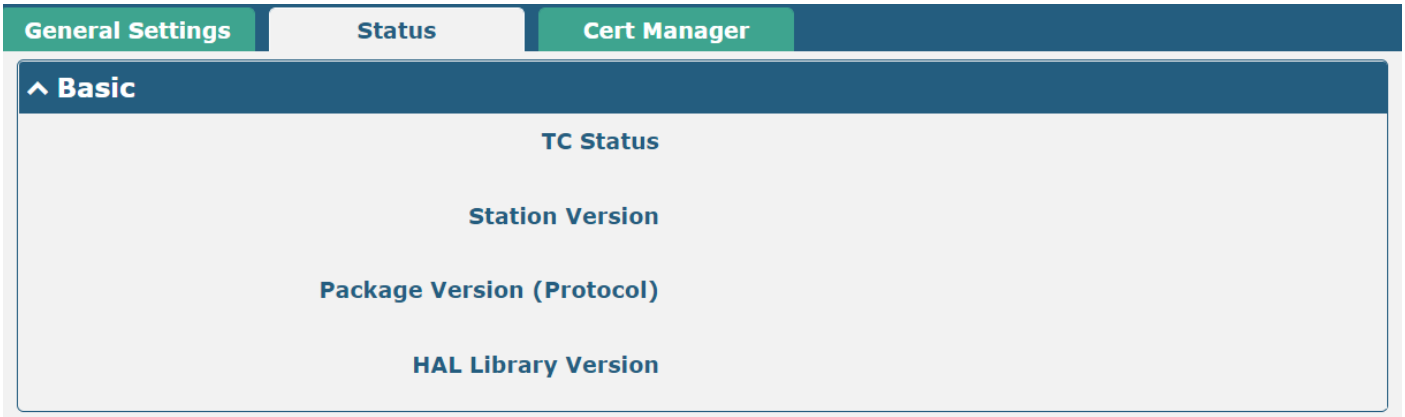
1) 一般設定



一般設定		
ゲートウェイ設定		
アイテム	説明	デフォルト
エネーブル	アプリケーションを有効にします。	オフ
TLS 有効	TLS 暗号化送信を有効にします。	オフ
サーバーアドレス	サーバーアドレス(例:127.0.0.1)	
サーバ ポート	サーバーのポート 番号。	

2) ステータス

このセクションでは、 基本ステーションのステータスを表示できます。

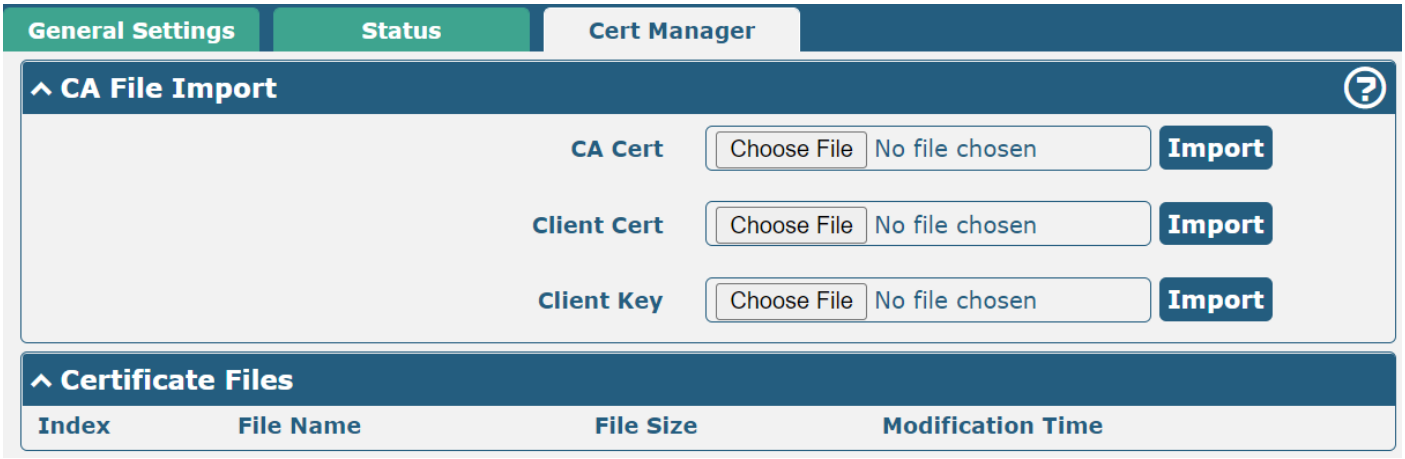


アイテム	説明
TC ステータス	プラットフォームの接続状態。
ステーション バージョン	アプリケーションのバージョン。

パッケージ バージョン (プロトコル)	アプリケーション パッケージのバージョン。
HAL ライブラリのバージョン	LoRaWAN HAL ライブラリのバージョン。

3) 証明書マネージャー

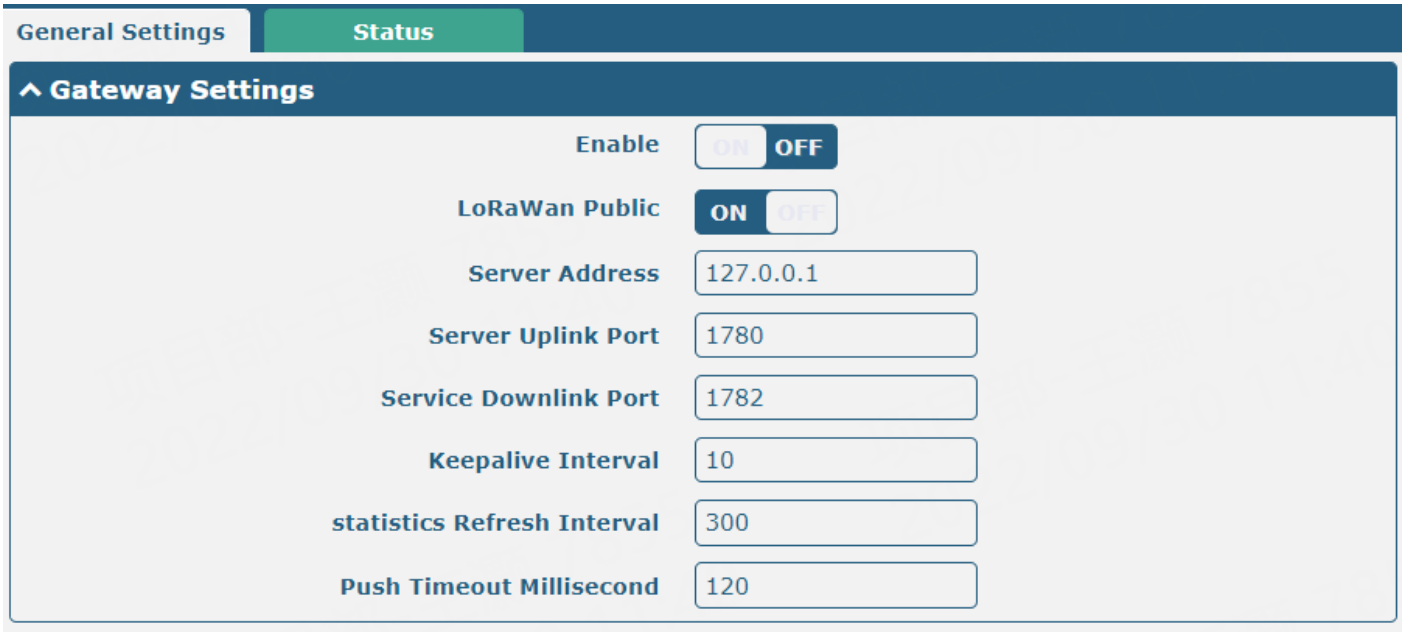
このセクションでは、証明書を表示およびインポートできます。



証明書マネージャー		
CA ファイルのインポート		
アイテム	説明	デフォルト
CA 証明書	サーバー証明書。	Null
クライアント証明書	証明書は、サーバーによってクライアントに割り当てられます。	Null
クライアントキー	サーバーは、証明書の秘密鍵をクライアントに割り当てます。	Null

3.3.2 Semtech UDP フォワーダー

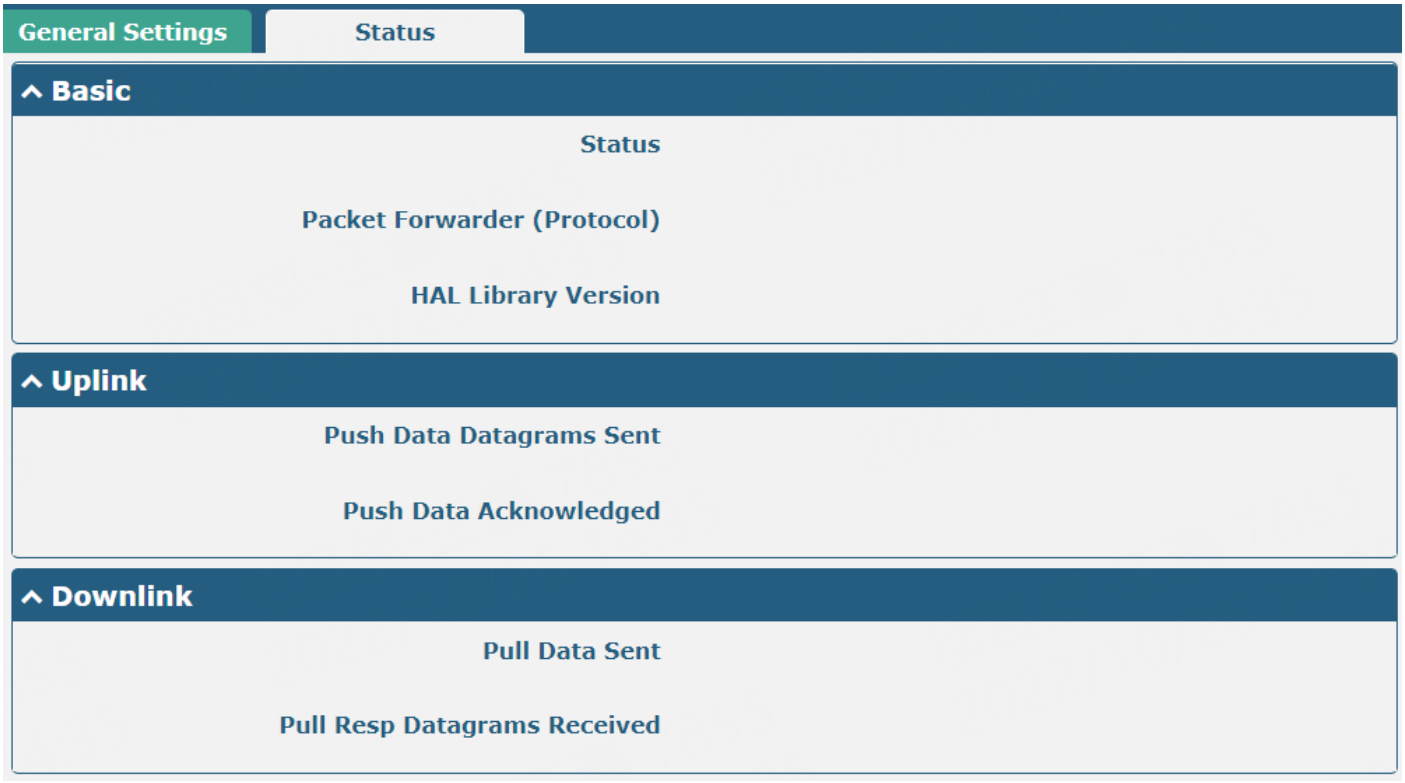
1) 一般設定



一般設定		
ゲートウェイ設定		
アイテム	説明	デフォルト
エネーブル	切り替えボタンをクリックして、このオプションを有効/無効にします。	オフ
LoRaWan パブリック	切り替えボタンをクリックして、このオプションを有効/無効にします。	オン
サーバーアドレス	サーバーアドレスを設定します。	127.0.0.1
サーバアップリンクポート	UDP アップリンク接続ポート。	1780
サービスダウンリンクポート	UDP ダウンリンク接続ポート。	1782
キープアライブインターバル(Keepalive Interval)	ダウンリンクデータを取得する時間インターバル。	10
統計情報の更新インターバル	統計インターバル、USI 更新インターバル。	300
プッシュタイムアウト(ミリ秒)	アップリンクデータのタイムアウト。	120

2) ステータス

このセクションでは、Semtech UDP フォワーダのステータスを表示できます。



ステータス	
アイテム	説明
基本的な	
ステータス	ゲートウェイの LoRaWAN ステータスを表示します。
Packet Forwarder (プロトコル)	パケットフォワーダーの version を表示します。
HAL ライブラリのバージョン	ゲートウェイ内の LoRaWAN チップセットのドライババージョンを表示します。
アップリンク	
転送された RF パケット	CRC が検証したパケットは、ゲートウェイからサーバーに送信されます。
送信されたプッシュ・データ・データグラム	ゲートウェイからサーバに送信されたパケットの総量(転送された RF パケットと統計パケットを含む)。
確認されたデータのプッシュ	送信されたプッシュデータデータグラムのうち、確認されたパケットの割合:
ダウンリンク	
送信されたデータのプル	サーバに送信されたキープアライブ パケットの数と、サーバからのキープアライブ パケットに関する確認応答パケットの割合を表示します。
受信したデータグラムのプル(Pull Resp Datagrams Received)	サーバからゲートウェイに送信されるパケット数とサイズを表示します。

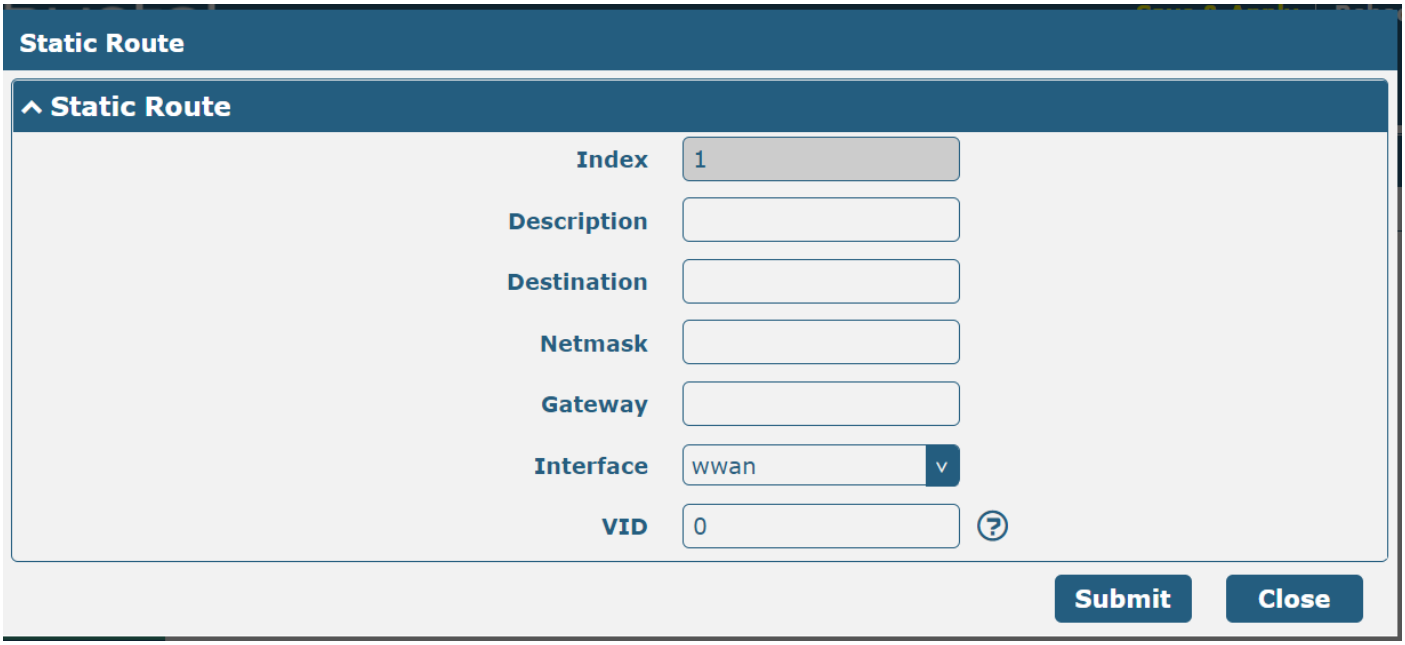
3.4 ネットワーク

3.4.1 ルート

このセクションでは、スタティックルートを設定できます. スタティック ルートは、 ルーティング これは、デバイスが動的ルーティングトラフィックからの情報ではなく、手動で設定されたルーティングエントリを使用する場合に発生します。 ルート情報プロトコル (RIP)は広く利用されています ある 小規模なネットワーク ある 安定した使用率。 最短パスを最初に開く (OSPF)は、単一の自律システム内のデバイスになり、 ある 大規模なネットワーク。

1) スタティック ルート

クリック + すると、スタティック ルートが追加されます。最大数は **20 です**。



スタティック ルート		
アイテム	説明	デフォルト
インデックス	リストの序数を示します。	--
説明	このスタティック ルートの説明を入力します。	Null
行き先	宛先ホストまたは宛先ネットワークの IP アドレスを入力します。	Null
ネットマスク/プレフィックス長 (Netmask/Prefix Length)	宛先ホストまたは宛先ネットワークのネットマスクを入力します。	Null
デバイス	宛先のデバイスを定義します。	Null

スタティックルート		
アイテム	説明	デフォルト
インターフェイス	設定するリンクの対応するポートを選択します。	WWAN(ワン)
VID の	0 は VLAN ID がないことを意味します。	0

2) ステータス

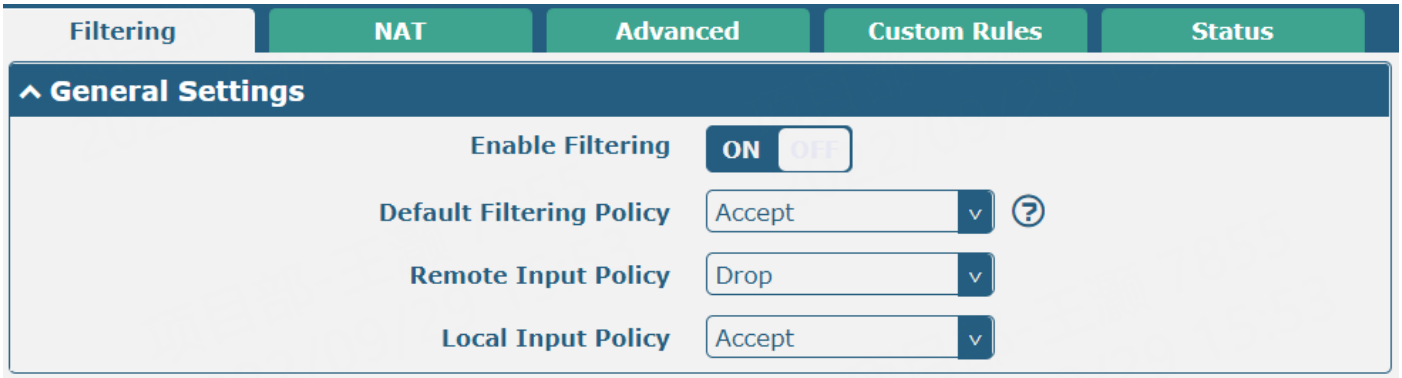
このウィンドウでは、デバイスのステータスを表示できます。

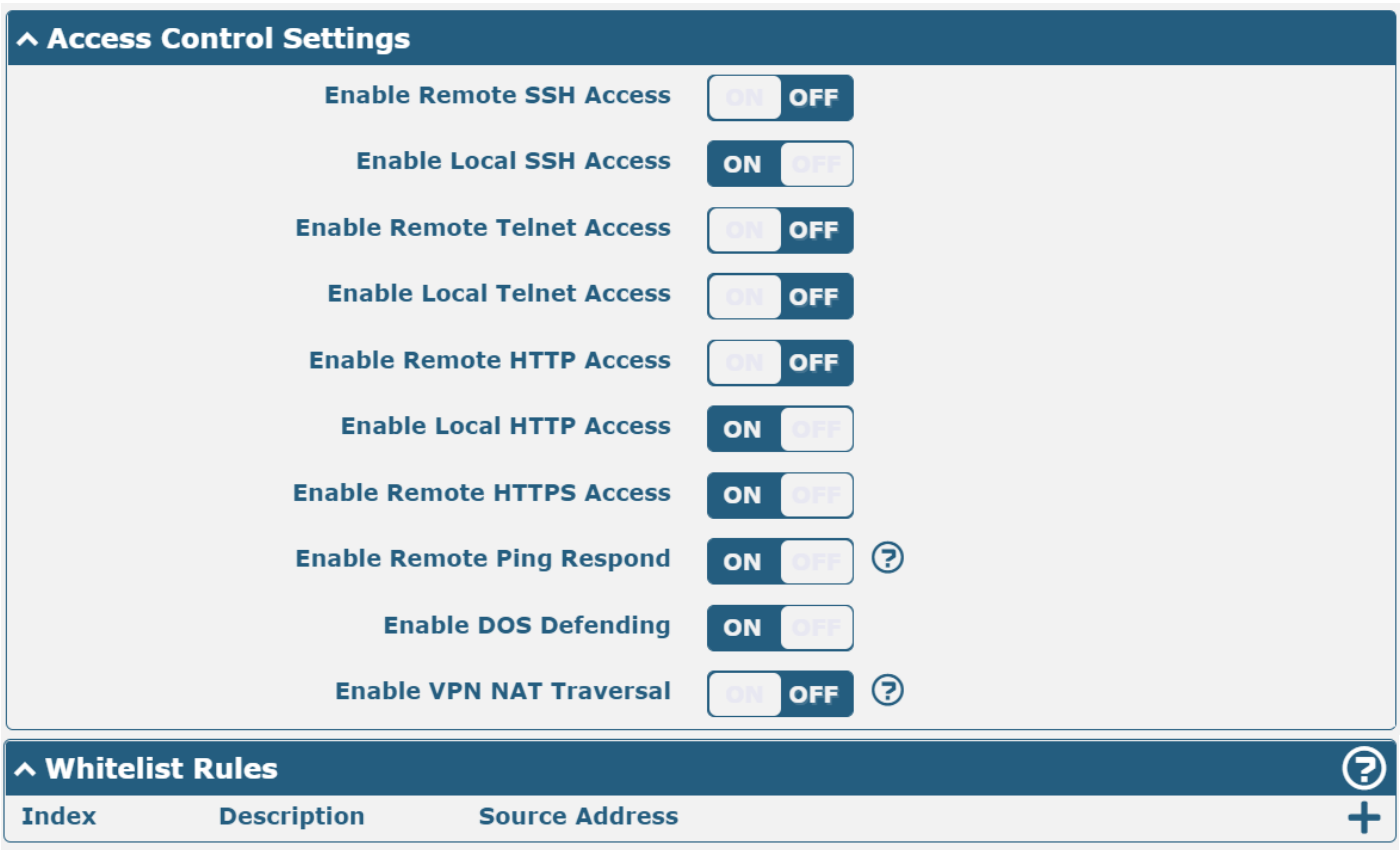
Route Table

Index	Destination	Netmask	Gateway	Interface	Metric
1	0.0.0.0	0.0.0.0	10.21.8.149	wwan	0
2	10.21.8.148	255.255.255.252	0.0.0.0	wwan	0
3	192.168.0.0	255.255.255.0	0.0.0.0	lan0	0

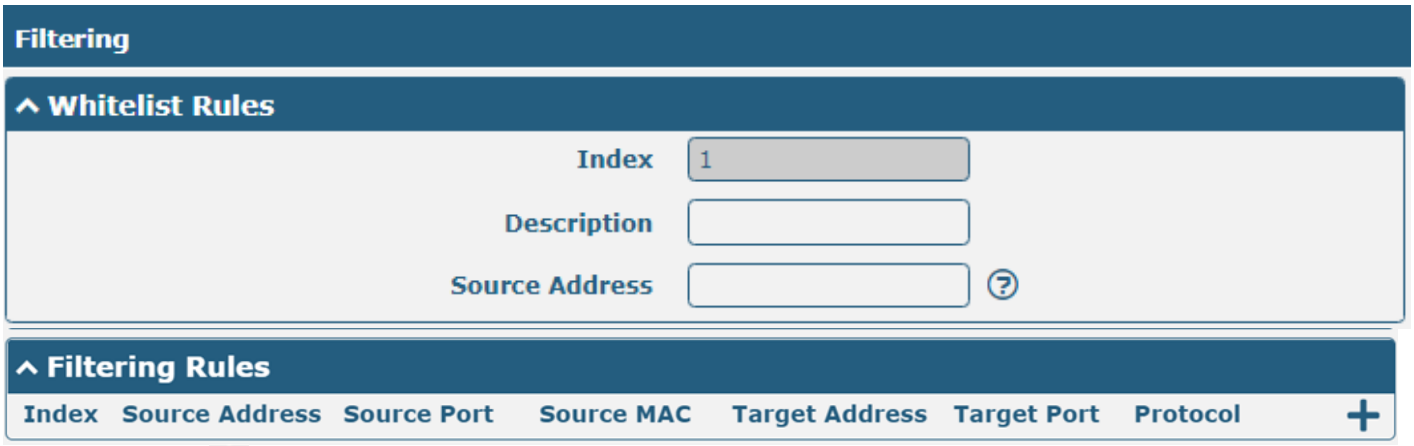
3.4.2 ファイアウォール

このセクションでは、ファイアウォールとそれに関連するパラメータ(フィルタリング、NAT、 IPset など)を設定できます。 フィルタリングルールを使用して、特定のユーザーまたはポートによるデバイスへのアクセスを許可またはブロックできます。 「**ネットワーク>ファイアウォール>フィルター**」をクリックします。次の情報が表示されます。

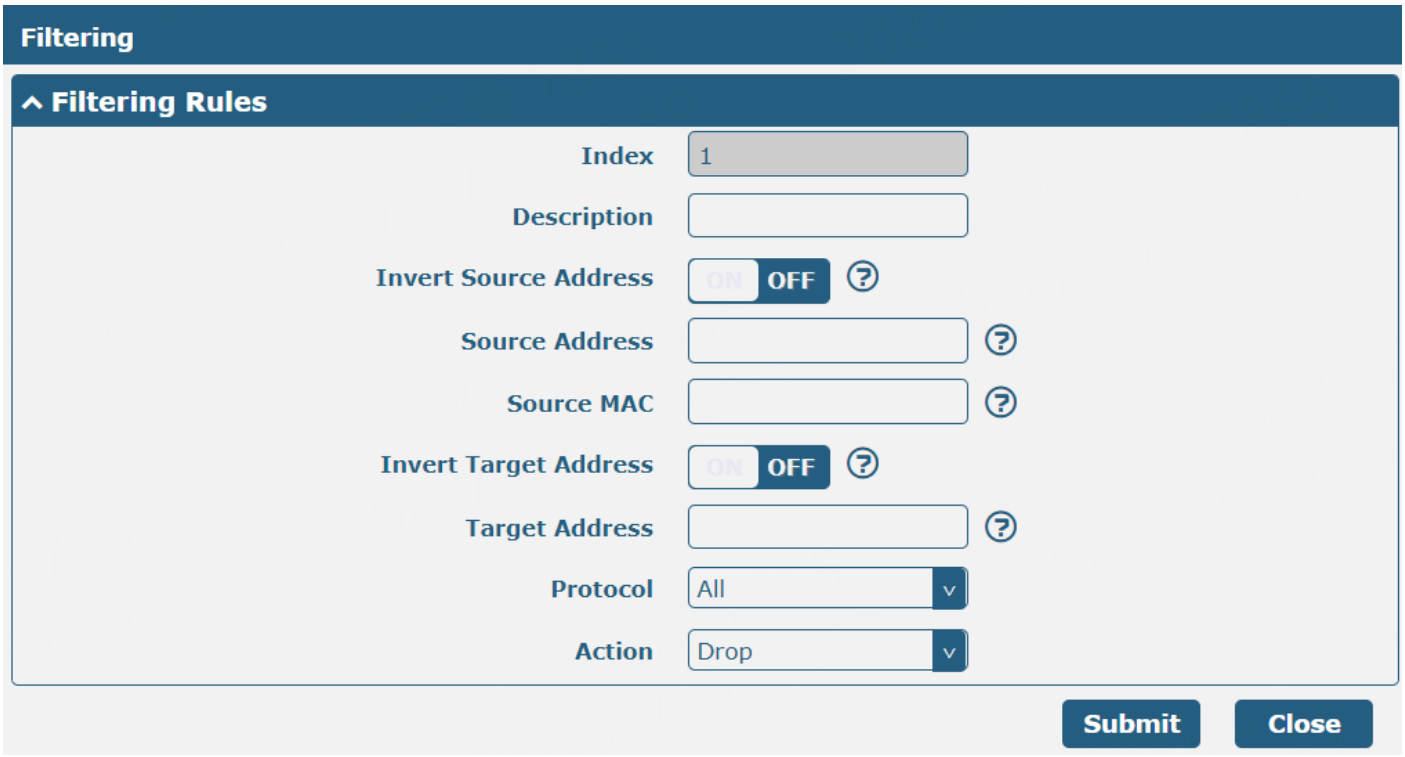




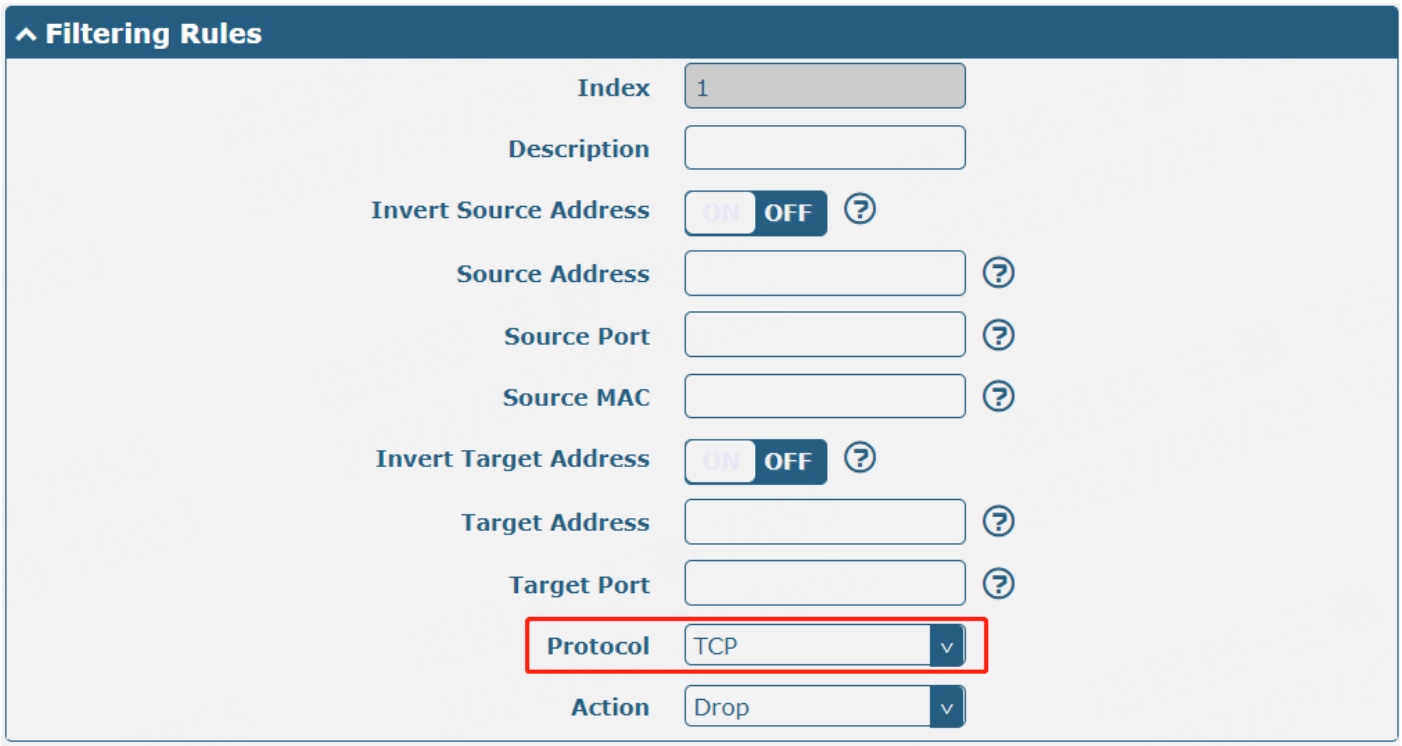
クリック + すると、ホワイトリストルールが追加されます。



クリックすると + 、フィルタリングルールが追加されます。最大数は 50 です。 デフォルトの「すべて」またはプロトコルとして「ICMP」を選択した場合、ウィンドウは次のように表示されます。 ここでは、「すべて」を例 にとります。


Filtering
Filtering Rules
Index
1
Description
Invert Source Address
ON
OFF
Source Address
Source MAC
Invert Target Address
ON
OFF
Target Address
Protocol
All
Action
Drop
Submit
Close

プロトコルとして「TCP」、「UDP」、または「TCP-UDP」を選択すると、ウィンドウが下に表示されます。ここで「TCP」は一例です。



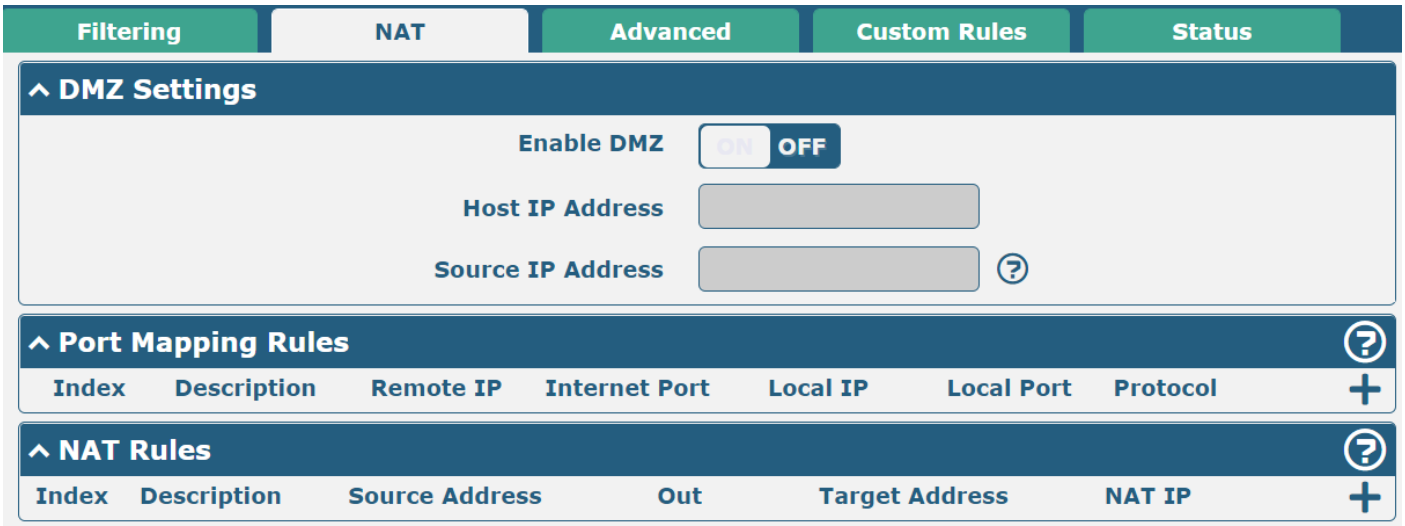
フィルタリング		
アイテム	説明	デフォルト
一般設定		
フィルタリングを有効にする	切り替えボタンをクリックして、フィルタリングオプションを有効/無効にします。	オン
デフォルトのフィルタリングポリシー	「Accept」または「Drop」 から選択します。 • [承認(Accept)]:デバイスは、ドロップ フィルタ リストに適合するホストを除くすべての接続要求を受け入れ ます • ドロップ:デバイスは、受け入れられたフィルタリストに適合するホストを除くすべての接続要求をドロップします	受け入れる
リモート入力ポリシー	「Accept」または「Drop」 から選択します。 • [承認(Accept)]:デバイスは、ドロップ フィルタ リストに適合するホストを除くすべての接続要求を受け入れ ます • ドロップ:デバイスは、受け入れられたフィルタリストに適合するホストを除くすべての接続要求をドロップします • 拒否: デバイスは、受け入れられたフィルター リストに適合するホストを除くすべての接続要求を拒否し、拒否 (終了) パケットが返されます	落とす
ローカル入力ポリシー	「Accept」または「Drop」 から選択します。 • [承認(Accept)]:デバイスは、ドロップ フィルタ リストに適合するホストを除くすべての接続要求を受け入れ ます • ドロップ:デバイスは、受け入れられたフィルタリストに適合するホストを除くすべての接続要求をドロップします • 拒否: デバイスは、受け入れられたフィルター リストに適合するホストを除くすべての接続要求を拒否し、拒否 (終了) パケットが返されます	受け入れる

フィルタリング		
アイテム	説明	デフォルト
アクセス制御設定		
リモート SSH アクセスの有効化	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、インターネットユーザーは SSH 経由でデバイスにリモートでアクセスできます。	オフ
ローカル SSH アクセスの有効化	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、LAN ユーザーは SSH 経由でローカルにデバイスにアクセスできます。	オン
リモート Telnet アクセスの有効化	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、インターネットユーザーは Telnet を介してデバイスにリモートでアクセスできます。	オフ
ローカル Telnet アクセスの有効化	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、LAN ユーザは Telnet 経由でローカルでデバイスにアクセスできます。	オフ
リモート HTTP アクセスの有効化	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、インターネットユーザーは HTTP 経由でデバイスにリモートでアクセスできます。	オフ
ローカル HTTP アクセスの有効化	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、LAN ユーザーは HTTP 経由でローカルでデバイスにアクセスできます。	オン
リモート HTTPS アクセスを有効にする	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、インターネットユーザーは HTTPS 経由でデバイスにリモートでアクセスできます。	オン
リモート Ping 応答を有効にする	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、デバイスはインターネット上の他のホストからの Ping 要求に応答します。	オン
DOS 防御を有効にする	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、デバイスは DOS を防御します。 DoS 攻撃とは、マシンやネットワークリソースを意図したユーザーが利用できないようにしようとする試みです。	オン
VPN_NAT トラバーサルを有効にする	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、GRE/L2TP/PPTP VPN パケットの NAT トラバーサルが有効になります。	オフ
ホワイトリストルール		
インデックス	リストの序数を示します。	--
説明	このホワイトリストルールの説明を入力します。	Null
送信元アドレス	アクセスの発信元を指定し、その送信元アドレスを入力します。	Null
フィルタリングルール		
インデックス	リストの序数を示します。	--
説明	このフィルタリングルールの説明を入力します。	Null
送信元アドレスの反転	ユーザー入力のソースアドレスを反転できるようにする	オフ
送信元アドレス	アクセスの発信元を指定し、その送信元アドレスを入力します。	Null
送信元ポート	アクセスの発信元を指定し、その送信元ポートを入力します。	Null
送信元 MAC	アクセス発信元を指定し、その送信元 MAC アドレスを入力します。	Null

フィルタリング		
アイテム	説明	デフォルト
ターゲット・アドレスの反転	ユーザー入力のターゲットアドレスを反転できるようにする	オフ
ターゲット・アドレス	アクセスの発信元がアクセスするターゲットアドレスを入力します。	Null
ターゲット・ポート	アクセスの発信元がアクセスするターゲット・ポートを入力します。	Null
プロトコル	「すべて」、「TCP」、「UDP」、「ICMP」、「ICMPv6」、「TCP-UDP」から選択します。 *注: 使用するアプリケーションのプロトコルがわからない場合は、「すべて」を選択することをお勧めします。*	すべての
アクション	「Accept」または「Drop」から選択します。 • [Accept]:デフォルトのフィルタリングポリシーが ドロップされると、デバイスは、この受け入れフィルタリングリストに適合するホストを除くすべての接続要求をドロップします。 • ドロップ:デフォルトのフィルタリングポリシーが受け入れられると、デバイスは、このドロップフィルタリングリストに適合するホストを除くすべての接続要求を受け入れます。	落とす

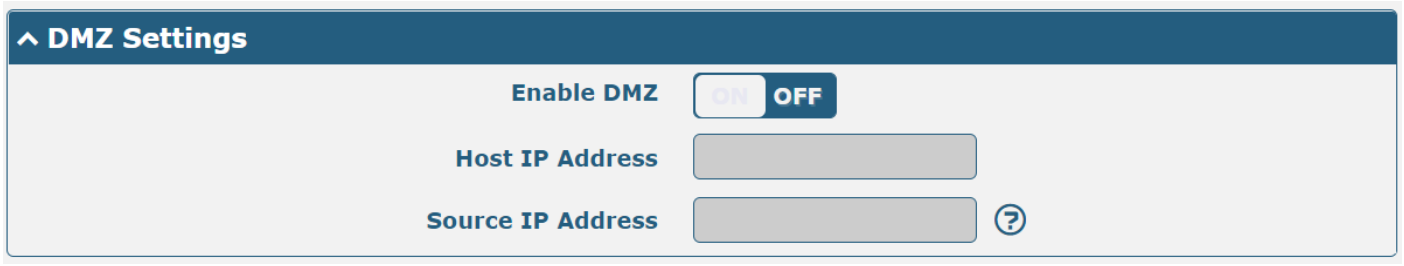
1) NAT

このセクションでは、DMZ、ポートマッピング、NAT などの NAT 関連機能を設定できます。



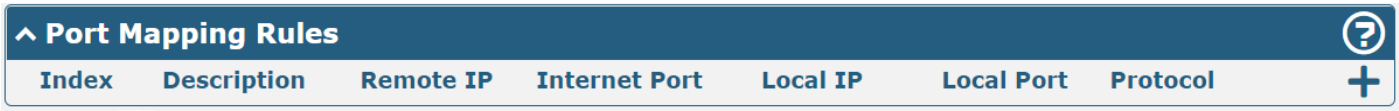
DMZ(非武装地帯)は、非武装地帯とも呼ばれます。これは、ファイアウォールをインストールした後、外部ネットワークにアクセスするユーザーが内部ネットワークサーバーにアクセスできないという問題を解決するために設定された、セキュリティで保護されていないシステムとセキュリティシステムの間のバッファーです。DMZ ホストは、占有され転送されるポートを除くすべてのポートが指定されたアドレスに対して開かれているイントラネット ホストです。

「**ネットワーク>ファイアウォール>NAT>DMZ**」をクリックします。次の情報が表示されます。

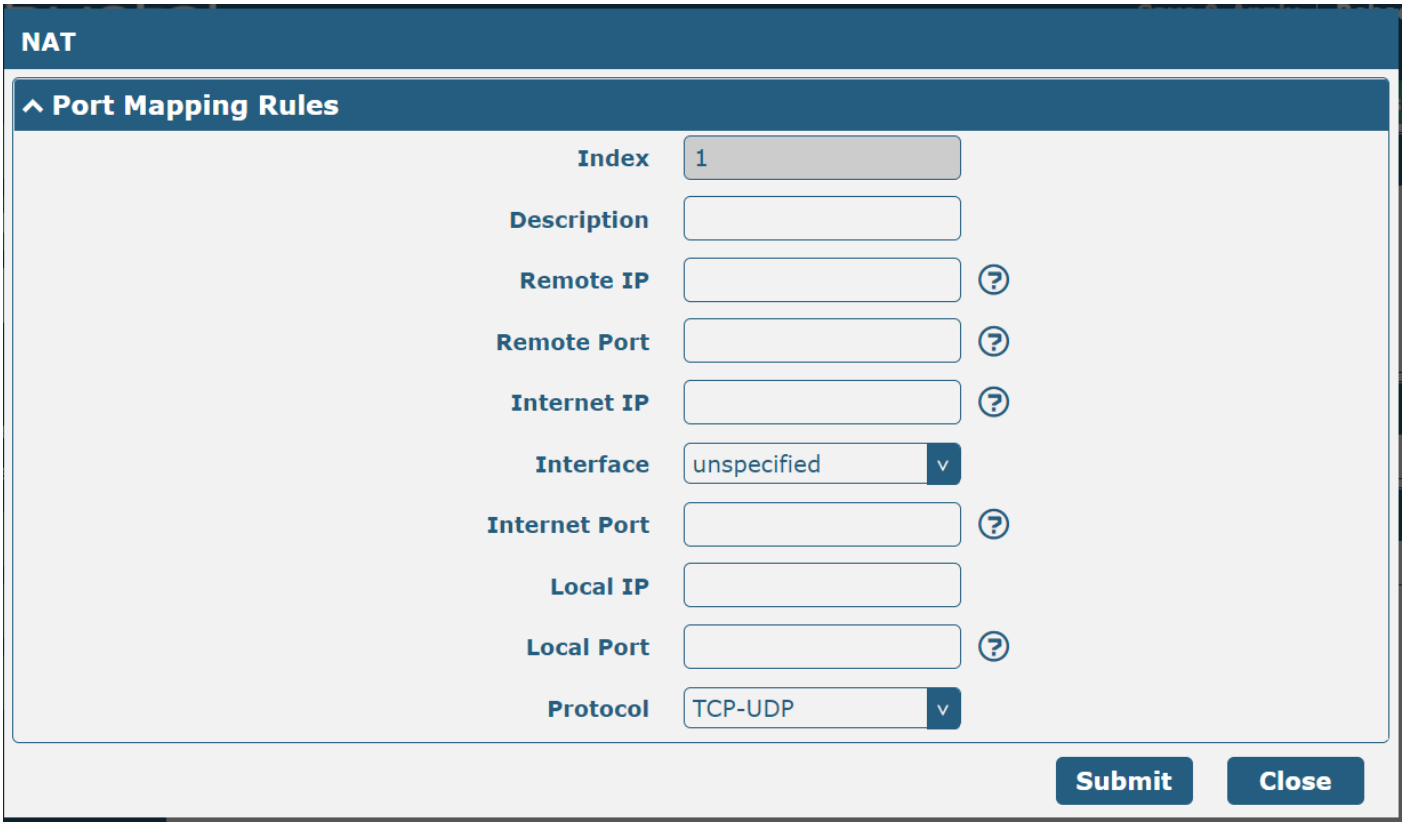


DMZ 設定		
アイテム	説明	デフォルト
DMZ の有効化	トグルボタンをクリックして、DMZ を有効/無効にします。 DMZ ホストは、転送されるポートを除くすべてのポートが公開されている内部ネットワーク上のホストです。	オフ
ホスト IP アドレス	内部ネットワーク上の DMZ ホストの IP アドレスを入力します。	Null
送信元 IP アドレス	DMZ ホストと通信できるアドレスを設定します。 Null は、任意のアドレスを意味します。	Null

ポートマッピングはデバイスで手動で定義され、パブリックネットワーク上の特定のポートから受信したすべてのデータは、内部ネットワーク内の特定の IP の特定のポートに転送されます。「**ネットワーク>ファイアウォール>NAT>ポートマッピング**」をクリックすると、次の情報が表示されます。

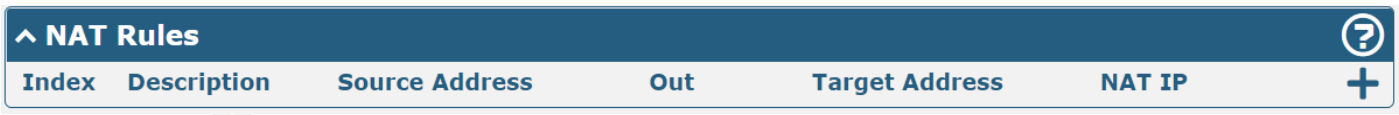


クリック + すると、ポート マッピング ルールが追加されます。ルールの最大数は **50** です。

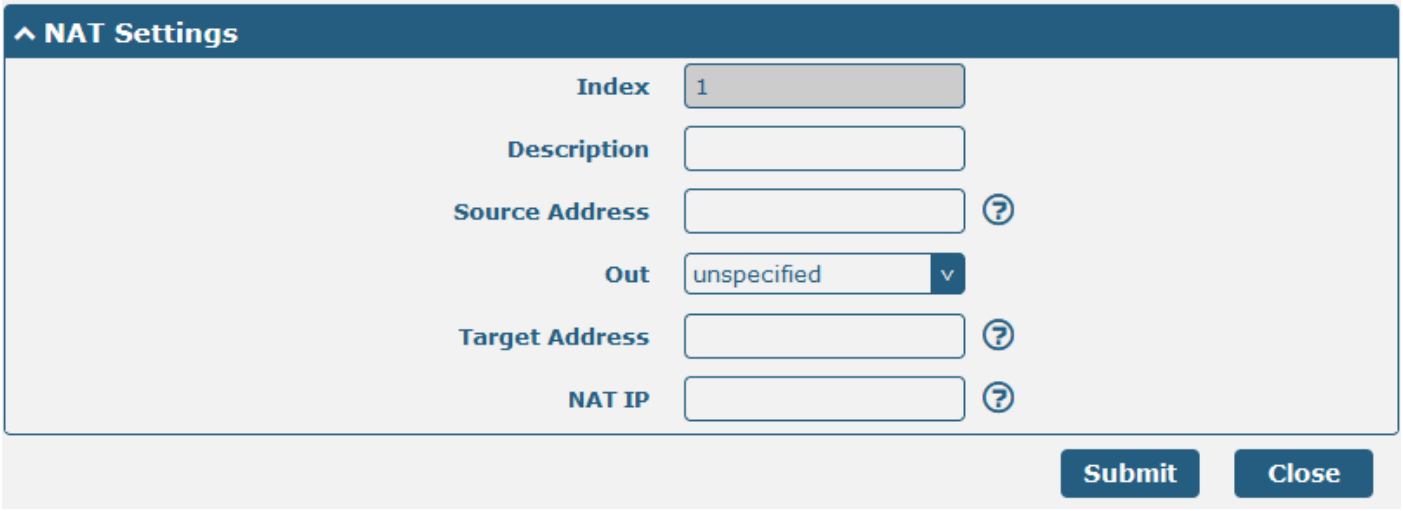


ポート マッピング ルール		
アイテム	説明	デフォルト
インデックス	リストの序数を示します。	--
説明	このポート マッピングの説明を入力します。	Null
リモート IP	ローカル IP アドレスにアクセスできるホストまたはネットワークを指定します。空は無制限を意味します (例:10.10.10.10/255.255.255.255 または 192.168.1.0/24)。	Null
リモートポート	ローカル IP アドレスにアクセスできるホストまたはネットワークのポートを指定します。空は無制限を意味します。	Null
インターネット IP	インターネットから他のホストからアクセスできるデバイスのインターネット IP を入力します。	Null
インターフェイス	設定するリンクの対応するポートを選択します。	未指定
インターネットポート	インターネットから他のホストからアクセスできるデバイスのインターネットポートを入力します。	Null
ローカル IP	デバイスのインターネットポートに転送するデバイスの LAN IP を入力します。	Null
ローカルポート	デバイスの LAN IP のポートを入力します。	Null
プロトコル	アプリケーションに応じて「TCP」、「UDP」、「TCP-UDP」から選択します。	TCP-UDP の

