



ecCLOUD コントローラ

ユーザマニュアル

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

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 コントローラウェ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 コントローラウェ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。

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 [151 ページの「SSID を追加する」](#) および [195 ページの「OpenRoaming」](#) を参照。
- RF アイソレーションの追加 ([162 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 ([162 ページの「無線設定」](#) を参照)
- サイト・グループ化の追加 ([57 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 ([61 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、[163 ページの「グローバル設定」](#) 参照
- 802.11v を追加、[151 ページの「SSID を追加する」](#) を参照
- BLE Tx Power を追加、[194 ページの「iBeacon」](#) 参照
- BLE スキャンの追加、[223 ページの「iBeacon」](#) 参照
- 更新されたチャンネル帯域幅は、[163 ページの「電波設定」](#) および [219 ページの「電波設定」](#) を参照
- BSS Coloring の更新 [163 ページの「電波設定」](#)、[219 ページの「電波設定」](#) 参照
- 更新された最小許容信号、[103 ページの「SSID を追加する」](#)、[151 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 ([243 ページの「Terragraph デバイス構成」](#) 参照)。
- サイト Terragraph の VLAN 設定を追加、[203 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。24 ページの「クラウドを作成する」、81 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、49 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 (84 ページの「WiFi 構成」を参照)
- 100 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、103 ページの「SSID を追加する」参照
- OSEN の追加、103 ページの「SSID を追加する」参照
- AuthPort External RADIUS を追加、112 ページの「無線設定」を参照
- 無効な W52 チャンネルを追加、112 ページの「無線設定」参照
- IPv6 設定を追加しました。116 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、119 ページの「VLAN の設定」「VLAN 設定」(108 ページ) 参照
- 追加 RSTP の有効化、123 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、123 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、127 ページの「ARP インスペクション」参照
- DHCP Snooping を追加、128 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、129 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、129 ページの「ホットスポットの設定」参照
- 追加 NAS ID の生成、132 ページの「RADIUS サーバー」参照
- HTTPS ログインを追加、134 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、136 ページの「システムの設定」参照

- MSP モードの追加、136 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、142 ページの「SNMP」参照
- IGMP Snooping を追加、145 ページの「IGMP スヌーピング」参照
- LLDP を追加、146 ページの「LLDP」参照
- iBeacon を追加、146 ページの「iBeacon」参照
- SNMPv3 User を追加しました。147 ページの「SNMPv3 ユーザ」を参照
- 149 ページの「サイト WiFi 6 構成」の章を追加しました。
- 199 ページの「サイト Terragraph の構成」の章を追加しました。
- 204 ページの「WiFi 5 デバイス構成」の章を改称しました。
- 213 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。
- 30 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

このマニュアルの使い方	3
目次	7
図を使っての説明	13

セクション I	操作を開始する	21
1	イントロダクション	22
	ecCLOUD にログインする	23
	クラウドを作成する	24
	QR コードによる機器登録	30
	設定の引継ぎを理解する	33
	デバイスの登録	34
	デバイス設定の変更	36
	設定のエラー	37
	設定が保留されるエラー	38

セクション II	クラウドの設定	39
2	クラウドの管理	40
	クラウドの管理	40
	登録済みのアカウントで新しいクラウドの作成	41
	クラウドの情報を編集する	43
	クラウドのプロパティの変更	44
	クラウドの削除	45
	クラウドダッシュボードの表示	46
	カスタマイズされたクラウドのダッシュボードの作成	47
	デバイスの管理	49
	デバイスのリストをフィルターにかける	50

設定を引き継ぐ際のポリシー	50
デバイスについての情報を見る	52
デバイスの追加	52
デバイスのファームウェアをアップグレードする	52
システムのアクティビティを表示する	54
サイトの管理	55
ユーザの管理	56
サイトグルーピング	57
常にクラウド設定に従う	61
ライセンスと請求の管理	64
アドオン	66
AuthPort アドオンを使用する	67
サービスプラン	68
アカウント	70
AuthPort 認証	72
キャプティブポータル	73
SSID の設定	74
3 基本のサイトの設定	76
サイトの全体像	77
サイトの作成	78
サイトの設定	80
デバイスを追加する	81
マップにデバイスを載せる	82
フロアマップを設定する	83
WiFi 構成	84
サイトのダッシュボードの表示	85
カスタマイズされたサイトのダッシュボード	87
無線 AP とクライアントをモニターする	89
メンテナンスタスクのスケジュールを立てる	94
ファームウェアをアップグレードする	95
一括再起動	95
サイトの通知	96
4 サイト WiFi 5 構成	100

無線 SSID の設定	101
SSID を追加する	103
無線スケジュールを設定する	111
無線設定	112
一般的なネットワーキングの設定	115
インターネットの設定	116
イーサネットの設定	119
VLAN の設定	119
ローカルネットワーク設定	123
ファイアーウォールの設定	125
ポートフォワードイング	126
ARP インスペクション	127
DHCP スヌーピング	128
ホットスポットの設定	129
一般設定	129
ネットワークの設定	131
DHCP サーバー	132
RADIUS サーバー	132
キャプティブポータル	134
認証の除外	136
システムの設定	136
一般設定	136
SSH	138
検出ツール	139
Telnet	139
ウェブサーバー	140
ネットワークタイム	141
SNMP	142
リモート Syslog	143
Ping ウォッチドグ	144
BLE の設定	144
マルチキャスト DNS	145
IGMP スヌーピング	145
LLDP	146
iBeacon	146

SNMPv3 ユーザ	147
5 サイト WiFi 6 構成	149
無線 SSID の設定	150
SSID を追加する	151
無線スケジュールを設定する	161
無線設定	162
一般的なネットワーキングの設定	166
インターネットの設定	167
イーサネットの設定	170
VLAN の設定	171
ローカルネットワーク設定	173
ファイアーウォールの設定	175
ポートフォワードイング	176
ARP インスペクション	177
DHCP スヌーピング	178
ホットスポットの設定	179
一般設定	179
ネットワークの設定	181
DHCP サーバー	181
RADIUS サーバー	182
キャプティブポータル	184
認証の除外	186
システムの設定	186
一般設定	186
SSH	187
検出ツール	188
ネットワークタイム	188
SNMP	190
Telnet	191
ウェブサーバー	191
リモート Syslog	192
マルチキャスト DNS	193
LLDP	193
iBeacon	194

OpenRoaming	195
6 サイト Terragraph の構成	199
Metrolinq Terragraph の構成	200
VLAN 設定	203
7 WiFi 5 デバイス構成	204
デバイスレベルの設定へのアクセス	205
デバイスの無線設定	207
8 WiFi 6 デバイス構成	213
デバイスレベルの設定へのアクセス	214
デバイスの無線設定	216
システム設定	223
iBeacon	223
9 Metrolinq デバイスの設定	226
Metrolinq の設定	227
無線 SSID	227
無線設定	228
グローバル設定	228
無線 5GHz	229
無線 2.4GHz	231
無線 60GHz	233
一般的な無線設定	233
クオリティオブサービスの設定	237
トラフィックコントロール	238
リンクパスツールの使用	239
RSSI と距離の関係グラフ	242
10 Terragraph デバイス構成	243
Terragraph 構成	244
ネットワーク全般の設定	245
無線設定	247
システム設定	249
11 スイッチ装置の設定	252
スイッチの設定	253

ポート設定	254
トランクの設定	254
LACP トランク	255
VLAN の設定	256
VLAN ポートメンバーの追加	257
ネームサーバーの設定	258
静的 IP ルートの設定	259
ポートレートの制限 (QoS) の設定	259
STP の設定	260
ポートセキュリティの設定	261
802.1X ポート認証の設定	262
ACL 設定	263
ポートを ACL にバインドする	264
スイッチサービスを設定する	265
ポートのミラーリングの設定	266
ローカルログインを設定する	267
システムの設定	268
ログイン認証を設定する	268

図を使っての説明

図 1: ecCLOUD コントローラにログインする	23
図 2: 新しいユーザの登録	24
図 3: クラウドを作成する	25
図 4: クラウドを作成する	25
図 5: サイトの設定	26
図 6: サイトの設定を保存する	27
図 7: 装置を加える方法	27
図 8: 装置の管理	27
図 9: デバイスの追加	28
図 10: デバイスが追加された場合の通知メッセージ	29
図 11: ファームウェアのアップグレードボタン	29
図 12: 装置のフィルター処理	30
図 13: 装置をマップにのせる	30
図 14: AP の QR コードのスキャン	31
図 15: ecCLOUD のログインページ	32
図 16: ecCLOUD のデバイス登録	32
図 17: 新しいデバイスの登録	34
図 18: デバイスの設定を書き換える	36
図 19: 装置の設定の書き換えを元に戻す	37
図 20: クラウドのメニュー	40
図 21: クラウドのメンバーシップを表示する	41
図 22: クラウドの情報を入力する	42
図 23: クラウドアクションを表示	43
図 24: クラウドプロパティの変更	44
図 25: クラウド削除の確認	45
図 26: クラウドのダッシュボード	46
図 27: クラウドのダッシュボードのカスタマイズ	47
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	48
図 29: カスタマイズされたダッシュボードにウィジェットを加える	48

図 30:	カスタマイズされたダッシュボードにウィジェットを選択する	48
図 31:	カスタマイズされたウィ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	49
図 32:	クラウドメニュー内のデバイス	49
図 33:	デバイスの管理	50
図 34:	設定の引継ぎについての表示	50
図 35:	デバイスのアクションメニューの管理	51
図 36:	デバイスの詳細にアクセスする	52
図 37:	クラウドにデバイスを追加する	52
図 38:	ファームウェアアップグレードのお知らせ	52
図 39:	装置のファームウェアのアップグレード	53
図 40:	全てのシステムのアクティビティを表示する	54
図 41:	アクティビティの種類でフィルターにかける	54
図 42:	サイトの管理ページ	55
図 43:	サイトのダッシュボード	55
図 44:	ユーザの管理	56
図 45:	新しいユーザを招待する	57
図 46:	サイトグルーピングへのアクセス	58
図 47:	サイトグルーピングページ	58
図 48:	サイトグループの作成	59
図 49:	サイトグループの管理	59
図 50:	サイトグループの情報を閲覧する	60
図 51:	サイトグルーピングのリセット	60
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	62
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	62
図 54:	フォロークラウドの設定を管理	63
図 55:	強制設定プッシュの使用	63
図 56:	"自動的にクラウド設定に従う" の使用方法	64
図 57:	ライセンスと請求の管理	64
図 58:	アドオンメニュー	66
図 59:	AuthPort アドオン	67
図 60:	AuthPort メニュー	68
図 61:	サービスプランを追加する	68
図 62:	サービスプランの全体像を見る	69

図 63:	一つのアカウントを作成する	70
図 64:	複数アカウントを一度に作成する	70
図 65:	アカウントのリスト	71
図 66:	AuthPort 認証	72
図 67:	オースポートキャプティブポータルの特マの例	73
図 68:	AuthPort キャプティブポールのエディター	74
図 69:	AuthPort SSID の設定	74
図 70:	デフォルトサイトのダッシュボード	77
図 71:	新しいサイトを作成する	78
図 72:	基本のサイトのプロパティをてみよう	79
図 73:	基盤となる国の設定	80
図 74:	ローカルログインの設定	80
図 75:	デバイスを追加する誘導	81
図 76:	新しいデバイスを登録する	82
図 77:	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	82
図 78:	マップにデバイスの位置を追加する	83
図 79:	新しいフロアマップを追加する	83
図 80:	フロアマップを設定する	83
図 81:	デバイスをフロアマップ内に位置付ける	84
図 82:	WiFi5 構成	84
図 83:	サイトのダッシュボード	85
図 84:	ダッシュボードをカスタマイズする	87
図 85:	カスタマイズされたサイトのダッシュボード	87
図 86:	カスタマイズされたサイトのダッシュボードにウィジェットを追加する	87
図 87:	カスタマイズされたサイトのダッシュボードにウィジェットを選択する	88
図 88:	新しいサイトのダッシュボードウィジェットをカスタマイズする	88
図 89:	カスタマイズされたサイトのダッシュボード	89
図 90:	無線クライアントのページ	90
図 91:	無線 AP の情報	91
図 92:	無線 AP ライブステータス	92
図 93:	を頻繁に使用する無線クライアント	92
図 94:	クライアントの情報ページ	93
図 95:	無線クライアントの名前をてえる	93
図 96:	メンテナンスタスクの管理	94
図 97:	新しいファームウェアアップグレードタスクのページ	95

図 98: 一括再起動を管理するページ	96
図 99: サイトの通知の設定	97
図 100: サイト WiFi5 構成	101
図 101: 無線設定	103
図 102: ブリッジからインターネット	105
図 103: ルートからインターネット	106
図 104: 無線スケジュール	111
図 105: WiFi5 無線設定	112
図 106: 5GHz 無線チャンネル	113
図 107: 2.4GHz 無線チャンネル	114
図 108: 一般的なネットワーキング設定	115
図 109: インターネットの設定	116
図 110: 管理 VLAN の設定	117
図 111: IPv6 設定	118
図 112: イーサネットの設定	119
図 113: VLAN の設定	120
図 114: VLAN を追加する	121
図 115: ローカルネットワークの設定	123
図 116: ファイアーウォールの設定	125
図 117: ポートフォワーディング	127
図 118: ARP インスペクション	127
図 119: DHCP スヌーピング	128
図 120: ホットスポットの一般設定	129
図 121: ホットスポットネットワークの設定	131
図 122: ホットスポット DHCP サーバーの設定	132
図 123: ホットスポット RADIUS サーバーの設定	132
図 124: ホットスポットキャプティブポータルの設定	134
図 125: ホットスポットでの認証の除外	136
図 126: 一般的なシステムの設定	137
図 127: SSH サーバーの設定	138
図 128: 検出ツールの設定	139
図 129: Telnet サーバーの設定	139
図 130: ウェブサーバーの設定	140
図 131: NTP の設定	141

図 132: SNMP の設定	142
図 133: リモートログの設定	143
図 134: ping ウォッチドグの設定	144
図 135: BLE の設定	144
図 136: マルチキャスト DNS の設定	145
図 137: IGMP スヌーピング設定	145
図 138: LLDP 設定	146
図 139: iBeacon 設定	146
図 140: SNMPv3 ユーザ設定	147
図 141: サイト WiFi6 構成	150
図 142: 無線設定	151
図 143: ブリッジからインターネット	158
図 144: ルートからインターネット	159
図 145: 無線スケジュール	161
図 146: WiFi6 無線設定	162
図 147: 5GHz 無線チャンネル	164
図 148: 2.4GHz 無線チャンネル	164
図 149: 一般的なネットワーキング設定	166
図 150: インターネットの設定	167
図 151: 管理 VLAN の設定	168
図 152: DHCP Relay	169
図 153: IPv6 設定	169
図 154: イーサネットの設定	170
図 155: VLAN の設定	172
図 156: VLAN の追加	172
図 157: ローカルネットワークの設定	173
図 158: ファイアーウォールの設定	175
図 159: ポートフォワーディング	176
図 160: ARP インスペクション	177
図 161: DHCP スヌーピング	178
図 162: ホットスポットの一般設定	179
図 163: ホットスポットネットワークの設定	181
図 164: ホットスポット DHCP サーバーの設定	181
図 165: ホットスポット RADIUS サーバーの設定	182
図 166: ホットスポットキャプティブポータルの設定	184

図 167: ホットスポットでの認証の除外	186
図 168: 一般的なシステムの設定	186
図 169: SSH サーバーの設定	188
図 170: 検出ツールの設定	188
図 171: NTP の設定	189
図 172: SNMP の設定	190
図 173: Telnet サーバーの設定	191
図 174: ウェブサーバーの設定	192
図 175: リモートログの設定	192
図 176: マルチキャスト DNS の設定	193
図 177: LLDP 設定	193
図 178: iBeacon 設定	194
図 179: OpenRoaming プロファイル	195
図 180: サイト Terragraph の構成	200
図 181: Terragraph ノードの追加	201
図 182: Terragraph ノードを削除する	201
図 183: Terragraph Link を追加する	202
図 184: Terragraph Link を削除する	202
図 185: サイト Terragraph VLAN 設定	203
図 186: デバイスレベルの設定にアクセスする	205
図 187: デバイスレベルのダッシュボード	206
図 188: デバイスの設定	206
図 189: デバイスのグローバル無線設定	207
図 190: デバイスの一般的な無線設定	207
図 191: デバイスの高度な無線設定	208
図 192: デバイスのフィジカル無線設定	209
図 193: 5GHz 無線チャンネル	210
図 194: 2.4GHz 無線チャンネル	210
図 195: デバイスレベルの設定にアクセスする	214
図 196: デバイスレベルのダッシュボード	215
図 197: デバイスの設定	215
図 198: デバイスのグローバル無線設定	216
図 199: デバイス Mesh 設定	217
図 200: デバイスの一般的な無線設定	218

図 201:	デバイスの高度な無線設定	219
図 202:	デバイスのフィジカル無線設定	219
図 203:	5GHz 無線チャンネル	220
図 204:	2.4GHz 無線チャンネル	221
図 205:	デバイス iBeacon 設定	223
図 206:	MetroLinq デバイスのダッシュボード	227
図 207:	MetroLinq デバイスのダッシュボード	228
図 208:	MetroLinq デバイス 5GHz 無線設定	228
図 209:	5GHz 無線チャンネル	230
図 210:	MetroLinq デバイス 2.4GHz 無線設定	231
図 211:	2.4GHz 無線チャンネル	232
図 212:	MetroLinq デバイス 60GHz 無線設定	233
図 213:	60GHz 無線チャンネル	235
図 214:	MetroLinq 無線の無線ビーム幅	236
図 215:	MetroLinq QOS の設定	237
図 216:	MetroLinq トラフィック制御の設定	238
図 217:	MetroLinq リンクパスの設定	240
図 218:	MetroLinq リンクバジェットの結果	241
図 219:	MetroLinq パス予想 RSSI のグラフ	242
図 220:	Terragraph デバイスダッシュボード	244
図 221:	Terragraph デバイス全般の設定	245
図 222:	Terragraph デバイス無線設定	247
図 223:	Terragraph デバイスシステム設定	249
図 224:	スイッチデバイスダッシュボード	253
図 225:	スイッチポート	254
図 226:	トランクを設定する	255
図 227:	トランクポートの設定	255
図 228:	LACP トランクの設定	256
図 229:	VLAN の設定	257
図 230:	VLAN ポートメンバーシップの設定	257
図 231:	VLAN ポートの設定	258
図 232:	ネームサービスの設定	258
図 233:	IP ルートの設定	259
図 234:	ポートレートの制限を設定する	260
図 235:	STP の設定	261

図 236: ポートセキュリティの設定	261
図 237: ポートの認証の設定	262
図 238: ポートの認証の設定	263
図 239: ACL の設定	264
図 240: 新しい ACL を追加する	264
図 241: ポート ACL のバインディング	265
図 242: ポートを ACL にバインドする	265
図 243: スイッチのサービス	266
図 244: ポートミラーリング	267
図 245: ローカルログインの設定	267
図 246: システムの設定	268
図 247: グイン認証	269
図 248: 認証サーバーを追加する	269

セクション |

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ェ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。

- [22 ページの「イントロダクション」](#)

1

イントロダクション

この章は以下の内容を含みます。

- 23 ページの「ecCLOUD にログインする」
- 24 ページの「クラウドを作成する」
- 30 ページの「QR コードによる機器登録」
- 33 ページの「設定の引継ぎを理解する」
- 34 ページの「デバイスの登録」
- 36 ページの「デバイス設定の変更」
- 37 ページの「設定のエラー」

Edgecore ecCLOUD コントローラは、どんな場所からでもウェ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ェ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。

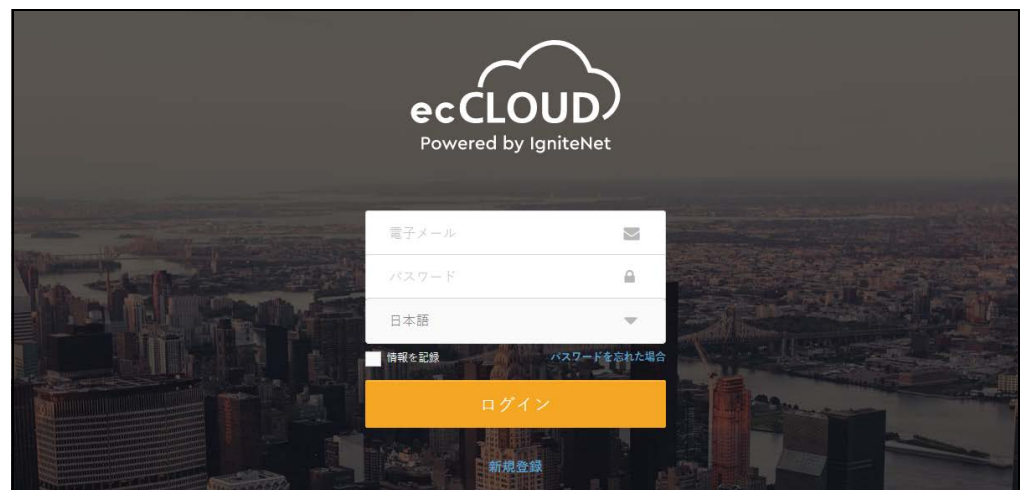
ecCLOUD は下記の装置をサポートしています。

- Edgecore AP: EAP101, EAP102, ECW5211-L, ECWO5211-L, OAP100, ECW5410-L
- Edgecore Switch: 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
- IgniteNet AP と MetroLinq: SP-W2-AC1200(L), SP-W2M-AC1200, SP-W2M-AC1200-POE, SS-W2-AC2600, SS-N300, GW-AC1200, SP-AC750, ML1-60, ML2.5-60, ML2.5-60-BF, ML-60-LW, ML-5-LW, ML-60-10G-360
- IgniteNet Switch: FusionSwitch PoE 10-Port, FusionSwitch PoE 24-Port, FusionSwitch Fiber, MeshLinq

ecCLOUD にログインする

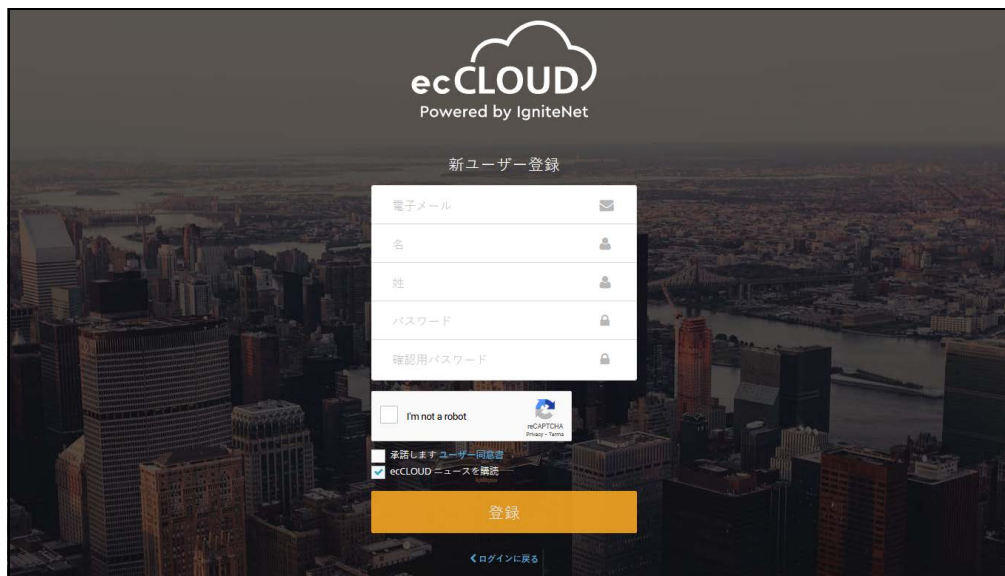
ウェブのブラウザから、cloud.ignitenet.com に入ってアカウントの登録をしてください。あなたのクラウドのネットワークとサイトを作成しましょう。

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。

i 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。

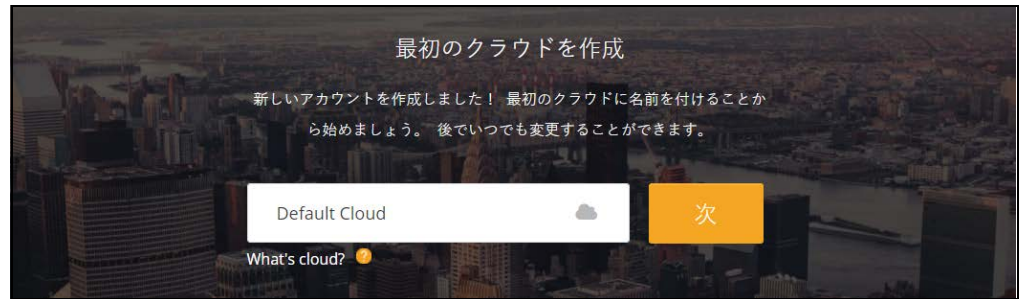
確認メールが ecCLOUD コントローラから届いたら、指示されたリンクにアクセスし登録してください。

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。

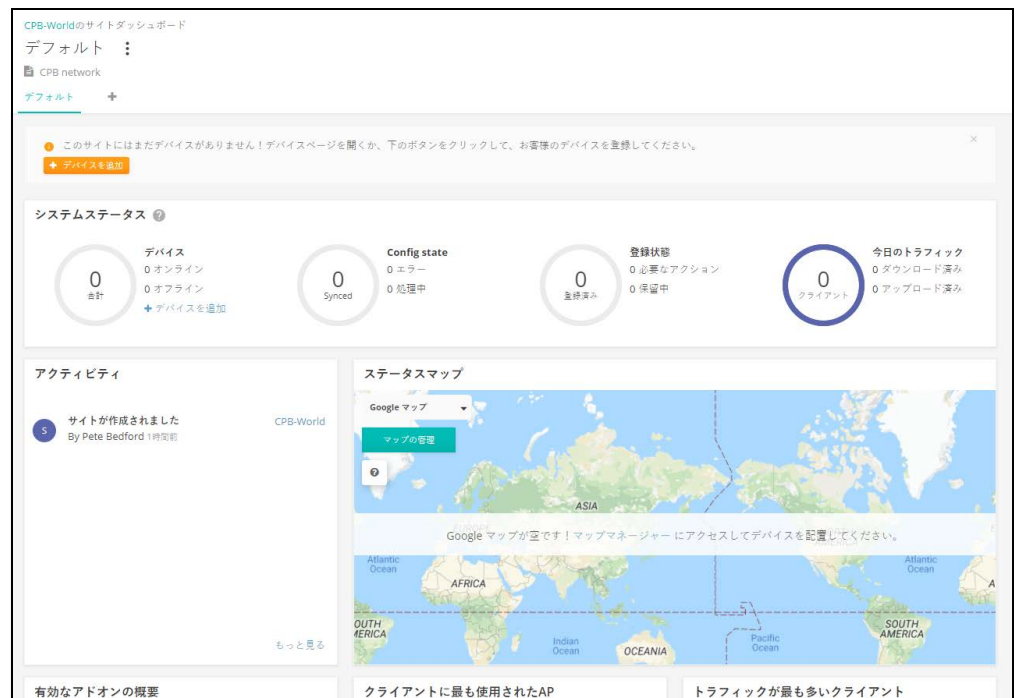
ecCLOUD コントローラのユーザとして登録すれば、最初にログインした時から自分のクラウドを作成できます。

図 3: クラウドを作成する



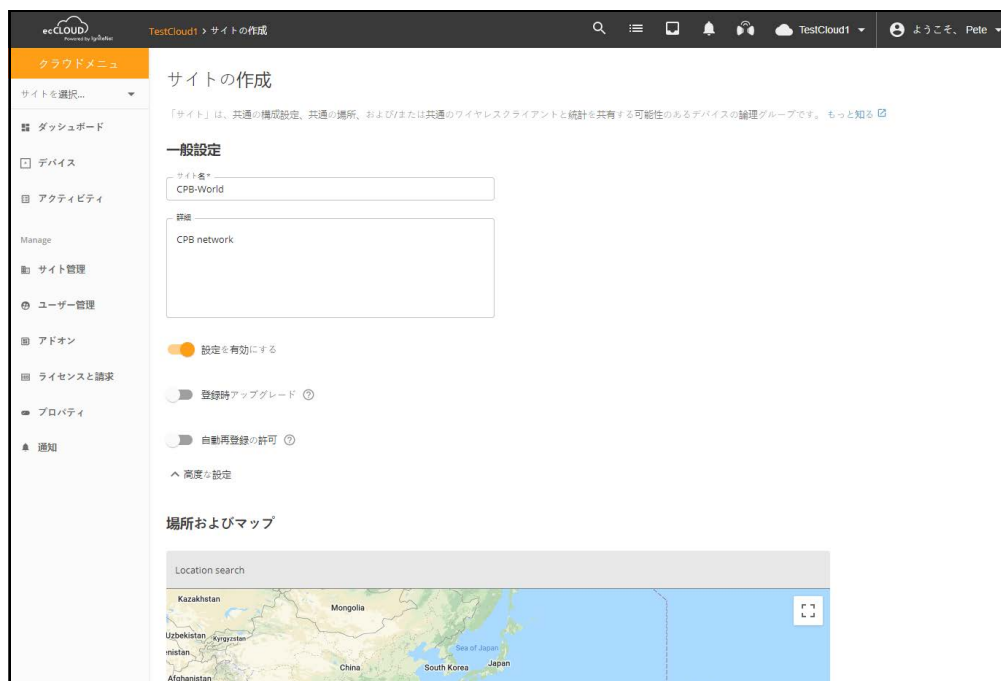
クラウドに名前を入力して、“作成”をクリックしてください。クラウドのダッシュボードが表示されます。

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、最新のファームウェ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、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、ジューリングス：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 (30 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なら、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、61 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。

