ecCLOUD コントローラ

ユーザマニュアル

www.edge-core.com

ユーザマニュアル

ecCLOUD コントローラ

クラウドベース　有線／無線ネットワークコントローラ

E072024-MR-R08(JP)

このマニュアルの使い方

本マニュアルの目的は、Edgecore ecCLOUD コントローラのクラウドやサイトの作り方などの情報と、AP や他のデバイスの使い方の手引きを提供することです。ネットワークデバイスをできるだけトラブルのない状態で効率よく使用するためには、このマニュアルを読むことでデバイスの性能を理解しておくことが大切です。

誰がこのマニュアルを必要とするか

このマニュアルはネットワーク機器を操作し、メンテナンスを行う管理者のために作られました。読者は基本的な LAN（ローカルエリアネットワーク）、IP（インターネットプロトコル）、SNMP（シンプルネットワーク管理プロトコル）の知識があることを仮定しています。

このマニュアルについて

このマニュアルは ecCLOUD コントローラウエブ管理インターフェースに基づいて書かれています。システムの紹介と構成の詳細も提供しています。

マニュアルは以下のセクションを設けています。

- セクションI"操作を開始する" — この章はecCLOUDコントローラの'使い方とシステムへのアクセスの方法について書かれています。
- セクションII"クラウドの設定" — ecCLOUD コントローラウエブサイトを使うことで得られる管理方法のオプションについて説明します。ecCLOUD コントローラとアクセスの方法について。

注意喚起

下記はマニュアル内で使われている注意喚起の方法です。

注意：デバイスについての特別な注意事項と扱いについて。

警報：データの紛失、システムやデバイスに損害が起こる可能性があります。

警告：負傷事故が起こる可能性があります。

修正履歴

このセクションはマニュアルが修正された履歴を説明します。

2024年7月改訂版

本ガイドは今回で8回目の改訂です。以下の変更点が含まれています:

- キャプティブポータルおよび SSID 構成の説明に Microsoft 365 認証を追加しました、81 ページの「SSID の設定」および 図 74 を参照してください。
- トポロジーの更新時間の可視性を追加しました、91 ページの「位置とマップ」および図 85 を参照してください。
- Microsoft 365 認証のサポートを追加しました、172 ページの「Microsoft 365 認証」および 図 158 を参照してください。
- WiFi 6 サイトのシステム設定を更新し、SNMP トラップサーバーを追加しました、204 ページの「SNMP」および図 186 を参照してください。

2024年3月改訂版

これは本ガイド7回目の改訂です。以下の変更が含まれています:

- レポート管理機能の追加、69 ページの「レポート管理」を参照ください。
- Aprecomm の Virtual Wireless Expert アドオンを追加、83 ページの「Aprecomm アドオンを使用する」を参照ください。
- LinqPath ツールを更新して、Distance Steps とそれに対応する予想 MCS とデータレートを追加しました。261 ページの「リンクパスツールの使用」および 264 ページの「MetroLinq パス予想 RSSI のグラフ」を参照してください。

2023年12月改訂版

これは本ガイドの6回目の改訂です。以下の変更が含まれています :

- 更新されたサポートモデルは、27 ページの「ecCLOUD にログインする」を参照ください。
- 図 20 を更新しました、40 ページの「デバイス設定の変更」を参照ください。
- クラウドマネジメントア 73 ページの「アドオン」を更新しました。

- ファイアウォール設定のターゲットオプションの変更、WiFi-5 136 ページの「ファイアーウォールの設定」および WiFi-6 188 ページの「ファイアーウォールの設定」を参照ください。
- SSID アイソレーションのサポートを追加しました 160 ページの「無線 SSID の設定」。
- ダイナミック PSK キーのサポートを追加しました 163 ページの「一般設定」。
- Mgmtd Log および SysLog Level 機能の追加については、199 ページの「システムの設定」を参照ください。
- WiFi-6 用の SNMPv3 ユーザーサポートを追加しました 209 ページの「SNMPv3 ユーザー」。
- サイト SD-WAN 設定の追加については221 ページの「サイト SD-WAN の構成」を参照ください。
- 6 GHz 帯域のサポートを追加しました、235 ページの「WiFi 6 デバイス構成」を参照ください。
- デバイス SD-WAN 設定を追加しました 293 ページの「SD-WAN デバイス構成」。

2023年8月改訂

本ガイドの 5 回目の改訂です。以下の変更が含まれています：

- OpenRoaming が追加 162 ページの「SSID を追加する」および 210 ページの「OpenRoaming」を参照。
- RF アイソレーションの追加（175 ページの「無線設定」を参照）
- ブロードキャスト・レートの変更（175 ページの「無線設定」を参照）
- サイト・グループ化の追加（61 ページの「サイトグルーピング」を参照）
- “ 常にクラウド設定に従う ” を追加 (65 ページの「常にクラウド設定に従う」を参照)

2023 年 3 月改訂
これは、このガイドの 4 番目の改訂版です。これには、次の変更が含まれます。

- Airtime Fairness を追加、176 ページの「グローバル設定」参照

- 802.11v を追加、162 ページの「SSID を追加する」を参照
- BLE Tx Power を追加、209 ページの「iBeacon」参照
- BLE スキャンの追加、245 ページの「iBeacon」参照
- 更新されたチャネル帯域幅は、176 ページの「電波設定」および 241 ページの「電波設定」を参照
- BSS Coloring の更新 176 ページの「電波設定」、241 ページの「電波設定」参照
- 更新された最小許容信号、114 ページの「SSID を追加する」、162 ページの「SSID を追加する」参照
- Terragraph デバイスの設定を追加しました（265 ページの「Terragraph デバイス構成」参照）。
- サイト Terragraph の VLAN 設定を追加、219 ページの「VLAN 設定」参照

2022 年 11 月改訂版
本書は、本ガイドの 3 回目の改訂版です。以下変更点が含まれています。

- 一括アップロード情報を追加しました。28 ページの「クラウドを作成する」、92 ページの「デバイスを追加する」をご参照ください。
- 更新されたクラウドメニュー、53 ページの「デバイスの管理」参照
- WiFi 5/WiFi 6 の設定を更新しました（95 ページの「WiFi 構成」を参照）
- 111 ページの「サイト WiFi 5 構成」の章を改名
- マルチキャスト / ブロードキャストレートの追加、114 ページの「SSID を追加する」参照
- OSEN の追加、114 ページの「SSID を追加する」参照
- AuthPort External RADIUS を追加、123 ページの「無線設定」を参照
- 無効な W52 チャネルを追加、123 ページの「無線設定」参照
- IPv6 設定を追加しました。127 ページの「インターネットの設定」を参照
- アップリンク 802.1P を追加、130 ページの「VLAN の設定」「VLAN 設定」（108 ページ）参照
- 追加 RSTP の有効化、134 ページの「ローカルネットワーク設定」参照

- DNS エントリーの追加、134 ページの「ローカルネットワーク設定」参照
- ARP インスペクションを追加、138 ページの「ARP インスペクション」参照
- DHCP Snooping を追加、139 ページの「DHCP スヌーピング」を参照。
- 外部 RADIUS を使用した AuthPort リモートスプラッシュページの追加、140 ページの「ホットスポットの設定」参照
- DNS エントリーと DNS マッピングを追加、140 ページの「ホットスポットの設定」参照
- 追加 NAS ID の生成、143 ページの「RADIUS サーバー」参照
- HTTPS ログインを追加、145 ページの「キャプティブポータル」参照
- クラウドと無線機の LED を変更、147 ページの「システムの設定」参照
- MSP モードの追加、147 ページの「システムの設定」参照
- SNMP IPv6 Write Community と SNMP Location を追加しました、153 ページの「SNMP」参照
- IGMP Snooping を追加、156 ページの「IGMP スヌーピング」参照
- LLDP を追加、157 ページの「LLDP」参照
- iBeacon を追加、157 ページの「iBeacon」参照
- SNMPv3 User を追加しました。158 ページの「SNMPv3 ユーザ」を参照
- 159 ページの「サイト WiFi 6 構成」の章を追加しました。
- 215 ページの「サイト Terragraph の構成」の章を追加しました。
- 225 ページの「WiFi 5 デバイス構成」の章を改称しました。
- 235 ページの「WiFi 6 デバイス構成」の章を追加しました。

2021 年 5 月改訂
これは、このガイドの 2 番目の改訂版です。これには、次の変更が含まれます。

- EAP101 および EAP102 のサポートが追加されました。
- 34 ページの「QR コードによる機器登録」のセクションを追加

2020 年 12 月改訂
これがマニュアルの初版の改訂です。

目次

図を使っての説明

セクション I

操作を開始する

このセクションは ecCLOUD コントローラのソフトウエアの全体的な詳細と、装置の操作を開始する際の手順について説明します。

このセクションは以下のチャプターを含みます。

1 イントロダクション

この章は以下の内容を含みます。

Edgecore ecCLOUD コントローラは、どんな場所からでもウエブブラウザを通して使用できる、クラウドベースのネットワークサービスです。

Edgecore コントローラソフトウエアは拡張が可能であり、管理できるネットワークサービスと装置の数は限りがありません。ネットワークを管理する機能 と、無線のコントローラであるという特徴を生かせば、ecCLOUD コントローラは、Edgecore AP とスイッチを自動的に接続させ、一つのネットワークとして管理できます。

ecCLOUD は下記の装置をサポートしています。

- Edgecore APシリーズ: EAP101, EAP102, EAP104, EAP104 Lite, ECW5211-L, ECW5410-L, ECWO5211-L, OAP100, OAP100e, OAP101, OAP101 6E, SP-W2-AC1200 (L), SP-W2M-AC1200, SP-W2M-AC1200-POE, SS-W2-AC2600
- Edgecore スイッチシリーズ : ECS2100-10P, ECS2100-10T, ECS2100-28P, ECS2100- 28PP, ECS2100-28T, ECS2100-52T, ECS4100-12PH, ECS4100-12T, ECS4100-28P, ECS4100-28T, ECS4100-52P, ECS4100-52T, ECS4120-28Fv2, ECS4120-28Fv2-I, ECS4120-28T, ECS4120-52T, ECS4125-10P, ECS4150-28P
- MLTG シリーズ : MLTG-360, MLTG-CN, MLTG-CN LR
- SD-WAN シリーズ : SDW102

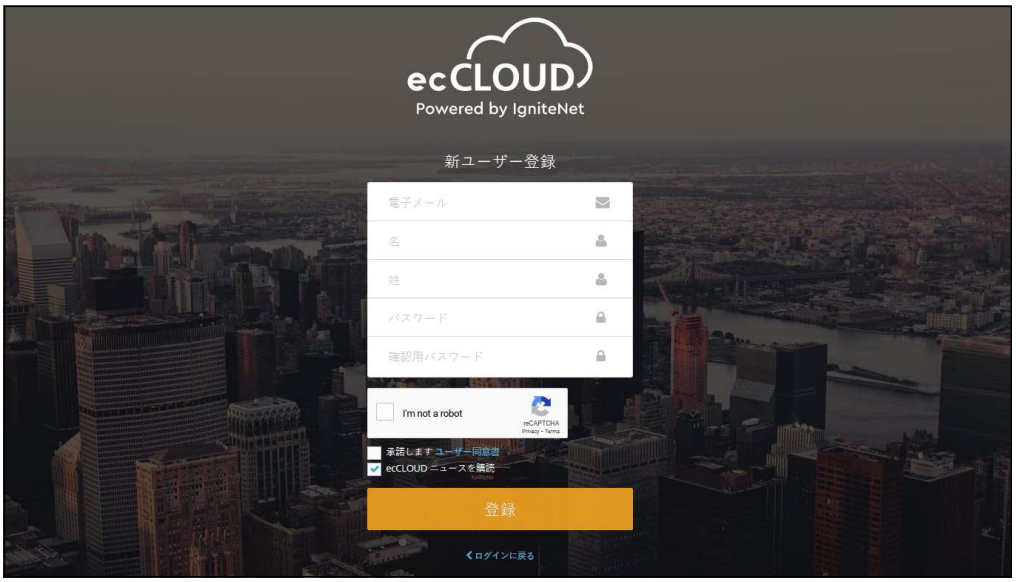
ecCLOUD にログインする

ウエブのブラウザから、cloud.ignitenet.com に入ってアカウントの登録をしてください。あなたのクラウドのネットワークとサイトを作成しましょう。

図 1: ecCLOUD コントローラにログインする

“ 登録する ” をクリックして、アカウントを作成してください。

図 2: 新しいユーザの登録



メールアドレス、氏名を入力します。セキュリティのためパスワードを設定し “ 私はロボットではありません “ をクリックしてください。最後に登録をクリックすれば完了です。

注意：ユーザプロフィールを作成するためには正確なメールアドレスが必要です。

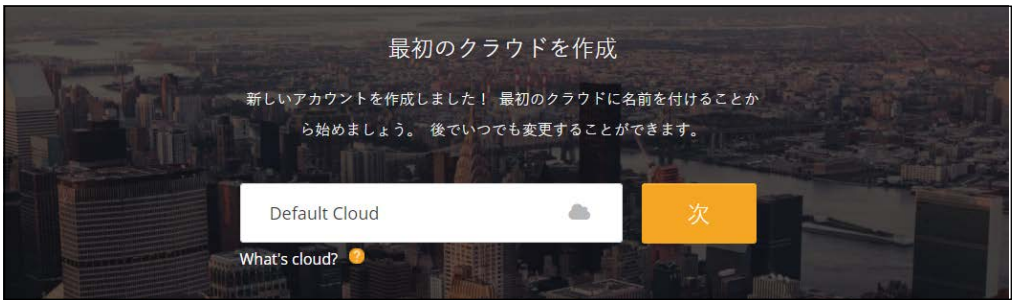
確認メールが ecCLOUD コントローラから届いたら、指示されたリンクにアクセスし登録してください。

クラウドを作成する

ecCLOUD コントローラはクラウドに似ております。あなたが管理する装置をロジカルグループとしてサイトで管理します。それぞれのクラウドにはユーザグループが存在します。エンドユーザとして、あなたはそれぞれ異なるルールを持つクラウドを、いくつでも使用できます。

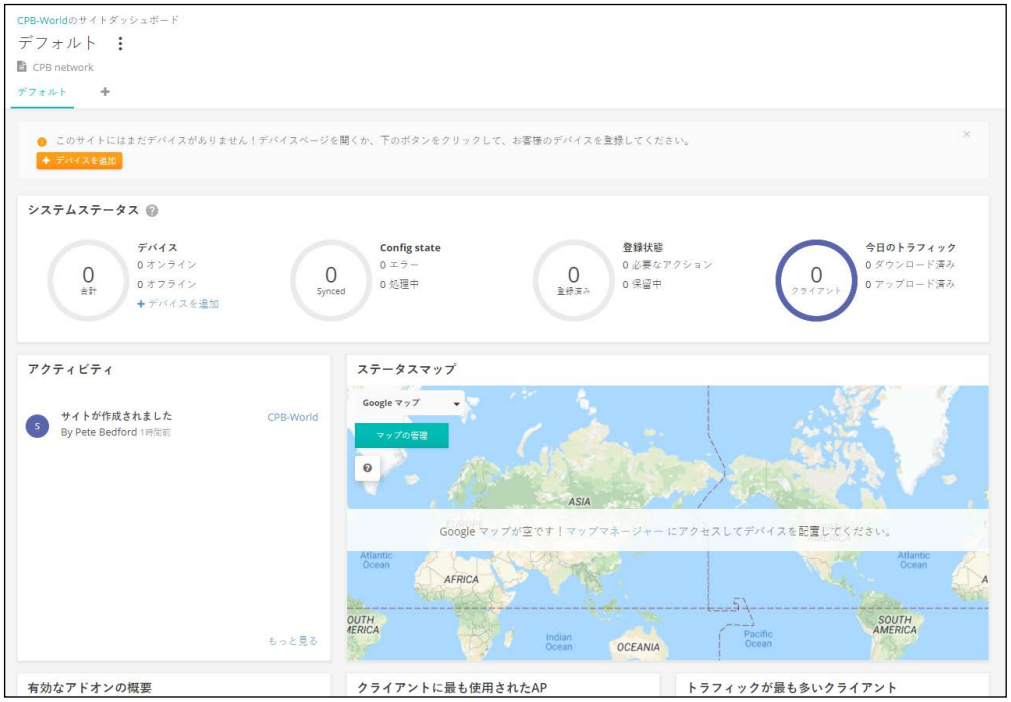
ecCLOUD コントローラのユーザとして登録すれば、最初にログインした時から自分のクラウドを作成できます。

図 3: クラウドを作成する



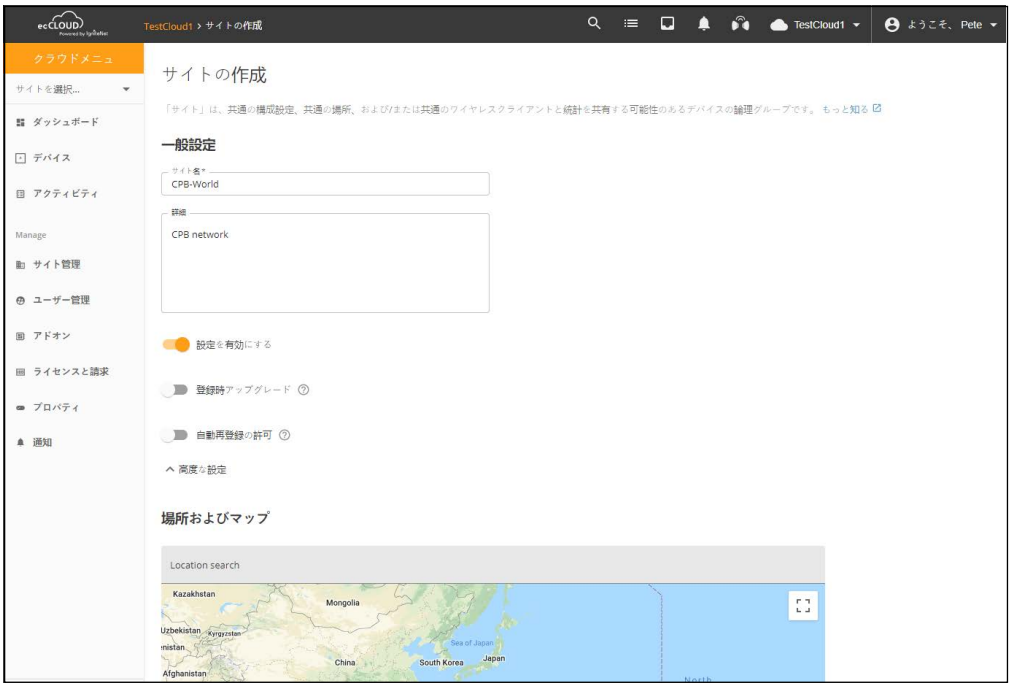
クラウドに名前を入力して、“ 作成 “ をクリックしてください。クラウドのダッシュボードが表示されます。

図 4: クラウドを作成する



“ サイトを追加する “ をクリックしてサイトに情報を加えてください。

図 5: サイトの設定



サイトのデバイスについての下記のプロパティを加えてください。

- 設定の有効化：この設定には以下のオプションがあります。
  - オン：デバイスの設定を遠隔操作できます。（デフォルトはこの状態です）。
  - オフ：デバイスの設定は遠隔操作できず、直に行う必要があります。モニターは隔離状態で行うことができ、デバイスがオフラインになった場合には注意喚起の通知が届きます。
- 登録時アップグレード：この設定にすると、デバイスのアップグレードが自動的に行われ、最新のフファームウエアの状態で使用し続けることができます。この設定にしておくことをお勧めします。
- 自動再登録の許可：この設定にしておくと、デバイスがデフォルトの状態になった場合でも自動的に再登録できます。この設定が無効になった場合はデバイスが再登録を試み、ユーザ自身がクラウドにログインし、手動で手続きをしてください。

サイトの情報が設定できたら、“ 作成 “ をクリックしサイトを作成してください。

国とローカルログインの設定が完了したら、“ 保存 “ をクリックしてください。

図 6: サイトの設定を保存する

サイトの設定を保存すると、新しいデバイス（無線、スイッチ、メッシュリングス：MeshLinqs、ジーリングス：GLinqs）を新しいサイトに追加するよう誘導されます。“ デバイスを追加 “ をクリックし手順に従ってください。

図 7: 装置を加える方法

メインメニューの “ 無線デバイス “ または “ スイッチ “ をクリックしてデバイスの管理ページにアクセスしてください。

Edgecore AP またはスイッチをクラウドに加える準備ができました。

図 8: 装置の管理

“ デバイスを追加 “ をクリックし “ 新しいデバイスを追加 “ ページにアクセスしてください。

シリアル番号、MAC アドレス、名前を記入し、保存をクリックします。また、端末の QR コード（34 ページの「QR コードによる機器登録」参照）、またはバーコードスキャナーを使用することもできます。また端末の情報を一括してファイルにアップロードすることもできます。

バーコードスキャンモードを有効化」を ON にすると、バーコードを素早く読み取り、機器のシリアル番号や MAC アドレスを入力できます。入力したら、バーコードスキャンモードをオフにして、デバイスの名前を手動で入力します。新しいデバイスを追加する準備ができたら、保存ボタンをクリックしてください。

“ 常にクラウド設定に従う ” 機能をオンにすると、デバイスから受信したローカルの構成変更を無視します。詳細については、65 ページの「常にクラウド設定に従う」を参照してください。

一括アップロードの場合は、端末のリストを CSV（カンマ区切り）ファイルで用意してください。CSV ファイルとは、情報をカンマで区切ったプレーンテキストファイルです。各機器について、以下のフォーマットのように、シリアル番号、MAC アドレス、名称を 1 行で入力してください。

```
<Serial Number 1>,<MAC 1>,<Device Name 1>
<Serial Number 2>,<MAC 2>,<Device Name 2>
```

アップロードボタンをクリックして、CSV ファイルをアップロードします。

38 ページの「デバイスの登録」をご覧ください。

図 9: デバイスの追加

すべての“新しいデバイスを加える“ページの上の部分に、新しく追加されたデバイスについての通知が表示されます。メッセージ内の“マップの管理“のブルーリンクをクリックして、デバイスをマップに加えてください。(34 ページの「装置をマップにのせる」を参照してください)。

図 10: デバイスが追加された場合の通知メッセージ

一つ目のデバイスがサイトに追加されると、“ファームウエアをアップグレードする“ボタンがデバイスのリストの上に表示されます。105 ページの「メンテナンスタスクのスケジュールを立てる」をお読みください。

図 11: ファームウエアのアップグレードボタン

デバイス管理ページの左側にロート型をしたカテゴリーボタンがあります。カテゴリーボタンをクリックするとそれぞれのデバイスのプロパティについてフィルター処理できます。ステータス、健康状態、登録、ブロック、無効、設定ステータス、コンフィギュ レーションの引継ぎポリシーなどの選択肢から必要なプロパティを選択してください。

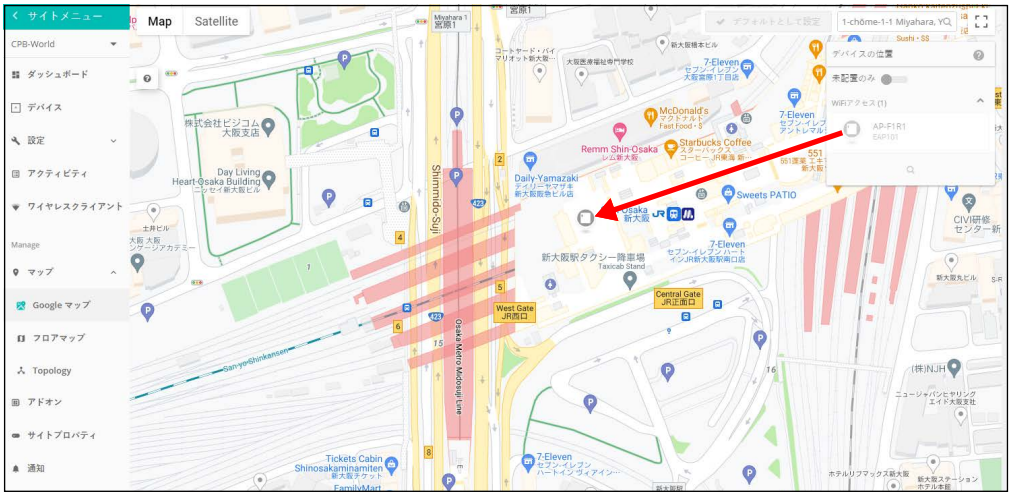
フィルターをリセットするには“解除“ボタンをクリックしてください。

図 12: 装置のフィルター処理

装置をマップにのせる

デバイスの追加完了の通知メッセージ内の、マップ管理リンクをクリックしてください。マップビューページが表示されます。マウスを使って追加されたデバイスを設置場所まで移動させてください。

図 13: 装置をマップにのせる



QR コードによる機器登録

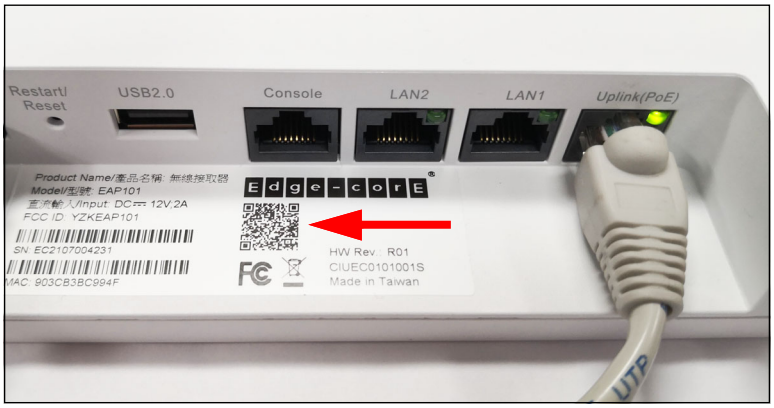
ecCLOUD コントローラで AP の設定や登録を迅速に行うために、携帯電話を使って、AP 上の QR コードをスキャンできます。

以下の手順に従ってください :

1. AP の電源を ON します。
2. AP をインターネットに接続します。ネットワークかインターネットアクセス機器を、AP の RJ-45 アップリンクポートへつないでください。

3. AP の QR コードをスキャンするには、iPhone の場合はカメラを、Android の場合はバーコードアプリを使用します。QR コードは、AP のラベルに印刷してあります。

図 14: AP の QR コードのスキャン



4. メッセージがポップアップしたら、Wi-Fi ネットワークに参加するために、" はい " をタップしてください。(iPhone の場合、ポップアップさせるために、設定 > Wi-Fi を開く必要があります。)

   ウェブブラウザが開き、セットアップウィザードのページにリダイレクトされます。

注意：もし携帯電話が Wi-Fi ネットワークに接続できない場合、SSID (ネットワーク名) とパスワードを手入力で打ち込んでください。SSID 名は AP のシリアル番号 (例えば、EC0123456789)、パスワードは AP の MAC アドレス (例えば、903CB3BC1234) です。

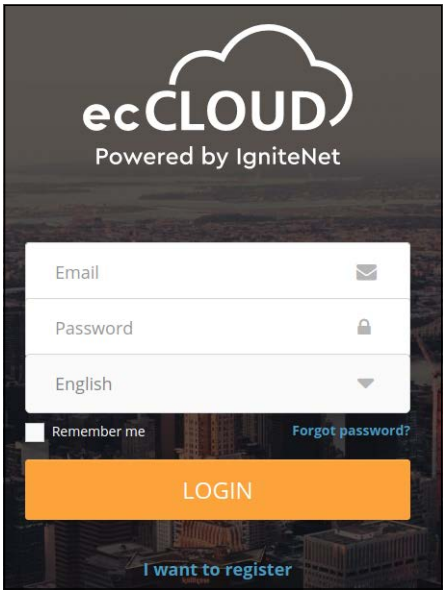
5. ec クラウドコントローラを使って AP を管理するのか、スタンドアロンモードで AP を管理するのかを選択してください。

   a. スタンドアロンモード: デフォルトの無線ネットワーク設定で使うか、ネットワーク名とパスワードをカスタマイズしてください。セットアップウィザードを終わるには、" 完了 " をクリックしてください。

      AP が設定を更新するまで 2 分ほど待つと、セットアップウィザードで設定したネットワーク名でつながります。ブラウザは AP へのログインページにリダイレクトされます。

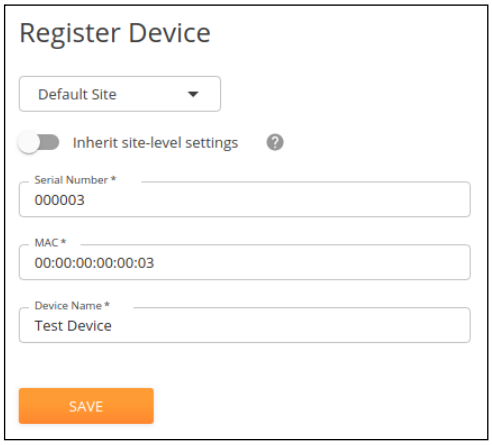
   b. クラウド管理モード : セットアップウィザードを終わるために " 完了 " をクリックすると、ブラウザは ecCLOUD へのログインページにリダイレクトされます。

図 15: ecCLOUD のログインページ



既に ecCLOUD のアカウントを持っている場合、ログインして AP のサイトを選択してください。クラウド管理するために、AP は自動的に登録されます。“ 保存 ” をタップした後、クラウドコントローラが AP の設定を更新するまで 2 分ほど待ちます。

図 16: ecCLOUD のデバイス登録



ecCLOUD のアカウントを持っていない場合、“I want to register” をタップし、アカウントをセットアップしてください。クラウドとサイトを作成したら、規制国名を確認します。その後、“ 次に ” をタップすると、クラウド管理するために、AP は自動的に登録されます。

“ 保存 ” をタップした後、クラウドコントローラが AP の設定を更新するまで 2 分ほど待ちます。

設定の引継ぎを理解する

新しいデバイスをクラウドに追加する場合、“ サイト内でのコンフィギュレーションの引継ぎ “ 機能を選択する必要があります。クラウド内でのデバイスの設定は、この “ 引継ぎポリシー “ に基づいて行われます。クラウドの設定は柔軟です。デバイスの設定を必要に応じて書き換え、必要なサイト内の設定のみを引き継ぐことができます。

サイト内で引き継がれる設定は、初めにデバイスを登録した際に設定されます。後で設定を変更することも可能です。

二種類の引継ぎポリシーがあります。

- サイトレベルの設定を継承する — 単一ユニットのデバイスに基本の設定をしている場合はこの引継ぎのポリシーをお勧めします。WiFi にアクセスするデバイスを設定する際に向いています。ホテルやビジネスなどで、会社が WiFi を配置している状況でよく使われるポリシーです。

  追加されるデバイスは、サイトからほとんどの設定を引継ぎますが、デバイスの用途を考慮し、デバイス設定ページからサイト内の設定を変えることが可能です。

- サイト内の設定を引き継がない — サイト内の設定を新しく加えるデバイスに引き継がせたくない場合は、このポリシーを選択してください。

  新しく加えられるデバイスがインフラストラクチャー、バックホールなど、サイト内の他のデバイスから独立した設定をする必要がある場合は、このポリシーを選択してください。Metrolinq ポイント トゥーポイントリンクスなどはこのポリシーの使用例です。

サイト内でデバイスの設定について引継ぎをする際に、考慮する必要がある設定の種類は以下の通りです。

- サイトのデバイスに対する設定。

- 基本的にサイト内のデバイスに対する設定ですが、特定のデバイスに関しては内容が書き換えられた設定。

- 特定のデバイスに対してのみ設けられた設定。サイト内のその他のデバイスに対しては使用されない設定。

注意：特定のデバイスに対して書き換えられていた設定を修正したい場合、そのデバイスに関するページ内の “ サイトの設定 “ ボタンをクリックしてください。

SSID、ローカルログイン、VLAN など、特定の種類のデバイスの設定を書き換えた場合、書き換えをしていないその他の設定までも書き換えられてしまうのでご注意ください。例えば、SSID に関してのサイト内での設定を一部書き変えた場合、変えていないその他の設定も書き換えられてしまいま す。一度設定が書き換えられてしまうと、その後加えられた SSID に関するサイト内の新しい設定も、デバイスの設定には反映されません。

デバイスの登録

新しいデバイスは、クラウドの “ デバイスを加える “ 欄にシリアル番号と MAC アドレスを入力またはスキャンすることで簡単にサイトに加えることができます。

図 17: 新しいデバイスの登録

注意：デバイスのシリアル番号と MAC アドレスはデバイスの箱、またはメインダッシュボードページのローカルウエブ UI で見つけることができます。

デバイスの登録を行う際に、以下のプロセスが必要になりがちです。

1. 装置がサイトに登録されると、“ 登録が保留されています “ というサイトが表示されるかもしれません。クラウドが、新しく登録されたデバイスの承認を着呼している状態です。以後、クラウドとデバイスとの接続を問題なく行うための準備です。

2. デバイスがクラウドと接続し、登録を完了すると、クラウドは 登録したデバイスのサイトが " 自動的にファームウエアをアップグレードする " ことができるかを確認します。もしこれが可能なデバイスであるならば、クラウドは自動的にアップグレードを行うためのタスクを作成します。

3. デバイスがアップグレードされた後、(またはアップグレードの過程がスキップされた後)、デバイスはクラウドに対し現在の設定についての情報を送信します。このクラウドが " コンフィギュレーションを受け取る " 間は、デバイスのアクティビティのページで閲覧できます。クラウドはデバイスだけでなく、ファームウェアの設定も収集する必要があります。デバイスの元々の設定を収集した後で、サイト内での新しい設定をデバイスに引継ぎます。

4. クラウドはサイト内の設定と、登録されたデバイスの元々の設定を混ぜ合わせ、" 設定の変更 " タスクとしてデバイスに引継ぎをします。(クラウドは、登録された設定に引継ぎができるものとしてプロセスします)。サイト内の設定の引継ぎが成功した場合、クラウド内に最初に表示されていたデバイスの設定が、交換された設定と置き換えられます。登録前にローカル UI によって変えられていた設定は、クラウドが新しい設定をデバイスに引き継ぐ際に取り消されます。

基本的な設定が完了するとデバイスの登録作業は終了しており、通常の操作が可能になります。デバイスの " アクティビティ " ページではデバイスの登録と設定プロセスの進み具合を把握できます。

デバイスを登録するには四段階のプロセスがあります。

- 登録されていない状態：デバイスの登録ができていないので、クラウドデーターベースに記録がありません。

- 登録保留中：クラウドのユーザがデバイスのシリアル番号と MAC アドレスをサイトに加えました。クラウドはデバイスとの接続を着呼しています。この時点では、デバイスはまだクラウドへの登録を開始していません。もしこの状態が長く続く場合、デバイスのインターネット接続かアップストリームファイアーウォールの設定を確認してください。

- 登録終了：デバイスが登録プロセスを完了し、クラウドに登録されました。クラウドはデバイスからの認証を得たので、今後の接続が可能になりました。" 登録された " 状態が、クラウド内でのデバイスの通常の状態です。

- 再登録：以前は登録されていたデバイスを、もう一度登録する状態です。システムが通知を出し、ユーザのクラウドアカウントへのログインが必要になります。ログインした後、デバイスの再登録をするか、デバイスのクラウド内での設定についてなど、必要なアクションを選択します。

注意：サイトプロパティのページで、“ 自動 “ 再登録設定を選択できます。この設定をすると、再登録アラートを解決するための手動の操作が不要になります。

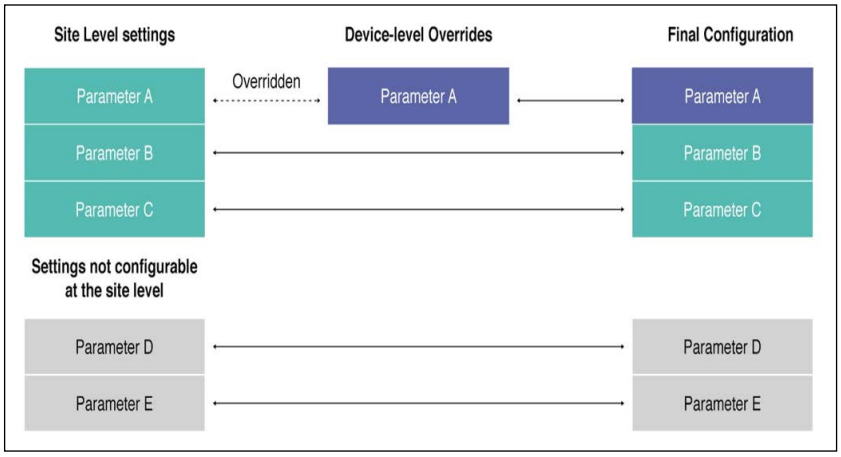
デバイス設定の変更

デバイスレベルの設定またはサイトレベルの設定が変更されるたび、クラウドは設定を変更したデバイスと変更内容を把握する必要があります。把握した後で該当するデバイスへ変更を引継ぎます。

該当するデバイスが “ サイトレベルの設定の引継ぎ “ に対応している場合、最終的な設定はデバイス自体の設定とクラウドの設定を合わせたものになります。

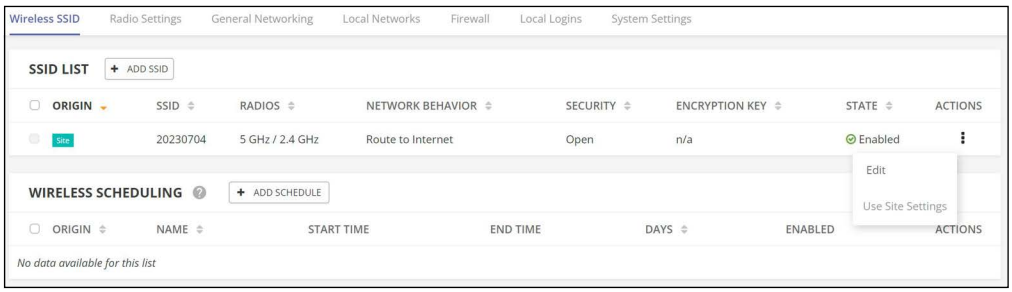
- 登録したデバイスの種類に関係する基本的なサイトレベルの設定。
- 登録したデバイスの独自の設定で、サイト内の他のデバイスには設定にできないもの。例えば無線設定など、そのデバイスにのみ関係する設定です。デバイスに対する設定はサイト内で書き換えられます。

図 18: デバイスの設定を書き換える



デバイスレベルの設定の書き換えは、サイトの設定に組み込まれ済みのデバイスレベルの設定を変えることで可能になります。この種の設定の書き換えは、設定の隣にある紫の矢印ボタンまたは“サイトの設定”ボタンをクリックし、いつでも変更できます。

図 19: 装置の設定の書き換えを元に戻す



デバイスの設定を変えた場合、下記の状態になります。

1. “設定を変える”タスクが作られて、デバイスのどの設定が変化したのかが表示されます。このタスクは該当するデバイスのアクティビティページで閲覧できます。

2. クラウドは新しい設定をデバイスに引継ぎ、引継ぎの成功を知らせる設定 ACK をデバイスから受け取ります。

3. ACK を受け取ると、タスクの完了が記録されます。デバイスがうまく接続せず、新しい設定が引き継がれなかった場合、デバイスの設定は元の状態に戻り、クラウドに“失敗”を知らせる通知が送られます。これは“同期化の失敗”のエラーです。

設定のエラー

設定のプロセスで起こりがちなエラーは二種類あります。

- 設定の同期化に失敗した場合：このエラーは設定を変えた際にデバイスがクラウドと接続できず、デバイスの設定が元の状態に戻る場合に起こります。デバイスの現在のコンフィギュレーションがクラウドの設定と異なる状態です。

- 対応策：このエラーの対応策は、デバイスのクラウド設定の設定ミスを見つけ出して修正することです。その後“再び同期化する”ボタンをクリックしてください。例えば、デバイスがクラウドの設定ページでは AP モードで操作しているはずが、エラーによりクライアントモードで操作しているとします。クラウドの設定が変えられた後、デバイスはインターネットやクラウドにアクセスできなくなります。デバイスのクラウドのコンフィギュレーションがクライアントから AP に変更される必要があります。

設定が保留されるエラー

デバイスの設定が保留されている間は、クラウドからデバイスへの設定の引継ぎはできません。デバイスがプロセスした設定はクラウドから引き継がれたものではありません。

デバイスの設定が保留される原因は以下の二つです。

- デバイスがダウングレードされている：2019 年 2 月 1 日現在、クラウドに登録したデバイスが、デフォルト状態にリセットをしたわけではないのにダウングレードされていた場合、デバイスに対するクラウドのコンフィギュレーションの引継ぎは保留になります。この状態になる理由は、デバイスの設定がクラウドがサポートしていないキーや数値を含んでいること、またはクラウドとファームウェアの古いバージョンが相容れないことが考えられます。この状態はシステムのエラーやデバイスの想定外の動きを引き起こす可能性があります。

  対処方法：デバイスをデフォルト状態に戻し、再登録してクラウドに接続し直します。

- システムのエラー：滅多にありませんが、クラウドがデバイスのコンフィギュレーションに関するキーを読み込めず、システムがエラー状態になることがあります。

  対処方法：ほとんどの場合、デバイスをデフォルト状態に戻すことで解決します。再登録の際に " デバイスの現在の設定 " を選択してください。

注意：上で詳細された対処法を取ることで、" 対処できない " クラウドレベルの設定キーを取り除く事はできますが、デバイスの設定の書き換えられた部分も取り除かれます。

これらの対処法で解決できない場合は、サポート、開発チームがエラーの原因を調査します。エラーの対処が出来次第、クラウドに登録したアカウント所有者にメールで連絡し、問題が解決したことを知らせます。

セクション II

クラウドの設定

このセクションではクラウドの作成と管理方法と、アクセスポイントの設定方法を説明します。

このセクションは下記の内容について説明します。

2 クラウドの管理

このチャプターは下のチャプターを含みます

クラウドの管理

画面の右上にあるクラウドのプルダウンメニューから “ クラウドの管理 “ を選択し、クラウドの管理ページを探します。

図 20: クラウドのメニュー

登録済みのアカウントで新しいクラウドの作成

登録済みのアカウントから新しいクラウドを作成する場合は以下の手順を行ってください。

1. クラウドにログインすると画面の右上に表示される “ クラウドを管理する “ を選択して、クラウドのメンバーシップページを開いてください。
2. “ クラウドを加える “ をクリックしてください。

図 21: クラウドのメンバーシップを表示する

3. クラウド名とその他の情報を入力してください。
4. 保存をクリックしてください。

図 22: クラウドの情報を入力する

クラウドの情報を編集する

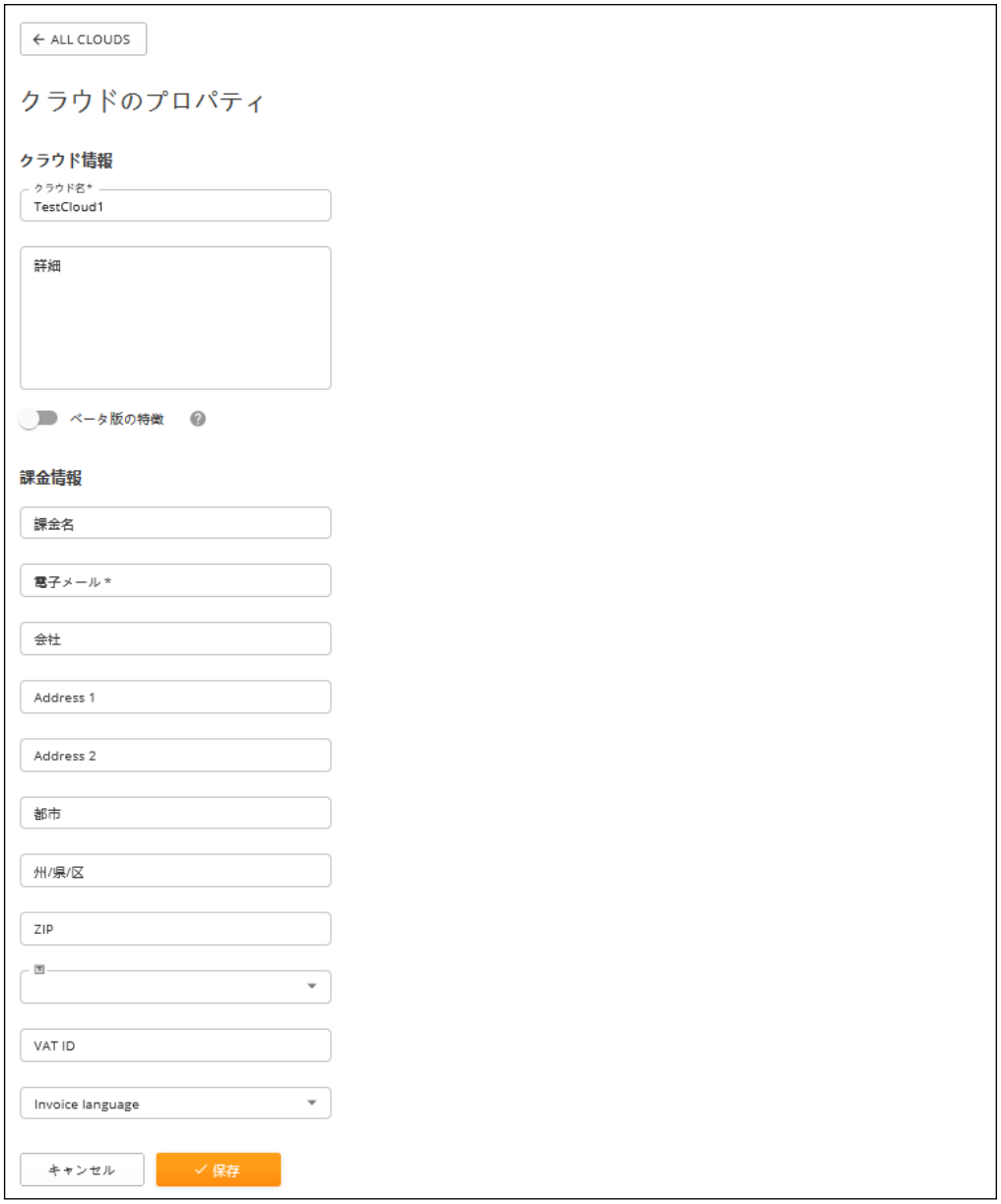
展開アイコンをクリックして削除と編集ボタンを表示してください。

図 23: クラウドアクションを表示

クラウドのプロパティの変更

展開アイコンをクリックしてクラウドの管理リストを表示し、リストの右下の編集ボタンをクリックしてください。クラウド情報のプロパティが表示されます。クラウドプロパティを編集し、保存ボタンをクリックしてください。

図 24: クラウドプロパティの変更



クラウドの削除

クラウドの管理リストを展開させて、リストの右下の削除ボタンをクリックしてください。クラウドが削除されます。確認ウィンドウが表示されますので、OK を押し削除してください。

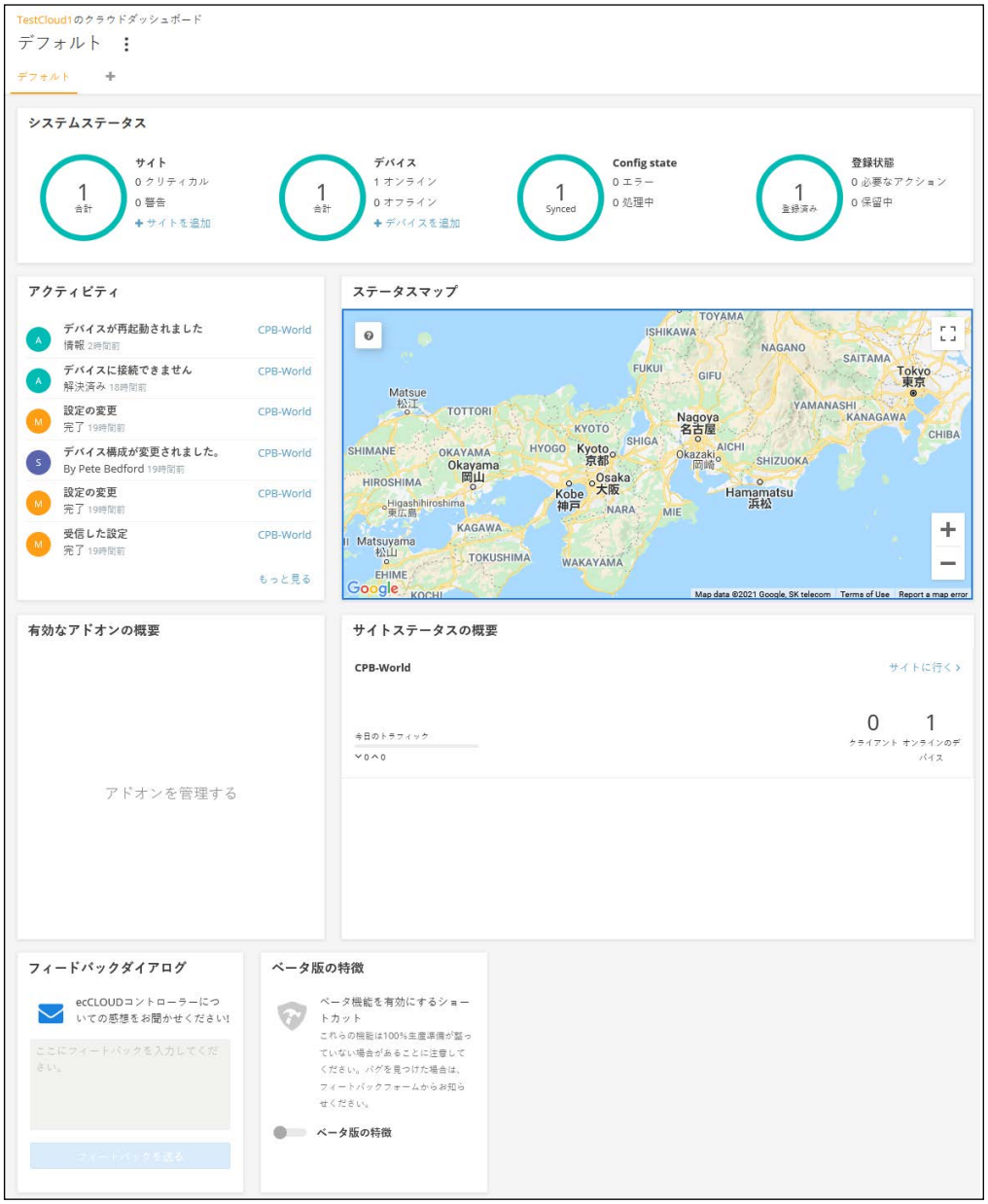
図 25: クラウド削除の確認

注意：一度クラウドを削除すると元に戻せません。AP、クライアント、サイト、システムアクティビティログ、クラウド内でのデバイスの設定など、関連する全ての記録が失われます。

クラウドダッシュボードの表示

クラウドのダッシュボードを使用すると、設定されたデバイスのシステムステータスの全体像を知ることができます。デバイスの最近のアクティビティ、クラウドのステータスマップ、サイトの全体的なステータスなどの情報を提供します。

図 26: クラウドのダッシュボード



以下のアイテムがクラウドダッシュボードに表示されます。

- システムステータス — 上段の 4 つの円は、左からサイトの数、装置の数（オフラインとオンラインに分けて表示されます）、同期化されたコン

フィギュレーションのデバイスの数、登録されたデバイスの数を表しています。

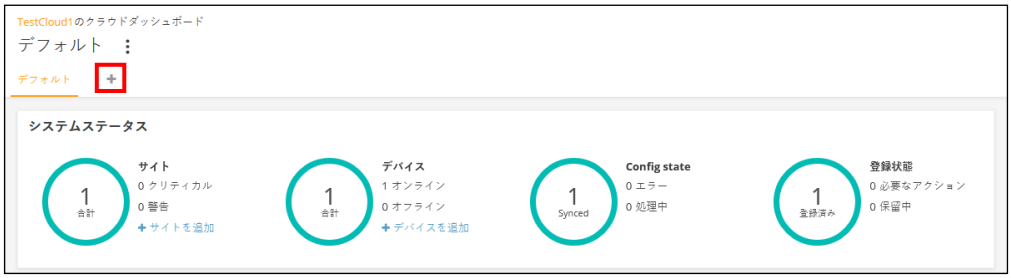
注意：カーソルを 4 つの円に合わせると、より多くの情報を得ることができます。

- アクティビティ — 最近の出来事を報告します。内容は、デバイス、ネットワーク、システムの警報、ネットワークが繋がらなかったり、再起動したことについての通知などです。情報をクリックすると、詳細の情報を得られます。
- クラウドマップ — クラウドのサイトと、サイト内でのデバイスの位置の地理的な情報を表示します。クラウドマップを使用してデバイスの周りを調べると、デバイスのさらなる情報を得ることができます。
- 可能なアドオンのお知らせ — 現在使用可能なアドオンについて報告します。ボックスをクリックするとアドオンの管理ビューが表示されます。
- サイトステータスの概要 — 当日のトラフィック、クライアントの人数、オンライン装置の数などのサイトについての統計を報告します。
- フィードバックダイアログ —Edgecore に自分のコメントや意見を送信できます。
- ベータ版の機能 — ベータ版の新しいクラウドコントローラの機能を使用できます。

カスタマイズされたクラウドのダッシュボードの作成

デフォルト状態のクラウドのダッシュボードの、デフォルトの隣にある＋マークをクリックして、より自分の必要性に適したダッシュボードを作成できます。

図 27: クラウドのダッシュボードのカスタマイズ



新しくカスタマイズされたダッシュボードに名前をつけて送信をクリックしてください。

図 28: カスタマイズされたクラウドのダッシュボードに名前をつける

デフォルトダッシュボードのタブが、カスタマイズされたダッシュボードの名前で表示されます。“ ウィジェットを追加する “ ボタンをクリックして新しいダッシュボードに必要なウィジェットを加えてください。

図 29: カスタマイズされたダッシュボードにウイジェットを加える

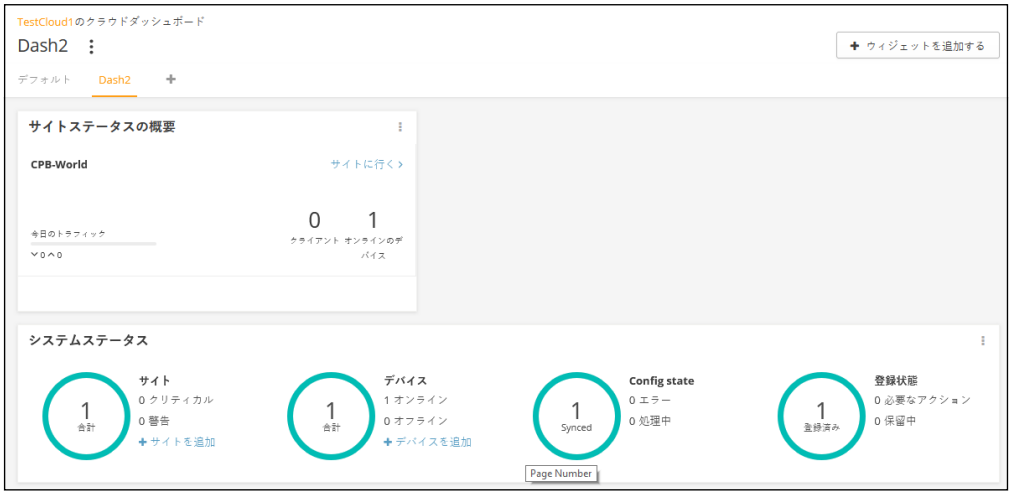
ウイジェットを選択したら、“ 追加 “ ボタンをクリックしてください。

図 30: カスタマイズされたダッシュボードにウイジェットを選択する

上の手順を踏んだ後はカスタマイズされたダッシュボードにはウイジェットが表示されるようになります。ウイジェットの大きさはウイジェットボックスの角をドラッグすることで調節できます。また、ボックスの右上にある 3 つの点をクリックすることで、ウイジェットの名前を変更したり、ウイジェットを削除できます。

“ ウイジェットを追加する “ ボタンをクリックするとさらに多くのウイジェットを加えることができます。

図 31: カスタマイズされたウイジェットをカスタマイズされたクラウドダッシュボードに追加する



デバイスの管理

クラウドメニューの「デバイス」セクションをクリックすると、全サイトのクラウドデバイスが表示されます。

図 32: クラウドメニュー内のデバイス

デバイスのリストをフィルターにかける

ウィンドウの左上にあるロート型をしたカテゴリーボタンをクリックすると、デバイスリストのフィルタリングオプション（Status、Health、State、Blocked、Disabled、Configuration Status、Configuration Inheritance Policy、Product Type）が開きます。表示されたデバイスは、各列の上部にある昇順または降順の矢印をクリックすることでソートすることもできます。

図 33: デバイスの管理

設定を引き継ぐ際のポリシー

一つ目のデバイスの登録時、サイトの設定の引継ぎポリシーがルールます。しかしこのポリシーはその後の状況によって変えることができます。詳細については、37 ページの「設定の引継ぎを理解する」をお読みください。

クラウドのデバイスリストにはギアアイコンをクリックすると表示される欄があります。この欄には、設定の引継ぎが可能なデバイスについて詳細されています。設定の引継ぎポリシーはフィルターを使用できます。また、デバイスに対してのポリシーは“ アクション “ リストを使って変えることができます。

図 34: 設定の引継ぎについての表示

最初の欄の中のチェックマークをクリックしてデバイスを選択してください。欄のヘッダーに“アクション”ボタンが表示されます。アクションボタンをクリックして、選択したデバイスに使用できるアクションを選択してください。

図 35: デバイスのアクションメニューの管理

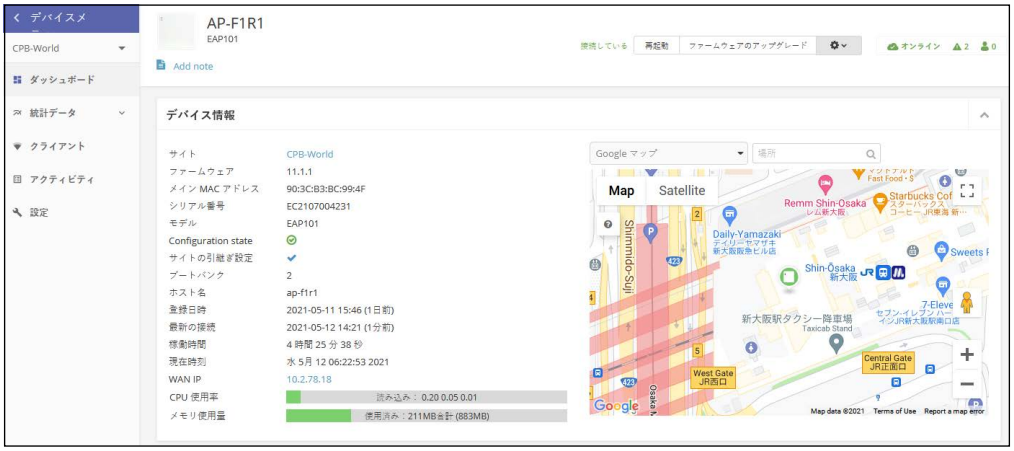
アクションメニューには以下のアイテムが表示されます。

- 引継ぎのポリシーを変える — 選択されたデバイスは、コンフィギュレーションの引継ぎポリシーを、現在の設定に基づいて、“サイトレベルの設定を引き継がない”または“サイトレベルの設定を引き継ぐ”に変更されます。
- サイトに移動する — 選択されたデバイスは他のサイトに移動します。移動したデバイスは、移動先の設定を引き継ぐことになります。
- ブロック — 選択されたデバイスは、クラウドのコミュニケーションからブロックされます。
- 無効 — デバイスをクラウドの全てのコミュニケーションからブロックし、全てのダッシュボードから探せない状態にします。デバイスの記録は残ります。
- 削除 — クラウドから永遠に取り除かれます。

デバイスについての情報を見る

名前の欄からデバイスの名前のリンクをクリックすると、詳しい情報にアクセスできます。

図 36: デバイスの詳細にアクセスする



デバイスの追加

デバイスを追加するボタンをクリックして、“ 新しいデバイスを登録する “ ページを開き、デバイスをクラウドに加えてください。

図 37: クラウドにデバイスを追加する

デバイスのファームウエアをアップグレードする

デバイスに新しいファームウェアを追加したいときは、FW 欄のアップグレードアイコンをクリックしてください。自動化したファームウェアのアップグレードページが表示されます。

図 38: ファームウェアアップグレードのお知らせ

ファームウエアの種類を選択した後、アップグレードする日時を決めてください。その後、作成ボタンをクリックしてアップグレードを確認してください。

図 39: 装置のファームウエアのアップグレード

システムのアクティビティを表示する

クラウドメニューのアクティビティをクリックすると、全ての記録されたシステムのアラート、メンテナンスタスク、記録されたイベントが表示されます。左側のカテゴリーボタンをクリックして、データの日付や時間帯を選んでください。表示されるメッセージはデータ欄の上にある上むきまたは下向きの矢印をクリックするとさらに分類できます。

図 40: 全てのシステムのアクティビティを表示する

ページの上の部分にあるカテゴリーボタンを使用して、可能なカテゴリー（アラート、メンテナンス、システムの記録）でデータをフィルターにかけてください。

図 41: アクティビティの種類でフィルターにかける

サイトの管理

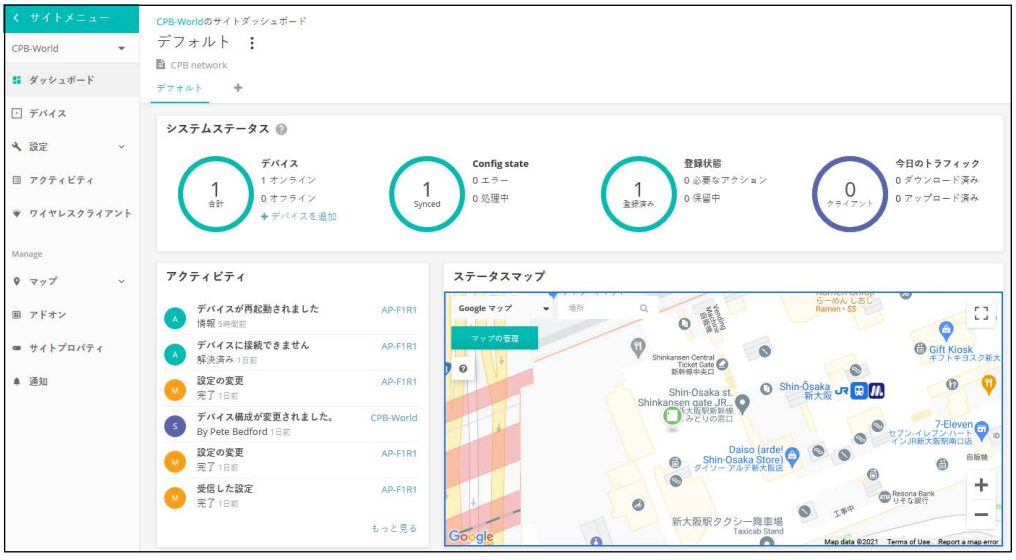
クラウドのメニューからサイト管理のメニューをクリックしてください。

図 42: サイトの管理ページ

すべてのサイトの名前、作成した日時、ユーザーのリスト、場所が表示されます。編集ボタンをクリックしてサイトのプロパティの編集や、サイトに登録されているデバイスがない場合は、削除ボタンをクリックし削除可能です。

サイトの名前をクリックしてサイトのダッシュボードを開いてください。

図 43: サイトのダッシュボード



3“ サイトの設定とさらに詳しいサイトの管理や設定の情報 “ をご覧ください。

ユーザの管理

クラウドサイトを作成した人がそのクラウドの所有者です。所有者は何人でもユーザを招待でき、所有者、管理者、レギュラーユーザなどを決定できます。

ユーザには下記のアクセスの権利があります。

- 所有者 — クラウドの所有者は、全てのウィジェットを書き込む権利があり、管理する全てのサイトとデバイスにアクセスできます。
- 管理者 — クラウドの管理者はほぼ全てのウィジェットを書き込む権利があり、管理する全てのサイトとデバイスにアクセスできます。管理者はデフォルト状態からの請求書とライセンスの設定をすることはできません。しかし、必要があれば、所有者が管理者にこの権利を与えることができます。
- レギュラーユーザ — サイトのユーザは所有者が設定したサイトに繋がっています。レギュラーユーザの中から、設定されたサイト内でのマネージャー（全ての書き込みをする権利があります）とゲスト（読むだけです）に分けられます。

クラウドメニューの " ユーザの管理 " をクリックしてください。

図 44: ユーザの管理

ユーザを管理するページを使うと、新しいユーザの招待、ユーザアカウントの取り消し、ユーザのアクセスに対する許可の編集を行うことができます。

ユーザを招待するをクリックして招待ページを開いてください。ユーザのメールアドレスと所有者、管理者、レギュラーユーザなどの役割を入力してください。管理者は 2 つの権利を選択できます。招待をクリックして、新しいユーザをサイトに招待してください。

図 45: 新しいユーザを招待する

“ 追加の権利 “ は任意となりますが、下記のアイテムが含まれます。

- ライセンスと請求を管理する — ライセンスと請求にアクセスする全ての権利があります。
- VPC の設定を管理する — VPC（バーチャルプライベートクラウド）を使用してクラウドをカスタマイズできます。カスタマイズされたクラウドでは Edgecore ブランドを取り除き、カスタマイズした名前とロゴなどを使用できます。

サイトグルーピング

同じクラウド内で複数のサイトを管理する必要がある場合、サイトグルーピングを使用すると、さまざまなサイトの情報を 1 つのページに集約することができます。

サイトグルーピングを使用すると、関連するサイトの論理的なコレクションを作成できます。サイトグルーピングを使用できるのは、クラウド所有者とクラウド管理者のみです。

サイトグループを作成するには、サイトの管理ページに行き、″ サイトグルーピングの管理 ″ をクリックします。

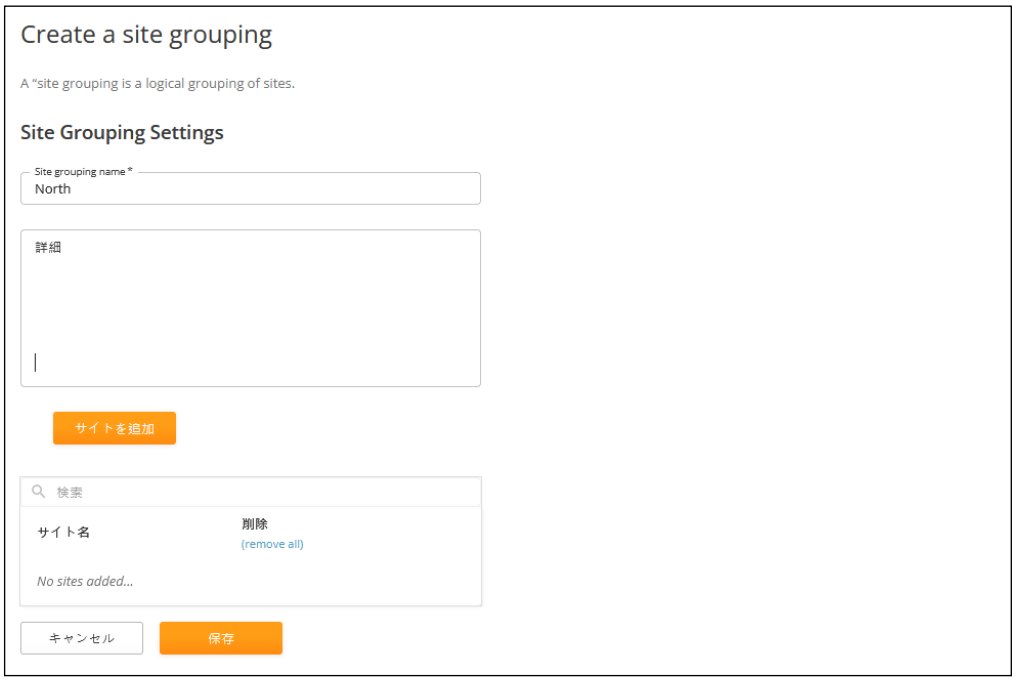
図 46: サイトグルーピングへのアクセス

サイトグルーピングページで、サイトグルーピングの追加をクリックしてください。

図 47: サイトグルーピングページ

サイトグループの名前と説明を入力します。「サイトを追加」をクリックし、リストから利用可能なサイトをグループに追加します。その後「保存」をクリックしてグループを作成します。

図 48: サイトグループの作成

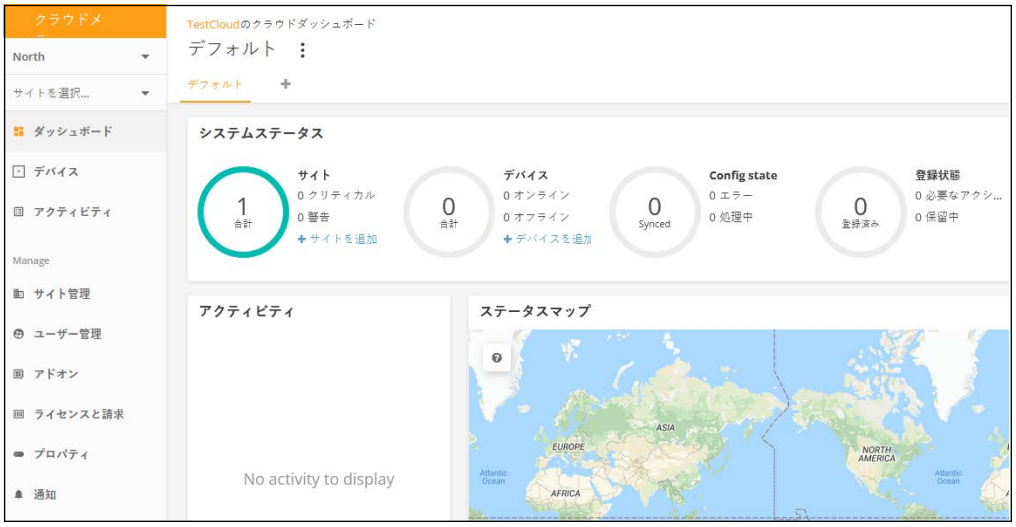


サイトグルーピングの管理ページでは、グループの編集や削除ができ、ページ左上の「グループを選択する」メニューを使ってグループ間を素早く切り替えることができます。

図 49: サイトグループの管理

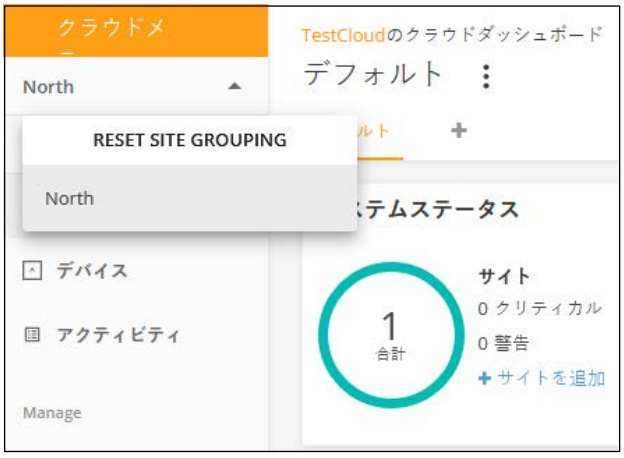
サイトグループを選択するとページがリフレッシュされ、グループ内のサイトから集約された情報を見ることができます。