NAT 設定、カスタム NAT ルール。「**Network > Firewall > NAT> NAT Rules**」をクリックすると、以下が表示されます。



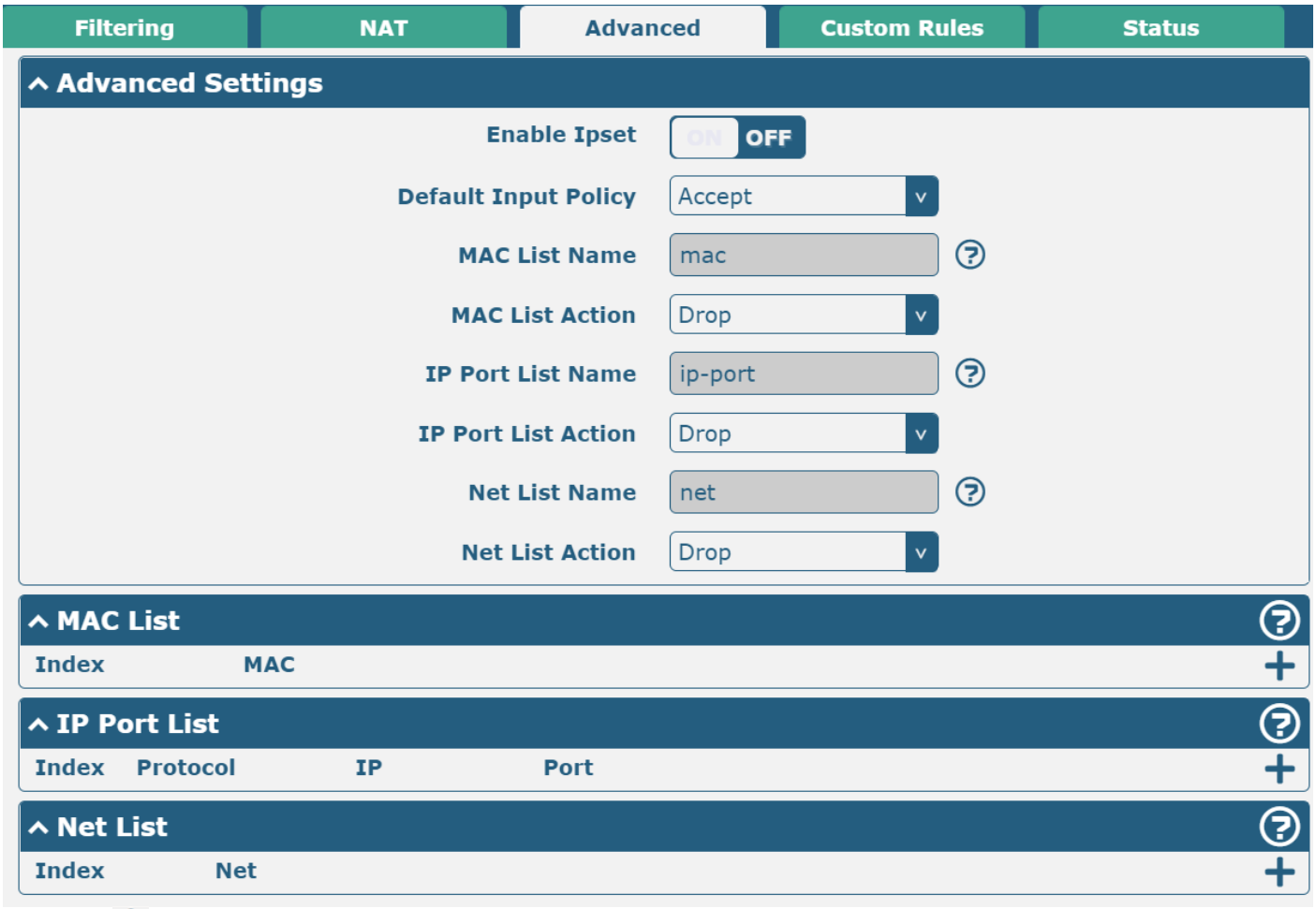
クリックすると ＋、カスタムルールを追加できます。



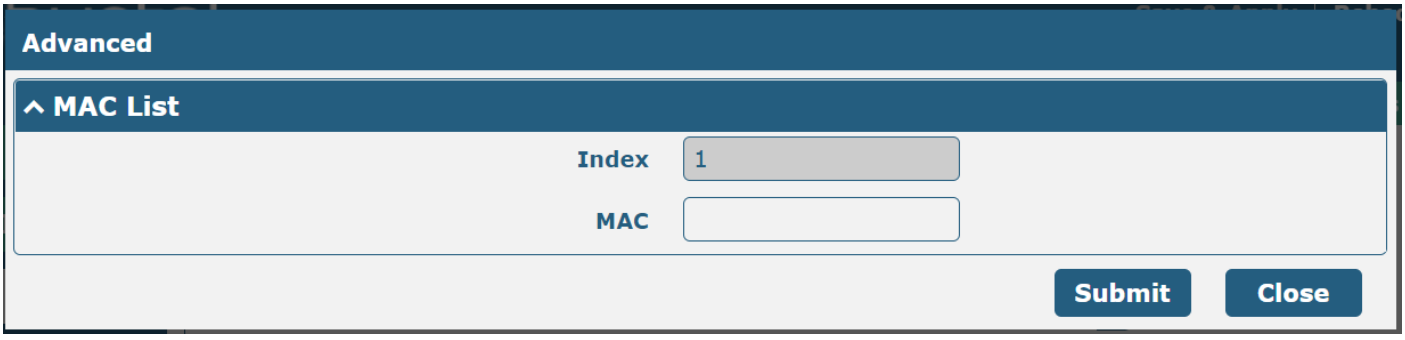
NAT 設定		
アイテム	説明	デフォルト
インデックス	リストの序数を示します。	--
説明	この NAT ルールの説明を入力します。	Null
送信元アドレス	送信元アドレスを x.x.x.x、x.x.x.x/xx、x.x.x.x-x.x.x.x、または null の形式で入力して、任意のアドレスを示します。	Null
アウト	出力インターフェイスを選択します。unspecified を選択すると、任意の出力インターフェイスが生成されます。	未指定
ターゲット・アドレス	ターゲット・アドレスを x.x.x.x、x.x.x.x/xx、x.x.x.x-x.x.x.x の形式で入力します。	Null
NAT IP (英語)	NAT アドレスを x.x.x.x の形式で入力します。	Null

2) アドバンスド

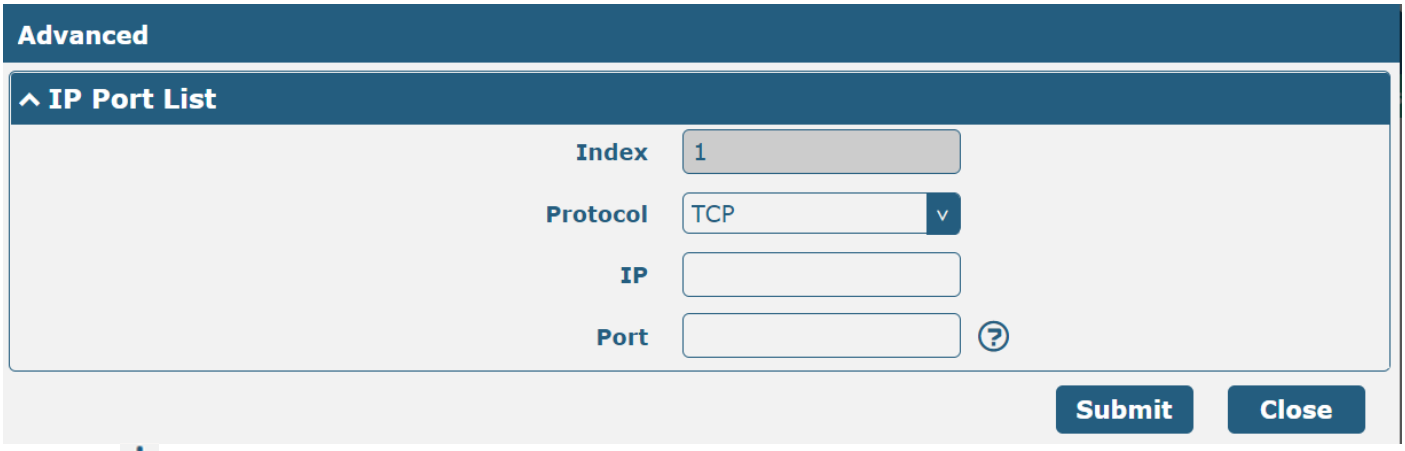
IP セットは Linux カーネル内のフレームワークで、IPset ユーティリティで管理できます。タイプに応じて、IP セットには IP アドレス、ネットワーク、(TCP/UDP)ポート番号、MAC アドレス、インターフェイス名、またはそれらの組み合わせが格納され、エントリをセットと照合するときに超高速が保証されます。「ネットワーク>ファイアウォール>**詳細」をクリックします**。次の情報が表示されます。



クリック＋すると、MAC リストが追加されます。 最大数は 50 です。



クリックすると＋、IP ポート リストが追加されます。最大数は 50 です。



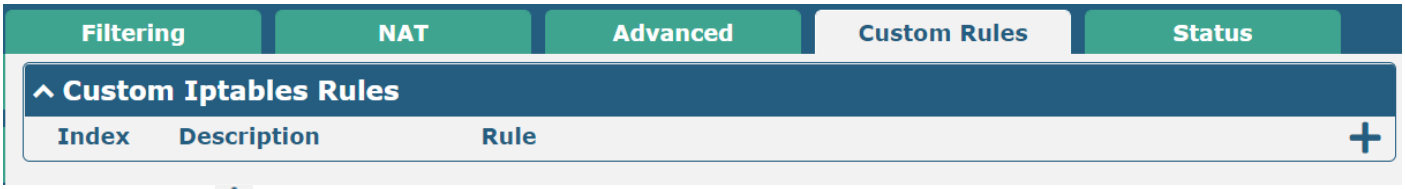
クリック＋すると、ネットリストが追加されます。最大数は 50 です。

アドバンスド		
アイテム	説明	デフォルト
一般設定		
Ipset を有効にする	トグルボタンをクリックして、Ipset オプションを有効/無効にします。	オン
デフォルトの入力ポリシー	「Accept」または「Drop」 から選択します。 • Accept:デバイスは、MAC / IP-Port / Net のドロップリストに適合するホストを除くすべての入力接続要求を受け入れます。 • ドロップ: デバイスは、MAC / IP ポート/ネットの受け入れリストに適合するホストを除くすべての入力接続要求をドロップします。	受け入れる
MAC リスト名	MAC リストの名前を入力します 。 純粋な数値の入力はサポートできません。	マック
MAC リスト アクション	「Accept」または「Drop」から選択します。 • [Accept]:[Default Input Policy] がドロップされると、デバイスは、この受け入れられた MAC リストに適合するホストを除くすべての接続要求をドロップします。 • [ドロップ(Drop)]:[デフォルト入力ポリシー(Default Input Policy)] が受け入れられると、デバイスは、このドロップ MAC リストに適合するホストを除くすべての接続要求を受け入れます。	落とす
IP ポート リスト名	MAC リストの名前を入力します 。 純粋な数値の入力はサポートできません。	IP ポート

アドバンスド		
アイテム	説明	デフォルト
IP ポートリストアクション	「Accept」または「Drop」から選択します。 • [Accept]:[Default Input Policy]がドロップされると、デバイスは、この[Accept] IP Port リストに適合するホストを除くすべての接続要求をドロップします。 • ドロップ:デフォルトの入力ポリシーが受け入れられると、デバイスは、このドロップ IP ポートリストに適合するホストを除くすべての接続要求を受け入れます。	落とす
ネットリスト名	MAC リストの名前を入力します 。 純粋な数値の入力はサポートできません。	網
ネットリストアクション	「Accept」または「Drop」から選択します。 • [Accept]:[Default Input Policy]がドロップされると、デバイスは、この受け入れられたネットリストに適合するホストを除くすべての接続要求をドロップします。 • [ドロップ(Drop)]:[デフォルト入力ポリシー(Default Input Policy)] が受け入れられると、デバイスは、このドロップ ネットリストに適合するホストを除くすべての接続要求を受け入れます。	落とす
MAC リスト(MAC List)		
インデックス	リストの序数を示します。	--
MAC アドレス	MAC アドレスを入力します。形式: XX:XX:XX:XX:XX:XX。	Null
IP ポートリスト		
インデックス	リストの序数を示します。	--
プロトコル	「TCP」または「UDP」から選択します。	TCP の
IP アドレス	IP アドレスを入力します。	Null
港	ポート番号を入力します。	Null
ネット一覧		
インデックス	リストの序数を示します。	--
網	ドメイン名/ IP / IP セグメントを入力してください	Null

3) カスタムルール

このセクションでは、 自分自身を定義するルールを追加できます。**「ネットワーク>ファイアウォール>カスタムルール」をクリックすると、**次の項目が表示されます。

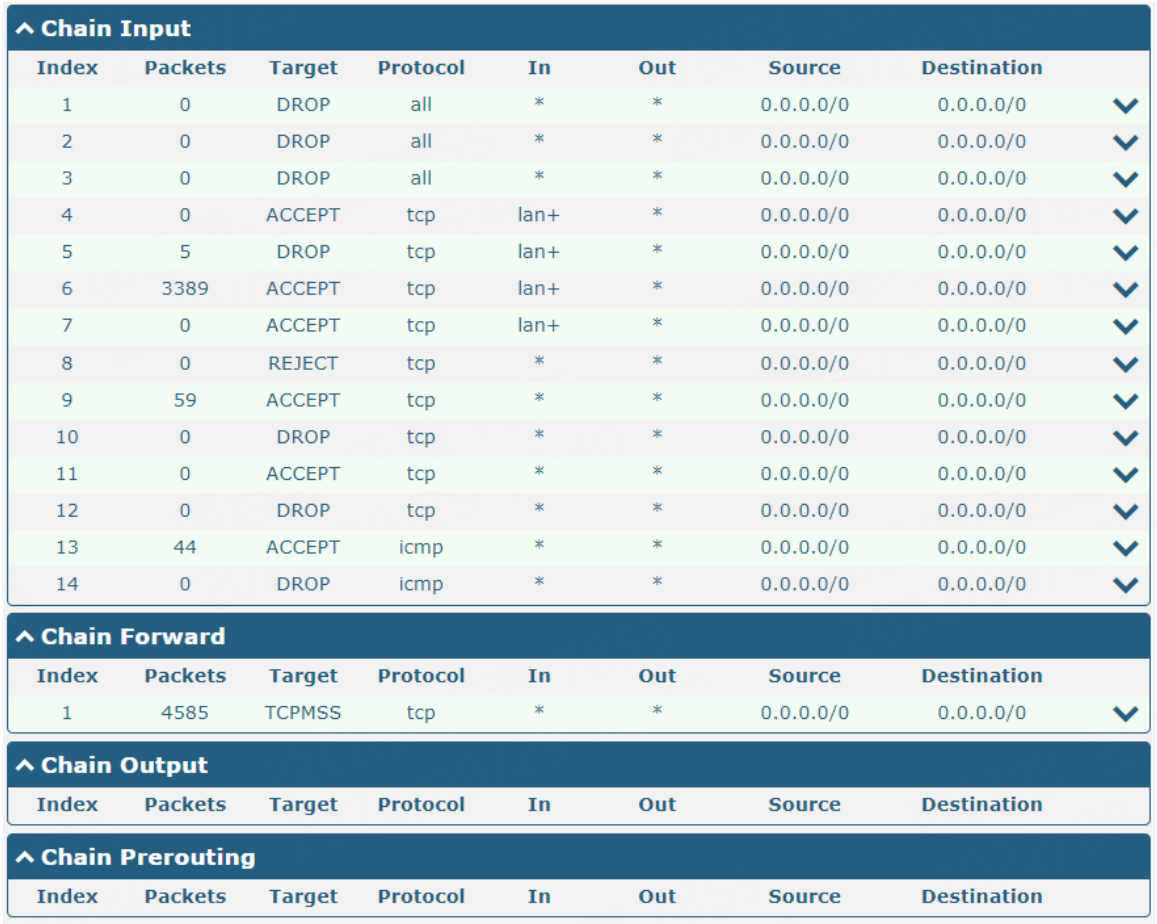


クリックすると ＋、カスタムルールを追加できます。 最大数は 20 **です。**

カスタム ファイアウォール ルール		
アイテム	説明	デフォルト
インデックス	リストの序数を示します。	--
説明	これらのカスタム ファイアウォール ルールの説明を入力します。	Null
支配	カスタムルールを入力します。	Null

4) ステータス

このセクションでは、デバイスのファイアウォールのステータスを表示できます。



Chain Input

Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0
2	0	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0
3	0	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0
4	0	ACCEPT	tcp	lan+	*	0.0.0.0/0	0.0.0.0/0
5	5	DROP	tcp	lan+	*	0.0.0.0/0	0.0.0.0/0
6	3389	ACCEPT	tcp	lan+	*	0.0.0.0/0	0.0.0.0/0
7	0	ACCEPT	tcp	lan+	*	0.0.0.0/0	0.0.0.0/0
8	0	REJECT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
9	59	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
10	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
11	0	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
12	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
13	44	ACCEPT	icmp	*	*	0.0.0.0/0	0.0.0.0/0
14	0	DROP	icmp	*	*	0.0.0.0/0	0.0.0.0/0

Chain Forward

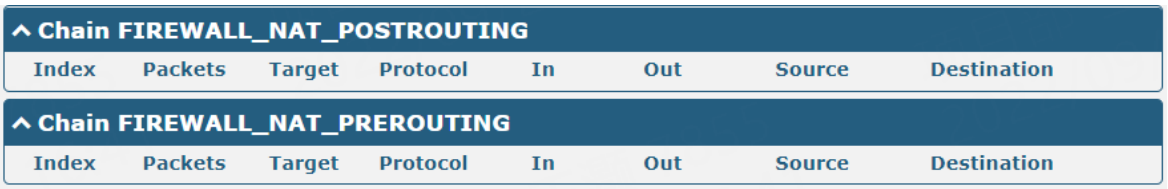
Index	Packets	Target	Protocol	In	Out	Source	Destination
1	4585	TCPMSS	tcp	*	*	0.0.0.0/0	0.0.0.0/0

Chain Output

Index	Packets	Target	Protocol	In	Out	Source	Destination

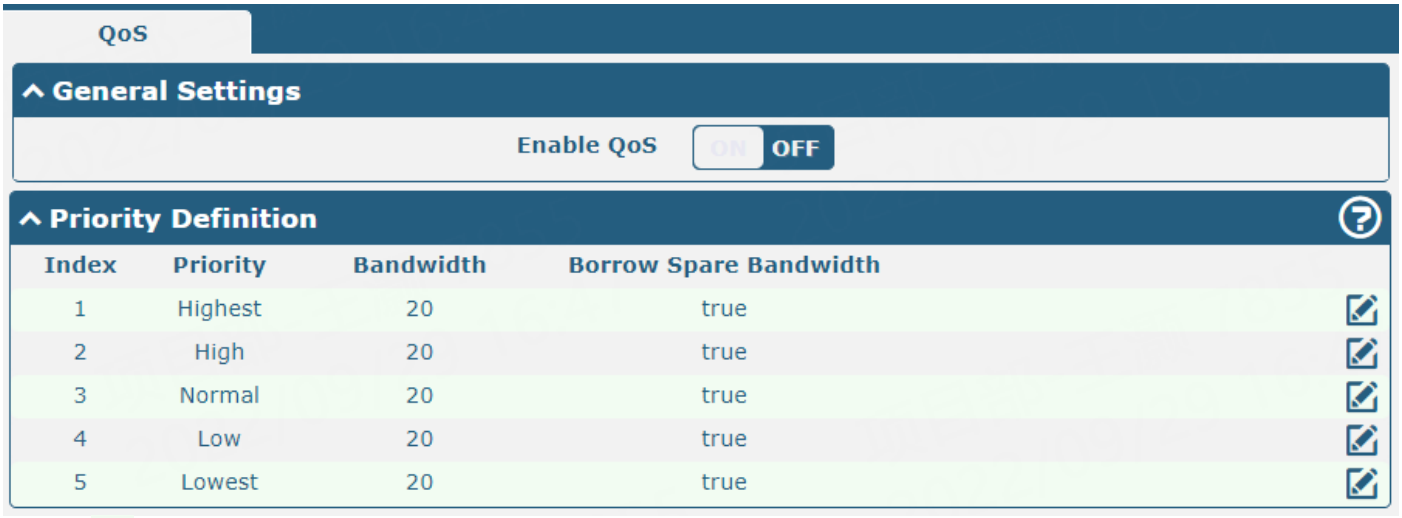
Chain Prerouting

Index	Packets	Target	Protocol	In	Out	Source	Destination

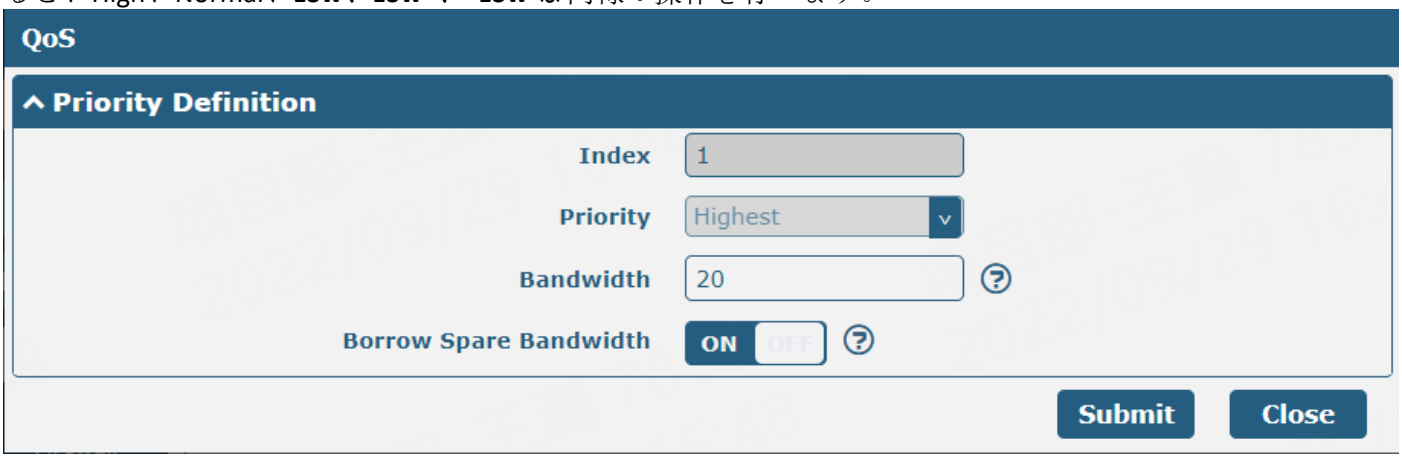


3.4.3 QoS

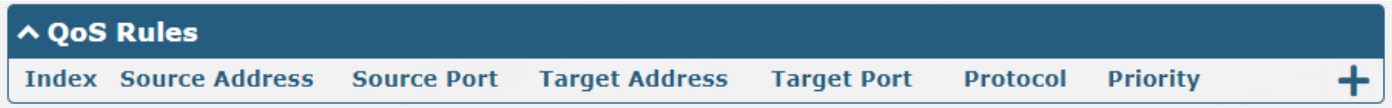
「Network **> QoS > Enable QoS**」をクリックして、QoS 機能を有効または無効にします。



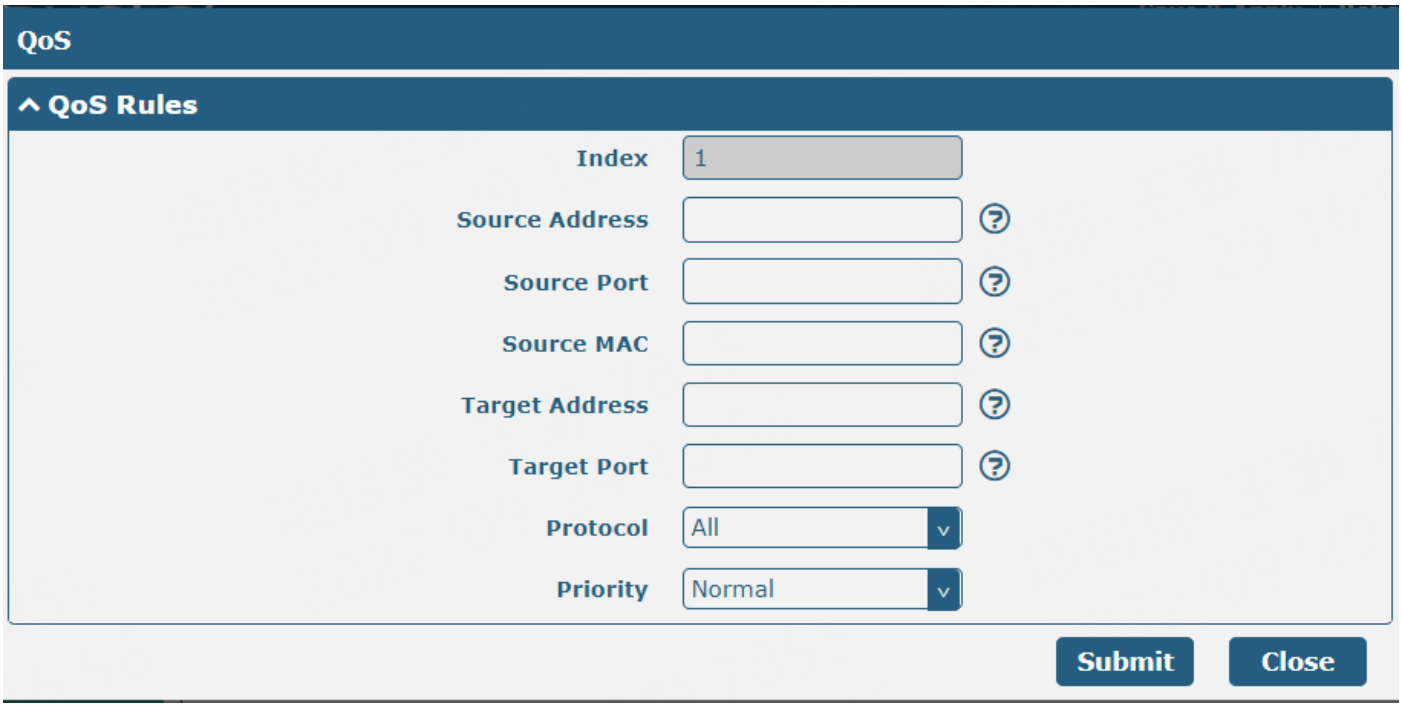
右端の ボタンをクリックして、QoS プライオリティを変更します。ここでは、Highest Priority を例にとると、High、Normal、**Low**、**Low** 、 **Low** は同様の操作を行います。



優先度の定義		
アイテム	説明	デフォルト
帯域幅	合計帯域幅のパーセンテージを入力します。Full は 100 です。	20
予備の帯域幅の借用	有効にすると、スイッチが有効なときに、他のプライオリティから未使用の帯域幅を借用できます。	オン



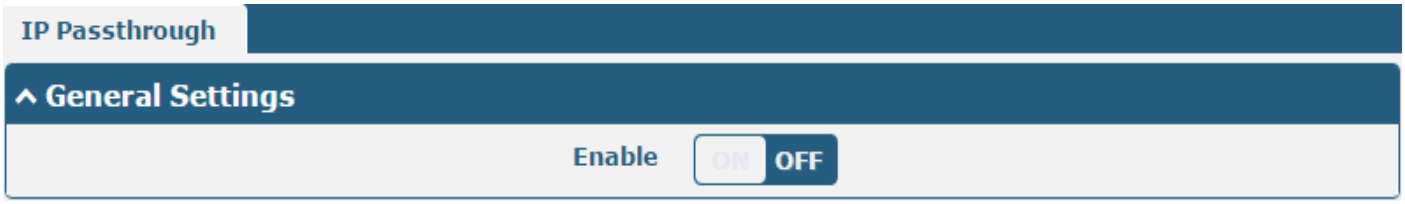
クリック すると、QoS ルールが追加されます。 最大数は 20 です。



QoS ルール		
アイテム	説明	デフォルト
送信元アドレス	形式: x.x.x.x、x.x.x.x/xx、x.x.x.x-x.x.x.x、空は任意の場所を意味します	Null
送信元ポート	フォーマット: port[:p card]	オン
送信元 MAC	フォーマット:XX:XX:XX:XX:XX:XX	Null
ターゲット・アドレス	形式: x.x.x.x、x.x.x.x/xx、x.x.x.x-x.x.x.x、空は任意の場所を意味します	Null
ターゲット・ポート	フォーマット: port[:p card]	Null
プロトコル	プロトコルに TCP、UDP、ICMP、TCP-UDP を設定します	すべての
優先権	QoS のプライオリティの設定	正常

3.4.4 IP パススルー

「IP パススルー**>ネットワーク>IP パススルー**」をクリックして、IP パススルーオプションを有効または無効にします。



デバイスが IP パススルーを有効にすると、端末デバイス(PC など)は DHCP クライアントモードを有効にし てデバイスの LAN ポートに接続し、デバイスが正常にダイヤルアップすると、PC は ISP によって割り当てられた IP アドレスと DNS サーバーアドレス を自動的に取得します。

手記:

（1） IP パススルー機能では、ネットワーク プロバイダー アドレスを 1 つだけ割り当てることができます。

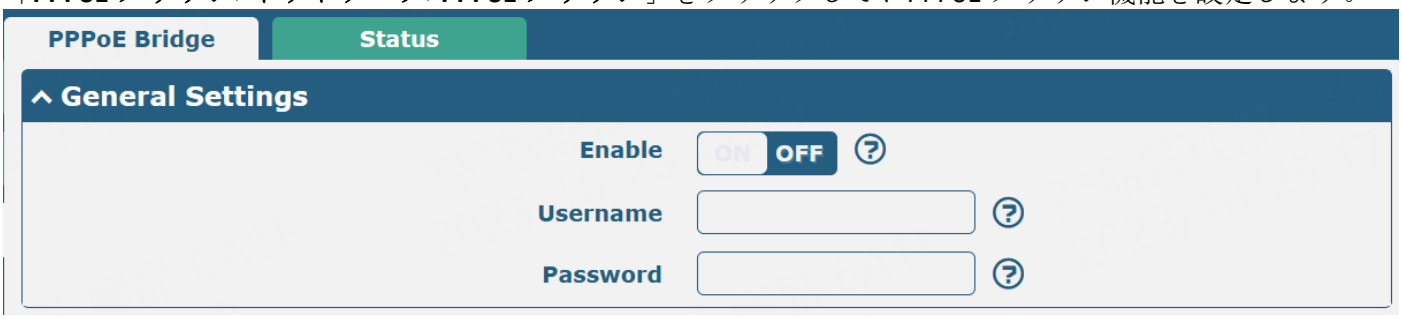
（2） この機能を使用するには、メイン リンクを WWAN に設定し、バックアップ リンクを None に設定する必要があります。

3.4.5 PPPoE ブリッジ

このセクションは、PPPoE ブリッジング機能に関連するパラメータを設定するために使用されます。この機能を有効にすると、ダウンストリーム デバイスは PPPoE ダイヤルアップを介して WWAN IP アドレスを取得できます。

注: *この機能を使用するには、プライマリリンクを WWAN に設定し、バックアップリンクを None に設定する必要があります。*

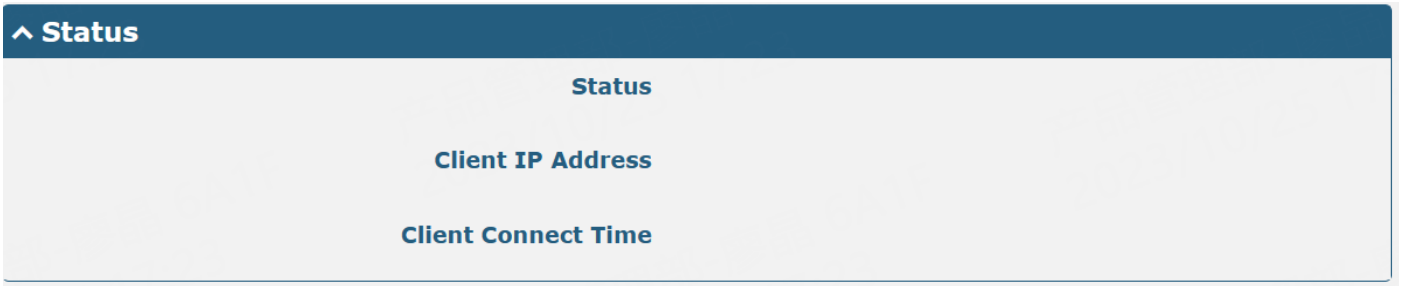
「**PPPoE ブリッジ>ネットワーク>PPPoE ブリッジ**」をクリックして、PPPoE ブリッジ機能を設定します。



一般設定@PPPoE ブリッジ		
アイテム	説明	デフォルト
エネーブル	PPPoE ブリッジング機能を有効/無効にします。	オフ
ユーザー名	認証と IP アドレスの取得のためのカスタムユーザー名を入力します。	Null
パスワード	認証と IP アドレスの取得のために、カスタマイズされたユーザー名に対応するパスワードを入力します。	Null

1) ステータス

このセクションは、PPPoE ブリッジのステータスを表示するために使用されます。



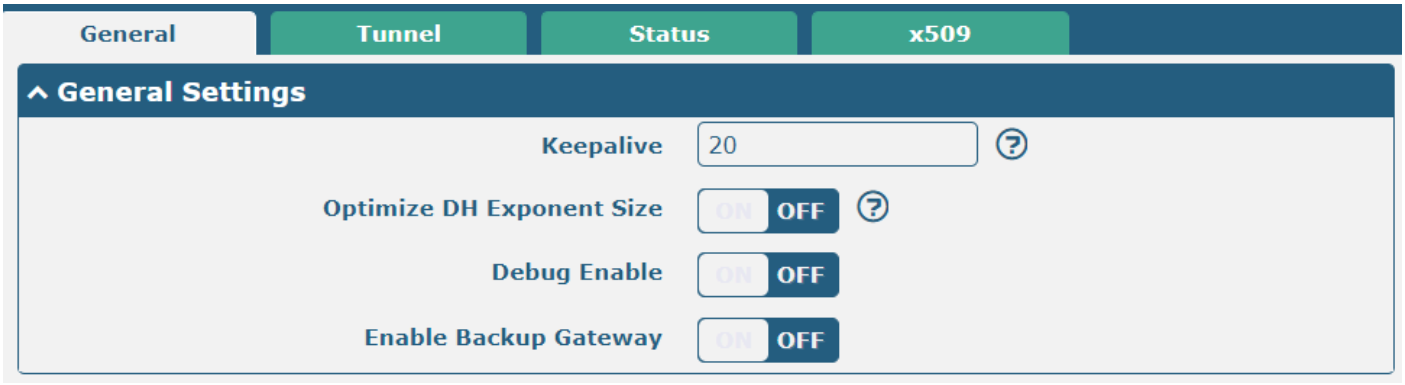
注: [**Network > PPPoE Bridge > Status**] をクリックすると、現在のアプリケーションの実行ステータス、クライアント IP、および最後の接続時間が表示されます。

3.5 VPN 接続

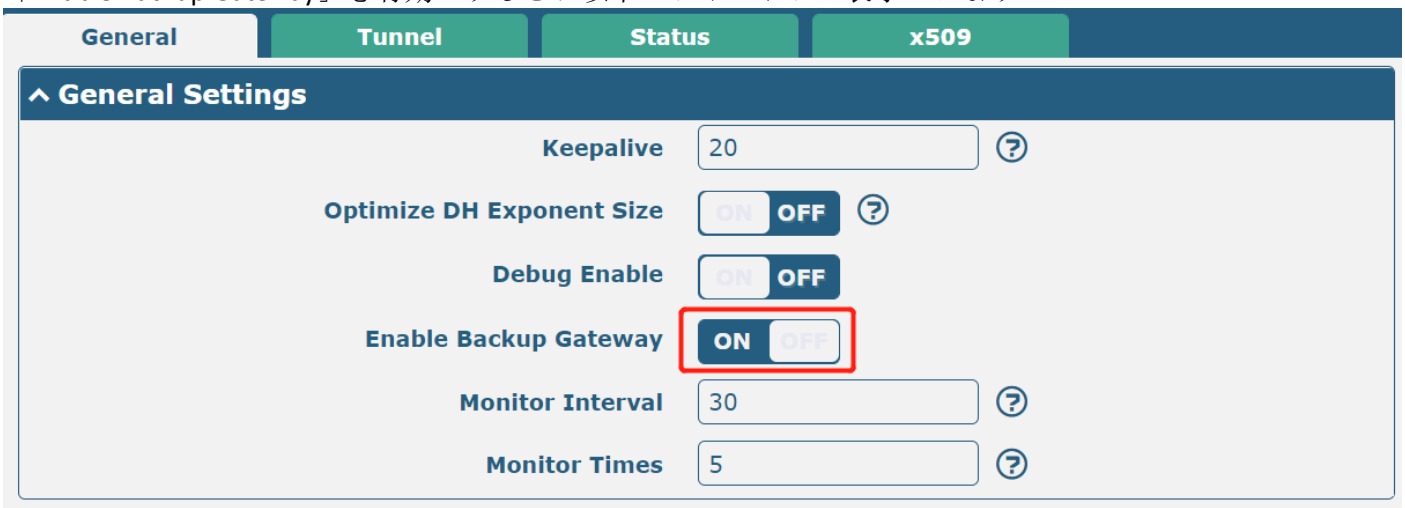
3.5.1 IPsec (IPsec)

このセクションでは、IPsec および関連パラメータを設定できます。インターネット プロトコル セキュリティ (IPsec) は、プロトコルスイート 安全なもののために インターネットプロトコル (IP)通信 認証 そして暗号化 各 IP パケット 通信セッションの。
[**VPN > IPsec] > [General]** をクリックして、IPsec パラメータを設定します。

1) 全般



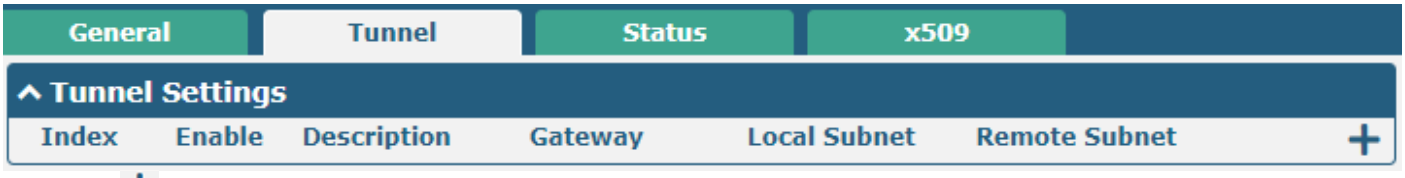
「Enable Backup Gateway」を有効にすると、以下のウィンドウが表示されます。



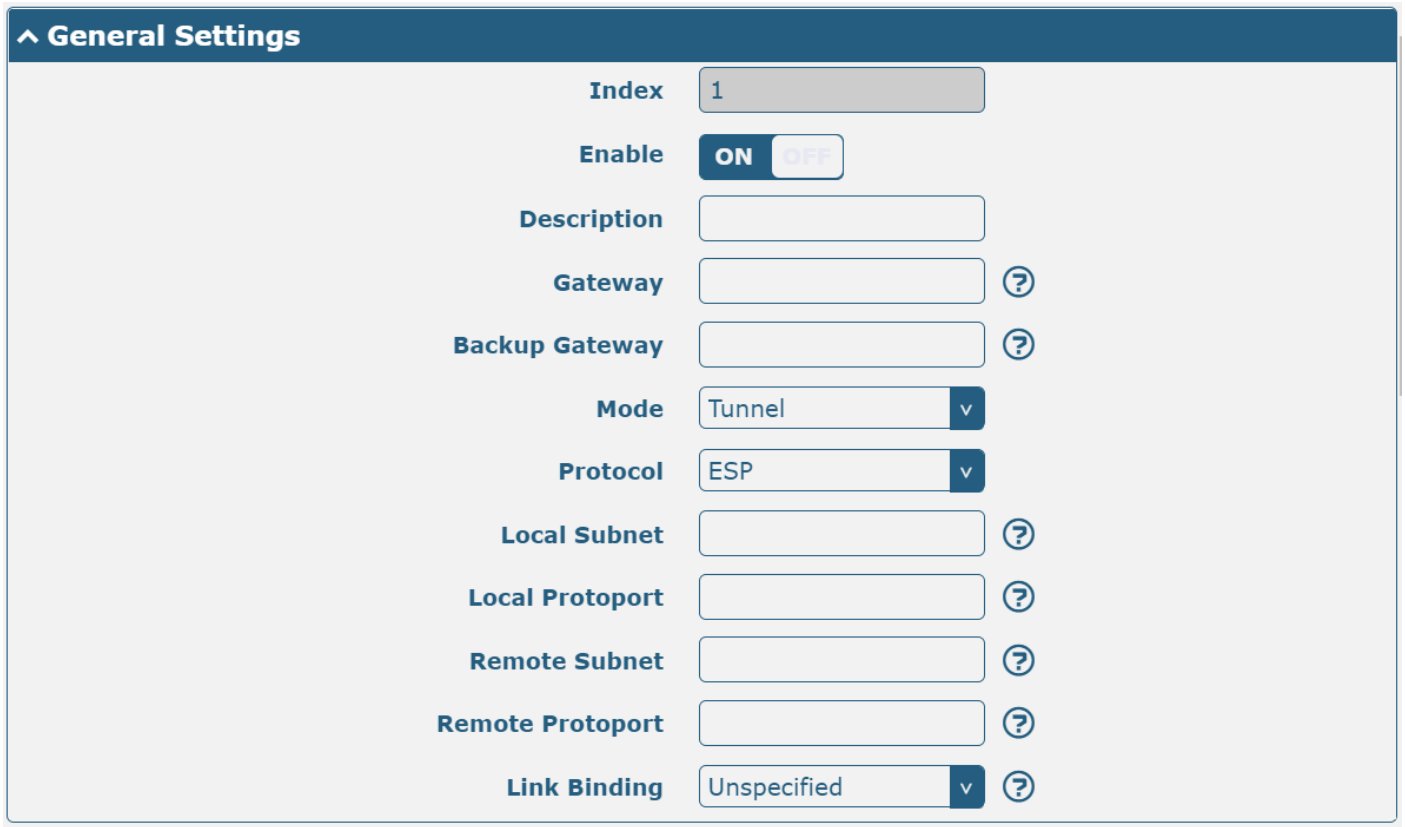
一般設定 @ 一般		
アイテム	説明	デフォルト
キープアライブ	存続時間を秒単位で設定します。デバイスは、キープアライブ パケットを NAT(ネットワーク アドレス変換)サーバに定期的に送信して、NAT テーブル上のレコードが消えるのを防ぎます。	20
DH サイズの最適化	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、dhgroup17 または dhgroup18 を使用するときに、DH キーの生成時間を短縮するのに役立ちます。	オフ

デバッグ有効(Debug Enable)	切り替えボタンをクリックして、このオプションを有効/無効にします。デバッグポートへの IPsec VPN 情報出力を有効にします。	オフ
バックアップ・ゲートウェイの有効化		
モニターインターバル	「モニターインターバル」と入力します。単位:秒。	30
監視時間	IPsec プライマリ デバイスの番号 maxim が応答されていないと入力します。	5

2) トンネル



クリック + すると、IPsec トンネル設定を追加できます。最大数は **6 です**。



一般設定 @ トンネル		
アイテム	説明	デフォルト
インデックス	リストの序数を示します。	--
エネーブル	トグルボタンをクリックして、この IPsec トンネルを有効/無効にします。	オン
説明	この IPsec トンネルの説明を入力します。	Null
ゲートウェイ	リモート側の IPsec VPN サーバのアドレスを入力します。0.0.0.0 は任意のアドレスを表します。	Null
バックアップ・	リモート側の IPsec VPN サーバのバックアップアドレスを入力します。空は無効を意味します。	Null

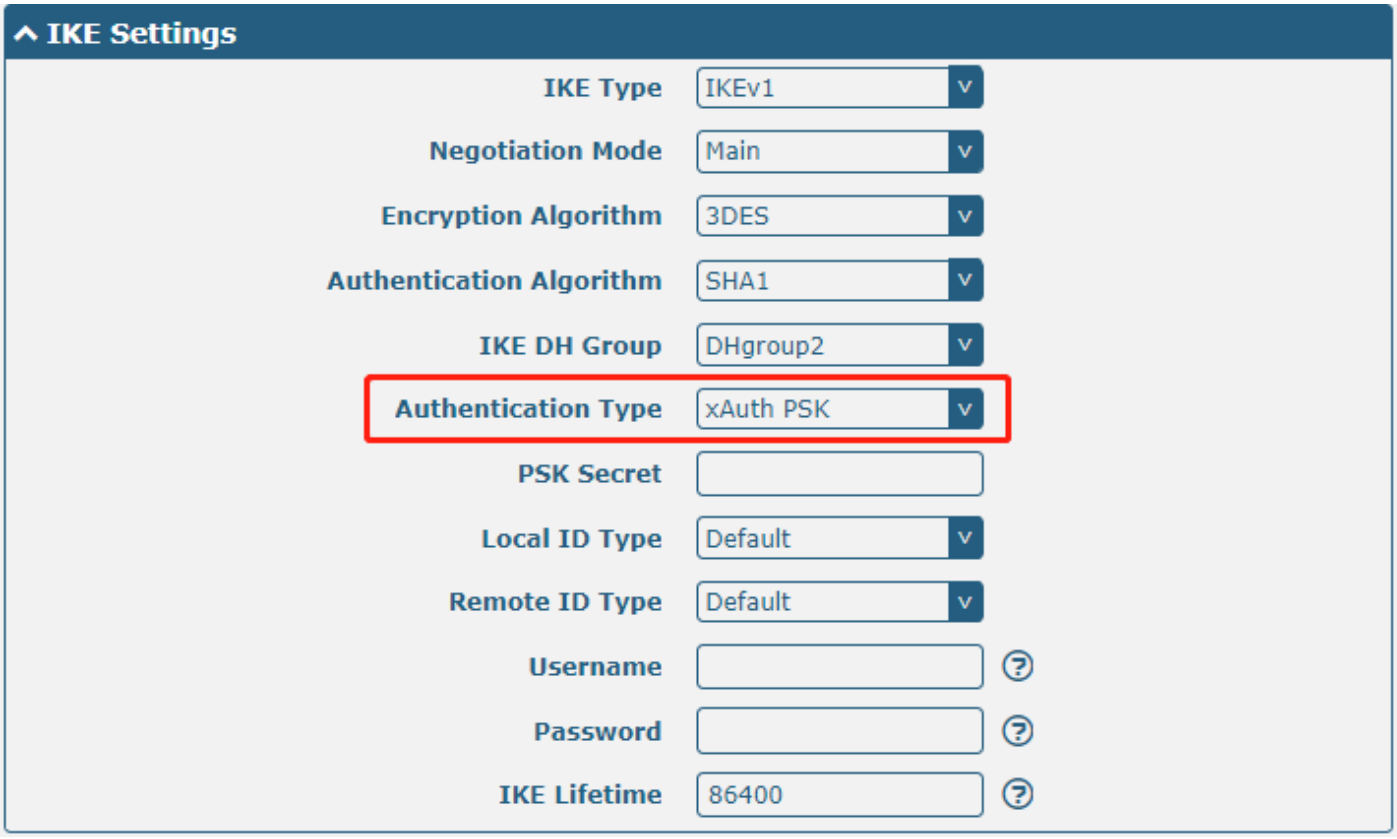
ゲートウェイ		
モード	「トンネル」と「トランスポート」を選択します。 • トンネル:デバイス間、またはデバイスへのエンドステーションで一般的に使用され、デバイスはその背後にあるホストのプロキシとして機能します。 • トランスポート:デバイスがホストとして扱われている場合、たとえば、デバイスが実際の宛先であるワークステーションからデバイスへの暗号化された Telnet セッションなど、エンドステーション間またはエンドステーションとデバイス間で使用されます。	トンネル
プロトコル	セキュリティプロトコルを「ESP」と「AH」から選択します。 • ESP: ESP プロトコルを使用します。 • AH: AH プロトコルを使用します。	ESP の
ローカルサブネット	IPsec で保護されたマスクを使用してローカルサブネットのアドレスを入力します(例:192.168.1.0/24)。	Null
ローカルプロトポート	ポートでプロトコルを入力します (例: tcp/443; udp/1701)。 ローカル protoport とリモート protoport は 、両方が空でない場合は同じである必要があります。	Null
リモートサブネット	IPsec で保護されたマスクを使用してリモートサブネットのアドレス を入力します(例:10.8.0.0/24)。	Null
リモートプロトポート	ポートでプロトコルを入力します (例: tcp/443; udp/1701)。 ローカル protoport とリモート protoport は 、両方が空でない場合は同じである必要があります。	Null
リンクバインディング	IPsec を構築するためのリンクを選択します。	自由