34 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

新しいデバイスの登録

デバイスのシリアル番号とMACアドレスを入力 (またはスキャン) することで、新しいデバイスをサイトに追加できます。 [もっと知る](#)

シリアル番号とMACアドレスは、製品ボックスか製品の背面に記載されています。

次のサイトにデバイスを追加します

サイトレベルの設定を継承する

このサイトのデバイスを、共通の構成を持つ単一のユニットのように管理する場合は、これを有効にします。 [もっと知る](#)

バーコードスキャンモードを有効化 [?](#)

Always follow cloud configuration [?](#)

Batch Upload File

<input type="text" value="シリアル番号"/>	<input type="text" value="MAC アドレス"/>	<input type="text" value="名前
0"/>
-------------------------------------	---------------------------------------	---

最大 48 台のデバイスを登録できます。

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。(30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、“ファームウェ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。94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: ファームウェ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ル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。

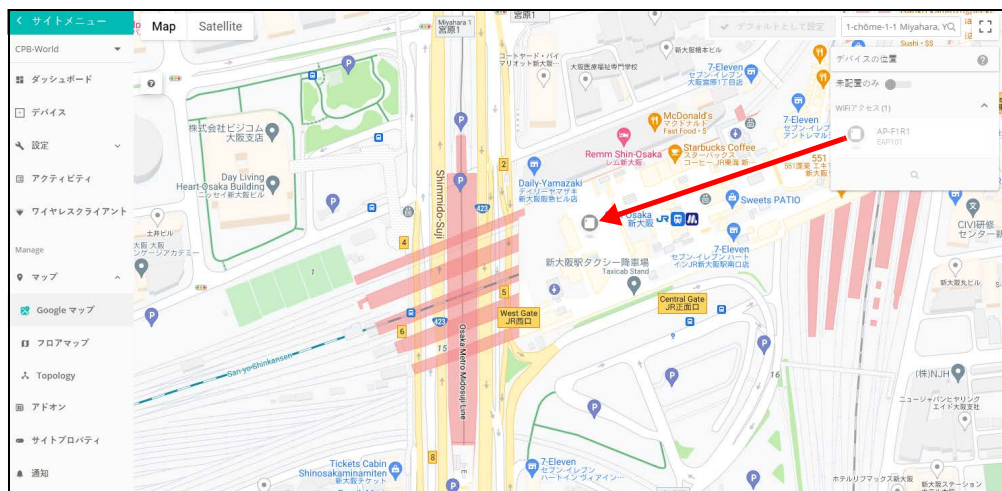
図 12: 装置のフィルター処理



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

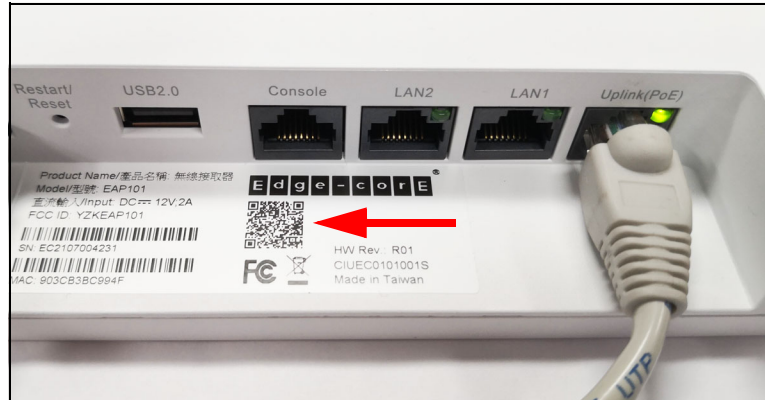
ecCLOUD コントローラで AP の設定や登録を迅速に行うために、携帯電話を使って、AP 上の QR コードをスキャンできます。

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。

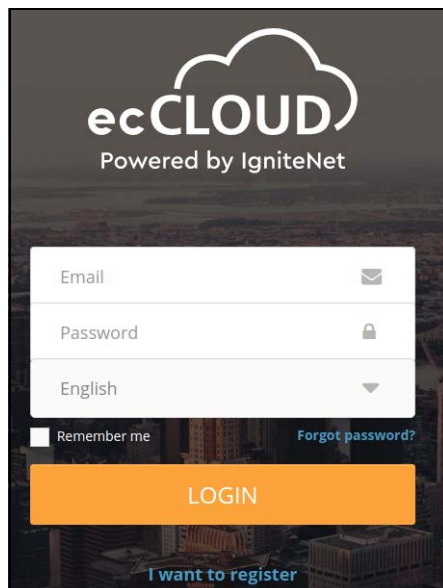
i 注意：もし携帯電話が Wi-Fi ネットワークに接続できない場合、SSID (ネットワーク名) とパスワードを手入力で打ち込んでください。SSID 名は AP のシリアル番号 (例えば、EC0123456789)、パスワードは AP の MAC アドレス (例えば、903CB3BC1234) です。

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更することが可能です。

- 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。MetroInq 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

新しいデバイスの登録

デバイスのシリアル番号とMACアドレスを入力（またはスキャン）することで、新しいデバイスをサイトに追加できます。 [もっと知る](#)
シリアル番号とMACアドレスは、製品ボックスが製品の裏面に記載されています。

次のサイトにデバイスを追加します

サイトレベルの設定を継承する
このサイトのデバイスを、共通の構成を持つ単一のユニットのように管理する場合は、これを有効にします。 [もっと知る](#)

バーコードスキャンモードを有効化 [?](#)

Always follow cloud configuration [?](#)

Batch Upload File

最大 48 台のデバイスを登録できます。



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ェブ 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ェ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待機しています。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。

i 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。

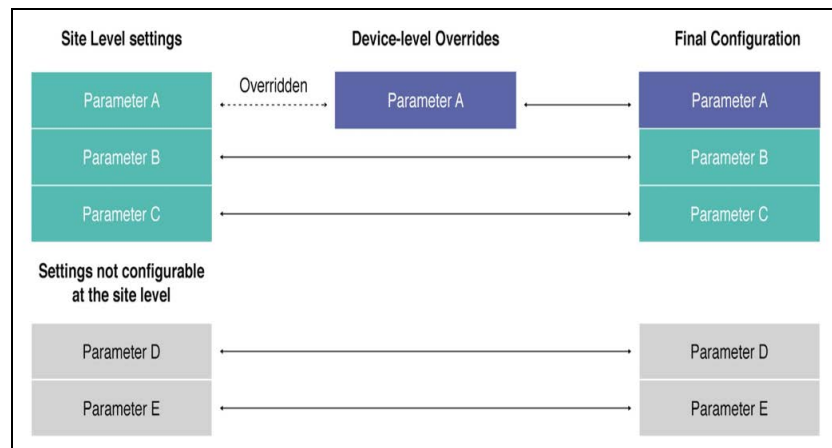
デバイス設定の変更

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。

i **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。

- 40 ページの「クラウドの管理」
- 76 ページの「基本のサイトの設定」
- 100 ページの「サイト WiFi 5 構成」
- 204 ページの「WiFi 5 デバイス構成」
- 226 ページの「Metrolinq デバイスの設定」

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

- 40 ページの「クラウドの管理」
- 46 ページの「クラウドダッシュボードの表示」
- 47 ページの「カスタマイズされたクラウドのダッシュボードの作成」
- 49 ページの「デバイスの管理」
- 55 ページの「サイトの管理」
- 56 ページの「ユーザの管理」
- 57 ページの「サイトグルーピング」
- 61 ページの「常にクラウド設定に従う」
- 64 ページの「ライセンスと請求の管理」
- 66 ページの「アドオン」
- 67 ページの「AuthPort アドオンを使用する」

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

← ALL CLOUDS

クラウドのプロパティ

クラウド情報

クラウド名*

詳細

ベータ版の特徴 [?](#)

課金情報

課金名

電子メール*

会社

Address 1

Address 2

都市

州/県/区

ZIP

VAT ID

Invoice language

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

← ALL CLOUDS

クラウドのプロパティ

クラウド情報

クラウド名*
TestCloud1

詳細

ベータ版の特徴 ?

課金情報

課金名

電子メール*

会社

Address 1

Address 2

都市

州/県/区

ZIP

国

VAT ID

Invoice language

キャンセル

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

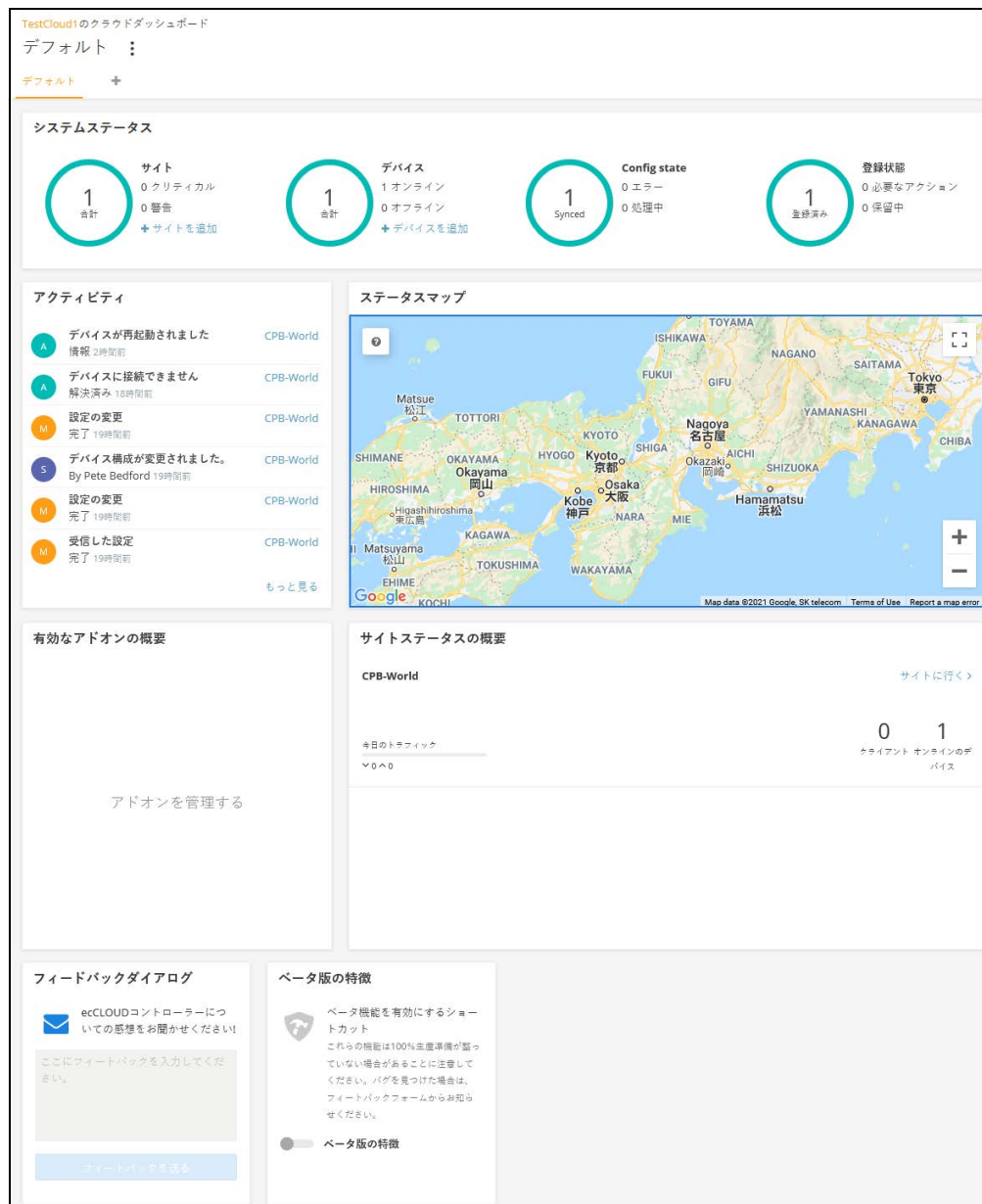


注意：一度クラウドを削除すると元に戻せません。AP、クライアント、サイト、システムアクティビティログ、クラウド内でのデバイスの設定など、関連する全ての記録が失われます。

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。

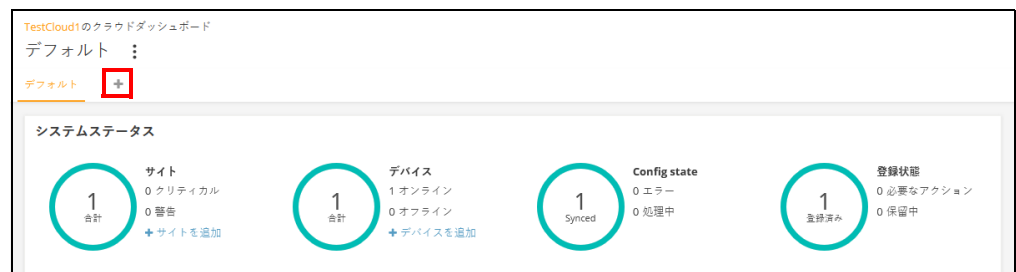
i 注意：カーソルを4つの円に合わせると、より多くの情報を得ることができます。

- 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ィジェットを加える



ウィ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。

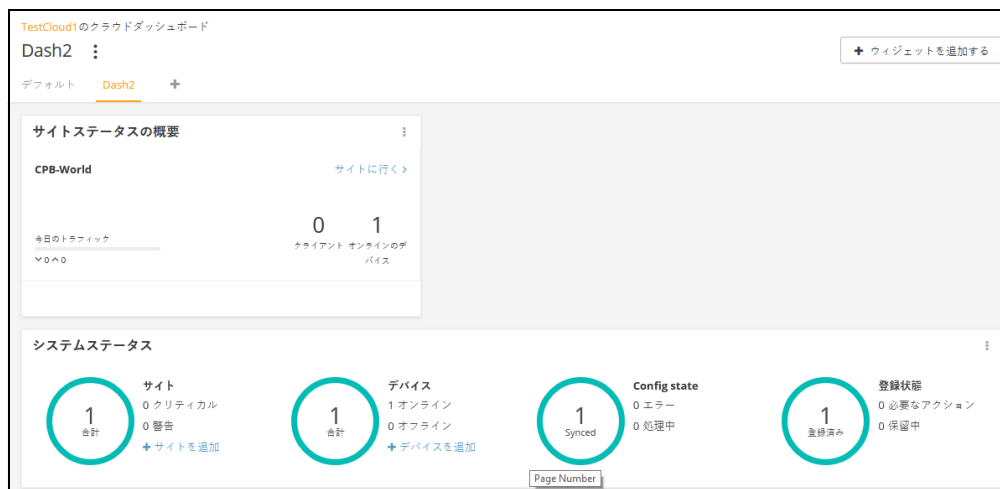
図 30: カスタマイズされたダッシュボードにウィジェットを選択する



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ィジェットが表示されるようになります。ウィジェットの大きさはウィ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、ウィジェットの名前を変更したり、ウィジェットを削除できます。

“ウィ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ィジェットを加えることができます。

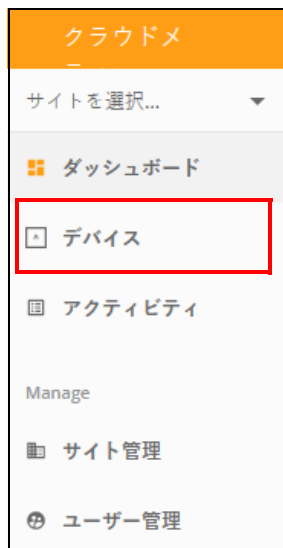
図 31: カスタマイズされたウィジェットをカスタマイズされたクラウドダッシュボードに追加する



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。

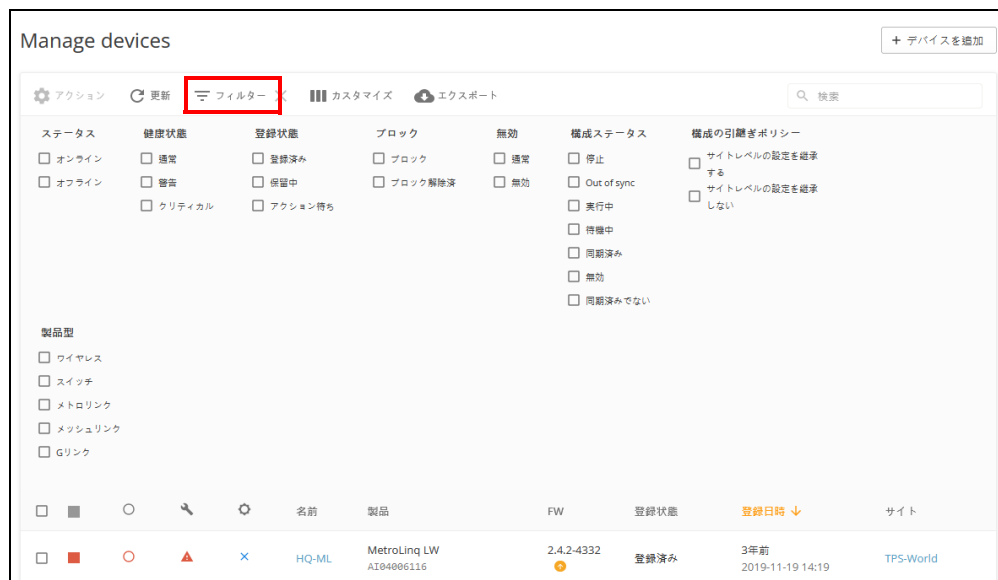
図 32: クラウドメニュー内のデバイス



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です。しかしこのポリシーはその後の状況によって変更することができます。詳細については、33 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”リストを使って変更することができます。

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

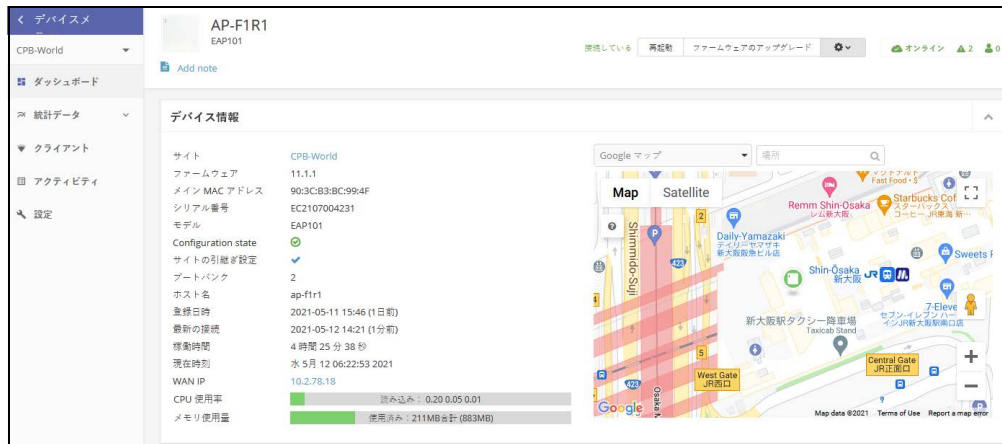


アクションメニューには以下のアイテムが表示されます。

- 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



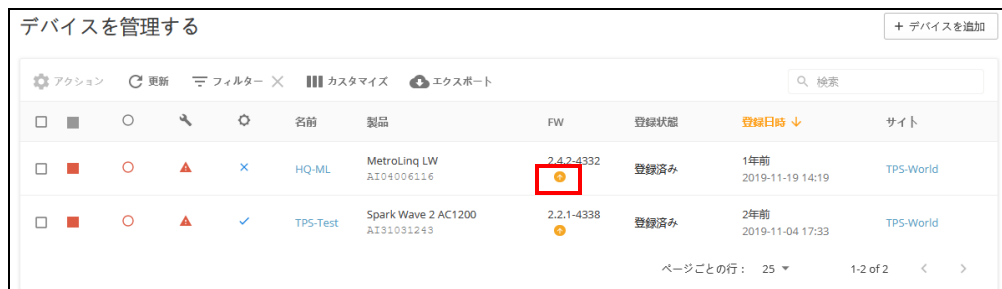
デバイスの追加 デバイスを追加するボタンをクリックして、“新しいデバイスを登録する”ページを開き、デバイスをクラウドに加えてください。

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ェ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



ファームウェ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: 装置のファームウェアのアップグレード

新しいファームウェア アップグレードタスク

製品ラインを選択する

モデルの選択

次のバージョンにアップグレード

このタスクに名前を付ける

アップグレードをいつ開始しますか? 今すぐ 後で

アップグレードをどのように実行しますか? 全て同時に 1つずつ 10分

どのデバイスをアップグレードしますか? すべて期限切れ互換性のあるデバイス 選択する 以下のみ: **HQ-ML**

デバイスをデフォルトにリセットしますか?

Upgrade firmware to two bootbanks

選択したデバイス数: 1

デバイス名	製品	現在のFW	新しいFW	MAC
<input checked="" type="checkbox"/> HQ-ML	MetroLinq LW	2.4.2-4332	2.4.2-4531	28:76:10:14:36:C6

10 エントリを表示 of 1 entries (filtered from 2 total entries)

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向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

The screenshot shows the 'アクティビティ' (Activities) page. At the top, there are three category buttons: 'All' (selected), 'アラート' (Alerts), and 'メンテナンス' (Maintenance). Below these are filter options for '日付範囲' (Date Range) and 'クリア' (Clear). A red box highlights the '日付範囲' section, which includes 'から' (From) and 'まで' (To) date pickers. Below the filter is a table of activities.

日付	タイプ	ステータス	AFFECTED	詳細
5時間前 2021-05-12 09:58	警告アラート	情報	AP-F1R1	Device has rebooted.
21時間前 2021-05-11 17:33	重要なアラート	解決済み	AP-F1R1	デバイスに接続できません
1日前 2021-05-11 17:08	設定の変更 (デバイス)	完了	AP-F1R1	デバイスで設定が更新されました。 デバイスに送信された設定: ワイヤレス

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

The screenshot shows the 'アクティビティ' (Activities) page with the 'メンテナンス' (Maintenance) category selected. The table displays maintenance tasks.

日付	ステータス	タイプ	AFFECTED	詳細
1日前 2021-05-11 17:08	完了 2021-05-11 17:09	設定の変更 (デバイス)	AP-F1R1	デバイスで設定が更新されました。 デバイスに送信された設定: ワイヤレス
1日前 2021-05-11 17:01	完了 2021-05-11 17:03	設定の変更 (システム)	AP-F1R1	Initial configuration was successfully sent to the device. デバイスに送信された設定: Ignite, DHCP, Dropbear, イーサネット, ファイアーウォール, 言語, ネットワーク, システム, ユーザー, ワイヤレス, Files
1日前 2021-05-11 17:01	完了 2021-05-11 17:01	受信した設定 (デバイス)	AP-F1R1	Configuration was successfully created on the cloud. デバイスから受信した設定: Ignite, DHCP, Dropbear, イーサネット, ファイアーウォール, 言語, ネットワーク, システム, ユーザー, ワイヤレス

100 エントリを表示 of 3 entries

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。

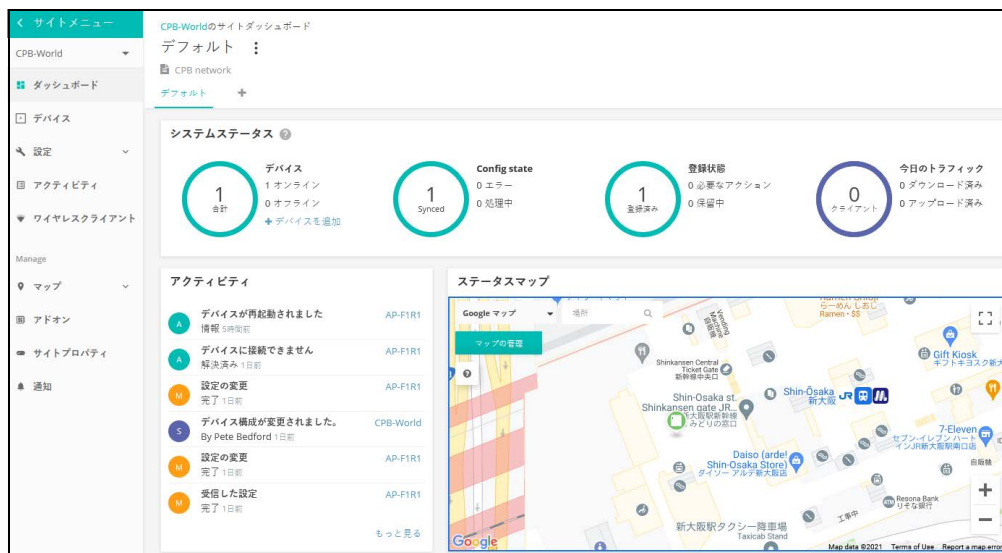
図 42: サイトの管理ページ



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

← 全てのユーザーに戻る

ユーザーを招待する

電子メール

example@domain.com

役割

所有者
クラウドの所有者は、クラウド内のすべての設定を完全に制御できます。

管理者
クラウド管理者は、管理するクラウド内の全てのサイトおよびデバイスへのほぼ完全な書き込み権限とアクセス権を持っています。ただし、アフォルトでは請求とライセンス設定を管理できません。これを行えるのはクラウドの所有者のみです。以下のチェックボックスを使用し、管理者に追加の権限を付与できます。

追加の許可

ライセンスと請求を管理する ⓘ

VPCの設定を管理する ⓘ

ゲスト
ゲストはクラウド内のすべてのサイトとデバイスにアクセスできますが、それらに変更を加えることはできません。ゲストは、デバイスとサイトの構成でパスワードを確認することもできます。

サイトユーザー
サイトレベルのユーザーは、以下で指定するサイトにバインドされます。さらに、指定されたサイト内で、マネージャー（全ての書き込み権限を持つ）またはゲスト（読み取りのみの権限を持つ）として分類できます。

メッセージ

こんにちは。私のクラウドに参加してください。

キャンセル 招待

“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。

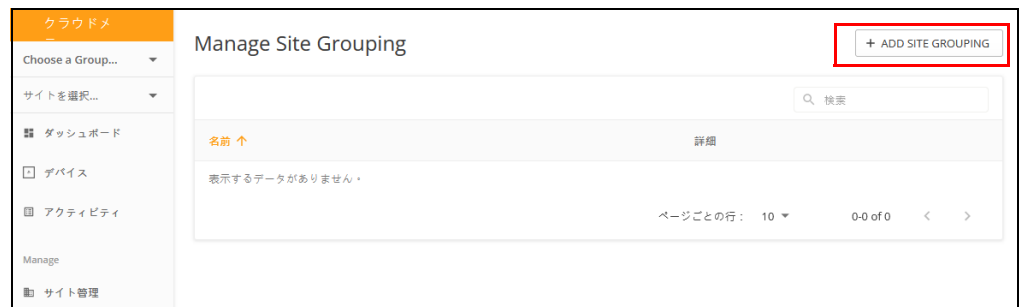
サイトグループを作成するには、サイトの管理ページに行き、“サイトグルーピングの管理”をクリックします。

図 46: サイトグルーピングへのアクセス



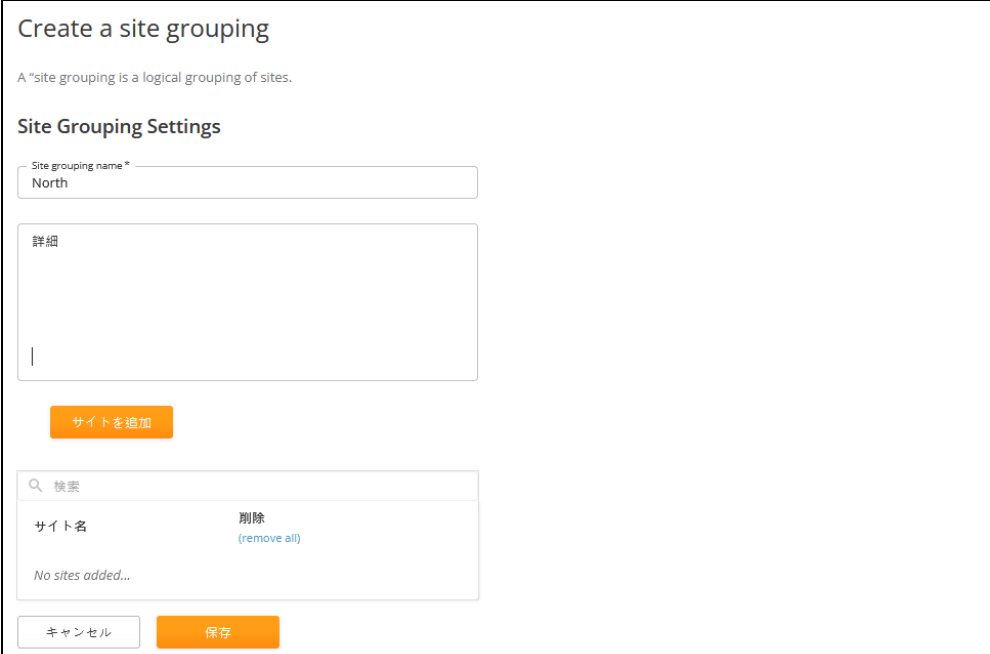
サイトグルーピングページで、サイトグルーピングの追加をクリックしてください。

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



Create a site grouping

A site grouping is a logical grouping of sites.

Site Grouping Settings

Site grouping name *
North

詳細

サイトを追加

検索

サイト名	削除
No sites added...	

キャンセル 保存

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



クラウドメ

Choose a Group...

サイトを選択...