図 50: サイトグループの情報を閲覧する



サイトグルーピングをグローバルビューにリセットするには、サイトグルーピングドロップダウンリストの「サイトグルーピングをリセット」をクリックしてください。

図 51: サイトグルーピングのリセット



常にクラウド設定に従う

サイト継承とデバイスレベルの変更に加え、ecCLOUD はクラウドとデバイス設定の双方向同期をサポートしています。ユーザーがウェブインターフェイスを通してローカルにデバイスのコンフィギュレーションを変更すると、その変更は ecCLOUD のコンフィギュレーションにプッシュバックされます。

ローカルのデバイスの変更によって ecCLOUD のコンフィギュレーションが変更されるのを防ぐために、ecCLOUD はデバイスから受け取ったローカルのコンフィギュレーションの変更を無視する " 常にクラウド設定に従う " 機能を提供します。この機能はデバイスのタイプやファームウェアのバージョンとは完全に独立しています。

注意：常にクラウド設定に従う」が有効になっているデバイスでは、ファームウェアのアップグレードを開始できません。ファームウェアのアップグレードを実行する前に、まずこの機能を無効にしてください。

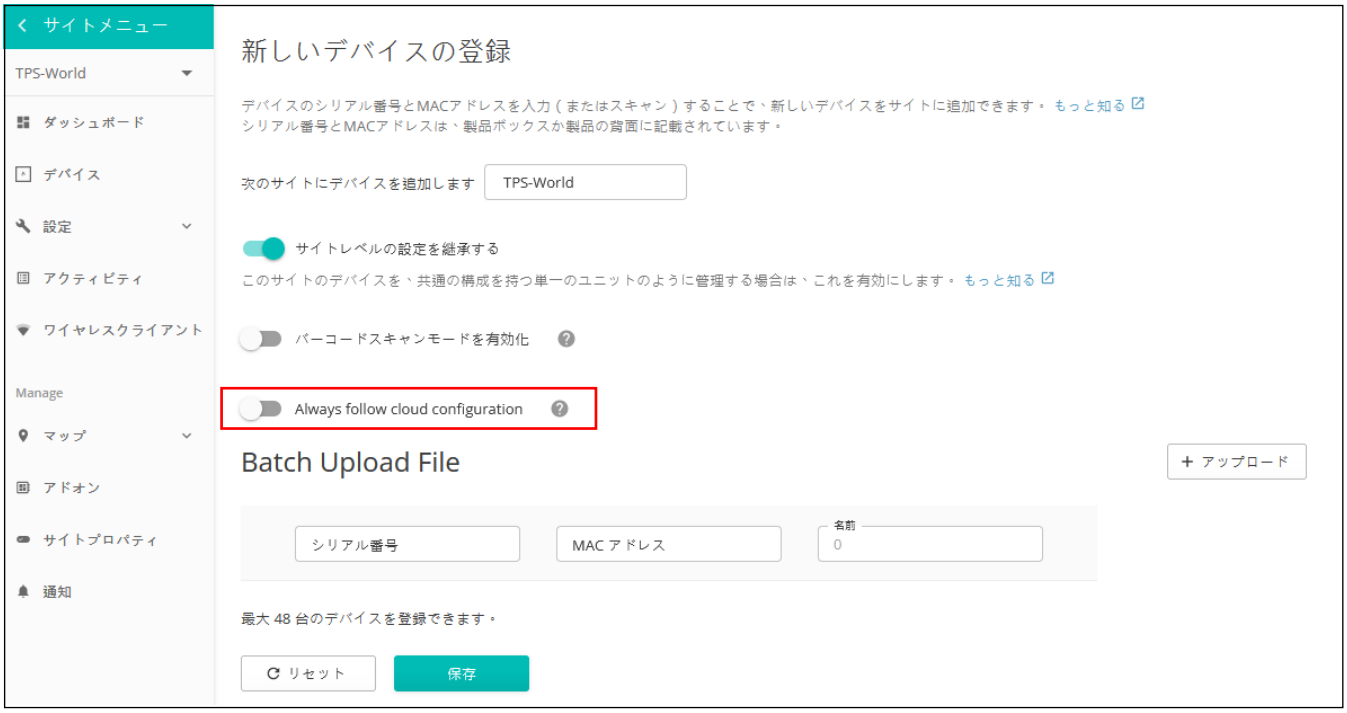
クラウドとデバイスの間でコンフィギュレーションが不一致の場合、ecCLOUD は " クラウドとデバイスの構成が一致していません " というメッセージでクラウド管理者に通知し、" 構成ステータス " は " 構成が一致していません " と表示されます。

クラウド管理者は、ecCLOUD のコンフィグレーションをデバイスに手動でプッシュするか、" 自動的にクラウド設定に従う " を有効にしてコンフィグレーションの不一致を自動的に解決するかを選択できます。

新しいデバイスを登録する際、" 常にクラウド設定に従う " を有効にすることができます。

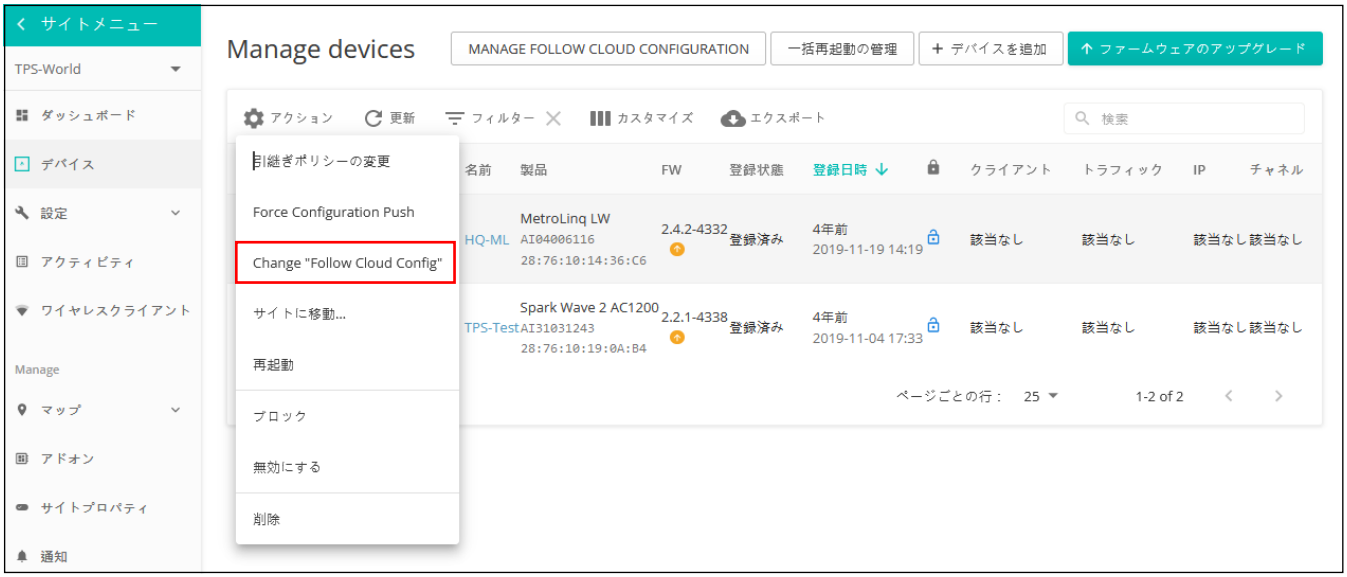
注意：QR コードオンボーディングによってデバイスが追加されると、「常にクラウド設定に従う」は自動的に無効になります。

図 52: デバイス登録時にクラウド設定に常に従うようにする



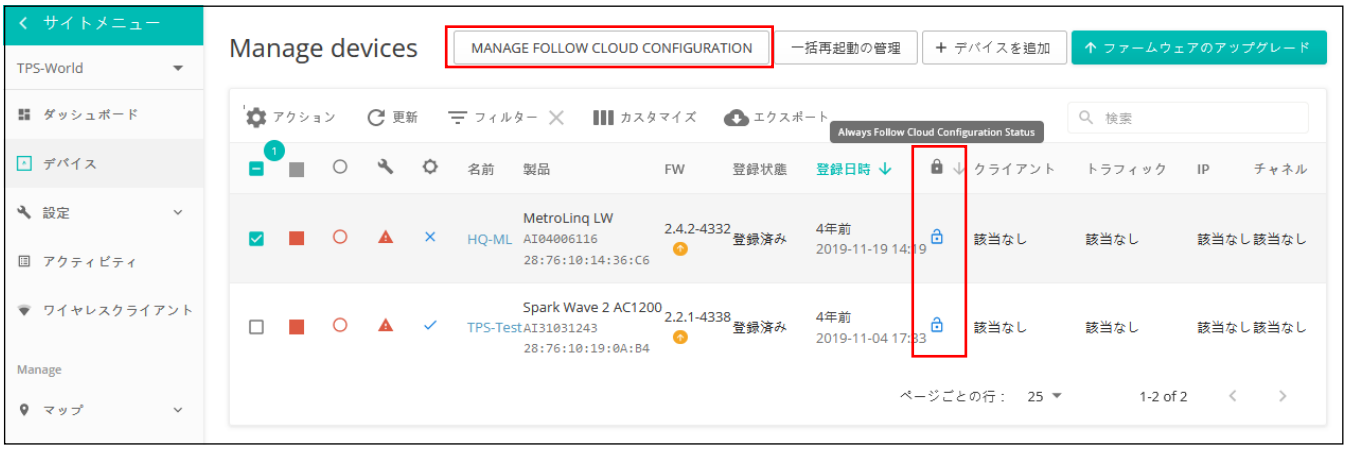
“ サイトレベルのデバイス ” ページから、複数のデバイスに対して " 常にクラウド設定に従う " を有効または無効にすることもできます。

図 53: デバイスページで ” 常にクラウド設定に従う ” を有効にする



サイトレベルの「デバイス」ページから、デバイスの「常にクラウド設定に従う」ステータスを確認したり、「フォロークラウドの設定を管理」ボタンを使用してこの機能を有効 / 無効にしたりできます。

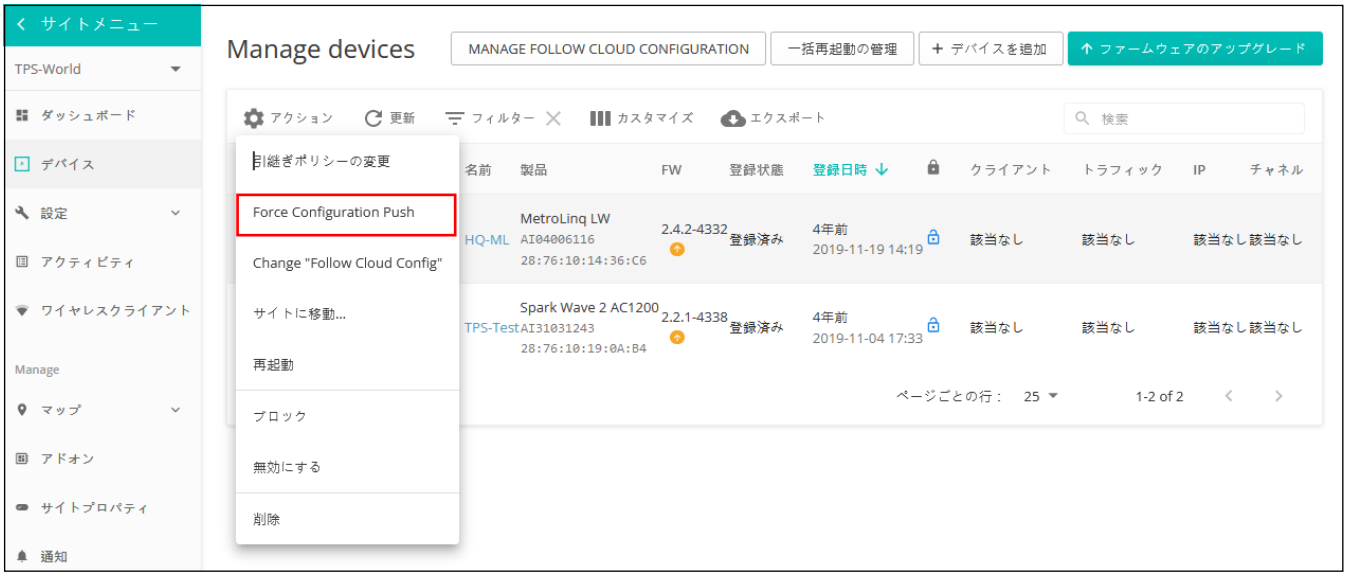
図 54: フォロークラウドの設定を管理



“ 常にクラウド設定に従う " を有効にすると、ecCLOUD はデバイスからの設定変更を受信しますが、クラウド上の設定は更新されません。この状況では、ecCLOUD は設定状態を " 構成が一致していません " とマークします。

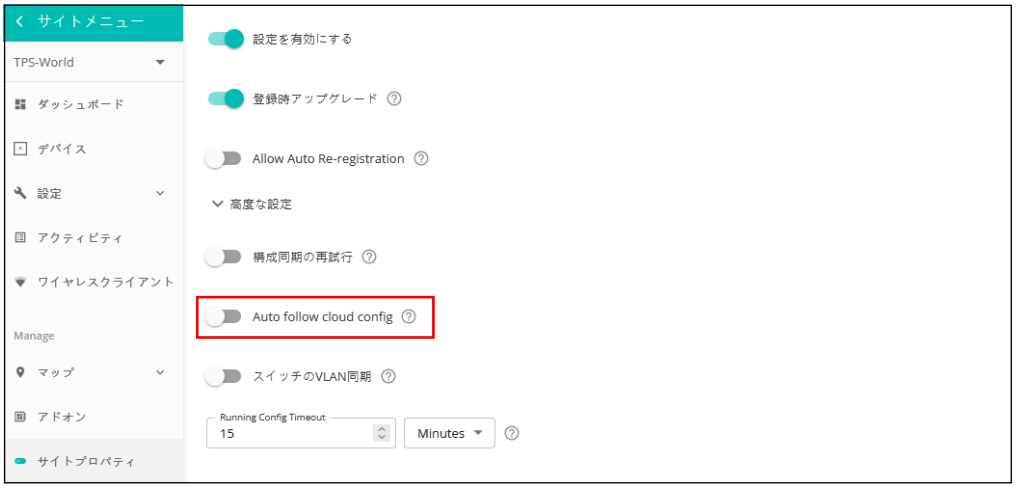
クラウドとデバイスの設定を同期するには、デバイスレベルの設定で " 同期する " をクリックするか、サイトレベルのデバイスページから設定をプッシュします。

図 55: 強制設定プッシュの使用



サイト詳細ページで " 自動的にクラウド設定に従う " を有効にすれば、設定を自動的にデバイスにプッシュすることができます。

図 56: “ 自動的にクラウド設定に従う ” の使用方法

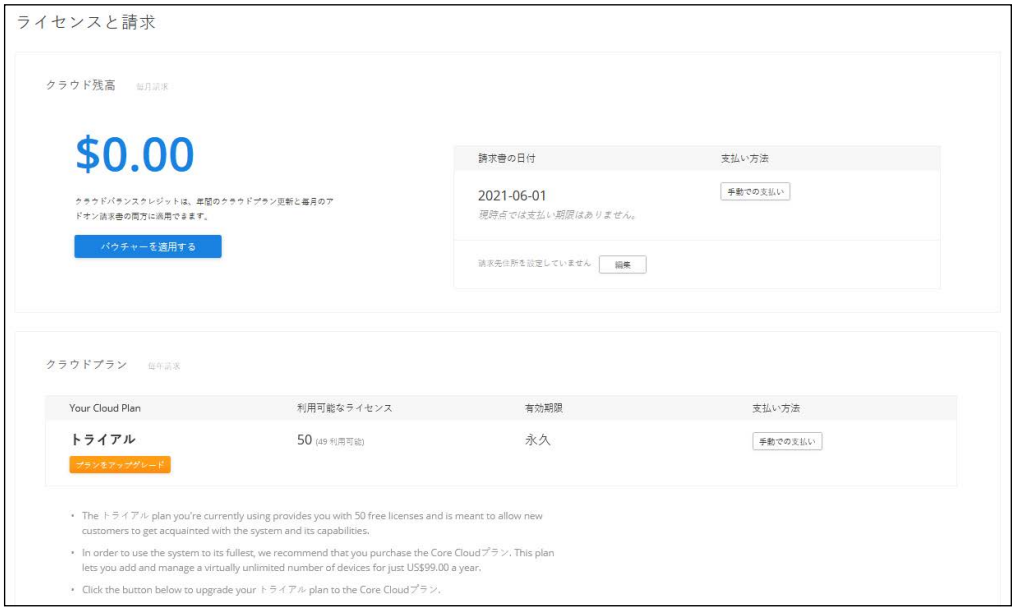


注意：MSP モードと " 常にクラウド設定に従う " を同時に有効にしないでください。デバイスの設定が ecloud に正しく更新されなくなります。

ライセンスと請求の管理

クラウドメニューのライセンスと請求をクリックすると自分の ecCLOUD の支払いプランを管理できます。

図 57: ライセンスと請求の管理



ライセンスと請求ページからは以下のことが可能です。

- バウチャーコードを申請して、自分のクラウドプランの支払いや、アドオンインボイスにクレジットを追加してください。
- クラウドプランをトライアルプランからコアクラウドプランやバーチャルプライベートクラウドプランにアップグレードしてください。アップグレードはクレジットカードでの、シングルマニュアルペイメントまたは自動的リニューアルペイメントによる支払いの際に可能になります。アップグレードされた支払いの際に、Edgecore バウチャーを申請できます。
- 使用可能なアドオンと請求記録を閲覧できます。

レポート管理

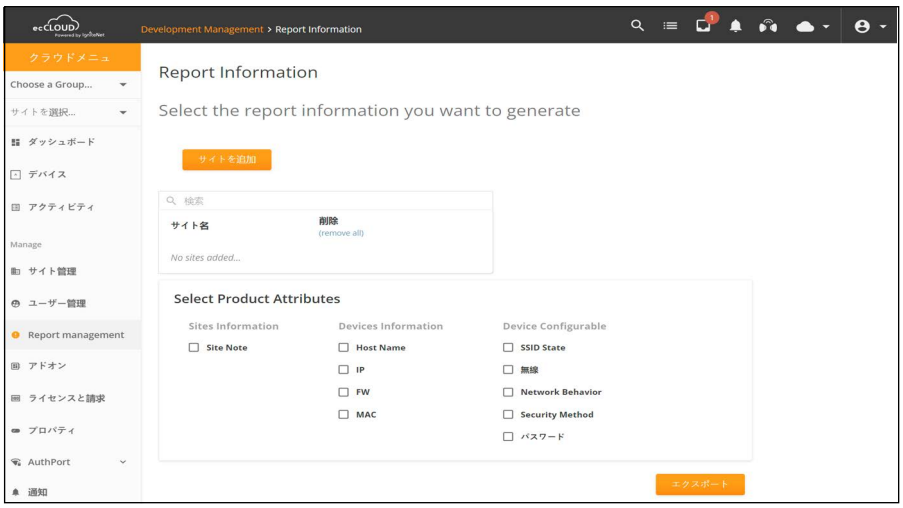
ecCLOUD のレポート管理機能は、クラウド所有者と管理者がネットワーク内のサイトの情報を含むカスタムレポートを生成し、ダウンロードする便利な方法を提供します。

レポートの生成

カスタム・レポートを作成するには、以下の手順に従ってください：

1. クラウドメニューの“レポート管理”

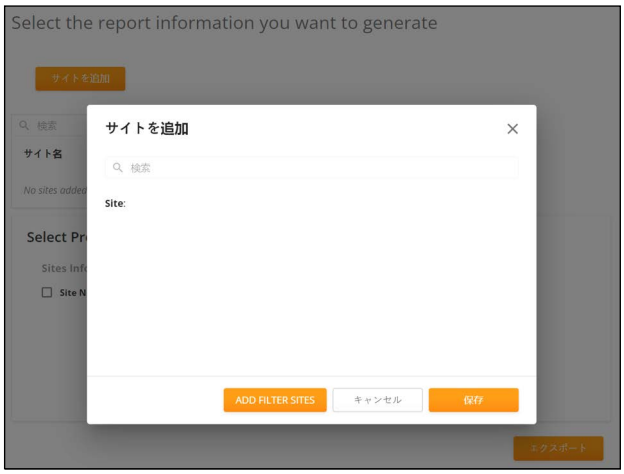
図 58: ライセンスと請求の管理



2. “サイトを追加”をクリックし、サイトをレポートに含めます。検索バーを使用し特定のサイトを検索するか、“Add Filter Sites”を使用

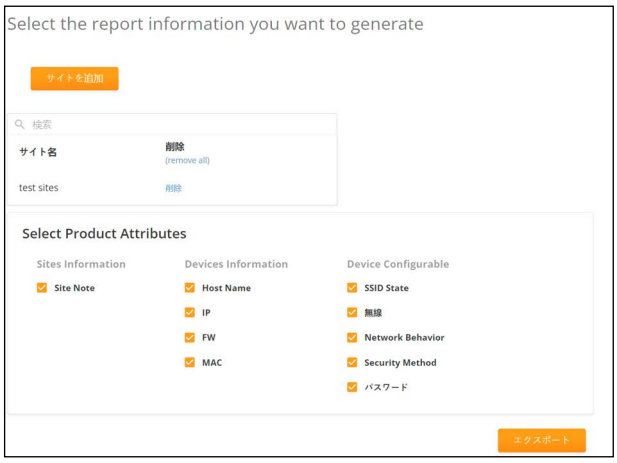
して特定の条件を満たす全てのサイトを含めます。“保存”をクリックし保存します。

図 59: サイトの追加



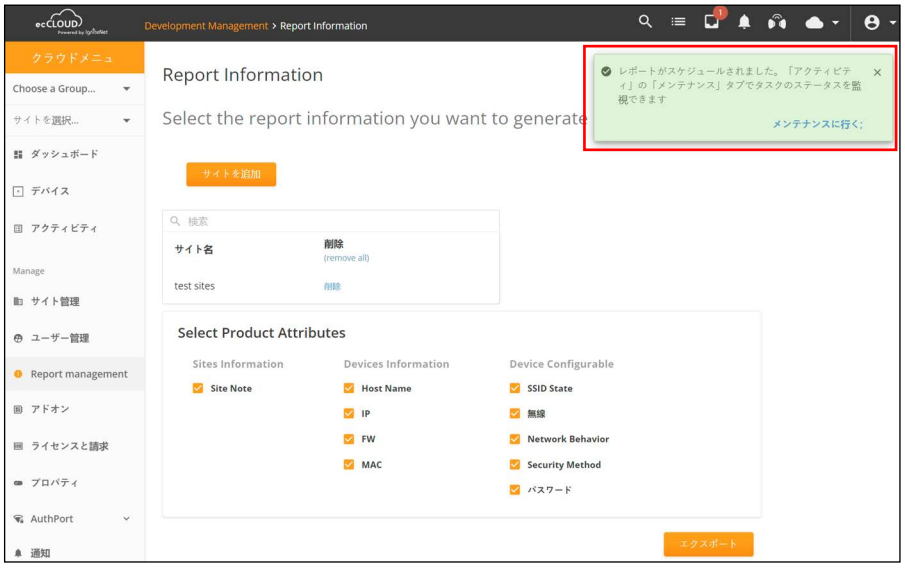
3. “Select Product Attributes（商品属性の選択）”からレポートに含める属性を選択します。

図 60: Site Attributes の選択



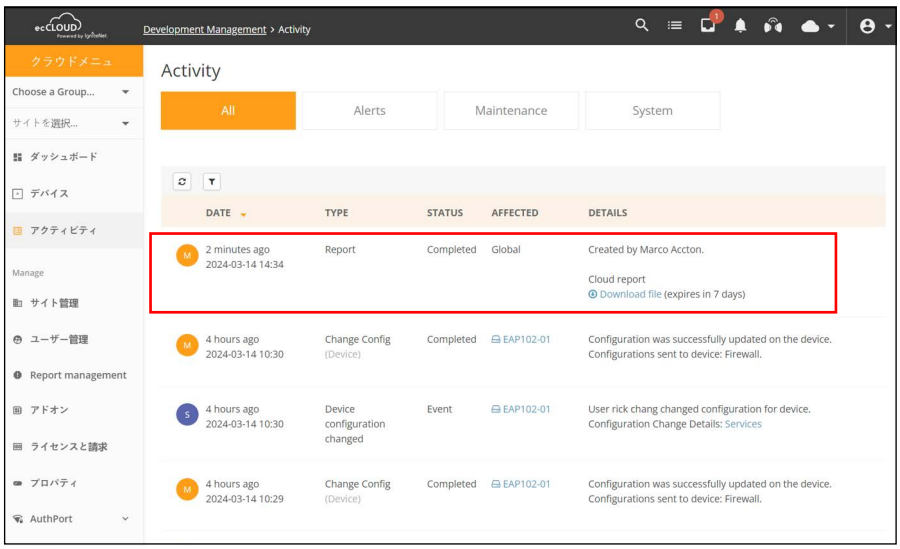
4. “エクスポート”をクリックしレポートを作成します。アクションの確認として、右上に緑色の通知が表示されます。

図 61: スケジュールレポートエクスポート



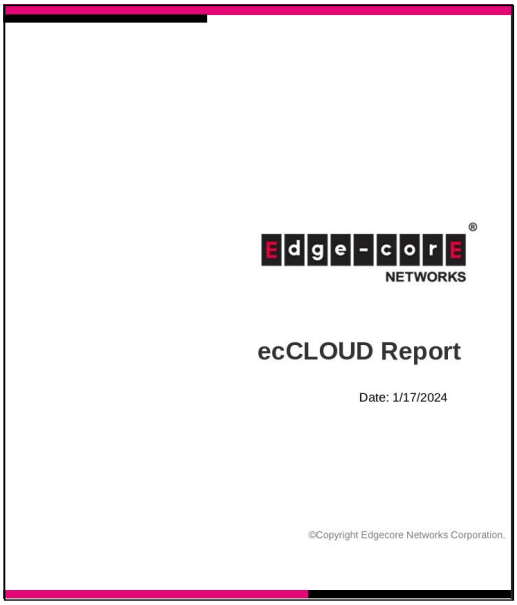
5. “アクティビティ”セクションでレポート作成のステータスを監視します。タスクが完了すると、レポートをダウンロードできるようになります。ファイルの有効期限は7日間です。

図 62: 活動セクションに関するレポート



6. “ファイルをダウンロード”リンクをクリックし、レポートをダウンロードしてください。レポートはお使いのローカルデバイスに保存されます。

図 63: レポートファイル



アドオン

このチャプターは下記のようなアドオンについて説明します。

- ゲスト WiFi とエクスターナルキャプティブポータルサービスを強化する。
- セキュリティとファミリーサービス。
- ecCLOUD のエクステンション
- 追加できるハードウエアのサポート

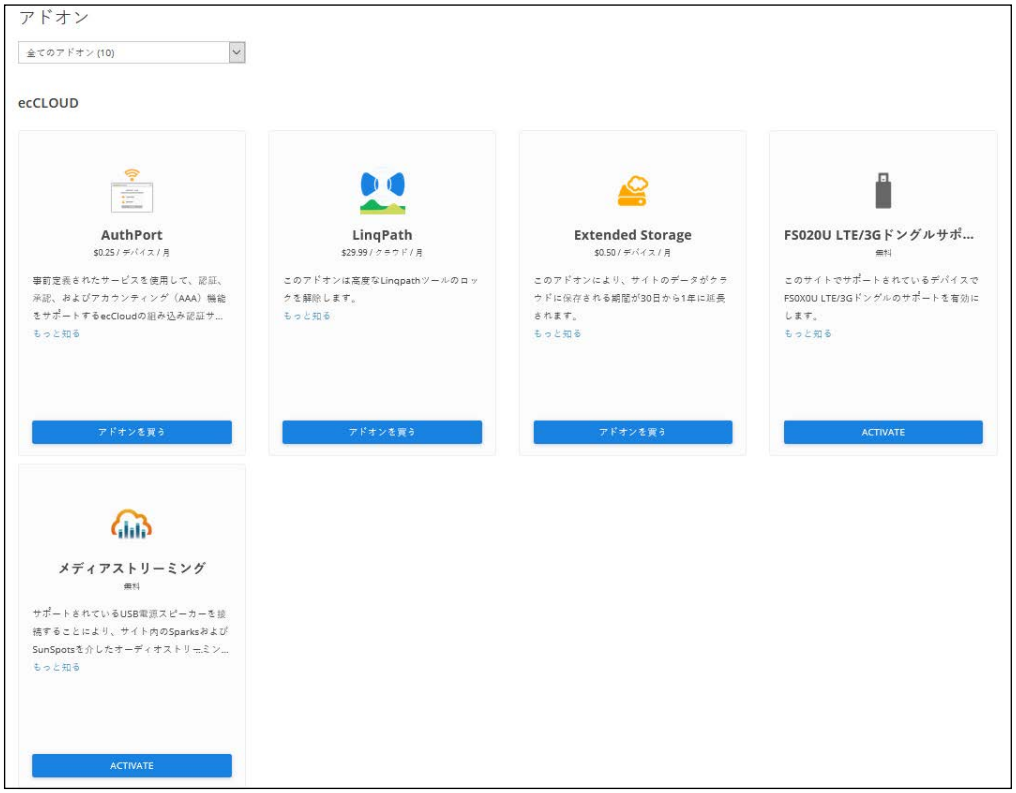
アドオンを使用する

クラウドレベルとサイトレベルの両方で利用可能なアドオンメニューから、選択アイコンをクリック、"Learn More " をクリックし、選択したサービスを使用するために "Activate " ボタンをクリックしてください。

特定のアドオンは、その機能がクラウド展開全体に影響するため、クラウドレベルでのみアクセス可能です。例えば、以下のようなものがあります：

- Wedge セキュリティサービス
- スマートインドアロケーション

図 64: アドオンメニュー



AuthPort アドオンを使用する

Authport アドオンは、ecCLOUD の内蔵型認証サーバーで す。無線のクライアントに対して、承認、認定、経理（AAA）機能を提供します。Authport を使えるようになると、時間とデータごとに計算された、異なるサービスプランに基づいたアカウンティングをできるようになります。無線のクライアントはネットワークに接続し、アカウントにログインして、インターネットにアクセスできます。

注意：現在のところ、Authport は以下のモデルでのみサポートされています。

ECW5211-L, ECWO5211-L, OAP100, ECW5410-L, SP-W2-AC1200 (L), SS-W2-AC2600, EAP101, EAP102, EAP104.

このアドオンメニューはクラウドまたはサイトメニューの " アドオン " メニューで購入できます。AuthPort アドオンの、" アドオンを購入する " ボタンをクリックしてください。

図 65: AuthPort アドオン

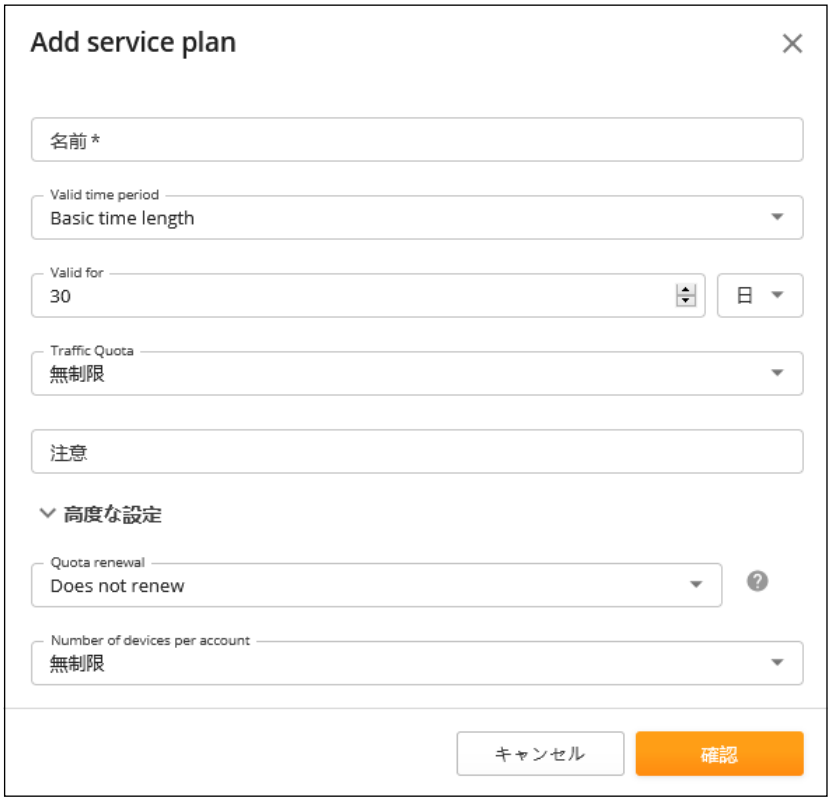
Authport アドオンを使えるようになると、クラウドメニューに Authport 設定メニューが表示されます。サービスプラン、経理、認証、キャプティブポータルの設定をしてください。

図 66: AuthPort メニュー

サービスプラン

サービスプランは、アカウントごとに使用できるサービスに制限を設けます。アカウントを作る前に、まずはサービスプランの計画をしてください。

図 67: サービスプランを追加する



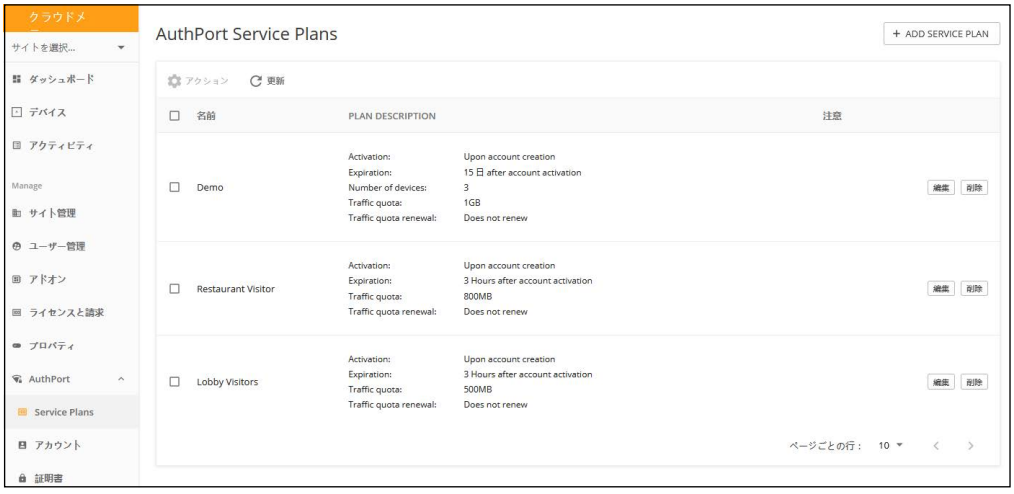
以下のリストはサービスプランとして設定可能なアイテムです。

- 名前：サービスプランの名前

- プランを使用可能な期間 — アカウントは決められた期間内のみ使用可能です。使用期間はアクティベーションと満期日で定義されます。
- アクティベーションタイム — クライアントはアクティベーションタイムが来る前にログインしてください。もし怠れば、アカウントの期限が切れ、使用不可となります。
- 満期日 — 満期日を過ぎると、アカウントは期限切れとなり、使用できなくなります。
- トラフィッククオータ — アカウントで使用できるデータのトラフィックの割り当て分の上限です。クライアントが割り当てられた以上のトラフィックを使用すると、アカウントは " クオータ不足 " の状態となり、ログインができなくなります。
- ノート — プランに追加する様々な情報。
- クオータリニューアル — データのトラフィッククオータを更新する時期を設定します。クオータは日々、週ごと、またはひと月ごとに更新できます。
- アカウントごとのデバイスの数 — 一度のログインで一つのアカウントから管理できるデバイスの数です。

サービスプランページからは、存在する全てのプランのリストを閲覧できます。新しいプランを追加したり、すでにあるプランを編集した り、必要がないプランを削除できます。

図 68: サービスプランの全体像を見る



アカウント

無線クライアントのアカウントは、サービスプランに基づいて作成できます。アカウントは 1 つずつでも、いくつかのアカウントをグループとしてでも作成できます。一つのアカウントを作成するためには、ユーザ名とパスワードを手動で設定する必要があります。いくつかのアカウントを一度に作成する場合には、ユーザ名をパスワードはランダムに作られます。

図 69: 一つのアカウントを作成する

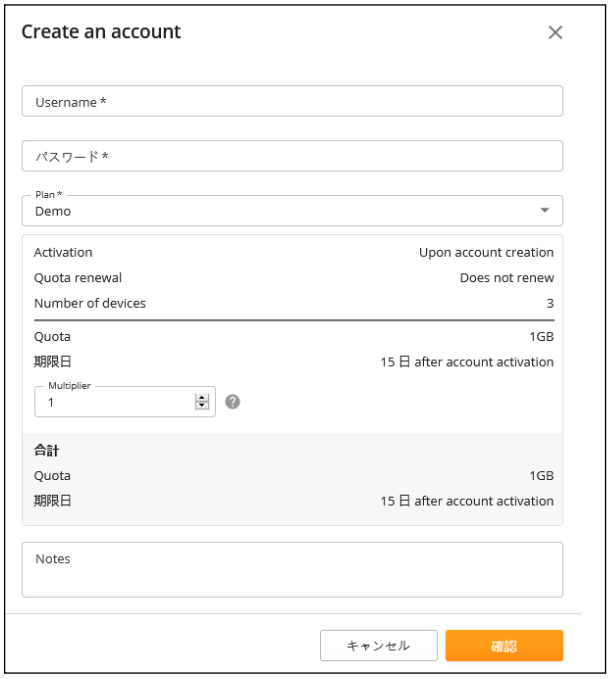
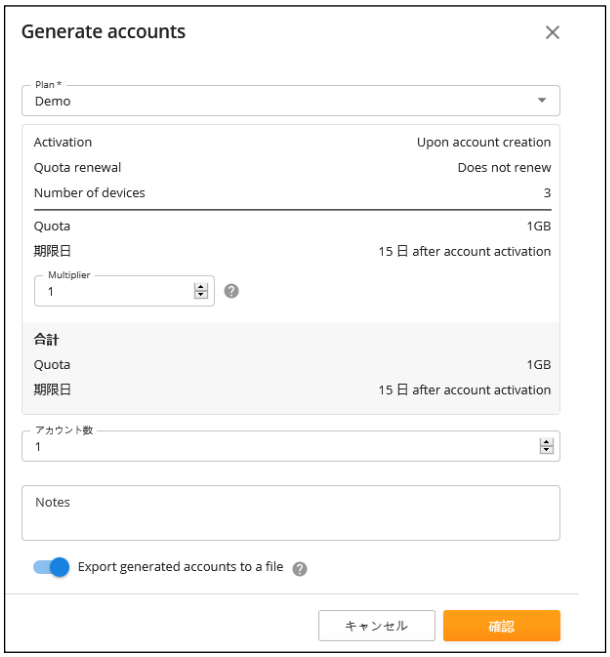
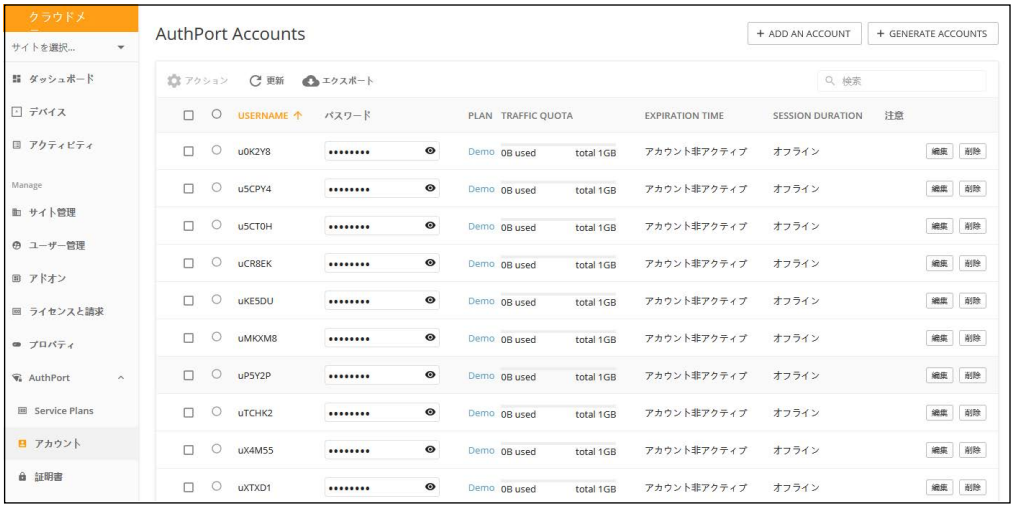


図 70: 複数アカウントを一度に作成する



アカウントを作成するどちらの方法も、クオータを " 掛け算 " できます。アカウントが作成したサービスプランに対して、基本量のクオータ量を倍増して設定できます。例えば、あるアカウントが 10GB クオータを所持するサービスプランを作成したとします。この基本のクオータを 3 倍にして、30GB クオータ分の設定できます。

図 71: アカウントのリスト



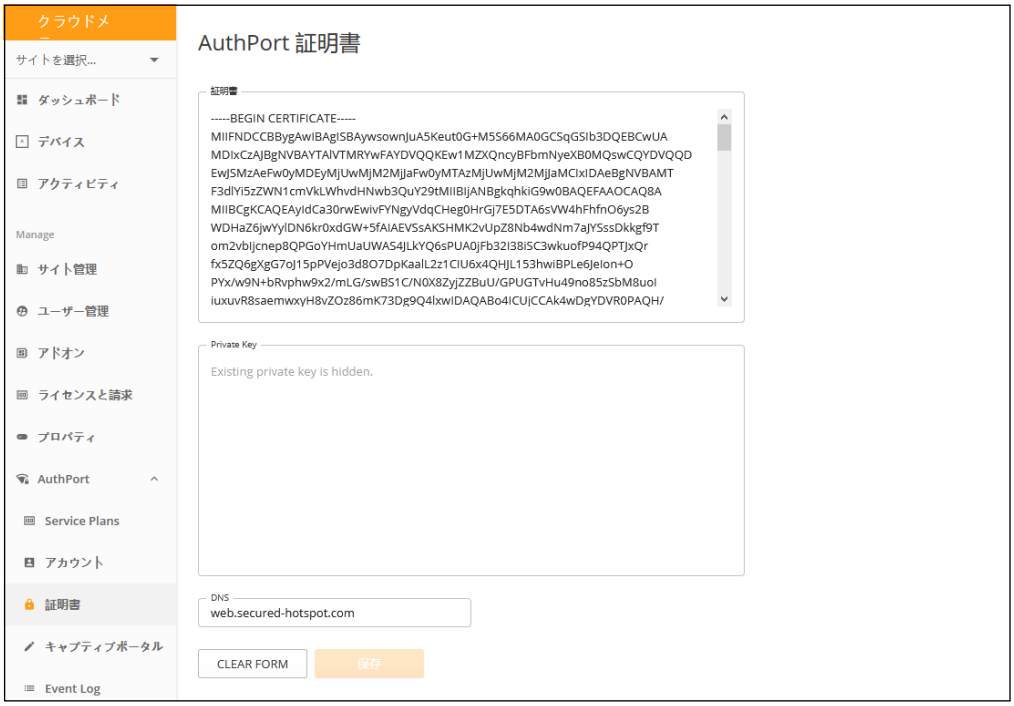
作成されたアカウントはアカウントリストに表示されます。アカウントリストからは、アカウントのステータス、アカウントに該当するプラン、満了の日時、トラフィッククオータについての情報を閲覧できます。

管理者は、それぞれのアカウントのパスワード、該当する サービスプラン、クオータ合計の倍数を編集できます。さらに管理者は、選択したアカウントを CSV フォーマットのファイルに送信したり、無線クライアントに配布できます。

AuthPort 認証

Authport 認証が有効な場合、クライアントが SSID に接続した際に、キャプティブポータルページが表示されます。管理者はセキュリティ認証をアップロードし、キャプティブポータルページにおいてのクライアントのドメインネームを設定できます。

図 72: AuthPort 認証



認証が設定されなかった場合、無線クライアントは暗号化されていない HTTP 接続状態のキャプティブポータルページに戻されます。セキュリ ティを考慮すると、有効な認証をアップロードすることを推奨します。有効な認証が可能になると、キャプティブポータルが HTTPS に保護されます。また、証明とプライベートキーは PEM フォーマットを使用することをお勧めします。認証ファイルとプライベートキーファイルの該当する部分をコピー、ペーストしてください。

ドメインネームサービス（DNS）について説明します。アドミニストレーターは無線クライアントのドメインネーム（DNS）を設定し、クライアントがキャプティブポータルページを閲覧できるようにしてください。ドメインネームサービス（DNS）が設定されていない場合は、クライアントのキャプティブポータルページの URL 内に、アクセスポイント（AP）モードの IP アドレスが表示されます。

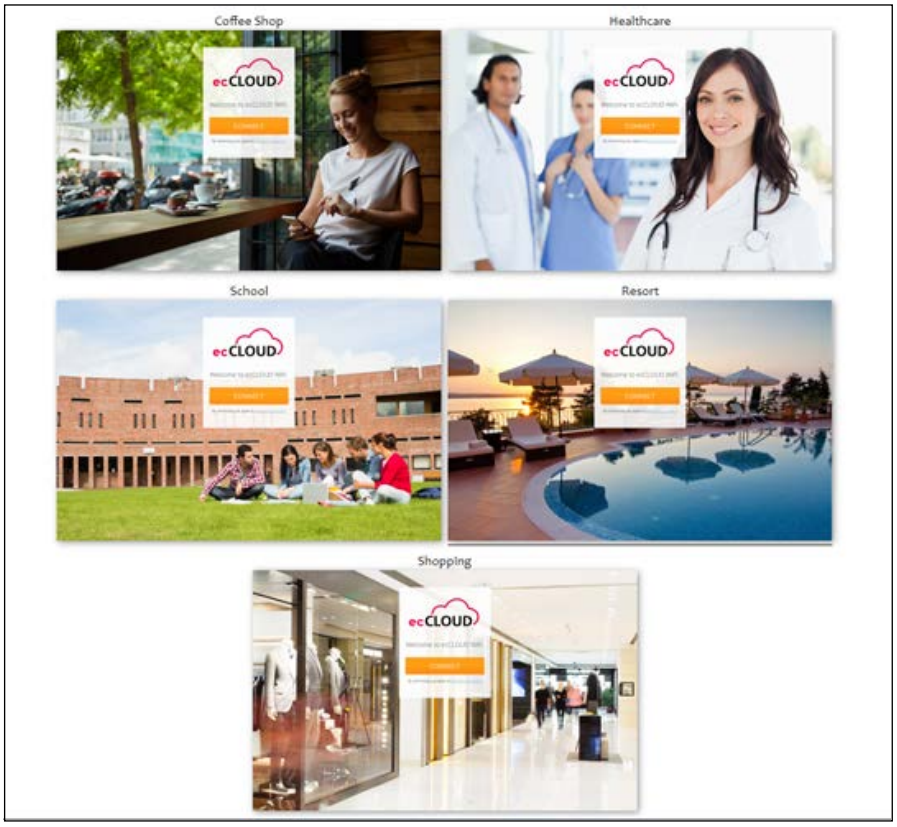
Web ブラウザにセキュリティ警告が起こらないようにするために、信頼できる機関の認証を受けるようにしてください。また、ドメインネームが、認証に使われた " コモンネーム（CN）" と同じであるように設定してください。

キャプティブポータル

Authport を使用すると、エディターでキャプティブポータルページをカスタマイズできます。多数のキャプティブポータルのテンプレートを準備可能なため、Authport が有効な SSID が複数ある場合は、それぞれ異なるテンプレートを使用できます。

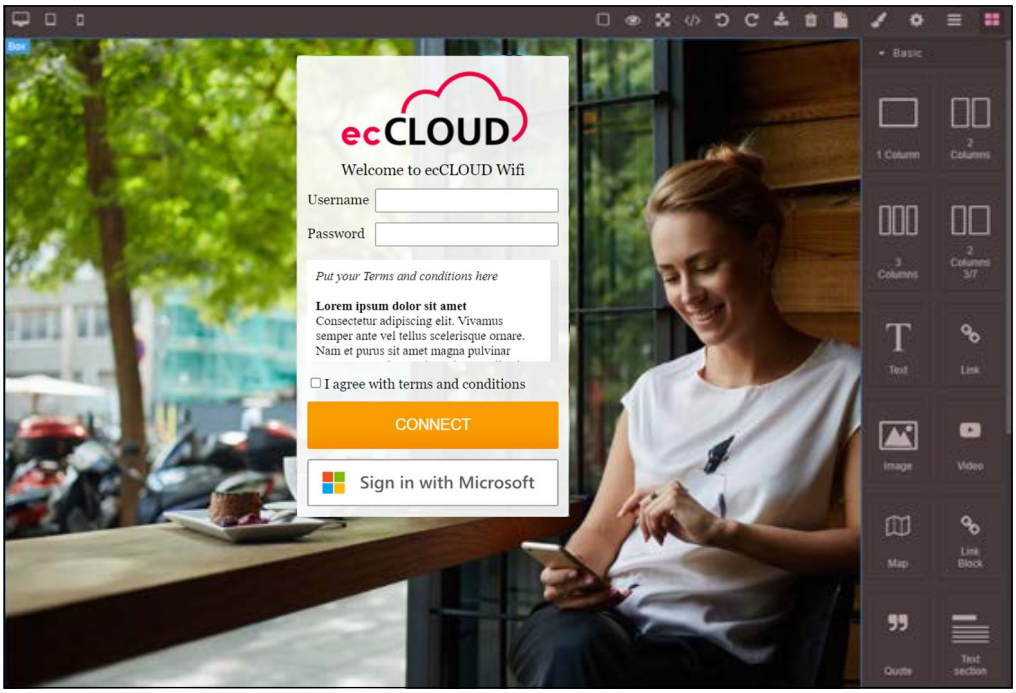
もしキャプティブポータルを作成し、エディターにアクセスするのが初めてな場合は、自分のキャプティブポータルのテーマを選択するように誘導されます。自分のサービスにより近いテーマを選択し、ページの内容を編集してください。

図 73: オースポートキャプティブポータルのテーマの例



テンプレートを選択すると、キャプティブポータルエディターに誘導されます。エディターのレイアウトは大まかに 3 つの部分があります。ツールバー、オプション／アトリビュートパネル、プレビューフレームです。ツールバーはエディターの上の部分にあります。右側にはオプションとアトリビュートが設定できるようになっています。プレビューフレームを使うと、ドラッグアンドドロップ形式でページ内のウィジェットを探したり、自分のポータルデザインをリアルタイムで閲覧したりできます。

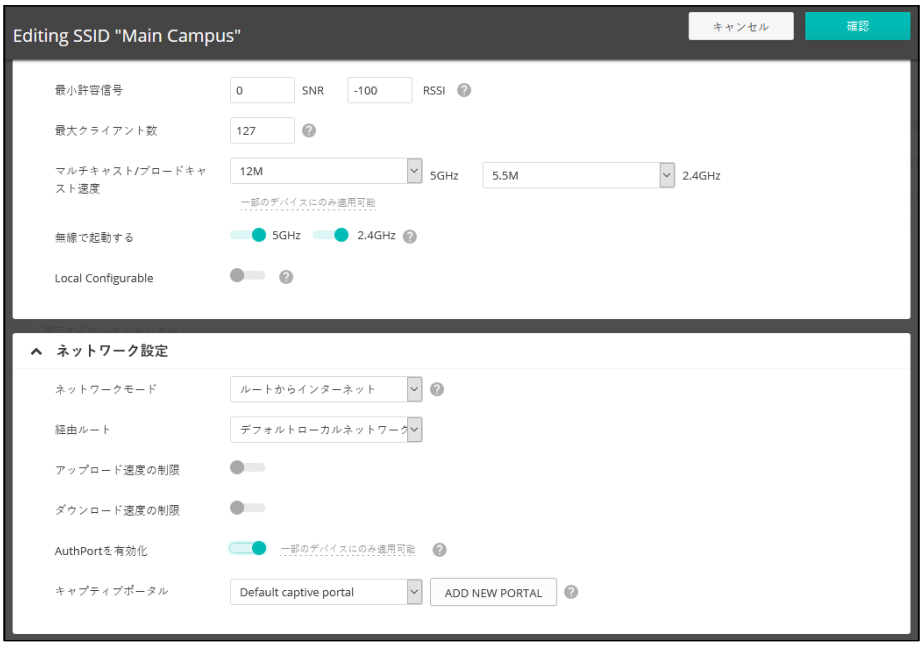
図 74: AuthPort キャプティブポートのエディター



SSID の設定

例えば、1 つ目はスタッフ用で 2 つ目は顧客用の、2 つの SSID があるとします。この場合、顧客用の SSID だけに Authport の認証機能を設定できます。スタッフがスタッフ SSID にアクセスしたい時は、すぐに接続できます。スタッフが顧客 SSID に接続する場合は、キャプティブポータルページが表示され、ログインが必要です。

図 75: AuthPort SSID の設定



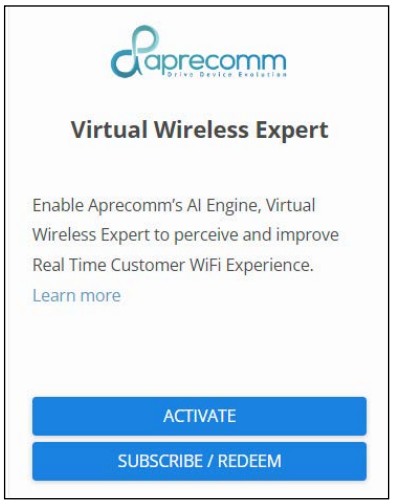
Authport 認証はキャプティブポータルだけでなく、EAP 認証でも使用できます。セキュリティの方法がオープン、WPA-PSK、WPA2-PSK のいずれかであり、Authport が SSID に対して有効である場合、無線クライアントは接続の際にキャプティブポータルページに誘導されます。クライアントは Authport で作成したアカウントでログインしてインターネットに接続できます。クライアントは、AuthPort で作成したアカウントまたは Microsoft 365 の認証情報を使用してログインし、インターネットにアクセスすることができます。

セキュリティの方法が WPA-EPA または WPA2-EPA であり、オースポート（AuthPort）が SSID に対して有効であれば、クラウドは EPA 認証に対して RADIUS サーバーとなります。無線クライアントは、オースポート（AuthPort）で作成したアカウントをクレデンシャルとして使用し、トランスペアレントログインを行うことができます。

Aprecomm アドオンを使用する

Aprecomm add-onは、Virtual Wireless Expert (VWE)を通し、ISPにリアルタイムのネットワーク可視性と洞察のための統合ツールを提供し、トラブルシューティングを簡素化します。

図 76: Aprecomm アドオン

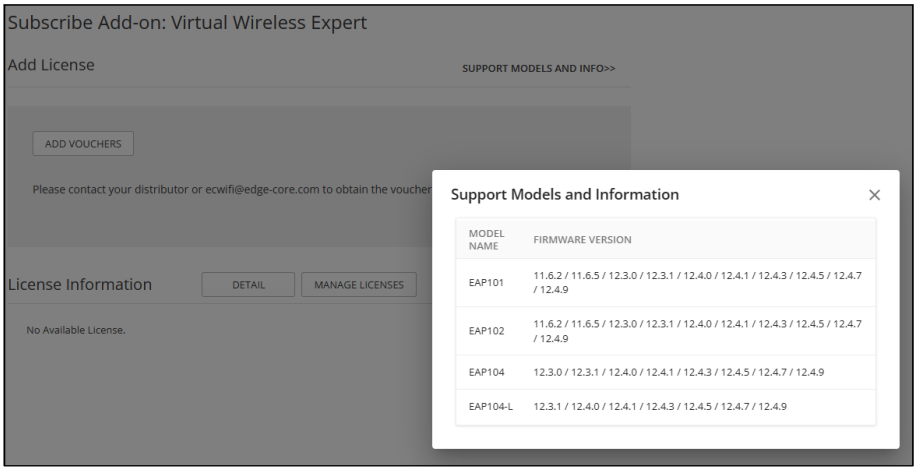


対応済みデバイスとファームウェア

サポートされているEdgecore Wi-Fi APの情報を表示するには、以下の手順をご確認ください：

1. クラウド、サイト、またはデバイスレベルの「アドオン」メニューで、“Subscribe/ Redeem”をクリックします。
2. “Support Models and Info” を選択し、サポートされているモデル名とファームウェアの詳細を表示できます。

Figure 77: 対応済みデバイスとファームウェア



Freemiumの有効化

Freemiumバージョンは、クラウドレベルでグローバルに有効化し、サイトレベルでも個別に有効化できます。

1. クラウドまたはサイトメニューの“Add-on”をクリックし、Aprecommの Virtual Wireless Expertの“Activte”をクリックします。
2. 有効化を確認すると、互換性のあるファームウェアを実行しているデバイスにAprecommのパッケージが自動的にインストールされます

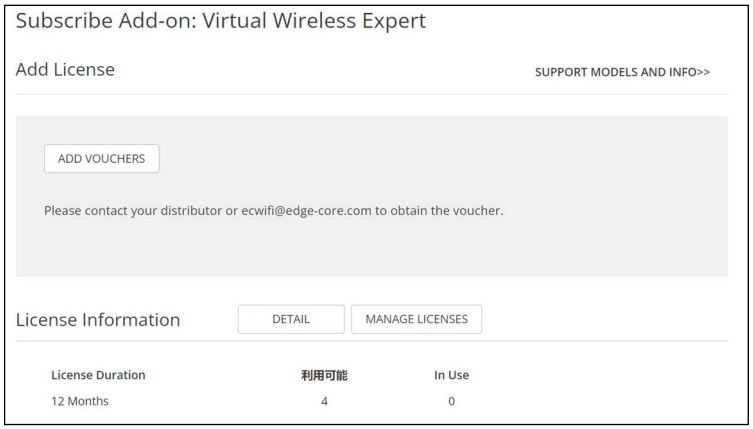
注意：デバイス上のクラウドエージェントは、Aprecomm のパッケージを含む、インストールする新しいパッケージを ecCLOUD に定期的に問い合わせます。デバイスを再起動することで、プロセスが早くなる場合があります。

ライセンスの購入

Freemiumを超えて可視性とインサイトを強化するには、以下の手順に従ってAprecomm VWEライセンスを購入し、適用してください：

1. バウチャーコードを購入するか以下のメールに問い合わせください。ecwifi@edge-core.com.
2. クラウドメニューの“Add-on”から“Subscribe/Redeem”を選択し、ecCLOUDにライセンスを追加します。“Add Voucher”をクリックし、提供されたバウチャーコードを入力してください。

図 78: VWE Licenses の追加

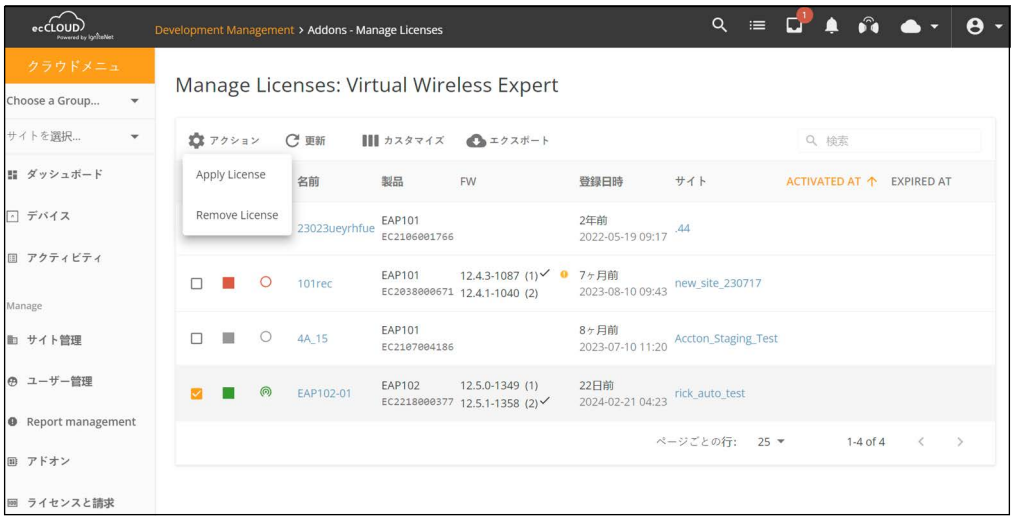


3. クラウドメニューの“Add-ons”から“Subscribe / Redeem”を選択し、ライセンスを有効にします。
4. “Manage Licenses”をクリックし、サポートされているデバイスをリストアップします。

5. お求めのデバイスを選択します。

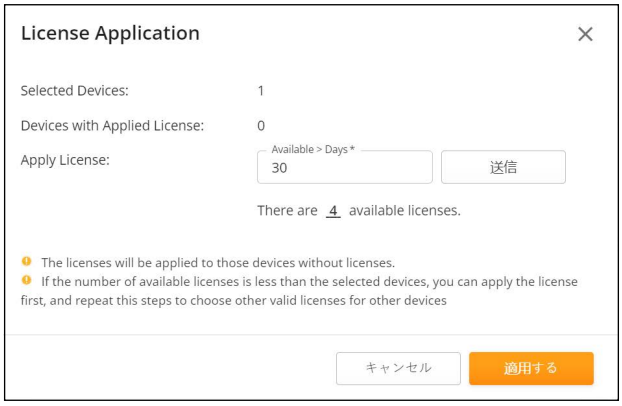
6. “アクション”と“Apply License”をクリックします。

Figure 79: VWE Licensesの適用



7. 利用可能なライセンスを利用可能な日数で絞りこみ、必要に応じ申請してください。

Figure 80: 日数あたりのVWEライセンス



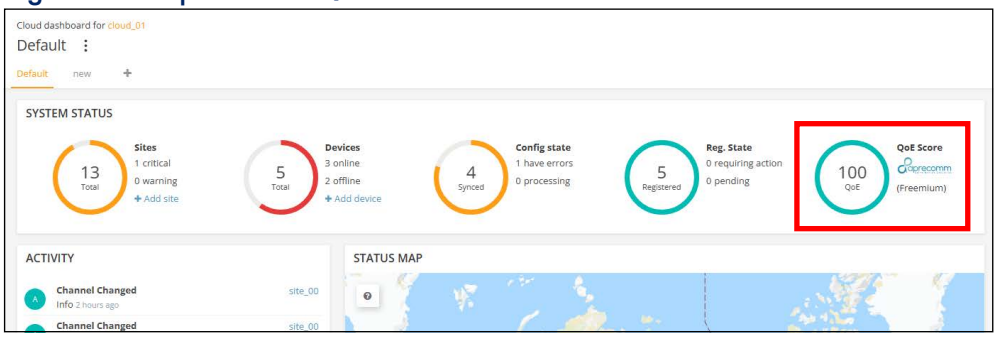
8. ライセンスの適用後、選択したデバイスにAprecommのパッケージを自動的にインストールします。

注意：デバイス上のクラウドエージェントは、定期的に ecCLOUD に Aprecomm のパッケージと関連ライセンスを含む新しいパッケージのインストールを問い合わせます。デバイスを再起動することで、このプロセスを促進できます。

VWEダッシュボードにアクセスする

Freemiumプランでは、AprecommのQoEスコアはダッシュボードでクラウド、サイト、デバイスレベルで確認できます。

Figure 81: Aprecomm QoE Score



3 基本のサイトの設定

このチャプターではサイトの設定について説明します。サイト内のデバイスをはじめ、いろいろな場面で使用するパラメーターの設定についても言及します。

サイトの全体像

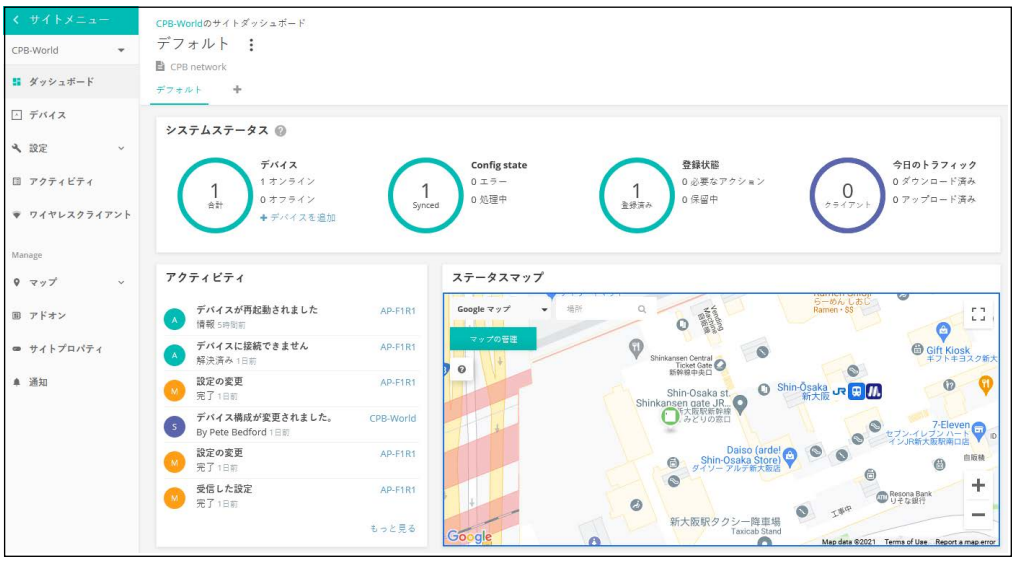
一つのサイトはデバイスを論理的にグループ化していますが、全てのデバイスが同じ設定であるとは限りません。1 つのグループのデバイスは、大体同じサイトに位置されています。

例えば、ホテルチェーン用に 50AP を設置するとします。ecCLOUD コントローラは、それぞれのホテルを異なるサイトとして設定します。それぞれのホテルは地理的な理由でまとめられ、フロアマップ、適する言語、タイムゾーンの設定が行われます。

注意：1 つのサイトごとのデバイスは 500 以下に限られています。

クラウドに追加することのできるサイトの数は、クラウドプランによって異なります。コアクラウドプランでは 500 サイト以下に決められていますが、バーチャルプライベートクラウドプランならば 5000 サイトまで追加できます。

図 82: デフォルトサイトのダッシュボード



サイトの作成

初めてのクラウドを作成するということは、初めてのサイトを作り、デバイスを追加するということです。詳しくは、28 ページの「クラウドを作成する」をご覧ください。

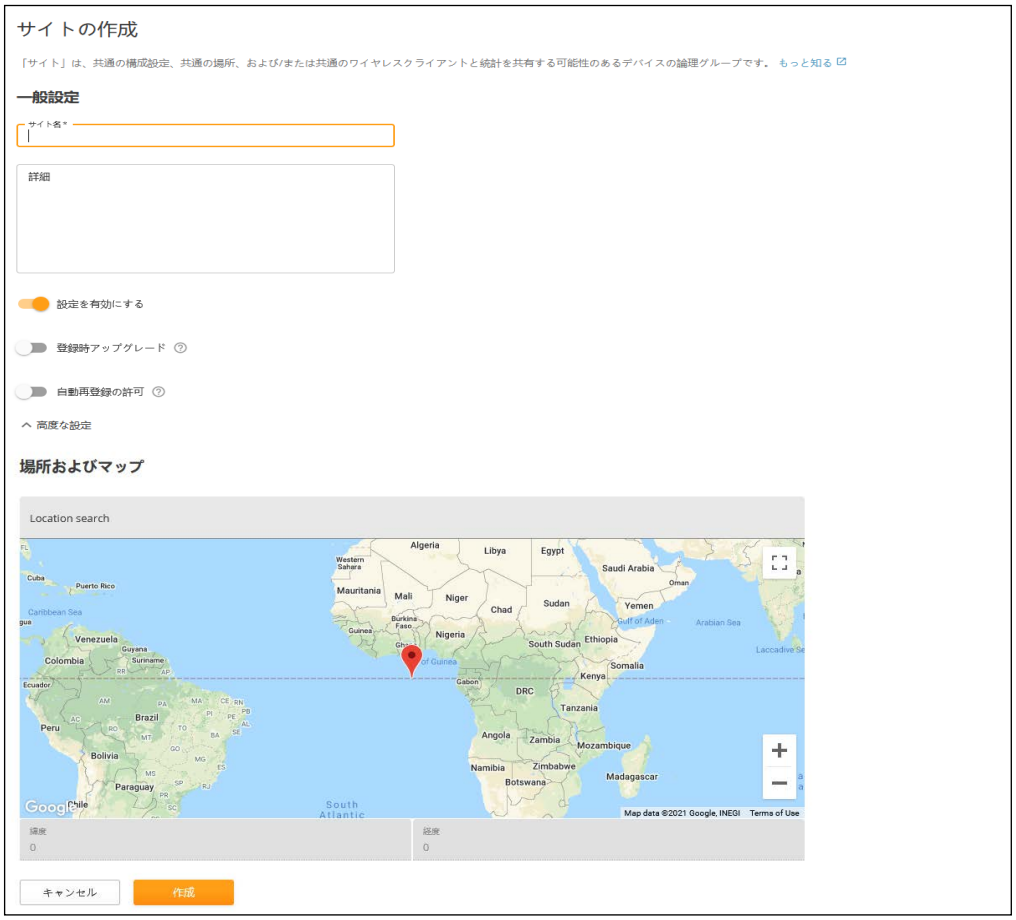
サイトメニューからさらにサイトを追加する場合は、メニューの上側にあるプルダウンリストをクリックして、リストの一番下の " 新しいサイトを作成する " をクリックしてください。