認証タイプとして「PSK」を選択すると、以下のウィンドウが表示されます。

認証タイプとして「CA」を選択すると、以下のウィンドウが表示されます。

認証タイプとして「PKCS#12」を選択すると、以下のウィンドウが表示されます。

認証タイプとして「xAuth PSK」を選択すると、以下のウィンドウが表示されます。



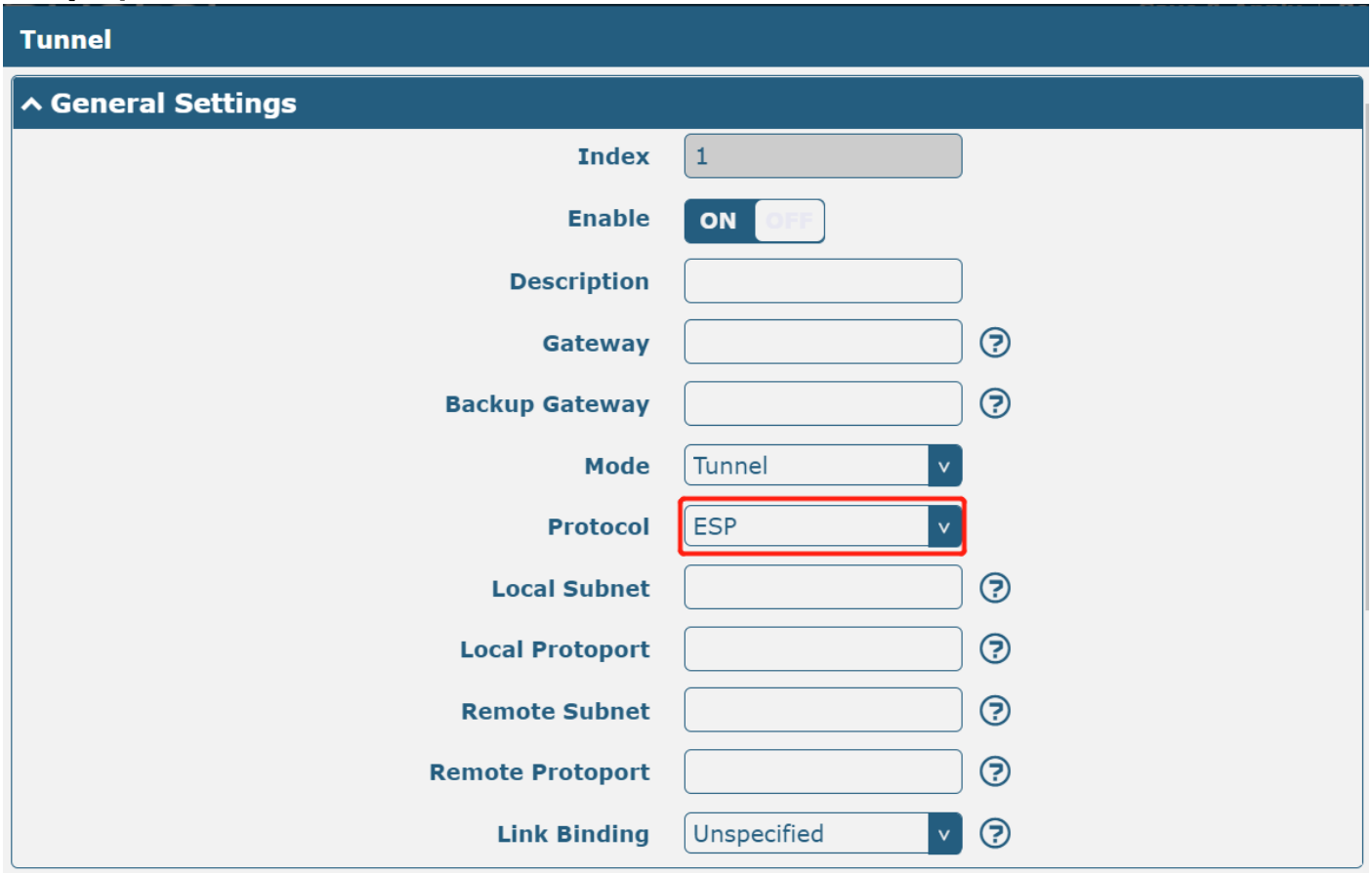
認証タイプとして「xAuth CA」を選択すると、以下のウィンドウが表示されます。

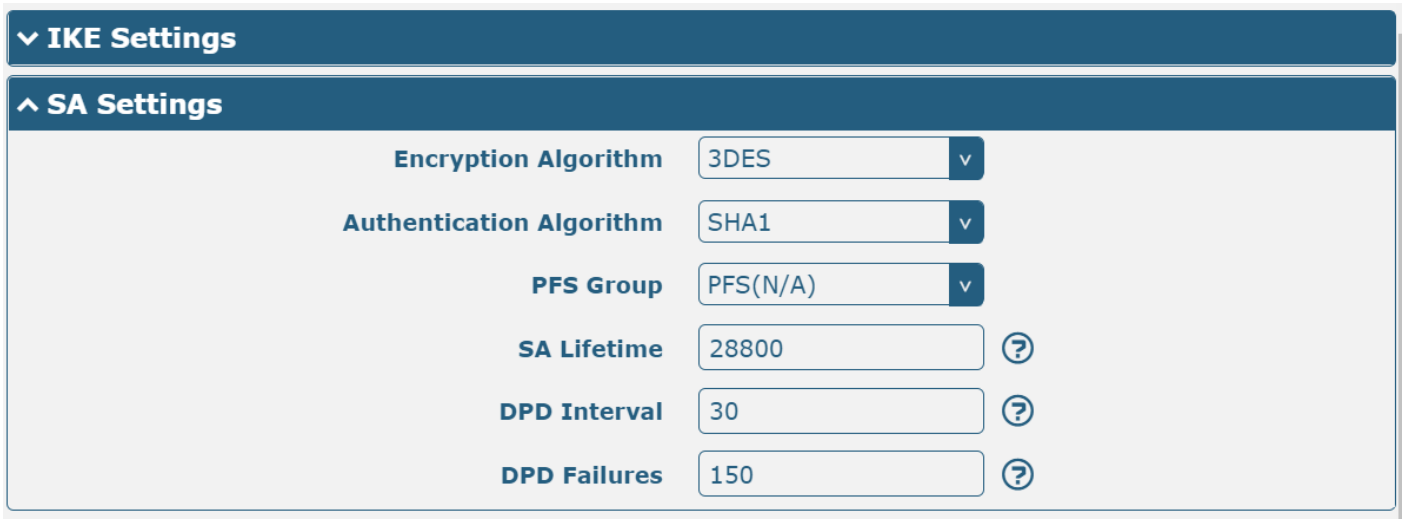
IKE 設定		
アイテム	説明	デフォルト
IKE タイプ	「IKEv1」と「IKEv2」から選択します。	IKEv1 (IKEv1)
ネゴシエーション	フェーズ 1 の IKE ネゴシエーション モードを "Main" と "Aggressive" か	メイン

IKE 設定		
アイテム	説明	デフォルト
モード	ら選択します。IPsec トンネルの一方の端の IP アドレスを動的に取得する場合、IKE ネゴシエーション モードはアグレッシブである必要があります。この場合、ユーザ名とパスワードが正しい限り、SA を確立できます。	
暗号化アルゴリズム	IKE ネゴシエーションで使用する「3DES」、「AES128」、「AES192」、「AES256」から選択します。 • 3DES: CBC モードで 168 ビットの 3DES 暗号化アルゴリズムを使用します。 • AES128: CBC モードで 128 ビットの AES 暗号化アルゴリズムを使用します。 • AES128: CBC モードで 192 ビットの AES 暗号化アルゴリズムを使用します。 • AES256: CBC モードで 256 ビットの AES 暗号化アルゴリズムを使用します。	3DES の
認証アルゴリズム	IKE ネゴシエーションで使用する「MD5」、「SHA1」、「SHA2 256」、「SHA2 512」から選択します。	SHA1 の
IKE DH グループ	キー ネゴシエーション フェーズ 1 で使用する "DHgroup1"、"DHgroup2"、"DHgroup5"、"DHgroup14"、"DHgroup15"、"DHgroup16" 、 " DHgroup17"、または "DHgroup18" から選択します。	DH グループ 2
認証 の種類	IKE ネゴシエーションで使用する「PSK」、「CA」、「xAuth PSK」、「PKCS#12」、「xAuth CA」から選択します。 • PSK: 事前共有キー。 • CA: 認証局。 • xAuth:AAA サーバへの拡張認証。 • PKCS#12: デジタル証明書認証を交換します。	PSK の
PSK シークレット	事前共有キーを入力します。	Null
ローカル ID タイプ (Local ID Type)	IKE ネゴシエーションには、「デフォルト」、「FQDN」、および「ユーザーFQDN」を選択します。 • デフォルト: IKE ネゴシエーションの ID として IP アドレスを使用します。 • FQDN:IKE ネゴシエーションの ID として FQDN タイプを使用します。このオプションを選択した場合は、ローカルセキュリティデバイスの名前を記号(@)なしで入力します(例:test.robustel.com)。 • ユーザー FQDN: IKE ネゴシエーションの ID としてユーザー FQDN タイプを使用します。このオプションを選択した場合は、ローカルセキュリティデバイスの記号「@」を付けた名前文字列を入力します(例:test@robustel.com)。	デフォルト
リモート ID の種類	IKE ネゴシエーションには、「デフォルト」、「FQDN」、および「ユーザーFQDN」を選択します。 • デフォルト:IKE ネゴシエーションの ID として IP アドレスを使用します。 • FQDN:IKE ネゴシエーションの ID として FQDN タイプを使用します。このオプションを選択した場合は、ローカルセキュリティデバイスの名前を記号(@)なしで入力します(例:test.robustel.com)。 • ユーザー FQDN: IKE ネゴシエーションの ID としてユーザー FQDN タイプを使用します。このオプションを選択した場合は、ローカルセキュリティデバイスの記号「@」を付けた名前文字列を入力し	デフォルト

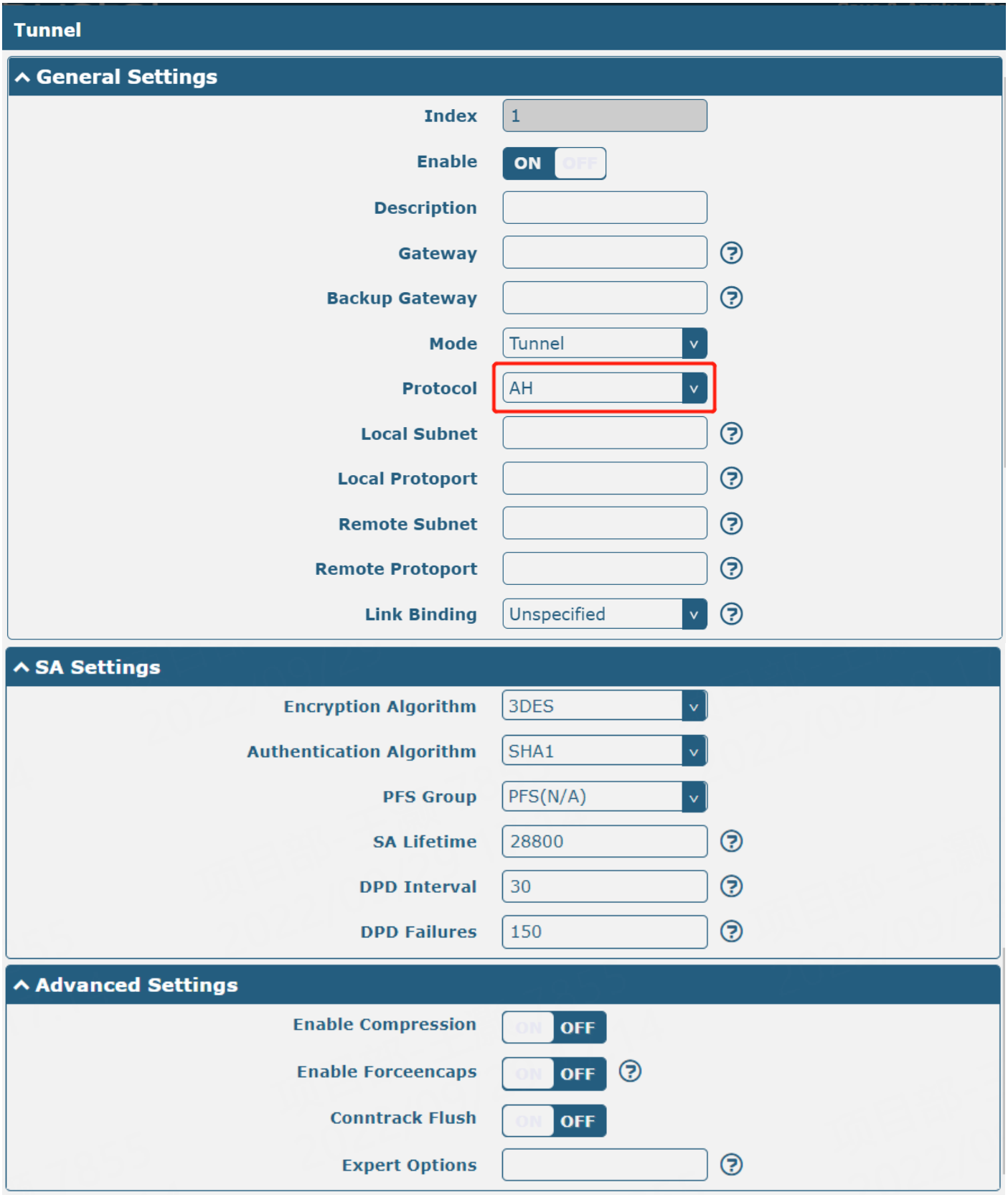
IKE 設定		
アイテム	説明	デフォルト
	ます(例:test@robustel.com)。	
IKE ライフタイム	IKE ネゴシエーションでライフタイムを設定します。SA の期限が切れる前に、IKE は新しい SA をネゴシエートします。新しい SA が設定されるとすぐに有効になり、有効期限が切れると古い SA は自動的にクリアされます。	86400
秘密 キーのパスワード	「CA」および「xAuth CA」認証タイプに秘密鍵を入力します。	Null
ユーザー名	「xAuth PSK」および「xAuth CA」認証タイプに使用するユーザー名を入力します。	Null
パスワード	「xAuth PSK」および「xAuth CA」認証タイプに使用する p assword を入力します。	Null

[全般設定(General Settings)] > [VPN] > [IPsec > トンネル(IPsec Tunnel)] をクリックした場合は、プロトコルとして **[ESP]** を選択します。具体的なパラメータ設定を以下に示します。




IKE Settings
SA Settings
Encryption Algorithm
3DES
Authentication Algorithm
SHA1
PFS Group
PFS(N/A)
SA Lifetime
28800
DPD Interval
30
DPD Failures
150

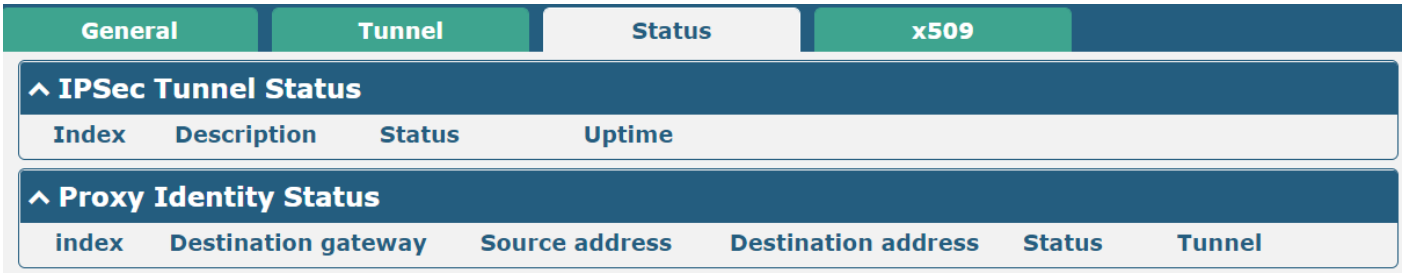
「仮想プライベートネットワーク>IPsec>トンネル>一般設定」のプロトコルが「**AH**」を選択すると、SA 設定が次のように表示されます。



SA 設定		
アイテム	説明	デフォルト
暗号化アルゴリズム	「プロトコル」で「ESP」を選択した場合は、「3DES」、「AES128」、「AES192」、または「AES256」を選択します。 セキュリティが高いほど、実装が複雑になり、速度が低下します。DES は、一般的な要件を満たすのに十分です。高い機密性とセキュリティが必要な場合は、3DES を使用します。	3DES の
認証アルゴリズム	SA ネゴシエーションで使用する「MD5」、「SHA1」、「SHA2 256 」、「SHA2 512」から選択します。	SHA1 の
PFS グループ	使用する「PFS(N/A)」、「DHgroup1」、「DHgroup2」、「DHgroup5」、「DHgroup14」、「DHgroup15」、「DHgroup16」、「DHgroup17」、または「 DHgroup18」から選択します SA ネゴシエーション。	PFS(該当なし)
SA ライフタイム	IPsec SA のライフタイムを設定します。IPsec SA を設定するためにネゴシエートする場合、IKE はローカルで設定されたライフタイムとピアによって提案されたライフタイムの間の小さい方を使用します。	28800
DPD インターバル	ピアから IPsec で保護されたパケットが受信されない場合に DPD がトリガーされるまでのインターバルを設定します。DPD は デッドピア検出です。DPD は、デッド IKE ピアを不規則に検出します。ローカルエンドが IPsec パケットを送信すると、DPD は最後の IPsec パケットがピアから受信された時刻をチェックします。時間が DPD インターバルを超えると、ピアに DPD hello が送信されます。ローカル エンドは、DPD パケットの再送信インターバル内に DPD 確認応答を受信しない場合、DPD hello を再送信します。ローカル エンドは、最大回数の再送信試行を行っても DPD 確認応答を受信しない場合、ピアがすでに停止していると見なし、IKE SA に基づいて IKE SA と IPsec SA をクリアします。	30
DPD の障害	DPD(Dead Peer Detection)パケットのタイムアウトを設定します。	150
詳細 設定		
圧縮を有効にする	切り替えボタンをクリックして、このオプションを有効/無効にします。 IP パケットの内部ヘッダを圧縮できるようにします。	オフ
Forceencaps を有効にする	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、NAT 条件が検出されない場合でも、esp パケットの UDP カプセル化が強制されます。これは、制限の厳しいファイアウォールを克服するのに役立つ可能性があります。	オフ
Conntrack フラッシュ	切り替えボタンをクリックして、このオプションを有効/無効にします。IPsec の確立後に conntrack をクリアします。	オフ
エキスパートオプション	ここに PPP 設定オプションを追加します (形式: config-desc;config-desc、例: protostack=netkey;plutodebug=none です。	Null

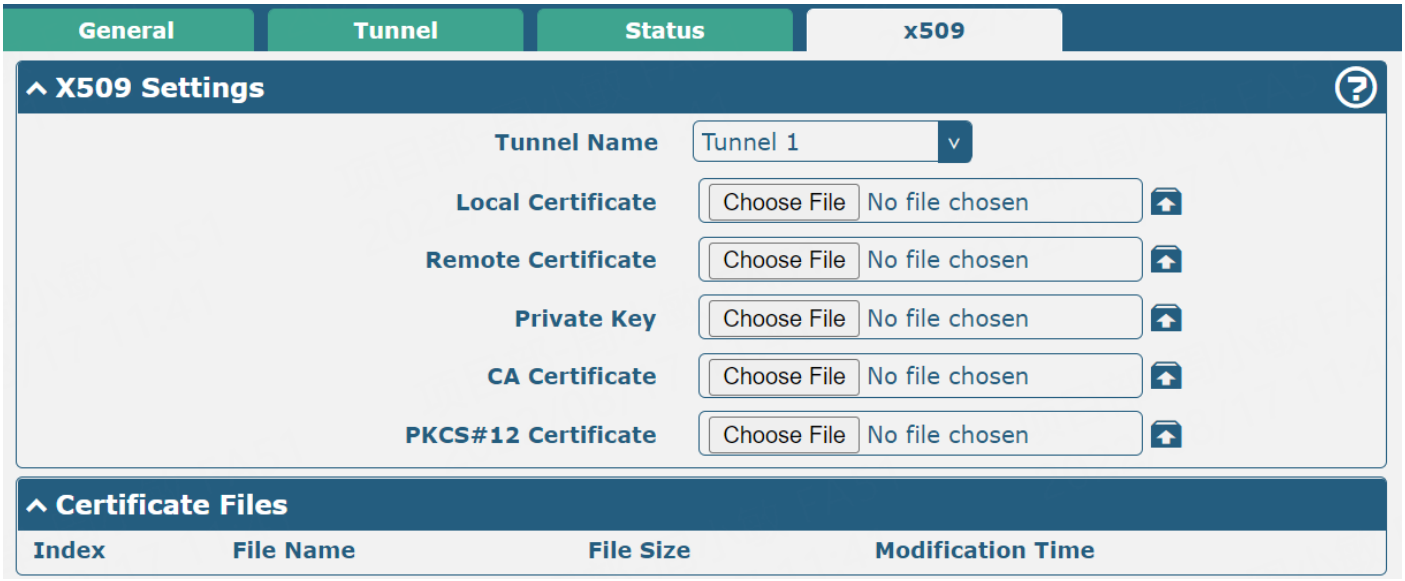
3) ステータス

このセクションでは、IPsec トンネルのステータスを表示できます。



4) x509

ユーザーは、このセクションで IPsec トンネルの証明書をアップロードできます。



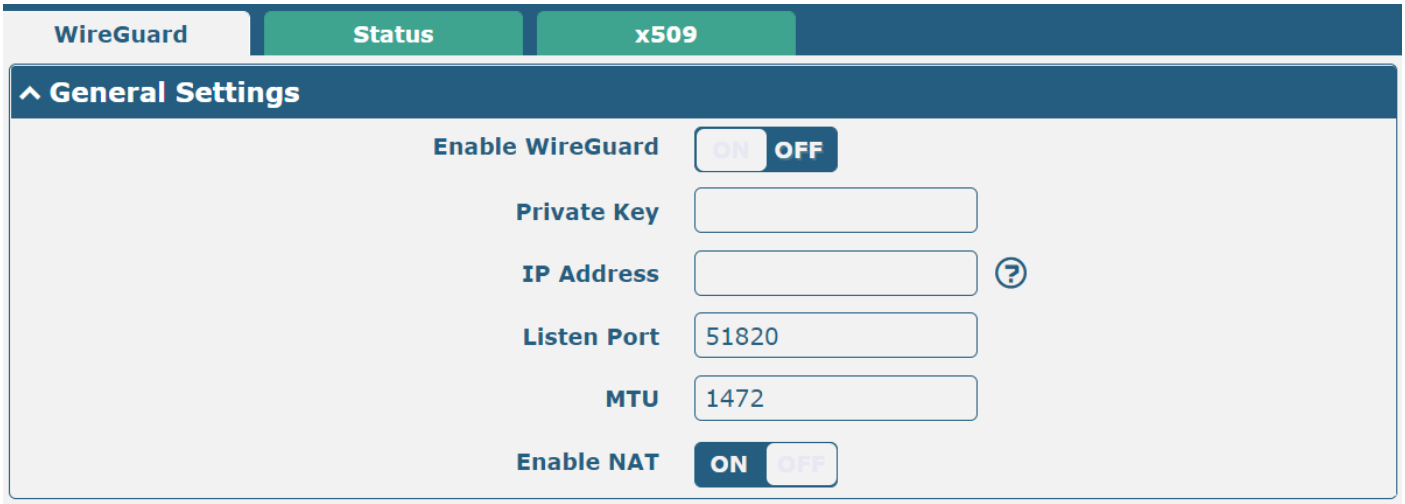
x509 の		
アイテム	説明	デフォルト
X509 設定		
トンネル名(Tunnel Name)	有効なトンネルを選択します。「トンネル 1」、「トンネル 2」、「トンネル 3」、「トンネル 4」、「トンネル 5」、「トンネル 6」から 選択します。	トンネル 1
ローカル 証明書	「ファイルを選択」をクリックして、ローカルコンピューターから証明書ファイルを見つけ 、このファイルをデバイスにインポートします。	--
リモート 証明書	「ファイルの選択」をクリックしてリモートコンピューターから証明書ファイルを見つけ 、このファイルをデバイスにインポートします。	--
秘密鍵	「ファイルを選択」をクリックして、秘密鍵ファイルを見つけます。	--
CA 証明書	「ファイルの選択」をクリックして、 正しい CA 証明書ファイルを見つけます。	--
PKCS#12 証明書	「ファイルの選択」をクリックして、PKCS#12 証明書ファイルを見つけます。	--
証明書ファイル		

x509 の		
アイテム	説明	デフォルト
X509 設定		
インデックス	リストの序数を示します。	--
ファイル名	インポートされた証明書の名前を表示します。	Null
ファイルサイズ	証明書ファイルのサイズを表示します。	Null
最終更新日	証明書ファイルを最後に変更した時刻を表示します。	Null

3.5.2 WireGuard

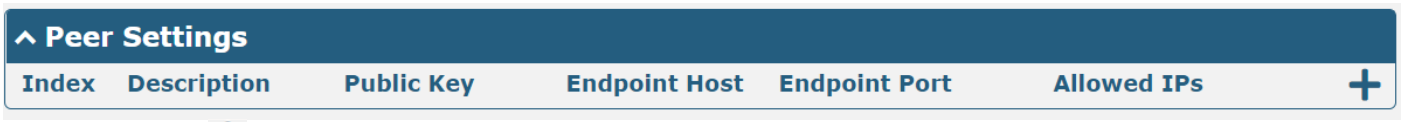
このセクションは、オープンソースの SSL ベースの VPN システムである WireGuard VPN のパラメータを設定するために使用されます。デバイスの WireGuard 機能は、ポイントツーポイントとポイントツーマルチポイントの両方の VPN チャネルをサポートできます。

「**VPN>WireGuard**」をクリックして、WireGuard パラメータを設定します。

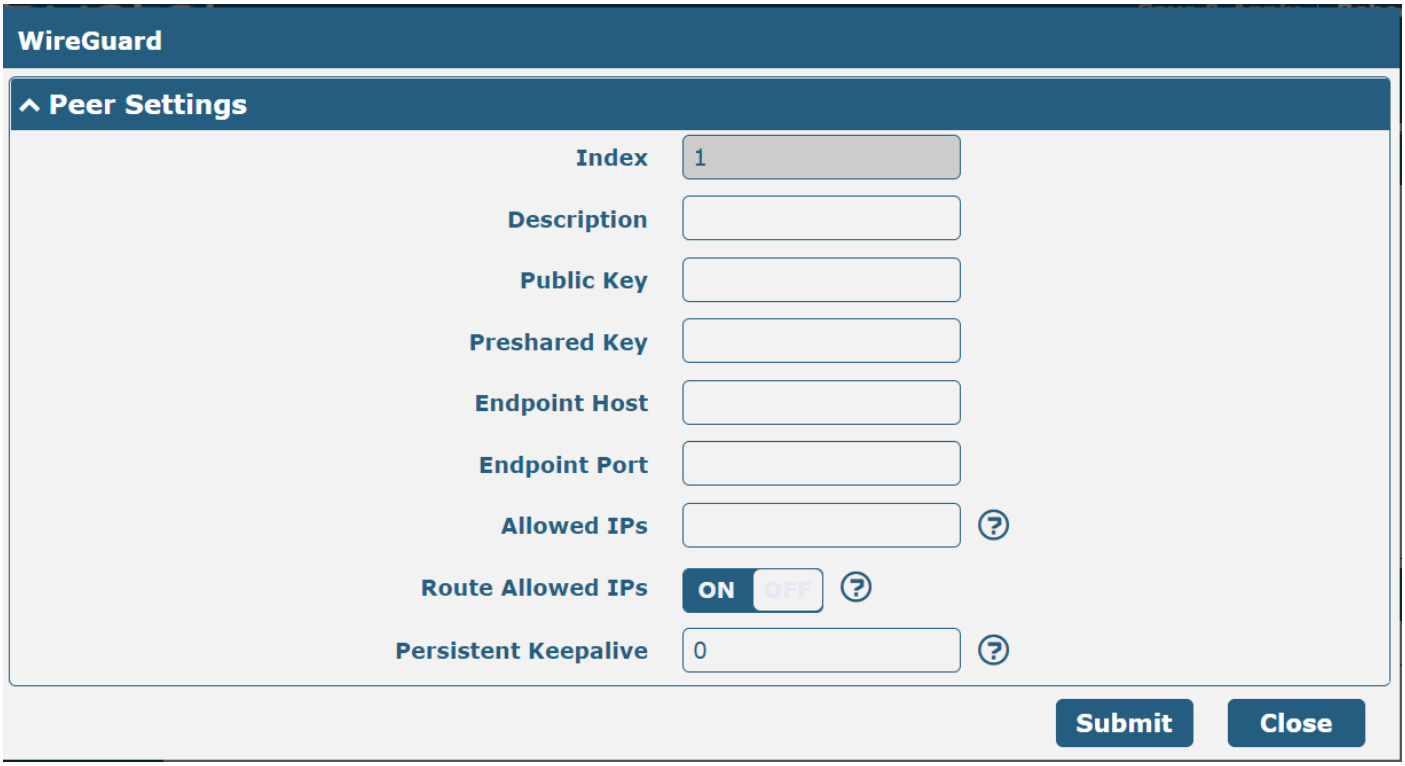


WireGuard@General 設定		
アイテム	説明	デフォルト
WireGuard を有効にする	WireGuard を有効または無効にする	オフ
秘密鍵	ローカル秘密キーを入力します。自動的に生成することも、X509 設定を使用して手動でインポートすることもできますが、空にすることはできません。	Null
IP アドレス	仮想インターフェイスの IP アドレスを入力します。空にすることはできません。	Null
リッスンポート	仮想インターフェイスのリスニングポートを入力します。空にすることはできません。	51820
MTU (英語)	仮想インターフェイスのスライス サイズを入力します。	1472
NAT を有効にする	NAT 機能を有効/無効にします。有効にすると、IP アドレスがインターフェイスの仮想 IP アドレスに変換されます。	オン

注: クリック するとヘルプが表示されます。



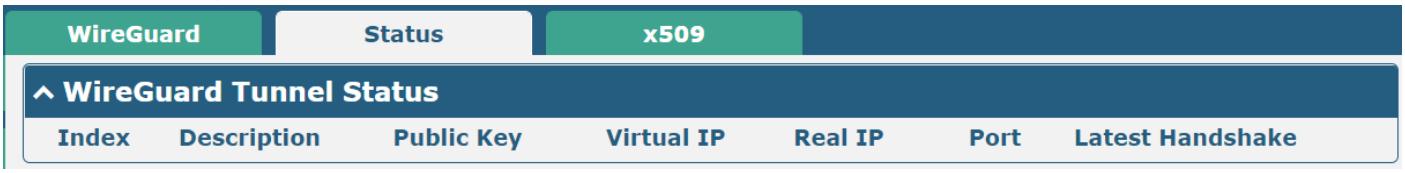
クリックすると＋、ピア設定が追加されます。最大数は **20 です**。



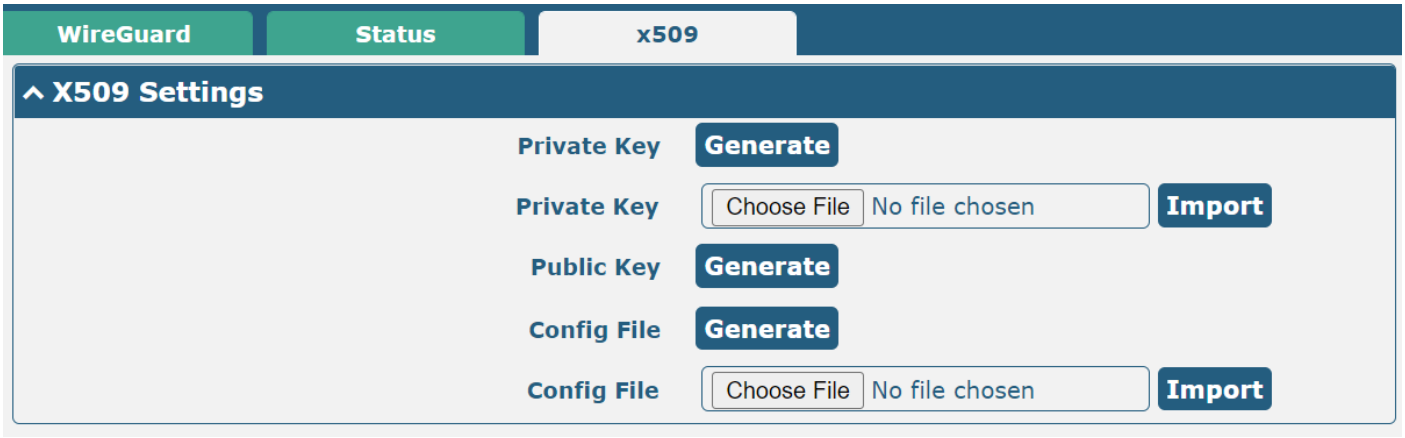
WireGuard@ピア設定		
アイテム	説明	デフォルト
ピア設定		
インデックス	インデックスを表示します。	--
説明	ピアの説明を入力します。	Null
公開鍵	公開鍵を入力し、空にすることはできません。	Null
事前共有キー	事前共有キーを入力し、空にすることはできません。	Null
エンドポイントホスト	ピアの IP アドレスを入力します。null 値を指定すると、接続要求は開始されません。	Null
エンドポイントポート(Endpoint Port)	ピア ポートを入力します。null 値を指定すると、接続要求は開始されません。	Null
許可された IP	許可された IP アドレスを入力しますが、空にすることはできません。	Null
許可された IP のルート	機能を有効/無効にします。有効にすると、このピアに許可されたネットワークのルートが作成されます。許可されたネットワークが 0.0.0.0/0 の場合、このピアがデフォルトルートとして設定されます。	オン
パーシステントキープアライブ	パーシステントキープアライブ メッセージの送信インターバルを秒単位で入力します。0 は、機能を無効にすることを意味します。	0

1) ステータス

ステータスバーでは、WireGuard の接続ステータスを表示できます。行の 1 つをクリックすると、そのリンク接続の詳細が現在の行の下に表示されます。



このセクションは、秘密鍵と公開鍵を生成またはインポートするために使用されます。



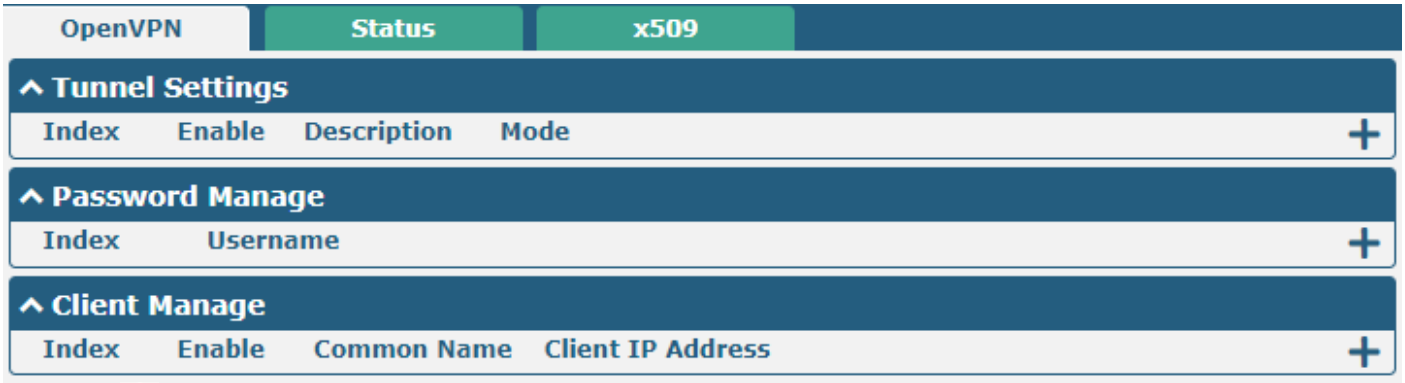
x509 の		
アイテム	説明	デフォルト
X509 設定		
秘密鍵	Generate ボタンをクリックして 秘密鍵を生成します。	--
秘密鍵	Choose File ボタンをクリックしてコンピュータから秘密鍵を見つけ、ボタンをクリックして Import 秘密鍵をインポートします。	--
公開鍵	Generate ボタンをクリックして 公開鍵を生成します。	--
構成ファイル	Generate ボタンをクリックして、設定ファイルを生成します	--
構成ファイル	ボタンをクリックしてコンピュータから Choose File 設定ファイルを探し、ボタンをクリックして設定ファイルを Import インポートします。	--

3.5.3 OpenVPN

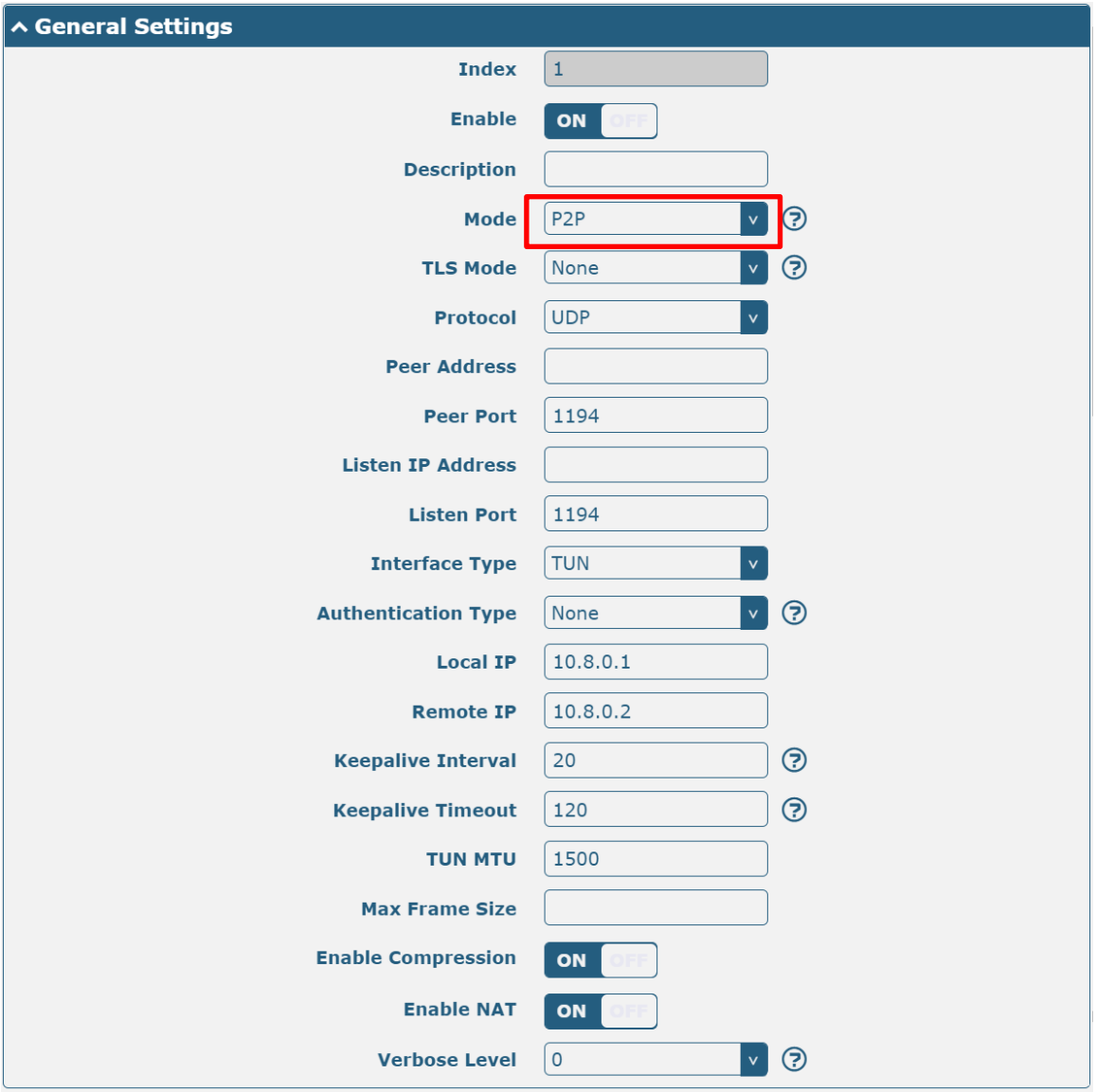
このセクションでは、OpenVPN と関連するパラメータを設定できます。OpenVPN は、 仮想プライベートネットワーク (VPN)ルーテッドまたはブリッジ構成およびリモートアクセス機能でセキュアなポイントツーポイント接続またはサイト間接続を作成するための手法。デバイス ポイント・ツー・ポイント接続とポイント・ツー・ポイント接続をサポートします。

「**VPN > OpenVPN > OpenVPN**」をクリックすると、以下のように表示されます。

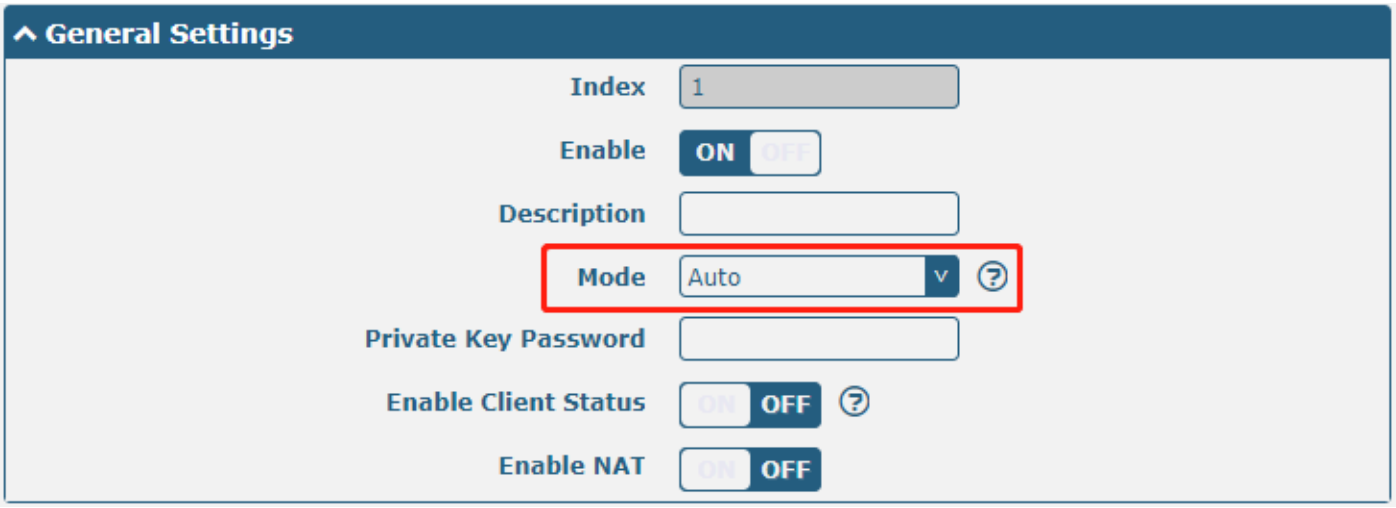
1) OpenVPN



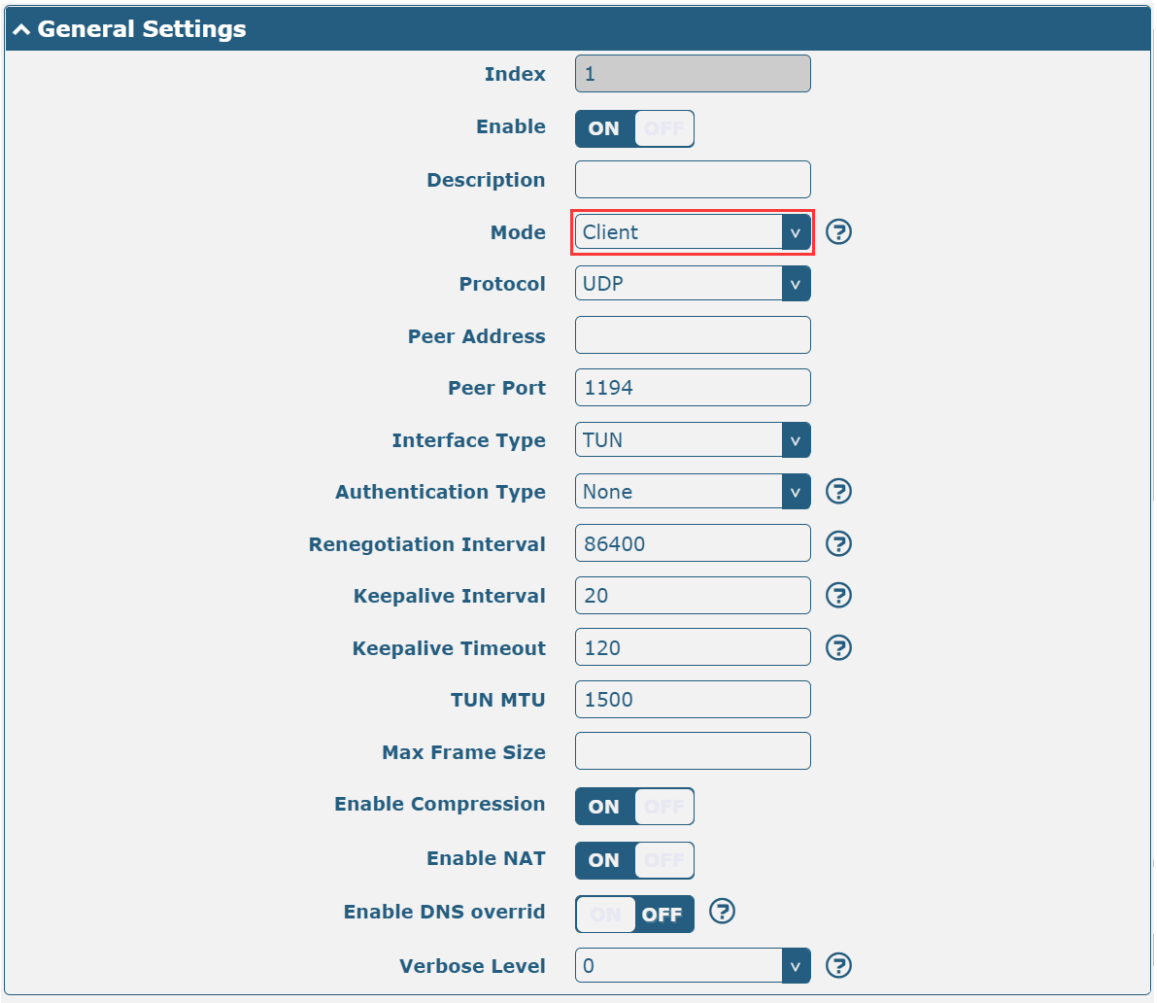
クリック＋すると、OpenVPN トンネルの設定が追加されます。最大数は **5 です**。「モード」はデフォルトで「P2P」に設定されています。モードとして「P2P」を選択すると、ウィンドウが下に表示されます。