ダッシュボード

デバイス

アクティビティ

Manage

サイト管理

Manage Site Grouping

+ ADD SITE GROUPING

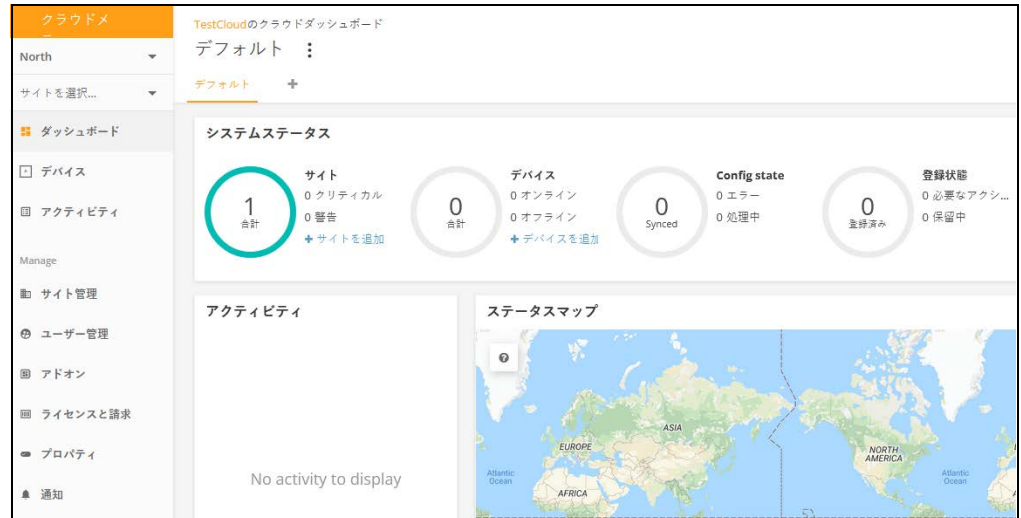
検索

名前	詳細
North	編集 削除

ページごとの行: 10 1-1 of 1

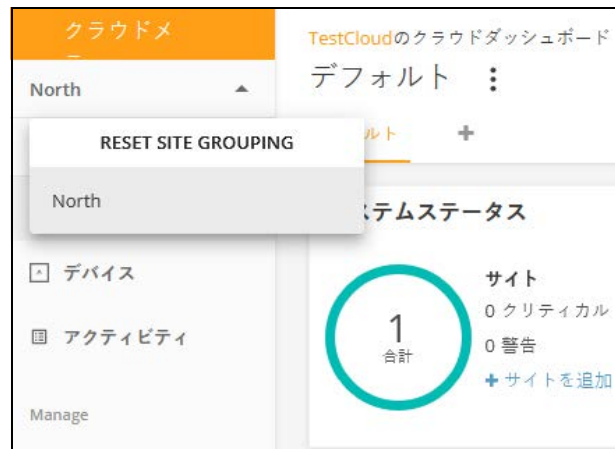
サイトグループを選択するとページがリフレッシュされ、グループ内のサイトから集約された情報を見ることができます。

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。

i 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 のコンフィギュ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ギュ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。

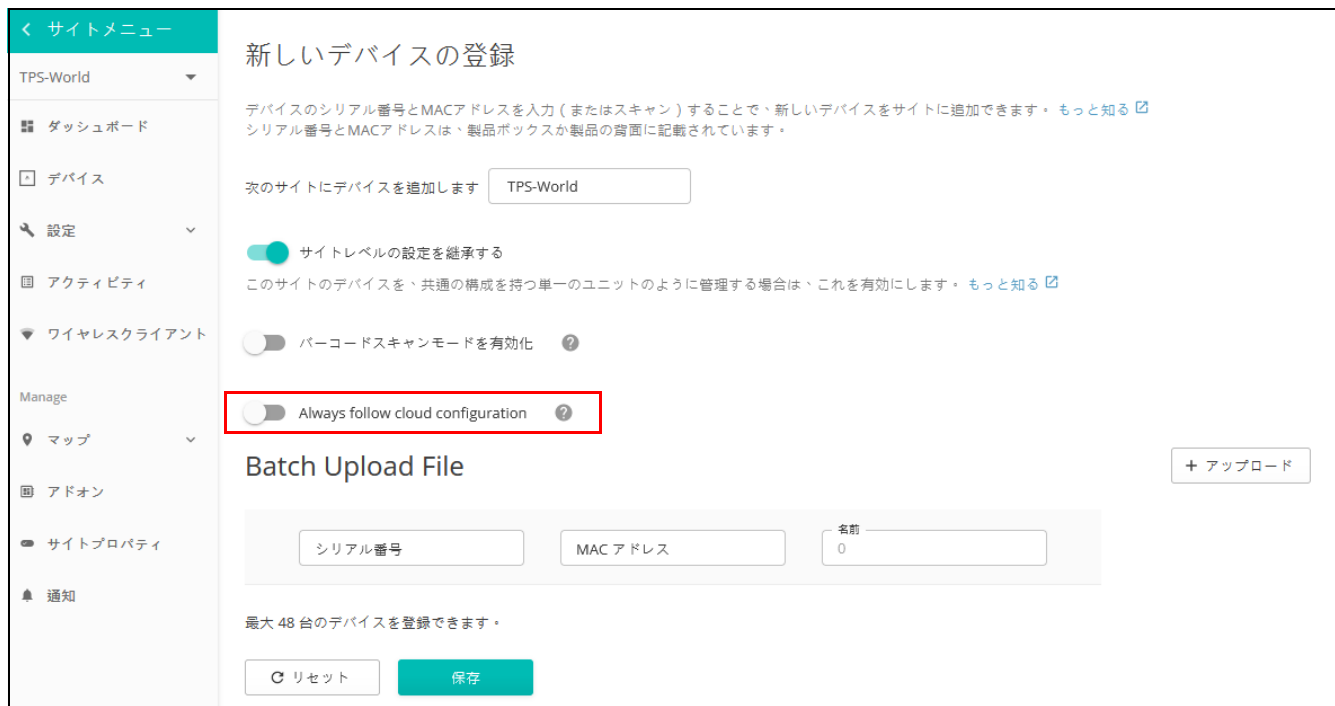
新しいデバイスを登録する際、"常にクラウド設定に従う" を有効にすることができます。

i 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。

章 2 | クラウドの管理

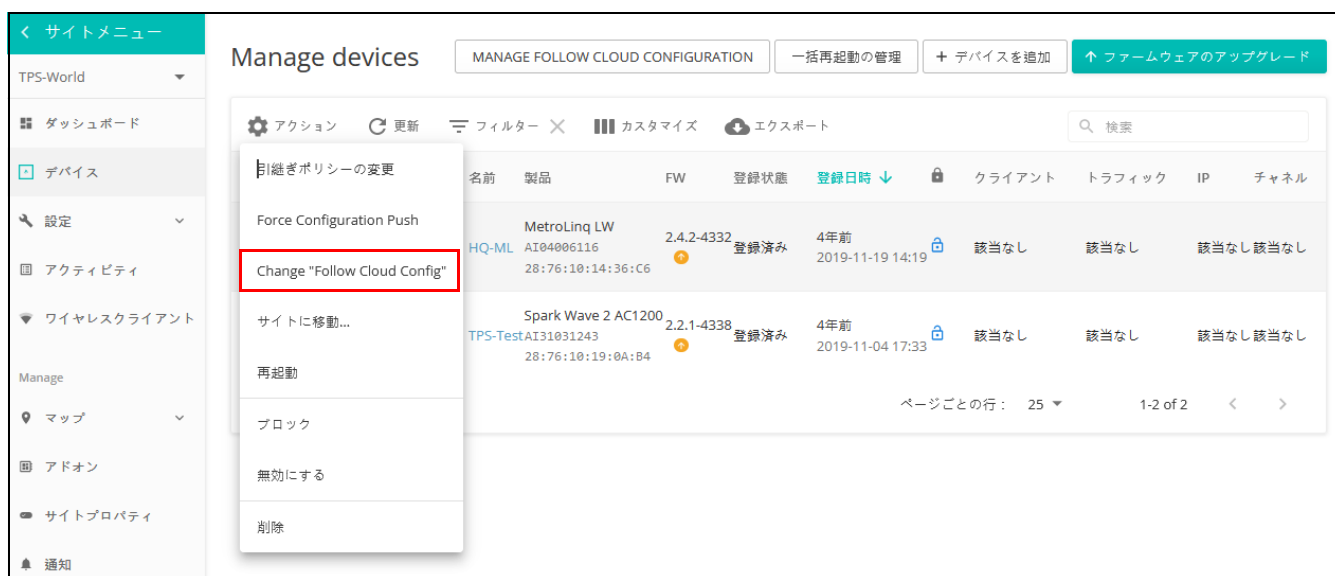
常にクラウド設定に従う

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。

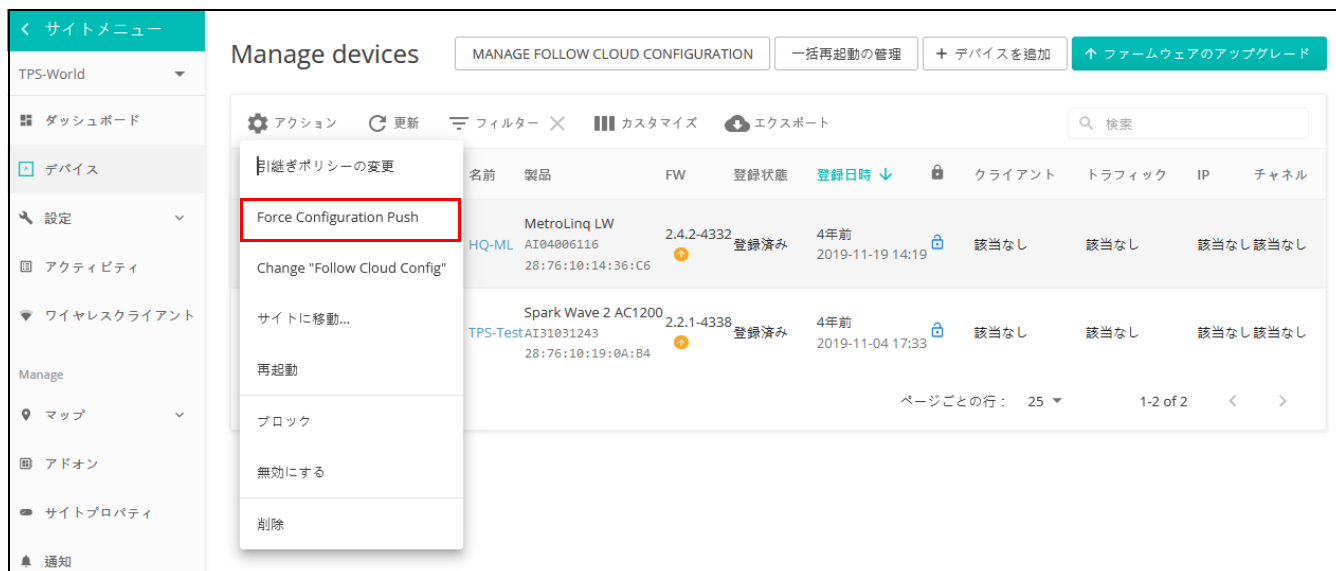
図 54: フォロークラウドの設定を管理



“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。

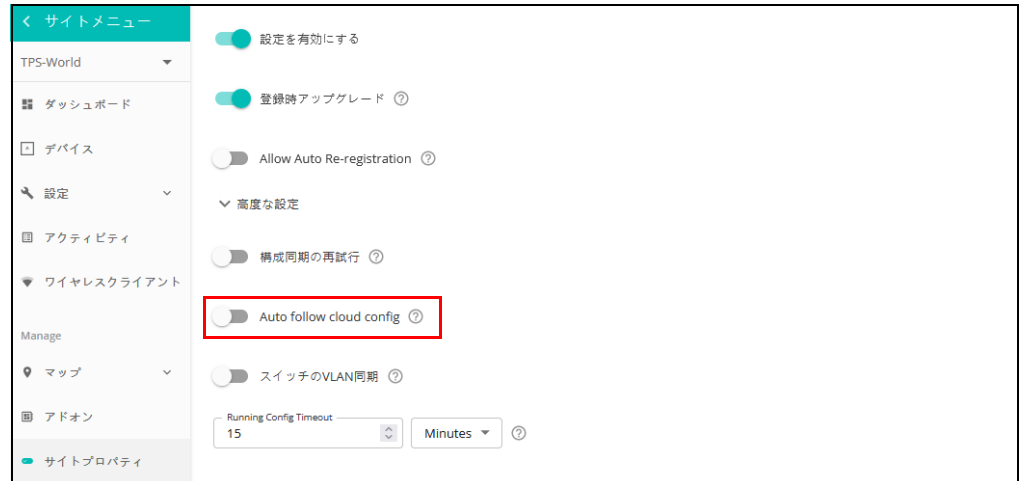
クラウドとデバイスの設定を同期するには、デバイスレベルの設定で“同期する”をクリックするか、サイトレベルのデバイスページから設定をプッシュします。

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

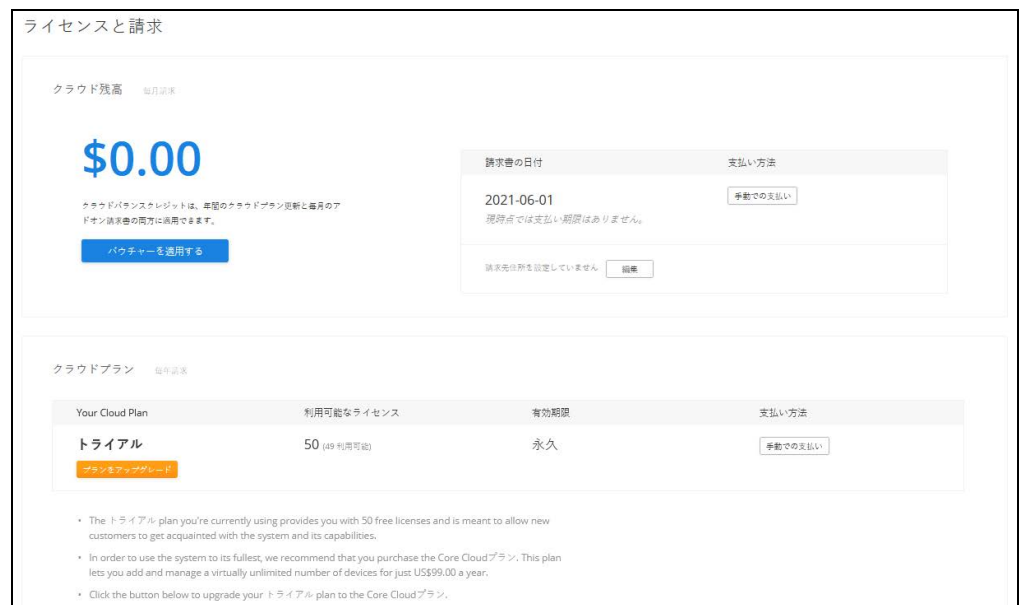


i 注意 : MSP モードと "常にクラウド設定に従う" を同時に有効にしないでください。デバイスの設定が ecloud に正しく更新されなくなります。

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、シングルマニユ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。

アドオン

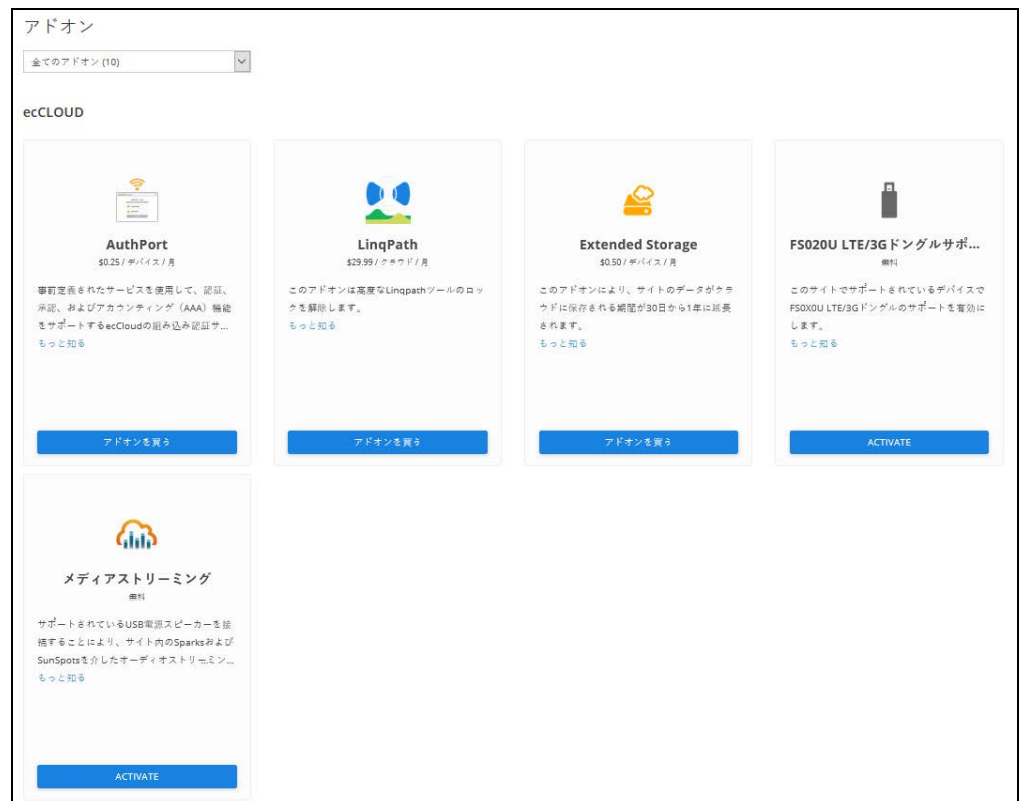
このチャプターは下記のようなアドオンについて説明します。

- 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ェアのサポート

アドオンを使用する

アドオンメニューから選択ボタンをクリックして、“さらに知りたい”をクリックします。“ACTIVE” ボタンをクリックすると選択したサービスが使用できます。

図 58: 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トリ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。

i 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 59: AuthPort アドオン



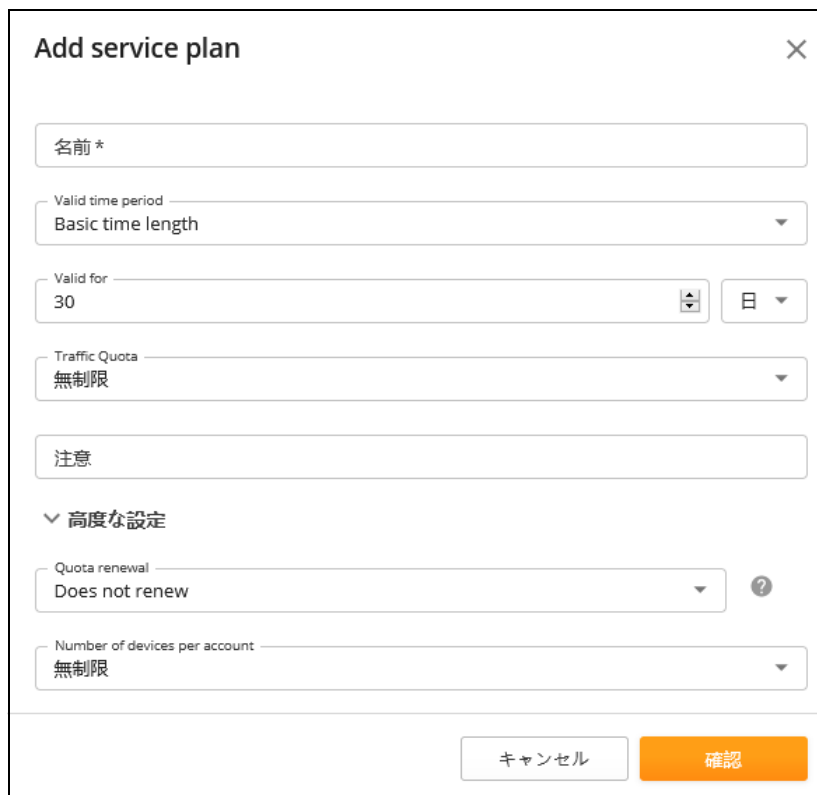
Authport アドオンを使えるようになると、クラウドメニューに Authport 設定メニューが表示されます。サービスプラン、経理、認証、キャプティブポータルを設定をしてください。

図 60: 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 61: サービスプランを追加する

A screenshot of the 'Add service plan' form. The form has a title bar with 'Add service plan' and a close button (X). Below the title bar are several input fields: '名前*' (Name), 'Valid time period' (Basic time length), 'Valid for' (30 days), 'Traffic Quota' (無制限), and a '注意' (Note) field. There is a section titled '高度な設定' (Advanced settings) with a dropdown for 'Quota renewal' (Does not renew) and a dropdown for 'Number of devices per account' (無制限). At the bottom right, there are two buttons: 'キャンセル' (Cancel) and '確認' (Confirm).

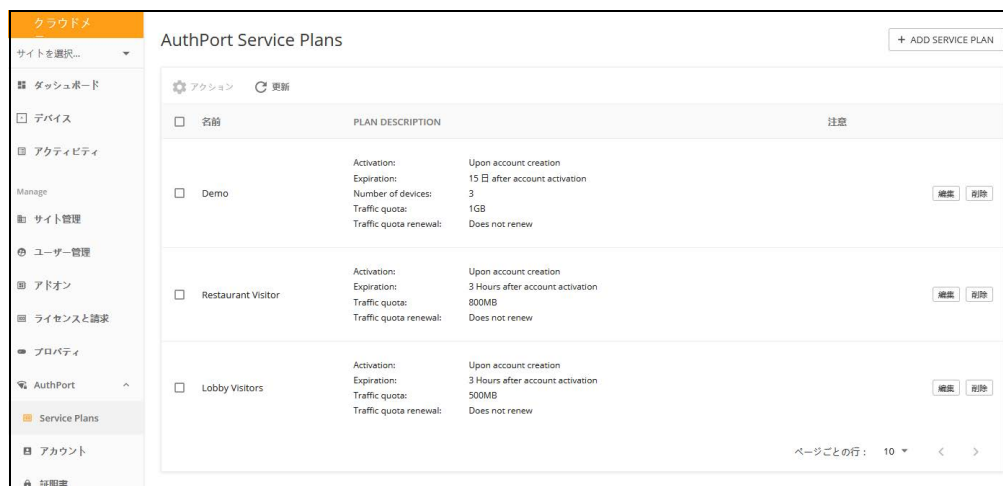
以下のリストはサービスプランとして設定可能なアイテムです。

- 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。
- トラフィッククォータ — 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“クォータ不足”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。
- クォータリニューアル — データのトラフィッククォータを更新する時期を設定します。クォータは日々、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 62: 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 63: 一つのアカウントを作成する

Username *

パスワード *

Plan *
Demo

Activation	Upon account creation
Quota renewal	Does not renew
Number of devices	3
Quota	1GB
期限日	15 日 after account activation

Multiplier
1

合計	
Quota	1GB
期限日	15 日 after account activation

Notes

キャンセル 確認

図 64: 複数アカウントを一度に作成する

Plan *
Demo

Activation	Upon account creation
Quota renewal	Does not renew
Number of devices	3
Quota	1GB
期限日	15 日 after account activation

Multiplier
1

合計	
Quota	1GB
期限日	15 日 after account activation

アカウント数
1

Notes

Export generated accounts to a file

キャンセル 確認

アカウントを作成するどちらの方法も、クォータを“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、基本量のクォ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 クォータを所持するサービスプランを作成したとします。この基本のクォータを 3 倍にして、30GB クォータ分の設定できます。

図 65: アカウントのリスト

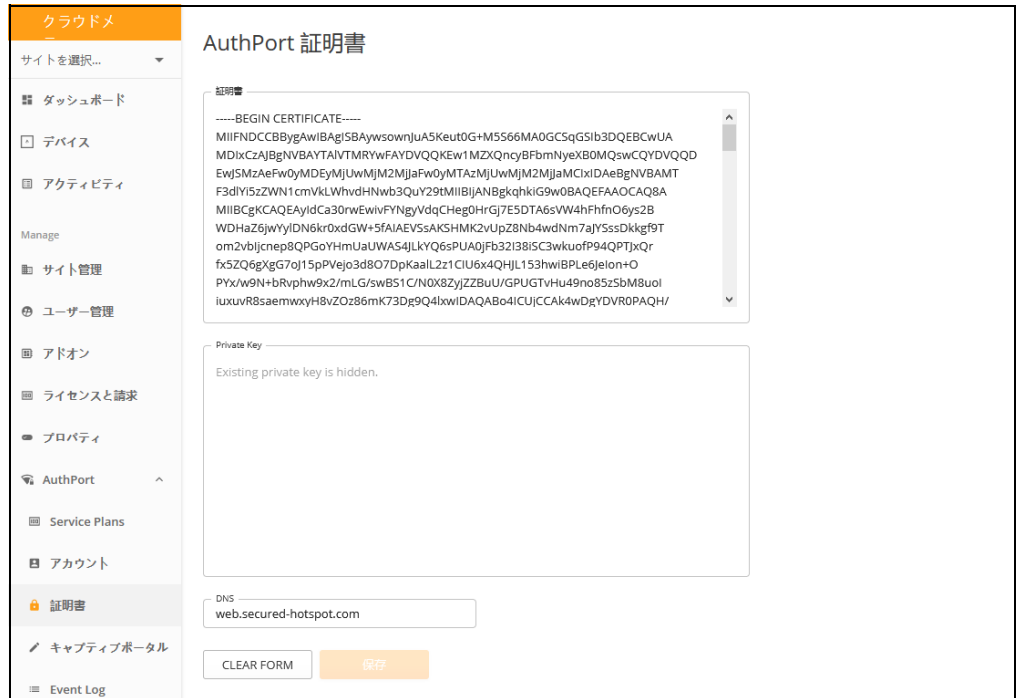
アクション	更新	エクスポート	検索					
<input type="checkbox"/>	<input type="checkbox"/>	USERNAME ↑	パスワード	PLAN	TRAFFIC QUOTA	EXPIRATION TIME	SESSION DURATION	注意
<input type="checkbox"/>	<input type="checkbox"/>	u0KZY8	*****	Demo	0B used / total 1GB	アカウント非アクティブ	オフライン	編集 削除
<input type="checkbox"/>	<input type="checkbox"/>	u5CPY4	*****	Demo	0B used / total 1GB	アカウント非アクティブ	オフライン	編集 削除
<input type="checkbox"/>	<input type="checkbox"/>	u5CT0H	*****	Demo	0B used / total 1GB	アカウント非アクティブ	オフライン	編集 削除
<input type="checkbox"/>	<input type="checkbox"/>	uCR8EK	*****	Demo	0B used / total 1GB	アカウント非アクティブ	オフライン	編集 削除
<input type="checkbox"/>	<input type="checkbox"/>	uKESDU	*****	Demo	0B used / total 1GB	アカウント非アクティブ	オフライン	編集 削除
<input type="checkbox"/>	<input type="checkbox"/>	uMKXMB	*****	Demo	0B used / total 1GB	アカウント非アクティブ	オフライン	編集 削除
<input type="checkbox"/>	<input type="checkbox"/>	uP5YZP	*****	Demo	0B used / total 1GB	アカウント非アクティブ	オフライン	編集 削除
<input type="checkbox"/>	<input type="checkbox"/>	uTCHK2	*****	Demo	0B used / total 1GB	アカウント非アクティブ	オフライン	編集 削除
<input type="checkbox"/>	<input type="checkbox"/>	uX4M55	*****	Demo	0B used / total 1GB	アカウント非アクティブ	オフライン	編集 削除
<input type="checkbox"/>	<input type="checkbox"/>	uXTXD1	*****	Demo	0B used / total 1GB	アカウント非アクティブ	オフライン	編集 削除

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、トラフィッククォ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、クォ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 66: 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。

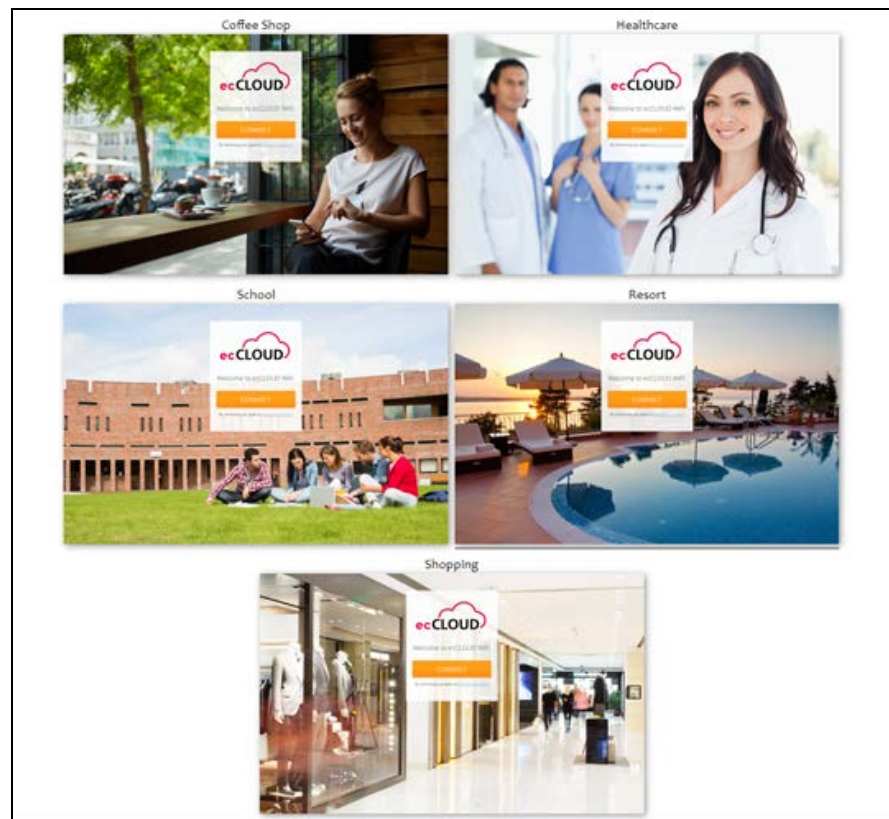
ドメインネームサービス (DNS) について説明します。アドミニストレーターは無線クライアントのドメインネーム (DNS) を設定し、クライアントがキャプティブポータルページを閲覧できるようにしてください。ドメインネームサービス (DNS) が設定されていない場合は、クライアントのキャプティブポータルページの URL 内に、アクセスポイント (AP) モードの IP アドレスが表示されます。