図 83: 新しいサイトを作成する

" 新しいサイトを作成する " ページを開いたら、新しいサイトのプロパティを入力し、マップを使って地理的情報を選択してください。

注意：アステリスク（＊）マークのついた欄は入力必須です。

図 84: 基本のサイトのプロパティを見てみよう



一般的な設定

- サイトの名前 – 自分のサイトに名前をつけます。短くても意味がわかりやすい名前を選びましょう。例えば、“ アトランタにあるパークサイドホテル “ のサイトには、“ パークサイドアトランタ “ という名前はどうでしょうか。
- 詳細 - この欄はサイトについて自由に書き込むことができます。
- 可能な設定 : 下記の設定が可能です。
  - オン : デフォルトはこの状態です。隔離した状態で設定が行えます。
  - オフ : 直に設定を行う必要があります。隔離状態でデバイスをモニターしたり、デバイスがオフラインになった際のアラートを受け取ることができます。
- 登録の際にアップグレードする : この設定にすると、登録後、ファームウエアが自動的に最新の状態にアップグレードされ続けます。この設定にすることをお勧めします。

- 自動再登録：この設定をすると、デバイスがリセットされてデフォルト状態になっても自動的に再登録されます。この設定がされていない場合は、ログインし直して手動でデバイスの再登録を行う必要があります。

位置とマップ

位置 - 位置の設定は、デフォルト状態の時にダッシュボードにどのマップが表示されるか、さらに無線での設定の場合にどの国を基盤とするかを決定します。

図 85: タイムスパンプによるトポロジー・マップ

トポロジーマップ - ecCLOUD は、ネットワーク通信に基づいてインタラクティブなネットワークトポロジーを自動的に描画します。ページには、最新の更新時間を示す "Last Updated " タイムスタンプが表示されます。最小更新間隔は 1 時間です。

サイトの設定

サイトの情報を全て入力したら、作成をクリックしてサイトを作ってください。新しいサイトの基盤となる国と地域とローカルログインなどの一般設定を行ってください。

図 86: 基盤となる国の設定

基盤となる国は、基本的にサイトの位置とマップの設定に基づいてすでに設定済みになっていることが多いです。ローカルログインも、適当に作られたパスワードを伴ったデフォルト状態のアカウントがすでに設定されていることでしょう。必要に伴って、パスワードを変えたり、追加のローカルアカウントを設定してください。

注意：ローカルログインした際の ecCLOUD のデフォルト状態のアカウントは、以前デバイスを登録していたローカルユーザのアカウントのデフォルトに上書きされています。デバイスにサイト内での設定を施した後は、ecCLOUD のサイトレベルで設定したローカルログインを使用してください。

図 87: ローカルログインの設定

基盤となる国とローカルログインを設定したら、“ 保存 “ をクリックして設定を保存してください。

デバイスを追加する

サイトの設定を初めて保存すると、無線、スイッチ、メッシュリンクス（MeshLinqs）、ジーリンクス（GLinqs）などに分類してデバイスをサイトに追加するように誘導されます。“ デバイスを追加する “ をクリックして手順を進めてください。

図 88: デバイスを追加する誘導

“ 新しいデバイスを登録する “ ページにシリアル番号、MAC アドレス、名前を入力し、送信をクリックしてください。“ バーコードスキャンモード “ を ON にしてバーコードをスキャンする方法もあります。スキャナーを使用す

ると、デバイスのシリアル番号と MAC アドレスの入力が簡単になります。入力が完了すると、バーコードスキャンモードを切って、デバイスの名前を手動で入力してください。デバイスをサイトに追加する準備ができたら、送信ボタンをクリックしてください。

また、一括アップロードのオプションもあります。まず、CSV でデバイスのリストを用意する (comma-separated values) ファイルです。CSV ファイルは、プレーンテキストファイルであり、情報がをカンマで区切って表示します。各機器について、シリアル番号、MAC アドレス、名前は、以下の書式のように 1 行で入力する必要があります。

```
<Serial Number 1>,<MAC 1>,<Device Name 1>
<Serial Number 2>,<MAC 2>,<Device Name 2>
```

アップロード ボタンをクリックして、CSV ファイルをアップロードします。

図 89: 新しいデバイスを登録する

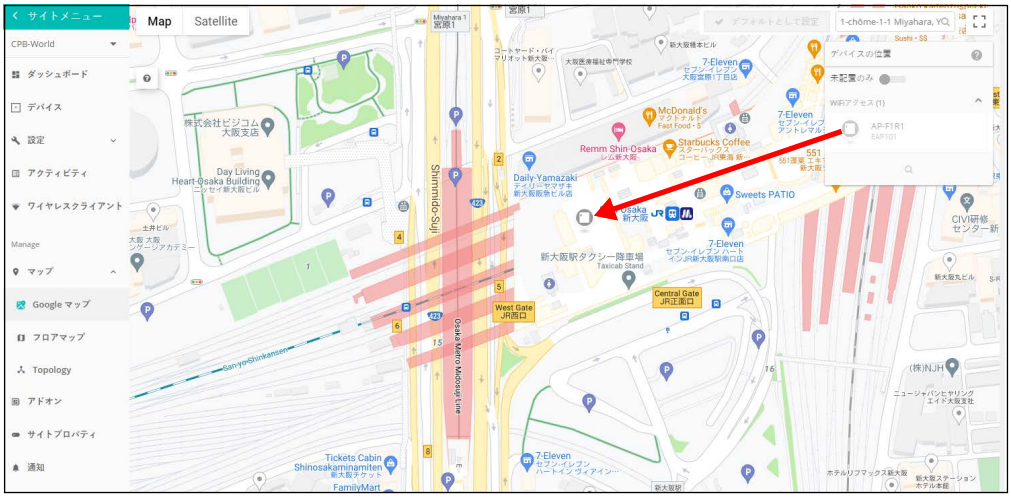
デバイスが無事に追加されると、“ 新しいデバイスを登録する “ ページの上側にメッセージが表示されます。“ マップの管理 “ という青いリンクをクリックして、デバイスをマップに加えてください。

図 90: デバイスが無事に追加されたことを知らせるメッセージ

マップにデバイスを載せる

Google マップページ上に、マウスのクリックアンドドラッグ機能を使って、デバイスを追加できます。

図 91: マップにデバイスの位置を追加する



フロアマップを設定する

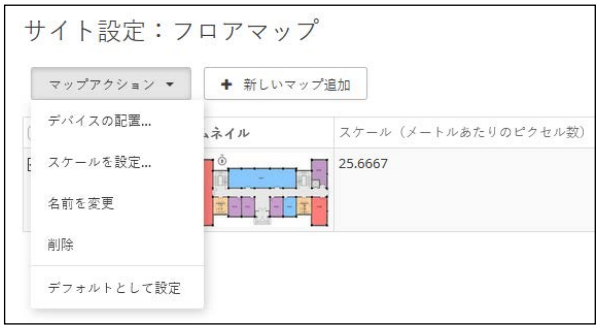
フロアマップはそれぞれの AP の位置とカバーしているエリアを示唆するサイトのグラフィックビューを添えてくれます。建物の中での AP の位置とクライアントがいる場所を知りたい時に使用すると便利です。

新しいマップを追加する“ をクリックすると、フロアプランを作る際に役立つ、カスタマイズされたフロアのイメージマップをアップロードできます。

図 92: 新しいフロアマップを追加する

アクションアイコンまたはプルダウンメニューにある“ デバイスを設置する“ 機能を使用して、フロアイメージマップに無線のデバイスを追加します。

図 93: フロアマップを設定する



ページの右端のリストから AP を引き出してください。まだ設置されていないデバイスが表示されます。まだ設置されていないデバイスを、イメージする位置に設置してください。カーソルでデバイスを指すとデバイスについての詳しい情報が表示されます。“ カバーする場所を表示する “ をクリックしてそのデバイスがカバーするエリアを表示してください。

図 94: デバイスをフロアマップ内に位置付ける

WiFi 構成

サイトメニューから “ 設定 “ の次に “WiFi アクセス “ を選択して無線の設定をしてください。無線の設定はサイトの全ての AP デバイスをはじめ、サイトに追加される全てのデバイスに引き継がれます。

注意：WiFi アクセスの設定は “ サイトレベルの設定を引き継がない “ 設定をしているデバイスには適応しません。

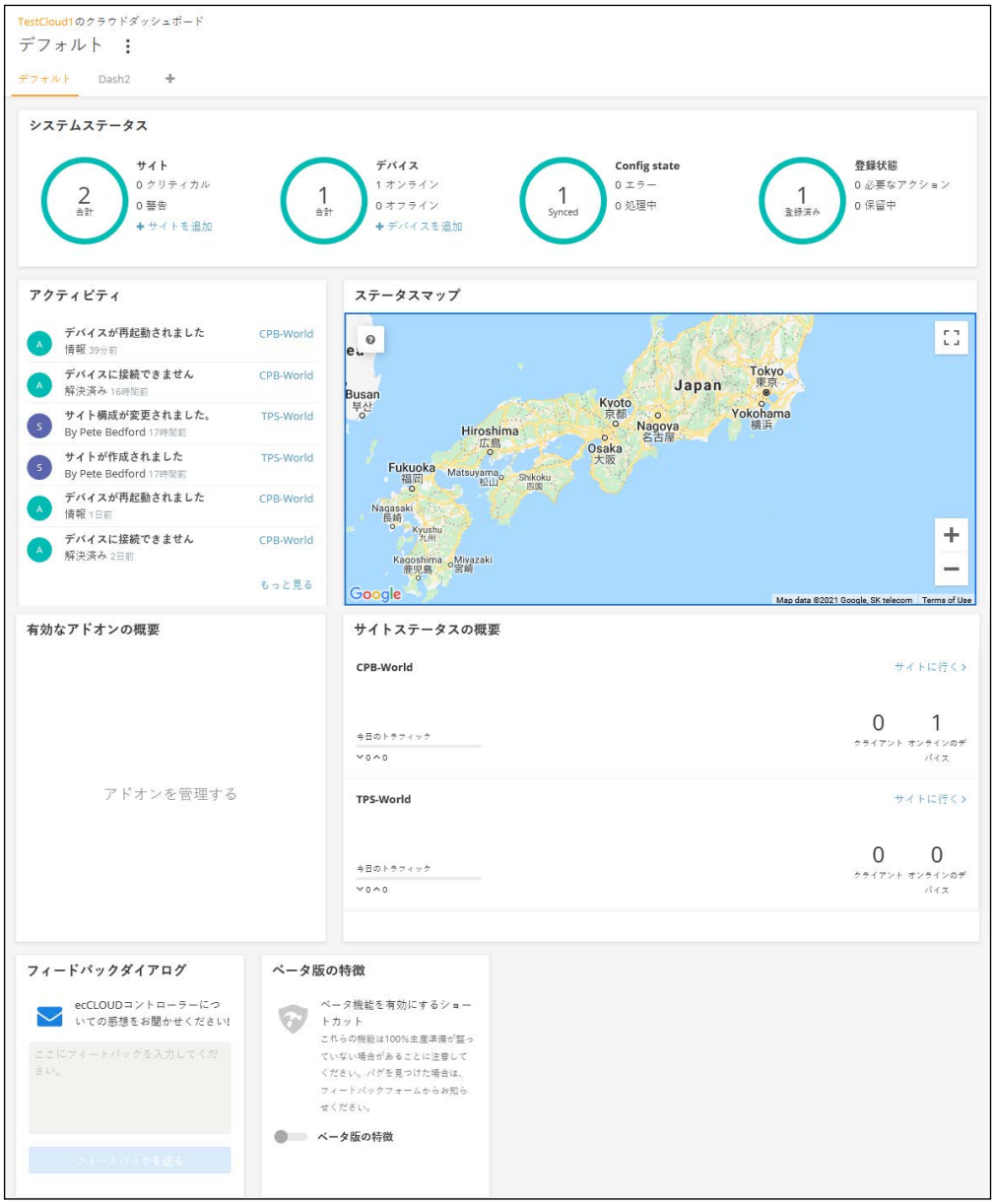
無線のデバイスの設定についてより詳しく知りたい場合は、111 ページの「サイト WiFi 5 構成」をお読みください。

図 95: WiFi5 構成

サイトのダッシュボードの表示

サイトのダッシュボードが提供する情報は以下についてです：設定されたデバイスのステータス、クライアントのアクティビティ、特に使用頻度の高いクライアントについての情報、特に使用頻度の高いアプリケーションについての情報、ゲートウエイインターフェース、サイトマップ、サイトのアクティビティ。

図 96: サイトのダッシュボード



サイトのダッシュボードに表示されるのは以下のアイテムです。

- システムステータス — 4 つの円を使って左側から、デバイスの数量（オンライン、オフラインで分けて表示します）、設定が同期されたデバイスの数量、登録されたデバイスの数量、当日のクライアントのトラフィックを表示します。

注意：カーソルで 4 つの円を指すと、さらに詳しい情報が表示されます。

- アクティビティ - 最近のデバイス、ネットワーク、システムのアラートや、デバイスのアクセス不可、再起動などによるメンテナンスの必要を知らせる通知についての記録をまとめて知らせます。それぞれのエントリーをクリックすると、さらなる情報を得ることができます。
- ステータスマップ - サイトとサイト内のデバイスの地理的な位置を表示します。カーソルでデバイスを指すとさらなる情報が表示されます。
- 有効なアドオンの概要現在使用可能なアドオンをまとめて知らせます。ボックスをクリックすると、サイトのアドオンの管理についての情報を得ることができます。
- クライアントから特に頻繁に使用された AP- 特定のクライアントが特に頻繁に使用したネットワークのアクティビティ（ダウンロードやアップロードなどのトラフィック量など）を表示します。AP をクリックしてダッシュボードが表示するビューをご覧ください。下の部分をクリックすると、10 分、1 時間、1 日、1 週間内の情報を閲覧できます。
- ラフィック量が特に多かったクライアント - 例えば過去 10 分間でダウンロードやアップロードのトラフィック量が多かったなど、特にネットワークの使用量が多かったクライアントについて表示します。クライアントをクリックするとさらなる情報を得ることができます。
- トラフィック量が特に多かった AP- このグラフは特にダウンロードやアップロードのトラフィック量が多かったなど、ネットワークアクティビティの量が多かった AP を表示します。下の部分をクリックすると、1 時間、1 日、1 週間、1ヶ月の間の情報を閲覧できます。
- 無線のクライアントの人数 - このグラフは測定ウインドウ内のクラウドに登録したクライアントの人数を表示します。下の部分をクリックすると、1 日、1 週間、1ヶ月間の情報を閲覧できます。

カスタマイズされたサイトのダッシュボード

デフォルトのサイトダッシュボードの、デフォルトタブの隣のプラスサインをクリックすると、必要に応じたダッシュボードを作成できます。

図 97: ダッシュボードをカスタマイズする

新しくカスタマイズしたダッシュボードの名前を入力して送信をクリックしてください。

図 98: カスタマイズされたサイトのダッシュボード

デフォルトダッシュボードタグの隣に、カスタマイズされた新しいダッシュボードの名前のタブが表示されます。ウイジェットを追加する＋“ボタンをクリックして新しいダッシュボードに必要なアイテムを追加してください。

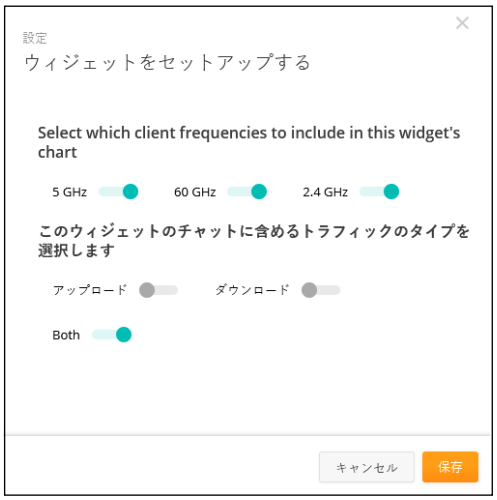
図 99: カスタマイズされたサイトのダッシュボードにウイジェットを追加する

ウイジェットを選択したら、“ 追加 “ ボタンをクリックしてください。

図 100: カスタマイズされたサイトのダッシュボードにウイジェットを選択する

ウイジェットの種類によってはカスタムセットアップコントロールが使用できます。使用できる場合は新しいウインドウで通知されるので、必要なウイジェットの設定を選択し、“ 保存 “ ボタンをクリックしてください。

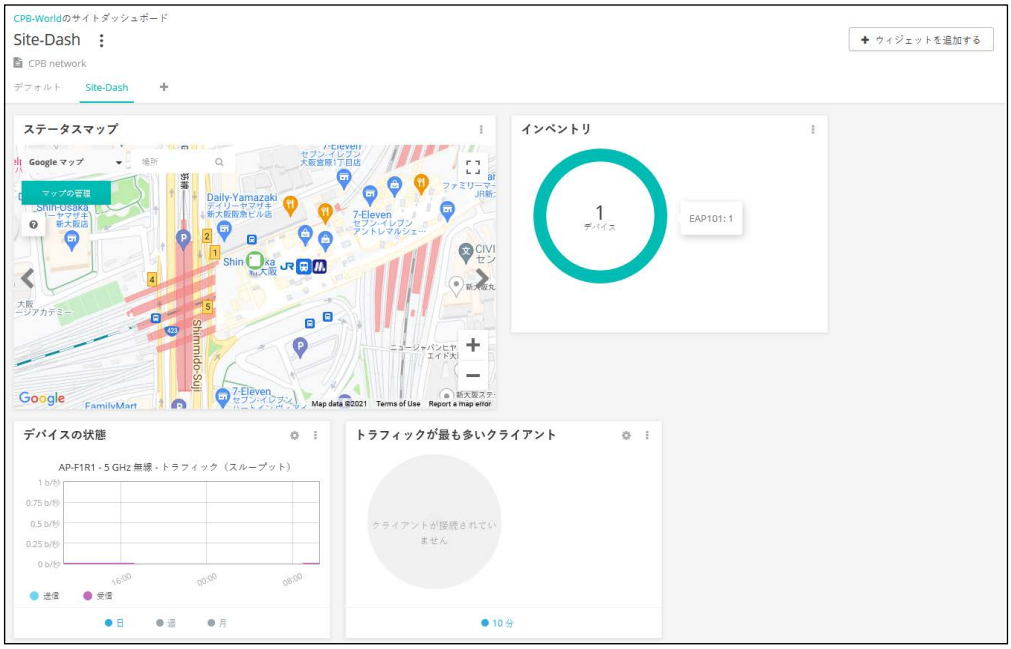
図 101: 新しいサイトのダッシュボードウイジェットをカスタマイズする



選択して設定が完了すると、新しいカスタマイズされたダッシュボードにウイジェットが表示されます。ウイジェットボックスの四方を引っ張ることでボックスのサイズを調整できます。ウイジェットは、右上の 3 つのドットアイコンをクリックすることで名前を変えたり削除できます。また、ギアアイコンをクリックすると設定を変えられます。

“ ウィジェットを追加する “ ボタンをもう一度クリックして、カスタマイズされたダッシュボードにウィジェットを追加します。

図 102: カスタマイズされたサイトのダッシュボード

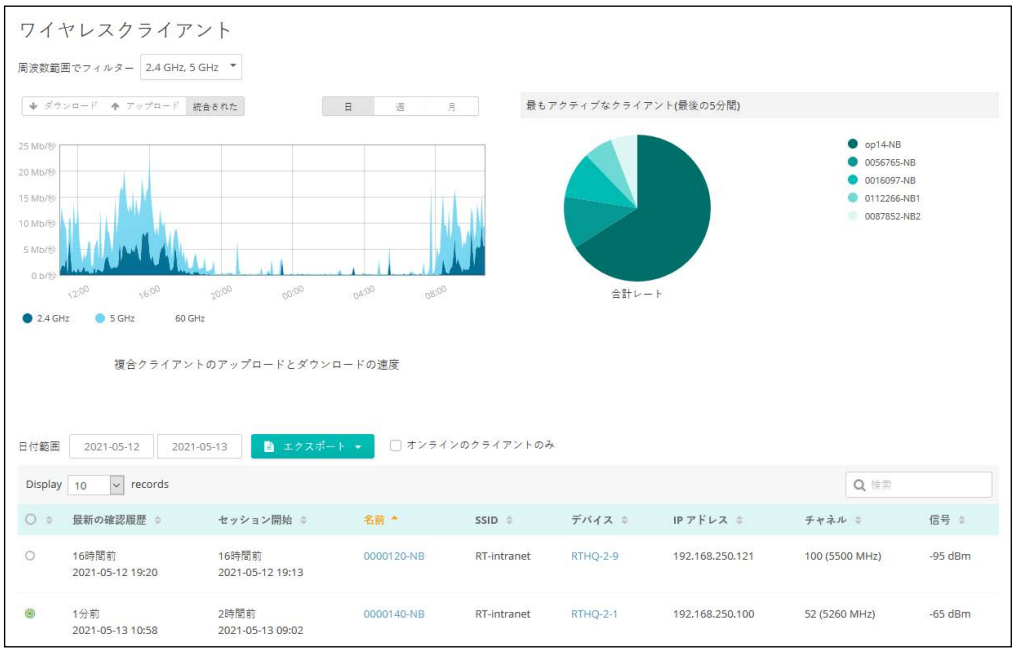


無線 AP とクライアントをモニターする

無線のクライアントのリストページは無線のクライアントのリストだけではなく、クライアントの情報、使用している AP、ネットワークアクティビティを表示します。ネットワークアクティビティは、スループッ ト、最もアクティブなクライアント、およびセッションログの組み合わせとして表示します。

ページ上の無線クライアントのデータは、バンドの選択（2．4ghz、5GHz、60ghz）を基にして、同じようにデータのトラフィックはダウンドード、アップロードなどのディレクションを基にしてフィルターにかけることができます。日数、週、月、または指定した日など、時間帯を基にしてフィルターにかけることもできます。

図 103: 無線クライアントのページ



無線クライアントのページに表示されるのは以下のアイテムです。

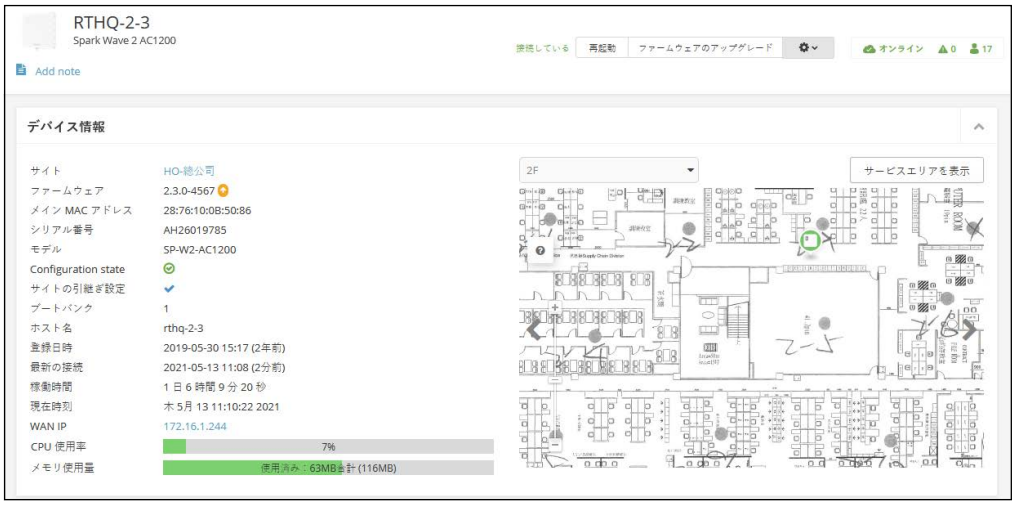
- 使用頻度によってのフィルター —2.4ghz、5GHz、60GHz など、使用頻度によってデータをフィルターにかけます。
- ダウンロード／アップロード／混合 — チャート内に表示したい（ダウンロード、アップロード、混合の）トラフィックスループットを選択してください。
- 日／週／月 — トラフィックスループットの基盤となる期間を選択してください。
- 特に使用量が多かったクライアント — 過去 5 分間で特に使用量（合計量）が多かったクライアントを表示します。円形グラフの中の特定のクライアントをクリックすると、クライアント情報ページが表示されます。
- 日付範囲 — 設定された日付範囲内のセッションログでの無線クライアントデータを表示します。
- エクスポート — 無線クライアントの情報を、メンテナンス枠内の、アクティビティメニューで使用可能な CSV エクセルシートにエクスポートします。
- オンラインクライアントのみ — 現在オンラインであるクライアントにのみ表示されるセッションログです。

セッションログ

セッションログを分類するには、欄のヘディング部分にある上向きまたは下むきの矢印をクリックしてください。

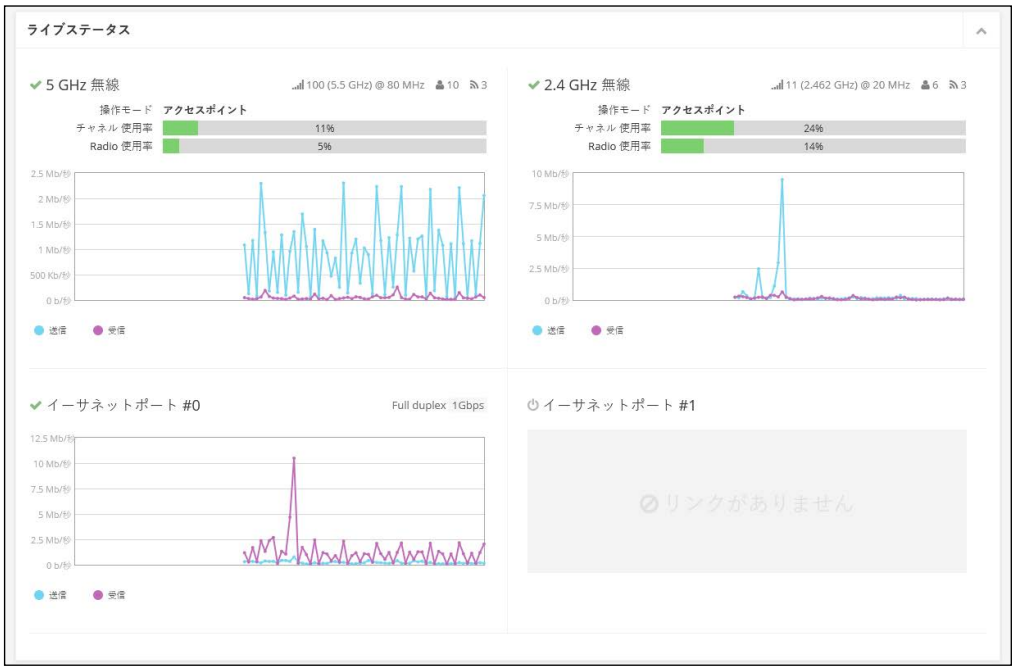
デバイス欄にあるデバイスの名前（どれでもいい）をクリックしてデバイスの情報ページを表示すると、特定の AP の詳細を閲覧できます。デバイスの情報ページの最初のセクションは、位置を示すマップを含めた AP の詳細を表示します。

図 104: 無線 AP の情報



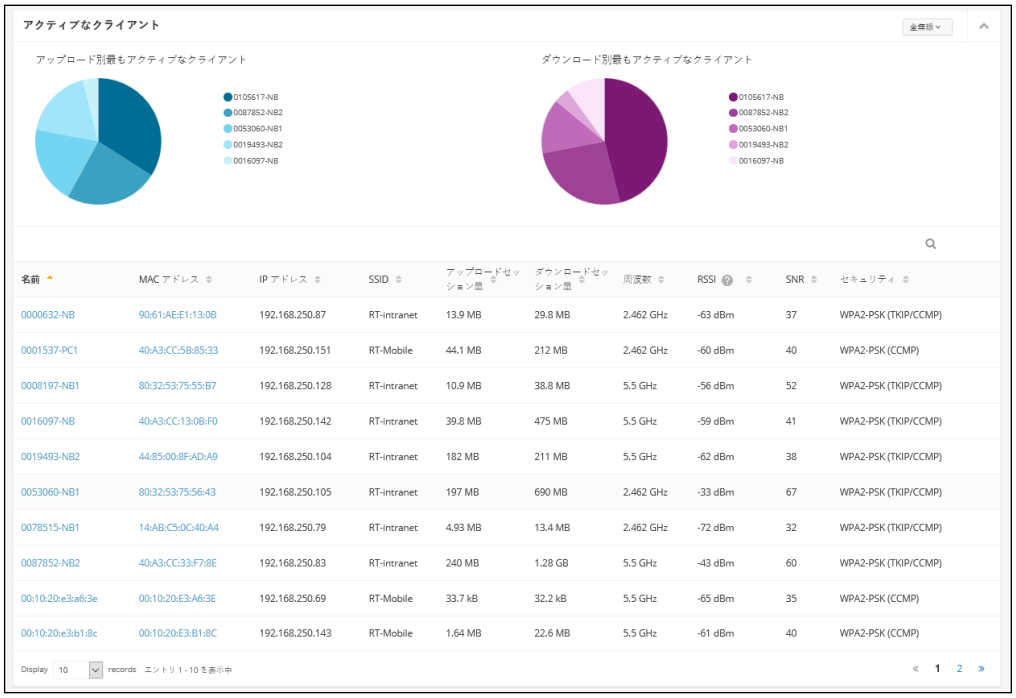
デバイスの情報ページの二つ目のセクションは、AP のレートとイーサネットインターフェースについてのスループットと利用のデータを説明します。

図 105: 無線 AP ライブステータス



デバイスの情報ページの三つ目のセクションは、AP を使用する無線クライアントの詳細を表示します。

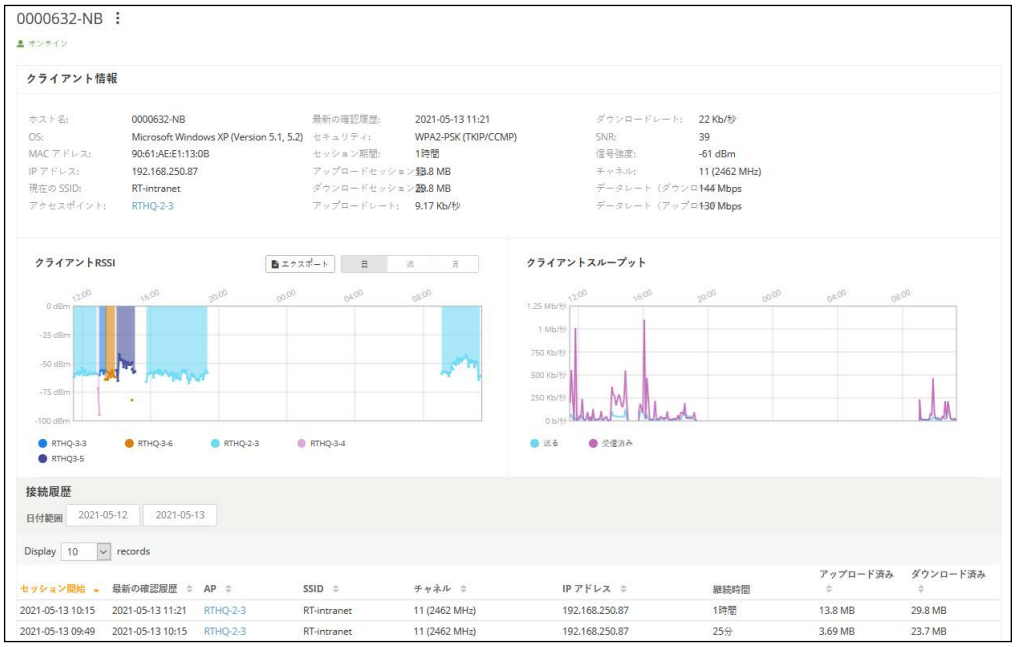
図 106: を頻繁に使用する無線クライアント



無線クライアントのセッションログ、または AP のアクティブクライアントログに入り、クライアントの名前（誰でもいい）をクリックしてクライアントの情報ページに入ると、特定のクライアントの詳細を閲覧できます。

クライアントの情報ページでは、クライアントについての詳細、シグナルの強弱、スループットデータ、クライアントの接続記録のリストを閲覧できます。

図 107: クライアントの情報ページ



クライアントの名前を変えるためには、クライアントの情報ページに入り、ページトップのクライアントの名前の隣にある 3 つのドットアイコンをクリックしてください。

図 108: 無線クライアントの名前を変える

クライアントの名前を元の状態にリセットする場合は、改名のダイアログボックスをブランクにしたまま、送信ボタンをクリックしてください。

メンテナンスタスクのスケジュールを立てる

サイトメニューのデバイスをクリックしてから、無線（または異なるデバイスの種類）をクリックしてください。“ 自分のデバイスを管理する “ ページが表示されます。このページを使用すると、一括再起動やファームウェアのアップデートを管理できます。

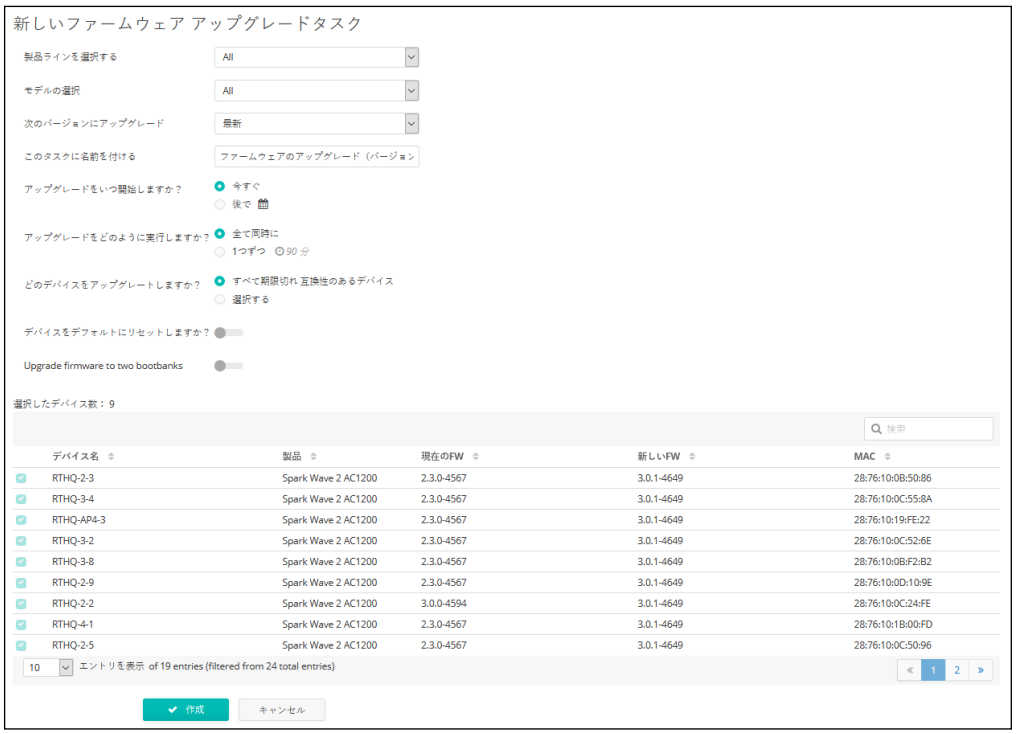
図 109: メンテナンスタスクの管理

ファームウエアをアップグレードする

ファームウエアのアップグレードボタンをクリックして新しいファームウエアのアップグレードタスクページを開いてください。

特定のファームウェアをアップグレードする場合は、ファームウェアのプロダクトライン、モデル番号を選択してください。全てをアップグレードする場合は、“ 全てのままの状態にしてください。いつアップグレードを開始するか、どのデバイスをアップグレードするかを選択できます。設定が完了したら、そのタスクに名前をつけて、作成をクリックしてくださ い。

図 110: 新しいファームウエアアップグレードタスクのページ



一括再起動

一括再起動の管理ボタンをクリックして一括再起動ページを表示してください。このページを使用すると、サイトの全てのデバイスを一斉に、または交代制で再起動できます。特定の機関や日数ごとに再起動させる設定も行えます。

交代制の再起動とは、デバイスが同時にではなく、一つずつ再起動することです。一つのデバイスの再起動が時間切れになると、その後に続くはずであったデバイスの再起動はキャンセルされます。

図 111: 一括再起動を管理するページ

サイトの通知

サイトメニューの“通知“をクリックして選択したサイトの通知の設定を行います。サイト内で送られるメールやスラック通知の送信の設定をします。

注意：スラックアドオンがサイトで使用可能でない場合は、もし“スラックを知らせる“が ON 担っていたとしても、スラックアカウントでの通知を受け取ることはできません。クラウドやサイトメニューから“アドオン“を選択して、スラックアドオンをインストールしてください。詳細については 73 ページの「アドオン」をお読みください。

個人のアラートの送信については、通知の設定ページのトグルスイッチを使用して設定できます。もし“メールを送る“や“スラックを知らせる“が設定されていても、アラートが使用できない設定であれば、通知を送信できません。

図 112: サイトの通知の設定

通知の設定ページでは以下のアイテムが表示されます。

- 言語 — アラートメールで使用される言語
- メールでの連絡先 — デバイスがオフラインになったり、なんだかのアクションが必要になった場合にアラートが送信されるメールアドレスです。複数のアドレスを入力する場合には、間にスペースを開けてください。

  “ メールでの連絡先 “ を入力しない場合は、アラートを “ メールを受け取る “ 設定にしていても通知を受け取ることはできないので注意してください。
- タイムゾーン — アラートに関するメールを送信する際に考慮されるタイムゾーンです。

アラート

- デバイスに接続できません — このアラートは、一つ以上のデバイスが接続できない場合に送信されます。
- プロセスの遅れ — デバイスに接続ができない（またはデバイスがオフラインである）場合のアラートは、一つ以上のデバイスが設定された時間帯内にクラウドと接続できない場合に送信されます。サイト一帯が停電になった場合、システムが全てのオフラインまたは接続できないデバイスについて一通のアラートメールを送信します。（デフォルトでは 8 分間の遅れが通知の対象となります）。
- デバイスの設定が失敗しました — このアラートは、一つ以上のデバイス設定のアップデートに失敗した場合に送信されます。

- デバイスがアクションを必要としています — このアラートは、デバイスの登録に関する問題を使用者に知らせる必要がある場合に送信されます。
- デバイスが再登録されました — このアラートは、デバイスがクラウドコントローラに自動的に再登録した場合に送信されます。
- デバイスの再起動 — このアラートは、一つ以上のデバイスが再起動した場合に送信されます。
- Metrolinq 60GHz のリンクがダウンしました — このアラートは、Metrolinq の 60GHz リンクがダウンしてしまい、もし可能であれば 5GHz フェールオーバーが起動した場合に送信されます。
- 時間が同期していません — このアラートは、デバイスに設定された時間がクラウドと同期していない場合に送信されます。
- チャネルが変わりました — このアラートは、DFS のイベントやその他の理由で、一つ以上のデバイスの無線のチャネルが変わった場合に送信されます。
- ストリームのエラーです — このアラートは、一つ以上のデバイスがオーディオストリームの再生に失敗した場合に送信されます。
- メンテナンスタスクの失敗 — このアラートは、一つ以上のデバイスで予定されていたメンテナンスタスクが失敗した場合に送信されます。
- ファイルの同期化の失敗 — このアラートは、一つ以上のデバイスのファイルにおいて、例えばホットスポットロゴなどのファイルの同期化が失敗した場合に送信されます。
- ファームウエアがダウングレードされました。— このアラートは、ファームウエアがダウングレードされたまたはブートバンク（Bootbank）が失敗した場合に送信されます。
- ファームウエアがアップグレードされました — 装置の UI によってアップグレードされた場合のみ通知されます。クラウドのアップグレードはタスクとして登録されています。

メンテナンスタスク

- 設定を変える — クラウドが、一つ以上のデバイスの設定を変えた場合に通知されます。
- 設定を受け取りました — デバイスがクラウドに設定を伝達した場合に通知されます。
- ファームウエアがアップグレードしました — クラウドが一つ以上のデバイスのファームウエアをアップグレードした場合に通知されます。

- ファームウエアが自動でアップグレードしました — クラウドが自動的にデバイスのファームウェアをアップグレードした場合に通知されます。
- ローリングファームウエアがアップグレードしました — クラウドがデバイスのローリングファームウエアをアップグレードした場合に通知されます。
- トラブルシューティング — デバイスがクラウドを通して要請しているトラブルシューティングファイルが使用可能になった際に通知されます。
- パケットキャプチャー — デバイスがクラウドを通して要請しているパケットキャプチャーが使用可能になった際に通知します。
- レポート — デバイスがクラウドを通して要請しているレポートが使用可能になった場合に通知されます。
- 再起動 — クラウドが一つ以上のデバイスを再起動させた際に通知されます。

4 サイト WiFi 5 構成

この章では、WiFi 5 アクセスポイントの設定について説明します。次のセクションが含まれます。

無線 SSID の設定

サイトメニューから “ 設定 “、続いて “WiFi5“ を開き、サイト内の全ての Edgecore　WiFi5 アクセスポイントに適応する設定のオプションを表示してください。

Edgecore WiFi アクセスポイントは数種類の無線モード（802.11a/a+n/ac+a+n(5GHz) または 802.11b+g/b+g+n(2.4GHz)）に適応します。使用できるモードはアクセスポイントのモデルによって異なります。デュアルバンドアクセスポイントは 2.4GHz と 5GHz で同時に操作できるのでご注意ください。

それぞれの無線は 8 つのサービスセット識別子（SSID）、またはバーチャルアクセスポイント（VAP）インターフェースに適応しています。一つ一つの VAP は、独立したアクセスポイントとして機能し、それぞれ個別の SSID とセキュリティの設定を行います。ほとんどの無線信号パラメーターは全ての VAP インターフェースに対応しています。しかし、特定の VAP に対してのトラフィックはユーザグループやアプリケーションのトラフィックの関係で届かないかもしれません。Edgecore の AP デバイスは一台の無線ごとに、最多で 128 人の SSID インターフェースを利用する無線クライアントに対応します。

図 113: サイト WiFi5 構成

WiFi5 アクセス設定ページの無線 SSID タブが詳細するのは以下のアイテムです。

- グローバル設定 — 全ての SSID インターフェースに対応する設定。

- 自動的にブロードキャストが無効化する—WiFi デバイスがクラウドに接続できない場合は、自動的に SSID ブロードキャストが使用できなくなります。

- SSID リスト — サイトの WiFi デバイスのために設定された SSID インターフェースのリストです。もし特別な設定がされていない限り、それぞれの SSID は 2．4GHz と 5GHz のどちらにもに対応します。最多で 8 つの SSID を設定できます。“SSID を追加する “ をクリックして SSID のインターフェースを作ってください。

- 無線スケジューリング— AP 無線をON にしたりOFF にしたりするために設定されたスケジュールのリストです。このスケージュールは 2.4GHz と 5GHz のどちらの AP にも対応します。“ スケジュールを追加する “ をクリックして無線のスケジュールを作成してください。

SSID を追加する

WiFi アクセスの設定ページにある SSID の追加ボタンをクリックして、下の図に示されているように SSID、ネットワーク、セキュリティの設定を表示してください。

図 114: 無線設定

SSID の追加ページでは以下のアイテムが表示されます。

一般設定

- SSID を使用できるようにする —SSID のインターフェースを、使用可能／不可能にします。
- SSID—VAP インターフェースが提供する基本サービスの名前です。アクセスポイントを使用してネットワークに接続したいクライアントは、アク

セスポイントの VAP インターフェースと同じく SSID を設定しなければいけません。（ネットワーク名は 32 文字まで）。

- ブロードキャスト SSID -SSID は規則正しい間隔で放送を行うので、コネクションを探す無線ステーションと比較的簡単に接続できます。そのため、無線クライアントは自由に無線 LAN を楽しむことができます。この特質を利用されると自宅のネット ワークへのハッキングの恐れもあります。SSID は暗号化されていないので、AP を通して SSID から放送されるメッセージを受信する無線 LAN をスキャンすることは簡単です。（デフォルトは ON の状態です）。

- クライアントの分離 - この設定を有効にすると、無線クライアントは LAN と通信できます。この通信が利用可能な場合は、インターネットに到達できますが、相互に通信できません。（デフォルトでは OFF の状態です）。

- マルチキャストトラフィックの転送をブロックする - マルチキャストトラフィックを、SSID に接続している無線クライアントに転送することを停止します。（デフォルトでは OFF の状態です）。

- 信号の最小限クライアントの信号の強度（RSSI）が特定の数値と同等またはそれ以上でないと SSID を使用できません。この機能は設定値を -100 にすると使えなくなります。すでに繋がっているクライアントについては定期的に確認します。

  この機能を使うことで、クライアントはより信号の強度が高い（アシステッドローミングとも言う）AP を使用することになります。推奨値は、アクセス ポイントの密度とカバレッジに応じて -70 ～ -80 です。

  RSSI（受信信号強度）を -1 から -100db デシベルで入力してください。数値が 0 に近づくほど強度が高くなります。(デフォルト : -70)

- クライアントの最大限の人数 - 同時に SSID に接続できる、最大限の無線クライアントの人数を設定してください。（デフォルトでは 127 人です。人数の範囲は 0 から 127 人です）。

- マルチキャスト / ブロードキャストレート — マルチキャストおよびブロードキャストパケットによって消費される無線帯域幅に制限をかけることができるようにします。

  - 無線 5 Ghz — オプション: 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M; デフォルト : 6M

  - 無線 2.4 Ghz — オプション : 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M; デフォルト : 5.5M

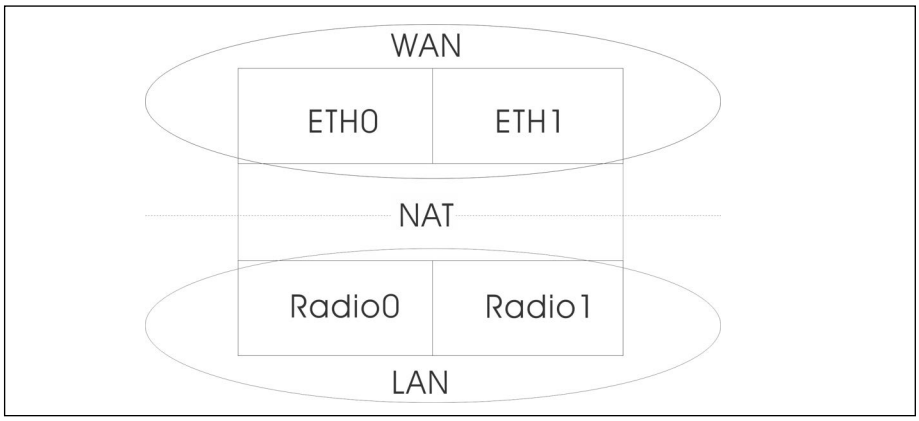
- 無線を起動する - SSID を設置する無線を選択してください。もしデバイスの両方の無線で SSID がアクティブ化されている場合、(SSID がミラーリングされているという意味です) SSID 使用の記録を、どちらかの設定タブから編集してください。この編集は 2.4GHz と 5GHz の記録に反映されます。(デフォルトでは 2.4GHz と 5GHz 両方が有効です)。

ネットワークの設定

- ネットワークモード - 下記の接続方法から指定してください (デフォルトではルートからインターネットです)。
  - ブリッジからインターネット (AP ブリッジモード) - インターフェースを WAN (インターネット) に接続する設定です。

    下の図では、イーサネットポート 1 とイーサネットポート 2 がどちらも WAN に接続されています。このインターフェースから発せられるトラフィックは直接インターネットに送られます。イーサネットや無線のインターフェースはこのように設定できます。

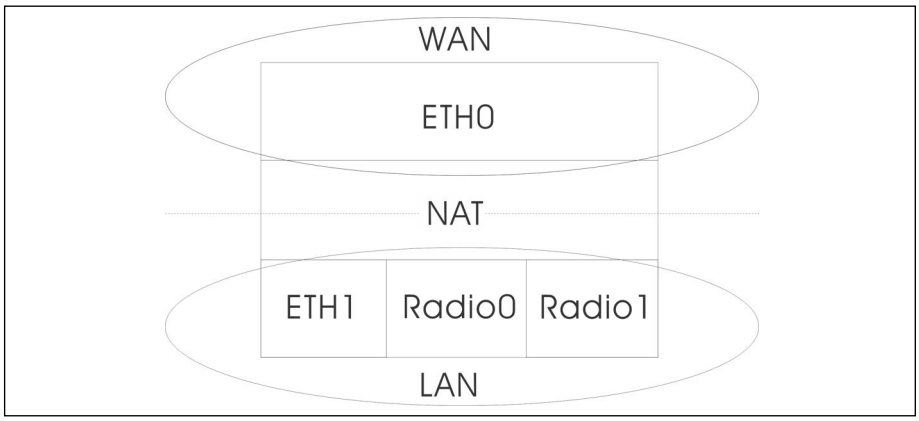
図 115: ブリッジからインターネット



  - ルートからインターネット —インターフェースをLANの一つとして設定します。

    下の図では、イーサネット LAN0 (5GHz 無線) と無線 LAN1 (2.4GHz 無線) はどちらも LAN に含まれています。これらのインターフェースから発せられたトラフィックはイーサネットポート 0 のアクセスポイントを通ってインターネットに接続されます。

図 116: ルートからインターネット



- 経由ルート - 経路制御されるネットワークです。デフォルトは、LAN の設定で表示されているように、“ デフォルトローカルネットワーク “ です。

- ゲストネットワークを追加する - このインターフェースはゲストネットワークのみをサポートします。

- ホットスポットコントロール - このインターフェースはホットスポットサービスのみサポートします。

  - ウォールド・ガーデン - キャプティブポータルによって認証される前にホットスポットユーザがアクセスできるドメインや IP アドレスのリストを CIDR 表記で入力します。このようなドメインは domain.com（ドメインま たはサブドメインに使用できます）または .domain.com（サブドメインにのみ使用できます）のフォーマットを使ってください。

- VLAN タグトラフィック -SSID インターフェースからイーサネットポートに送信されるパケットは、130 ページの「VLAN の設定」に基づいてタグ付けしてください。

注意：ecCLOUD は、AP とスイッチ間の VLAN 同期をサポートします。SSID に VLAN タグが有効になっている場合、設定された VLAN ID は ecCLOUD によって接続されたスイッチポートに自動的に設定されます。これにより、AP からの VLAN タグ付きトラフィックがスイッチポートで受け入れられるようになり、通信断を回避できます。

- アップロード速度の制限 -SSID インターフェースから有線ネットワークに送信されるトラフィックのレートを制限できます。最大値を Kbytes ／秒単位で設定できます。（範囲は 256－10048576kbyte ／秒。デフォルトは OFF の状態です）。

- ダウンロード速度の制限 - 有線ネットワークから SSID インターフェースに送信されるトラフィックのレートを制限できます。最大数値を kbyte/秒単位で設定できます。（範囲は 256－10048576kbyte ／秒です。デフォルトは OFF の状態です）。

セキュリティの設定

- OSEN — OSU Server-Only Authenticated L2 Encryption Network のためにこのオプションを有効にします。
- 方法 — それぞれの SSID にアソシエーションモード、暗号化、認証などの無線セキュリティを設定します。
  - オープン -SSID インターフェースは、設定済みの SSID を含むビーコン信号をブロードキャストします。SSID で " 全て " 設定の無線クライアントは、ビーコンの SSID を読み込むことができ、自動的に接続できます。
  - WPA-PSK — 会社での設置を考えると、WPA を使用するには、RADIUS 認証のサーバーが、ネットワーク上で設定されている必要があります。しかしながら規模の小さなオフィスでネットワークを使用する場合、RADIUS サーバーを保持する資力が不足しているかもしれません。その場合、WPA は事前共有鍵（PSK）でネットワークのアクセスを運転できます。事前共有鍵モードは共通のパスワードを認証に使用します。パスワードは全ての無線クライアントに使用され、手動で入力されます。事前共有鍵モードは、会社用の WPA と同じ TKIP パケット暗号とパスワードの管理方法を使っていますが、規模の小さなネットワークで扱いやすいサービスを提供しています。
    - 暗号化 — データの暗号化は以下のように行われます :
      - AES — AES-CCMP はマルチキャスト暗号として使用されます。AES-CCMP は WPA2 が必要とする、基本の暗号機能です。（これはデフォルトの設定です。）
      - TKIP ＋ AEST — クライアントに使用される暗号化技術はアクセスポイントで知ることができます。
    - キー — WPAは無線クライアントとSSIDインターフェースの間を伝達するデータを暗号化します。WPA は共有のキーを使用しており、（長さが決まった 16 進数、または数字かアルファベットの文字列）、必要があるクライアントに手動で配布されます。

      文字列は 8 から 63 アスキー（ASCII）文字（文字または数字）である必要があります。特異な文字は使えません。

- WPA2-PSK — 共有キーを持っている WPA2 クライアントは認証を受けることができます。

  WPA は、WEP が IEEE802.11i 無線セキュリティスタンダードの認定を保留している間の暫定的な解決策として開発されました。事実上、WPA は 802.11i のサブネットです。WPA2 は現在は承認されている 802.11i スタンダードを含んでおり、WPA にも対応しています。WPA2 は 802.1x と PSK モードで操作でき、TKIP 暗号化技術をサポートしています。

  暗号化技術とキーについての詳細は WPA-PSK を参照してください。

- WPA-EAP — WPA はいくつかの技術を用いて 802.11 無線ネットワークのセキュリティを強化しています。RADIUS サーバーは認証のために使用されており、アカウンティングに使われることもあります。

  暗号化技術については WPA-PSK を参照してください。

  RADIUS の設定

  RADIUS サーバーが、IEEE802.1x ネットワークアクセスコントロールと、WiFi プロテクテッドアクセス（WPA）の無線セキュリティを使用するためには、アクセスポイントを設定しなくてはいけません。

  RADIUS アカウンティングを設定して、アクセスポイントからユーザセッションのアカウンティング情報を得ることもできます。RADIUS アカウンティングは、ネットワーク上でのユーザのアクティビティにおいて、価値のある情報を提供するでしょう。

注意：このマニュアルはお客様がすでに RADIUS サーバーの設定を済ませており、アクセスポイントへ接続できることを前提としています。RADIUS サーバーソフトウエアの設定については当マニュアルでは詳細されていません。RADIUS サーバーソフトウエアについてのマニュアルを参照してください。

- 802.11r — が SSID インターフェースに素早くローミングできます。この機能は 2.2.0+ ファームウェアを使用している AC ウエーブ（Wave）の二つのデバイス（サンスポットウエーブ 2、スパークウエーブ 2）でのみサポートされています。（デフォルトでは使用不可です）。

- モビリティドメイン— AP を操作する802.11r ドメインを識別する AD 番号です。（範囲は 1−65536）。

- 暗号化キー — ファーストローミングのための事前共有鍵です。この鍵は丁度 16 文字であり、含まれる文字は A-Z、a-z,0-9, スペースと ~!@$%^*()_+-=[]{}|:;<>?,./ のみです。

- Transition over the DS — 無線ディストリビューションシステム（WDS）への素早い移動をサポートします。

- MAC NASID リスト — MAC アドレスと NAS ID を行ごとに入力してください。例 : 00:12:34:56:78:9a a00123456789

- RADIUS MAC 認証 — RADIUS 認証を使用します。この設定がされている場合、AP が、クライアントのデバイスの MAC アドレスを、特定の RADIUS サーバーに、認証のために送信します。サーバーはユーザの MAC を認証し、AP に対してダイナミック VLAN ID（設定済みであれば）を返信し、クライアントのデバイ スには異なる情報を送信します。

  注意 : RADIUS サーバーの認証を得るためには、クライアントのデバイスの WiFi MAC に句読点を含まない形でユーザ ID とパス ワードが設定されている必要があります。

  この機能は v1.1.1 ファームウェアの " オープンセキュリティ " や、WEP を除いたその他のセキュリティでサポートされています。

- RADIUS 認証— WPA-EAP や WPA2-EAP セキュリティを使用するためには、RADIUS サーバーが設定される必要があります。

- RADIUS 認証サーバー - 特定の IP アドレスや、RADIUS 認証サーバーのホストネームが必要です。

- RADIUS 認証ポート -RADIUS サーバーが認証のメッセージを送信するために使用するポート番号です。（範囲は 1024-65535 です。デフォルト状態の場合は 1812 です）。

- RADIUS オース（Auth）シークレット - アクセスポイントと RADIUS サーバーの間でメッセージの暗号化のために使われるメッセージです。同じ文字列が RADIUS 認証サーバーで使われていることを確認してください。文字列にスペースを使用しないでください。（最長 255 文字です）。

- NAS ID — SSID インターフェースの RADIUS NAS 認証装置です。クライアントをサーバーに識別するために、IP アドレスの代わりに NAS ID を使用できます。サーバーはクライアントを認証するために、IP アドレスの代わりに NAS ID を使用できます。

- バックアップ RADIUS 認証 - 基本のサーバーが使用不可能になった場合に、予備の RADIUS サーバーとしてバックアップするように設定されています。
- RADIUS アカウンティングを使用 -RADIUS アカウンティングを使って、請求書の発行やセキュリティの目的でアカウントサービスを使用 することを可能にします。
- RADIUS アカウント　サーバー-RADIUS アカウンティングサーバーの IP アドレスやホストネームを明示します。
- RADIUS アカウント ポート - アカウンティングメッセージを送信するために RADIUS サーバーが使用する UDP ポート番号です。（範囲は 1024-65535 です。デフォルト状態の時は 1813 です）。
- RADIUS アカウント　シークレット - アクセスポイントと RADIUS サーバーの間で共有されるメッセージを暗号化するために使われるテキスト文字列です。RADIUS アカウントサーバーで、同じテキスト文字列が使われていることを確認してください。文字列にはスペースを使用しないでください。（最多で 255 文字までです）。

- WPA2-EAP — WPA は、WEP が IEEE802.11i 無線セキュリティスタンダードの認定を保留している間の暫定的な解決策として開発されました。事実上、WPA は 802.11i のサブネットです。WPA2 は現在承認されている 802.11i スタンダードを含んでおり、WPA にも対応しています。WPA2 は 802.1x と PSK モードで操作でき、TKIP 暗号技術をサポートしています。

  RADIUS サーバーは認証だけではなく、下の目的に使用できます。

  暗号化方式の詳細については、WPA-PSK を参照してください。

  RADIUS サーバーの設定については、WPA-EAP を参照してください。

- アクセスの制限リスト — アクセスポイントで設定されたローカルデータベースは、無線クライアントの MAC アドレスを確認することで認証を行います。（デフォルトでは OFF の状態です）。

- ダイナミック認証 - ダイナミック認証拡張機（DAE）を使用すると、RADIUS はすでにネットワークに接続しているクライアントの接続を切断したり、認証を変えたりできます。
  - DAE ポート -DAE メッセージを使用するための DUP ポート番号です。（デフォルトは 3799 です）。
  - DAE クライアント -RADIUS サーバーの IPv4 アドレスです。

- DAE シークレット - アクセスポイントと RADIUS サーバーが DAE メッセージを暗号化するために共有するテキスト文字列です。

無線スケジュールを設定する

無線スケジュールを設定すると、AP 無線を特定の時間に ON または OFF の状態にできます。このスケジュールのルールは、全てのサイト AP の 2.4GHz と 5HGz のインターフェースに伝達されます。“ ADD SCHEDULE“ ボタンをクリックして、無線スケジュールを作成してください。

図 117: 無線スケジュール

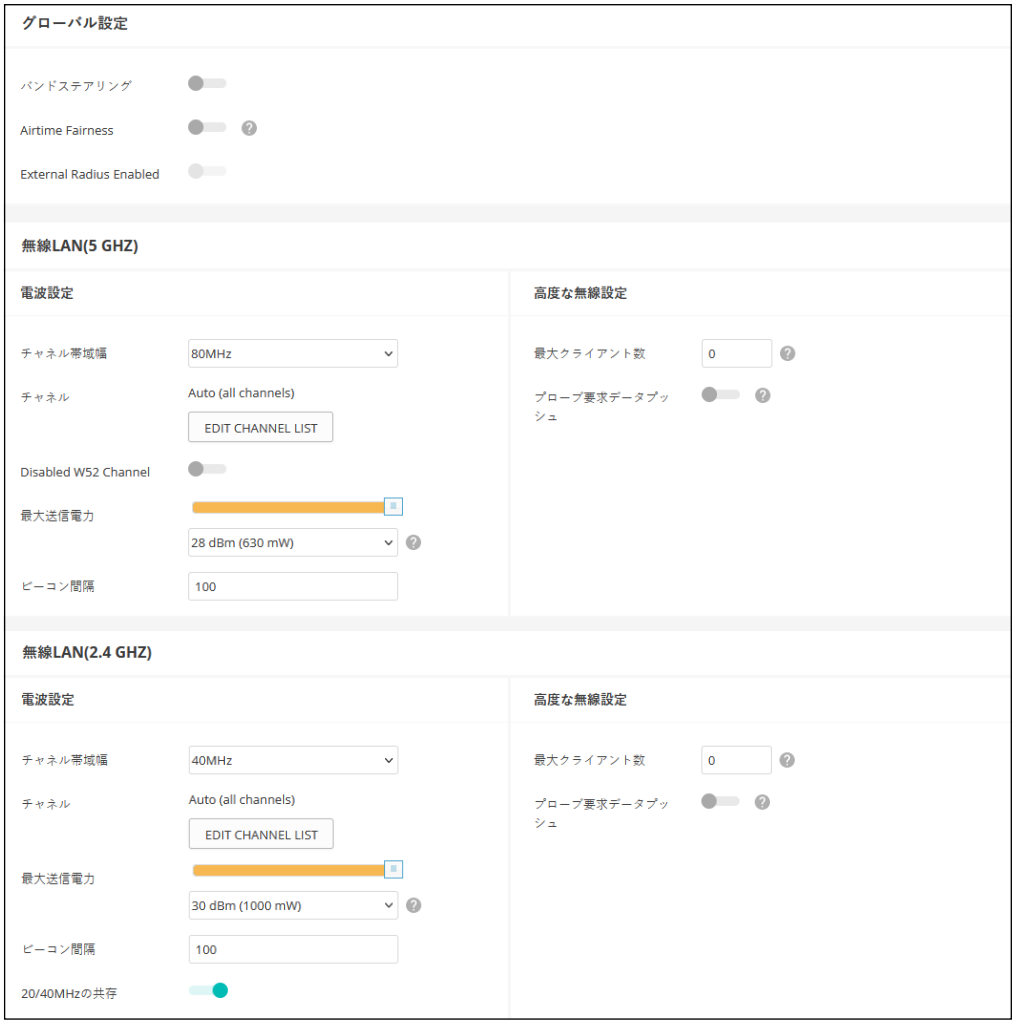
ADD SCHEDULE ページでは以下のアイテムが説明します。

- 使用可能にする - 設定したスケジュールを使用できるようにします。（デフォルトでは使用不可です）。
- 名前 - スケジュールを識別するテキスト文字列です。
- 開始時間 - 無線のスイッチを ON にする時間です。
- 終了時間 - 無線のスイッチを OFF にする時間です。
- 日 —1 週間のうちで、スケジュールが適応される曜日を選択します。

無線設定

5GHz と 2.4GHz の無線設定をするためには、“WiFi アクセスページ “ で、“ 無線設定 “ タブをクリックしてください。この設定は全ての設定された SSID に適応するので注意してください。

図 118: WiFi5 無線設定



無線設定タブは、下記のアイテムを表示します。特に注意事項がなければ、設定のオプションは、5GHz と 2.4GHz どちらの無線にも適応します。

グローバル設定

- バンドステアリング — バンドステアリングを有効にすると、2.4GHz と 5GHz をサポートするクライアントは、まず 5GHz 無線に接続されます。この機能はクライアントを二種類の無線バンドに分散するのに役立ちます。この機能が適応するためには、どちらの無線も SSID に設定されている必要があるので注意してください。

- Airtime Fairness — この機能を有効にすると、無線ネットワーク全体のパフォーマンスが向上します。(デフォルト : 無効)

- External Radius の有効化 — これは AuthPort アドオン機能です（60 ページの「AuthPort アドオン」参照）。AuthPort アドオンを使用する場合、外部 RADIUS サーバーの設定を構成できます。

フィジカル無線設定

- チャネルの帯域幅 — 基本の WiFi チャネル帯域幅は 20MHz ですが、チャネルを結合させると、40MHz または 80MHz チャネルを作り上げることができます。チャネルの帯域幅を広げると、使用できるチャネルの数が減少するので注意してください。

  - 5GHz 無線 —20、40、80MHz か選択できます。（デフォルトは 80MHz です）。

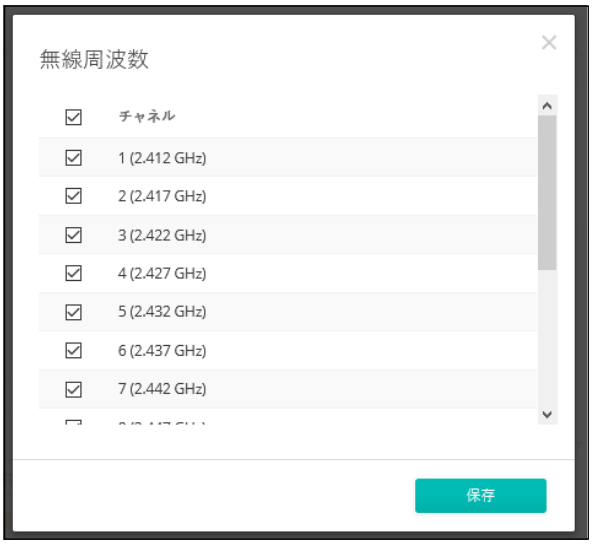
  - 2.4GHz 無線 —20、40MHz から選択できます。（デフォルトは 40MHz です）。

- チャネル — 無線クライアントと連絡をとるためにアクセスポイントが使用する無線チャネルです。使用可能なチャネルは、無線、チャネルの帯域幅、規制している国の設定によって異なります。“ チャネルのリストを編集する “ ボタンをクリックして、どちらの無線インターフェースでも使用できる特定のチャネルを選択できます。

  自動設定にすると、アクセスポイントが使用可能な無線チャネルを自動的に選択します。

図 119: 5GHz 無線チャネル

図 120: 2.4GHz 無線チャネル



- Disabled W52 Channel — 5GHz 無線にのみ適用されます。この機能は、ソフトウェアバージョン v2.3.1 以降の Spark AC Wave2 Mini AP 向けに設計されています。この機能を有効にすると、チャネル 36 ～ 48 が自動的に無効になります。

- マックス TX パワー（Max TX パワー）— アクセスポイントから送信される無線信号の最大電力を調整します。送信電力が高いほど、送信範囲が広くなります。電力を調整すると、カバレージエリアとサポートできるクライアントの人数に影響があります。でもそれだけではありません。送信電力の高い信号が、サービスエリアのほかのデバイスの邪魔をしないことも大切です。（設定できる電力の範囲とデフォルトの電力は、AP モデルと規制している国の設定によって異なります）。

- ビーコン間隔 — アクセスポイントから送信されるビーコン信号の間隔です。無線クライアントは、ビーコン信号を使ってアクセスポイントと接続した状態を保っています。ビーコン信号は、電源管理やその他の情報を含んでいます。（範囲は 100−1024TUs で す。デフォルトの状態は、100TUs です）。

- 20 ／ 40MHz コエクジスト 20（Coexist20）—2.4GHz 無線にのみ適応します。このオプションを使用すると、802.11n20MHz と 40MHz チャネル帯域幅が同じネットワークで操作できます。（デフォルトでは ON の状態です）。

高度な無線設定

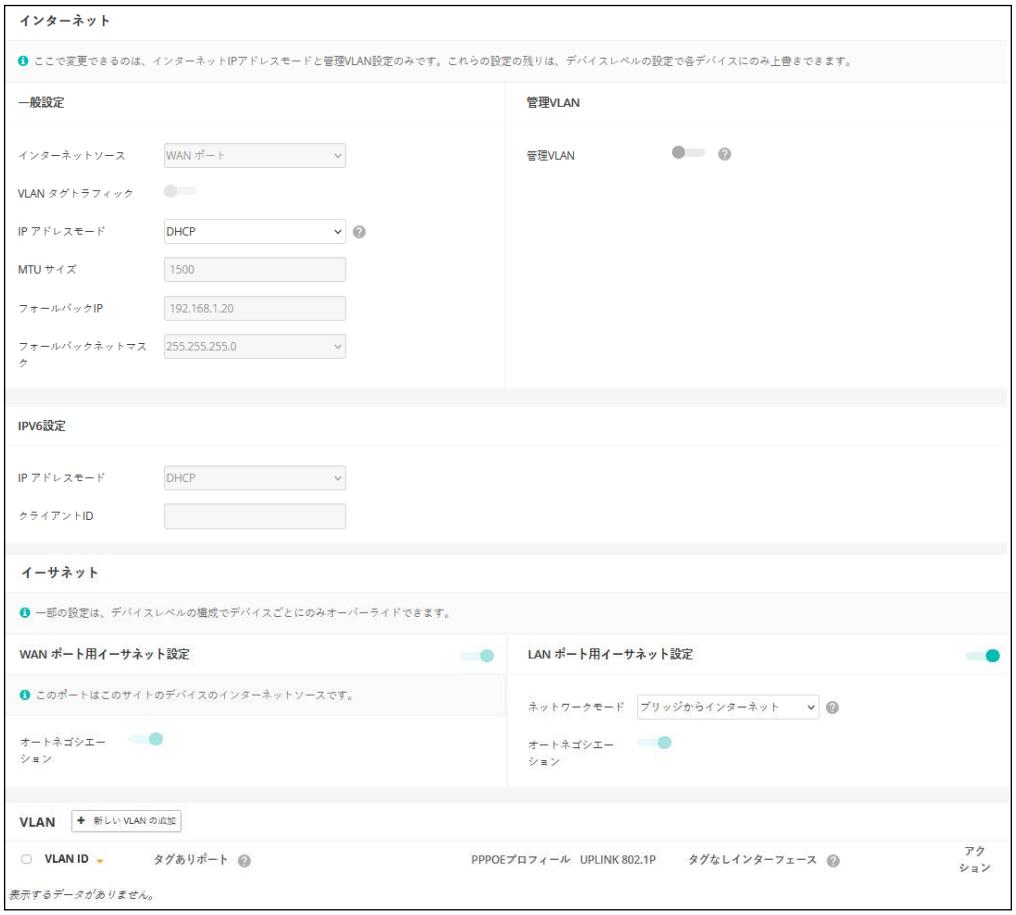
- クライアントの最大限人数 — 無線に接続できる、クライアントの最大限の人数を設定できます。もしこの機能を使いたくなければ、数値を 0 にしてください。（範囲は 0−64 です。デフォルトは 0 の状態です）。

- プローブ要求データプッシュ — クライアントの無線に対してのプローブリクエストデータを受け取ることができるようになります。使用可能になると、クライアントプローブリクエストデータを、無線が JSON フォーマットにし、指定の URL に送信します。

一般的なネットワーキングの設定

“WiFI アクセス “ ページの “ 一般的なネットワーキング “ タブをクリックして、サイトの全てのデバイスの、インターネット、イーサネットポート、VLAN 設定を設定します。デバイスによっては、現在の設定を表示するのみで、設定を変えることができないかもしれません。ここで設定を変えることができないデバイスは、デバイスレベルの設定でのみ書き換えができます。