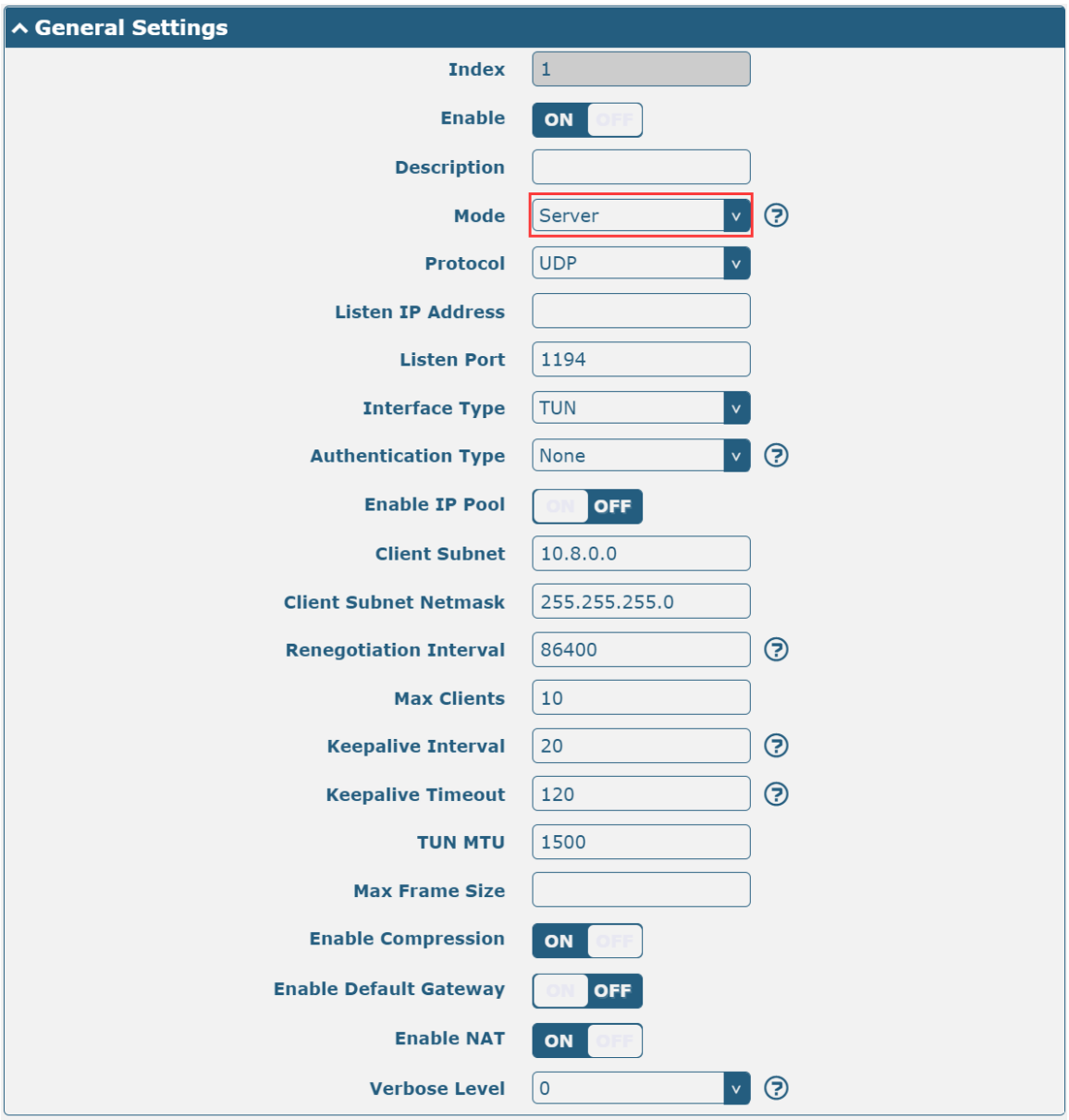
モードとして「自動」を選択すると、ウィンドウが下に表示されます。



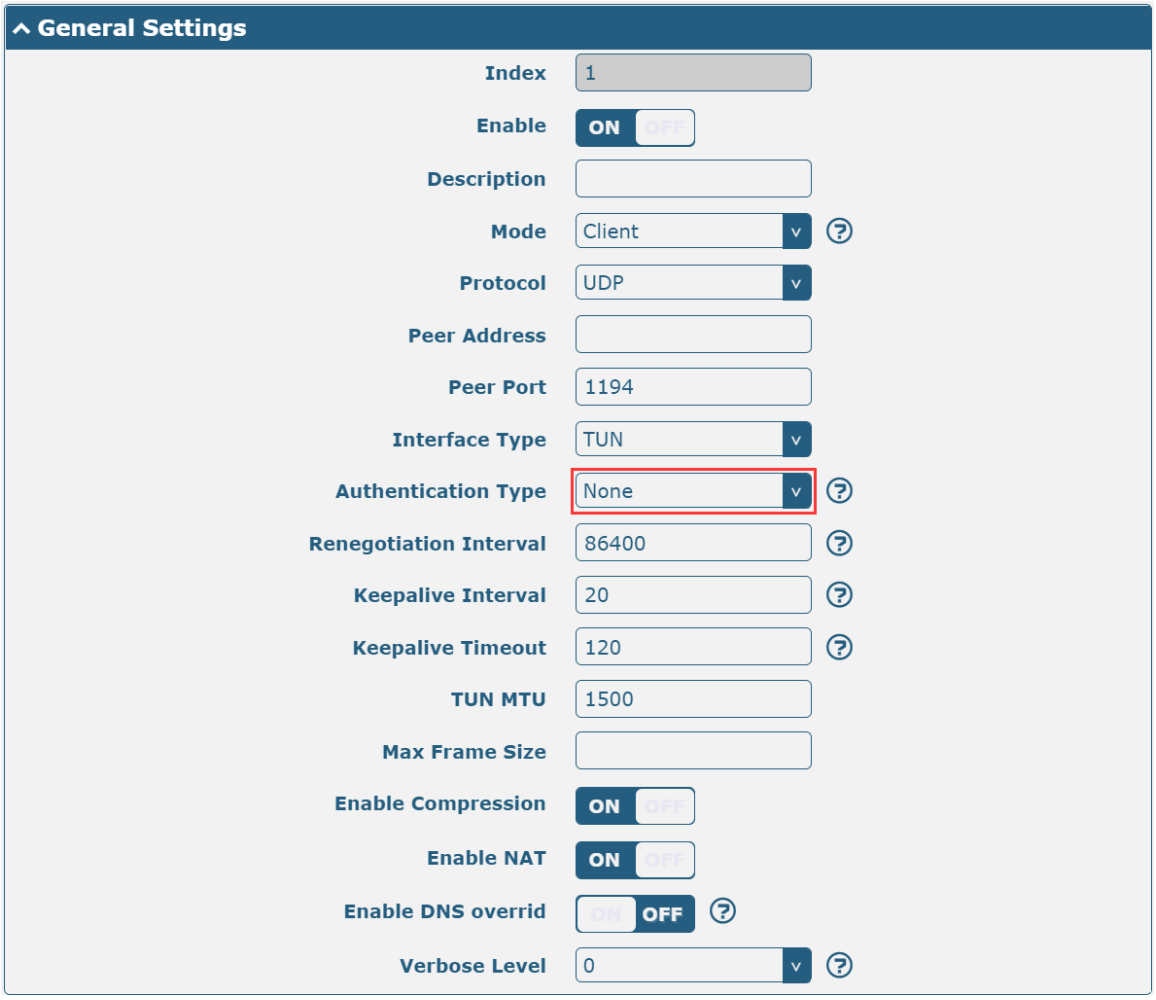
モードとして「クライアント」を選択すると、ウィンドウが下に表示されます。



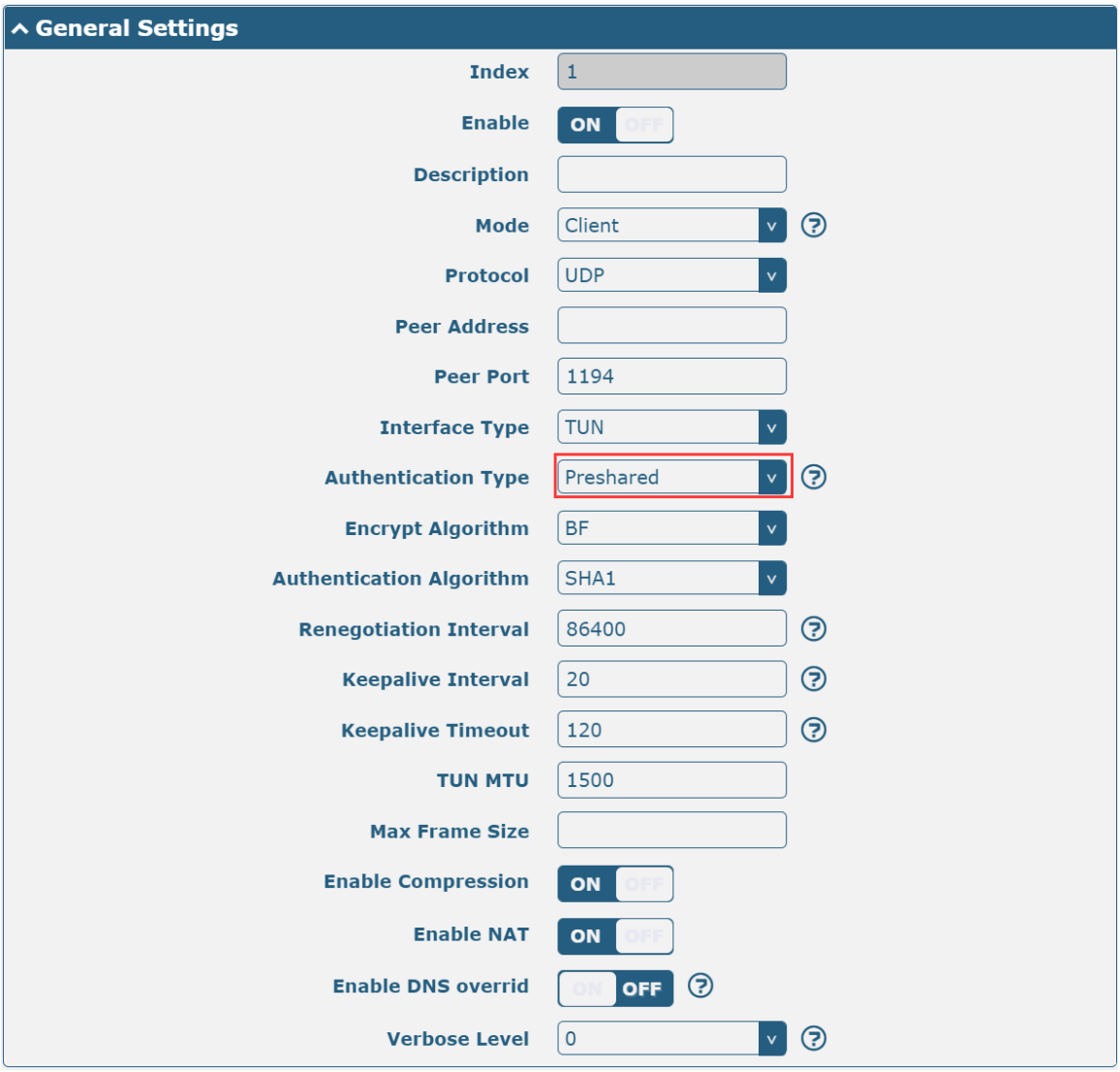
モードとして「サーバー」を選択すると、ウィンドウが下に表示されます。



認証タイプを「なし」にすると、以下のウィンドウが表示されます。

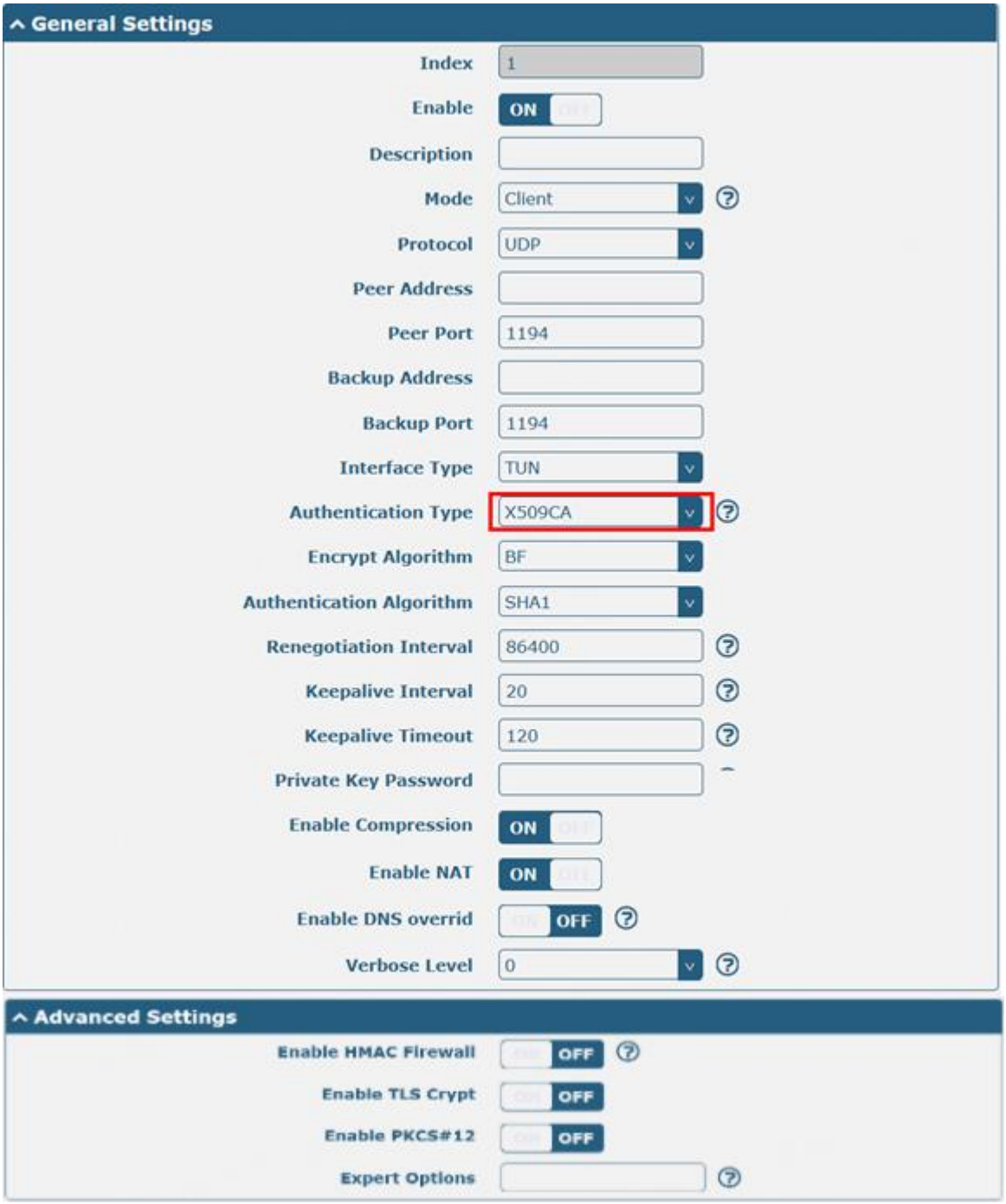


認証タイプとして「事前共有」を選択すると、ウィンドウが下に表示されます。



認証タイプとして「パスワード」を選択すると、以下のウィンドウが表示されます。

認証タイプに「X509CA」を選択すると、以下のウィンドウが表示されます。



認証タイプとして「X509CA Password」を選択すると、以下のウィンドウが表示されます。

一般 設定 @ OpenVPN		
アイテム	説明	デフォルト
インデックス	リストの序数を示します。	--
エネーブル	トグルボタンをクリックして、この OpenVPN トンネルを有効/無効にします。	オン
説明	この OpenVPN トンネルの説明を入力します。	Null

一般 設定 @ OpenVPN		
アイテム	説明	デフォルト
モード	「自動」、「P2P」、「クライアント」、「サーバー」から選択します。	P2P の
プロトコル	「UDP」、「TCP-Client」、「TCP-Server」から選択します。	UDP の
サーバー アドレス	リモート OpenVPN サーバーのエンドツーエンド IP アドレスまたはドメインを入力します。	Null
サーバ ポート	OpenVPN サーバーのエンドツーエンドリスナーポートまたはリスナーポートを入力します。	1194
リッスン IP アドレス	IP アドレスまたはドメイン名を入力します。	Null
リッスン ポート	この端にリスナーポートを入力します。	1194
インターフェイス タイプ	「TUN」と「TAP」は、OpenVPN 用の 2 種類のデバイスインターフェースから選択します。TUN デバイスと TAP デバイスの違いは、TUN デバイスがネットワーク上のポイントツーポイント仮想デバイスであるのに対し、TAP デバイスはイーサネット上の仮想デバイスである 点です。	TUN の
ユーザー名	「パスワード」または「X509CA パスワード」認証タイプに使用するユーザー名を入力します。	Null
パスワード	認証タイプ「パスワード」または「X509CA パスワード」に使用するパスワードを入力します。	Null
認証 の種類	「なし」、「事前共有」、「パスワード」、「X509CA」、「X509CA パスワード」から選択します。 *注: 「なし」および「事前共有」認証 タイプは、P2P モードでのみ機能します。*	何一つ
IP プールの有効化	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、クライアントはアドレス プールから仮想 IP を取得します。 *注:[Enable IP Pool]は、[Mode]が[Server]の場合のみ使用できます。*	オフ
ローカル IP	ローカル仮想 IP を入力します。	10.8.0.1
リモート IP	リモート仮想 IP を入力します。	10.8.0.2
クライアント サブネット	クライアントの仮想 IP ネットワーク アドレス。	10.8.0.0
クライアント サブネット ネットマスク	クライアント仮想 IP ネットワーク アドレス マスク。	255.255.255.0

一般 設定 @ OpenVPN		
アイテム	説明	デフォルト
暗号化 アルゴリズム	「BF」、「DES」、「DES-EDE3」、「AES-128」、「AES-192」、「AES-256」から選択します。 • BF: CBC モードで 128 ビットの BF 暗号化アルゴリズムを使用します。 • DES: CBC モードで 64 ビットの DES 暗号化アルゴリズムを使用します。 • DES-EDE3: CBC モードで 192 ビット 3DES 暗号化アルゴリズムを使用 • AES128: CBC モードで 128 ビットの AES 暗号化アルゴリズムを使用 • AES192: CBC モードで 192 ビットの AES 暗号化アルゴリズムを使用 • AES256: CBC モードで 256 ビットの AES 暗号化アルゴリズムを使用	BF の
認証アルゴリズム	「MD5」、「SHA1」、「SHA256」、「SHA384」、「SHA512」から選択します。	SHA1 の
最大クライアント数	保持タイムアウトを設定します。この間、接続がタイムアウトし続けると、OpenVPN トンネルが再確立されます。 *注: [Max Clients] は [Mode] が [Server] の場合のみ使用できます。*	10
再ネゴシエーションインターバル	再ネゴシエーションインターバルを設定します。 接続に失敗した場合、再ネゴシエーションインターバルに達すると OpenVPN は再ネゴシエ ートします。	86400
キープアライブインターバル (Keepalive Interval)	キープアライブ (ping) インターバルを設定して、トンネルがアクティブかどうかを確認します。	20
キープアライブ タイムアウト (Keepalive Timeout)	キープアライブ タイムアウトを設定します。リモートから ping またはその他のパケットを受信せずに n 秒が経過した後、OpenVPN の再起動をトリガーします。	120
TUN MTU	トンネルの MTU を設定します。	1500
最大フレーム サイズ(Max Frame Size)	トンネル経由で送信するデータのシャードサイズを設定します。	Null
秘密キーのパスワード	「X509CA」および「X509CA パスワード」認証の下に秘密鍵のパスワードを入力します。	Null
圧縮を有効にする	スイッチボタンをクリックして、このオプションを有効/無効にします。この機能を有効にすると、IP パケットのヘッダーが圧縮されます。	オン
DNS オーバーライドを有効にする	スイッチボタンをクリックして、このオプションを有効/無効にします。有効にすると、サーバーによってプッシュされた DNS がローカル DNS サーバーとして受信されます。	オフ
ブリッジの有効化 LAN0 (LAN0)	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、仮想インターフェイスを Lan0 でブリッジできます。 *注: LAN0 でブリッジを有効にするには、「モード」がクライアントである場合にのみ使用できます。*	オン
デフォルトを有効にする ゲートウェイ	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、サーバーによってプッシュされたゲートウェイをローカルゲートウェイとして受信します。	オフ

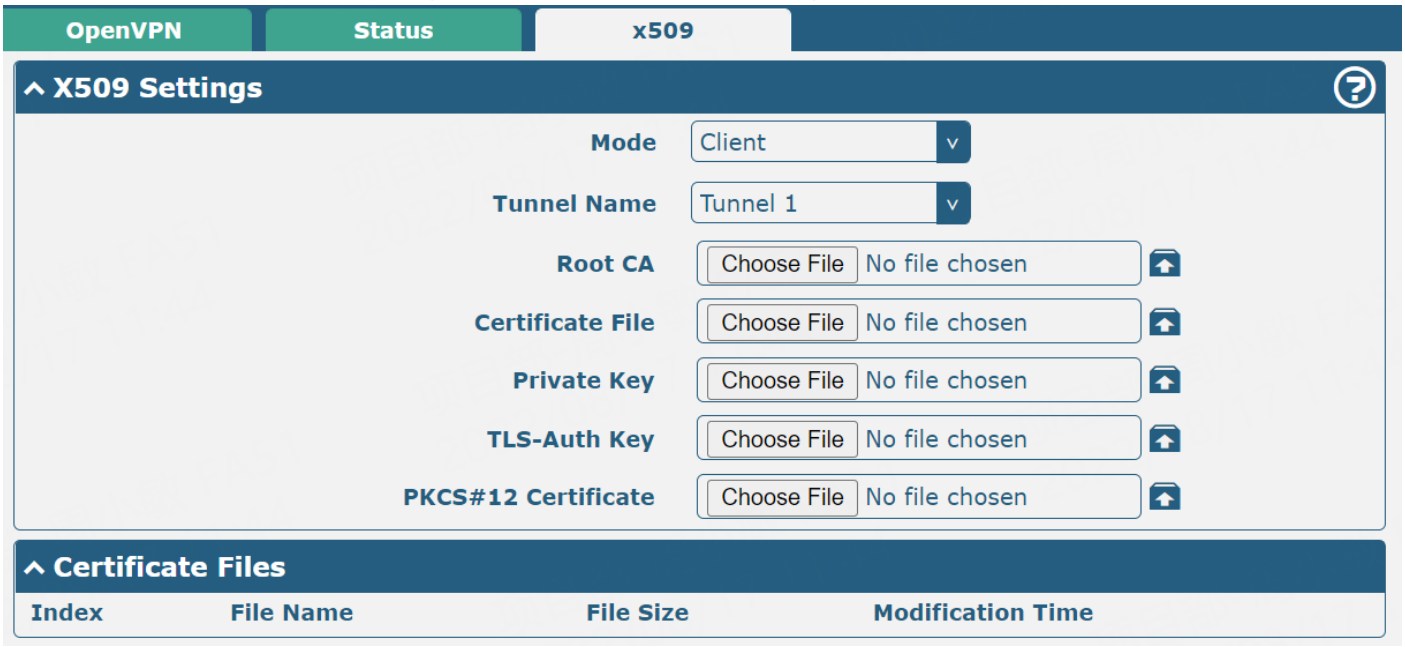
一般 設定 @ OpenVPN		
アイテム	説明	デフォルト
クライアントステータスの有効化	切り替えボタンをクリックして、このオプションを有効/無効にします。サーバーが使用可能になると、接続されているクライアントのステータス情報を表示できます。	オフ
NAT を有効にする	トグルボタンをクリックして、NAT オプションを有効/無効にします。有効にすると、リモート OpenVPN クライアントにアクセスする前に、デバイスの背後にあるホストの送信元 IP アドレスが偽装されます。	オフ
詳細レベル	出力ログのレベルと値を 0 から 11 まで選択します。 • 0: 致命的なエラー以外の出力はありません • 1~4: 通常の使用範囲 • 5: パケットの読み取りと書き込みごとに R 文字と W 文字をコンソールに出力します。 • 6~11: デバッグ情報範囲	0
詳細 設定 @ OpenVPN		
アイテム	**説明**	**デフォルト**
HMAC ファイアウォールを有効にする	切り替えボタンをクリックして、このオプションを有効/無効にします。 DoS 攻撃から保護するために、TLS 制御チャネルの上に HMAC 認証のレイヤーを追加します。	オフ
TLS 暗号化を有効にする	トグルボタンをクリックして、TLS 暗号化プロトコルを有効/無効にします。TLS Crypt は、OpenVPN のセキュリティを強化するためのオプションであり、より高度なセキュリティを提供します。	オフ
PKCS#12 の有効化	トグルボタンをクリックして、PKCS#12 証明書を有効または無効にします。 これは 、個人の識別情報を記述するために使用されるデジタル証明書暗号化標準の交換です。	オフ
nsCertType を有効にする	切り替えボタンをクリックして、nsCertType を有効/無効にします。 ピア証明書が「server」の明示的な nsCertType 指定で署名されていることを要求します。	オフ
エキスパートオプション	このフィールドに OpenVPN の他のオプションを入力します。各表現で区切ることができます。';'.	Null

2) ステータス

このセクションでは、OpenVPN トンネルのステータスを表示できます。

3) x509

このセクションは、CA などの証明書をインポートするために使用されます。



x509		
アイテム	説明	デフォルト
X509 設定		
トンネル名(Tunnel Name)	有効なトンネルを選択します。「トンネル 1」、「トンネル 2」、「トンネル 3」、「トンネル 4」、「トンネル 5」、「トンネル 6」から 選択します。	トンネル 1
モード	トンネルで選択したモード	クライアント
ルート CA	「ファイルの選択」をクリックしてルート CA ファイルを見つけ、このファイルをデバイスにインポートします。	--
証明書ファイル	「ファイルの選択」をクリックして証明書ファイルを見つけ、このファイルをデバイスにインポートします。	--
秘密鍵	「ファイルを選択」をクリックして秘密鍵ファイルを見つけ、このファイルをデバイスにインポートします。	--
TLS-認証キー	「ファイルの選択」をクリックして TLS 認証キーファイルを見つけ、このファイルをデバイスにインポートします。	--

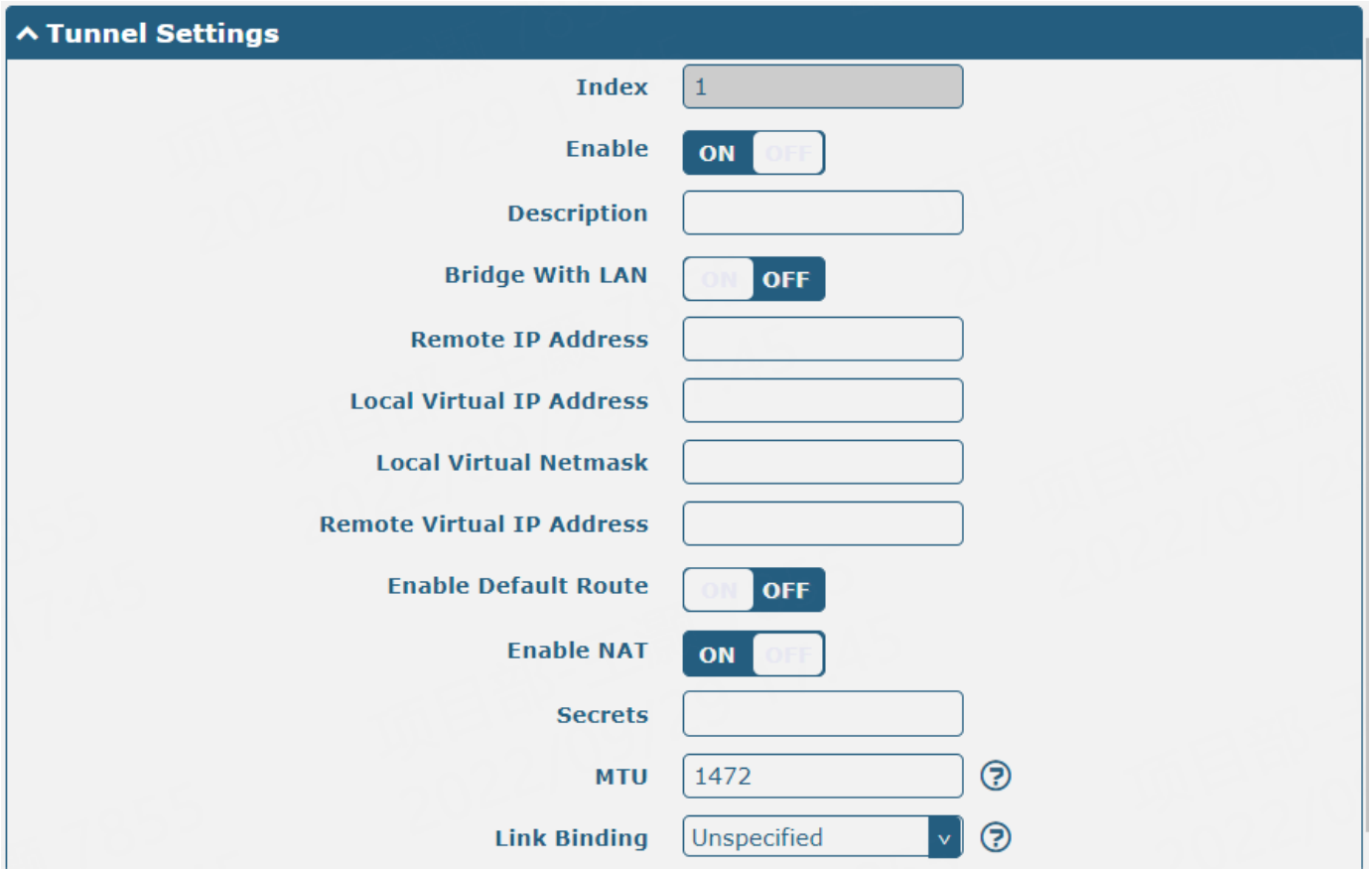
x509		
アイテム	説明	デフォルト
X509 設定		
PKCS#12 証明書	[ファイルの選択] をクリックして PKCS#12 証明書ファイルを見つけ、このファイルをデバイスにインポートします。	--
証明書ファイル		
インデックス	リストの序数を示します。	--
ファイル名	インポートされた証明書の名前を表示します。	Null
ファイルサイズ	証明書ファイルのサイズを表示します。	Null
変更時刻	証明書ファイルを最後に変更したときのタイムスタンプを表示します。	Null

3.5.4 GRE

このセクションでは、GRE のおよび関連するパラメータ。Generic Routing Encapsulation(GRE)は、トンネリングプロトコルそれはできるカプセル化多種多様なネットワーク層プロトコル内部仮想ポイント・ツー・ポイント・リンクインターネットプロトコルネットワーク。GRE プロトコルには、内部プロトコルカプセル化とプライベートアドレスカプセル化の 2 つの主な用途があります。

1) GRE

クリック + すると、トンネル設定を追加できます。最大数は **5 です**。

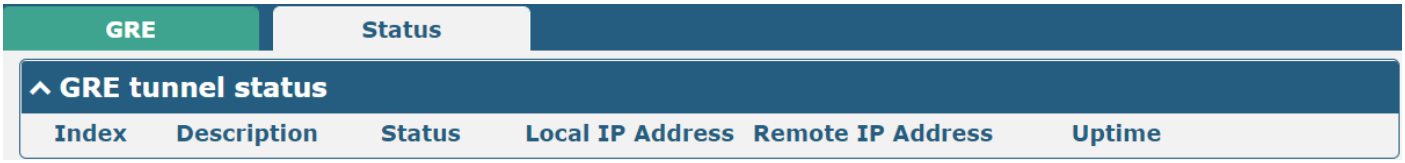


トンネル設定@ GRE		
アイテム	説明	デフォルト
インデックス	リストの序数を示します。	--
エネーブル	トグルボタンをクリックして、この GRE トンネルを有効/無効にします。 GRE(Generic Routing Encapsulation)は、IP ネットワーク内の他のプロトコルのパケットをルーティングできるように、データパケットをカプセル化するプロトコルです。	オン
説明	この GRE トンネルの説明を入力します。	Null
LAN によるブリッジ	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、仮想インターフェイスを lan0 でブリッジできます。	オフ
リモート IP アドレス	GRE トンネルの リモート実 IP アドレスを設定します。	Null
ローカル仮想 IP アドレス	GRE トンネルのローカル仮想 IP アドレスを設定します。	Null
ローカル仮想ネットマスク	GRE トンネルのローカル仮想ネットマスクを設定します。	Null
リモート 仮想 IP アドレス	GRE トンネルのリモート仮想 IP アドレスを設定します。	Null
デフォルトルートの有効化	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、ゲートウェイのすべてのトラフィックが GRE VPN を通過します。	オフ
NAT を有効にする	切り替えボタンをクリックして、このオプションを有効/無効にします。 このオプションは、デバイスが NAT 環境下にある場合に有効にする必要があります。	オン
シークレッツ	GRE トンネルにキーを設定します。	Null

MTU (英語)	「Maximum Transmission Unit」と入力します。	1472
リンクバインディング	GRE を構築するためのリンクを選択します。	自由

2) ステータス

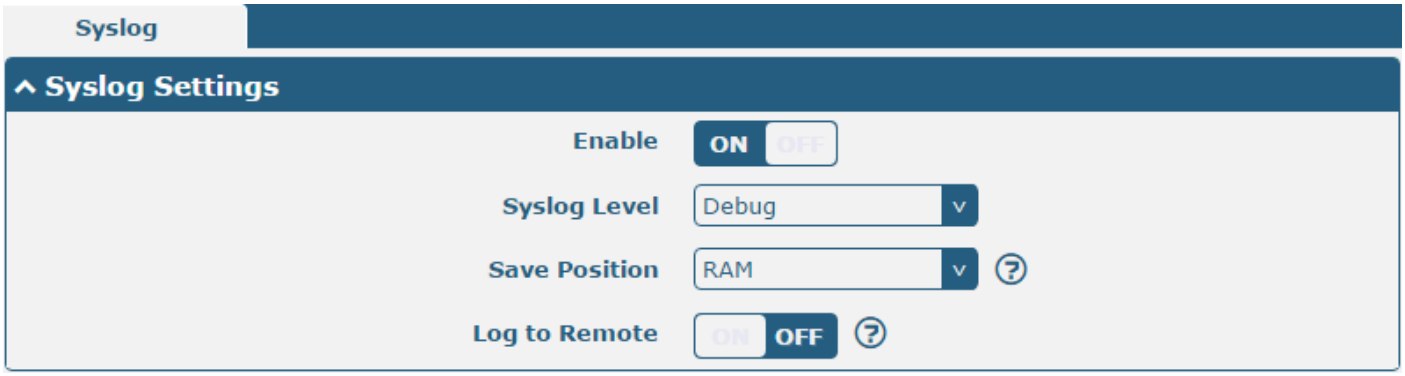
このセクションでは、GRE トンネルのステータスを表示できます。



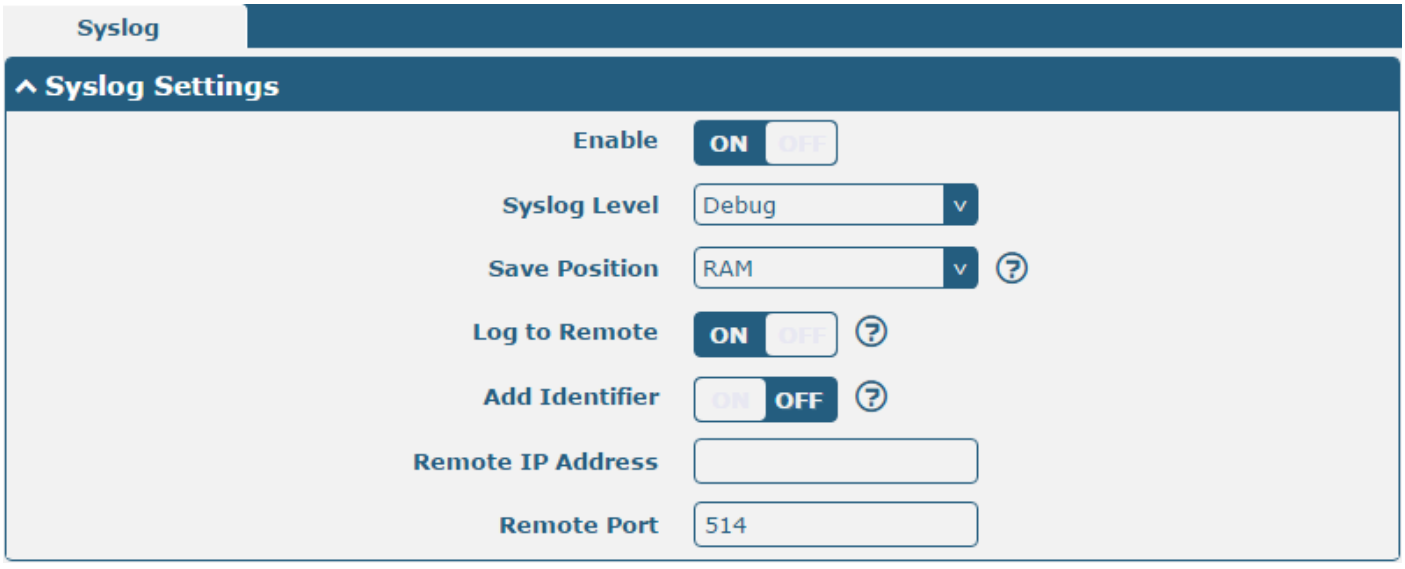
3.6 サービス

3.6.1 Syslog

このセクションでは、Syslog パラメータを設定できます。デバイスのシステムログはローカルに保存でき、リモートログサーバーへの送信やアプリケーションのデバッグもサポートしています。デフォルトでは、「リモートにログ」オプションは無効になっています。



「リモートにログ」オプションを有効にすると、ウィンドウが下に表示されます。

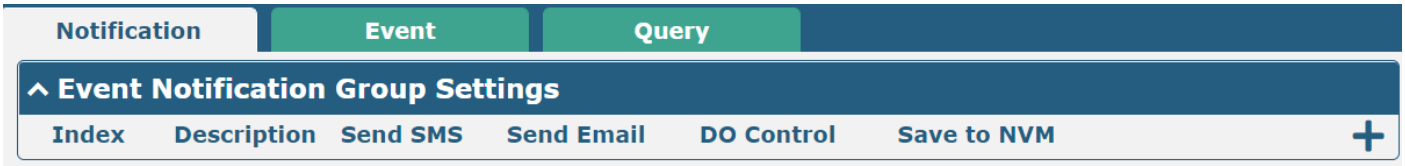


Syslog 設定		
アイテム	説明	デフォルト
エネーブル	トグルボタンをクリックして、Syslog 設定オプションを有効または無効にします。	オン
Syslog レベル	「Debug」、「Info」、「Notice」、「Warning」、「Error」のいずれかを低 から高から選択します。下位レベルは、より詳細な Syslog を出力します。	デバッグ
位置を保存	保存位置を「RAM」、「NVM」、または「コンソール」から選択します。 「RAM」を選択すると、再起動後にデータが消去されます。 *注:Syslog を NVM(不揮発性メモリ)に長期間保存することは推奨されません。*	ラム
リモートにログを記録	切り替えボタンをクリックして、このオプションを有効/無効にします。 デバイスがリモート Syslog サーバに Syslog を送信できるようにします。 Syslog サーバーの IP とポートを入力する必要があります。	オフ
識別子を追加	切り替えボタンをクリックして、このオプションを有効/無効にします。 有効にすると、Syslog を RobustLink にロードするために使用されるシリアル番号を Syslog メッセージに追加できます。	オフ
リモート IP アドレス	「Log to Remote」オプションを有効にするときに、Syslog サーバーの IP アドレスを入力します。	Null
リモートポート	「Log to Remote」オプションを有効にするときに、Syslog サーバーのポートを入力します。	514

3.6.2 イベント

このセクションでは、イベントパラメータを設定できます。 イベント機能は、特定のシステムイベントが発生したときに SMS または電子メールでアラートを送信できます。

1) 通知



+ボタンをクリックして、イベントパラメータを追加します。

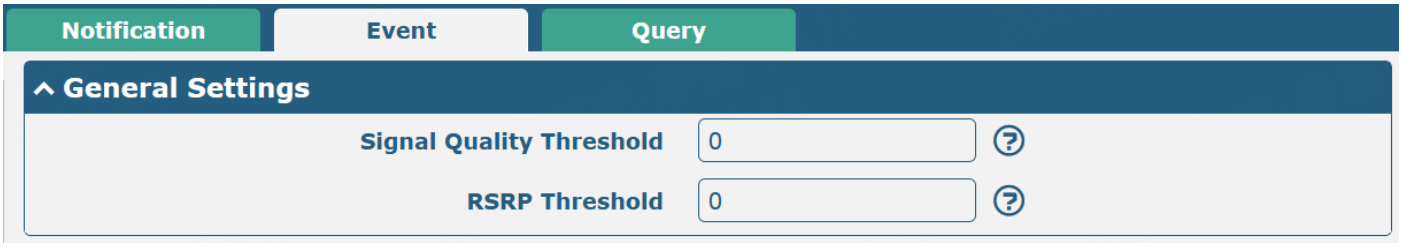
一般設定 @ 通知		
アイテム	説明	デフォルト
インデックス	リストの序数を示します。	--
説明	このグループの説明を入力します。	Null
送信済み SMS	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、イベントが発生した場合、デバイスは 指定された電話番号に SMS 経由で通知 を送信します。関連するポイント番号 を「**3.6.5 Services > Email**」を使用し、「;' を使用して各数値を区切ります。	オフ
メールを送る	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、イベントが発生した場合、デバイスは 指定された電子メールボックスに電子メールで通知 を送信します。関連するメールアドレスを「**3.6.5 電子メール>サービス**」を参照してください。	オフ
DO 制御	切り替えボタンをクリックして、このオプションを有効/無効にします。電源を入れると、イベントデバイスは対応する DO に Low/High レベルの形式で送信します。	オフ
NVM に保存	切り替えボタンをクリックして、このオプションを有効/無効にします。イベントを不揮発性メモリに保存できるようにします。	オフ

Event Selection

System Startup	OFF
System Reboot	OFF
System Time Update	OFF
Configuration Change	OFF
Cellular Network Type Change	OFF
Cellular Data Stats Clear	OFF
Cellular Data Traffic Overflow	OFF
Poor Signal Quality	OFF
Wan data traffic stats clear	OFF
Wan data traffic overflow	OFF
Link Switching	OFF
WAN Up	OFF
WAN Down	OFF
WLAN Up	OFF
WLAN Down	OFF
WWAN Up	OFF
WWAN Down	OFF
IPSec Connection Up	OFF
IPSec Connection Down	OFF
OpenVPN Connection Up	OFF
OpenVPN Connection Down	OFF
LAN Port Link Up	OFF
LAN Port Link Down	OFF
USB Device Connect	OFF
USB Device Remove	OFF
DDNS Update Success	OFF
DDNS Update Fail	OFF
Received SMS	OFF
SMS Command Execute	OFF
DI 1 ON	OFF
DI 1 OFF	OFF
DI 1 Counter Overflow	OFF

2) イベント

このセクションでは、イベントを設定できます。



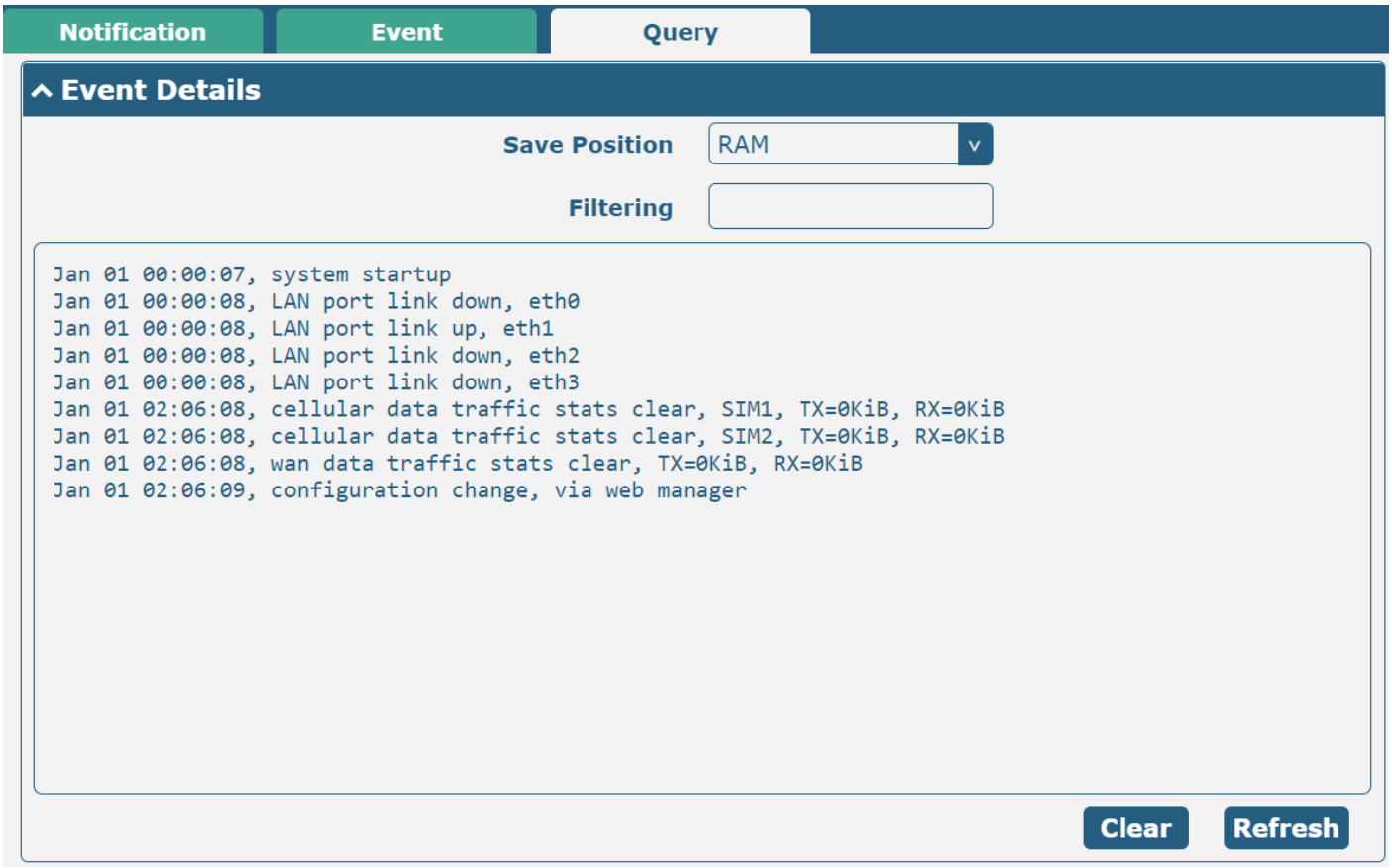
一般設定 @ イベント		
アイテム	説明	デフォルト
信号品質しきい値	信号品質のしきい値 を設定します。デバイスは、実際のしきい値が指定されたしきい値を下回る と、ログイベントを生成します。 0 は、このオプションを無効にすることを意味します。	0
RSRP しきい値(RSRP Threshold)	信号品質のしきい値を設定します。実際のしきい値が指定された RSRP しきい値よりも小さい場合、デバイスはログ イベントを生成します。0 を指定すると、このオプションは無効になります。このオプションは、5G ネットワーク専用です。	0

3) クエリ

次のウィンドウでは、 さまざまなタイプのイベントレコードを照会できます。

クリック Refresh すると、フィルタリングされたイベントが照会されます。

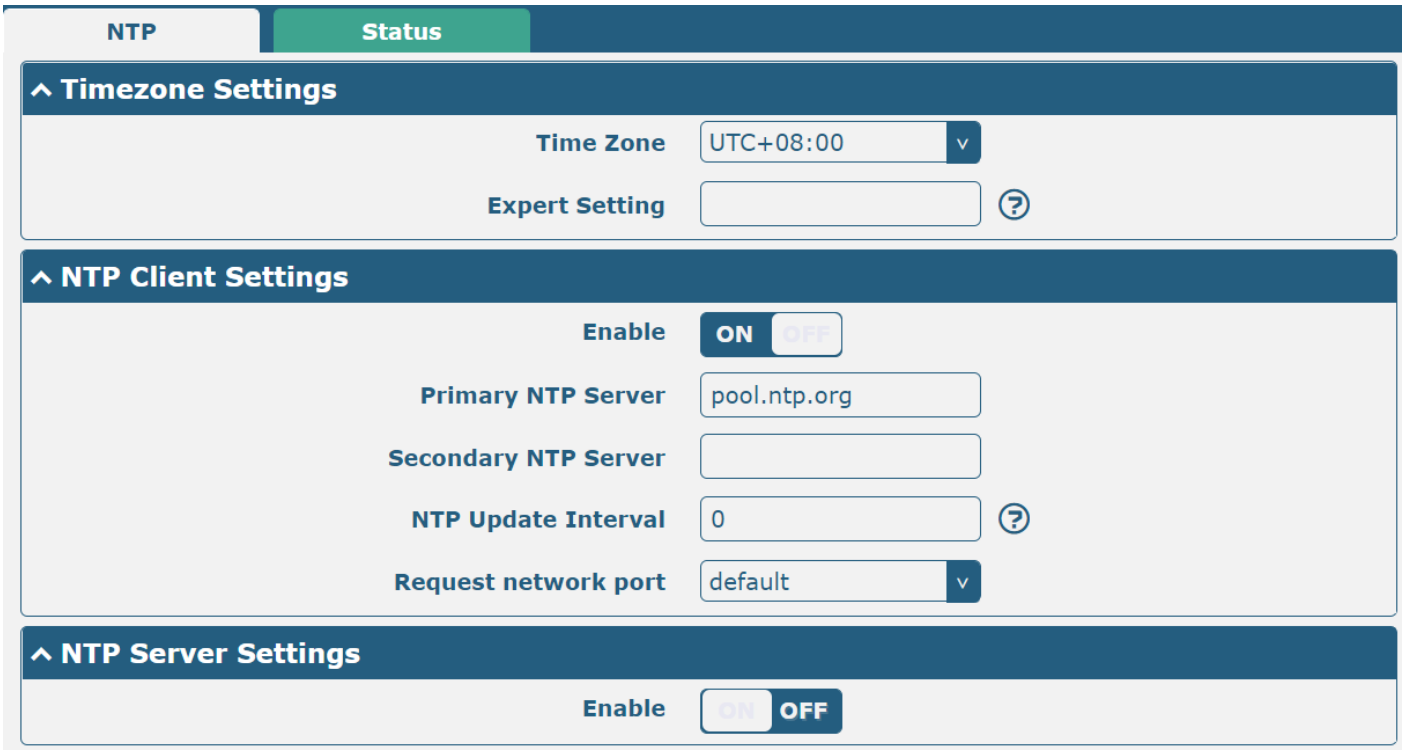
クリック Clear すると、ウィンドウ内のイベントレコードがクリアされます。



イベントの詳細はこちら		
アイテム	説明	デフォルト
位置を保存	イベントの保存位置を「RAM」または「NVM」から選択します 。 • RAM:ランダムアクセスメモリ。 • NVM: 不揮発性メモリ。	ラム
フィルタリング	ユーザーが設定したキーワードに基づいてフィルタリングメッセージを入力します。「更新」ボタンをクリックすると、フィルタリングされたイベントが次のボックスに表示されます。 message1&message2 のように、複数のフィルター メッセージを区切るには "&" を使用します。	Null

3.6.3 NTP

このセクションでは、関連する NTP(Network Time Protocol)パラメータを設定できます。

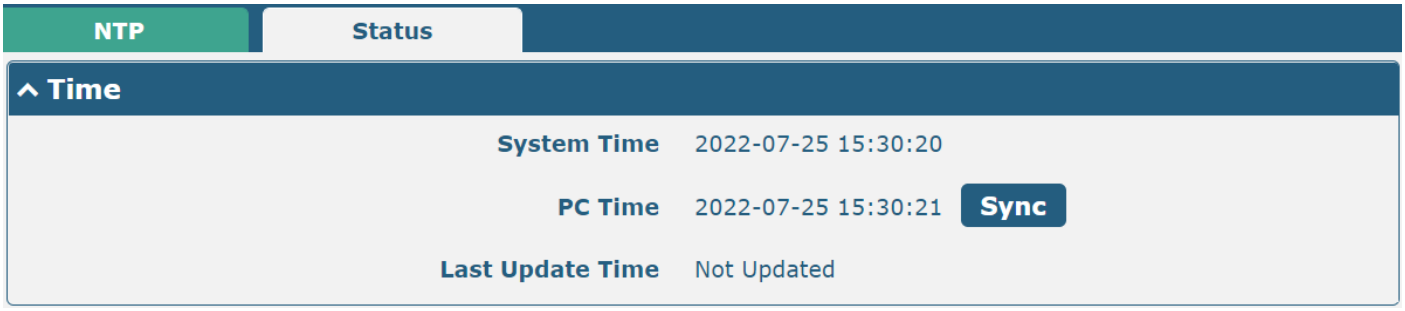


NTP の		
アイテム	説明	デフォルト
タイムゾーン設定		
タイム ゾーン	ドロップダウンリストをクリックして、現在のタイムゾーンを選択します。	UTC+08:00
エキスパート設定	夏時間でタイムゾーンを TZ 環境変数形式で指定します。この場合、「タイム・ゾーン」オプションは無視されます。	Null
NTP クライアント設定		
エネーブル	切り替えボタンをクリックして、このオプションを有効/無効にします。 NTP サーバと時刻を同期できるようにします。	オン
プライマリ NTP サーバ	プライマリ NTP サーバの IP アドレスまたはドメイン名を入力します。	pool.ntp.org
セカンダリ NTP サーバ(Secondary NTP Server)	セカンダリ NTP サーバの IP アドレスまたはドメイン名を入力します。	Null
NTP 更新インターバル	NTP クライアント時刻を NTP サーバと同期するインターバル(分)を入力します。分は次の更新を待機し、0 は 1 回だけ更新されることを意味します。	0
ネットワークポートの要求	「デフォルト」または「LAN」 からネットワークポートを要求するを選択します。	デフォルト
NTP サーバ設定		
エネーブル	トグルボタンをクリックして、NTP サーバオプションを有効/無効にします。	オフ

1) ステータス

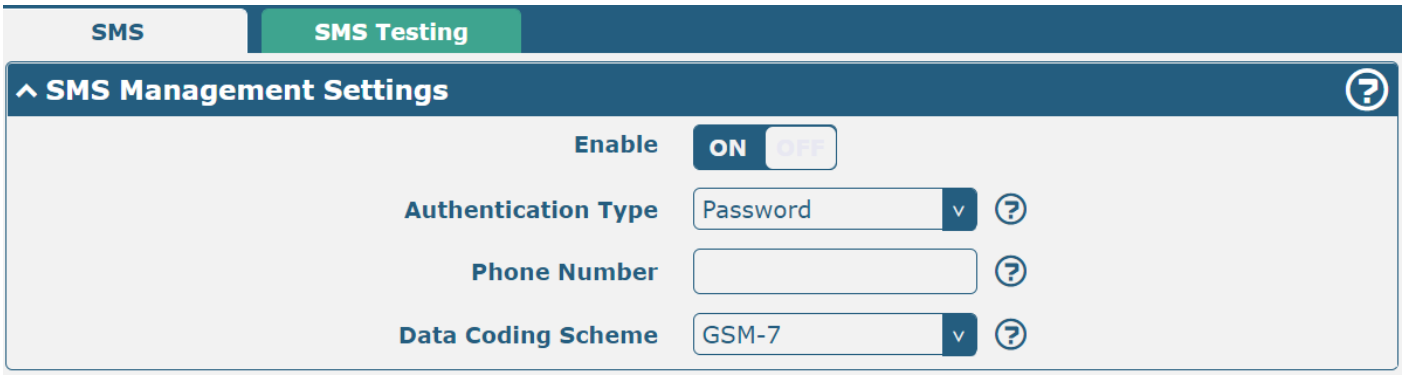
このウィンドウでは、デバイスの現在の時刻を表示 したり、デバイスの時刻を同期したりできます。

Sync ボタンをクリックして、デバイスの時刻を PC の時刻と同期させます。



3.6.4 SMS

このセクションでは、SMS パラメータを設定できます。デバイスは SMS 管理をサポートしていますが表示され、ユーザーは SMS を送信してデバイスを制御および構成できます。 SMS 制御の詳細については、 [4.1.2 SMS リモートコントロール](#).