Web ブラウザにセキュリティ警告が起これ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。

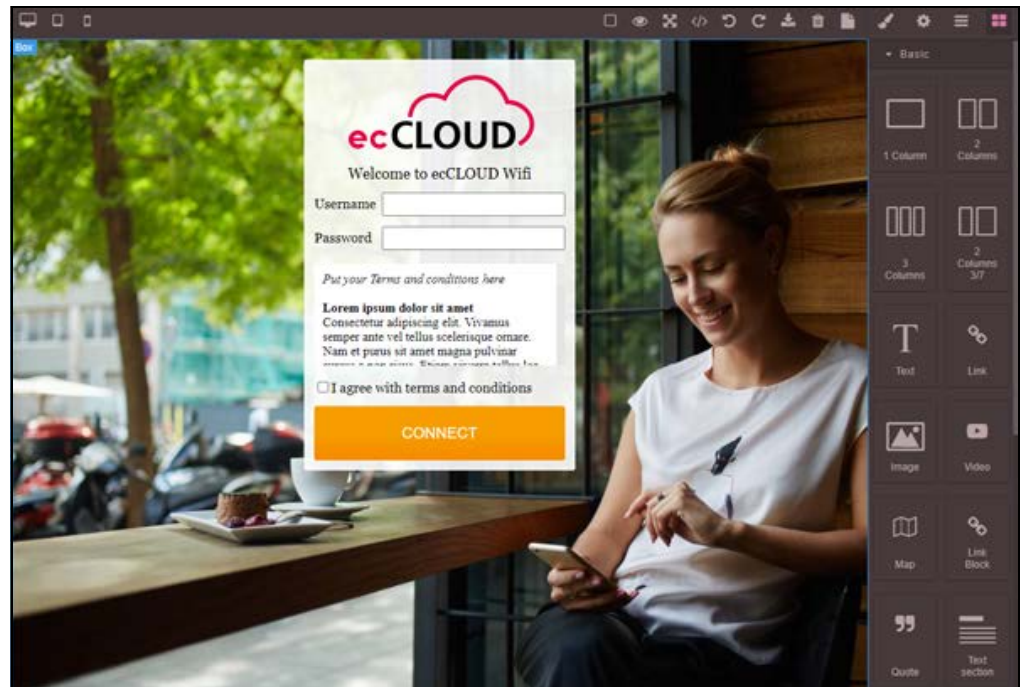
もしキャプティブポータルを作成し、エディターにアクセスするのが初めての場合は、自分のキャプティブポータルのテーマを選択するように誘導されます。自分のサービスにより近いテーマを選択し、ページの内容を編集してください。

図 67: オースポートキャプティブポータルのテーマの例



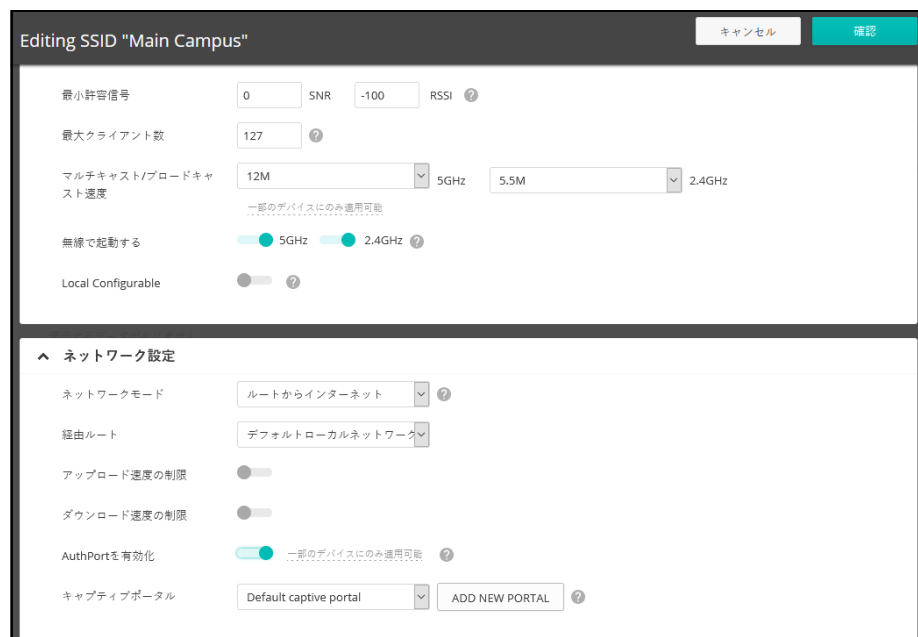
テンプレートを選択すると、キャプティブポータルエディターに誘導されます。エディターのレイアウトは大まかに 3 つの部分があります。ツールバー、オプション/アトリビュートパネル、プレビューフレームです。ツールバーはエディターの上の部分にあります。右側にはオプションとアトリビュートが設定できるようになっています。プレビューフレームを使うと、ドラッグアンドドロップ形式でページ内のウィジェットを探したり、自分のポータルデザインをリアルタイムで閲覧したりできます。

図 68: 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 69: 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。

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。

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。

- 77 ページの「サイトの全体像」
- 78 ページの「サイトの作成」
- 85 ページの「サイトのダッシュボードの表示」
- 87 ページの「カスタマイズされたサイトのダッシュボード」
- 89 ページの「無線 AP とクライアントをモニターする」
- 94 ページの「メンテナンスタスクのスケジュールを立てる」
- 96 ページの「サイトの通知」

サイトの全体像

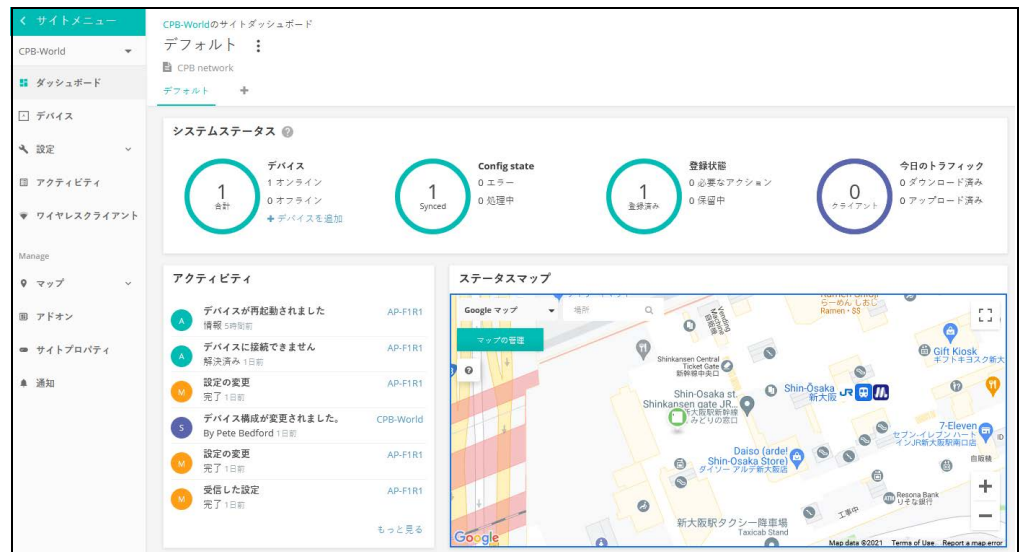
一つのサイトはデバイスを論理的にグループ化していますが、全てのデバイスが同じ設定であるとは限りません。1つのグループのデバイスは、大体同じサイトに位置されています。

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。

i 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 70: 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、[24 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。

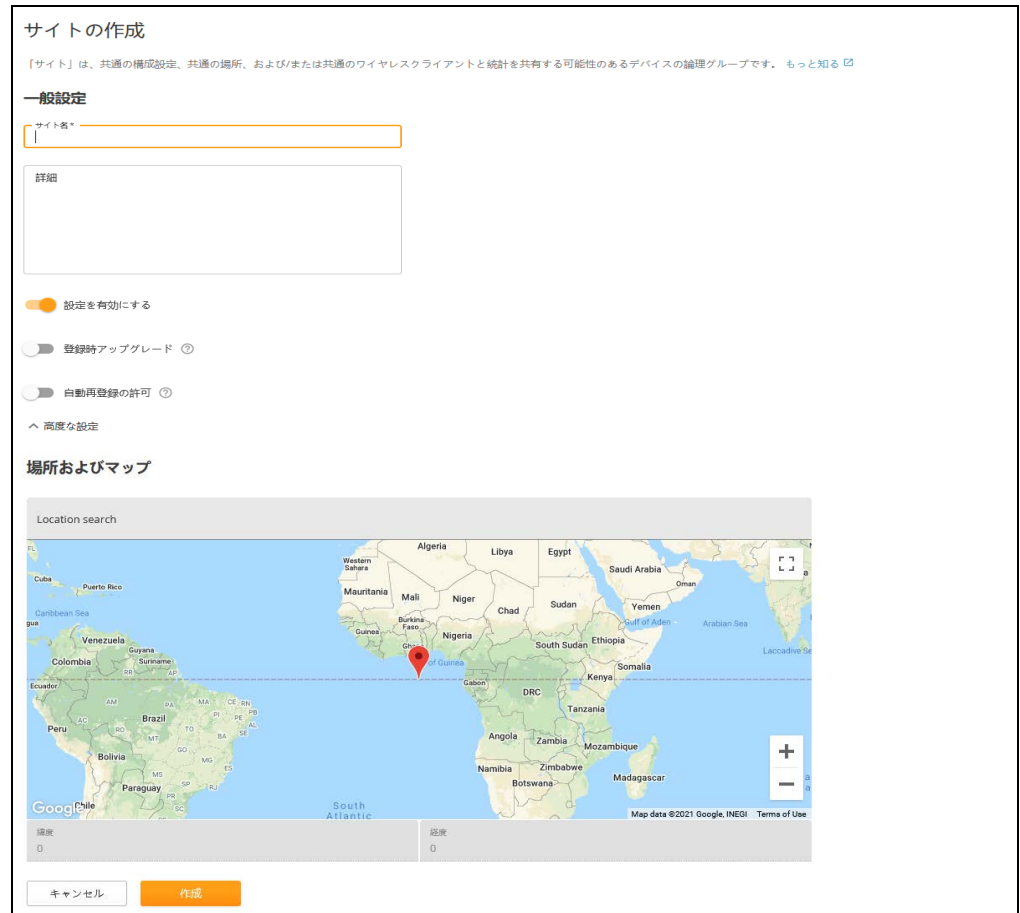
図 71: 新しいサイトを作成する



“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。

i 注意：アスタリスク（*）マークのついた欄は入力必須です。

図 72: 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、ファームウェ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。

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 73: 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。

i 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 74: 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 75: 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なら、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。

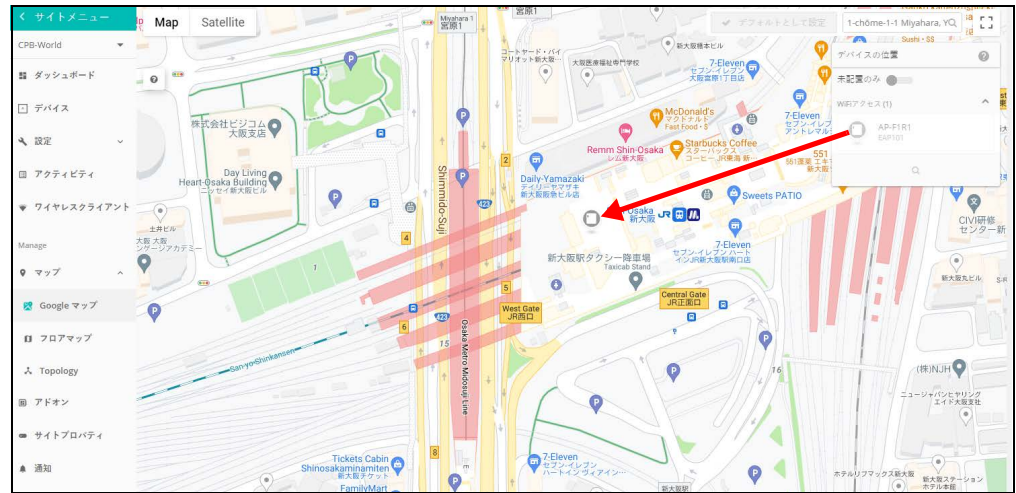
図 76: 新しいデバイスを登録する

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 77: 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 78: 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。

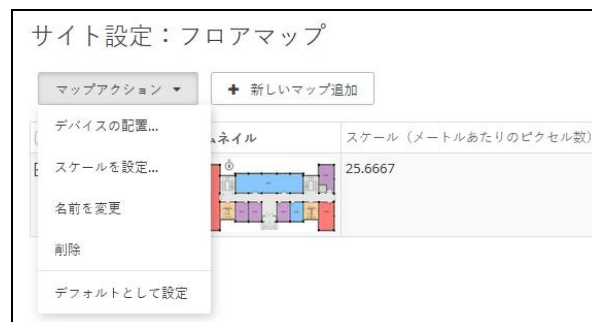
新しいマップを追加する “ をクリックすると、フロアプランを作る際に役立つ、カスタマイズされたフロアのイメージマップをアップロードできます。

図 79: 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 80: 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 81: 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。

i 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、100 ページの「[サイト WiFi 5 構成](#)」をお読みください。

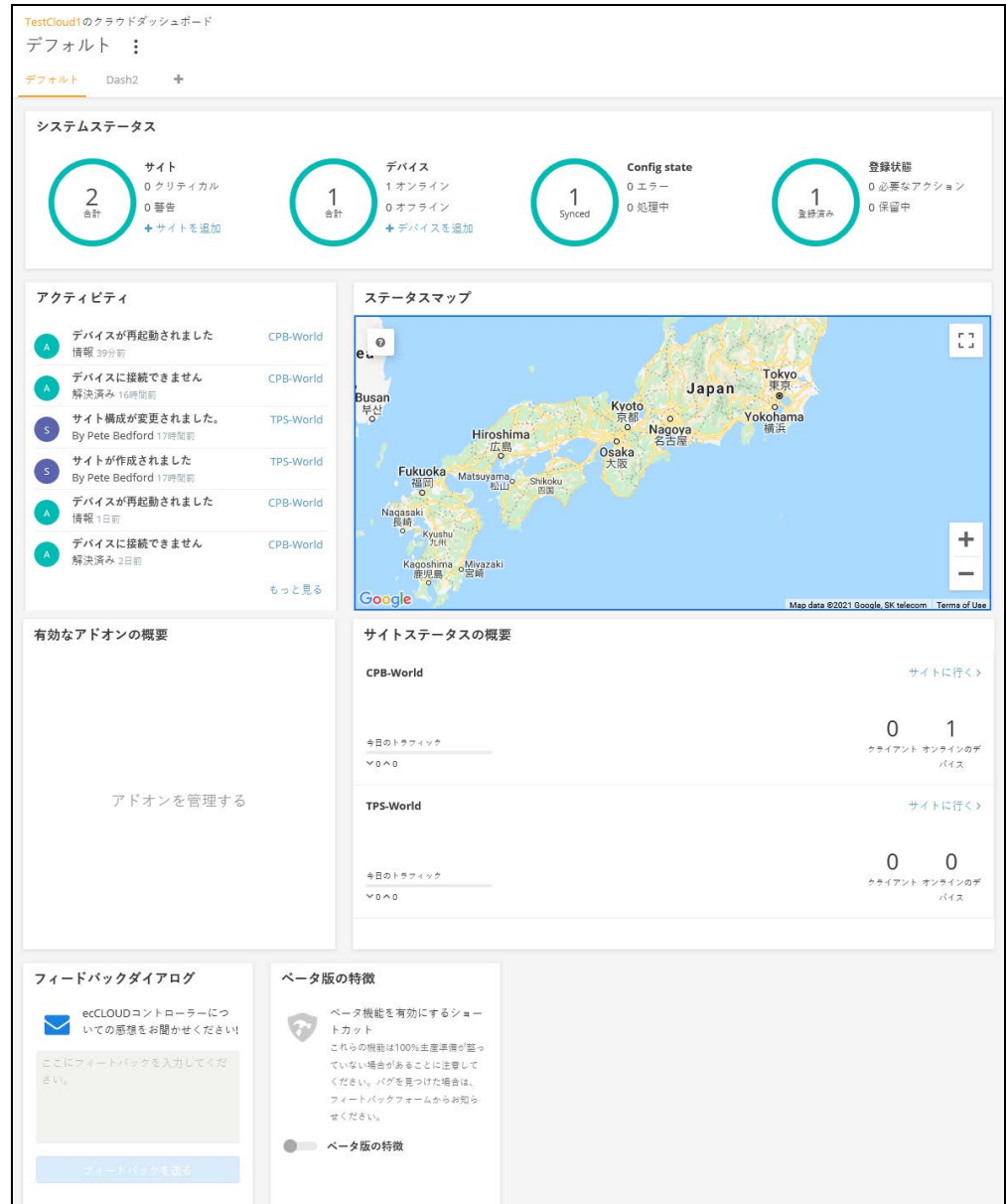
図 82: WiFi5 構成



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、ゲートウェ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 83: 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。

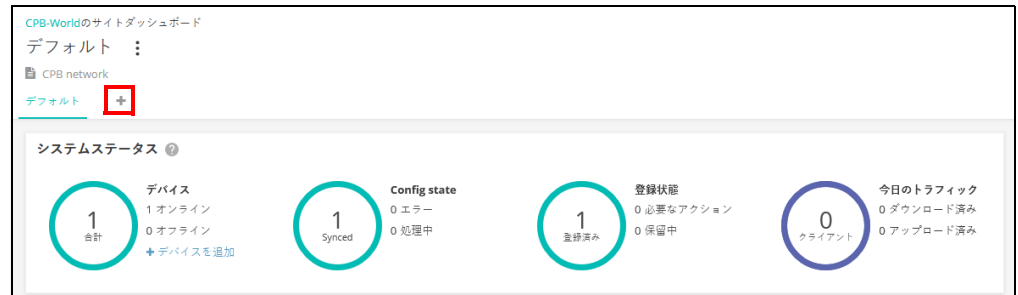
i 注意：カーソルで4つの円を指すと、さらに詳しい情報が表示されます。

- 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ィ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 84: 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 85: 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ブの隣に、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アイテムを追加してください。

図 86: カスタマイズされたサイトのダッシュボードにウィジェットを追加する



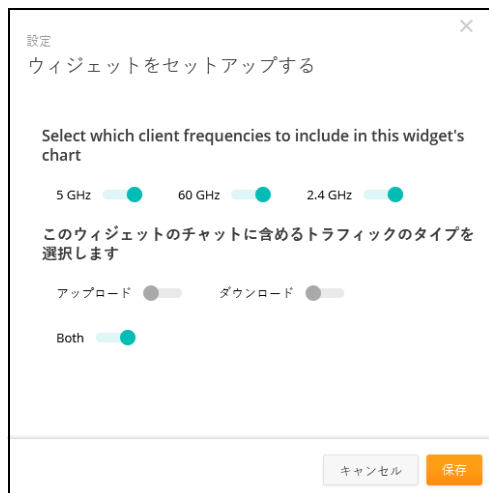
ウィジェットを選択したら、“追加”ボタンをクリックしてください。

図 87: カスタマイズされたサイトのダッシュボードにウィジェットを選択する



ウィ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ィンドウで通知されるので、必要なウィ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。

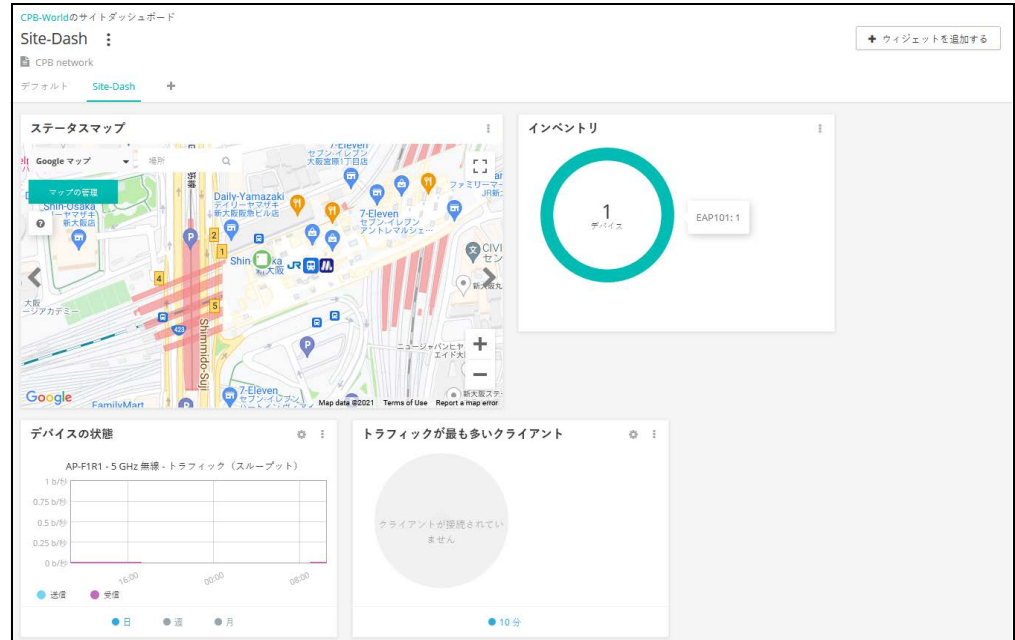
図 88: 新しいサイトのダッシュボードウィジェットをカスタマイズする



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ィジェットが表示されます。ウィ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。ウィジェットは、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。

☒ 89: カスタマイズされたサイトのダッシュボード

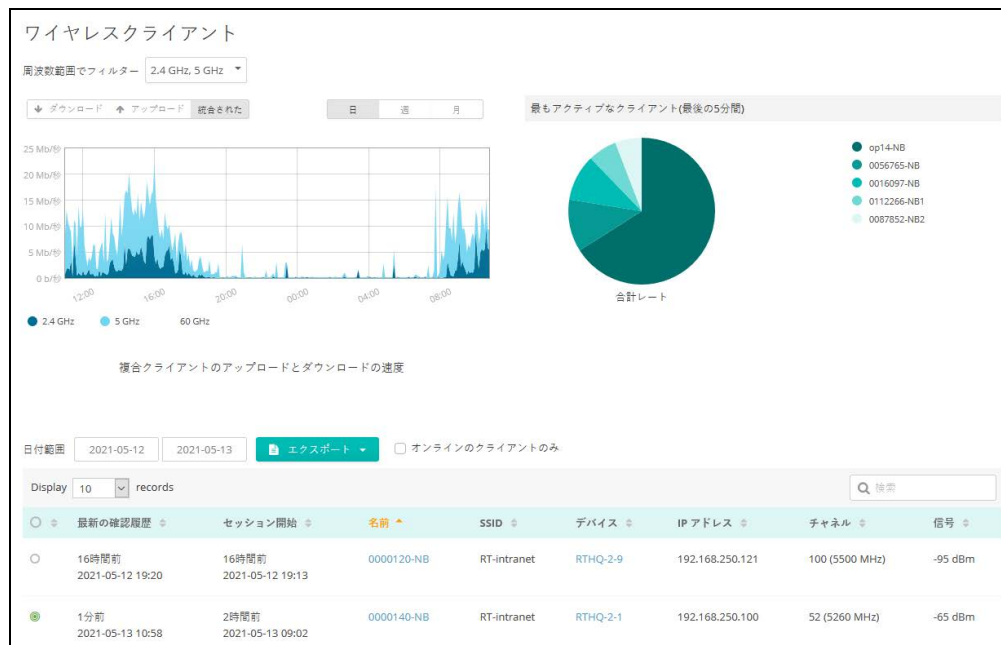


無線 AP とクライアントをモニターする

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ロード、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られます。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られることもできます。

図 90: 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 91: 無線 AP の情報

RTHQ-2-3
Spark Wave 2 AC1200

操作している 再起動 ファームウェアのアップグレード

オンライン 0 17

Add note

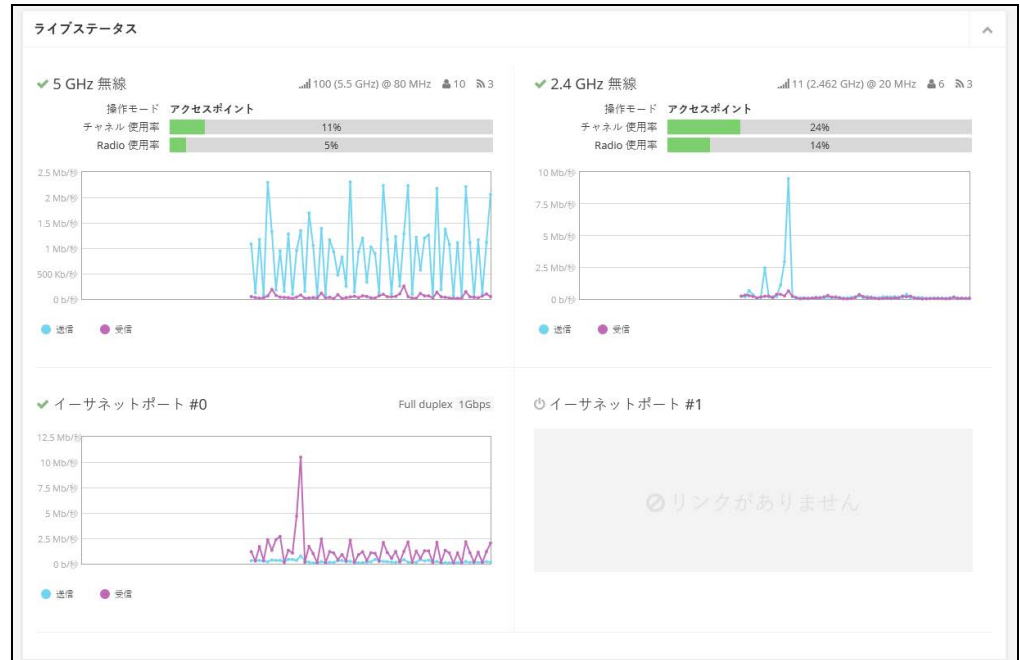
デバイス情報

サイト	HO-総公司
ファームウェア	2.3.0-4567
メイン MAC アドレス	28:76:10:08:50:86
シリアル番号	AH26019785
モデル	SP-W2-AC1200
Configuration state	🟢
サイトの引継ぎ設定	✓
ブートバンク	1
ホスト名	rthq-2-3
登録日時	2019-05-30 15:17 (2年前)
最新の接続	2021-05-13 11:08 (2分前)
稼働時間	1日6時間9分20秒
現在時刻	木5月13日11:10:22 2021
WAN IP	172.16.1.244
CPU 使用率	7%
メモリ使用量	使用済み: 63MB / 計 (116MB)

2F サービスエリアを表示

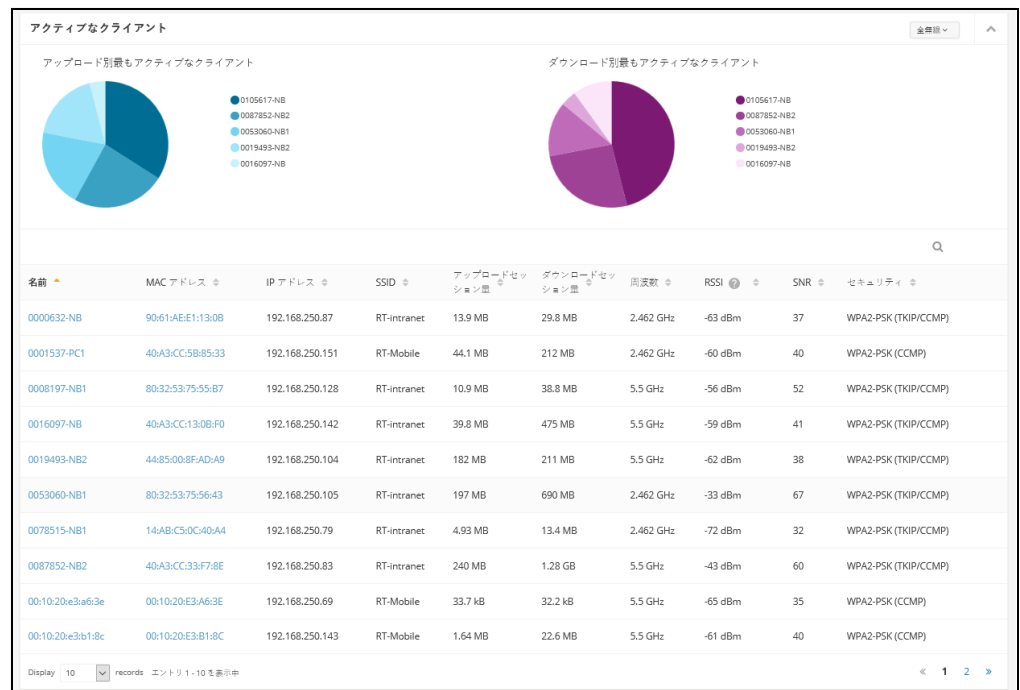
デバイスの情報ページの二つ目のセクションは、AP のレートとイーサネットインターフェースについてのスループットと利用のデータを説明します。

図 92: 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。

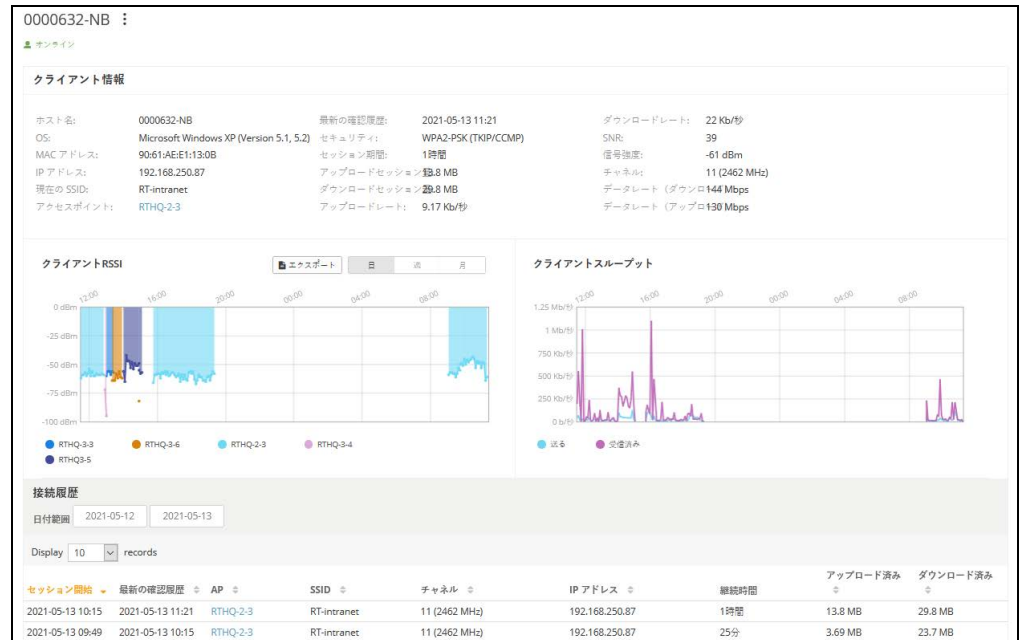
図 93: を頻繁に使用する無線クライアント



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 94: 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 95: 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空白にしたまま、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 96: メンテナンスタスクの管理



デバイス管理画面のスクリーンショット。表には以下のデータが含まれています。

名前	製品	FW	登録状態	登録日時	クライアント	トラフィック
2-8	SunSpot AC1200 AG33033882	1.4.2-3073	登録済み	1年前 2020-01-14 11:41	2	120 Kb/秒
3-10	Spark Wave 2 AC1200 AK08028907T		登録保留中	4ヶ月前 2021-01-05 10:09	該当なし	該当なし
RTHQ-2-1	SunSpot AC1200 AG33033809	1.4.2-3073	登録済み	4年前 2017-04-06 09:46	3	245 Kb/秒

ファームウェアをアップグレードする

ファームウェ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ェ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 97: 新しいファームウェアアップグレードタスクのページ

新しいファームウェア アップグレードタスク

製品ラインを選択する: All

モデルの選択: All

次のバージョンにアップグレード: 最新

このタスクに名前を付ける: ファームウェアのアップグレード (バージョン)

アップグレードをいつ開始しますか? 今すぐ 後で

アップグレードをどのように実行しますか? 全て同時に 1つずつ 90分

どのデバイスもアップグレードしますか? すべて期限切れ 互換性のあるデバイス 選択する

デバイスをデフォルトにリセットしますか?