図 121: 一般的なネットワーキング設定



インターネットの設定

このページでは、インターネットの IP アドレスモードと、管理 VLAN の設定のみ変えられます。その他の設定は、固有のデバイスに対して一件ずつ対応しなくてはいけません。デバイスレベルの設定でのみ書き換えられます。

図 122: インターネットの設定

このページでは下記のアイテムを説明します。

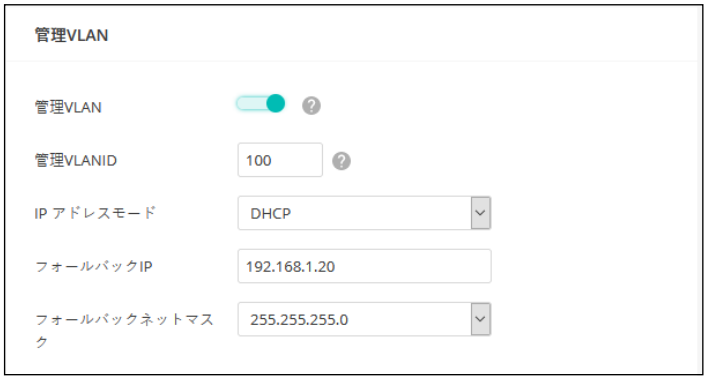
一般設定

- インターネットソース — インターネットにアクセスに使用されるデバイスのインターフェースです。
- VLAN タグ トラフィック — このインターフェースでタグ付けを有効にし、2 から 4094 までのタグ付け ID 値を選択します。
- IPアドレスモード—インターネットアクセスポートにIPアドレスを提供する方法です。(DHCP を使うか、デバイスの設定を使うことができます。デフォルトは DHCP です)。
  - DHCP— インターネットへの接続を可能にします。
  - デバイスの設定を使用する—登録の前にデバイスに対して静的IP を使用することを考えているなら、このオプションを選択して ください。また、静的 IP と DHCP ベースのモードを混合して使用する場合もこれを選択してください。デフォルトでは特別に設定されていない場合は DHCP を使用します。
- MTU サイズ — ネットワークで送信するパケットの、最大限の伝送ユニット（ MTU）を設定したください。
- フォールバック IP— デバイスの IP アドレスにアクセスできない場合は、この IP アドレスが使用されます。

- フォールバックネットマスク — フォールバック IP アドレスと関連するネットワークマスクです。

管理 VLAN の設定

図 123: 管理 VLAN の設定



- 管理 VLAN— このオプションを選択すると、サイトのデバイスの管理 VLAN が使用できるようになります。一度このオプションを使用すると、二度とデバイスに内蔵されたローカルネットワーク（例えば 192.168.2.1）にアクセスができなくなります。特定の VLAN ネットワークを使ってのみデバイスにアクセスが可能になります。もしデバイスの IP が DHCP に設定されている場合は、VLAN ネットワークのサブネット範囲の新しい IP アドレスが必要になります。

- 管理 VLAN ID— 管理 VLAN の ための ID です。

- IIPアドレスモード — 管理VLANを介してデバイスにIPアドレスを提供する方法です。（オプションは DHCP と静的 IP がありま す。デフォルトは DHCP です）。

  - DHCP — 管理 VLAN が使用できるようになります。

  - 静的 IP— サイトのデバイスに管理 VLAN を介してアクセスできるように、静的 IP、サブネットマスク、デフォルトゲートウエイアドレスを設定してください。

- フォールバック IP—DHCP アドレスが使用できない場合に管理 VLAN を介してデバイスと接続するために使用できる IP アド レスです。

- フォールバックネットマスク — フォールバック IP アドレスに関連するネットワークマスクです。

IPV6 設定

図 124: IPv6 設定

この部分には、次の項目が表示されます：

- IP アドレスモード — インターネットアクセスポートに IPv6 アドレスを提供するために使用する方法です。(デフォルト：DHCP、オプション：DHCP、静的 IP)。
  - DHCP — DHCP を構成する場合、クライアント ID を指定する必要があります。
    - クライアント ID — DHCP のクライアント ID を手動で入力します。
  - 静的IP — インターネットアクセスポートに静的IPv6アドレスを設定する場合は、以下の項目を指定する必要があります。
    - IP アドレス — アクセスポイントの IPv6 アドレスを指定します。IPv6 アドレスは、RFC 2373 に従って、8 つのコロンで区切られた 16 ビット 16 進値を使用して構成する必要があります。未定義のフィールドを埋めるために必要な適切な数のゼロを示すために、アドレス内で 1 つのダブルコロンを使用できます。
    - デフォルトゲートウェイ — 要求された宛先アドレスがローカルサブネット上にない場合に使用される、デフォルトゲートウェイの IPv6 アドレス。
    - DNS サーバー — ネットワーク上のドメイン・ネーム・サーバーの IPv6 アドレスです。DNS サーバー は、数値の IPv6 アドレスをドメイン名にマッピングし、IPv6 アドレスの代わりに馴染みのある名前でネットワークホストを識別するために使用できます。ローカルネットワークに DNS サーバーがある場合は、IPv6 アドレスをテキストフィールドに入力してください。

イーサネットの設定

このセクションはサイトの AP のための、基本的なイーサネットの設定について説明します。この設定は、デバイスの設定の、デバイスごとの設定のみ上書きできます。

図 125: イーサネットの設定

このセクションでは下記のアイテムを説明します。

WAN ポート用イーサネット設定

デフォルトでは、WAN ポートインターフェースはインターネットソースとして設定されており、“ このポートは当サイトのデバイスのインターネットソースです “ と表示されています。

もし複数のインターフェースがインターネットに接続されている場合、最後に設定されたインターフェースが使用されます。

- オートネゴシエーション — WAN ポートインターフェースのオートネゴシエーションを使用可能／使用不可能な状態にします。

LAN ポート用のイーサネット設定

- ネットワークモード — ネットワークの接続方法（LAN ポートの使用方法）を表示します。
- オートネゴシエーション — 対応するポートインターフェースで、オートネゴシエーションを使用可能／使用不可能にします。

  1000BASE-T は強制モードをサポートしていません。1000BASE-T と接続するためには、オートネゴシエーションを使用する必要があります。

  オートネゴシエーションが有効になっている場合、アクセスポイントが、宣伝された機能に基づいて、リンクの最適な設定の使用を可能にします。

VLAN の設定

アクセスポイントが VLAN タギングを利用すると、ネットワークリソースへのアクセスを制御し、セキュリティを強化できます。LAN はアクセスポイント間のトラフィック、関連するクライアント、有線ネットワークを分類します。

VLAN（仮想ローカルエリアネットワーク）はデフォルトでは OFF の状態です。ON の状態になると、関連する VAP（仮想アクセスポイント）からイーサネット（Ethernet）ポートに伝達されたパケットに自動的にタグ付けされます。特定の VAP は VLAN のタギングを有効／無効にできるので注意してください。

アクセスポイントの VLAN サポートについては、下記に注意してください。

- イーサネット LAN ポートに VLAN ID が割り当てられている場合、そのポートに入る全てのトラフィックにも同じ VLAN ID がタグ付けされる必要があります。
- アクセスポイントに関連付けられている無線クライアントも、VLAN に割り当てることができます。無線クライアントは、彼らが関連付けられている VAP インターフェースの VLAN に割り当てられます。アクセスポイントは、正確な VLAN ID にタグ付けされたトラフィックの みを、VAP インターフェース上の関連するクライアントに転送します。
- アクセスポイントで VLAN サポートが有効になっている場合、有線ネットワークに渡されるトラフィックに正確な VLANID がタグ付けされます。アクセスポイントのイーサネットポートが VLAN のメンバーとして設定されている場合、有線ネットワークから受信されたトラフィックも同じ VLAN ID にタグ付けされる必要があります。不明な VLAN ID でタグ付けされていたり、タグ付けされていないトラフィックは受信されません。
- VLAN サポートが無効になっている場合、アクセスポイントは有線ネットワークに渡すトラフィックにタグ付けをしません。また、受信したフレームの VLAN タグを無視します。

注意：アクセスポイントで VLAN タグ付けを有効にする前に、アクセスポイントで設定された VLAN ID にタグ付けされた VLAN フレームをサポートするように、ネットワークスイッチポートを設定してください。この設定がなければ、VLAN 機能が有効になった場合にアクセスポイントへの接続ができなくなります。

図 126: VLAN の設定

このセクションでは下記のアイテムを説明します。

- VLAN ID—VLAN に割り当てられた識別子です。（範囲は 2–4094 です）。

- タグありポート —VLAN に割り当てられたイーサネットポートです。オプションとしては WAN ポートと LAN ポートがあります。
- PPPoE プロフィール —VLAN に対して、PPPoE が有効か無効化を確認します。
- Uplink 802.1P — この VLAN のトラフィックの IEEE 802.1p 優先順位設定を示します。
- タグなしインターフェース — “SSID を設定する “ のリンクをクリックして、無線 SSID タブを開きます。次に指定した VLAN のメンバーになるように SSID インターフェースを編集または作成します。（114 ページの「SSID を追加する」を参照してください）。
- アクション — クリックして選択し、すでに設定されている VLAN を編集または消去します。

VLAN を追加する

“ 新しい VLAN の追加 “ ボタンをクリックして VLAN を作成します。

図 127: VLAN を追加する

このセクションでは以下のアイテムを説明します。

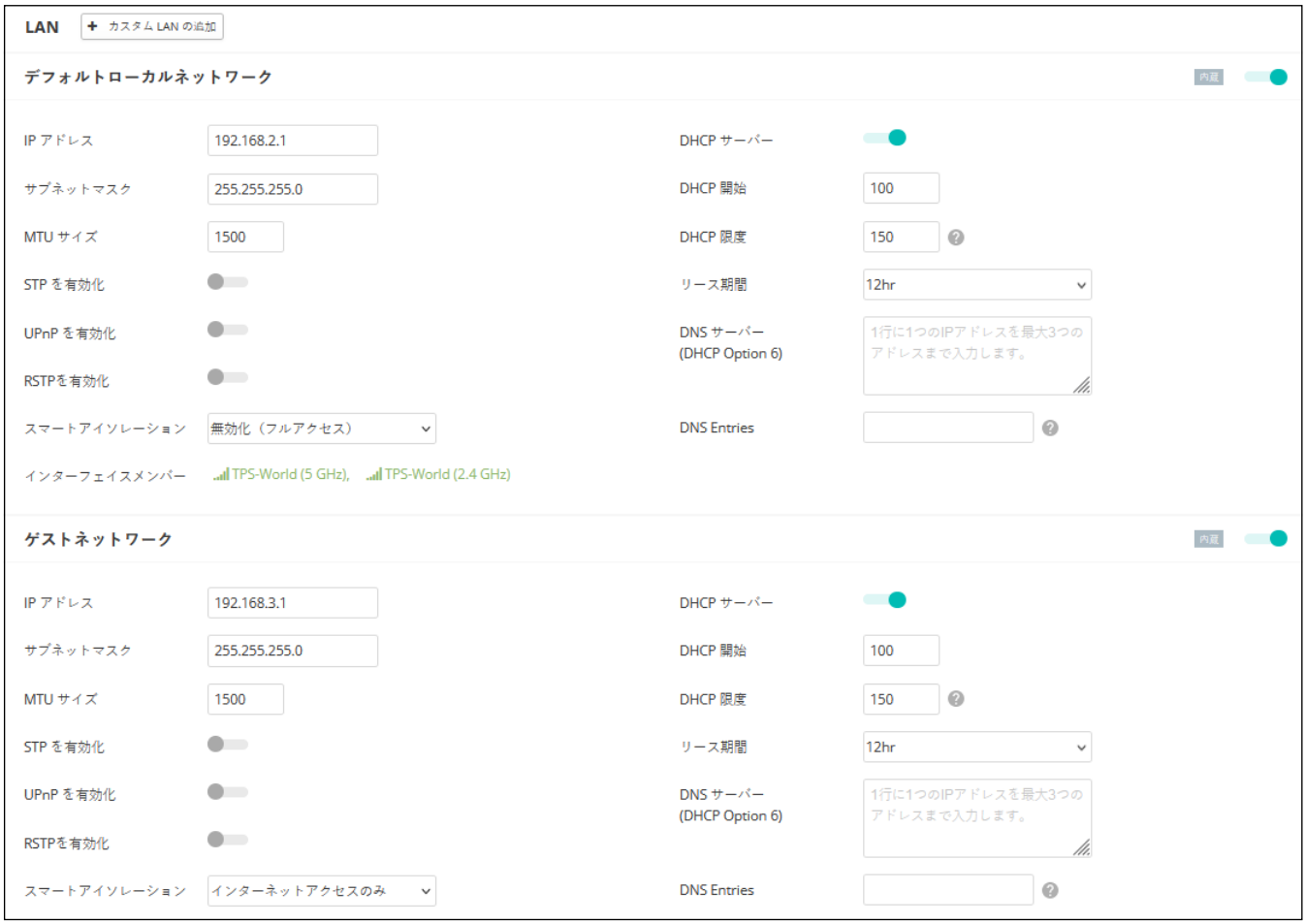
- VLAN ID— 割り当てられる VLAN 識別子です。（範囲は 2–4094 です）。
- ポート —VLAN に割り当てられたイーサネットポートです。オプションには WAN ポートや LAN ポートがあります。

- PPPoE プロフィール — ポイントトゥーポイントオーバーイサーネット（PPPoE）は、サービスプロバイダーとローカルネットワーク間の安全な “ トンネル “ 接続を提供する一般的な WAN プロトコルです。
  - ユーザ名 — サービスプロバイダーとの接続に使用する名前です。
  - パスワード—サービスプロバイダーとの接続に使用するパスワードです。
  - IP アドレス—サービスプロバイダーとの接続に使用する IP アドレスです。
- Uplink 802.1P — この VLAN のトラフィックの IEEE 802.1p 優先度を設定します。優先順位は「Best Effort」（最低）から「Network Control」（最高）までの範囲です。

ローカルネットワーク設定

ローカルネットワークタブは、デフォルトの LAN ネットワーク、ゲストネットワーク、その他のカスタムネットワークの設定を設定します。

図 128: ローカルネットワークの設定



このページは以下のアイテムを説明します。

- このボタンをクリックすると、利用者用にカスタマイズされたネットワークを追加できます。最多で 10 個のカスタマイズされた LAN を作成できます。
- IPアドレス—ローカルネットワークまたはゲストネットワークのIPアドレスを決めてください。有効な IP アドレスはピリオドで区切られた、0–255 の 4 つの 10 新法の数で作成してください。（デフォルトは 192.168.2.1 です）。
- サブネットマスク — ローカルサブネットマスクのことです。（デフォルトでは 255.255.255.0 です）。

- MTU サイズ — このネットワークで送信されるパケットの最大送信単位（MTU）を設定してください。（デフォルトは 1500 です）。
- STP の有効化 — スパニングツリープロトコルメッセージの処理を有効／無効にします。
- UPnP の有効化 — ユニバーサルプラグアンドプレイブロードキャストメッセージを有効／無効にします。
- RSTP の有効化 — ラピッド スパニング ツリー プロトコル メッセージの処理を有効または無効にします。(デフォルト : 無効)
- スマートアイソレーション — ネットワークトラフィックを特定のネットワークで制限できます。
  - 無効（フルアクセス）— トラフィックは分離しません。クライアントはローカル LAN 上のインターネットやその他のデバイスにアクセスできます。もしネットワークに接続するクライアントが信頼できる人物である場合にこのオプションを選択してください。
  - インターネットアクセスのみ—このネットワークからのトラフィックは、インターネットとの間のみ送信／受信できます。このオプションはホットスポットユーザまたはゲストユーザを対象として選択してください。
  - LAN アクセスのみ — このネットワークからのトラフィックは、ローカル LAN のデバイスでのみ使用できます。
  - インターネットのみ (厳密)— このオプションは " インターネットアクセスのみ " の場合と基本は同じですが、さらに制限条件が上乗せされてお り、ユーザは、プライベートネットワーク（192.168.0.0、172.16.0.0、10.0.0.0 など）上のリソースまたはデバイスにアクセスできません。この設定は、AP が " ダブル NAT" であり、ネットワークが AP の上流にあるときに役に立ちます。
- インターフェースメンバー — ローカルエリアネットワークに接続されているインターフェースです。
- DHCP サーバー — このネットワーク上で DHCP を有効／無効にします。（デフォルトは有効の状態です）。
  - DHCP スタート — アドレスプールの最初のアドレスです。（範囲は 1-256 です。デフォルトは xxx100 です）。
  - DHCP 制限 — アドレスプールの中で最大数のアドレスです。（範囲は 1−254 です。デフォルトは 150 です）。

- リースタイム — 割り当てられた IP アドレスが有効である時間です。
- DNSサーバー —最大3つの DNSサーバーIPアドレスをリストアップします。一行につき一つずつ書き出します。

- DNS Entries — Spark AC Wave2 Mini AP にのみ適用されます。クライアントがローカルネットワークから指定されたドメインを通じて Web インターフェースにアクセスすることを許可します。

ファイアーウォールの設定

ファイアーウォールフィルタリングは、侵入によるリスクを減らすために、接続するパラメーターを制限します。ファイアーウォール設定を使用すると、トラフィックを送信元と送信先の IP アドレスとポートに基づいてフィルターにかける際のルールを、順序立ててリストできます。入力パケットは、フィルタールールに基づいて、一つずつ検査されます。パケットがルールと一致すると、設定されたアクションが実施されます。

Allow-Ping はインターネットからの Ping パケットを許可するように前もって設定されています。このルールを有効または無効にすることはできますが、書き換えたり取り消すことはできません。“ ADD RULE “ ボタンをクリックして新しいファイアーウォールルールを追加してください。

図 129: ファイアーウォールの設定

このページには以下のアイテムが表示されています。

- 有効 — 設定されたファイアーウォールを有効にします。
- 名前 — フィルタリングルールの名前を決めてください。(範囲は 1–30 文字です)。

- ソース IP アドレス —CIDR 表記の IPv4 アドレス。IP アドレスの後にスラッシュで、10 進数のネットワークマスクを定義します。
- 送信元ポート — 送信元プロトコルポートです。（範囲は 1–65535 です）。
- 宛先 IP — 送信の宛先となる IPv4 アドレスです。
- ソースポート — 送信の宛先となるプロトコルポートです。（範囲は 1–65535 です）。
- 対象 — 構成されたルールがパケットに一致したときに実行するアクションです。(オプション : Accept、Reject、Drop)
- ファミリー —IPv4 または IPv6 トラフィック、あるいは両方を指定してください。（IPv4、IPv6、全て）
- ソース — ソースとなるインターフェースです。（オプションは全て、デフォルトであるローカルネットワーク、インターネット、ゲストネットワーク、ホットスポットネットワークがあります）。
- プロトコル — パケットのプロトコルタイプを決めてください。（オプションは全て、TCP ＋ UDP、TCP、UDP、ICMP があります）。
- 送信先 — 宛先のインターフェースです。（オプションは全て、デフォルトのローカルネットワーク、インターネット、ホットスポットネットワークです）。

ポートフォーワーディング

ポートフォーワーディングは、インバウンドプロトコルタイプ（TCP ／ UDP）とポートを、“ 内部 “IP アドレスとマッピングするために使用できます。内部（ローカル）IP アドレスは、ネットワークのエッジにあるローカルデバイスに割り当てられた IP アドレスであり、外部 IP アドレスは、AP 内部に割り当てられた IP アドレスです。これにより、リモート ユーザが、単一のパブリック IP アドレスを使用し、ローカルネットワーク上の様々なサーバーにアクセスできます。

パブリック IP アドレスを介してローカルサイトでウエブや FTP などのサービスにアクセスするリモートユーザは、ほかのローカルサーバーの IP アドレスと TCP ／ UDP ポート番号にリダイレクト（マッピング）されます。例えば、プロトコル／外部ポートを TCP ／ 80（HTTP または Web）に設定し、宛先 IP ポートを 192.168.3.9/80 に設定すると、外部ユーザからの全ての HTTP リクエストは、ポート 80 で 192.168.3.9 に転送されます。したがっ て、ISP から提供された外部 IP アドレスを使用するだけで、インターネットユーザはリダイレクト先のローカルアドレスで、必要なサービスにアクセスできるのです。

より一般的な TCP サービスポート番号は、HTTP：80、FTP：21、Telnet：23、POP3：110 があります。

図 130: ポートフォーワーディング

このページは以下のアイテムを説明します。

- 有効 — ポート転送を有効にします。
- 名前 — ユユーザを定義する名前（範囲は 1–30 文字です）。
- プロトコル — ポート転送が適用されるプロトコルタイプを設定してください。（オプションは TCP、UDP、TCO ＋ UDP があります）。
- 外部ポート—インターネットトラフィックの TCP／UDP ポート番号です。（範囲は 1–65535 です）。
- 送信先 IP アドレス — ローカルネットワーク上の宛先 IP アドレスです。
- ソースポート — 送信の宛先プロトコルポートです。（範囲は 1–65535 です）。

ARP インスペクション

ARP Inspection は、Address Resolution Protocol パケットの MAC Address バインディングを検証するセキュリティ機能です。これは、ある種の「中間者」攻撃の基礎となる、無効な MAC-IP アドレスバインディングを持つ ARP トラフィックに対する保護を提供します。これは、すべての ARP リクエストとレスポンスを傍受し、ローカル ARP キャッシュが更新されるか、パケットが適切な宛先に転送される前に、これらのパケットのそれぞれを検証することによって実現されます。無効な ARP パケットはドロップされます。

図 131: ARP インスペクション

このページでは、以下の項目が表示されます：

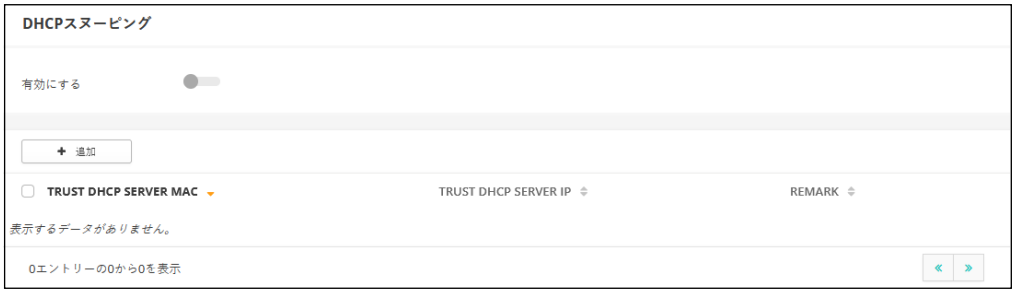
- ARP Inspection — 有効にすると、ARP パケットは ARP スプーフィングに対して検証されます。
- Force DHCP — AP が MAC/IP ペア情報のみを学習することを許可します。AP が DHCP パケットを介して MAC/IP ペア情報のみを学習できるようにします。静的 IP アドレスで設定された機器は、DHCP パケットを送信しないため、DHCP パケットを送信することはありません。DHCP トラフィックは、静的 IP アドレスを持つクライアントは、AP によってブロックされます。その MAC/IP ペアは、静的トラストリストにリストされ、有効になっています。
- Trust List Broadcast — 他の AP が信頼できる MAC/IP ペアを学習して、ARP 要求を発行できるようにします。
- Static Trust List — ARP 要求を発行するために信頼されるデバイスの MAC または MAC/IP ペアを追加します。他のネットワークノードは ARP 要求を送信できますが、その IP が異なる MAC で静的リストに表示されている場合、その ARP 要求はドロップされます。

DHCP スヌーピング

DHCP snooping は、AP が受信した DHCP メッセージの検証およびフィルタリングに使用されます。DHCP snooping が有効な場合、DHCP snooping テーブルに記載されていないデバイスから受信した DHCP メッセージは、ドロップされます。

MAC アドレスと IP アドレスを指定することで、既知の信頼できる DHCP サーバーをテーブルに追加できます。

図 132: DHCP スヌーピング



このページでは、以下の項目が表示されます：

- 有効 — DHCP スヌーピングを有効にします。
- Trust DHCP Server MAC - 既知で信頼できる DHCP の MAC アドレスです。

- Trust DHCP Server IP - 既知の信頼できるDHCPサーバーのIPアドレスです。
- Remark - 設定された DHCP サーバーに関連するコメントです。

ホットスポットの設定

ホットスポットの設定のページは、コーヒーショップ、図書館、病院などでの一般の人々のインターネットアクセスの設定を説明します。特定のアクセス権は、RADIUS サーバーを介し決定できます。

ホットスポットサービスを設定する際には、無線 SSID の設定ページに移動して、SSID インターフェースでの Network Behavior として、“ ホットスポットで制御する “ を選択しなくてはいけません。(112 ページの「無線 SSID の設定」を参照してください)。

一般設定

ホットスポットページの一般設定セクションでは基本的なホットスポットモードを設定できます。

図 133: ホットスポットの一般設定

このセクションは以下のアイテムを説明します。

- ホットスポット有効化—ホットスポットサービスを有効／無効にします。

  以下のホットスポットモードを選択してください。(ホットスポットモードは 1.1.4 以降のファームウェアに対して静的に “ エクスターナルポータル “ として設定されます。この設定を有効に利用するには、1.1.4 以降のファームウェアにアップグレードしてください)。

  - このオプションはホットスポットゲストに、外部でホストされているキャプティブポータルスプラッシュページを表示し、(サービス設定の設定によって異なりますが)、ログインを誘導する場合があります。サードパーティキャプティブポータルサービスプロバイダーにサインアップしている場合は、このオプションを選択してください。

- 認証なし — このオプションは、ホットスポットのゲストに、カスタマイズされた、ローカルホストのキャプティブポータルスプラッシュページを表示します。ゲストはログインすることなくインターネットにアクセスできます。もしオプションである利用規約のテキストを記入した場合、ゲストがインターネットにアクセスする前にこの規約に同意する必要が生じます。

- シンプルなパスワードのみのスプラッシュページ — このオプションでは、ホットスポットゲストに、カスタマイズされたローカルホストのキャプティブポータルのスプラッシュページを表示しますが、ログインしてインターネットにアクセスする際に簡単なパスワードを入力する必要があります。（オプションである）利用規約に記入すると、ゲスト がインターネットにアクセスする前に、この規約に同意する必要が生じます。

- 外部 RADIUS を使用したローカルスプラッシュページ — このオプションでは、カスタマイズされた、ローカルホストのキャプティブポータルスプラッシュページを、ホットスポットゲストに表示できます。しかしゲストは、ログインしてインターネットにアクセスするために、有効な RADIUS ユーザ名とパスワードを入力する必要があります。（オプションである）利用規約のテキストを記入する場合、ゲストがインターネットにアクセスするために、この規約に同意する必要が生じます。

- 外部 RADIUS 付きリモートスプラッシュページ - これは AuthPort アドオン機能です（74 ページの「AuthPort アドオンを使用する」を参照）。ホットスポットは外部スプラッシュページにリダイレクトされ、外部 RADIUS サーバーで認証されます。

- スマートアイソレーション — ネットワークトラフィックが特定のネットワークに対して制限される設定です。

  - 無効（フルアクセス）— トラフィックの分離はありません。クライアントは、ローカル LAN 上のインターネットやその他のデバイスにアクセスできます。ネットワークに接続するゲストが信頼できる人物である場合の選択肢です。

  - インターネットアクセスのみ — このネットワークからのトラフィックは、インターネットとの間でのみ通信できます。ホットスポットユーザやゲストネットワークに接続しているユーザのためのオプションです。

  - LAN アクセスのみ — このネットワークからのトラフィックは、ローカル LAN デバイスにのみ通信できます。

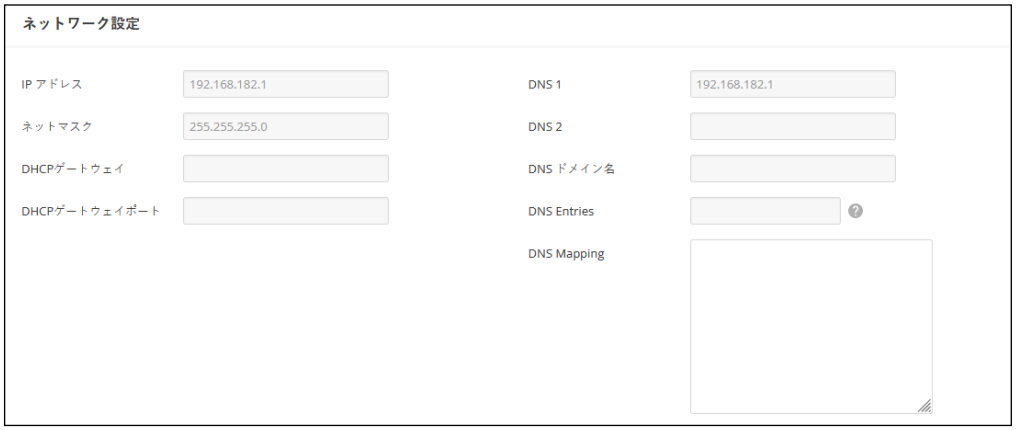
  - インターネットのみ（厳密）—“ インターネットアクセスのみ “ と基本的に同じですが、さらに条件が上乗せされます。ユーザは、プライベートネットワーク（192.168.0.0、172.16.0.0、10.0.0.0 など）上

のリソースまたはデバイスにアクセスできません。これは AP が “ ダブル NAT“ であり、AP のゲートウエイの上流のネットワークが、別のプライベートネットワークである場合に役に立ちます。

ネットワークの設定

ホットスポットページのネットワークの設定セクションでは、ホットスポットサービスのためのローカルネットワークの設定を説明します。

図 134: ホットスポットネットワークの設定



このセクションは以下のアイテムを説明します。

- IP アドレス — ホットスポットの IP アドレスを決めてください。有効な IPv4 アドレスは、ピリオドで区切られた 0–255 の 4 つの 10 進法数で構成されます。（デフォルトは 192.168.182.1 です）。
- ネットマスク — 関連付けられた IP サブネットのネットワークマスクです。このマスクは、特定のサブネットへの通信に使われるホストアドレスビットを識別します。
- DHCP ゲートウエイ — DHCP サーバーにアクセスするために使用するゲートウエイです。
- DHCP ゲートウエイポート — DHCP サーバーへのアクセスに使用される UDP ／ TCP ポートです。
- DNS1 — ネットワーク上のプライマリードメインネームサーバーの IP アドレスです。DNS は IP アドレスの数値をドメイン名にマッピングするので、IP アドレスの代わりに、使い慣れた名前でネットワークホストを識別できるようになります。
- DNS2 — DHCP クライアントが利用できる補助的な DNS サーバーです。
- DNS ドメイン名 — ドメインネームシステムを介して、不完全なホスト名を解決するために使用されるドメイン名です。

- DNS Entries — Spark AC Wave2 Mini AP にのみ適用されます。クライアントがローカルネットワークから指定されたドメインを通じて Web インターフェースにアクセスすることを許可します。
- DNS Mapping — ユーザが指定した IP とドメインに対する DNS マッピングを設定します。

DHCP サーバー

ホットスポットページの DHCP サーバーセクションでは、ホットスポットサービスの DHCP アドレスプールを設定します。

図 135: ホットスポット DHCP サーバーの設定

このセクションでは以下のアイテムを説明します。

- スタート — アドレスプール内の（最後の数値フィールドの）最初の番号です。（範囲は 1−254 です。デフォルトは 10 です）。
- DHCP リミット — アドレスプール内の（最後の数値フィールドの）終了番号です。（範囲は 1−245 です。デフォルトは 245 です）。
- リースタイム —IPアドレスがDHCPクライアントに割り当てられている時間です。（範囲は 600−43200 秒です。デフォルトは 3600 秒です）。

RADIUS サーバー

ホットスポットページの RADIUS サーバーセクションは、ホットスポットサービスの RADIUS サーバーを設定します。

図 136: ホットスポット RADIUS サーバーの設定

このセクションでは以下のアイテムを説明します。

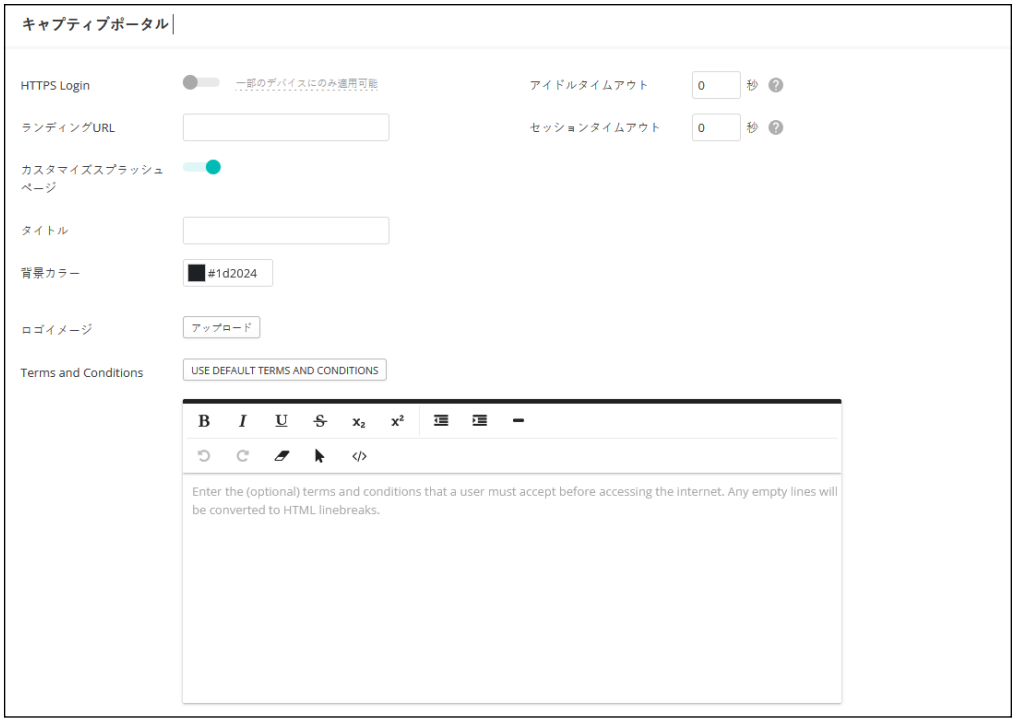
- RADIUS 認証の有効化 — キャプティブポータルにアクセスしようとしているクライアントの RADIUS 認証を有効にします。
- RADIUS サーバーアドレス — プライマリーRADIUS サーバーの IP アドレスまたはホスト名です。
- バックアップRADIUSサーバーアドレス —補助的なRADIUSサーバーのIPアドレスまたはホスト名です。
- RADIUSサーバー共有シークレット—アクセスポイントとRADIUSサーバー間のメッセージを暗号化するために使用される共有テキスト文字列です。RADIUS サーバーで同じ文字列が明示されていることを確認してください。文字列に空白を使用しないでください。(範囲は 1−255 文字です)。
- RADIUS サーバーauth ポート — 認証メッセージに使用される RADIUS サーバーの UDP ポートです。(範囲は 1−65535 です。デフォルトは 1812 です)。
- RADIUS サーバーアカウンティングポート — アカウンティングメッセージに使用される RADIUS サーバー UDP ポートです。(範囲は 1−65535 です。デ フォルトは 1813 です)。
- RadSecの有効化—TCPやTLSを介してRADIUSデータグラムを転送するための認証及び承認プロトコルです。RadSec は、初期の RADIUS デザインで使用されていた UDP に代わるものであり、信頼できるトランスポートプロトコルとパケットペイロードに対してのより広範囲のセキュリティを提供します。
- 認証方法 —APとRADIUSサーバー間のメッセージのために使用する暗号化の方法を CHAP、PAP、MS-CHAPV2 から選択してください。暗号化の方法は、RADIUS サーバーで使用されている方法と一致しなければいけません。
- ローカル ID — ローカル RADIUS サーバーの識別子です。
- ローカル名 — ローカル RADIUS のサーバー名です。
- NASID の生成 - このオプションは、このサイトの各デバイスに固有の NAS ID を生成します。
- NAS ID— ローカル RADIUS サーバー操作の識別子です。

キャプティブポータル

ホットスポットページのキャプティブポータルセクションでは、ホットスポットサービスでのポータルの詳細を設定します。

キャプティブポータルは、ホットスポットクライアントがウエルカム web ページにアクセスする前に、インターネットへのアクセスを強化するように誘導します。ウエルカムページへのアクセスは認証や支払いが必要の場合があります。

図 137: ホットスポットキャプティブポータルの設定



選択肢たホットスポットモードによって異なりますが、このセクションでは下記のアイテムが表示されます。

全てのモードに共通するアイテム

- ランディング URL — キャプティブポータルにログインした後にユーザが誘導される URL です。
- アイドルタイムアウト — アクティブでない状態で接続を保持できる最大値です。(範囲は 0−86400 秒です)。
- セッションタイムアウト — クライアントがホットスポットにログインした状態を保持できる最長時間です。(範囲は 0−86400 秒です)。

外部キャプティブポータルサービス、外部 RADIUS によるリモートスプラッシュページを除く全モード共通。

- HTTPS ログイン - キャプティブの HTTPS を有効にします。

外部のキャプティブポータルサービスを除いた全てのモードに共通するアイテム

- カスタマイズスプラッシュページ — 有効になると、ローカルのキャプティブポータルのウエルカムページを作成するために必要な情報を入力できるようになります。
  - タイトル — ページのタイトルとして表示したいテキストを入力してください。
  - 背景カラー — ボタンをクリックして背景となる色を選択してください。
  - ロゴイメージ —“アップロード“ボタンをクリックして画像ファイルを送信してください。ファイルのサイズは 1MB に制限されています。また、画像の高さは 1000 ピクセルまでである必要があります。
  - Terms and Conditions — キャプティブポータルの契約条件を定義するテキストをウインドウに入力し、コントロールを使用してフォーマットを調整してください。または、“ USE DEFAULT TERMS AND CONDITIONS “ ボタンをクリックしてインポートしたテキストを必要に応じて編集し、使用します。

外部のキャプティブポータルサービスモード

- キャプティブポータルURL—ホットスポットインターネットサービスのホスト名です。
- キャプティブポータル秘密鍵 — ホットスポットでのログインに使用されるパスワードです。
- Octetsを交換する— “入力オクテット“と“出力オクテット“の数値を交換します。

シンプルなパスワードのみのスプラッシュページモード

- スプラッシュページのパスワード — ユーザがログインしてインターネットにアクセスする際に必要なパスワードです。

認証の除外

ホットスポットページの認証の除外ページでは、ホットスポットサービスの“ウォールド・ガーデン“とホワイトリストを設定します。

図 138: ホットスポットでの認証の除外

このセクションでは以下のアイテムが表示されます。

- ウォールド・ガーデン — ホットスポットユーザがキャプティブポータルに認証される前にアクセスが可能なドメインや IP アドレスのリストを、CIDR 表記で入力してください。ワイルドカードドメインは domain.com のフォーマット（ドメインと全てのサブドメインを許可）または .domain.com のフォーマット（サブドメインのみを許可）を指定してください。
- 認証ホワイトリスト — キャプティブポータルを経路としてインターネットにアクセスできる MAC アドレスのリストです。

システムの設定

システムの設定ページでは、AP へのリモート管理アクセスを制御し、NTP タイムサーバーを設定できます。Telnet、Web、SNMP 管理イン ターフェースが有効になっているので、インターネットからアクセスできます。セキュリティ強化のために、特定のサービスを無効にして、インターネットからの管理アクセスを防ぐこともできます。

一般設定

システムの設定ページの一般設定セクションを使用すると、クラウドステータス LED、リセットボタン、タームゾーンを設定できます。

図 139: 一般的なシステムの設定

このページでは以下のアイテムが表示されます。

- クラウドステータスの有効化 — 部のデバイス（SkyFire、SunSpot、Spark、Spark Wave 2 Mini）では、AP が ecCLOUD に正常に接続され、正常に動作している場合、LED が緑色になります。
- 無線 LED を有効化 - ECW5211、ECWO5211、OAP100、Spark Wave 2/ SunSpot Wave 2 で 3.0.0+ ファームウェアを実行している場合のみサポートしています。無線が有効で正常に動作している場合、LED は点灯しています。
- リセットボタンの有効化 — ハードウエアリセットボタンを有効または無効にします。リセットボタンはサイトでは無効にできないので注意してください。
- タイムゾーン — 現地時間に対応する時間を表示するには、プルダウンリストが表示するタイムゾーンを選択してください。
- ブート再試行の回数 — 次のブートバンクに切り替えるまでのブートアップの再試行の最大数です。（範囲は 1−254 です。デフォルトは 3 です）。
- プレログイン PPPoE フォームを有効化 — この設定をオンにすると、インターネットにアクセスできない兆候がある場合に、ローカルウエブ UI ログインフォームの前に、PPPoE ユーザ名／パスワード入力フォーム が表示される用になります。こうすることで、エンドユーザがデバイス UI にログインしなくても、PPPoE 資格情報を入力できます。
- MSP モード — エンドユーザがユーザ定義のユーザアカウントからほとんどのデバイス設定にアクセスし、変更することを防ぐ Managed Service Provider (MSP) モードを有効にできます。root」と「admin」アカウントからの管理アクセスは、すべてのデバイス設定へのフルアクセスを提供します。(初期値：無効）

MSP モードを有効にすると、サービスプロバイダーは、「ローカル設定可能」設定を有効にすることで、特定の無線 SSID 設定をユーザ設定に利用できるようにするオプションがあります。

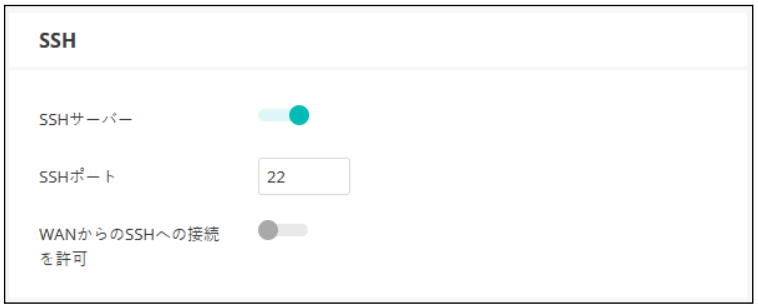
注意：MSP モードと " 常にクラウド設定に従う "（65 ページ）を同時に有効にしないでください。デバイスの設定が ecCLOUD に正しく更新されなくなります。

SSH

Secure Shell (SSH) は Telnet の安全な代替品として機能します。SSH プロトコルは、生成されたパブリックキーを使用して、アクセスポイントと SSH 対応の管理ステーションクライアントとの間を通過する、全ての転送されたデータを暗号化します。こうすることで、ネットワーク上を通過する データが、変換されずに宛先に届くようになります。クライアントはアクセスの認証時にローカルユーザ名と、パスワードを安全に使用できるようになります。

SSH プロトコルを介して管理業務のためにアクセスポイントにアクセスするには、SSH クライアントソフトウエアを管理ステーションにインストールする必要があるので注意してください。

図 140: SSH サーバーの設定



このページでは以下のアイテムが表示されます。

- SSH サーバー — アクセスポイントへの SSH アクセスを有効／無効にします。（デフォルトは無効です）。
- SSH ポート — アクセスポイントの SSH サーバーの TCP ポート番号を設定します。（範囲は 1 – 65535 です。デフォルトは 22 です）。
- WAN からの SSH への接続を許可する — WAN からの SSH 管理アクセスを許可します。

検出ツール

Edgecore Discovery エージェントを使用する と、AP を、ローカルネットワーク上の他のデバイスまたはインターネット経由で検出できます。

図 141: 検出ツールの設定

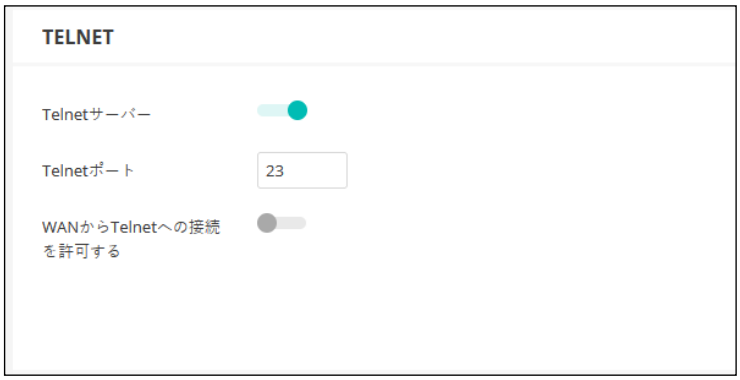
このページでは以下のアイテムを表示します。

- 検出ツール — 検出ツールを有効／無効にします。（デフォルトは有効です）。
- WAN を許可 —WAN からの検出ツールのアクセスを許可します。

Telnet

Telnet は、ネットワーク内のどこからでもアクセスポイントを設定できる管理用ツールです。ただし、Telnet は悪意のある攻撃には弱いので注意してください。Telnet はデバイスの分析とデバッグに使用されるリナックス（Linux）ベースのインターフェースへのアクセスを提供します。

図 142: Telnet サーバーの設定



このページでは以下のアイテムを表示します。

- Telnet サーバー — アクセスポイントへの Telnet アクセスを有効／無効にします。（デフォルトは無効です）。
- Telnet ポート — アクセスポイントの Telnet サーバーの TCP ポート番号を設定します。（範囲は 1－65535 です。デフォルトは 23 です）。

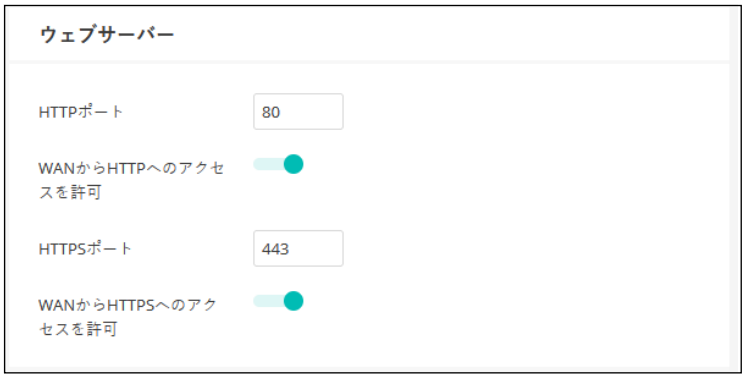
- WANからTelnetへの接続を許可する — WAN からの Telnet 管理アクセスを許可します。

ウエブサーバー

ウエブブラウザは、アクセスポイントを管理するための主要な方法を提供します。HTTP サービスと HTTPS サービスに、個別にアクセスできます。もし HTTP を有効にする場合は、URL に https://device:port_number を入力してください。

- クライアントは、サーバーのデジタル認証を使用してサーバーを認証します。
- クライアントとサーバーは、接続に使用する一連のセキュリティプロトコルを交渉します。
- クライアントとサーバーは、データの暗号化や複合化のためのセッションキーを作成します。
- クライアントとサーバーは安全な暗号化された接続を確立します。
- ほとんどのブラウザは、ステータスバーにパッドロックアイコンが表示されます。

図 143: ウエブサーバーの設定



このページでは以下のアイテムが表示されます。

- HTTP ポート — HTTP ウエブブラウザインターフェースで使用される TCP ポートです。(範囲は 1–65535 です。デフォルトは 80 です)。
- WANからHTTPへのアクセスを許可 — WANからのHTTP管理目的のアクセスを許可します。
- HTTPS ポート —HTTPS ウエブブラウザインターフェースで使用される TCP ポートです。(範囲は 1–655535 です。デフォルトは 443 です)。
- WANからHTTPSへのアクセスを許可 — WANからのHTTPS管理目的のアクセスを許可します。

ネットワークタイム

ネットワークタイムプロトコル（NTP）を使用すると、アクセスポイントは、タイムサーバー（SNTP または NTP）からの定期的な更新に基づいて、内蔵クロックを設定できます。アクセスポイントが常に時刻を維持できるので、システムログはイベントの正確な日と時刻を記録できます。クロックが設定されていない場合、アクセスポイントは、最後の起動時の工場出荷時のデフォルトなどから時間のみを記録します。

アクセスポイントは NTP クライアントとして機能し、定期的に時刻同期要求を送信します。また、アクセスポイントは、設定された順序で各サーバーを調査し、時刻の更新を受信します。

図 144: NTP の設定

このページは以下のアイテムを表示します。

- NTP プロトコル — 時間更新の要求の送信を有効／無効にします。（デフォルトは有効です）。
- NTP サーバー — タイムサーバーのホスト名を設定します。スイッチは最初のサーバーから時刻を更新しようとしますが、これに失敗した場合は、設定された順番で次に当たるサーバーから更新します。追加のサーバーを設定するには、リストの下部にある空白フィールドにエントリーを書き込んでください。

SNMP

Simple Network Management Protocol (SNMP) は、ネットワーク上のデバイスを管理するために特別にデザインされた通信プロトコルです。これは通常、ネットワーク環境でデバイスが適切な操作を行うように設定するため、及びパフォーマンスを評価したり潜在的な問題を検出するなど、デバイスを監視するために使用されます。

図 145: SNMP の設定

このページでは以下のアイテムが表示されます。

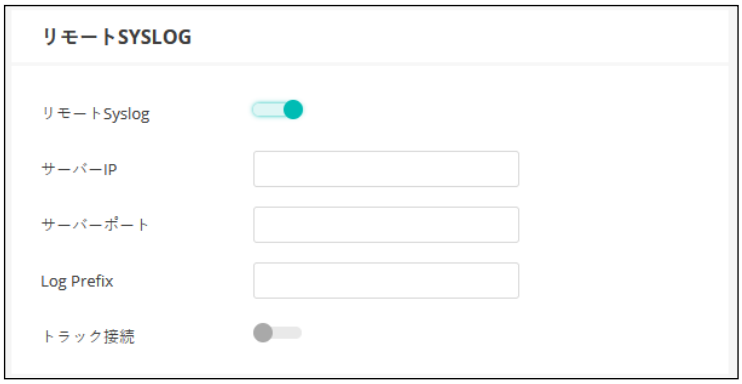
- SNMP サーバー — アクセスポイントで SNMP を有効／無効にします。(デフォルトは有効です)。
- 連絡先 — アクセスポイントの管理者の連絡先です。
- コミュニティストリング — パスワードのように機能し、SNMP プロトコルへのアクセスを許可するための文字列です。(範囲は 1–32 です。大文字と小文字を区別します。デフォルトは public です)。

  デフォルトの文字列 “public” は、アクセスポイントの管理情報（MIB）の読み取りのみのアクセスを提供します。
- IPv6 Write Community — アクセスポイントの管理情報（MIB）データベースへの IPv6 アクセス用のコミュニティ文字列です。(範囲：1-32 文字、大文字と小文字を区別します。デフォルト：private6)
- 場所 — SNMP システムロケーション文字列を設定します。(最大長：255 文字)
- すべてのWANのSNMPを許可する — WANからのSNMP管理目的のアクセスを許可します。

リモート Syslog

この機能を使用して、ログメッセージをシスログ（Syslog）サーバーに送信します。

図 146: リモートログの設定



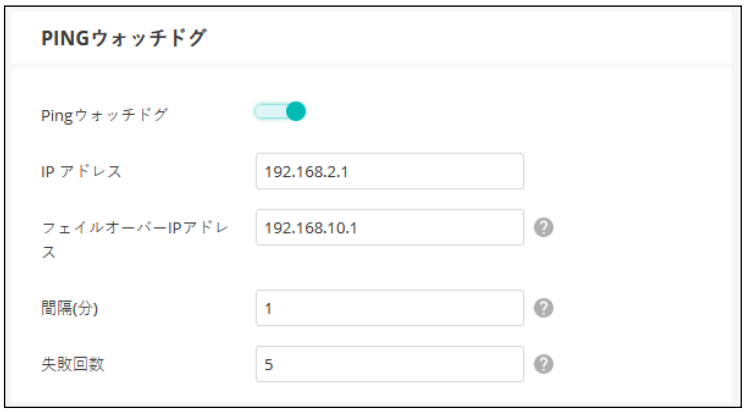
このページでは以下のアイテムを表示します。

- リモート Syslog — リモートログプロセスへのデバッグ、またはエラーメッセージのロギングを有効／無効にします。
- サーバー IP — シスログ（Syslog）メッセージが送信される、リモートサーバーの IP アドレスを指定します。
- サーバーポート — リモートサーバーが使用する UDP ポート番号を指定します。（範囲は 1－65535 です）。
- Log Prefix — 指定したサーバーに送信されるログファイルのプレフィックスを設定します。ファイルサフィックス " ログ " が使用されます。
- トラック接続 — 無線クライアントの接続ログメッセージをシスログ（Syslog）サーバーに送信します。

Ping ウォッチドグ

この機能を使用すると、Ping プローブパケットを定義済みの IP アドレスに送信し、接続を確認します。

図 147: ping ウォッチドグの設定



このページでは以下のアイテムを表示します。

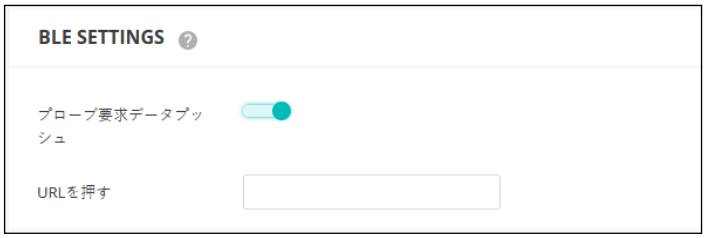
- ping ウォッチドグ — 接続を確認するために、定義された IP アドレスへの Ping プローブパケットの送信を有効にします。
- IP アドレス — Ping を実行する主要な IP アドレスです。
- フェイルオーバーIP アドレス — 主要な IP への Ping プローブが失敗した場合に Ping を実行する（オプションの）、フェイルオーバー IP アドレスです。フェイルオーバー IP に正常に Ping ができる場合、失敗カウンターは再びゼロにリセットされるので注意してください。
- 間隔（分）— Ping チェックを分単位で実行する頻度です。
- 失敗回数 — デバイスが再起動するまでに Ping が連続で失敗する数値です。

BLE の設定

この機能を使用すると、デバイスが Bluetooth Low Energy プローブ要求の記録を、指定された URL にプッシュできるようになります。

BLE の設定は、BLE をサポートするデバイスでのみ使用できます。

図 148: BLE の設定



このページでは以下のアイテムが表示されます。

- プローブ要求データプッシュ —AP のための BLE プローブ要求データプッシュです。有効にすると、AP は JSON 形式の BLE プローブ要求データを指定された URL にプッシュします。
- URL を押す — データの送信先の URL です。

マルチキャスト DNS

この機能を使用して、AP でマルチキャスト DNS サポートが有効にします。マルチキャスト DNS は、ホスト名をマルチキャスト IP アドレスとする DNS サーバーがない小規模なネットワークで使用できます。

マルチキャスト DNS の設定は DNS をサポートしているデバイスでのみ使えます。

図 149: マルチキャスト DNS の設定

このページでは下記のアイテムが表示されます。

- MDNS — マルチキャスト DNS サポートを有効／無効にできます。（デフォルトは有効です）。

IGMP スヌーピング

AP は IGMP（Internet Group Management Protocol）を使って、特定のマルチキャストサービスの受信を希望するクライアントを確認できます。そして、AP はサービス要求を近隣のマルチキャストスイッチ / ルーターに伝搬させ、クライアントがマルチキャストサービスを継続して受信できるようにします。

図 150: IGMP スヌーピング設定

このページでは、以下の項目が表示されます：

- IGMP Snooping の有効化 — IGMP Snooping サービスを有効にします。(初期値：無効)

LLDP

LLDP（Link Layer Discovery Protocol）は、ネットワーク上の隣接するデバイスの基本情報を発見するために使用されます。LLDP はレイヤ 2 プロトコルであり、定期的なブロードキャストを使用して、送信側デバイスの情報をアドバタイズします。

図 151: LLDP 設定

このページでは、以下の項目が表示されます：

- LLDP Advertisementの有効化 — APに関するLLDPアドバタイズメントを以下のように送信することを有効にします。
- Tx Interval (seconds) — LLDP アドバタイズメントの定期的な送信間隔を設定します。(範囲：5 ～ 32768 秒、デフォルト：30 秒)。
- Tx Hold (number of time(s)) — LLDP 広告で送信される TTL（time-to-live）値を下式に示すように設定する。(範囲：2 ～ 10、デフォルト：4)

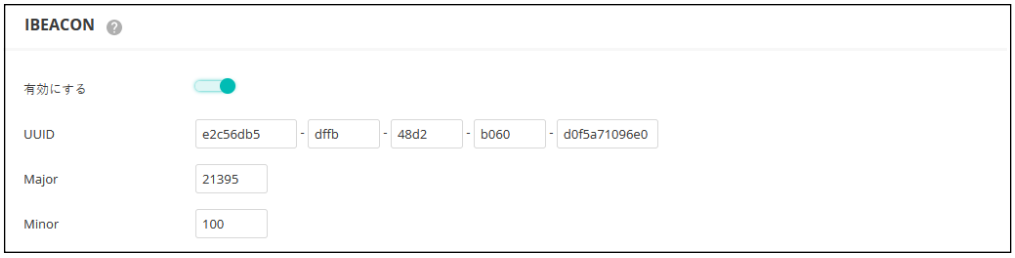
  time-to-live は、受信側の LLDP エージェントに送信側デバイスがタイムリーに更新を送信しない場合、送信側デバイスに関連するすべての情報を保持する期間を指示します。

  秒単位の TTL は、以下のルールに基づいています：
  最小値（(Tx Interval * Tx Hold)、または 65535）
  したがって、デフォルトの TTL は 4*30 = 120 秒です。

iBeacon

AP は、Bluetooth Low Energy（BLE）に基づく iBeacon 規格をサポートしています。BLE ビーコンを搭載したデバイスは、ビーコン広告を認識し、提供された情報を抽出し、その内容に基づいてアクションを起こすことができる電話などの BLE クライアントに位置情報サービスを提供できます。

図 152: iBeacon 設定



このページでは、以下の項目が表示されます：

- iBeacon の有効化 - AP の iBeacon サポートを有効にします。(デフォルト：有効にする)
- UUID - ビーコンサービスを宣伝する iBeacon Universally Unique Identifier です。UUID は、ハイフンで区切られた 5 つのグループに分かれた 32 の 16 進数で構成されています。
- Major - ビーコングループを識別するために使用される iBeacon 値です。(範囲 : 0-65535)
- Minor - グループ内の個々のビーコンを識別するために使用されるiBeacon 値です。(範囲 : 0-65535)

SNMPv3 ユーザ

SNMP プロトコルバージョン 3 は、アカウント認証とデータの暗号化により、安全なアクセスを提供します。SNMP v3 ユーザは、Add ボタンをクリックすることで定義できます。

図 153: SNMPv3 ユーザ設定

このページでは、以下の項目が表示されます：

- 名前 — SNMP サービスにアクセスするために使用されるユーザ名。
- Access Auth — アクセス許可を "Read Only" または "Write" として選択します。
- Auth Type — 認証のためのハッシュアルゴリズムを選択します。
- Auth Pwd — 認証用のパスワードを設定します。
- Encryption Type — データパケットの暗号化アルゴリズムを選択します。
- Encryption Pwd — データ暗号化用のパスワードを設定します。

5 サイト WiFi 6 構成

この章では、WiFi 6 アクセスポイントの設定について説明します。次のセクションが含まれます。

無線 SSID の設定

サイトメニューから “ 設定 “、続いて “WiFi6“ を開き、サイト内の全ての Edgecore WiFi 6 アクセスポイントに適応する設定のオプションを表示してください。

Edgecore WiFi 6 アクセスポイントは数種類の無線モード（802.11a/a+n/ac+a+n/ax(5GHz) または 802.11b+g+n/ax(2.4GHz) に適応します。使用できるモードはアクセスポイントのモデルによって異なります。デュアルバンドアクセスポイントは 2.4GHz と 5GHz で同時に操作できるのでご注意ください。

それぞれの無線は 8 つのサービスセット識別子（SSID）、またはバーチャルアクセスポイント（VAP）インターフェースに適応しています。一つ一つの VAP は、独立したアクセスポイントとして機能し、それぞれ個別の SSID とセキュリティの設定を行います。ただし、ほとんどの無線信号パラメータ設定は、すべての VAP インターフェイスに適用されます。特定の VAP へのトラフィックは、ユーザグループまたはアプリケーショントラフィックに基づいて分離できます。Edgecore の AP デバイスは一台の無線ごとに、最多で 128 人の SSID インターフェースを利用する無線クライアントに対応します。

図 154: サイト WiFi6 構成

WiFi6 設定ページの無線 SSID タブが詳細するのは以下のアイテムです。

- SSID リスト — このサイトの Wi-Fi デバイス用に設定された SSID インターフェースのリストです。各 SSID は、特に設定されていない限り、2.4 GHz、5 GHz、および 6 GHz 無線の両方に適用されることに注意してください。最大 8 つの SSID を設定できます。SSID を追加」ボタンをクリックして、SSID インターフェースを作成できます。

- 無線スケジューリング — 指定された時間に AP 無線をオン／オフするために設定されたスケジュールのリストです。スケジューリングルールは、

すべてのサイト AP の 2.4GHz、5GHz、6GHz インターフェースに適用されます。ワイヤレススケジュールを作成するには、"Add Schedule " ボタンをクリックしてください。

SSID を追加する

Wireless SSID 設定ページにある SSID の追加をクリックして、下の図に示されているように SSID、ネットワーク、セキュリティの設定を表示してください。

図 155: 無線設定

SSID の追加ページでは以下のアイテムが表示されます。

一般設定

- SSID を有効化 — SSID のインターフェースを、使用可能／不可能にします。
- SSID—VAP インターフェースが提供する基本サービスの名前です。アクセスポイントを使用してネットワークに接続したいクライアントは、アクセスポイントの VAP インターフェースと同じく SSID を設定しなければいけません。（ネットワーク名は 32 文字まで）。
- ブロードキャスト SSID -SSID は一定の間隔でブロードキャストを行うので、コネクションを探す無線ステーションと比較的簡単に接続できます。そのため、無線クライアントは自由に無線 LAN を楽しむことができます。この特質を利用されると自宅のネット ワークへのハッキングの恐れもあります。SSID は暗号化されていないので、AP を通して SSID からブロードキャストされるメッセージを受信する無線 LAN をスキャンすることは簡単です。（デフォルトは ON の状態です）。
- SSID Isolation - 有効にすると、同じ無線カード上の異なる SSID に接続されたワイヤレスクライアントが互いに隔離されます。(デフォルトはオフ）
- クライアントアイソレーション - この設定を有効にすると、無線クライアントは LAN と通信できます。この通信が利用可能な場合は、インターネットに到達できますが、相互に通信することはできません。（デフォルトでは OFF の状態です）。
- マルチキャストをユニキャストに変換 — 有効にすると、AP は、すべてのクライアントにトラフィックをブロードキャストする代わりに、マルチキャストトラフィックを要求するクライアントにのみ、マルチキャストトラフィックを転送します。この機能は、クライアント分離が無効の場合は自動的に有効になり、クライアント分離が有効の場合は無効になります。この機能は、手動で設定することはできません。(デフォルトは有効)
- 最大クライアント数 — 同時に SSID に接続できる、最大限の無線クライアントの人数を設定してください。（デフォルトでは 127 人です。人数の範囲は 0 から 127 人です）。
- 最小許容信号 — 信号の最小限クライアントの信号の強度（RSSI）が特定の数値と同等またはそれ以上でないと SSID を使用できません。この機能は設定値を -100 にすると使えなくなります。すでに繋がっているクライアントについては定期的に確認します。

この機能を使うことで、クライアントはより信号の強度が高い AP を使用することになります（アシステッドローミングとも言う）。推奨値は、アクセス ポイントの密度とカバレッジに応じて -70 ～ -80 です。

RSSI（受信信号強度）を -1 から -100db デシベルで入力してください。数値が 0 に近づくほど強度が高くなります。(デフォルト : -70)

- 無線で起動する - SSID を設置する無線を選択してください。もしデバイスの両方の無線で SSID がアクティブ化されている場合、（SSID がミラーリングされているという意味です ）SSID 使用の記録を、どちらかの設定タブから編集してください。この編集は 2.4GHz と 5GHz の記録に反映されます (デフォルト : 6GHz、5GHz、2.4GHz に有効)。

セキュリティの設定

- 方法 - それぞれの SSID にアソシエーションモード、暗号化、認証などの無線セキュリティを設定します。

注意 :OAP101-6E 6GHz 無線機は、WPA3 パーソナル、WPA3 エンタープライズ、WPA3 エンタープライズ 192 ビット、および OWE のみをサポートします。(デフォルト : WPA3 パーソナル)。

  - オープン -SSID インターフェースは、設定済みの SSID を含むビーコン信号をブロードキャストします。SSID で " 全て " 設定の無線クライアントは、ビーコンの SSID を読み込むことができ、自動的に接続できます。

  - WPA-PSK — 会社での設置を考えると、WPA を使用するには、RADIUS 認証のサーバーが、ネットワーク上で設定されている必要があります。しかしながら規模の小さなオフィスでネットワークを使用する場合、RADIUS サーバーを保持する資力が不足しているかもしれません。その場合、WPA は事前共有鍵（PSK）でネットワークのアクセスを運転できます。事前共有鍵モードは共通のパスワードを認証に使用します。パスワードは全ての無線クライアントに使用され、手動で入力されます。事前共有鍵モードは、会社用の WPA と同じ TKIP パケット暗号とパスワードの管理方法を使っていますが、規模の小さなネットワークで扱いやすいサービスを提供しています。

    - 暗号化 - データの暗号化は以下のように行われます :

      - AES — AES-CCMP はマルチキャスト暗号として使用されます。AES-CCMP は WPA2 が必要とする、基本の暗号機能です。（これはデフォルトの設定です。）

- TKIP＋AES —クライアントに使用される暗号化技術はアクセスポイントで知ることができます。

- キー — WPAは無線クライアントとSSIDインターフェースの間を伝達するデータを暗号化します。WPA は、ネットワークを使用するすべてのクライアントに手動で配布される共有鍵 (固定長の 16 進数または英数字の文字列) を使用します。

  文字列は 8 から 63 文字（英数字）である必要があります。特異な文字は使えません。

- Dynamic Keys - RADIUS 認証サーバーによって定期的に生成および更新される動的 PSK キーの使用を有効にします。RADIUS サーバーの IP アドレス、UDP ポート、および秘密のテキスト文字列を指定する必要があります。

  Dynamic Keys は、WPA2-PSK セキュリティでのみサポートされます。

- Multiple Keys - 1 行に 1 つずつ､複数のキーを入力できるようにします。　特定の MAC アドレスを持つキーを入力すると、そのキーは 1 つのクライアントで使用できるように制限されます。MAC アドレスのないキーを入力すると、そのキーはすべてのクライアントで使用できるようになります。

  複数のキーは、WPA-PSK、WPA2-PSK、および WPA3 Personal Transition セキュリティに対応しています。

- WPA2-PSK — 共有キーを持っている WPA2 クライアントは認証を受けることができます。

  WPA は、WEP が IEEE802.11i 無線セキュリティスタンダードの認定を保留している間の暫定的な解決策として開発されました。事実上、WPA は 802.11i のサブネットです。WPA2 は現在は承認されている 802.11i スタンダードを含んでおり、WPA にも対応しています。WPA2 は 802.1x と PSK モードで操作でき、TKIP 暗号化技術をサポートしています。

  暗号化技術とキーについての詳細は WPA-PSK を参照してください。

- WPA-EAP — WPA はいくつかの技術を用いて 802.11 無線ネットワークのセキュリティを強化しています。RADIUS サーバーは認証のために使用されており、アカウンティングに使われることもあります。

  暗号化技術については WPA-PSK を参照してください。

  RADIUS の設定

IEEE802.1X ネットワークアクセスコントロールと Wi-Fi Protected Access (WPA) ワイヤレスセキュリティを実装するには、アクセスポイントに RADIUS サーバを指定する必要があります。

RADIUS アカウンティングを設定して、アクセスポイントからユーザセッションのアカウンティング情報を得ることもできます。RADIUS アカウンティングは、ネットワーク上でのユーザのアクティビティにおいて、価値のある情報を提供するでしょう。

注意：このマニュアルはお客様がすでに RADIUS サーバーの設定を済ませており、アクセスポイントへ接続できることを前提としています。RADIUS サーバーソフトウエアの設定については当マニュアルでは説明されていません。RADIUS サーバーソフトウエアについてのマニュアルを参照してください。

- RADIUS MAC 認証 -RADIUS 認証を使用します。この設定がされている場合、AP が、クライアントのデバイスの MAC アドレスを、特定の RADIUS サーバーに、認証のために送信します。サーバは MAC が有効なユーザであることを確認した後、ダイナミック VLAN ID (設定されている場合) およびクライアントデバイスのその他のリソースを AP に応答します。

  注意 : RADIUS サーバーの認証を得るためには、クライアントのデバイスの WiFi MAC に句読点を含まない形でユーザ ID とパス ワードが設定されている必要があります。

  この機能は v1.1.1 ファームウェアの " オープンセキュリティ " や、WEP を除いたその他のセキュリティでサポートされています。

- RADIUS オース (Auth) - WPA-EAP や WPA2-EAP セキュリティを使用するためには、RADIUS サーバーが設定される必要があります。

- RADIUS 認証サーバー- RADIUS 認証サーバの IP アドレスまたはホスト名を指定します。

- RADIUS 認証ポート -RADIUS サーバーが認証のメッセージを送信するために使用するポート番号です。(範囲は 1024-65535 です。デフォルト状態の場合は 1812 です)。

- RADIUS 認証秘密鍵 - アクセスポイントと RADIUS サーバーの間でメッセージの暗号化のために使われるテキスト配列です。同じ文字列が RADIUS 認証サーバーで使われていることを確認してください。文字列にスペースを使用しないでください。
  (最長 255 文字です)。

- バックアップ RADIUS 認証 - 基本のサーバーが使用不可能になった場合に、予備の RADIUS サーバーとしてバックアップするように設定されています。

- RADIUS アカウンティングを使用 -RADIUS アカウンティングを使って、請求書の発行やセキュリティの目的でアカウントサービスを使用 することを可能にします。

- RADIUS アカウンティングサーバー -RADIUS アカウンティングサーバーの IP アドレスやホストネームを指定します。

- RADIUS アカウンティングポート - アカウンティングメッセージを送信するために RADIUS サーバーが使用する UDP ポート番号です。(範囲は 1024-65535 です。デフォルト状態の時は 1813 です)。

- RADIUS アカウンティング秘密鍵 - アクセスポイントと RADIUS サーバーの間で共有されるメッセージを暗号化するために使われるテキスト文字列です。RADIUS アカウントサーバーで、同じテキスト文字列が使われていることを確認してください。文字列にはスペースを使用しないでください。(最長で 255 文字です)。