SMS 管理設定		
アイテム	説明	デフォルト
エネーブル	トグルボタンをクリックして、SMS 管理オプションを有効/無効にします。 *注: このオプションが無効になっている場合、SMS 設定は無効です。*	オン
認証の種類	認証タイプを「パスワード」、「電話番号」、または「両方」から選択します。 • パスワード:認証には、WEB マネージャーと同じユーザー名とパスワードを使用します。たとえば、SMS の形式は「username:password;cmd1 です。cmd2 です。...」 ***注意:** 設定 WEB [システム>ユーザー管理] セクションで**マネージャー のパスワード。*** • Phonenum: 認証に電話番号を使用し、ユーザーは SMS 管理に許可される電話番号を設定する 必要があります。 SMS の形式は「cmd1;cmd2 です。...」 • 両方: 認証に「パスワード」と「電話番号」の両方を使用します。ユーザーは、 SMS 管理に許可される電話番号を設定する必要があります。 SMS の形式は「ユーザー名:パスワード;cmd1 です。cmd2 です。...」	パスワード
電話番号	SMS 管理に使用する電話番号を設定し、';'を使用して各数値を区切りま	Null

	す。 *注: 認証タイプとして「パスワード」を選択した場合は、null にすることができます。*	
データ符号化方式	Data Coding Scheme を「GSM-7」または「ucs2」から選択します。	GSM-7 型

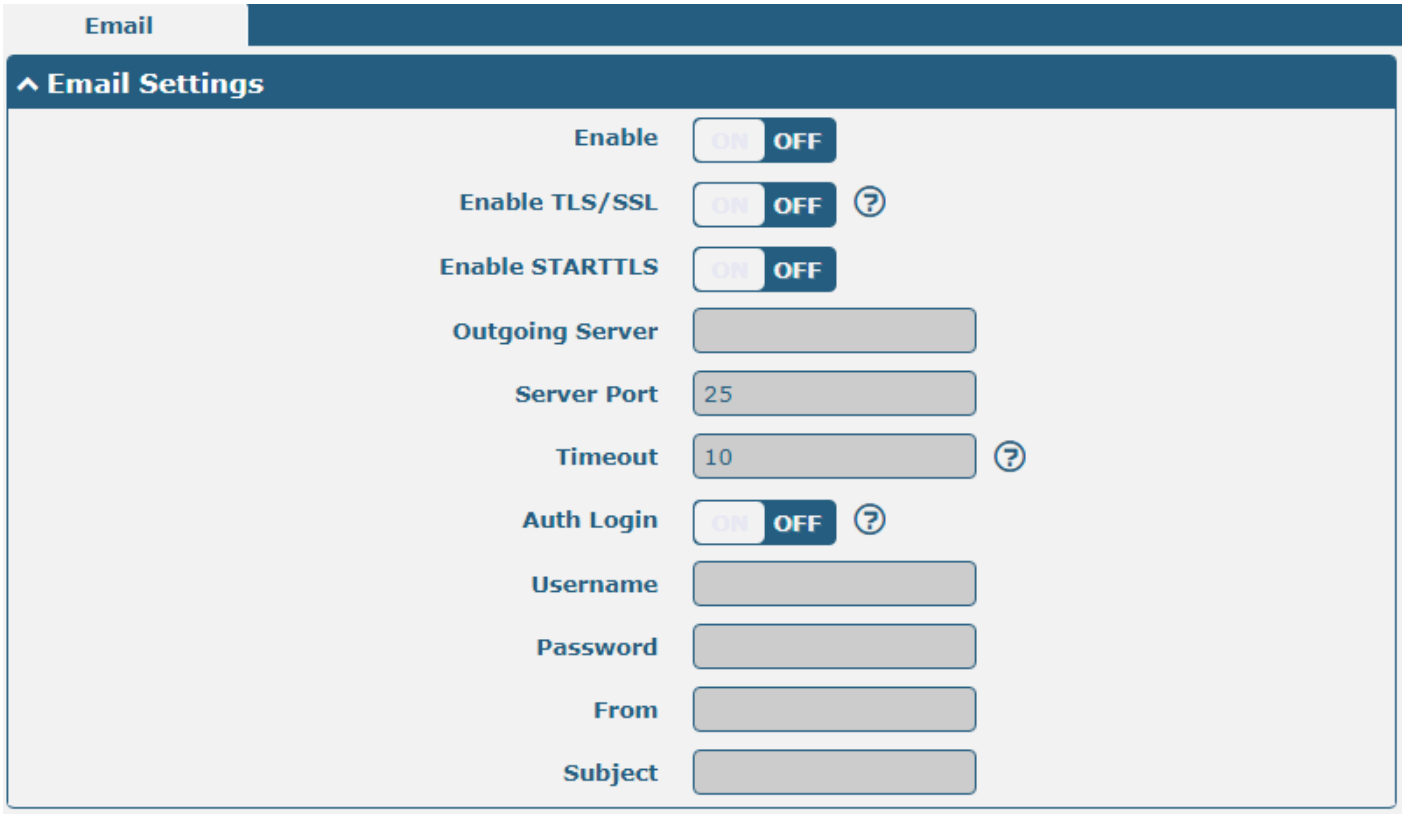
1) SMS テスト

このセクションでは、現在の SMS サービスが利用可能かどうかをテストできます。

SMS テスト		
アイテム	説明	デフォルト
電話番号	デバイスから SMS を受信できる指定された電話番号を入力します。	Null
メッセージ	デバイスが指定した電話番号に送信するメッセージを入力します。	Null
結果	SMS テストの結果が結果ボックスに表示されます。	Null
Send	ボタンをクリックして、テストメッセージを送信します。	--

3.6.5 電子メール

電子メール機能は、指定された受信者に電子メールを介してイベント通知 を送信することをサポートします。



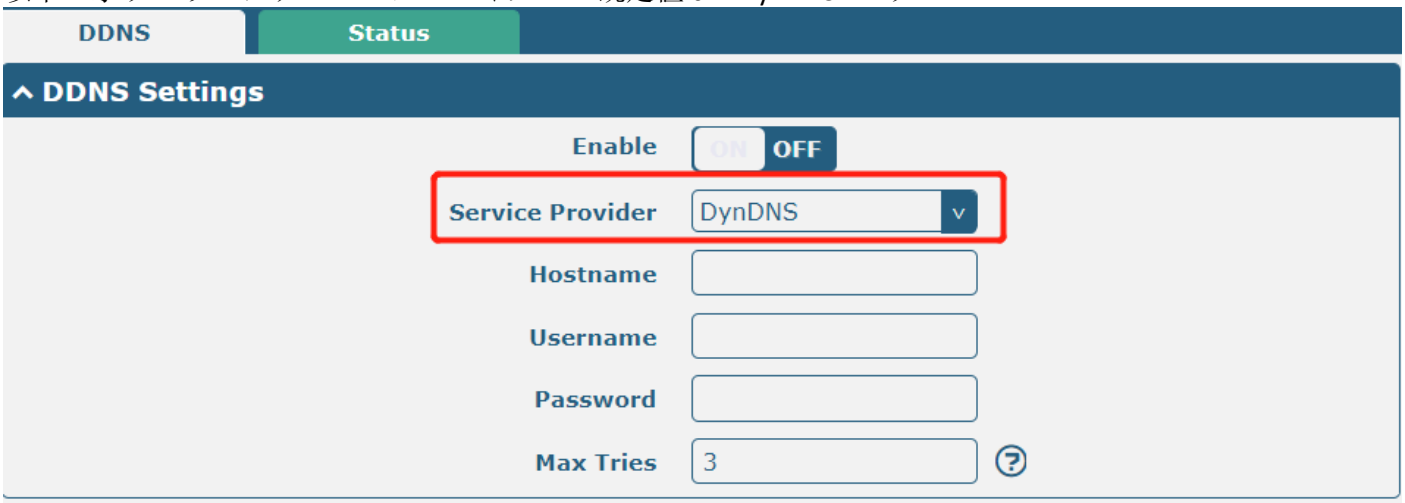
メール 設定		
アイテム	説明	デフォルト
エネーブル	トグルボタンをクリックして、[電子メール]オプションを有効/無効にします。	オフ
TLS/SSL を有効にする	トグルボタンをクリックして、TLS/SSL オプションを有効/無効にします。	オフ
STARTTLS を有効にする	トグルボタンをクリックして、STARTTLS 暗号化を有効/無効にします。	オフ
送信サーバー	SMTP サーバーの IP アドレスまたはドメイン名を入力します。	Null
サーバー・ポート	SMTP サーバーポートを入力します。	25
タイムアウト	SMTP サーバーに電子メールを送信する最大時間を設定します。この時間内にサーバーがメールを受信しない場合、サーバーは再送信を試みます。	10
認証ログイン	メールサーバが認証ログインをサポートしている場合は、このボタンを有効にして、ユーザ名とパスワードを設定する必要があります。	オフ
ユーザー名	SMTP サーバーから登録したユーザー名を入力します。	Null
パスワード	上記のユーザー名のパスワードを入力します。	Null
差出人	メールの送信元アドレスを入力します。	Null
件名	このメールの件名を入力します。	Null

3.6.6 DDNS

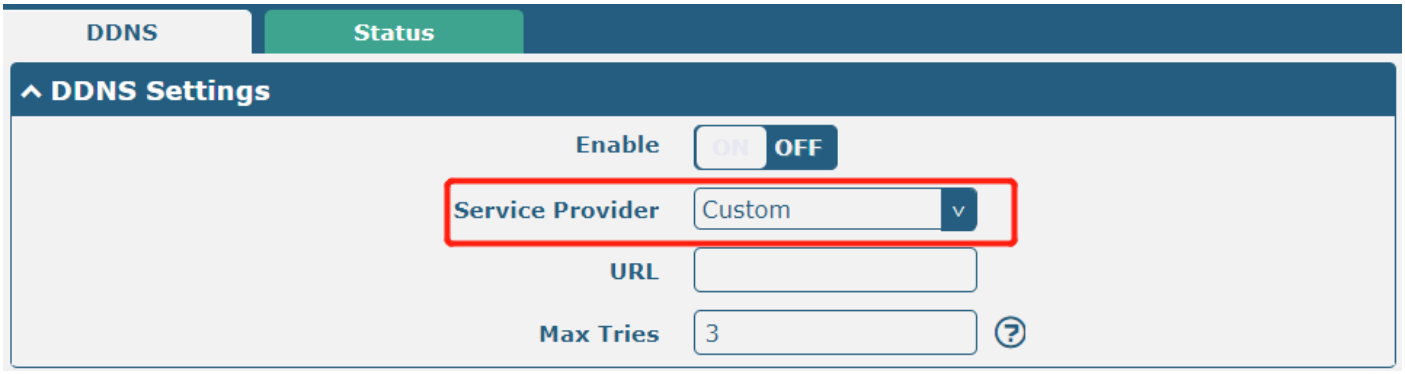
このセクションでは、DDNS パラメータを設定できます。ダイナミック DNS 機能を使用すると、動的 IP アドレスを静的ドメイン名にエイリアス化でき、ISP が静的 IP アドレスを割り当てていない場合でもドメイン名を使用できます。これは、接続を介してサーバーをホストする場合に特に便利で、接続を希望する人は誰でも、時々変更される動的 IP アドレスを使用するのではなく、ドメイン名を使用できます。この動的 IP アドレスは、ISP によって割り当てられたデバイスの WAN IP アドレスです。

1) DDNS

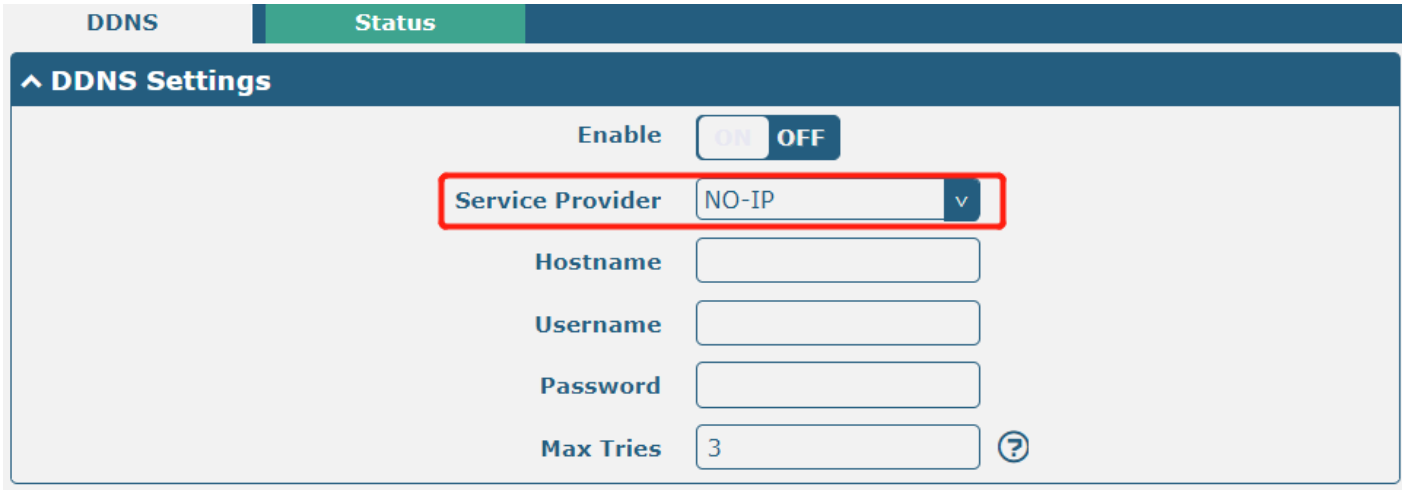
以下に示すように、サービスプロバイダーの既定値は "DynDNS" です。



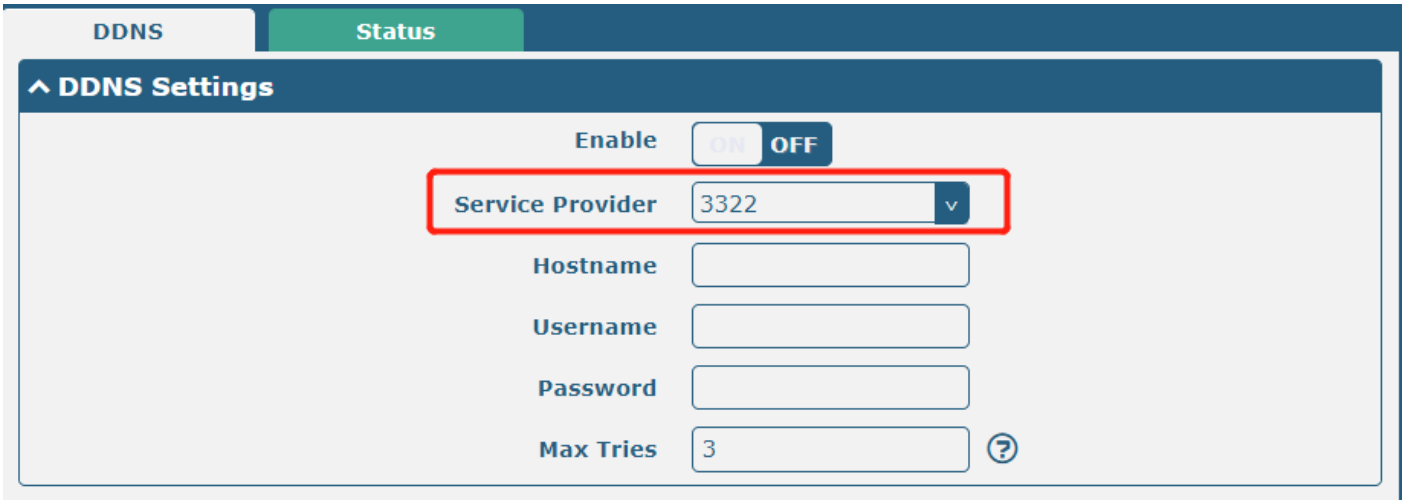
「カスタム」サービスプロバイダを選択すると、以下のようなウィンドウが表示されます。



「NO-IP」 サービスプロバイダ を選択すると 、以下のようなウィンドウが表示されます。



「3322」 サービスプロバイダ を選択すると 、以下のようなウィンドウが表示されます。



DDNS 設定		
アイテム	説明	デフォルト
エネーブル	トグルボタンをクリックして、DDNS オプションを有効/無効にします。	オフ
サービスプロバイダー	DDNS サービスを「DynDNS」、「NO-IP」、「3322」、または「Custom」から選択します。 *注:DDNS サービスは、対応するサービスプロバイダーによって登録 された後にのみ使用できます 。*	ダイン DNS の
ホスト名	DDNS サーバから提供されたホスト名を入力します。	Null
ユーザー名	DDNS サーバから提供されたユーザ名を入力します。	Null
パスワード	DDNS サーバから提供されたパスワードを入力します。	Null
URL (英語)	ユーザーがカスタマイズした URL を入力します 。	Null
最大試行回数	最大試行回数を入力します。	3

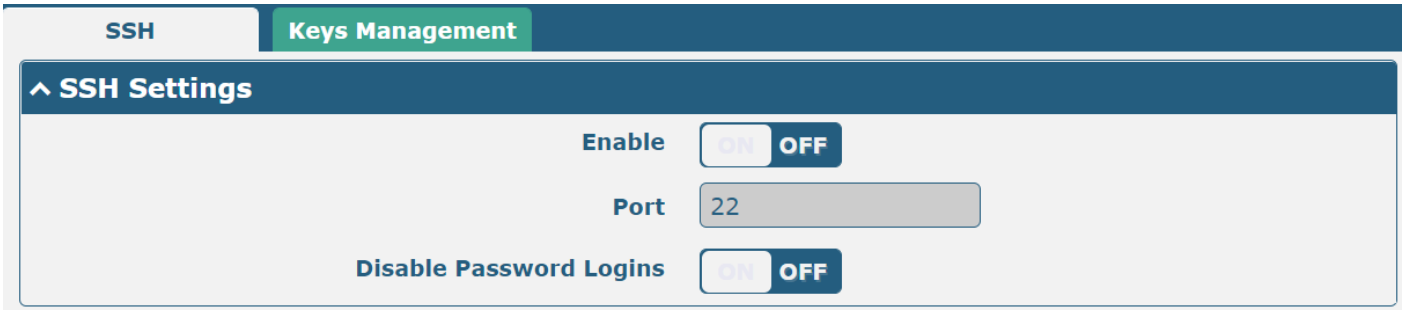
2) ステータス

このセクションでは、DDNS のステータスを表示できます。

DDNS ステータス	
アイテム	説明
ステータス	DDNS の現在のステータスを表示します。
最終更新時刻	DDNS の表示日時は、最後に正常に更新されました。

3.6.7 SSH

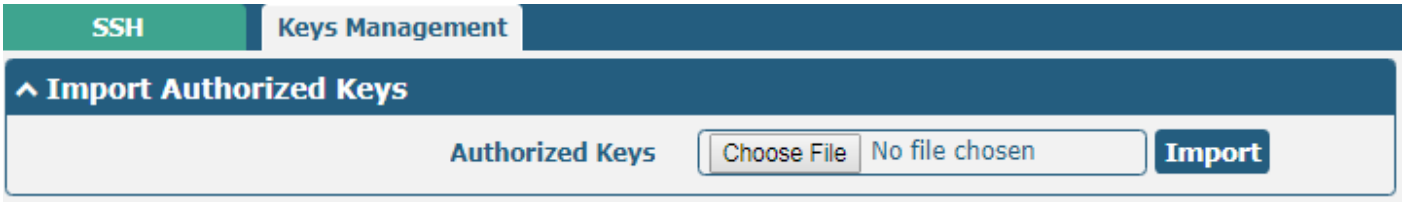
デバイスは 、SSH パスワード アクセスと秘密キー アクセスをサポートしています。



SSH 設定		
アイテム	説明	デフォルト
エネーブル	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、SSH 経由でデバイスにアクセスできます。	オフ
港	SSH アクセスのポートを設定します。	22
パスワードログインの無効化	切り替えボタンをクリックして、このオプションを有効/無効にします。有効にすると、 ユーザー名とパスワードを使用して SSH 経由でデバイスにアクセスすることはできません。この場合、ログインに使用できるのはキーのみです。	オフ

1) キー管理

このセクションでは、認証されたキーをインポートできます。



認証キーのインポート	
アイテム	説明
承認済みキー	「ファイルの選択」をクリックして PC から認証されたキーを見つけ、「インポート」をクリックしてこのキーをデバイスにインポートします。 *注: このオプションは、パスワード ログイン オプションを有効にした場合に有効です。*

3.6.8 電話

このセクションでは、音声機能の関連パラメーターを設定できます。デバイスに音声入力がある場合、このページは設定可能です。

手記:

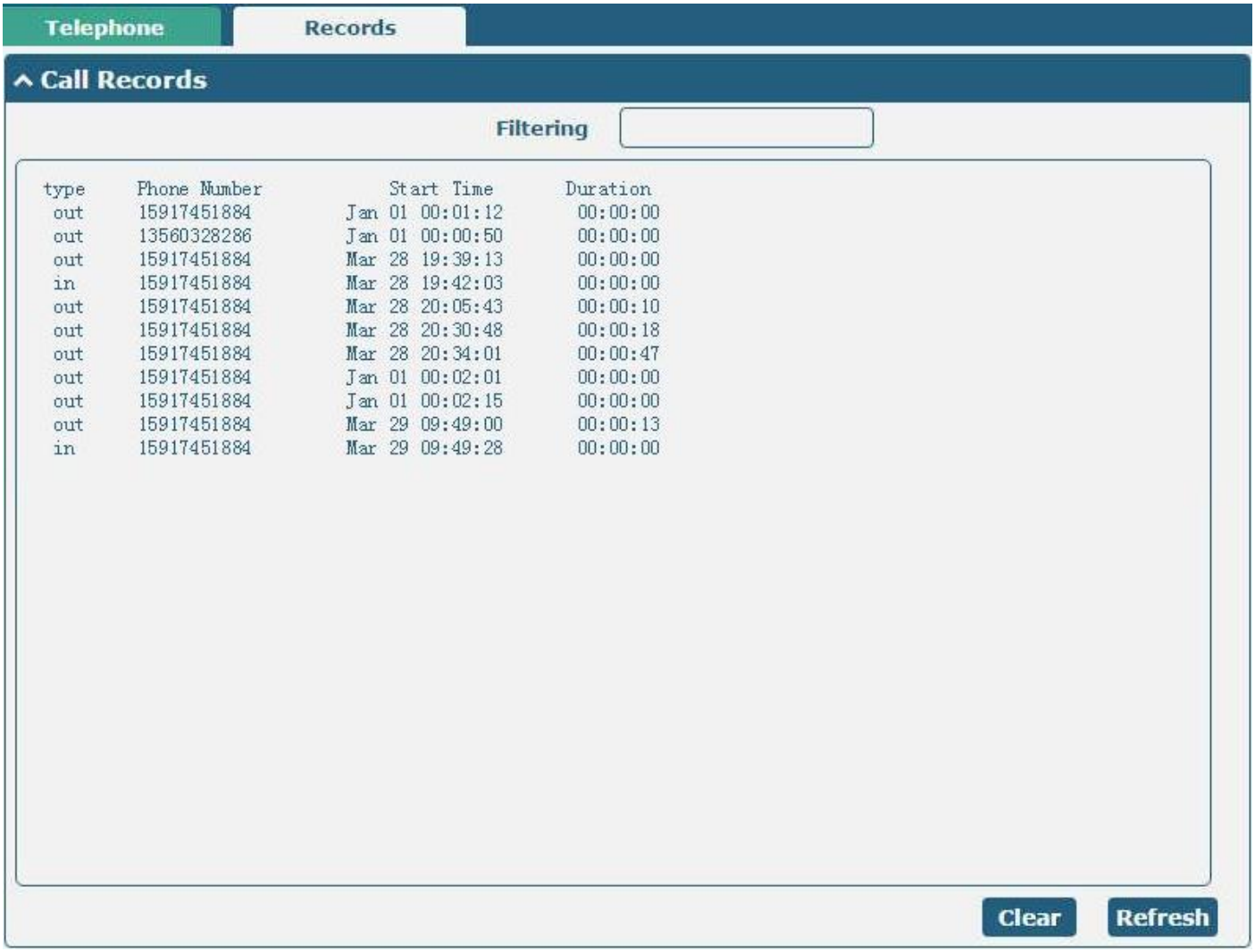
1) 音声通話とデータ通信を同時に使用できるかどうかは、ISP ネットワークによって異なります。

2) R2000-Ent、R3010 は「電話」機能に対応しています。

一般設定@電話		
アイテム	説明	デフォルト
待機番号のタイムアウト	ダイヤル プランの待機回数のタイムアウトを秒単位で設定します。	5
ディジットマップ (Digitmap)	音声通話時に電話番号を照合するディジットマップを入力します。一致すると、システムはすぐにこの番号に電話をかけ、ダイヤルアップタイムアウトを待つ必要はありません。このオプションは、短縮ダイヤルに使用されます。	Null

1) レコード

このセクションでは、通話記録を表示できます。



一般設定		
アイテム	説明	デフォルト
フィルタリング	ダイヤル プランの待機回数のタイムアウトを秒単位で設定します。	--
Clear	ボタンをクリックして、通話記録をクリアします。	--
Refresh	ボタンをクリックすると、通話記録が更新されます。	--

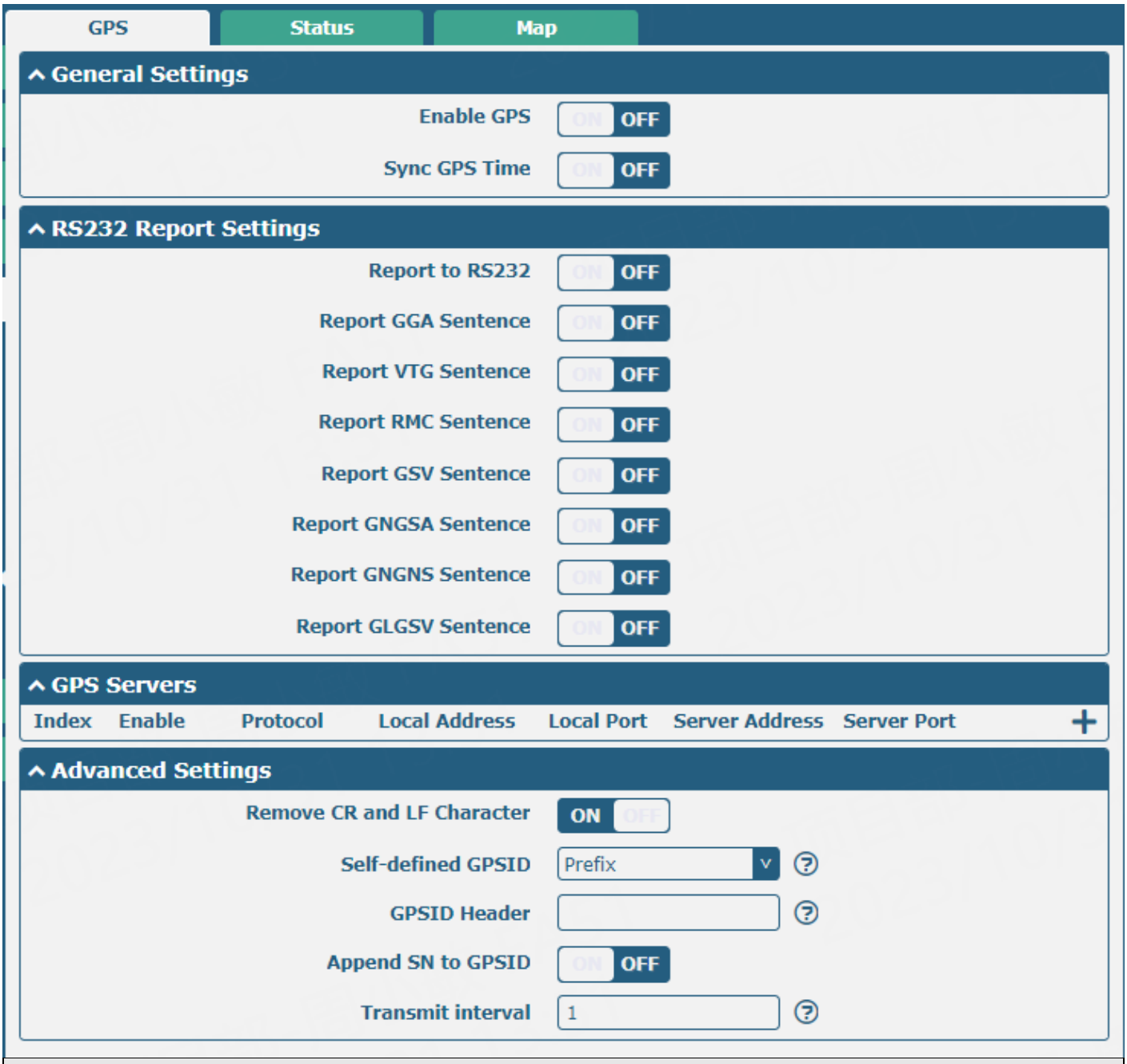
3.6.9 イグニッション

このセクションは、Ignition のパラメーターを構成するために使用されます。
注: R5020 および R2110 は イグニッション機能をサポートしています。

一般設定		
アイテム	説明	デフォルト
シャットダウンの遅延	電源オフを遅らせる時間を秒単位で入力します。遅延電源切断のタイムアウトは 60 秒から 3600 秒です。	60

3.6.10 GPS(全日本座標系)

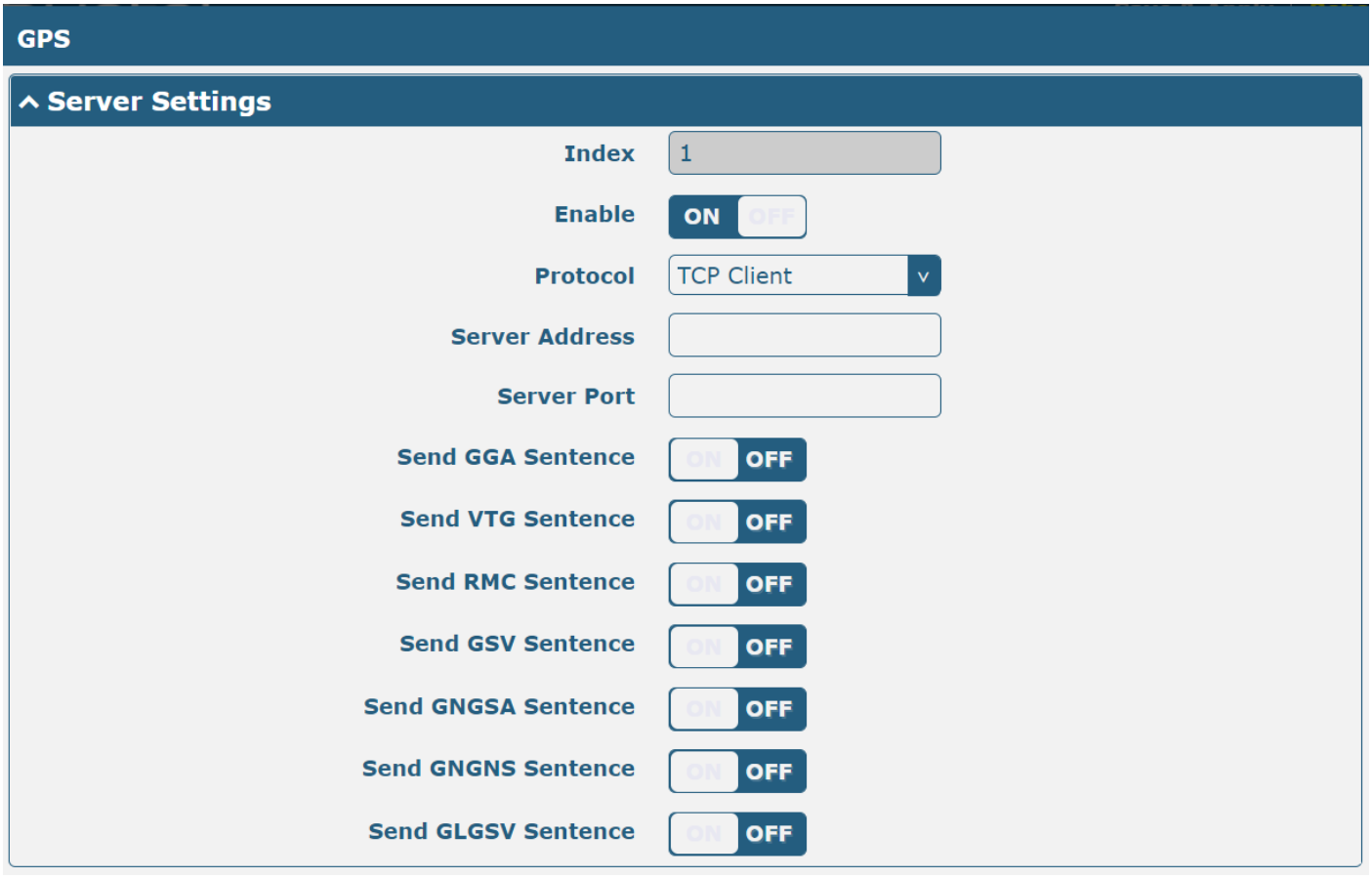
このセクションは、GPS のパラメータを設定するために使用されます。デバイスの GPS 機能は、デバイスの位置情報を見つけて取得し、指定されたサーバーに報告することができます。



GPS(全日本座標系)		
アイテム	説明	デフォルト
一般 設定		
エネーブル	トグルボタンをクリックしてオンにし、GPS を有効にします。	オフ
同期 GPS 時刻	トグルボタンをクリックしてオンにし、GPS 時刻を同期します。	オフ
RS232 レポート データ設定		
RS232 によるデータのレポート作成	RS232 による GPS 情報の報告。	オフ
GGA センテンスの報告	GGA センテンス情報の報告。	オフ
VTG センテンスの報	VTG センテンス 情報の報告。	オフ

GPS(全日本座標系)		
アイテム	説明	デフォルト
一般 設定		
告		
RMC センテンスの報告	RMC センテンス情報の報告。	オフ
GSV センテンスの報告	GSV センテンス 情報の報告。	オフ
詳細 設定		
CR と LF の文字を削除	キャリッジリターンの改行文字を削除できるようにしました	オン
自己定義の GPSID	GPSID は、送信前に NMEA メッセージに追加されます。「なし」、「接頭辞」、「接尾辞」を選択できます。	何一つ
GPSID ヘッダー	GPSID ヘッダーを追加しました。通常は大文字で 7 文字を使用します。	該当なし
SN を GPSID に追加	GPSID に SN を追加できるようにする	オフ
送信インターバル	データレポート期間を入力します。0 は、データがアップロードされないことを意味します。	1

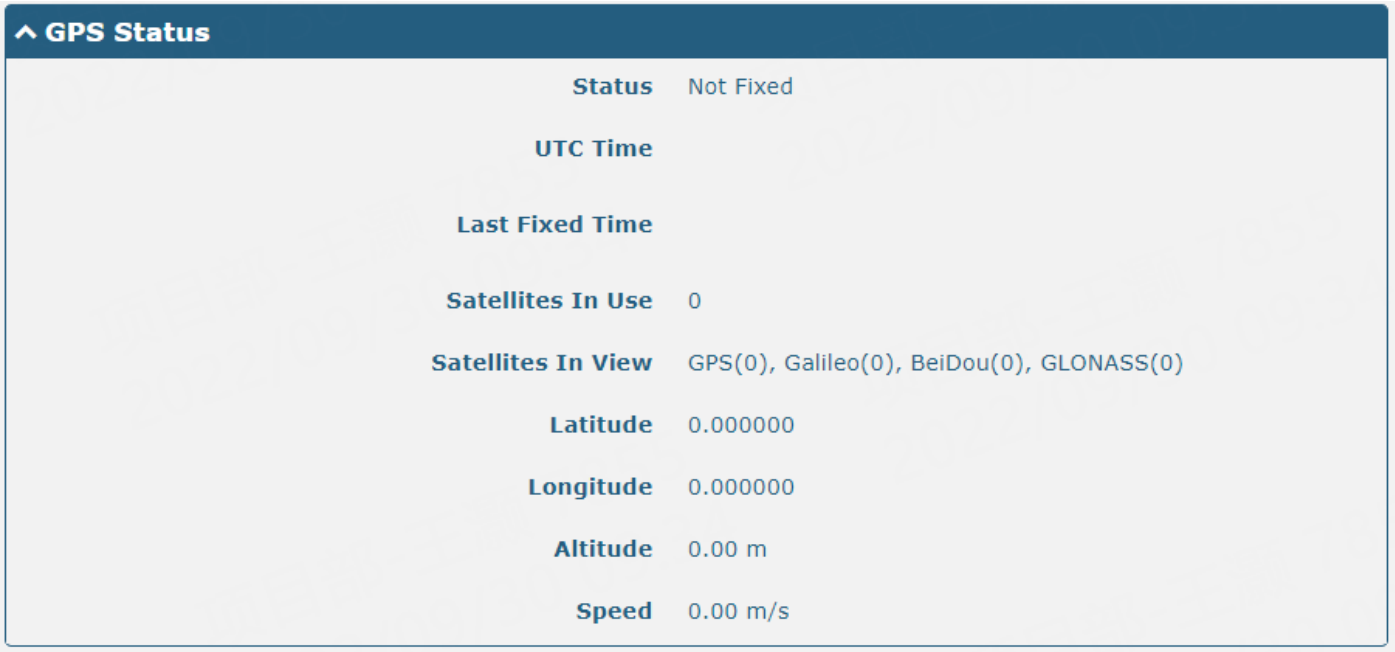
クリック + すると、新しい GPS サーバーが追加されます。



アイテム	説明	デフォルト
インデックス	リストの序数を示します。	--
エネーブル	トグルボタンをクリックして、サーバーを有効/無効にします。	オン
プロトコル	「TCP クライアント」、「TCP サーバー」、「UDP」から選択します。	TCP クライアント
サーバー/ローカルアドレス	サーバーまたはローカルの IP アドレス。	Null
サーバー/ローカルポート	サーバーまたはローカル IP ポート。	Null
Sendu GGA setningu	切り替えボタンをクリックして、このオプションを有効/無効にします。	オフ
千田 VTG の setningu	切り替えボタンをクリックして、このオプションを有効/無効にします。	オフ
RMC センテンスを送信	切り替えボタンをクリックして、このオプションを有効/無効にします。	オフ
GSV センテンスを送信	切り替えボタンをクリックして、このオプションを有効/無効にします。	オフ
Sendu GNGSA setningu	切り替えボタンをクリックして、このオプションを有効/無効にします。	オフ
GNGNS センテンスを送信する	切り替えボタンをクリックして、このオプションを有効/無効にします。	オフ
GLGSV センテンスを送信	切り替えボタンをクリックして、このオプションを有効/無効にします。	オフ

1) ステータス

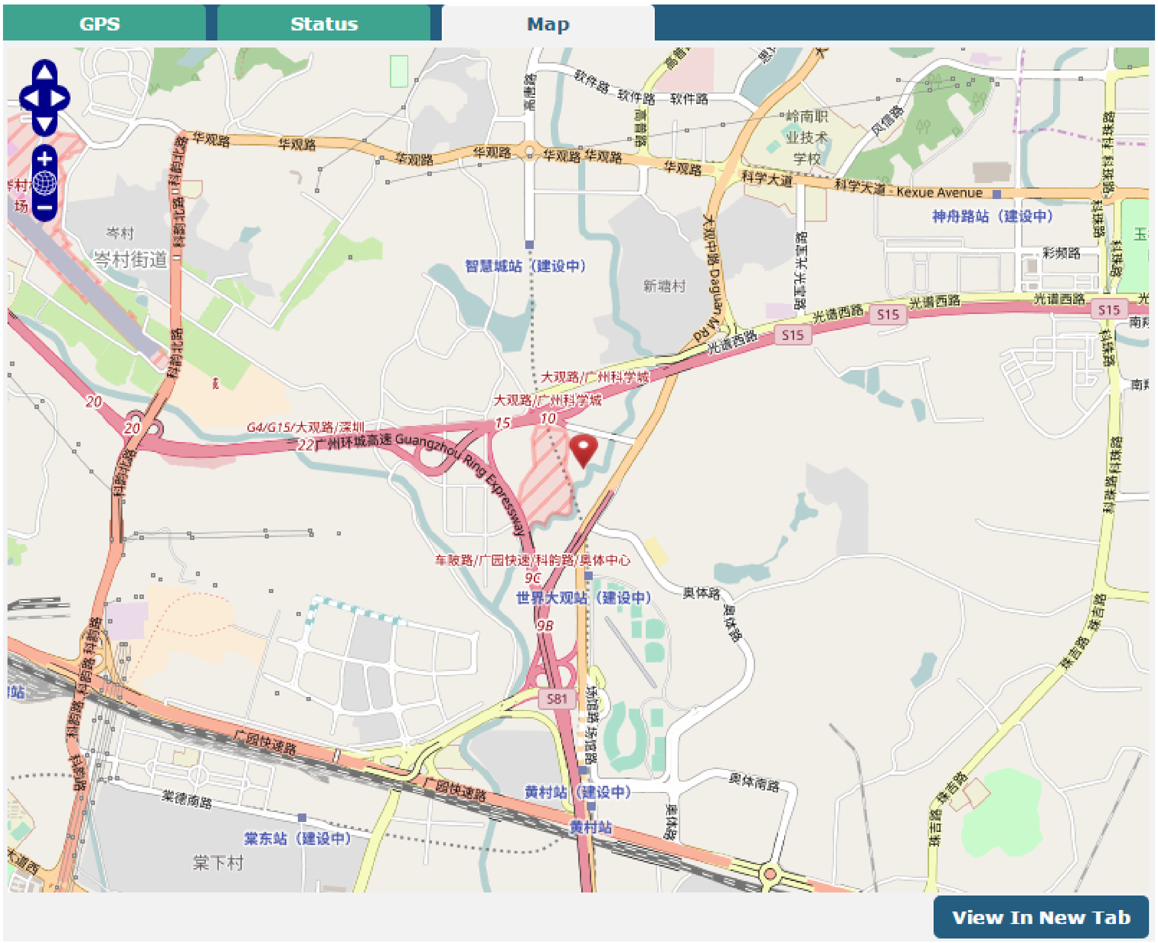
このセクションでは、GPS のステータスを表示できます。



アイテム	説明
ステータス	デバイスの現在の GPS ステータスを表示します。
UTC 時刻	衛星の UTC を表示します。 ***注:*** *UTC は世界統一時刻であり、現地時間ではありません。*
最終固定時刻	最後にポジショニングが成功した時刻。
使用中の衛星	使用されている衛星の数。
サテライト・イン・ビュー	可視衛星の数。
緯度	デバイスの Latitude 情報を表示します。
経度	デバイスの経度情報を表示します。
高度	デバイスの高さ情報を表示します。
速度	デバイスの速度情報を表示します。