Upgrade firmware to two bootbanks:

選択したデバイス数: 9

デバイス名	製品	現在のFW	新しいFW	MAC
<input checked="" type="checkbox"/> RTHQ-2-3	Spark Wave 2 AC1200	2.3.0-4567	3.0.1-4649	28:76:10:0B:50:86
<input checked="" type="checkbox"/> RTHQ-3-4	Spark Wave 2 AC1200	2.3.0-4567	3.0.1-4649	28:76:10:0C:55:8A
<input checked="" type="checkbox"/> RTHQ-AP4-3	Spark Wave 2 AC1200	2.3.0-4567	3.0.1-4649	28:76:10:19:FE:22
<input checked="" type="checkbox"/> RTHQ-3-2	Spark Wave 2 AC1200	2.3.0-4567	3.0.1-4649	28:76:10:0C:52:6E
<input checked="" type="checkbox"/> RTHQ-3-8	Spark Wave 2 AC1200	2.3.0-4567	3.0.1-4649	28:76:10:0B:F2:82
<input checked="" type="checkbox"/> RTHQ-2-9	Spark Wave 2 AC1200	2.3.0-4567	3.0.1-4649	28:76:10:0D:10:9E
<input checked="" type="checkbox"/> RTHQ-2-2	Spark Wave 2 AC1200	3.0.0-4594	3.0.1-4649	28:76:10:0C:24:FE
<input checked="" type="checkbox"/> RTHQ-4-1	Spark Wave 2 AC1200	2.3.0-4567	3.0.1-4649	28:76:10:1B:00:FD
<input checked="" type="checkbox"/> RTHQ-2-5	Spark Wave 2 AC1200	2.3.0-4567	3.0.1-4649	28:76:10:0C:50:96

10 エントリを表示 of 19 entries (filtered from 24 total entries)

作成 キャンセル

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 98: 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。

i 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 [66 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 99: サイトの通知の設定

サイト通知設定

リセット 保存

一般

言語
繁體中文

Timezone *
(GMT +08:00) Asia/Taipei

メールアドレス

✉ [redacted] ×

Add email address + ?

アラート

アラートが作成されるたびに、電子メールやSlack通知を受信します。トグルスイッチを使用して、個々のアラートの作成を無効にできることに注意してください。*電子メールの送信*および*Slackの通知*の設定に関係なく、無効なアラートの通知は送信されません。

デバイスに接続できません
このアラートは、1つ以上のデバイスに接続できないときに作成されます。 サイト メールを送る Slackに通知

遅延 *
クリテ...
プロセスの遅れ
20 分 ?

デバイス構成に失敗しました
このアラートは、デバイスのいずれかで構成を更新しようとして失敗すると作成されます。 サイト メールを送る Slackに通知

遅延 *
警告

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、なんら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。
- Metroling 60GHz のリンクがダウンしました — このアラートは、Metroling 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。
- チャン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ン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。
- ファームウェアがダウングレードされました。 — このアラートは、ファームウェ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。
- ファームウェ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。
- ファームウェ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ェアをアップグレードした場合に通知されます。

- ファームウェ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ェ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ェ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せん。

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。

- 101 ページの「無線 SSID の設定」
- 112 ページの「無線設定」
- 115 ページの「一般的なネットワーキングの設定」
- 123 ページの「ローカルネットワーク設定」
- 125 ページの「ファイアウォールの設定」
- 129 ページの「ホットスポットの設定」
- 136 ページの「システムの設定」

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 100: サイト WiFi5 構成

The screenshot shows the 'Wireless SSID' configuration page. The left sidebar contains a menu with items like 'ダッシュボード', 'デバイス', '設定', 'WiFi5', 'WiFi6', 'メトロリンク', 'Gリンク', 'スイッチ', 'MLTG', and 'アクティビティ'. The main content area is titled 'サイトの設定 - WiFiアクセス' and has tabs for 'Wireless SSID', '無線設定', '一般的なネットワークング', 'Local Networks', 'ファイアウォール', 'ホットスポット', and 'システム設定'. Below the tabs, there is a notification: 'In this site menu, affect 1 device(s): SP-W2-AC1200.'. The 'グローバル設定' section has a toggle for '自動的にブロードキャストを無効化'. The 'SSIDリスト' section has a table with columns: SSID, 無線, ネットワークモード, セキュリティ, 暗号化キー, 登録状態, and アクション. The table contains one entry: 'TPS-World' with '5 GHz / 2.4 GHz' for wireless, 'ルータからインターネット' for network mode, 'オープン' for security, 'n/a' for key, and '有効' for status. Below the table is a section for 'ワイヤレススケジューリング' with a table for scheduling, which is currently empty.

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 101: 無線設定

The screenshot shows the 'SSIDを追加' (Add SSID) configuration page. It is divided into three main sections:

- 一般設定 (General Settings):**
 - SSID を有効化:
 - SSID:
 - ブロードキャスト SSID:
 - クライアントアイソレーション:
 - マルチキャスト転送をブロックする: ?
 - 最小許容信号: SNR RSSI ?
 - 最大クライアント数: ?
 - マルチキャスト/ブロードキャスト速度: 5GHz 2.4GHz (一部のデバイスにのみ適用可能)
 - 無線で起動する: 5GHz 2.4GHz ?
 - Local Configurable: ?
- ネットワーク設定 (Network Settings):**
 - ネットワークモード: ?
 - 経由ルート:
 - アップロード速度の制限:
 - ダウンロード速度の制限:
 - AuthPortを有効化: (一部のデバイスにのみ適用可能) ?
- セキュリティ設定 (Security Settings):**
 - OSEN: (一部のデバイスにのみ適用可能)
 - メソッド:
 - RADIUS MAC認証: ?
 - アクセスコントロールリスト:

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に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

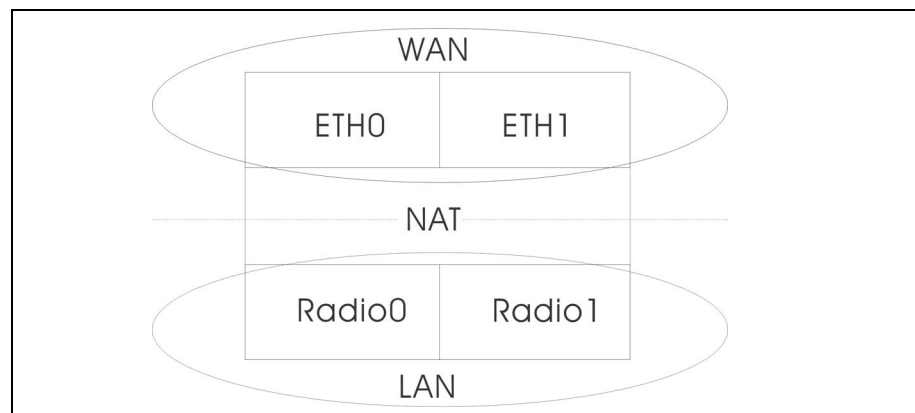
- 無線を起動する - SSID を設置する無線を選択してください。もしデバイスの両方の無線で SSID がアクティブ化されている場合、(SSID がミラーリングされているという意味です) SSID 使用の記録を、どちらかの設定タブから編集してください。この編集は 2.4GHz と 5GHz の記録に反映されます。(デフォルトでは 2.4GHz と 5GHz 両方が有効です)。

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。

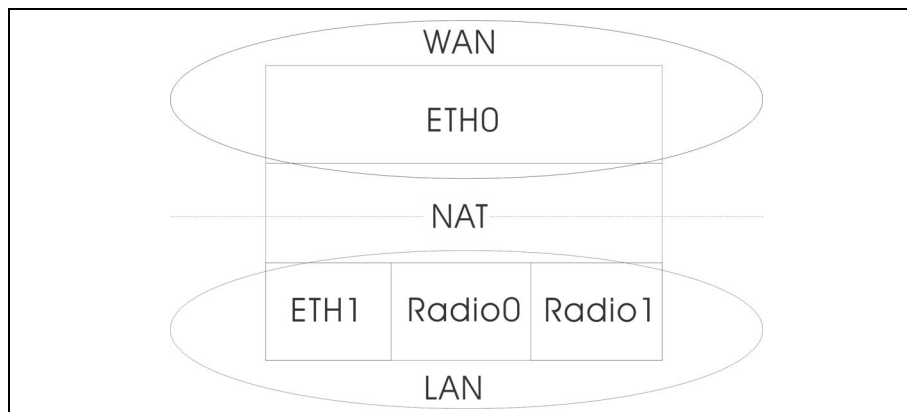
図 102: ブリッジからインターネット



- 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過してインターネットに接続されます。

図 103: 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をサポートします。
- 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、119 ページの「VLAN の設定」に基づいてタグ付けしてください。

i 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、アカウントिंग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 プロテクトドアクセス (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なりません。

RADIUS アカウントिंग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トING情報を得ることもできます。RADIUS アカウントING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 サーバーソフトウェ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 サーバーソフトウェ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 ウェーブ (Wave) の二つのデバイス (サンスポットウェーブ 2、スパークウェーブ 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。

☒ 104: 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 105: WiFi5 無線設定

グローバル設定

バンドステアリング

Airtime Fairness ?

External Radius Enabled

無線LAN(5 GHZ)

電波設定	高度な無線設定
チャンネル帯域幅: 80MHz	最大クライアント数: 0 ?
チャンネル: Auto (all channels) EDIT CHANNEL LIST	プローブ要求データプッシュ: <input type="checkbox"/> ?
Disabled W52 Channel: <input type="checkbox"/>	
最大送信電力: 28 dBm (630 mW) ?	
ビーコン間隔: 100	

無線LAN(2.4 GHZ)

電波設定	高度な無線設定
チャンネル帯域幅: 40MHz	最大クライアント数: 0 ?
チャンネル: Auto (all channels) EDIT CHANNEL LIST	プローブ要求データプッシュ: <input type="checkbox"/> ?
最大送信電力: 30 dBm (1000 mW) ?	
ビーコン間隔: 100	
20/40MHzの共存: <input checked="" type="checkbox"/>	

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

- チャンネルの帯域幅 — 基本の WiFi チャンネル帯域幅は 20MHz ですが、チャンネルを結合させると、40MHz または 80MHz チャンネルを作り上げることができます。チャンネルの帯域幅を広げると、使用できるチャン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 が選択できます。(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)。
- チャンネル — 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ンネルです。使用可能なチャンネルは、無線、チャンネルの帯域幅、規制している国の設定によって異なります。“チャン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ン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ンネルを自動的に選択します。

☒ 106: 5GHz 無線チャンネル

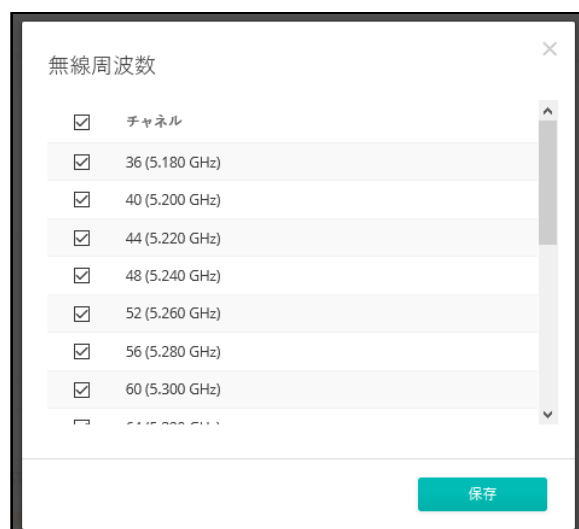
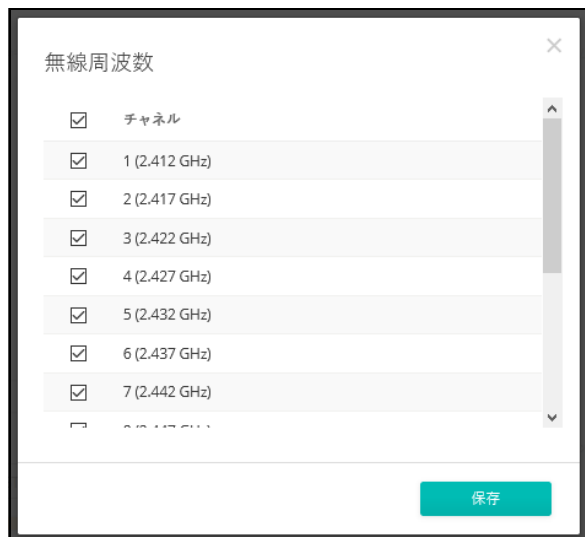


図 107: 2.4GHz 無線チャンネル



- 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、チャンネル 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、送信範囲が広がります。電力を調整すると、カバレッ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 コエグジスト 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 チャン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 108: 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 の設定のみ変更されます。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なりません。デバイスレベルの設定でのみ書き換えられます。

図 109: 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 110: 管理 VLAN の設定

管理VLAN	
管理VLAN	<input checked="" type="checkbox"/>
管理VLANID	100
IP アドレスモード	DHCP
フォールバックIP	192.168.1.20
フォールバックネットマスク	255.255.255.0

- 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ェ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 111: IPv6 設定



The screenshot shows a configuration window titled "IPv6設定". It contains two main settings:

- IP アドレスモード**: A dropdown menu currently set to "DHCP".
- クライアントID**: An empty text input field.

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すべて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 112: 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 のタグging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。

i **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 113: 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。(103 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 114: VLAN を追加する

新しい VLAN の追加

キャンセル 確認

一般設定

VLAN ID 99

ポート

● WAN ポート

● LAN ポート

PPPoEプロフィール

有効にする

Uplink 802.1p

Uplink 802.1p 無効

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 115: ローカルネットワークの設定

The screenshot displays the 'LAN' settings page with two sections: 'デフォルトローカルネットワーク' (Default Local Network) and 'ゲストネットワーク' (Guest Network). Both sections have a '内蔵' (Built-in) toggle switch turned on. The 'デフォルトローカルネットワーク' section includes fields for IP Address (192.168.2.1), Subnet Mask (255.255.255.0), MTU Size (1500), and Smart Isolation (Disabled - Full Access). It also features DHCP settings: DHCP Server (on), DHCP Start (100), DHCP Limit (150), Lease Time (12hr), DNS Server (DHCP Option 6), and DNS Entries. The 'ゲストネットワーク' section has similar fields but with IP Address (192.168.3.1) and Smart Isolation (Internet Access Only). At the bottom, the interface shows two active Wi-Fi networks: 'TPS-World (5 GHz)' and 'TPS-World (2.4 GHz)'.

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せんが、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 116: ファイアーウォールの設定

The screenshot shows the Firewall configuration page. At the top, there is a header 'ファイアーウォール' and a '+ ADD RULE' button. Below this is a table with columns: '有効' (Enabled), '名前' (Name), 'ソースIPアドレス' (Source IP Address), 'ソースポート' (Source Port), '送信先IPアドレス' (Destination IP Address), and '送信先ポート' (Destination Port). The first row is highlighted and has a red box around the '有効' checkbox, which is checked. The name of the rule is 'Allow-Ping'. Below the table, there are configuration options for the selected rule: '対象:' (Target) set to '承諾' (Accept), 'ファミリー:' (Family) set to 'ipv4', 'ソース:' (Source) set to 'インターネット' (Internet), 'プロトコル:' (Protocol) set to 'ICMP', and '送信先:' (Destination) set to '全て' (All). At the bottom, it says 'Showing 1 to 1 of 1 entries' and has a pagination control showing '1'.

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 — 設定されたルールがパケットに一致した場合に実行されるアクションです。(承諾、拒否、ドロップする、マークする、NOTRACK)
- 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)。

ポートフォワード ディング

ポートフォワードディングは、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ェブや 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 117: ポートフォワーディング

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 — ユーザーを定義する名前（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、TCP + 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спек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 118: ARP インспек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 119: DHCP スヌーピング

TRUST DHCP SERVER MAC	TRUST DHCP SERVER IP	REMARK
表示するデータがありません。		

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”を選択しなくてはなりません。(101 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 120: 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あります。

- 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あります。
- 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あります。
- 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（67 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 のゲートウェ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 121: ホットスポットネットワークの設定

ネットワーク設定	
IP アドレス	192.168.182.1
ネットマスク	255.255.255.0
DHCPゲートウェイ	
DHCPゲートウェイポート	
DNS 1	192.168.182.1
DNS 2	
DNS ドメイン名	
DNS Entries	
DNS Mapping	

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 ゲートウェイ — DHCP サーバーにアクセスするために使用するゲートウェイです。
- DHCP ゲートウェイポート — 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、使い慣れた名前でも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 インターフェイ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 122: ホットスポット DHCP サーバーの設定

DHCP サーバー	
DHCP 開始	10
リース期間	3600 秒
DHCP 限度	245

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 123: ホットスポット RADIUS サーバーの設定

RADIUS サーバー	
RADIUS 認証を有効にする	<input checked="" type="checkbox"/>
RadSec の有効(化)	<input type="checkbox"/>
RADIUS サーバーアドレス	RADIUS サーバーの IP アドレスを入力
バックアップ RADIUS サーバーアドレス	RADIUS サーバーの IP アドレスを入力
RADIUS サーバー共有シークレット	<input type="text"/>
RADIUS サーバー auth ポート	1812
RADIUS サーバー アカウンティングポート	1813
認証方法	CHAP
ローカル ID	0
ローカル名	<input type="text"/>
NASID の生成	<input checked="" type="checkbox"/>
NAS ID	<input type="text"/>

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 サーバーアカウントングポート — アカウント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な場合があります。

図 124: ホットスポットキャプティブポータルの設定

キャプティブポータル

HTTPS Login 一部のデバイスにのみ適用可能

ランディングURL

カスタマイズブラッシュアップページ

タイトル

背景カラー

ロゴイメージ

Terms and Conditions

アイドルタイムアウト 秒

セッションタイムアウト 秒

B I U

Enter the (optional) terms and conditions that a user must accept before accessing the internet. Any empty lines will be converted to HTML linebreaks.

選択され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 によるリモートブラッシュアップ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ェ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 125: 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 126: 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 — 一部のデバイス (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 — ハードウェ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、ローカルウェブ 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。

i 注意 : MSP モードと " 常にクラウド設定に従う " (61 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ェアを管理ステーションにインストールする必要がありますので注意してください。

図 127: SSH サーバーの設定

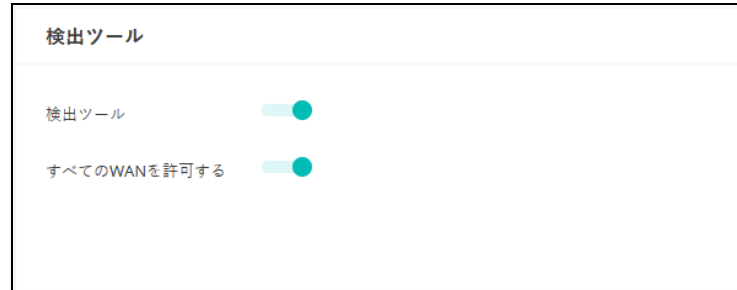
SSH	
SSHサーバー	<input checked="" type="checkbox"/>
SSHポート	22
WANからのSSHへの接続を許可	<input type="checkbox"/>

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 128: 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 129: 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。

ウェブサーバー ウェブブラウザは、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 130: ウェブサーバーの設定

ウェブサーバー	
HTTPポート	80
WANからHTTPへのアクセスを許可	<input checked="" type="checkbox"/>
HTTPSポート	443
WANからHTTPSへのアクセスを許可	<input checked="" type="checkbox"/>

このページでは以下のアイテムが表示されます。

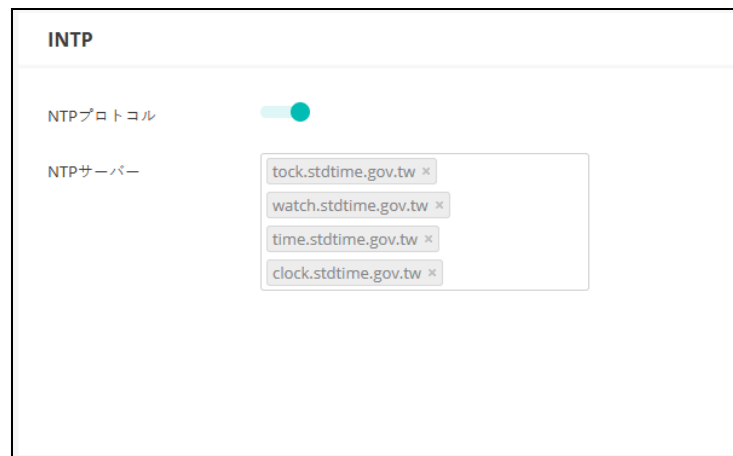
- HTTP ポート — HTTP ウェブブラウザインターフェースで使用される TCP ポートです。(範囲は 1-65535 です。デフォルトは 80 です)。
- WANからHTTPへのアクセスを許可 — WANからのHTTP管理目的のアクセスを許可します。
- HTTPS ポート —HTTPS ウェブブラウザインターフェースで使用される TCP ポートです。(範囲は 1-65535 です。デフォルトは 443 です)。

- 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 131: 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せんが、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 132: SNMP の設定

SNMP	
SNMPサーバー	<input checked="" type="checkbox"/>
連絡先	<input type="text" value="www.ignitenet.com"/>
コミュニティストリング	<input type="text" value="public"/>
IPv6 Write Community	<input type="text" value="private6"/>
場所	<input type="text"/>
すべてのWANのSNMPを許可する	<input checked="" type="checkbox"/>

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 133: リモートログの設定

リモートSYSLOG

リモートSyslog

サーバーIP

サーバーポート

Log Prefix

トラック接続

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 134: ping ウォッチドグの設定

PINGウォッチドグ	
Pingウォッチドグ	<input checked="" type="checkbox"/>
IP アドレス	<input type="text" value="192.168.2.1"/>
フェイルオーバーIPアドレス	<input type="text" value="192.168.10.1"/>
間隔(分)	<input type="text" value="1"/>
失敗回数	<input type="text" value="5"/>

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 135: BLE の設定

BLE SETTINGS	
プローブ要求データプッシュ	<input checked="" type="checkbox"/>
URLを押す	<input type="text"/>

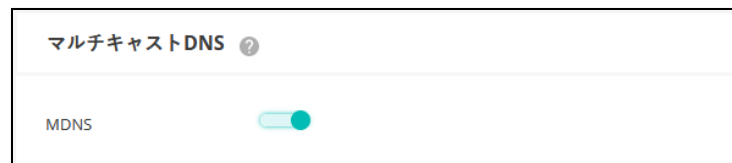
このページでは以下のアイテムが表示されます。

- 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 136: 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 137: 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 138: LLDP 設定



LLDP	
有効にする	<input checked="" type="checkbox"/>
Tx Interval (seconds)	<input type="text" value="30"/>
Tx Hold (number of time(s))	<input type="text" value="4"/>

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 139: iBeacon 設定



IBEACON	
有効にする	<input checked="" type="checkbox"/>
UUID	<input type="text" value="e2c56db5"/> - <input type="text" value="dffb"/> - <input type="text" value="48d2"/> - <input type="text" value="b060"/> - <input type="text" value="d0f5a71096e0"/>
Major	<input type="text" value="21395"/>
Minor	<input type="text" value="100"/>

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 140: SNMPv3 ユーザ設定

SNMP V3 USER		+ 追加			
名前	ACCESS AUTH	AUTH TYPE	AUTH PWD	ENCRYPTION TYPE	ENCRYPTION PWD
表示するデータがありません。					

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。

- 150 ページの「無線 SSID の設定」
- 162 ページの「無線設定」
- 166 ページの「一般的なネットワーキングの設定」
- 173 ページの「ローカルネットワーク設定」
- 175 ページの「ファイアウォールの設定」
- 179 ページの「ホットスポットの設定」
- 186 ページの「システムの設定」
- 195 ページの「OpenRoaming」

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) インターフェイ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 インターフェイスを利用する無線クライアントに対応します。

図 141: 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 — サイトの WiFi デバイスのために設定された SSID インターフェイスのリストです。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 のインターフェイ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。このスケジュールは 2.4GHz と

5GHz のどちらの AP にも対応します。“Add Schedule” 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 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 142: 無線設定

The screenshot shows the 'Add SSID' configuration page with three main sections: General Settings, Security Settings, and Network Settings. At the top right, there are 'キャンセル' (Cancel) and '確認' (Confirm) buttons.