- WPA2-EAP — WPA は、WEP が IEEE802.11i 無線セキュリティスタンダードの認定を保留している間の暫定的な解決策として開発されました。事実上、WPA は 802.11i のサブネットです。WPA2 は現在承認されている 802.11i スタンダードを含んでおり、WPA にも対応しています。WPA2 は 802.1x と PSK モードで操作でき、TKIP 暗号技術をサポートしています。

  RADIUS サーバーは認証だけではなく、下の目的に使用できます。

  暗号化方式の詳細については、WPA-PSK を参照してください。

  RADIUS サーバーの設定については、WPA-EAP を参照してください。

- WPA3 Personal — SAE（Simultaneous Authentication of Equals）付き WPA3 を使用しているクライアントは、認証に応じます。

  WPA3 では、WPA2-Personal の Pre-Share Key（PSK）に代わり、Simultaneous Authentication of Equals（SAE）という、より強固なパスワードベースの認証が提供されます。この技術により、オフラインの辞書攻撃を防ぐことができるため、データトラフィックを安全に伝送できます。

- WPA3 Personal Transition — SAE付きのWPA3を使用しているクライアント、または PSK 付きの WPA2 を使用しているクライアントは、認証のために受け入れられます。AP は、ネットワークへのアクセスを許

可する前に、サポートされている認証と暗号化を各クライアントと交渉します。

- WPA3 Enterprise — WPA2-EAP セキュリティの強化版で、より強固な暗号化を使用します。クライアントがネットワークにアクセスするには、より強力な WPA3 暗号化オプションのいずれかをサポートし、Protected Management Frames (PMF) を使用する必要があります。IEEE 802.1X ネットワークアクセスコントロールと RADIUS サーバーを使用する必要があります。

  RADIUS の設定については、上記の「RADIUS 設定」を参照してください。

- WPA3 Enterprise Transition — WPA3 および WPA2 クライアントによるネットワークへのアクセスを許可します。暗号化オプションと Protected Management Frames (PMF) の使用は、ネットワークへのアクセスを許可する前に各クライアントとネゴシエーションされます。

  RADIUS の設定については、上記の「RADIUS 設定」を参照してください。

- PMF - Protected Management Frames（PMF）は、AP とクライアント間のユニキャストおよびマルチキャスト管理フレームに WPA2/WPA3 セキュリティを提供します。「Optional」設定では、PMF をサポートしていないクライアントがネットワークにアクセスできるようになります。「Mandatory」設定では、PMF をサポートするクライアントのみがネットワークにアクセスできるようになります。(初期値：Optional)

- 802.11k - ローミング時に近隣のAPに関する情報をクライアントに提供します。クライアントが AP からローミングしようとするとき、利用可能な AP のリストと関連情報を含む「Neighbor Report」のリクエストを送信します。これにより、クライアントは全チャネルをスキャンすることなく、ローミング先となる最適な AP を素早く特定できます。(デフォルト：無効)

- 802.11v - 無線ネットワークの全体的な改善を促進する情報を関連クライアントに提供します。また、アイドル時間を設定することで、クライアントがバッテリーの寿命を向上させるのに役立ちます。(デフォルト：無効)

- 802.11r - AP 間の高速移行ローミングのための方法を提供します。クライアントが新しい AP にローミングする前に、最初のハンドシェイクと暗号化計算が事前に実行されるため、再度のハンドシェイクを必要とせず、高速なハンドオフが可能。(初期値：無効)

- OWE - Opportunistic Wireless Encryption (OWE) は、公衆 Wi-Fi ネットワークのユーザがパスワードを使用せずに安全なアクセスを得ることを可能

にする WPA3 オープンネットワークセキュリティです。OWE は、AP と各クライアント間のデータ通信を個別に暗号化しますが、ユーザ ID の認証は提供しません。

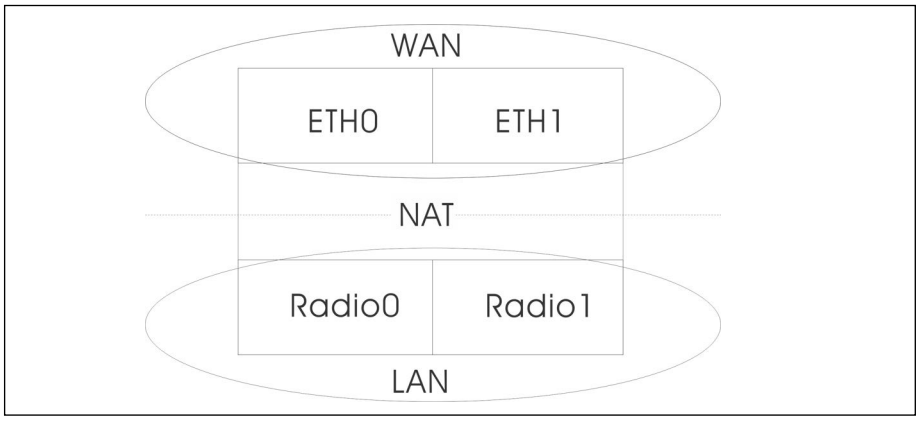
- アクセスコントロールリスト — アクセスポイントで設定されたローカルデータベースは、無線クライアントの MAC アドレスを確認することで認証を行います。(デフォルトでは OFF の状態です)。
  - ポリシー — MAC リストは、指定されたクライアントへのネットワーク アクセスを許可または拒否するように構成できます。(デフォルト : リストのすべての MAC を許可)
  - MAC フィルターリスト - クライアントの MAC アドレスのリストです。
- ダイナミック認証 - Dynamic Authorization Extensions (DAE) を使用すると、RADIUS はすでにネットワークに接続しているクライアントの接続を切断したり、認証を変えたりできます。
  - DAE ポート -DAE メッセージを使用するための DUP ポート番号です。(デフォルトは 3799 です)。
  - DAE クライアント -RADIUS サーバーの IPv4 アドレスです。
  - DAE シークレット - アクセスポイントと RADIUS サーバーが DAE メッセージを暗号化するために共有するテキスト文字列です。

ネットワークの設定

- ネットワークモード - 下記の接続方法から指定してください (デフォルトではルートからインターネットです)。
  - ブリッジからインターネット (AP ブリッジモード) - インターフェースを WAN (インターネット) に接続する設定です。

    下の図では、イーサネットポート 1 とイーサネットポート 2 がどちらも WAN に接続されています。このインターフェースから発せられるトラフィックは直接インターネットに送られます。イーサネットや無線のインターフェースはこのように設定できます。

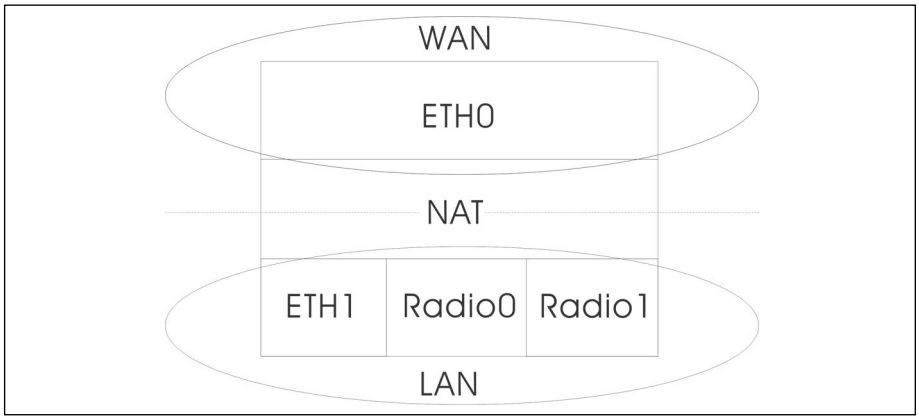
図 156: ブリッジからインターネット



- ルートからインターネット —インターフェースをLANの一つとして設定します。

  下の図では、イーサネット LAN0（5GHz 無線）と無線 LAN1（2.4GHz 無線）はどちらも LAN に含まれています。これらのインターフェースから発せられたトラフィックはイーサネットポート 0 のアクセスポイントを通ってインターネットに接続されます。

図 157: ルートからインターネット



  - 経由ルート - 経路制御されるネットワークです。デフォルトは、LAN の設定で表示されているように、“ デフォルトローカルネットワーク “ です。

- ゲストネットワークに追加 - このインターフェースはゲストネットワークのみをサポートします。

- ホットスポットで制御 - このインターフェースはホットスポットサービスのみサポートします。

- ウォールド・ガーデン - キャプティブポータルによって認証される前にホットスポットユーザがアクセスできるドメインや IP アドレスのリストを CIDR 表記で入力します。このようなドメインは domain.com（ドメインまたはサブドメインに使用できます）または .domain.com（サブドメインのみ使用できます）のフォーマットを使ってください。

- VLAN タグトラフィック -SSID インターフェースからイーサネットポートに送信されるパケットは、184 ページの「VLAN の設定」に基づいてタグ付けしてください。

注意：ecCLOUD は、AP とスイッチ間の VLAN 同期をサポートします。SSID に VLAN タグが有効になっている場合、設定された VLAN ID は ecCLOUD によって接続されたスイッチポートに自動的に設定されます。これにより、AP からの VLAN タグ付きトラフィックがスイッチポートで受け入れられるようになり、通信断を回避できます。

- アップロード速度の制限 - SSID インターフェースから有線ネットワークに送信されるトラフィックのレートを制限できます。最大値を Kbytes ／秒単位で設定できます。（範囲は 256－10048576kbyte ／秒。デフォルトは OFF の状態です）。

- ダウンロード速度の制限 - 有線ネットワークから SSID インターフェースに送信されるトラフィックのレートを制限できます。最大数値を kbyte/秒単位で設定できます。（範囲は 256－10048576kbyte ／秒です。デフォルトは OFF の状態です）。

- OpenRoaming — WPA2-EAP セキュリティが選択されている場合に利用可能な OpenRoaming (Hotspot 2.0) は、無線ネットワーク間のシームレスなローミングをサポートする公衆アクセス Wi-Fi ネットワークの標準を提供します。OpenRoaming AP は、クライアントがネットワークに接続するかどうかを決めることができるよう、その公衆 Wi-Fi 機能とサービスをアドバイスします。(デフォルト : 無効)

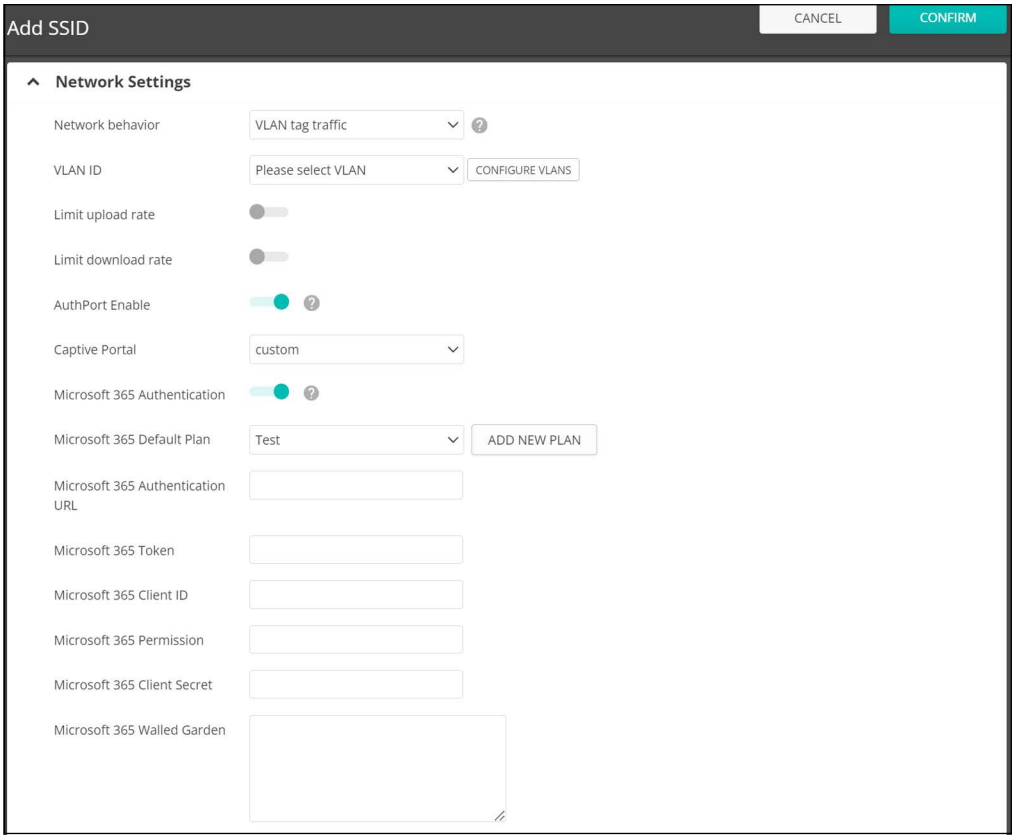
  - プロファイルの選択 — ワイヤレスネットワークに適用する設定済みプロファイルを選択します。

  - OpenRoaming の構成 — クリックすると、OpenRoaming プロファイル設定ページにアクセスします。プロファイル設定については、210 ページの「OpenRoaming」を参照してください。

- AuthPort 有効にする — このオプションを有効にすると、Wi-Fi ユーザはインターネットアクセスを許可される前に、設定可能な ecCLOUD ホストアカウントデータベースに対して認証するよう求められます。このオプ

ションを有効にするには、AuthPort アドオンを有効にする必要があります（74 ページの「AuthPort アドオンを使用する」を参照）。

図 158: Microsoft 365 認証の有効化



- キャプティブポータル — Microsoft ログインボタンを含むキャプティブポータルを選択します（80 ページの「キャプティブポータル」参照）。
- Microsoft 365 認証 — 管理者は Microsoft 365 認証を有効にできます。
- Microsoft 365 デフォルト プラン — クライアントが関連付けられ、認証されたときに消費される課金プランを関連付けます。リストから既存のプランを選択するか、新しいプランを追加します。
- Microsoft 365 認証 URL — Microsoft 365 認証サーバーのエンドポイントを設定します。
- Microsoft 365 トークン — Microsoft 365 認証用のトークンを設定します。
- Microsoft 365 クライアント ID — Microsoft Entra 管理センターがアプリに割り当てるアプリケーション (クライアント) ID - アプリの登録経験です。

- Microsoft 365 Permission — Microsoft 365 認証サーバーへの読み取りと書き込みの権限を指定します。
- Microsoft 365 クライアントシークレット — Microsoft 365 認証用のクライアントシークレットを設定します。
- Microsoft 365 Walled Garden — Microsoft 365 ログインフロー中のウォールガーデンを指定します。
- プロキシ ARP — プロキシ ARP が有効な場合、AP は独自の ARP ルックアップテーブルを維持し、下流のステーションに代わって ARP リクエストに返信する ため、ネットワークの非効率性を回避できます。この機能は、クライアント分離が無効の場合は自動的に有効になり、クライアント分離が有効の場合は無効になります。この機能は、手動で設定することはできません。プロキシ ARP は、Network Behavior が " ブリッジからインターネット " または "VLAN Tag Traffic " の場合にサポートされます。

無線スケジュールを設定する

無線スケジュールを設定すると、AP 無線を特定の時間に ON または OFF の状態にできます。スケジューリング・ルールは、すべてのサイト AP の 2.4 GHz、5 GHz、および 6 GHz インターフェースに適用されます。“ ADD SCHEDULE“ ボタンをクリックして、無線スケジュールを作成してください。

図 159: 無線スケジュール

ADD SCHEDULE ページでは以下のアイテムが説明します。

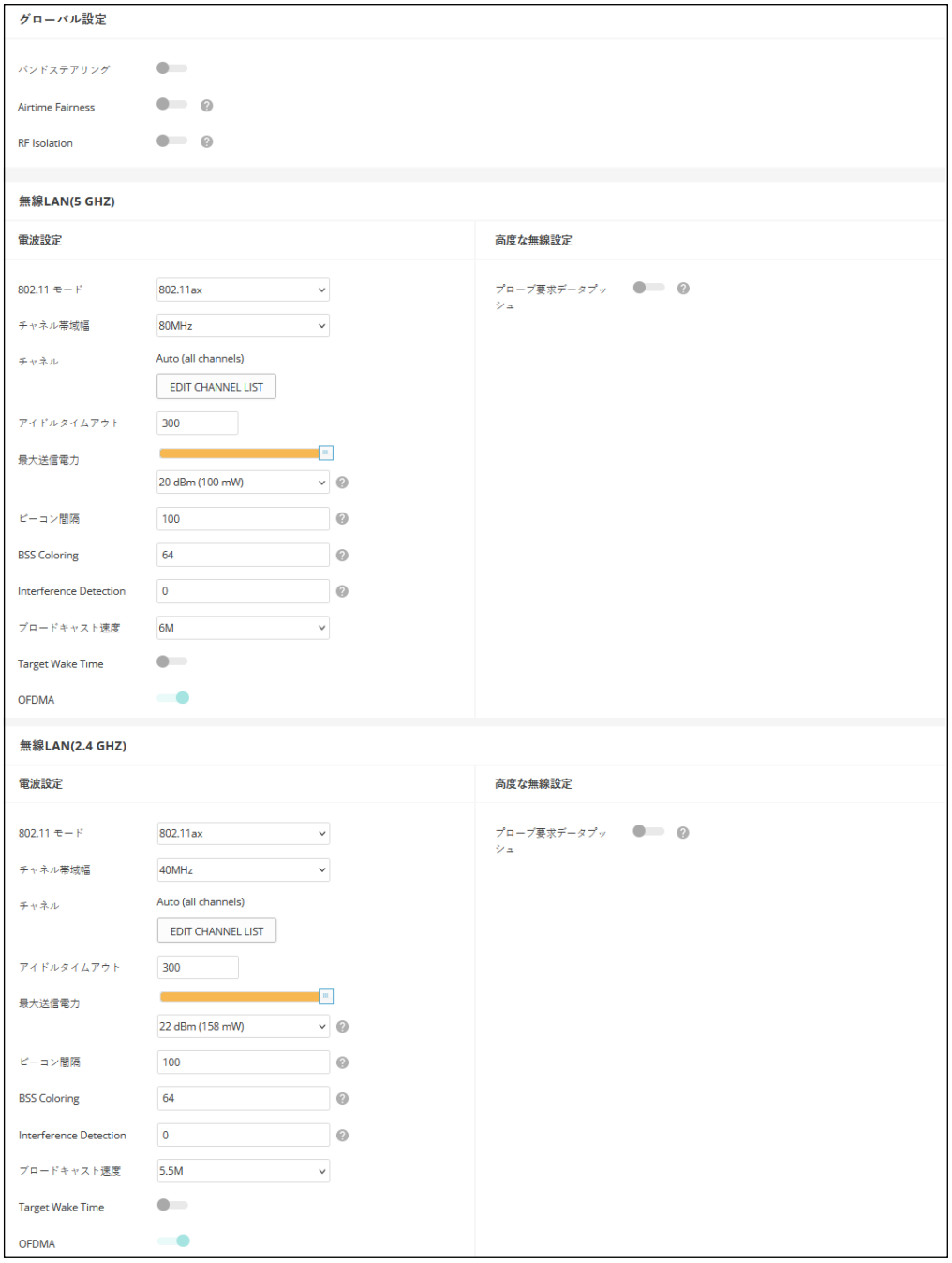
- 有効化 - 設定したスケジュールを使用できるようにします。（デフォルトでは使用不可です）。
- スケジュール名 - スケジュールを識別するテキスト文字列です。
- 開始時間 - 無線のスイッチを ON にする時間です。

- 終了時間 - 無線のスイッチを OFF にする時間です。
- 日 — 1 週間のうちで、スケジュールが適応される曜日を選択します。

無線設定

5GHz と 2.4GHz 無線設定をするためには、“WiFi アクセスページ “ で、“ 無線設定 “ タブをクリックしてください。この設定は全ての設定された SSID に適応するので注意してください。

図 160: WiFi6 無線設定



無線設定タブは、下記のアイテムを表示します。特に注意事項がなければ、設定のオプションは、5GHz と 2.4GHz どちらの無線にも適応します。

グローバル設定

- 有効にすると、2.4GHz、5GHz、6GHz をサポートするクライアントは、まず 6GHz 無線に接続されます。この機能はクライアントを二種類の無線バンドに分散するのに役立ちます。この機能が適応するためには、両方のラジオに一致する SSID が設定されている必要がある。

- Airtime Fairness — この機能を有効にすると、無線ネットワーク全体のパフォーマンスが向上します。(デフォルト : 無効)

- RF アイソレーション — 有効にすると、クライアントは異なる無線カード間で絶縁されます。

電波設定

- 802.11 Mode — 無線操作モードを定義します。
  - 6 GHz 無線 — デフォルト : 11ax; オプション : オプション : 11ax
  - 5GHz 無線 — デフォルト : 11ax、オプション : 11a、11a+n、11ac+a+n、11ax
  - 2.4 GHz 無線 — デフォルト : 11ax; オプション : オプション : 11ax

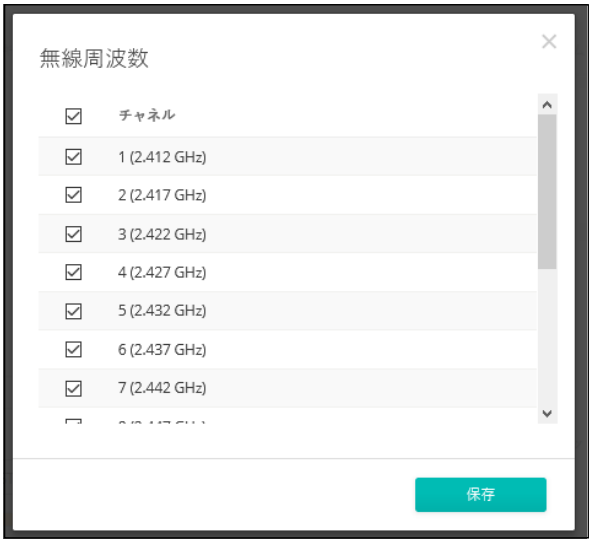
- チャネルの帯域幅 — Wi-Fi のチャネル帯域は 20MHz が基本ですが、チャネルを結合して 40MHz、80MHz、160MHz のチャネルを作ることで、より高速なデータ転送を実現できます。ただし、チャネル帯域幅を広くすると、利用できる無線チャネルの数が少なくなります。利用可能なチャネル帯域幅は、802.11 モードに依存します。(デフォルト : 2.4GHz 無線では 20MHz、6GHz 無線では 80MHz、オプション :20MHz、40MHz、80MHz、160MHz)
  - 20MHz — 802.11b+g+n および 802.11ax 用
  - 40MHz — 802.11b+g+n、802.11a、802.11a+n、802.11ac+a+n および 802.11ax 用
  - 80MHz — 802.11ac+a+n および 802.11ax 用
  - 160MHz —（EAP104 5GHz 無線機、OAP101 5GHz 無線機、OAP101-6E 5GHz および 6GHz 無線機でサポート）802.11ac+a+n および 802.11ax 用

- チャネル — 無線クライアントと連絡をとるためにアクセスポイントが使用する無線チャネルです。使用可能なチャネルは、無線、チャネルの帯域幅、規制している国の設定によって異なります。“ チャネルのリストを編集する “ ボタンをクリックして、どちらの無線インターフェースでも使用できる特定のチャネルを選択することもできます。

  自動設定にすると、アクセスポイントが使用可能な無線チャネルを自動的に選択します。

図 161: 5GHz 無線チャネル

図 162: 2.4GHz 無線チャネル



- アイドルタイムアウト - 接続がクローズされる前に、非アクティブな状態を維持できる最大時間です。(デフォルト : 300 秒)

- マックス TX パワー（Max TX パワー）— アクセスポイントから送信される無線信号の最大電力を調整します。送信電力が高いほど、送信範囲が広くなります。電力を調整すると、カバレージエリアとサポートできるクライアントの人数に影響があります。でもそれだけではありません。送信電力の高い信号が、サービスエリアのほかのデバイスの邪魔をしないことも大切です。（設定できる電力の範囲とデフォルトの電力は、AP モデルと規制している国の設定によって異なります）。

- ビーコン間隔 — アクセスポイントから送信されるビーコン信号の間隔です。無線クライアントは、ビーコン信号を使ってアクセスポイントと接続した状態を保っています。ビーコン信号は、電源管理やその他の情報を含んでいます。（範囲は 100−1024TUs で す。デフォルトの状態は、100TUs です）。

- BSS Coloring — 802.11ax（Wi-Fi 6）モードでは、BSS Coloring により、同じ周波数で動作する近くの AP が、自身の基本サービスセット（BSS）に属するトラフィックを識別できます。BSS Coloring により、近隣の AP とクライアントの送信が重なる高密度環境において、Wi-Fi 6 ネットワークがより効率的に動作するようになります。無線 BSS を識別するためのカラー値（1 ～ 63 の数値）を割り当てるか、AP がカラー値 をランダムに選択するようにするために値 64 を入力します。(範囲 : 1 ～ 63、64 ランダム、デフォルト : 64)

- ブロードキャストレート — ブロードキャストパケットによって消費されるワイヤレス帯域幅に制限をかけることができます。

  - 6 GHz 無線 — オプション : 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M; デフォルト : 6M

  - 5 Ghz 無線 — オプション : 6M、9M、12M、18M、24M、36M、48M、54M、初期値 : 6M

  - 2.4 Ghz 無線 — オプション : 5.5M、6M、9M、11M、12M、18M、24M、36M、48M、54M、初期値 : 5.5M

- Target Wake Time — 802.11ax（Wi-Fi 6）モードでは、AP は、クライアントが定期的なビーコンに依存するのではなく、フレームを送信または受信するために特定の Target-Wakeup Time（TWT）を要求できるようにできます。この機能により、クライアントデバイスのスリープ状態を大幅に延長でき、大幅な省電力化を実現します。また、AP はクライアントの TWT を制御してスケジュールすることで、ネットワーク内の競合を管理し、遅延に敏感なトラフィックに対応できます。(デフォルト : 無効)

- OFDMA — 802.11ax（Wi-Fi 6）モードは Orthogonal Frequency Division Multiple Access (OFDMA) をサポートし、これを無効にすることはできません。

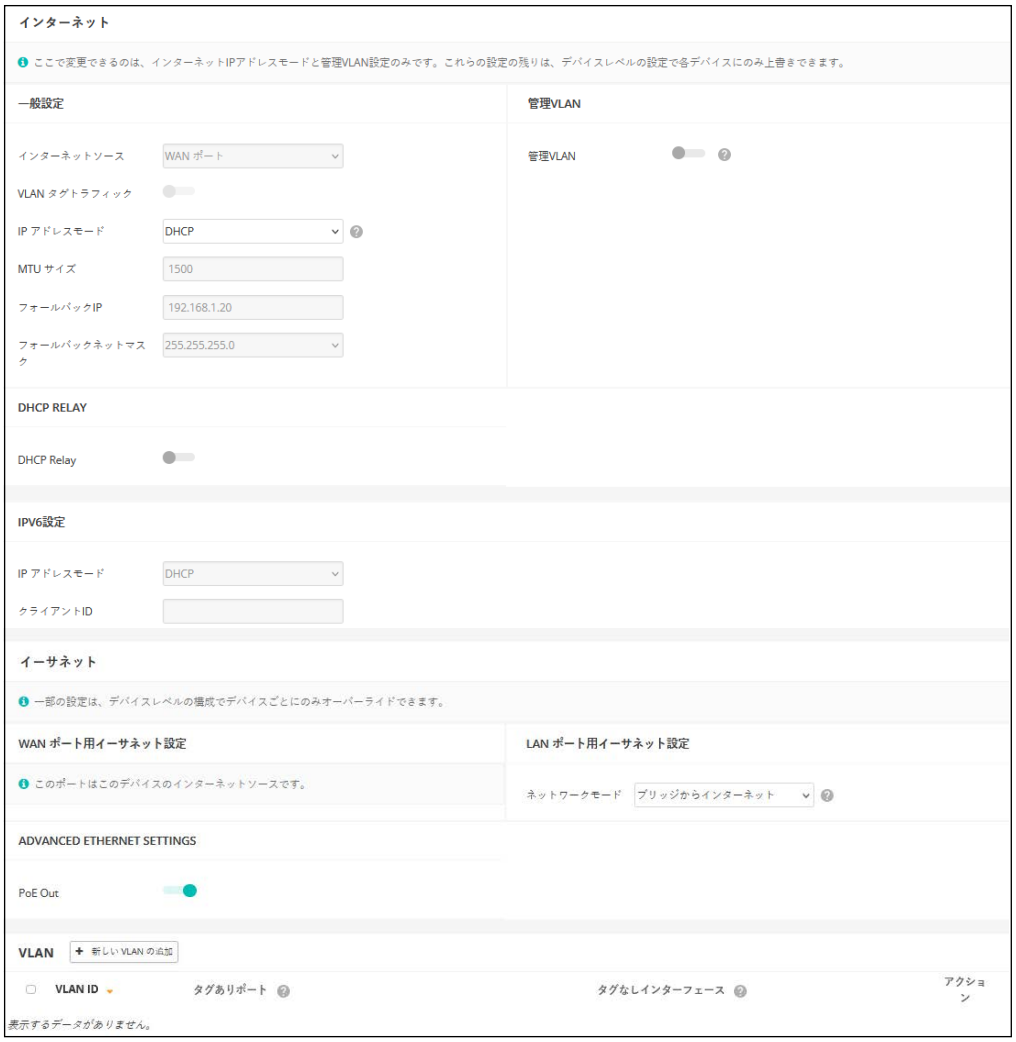
高度な無線設定

- プローブ要求データプッシュ — クライアントの無線に対してのプローブリクエストデータを受け取れるようになります。使用可能になると、クライアントプローブリクエストデータを、無線が JSON フォーマットにして、指定の URL に送信します。

一般的なネットワーキングの設定

“WiFi アクセス “ ページの “ 一般的なネットワーキング “ タブをクリックして、サイトの全てのデバイスの、インターネット、イーサネットポート、VLAN 設定を設定します。デバイスによっては、現在の設定を表示するのみで、設定を変えることができないかもしれません。ここで設定を変えることができないデバイスは、デバイスレベルの設定でのみ書き換えができます。

図 163: 一般的なネットワーキング設定



インターネットの設定

このページでは、インターネットの IP アドレスモードと、管理 VLAN の設定のみ変えることができますその他の設定は、固有のデバイスに対して一件ずつ対応しなくてはいけません。デバイスレベルの設定でのみ書き換えられます。

図 164: インターネットの設定

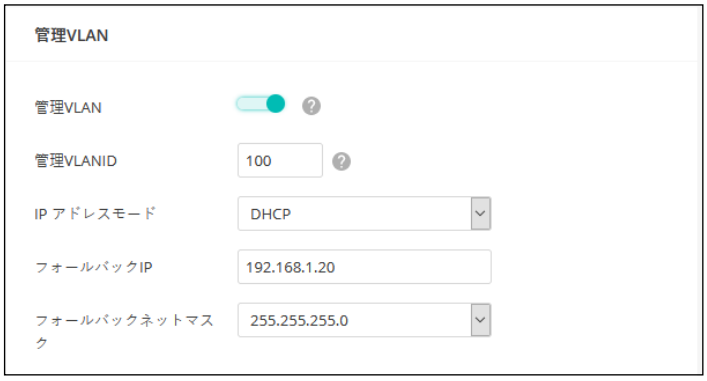
このページでは下記のアイテムを説明します。

一般設定

- インターネットソース — インターネットにアクセスに使用されるデバイスのインターフェースです。
- VLAN タグ トラフィック — このインターフェースでタグ付けを有効にし、2 から 4094 までのタグ付け ID 値を選択します。
- IPアドレスモード—インターネットアクセスポートにIPアドレスを提供する方法です。(DHCP を使うか、デバイスの設定を使うことができます。デフォルトは DHCP です)。
  - DHCP— インターネットへの接続を可能にします。
  - デバイスの設定を使用する—登録の前にデバイスに対して静的IP を使用することを考えているなら、このオプションを選択して ください。また、静的 IP と DHCP ベースのモードを混合して使用する場合もこれを選択してください。デフォルトでは特別に設定されていない場合は DHCP を使用します。
- MTU サイズ — ネットワークで送信するパケットの、最大限の伝送ユニット（ MTU）を設定してください。
- フォールバック IP — デバイスの IP アドレスにアクセスできない場合は、この IP アドレスが使用されます。
- フォールバックネットマスク — フォールバック IP アドレスと関連するネットワークマスクです。

管理 VLAN の設定

図 165: 管理 VLAN の設定



- 管理 VLAN— このオプションを選択すると、サイトのデバイスの管理 VLAN が使用できるようになります。一度このオプションを使用すると、二度とデバイスに内蔵されたローカルネットワーク（例えば 192.168.2.1）にアクセスができなくなります。特定の VLAN ネットワークを使ってのみデバイスにアクセスが可能になります。もしデバイスの IP が DHCP に設定されている場合は、VLAN ネットワークのサブネット範囲の新しい IP アドレスが必要になります。

- 管理 VLAN ID— 管理 VLAN の ための ID です。

- IP アドレスモード —管理 VLAN を介してデバイスに IP アドレスを提供する方法です。（オプションは DHCP と静的 IP がありま す。デフォルトは DHCP です）。

  - DHCP — 管理 VLAN が使用できるようになります。

  - 静的 IP— サイトのデバイスに管理 VLAN を介してアクセスできるように、静的 IP、サブネットマスク、デフォルトゲートウエイアドレスを設定してください。

- フォールバック IP — DHCP アドレスが使用できない場合に管理 VLAN を介してデバイスと接続するために使用できる IP アド レスです。

- フォールバックネットマスク — フォールバック IP アドレスに関連するネットワークマスクです。

DHCP Relay 設定

DHCP Relay が有効な場合、AP はすべてのクライアントのエージェントとして機能し、すべてのブロードキャスト DHCP 要求を指定された DHCP サーバーに直接送信します。DHCP サーバーの IP アドレスとポートを設定し、オプションでバックアップサーバーを設定する必要があります。

図 166: DHCP Relay

このページでは、以下の項目が表示されます：

- DHCP Relay — AP の DHCP リレー機能を有効にします。
- DHCP Relay Server — DHCP サーバーの IP アドレスを指定します。
- DHCP Relay Port — DHCP サーバーのポートを指定します。
- Backup DHCP Relay — オプションで、プライマリサーバーからの応答がない場合に使用するバックアップ DHCP サーバーの IP アドレスとポートを指定します。
- リモート ID — ホスト名をリモート ID として使用するか、テキスト文字列をリモート ID として手動で設定します。

IPV6 設定

図 167: IPv6 設定

この部分には、次の項目が表示されます：

- IP アドレスモード — インターネットアクセスポートに IPv6 アドレスを提供するために使用する方法です。(デフォルト：DHCP、オプション：DHCP、静的 IP)。
  - DHCP — DHCP を構成する場合、クライアント ID を指定する必要があります。

- クライアント ID — DHCP のクライアント ID を手動で入力します。

- 静的IP — インターネットアクセスポートに静的IPv6アドレスを設定する場合は、以下の項目を指定する必要があります。

  - IP アドレス — アクセスポイントの IPv6 アドレスを指定します。IPv6 アドレスは、RFC 2373 に従って、8 つのコロンで区切られた 16 ビット 16 進数を使用して構成する必要があります。未定義のフィールドを埋めるために必要な適切な数のゼロを示すために、アドレス内で 1 つのダブルコロンを使用できます。

  - デフォルトゲートウェイ — 要求された宛先アドレスがローカルサブネット上にない場合に使用される、デフォルトゲートウェイの IPv6 アドレス。

  - サーバー — ネットワーク上のドメイン・ネーム・サーバーの IPv6 アドレスです。DNS は、数値の IPv6 アドレスをドメイン名にマッピングし、IPv6 アドレスの代わりに馴染みのある名前でネットワークホストを識別するために使用できます。ローカルネットワークに DNS サーバーがある場合は、IPv6 アドレスをテキストフィールドに入力してください。

イーサネットの設定

このセクションはサイトの AP のための、基本的なイーサネットの設定について説明します。この設定は、デバイスの設定の、デバイスごとの設定においてのみ上書きできます。

図 168: イーサネットの設定

このセクションでは下記のアイテムを説明します。

WAN ポート用イーサネット設定

デフォルトでは、WAN ポートインターフェースはインターネットソースとして設定されており、“ このポートは当サイトのデバイスのインターネットソースです “ と表示されています。

もし複数のインターフェースがインターネットに接続されている場合、最後に設定されたインターフェースが使用されます。

LAN ポート用のイーサネット設定

- ネットワークモード — ネットワークの接続方法（LAN ポートの使用方法）を表示します。

ADVANCED ETHERNET SETTINGS

- PoE Out — PoE ソースが 802.3at として検出された場合に PoE Out機能を有効にし、それ以外の場合は PoE Out 機能を無効にします。Off に設定すると、PoE Out は常に無効となります。

VLAN の設定

アクセスポイントが VLAN タギングを利用すると、ネットワークリソースへのアクセスを制御し、セキュリティを強化できます。LAN はアクセスポイント間のトラフィック、関連するクライアント、有線ネットワークを分離し最大 12 の VLAN タグ付きネットワークを作成できます。

VLAN（仮想ローカルエリアネットワーク）はデフォルトでは OFF の状態です。ON の状態になると、関連する VAP（仮想アクセスポイント）からイーサネット（Ethernet）ポートに伝達されたパケットに自動的にタグ付けされます。特定の VAP は VLAN のタギングを有効／無効にできるので注意してください。

アクセスポイントの VLAN サポートについては、下記に注意してください。

- イーサネット LAN ポートに VLAN ID が割り当てられている場合、そのポートに入る全てのトラフィックにも同じ VLAN ID がタグ付けされる必要があります。

- アクセスポイントに関連付けられている無線クライアントも、VLAN に割り当てることができます。無線クライアントは、彼らが関連付けられている VAP インターフェースの VLAN に割り当てられます。アクセスポイントは、正確な VLAN ID にタグ付けされたトラフィックのみを、VAP インターフェース上の関連するクライアントに転送します。

- アクセスポイントで VLAN サポートが有効になっている場合、有線ネットワークに渡されるトラフィックに正確な VLANID がタグ付けされます。アクセスポイントのイーサネットポートが VLAN のメンバーとして設定されている場合、有線ネットワークから受信されたトラフィックも同じ VLAN ID にタグ付けされる必要があります。不明な VLAN ID でタグ付けされていたり、タグ付けされていないトラフィックは受信されません。

- VLAN サポートが無効になっている場合、アクセスポイントは有線ネットワークに渡すトラフィックにタグ付けをしません。また、受信したフレームの VLAN タグを無視します。

注意：アクセスポイントで VLAN タグ付けを有効にする前に、アクセスポイントで設定された VLAN ID にタグ付けされた VLAN フレームをサポートするように、ネットワークスイッチポートを設定してください。この設定がなければ、VLAN 機能が有効になった場合にアクセスポイントへの接続ができなくなります。

図 169: VLAN の設定

このセクションでは下記のアイテムを説明します。

- VLAN ID — VLAN に割り当てられた識別子です。（範囲は 2−4094 です）。
- タグありポート — VLAN に割り当てられたイーサネットポートです。オプションとしては WAN ポートと LAN ポートがあります。
- タグなしインターフェース — “SSID を設定する “ のリンクをクリックし、無線 SSID タブを開きます。次に指定した VLAN のメンバーになるよう SSID インターフェースを編集または作成します。（162 ページの「SSID を追加する」を参照してください）。
- アクション — クリックして選択し、すでに設定されている VLAN を編集または消去します。

VLAN の追加

“ 新しい VLAN の追加 “ ボタンをクリックして VLAN を作成します。

図 170: VLAN の追加

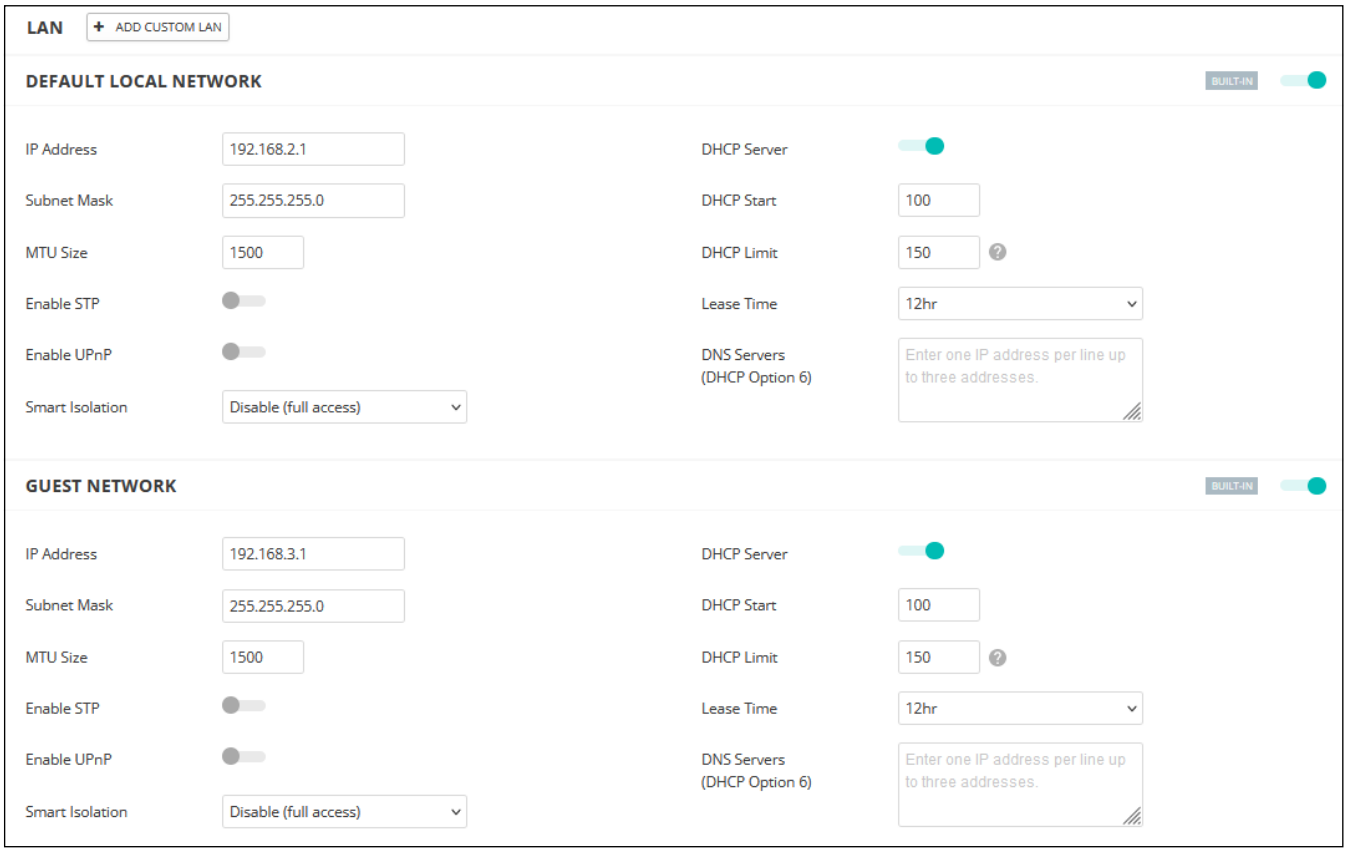
このセクションでは以下のアイテムを説明します。

- VLAN ID— 割り当てられる VLAN 識別子です。（範囲は 2−4094 です）。
- ポート —VLAN に割り当てられたイーサネットポートです。オプションには WAN ポートや LAN ポートがあります。

ローカルネットワーク設定

ローカルネットワークタブは、デフォルトの LAN ネットワーク、ゲストネットワーク、その他のカスタムネットワークの設定を設定します。

図 171: ローカルネットワークの設定



このページは以下のアイテムを説明します。

- カスタム LAN — このボタンをクリックすると、利用者用にカスタマイズされたネットワークを追加できます。最多で 10 個のカスタマイズされた LAN を作成できます。
- IPアドレス—ローカルネットワークまたはゲストネットワークのIPアドレスを決めてください。有効な IP アドレスはピリオドで区切られた、0–255 の 4 つの 10 新法の数で作成してください。(デフォルトは 192.168.2.1 です)。
- サブネットマスク — ローカルサブネットマスクのことです。(デフォルトでは 255.255.255.0 です)。
- MTU サイズ — このネットワークで送信されるパケットの最大送信単位(MTU)を設定してください。(デフォルトは 1500 です)。

- STP の有効化 — スパニングツリープロトコルメッセージの処理を有効／無効にします。
- UPnP の有効化 — ユニバーサルプラグアンドプレイブロードキャストメッセージを有効／無効にします。
- RSTP の有効化 — ラピッド スパニング ツリー プロトコル メッセージの処理を有効または無効にします。(デフォルト : 無効)
- スマートアイソレーション — ネットワークトラフィックを特定のネットワークで制限できます。
  - 無効（フルアクセス）— トラフィックは分離しません。クライアントはローカル LAN 上のインターネットやその他のデバイスにアクセスできます。もしネットワークに接続するクライアントが信頼できる人物である場合にこのオプションを選択してください。
  - インターネットアクセスのみ—このネットワークからのトラフィックは、インターネットとの間のみ送信／受信できます。このオプションはホットスポットユーザまたはゲストユーザを対象として選択してください。
  - LAN アクセスのみ — このネットワークからのトラフィックは、ローカル LAN のデバイスでのみ使用できます。
  - インターネットのみ (厳密)— このオプションは " インターネットアクセスのみ " の場合と基本は同じですが、さらに制限条件が上乗せされてお り、ユーザは、プライベートネットワーク（192.168.0.0、172.16.0.0、10.0.0.0 など）上のリソースまたはデバイスにアクセスできません。この設定は、AP が " ダブル NAT" であり、ネットワークが AP の上流にあるときに役に立ちます。
- DHCP サーバー — このネットワーク上で DHCP を有効／無効にします。（デフォルトは有効の状態です）。
  - DHCP スタート — アドレスプールの最初のアドレスです。（範囲は 1-256 です。デフォルトは xxx100 です）。
  - DHCP 制限 — アドレスプールの中で最大数のアドレスです。（範囲は 1−254 です。デフォルトは 150 です）。
  - リースタイム — 割り当てられた IP アドレスが有効である時間です。
  - DNSサーバー —最大3つの DNSサーバーIPアドレスをリストアップします。一行につき一つずつ書き出します。

ファイアーウォールの設定

ファイアーウォールフィルタリングは、侵入によるリスクを減らすために、接続するパラメーターを制限します。ファイアーウォール設定を使用すると、トラフィックを送信元と送信先の IP アドレスとポートに基づいてフィルターにかける際のルールを、順序立ててリスト化できます。入力パケットは、フィルタールールに基づいて、一つずつ検査されます。パケットがルールと一致すると、設定されたアクションが実施されます。

“ Allow-Ping“ はインターネットからの Ping パケットを許可するように前もって設定されています。このルールを有効または無効にすることはできますが、書き換えたり取り消すことはできません。“ADD RULE “ ボタンをクリックして新しいファイアーウォールルールを追加してください。

図 172: ファイアーウォールの設定

このページには以下のアイテムが表示されています。

- 有効 — 設定されたファイアーウォールを有効にします。
- 名前 — フィルタリングルールの名前を決めてください。(範囲は 1–30 文字です)。
- ソース IP アドレス —CIDR 表記の IPv4 アドレス。IP アドレスの後にスラッシュで、10 進数のネットワークマスクを定義します。
- 送信元ポート — 送信元プロトコルポートです。(範囲は 1–65535 です)。
- 宛先 IP — 送信の宛先となる IPv4 アドレスです。
- ソースポート — 送信の宛先となるプロトコルポートです。(範囲は 1–65535 です)。

- 対象 — 構成されたルールがパケットに一致したときに実行するアクションです。(オプション : Accept、Reject、Drop)
- ファミリー — IPv4 または IPv6 トラフィック、あるいは両方を指定してください。(IPv4、IPv6、全て)
- ソース — ソースとなるインターフェースです。(オプションは全て、デフォルトであるローカルネットワーク、インターネット、ゲストネットワーク、ホットスポットネットワークがあります)。
- プロトコル — パケットのプロトコルタイプを決めてください。(オプションは全て、TCP + UDP、TCP、UDP、ICMP があります)。
- 送信先 — 宛先のインターフェースです。(オプションは全て、デフォルトのローカルネットワーク、インターネット、ホットスポットネットワークです)。

ポートフォーワーディング

ポートフォーワーディングは、インバウンドプロトコルタイプ (TCP ／ UDP) とポートを、" 内部 "IP アドレスとマッピングするために使用できます。内部 (ローカル) IP アドレスは、ネットワークのエッジにあるローカルデバイスに割り当てられた IP アドレスであり、外部 IP アドレスは、AP 内部に割り当てられた IP アドレスです。これらのことにより、リモート ユーザが、単一のパブリック IP アドレスを使用して、ローカルネットワーク上の様々なサーバーにアクセスできるのです。

パブリック IP アドレスを介してローカルサイトでウエブや FTP などのサービスにアクセスするリモートユーザは、ほかのローカルサーバーの IP アドレスと TCP ／ UDP ポート番号にリダイレクト (マッピング) されます。例えば、プロトコル／外部ポートを TCP ／ 80 (HTTP または Web) に設定し、宛先 IP ポートを 192.168.3.9/80 に設定すると、外部ユーザからの全ての HTTP リクエストは、ポート 80 で 192.168.3.9 に転送されます。したがっ て、ISP から提供された外部 IP アドレスを使用するだけで、インターネットユーザはリダイレクト先のローカルアドレスで、必要なサービスにアクセスできるのです。

より一般的な TCP サービスポート番号は、HTTP : 80、FTP : 21、Telnet : 23、POP3 : 110 があります。

図 173: ポートフォーワーディング

このページは以下のアイテムを説明します。

- 有効 — ポート転送を有効にします。
- 名前 — ユーザを定義する名前（範囲は 1–30 文字です）。
- プロトコル — ポート転送が適用されるプロトコルタイプを設定してください。（オプションは TCP、UDP、TCO ＋ UDP があります）。
- 外部ポート—インターネットトラフィックの TCP／UDP ポート番号です。（範囲は 1–65535 です）。
- 送信先 IP アドレス — ローカルネットワーク上の宛先 IP アドレスです。
- ソースポート — 送信の宛先プロトコルポートです。（範囲は 1–65535 です）。

ARP インスペクション

ARP Inspection は、Address Resolution Protocol パケットの MAC Address バインディングを検証するセキュリティ機能です。これは、ある種の「中間者」攻撃の基礎となる、無効な MAC-IP アドレスバインディングを持つ ARP トラフィックに対する保護を提供します。これは、すべての ARP リクエストとレスポンスを傍受し、ローカル ARP キャッシュが更新されるか、パケットが適切な宛先に転送される前に、これらのパケットのそれぞれを検証することによって実現されます。無効な ARP パケットはドロップされます。

図 174: ARP インスペクション

このページでは、以下の項目が表示されます：

- ARP Inspection の有効化 — 有効にすると、ARP パケットは ARP スプーフィングに対して検証されます。
- Force DHCP — AP が MAC/IP ペア情報のみを学習することを許可します。AP が DHCP パケットを介して MAC/IP ペア情報のみを学習できるようにします。静的 IP アドレスで設定された機器は、DHCP パケットを送信しないため、DHCP パケットを送信することはありません。DHCP トラフィックは、静的 IP アドレスを持つクライアントは、AP によってブロッ

クされます。その MAC/IP ペアは、静的トラストリストにリストされ、有効になっています。

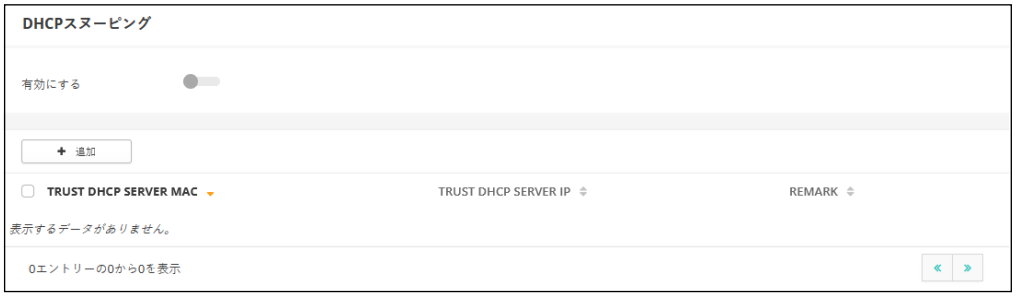
- Trust List Broadcast — 他の AP が信頼できる MAC/IP ペアを学習して、ARP 要求を発行できるようにします。
- Static Trust List — ARP 要求を発行するために信頼されるデバイスの MAC または MAC/IP ペアを追加します。他のネットワークノードは ARP 要求を送信できますが、その IP が異なる MAC で静的リストに表示されている場合、その ARP 要求はドロップされます。

DHCP スヌーピング

DHCP snooping は、AP が受信した DHCP メッセージの検証およびフィルタリングに使用されます。DHCP snooping が有効な場合、DHCP snooping テーブルに記載されていないデバイスから受信した DHCP メッセージは、ドロップされます。

MAC アドレスと IP アドレスを指定することで、既知の信頼できる DHCP サーバーをテーブルに追加できます。

図 175: DHCP スヌーピング



このページでは、以下の項目が表示されます：

- 有効 — DHCP スヌーピングを有効にします。
- Trust DHCP Server MAC — 既知で信頼できる DHCP の MAC アドレスです。
- Trust DHCP Server IP — 既知の信頼できる DHCP サーバーの IP アドレスです。
- Remark — 設定された DHCP サーバーに関連するコメントです。

ホットスポットの設定

ホットスポットの設定のページは、コーヒーショップ、図書館、病院などでの一般の人々のインターネットアクセスの設定を説明します。特定のアクセス権は、RADIUS サーバーを介し決定できます。

ホットスポットサービスを設定する際には、無線 SSID の設定ページに移動して、SSID インターフェースでの Network Behavior として、“ ホットスポットで制御する “ を選択しなくてはいけません。(160 ページの「無線 SSID の設定」を参照してください)。

一般設定

ホットスポットページの一般設定セクションでは基本的なホットスポットモードを設定できます。

図 176: ホットスポットの一般設定

このセクションは以下のアイテムを説明します。

- ホットスポット有効化—ホットスポットサービスを有効／無効にします。

  以下のホットスポットモードを選択してください。(ホットスポットモードは 1.1.4 以降のファームウェアに対して静的に “ エクスターナルポータル “ として設定されます。この設定を有効に利用するには、1.1.4 以降のファームウェアにアップグレードしてください)。

  - 外部キャプティブポータルサービス　このオプションはホットスポットゲストに、外部でホストされているキャプティブポータルスプラッシュページを表示し、(サービス設定の設定によって異なりますが)、ログインを誘導する場合があります。サードパーティキャプティブポータルサービスプロバイダーにサインアップしている場合は、このオプションを選択してください。

  - 認証なし — このオプションは、ホットスポットのゲストに、カスタマイズされた、ローカルホストのキャプティブポータルスプラッシュページを表示します。ゲストはログインすることなくインターネットにアクセスできます。もしオプションである利用規約のテキストを記

入した場合、ゲストがインターネットにアクセスする前にこの規約に同意する必要が生じます。

- シンプルなパスワードのみのスプラッシュページ—このオプションでは、ホットスポットゲストに、カスタマイズされたローカルホストのキャプティブポータルのスプラッシュページを表示しますが、ログインしてインターネットにアクセスする際に簡単なパスワードを入力する必要があります。（オプションである）利用規約に記入すると、ゲストがインターネットにアクセスする前に、この規約に同意する必要が生じます。

- 外部 RADIUS を使用したローカルスプラッシュページ— このオプションでは、カスタマイズされた、ローカルホストのキャプティブポータルスプラッシュページを、ホットスポットゲストに表示できます。しかしゲストは、ログインしてインターネットにアクセスするために、有効な RADIUS ユーザ名とパスワードを入力する必要があります。（オプションである）利用規約のテキストを記入する場合、ゲストがインターネットにアクセスするために、この規約に同意する必要が生じます。

- 外部 RADIUS 付きリモートスプラッシュページ - これは AuthPort アドオン機能です（74 ページの「AuthPort アドオンを使用する」を参照）。ホットスポットは外部スプラッシュページにリダイレクトされ、外部 RADIUS サーバーで認証されます。

- スマートアイソレーション — ネットワークトラフィックが特定のネットワークに対して制限される設定です。

  - 無効（フルアクセス）— トラフィックの分離はありません。クライアントは、ローカル LAN 上のインターネットやその他のデバイスにアクセスできます。ネットワークに接続するゲストが信頼できる人物である場合の選択肢です。

  - インターネットアクセスのみ — このネットワークからのトラフィックは、インターネットとの間でのみ通信できます。ホットスポットユーザやゲストネットワークに接続しているユーザのためのオプションです。

  - LAN アクセスのみ — このネットワークからのトラフィックは、ローカル LAN デバイスにのみ通信できます。

  - インターネットのみ（厳密）—“ インターネットアクセスのみ “ と基本的に同じですが、さらに条件が上乗せされます。ユーザは、プライベートネットワーク（192.168.0.0、172.16.0.0、10.0.0.0 など）上のリソースまたはデバイスにアクセスできません。これは AP が “ ダブル NAT“ であり、AP のゲートウエイの上流のネットワークが、別のプライベートネットワークである場合に役に立ちます。

ネットワークの設定

ホットスポットページのネットワークの設定セクションでは、ホットスポットサービスのためのローカルネットワークの設定を説明します。

図 177: ホットスポットネットワークの設定

このセクションは以下のアイテムを説明します。

- IP アドレス — ホットスポットの IP アドレスを決めてください。有効な IPv4 アドレスは、ピリオドで区切られた 0–255 の 4 つの 10 進法数で構成されます。（デフォルトは 192、168、182、1 です）。
- ネットマスク —関連付けられた IP サブネットのネットワークマスクです。このマスクは、特定のサブネットへの通信に使われるホストアドレスビットを識別します。
- DHCP ゲートウエイ — DHCP サーバーにアクセスするために使用するゲートウエイです。
- DHCP ゲートウエイポート — DHCP サーバーへのアクセスに使用される UDP ／ TCP ポートです。
- DNS1— ネットワーク上のプライマリードメインネームサーバーの IP アドレスです。DNS は IP アドレスの数値をドメイン名にマッピングするので、IP アドレスの代わりに、使い慣れた名前でネットワークホストを識別できるようになります。
- DNS2 — DHCP クライアントが利用できる補助的な DNS サーバーです。
- DNS ドメイン名 — ドメインネームシステムを介して、不完全なホスト名を解決するために使用されるドメイン名です。

DHCP サーバー

ホットスポットページの DHCP サーバーセクションでは、ホットスポットサービスの DHCP アドレスプールを設定します。

図 178: ホットスポット DHCP サーバーの設定

このセクションでは以下のアイテムを説明します。

- DHCP スタート — アドレスプール内の（最後の数値フィールドの）最初の番号です。（範囲は 1–254 です。デフォルトは 10 です）。
- DHCP 限度 — アドレスプール内の（最後の数値フィールドの）終了番号です。（範囲は 1–245 です。デフォルトは 245 です）。
- リースタイム —IPアドレスがDHCPクライアントに割り当てられている時間です。（範囲は 600–43200 秒です。デフォルトは 3600 秒です）。

RADIUS サーバー

ホットスポットページの RADIUS サーバーセクションは、ホットスポットサービスの RADIUS サーバーを設定します。

図 179: ホットスポット RADIUS サーバーの設定

このセクションでは以下のアイテムを説明します。

- RADIUS 認証を有効にする — キャプティブポータルにアクセスしようとしているクライアントの RADIUS 認証を有効にします。
- RADIUS サーバーアドレス — プライマリーRADIUS サーバーの IP アドレスまたはホスト名です。
- バックアップRADIUSサーバーアドレス —補助的なRADIUSサーバーのIPアドレスまたはホスト名です。
- RADIUSサーバー共有シークレット—アクセスポイントとRADIUSサーバー間のメッセージを暗号化するために使用される共有テキスト文字列です。RADIUS サーバーで同じ文字列が明示されていることを確認してください。文字列に空白を使用しないでください。（範囲は 1–255 文字です）。
- RADIUS サーバーauth ポート — 認証メッセージに使用される RADIUS サーバーの UDP ポートです。（範囲は 1–65535 です。デフォルトは 1812 です）。

- RADIUS サーバーアカウンティングポート—アカウンティングメッセージに使用される RADIUS サーバー UDP ポートです。（範囲は 1－65535 です。デフォルトは 1813 です）。

- RadSecの有効化—TCPやTLSを介してRADIUSデータグラムを転送するための認証及び承認プロトコルです。RadSec は、初期の RADIUS デザインで使用されていた UDP に代わるものであり、信頼できるトランスポートプロトコルとパケットペイロードに対してのより広範囲のセキュリティを提供します。

- 認証方法 —APとRADIUSサーバー間のメッセージのために使用する暗号化の方法を CHAP、PAP、MS-CHAPV2 から選択してください。暗号化の方法は、RADIUS サーバーで使用されている方法と一致しなければいけません。

- ローカル ID — ローカル RADIUS サーバーの識別子です。

- ローカル名 — ローカル RADIUS のサーバー名です。

- NASID の生成 — このオプションは、このサイトの各デバイスに固有の NAS ID を生成します。

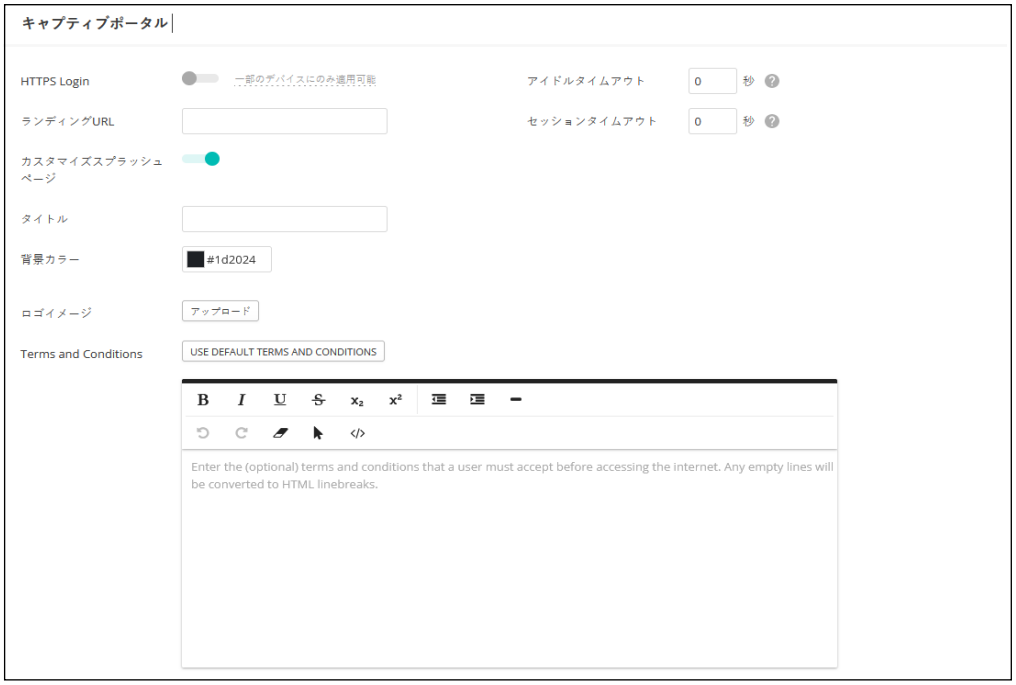
- NAS ID — ローカル RADIUS サーバー操作の識別子です。

キャプティブポータル

ホットスポットページのキャプティブポータルセクションでは、ホットスポットサービスでのポータルの詳細を設定します。

キャプティブポータルは、ホットスポットクライアントがウエルカム web ページにアクセスする前に、インターネットへのアクセスを強化するように誘導します。ウエルカムページへのアクセスは認証や支払いが必要の場合があります。

図 180: ホットスポットキャプティブポータルの設定



選択肢たホットスポットモードによって異なりますが、このセクションでは下記のアイテムが表示されます。

全てのモードに共通するアイテム

- ランディング URL — キャプティブポータルにログインした後にユーザが誘導される URL です。
- アイドルタイムアウト — アクティブでない状態で接続を保持できる最大値です。(範囲は 0−86400 秒です)。
- セッションタイムアウト — クライアントがホットスポットにログインした状態を保持できる最長時間です。(範囲は 0−86400 秒です)。

外部キャプティブポータルサービス、外部 RADIUS によるリモートスプラッシュページを除く全モード共通。

- HTTPS ログイン - キャプティブの HTTPS を有効にします。

外部のキャプティブポータルサービスを除いた全てのモードに共通するアイテム

- カスタマイズスプラッシュページ — 有効になると、ローカルのキャプティブポータルのウエルカムページを作成するために必要な情報を入力できるようになります。
  - タイトル — ページのタイトルとして表示したいテキストを入力してください。
  - 背景カラー — ボタンをクリックして背景となる色を選択してください。
  - ロゴイメージ — “アップロード“ボタンをクリックして画像ファイルを送信してください。ファイルのサイズは 1MB に制限されています。また、画像の高さは 1000 ピクセルまでである必要があります。
  - Terms and Conditions — キャプティブポータルの契約条件を定義するテキストをウインドウに入力し、コントロールを使用してフォーマットを調整してください。または、“ USE DEFAULT TERMS AND CONDITIONS “ ボタンをクリックしてインポートしたテキストを必要に応じて編集し、使用します。

外部のキャプティブポータルサービスモード

- キャプティブポータルURL—ホットスポットインターネットサービスのホスト名です。
- キャプティブポータル秘密鍵 — ホットスポットでのログインに使用されるパスワードです。
- Octetsを交換する— “入力オクテット“と“出力オクテット“の数値を交換します。

シンプルなパスワードのみのスプラッシュページモード

- スプラッシュページのパスワード — ユーザがログインしてインターネットにアクセスする際に必要なパスワードです。

認証の除外

ホットスポットページの認証の除外ページでは、ホットスポットサービスの“ウォールド・ガーデン“とホワイトリストを設定します。

図 181: ホットスポットでの認証の除外

このセクションでは以下のアイテムが表示されます。

- ウォールド・ガーデン — ホットスポットユーザがキャプティブポータルに認証される前にアクセスが可能なドメインや IP アドレスのリストを、CIDR 表記で入力してください。ワイルドカードドメインは domain.com のフォーマット（ドメインと全てのサブドメインを許可）または .domain.com のフォーマット（サブドメインのみを許可）を指定してください。
- 認証ホワイトリスト — キャプティブポータルを経路としてインターネットにアクセスできる MAC アドレスのリストです。

システムの設定

システムの設定ページでは、AP へのリモート管理アクセスを制御し、NTP タイムサーバーを設定できます。Telnet、Web、SNMP 管理イン ターフェースが有効になっているので、インターネットからアクセスできます。セキュリティ強化のために、特定のサービスを無効にして、インターネットからの管理アクセスを防ぐこともできます。

一般設定

システムの設定ページの一般設定セクションを使用すると、クラウドステータス LED、リセットボタン、タームゾーンを設定できます。

図 182: 一般的なシステムの設定

このページでは以下のアイテムが表示されます。

- Enable LEDs — ECW5211、ECWO5211、OAP100、Spark Wave 2/ SunSpot Wave 2 で 3.0.0+ ファームウェアを実行している場合のみサポートしています。無線が有効で正常に動作している場合、LED は点灯しています。
- リセットボタンを有効にする — ハードウエアリセットボタンを有効または無効にします。リセットボタンはサイトでは無効にできないので注意してください。
- タイムゾーン — 現地時間に対応する時間を表示するには、プルダウンリストが表示するタイムゾーンを選択してください。
- ブート再試行の回数 — 次のブートバンクに切り替えるまでのブートアップの再試行の最大数です。(範囲は 1−254 です。デフォルトは 3 です)。
- MSP モード — エンドユーザがユーザ定義のユーザアカウントからほとんどのデバイス設定にアクセスし、変更することを防ぐ Managed Service Provider (MSP) モードを有効にできます。root」と「admin」アカウントからの管理アクセスは、すべてのデバイス設定へのフルアクセスを提供します。(初期値：無効)

  MSP モードを有効にすると、サービスプロバイダーは、「ローカル設定可能」設定を有効にすることで、特定の無線 SSID 設定をユーザ設定に利用できるようにするオプションがあります。

注意：MSP モードと " 常にクラウド設定に従う "（page 65）を同時に有効にしないでください。この場合、デバイスの設定が ecCLOUD に正しく更新されなくなります。

- Mgmtd Log Level — メニューを使用して、ecCLOUD デーモン (mgmtd) のシステムログレベルの重大度を選択します。選択した重大度レベルのログと、それ以上の重大度のすべてのログが記録されます。例えば、Debug を選択した場合、ログに記録されるメッセージには Debug、Informational、Warning、および Error が含まれます。デフォルトの重大度レベルは Informational(2) です。重要度は以下のレベルのいずれかになります：

表 1: 管理デーモンのログレベル

レベル	重大度名	概要
4	トレース	システムの相互作用、状態変化、ネットワーク通信に関する詳細な情報
3	デバッグ	デバッグメッセージ
2	インフォ	情報メッセージのみ
1	警告	警告条件（例：False を繰り返す、予期せぬリターン）
0	エラー	エラー状態（無効な入力、デフォルトの使用など）

- Syslog Level — メニューを使用して、コンソールに出力するログの重大度を選択する。デフォルトの重大度レベルは Informational(6) です。重要度は以下のレベルのいずれかになります：

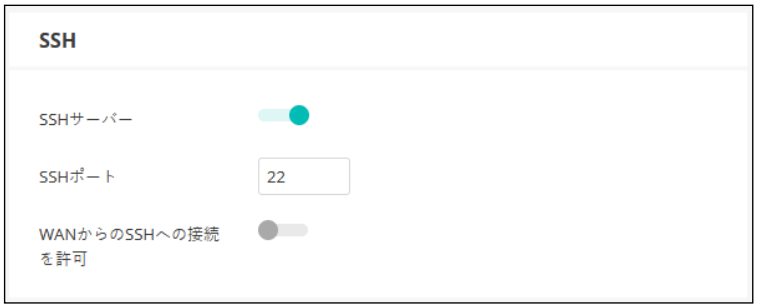
表 2: システムログレベル

レベル	重大度名	概要
7	デバッグ	デバッグメッセージ
6	インフォ	情報メッセージのみ
5	通知	コールドスタートなど、正常だが重大な状態
4	警告	警告条件（例：False を返す、予期せぬリターン）
3	エラー	エラー状態（無効な入力、デフォルトの使用など）
2	クリティカル	クリティカルな状態（例：メモリ割り当て、空きメモリエラー - リソースの枯渇）
1	アラート	早急な対応が必要
0	緊急	システム使用不能