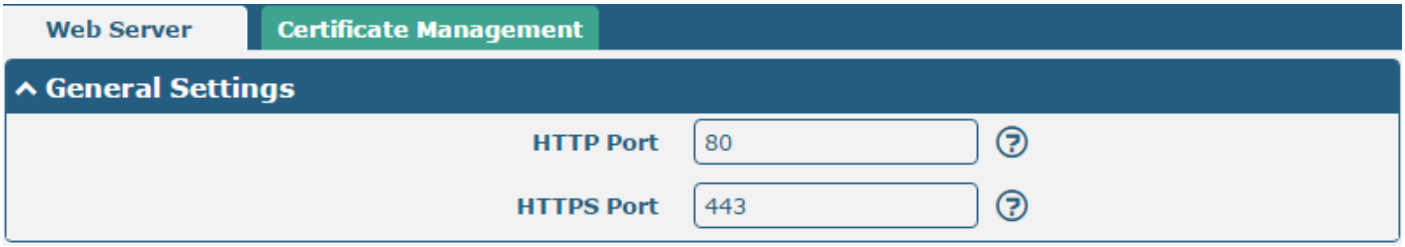
2) マップ

[マップ] ページには、デバイスの現在の座標とマップ上の位置が表示されます。地図上でデバイスの位置を確認するには、GPS アンテナをデバイスに接続し、GPS ページで GPS を有効にしてください 。


GPS
Status
Map
华观路
科学大道
Kexue Avenue
神舟路站（建设中）
智慧城站（建设中）
新塘村
岑村
岑村街道
光谱西路
S15
大观路/广州科学城
G4/G15/大观路/深圳
广州环城高速 Guangzhou Ring Expressway
车陂路/广园快速/科韵路/奥体中心
世界大观站（建设中）
奥体路
S81
广园快速路
黄村站（建设中）
黄村站
奥体南路
棠东站（建设中）
棠下村
棠德南路
View In New Tab

3.6.11 Web サーバー

このセクションでは、Web サーバーのパラメータを変更できます。



一般設定 @ Web サーバー		
アイテム	説明	デフォルト
HTTP ポート	デバイスの Web サーバーで変更する HTTP ポート番号を入力します。Web サーバーでは、ポート 80 は、サーバーが Web クライアントから "リッスン" する、または受信するポートです。80 以外の HTTP ポート番号でデバイスを設定し、そのポート番号のみを追加すると、 デバイスの Web サーバにログインできます。	80
HTTPS ポート	デバイスの Web サーバーで変更する HTTPS ポート番号を入力します。Web サーバーでは、ポート 443 は、サーバーが Web クライアントから "リッスン" する、または受信するポートです。443 以外の HTTPS ポート番号でデバイスを設定し、そのポート番号のみを追加すると、 デバイスの Web サーバーにログインできます。 *注: HTTPS は HTTP よりも安全です。多くの場合、クライアントは機密情報をサーバーと交換している可能性があり、不正アクセスを防ぐためにセキュリティで保護する必要があります。このため、HTTP は Netscape 社によって開発され、承認と安全なトランザクションを可能にしました。*	443

1) 証明書 の管理

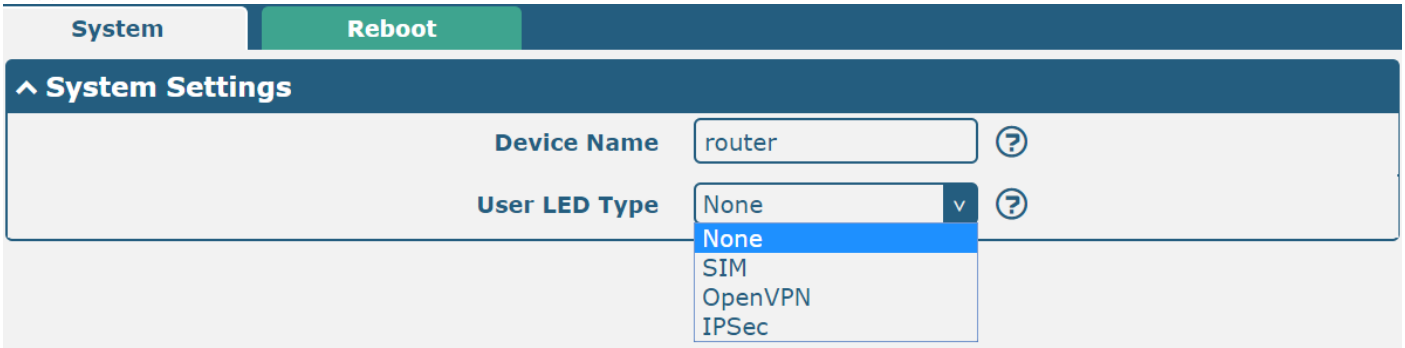
このセクションでは、証明書ファイルをデバイスにインポートできます。

証明書のインポート		
アイテム	説明	デフォルト
インポートの種類	「CA」と「秘密鍵」を選択します。 • CA: CA センターが発行するデジタル証明書。 • 秘密鍵:秘密鍵 ファイル。	CA
HTTPS 証明書	「ファイルの選択」をクリックして PC から証明書ファイルを見つけ 、「インポート」をクリックしてこのファイルをデバイスにイ	--

証明書のインポート		
アイテム	説明	デフォルト
	ンポートします。	

3.6.12 アドバンスド

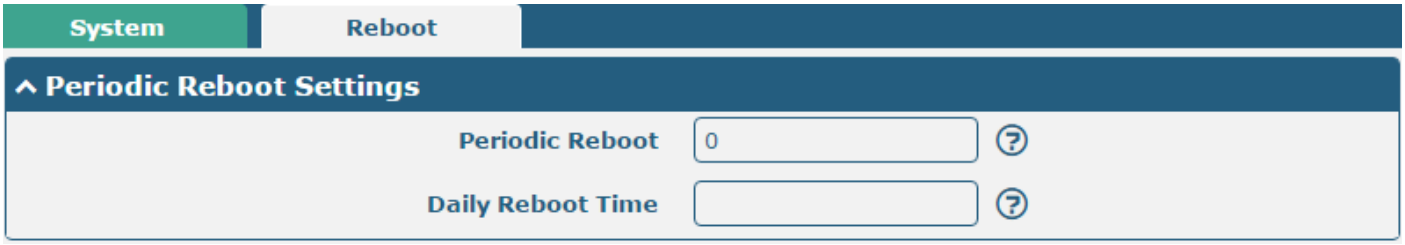
このセクションでは、 詳細 パラメータを設定できます。デバイスの詳細設定には、システム設定と再起動が含まれます。



システム設定		
アイテム	説明	デフォルト
デバイス名	このデバイスの名前を設定して、ブラウザのタブページに現在のデバイス名を表示します。有効な文字は、a から z、A から Z、0 から 9、@、.、-、#、$、および * です。	ルーター
ユーザーLED タイプ	USR LED の表示タイプを指定します。「なし」、「OpenVPN」、または「IPsec」から選択します。 • なし:無意味な表示で、LED は消灯しています。 • SIM:SIM ステータスを示す USR インジケーター。 • OpenVPN:OpenVPN のステータスを示す USR インジケーター。 • IPsec: IPsec ステータスを示す USR インジケータ。	何一つ

1) リブート

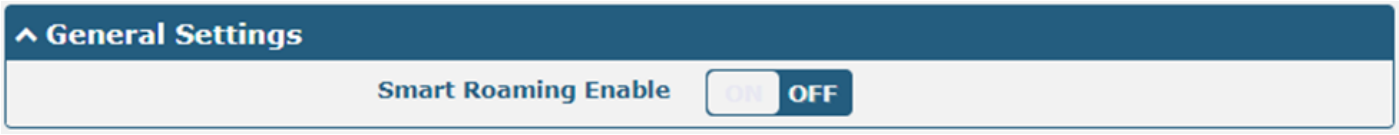
このセクションでは、 再起動タイプを設定できます。



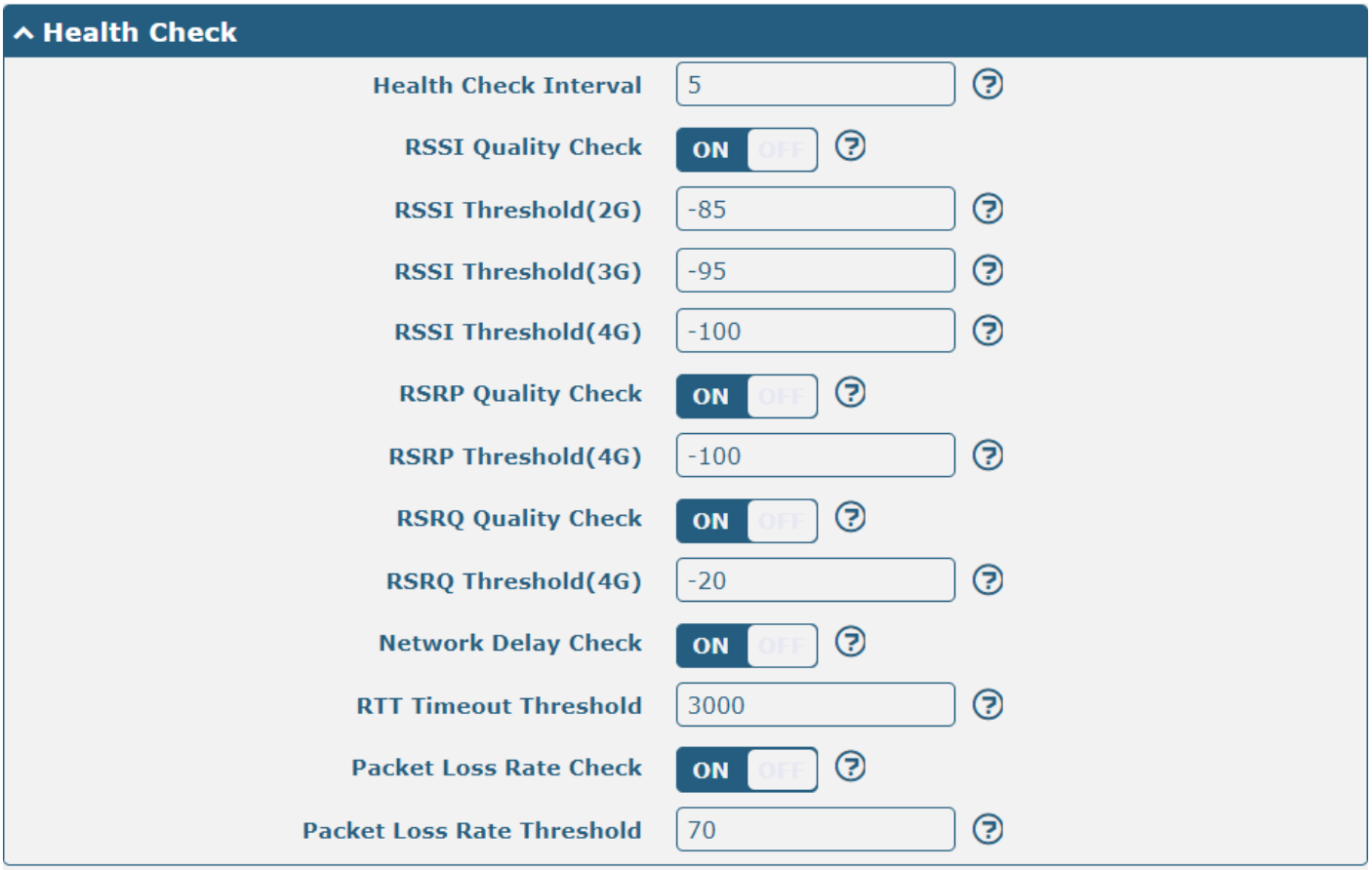
定期的な再起動設定		
アイテム	説明	デフォルト
定期的な再起動	デバイスの再起動期間を設定します。 0 は無効を意味します。	0
毎日の再起動時間	デバイスの毎日の再起動時間を設定します。HH:MM の形式に従う必要があり、24 時間 枠で、そうしないとデータが無効になります。 空のままにすると、無効になります。	Null

3.6.13 スマートローミング V2

スマートローミングには、一般設定、ヘルスチェック、PING 設定、および詳細設定が含まれます。

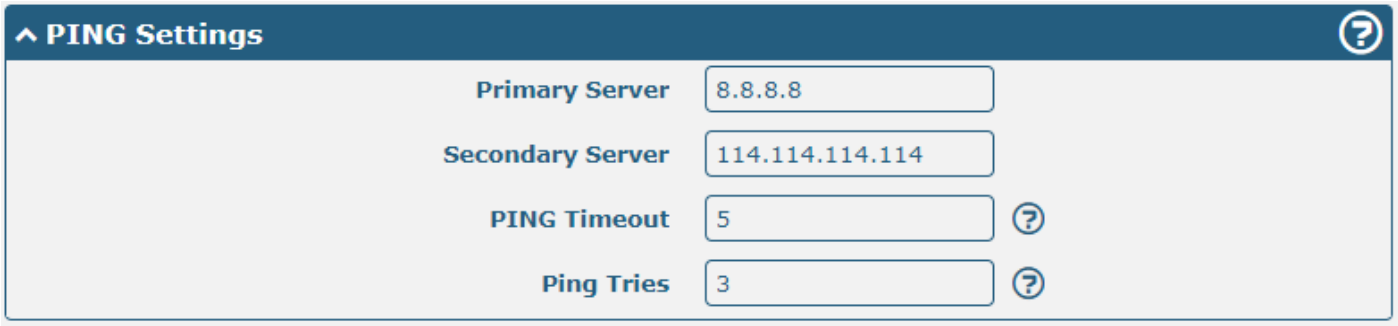


一般設定		
アイテム	説明	デフォルト
スマートローミング有効(Smart Roaming Enable)	スマートローミング機能を有効にする	オフ



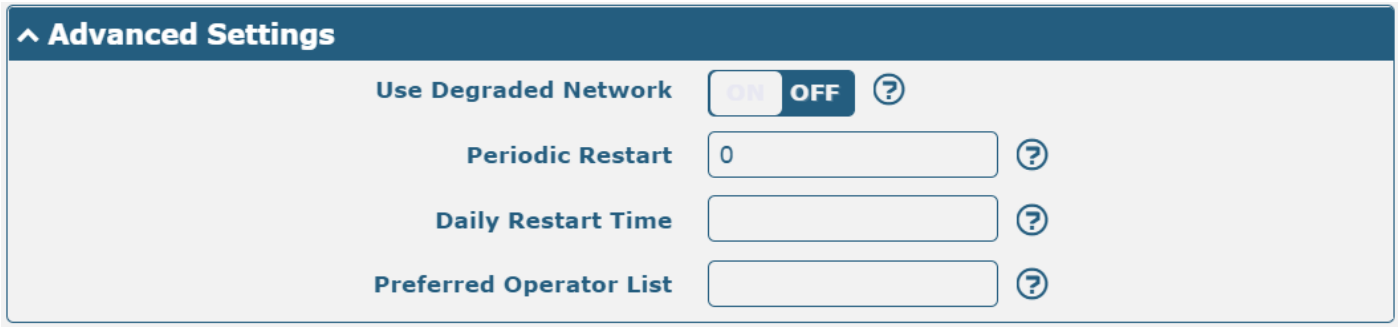
ヘルスチェック		
アイテム	説明	デフォルト
ヘルスチェックインターバル	現在の接続のヘルスチェックインターバルは分単位です。ヘルスチェックに失敗した場合、スマートローミングは別のキャリアネットワークへの切り替えを試みます。すべてのチェック条件を理論的に達成不可能な値に設定しないように注意してください。	5 分間
RSSI 品質チェック	「RSSI 品質チェック」機能を有効/無効にします。	オン

ヘルスチェック		
アイテム	説明	デフォルト
ヘルスチェックインターバル	現在の接続のヘルスチェックインターバルは分単位です。ヘルスチェックに失敗した場合、スマートローミングは別のキャリアネットワークへの切り替えを試みます。すべてのチェック条件を理論的に達成不可能な値に設定しないように注意してください。	5 分間
RSSI しきい値(2G)	2G ネットワークの信号強度のしきい値。	-85 デシベルメートル
RSSI しきい値(3G)	3G ネットワークの信号強度のしきい値。	-95dBm の
RSSI しきい値(4G)	4G ネットワークの信号強度のしきい値。	-100dBm の
RSRP 品質チェック	「RSRP 品質チェック」機能を有効/無効にします。	オフ
RSRP しきい値(4G)	4G ネットワークの基準信号受信電力しきい値。	-100dBm の
RSRQ 品質チェック	「RSRQ 品質チェック」機能を有効/無効にします。	オフ
RSRQ しきい値(4G)	4G ネットワークの基準信号受信品質しきい値。	-20dBm の
ネットワーク遅延チェック	「ネットワーク遅延チェック」機能を有効/無効にします。	オフ
RTT タイムアウトしきい値(RTT Timeout Threshold)	4G ネットワークの基準信号受信電力しきい値。	3000 ミリ秒
パケット損失率チェック	「パケット損失率チェック」機能を有効/無効にします。	オン
パケット損失率しきい値(Packet Loss Rate Threshold)	パケット損失率のしきい値。	70

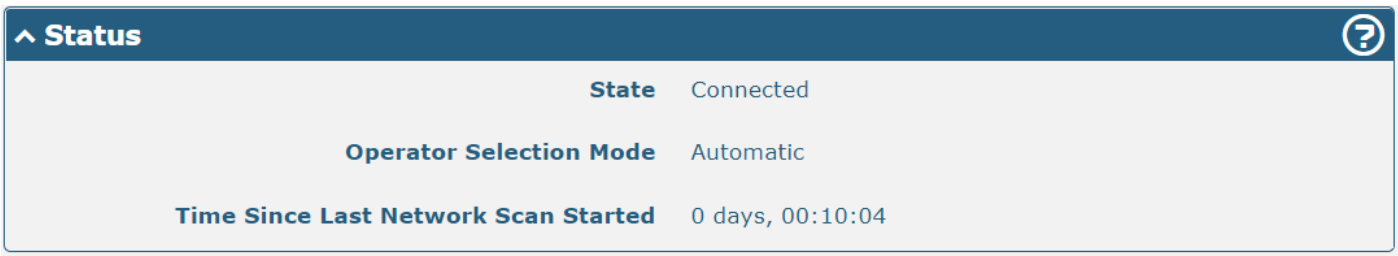


PING 設定		
アイテム	説明	デフォルト
プライマリ サーバ	デバイスはプライマリアドレス/ドメイン名に ping を実行して、現在の接続が常に有効かどうかを検出します。	8.8.8.8
セカンダリ サー	デバイスはセカンダリアドレス/ドメイン名に ping を実行して、現在の	114.114.11

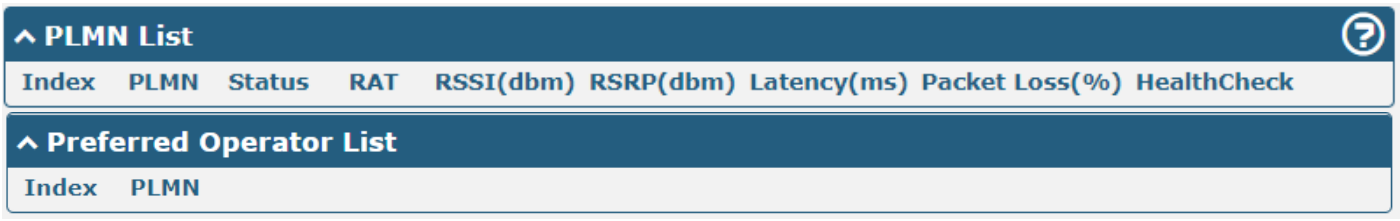
PING 設定		
アイテム	説明	デフォルト
バ	接続が常に有効かどうかを検出します。	4.114
Ping タイムアウト	Ping タイムアウトを設定します。	5 秒
Ping の試行回数	ヘルスチェックごとの ping 試行回数。各 ping 試行はデフォルトで 3 つの ping メッセージを送信するため、ヘルスチェックごとに送信される ping メッセージの合計数は (3 * ping 試行回数) になります。	3 トン IMES



詳細設定		
アイテム	説明	デフォルト
劣化したネットワークを使用する	「劣化したネットワークを使用する」機能を有効/無効にします。劣化したネットワークは、接続はできるが、ネットワーク品質がヘルスチェックのしきい値を満たしていないネットワークとして定義されます。	オフ
定期的な再起動	「スマートローミング」機能を再起動する期間を時間単位で設定します。0 は、定期的な再起動が有効になっていないことを意味します。「スマートローミング」を再起動すると、利用可能なキャリアネットワークが再検出され、利用可能なプロバイダーネットワークの検索に時間がかかるため、現在のステータスがリセットされ、再起動に 3〜5 分かかる場合があります。	0
毎日の再起動時間	「スマートローミング」を毎日 HH:MM(24 時間制)の形式で再起動する時点を設定します。この項目が空の場合は、タイマーの再起動を無効にすることを意味します。	Null
優先演算子リスト	PLMN による優先演算子のリストを設定します。複数の演算子が必要な場合は、セミコロンで区切ります(例:46000)。46001 年	Null



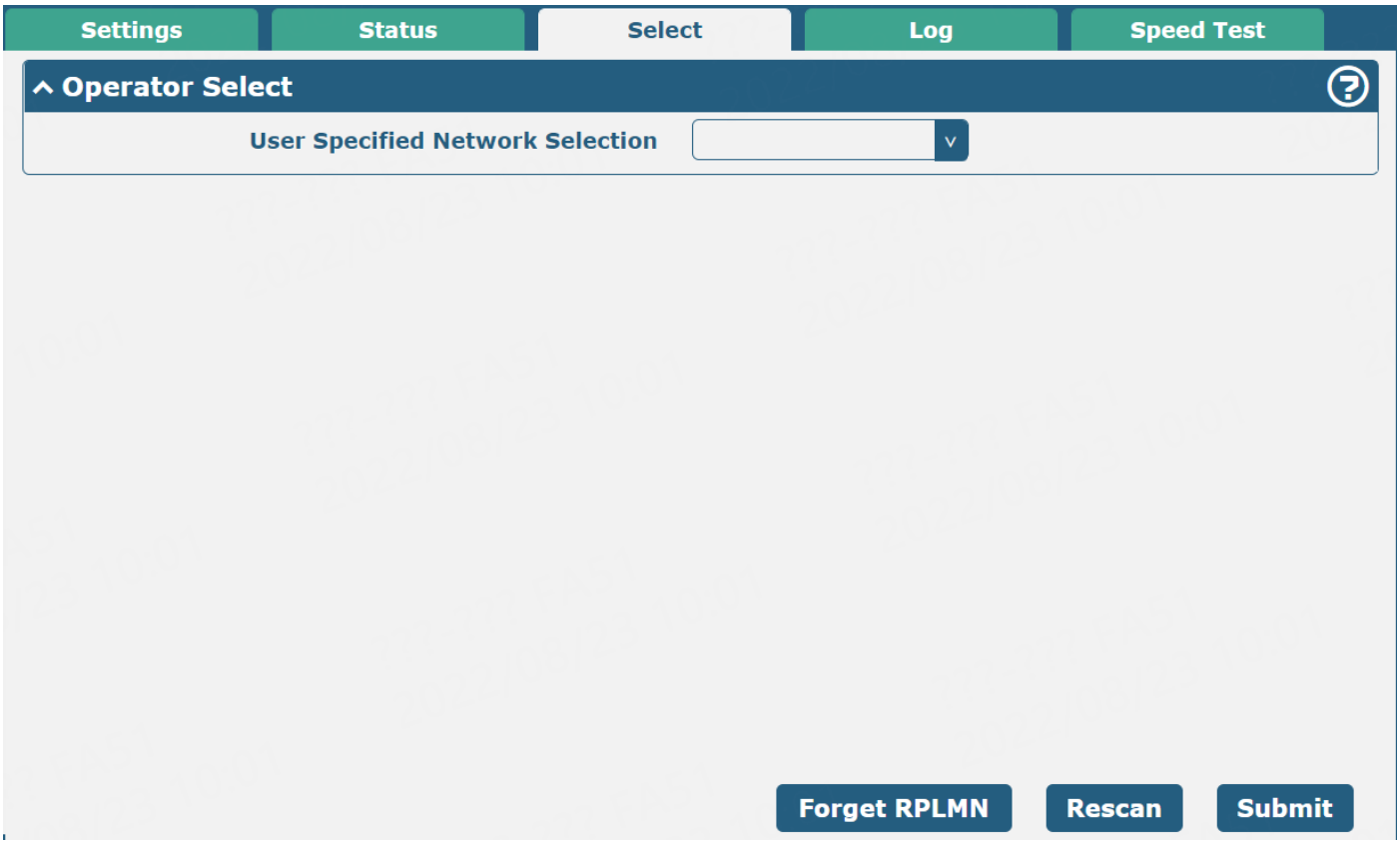
ステータス	
アイテム	**説明**
ステータス	「スマートローミング」の現在のステータスを表示します。これには、スキャン中、接続中、接続済み、および非アクティブステータスが含まれ、ネットワークが使用可能なネットワークを検索している、接続中のネットワーク、ネットワークが接続されている、および機能が開始されていないことをそれぞれ示します。
演算子選択モード	現在選択されているキャリアネットワークを表示します。これらには、標準仕様による自動選択とネットワーク品質に基づくソフトウェア選択を指す自動と手動が含まれ、ソフトウェアは 2 つの方法を循環します。
前回のネットワークスキャンからの経過時間	使用可能なネットワークを最後に検索してからの経過時間を表示します。今回は「スマートローミング」の再起動が更新されます。



PLMN リスト	
アイテム	**説明**
インデックス	PLMN リスト インデックス
PLMN	PLMN = MCC + MNC は、モバイルの国コードとモバイル ネットワーク コードの組み合わせです。
ステータス	現在のネットワークステータス(現在、表示、禁止、不明など)は、このネットワークの現在の使用状況、使用可能なネットワーク、禁止されているネットワーク、不明なネットワークをそれぞれ示します。
ラット (dBm)	2G/3G/4G を含む現在のワイヤレスアクセス技術。
RSSI (dBm)	3G および 4G ネットワークの現在の信号品質。
RSRP (dBm)	4G ネットワークの現在の基準信号受信電力。
レイテンシー	現在のネットワーク遅延。
パケット損失 (%)	現在のネットワーク パケット損失率。
ヘルス チェック	現在のヘルスチェックステータス(Pending、Good、Degraded、Failed など)は、現在のネットワークがまだヘルスチェックされていないことを示します。ネットワーク品質は良好です。ネットワークが劣化しています。ネットワーク品質が悪い(切断されている、ヘルスチェックのしきい値を満たしていないなど)。
優先 PLMN リスト	
インデックス	PLMN リスト インデックス
PLMN	PLMN = MCC + MNC は、モバイルの国コードとモバイル ネットワーク コードの組み合わせです。

1) セレクト

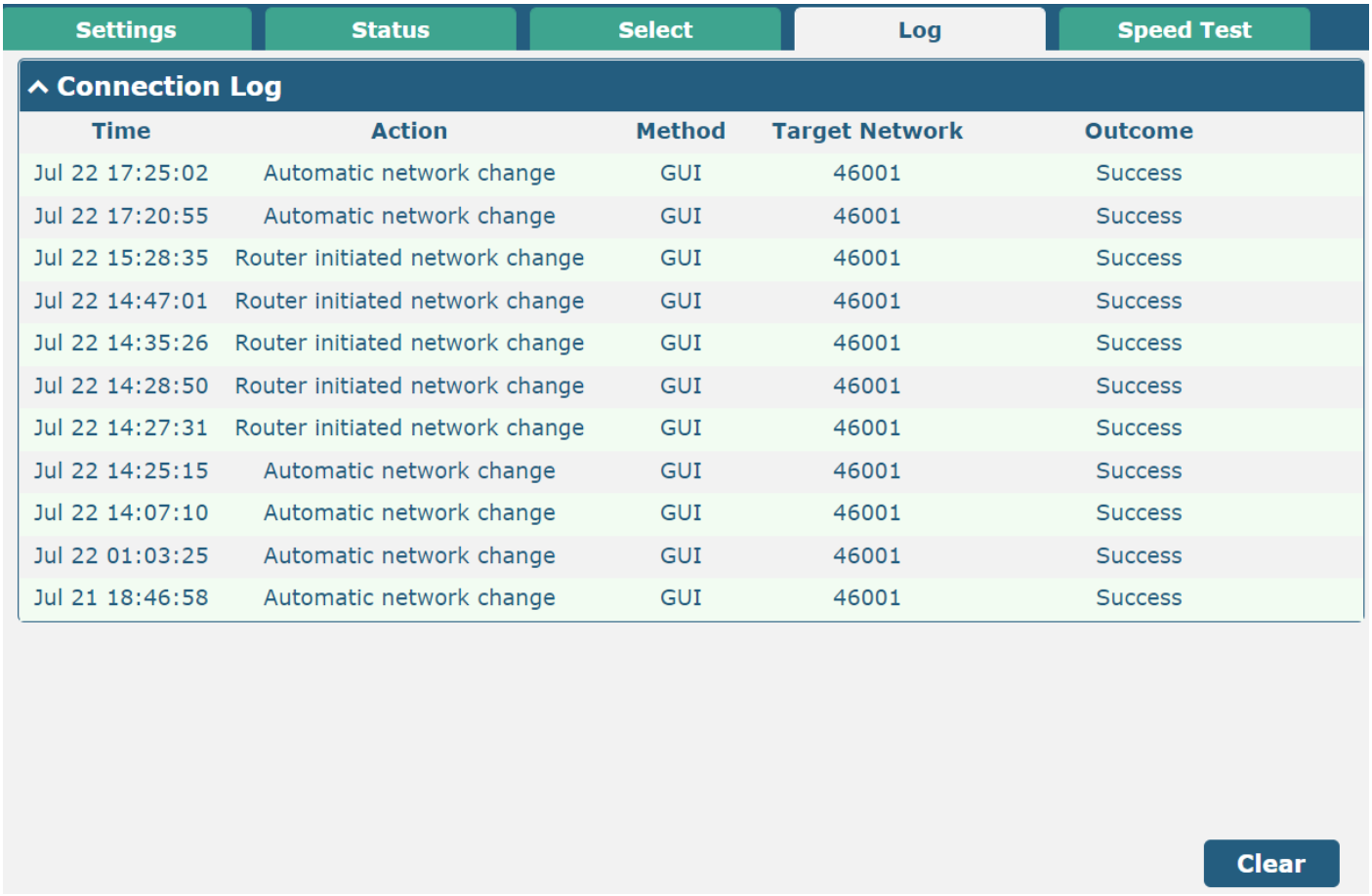
このセクションでは、ネットワークを選択できます。



演算子の選択		
アイテム	説明	デフォルト
ユーザー指定ネットワークの選択	[指定したネットワーク] を選択します。	--
Forget RPLMN	SIM からすべての位置情報を強制的に削除します。	--
Rescan	オペレータリストを再スキャンすると、スマートローミングが再開されます。	--
Submit	ドロップダウンボックスで選択した演算子を送信します。	--

2) ログ

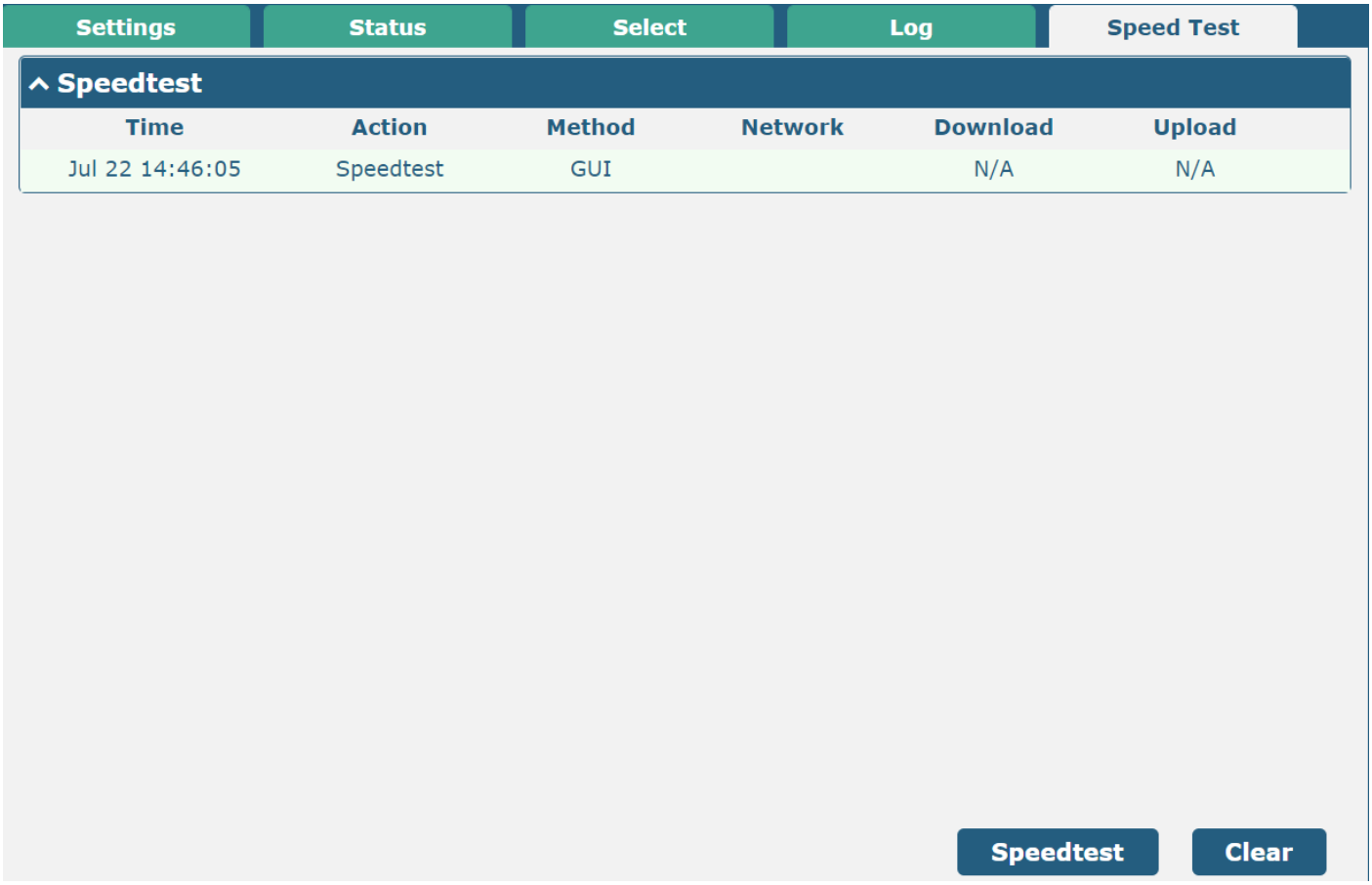
このセクションでは、接続ログを表示できます。



接続ログ		
Clear	ボタンをクリックして、接続ログをクリアします。	--

3) スピードテスト

このセクションでは、ネットワーク速度をテストできます。

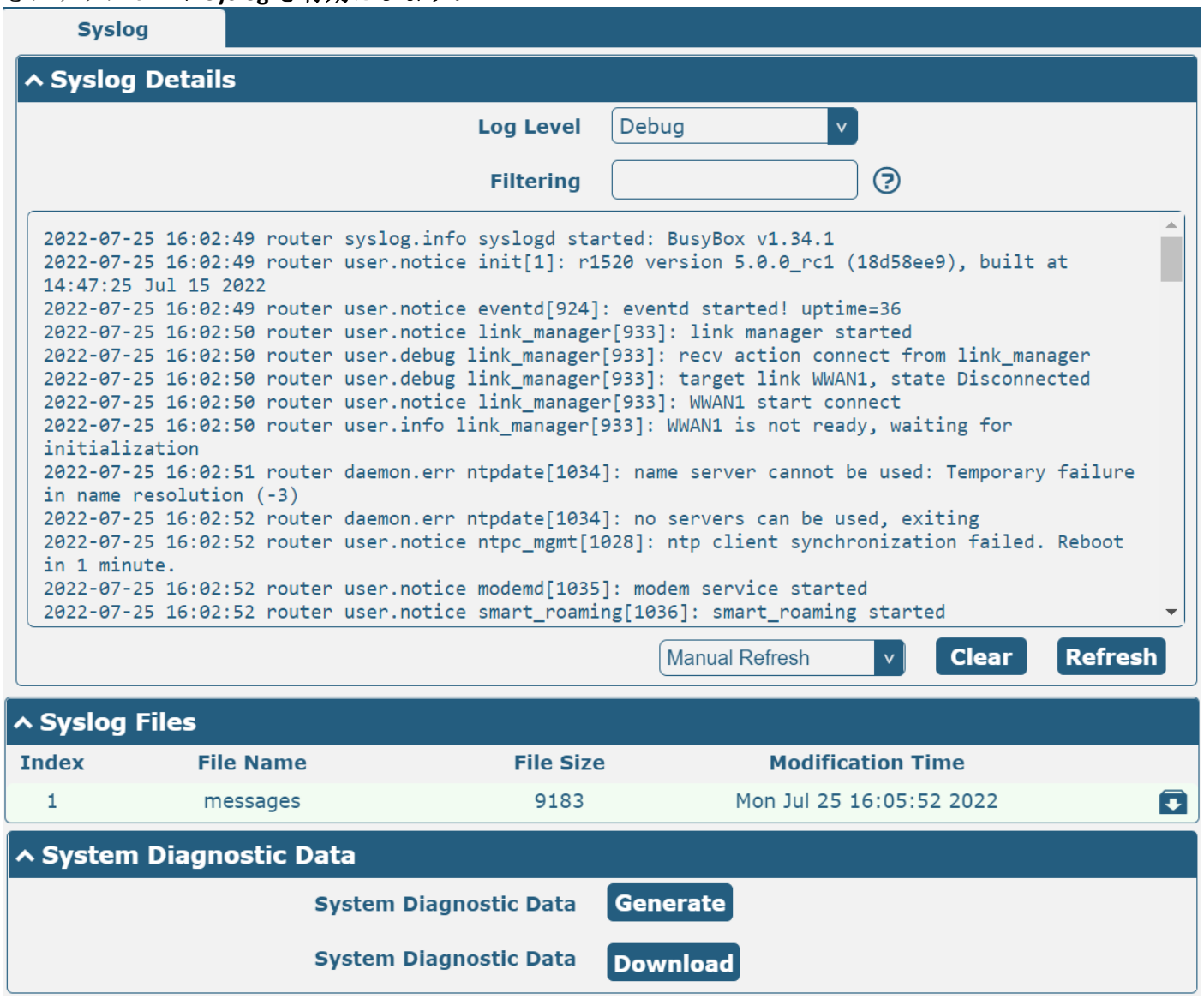


スピードテスト		
Speedtest	ボタンをクリックして、ネットワーク速度テストを開始します。	--
Clear	ボタンをクリックして、速度テストログをクリアします。	--

3.7 システム

3.7.1 デバッグ

このセクションでは、Syslog の詳細を確認およびダウンロードできます。[Service > Syslog > Syslog Settings] をクリックして、**Syslog を有効にします。**



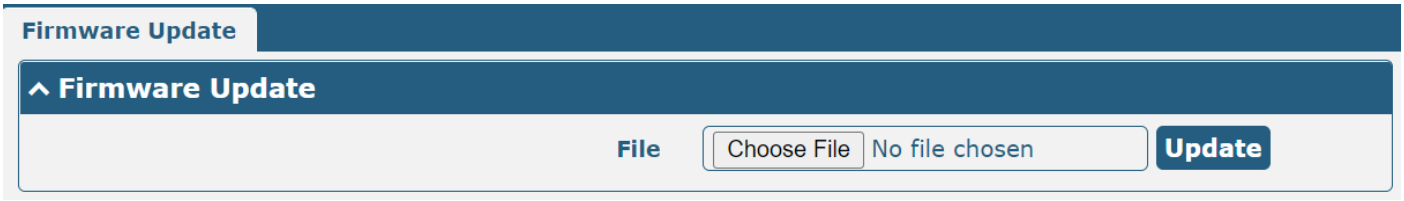
Syslog(シスログ)		
アイテム	説明	デフォルト
Syslog の詳細		
ログレベル	「デバッグ」、「情報」、「通知」、「警告」、「エラー」を低から高に選択します 。下位レベルは、より詳細な Syslog を出力します。	デバッグ
フィルタリング	キーワードに基づいてフィルタリング メッセージを入力します。「keyword1&keyword2」のように、複数のフィルターメッセージを区切るには、「&」を使用します。	Null
リフレッシュ	「手動更新」、「5 秒」、「10 秒」、「20 秒」、「30 秒」から選択します。 こ	手動更新

	れらのインターバルを選択すると、次のボックスに表示されるログ情報を更新できます。「手動更新」を選択した場合は、更新ボタンをクリックして Syslog を更新する必要があります。	
Clear	ボタンをクリックして、Syslog をクリアします。	--
Refresh	ボタンをクリックして、Syslog を更新します。	--
Syslog ファイル		
Syslog ファイルリスト	リストには最大 5 つの Syslog ファイルを表示でき、ファイルの名前は message0 から message4 までの範囲です。そして、最新の Syslog ファイルがリストの一番上に配置されます。	--
システム診断データ		
Generate	クリックすると、Syslog 診断ファイルが生成されます。デバイスに問題がある場合は、システム診断データを生成し、**堅牢なテクニカルサポート担当者に送信し**て支援を求めることができます。	--

3.7.2 更新

このセクションでは、ファームウェアファイルをインポートおよび更新することで、デバイスシステムをアップグレードし、システムアップデートを実装できます。ファームウェアファイルを PC からデバイスにインポートし、Update プロンプトに従ってデバイスをクリックして再起動し、ファームウェアの更新を完了します。

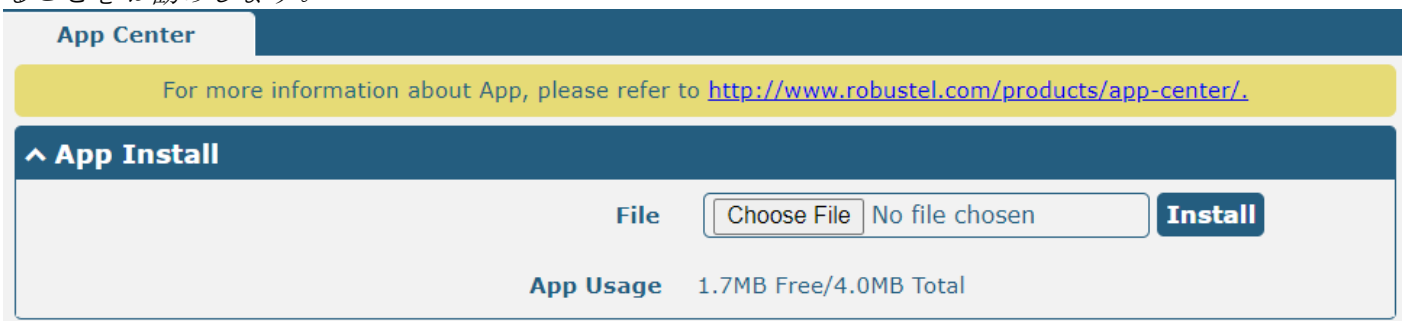
注意: *最新のファームウェアにアクセスするには file テクニカルサポートエンジニアにお問い合わせください。*



3.7.3 アプリセンター

このセクションでは、必要なアプリケーションまたはカスタマイズされたアプリケーションをデバイスに追加できます。アプリケーションを App Center にインポートしてインストールし、システムプロンプトに従ってデバイスを再起動します。インストールされている 各アプリケーションは「サービス」メニューの下に表示され、VPN に関連する他のアプリケーションは「VPN」メニューの下に表示されます。

注: *アプリケーションをデバイスにインポートした後、ブラウザのキャッシュが原因でページの表示がわずかに遅れる場合があります。最初にブラウザのキャッシュをクリアしてから、デバイスに再度ログインすることをお勧めします。*



正常にインストールされたアプリは、次のリストに表示されます。クリックして ✕ アプリをアンインストールします。

Installed Apps

Index	Name	Version	Status	Description	
1	vrrp	3.1.0	Stopped	VRRP Daemon	✕
2	dynamic_route	4.0.0	Stopped	Dynamic Route	✕
3	rcms	4.0.0	Stopped	rcms Client Connected to RCMS	✕

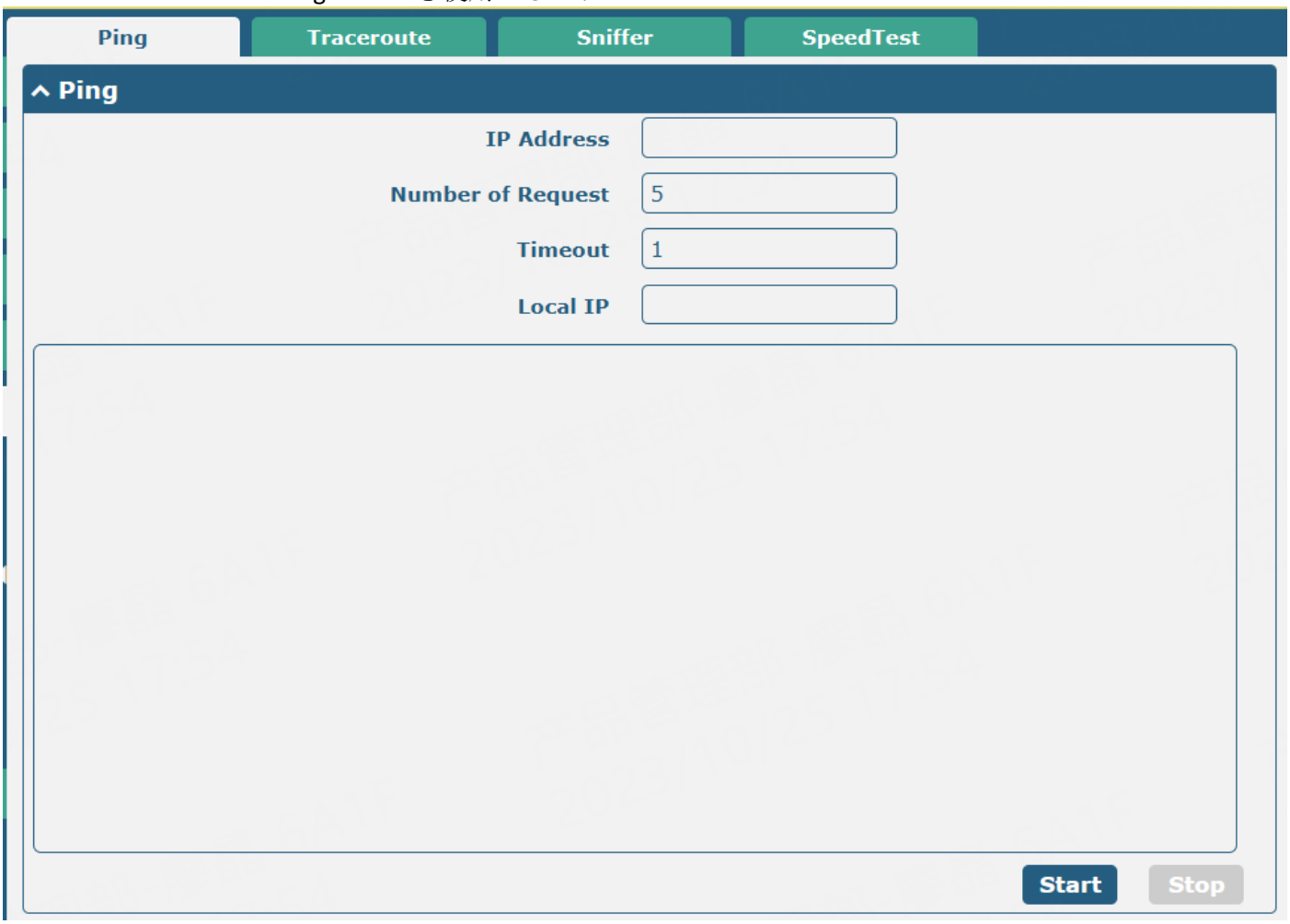
アプリセンター		
アイテム	説明	デフォルト
アプリのインストール		
ファイル	「ファイルの選択」をクリックして PC からアプリファイルを見つけ 、Install クリックしてこのファイルをデバイスにインポートします。 *注:ファイル形式は xxx.rpk(例:r1520-vrrp-5.0.0.rpk) である必要があります。*	--
インストール済みアプリ		
インデックス	リストの序数を示します。	--
名前	アプリ名を表示します。	Null
バージョン	アプリのバージョンを表示します。	Null
ステータス	アプリのステータスを表示します。	Null
説明	アプリの説明を表示します。	Null

3.7.4 ツール

このセクションでは、Ping、Traceroute、Sniffer、SpeedTest の 4 つのツールを提供します。Ping は、ネットワーク接続を確認するために使用されます。