- 一般設定 (General Settings):**
 - SSID を有効化:
 - SSID:
 - ブロードキャスト SSID:
 - クライアントアイソレーション:
 - マルチキャストをユニキャスト変換:
 - 最大クライアント数: ?
 - 最小許容信号: RSSI ?
 - 無線で起動する: 5GHz 2.4GHz ?
- セキュリティ設定 (Security Settings):**
 - メソッド: ▼
 - 暗号化: ▼
 - PMF: ▼
 - RADIUS MAC 認証: ?
 - RADIUS 認証を使用:
 - RADIUS 認証サーバー:
 - RADIUS 認証ポート:
 - RADIUS 認証秘密鍵:
 - バックアップ RADIUS 認証:
 - RADIUS アカウンティングを使用:
 - アクセスコントロールリスト:
- ネットワーク設定 (Network Settings):**
 - ネットワークモード: ▼ ?
 - 経由ルート: ▼
 - アップロード速度の制限:
 - ダウンロード速度の制限:
 - OpenRoaming:
 - Choose Profile: ▼

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)。
- 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。(デフォルトでは 2.4GHz と 5GHz 両方が有効です)。

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。
 - 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。

- 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、アカウントिंग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 アカウントING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トING情報を得ることもできます。RADIUS アカウントING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 サーバーソフトウェ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 サーバーソフトウェ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 アドレスやホスト名前を指定します。
- 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 スタンドアードを含んでおり、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ン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。

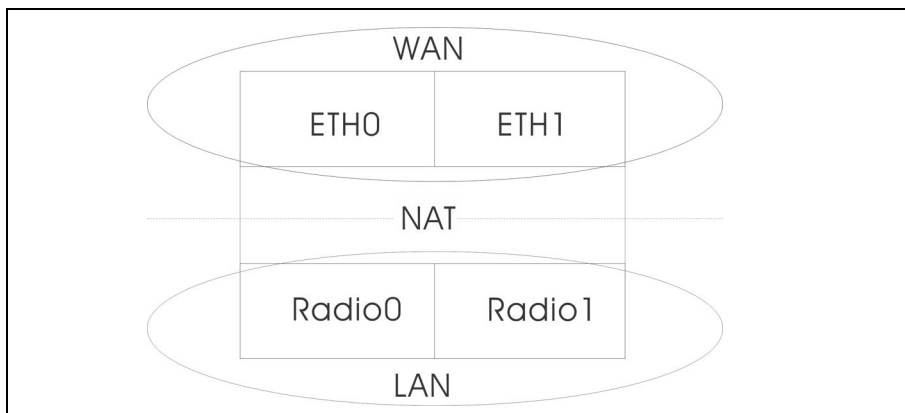
- ダイナミック認証 - Dynamic Authorization Extensions (DAE) を使用すると、RADIUS はすでにネットワークに接続しているクライアントの接続を切断したり、認証を変えたりできます。
- DAE ポート - DAE メッセージを使用するための DUP ポート番号です。(デフォルトは 3799 です)。
- DAE クライアント - RADIUS サーバーの IPv4 アドレスです。
- DAE シークレット - アクセスポイントと RADIUS サーバーが DAE メッセージを暗号化するために共有するテキスト文字列です。

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。

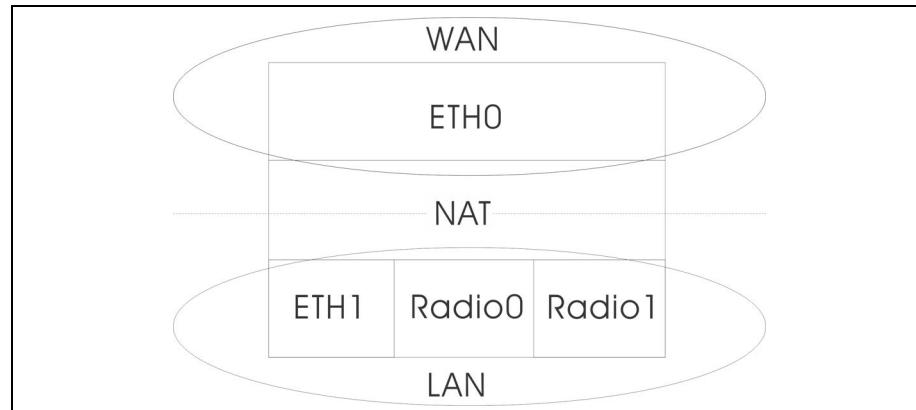
図 143: ブリッジからインターネット



- 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してインターネットに接続されます。

図 144: ルートからインターネット



- 経路制御 - 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をサポートします。
- 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、171 ページの「VLAN の設定」に基づいてタグ付けしてください。

i 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、[195 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([67 ページの「AuthPort アドオンを使用する」](#)を参照)。
- 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。このスケジュールのルールは、全てのサイト AP の 2.4GHz と 5GHz 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 145: 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 146: WiFi6 無線設定

The screenshot displays the WiFi6 wireless settings interface, organized into three main sections: Global Settings, 5GHz Radio Settings, and 2.4GHz Radio Settings.

グローバル設定 (Global Settings):

- バンドステアリング:
- Airtime Fairness: ?
- RF Isolation: ?

無線LAN(5 GHz) (Wireless LAN 5 GHz):

電波設定 (Radio Settings):

- 802.11 モード: 802.11ax
- チャンネル帯域幅: 80MHz
- チャンネル: Auto (all channels) [EDIT CHANNEL LIST]
- アイドルタイムアウト: 300
- 最大送信電力: 20 dBm (100 mW)
- ピーコン間隔: 100
- BSS Coloring: 64
- Interference Detection: 0
- ブロードキャスト速度: 6M
- Target Wake Time:
- OFDMA:

高度な無線設定 (Advanced Wireless Settings):

- プローブ要求データプッシュ: ?

無線LAN(2.4 GHz) (Wireless LAN 2.4 GHz):

電波設定 (Radio Settings):

- 802.11 モード: 802.11ax
- チャンネル帯域幅: 40MHz
- チャンネル: Auto (all channels) [EDIT CHANNEL LIST]
- アイドルタイムアウト: 300
- 最大送信電力: 22 dBm (158 mW)
- ピーコン間隔: 100
- BSS Coloring: 64
- Interference Detection: 0
- ブロードキャスト速度: 5.5M
- Target Wake Time:
- OFDMA:

高度な無線設定 (Advanced Wireless Settings):

- プローブ要求データプッシュ: ?

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、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。

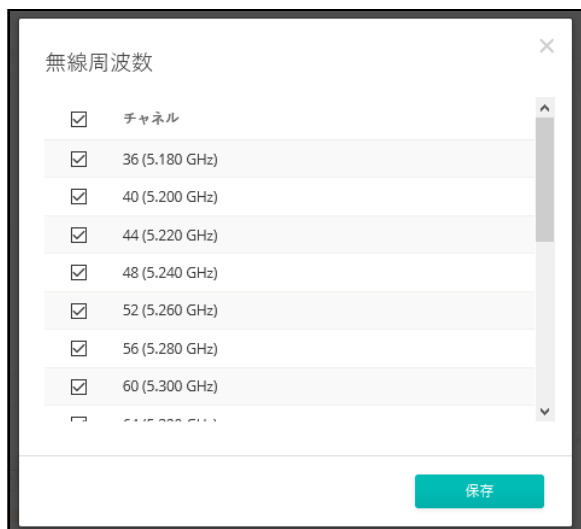
電波設定

- **802.11 Mode** — 無線操作モードを定義します。
 - **無線 5GHz** — デフォルト: 11ax、オプション: 11a、11a+n、11ac+a+n、11ax
 - **無線 2.4 GHz** — デフォルト: 11ax、オプション: 11b+g+n、11ax
- **チャンネルの帯域幅** — Wi-Fi のチャンネル帯域は 20MHz が基本ですが、チャンネルを結合して 40MHz、80MHz、160MHz のチャンネルを作ることで、より高速なデータ転送を実現できます。ただし、チャンネル帯域幅を広くすると、利用できる無線チャンネルの数が少なくなります。利用可能なチャンネル帯域幅は、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
- **チャンネル** — 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ンネルです。使用可能なチャンネルは、無線、チャンネルの帯域幅、規制している国の設定によって異なります。“チャンネルのリストを

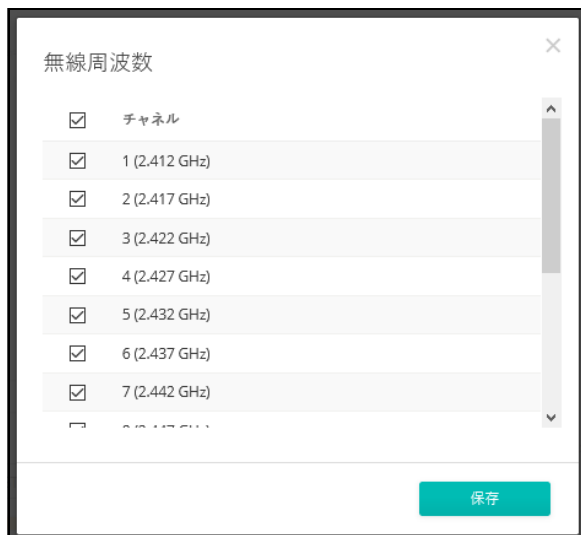
編集する “ ボタンをクリックして、どちらの無線インターフェースでも使用できる特定のチャンネルを選択することもできます。

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ンネルを自動的に選択します。

☒ 147: 5GHz 無線チャンネル



☒ 148: 2.4GHz 無線チャンネル



- 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、送信範囲が広がります。電力を調整すると、カバレッ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。
 - 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
- 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 149: 一般的なネットワーキング設定

The screenshot shows the 'インターネット' (Internet) configuration page. It is divided into several sections:

- インターネット**: A header section with a note: "ここで変更できるのは、インターネットIPアドレスモードと管理VLAN設定のみです。これらの設定の残りは、デバイスレベルの設定で各デバイスにのみ書きできます。"
- 一般設定**: Contains settings for 'インターネットソース' (WAN Port), 'VLAN タグトラフィック' (disabled), 'IP アドレスモード' (DHCP), 'MTU サイズ' (1500), 'フォールバックIP' (192.168.1.20), and 'フォールバックネットマスク' (255.255.255.0).
- 管理VLAN**: A section with a '管理VLAN' toggle switch (disabled).
- DHCP RELAY**: Contains a 'DHCP Relay' toggle switch (disabled).
- IPv6設定**: Contains 'IP アドレスモード' (DHCP) and 'クライアントID' (empty).
- イーサネット**: A section with a note: "一部の設定は、デバイスレベルの構成でデバイスごとにのみオーバーライドできます。"
- WAN ポート用イーサネット設定**: Contains a note: "このポートはこのデバイスのインターネットソースです。"
- LAN ポート用イーサネット設定**: Contains 'ネットワークモード' (ブリッジからインターネット).
- ADVANCED ETHERNET SETTINGS**: Contains 'PoE Out' (enabled).
- VLAN**: A section with a '+ 新しいVLANの追加' button and a table with columns: 'VLAN ID', 'タグありポート', 'タグなしインターフェース', and 'アクション'. The table is currently empty.

表示するデータがありません。

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 の設定のみ変更することができます。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なりません。デバイスレベルの設定でのみ書き換えられます。

図 150: 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 151: 管理 VLAN の設定

管理VLAN	<input checked="" type="checkbox"/>	?
管理VLANID	<input type="text" value="100"/>	?
IP アドレスモード	<input type="text" value="DHCP"/>	▼
フォールバックIP	<input type="text" value="192.168.1.20"/>	
フォールバックネットワーク	<input type="text" value="255.255.255.0"/>	▼

- 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ェ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ワークマスク — 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。

☒ 152: 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

☒ 153: 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を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 154: 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 VLAN ID 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。

i **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 155: VLAN の設定



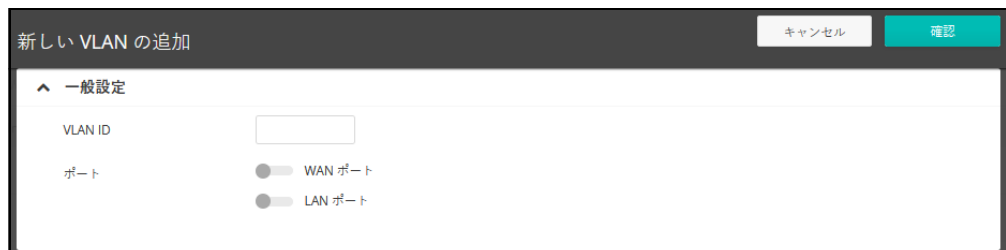
このセクションでは下記のアイテムを説明します。

- 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。(151 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 156: 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 157: ローカルネットワークの設定

The screenshot displays the 'LAN' settings page with two main sections: 'DEFAULT LOCAL NETWORK' and 'GUEST NETWORK'. Each section has a 'BUILT-IN' toggle switch set to 'ON'. The 'DEFAULT LOCAL NETWORK' section includes the following settings: IP Address (192.168.2.1), Subnet Mask (255.255.255.0), MTU Size (1500), Enable STP (disabled), Enable UPnP (disabled), Smart Isolation (Disable (full access)), DHCP Server (enabled), DHCP Start (100), DHCP Limit (150), Lease Time (12hr), and DNS Servers (DHCP Option 6) (empty field with instructions). The 'GUEST NETWORK' section has identical settings, with the IP Address set to 192.168.3.1. At the top left, there is a '+ ADD CUSTOM LAN' button.

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乘せされており、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せんが、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 158: 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 — 設定されたルールがパケットに一致した場合に実行されるアクションです。(承諾、拒否、ドロップする、マークする、NOTRACK)
- 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)。

ポートフォワード ディング

ポートフォワードディングは、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ェブや 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 159: ポートフォワードディング

有効	名前	プロトコル	外部ポート	送信先IPアドレス	送信先ポート	
<input checked="" type="checkbox"/>		TCP+UDP				削除

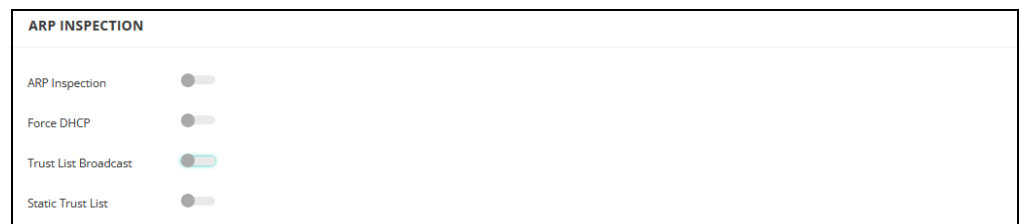
Showing 1 to 1 of 1 entries

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спек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 160: ARP インспек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。

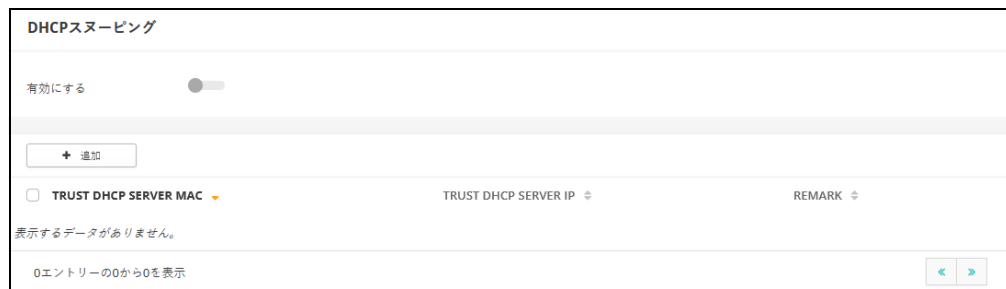
- Trust List Broadcast — 他の AP が信頼できる MAC/IP ペアを学習して、ARP 要求を発行できるようにします。
- Static Trust List — ARP 要求を発行するために信頼されるデバイスの MAC または MAC/IP ペアを追加します。他のネットワークノードは ARP 要求を送信できますが、その IP が異なる MAC で静的リストに表示されている場合、その ARP 要求はドロップされます。

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 161: 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”を選択しなくてはなりません。(150 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 162: 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あります。

- 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あります。
- 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あります。
- 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 (67 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、さらに条件が上乘せされます。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 のゲートウェ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 163: ホットスポットネットワークの設定

ネットワーク設定			
IP アドレス	192.168.182.1	DNS 1	192.168.182.1
ネットマスク	255.255.255.0	DNS 2	
DHCP ゲートウェイ		DNS ドメイン名	
DHCP ゲートウェイポート			

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 ゲートウェイ — DHCP サーバーにアクセスするために使用するゲートウェイです。
- DHCP ゲートウェイポート — 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、使い慣れた名前でも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 164: ホットスポット DHCP サーバーの設定

DHCP サーバー			
DHCP 開始	10	リース期間	3600 秒
DHCP 限度	245		

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 165: ホットスポット RADIUS サーバーの設定

RADIUS サーバー	
RADIUS認証を有効にする	<input checked="" type="checkbox"/>
RADIUSサーバーアドレス	<input type="text" value="RADIUSサーバーのIPアドレスを入力"/>
バックアップRADIUSサーバーアドレス	<input type="text" value="RADIUSサーバーのIPアドレスを入力"/>
RADIUSサーバー共有シークレット	<input type="text" value=""/>
RADIUSサーバーauthポート	<input type="text" value="1812"/>
RADIUSサーバーアカウントングポート	<input type="text" value="1813"/>
RadSecの有効化(化)	<input type="checkbox"/>
認証方法	<input type="text" value="CHAP"/>
ローカルID	<input type="text" value="0"/>
ローカル名	<input type="text" value=""/>
NASIDの生成	<input checked="" type="checkbox"/>
NAS ID	<input type="text" value=""/>

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 サーバーアカウントングポート—アカウント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な場合があります。

図 166: ホットスポットキャプティブポータルの設定

選択され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ェ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 167: 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、タイムゾーンを設定できます。

図 168: 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 — ハードウェ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)

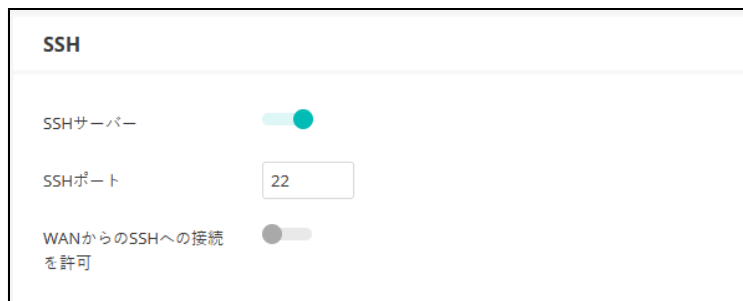
MSP モードを有効にすると、サービスプロバイダーは、「ローカル設定可
能」設定を有効にすることで、特定の無線 SSID 設定をユーザ設定に利用
できるようにするオプションがあります。

i 注意：MSP モードと "常にクラウド設定に従う" ([page 61](#)) 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。

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ェ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 169: SSH サーバーの設定

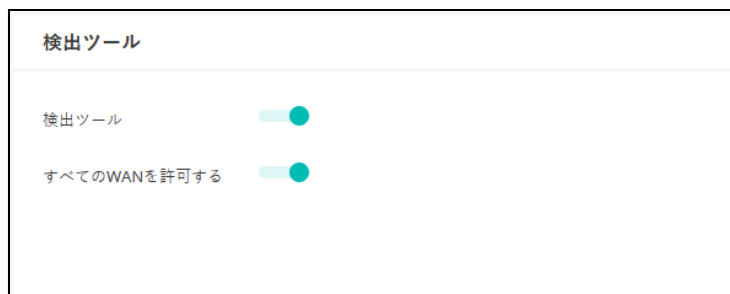


このページでは以下のアイテムが表示されます。

- 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 Edgework 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 170: 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 171: 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せんが、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 172: SNMP の設定



SNMP	
SNMPサーバー	<input checked="" type="checkbox"/>
Write Community	public
IPv6 Write Community	private6
Read Community	ecpublic
IPv6 Read Community	public6

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)

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 173: 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

ウェブサーバー ウェブブラウザは、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 174: ウェブサーバーの設定

ウェブサーバー	
HTTPポート	80
WANからHTTPへのアクセスを許可	<input checked="" type="checkbox"/>
HTTPSポート	443
WANからHTTPSへのアクセスを許可	<input checked="" type="checkbox"/>

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 ウェ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 ウェ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 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 175: リモートログの設定

リモートSYSLOG	
リモートSyslog	<input checked="" type="checkbox"/>
サーバーIP	<input type="text"/>
サーバーポート	<input type="text"/>
Log Prefix	<input type="text"/>
トラック接続	<input type="checkbox"/>

このページでは以下のアイテムを表示します。

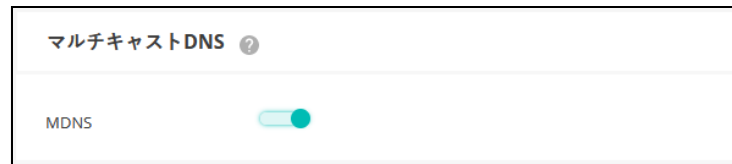
- リモート Syslog — リモートログプロセスへのデバッグ、またはエラーメッセージのロギングを有効/無効にします。

- 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 176: 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 177: 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 178: 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)。

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ダプタサイズします。

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 (151 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 179: OpenRoaming プロファイル

The screenshot displays the configuration page for an OpenRoaming profile named "TEST1". At the top, there is a header "OPENROAMING" with a plus icon and a button labeled "+ ADD CUSTOM OPENROAMING". Below the header, the profile name "TEST1" is shown. The main configuration area includes several sections:

- Internet Access:** A toggle switch is currently turned off.
- Access Network Type:** A dropdown menu set to "Private network: Home and Enter".
- HESSID:** A text input field containing "ff.ff.ff.ff.ff".
- Venue Group:** A dropdown menu set to "Unspecified".
- Venue Type:** A dropdown menu set to "Unspecified".
- Network Auth Type:** A dropdown menu set to "Acceptance of terms and conditic".
- IPv4 Address Type:** A dropdown menu set to "Address type not available".
- IPv6 Address Type:** A dropdown menu set to "Address type not available".
- Operating Class:** A text input field containing "5173".

Below these settings are several sections for adding rules, each with a "+ ADD RULE" button:

- VENUE NAME INFORMATION
- NAI REALM LIST
- OPERATOR FRIENDLY NAME
- CELLULAR NETWORK INFORMATION LIST(PLMN)
- DOMAIN NAME LIST
- ROAMING CONSORTIUM LIST

At the bottom of the form, there are two buttons: "名前を変更" (Change Name) and "削除" (Delete).

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ン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alm・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alm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、MetroInq 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：

- 200 ページの「MetroInq Terragraph の構成」
- 203 ページの「VLAN 設定」

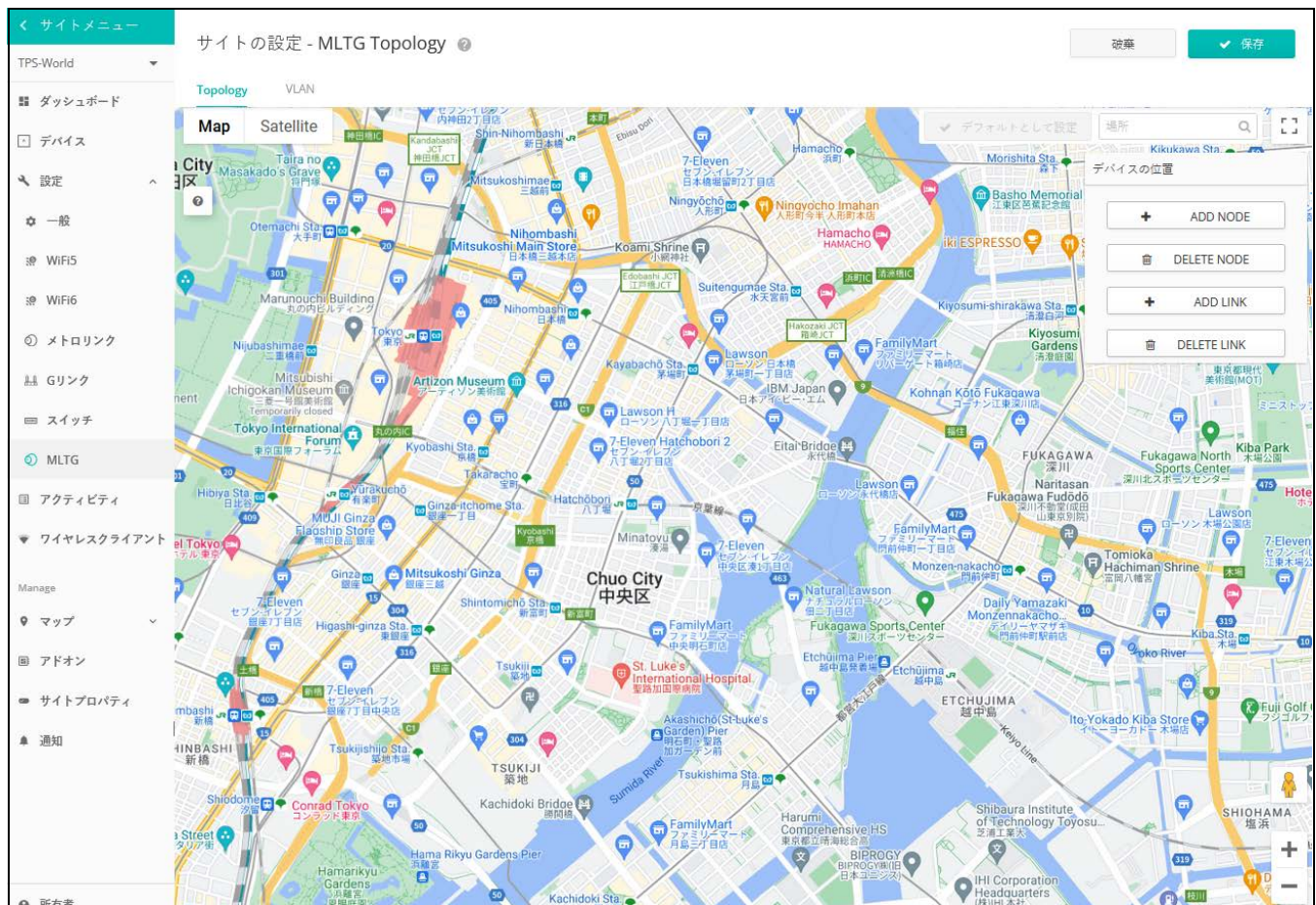
MetroInq Terragraph の構成

MetroInq 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。

i 注意 : MetroInq 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。

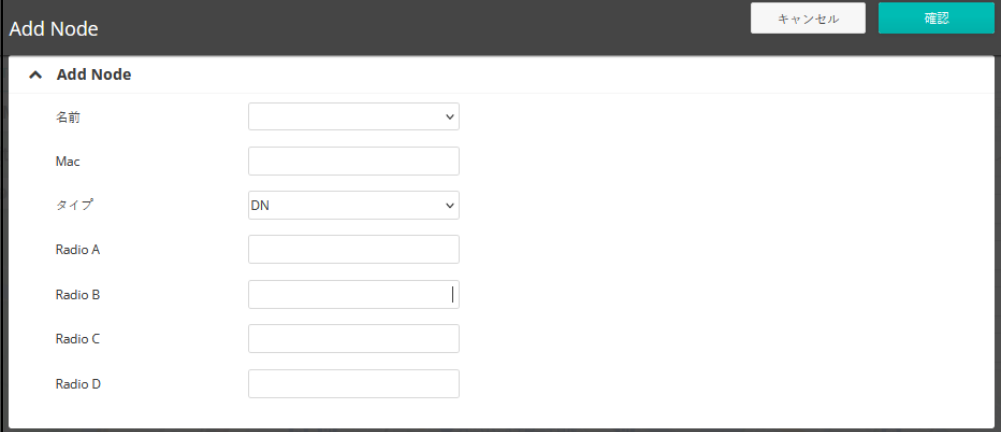
図 180: サイト Terragraph の構成



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 181: Terragraph ノードの追加

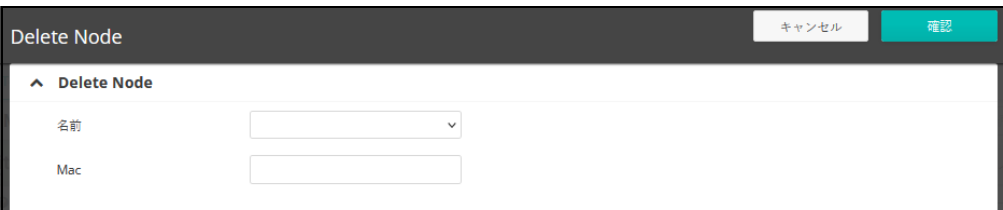


- Name — ノードの名前です。ノードの種類に応じて自動的に定義されますが、後から変更することも可能です。
- MAC — ノードのシステム MAC アドレス。DN の場合、システム MAC アドレスは、デバイスのラベルまたは Dashboard タブで確認できます。CN の場合、無線 MAC をノード MAC として使用します。
- タイプ — ノードをディストリビューションノード (DN) またはクライアントノード (CN) に設定します。
- Radio A/B/C/D — 無線の MAC アドレスです。
- Pop — トポロジー内の PoP ノードは、MLTG-360 のうち 1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

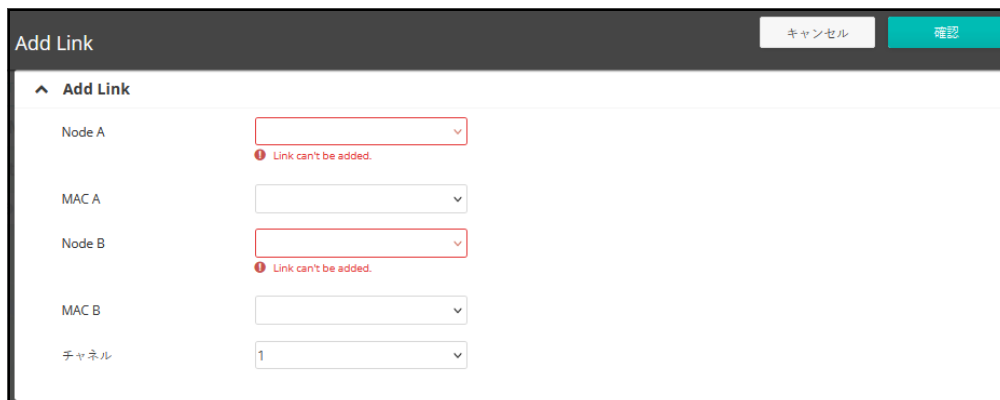
- Delete Node — トポロジーからノードを削除します。ノードを削除する前に、関連するリンクをすべて削除する必要があります。

図 182: Terragraph ノードを削除する



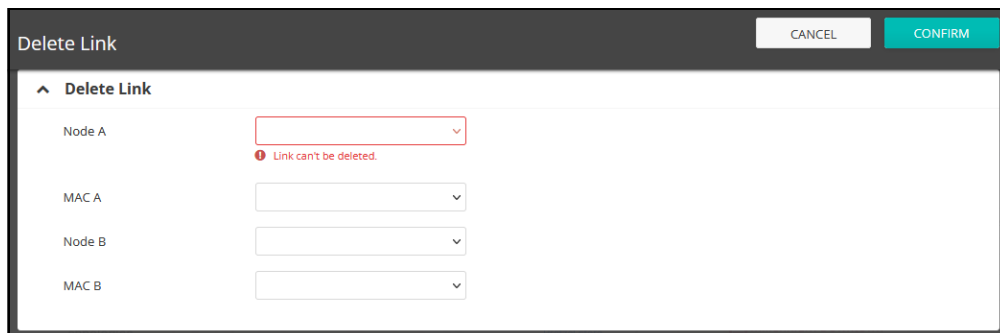
- Name — ノードの名前。
- MAC — ノードのシステム MAC アドレスです。
- Add Link — 2つのノードと対応する無線 MAC を選択し、リンクを確立します。