SSH Secure Shell (SSH) は Telnet の安全な代替品として機能します。SSH プロトコルは、生成されたパブリックキーを使用して、アクセスポイントと SSH 対応の管理ステーションクライアントとの間を通過する、全ての転送されたデータを暗号化します。こうすることで、ネットワーク上を通過する データが、変換されずに宛先に届くようになります。クライアントはアクセスの認証時にローカルユーザ名と、パスワードを安全に使用できるようになります。

SSH プロトコルを介して管理業務のためにアクセスポイントにアクセスするには、SSH クライアントソフトウエアを管理ステーションにインストールする必要があるので注意してください。

図 183: SSH サーバーの設定



このページでは以下のアイテムが表示されます。

- SSH サーバー — アクセスポイントへの SSH アクセスを有効／無効にします。（デフォルトは無効です）。
- SSH ポート — アクセスポイントの SSH サーバーの TCP ポート番号を設定します。（範囲は 1 – 65535 です。デフォルトは 22 です）。
- WANからのSSHへの接続を許可 — WANからのSSH管理アクセスを許可します。

検出ツール

Edgecore Discovery エージェントを使用する と、AP を、ローカルネットワーク上の他のデバイスまたはインターネット経由で検出できます。

図 184: 検出ツールの設定

このページでは以下のアイテムを表示します。

- 検出ツール — 検出ツールを有効／無効にします。（デフォルトは有効です）。
- WAN を許可 —WAN からの検出ツールのアクセスを許可します。

ネットワークタイム

ネットワークタイムプロトコル（NTP）を使用すると、アクセスポイントは、タイムサーバー（SNTP または NTP）からの定期的な更新に基づいて、内蔵クロックを設定できます。アクセスポイントが常に時刻を維持できるので、

システムログはイベントの正確な日と時刻を記録できます。クロックが設定されていない場合、アクセスポイントは、最後の起動時の工場出荷時のデフォルトなどから時間のみを記録します。

アクセスポイントは NTP クライアントとして機能し、定期的に時刻同期要求を送信します。また、アクセスポイントは、設定された順序で各サーバーを調査し、時刻の更新を受信します。

図 185: NTP の設定

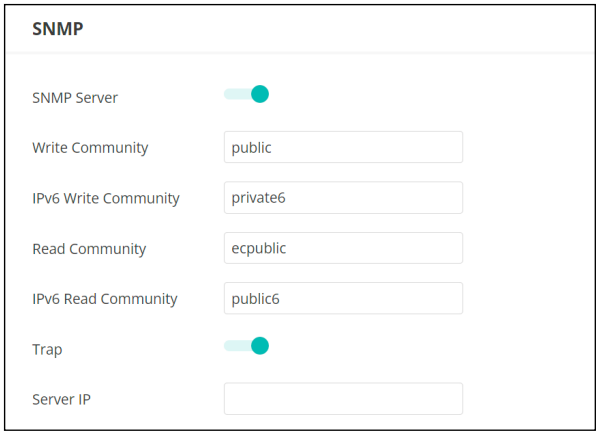
このページは以下のアイテムを表示します。

- NTP プロトコル — 時間更新の要求の送信を有効／無効にします。(デフォルトは有効です)。
- NTP サーバー — タイムサーバーのホスト名を設定します。スイッチは最初のサーバーから時刻を更新しようとしますが、これに失敗した場合は、設定された順番で次に当たるサーバーから更新します。追加のサーバーを設定するには、リストの下部にある空白フィールドにエントリーを書き込んでください。

SNMP

Simple Network Management Protocol（SNMP）は、ネットワーク上のデバイスを管理するために特別にデザインされた通信プロトコルです。これは通常、ネットワーク環境でデバイスが適切な操作を行うように設定するため、及びパフォーマンスを評価したり潜在的な問題を検出するなど、デバイスを監視するために使用されます。

図 186: SNMP の設定



このページでは以下のアイテムが表示されます。

- SNMP サーバー — アクセスポイントで SNMP を有効／無効にします。(デフォルトは有効です)。
- Write Community — パスワードのように機能し、SNMP プロトコルへのアクセスを許可するための文字列です。(範囲は 1—32 です。大文字と小文字を区別します。デフォルトは public です)。

  デフォルトの文字列 “public” は、アクセスポイントの管理情報（MIB）の読み取りのみのアクセスを提供します。
- IPv6 Write Community — アクセスポイントの管理情報（MIB）データベースへの IPv6 アクセス用のコミュニティ文字列です。(範囲 : 1-32 文字、大文字と小文字を区別します。デフォルト : private6)
- Read Community — アクセスポイントの管理情報（MIB）データベースに読み取り専用でアクセスするためのコミュニティ文字列です。(範囲 : 1-32 文字、大文字と小文字を区別します。デフォルト : public)
- IPv6 Read Community — アクセスポイントの管理情報（MIB）データベースに IPv6 読み取り専用でアクセスするためのコミュニティ文字列です。(範囲 : 1-32 文字、大文字と小文字を区別します。デフォルト : public6)
- Trap — 指定したサーバーへの SNMP トラップ メッセージの送信を有効にします。アクセス ポイントは、コールド スタート、ウォーム スタート、

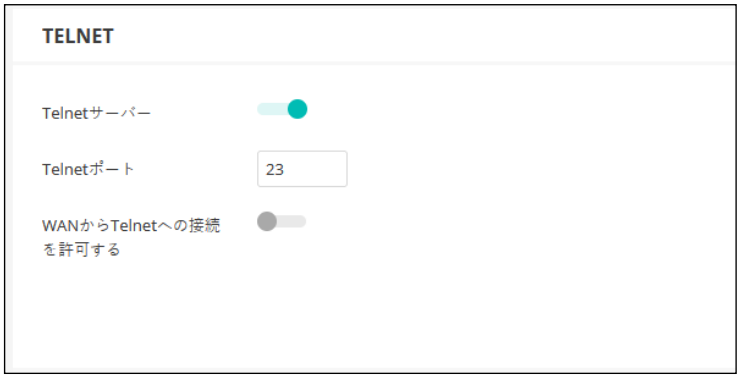
リンク アップ、およびリンク ダウンというトラップ メッセージを送信します。(デフォルト：無効)

- Server IP — トラップ・メッセージを受信する SNMP トラップ・サーバーの IP アドレスです。

Telnet

Telnet は、ネットワーク内のどこからでもアクセスポイントを設定できる管理用ツールです。ただし、Telnet は悪意のある攻撃には弱いので注意してください。Telnet はデバイスの分析とデバッグに使用されるリナックス（Linux）ベースのインターフェースへのアクセスを提供します。

図 187: Telnet サーバーの設定



このページでは以下のアイテムを表示します。

- Telnet サーバー — アクセスポイントへの Telnet アクセスを有効／無効にします。（デフォルトは無効です）。
- Telnet ポート — アクセスポイントの Telnet サーバーの TCP ポート番号を設定します。（範囲は 1－65535 です。デフォルトは 23 です）。
- WAN から TELNET への接続を許可する — WAN からの Telnet 管理アクセスを許可します

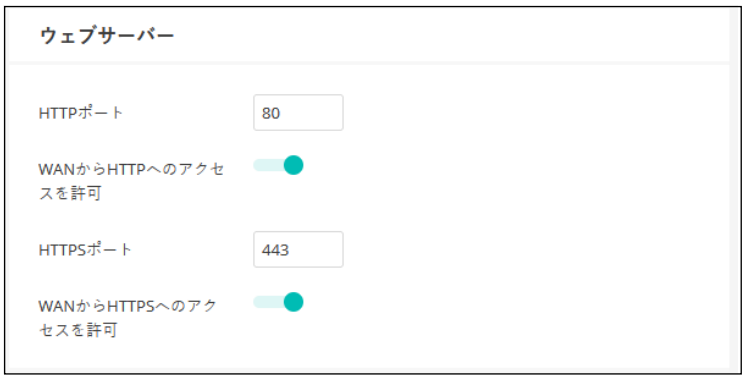
ウエブサーバー

ウエブブラウザは、アクセスポイントを管理するための主要な方法を提供します。HTTP サービスと HTTPS サービスに、個別にアクセスできます。もし HTTP を有効にする場合は、URL に https://device:port_number を入力してください。

- クライアントは、サーバーのデジタル認証を使用してサーバーを認証します。
- クライアントとサーバーは、接続に使用する一連のセキュリティプロトコルを交渉します。

- クライアントとサーバーは、データの暗号化や複合化のためのセッションキーを作成します。
- クライアントとサーバーは安全な暗号化された接続を確立します。
- ほとんどのブラウザは、ステータスバーにパッドロックアイコンが表示されます。

図 188: ウエブサーバーの設定



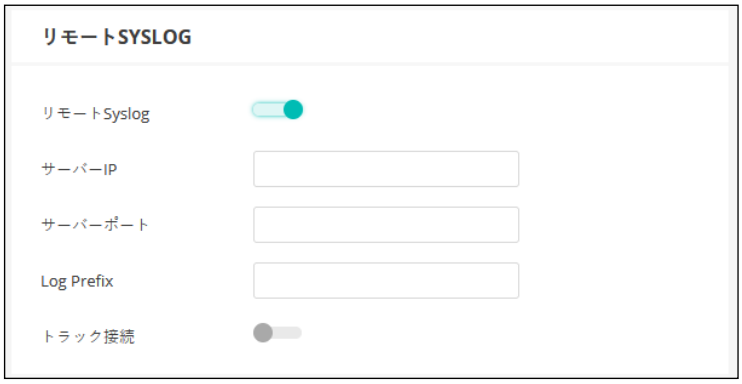
このページでは以下のアイテムが表示されます。

- HTTP ポート —HTTP ウエブブラウザインターフェースで使用される TCP ポートです。(範囲は 1–65535 です。デフォルトは 80 です)。
- WANからHTTPへのアクセスを許可 — WANからのHTTP管理目的のアクセスを許可します。
- HTTPS ポート —HTTPS ウエブブラウザインターフェースで使用される TCP ポートです。(範囲は 1–655535 です。デフォルトは 443 です)。
- WANからHTTPSへのアクセスを許可 — WANからのHTTPS管理目的のアクセスを許可します。

リモート Syslog

この機能を使用して、ログメッセージをシスログ（Syslog）サーバーに送信します。

図 189: リモートログの設定



このページでは以下のアイテムを表示します。

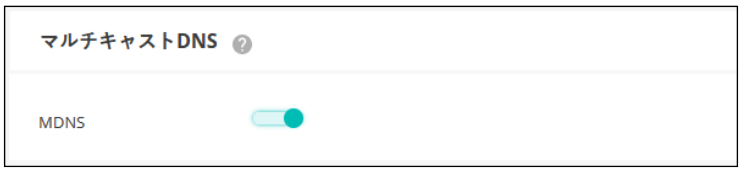
- リモート Syslog — リモートログプロセスへのデバッグ、またはエラーメッセージのロギングを有効／無効にします。
- サーバー IP— シスログ（Syslog）メッセージが送信される、リモートサーバーの IP アドレスを指定します。
- サーバーポート — リモートサーバーが使用する UDP ポート番号を指定します。（範囲は 1－65535 です）。
- Log Prefix — 指定したサーバーに送信されるログファイルのプレフィックスを設定します。ファイルサフィックス " ログ " が使用されます。
- トラック接続 — 無線クライアントの接続ログメッセージをシスログ（Syslog）サーバーに送信します。

マルチキャスト DNS

この機能を使用して、AP でマルチキャスト DNS サポートが有効にします。マルチキャスト DNS は、ホスト名をマルチキャスト IP アドレスとする DNS サーバーがない小規模なネットワークで使用できます。

マルチキャスト DNS の設定は DNS をサポートしているデバイスでのみ使用できます。

図 190: マルチキャスト DNS の設定



このページでは下記のアイテムが表示されます。

- MDNS — マルチキャスト DNS サポートを有効／無効にできます。(デフォルトは有効です)。

LLDP

LLDP（Link Layer Discovery Protocol）は、ネットワーク上の隣接するデバイスの基本情報を発見するために使用されます。LLDP はレイヤ 2 プロトコルであり、定期的なブロードキャストを使用して、送信側デバイスの情報をアドバタイズします。

図 191: LLDP 設定

このページでは、以下の項目が表示されます：

- 有効にする — APに関するLLDPアドバタイズメントを以下のように送信することを有効にします。
- Tx Interval (seconds) — LLDP アドバタイズメントの定期的な送信間隔を設定します。(範囲：5 ～ 32768 秒、デフォルト：30 秒)。
- Tx Hold (number of time(s)) — LLDP 広告で送信される TTL（time-to-live）値を下式に示すように設定する。(範囲：2 ～ 10、デフォルト：4)

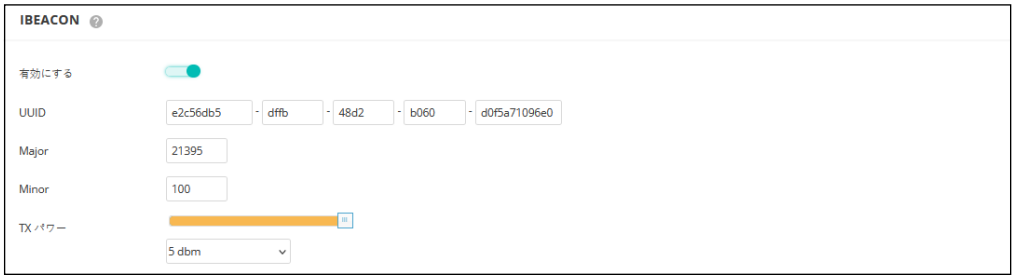
  time-to-live は、受信側の LLDP エージェントに、送信側デバイスがタイムリーに更新を送信しない場合に、送信側デバイスに関連するすべての情報を保持する期間を指示します。information

  秒単位の TTL は、以下のルールに基づいています：
  最小値（(Tx Interval * Tx Hold)、または 65535）
  したがって、デフォルトの TTL は 4*30 = 120 秒です。

iBeacon

AP は、Bluetooth Low Energy（BLE）に基づく iBeacon 規格をサポートしています。BLE ビーコンを搭載したデバイスは、ビーコン広告を認識し、提供された情報を抽出し、その内容に基づいてアクションを起こせる電話などの BLE クライアントに位置情報サービスを提供できます。

図 192: iBeacon 設定



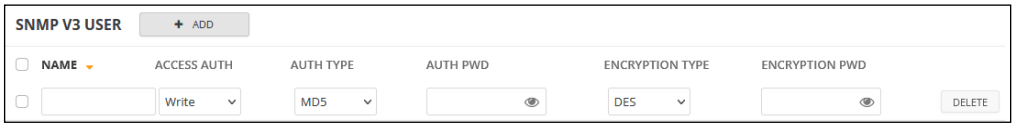
このページでは、以下の項目が表示されます：

- 有効にする — AP の iBeacon サポートを有効にします。(デフォルト : 有効にする)
- UUID — ビーコンサービスを宣伝する iBeacon Universally Unique Identifier です。UUID は、ハイフンで区切られた 5 つのグループに分かれた 32 の 16 進数で構成されています。
- Major — ビーコングループを識別するために使用される iBeacon 値です。(範囲 : 0-65535)
- Minor — グループ内の個々のビーコンを識別するために使用される iBeacon 値です。(範囲 : 0-65535)
- TX パワー — BLE 無線の送信電力を設定します (EAP101 と EAP104 でのみサポートされています)。(範囲 : 5dBm ～ -20dBm、デフォルト : 5dBm)。

SNMPv3 ユーザー

SNMP プロトコル・バージョン 3 は、アカウント認証とデータ暗号化により、安全なアクセスを提供します。SNMP v3 ユーザーは、Add ボタンをクリックして定義することができます。

図 193: SNMPv3 ユーザー設定



このページには以下の項目が表示されます：

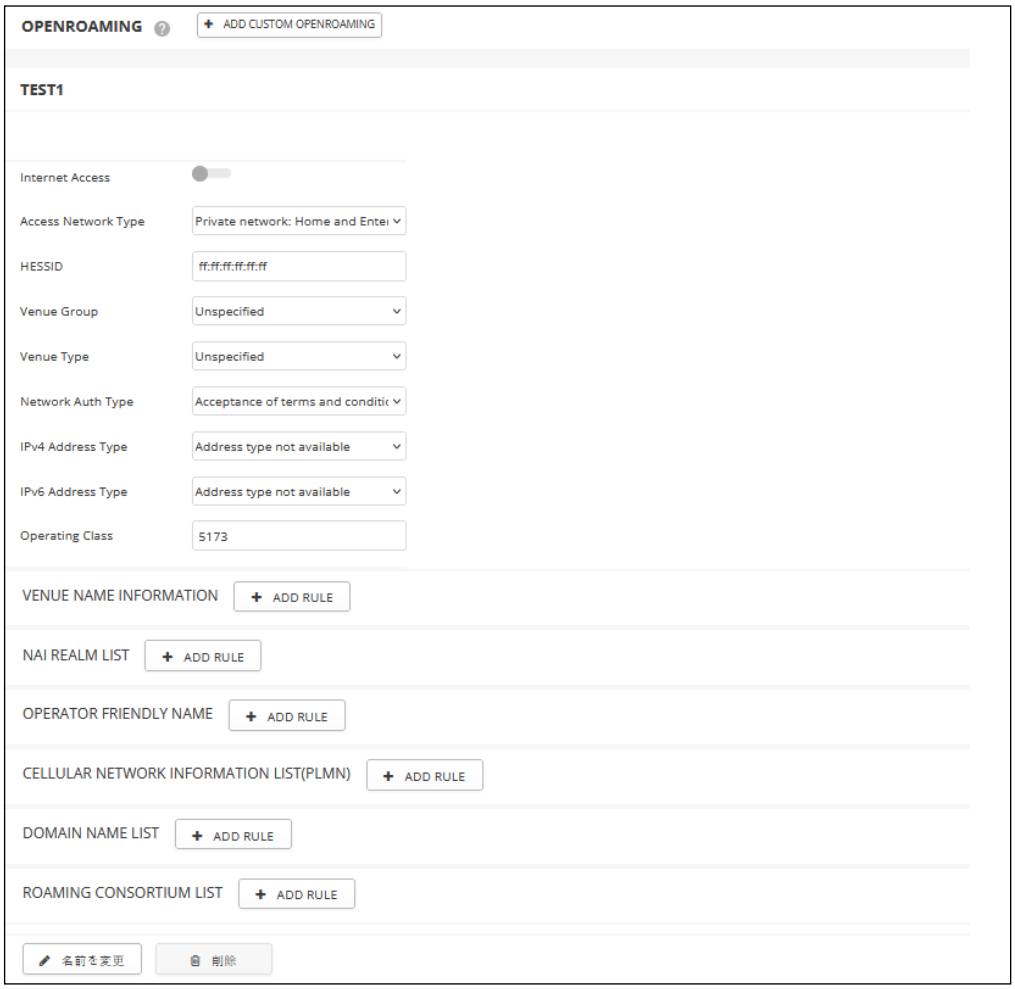
- Name — SNMP サービスへのアクセスに使用されるユーザー名です。
- Access Auth — アクセス許可を "読み取り専用 "または "書き込み専用 "から選択します。
- Auth Type — 認証用のハッシュ アルゴリズムを選択します。
- Auth Pwd — 認証用のパスワードを構成します。
- Encryption Type — データ・パケットの暗号化アルゴリズムを選択します。
- Encryption Pwd — データ暗号化のパスワードを構成します。

OpenRoaming

OpenRoaming は、無線ネットワーク間のシームレスなローミングをサポートするための公衆アクセス Wi-Fi ネットワークの標準を提供します。OpenRoaming ネットワークは、クライアントがネットワークに接続するかどうかを決定できるように、その公衆 Wi-Fi 機能とサービスをアドバタイズします。

最大 32 の OpenRoaming プロファイルを設定し、特定のワイヤレスネットワークに適用できます（162 ページの「SSID を追加する」の下の「OpenRoaming」を参照）。「カスタム Openroaming を追加」をクリックしてプロファイルを設定します。

図 194: OpenRoaming プロファイル



以下の項目が本ページに表示されます :

- Internet Access — このネットワークがインターネットへのアクセスを提供する場合に有効にします。
- Access Network Type（アクセス・ネットワーク・タイプ）— 定義済みのリストから 1 つを選択します。
  - プライベート・ネットワーク — 許可されていないユーザーがアクセスできない家庭や企業のネットワーク。
  - ゲストアクセス付きプライベートネットワーク — ゲストアクセスを提供するプライベートネットワーク。典型的な例は、ゲスト・アクセスを提供する企業ネットワークです。
  - 有料公衆ネットワーク — すべてのユーザーが利用できるが、料金が必要なネットワーク。

- 無料パブリック・ネットワーク — すべてのユーザーが無料で利用できるネットワーク。
- パーソナル・デバイス・ネットワーク — アドホック・モードの周辺機器接続用ネットワーク。例えばプリンターに接続するカメラなど。
- 緊急サービス専用ネットワーク — 緊急サービス専用ネットワーク。
- テスト — テストや実験的作業のためのネットワーク。
- Wildcard — これを選択すると、AP はクライアントのクエリで要求されたネットワークタイプに関係なくクライアントに返信します。

- HESSID — OpenRoaming ネットワークの HESSID（Homogenous Extended Service Set Identifier）。設定されると、HESSID（MAC アドレス）は同じネットワークに属するすべての AP を一意に識別します。
- Venue Group — 会場の一般的なクラスを示します。定義済みのリストから選択してください。
- Venue Type — 各グループ内の特定のタイプの会場を特定します。
- Network Auth Type — ネットワークに必要な認証を指定します。定義済みのリストからオプションを選択します。(デフォルト：「Acceptance of terms and conditions」)。
- IPv4 Address Type — ネットワークから利用可能なIPv4アドレスの種類を指定します。
- IPv6 Address Type — ネットワークから利用可能なIPv6アドレスタイプを指定します。
- 動作クラス — AP がサポートする動作チャネルを指定する標準インデックス（IEEE Std 802.11-2012 Annex E に基づく）。
- Venue Name Information — 最大 10 の会場名のリストを設定します。
  - 言語 — リストから言語を選択します。(デフォルト：英語）
  - 名前 — ネットワーク会場の名前。複数の名前をリストに追加できます。
  - URL — ユーザーに追加の会場情報を提供する URL を指定します。
- NAI Realm List — (オプション）ネットワーク・アクセス識別子（NAI）レルム・リストは、AP を介してアクセス可能なサービス・プロバイダまたはその他のネットワークを識別します。ネットワークでサポートされて

いる認証レルムを検出することで、モバイルデバイスは優先するネットワークに選択的に認証できます。最大 10 の識別子を設定できます。

- Operator Friendly Name（オペレーター・フレンドリー・ネーム）— ネットワーク・オペレーターの名前と指定言語です。最大 10 個の名前を設定できます。

- セルラーネットワーク情報リスト（PLMN）— （オプション）AP を通じて利用可能な 3GPP セルラーネットワークを識別します。具体的には、このフィールドは、移動体通信事業者の移動国コード（MCC）と移動体ネットワークコード（MNC）で構成される公衆陸上移動体通信網（PLMN）ID を識別します。最大 10 個の PLMN ID を設定できます。
  MCC、MNC のペアを入力します。
  例 : 400, 00
  MCC: 小数点以下 3 桁 (000-999)
  MNC: 小数点以下 2 桁（00 ～ 99）または 3 桁 (000-999)

- Domain Name List — AP を操作するエンティティについて、1 つまたは最大 10 のドメイン名をリストします。これは OpenRoaming ネットワーク選択ポリシーにとって重要です。モバイルデバイスがホームホットスポットにいるのか、訪問先のホットスポットにいるのかを示します。

- Roaming Consortium List — （オプション）ローミング・コンソーシアムとは、ユーザのクレデンシャルを認証に使用できるサービス・プロバイダ（SP）のグループです。各ローミング・コンソーシ アムは、IEEE が割り当てる組織識別子（OI）によって識別されます。OI の長さは 24 ビットであることが多いですが、36 ビットにすることもできます。最大 10 個の識別子を設定できます。

6 サイト Terragraph の構成

この章では、Metrolinq Terragraph ユニットの Site レベルでの構成設定について説明します。以下のセクションが含まれています：

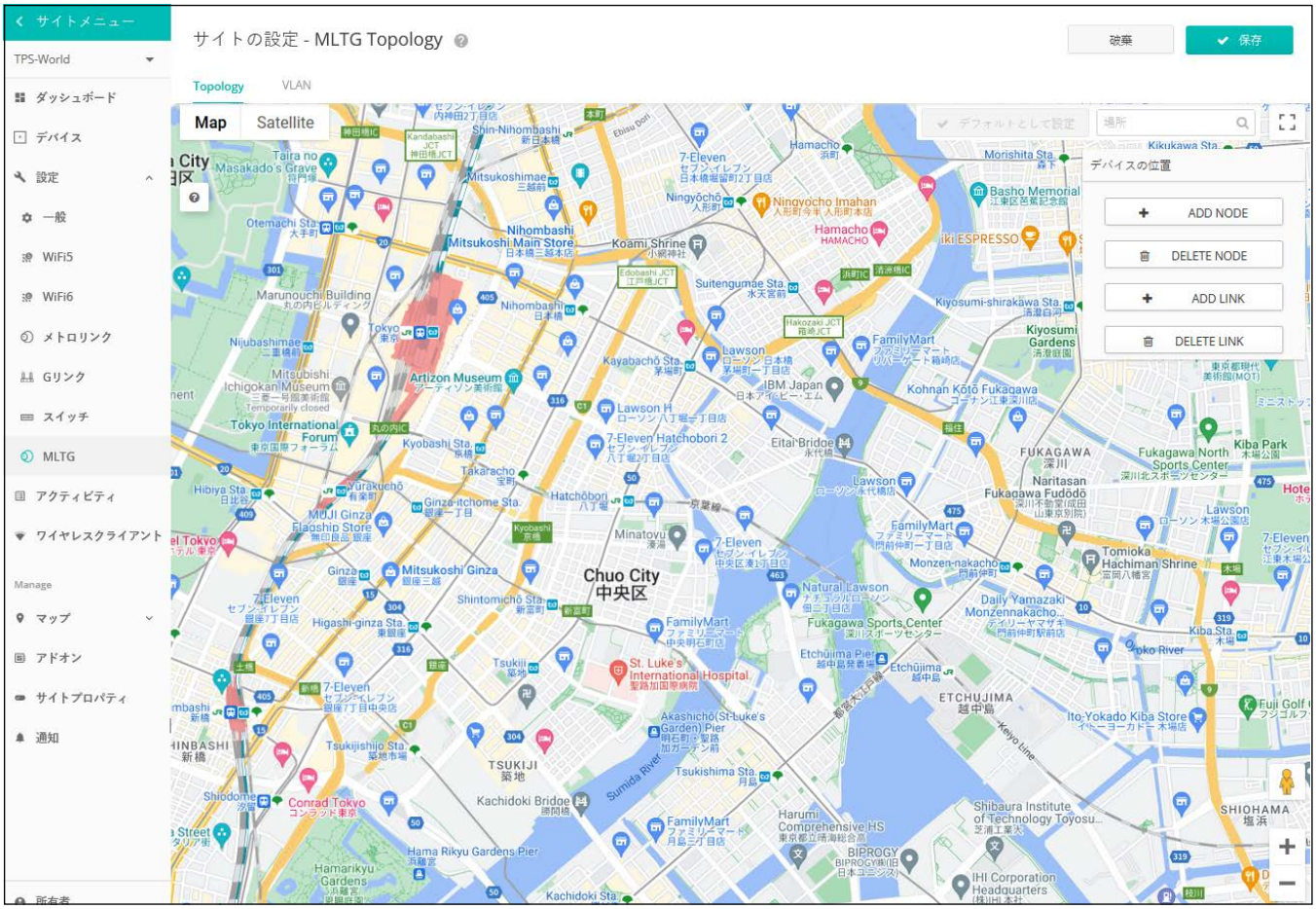
Metrolinq Terragraph の構成

Metrolinq Terragraph ユニットのネットワーク接続とトポロジーは、ローカルコントローラが有効な場合、PoP ノードで定義できます。トポ ロジーを定義した後、PoP はノードを見つけ、自動的にリンクを設定します。

注意：Metrolinq Terragraph ユニットを構成する場合は、必ず以下の点を守ってください：

1. PoP ノードをデフォルトにリセットした後、すべてのノードとリンクを削除し、サイト構成ページに再追加する必要があります。
2. デバイスを削除したり、別のサイトに移動したりする前に、必ず関連するリンクやノードをすべて削除してください。

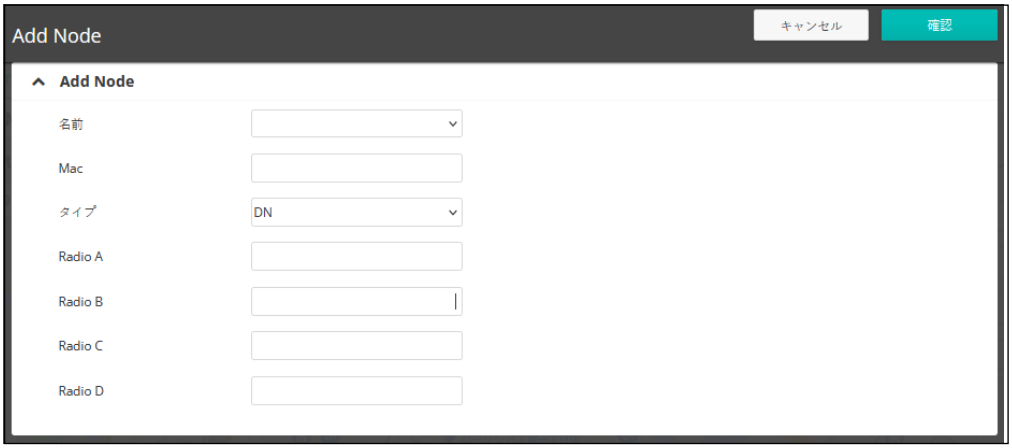
図 195: サイト Terragraph の構成



Terragraph のサイト設定画面には、以下の項目があります：

- Add Node — 対応するタイプと無線 MAC を記入して、ノードを追加します。

図 196: Terragraph ノードの追加



  - Name — ノードの名前です。ノードの種類に応じて自動的に定義されますが、後から変更することも可能です。
  - MAC — ノードのシステム MAC アドレス。DN の場合、システム MAC アドレスは、デバイスのラベルまたは Dashboard タブで確認できます。CN の場合、無線 MAC をノード MAC として使用します。
  - タイプ — ノードをディストリビューションノード（DN）またはクライアントノード（CN）に設定します。
  - Radio A/B/C/D — 無線の MAC アドレスです。
  - Pop — トポロジー内の PoP ノードは、MLTG-360 のうち 1 台のみとなります。

    なお、POP DN は "POP " という名前しか付けられない。

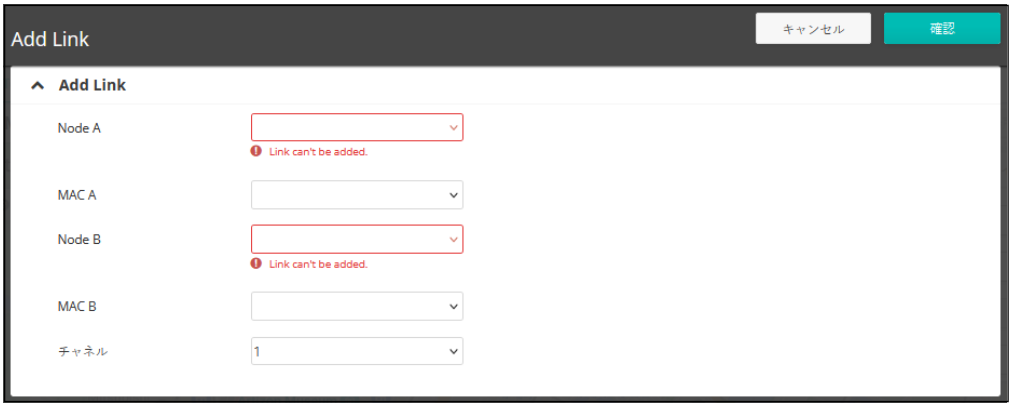
- Delete Node — トポロジーからノードを削除します。ノードを削除する前に、関連するリンクをすべて削除する必要があります。

図 197: Terragraph ノードを削除する

- Name — ノードの名前。
- MAC — ノードのシステム MAC アドレスです。

- Add Link — 2 つのノードと対応する無線 MAC を選択し、リンクを確立します。

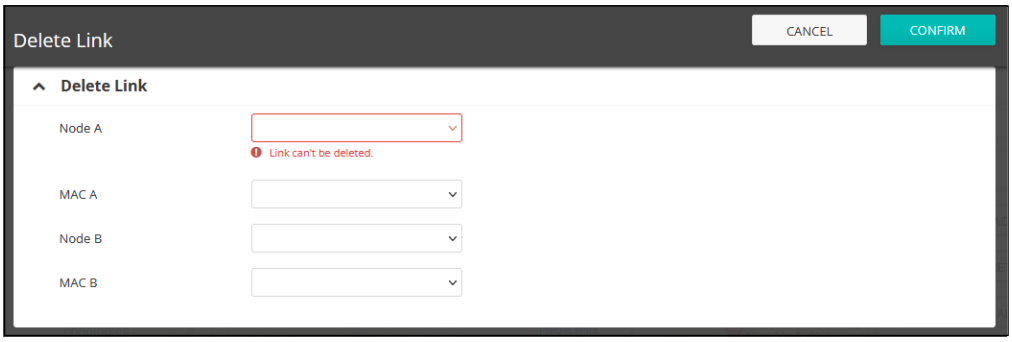
図 198: Terragraph Link を追加する



- Node A — ノード A の名称を選択します。
- MAC A — ノード A の無線 MAC アドレスを選択します。
- Node B — ノード B の名称を選択します。
- MAC B — ノード B の無線 MAC アドレスを選択します。
- Channel — 作業チャネルを選択します。チャネル 1 ～ 4 が使用可能です。

- リンクの削除 — 特定のノードペアを選択して、リンクを削除します。

図 199: Terragraph Link を削除する



- Node A — ノード A の名称を選択します。

- MAC A — ノード A の無線 MAC アドレスを選択します。
- Node B — ノード B の名称を選択します。
- MAC B — ノード B の無線 MAC アドレスを選択します。

VLAN 設定

QinQ タグは、イーサネットフレームに 2 つ目の VLAN タグを追加し、元の VLAN タグとサービスプロバイダー VLAN などの追加情報を含んでいます。これにより、ネットワーク事業者は、複数のスイッチやサービスプロバイダネットワークに VLAN を拡張し、よりスケーラブルで柔軟なネットワークアーキテクチャを構築できます。

VLAN の設定後、CN 機器の LAN 側からのデータトラフィックは、設定された S-VLAN および C-VLAN ヘッダーでカプセル化され、POP ノードのアップリンクに転送されます。

本機能は、ファームウェア 1.5.0 以上の MLTG デバイスで利用可能です。

図 200: サイト Terragraph VLAN 設定

このページでは、以下の項目が表示されます：

- 名前 — VLAN 構成を識別するための名前です。
- S-VLAN ID — サービス VLAN を、区別するための VLAN です。サービスプロバイダネットワークの異なる顧客やサービスからのトラフィック。
- C-VLAN ID — カスタマー VLAN。サービスプロバイダネットワークにおいて、異なる顧客からのトラフィックを区別します。

7 サイト SD-WAN の構成

この章では、サイトレベルでの SD-WAN デバイスの構成設定について説明します。以下のセクションが含まれます：

VPN グループ構成

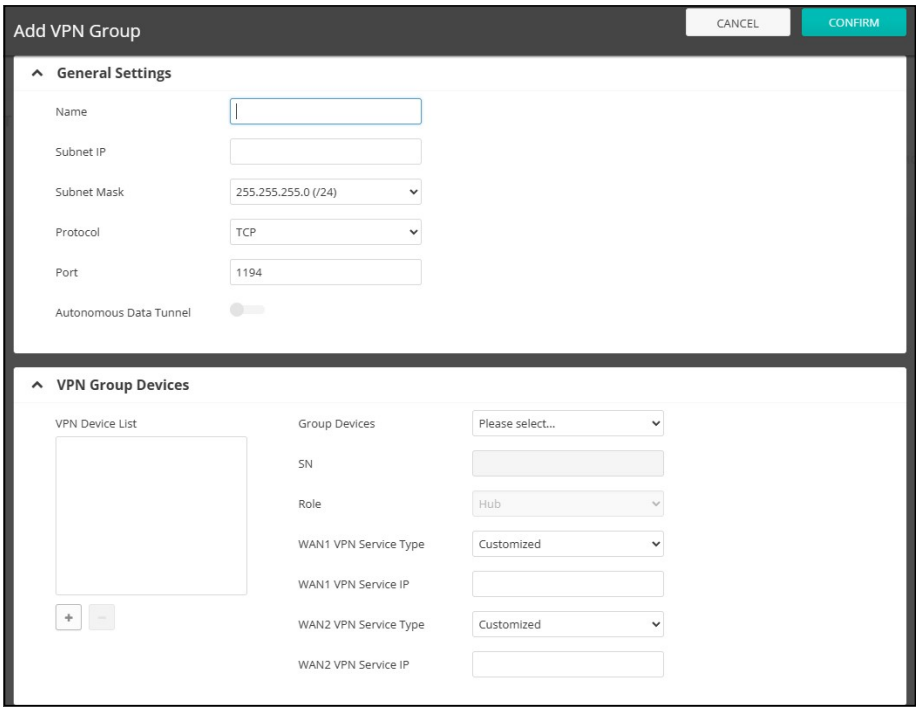
Site メニューから、"Configuration" を開き、"SDWAN" を開くと、同じサイト内のすべての SD-WAN デバイスに適用される設定オプションが表示されます。

VPN グループ

SD-WAN 設定ページの VPN グループタブには以下の項目があります：

- 一般設定
  - Name — 新しい VPN グループの名前です。
  - Subnet IP — VPN トンネルの仮想 IP アドレスを指定してください。グループ内のデバイスの WAN IP や LAN サブネットとは重複しません。
  - Subnet Mask — 仮想トンネル IP のサブネットマスクを選択してください。
  - Protocol — VPN トンネルの TCP（デフォルトおよび推奨）または UDP を選択してください。
  - Port — VPN グループ内のハブデバイスが使用するポートです。ハブデバイスで使用中のポートと競合しないようにしてください。
  - Autonomous Data Tunnel（自律データトンネル）— 手動操作なしで独立したデータトンネルの作成を可能にするために、自律トンネリングを有効または無効にしてください。

図 201: 新しい VPN グループの追加



- VPN グループデバイス
  - グループデバイス — 利用可能なリストから選択して、VPN デバイスリストにデバイスを追加してください。
  - SN — このサイトデバイスのシリアル番号です。
  - ロール — VPN グループ内のデバイスには、以下の役割のいずれかが割り当てられています：
  - ハブ — VPN サーバーとして動作する中央ノード。NAT の背後にあるハブには、NAT ルーターの WAN IP で WAN VPN Service Type を 'Customized' に設定します。VPN Group ごとに許可されるハブは 1 つだけです。
  - Spoke — VPN クライアントとして動作するデバイスです。インターネット・アクセスはサイト・デバイスのローカルで行われます。
  - To Server — VPN クライアントとして動作するデバイスで、インターネットトラフィックは VPN トンネルを経由してハブにルーティングされます。
  - WAN1/WAN2 VPN 構成 — ハブ・デバイスの場合、WAN1 と WAN2 のサービス・タイプをカスタマイズとドメイン名の間で指定してください。カスタマイズを選択した場合は、対応する WAN のサービス IP

を手動で入力してください。ドメイン名を選択した場合は、サービスドメインを手動で入力してください。

8 WiFi 5 デバイス構成

このチャプターでは、デバイスレベルでのアクセスポイントの設定について説明します。

デバイスレベルの設定へのアクセス

デバイスの“引継ぎのポリシー“が有効になっている場合、デバイスはサイトレベルで設定されます。ただし、デバイスはデバイスのレベルで個別に設定でき、設定はサイトレベルの設定を上書きします。

注意：設定が変更されたページの“復元“ボタンをクリックすると、個別のデバイスの設定をリセットできます。

さらに、無線のデバイスは、高度な無線設定や特定の製品に固有の機能など、サイトレベルで設定できない設定を有しています。これらの設定は、デバイスレベルでのみ行うことができます。

デバイスの設定にアクセスするには、サイトメニューのデバイスからデバイス名をクリックしてください。（クラウドメニューのデバイスからもアクセスが可能です）。

図 202: デバイスレベルの設定にアクセスする

デバイスのダッシュボードから、デバイスメニューの“設定“をクリックして、デバイスの設定にアクセスします。

図 203: デバイスレベルのダッシュボード

デバイスの設定ページには、サイトの設定ページと同様のタブ付きセクションがあります。

図 204: デバイスの設定

SSID のデバイスレベルの設定は、SSID リストの " オリジン " 欄に表示されています。" サイト " または " デバイス " のいずれかが表示されます。デバイスレベルの他の設定アイテムは、サイトレベルのものと同じです。

このチャプターでは 111 ページの「サイト WiFi 5 構成」に記載されているように、サイトレベルの設定とは異なる設定についてのみ説明します。

デバイスの無線設定

“ 無線設定 “ をクリックして、5GHz 及び 2.4GHz の無線設定を設定します。設定は、設定されている全ての SSID インターフェースに適応します。

無線設定タブには、次のアイテムが表示されます。設定オプションは、特に明記されいない限り、5GHz と 2.4GHz のどちらにも適応します。

グローバル設定

図 205: デバイスのグローバル無線設定

- 規制国 — 無線デバイスの規制設定です。この設定は表示されますが、デバイスレベルでの設定はできません。

  AP の国コードを正しく設定して、許可された地域の規定に従って無線が操作するようにする必要があります。国コードを設定すると、AP の操作が、指定された国の無線ネットワークで許可されている無線チャネルと送信電力に制限されます。

- バンドステアリング — 有効にすると、2.4GHz 及び 5GHz をサポートするクライアントが最初に 5Ghz 無線に接続されます。この機能は、2 つの無線帯域でクライアントの負荷を分散するのに役立ちます。この機能が完全に動作するには、両方の無線で一致する SSID が設定されている必要があるので注意してください。

一般的な無線設定

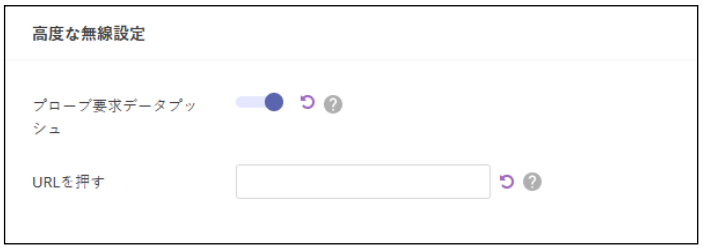
図 206: デバイスの一般的な無線設定

- 無線の有効化 — このインターフェースの無線サービスを有効／無効にします。

- 操作モード — AP 無線が機能するモードを選択します。
  - アクセスポイント（自動 WDS）— AP は WDS モードのアクセスポイントとして操作し、クライアント WDS モードの AP からの接続を受け 入れます。（これはデフォルト設定です）。
  - このモードでは、AP は通常のアクセスポイントとしてクライアントにサービス提供します。WDS は、同じ SSID とセキュリティ設定を使用して他の AP ノードを自動的に検索して接続するために使用されます。
  - クライアント — AP は別の AP への無線接続を提供できます。このモードでは、ローカルに配線されたホストとの間で情報をやり取りできますが、無線クライアントにはサービスを提供しません。
  - クライアント WDS — AP は WDS モードでクライアントステーションとして操作し、自動 WDS モードで他のアクセスポイントに接続します。別の AP への接続は、自動 WDS モードで操作している他のアクセスポイントによって自動的に行うことができます。
- Site Survey — このボタンをクリックしてデバイスの場所にある他の WiFi デバイスをスキャンできます。

高度な無線設定

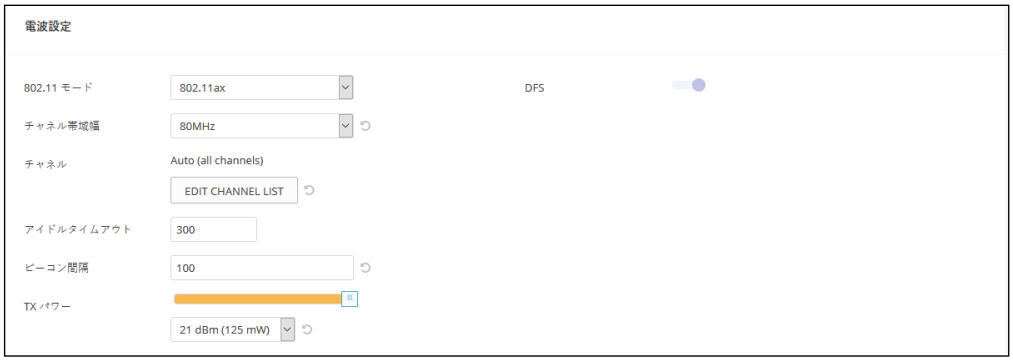
図 207: デバイスの高度な無線設定



- プローブ要求データプッシュ — クライアントリクエストデータプッシュを有効にすると、無線はクライアントプローブの要求データを JASON 形式で指定された URL にプッシュします。
- プッシュ URL— この無線からのプローブリクエストセータがプッシュされるウエブアドレスです。

電波設定

図 208: デバイスのフィジカル無線設定

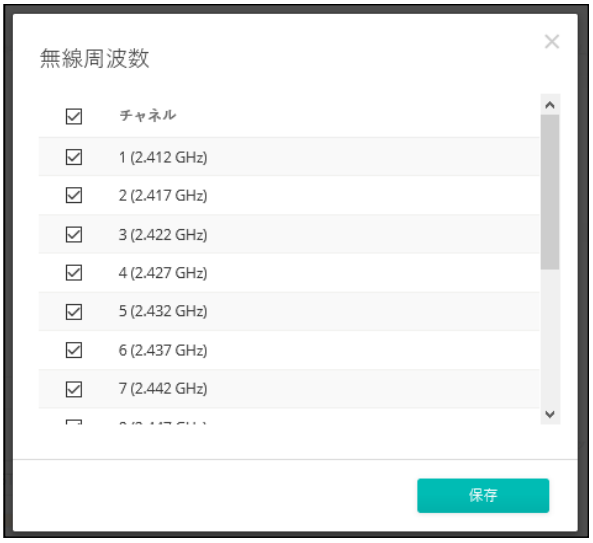


- 802.11 モード — 無線の操作モードを定義します。
  - 5GHz 無線 — オプション : 802.11a, 802.11a+n, 11ac+a+n; デフォルト設定 : 802.11ac+a+n
  - 2.4GHz 無線 — 固定 : 802.11b+g+n
- チャネル帯域幅 — 基本的な WiFi チャネル帯域幅は 20MHz ですが、チャネルを結合して 40MHz または 80mHZ チャネルを作成できます。80MHz チャネルを作成することにより、より高いデータ転送速度を実現できます。ただし、より広いチャネル帯域幅を選択すると、使用可能な無線チャネルの数が減少します。
  - 5GHz 無線 — オプションは 20、40、80MHz があります。(デフォルトは 80MHz です)。
  - 2.4GHz 無線 — オプションは 20、40MHz があります。(オプションは 40MHz です)。
- チャネル — アクセスポイントが無線クライアントとの通信に使用する無線チャネルです。使用可能なチャネルは、無線、チャネル帯域幅、及び規制国の設定によって異なります。“ EDIT CHANNEL LIST“ ボタンをクリックして、各無線インターフェースで使用する特定の使用可能なチャネルを選択できます。

  自動機能を選択すると、アクセスポイントが、使用されていない無線チャネルを自動的に選択します。(デフォルトは自動の状態です)。

図 209: 5GHz 無線チャネル

図 210: 2.4GHz 無線チャネル



- Tx パワー — アクセスポイントから送信される無線最大電力を調整します。送信電力が高いほど、送信範囲は広くなります。電力の選択は、カバレッジエリアとサポートされるクライアントの最大数のトレードオフであるだけだと考えてはいけません。高出力信号が、サービスエリアの他の無線デバイスの操作の邪魔をしないようにす必要があります。(電力設定とデフォルトの範囲は、AP モデルと規制国の設定によって異なります)。

- フラグメンテーションスレッシュ — パケットが分割化される最大フレームサイズを設定します。これにより、フレームの送信に必要な時間が短縮され、破損する可能性が低くなります。(データのオーバーヘッドが増加します。)。(範囲は 256–2346 バイトです。デフォルトは 2346 バイトです)。

- RTS スレッシュ — 送信ステーションが通信を開始する前に、“ 送信要求（RTS）フレーム “ を受信ステーションに送る必要がありますが、そのパケットサイズの、しきい値を設定します。アクセスポイントは、送信を交渉するために、CTS フレームを受信ステーションに送信します。RTS フレームを受信した後、アクセスポイントは CTS（送信許可）フレームを送信して、データの送信を開始することを送信ステーションに通知します。

  RTS しきい値が q に設定されている場合、アクセスポイントは常に RTS 信号を送信します。2347 に設定されている場合、アクセスポインとは RTS 信号を送信しません。他の値に設定され、パケットサイズが RTS しきい値以上の場合、RTS ／ CTS（送信要求／送信クリア）メカニズムが有効になります。

  メディアをめぐって競走するアクセスポイントは、お互いを認識しない可能性があります。RTS/CTS メカニズムは、この “ 隠されたノード問題 “ を解決できます。

- SGI — 11n ドラフトでは、400ns（短い）と 800ns（長い）の二つのガード間隔が指定されています。400ns の短いガード間隔のサポートは、送信と受信ではオプションです。ガータ間隔の目的は、デジタルデータが通常非常に敏感である伝搬の遅れ、エコー、及び反射に対する耐性を導入することです。SGI を有効にすると、400ns に設定されます。（デフォルトは有効です）。

- STBC — 時空間ブロックコーディングは、データ転送の信頼性を向上させるためのさまざまな受信バージョンを使用して、同じデータの複数のコピーを複数のアンテナを介して送信します。送信された信号は錯乱、反射、屈折などの難しい環境を通過する可能性があります。受信機の熱雑音によってさらに破損する可能性があるため、受信したコピーの一部は他のコピーよりも優れている状態になります。このため、一つ以上の受信コピーを使用すると、受信信号を正しくデコードできる可能性が高くなります。（デフォルトは無効の状態です）。

- DFS — この分野は選択した無線モードが5GHz周波数で操作している場合のみに使用できます。

  5GHz 帯域の無線が、DFS サポートが ON の状態で、規制ドメインがチャネルでレーダ検出を必要とする場合、802.11h の Dynamic Frequency Selection (DFS) 及び Transmit Power Control (TPC) 機能がアクティブになります。

  DFS は、無線デバイスがスペクトルを共有すること、5GHz 帯域のレーダーシステムと同一チャネル動作を回避することを要求するメカニズムです。DFS 要求は、AP の国コード設定によって決定される規制ドメインによって異なります（デフォルトは有効の状態です）。

- 2.4GHz 無線にのみ適応されます。このオプションにより、802.11n 20MHz 及び 40MHz チャネル帯域幅を同じネットワークで一緒に操作できます。（デフォルトは ON の状態です）。

9 WiFi 6 デバイス構成

この章では、WiFi 6 アクセスポイントのデバイスレベルでの構成設定について説明します。以下のセクションが含まれています：

デバイスレベルの設定へのアクセス

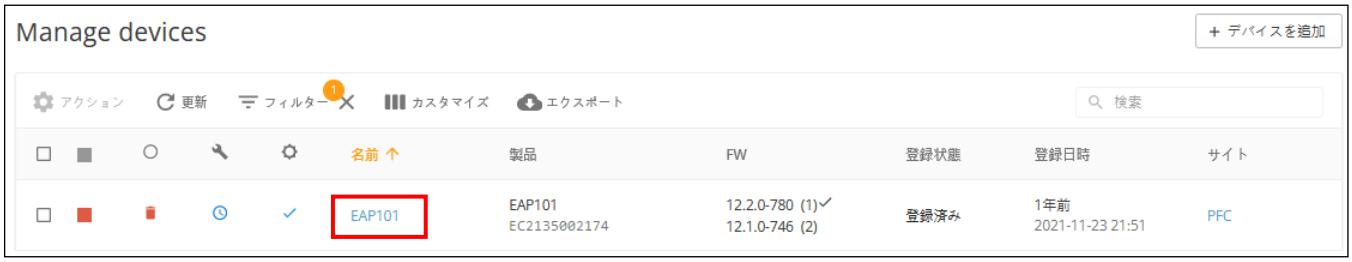
デバイスの“引継ぎのポリシー“が有効になっている場合、デバイスはサイトレベルで設定されます。ただし、デバイスはデバイスのレベルで個別に設定でき、設定はサイトレベルの設定を上書きします。

注意：設定が変更されたページの“復元“ボタンをクリックすると、個別のデバイスの設定をリセットできます。

さらに、無線のデバイスは、高度な無線設定や特定の製品に固有の機能など、サイトレベルで設定できない設定を有しています。これらの設定は、デバイスレベルでのみ行うことができます。

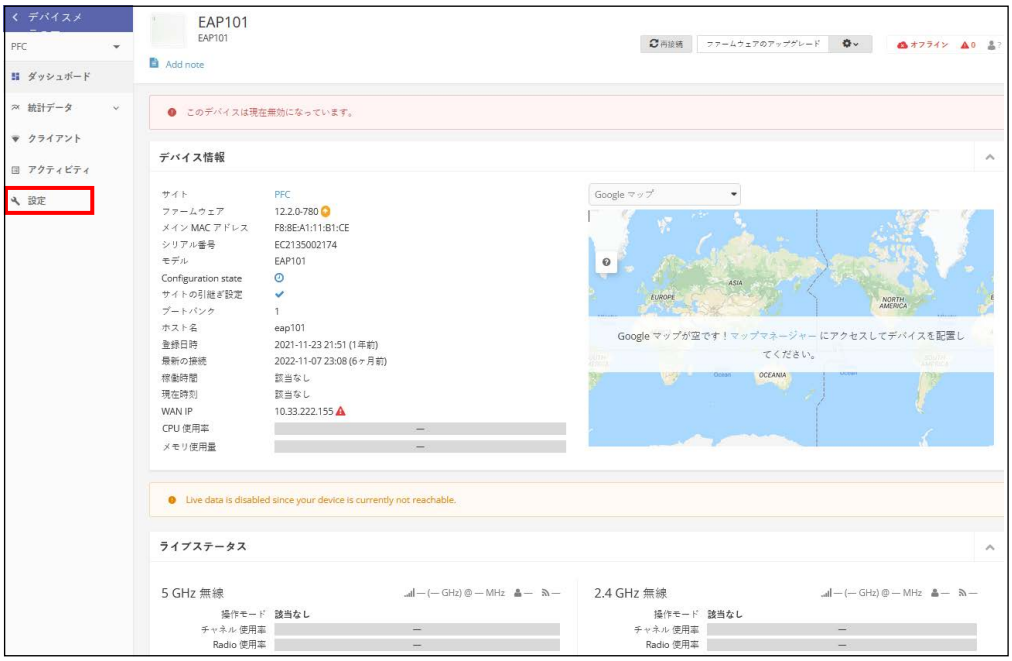
デバイスの設定にアクセスするには、サイトメニューのデバイスからデバイス名をクリックしてください。（クラウドメニューのデバイスからもアクセスが可能です）。

図 211: デバイスレベルの設定にアクセスする



デバイスのダッシュボードから、デバイスメニューの“設定“をクリックして、デバイスの設定にアクセスします。

図 212: デバイスレベルのダッシュボード



デバイスの設定ページには、サイトの設定ページと同様のタブ付きセクションがあります。

図 213: デバイスの設定

SSID のデバイスレベルの設定は、SSID リストの " オリジン " 欄に表示されています。" サイト " または " デバイス " のいずれかが表示されます。デバイスレベルの他の設定アイテムは、サイトレベルのものと同じです。

このチャプターでは 159 ページの「サイト WiFi 6 構成」に記載されているように、サイトレベルの設定とは異なる設定について説明します。

デバイスの無線設定

“ 無線設定 “ をクリックして、5GHz 及び 2.4GHz の無線設定を設定します。設定は、設定されている全ての SSID インターフェースに適応します。

無線設定タブには、次のアイテムが表示されます。設定オプションは、特に明記されいない限り、5GHz と 2.4GHz のどちらにも適応します。

グローバル設定

図 214: デバイスのグローバル無線設定

- 規制国 — 無線デバイスの規制設定です。この設定は表示されますが、デバイスレベルでの設定はできません。

  AP の国コードを正しく設定して、許可された地域の規定に従って無線を操作する必要があります。国コードを設定すると、AP の操作が、指定された国の無線ネットワークで許可されている無線チャネルと送信電力に制限されます。

- バンドステアリング — 有効にすると、2.4GHz 及び 5GHz をサポートするクライアントが最初に 5Ghz 無線に接続されます。この機能は、2 つの無線帯域でクライアントの負荷を分散するのに役立ちます。この機能が完全に動作するには、両方の無線で一致する SSID が設定されている必要があるので注意してください。

Mesh 設定

オープンメッシュは、相互に接続されたノード AP のネットワークで、そのうち 1 台だけがネットワーク（およびインターネット）に有線で接続されています。他の AP ノードは、互いに無線接続を提供し、一部は無線クライアントへの接続をサポートします。メッシュネットワークは、無線接続をより遠くまで拡張するだけでなく、ネットワーク内の 1 つのノードが故障した場合のバックアップリンクも提供します。

図 215: デバイス Mesh 設定

- Open Mesh — SSID インターフェースで Open Mesh サポートを有効にします。
- Mesh ID — メッシュネットワークの名前です。
- Mesh Method — Open Mesh リンクに適用されるセキュリティ。
  - オープン — なし。
  - WPA3-Personal - 他の AP とのメッシュリンクで SAE（Simultaneous Authentication of Equals）付きの WPA3 を使用します。
- Network Behavior — 以下の接続方法のいずれかを指定する必要があります。(初期値：ルートからインターネット)
  - インターネットへのブリッジ — WAN に接続されたインターフェースとして設定します。このインターフェースからのトラフィックは、インターネットに直接ブリッジされます。(図 135、142 ページの「インターネットへのブリッジ」を参照してください)。
  - ルートからインターネット — インターフェースを LAN のメンバーとして設定します。このインターフェースからのトラフィックは、アクセスポイントを横切って、インターネットにブリッジされているインターフェースを経由して外にルーティングされます。(図 136 の「ルートからインターネット」を参照してください)。
    - ネットワーク名 - ルーティングされるネットワークです。デフォルトは、「LAN 設定」-「ローカルネットワーク」で表示される「デフォルトのローカルネットワーク」です。

- Mesh 無線 — AP をメッシュネットワークのノードとして設定する場合、1 つの無線インターフェース（2.4GHz または 5GHz）を選択し、特定のチャネルで動作するように設定します（「自動」を選択しないでください）。他の AP ノードが同じ無線インターフェース、チャネル、同じ SSID で動作するように設定します。

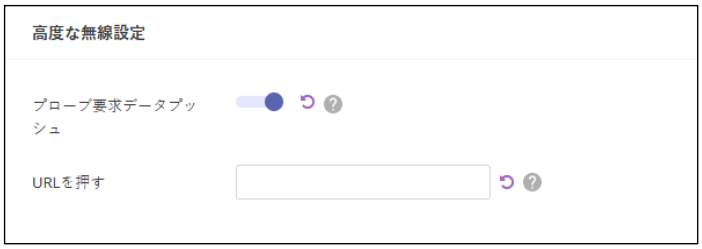
一般的な無線設定

図 216: デバイスの一般的な無線設定

- 無線の有効化 — このインターフェースの無線サービスを有効／無効にします。
- 操作モード —AP 無線が機能するモードを選択します。
  - アクセスポイント（自動 WDS）—AP は WDS モードのアクセスポイントとして操作し、クライアント WDS モードの AP からの接続を受け 入れます。（これはデフォルト設定です）。
  - このモードでは、AP は通常のアクセスポイントとしてクライアントにサービス提供します。WDS は、同じ SSID とセキュリティ設定を使用して他の AP ノードを自動的に検索して接続するために使用されます。
  - クライアント —AP は別の AP への無線接続を提供できます。このモードでは、ローカルに配線されたホストとの間で情報をやり取りできますが、無線クライアントにはサービスを提供しません。
  - クライアント WDS—AP は WDS モードでクライアントステーションとして操作し、自動 WDS モードで他のアクセスポイントに接続します。別の AP への接続は、自動 EDS モードで操作している他のアクセスポイントによって自動的に行うことができます。
- Site Survey— このボタンをクリックしてデバイスの場所にある他の WiFi デバイスをスキャンできます。

高度な無線設定

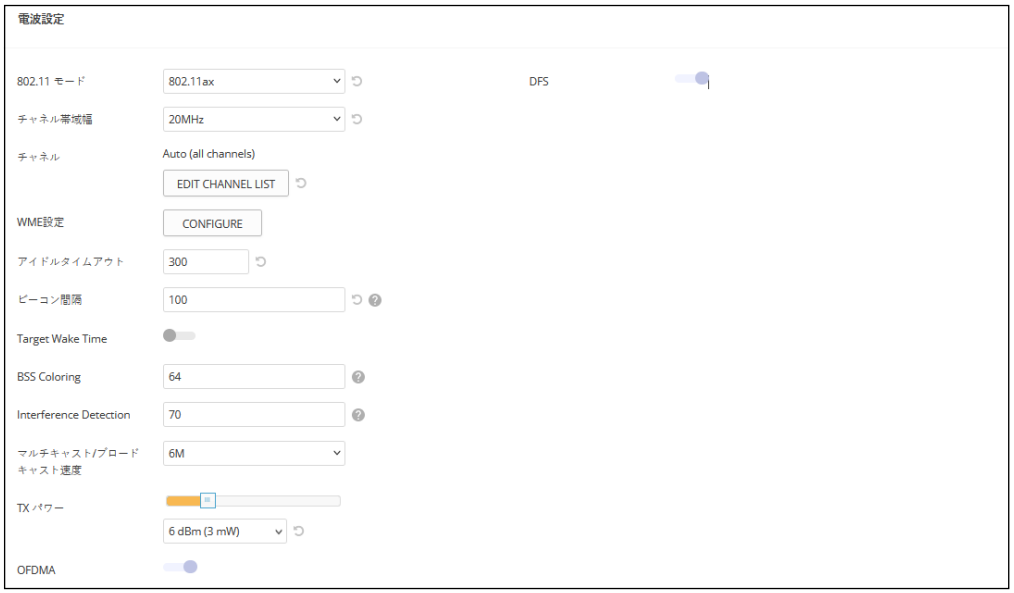
図 217: デバイスの高度な無線設定



- プローブ要求データプッシュ — クライアントリクエストデータプッシュを有効にすると、無線はクライアントプローブの要求データを JASON 形式で指定された URL にプッシュします。
- プッシュ URL— この無線からのプローブリクエストセータがプッシュされるウエブアドレスです。

電波設定

図 218: デバイスのフィジカル無線設定



- 802.11 モード — 無線の操作モードを定義します。
  - 5GHz 無線 — オプション : 802.11a, 802.11a+n, 802.11ac+a+n, 802.11ax; デフォルト設定 : 802.11ax
  - 2.4GHz 無線 — オプション : 802.11b+g+n, 802.11ax; デフォルト : 802.11ax
- チャネルの帯域幅 — Wi-Fi のチャネル帯域は 20MHz が基本ですが、チャネルを結合して 40MHz、80MHz、160MHz のチャネルを作ることで、よ

り高速なデータ転送を実現できます。ただし、チャネル帯域幅を広くすると、利用できる無線チャネルの数が少なくなります。利用可能なチャネル帯域幅は、802.11 モードに依存します。(デフォルト : 2.4GHz 無線では 20MHz、5GHz 無線では 80MHz、オプション :20MHz、40MHz、80MHz、160MHz)

- 20MHz — 802.11b+g+n および 802.11ax 用
- 40MHz — 802.11b+g+n、802.11a、802.11a+n、802.11ac+a+n および 802.11ax 用
- 80MHz — 802.11ac+a+n および 802.11ax 用
- 160MHz — （EAP104 5GHz 無線機のみ対応）802.11ac+a+n および 802.11ax 用

- チャネル — アクセスポイントが無線クライアントとの通信に使用する無線チャネルです。使用可能なチャネルは、無線、チャネル帯域幅、及び規制国の設定によって異なります。“ EDIT CHANNEL LIST“ ボタンをクリックし、各無線インターフェースで使用する特定の使用可能なチャネルを選択することもできます。

  自動機能を選択すると、アクセスポイントが、使用されていない無線チャネルを自動的に選択します。（デフォルトは自動の状態です）。

図 219: 5GHz 無線チャネル

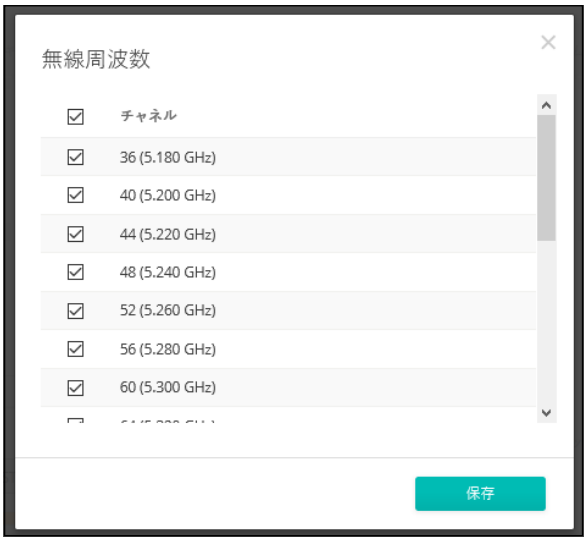
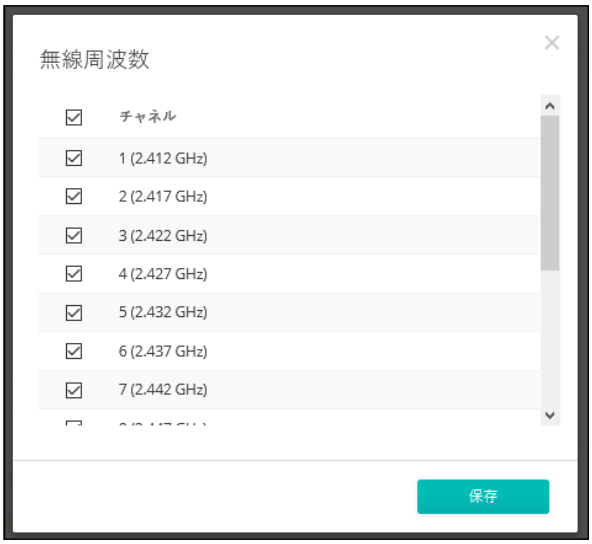


図 220: 2.4GHz 無線チャネル



- WME 設定 — Wi-Fi Multimedia（WMM）としても知られる Wireless Multimedia Extensions（WME）は、IEEE 802.11e 規格に基づく Wi-Fi Alliance の相互運用性認定です。IEEE 802.11 ネットワークに基本的な QoS（Quality of Service）機能を提供します。アクセスプライオリティは、以下のパラメータを使用して 4 つの「アクセスカテゴリー」（AC）タイプに設定できます：

  - CW Min (Minimum Contention Window) — 無線媒体アクセスが試みられるまでのランダムバックオフ待ち時間の初期上限値である。初期待ち時間は、ゼロと CWMin 値の間のランダムな値です。CWMin 値は、0 ～ 15 マイクロ秒の範囲で指定します。なお、CWMin 値は CWMax 値と同じかそれ以下である必要があります。

  - CW Max (Maximum Contention Window) — 無線媒体アクセスが試みられるまでのランダムバックオフ待ち時間の最大上限値です。衝突が検出されるたびに、CWMax 値までコンテンションウィンドウが 2 倍になります。CWMax 値は、0 ～ 15 マイクロ秒の範囲で指定します。なお、CWMax 値は CWMin 値以上である必要があります。

  - AIFS（Arbitration Inter-Frame Space）— 次のデータ送信を試みるまでの最小の待ち時間です。AIFS の値は、0 ～ 15 マイクロ秒の範囲で指定します。

  - TXOP Limit (Transmit Opportunity Limit) — AC 送信キューが無線媒体にアクセスできる最大時間です。AC キューに送信機会が与えられると、TXOP Limit までの時間、データを送信できます。このデータバーストにより、高データレートのトラフィックに対する効率が大幅に改善されます。0 ～ 8192 マイクロ秒の範囲で値を指定します。

- アイドルタイムアウト — AP は、設定された時間、アクティビティがない場合、クライアントを切断します。(デフォルト：300 秒、範囲：60 ～ 60000 秒)。

- ビーコン間隔 — ビーコン信号がアクセスポイントから送信される速度です。ビーコン信号により、無線クライアントはアクセスポイントとの接触を維持できます。また、電源管理などの情報も伝達されます。(範囲：100 ～ 1024TU、初期値：100TU)。

- Target Wake Time — 802.11ax（Wi-Fi 6）モードでは、AP は、クライアントが定期的なビーコンに依存するのではなく、フレームを送信または受信するために特定の Target-Wakeup Time（TWT）を要求できるようにできます。この機能により、クライアントデバイスのスリープ状態を大幅に延長でき、大幅な省電力化を実現します。また、AP はクライアントの TWT を制御してスケジュールすることで、ネットワーク内の競合を管理し、遅延に敏感なトラフィックに対応できます。(デフォルト：無効)

- BSS Coloring — 802.11ax（Wi-Fi 6）モードでは、BSS Coloring により、同じ周波数で動作する近くの AP が、自身の基本サービスセット

- （BSS）に属するトラフィックを識別できます。BSS Coloring により、近隣の AP とクライアントの送信が重なる高密度環境において、Wi-Fi 6 ネットワークをより効率的に運用できます。無線 BSS を識別するためのカラー値（1 ～ 63 の数値）を割り当てるか、AP がカラー値 をランダムに選択するようにするために値 64 を入力します。(範囲：1 ～ 63、64 ランダム、デフォルト：64)

- マルチキャスト / ブロードキャストレート — マルチキャストおよびブロードキャストパケットによって消費される無線帯域幅に制限をかけることができるようにします。