1) Ping

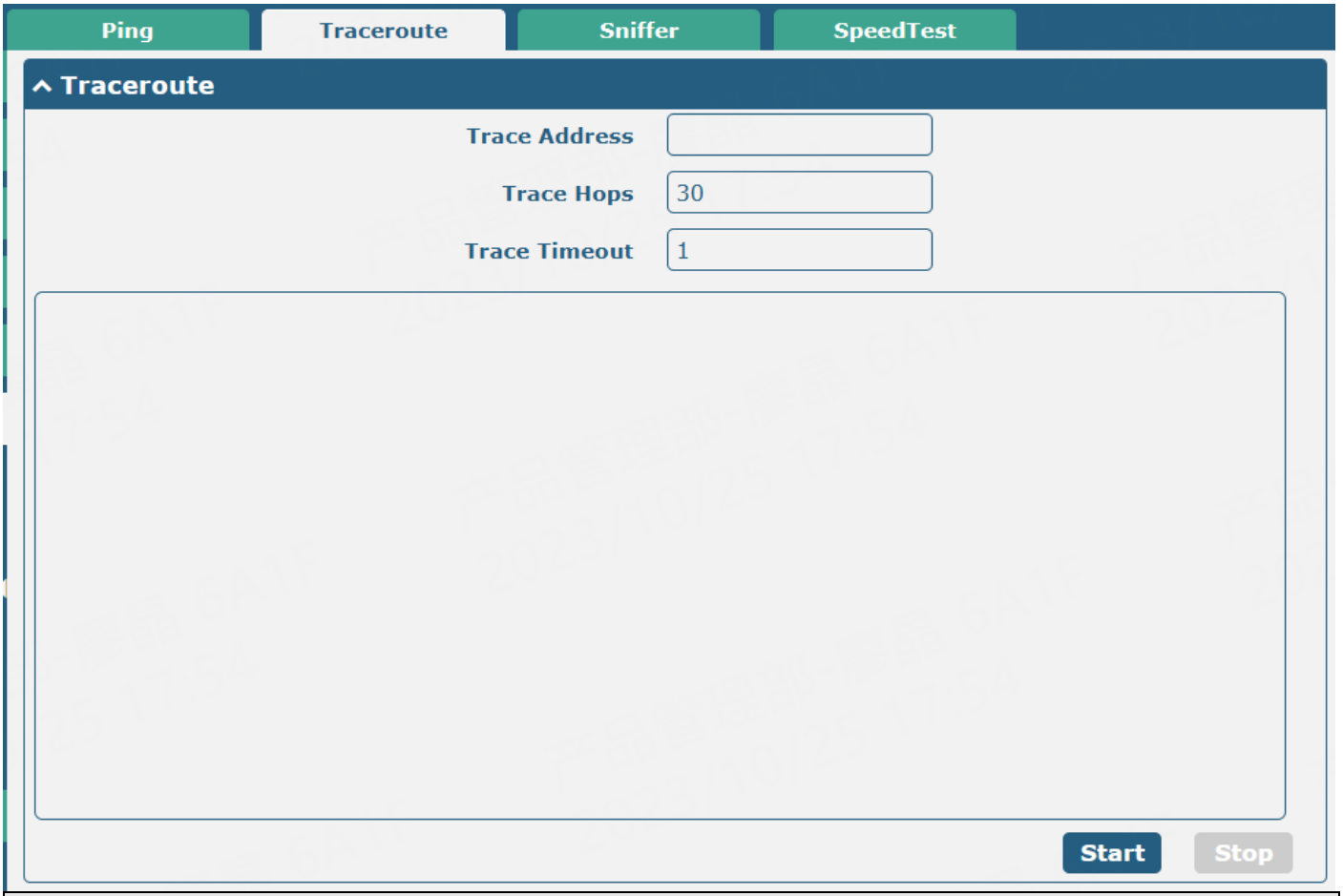
このセクションでは 、Ping ツールを使用できます。



ピン		
アイテム	説明	デフォルト
IP アドレス	ping の宛先 IP アドレスまたは宛先 ドメインを入力します。	Null
要求の数	ping 要求の数を指定します。	5
タイムアウト	ping 要求のタイムアウトを指定します。	1
ローカル IP	セルラーWAN、イーサネット WAN、またはイーサネット LAN からローカル IP を指定します。Null は、これら 3 つのアドレスからローカル IP アドレスを自動的に選択することを意味します。	Null
Start	ボタンをクリックすると ping リクエストが開始され、以下のボックスにログが表示されます。	--
Stop	ボタンをクリックして、ping 要求を停止します。	--

2) Traceroute

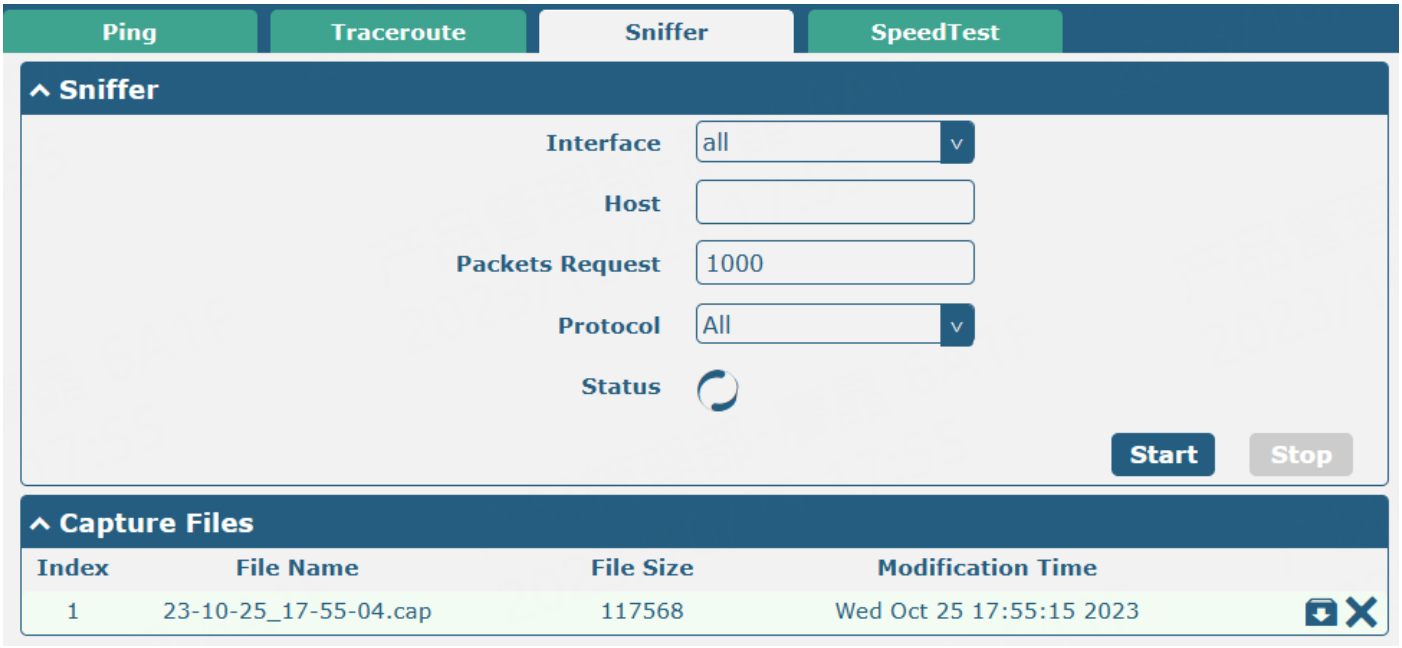
このセクションでは 、Traceroute ツールを使用できます。



トレースルート		
アイテム	説明	デフォルト
トレース・アドレス	トレースの宛先 IP アドレスまたは宛先ドメインを入力します。	Null
トレース ホップ	最大トレース ホップ数を指定します。トレース ホップが最大値に達すると、宛先に到達したかどうかに関係なく、デバイスはトレースを停止します。	30
トレース タイムアウト	Traceroute リクエストのタイムアウトを指定します。	1
Start	このボタンをクリックすると、Traceroute リクエストが開始され、以下のボックスにログが表示されます。	--
Stop	このボタンをクリックすると、Traceroute 要求が停止します。	--

3) Sniffer

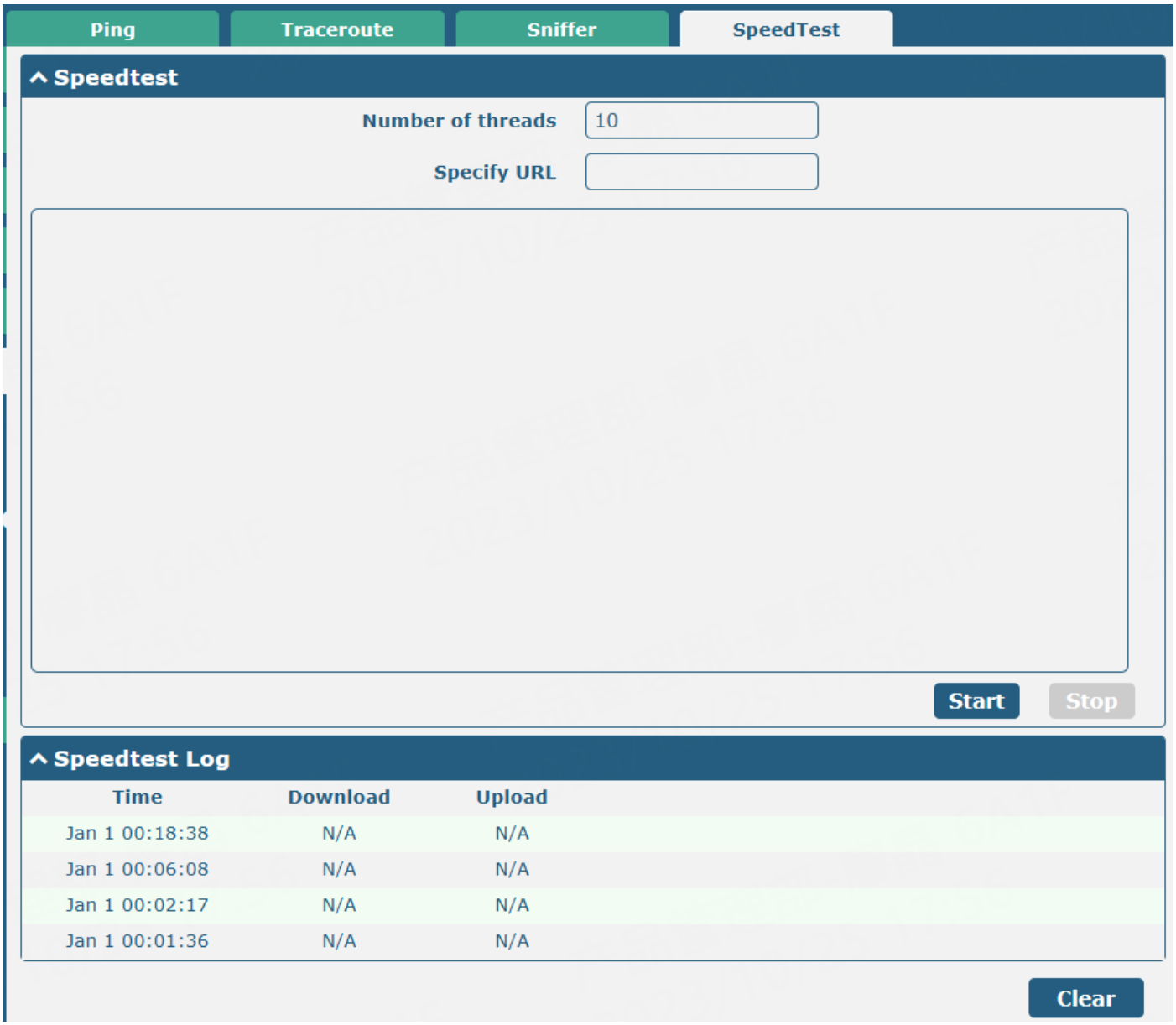
このセクションでは、スニファー ツールを使用できます。



スニファ		
アイテム	説明	デフォルト
インターフェイス	イーサネット構成に応じてインターフェイスを選択します。	すべての
ホスト	指定した IP アドレスを含むパケットをフィルター処理します。	Null
パケット要求	デバイスが一度にスニファできるパケット番号を設定します。	1000
プロトコル	「すべて」、「 IP」、「TCP」、「 UDP」、「ARP」から選択します。	すべての
ステータス	スニファの現在のステータスを表示します。	--
Start	ボタンをクリックしてスニファを開始します。	--
Stop	ボタンをクリックしてスニファを停止します。 このボタンをクリックすると、次のリストに新しいログファイル が表示されます。	--
ファイルのキャプチャ	スニファーログのたびに、新しいファイルとして自動的に保存されます。このスニファ トラフィック データ リストからファイルを見つけるには、クリックしてログをダウンロードし 、クリックしてログ ファイルを削除します。 最大 5 つのファイルをキャッシュできます。	--

4) スピードテスト

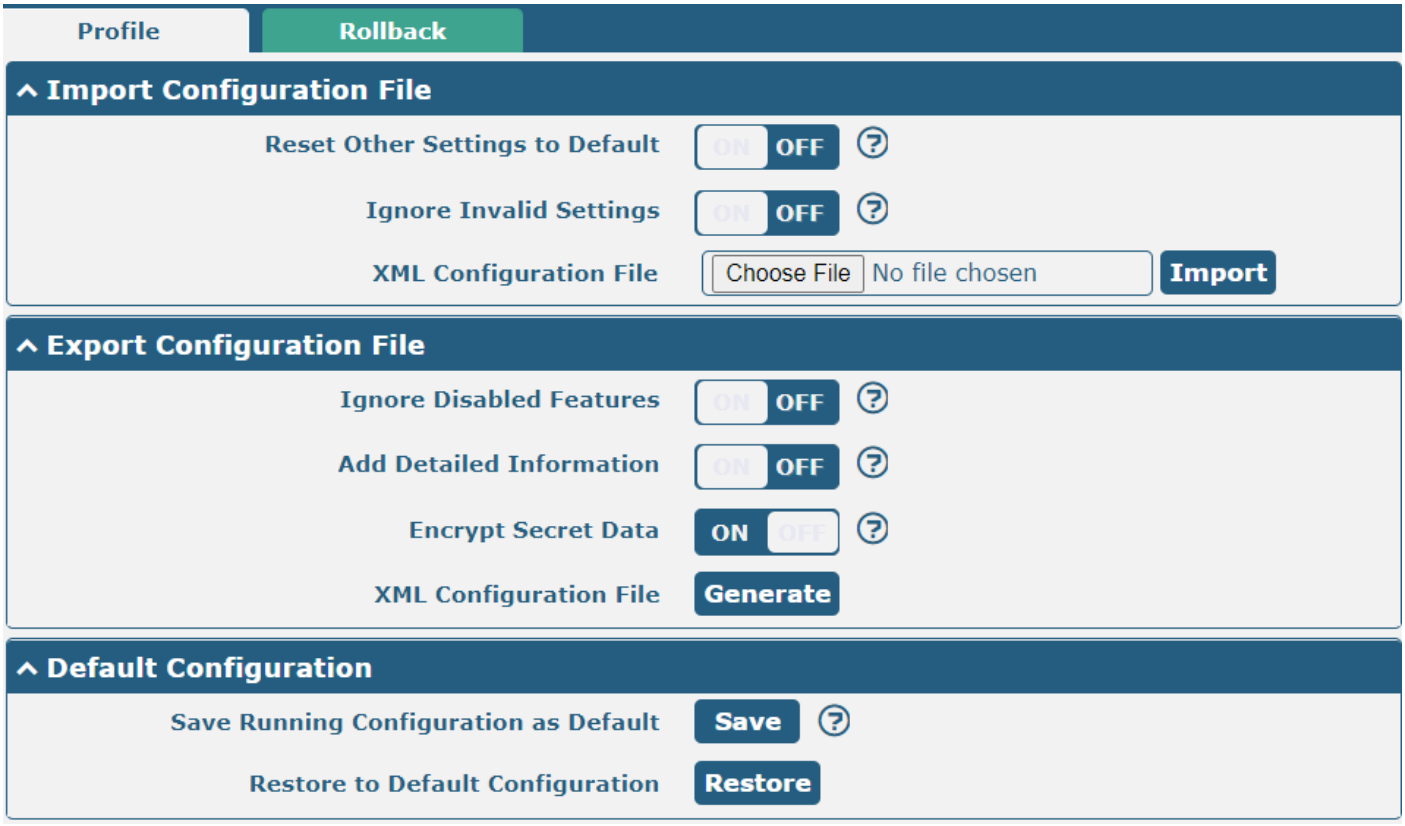
このセクションでは、SpeedTest ツールを使用できます。



スピードテスト		
アイテム	説明	デフォルト
スレッドの数	エキスパート設定項目には、ネットワーク速度テストスクリプトの実行時に有効にするスレッド数を入力します。10 に設定することをお勧めします。	10
ホスト	テスト中にアクセスするために指定した速度テスト サーバーの URL を入力します。空の場合は、最適なサーバーが自動的に選択されます。	Null
Start	このボタンをクリックすると、速度テストが開始され、上部ウィンドウにテスト情報がリアルタイムで表示されます。	--
Stop	このボタンをクリックすると、現在のテストの実行が停止します。	--
Clear	このボタンをクリックすると、ネットワークテストログのすべてのテスト結果がクリアされます。	--

3.7.5 プロフィール

このセクションでは、コンフィギュレーション ファイルをインポートまたはエクスポートし、デバイスを工場出荷時のデフォルト設定に復元できます。

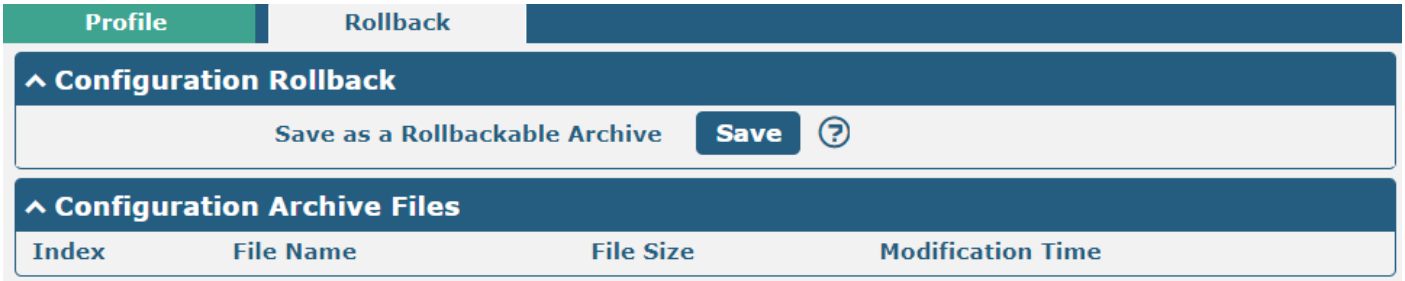


プロフィール		
アイテム	説明	デフォルト
構成ファイルのインポート		
その他の設定をデフォルトにリセット	トグルボタンを「ON」としてクリックすると、他のパラメータがデフォルト設定に戻ります。	オフ
無効な設定を無視	トグルボタンを「OFF」としてクリック すると、無効な設定が無視されます。	オフ
XML 構成ファイル	をクリックして Choose File PC から XML 構成ファイルを見つけ 、クリック Import してこのファイルをデバイスにインポートします。	--
構成ファイルのエクスポート		
無効な機能を無視 (Ignore Disabled Features)	トグルボタンを「OFF」としてクリックすると、無効になっている機能が無視されます。	オフ
詳細情報を追加する	トグルボタンを「オン」にして、詳細情報を追加します。	オフ
シークレットデータの暗号化	トグルボタンを「ON」としてクリックし、シークレットデータを暗号化します。	オン

XML 構成ファイル	Generate ボタンをクリックして XML 構成ファイルを生成し、 をクリックして XML 構成 Export ファイルをエクスポートします。	--
デフォルト設定		
実行コンフィギュレーションをデフォルトとして保存 (Save Running Configuration as Default)	Save ボタンをクリックして、現在の実行パラメータを デフォルト設定として保存します。	--
デフォルト設定への復元	ボタンをクリックして、工場出荷時のデフォルトに戻します。	--

1) ロールバック

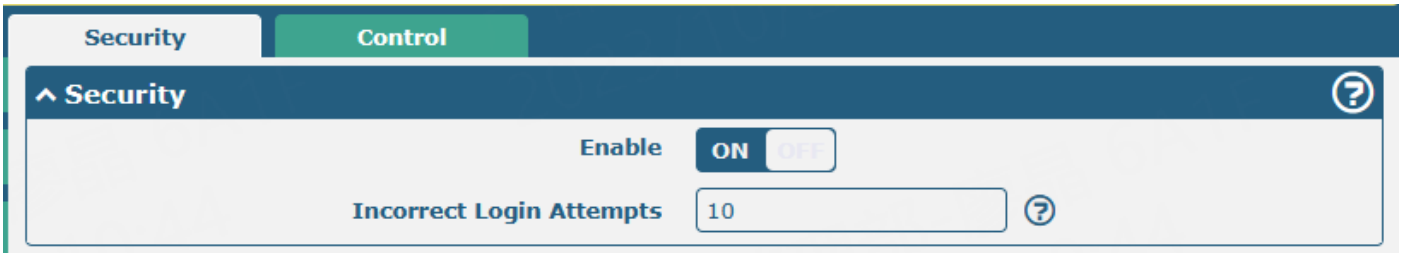
このセクションでは、設定をロールバックできます。



ロールバック		
アイテム	説明	デフォルト
設定のロールバック		
ロールバック可能なアーカイブとして保存	セーブポイントを手動で作成します。さらに、構成が変更されると、システムは毎日自動的にセーブポイントを作成します。	--
コンフィギュレーション アーカイブ ファイル		
コンフィギュレーション アーカイブ ファイル	構成アーカイブ・ファイルに関する関連情報(名前、サイズ、変更時刻など)を表示します。	--

3.7.6 アクセス制御

このセクションは、デバイスのセキュリティアクセス制御管理に関連する設定に使用されます。同じ IP アドレスが間違ったアカウントまたはパスワードを指定された回数入力すると、この IP はデバイスへのアクセスが制限されます。また、IP アドレスのブロックをバッチまたは個別に解除する機能も提供します。
注: 不正ログイン試行の上限に達する前に、ログイン成功後に累積エラー数がクリアされます。



Security@Access 制御		
アイテム	説明	デフォルト
エネーブル	セキュアなログインアクセスを有効/無効にします。	オン
不正なログイン試行	同じ IP アドレスが指定された回数間誤って入力された場合、この IP はデバイスへのアクセスが制限されます。値の範囲は 1~30 です。	10

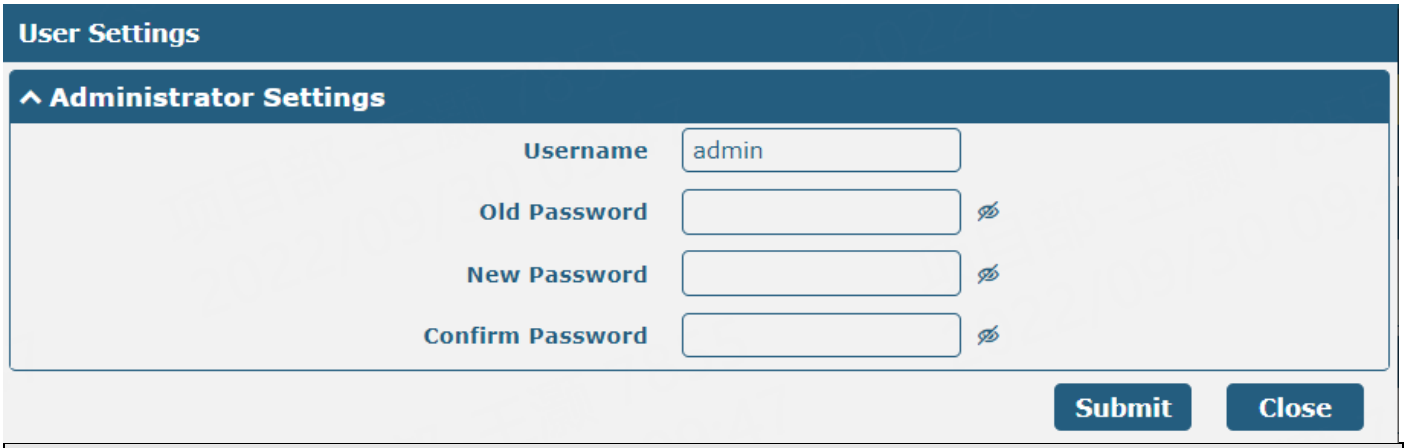
Control@Access 制御		
アイテム	説明	デフォルト
すべてブロック解除	[Unblock 有効/無効]ボタンをクリックして、デバイス上で制限されたアクセスを記録した IP アドレスをバッチで解放します。	--

注: すべてのアクセス制限付きデバイスの IP の表示をサポートし、IP 制限を個別に解除します。

3.7.7 ユーザー管理

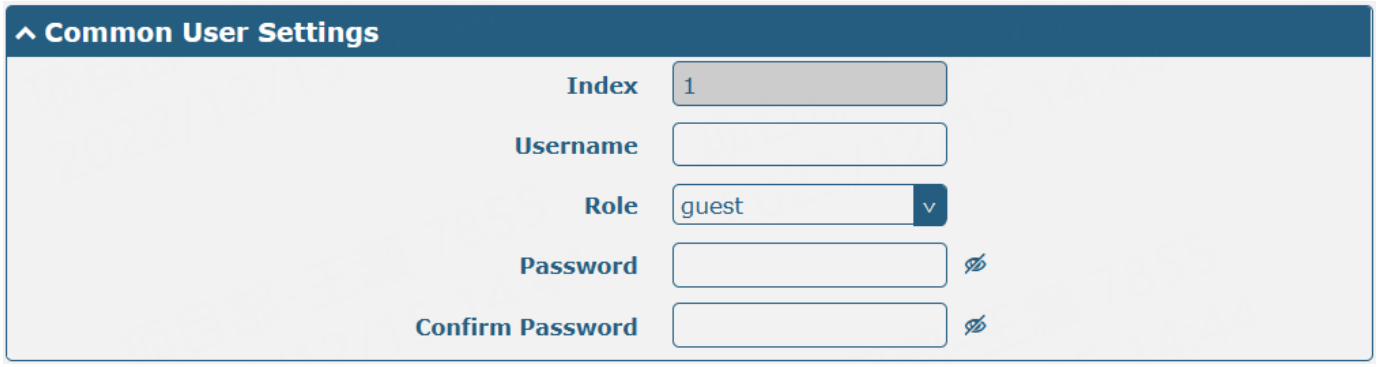
このセクションでは、ユーザー名とパスワードを変更したり、ユーザーアカウントを作成または管理したりできます。

クリックすると、管理者情報を変更できます。



アドミネーター設定		
アイテム	説明	デフォルト
ユーザー名	作成する新しいユーザー名を入力します。有効な文字は、a から z、A から Z、0 から 9、@,., -, #、$、および * です。	Null
古いパスワード	デバイスの古いパスワードを入力します。デフォルトは「admin」です。	Null
新しいパスワード	作成する新しいパスワードを入力します 。有効な文字は、a から z、A から Z、0 から 9、@,., -, #、$、および * です。	Null
パスワードの確認	確認のため、新しいパスワードをもう一度入力します。	Null

クリックすると、共通ユーザーを追加できます。



共通ユーザー設定		
アイテム	説明	デフォルト
ユーザー名	作成する新しいユーザー名を入力します。有効な文字は、a から z、A から Z、0 から 9、@,., -, #、$、および * です。	Null

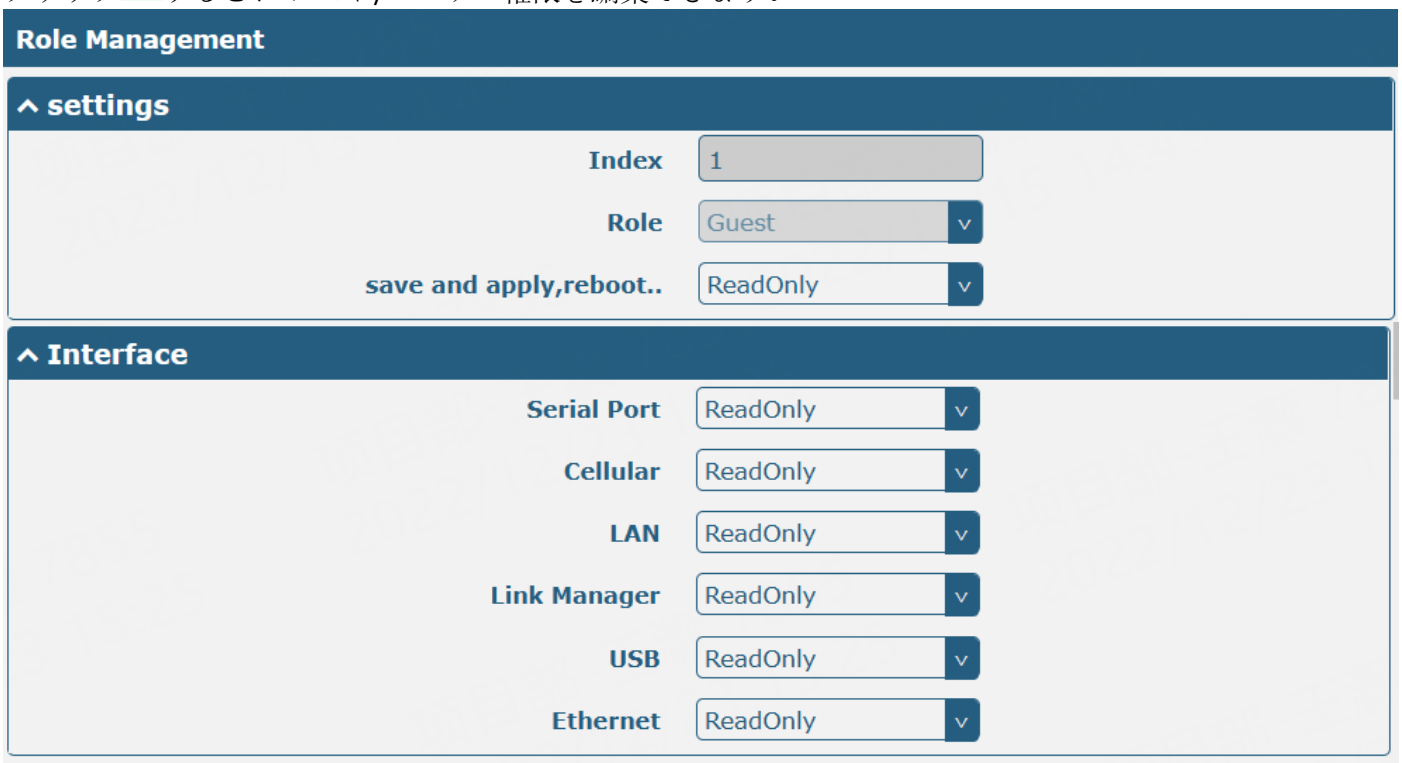
共通ユーザー 設定		
アイテム	説明	デフォルト
役割	共通ユーザーロールを選択します。ユーザーまたはゲストから選択	風
新しいパスワード	作成する新しいパスワードを入力します 。有効な文字は、a から z、A から Z、0 から 9、@,., -, #、$、および * です。	Null
パスワードの確認	確認のため、新しいパスワードをもう一度入力します。	Null

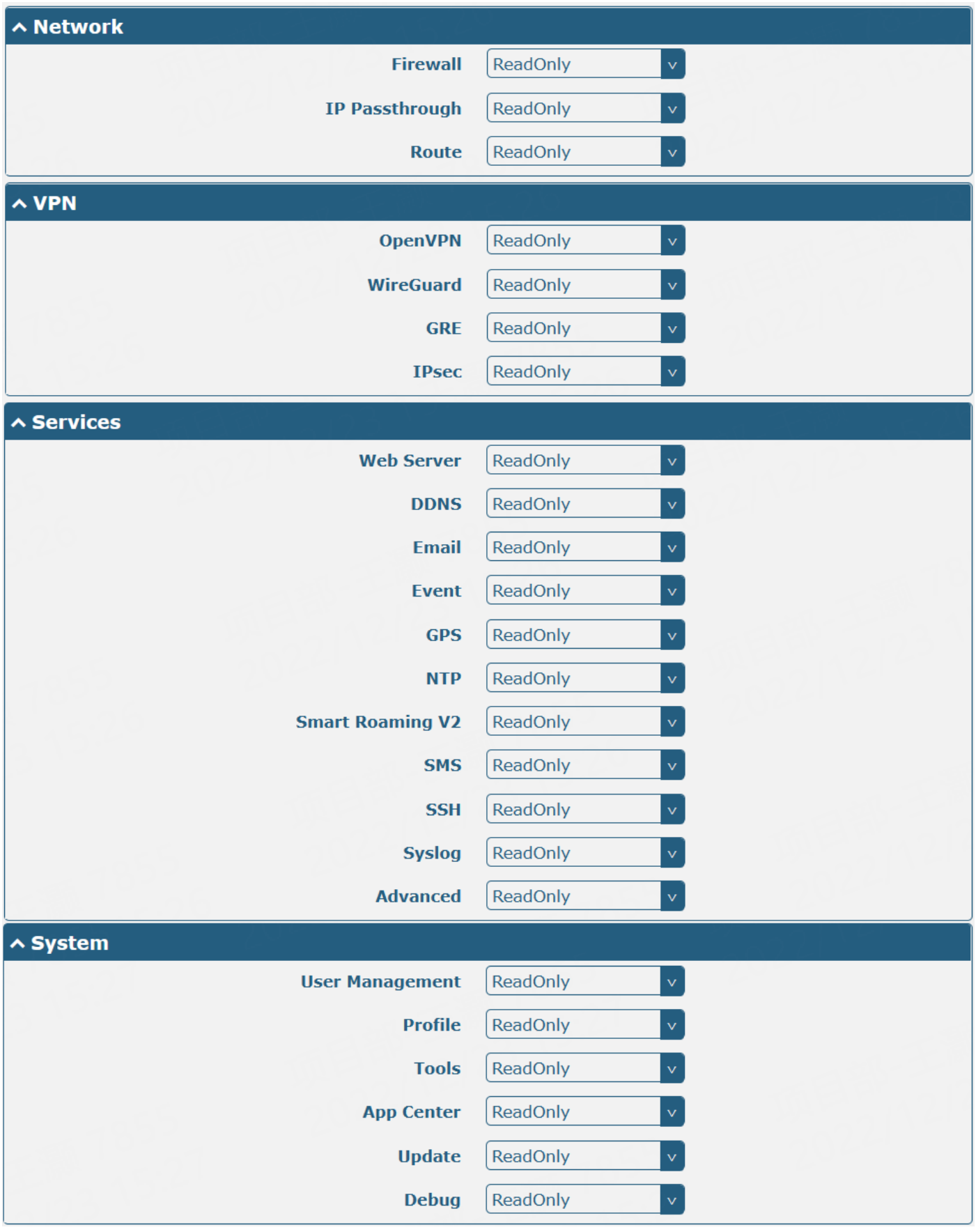
3.7.8 ロール 管理

このセクションは、ユーザーの役割を管理し、さまざまな役割のユーザーの権限を管理するために使用されます。

ロール名 @ ロール管理		
アイテム	説明	デフォルト
客	有効な文字は、a-z、A-Z、0-9、@,., -,、#、$、および * です。	客
利用者	ユーザー名を入力します。有効な文字は、a から z、A から Z、0 から 9、@,., -, #、$、および * です。	利用者

クリック すると、 ゲスト/ユーザー権限を編集できます。




Network
Firewall
ReadOnly
IP Passthrough
ReadOnly
Route
ReadOnly
VPN
OpenVPN
ReadOnly
WireGuard
ReadOnly
GRE
ReadOnly
IPsec
ReadOnly
Services
Web Server
ReadOnly
DDNS
ReadOnly
Email
ReadOnly
Event
ReadOnly
GPS
ReadOnly
NTP
ReadOnly
Smart Roaming V2
ReadOnly
SMS
ReadOnly
SSH
ReadOnly
Syslog
ReadOnly
Advanced
ReadOnly
System
User Management
ReadOnly
Profile
ReadOnly
Tools
ReadOnly
App Center
ReadOnly
Update
ReadOnly
Debug
ReadOnly

ユーザー権限 @ ロール管理	
アイテム	**説明**
何一つ	ユーザーには、この設定にアクセスしたり変更したりする権限がありません。
読み取り専用	ユーザーには読み取り権限のみがあります。
読み取り/書き込み	ユーザーには、この設定にアクセスまたは変更する権限があります。

手記:

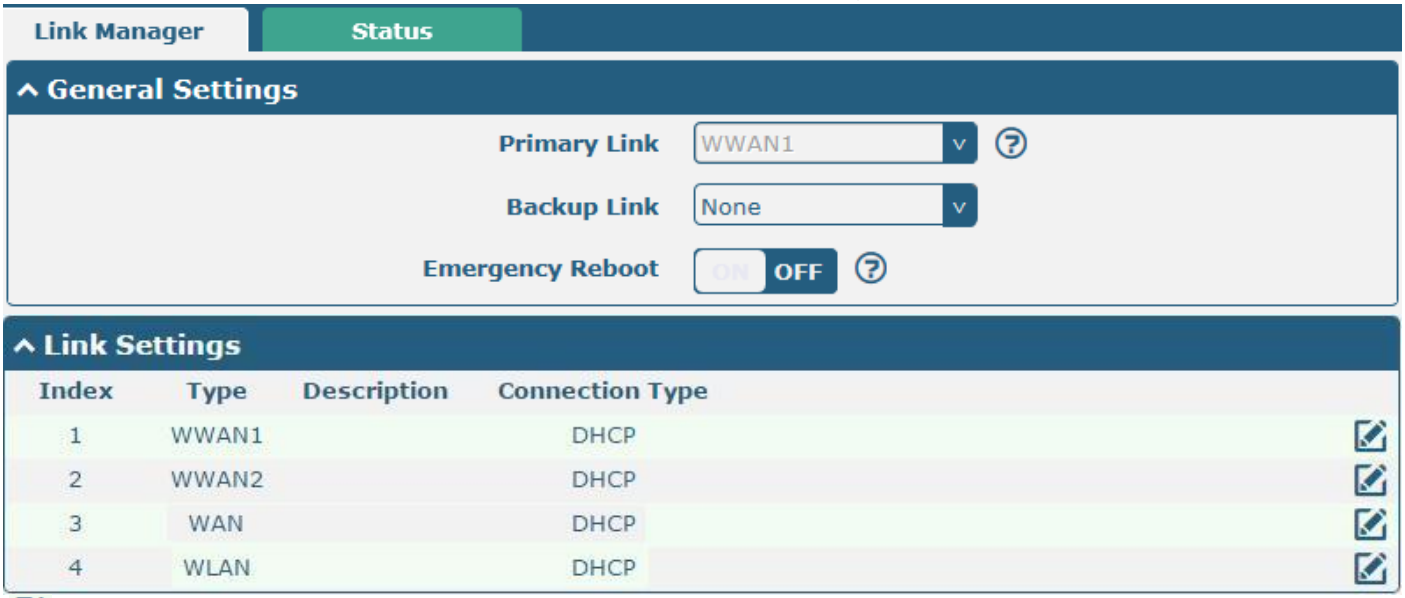
1. ゲスト/ユーザーでログインする場合、「プロファイル」は使用できません。
2. ゲストの「保存して適用し、再起動する」権限が「読み取り専用」に設定されている場合。ゲストでログイン後、「保存して適用」「再起動」ボタンは表示されません。

4. 設定例

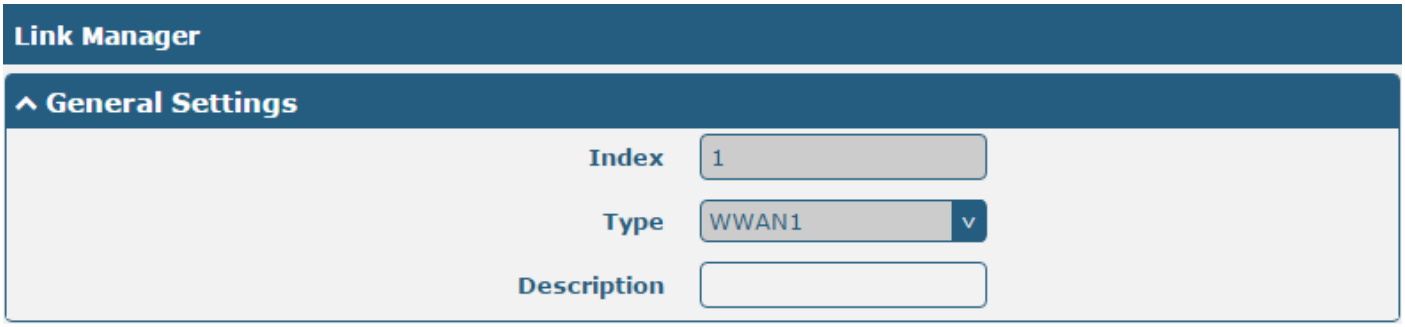
4.1 セルラー

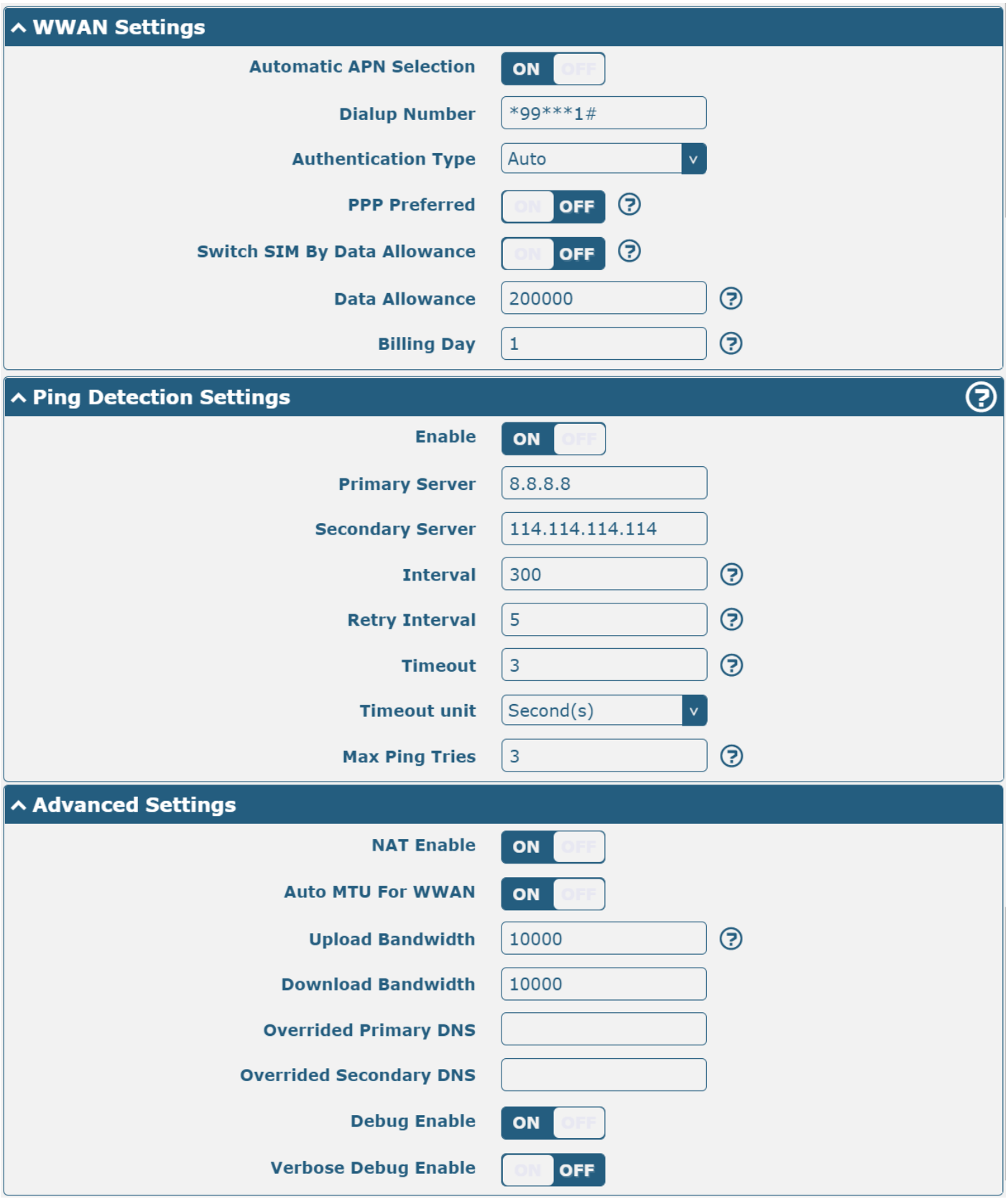
4.1.1 セルラーダイヤルアップ

このセクションでは、プライマリ SIM カードとバックアップ SIM カードをセルラーダイヤルアップ用に構成する方法について説明します。デバイスを正しく接続し、2 つの SIM を挿入してから、設定ページを開きます。ホームページメニューで、[**Interface > Link Manager > Link Manager > General Settings]をクリックし、プライマリリンクとして「WWAN1」、バックアップリンクとして「**WWAN2」を選択し、バックアップモードとして 「コールドバックアップ」を設定してから、「送信」をクリックします。



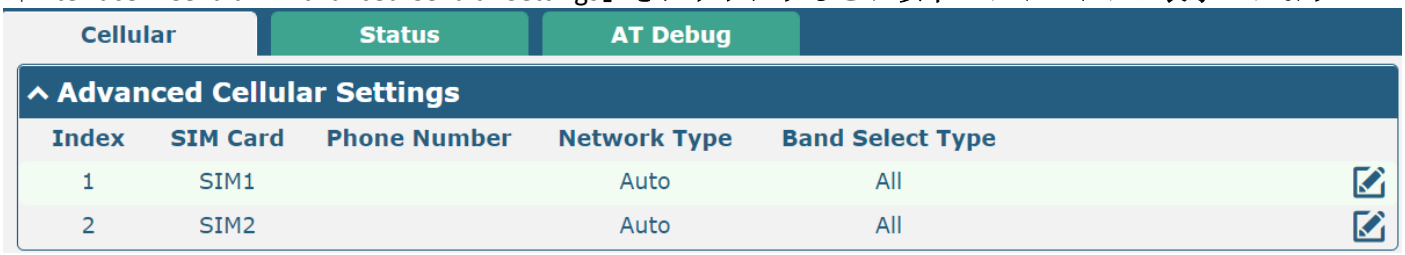
WWAN1 のボタンをクリックして、現在の ISP に従ってパラメータを設定します。



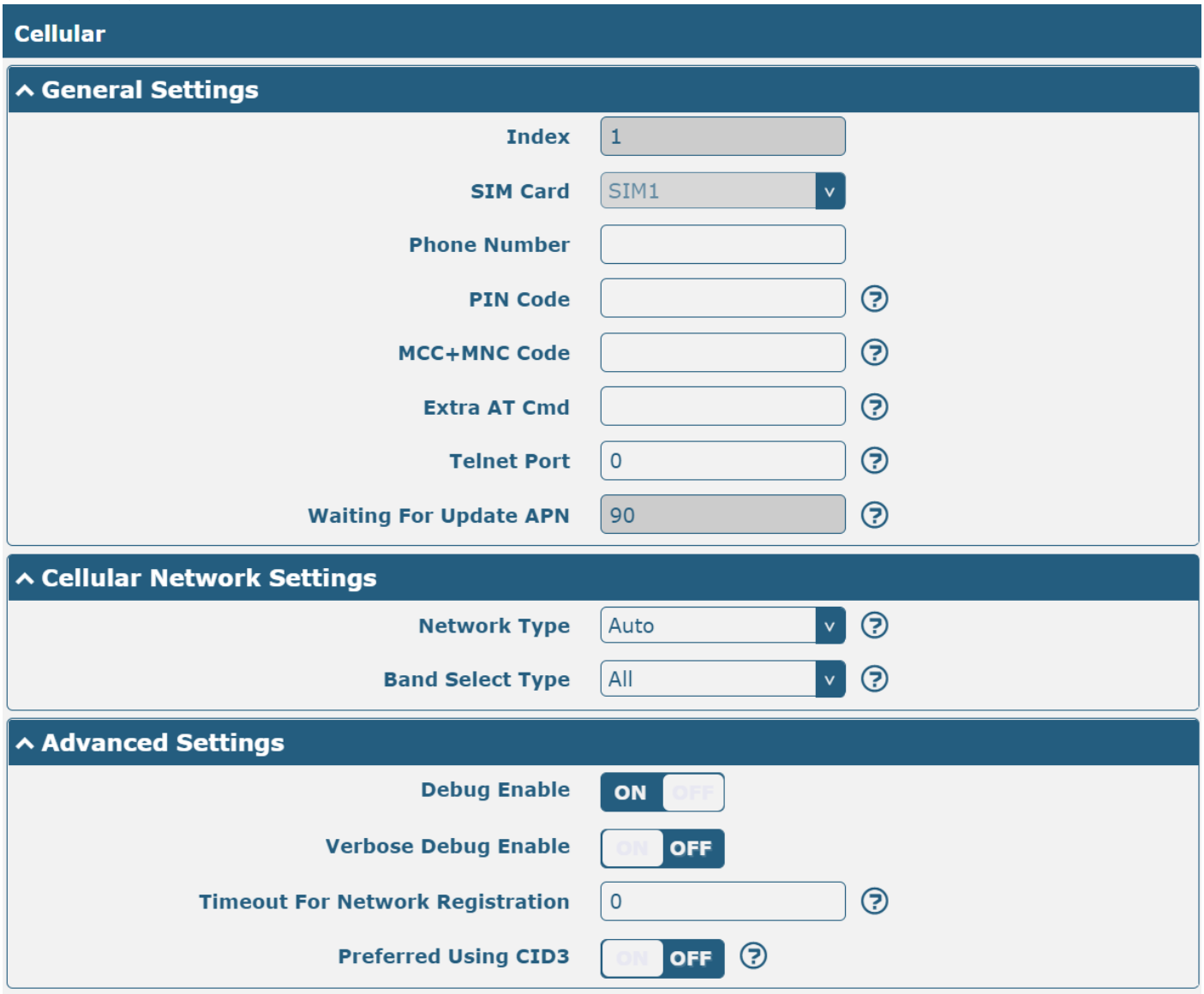


終了したら、「**Submit > Save & Apply**」をクリックして設定を有効にします。

「Interface > Cellular > Advanced Cellular Settings」をクリックすると、以下のウィンドウが表示されます。



SIM1 の編集ボタンをクリックして、アプリケーションの要求に応じてパラメータを設定します。



終了したら、「**Submit > Save & Apply**」をクリックして設定を有効にします。

4.1.2 SMS リモートコントロール

R2011 は SMS によるリモート コントロールをサポートしています。 次のコマンドを使用して、デバイスのステータスを取得し、デバイスのすべてのパラメーターを設定できます。

SMS コマンドの構造は次のとおりです。

1. パスワード モード:ユーザ名:**パスワード。cmd1 です。cmd2 です。cmd3 です。...cmdn** (すべての電話番号で使用可能)。
2. Phonenum モード -- **パスワード; cmd1; cmd2; cmd3; ...cmdn** (デバイスの電話グループに追加された電話番号から SMS が送信された場合に使用可能)。
3. 両方のモード-ユーザー名:**パスワード。cmd1 です。cmd2 です。cmd3 です。...cmdn** (デバイスの電話グループに追加された電話番号から SMS が送信された場合に使用可能)。

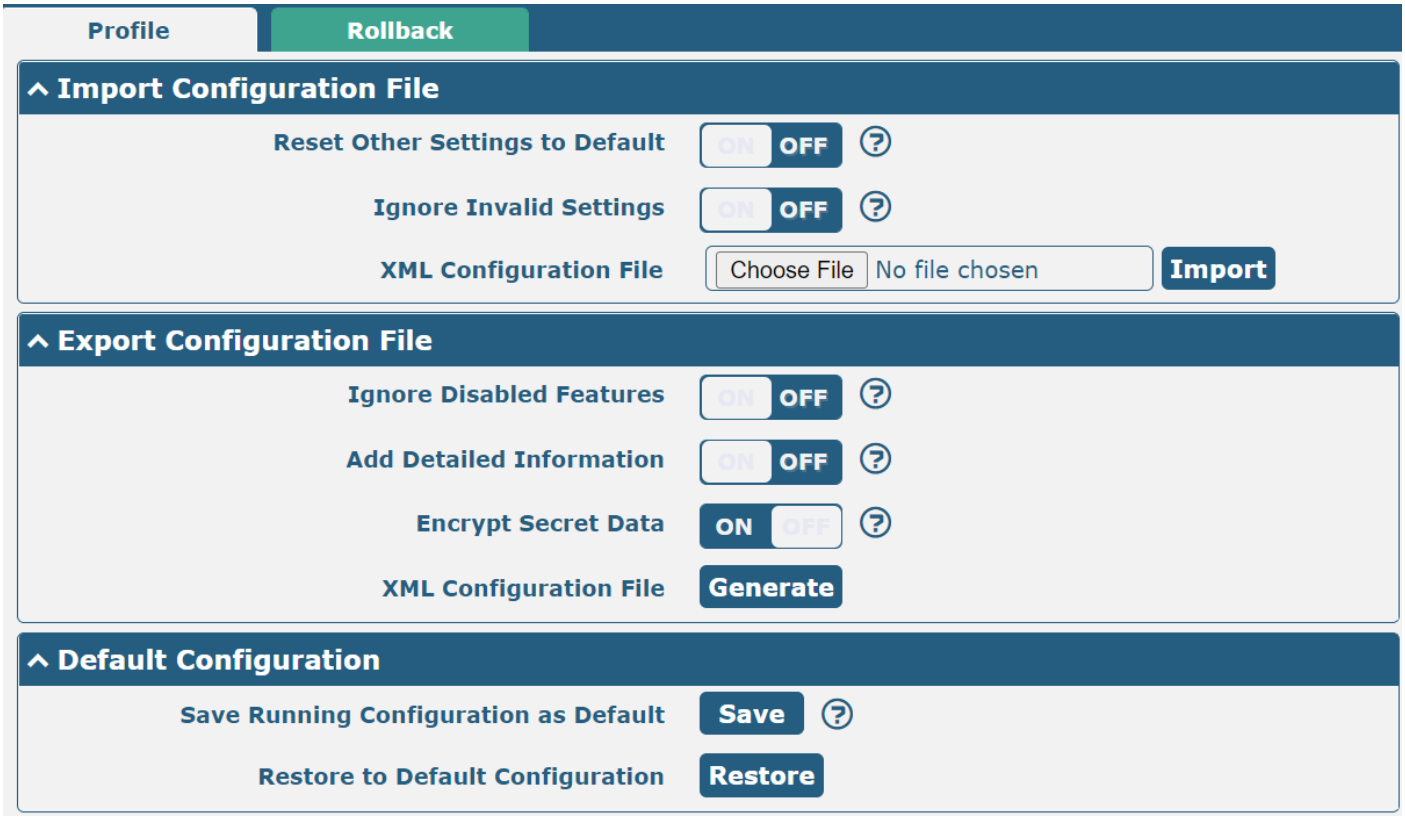
注: すべてのコマンド記号は、英語入力方式の半角モードで入力する必要があります。

SMS コマンドの説明:

1. ユーザー名とパスワード: 認証に WEB マネージャーと同じユーザー名とパスワードを使用します。
2. **cmd1, cmd2, cmd3 から cmdn へ**, コマンド形式は CLI コマンドと同じです、CLI cmd の詳細については、5.1 CLI とは.