図 183: 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 — 作業チャンネルを選択します。チャンネル 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 184: 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 185: 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

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。

- [205 ページの「デバイスレベルの設定へのアクセス」](#)
- [207 ページの「デバイスの無線設定」](#)

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。

i 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 186: デバイスレベルの設定にアクセスする



デバイスを管理する

一括再起動の管理 + デバイスを追加 ↑ ファームウェアのアップグレード

アクション 更新 フィルター カスタマイズ エクスポート 検索

	名前	製品	FW	登録状態	登録日時 ↓	クライアント	トラフィック
<input type="checkbox"/>	AP-F1R1	EAP101 EC2107004231	11.1.1	登録済み	2日前 2021-05-11 15:46	0	0 b/秒

ページごとの行: 25 ▼ 1-1 of 1 < >

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 187: 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 188: 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 100 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。

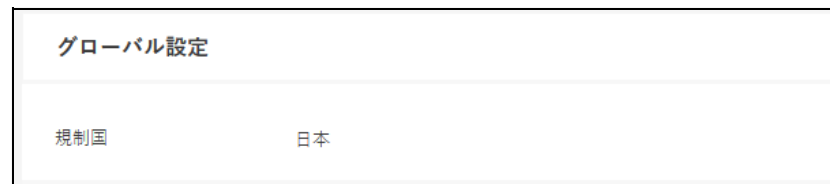
デバイスの無線設定

“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用します。

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、特に明記されない限り、5GHz と 2.4GHz のどちらにも適用します。

グローバル設定

図 189: 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ン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りますので注意してください。

一般的な無線設定

図 190: デバイスの一般的な無線設定

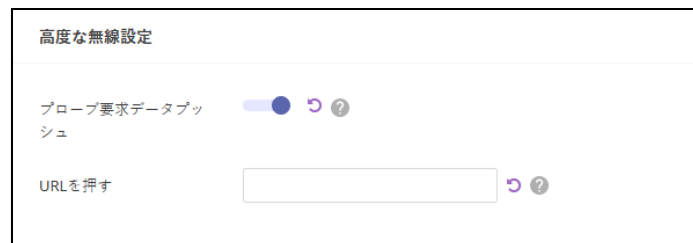


- 無線の有効化 — このインターフェースの無線サービスを有効/無効にします。
- 操作モード — AP 無線が機能するモードを選択します。

- 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

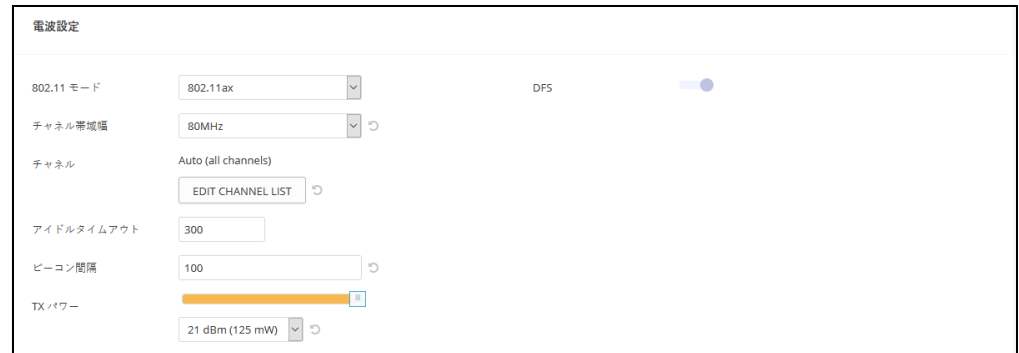
図 191: デバイスの高度な無線設定



- 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ェブアドレスです。

電波設定

図 192: 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
- チャンネル帯域幅 — 基本的な WiFi チャンネル帯域幅は 20MHz ですが、チャンネルを結合して 40MHz または 80MHz チャンネルを作成できます。80MHz チャン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、より広いチャンネル帯域幅を選択すると、使用可能な無線チャン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)。
- チャンネル — 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ンネルです。使用可能なチャンネルは、無線、チャンネル帯域幅、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ン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ン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 193: 5GHz 無線チャンネル

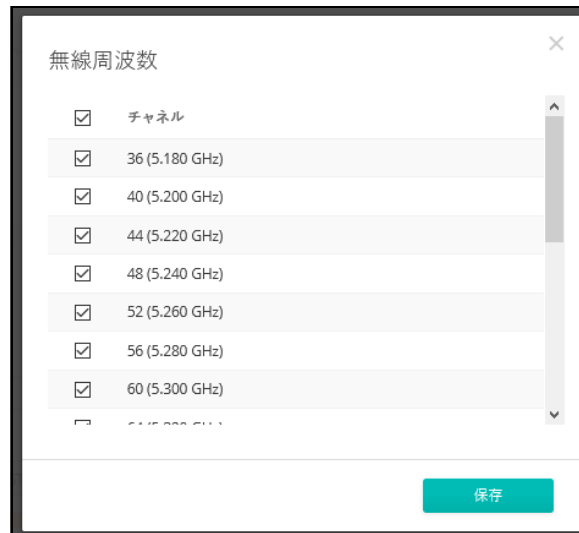
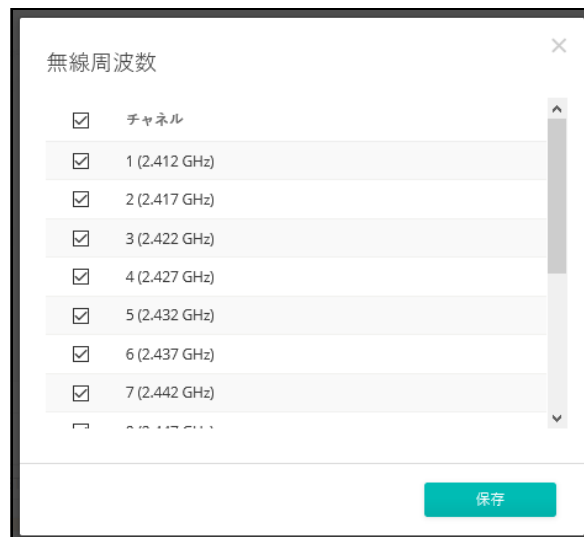


図 194: 2.4GHz 無線チャンネル



- 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、送信範囲は広がります。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る必要があります。(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、アクセスポイントとは 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。ガード間隔の目的は、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ン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 帯域のレーダシステムと同一チャン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 チャンネル帯域幅を同じネットワークと一緒に操作できます。(デフォルトは ON の状態です)。

8

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：

- [214 ページの「デバイスレベルの設定へのアクセス」](#)
- [216 ページの「デバイスの無線設定」](#)
- [223 ページの「システム設定」](#)

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。

i 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 195: デバイスレベルの設定にアクセスする

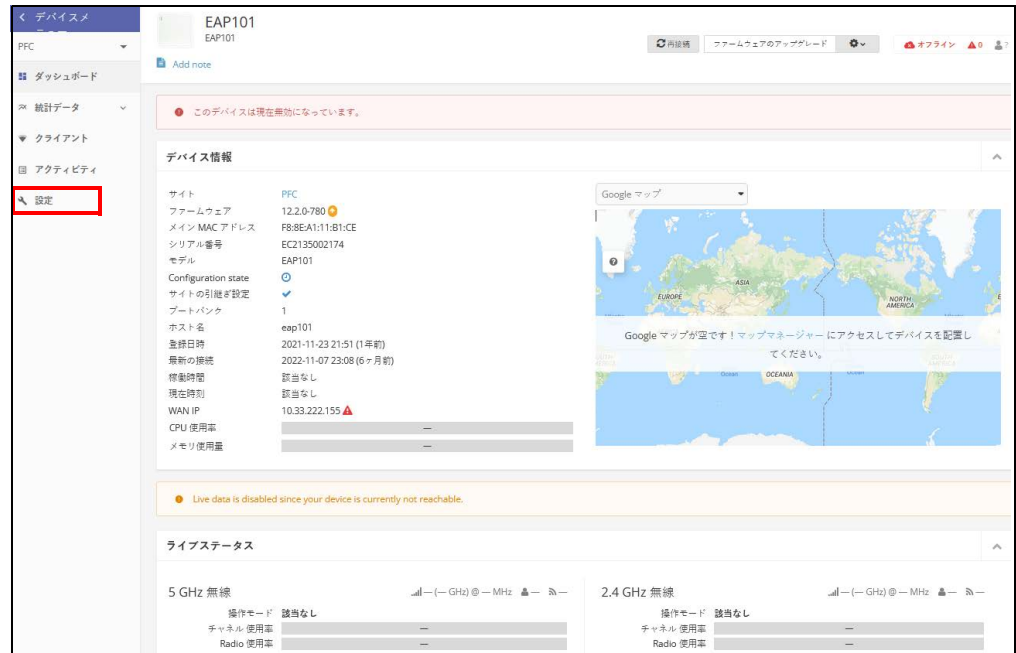


The screenshot shows a 'Manage devices' dashboard. At the top right is a '+ デバイスを追加' button. Below it are navigation icons for 'アクション', '更新', 'フィルター', 'カスタマイズ', and 'エクスポート', along with a search bar labeled '検索'. A table lists devices with columns for '名前', '製品', 'FW', '登録状態', '登録日時', and 'サイト'. The first device, 'EAP101', is highlighted with a red box. Its details are: Product 'EC2135002174', FW '12.2.0-780 (1) ✓' and '12.1.0-746 (2)', Status '登録済み', Registered '1年前 2021-11-23 21:51', and Site 'PFC'.

名前	製品	FW	登録状態	登録日時	サイト
EAP101	EC2135002174	12.2.0-780 (1) ✓ 12.1.0-746 (2)	登録済み	1年前 2021-11-23 21:51	PFC

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 196: 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 197: 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 149 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。

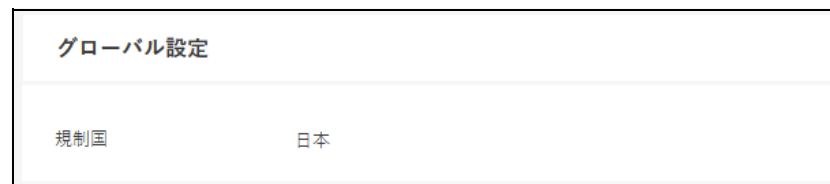
デバイスの無線設定

“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用します。

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、特に明記されない限り、5GHz と 2.4GHz のどちらにも適用します。

グローバル設定

図 198: 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ン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ります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 199: デバイス Mesh 設定

The screenshot shows the 'MESH SETTINGS' configuration page. At the top, there is a toggle for 'Open Mesh' which is currently turned on. Below this are four configuration fields: 'Mesh Id' with the text 'openmesh', 'Mesh Method' with a dropdown menu showing 'オープン', 'Network Behavior' with a dropdown menu showing 'ブリッジからインターネット', and 'Mesh Radio' with a dropdown menu showing '5GHz'.

- 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、特定のチャン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、チャンネル、同じ SSID で動作するように設定します。

一般的な無線設定

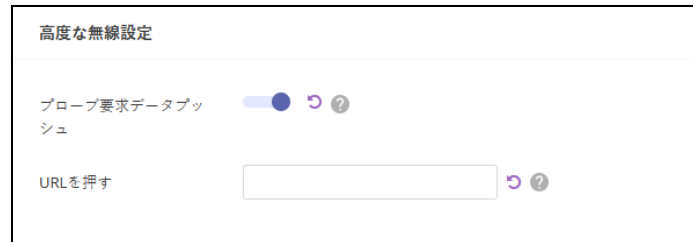
図 200: デバイスの一般的な無線設定



- 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

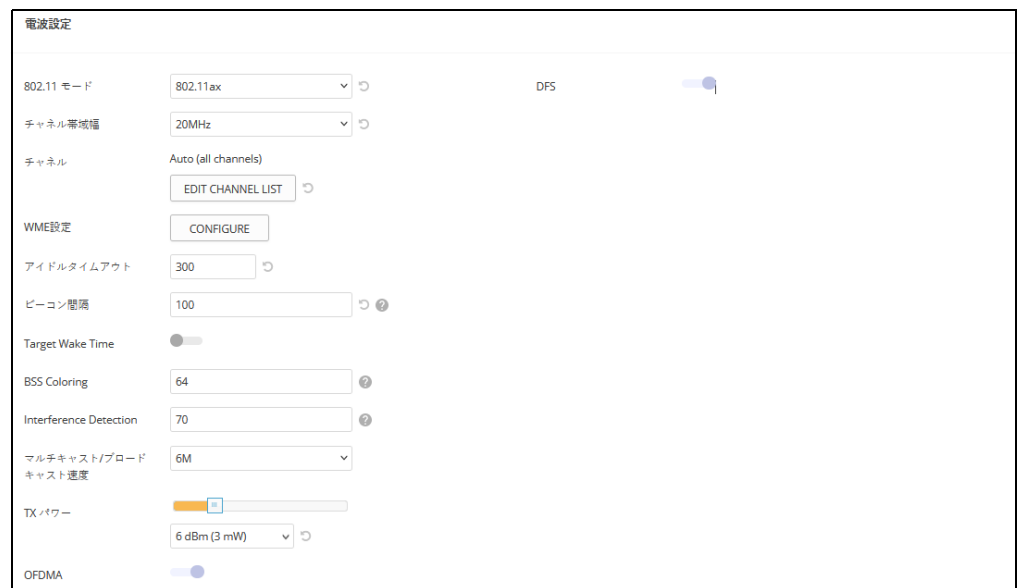
図 201: デバイスの高度な無線設定



- 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ェブアドレスです。

電波設定

図 202: 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
- チャンネルの帯域幅 — Wi-Fi のチャンネル帯域は 20MHz が基本ですが、チャンネルを結合して 40MHz、80MHz、160MHz のチャンネルを作ることで、よ

り高速なデータ転送を実現できます。ただし、チャンネル帯域幅を広くすると、利用できる無線チャンネルの数が少なくなります。利用可能なチャンネル帯域幅は、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
- チャンネル — 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ンネルです。使用可能なチャンネルは、無線、チャンネル帯域幅、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ン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ン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 203: 5GHz 無線チャンネル

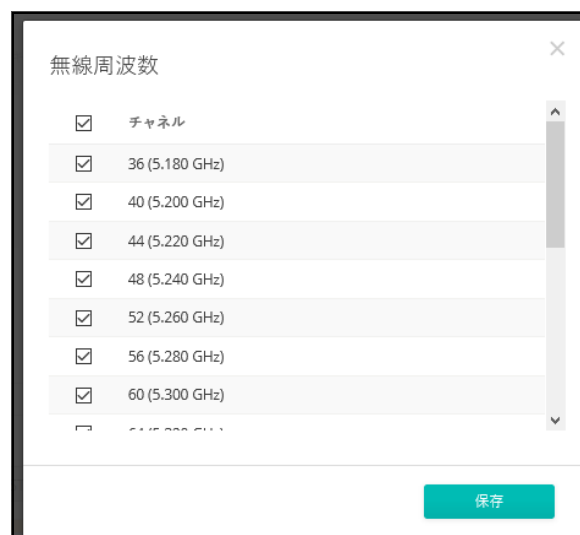
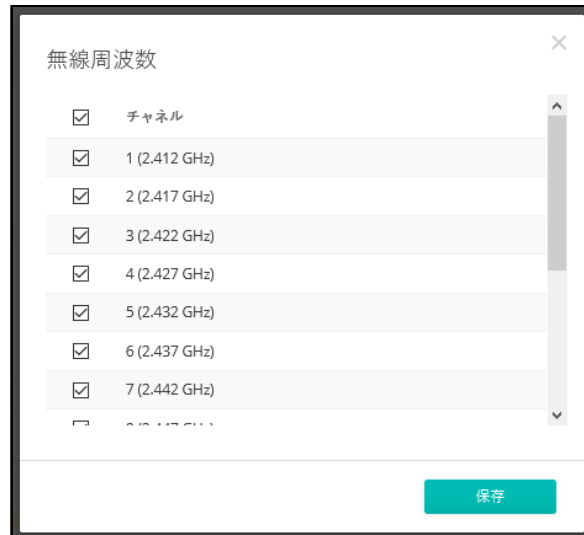


図 204: 2.4GHz 無線チャンネル



- 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、送信範囲は広がります。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る必要があります。(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ン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ン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 205: 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-UUID、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)。

9

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。

- 227 ページの「Metrolinq の設定」
- 227 ページの「無線 SSID」
- 228 ページの「無線設定」
- 237 ページの「クオリティオブサービスの設定」
- 238 ページの「トラフィックコントロール」
- 239 ページの「リンクパスツールの使用」

MetroInq の設定

2.4GHz 及び 5GHz 帯域をサポートする MetroInq 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、MetroInq 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、204 ページの「WiFi 5 デバイス構成」を参照してください。

図 206: MetroInq デバイスのダッシュボード

The screenshot displays the MetroInq device dashboard for device ML-2.5-77. The left sidebar contains navigation options: デバイスメニュー, ML_Site, ダッシュボード, 統計データ, クライアント, アクティビティ, and 設定 (highlighted with a red box). The main content area is divided into sections:

- デバイス情報:** Lists site details such as Site (ML_Site), Firmware (2.4.2-4199), Main MAC Address (28:76:10:20:35:85), Serial Number (AK0700QC9VP), Model (ML2.5-60-35), Configuration state (checked), Site inheritance (unchecked), Boot bank (0), Host name (ml-2.5-77), Registration date (2020-03-19 19:39), Latest connection (2021-05-14 11:13), Uptime (7 days 19 hours 57 minutes 36 seconds), Current time (Sun May 14 03:18:40 2021), WAN IP (192.168.1.77), and connection status (connected).
- 無線ステータス:** Shows the status of wireless networks. The 5 GHz network (ML2.5-5G-Backup) is in Client (WDS) mode with a Local RSSI of -66 dBm and WPA2 PSK (CCMP) security. The 60 GHz network (ML2.5) is also in Client mode with a Local RSSI of -53 dBm and a Remote RSSI of -52 dBm.

無線 SSID

MetroInq 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。60GHz 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、101 ページの「無線 SSID の設定」を参照してください。

図 207: MetroInq デバイスのダッシュボード



オリジン	SSID	無線	DATA VLAN	セキュリティ	暗号化キー	登録状態	アクション
デバイス	ML2.5 60GHZ SSID	60 GHz	該当なし	オフ	n/a	有効	

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 208: MetroInq 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 — MetroInq 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なりません。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ン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、60GHz 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ックユニットは、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。

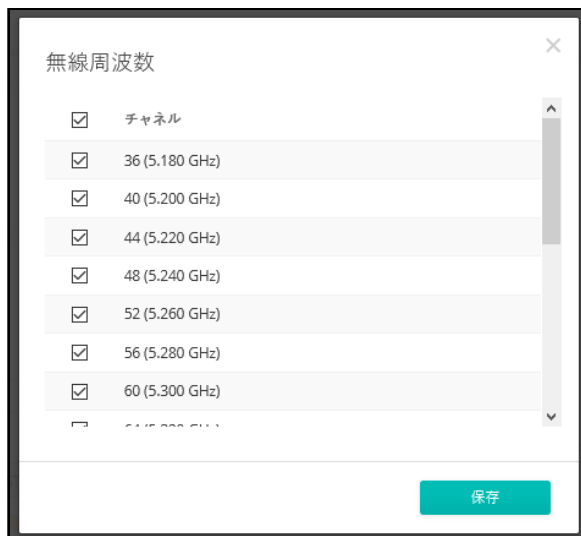
- CCMP (AES) — AES-CCMP は、WPA2 に必要な標準の暗号化された暗号です。(これはデフォルトの設定です)。
- 自動 : TKIP + CCMP (AES) — 使用されている暗号化方式は、リンクパートナーとの関連付けにおいて検出されます。
- キー — 暗号化に使用する WPA2 時前共有キーを設定します。

フィジカル無線設定

- 一般的な WiFi チャンネルの帯域幅は 20MHz ですが、チャンネルを結合して 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、より広いチャンネル帯域幅を選択すると、使用可能な無線チャンネルの数が減少してしまいます。(オプションは 20、40、80MHz です。デフォルトは 80MHz です)。
- チャンネル — 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ンネルです。使用可能なチャンネルは、無線、チャンネルの帯域幅、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ン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ンネルを自動的に選択できます。

図 209: 5GHz 無線チャンネル



- 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、送信範囲が広がります。電力の選択が、カバレッ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。

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 210: Metrolinq デバイス 2.4GHz 無線設定

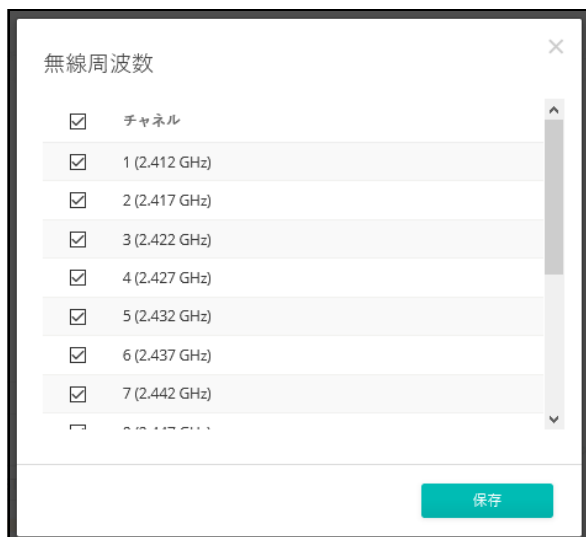
このセクションは以下のアイテムを表示します。

- 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。
- チャンネルの帯域幅 — 基本的な WiFi チャンネル帯域幅は 20MHz ですが、チャンネルを結合して 40MHz または 80MHz チャン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、より広いチャンネル帯域幅を選択すると、使用可能な無線のチャン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)。
- チャンネル — 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ンネルです。使用可能なチャンネルは、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ン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ンネルを自動的に選択します。

図 211: 2.4GHz 無線チャンネル



- 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、カバレッ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 packets をユニキャスト packets 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 212: MetroInq デバイス 60GHz 無線設定

無線LAN(60 GHz)	
一般設定	無線ネットワーク
無線を有効化 <input checked="" type="checkbox"/>	SSID <input type="text" value="igniteNet3-1"/>
操作モード <input type="text" value="Master"/>	暗号化 <input type="checkbox"/>
5 GHz backup <input checked="" type="checkbox"/>	
BACKUP SSID (5 GHz)	
SSID <input type="text" value="igniteNet0-1-5G-Backup"/>	
ブロードキャスト SSID <input checked="" type="checkbox"/>	
暗号化 <input type="checkbox"/>	
電波設定	
MCS Rate <input type="text" value="Auto"/>	
チャンネル帯域幅 <input type="text" value="2160MHz"/>	
チャンネル <input type="text" value="3 (62.640 GHz)"/>	
TX パワー <input type="text" value="14 dBm (25 mW)"/>	
AMPDU <input checked="" type="checkbox"/>	
クライアントアイソレーション <input type="checkbox"/>	
IGMP Snooping <input type="checkbox"/>	
RSSI based failover <input type="checkbox"/>	
Radio beamwidth <input type="text" value="120 degrees"/>	

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 MetroInq 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。MetroInq 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 MetroInq 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 事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)

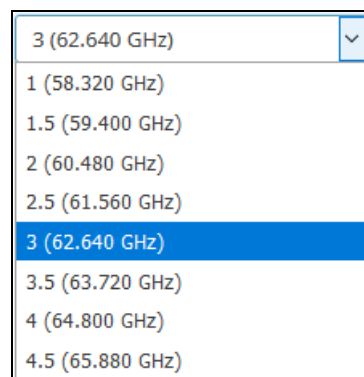
- SSID — バックアップ 5GHz インターフェースのサービスセット識別子の独自の名前を入力します。ポイントトゥーポイントリンクの両端にある Metrolinq ユニットは、同じ 5GHz バックアップ SSID に設定する必要があります。
- ブロードキャスト SSID — ビーコンメッセージで設定された SSID の送信を有効/無効にします。

- 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う。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。
- チャンネルの帯域幅 — 60GHz 無線の場合、2160MHz または 1080MHz のチャンネル帯域幅が選択できます。(デフォルトは 2160MHz です)。
- チャンネル — 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ンネルです。使用可能なチャンネルは、無線、チャンネル帯域幅。及び規制国の設定によって異なります。

図 213: 60GHz 無線チャンネル

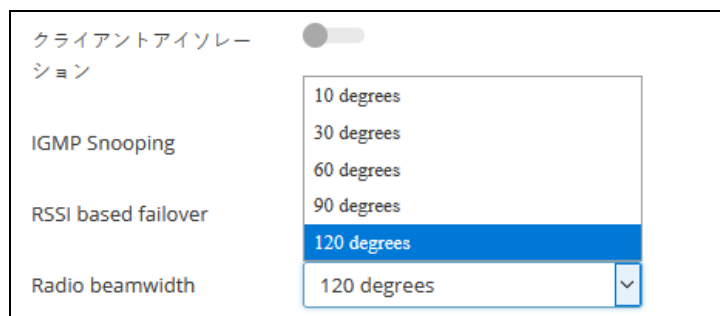


- Tx パワー — 60GHz インターフェースで送信される、無線信号の最大電力を調整します。送信電力が高いほど、送信範囲が広くなり、データレートが高くなります。(電力設定とデフォルトの範囲は、AP モデルと規制国の設定によって異なります)。

- 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 (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 -65 です。範囲は -95 から -25 です)

Metrolinq 60LW、2.5-60-18-BF、10G Tri-Band Omni の設定

図 214: 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となります。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)。

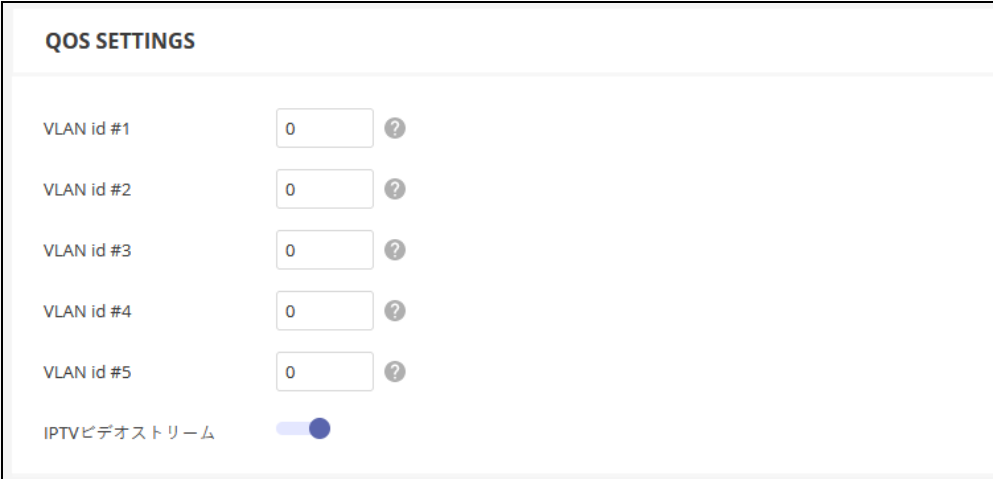
クオリティオブサービスの設定

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となります。

図 215: MetroLinq QOS の設定



QOS SETTINGS	
VLAN id #1	0 ?
VLAN id #2	0 ?
VLAN id #3	0 ?
VLAN id #4	0 ?
VLAN id #5	0 ?
IPTVビデオストリーム	<input checked="" type="checkbox"/>

このページは以下のアイテムを表示します。

- VLAN ID # 5—VLAN 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 216: MetroLinq トラフィック制御の設定

グローバル設定				
Traffic Control Enable <input type="checkbox"/>				
TRAFFIC PROFILE + ADD PROFILE				
オリジン	PROFILE	DOWNLINK (MBPS)	UPLINK (MBPS)	アクション
<input type="checkbox"/> デバイス	Default	0	0	削除
Showing 1 to 1 of 1 entries				« 1 »
TRAFFIC CONTROL + ADD CONTROL				
オリジン	MAC	PROFILE	アクション	
表示するデータがありません。				
0 エントリーの 0 から 0 を表示				« »

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、0–1000Mbps 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 0–1000Mbps 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ァイルを 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。
 - プロファイル — プロファイ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、Metroling 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 217: 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 — PTPP 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。
- チャンネル — リンクが操作する無線のチャンネルです。
- チャンネルの幅 — 設定された無線のチャンネル幅です。
- 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 218: MetroLinq リンクバジェットの結果

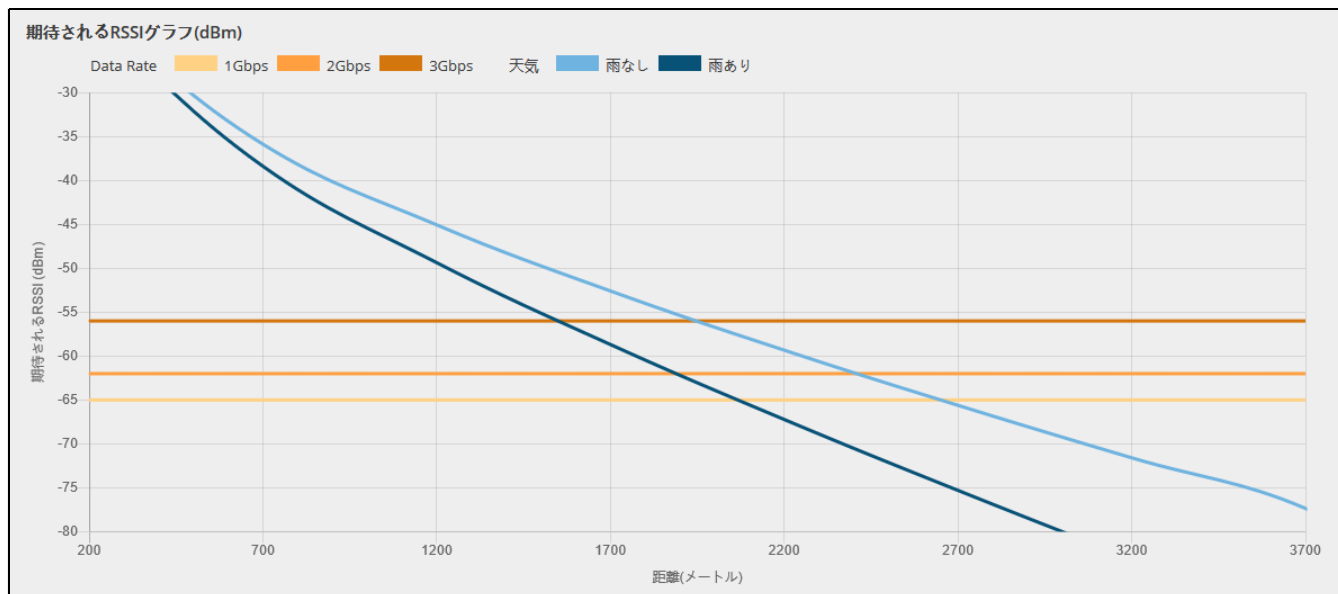


このセクションでは以下のアイテムを表示します。

- 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。
- 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。紫色のグラフは、“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 219: MetroLinq パス予想 RSSI のグラフ



10

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：

- 244 ページの「Terragraph 構成」
- 245 ページの「ネットワーク全般の設定」
- 247 ページの「無線設定」
- 249 ページの「システム設定」

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 220: Terragraph デバイスダッシュボード

The screenshot displays the Terragraph device dashboard for a device named LR-RTK (Edgecore MetroLinq MLTG-CN_LR). The interface includes a left sidebar with navigation options like 'ML_Site', 'ダッシュボード', '統計データ', 'アクティビティ', and '設定'. The main content area is divided into sections: 'デバイス情報' (Device Information) and '無線ステータス' (Wireless Status). The device information section lists various parameters such as site name, firmware version, MAC address, serial number, model, configuration state, and boot bank. The wireless status section shows that the device is connected to a 60 GHz wireless network in Client mode with WPA2 PSK security. A map of the world is also visible, with a notification indicating that the Google Maps API is not configured.