  - 無線 5 Ghz — オプション：6M、9M、12M、18M、24M、36M、48M、54M、初期値：6M

  - 無線 2.4 Ghz — オプション：5.5M、6M、9M、11M、12M、18M、24M、36M、48M、54M、初期値：5.5M

- Tx パワー — アクセスポイントから送信される無線最大電力を調整します。送信電力が高いほど、送信範囲は広くなります。電力の選択は、カバレッジエリアとサポートされるクライアントの最大数のトレードオフであるだけだと考えてはいけません。高出力信号が、サービスエリアの他の無線デバイスの操作の邪魔をしないようにす必要があります。(電力設定とデフォルトの範囲は、AP モデルと規制国の設定によって異なります)。

- OFDMA — 802.11ax（Wi-Fi 6）モードは Orthogonal Frequency Division Multiple Access (OFDMA) をサポートし、これを無効にはできません。

- DFS — この分野は選択した無線モードが5GHz周波数で操作している場合のみに使用できます。

  5GHz 帯域の無線が、DFS サポートが ON の状態で、規制ドメインがチャネルでレーダ検出を必要とする場合、802.11h の Dynamic Frequency Selection (DFS) 及び Transmit Power Control (TPC) がアクティブになります。

  DFS は、無線デバイスがスペクトルを共有すること、5GHz 帯域のレーダーシステムと同一チャネル動作を回避することを要求するメカニズムです。DFS 要求は、AP の国コード設定によって決定される規制ドメインによって異なります（デフォルトは有効の状態です）。

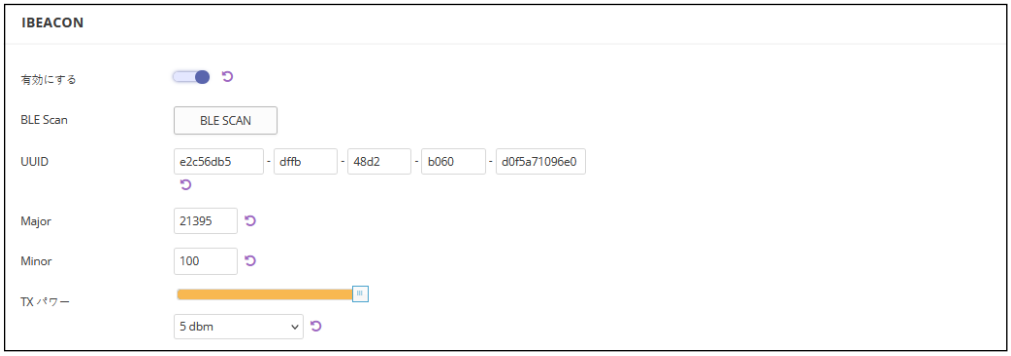
システム設定

「システム設定」タブをクリックすると、デバイスレベルの機能を設定できます。

iBeacon

AP は Bluetooth Low Energy（BLE）をベースとした iBeacon 規格に対応しています。BLE ビーコンを搭載したデバイスは、ビーコン広告を認識し、提供された情報を抽出し、その内容に基づいてアクションを起こせる電話などの BLE クライアントに位置情報サービスを提供できます。

図 221: デバイス iBeacon 設定



このページでは、以下の項目が表示されます：

- 有効にする — AP の iBeacon サポートを有効にします。(デフォルト：有効にする)

- BLE スキャン — （EAP101 および EAP104 のみ）以下の 4 つのタイプを含む、すべての BLE デバイスをスキャンします：EddyStone-UID、EddyStone-URL、EddyStone-TLM、および ibeacon。

- UUID — ビーコンサービスを宣伝する iBeacon Universally Unique Identifier です。UUID は、ハイフンで区切られた 5 つのグループに分かれた 32 の 16 進数で構成されています。
- Major — ビーコングループを識別するために使用される iBeacon 値です。(範囲 : 0-65535)
- Minor — 内の個々のビーコンを識別するために使用される iBeacon 値です。
- TX パワー — BLE 無線の送信電力を設定します (EAP101 と EAP104 でのみサポートされています)。(範囲 : 5dBm ～ -20dBm、デフォルト : 5dBm)。

10 Metrolinq デバイスの設定

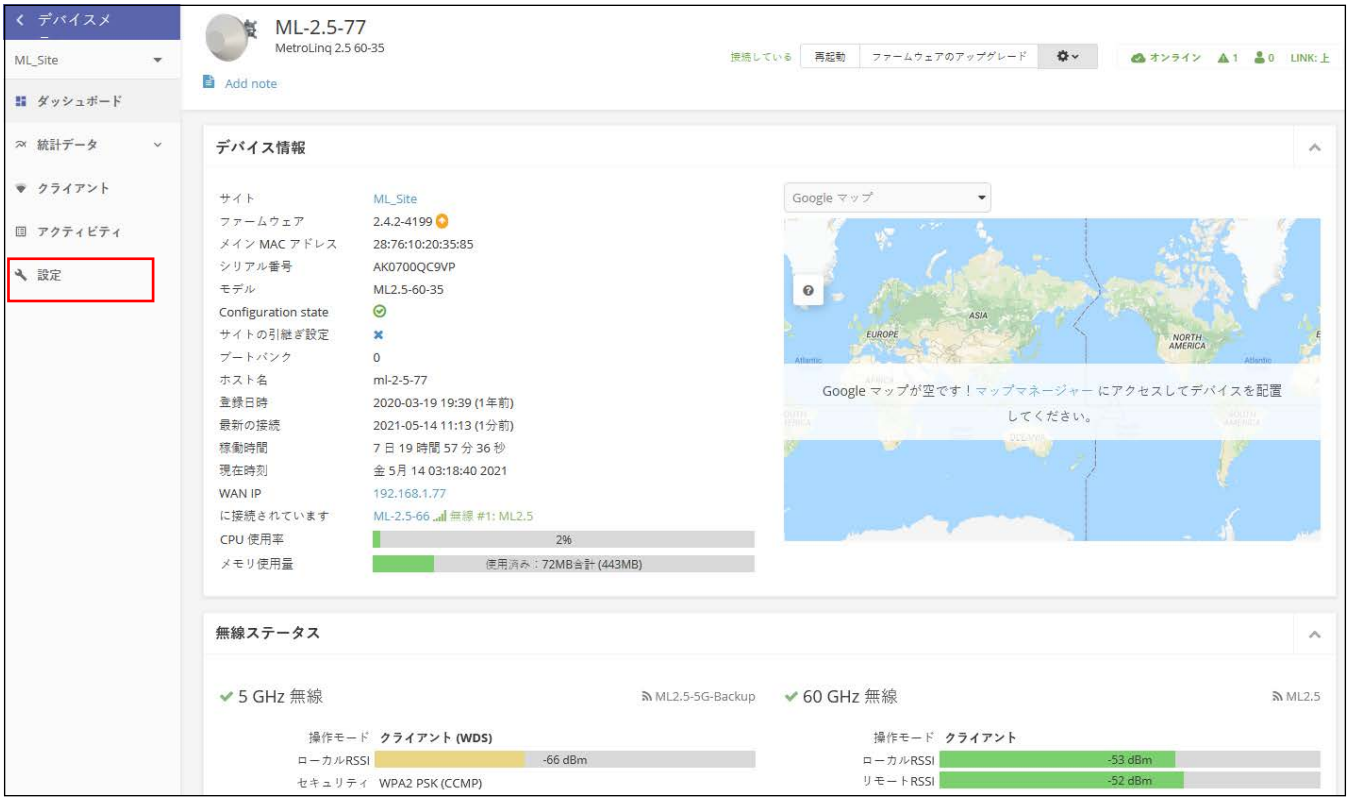
このチャプターでは、Metrolinq ユニットのデバイスレベルでの設定について説明します。下記のセクションがあります。

Metrolinq の設定

2.4GHz 及び 5GHz 帯域をサポートする Metrolinq デバイスは、これらの無線インターフェースのサイトレベルから設定を引き継ぐことができます。60GHz 無線設定は、サイトレベルからの引継ぎができないため、デバイスレベルで設定する必要があります。

このセクションでは、サイトレベルでは使用できない特定の設定を含む、Metrolinq デバイスのデバイスレベルの設定について説明します。一般的なデバイスレベルの設定については、225 ページの「WiFi 5 デバイス構成」を参照してください。

図 222: Metrolinq デバイスのダッシュボード



無線 SSID

Metrolinq デバイスは、60GHz 無線をサポートし、多くの場合 5GHz 及び 2.4GHz 無線が含まれます。SSID は、無線 SSID ページから 5GHz と 2.4GHz に対しての設定を行うことができます。60HGz 無線は 1 つの SSID のみをサポートします。

無線のバックアップとして設定されている場合は、無線設定ページでも SSID を設定する必要があります。

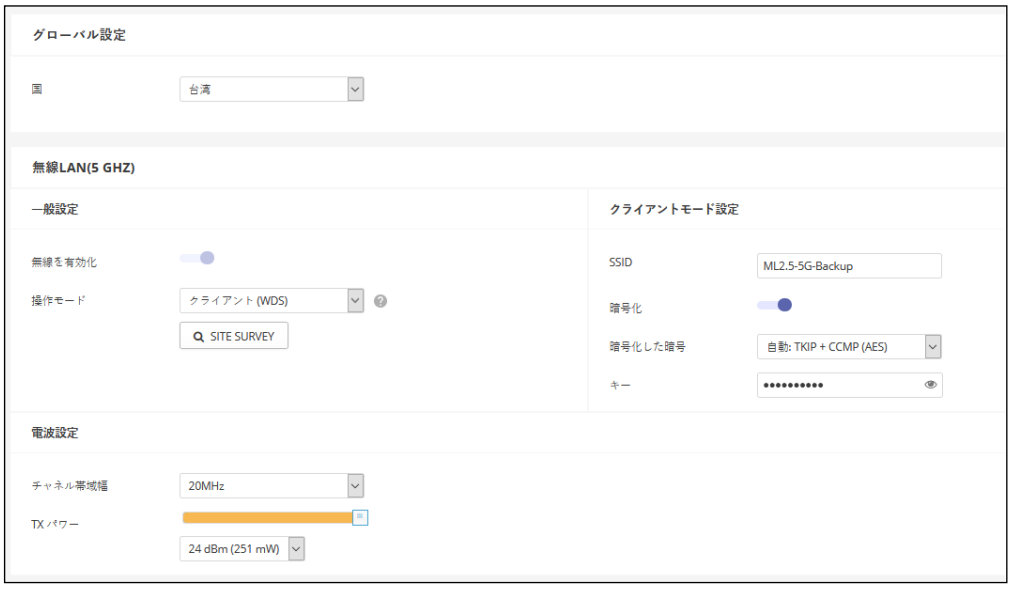
WiFi アクセスの SSID の設定についての詳細は、112 ページの「無線 SSID の設定」を参照してください。

図 223: Metrolinq デバイスのダッシュボード

無線設定

“ 無線設定 “ タブをクリックして、60GHz、5GHz、2.4GHz の無線を設定します。

図 224: Metrolinq デバイス 5GHz 無線設定



グローバル設定

このセクションは下記のアイテムがあります。

- 国 — Metrolinq デバイスへの規制に対応しての設定です。

Metrolinq の国コードは、無線が許可された地域の規制に従って操作 するために、正しく設定しなくてはいけません。国コードを設定すると、Metrolinq の操作が、指定された国の無線ネットワークで許可 されている無線チャネルと送信レベルに規制されます。

無線 5GHz 一般的な無線設定

- 無線を有効にする—5GHz インターフェースで無線サービスを有効 / 無効にします。5GHz 無線は、690GHz 無線のバックアップとして操作できることに注意してください。

- 操作モード — 5GHz 無線が機能するモードを選択します。

  - アクセスポイント（自動 WDS）— 5GHz 無線は、クライアント WDS モードの AP からの接続を受け入れる、WDS モードのアクセスポイントとして操作します。（これはデフォルトの設定です）。

    このモードでは、5GHz 無線が、通常のアクセスポイントとしてクライアントにサービスを提供します、WDS は、同じ SSID とセキュリティの設定を使用して、他の AP ノードを自動的に検索して接続します。

  - クライアント WDS — 2 つの Metrolinq ユニット間のポイントトゥーポイント無線リンクで、バックアップ無線ブリッジクライアントとしてのみ操作するように、5GHz 無線を設定します。

- Site Survey — このボタンをクリックすると、デバイスの場所にある他のデバイスをスキャンできます。

クライアントモードの設定

- 5GHz インターフェースのサービスセット識別子の、独自の名前を入力してください。ポイントトゥーポイントバックアップリンクの両端にある Metrolinq ユニットは、同じ SSID に接続されている必要があります。（範囲は 1–32 文字です）。

- リンクにマスターユニットの MAC アドレスを入力し、クライアント無線をそのユニットのみにロックします。

- 暗号化 — 5GHz インターフェースの無線セキュリティ方式を設定します。無効にすると、無線リンクにセキュリティがない状態になります。有効にすると、ポイントトゥーポイントバックアップリンクのメトリリンクユニットは、認証と暗号化に、事前共有キーを使用した WPA2 セキュリティを使用します。

  - 暗号化された暗号 —WPA2 時まえ共有キーに使用する暗号化された暗号を設定します。

- CCMP (AES) —AES-CCMP は、WPA2 に必要な標準の暗号化された暗号です。（これはデフォルトの設定です）。
- 自動 : TKIP + CCMP (AES) — 使用されている暗号化方式は、リンクパートナーとの関連付けにおいて検出されます。

- キー — 暗号化に使用する WPA2 時前共有キーを設定します。

フィジカル無線設定

- 一般的な WiFi チャネルの帯域幅は 20MHz ですが、チャネルを結合して 40MHz または 80MHz を作成できます。こうすると、より高いデータ送信速度を実現できます、ただし、より広いチャネル帯域 幅を選択すると、使用可能な無線チャネルの数が減少してしまいます。
（オプションは 20、40、80Mz です。デフォルトは 80MHz です）。

- チャネル — アクセスポイントが無線クライアントとの通信に使用する無線チャネルです。使用可能なチャネルは、無線、チャネルの帯域幅、規制国の設定によって異なります。“ EDIT CHANNEL LIST “ ボタンをクリックして、使用できる特定のチャネルを選択することもできます。

  自動機能を選択すると、アクセスポイントが、占領されていない無線チャネルを自動的に選択できます。

図 225: 5GHz 無線チャネル

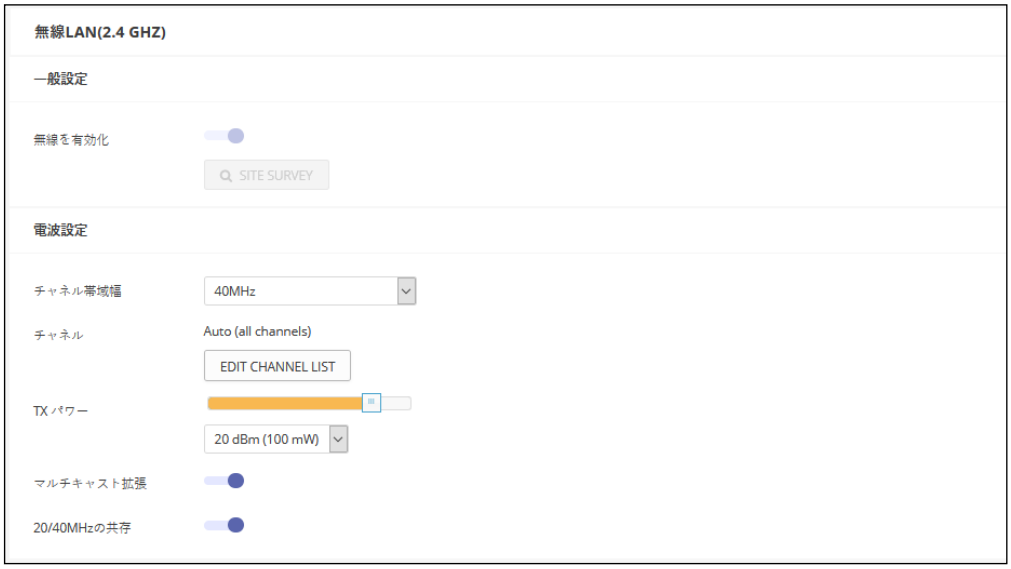
- Tx パワー — アクセスポイントから送信される無線信号の最大電力を調整します。送信電力が高いほど、送信範囲が広くなります。電力の選択が、カバレージエリアとサポートできるクライアントの人数との単純なトレードオフであると考えてはいけません。高出力信号が、サービスエリアの他のデバイスの操作の邪魔にならないように注意する必要がありま

す。(電力の設定とデフォルトの範囲は、AP モデルと、規制国の設定によって異なります)。

- マルチキャストエンハンスメント — この機能は、クライアントに転送する前のマルチキャストパケットを、ユニキャストパケットに変換します。このことにより、送信の安定度と速度が向上するからです。無線 クライアントがマルチキャストストリーミングに不満足である場合は、この機能を有効にしてパフォーマンスを向上させることができます。(5GHz 無線がクライアント WDS モードに設定されている場合、この機能は使用できません)。

無線 2.4GHz

図 226: Metrolinq デバイス 2.4GHz 無線設定



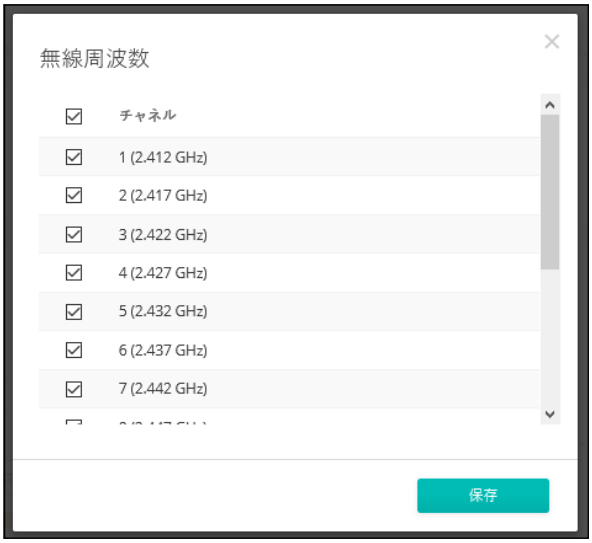
このセクションは以下のアイテムを表示します。

- 無線を有効にする — 2.4GHz インターフェースサービスを有効／無効にします。
- サイト調査 — このボタンをクリックして、デバイスが設置されている場所にある他の WiFI デバイスをスキャンします。
- チャネルの帯域幅 — 基本的な WiFi チャネル帯域幅は 20MHz ですが、チャネルを結合して 40MHz または 80MHz チャネルを作成すること により、より高いデータ送信速度を実現できます。ただし、より広いチャネル帯域幅を選択すると、使用可能な無線のチャネル の数が減少します。(オプション者 20MHz と 40MHZ です。デフォルト は 20MHz です)。
- チャネル — アクセスポイントが無線クライアントとの通信に使用する無線チャネルです。使用可能なチャネルは、無線、チャンネル帯域幅、規

制国の設定によって異なります。“ EDIT CHANNEL LIST “ をクリックして、使用できる特定のチャネルを選択することもできます。

自動機能を選択すると、アクセスポイントが、占領されていない無線チャネルを自動的に選択します。

図 227: 2.4GHz 無線チャネル

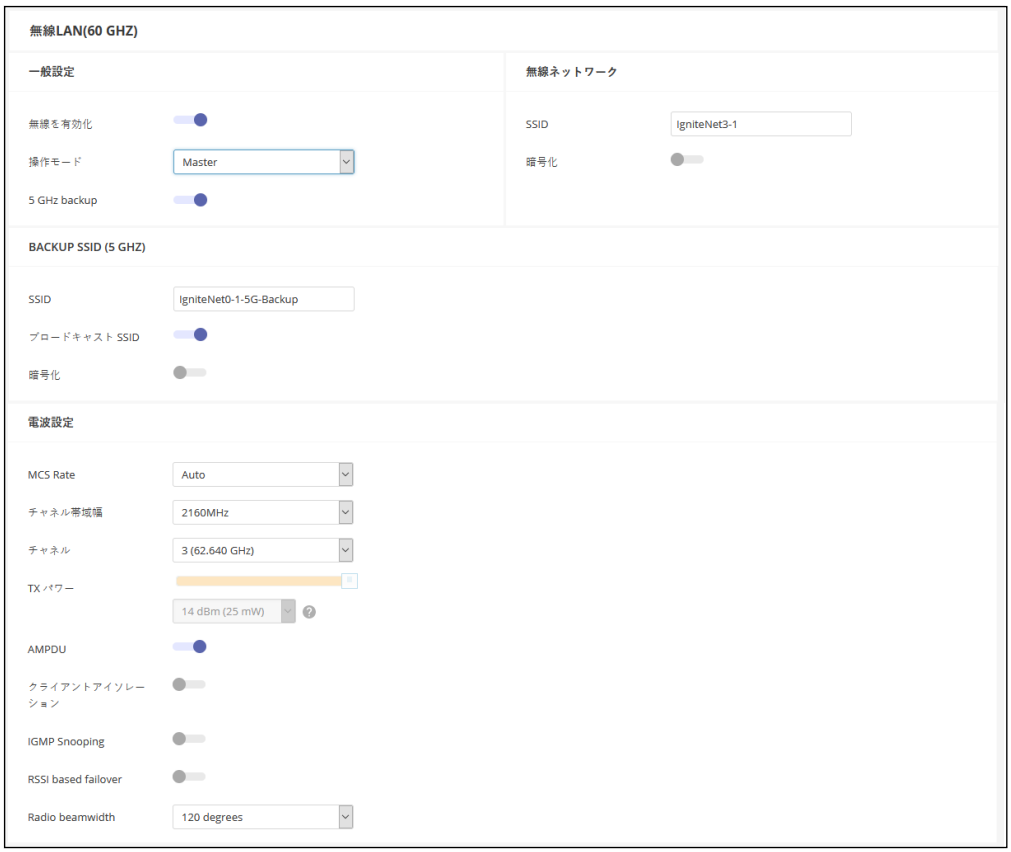


- TX パワー — アクセスポイントから送信される無線信号の最大電力を調整します。送信電力が高いほど、送信範囲は広くなります。電力の選択は、カバレージエリアとサポートされるクライアントの人数の最大値に影響するだけではありません。高出力信号が、サービスエリアの他の無線デバイスの操作に影響しないように注意する必要があります。(電源の設定の範囲とデフォルトの数値は、AP モデルと規制国の設定によって異なります)。

- マルチキャストの機能強化 — この機能は、クライアントに転送する前にマルチキャストパケットをユニキャストパケットに変換します。こうすることにより、送信過程の安定化と高速化が実現します。無線クライアントのマルチキャストストリーミングに問題がある場合は、この機能を有効にするとパフォーマンスの向上が望めます。

無線 60GHz

図 228: Metrolinq デバイス 60GHz 無線設定



一般的な無線設定

このセクションでは以下のアイテムを表示します。

- 無線の有効化 —60GHz のインターフェースで無線サービスを有効にします。
- 動作モード —60GHz インターフェースが操作するモードを選択します。
  - マスター — 二つ以上の Metrolinq ユニット間のポイントトゥーポイントまたは、ポイントトゥーマルチポイント無線リンクのマスターとして、60GHz インターフェースを設定します。Metrolinq 無線リンクでは、一方のユニット をマスターとして設定し、もう一方をクライアントとして設定する必要があります。Edgecore 以外のデバイスへのリンク は、サポートされていません。
  - クライアント — 二つの Metrolinq ユニット間のポイントトゥーポイント無線リンクのクライアントとして、60GHz インターフェースを設定します。
- 5GHzバックアップ—60GHzの無線リンクへのバックアップとして機能するように、5GHz インターフェースを設定します。60GHz リンクに障害

が発生した場合、接続を維持するために 5GHz リンクが有効になります。5GHz バックアップは、60GHz インターフェースがマスターモードに設定されている場合にのみ設定できます。（デフォルトは無効です）。

無線ネットワーク（マスターモードに設定された 60GHz 無線）

- SSID —60GHz インターフェースのサービスセット識別子の、独自の名前を入力します。ポイントトゥーポイントリンクの両端にある Metrolinq のユニットは、同じ SSID に設定する必要があります。

- 暗号化 —60GHz インターフェースの無線セキュリティの方法を設定します。無効にすると、無線リンクにセキュリティがなくなります。有効にすると、ポイントトゥーポイントの Metrolinq ユニットは、認証と暗号化に、事前に共有しておいた WPA2 セキュリティを使用します。（デフォルトは無効です）。

  - キー — 暗号化に使用する WPA2 時前共有キーを設定します。

クライアントモードの設定（クライアントモードに設定された 60GHz 無線）

- SSID—60GHz インターフェースのサービスセット識別子の独自の名前を入力します。ポイントトゥーポイントリンクの両端にある Metrolinq ユニットは、同じ SSID に設定されている必要があります。（範囲は 1－32 文字、60GHz です）。

- BSS ID Lock — リンクにマスターユニットの MAC アドレスを入力して、クライアントの無線をそのユニットだけにロックします。

- 暗号化 —60GHz インターフェースの無線セキュリティの方法を設定します。無効にすると、無線リンクにセキュリティはありませ ん。有効にすると、ポイントトゥーポイントの Metrolinq ユニットは、認証と暗号化に事前に共有した WPA2 セキュリティを使用 します。（デフォルトは無効です）。

  - キー — 暗号化に使用する WPA2 の事前共有キーを設定します。

バックアップ SSID（5GHz）

- SSID — バックアップ 5GHz インターフェースのサービスセット識別子の独自な名前を入力します。ポイントトゥーポイントリンクの両端にある Metrolinq ユニットは、同じ 5GHz バックアップ SSID に設定する必要があります。

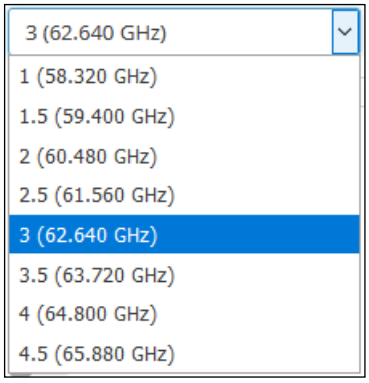
- ブロードキャスト SSID — ビーコンメッセージで設定された SSID の送信を有効／無効にします。

- 暗号化 — 60GHz インターフェースの無線セキュリティの方法を設定します。無効にすると、無線リンクにセキュリティがなくなってしまいます。有効にすると、ポイントトゥーポイントリンクの Metrolinq ユニットは、認証と暗号化に、事前に共有した WPA2 セキュリティを使用します。（デフォルトは無効です）。
  - 暗号化した暗号 —WPA2 事前共有キーに使用する暗号化した暗号を設定します。
    - CCMP（AES）—AES-COMP は、WPA2 に必要な暗号化された暗号です。
    - 自動 : TKIP ＋ CCMP（AES）— この機能を使用すると、使用されている暗号化の方法を、リンクパートナーと関連づけている間に検出できます。
  - キー — 暗号化に使用する、WPA2 事前共有キーを設定します。

フィジカル無線設定

- MCS レート — Metrolinq が、60GHz インターフェースで、パケットを送信するデータレートを設定するために使用される、変調及びコーディングスキームです。
- チャネルの帯域幅 —60GHz 無線の場合、2160MHz または 1080MHz のチャネル帯域幅が選択できます。（デフォルトは 2160MHz です）。
- チャネル —60GHz インターフェースで通信するために Metrolinq（Metrolinq）が使用する無線チャネルです。使用可能なチャネルは、無線、チャネル帯域幅。及び規制国の設定によって異なります。

図 229: 60GHz 無線チャネル



- Tx パワー —60GHz インターフェースで送信される、無線信号の最大電力を調整します。送信電力が高いほど、送信範囲が広くなり、データレートが高くなります。（電力設定とデフォルトの範囲は、AP モデルと規制国の設定によって異なります）。

- AMPDU —集約されたMACプロトコルデータユニットの使用を有効／無効にします。802.11 プロトコルのオーバーヘッドのため、物理層（PHY）のデータレートが向上しても、実際のスループットは 1 ポイント以上の増加も見せません。パフォーマンスを向上させる主なメディアアクセス制御機能は集約することによって行われます。MAC プロトコルデータユニット (MPDU) の集約は、MPDU 集約または A-MPDU 集約と呼ばれます。（デフォルトは有効セル）。

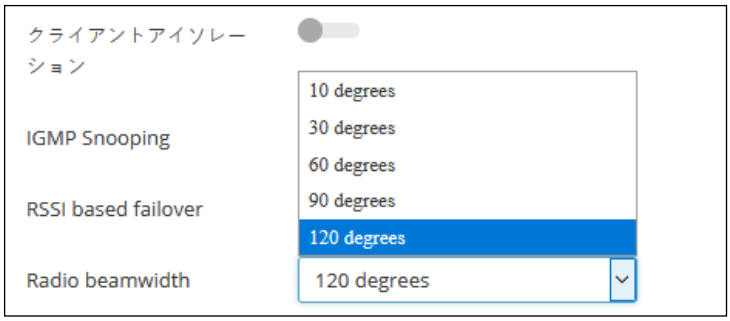
- クライアントの分離 — この機能を有効にすると、無線クライアントは LAN と通信し、インターネットへ到達できます。しかし相互に通信することはできません。（デフォルトは OFF の状態です）。

- IGMP スヌーピング — この機能を有効にすると、60GHz インターフェースを介してマルチキャストストリームを管理及びフィルタリングを行うことができます。

- RSSI ベースのフェールオーバー — この機能が有効になると、60GHz リンクの受信強度のインディケーター（RSSI）が “RSSI フェールオーバーの限度 “ を下回ると、リンクが 5GHz バックアップリンクにフェールオーバーするようになります。（デフォルトはー 65 です。範囲はー 95 から −25 です）

Metrolinq 60LW、2.5-60-18-BF、10G Tri-Band Omni の設定

図 230: Metrolinq 無線の無線ビーム幅



- 電波ビーム幅 — Metrolinq60lw、2.5−60−18-BF、と 10G Tri-Band Omni のセクターアンテナビーム幅を設定します。ビーム幅が狭いほど、信号の指向性が高くなり、アンテナゲインが高くなります。（オプションは 10、30、60、90、120 度です。デフォルトは 120 度です）。

- DBSC— この機能を有効にすると、指向性ビームスキャンと接続（DBSC）が、フェーズドアンテナ配列に、準オムニ単一指向性ビームのみを使わせ、広い範囲でのスキャンニングが可能になります。準オムニビームのゲインが低いと、接続してトラフィックを維持する最長の距離が制限されることになります。DBSC を有効にすることで、スキャンを行なってい

る際に方向性のあるビームを使用することになり、低レベルのゲインによる問題を解決できます。（デフォルトは無効です）。

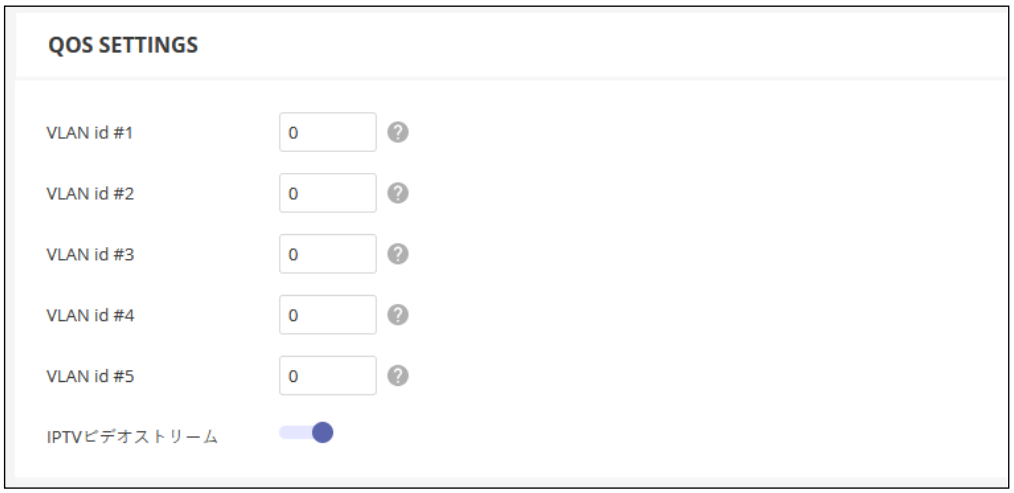
クオリティオブサービスの設定

クオリティオブサービス（QOS）の設定のタブを使用すると、特定の VLAN を優先度の高いトラフィックとして割り当てることができます。データパケットは高優先度トラフィックとしてタグづけされ、他のパケットよりも先に送信されます。

MetroLinq インターフェースは 3 つの有線キューを有します。一つ目は制御メッセージ用、二つ目は優先度の高いトラフィック、三つ目は他のすべてのトラフィックです。優先度が 4 から 7 の IEEE802．1p、または同じく優先度が 4 から 7 の IP ／ TOS など、高い数値でタグづけされたパケットは、高優先度のトラフィックとして分類され、デフォルトでは優先度キューに配置されます。

QOS の設定ページでは、最大 5 つの VLAN を優先度の高いトラフィックとして設定できます。つまり VLAN ID を持つデータフレームは、すべて高優先度のトラフィックとして分類され、高優先度キューに入れられることになります。

図 231: Metrolinq QOS の設定



このページは以下のアイテムを表示します。

- VLAN ID # 5—VLAND ID を優先度の高いトラフィックとして設定します。全ての 5 つの VLAN の優先度は同じです。（範囲は 1－4094 です。　数値が 0 の場合は無効です）。

- IPTV ビデオストリーム — 有効にすると、全てのマルチキャストフレームが高優先度として分類され、IPTV ストリームのパフォーマンスが向上します。（デフォルトは無効の状態です）。

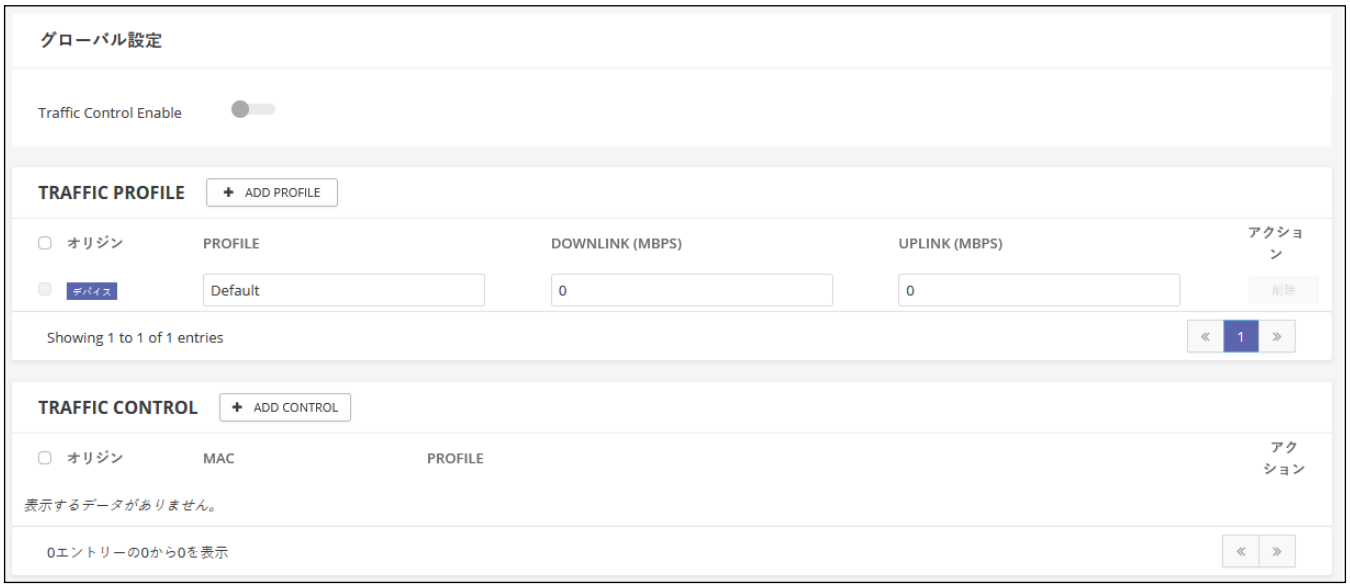
トラフィックコントロール

トラフィックを制御する設定を使用して、指定したデバイスのアップリンクとダウンリンク帯域幅を制限します。まずアップリンクとダウンリンクの帯域幅を指定するトラフィックプロフィールを作成してから、プロフィールを特定のデバイスの MAC アドレスにバインドします。

“ プロフィールを追加する “ ボタンをクリックして、新しいファイルを追加します。プロフィールに名前をつけ、帯域幅の制限を指定します。

プロフィールを MAC アドレスにバインドするためには、“ コントロールを追加する “ ボタンをクリックしてからデバイスの MAC アドレスを入力し、プルダウンリストからプロフィール名を選択します。

図 232: MetroLinq トラフィック制御の設定



このページには以下のアイテムが表示されます。

- トラフィックの制御が有効 — 設定されたトラフィックの制御設定を有効にします。
- トラフィックプロフィール — 必要なプロフィールを設定します。
  - プロフィール — プロフィールの特徴の詳細となる名前をつけます。

- ダウンロード（Mbps）— (Default: 0) 最大ダウンリンクレートを、0−1000Mbp の値に設定します。
- アップロード (Mbps) — 最大アップリンクレートを 0−1000Mbp の値に設定します。（デフォルトは 0 の状態です）。

- トラフィックの制御— トラフィックプロフィールをMAC アドレスにバインドします。
  - MAC— デバイスの MAC アドレスです。
  - プロフィール — プロフィールの名前を設定します。

リンクパスツールの使用

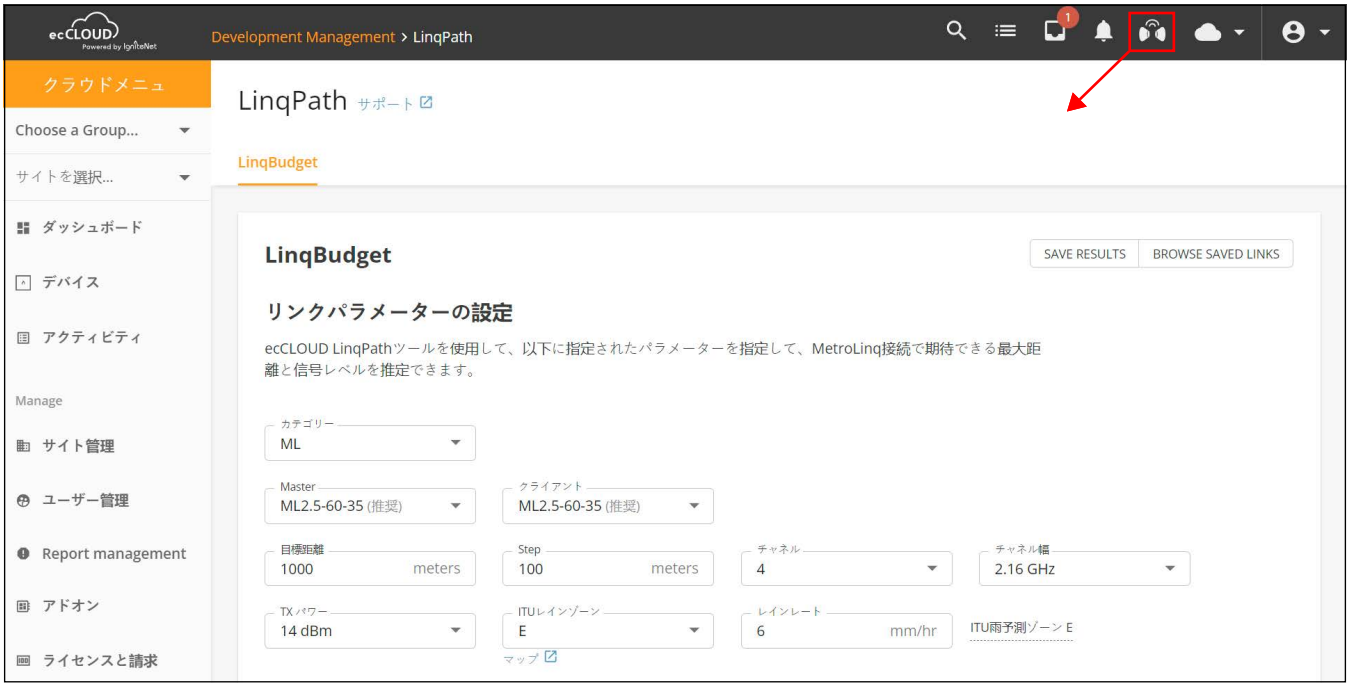
Edgecore リンクパスツールを使用すると、特定のパラメー ターで接続した時の、Metrolinq との最大限の距離と信号のレベルを推定できます。ITU レインモデルを使用すると、統計的な雨や雪などによる接続への影響のデータも知ることができます。

リンクパスツールは、無料の ecCLOUD アカウントで使用できます。上部のナビゲーションメニューのアイコンをクリックすると、リンクパスにアクセスできます。

リンクバジェットセクションで計画されたリンクの詳細を指定し、結果と RSSI グラフを表示して、必要なリンクパフォーマンスを満たしているか確認します。

“ 結果の保存 “ ボタンを使用して、リンクパスの計算を保存できます。最大 10 件までのリンク結果をリンクパス履歴に保存できます。

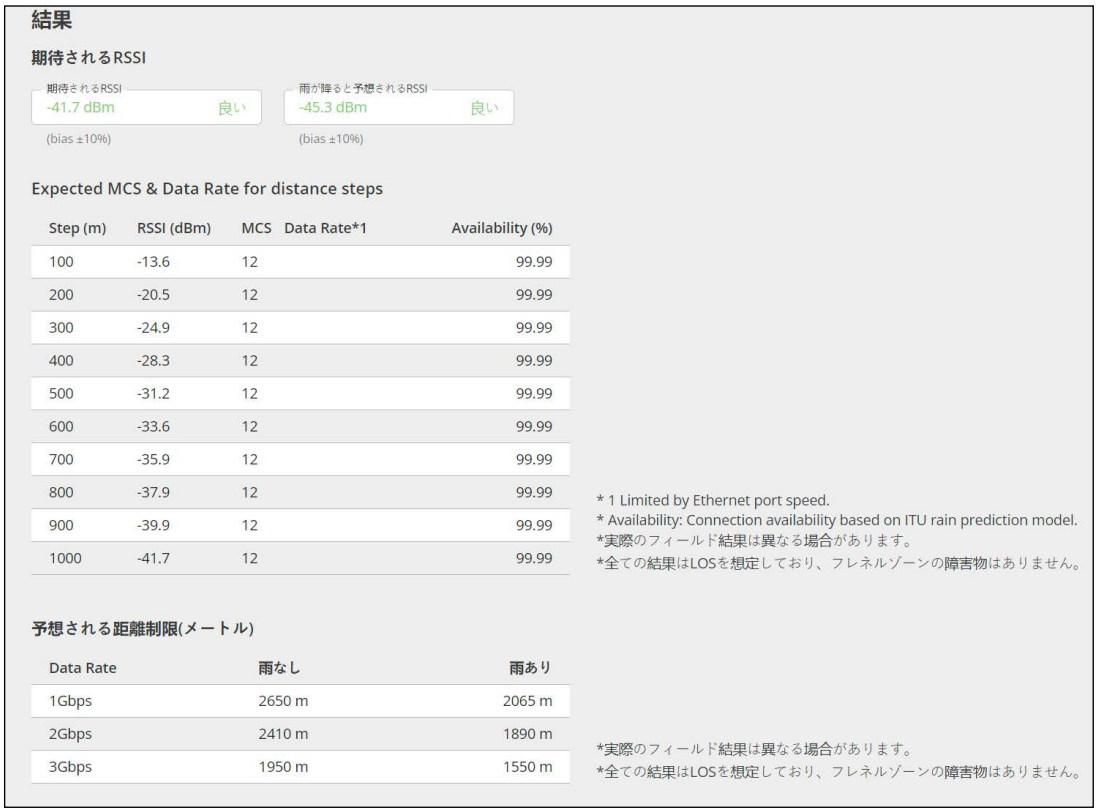
図 233: MetroLinq リンクパスの設定



このセクションは以下のアイテムを表示します。

- マスター —PTTP または PTMP マスターとして使用される Metrolinq モデルです。
- クライアント —PTP または PTMP クライアントとして使用される Metrolinq モデルです。
- 目標距離 — リンクの目標距離として意図された距離です。
- Step — ターゲット距離までの様々な距離で期待されるリンク性能を評価するための距離間隔。(デフォルト：ターゲット距離の 10)
- チャネル — リンクが操作する無線のチャネルです。
- チャネルの幅 — 設定された無線のチャネル幅です。
- Tx パワー — Metrolinq60GHz 無線用に設定される送信電力です。
- ITU レインゾーン —ITU レインゾーンの中でリンクが運転します。さまざまな雨天の地域をハイライトする地図が、リンクパスツールによって提供されます。
- 降水量 — 指定された地域の予測 ITU 降水量（mm/ 時間）です。

図 234: MetroLinq リンクバジェットの結果



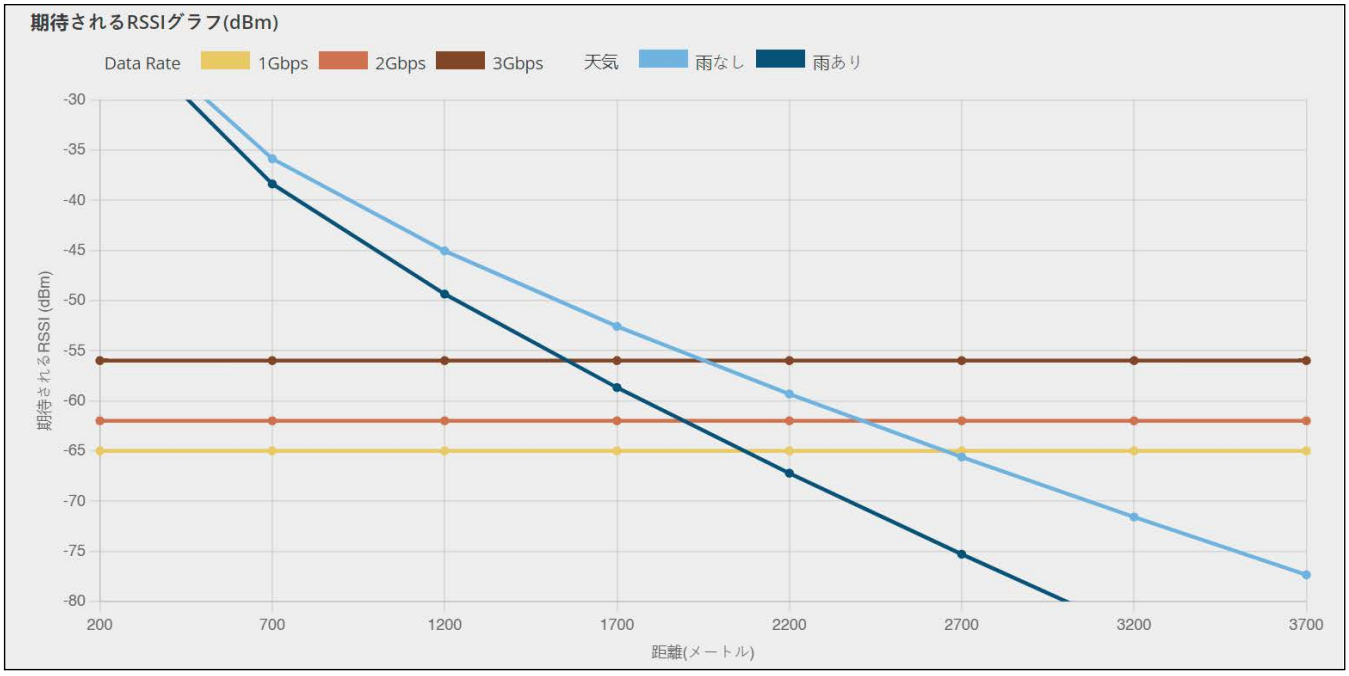
このセクションでは以下のアイテムを表示します。

- 期待される RSSI — 対象となる距離入力ボックスで指定された距離に基づいて、リンクの期待される RSSI を表示します。
- 雨天時の予想される RSSI — 雨が降っている時の、リンクの予想される RSSI を、対象となる距離入力ボックスに指定された距離に基づいて表示します。
- 距離ステップの予想 MCS とデータレート（MLTG 製品のみ対応）— 設定した目標距離までの各ステップ間隔における予想 RSSI、MCS 値、対応するデータレートを表示します。
  - Data Rate — イーサネットポート速度によって制限される、予想されるデータ速度。
  - Availability — ITU 雨量予測モデルに基づく接続可用性。
- 予想される距離の限度 — 選択した Metrolinq モデルのリンクが 3Gbps、2Gbps、1Gbps を達成する、最大距離を予想して表示します。“ ウイズレイン “ の数値には、ITU レインゾーン及びレインレート設定を使用して統計を出した、雨天によるフェージングについての情報も提供します。

RSSI と距離の関係グラフ

リンクパスは、予想される RSSI 対距離のグラフも表示します。紫色のグラフ、“ 雨が降らない状態 “ の線は、雨が降らない状態での RSSI を示しています。青い “ 雨が降っている状態の線は、ドロップダウンメニューの “60GHz レインリライアビリティ “ で選択した時間の割合を超える、予想 RSSI の値です。1Gbps、2Gbps、3Gbps の回線は、各データレートを達成できる RSS レベルを示しています。

図 235: MetroLinq パス予想 RSSI のグラフ



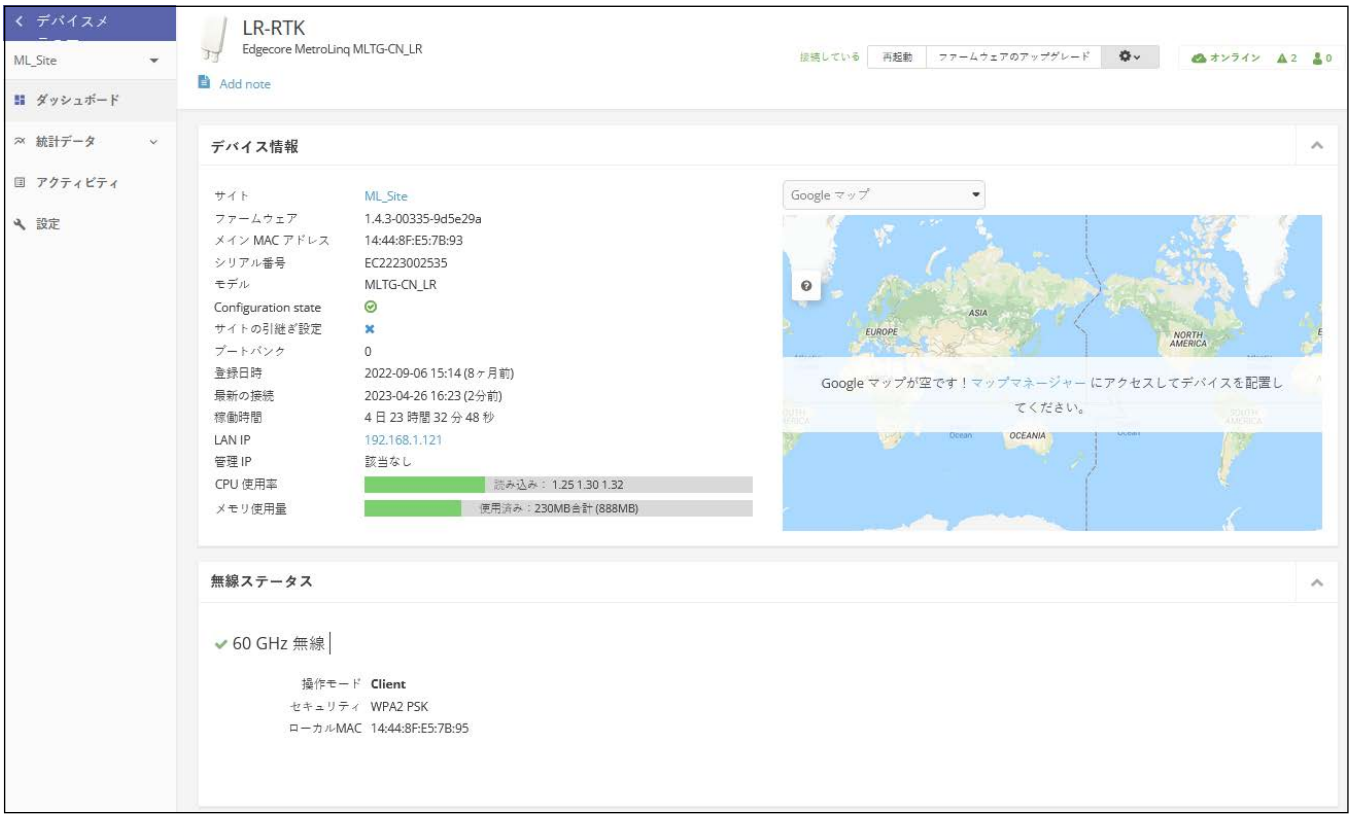
11 Terragraph デバイス構成

この章では、Terragraph MLTG-CN ユニットのデバイスレベルでの設定について説明します。以下のセクションが含まれています：

Terragraph 構成

このセクションでは、Terragraph MLTG-CN デバイスのデバイスレベルの設定について、サイトレベルでは利用できない特定の設定を含めて説明します。

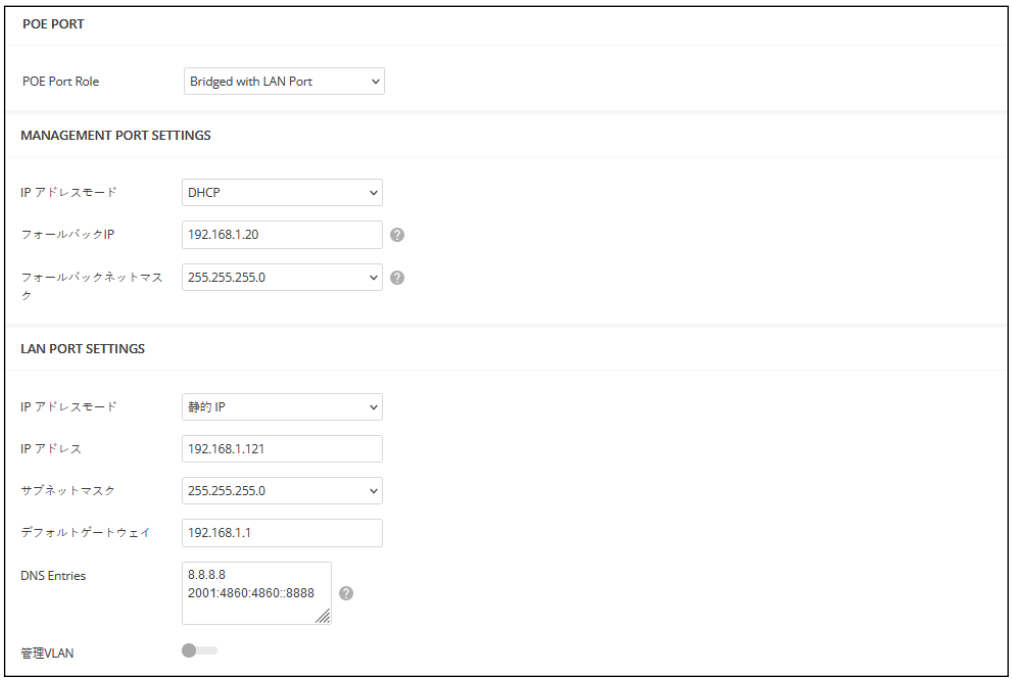
図 236: Terragraph デバイスダッシュボード



ネットワーク全般の設定

General Networking タブをクリックし、管理ポートおよび LAN ポートの設定を行います。

図 237: Terragraph デバイス全般の設定



このページでは、以下の項目が表示されます：

PoE Port

- POE Port Role — アップリンクポート (PoE ポート) の機能を選択します。このポートは、デフォルトでは専用の管理ポートとして機能します。役割を「LAN ポートとのブリッジ」に変更することで、LAN ポートとして機能するようになります。

Management Port Settings

- IP アドレスモード — インターネットアクセスポートに IP アドレスを提供するために使用する方法を設定します。(デフォルト：DHCP、オプション：DHCP、静的 IP)。
- Fallback IP — DHCP サーバーが利用できない場合に使用される IPv4 アドレスです。(デフォルト：192.168.1.20)
- Fallback Netmask — Fallback IP アドレスに使用されるサブネットマスクです。(デフォルト：255.255.255.0)

LAN ポート設定

- IP アドレスモード — LAN インターフェースを静的IP モードまたは DHCP モードに設定します。DHCP モードでは、Network Behavior がレイヤー 2 ブリッジに設定されている場合、DCHP 要求がレイヤー 2 ネットワークにブロードキャストされます。Network Behavior が VXLAN に設定されている場合、DHCP リクエストは VXLAN トンネルを経由してコアネットワークに送信されます。

- IP アドレス — IP アドレスモードが "Static IP " の場合の静的な IP アドレスです。

- サブネットマスク — IP アドレスモードが "Static IP "のときのサブネットマスク。

- デフォルトゲートウェイ — デフォルトゲートウェイの IPv4 アドレスで、以下の場合に使用されます。

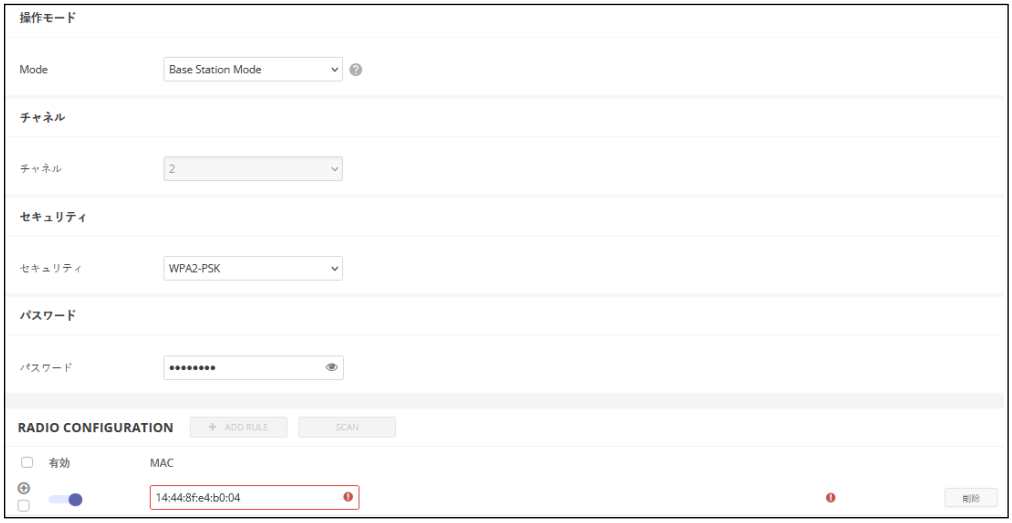
- DNS エントリ — クライアントがローカルネットワークから指定されたドメインを通じて Web インターフェースにアクセスできるようにします。

- 管理 VLAN — サイトデバイスの管理 VLAN を有効にするには、このオプションを選択します。このオプションを有効にすると、内蔵のローカルネットワーク（例：192.168.2.1）上のデバイスにアクセスできなくなります。指定した VLAN ネットワークのデバイスにのみアクセスできるようになります。デバイスの IP モードが DHCP に設定されている場合、デバイスは VLAN ネットワークに割り当てられたサブネット範囲の新しい IP アドレスも要求します。

無線設定

「無線設定」タブをクリックすると、動作モードやセキュリティの設定を行うことができます。

図 238: Terragraph デバイス無線設定



このページでは、以下の項目が表示されます：

Operation モード

- モード — 1.4.2 より前のファームウェアバージョンの場合：
  - クライアントモード（Terragraph Mode）— Terragraph DN デバイスへの接続を許可する。このモードでは、クライアントは DN デバイスが接続するのを受動的に待ちます。
  - クライアントモード（ポイントツーポイントモード）— ベースステーションモード CN デバイスへの接続を許可する。このモードでは、クライアントは受動的に基地局モード CN が接続するのを待ちます。
  - 基地局モード — クライアントモード（ポイントツーポイントモード）の CN 装置とのリンクを作成できます。MLTG-CN ユニッ トでは、最大 15 リンクまで作成可能です。MLTG-CN LR の場合は、1 リンクのみ作成可能です。
- モード — 1.5.0 以降のファームウェアバージョンの場合：
  - クライアントモード - DN またはベースステーションモードの CN デバイスへの接続を許可する。このモードでは、クライアントは受動的に接続を待ちます。

- 基地局モード - クライアントモード（ポイントツーポイントモード）の CN 装置とのリンクを作成できます。MLTG-CN ユニットでは、最大 15 リンクまで作成可能です。MLTG-CN LR の場合は、1 リンクのみ作成可能です。

Channel

- チャネル - ベースステーションモードでは、リンクの作業チャネル（1 ～ 4）を選択できます。

Security

- Security - リンクに使用されるセキュリティ方法です。現在のバージョンでは、WPA2-PSK のみサポートされています。

Password

- Password - WPA2-PSK のパスワードを設定します。

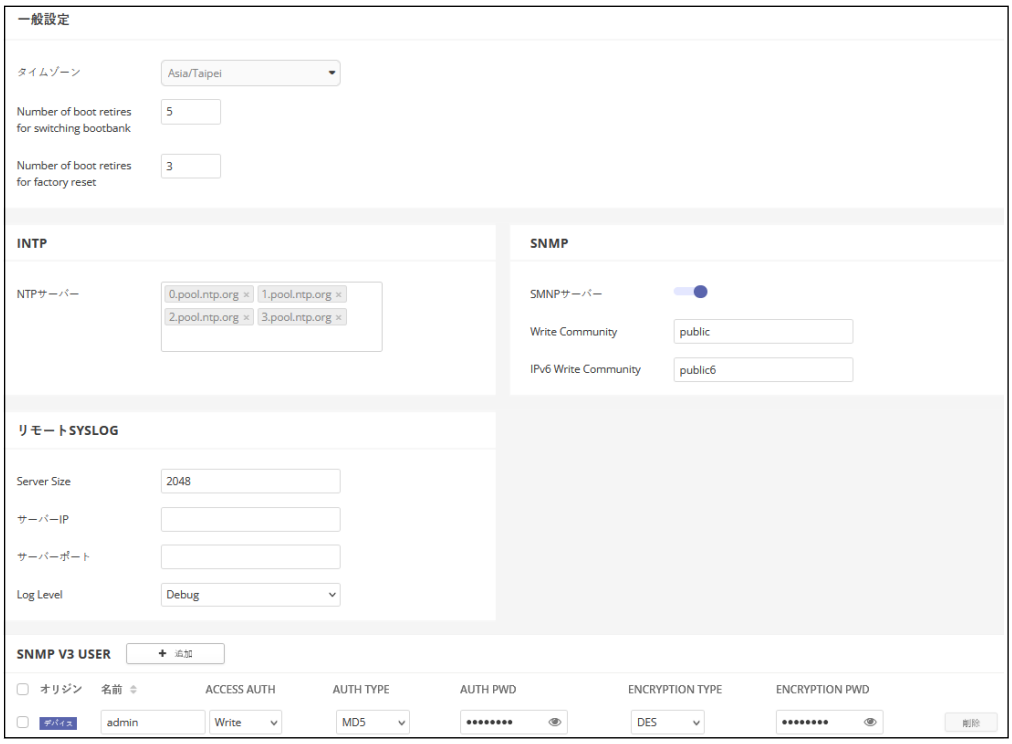
Radio Configuration

- 基地局モードで「ADD RULE」をクリックし、別の MLTG-CN 機器の 60GHz 無線 MAC アドレスを入力します。また、"SCAN " をクリックすると、他の MLTG-CN 機器の MAC アドレスを検索して選択できます。

システム設定

システム設定」タブをクリックすると、一般設定、NTP、SNMP、syslog を設定できます。

図 239: Terragraph デバイスシステム設定



このページでは、以下の項目が表示されます：

General Settings

- タイムゾーン — 現地時間に対応した時刻を表示するには、プルダウンリストから定義済みのタイムゾーンのいずれかを選択します。
- ブートバンク切り替えのためのブートリトライ回数 — 次のブートバンクに切り替えるまでのブートリトライ回数の最大値です。(範囲 : 1-254; デフォルト : 5)
- Number of boot retires for factory reset — デバイスをデフォルトにリセットするまでの起動再試行回数の最大値を指定します。(範囲 : 1-254; デフォルト : 3)

Network Time (NTP)

ネットワークタイムプロトコル（NTP）により、デバイスはタイムサーバーからの定期的な更新に基づき、内部クロックを設定できます。デバイスは NTP クライアントとして動作し、指定されたタイムサーバーに定期的に時刻

同期要求を送信します。デバイスは、設定された順序で各サーバーをポーリングし、時刻の更新を受信しようとします。

- NTP サーバー — NTP サーバーの IP アドレスを入力します。

SNMP

SNMP（Simple Network Management Protocol）は、ネットワーク上のデバイスを管理するために特別に設計されています。一般的には、ネットワーク環境で適切に動作するようにデバイスを設定したり、パフォーマンスを評価したり、潜在的な問題を検出するためにデバイスを監視したりするために使用されます。

- SNMP Server — SNMP の有効 / 無効を設定します。
- 書き込みコミュニティ — パスワードのように動作し、SNMP プロトコルバージョン 2 によるアクセスを許可するテキスト文字列です。このコミュニティ文字列は、IPv4 ユーザのアクセスを確認します。
- IPv6 Write Community — パスワードのように動作し、SNMP プロトコルバージョン 2 によるアクセスを許可するテキスト文字列です。このコミュニティ文字列は、IPv6 ユーザのアクセスを検証します。

リモート Syslog

このデバイスでは、記録されるイベントの種類を含むエラーメッセージのロギングを制御し、リモートシステムログ（syslog）サーバーまたは他の管理ステーションへのロギングを構成できます。

- Server Size — エラーメッセージのロギングに使用する利用可能なメモリーを指定します。(デフォルト：64KiB)
- Server IP — syslog メッセージを送信するリモートサーバーの IPv4 または IPv6 アドレスを指定します。
- Server Port — リモートサーバーが使用する UDP ポート番号を指定します。(範囲：1 ～ 65535、デフォルト：514)。
- ログレベル — メニューを使用して、コンソールに印刷するログの重大度を選択します。選択した深刻度レベルのログと、それ以上の深刻度のすべてのログが印刷されます。たとえば、[エラー] を選択した場合、ログに記録されるメッセージには、[エラー]、[クリティカル]、[アラート]、[緊急] があります。デフォルトの深刻度レベルは Debug(7) です。深刻度は、次のレベルのいずれかになります：

表 3: ロギングレベル

レベル	重大度名	概要
7	デバッ	デバッギングメッセ
6	インフォメ	情報提供メッセージのみ
5	お知	コールドスタートなど、正常だが重要な状態
4	警告	警告条件（例：return false、予期せぬ return）。
3	エラ	エラー状態（例：入力が無効、デフォルトが使用されているなど）。
2	クリテ	クリティカルな状態（例：メモリ確保、または空きメモリエラー - リソース枯渇）
1	アラート	早急な対策が必要
0	緊急	システム使用不可

* 現在のファームウェアリリースでは、レベル 2、5、6 のエラーメッセージのみです。

SNMP V3 User

SNMP プロトコルバージョン 3 は、アカウント認証とデータの暗号化により、安全なアクセスを提供します。SNMP v3 のユーザリストは、以下の項目で定義できます。

- 名前 — SNMP サービスにアクセスするために使用されるユーザ名。
- Access Auth. — アクセス許可を " 読み取り専用 " または " 書き込み " で選択します。
- Auth. Type — 認証のためのハッシュアルゴリズムを選択します。
- Auth. Pwd。— 認証用のパスワードを設定する。
- Encryption Type — データパケットの暗号化アルゴリズムを選択します。
- Encryption Pwd — データ暗号化用のパスワードを設定します。

12 スイッチ装置の設定

このチャプターはデバイスレベルでの設定の設定を説明します。以下のセクションがあります。

スイッチの設定

Edgecore スイッチデバイスはサイトレベルからのみサイト ポートセキュリティを引き継ぐことができます。その他の設定は、デバイスレベルで設定する必要があります。

このセクションでは、スイッチデバイスの設定について説明します。ecCLOUD は、下記の Edgecore モデルをサポートしています。

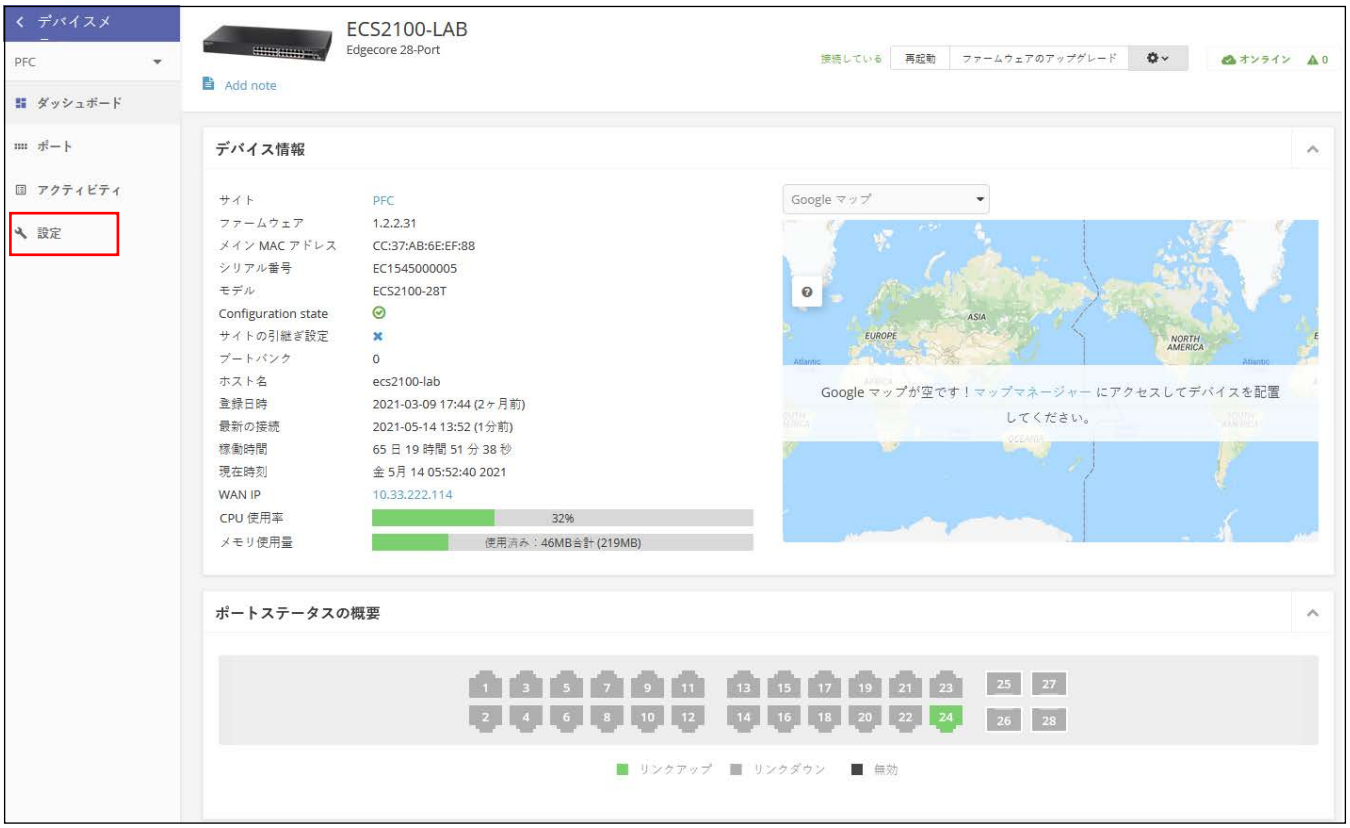
ECS2100-10P, ECS2100-10T, ECS2100-28P, ECS2100-28T, ECS2100-28PP, ECS2100-52T

ECS4100-12T, ECS4100-12PH, ECS4100-28P, ECS4100-28T, ECS4100-52P

ECS4120-28Fv2, ECS4120-28Fv2-I, ECS4120-28T, ECS4120-52T

注意：このチャプターでは、ecCLOUD から入手できるスイッチ設定の例を説明します。完全な機能のサポートと設定については、ウエブ管理ガイドと、CLI リファレンスガイドをご覧ください。www.edgecore.com. からダウンロードできます。

図 240: スイッチデバイスダッシュボード

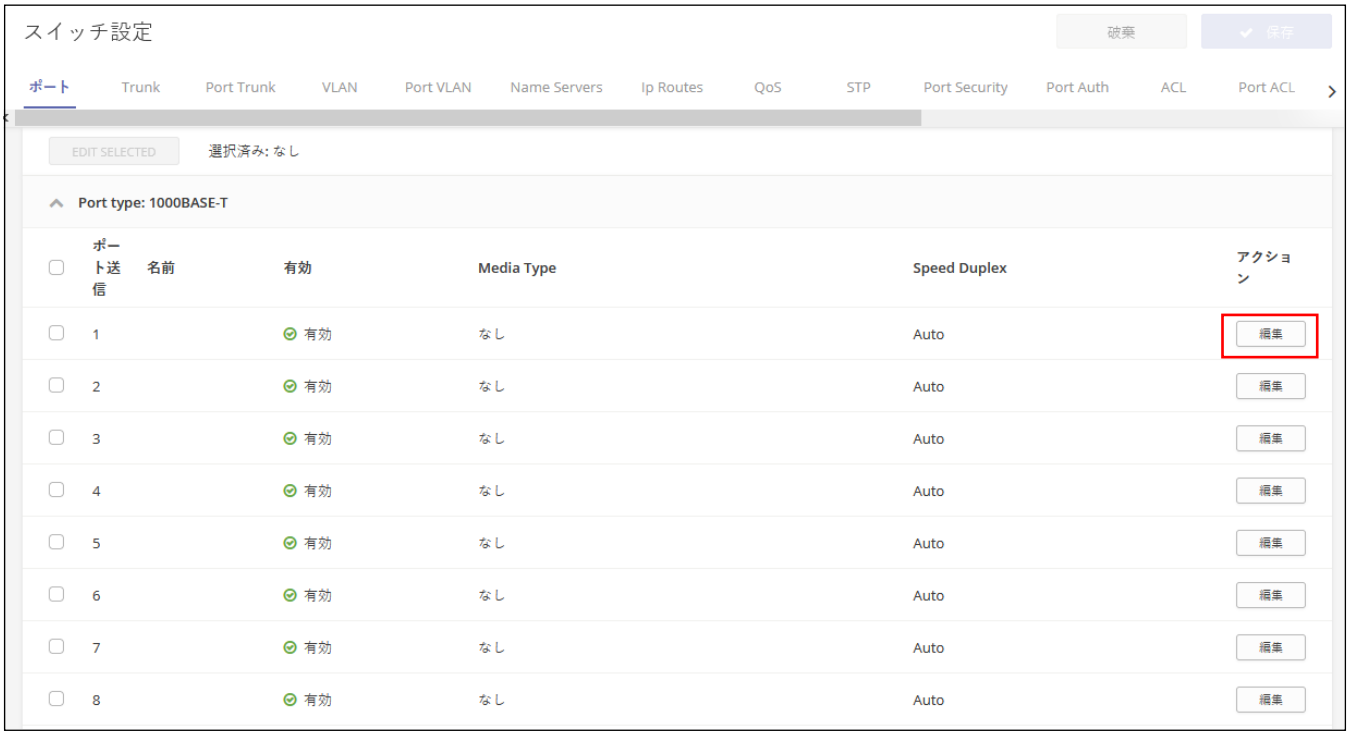


ポート設定

スイッチ設定ポートタブを使用すると、基本的なポート設定にアクセスできます。

編集ボタンをクリックして、ポートインターフェースを有効／無効にできます。オートネゴシエーションとインターフェース機能を設定して宣伝をしたり、速度、デュプレックスモード、フローの制御を手動で修正できます。

図 241: スイッチポート



トランクの設定

トランクは 1 つの仮想集約リンクとして機能する、デバイス間の複数のリンクです。ポートトランクは、ボトルネックが存在するネットワークセグメントの帯域幅を劇的に増加させるだけではなく、2 つのデバイス間にフォールトトレランスリンクを提供します.

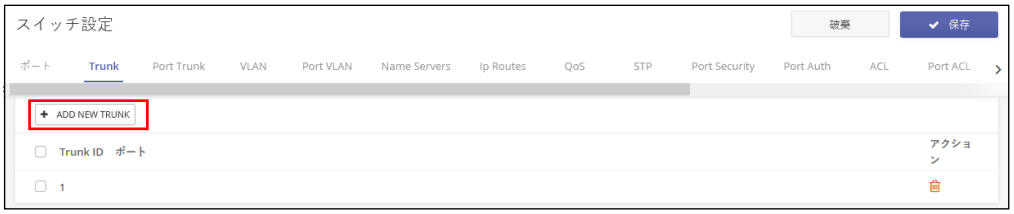
スイッチ間に静的トランクを設定する際は以下のことに注意してください.

- 1 ループの作成を回避するために、スイッチ間に対応するネットワークケーブルを接続する前に、トランクの設定を完了してください。
- 接続部の両端のポートは、トランクポートとして設定される必要があります。

- 異なるタイプのスイッチで静的トランクを設定する場合、シスコイーサチャネル（Cisco Ether Channel）基準を満たすものである必要があります。
- トランクの両端のポートは、スピード、デュープレックス、フロウの制御、VLAN 割り当てなどにおいて、同じ方法で設定してください。

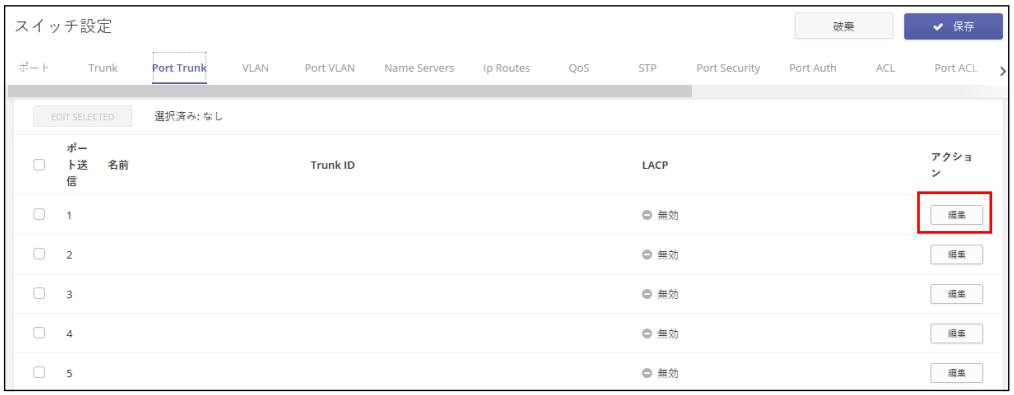
トランクタブをクリックしてから " 新しいトランクを追加する " ボタンをクリックして、トランク識別子を作成します。

図 242: トランクを設定する



タブをクリックして、メンバーポートを静的トランクに追加します。編集ボタンをクリックして、トランク ID ポートに割り当てます。

図 243: トランクポートの設定



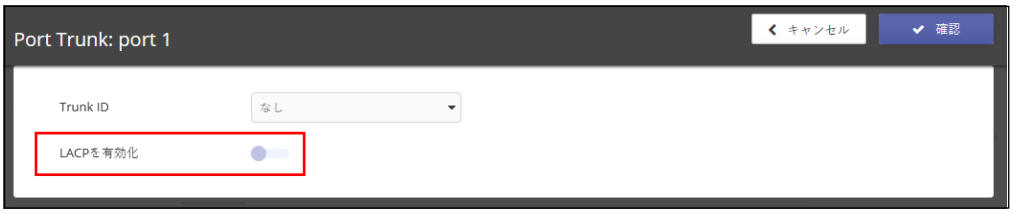
LACP トランク

リンク集約のコントロールプロトコル（ LACP）を使用すると、2 つのスイッチ間に動的トランクを作成できます。LACP で設定されたポートは、別のデバイスの LACP で設定されたポートとトランクリンクを自動的に交渉します。静的トランクの一部としてまだ設定されていない限り、スイッチ上の任意の数のポートを LACP として設定できます。別のデバイスのポートが LACP として設定されている場合、スイッチとそのデバイスはトランクリンクの交渉をします。

LACP トランクを設定する際は、下記の点を注意してください。

- ネットワークでループができることを防ぐためには、ポートを接続する前に LACP を有効にしてください。また LACP を無効にする前にポートを切断してください。
- 対象のスイッチが接続したポートの LACP を有効にした場合、トランクは自動的に起動します。
- LACP を使用して別のスイッチで作られたトランクには、次回に使用可能なトランク ID が自動的に与えられます。
- 同じ対象スイッチに接続されていて、LACP が有効になっているポートの数が、ポートの最大数を超えている場合、後から追加された ポートはスタンバイモードとなり、アクティブなリンクにエラーが出た場合のみ有効化されます。
- LACP トランクの両端の全てのポートは、フルデュープレックス（重複）の状態で、自動に交渉ができるように設定する必要があります。

図 244: LACP トランクの設定



VLAN の設定

VLAN タブをクリックして、VLAN グループを作成、または削除してください。あるいは管理ステータスを設定してください。このスイッチで使用される VLAN グループに関する情報を、外部のネットワークデバイスに伝達するには、これらのグループに VLAN ID を示す必要があります。

新しい VLAN を追加するボタンをクリックして、新しい VLAN ID を作成します。VLAN を 3 レイヤーのインターフェースとして定義することもできます。ただし、このことについては、VLAN に IP アドレスを割り当てる前に設定してください。

図 245: VLAN の設定

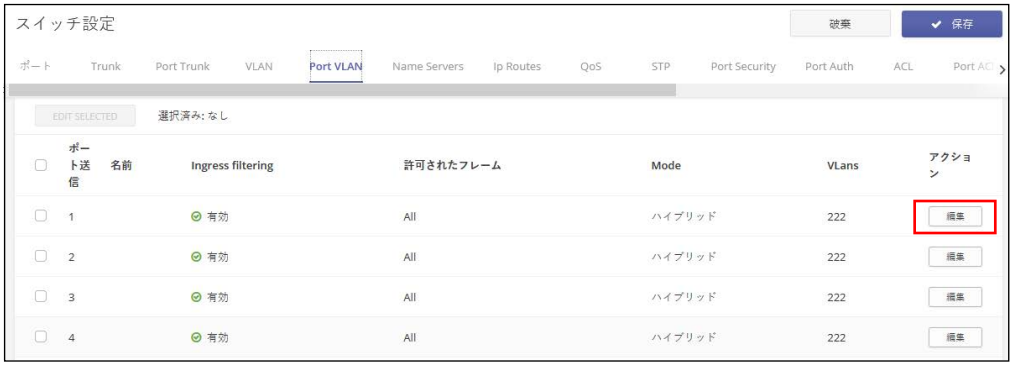
VLAN ポートメンバーの追加

スイッチの VLAN を作成して有効にする際には、各ポートを、参加する VLAN グループに割り当てる必要があります。デフォルトでは、全てのポートが、タグづけされていないポートとして VLAN1 に割り当てられている状態です。もしポートに、一つ以上の VLAN までトラフィックを伝達させ、接続のもう片方にある中間ネットワークデバイスやホストにその VLAN をサポートさせたい場合は、そのポートをタグ付けした状態で追加してください。次にポートを、同じ VLAN にトラフィックを運ぶパスに沿った、別の VLAN 対応ネットワークデバイスに割り当てます。ただし、このスイッチのポートを、1 つ以上の VLAN と関連づけたいにもかかわらず、中間ネットワークデバイスのもう片側にあるホストが VLAN をサポートしていない場合は、ポートをタグ付けしないで追加してください。

注意： ecCLOUD は、AP とスイッチ間の VLAN 同期をサポートします。VLAN タギングが SSID に対して有効になっている場合、設定された VLAN ID は、ecCLOUD によって接続されたスイッチポートに自動的に " プッシュ " されます。これによって AP からの VLAN タグづきトラフィックをスイッチポートで受け入れることができ、接続の失敗を回避できます。

ポート VLAN タブをクリックすると、ポート VLAN メンバーシップを表示できます。

図 246: VLAN ポートメンバーシップの設定



編集ボタンをクリックすると、操作モード（ハイブリットまたは 10 トランク）、デフォルトの VLAN ID （PVID）、受け入れられたフレームのタイプ、入力フィルターなど、特定のポートに対しての VLAN の操作を設定できます。ポートが 802．1QVLAN 準拠のデバイスに接続されている場合 は、タグづきとして割り当てます。VLAN 対応のデバイスに接続されていない場合は、タグづけなしとして割り当てるか、あるいはスイッチが VLAN に追加することを禁止する設定をしてください。

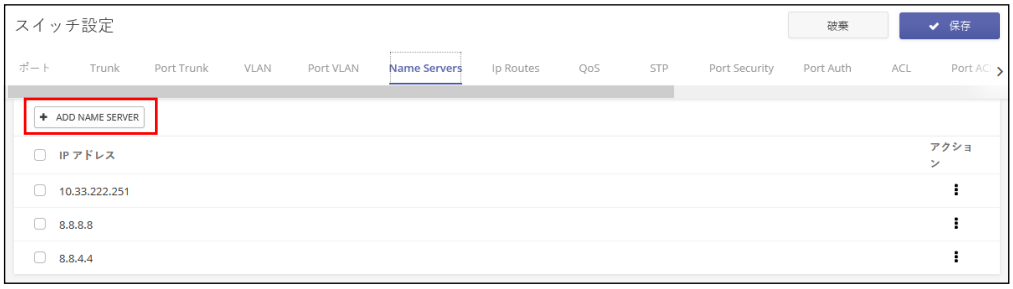
図 247: VLAN ポートの設定

ネームサーバーの設定

ネームサーバータグをクリックして、ダイナミック DNS ルックアップに使用するネームサーバーのリストを設定します。複数のネームサーバーが指定されている場合、サーバーは応答を受信するか、応答なしの状態のままでリストの順番が回ってくるまで保留されてから、照合されます。

ネームサーバーを追加するボタンをクリックしてから、ドメインネームのサーバーの IPv4,IPv6 のアドレスを指定して、ネームトゥーアドレスレゾリューションを使用します。

図 248: ネームサービスの設定



静的 IP ルートの設定

Edgecore スイッチは静的ルーティング定義を介した IP ルーティングとルーティングパス管理をサポートしています。IP ルーティングが機能している場合、スイッチはワイヤースピードルーターとして機能します。異なる IP インターフェースを持つ VLAN 間でトラフィックを運ぶだけでなく、トラフィックを外部 IP ネットワークにルーティングします。ただし、スイッチが初めて起動された時の場合、デフォルトのルーティングはローカルの IP インターフェース間のトラフィックしか運びません。

サブネットへの特定のルートを強制的に使用するには、静的ルートが必要になる場合があります。静的ルートはネットワークトポロジーの変更に応じて自動的に変換されることがないため、ネットワークのアクセスする機能を良い状態に保つためには、少数の安定したルートのみを設定する必要があります。

ルーティングテーブルに静的ルートを入力するには、IP ルートタブをクリックしてから、IP ルートの追加ボタンをクリックします。宛先となるアドレスとネットマスク、及びルートに使用される次のルーターホップの IP アドレスを指定します。

図 249: IP ルートの設定

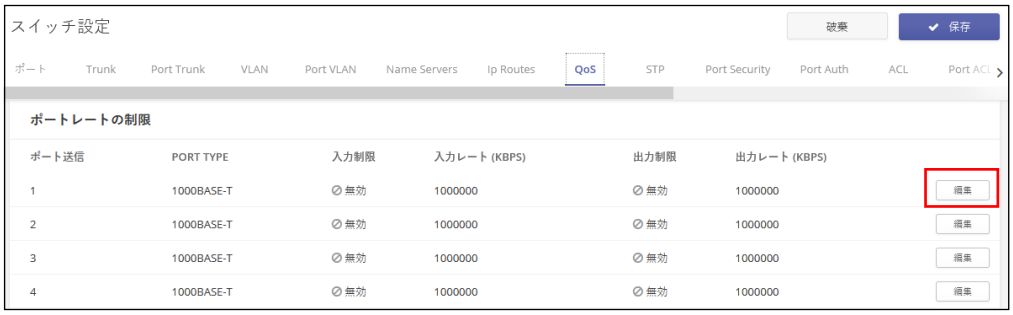
ポートレートの制限（QoS）の設定

QoS タブをクリックして、入力ポートまたは出力ポートにレート制限を申請します。この機能により、ネットワーク管理者は、ポートインターフェースで送信／受信されるトラフィックの最大レートをコントロールできます。レートの制限は、ネットワークの端にあるインターフェースで設定され、ネットワークに出入りするトラフィックを制限します。

レートの制限は、ここのポートまたはトランクに適応します。インターフェースがこの機能で設定されている場合、トラフィックレートはスイッチハードウエアによって監視され、適合性を確認されます。非適合のトラフィックはドロップされ、適合トラフィックは変更されることなく運ばれます。

ポートインターフェースの編集ボタンをクリックすると、入力または出力のレート制限を有効にし、必要なレート制限を設定できます。

図 250: ポートレートの制限を設定する



STP の設定

スパニングツリープロトコル（STP）を使用すると、ネットワークループを検出して無効にし、スイッチ、ブリッジ、またはルーター間のバックアップリンクを提供できます。これにより、スイッチはネットワーク内の他のブリッジングデバイス（STP 準拠のスイッチ、ブリッジ、またはルーター）と交渉して、ネットワーク上の任意の 2 つのステーション間に 1 つのルートのみが存在するようにします。そして、主要なリンクがダウンした場合には、自動的に引き継ぐバックアップリンクを提供します。

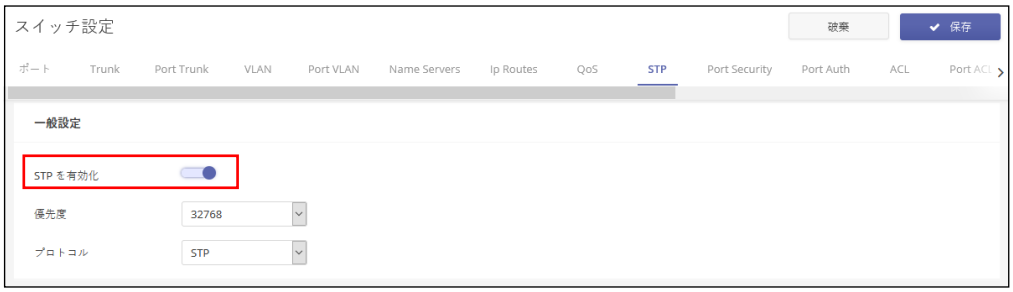
Edgecore スイッチは、以下の三種類のスパンイングツリープロトコルをサポートしています。

- STP — スパニングツリープロトコル（IEEE802．1D）です．（このオプションを選択すると、スイッチは STP 強制互換モードに設定された RSTP を使用します）。
- RSTP — ラピッドスパニングツリーです。（IEEE802．1w）
- MSTP— マルチプルスパニングツリーです。（IEEE802．1s）

STP タブをクリックして、STP を有効にします。プロトコルを選択し、スパニングツリールートデバイス（最も優先度の高いネットワークデバイスが STP ルートデバイスとなります）に使用されるブリッジプライオリティを設定します。

注意：STP の設定についての詳細は、www.edgecore.com から入手できる、特定のスイッチモデルについてのウエブ管理ガイドと CLI リファレンスガイドを参照してください。

図 251: STP の設定



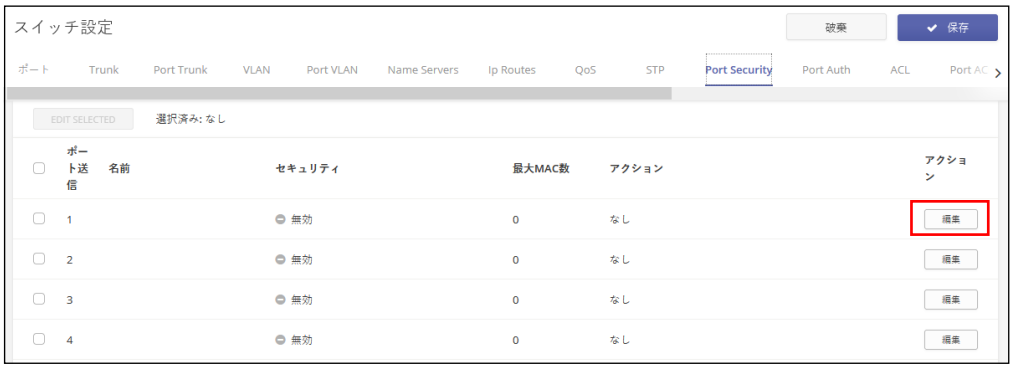
ポートセキュリティの設定

ポートセキュリティを使用して、スイッチポートが学習し、アドレステーブルに保存し、ネットワークへのアクセスを許可できるデバイス MAC アドレスの最大数を設定できます。

ポートでポートセキュリティが有効になっている場合、設定された最大値に達すると、スイッチは、指定されたポートでの新しい MAC アドレスの学習を停止します。アドレステーブルに既に保存されている送信元のアドレスを持つ着信トラフィックのみが、ポートを介したネットワークへのアクセスを許可されます。許可されていない MAC アドレスを持つデバイスがスイッチポートを使用しようとすると、侵入が検出され、スイッチが自動的にポートを無効にして、トラップメッセージを送信します。

ポートセキュリティタブをクリックしてから、設定する必要があるポートの編集ボタンをクリックしてください。ポートのセキュリティを有効にして、ポートで無効なアドレスが検出された時の実行するアクションを設定し、ポートで許可される MAC アドレスの最大数を設定します。

図 252: ポートセキュリティの設定



802.1X ポート認証の設定

IEEE802.1X(802.1X, または dot1X) 標準は、ユーザ認証の方法として、最初に資格情報を送信することを要求して、ネットワークへの不正アクセスを防止するポートベースのアクセス制御手順を定義します。ネットワーク内の全てのスイッチポートへのアクセスは、サーバーが中心となってコントロールできます。つまり、許可されたユーザは、ネットワーク内のどのポイントからでも、同じ資格情報を使用して認証を得ることができます。

ポートの認証タブをクリックして、スイッチの 802.1x ポート設定をローカルなオーセンティフィケーターとして設定します。802.1x が有効になっている場合は、クライアントとスイッチ（オーセンティフィケーター）の間で実行される認証プロセス、及びスイッチと認証サーバーの間で実行されるクライアント ID ルックアッププロセスのパラメーターを設定する必要があります。

認証サーバーの設定については、290 ページの「ログイン認証を設定する」を参照してください。

ポートの編集ボタンをクリックして、ポート認証の詳細を設定します。

図 253: ポートの認証の設定

スイッチがスイッチポートに接続されたサプリカントデバイスと認証サーバーとの間でローカルオーセンティフィケーターとして機能する場合、オーセンティフィケーター設定ページで、オーセンティフィケーターとクライアント間で EAP メッセージを交換するためのパラメーターを設定する必要があります。

ポート認証の詳細ページで、ポート制御モードを " 自動 " に設定して認証を有効にします。

図 254: ポートの認証の設定

注意：ポートの認証の設定の詳細については、www.edgecore.com から入手できる特定のスイッチモデルのウエブ管理ガイド及び CLI ガイドを参照してください。

ACL 設定

アクセスコントロールリスト（ACL）は、IPv4/IPv6 フレーム（アドレス、プロトコル、4 レイヤープロトコルポート番号または TCP 制御コードに基づく）、IPv6 フレーム（アドレス、DSCP トラフィッククラスに基づく）、または任意のフレーム（MAC アドレスやイーサネットタイプに基づく）入力パケットフィルタリングを提供します。着信パケットをフィルタリングするには、最初にアクセスリストを作成し、必要なルールを追加してから、リストを特定のポートにバインドします。

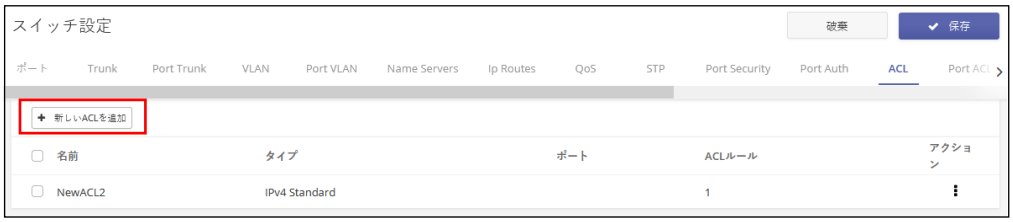
ACL は、IP アドレス、MAC アドレス、またはその他のより具体的な基準によって許可／拒否されるリストです。スイッチは、それぞれの入力パケットを、ACL の条件に従ってテストします。条件を満たすパケットはすぐに受け入れられますが、拒否ルールと一致すると削除されてしまいます。一致するルールがない場合、パケットは受け入れられます。

ACL を設定するためには、ACL タブをクリックしてから、新しい ACL の追加ボタンをクリックします。設定する ACL のタイプを選択してください。

- IPv4 スタンダード — 送信元 IPv4 アドレスに基づいて ACL を設定します。

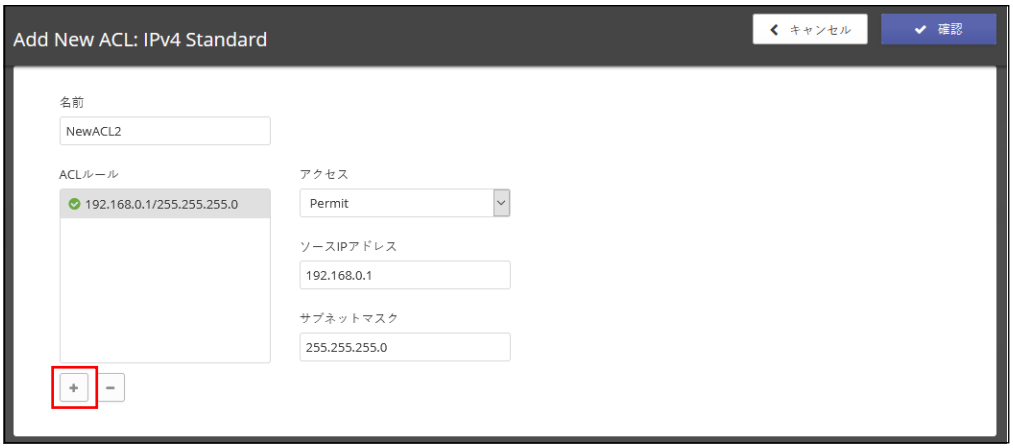
- IPv4 拡張 — 送信元及び送信先 IP アドレス v4 アドレス、TCP ／ UDP ポート番号、プロトコルタイプ、及び TCP 制御コードに基づいて ACL を設定します。
- IPv6 スタンダード — 送信元 IPv6 アドレスに基づいて ACL を設定します。
- IPv6 拡張 — 送信元および宛先 IPv6 アドレス、DSCP トラフィッククラス、または次のヘッダータイプに基づいて ACL を設定します。
- MAC — ハードウエアアドレス、パケットのフォーマット、イーサネットのタイプに基づいて ACL を設定します。
- ARPARP —ARP メッセージアドレスに基づいて、ACL を設定します。

図 255: ACL の設定



新しい ACL ページを追加するページで、ACL に名前を与え、“ ＋ ” ボタンをクリックして ACL に追加するルールを設定してください。

図 256: 新しい ACL を追加する

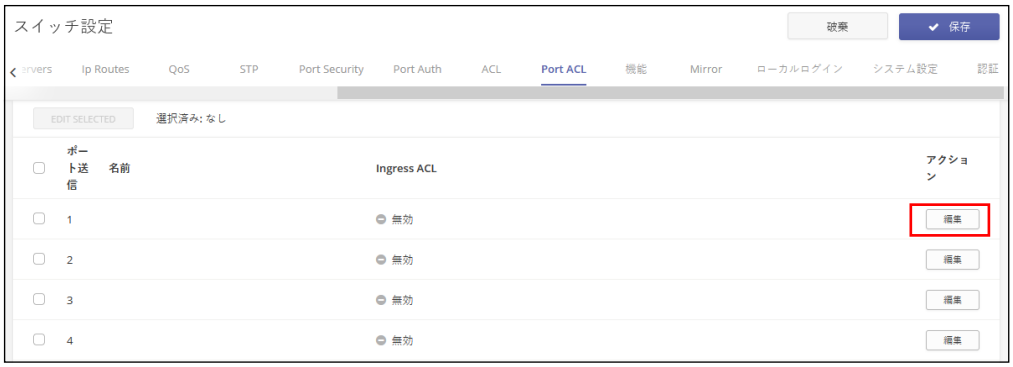


ポートを ACL にバインドする

ACL を設定したのち、ポート ACL タブをクリックして、受信するトラフィックをフィルタリングして、対応するポートに運ぶ働きをするポートをバインドしてください。

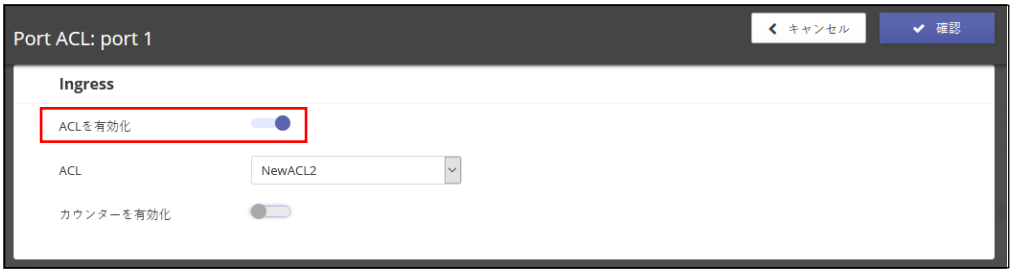
編集ボタンをクリックしてポートの ACL を設定してください。

図 257: ポート ACL のバインディング



ポート ACL の編集ページで、設定済みの ACL 名を選択し、ACL を有効にしてください。またオプションでカウンターを有効にして、ACL の統計を収集できます。

図 258: ポートを ACL にバインドする



注意 : ACL の設定の詳細については、www.edgecore.com から入手できる特定のスイッチモデルのウエブ管理ガイド及び CLI リファレンスガイドを参照してください。

スイッチサービスを設定する

サービスタブをクリックして、スイッチへの Telnet 及びウエブサーバーのアクセスと、ネットワークタイムを設定します。

Telnet 接続を介して、スイッチ C LI にアクセスするために Telnet サーバーを有効にします。

ウエブブラウザインターフェースを使用して、スイッチ管理にアクセスできるように、HTTP ウエブサーバーを有効にします。

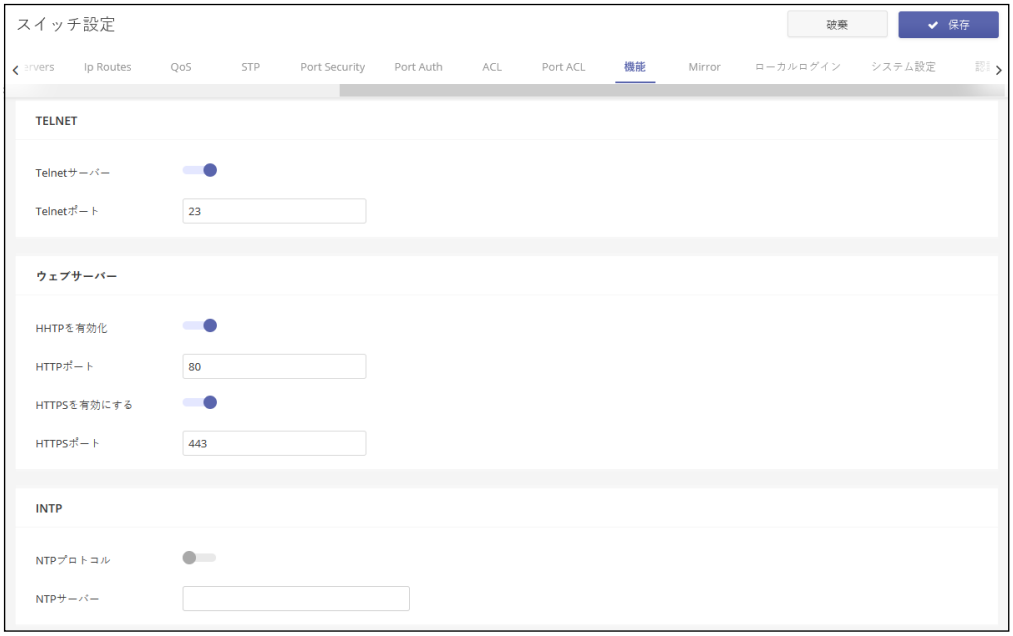
また、セキュアソケットレイアー（SSL）を介して HTTP を有効にして、スイッチのウエブインターフェースへの安全なアクセス（暗号化された接続）を提供することもできます。

HTTP サービスと HTTPS サービス両方を、スイッチで個別に有効化できます。ただし、同じ TCP ポートを使用するように両方のサービスを設定することはできません。

ネットワークタイムプロトコル（NTP）を使用すると、スイッチはタイムサーバーからの定期的な更新に基づいて内部クロックを設定できます。スイッチの正確な時刻を維持することにより、システムログはイベントエントリの意味のある日時の記録できます。

NTP を設定するには、最大で 3 つのダイムサーバーの IPv4 アドレスを入力してから、NTP サービスを有効にしてください。スイッチは、設定された全てのタイムサーバーを調査し、受信した応答をフィルタリングして比較し、スイッチの最も信頼性が高く、正確な時間への更新を実行します。

図 259: スイッチのサービス



ポートのミラーリングの設定

ミラータブを使用して、リアルタイム分析を目的として、任意の送信元ポートから、対象ポートにトラフィックをミラーリングします。次に、ロ ジックアナライザーまたは RMON プローブを対象ポートに接続し、邪魔にならない方法で、送信元を通過するトラフィックの調査を行うことができます。

ミラーリングを有効にすると、送信元ポートとソースポート、及びミラーリングするトラフィックの種類（受信、送信、またその両方）を選択できます。

図 260: ポートミラーリング

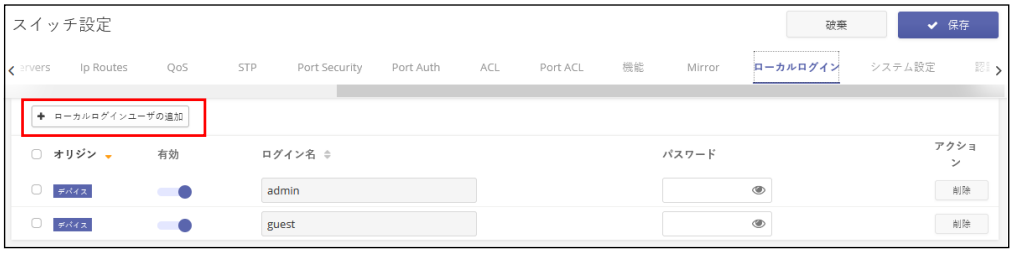
ローカルログインを設定する

ローカルログインタブを使用すると、手動で設定されたユーザ名と、パスワードに基づき、スイッチへの管理アクセスを操作できます。

ローカルログインは、ランダムに作成されたパスワードを使用した、デフォルトのアカウントを一つ持っています。必要に応じてパスワードを変更し、追加のローカルアカウントを設定できます。

注意：ローカルログインのデフォルトアカウントは ecCLOUD サイトレベルの設定がされており、デバイスのローカルユーザインターフェースで設定されていたデフォルトアカウントを上書きした状態です。サイトレベルの設定がデバイスにプッシュされた場合は、ecCLOUD デバイスレベルで設定されたローカルログインアカウントを使用する必要があります。

図 261: ローカルログインの設定



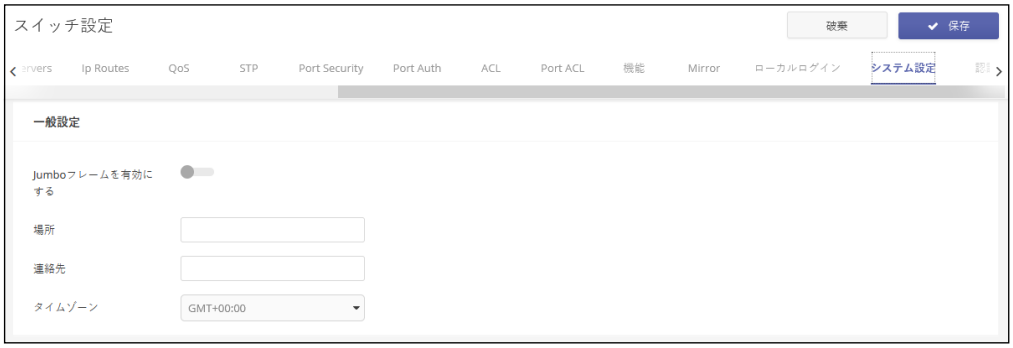
システムの設定

システム設定のタブを使用すると、デバイスの場所や連絡先情報などの情報を表示することで、システムを識別できます。ジャンボフレームを有効にし、ローカルタイムゾーンを設定できます。

Edgecore スイッチには、2 レイヤージャンボフレームのサポートが含まれています。スイッチは、ギガビットイーサネットの 10240 バイトまでのジャンボフレームや、10 ギガビットイーサネットポートまたはトランクをサポートすることにより、大規模なシーケンシャルデータ転送に対してより効率的なスループットを提供します。

またスイッチの場所のタイムゾーンも設定する必要があります。NTP は、イギリスのグリニッジを通過する地球の本初子午線、経度 0 度の時刻に基づいて、協定世界時（または GMT）を使用しています。現地時間に対応するには、タイムゾーンが UTC の東（前）または西（後）である時間と分を指定する必要があります。事前定義されたタイムゾーンの定義を選択することもできます。

図 262: システムの設定



ログイン認証を設定する

認証タブを使用して、ローカル認証またはリモート認証を指定します。ローカルまたはリモートログイン認証コントロール管理はコンソールポート、ウエブブラウザ、または Telnet を介してアクセスします。

ローカル認証は、ユーザ名とパスワードに基づいて管理者のアクセスを制限します。リモート認証は、RADIUS または TACACS +プロトコルに基づくリモートアクセス認証サーバーを使用して、管理アクセスを検証します。

デフォルトでは、管理アクセスは常にローカル認証データベースに対してチェックされます。リモート認証サーバーを使用する場合は、認証シーケン

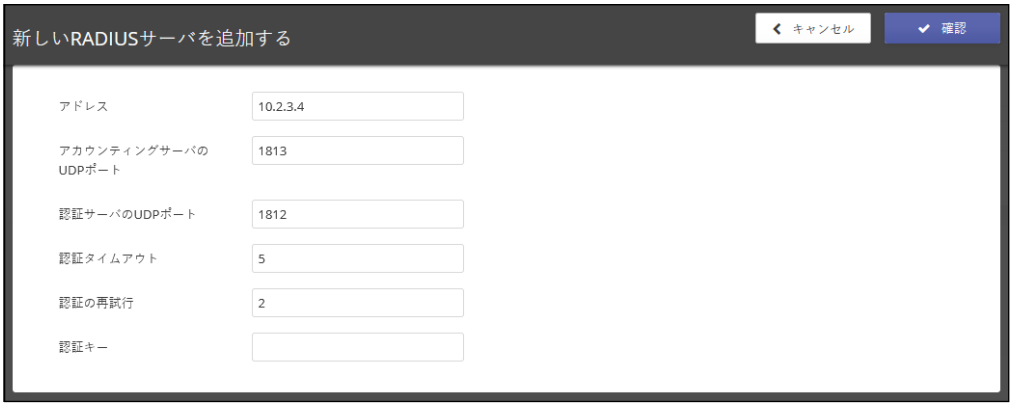
スを指定する必要があります。次にリモート認証サーバーに対応するパラメーターを指定します。

認証シーケンスを示すために、任意のユーザに対して最大三つの認証方法を指定できます。例えば、1）RADIUS、2）TACACS、及び 3）ローカルを選択した場合、RADIUS サーバーのユーザ名とパスワードが最初に確認されます。RADIUS サーバーの使用できない場合は、TACACS ＋サーバーを使用して試行され、最後にローカルユーザの名前とパスワードチェックされます。

図 263: グイン認証

認証サーバーを追加するためには、新しい RADIUS サーバーを追加するボタンをクリックして、IP アドレスとその他のサーバーの詳細を設定します。

図 264: 認証サーバーを追加する



13 SD-WAN デバイス構成

この章では、デバイスレベルでの SD-WAN のコンフィギュレーション設定について説明します。以下のセクションが含まれます：

SD-WAN デバイスレベル設定へのアクセス

デバイスの「継承ポリシー」が有効な場合、デバイスはサイト・レベルから設定されます。ただし、デバイスはデバイス・レベルで個別に設定でき、その設定はサイト・レベルの設定より優先されます。

注意：個々のデバイスのオーバーライドは、設定が変更されたページで [Use Site Settings] (サイト設定を使用) ボタンをクリックすることで、サイトレベルの設定にリセットできます。

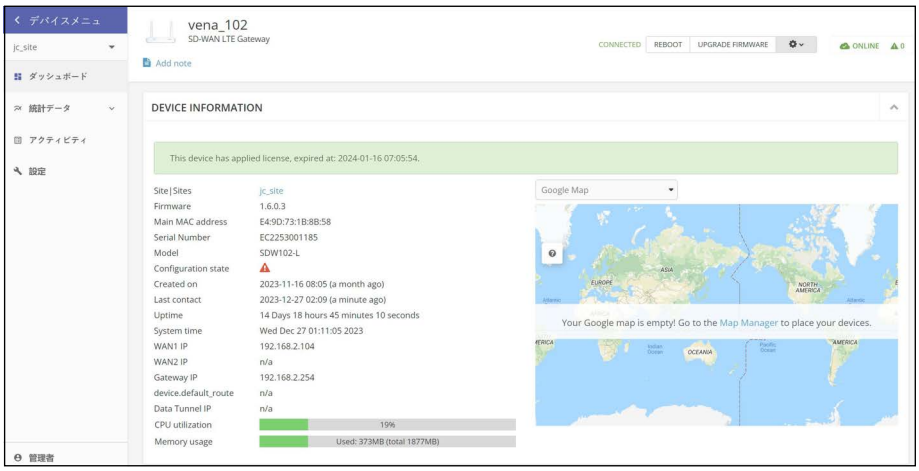
さらに、SD-WAN デバイスには、特定の製品に固有の高度な設定や機能など、サイトレベルでは構成できない設定が含まれています。これらの設定はデバイスレベルでしか設定できません。

デバイスの設定にアクセスするには、サイトレベルのデバイスリストからデバイス名をクリックします（クラウドレベルのデバイスリストからも利用できます）。

図 265: デバイスレベルの設定にアクセス

デバイスダッシュボードから、デバイスメニューの「Configuration」をクリックし、デバイスの設定にアクセスします。

図 266: デバイスレベルのダッシュボード



この章では、194 ページの「サイト SD-WAN の設定」で説明されているように、サイトレベルの設定とは異なるデバイスの設定のみを説明します。

WAN

WAN タブをクリックして設定を行います。WAN タブには以下の項目が表示されます。

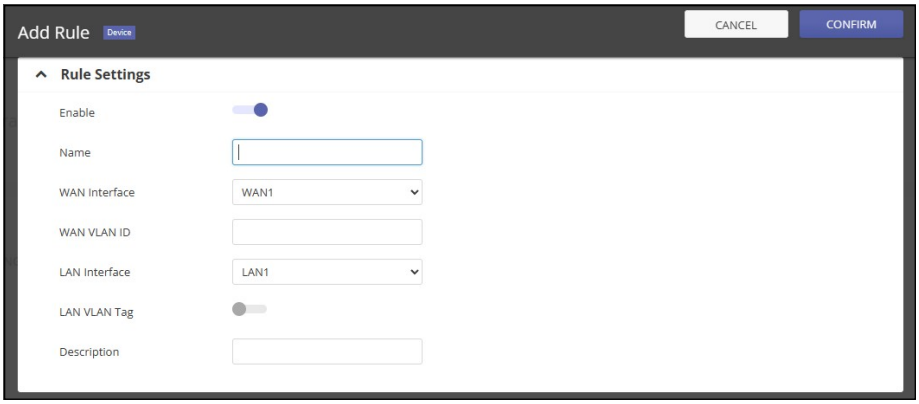
WAN

図 267: デバイス WAN 構成

- WAN Provisioning — WAN1 と WAN2 の設定を行います。各インターフェイスは個別に設定できます。
- Type — WAN インターフェースに IP アドレスを提供するために使用される方法です。(デフォルト：DHCP、その他のオプション：スタティック IP、PPPOE)
- IP Address — ここに IP アドレスを入力してください。
- Netmask — WAN1 IP アドレスに関連付けられたサブネットマスクを指定してください。
- ゲートウェイ — ローカル ネットワーク外のトラフィックをルーティングする WAN1 のゲートウェイ IP アドレスを入力してください。
- DNS 1 — プライマリ DNS サーバー IP アドレスを入力してください。
- DNS 2 — セカンダリ DNS サーバー IP アドレスを入力してください。
- NAT — NAT 機能を有効または無効にしてください。

WAN VLAN パススルー

図 268: 新しい WAN VLAN パススルー・ルールの作成



WAN から指定した LAN インターフェースへのトラフィックの通過を許可するルールを追加します。WAN VLAN Passthrough テーブルでは、各エントリを有効または無効にして構成できます：

- [名前] — パススルー ルールの名前を指定してします。
- WAN インターフェイス — ルールに指定する WAN インターフェイスです。
- WAN VLAN ID — WAN 用にタグ付けされた VLAN ID です。どの VLAN のトラフィックを通過させるかを指定してください。
- LAN インターフェイス — VLAN トラフィックのターゲット LAN インターフェイスです。
- LAN VLAN タグ — VLAN タグが有効な場合に、LAN インターフェースに割り当てられる VLAN ID です。
- [メモ] — ルールを説明する簡単なメモです。

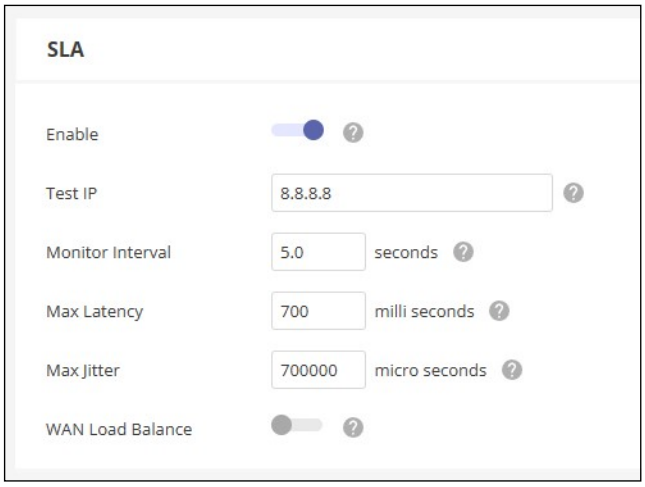
WAN 優先インターネット

図 269: インターネット接続に優先する WAN インターフェースを選択

- Prefer WAN — インターネットトラフィックを優先する WAN インターフェース（WAN1 または WAN2）を選択してください。Disable を選択した場合、優先順位は与えられず、デバイスは可用性または他の負荷分散設定に基づいて WAN 選択を管理します。

SLA

図 270: SLA 設定



- Test IP — リンク品質のテストに使用する IP アドレスを入力してください。
- Monitor Interval — リンク品質を評価する頻度の時間間隔を秒単位で設定してください。
- Max Latency — 適格サービスレベルの最大許容遅延をミリ秒単位で指定してください。この閾値を超えると、デバイスはデフォルト・ルートを変更します。
- Max Jitter — マイクロ秒単位の認定サービス・レベルの許容可能な最大ジッターです。この閾値を超えると、デバイスはデフォルトルートを変更します。
- WAN Load Balance — インターネットアクセスの WAN インターフェイス間のロードバランシングを有効または無効にしてください。

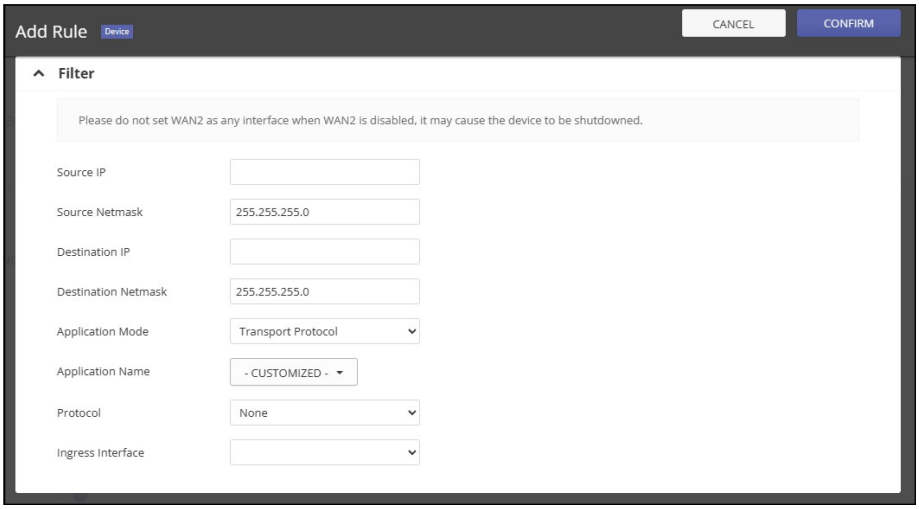
トラフィックステアリング

特定のルールに基づいてネットワークトラフィックの方向を管理できるようにする。

- Name — ルールの名前を入力してください。
- [モード] — ステアリングの動作 (利用可能、必須、ロード バランス) を指定してください。

- IP Address (Source > Destination) — 対象パケットの送信元および宛先 IP アドレスです。
- Application/Protocol (Source > Destination) — 定義済みのアプリケーションを選択するか、トラフィック マッチングのカスタム パラメータを設定するか、カスタマイズを選択して使用するプロトコルを指定してください。
- Interface Preferred/Backup — 優先インターフェイスが使用できない場合に、ルールに一致するターゲット パケットを転送するリンク (インターフェイス) です。
- アクション — このトラフィック ステアリング ルール構成を編集または削除してください。

図 271: トラフィックステアリングフィルタリングルールの追加



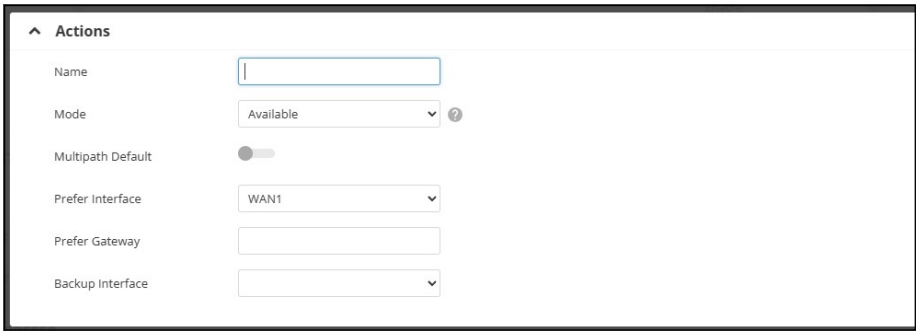
新しいステアリングルールを追加して、トラフィックがネットワークをどのように経由するかを制御してください :

- Source IP — ソース IP またはネットワーク IP を入力してください。
- Source Netmask — ソース IP のネットワーク ネットマスクを指定してください。
- 宛先 IP — 宛先 IP またはネットワーク IP を指定してください。
- Destination Netmask — 宛先 IP のネットワーク マスクを指定してください。
- アプリケーション — 一般的なアプリケーションのフィルタ ルールの IP プロトコル番号、既定の宛先 IP ポートを自動的に設定します。

- カスタマイズされたアプリケーションでは、ソース ポートと宛先ポート、および IP プロトコル ルール番号を手動で指定する必要があります。
- GRE プロトコル、IP プロトコル番号：47
- ESP プロトコル、IP プロトコル番号：50
- IGMP プロトコル IGMP プロトコル、IP プロトコル番号：2
- SNMP プロトコル、UDP 宛先ポート：21
- SSH プロトコル、TCP 宛先ポート：22
- Telnet プロトコル、TCP 宛先ポート：23
- Web HTTP プロトコル、TCP 宛先ポート：80
- Web HTTPS プロトコル、TCP 宛先ポート：443
- 電子メール POP3 プロトコル、TCP 宛先ポート：110
- 電子メール SMTP プロトコル、TCP 宛先ポート：25
- 電子メール IMAP プロトコル、TCP 宛先ポート：143
- ビデオ RTP プロトコル、UDP 宛先ポート：5004、5005
- ビデオ RTSP プロトコル、TCP/UDP 宛先ポート：554
- ビデオ RSVP プロトコル、TCP/UDP 宛先ポート：3455
- VPN L2TP プロトコル、UDP 宛先ポート：1701
- VPN PPTP プロトコル、TCP 宛先ポート：1723
- VPN ISAKMP プロトコル、UDP 宛先ポート：500
- VPN IPSec プロトコル、UDP 宛先ポート：4500
- VoIP H.323 プロトコル、TCP 宛先ポート：1720
- VoIP SIP プロトコル、TCP 宛先ポート：5060

- Ingress Interface — WAN1、WAN2、TUN、LAN、または特定の VPN トンネルなどのオプションからイングレスインターフェースを選択してください。

図 272: パケットをフィルタリングするアクションの設定



- [アクション] — このトラフィック ステアリング ルールの構成を編集または削除してください。
  - [名前] — フィルタリング ルールに名前を付けてください。
  - Mode — トラフィック ステアリングの動作を設定してください :
    - Available — トラフィックは優先インターフェースにデフォルト設定され、必要に応じてバックアップインターフェースにフォールバックします。
    - Mandatory — トラフィックは優先インターフェースを通じて厳密に送信されるか、利用できない場合はドロップされます。
    - ロードバランス — 現在の負荷と可用性に基づいて、優先インターフェースとバックアップインターフェースの間でトラフィックを分散します。
  - Multipath Default — トラフィック・マルチパス機能を有効または無効にします。(デフォルトは無効)
  - Prefer Interface — ルールに一致するパケットを転送するプライマリ インターフェイスを選択してください。
  - Prefer Gateway — プライマリ ゲートウェイの IP アドレスを指定してください。
  - [バックアップ インターフェイス] — 優先インターフェイスが使用できない場合に、ルールに一致するパケットを転送する代替インターフェイスを選択してください。
  - [バックアップ ゲートウェイ] — (オプション) 優先ゲートウェイが使用できない場合に使用する代替ゲートウェイを指定してください。

LAN

LAN タブをクリックして、デフォルト LAN 設定、DHCP サーバー設定、および追加の LAN サブネットを指定してください。

Default LAN

図 273: デフォルトの LAN と DHCP サーバーの設定

- IP Address — デフォルト LAN インターフェイスの IP アドレスを入力してください。
- Subnet Mask — デフォルト LAN のネットマスクを選択してください。
- DHCP Server — DHCP（Dynamic Host Configuration Protocol）サーバーの有効 / 無効を切り替えられます。
- DHCP Start and End — DHCP プール内の IP アドレスの範囲を指定してください。
- リース時間 — IP アドレスが DHCP クライアントに割り当てられる時間（秒）です。
- DNS1 — ネットワークの名前解決のためのプライマリドメインネームサーバーの IP アドレスです。
- DNS2 — ネットワーク名解決用のセカンダリドメインネームサーバーの IP アドレスです。

Additional LAN Subnet

Add LAN " をクリックし、LAN サブネットを追加設定してください :

- Name — 新しいサブネットの名前を指定してください。
- IP Address — サブネットの LAN IP アドレスを設定してください。
- Subnet Mask — LAN IP アドレスのネットマスクを選択してください。

- Port — サブネットのローカル物理ネットワーク インタフェースを選択してください。
- VLAN Tag — トラフィック分割のための VLAN タギングを有効または無効にしてください。
  - VLAN ID — VLAN ID を 1 ～ 3999 の範囲で設定してください。
- Remote Accessible — VPN GroupまたはP2P トンネルポートがアクセスするために、サブネットを他のエッジできます。
- DHCP Server — DHCP（Dynamic Host Configuration Protocol）サーバーの有効 / 無効を切り替えられます。
- DHCP Start and End — DHCP プール内の IP アドレスの範囲を、割り当て可能な最小アドレスから開始し、最大アドレスで終了するように指定してください。
- リース時間 — IP アドレスが DHCP クライアントに割り当てられる時間（秒）です。
- DNS1 — ネットワークの名前解決のためのプライマリドメインネームサーバーの IP アドレスです。
- DNS2 — ネットワーク名解決用のセカンダリドメインネームサーバーの IP アドレスです。

Static Route

Static Route タブをクリックしてリストを設定してください。

図 274: Static Route 設定

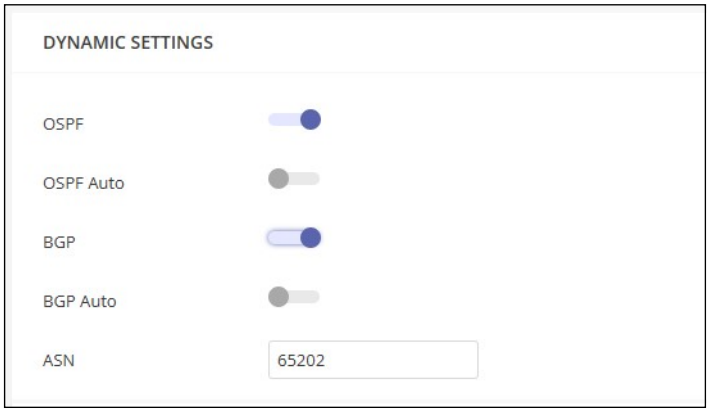
- Destination IP — 宛先 IP アドレスを入力してください。有効な IP アドレスは、ピリオドで区切られた 0 ～ 255 の 4 つの 10 進数で構成されます。
- [Netmask] — 宛先 IP アドレスに対応するネットマスクを選択してください。(デフォルト：255.255.255.0)

- ゲートウェイ — ローカルネットワーク以外の宛先にトラフィックをルーティングするために使用されるゲートウェイルーターの IP アドレスです。
- インターフェース — デバイスとプライベートまたはパブリックネットワークとの相互接続ポイントです。WAN や LAN などの物理インターフェイスや、マルチサブネットなどの仮想インターフェイスがあります。
- メトリック — ルーティングテーブル内での優先順位を決定するために使用されるメトリック値をルートに割り当てます。メトリック値が低いほど、ルートの優先順位が高くなります。

Dynamic Route

OSPF（Open Shortest Path First）および BGP（Border Gateway Protocol）プロトコルを管理し、ダイナミックルートを設定するには、"Dynamic Route " タブをクリックします。

図 275: Dynamic 設定



- OSPF — OSPF プロトコルを有効または無効にしてください。
- OSPF Auto — 有効にすると、デフォルト LAN、「リモートアクセス可能」とマークされたマルチサブネット、VPN グループサブネット、および P2P トンネル IP サブネットを含む OSPF 構成が自動化されます。
- BGP — BGP プロトコルを有効または無効にしてください。
- BGP Auto — デフォルトの LAN、「リモートアクセス可能」とマークされたマルチサブネット、VPN グループサブネット、P2P トンネル IP サブネット、および BGP ネイバーを含む BGP 設定を自動的に構成します。

- BGP ASN — BGP ルーティングネットワークでデバイスを識別するための BGP 自律システム番号（ASN）を入力してください。

図 276: 新しい Dynamic Route の追加

- Classification — OSPF か BGP か、新しいルートのプロトコル分類を選択してください。
- Protocol — BGP Network、OSPF Network、BGP Neighbor など、設定するプロトコル項目の種類を選択してください。
- IP アドレス — BGP または OSPF ネットワークの場合はネットワーク IP を、BGP ネイバー構成の場合はネイバー IP を指定してください。
- ネットマスク — BGP または OSPF ネットワーク、または BGP ネイバーのネットマスクを選択してください。
- Area/ASN — 選択したプロトコルに該当する OSPF エリア番号または BGP ASN を入力してください。

Access Control

アクセス・コントロールタブに移動し、エンドポイントのセキュリティ設定を行ってください。

図 277: デフォルトフィルターポリシーの指定

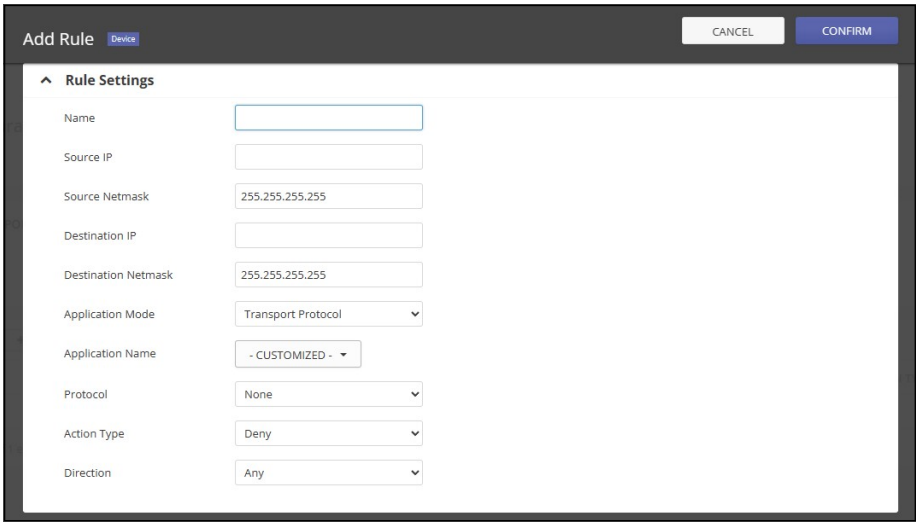
- デフォルトフィルタポリシー — ネットワークトラフィックを拒否または許可するデフォルトのアクセスコントロールを設定してください。

ACL Rules

- 名前 — ルールの名前を指定してください。

- [アプリケーション モード] — ルールのアクティブ モードを定義するために、プロトコル「トランスポート プロトコル」（プロトコル モードに依存）またはアプリケーション層プロトコル（アプリケーション層プロトコルに基づいて）のいずれかを選択してください。
- Address (Source > Destination) — ルールに一致するトラフィックのソース IP と宛先 IP を指定してください。
- プロトコル / ポート (送信元 > 宛先) — ルールに一致するトラフィックの送信元および宛先ポートを指定してください。
- [アクション タイプ] — ルールがトラフィックを拒否するか許可するかを選択してください。
- Direction — 保護方向として、「Outbound」（送信トラフィックのみ）と「ANY」（受信トラフィックと送信トラフィックの両方）のいずれかを選択してください。
- Actions — 選択した ACL ルールを変更または削除してください。

図 278: 新しいアクセスコントロールのルール設定



- 名前 — ルール名の名前を指定してください。
- Source IP — 元のソース IP 値を指定してください。
- Source Netmask — ソース IP サブネット マスクを設定してください。
- 宛先 IP — 宛先 IP 値を設定してください。
- 宛先ネットマスク — 宛先 IP サブネット マスクを設定してください。

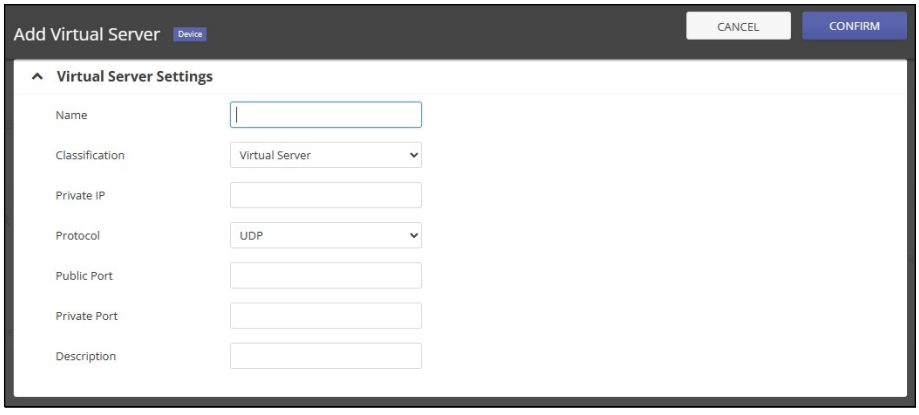
- アプリケーションモード — プロトコルモード（トランスポートプロトコル）またはアプリケーションモード（アプリケーションツーレイヤープロトコル）に依存するアクティブモードを選択してください。
- アプリケーション名 — システムが関連するパブリックアプリケーションプロトコルを設定してください。
- プロトコル — UDP、TCP、または UDP/TCP を選択し、ソースと宛先のポートに 1 ～ 65535 の有効なポート番号を入力してください。IP プロトコルを選択した場合は、IP アドレスのみが必要です。
- Action Type — ルールがトラフィックを拒否するか許可するかを選択してください。
- Direction — 保護方向を「Outbound」（送信のみ）または「ANY」（受信と送信の両方）のいずれかを選択してください。Application Layer Protocol」を使用する場合、「Direction」は「ANY」に設定されます。

Virtual Server

仮想サーバーを使用すると、リモートコンピュータはプライベート LAN (Local Area Network) 内の特定のコンピュータまたはサービスに接続できます。これには主に 2 つのメカニズムがあります：仮想サーバー （ポート転送とも呼ばれる）と 1 対 1 NAT （ネットワークアドレス変換）マッピングです。

仮想サーバーセクションには、設定されているすべての仮想サーバーが表示されます。

図 279: 新しい仮想サーバーの設定



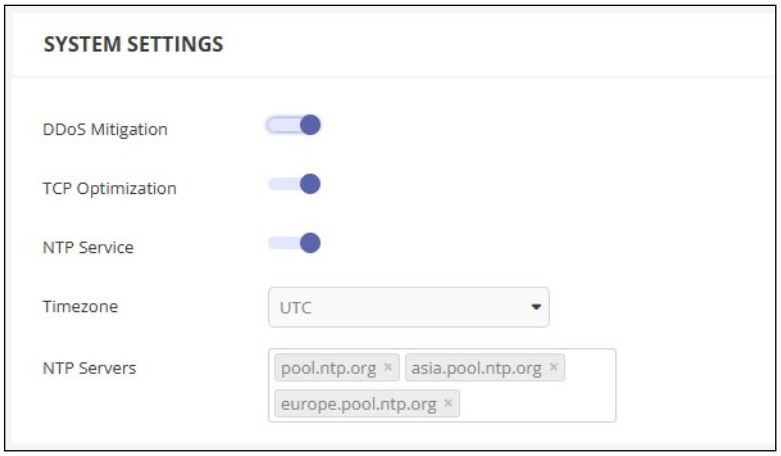
仮想サーバーの追加をクリックし、新しい仮想サーバーの設定を行ってください：

- Name — 仮想サーバーエントリーの名前を入力してください。
- Classification — 配備する仮想サーバーのタイプを選択してください：
  - 仮想サーバー — ネットワーク・ゲートウェイを通過する間、あるアドレスとポート番号から別のアドレスとポート番号に通信要求をリダイレクトします。宛先アドレスとポート番号を WAN インターフェース経由で内部ホストに再マッピングすることで、保護されたネットワーク内のホストのサービスにアクセスする場合に便利です。
  - 1to1 NAT — LAN サブネット内の 1 つの外部 IP アドレス（通常はパブリック）を 1 つの内部 IP アドレスにマッピングします。プライベート IP アドレスからインターネットへのトラフィックに対しては、アウトバウンド NAT 設定を上書きします。
- パブリック IP エイリアス受信インターフェイス — パブリック IP エイリアスに関連付けられた送信 WAN インターフェイス（WAN1 または WAN2）を選択してください。
- パブリック IP エイリアス — マッピングする外部（パブリック）IP アドレスを指定してください。
- プライベート IP — パケットを転送する内部 IP アドレスを指定してください。
- Protocol — 仮想サーバーのプロトコル（UDP または TCP）を選択してください。
- Public Port — WAN インターフェイス経由のパケットの元の宛先ポートを設定してください。
- Private Port — パケットをリダイレクトする内部ポートを指定してください。
- Description — この仮想サーバー設定を識別するための簡単なコメントを追加してください。

システム設定

システム設定タブにアクセスし、デバイスレベルで SD-WAN 機能を管理してください。

図 280: SD-WAN デバイスシステム設定



このページには以下の項目が含まれます :

- DDoS Mitigation — ルーティング / システム制御ドメイン内で分散サービス拒否（DDoS）ミティゲーションメカニズムを有効にしてください。
- TCP Optimization — TCP Optimization を有効にして、ネットワーク上の TCP（Transmission Control Protocol）トラフィックのパフォーマンスを向上させます。
- NTP サービス — 正確なシステム時刻を維持するために、時刻更新要求を送信する NTP（Network Time Protocol）サービスを有効にしてください。
- タイムゾーン — ドロップダウンリストから適切なタイムゾーンを選択し、デバイスがローカルタイムを正確に表示するようにします。
- NTP サーバー — NTP サーバーのホスト名を設定してください。Bsta サーバーは最初に最初のサーバーと時刻の同期を試みます。失敗した場合は、リストの次のサーバーとの同期を順次試みます。