   注: 設定済みの Web ブラウザから設定済みの XML ファイルをダウンロードします。 SMS 制御コマンドの 形式は、XML ファイルのデータを参照できます。

   「System > Profile > Export Configuration File」**に移動し**、クリックして XML ファイルを生成し、クリックして XML ファイルをエクスポートします。



XML コマンド:

<蘭>

<ネットワーク max_entry_num="5" >

<id>1</id>

<interface>lan0</interface>

<ip>172.16.24.24</ip>

<netmask>255.255.0.0</netmask>

<MTU>1500</MTU>

SMS コマンド:

LAN ネットワーク 1 インターフェイス lan0 を設定します

LAN ネットワーク 1 の IP アドレス 172.16.24.24 を設定します

LAN ネットワーク 1 ネットマスク 255.255.0.0 を設定します

LAN ネットワーク 1 MTU 1500 を設定します

3. セミコロン文字(';')は、1 つの SMS にパックされた複数のコマンドを区切るために使用されます。
4. 例えば。

admin:admin です。ステータスシステム

このコマンドでは 、ユーザー名は「admin」、パスワードは「admin」、制御コマンドは「status system」で、コマンドの機能はシステムステータスを取得することです。

SMS 受信:

hardware_version = 1.0

firmware_version = beta210618

firmware_version_full = "beta210618 (Rev 4250)"

kernel_version = 4.9.152

device_model = R2011

serial_number = ""

稼働時間= "0 日、01 時 25 分 16 秒"

system_time = "2021 年 4 月 21 日 17:09:04 火曜日"

ram_usage = "77M Free/128M Total"

admin:admin です。リブート

このコマンドでは 、ユーザ名は「admin」、パスワードは「admin」、コマンドはデバイスをリブートすることです。

SMS 受信:

わかりました

admin:admin です。ファイアウォールを false remote_ssh_access 設定します。ファイアウォールを false remote_telnet_access 設定する

このコマンドでは、ユーザ名は「admin」、パスワードは「admin」で、コマンド は remote_ssh と remote_telnet アクセスを無効にすることです。

SMS 受信:

わかりました

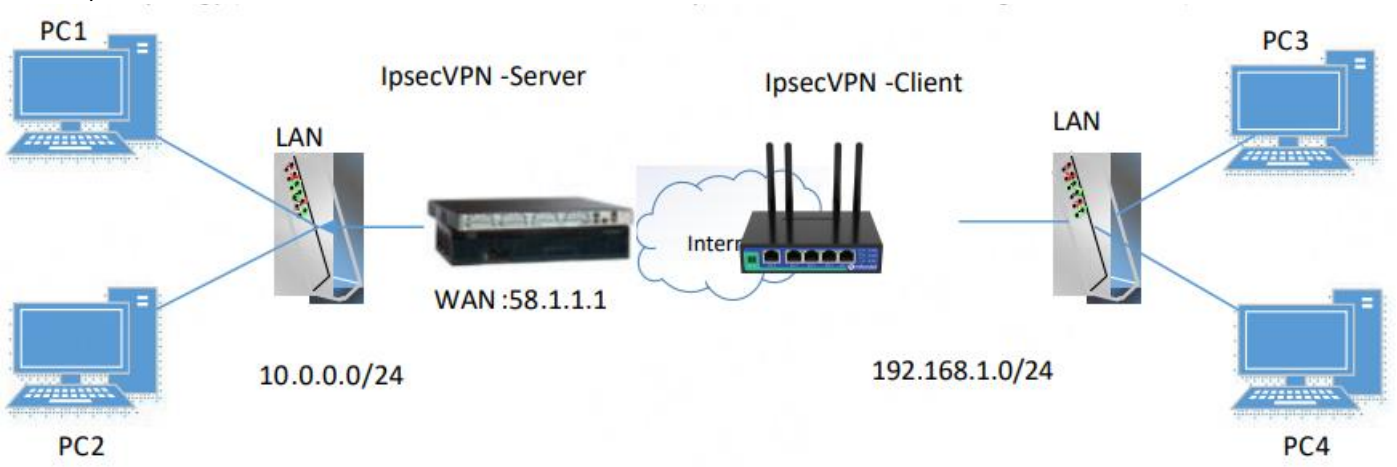
わかりました

admin:admin です。LAN ネットワーク 1 インターフェイス lan0 を設定します。LAN ネットワーク 1 IP 172.16.24.24 を設定します。LAN ネットワーク 1 ネットマスク 255.255.0.0 を設定します。LAN ネットワーク 1 MTU 1500 を設定します
このコマンドでは、ユーザ名は「admin」、パスワードは「admin」で、コマンドは LAN パラメータを設定することです。
SMS 受信:
わかりました
わかりました
わかりました
わかりました

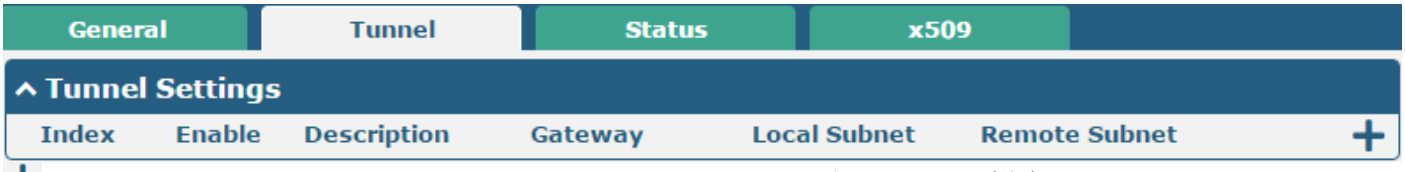
4.2 VPN の設定例

4.2.1 IPsec VPN

IPsec VPN トポロジ(サーバ側とクライアント側の IKE パラメータと SA パラメータを同じに設定する必要があります)。



IPsec VPN_Client:
「VPN > IPsec > Tunnel」をクリックすると、以下のウィンドウが表示されます。"



ボタンをクリックして、IPsec クライアントのパラメータを以下のように設定します。

Tunnel

General Settings

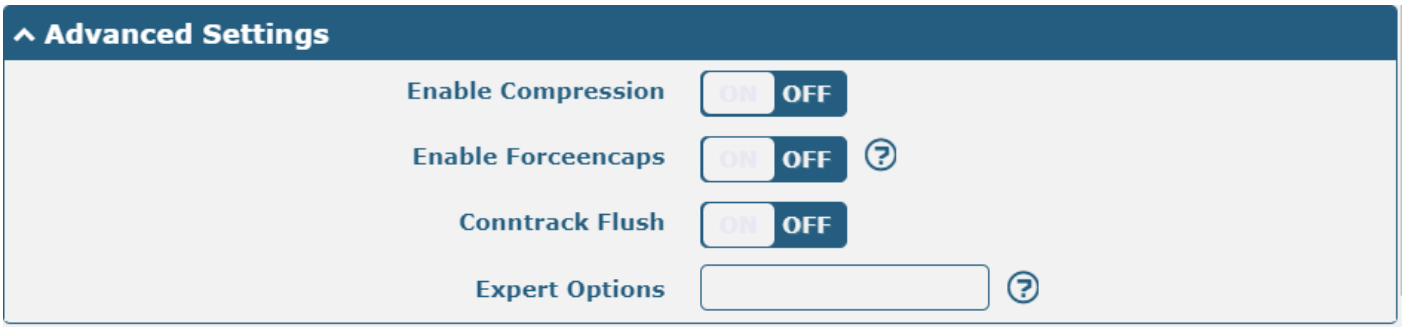
Index	1
Enable	ON OFF
Description	
Gateway	
Backup Gateway	
Mode	Tunnel
Protocol	ESP
Local Subnet	
Local Protoport	
Remote Subnet	
Remote Protoport	
Link Binding	Unspecified

IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	PSK
PSK Secret	
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	86400

SA Settings

Encryption Algorithm	3DES
Authentication Algorithm	SHA1
PFS Group	DHgroup2
SA Lifetime	28800
DPD Interval	30
DPD Failures	150



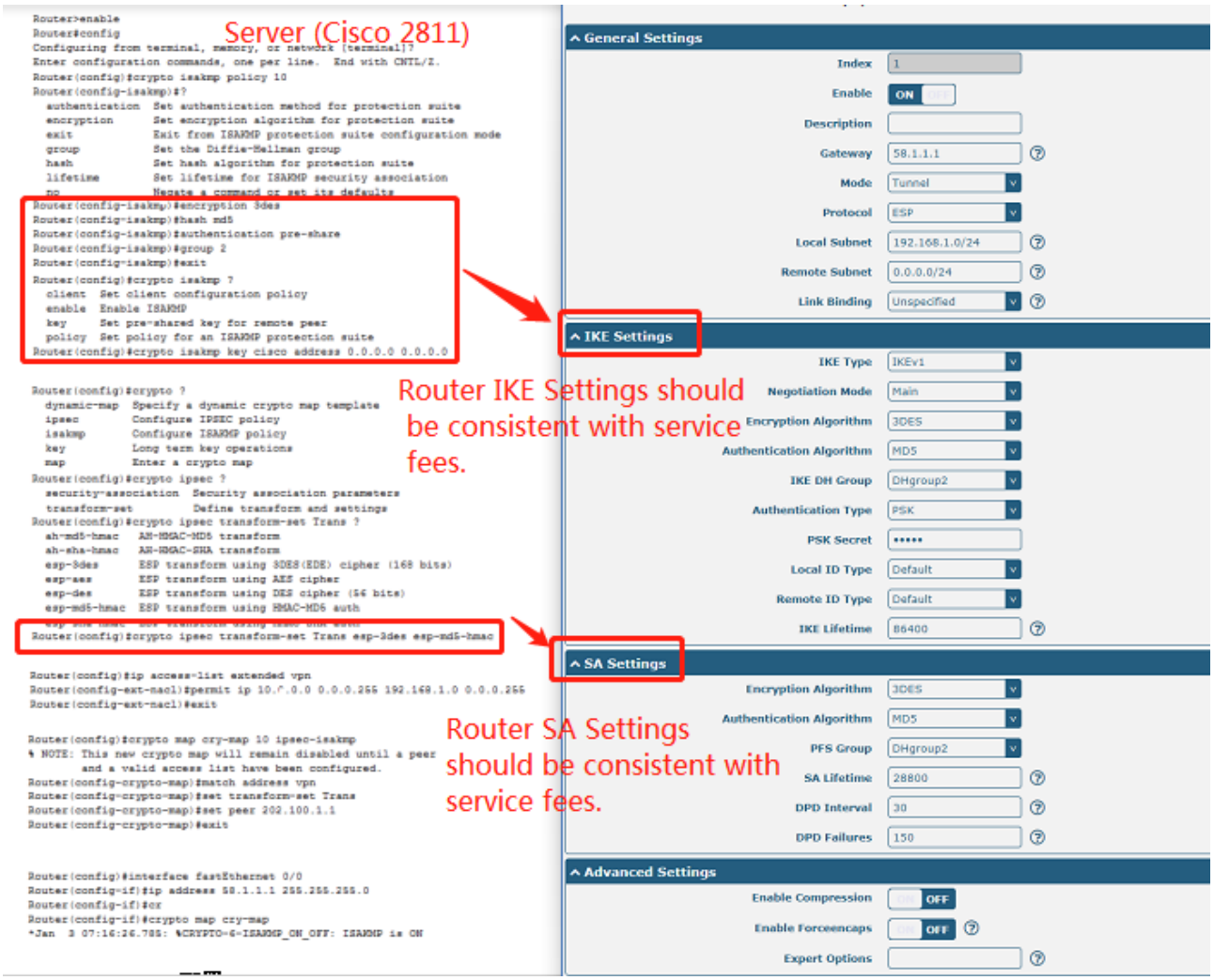
終了したら、「**Submit > Save & Apply**」をクリックして設定を有効にします。

IPsecVPN_Server:

シスコ 2811:

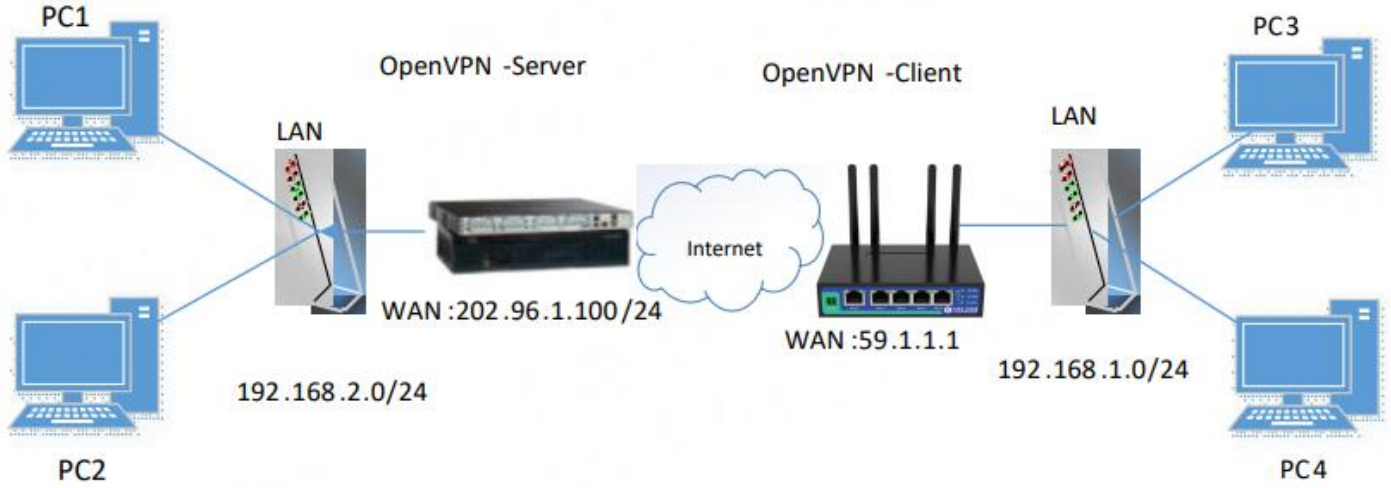
```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp ?
  client  Set client configuration policy
  enable  Enable ISAKMP
  key     Set pre-shared key for remote peer
  policy  Set policy for an ISAKMP protection suite
Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0


Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association parameters
  transform-set         Define transform and settings
Router(config)#crypto ipsec transform-set Trans ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-sha-hmac  ESP transform using HMAC-SHA auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac


Router(config)#ip access-list extended vpn
Router(config-ext-nacl)#permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config-ext-nacl)#exit

Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1
Router(config-crypto-map)#exit



Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 58.1.1.1 255.255.255.0
Router(config-if)#cr
Router(config-if)#crypto map cry-map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

サーバーとクライアントの比較は以下の通りです。



4.2.2 OpenVPN の

OpenVPN は、クライアントと P2P の 2 つのモードをサポートしています。ここでは、クライアントを例に説明します。

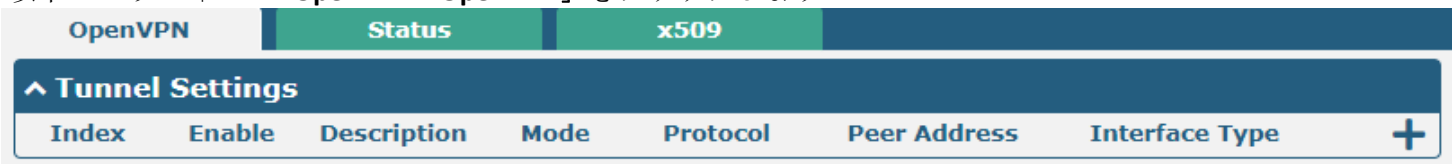


OpenVPN_Server:

最初にサーバー側で関連する OpenVPN 証明書を生成し、次のコマンドを参照してサーバーを構成します。
ローカル 202.96.1.100
モード・サーバー (mode server)
ポート 1194
したがって、UDP
dev tun (デヴ トゥン)
TUN-MTU 1500
フラグメント 1500
CA ca.crt (英語)
cert Server01.crt (英語)
キー Server01.key
の dh dh1024.pem
サーバー 10.8.0.0 255.255.255.0
ifconfig-セミパーシステント ipp.txt
「ルート 192.168.3.0 255.255.255.0」をプッシュします
client-config-dir ccd (クライアント設定ディレクトリ ccd)
ルート 192.168.1.0 255.255.255.0
キープアライブ 10 120
暗号 BF-CBC
コンプ- LZO
最大クライアント数 100
永続キー (persist-key)
persist-tun (永続 tun)
ステータス openvpn-status.log
動詞 3
注:設定の詳細については、テクニカルサポートエンジニアにお問い合わせください。

OpenVPN_クライアント:

以下のように「**VPN > OpenVPN > OpenVPN**」をクリックします。

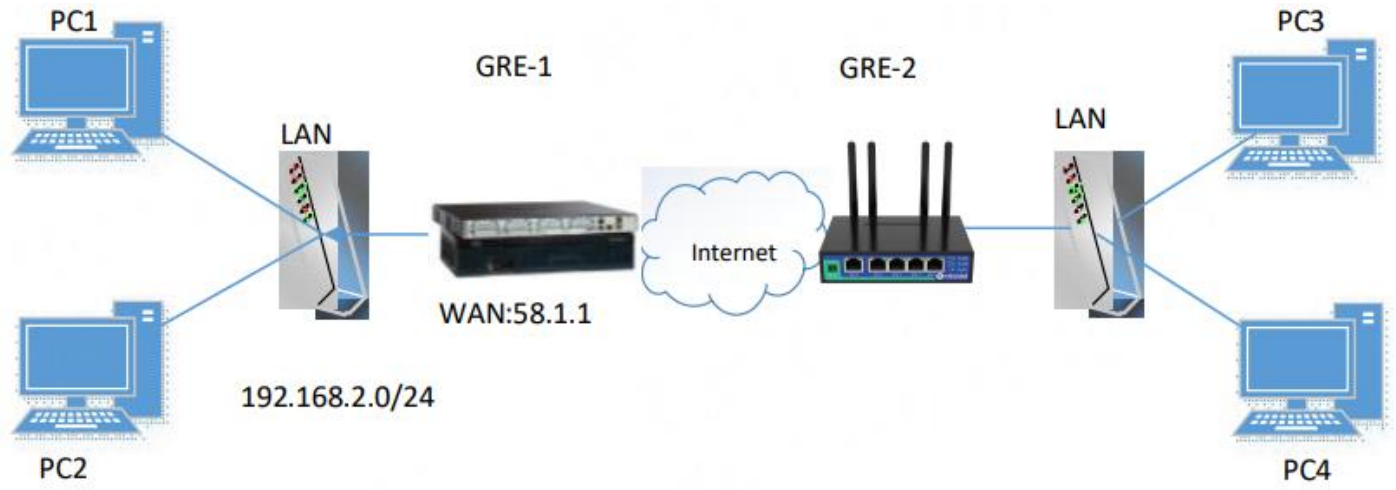


クリック＋すると、Client01 が次のように構成されます。

終了したら、「**Submit > Save & Apply**」をクリックして設定を有効にします。

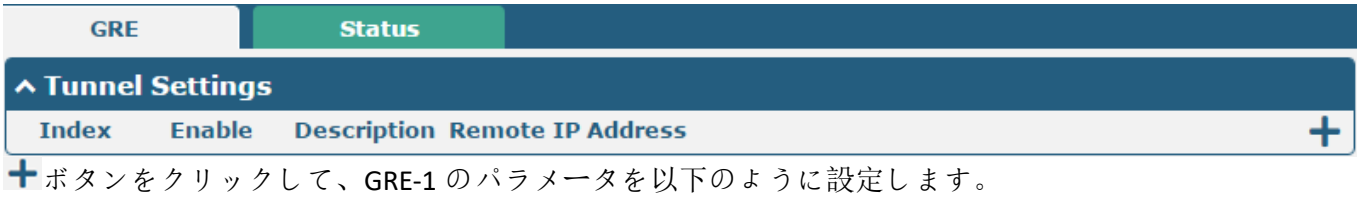
4.2.3 GRE VPN

GRE VPN トポロジ

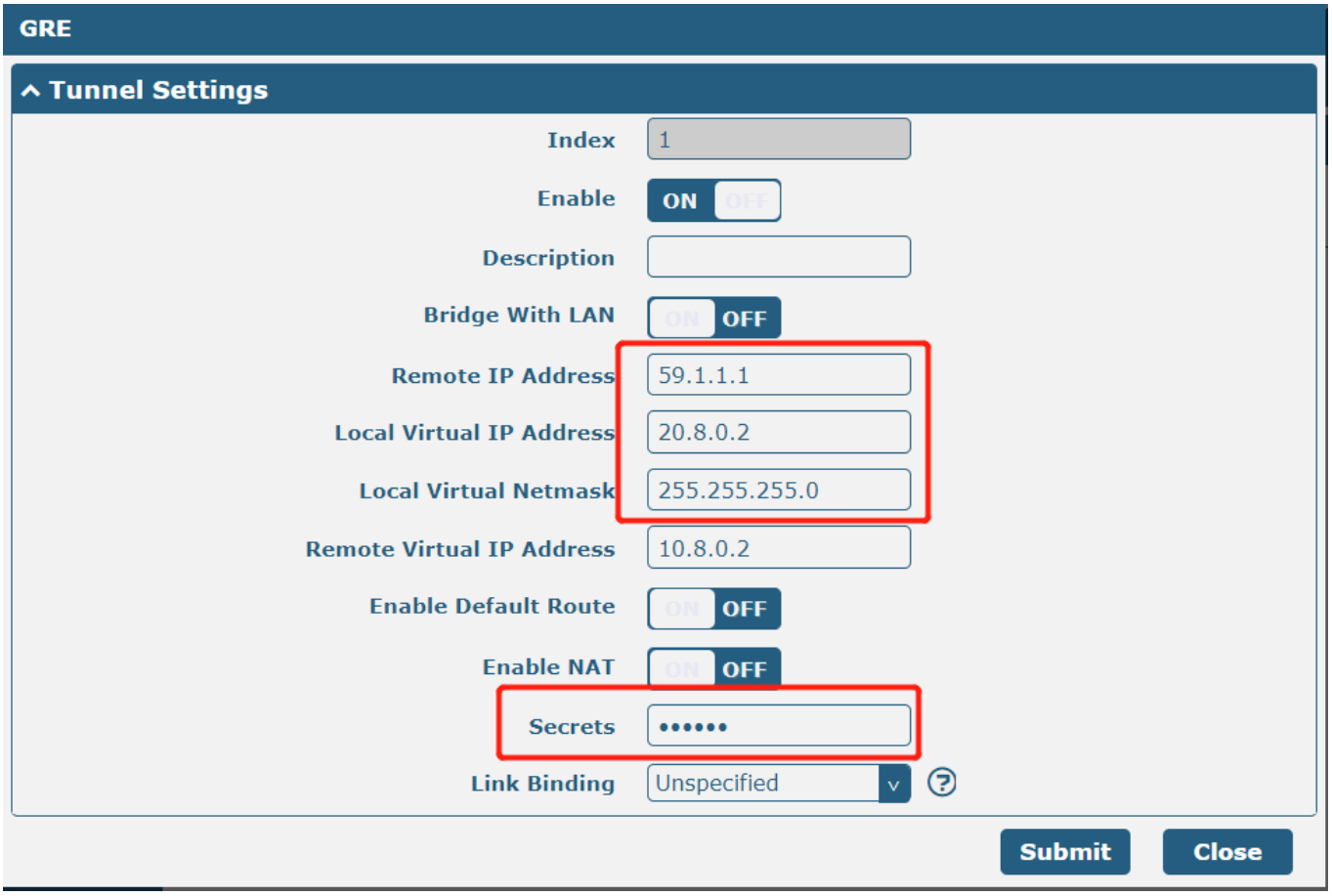


GRE-1:

「VPN > GRE > GRE」をクリックすると、以下のウィンドウが表示されます。



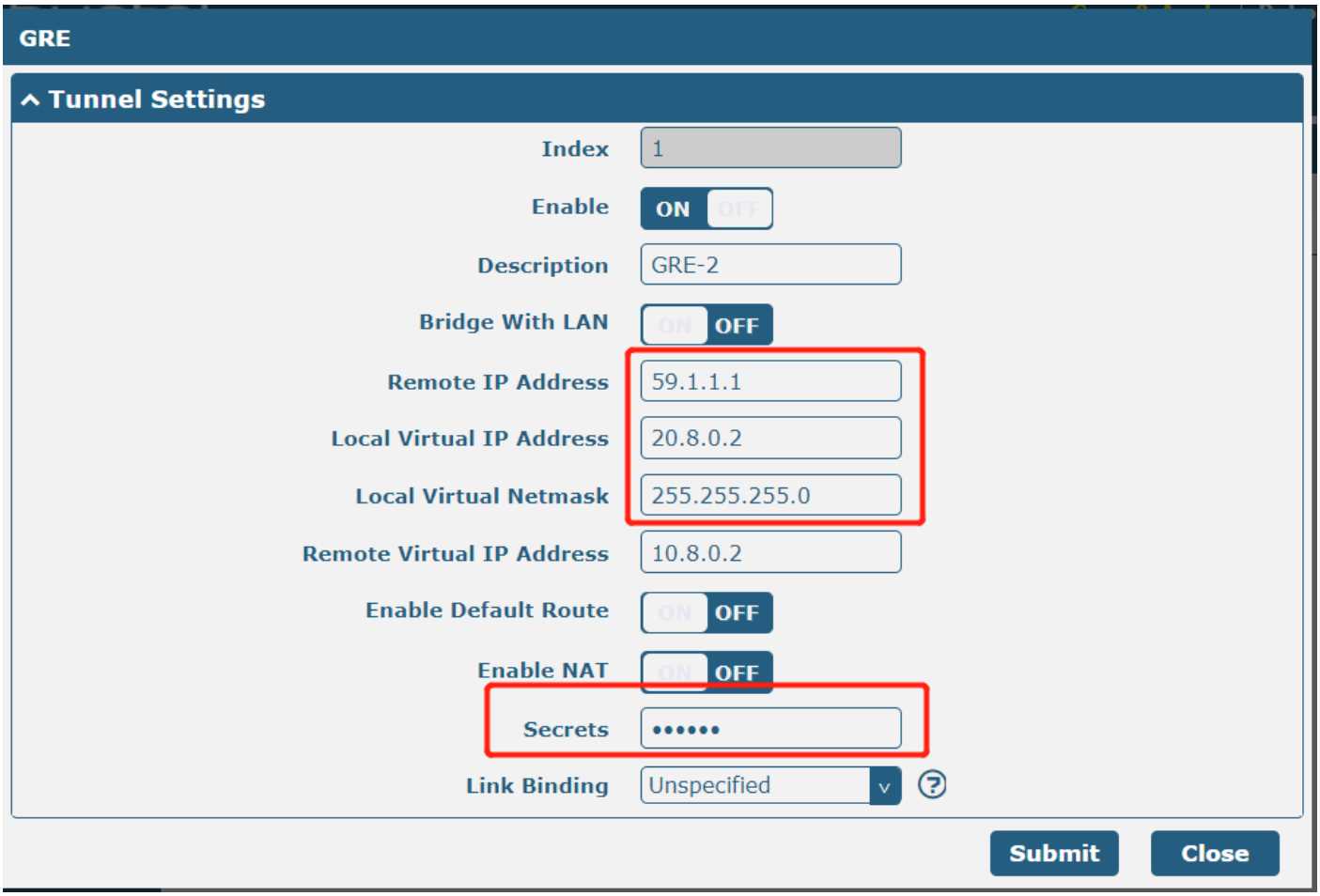
ボタンをクリックして、GRE-1 のパラメータを以下のように設定します。



終了したら、「**Submit > Save & Apply**」をクリックして設定を有効にします。

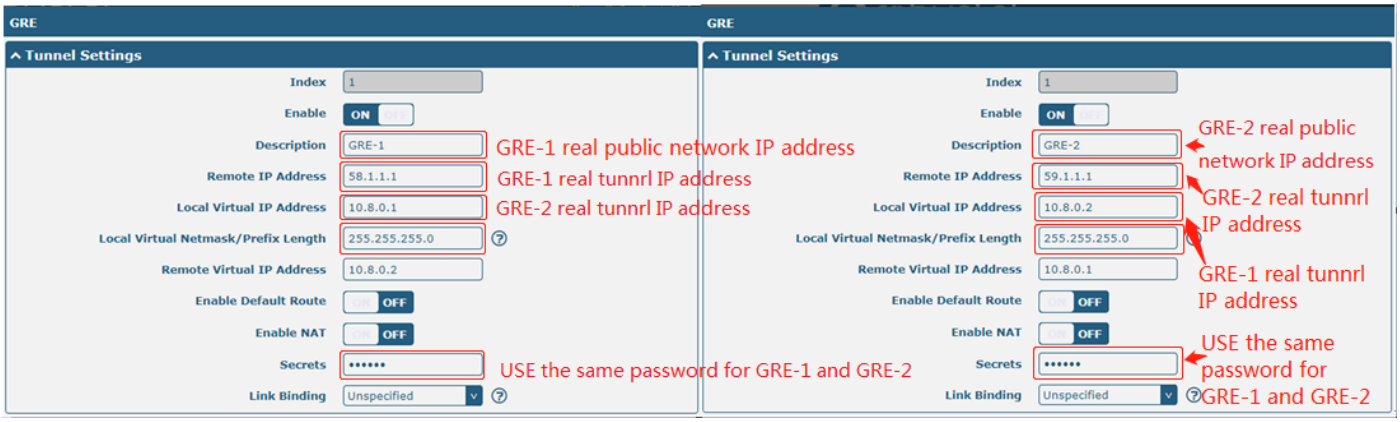
GRE-2:

ボタンをクリックして、GRE-2 のパラメータを以下のように設定します。



終了したら、「**Submit > Save & Apply**」をクリックして設定を有効にします。

GRE-1 と GRE-2 の比較は以下の通りです。



5. CLI の概要

5.1 CLI とは

コマンドラインインターフェイス(CLI)は、SSH または Telnet ネットワーク接続を介して機器のパラメータを設定する別の方法を提供するソフトウェアインターフェイスです 。デバイスとの Telnet または SSH 接続を確立した後、次に示すように、ログインアカウントとパスワード(デフォルトの admin/admin)を入力して、デバイスの設定モードに入ります。

ルートログイン:

デバイス ログイン:admin

パスワード: admin

#

CLI コマンド:

?

! コメント

add 設定のリストエントリを追加

add_preferred スマート ローミング 優先 PLMN リストの追加

clear 統計のクリア

config 構成操作

debug デバッグ情報をコンソールに出力します

del 設定のリストエントリを削除する

スマートローミング delete_preferred、優先するすべての通信事業者を削除する

do do のレベル状態を設定します。

exit CLI を終了します

スマートローミングネットワークの再スキャン force_rescan

forget_rplmn スマート ローミング RPLMN を忘れる

help CLI 構文の概要を表示します。

ipsec_cert_get http または ftp 経由で IPSec 証明書ファイルをダウンロードする

ovpn_cert_get OpenVPN 証明書ファイルを http または ftp 経由でダウンロードする

ping を実行 ネットワークホストにメッセージを送信する

reboot 停止してコールドリスタートを実行する

saveConfig 実行コンフィギュレーションをデフォルトとして保存

スマートローミング選択演算子の選択

set システム構成の設定

show システム構成の表示

show_networks スキャンするネットワークを表示します。

スピードテスト スピードテスト

status 実行中のシステム情報を表示する

tftp_upload_diagnostic TFTP を使用して診断ファイルを生成し、アップロードします
tftpupdate tftp を使用してファームウェアまたは設定ファイルを更新する
traceroute ネットワークホストへのルートパケットトレースを出力します
トリガー トリガー アクション
アンインストール アプリをアンインストールする
UploadConfig 現在の UCI 設定を FTP サーバにアップロード
urlupdate http や ftp でファームウェアを更新する
ver ファームウェアのバージョンを表示

5.2 CLI の設定方法

以下の表は、ヘルプの説明と、構成プログラムで発生するエラーに関するものです。

コマンド/ヒント	説明
?	疑問符「?」を入力すると、 ヘルプ情報が表示されます。 例えば。 # config('?' を押します。) config 構成操作 # config(スペースバー+'?') commit 設定変更を保存し、変更した設定を有効にします save_and_apply 設定の変更を保存し、変更した設定を有効にします loaddefault 工場出荷時の設定の復元
Ctrl + C キー	これら 2 つのキーを同時に押すと、「コピー」機能がなくなりますが、設定プログラムから「抜け出す」ためにも使用できます。
構文エラー: コマンドが完了していません	コマンドは完了しません。
目盛りスペースキー+Tab キー	それはあなたがあなたのコマンドを完了するのを助けることができます。 例: # config (tick enter キー) 構文エラー: コマンドが完了していません # config (ティックスペースキー+Tab キー) loaddefault save_and_apply コミット
コミット #config # コンフィグ save_and_apply	設定が完了したら、これらのコマンドを入力して、デバイスで設定を有効にする必要があります 。 ***注:*** *コミットと save_and_apply は同じ役割を果たします。*

5.3 コマンド リファレンス

コマンド	構文	説明
デバッグ	デバッグ パラメーター	デバッグ機能をオンまたはオフにする
見せる	パラメータを表示	各関数の現在の構成を表示します。
セット	パラメータの設定	すべての関数パラメータはコマンド set と add によって設定さ

足す	*パラメーターを追加する*	れますが、違いは set が単一のパラメータ用であり、add が list パラメータ用であることです

注: *構成済みの Web ブラウザーから config.XML ファイルをダウンロードします。コマンド形式は、config.XML ファイル形式を参照できます。*

5.4 設定例を使用したクイックスタート

CLI をマスターする最良かつ最速の方法は、まず Web ページからすべての機能を表示し、次に一度にすべての CLI コマンドを読み、最後にいくつかの参照例を使用して設定方法を学ぶことです。

例 1: 現在のバージョンを表示する

```
# ステータスシステム
hardware_version = 1.0
firmware_version = beta210618
firmware_version_full = "beta210618 (Rev 4250)"
kernel_version = 4.9.152
device_model = R2011
serial_number = ""
稼働時間= "0 日、01 時 25 分 16 秒"
system_time = "2021 年 4 月 15 日火曜日 17:09:04"
ram_usage = "77M Free/128M Total"
```

例 2:TFTP 経由でファームウェアを更新する

```
#tftpupdate (スペース+?)
  ファームウェア 新しいファームウェア
 config 新しい設定ファイル
#tftpupdate ファームウェア (スペース+?)
  filename 新しいファイル
# tftpupdate firmware filename R2011-firmware-sysupgrade-unknown.ruf host 192.168.100.99  //新しいファームウェア名を入力
ダウンロード
ダウンロードに成功しました。
アップグレード
アップグレードに成功しました。      更新成功
# reboot //再起動後に有効になります
再起動。。。
わかりました
```

例 3: link-manager を設定する

```
# 設定
# set (スペース+?)
 セルラー セルラー
 DDNS の DDNS の
 dido DIDO (ディドディド)
 email メールアドレス
 イーサネットイーサネット
 イベント イベント管理
```

firewall ファイアウォール
GRE の GRE
ip_passthrough IP パススルー
ipsec IPSec (ipsec IPSec)
LAN ローカルエリアネットワーク
link_manager リンク マネージャー
NTP の NTP
OpenVPN の OpenVPN の
reboot 自動再起動
ルートルート
serial_port シリアル
SMS の SMS
ssh の SSH
Syslog Syslog
システム
user_management ユーザー管理
web_server Web サーバー

set link_manager(space+?)
primary_link 1 次リンク
backup_link バックアップリンク
backup_mode BackSup モード
revert_interval Revert Interval (復帰インターバル)
emergency_reboot 緊急再起動
リンク リンク設定
set link_manager primary_link(space+?)
列挙プライマリ リンク (wwan1/wan)
set link_manager primary_link wwan1 //primary_link "wwan1" を選択
OK //設定成功
#set link_manager リンク 1(スペース+?)
種類 種類
desc 説明
connection_type 接続タイプ
WWAN WWAN 設定
static_addr 静的アドレス設定
pppoe PPPoE 設定
ping を実行します Ping 設定
nat_enable NAT 有効(NAT Enable)
MTU MTU (ミリ秒)
重量 重さ
upload_bandwidth アップロード帯域幅
download_bandwidth ダウンロード帯域幅
dns1_overrided オーバーライドされたプライマリ DNS
dns2_overrided オーバーライドされたセカンダリ DNS
debug_enable デバッグ有効(Debug Enable)
verbose_debug_enable 詳細デバッグの有効化
リンク 1 タイプ wwan1 link_manager 設定
わかりました
リンク 1 link_manager 設定 wwan(space+?)
auto_apn APN の自動選択

APN の　　APN の
ユーザー名　　ユーザー名
password パスワード
dialup_number　　ダイヤルアップ番号
auth_type　　認証の種類
data_allowance　　データ許容量
billing_day 請求日
リンク 1 wwan data_allowance 100 link_manager 設定 //セルラー switch_by_data_traffic を有効にする
OK //設定成功
set link_manager link 1 wwan billing_day 1 //課金の日付を指定する設定
OK　　// 設定成功
...
コンフィグ save_and_apply
OK // 現在の設定を保存して適用し、設定を有効にします

例 4: イーサネットの設定

set Ethernet port_setting 2 port_assignment lan0 //テーブル 2(eth1)を lan0 に設定
わかりました
config save_and_apply //設定成功
わかりました

例 5:LAN の IP アドレスを設定する

#すべて LAN を表示
ネットワーク{
  ID = 1
  インターフェイス = LAN0
  IP アドレス= 192.168.0.1
  ネットマスク = 255.255.255.0
  MTU = 1500
  dhcp の{
    有効 = true
    モード = サーバー
    relay_server = ""
    pool_start = 192.168.0.2
    pool_end = 192.168.0.100
    ネットマスク = 255.255.255.0
    デバイス = ""
    primary_dns = ""
    secondary_dns = ""
    wins_server = ""
    lease_time = 120
    static_lease = ""
    expert_options = ""
    debug_enable = false
  }
  vlan_id = 0
}
#

```
# set lan(space+?)
 ネットワーク          ネットワーク設定
 multi_ip        複数の IP アドレス設定
# LAN ネットワークを設定 1(space+?)
 インターフェイス     インターフェイス
 IP アドレス          IP アドレス
 ネットマスク         ネットマスク
 MTU の        MTU (英語)
 DHCP の       DHCP 設定
 Vlan_id VLAN ID
#LAN ネットワーク 1 インターフェイス lan0 を設定します
わかりました
# set lan network 1 ip 172.16.24.24  //LAN の IP アドレスを設定
OK //設定成功
#LAN ネットワーク 1 ネットマスク 255.255.0.0 を設定
わかりました
#
...
# コンフィグ save_and_apply
OK // 現在の設定を保存して適用し、設定を有効にします
```

例 6:セルラーを設定するための CLI

```
#セルラーをすべて表示
シム{
   ID = 1
   カード = SIM1
   phone_number = ""
   pin_code = ""
   extra_at_cmd = ""
   telnet_port = 0
   network_type = 自動
   band_select_type = すべて
   band_settings {
      gsm_850 = false
      gsm_900 = false
      gsm_1800 = false
      gsm_1900 = false
      wcdma_800 = false
      wcdma_850 = false
      wcdma_900 = false
      wcdma_1900 = false
      wcdma_2100 = false
      wcdma_1700 = false
      wcdma_band19 = false
      lte_band1 = false
      lte_band2 = false
      lte_band3 = false
      lte_band4 = false
      lte_band5 = false
      lte_band7 = false
      lte_band8 = false
      lte_band13 = false
```

```
      lte_band17 = false
      lte_band18 = false
      lte_band19 = false
      lte_band20 = false
      lte_band21 = false
      lte_band25 = false
      lte_band28 = false
      lte_band31 = false
      lte_band38 = false
      lte_band39 = false
      lte_band40 = false
      lte_band41 = false
    }
    telit_band_settings {
      gsm_band = 900_and_1800
      wcdma_band = 1900
    }
    debug_enable = true
    verbose_debug_enable = false
}
# set(スペース+スペース)
セルラーDDN、DIDO 電子メール、イーサネット
イベントファイアウォール GRE ip_passthrough IPsec
openVPN link_manager l2tp
PPTP リブート ルート          serial_port     SMS
SSH syslog システム user_management web_server
# set cellular(space+?)
  simSIM 設定
# セルラー sim(space+?) を設定
  整数インデックス (1..1)

# セルラーSIM 1 を設定(スペース+?)
  カード SIM カード
  phone_number 電話番号
  pin_code PIN コード
  extra_at_cmd 追加の AT コマンド
  telnet_port Telnet ポート
  network_type ネットワークの種類
  band_select_type バンド選択タイプ
  band_settings バンド設定
  telit_band_settings バンド設定
  debug_enable デバッグ有効(Debug Enable)
  verbose_debug_enable 詳細デバッグの有効化
# セルラーSIM 1 を phone_number 18620435279 設定
わかりました
...
# コンフィグ save_and_apply
OK // 現在の設定を保存して適用し、設定を有効にします
```

6.用語集

略称。	説明
AC	交流
APN	アクセスポイント名
ASCII	情報交換のための米国標準コード
CE	欧州適合
CHAP	チャレンジ ハンドシェイク認証プロトコル
CLI	バッチスクリプティング用のコマンドラインインターフェイス
CSD	回線交換データ
CTS	送信にクリア
dB	デシベル
dBi	等方性ラジエーターに対するデシベル
DC	直流
DCD	データキャリア検出
DCE	データ通信機器(通常はモデム)
DCS 1800	デジタルセルラーシステム(PCN)
DI	デジタル入力
DO	デジタル出力
DSR	データ・セット・レディ
DTE	データ端末機器
DTMF	デュアルトーン多周波
DTR	データ端末対応
EDGE	GSM と IS-136 のグローバル展開のためのデータレートの向上
EMC	電磁両立性
EMI	電磁干渉
ESD	静電気放電
ETSI	欧州電気通信標準化機構
EVDO	進化-データ最適化
FDD LTE	周波数分割複信の長期進化
GND	地面
GPRS	一般パケット無線サービス
GRE	汎用ルートのカプセル化
GSM	移動体通信のグローバルシステム
HSPA	高速パケットアクセス
ID	識別データ (identification data)
IMEI	国際移動体機器識別
IP	インターネットプロトコル
IPsec	インターネットプロトコル セキュリティ
kbps	キロビット/秒
L2TP	レイヤ 2 トンネリング プロトコル
LAN	ローカルエリアネットワーク
LED	発光ダイオード

略称。	説明
M2M	マシン・ツー・マシン
MAX	最大
Min	最低限
MO	モバイル発信
MS	モバイルステーション
MT	モバイル終了
OpenVPN	オープン・バーチャル・プライベート・ネットワーク
PAP	パスワード認証プロトコル
PC	パソコン
PCN	パーソナル・コミュニケーションズ・ネットワーク (DCS 1800 とも呼ばれる)
PCS	パーソナル・コミュニケーション・システム (GSM 1900 とも呼ばれる)
PDU	プロトコル・データ・ユニット
PIN	個人識別番号
PLCs	プログラムロジック制御システム
PPP	ポイント・ツー・ポイント・プロトコル
PPTP	ポイントツーポイントトンネリングプロトコル
PSU	電源ユニット
PUK	個人用ブロック解除キー
R&TTE	無線・通信端末機器
RF	無線周波数
RTC	リアルタイムクロック
RTS	送信要求
RTU	リモート端末ユニット
Rx	受信方向
SDK	ソフトウェア開発キット
SIM	加入者識別モジュール
SMA antenna	スタビーアンテナまたはマグネットアンテナ
SMS	ショートメッセージサービス
SNMP	簡易ネットワーク管理プロトコル
TCP/IP	伝送制御プロトコル/インターネットプロトコル
TE	ターミナル機器は DTE とも呼ばれます
Tx	送信方向
UART	ユニバーサル非同期受信/送信機
UMTS	ユニバーサル移動通信システム
USB	ユニバーサルシリアルバス
USSD	非構造化補足サービスデータ
VDC	ボルト 直流
VLAN	仮想ローカルエリアネットワーク
VPN 接続	仮想プライベートネットワーク
VSWR	電圧定常波比
WAN (英語)	広域ネットワーク