デバイス情報	
サイト	ML_Site
ファームウェア	1.4.3-00335-9d5e29a
メイン MAC アドレス	14:44:8F:E5:7B:93
シリアル番号	EC2223002535
モデル	MLTG-CN_LR
Configuration state	🟢
サイトの引継ぎ設定	✖
ブートバンク	0
登録日時	2022-09-06 15:14 (8ヶ月前)
最新の接続	2023-04-26 16:23 (2分前)
稼働時間	4 日 23 時間 32 分 48 秒
LAN IP	192.168.1.121
管理 IP	該当なし
CPU 使用率	読み込み: 1.25 1.30 1.32
メモリ使用量	使用済み: 230MB 合計 (888MB)

無線ステータス	
🟢 60 GHz 無線	
操作モード	Client
セキュリティ	WPA2 PSK
ローカルMAC	14:44:8F:E5:7B:95

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 221: Terragraph デバイス全般の設定

The screenshot displays the configuration page for a Terragraph device, divided into three main sections:

- POE PORT:**
 - POE Port Role: Bridged with LAN Port (dropdown menu)
- MANAGEMENT PORT SETTINGS:**
 - IP アドレスモード: DHCP (dropdown menu)
 - フォールバックIP: 192.168.1.20 (text input)
 - フォールバックネットマスク: 255.255.255.0 (dropdown menu)
- LAN PORT SETTINGS:**
 - IP アドレスモード: 静的 IP (dropdown menu)
 - IP アドレス: 192.168.1.121 (text input)
 - サブネットマスク: 255.255.255.0 (dropdown menu)
 - デフォルトゲートウェイ: 192.168.1.1 (text input)
 - DNS Entries: 8.8.8.8, 2001:4860:4860:8888 (text input)
 - 管理VLAN: (toggle switch, currently off)

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 222: 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

- チャンネル - ベースステーションモードでは、リンクの作業チャンネル (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 223: 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 retries 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 1: ログインレベル

レベル	重大度名	概要
7	デバツ	デバッグメッセ
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。

11

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。

- 253 ページの「スイッチの設定」
- 254 ページの「ポート設定」
- 256 ページの「VLAN の設定」
- 258 ページの「ネームサーバーの設定」
- 259 ページの「静的 IP ルートの設定」
- 259 ページの「ポートレートの制限 (QoS) の設定」
- 260 ページの「STP の設定」
- 261 ページの「ポートセキュリティの設定」
- 262 ページの「802.1X ポート認証の設定」
- 263 ページの「ACL 設定」
- 265 ページの「スイッチサービスを設定する」
- 266 ページの「ポートのミラーリングの設定」
- 267 ページの「ローカルログインを設定する」
- 268 ページの「システムの設定」
- 268 ページの「ログイン認証を設定する」

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

i **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、ウェブ管理ガイドと、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 224: スイッチデバイスダッシュボード

The screenshot displays the dashboard for an ECS2100-LAB Edgecore 28-Port switch. The left sidebar contains navigation options: デバイスメ, PFC, ダッシュボード, ポート, アクティビティ, and 設定 (highlighted with a red box). The main content area is divided into sections:

- デバイス情報:** Lists details such as Site (PFC), Firmware (1.2.2.31), MAC address (CC:37:AB:6E:EF:88), Serial number (EC1545000005), Model (ECS2100-28T), Configuration state (checked), Site inheritance (crossed out), Boot bank (0), Hostname (ecs2100-lab), Registration time (2021-03-09 17:44), Last connection (2021-05-14 13:52), Uptime (65 days 19 hours 51 minutes 38 seconds), Current time (May 5, 2021 10:33:22Z), WAN IP (10.33.222.114), CPU usage (32%), and Memory usage (46MB of 219MB).
- Map:** A Google Map showing the device location. A message indicates that the map is empty and suggests using the map manager to configure the device.
- ポートステータスの概要:** A grid of 28 port status indicators. Port 24 is highlighted in green, indicating it is 'リンクアップ' (Link Up). Other ports are grey (Link Down) or black (無効/Inactive).

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 225: スイッチポート

スイッチ設定

破棄 保存

ポート Trunk Port Trunk VLAN Port VLAN Name Servers Ip Routes QoS STP Port Security Port Auth ACL Port ACL

EDIT SELECTED 選択済み: なし

Port type: 1000BASE-T

ポート送信	名前	有効	Media Type	Speed Duplex	アクション
<input type="checkbox"/>	1	有効	なし	Auto	編集
<input type="checkbox"/>	2	有効	なし	Auto	編集
<input type="checkbox"/>	3	有効	なし	Auto	編集
<input type="checkbox"/>	4	有効	なし	Auto	編集
<input type="checkbox"/>	5	有効	なし	Auto	編集
<input type="checkbox"/>	6	有効	なし	Auto	編集
<input type="checkbox"/>	7	有効	なし	Auto	編集
<input type="checkbox"/>	8	有効	なし	Auto	編集

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。

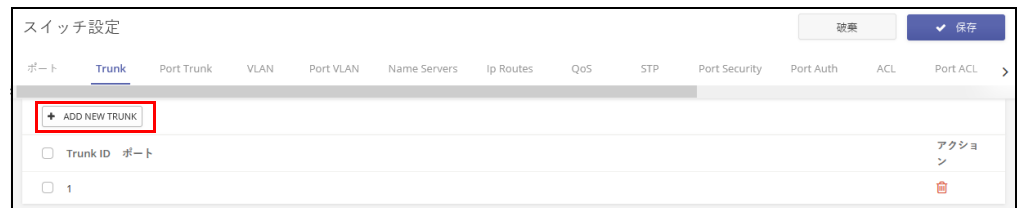
スイッチ間に静的トランクを設定する際は以下のことに注意してください。

- 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、フローの制御、VLAN 割り当てなどにおいて、同じ方法で設定してください。

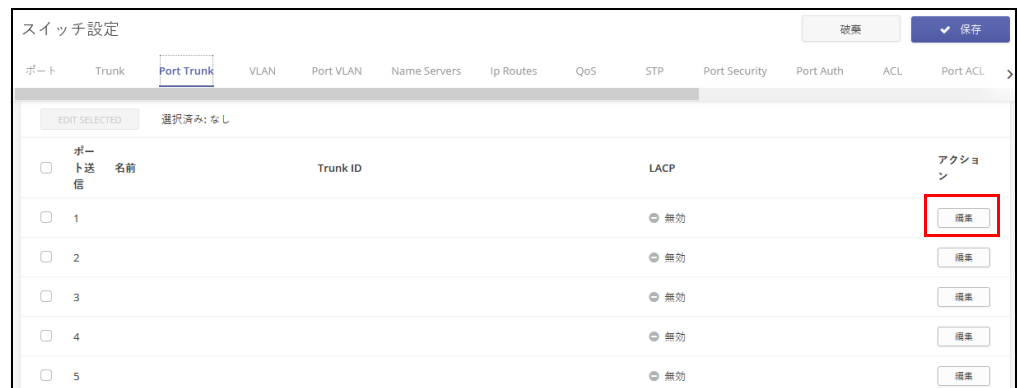
トランクタブをクリックしてから“新しいトランクを追加する”ボタンをクリックして、トランク識別子を作成します。

図 226: 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 227: トランクポートの設定

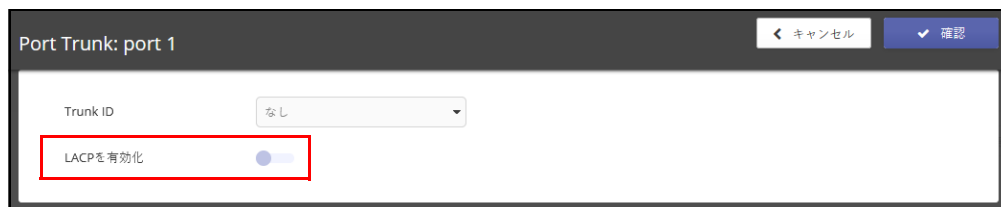


LACP トランク リンク集約のコントロールプロトコル（LACP）を使用すると、2つのスイッチ間に動的トランクを作成できます。LACP で設定されたポートは、別のデバイスの LACP で設定されたポートとトランクリンクを自動的に交渉します。静的トランクの一部としてまだ設定されていない限り、スイッチ上の任意の数のポートを LACP として設定できます。別のデバイスのポートが LACP として設定されている場合、スイッチとそのデバイスはトランクリンクの交渉をします。

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、自動に交渉ができるように設定する必要があります。

図 228: LACP トランクの設定

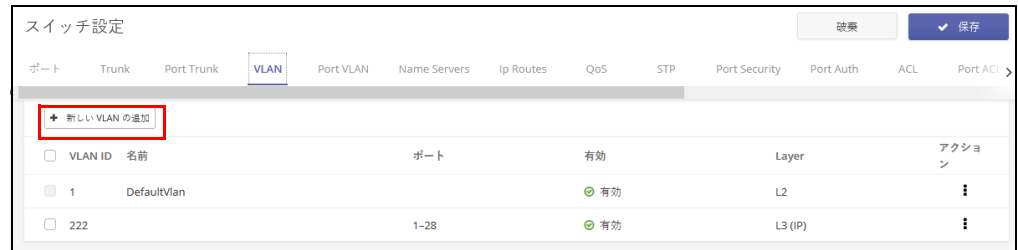


VLAN の設定

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 229: VLAN の設定



VLAN ポートメン バーの追加

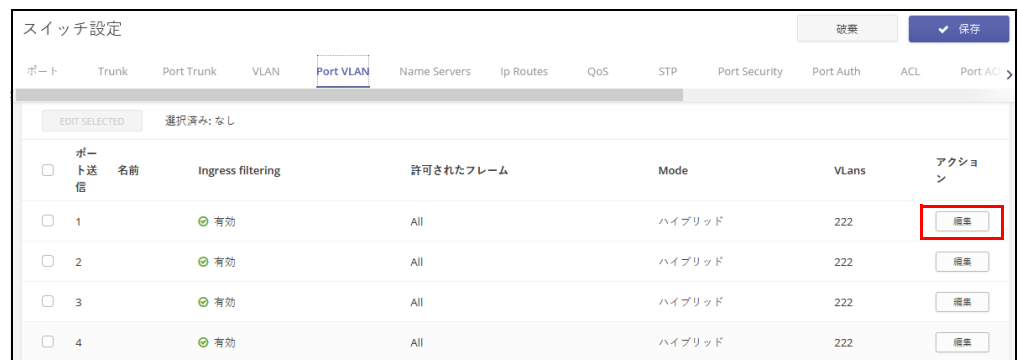
スイッチの VLAN を作成して有効にする際には、各ポートを、参加する VLAN グループに割り当てる必要があります。デフォルトでは、全てのポートが、タグづけされていないポートとして VLAN1 に割り当てられている状態です。もしポートに、一つ以上の VLAN までトラフィックを伝達させ、接続のもう片方にある中間ネットワークデバイスやホストにその VLAN をサポートさせたい場合は、そのポートをタグ付けした状態で追加してください。次にポートを、同じ VLAN にトラフィックを運ぶパスに沿った、別の VLAN 対応ネットワークデバイスに割り当てます。ただし、このスイッチのポートを、1つ以上の VLAN 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 タグging 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 タグ付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 230: 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（ハイブリッドまたは 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 802.1Q VLAN 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 231: VLAN ポートの設定

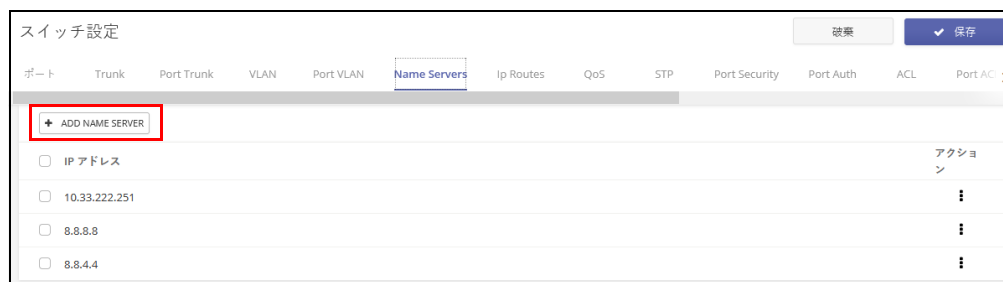


ネームサーバーの設定

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、ドメイン名のサーバーの 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 232: ネームサービスの設定



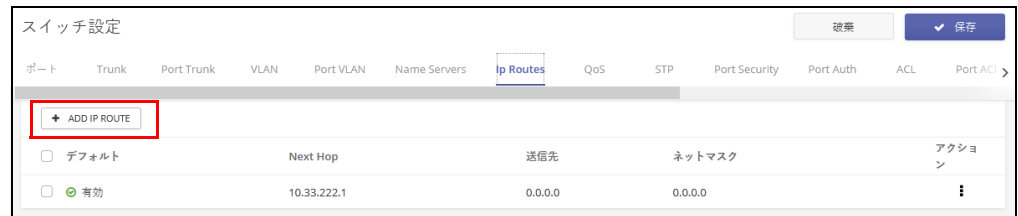
静的 IP ルートの設定

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 インターフェイスを持つ 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 インターフェイ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が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 233: IP ルートの設定



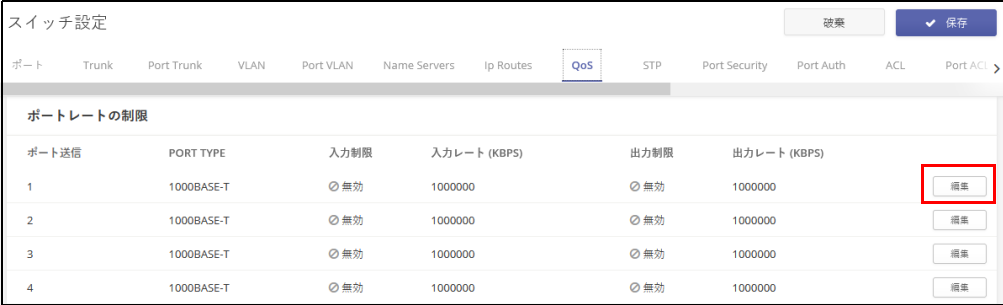
ポートレートの制限 (QoS) の設定

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ェ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 234: ポートレートの制限を設定する



ポート送信	PORT TYPE	入力制限	入力レート (KBPS)	出力制限	出力レート (KBPS)	
1	1000BASE-T	⊗ 無効	1000000	⊗ 無効	1000000	編集
2	1000BASE-T	⊗ 無効	1000000	⊗ 無効	1000000	編集
3	1000BASE-T	⊗ 無効	1000000	⊗ 無効	1000000	編集
4	1000BASE-T	⊗ 無効	1000000	⊗ 無効	1000000	編集

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。

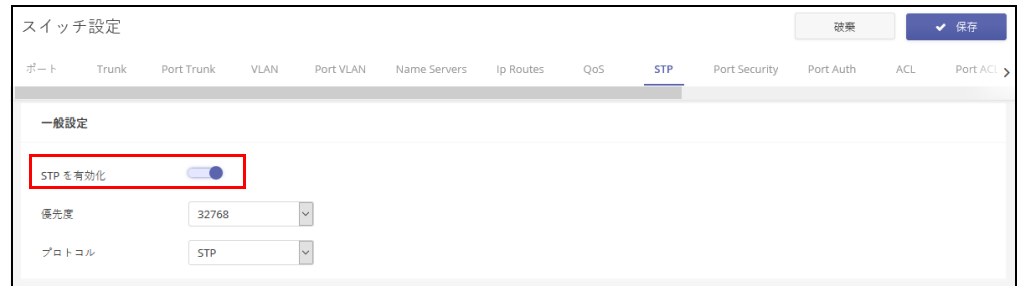
Edgecore スイッチは、以下の三種類のスパニングツリープロトコルをサポートしています。

- 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。

i **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ェブ管理ガイドと CLI リファレンスガイドを参照してください。

図 235: STP の設定



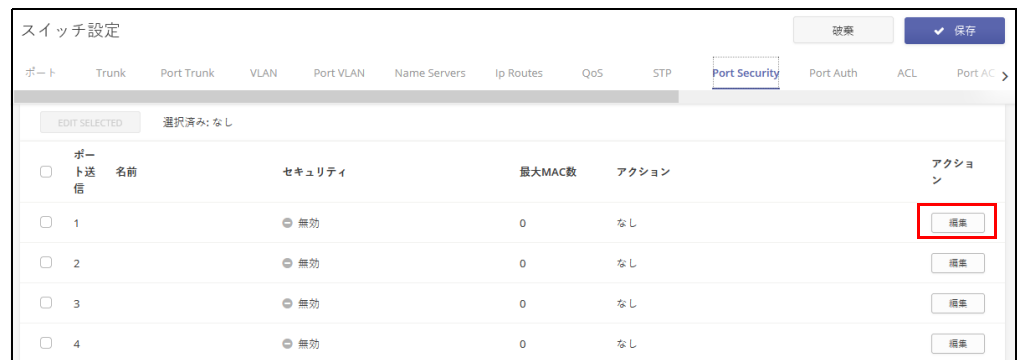
ポートセキュリティの設定

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、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 236: ポートセキュリティの設定



802.1X ポート認証の設定

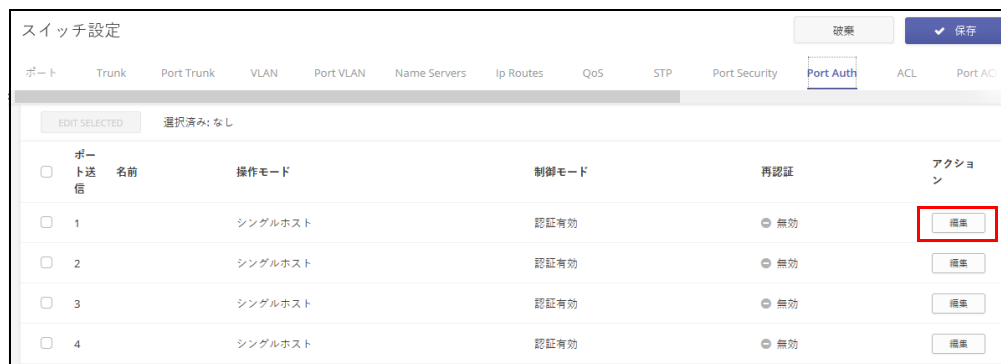
IEEE802.1X(802.1X, または dot1X) 標準は、ユーザ認証の方法として、最初に資格情報を送信することを要求して、ネットワークへの不正アクセスを防止するポートベースのアクセス制御手順を定義します。ネットワーク内の全てのスイッチポートへのアクセスは、サーバーが中心となってコントロールできます。つまり、許可されたユーザは、ネットワーク内のどのポイントからでも、同じ資格情報を使用して認証を得ることができます。

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ァイ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（オーセンティファイケーター）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、268 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 237: 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ブクライア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ァイケーターとして機能する場合、オーセンティファイケーター設定ページで、オーセンティファイ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 238: ポートの認証の設定

i 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ェブ管理ガイド及び 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。

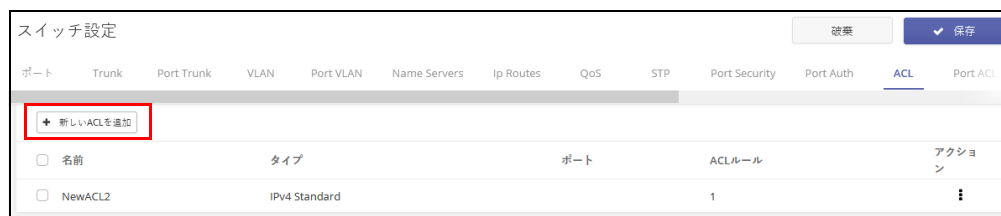
ACL は、IP アドレス、MAC アドレス、またはその他のより具体的な基準によって許可/拒否されるリストです。スイッチは、それぞれの入力パケットを、ACL の条件に従ってテストします。条件を満たすパケットはすぐに受け入れられますが、拒否ルールと一致すると削除されてしまいます。一致するルールがない場合、パケットは受け入れられます。

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、または次のヘッダタイプに基づいて ACL を設定します。
- MAC — ハードウェアアドレス、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。
- ARP ARP — ARP メッセージアドレスに基づいて、ACL を設定します。

図 239: 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 240: 新しい ACL を追加する

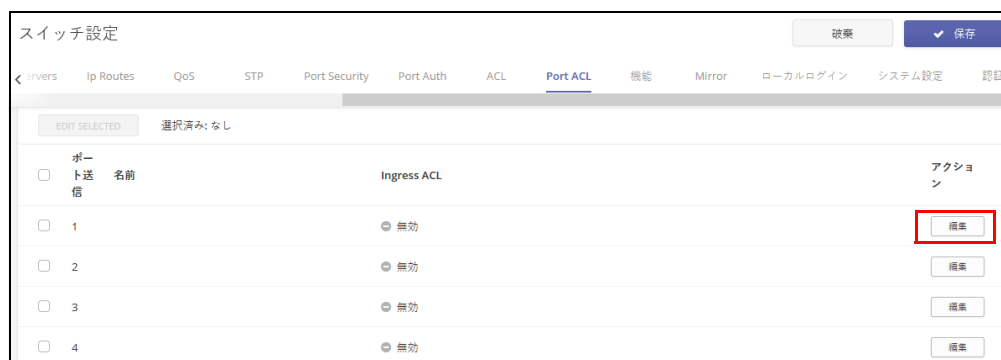


ポートを **ACL** にバインドする

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 241: 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 242: ポートを ACL にバインドする



i 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ェブ管理ガイド及び 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 及びウェ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 CLI にアクセスするために Telnet サーバーを有効にします。

ウェ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 ウェブサーバーを有効にします。

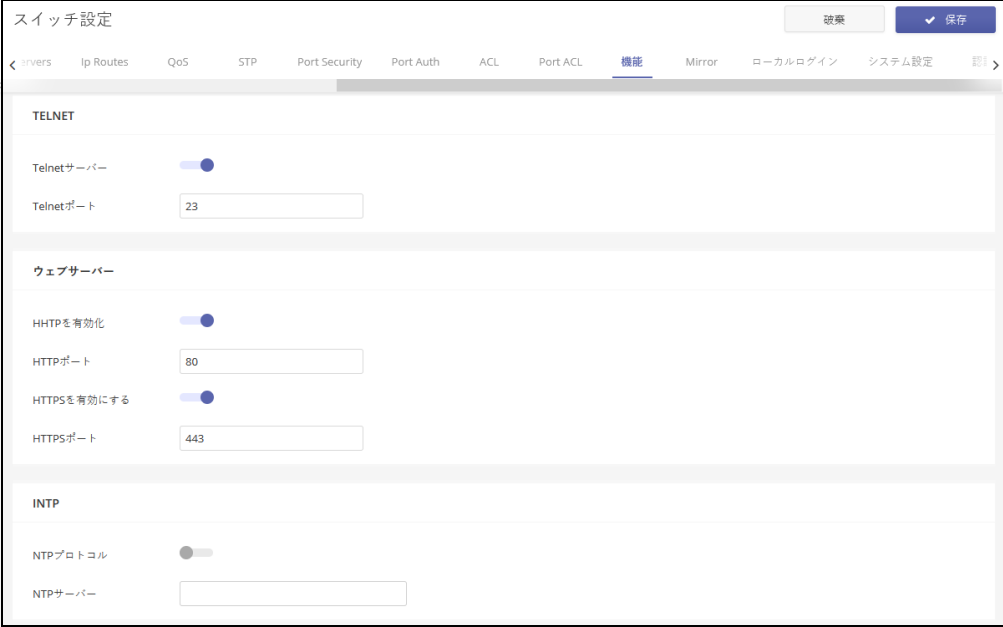
また、セキュアソケットレイヤー（SSL）を介して HTTP を有効にして、スイッチのウェブインターフェースへの安全なアクセス（暗号化された接続）を提供することもできます。

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 つのタイムサーバーの 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 243: スイッチのサービス



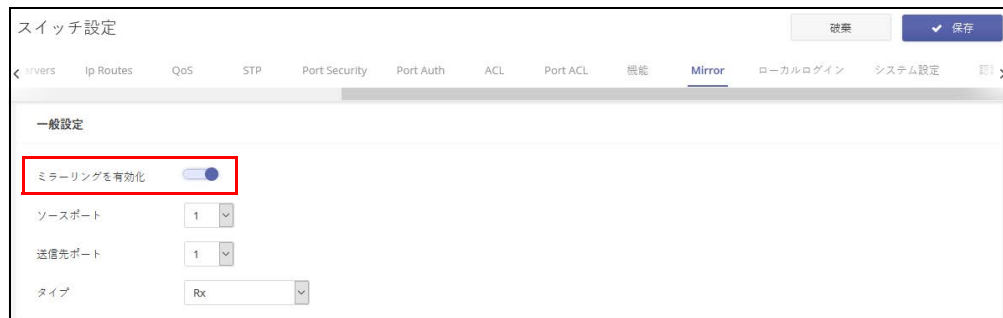
The screenshot shows the 'スイッチ設定' (Switch Settings) page with a navigation menu at the top including 'Invers', 'Ip Routes', 'QoS', 'STP', 'Port Security', 'Port Auth', 'ACL', 'Port ACL', '機能' (Features), 'Mirror', 'ローカルログイン', and 'システム設定'. The '機能' tab is active. The settings are organized into sections: TELNET, ウェブサーバー (Web Server), and INTP. TELNET settings include 'Telnetサーバー' (enabled) and 'Telnetポート' (23). Web Server settings include 'HTTPを有効化' (enabled), 'HTTPポート' (80), 'HTTPSを有効にする' (enabled), and 'HTTPSポート' (443). INTP settings include 'NTPプロトコル' (disabled) and an empty 'NTPサーバー' field. Buttons for '破棄' (Delete) and '保存' (Save) are visible at the top right.

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 244: ポートミラーリング



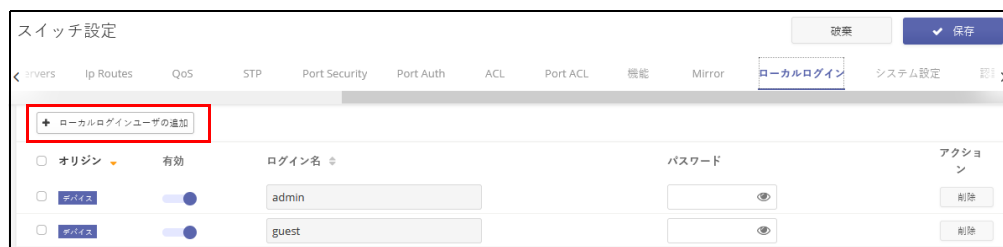
ローカルログインを設定する

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。

i **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 245: 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 246: システムの設定

The screenshot shows the 'System Settings' (システム設定) configuration page. The 'General Settings' (一般設定) section includes the following options:

- Jumboフレームを有効にする**: A toggle switch currently set to 'Off'.
- 場所**: An empty text input field.
- 連絡先**: An empty text input field.
- タイムゾーン**: A dropdown menu currently showing 'GMT+00:00'.

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、ウェブブラウザ、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 247: ゲイン認証

アドレス	アカウントサーバーのUDPポート	認証サーバーのUDPポート	認証タイムアウト	認証の再試行	認証キー	アクション
<input type="checkbox"/>	34.107.161.48	9200	9200	5	2	

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 248: 認証サーバーを追加する

新しいRADIUSサーバを追加する

キャンセル 確認

アドレス: 10.2.3.4

アカウントサーバーのUDPポート: 1813

認証サーバーのUDPポート: 1812

認証タイムアウト: 5

認証の再試行: 2

認証キー:

